

Securing Networks with
Cisco FTD

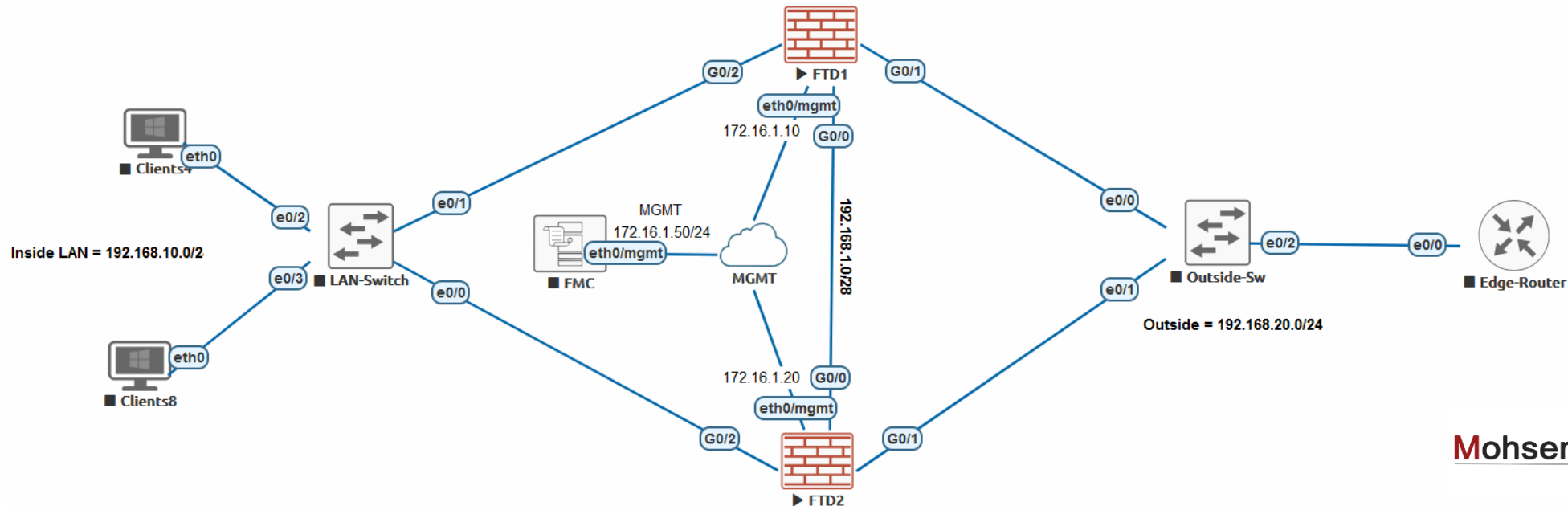
Chapter 20

High Availability

Mohsen Kheradmand

High Availability (Fail Over)

- By HA, two identical FTD devices Connected to each other through a dedicated failover link , means if primary device fails, the secondary device takes over to forward the traffic.
- Active/Standby failover :
 - The Active unit passes traffic
 - The standby unit does not actively pass traffic, but synchronizes configuration from the active unit
 - When a failover occurs, the active unit fails over to the standby unit, which then becomes active
- The health of the active unit (hardware, interfaces, software, and environmental status) is monitored for failover condition



Hardware Requirements

- The two units in a HA configuration must:
 - Be the same model
 - Be in the same firewall mode (routed or transparent).
 - Have the same software version.
 - Be in the same domain or group on the FMC.
 - Have the same NTP configuration
 - Not have DHCP or PPPoE configured in any of their interfaces
 - Be fully deployed on the FMC with no uncommitted changes
 - Must have the same licenses. (Require two smart license entitlements; one for each device in the pair)

Failover and Stateful Failover Links

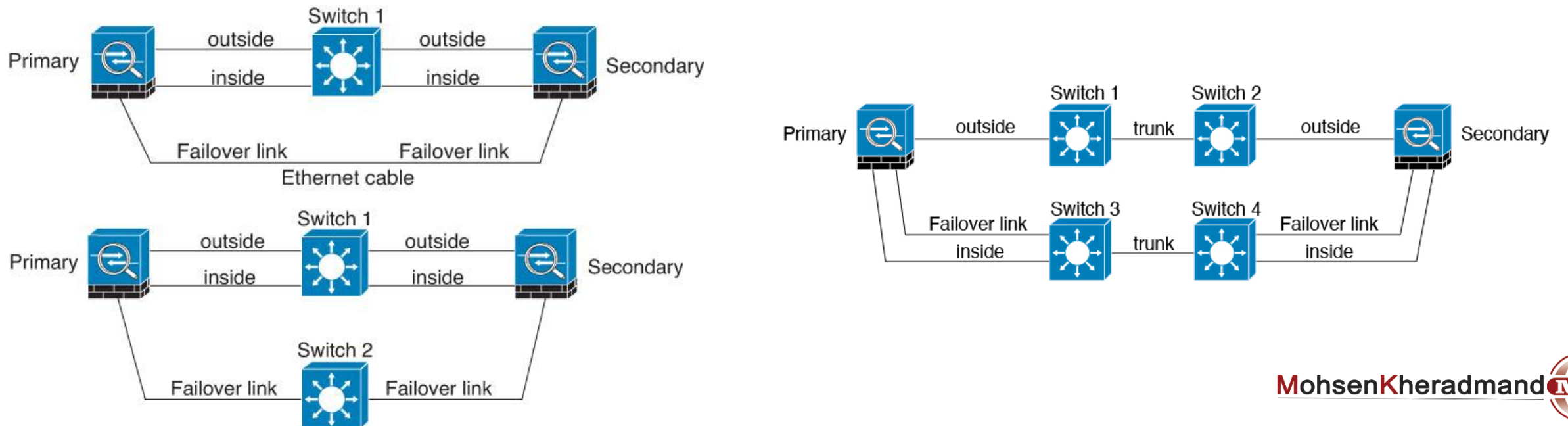
- **Failover link** : dedicated connections between the two units (better to be same physical interface on both FTDs)
 - **Failover Data** :
 - ✓ The unit state (active or standby)
 - ✓ Hello messages (keep-alives)
 - ✓ Network link status
 - ✓ MAC address exchange
 - ✓ Configuration replication and synchronization
- ✓ **State link**: synchronize connection state information like session table and NAT table, so that if a failover occurs, existing connections are not disrupted.
 - An Interface that is configured with a name can not be used for failover
 - The FTD does not support sharing interfaces between user data and the failover link
 - If you use EtherChannel for failover link , to prevent out-of-order packets, only one interface in the EtherChannel is used

