

Lab Setup Overview

Software Versions:

- **FMC (Firepower Management Center):** v6.7
- **FTD (Firepower Threat Defense):** v6.4
- **Windows PCs:** Windows 7
- **Cloud:** Acts as the **outside network** (Internet access)
- **Switch:** Used for **management connectivity** between all devices

System Resources:

- **FMC:** 16 GB RAM
- **FTD:** 8 GB RAM
- **Each PC & Switch:** 1 GB RAM

IP Addressing Scheme

Device	Role	IP Address
Management PC	Used to access FMC GUI	192.168.100.100
FMC	Management Server	192.168.100.10
FTD	Security Appliance	192.168.100.1

Connectivity Check

Before starting configuration, **verify connectivity** between:

- Management PC ↔ FMC
- FMC ↔ FTD
- PC ↔ FTD

You can use ping to confirm all devices can reach each other.

Accessing FMC GUI

- From the **Management PC**, open a browser.
 - Access the FMC GUI using:
 - `https://192.168.100.10`
 - Enter the **default credentials**:
 - Username: admin
 - Password: Admin123
 - Change the password when prompted.
 - Activate the **90-day evaluation license** to begin.
-

Registering FTD with FMC

When initializing the **FTD**, ensure you **select to manage it from the FMC**, not locally.

- **FTD → FMC communication:**
Uses **TCP port 8305** (outbound from FTD to FMC)
- On the FTD CLI, run the following command:
- `configure manager add 192.168.100.10 key123`
 - 192.168.100.10 → FMC IP
 - key123 → Registration key (must match what you set in FMC during device registration)

```
> configure manager add 192.168.100.10 key123
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

Verify the registration status:

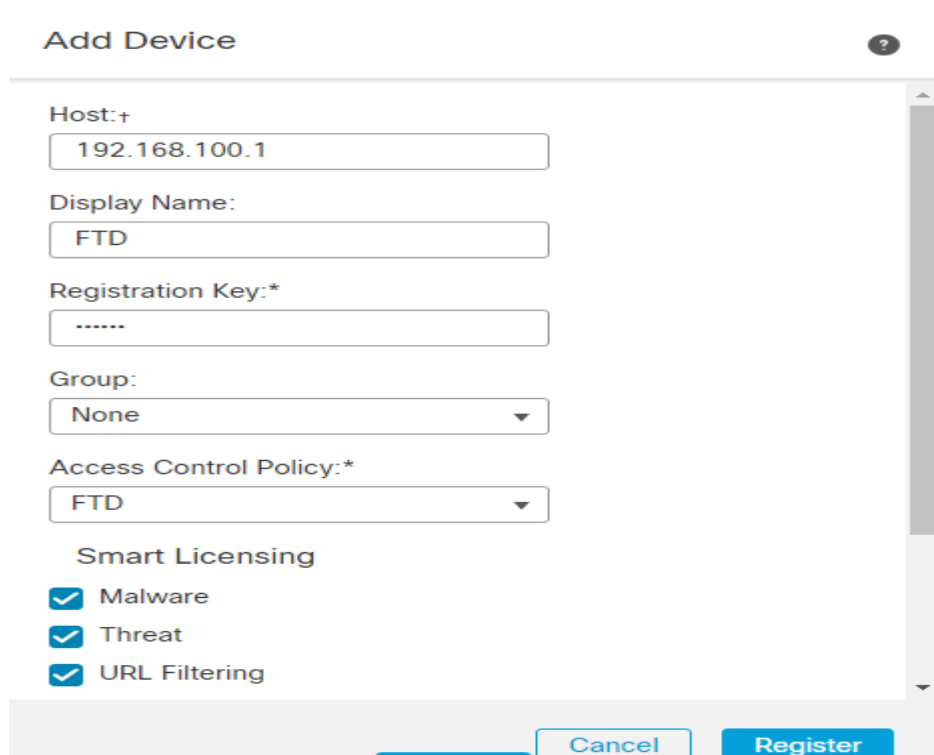
`#show managers`

You should see the FMC listed with a **“Pending”** status — this is normal until you confirm the registration from the FMC GUI.

