

Network Security Concepts and Specifications



Foreword

- With the popularization of the Internet, many enterprises, organizations, government departments, and institutions are building and developing their own information networks. These information systems have become the critical infrastructure of countries and governments. In this context, the entire society is increasingly dependent on networks. Networks have become a powerful driving force for social and economic development and play an increasingly important role. Accordingly, how to ensure network and information security is also important. During data communication, various insecure factors may cause information breach, incompleteness, or unavailability, incurring great negative impact. This course describes the basic concepts and development history of information security, as well as the future development trend of the security industry and technologies, laying a foundation for subsequent security-related courses.
- Network security standards provide guidance and supervision for network security management systems established in various industries. This course describes network security standards in and out of China and the certification process of these standards.

Objectives

- Upon completion of this course, you will be able to:
 - Describe the definition and characteristics of network security.
 - Describe the development history and trend of network security.
 - Describe the ISO 27001 information security management system.
 - Describe Cybersecurity Classified Protection 2.0.

Contents

1. Network Security Definition

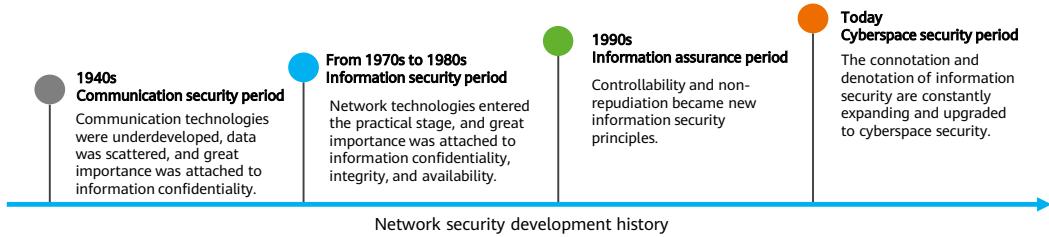
- Overview and Development History of Network Security
 - Common Network Security Threats

2. Future Network Security Trends

3. Information Security Standards and Specifications

Network Security

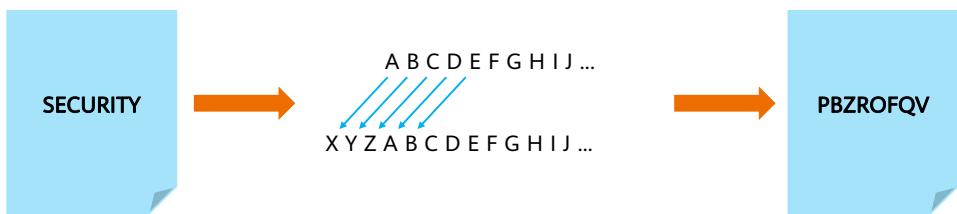
- In a broad sense, network security refers to cybersecurity, which is cyberspace security at a national level. Cyberspace consists of separate and interdependent information infrastructure and networks, including the Internet, telecom networks, computer systems, and embedded processors and controllers.
- In a narrow sense, network security generally refers to taking necessary measures to prevent attacks, intrusions, interference, damage, and unauthorized use of networks and information transmitted over networks, as well as unexpected accidents, to help networks run in a stable and reliable state and ensure the integrity, confidentiality and availability of network information and data.



- In a broad sense, network security refers to cybersecurity, and national laws, regulations, and processes are formulated to provide guidance for government agencies, organizations, industries, and even individuals to jointly build cybersecurity at a national level.
- In a narrow sense, network security includes network security devices and solutions provided by vendors for various industry customers to ensure secure running of various networks, such as enterprise networks. Passing Huawei HCIA-Security certification proves that you are qualified to assist in designing, deploying, operating, and maintaining the network security architectures for small and medium-sized enterprises (SMEs).
- This course describes the security technologies and solutions involved in network security in a narrow sense.

Communication Security Period

- In the 1940s, communication technologies were underdeveloped, and data was stored in different locations. Information system security was limited to physical security of information and cipher-based security of communication (mainly stream cipher). For example, information was stored in a relatively secure place, and unauthorized users were prohibited from accessing the information; cryptographic technologies were used to ensure the security of different information exchange processes such as telephone, telegraph, and fax, thereby ensuring data security. It was crucial to ensure data security during transmission between two locations.
- Information system security was limited to ensuring physical security of information and confidentiality of communication security.



Information Security Period

- The application of computer and network technologies entered into a practical and large-scale use stage, and data transmission could be completed through computer networks.
- The main objective of information security was to ensure information integrity, availability, and confidentiality.

Integrity

- Ensure that information is not tampered with during transmission. If information is tampered with, the receiver can detect the tampering.

Availability

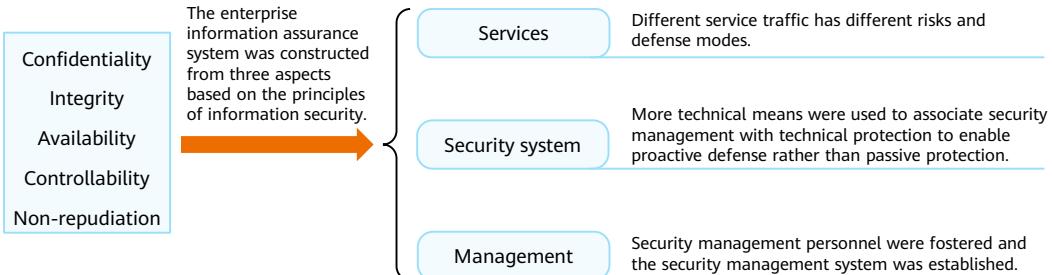
- Ensure that authorized personnel can obtain and use related information assets as required.

Confidentiality

- Ensure that information can be obtained and used only by authorized personnel. Even if attackers steal data, they cannot read correct information.

Information Assurance Period

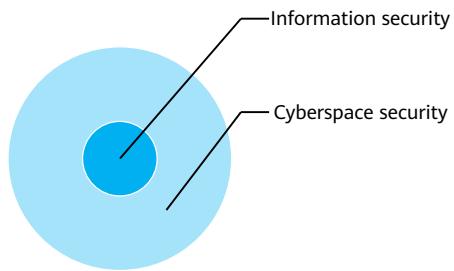
- Controllability and non-repudiation became the new focus of information security in addition to confidentiality, integrity, and availability.
- An enterprise information assurance system was constructed from three aspects: services, security system, and management.



- Since the 1990s, with the rapid development of Internet technologies, information security problems have involved a wider scope of time and space. In this context, controllability and non-repudiation have become the new focus of information security in addition to the traditional three principles of confidentiality, integrity, and availability.
 - Availability: Ensure that authorized personnel can obtain and use related information assets as required.
 - Confidentiality: Ensure that information can be obtained and used only by authorized personnel.
 - Integrity: Ensure that information is not tampered during transmission.
 - Controllability: Implement security monitoring to protect information and its systems against attacks.
 - Non-repudiation: Prevent the information sender or receiver from denying the information.

Cyberspace Security Period

- The connotation and denotation of information security are expanding and upgraded to cyberspace security. The objective is to ensure the system security of the entire cyberspace, including facilities, data, users, and operations.
- National standards and regulations (such as Cybersecurity Classified Protection) are issued to guide enterprises to establish an information security management system.



 HUAWEI

Significance of Building Network Security

Importance	Compliance	Profitability
<p>Network security is critical to national security.</p> <ul style="list-style-type: none">• Network security has become the foundation of economic prosperity, social stability, and national development.• The geopolitical competition of different countries has gone beyond the limitation of physical space and extended to cyberspace.	<p>The building of the enterprise information security management system must comply with network security policies.</p> <ul style="list-style-type: none">• China is constantly improving the information security policy system in terms of policies, regulations, and standards.• Networks of government agencies and enterprises must comply with classified security protection specifications.	<p>By building network security, enterprises can reduce losses caused by network attacks.</p> <ul style="list-style-type: none">• As network attacks become a service, enterprises face more network risks.• Enterprises will suffer huge losses if their application systems break down and user information leaks due to network attacks.

Contents

- 1. Network Security Definition**
 - Overview and Development History of Network Security
 - Common Network Security Threats
2. Future Network Security Trends
3. Information Security Standards and Specifications

Network Security Threats



Hackers are the initiators of information security incidents. They attack networks to obtain useful information or substantial rewards, which is usually accompanied by criminal acts.



Vulnerabilities are the root cause of all security problems. New vulnerabilities increase rapidly, while vulnerability discovery penetrates from the application layer to bottom-layer components, and even to the architecture layer, expanding the impact.



The number of **ransomware attacks** continues to grow. As the attack threshold is lowered, multiple ransom policies may become the attack mainstream. The requested ransom becomes higher, and phishing and remote desktop protocols are the main media of ransomware attacks.



Information breach is the most common information security incident on networks. By implanting Trojan horses or installing eavesdropping devices on user devices and using other means, hackers can mine the collected information and analyze personal contact information and behavior from photos, emails, video conferences, and social materials.



DDoS attacks are becoming a service and a new means for attackers to gain profits. Attackers obtain economic benefits by selling cybercrime toolkits and services, and cybercrime is rising.



Supply chain threats and attacks are increasing. Because a supply chain involves a large number of downstream enterprises and users, successful attacks may cause extensive impact.

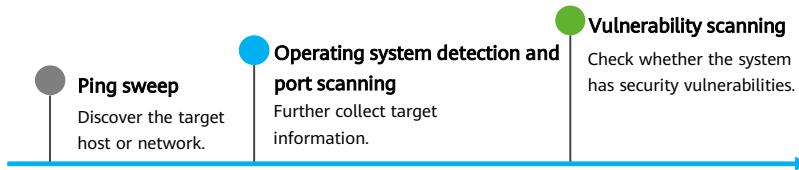
Hacker

- A hacker is a person who has a deep understanding of software design, programming, and computer science.
 - In terms of computer software, hackers are a group of people who are particularly interested in computers and computer network systems and have a deep understanding of them.
 - In terms of amateur computer technology, hackers refer to amateurs who study how to modify computer-related products.
 - In terms of information security, hackers refer to people who study how to intellectually access computer security systems. They use public communication networks, such as telephone systems and the Internet, to log in to others' systems in an unauthorized way and operate the systems.



Vulnerability

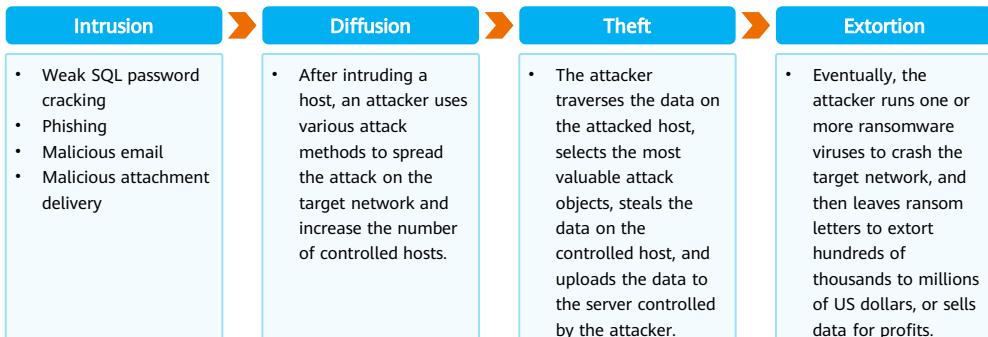
- A vulnerability is a defect or weakness in the hardware, software, or protocols of computer systems or in system security policies.
- Information security incidents, such as permission bypass, permission escalation, execution of unauthorized instructions, data disclosure, and DoS attacks, may occur in information systems.
- On a live network, engineers perform vulnerability scanning to detect the vulnerability of the target network or host. It can be used for attack simulation and security audit.



- Vulnerabilities pose the following security threats to network systems:
 - Permission bypass and permission escalation are mainly used to obtain expected data operation capabilities, for example, increasing the permissions of common users and obtaining administrator permissions.
 - In a DoS attack, the attacker obtains the control rights of certain services in the system to stop the services.
 - Data disclosure is mainly caused by hackers' access to unauthorized data or confidential information, such as reading restricted files and publishing server information.
 - The execution of unauthorized instructions forces a program to execute input content as codes. This obtains the access permission of a remote system or higher permissions of a local system. Examples are SQL injection and buffer overflow.
- Vulnerability scanning process: Perform ping sweep to determine the IP address of the target host. Conduct port scanning to identify open ports on the target host. Perform operating system detection based on the port scanning result. Finally, conduct vulnerability scanning based on obtained information.

Ransomware Attack

- A refined oil pipeline operator was attacked by ransomware, and computers that manage the pipeline were affected. As a result, some fuel supply systems were forced to go offline. The incident was a devastating network attack on critical infrastructure.
- Ransomware attack process



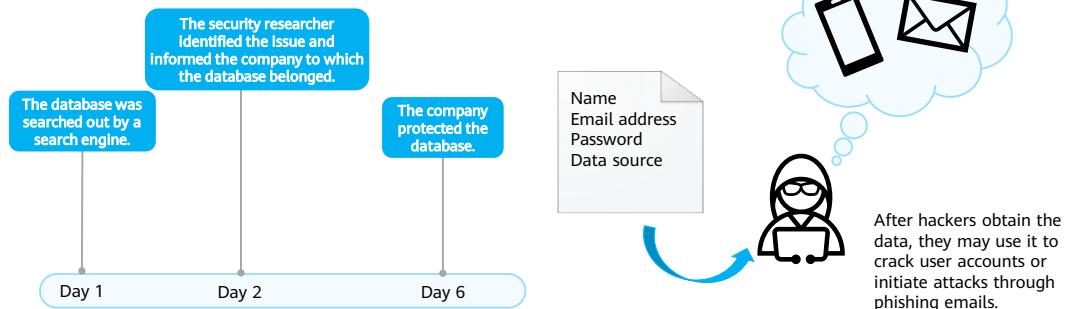
15 Huawei Confidential



- Attack process:
 - The upstream developer of ransomware compiles complete ransomware and authorizes a downstream attack organization to use the ransomware. The developer may charge the rental or authorization fee.
 - The downstream organization may maintain a phishing website, upload ransomware to the website, and lure victims to access it.
 - The downstream organization may send the phishing website link to victims through phishing emails or other channels.
 - A victim accesses the phishing website containing ransomware.
 - The victim proactively downloads ransomware at the phishing link or passively downloads ransomware to the local host due to remote code execution.
 - The victim proactively runs ransomware locally or the ransomware silently runs due to remote code execution. The ransomware encrypts local disk files and found shared network files, and leaves a ransom letter on the victim's computer, which instructs the victim to pay a ransom.
 - The victim pays the ransom to the downstream agency according to the instructions in the ransom letter.
 - The downstream agency of the ransomware launders the ransom money to conceal the upstream developer and downstream attack organization.
 - The downstream attack organization sends the decryption program to the victim, and the victim restores encrypted files.

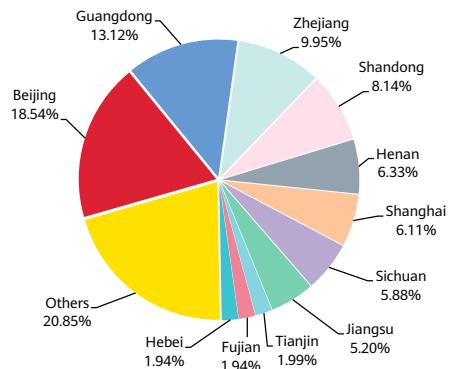
Information Breach

- A security researcher found that an unprotected database exists on the network. The database collected about 5 billion pieces of data and could be accessed without identity authentication. The researcher informed the company to which the database belonged. Three days later, the company protected the database, but the data may have been leaked.



DDoS Attack

- Hackers (individuals or organizations) initiate distributed denial of service (DDoS) attacks to exhaust the network or system resources of the target server. As a result, the services of the server are temporarily interrupted or stopped, and authorized users cannot access the services.
- With the emergence of the Internet of Things (IoT), more and more IoT devices are connected to networks. Against this backdrop, hackers can quickly launch large-scale DDoS attacks by exploiting device hardware or management vulnerabilities. Hackers use DDoS attack resources to provide capability leasing services, and attackers who lack technical capabilities can customize attacks as required. This has become the mainstream way for hacker organizations that have DDoS attack capabilities to gain profits.

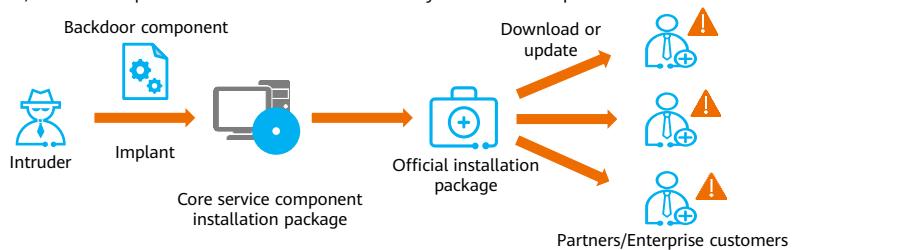


2018 Website Attack Situation and Attack Gang Mining and Analysis Report of CNCERT
Distribution of IP addresses of servers that undergo website attacks in China (by province)



Supply Chain Attack

- Supply chain attacks are network attacks launched against supply chains, and the attack impact is extended to relevant partners and enterprise customers through supply chains.
- The incident of a supply chain attack on products of a famous information system management and network monitoring software development company was unveiled, drawing global attention. The company suffered the supply chain attack launched by an advanced persistent threat (APT) attack organization. The installation package of the company's platform software was implanted with a backdoor, and all customers using the software were at the risk of being intruded. This software is a piece of management platform software that provides real-time monitoring and analysis for network devices. Its customers include government, military, education agencies, and other important institutions and internationally renowned enterprises.



- The disclosure of supply chain attacks exposes key issues in the software industry such as insufficient association, fragile ecosystems, hypotheses in system design, and direct receipt of updates from known "trusted" vendors.
- Supply chain attack means:
 - Steal authorized developer accounts to release applications with similar names or with malicious code added to replace official applications.
 - Launch malicious applications or code through third-party download sites, communities, software alliances, and black market organizations.
 - Pollute upstream SaaS services, poison open-source software repositories, disguise as well-known software, domain names, and websites, and intrude legitimate websites to replace download links.
 - Hijack the domain name of the official update download address, and poison DNS resolution, download nodes, and CDN and P2P caches.
 - Intrude the official update and upgrade system, intrude software and hardware development companies, and implant malicious code.
 - Hijack warehousing and logistics links to steal the remote control capabilities reserved by vendors and accounts with super permissions.
 - Pollute compilation environments, development tools, application running environments, and application component environments, and implant backdoors.

Contents

1. Network Security Definition
- 2. Future Network Security Trends**
3. Information Security Standards and Specifications

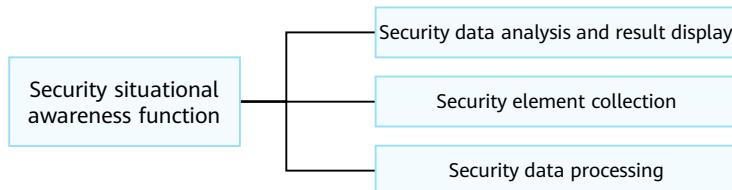
Gartner's Top 8 Security and Risk Trends

No.	Security and Risk Trend
1	Cybersecurity mesh: The cybersecurity mesh is a modern conceptual approach to security architecture that enables the distributed enterprise to deploy and extend security where it is most needed to address future cybersecurity threats.
2	Cyber-savvy boards: Enterprises are paying more attention to cybersecurity, and dedicated committees that focus on cybersecurity matters are formed, often led by a board member with security experience.
3	Vendor consolidation: Vendor consolidation and security products with higher integration can improve O&M efficiency and reduce enterprise costs.
4	Identity-first security: As attackers focus on obtaining identity and access and management permissions, identity-first security becomes more urgent.
5	Managing machine identities becoming a critical security capability: There has been an explosive growth in the numbers of nonhuman entities that make up modern applications. Therefore, managing machine identities has become a vital part of security operations.
6	"Remote work" is now just "work": To implement remote office work in the future, enterprises require a total reboot of security policies and tools to better mitigate security risks.
7	Breach and attack simulation (BAS): A new BAS market is emerging to help enterprises validate their security situation and improve their security protection capabilities.
8	Privacy-enhancing computation techniques: These techniques enable secure data processing, sharing, cross-border transfers, and analytics, even in untrusted environments.

- Gartner is a world-leading research and consulting company. It provides in-depth business and technical insights for all key business functions of enterprises from a global perspective.
- The preceding table lists the security trends proposed by Gartner in 2021 based on network risks and customer service requirements in the security field.
- To cope with emerging threats on customers' live networks, security device vendors provide different network security solutions based on industry development trends, such as network security situational awareness and zero trust.

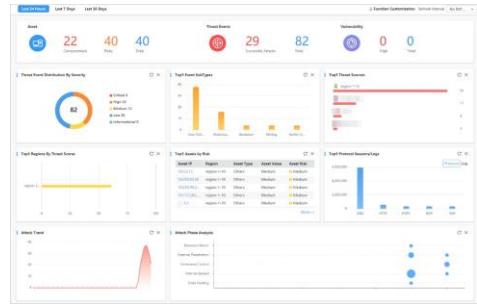
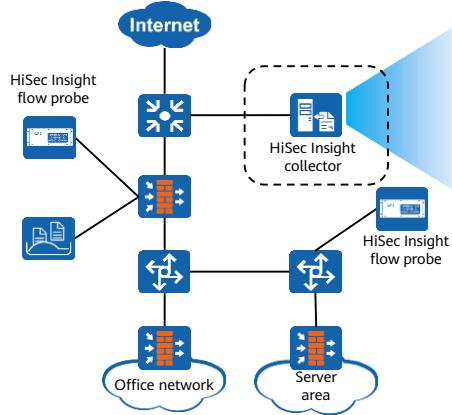
Network Security Situational Awareness (1/2)

- As the enterprise network scale grows, the security architecture becomes increasingly complex, and various types of security devices and security data are increasing, posing greater security O&M pressure on enterprises.
- Currently, security devices deployed on enterprise networks mainly implement single-point detection. Such isolated security protection systems can hardly address new network threats represented by APTs.
- Network security situational awareness enables dynamic and comprehensive security risk identification based on the environment. It uses technologies such as data convergence, data mining, intelligent analysis, and visualization to clearly display the real-time security status of the network environment, providing technical support for network security assurance.



- Security data analysis and result display: Use technologies such as data mining and intelligent analysis to extract system security features and indicators, detect network security risks, and summarize valuable intelligence, and clearly display network security risks using visualization technologies.
- Security element collection: Collect massive data from various security devices, including traffic data, logs, vulnerabilities, Trojan horses, and virus samples.
- Security data processing: Cleanse, classify, standardize, associate, and supplement collected security element data, adds tags to the data, and load standard data to data storage.

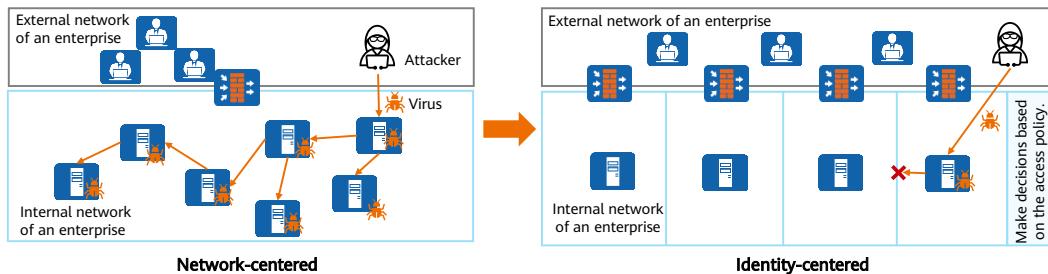
Network Security Situational Awareness (2/2)



The HiSec Insight is deployed on enterprise networks to collect basic network data such as traffic and device logs using the flow probe. Based on big data analysis, machine learning, expert reputation, and intelligence drive, the HiSec Insight can effectively detect potential threats and advanced threats on enterprise networks, implementing network-wide security situational awareness. The analysis results are centrally displayed on the GUI.

Zero Trust Security

- Zero trust is a set of evolving network security paradigms that shift network defense from static network boundaries to users, assets, and resources. Zero Trust Architecture (ZTA) is an enterprise network security strategy based on the zero trust principle. It aims to prevent data disclosure and restrict the lateral movement of attacks on a network.
- The core idea of zero trust is that all users, devices, or systems inside and outside the network are not trusted by default, and the trust basis needs to be established through authentication, authorization, and access control. That is, never trust, always verify.



23 Huawei Confidential



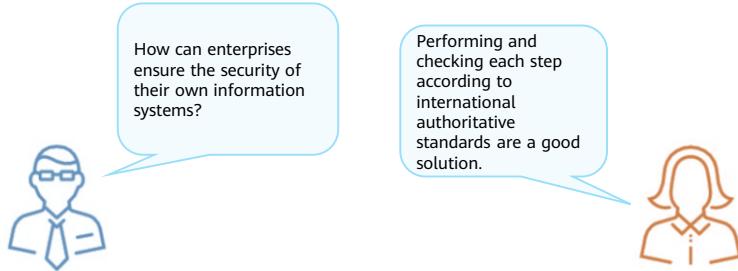
- Network-centered: The trustworthiness control model based on network locations considers that the internal network is trusted and the external network is untrusted. The internal and external network border security is protected by devices such as firewalls. There is an over-trust problem, and attacks initiated from the internal network cannot be defended against.
- Identity-centered: Any connection or service request initiated by any user or device inside or outside the network is considered untrusted before passing the access policy. In this way, fine-grained and adaptive access control is implemented for resources based on the identity.

Contents

1. Network Security Definition
2. Future Network Security Trends
- 3. Information Security Standards and Specifications**
 - Overview of Information Security Standards
 - Introduction to the ISO 27001 Information Security Management System
 - Cybersecurity Classified Protection System

Significance of Information Security Standards

- Information security standards are normative documents that are formulated based on consensus, approved by recognized authorities, and used throughout the industry to achieve the best security.
- Information security standardization is an important part of the national network security assurance system.



Information Security Standards Organizations

- International organizations related to information security standardization include:
 - International Organization for Standardization (ISO)
 - International Electrotechnical Commission (IEC)
- Security standards organizations in China include:
 - National Information Security Standardization Technical Committee (TC260)
 - Network and Information Security Technical Committee of China Communications Standards Association (CCSA)
- Other standards organizations include:
 - International Telecommunication Union (ITU)
 - Internet Engineering Task Force (IETF)
 - National Institute of Standards and Technology (NIST)



- International information security standardization began in the middle of the 1970s, rapidly developed in the 1980s, and drew global attention in the 1990s. At present, there are nearly 300 international and regional organizations establishing standards or technical rules.
- ISO is a global non-governmental organization and also a very important international organization for standardization. It has published international standards and related documents for most fields (including monopolized industries such as military, oil, and shipping).
- IEC is the first international organization established for the preparation and publication of international standards for all electrical, electronic and related technologies.
- ITU is the United Nations specialized agency for information and communication technologies. It allocates global radio spectrum and satellite orbits, develops global telecommunication standards, works to improve telecommunication infrastructure in the developing world, and promotes global telecommunication development.
- IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

Common Information Security Standards and Specifications

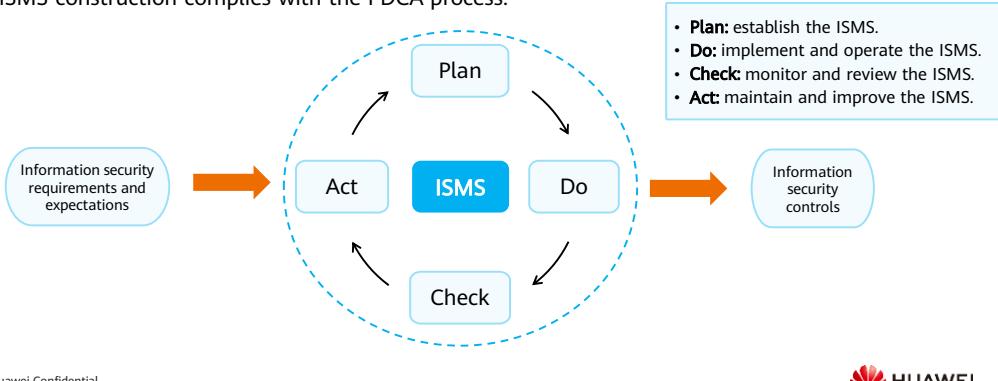
Standard and Specification	Definition
Cybersecurity Classified Protection System	Cybersecurity Classified Protection System is a system that protects information and information carriers according to their importance.
ISO 27001	ISO 27001 is the international standard for an information security management system (ISMS). It can help enterprises establish and optimize their own ISMS and evaluate it.
TCSEC	Trusted Computer System Evaluation Criteria (TCSEC) is proposed by the Defense Science Board in 1970 and published by the United States Department of Defense in December 1985. It is the first formal standard for computer system security evaluation.
ITSEC	Information Technology Security Evaluation Criteria (ITSEC) is formulated by the UK, France, Germany, and the Netherlands. The ITSEC makes better progress in function flexibility and related evaluation technologies than TCSEC. It can be applied in military, government, and business.

Contents

1. Network Security Definition
2. Future Network Security Trends
3. **Information Security Standards and Specifications**
 - Overview of Information Security Standards
 - Introduction to the ISO 27001 Information Security Management System
 - Cybersecurity Classified Protection System

Information Security Management System

- The information security management system (ISMS) is a system in which an organization establishes information security policies and objectives in the whole or a specific scope and uses some methods to achieve these objectives. The concept of ISMS originated from the BS 7799 standard formulated by the British Standards Institute (BSI) and was widely accepted as an international standard.
- The ISMS construction complies with the PDCA process.



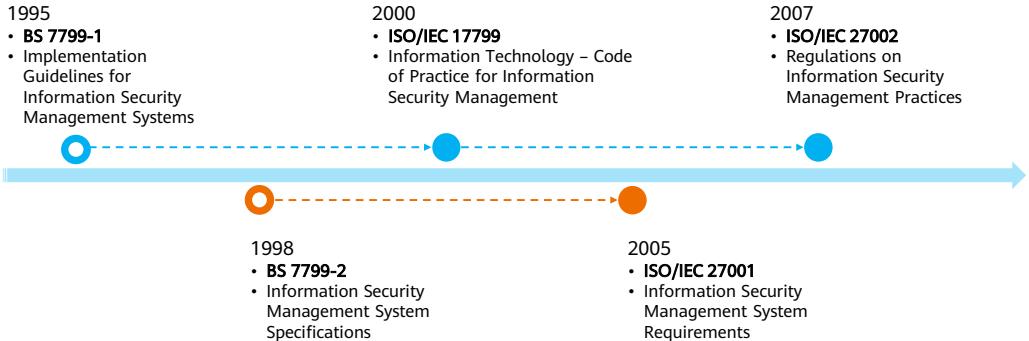
29 Huawei Confidential



- Plan: ISMS planning and preparation. Establish security policies, objectives, processes, and procedures relevant to managing risks and improving information security to deliver results in accordance with an organization's overall policies and objectives. ISO 27002 helps organizations establish the ISMS.
- Do: ISMS document development. Implement and operate the ISMS policy, controls, processes and procedures. ISO 27003 provides implementers with a reference approach to establishing the ISMS.
- Check: ISMS operation. Assess and, where applicable, measure process performance against ISMS policies, objectives, and practical experience and report the results to the management for review. ISO 27004 provides measurement methods and indicators for managers.
- Act: ISMS examination, review, and continuous improvement. Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS. The ISO 27005 risk management approach runs through the entire risk identification, monitoring, assessment, and disposal process.

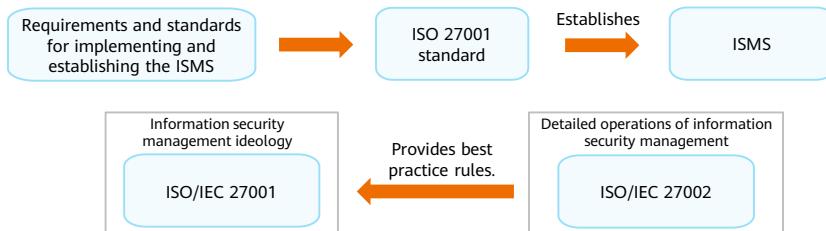
ISO 27000 Evolution

- The BS 7799 standard was later adopted by ISO and became a formal international standard.
- ISO/IEC 27001 and ISO/IEC 27002, released in 2013, are the currently used standards.



ISMS and ISO/IEC 27000

- ISO/IEC 27001 is an international standard for the ISMS.
- ISO 27001 certification requires an organization to achieve dynamic, systematic, all-staff-involved, institutionalized, and prevention-led information security management through a series of processes, such as determining the scope of the ISMS, specifying information security policies and strategies, specifying management responsibilities, and selecting control objectives and control measures based on risk assessment.
- ISO/IEC 27002 proposes 35 control objectives and 113 control measures from 14 aspects. These control objectives and measures are the best practices of information security management.



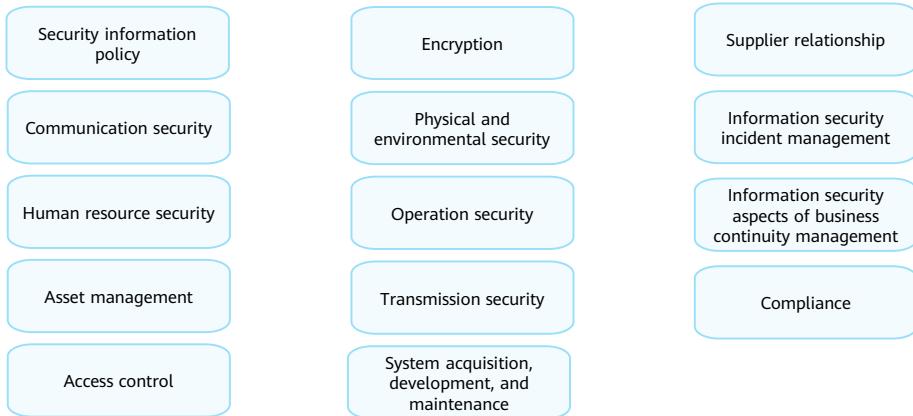
31 Huawei Confidential



- Any company can implement an ISMS, but how? What requirements must be met? ISO 27000 provides detailed requirements or standards. Organizations can establish an ISMS based on the detailed standards or requirements of ISO 27001.
- ISO 27001 is to manage information security risks based on risk assessments and to comprehensively, systematically, and continuously improve information security management using the Plan, Do, Check, Act (PDCA) cycle. It can be used to establish and implement ISMSs and ensure information security of organizations.
- ISO 27001 is a general guideline based on the Deming Cycle (PDCA). It is an overall information security management framework and emphasizes the establishment of a continuous, cyclic, and long-term management mechanism. ISO 27002 is a specific information security management process, which provides detailed information security information under the guidance of the ISO 27001 framework.

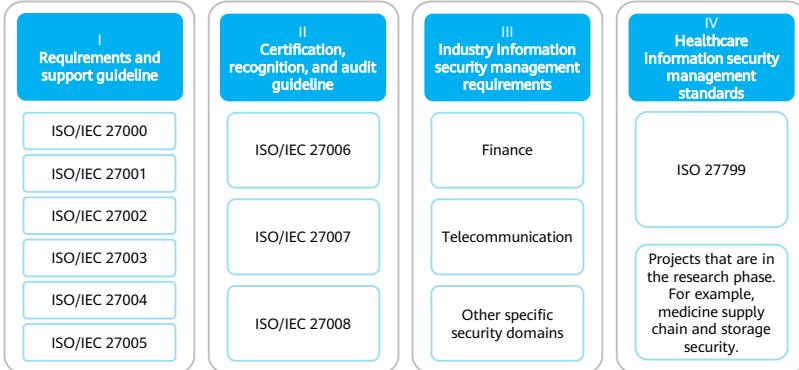
ISMS Content

- The 14 control domains in ISO 27002 are as follows:



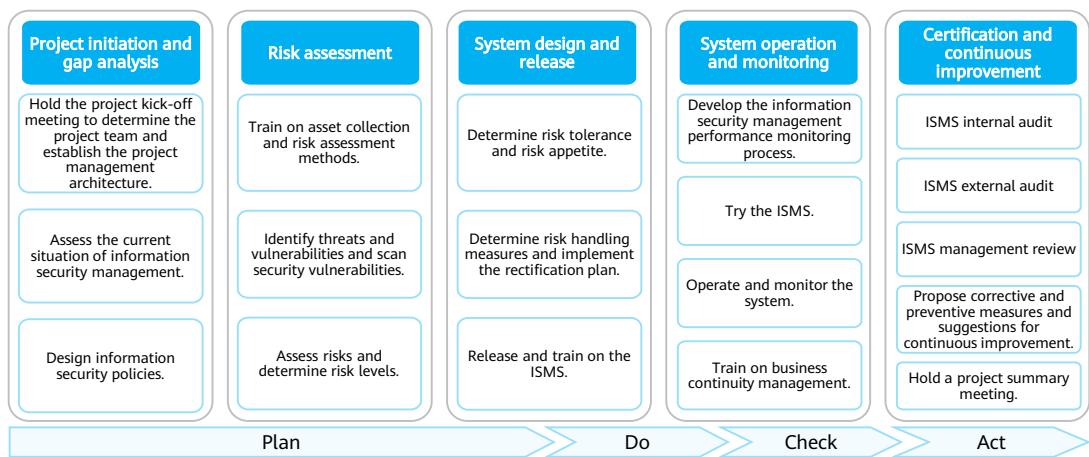
ISO 27000 ISMS Family

- In addition to ISO/IEC 27001 and ISO/IEC 27002, the ISO 27000 series standards include standards related to certification and audit guidelines and industry standards. The ISO 27000 series standards aim to help enterprises and organizations of different types and sizes establish and run the ISMS.



- Only ISO/IEC 27001 can be certified. Other standards are specific clauses and operation guides for the certification.

ISO 27001 Project Implementation Methodology and Procedure



Contents

1. Network Security Definition
2. Future Network Security Trends
3. **Information Security Standards and Specifications**
 - Overview of Information Security Standards
 - Introduction to the ISO 27001 Information Security Management System
 - Cybersecurity Classified Protection System

Definition of Cybersecurity Classified Protection

- Cybersecurity classified protection: protects information and information carriers based on their importance levels.
- The cybersecurity classified protection system has become the basic national policy, basic system, and basic method in the field of network security. Classified protection is a "must-pass benchmark" for security construction.

Cybersecurity Law of the People's Republic of China

Article 21 The State implements a cybersecurity multi-level protection system (MLPS). Network operators shall, according to the requirements of the multi-level protection system, fulfill the following security obligations so as to ensure that the network is free from interference, damage or unauthorized access, and prevent network data from being divulged, stolen or falsified.

Article 31 The State implements key protection on the basis of the cybersecurity multi-level protection system for public communication and information services, power, traffic, water resources, finance, public service, e-government, and other critical information infrastructure which — if destroyed, suffering a loss of function, or experiencing disclosure of data — might seriously endanger national security, national welfare, the people's livelihood, or the public interest. The State Council will formulate the specific scope and security protection measures for critical information infrastructure.

Article 59 Where network operators do not perform cybersecurity protection duties provided for in Articles 21 and 25 of this Law, the competent departments will order corrections and give warnings; where corrections are refused or it leads to harm to cybersecurity or other such consequences, a fine of between RMB 10,000 and 100,000 shall be levied; and the directly responsible management personnel shall be fined between RMB 5,000 and 50,000.

- Classified protection of information security refers to: classified security protection of crucial government information, private and public information of legal persons/organizations/citizens, and information systems that store, transmit, and process the information; classified management of information security products in information systems; classified response to and handling of information security incidents in information systems.
- Legal liability for classified protection: A corporate sector that does not carry out assessment for classified protection will be rectified according to relevant regulations. If it violates the provisions of Cybersecurity Law of the People's Republic of China, it will be punished according to relevant laws and regulations.

Significance of Cybersecurity Classified Protection



Legal and regulatory compliance

Meet legal and regulatory compliance requirements, implement network security protection obligations, and properly avoid risks.

Security systematization

Clarify the overall objectives of the organization, change the single defense mode, and make security construction more systematic.

Security awareness improvement

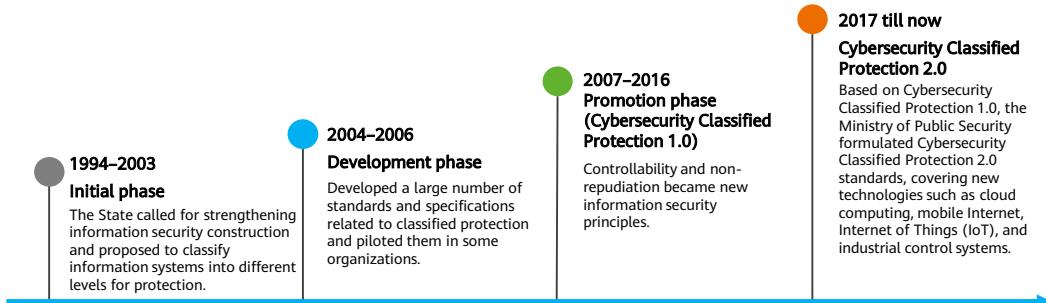
Improve personnel's security awareness, establish classified protection ideas, and properly allocate network security investment.

Service security requirements

Strengthen network security construction based on classified protection to meet service security requirements.

Development History of Cybersecurity Classified Protection

- After more than 20 years of development, Cybersecurity Classified Protection has gone through four phases and has upgraded from V1.0 to V2.0.

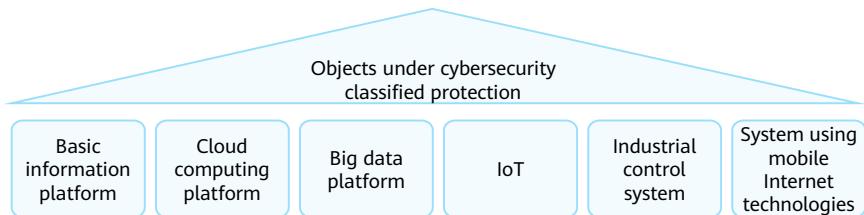


- Timeline of Cybersecurity Classified Protection development:
 - On February 18, 1994, decree No.147 of the State Council of the People's Republic of China issued the *Regulations of the People's Republic of China for Safety Protection of Computer Information Systems*.
 - In September 2003, the General Office of the CPC Central Committee and the General Office of the State Council issued the *Opinions of the Leading Group for Strengthening Information Security Assurance Work* (No. 27 [2003]).
 - In November 2004, the Ministry of Public Security, National Administration of State Secrets Protection, State Cryptography Administration, and State Council Information Office jointly issued the *Notice on Printing and Distributing the Implementation Opinions on Classified Protection of Information Security* (No. 66 [2004]).
 - In September 2005, the State Council Information Office issued the *Implementation Guide for Classified Protection of E-Government Information Security (Trial)* (No. 25 [2004]).
 - At the end of 2005, the Ministry of Public Security and the State Council Information Office jointly issued the *Notice on Carrying out Basic Investigations on Classified Protection of Information Systems* (No. 1431 [2005]).

- In January 2006, the Ministry of Public Security, National Administration of State Secrets Protection, State Cryptography Administration, and State Council Information Office jointly issued the *Notice on Printing and Distributing the Measures for Administration of Classified Protection of Information Security (Trial)* (No. 7 [2006]).
- In June 2007, the Ministry of Public Security, National Administration of State Secrets Protection, State Cryptography Administration, and State Council Information Office jointly issued the *Regulations on Classified Protection of Information Security* (No. 43 [2007]).
- In 2008, GB/T 22239 *Baseline for Classified Protection of Information System Security* and GB/T 22240 *Guidelines for Grading of Classified Cybersecurity Protection* were issued.
- In 2009, the Ministry of Public Security issued the *Guiding Opinions on Carrying out Rectification of Security Construction of Classified Protection of Information Systems* (No. 1429 [2009]).
- In March 2010, the Ministry of Public Security issued the *Notice on Promoting the Construction of the Information Security Classified Protection Evaluation System and Carrying out Classification Evaluation* (No. 303 [2010]).
- In 2017, *Cybersecurity Law of the People's Republic of China* was officially implemented, opening the era of Cybersecurity Classified Protection 2.0.

Objects Under Cybersecurity Classified Protection

- An object under cybersecurity classified protection generally refers to a system consisting of computers or other information terminals and related devices that collects, stores, transmits, exchanges, and processes information in accordance with certain rules and procedures. Such objects include basic information networks, cloud computing platforms/systems, big data applications/platforms/resources, IoT, industrial control systems, and systems that use mobile Internet technologies.



Information Security Protection Levels

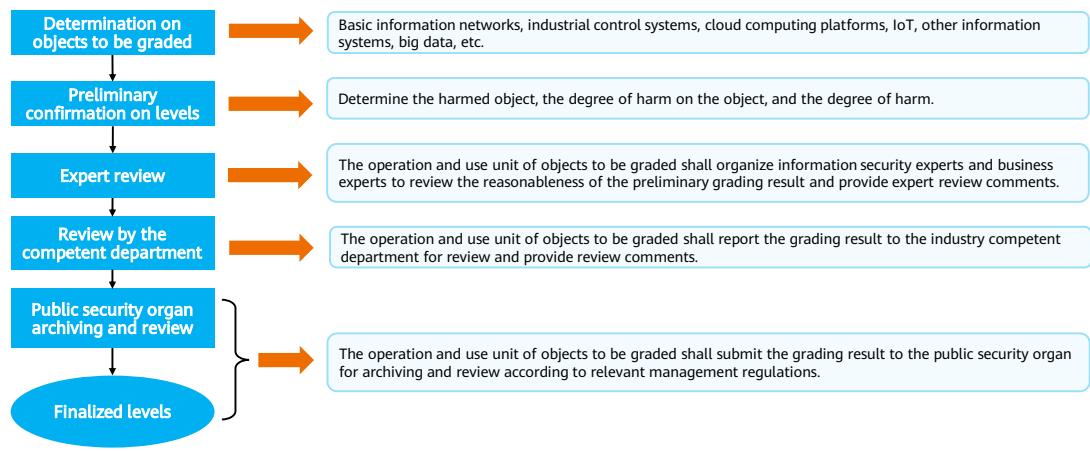
- The objects are classified into five levels of cybersecurity protection according to their importance in national security, economic construction, and social life, and their adverse impact to national security, social order, public interests as well as the legitimate rights and interests of citizens, legal persons, and other organizations when the information systems of the objects are attacked.

Harmed Object	Degree of Harm on Object		
	Minor Harm	Grave Harm	Especially Grave Harm
Legitimate rights and interests of citizens, legal persons, and other organizations	Level 1	Level 2	Level 3
Social order Public interests	Level 2	Level 3	Level 4
National security	Level 3	Level 4	Level 5

Relationship between grading elements and security protection levels

- Level 1: After the information system is damaged, harm is inflicted upon the legitimate rights and interests of citizens, legal persons, and other organizations, but national security, social order, and public interests are not endangered.
- Level 2: After the information system is damaged, grave harm is done to the legitimate rights and interests of citizens, legal persons, and other organizations, or harm is inflicted upon social order and public interests, but national security is not harmed.
- Level 3: After the information system is damaged, grave harm is inflicted upon social order and public interests, or harm is inflicted upon national security.
- Level 4: After the information system is damaged, especially grave harm is inflicted upon social order and public interests, or grave harm is inflicted upon national security.
- Level 5: After the information system is damaged, especially grave harm is inflicted upon national security.

Grading Process of the Cybersecurity Classified Protection System

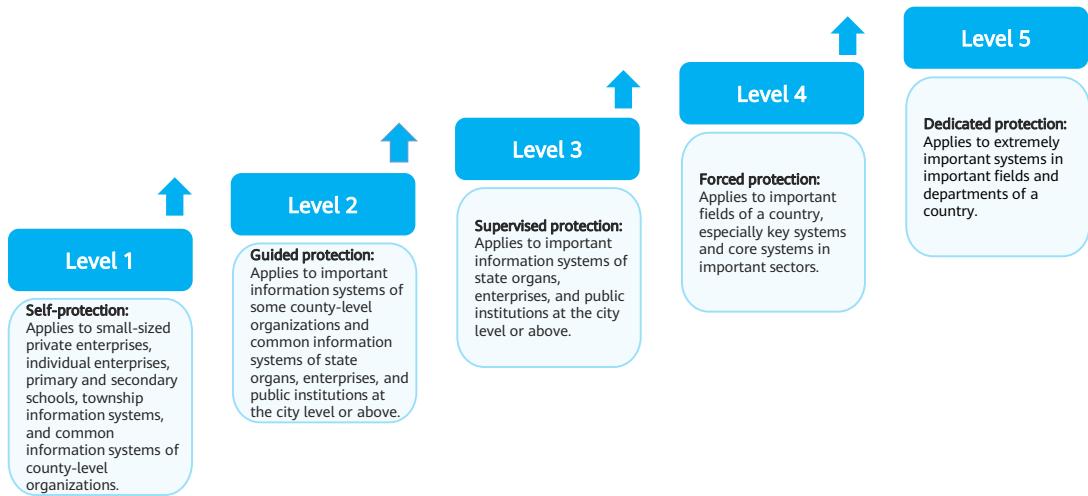


42 Huawei Confidential



- If the security protection is preliminarily determined to be Level 2 or above, the network operator must engage qualified experts to carry out additional reviews according to standards described in this document, and submit the result to the competent department for archiving and review, and determine the final security protection level.
- If the security protection is preliminarily determined to be Level 1, the network operator can determine the final security protection level on its own according to standards described in this document, without expert review, or archiving and review by the competent department.

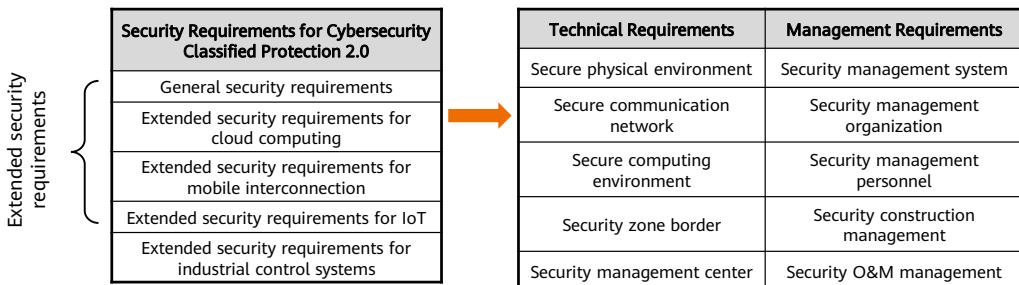
Security Protection Capabilities at Different Levels



- Level 1: self-protection. It shall be able to protect against critical resource damage caused by malicious attacks from threat sources with few resources, general natural disasters, and other threats of a considerable degree of harm. After the damage, it may restore some functions.
- Level 2: guided protection. It shall be able to protect against important resource damage caused by malicious attacks from small external sources and threat sources with a small amount of resources, general natural disasters, and other threats of considerable harm. It may find important security loopholes and handle security incidents, and restore some functions within a period of time after being damaged.
- Level 3: supervised protection. It shall be able to protect against major resource damage caused by malicious attacks from externally organized groups and threat sources with rich resources, severe natural disasters, and other threats of considerable harm. It may find and monitor attack behaviors and handle security incidents, and restore most functions within a period of time after being damaged.
- Level 4: forced protection. Based on the unified security policy, it shall be able to protect against malicious attacks from national, hostile organizations, and threat sources with richer resources, more severe natural disasters, and resource damage caused by other threats of considerable harm. It may find and monitor attack behaviors and handle security incidents, and restore all functions within a period of time after being damaged.
- Level 5: dedicated protection. Based on the unified security policy and dedicated security protection, the security of the system can be enhanced through a verifiable design. In this way, the system has the anti-penetration capability, data information is protected from unauthorized disclosure and damage, and the highest security of system services is ensured.

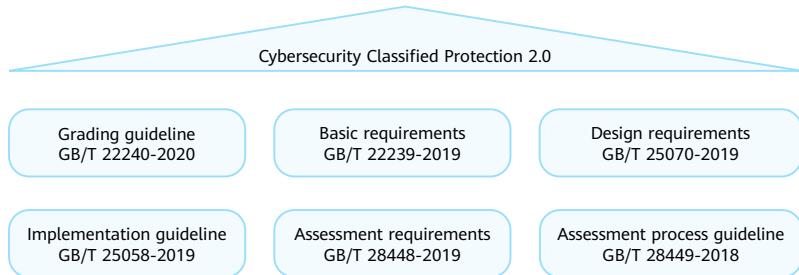
Security Requirements for Cybersecurity Classified Protection

- Security requirements for Cybersecurity Classified Protection 2.0 are classified into general security requirements and extended security requirements to implement common and personalized protection for protected objects at different levels and in different forms.
- Both general security requirements and extended security requirements are classified into technical requirements and management requirements. Different security levels correspond to different requirements. The higher the security level, the stricter the requirements.

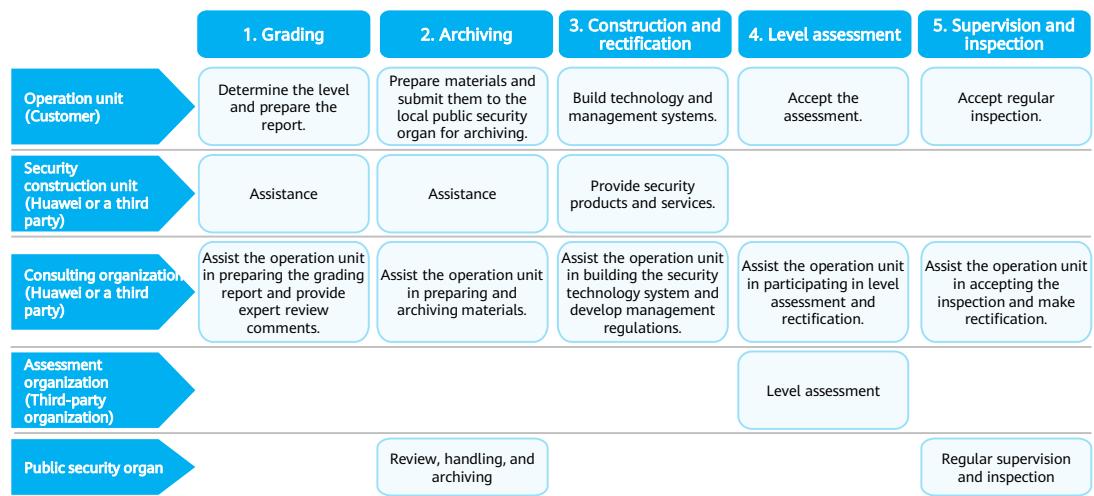


Cybersecurity Classified Protection 2.0

- In addition to GB/T 22239-2019 that specifies the basic requirements of cybersecurity classified protection, Cybersecurity Classified Protection 2.0 also specifies a series of other standards to guide its grading, implementation, and assessment.



Working Process of Cybersecurity Classified Protection



46 Huawei Confidential



- If the security protection is preliminarily determined to be Level 1, the network operator can determine the final security protection level on its own according to standards described in this document, without expert review, or archiving and review by the competent department. If the security protection is preliminarily determined to be Level 2 or above, the network operator must engage qualified experts to carry out additional reviews according to standards described in this document, and submit the result to the competent department for archiving and review, and determine the final security protection level.
- If an enterprise or organization has an industry competent (supervision) department, it shall submit the grading result to the industry competent (supervision) department for review in addition to providing expert review comments.

Quiz

1. (Single-answer question) In Cybersecurity Classified Protection 2.0, a network operator can determine the final level of security protection on its own when the security protection level is preliminarily determined to be ____.
 - A. Level 1
 - B. Level 2
 - C. Level 3
 - D. Level 4
2. (True or false) ISO 27002 can be used to certify an enterprise's information security system.
 - A. True
 - B. False

1. A
2. B

Summary

- This course briefly introduces the four development phases of information security: communication security, information security, information assurance, and cyberspace security, and describes security concepts and solutions such as network security situational awareness and zero trust security. This course also illustrates the formulation of various international and national information security standards, such as ISO 27001 and Cybersecurity Classified Protection 2.0. These standards and specifications promote the construction of enterprise information security management systems. Upon completion of this course, you will be able to understand the concepts and specifications of information security.

Recommendations

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

Acronyms and Abbreviations (1/2)

Acronym/Abbreviation	Full Spelling
APT	Advanced Persistent Threat
BS	British Standard
CCSA	China Communications Standards Association
CDN	Content Delivery Network
DDoS	Distributed Denial of Service
DNS	Domain Name System
GB	China National Standards
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IoT	Internet of Things
ISMS	Information Security Management System
ISO	International Organization for Standardization

Acronyms and Abbreviations (2/2)

Acronym/Abbreviation	Full Spelling
ITSEC	Information Technology Security Evaluation Criteria
ITU	International Telecommunication Union
NIST	National Institute of Standards and Technology
P2P	Peer to Peer
PDCA	Plan-Do-Check-Act
SaaS	Software as a Service
SQL	Structured Query Language
TC260	National Information Security Standardization Technical Committee
TCSEC	Trusted Computer System Evaluation Criteria
ZTA	Zero Trust Architecture

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
portfolio, new technology, 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 Basics



Foreword

- With the development of the Internet, network attacks keep emerging and network security becomes all the more important. The application of security technologies to data communication is an extension of data communication technologies. Before learning security technologies, knowing basic concepts of networks, such as basic network communication principles, network infrastructure, and common network protocols, can help you better understand the working principles and application scenarios of various security technologies.
- This chapter describes the typical enterprise network architecture, common network devices and their working principles, as well as the CLI-based and GUI-based firewall configuration modes.

Objectives

- On completion of this course, you will be able to:
 - Understand the data definition and transmission process.
 - Describe the working principles of the TCP/IP protocol stack.
 - Describe the working principles of common protocols.
 - Describe common network devices and their working principles.

Contents

1. Network Reference Model

- OSI Reference Model and TCP/IP Reference Model
 - Application Layer
 - Transport Layer
 - Network Layer
 - Data Link Layer

2. Common Network Devices

Application and Data

- Applications are developed to meet users' various requirements, such as web page access, online gaming, and online video play. Information is generated along with applications, which is presented in different modes, such as texts, pictures, and videos.
- For network engineers, applications can generate data. Data is the carrier of all kinds of information and the physical symbol or the combination of various physical symbols recording the nature, status, and relationships of objects. Data can be symbols, texts, digits, voice, images, and videos.
- Data generated by most applications needs to be transmitted between devices. Network engineers need to pay more attention to the end-to-end data transmission process.



- A computer can only identify digital data consisting of 0s and 1s. It is incapable of reading other types of information, so the information needs to be translated into data by certain rules.
- However, people do not have the capability of reading electronic data. Therefore, data needs to be converted into information that can be understood by people.

OSI Reference Model

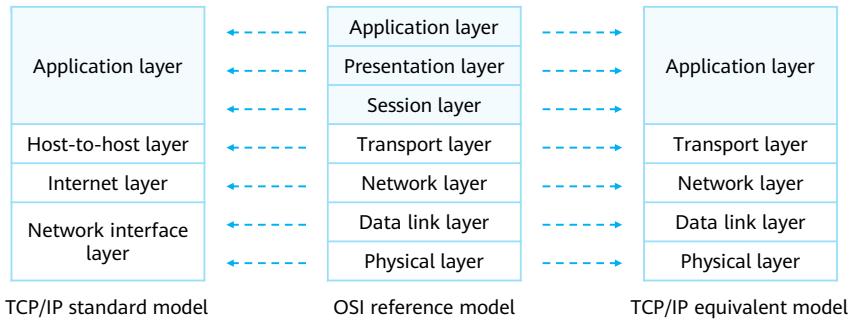
- The open systems interconnection (OSI) reference model was proposed by the International Organization for Standardization (ISO) in 1984 for network interconnection. The OSI reference model has a seven-layer architecture.

Layer	Function
Application layer	Provides network interfaces for applications.
Presentation layer	Translates data formats to ensure that the application-layer data of one system can be identified and understood by the application layer of another system.
Session layer	Establishes, manages, and terminates sessions between communicating parties.
Transport layer	Establishes, maintains, and cancels an end-to-end data transmission process. Controls transmission speeds and adjusts data sequences.
Network layer	Defines logical addresses and transfers data from sources to destinations.
Data link layer	Encapsulates packets into frames, transmits frames in point-to-point or point-to-multipoint mode, and implements error detection.
Physical layer	Transmits bitstreams over transmission media and defines electrical and physical specifications.

- The OSI reference model was included in the ISO 7489 standards and released in 1984.
- The OSI reference model is also called the seven-layer model. The seven layers from top to bottom are as follows:
 - Application layer: provides network services for applications and is closest to users.
 - Presentation layer: provides data encoding and conversion functions so that data sent by the application layer of one system can be identified by the application layer of another system.
 - Session layer: establishes, manages, and terminates communication sessions between entities at the presentation layer. Communication at this layer is implemented through service requests and responses transmitted between applications on different devices.
 - Transport layer: implements connection-oriented and non-connection-oriented data transmission, as well as error detection.
 - Network layer: defines logical addresses for routers to determine paths and transmits data from source networks to destination networks.
 - Data link layer: encapsulates bits into bytes and bytes into frames, uses link-layer addresses (MAC addresses in Ethernet) to access media, and implements error detection.
 - Physical layer: transmits bitstreams between devices and defines physical specifications such as electrical levels, speeds, and cable pins.

TCP/IP Reference Model

- The OSI reference model is complex, and the TCP and IP protocols are widely used in the industry. Therefore, the TCP/IP reference model has become the actual reference model of the Internet.



- The transmission control protocol/Internet protocol (TCP/IP) model is widely used because of its openness and usability.
- The TCP/IP model is similar to the OSI model in structure and adopts a hierarchical architecture. Adjacent layers in the TCP/IP model are closely related. The difference between the TCP/IP model and the OSI model is that in TCP/IP model, the presentation layer and the session layer are combined into the application layer. Therefore, the TCP/IP model has four layers from bottom to top: network interface layer, network layer, transport layer, and application layer.
- The TCP/IP standard model combines the data link layer and the physical layer in the OSI model into the network interface layer. However, in practice, data is separately processed at the data link layer and physical layer. Therefore, the TCP/IP equivalent model that integrates the TCP/IP standard model and the OSI reference model is proposed. Contents in the following slides are based on the TCP/IP equivalent model.

Common Protocols of the TCP/IP Protocol Stack

- The TCP/IP protocol stack defines a series of standard protocols.

Application layer	Telnet	FTP	TFTP	SNMP
	HTTP	SMTP	DNS	DHCP
Transport layer	TCP		UDP	
Network layer	ICMP		IGMP	
	IP			
Data link layer	PPPoE			
	Ethernet		PPP	
Physical layer	...			

- Application layer: provides network interfaces for applications.
 - Hypertext Transfer Protocol (HTTP): is used to access various pages on web servers.
 - File Transfer Protocol (FTP): provides a method for transferring files. It allows data to be transferred from one host to another.
 - Domain Name Service (DNS): translates host domain names into IP addresses.
- Transport layer: sets up end-to-end connections.
 - Transmission Control Protocol (TCP): provides reliable connection-oriented communication services for applications. Currently, TCP is used by many popular applications.
 - User Datagram Protocol (UDP): provides connectionless communication services, without guaranteeing the reliability of data packet transmission.
- Network layer: performs addressing and routing.
 - Internet Protocol (IP): encapsulates transport-layer data into data packets and forwards packets from source sites to destination sites. IP provides connectionless and unreliable services.
 - Internet Group Management Protocol (IGMP): manages IP multicast group memberships. Specifically, IGMP sets up and maintains memberships between IP hosts and their directly connected multicast routers.

