Securing Networks with

Cisco FTD

Chapter 5

FTD Interface Modes

Mohsen Kheradmand

interface modes

In FTD you can choose any interface mode , regardless of the deployment mode (routed or transparent)

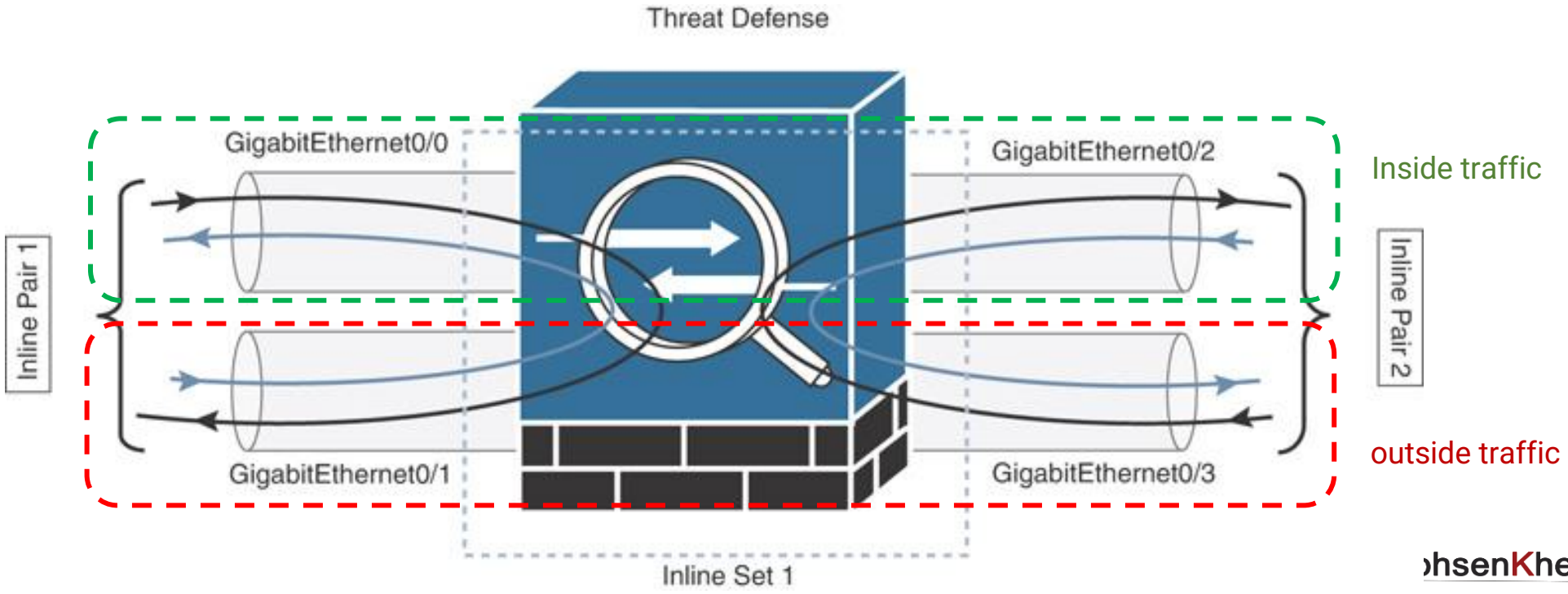
Interface modes :

Interface mode	Deployment mode	Action to traffic
Inline mode	Routed or Transparent	Prevention
Inline -tap	Routed or Transparent	Detection
Passive (SPAN)	Routed or Transparent	Detection
Passive (ERSPAN)	Routed	Detection

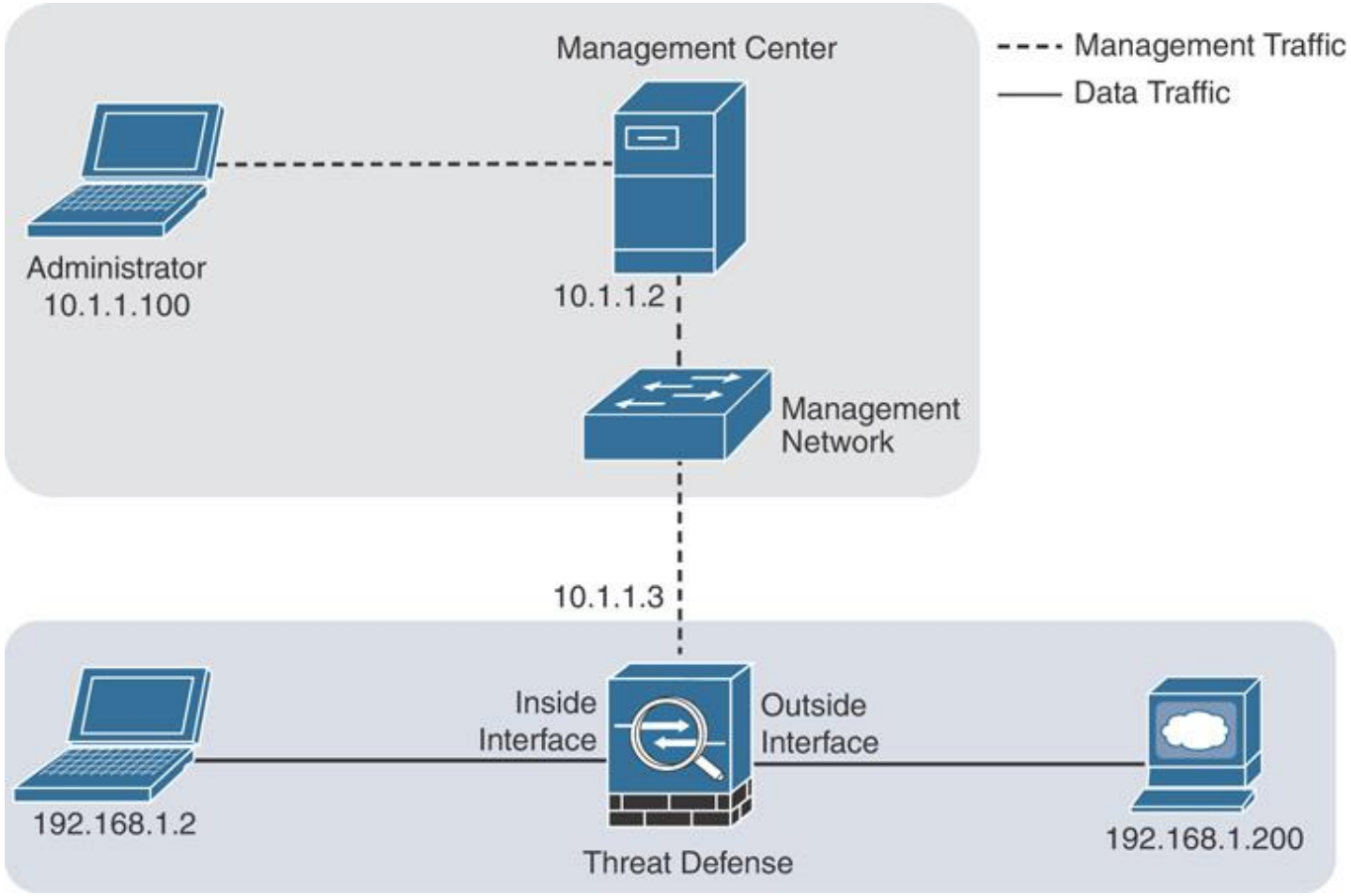
Inline mode (IPS)

- INLINE mode (IPS mode) : prevent any potential intrusion attempt in real time

- In inline mode, the ingress and egress interfaces are bundled into an **interface pair**
- Each pair must be associated with an **inline set** (a logical group of one or more interface pair)