Failover and Stateful Failover Links

➤ Scenario 1—Not Recommended topologies



➤ Scenario 2—Recommended topologies



HA configuration

- 1) Configure initial setup on both FTDs and add them to FMC
 - Devices -> Device Management -> Add -> Device
- 2) Add devices to HA party
 - Devices -> Device Management -> Add -> High Availability
 - Enter a name for HA
 - Select Firepower Threat defense
 - Select FTD1 as a Primary
 - Select FTD2 as a secondary
 - Click Continue (click Yes)

Warning

This operation restarts the Snort processes of primary and secondary devices, temporarily causing traffic interruption.

Do you want to continue?

☐ Do not display this message again

Add High Availability Pair

Name:*

Device Type:

Primary Peer:

Secondary Peer:

i Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be converted to their high availability versions and applied on both peers.

Add Device

Host:†

Display Name:

Registration Key:*

Group:

Access Control Policy:*

Smart Licensing

Note: All virtual FTDs require a performance tier license. Make sure your Smart Licensing account contains the available licenses you need. It's important to choose the tier that matches the license you have in your account. Click [here](#) for information about the FTD performance-tiered licensing. Until you choose a tier, your FTDv defaults to the FTDv50 selection.

Performance Tier (only for FTDv 7.0 and above):

☒ Malware
☒ Threat
☒ URL Filtering

Advanced

Unique NAT ID:†

☒ Transfer Packets

HA configuration

3) Configure HA and State link

- Select HA interface of FTD1
- Enter a name for Logical interface
- Enter an IP address for HA interface
- Enter Secondary IP for FTD2 HA interface
- Enter subnet mask
- You can use same interface for state Link
- Enable IPsec Encryption , and specify a password for more security on HA
- Click Add

High Availability Pair Added

Configure interface monitoring options to protect the HA pair interfaces. Apply the same health policies to the primary and secondary nodes of the HA pair.

OK

Add High Availability Pair



High Availability Link

Interface:* GigabitEthernet0/0 ▼

Logical Name:* HA-Link

Primary IP:* 172.16.1.10

☐ Use IPv6 Address

Secondary IP:* 172.16.1.20

Subnet Mask:* 255.255.255.0

IPsec Encryption

☒ Enabled

Key Generation: Custom ▼

Shared Key:* ●●●●●●●●●● 🔍

Confirm Key:* ●●●●●●●●●● 🔍

i LAN failover link is used to sync configuration, stateful failover link is used to sync application content between peers. Selected interface links and encryption settings cannot be changed later.

State Link

Interface:* Same as LAN Failover Link ▼

Logical Name:* HA-Link

Primary IP:* 172.16.1.10

☐ Use IPv6 Address

Secondary IP:* 172.16.1.20

Subnet Mask:* 255.255.255.0

Cancel

Add

HA configuration

- Both devices will appear under a HA configuration showing the high availability configuration

Firepower Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects AMP Intelligence

Deploy 🔍 ⚠️ ⚙️ ? admin ▼

View By: **Group** [Deployment History](#)

All (2) ● Error (0) ● Warning (1) ● Offline (0) ● Normal (1) ● Deployment Pending (0) ● Upgrade (0) ● Snort 3 (2) [Add](#) ▼

[Collapse All](#)

☐	Name	Model	Version	Chassis	Licenses	Access Control Policy	
☐	▼ Ungrouped (1)						
☐	▼ HA High Availability						✎ ⋮
☒	✓ FTD1(Primary, Active) Snort 3 192.168.10.201 - Routed	FTDv for VMware	7.0.1	N/A	Base, Threat (2 more...)	Default-Block-Policy	⋮
☒	⚠️ FTD2(Secondary, Standby) Snort 3 192.168.10.202 - Routed	FTDv for VMware	7.0.1	N/A	Base, Threat (2 more...)	Default-Block-Policy	⋮

- You cannot configure each device separately (only configure HA that publish the configuration in both devices)

HA Verification

- Command Line :
 - ✓ Show failover state