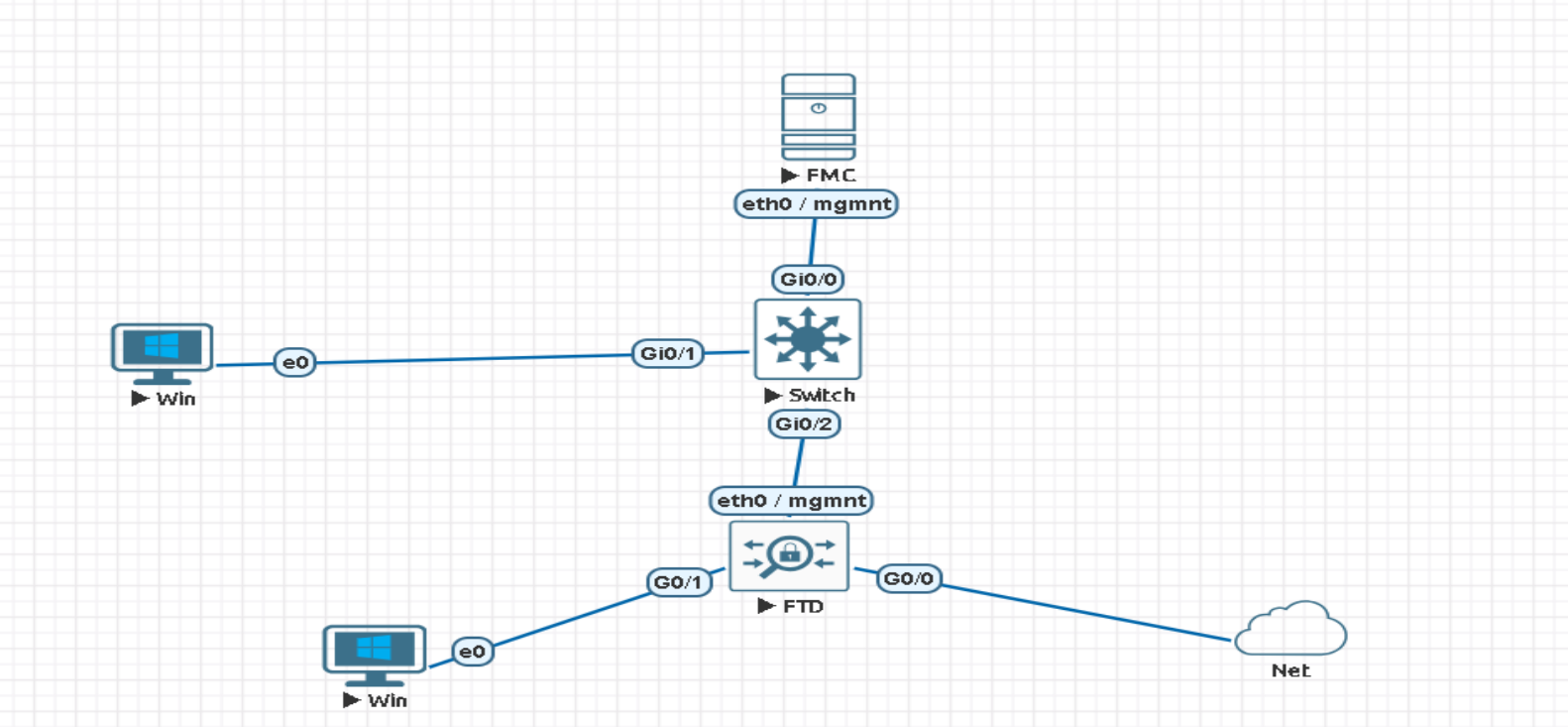


Lab Setup Overview

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:

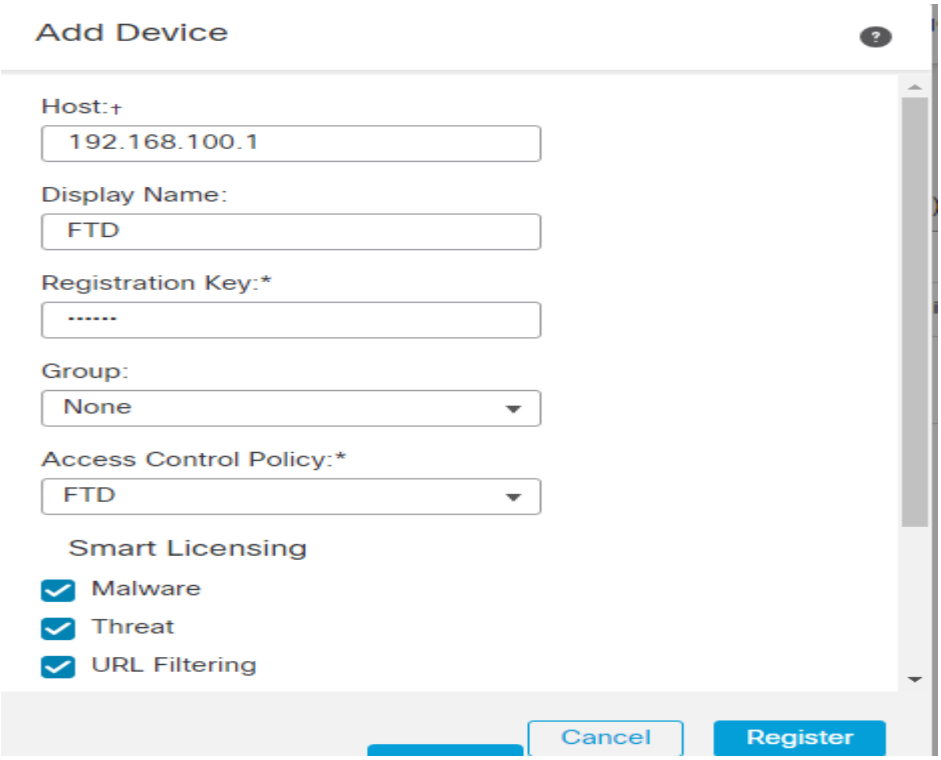
#show managers

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**.



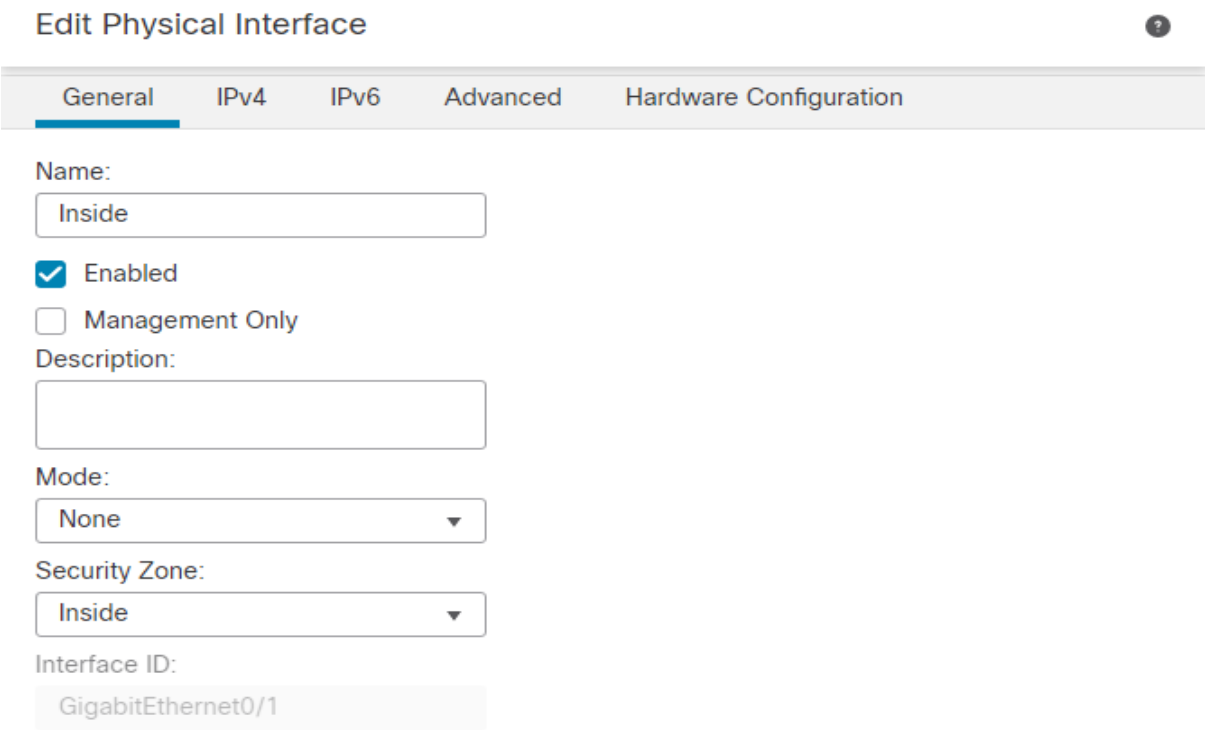

```
> show managers
Type                          : Manager
Host                          : 192.168.100.10
Registration                  : Completed
```