Inline set configuration

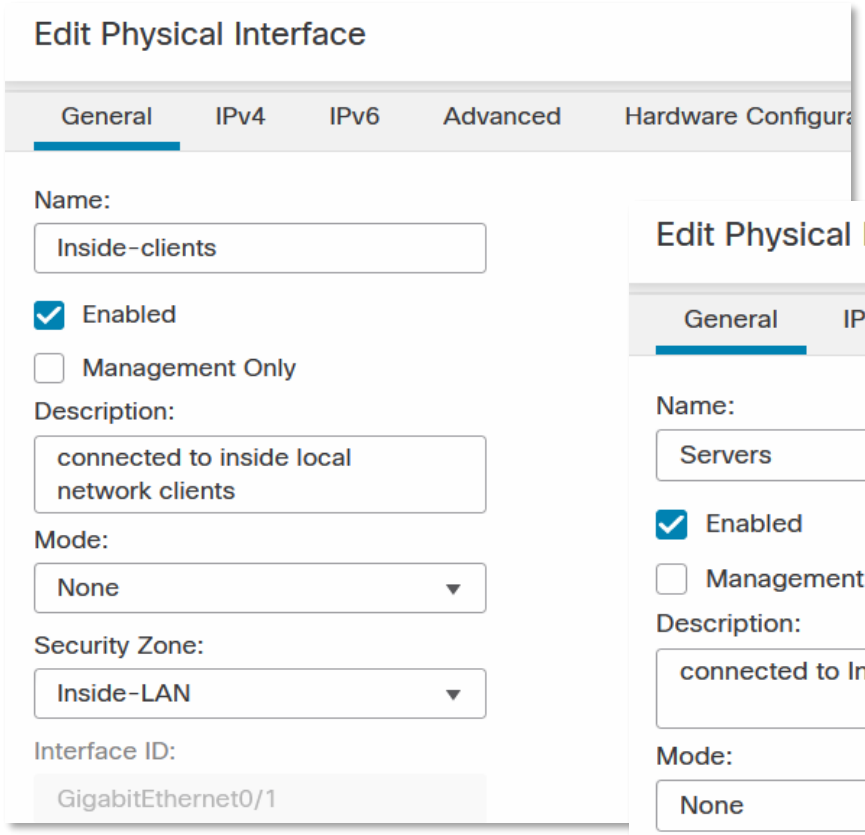


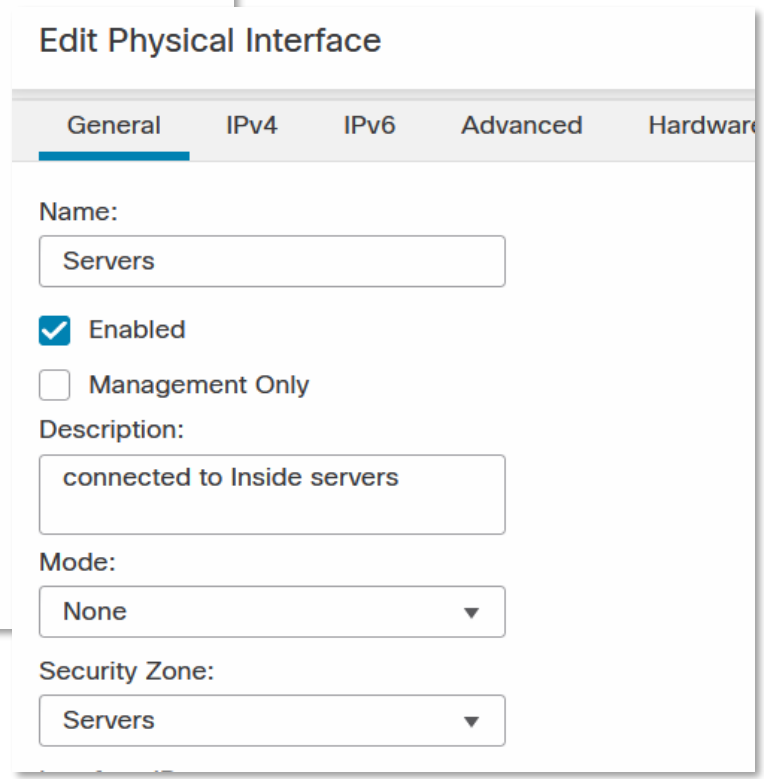
Inline set configuration

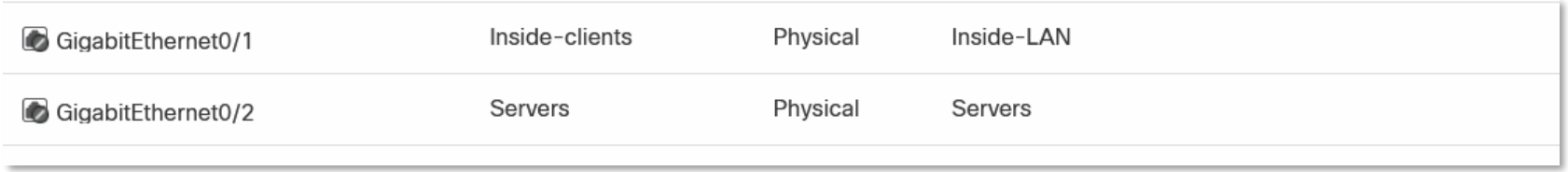
1) Device / select FTD
2) Click Edit interface
3) Enter name and select Enabled
4) Select None mode (inline mode)

✓ IP address / security zone is not necessary

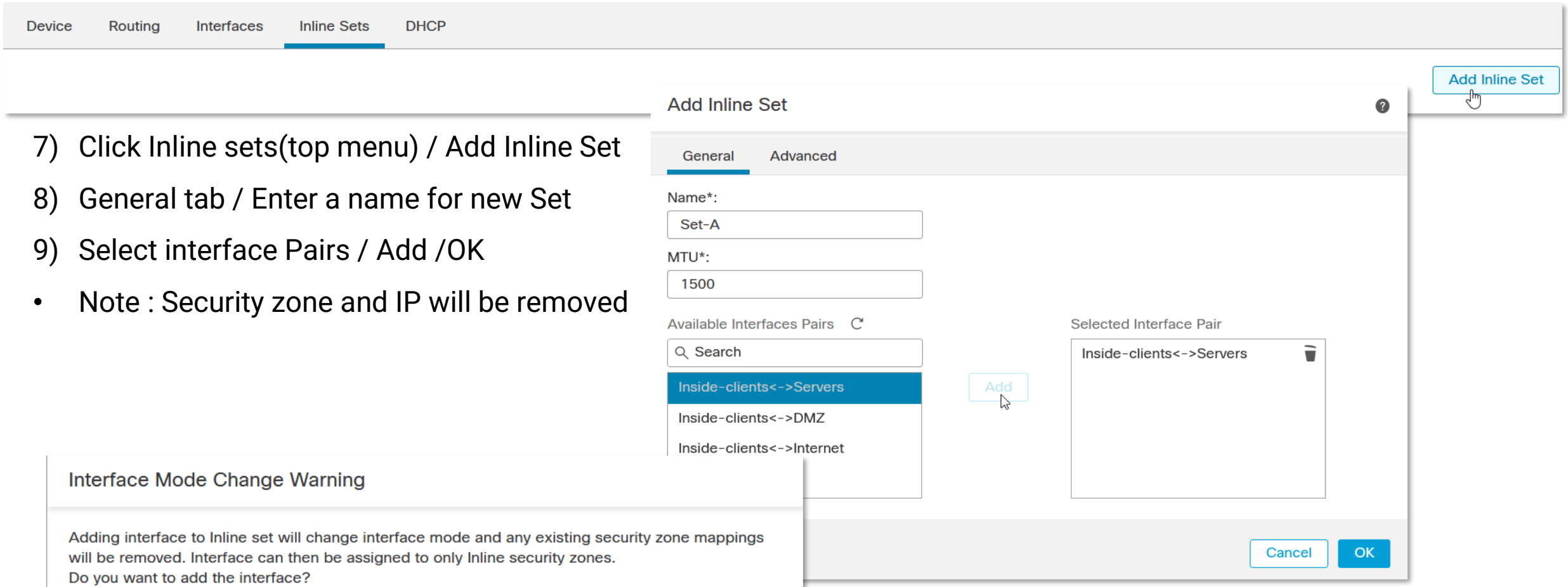
5) Repeat the same for other interfaces
6) Click save







