Securing Networks with

Cisco FTD

Chapter 4

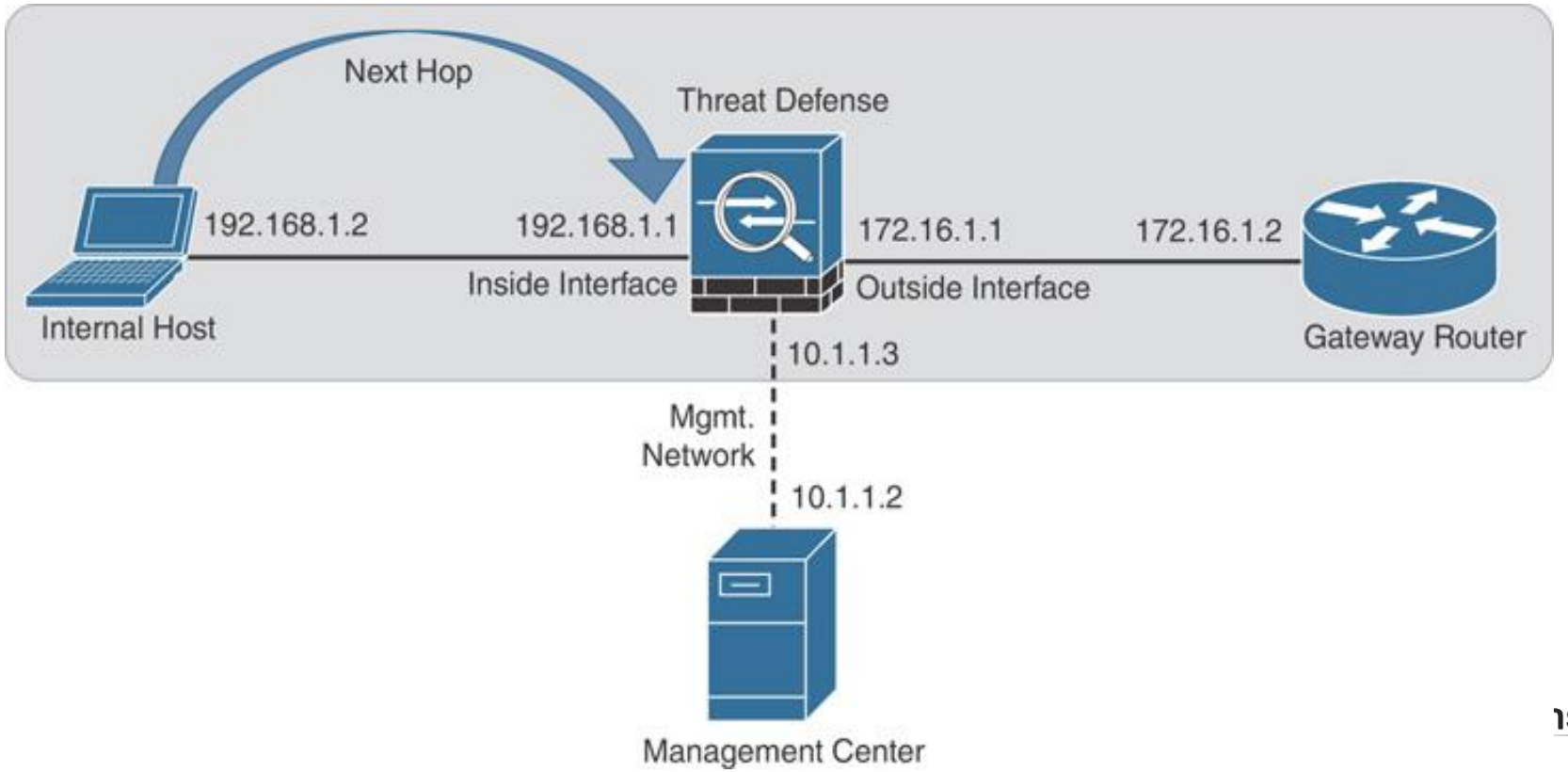
FTD Deployment Modes

Mohsen Kheradmand

Deployment in Routed Mode

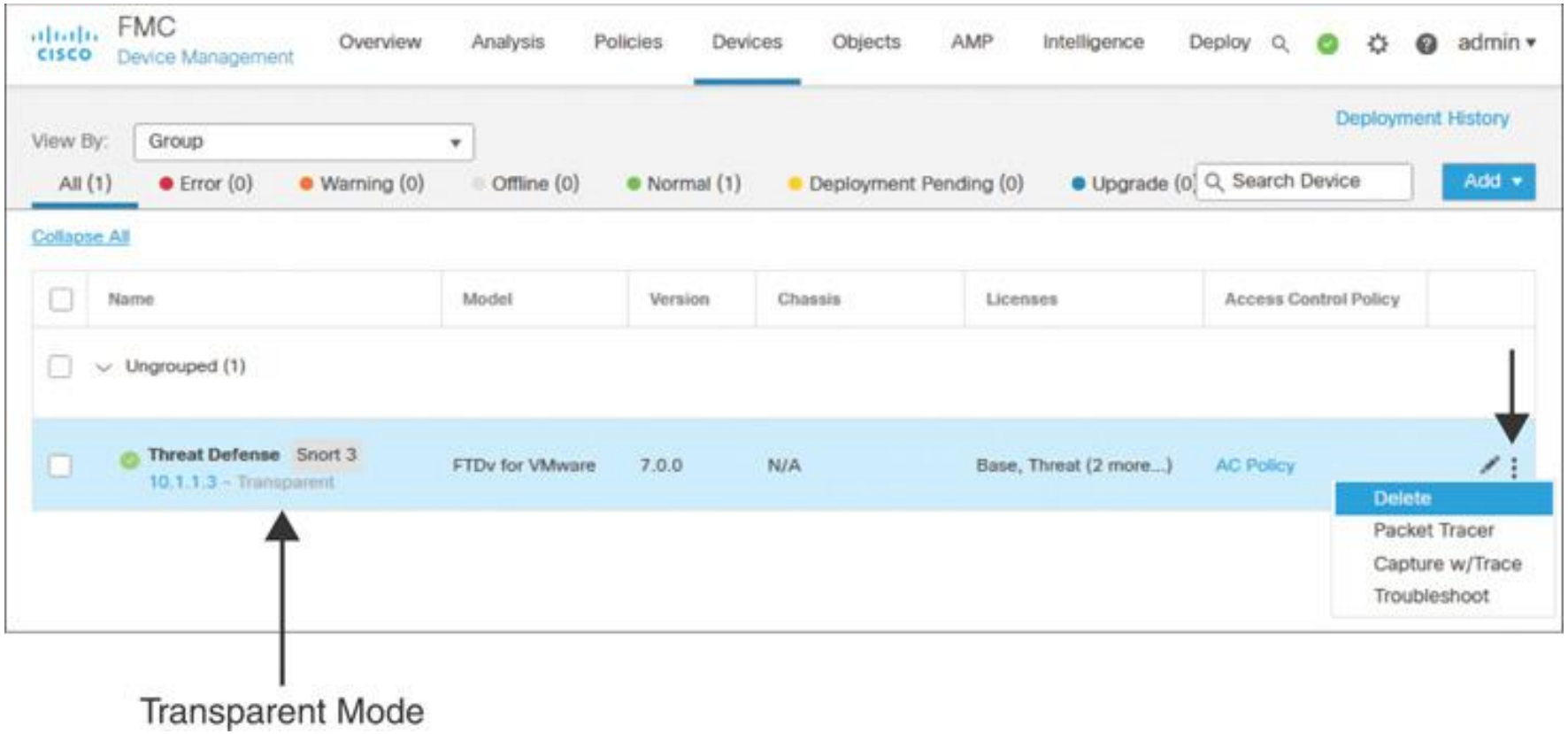
Routed mode

- In Routed mode, a threat defense acts like a Layer 3 Router
- Each interface has a different IP and subnet and act as the default gateway for that subnet.
- The FTD also route traffic between different subnets, like a Layer 3 router.



Change FTD mode to Routed mode

- If the FTD is in transparent mode and registered in FMC , first Unregister it



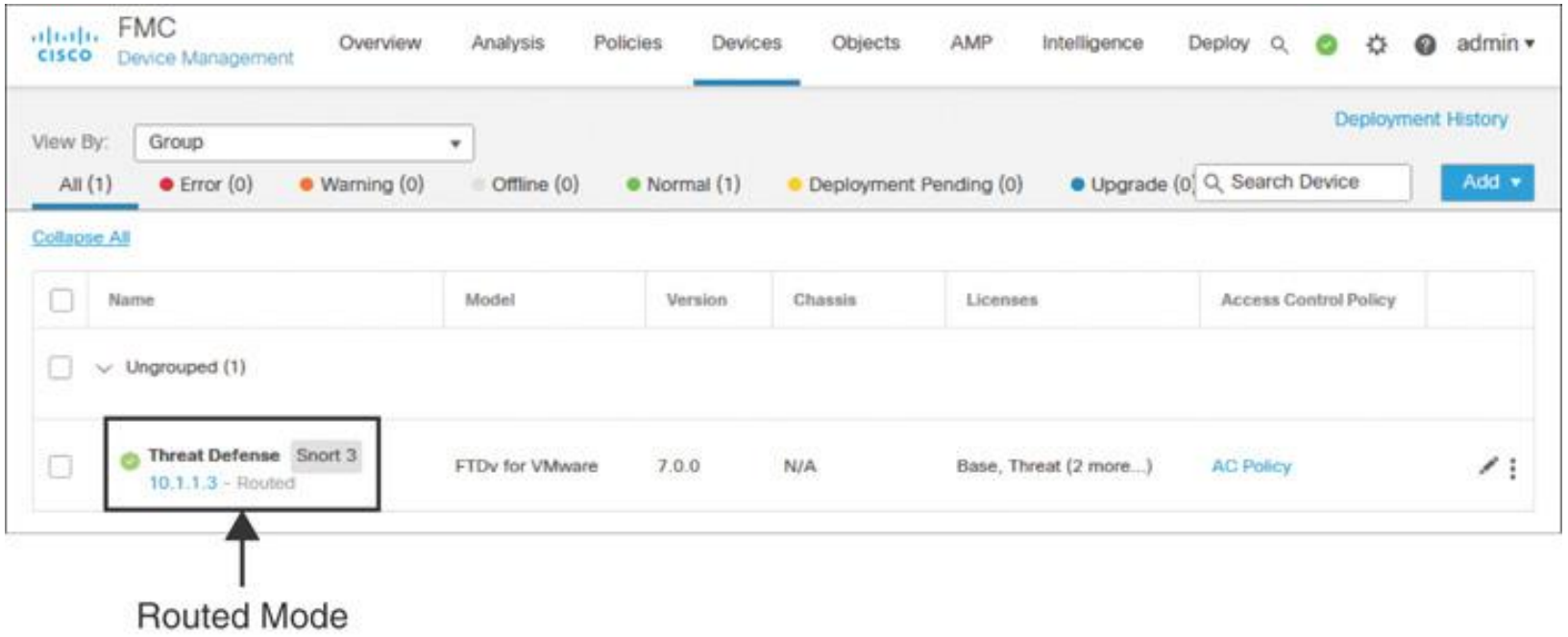
✓ Note : Changing the firewall mode wipes out any existing configurations on a threat defense.

