2019/5/14 Security Level:

NETWORK SECURITY FIREWALL & NAT

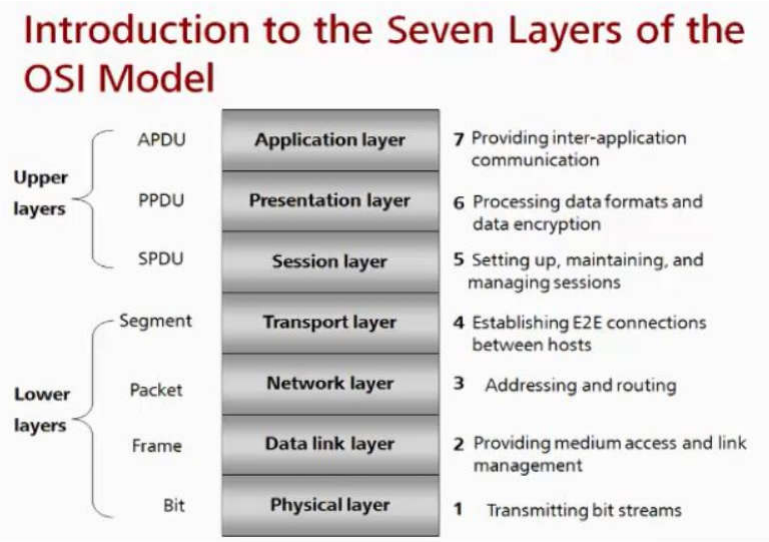
Huawei Turkey Enterprise & Openlab

www.huawei.com

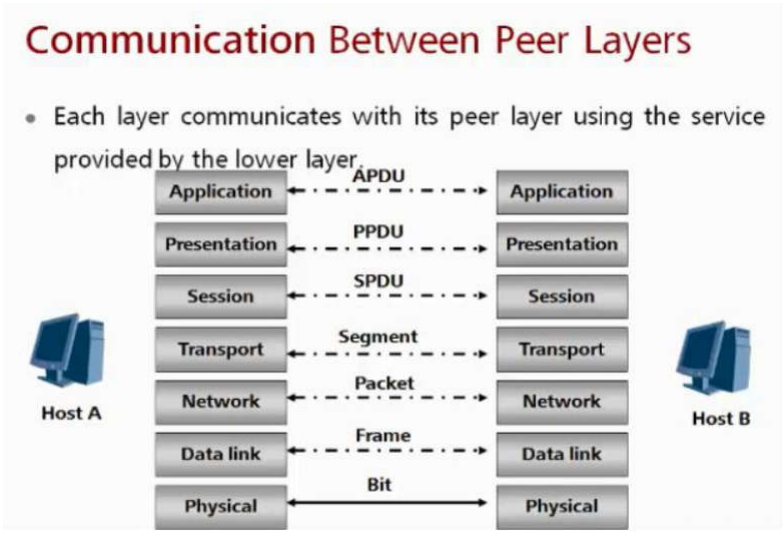
TRAINER: AHMET KAYHAN ŞEKER / 00263551

Contents

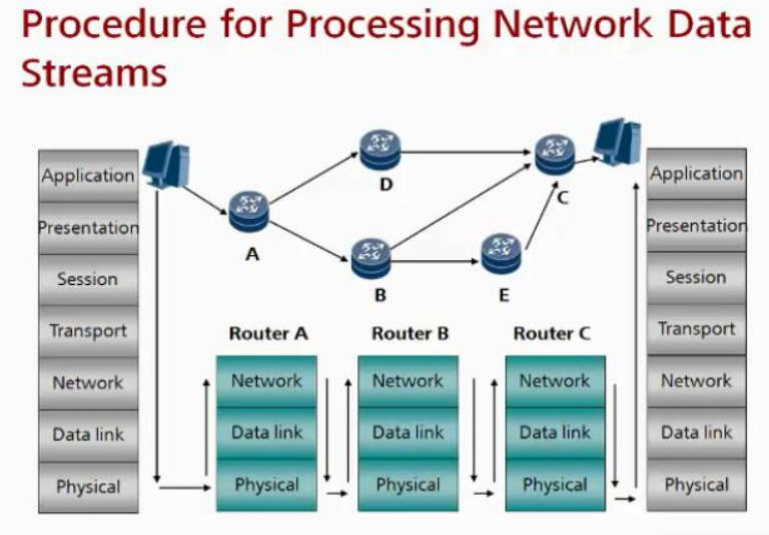
