Securing Networks with

Cisco FTD

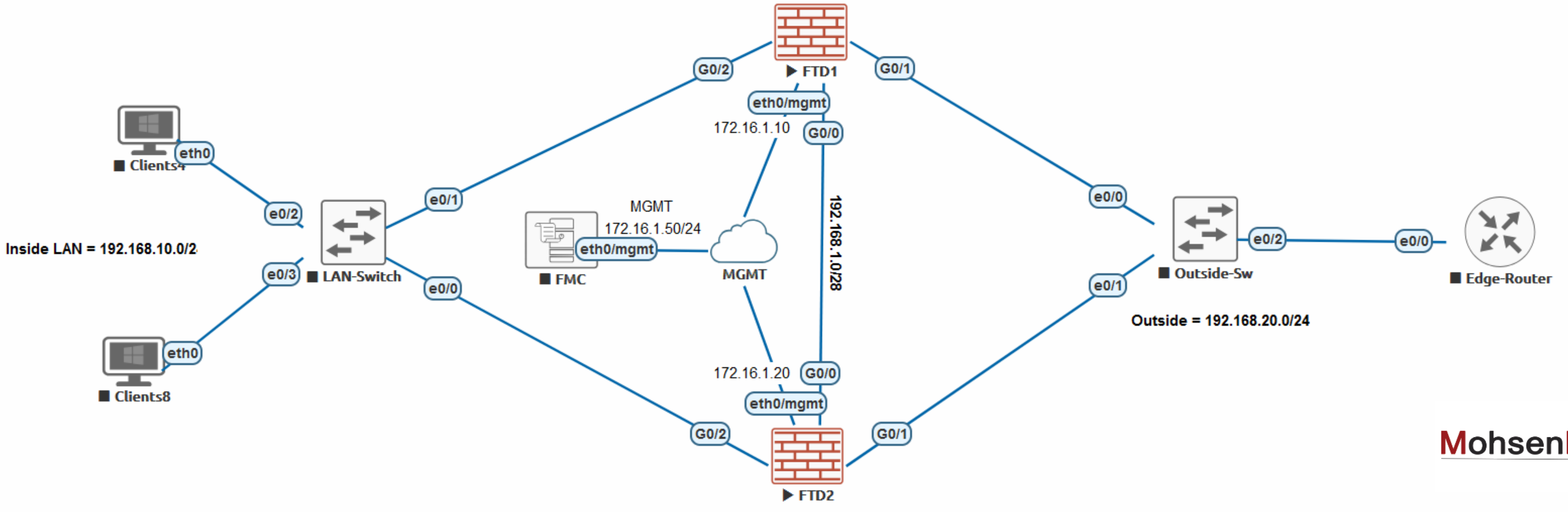
Chapter 20

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



MohsenKheradmand

Hardware Requirements

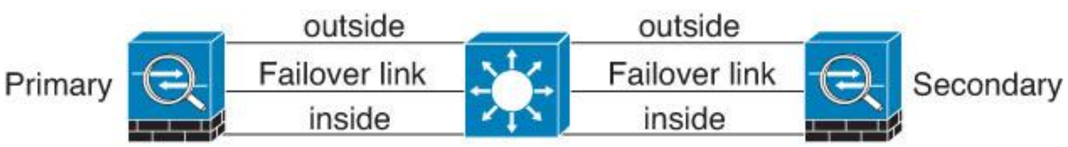
- The two units in a HA configuration must:
  - Be the same model
  - Be in the same firewall mode (routed or transparent).
  - Have the same software version.
  - Be in the same domain or group on the FMC.
  - Have the same NTP configuration
  - Not have DHCP or PPPoe configured in any of their interfaces
  - 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)