Change FTD mode to Routed mode

- Connect to FTD via SSH or console
- Enter command : Configure firewall routed

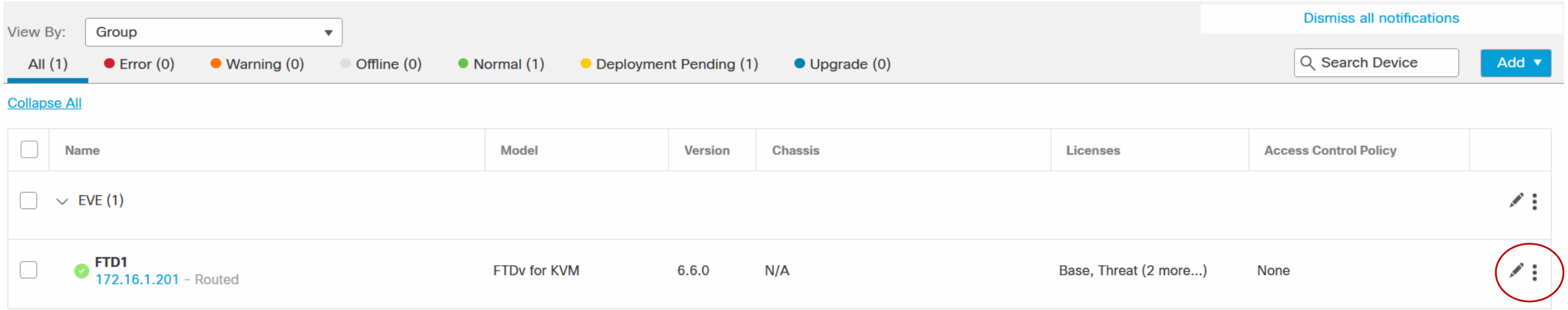
```
> configure firewall
  routed       Change to routed firewall mode
  transparent  Change to transparent firewall mode
```

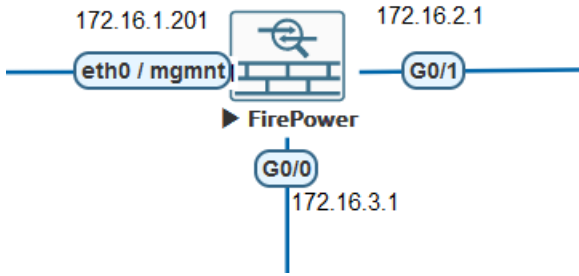
- After routed mode applies , specify Manager again
- Go to the FMC and add FTD via Device menu



Configuration of the Routed Interface

- Click on FTD device or click pencil icon





Configuration of the Routed Interface

- Click on FTD device or click pencil icon

FTD1

Cisco Firepower Threat Defense for KVM

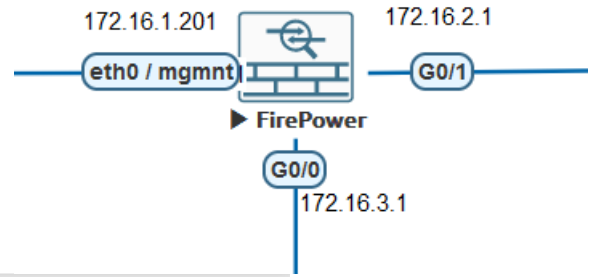
Save | Cancel

Device | Routing | Interfaces | Inline Sets | DHCP

Search by name | Sync Device | Add Interfaces

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Virtual Router
Diagnostic0/0	diagnostic	Physical				Global
GigabitEthernet0/0		Physical				
GigabitEthernet0/1		Physical				
GigabitEthernet0/2		Physical				
GigabitEthernet0/3		Physical				

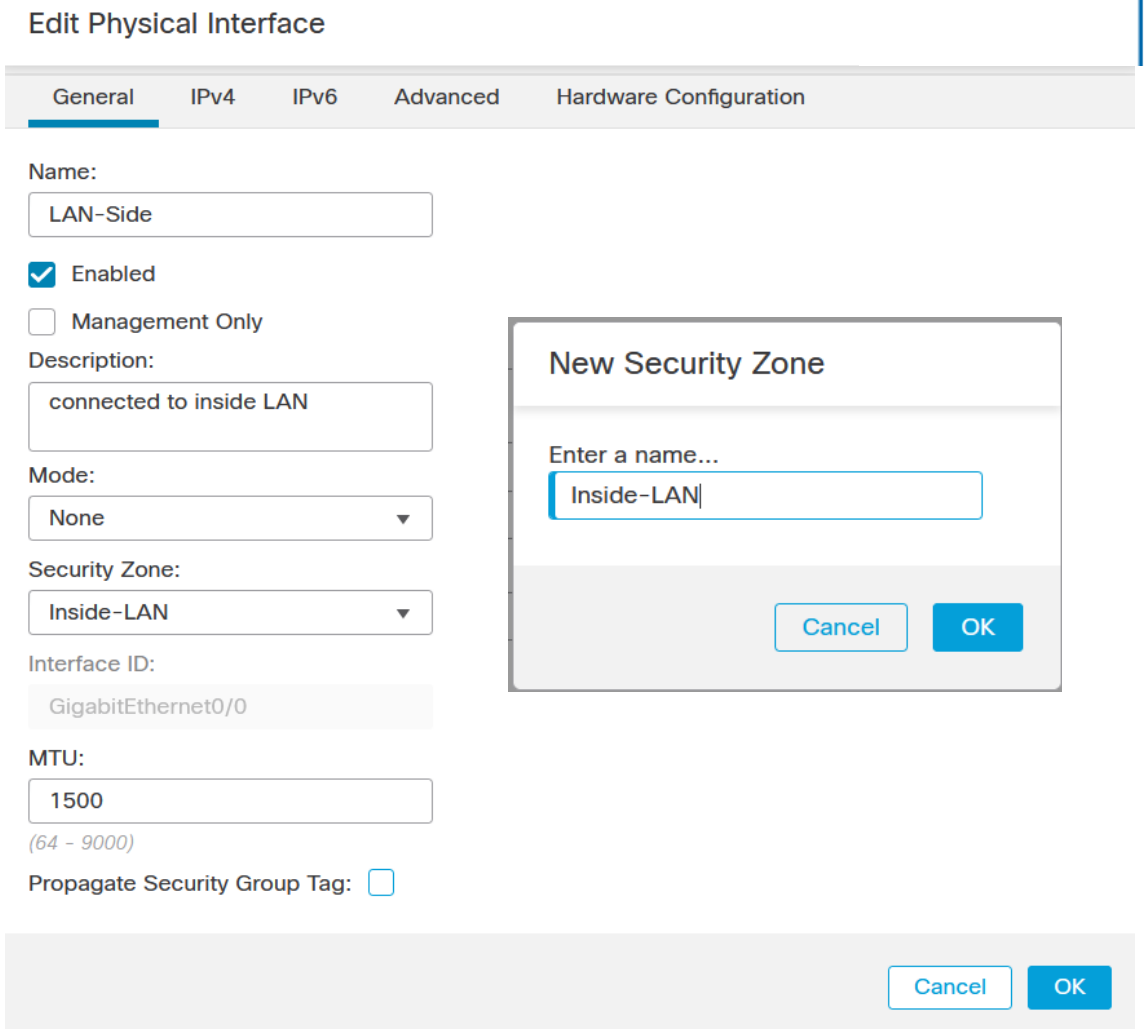
Configuration of the Routed Interface

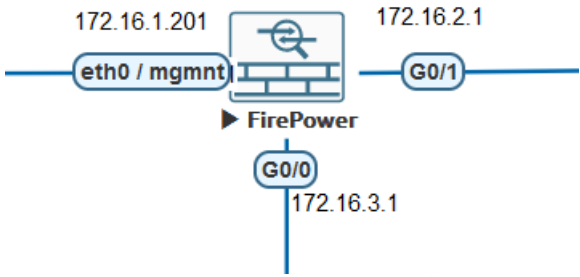


General tab:

- Enter a name for interface
- Select Enabled

- Mode: None / Passive / ERSPAN
- Security Zone : select one or create a new zone





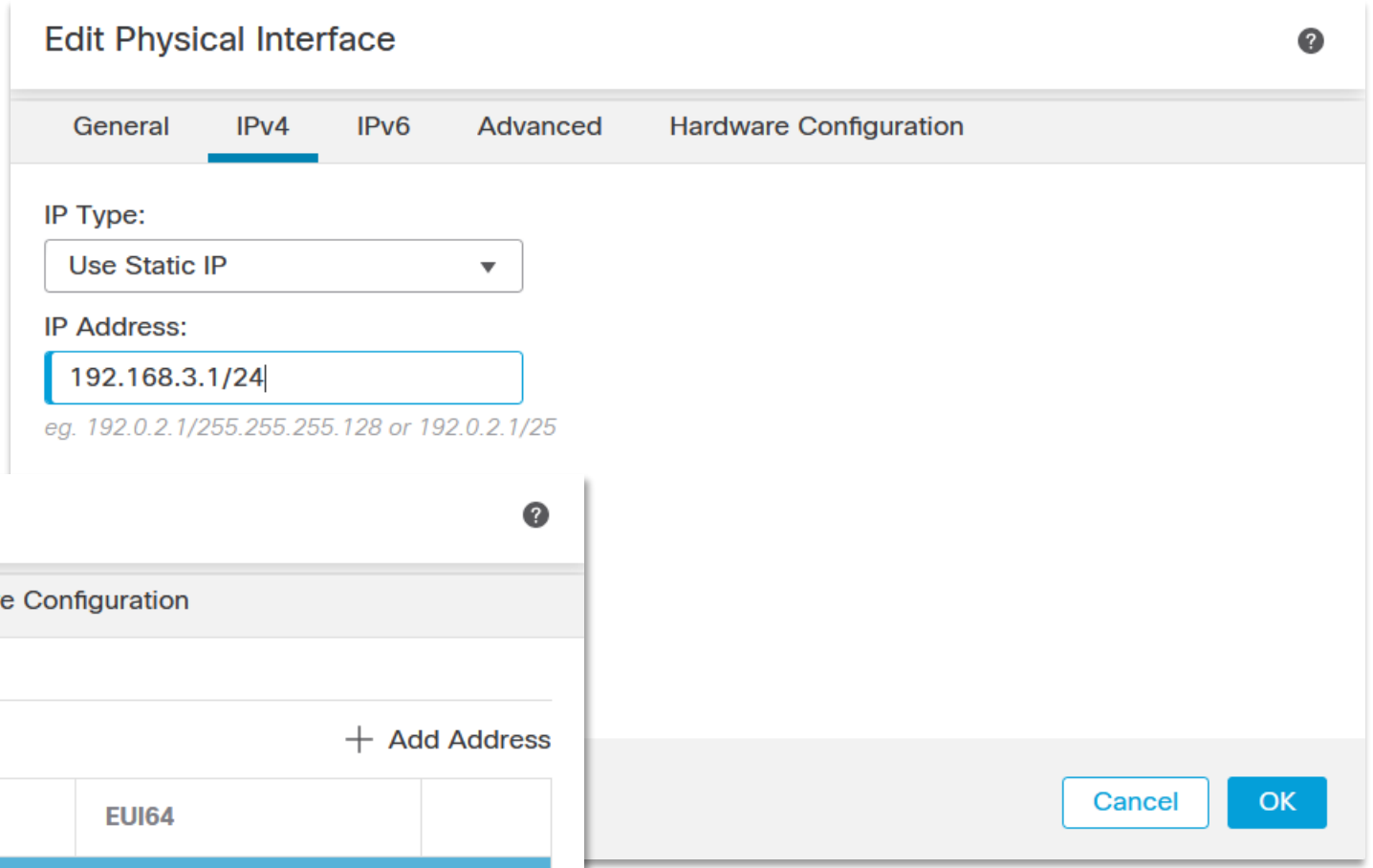
Configuration of the Routed Interface

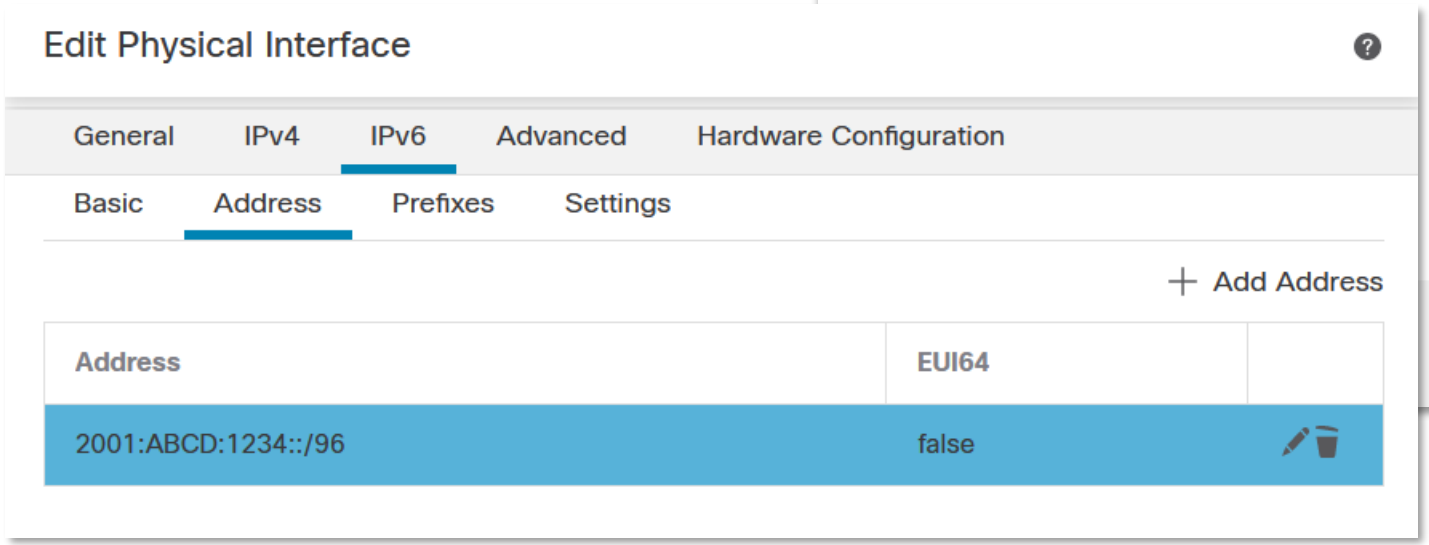
IPV4 tab

- Select IP type : Static / DHCP / PPOPE
- Enter IP address/prefix (in statis type)