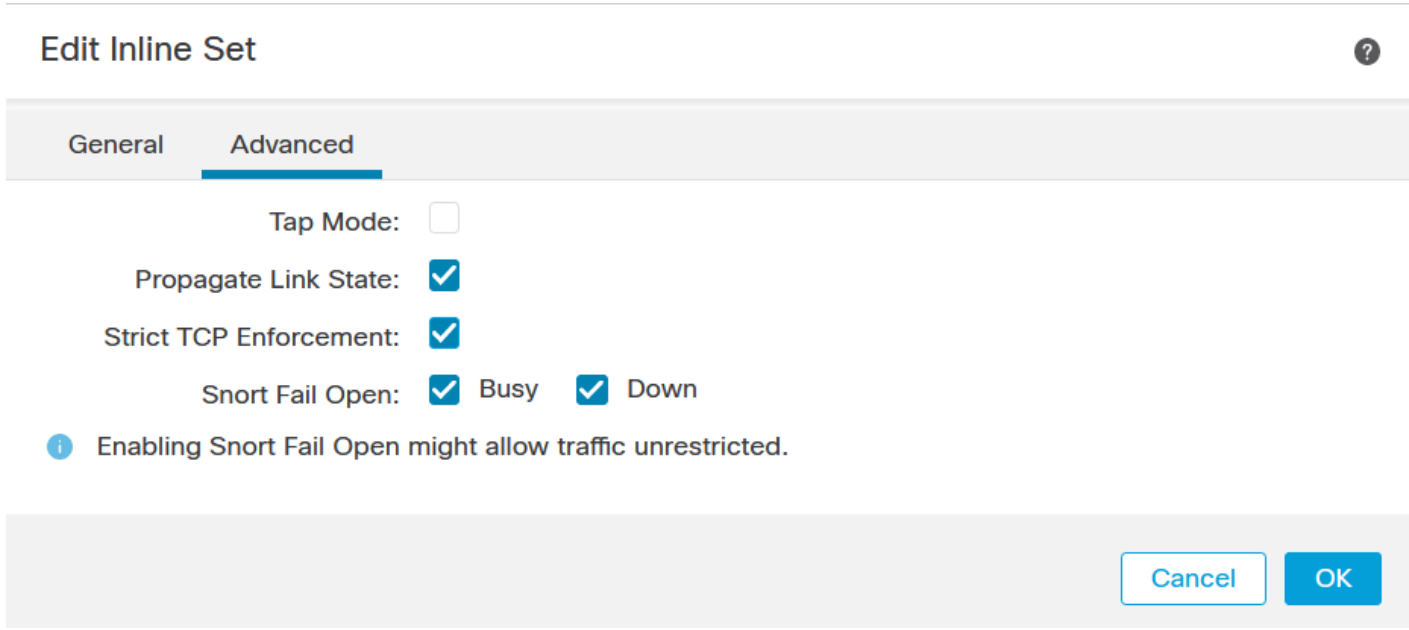
Inline set configuration



7) Click Inline sets(top menu) / Add Inline Set
8) General tab / Enter a name for new Set
9) Select interface Pairs / Add /OK

- Note : Security zone and IP will be removed

Inline set configuration

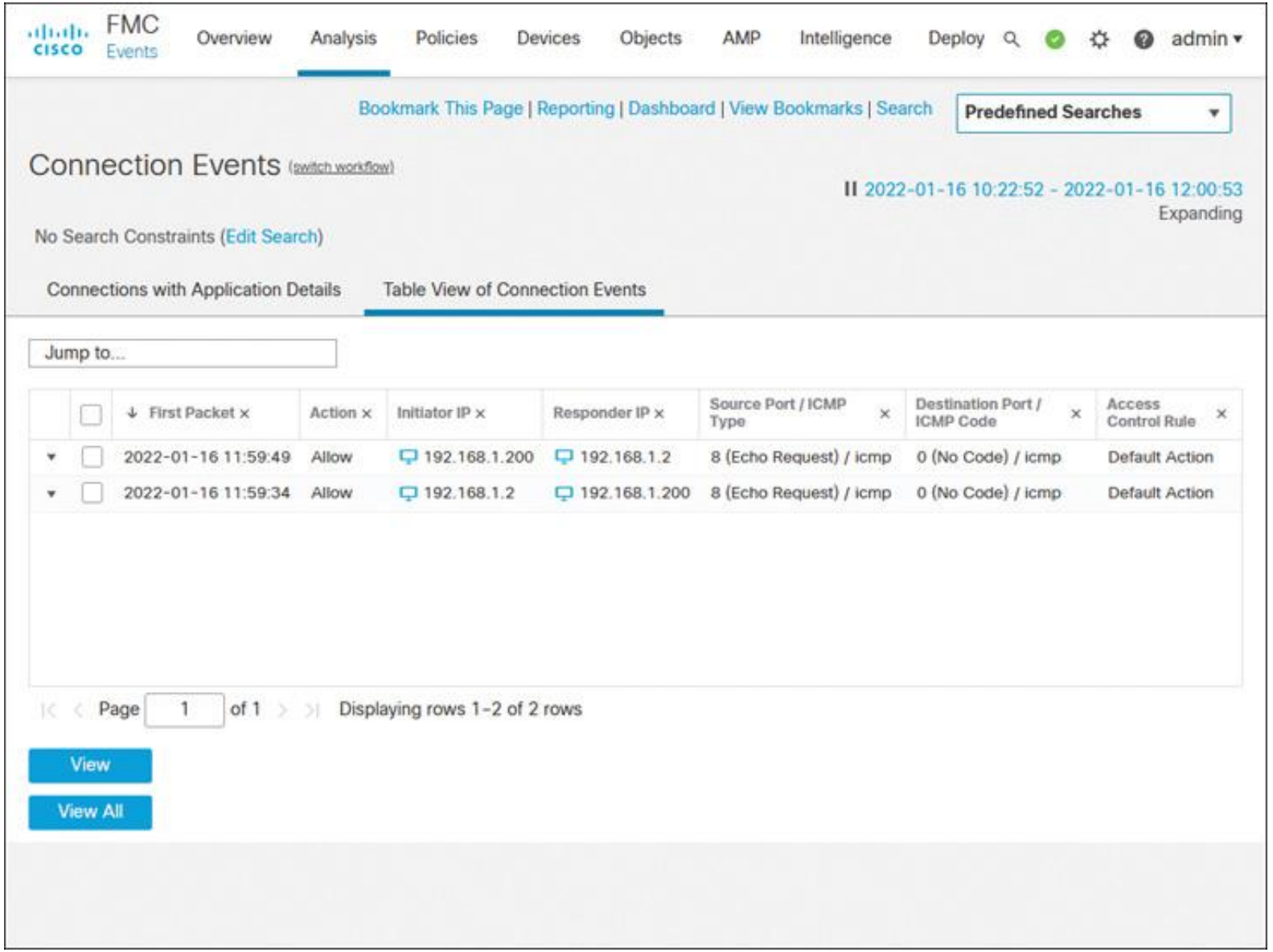


- Tap Mode : monitors the traffic without taking action if something malicious is found (IDS mode – Directly connected)
- Propagate Line state : automatically brings the remaining interface down if one of the interfaces in an inline pair goes down(reduces the routing convergence time)
- Strict TCP Enforcement : blocks connections where the three-way handshake was not completed.
- Snort Fail Opens : In case of an inspection failure , FTD allow traffic pass through without inspection
  - Busy : when the interface buffer is full and drops traffic
  - Down : when the Snort goes down due to a restart

Verification

Table view of connection events.

The events confirm that hosts 192.168.1.2 and 192.168.1.200 are able to communicate through the FTD



Verification

> show interface GigabitEthernet 0/0

```
Interface GigabitEthernet0/0
"INSIDE_CLIENTS", is up, line protocol is up
  Hardware is net_vmxnet3, BW 10000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(10000 Mbps)

        Input flow control is unsupported, output flow contrBX1_CODE_MIDol
is unsupported

        MAC address 000c.2916.38a3, MTU 1500

        IPS Interface-Mode: inline, Inline-Set: SET-A
```

Verification

> show inline-set

```
Inline-set SET-A
Mtu is 1500 bytes
  Fail-open for snort down is on
  Fail-open for snort busy is on
  Tap mode is off
  Propagate-link-state option is on
  hardware-bypass mode is disabled
  Interface-Pair[1]:
Interface: GigabitEthernet0/1
"INSIDE_CLIENTS"
      Current-Status: UP
    Interface: GigabitEthernet0/2
“SERVERS"
      Current-Status: UP
```

Best Practices for Inline Mode

- When the inbound and outbound traffic go through two different interface pairs, you should include both interface pairs in the same interface set. (ensures that the FTD does not see just half of the traffic)
- If FTD is connected to switches , you should enable portfast on the associated switch port (fast convergence)
- It’s better enable the fail open features (continue moving traffic)

- Unsupported Firewall Features on IPS Interfaces
  - ✓ DHCP server
  - ✓ DHCP relay
  - ✓ DHCP client
  - ✓ TCP Intercept
  - ✓ Routing
  - ✓ NAT
  - ✓ VPN
  - ✓ QoS
  - ✓ NetFlow
  - ✓ VXLAN
  - ✓ Application inspection