```
> show managers
Host                : 192.168.100.10
Registration Key     : ****
Registration        : pending
RPC Status          :
```

Confirming Registration from FMC

1. Log in to the **FMC GUI**.
2. Navigate to:
3. Devices → Device Management → Add Device
4. Enter the following details:
 - **Host:** 192.168.100.1 (FTD IP)
 - **Registration Key:** key123 (must match what you entered on the FTD)
 - **Display Name:** (Choose any meaningful name, e.g. FTD-Lab)
 - **Access Control Policy:** Select an existing one or create a new policy (e.g. “Lab-Access-Policy”).
5. Click **Register**.
 - The FMC will establish a secure connection with the FTD using the key and complete the registration process.
6. Once registration is successful, the FTD status will change from **Pending** to **Online**.



Add Device

Host: +
192.168.100.1

Display Name:
FTD

Registration Key: *
.....

Group:
None

Access Control Policy: *
FTD

Smart Licensing

☒ Malware

☒ Threat

☒ URL Filtering

Cancel Register



Register

Registration

Communication with FTD has been established,
discovery in progress

```
> show managers
Type                : Manager
Host                : 192.168.100.10
Registration         : Completed
```

Post-Registration Configuration

By this point, the **registration is completed**, and you can now **fully manage the FTD from the FMC**.

Next Step – Configure FTD Interfaces

- 1. In FMC, go to:
- 2. Devices → Device Management → <Your FTD> → Edit
- 3. Navigate to the **Interfaces** tab.
- 4. Select an interface (e.g., GigabitEthernet1/1).
- 5. Configure the following:
 - **Name:** (e.g., Outside or Inside)
 - **Security Zone:** Assign or create a new one (e.g., OUTSIDE or INSIDE)
 - **IPv4 Configuration:**
 - Choose **Static** or **DHCP**
 - Enter the appropriate IP address and subnet mask
Example:
 - 192.168.1.1 /24
 - Optionally, enable the **Management Access** checkbox if you plan to manage or ping via this interface.
- 6. Click **Save**, then **Deploy** the changes to push the configuration to the FTD.

Edit Physical Interface



General

IPv4

IPv6

Advanced

Hardware Configuration

Name:

Inside

☒ Enabled

☐ Management Only

Description:

Mode:

None

Security Zone:

Inside

Interface ID:

GigabitEthernet0/1

Device	Routing	Interfaces	Inline Sets	DHCP			
					Q Search by name	Sync Device	Add Interfaces ▼
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address		
Diagnostic0/0	diagnostic	Physical				/	
GigabitEthernet0/0	Outside	Physical	Outside		192.168.1.11/24(Static)	/	
GigabitEthernet0/1	Inside	Physical	Inside		192.168.2.1/24(Static)	/	

Configuring DHCP Server for Inside Zone

To automatically assign IP addresses to internal hosts:

1. In FMC, navigate to:
2. Devices → Device Management → <Your FTD> → Edit
3. Go to the **DHCP** tab.
4. Under **DHCP Server Configuration**, click **Add**.

Server

Advanced

+ Add

Interface	Address Pool	Enable DHCP Server	
Inside	192.168.2.2-192.168.2.254		

Then deploy and see the ip of the inside zone PC:

```
Administrator: Command Prompt

Tunnel adapter isatap.{42A1F8B7-30A8-4EF7-81AF-C694F5F3D81B}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
C:\Users\user>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::64a1:d610:e046:f714%11
    IPv4 Address. . . . . : 192.168.2.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1