IPV6 tab

- Enter IPv6 address and setting (in case)



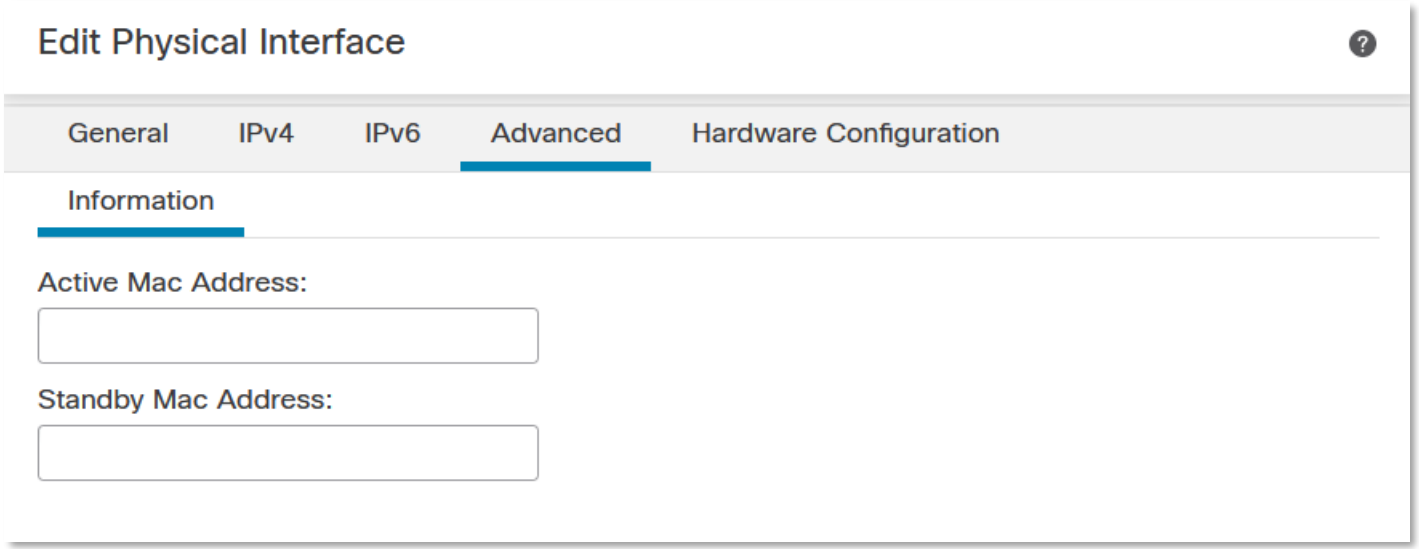


MohsenKheradmand MK

Configuration of the Routed Interface

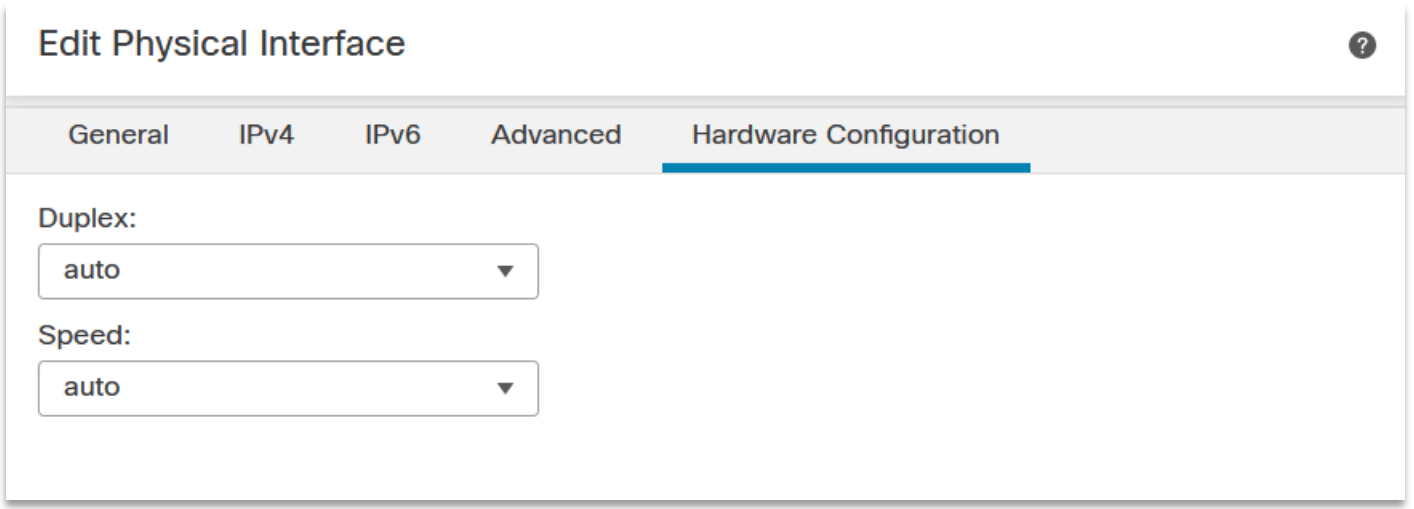
Advanced tab

- You can enter optional Active and standby MAC address



Hardware configuration tab

- Duplex setting : auto/full/half
- Speed : auto/10/100/1000

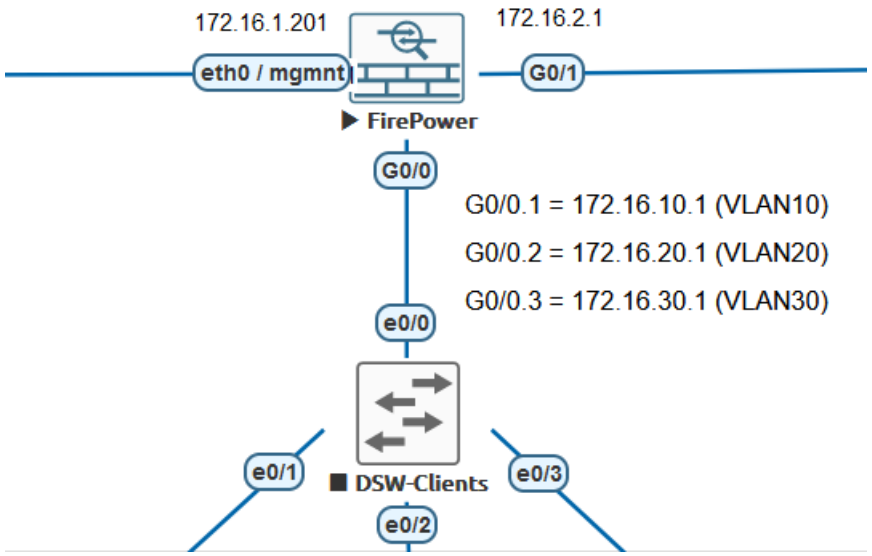


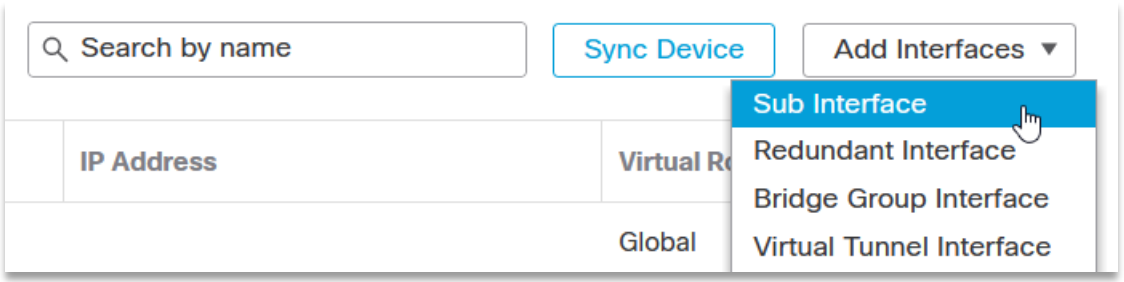
- ➢ Click OK
- ➢ Then Click Save in FMC

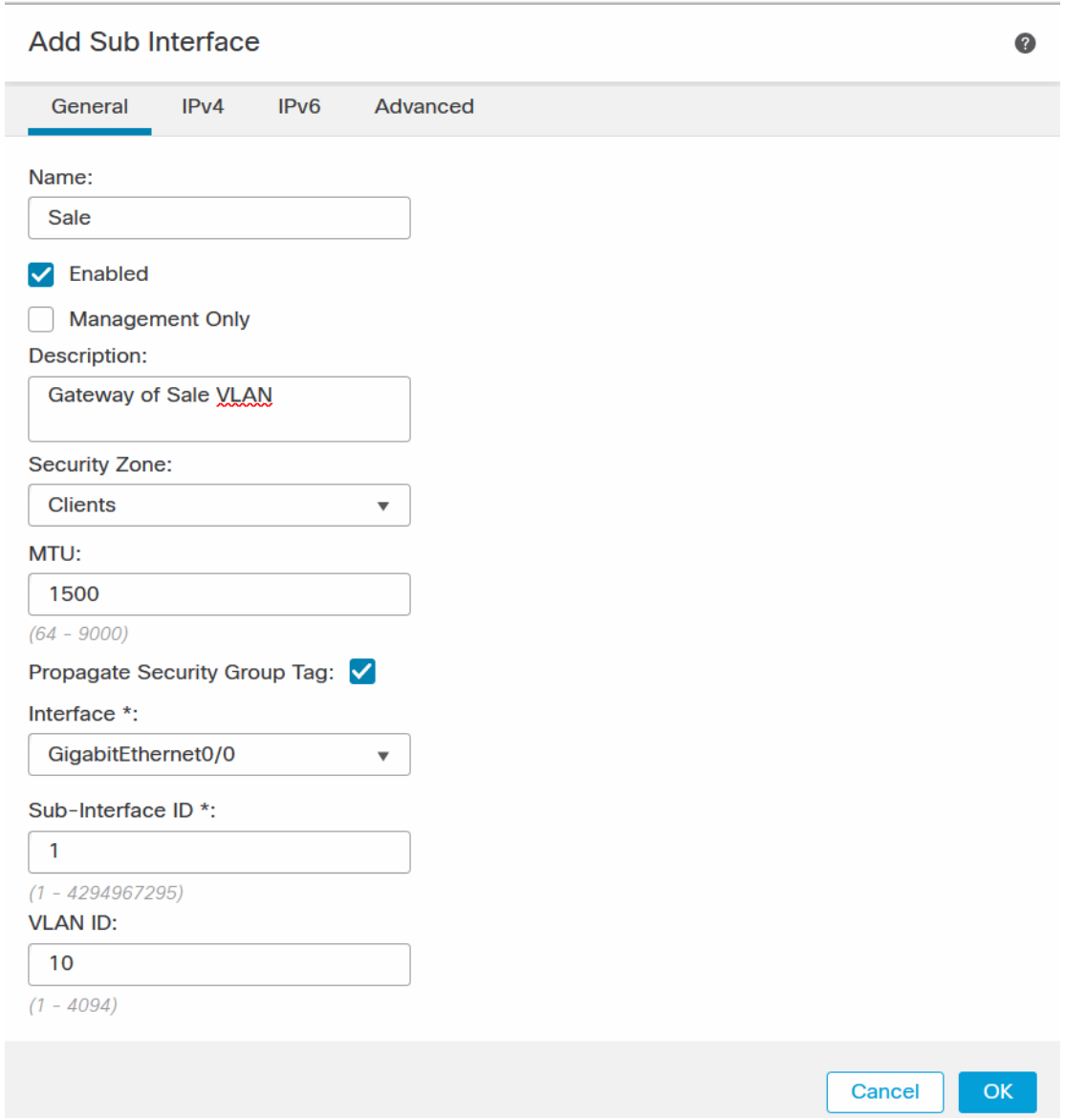
- ➢ After all click deploy to deploy configs to FTD