Inline Mode Versus Transparent Mode

Both inline mode and transparent mode work like bump in the wire

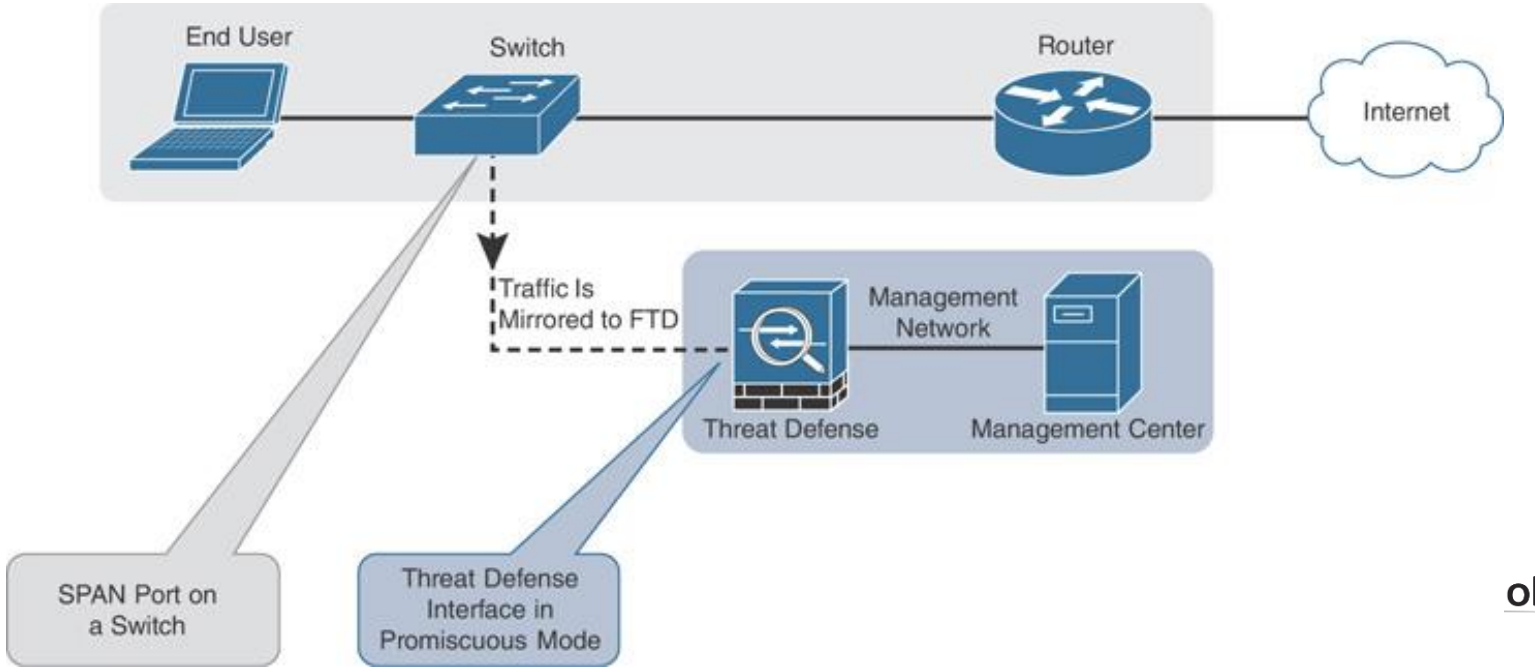
InLine mode	Transparent mode
invisible to the connected devices	invisible to the connected devices
Is a interface mode (deployable in Routed or transparent)	Is a FTD mode with many interface modes
No need to configure IP for interfaces inside the Pairs	All interfaces are in switching mode
the FTD , put the interfaces in to interface pair , send and receive any traffic are based on policies	Traffic that originates from a FTD uses a (BVI) as its source interface
a threat defense does not support NAT	you can enable Network Address Translation (NAT)

Detection-Only Modes

When you consider to deploy Detection only , mainly have two choices :Passive mode and Inline tap mode.

➢ Passive mode

- When an interface is configured in passive mode ,it is set into promiscuous mode
- Promiscuous mode allows an interface to see any packet in a network segment
- In passive mode , FTD monitors the network activities without being an active part of a network.



Passive mode

SPAN port :

- Some switch models can replicate traffic from other ports and send the copies to a specific switch port
- This feature is known as port mirroring and that port knows as Switched Port Analyzer (SPAN) port
- A SPAN port can receive mirrored traffic from the same Layer 2 switch

ERSPAN

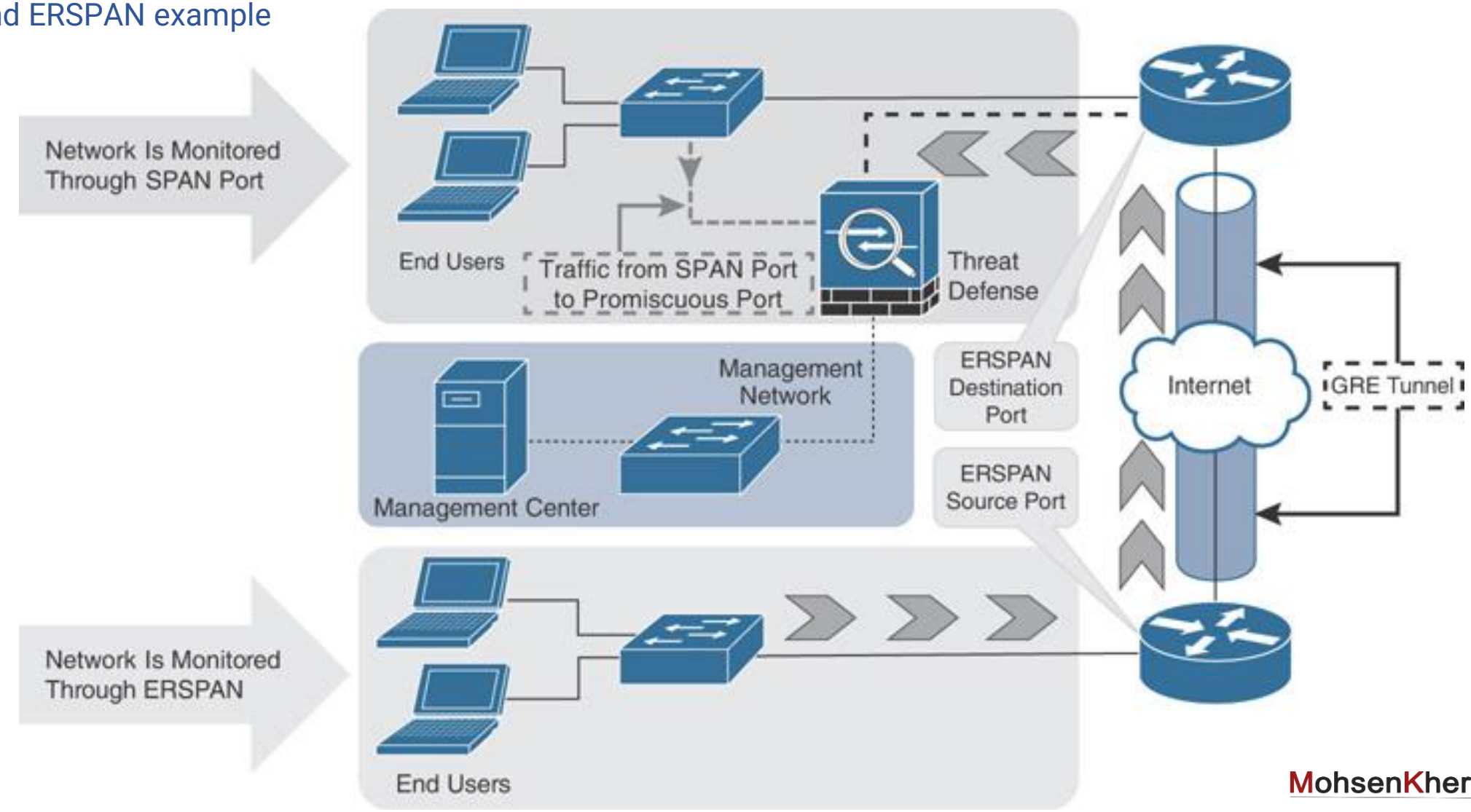
- Transports mirrored traffic over a Layer 3 network by encapsulating it using the (GRE) tunneling protocol.

➢ A threat defense supports inspection of both SPAN and ERSPAN traffic.

Recommendation : enable portfast on the associated switch ports to reduces hardware bypass time.