- Internet Control Message Protocol (ICMP): sends control messages based on the IP protocol and provides the monitoring and feedback information about various problems that may exist in the communication environment. Such information helps administrators diagnose the problems and take proper measures to resolve them.
- Data link layer: encapsulates data frames and provides intra-segment communication for the network layer.
 - Point-to-Point Protocol (PPP): is a point-to-point data link layer protocol and is commonly used on wide area networks (WANs).
 - Ethernet: is a multi-access broadcast data link layer protocol and is most widely used on local area networks (LANs).
 - Point-to-Point Protocol over Ethernet (PPPoE): enables a bridged access server to connect multiple hosts on a network to a remote access concentrator. PPPoE is usually used by home users to access the Internet via dialup.
- Physical layer: transmits bitstreams over media.

Contents

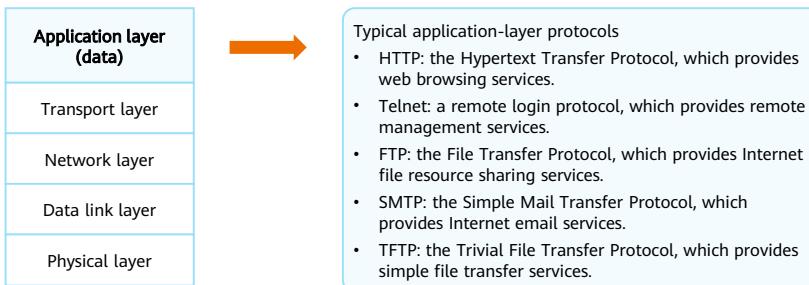
1. Network Reference Model

- OSI Reference Model and TCP/IP Reference Model
 - Application Layer
 - Transport Layer
 - Network Layer
 - Data Link Layer

2. Common Network Devices

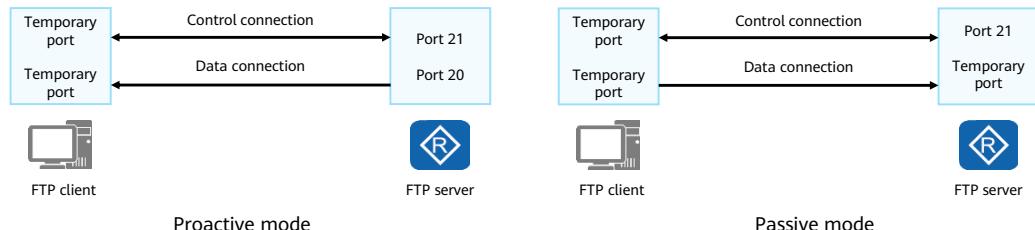
Application Layer

- The application layer provides interfaces for application software so that applications can use network services. Based on a transport-layer protocol, applications define the port number used at the transport layer.



FTP

- File Transfer Protocol (FTP) transfers files from one host to another to implement file download and upload. This protocol adopts the client/server (C/S) structure. When FTP is used to transmit data, the control connection and data connection are established between the server and client.
- The FTP connection can be set up in either proactive or passive mode. The difference between the two modes lies in whether the data connection is initiated by the server or client. By default, the proactive mode is used. Users can switch to the passive mode through commands.

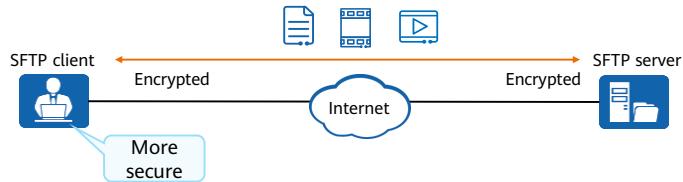


- In proactive mode, if a firewall is deployed on the client, a data connection may fail to be established because it is initiated by the server. In passive mode, this issue is solved. However, the proactive mode facilitates the management of the FTP server but impairs the management of the client. The opposite is true in passive mode.
- By default, port 21 of the server is used to transmit control commands, and port 20 is used to transmit data.
- The establishment process of FTP connection in proactive mode:
 - The server enables port 21 to enable the listener and set up a control connection with the client.
 - The client initiates a control connection setup request and the server responds.
 - The client sends the PORT command through the control connection to notify the server of the temporary port number used for the client data connection.
 - A data connection is set up between the temporary port on the client and port 20 on the server.

- The establishment process of FTP connection in passive mode:
 - The server enables port 21 to enable the listener and set up a control connection with the client.
 - The client initiates a control connection setup request and the server responds.
 - The client sends the PASV command through the control connection to notify the server that the client is in passive mode.
 - The server responds and informs the client of the temporary port number used for data connection.
 - A data connection is set up between the temporary ports on the client and the server.

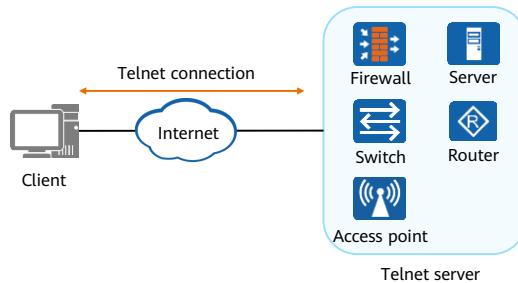
SFTP

- Secure File Transfer Protocol (SFTP) transmits files securely based on secure shell (SSH).
- FTP transmits data in plaintext, which is not secure. SFTP encrypts the authentication information and data to be transmitted, with higher security compared with FTP.
- SFTP is a single-channel protocol and its default destination port number is 22. The client and server are securely connected using SSH to transfer files. FTP is a dual-channel protocol, including the control channel and data channel.



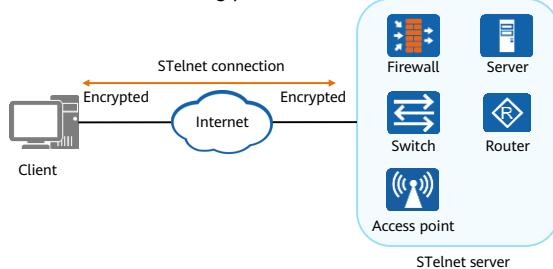
Telnet

- Telnet is a standard protocol that provides remote login services on a network.
- It helps users to operate remote devices through local PCs.
- Users log in to a Telnet server through a Telnet client program. The commands entered on the Telnet client are executed on the Telnet server, as if the commands were entered on the console of the server.



STelnet

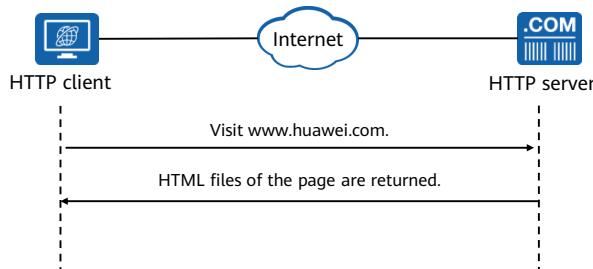
- Secure Telnet (STelnet) is a secure Telnet service enabling users to remotely and securely log in to devices. Through STelnet, all exchanged data is encrypted, thus implementing secure sessions. Telnet transmits data in plaintext, which is not secure. Network security can be greatly improved using STelnet.
- STelnet is implemented based on SSH and the destination port number is 22 by default. Negotiations between an STelnet server and an STelnet client include the following phases:
 - Version negotiation
 - Algorithm negotiation
 - Key exchange
 - User authentication
 - Session interaction



- Version negotiation phase: SSH is available in SSHv1 and SSHv2. The server and client determine which SSH version to be used through version negotiation.
- Algorithm negotiation phase: SSH supports multiple encryption algorithms. Based on their supported algorithms, the server and client determine which algorithm to be used through negotiations.
- Key exchange phase: A session key is generated using a key exchange algorithm. After that, sessions between the server and client are encrypted through session keys.
- User authentication phase: The SSH client sends an authentication request to the SSH server and the server authenticates the client.
- Session interaction phase: After the authentication succeeds, the server and client exchange data.

HTTP

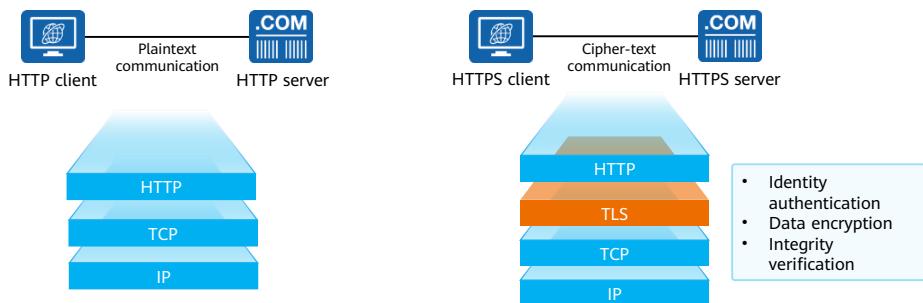
- Hypertext Transfer Protocol (HTTP) is one of the most widely used network protocols on the Internet. HTTP was originally designed to provide a method for publishing and receiving hypertext markup language (HTML) pages.



- WWW is short for World Wide Web, also known as 3W or Web. As a next-generation user interface on the Internet, WWW replaces the traditional plaintext mode in which information is exchanged in plain text. Hypertext is a holistic information architecture, which establishes links for different parts of a document through keywords so that information can be transmitted in interactive mode. With the emerging and development of multimedia technologies, the coverage of hypertext technologies has been extended from plain texts to multimedia. The concept of hypermedia is therefore developed.
- On the Internet, hypermedia and hypertext modes are combined and information links are extended to the entire Internet. Web is a kind of hypertext information system, enabling texts to be switched from one position to another instead of being fixed at a certain position. Web is unique for its multiple links.

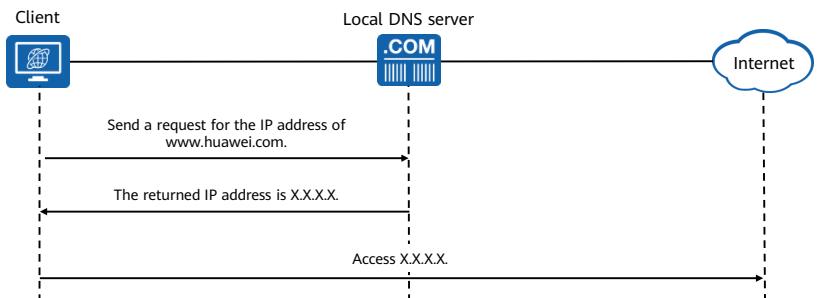
HTTPS

- Hypertext Transfer Protocol Secure (HTTPS): provides secure HTTP channels.
- The Transport Layer Security (TLS) protocol is added to HTTPS based on HTTP to enable identity authentication, data encryption, and integrity verification for data transmissions. The destination port number of HTTPS is 443 and the destination port number of HTTP is 80 by default. Currently, most websites use HTTPS to provide secure data transmission.



DNS

- To visit a website, users need to enter the character string of the website address. However, a computer needs to know the IP address corresponding to the domain name of the website for access. In this case, a domain name system (DNS) is required.
- DNS is classified into dynamic and static domain name resolution. Static domain name resolution is first used to resolve a domain name. If the resolution fails, dynamic domain name resolution is used.



19 Huawei Confidential



- IPv4 static domain name resolution requires a static domain name resolution table, which lists the mapping created manually between domain names and IPv4 addresses. This table is similar to the **hosts** file in a Windows operating system. The table contains commonly used domain names. After searching for a specified domain name in the resolution table, the client can obtain the IP address mapped to the domain name. This process improves domain name resolution efficiency.
- Dynamic domain name resolution requires a dedicated DNS server. This server runs the domain name resolution program, maps domain names to IP addresses, and receives DNS requests from clients.

Contents

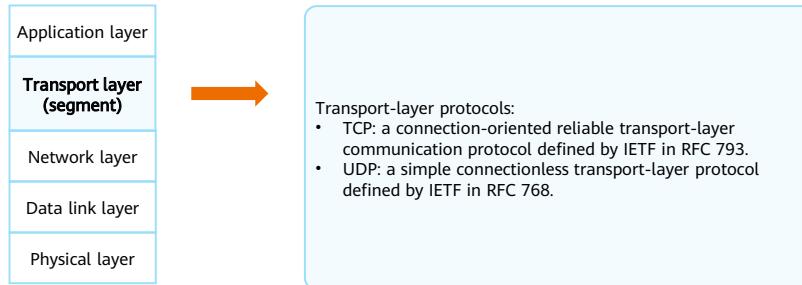
1. Network Reference Model

- OSI Reference Model and TCP/IP Reference Model
- Application Layer
- **Transport Layer**
- Network Layer
- Data Link Layer

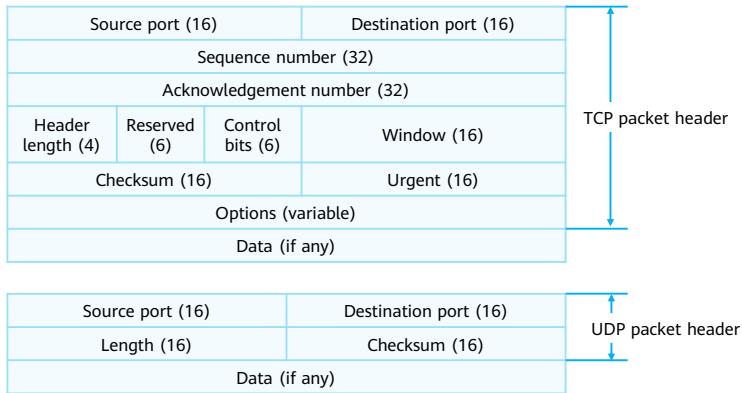
2. Common Network Devices

Transport Layer

- A transport-layer protocol receives data from an application-layer protocol, encapsulates the data with the corresponding transport-layer protocol header, and helps establish an end-to-end connection.



TCP and UDP – Packet Formats

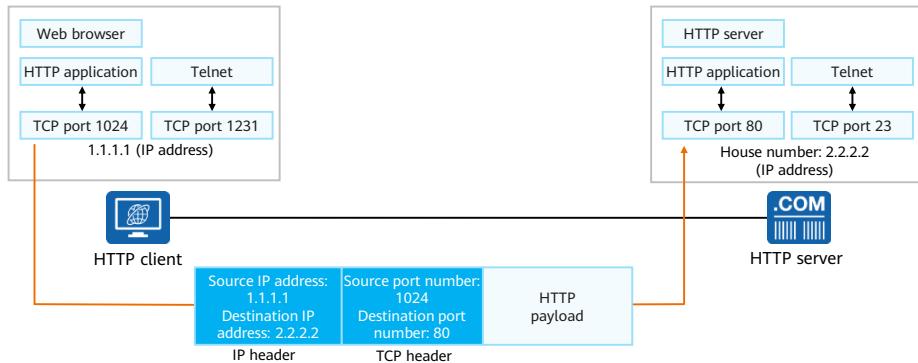


- **TCP packet header:**
 - Source port: This field identifies the application that sends the packet. This field is 16 bits long.
 - Destination port: This field identifies the application that receives the packet. This field is 16 bits long.
 - Sequence number: This field indicates the sequence number of each byte in a data flow transmitted over a TCP link. The sequence number field value refers to the sequence number of the first byte of data sent by the packet segment. This field is 32 bits long.
 - Acknowledgment number: This field indicates the sequence number of the next segment's first byte that the receiver is expecting to receive. The value of this field is 1 plus the sequence number of the last byte in the previous segment that is successfully received. This field is valid only when ACK is set to 1. This field is 32 bits long.
 - Header length: This field indicates the length of the TCP header. The unit is 32 bits (4 bytes). If the Options field is empty, the value of this field is 5, indicating that the header contains 20 bytes.
 - Reserved: The value must be 0. This field is 6 bits long.
 - Control bits: This field indicates TCP data segments in different states including FIN, ACK, and SYN flags.

- Window: This field indicates the maximum number of bytes that are allowed by the receiver for implementing TCP traffic control. The maximum window size is 65535 bytes. This field is 16 bits long.
 - Checksum: This field indicates a mandatory field calculated and stored by the sender and verified by the receiver. During checksum computation, the TCP packet header and TCP data are included, and a 12-byte pseudo header is added in front of the TCP packet segment. This field is 16 bits long.
 - Urgent: The field is significant only when URG is set to 1. The local device sends urgent data to the peer device using the urgent pointer. The field is used to indicate the number of bytes in the urgent data of the packet segment and is placed at the beginning of the packet segment. This field is 16 bits long.
 - Options: The field is significant and ranges from 0 bytes to 40 bytes.
- UDP packet header:
 - Source port: The field identifies the application that sends the packet and is 16 bits long.
 - Destination port: The field identifies the application that receives the packet and is 16 bits long.
 - Length: The field specifies the total length of a UDP packet header and data. The possible minimum length of the field is 8 bytes, as a UDP packet header has used 8 bytes. Due to this field, the total length of a UDP packet cannot exceed 65535 bytes, including an 8-byte header and 65527 bytes of data.
 - Checksum: The field indicates the checksum of a UDP packet header and UDP data and is 16 bits long.

TCP and UDP – Port Numbers

- TCP and UDP distinguish different services using different port numbers. Generally, the source port used by a client is randomly allocated, and the destination port is specified by the application of a server. The source port number is usually greater than 1023 and is not being used. The destination port number indicates the listening port number of the application (service) enabled on the server. For example, the default port number for HTTP is 80.



Contents

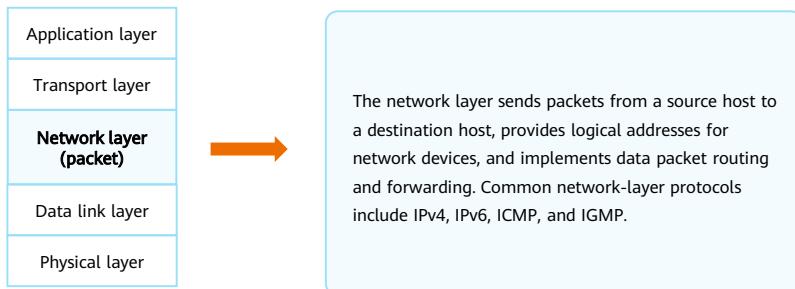
1. Network Reference Model

- OSI Reference Model and TCP/IP Reference Model
- Application Layer
- Transport Layer
- **Network Layer**
- Data Link Layer

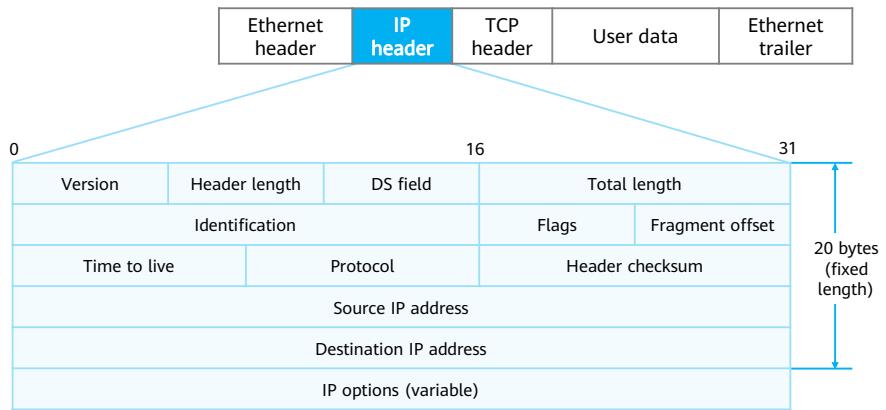
2. Common Network Devices

Network Layer

- The transport layer establishes connections between processes on different hosts, and the network layer transmits data from one host to another.

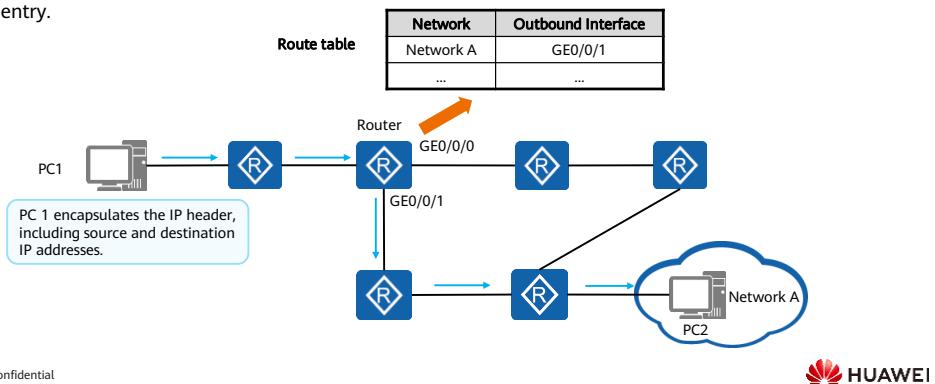


IP Packet Header



IP Packet Forwarding

- The network-layer header of a packet sent by a source device carries the network-layer addresses of the source and destination devices. Each network device (such as a router) with routing functions maintains a routing table. After receiving a packet, the network device reads the network-layer destination address of the packet, searches the address in the routing table for the matching entry, and forwards the packet according to the instruction of the matching entry.

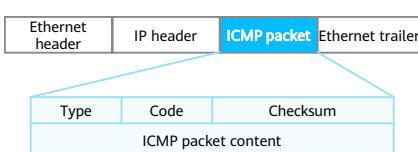


28 Huawei Confidential

- When IP is used as the network-layer protocol, the two communicating devices are separately assigned with a unique IP address to identify themselves. An IP address can be written as a 32-bit binary integer and is usually represented in dotted decimal notation to facilitate reading and analysis. The four bytes of an IP address are separated from each other by dot (.) in decimal notation, such as 192.168.1.1.
- Encapsulation and forwarding of IP packets:
 - When receiving data from an upper layer (such as the transport layer), the network layer encapsulates an IP packet header and adds the source and destination IP addresses to the header.
 - Each passing network device, such as a router, maintains a routing table that guides IP packet forwarding like a map. After receiving an IP packet, the router forwards the packet by searching its IP routing table based on the destination IP address.
 - When the IP packet reaches the destination host, the destination host determines whether to accept the packet based on the destination IP address and then processes the packet accordingly.
- The IP protocol works together with routing protocols such as OSPF, IS-IS, and BGP to help routers establish routing tables and to conduct network control and network status diagnosis.

ICMP

- The Internet Control Message Protocol (ICMP) is an auxiliary IP protocol.
- ICMP is used to transmit error and control information between network devices. It plays an important role in collecting network information as well as diagnosing and rectifying network faults.

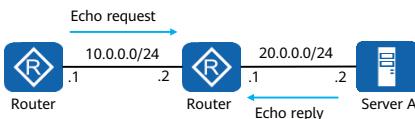


Type	Code	Description
0	0	Echo reply
3	0	Network unreachable
3	1	Host unreachable
3	2	Protocol unreachable
3	3	Port unreachable
5	0	Redirection
8	0	Echo request

- ICMP works at the network layer to ensure correct forwarding of IP packets and successful data packet exchange. ICMP allows hosts or devices to report errors or exceptions during packet transmission.
- ICMP messages are encapsulated in IP packets. If the Protocol value in the IP header is 1, the used protocol is ICMP.
- ICMP field resolution:
 - The format of an ICMP message depends on the Type and Code fields. The Type field indicates the message type, and the Code field indicates specific parameters of the message type.
 - The Checksum field is used to check whether the message is complete.
 - An ICMP message contains a 32-bit variable field. Generally, this field is not used and is set to 0.
 - An ICMP Redirect message specifies a gateway IP address. A host redirects packets to the specified gateway based on this address.
 - An Echo Request message contains the identifier and sequence number. The source device associates a received Echo Reply message with an Echo Request message it sends based on the two parameters. Especially when the source sends multiple Echo Request messages to the destination, the Echo Request and Echo Reply messages must be matched based on the identifiers and sequence numbers.

ICMP Error Check

- The ICMP Echo Request message and ICMP Echo Reply message are usually used to check network connectivity between source and destination addresses, and to provide other information, such as the round-trip time of packets.
- A typical ICMP application is the ping command. Ping is a common tool for checking network connectivity and collecting related information. In the ping command, users can assign different parameters, such as the length and number of ICMP packets, and the timeout period for waiting for a reply. Devices construct and send ICMP packets based on the parameters to perform ping tests.

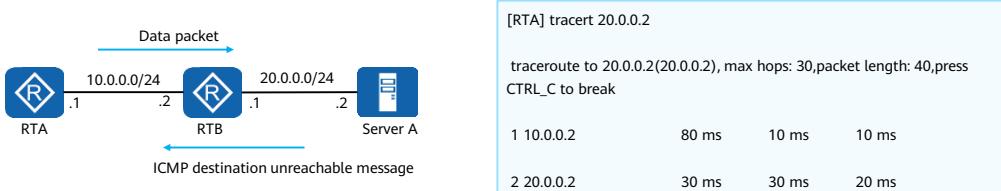


```
[RTA] ping 20.0.0.2
PING 20.0.0.2: 56 data bytes, press CTRL_C to break
Reply from 20.0.0.2: bytes=56 Sequence=1 ttl=254 time=70 ms
Reply from 20.0.0.2: bytes=56 Sequence=2 ttl=254 time=30 ms
Reply from 20.0.0.2: bytes=56 Sequence=3 ttl=254 time=30 ms
Reply from 20.0.0.2: bytes=56 Sequence=4 ttl=254 time=40 ms
Reply from 20.0.0.2: bytes=56 Sequence=5 ttl=254 time=30 ms
--- 20.0.0.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 30/40/70 ms
```



ICMP Error Report

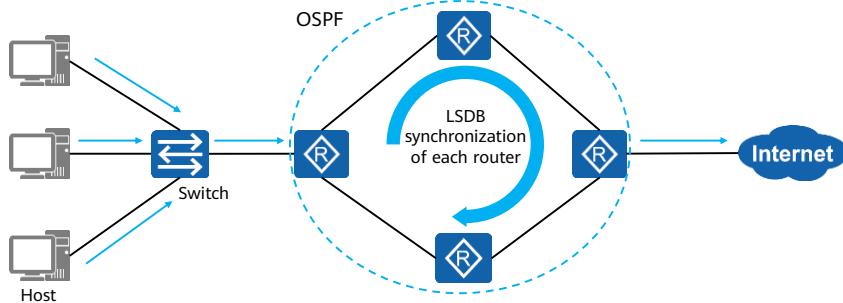
- ICMP defines various error messages for diagnosing network connectivity faults. Based on the error messages, the source device can determine the cause of a data transmission failure. For example, when a network device cannot access a target network, it automatically sends an ICMP destination unreachable message to the transmit device.
- Tracert traces the packet forwarding path hop by hop based on the time to live (TTL) value in the packet header. It is an effective method to check the packet loss and delay and to help administrators find routing loops on a network.



- ICMP defines various error messages for diagnosing network connectivity faults. Based on the error messages, the source can determine the cause of a data transmission failure.
 - If a loop occurs on a network, packets are looped and the TTL times out. In this case, the device sends a TTL timeout message to the sender.
 - If the destination is unreachable, the intermediate device sends a destination unreachable message to the sender. Destinations are unreachable due to various causes. If the device cannot find the destination network, it sends a destination network unreachable message. If the device cannot find the destination host on the destination network, it sends a message indicating the destination host is unreachable.
- Tracert is another typical application of ICMP. Tracert traces the packet forwarding path hop by hop based on the TTL value in the packet header. To trace the path to a specific destination address, the source end first sets the TTL value of the packet to 1. After the packet reaches the first node, the TTL times out. Therefore, this node sends a TTL timeout message carrying the timestamp to the source end. Then, the source end sets the TTL value of the packet to 2. After the packet reaches the second node, the TTL times out. This node also returns a TTL timeout message. The process repeats until the packet reaches the destination. In this way, the source end can trace each node through which the packet passes according to the returned messages. This allows the source end to calculate the round-trip time according to the timestamp information.

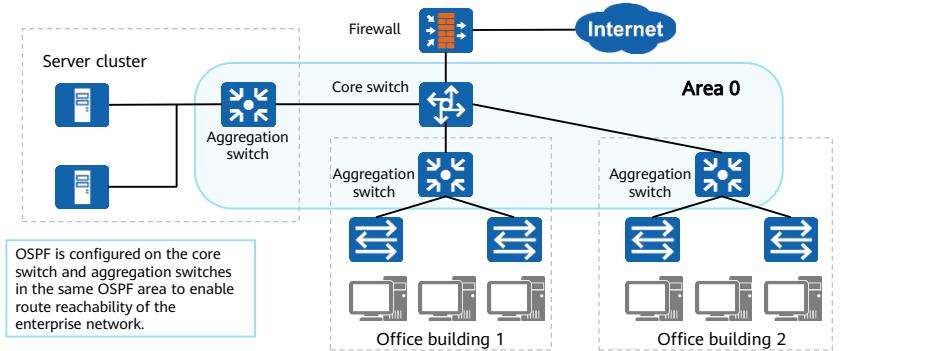
OSPF

- Communications between different networks are implemented through routes. There are three types of routes: direct routes, static routes, and dynamic routes. Dynamic routes have been widely used on networks for high flexibility, reliability, and scalability.
- OSPF is the most widely used dynamic routing protocol on enterprise networks.



OSPF Area

- An OSPF area ID is used to identify an OSPF area.
- An OSPF area is regarded as a logical group of devices.
- Single-area or multi-area networking can be deployed in enterprises based on scales and requirements.

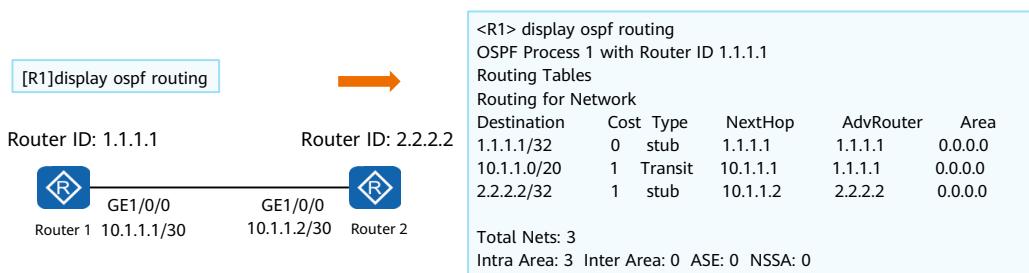


33 Huawei Confidential

- OSPF areas are classified as either a backbone area (with area ID 0) or non-backbone areas.
- On large-scale enterprise networks, OSPF areas can be planned hierarchically. A backbone area (with area ID 0) can be planned between egress and core switches, and non-backbone areas (with area ID 10 and area ID 20) can be planned between core and aggregation switches.

OSPF Routing Table

- Must-knows of OSPF routing tables:
 - An OSPF routing table contains the information used to guide packet forwarding, including the destination address, cost, and next hop.
 - You can run the **display ospf routing** command to check information about the OSPF routing table.



Contents

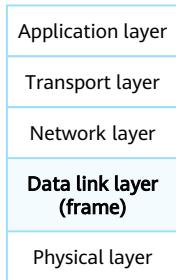
1. Network Reference Model

- OSI Reference Model and TCP/IP Reference Model
- Application layer
- Transport Layer
- Network Layer
- Data Link Layer

2. Common Network Devices

Data Link Layer

- The data link layer is located between the network layer and the physical layer, providing services for protocols such as IP and IPv6 at the network layer.
- Ethernet is the most common data link layer protocol.

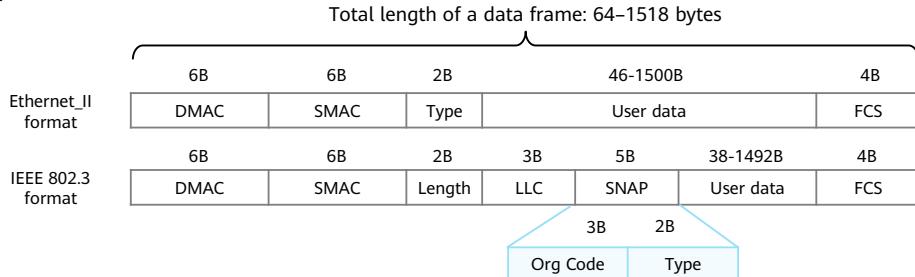


The data link layer is located between the network layer and the physical layer.

- The data link layer provides intra-segment communication for the network layer.
- The functions of the data link layer include framing, physical addressing, and error control.
- Common data link layer protocols include Ethernet, PPPoE, and PPP.

Ethernet Frame Structure

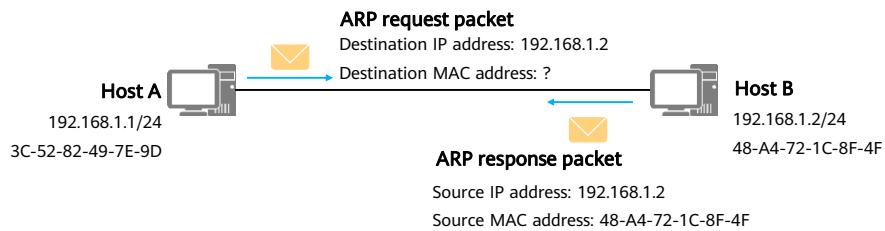
- The frames used by Ethernet technology are referred to as Ethernet frames. Ethernet frames are in two formats, namely, Ethernet II and IEEE 802.3.
- A medium access control (MAC) address uniquely identifies a network interface card (NIC). MAC addresses are used for intra-segment communication, with 48 bits in length, such as 00-1E-10-DD-DD-02.



- Ethernet II frame:
 - DMAC: indicates the destination MAC address, with 6 bytes in length, identifying the MAC address of the receiver.
 - SMAC: indicates the source MAC address, with 6 bytes in length, identifying the MAC address of the sender.
 - Type: indicates the protocol type, with 2 bytes in length. Common values are as follows:
 - 0 x 0800: Internet Protocol Version 4 (IPv4)
 - 0 x 0806: Address Resolution Protocol (ARP)
- IEEE 802.3 LLC frame:
 - SNAP: Sub-network Access Protocol, consisting of the Org Code field and the Type field.
 - FCS: Frame Check Sequence, acting as a 32-bit cyclic redundancy check code (CRCC) detecting whether any error occurs during frame transmission.
 - Logical link control (LLC) consists of the destination service access point (DSAP), source service access point (SSAP), and Ctrl field.
 - DSAP: indicates the destination service access point, with 1 byte in length. If the subsequent type is IP frame, the value is set to 0x06. The function of a service access point is similar to the Type field in an Ethernet II frame or the port number in TCP/UDP.
 - SSAP: indicates the source service access point, with 1 byte in length. If the subsequent type is IP frame, the value is set to 0x06.
 - Ctrl: indicates unnumbered IEEE 802.2 information of a connectionless service, with 1 byte in length, usually set to 0x03.

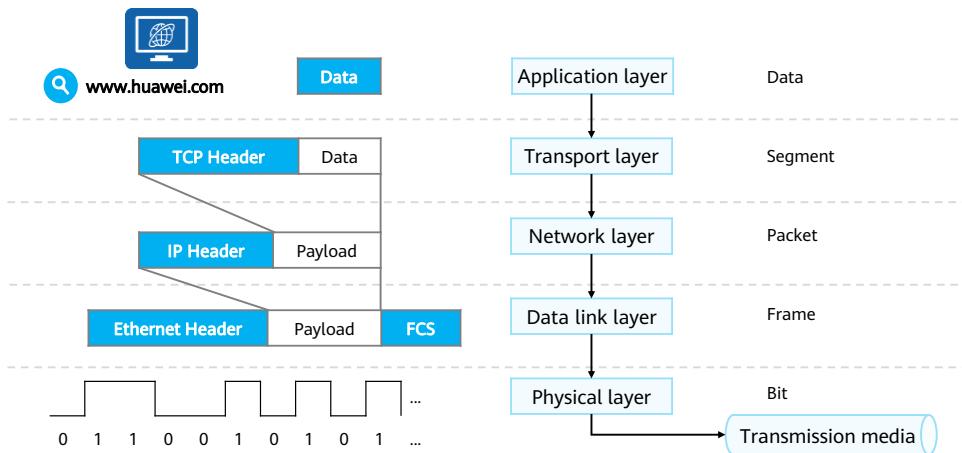
ARP

- To enable normal packet forwarding, the destination address or the gateway MAC address should be obtained. As such, Address Resolution Protocol (ARP) is used to obtain the corresponding MAC address based on the known IP address.



- ARP is a TCP/IP protocol that obtains the data link layer address associated with a given IP address.
- ARP is an indispensable IPv4 protocol, which provides the following functions:
 - Mapping IP addresses into MAC addresses.
 - Maintaining the ARP entry used to store the mapping between a MAC address and a destination IPv4 address.
 - Detecting duplicate IP addresses on a network segment.

Data Encapsulation of a Sender



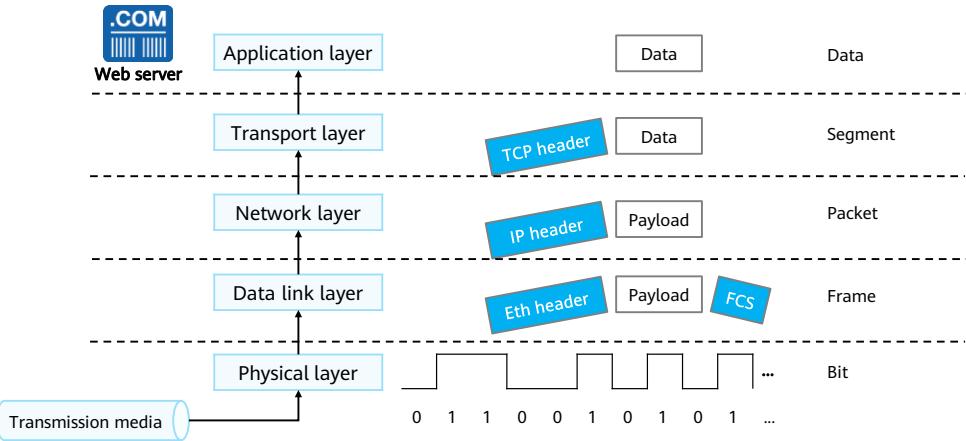
39 Huawei Confidential



- Assume that you are accessing Huawei's official website through the IE browser. After you enter the website address in the address box and press **Enter**, the following things occur on your computer:
 - The IE browser (the application) uses HTTP (the application-layer protocol) to encapsulate the application-layer data. (As shown in the above figure, data should also include an HTTP header, which is not shown here.)
 - HTTP relies on transport-layer protocols (such as TCP) to ensure the reliability of data transmission and transmits the encapsulated data to a transport-layer protocol module.
 - The TCP module adds the corresponding TCP header information (such as the source and destination port numbers) to the data transmitted from the application layer. In this case, the protocol data unit (PDU) is called a segment.
 - On an IPv4 network, the TCP module sends the encapsulated segment to the IPv4 module at the network layer. (On an IPv6 network, the segment is sent to the IPv6 module.)
 - After receiving the segment from the TCP module, the IPv4 module encapsulates the IPv4 header. In this case, the PDU is called a packet.

- As the data link layer uses the Ethernet protocol, after the IPv4 module completes encapsulation, the packet is sent to the Ethernet module (such as the Ethernet NIC).
- After receiving the packet from the IPv4 module, the Ethernet module adds the corresponding Ethernet header and FCS frame trailer to the packet. In this case, the PDU is called a frame.
- After the Ethernet module encapsulates the packet, it sends the data to the physical layer.
- Based on the physical media, the physical layer converts digital signals into electrical signals, optical signals, or electromagnetic (wireless) signals.
- The converted signals are transmitted on the network.

Data Decapsulation of a Receiver

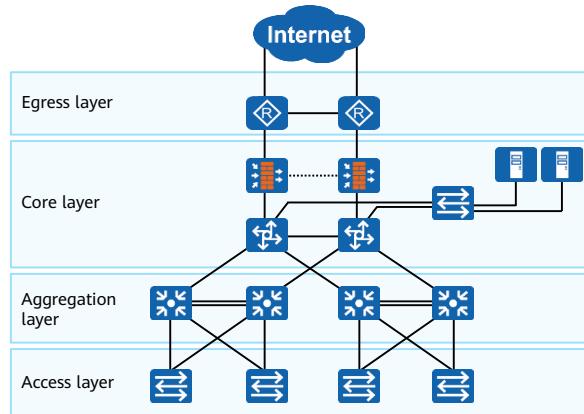


Contents

1. Network Reference Model
2. **Common Network Devices**

Typical Enterprise Campus Network Architecture

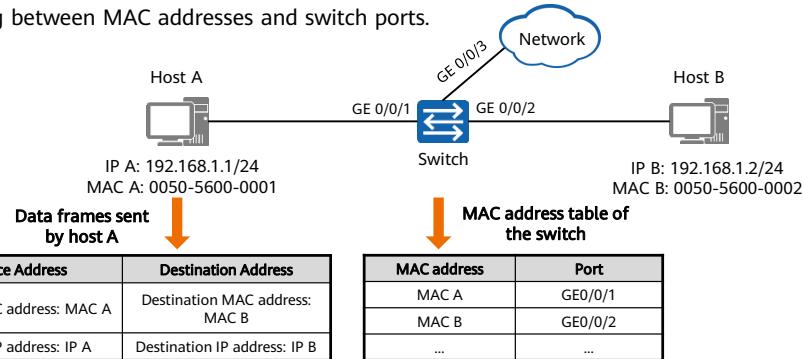
- A typical enterprise campus network consists of switches, routers, firewalls, and servers.



- A typical campus network, consisting of different devices, such as routers, switches, and firewalls, uses a multi-layer architecture which includes the access layer, aggregation layer, core layer, and egress layer.
- A switch is a communication device on the same network segment or across network segments.
- A router is a communication device across network segments.
- A firewall can be deployed at the network egress to implement security protection.

Switch

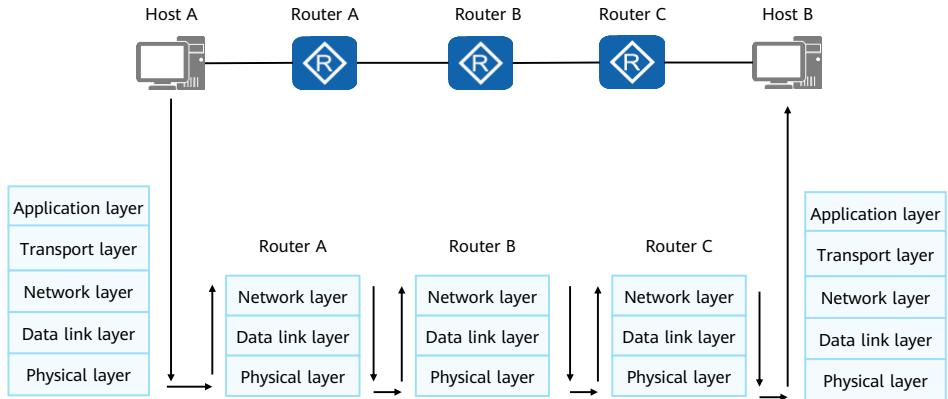
- A switch is the device closest to end users and is used to connect terminals to the network, enabling the forwarding of data frames on the same network segment.
- Switches work at the data link layer and forward data frames based on MAC address tables that store the mapping between MAC addresses and switch ports.



- Layer 2 switches work at the data link layer and forward frames based on MAC addresses. The switch ports used to send data are independent of the switch ports used to receive data. Each port belongs to a different collision domain, which effectively isolates collision domains on the network.
- Layer 2 switches maintain the mapping between MAC addresses and ports by learning the source MAC addresses of Ethernet frames. The table that stores the mapping between MAC addresses and ports is called a MAC address table. Layer 2 switches look up the MAC address table to determine the port to which frames are forwarded based on the destination MAC address.

Router

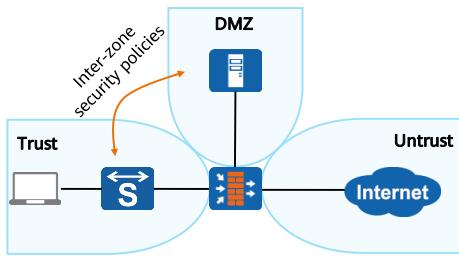
- Routers work at the network layer to ensure that packets can be forwarded between different networks.



- A router is a network-layer device that forwards packets between different networks. As shown in the above figure, host A and host B on different networks (links) can communicate with each other. A router on the same network as host A receives a data frame sent by host A. The data link layer of the router confirms that the frame is sent to itself after analyzing the frame header, and then sends the frame to the network layer. The network layer then determines to which network segment the destination address belongs based on the network-layer packet header of the frame. The router then forwards the frame to the next-hop device through the corresponding interface by checking the routing table until the frame reaches host B.

Firewall

- Firewalls are mainly deployed at network borders to control network access behaviors, with security protection as the key feature.
- Firewalls consider that data flows in the same security zone do not have security risks and no security policy is required. Device security checks are triggered only when data flows between different security zones and security policies are implemented.

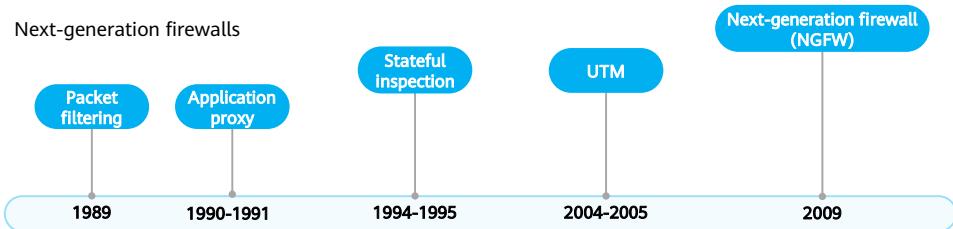


Zone	Default Security Priority
Untrust zone	5 (low security level)
DMZ	50 (medium security level)
Trust zone	85 (high security level)
Local zone	100 (highest security level). A local zone defines a device itself, including interfaces on the device.

- Firewall technologies play an indispensable role in computer network security protection. In a network environment with a large application scope, firewalls technologies are applied to computer network systems to provide effective protections for the collected data. And hardware firewalls are used to solve network security problems in a centralized manner. They are applicable to various scenarios and provide efficient filtering. In addition, they provide security features such as access control, identity authentication, data encryption, VPN technology, and address translation. Users can configure security policies based on their network environments to prevent unauthorized access and protect their networks.

Firewall Development History

- As technologies advance, firewalls have been upgraded from a low level to a higher level, with related functions developing in a simple-to-complex manner. The development of network technologies and the proliferation of demands continue to promote the firewall upgrade.
- Based on the development history, firewalls can be classified into:
 - Packet filtering firewalls
 - Stateful inspection firewalls
 - Next-generation firewalls

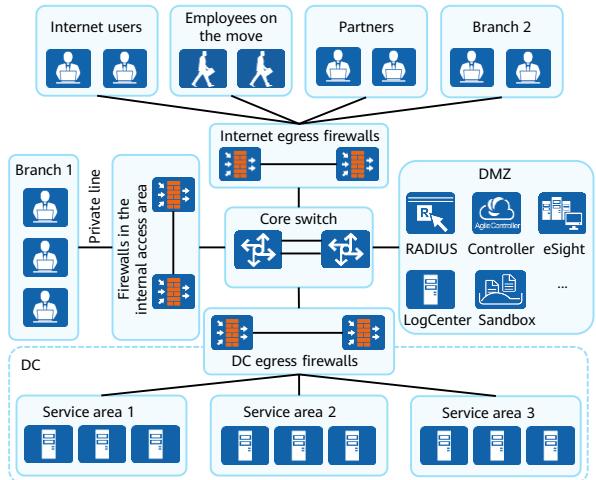


- The earliest firewalls were developed in the 1980s. Over the two decades, the development history of firewalls can be divided into the following three phases:
 - First phase (from 1989 to 1994): Packet filtering firewalls, also known as first-generation firewalls, were developed in 1989 for simple access control. Then, proxy firewalls, also known as second-generation firewalls, were developed, acting as a proxy for communication between the intranet and extranet at the application layer. After that, firewalls based on the stateful inspection technology were developed by Check Point in 1994. The firewalls determine the actions to be taken on packets by dynamically analyzing packet status. They are also known as third-generation firewalls due to fast processing speed and high security as they do not need to proxy each application.
 - Second phase (from 1995 to 2004): Other functions, such as VPN, were added to firewalls. In addition, web application firewalls (WAFs) were developed for web server security protection. In 2004, the industry proposed the concept of United Threat Management (UTM). With UTM, a firewall can implement all-round network security protection with the integration of various functions, including traditional firewall functions, intrusion detection, antivirus, URL filtering, application control, and mail filtering.

- Third phase (from 2005 until now): The rapid development of the UTM market since 2004 led to the proliferation of UTM products, causing new challenges. First, the application-layer information detection is limited and a more advanced detection method is required, facilitating the wide application of the deep packet inspection (DPI) technology. Second, performance is affected. When multiple functions are running at the same time, the processing performance of UTM devices deteriorates greatly. To solve the performance deterioration issue, the next-generation firewall was released in the industry in 2008. The firewall can perform management and control based on users, applications, and content. In 2009, the industry specified the functions and features of the next-generation firewall. Subsequently, multiple security vendors launched their next-generation firewall products, leading to a new era of firewalls.

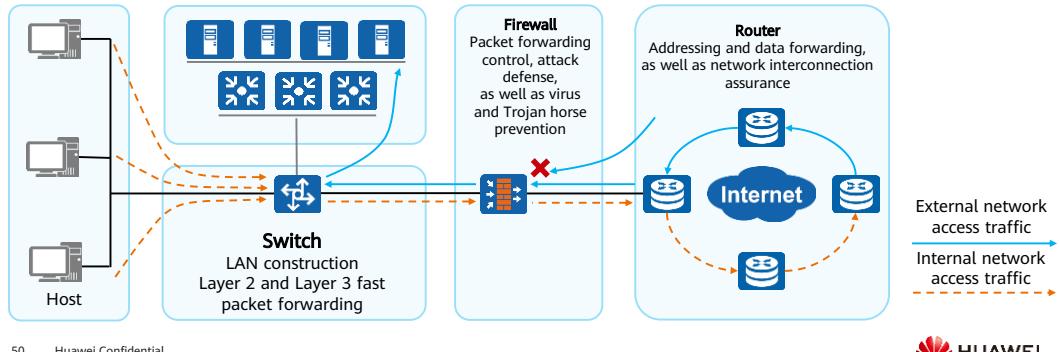
Firewall Functions

- Firewalls protect a network against attacks and intrusions from another network. With isolation and defense attributes, firewalls can be deployed at enterprise network egresses, subnet borders of large-scale networks, and data center (DC) borders.
- The functions of firewalls are as follows:
 - Isolating networks of different security levels
 - Implementing access control (using security policies) between networks of different security levels
 - Implementing user identity authentication
 - Implementing remote access
 - Implementing data encryption and VPN services
 - Implementing network address translation
 - Implementing other security functions



Comparison Between Firewalls, Switches and Routers

- The main functions of switches, routers, and firewalls are different, as switches for constructing LANs, routers for connecting different networks, and firewalls deployed at network borders.
- The core feature of routers and switches is packet forwarding, while that of firewalls is network access control.



50 Huawei Confidential



- Differences between firewalls, routers, and switches:
 - The core feature of routers and switches is packet forwarding, while that of firewalls is network access control.
 - Routers connect different networks and provide connectivity using routing protocols to ensure that packets are forwarded to the destination.
 - Switches are usually used to construct LANs as important hubs for LAN communication and forward packets quickly through Layer 2 or Layer 3 switching.
 - Firewalls are usually deployed at network borders to control network access with security protection as the core feature.

Network Device Login and Configurations

- Network device configurations are involved in the deployment, operation, and maintenance processes. You need to log in to a device before configuring it.
- Administrators can configure network devices on the web UI or through the CLI.

Console login

Telnet login

SSH login

```
Username: admin
Password: Admin@123
Info: The max number of VTY users is 21, the number of current VTY users online is 0, and total number of terminal users online is 1.
<FW> display this
#
sysname FW
#
command-privilege level 0 view system interface
#
Return
```

Web login



HUAWEI
USG6325E

Username: Password:

Login

Download CA Certificate

51 Huawei Confidential



- The default login interface of a firewall is GigabitEthernet0/0/0, which is also called the MGMT interface.
- Web login
 - Default website: <https://192.168.0.1:8443> (or <http://192.168.0.1>)
 - Default user name: admin
 - Default password: Admin@123.

Basic Configuration Commands (1/2)

- Configure an interface IP address.

```
[FW] interface GigabitEthernet 0/0/1  
[FW-GigabitEthernet0/0/1] ip address 10.102.0.1 255.255.255.0
```

This command is used to configure an IP address for a physical or logical interface on a device.

- View current configurations.

```
<FW> display current-configuration
```

- Save a configuration file.

```
<FW> save
```

- Display the saved configuration data.

```
<FW> display saved-configuration
```

- An IP address must be configured for an interface to run the IP service. Generally, an interface needs only one IP address. If a new primary IP address is configured on the interface, the original one is replaced.
- Users can run the **ip address ip-address { mask | mask-length } [sub]** command to configure an IP address for an interface. In this command, the mask field indicates the subnet mask, such as 255.255.255.0, and the mask-length field indicates the mask length, such as 24. Users can either configure the subnet mask or mask length.
- A loopback interface is a logical interface for network or IP host virtualization. A loopback interface can be used as a management interface for its stability and reliability if multiple protocols run at the same time.
- When configuring an IP address for a physical interface, check the physical status of the interface. By default, an interface of a Huawei router or switch is in the Up state. If the interface has been manually disabled, run the **undo shutdown** command to enable the interface.

Basic Configuration Commands (2/2)

- Clear saved configuration data.

```
<FW> reset saved-configuration
```

- View system startup configuration parameters.

```
<FW> display startup
```

This command is used to display related system software, backup system software, configuration files, license files, patch files, and voice files for current and next startup.

- Configure the configuration file for next startup.

```
<FW> startup saved-configuration configuration-file
```

The device loads a specified configuration file for next startup during an upgrade by running this command.

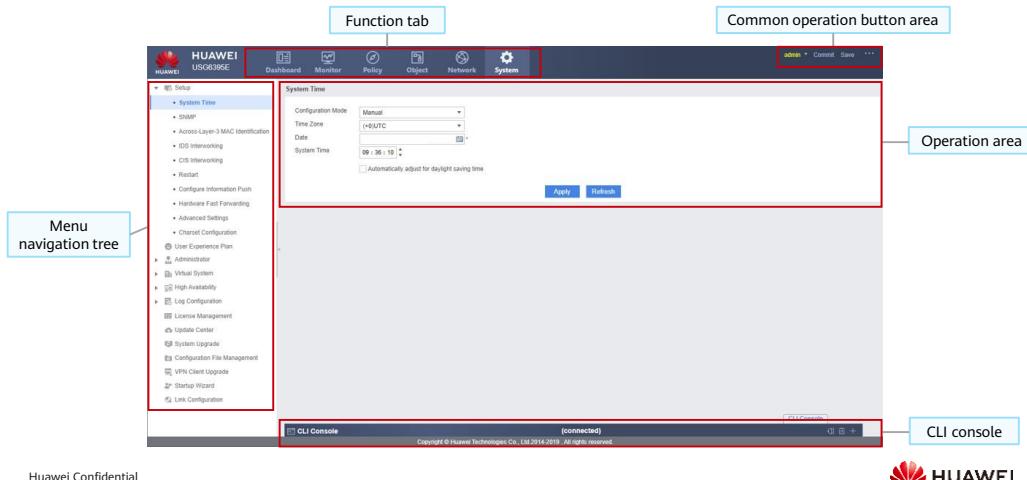
- Restart the device.

```
<FW> reboot
```

- The **reset saved-configuration** command is used to delete configuration files or the saved contents in the files. If the **startup saved-configuration *configuration-file*** command is not run to respecify a configuration file for next startup or the **save** command is not run to save the current configuration, the device is initiated using default parameters for next startup after running the **reset saved-configuration** command.
- The **display startup** command is used to display related system software, backup system software, configuration files, license files, patch files, and voice files for current and next startup.
- The **startup saved-configuration *configuration-file*** command is used to specify the configuration file for next startup and the ***configuration-file*** parameter specifies the name of the configuration file for next startup.
- The **reboot** command is used to restart a device and prompt users to confirm whether to save current configurations before the device restarts.

GUI (1/2)

- Firewall GUIs include the function tab, menu navigation tree, operation area, common operation button area, and CLI console.



GUI (2/2)

- The function tab on the GUI displays firewall functions based on types and is commonly used during firewall configurations on the web UI.

Function Tab	Description
Dashboard	Allows you to quickly view device status and monitor the system running status.
Monitor	Provides comprehensive O&M methods, allowing you to view logs and statistics as well as diagnosing device faults.
Policy	Allows you to configure service policies such as security policies and bandwidth policies to control traffic forwarding and defend against network threats.
Object	Allows you to configure common elements such as addresses and services that are referenced by various service policies, simplifying service configuration.
Network	Allows you to configure network communication functions, such as interfaces, routes, and VPNs, which are the basis for devices to access the network.
System	Allows you to configure device management functions, such as administrator, clock, SNMP, and system upgrade, providing a basis for normal system running.

Configuration File Management

- Choose **System > Configuration File Management** to view the current configuration file and specify a configuration file for next startup.

The screenshot shows the HUAWEI Network Manager interface. On the left, there's a sidebar with various system management options. In the center, under the 'System' category, there's a 'Configuration File Management' section. A red box highlights the 'Configuration File Management' link in the sidebar. Another red box highlights the 'Select' button in the 'Next Startup Configuration File' dropdown. A third red box highlights the 'Save' button in the 'Current Configuration' section. A fourth red box highlights the 'Manage Configuration File' button at the top right of the main content area. A callout arrow points from the 'Manage Configuration File' button to a separate 'Manage Configuration File' dialog box. This dialog box shows a table with two files: 'hdsl1.Hipcdg.zip' and 'hdsl1.Hipcdk.zip'. The 'hdsl1.Hipcdg.zip' file is selected as the 'Next Startup Configuration File'.

File Name	File Size (bytes)	Time of Last Modification	State	Edit	Download
hdsl1.Hipcdg.zip	2,190		Next Startup Configuration File		
hdsl1.Hipcdk.zip	4,074				

Version Upgrade

- Choose **System > System Upgrade** to upgrade the system software, patch files, and feature package files.

The screenshot shows two overlapping windows from the HUAWEI USG6300E management interface.

Left Window: System Upgrade

- Header: HUAWEI USG6300E, Dashboard, Monitor, Policy, Object, Network, **System**, System Upgrade.
- Current Version: USG6300E V100R007C00SPC200 (VRP R) software, Version 5.170.
- Buttons: Delete (highlighted), Download.
- Table: System Upgrade File List

File Name	Current File	Mapfile	Status	Operation
System File	Nat1.v100R007C00SPC200.bin	Nat1V100R007C00SPC200.map	Current file	[Show/Check Upgraded] [Show]
Patch File			Matched with the system set.	[Show/Check Upgraded] [Show]
Current Remotely Con	nat1_v100r007c00spc200_contents...	nat1_v100r007c00spc200_contents...	Matched with the system set.	[Show/Check Upgraded] [Show]
Current Remotely Con			Matched with the system set.	[Show/Check Upgraded] [Show]
URL Remote Query C			Not needed	[Online Upgrade] [Locally Upgraded] [Show]
Closed Sandbox C...			Not needed	[Online Upgrade] [Locally Upgraded] [Show]

Right Window: System Software Management

- Buttons: Upload, Delete, Refresh.
- Table: System Software Management

File Name	File Size (bytes)	Last Modified	Status	Edit	Download
hd1:v100R007C00SPC200.bin	214,261,264		Run		

Quiz

1. (Multiple-answer question) Which of the following protocols can be applied to the application layer? ()
 - A. HTTP
 - B. DNS
 - C. FTP
 - D. OSPF
2. (True or False) Data connection is initiated by the client in active FTP mode. ()
 - A. True
 - B. False

1. ABC
2. B

Summary

- This course describes the TCP/IP reference model, consisting of five layers, including the application layer, transport layer, network layer, data link layer, and physical layer. Each layer provides services for the upper layer, each applied with different protocols. The course also introduces some common protocols, such as ARP, ICMP, FTP, and HTTPS.
- This course describes the typical enterprise network architecture, common network devices, such as switches, routers, and firewalls, as well as the CLI-based and GUI-based firewall configuration modes.

Recommendations

- Visit 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 (1/3)

Acronym and Abbreviation	Full Name
ACK	Acknowledge
ARP	Address Resolution Protocol
C/S	Client/Server
CLI	Command Line Interface
FIN	Finish
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol

Acronyms and Abbreviations (2/3)

Acronym and Abbreviation	Full Name
IS-IS	Intermediate System to Intermediate System
MAC	Media Access Control
OSI	Open Systems Interconnection
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
SFTP	Secure File Transfer Protocol
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell Protocol
STelnet	Secure Telnet
SYN	Synchronize Sequence Numbers
TCP	Transmission Control Protocol

Acronyms and Abbreviations (3/3)

Acronym and Abbreviation	Full Name
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TTL	Time To Live
UDP	User Datagram Protocol
URL	Universal Resource Locator
UTM	United Threat Management
VPN	Virtual Private Network
WAF	Web Application Firewall
WWW	World Wide Web
OSPF	Open Shortest Path First
LSDB	Link State Database

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
portfolio, new technology, 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.



Common Network Security Threats and Threat Prevention



Foreword

- With the development of Internet technologies, the types and frequency of network attacks are increasing. Due to their vulnerability, sensitivity, and confidentiality, information and information systems are vulnerable to threats or attacks, such as DDoS attacks, network intrusions, data breach, and man-in-the-middle attacks. Information system security can be better ensured only when we are familiar with various threat sources and their countermeasures.
- An enterprise network implements data transmission within the enterprise and data exchange between the enterprise and external networks. Enterprise network security is critical to secure production of enterprises. This course describes common network security threats and countermeasures on enterprise networks.

Objectives

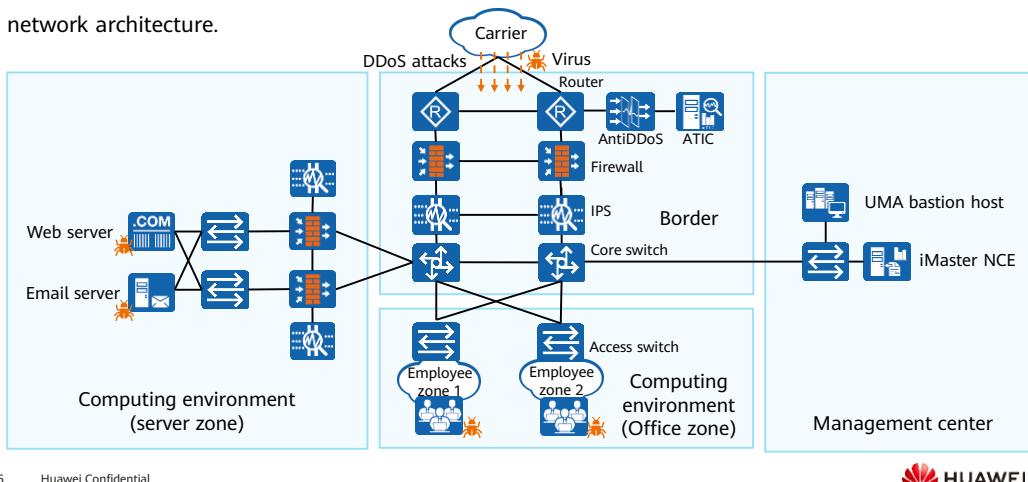
- On completion of this course, you will be able to:
 - Describe common security threats to enterprise networks.
 - Describe how to cope with common network security threats.