Configuration of the Routed Interface

- Create sub interface

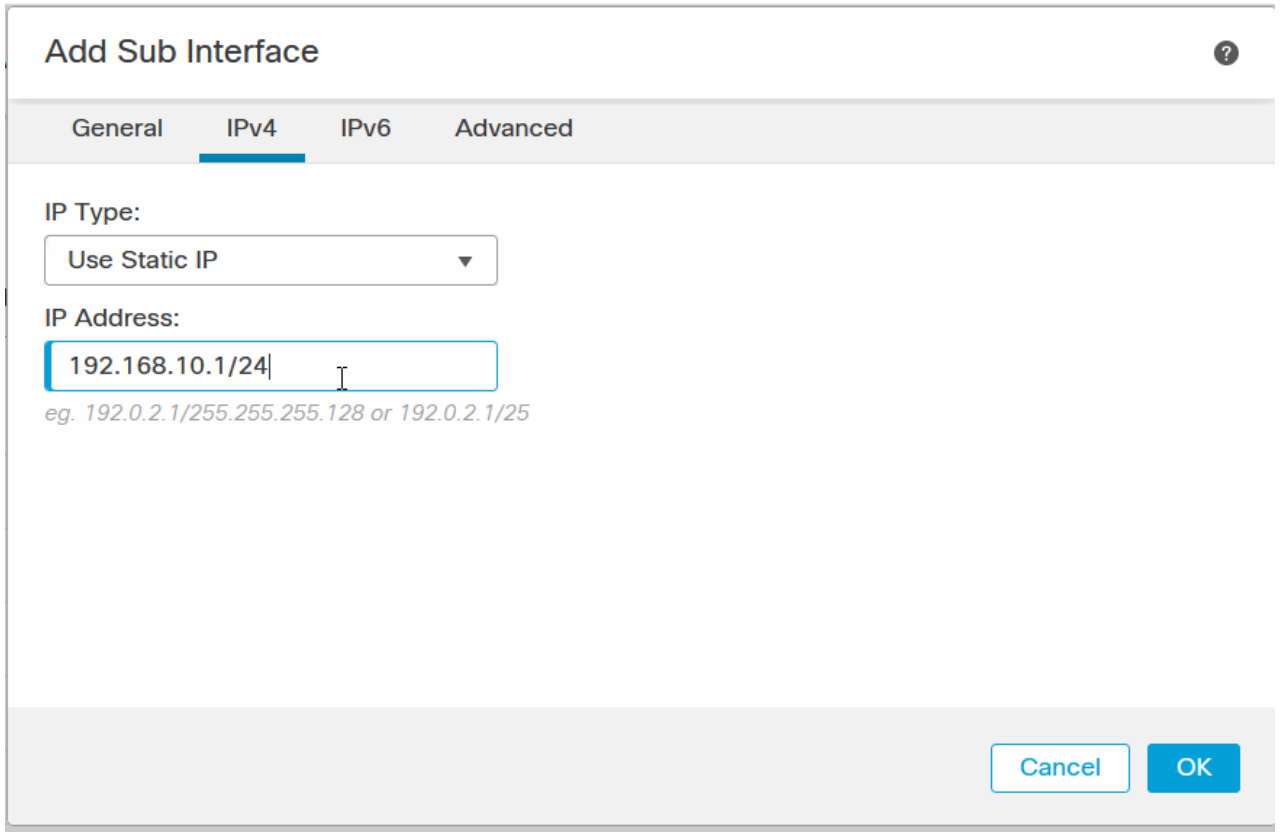




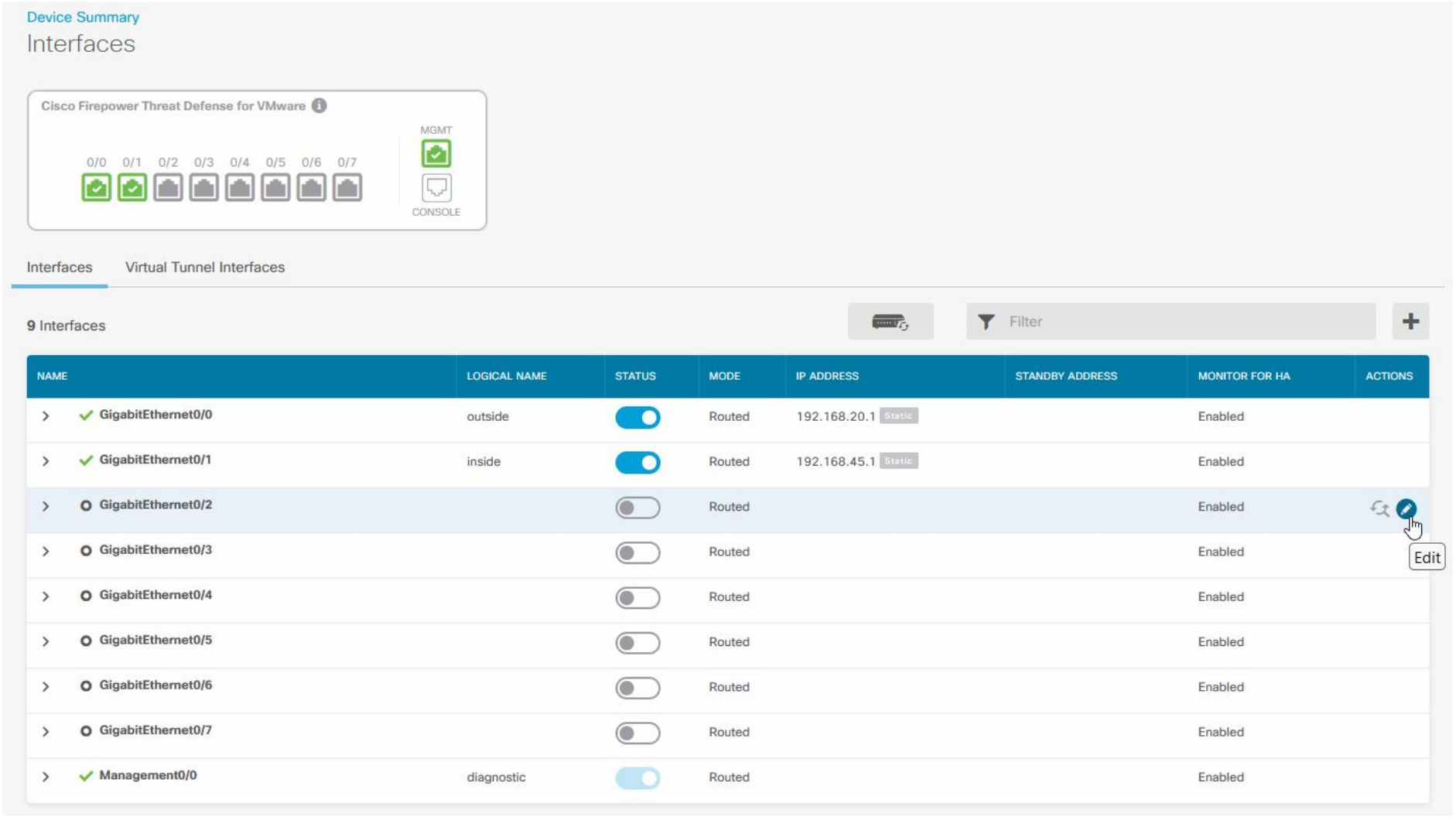


Configuration of the Routed Interface

- Create sub interface

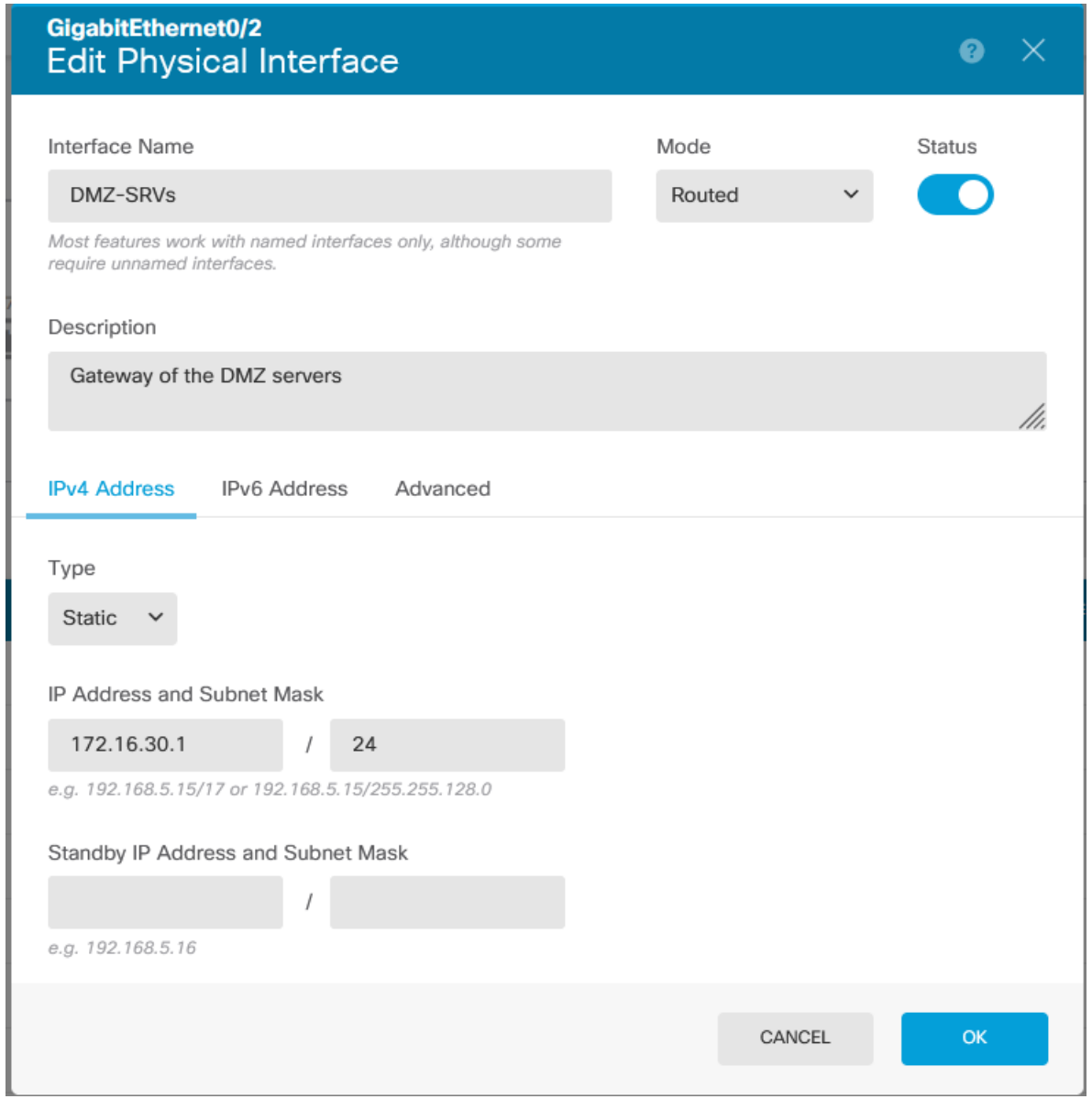


FTD Interface Setting via FDM



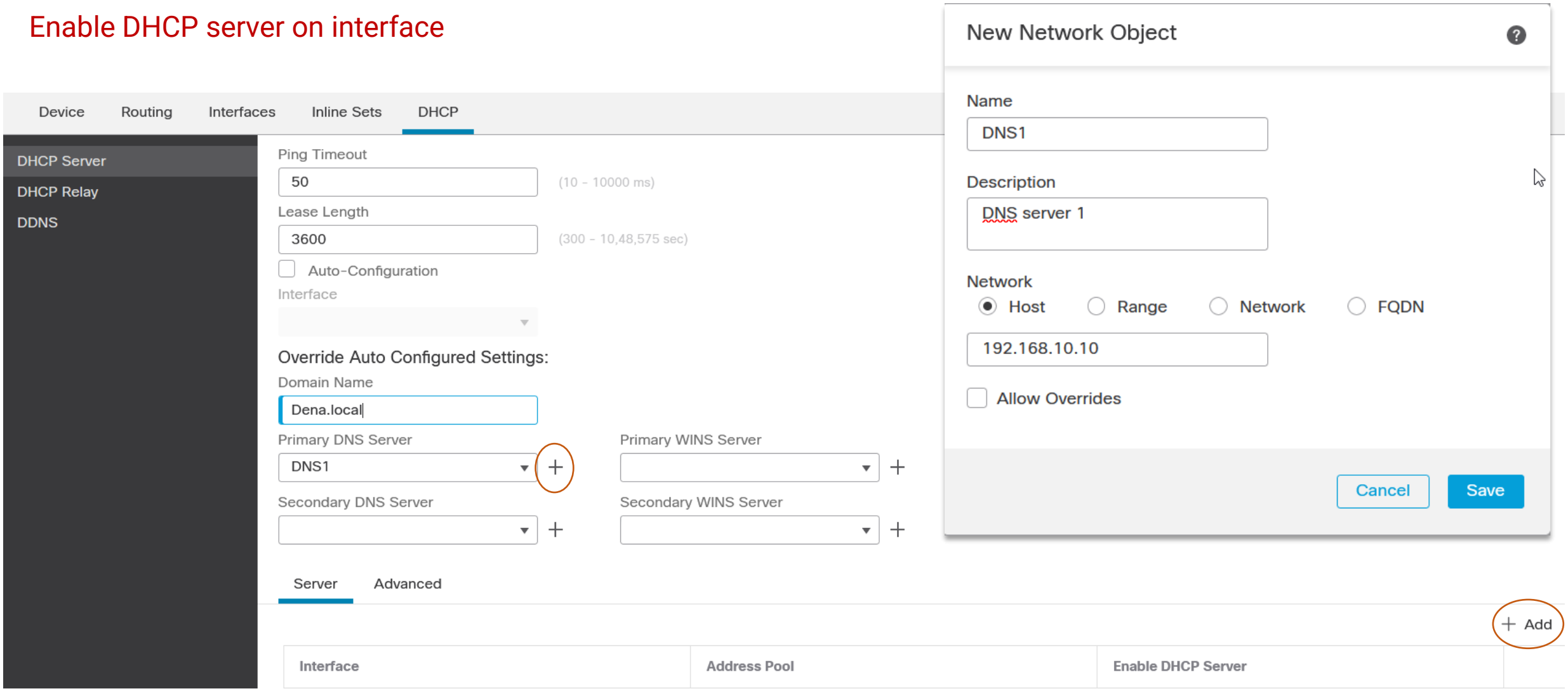
FTD Interface Setting via FDM

- Type a name for interface
- Select mode: routed
- Enter IPv4 and IPv6 configuration
- Click OK and Deploy to FTD



