

Host Firewalls and Antivirus Software

Lecture 6

HCIA-Security

Prepared by
Dr. Abdelrhman Ahmed

Foreword

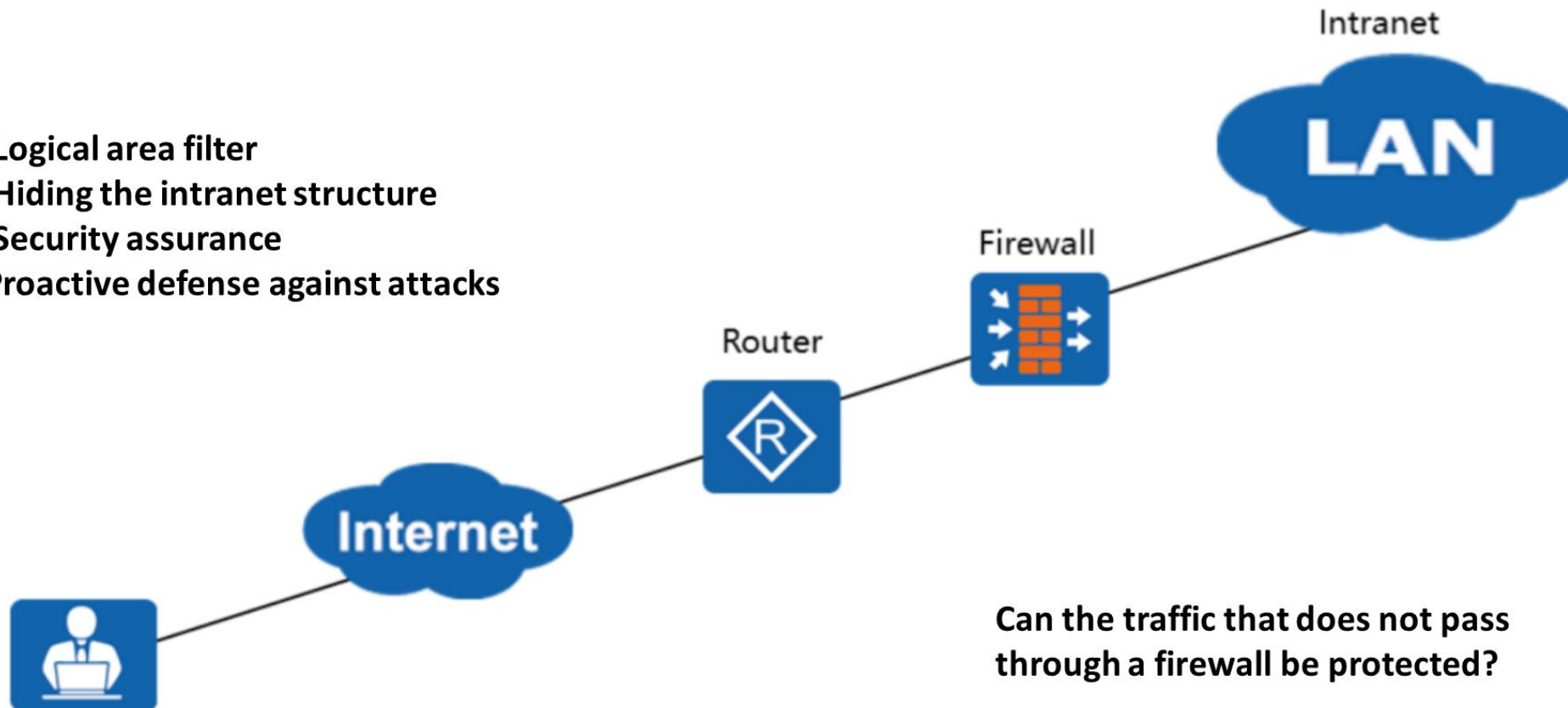
- During data communication, insecure factors may cause information leakage, incomplete information, unavailable information, etc. Therefore, firewalls are required during network deployment.
- This course introduces the history, features, typical networking modes, application scenarios, and technical specifications of Huawei firewalls.

Objectives

- **Upon completion of this course, you will be able to:**
 - ❑ **Understand the basic concepts of firewalls.**
 - ❑ **Understand firewall security policies.**
 - ❑ **Have a good command of firewall security policy configuration.**

Firewall Features

- Logical area filter
- Hiding the intranet structure
- Security assurance
- Proactive defense against attacks



