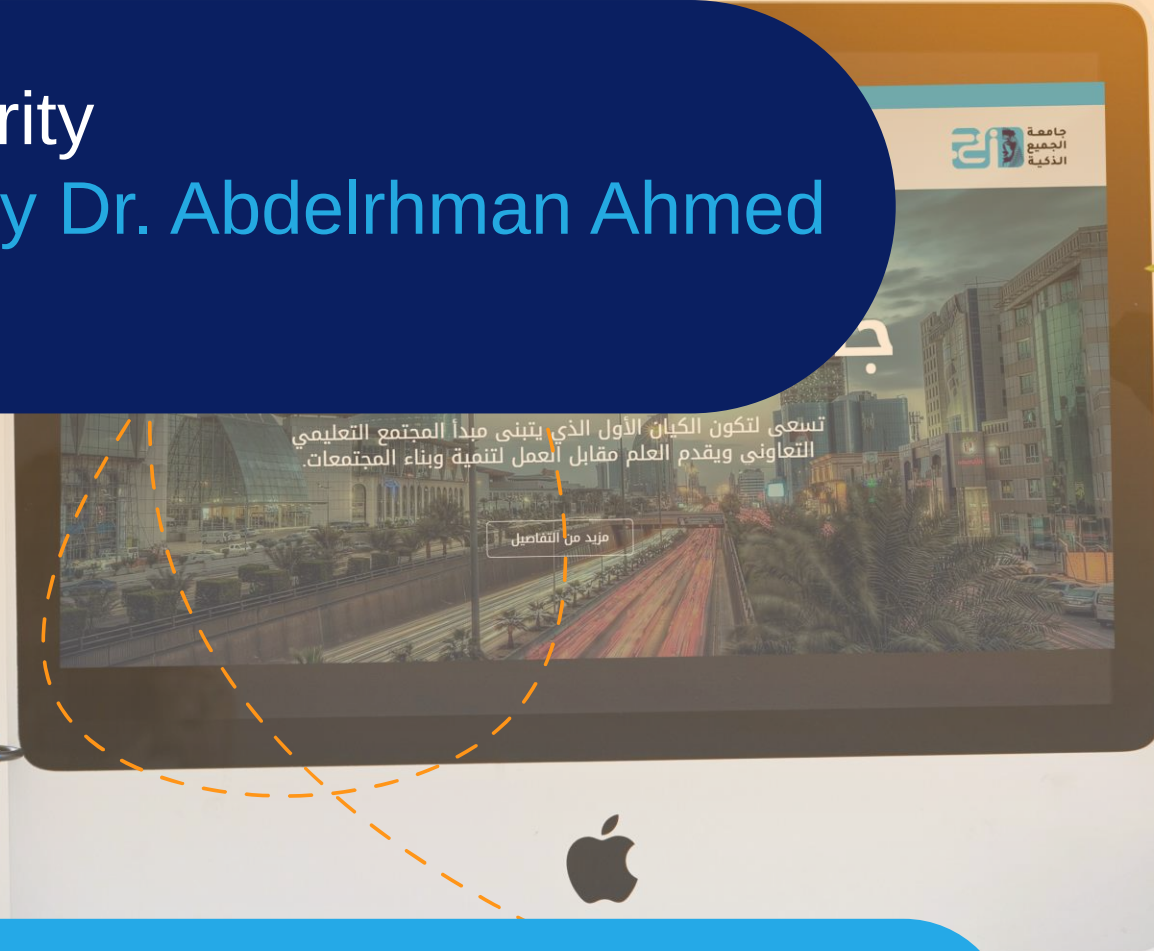


HCIA Security

Prepared by Dr. Abdelrhman Ahmed

Lecture 7



Network Address Translation



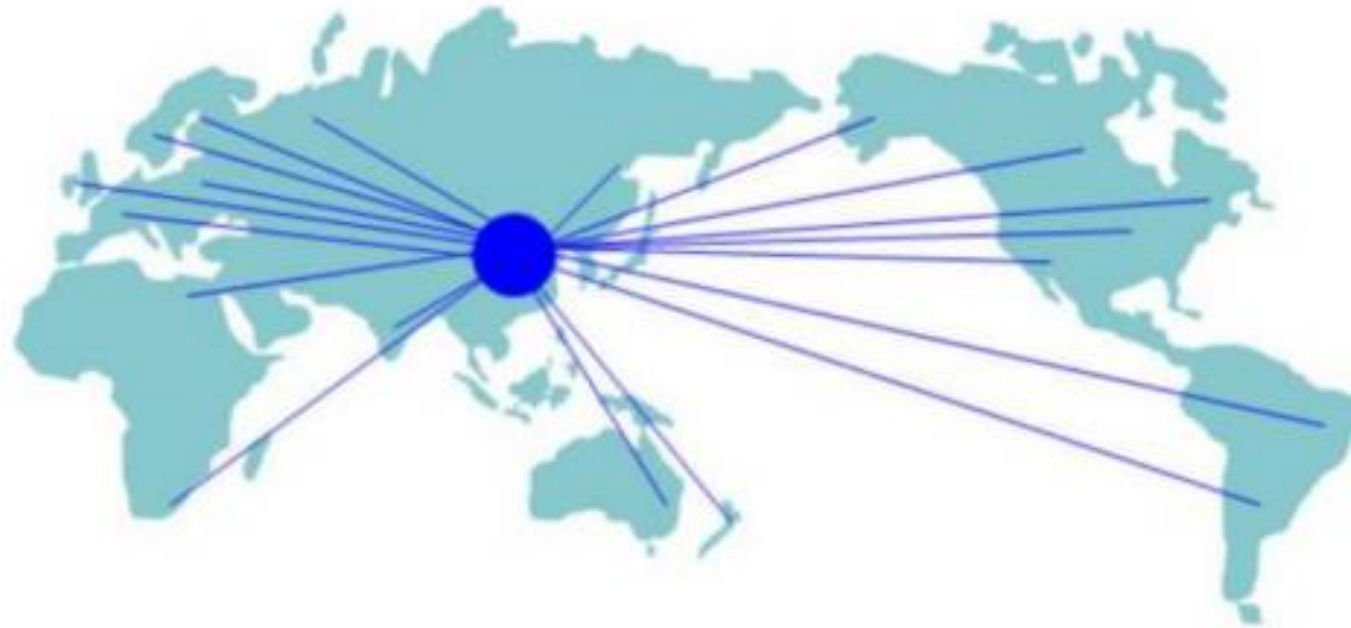
جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- **Network address translation (NAT) translates an IP address carried in the header of an IPv4 packet into another IP address. Generally, NAT is used to translate private addresses into public addresses so that devices can communicate across private and public networks.**
- **To alleviate the public IPv4 address shortage caused by Internet expansion, NAT emerged as a temporary solution.**

Objectives

- **Upon completion of this course, you will be able to:**
 - ☐ **Recognize NAT application scenarios.**
 - ☐ **Understand how NAT works.**
 - ☐ **Configure NAT on firewalls.**

- IPv4 addresses are depleted.
- IPv6 cannot completely replace IPv4 immediately.
- Technologies to mitigate IPv4 address exhaustion (NAT, for example) continue to emerge.