DHCP server

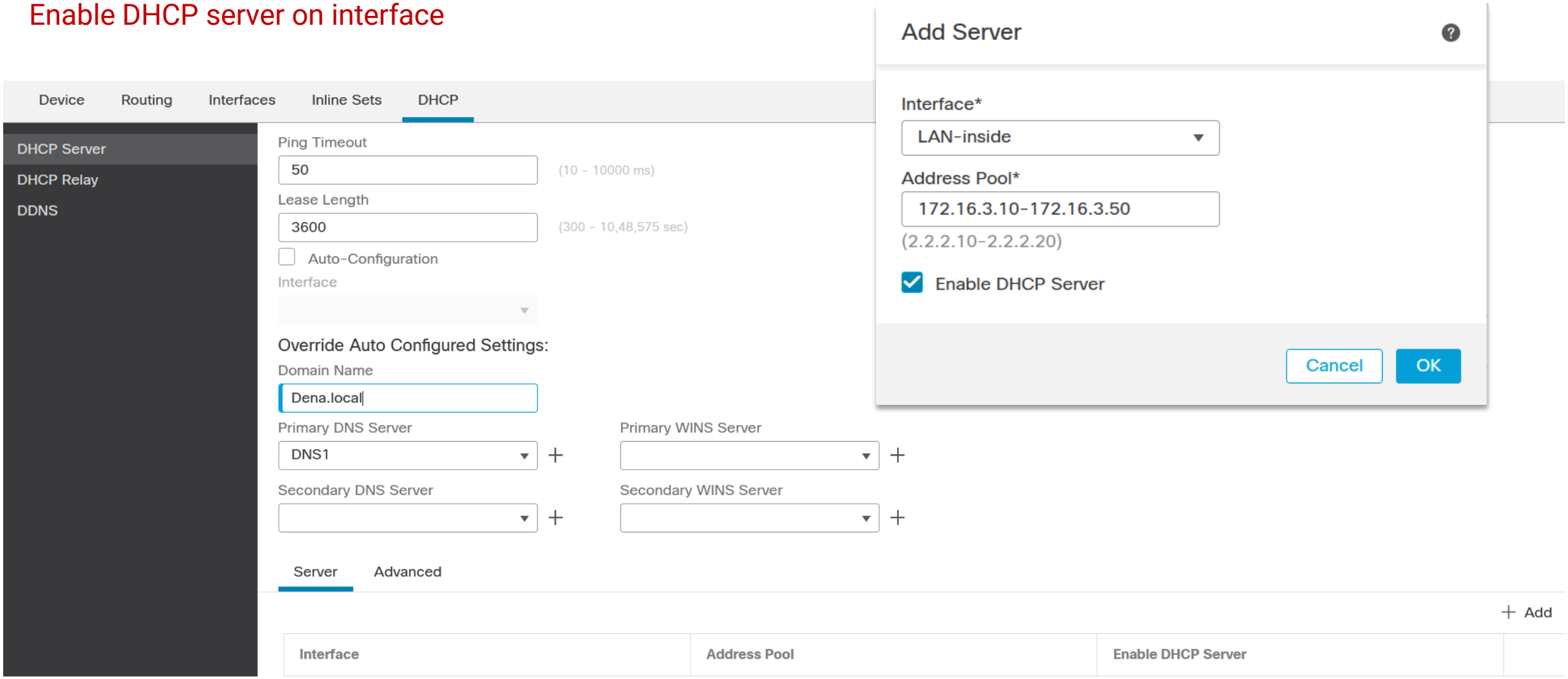
Enable DHCP server on interface



MohsenKheradmand MK

DHCP server

Enable DHCP server on interface



MohsenKheradmand MK

Basic verification commands

Debugging ICMP Traffic FTD

<debug icmp trace

Interface status and configuration

> show ip
>show interface ip brief
>show interface interface_ID
>show running-config interface

IP Address Assignment from a DHCP Address Pool

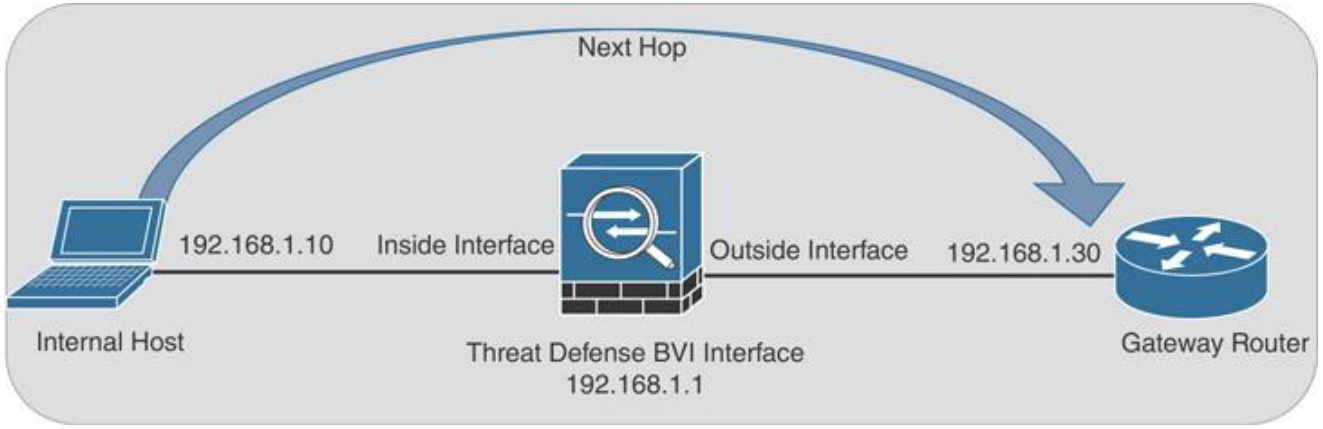
> show dhcpd binding
> debug dhcpd packet

Deployment in Transparent Mode

Transparent mode

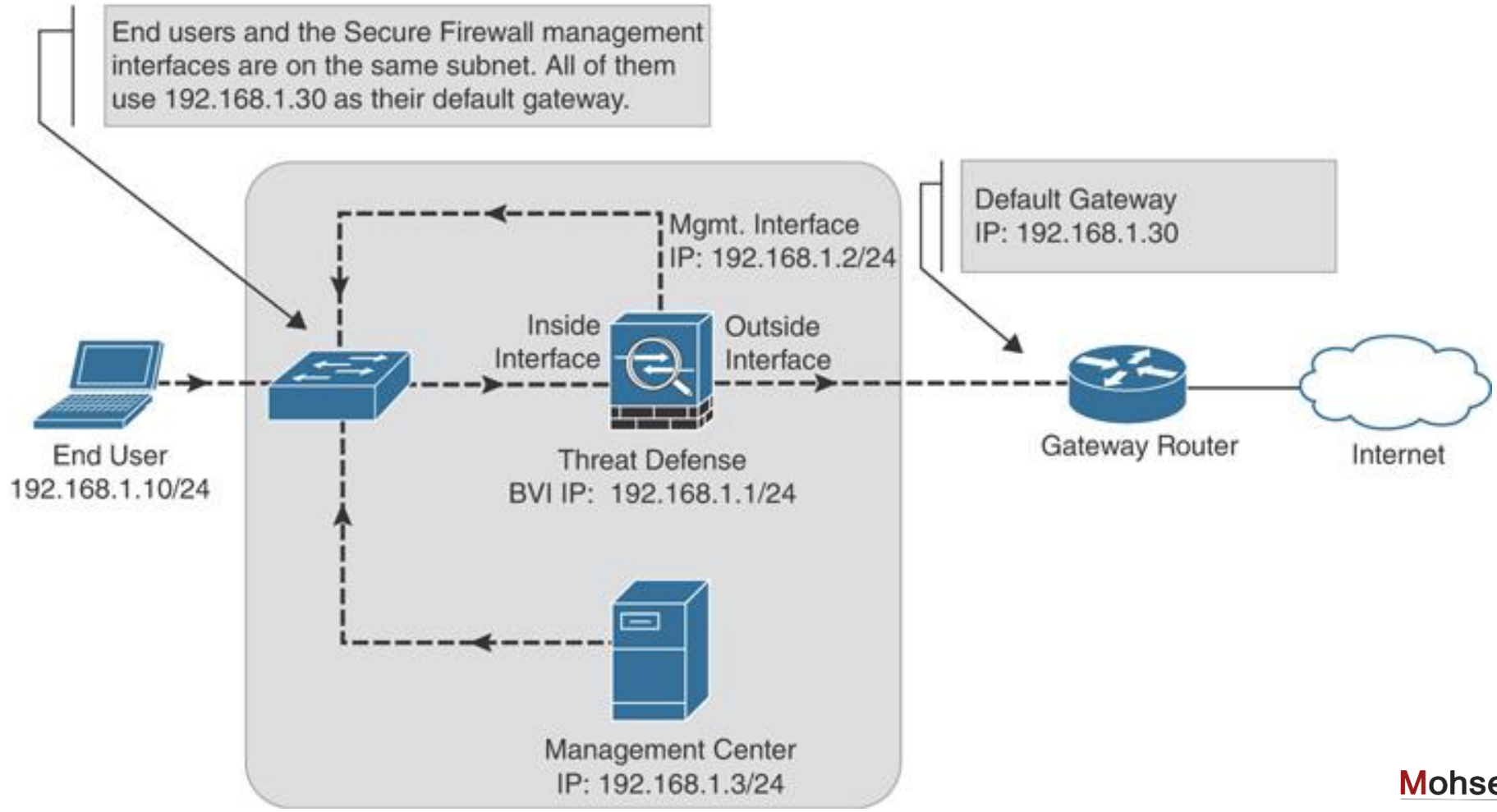
- In transparent mode, a FTD bridges the inside and outside interfaces into a single Layer 2 network

- In this mode , FTD can control traffic as a firewall and inspect traffic as an IPS while remains transparent to the hosts
- No IPv4 assignment to a directly connected interface
- You can, however, assign an IP address to the Bridge Virtual Interface (BVI) that comes with each bridge group
- A firewall in routed-mode can also be used as a VPN server. but in transparent mode can not be a VPN server
- You can still enable NAT feature in transparent mode firewall



Transparent mode

- Example : A Threat Defense in Transparent Mode Is Deployed in a Typical Network



Transparent mode

when you plan to deploy the FTD in transparent mode :

1) Changing the firewall mode wipes out any existing threat defense configurations.
2) Take a backup of your security policy configuration is not necessary (the policies are defined and stored on the FMC)
3) Do not use the BVI IP address as the default gateway for the connected hosts
4) By default, FTD in transparent mode blocks the DHCP traffic, multicast traffic, and Dynamic Routing Protocol traffic so , add access control rules to allow any necessary network management traffic
5) If you need a dedicated IPS-only , deploy FTD in inline mode instead of the transparent mode (no BVI , less overhead)