Firewall Features

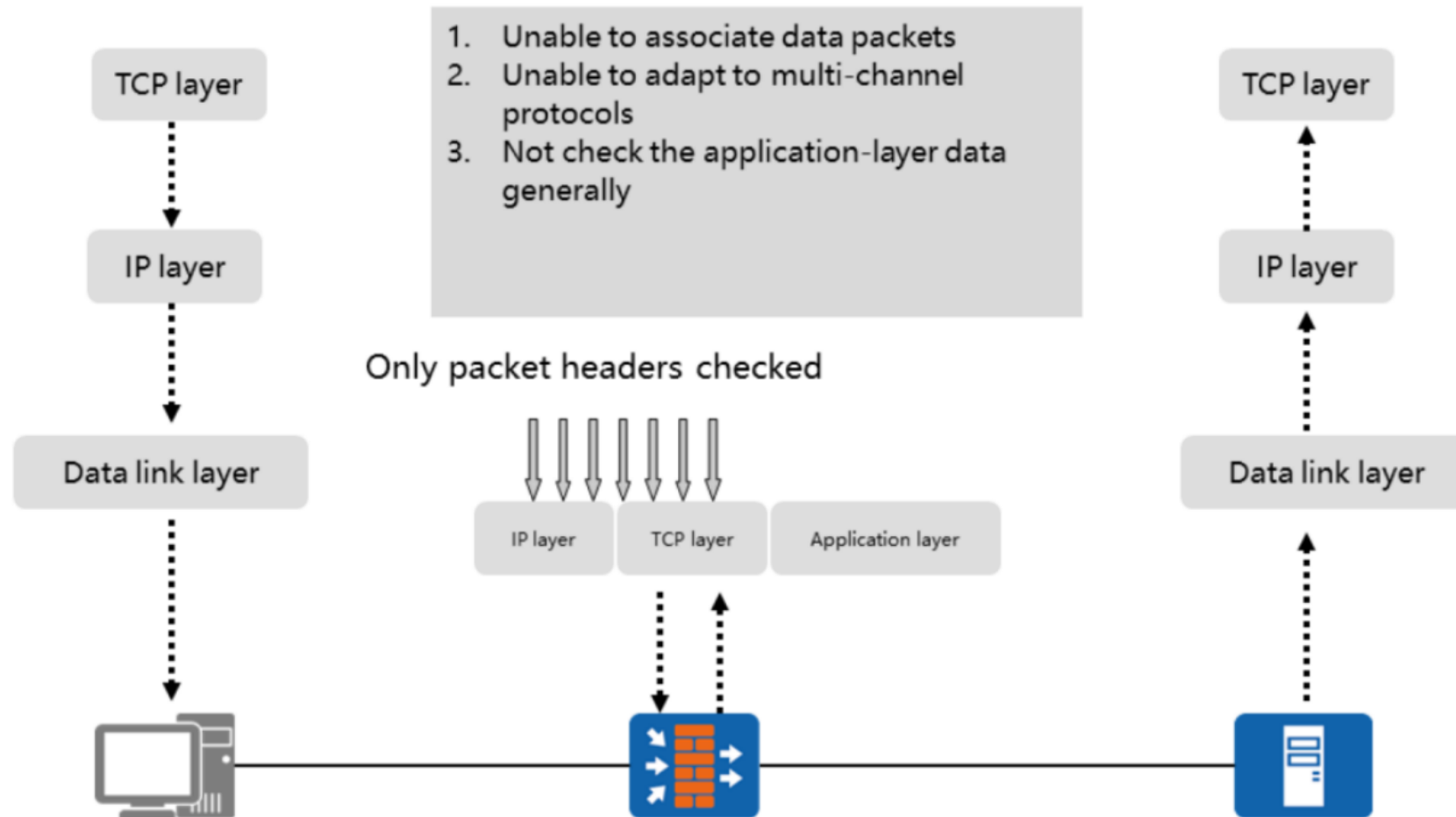
- Originally, a firewall referred to a wall built between houses to prevent fire from spreading. The firewall technology is an important part of security technology. This course discusses hardware firewalls. Hardware firewalls integrate security technologies to protect private networks (computers). To do this, they use the dedicated hardware structure, high-speed CPUs, and embedded OS, and support various high-speed interfaces (LAN interfaces). Hardware firewalls are independent of OSs (such as HP-UNIX, SUN OS, AIX, and NT) and computers (such as the IBM6000 and common PC). 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.
- The modern firewall system should not be just an "entrance barrier". Firewalls should be the access control points of networks. All data flows entering and leaving the network should pass through the firewall that serves as a gateway for incoming and outgoing information. Therefore, a firewall not only protects the security of an intranet on the Internet, but also protects the security of hosts on the intranet. All computers in a security zone configured on a firewall are considered "trustworthy" and communications between them are not affected by the firewall. However, communications between networks that are separated by a firewall must follow the policies configured on the firewall.

Firewall Classification

- **Firewalls are classified into the following types according to access control modes:**
 - ❑ **Packet filtering firewalls**
 - ❑ **Proxy firewalls**
 - ❑ **Stateful inspection firewalls**
- **Firewalls have been developed for three generations, and their classification methods are various. For example, firewalls can be classified into hardware firewalls and software firewalls by form or standalone firewalls and network firewalls by protection object. In general, the most popular classification method is by access control mode.**
- **Network firewalls can protect the entire network in a distributed manner. Their features are as follows:**
 - ❑ **Centralized security policies**
 - ❑ **Diversified security functions**
 - ❑ **Maintenance by dedicated administrators**
 - ❑ **Low security risks**
 - ❑ **Complicated policy configuration**

Chapter
06

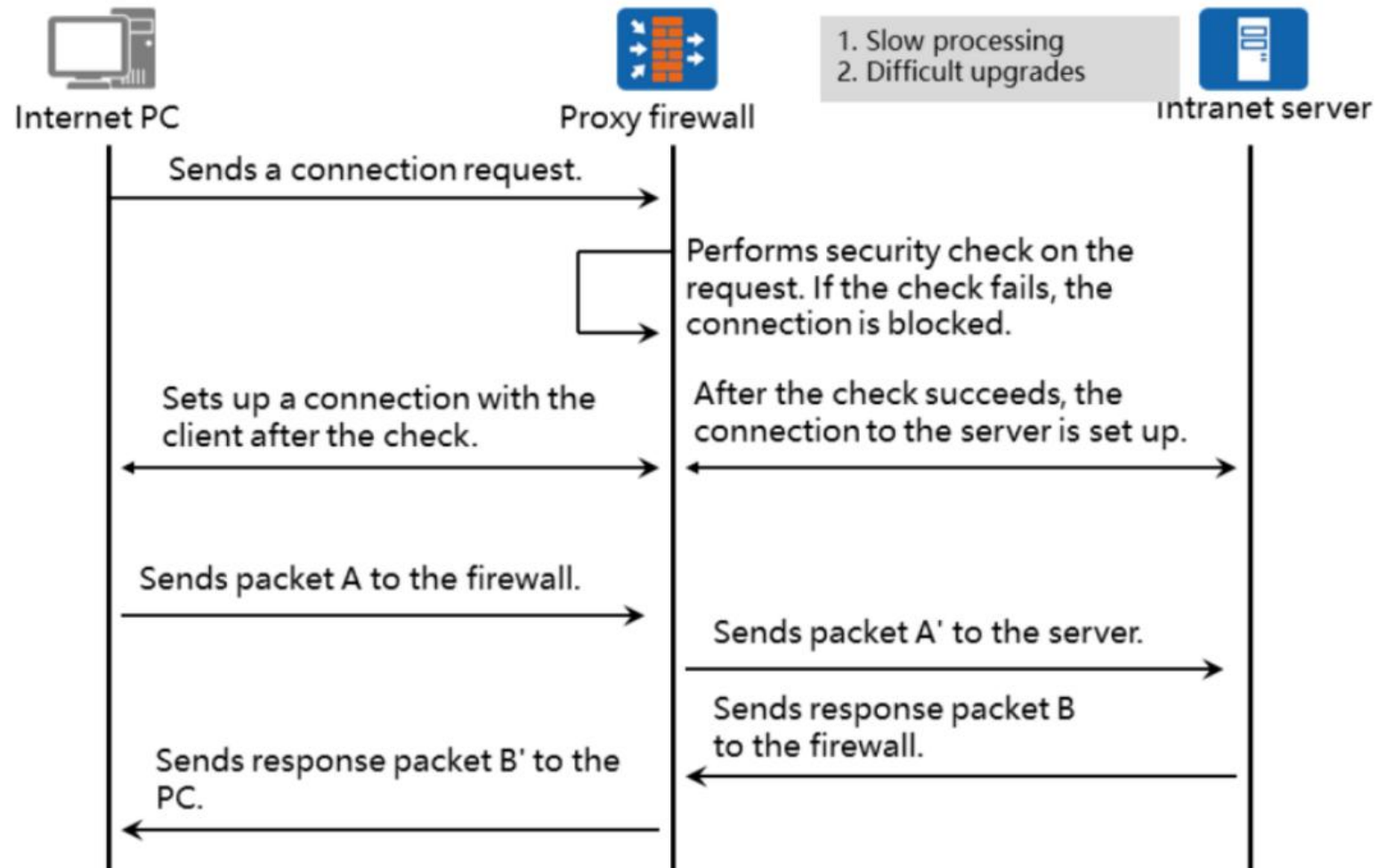
Firewall Classification: Packet Filtering Firewall