- In the early 1990s, relevant Request For Comments (RFC) documents began raising the possibility of IP address exhaustion. As more and more IPv4 addresses are requested, driven in part by the Internet's rapid growth due to TCP/IP-based web applications, sustainable development of the Internet is becoming a major challenge. To address this challenge, IPv6 is developed as the successor to IPv4. In contrast to IPv4, which defined an IP address as a 32-bit value, IPv6 addresses have a size of 128 bits. For network applications, IPv6 has a significantly larger address space compared to IPv4. However, IPv6 has a long way to go before it can completely replace IPv4, due to the immature technologies and huge update costs associated with IPv6.
- Because IPv6 will not completely replace IPv4 immediately, certain workarounds are required to extend the use of IPv4. For example, classless inter-domain routing (CIDR), variable length subnet mask (VLSM), and NAT can be used.
- Private addresses are used to implement address reuse and increase the utilization of IP address resources. Defined in RFC 1918, the following private addresses are reserved for private networks:
 - ❑ Class A: 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
 - ❑ Class B: 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
 - ❑ Class C: 192.168.0.0 to 192.168.255.255 (192.168.0.0/16)
- Private addresses are used on private networks, whereas public addresses are used on public networks (for example, the Internet). To allow communication between private and public addresses, NAT must be used to translate the addresses.

- **Advantages:**

- ☐ IP addresses can be reused.
- ☐ The address translation process is transparent to users.
- ☐ Privacy protection is available to internal users.
- ☐ Load balancing among internal servers is available.

- **Disadvantages:**

- ☐ Network monitoring is more difficult.
- ☐ Some applications are restricted.

- In addition to address reuse, NAT continues to evolve and provides other advantages. The main advantages and disadvantages of NAT are as follows:

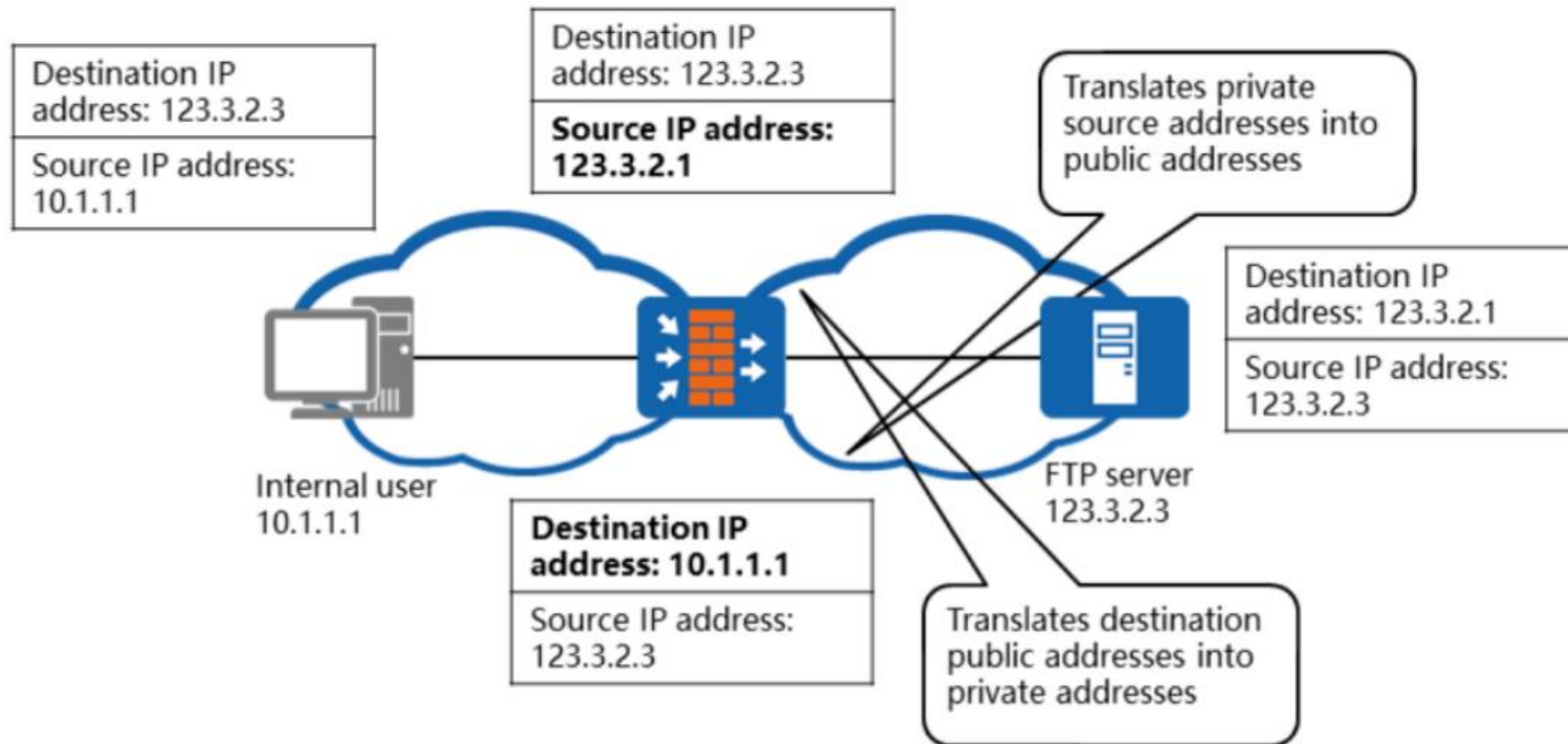
- **Advantages:**

- ❑ Numerous hosts on a local area network (LAN) can use a few public addresses to access external resources, and internal World Wide Web (WWW), File Transfer Protocol (FTP), and Telnet services can be used by external networks.
- ❑ 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 can be configured for load balancing, reducing the pressure of each server in case of heavy traffic.

- **Disadvantages:**

- ❑ NAT cannot be performed if the packet header is encrypted. For example, for an encrypted FTP connection, the port command cannot translate IP addresses.
- ❑ Network supervision becomes more difficult. For example, tracing a hacker who attacks a server on the public network from a private network is difficult because the IP address of the hacker has been NAT.

- NAT translates the source and destination IP addresses in IP packet headers so that numerous private addresses can access the public network through a limited number of public addresses.



