

Securing Networks with
Cisco FTD

Chapter 4

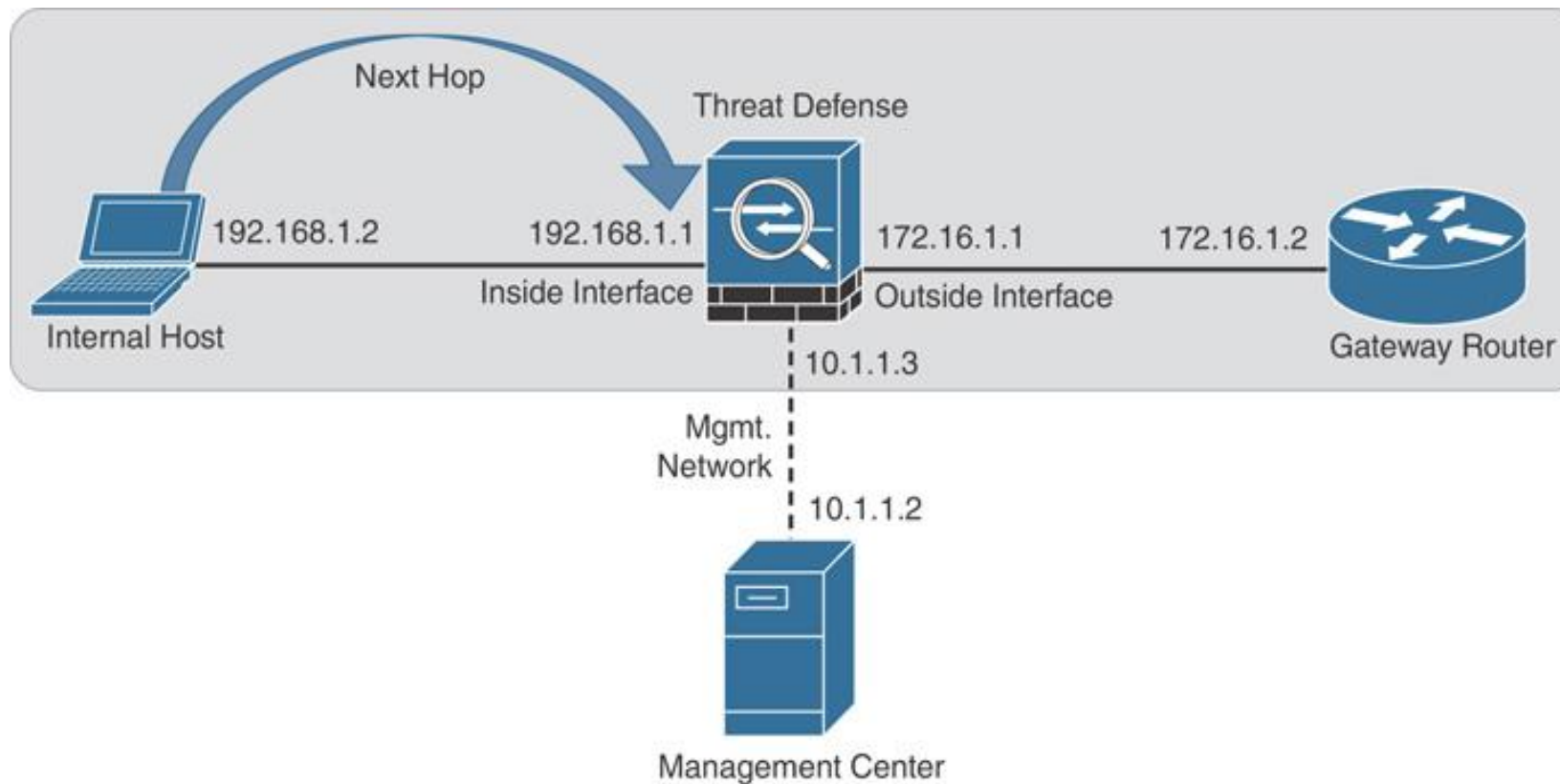
FTD Deployment Modes

Mohsen Kheradmand

Deployment in Routed Mode

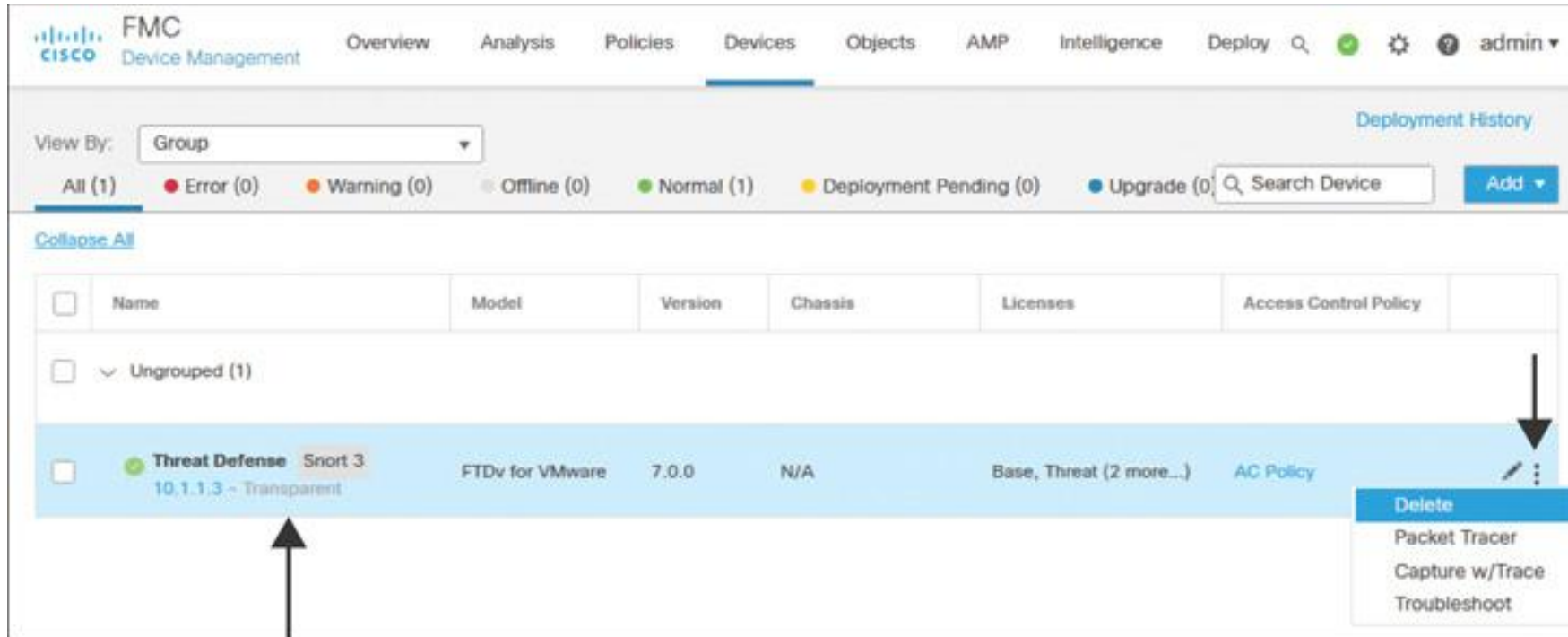
Routed mode

- 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



Transparent Mode

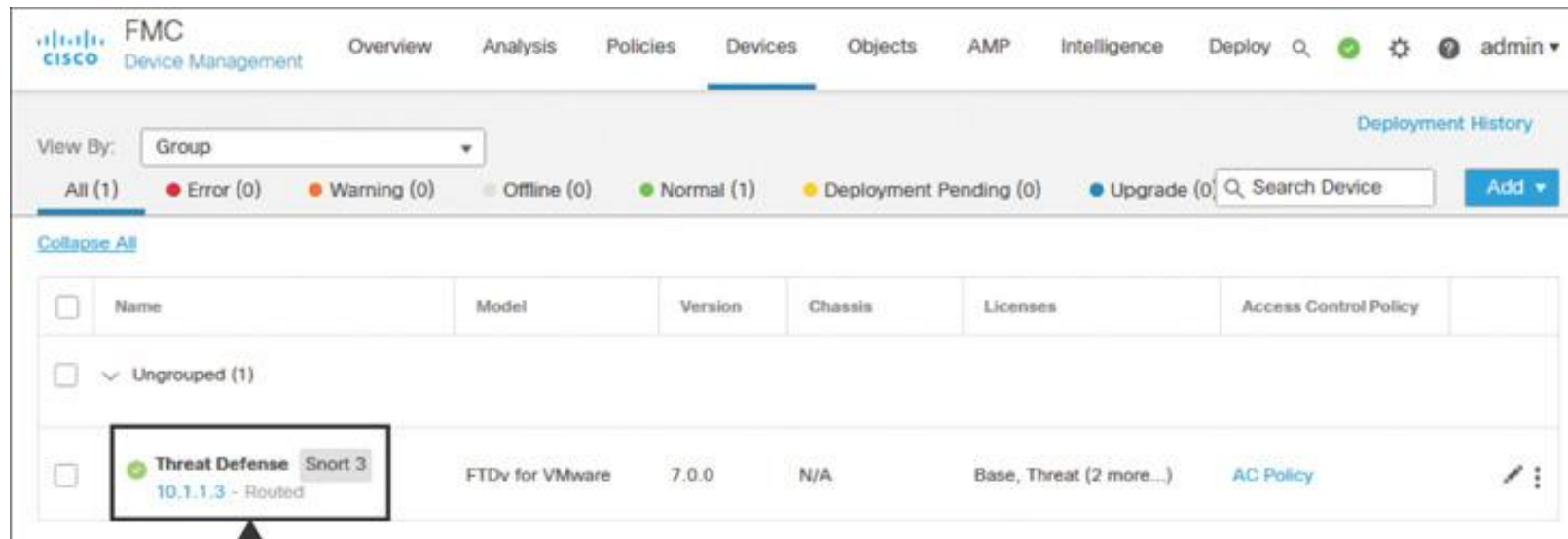
- ✓ Note : Changing the firewall mode wipes out any existing configurations on a threat defense.