Firewall Classification: Packet Filtering Firewall

- Packet filtering checks each packet at the network layer and forwards, or discards packets based on configured security policies. The basic principle of the packet filtering firewall is to configure ACLs to filter data packets based on the source/destination IP address, source/destination port number, IP identifier, and packet transmission direction in a data packet.
- The packet filtering firewall is simple in design, easy to implement, and cost-effective.
- The disadvantages of the packet filtering firewall are as follows:
 - As ACL complexity and length increase, filtering performance decreases exponentially.
 - Static ACL rules cannot meet dynamic security requirements.
 - Packet filtering does not check session status or analyze data, which makes it easy for attackers to escape. For example, an attacker sets the IP address of their host to an IP address permitted by a packet filter. In this way, packets from the attacker's host can easily pass through the packet filter.
- **Note:** A multi-channel protocol example is FTP. Based on the negotiation of the control channel, FTP generates the dynamic data channel port. Then, data exchange is performed on the data channel.

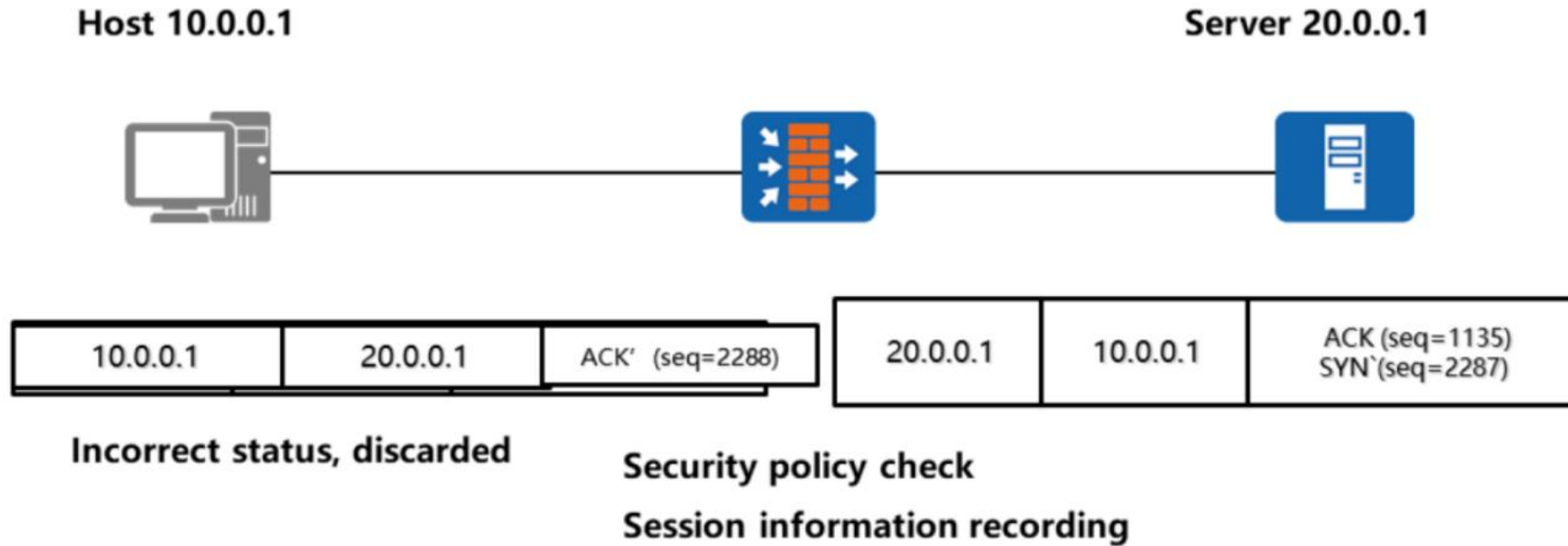
Firewall Classification: Proxy Firewall



Firewall Classification: Proxy Firewall

- The proxy applies to the application layer of the network. The proxy checks the services directly transmitted between intranet and Internet users. After the request passes the security policy check, the firewall establishes a connection with the real server on behalf of the Internet user, forwards the Internet user's request, and sends the response packet returned by the real server to the Internet user.
- The proxy firewall can completely control the exchange of network information and the session process, achieving high security. Its disadvantages are as follows:
 - ❑ Software implementation limits its processing speed. Therefore, the proxy firewall is vulnerable to DoS attacks.
 - ❑ Application-layer proxy must be developed for each protocol. The development period is long, and the upgrade is difficult.