To change the firewall mode :

1) Unregister the FTD in FMC
2) In FTD CLI enter command : > configure firewall transparent
3) Register the FTD in FMC again

Verifying Firewall Deployment Mode

> show firewall

> show managers

Bridge Groups

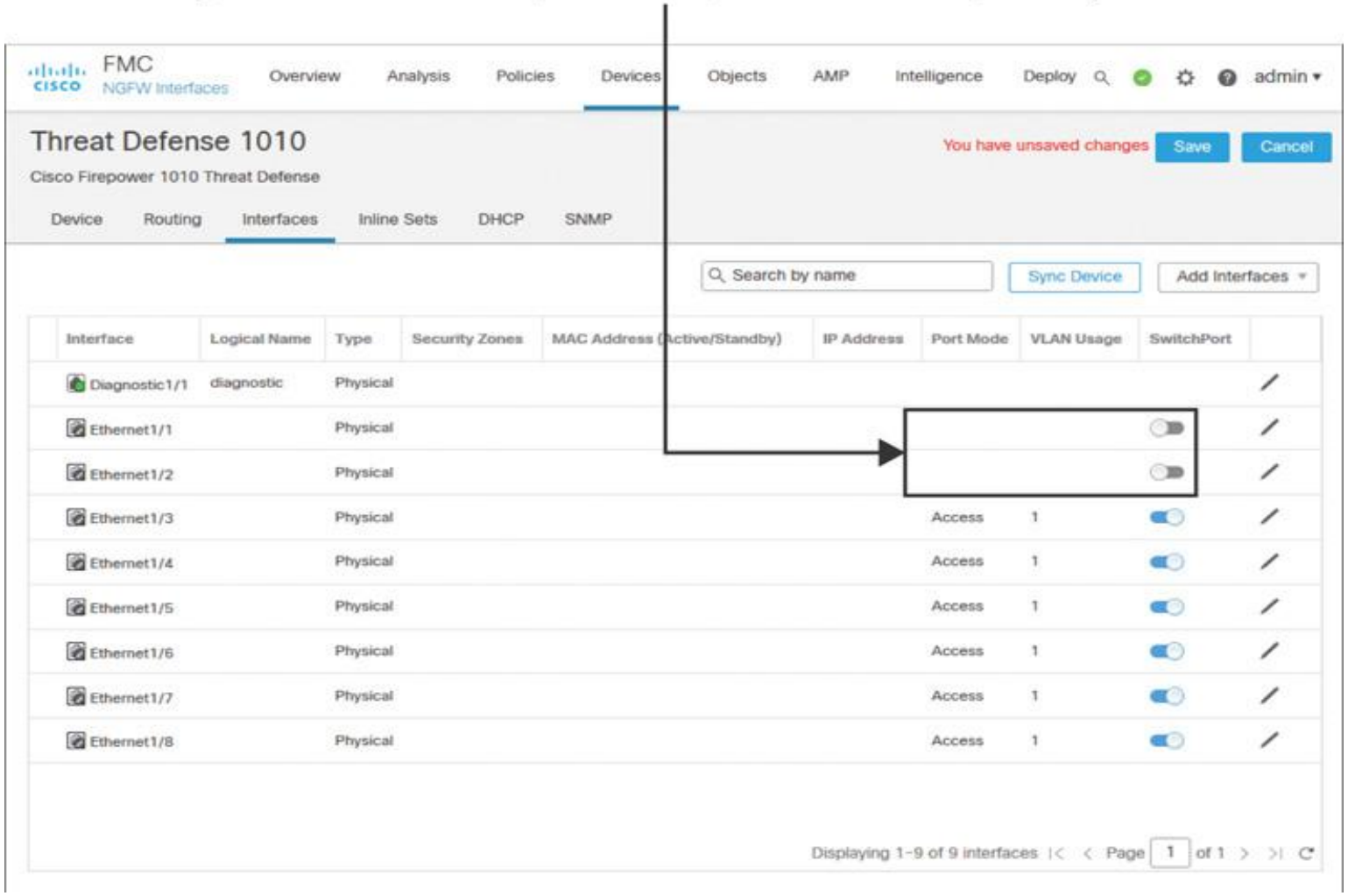
- A bridge group is a group of interfaces that the FTD device bridges instead of routes
- Bridge groups are supported in both transparent and routed firewall mode
- A bridge group represents a unique Layer 2 network (like VLAN)
- You can create multiple bridge groups on a single threat defense
- Hosts within different bridge groups cannot communicate with each other without a router

Bridge Virtual Interface (BVI)

- Each bridge group includes a Bridge Virtual Interface (BVI).
- The FTD device uses the BVI IP address as the source address for packets originating from the bridge group
- The BVI IP address must be on the same subnet as the bridge group member interfaces
- In routed mode: The BVI acts as the gateway between the bridge group and other routed interfaces
- For some interface-based features, you can use the BVI itself:
  - ✓ DHCPv4 server—Only the BVI supports the DHCPv4 server configuration.
  - ✓ Static routes: You can configure static routes for the BVI; you cannot configure static routes for the member interfaces.
  - ✓ Syslog server and other traffic sourced from the FTD device (Syslog , SNMP)

Configure interface in Transparent mode

To configure an interface in transparent mode, disable the switch port using the slider.



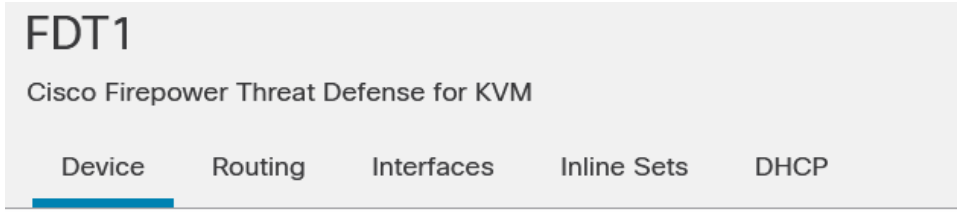
In some FTD models (like 1000 series) there is switchport interfaces

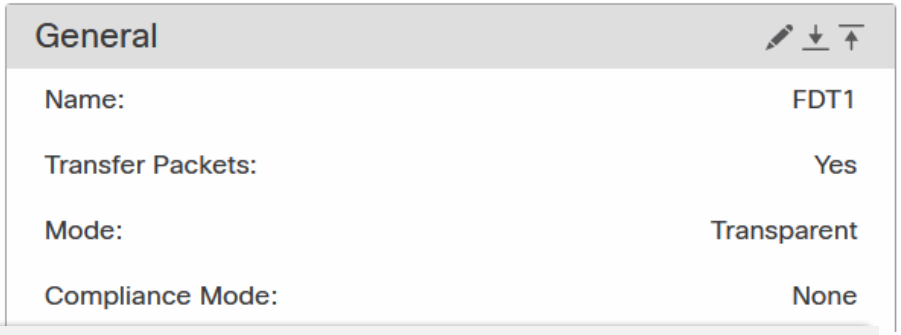
Switchport interfaces cannot be configured in a transparent mode so switchport must be disabled

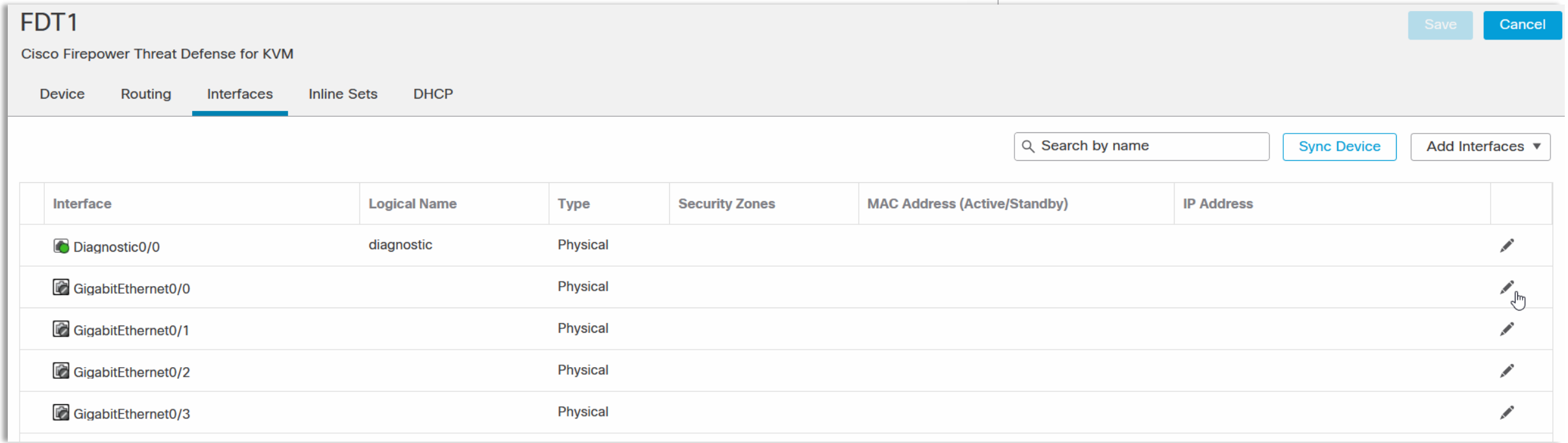
Configure interface in Transparent mode

Click device to check whether is in transparent mode

Click Interface and click on pencil icon







Configure interface in Transparent mode

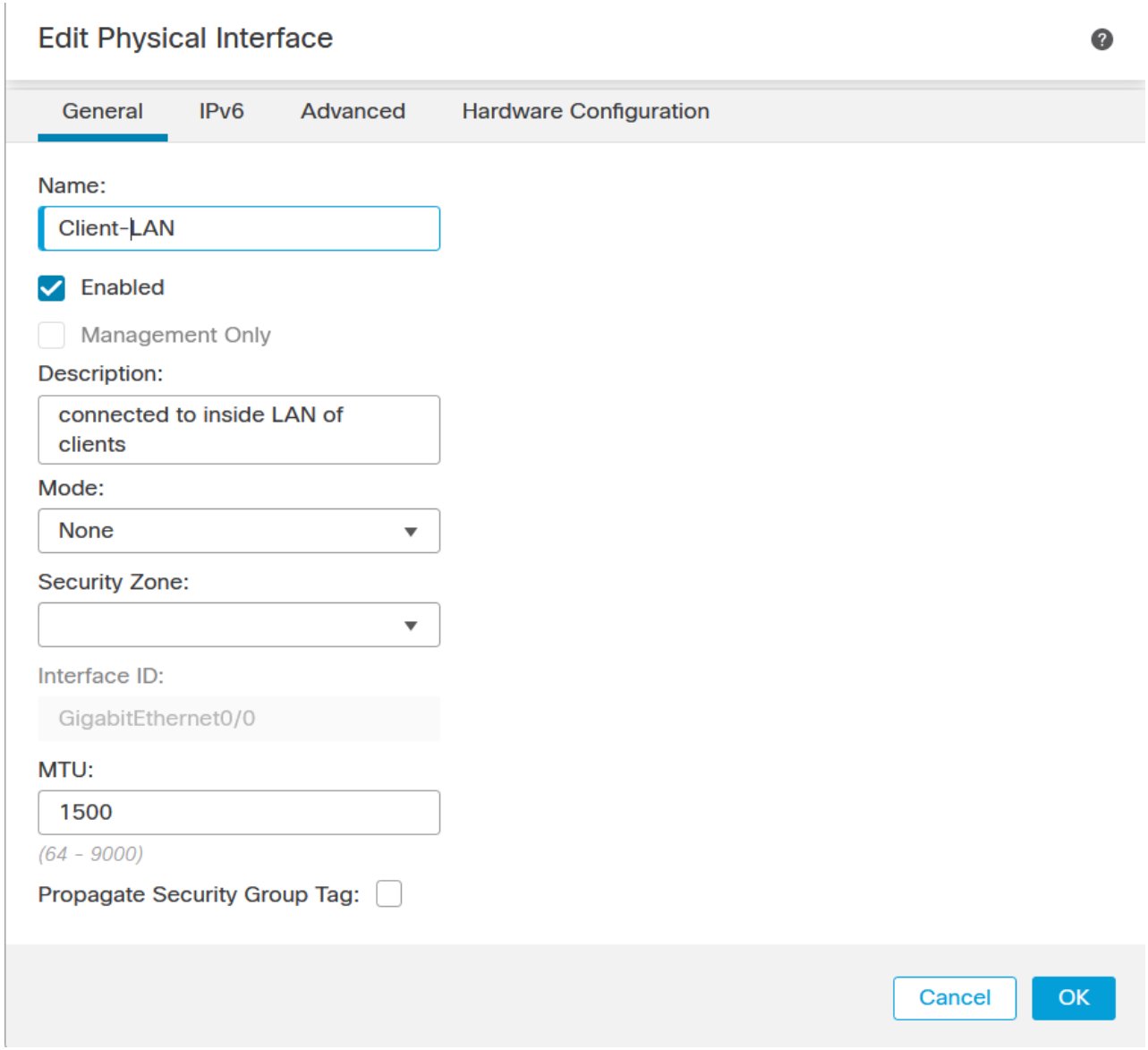
Enter a name for interface

Click Enabled

Description : (optional)