- NAT translates the IP addresses in IP packet headers to other IP addresses so that users on internal network can access external networks. Generally, every NAT device maintains an address translation table. The IP addresses of packets that pass through the NAT device and require address translation will be translated against this table. The NAT mechanism involves the following processes:
 - Translate the IP addresses and port numbers of internal hosts into the external addresses and port numbers of the NAT device.
 - Translate the external addresses and port numbers into the IP addresses and port numbers of internal hosts.
- That is, NAT implements translation between private address+port number and public address+port number.
- NAT devices are located between internal and external networks. The packets exchanged between internal hosts and external servers all pass through the NAT devices. Common NAT devices include routers and firewalls.

- NAT is divided into three categories based on application scenarios.
 - **Source NAT:** enables multiple private network users to access the Internet at the same time.
 - **Address pool mode:** The public addresses in the address pool are used to translate users' private addresses. This mode applies when many private network users access the Internet.
 - **Outbound interface address mode (easy IP):** The IP addresses of internal hosts are translated into the public address of an outbound interface on the public network. This mode applies when the public address is dynamically allocated.
 - **Server mapping:** enables external users to access servers on private networks.
 - **Static mapping (NAT server):** maps one private address to one public address.

This mode applies when public network users access servers on private networks.

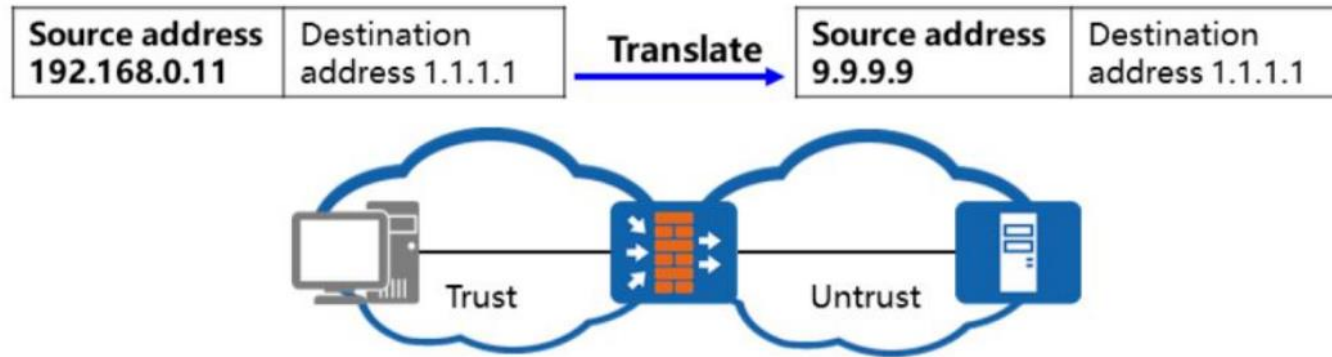
Source
NAT

- Address pool mode
- Outbound interface address mode (easy IP)

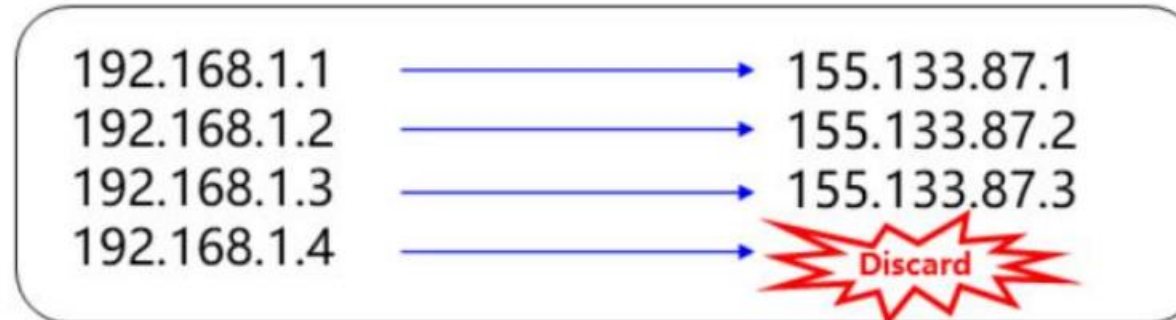
Server
mapping

- Static mapping (NAT server)

- Address pool mode without port translation

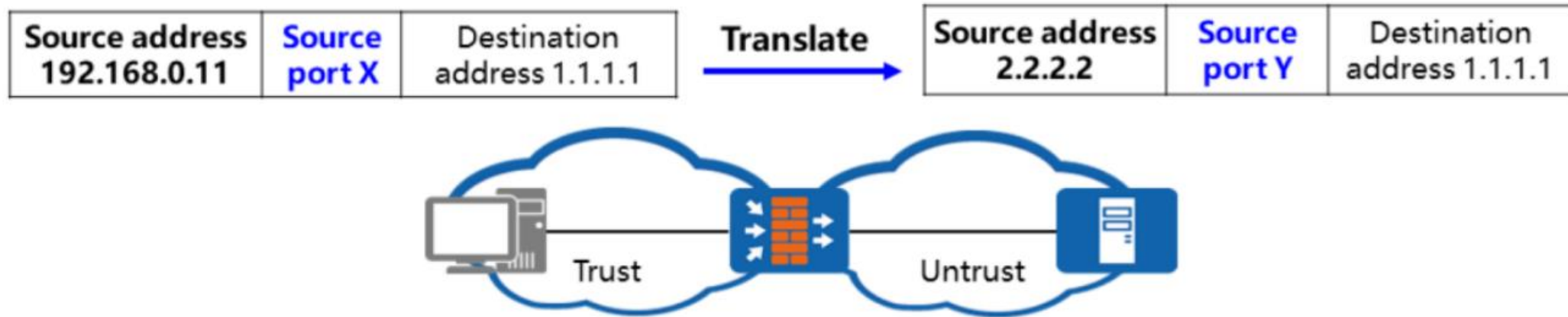


- One-to-one address translation is performed without port translation.



- **Source NAT translates the source IP address (the internal host's address) in IP packet header into a public address. This enables numerous internal hosts to access external resources through limited public addresses and effectively hides the host IP addresses on the LAN.**
- **The address pool mode without port translation is implemented using a NAT address pool that contains multiple public addresses. Only IP addresses are translated, and only one private address is mapped to a public address. If all addresses in the address pool are allocated, NAT cannot be performed for the remaining internal hosts until the address pool has available addresses.**