Firewall Classification: Stateful Inspection Firewall



1. Fast processing of subsequent packets
2. High security

Firewall Classification: Stateful Inspection Firewall

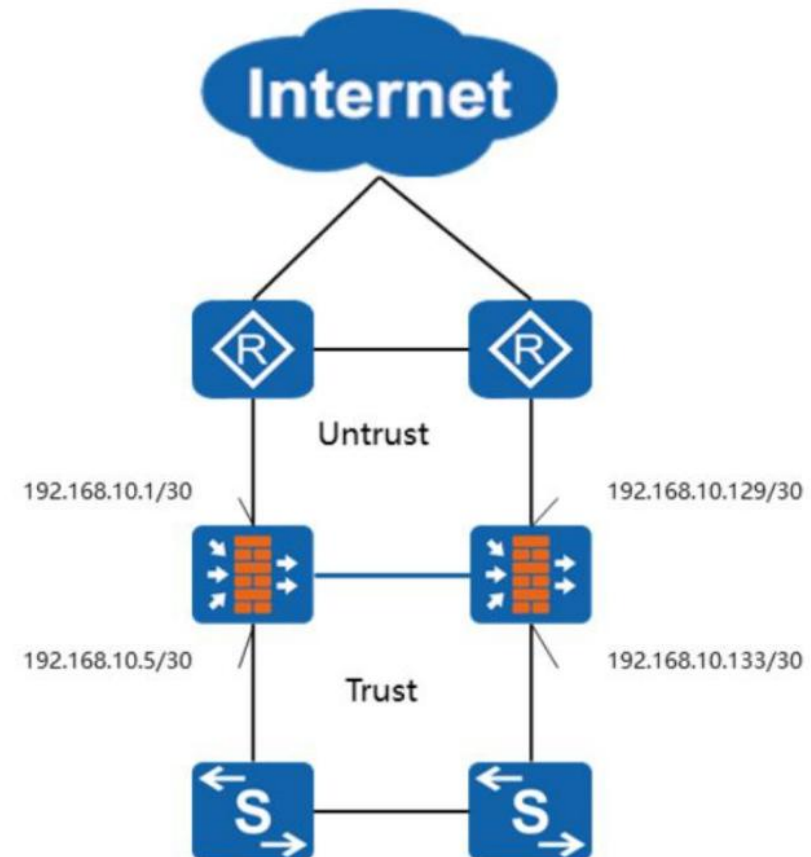
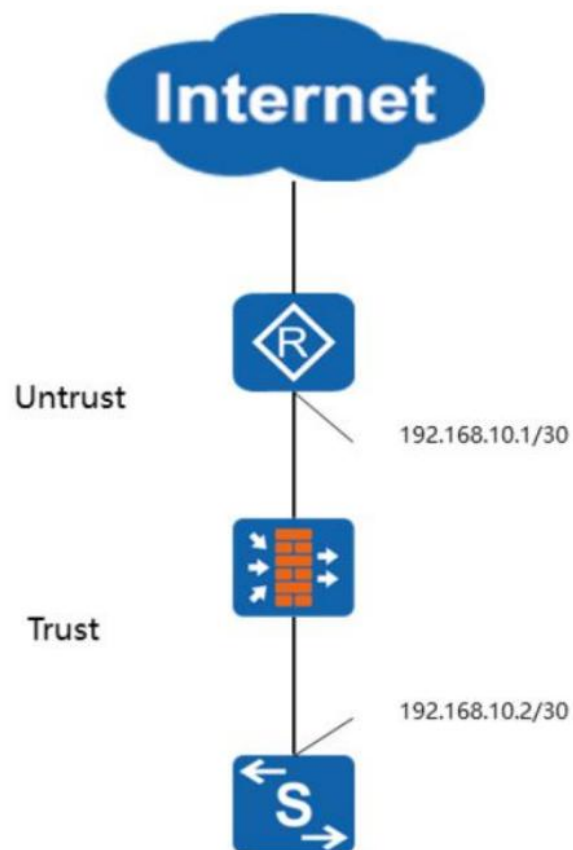
- **Stateful inspection is an extension of the packet filtering technology. Packets are filtered based on connection status, with each packet treated as an independent unit and the historical association of packets considered. All data flows based on reliable connections (TCP-based data flows) are processed in three phases: client request, server response, and client response (three-way handshakes). This indicates that each data packet does not exist independently but is closely related to preceding and subsequent packets. Based on the status association, the stateful inspection technology is developed.**
- **Its mechanism is as follows:**
 - ❑ **A stateful inspection firewall uses various session tables to trace activated TCP sessions and pseudo UDP sessions. The ACL determines the sessions to be established. A data packet is forwarded only when it is associated with a session. A pseudo UDP session monitors the status of the UDP connection process. The pseudo UDP session is a virtual connection established for the UDP data flow when UDP packets are processed (UDP is a connectionless protocol).**
 - ❑ **The stateful inspection firewall intercepts data packets at the network layer, extracts the status information required by security policies from each application layer, and saves the information to the session table. The session table and subsequent connection requests related to the data packets are analyzed to make proper decisions.**

Firewall Classification: Stateful Inspection Firewall

- **Stateful inspection firewalls have the following advantages:**
 - **Outstanding performance for processing subsequent packets:** When checking data packets based on ACLs, a stateful inspection firewall records the connection status of the data flows. The subsequent packets in the data flows do not need to be checked based on the ACLs. Instead, the firewall checks the connection status records of the newly received packets according to the session table. After the check is passed, the connection status record is refreshed to avoid repeatedly checking the data packets with the same connection status. The sequence of records in the connection session table can be adjusted as required, which is different from an ACL whose records are arranged in a fixed sequence. Therefore, a stateful inspection firewall may perform fast search by using algorithms such as a binary tree or a hash algorithm, thereby improving transmission efficiency of the system.
 - **High security:** The connection status list is dynamically managed. After a session is complete, the temporary return packet entry created on the firewall is closed, ensuring real-time security of the internal network. In addition, the stateful inspection firewall uses real-time connection status monitoring technology to identify connection status factors such as response in the session table, which enhances system security.