Mode : None / passive

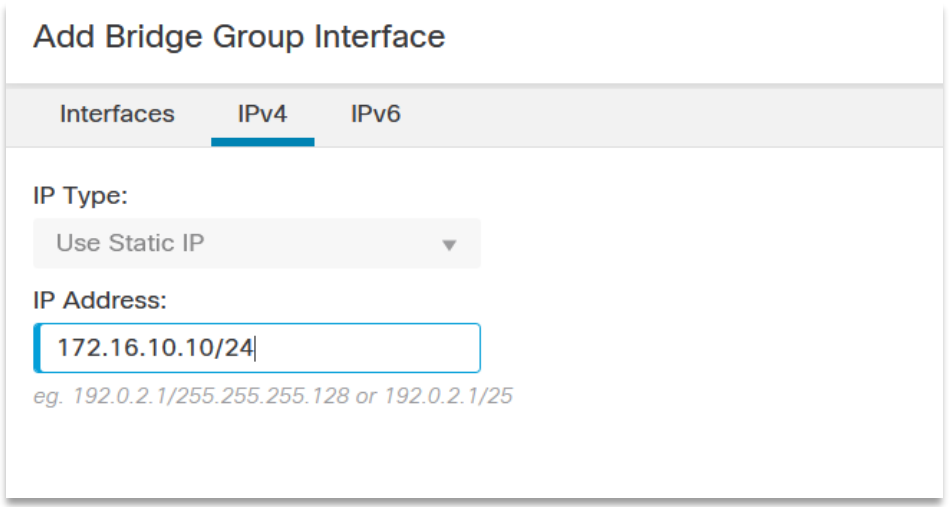
Security zone : (optional)

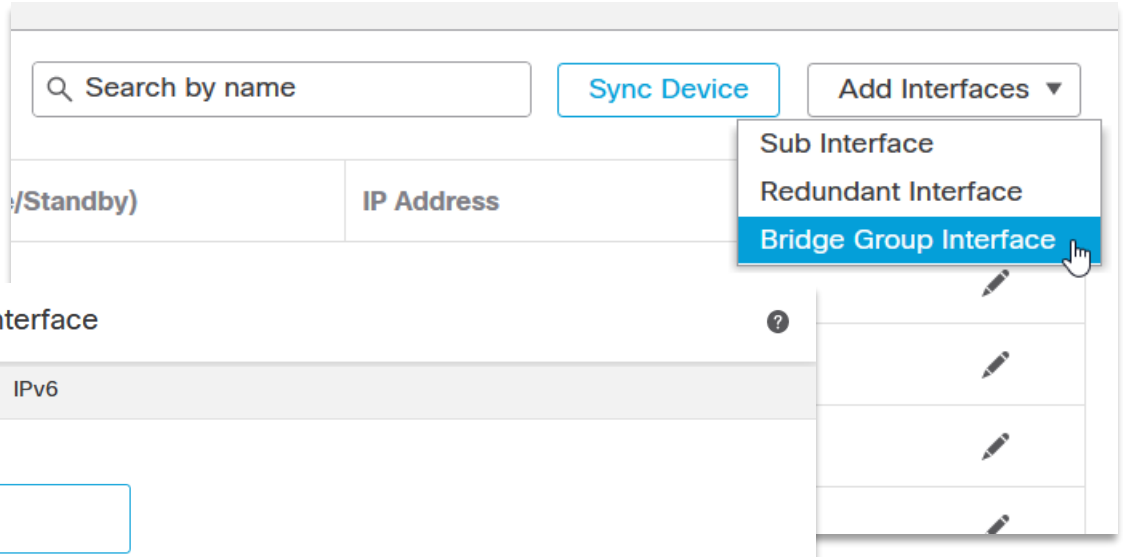


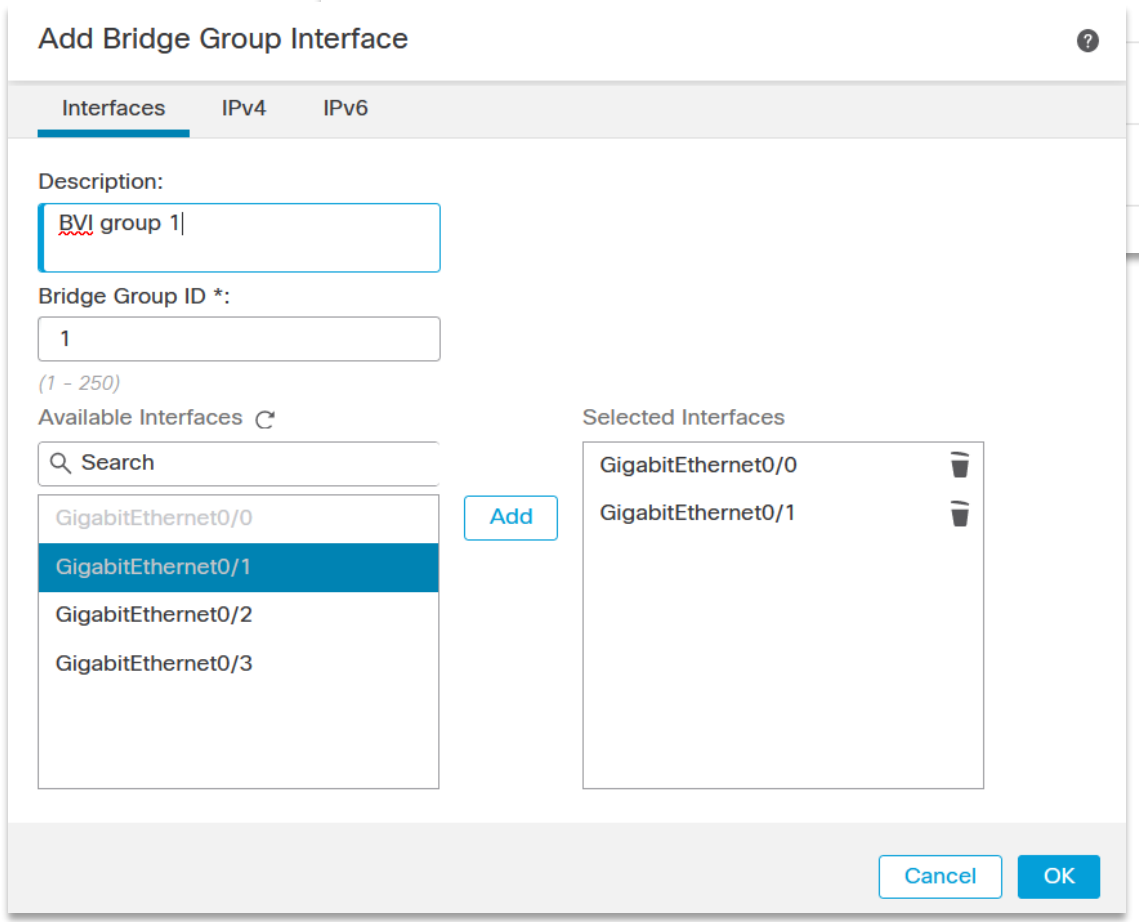
Configure BVI in Transparent mode

1) Before deploy previous configs , create a BVI interface
2) Click Add Interface
3) Click Bridge Group Interface
4) Enter a Group ID and description
5) Add physical interfaces to group
6) Click IPV4 tab to Enter an IPv4 address