- Address pool mode with port translation

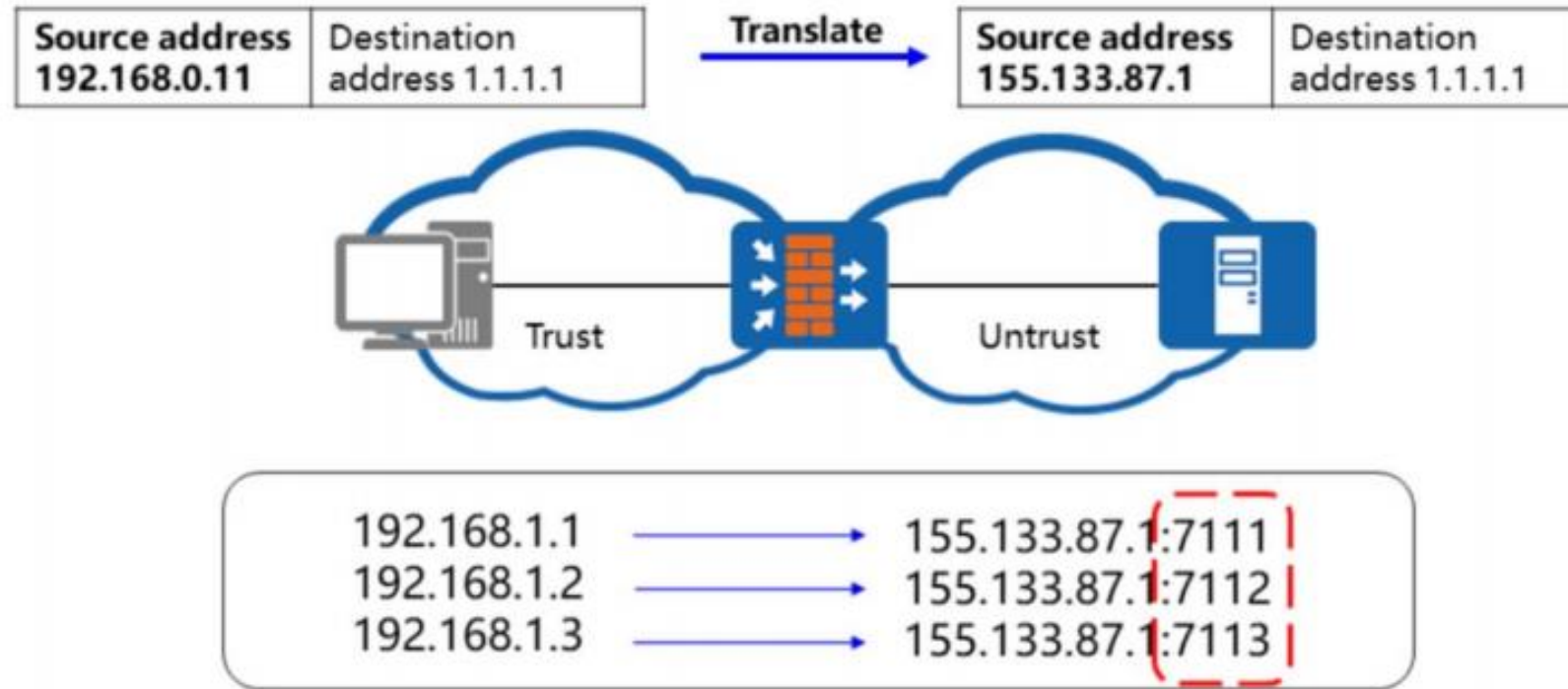


- Different private addresses are mapped to the same public address but different port numbers to implement many-to-one address translation.

192.168.1.1	→	155.133.87.1:7111
192.168.1.2	→	155.133.87.1:7112
192.168.1.3	→	155.133.87.1:7113

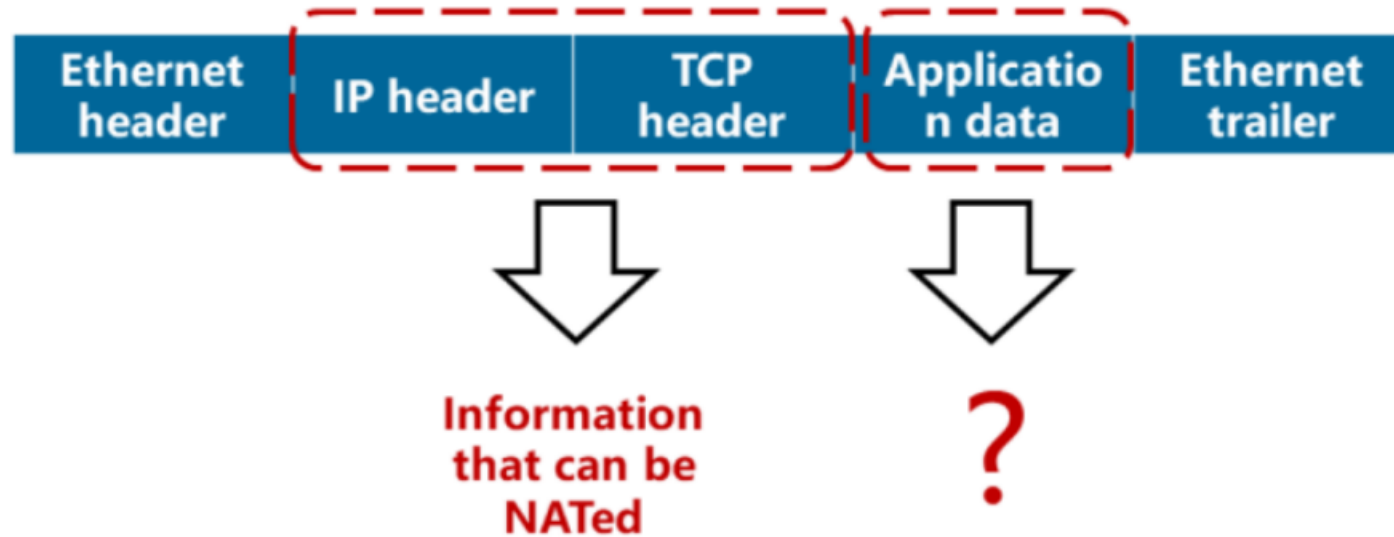
- The address pool mode with port translation is implemented using a NAT address pool that contains one or more public addresses. Addresses and port numbers are both translated so that private addresses share one or more public addresses.
- Because addresses and port numbers are both translated, multiple users on a private network can share one public address to access the Internet. The firewall can distinguish users based on port numbers, so numerous users can access the Internet at the same time. This technology uses Layer 4 information to extend Layer 3 addresses. Theoretically, 65,535 private addresses can be translated into the same public address because 65,535 ports are available for each address. The firewall can map data packets from different private addresses to different port numbers of one public address. Compared with one- to-one or multi-to-multi address translation, this mode greatly improves IP address utilization. Therefore, the address pool mode with port translation is most commonly used.