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



Routed Mode

Configuration of the Routed Interface

- Click on FTD device or click pencil icon

View By:

Group

Dismiss all notifications

All (1)

Error (0)

Warning (0)

Offline (0)

Normal (1)

Deployment Pending (1)

Upgrade (0)

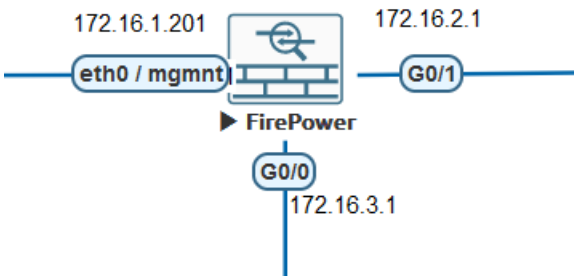
Search Device

Add

[Collapse All](#)

Configuration of the Routed Interface

- Click on FTD device or click pencil icon



FTD1

Cisco Firepower Threat Defense for KVM

Device

Routing

Interfaces

Inline Sets

DHCP

Save

Cancel

Search by name

Sync Device

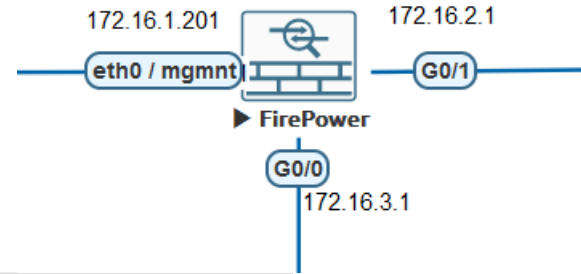
Add Interfaces

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



Edit Physical Interface

General

IPv4

IPv6

Advanced

Hardware Configuration

Name:

LAN-Side

☒ Enabled

☐ Management Only

Description:

connected to inside LAN

Mode:

None

Security Zone:

Inside-LAN

Interface ID:

GigabitEthernet0/0

MTU:

1500

(64 - 9000)

Propagate Security Group Tag:

☐

Cancel

OK

New Security Zone

Enter a name...

Inside-LAN

Cancel

OK

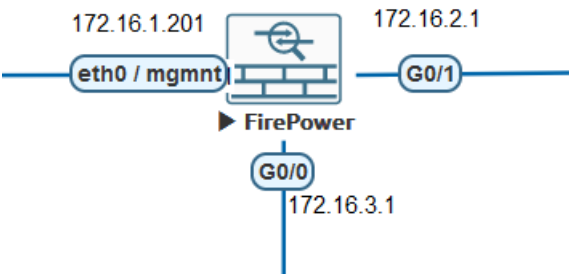
Configuration of the Routed Interface

IPv4 tab

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

IPv6 tab

- Enter IPv6 address and setting (in case)



Edit Physical Interface

GeneralIPv4IPv6AdvancedHardware Configuration

IP Type:

Use Static IP

IP Address:

192.168.3.1/24

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

Cancel

OK

Edit Physical Interface

GeneralIPv4IPv6AdvancedHardware Configuration

BasicAddressPrefixesSettings

+ Add Address

Address	EUI64	
2001:ABCD:1234::/96	false	 

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

Edit Physical Interface

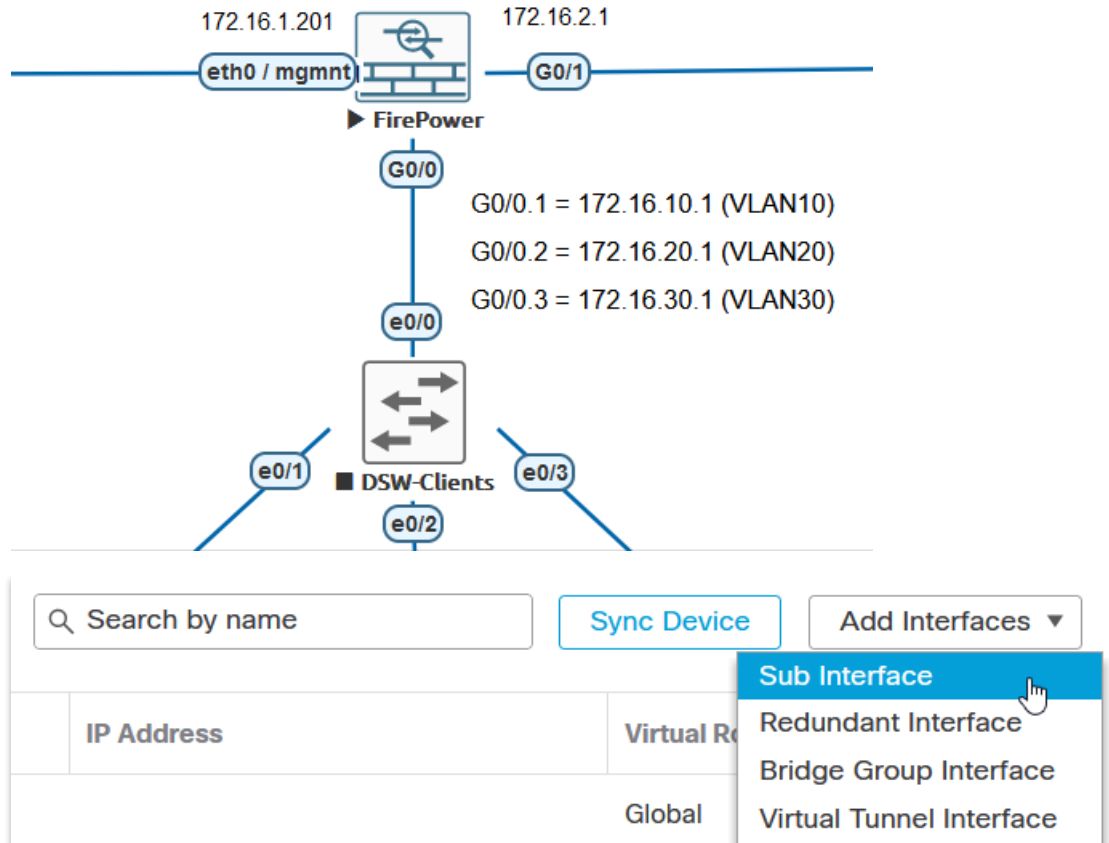
General	IPv4	IPv6	Advanced	Hardware Configuration
Information				
Active Mac Address: 				
Standby Mac Address: 				

