

Securing Networks with
Cisco FTD

Chapter 15

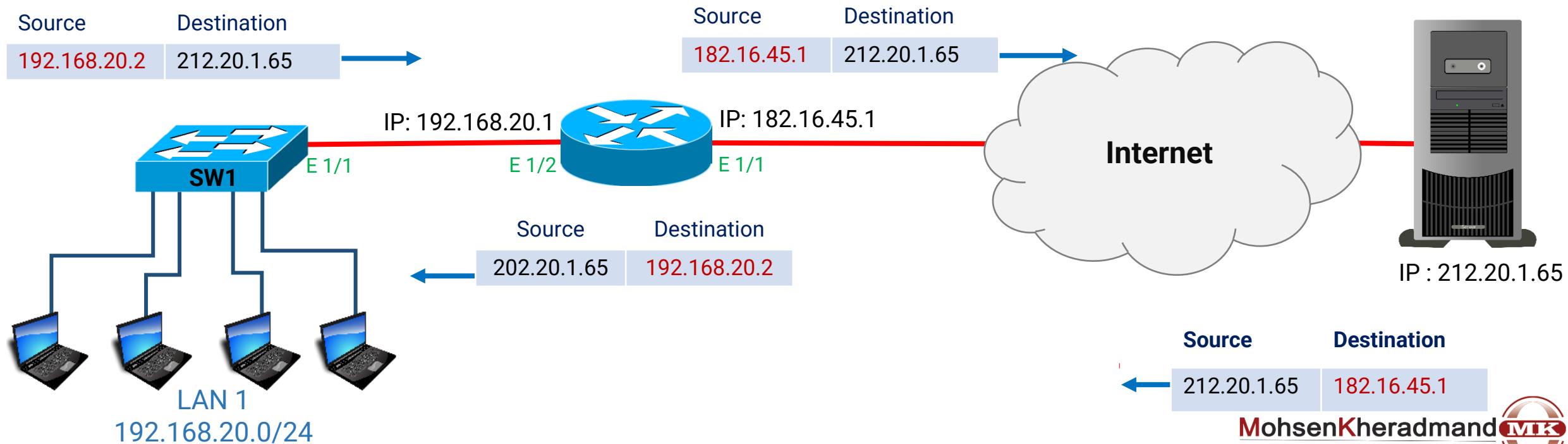
Network Address Translation

(NAT)