- Outbound interface address mode (easy IP)

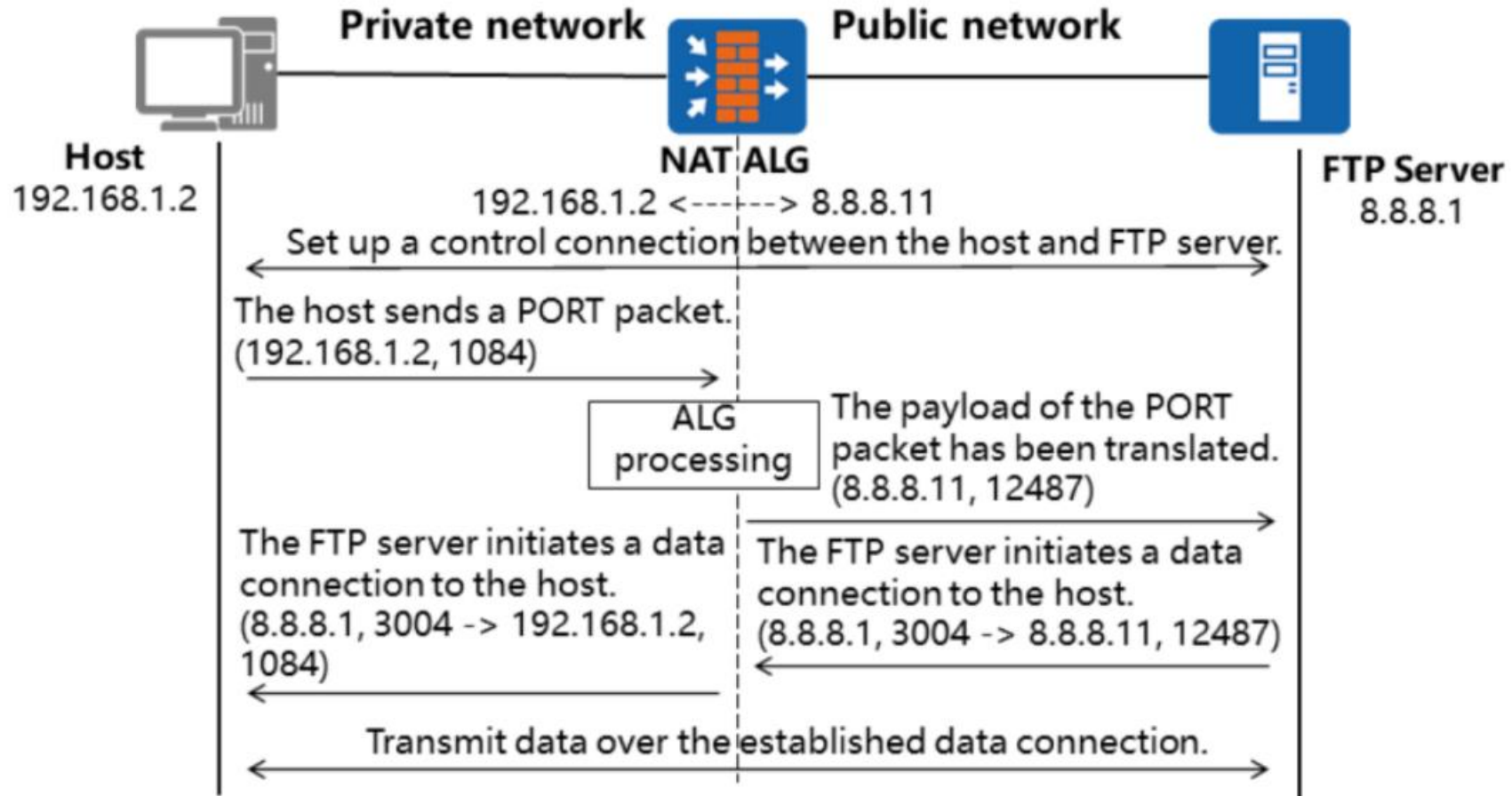


- Easy IP translates private addresses into the public address of the outbound interface, without the need of configuring a NAT address pool. Addresses and port numbers are both translated so that private addresses share public addresses of outbound interfaces.

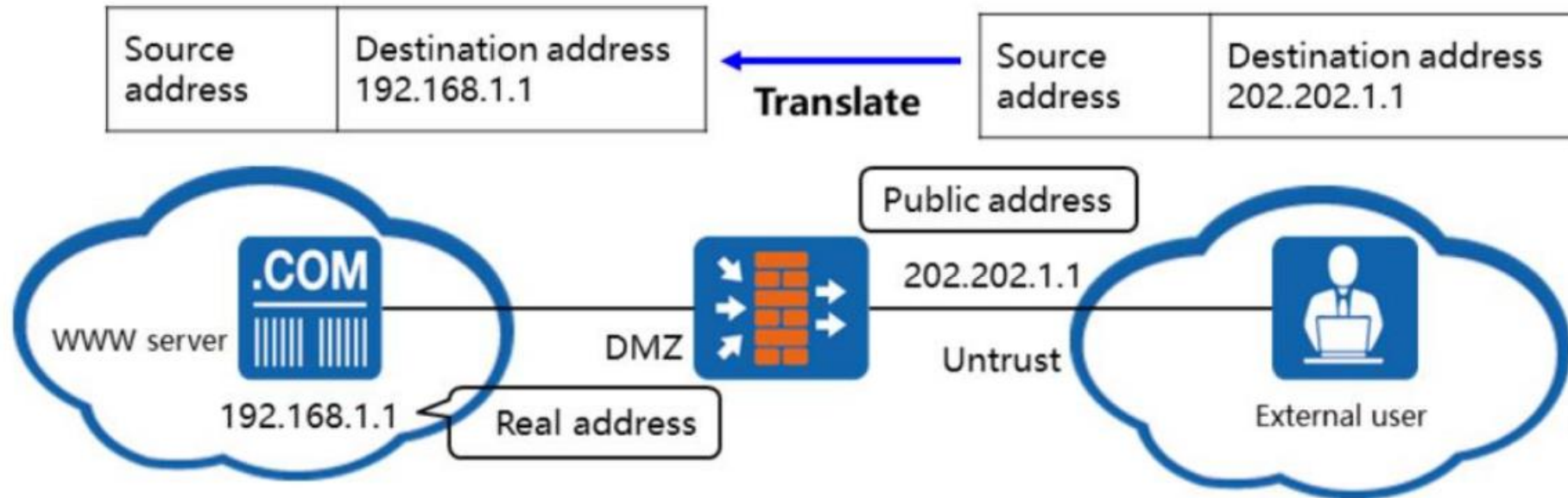
- The NAT application-level gateway (ALG) is a translation proxy used for certain application protocols and can translate the address and port number carried in application layer data.



- NAT ALG application in FTP active mode



- The NAT server function uses a public address to represent the private address of an internal server.



- On the firewall, a public address is configured to represent the server's private address. External users access the server through this public address.

- In the NAT server function, NAT hides the topology of an internal network. That is, NAT masks the internal hosts. In practice, external users may need to access the internal hosts, for example, a WWW server. External hosts, however, do not have routes destined for the internal hosts. In this case, the NAT server function can be applied.
- NAT allows you to add internal servers flexibly. For example, a public address such as 202.202.1.1 or an IP address and port number such as 202.202.1.1:8080 can be used as the external address of the web server.
- When external users access internal servers, the following operations are involved:
 - ❑ The firewall translates destination addresses of external users' request packets into private addresses of internal servers.
 - ❑ The firewall translates source addresses (private addresses) of internal servers' response packets into public addresses.
- The firewall supports security zone-based internal servers. For example, if the firewall provides access to external users on multiple network segments, you can configure multiple public addresses for an internal server based on security zone configurations. By mapping different levels of the firewall's security zones to different external network segments and configuring different public addresses for the same internal server based on security zones, you can enable external users on different network segments to access the same internal server.