Chapter
06

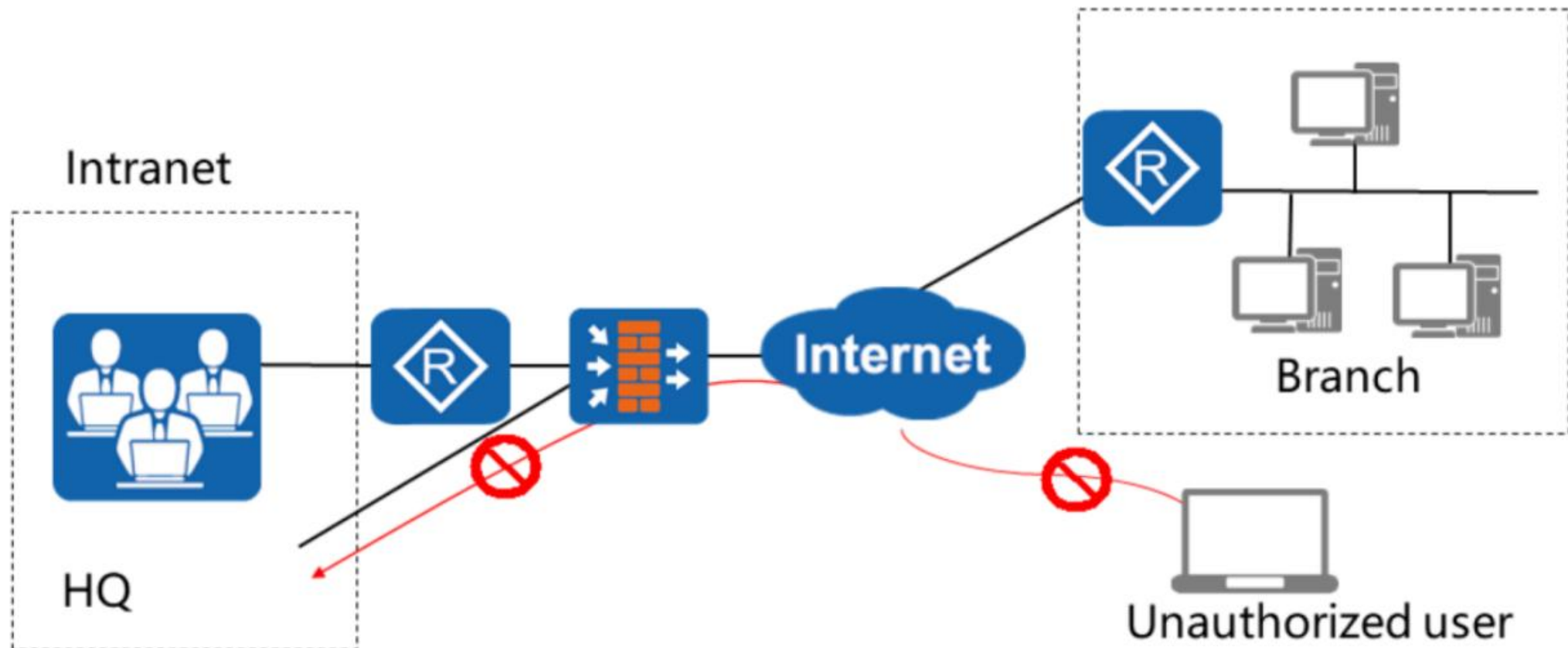
Firewall Networking Modes



Firewall Networking Modes

- **Mode 1:** A firewall only forwards packets and does not perform routing. The two service networks interconnected by the firewall must be in the same network segment. In this mode, the upstream and downstream interfaces of the firewall work at Layer 2 and do not have IP addresses.
- This networking mode avoids issues caused by topology changes. Deploy a firewall like a bridge on the network. There is no need to modify existing configurations. The firewall filters IP packets and protects users on the intranet.
- **Mode 2:** A firewall is located between the intranet and the Internet. The upstream and downstream service interfaces on the firewall work at Layer 3 and must be configured with IP addresses in different network segments. The firewall performs routing on the intranet and Internet, like a router.
- In this mode, the firewall supports more security features, such as NAT and UTM, but the original network topology must be modified. For example, the intranet users must modify their gateway configurations, or the route configuration on a router must be modified. Therefore, the design personnel should consider factors such as network reconstruction and service interruption when selecting a networking mode.

Packet Filtering Technology



Packet Filtering Technology

- When receiving a packet, the firewall obtains the header, compares the header with specified rules, and decides to forward or discard the packet.
- The core technique for packet filtering is the access control list (ACL).
- As a network security protection mechanism, packet filtering mainly controls the forwarding of various traffic on the network.
- A traditional packet-filtering firewall obtains header information (including the source and destination IP addresses, IP-bearing upper-level protocol number, and source and destination port numbers) from a packet to be forwarded, matches the predefined packet-filtering rules, and forwards or discards the packets according to the matching result.
- As the packet-filtering firewall matches packets with packet-filtering rules one by one and checks the packets, the forwarding efficiency is low. Currently, a firewall usually uses the stateful inspection mechanism to check the first packet of each connection. If the first packet passes the check (matching a packet-filtering rule), the firewall creates a session and directly forwards subsequent packets according to the session.

Chapter
06

Firewall Security Policies

- **Definition**

- Security policies control traffic forwarding according to specified rules and apply integrated content security detection to traffic.
- The rules focus on packet filtering.

- **Major Applications**

- Security policies control network communication through the firewall.
- Security policies control access to the firewall.

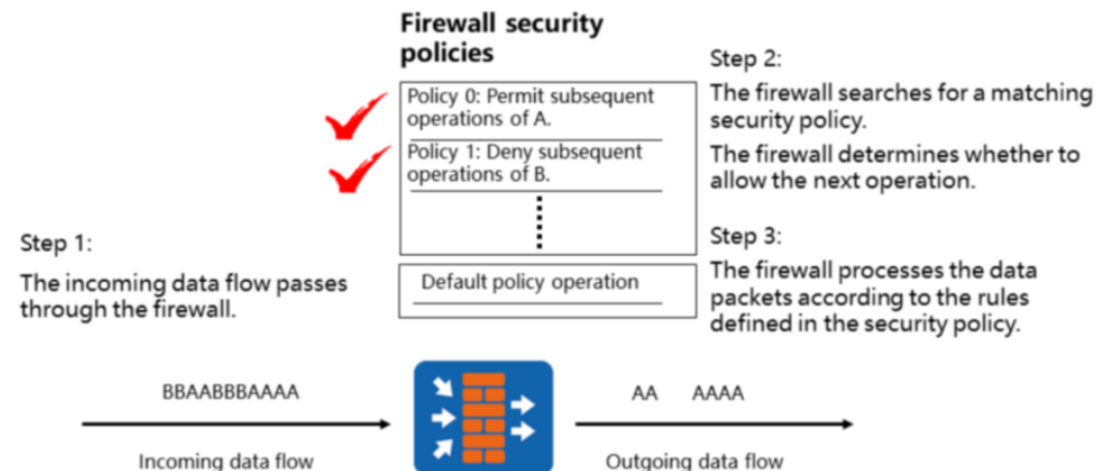
- The basic function of firewalls is to protect a network from being attacked by any untrust network while permitting legitimate communication between two networks. Security policies check passing data flows. Only the data flows that match the security policies are allowed to pass through firewalls.