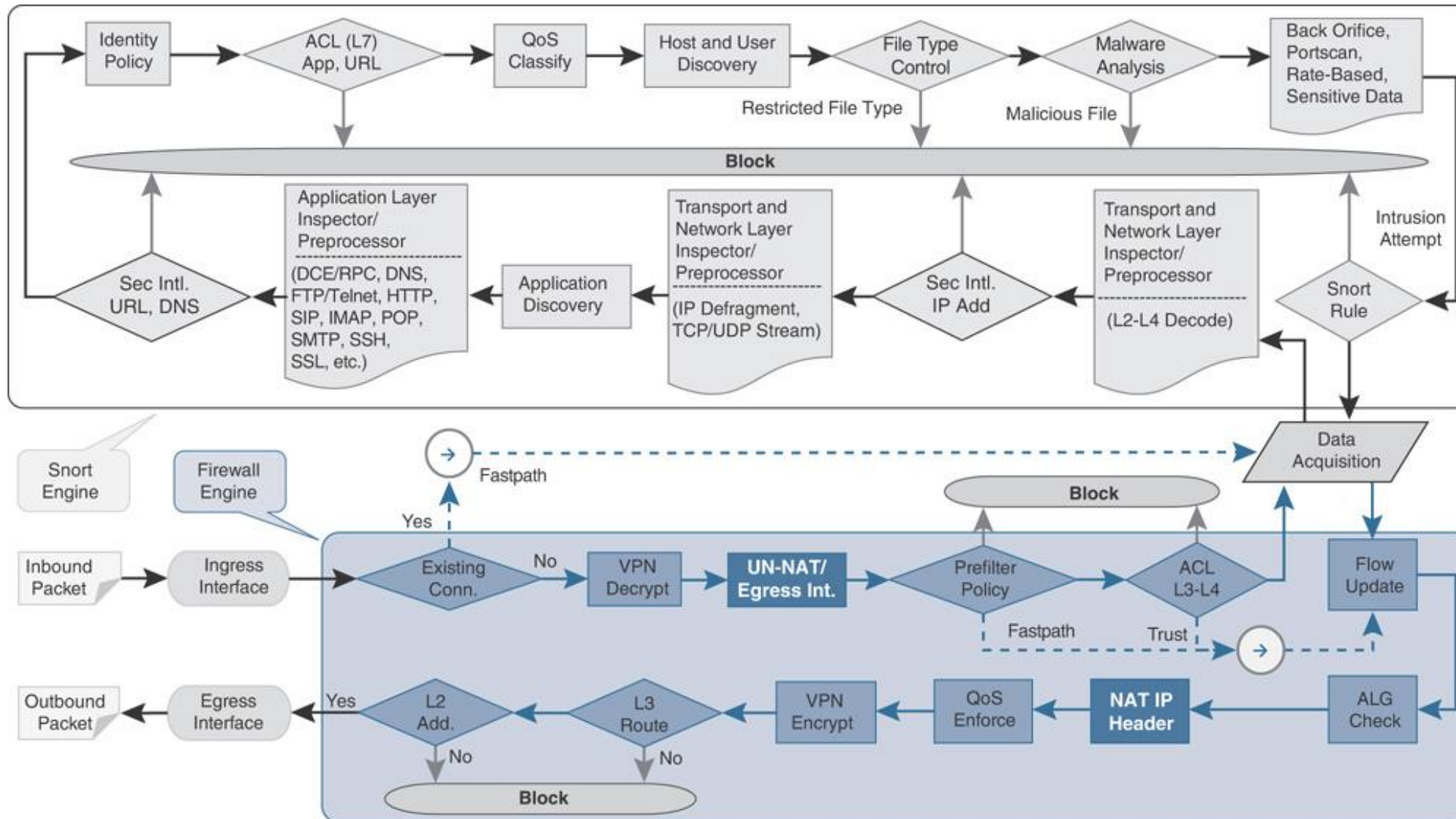
Mohsen Kheradmand

Network Address Translation

- Defined in RFC 3022
 - Describes methods for connecting private (internal) IP addresses to the external (Internet)
 - NAT uses a one-to-one, one-to-many, many-to-one, many-to-many, few to-many, and many-to-few mapping method
 - One or more private IP clients gain access to the Internet by mapping the private IP addresses to public IP addresses



Network Address Translation



NAT types:

Static NAT

- The simplest form of NAT
- A single private IP address is mapped to a single public IP address or vice-versa

Dynamic NAT

- Maps a one or group of local IP addresses to a group of Internet IP addresses

Port address translation (PAT)

- Also known as overloading , Is a special form of dynamic NAT
- Maps a group of local IP addresses to one or a group of Public IP addresses by using TCP and UDP ports

NAT implementation types

Source NAT:

- Internal users with private IP addresses connects to the internet.

Destination NAT:

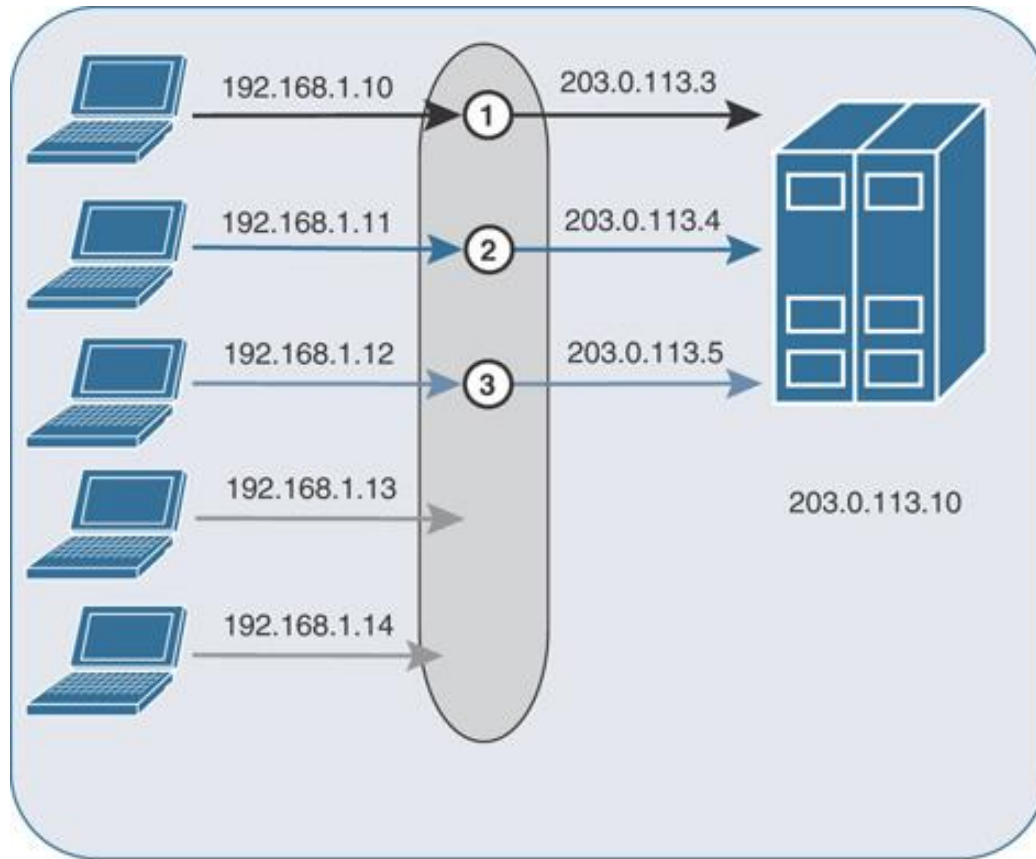
- Users from the internet, connect to the enterprise servers with private IP addresses.

Policy NAT:

- Occurs based upon matching both the source and destination of traffic

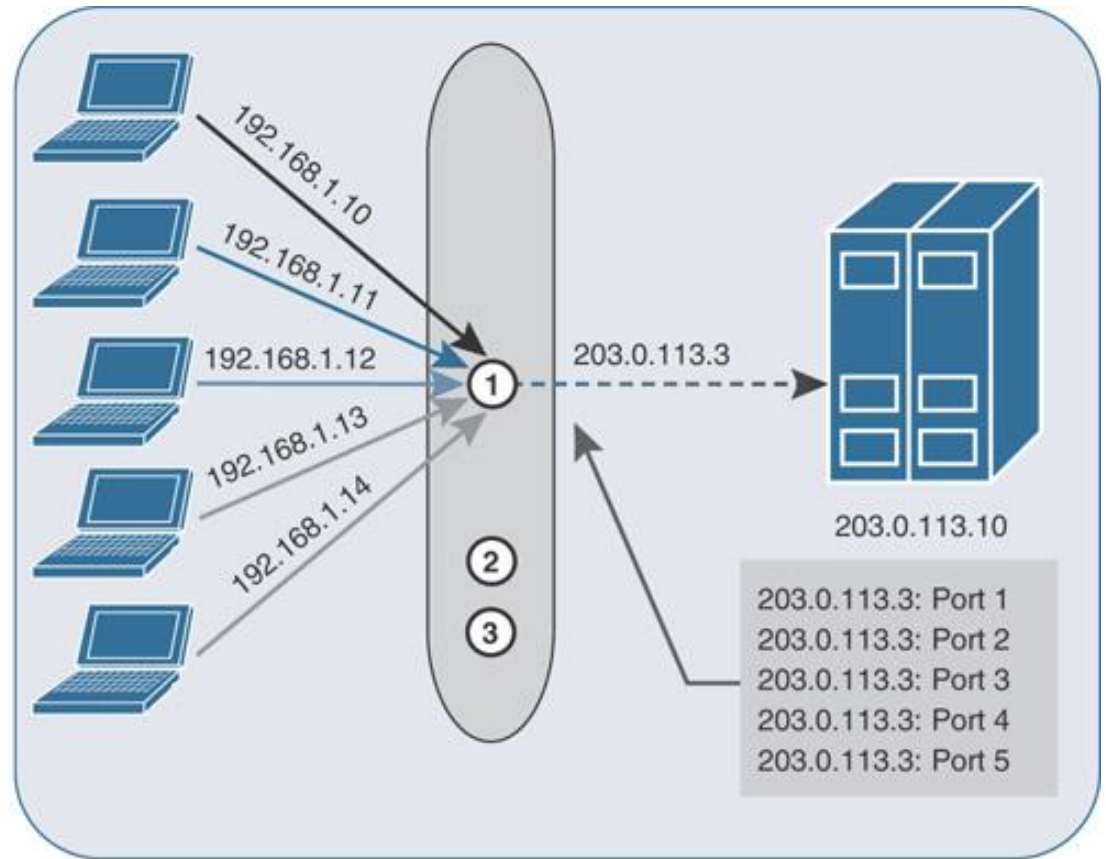
Identity NAT:

- We will exclude some traffic to be translated especially over VPN tunnels.



Network Address Translation (NAT)

If the first three hosts are dynamically assigned, the last two hosts must wait until the timeout value expires. But if they are assigned statically, the last two hosts have no chance.



Port Address Translation (PAT)

One address can multiplex more than 65,000 connections over a single IP address before another address is selected from a pool.

NAT Rule Types

Auto NAT:

- An Auto NAT rule can translate one address—either a source or destination address—in a single rule.
- This means that to translate both source and destination addresses, two separate Auto NAT rules are necessary.

Manual NAT:

- A Manual NAT rule allows the translation of both source and destination addresses within the same rule.
- A Manual NAT rule may be necessary when you want to make an exception for translation.

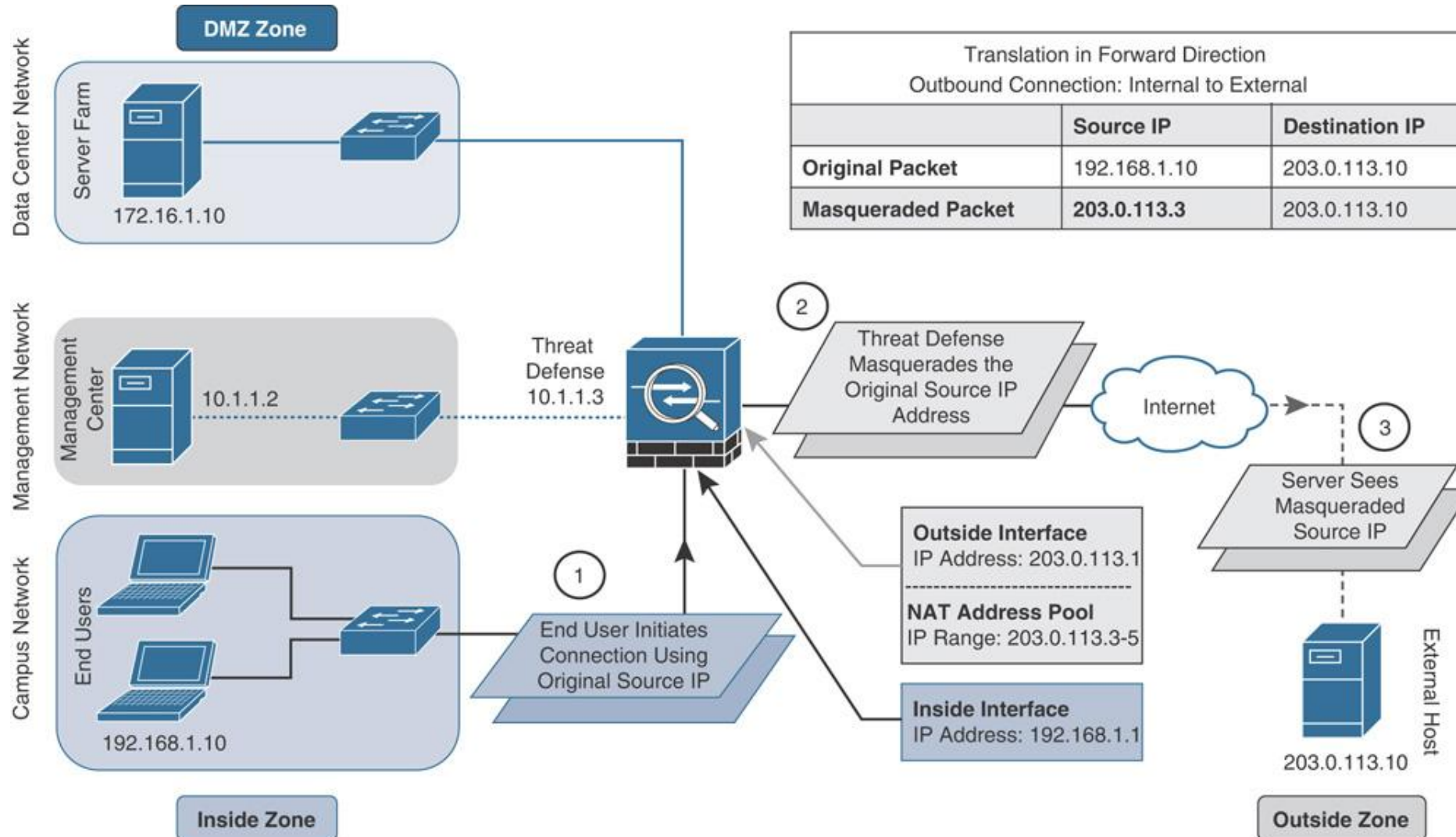
A NAT policy editor categorizes NAT rules into three groups

- ✓ NAT Rules Before (manual NAT policies)
- ✓ Auto NAT Rules
- ✓ NAT Rules After (manual NAT policies)

NAT Prerequisites

- Configuring an Auto NAT rule is simpler than configuring a Manual NAT rule (recommended)
- If you modify or redeploy a new NAT policy , the new policy does not work until the timer for any existing connections expires. (use **clear xlate** command to act immediately)
- To improve performance, prefer static NAT to dynamic NAT or PAT
- Interfaces that participate in a NAT have to be in a regular firewall mode—routed or transparent (FTD , does not support NAT on IPS-only)
- If you used a threat defense in an IPS-only mode, make sure all the associated interfaces where you want to enable NAT are now configured with IP address and security zones
- Static NAT always has higher priority than dynamic NAT. So if an IP address is matched with both static and dynamic NAT, static NAT has more priority.