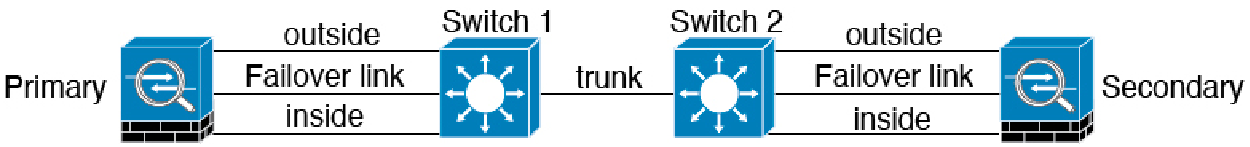
Failover and Stateful Failover Links

- ➢ 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

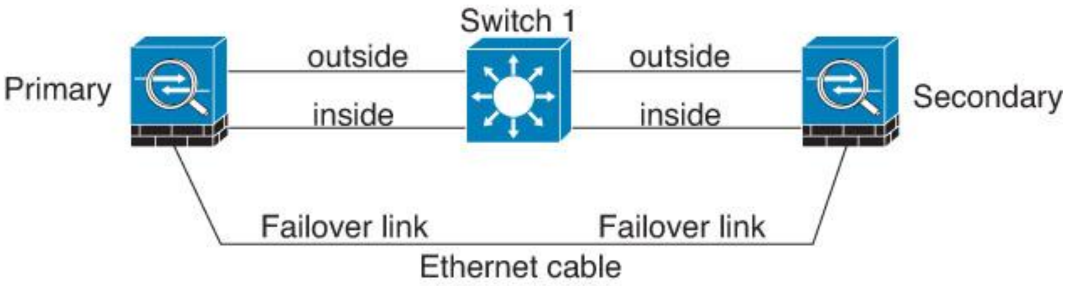
Failover and Stateful Failover Links

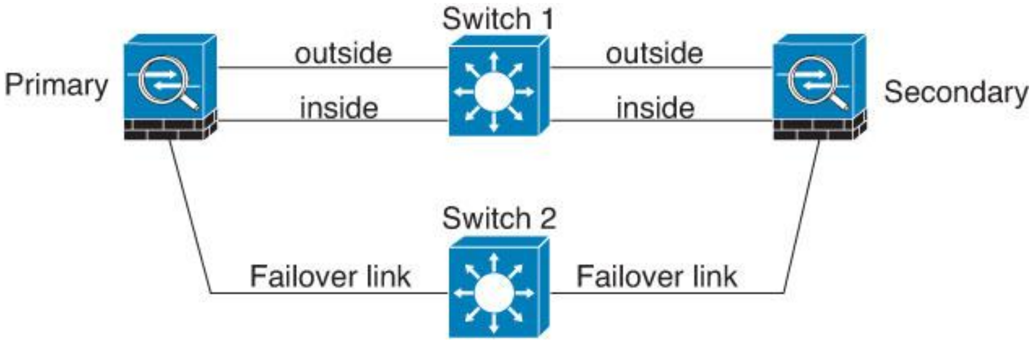
- ➢ Scenario 1—Not Recommended topologies

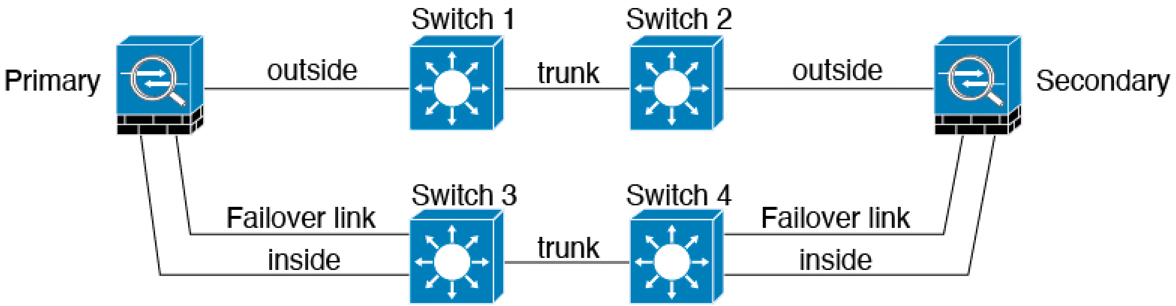




- ➢ Scenario 2—Recommended topologies



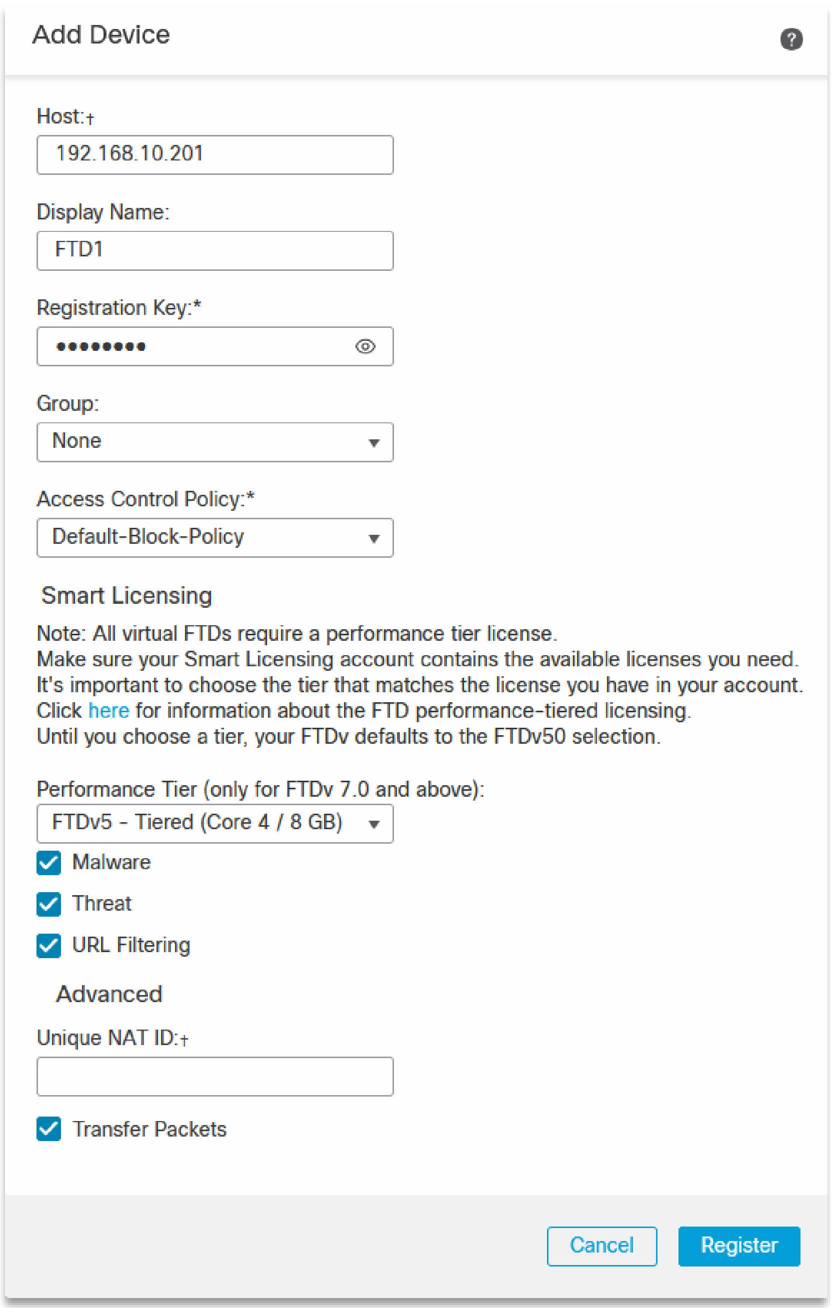


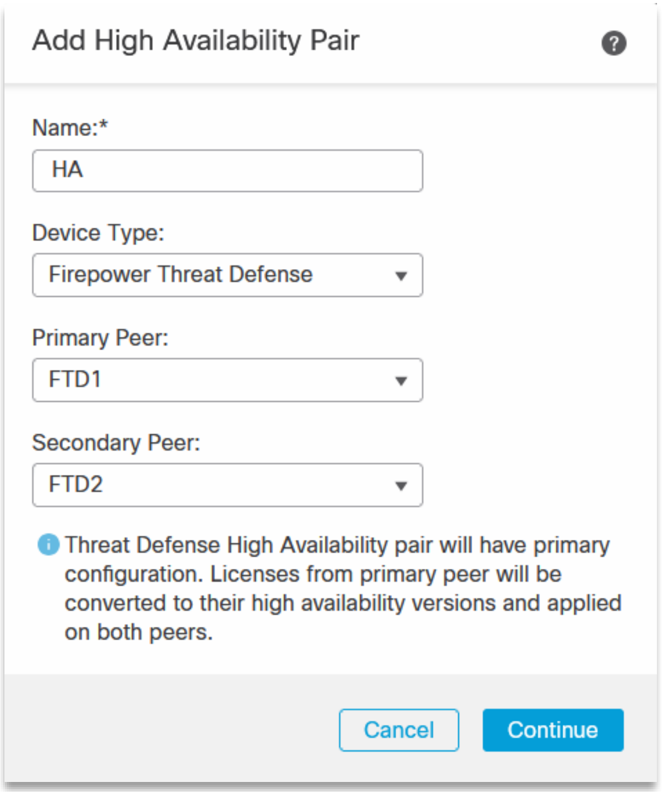


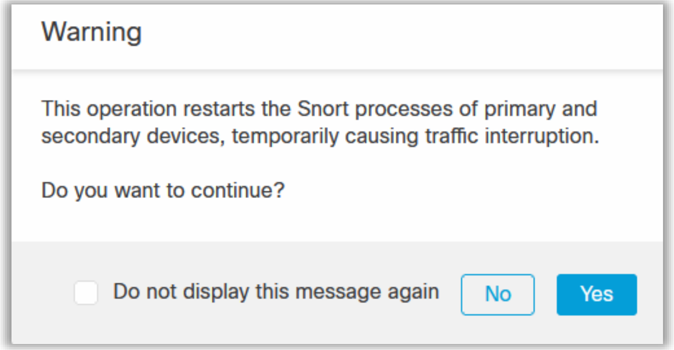
HA configuration

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)