- The IP address must be on the same subnet as the hosts and default gateway



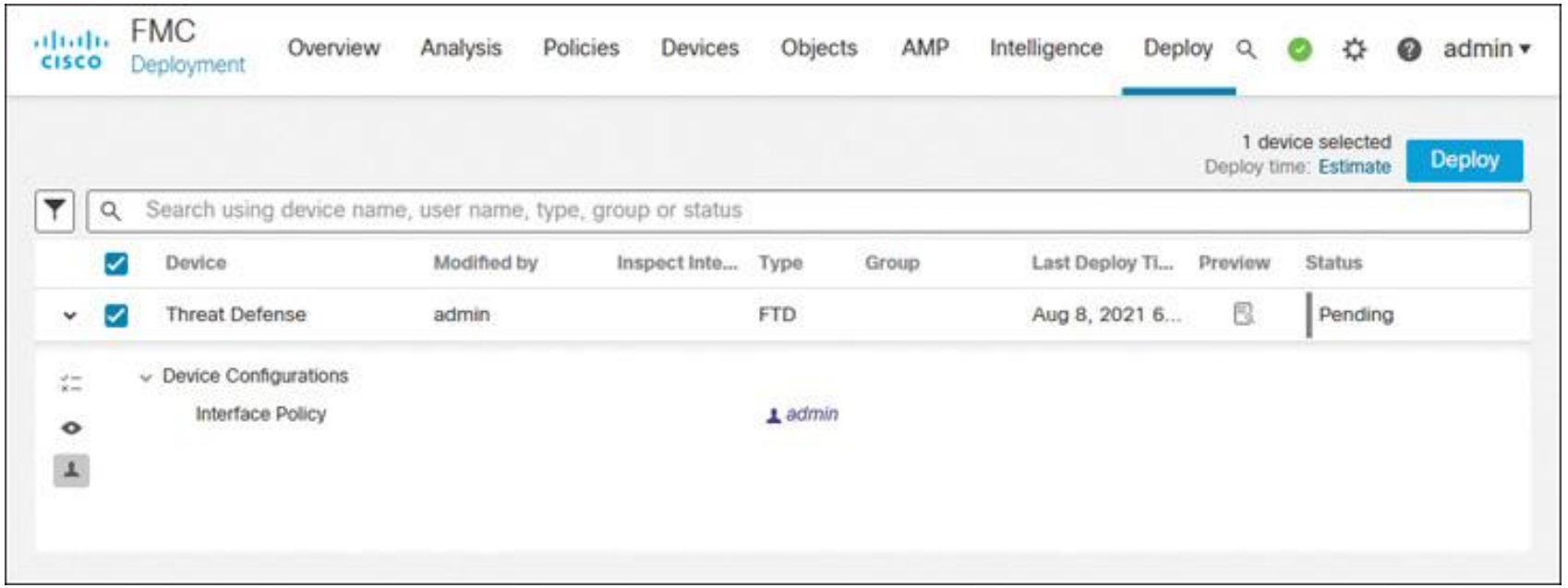




MohsenKheradmand MK

Configure BVI in Transparent mode

Now you can deploy interface setting to FTD



Verifying the Interface Status

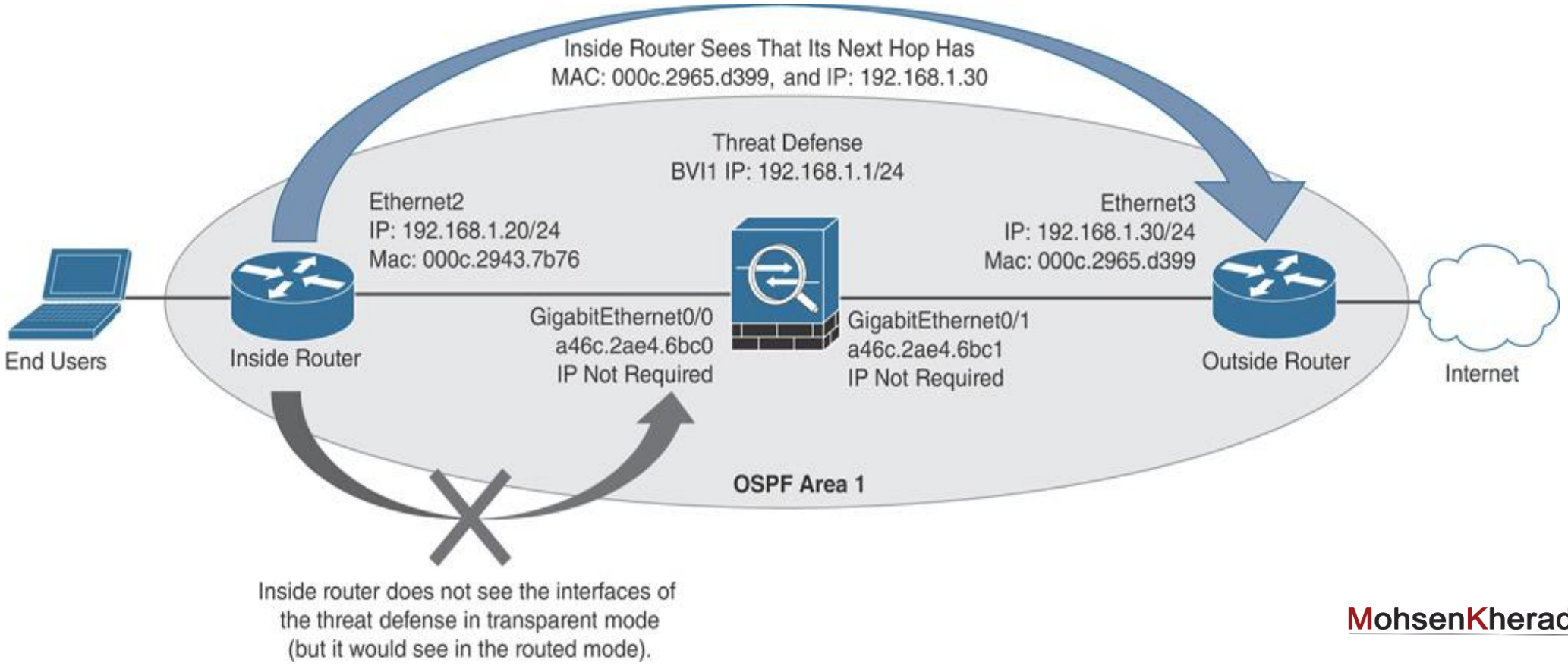
> show running-config interface

> show interface ip brief

Transparent mode

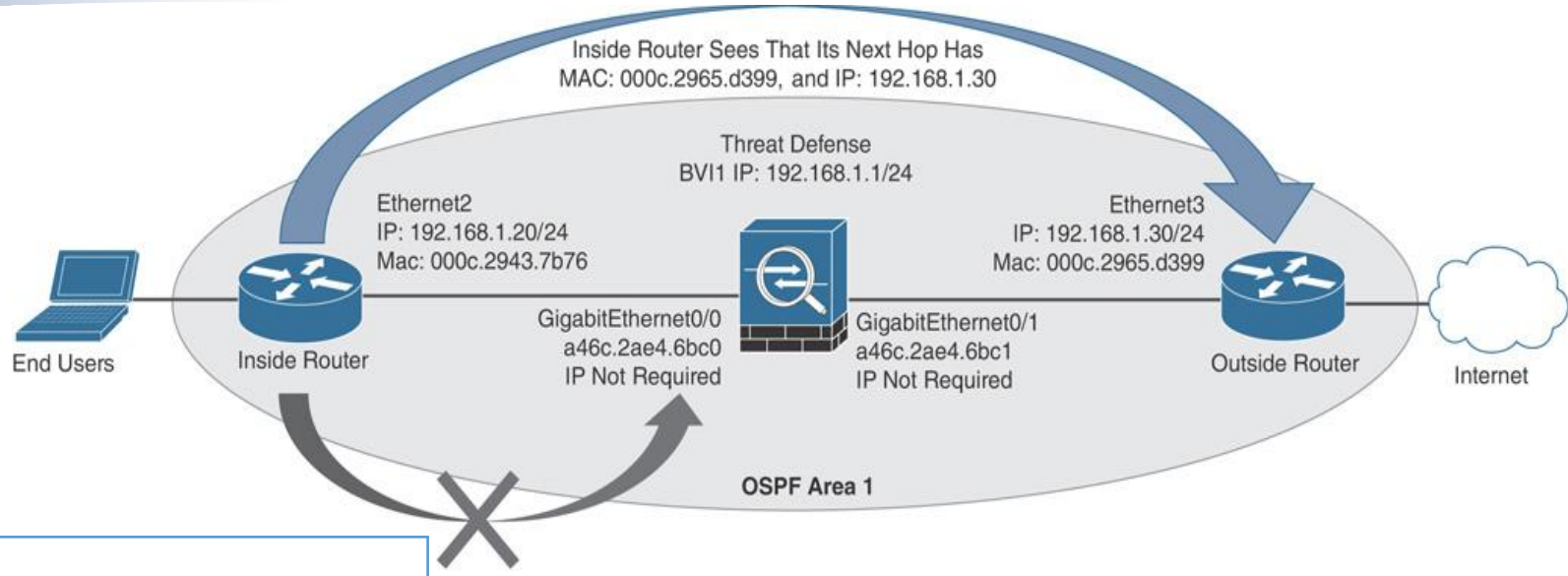
Verifying Basic Connectivity

- ✓ Through communication via FDT , Hosts can not see the FTD
- ✓ Instead, it sees the devices deployed on the other side of the FTD



Transparent mode

Verifying Basic Connectivity



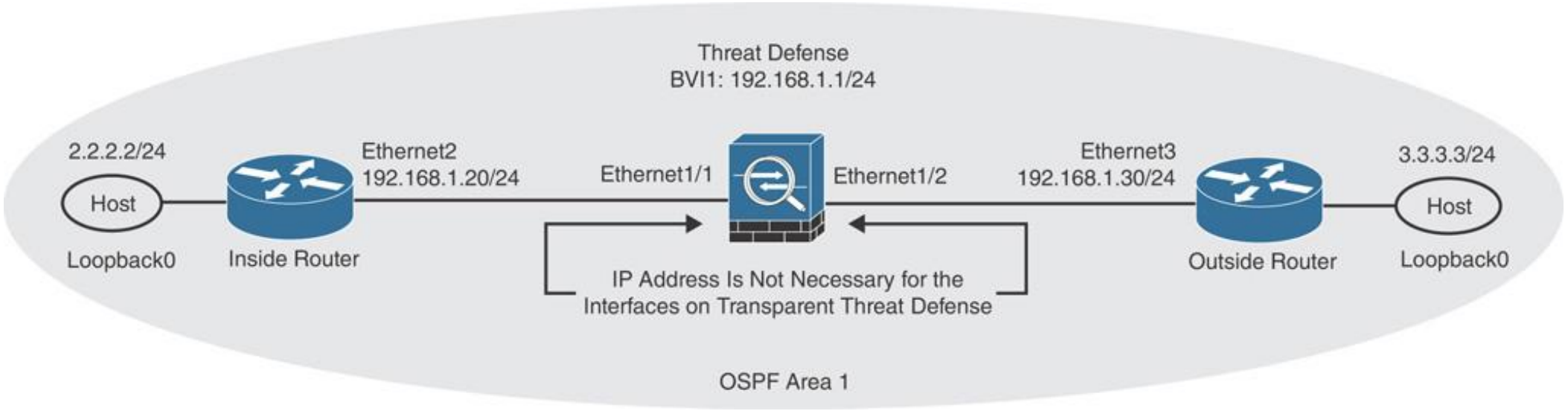

```
Inside-Router# ping 192.168.1.30
Sending 5, 100-byte ICMP Echos to 192.168.1.30, timeout is 2 seconds:
.!!!!
```

```
<debug icmp trace

ICMP echo request from INSIDE_INTERFACE:192.168.1.20 to OUTSIDE_INTERFACE:192.168.1.30 ID=8 seq=1 len=72
ICMP echo reply from OUTSIDE_INTERFACE:192.168.1.30 to INSIDE_INTERFACE:192.168.1.20 ID=8 seq=1 len=72
```

```
Inside-Router# show arp
  Protocol Address          Age (min)      Hardware Addr     Type      Interface
  Internet 192.168.1.20      -             000c.2943.7b76    ARPA      Ethernet2
  Internet 192.168.1.30      2             000c.2965.d399     ARPA     Ethernet2
```

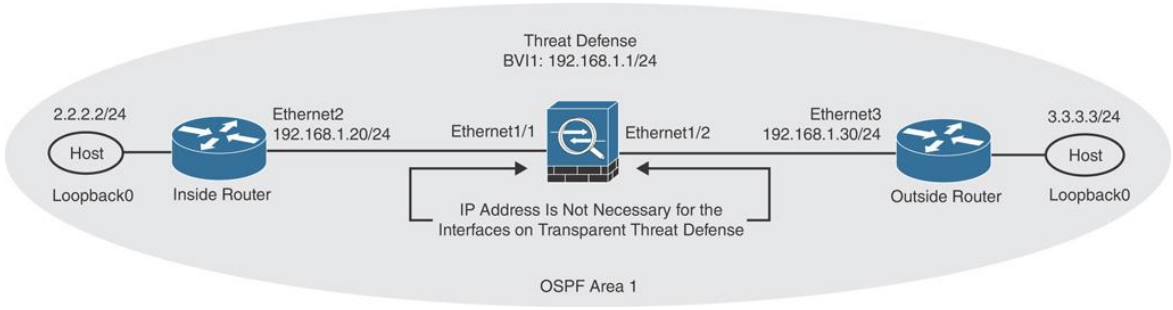
Deploying a Threat Defense Between Layer 3 Networks



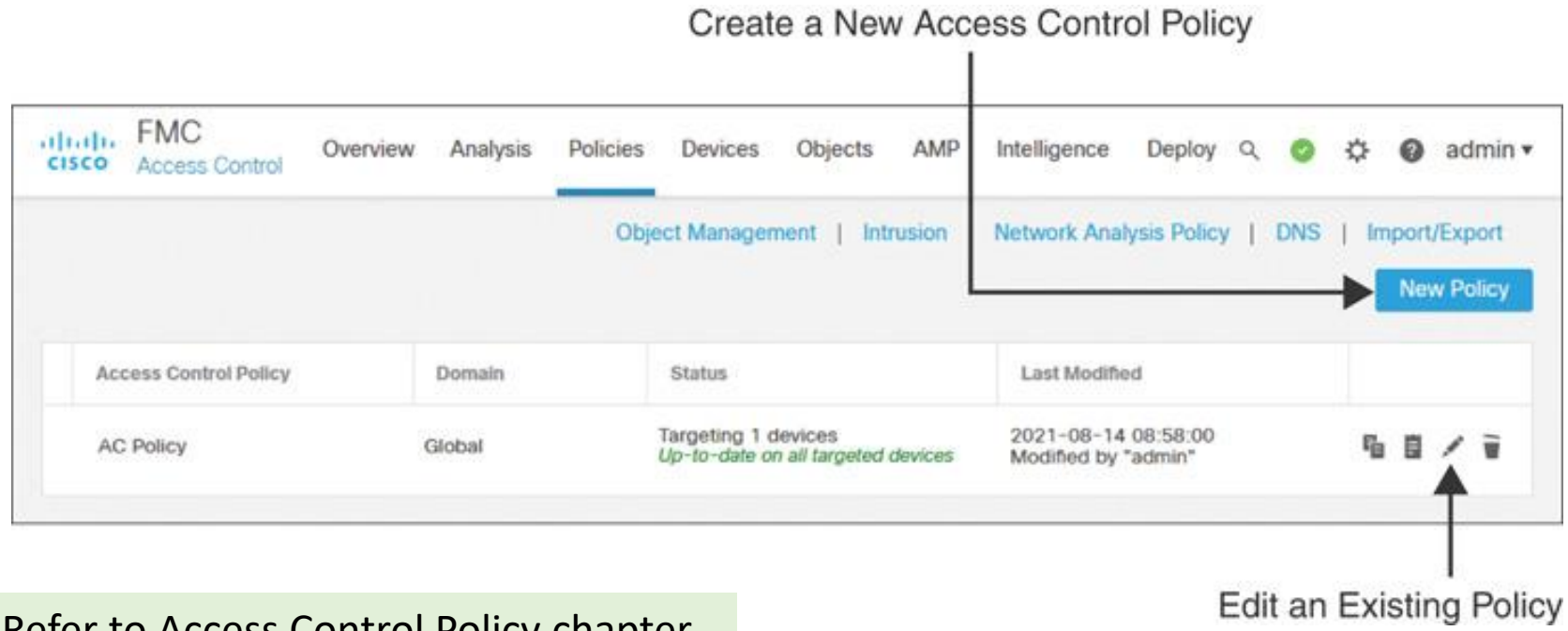
- Default action = how a threat defense handles traffic when no matching access control rule is available

- In transparent mode , the threat defense blocks the routing traffic until you allow it in an access control policy
- To allow routing traffic , you have 2 option:
  - Select a nonblocking policy as the default action (fewer steps to set up).
  - Add an access control rule to allow desired traffic (more steps to set up).

Deploying a Threat Defense Between Layer 3 Networks



You have to create new policy or edit default policy to allow routing protocols(or other) packets pass through



Refer to Access Control Policy chapter