NAT Configuration



NAT Configuration

- Devices > NAT
- Select Threat Defense NAT Policy

The screenshot displays the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes the Cisco logo, the title 'Firepower Management Center', and the breadcrumb 'Devices / NAT'. The main navigation tabs are Overview, Analysis, Policies, Devices (selected), Objects, AMP, and Intelligence. On the right, there are links for Deploy, a search icon, a notification icon with a '2', a settings icon, a help icon, and the user 'admin'. The left sidebar shows a tree view with 'NAT Policy' selected under the 'Devices' category. The main content area features a table with one row labeled 'NAT Policy' and a 'Device Type' column. Below the table, a message states 'There are no policies created. Add a new policy.' A 'New Policy' button is located in the top right corner of the main content area.

NAT Configuration

NAT Policy	Device Type	Status
There are no policies created. Add a new Firepower NAT Policy (or) Threat Defense NAT Policy		

New Policy

Name:

Inside-to-internet

Description:

local user address to public address

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Q Search by name or value

FTD1

Add to Policy

Selected Devices

FTD1

Cancel

Save

FMC offers two types of NAT policies :

- **The Firepower NAT Policy**
 - Applies to IPS appliances, like the 7000 or 8000 series.
- **Threat Defense NAT Policy**
 - Applies to anything running the FTD image (ASA X-Series and Firepower appliance)
- Click threat defense NAT policy
- Enter a name for NAT policy and select the device in which configuration will be applied

NAT Configuration

- Click Add Rule

Inside-to-internet

local user address to public addresses

Rules

Show Warnings Save Cancel

Policy Assignments (1)

[Filter by Device](#)

Filter Rules

×

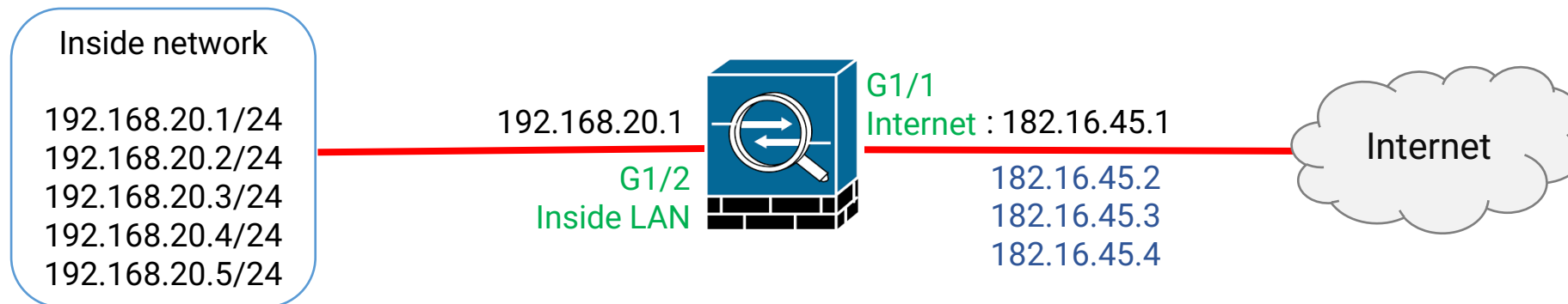
Add Rule

					Original Packet			Translated Packet				
#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
NAT Rules Before												
Auto NAT Rules												
NAT Rules After												

NAT Configuration

1) Dynamic Source NAT

- A group of real IP addresses are mapped to a (usually smaller) group of mapped IP addresses
- The translation is created only when the real host initiates the connection



NAT Configuration

1) Dynamic Source NAT

- Select Auto NAT Rule
- Select Dynamic type
- Add inside local interface to source
- Add global interface with translated address to destination

Add NAT Rule

NAT Rule:

Auto NAT Rule

Type:

Dynamic

☒ Enable

Interface Objects

Translation

PAT Pool

Advanced

Available Interface Objects

DMZ
Inside-LAN
Internet

Add to Source

Add to Destination

Source Interface Objects

(1)