- After the NAT server is configured, the device automatically generates server map entries that map public and private addresses.

```
[NGFW]nat server server1 protocol tcp global 202.202.1.1 inside 192.168.1.1
```

↓
Protocol
carried
over IP

↓
Post-NAT
public
address

↓
Private
address

- Example: server map entry

```
Type: Nat Server, ANY ->202.202.1.1:21[192.168.1.1:21], Zone:---, protocol:tcp
Vpn: public --> public
Type: Nat Server Reverse, 192.168.1.1[202.202.1.1] -> ANY, Zone:---,
protocol:tcp Vpn: public --> public, counter: 1
```

- Generally, if strict packet filtering is configured, the device permits only internal users to proactively access external networks. In practice, however, this may prevent successful file transfers in FTP. For example, when FTP in port mode is used, the client needs to proactively initiate a control connection to the server, and the server needs to proactively initiate a data connection to the client. If packet filtering configured on the device allows packets through in only one direction, FTP file transfer will fail.
- To resolve such issues, the USG device introduces the server map table. The server map is based on triplets and is used to record data connection mappings negotiated using control data or address mappings configured for NAT to allow external users to access internal networks.
- If a data connection matches an entry in the server map table, the device will forward the associated packet without looking up the session table.
- After the NAT server is configured, the device automatically generates server map entries that record the mappings between public and private addresses.
- If no-reverse is not specified, a pair of forward and return static server map entries is generated for each valid NAT server. If no-reverse is specified, the valid NAT server generates only the forward static server map entry. If a NAT server is deleted, the associated server map entries are deleted at the same time.
- After No PAT is configured, the device creates a server map table for data flows generated by the configured multi-channel protocol.

- After no-reverse is specified, the device generates only forward server map entries.

```
[NGFW]nat server server1 protocol tcp global 202.202.1.1 inside 192.168.1.1  
no-reverse
```

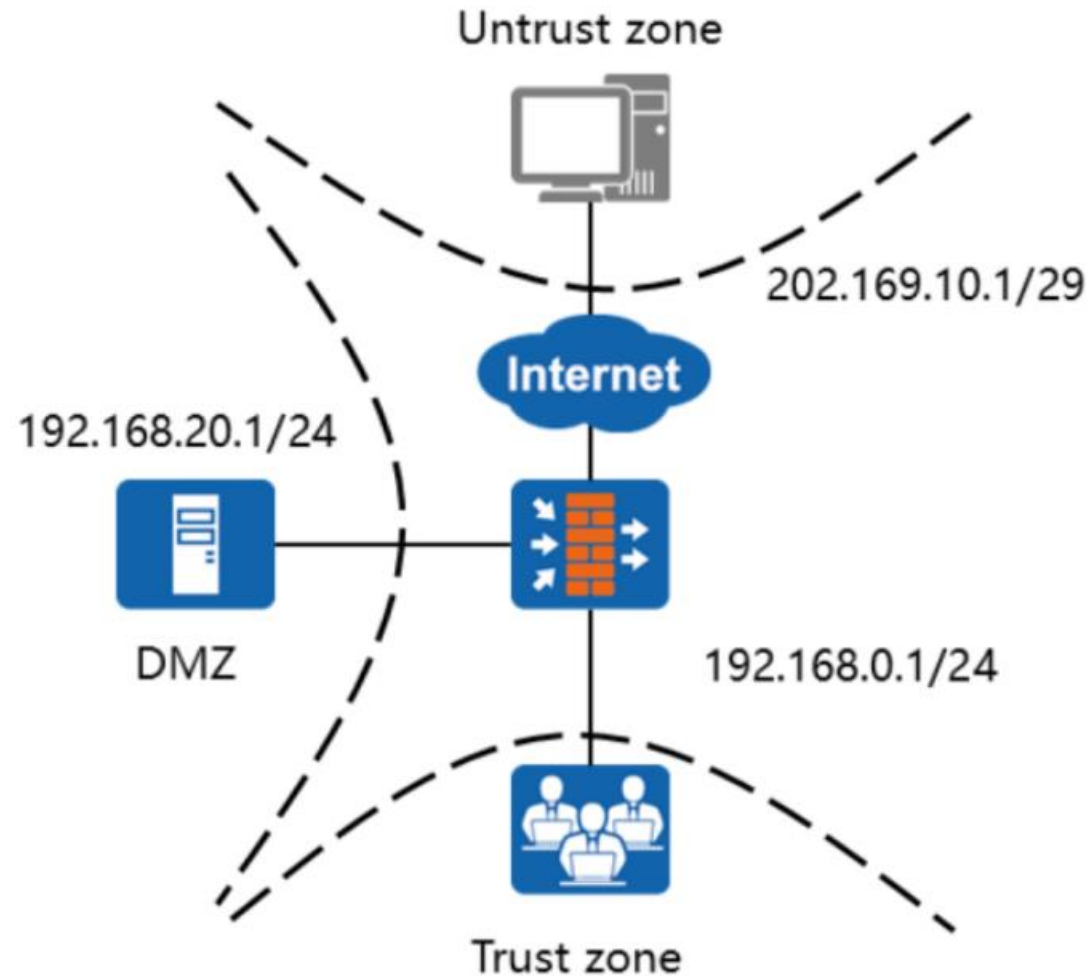
- Example: server map entry

```
Type: Nat Server, ANY -> 202.202.1.1[192.168.1.1], Zone:---, protocol:tcp  
Vpn: public -> public
```

- When an internal server proactively access an external network, the device cannot translate the private address of the internal server into a public address. Therefore, the internal server cannot initiate a connection to the external network. In this case, you can specify the no-reverse parameter to prevent internal servers from proactively accessing external networks.
- If an internal server advertises multiple public addresses for external networks through the NAT server function with no-reverse specified, the internal server cannot access external networks proactively. To enable an internal server to access an external network, configure a source NAT policy. This policy is configured between the security zone of the internal server and the security zone of the external network to translate the private address of the internal server to a public address. The source NAT policy can reference the global address or another public address.

- Application scenarios:

- ☐ Source NAT application
- ☐ NAT server application



- Configure a NAT address pool.

Add Source Translation Address Pool

Name: 1

IP Address Range: 202.169.10.2-202.169.10.6

Enter each IP address or range on a separate line. For example:
192.168.10.10-192.168.10.20
192.168.10.30

Health Check: Select a health check item. [Configure]

Configure Black-Hole Route: ☐

PAT: ☒

Advanced

OK Cancel

- Configure a source NAT policy.
- The source security zone is usually the zone where the pre-NAT private address resides. In this example, it is the trust zone. The destination security zone is usually the zone where the post-NAT public address resides. In this example, it is the untrust zone.