Tunnel adapter isatap.{42A1F8B7-30A8-4EF7-81AF-C694F5F3D81B}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
C:\Users\user>
```

Internet Access Components

To allow the inside network to access the Internet, you need to configure **three core components**:

- Static Route
- NAT
- Access Control Policy

Then we going to start with configuring a static route from the routing tap:

Type:

☒ IPv4

☐ IPv6

Interface*

Outside

Available Network

Search

any-ipv4

Home_ip

IPv4-Benchmark-Tests

IPv4-Link-Local

IPv4-Multicast

IPv4-Private-10.0.0.0-8

Add

Selected Network

any-ipv4

Gateway*

Home_ip

Metric:

1

(1 - 254)

Tunneled:

☐

(Used only for default Route)

OK

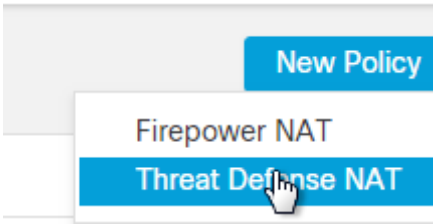
Cancel

Click **Add** and set:

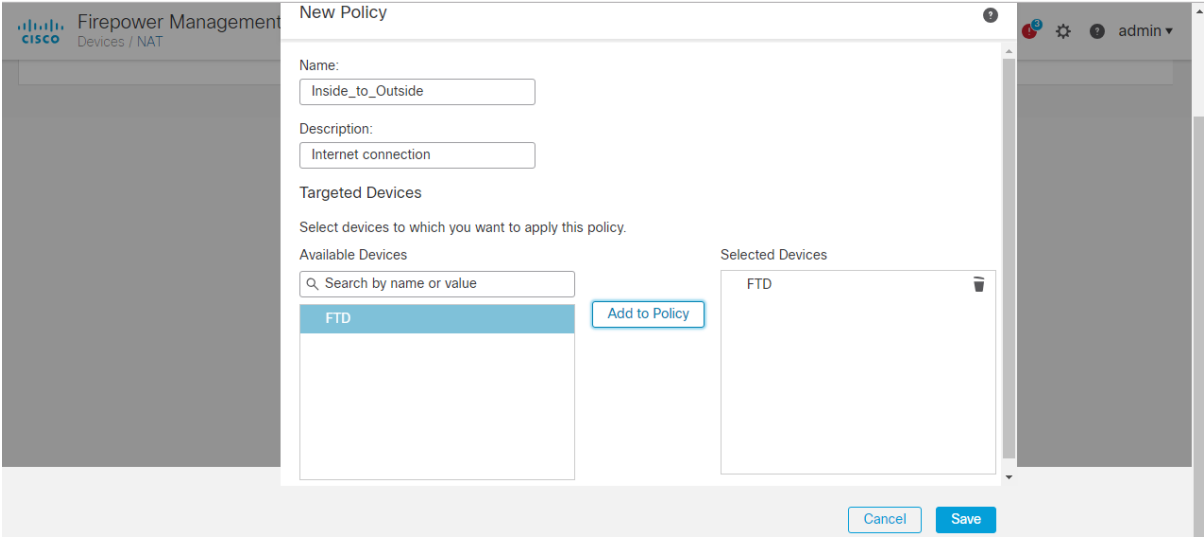
- **Interface:** Outside
- **Network:** 0.0.0.0/0
- **Gateway:** (the next-hop IP of your cloud/internet network)

In the FMC devices tap choose the NAT option

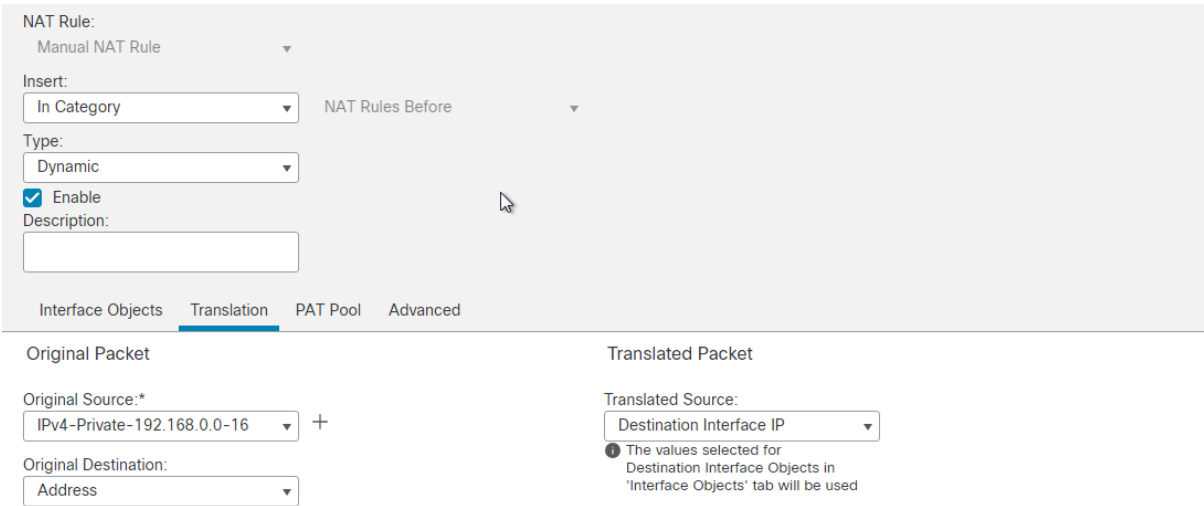
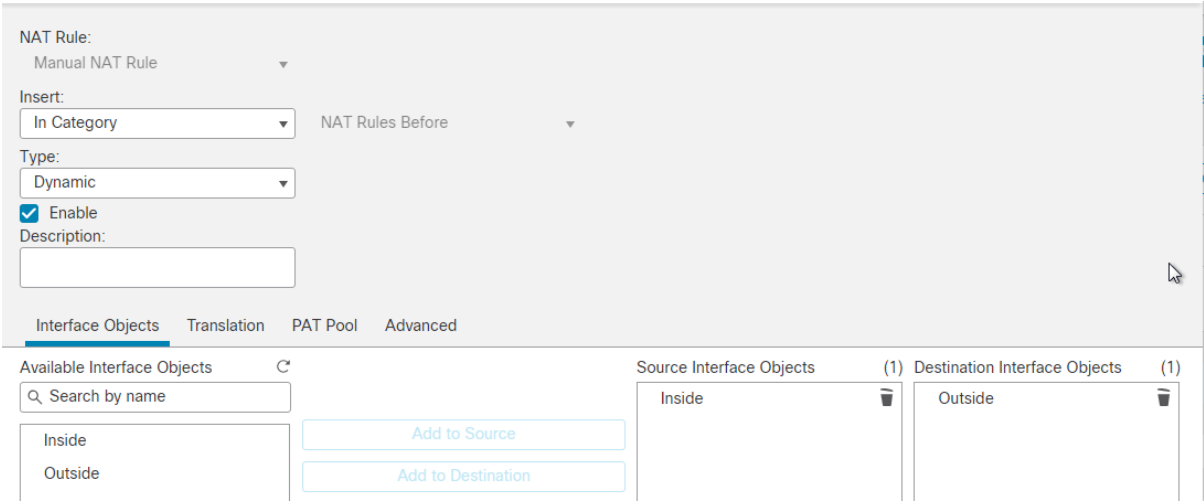
Then create a new policy for FTD



Choose the FTD device



Then create the NAT rule:



We'll wrap this up from the **Policies tab** → **Access Control** section.

1.

Editing Rule - Internet Access

Name

Internet Access

☒ Enabled

Move

Action

Allow

Time Range

None

+

Zones

Networks

VLAN Tags

Users

Applications

Ports

URLs

SGT/ISE Attributes

Inspection

Logging

Comments

Available Zones C

Q Search by name

Inside

Outside

Add to Source

Add to Destination

Source Zones (1)

Inside

Destination Zones (1)

Outside

Then it works:

```
C:\Users\user>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\user>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=113ms TTL=119
Reply from 8.8.8.8: bytes=32 time=105ms TTL=119
Reply from 8.8.8.8: bytes=32 time=63ms TTL=119
Reply from 8.8.8.8: bytes=32 time=53ms TTL=119

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 53ms, Maximum = 113ms, Average = 83ms
```