- By using firewall security policies, you can control the access rights of the intranet to the Internet and control the access rights of the subnets of different security levels on the intranet. In addition, security policies can control the access to a firewall, for example, by restricting the IP addresses that can be used to log in to the firewall through Telnet and the web UI, and by controlling the communication between the NMS/NTP server and the firewall.

Chapter
06

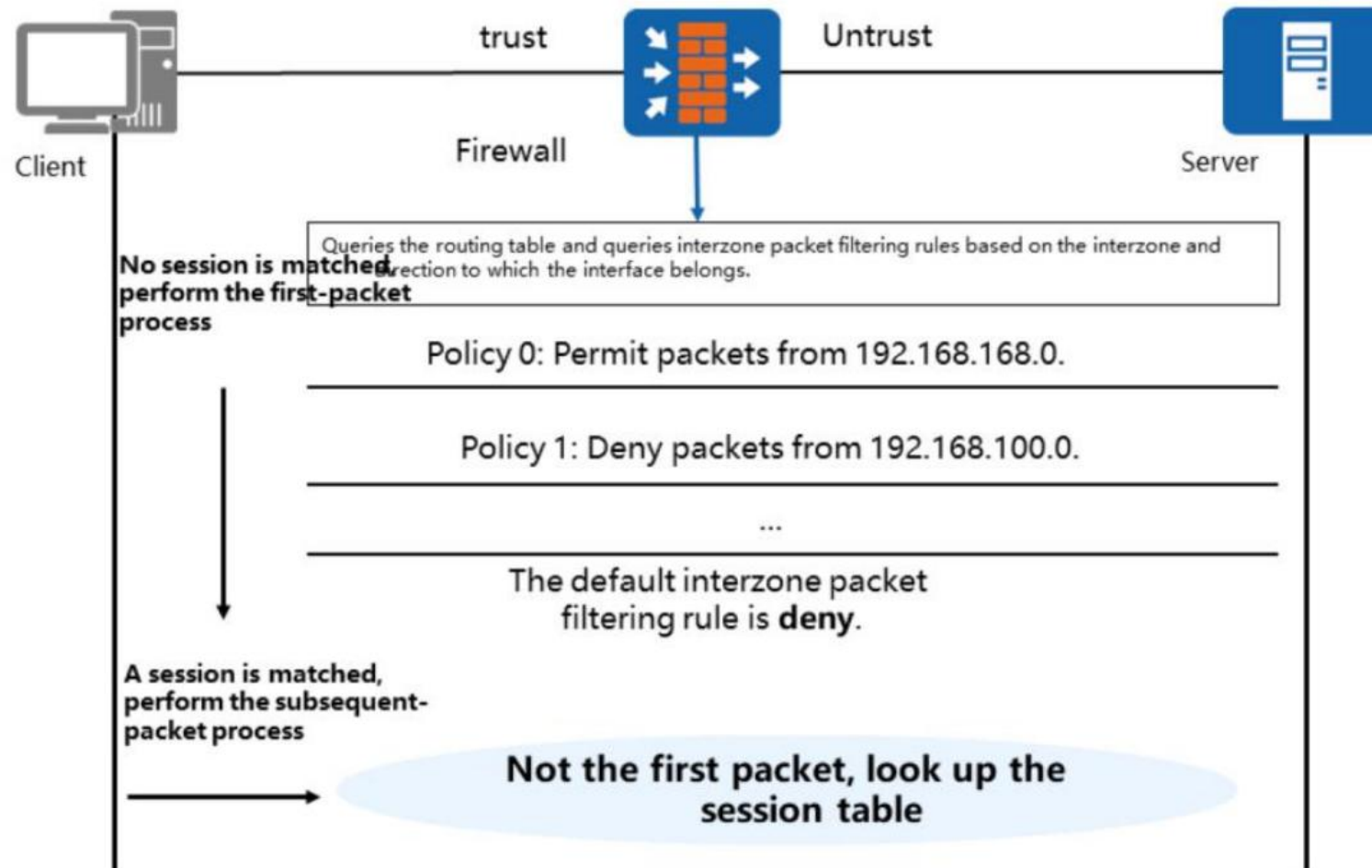
Firewall Security Policy Mechanism

- Function of firewall security policies: Filter the traffic passing through the firewall according to defined rules, and determine the next operation according to keywords.
- Security policies define rules for processing data flows on a firewall. The firewall processes data flows according to the rules. Therefore, the core functions of security policies are as follows: Filter the traffic passing through the firewall according to the defined rules, and determine the next operation performed on the filtered traffic based on keywords.
- In firewall application, security policies are a basic means of network security access to the data flows passing through the firewall, and determine whether subsequent application data flows are processed. The firewall analyzes traffic and retrieves the attributes, including the source security zone, destination security zone, source IP address, source region, destination IP address, destination region, user, service (source port, destination port, and protocol type), application, and schedule.