Network Security



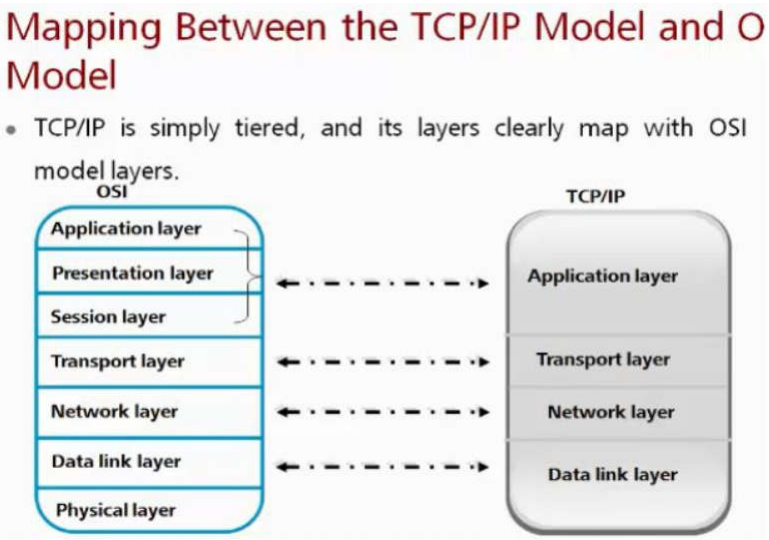
Network Security-2



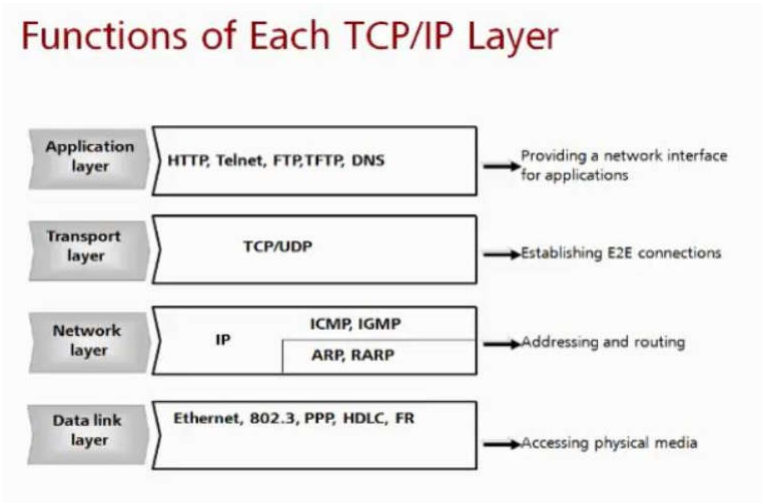
Network Security-3



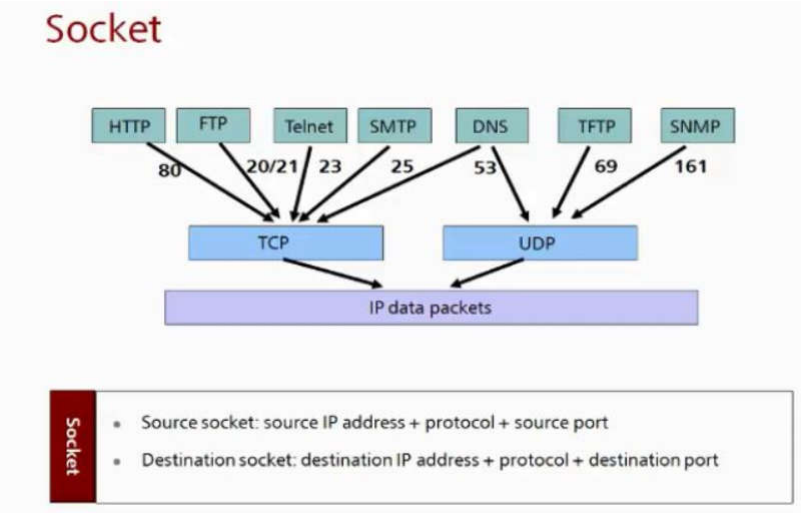
Network Security-4



Network Security-5



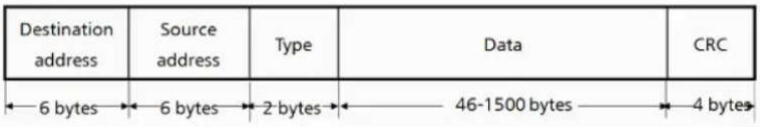