Contents

1. Overview of Enterprise Network Security Threats
2. Communication Network Security Requirements and Solutions
3. Zone Border Security Threats and Threat Prevention
4. Computing Environment Security Threats and Threat Prevention
5. Security Requirements and Solutions of the Management Center

Overview of Enterprise Network Security Threats (1/2)

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



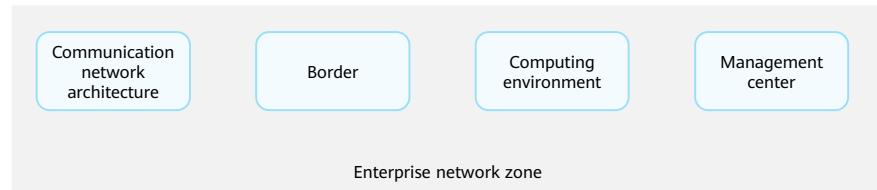
5 Huawei Confidential



- Security threats to enterprise networks are classified into:
 - External threats: security threats from external networks, such as DDoS attacks, network intrusions (such as viruses, Trojan horses, and worms), network scanning, junk mails, phishing emails, and attacks on web servers
 - Internal threats: unreliable network structure, not isolated network, terminals with vulnerabilities, uncontrolled employee behavior, information security violation operations, information breach, malicious employees, permission management disorder, and unauthorized access

Overview of Enterprise Network Security Threats (2/2)

- Enterprises usually take management and technical measures to avoid security risks. In terms of management, enterprises usually formulate various security regulations, O&M requirements, or emergency processes to improve employees' security awareness.
- Security awareness is the basis of all defense measures. Regular security awareness training for all employees and clear security regulations and rules can help enterprises prevent information breach or other information security events caused by misoperations.
- To defend against network security threats, enterprise engineers divide a network into different zones based on threat sources.



- Security threats and defense measures in different zones of an enterprise network:
 - Communication network architecture: is highly reliable to ensure normal service running. Measures such as VPN are taken to ensure the confidentiality and integrity of data transmission.
 - Border zone: The anti-DDoS solution is deployed to defend against DoS attacks. Firewalls are deployed to isolate networks and control traffic. IPS devices are deployed to defend against viruses and intrusions from external networks.
 - Computing environment: Terminal security is hardened to prevent threats caused by vulnerabilities. IPS devices are deployed to defend against intrusions from external networks. Terminal IPS or antivirus software is deployed to defend against virus intrusion.
 - Management center: Bastion hosts are used to control administrator permission, reduce the impact of malicious operations, and monitor O&M operations to ensure that the O&M process is traceable. iMaster-NCE controls employee permission, reduces information breach risks, and prevents unauthorized access.

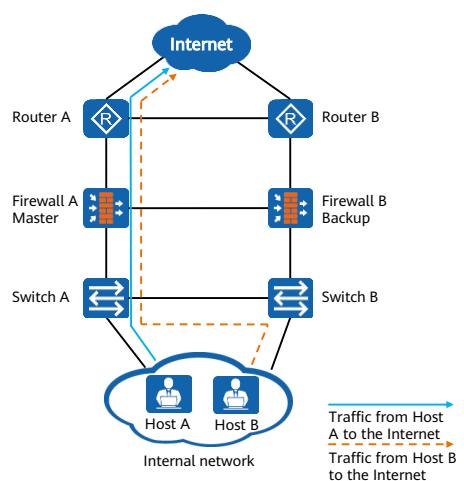
- The preceding network solution involves the following network devices:
 - Router: a communication device on the same network segment or across network segments. It is a basic network device that forwards traffic. For details about routers, refer to *Network Basics*.
 - Switch: a communication device on the same network segment. It is a basic network device that forwards traffic. For details about switches, refer to *Network Basics*.
 - Firewall: the most common security device. It is usually deployed at the enterprise egress for network isolation or traffic control. For details about firewalls, refer to *Network Basics*.
 - IPS device: a professional intrusion prevention device that is usually deployed at the back end of the egress firewall to defend against security threats destined for the internal network. It is typically deployed by midsize and large enterprises.
 - Anti-DDoS device: a professional anti-DDoS device, which is expensive and mainly used by large enterprises, such as banks and Internet companies.
 - UMA bastion host: a professional O&M audit device that is used to manage and control administrators' operation permission and monitor operation processes. It is usually deployed by enterprises as required.
 - iMaster NCE: a common access control device on enterprise networks. It works with switches or firewalls to form the NAC solution that can authenticate employees, authorize access resources, and audit online behaviors.

Contents

1. Overview of Enterprise Network Security Threats
2. **Communication Network Security Requirements and Solutions**
3. Zone Border Security Threats and Threat Prevention
4. Computing Environment Security Threats and Threat Prevention
5. Security Requirements and Solutions of the Management Center

Requirement 1: Network Architecture Reliability

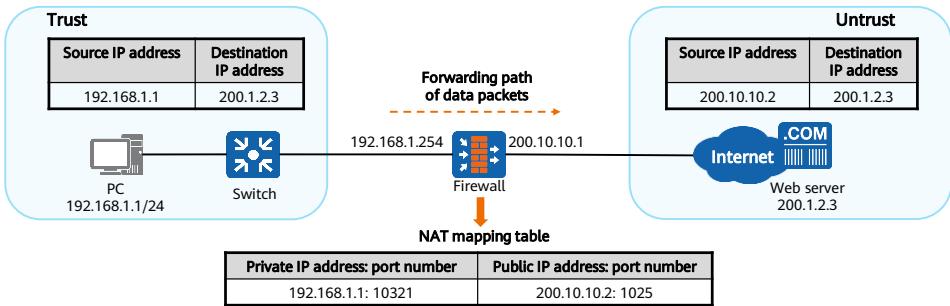
- Starting from grade 3 classified protection (supervised protection), the architecture of the secure communication network must provide hardware redundancy of communication lines, key network devices, and key computing devices to ensure system availability.
- As key devices at the egress of an enterprise network, firewalls must be highly reliable, not only in terms of lines but also in terms of devices. The figure on the right shows the high-reliability networking of firewalls.



- How is traffic forwarded and how can we ensure high service reliability in a scenario where firewalls work in hot standby mode? For details, refer to *Firewall Hot Standby Technologies*.

Requirement 2: Zone Isolation

- Enterprise network resources cannot be directly exposed to the public network to prevent attacks from the Internet. In addition, unauthorized users on the Internet may use IP address scanning or other methods to probe the enterprise network so as to further initiate attacks.
- Generally, a firewall is deployed at the network egress. The firewall isolates the internal network from the external network by dividing the connected network into different security zones. Network address translation (NAT) technology is deployed on the firewall to hide the internal IP addresses to some extent, thereby protecting the internal network.



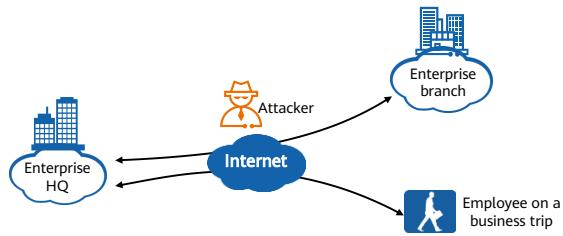
10 Huawei Confidential



- Security zone: It is a basic firewall mechanism. To isolate networks, different security zones cannot directly communicate with each other. To allow traffic from different zones to pass, we need to configure security policies. For details about the principles of security zones and security policies, refer to *Firewall Security Policy*.
- NAT: Multiple private addresses are translated into one or more public addresses. For public network users, only the public addresses of the sender and receiver are visible, which makes the internal network structure invisible. For details about the NAT principle, refer to *Firewall NAT Technologies*.

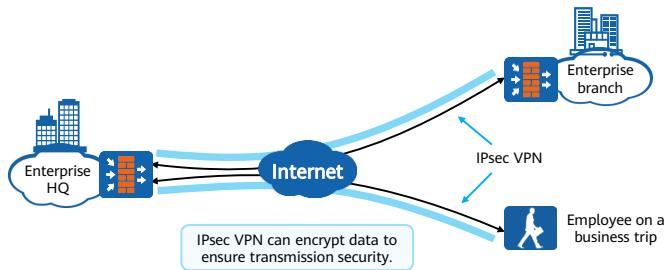
Requirement 3: Information Confidentiality

- An enterprise has employees on business trips, or a large enterprise has multiple branches. When data is transmitted between an employee on a business trip and the headquarters (HQ) or between a branch and the HQ over the insecure Internet, data may be stolen or tampered with due to the following reasons:
 - Enterprise data transmission is not encrypted or the encryption level is insufficient.
 - Man-in-the-middle attack: An attacker establishes an independent connection with each of the two communication parties and exchanges the received data. In this way, the two communication parties consider that they are communicating with each other through a private connection. In fact, the entire session is completely controlled by the attacker. In a man-in-the-middle attack event, the attacker can intercept all packets going between the two communication parties and insert new ones.



Information Confidentiality Security Solution

- Due to the openness of the Internet, the security of data transmission between an enterprise and its branches cannot be ensured. This is where virtual private network (VPN) technology comes in. This technology can be used to establish secure and reliable transmission tunnels on the Internet. Enterprises with great economic strength and high security and reliability requirements can purchase private lines from carriers to meet the interconnection requirements between the HQ and branches.
- Employees on business trips can use L2TP over IPsec or SSL VPN to securely access the enterprise network.



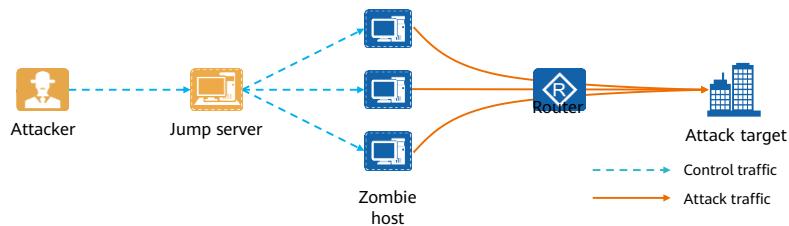
- For details about the principle and configuration of VPN technology, refer to *Encryption Technology Applications*.

Contents

1. Overview of Enterprise Network Security Threats
2. Communication Network Security Requirements and Solutions
3. **Zone Border Security Threats and Threat Prevention**
4. Computing Environment Security Threats and Threat Prevention
5. Security Requirements and Solutions of the Management Center

Threat 1: DDoS Attack

- In a DDoS attack event, an attacker controls a large number of zombie hosts to send a large number of attack packets to the attack target. As a result, links of the network where the attack target resides are congested, system resources are exhausted, and the attack target cannot provide services for authorized users.
- Some malicious competitors may launch DDoS attacks, causing great economic losses to legitimate enterprises. For example, DDoS attacks are launched on online shopping platforms during shopping festivals.

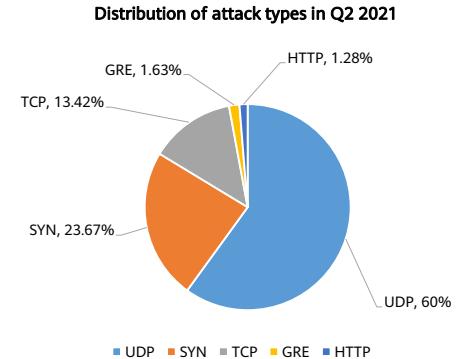


- As more and more IoT devices are connected to the network, hackers can quickly initiate large-scale DDoS attacks by exploiting device hardware or management vulnerabilities. In addition, some attacks tend to speculate people's behavior and habits, and the effect of such attacks becomes more and more obvious.

Types of DDoS Attacks

- DDoS attacks can be classified into TCP flood, UDP flood, ICMP flood, HTTP flood, and GRE flood based on the types of attack packets.

Attack Type	Description
TCP flood	DDoS attacks initiated using TCP, such as SYN flood, SYN+ACK flood, ACK flood, and FIN/RST flood
UDP flood	DDoS attacks initiated using UDP, such as UDP flood and UDP fragment attacks
ICMP flood	An attacker sends a large number of ICMP packets in a short period of time to break down the network, or sends oversized packets to congest network links.
HTTP flood	HTTP flood or low-rate HTTP attacks are initiated via HTTP interaction.
GRE flood	GRE packets are used to initiate DDoS attacks. In a DDoS attack event, GRE packets are decapsulated to consume computing resources of the attack target.

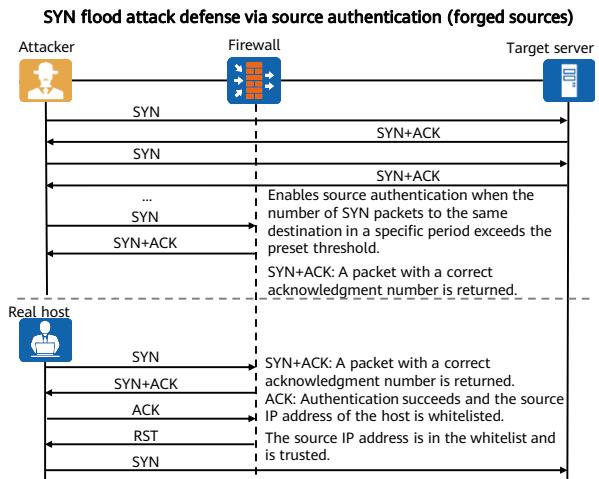


Data source: *kaspersky securelist-DDoS attacks in Q2 2021*



DDoS Attack Defense

- Anti-DDoS devices use different modes, such as source authentication and traffic limiting, to defend against different types of DDoS attacks. The figure on the right shows the working mechanism of defense against SYN flood via source authentication.
- Attackers send SYN packets with forged source addresses to hosts to initiate SYN flood. The hosts reply with SYN+ACK packets to the source addresses, but will not receive any ACK packets. As a result, the hosts keep many half-open connections until the connections time out. These half-open connections exhaust host resources. Therefore, the host fails to establish TCP connections.



- Firewalls or anti-DDoS devices are deployed at the egress of the enterprise network to block external DDoS attacks. Professional anti-DDoS devices can be used to defend against heavy-traffic DDoS attacks.
- When firewalls and anti-DDoS devices are deployed at the same time, the anti-DDoS devices must be deployed in front of the firewalls. Although some firewalls have the anti-DDoS function, the performance of the firewalls may be greatly consumed in the case of heavy-traffic DDoS attacks. As a result, exceptions such as system breakdown may occur.
- In the TCP/IP protocol, TCP uses the three-way handshake mechanism to set up reliable connections. In SYN flood attack events, attackers forge a large number of SYN packets and send them to the victims without completing the three-way handshake.
- SYN flood attacks use forged source IP addresses. That is, attackers send a large number of SYN packets with changing source IP addresses or source port numbers to exhaust the network resources or the target host resources. The anti-DDoS devices can verify the source IP addresses to defend against SYN flood attacks.

Threat 2: Single-Packet Attack

- Unlike DDoS attacks that cause network congestion or consume system resources, single-packet attacks are initiated by sending malformed packets to make hosts or servers break down when processing such packets, or sending special control packets or scanning packets to probe the network structure before launching real attacks.



An attacker uses ICMP packets to probe the target IP address so as to determine which target systems are alive and connected to the target network. Alternatively, the attacker scans ports to probe the open ports of the attacked object and determine the attack mode.



An attacker sends a large number of malformed packets to a host or server. As a result, the host or server breaks down when processing these packets. Typical attacks include Teardrop, Smurf, and Land attacks.

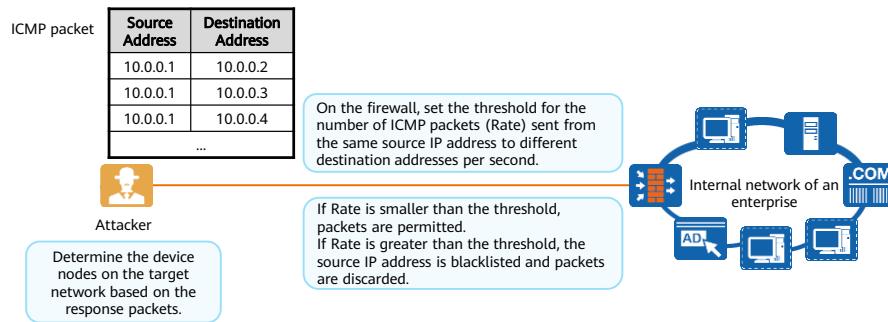


A potential attack behavior that does not directly damage the network. An attacker sends special control packets to probe the network structure and prepare for subsequent attacks. Typical attacks include ultra-large ICMP packet control attacks and IP packet control attacks.

- Scanning attack
 - IP Scan: An attacker probes the target address using the IP address scanning tools to determine whether the target system is alive.
- Malformed packet attack
 - Smurf attack: An attacker sends an ICMP request packet with the destination IP address as the broadcast IP address of the target network and the source IP address as the server address. All hosts on the network respond to the request. All the response packets are sent to servers. As a result, the servers cannot provide services.
- Special packet control attack
 - Tracert packet attack: An attacker discovers the packet transmission path using the ICMP timeout packets returned when the TTL value is 0 and ICMP port unreachable packets returned when the packets reach the destination IP address. In this way, the attacker probes the network structure.
- Both single-packet attacks and DDoS attacks are DoS attacks.

Single-Packet Attack Defense

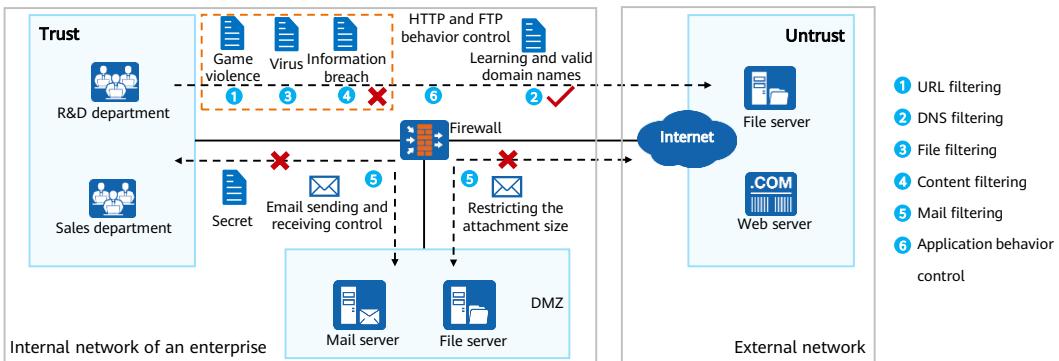
- Firewalls provide the single-packet attack defense function to effectively defend against scanning attacks, malformed packet attacks, and special packet control attacks.
- The mechanisms of single-packet attacks are different, and the defense mechanisms of firewalls are also different. The following describes the mechanism of initiating address scanning attacks as well as the mechanism of defending against such attacks.



- Rate: indicates the number of ICMP packets sent from the same source IP address to different destination IP addresses per second.

Threat 3: Uncontrolled User Behavior

- 70% of information security incidents are caused by misoperations of internal employees or insufficient security awareness. In addition to enhancing employees' security awareness, enterprises need to manage and control employees' Internet access behavior at the technical level. iMaster NCE can be used to manage and control users' access rights, and the content filtering function of the firewall can be used to manage and control users' online behavior.



19 Huawei Confidential



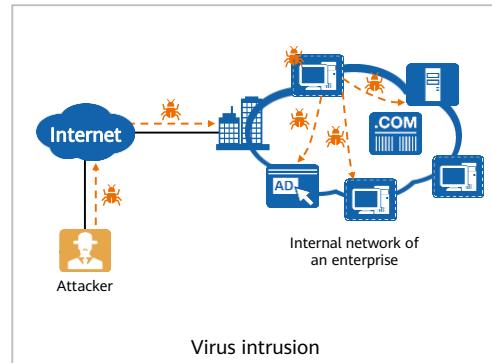
- Enterprises also need to manage and control employees' Internet access behaviors at the technical level. For example, enterprises need to prevent employees from accessing pornographic, gambling, and drug websites, prevent employees from accessing entertainment websites during working hours to improve work efficiency, and prevent employees from unintentionally disclosing personal or important enterprise information.
- Content filtering:
 - Uniform Resource Locator (URL) filtering: controls which URLs are accessible to users to regulate online behaviors.
 - DNS filtering: is implemented in the domain name resolution phase to prevent employees from accessing illegal or malicious websites that may bring threats such as viruses, Trojan horses, and worms.
 - File filtering: blocks the transfer of certain types of files, which reduces the risks of executing malicious codes and infecting viruses on the internal network and prevents employees from transferring enterprises' confidential files to the Internet.

- Content filtering: falls into file content filtering and application content filtering. File content filtering filters the uploaded and downloaded files by keyword. Administrators can specify the protocols for file transfer or the types of files to be filtered. Application content filtering filters application content by keyword. The content filtered varies according to different applications.
- Mail filtering: filters mails by checking the email addresses of the sender and recipient, attachment size, and number of attachments.
- Application behavior control: implements refined control on HTTP- and FTP- based online behaviors (such as upload and download).

Threat 4: External Network Intrusion

- As long as the internal network of an enterprise is connected to an external network, it is vulnerable to external attacks, such as viruses, SQL injection, and DDoS attacks.

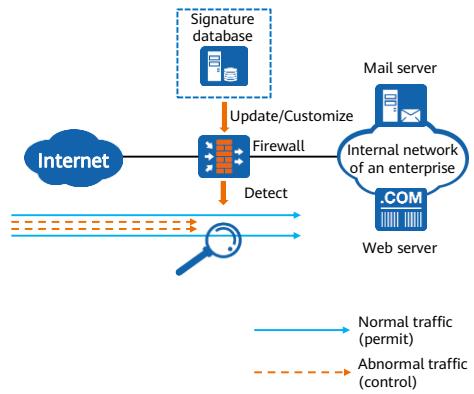
Intrusion Type	Description
Virus	A type of malicious code that can infect or attach to applications or files. It is spread through email or file sharing protocols and threatens the security of user hosts and networks. Viruses can replicate themselves, but they need to be activated manually by opening infected files or enabling macros.
SQL injection	In SQL injection attack events, attackers construct special input as parameters and transfer them to web applications. Most of the input is a combination of SQL syntax. By destroying the original logic of SQL statements, attackers can perform desired operations. SQL injection is a high-risk web vulnerability.
DDoS attack	In DDoS attack events, attackers send a large number of data packets to overload target devices. As a result, network bandwidth or device resources are exhausted.



- After a host on the internal network of an enterprise is infected with viruses, attackers may use the infected host to intrude other hosts and expand the attack effect. As a result, a large number of hosts on the internal network are infected with viruses.

Intrusion Prevention and Security Protection

- The intrusion prevention function of firewalls detects and analyzes all passing packets and determines whether to permit or block the packets in real time. IPS devices can also be used to defend against network intrusions.
- Firewalls and IPS devices are usually deployed at the network egress to defend against threats from the Internet.
- Firewalls and IPS devices are equipped with the intrusion prevention function module. This module compares the traffic passing through the firewalls and IPS devices with the loaded signature database, and processes the traffic based on the risk level. The signature database is a collection of signatures.
- Signature: describes the features of the intrusion behavior on the network and the actions to be taken by a device.



- For more details about the intrusion prevention principle, refer to *Firewall /IPS*.

Contents

1. Overview of Enterprise Network Security Threats
2. Communication Network Security Requirements and Solutions
3. Zone Border Security Threats and Threat Prevention
- 4. Computing Environment Security Threats and Threat Prevention**
5. Security Requirements and Solutions of the Management Center

Terminal Software Vulnerability

- Terminal software on the internal network of an enterprise has vulnerabilities, which can be exploited by attackers. No matter viruses come from the internal or external network, once a terminal on the internal network is infected with viruses, the viruses spread horizontally based on the trust relationships between devices on the internal network. As a result, a large number of terminals on the internal network are infected.
- Common Vulnerabilities and Exposures (CVE) is a platform for disclosing vulnerabilities. It offers IDs as character string features of vulnerabilities.

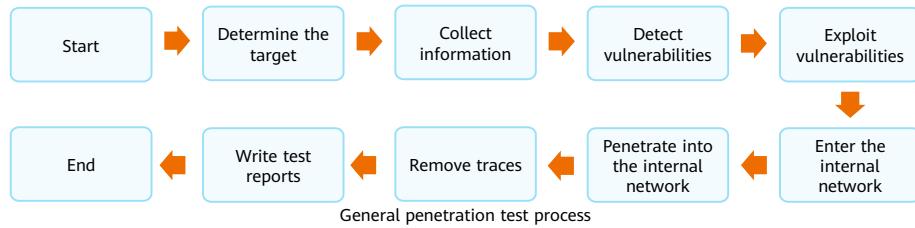
The famous WannaCry ransomware exploits the vulnerabilities of the Windows operating system (OS) to initiate attacks. Many victims may fail to install patches in time. As a result, they are attacked by viruses and files in their computers are encrypted.

A known vulnerability in MSHTML is exploited by a ransomware group to infect victims with malicious ads and encrypt their devices. Attackers can also exploit this vulnerability to send malicious WinWord attachments to Windows users.

A recently disclosed VM software vulnerability can be used to damage the VM management program and punish DoS. This vulnerability can be easily exploited by attackers with high permissions. Once the permissions are obtained, the VM environment may be suspended or frequently broken down.

Terminal Software Vulnerability Handling Methods

- Install patches for system software and application software of enterprise network terminals in a timely manner, and install antivirus software.
- The Network Admission Control (NAC) solution is used to check the security of enterprise network terminals and external terminals and prevent unauthorized terminals from accessing the network.
- Use vulnerability scanning tools to scan enterprise networks and evaluate information security risks. Detect and fix vulnerabilities in network devices in a timely manner.
- Perform penetration tests, employ professionals to evaluate the security of enterprise network systems, and take targeted improvement measures.



Contents

1. Overview of Enterprise Network Security Threats
2. Communication Network Security Requirements and Solutions
3. Zone Border Security Threats and Threat Prevention
4. Computing Environment Security Threats and Threat Prevention
5. Security Requirements and Solutions of the Management Center

Requirement 1: Administrator Permission Control

- In some cases, enterprise employees may perform behaviors that endanger enterprise information security due to interest conflicts or dissatisfaction. For example, they steal enterprise confidential data or damage enterprise network infrastructure.



Driven by virtual currency interests, an employee of an enterprise exploited computing resources of the enterprise's servers to conduct mining activities and gained hundreds of thousands of CNY. The employee's behavior was disclosed and sanctioned by laws. However, the enterprise's server resources were embezzled, affecting the normal running of services.

An employee of an enterprise maliciously damaged the online production environment of the enterprise due to personal mental status and life reasons. The production environment and data were severely damaged, and the interests of the enterprise and its customers were also severely impaired. Eventually, the employee was sanctioned by laws.

Driven by interests, an employee of an enterprise stole confidential information of the enterprise by taking photos or sending emails to external mail accounts before resignation. The employee was finally sanctioned by laws.

Solution: Administrator Permission Control

- The possible information security risk behaviors of enterprise employees can be handled from two aspects: technology and management.
- Technology
 - **More strict permission management:** Accounts with different permissions are set for enterprise employees at different levels. The O&M permission must comply with the minimum authorization principle. For example, the UMA can be used to centrally control the O&M permissions of administrators and monitor administrator behaviors.
 - **More reliable backup mechanism:** If the production environment and data are damaged, the data can be quickly restored to minimize the loss.
- Management
 - Frequently publicize information security cases in enterprises to improve employees' security awareness.
 - The access control system can be used in zones with high security requirements.
 - Pay attention to the work and life status of employees and provide timely psychological counseling to prevent information security risks caused by psychological problems.

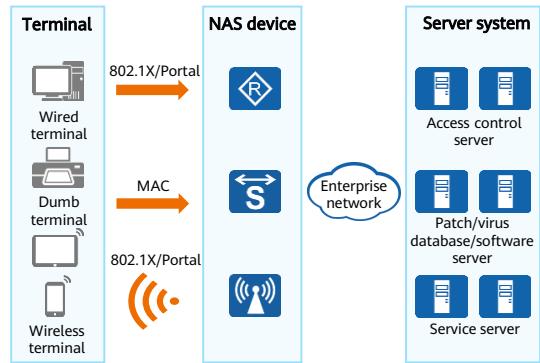
Requirement 2: Internet Access Permission Control

- In addition to the security risks brought by external networks, the security risks brought by the internal networks of enterprises are increasing. Unauthorized access to the enterprise networks may cause damage to the service systems and breach of key information assets.
 - Malicious users may damage or steal information after accessing the network.
 - If a terminal that accesses the internal network of an enterprise is infected with viruses, the viruses may spread on the network.
- We can cope with unauthorized access from two aspects: technology and management.
 - Technology: Use the NAC solution.
 - Management: Strict administrative management is performed on personnel entering and leaving the enterprise.



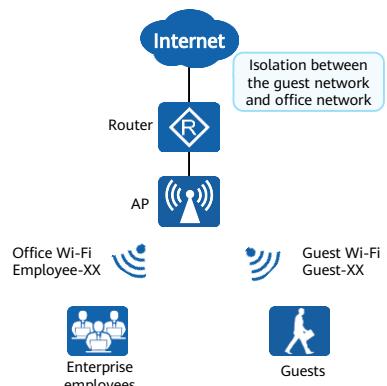
Solution: Internet Access Permission Control (1/2)

- To prevent unauthorized access, Huawei provides the NAC solution to implement security control on access users. Only authorized users and secure terminals can access the network.
- The solution provides the following functions:
 - **Identity authentication:** Authenticate the identities of users who attempt to access the enterprise network. Only authorized users can access the network.
 - **Access control:** Users are precisely matched based on the user identity, access time, access location, terminal type, and access mode to control the resources that users can access.
 - **Terminal security check:** Only healthy and secure terminals can access the network.



Solution: Internet Access Permission Control Solution (2/2)

- Management approaches can be used to regulate the entry of employees into the enterprise and strictly control the entry of external personnel.
 - Visitors must register in advance and show valid certificates before entering the enterprise.
 - Employ security personnel and use security equipment to control the entry of visitors and vehicles.
 - The access control system can be used in important zones of the enterprise to prevent unauthorized personnel from entering these zones.
 - Storage devices such as USB flash drives are forbidden from being inserted into devices such as computers without permission.
- Create a guest network for external users to access. The guest network is isolated from the enterprise office network to eliminate security risks.



Quiz

1. (Single-answer question) Which of the following data filtering functions can prevent employees from disclosing their identity information to the Internet? ()
 - A. Mail filtering
 - B. File filtering
 - C. URL filtering
 - D. Content filtering
2. (True or false) Even if illegitimate traffic is filtered out through source authentication, the traffic destined for the target server is still heavy. In this case, traffic limiting can be performed to protect the target server. ()
 - A. True
 - B. False

1. D
2. A

Summary

- This course briefly introduces the types and sources of common information security threats, describes the principles and impacts of different attacks, and outlines the countermeasures and solutions for different threats.
- On completion of this course, you will be able to have a comprehensive grasp of security threats and lay a foundation for further study.

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 and Abbreviation	Full Name
AntiDDoS	Anti Distributed Denial of Service
ATIC	Abnormal Traffic Inspection & Control System
CVE	Common Vulnerabilities and Exposures
DMZ	Demilitarized Zone
DoS	Denial of Service
GRE	Generic Routing Encapsulation
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
L2TP	Layer 2 Tunneling Protocol
NAC	Network Admission Control
SSL	Secure Sockets Layer
UMA	Unified Maintenance Audit

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
portfolio, new technology, 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 Security Policies



Foreword

- Communication has always been with us ever since the origin and development of human society. The rapid development of information technologies, especially the emergence of new technologies, business forms, and applications, brings great dividends to social development and people's lives. However, this also brings new challenges to cyber security. As the first line of defense for cyber security protection, firewalls play a vital role.
- This course introduces the principles and application scenarios of firewall security policies.

Objectives

- Upon completion of this course, you will be able to:
 - Describe firewall security zones.
 - Describe the stateful inspection and session mechanisms of the firewall.
 - Describe the application scenarios of the firewall on the network.

Contents

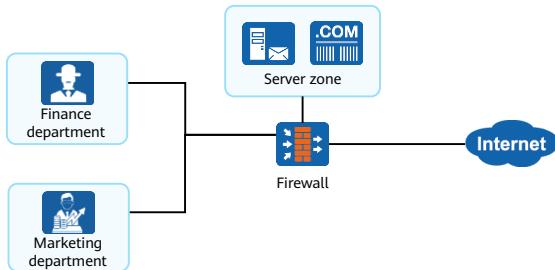
1. Firewall Basic Principles

- Security Zone
 - Security Policy
 - Stateful Inspection and Session Mechanisms
 - ASPF Technology

2. Application Scenarios of Firewalls in Cyber Security Solutions

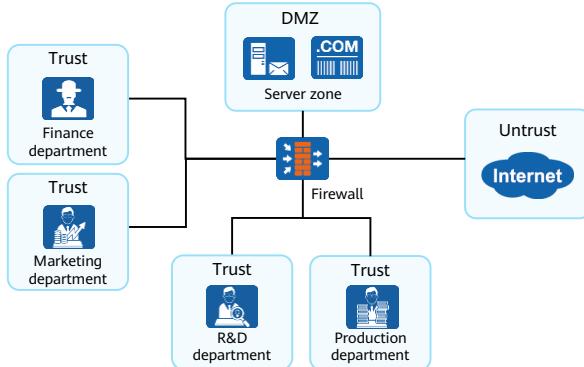
Background of Firewall Security Zones

- A firewall is not only an "ingress barrier", but also an access control point for multiple networks. All data flows entering and leaving the intranet pass through the firewall to serve as a gateway for information incoming and outgoing.
- As shown in the figure, the firewall is an important part of the enterprise network and connects the finance department network, the marketing department network, as well as the server network. The firewall is generally deployed at the enterprise network egress and is connected to the Internet.



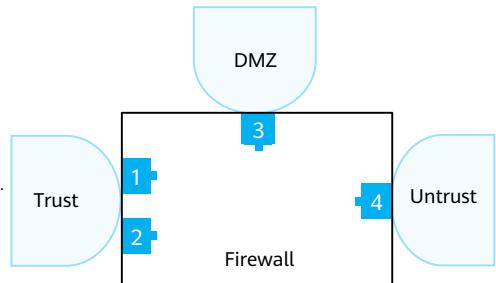
Basic Concepts of Firewall Security Zones

- A security zone contains one or more interfaces. This is the main feature that distinguishes a firewall from a router. Firewalls use security zones to divide networks and mark the "routes" of packets. Security checks are triggered only when packets travel between security zones.



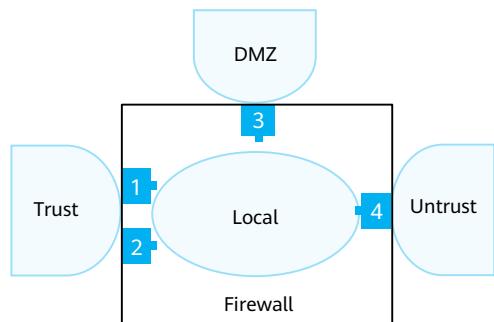
Default Security Zones

- By default, Huawei firewalls provide three configurable security zones: Trust, DMZ, and Untrust.
 - Trust zone
 - The network is highly trusted.
 - It is used to define the network where internal users reside.
 - DMZ zone
 - The network is moderately trusted.
 - It is used to define the network where internal servers are located.
 - Untrust zone
 - The network is not trusted.
 - It usually defines insecure networks such as the Internet.



Local Security Zone

- The Local zone represents the firewall itself.
- Packets that are actively sent by the firewall can be considered as being sent from the Local zone. Packets that need to be responded to and processed by the firewall (not forwarded) can be considered as being received by the Local zone.
- No interface can be added to the Local zone, but all service interfaces on the firewall belong to the Local zone.
- Due to the special characteristics of the Local zone, in the scenarios where the device needs to transmit and receive packets, you should enable the security policy between the Local zone and the security zone where the peer device resides. Such applications include Telnet login, web page login, and SNMP NMS access.



Security Zones, Trust Levels, and Priorities

- Different networks have different trust levels. How can we determine the trust level of a security zone on a firewall?
- On a Huawei firewall, each security zone has a unique priority, represented by a number ranging from 1 to 100. A greater number indicates a more trusted security zone.
 - Trust levels of the default security zones: Local > Trust > DMZ > Untrust.
 - You can create security zones and define their priorities based on the actual networking.

Security Zone	Priority	Description
Local	100	Zone of the device itself, including its interfaces.
Trust	85	Zone where intranet device users are located.
DMZ	50	Zone where intranet servers are located.
Untrust	5	Zone of insecure networks, such as the Internet.

Packets between different security zones are controlled by the firewall. How can we ensure the interzone communication?

Contents

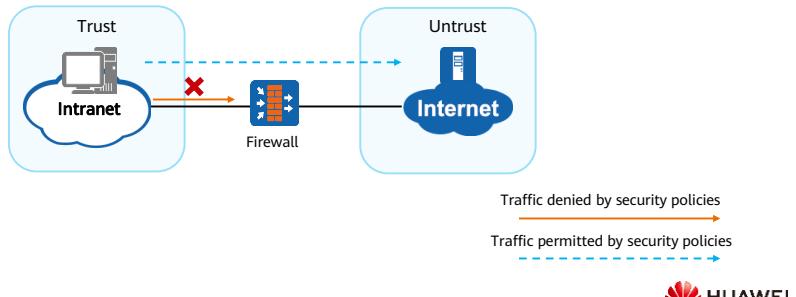
1. Firewall Basic Principles

- Security Zone
- **Security Policy**
- Stateful Inspection and Session Mechanisms
- ASPF Technology

2. Application Scenarios of Firewalls in Cyber Security Solutions

Interzone Communication: Security Policies

- The basic function of a firewall is to control access of data entering and leaving the network. It protects a specific network against attacks from "untrusted" networks, and also allows legitimate communication between two networks. A firewall generally uses security policies to implement the preceding functions.
- Security policies consist of matching conditions (such as 5-tuples, users, and time ranges) and actions. After receiving traffic, the firewall identifies traffic attributes (such as 5-tuples, users, and time ranges) and matches the traffic attributes with the matching conditions of the security policy.

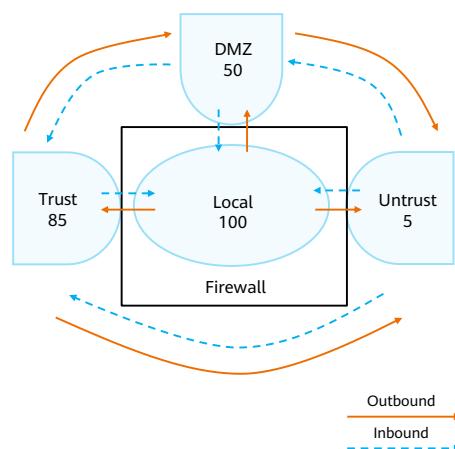


11 Huawei Confidential

- Security policies consist of matching conditions (such as 5-tuples, users, and time ranges) and actions. After receiving traffic, the firewall identifies traffic attributes (such as 5-tuples, users, and time ranges) and matches the traffic attributes with the matching conditions of the security policy. If all conditions of a security policy are matched, the traffic matches the security policy. In this case, the device performs the following actions:
 - If the action is permit and content security detection is not configured, the traffic is allowed to pass through.
 - If the action is permit and content security detection is configured, the device determines whether to allow the traffic according to the result of content security detection.
 - If the action is set to deny, traffic is not allowed to pass through.

Security Interzone, Security Policy, and Packet Flow Direction

- A security interzone specifies the traffic transmission channel, which is the only "road" between two zones. If you want to detect the traffic passing through this channel, you must set a "passcard" on the channel, such as a firewall security policy.
 - Any two security zones form an interzone and have a separate interzone view.
 - Data flows between security zones are directional, including inbound and outbound.



Security Policy Matching Process

- The basic design principle of a firewall is to **deny all traffic by default unless otherwise specified**. This ensures that the firewall can protect the cyber security once it is connected to the network.
- To allow certain traffic, create a security policy. Generally, multiple security policies are configured for different service traffic.
- The security policy matching process is as follows:

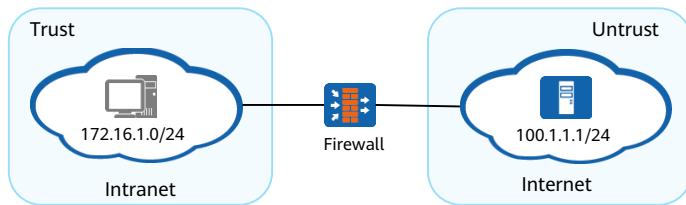


Policy ID	Matching Condition				Action
Policy 1:	Matching condition 1	Matching condition 2	...	Matching condition N	Permit or Deny
Policy 2:	Matching condition 1	Matching condition 2	...	Matching condition N	Permit or Deny
...					
Policy N:	Matching condition 1	Matching condition 2	...	Matching condition N	Permit or Deny
Default:	Any				Deny

- Whether traffic in the same security zone and traffic between different security zones is controlled by the default security policy is described as follows:
 - Traffic between different security zones (including but not limited to traffic sent from firewalls and traffic received by firewalls) is controlled by the default security policy.
 - By default, traffic in the same security zone is not controlled by the default security policy, and the default forwarding action is permit. If traffic in the same security zone needs to be controlled by the default security policy, you can enable this function as required. After it is enabled, the configuration of the default security policy will take effect on the traffic in the same security zone, including the actions of the default security policy and the logging function.
- The default action and logging function (including policy matching logs, session logs, and traffic logs) can be modified in the default security policy.

Security Policy Configuration Example (1)

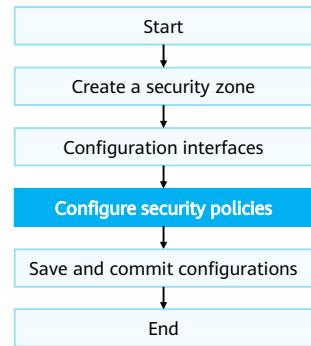
- Requirement description:
 - A company deploys a firewall at the network border as a security gateway. To ensure that users on the 172.16.1.0/24 network segment can access the Internet, configure corresponding security policies on the firewall.
 - PCs at 172.16.1.1, 172.16.1.2, and 172.16.1.3 have high security requirements and are not allowed to access the Internet.



- Multiple types of service traffic may exist on the network. Multiple security policies are configured on the device for different service traffic. To ensure correct security policy configuration, the administrator needs to plan security policies before configuring them. The roadmap for security policy planning is as follows:
 - Understand the information assets and services of the company and assess the possible risks.
 - Understand the company's services and identify information assets that need to be protected, including potential threats to the assets. For example, intellectual property is the most valuable asset of a technology company. One of the biggest threats to the company's assets is source code theft.
 - Dividing the network into security zones simplifies management. The administrator needs to specify the security zones to be divided, how the interfaces are connected, and the security zones to which interfaces are to be added. Traffic cannot flow across security zones unless a security policy with the action of permit is configured, which prevents attackers from entering the network. Deploying security policies based on security zones, users, and applications can prevent attackers from moving horizontally. A fine-grained zone allows only specific users to access specific applications and resources.
 - Identify services and applications, and determine the service blacklist, whitelist, and graylist.
 - Identify the application whitelist (applications that can be accessed), classify the applications based on services, and apply different policies to the applications.
 - Identify the blacklist of applications that are not allowed and apply different policies to them.
 - Add authorized applications that are detected during the operation of the enterprise to the graylist, for example, applications that use non-well-known ports and applications developed by enterprises.

Security Policy Configuration Example (2)

- Configuration roadmap:
 - The administrator specifies the security zones to be divided, how the interfaces are connected, and the security zones to which interfaces are to be added.
 - The administrator classifies employees by source IP address or user.
 - To allow access from a certain type of network, set the action of the security policy to permit. To deny access from certain addresses, set the action of the security policy to deny.
 - List the parameters in the security policies, sort the policies from the most specific to the least specific, and configure security policies in this order.



Security Policy Configuration Example (3)

- Create a security policy rule that denies the access of three special IP addresses to the Internet.

```
[FW] security-policy  
[FW-policy-security] rule name policy1  
[FW-policy-security-rule-policy1] source-zone trust  
[FW-policy-security-rule-policy1] destination-zone untrust  
[FW-policy-security-rule-policy1] source-address 172.16.1.1 32  
[FW-policy-security-rule-policy1] source-address 172.16.1.2 32  
[FW-policy-security-rule-policy1] source-address 172.16.1.3 32  
[FW-policy-security-rule-policy1] action deny
```

- Create a security policy rule that allows the 172.16.1.0/24 network segment to access the Internet.

```
[FW] security-policy  
[FW-policy-security] rule name policy2  
[FW-policy-security-rule-policy2] source-zone trust  
[FW-policy-security-rule-policy2] destination-zone untrust  
[FW-policy-security-rule-policy2] source-address 172.16.1.0 24  
[FW-policy-security-rule-policy2] action permit
```

Contents

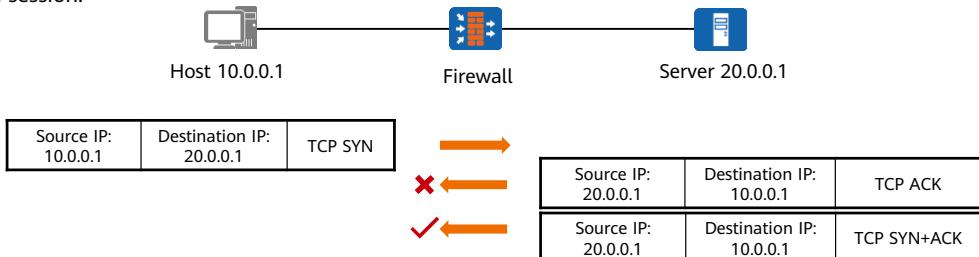
1. Firewall Basic Principles

- Security Zone
- Security Policy
- **Stateful Inspection and Session Mechanisms**
- ASPF Technology

2. Application Scenarios of Firewalls in Cyber Security Solutions

Stateful Inspection Mechanism

- A stateful inspection firewall uses a detection mechanism based on the connection status and treats all the packets belonging to one connection as a data flow. It considers packets in a data flow related to each other.
- When the stateful inspection mechanism is enabled, a session can be created only when the first packet passes the inspection performed by the firewall. Subsequent packets are forwarded based on the session.



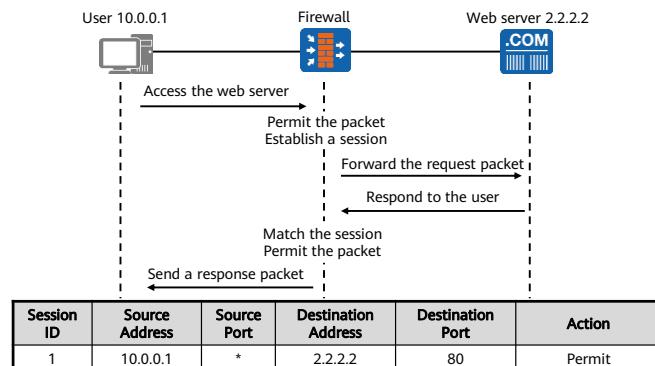
18 Huawei Confidential



- When the stateful inspection mechanism is disabled, even if the first packet does not pass through the firewall, subsequent packets can trigger the generation of a session as long as they pass through the firewall.
- In a network where the incoming and outgoing paths of packets are different, the firewall may receive only the subsequent packets during communication. In this case, you must disable stateful inspection of firewall to ensure normal services. After the stateful inspection function is disabled, sessions can be established through subsequent packets to ensure proper service running.

Session Mechanism

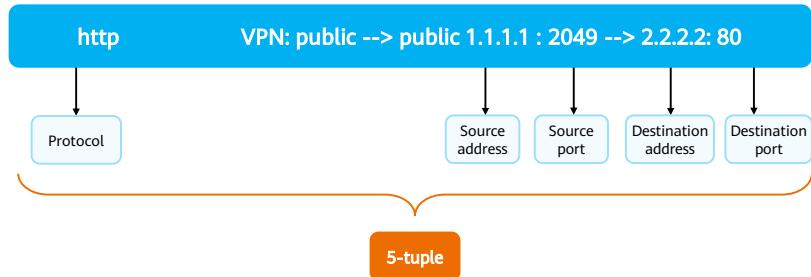
- The firewall treats all packets belonging to a connection as a data flow (session). A session is an entry used to record the connection status of protocols such as TCP, UDP, and ICMP, and is fundamental for the firewall to forward packets.



- The firewall adopts the state-based packet control mechanism. The firewall determines the status of a connection by detecting only the first packet or a small number of packets. A large number of subsequent packets are controlled based on the status of the connection. This stateful detection mechanism rapidly improves the detection and forwarding efficiency of the firewall. The session table records the status of a connection. When forwarding TCP, UDP, and ICMP packets, the device needs to query the session table to determine the connection to which the packets belong and take corresponding measures.

5-Tuple Information in Session Tables

- A session represents a connection between communication parties and indicates the connection status.
 - 5-tuple information in the session table can uniquely identify a connection between two communication parties.
 - On firewalls, the time before a session is deleted is called the aging time of the session.
 - A session represents a connection between two communication parties. Multiple session entries form a session table.



- The firewall sets the session aging mechanism for various protocols. A session that is matched by no packet within the aging time is deleted from the session table. This mechanism prevents the device resources of the firewall from being consumed by a large number of useless and outdated session entries. For some special services, the interval between two consecutive packets of a session can be long. Examples are as follows:
 - When users download large files through FTP, control packets are sent over the control channel only after a long period of time.
 - Users query the data on a database server, and the time between two query operations is far greater than the aging time of the TCP session.
- In the preceding scenarios, if the session entries are deleted, the corresponding service is interrupted. The persistent connection mechanism sets an excessively long aging time for some connections to effectively solve this problem.

Other Information in Session Tables

- Run the **display firewall session table** command on the firewall to view the established sessions.

```
<FW> display firewall session table
Current Total Sessions : 1
telnet VPN:public --> public 192.168.3.1:2855-->192.168.3.2:23
```

- Run the **display firewall session table verbose** command on the firewall to view detailed information about the session table. Because the **verbose** parameter is used, you can view information in addition to the 5-tuple information.

```
<FW> display firewall session table verbose
Current Total Sessions : 1
icmp VPN:public --> public ID: a58f3fe91023015aa15344e75b
Zone: local--> trust TTL: 00:00:20 Left: 00:00:09*
Interface: GigabitEthernet0/0/0 NextHop: 10.1.2.2 MAC: 4437-e697-78fe
<-packets:3 bytes:252 -->packets:3 bytes:252
10.1.1.1:43982[1.1.1.1:2107]-->10.1.2.2:2048
```

- Description of the **display firewall session table** command output:
 - Current Total Sessions**: number of current session entries.
 - telnet**: protocol name. In the command output, **telnet** indicates the Telnet protocol.
 - VPN: public -->public**: *Name of a VPN instance*: in the format of source direction --> destination direction.
 - 192.168.3.1:2855-->192.168.3.2:23**: session table information.
- Description of the **display firewall session table verbose** command output:
 - Current Total Sessions**: number of current session entries.
 - icmp**: protocol name. In the command output, **icmp** indicates the protocol.
 - VPN: public --> public**: *Name of a VPN instance*: in the format of source direction --> destination direction.
 - ID**: session ID.
 - Zone: local--> trust**: security zone of the session, in the format of source security zone --> destination security zone.
 - TTL**: total lifetime of the session table.
 - Left**: remaining lifetime of the session entry.
 - Interface**: outbound interface of forward packets.
 - NextHop**: next-hop IP address of forward packets.

Contents

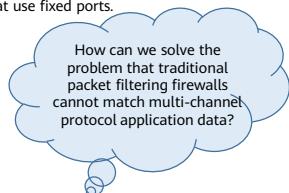
1. Firewall Basic Principles

- Security Zone
- Security Policy
- Stateful Inspection and Session Mechanisms
- ASPF Technology

2. Application Scenarios of Firewalls in Cyber Security Solutions

Background of ASPF

- In the TCP/IP model, the application layer provides common network application services, such as Telnet, HTTP, and FTP. Application layer protocols can be classified into single-channel and multi-channel application layer protocols based on the number of occupied ports.
 - Single-channel application layer protocol: protocol that occupies only one port during communication. For example, Telnet occupies only port 23 and HTTP occupies only port 80.
 - Multi-channel application layer protocol: protocol that occupies two or more ports during communication. For example, in FTP passive mode, port 21 and a random port are occupied.
- Traditional packet filtering firewalls have the following disadvantages for multi-channel application layer protocol access control:
 - Traditional packet filtering firewalls can only implement simple access control.
 - Traditional packet filtering firewalls can only block application data for some single-channel protocols that use fixed ports.

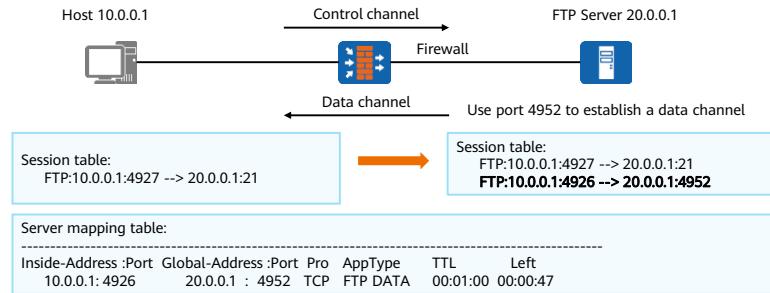


How can we solve the problem that traditional packet filtering firewalls cannot match multi-channel protocol application data?

- Multi-channel protocols need to negotiate the address and port of the subsequent data channel in the control channel, and then establish the data channel connection according to the negotiation result. The IP addresses and ports of data channels are dynamically negotiated and cannot be known by the administrator. Therefore, precise security policies cannot be formulated. To ensure the smooth establishment of data channels, all ports must be opened. This may cause attacks on the server or client.

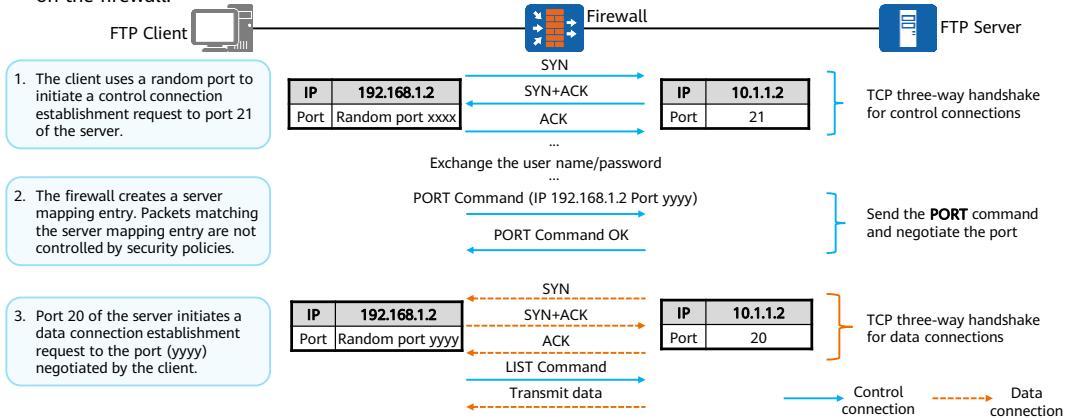
Application of ASPF in Multi-channel Application Protocols

- ASPF is used to filter packets at the application layer.
 - By detecting the address and port information carried at the application layer of negotiation packets, the firewall automatically generates a corresponding server mapping entry. When the first packet of a data channel passes through the firewall, the firewall generates a session based on the server mapping entry to permit subsequent packets in the data channel, which is equivalent to automatically creating a refined security policy. For all connections of a specified application protocol, ASPF maintains status information of each connection and dynamically determines whether to permit data packets to pass through the firewall or discard data packets.



ASPF in FTP Active Mode

- The server mapping table is a refined security policy automatically generated by ASPF and is an "invisible channel" on the firewall.



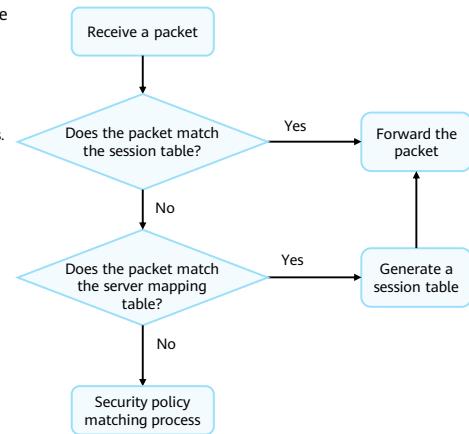
25 Huawei Confidential



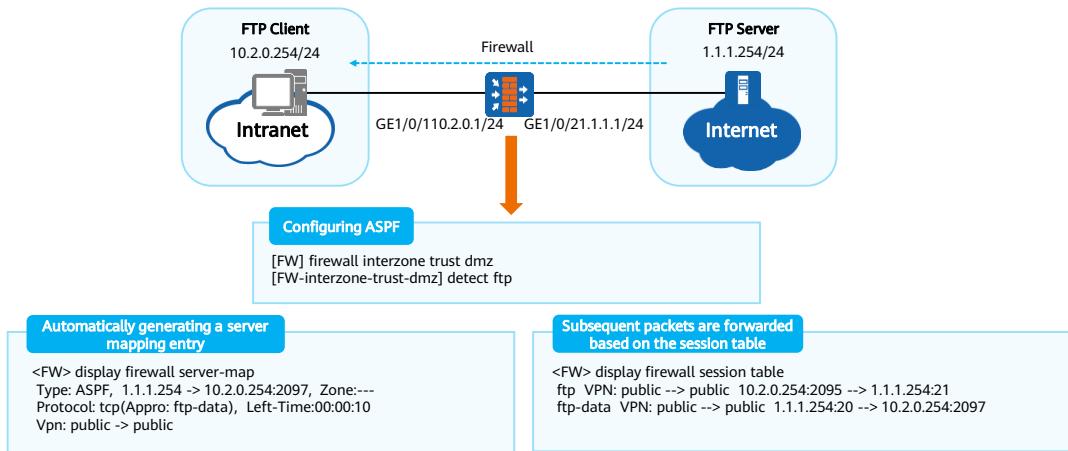
- In FTP active mode, the client uses the random port xxxx to send a connection setup request to port 21 on the server to set up a control connection, and then uses the **PORT** command to negotiate the port number that is used in the data connection. The negotiated port number is yyyy. Then, the server initiates a connection request to port yyyy of the client to establish a data channel. Data is transmitted after the data channel is successfully established.
- During configuration of the security policy, if the security policy that allows the client to access port 21 of the server is configured, the control connection can be established successfully. However, when the packet from the server to the client's port yyyy reaches the firewall, the packet represents a new connection instead of the subsequent packet of the previous connection. To ensure that the packet can reach the FTP client, a security policy needs to be configured on the firewall. If there is no security policy configured in the direction from the server to the client, the packet cannot pass through the firewall. The result is that users can access the server, but cannot request data.
- The application layer information in the **PORT** command contains the client's IP address and a random port open to the server. By analyzing the application layer information in the **PORT** command, the firewall can predict the behavior of subsequent packets. Then it creates the server mapping table based on the IP address and port in the application layer information. After the packet that initiates a data connection from the server to the client reaches the firewall, it matches the server mapping entry and is no longer controlled by the security policy.

Relationship Between the Server Mapping Table and the Session Table

- The relationship between the server mapping table and the session table is as follows:
 - The server mapping table records key information at the application layer. Packets that match this table are not controlled by security policies.
 - The session table represents the connection status of the communication parties.
 - The server mapping table is not the current connection information, but the prediction of incoming packets based on the analysis of an existing connection.
- The procedure for the firewall to receive packets is shown in the figure:
 - When receiving a packet, the firewall checks whether the packet matches the session table.
 - If not, it checks whether the packet matches the server mapping table.
 - If the packet matches the server mapping table, it is not controlled by security policies.
 - Finally, the firewall creates a session table for the data that matches the server mapping table.



Example for Configuring the Server Mapping Table

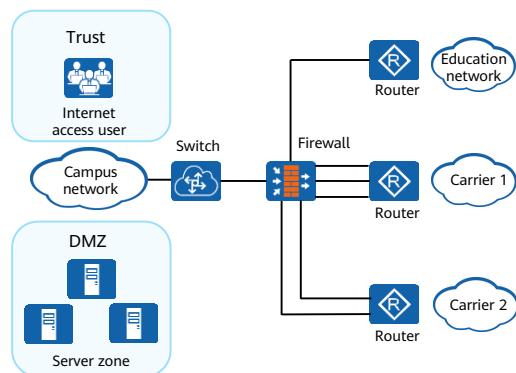


Contents

1. Firewall Basic Principles
2. Application Scenarios of Firewalls in Cyber Security Solutions

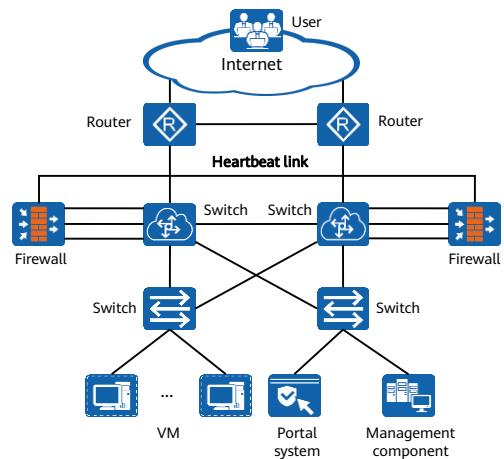
Application of Firewalls in the Campus Egress Security Solution

- The campus network faces different security threats from the network layer to the application layer.
 - Network border protection
 - Intranet security protection
- As shown in the figure, the firewall is deployed as a security gateway at the campus network egress.
 - It provides security isolation and protection for internal and external network access, for example, traditional IP address-based security policy formulation and network access control.
 - It also provides user-based access control and behavior tracing.



Application of Firewalls in Cloud Computing Networks

- The rapid development of cloud computing helps enterprises easily access cloud computing networks and obtain resources such as servers, storage, as well as applications. This reduces investment costs for building IT infrastructure, and greatly accelerates the informatization process.
- As shown in the figure, firewalls can be deployed on the cloud computing network to:
 - Isolate services when users on different external networks access VMs.
 - Enable enterprise users to access internal VMs and portals through public network addresses.
 - Improve the reliability of services. Services will not be interrupted due to one faulty device.



Quiz

1. (True or False) When the stateful detection mechanism is disabled, the firewall creates sessions for ICMP Reply packets. ()
 - A. True
 - B. False

1. A

Summary

- This course introduces the basic concepts and development history of firewalls, as well as security zones, security policies, and corresponding control principles.
- By taking this course, along with exercises in actual environments, you will be able to independently configure security policies on Huawei firewalls and grasp the deployment scenarios of firewalls in cyber security solutions.

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 and Abbreviation	Full Name
ASPF	Application Specific Packet Filter
DPI	Deep Packet Inspection
SNMP	Simple Network Management 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
portfolio, new technology, 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 NAT Technologies



Foreword

- As the Internet develops and network applications grow, limited public IPv4 addresses have become the bottleneck of network development. Although IPv6 can resolve the problem of insufficient IPv4 address space, most network devices and applications use IPv4 addresses. Therefore, the Network Address Translation (NAT) technology emerges before IPv6 is widely used.
- NAT allows public IPv4 addresses to be reused, offering a short-term solution to alleviate IPv4 address exhaustion.
- This course describes the technical background, working principles, and application scenarios of different types of NAT.

Objectives

- On completion of this course, you will be able to:
 - Describe the technical background of NAT.
 - Know the classification and working principles of NAT.
 - Know the application scenarios of different types of NAT.