Inside-LAN

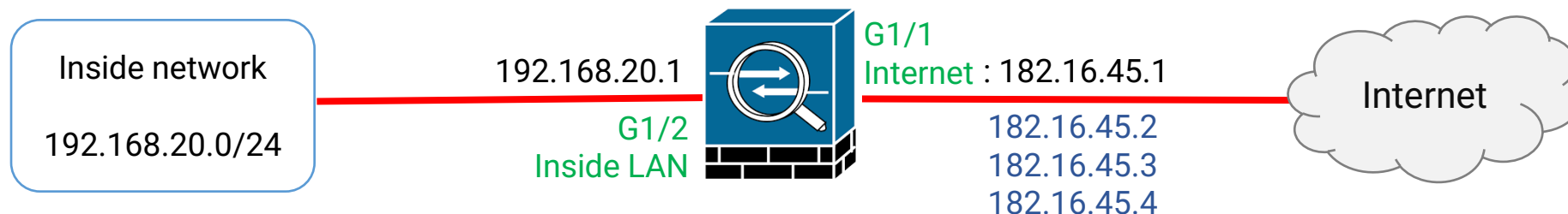
Destination Interface Objects

(1)

Internet

Cancel

OK



NAT Configuration

1) Dynamic Source NAT

- Original source**
 The network or IP to use NAT
- Translated Source :**
Destination Interface IP : NAT all inside addresses via outbound interface

Address : use a network or Range of IP
- Click OK to add this Rule

Add NAT Rule

NAT Rule:

Auto NAT Rule

Type:

Dynamic

☒ Enable

Interface Objects

Translation

PAT Pool

Advanced

Original Packet

Translated Packet

Original Source:*

IT-Admins

+

Translated Source:

Address

+

Original Port:

TCP

Translated Port:

Cancel

OK



NAT Configuration

1) Dynamic Source NAT

- Note :

You can define a new Host , Range of IP addresses , A network or FQDN to use in NAT