Add NAT Policy

[Show Overview]

Name: natpolicy

Description:

Tag: Select or enter a tag.

NAT Type: ☒ NAT ☐ NAT64

NAT Mode: Source address translation

Schedule: Select a time range.

Original Data Packet

Source Zone: trust

Destination Type: ☒ Destination Zone ☐ Outbound Interface

Destination Zone: untrust

Source Address: Select or enter an address.

Destination Address: Select or enter an address.

Service: Select or enter a service.

Translated Data Packet

Source Address Translated To: ☐ Outbound Interface ☒ IP Addresses in the IP Address Pool

Source Translation Address Pool: 1

OK Cancel

In this example, the configuration enables users in the **trust** zone to access Internet resources in the **untrust** zone. Therefore, the source security zone is **trust** and the destination security zone is **untrust**.

Select the configured address pool.

- Configure the internal web and FTP servers.
- During NAT server configuration, the external address is the public IP address that the internal server provides for external users.
- The internal address is the IP address of an internal server on the LAN.

Add Server Mapping

[Show Overview]

Name: ftpsrvr

Zone: [dropdown]

Public IP Address: 202.169.10.1

Private IP Address: 192.168.20.3

☒ Specify Protocol

Protocol: TCP

Public Port: 21

Private Port: 21

☒ Allow the Server to Use the Public IP Address for Internet Access

☒ Configure Black-Hole Route

Note: To ensure that the device can properly forward NAT service traffic, configure a security policy. [Add Security Policy]

OK Cancel

External and internal addresses. The public address is the address used by external users for access. The private address is the internal server's address on the LAN.

- Configure an interzone security policy
- On the web configuration page, perform the following steps to configure interzone packet filtering rules:
 - ❑ Choose Firewall > Security Policy > Forward Policy.
 - ❑ Under Forward Policy List, click Add.
 - ❑ Set the parameters.

Add Security Policy

Note: You can use a policy template to quickly define the required policy. [\[Select Template\]](#) [Switch Source and Destination](#)

Name: nat_server_policy

Description:

Policy Group: -- NONE --

Tag: Select or enter a tag.

Source Zone: untrust [Multiple]

Destination Zone: dmz [Multiple]

Source Address/Region: Select or enter an address.

Destination Address/Region: 192.168.20.3/24 x

User: Select or enter a user name. [Multiple]

Access Mode: Select an access mode.

Device: Select or enter a device.

Service: ftp x

Application: Select or enter an application. [Multiple]

Specifying application will automatically enable the SA function. This function reduces system performance.

URL Category: Select or enter a url category. [Multiple]

Schedule: Select a time range.

Action: ☒ Permit ☐ Deny

- Configure interzone access rules.
- Specify the network segment 192.168.0.0 as the source address. (Detailed configurations are not described here.)
- Configure an address pool.

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

- Configure a source NAT policy.

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

- Configure the internal web and FTP servers.

```
[USG] nat server wwwserver protocol tcp global 202.169.10.1 80 inside
192.168.20.2 8080
[USG] nat server ftpserver protocol tcp global 202.169.10.1 ftp inside
192.168.20.3 ftp
```

- Configure interzone packet filtering rules.

```
[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
```

- When both NAT and internal servers are configured on the USG, the internal servers have a higher priority and take effect first.
- If multiple internal servers use the same public address, you can run the nat server command multiple times to configure them, and distinguish them using protocols.

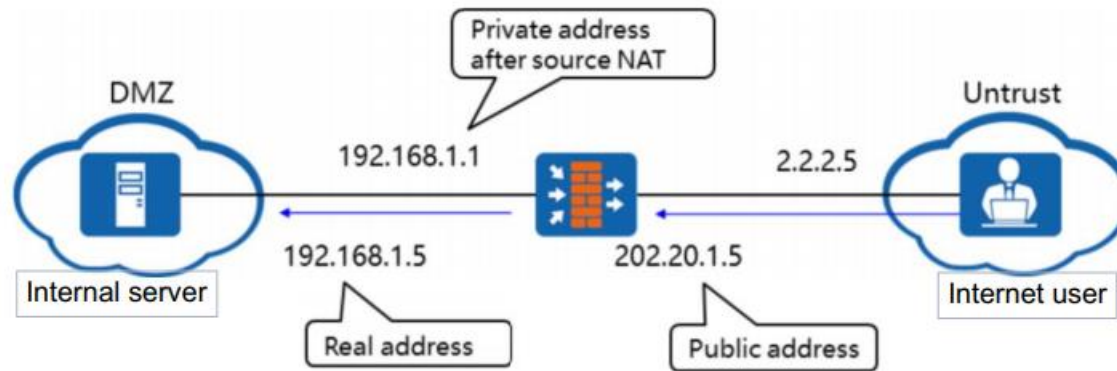
- **Application scenarios:**

- ☐ **NAT server + source NAT**
- ☐ **Intrazone NAT**

- **When either communication party accesses the other party in a twice NAT scenario, the destination address is not a real address but a NAT address. Generally, internal networks belong to high-priority zones, and external networks belong to low-priority zones. When an external user in a low-priority zone accesses the public address of an internal server, the destination address of the packet is translated into the private address of the internal server. The route destined for the public address must be configured on the internal server.**