Network Security-6



Network Security-7

Data Link Layer Protocol

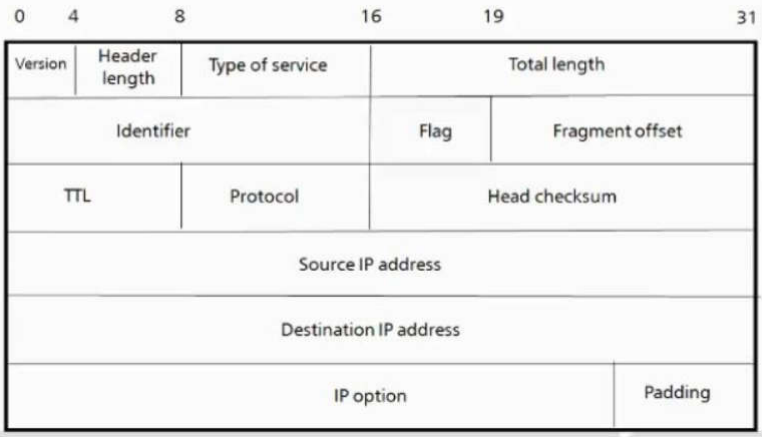
- Ethernet protocol encapsulation



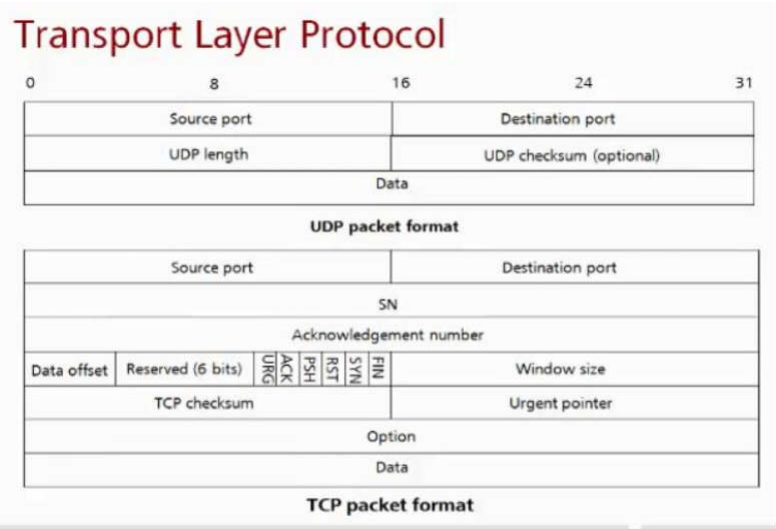
- Type
  - Type 0800: indicates IP.
  - Type 0806: indicates ARP.
  - Type 8035: indicates RARP.