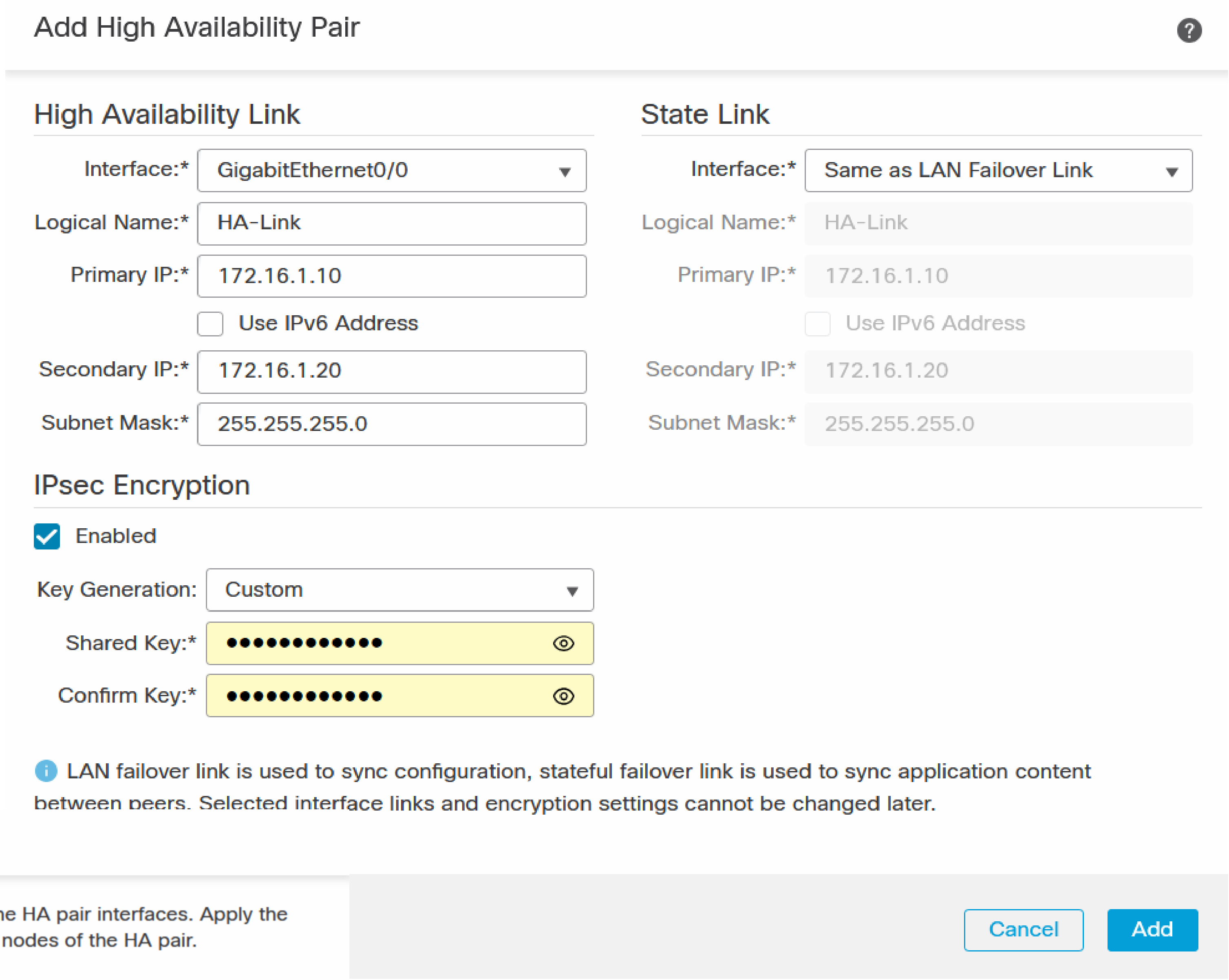


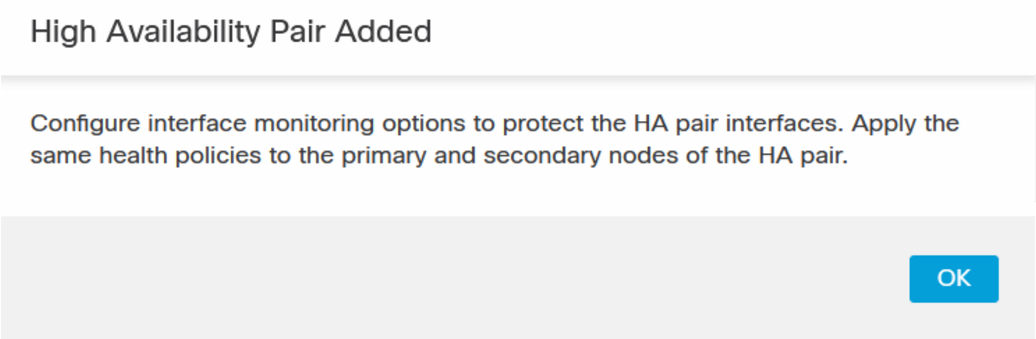


HA configuration

3) Configure HA and State link

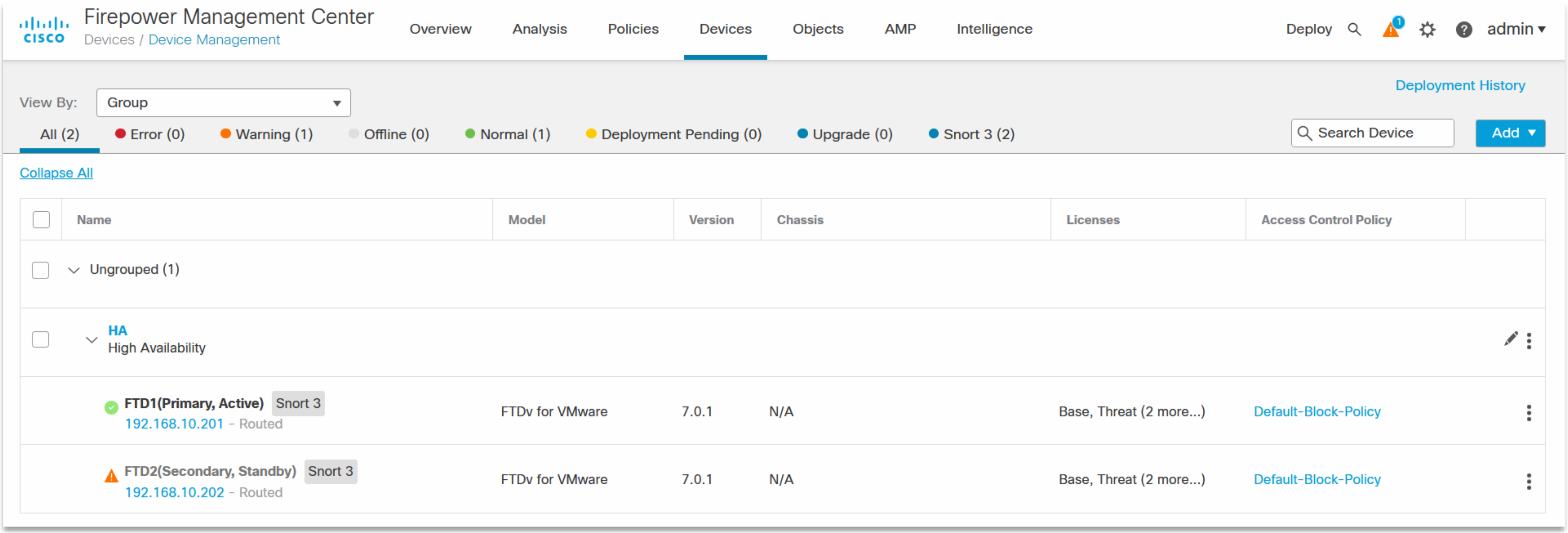
- Select HA interface of FTD1
- Enter a name for Logical interface
- Enter an IP address for HA interface
- Enter Secondary IP for FTD2 HA interface
- Enter subnet mask
- You can use same interface for state Link
- Enable IPsec Encryption , and specify a password for more security on HA
- Click Add





HA configuration

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



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

HA Verification

- Command Line :
  - ✓ Show failover state