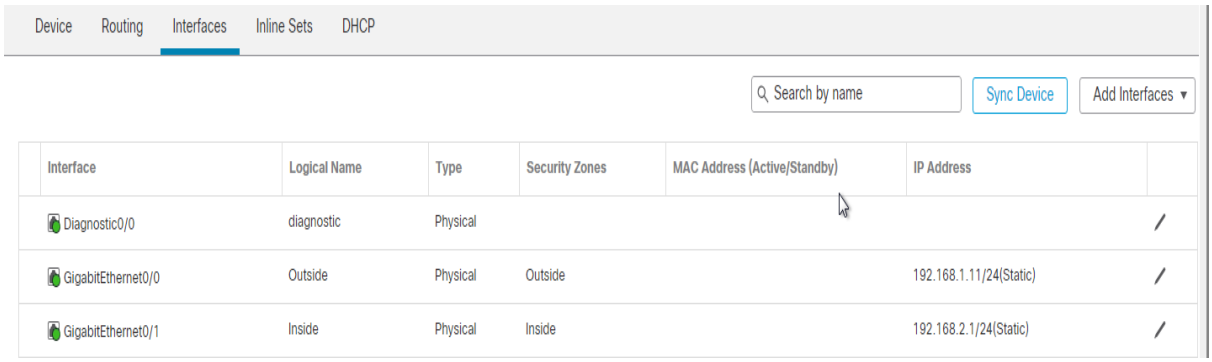
Post-Registration Configuration

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.

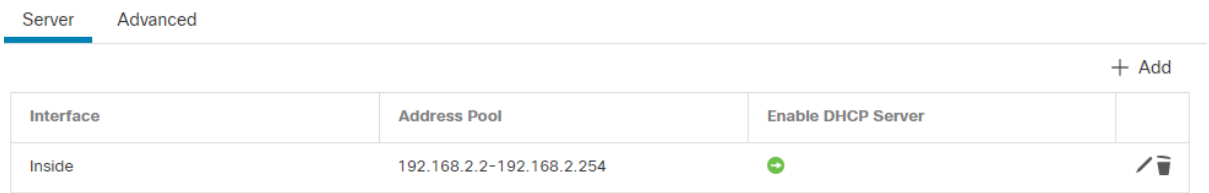




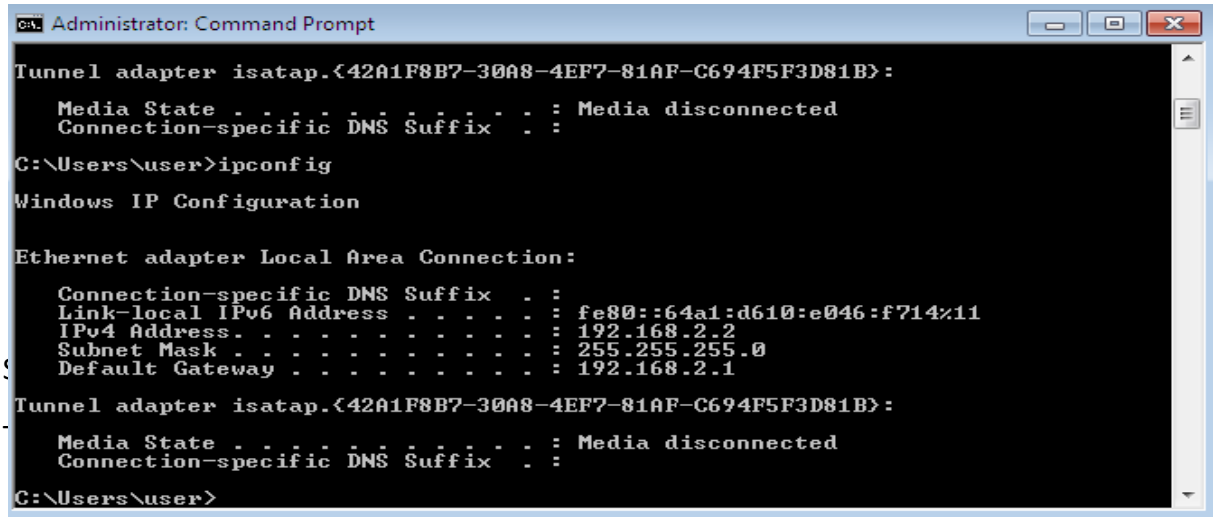
Configuring DHCP Server for Inside Zone

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**.