Network Security-8

Network Layer Protocol

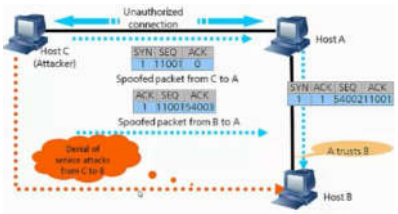


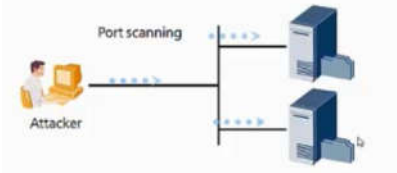
Network Security-9

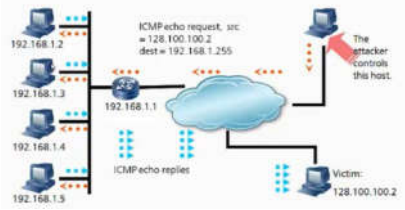


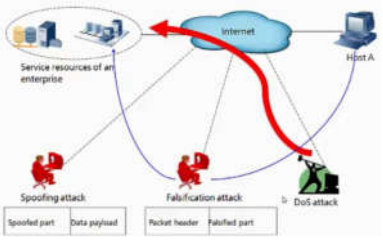
Network Security-9

- Mac Spoofing Attack
- Mac Flooding Attack
- Arp Spoofing Attack
- IP Spoofing Attack
- Smurf Attack
- ICMP Redirect and Unreachable Packet Attack
- IP Sweep Attack
- TCP Spoofing Attack
- SYN Flood Attack
- UDP Flood Attack
- Port Scanning Attack
- Buffer Overflow Attack
- Web Application Attack
- SQL Injection Attack
- DoS & DDoS Attack