Contents

- 1. Overview of NAT**
2. Source NAT
3. Destination NAT
4. Bidirectional NAT
5. NAT ALG and NAT Server

Background of NAT

- An increasing number of network devices require more IPv4 addresses, causing exhaustion of available public IPv4 addresses. An expedient solution to this problem is to assign reusable private address segments to enterprises or home users.
- The differences between public and private addresses are as follows:
 - Public IP addresses: are managed and assigned by dedicated organizations and can be used for direct communication on the Internet.
 - Private IP addresses: can be used by organizations or individuals randomly on internal networks, but cannot be used for direct communication on the Internet.
- The following Classes A, B, and C addresses are reserved as private IP addresses:
 - Class A: 10.0.0.0 to 10.255.255.255
 - Class B: 172.16.0.0 to 172.31.255.255
 - Class C: 192.168.0.0 to 192.168.255.255

Firewall NAT Implementation: NAT Policy

- The NAT function of firewalls can be implemented by configuring a NAT policy.
- A NAT policy consists of post-NAT addresses (addresses in an address pool or outbound interface addresses), matching conditions, and actions.
 - Address pools are classified into source address pools and destination address pools. You can use an address pool of a specific type or outbound interface address as the post-NAT address based on the NAT translation mode you select.
 - Matching conditions include the source address, destination address, source security zone, destination security zone, outbound interface, service, and time range. You can configure different matching conditions to perform NAT translation on the traffic matching these conditions.
 - Actions include source address translation and destination address translation. You can configure whether to perform NAT translation on the traffic matching certain conditions regardless of the chosen action.

- If multiple NAT policies are created, the firewall matches traffic against these policies in top-down order, and stops matching once a match is found.
- Bidirectional NAT policies and destination NAT policies are placed before source NAT policies. Bidirectional NAT policies and destination NAT policies are arranged in configuration order, and source NAT policies are also arranged in configuration order. A newly added policy or a policy with the NAT action modified is placed at the end of the corresponding NAT policy list.
- You can adjust the matching order of NAT policies as required, but source NAT policies cannot be placed before bidirectional or destination NAT policies.

Classification, Advantages, and Disadvantages of NAT

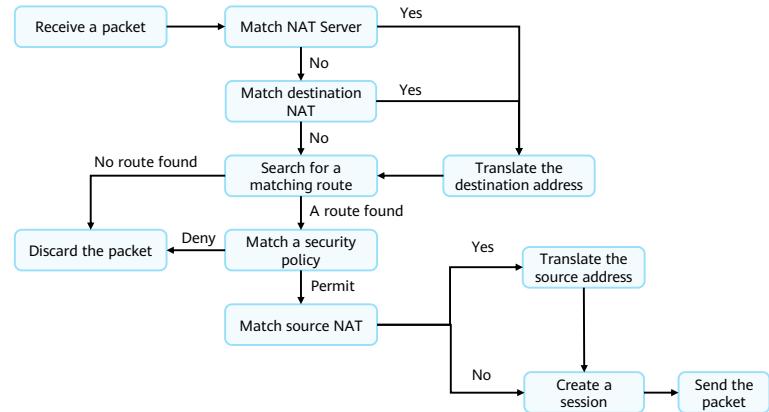
- NAT is classified into three categories based on application scenarios.
 - Source NAT: allows users to access the Internet using private IP addresses.
 - Destination NAT: allows users to access private network servers using public IP addresses.
 - Bidirectional NAT: allows communication parties to access each other using NATed addresses instead of real addresses as the destination addresses.
- Advantages of NAT:
 - Saves IP address resources by reusing addresses.
 - Prevents attacks from external networks and provides privacy protection for internal users, greatly improving network security.
- Disadvantages of NAT:
 - Increases the network monitoring difficulty.
 - Restricts some applications.

- In addition to saving IP address resources by reusing addresses, NAT continues to evolve and provides other advantages.
- Advantages of NAT:
 - Multiple hosts on a LAN can use a few valid addresses to access external resources, and internal services such as FTP and Telnet can be provided to external networks, resolving the problem of IP address shortage.
 - Internal and external network users are unaware of the IP address translation process.
 - Privacy protection is provided for internal network users. External network users cannot directly obtain the IP addresses and service information of internal network users.
 - Multiple internal servers of the same type can be configured for load balancing, reducing the pressure of a single server in case of heavy traffic and also ensuring security.

- Disadvantages of NAT:
 - The header of a packet containing an IP address cannot be encrypted as IP address translation is performed. For a packet of an application protocol, if an address or port number in the packet header needs to be translated, the packet cannot be encrypted. For example, an FTP connection cannot be encrypted; otherwise, the port number specified in the FTP PORT command cannot be translated.
 - NAT makes network monitoring more difficult. For example, it is hard to trace a hacker who attacks a server on the public network from a private network. This is because the host used by the hacker cannot be identified because the IP address of the attack packet has been translated through NAT.

NAT Processing Flow

- Different NAT types use different policies.



- The NAT processing flow is as follows:

- Step 1: When receiving a packet, the firewall searches for a matching server mapping entry generated by NAT Server. If a match is found, the firewall translates the destination address of the packet accordingly and proceeds to step 3. If no match is found, the device proceeds to step 2.
- Step 2: The firewall checks whether the packet meets the conditions of a destination NAT policy. If so, the firewall translates the destination address of the packet, and then proceeds to step 3. If the packet does not match any destination NAT policy, the firewall proceeds to step 3.
- Step 3: The firewall searches for a matching route (including routes available in PBR scenarios) for the packet. If a match is found, the firewall proceeds to step 4. If no match is found, the firewall discards the packet.
- Step 4: The firewall searches for a security policy matching the packet, and one of the following situations occurs: If the security policy permits the packet and the packet does not match any earlier destination or bidirectional NAT policy, the firewall proceeds to step 5. If the security policy permits the packet and the packet matches an earlier bidirectional NAT policy, the firewall translates the source address of the packet, creates a session, and proceeds to step 6. If the security policy permits the packet and the packet matches an earlier destination NAT policy, the firewall creates a session for the packet and proceeds to step 6. If the security policy denies the packet, the firewall discards the packet.

- Step 5: The firewall searches for a source NAT policy matching the packet. If a match is found, the firewall translates the source address of the packet into a public address, and creates a session for the packet. If no match is found, the firewall creates a session for the packet without address translation and proceeds to step 6.
- Step 6: The firewall sends the packet out according to the matching route.

Contents

1. Overview of NAT

2. Source NAT

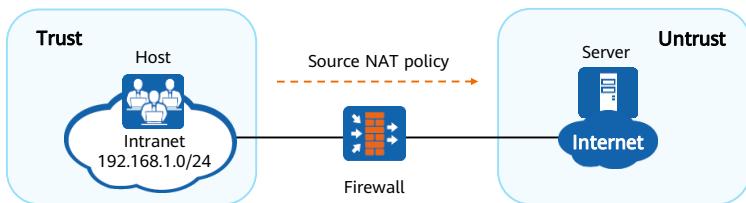
3. Destination NAT

4. Bidirectional NAT

5. NAT Server

Overview of Source NAT

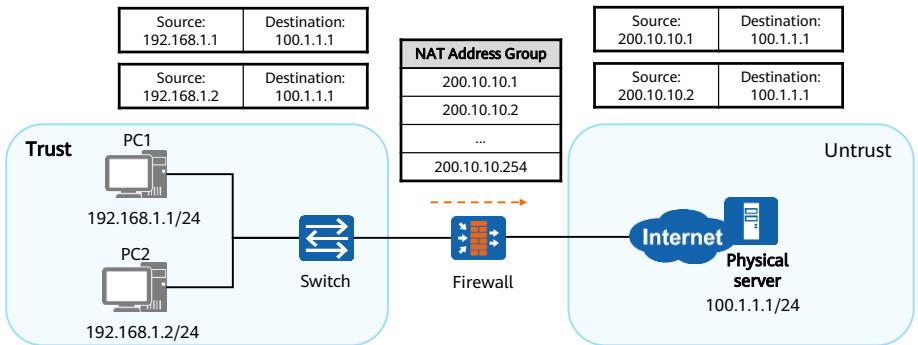
- Background: Enterprise users and home users reside on private networks and use private addresses. Carriers maintain public networks and use public addresses. Private addresses cannot be used for communication on public networks.
- Solution: Source NAT can be used to enable multiple users to share a few public addresses for Internet access.
 - Source NAT translates only source addresses of packets.
 - Source NAT is categorized into NAT No-PAT, NAPT, Easy IP, and Triplet NAT.



- On campus and enterprise networks, it is usually expected to allow multiple users to access the Internet using a few public IP addresses. Source NAT can be used to meet this requirement. Source NAT translates only source addresses of packets. A source NAT policy is configured to translate source addresses in IPv4 packet headers, so that intranet users can access the Internet using public IP addresses.
- As shown in the figure, the firewall is deployed at the network border. A source NAT policy is deployed on the firewall to translate the source addresses of packets sent from intranet users to the Internet into public addresses. In this way, these users can successfully access the Internet.

NAT No-PAT

- NAT no-port address translation (No-PAT) translates a private source IP address into a unique public address, but does not translate port numbers. NAT No-PAT cannot improve the utilization of public addresses.
- NAT No-PAT applies to the scenario where there are a small number of Internet access users and the number of public IP addresses is the same as the number of concurrent Internet access users.



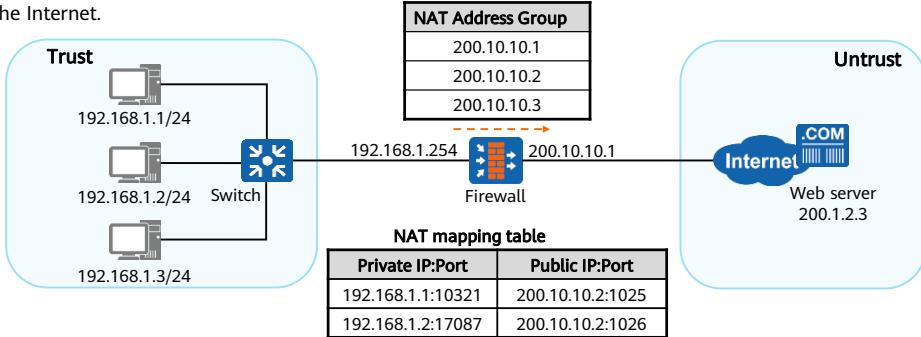
13 Huawei Confidential



- When PC1 and PC2 on the intranet communicate with the destination server on the Internet, the firewall assigns a unique available public address from the configured address pool to each PC, and creates a mapping between the private and public addresses. When receiving a response packet, the firewall performs address translation again based on the mapping and forwards the packet to the corresponding PC. If a connection is not required, the firewall deletes the corresponding address mapping, and the public IP address is available again in the address pool.
- After IP addresses in the dynamic NAT address pool are used up, other hosts cannot use public IP addresses to access the Internet until the occupied public IP addresses are released.
- When the No-PAT parameter is specified in the NAT configuration, the device performs one-to-one translation between private and public IP addresses, but does not perform port translation. In this case, all port numbers of a private IP address remain unchanged during address translation. In this way, Internet users can initiate connections to any port of the intranet user. Therefore, after NAT No-PAT is configured, the device creates server mapping entries for data flows to store the mappings between private and public IP addresses. The device translates IP addresses of packets according to the mappings before forwarding them.

NAPT

- Network Address and Port Translation (NAPT) translates both IP addresses and port numbers to allow multiple private addresses to be translated into the same public address. NAPT can effectively improve the utilization of public addresses.
- NAPT applies to scenarios where a limited number of public addresses exist but many private users require access to the Internet.



- NAPT translates both IP addresses and port numbers, allowing multiple private addresses (different private addresses, different source port numbers) to be translated into the same public address (same public address, different source port numbers).

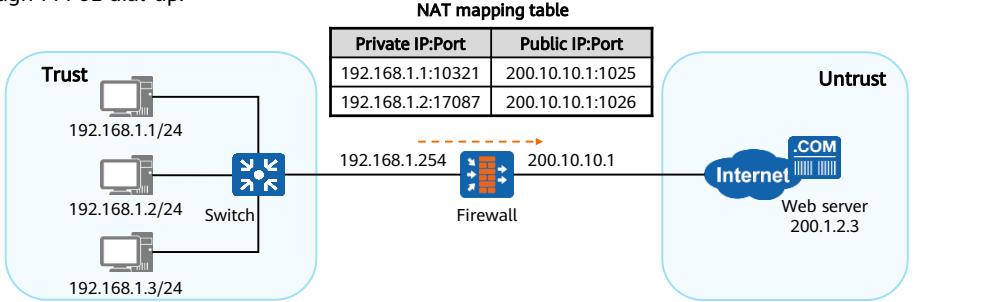
Differences Between NAT No-PAT and NAPT

- NAT No-PAT: address pool mode without port translation
- NAPT: address pool mode with port translation

Source NAT Mode	Function	Scenario	Public Address Utilization
NAT No-PAT	Translates only addresses.	There are a few intranet users who need to access the Internet, and the number of available public IP addresses is almost the same as the maximum number of concurrent Internet access users.	1:1
NAPT	Translates both addresses and port numbers.	There are only a few public IP addresses but many intranet users requiring access to the Internet.	1:N

Easy IP

- Similar to NAPT, Easy IP translates both IP addresses and transport-layer port numbers. The difference lies in that Easy IP uses the public IP address of the WAN interface, instead of an address pool, as the post-NAT address.
- Easy IP applies to scenarios where no fixed public IP address is available, for example, Internet access through PPPoE dial-up.



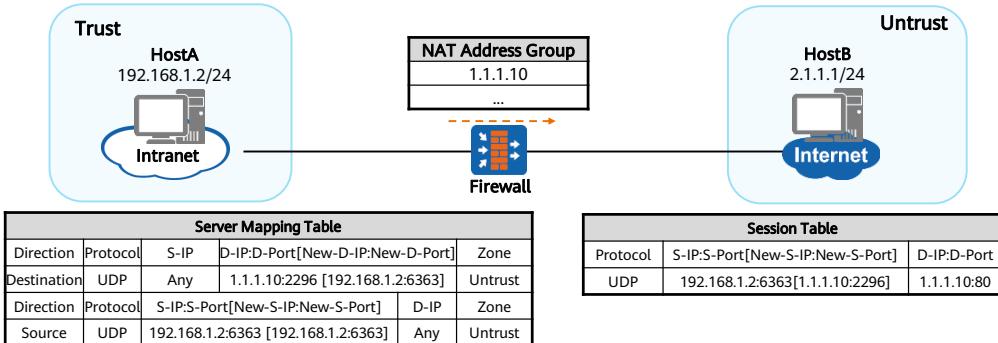
16 Huawei Confidential



- Point-to-Point Protocol over Ethernet (PPPoE) is widely used in a series of applications such as cell networking.

Triplet NAT

- Triplet NAT translates both addresses and port numbers of packets, allowing multiple private addresses to be translated into the same public address.
- Triplet NAT also enables Internet users to proactively access intranet users for file sharing, audio communication, and video transmission.



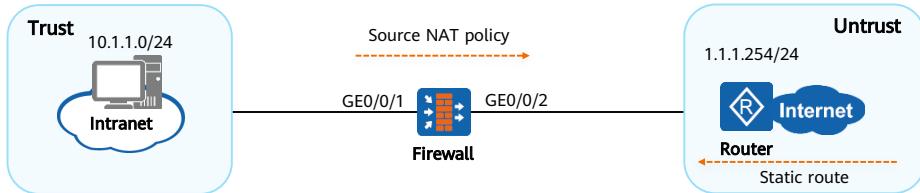
17 Huawei Confidential



- When HostA on the intranet accesses HostB on the Internet, the Triplet NAT process on the firewall is as follows:
 1. When receiving a packet from HostA, the firewall discovers that the packet needs to travel from the Trust zone to the Untrust zone based on the destination IP address, so it searches for a matching inter-zone security policy. If the inter-zone security policy allows the packet to pass through, the firewall searches for a matching inter-zone NAT policy and discovers that the packet requires NAT translation.
 2. The firewall replaces the source IP address of the packet with a public IP address (1.1.1.10 in this example) from the NAT address pool and the source port number with 2296, creates a session entry and server mapping entry accordingly, and sends the packet to HostB.
 3. When receiving a response packet from HostB, the firewall searches the session table for the entry created in step 2, replaces the destination IP address of the packet with 192.168.1.2 (private IP address of HostA) and the port number with 6363 accordingly, and then forwards the packet to HostA.
- The server mapping table generated by the firewall stores the mappings between the private and public IP addresses of hosts.
 - Forward server mapping entries ensure that the post-NAT addresses and port numbers of intranet PCs remain unchanged.
 - Reverse server mapping entries allow extranet devices to proactively access intranet PCs.

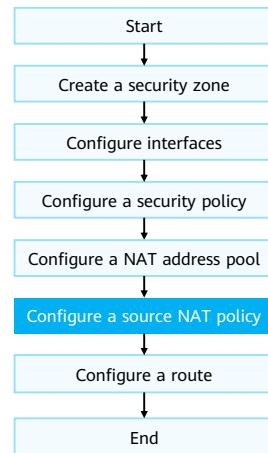
Example of Configuring a Source NAT Policy (1)

- Requirements:
 - An enterprise has deployed a firewall as a security gateway at the intranet border. A source NAT policy needs to be configured on the firewall so that intranet users on the 10.1.1.0/24 network segment can access the Internet.
 - In addition to the public IP address of the WAN interface on the firewall, the enterprise has obtained six public IP addresses (1.1.1.10 to 1.1.1.15) from a carrier for address translation. As shown in the figure, the router is the access gateway provided by the carrier.



Example of Configuring a Source NAT Policy (2)

- Configuration roadmap:
 - Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
 - Configure a security policy to allow intranet users on a specified network segment to access the Internet.
 - Configure a NAT address pool and enable port translation so that public addresses can be reused.
 - Configure a source NAT policy to enable source address translation for intranet users on a specified network segment to access the Internet.
 - Configure a default route on the firewall, enabling it to forward traffic sent from intranet users to the carrier's router.



Example of Configuring a Source NAT Policy (3)

- Add firewall interfaces to security zones.

```
[FW] firewall zone trust  
[FW-zone-trust] add interface GigabitEthernet 0/0/1  
[FW-zone-trust] quit  
[FW] firewall zone untrust  
[FW-zone-untrust] add interface GigabitEthernet 0/0/2  
[FW-zone-untrust] quit
```

- Configure a security policy to allow intranet users on a specified network segment to access the Internet.

```
[FW] security-policy  
[FW-policy-security] rule name policy1  
[FW-policy-security-rule-policy1] source-zone trust  
[FW-policy-security-rule-policy1] destination-zone untrust  
[FW-policy-security-rule-policy1] source-address 10.1.1.0 24  
[FW-policy-security-rule-policy1] action permit  
[FW-policy-security-rule-policy1] quit
```

Example of Configuring a Source NAT Policy (4)

- Configure a NAT address pool and enable port translation so that public addresses can be reused.

```
[FW] nat address-group group1  
[FW-address-group-addressgroup1] mode pat  
[FW-address-group-addressgroup1] section 0 1.1.1.10 1.1.1.15  
[FW-address-group-addressgroup1] route enable
```

- Configure a source NAT policy to enable source address translation for intranet users on a specified network segment to access the Internet.

```
[FW] nat-policy  
[FW-policy-nat] rule name policy1  
[FW-policy-nat-rule-policy1] source-zone trust  
[FW-policy-nat-rule-policy1] destination-zone untrust  
[FW-policy-nat-rule-policy1] source-address 10.1.1.0 24  
[FW-policy-nat-rule-policy1] action source-nat address-group group1
```

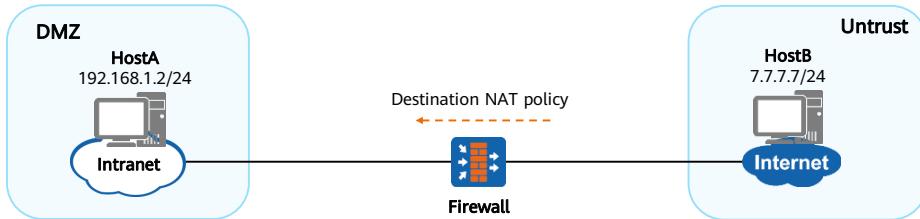
- Configure a default route on the firewall, enabling it to forward traffic sent from intranet users to the carrier's router.
- Configure the default gateway address on each intranet host, enabling them to send traffic destined for the Internet to the firewall.

Contents

1. Overview of NAT
2. Source NAT
- 3. Destination NAT**
4. Bidirectional NAT
5. NAT ALG and NAT Server

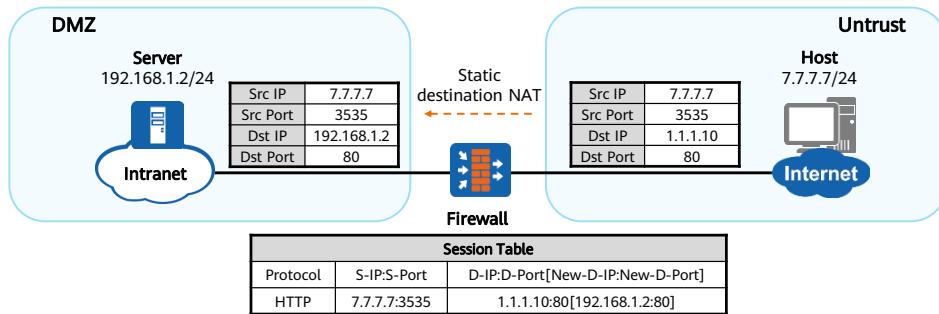
Overview of Destination NAT

- Destination NAT translates both the destination addresses and port numbers of packets. It translates public IP addresses into private IP addresses so that users on the Internet can access intranet servers using public IP addresses.
- When an Internet user accesses a server on the intranet, the destination NAT process on the firewall is as follows:
 - When receiving a packet from the host, the firewall translates the destination public address of the packet into a private address.
 - When receiving a return packet from the server on the intranet, the firewall translates the source private address back into the public address of the host.
- Based on whether post-NAT destination addresses are fixed, destination NAT is categorized into static or dynamic destination NAT.



Static Destination NAT

- Static destination NAT translates the destination IP addresses of packets, and fixed mappings exist between the pre-NAT and post-NAT addresses.
- For security reasons, Internet users are sometimes not granted proactive access to intranets. In certain scenarios, however, it is expected that access will be permitted from the Internet. For example, an enterprise intends to provide intranet resources to employees on a business trip and customers on external networks.



24 Huawei Confidential

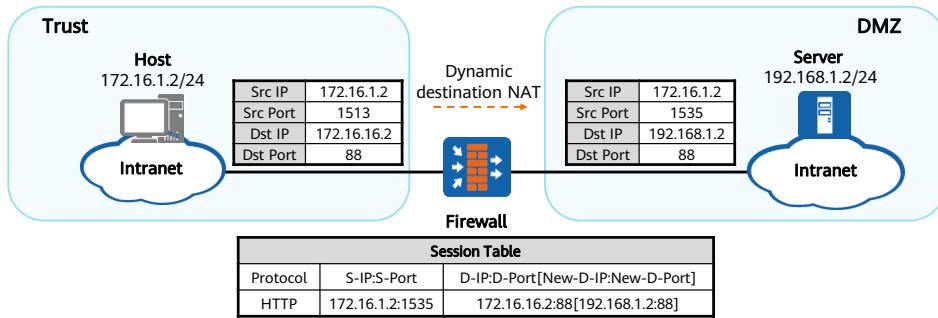


When a host on the Internet accesses a server on the intranet, the destination NAT process on the firewall is as follows:

1. When receiving a packet destined for 1.1.1.10 (public IP address used by the intranet server to provide services) from the host on the Internet, the firewall discovers that the packet matches a destination NAT policy.
2. The firewall translates the destination IP address of the packet into the private IP address of the server. It also replaces the destination port number with a new one or ensures the destination port number remains unchanged, depending on the configuration. In scenarios where one-to-one mappings exist between public and private IP addresses, the firewall selects private IP addresses from the NAT address pool in sequence as post-NAT destination addresses, and translates the destination addresses of packets according to these mappings.
3. If the packet is permitted according to a matching security policy, the firewall creates a session entry and forwards the packet to the server on the intranet.
4. When receiving a return packet from the server, the firewall searches the session table for the entry created in step 3, translates the source IP address (192.168.1.2, IP address of the server) into 1.1.1.10 accordingly, and then forwards the packet to the host.
5. When receiving subsequent packets sent from the host to the server, the firewall directly translates addresses according to the session entry.

Dynamic Destination NAT

- Dynamic destination NAT dynamically translates the destination IP addresses of packets, and fixed mappings do not exist between the pre-NAT and post-NAT addresses.
- Although static destination NAT satisfies the needs of most destination address translation scenarios, dynamic destination NAT can be used in scenarios that require the post-NAT address not be fixed. For example, mobile devices access wireless networks through destination address translation.



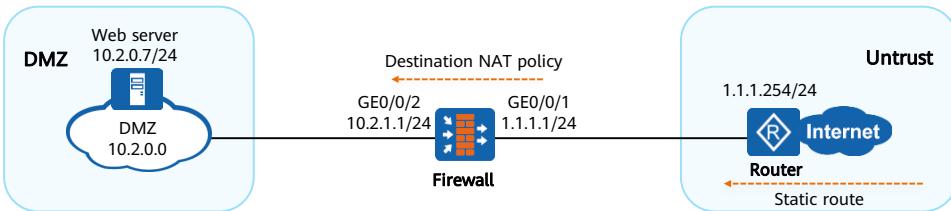
25 Huawei Confidential



- When a host on the intranet accesses a server on the Internet, the destination NAT process on the firewall is as follows:
 1. When receiving a packet from the host, the firewall discovers that the packet matches a destination NAT policy, and translates the destination address of the packet into an address randomly selected from the address pool. In this example, the firewall translates the destination IP address 172.16.16.2 into 192.168.1.2.
 2. If the packet is permitted according to a matching inter-zone security policy, the firewall creates a session entry and forwards the packet to the server.
 3. When receiving a return packet from the server, the firewall searches the session table for the entry created in step 2, translates the source address of the packet into 172.16.16.2 accordingly, and then forwards the packet to the host.

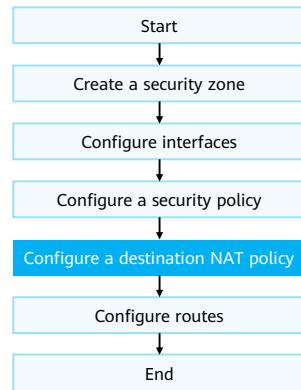
Example of Configuring a Destination NAT Policy (1)

- Requirements:
 - An enterprise has deployed a firewall as a security gateway at the intranet border. Destination NAT needs to be configured on the firewall so that the web server on the intranet can provide services to Internet users.
 - In addition to the public IP address of the WAN interface on the firewall, the enterprise has obtained another public IP address (1.1.10.10) from the carrier, which is used by the intranet server to provide services to Internet users. As shown in the figure, the router is the access gateway provided by the carrier.



Example of Configuring a Destination NAT Policy (2)

- Configuration roadmap:
 - Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
 - Configure a security policy so that Internet users can access the intranet server.
 - Configure the destination NAT function so that the firewall can forward traffic to the intranet server when Internet users access the intranet server.
 - Configure default routes on the firewall and router so that traffic can be transmitted between the intranet server and the carrier's router.



Example of Configuring a Destination NAT Policy (3)

- Add firewall interfaces to security zones.

```
[FW] firewall zone DMZ  
[FW-zone-dmz] add interface GigabitEthernet 0/0/2  
[FW-zone-dmz] quit  
[FW] firewall zone untrust  
[FW-zone-untrust] add interface GigabitEthernet 0/0/1  
[FW-zone-untrust] quit
```

- Configure a security policy so that Internet users can access the intranet server.

```
[FW] security-policy  
[FW-policy-security] rule name policy1  
[FW-policy-security-rule-policy1] source-zone untrust  
[FW-policy-security-rule-policy1] destination-zone dmz  
[FW-policy-security-rule-policy1] destination-address 10.2.0.0 24  
[FW-policy-security-rule-policy1] action permit  
[FW-policy-security-rule-policy1] quit
```

Example of Configuring a Destination NAT Policy (4)

- Configure a destination NAT address pool.

```
[FW1]destination-nat address-group group1  
[FW1-dnat-address-group-group1]section 10.2.0.7 10.2.0.8  
[FW-address-group-group1] quit
```

- Configure a destination NAT policy so that the firewall can forward traffic to the intranet server when Internet users access the intranet server.

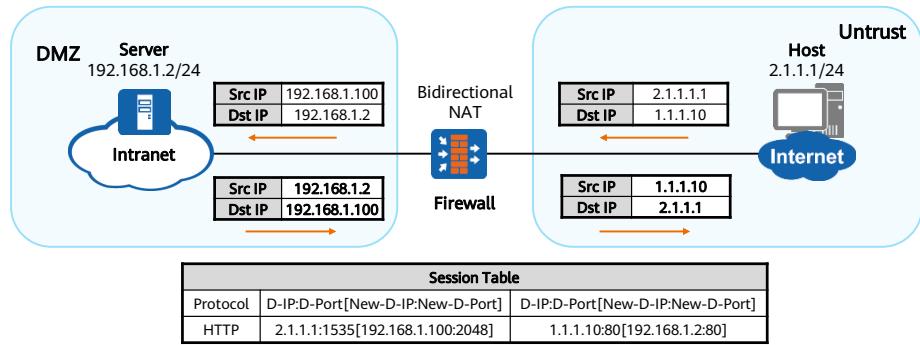
```
[FW] nat-policy  
[FW-policy-nat] rule name policy1  
[FW-policy-nat-rule-policy1] source-zone untrust  
[FW-policy-nat-rule-policy1] destination-address 1.1.10.10 1.1.10.11  
[FW-policy-nat-rule-policy1] service http  
[FW-policy-nat-rule-policy1] action destination-nat static address-to-address address-group group1  
[FW-policy-nat-rule-policy1] quit
```

Contents

1. Overview of NAT
2. Source NAT
3. Destination NAT
- 4. Bidirectional NAT**
5. NAT ALG and NAT Server

Bidirectional NAT

- Bidirectional NAT translates both source and destination IP addresses of packets. It is a combination of source NAT and destination NAT.
- Bidirectional NAT applies to the same flow. When receiving a packet, the firewall translates both its source and destination addresses.



31 Huawei Confidential



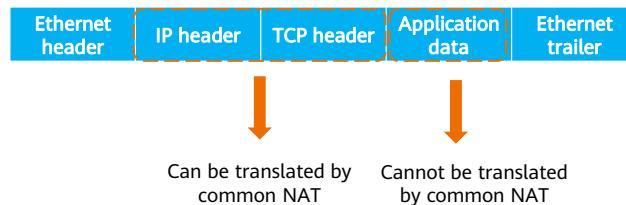
- Bidirectional NAT applies to the following scenarios:
 - Internet users access intranet servers.
 - Intranet users access intranet servers.
- Bidirectional NAT can be used when an Internet user accesses an intranet server. It translates both the source and destination addresses of packets, removing the need to set the gateway address on the intranet server, thereby simplifying configuration.
- As shown in the figure, the firewall performs the following when a host on the Internet accesses an intranet server:
 1. When receiving a packet from the host, the firewall discovers that the packet matches a bidirectional NAT policy.
 2. The firewall translates the destination IP address of the packet into the private IP address of the server and replaces the destination port number with a new one.
 3. If the packet is permitted according to a matching security policy, the firewall translates the source IP address of the packet into a private IP address from the source NAT address pool and replaces the source port number with a new one. The firewall then creates a session entry and forwards the packet to the intranet server.
 4. When receiving a return packet from the server, the firewall searches the session table for the previously created entry, translates the source and destination addresses as well as the source and destination ports according to the entry, and then forwards the packet to the host on the Internet.

Contents

1. Overview of NAT
2. Source NAT
3. Destination NAT
4. Bidirectional NAT
- 5. NAT ALG and NAT Server**

Overview of NAT ALG

- ASPF can match data of multi-channel application protocols and create server mapping entries based on IP addresses and port numbers in application-layer data. The NAT application level gateway (ALG) is a translation proxy of some application protocols and can translate the IP addresses and port numbers carried in application-layer data. The differences between ASPF and NAT ALG are as follows:
 - ASPF is mainly used to analyze the packets of application-layer protocols and apply packet filtering rules to these packets.
 - NAT ALG is mainly used to apply NAT rules to application-layer packets.
 - Generally, ASPF is used together with NAT ALG, and you can enable both the functions by running only one command.

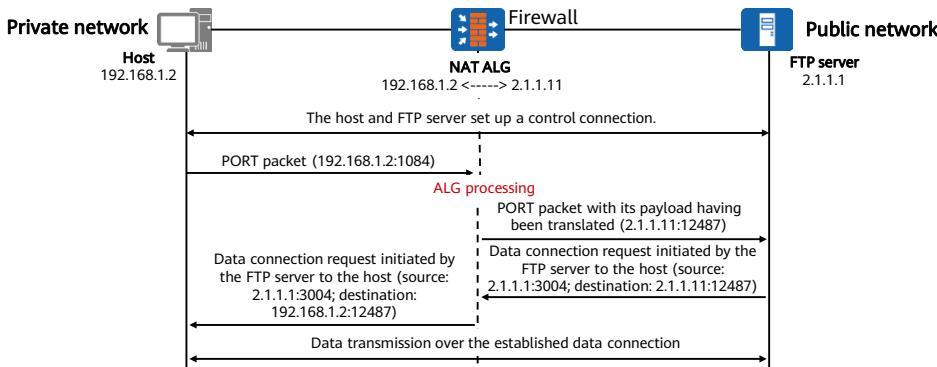


- In an Ethernet data frame, the IP header contains a 32-bit source address and a 32-bit destination address, and the TCP header contains a 16-bit source port number and a 16-bit destination port number.
- Many protocols use the data payloads of IP packets to negotiate new ports and IP addresses. After the negotiations are complete, communication parties establish new connections for transmitting subsequent packets. As the negotiated ports and IP addresses are random, an administrator cannot configure NAT rules in advance. As a result, these protocols may encounter errors during NAT.
- Common NAT can translate the IP addresses and port numbers in UDP and TCP packet headers, but not fields in application-layer data payloads. In many application-layer protocols, such as multimedia protocols (H.323, SIP, etc.), FTP, and STelnet, the TCP/UDP payload carries address or port information that cannot be translated through common NAT. To address this problem, NAT ALG is introduced to parse the application-layer packet information of multi-channel protocols and translate IP addresses and port numbers or specific fields in payloads to ensure proper communication at the application layer.
- For example, the FTP application requires both a data connection and a control connection, and the establishment of the data connection is dynamically determined by the payload field information in the control connection. Therefore, ALG needs to translate the payload field information to ensure proper establishment of the data connection.

- The ASPF function is proposed to implement the forwarding policy of application-layer protocols. ASPF analyzes the packets of application-layer protocols and applies corresponding packet filtering rules, whereas NAT ALG applies corresponding NAT rules to these packets. Generally, ASPF is used together with NAT ALG, and you can enable both the functions by running only one command.

Implementation of NAT ALG

- A host on a private network needs to access the FTP server on the public network. To meet this requirement, the mapping between the private address 192.168.1.2 and the public address 2.1.1.11 is configured on the NAT device. If ALG does not process the packet payload, the server cannot perform addressing based on the private address in the PORT packet received from the host on the private network. As a result, a data connection cannot be established.



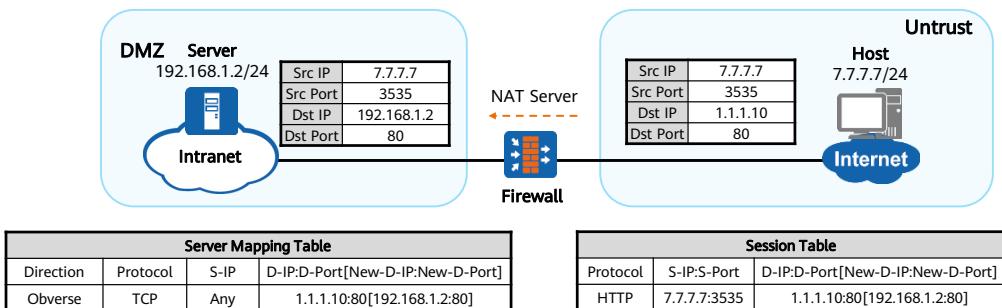
35 Huawei Confidential



- The communication process consists of four stages:
 - The host on the private network and the FTP server on the public network establish a control connection through a TCP three-way handshake.
 - The host sends a PORT packet carrying a destination IP address and port number to the FTP server, requesting the FTP server to use this IP address and port number to establish a data connection.
 - The ALG-enabled NAT device translates the private address and port number carried in the packet payload into the corresponding public address and port number. That is, the device translates the private address 192.168.1.2 and port number 1084 in the payload of the received PORT packet into the public address 2.1.1.11 and port number 12487.
 - The FTP server parses the received PORT packet and initiates a data connection to the host, with the destination address of 2.1.1.11 and the destination port number of 12487. (Generally, the source port number of a data connection request initiated by a server is 20. However, this port number is sometimes set to a random value greater than 1024, as the FTP protocol does not have strict requirements on this port. In this example, the FTP server sets the source port number to 3004.) Since the destination address is a public address, the data connection can be established and the host can then access the FTP server.

NAT Server

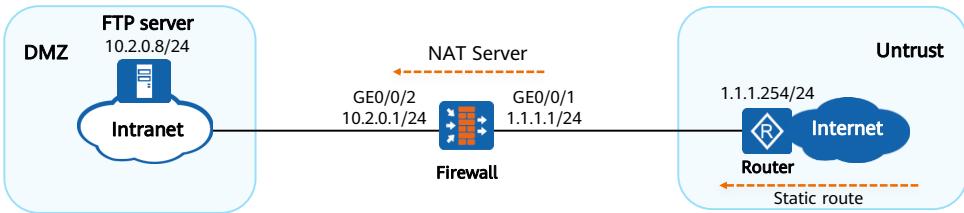
- NAT Server is a static destination address translation technology that maps a public IP address to the private IP address of an intranet server, allowing Internet users to access the intranet server using public IP addresses.



- NAT Server is a static destination address translation technology that maps public IP addresses of packets to private IP addresses.
- When Internet users initiate access requests to an intranet server, the IP addresses and port numbers of the users are unknown, but the IP address and port number of the intranet server are known. Therefore, after NAT Server is configured on the device to determine the mappings between public and private IP addresses, the device generates server mapping entries to store the mappings. The device performs address translation for packets according to these mappings before forwarding the packets.
- As shown in the figure, the firewall performs the following when a host on the Internet accesses a server on the intranet:
 - When receiving the first packet destined for 1.1.1.10 from the host on the Internet, the firewall searches for a matching server mapping entry, and translates the destination IP address of the packet into 192.168.1.2 accordingly.
 - Based on the destination IP address, the firewall determines that the packet needs to travel between the Untrust zone and the DMZ. If the packet is permitted according to a matching inter-zone security policy, the firewall creates a session entry and forwards the packet to the server on the intranet.
 - When receiving a return packet from the server, the firewall searches the session table for the previously created entry, replaces the source address of the packet with 1.1.1.10, and forwards the packet to the host on the Internet.
 - Upon receipt of subsequent packets sent from the host to the server, the firewall performs NAT translation for the packets according to the session entry, instead of searching for a server mapping entry.
- You can configure NAT Server flexibly to meet various requirements of different scenarios. For example, you can configure whether port translation is performed or whether an intranet server is allowed to use a public IP address to access the Internet.

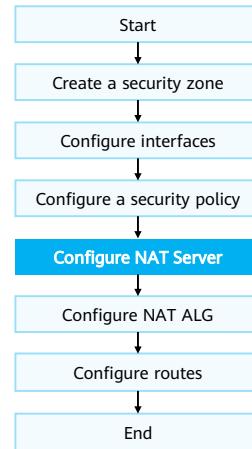
Example of Configuring NAT Server (1)

- Requirements:
 - An enterprise has deployed a firewall as a security gateway at the intranet border. NAT Server needs to be configured on the firewall so that the FTP server can provide services to Internet users.
 - In addition to the public IP address of the WAN interface on the firewall, the enterprise has obtained another public IP address (1.1.1.10) from the carrier, which is used by the intranet server to provide services to Internet users. As shown in the figure, the router is the access gateway provided by the carrier.



Example of Configuring NAT Server (2)

- Configuration roadmap:
 - Configure IP addresses for interfaces and add them to security zones, enabling network connectivity.
 - Configure a security policy so that Internet users can access the intranet server.
 - Configure NAT Server to implement address translation for the FTP server.
 - Enable the NAT ALG function for FTP to translate the IP address and port number carried in the application-layer data.
 - Configure default routes on the firewall and router so that traffic can be transmitted between the intranet server and the carrier's router.



Example of Configuring NAT Server (3)

- Add firewall interfaces to security zones.

```
[FW] firewall zone dmz  
[FW-zone-dmz] add interface GigabitEthernet 0/0/2  
[FW-zone-dmz] quit  
[FW] firewall zone untrust  
[FW-zone-untrust] add interface GigabitEthernet 0/0/1  
[FW-zone-untrust] quit
```

- Configure a security policy so that Internet users can access the intranet server.

```
[FW] security-policy  
[FW-policy-security] rule name policy1  
[FW-policy-security-rule-policy1] source-zone untrust  
[FW-policy-security-rule-policy1] destination-zone dmz  
[FW-policy-security-rule-policy1] destination-address 10.2.0.0 24  
[FW-policy-security-rule-policy1] action permit  
[FW-policy-security-rule-policy1] quit
```

Example of Configuring NAT Server (4)

- Configure NAT Server.

```
[FW] nat server policy_ftp protocol tcp global 1.1.1.10 ftp inside 10.2.0.8 ftp unr-route
```

- Enable the NAT ALG function for FTP.

```
[FW] firewall interzone dmz untrust  
[FW-interzone-dmz-untrust] detect ftp  
[FW-interzone-dmz-untrust] quit
```

- Configure a default route on the firewall to enable it to forward traffic from the intranet server to the carrier's router.

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

- If the public address configured in NAT Server and the WAN interface address are on different network segments, a blackhole route is required.
- If the public address configured in NAT Server and the WAN interface address are on the same network segment, a blackhole route is recommended.
- If the public address configured in NAT Server is the same as the WAN interface address, a routing loop will not occur. In this case, a blackhole route is not required.

Quiz

1. (Short-answer question) Which type of NAT allows an intranet server to be accessed by both intranet and Internet users?
2. (Short-answer question) What are the advantages of NAPT compared with NAT No-PAT?

1. After NAT Server is configured to bind a public IP address to the server's private IP address, Internet hosts can access the intranet server through the server's public IP address. In addition, users with private IP addresses can access the intranet server through the server's private IP address.
2. NAPT can translate multiple private IP addresses into one public IP address, improving utilization of public IP addresses.

Summary

- This course describes principles of different types of NAT, including source NAT, destination NAT, bidirectional NAT, NAT ALG, and NAT Server.
- Upon completion of this course, you will be able to independently configure NAT policies on Huawei devices and master various application scenarios of NAT technologies.

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
ALG	Application Layer Gateway
NAPT	Network Address and Port Translation
NAT	Network Address Translation
No-PAT	No-Port Address Translation

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
portfolio, new technology, 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 Hot Standby Technologies



Foreword

- With the rapid development of services such as mobile office, online shopping, instant messaging, Internet finance, and Internet education, networks carry more and more important services. Therefore, how to ensure uninterrupted service transmission on networks becomes an urgent problem to be resolved during network development.
- Hot standby technologies enable firewalls to be deployed at the network egress to ensure communication reliability between internal and external networks.

Objectives

- On completion of this course, you will be able to:
 - Understand the hot standby fundamentals.
 - Master the basic hot standby configurations.

Contents

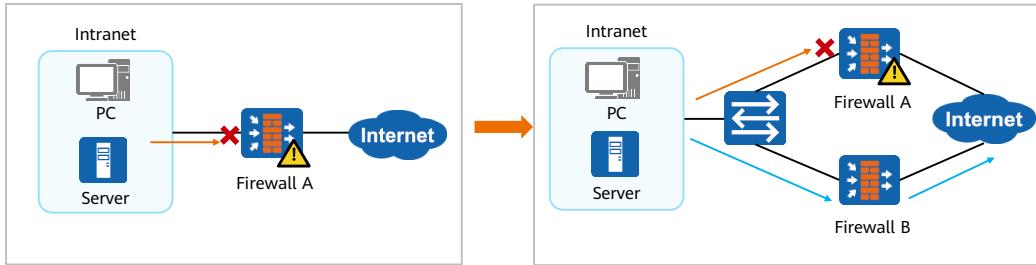
1. Hot Standby Fundamentals

- VRRP
 - VGMP Group
 - HRP
 - Firewall Hot Standby

2. Hot Standby Basic Networking and Configuration

Background of Hot Standby Technologies

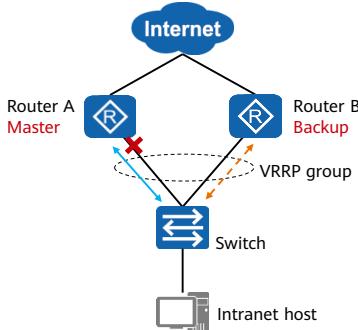
- As shown in the figure on the left, all packets exchanged between intranet and Internet users pass through firewall A. If firewall A is faulty, all hosts that use firewall A as the default gateway on the intranet cannot communicate with the Internet. As a result, communication reliability cannot be ensured.
- As a security device, a firewall is typically deployed between a network to be protected and an unprotected network, that is, on the network border. If only one firewall is deployed on the network border, the system may face the risk of network interruptions caused by a single point of failure no matter how highly reliable the firewall is. To prevent this problem, two firewalls can be deployed to implement hot standby.



- In hot standby networking, one firewall forwards traffic, and the other functions as a backup. In this case, VRRP is required to help the two firewalls work together. VRRP was initially used in the router reliability networking.

VRRP-based Router Redundancy Deployment

- Virtual Router Redundancy Protocol (VRRP) is a fault tolerance protocol that enables a backup router to automatically replace a faulty master router — the next hop (default gateway) of a host. In this way, the backup router can forward packets if a fault occurs, thereby ensuring the continuity and reliability of network communication. Routers in a VRRP group play two roles: master and backup.



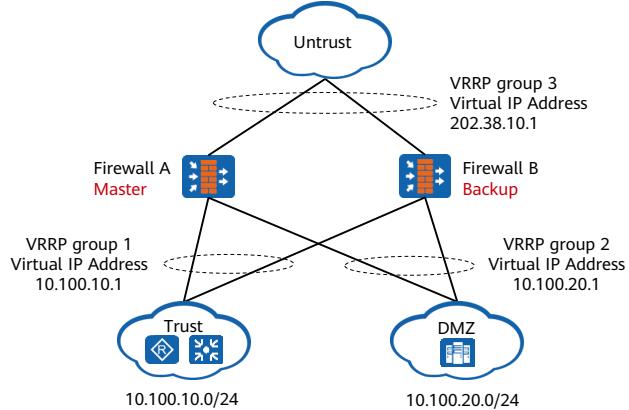
- When Router A is working properly:
 - Router A functions as the master device in the VRRP group and is responsible for forwarding data traffic.
- When Router A is faulty:
 - Router B detects VRRP heartbeat timeout and is elected as the new master device.
 - Router B sends a gratuitous ARP packet. After receiving the packet, the switch updates its MAC address table.
 - Router B responds to users' ARP requests and forwards traffic.

- VRRP group:** A group of routers in the same broadcast domain form a virtual router, namely, a VRRP group. It provides a virtual IP address as the gateway address of the intranet to implement gateway redundancy.
- When the master device is working properly, intranet hosts communicate with external networks through the master device. If the master device fails, the backup device becomes the new master device and takes over packet forwarding to ensure network continuity.
 - Master:** indicates the master state. A device whose VRRP group state is Master is called the master device. The master device is the owner of the virtual IP address and virtual MAC address of the VRRP group. When the master device receives an ARP request with the destination IP address being the virtual IP address, it responds to the ARP request. Among multiple routers in the same VRRP group, only one router is in active state, and only the master router can forward the packets with the virtual IP address as the next hop.
 - Backup:** indicates the backup state. A device whose VRRP group state is Backup is called a backup device. The backup device does not respond to ARP requests with the destination IP address being the virtual IP address. Among the routers in the same VRRP group, all the routers except the master router are backup routers. When the master device fails, a new master device is elected from the remaining backup devices.
- Master election rules:** The device with a higher priority (ranging from 0 to 255) is elected as the master device. If all devices have the same priority, the device with a larger interface IP address is elected as the master device. The priority of the master device then automatically changes to 255.
- The master router periodically sends VRRP Hello packets to the backup routers in multicast mode. The backup routers listen to the Hello packets to determine their status. VRRP Hello packets are multicast packets. Therefore, routers in the VRRP group must be connected through Layer 2 devices.

- When Router A is working properly, the traffic forwarding process is as follows:
 - Router A sends a gratuitous ARP packet that contains the VRRP virtual IP address and virtual MAC address.
 - The switch updates its MAC address table. That is, in the MAC address table, the virtual MAC address is mapped to the interface that receives the gratuitous ARP packet.
 - An intranet user sends an ARP request to query the gateway address, which is the virtual IP address.
 - Router A responds to the ARP request by sending the virtual MAC address to the user.
 - Traffic from the intranet user is sent to the gateway, Router A. The intranet user sends traffic to the virtual MAC address, and the switch forwards the traffic to Router A based on the MAC address table.
- When Router A is faulty, the traffic forwarding process is as follows:
 - If Router B does not receive VRRP packets from Router A within three packet sending intervals, Router B automatically becomes the new master.
 - Router B sends a gratuitous ARP packet that contains the VRRP virtual IP address and virtual MAC address.
 - The switch updates its MAC address table. That is, in the MAC address table, the virtual MAC address is mapped to the interface that receives the gratuitous ARP packet.
 - An intranet user sends an ARP request to query the gateway address, which is the virtual IP address.
 - Router B responds to the ARP request by sending the virtual MAC address to the user.
 - Traffic from the intranet user is sent to the gateway, Router B. The intranet user sends traffic to the virtual MAC address, and the switch forwards the traffic to Router B based on the MAC address table.

VRRP Application in Multi-Zone Firewall Networking

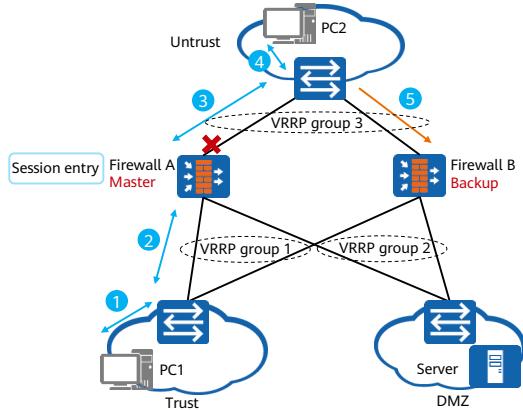
- When hot standby is required for firewalls in multiple zones, you need to configure multiple VRRP groups on each firewall.



- When hot standby is required for firewalls in multiple zones, you need to configure multiple VRRP groups on the firewall.
- As USG firewalls are stateful firewalls, they require the forward and return paths of packets to pass through the same firewall. To meet this requirement, the status of all VRRP groups on the same firewall must be the same. That is, the status of all VRRP groups on the master firewall must be master. This ensures that all packets pass through this firewall and the other firewall functions as the backup firewall.

Defects of VRRP in Firewall Applications

- Traditional VRRP cannot ensure the state information consistency and VRRP status consistency between the master and backup firewalls in multiple VRRP groups.



- When the VRRP status of Firewall A is the same as that of Firewall B:
 - When PC1 in the Trust zone accesses PC2 in the Untrust zone, the forward and return paths of the packets are the same, Firewall A passes the stateful inspection, and the communication is normal.
- When the VRRP status of Firewall A is different from that of Firewall B:
 - The upstream link of Firewall A is faulty, and Firewall B becomes the new master device of VRRP group 3.
 - When PC1 in the Trust zone accesses PC2 in the Untrust zone, the forward and return paths of the packets are inconsistent, Firewall B fails the stateful inspection, and packet loss occurs.

- Assume that the VRRP status of Firewall A is the same as that of Firewall B. That is, all interfaces on Firewall A are in master state, and all interfaces on Firewall B are in backup state.
 - In this case, PC1 in the Trust zone can access PC2 in the Untrust zone, and the packet forwarding path is (1)-(2)-(3)-(4). Firewall A forwards the access packets and dynamically generates a session entry. When the packets returned by PC2 reach Firewall A along the path (4)-(3), the packets can match the session entry and then reach PC1 along the path (2)-(1). Similarly, PC2 and the server in the DMZ can access each other.
 - Assume that the VRRP status of Firewall A is different from that of Firewall B. For example, the interface connecting Firewall B to the Trust zone is in backup state, and the interface connecting Firewall B to the Untrust zone is in master state. After the packets from PC1 reach PC2 through Firewall A, Firewall A dynamically generates a session entry. The packets returned by PC2 are sent along the path (5). In this case, Firewall B does not have the session entry of the corresponding data flow. If no other packet filtering rule permits the packets, Firewall B discards the packets. As a result, the session is interrupted.

- The cause of this problem is that the packet forwarding mechanisms are different.
 - When forwarding a packet, a router searches the routing table based on the destination of the packet and forwards the packet only when the packet matches a routing entry in the routing table. After a link switchover, subsequent packets continue to be forwarded without being affected.
 - When forwarding a packet, a stateful inspection firewall checks whether the first packet is permitted. If so, the firewall establishes a 5-tuple session entry. Only subsequent packets (including returned packets) matching the session entry can pass through the firewall. If subsequent packets cannot match the session entry after a link switchover, services are interrupted.
- To implement hot standby of firewalls, firewalls must have the consistent VRRP status and consistent status information.

Contents

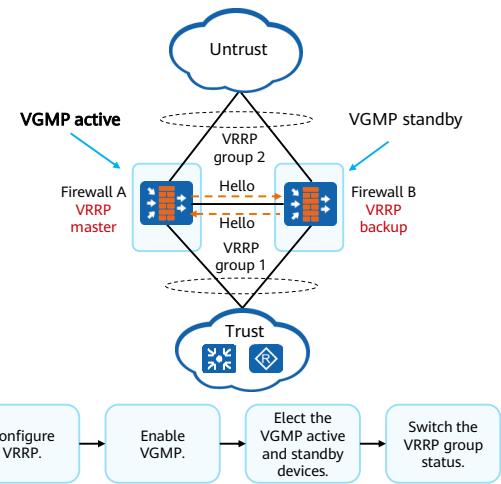
1. Hot Standby Fundamentals

- VRRP
- VGMP Group
- HRP
- Firewall Hot Standby

2. Hot Standby Basic Networking and Configuration

VGMP Basic Principles (1)

- To ensure the consistent VRRP group status, the VRRP Group Management Protocol (VGMP) is introduced based on VRRP. Multiple VRRP groups on a firewall are added to the same VGMP group. The VGMP group manages the status of all VRRP groups in a unified manner to ensure the consistent VRRP group status.
 - The VGMP group state of firewalls can be load-balance, active, or standby.
 - A VGMP group notifies its running status by sending VGMP packets, and elects the VGMP active and standby devices based on Hello priority. The VGMP group state of the VGMP active device is active, and that of the VGMP standby device is standby.
 - When the VGMP group state of a firewall is active/standby, all VRRP groups in the VGMP group are in active/standby state.
- The figure shows the process of electing the VGMP active and standby devices.



12 Huawei Confidential

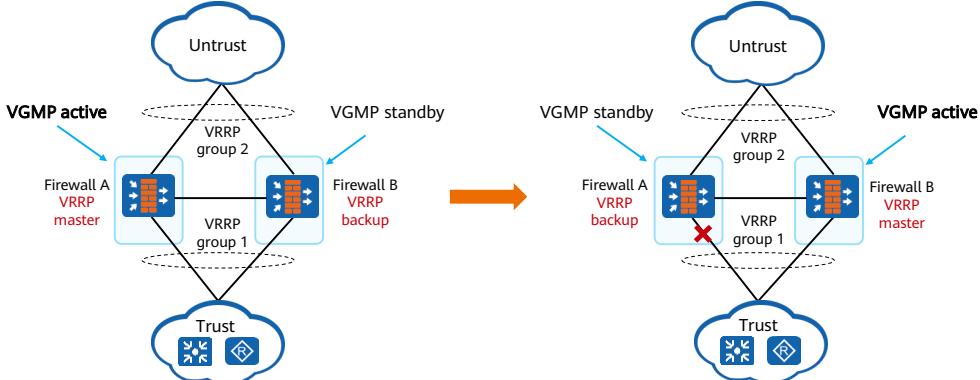


- VGMP enables firewalls to implement active/standby state management based on VGMP groups.
- VGMP group states:
 - Initialize is the initial state when hot standby is not enabled on the device.
 - If the VGMP group priority of the local device is the same as that of the peer device, the VGMP group state of the local device is load-balance.
 - If the VGMP group priority of the local device is higher than that of the peer device, the VGMP group state of the local device is active.
 - If the VGMP group priority of the local device is lower than that of the peer device, the VGMP group state of the local device is standby.
 - When the local device does not receive VGMP packets from the peer device, it cannot learn the VGMP group priority of the peer device, and therefore maintains its VGMP group state as active.
 - When the VGMP group state 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 VGMP active firewall. In this case, the VGMP group state of the other firewall is standby, and this firewall becomes the VGMP standby firewall.
- VGMP packets include VGMP Hello packets, HRP Hello packets, and HRP data packets.
 - VGMP packets are sent through a heartbeat interface at an interval of 1s by default.

- VGMP Hello packets are used to negotiate the active/standby status of firewalls. The active and standby firewalls periodically send VGMP Hello packets to notify the peer end of their running status (such as the priority and device status). When an event is triggered (for example, VGMP is enabled or the priority is changed), VGMP Hello packets are also sent.
 - HRP Hello packets are used to detect whether the peer VGMP group is working. The active and standby firewalls periodically send HRP Hello packets to the peer end. If the standby firewall does not receive any HRP Hello packet from the peer end within five packet transmission intervals, it considers that the peer end is faulty and switches to the active state.
- The process of electing the active device in a VGMP group is as follows:
 - Configure VRRP groups 1 and 2. In VRRP groups 1 and 2, specify Firewall A as the master device and Firewall B as the backup device.
 - Enable VGMP. VRRP groups 1 and 2 are then managed by the VGMP group of Firewall A and Firewall B.
 - Elect the VGMP active device: After VGMP is enabled, the VRRP group priority becomes invalid, and the VRRP master device is selected based on the VGMP priority. Firewall A and Firewall B send VGMP Hello packets to each other. By default, the VGMP group priorities of the two firewalls are the same, which is 45000 (varying with the firewall model and version). In this case, the VGMP group status of the firewalls is determined based on the VRRP configuration.
 - Switch the VRRP group status: Based on the configuration, Firewall A becomes the active device, and Firewall B becomes the standby device. In this case, Firewall A functions as the master device in VRRP groups 1 and 2 to forward traffic.

VGMP Basic Principles (2)

- When a fault occurs, VGMP switches the status of VRRP groups 1 and 2. When a VGMP group is in active state, the state of all VRRP groups in the VGMP group is master. When a VGMP group is in standby state, the state of all VRRP groups in the VGMP group is backup.



14 Huawei Confidential

HUAWEI

- The figure on the left shows the working principle when Firewall A is working properly. VRRP groups 1 and 2 on Firewall A are added to the active VGMP group, and VRRP groups 1 and 2 on Firewall B are added to the standby VGMP group. The status of a VGMP group determines the status of the VRRP groups in the VGMP group. Therefore, the status of VRRP groups 1 and 2 on Firewall A is Master, and that on Firewall B is Backup. In this case, Firewall A is the master device in VRRP groups 1 and 2, and Firewall B is the backup device in VRRP groups 1 and 2. Therefore, upstream and downstream service traffic is diverted to Firewall A for forwarding.
- The figure on the right shows the working principle when a firewall is faulty. When an interface of Firewall A is faulty, the VGMP group controls the status switchover of VRRP groups in a unified manner as follows:
 - When the downstream interface of Firewall A is faulty, the status of VRRP group 1 on Firewall A changes from master to initialize.
 - The VGMP group on Firewall A detects the fault, decreases its priority, compares the priority with that of the VGMP group on Firewall B, and renegotiates the active/standby status.
 - After the negotiation, the VGMP group status of Firewall A changes from active to standby, and that of Firewall B changes from standby to active.

- The VGMP group status determines the status of the VRRP groups in the VGMP group. Therefore, the VGMP group on Firewall A forces VRRP group 2 to switch from the master state to the backup state, and the VGMP group on Firewall B forces VRRP groups 1 and 2 to switch from the backup state to the master state. In this way, Firewall B becomes the master device in VRRP groups 1 and 2, and Firewall A becomes the backup device in VRRP groups 1 and 2.
- Firewall B then sends gratuitous ARP packets to the Trust and Untrust zones to update their MAC address tables so that the upstream and return packets from the Trust zone to the Untrust zone are forwarded to Firewall B. The status of all VRRP groups is centrally switched, preventing service interruptions.
- The following faults will trigger the VGMP group status switchover. The reduced priority value varies according to the fault:
 - An interface monitored by a VGMP group is faulty.
 - A link monitored by VGMP is faulty.
 - An LPU is faulty.
 - A service board is faulty.
 - An SFU is faulty.

VGMP Group Management

- Status consistency management
 - A VGMP group controls the status switchover of all VRRP groups in a unified manner. After a VRRP group is added to a VGMP group, the status of the VRRP group cannot be switched independently.
- Preemption management
 - When the original active device recovers, the priority of its VGMP group is also restored. In this case, the original active device preempts to be the active device.
 - After a VRRP group is added to a VGMP group, the preemption function of the VRRP group becomes ineffective, and the VGMP group determines whether to perform preemption.
- Channel management
 - Channel management determines available interfaces between two firewalls in hot standby mode. The VGMP and HRP modules automatically select available interfaces to send VGMP and HRP packets.

Contents

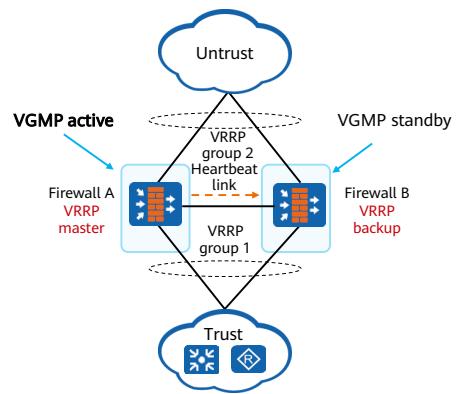
1. Hot Standby Fundamentals

- VRRP
- VGMP Group
- HRP
- Firewall Hot Standby

2. Hot Standby Basic Networking and Configuration

Basic HRP Concepts

- The Huawei Redundancy Protocol (HRP) dynamically backs up status data and key configuration commands between the active and standby firewalls.
- Backup direction
 - Configuration commands that can be backed up can be executed only on the active device. These commands are automatically backed up to the standby device, for example, security and NAT policy configuration commands.
 - In active/standby networking, only the active device processes services, generates service entries, and backs up the service entries to the standby device. In load balancing networking, both devices process services, generate service entries, and back up the service entries to the peer device.
- Backup channel
 - The network administrator needs to specify a backup channel interface to back up configuration and status data. Generally, the directly connected ports on two firewalls set up the backup channel, which is also called the heartbeat link (VGMP uses this channel for communication).



Configuration and Status Backup

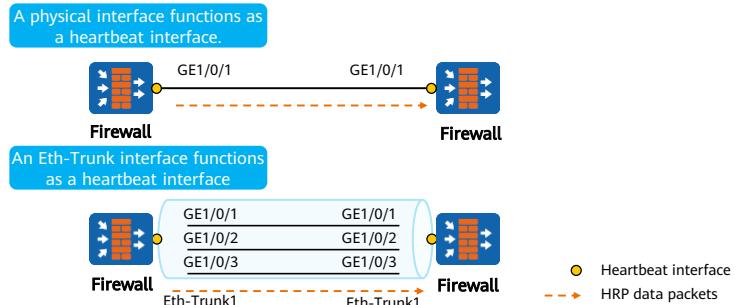
- To ensure smooth service switchover between two devices, the two devices need to back up their configurations and status information.