Chapter
06

Firewall Interzone Forwarding



Chapter
06

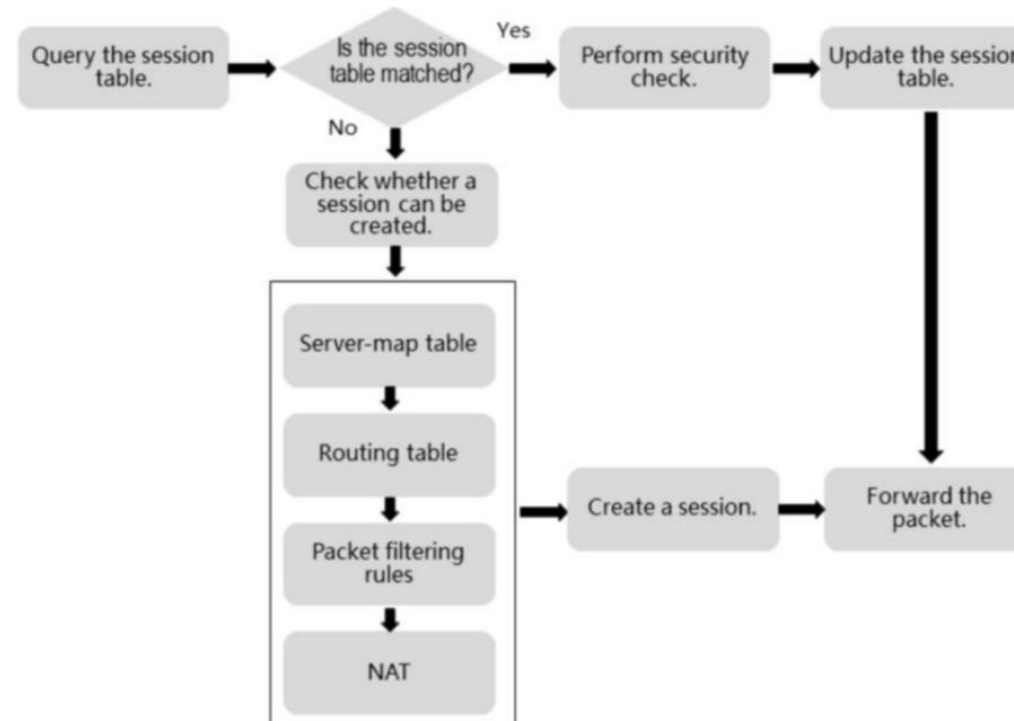
Firewall Interzone Forwarding

- Early packet-filtering firewalls match packets one by one with packet filtering rules. Firewalls check all received packets to decide whether to allow them to pass through. This mechanism greatly affects the forwarding efficiency and create forwarding bottlenecks on networks.
- Therefore, more and more firewalls use the stateful inspection mechanism for packet filtering. The stateful inspection mechanism checks and forwards packets based on data flows; a firewall checks the first packet of a data flow with packet-filtering rules, and records the result as the status of the data flow. For subsequent packets of the data flow, the firewall determines whether to forward (or perform content security detection) or discard the packets according to the status. This "status" is presented as a session entry. This mechanism improves the detection rate and forwarding efficiency of firewall products and has become the mainstream packet filtering mechanism.
- Generally, a firewall checks five elements (quintuple) in an IP packet. They are the source IP address, destination IP address, source port number, destination port number, and protocol type. By checking the quintuple of each IP packet, the firewall can determine the IP packets in one data flow. In addition to the quintuple, an NGFW also checks users, applications, and schedules of packets.
- Generally, in the three-way handshake phase, fields in addition to the quintuple in TCP data packets are calculated and checked. After the three-way handshake succeeds, the firewall matches subsequent packets with the quintuple in the session table to determine whether to allow the packets to pass through.

Chapter
06

Querying and Creating Sessions

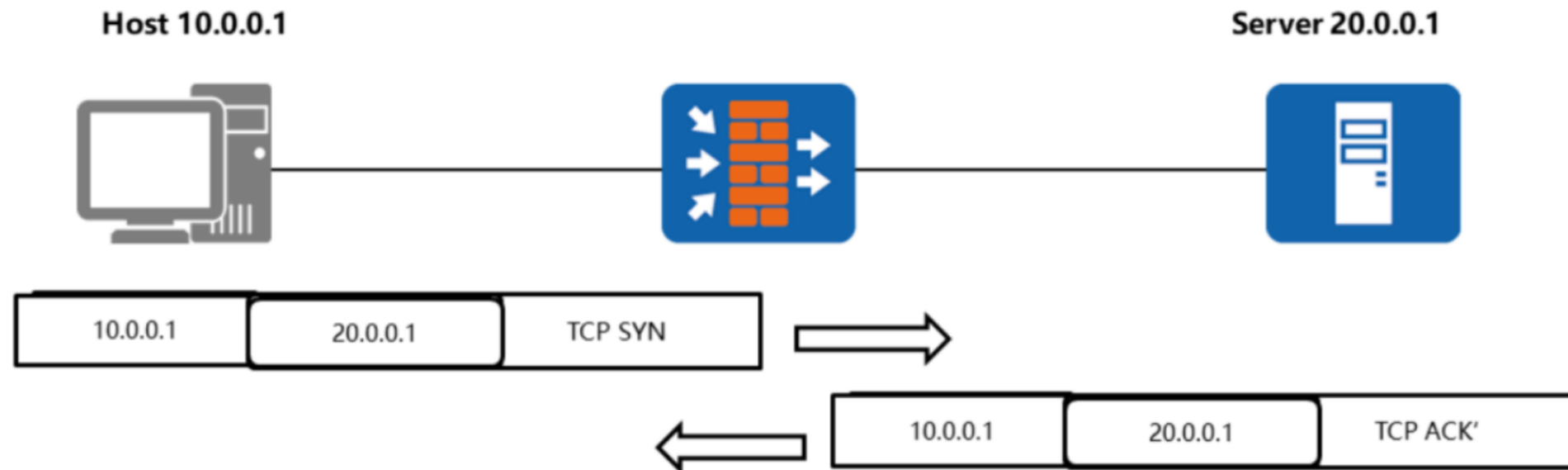
- Inspection on the packets that match a session takes much shorter time than on the packets that do not match any sessions. After the first packet of a connection is inspected and considered legitimate, a session is created and most subsequent packets are not inspected. This is where a stateful inspection firewall outperforms a packet inspection firewall in inspection and forwarding efficiency.



Chapter
06

Stateful Inspection Mechanism

- 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.
- 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.



Stateful Inspection Mechanism

- For TCP packets:
 - ❑ If stateful inspection is enabled and the first packet is a SYN packet, a session is created. If the first packet is not a SYN packet and does not match any session, the packet is discarded, and no session is created.
 - ❑ If stateful inspection is disabled, a session is created as long as a packet that does not match any session passes the inspections.
- For UDP packets:
 - ❑ UDP is a connectionless protocol. If a UDP packet does not match any session and passes the inspections, a session is created.
- For ICMP packets:
 - ❑ If stateful inspection is enabled, an ICMP echo message does not match any session, and no ICMP reply is sent in response, the ICMP echo message is discarded.
 - ❑ If stateful inspection is disabled, an ICMP echo message does not match any session, and no ICMP reply is sent in response, the ICMP echo message is processed as the first packet.