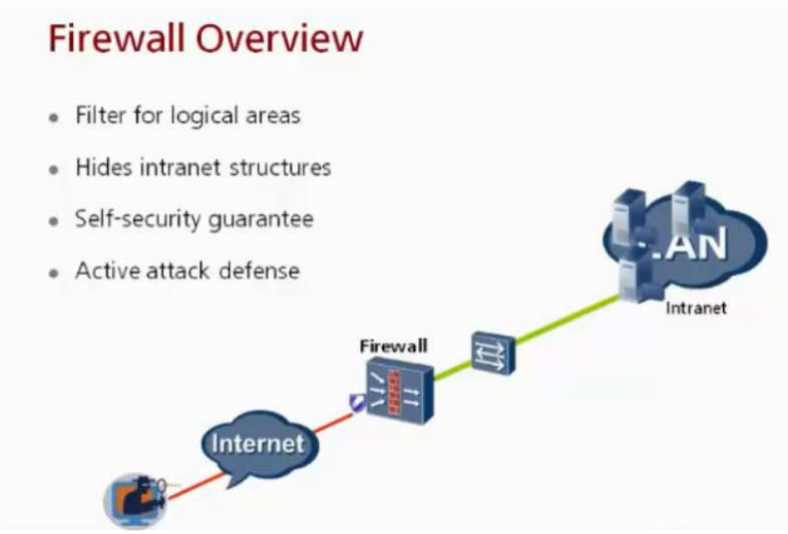




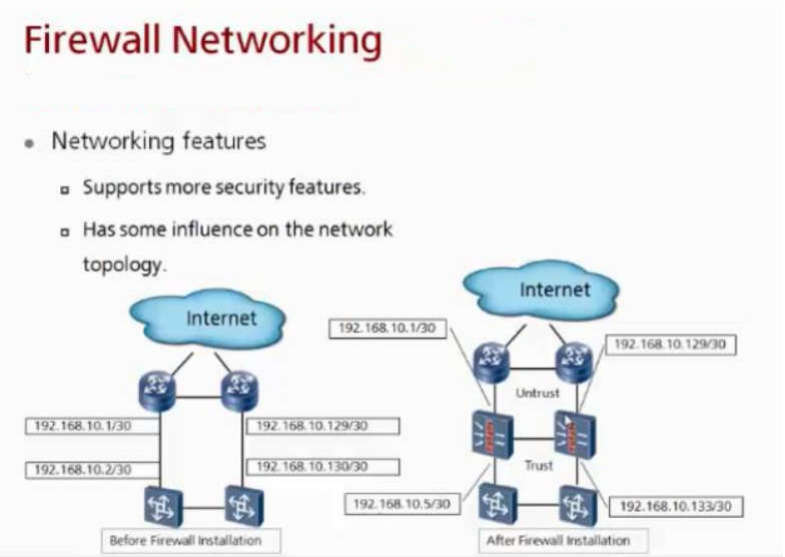




FIREWALL



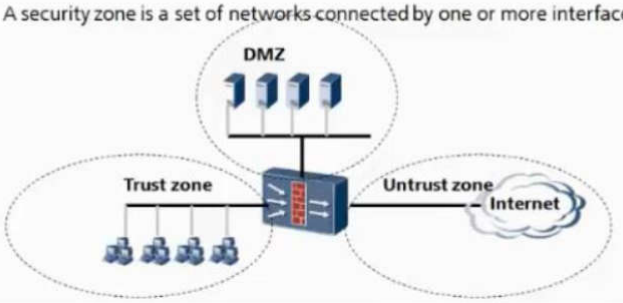
FIREWALL-2



FIREWALL-3

What Is a Security Zone

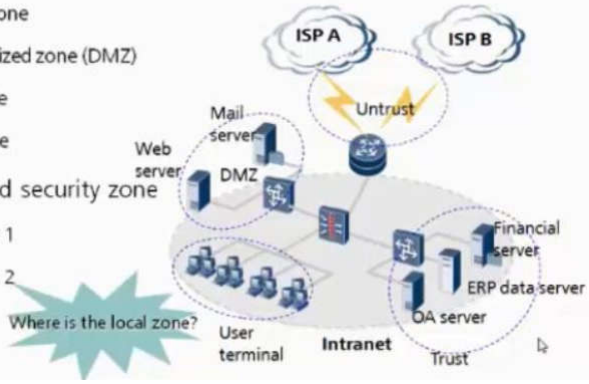
- Security zone (Zone)
  - A security zone (also named zone) is a local logical security area, based on which most security policies are implemented.
  - A security zone is a set of networks connected by one or more interfaces.



FIREWALL-4

Definition of Security Zones

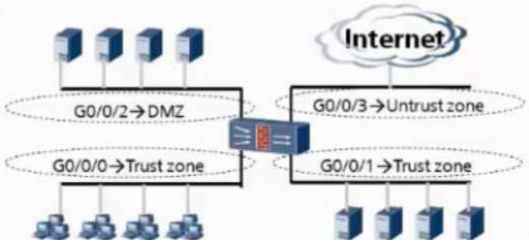
- Default security zones
  - Untrust zone
  - Demilitarized zone (DMZ)
  - Trust zone
  - Local zone
- User-defined security zone
  - User Zone 1
  - User Zone 2



FIREWALL-5

Relationship Between Firewall Security Zones and Interfaces

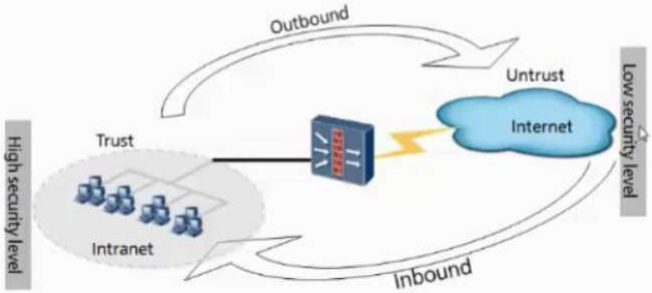
- Whether can the firewall have two security zones with the same security level?
- Whether does the firewall allow one physical interface to belong to two different security zones?
- Whether can different interfaces of the firewall belong to the same security zone?



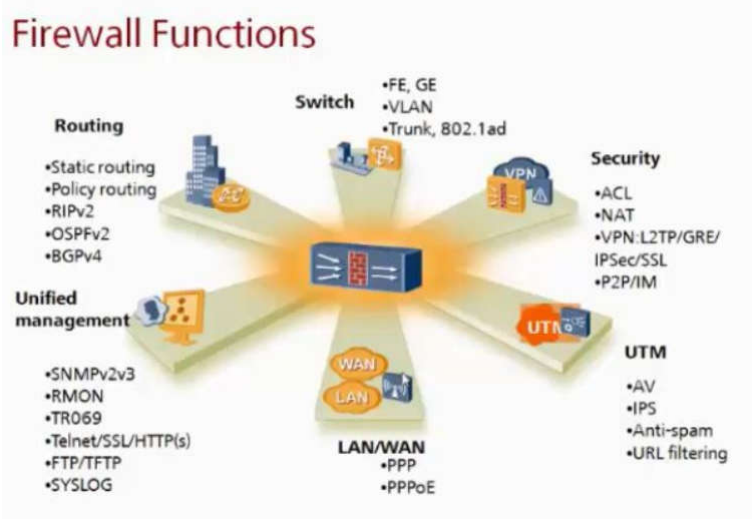
FIREWALL-6

Definition of Inbound and Outbound Directions

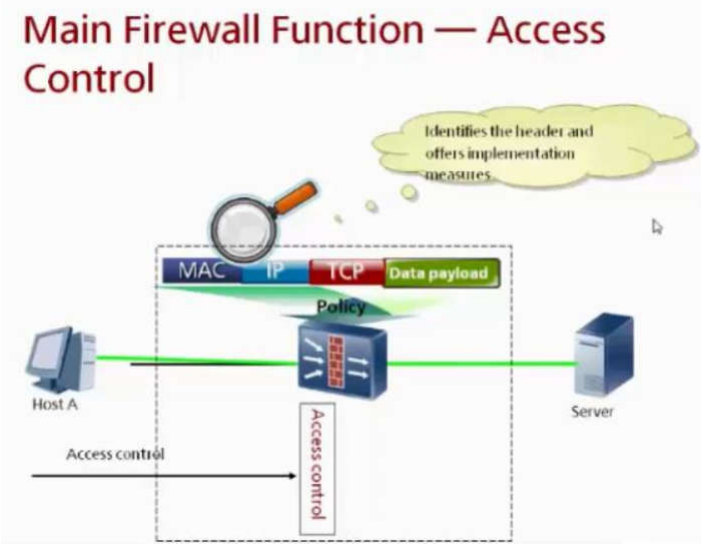
- What is the inbound direction?
- What is the outbound direction?



FIREWALL-7



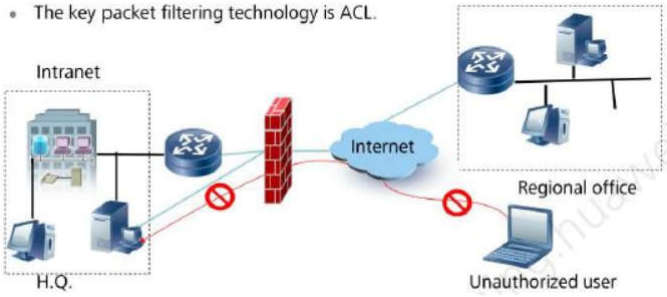
FIREWALL-8



FIREWALL-9

Packet Filtering Technology

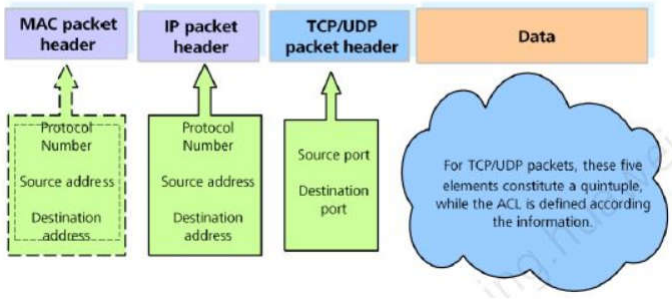
- For the packets to be forwarded, the firewall obtains the packet header and compares the header information against the defined rules to determine to forward or discard the packets.
- The key packet filtering technology is ACL.



FIREWALL-10

Packet Filtering Mechanism

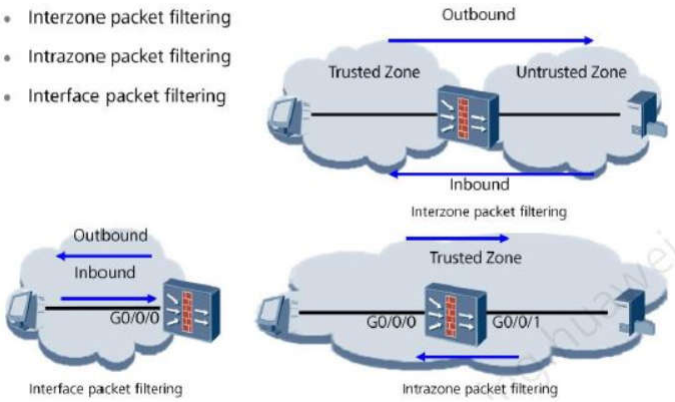
- The TCP/IP packet format is shown in the following figure. In this figure, the upper-layer protocol is TCP/UDP.