Edit Physical Interface

General	IPv4	IPv6	Advanced	Hardware Configuration
Duplex: auto				
Speed: auto				

Configuration of the Routed Interface

➤ Create sub interface



Add Sub Interface

General IPv4 IPv6 Advanced

Name:

Sale

☒ Enabled

☐ Management Only

Description:

Gateway of Sale VLAN

Security Zone:

Clients

MTU:

1500

(64 - 9000)

Propagate Security Group Tag: ☒

Interface *:

GigabitEthernet0/0

Sub-Interface ID *:

1

(1 - 4294967295)

VLAN ID:

10

(1 - 4094)

Cancel

OK

Configuration of the Routed Interface

➤ Create sub interface

Add Sub Interface

GeneralIPv4IPv6Advanced

IP Type:

Use Static IP

IP Address:

192.168.10.1/24

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

Cancel

OK

FTD Interface Setting via FDM

Device Summary
Interfaces

Cisco Firepower Threat Defense for VMware ⓘ

0/0 0/1 0/2 0/3 0/4 0/5 0/6 0/7 MGMT CONSOLE

Interfaces Virtual Tunnel Interfaces

9 Interfaces

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
> ✓ GigabitEthernet0/0	outside	☒	Routed	192.168.20.1 Static		Enabled	
> ✓ GigabitEthernet0/1	inside	☒	Routed	192.168.45.1 Static		Enabled	
> ○ GigabitEthernet0/2		☐	Routed			Enabled	
> ○ GigabitEthernet0/3		☐	Routed			Enabled	
> ○ GigabitEthernet0/4		☐	Routed			Enabled	
> ○ GigabitEthernet0/5		☐	Routed			Enabled	
> ○ GigabitEthernet0/6		☐	Routed			Enabled	
> ○ GigabitEthernet0/7		☐	Routed			Enabled	
> ✓ Management0/0	diagnostic	☒	Routed			Enabled	

FTD Interface Setting via FDM

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

GigabitEthernet0/2

Edit Physical Interface

Interface Name

DMZ-SRVs

Mode

Routed

Status

☒

Most features work with named interfaces only, although some require unnamed interfaces.

Description

Gateway of the DMZ servers

IPv4 Address

IPv6 Address

Advanced

Type

Static

IP Address and Subnet Mask

172.16.30.1 / 24

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask

/

e.g. 192.168.5.16

CANCEL

OK

Enable DHCP server on interface

Device

Routing

Interfaces

Inline Sets

DHCP

DHCP Server

DHCP Relay

DDNS

Ping Timeout

50

(10 - 10000 ms)

Lease Length

3600

(300 - 10,48,575 sec)

☐ Auto-Configuration

Interface

Override Auto Configured Settings:

Domain Name

Dena.local

Primary DNS Server

DNS1

+

Secondary DNS Server

+

Primary WINS Server

+

Secondary WINS Server

+

Server

Advanced

Interface	Address Pool	Enable DHCP Server	
			+ Add

New Network Object

Name

DNS1

Description

DNS server 1

Network

☒ Host

☐ Range

☐ Network

☐ FQDN

192.168.10.10

☐ Allow Overrides

Cancel

Save

Enable DHCP server on interface

DeviceRoutingInterfacesInline SetsDHCP

DHCP ServerDHCP RelayDDNS

Ping Timeout50(10 - 10000 ms)

Lease Length3600(300 - 10,48,575 sec)

☐ Auto-Configuration

Interface

Override Auto Configured Settings:

Domain NameDena.local

Primary DNS ServerDNS1+Primary WINS Server+Secondary DNS Server+Secondary WINS Server+

ServerAdvanced

Interface	Address Pool	Enable DHCP Server
-----------	--------------	--------------------

Add Server?