Session

- **Sessions are the basis of a stateful inspection firewall. A session is created for each data flow passing through the firewall. With the quintuple (source and destination IP addresses, source and destination ports, and protocol number) used as the key value, a dynamic session table is created to ensure the security of data flows forwarded between zones. The NGFW extends quintuple, with two elements (user and application) added.**
- **The session table on an NGFW contains seven elements:**
 - ☐ **Source IP address**
 - ☐ **Source port**
 - ☐ **Destination IP address**
 - ☐ **Destination port**
 - ☐ **Protocol number**
 - ☐ **User**
 - ☐ **Application**

Chapter 06

Session

Host 192.168.1.1:20000

Server 1.1.1.1:23



The packet matches the session, and the firewall allows the packet to pass.

Client Server

Source IP Address	Source Port	Destination IP Address	Destination Port	Protocol	User	Application
192.168.1.1	20000	1.1.1.1	23	TCP	abc	Telnet

Server Client

Source IP Address	Source Port	Destination IP Address	Destination Port	Protocol	User	Application
1.1.1.1	23	192.168.1.1	20000	TCP	abc	Telnet

Session: TCP 192.168.1.1:20000 1.1.1.1:23

Querying the Session Table

- Display brief information about the firewall session table.

```
<sysname> display firewall session table
Current Total Sessions : 2
  telnet VPN:public --> public 192.168.3.1:2855-->192.168.3.2:23
  http VPN:public --> public 192.168.3.8:2559-->192.168.3.200:80
```

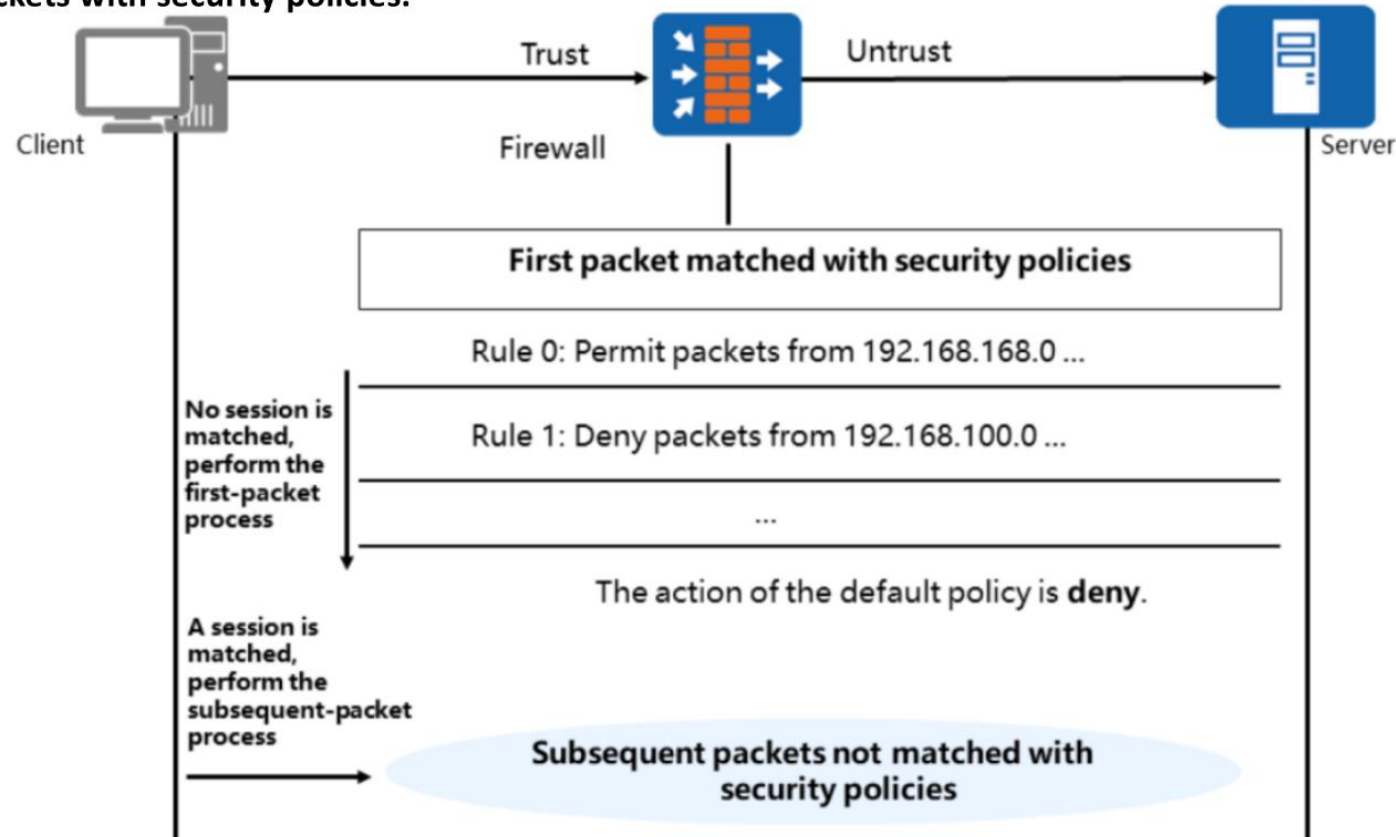
- Display detailed information about the firewall session table.

```
<sysname> display firewall session table verbose
Current Total Sessions : 1
  http VPN:public --> public ID: a48f3648905d02c0553591da1
  Zone: trust--> local TTL: 00:20:00 Left: 00:19:56
  Output-interface: InLoopBack0 NextHop: 127.0.0.1 MAC: 00-00-00-00-00-00
  <--packets:3073 bytes:3251431 -->packets:2881 bytes:705651
  128.18.196.4:1864-->128.18.196.251:80 PolicyName: test
```

Chapter
06

Security Policy Matching Principle

- In the first-packet process, the firewall matches the packet with security policies. In the subsequent-packet process, the firewall does not match the packets with security policies.





Thank You