FIREWALL-11

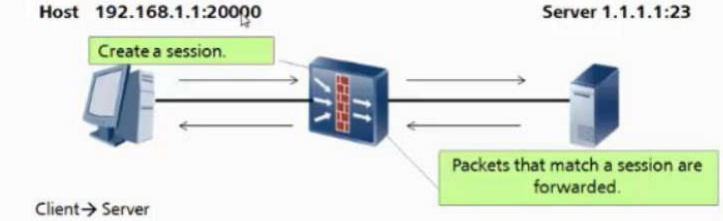
Packet Filtering Classification

- Interzone packet filtering
- Intrazone packet filtering
- Interface packet filtering



FIREWALL-12

Session Table



Client→ Server

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

Server→ Client

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

FIREWALL-13

Checking the Session Table

- **display 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
```

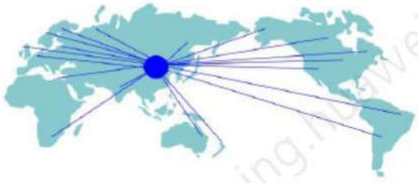
- **display firewall session table verbose**

```
<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
```


NAT

Background Information

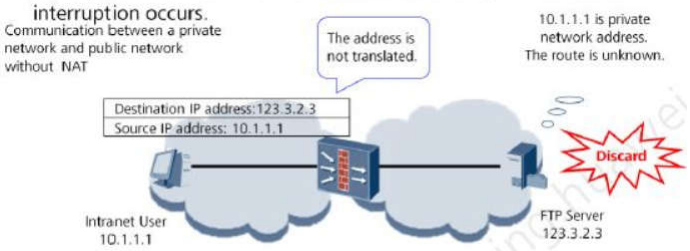
- IPv4 addresses are being depleted.
- IPv6 addresses cannot immediately replace IPv4 addresses in a large scale.
- To extend the IPv4 lifespan, various technologies emerge continuously. NAT is one of the technologies.



NAT-2

Why NAT is Required?

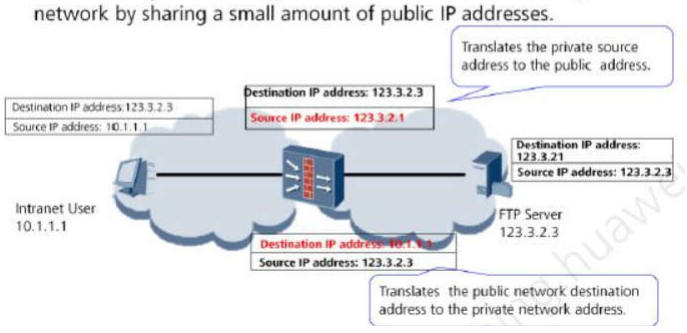
- NAT translates a large number of private network addresses into a small amount of public network addresses, ensuring communication services and saving IP address resources.
- Private network addresses are unreachable on public networks. If these private network addresses are not translated, communication interruption occurs.



NAT-3

Basic Principles of NAT

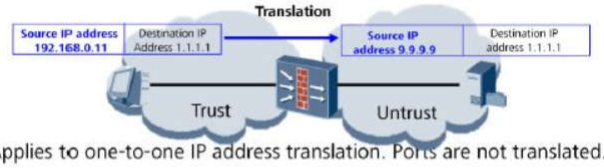
- NAT translates the private network source address or destination address in the IP packet header to a public network address. It enables a large number of private IP addresses to access the public network by sharing a small amount of public IP addresses.



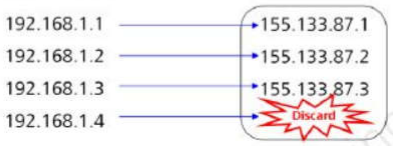
NAT-4

Source NAT - Address pool mode - 1

- Source NAT without translate ports



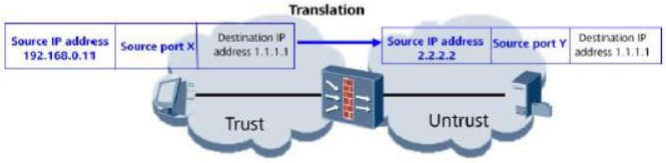
- Applies to one-to-one IP address translation. Ports are not translated. Also call it No-PAT mode.



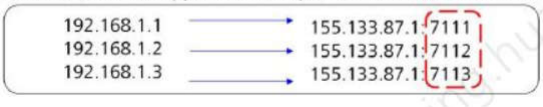
NAT-5

Source NAT - Address pool mode - 2

- Source NAT with translate ports



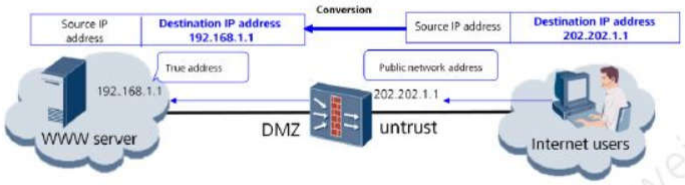
- Maps different private network addresses to different ports of a public network address and applies to multiple-to-one IP address translation.



NAT-6

NAT Server-Internal Server

- The NAT Server function uses a public network address to represent the internal server address.



- On the firewall, a dedicated public network address is configured for the internal server to represent the private network address. For Internet users, the Internet address configured on the firewall is the server address.

NAT-7

Firewall Source NAT Configuration (CLI)

- Configure an interzone access policy.
  - Configure the source address as the network segment 192.168.0.0/24. (omitted the detailed procedures)
- Configure a NAT address pool.