Backup Mode	Backup Content
<ul style="list-style-type: none">Automatic backup: This function can automatically back up configuration commands in real time and periodically back up status information. This function is enabled by default and applies to various networks that require hot standby.Manual batch backup needs to be manually triggered by the administrator. Each time the manual batch backup command is executed, the active device immediately synchronizes the configuration commands and status information to the standby device.Automatic configuration synchronization between the active and standby firewalls after device restart: The device that is successfully restarted automatically synchronizes the configuration from the firewall that is carrying services.Quick session backup: This function applies to the load balancing scenario where the forward and return paths of packets are inconsistent.	<ul style="list-style-type: none">Device configuration<ul style="list-style-type: none">Policies: include security policy, NAT policy, authentication policy, attack defense, and ASPF.Objects: include address, region, service, application, user, authentication server, time range, address pool, URL category, keyword group, mail address group, signature, and security profile.Networks: include logical interface, security zone, DNS, static route (static routes can be backed up only after the hrp auto-sync config static-route command is configured), IPsec, and SSL VPN.System: includes the administrator, virtual system, and log configuration.Status information: includes session table, server-map table, blacklist, whitelist, address mapping table, MAC address table, user table, IPsec SA, and tunnel.

- After quick session backup is enabled:
 - Sessions generated for packets originated from or destined for the devices are not backed up.
 - For ICMP, sessions are generated and backed up when a device receives an ICMP Echo Request message.
 - For TCP, sessions are generated and backed up when a device receives a SYN packet.
 - For UDP, sessions are generated and backed up when a device receives the first packet in the forward direction.

HRP Heartbeat Link

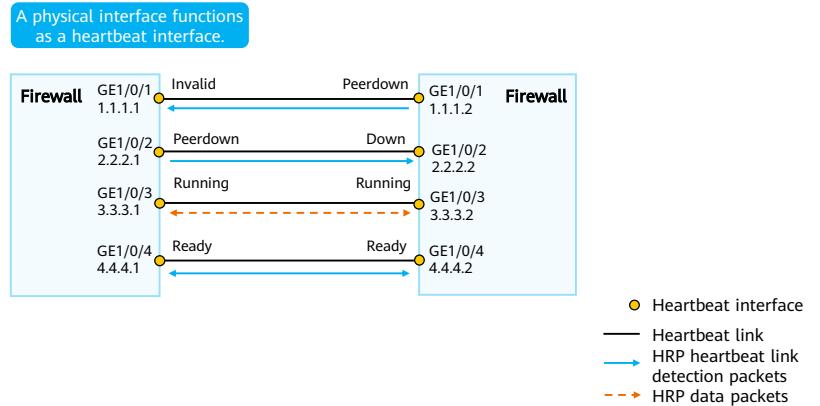
- In hot standby networking, two firewalls learn each other's status and back up configuration commands as well as various entries by exchanging messages through a heartbeat link.
 - The interfaces at both ends of a heartbeat link are called heartbeat interfaces.
 - A heartbeat interface can be a physical interface (GE interface) or a logical interface (Eth-Trunk) that is formed by bundling multiple physical interfaces.



- The packets exchanged through the heartbeat link include:
 - HRP Hello packets: Two firewalls send heartbeat packets to each other periodically (the default interval is 1 second) to check whether the peer device is alive. The heartbeat packets are also called HRP Hello packets.
 - VGMP Hello packets: are used to check the VGMP group status of the peer device to determine whether the current status of the local and peer devices is stable and whether a failover is required.
 - HRP data packets: are used to synchronize configuration commands and status information between two firewalls.
 - Heartbeat link detection packets: are used to detect whether the peer heartbeat interface can receive packets from the local heartbeat interface to determine whether the peer heartbeat interface is available.
 - Configuration consistency check packets: are used to check whether the key configurations of two firewalls are consistent, such as security policies and NAT.
 - The preceding packets are not controlled by the security policies of firewalls. Therefore, you do not need to configure security policies for these packets.
- In most cases, backup data accounts for 20% to 30% of service traffic. You can determine the number of Eth-Trunk member interfaces based on the amount of backup data.

Heartbeat Interface Status

- An HRP heartbeat interface has five states: Invalid, Down, Peerdown, Ready, and Running.



- Invalid: This state occurs when the heartbeat interface on the local firewall is incorrectly configured (the physical status is Up and the protocol status is Down). For example, the specified heartbeat interface is a Layer 2 interface or no IP address is configured for the heartbeat interface.
- Down: This state occurs when the physical status and protocol status of the heartbeat interface on the local firewall are Down.
- Peerdown: When both the physical status and protocol status of the heartbeat interface on the local firewall are Up, the heartbeat interface sends heartbeat link detection packets to the peer heartbeat interface. If the local heartbeat interface cannot receive any response packets from the peer heartbeat interface, the local firewall sets the local heartbeat interface to Peerdown. Even so, the local heartbeat interface continues sending heartbeat link detection packets so that the heartbeat link can be connected after the peer heartbeat interface goes Up.

- Ready: When both the physical status and protocol status of the heartbeat interface on the local firewall are Up, the heartbeat interface sends heartbeat link detection packets to the peer heartbeat interface. If the peer heartbeat interface can respond to the packets (and send heartbeat link detection packets), the firewall sets the status of the local heartbeat interface to Ready, indicating that the interface is ready to send and receive heartbeat packets. In addition, the local heartbeat interface continues sending heartbeat link detection packets to ensure that the heartbeat link is normal.
- Running: If the local firewall has multiple heartbeat interfaces in Ready state, the firewall selects the first configured heartbeat interface to establish a heartbeat link and sets the heartbeat interface status to Running. If there is only one heartbeat interface in Ready state, it becomes the heartbeat interface in Running state. The heartbeat interface in Running state sends HRP heartbeat packets, HRP data packets, HRP link detection packets, VGMP packets, and consistency check packets. In this case, other heartbeat interfaces in Ready state are in backup state. When the heartbeat interface in Running state or the heartbeat link is faulty, other heartbeat interfaces in Ready state take over services from the current heartbeat interface (in the sequence in which these heartbeat interfaces were configured).

Contents

1. Hot Standby Fundamentals

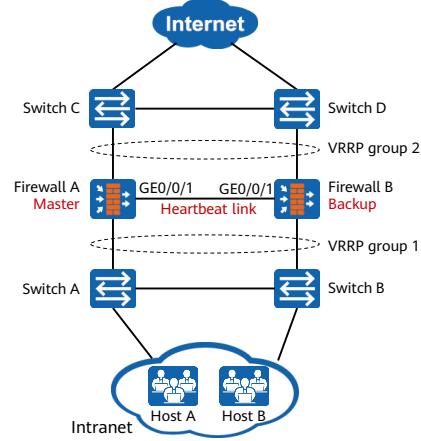
- VRRP
- VGMP Group
- HRP
- **Firewall Hot Standby**

2. Hot Standby Basic Networking and Configuration

Application Scenario of Firewall Hot Standby in Active/Standby Mode

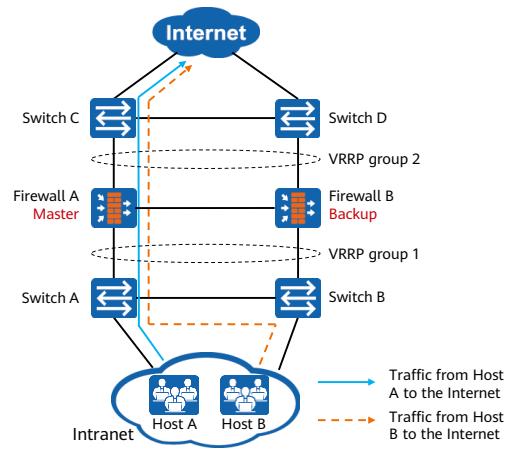
- Application scenario
 - Firewall hot standby applies to scenarios that require high reliability, such as enterprise office scenarios. To improve network reliability, two firewalls can be deployed at the egress of an enterprise network to implement hot standby. To meet service requirements, the firewalls work in active/standby mode.
- Configuration analysis
 - VGMP group status of firewalls: Firewall A is the master firewall, and its VGMP group status is active. Firewall B is the backup firewall, and its VGMP group status is standby.
 - VRRP group: VRRP group 1 is configured in the downstream direction of the firewalls, and VRRP group 2 is configured in the upstream direction of the firewalls. In VRRP groups 1 and 2, Firewall A is configured as the master device, and Firewall B as the backup device.
 - Backup mode: By default, the automatic backup mode is used.
 - Backup interface: Interfaces GE0/0/1 of the firewalls are the heartbeat interfaces and are connected through the heartbeat link.
 - Preemption: This function is enabled by default. The default preemption delay is 60s.

24 Huawei Confidential



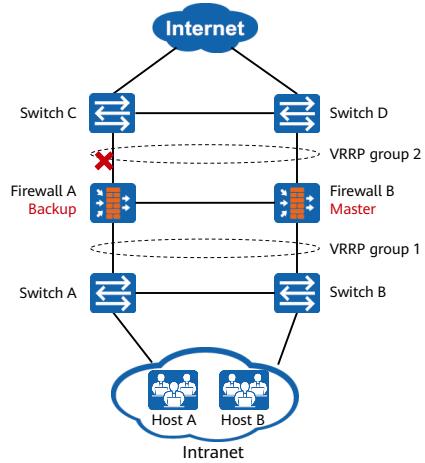
Working Process of Firewall Hot Standby in Active/Standby Mode

- Firewall status: Firewall A is the master device, its VGMP group status is active, and its status in VRRP groups 1 and 2 is master. Firewall B is the backup device, its VGMP group status is standby, and its status in VRRP groups 1 and 2 is backup.
- Configuration and status backup: The configuration and status of Firewall A are backed up to Firewall B through the heartbeat link in real time.
- Traffic forwarding path: 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. Switch A forwards the traffic to Firewall A based on the MAC address table, and then Firewall A forwards the traffic to the Internet. The traffic forwarding process is similar in the return direction.



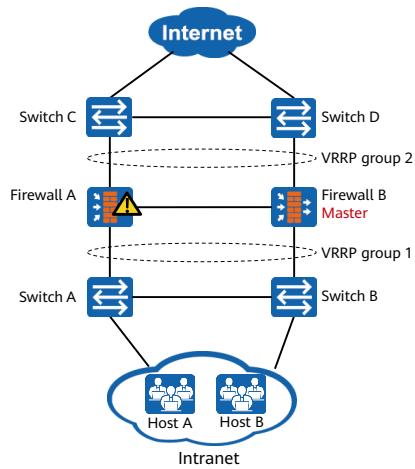
Active/Standby Switchover of Firewall Hot Standby (1)

- Service port/line fault
 - As shown in the figure, when the service interface or service line of Firewall A is faulty, the priority of the VGMP group on Firewall A 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.



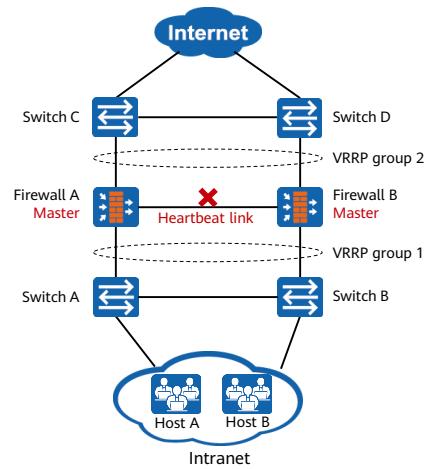
Active/Standby Switchover of Firewall Hot Standby (2)

- Device fault
 - 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 master device. Firewall B then changes its VGMP group status to active and the status of VRRP groups 1 and 2 to master.



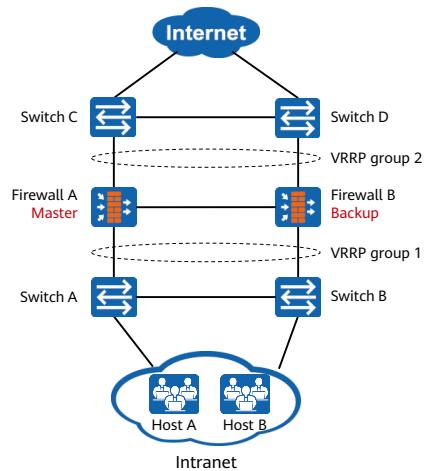
Active/Standby Switchover of Firewall Hot Standby (3)

- Heartbeat link fault
 - If the heartbeat link is faulty and Firewall B does not receive HRP Hello packets from Firewall A within five packet transmission intervals, Firewall B becomes the master device and changes its VGMP group status to active and the status of VRRP groups 1 and 2 to master. In this case, the dual-active situation occurs.



Active/Standby Switchback of Firewall Hot Standby

- After Firewall A recovers, the priority of its VGMP group is restored. 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.

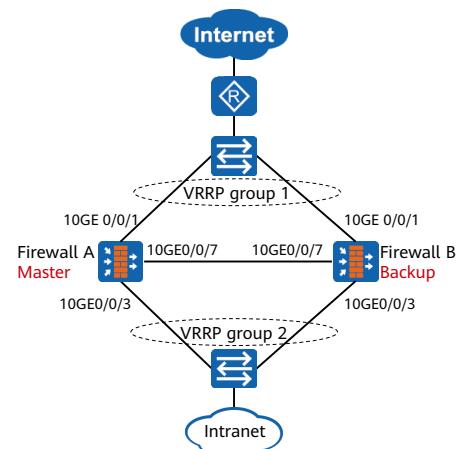


Contents

1. Hot Standby Fundamentals
2. Hot Standby Basic Networking and Configuration

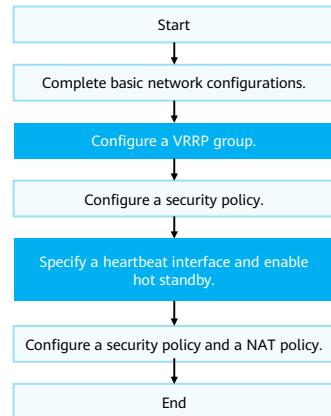
Example for Configuring Firewall Hot Standby in Active/Standby Mode (1)

- Requirements:
 - The service interfaces of Firewalls A and B work at Layer 3 and are connected to Layer 2 switches in both upstream and downstream directions. The upstream switch connects to the interface provided by the carrier who has assigned the IP address 1.1.1.1 to the enterprise. Firewalls A and B are required to work in active/standby mode. In normal cases, traffic is forwarded by Firewall A. If Firewall A fails, traffic is forwarded by Firewall B to ensure service continuity.
 - Virtual IP address of VRRP group 1: 1.1.1.1/24
 - Virtual IP address of VRRP group 2: 10.3.0.3/24
 - IP address of the heartbeat interface 10GE0/0/7 on Firewall A: 10.10.0.1/24
 - IP address of the heartbeat interface 10GE0/0/7 on Firewall B: 10.10.0.2/24



Example for Configuring Firewall Hot Standby in Active/Standby Mode (2)

- Configuration roadmap:
 - Complete basic network configurations, including configuring IP addresses for interfaces of two firewalls, adding interfaces to security zones, and configuring default routes.
 - Configure a VRRP group on the two firewalls.
 - Configure a security policy to allow heartbeat interfaces to exchange HRP packets.
 - Specify heartbeat interfaces, configure the authentication key, and enable hot standby.
 - Configure a security policy to allow intranet users to access the Internet.
 - Configure a NAT policy to allow intranet users to access the Internet.



Example for Configuring Firewall Hot Standby in Active/Standby Mode (3)

- Configure VRRP group 1 on the upstream service interface 10GE0/0/1 of Firewall A and set the status to active.

```
[FWA] interface 10ge0/0/1  
[FWA-10GE0/0/1] vrrp vrid 1 virtual-ip 1.1.1.1 active  
[FWA-10GE0/0/1] quit
```

```
[FWA] interface 10ge0/0/3  
[FWA-10GE0/0/3] vrrp vrid 2 virtual-ip 10.3.0.3 active  
[FWA-10GE0/0/3] quit
```

- Configure VRRP group 1 on the upstream service interface 10GE0/0/1 of Firewall B and set the status to standby.

```
[FWB] interface 10ge0/0/1  
[FWB-10GE0/0/1] vrrp vrid 1 virtual-ip 1.1.1.1 standby  
[FWB-10GE0/0/1] quit
```

```
[FWB] interface 10ge0/0/3  
[FWB-10GE0/0/3] vrrp vrid 2 virtual-ip 10.3.0.3 standby  
[FWB-10GE0/0/3] quit
```

Example for Configuring Firewall Hot Standby in Active/Standby Mode (4)

- Specify a heartbeat interface on Firewall A, configure the authentication key, and enable hot standby.

```
[FWA] hrp interface 10ge0/0/7 remote 10.10.0.2  
[FWA] hrp authentication-key Admin@123  
[FWA] hrp enable
```

- Specify a heartbeat interface on Firewall B, configure the authentication key, and enable hot standby.

```
[FWB] hrp interface 10ge0/0/7 remote 10.10.0.1  
[FWB] hrp authentication-key Admin@123  
[FWB] hrp enable
```

Quiz

1. (True/False) The HRP technology implements configuration synchronization between the active and standby firewalls and ensures that the configuration is not lost after a firewall restart. Then no information needs to be configured on the standby firewall. ()
 - A. True
 - B. False
2. (True/False) Firewall quick session backup applies to the load balancing scenario. ()
 - A. True
 - B. False

1. B
2. A

Summary

- This course describes the application scenarios, technical principles, packet forwarding process, and active/standby switchover logic of hot standby, as well as the key configurations and configuration processes of hot standby in different networking modes.
- Upon completion of this course, you will be able to understand the application scenarios of hot standby, independently configure hot standby for Huawei firewalls based on the lab in the actual environment, and master how to deploy firewalls in hot standby scenarios.

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 and Abbreviation	Full Name
GE	Gigabit Ethernet
HRP	Huawei Redundancy Protocol
USG	Universal Service Gateway
VGMP	VRRP Group Management Protocol
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
portfolio, new technology, 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 IPS



Foreword

- Currently, malware is the most common form of security threats, while the impact of greyware is increasing and security threats correlated to malicious code are critical to network security.
- Instead of dealing with traditional virus attacks, users now have to fend off combinations of network threats, including viruses, hacker intrusions, Trojan horses, botnets, and spyware. Therefore, the current anti-virus mechanism or single security technology struggles to mitigate such attacks.
- This course explains what intrusion is and describes to what degree Huawei firewalls support intrusion prevention.

Objectives

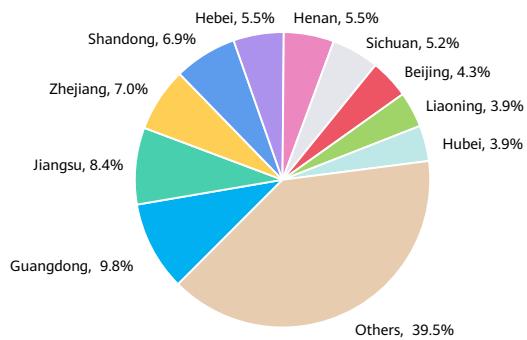
- Upon completion of this course, you will be able to:
 - Describe the different types of intrusion prevention.
 - Describe the fundamentals of intrusion prevention.
 - Deploy network antivirus policies.

Contents

- 1. Intrusion Overview**
2. Intrusion Prevention
3. Antivirus

Status Quo of Network Threats

- According to *2021 Midyear Cybersecurity Report* published by CNCERT/CC, the following pie chart shows the distribution of IP addresses attacked by computer malware in Chinese Mainland for the first half year in 2021.



- In the first half year of 2021, the captured malware samples and malware downloads per day amounted to about 23.07 million and 5.82 million. Besides, about 208,000 malware families were involved. The primary source of malware in Chinese mainland came from Henan, Guangdong, and Zhejiang provinces. Among the attack-targeted IP addresses, about 30.48 million IP addresses were attacked by malware in Chinese mainland, which accounts for around 7.8% of the total number of IP addresses in China. Among the jumping-off places for malware propagation, the majority of them were abroad. In addition, these attacked IP addresses mainly distributed in Guangdong, Jiangsu, and Zhejiang provinces.

Network Security Case Study

- Nowadays, most network threats, such as viruses, no longer only target at computer systems. Instead, they are also exploited by hackers and criminals for financial gain. This is causing conventional computer viruses and other network threats to evolve into interest-driven, all-round network threats.

Case study 1

Hackers breached the largest fuel pipeline in a country. Therefore, the company had to shut down the entirety of its energy supply system, dramatically affecting the supply of national fuel. In the meantime, it was the first time the country issued a national emergency declaration because of cyberattack.

Case study 2

The Internet service provider of a country's public sector was hit by massive Distributed Denial of Service (DDoS) attacks, causing disruption of the government's internal systems and public websites. In addition, many websites and services of the government were forced offline.

Case study 3

A computer giant has been hit by a ransomware attack, leading to the leakage of electronic spreadsheets and bank balances. The threat actors demanded the largest known ransom to date, \$50,000,000.

- Among current security threats, malware (viruses, worms, bots, rootkits, Trojan horses, backdoors, vulnerability attack programs, and mobile malware) accounts for a high proportion, while the impact of greyware (spyware and adware) is increasing. Moreover, security threats correlated to crimes are critical to network security.

Intrusion Overview

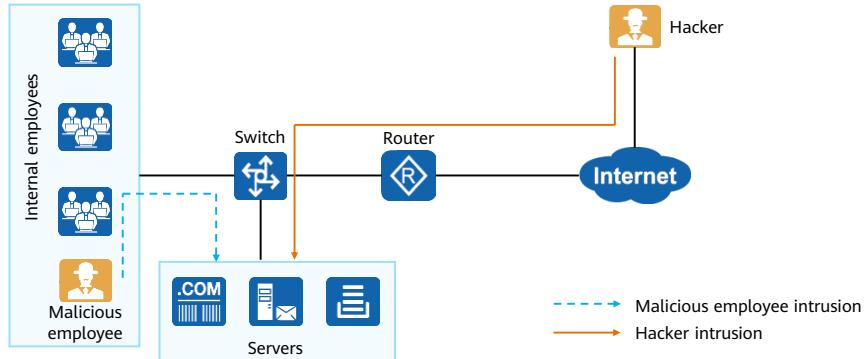
- An intrusion is a behavior that a user attempts to access information system resources or tamper data in the information system without authorization, to make the information system unreliable or unavailable.
- The purpose of intrusions is to compromise the integrity, confidentiality, availability, and controllability of information systems.
- Typical intrusions are as follows:
 - Attacks exploiting system and software vulnerabilities
 - DDoS attack
 - Viruses and malicious software security threats

Feature \ Threat	Unauthorized Access	Unauthorized Tampering	Unauthorized Damage
System and Software Vulnerabilities	✓	✓	✓
DDoS Attack	✓		✓
Virus and Malware	✓	✓	✓

- The typical intrusion behaviors are as follows:
 - Tamper with web pages
 - Crack system passwords
 - Copy and check sensitive data
 - Obtain user passwords by using network sniffer tools
 - Access unauthorized servers
 - Obtain raw packets by using special hardware
 - Implant Trojan horses on hosts

Vulnerability Threat

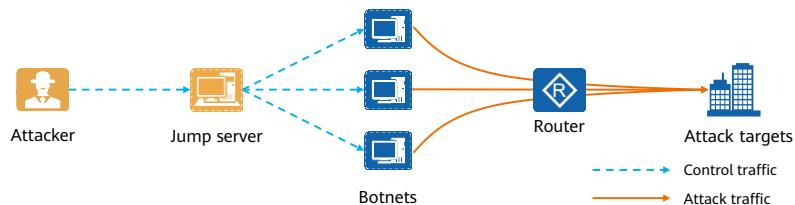
- Hackers and malicious employees exploit system and software vulnerabilities to intrude into servers, putting key service data at risk.



- Vulnerabilities will result in serious security threats:
 - Many application software running on enterprise intranets may have vulnerabilities.
 - The Internet helps vulnerabilities in application software spread rapidly.
 - Worms are widely spread by exploiting application software vulnerabilities, consuming network bandwidth, and damaging important data.
 - Hackers and malicious employees target vulnerabilities to intrude into enterprise servers, and tamper with, destroy, and steal confidential business information.

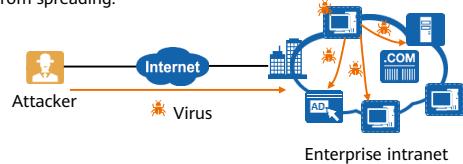
DDoS Attack

- DDoS refers to distributed denial of service. In DDoS attacks, attackers control many zombie hosts to send a large number of crafted attack packets to a target. As a result, links are congested, and system resources are exhausted on the attacked network. In this case, the attacked target fails to provide services for normal users.
- Currently, the Internet has many zombie hosts and botnets. DDoS attacks launched for financial gain become a major security threat to the Internet. When a DDoS attack occurs, a large amount of network bandwidth is occupied and networks break down. The resources of the attacked servers are exhausted and cannot respond to normal user requests, which may even result in system breakdown and enterprise service interruption.



Malicious Code Intrusion Threat

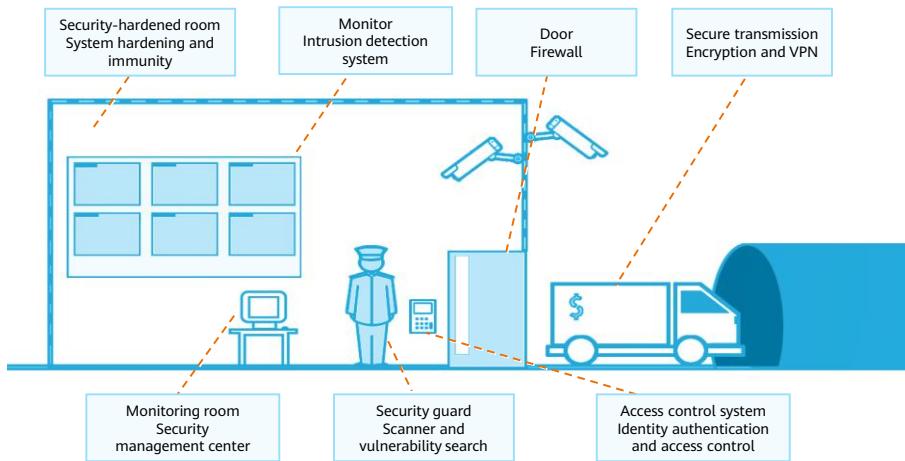
- Malicious code has various types, such as viruses, Trojan horses, and spyware. Malicious code infects or attaches to application programs or files, and spreads through emails or shared files, threatening the security of user hosts and networks. Malicious code intrusion has the following characteristics:
 - Web browsing and email transmission are the main ways for viruses, Trojan horses, and spyware to access intranets.
 - Viruses make computer systems crash, and tamper with or destroy service data.
 - Trojan horses not only steal the significant information from computers but also damage intranet hosts.
 - Spyware gathers, uses, and spreads sensitive information about enterprise employees, which severely affects normal services of enterprises.
 - Antivirus software for PC cannot globally prevent malicious code from spreading.



Contents

1. Intrusion Overview
2. **Intrusion Prevention**
 - Overview of Intrusion Prevention
 - Example for Configuring Intrusion Prevention
3. Antivirus

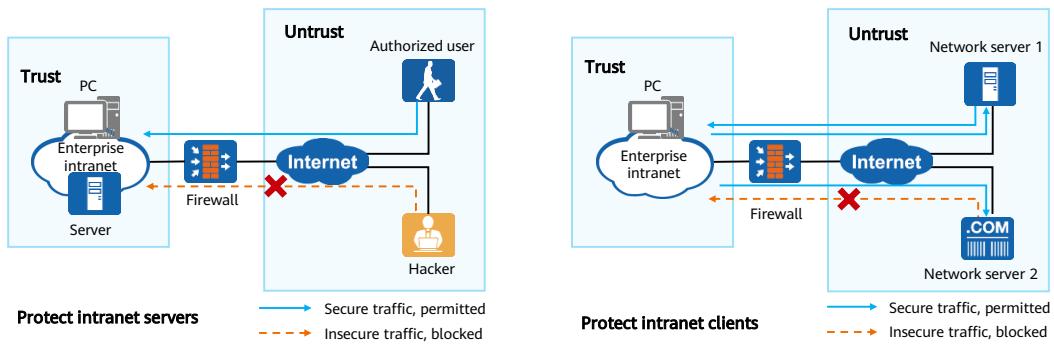
Positions of Security Devices in a Security System



- Intrusion Detection (ID) is a proactive and dynamic security and defense technology that can detect intrusion behaviors in real time by monitoring operations, auditing various data, and analyzing symptoms. In addition, ID covers various authorized and unauthorized intrusion behaviors.
- An Intrusion Detection System (IDS) immediately enables security mechanisms if any behavior that violates security policies or any sign indicating that the system is attacked is detected.
- In the security system, the IDS plays the role of a surveillance camera. It monitors and analyzes the traffic of key nodes in the information system and detects ongoing security events. In other words, the IDS is like a monitor in a security monitoring system. By using the IDS, security guards can obtain the traffic of key nodes and perform intelligent traffic analysis to discover abnormal and suspicious network behaviors and report them to administrators in monitoring rooms.

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.



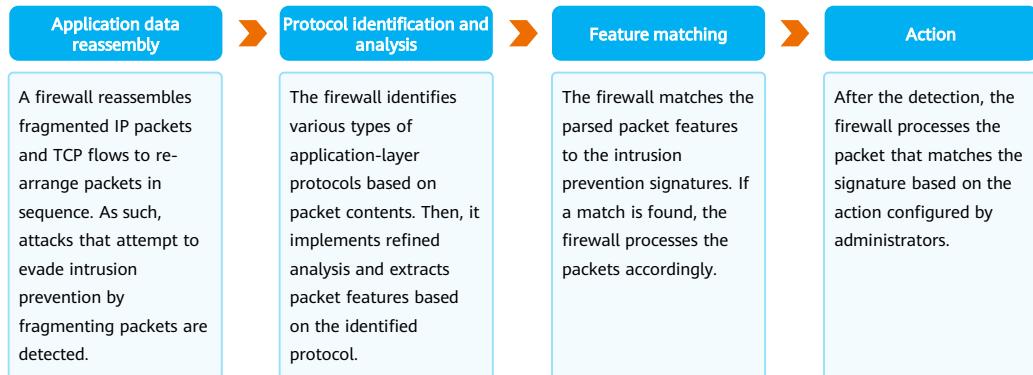
13 Huawei Confidential



- 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

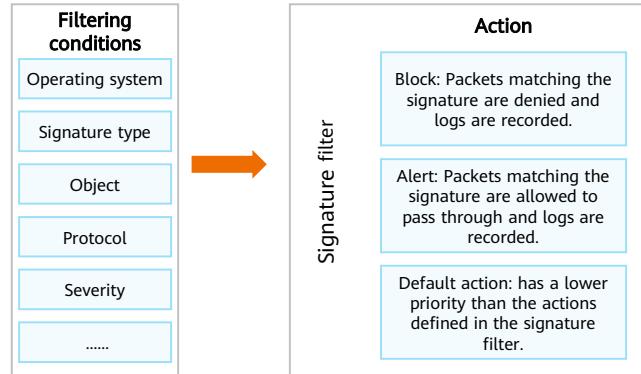
- Intrusion prevention signatures describe the features of network attacks. A firewall detects and defends against attacks by comparing data flows with the signatures.

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

- After the IPS signature database on a device is updated, a large number of signatures are generated but not categorized. In addition, features contained in some signatures do not exist on the local network. To deal with these issues, a signature filter can be configured to manage and filter unnecessary signatures. It defines actions to be taken on features matching different filtering conditions.



- A signature filter is a set of filtering conditions, including the type of signatures, object, protocol, severity, and operating system (OS). Only signatures that match all the filtering conditions can be added to a signature filter. If multiple values are configured in one condition, the relationship among these values is OR, which means that a signature matches a condition as long as the signature matches any value of this condition.
- The action of a signature filter can be **Block**, **Alert**, or **Default** (use the default actions of signatures). The action of a signature filter has a higher priority than the default action of a signature.
- Signature filters configured earlier have higher priorities. If two signature filters in a security profile contain the same signature, packets matching the signature are processed according to the signature filter with a higher priority.

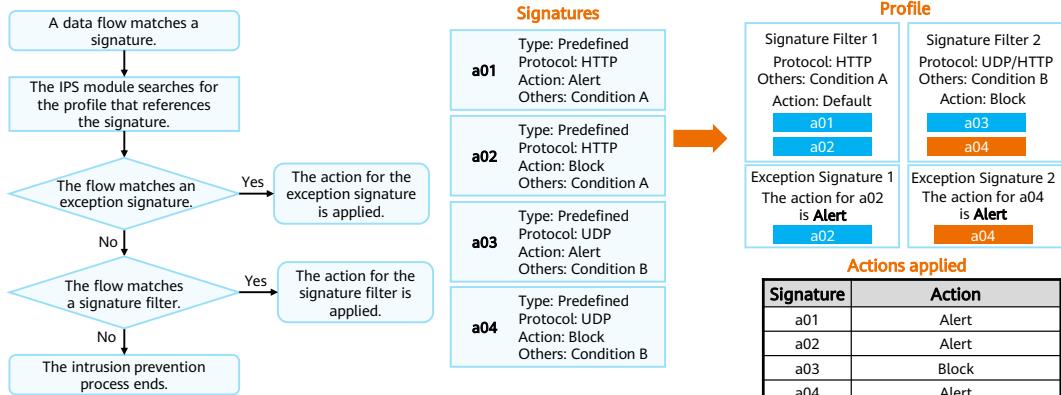
Exception Signature

- To facilitate management, the same action is taken on all signatures in a signature filter. If some signatures need to be configured with actions different from the action of the signature filter, these signatures can be specified as exception signatures and separate actions can be configured for them.
- The action for an exception signature can be one of the following:
 - Block: Packets matching the signature are denied and logs are recorded.
 - Alert: Packets matching the signature are allowed to pass through and logs are recorded.
 - Allow: Packets matching the signature are allowed to pass through and no log is recorded.
 - Blacklist: Packets matching the signature are discarded, the data flows to which the packets belong are blocked, logs are generated, and the source or destination IP addresses of the packets are blacklisted.
- The action for an exception signature has a higher priority than that for a signature filter. If an exception signature matches a signature filter, the action for the exception signature applies.

- Assume that the action for a batch of signatures filtered by a signature filter is **Block**. However, a self-developed software requested by an employee is also blocked. The log indicates that the self-developed software matches a signature in the signature filter so that the software is blocked unexpectedly. To deal with this issue, the signature can be specified as an exception signature with the **Allow** action.

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.



18 Huawei Confidential



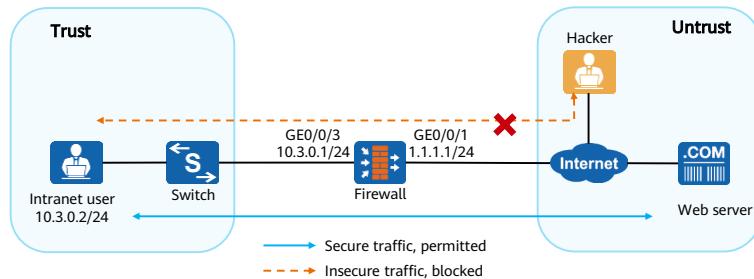
- When a data flow matches multiple signatures:
 - If the actions for these signatures are all **Alert**, the action applied to the data flow is **Alert**.
 - If the action for any signature is **Block**, the action applied to the data flow is **Block**.
- If the data flow matches multiple signature filters, the action for the signature filter with the highest priority is applied to the data flow.

Contents

1. Overview of Intrusion
2. **Intrusion Prevention**
 - Overview of Intrusion Prevention
 - Example for Configuring Intrusion Prevention
3. Antivirus

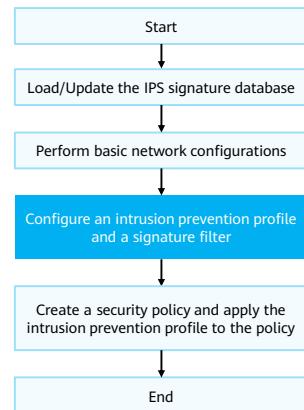
Example for Configuring Intrusion Prevention (1/4)

- Requirement description:
 - An enterprise deploys a firewall at the network border as a security gateway. In this networking, intranet users can access the web server on the Internet.
 - The enterprise needs to configure the intrusion prevention function on the firewall to protect intranet users from attacks, such as an attack launched from a website with malicious code, when the users access the Internet web server.



Example for Configuring Intrusion Prevention (2/4)

- Configuration roadmap:
 - Configure scheduled update of the IPS signature database to minimize the possibility of false positives and negatives.
 - Set basic network parameters, including configuring IP addresses for interfaces and adding interfaces to security zones.
 - Configure an intrusion prevention profile and a signature filter.
 - Create a security policy and apply the intrusion prevention profile to the policy.



- An IPS license is required to update the IPS signature database. If the license control item is not activated, the device does not automatically load the preset signature database, and the signature database cannot be manually loaded or updated. After the license control item is activated, the signature database can be loaded and updated. After the license control item expires, the signature database cannot be manually loaded or updated, and the intrusion prevention function is available. However, the signature database may not be up-to-date, and virus detection and defense capabilities are limited.

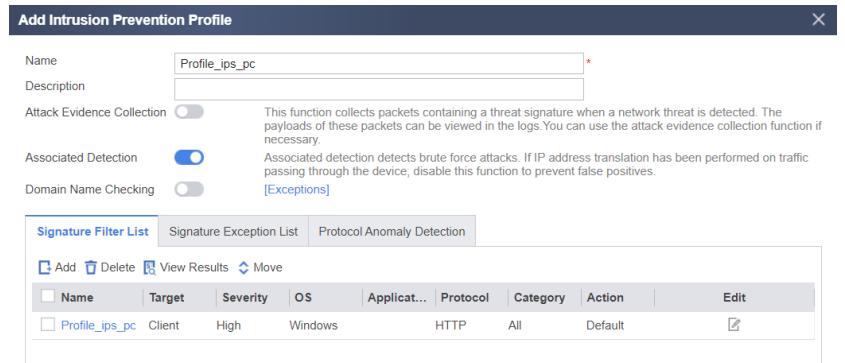
Example for Configuring Intrusion Prevention (3/4)

- Choose Object > Security Profiles > Intrusion Prevention > Add to create intrusion prevention profiles.

Name	Description	Attack Evidence Collection	Associated Detection	Domain Name Checking
default	This profile applies to all traffic.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
ids	This profile applies to IDS traffic.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
outside_firewall	This profile applies to traffic between the outside and untrust zones.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
dns	This profile applies to DNS traffic.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
inside_firewall	This profile applies to traffic between the inside and trust zones.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
mail_server	This profile applies to traffic to mail servers.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
dns_server	This profile applies to traffic to DNS servers.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
file_server	This profile applies to traffic to file servers.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
web_server	This profile applies to traffic to web servers.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
strict	This profile will force strict compliance.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
video_surveillance	This profile applies to traffic to video surveillance systems.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Example for Configuring Intrusion Prevention (4/4)

- In the **Add Intrusion Prevention Profile** dialog box, click **Add** and set the following parameters. The profile will be applied to a security policy that controls access between trust and untrust zones. Click **OK** after the configuration is completed.



Viewing Intrusion and Detection Behaviors

- Choose **Log > Threat Log** to view threat logs.

The screenshot shows the Threat Log List interface. On the left, there's a sidebar with options: Log, Traffic Log, Threat Log (which is selected and highlighted in red), URL Log, Operation Log, and System Log. The main area has a header with 'Threat Log List' and buttons for Export, Customize, View, Time, Threat Type (Intrusion), Risk Level (Low), Threat ID (1540), and Threat Name (Cisco Common Services Frame...). Below this is a table with two sections: 'Common Log Field' and 'Source' on the left, and 'Threat' and 'Destination' on the right. The 'Common Log Field' section contains fields like Time, Protocol (TCP), Security Policy (untrust), Application Category (Network), Application Subcategory (Infrastructure), and Application (HTTP). The 'Threat' section contains fields like Threat Type (Intrusion), Intrusion Subtype (Attack intrusion), Threat Name (Cisco Common Services Frame...), Threat ID (1540), Occurrences (1), Profile (strict), Action (Alert), Severity (Medium), Risk Level (Low), Target Type (Server), Operating System (all), Attack Category (XSS), and Accessed Content (icwphldevice:center.do?device=<sc...). The 'Source' section contains fields like Source Zone (untrust), Source Region (unknown-zone), Source Address (172.16.8.47), and Source Port (2882). The 'Destination' section contains fields like Destination Zone (trust), Destination Region (unknown-zone), Destination Address (172.16.8.102), and Destination Port (1741).

Common Log Field		Threat	
Time:		Threat Type:	Intrusion
Protocol:	TCP	Intrusion Subtype:	Attack intrusion
Security Policy:	untrust	Threat Name:	Cisco Common Services Frame...
Application Category:	Network	Threat ID:	1540
Application Subcategory:	Infrastructure	Occurrences:	1
Application:	HTTP	Profile:	strict
Action:	Alert	Severity:	Medium
Risk Level:	Low	Target Type:	Server
Operating System:	all	Operating System:	all
Attack Category:	XSS	Accessed Content:	icwphldevice:center.do?device=<sc...
Source		Destination	
Source Zone:	untrust	Destination Zone:	trust
Source Region:	unknown-zone	Destination Region:	unknown-zone
Source Address:	172.16.8.47	Destination Address:	172.16.8.102
Source Port:	2882	Destination Port:	1741

24 Huawei Confidential



- Pay attention to the following information about intrusion logs:
 - Profile:** indicates the security profile that matches the attack.
 - Threat Name:** An intrusion prevention signature describes the features of an attack on the network. Devices detect and defend against attacks by comparing data flows with intrusion prevention signatures.
 - Occurrences:** Whether logs are merged is determined by the mergence frequency and conditions. The value is 1 if logs are not merged.
 - Target Type:** indicates the attack target of the packet matching the signature. The value can be one of the following:
 - Server:** The attack target is a server.
 - Client:** The attack target is a client.
 - Both:** The attack targets are a server and a client.
 - Severity:** indicates severity of the attack launched by the packet matching the signature. The higher the severity, the more severe the consequences. The severity levels in the descending order from most to least severe: **High**, **Medium**, **Low**, and **Information**.

- **Operating System:** indicates the OS attacked by a packet detected by the signature. The options are as follows:
 - **all:** The attack is targeted at all OSs.
 - **android:** The attack is targeted at Android.
 - **ios:** The attack is targeted at iOS.
 - **unix-like:** The attack is targeted at UNIX.
 - **windows:** The attack is targeted at Windows.
 - **other:** The attack is targeted at other systems.
- **Intrusion Subtype:** indicates the threat category to which the features of the attack packet matching the signature belong.
- **Action:** indicates the action for a signature. The options are as follows:
 - **Alert:** The signature action is Alert.
 - **Block:** The signature action is Block.

Contents

1. Intrusion Overview
2. Intrusion Prevention
- 3. Antivirus**
 - Antivirus Fundamentals
 - Example for Configuring Antivirus

Computer Virus

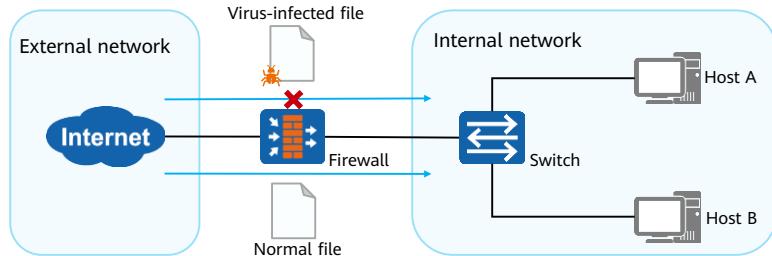
- A computer virus is a set of self-replicable instructions or program code compiled or embedded in computer programs to adversely affect a computer's use by damaging its functions or data.
- A computer virus has the following characteristics: infectivity, concealment, latency, excitability, expressivity, or destructiveness. There are three common types of malware: viruses, worms, and Trojan horses.

Item	Virus	Worm	Trojan Horse
Existence	Parasitic in files and boots	Independent entity	Implanted in files or applications
Replication mechanism	Self-replicating	Self-replicating	Not self-replicating
Infection means	Running on host programs	Relying on network and system vulnerabilities	Based on applications or carriers used for transmission
Infected target	Local computers	Other computers on the network	Computers that download applications and files implanted with Trojan horse
Triggering mechanism	Specific conditions	Programs	Computer users
Affected target	File system and hardware	Network and system performance	Information theft and denial of service
Prevention measure	Removing viruses from host programs	Installing patches for system hardening	Preventing Trojan horse implantation

- Common delivery methods for computer viruses: mobile media, network sharing, network scanning, email, and peer-to-peer (P2P) network.
- Common infected targets: OS, application, and device hardware (if a virus attacks on BIOS).
- Common computer virus carriers: executable files, scripts, macros, and boot sectors.

History of Antivirus

- With the continuous development of networks and applications, enterprise users frequently transfer and share files on networks, facing unprecedented virus threats. Enterprises can ensure data security and system stability only after viruses are prevented from networks. Therefore, it is critical for enterprises to protect computers and network systems from being attacked by viruses and to ensure normal running of network systems.
- Antivirus is a security mechanism that identifies and processes virus-infected files to ensure network security and avoid data corruption, permission change, and system crash caused by virus-infected files.



28 Huawei Confidential



- The antivirus function is used in the following scenarios to guarantee cyber security:
 - Intranet users can access the Internet and need to frequently download files from the Internet.
 - Internet users need to frequently upload files to servers on the internal network.
- As shown in the figure, the firewall serves as the gateway to isolate the external network from the internal network where user hosts and servers are located. The intranet users can download files from the Internet, and the Internet users can upload files to the intranet servers. To ensure the security of files to be uploaded or downloaded, it is necessary to configure the antivirus function on the firewall.

ASE for Virus Detection (1/2)

- The antivirus processing procedure consists of two parts: virus detection using the Adaptive Security Engine (ASE) and antivirus processing.
- The ASE detects viruses according to the following procedure:

1. Performs in-depth analysis on the traffic

- The Intelligent Awareness Engine (IAE) performs in-depth analysis on the traffic and identifies its protocol type and file transfer direction.

2. Checks whether virus detection applies to this protocol type and file transfer direction

- Firewalls perform virus detection for files transferred using the following protocols:
 - FTP, HTTP, POP3, SMTP, IMAP, NFS, and SMB
- Firewalls support virus detection for files in uploaded and downloaded directions:
 - Upload: indicates file transfer from a client to a server.
 - Download: indicates file transfer from a server to a client.

ASE for Virus Detection (2/2)

3. Checks whether files match the whitelist

- Firewalls do not perform virus detection on whitelisted files.
 - A whitelist comprises whitelist rules. Administrators can configure whitelist rules for trusted domain names, URLs, IP addresses, and IP address segments to improve antivirus detection efficiency.
 - A whitelist rule takes effect only on the antivirus profile to which the whitelist rule belongs. Each antivirus profile has its own whitelist.

4. Performs virus detection

- The IAE extracts features of a file to which antivirus is applicable and matches the extracted features against virus signatures in the antivirus signature database.
 - If a match is found, the file is considered infected and processed according to the action specified in the antivirus profile.
 - If no match is found, the file is allowed.

- Huawei analyzes and summarizes common virus signatures to construct the antivirus signature database. This database defines common virus signatures and assigns a unique virus ID to each signature. After the database is loaded on a device, the device can identify viruses that match the signatures defined in the database. To identify new viruses, the device needs to continuously download update packages from the security center to update its antivirus signature database.

Antivirus Processing (1/2)

- When a firewall detects that the file transferred is a virus-infected file, it performs the following operations:

1. Checks whether this virus matches a virus exception

- If a user recognizes a detected virus as a false positive, the user can add the corresponding virus ID to the virus exception.
- If a file is detected to be an exception, it is allowed to transfer.

2. Checks whether this virus matches an application exception

- If the virus does not match any virus exception, check whether it matches an application exception. If it matches an application exception, it is processed according to the action (allow, alert, or block) specified for the application exception.
- When actions are being configured:
 - If the action for a protocol is configured but no action is configured for any application, the action for the protocol applies to all applications that use the protocol.
 - If the action for a protocol and the action for an application that uses the protocol are both configured, the action for the application takes precedence over that for the protocol.

Antivirus Processing (2/2)

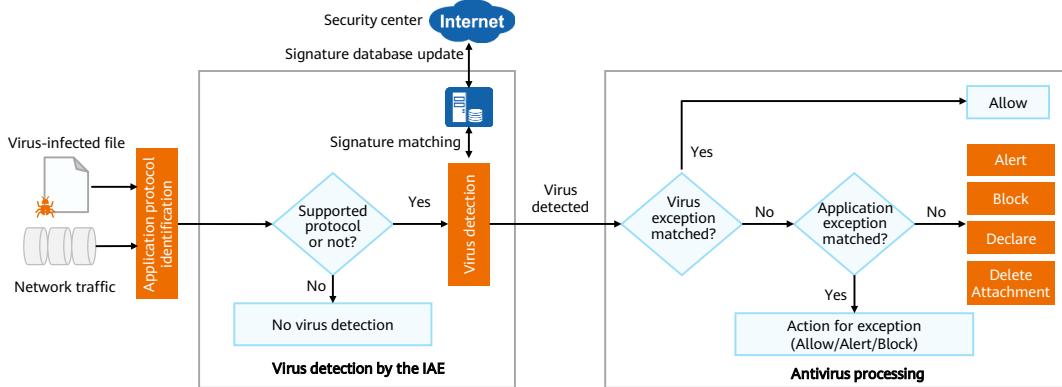
3. Applies the action for protocol and transfer direction specified in the profile

- If the virus matches neither virus exceptions nor application exceptions, the action for protocol and transfer direction specified in the antivirus profile applies.
- The following table shows actions that a firewall can take on files of different protocols and in different transfer directions.

Protocol	Transfer Direction	Action	Description
HTTP	Upload/Download	Alert/Block	
FTP	Upload/Download	Alert/Block	
NFS	Upload/Download	Alert	
SMB	Upload/Download	Alert/Block	
SMTP	Upload	Alert/Declare/Delete Attachment	Alert: The firewall allows virus-infected files and generates virus logs. Block: The firewall blocks virus-infected files and generates virus logs. Declare: For virus-infected email messages, the firewall allows them, but adds information to the email body to announce the detection of viruses, and generates virus logs. Delete Attachment: For virus-infected email messages, the firewall deletes attachments in infected emails to announce the detection of viruses and deletion of attachments in the email body, allows them, and generates virus logs.
POP3	Download	Alert/Declare/Delete Attachment	
IMAP	Upload/Download	Alert/Declare/Delete Attachment	

Antivirus Working Process

- A firewall uses the IAE and constantly updated antivirus signature database to detect and process virus-infected files.

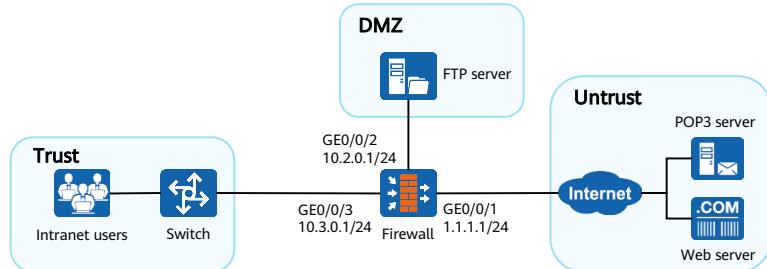


Contents

1. Intrusion Overview
2. Intrusion Prevention
- 3. Antivirus**
 - Antivirus Fundamentals
 - Example for Configuring Antivirus

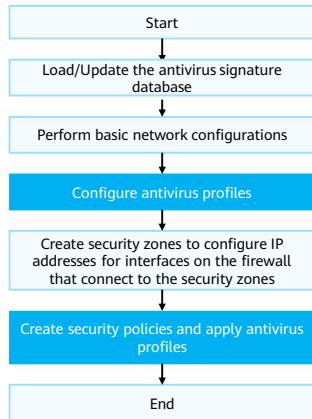
Example for Configuring Antivirus (1/5)

- Requirement description:
 - A company deploys a firewall at the network border as a security gateway. Intranet users need to download files and emails through web and POP3 servers, and Internet users need to upload files to the intranet FTP server.
 - The company requires that the firewall provides the antivirus function to prevent virus-infected files from entering the intranet to ensure the security of intranet users and servers.



Example for Configuring Antivirus (2/5)

- Configuration roadmap:
 - Configure scheduled update of the antivirus signature database to minimize the possibility of false positives or negatives.
 - Set basic network parameters for the firewall, including configuring interface IP addresses and adding interfaces to security zones.
 - Configure two antivirus profiles, one for defining matching conditions and actions for the HTTP and POP3 protocols and the other for the FTP protocol.
 - Create security policies, and apply antivirus profiles in the direction from the Trust to the Untrust zone and from DMZ to the Untrust zone, respectively.



- The update service of the antivirus signature database is controlled by the antivirus license control item. If the license control item is not activated, the device does not automatically load the preset signature database, and the signature database cannot be manually loaded or updated. After the license control item is activated, the signature database can be loaded and updated . After the license control item expires, the signature database cannot be manually loaded or updated, and the antivirus function is available. However, the signature database may not be up-to-date, and virus detection and defense capabilities are limited.

Example for Configuring Antivirus (3/5)

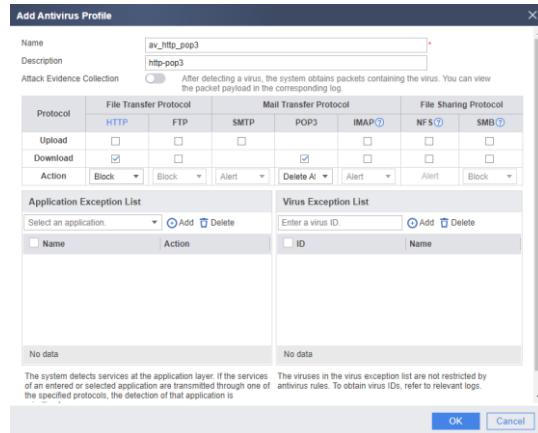
- Choose Object > Security Profiles > Antivirus to create an antivirus profile.

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes links for Dashboard, Monitor, Policy, Object (which is highlighted with a red box), Network, and System. The left sidebar lists various object types: Certificates, Address, Region, Service, Application, User, Device, Authentication Server, IP Address Pool, Schedule, Tag, URL Category, DNS Category, Keyword Group, MIME Header Group, Email Address Group, Signature, and Security Profiles. Under Security Profiles, there are three options: Content Security Configuration Wizard, Antivirus (which is highlighted with a red box), and Intrusion Prevention. The main content area is titled "Antivirus Profile List" and contains a table with one row for the "default" profile. The table columns are Name, Description, Attack Evidence Collection, and Protocol. The "default" row has a checkmark in the Name column and a note below it stating "This is the default profile for antivirus,c...". The "Protocol" column lists HTTP, FTP, SMTP, POP3, IMAP, NFS, and SMB.

Name	Description	Attack Evidence Collection	Protocol
default	This is the default profile for antivirus,c...		HTTP FTP SMTP POP3 IMAP NFS SMB

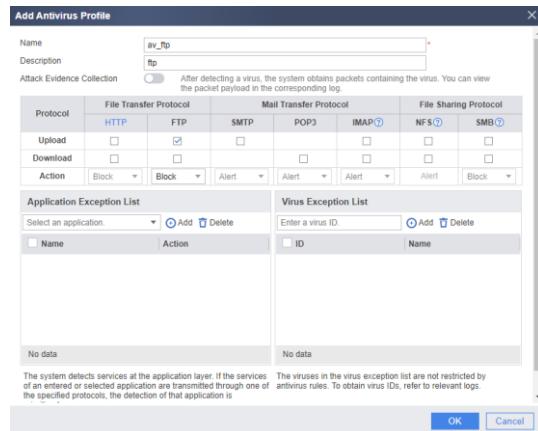
Example for Configuring Antivirus (4/5)

- Click **Add** and set parameters for the HTTP and POP3 protocols, as shown in the following figure.



Example for Configuring Antivirus (5/5)

- Repeat the preceding steps to set parameters for the FTP protocol, as shown in the following figure.



Quiz

1. (Multiple-choice question) Which of the following actions can be configured as the antivirus actions for SMTP? ()
 - A. Block
 - B. Alert
 - C. Declare
 - D. Delete attachment
2. (Single-answer question) Which of the following statements about antivirus characteristics is false? ()
 - A. The antivirus feature is not under license control.
 - B. In quick scan mode, antivirus only checks PE files by default.
 - C. The antivirus feature can detect RAR files.
 - D. The antivirus function on the firewall and the antivirus software on a host are mutually complementary.

1. CD
2. A

Summary

- This course describes the basic concepts of intrusion and virus, and typical intrusion behaviors. It also introduces the technical fundamentals and detection and block process of intrusion prevention and antivirus, as well as intrusion prevention and antivirus configurations on firewalls.
- After learning this course, you can have a better understanding of deployment scenarios of intrusion prevention. With the practice based on the actual environment, you can independently configure intrusion prevention on Huawei firewalls and master how to deploy firewalls in the intrusion prevention scenario.

Recommendations

- Huawei official websites
 - Enterprise services: <http://enterprise.huawei.com/en/>
 - Technical support: <http://support.huawei.com/enterprise/>
 - Online learning: <http://learning.huawei.com/en/>

Acronyms and Abbreviations



Acronym and Abbreviation	Full Name
BIOS	Basic Input Output System
CGI	Common Gateway Interface
CNCERT/CC	National Computer Network Emergency Response Technical Team Coordination Center of China
ID	Intrusion Detection
IDS	Intrusion Detection System
IMAP	Internet Message Access Protocol
NFS	Network File System
POP3	Post Office Protocol-Version 3
SMB	Server Message Block

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
portfolio, new technology, 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 User Management Technologies



Foreword

- Information security incidents occur frequently, and most of these incidents are caused by misoperations or weak security awareness of internal users and administrators. Improper permission management enlarges the impact scope of security incidents and worsens system damage.
- On an enterprise network, users access network resources. To ensure network resource security, users must be properly authenticated and authorized.
- User management technologies enable administrators to control users' access to network resources. User management is one of the most basic security management requirements for all networks.

Objectives

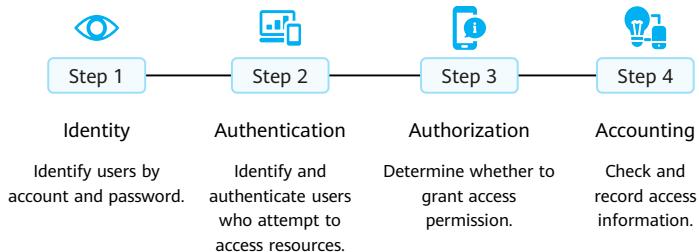
- On completion of this course, you will be able to:
 - Understand AAA principles.
 - Describe user authentication technologies.
 - Configure user authentication.

Contents

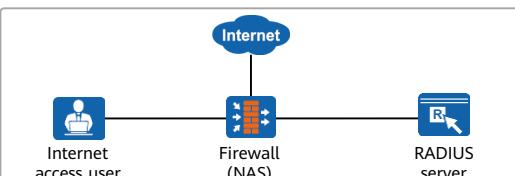
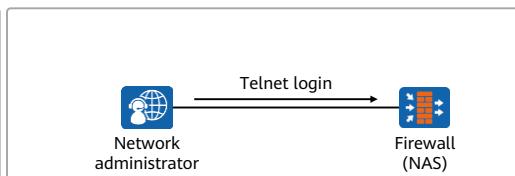
- 1. AAA Principles**
2. Firewall User Authentication and Application

AAA Overview

- 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.

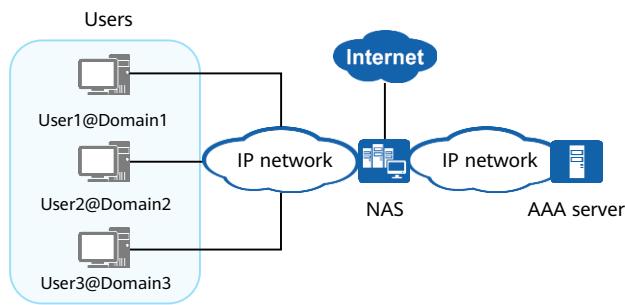


Common AAA Application Scenarios

User Internet access management through the RADIUS server	Network administrator permission control through local authentication
 <ul style="list-style-type: none">AAA schemes are configured on the NAS to implement interworking between the NAS and RADIUS server.After the user enters a user name and a password on the client, the NAS sends the user name and password to the RADIUS server for authentication.If the authentication succeeds, the user is granted the Internet access permission.The RADIUS server records the user's network resource usage during Internet access.	 <ul style="list-style-type: none">After local AAA schemes are configured on the firewall, the firewall compares the user name and password of the network administrator with the locally configured user name and password when the network administrator logs in to the firewall.After the authentication succeeds, the firewall grants certain administrator permissions to the network administrator.

Basic AAA Architecture

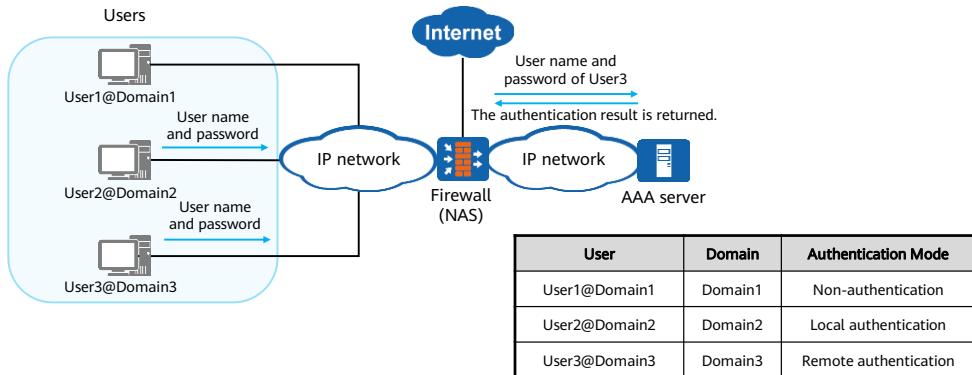
- The basic AAA architecture consists of the user, NAS, and AAA server.
 - The NAS collects and manages user access requests in a centralized manner. Common NAS devices on the live network include switches and firewalls.
 - The AAA server manages user information in a centralized manner.



- The NAS manages users based on domains. Each domain can be configured with different authentication, authorization, and accounting schemes to perform AAA on users in the domain.
 - Each user belongs to a specific domain. The domain to which a user belongs is determined by the character string following the at sign (@) in the user name. For example, if the user name is User1@Domain1, the user belongs to Domain1. If a user name does not contain the at sign (@), the user belongs to the default domain.
 - Multiple domains are created on the NAS to manage users. Different domains can be associated with different AAA schemes. When receiving a network access request from a user, the NAS determines the domain to which the user belongs based on the user name and controls user access based on the AAA schemes associated with the domain.

Authentication

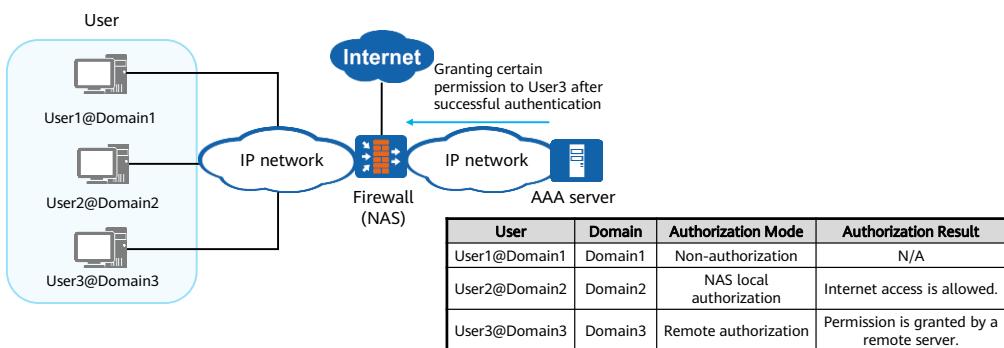
- Firewalls support three authentication modes: non-authentication, local authentication, and remote authentication.



- Firewalls support the following authentication modes:
 - Non-authentication:** Firewalls trust users and do not verify the user identity. For security purposes, this authentication mode is seldom used.
 - Local authentication:** Local user information (including the user name, password, and attributes) is configured on the NAS. In this case, the NAS functions as an AAA server. Local authentication is fast, reducing operating expense (OPEX). However, information storage capacity is limited by hardware. This authentication mode is typically used to manage users who log in to the device through Telnet or FTP.
 - Remote authentication:** User information (including the user name, password, and attributes) is configured on an authentication server. Firewalls support remote authentication through RADIUS. The NAS functions as a client to communicate with the RADIUS server.

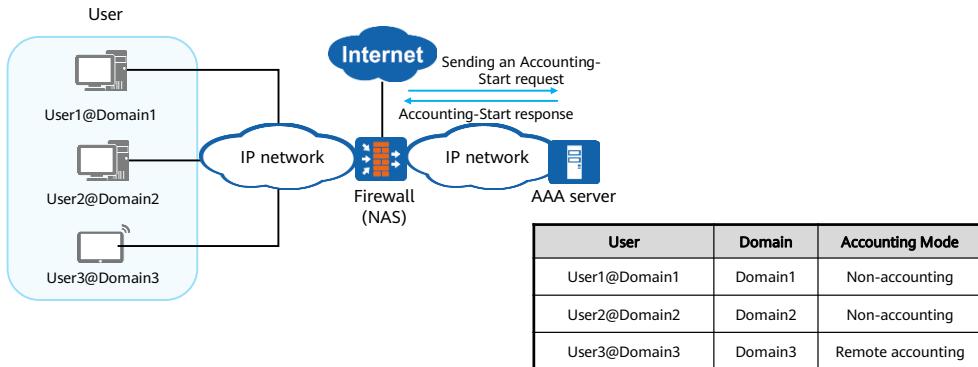
Authorization

- Authorization limits the services available to a user, such as public services and sensitive services.
- Firewalls support three authorization modes: non-authorization, local authorization, and remote authorization. The authorization content includes the user group, VLAN, and ACL.



Accounting

- Firewalls support two accounting modes: non-accounting and remote accounting.
- The accounting function monitors the network behavior and network resource usage of authorized users.



- The accounting function involves the following:
 - How long users stay online
 - How much money users spend
 - What operations users perform

Common AAA Solutions

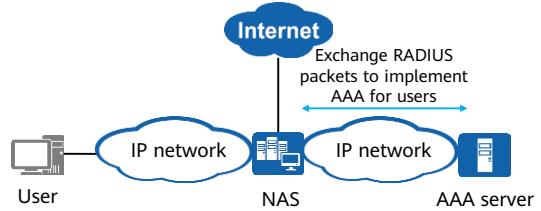
- Currently, Huawei devices can use RADIUS, HWTACACS, LDAP, and AD to implement AAA. RADIUS is most commonly used in actual applications.

Technical Solution	Interaction Protocol	Authentication	Authorization	Accounting
RADIUS	UDP	✓	✓	✓
HWTACACS	TCP	✓	✓	✓
LDAP	TCP	✓	✓	✗
AD	TCP	✓	✓	✗
Local authentication and authorization	/	✓	✓	✗

- 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, operates over TCP, and uses TCP port 49. The authentication, authorization, and accounting services provided by HWTACACS are independent of each other and can be implemented on different servers. HWTACACS applies to users accessing the Internet through Point-to-Point Protocol (PPP) or Virtual Private Dial-up Network (VPDN) and for administrators logging in to devices.
- In LDAP authentication, an LDAP client sends user passwords in plaintext to an LDAP server, which poses security risks. The Kerberos protocol provides a symmetrical key mechanism to improve password transmission security. Therefore, integrating the Kerberos protocol into LDAP authentication can prevent password leak during LDAP authentication. The authentication method integrating Kerberos and LDAP is called AD authentication.

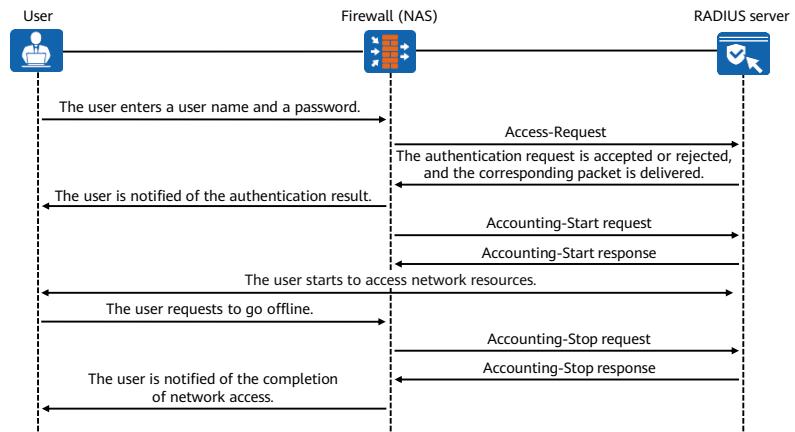
RADIUS Overview

- AAA can be implemented using different protocols. RADIUS is most frequently used in actual scenarios.
- RADIUS is a distributed information exchange protocol using the client/server model. It protects a network against unauthorized access and is often used on networks that require high security and control remote user access.
- RADIUS defines the UDP-based RADIUS packet format and transmission mechanism, and specifies UDP ports 1812 and 1813 as the default authentication and accounting ports respectively.
- RADIUS has the following characteristics:
 - Client/Server model
 - Secure message exchange mechanism
 - High scalability



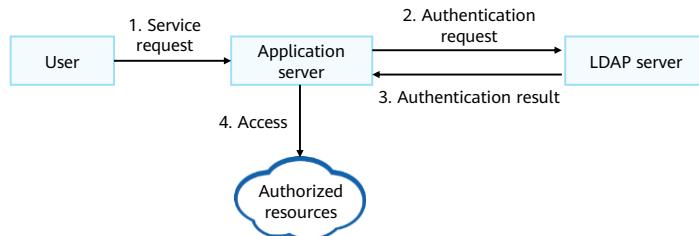
- RADIUS sometimes uses ports 1645 and 1646 as the default authentication port and accounting port respectively.

RADIUS Authentication Process



LDAP Overview

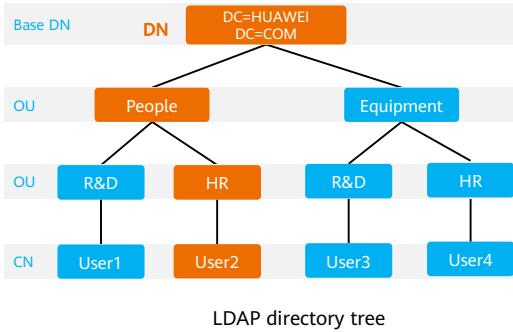
- Lightweight Directory Access Protocol (LDAP) uses the client/server architecture.
- The LDAP server authenticates user requests from the application server and specifies the range of resources available to users.
- LDAP defines multiple operations, for example, the bind and search operations for user authentication and authorization.



- Application scenario: A network access device connects to an LDAP server and uses LDAP bind and search operations to implement user authentication and authorization.

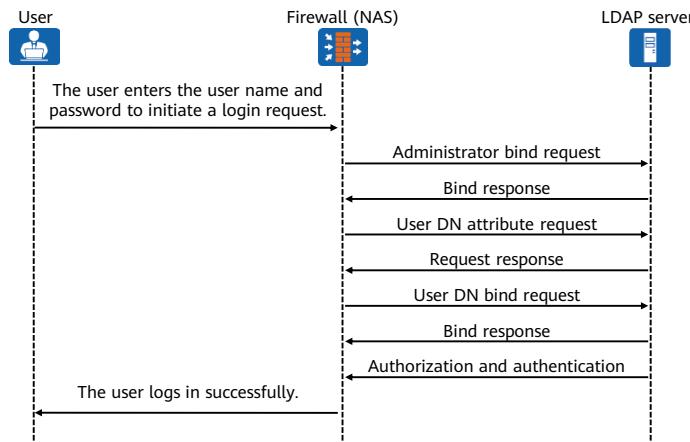
LDAP Directory

- A directory is a set of information with similar attributes that are organized in a logical and hierarchical manner. In LDAP, the directory consists of entries that are organized in a tree structure. An entry is a collection of attributes that have distinguished names (DNs). 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.
- Distinguished Name (DN): indicates the location of an object. It starts from the object, to its upper layers, until the root DN. For example, the DN of User2 is **CN=User2, OU=HR, OU=People, DC=HUAWEI, DC=COM**.
- Base DN: indicates the root DN.
- Organization Unit (OU): indicates the organization to which an object belongs.

LDAP Authentication Process



16 Huawei Confidential



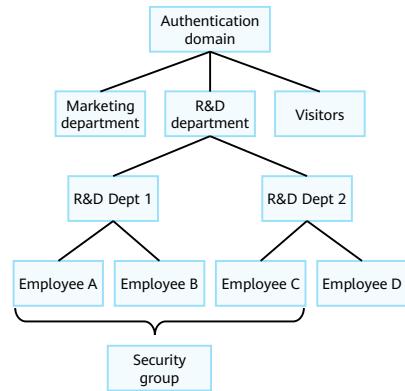
- The authentication process is as follows:
 - The user enters the user name and password to initiate a login request. The firewall establishes a TCP connection with the LDAP server.
 - The firewall sends a bind request carrying the administrator's DN and password to the LDAP server in order to obtain the search permission.
 - After the binding is successful, the LDAP server sends a bind response to the firewall.
 - The firewall sends a user DN search request carrying the entered user name to the LDAP server.
 - The LDAP server searches for the user DN. If the search is successful, the LDAP server sends a search response packet.
 - The firewall sends a user DN bind request 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 to the firewall.
 - After the authorization is successful, the firewall notifies the user that the login is successful.

Contents

1. AAA Principles
2. Firewall User Authentication and Application
 - User Organizational Structure and Classification
 - User Authentication Process
 - User Authentication Policies
 - User Authentication Configuration

User Organizational Structure and Management

- Users are network access subjects and basic units for network behavior control and network permission assignment by firewalls. The user organizational structure involves the following concepts:
 - Authentication domain: a container of the user organizational structure. The firewall provides a default authentication domain (default) and supports the creation of authentication domains as required.
 - User group/User: Users are organized in a tree structure and belong to groups (departments). An administrator can create departments and users based on the enterprise organizational structure.
 - Security group: a cross-department group in the horizontal organizational structure. The administrator can create cross-department security groups to manage users in a dimension other than by department. For example, the administrator can create a cross-department group in an enterprise.
- The system has a default authentication domain. Each user group can contain multiple users and user groups. Each user group can belong to only one parent user group. Each user must belong to at least one user group and can belong to multiple user groups.



- Authentication domain
 - Authentication domains are important in the authentication process. Their configurations determine users' authentication modes and organizational structure.
 - Authentication domains have different functions for users with different authentication modes.
- The firewall identifies the authentication domains contained in user names and assigns users who require authentication to the corresponding authentication domains. The firewall then authenticates the users based on the authentication domain configurations.
- To implement differentiated management and assign different permissions to different users or departments, you need to plan and manage the organizational structure. The firewall provides an organizational structure tree that resembles common administrative structure and therefore facilitates planning and management.
- Each user or user group can be referenced by security policies, traffic limiting policies, and authentication policies to implement user-specific permission and bandwidth control.
- If an administrator uses the default authentication domain to authenticate a user, the user needs only to enter the user name for login. If the administrator uses a newly created authentication domain to authenticate a user, the user needs to enter user name@authentication domain name for login.

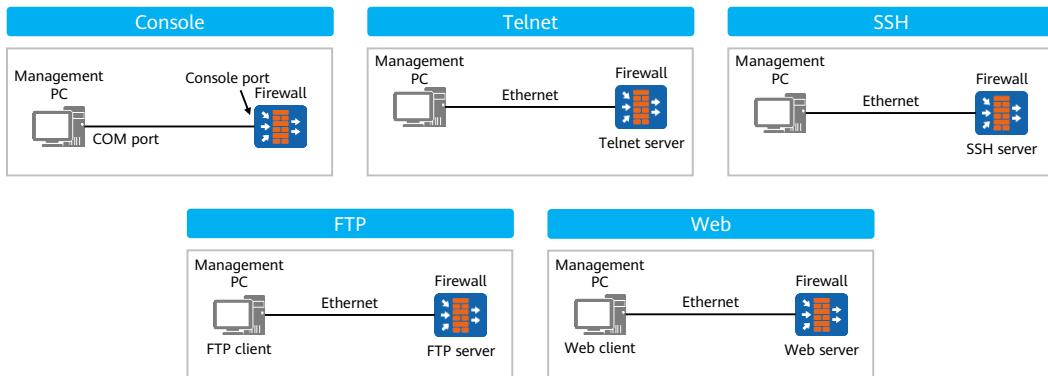
User Categories

- Administrator
 - Administrator: An administrator is a user who accesses the device through Telnet, SSH, web, FTP, or the console port and configures or performs operations on the device.
- Internet access user
 - An Internet access user is the entity for network access and also a basic unit for network permission management.
 - The device performs identity authentication on a user who accesses the network to obtain the user identity and implements policy control based on the user identity.
- Access user
 - An access user is an entity that accesses network resources on an external network, for example, an employee in an enterprise branch or on a business trip.
 - An access user first access the firewall through SSL VPN, L2TP VPN, IPsec VPN, or PPPoE before accessing network resources at the headquarters.

Contents

1. AAA Principles
2. **Firewall User Authentication and Application**
 - User Organization Structure and Classification
 - **User Authentication Process**
 - User Authentication Policy
 - User Authentication Configuration

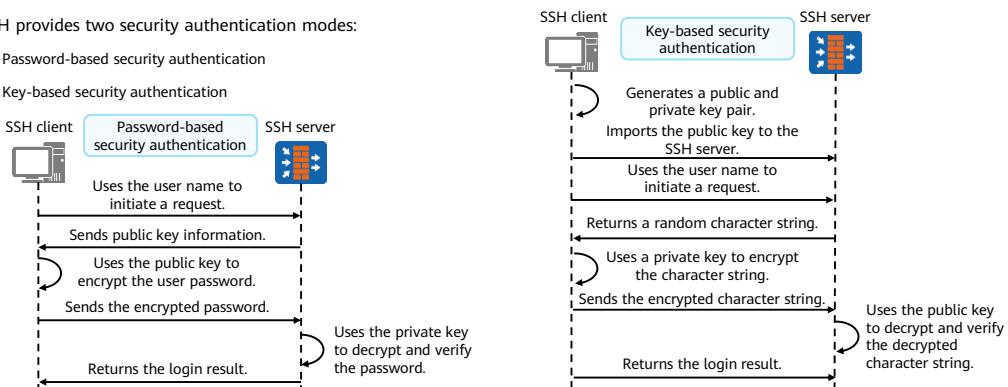
Administrator Authentication Login Modes



- To manage, configure, and maintain devices, an administrator can log in to a device using the following methods:
 - Through the console port: The console port allows the administrator to manage the device through the CLI. It is used when the device is configured for the first time or the configuration file of the device is lost. If the device fails to start, you can diagnose the fault or enter the BootROM to upgrade the system through the console port.
 - Through the web system: Terminals log in to the device through HTTP or HTTPS for remote configuration and management.
 - Using Telnet: Telnet is a traditional login mode, which is used to configure and manage the device through the CLI.
 - Using FTP: The FTP administrator uploads and downloads files in the storage space of the device.
 - Using SSH: SSH enhances information security and provides powerful authentication functions. It provides a secure channel on an insecure network. In this case, the device functions as an SSH server.

Administrator Authentication Mode - SSH

- The Secure Shell (SSH) protocol is a security protocol based on the application layer. It prevents data from being transmitted in plaintext. SSH is a highly reliable protocol that secures remote login sessions and other network services. It can effectively prevent information disclosure during remote management.
- SSH provides two security authentication modes:
 - >Password-based security authentication
 - Key-based security authentication

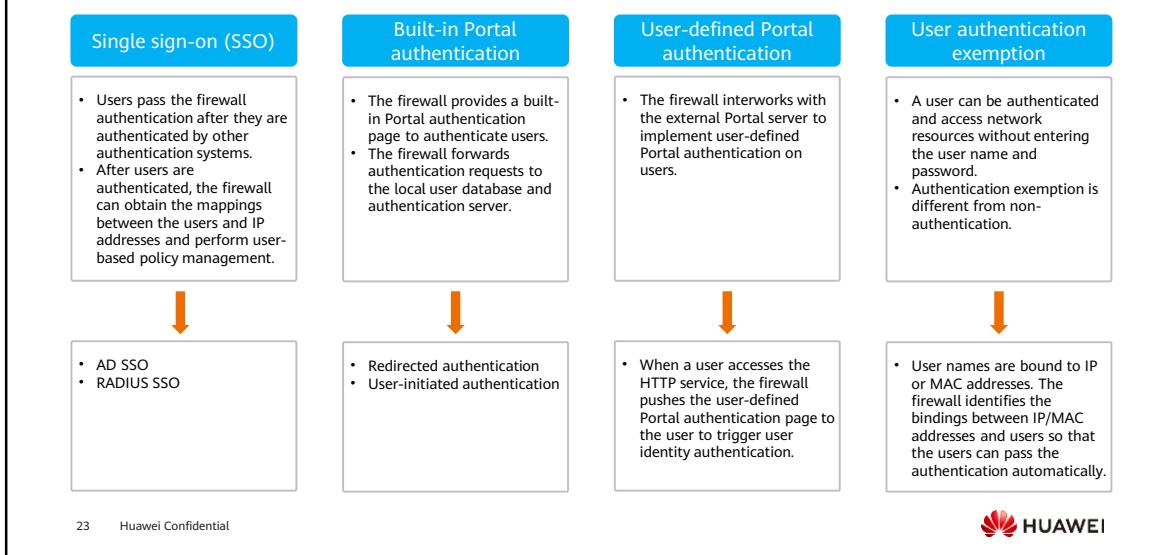


22 Huawei Confidential



- In short, SSH is a network protocol used for encrypted login between computers. If a user uses SSH to log in to a remote computer from a local computer, the login is secure. Even if the login is intercepted, the password will not be disclosed.
- The process for logging in to a remote host in SSH password-based security authentication mode is as follows:
 - A user initiates a login request.
 - The remote host returns its public key to the requesting host.
 - The requesting host uses the public key to encrypt the password entered by the user.
 - The requesting host sends the encrypted password to the remote host.
 - The remote host uses the private key to decrypt the password.
 - Finally, the remote host checks whether the decrypted password is the same as the user password. If so, the login is successful.
- The process for logging in to a remote host in SSH key-based security authentication mode is as follows:
 - A user host generates a key pair and imports the public key to the remote host.
 - The user initiates a login request.
 - The remote host returns a random character string to the user.
 - The host where the user is located uses the private key to encrypt the random character string and returns the encrypted random string to the remote host.
 - The remote host uses the imported public key to decrypt the encrypted random character string. If the decryption is successful, the user login information is correct and the login is allowed.

Authentication Modes of Internet Access Users



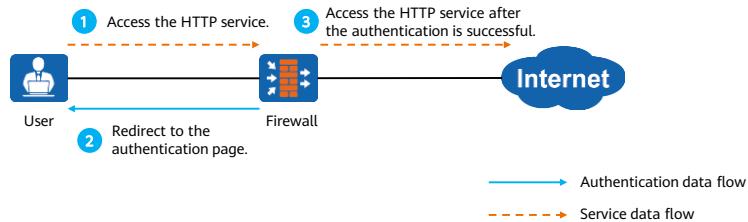
23 Huawei Confidential



- SSO: This mode applies to scenarios where the authentication system has been deployed before the user authentication function is deployed on the firewall.
- Built-in Portal authentication: This mode applies to scenarios where the firewall authenticates users.
- User-defined Portal authentication: Two types of user-defined Portal authentication are available. For details, see user-defined Portal authentication.
- User authentication exemption: Users do not need to enter the user name and password, but the firewall can obtain the bindings between users and IP addresses to implement user management.
- The following describes the authentication process for Internet access users using built-in Portal authentication.

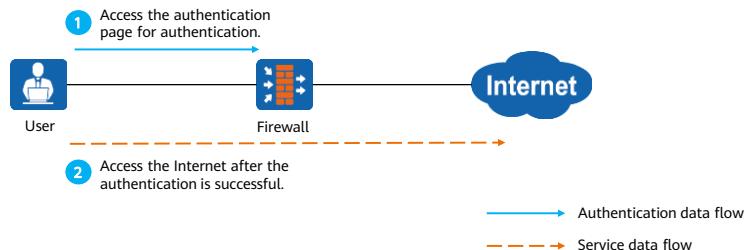
Built-in Portal Authentication - Redirected Authentication

- In redirected authentication, users do not initiate identity authentication. Instead, they access the HTTP service first and are authenticated during the access. Service access is allowed only after authentication is successful.
- When the firewall receives the first HTTP service access data flow from the user, it redirects the HTTP request to the authentication page to trigger identity authentication. If the authentication is successful, the user can access the HTTP service and other services.



Built-in Portal Authentication - User-initiated Authentication

- In user-initiated authentication, a user initiates identity authentication and can access network resources only after being authenticated successfully.
- The user initiates an authentication request to the authentication page provided by the firewall. After receiving the authentication request, the firewall authenticates the user. If the authentication is successful, the user can access the Internet.



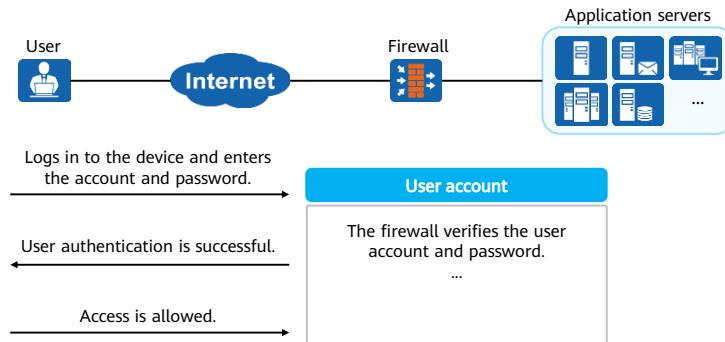
Access User Authentication Modes

- Access user authentication refers to the authentication of various VPN access users.

SSL VPN	L2TP VPN	IPsec VPN	PPPoE
<ul style="list-style-type: none">• A user logs in to the authentication page provided by the SSL VPN module to trigger authentication. After the authentication is complete, the SSL VPN access user can access network resources at the headquarters.• SSL VPN is a new lightweight remote access solution. Mobile office users do not need to install the SSL VPN client.	<ul style="list-style-type: none">• Layer 2 Tunneling Protocol (L2TP) VPN is a tunneling technology that is mainly used in remote office scenarios to provide intranet resource access services for traveling employees.• It can provide remote access services for traveling employees, regardless of whether they access the Internet through dial-up or Ethernet.	<ul style="list-style-type: none">• IPsec is a set of open network security protocols. It is a suite of protocols and services that provide security for IP networks, including the Authentication Header (AH) and Encapsulating Security Payload (ESP) protocols, key exchange, authentication, and encryption algorithms.• Through these protocols, an IPsec tunnel is established between two devices. Data is then forwarded through the IPsec tunnel to ensure secure transmission.	<ul style="list-style-type: none">• PPP over Ethernet (PPPoE) is a link layer protocol that encapsulates PPP frames into Ethernet frames. PPPoE enables multiple hosts on an Ethernet to connect to a broadband remote access server (BRAS).

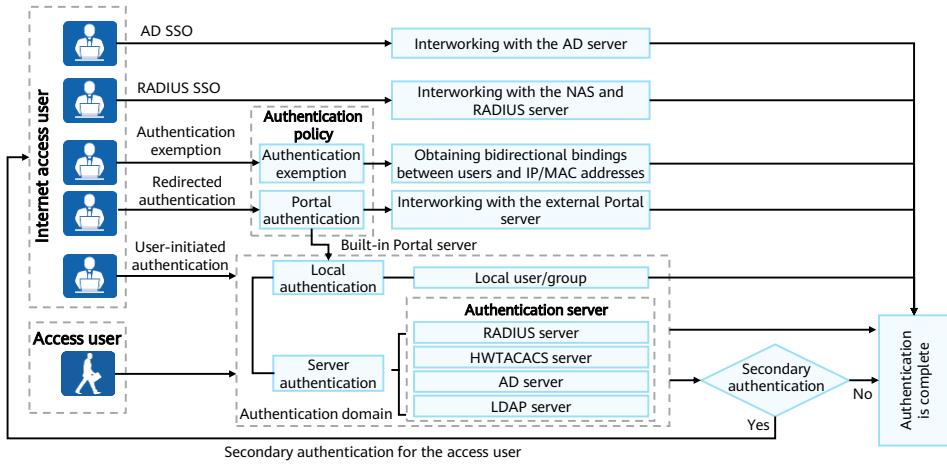
SSL VPN

- A user connects to the firewall through SSL VPN from the Internet to access intranet resources.



- The Secure Sockets Layer (SSL) VPN, as a VPN technology based on HTTPS, works between the transport layer and the application layer to provide confidentiality over the Internet. It provides web proxy, network extension, file sharing, and port forwarding services.
- The SSL handshake process is as follows:
 - The SSL client initiates a connection to the SSL server and requests the server to authenticate itself.
 - The server sends its own digital certificate to prove its identity.
 - The server sends a request to verify the client certificate.
 - After the authentication is successful, the server and client negotiate the message encryption algorithm for encryption and the hash function for integrity check. In most cases, the client provides a list of all supported encryption algorithms, and the server selects the most powerful one.
 - The client and server generate a session key after performing the following operations:
 - The client generates a random number, encrypts it using the public key of the server (obtained from the server certificate), and sends it to the server.
 - The server responds with random data (the client key is used if the client key is available; otherwise, the data is sent in plaintext).
 - A key is generated from the random data using the hash function.
- As shown in the preceding figure, an enterprise has deployed a firewall as the VPN access gateway at the network border to connect the intranet to the Internet. A traveling employee accesses the firewall through SSL VPN and uses the network extension service to access network resources.

Authentication Process Summary



Contents

1. AAA Principles
2. **Firewall User Authentication and Application**
 - User Organization Structure and Classification
 - User Authentication Process
 - **User Authentication Policy**
 - User Authentication Configuration

Authentication Policy

- An authentication policy determines which data flows need to be authenticated by a firewall. Data flows that match an authentication policy can pass through the firewall only after identity authentication is successful. By default, the firewall authenticates only the data flows that match authentication policies and does not authenticate the data flows passing through itself. If the traffic passing through the firewall matches an authentication policy, the following actions are triggered:
 - Redirected authentication: When a user accesses the HTTP service and the access data flow matches an authentication policy, the firewall pushes the authentication page to the user for authentication.
 - User-initiated authentication: To access non-HTTP services, a user needs to proactively access the authentication page for authentication. Otherwise, the firewall denies the service data flows that match an authentication policy.
 - Authentication exemption: If a user matches an authentication exemption policy when accessing services, the user can access network resources without entering the user name and password. The firewall identifies users based on the bindings between users and IP/MAC addresses.
 - SSO: The login of SSO users is not under the control of authentication policies. Policy control can be implemented only when user service traffic matches an authentication policy.

- The following types of traffic do not trigger authentication even if they match an authentication policy:
 - Traffic originated from or destined for a device
 - DHCP, BGP, OSPF, and LDP packets
 - The DNS packets of the first HTTP service data flow that triggers authentication are not controlled by an authentication policy. After a user is authenticated and logs in, the DNS packets are controlled by the authentication policy.

Composition of an Authentication Policy

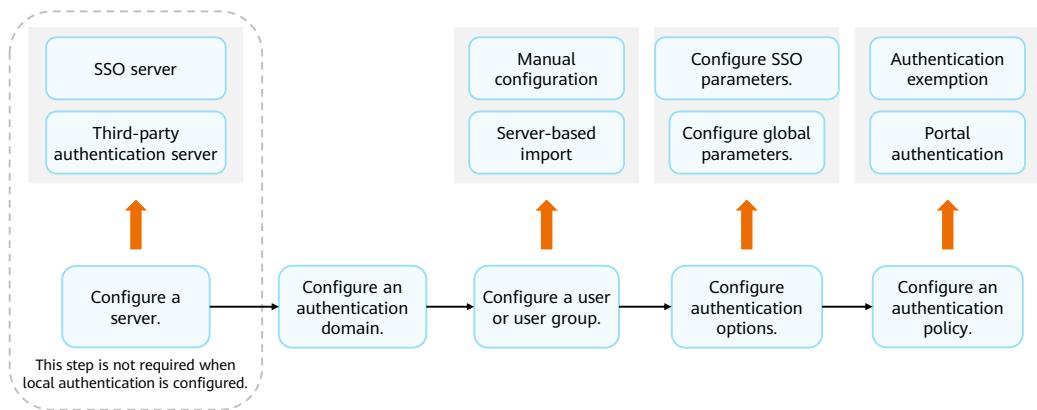
- An authentication policy is a set of rules. An authentication rule consists of conditions and an action. Conditions are used to match packets, including:
 - Source/Destination security zone
 - Source address/region
 - Destination address/region
- An action indicates how a firewall processes packets that match conditions:
 - Portal authentication
 - SMS authentication
 - Authentication exemption
 - Non-authentication

- Portal authentication is performed on data flows that meet conditions.
- SMS authentication is performed on data flows that meet conditions, and users need to enter the SMS verification code.
- Authentication exemption is performed on data flows that meet conditions. A firewall uses other methods to identify users. Authentication exemption applies to the following scenarios:
 - For top executives of enterprises, they want to access confidential data, which proposes higher security requirements. Additionally, they want to skip the authentication process. To meet these requirements, the administrator can bind top executives to IP or MAC addresses and configure the firewall not to implement authentication on the data flows of top executives when they access network resources using the specified IP or MAC addresses. The firewall identifies the users to which data flows belong based on the bindings between the users and IP or MAC addresses.
 - In an AD or RADIUS SSO scenario, the firewall has obtained user information from another authentication system and therefore exempts SSO users from authentication.
- Non-authentication: Data flows that meet conditions are not authenticated. This mode applies to the following scenarios:
 - Data flows do not need to be authenticated by the firewall, for example, data flows are transmitted between intranets.
 - In an AD or RADIUS SSO scenario, if data flows between a user to be authenticated and the authentication server passes through a firewall, the firewall does not authenticate the data flows.
- The firewall has a default authentication policy, in which all match conditions are any and the action is non-authentication.

Contents

1. AAA Principles
2. **Firewall User Authentication and Application**
 - User Organization Structure and Classification
 - User Authentication Process
 - User Authentication Policy
 - User Authentication Configuration

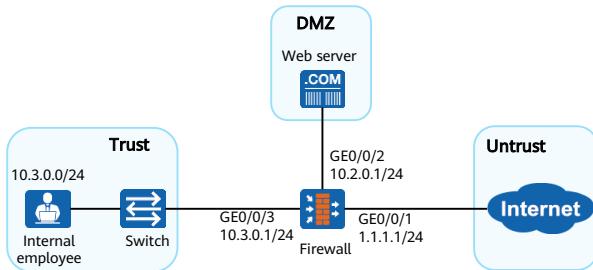
Internet Access User Authentication - Configuration Process



- Configure a user or user group: Before the device performs user-specific and user group-specific management, you must create a user or user group first. The device supports the manual configuration, local import, and server-based import of users and user groups.
- Manually configure users or user groups:
 - There is a default authentication domain on the firewall by default. You can create users or user groups in the default authentication domain. If you need to plan the organizational structure of another authentication domain, configure the authentication domain first.
 - This step is mandatory when you need to create user groups based on the enterprise's organizational structure and to manage network permission assignment based on user groups.
 - To perform local password authentication, create a local user and configure the local password.
- Local import:
 - You can import a CSV file to the device.
- Server import:
 - Third-party authentication servers are widely used on networks. Many enterprises select authentication servers to store information about all users and user groups. Through server-based import, you can import user information on authentication servers in batches to the device.
- Configuring authentication options involves configuring global parameters, SSO, and customized authentication pages.

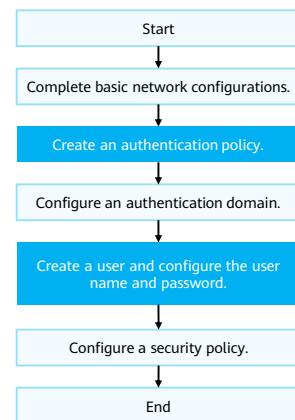
Example for Configuring Internet Access User Authentication (1)

- Requirements:
 - An enterprise deploys a firewall at the network border as an egress gateway to connect the intranet and Internet. Employees on the intranet dynamically obtain IP addresses. These employees must be successfully authenticated by the firewall before accessing network resources.
 - When an employee uses a browser to access a web page, the firewall redirects the browser to the authentication page. After the authentication is successful, the browser automatically switches to the web page that the user needs to access.



Example for Configuring Internet Access User Authentication (2)

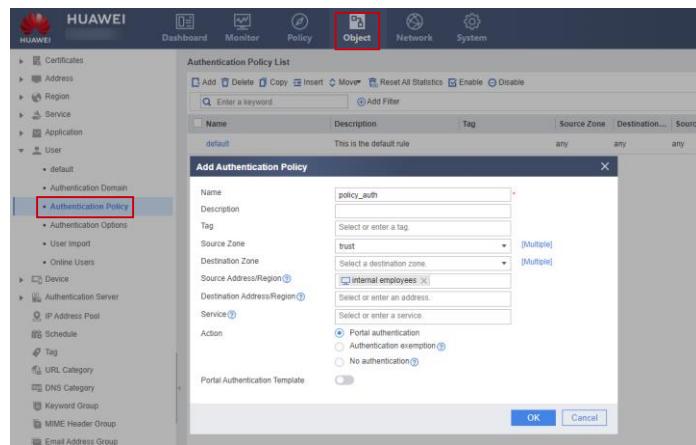
- Configuration roadmap:
 - Complete basic network configurations, including configuring IP addresses for interfaces of the firewall, adding interfaces to security zones, and configuring default routes.
 - Create an authentication policy and set match conditions and the authentication action.
 - Configure an authentication domain. Set Scenario to Online Behavior Management and User Location to Local.
 - Create a user group, user name, and password in the local domain for internal employee authentication.
 - Configure a security policy to allow authenticated employees to access the authentication page and access the Internet.



- The security policy configured in the configuration process allows visitors to access the authentication page. The configuration is for your reference.

Example for Configuring Internet Access User Authentication (3)

- Choose Object > User > Authentication Policy > Create to create an authentication policy.



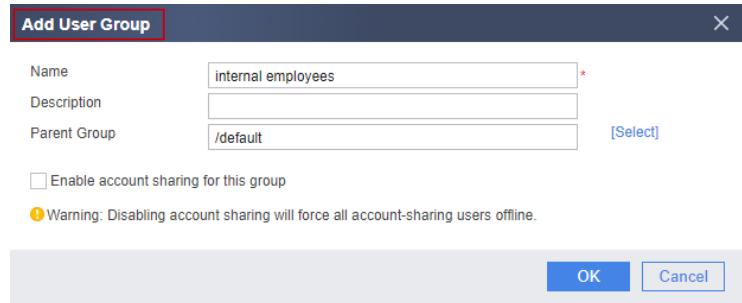
Example for Configuring Internet Access User Authentication (4)

- Choose **Object > User > default** to configure local authentication.

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes links for Dashboard, Monitor, Policy, Object (which is highlighted with a red box), Network, and System. The left sidebar menu lists various objects: Certificates, Address, Region, Service, Application, and User. Under the User section, 'default' is selected and highlighted with a red box. The main content area is titled 'User Management' and contains two tabs: 'Authentication Mode and Policy Settings' and 'User Configuration'. In the 'Authentication Mode and Policy Settings' tab, the 'Internet Access Authentication Mode' is set to 'Portal authentication'. In the 'User Configuration' tab, 'User Location' is set to 'Local' (with a checked checkbox). Below these tabs is a table titled 'User/User Group/Security Group Management List' with columns for Name, Description, and User Group. The table contains three entries: 'auth_exemption' (User Group: /default), 'normal' (User Group: /default), and 'user01' (User Group: /default/normal).

Example for Configuring Internet Access User Authentication (5)

- Choose **Object > User > default > Create** to create a user group.



Example for Configuring Internet Access User Authentication (6)

- Choose **Object > User > default > Create** to create a user.

Add User

User Name	<input type="text" value="zhangsan"/> *
Display Name	<input type="text"/>
Description	<input type="text"/>
User Group	<input type="text" value="/default/internal employees"/> [Select]
Security Group	<input type="text"/> [Select]
Password	<input type="password"/> *
The password must be a string of 6 to 16 characters containing at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters. The password cannot be the same as the user name.	
Confirm Password	<input type="password"/> *
<input type="checkbox"/> User Attributes	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Quiz

1. (Single-Answer Question) Which of the following is not included in AAA? ()
 - A. Authentication
 - B. Authorization
 - C. Accounting
 - D. Management

1. D

Summary

- This course describes the user management architecture, user authentication scheme, authentication process, user types, and user authentication configuration.
- Upon completion of this course, you will understand user types and user authentication protocols, independently complete user management configurations on Huawei firewalls, and know how to deploy firewalls in authentication scenarios.

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 (1)

Acronym/Abbreviation	Full Name
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AD	Active Directory
AH	Authentication Header
BGP	Border Gateway Protocol
CN	Common Name
COM	Cluster Communication Port
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
DN	Distinguished Name

Acronyms and Abbreviations (2)

Acronym/Abbreviation	Full Name
ESP	Encapsulated Security Payload
HWTACACS	Huawei Terminal Access Controller Access Control System
LDAP	Lightweight Directory Access Protocol
LDP	Label Distribution Protocol
NAS	Network Access Server
OU	Organization Unit
RADIUS	Remote Authentication Dial In User Service
VLAN	Virtual Local Area Network
VPDN	Virtual Private Dial-up 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
portfolio, new technology, 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.



Fundamentals of Encryption and Decryption Technologies



Foreword

- The Internet connects the whole world, which is benefiting countless enterprises. However, the initial design of the TCP/IP protocol suite does not focus on security issues. As a result, there are many insecure factors when file transfer, email, and a lot more other data is transmitted on the Internet. Using encryption algorithms to encrypt data is a common method to improve data communication security.
- This course describes the development of encryption and decryption, as well as the working principles and processes of common algorithms such as symmetric encryption algorithms, asymmetric encryption and decryption algorithms, and hash algorithms.

Objectives

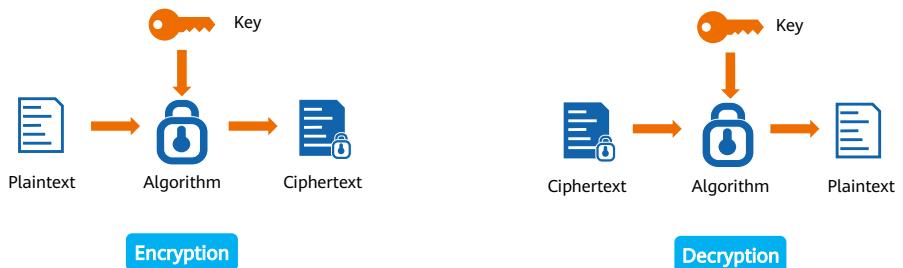
- On completion of this course, you will be able to know well about:
 - Development of encryption and decryption technologies
 - Processes of various encryption and decryption methods
 - Principles of encryption and decryption algorithms

Contents

- 1. Encryption/Decryption Technology Development**
2. Encryption/Decryption Technology Fundamentals
3. Common Encryption/Decryption Algorithms
4. Hash Algorithms

Encryption/Decryption Definition

- The basic process of data encryption is to process plaintext files or data using a certain algorithm so that the files or data becomes unreadable code, which is usually called ciphertext. In this way, data is protected from being stolen or read by unauthorized personnel.
- Data decryption is a process of decrypting ciphertext into plaintext by using a corresponding algorithm and key.



Encryption Background

Major considerations for using encryption technologies

- Comply with information security regulations and requirements.
- Protect enterprises' intellectual property rights.
- Protect information from risks.
- Protect customer information.
- Limit the liabilities for breach of contract or improper disclosure.
- Reduce the scope of compliance review.
- Comply with the company's internal policies.
- Prevent data from being disclosed after a data breach.
- ...

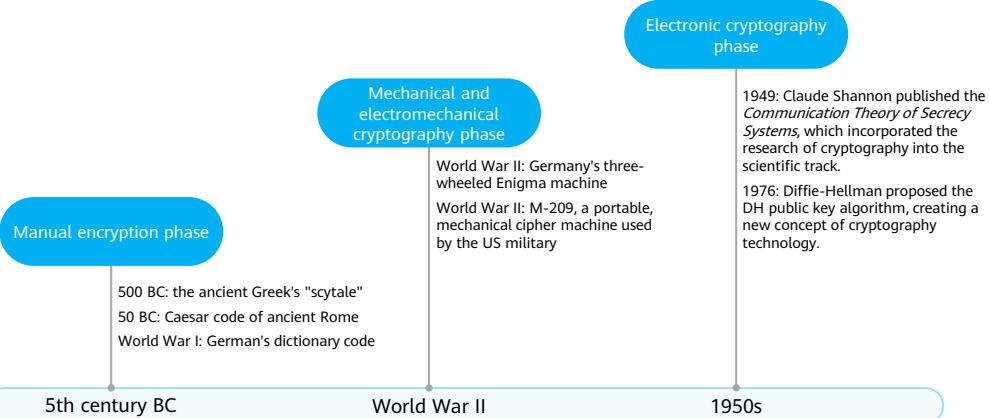
Encryption Purposes

- Encryption guarantees the confidentiality, integrity, identifiability, and non-repudiation of information.

Confidentiality	Integrity	Identifiability	Non-repudiation
<ul style="list-style-type: none">• Realized through data encryption• Allows only some users to access and read the information, making the information incomprehensible to unauthorized users.	<ul style="list-style-type: none">• Realized through data encryption, hash algorithm, or digital signature• Ensures that data is not modified without authorization during storage and transmission.	<ul style="list-style-type: none">• Realized through data encryption, hash algorithm, or digital signature• Provides services related to data and identification, that is, authenticating the identities of the sender and recipient of data.	<ul style="list-style-type: none">• Realized through symmetric/asymmetric encryption and digital signature with the assistance of a trusted registration authority (RA) or certificate authority (CA)• Provides non-repudiation services that prevent users from denying previous comments or behaviors.

- Encryption is the process of making information only readable to certain receivers and incomprehensible to other users. It achieves this by enabling the original content to be shown only after the correct key is used to decrypt the information.
- It prevents interception and theft of private information over networks.
Encryption guarantees the confidentiality, integrity, identifiability, and non-repudiation of information.

Encryption Technology Development

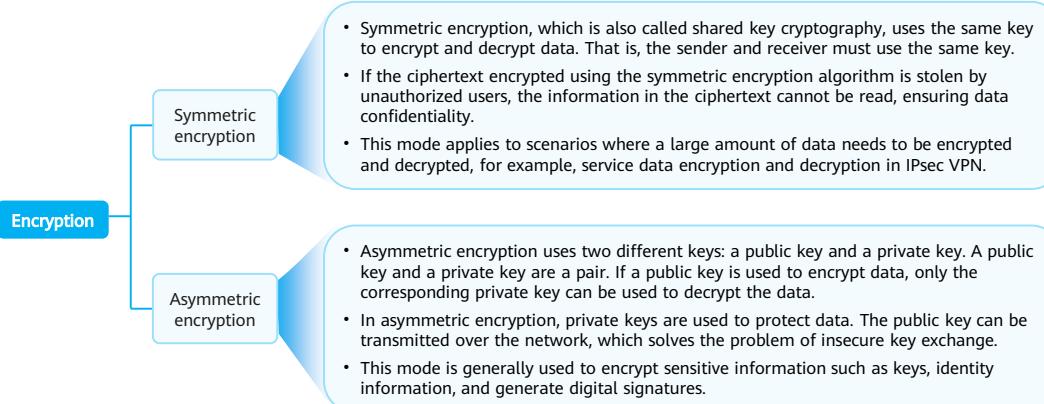


- As a method for information security protection, cryptography is not a modern invention. It dates back to a long time ago, when human beings tried to learn how to communicate while keeping their correspondence confidential. They had to find a way to ensure the confidentiality of their correspondence.
- Ancient Greeks might be the first people to use techniques to encrypt information, which they did prior to the 5th century BC. They used a rod called a scytale, with a piece of parchment wrapped around it, on which a message was written. Then the parchment was sent to the receiver. Anyone who did not know the diameter of the rod, which was the key in this case, could not understand the information on the message.
- In about 50 BC, the Roman emperor Caesar invented a method for encrypting information during times of war, which was later called the Caesar cipher (Caesar code). The principles are that each alphabet in the message is replaced by three places down. For example, after encryption, HuaweiSymantec becomes KxdzhlvBPdqwhf.
- During World War I, Germany wrote codes based on a dictionary. For example, 10-4-2 means the 2nd word in the 4th paragraph on the 10th page of a dictionary.
- In World War II, the most well-known cipher machine was the three-wheeled Enigma machine used by Germans to encrypt information.
- There are two milestones in the electronic cryptography phase:
 - In 1949, Claude Shannon published the *Communication Theory of Secrecy Systems*, which incorporated the research of cryptography into the scientific track.
 - In 1976, Diffie-Hellman proposed the DH public key algorithm, creating a new concept of cryptography technology.

Contents

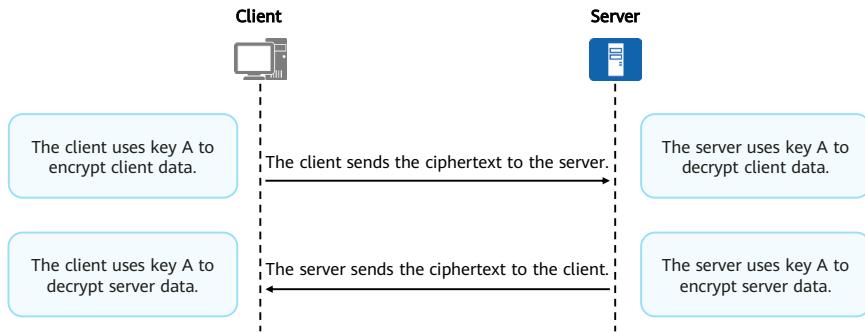
1. Encryption/Decryption Technology Development
2. **Encryption/Decryption Technology Fundamentals**
3. Common Encryption/Decryption Algorithms
4. Hash Algorithms

Classification of Encryption Technologies



Symmetric Encryption Algorithm

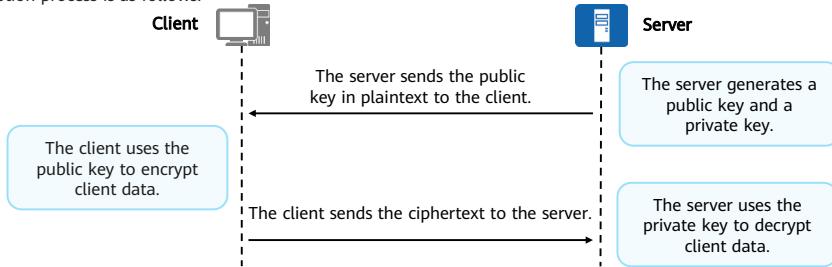
- The symmetric encryption algorithm uses **the same key** for encryption and decryption.
- As shown in the figure, a symmetric encryption algorithm is used for data exchange between the client and server. The client and server negotiate symmetric key A in advance. The encryption and decryption process is as follows:



- If both communication parties have the same key and no one knows the key, the communication security between the two parties can be ensured unless the key is cracked. However, the biggest problem is how the key is known to both communication parties and not to others. When the server generates a key and transmits it to the browser, if the key is hijacked during the transmission, the key can be used to decrypt any content transmitted between the two parties. If the key of website A is pre-stored in the browser and no one except the browser and website A knows the key, symmetric encryption can be used theoretically. In this way, the browser only needs to store the keys of all HTTPS websites in the world. Obviously, it is unrealistic to do so. To solve this problem, asymmetric encryption is required.

Asymmetric Encryption Algorithm

- The asymmetric encryption algorithm requires **a pair of keys**, including a **public key** and a **private key**. The two keys appear in pairs.
- Asymmetric encryption prevents the security risks in the distribution and management of a symmetric key. In an asymmetric key pair, the public key is used to encrypt data and the private key is used to decrypt data. The two communication parties do not need to exchange keys before a secure communication session. The sender uses the public key of the receiver to encrypt the data, and the receiver uses its own private key to decrypt data.
- As shown in the figure, an asymmetric encryption algorithm is used for data exchange between the client and server. The encryption and decryption process is as follows:



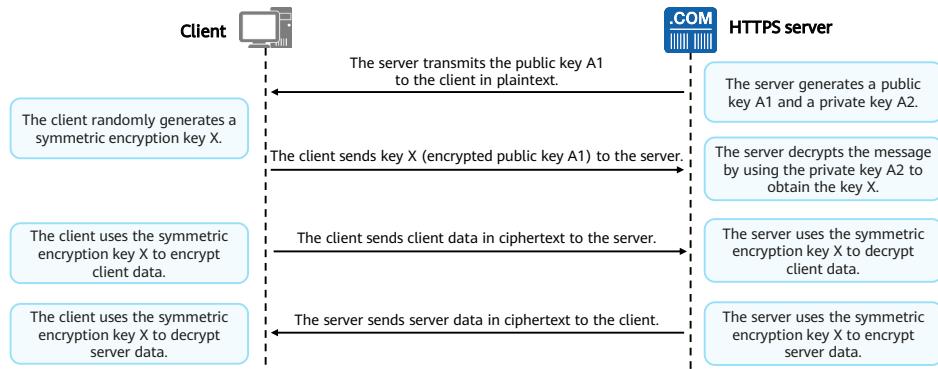
Symmetric Encryption vs. Asymmetric Encryption

Encryption Algorithm	Advantage	Disadvantage	Usage Scenario
Symmetric encryption	High efficiency, simple algorithm, and low system overhead, suitable for encrypting a large amount of data.	The implementation is difficult and the scalability is poor.	Encrypts and decrypts a large amount of data.
Asymmetric encryption	The other key cannot be derived from one key. Information encrypted by the public key can be decrypted only by the private key.	It takes a long time to encrypt a large amount of data, and the encrypted data is too long, consuming much bandwidth.	Encrypts sensitive information, such as keys or identity information.

Question: Can we combine the advantages of the two?

Combination of Asymmetric Encryption and Symmetric Encryption

- The combination of asymmetric encryption and symmetric encryption can reduce the number of asymmetric encryption times. HTTPS uses this solution. Asymmetric encryption is used to exchange the symmetric encryption key, and then the symmetric encryption algorithm is used to encrypt service data. The interaction process is as follows:



Contents

1. Encryption/Decryption Technology Development
2. Encryption/Decryption Technology Fundamentals
- 3. Common Encryption/Decryption Algorithms**
4. Hash Algorithms

Common Symmetric Encryption and Decryption Algorithms

Algorithm	Description
DES	Data Encryption Standard. The DES algorithm divides data into multiple 64-bit blocks at the encryption end and encrypts each block to generate a ciphertext. At the decryption end, the 64-bit ciphertext is converted into a 64-bit plaintext. The blocks are associated with each other. DES uses 16 iterative blocks to complete iteration, in which a 56-bit key is used for encryption and decryption.
3DES	Triple DES.
AES	Advanced Encryption Standard. AES supports multiple variable-length keys, such as 128-bit, 192-bit, 256-bit, and 384-bit keys.
SM1	SM1 has the same encryption strength as AES. This algorithm is not disclosed. You need to invoke the algorithm through the interface of the encryption chip.
SM4	Packet data algorithm based on the WLAN standard. It adopts symmetric encryption with both key and packet lengths of 128 bits.
Other	IDEA, etc.

- DES was developed by the National Institute of Standards and Technology (NIST). DES is the first widely used cryptographic algorithm which uses the same key for encryption and decryption. DES is a symmetric-key block cipher, in which a 64-bit plaintext and a 56-bit key are input to generate a 64-bit ciphertext (data is encrypted to a 64-bit block). The password capacity is 56 bits only, delivering insufficient security. In response, the 3DES algorithm is proposed.
- 3DES uses a 128-bit key. Data is first encrypted using a 56-bit key, then encoded using another 56-bit key, and finally encrypted using the first 56-bit key. In this way, 3DES uses a valid 128-bit key. The greatest advantage of 3DES is that the existing software and hardware can be used, and it can be easily implemented based on DES.
- AES uses a 128-bit block length and supports 128-bit, 192-bit, 256-bit, and 384-bit key lengths. It supports different platforms. A 128-bit key can provide sufficient security and takes less time for processing than longer keys. To date, the AES does not have any serious weakness. DES can still be used due to the production of a large number of fast DES chips. However, AES will gradually replace the DES and 3DES to enhance security and efficiency.
- SM1 and SM4 are commercial cipher block standard symmetric algorithms compiled by China's State Cryptography Administration. The block length and key length are both 128 bits. Therefore, SM1 and SM4 can meet high security requirements.
- International Data Encryption Algorithm (IDEA): The IDEA is a symmetric key block cipher encryption algorithm, with a 64-bit plaintext and a 128-bit key input to generate a 64-bit ciphertext. The IDEA is widely used. For example, SSL includes the IDEA in its encryption algorithm library.

Common Asymmetric Encryption and Decryption Algorithms

Algorithm	Description
DH	The Diffie-Hellman (DH) algorithm is especially important in IPsec and is used to solve the key exchange problem. The same key cannot be used for a long time. To ensure security, the key needs to be dynamically obtained at both ends.
RSA	RSA was named after the initials of its co-founders, Ron Rivest, Adi Shamir and Leonard Adleman. RSA derives its security from the difficulty of factoring large integers that are the product of two large prime numbers. RSA can implement both digital signature and encryption/decryption.
DSA	Digital Signature Algorithm, which is also called Digital Signature Standard (DSS). DSA can implement only digital signatures and cannot be used for encryption or decryption.

- The asymmetric encryption algorithm has two functions:
 - A pair of public and private keys is automatically generated based on the algorithm.
 - Exchange data based on the asymmetric encryption algorithm.
- Common asymmetric encryption algorithms include DH, RSA, and DSA.
 - The DH algorithm is usually used by the two parties involved to negotiate a symmetric encryption key (same key used for encryption and decryption). In essence, the two parties share some parameters and generate their respective keys, which are the same key according to mathematical principles. This key is not transmitted over links, but the parameters exchanged may be transmitted over links.
 - The RSA algorithm is named after Ron Rivest, Adi Shamir, and Leonard Adleman, who jointly developed it at the Massachusetts Institute of Technology (MIT) in 1977. RSA is currently the most influential public key encryption algorithm. It can resist all known password attacks and has been recommended by ISO as the public key data encryption standard. In addition, it is the first algorithm that can be used for both encryption and digital signature.
 - DSA plays an important role in ensuring data integrity and non-repudiation. DSA is based on discrete logarithms in finite fields and delivers the same level of security as RSA. In DSA digital signature and authentication, the sender uses his/her own private key to sign the file or message. After receiving the message, the receiver uses the public key of the sender to verify the authenticity of the signature. DSA is only an algorithm. In contrast to RSA, DSA cannot be used for encryption, decryption, or key exchange. It is used only for signature and is much faster than RSA in this regard.

Contents

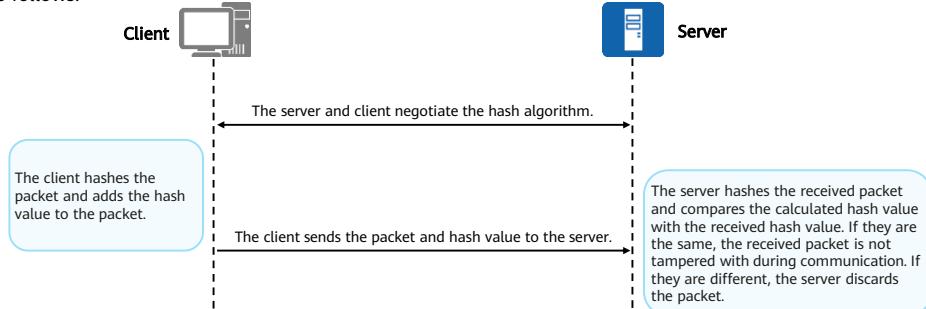
1. Encryption/Decryption Technology Development
2. Encryption/Decryption Technology Fundamentals
3. Common Encryption/Decryption Algorithms
- 4. Hash Algorithms**

Hash Algorithm Overview

- During communication, encryption technologies are used to ensure data confidentiality. However, for users who have high security requirements, data encryption is not enough because data can still be cracked and modified without authorization. The hash algorithm can be used to check whether data is tampered with during communication, thereby implementing data integrity check.
- The hash algorithm uses data of any length as the input and obtains an output value of a fixed length. The output value is a hash value, which is a data compression mapping relationship. Simply put, it is a function that converts a message of any length into a message digest of a fixed length. The hash algorithm is forward fast, irreversible, input sensitive, and anti-collision.
 - Forward fast: The hash value is calculated within limited time and resources based on the given plaintext and hash algorithm.
 - Irreversible: It is difficult to deduce the plaintext in a limited time based on the given any hash value.
 - Input sensitive: If the input data is slightly modified, the output hash value changes obviously.
 - Anti-collision: The output hash values of different input data cannot be the same. For a given data block, it is extremely difficult to find a data block that has a same hash value as the data block.

Hash Algorithm Application

- During data communication, the sender hashes the packet and sends the packet and hash value to the receiver. The receiver uses the same algorithm to hash the packet and compares the two hash values to determine whether the packet has been tampered with during communication. In this way, integrity check is implemented.
- As shown in the figure, the client exchanges data with the server using the hash algorithm. The interaction process is as follows:



Common Hash Algorithms

Algorithm	Description
MD5	Message Digest Algorithm 5. It is a one-way cryptographic hash algorithm developed by RSA Data Security, Inc. It features high stability, fast computing speed, fixed output length, irreversible computing, and high discreteness.
SHA	Secure Hash Algorithm. It can generate a 160-bit character string based on data of any length.
SM3	SM3 is a commercial cryptographic algorithm compiled by China's State Cryptography Administration. It is used to verify the digital signature, generate and verify message authentication codes, and generate random numbers. It can meet the security requirements of multiple password applications.
Other	HMAC, etc.

- MD5 is a hash function widely used in the computer security field to protect the integrity of messages. It calculates data as another fixed-length value.
- SHA is a hash algorithm developed by NIST. Like MD5, SHA can be used as the digital signature algorithm (DSA) defined in the digital signature standard (DSS).
 - SHA-0: is the earliest algorithm defined by NIST. It is soon withdrawn after being released and replaced by SHA-1.
 - SHA-1: The data block can generate a 160-bit message digest using the SHA-1 algorithm. SHA-1 is slower but more secure than MD5. Because its signature is long, it has more powerful anti-collision capability and can discover the shared key more effectively.
 - SHA-2: is a more advanced version of SHA-1. SHA-2 has a longer key than SHA-1 and is therefore much more secure. SHA-2 includes SHA2-256, SHA2-384, and SHA2-512, with 256-bit, 384-bit, and 512-bit keys respectively.
- SM3 is a Chinese cryptographic algorithm approved by the State Cryptography Administration.
- HMAC: a message authentication code that makes use of a cryptographic key along with a hash function, which is widely used in IPsec and SSL.
- These algorithms each have their own characteristics. MD5 is faster but less secure than SHA-1. SHA-2 and SM3 are much more secure than SHA-1 because they have a larger key length than SHA-1, which increases the difficulty in key cracking.

Quiz

1. (Multiple-Answer Question) Which of the following algorithms are symmetric encryption algorithms? ()
 - A. MD5
 - B. RSA
 - C. DES
 - D. AES

1. CD

Summary

- This course describes the application scenarios of different encryption technologies, concepts of data encryption and decryption, development history of encryption technologies, principles and differences between symmetric and asymmetric encryption technologies, as well as common encryption and decryption algorithms and hash algorithms.
- Upon completion of this course, you are able to know well about encryption technologies.

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
AES	Advanced Encryption Standard
DES	Data Encryption Standard
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
3DES	Triple Data Encryption Standard
HMAC	Hash-based Message Authentication Code
IDEA	International Data Encryption Algorithm
MD5	Message Digest Algorithm 5
RSA	Ron Rivest, Adi Shamir, Leonard Adleman
SHA	Secure Hash Algorithm
SM	Shang Mi (pinyin)

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
portfolio, new technology, 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.



PKI Certificate System



Foreword

- As the network and information technologies develop, e-commerce is widely used and accepted. However, e-commerce has the following problems: The transaction parties cannot verify the identities of each other; data may be eavesdropped and tampered with during transmission, and information security cannot be ensured; no paper receipt is used in transaction, making arbitration difficult.
- To address these problems, public key infrastructure (PKI) uses public keys to implement identity verification, confidentiality, data integrity, and non-repudiation of transactions. Therefore, PKI is widely used in network communication and transactions, especially e-government and e-commerce.
- This course describes the secure data communication process, PKI certificate system architecture, and PKI working mechanism.

Objectives

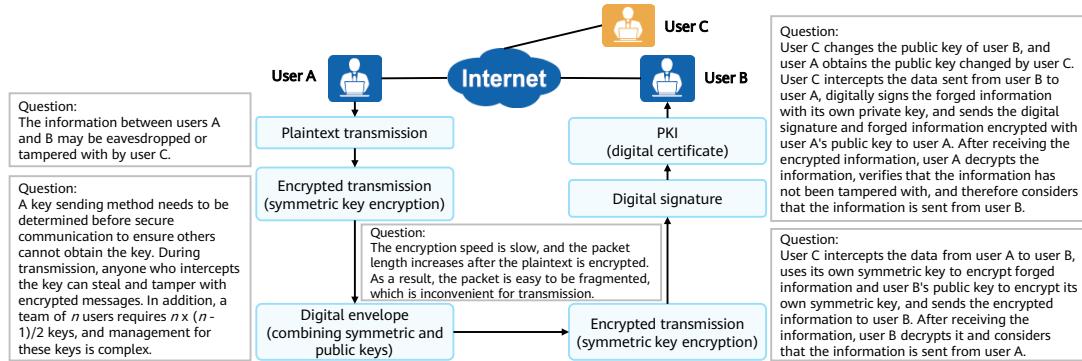
- Upon completion of this course, you will be able to:
 - Describe data communication security technologies.
 - Describe the PKI certificate system architecture.
 - Describe the PKI working mechanism.

Contents

- 1. Data Communication Security Technologies**
2. PKI System Structure
3. PKI Working Mechanism

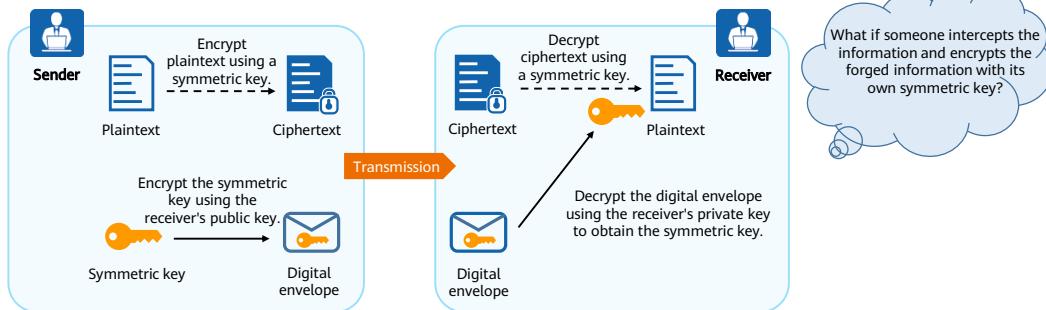
Evolution of Data Communication Security Technologies

- PKI manages the entire lifecycle of digital certificates, including applying for, issuing, and using digital certificates. During the lifecycle, PKI uses the symmetric key encryption, public key encryption, digital envelope, and digital signature technologies.
- The following figure shows the evolution of these technologies. Users A and B communicate through the Internet, and user C is the attacker who targets the communication data between users A and B.



Digital Envelope

- In real life, we can put letters in envelopes so that the contents of the letters will not be snooped by others. In data communications, we can also put communication data in digital envelopes.
- A digital envelope contains the symmetric key encrypted by the sender using the receiver's public key. When receiving a digital envelope, the receiver uses its own private key to decrypt the digital envelope and obtains the symmetric key. The digital envelope encryption and decryption process is as follows:



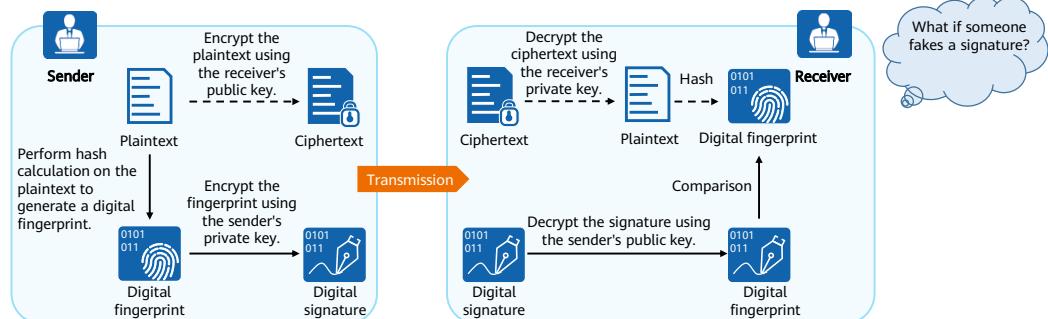
6 Huawei Confidential



- Assume that the sender has obtained the public key of the receiver. The encryption and decryption process is as follows:
 - The sender uses a symmetric key to encrypt the plaintext, generating ciphertext.
 - The sender uses the receiver's public key to encrypt the symmetric key, generating a digital envelope.
 - The sender sends both the digital envelope and ciphertext to the receiver.
 - The receiver uses its own private key to decrypt the digital envelope, obtaining the symmetric key.
 - The receiver uses the symmetric key to decrypt the ciphertext, obtaining the original plaintext.
- The digital envelope has the advantages of both symmetric key encryption and public key encryption. It solves the problem of releasing symmetric keys and speeds up public key encryption, improving key security, scalability, and efficiency.
- However, the following vulnerability should be noted regarding the digital envelope: An attacker may intercept information from the sender, use its own symmetric key to encrypt forged information, use the receiver's public key to encrypt its own symmetric key, and send the information to the receiver. After receiving the encrypted information, the receiver decrypts the information to obtain the plaintext and considers that the information is sent from the sender. To address this problem, the digital signature is used, ensuring that the received information is sent from the correct sender.

Digital Signature

- A digital signature is generated by the sender by encrypting the digital fingerprint using its own private key.
- A digital fingerprint, also called information digest, is calculated by the sender using the hash algorithm based on plaintext information. The sender transmits both the digital fingerprint and plaintext to the receiver, which also performs hash calculation on the plaintext to generate a digital fingerprint. If the two fingerprints match, the receiver determines that the plaintext information has not been tampered with.



7 Huawei Confidential

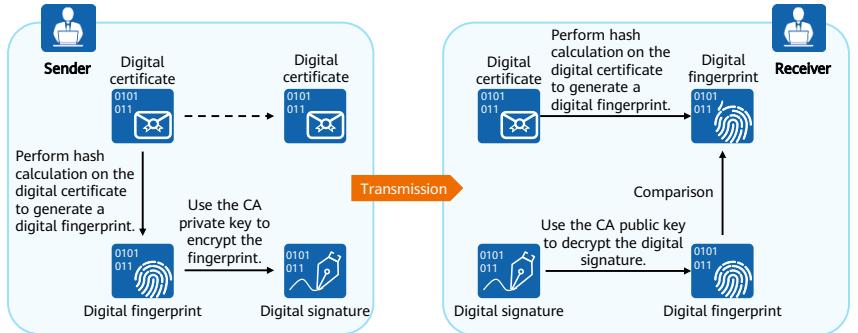


- Assume that the sender has obtained the public key of the receiver. The encryption and decryption process is as follows:
 - The sender uses the receiver's public key to encrypt the plaintext, generating ciphertext.
 - The sender performs hash calculation on the plaintext, generating a digital fingerprint.
 - The sender uses its own private key to encrypt the digital fingerprint, generating a digital signature.
 - The sender sends both the ciphertext and digital signature to the receiver.
 - The receiver uses the sender's public key to decrypt the digital signature, obtaining the digital fingerprint.
 - After receiving the ciphertext from the sender, the receiver uses its own private key to decrypt the information, obtaining the original plaintext.
 - The receiver performs hash calculation on the plaintext, generating a digital fingerprint.
 - The receiver compares the generated digital fingerprint with the obtained digital fingerprint. If they are the same, the receiver accepts the plaintext. If they are different, the receiver discards the plaintext.

- The digital signature proves that information has not been tampered with and verifies the sender's identity. The digital signature and digital envelope can be used together.
- However, the digital signature still has a vulnerability. If the attacker changes the public key of the receiver, the sender obtains the attacker's public key. The attacker can obtain information from the receiver to the sender, digitally sign the forged information using its own private key, and send the digital signature and forged information encrypted using the sender's public key to the sender. After receiving the encrypted information, the sender decrypts the information, verifies that the information has not been tampered with, and therefore considers that the information is sent by the receiver. In this case, a method is required to ensure that a specific public key belongs to a specific owner.

Digital Certificate

- A digital certificate is a digitally signed file issued by a certification authority (CA), containing the owner's public key and identity information. It ensures that one public key is possessed by only one owner.
- The digital certificate is similar to a passport or identity card. People are requested to show their passports when entering foreign countries. Digital certificates serve as the identity on the Internet.



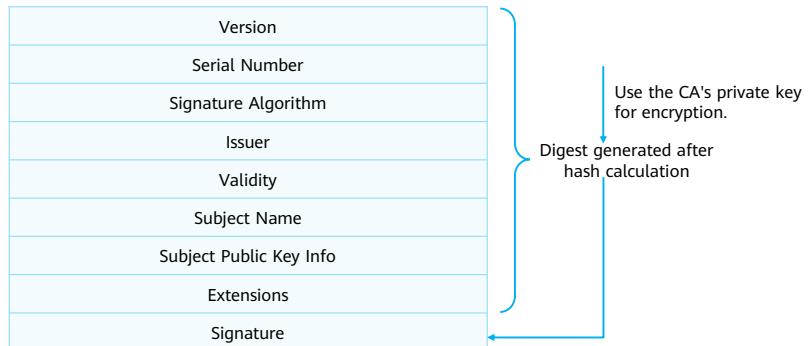
9 Huawei Confidential



- Digital certificate generation: After receiving a digital certificate application and authenticating the applicant's identity, the CA performs hash calculation on the applicant's public key, identity information, and digital certificate validity period (similar to the plaintext used in the digital signature generation process on the previous slide) to generate a digest and uses its private key to encrypt the digest to generate a digital signature. The digital signature and the certificate owner's public key, identity information, and certificate validity period constitute a digital certificate.
- The CA public key is used to decrypt the digest to prove that the certificate is issued by the CA.
- The two digests are compared to check whether the certificate content is modified during transmission. If the public key and identity information in plaintext belong to the CA, the plaintext is self-signed by the CA.
- The digital certificate is initially used to establish the mapping between the public key and the user.
 - The public key is generated randomly and cannot be used to determine the public key owner. To map public keys to users, PKI uses digital certificates to establish the mapping between public keys and users.
 - A digital certificate contains user identity and public key information, which can be used to determine the public key owner.
 - Because a digital certificate does not contain confidential information, the digital certificate can be released publicly.

Digital Certificate Structure

- In its simplest form, a certificate contains a public key, name, and digital signature of a CA.
- In most cases, the certificate also includes information such as the public key validity period, issuer name (CA), and certificate serial number. The certificate structure complies with X.509 v3.



- The fields in the certificate are described as follows:
 - Version: version of X.509. Generally, the v3 (0x2) version is used.
 - Serial Number: a positive and unique integer assigned by the issuer to the certificate. Each certificate is uniquely identified by the issuer name and the serial number.
 - Signature Algorithm: signature algorithm used by the issuer to sign the certificate.
 - Issuer: name of the device that has issued a certificate. It must be the same as the subject name in the issuer's certificate. Generally, the issuer name is the CA server's name.
 - Validity: time interval within which a digital certificate is valid, including the start and end dates. The expired certificates are invalid.
 - Subject Name: name of the entity that possesses a certificate. In a self-signed certificate, the issuer name is the same as the subject name.
 - Subject Public Key Info: public key and the public key algorithm.
 - Extensions: a sequence of optional fields such as certificate usage and CRL distribution point.
 - Signature: signature signed on a certificate by the issuer using a private key.

Classification of Digital Certificates

- There are three types of digital certificates: CA certificate, local certificate, and self-signed certificate.

CA certificate	Local certificate	Self-signed certificate
<ul style="list-style-type: none">• CA's own certificate.• If a PKI system has no hierarchical CA, the CA at the top is the root CA, which holds a self-signed certificate.• If a PKI system has hierarchical CAs, the CA at the top is the root CA, which holds a self-signed certificate.• An applicant trusts a CA by verifying its digital signature. Any applicant can obtain the CA's certificate (including a public key) to verify the local certificate issued by the CA.	<ul style="list-style-type: none">• A certificate issued by a CA to an applicant.• In most cases, a user applies for a local certificate from a CA, and the CA approves the application and issues the certificate to the user.	<ul style="list-style-type: none">• A self-signed certificate is issued by a device to itself and is signed by the CA preset on the device.• An unsigned certificate, as its name implies, is not signed. It is issued by a device to itself. A signature needs to be obtained from the CA, and the certificate issuer is the CA.• A device can generate a self-signed or unsigned certificate for itself, which is a simple certificate issuing function.

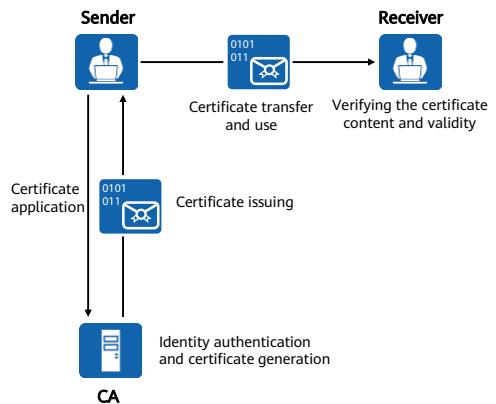
Digital Certificate Formats

- Digital certificates can be saved in three formats.

Format	Description
PKCS#12	Saves certificate files (with or without private keys) in binary format. Common file name extensions are .P12 and .PFX.
DER	Saves certificate files (without private keys) in binary format. Common file name extensions are .DER, .CER, and .CRT.
PEM	Saves certificate files (with or without private keys) in ASCII format. Common file name extensions are .PEM, .CER, and .CRT.

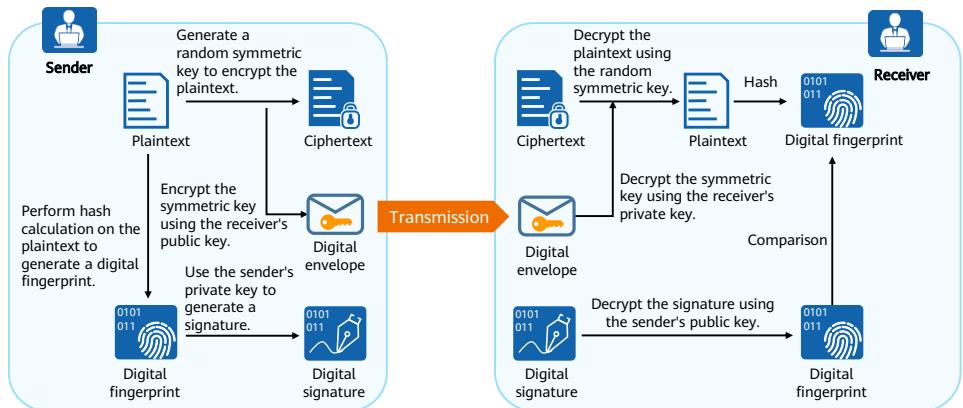
Data Communication Process (1)

- A digital certificate provides an easy way to issue a public key. Users can apply to the CA for authentication to issue their own public keys, as well as verify with the CA to confirm that they have obtained the public key of another user.
- The process of applying for, issuing, and using a digital certificate is as follows:
 - The sender applies for a digital certificate from the CA.
 - The CA authenticates the sender and generates a digital certificate after the authentication succeeds.
 - The CA issues the generated digital certificate to the sender.
 - The receiver downloads the digital certificate of the sender.
 - After receiving the digital certificate, the receiver uses the CA public key to decrypt the digital signature and generates a message digest. Then, the receiver performs hash calculation on the certificate content to generate another message digest, and then compares the two message digests to verify the integrity and authenticity of the certificate content.



Data Communication Process (2)

- The following figure shows the communication process after the two communication parties obtain the public keys and complete identity authentication.



14 Huawei Confidential



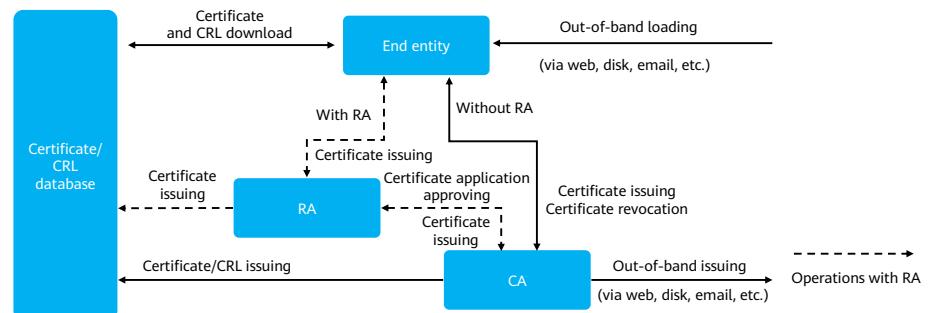
- The processing procedure of the sender is as follows:
 - The sender performs hash calculation on the message plaintext to be transmitted, generates a digital fingerprint, and uses its own private key to generate a digital signature.
 - The sender randomly generates a symmetric key and uses it to encrypt the plaintext, generating a ciphertext.
 - The sender uses the receiver's public key to encrypt the symmetric key.
 - The sender sends the encrypted symmetric key, digital signature, and ciphertext to the receiver.
- The processing procedure of the receiver is as follows:
 - After receiving the message, the receiver uses its own private key to decrypt the symmetric key.
 - The receiver uses the symmetric key to decrypt the ciphertext, obtaining the plaintext.
 - The receiver performs hash calculation on the plaintext to generate a digital fingerprint and uses the sender's public key to decrypt the signature to obtain another digital fingerprint. The receiver then compares the two digital fingerprints. If they are the same, the receiver receives the message. If they are different, the receiver discards the message.
- Asymmetric encryption features high security but low efficiency due to heavy calculation workload. Therefore, symmetric keys are used to encrypt the main communication content. Symmetric keys are randomly generated each time and are discarded after being used to reduce risks.
- The receiver's public key is used to encrypt the symmetric key to ensure that only the receiver can decrypt the ciphertext. The sender's private key is used for signature so that the receiver can check whether the message sender and the message content have been modified. This ensures the integrity and non-repudiation of messages.

Contents

1. Data Communication Security Technologies
- 2. PKI System Structure**
3. PKI Working Mechanism

PKI System Structure

- The PKI uses the public key technology and digital certificates to provide system information security services and verifies the identities of digital certificate owners. The essence of PKI is to standardize asymmetric key management.
- A PKI system consists of the end entity, CA, registration authority (RA), and certificate/certificate revocation list (CRL) database.

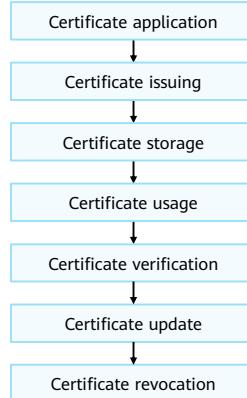


- An end entity, or PKI entity, is the end user of PKI products or services. It can be an individual, an organization, a device (for example, a router or firewall), or process running on a computer.
- A CA is a trusted entity that issues and manages digital certificates. It is an authoritative, trusted, and impartial organization. Generally, a CA is a server.
 - In most cases, a hierarchical CA is used. The CA on the top of the hierarchy is the root CA and the others are subordinate CAs.
 - The root CA is the first CA (trustpoint) in the PKI system. It issues certificates to subordinate CAs, computers, users, and services. In most certificate-based applications, the root CA can be traced through the certificate chain. The root CA holds a self-signed certificate.
 - A subordinate CA can obtain a certificate only from its upper-level CA, which can be the root CA or another subordinate CA authorized by the root CA to issue certificates. The upper-level CA is responsible for issuing and managing certificates of lower-level CAs, and the CAs at the bottom issue certificates to end entities. For example, CA2 and CA3 are subordinate CAs, holding the certificates issued by CA1; CA4, CA5, and CA6 are also subordinate CAs, holding the certificates issued by CA2.
 - When a PKI entity trusts a CA, the trust is extended along the certificate chain, which is a set of certificates from the end entity's certificate to the root certificate. When a PKI entity in communication receives a certificate to be authenticated, it verifies each issuer along the certificate chain.
 - Certificate management is the primary function of CAs, and includes issuing, updating, revoking, querying, and archiving certificates, as well as publishing CRLs.

- An RA enrolls and approves digital certificates. It provides extended applications of certificate issuing and management. The RA processes the certificate enrollment and revocation requests from users, verifies user identities, and decides whether to submit certificate issuing or revocation requests to the CA. The RA is a part of the CA. In actual applications, the RA is usually integrated with the CA. The RA can also be deployed independently to share some functions of the CA. This reduces the workload of the CA and enhances the CA system security.
- A certificate may need to be revoked for reasons such as entity name changing, private key leaking, or service interruptions. Revoking a certificate is to unbind the public key from the PKI entity identity information. The PKI system uses a CRL to revoke certificates. After a certificate is revoked, the CA publishes a CRL to declare that the certificate is invalid and lists the serial numbers of all revoked certificates. The CRL provides a method of verifying certificate validity. The certificate/CRL database stores and manages information about certificates and CRLs, and enables information to be queried. The certificate/CRL database can be built using a Lightweight Directory Access Protocol (LDAP) server, File Transfer Protocol (FTP) server, Hypertext Transfer Protocol (HTTP) server, or database. LDAP simplifies the directory access protocol X.500. It supports TCP/IP and has been widely used in certificate issuing, CRL issuing, and CA policy and information issuing. If the number of certificates is small, the certificates can be stored on an HTTP or FTP server and are allowed to be downloaded.

PKI Certificate Application Process

- PKI manages the entire lifecycle of local certificates, including applying for, issuing, storing, downloading, installing, authenticating, updating, and revoking local certificates.



- Certificate application: also known as certificate enrollment, is a process in which a PKI entity introduces itself to a CA, which then issues it a certificate.
- Certificate issuing: If an RA is available, the RA verifies the PKI entity's identity information when the PKI entity applies for a local certificate from the CA. After the verification, the RA sends the request to the CA. The CA generates a local certificate based on the public key and identity information of the PKI entity, and then sends the local certificate information to the RA. If no RA is available, the CA verifies the PKI entity's identity information.
- Certificate storage: After the CA generates a local certificate, the CA or RA issues the certificate to the certificate/CRL database. Users can download certificates or browse the certificate directory in the database.
- Certificate download: A PKI entity can download a local certificate, a CA/RA certificate, or a local certificate of another PKI entity from the CA server using the SCEP, CMPv2, LDAP, HTTP, or out-of-band mode.
- Certificate installation: In order for a downloaded certificate to take effect, it must be installed on the device (specifically imported to the device memory). The certificate can be a local certificate of the PKI entity, a CA/RA certificate, or a local certificate of another PKI entity. When using SCEP to apply for a certificate, the PKI entity obtains a CA certificate and imports it to the device memory, and then obtains a local certificate and imports it to the device memory.

- Certificate authentication: Before a PKI entity uses a certificate obtained from the peer, for example, for the purposes of setting up a security tunnel or connection with peer, the PKI entity needs to authenticate the local certificate and CA of the peer (specifically, checking whether the certificate is valid and issued by the expected CA). If the certificate of a CA is invalid, the PKI considers all certificates issued by this CA invalid. This seldom occurs because a device updates the CA certificate before expiration in normal cases.
- Certificate update: When a PKI entity's certificate expires or certificate key is disclosed, the PKI entity must replace the certificate. In this case, the PKI entity can apply for a new certificate or use SCEP or CMPv2 to implement automatic certificate update.
- Certificate revocation: In scenarios involving a change of user identity, user information, or public key or involving user service suspension, the PKI entity must revoke the digital certificate, that is, unbind the public key from its own identity information. The CA uses CRL or OCSP to revoke certificates for PKI entities, whereas a PKI entity revokes its own certificate in out-of-band mode.

PKI Certificate Application Process

- The PKI certificate application process is as follows:
 - Submitting an application: A user obtains a digital certificate (root certificate) from the CA, establishes a connection with the security server, generates its own public key and private key, and submits the public key and identity information to the security server. The security server sends the application information to the RA server.
 - Reviewing the application: The RA verifies the identity of the user after receiving the application from the user. If the RA approves the user's certificate request, it digitally signs the certificate request. Otherwise, it does not digitally sign the certificate request.
 - Issuing a certificate: The RA sends the user request and RA signature to the CA. The CA authenticates the RA digital signature. If the authentication succeeds, the CA approves the user request, issues a certificate, and outputs the certificate. If the authentication fails, the CA rejects the certificate request.
 - Forwarding the certificate. After receiving the issued certificate from the CA, the RA sends the certificate to the LDAP server for browsing and notifies the user of the certificate serial number so that the user can download the certificate from the specified website.
 - Obtaining the certificate: The user uses the certificate serial number to download the digital certificate from the specified website. The certificate can be successfully downloaded only when the user's private key matches the public key submitted in the certificate application.



Certificate Application Methods

- A PKI entity can use one of the following methods to apply for a local certificate from CA.

Mode	Description
Simple Certificate Enrollment Protocol (SCEP)	SCEP is mainly used for online application and is an industry standard for PKI certificate application of VPN devices. HTTP is supported by most VPN and CA vendors, providing a simple and powerful certificate application mode for VPN devices (VPN end users).
Certificate Management Protocol version 2 (CMIPv2)	A PKI entity can use CMIPv2 to send a certificate enrollment request to a CA to apply for a local certificate.
File-based	The file-based mode is used for offline certificate application. A PKI entity prints a local certificate enrollment request in PKCS#10 format and saves it in a file. Then the PKI entity sends the file to the CA in out-of-band mode (such as web, disk, or email).

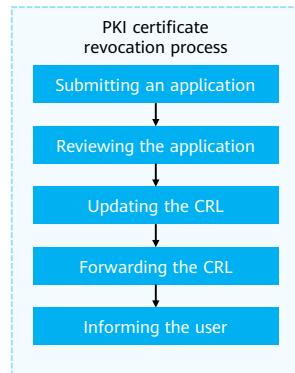
PKI Certificate Verification

- After obtaining a peer certificate, a PKI entity needs to verify the local certificate and CA of the peer before using the certificate. There are three ways to check the certificate status: CRL, OCSP, and None.
 - CRL
 - A PKI entity can download CRLs using the SCEP, HTTP, LDAP, and LDAPv3 template.
 - When a PKI entity authenticates a local certificate, it searches for the CRL in the local memory. If no CRL is available in the local memory, the PKI entity downloads the CRL from the CRL database and installs it in the local memory. If the local certificate of the peer entity is in the CRL, the certificate has been revoked.
 - OCSP
 - In IPsec scenarios, when PKI entities use certificates for IPsec negotiation, the certificate status of the peer entity can be checked in real time using OCSP.
 - OCSP overcomes the following defect of CRL: A PKI entity must frequently download the CRL to keep it up to date. When a PKI entity accesses the OCSP server, it sends a request for obtaining certificate status information. The OCSP server returns a response containing the keyword valid, expired, or unknown.
 - None
 - If no CRL or OCSP server is available to the PKI entity or the PKI entity does not need to check the local certificate status, this mode can be used. In this mode, the PKI entity does not check certificate revocation.

- In OCSP mode, the server returns one of the following responses:
 - Valid: The certificate is not revoked.
 - Expired: The certificate has been revoked.
 - Unknown: The OCSP server cannot determine the certificate status.

PKI Certificate Revocation Process

- The certificate revocation process is as follows:
 - Submitting an application: A user sends a signed and encrypted email to the RA to apply for certificate revocation.
 - Reviewing the application: The RA approves the certificate revocation application and signs the application.
 - Updating the CRL: The CA verifies the RA signature in the certificate revocation request. If the RA signature is correct, the CA accepts the request, updates the CRL, and outputs the CRL.
 - Forwarding the CRL: After receiving the CRL, the RA issues the CRL in multiple modes (including the LDAP server).
 - Informing the user: The user accesses the LDAP server to download or browse the CRL.

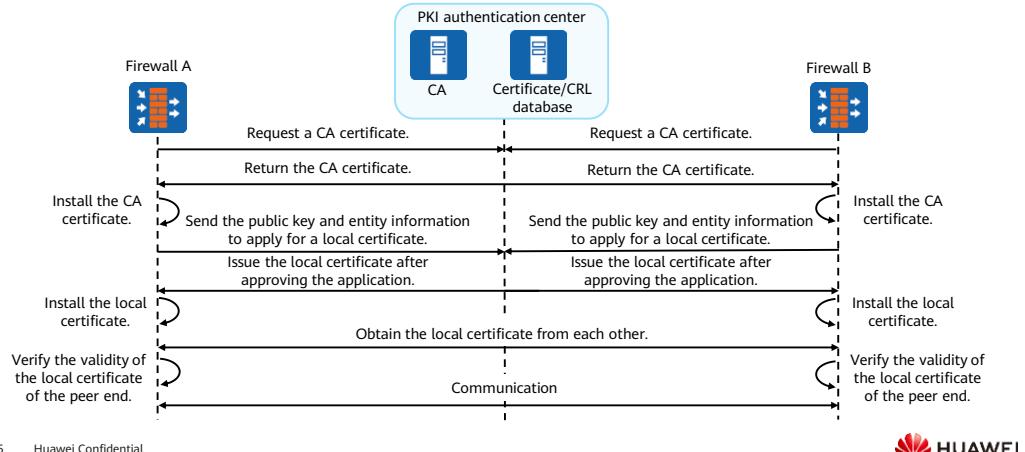


Contents

1. Data Communication Security Technologies
2. PKI System Structure
- 3. PKI Working Mechanism**

PKI Working Mechanism

- On a PKI network, a PKI entity applies for a local certificate from the CA and verifies the certificate validity. The PKI working process is as follows:



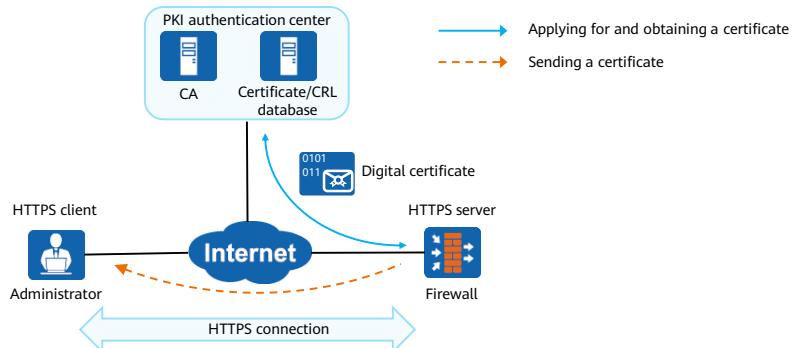
25 Huawei Confidential



- A PKI entity applies for a CA certificate (CA server's certificate) from the CA.
- When receiving the application, the CA sends its own certificate to the PKI entity.
- The PKI entity installs the CA certificate.
 - If the PKI entity uses SCEP for local certificate application, it performs hash calculation on the received CA certificate to generate a digital fingerprint, and compares the generated digital fingerprint with that pre-defined for the CA server. If the two fingerprints are the same, the PKI entity accepts the CA certificate; otherwise, it discards the CA certificate.
- The PKI entity sends a certificate enrollment message (including the public key carried in the configured key pair and PKI entity information) to the CA.
 - If the PKI entity uses SCEP for local certificate application, it encrypts the enrollment message using the CA certificate's public key and digitally signs the message using its own private key. If the CA server requires a challenge password, the enrollment message must contain a challenge password, which must be the same as the CA's challenge password.
 - If the PKI entity uses CMPv2 for local certificate application, it uses an additional identity certificate (local certificate issued by another CA) or message authentication code (MAC) for identity authentication.
 - Additional certificate: The PKI entity uses the CA certificate's public key to encrypt the certificate enrollment message and the additional identity certificate's private key to digitally sign the message.
 - MAC: The PKI entity uses the CA certificate's public key to encrypt the certificate enrollment message, and the message must contain the MAC's reference value and secret value (the values must be the same as those of the CA).

PKI Certificate Application Scenario - Logging In to the Web UI Using HTTPS

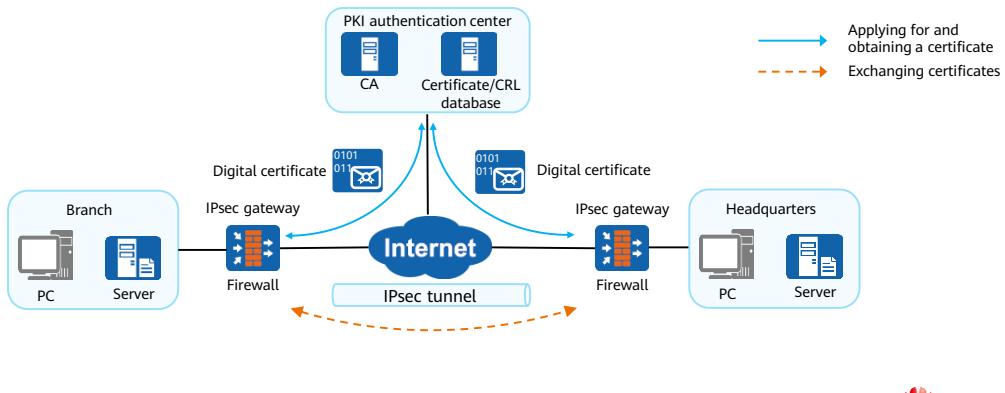
- Specify a local certificate for the HTTPS client on the device. The certificate is issued by a CA trusted by the web browser. Then the web browser can verify the local certificate, avoiding malicious attacks and ensuring secure login.



- During SSL connection setup, the HTTPS client and server interact with each other as follows:
 - The HTTPS server applies for a local certificate from the PKI authentication center.
 - The PKI authentication center issues a local certificate to the HTTPS server.
 - The HTTPS server sends a digital certificate carrying its public key to the HTTPS client.
 - The HTTPS client verifies the local certificate and uses the public key in the certificate to encrypt the key it randomly generates, and sends the encrypted key to the HTTPS server.
 - The HTTPS client and server negotiate the final key and encryption suite, which will be used to encrypt communication data.

PKI Certificate Application Scenario - IPsec VPN

- When PKI certificates are used for identity authentication in IPsec, communicating parties authenticate each other during IKE negotiation, ensuring security of key exchange.



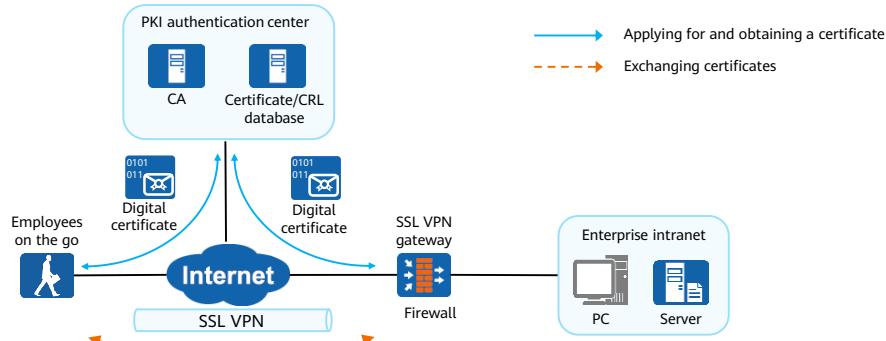
27 Huawei Confidential



- To ensure data security over the Internet, the devices set up IPsec tunnels with the peer ends. Generally, IPsec uses the pre-shared key (PSK) to negotiate IPsec tunnels. However, using a PSK on a large network is not secure in PSK exchange and causes heavy configuration workloads. To address this problem, the devices can use PKI certificates to authenticate each other in IPsec tunnel setup.
- When PKI certificates are used for identity authentication in IPsec, communicating parties authenticate each other during IKE negotiation, ensuring security of key exchange. In addition, the certificates provide a centralized key management function for IPsec and enhance scalability of the entire IPsec network. On an IPsec network using certificate authentication, each device has a local certificate issued by the PKI authentication center. When a new device is deployed, the new device can securely communicate with other devices by applying for a certificate, and the configurations on other devices do not need to be modified. This greatly reduces configuration workload.

PKI Certificate Application Scenario - SSL VPN

- Traveling employees can access the enterprise intranet through SSL VPN. To improve network access security, devices can authenticate users using PKI certificates.



Quiz

1. (Multiple-answer question) Which of the following are the functions of PKI in communication? ()
 - A. PKI ensures the identity of communication entities.
 - B. PKI ensures the confidentiality of communication entities.
 - C. PKI ensures the integrity of communication entities.
 - D. PKI ensures non-repudiation of communication entities.

1. ABCD

Summary

- This course briefly introduces the basic concepts and working principles of the digital envelope, digital signature, and digital certificate. It also systematically introduces the architecture and working mechanism of the PKI system and describes common application scenarios of digital certificates.
- Upon completion of this course, you will have a deep understanding of the PKI system architecture and be able to flexibly use digital certificates.

Recommendations

- Huawei official websites
 - Huawei enterprise website: <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 and Abbreviation	Full Name
CA	Certificate Authority
CMPv2	Certificate Management Protocol version 2
CRL	Certificate Revocation List
EE	End Entity
IKE	Internet Key Exchange
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
RA	Registry Authority
SCEP	Simple Certificate Enrollment 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 portfolio, new technology, 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.



Encryption Technology Applications



Foreword

- Encryption technologies ensure the security of data transmission on the network and protect data from being tampered with and snooped. Signature technologies ensure data integrity and prove the identity of the data sender. PKI certificate authentication technologies verify the validity of public keys and ensure that users access secure and legitimate networks.
- By using these technologies, enterprises can prevent unauthorized users from accessing their enterprise networks. Secure channels can be established between enterprise branches to ensure enterprise data security.

Objectives

- On completion of this course, you will be able to know well about:
 - Application scenarios of encryption technologies
 - Configuration methods for different VPN technologies

Contents

- 1. Application of Cryptography**
2. VPN Overview
3. VPN Configuration

Cryptography Application (1/2)

- In the field of information security, digital envelope, digital signature and digital certificate are mainly used.

Information Security Element	Threat to Be Handled	Cryptographic Technology
Confidentiality	Eavesdropping Sensitive information breach	Digital envelope Symmetric encryption and asymmetric encryption
Integrity	Tampering Sabotage	Digital signature Hash function
Identifiability	Masquerade Spoofing	Digital certificate and digital signature Password and shared secret
Non-repudiation	Denial of information sent Denial of information received	Digital certificate and digital signature Evidence storage
Authorization and access control	Unauthorized access Illegal access to data	Access control Attribute certificate

- Digital envelope: ensures the confidentiality of data in transit using symmetric and asymmetric encryption.
- Digital signature: ensures the integrity of data transmission using hash algorithms.
- Digital certificate: ensures the non-repudiation of data transmission using a third-party certificate authority (CA) to authenticate the public key.

Cryptography Application (2/2)

- Based on actual network application scenarios, digital envelopes, digital signatures, and digital certificates can be used in the following scenarios:
 - VPN: To ensure data confidentiality, many VPN technologies, such as IPsec VPN and SSL VPN, need to use encryption and decryption technologies.
 - IPv6: To prevent device spoofing, secure neighbor discovery (SEND) router authorization can be configured on the device. The digital certificate technology is used for selecting authorized gateway devices.
 - HTTPS login: The administrator can use HTTPS to securely log in to the web UI of the HTTPS server and manage network devices. To improve security of SSL connections, the CA trusted by the web browser is configured to issue local certificates for HTTPS clients. Then the web browser can verify local certificates, avoiding malicious attacks and ensuring secure login.
 - System login authorization: A digest algorithm processes the user password to generate a digest, which is stored and compared with the user-supplied password the next time the user logs in.

- The most important application scenario is VPN.
- This course introduces several encrypted VPN technologies and other common VPN technologies.

Contents

1. Application of Cryptography

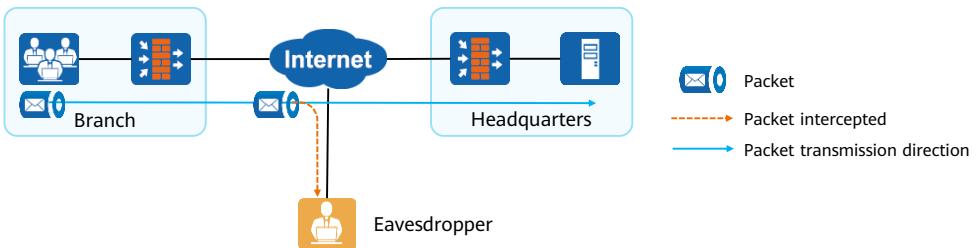
2. VPN Overview

- VPN Overview
 - GRE VPN
 - IPsec VPN
 - L2TP VPN
 - SSL VPN

3. VPN Configuration

Background of VPN

- Without VPN, data transmission on the Internet, which is a shared physical infrastructure, is insecure.
- As shown in the following figure, the headquarters and branch reside in different areas (countries or cities). Employees at the branch access servers at the headquarters over the Internet. Due to various security risks on the Internet, when an employee in a branch sends an access request to the server in the headquarters, the request may be intercepted or tampered with by a hacker. As a result, data may be leaked or important data may be damaged.



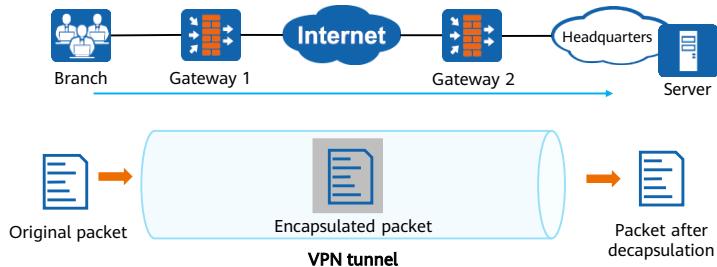
Definition of VPN

- VPN technology is used to construct a private virtual network on a public network and transmit private network traffic on the virtual network. A VPN is a secure and reliable logical network created from a physical network, without changing the network status.
- VPN has the following characteristics:
 - Private: A VPN is a network dedicated to VPN users. For VPN users, a VPN provides the same service experience as a traditional private network. A VPN provides security assurance to protect VPN information against external threats. VPN is independent from its bearer network (generally an IP network) to prevent unauthorized access.
 - Virtual: VPN users communicate with each other over public networks, which are used by non-VPN users at the same time. A VPN is only a logical private network. A public network that carries a VPN is called a VPN backbone network.
- VPNs encapsulate and encrypt data so that the data cannot be cracked even if it is stolen by hackers. This ensures data security. In addition, VPNs do not need to change the existing network topology, and no extra cost is required.

- Compared with traditional private networks, VPNs have the following advantages:
 - Secure: Secure connections are established between the headquarters and teleworkers, branches, partners, or suppliers to ensure confidentiality. This is particularly important for e-commerce and the integration of financial networks and communications networks.
 - Low-cost: VPN uses the shared public network, saving the cost of leasing private lines.
 - Support for mobile services: VPN users can access the headquarters anytime and anywhere.
 - Scalable: VPNs are logical networks and are not affected by the adding or change of physical network nodes.
 - In conclusion, VPNs are secure, reliable, easy to manage, and highly scalable and flexible. Users can enjoy VPN services as long as they have Internet access, regardless of their location.

VPN Encapsulation Principles

- VPN uses tunneling technologies to establish private tunnels on a VPN backbone to secure data transmission.
- Tunneling technologies use one protocol to encapsulate the packets of another protocol (usually IP packets), and can be encapsulated by another protocol, too. A tunnel is a logical link and has the same benefits as a private physical link.



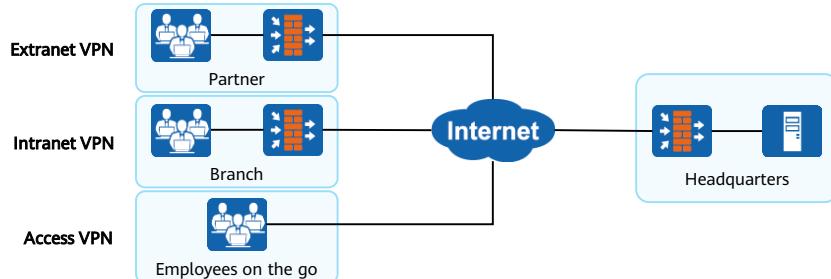
VPN Classification: By Application Scenario

- VPNs are widely used on enterprise networks where branches and employees on business trips connect to the headquarters network. The following describes common VPN classification modes.
- Classified by application scenario:
 - Client-to-site VPN: The client is connected to the intranet through the VPN tunnel. The client can be a firewall, a router, or a personal computer. In this scenario, the following VPN technologies can be used: SSL, IPsec, L2TP, and L2TP over IPsec.
 - Site-to-site VPN: Two LANs are connected through a VPN tunnel. The deployed device is usually a router or firewall. In this scenario, the following VPN technologies can be used: IPsec, L2TP, L2TP over IPsec, GRE over IPsec, and IPsec over GRE.

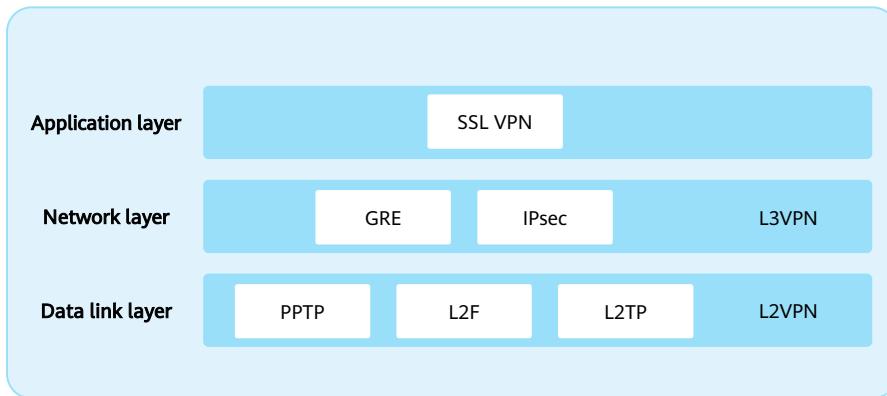


VPN Classification: By Application Object

- Classified by application object:
 - Extranet VPN: extends the enterprise network to partners through the VPN so that different enterprises can construct VPNs through the Internet.
 - Intranet VPN: connects the internal networks of an enterprise through a public network.
 - Access VPN: allows employees on business trips to remotely access the enterprise intranet across the public network.



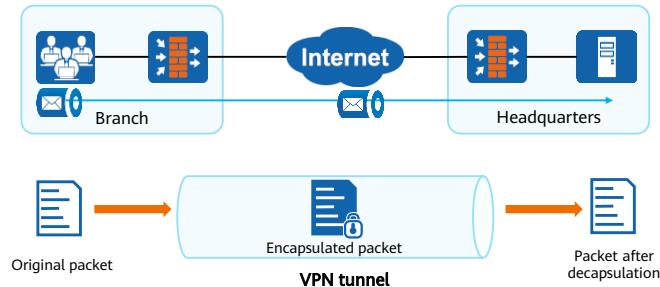
VPN Classification: By VPN Implementation Hierarchy



- L3VPN
 - An L3VPN works at the network layer of the protocol stack. In an IPsec VPN, the IPsec header and IP header work at the same layer; packets are encapsulated in IP-in-IP mode, or the IPsec header and IP header encapsulate the payload at the same time.
 - GRE VPN is another major type of L3VPN technologies. The GRE VPN emerges earlier and its implementation mechanism is simpler. A GRE VPN allows the packets of one protocol to be encapsulated in those of any other protocol. GRE VPN is less secure than IPsec VPN due to limited, simple security mechanisms.
- L2VPN
 - Similar to the L3VPN, the L2VPN refers to that the VPN technology works at the data link layer of the protocol stack. Protocols used by the L2VPN include the Point-to-Point Tunneling Protocol (PPTP), Layer 2 Forwarding (L2F), and Layer 2 Tunneling Protocol (L2TP).

Key VPN Technology: Tunneling Technology

- VPN uses tunneling technologies to establish private tunnels on a VPN backbone to secure data transmission.
- Tunneling technologies use one protocol to encapsulate the packets of another protocol (usually IP packets), and can be encapsulated by another protocol, too. A tunnel is a logical link and has the same benefits as a private physical link.



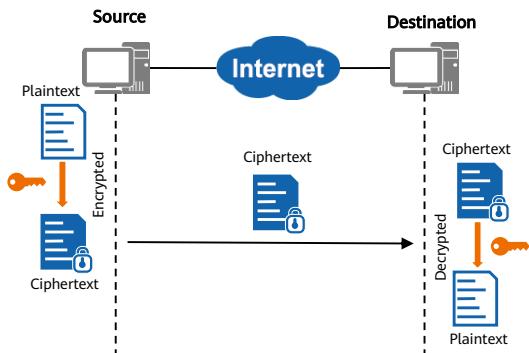
- The tunneling technology is a basic VPN technology, which is similar to the point-to-point connection technology. As shown in the figure, after receiving the original packet, the branch VPN gateway encapsulates the packet and transmits it to the headquarters VPN gateway over the Internet. The headquarters VPN gateway decapsulates the packet to obtain the original packet.
- The encapsulation/decapsulation process provides security protection for original packets. The logical path through which all encapsulated packets are transmitted on the Internet is called a tunnel.

Key VPN Technology: Identity Authentication

- The identity authentication technology is mainly used for remote access of mobile office users. The VPN gateway at the headquarters authenticates users to ensure that the users accessing the intranet are authorized users. Different VPN technologies provide different user identity authentication methods:
 - GRE: does not support user identity authentication.
 - L2TP: depends on PPP authentication. An access user can be authenticated locally or by a third-party RADIUS server. After the user is authenticated, an internal IP address is assigned to the user for authorization and management.
 - IPsec: supports EAP authentication when IKEv2 is used. The authentication mode is the same as that of L2TP. An IP address is assigned to a user after the user is authenticated. The IP address can be used to authorize and manage the user.
 - SSL VPN: supports local authentication, certificate authentication, and server authentication for access users. In addition, access users can authenticate the SSL VPN server to check the validity of the SSL VPN server.

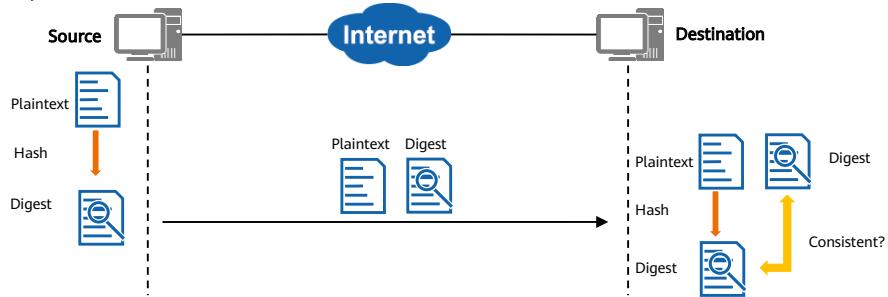
Key VPN Technology: Encryption Technology

- The encryption technology is a process of encrypting plaintext into ciphertext. In this way, even if a hacker intercepts a packet, the hacker cannot know the actual meaning of the packet. Encryption objects include data packets and protocol packets. A protocol that allows encryption of both protocol packets and data packets is more secure.
- GRE and L2TP do not provide encryption technologies. Therefore, GRE and L2TP are used together with IPsec and IPsec encryption technology provides security function for them .
- IPsec: supports encryption of data packets and protocol packets.
- SSL VPN: supports encryption of data packets and protocol packets.



Key VPN Technology: Data Verification Technology

- The data verification technology is used to check the authenticity of packets and discard forged and tampered packets. Verification is implemented through a technique called "digest".
- The digest technique uses the hash function to convert a long packet into a short packet. Packets are authenticated at both the sending and receiving ends. Only the packets with the same digest are accepted.



VPN Technology Comparison

Technology	Protection Scope	Application Scenario	Identity Authentication	Encryption & Verification
GRE	IP and upper-layer data	Intranet VPN	Not supported	Supports simple keyword verification and authentication.
IPsec	IP and upper-layer data	Access VPN Intranet VPN Extranet VPN	Supports pre-shared key or certificate authentication and IKEv2 EAP authentication.	Supported
L2TP	IP and upper-layer data	Access VPN Extranet VPN	Supports PPP-based CHAP, PAP, and EAP authentication.	Not supported
SSL VPN	Specific data at the application layer	Access VPN	Supports user name/password or certificate authentication.	Supported

Contents

1. Application of Cryptography

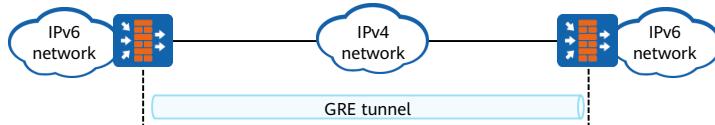
2. VPN Overview

- VPN Overview
- GRE VPN
- IPsec VPN
- L2TP VPN
- SSL VPN

3. VPN Configuration

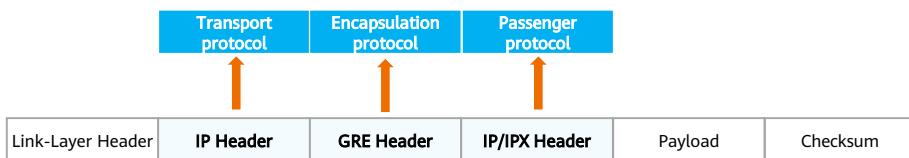
GRE VPN Overview

- Generic Routing Encapsulation (GRE) is a L3VPN encapsulation technology. GRE encapsulates the packets of a wide variety of network layer protocols, such as Internetwork Packet Exchange (IPX), IP, and AppleTalk, into IP tunneling packets, so that these packets can be transmitted over heterogeneous networks.
- The channel for transmitting packets over heterogeneous networks is called a "tunnel".
- Generally, a GRE tunnel is established over an IPv4 network to implement communication between two IPv6 networks.



GRE Protocol Stack

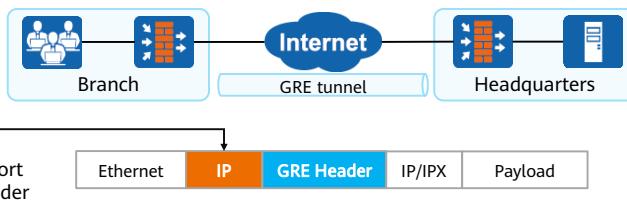
- The basic elements of the network encapsulation technology can be divided into three parts: passenger protocol, encapsulation protocol, and transport protocol. GRE is no exception. For easy understanding, we use the postal system as an example.
 - The passenger protocol can be seen as a letter written by ourselves. The letter can be written in Chinese, English, French, and so on. The writer and reader are responsible for the specific content.
 - The encapsulation protocol can be regarded as an envelope, which can be ordinary mail, registered mail, or EMS. Different envelopes correspond to multiple encapsulation protocols.
 - The transport protocol is like the transport mode of the letter, which can be land transport, sea transport, or air transport. Different transport modes correspond to different transport protocols.



- During GRE encapsulation, the packet before encapsulation is called the payload, and the packet protocol before encapsulation is called the passenger protocol. GRE then encapsulates the GRE header, and GRE becomes the encapsulation protocol, which is also called the carrier protocol. The protocol that is responsible for forwarding the encapsulated packet is called the transport protocol.

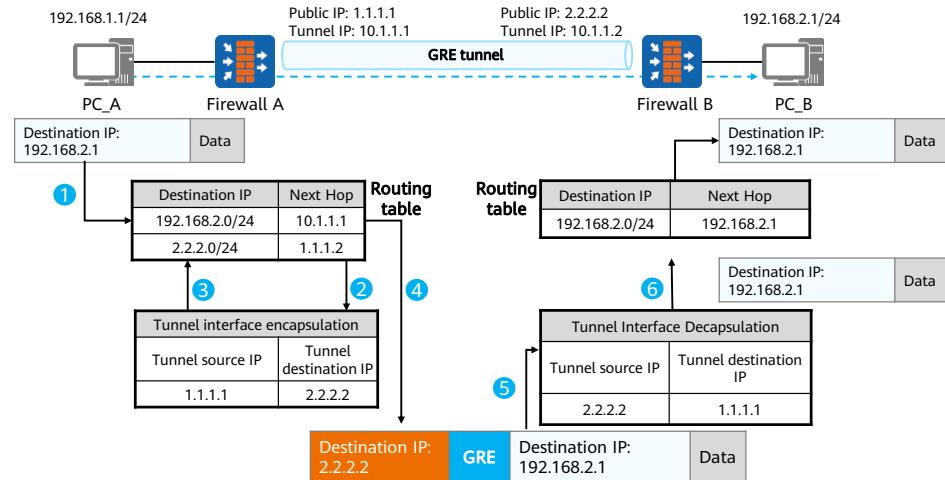
GRE Encapsulation

- GRE encapsulates packets layer by layer based on the protocol stack. The encapsulation process can be divided into two steps:
 - Step 1: Add a GRE header to the original packet.
 - Step 2: Add a new IP header before the GRE header.
- GRE encapsulation is completed by a tunnel interface. The tunnel interface is a common logical interface. The encapsulation protocol needs to be set to GRE for the tunnel interface.



- The GRE encapsulation and decapsulation process is as follows:
 - After receiving a packet from the interface connected to the private network, the device checks the destination IP address field in the packet header and searches the routing table for the outbound interface. If the outbound interface is a tunnel interface, the device sends the packet to the tunnel module for processing.
 - After receiving the packet, the tunnel module adds a GRE header to the packet based on the passenger protocol type and the check parameters configured for the GRE tunnel.
 - Then, the device adds a transport protocol packet header, that is, an IP packet header, to the packet. Then the source and destination addresses carried in the IP header are the source and destination addresses of the tunnel.
 - Finally, the device searches the routing table for the outbound interface based on the destination address in the IP header and sends the packet. Then, the encapsulated packet is transmitted over the public network.
 - After receiving the packet from the interface connected to the public network, the receiving device first analyzes the IP packet header. If the value of the protocol type field is 47, it indicates that the protocol is GRE. Then, the outbound interface sends the packet to the GRE module for processing. The GRE module removes the IP and GRE headers and finds that the passenger protocol of the packet is a protocol running on the private network based on the protocol type field in the GRE header. Then the GRE module sends the packet to the protocol for processing.

GRE Packet Handling Process



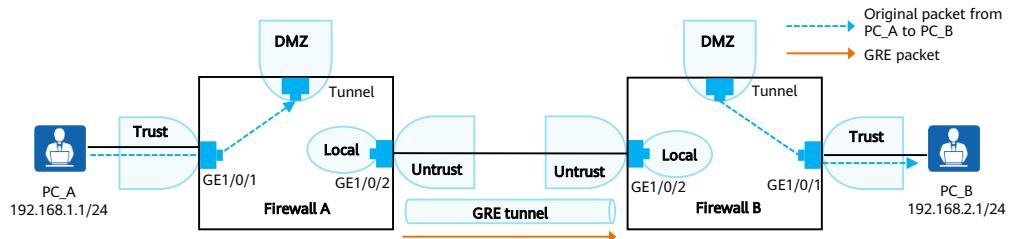
23 Huawei Confidential



- When PC_A accesses PC_B through the GRE tunnel, the packet forwarding process on firewall A and firewall B is as follows:
 - After the original packet from PC_A to PC_B enters firewall A, firewall A matches the packet with the routing table.
 - Based on the route search result, firewall A sends the packet to the tunnel interface for GRE encapsulation. The tunnel interface adds a GRE header and then a new IP header before the GRE header.
 - Firewall A searches the routing table again based on the destination address (2.2.2.2) in the new IP header of the GRE packet.
 - Firewall A forwards the packet to firewall B based on the route search result. Assume that the next hop address of the route to firewall B is 1.1.1.2.
 - After receiving the GRE packet, firewall B checks whether the packet is a GRE packet. The new IP header in the GRE packet has the **Protocol** field. If the **Protocol** field value is 47, the packet is a GRE packet, in which case firewall B forwards the packet to the tunnel interface for decapsulation. The tunnel interface removes the outer IP header and GRE header to restore the original packet. If the packet is not a GRE packet, firewall B forwards the packet as a common packet.
 - Firewall B searches the routing table again based on the destination address of the original packet and sends the packet to PC_B based on the route matching result.

GRE Security Policy

- When an original packet is sent from PC_A to the tunnel interface, the packet is sent from the Trust zone to the DMZ. When firewall A encapsulates and forwards it, it is sent from the Local zone to the Untrust zone.
- When the packet reaches firewall B, firewall B decapsulates the packet. In this process, the packet is sent from the Untrust zone to the Local zone. When firewall B decapsulates the GRE packet and forwards the original packet, the packet is sent from the DMZ to the Trust zone.



Contents

1. Application of Cryptography

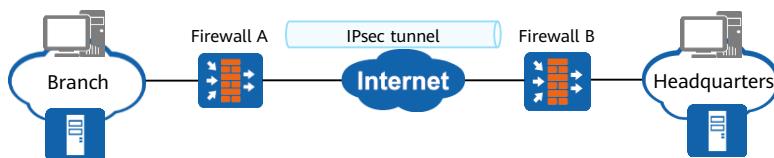
2. VPN Overview

- VPN Overview
- GRE VPN
- IPsec VPN
 - L2TP VPN
 - SSL VPN

3. VPN Configuration

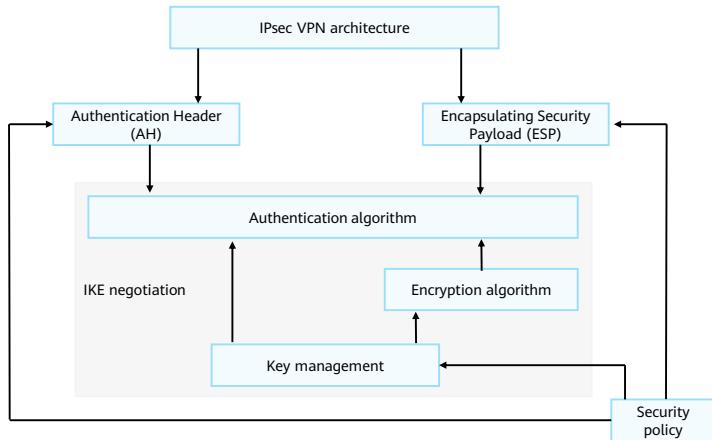
IPsec VPN Overview

- The IPsec protocol suite is a series of security protocols developed by the IETF. It provides a cryptology-based, interoperable, and high-quality security protection mechanism for end-to-end IP packet exchange. An IPsec VPN is a network layer VPN established through an IPsec tunnel.
- Both the L2TP VPN and GRE VPN transmit data in plaintext, failing to ensure security for users or enterprises. Deploying IPsec for these VPNs protects IP packets transmitted over an insecure network to reduce the risk of information breach.



- Leveraging encryption and authentication, IPsec secures service data transmission over the Internet through:
 - Data origin authentication: The receiver verifies whether the sender's identity is authorized.
 - Data encryption: The sender encrypts data packets and transmits them in ciphertext on the Internet. 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.
 - Anti-replay: The receiver rejects old or duplicate data packets to prevent malicious users from launching attacks by repeatedly sending captured packets.

IPsec VPN Architecture



- The IPsec VPN architecture consists of the Authentication Header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE) protocol suite. IPsec uses ESP to ensure the confidentiality of IP data transmission and uses AH/ESP to provide data integrity, data origin authentication, and anti-replay functions. ESP and AH define the formats and services of protocols and payload headers, but do not define the specific transcoding modes required for implementing the preceding capabilities. The transcoding modes include the data conversion mode, such as the algorithm and key length. To simplify the use and management of IPsec, IPsec can use IKE to automatically negotiate and exchange keys, and establish and maintain SAs.
 - AH: provides data origin authentication, data integrity check, and anti-replay. AH does not encrypt packets to be protected.
 - ESP: provides all the functions of AH (except that the integrity check does not cover the IP header) as well as packet encryption.
 - IKE: is used to automatically negotiate the cryptographic algorithm used by AH/ESP.

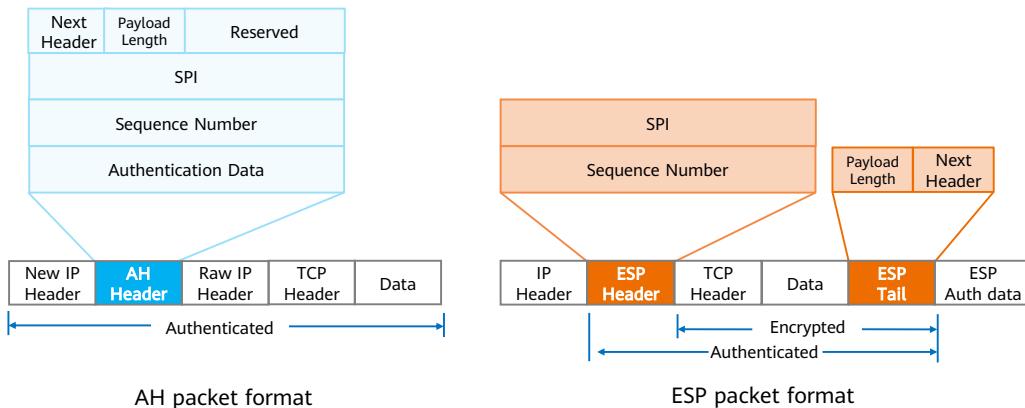
IPsec Protocol Framework

- IPsec protects IP packets using two security protocols: AH and ESP.
 - AH provides data origin authentication, data integrity check, and protection against replay attacks, but does not provide encryption.
 - ESP provides encryption, data origin authentication, data integrity check, and protection against replay attacks.

Security protocol	ESP				AH		
Encryption	DES	3DES	AES	SM1/ SM4			
Authentication	MD5	SHA1	SHA2	SM3	MD5	SHA1	SHA2
Key exchange	IKE (ISAKMP, DH)						

- Security functions provided by AH and ESP depend on the authentication and encryption algorithms used by IPsec.
- The keys used for IPsec encryption and authentication can be manually configured or dynamically negotiated using the IKE protocol.
- This course mainly describes how to establish an IPsec tunnel manually.