Passive mode

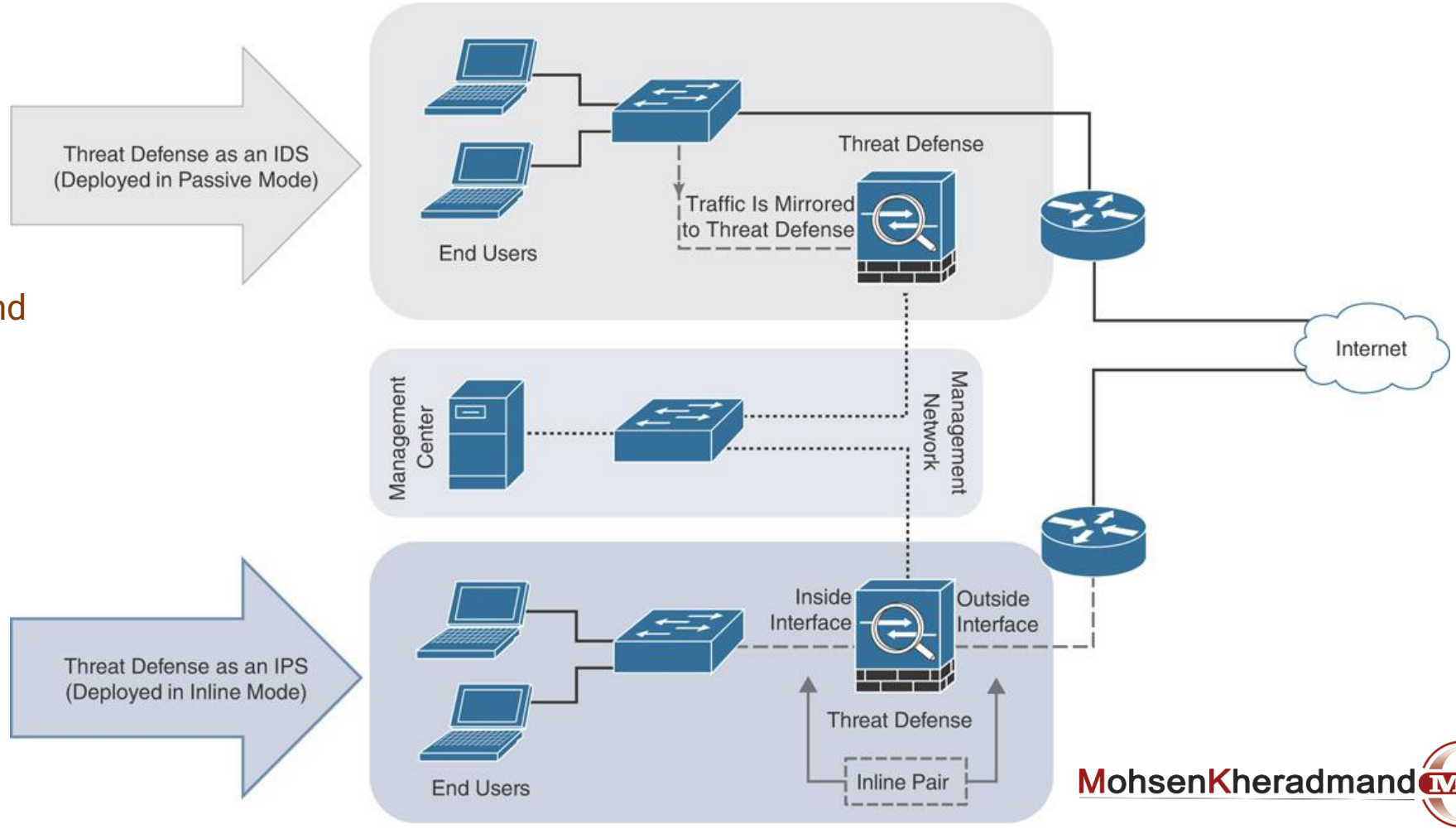
SPAN and ERSPAN example



TAP mode

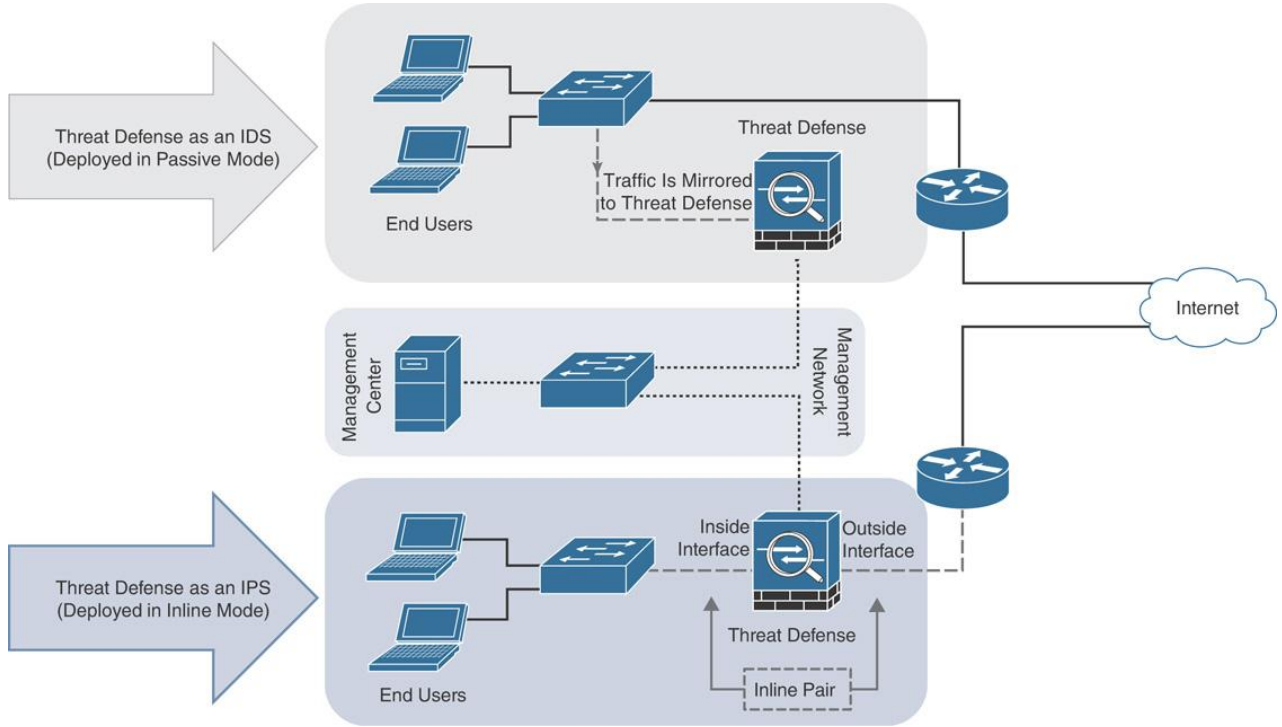
- A TAP is a network device that copies and transfers traffic to another system.
- TAP is dedicated hardware that is designed to replicate and transfer traffic.

Difference Between Inline and Passive Deployment Modes



TAP mode

Difference Between Inline / Inline TAP / Passive

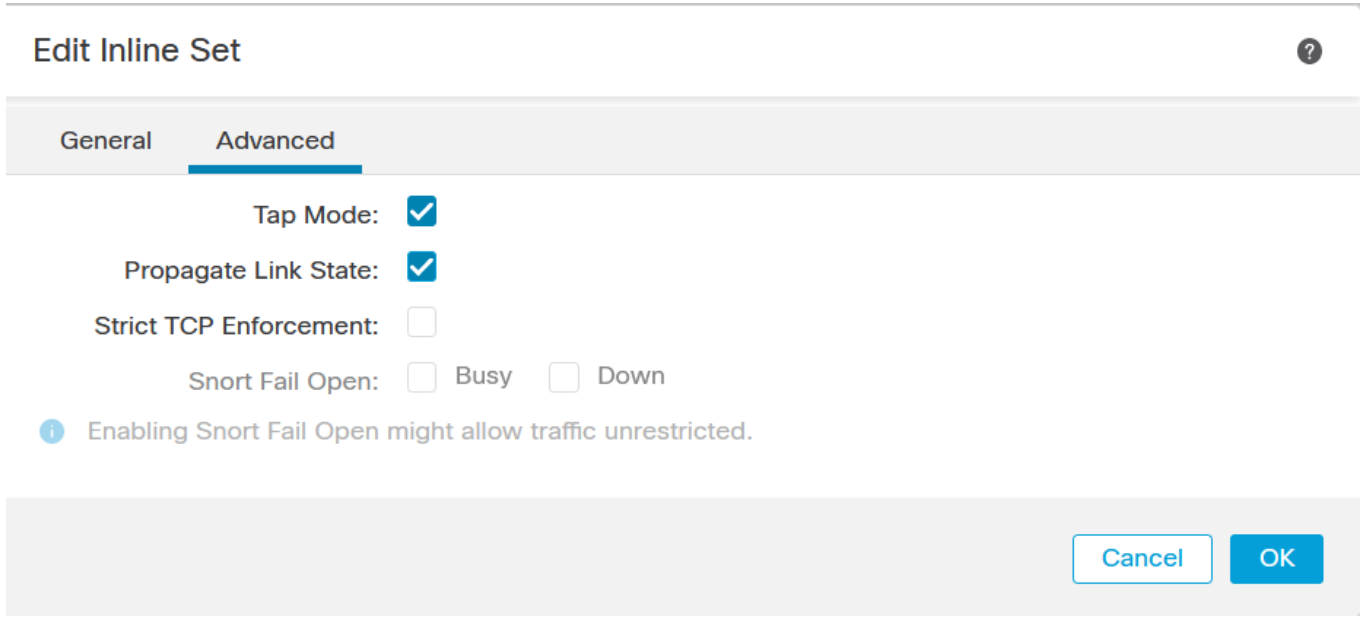


- Inline mode (IPS) allows a threat defense to block traffic based on rules
- In Passive and Inline tap modes , FTD just generate event against block rule (not prevention)
- Advantage of inline tap mode over passive mode :
  - ✓ The ease of transition to the inline mode (you can simply switch from inline tap to inline mode)
  - ✓ In SPAN fails , the FTD will lost visibility , but in inline mode , all traffic is captured continuously