```
[USG6600] nat address-group 1
[USG6600-nat-address-group-1] section 202.169.10.2 202.169.10.6
```

- Configure a NAT outbound policy.

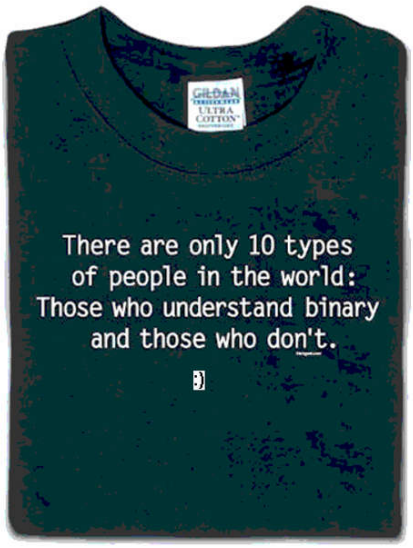
```
[USG6600] nat-policy
[USG6600-policy-nat] rule name nat1
[USG6600-policy-nat-rule-nat1] source-zone trust
[USG6600-policy-nat-rule-nat1] destination-zone untrust
[USG6600-policy-nat-rule-nat1] source-address 192.168.0.0 24
[USG6600-policy-nat-rule-nat1] action nat address-group 1
```

NAT-8

Firewall NAT Server Configuration (CLI)

- **Configure the interzone packet filtering policy.**

```
[USG] security-policy
[USG -policy-security] rule name p1
[USG -policy-security-rule-p1] source-zone untrust
[USG -policy-security-rule-p1] destination-zone dmz
[USG -policy-security-rule-p1] destination-address 192.168.20.2 32
[USG -policy-security-rule-p1] service http
[USG -policy-security-rule-p1] action permit
[USG -policy-security] rule name p2
[USG -policy-security-rule-p2] source-zone untrust
[USG -policy-security-rule-p2] destination-zone dmz
[USG -policy-security-rule-p2] destination-address 192.168.20.3 32
[USG -policy-security-rule-p2] service ftp
[USG -policy-security-rule-p2] action permit
```

THANK YOU

www.huawei.com