New Network Object

Name

NAT-Pool1

Description

reserved Public addresses for dynamic NAT

Network

☐ Host

☒ Range

☐ Network

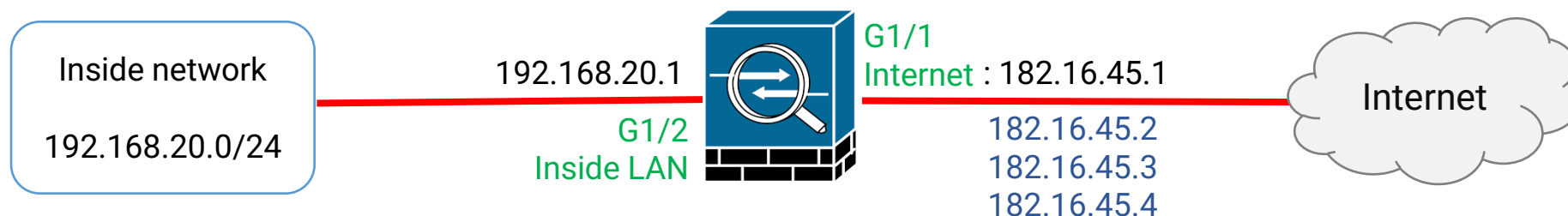
☐ FQDN

182.16.45.2-182.16.45.4

☐ Allow Overrides

Cancel

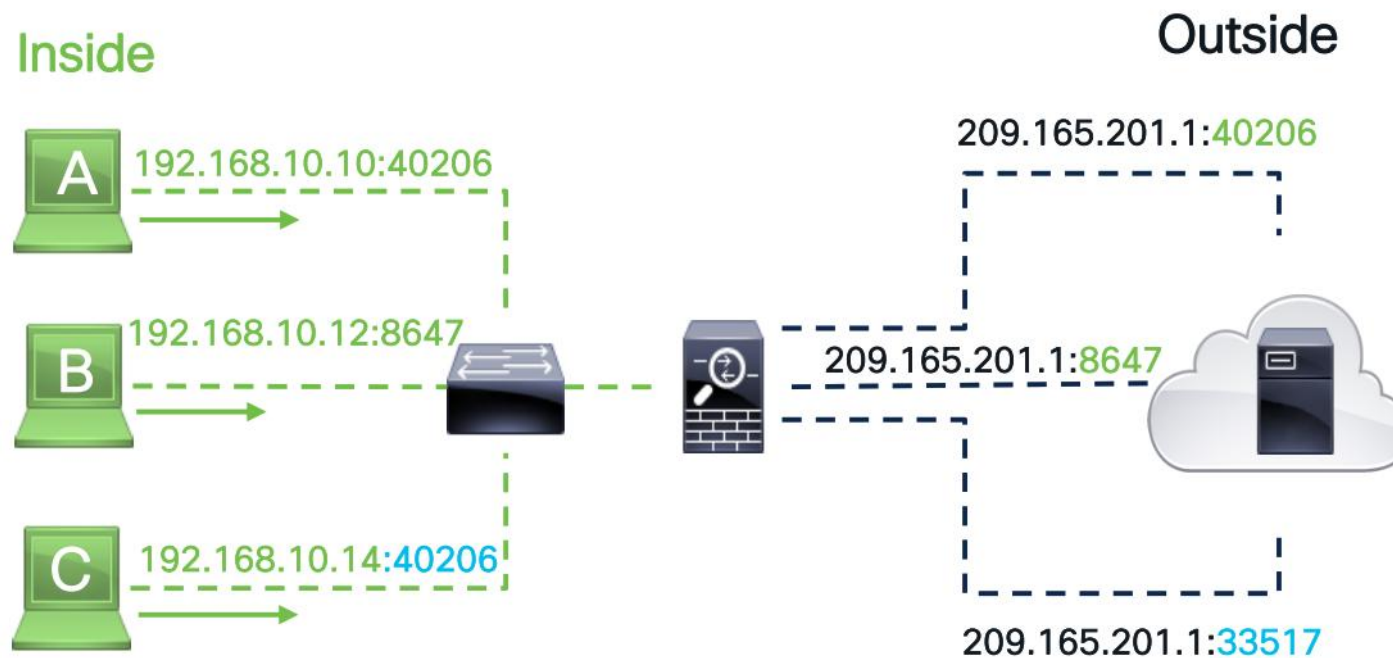
Save



NAT Configuration

2) Dynamic source **PAT**

- A group of real IP addresses are mapped to a single IP or group of addresses using a unique source port of that IP



NAT Configuration

2) Dynamic source **PAT**

- Same as previous section select source and destination zone to use in NAT

Add NAT Rule

NAT Rule:

Auto NAT Rule

Type:

Dynamic

☒ Enable

Interface Objects

Translation

PAT Pool

Advanced

Available Interface Objects

DMZ
Inside-LAN
Internet

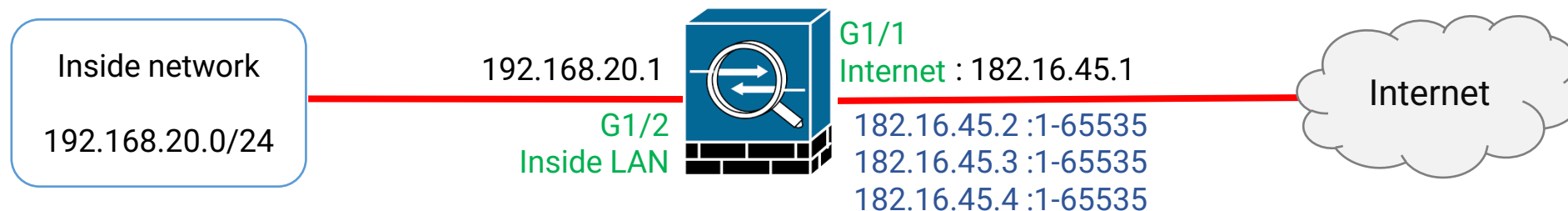
Add to Source
Add to Destination

Source Interface Objects (1)

Inside-LAN

Destination Interface Objects (1)

Internet



NAT Configuration

2) Dynamic source **PAT**

- Translation Tab
- Select original source IP / network
- Select **Address** from translated address but leave the value , blank

Add NAT Rule

NAT Rule:
Auto NAT Rule ▼

Type:
Dynamic ▼

☒ Enable

Interface Objects **Translation** PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* IT-Admins ▼ +	Translated Source: Address ▼ +
Original Port: TCP ▼	Translated Port:



NAT Configuration

2) Dynamic source **PAT**

- PAT Pool tab
- Select Address form PAT drop down
- Then select translated IP/network

Add NAT Rule

NAT Rule:
Auto NAT Rule ▼

Type:
Dynamic ▼

☒ Enable

Interface Objects Translation **PAT Pool** Advanced

☒ Enable PAT Pool

PAT:
Address ▼ NAT-Pool1 ▼ +

☐ Use Round Robin Allocation

☐ Extended PAT Table

☒ Flat Port Range ⓘ This option is always enabled on device(s) starting from v6.7.0, irrespective of its configured value.

☒ Include Reserve Ports

☐ Block Allocation



NAT Configuration

PAT pool options:

- ☐ Use Round Robin Allocation
- ☐ Extended PAT Table
- ☐ Flat Port Range i This option is always enabled on device(s) starting from v6.7.0, irrespective of its configured value.
- ☐ Include Reserve Ports
- ☐ Block Allocation

- **Use the round robin Allocation** : A source port from one IP is allocated, then the next request will take a port from the next IP address, and so on. If not enabled, all ports from one IP are used until they are exhausted.
- **Extended PAT Table** : enables the use of all available ports per service rather than uses the ports per source IP address.
- Round robin, especially when combined with extended PAT, can consume a large amount of memory.
- **Flat Port Range** : When the original source port is unavailable to use in PAT , tells Threat Defense to use a port that's close to the original source port.
- It does this by dividing all the source ports into groups of 512 ports
- **Include Reverse Ports** : By default, translation only uses ports from 1024 and above. This option extends this to all ports. (entire range of 1 to 65535)
- **Block allocation** : subsequent connections from the host use new randomly selected ports within the same block
- port blocks are allocated in the 1024-65535 range only.

NAT Configuration

3) Static NAT with Auto NAT Rule

- One to one translation
- Two-way NAT
- Click add Rule
 - ✓ Select Auto NAT Rule
 - ✓ Select Static Type
 - ✓ Add Source and Destination interfaces as well as you have done in previous section

Add NAT Rule

NAT Rule:
Auto NAT Rule

Type:
Static

☒ Enable

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

DMZ
Inside-LAN
Internet

Add to Source
Add to Destination

Source Interface Objects (1)
Inside-LAN

Destination Interface Objects (1)
Internet

Cancel OK



NAT Configuration

3) Static NAT with Auto NAT Rule

- Translation tab
- Select original source to translate
- Select original port of the source
- Select translated IP/Range
- Select translated port to use in PAT

Add NAT Rule

NAT Rule:
Auto NAT Rule ▼

Type:
Static ▼

☒ Enable

Interface Objects Translation PAT Pool Advanced

Original Packet	Translated Packet
Original Source:*	Translated Source:
Servers ▼ +	Address ▼
Original Port:	NAT-IP ▼ +
TCP ▼	Translated Port:
22	1800



NAT Configuration

3) Manual NAT

- Using policy NAT specify a specific IP/port to specific client for NAT process
- In the following example we need to configure NAT , so if the Server2 needs to connect to public IP 191.1.5.2 , so the translate IP address (182.16.45.2) assign to the traffic



NAT Configuration

3) Manual NAT

- Click add Rule
- Interface object tab
- Select Manual NAT Rule
- You can select NAT Rule Before or after Auto Rules to perform
- Select Dynamic/Static type of NAT
- Description is optional
- Add source and destination interface

Add NAT Rule

NAT Rule:

Manual NAT Rule

Insert:

In Category

NAT Rules Before

Type:

Dynamic

☒ Enable

Description:

NAT for get updates for FTD-FMC appliances through proxy server

Interface Objects

Translation

PAT Pool

Advanced

Available Interface Objects

DMZ

Inside-LAN

Internet

Add to Source

Add to Destination

Source Interface Objects

Inside-LAN

Destination Interface Objects

Internet



NAT Configuration

3) Manual NAT

➤ Translation tab

- Select original source IP/Network
- Select original Destination IP/network
- Select translated interface/IP to NAT
- Translated Destination could be the same as original destination
- Select original/destination ports if you need
- Click OK
- If you need you can use PAT for this Rule

Add NAT Rule

NAT Rule:

Manual NAT Rule

Insert:

In Category

NAT Rules Before

Type:

Dynamic

☒ Enable

Description:

NAT for get updates for FTD-FMC appliances through proxy server

Interface Objects

Translation

PAT Pool

Advanced

Original Packet

Original Source:*

FMC-FTD

+

Original Destination:

Address

Cisco-Servers

+

Original Source Port:

HTTPS

+

Original Destination Port:

HTTPS

+

Translated Packet

Translated Source:

Address

Proxy-IP-side

+

Translated Destination:

Cisco-Servers

+

Translated Source Port:

HTTPS

+

Translated Destination Port:

HTTPS

+

Cancel

OK

NAT Rule priority

FMC NGFW NAT Policy Editor

Overview Analysis Policies **Devices** Objects AMP Intelligen... Deploy

NAT Policy
Enter Description

Rules

To View the NAT Rules on CLI, Run
> show nat detail

Show Warnings Save Cancel

Policy Assignments (1)

Filter by Device Filter Rules Add Rule

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
1 2 3											
GUI: NAT Rules Before CLI: Section 1 Manual NAT policies. Top priority, when available.											
GUI: Auto NAT Rules CLI: Section 2 Static type has higher priority than Dynamic type. Longer prefix length has higher priority within type.											
GUI: NAT Rules After CLI: Section 3 Manual NAT policies. Lower priority than Auto NAT.											

Top to Bottom Priority

of 1 > >| <| <

NAT Configuration

ACP rule for NAT

- Create ACP to allow the traffic from inside to outside (Allow =All)
 - Create ACP to allow the specific traffic from outside to DMZ (based on our NAT policied)
-
- Select original source IP/Network
 - Select original Destination IP/network