TAP mode configuration

Inline tap mode configurations are similar to the regular inline mode

1. Configure general settings of interfaces.
2. Build an inline pair (General setting).
3. Enable inline tap (Advanced setting).
4. Save the configuration changes.
5. Deploy the configurations to threat defense



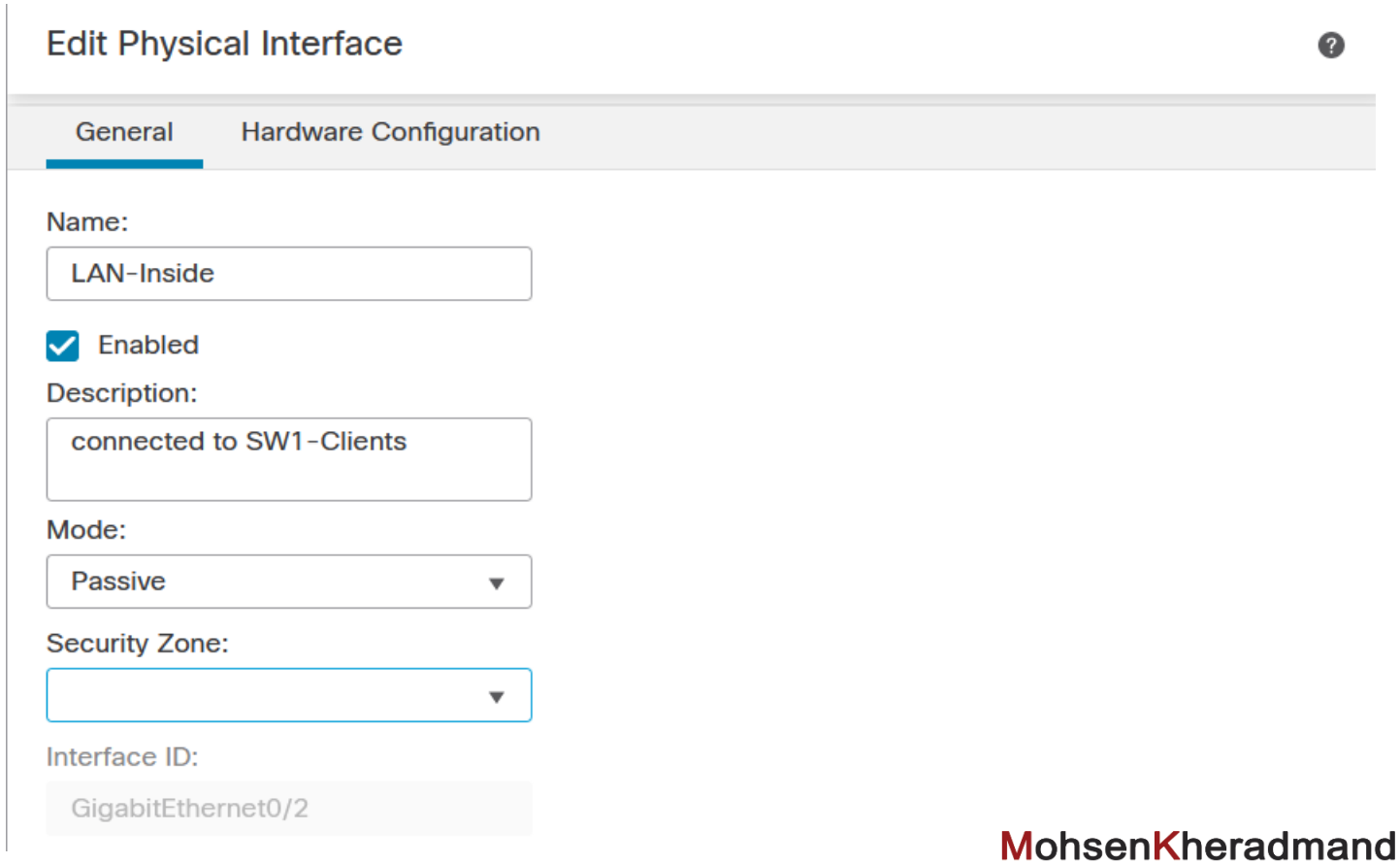
Verification of Inline Tap

<show inline-set

Passive mode configuration

- It is simple , use just one interface to receive traffic from a mirror port
- An egress interface is not necessary (traffic is not suppose to be forwarded)

SPAN mode configuration

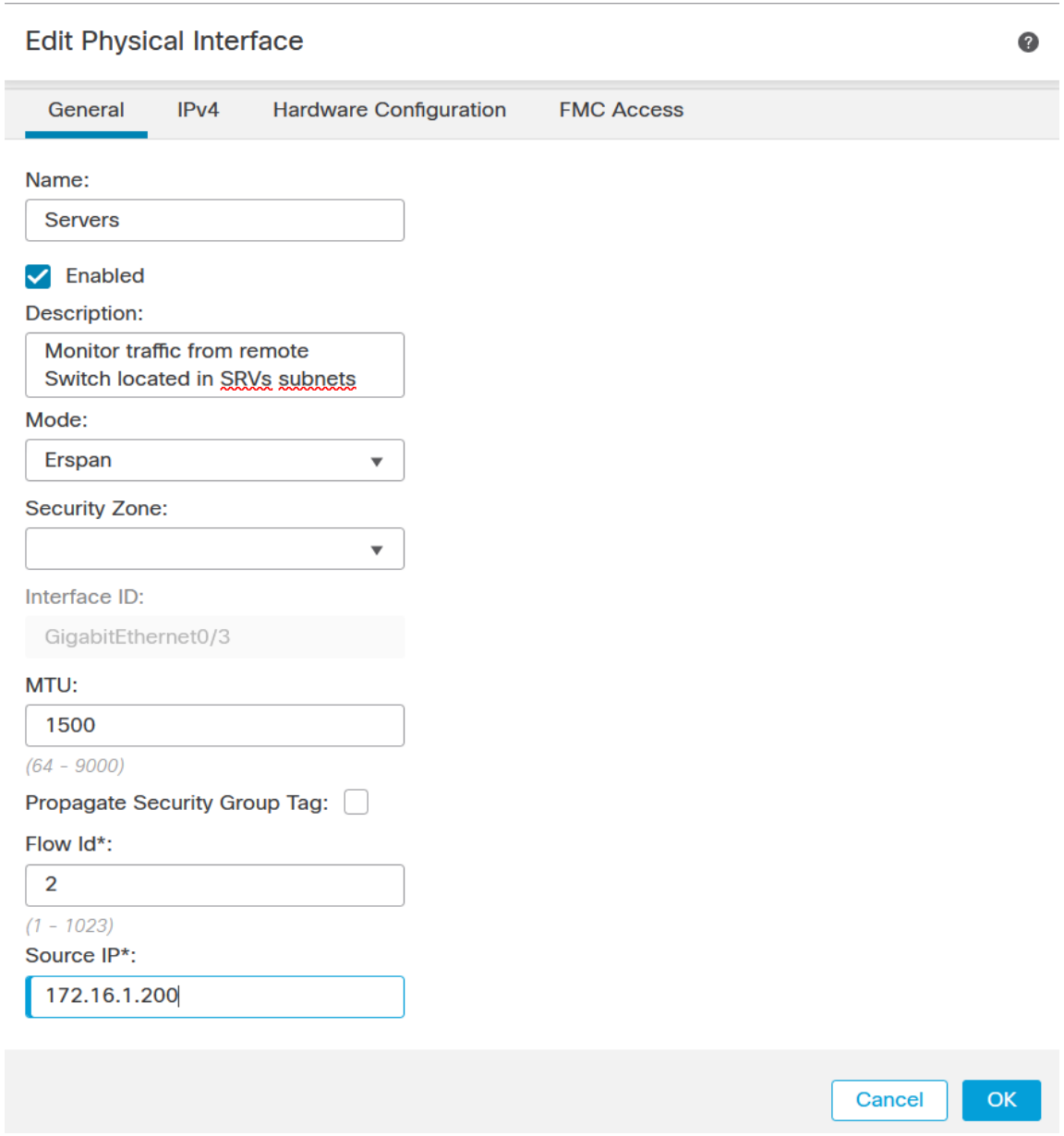


Passive mode configuration

ERSPAN mode configuration

Flow Id : Configure the ID used by the source and destination

Source IP : the IP address of the source of the ERSPAN traffic



Local Switched Port Analyzer (SPAN)

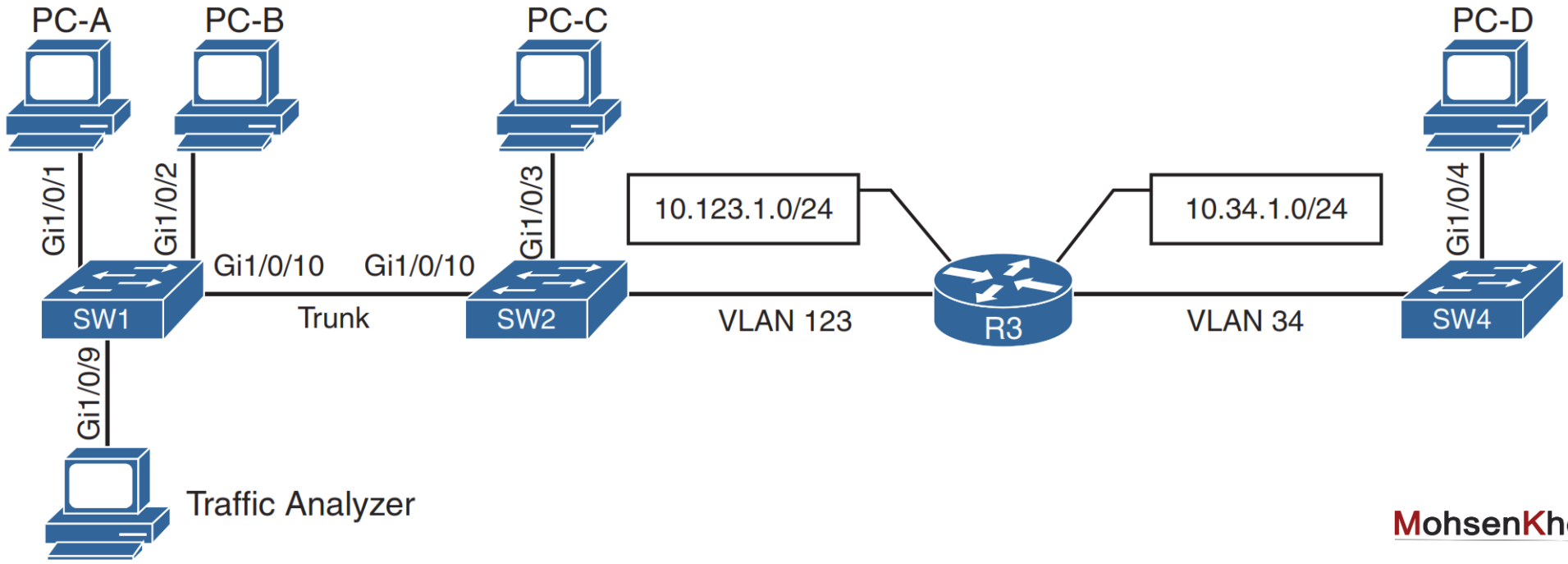
capture local network traffic on a switch

Remote Switched Port Analyzer (RSPAN)

Monitor multiple switch but traffic copied to central Analyzer

Encapsulated Remote Switched Port Analyzer (ERSPAN)

capture network traffic on a remote device (Layer 3 Routing)



Local SPAN

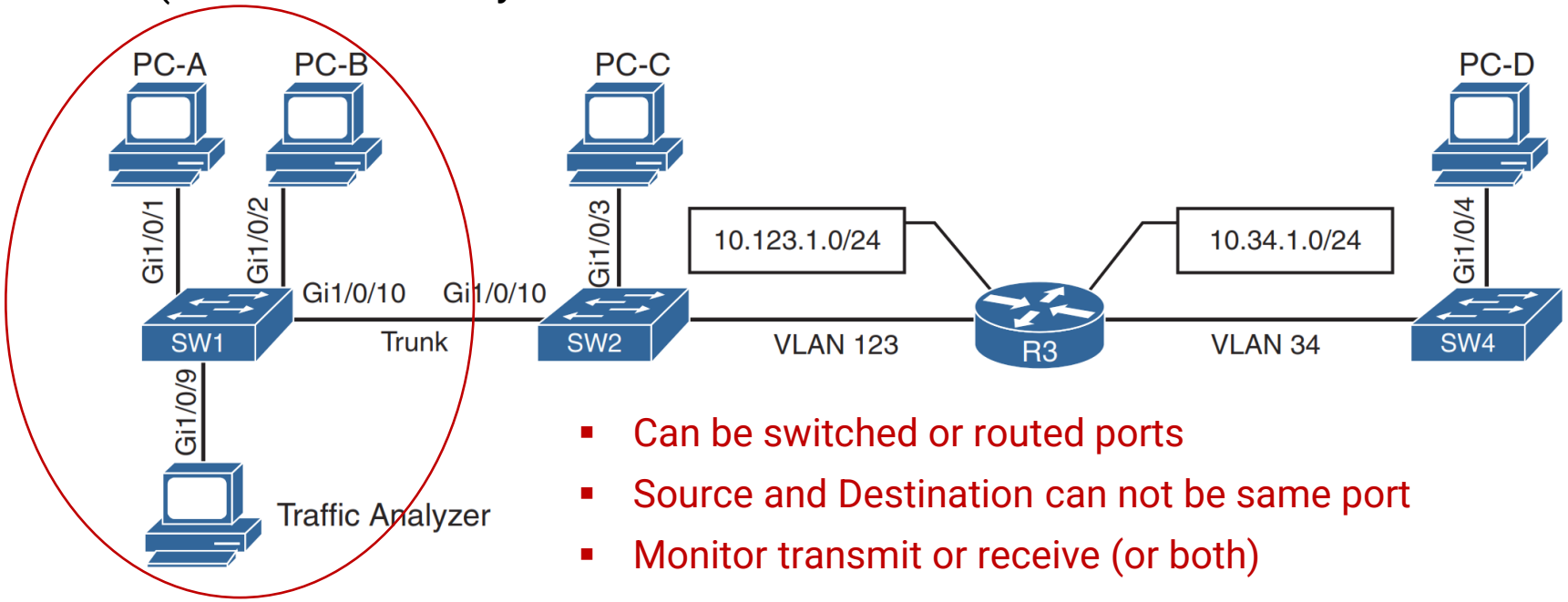
- The **destination** of the mirrored traffic : one or more local ports to the analyzer

- The **source** of the packet capture can be only one of the following:

✓ One or more specific switch ports

✓ A port channel (also known as an EtherChannel)

✓ A VLAN (traffic received by the switch the hosts associated to the VLAN not a SVI interface)



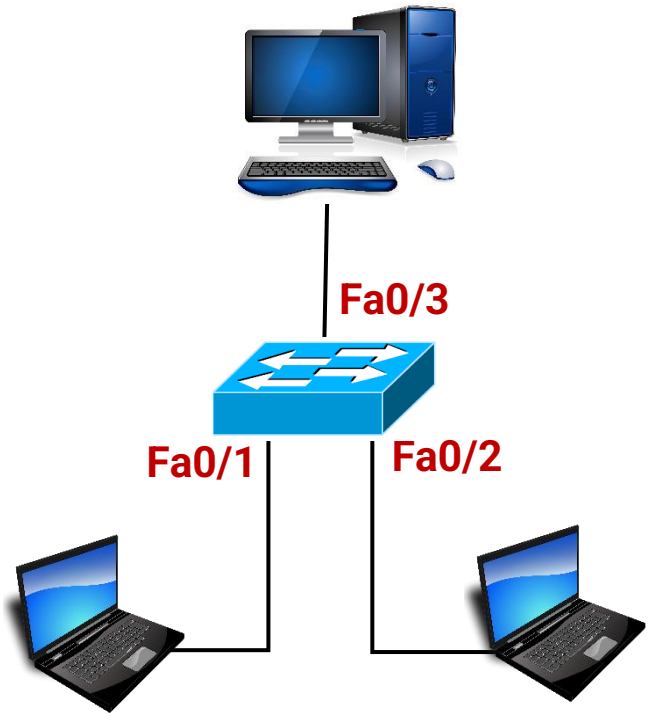
- Can be switched or routed ports
- Source and Destination can not be same port
- Monitor transmit or receive (or both)