Interface*LAN-inside

Address Pool*172.16.3.10-172.16.3.50(2.2.2.10-2.2.2.20)

☒ Enable DHCP Server

Cancel

OK

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
```

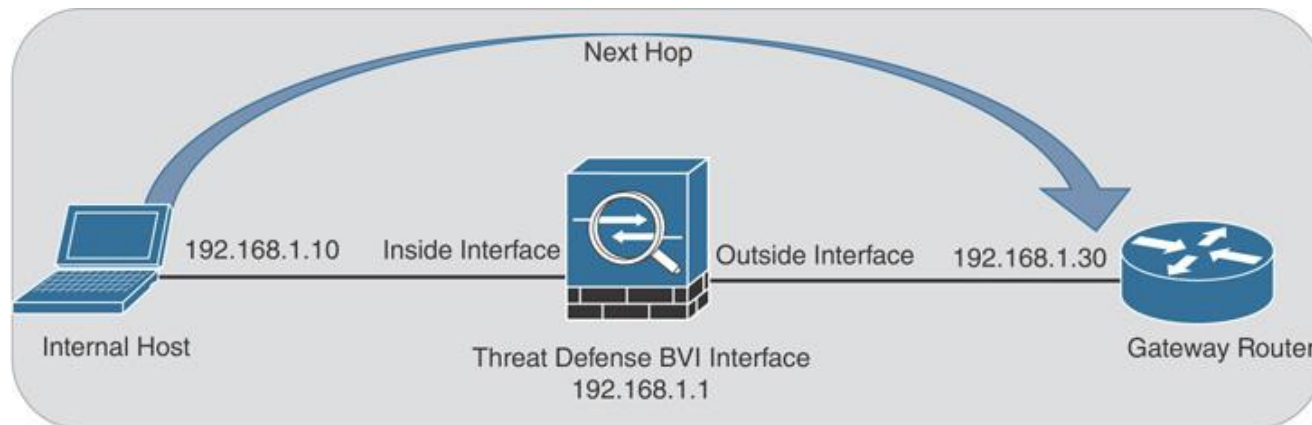
IP Address Assignment from a DHCP Address Pool

```
> show dhcpd binding  
> debug dhcpd packet
```

Deployment in Transparent Mode

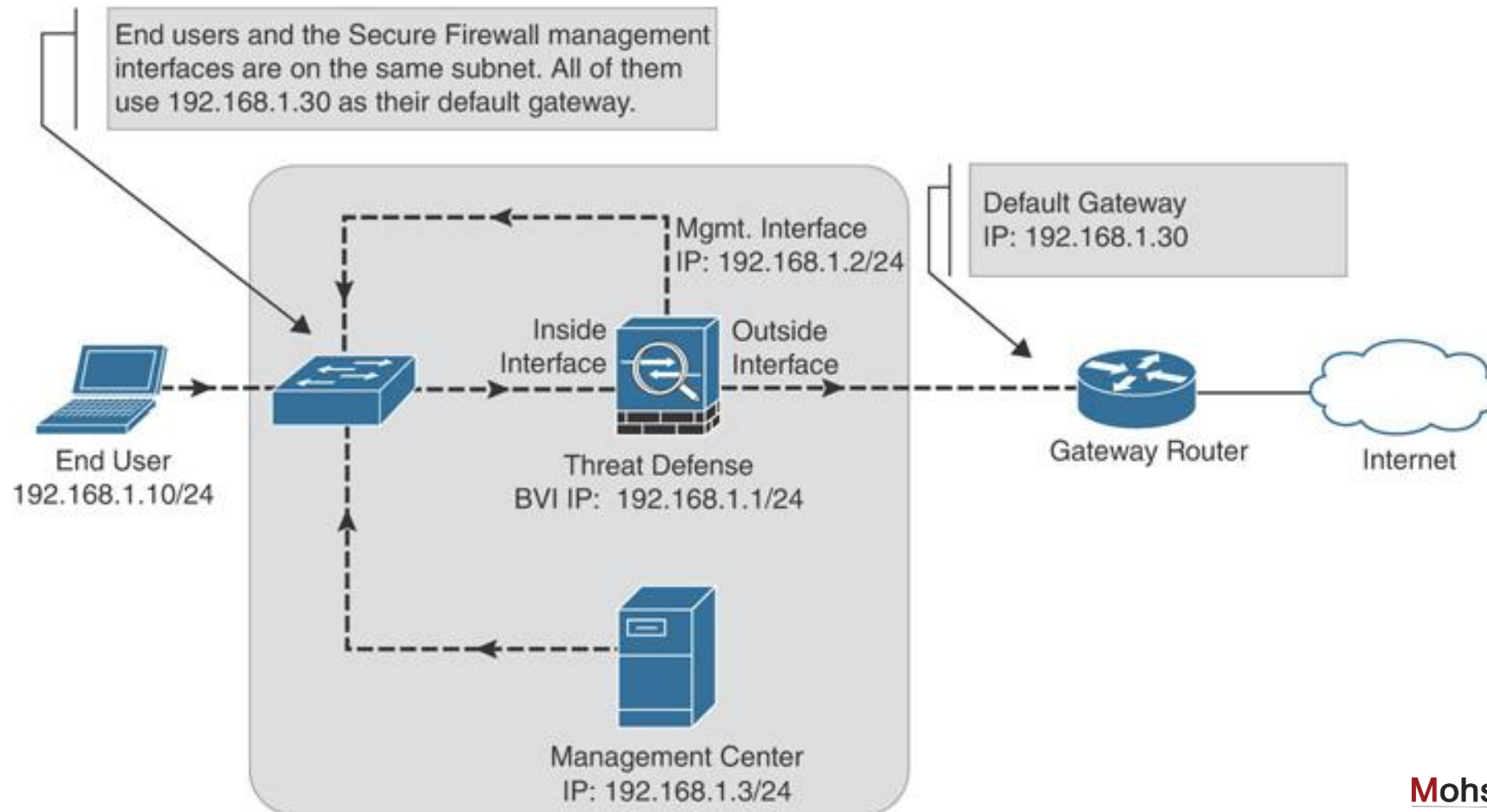
Transparent mode

- 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.

Threat Defense 1010

Cisco Firepower 1010 Threat Defense

Device Routing **Interfaces** Inline Sets DHCP SNMP

Search by name Sync Device Add Interfaces

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Port Mode	VLAN Usage	SwitchPort
Diagnostic1/1	diagnostic	Physical						
Ethernet1/1		Physical						☐
Ethernet1/2		Physical						☐
Ethernet1/3		Physical				Access	1	☒
Ethernet1/4		Physical				Access	1	☒
Ethernet1/5		Physical				Access	1	☒
Ethernet1/6		Physical				Access	1	☒
Ethernet1/7		Physical				Access	1	☒
Ethernet1/8		Physical				Access	1	☒

Displaying 1-9 of 9 interfaces |< < Page 1 of 1 > >|

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

FDT1

Cisco Firepower Threat Defense for KVM

DeviceRoutingInterfacesInline SetsDHCP

General