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

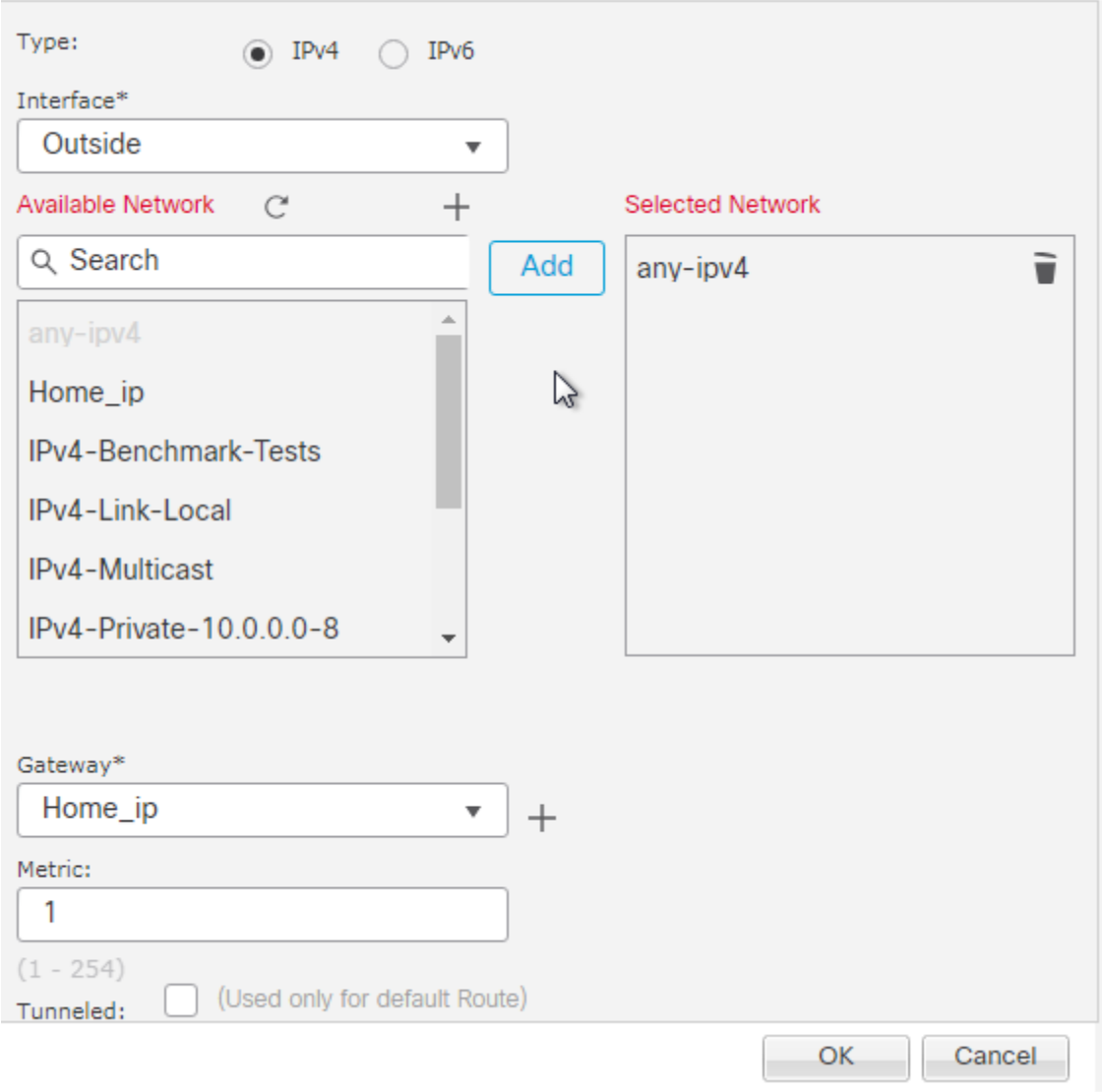


Internet Access Components

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:

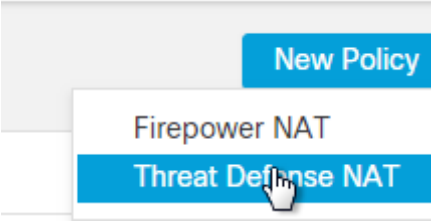


Click **Add** and set:

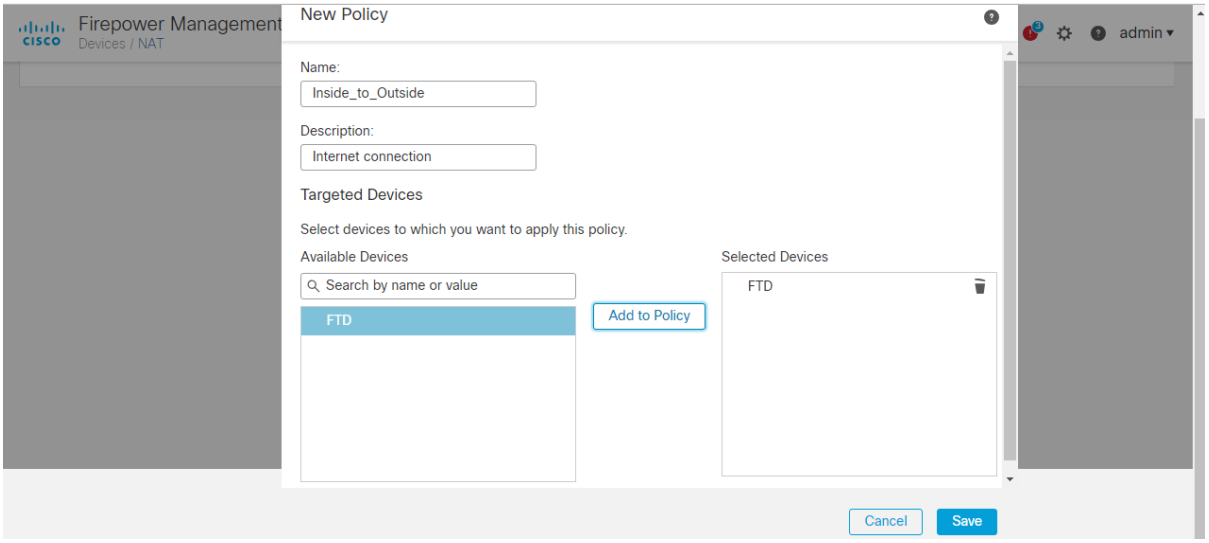
- **Interface:** Outside
- **Network:** 0.0.0.0/0
- **Gateway:** (the next-hop IP of your cloud/internet network)