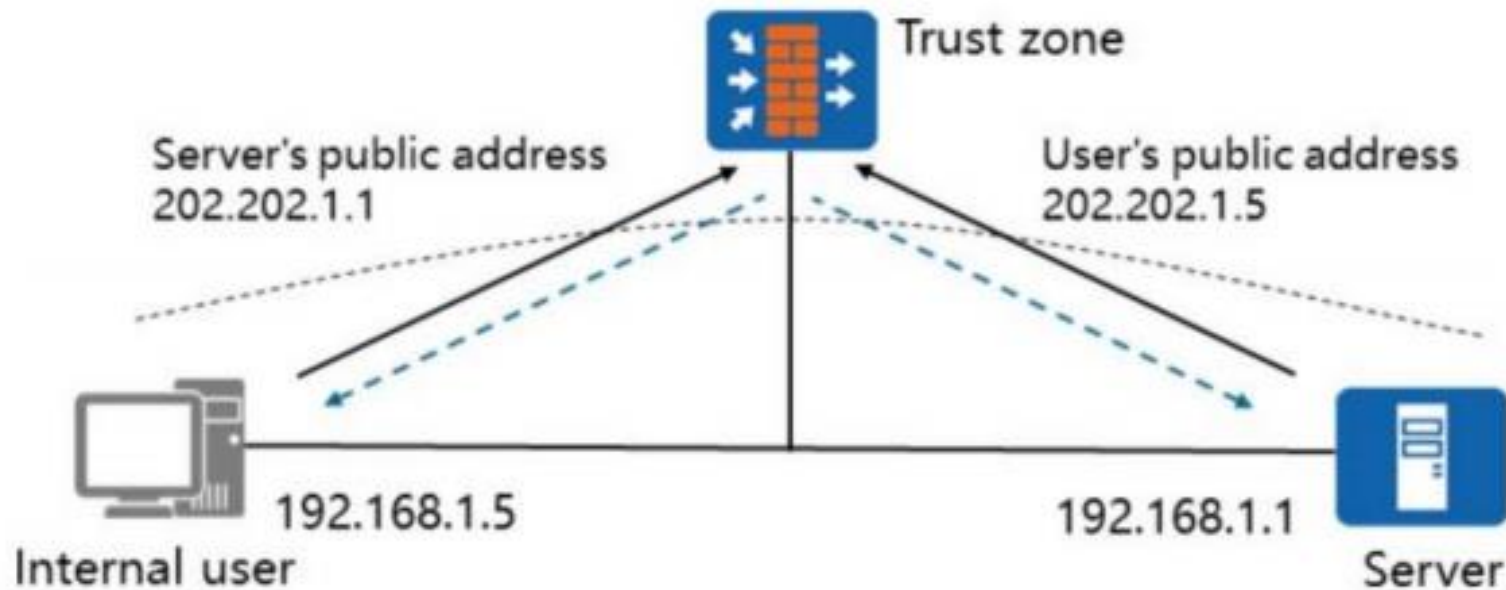
- **To avoid configuring a route destined for the public address, you can configure NAT from a low-priority zone to a high-priority zone. If NAT is required for access within the same security zone, configure intrazone NAT.**

- To simplify the configuration of the route from a server to a public network, you can configure source NAT based on the NAT server function.



- In NAT server configuration, the internal server can send the response packet only after the route destined for the public address is configured. To simplify configuration without configuring the route destined for the public address, you can configure the firewall to translate the source address of the external user. The source address after NAT must be on the same network segment as the private address of the internal server. In this way, the internal server sends the response packet to the device by default, and the device then forwards the response packet.

- The firewall translates the destination address of the user's request packet into the private address of the FTP server. In addition, it translates the source address into the public address of the user.
- The firewall translates the source address of the response packet from the FTP server into the public address. In addition, it translates the destination address into the private address of the user.

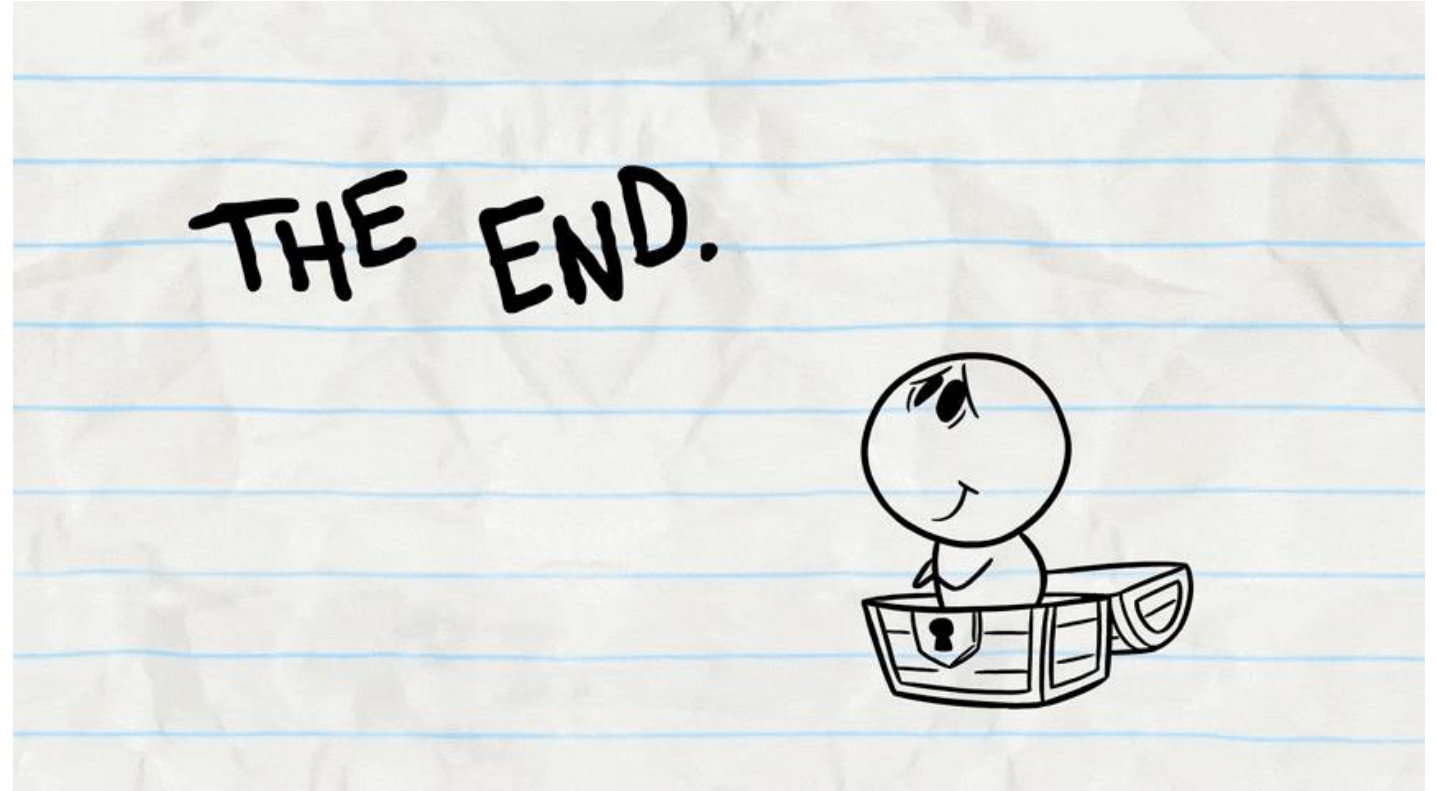


- If both parties that require address translation are in the same security zone, intra-zone NAT is involved. When both the user and FTP server are in the Trust zone, the user accesses the public address of the FTP server. In this way, all the packets exchanged between the user and FTP server pass through the firewall, and the internal server and intra-zone NAT must be configured.
- Intra-zone NAT is used when the internal user and server are in the same security zone, but the internal user is required to access only the public address of the server. In intra-zone NAT, the destination address of the packet sent to the internal server must be translated from a public address into a private address, and the source address must be translated from a private address into a public address.

The End

Please feel free to contact me anytime if you have any questions

Abdelrhman Ahmed Refaat:
abdelrhmanahmedrefaat@gmail.com



جامعة القادسية
EVERYONE'S SMART UNIVERSITY