Name:

FDT1

Transfer Packets:

Yes

Mode:

Transparent

Compliance Mode:

None

Save

Cancel

FDT1

Cisco Firepower Threat Defense for KVM

DeviceRoutingInterfacesInline SetsDHCP

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		Physical				
GigabitEthernet0/1		Physical				
GigabitEthernet0/2		Physical				
GigabitEthernet0/3		Physical				

Configure interface in Transparent mode

Enter a name for interface

Click Enabled

Description : (optional)

Mode : None / passive

Security zone : (optional)

Edit Physical Interface

General IPv6 Advanced Hardware Configuration

Name:

☒ Enabled
☐ Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:

(64 - 9000)

Propagate Security Group Tag: ☐

Cancel OK

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

Add Bridge Group Interface

Interfaces IPv4 IPv6

IP Type:
Use Static IP

IP Address:
172.16.10.10/24
eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

Search by name Sync Device Add Interfaces

Sub Interface
Redundant Interface
Bridge Group Interface

Add Bridge Group Interface

Interfaces IPv4 IPv6

Description:
BVI group 1

Bridge Group ID *:
1
(1 - 250)

Available Interfaces

GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/2
GigabitEthernet0/3

Add

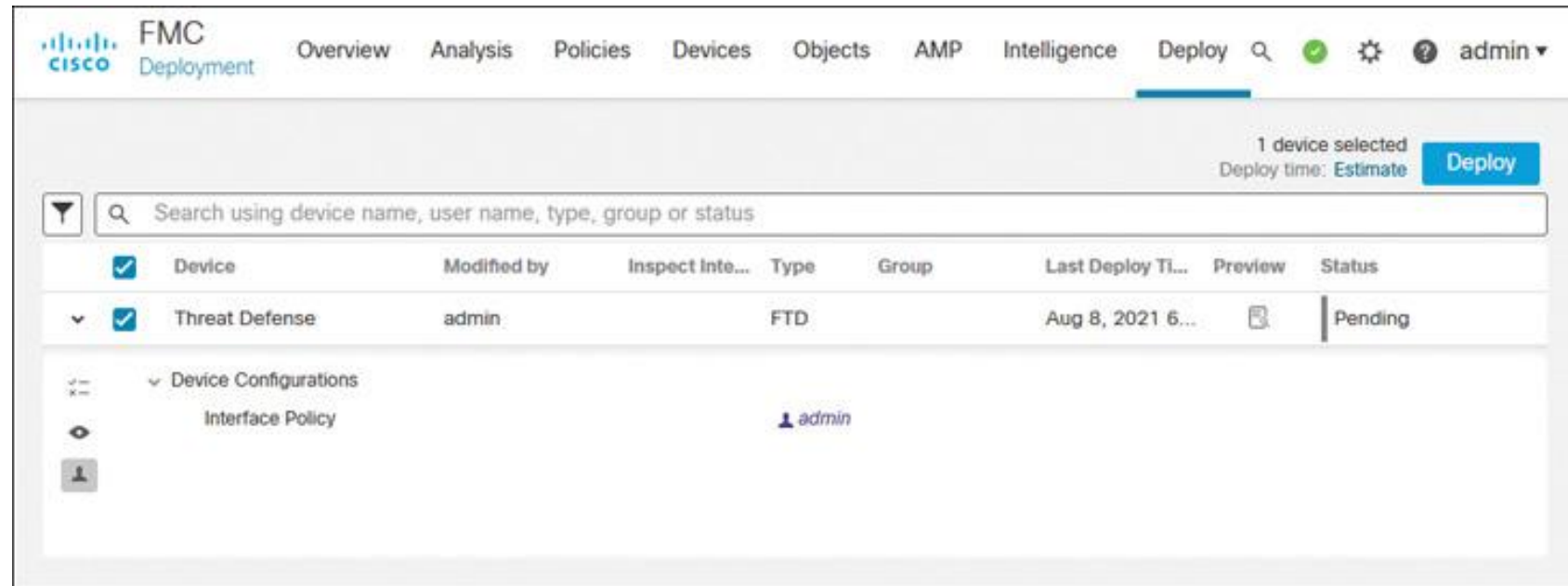
Selected Interfaces

GigabitEthernet0/0
GigabitEthernet0/1

Cancel OK

Configure BVI in Transparent mode

Now you can deploy interface setting to FTD



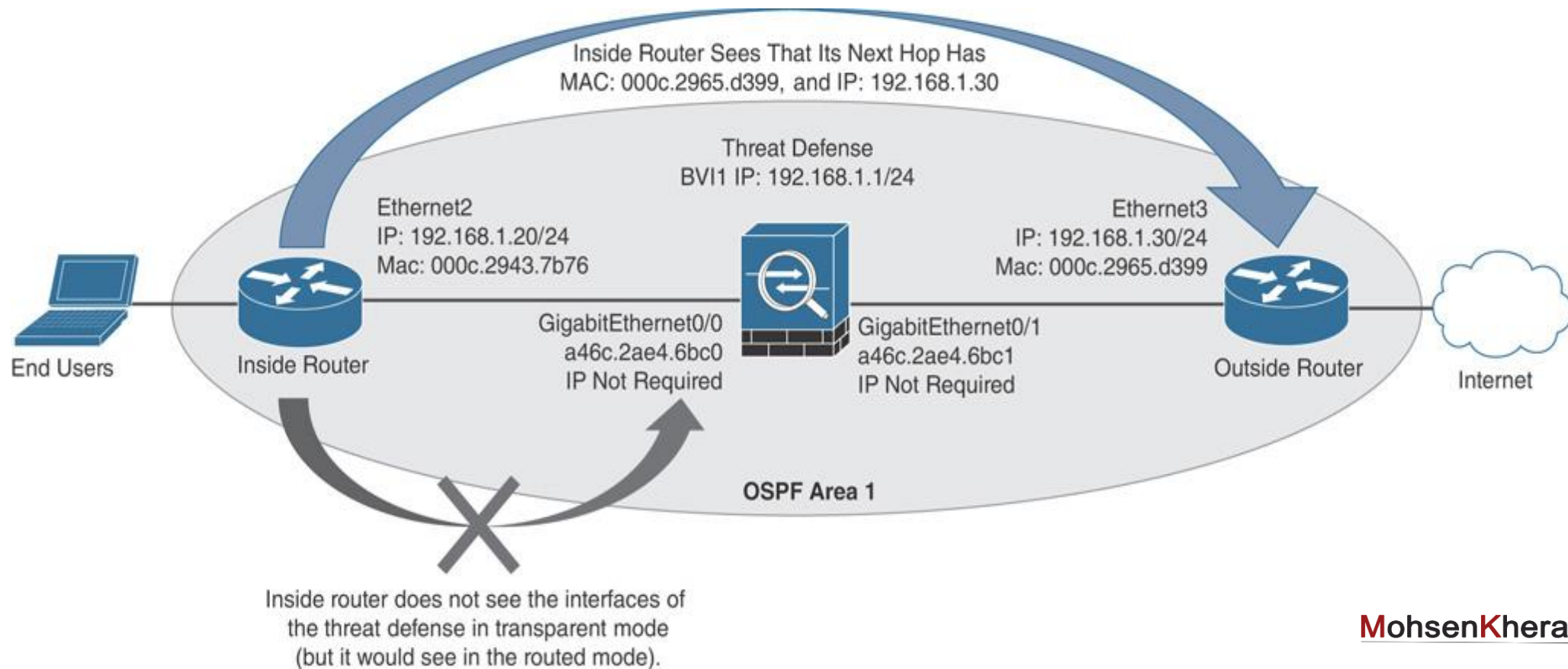
Verifying the Interface Status

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

Transparent mode

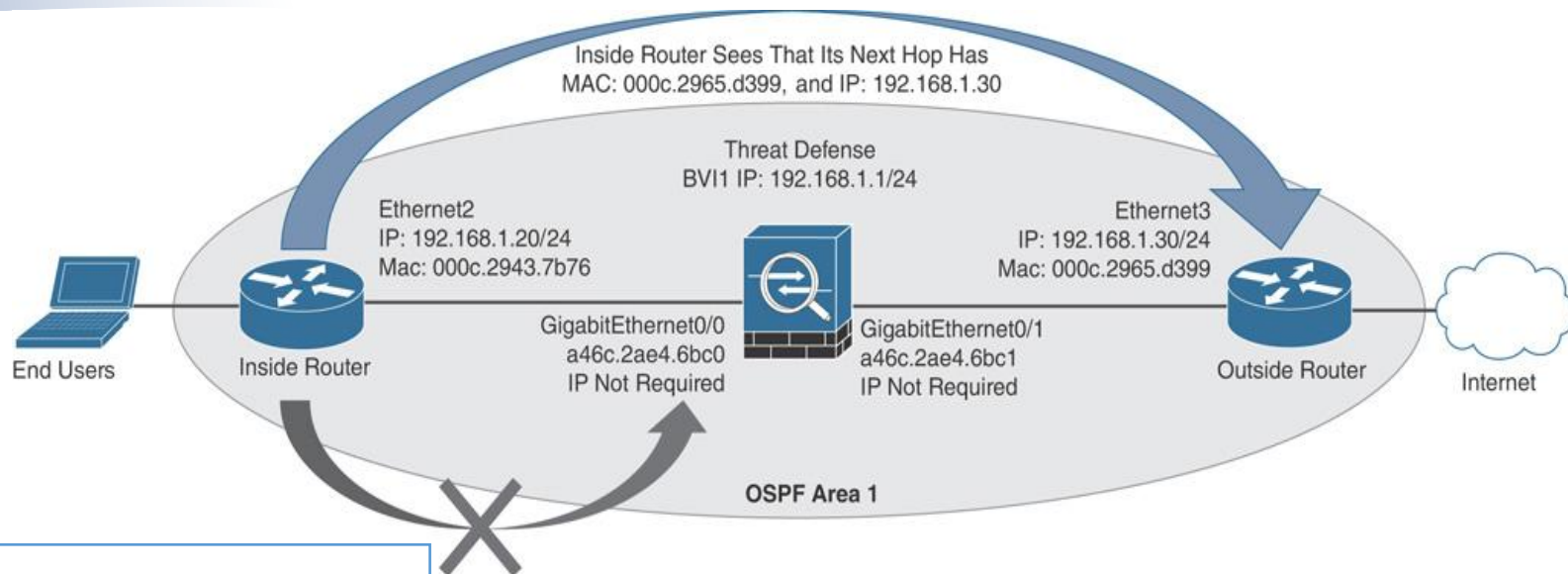
Verifying Basic Connectivity

- ✓ 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

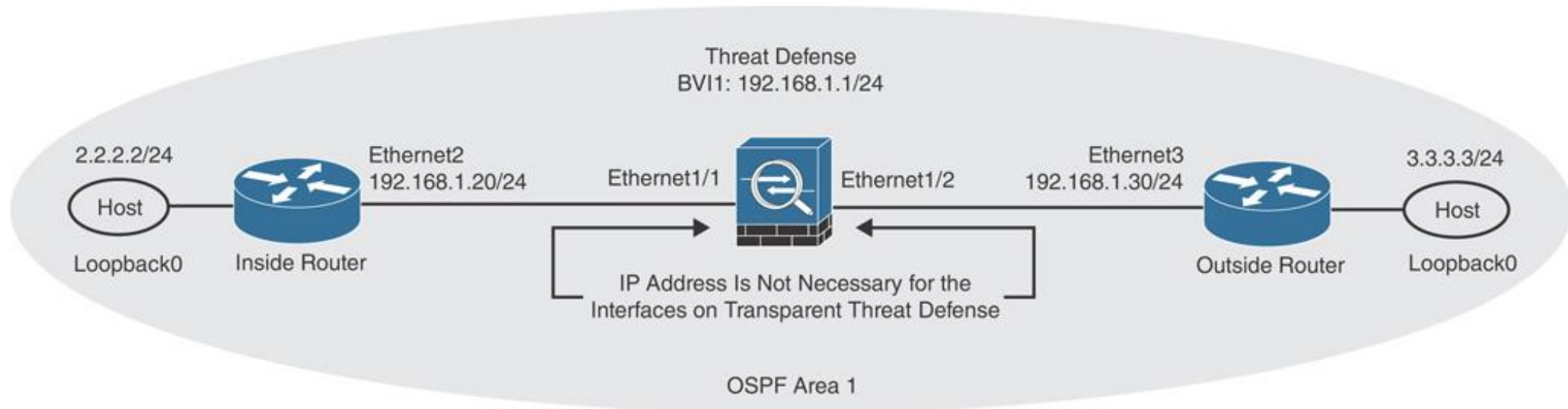
ICMP echo request from INSIDE_INTERFACE:192.168.1.20 to OUTSIDE_INTERFACE:192.168.1.30 ID=8 seq=1 len=72

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
```