Local SPAN Configuration

SW1(config)# monitor session 1 source interface Fa 0/1-2 both

SW1(config)# monitor session 1 destination interface Fa 0/3

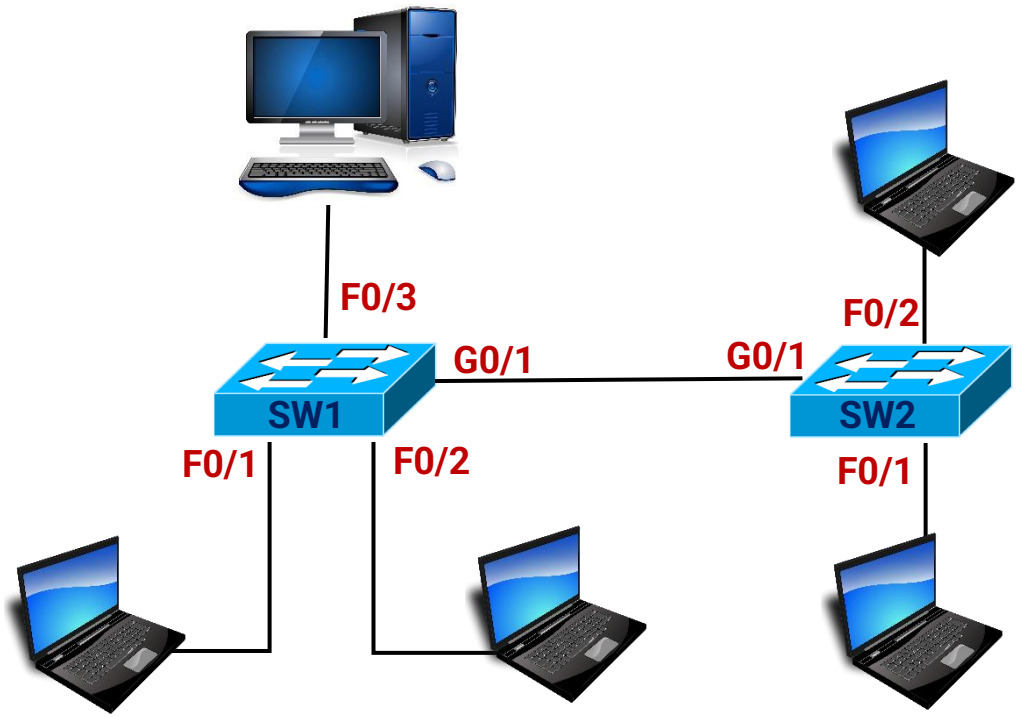
SW1# show monitor session 1



Remote SPAN Configuration

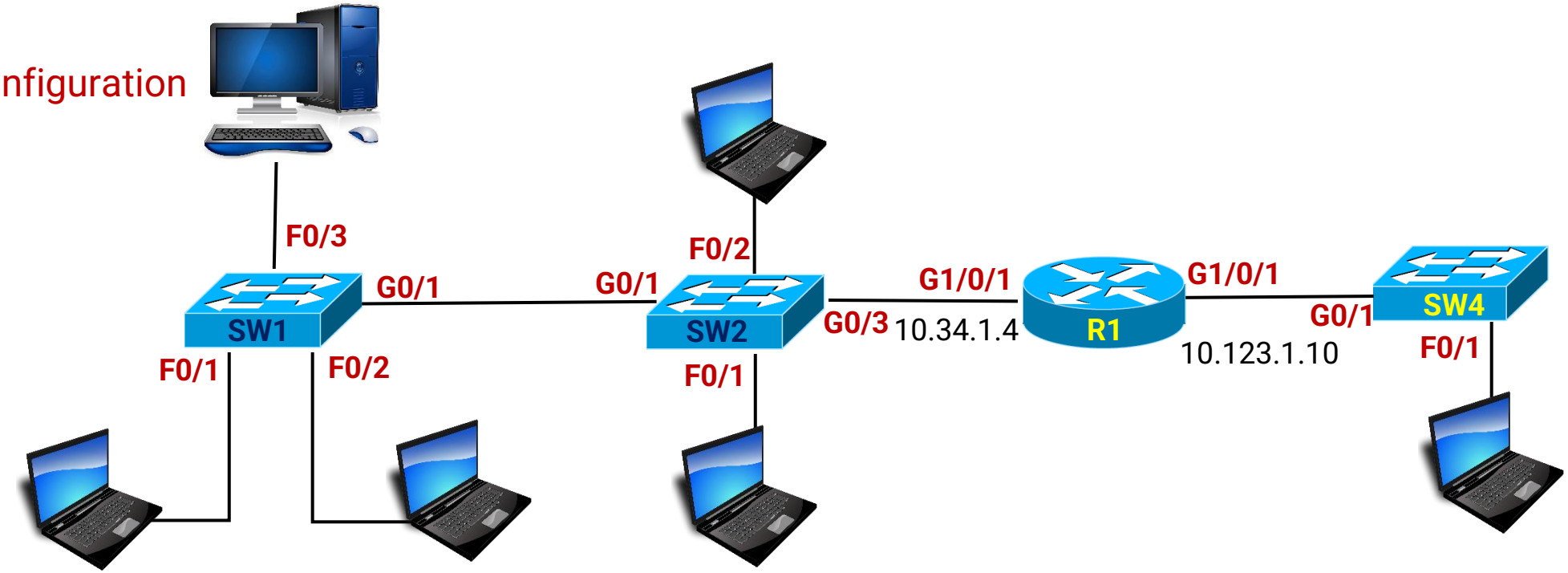
SW2(config-if)#int range F0/1-2
SW2(config-if-range)#swithport access vlan 10
SW2(config)#vlan 200
SW2(config-vlan)#remote-span
SW2(config-vlan)#name *RSPAN*
SW2(config-vlan)#exit
SW2(config)# monitor session 2 source interface Fa 0/1- 2
SW2(config)# monitor session 2 destination remote vlan 200

SW1(config-if)#int range F0/1-3
SW1(config-if-range)#sw access vlan 10
SW1(config)#vlan 200
SW1(config-vlan)#remote-span
SW1(config-vlan)#name *RSPAN*
SW1(config-vlan)#exit
SW1(config)# monitor session 2 source remote vlan 200
SW1(config)# monitor session 2 destination interface Fa 0/3



SW(config)#interface G0/1
SW(config-if)#switchport trunk encapsulation dot1q
SW(config-if)#switchport mode trunk

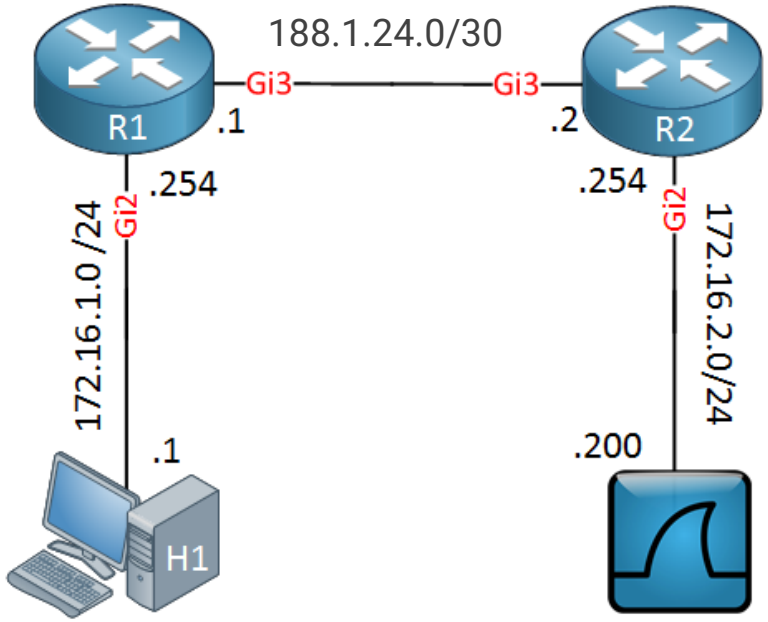
Encapsulated RSPAN Configuration




```
SW4(config)# monitor session 1 type erspan-source
SW4(config-mon-erspan-src)# source interface F0/1 rx
SW4(config-mon-erspan-src)# filter vlan 34
SW4(config-mon-erspan-src)# no shutdown
SW4(config-mon-erspan-src)# destination
SW4(config-mon-erspan-src-dst)# ip address 10.123.1.10
SW4(config-mon-erspan-src-dst)# erspan-id 2
SW4(config-mon-erspan-src-dst)# origin ip address 10.34.1.4
```

Encapsulated RSPAN Configuration

Example 2




```
R1(config)# monitor session 1 type erspan-source
R1(config-mon-erspan-src)# source interface GigabitEthernet 2 rx
R1(config-mon-erspan-src)# no shutdown
R1(config-mon-erspan-src)# destination
R1(config-mon-erspan-src-dst)# erspan-id 100
R1(config-mon-erspan-src-dst)# ip address 172.16.2.200
R1(config-mon-erspan-src-dst)# origin ip address 188.1.24.1
```

```
R2(config)# monitor session 1 type erspan-destination
R2(config-mon-erspan-dst)# no shutdown
R2(config-mon-erspan-dst)# destination interface GigabitEthernet 2
R2(config-mon-erspan-dst)# source
R2(config-mon-erspan-dst-src)# erspan-id 100
R2(config-mon-erspan-dst-src)# ip address 172.16.2.200
```