Comparison Between AH and ESP Packet Formats



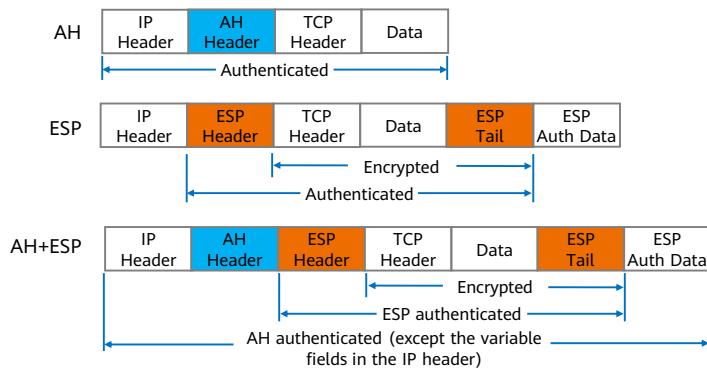
29 Huawei Confidential



- The fields in the AH header are described as follows:
 - Next Header: 8 bits, identifies the type of the payload following the AH header. In transport mode, the Next Header field value is the number of the protected upper-layer protocol (TCP or UDP) or ESP. In tunnel mode, the Next Header field value is the number of the IP or ESP protocol.
 - Payload length: 8 bits. The value of this field is the AH header length in 32-bit words minus 2. The default value is 4.
 - Reserved: 16 bits. This field is reserved and defaults to 0.
 - Security parameter index (SPI): 32 bits. It uniquely identifies an IPsec SA.
 - Sequence Number: 32 bits. It is a counter that starts from 1 and increases in ascending order. It uniquely identifies a packet to prevent replay attacks.
 - Authentication data: The field length is an integral multiple of 32 bits. It is 96 bits in common cases. This field contains the Integrity Check Value (ICV) and is used by the receiver for data integrity check. Available authentication algorithms are MD5, SHA-1, SHA-2 and SM3. The first three authentication algorithms are listed in ascending order of security. The authentication algorithm with a higher security has a more complex implementation mechanism and a low computing speed. SM3 cryptographic hash algorithm is an IPsec protocol specification defined by China's State Cryptography Administration.

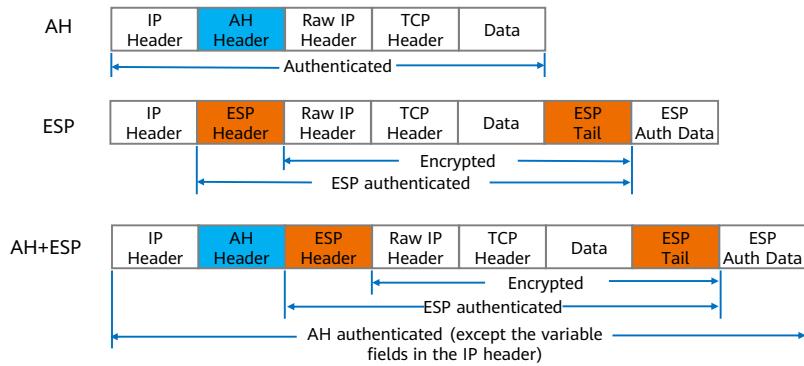
Encapsulation Mode — Transport Mode

- 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. The following example encapsulates a TCP packet in transport mode. The figure shows the packet format after encapsulation.



Encapsulation Mode — Tunnel Mode

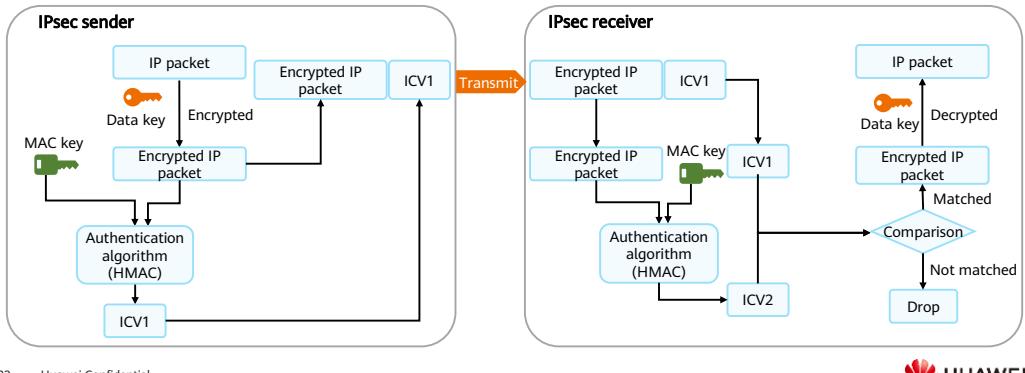
- In tunnel mode, an AH or ESP header is added before the raw IP header and then encapsulated into a new IP packet with a new IP header to protect the IP header and payload. The following example encapsulates a TCP packet in tunnel mode. The figure shows the packet format after encapsulation..



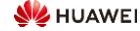
- The tunnel mode applies to communication between two VPN gateways or between a host and a VPN gateway.
- The two encapsulation modes differ in the following:
 - The tunnel mode is more secure than the transport mode. In tunnel mode, original IP packets can be authenticated and encrypted, and internal IP addresses, protocol types, and ports can be hidden.
 - In terms of performance, the tunnel mode occupies more bandwidth resources because of an extra IP header.
- When both AH and ESP are used to protect traffic, they must use the same encapsulation mode.

IPsec Data Encryption and Authentication

- IPsec provides two security mechanisms: encryption and authentication.
 - IPsec uses symmetric encryption algorithms to encrypt and decrypt data. These algorithms require that the sender and receiver use the same key (a symmetric key) to encrypt and decrypt data.
 - IPsec uses the Hash-based Message Authentication Code (HMAC) function to compare digital signatures to check data integrity and authenticity.

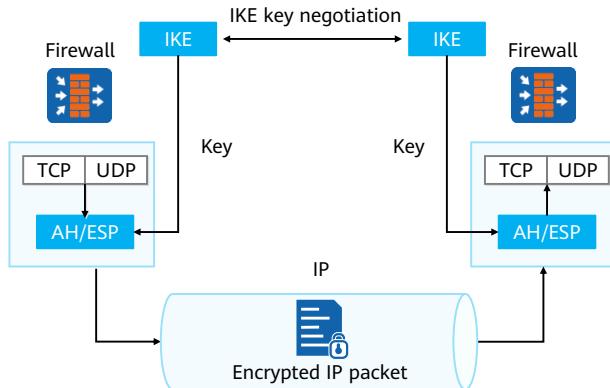


32 Huawei Confidential



- Integrity Check Value (ICV) is used by the receiver for integrity check. Available authentication algorithms are MD5, SHA1, SHA2, and SM3.
- Message Authentication Code (MAC) key is used for the HMAC algorithm.
- Common symmetric encryption algorithms used by IPsec include DES, 3DES, AES, and Chinese cryptographic algorithms (SM1 and SM4). DES and 3DES are not recommended because they are insecure and pose security risks.
- Common authentication algorithms used by IPsec include MD5, SHA1, SHA2, and SM3. MD5 and SHA1 are not recommended because they are insecure and pose security risks.
- IPsec encryption cannot verify the authenticity or integrity of information after decryption. IPsec uses the HMAC function to compare digital signatures to check integrity and authenticity of data packets. In most cases, encryption and authentication are used together. As shown in the preceding figure, the IPsec sender uses the authentication algorithm and symmetric key to generate an ICV for the encrypted packet and sends the IP packet and ICV to the receiver. The receiver uses the same authentication algorithm and symmetric key to process the encrypted packet and then generates an ICV. Then the receiver compares the received and generated ICVs to verify the data integrity and authenticity. If the packet passes the verification, the receiver decrypts it. Otherwise, the receiver discards it.

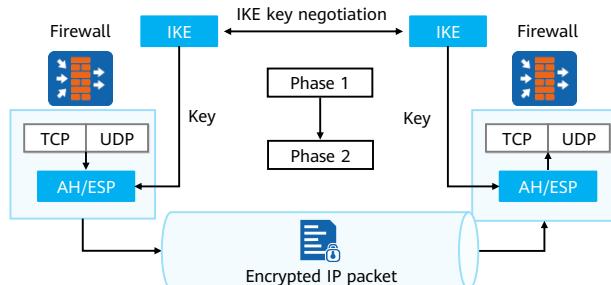
Relationship Between IKE and AH/ESP



- IKE is an application-layer protocol based on UDP and is the signaling protocol of IPsec. IKE generates a key for IPsec negotiation, which is used for AH/ESP encryption, decryption, and authentication. AH and ESP have their respective protocol numbers 51 and 50.
- IKE has two versions: IKEv1 and IKEv2.

IKE Exchange Phases

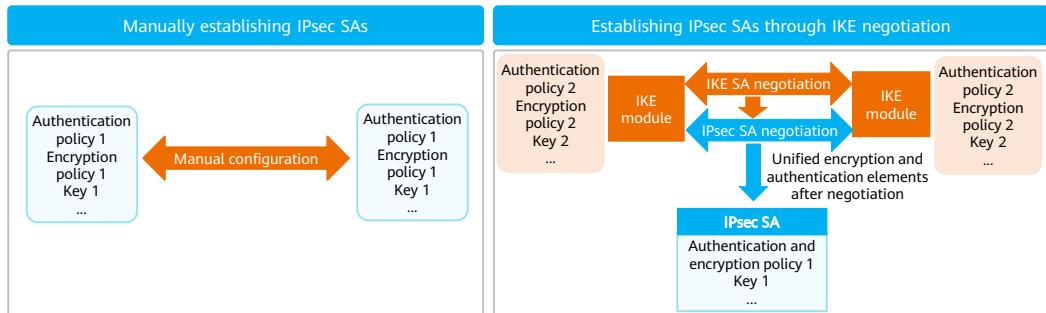
- IKE passes two phases to negotiate the key and establish SAs for IPsec.
 - Phase 1: The communication parties establish an IKE SA, which is an authenticated and protected tunnel. The negotiation mode can be main mode or aggressive mode. Authentication modes include pre-shared key, digital signature, and public key encryption.
 - Phase 2: The communication parties use the IKE SA to negotiate IPsec services and to establish an IPsec SA. The IPsec SA is used for secure IP data transmission. The negotiation mode is quick.



- IKE uses ISAKMP in two phases. In the first phase, an IKE security association (SA) is established. In the second phase, the established SA is used to negotiate a specific SA for IPsec.
- As defined in RFC 2409, IKE negotiation in the first phase can adopt two modes: main mode and aggressive mode. Both modes do the same thing, that is, establish an encrypted and authenticated communication channel (IKE SA) and generate an authenticated key to provide confidentiality, message integrity, and message source authentication services for IKE communication. All other exchanges defined in IKE require an authenticated IKE SA as the primary condition. Therefore, in either main mode or aggressive mode, the first phase must be completed before any other exchange.
- The IKE working process is as follows:
 - After IPsec is applied to an interface, packets sent from this interface are checked against IPsec policies.
 - If the packet matches an IPsec policy, the initiator checks whether an SA has been established. If no SA is established, IKE negotiation is triggered. IKE establishes the IKE SA in phase 1.
 - The initiator negotiates a phase 2 SA (IPsec SA) with the responder under the protection of the phase 1 SA (IKE SA).
 - IPsec SAs are employed to protect communication data.

IPsec SA

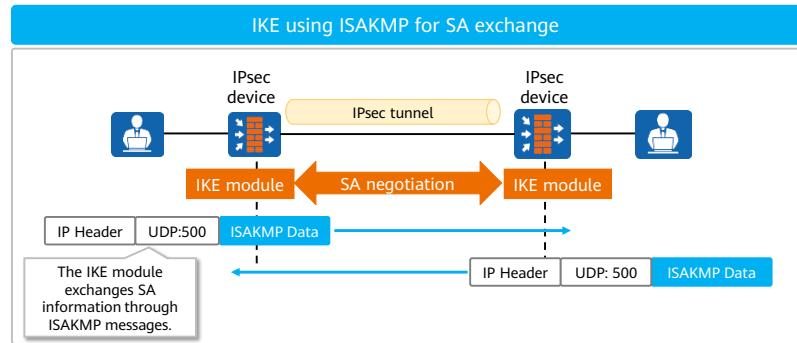
- An IPsec SA needs to be established between IPsec peers (two IPsec endpoints) before IPsec securely transmits data. SAs help IPsec define specific elements, for example, DES as the encryption algorithm, MD5 as the authentication algorithm, and tunnel as the encapsulation mode.
- An IPsec SA can be established manually or through IKE negotiation.



- IPsec technology supports multiple data encryption, authentication, and encapsulation algorithms. When devices at both ends use IPsec for secure communication, they must use the same encryption and authentication algorithms. Therefore, a mechanism is required to help the devices negotiate these parameters.
- An IPsec SA can be established in either of the following ways:
 - Manual mode:** Manually establishing IPsec SAs requires high management costs. The encryption authentication mode requires manual configuration and SA update. In addition, the SA information permanently exists and has low security. This mode is applicable to small networks.
 - IKE negotiation:** The management cost of IPsec SAs established through IKE negotiation is low. The encryption and authentication modes are generated using the Diffie-Hellman (DH) algorithm, SA information is generated periodically, and SAs are dynamically updated. This mode applies to small, midsize, and large networks.
- An IPsec SA is uniquely identified by three parameters: security parameter index (SPI), destination IP address, and security protocol ID (AH or ESP).
- An IKE SA is used to establish a secure channel for exchanging IPsec SAs.

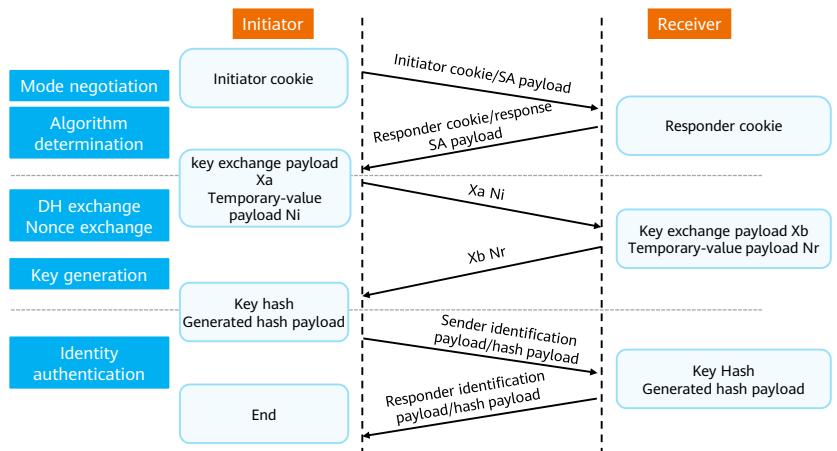
IKE SA

- On the live network, the IKE protocol is typically used to exchange symmetric keys.
- IKE is based on the Internet Security Association and Key Management Protocol (ISAKMP) and is a UDP-based application layer protocol. IPsec uses IKE for key auto-negotiation and IPsec SA establishment, simplifying IPsec configuration and maintenance.



- IKE supports the following authentication algorithms: MD5, SHA1, SHA2-256, SHA2-384, SHA2-512, and SM3.
- IKE supports the following encryption algorithms: DES, 3DES, AES-128, AES-192, AES-256, SM1, and SM4.
- ISAKMP is defined in RFC 2408, which defines the procedures for negotiating, establishing, modifying, and deleting SAs and defines the ISAKMP message format. ISAKMP provides a general framework for SA attributes and the methods of negotiating, modifying, and deleting SAs, without defining the specific SA format.
- ISAKMP messages can be transmitted using UDP or TCP through port 500. In most cases, ISAKMP messages are transmitted using UDP.

IKEv1 Negotiation Phase 1 — Pre-shared Key Negotiation in Main Mode



37 Huawei Confidential

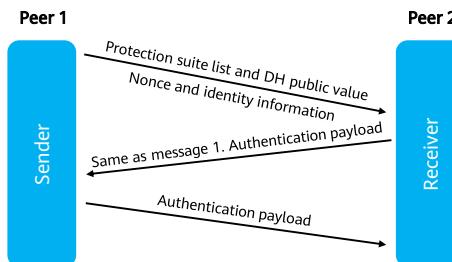


- Phase 1 of IKE Exchange - Main Mode Exchange
 - The main mode is designed as an exchange technology that separates key exchange information from identity authentication information. This separation ensures the security of identity information during transmission because the exchanged identity information is encrypted.
 - In main mode, a total of three steps (six messages in total) are required to complete phase 1 negotiation and establish an IKE SA. The three steps are mode negotiation, DH & nonce exchange, and peer identity authentication.
 - The main mode features identity protection and full use of ISAKMP negotiation capabilities. Identity protection is particularly important when the other party wants to hide its identity. When we discuss the aggressive mode, the full utilization of negotiation capabilities will also highlight its importance. If the pre-shared key method is used, before messages 1 and 2 are sent, the negotiation initiator and responder must calculate their own cookies to uniquely identify each individual negotiation exchange. The cookie is generated by the MD5 algorithm based on the source/destination IP address, random number, date, and time, and is put into the ISAKMP of message 1 to identify a single negotiation exchange.

- In the first exchange, the cookie and SA payloads of both parties need to be exchanged. The SA payload carries the parameters of the IKE SA to be negotiated, including the IKE hash type, encryption algorithm, authentication algorithm, and IKE SA negotiation time limit.
- After the first exchange and before the second exchange, both communication parties need to generate the DH value used to generate the DH shared key. The initiator and responder each generate a random number and use the DH algorithm to calculate the random numbers to obtain DH values Xa and Xb (Xa is the DH value of the initiator, and Xb is the DH value of the responder). Then, the two parties obtain temporary values Ni and Nr by using the DH algorithm.
- In the second exchange, both parties exchange their own key exchange payload (DH exchange) and temporary value payload (nonce exchange). The key exchange payload contains Xa and Xb, and the temporary value exchange payload contains Ni and Nr.
- After exchanging the Ni and Nr payloads, the two parties use the pre-shared key and a random function to generate an SKEYID. The SKEYID is the basis for generating subsequent keys. Based on the calculated DH value, exchanged DH value, and SKEYID, a shared key SKEYID_d is generated, which is known only by both parties. The shared key is not transmitted. Only the DH value and temporary value are transmitted. Therefore, the third party cannot calculate the shared key even if the third party obtains these materials.
- After the second exchange is complete, both parties can calculate all keys and use the keys to protect subsequent IKE messages. These keys include SKEYID_a and SKEYID_e. SKEYID_a is used to provide security services such as integrity and data source identity authentication for IKE messages. SKEYID_e is used to encrypt IKE messages.
- In the third exchange, the identification payload and the hash payload are exchanged. The identification payload contains the identifier, IP address, or host name of the initiator. The hash payload contains the hash value of the three groups of keys generated in the previous process. The two payloads are encrypted using SKEYID_e. If the two payloads are the same, the authentication is successful. The pre-shared key exchange in IKE phase 1 in main mode is complete.

IKEv1 Negotiation Phase 1 — Pre-shared Key Negotiation in Aggressive Mode

- In aggressive mode, three messages need to be exchanged:
 - Message 1 exchanges the SA payload, keying materials, and identity information.
 - Message 2 adds the hash authentication payload while exchanging the content of message 1.
 - Message 3 is used by the responder to authenticate the initiator.



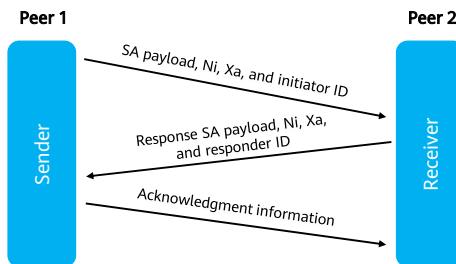
- Phase 1 of IKE Exchange - Aggressive Mode Exchange
 - It can be learned from the foregoing description of the main mode negotiation that a session key may be generated after the second exchange and the materials for generating the session key include a pre-shared key. When a peer negotiates SAs with multiple peers at the same time, a pre-shared key needs to be set for each peer. To correctly select a pre-shared key for each peer, the main mode differentiates peers based on the IP addresses in the exchanged information.
 - When the IP address of the initiator is dynamically allocated, the responder cannot obtain the IP address of the initiator in advance. In addition, both parties intend to use the pre-shared key authentication method. In this case, the responder cannot select the corresponding pre-shared key based on the IP address. The aggressive mode is used to solve this conflict.
 - Different from the main mode, the aggressive mode requires only three messages to establish an IKE SA. Because the number of messages is limited, the aggressive mode also limits its negotiation capability and does not provide identity protection.
 - In aggressive mode, the initiator provides a protection suite list, DH public value, nonce, and identity information. All the information is exchanged with the first message. The responder needs to select a protection suite, DH public value, nonce, identity information, and authentication payload. The initiator exchanges its authentication payload in the last message.
 - In aggressive mode, the identity information is carried in the first message. Therefore, the identity information cannot be encrypted, which reduces the negotiation security. In aggressive mode, however, the identity is not identified by the IP address. Therefore, the aggressive mode has more flexible applications.

Differences Between IKEv1 Main Mode and Aggressive Mode

- Exchanged messages:
 - Six for the main mode and three for the aggressive mode.
- Identity protection:
 - The last two messages in main mode are encrypted to provide identity protection. The messages in aggressive mode are highly integrated and therefore do not provide identity protection.
- Peer ID:
 - In main mode, only IP addresses can be used to identify IPsec peers. In aggressive mode, both IP addresses and names can be used to identify IPsec peers.

IKEv1 Negotiation in Phase 2 — Quick Mode

- In quick mode, three messages need to be exchanged:
 - In message 1 and message 2, the SA, key, nonce, and ID are exchanged, so as to negotiate algorithms, ensure PFS, and provide the "presence evidence".
 - Message 3 is used to verify whether the responder can communicate, and is equivalent to acknowledgment information.

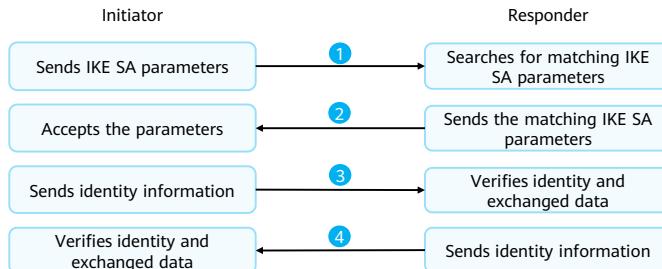


- IKE Exchange Phase 2 - Quick Mode Exchange
 - After an IKE SA is established (either in main mode or aggressive mode), it can be used to generate an SA for IPsec. The IPsec SA is established through the quick mode exchange. For the quick mode exchange, it is completed under the protection of the established IKE SA.
 - In a quick exchange, the communication parties need to negotiate the features of the IPsec SA and generate keys for the IPsec SA. The IKE SA protects the quick-mode exchange by encrypting it and authenticating the message. Message authentication is performed by using a pseudo-random function. The value of SKEYID_a from the IKE SA is used as a key to authenticate the entire message exchanged in quick mode. In addition to ensuring data integrity, this authentication also verifies the identity of the data source. After the message is received, we know that it can only come from the authenticated entity, and that the message does not change during transmission. Encryption (using SKEYID_e) ensures the confidentiality of the exchange.
 - In quick mode, the key used for the IPsec SA is derived from the SKEYID_d state. This key is used in the pseudo-random function to ensure that each SA has a unique key. Each SA has a unique SPI. Therefore, the key of the inbound SA is different from that of the outbound SA. All IPsec keys are derived from the same source. Therefore, they are associated with each other. If an attacker can determine the value of SKEYID_d based on the IKE SA, the attacker can easily obtain any key of the IPsec SA derived from SKEYID_d. In addition, it is obviously a big problem to continue to master all the keys to be derived in the future. None of these keys can guarantee the so-called Perfect Forward Secrecy (PFS). The quick mode provides a PFS option to meet this requirement. You can choose whether to use the PFS based on your security requirements.

- To implement PFS in the quick mode exchange, an additional DH exchange is required. The finally generated shared key is used in the process of generating a key for IPsec. Obviously, once the exchange is complete, the key no longer exists. Once completed, the memory location where it resides must be zeroed out and freed. In this way, it is ensured that the keys are irrelevant to each other.
- We described the quick mode earlier as a simple request/response exchange, but its practical utility goes far beyond that. The initiator may need presence evidence that the responder is online and has actually processed its initial fast-mode message. To meet this requirement, the responder needs to add the nonce of the initiator of the exchange and the message ID to the authentication hash payload. This digest can not only guarantee the integrity of the message, but also provide the source authentication function for the initiator. In addition, it can provide the presence evidence.
- The responder also needs presence evidence, and what comes from the initiator may be an expired message, replayed by an undesirable person. This person may not know the content of the message, but by analyzing the communication, he can know that it is a quick-mode message. If the message is replayed, the responder has to create redundant SAs. We can think of it as a "service denial" attack, which is a mild type because the responder increases unnecessary memory and SA management overhead based on this message. To defend against such attacks, a third message needs to be added to the quick-mode exchange. In this message, the initiator needs to include the nonce and the message ID of this exchange, and save them in an authentication hash payload. In this way, the initiator can confirm to the responder that it is a participant in the exchange.
- In the first two messages, both the initiator and responder send the SA payload. Like the main mode and aggressive mode, the SA payload is used to negotiate various protection algorithms. Ni, Nr, and ID are used to provide the "presence evidence". Xa and Xb are used to generate a new DH shared key to ensure PFS. Xa and Xb together with SKEYID_d, Ni, Nr, and SPI generated in IKE phase 1 generate a key for IPsec encryption.
- Finally, the initiator sends an acknowledgment message. After receiving the message, the responder knows that the initiator has received the second message. IKE phase 2 ends.

IKEv2 Negotiation — Initial Exchanges

- IKEv2 defines three exchanges: Initial Exchanges, CREATE_CHILD_SA Exchange, and Informational Exchange.
- In normal cases, IKEv2 can establish the first pair of IPsec SAs through Initial Exchanges. Corresponding to IKEv1 phase 1, Initial Exchanges involve four messages in two exchanges, as shown below.

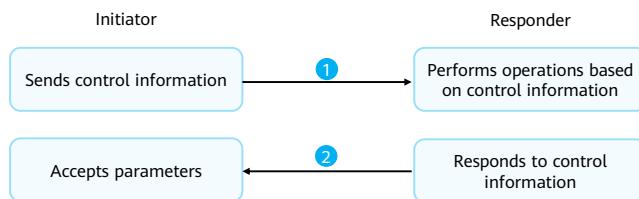


- The process of establishing SAs through IKEv2 negotiation is much simpler than that through IKEv1 negotiation. IKEv1 goes through two phases to establish a pair of IPsec SAs: "main mode + quick mode" or "aggressive mode + quick mode". The first one requires nine messages to be exchanged, whereas the second one requires at least six messages to be exchanged. IKEv2 requires two exchanges and four messages to establish a pair of IPsec SAs. If more than one pair of IPsec SAs needs to be set up, CREATE_CHILD_SA Exchanges are performed. One CREATE_CHILD_SA Exchange establishes one pair of IPsec SAs, that is, only two more messages are required to establish an additional pair of IPsec SAs.
- Initial Exchanges process
 - Messages 1 and 2 are used in exchange 1 (called IKE_SA_INIT). In exchange 1, IKE SA parameters are negotiated in plaintext, including the encryption key, authentication key, random number, and DH key. After IKE_SA_INIT is complete, a shared key material is generated, from which all IPsec SA keys are derived.
 - Messages 3 and 4 are used in exchange 2 (called IKE_AUTH). In exchange 2, identities of the two parties and the first two messages are authenticated, and IPsec SA parameters are negotiated. IKEv2 supports RSA signature authentication, PSK authentication, and EAP authentication. EAP authentication is implemented in IKE as an additional IKE_AUTH exchange. The initiator does not set the authentication payload in message 3 to indicate that EAP authentication is required.

- CREATE_CHILD_SA Exchange:
 - After one pair of IPsec SAs is established based on an IKE SA, CREATE_CHILD_SA Exchange can be performed to negotiate more pairs of IPsec SAs. In addition, CREATE_CHILD_SA Exchange can be performed for IKE SA re-negotiation.
 - CREATE_CHILD_SA Exchange involves two messages in one exchange and corresponds to IKEv1 phase 2. The initiator in CREATE_CHILD_SA Exchange can be the initiator or responder in Initial Exchanges. CREATE_CHILD_SA Exchange can be performed only after Initial Exchanges are complete. Messages transmitted in CREATE_CHILD_SA Exchange are protected by keys negotiated in Initial Exchanges.
 - Similar to IKEv1, if PFS is enabled, CREATE_CHILD_SA Exchange requires an additional DH exchange to generate a new keying material. All keys used by child SAs are derived from this keying material.

IKEv2 Negotiation — Notification Exchange

- IKEv2 peers perform Informational Exchange to exchange control information, including error information and notifications, as shown in the following figure.
- Informational Exchange must be performed under the protection of an IKE SA. Specifically, Informational Exchange is performed after Initial Exchanges are complete. Control information may belong to an IKE SA or a child SA. Therefore, Informational Exchange must be protected by the IKE SA or the IKE SA based on which the child SA is established accordingly.



Contents

1. Application of Cryptography

2. VPN Overview

- VPN Overview
- GRE VPN
- IPsec VPN
- **L2TP VPN**
- SSL VPN

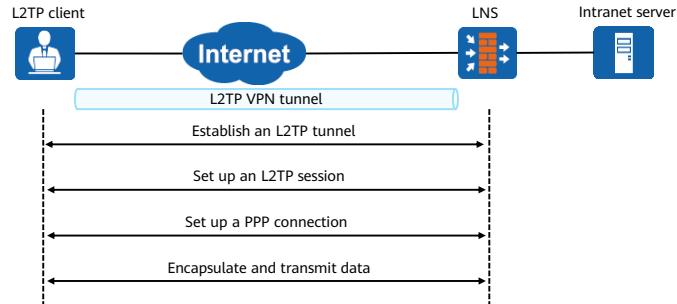
3. VPN Configuration

L2TP VPN Overview

- Layer Two Tunneling Protocol (L2TP) is another common VPN protocol.
 - L2TP is a tunneling protocol of the virtual private dial-up network (VPDN) and extends the Point-to-Point Protocol (PPP). A L2TP VPN is a VPN that provides access services for employees on business trips or enterprise branches to remotely access intranet resources in remote office scenarios.
- The L2TP VPN applies to the following scenarios:
 - NAS-Initiated VPN: A remote dial-up user initiates a VPN connection, and the remote system dials in to the LAC through the PSTN/ISDN. The LAC sends a request for establishing a tunnel to the LNS over the Internet. The LNS assigns an IP address to the dial-up user. The authentication and accounting for remote dial-in users can be performed by the LAC or LNS.
 - Call-LNS: In addition to providing remote access services for employees on business trips, L2TP can also be used for interconnection between enterprise branches and headquarters intranets so that branch users and headquarters users can communicate with each other.
 - Client-Initialized: LAC clients (L2TP-capable user terminals) directly initiate tunnel setup requests. The client needs to know the IP address of the LNS. The LAC client can directly initiate a request for establishing a tunnel to the LNS, and the request does not need to pass through an independent LAC. After receiving the request of the LAC client, the LNS authenticates the user name and password, and assigns a private IP address to the client.

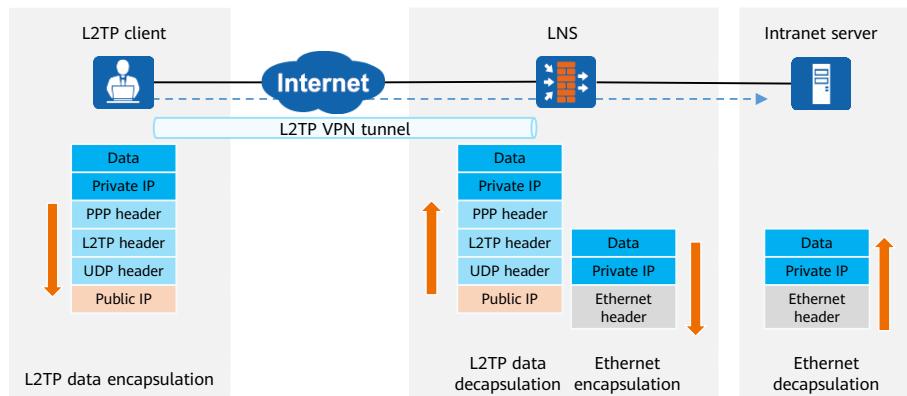
L2TP VPN Principles in the Client-Initiated Scenario (1/3)

- This section describes the mechanism of L2TP VPN in the client-initiated scenario in terms of tunnel negotiation, packet encapsulation, and security policy.
- Tunnel negotiation: Before a mobile user accesses the server at the enterprise headquarters, the user needs to use the L2TP VPN software to establish an L2TP VPN tunnel with the LNS. The figure shows how the mobile user establishes an L2TP VPN tunnel with the LNS and accesses the intranet resources.



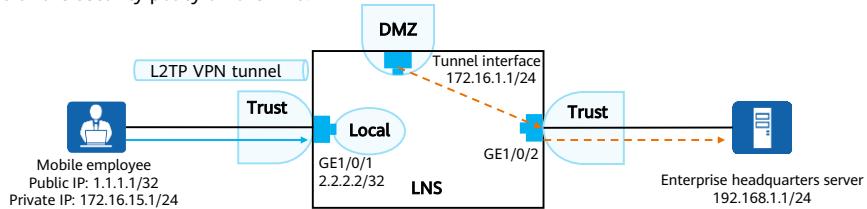
L2TP VPN Principles in the Client-Initiated Scenario (2/3)

- Packet encapsulation: The following figure shows the packet encapsulation and decapsulation processes.



L2TP VPN Principles in the Client-Initiated Scenario (3/3)

- Security policy: The following figure shows the interzones that packets pass through on the LNS and the matching conditions of the security policy on the LNS.



Service Direction	Device	Source Security Zone	Destination Security Zone	Source Address	Destination Address	Application
Packet sent by the mobile employee to access the server at the enterprise headquarters	LNS	Untrust	Local	Any	2.2.2.2/32	L2TP
		DMZ	Trust	172.16.1.2/24 to 172.16.1.100/24 (addresses in the address pool)	192.168.1.0/24	/
Packet sent by the server at the enterprise headquarters to the PC of the mobile employee	LNS	Trust	DMZ	192.168.1.0/24	172.16.1.2 to 172.16.1.100/24 (addresses in the address pool)	/

- When a mobile employee accesses an intranet server at the enterprise headquarters, the packets that pass through the LNS are classified into two types, and the security policy processes the two types of packets as follows:
 - L2TP packets between the mobile employee and the LNS: The L2TP packets include the L2TP negotiation packets sent by the mobile employee to establish a tunnel with the LNS and the pre-decapsulated service packets sent by the mobile employee to access the server at the enterprise headquarters. The L2TP packets are transmitted from the Untrust zone to the Local zone.
 - Service packets from the mobile employee to the intranet server at the enterprise headquarters: The VT interface of the LNS decapsulates the service packets sent by the mobile employee to the server at the enterprise headquarters. The packets are transmitted from the DMZ to the Trust zone. The tunnel interface on the LNS resides in the DMZ, and the interface connecting the LNS to the intranet server at the enterprise headquarters resides in the Trust zone.

Contents

1. Application of Cryptography

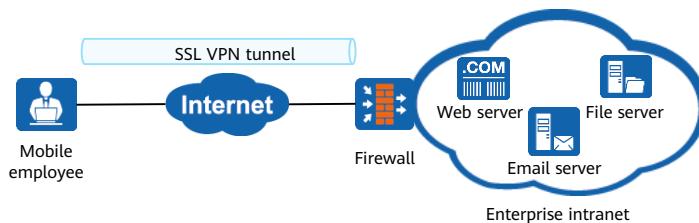
2. VPN Overview

- VPN Overview
- GRE VPN
- IPsec VPN
- L2TP VPN
- SSL VPN

3. VPN Configuration

SSL VPN Overview

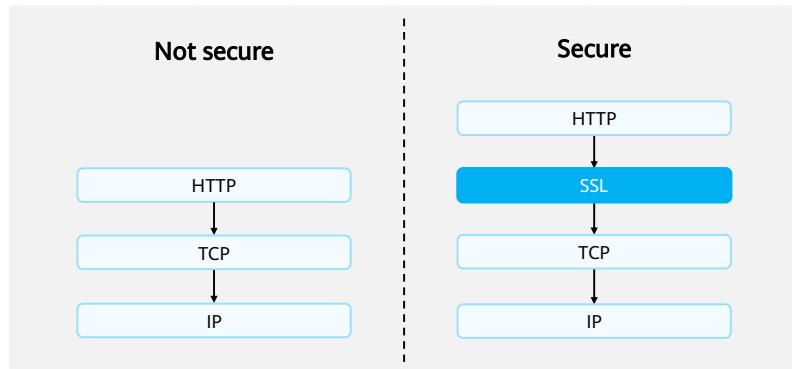
- Early VPN technologies such as IPsec and L2TP support remote access, but they have the following problems:
 - Mobile employees need to install specified client software.
 - Network deployment and maintenance are complex.
 - Refined control cannot be implemented on the access rights of mobile employees.
- As a new lightweight remote access solution, SSL VPN can effectively solve the preceding problems. SSL VPN is a VPN technology that implements secure remote access through the SSL protocol. It ensures that mobile employees can securely and efficiently access intranet resources from the external network.



- SSL VPN applies to the following scenario: Employees on business trips need to remotely access enterprise intranet resources through the Internet anytime and anywhere. In addition, multiple user authentication methods and fine-grained access permission control are needed to ensure the security of these resources.
- As shown in the preceding figure, the firewall functions as the enterprise egress gateway to connect to the Internet and provides SSL VPN access services for mobile employees (employees on business trips). After a mobile employee uses a terminal (such as a laptop, tablet, or smart phone) to establish an SSL VPN tunnel with the firewall, the employee can use the SSL VPN tunnel to remotely access intranet resources, such as the web server, file server, and mail server resources.

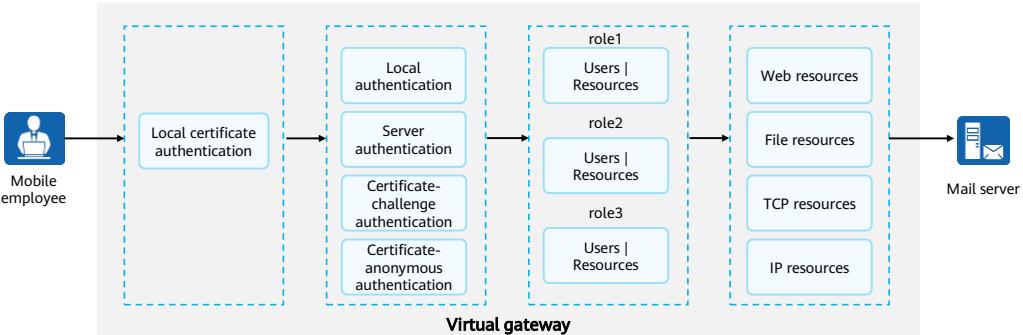
SSL VPN Encapsulation

- SSL encapsulation is located between the transport layer and application layer protocols to provide security support for data communication. It is established based on reliable transport protocols (such as TCP) and provides basic functions such as data encapsulation, compression, and encryption for upper-layer protocols.



SSL VPN Virtual Gateway

- The firewall provides SSL VPN access services for mobile employees 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. The system administrator creates SSL VPN virtual gateways on the firewall and the virtual gateways provide SSL VPN access services.



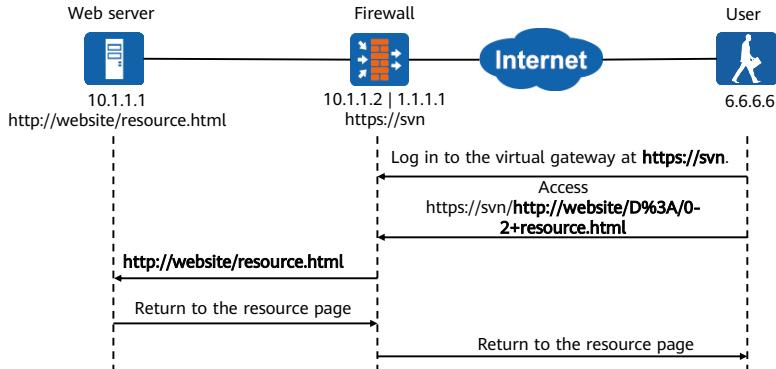
54 Huawei Confidential



- 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 remote user so that the user can authenticate the gateway. After the authentication succeeds, the remote user establishes an SSL connection with the virtual gateway, and the virtual gateway login page is displayed.
 - User authentication: After the user enters the user name and password on the login page, the virtual gateway authenticates the user in various 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.

SSL VPN Service — Web Proxy

- Mobile employees access intranet web resources through the web proxy service.
- The implementation of the web proxy is classified into web rewriting and web link.



55 Huawei Confidential

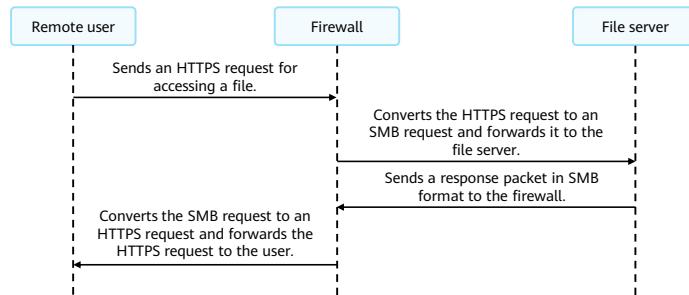


- Service interaction procedure:
 - The remote user accesses the virtual gateway at <http://svn>.
 - After logging in to the virtual gateway, the remote user views a list of accessible web resources and clicks the link of the intended web resource. The firewall rewrites the URL of the intended web resource (<http://website/resource.html>) when listing the web resource for the remote user. After the remote 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 returns the resource page that the web server sends to the remote user using HTTPS.

- Web rewriting: "Rewriting" has two meanings. The first meaning is encryption, that is, the virtual gateway encrypts the actual URL of the web resource requested by a remote user when the remote user clicks the URL of the requested web resource. The other meaning is adaptation. With the development of network technologies, terminals, such as smartphones, tablets, and laptops, are popularized among remote users. These terminals use various types of operating systems and browsers and they support different types of web resources. To eliminate the impacts of such differences, the firewall is required not only to encrypt requests from remote users but also adapt the requested web resources to the terminals used by remote users.
- Web link: With the web link function, the firewall transparently forwards the requests from remote users.

SSL VPN Service — File Sharing

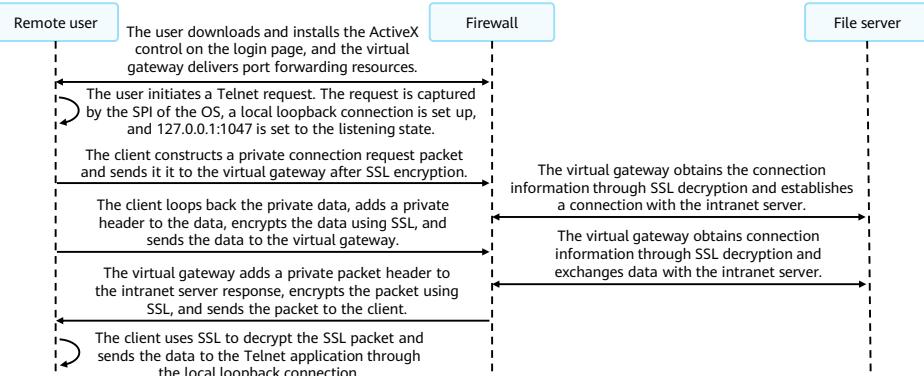
- Remote users access the intranet file server (running the SMB-capable Windows OS or NFS-capable Linux OS) using the file sharing service.
- Remote users can use web browsers to create and view folders as well as upload, download, rename, and delete files, just as they do on local file systems.



- In the file sharing service, the firewall functions as a protocol converter. The preceding figure shows the implementation process of accessing the Windows file server on the intranet.

SSL VPN Service — Port Forwarding

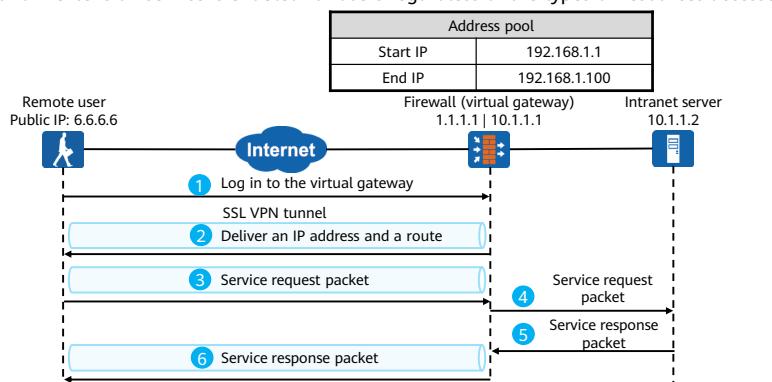
- The port forwarding service is used when remote users access intranet TCP resources. Port forwarding applies to TCP services, such as Telnet, remote desktop, FTP, and email. Port forwarding is a port-level security mechanism for accessing resources on an intranet from the Internet.



- You need to run an ActiveX control on the client as the port convertor to monitor the connections to the specified port. The preceding figure shows the process of port forwarding when a user logs in to the intranet server through Telnet.

SSL VPN Service — Network Extension (1/2)

- Remote users use the network extension service to access intranet IP resources. Web resources, file resources, and TCP resources are IP resources.
- Generally, the network extension service is enabled for users regardless of the types of resources accessed by the users.

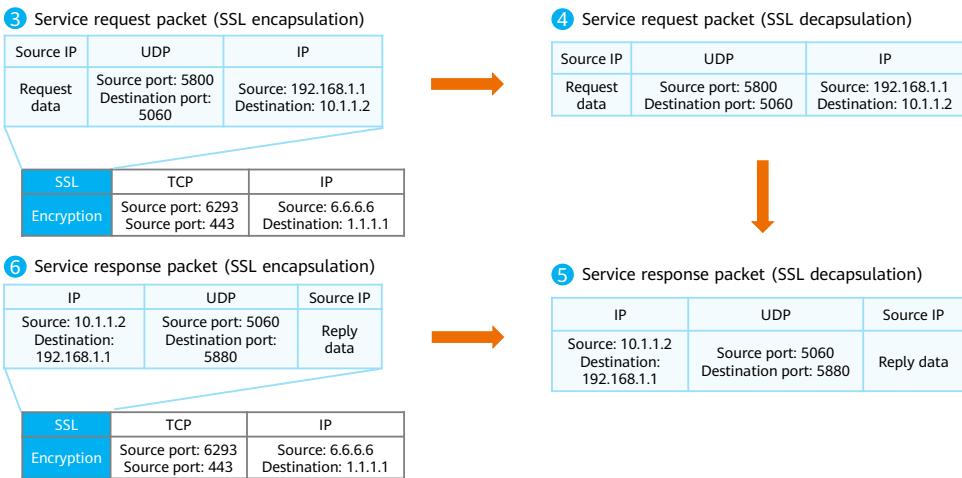


59 Huawei Confidential



- A remote user logs in to the virtual gateway using a browser.
- After login, the user enables the network extension function. After the network extension function is enabled:
 - The remote user and the virtual gateway establish an SSL VPN tunnel.
 - The local PC of the remote user automatically generates a virtual network adapter. The virtual gateway assigns an IP address in the address pool to the virtual adapter for the communication between the remote user and intranet server. With the IP address, the remote user can access intranet IP resources as an intranet user does.
 - The virtual gateway sends the remote user a route pointing to the intranet server based on network extension configurations.
- The remote 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 responds to the remote user's service request.
- The virtual gateway receives the response packet and forwards it to the user over the SSL VPN tunnel.

SSL VPN Service — Network Extension (2/2)



Contents

1. Application of Cryptography
2. VPN Overview
- 3. VPN Configuration**

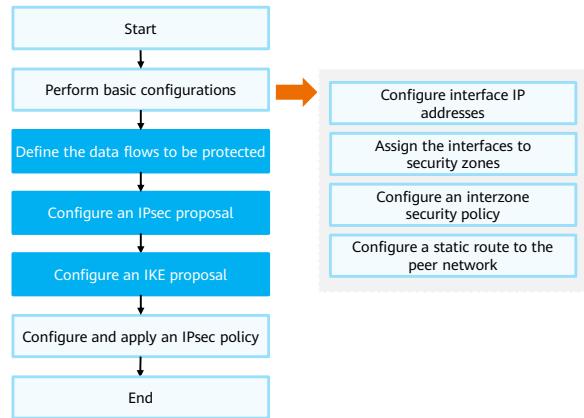
IPsec VPN Configuration Example (1/6)

- Requirement description:
 - The two gateways negotiate an IPsec VPN tunnel in IKE mode (using pre-shared key authentication) to implement secure access between LANs.
 - Network A and Network B are interconnected through an IPsec tunnel established between firewall A and firewall B.
 - Network A belongs to subnet 10.1.1.0/24 and is connected to firewall A through GE0/0/3.
 - Network B belongs to subnet 10.1.2.0/24 and is connected to firewall B through GE0/0/3.
 - Firewall A and firewall B are reachable to each other.



IPsec VPN Configuration Example (2/6)

- Configuration roadmap:
 - Perform basic interface configurations.
 - Configure security policies to allow devices on specified private network segments to exchange packets.
 - Create a route to the peer intranet.
 - Configure an IPsec policy, including basic IPsec policy information, data flows to be protected, and IPsec proposal negotiation parameters.



IPsec VPN Configuration Example (3/6)

- Define data flows to be protected.
 - Firewall A: Configure advanced ACL 3000 to allow users on network segment 10.1.1.0/24 to access network segment 10.1.2.0/24.

```
[FW_A] acl 3000  
[FW_A-acl-adv-3000] rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255  
[FW_A-acl-adv-3000] quit
```

- Firewall B: Configure advanced ACL 3000 to allow users on network segment 10.1.2.0/24 to access network segment 10.1.1.0/24.

```
[FW_B] acl 3000  
[FW_B-acl-adv-3000] rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255  
[FW_B-acl-adv-3000] quit
```

IPsec VPN Configuration Example (4/6)

- Configure an IPSec proposal. (The configuration on firewall A is the same as that on firewall B. You do not need to set default parameters.)

```
[FW_A] IPSec proposal tran1  
[FW_A-IPSec-proposal-tran1] esp authentication-algorithm sha2-256  
[FW_A-IPSec-proposal-tran1] esp encryption-algorithm aes-256  
[FW_A-IPSec-proposal-tran1] quit
```

- Configure an IKE proposal. (The configuration on firewall A is the same as that on firewall B.)

```
[FW_A] ike proposal 10  
[FW_A-ike-proposal-10] authentication-method pre-share  
[FW_A-ike-proposal-10] prf hmac-sha2-256  
[FW_A-ike-proposal-10] encryption-algorithm aes-256  
[FW_A-ike-proposal-10] dh group14  
[FW_A-ike-proposal-10] integrity-algorithm hmac-sha2-256  
[FW_A-ike-proposal-10] quit
```

IPsec VPN Configuration Example (5/6)

- Configure IKE peers.

```
[FW_A] ike peer b  
[FW_A-ike-peer-b] ike-proposal 10  
[FW_A-ike-peer-b] remote-address 1.1.5.1  
[FW_A-ike-peer-b] pre-shared-key Test!1234  
[FW_A-ike-peer-b] quit
```

```
[FW_B] ike peer a  
[FW_B-ike-peer-a] ike-proposal 10  
[FW_B-ike-peer-a] remote-address 1.1.3.1  
[FW_B-ike-peer-a] pre-shared-key Test!1234  
[FW_B-ike-peer-a] quit
```

- Configure IPsec policies.

```
[FW_A] IPSec policy map1 10 isakmp  
[FW_A-IPSec-policy-isakmp-map1-10] security acl 3000  
[FW_A-IPSec-policy-isakmp-map1-10] proposal tran1  
[FW_A-IPSec-policy-isakmp-map1-10] ike-peer b  
[FW_A-IPSec-policy-isakmp-map1-10] quit
```

```
[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 a  
[FW_B-IPSec-policy-isakmp-map1-10] quit
```

IPsec VPN Configuration Example (6/6)

- Reference to IPsec policy **map1**.
 - Firewall A: Apply IPsec policy **map1** to GE0/0/1.

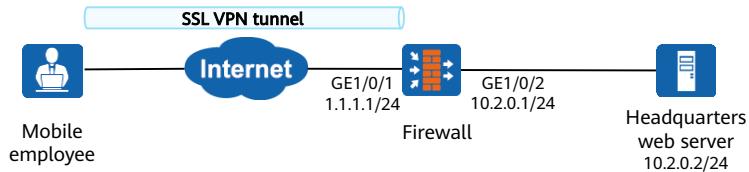
```
[FW_A] interface GigabitEthernet 0/0/1  
[FW_A-GigabitEthernet0/0/1] IPSec policy map1  
[FW_A-GigabitEthernet0/0/1] quit
```

- Firewall B: Apply IPsec policy **map1** to GE0/0/1.

```
[FW_B] interface GigabitEthernet 0/0/1  
[FW_B-GigabitEthernet0/0/1] IPSec policy map1  
[FW_B-GigabitEthernet0/0/1] quit
```

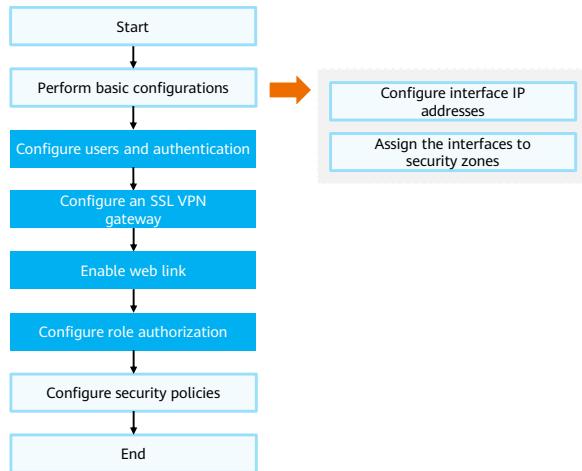
SSL VPN Configuration Example (1/7)

- Requirement description:
 - As shown in the figure, the enterprise requires that mobile employees access the enterprise's web server (web link) through the web proxy.
 - The enterprise authenticates employees in each department through local authentication on the firewall. Authenticated users can access the enterprise intranet.



SSL VPN Configuration Example (2/7)

- Configuration roadmap:
 - Perform basic interface configurations.
 - Configure users and authentication: Configure an authentication domain and create a user group and users.
 - Configure an SSL VPN gateway.
 - Configure the web link function: Enable the web link function and configure web link resources.
 - Configure role authorization: Add the user group to the virtual gateway, create a role, bind the role to the user group, and enable the web link function.
 - Configure security policies to allow mobile employees to log in to the SSL VPN gateway and allow employees on business trips to access web proxy resources.



SSL VPN Configuration Example (3/7)

- Configure users and authentication. Choose **Object > User > default**, set the parameters as follows, and click **Apply**.

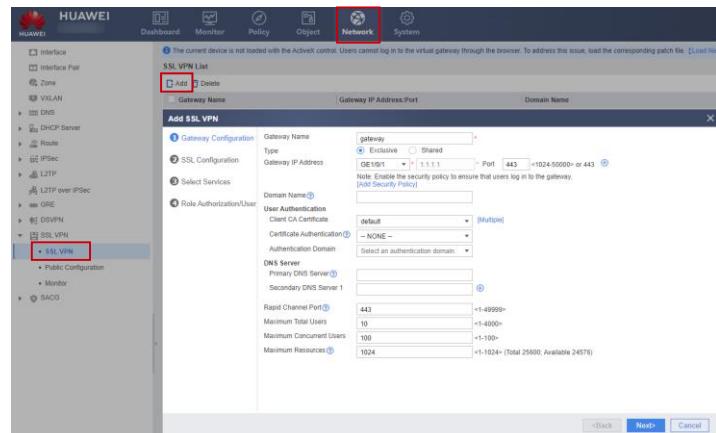
The screenshot shows the HUAWEI USG6300 Management Interface. The top navigation bar includes 'HUAWEI', 'Dashboard', 'Monitor', 'Policy', 'Object' (which is highlighted with a red box), 'Network', and 'System'. The 'admin' user is logged in. The main content area is titled 'User Management' under 'Object'. On the left, a sidebar lists 'Certificates', 'Address', 'Region', 'Service', 'Application', and 'User', with 'User' expanded and 'default' selected (highlighted with a blue box). The 'User Configuration' section contains fields for 'Scenario' (with 'SSL VPN access' checked), 'User Location' (set to 'Local' with 'Import User' selected), and 'Authentication Server' (set to 'None'). Below this is a table titled 'User/User Group/Security Group Management List' with columns: Name, Description, User Group, Source, Binding Inform..., Expiration Time, Activation, and Edit. A red box highlights the 'Add' button in the toolbar above the table. The bottom right corner features the HUAWEI logo.

70 Huawei Confidential

- The user **user0001** belongs to the user group **/default/group1**. The authentication mode is local authentication, and the password is **Password@123**. Before creating user **user0001**, you need to create group **/default/group1** so that you have a group to reference when creating a user.
- The CLI configuration is as follows:
 - [FW] aaa
 - [FW-aaa] domain default
 - [FW-aaa-domain-default] authentication-scheme default
 - [FW-aaa-domain-default] service-type ssl-vpn
 - [FW-aaa-domain-default] quit
 - [FW-aaa] quit
 - [FW] user-manage group /default/group1
 - [FW-usergroup-/default/group1] quit
 - [FW] user-manage user user0001 domain default
 - [FW-localuser-user0001] password Password@123
 - [FW-localuser-user0001] parent-group /default/group1
 - [FW-localuser-user0001] quit

SSL VPN Configuration Example (4/7)

- Configure an SSL VPN gateway. Choose **Network > SSL VPN > SSL VPN > Add** and set the parameters as follows:



71 Huawei Confidential

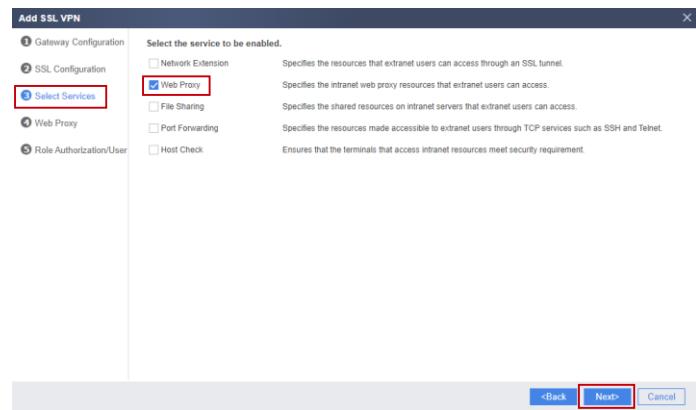


- The CLI configuration is as follows:

- [FW] v-gateway gateway interface GigabitEthernet 0/0/1 private
- [FW] v-gateway gateway udp-port 443
- [FW] v-gateway gateway authentication-domain default

SSL VPN Configuration Example (5/7)

- Configure the SSL version, cipher suite, session timeout, and session lifecycle. You can use the default settings. Select **Web Proxy** and click **Next**.



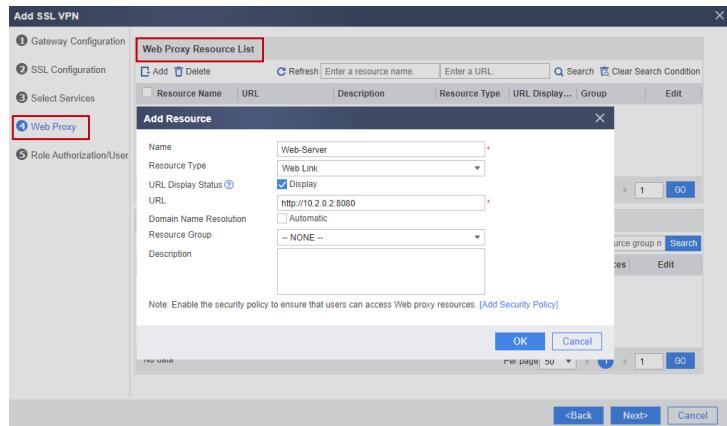
72 Huawei Confidential



- The CLI configuration is as follows:
 - [FW] v-gateway gateway
 - [FW-gateway] service
 - [FW-gateway-service] web-proxy enable
 - [FW-gateway-service] web-proxy web-link enable

SSL VPN Configuration Example (6/7)

- Configure the web proxy. Choose **Web Proxy Resource List > Add** and create a web proxy resource as follows.



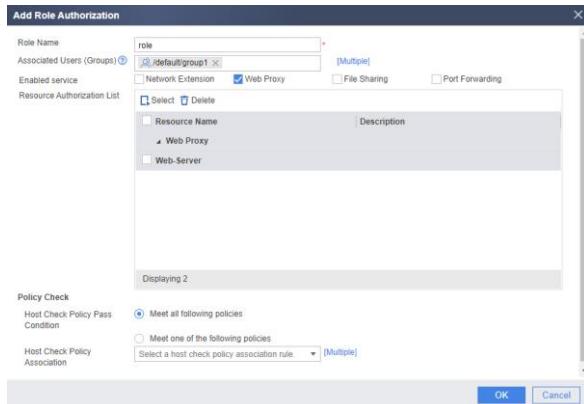
73 Huawei Confidential



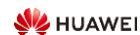
- The CLI configuration is as follows:
 - [FW-gateway-service] web-proxy link-resource Web-Server http://10.2.0.2:8080 show-link

SSL VPN Configuration Example (7/7)

- Configure role authorization for SSL VPN. Choose **Authorized Role List > Add** and set role authorization parameters, as shown in the following figure.



74 Huawei Confidential



- The CLI configuration is as follows:
 - [FW-gateway] vpndb
 - [FW-gateway-vpndb] group /default/sslvpn
 - [FW-gateway-vpndb] quit
 - [FW-gateway] role
 - [FW-gateway-role] role role
 - [FW-gateway-role] role role group /default/sslvpn
 - [FW-gateway-role] role role web-proxy enable
 - [FW-gateway-role] role role web-proxy resource Web-Server
 - [FW-gateway-role] quit
 - [FW-gateway] quit

Quiz

1. (True or False) IPsec uses asymmetric encryption algorithms to encrypt user data to ensure confidentiality of information transmission. ()
 - A. True
 - B. False
2. (Multiple-Answer Question) Which of the following are main SSL VPN functions of the firewall? ()
 - A. Port forwarding
 - B. Network extension
 - C. File sharing
 - D. Web proxy

1. B
2. ABCD

Summary

- This course describes the application scenarios of different encryption technologies, background of the VPN technology, implementations of encryption and decryption, as well as the configuration methods and typical cases of different VPN technologies.
- Upon completion of this course, you are able to independently configure multiple VPN technologies, such as IPsec VPN and SSL 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://learning.huawei.com/en/>

Acronyms and Abbreviations (1/2)

Acronym/Abbreviation	Full Name
CHAP	Challenge Handshake Authentication Protocol
EAP	Extensible Authentication Protocol
EMS	Express Mail Service
ICV	Integrity Check Value
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IPX	Internetwork Packet Exchange Protocol
ISAKMP	Internet Security Association Key Management Protocol
ISDN	Integrated Services Digital Network
L2F	Layer 2 Forwarding

Acronyms and Abbreviations (2/2)

Acronym/Abbreviation	Full Name
LAC	L2TP Access Concentrator
LNS	L2TP Network Server
PAP	Password Authentication Protocol
PFS	Perfect Forward Secrecy
PPTP	Point-to-Point Tunneling Protocol
PSTN	Public Switched Telephone Network
SA	Security Association
SEND	Secure Neighbor Discovery
SPI	Security Parameter Index

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
portfolio, new technology, 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.