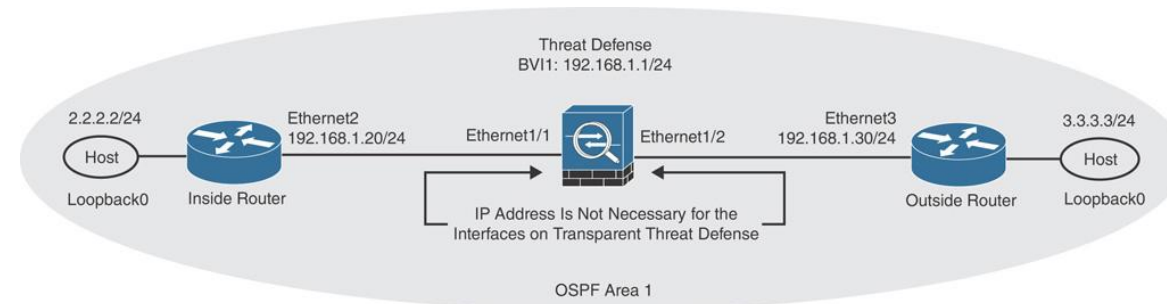
Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.1.20	-	000c.2943.7b76	ARPA	Ethernet2
Internet	192.168.1.30	2	000c.2965.d399	ARPA	Ethernet2

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

Create a New Access Control Policy

The screenshot shows the Cisco FMC Access Control interface. The 'Policies' tab is selected. A 'New Policy' button is visible. Below the button is a table of existing policies.

Access Control Policy	Domain	Status	Last Modified
AC Policy	Global	Targeting 1 devices Up-to-date on all targeted devices	2021-08-14 08:58:00 Modified by "admin"

Refer to Access Control Policy chapter

Edit an Existing Policy