In the FMC devices tap choose the NAT option

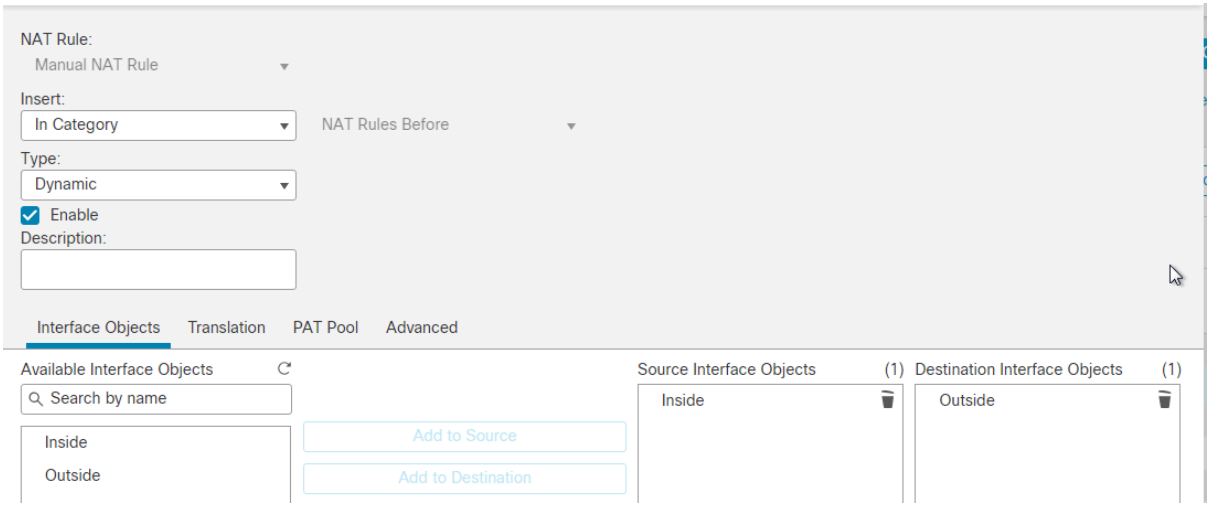
Then create a new policy for FTD

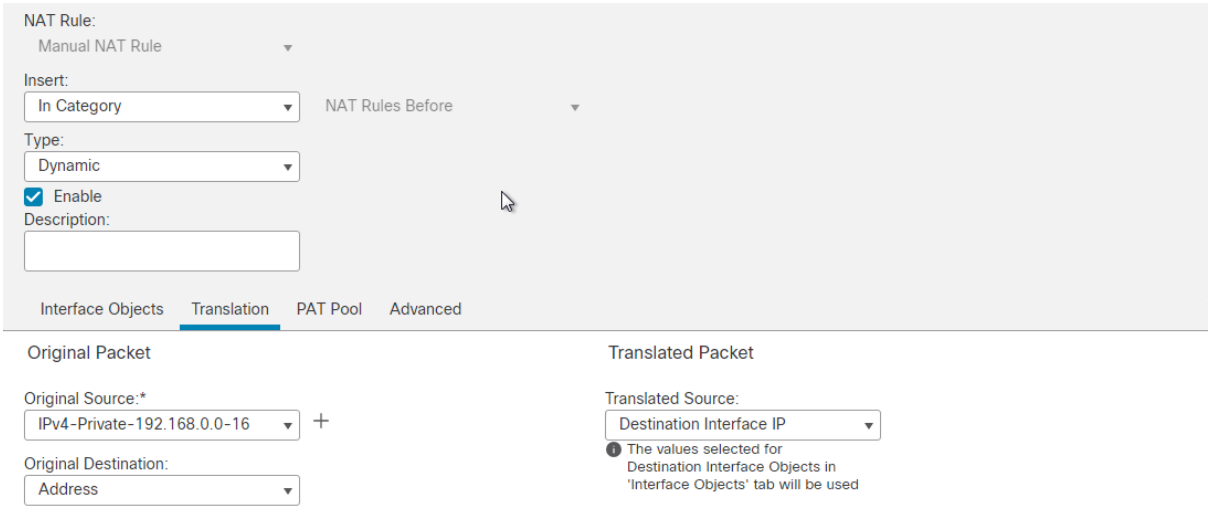


Choose the FTD device



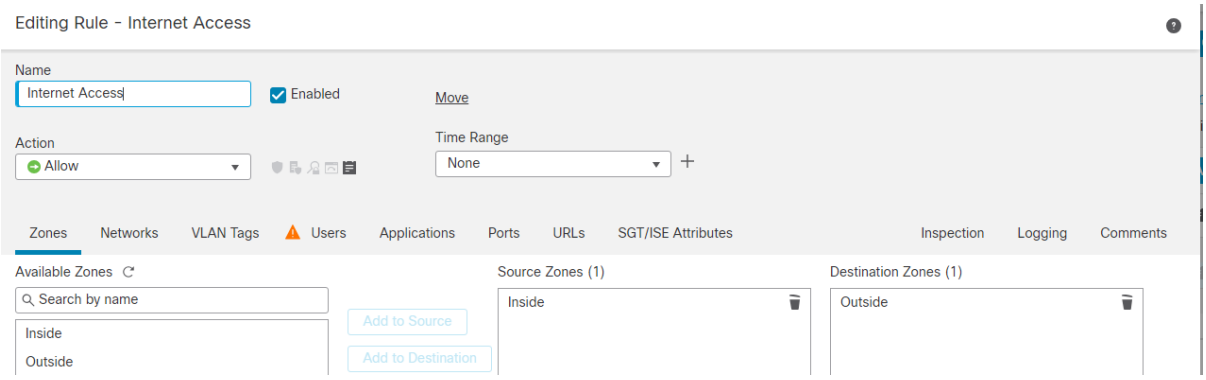
Then create the NAT rule:





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

1.



Then it works: