You make **possible**

NGFW Clustering Deep Dive

Andrew Ossipov, Distinguished Engineer

BRKSEC-3032

Barcelona | January 27-31, 2020

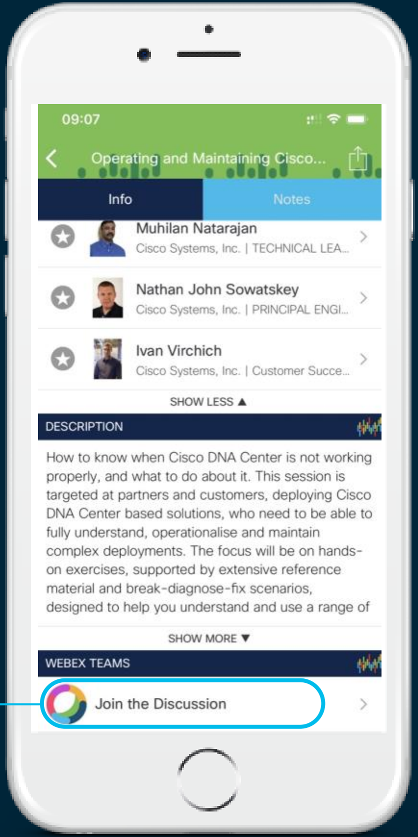
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



09:07

Operating and Maintaining Cisco...

Info | Notes

Muhilan Natarajan
Cisco Systems, Inc. | TECHNICAL LEA...

Nathan John Sowatskey
Cisco Systems, Inc. | PRINCIPAL ENGI...

Ivan Virchich
Cisco Systems, Inc. | Customer Succe...

SHOW LESS ▲

DESCRIPTION

How to know when Cisco DNA Center is not working properly, and what to do about it. This session is targeted at partners and customers, deploying Cisco DNA Center based solutions, who need to be able to fully understand, operationalise and maintain complex deployments. The focus will be on hands-on exercises, supported by extensive reference material and break-diagnose-fix scenarios, designed to help you understand and use a range of

SHOW MORE ▼

WEBEX TEAMS

Join the Discussion

Your Speaker

Andrew Ossipov

aeo@cisco.com

Distinguished Engineer

NGFW, Solution Architecture, Hybrid Cloud DC

IETF: OpSec and TLS Working Groups

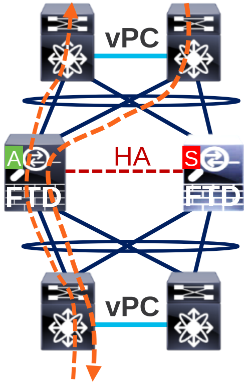
Agenda

- Clustering Overview
- Unit Roles and Functions
- Packet Flow
- Control and Data Interfaces
- Configuring Clustering
- Multi-Site Clustering
- Closing Remarks

Clustering Overview

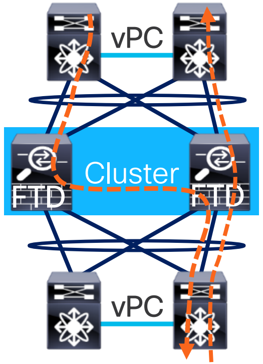
High Availability on ASA and FTD

- A pair of identical ASA or FTD devices can be configured in Failover/HA
  - Managed as a single entity
  - Data interface connections must be mirrored between the units with L2 adjacency
  - Virtual IP and MAC addresses on data interfaces move with Active unit
  - Stateful connection table is replicated to Standby in real time
- Failover/HA deliver high availability rather than scalability
  - Limited to two physical appliances/modules or virtual instances
  - Active/Standby for asymmetry avoidance in ASA or FTD
  - Active/Active with multiple contexts in ASA is impractical for scaling



ASA and FTD Clustering

- Up to 16 appliances or modules combine in one traffic processing system
- Preserve failover benefits by configuring and operating as a single entity
  - Virtual IP and MAC addresses for first-hop redundancy
  - Connection states are preserved after a single member failure
- Implement true scalability in addition to high availability
  - Fully distributed data plane for new and existing connections
  - Elastic scaling of throughput and maximum concurrent connections
  - Stateless external load-balancing through standard Etherchannel
  - Out-of-band Cluster Control Link for asymmetry normalization
  - No member-to-member communication on data interfaces



System Requirements

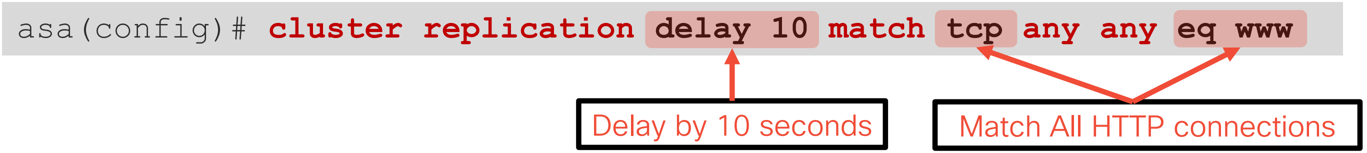
- ASA scales up to 16 identical appliances or modules
  - Up to 16 Firepower 4100 or 9300 modules with matching Export Compliance
  - Up to 16 ASA5585-X with Cluster and same 3DES and 10GE I/O licenses
  - Up to 2 ASA5500-X with Security Plus and matching 3DES licenses
- FTD scales up to 6 identical appliances or modules as documented
  - Up to 16 Firepower 4100 appliances or 9300 modules is configurable
  - Multi-instance capability in FTD 6.6 will no longer require identical hardware
  - Some advanced cluster settings must use FlexConfig
- Any standard-based switch is supported, some are explicitly validated

Unsupported Features

- Remote Access VPN: TLS VPN, Clientless SSL VPN, and IPSec
- S2S VPN on FTD only until 6.2.3.3
- DHCP client, DHCP server, DHCP Proxy
- Advanced Application Inspection and Redirection
  - CTIQBE, WAAS, MGCP, MMP, RTSP, Skinny/SCCP, H.323
  - Dead Connection Detection (DCD) until ASA 9.13, Botnet Traffic Filter, and WCCP
- Interfaces: Integrated Routing/Bridging (IRB), Virtual Tunnel Interface (VTI)
- Intermediate System-to-Intermediate System (IS-IS)
- Firepower Multi-Instance Capability until FTD 6.6

Scalability

- Throughput scales at 70-80% of the aggregated capacity on average
  - ASA: 16 Firepower 4145 at 50Gbps → 640Gbps of Multiprotocol Throughput
  - FTD: 6 Firepower 9300 SM-44 at 50Gbps → 240Gbps of NGFW AVC Throughput
- Replicated concurrent conn(ection)s scale at 60% of aggregated capacity
  - FTD: 6 Firepower 4150 at 35M → 126M concurrent conns
  - Firepower 9300 supports 120M (ASA) or 60M (FTD) conns per clustered chassis
- Conn rate with full replication scales at 50% of the aggregated capacity
  - ASA: 16 ASA5585-X SSP-60 at 350K CPS → 2.8M CPS
  - Short-lived connections may scale at 100% with delayed replication



```
asa(config)# cluster replication delay 10 match tcp any any eq www
```

Centralized Features

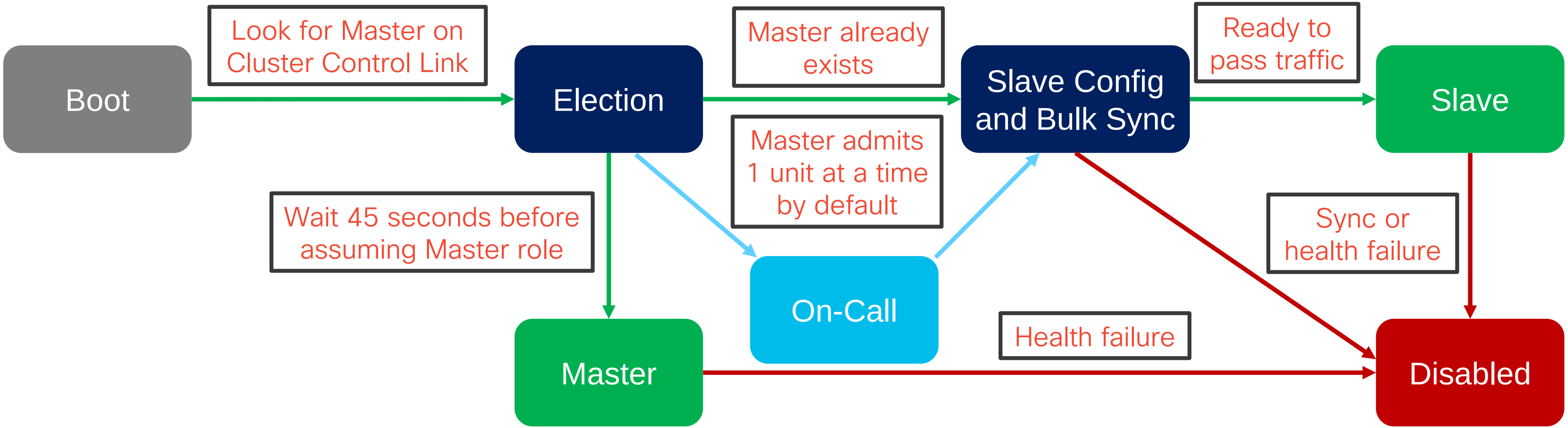
- Not all features are distributed, some are Centralized
  - Control and management connections
  - Non-Per-Session Xlates with PAT (e.g. ICMP)
  - DCERPC, ESMTP, IM, Netbios, PPTP, RADIUS, RSH, SNMP, SQLNet, SunRPC, TFTP, and XDMCP inspection engines
  - Site-to-site VPN until ASA 9.9(1) with optional distribution on Firepower 9300
  - Multicast in rare scenarios
- Any connections with these features always land on one cluster member
  - Switchover of such connections is not seamless

Unit Roles and Functions

Master and Slaves

- One cluster member is elected as the Master; others are Slaves
    - First unit joining the cluster or based on configured priority
    - New master is elected only upon a departure of the existing one
- Master unit handles all management and centralized functions
    - Configuration is blocked on all other members
    - Virtual IP address ownership for to-the-cluster connections
- Master and slaves process all regular transit connections equally
    - Management and centralized connections must reestablish upon Master failure
    - Disable or reload Master to transition the role

State Transition



Boot

Look for Master on Cluster Control Link

Election

Master already exists

Slave Config and Bulk Sync

Ready to pass traffic

Slave

Master admits 1 unit at a time by default

Wait 45 seconds before assuming Master role

On-Call

Sync or health failure

Master

Health failure

Disabled

```
ASA/master# show cluster history
==========================================================================
From State            To State              Reason
==========================================================================
15:36:33 UTC Dec 3 2018
DISABLED              DISABLED              Disabled at startup
15:37:10 UTC Dec 3 2018
DISABLED              ELECTION              Enabled from CLI
15:37:55 UTC Dec 3 2018
ELECTION              MASTER                Enabled from CLI
==========================================================================
```

```
ASA/master# show cluster info
Cluster sjfw: On
    Interface mode: spanned
    This is "A" in state MASTER
        ID         : 0
        Version    : 9.10(1)
        Serial No.: JAF1434AERL
        CCL IP     : 1.1.1.1
        CCL MAC    : 5475.d029.8856
        Last join : 15:37:55 UTC Dec 3 2018
        Last leave: N/A
```

Reference

Member Admission Optimization

- ASA 9.10(1) and FTD 6.3 allow parallel cluster join on Firepower 9300
  - Each chassis optionally bundles data interfaces only when all modules are ready

```
asa(cfg-cluster)# unit parallel-join 3 max-bundle-delay 5
```

How many modules must replicate configuration and state before enabling chassis data plane

Maximum wait time in minutes

Flow Owner

- All packets for a single stateful connection go through a single member
  - Unit receiving the first packet for a new connection typically becomes Flow Owner
  - Ensures symmetry for state tracking purposes and NGFW/NGIPS inspection

```
ASA/master# show conn
18 in use, 20 most used
Cluster stub connections: 0 in use, 0 most used
TCP outside  10.2.10.2:22 inside  192.168.103.131:35481, idle 0:00:00, bytes 4164516, flags UIO
```

- Another unit will become Flow Owner if the original one fails
  - Receiving packet for an existing connection with no owner
- The conn-rebalance ASA feature should be enabled with caution
  - An overloaded member may work even harder to redirect new connections
- Existing connections move only on unit departure or with Flow Mobility

Flow Director

- Flow Owner for a connection must be discoverable by all cluster members
  - Each possible connection has a deterministically assigned Flow Director
  - Compute hash of {SrcIP, DstIP, SrcPort, DstPort} for a flow to determine Director
  - Hash mappings for all possible flows are evenly distributed among members
  - All members share the same hash table and algorithm for consistent lookups
  - SYN Cookies reduce lookups for TCP flows with Sequence Number Randomization
- Other units ask Flow Director to identify Owner or restore flow from backup
  - New Owner can recover connection state from director upon original Owner failure

    ```
    TCP outside  172.18.254.194:5901 inside  192.168.1.11:54397, idle 0:00:08, bytes 0, flags  Y
    ```

  - Create Backup Flow when Director and Owner is same member or in same chassis

    ```
    TCP outside  172.18.254.194:5901 inside  192.168.1.11:54397, idle 0:00:08, bytes 0, flags  y
    ```

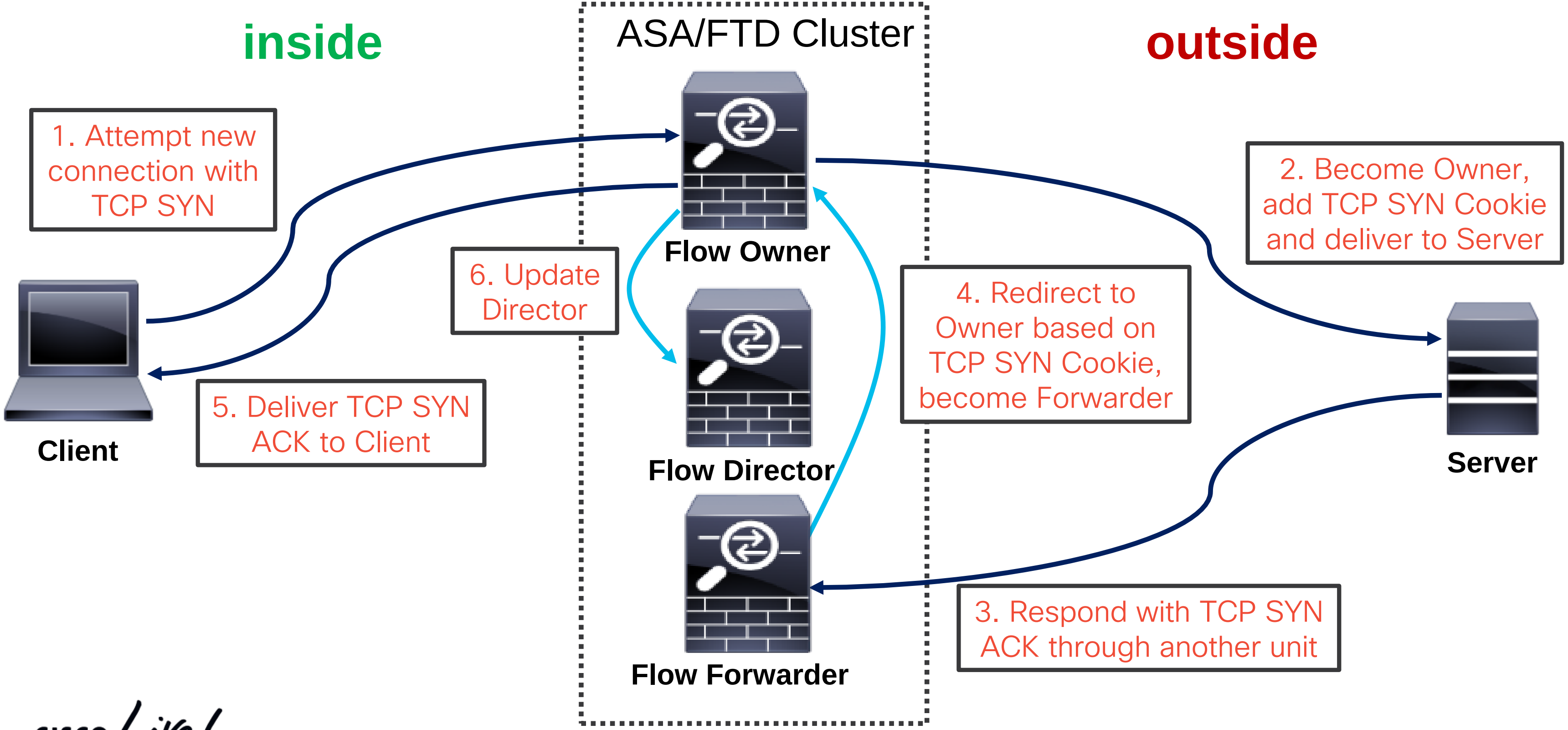
Flow Forwarder

- External stateless load-balancing does not guarantee symmetry
  - Only TCP SYN packets can reliably indicate that the connection is new
- Cluster member receiving a non-TCP-SYN packet must ask Flow Director
  - No existing connection → Drop if TCP, become Flow Owner if UDP
  - Existing connection with no Owner → Become Flow Owner
  - Existing connection with active Owner → Become Flow Forwarder
- Flow Forwarder maintains stub connection entry to avoid future lookups
  - Asymmetrically received packets are redirected to Owner via Cluster Control Link

```
ASA/slave# show conn detail
[…]
TCP inside: 192.168.103.131/52033 NP Identity Ifc: 10.8.4.10/22,
   flags  z, idle 0s, uptime 8m37s, timeout -, bytes 0,
   cluster sent/rcvd bytes 25728/0, cluster sent/rcvd total bytes 886204/0, owners (1,255)
```

Packet Flow

New TCP Connection



1. Attempt new connection with TCP SYN

2. Become Owner, add TCP SYN Cookie and deliver to Server

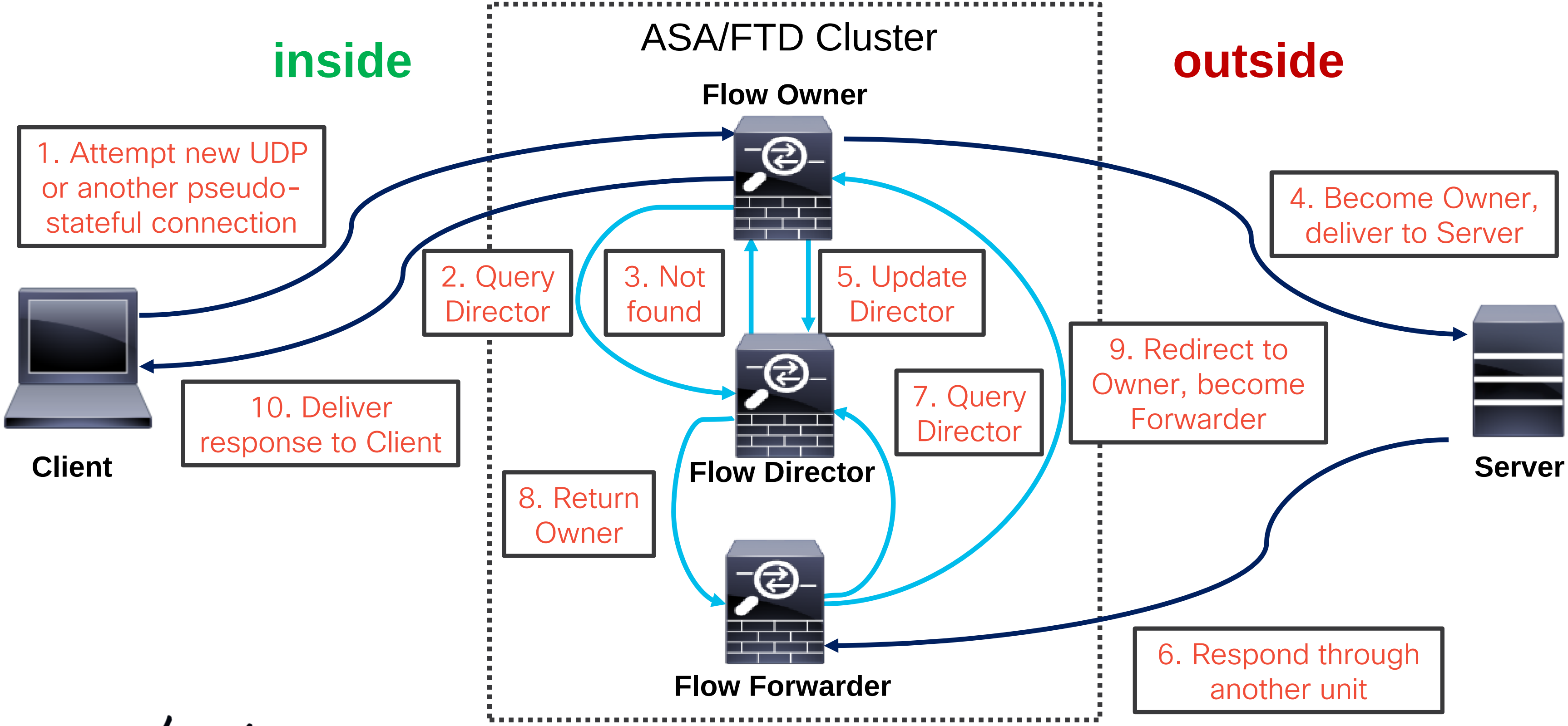
3. Respond with TCP SYN ACK through another unit

4. Redirect to Owner based on TCP SYN Cookie, become Forwarder

5. Deliver TCP SYN ACK to Client

6. Update Director

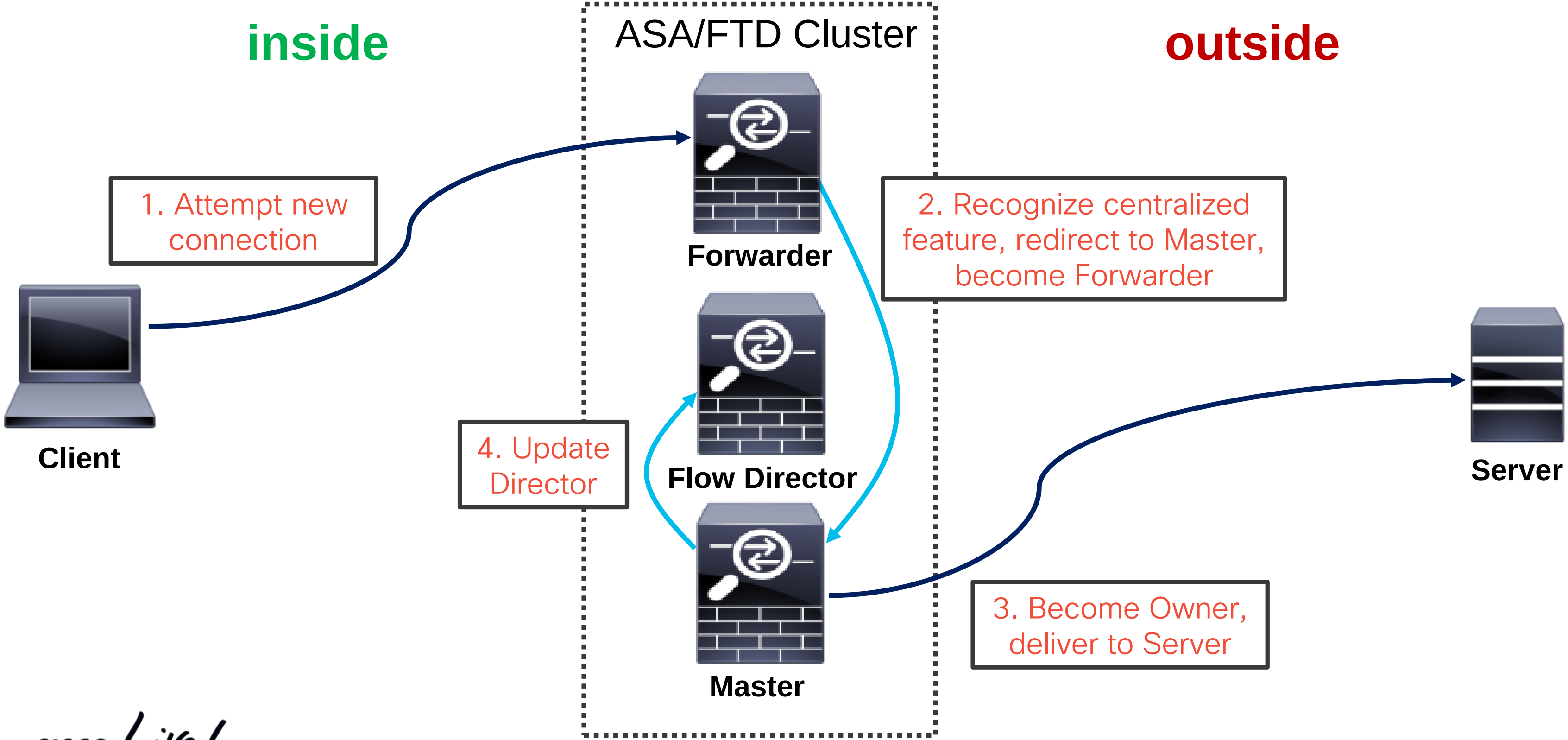
New UDP-Like Connection



inside
ASA/FTD Cluster
outside
Flow Owner
1. Attempt new UDP or another pseudo-stateful connection
2. Query Director
3. Not found
5. Update Director
4. Become Owner, deliver to Server
9. Redirect to Owner, become Forwarder
7. Query Director
10. Deliver response to Client
Client
Flow Director
Server
8. Return Owner
Flow Forwarder
6. Respond through another unit

Reference

New Centralized Connection



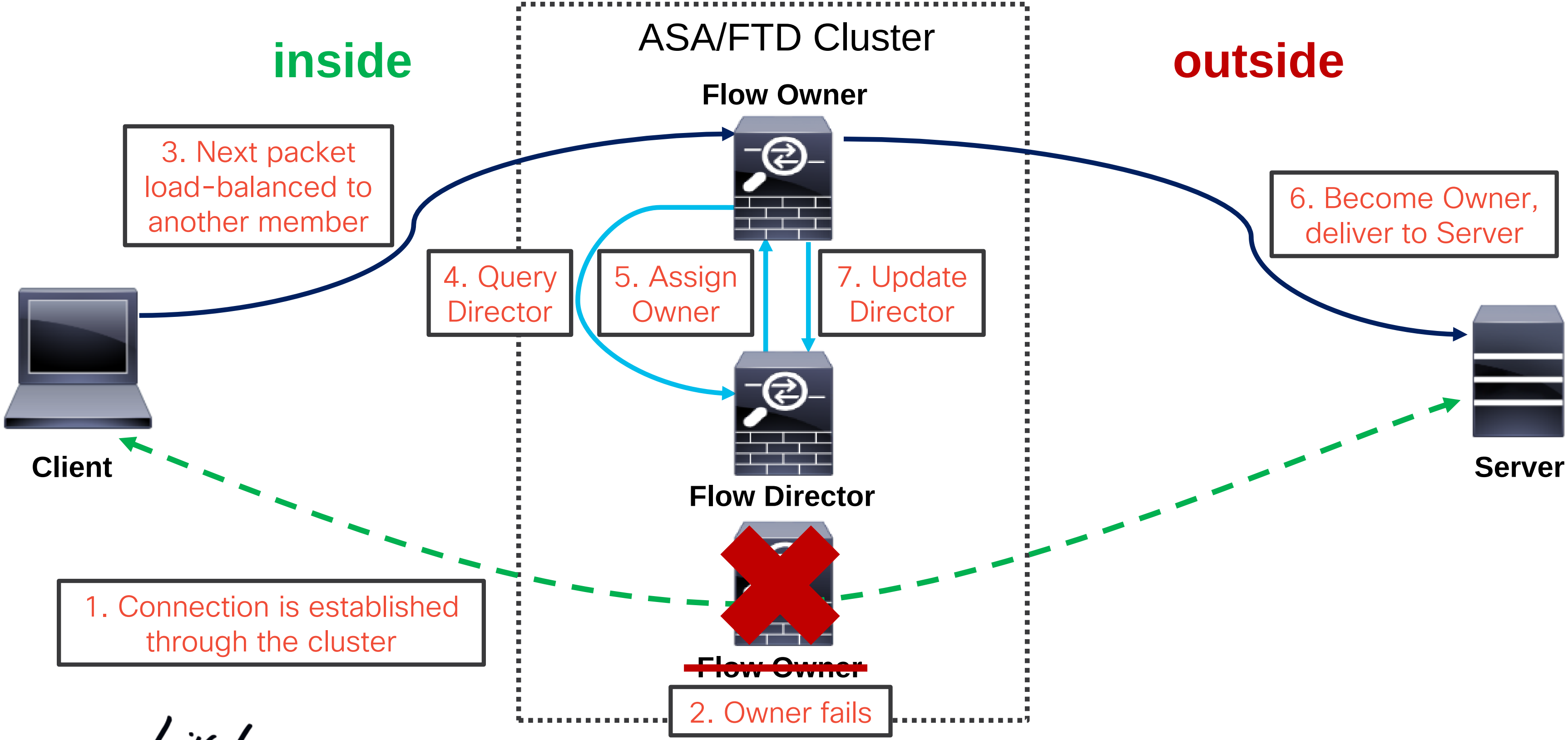
1. Attempt new connection

2. Recognize centralized feature, redirect to Master, become Forwarder

3. Become Owner, deliver to Server

4. Update Director

Owner Failure



cisco Live!

Basic Application Inspection

- Centralized
  - All packets for control and associated data connections are redirected to Master
  - Examples: ESMTP, SQLNet, TFTP
- Fully Distributed
  - Control and associated data connections are processed independently by all units
  - Examples: HTTP on ASA, FTP, GTP
- Semi Distributed
  - Control connections are processed independently by all units
  - Data connections are redirected to the associated control connections' Owners
  - Examples: SIP, SCTP, M3UA

Reference

Per-Session Port Address Translation (PAT)

- By default, dynamic PAT xlates have a 30-second idle timeout
  - Single global IP (65535 ports) allows about 2000 conn/sec for TCP and UDP
- **Per-Session Xlate** feature allows immediate reuse of the mapped port
  - Enabled by default for all TCP and DNS connections

```
ftd# show run all xlate
xlate per-session permit tcp any4 any4
xlate per-session permit tcp any4 any6
xlate per-session permit tcp any6 any4
xlate per-session permit tcp any6 any6
xlate per-session permit udp any4 any4 eq domain
xlate per-session permit udp any4 any6 eq domain
xlate per-session permit udp any6 any4 eq domain
xlate per-session permit udp any6 any6 eq domain
```

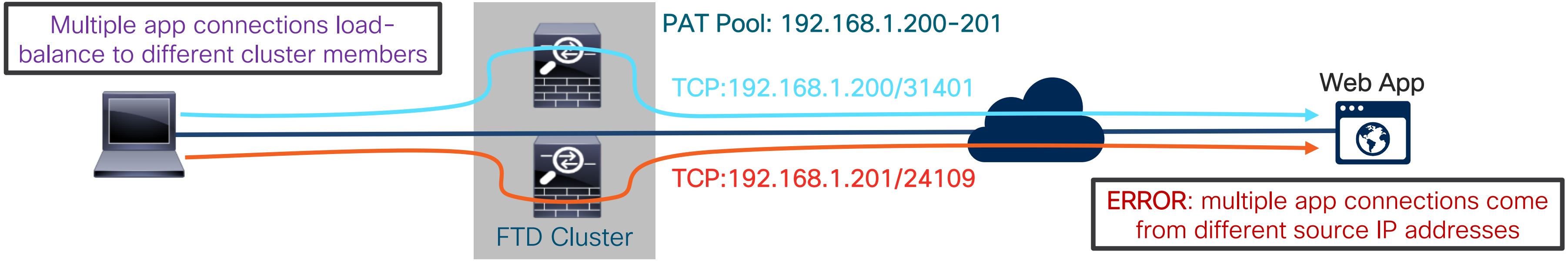
  - TCP Reset is generated to force immediate termination

Network Address Translation (NAT)

- Static NAT is performed by all cluster members based on configuration
- Master creates one-to-one Dynamic NAT xlates and replicates to Slaves
- Dynamic PAT is distributed to individual members
  - Master evenly allocates PAT addresses from the configured pools to each member
  - Provision at least as many pool IPs as cluster members to avoid centralization
  - Per-session xlates are local to the Owner with an Xlate Backup
- NAT limits clustering scalability with nearly guaranteed flow asymmetry
  - NAT and PAT pools are not advertised
  - No interface PAT or Proxy ARP in Individual mode

Distributed PAT in Clustering

- Today PAT pool is uniformly distributed to all cluster members at IP level



Multiple app connections load-balance to different cluster members

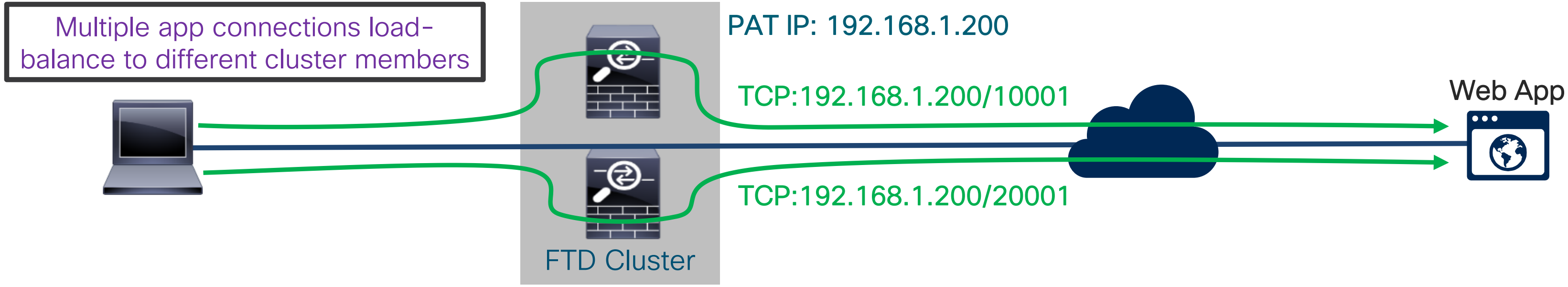
PAT Pool: 192.168.1.200-201

TCP:192.168.1.200/31401

TCP:192.168.1.201/24109

ERROR: multiple app connections come from different source IP addresses

- FTD 6.7 and ASA 9.15 will distribute each PAT pool IP at port block level



Multiple app connections load-balance to different cluster members

PAT IP: 192.168.1.200

TCP:192.168.1.200/10001

TCP:192.168.1.200/20001

Reference

Site-to-Site (S2S) IKEv2 VPN in Distributed Mode

- Supported on Firepower 9300 with ASA 9.9(1) and Carrier license only

```
asa(cfg-cluster)# vpn-mode distributed backup flat
```

- Tunnel establishment (IKEv2) is done through per-session VPN Director
- VPN Session Owner handles IPsec and clear text traffic for a single tunnel
  - Backup Owner assures uninterrupted forwarding on failure
  - Optional Remote Chassis Backup protects against full chassis failure

```
asa(cfg-cluster)# vpn-mode distributed backup remote-chassis
```

- Scalability is constrained by multiple factors
  - Concurrent S2S VPN tunnels scale at ~45% of aggregated capacity
  - Throughput impact from cleartext traffic redirection to VPN session owner
  - Runtime manual tunnel redistribution with cluster redistribute vpn-sessiondb

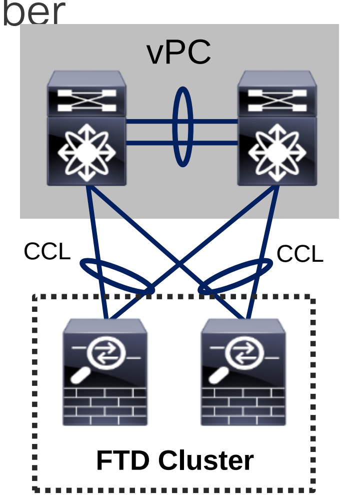
Control and Data Interfaces

Cluster Control Link (CCL)

- Carries all data and control communication between cluster members
  - Master discovery, configuration replication, keepalives, interface status updates
  - Centralized resource allocation (such as PAT/NAT, pinholes)
  - Flow Director updates and Owner queries
  - Centralized and asymmetric traffic redirection from Forwarders to Owners
- Must use same dedicated interfaces on each member
  - Separate physical interface(s), no sharing or VLAN sub-interfaces
  - An isolated non-overlapping subnet with a switch in between members
  - No packet loss or reordering; up to 10ms of one-way latency
- CCL loss forces the member out of the cluster
  - No direct back-to-back connections

CCL Best Practices

- Use a per-unit LACP Etherchannel for link redundancy and aggregation
  - Bandwidth should match maximum forwarding capacity of each member
  - 40Gbps of data traffic on Firepower 4140 AVC+IPS → 4x10GE CCL
  - Dual-connect to different physical switches in vPC/VSS
- Set MTU 100 bytes above largest data interface MTU
  - Avoids fragmentation of redirected traffic due to extra trailer
  - Minimum supported value is 1400 bytes
- Ensure that CCL switches do not verify L4 checksums
- Enable Spanning Tree Portfast and align MTU on the switch side



Data Interface Modes

- Recommended data interface mode is Spanned Etherchannel “L2”
  - Multiple physical interfaces across all members bundle into a single Etherchannel

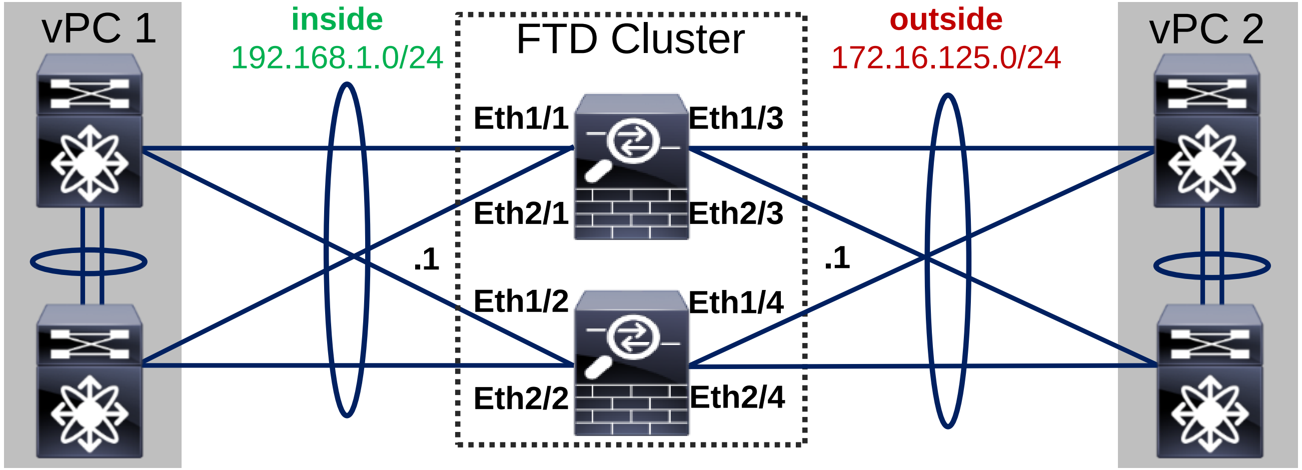
```
asa5585(config)# interface Port-Channel1
asa5585(config-if)# port-channel span-cluster
```

  - External Etherchannel load-balancing algorithm defines per-unit load
  - All units use the same virtual IP and MAC on each logical data interface
- Each member has unique IP on each data interface in Individual “L3” mode
  - Available only on ASA5500-X and ASA5585-X appliances running ASA image
  - Use Nexus ITD or PBR or dynamic routing protocols to load-balance traffic
  - Virtual IPs are owned by Master, interface IPs are assigned from configured pools

```
asa5585(config)# ip local pool INSIDE 192.168.1.2-192.168.1.17
asa5585(config-if)# interface Port-Channel1
asa5585(config-if)# ip address 192.168.1.1 255.255.255.0 cluster-pool INSIDE
```

Spanned Etherchannel Interface Mode

- Transparent and routed mode on ASA/FTD; NGIPS interfaces in FTD
- Must use Etherchannels: “firewall-on-a-stick” VLAN trunk or separate
- Use symmetric Etherchannel hashing algorithm with different switches
- Seamless load-balancing and unit addition/removal with cLACP



Clustering LACP (cLACP)

- Spanned Etherchannel is preferred for data interfaces on ASA appliances
  - Up to 32 (16 per unit) active total links with global static port priorities

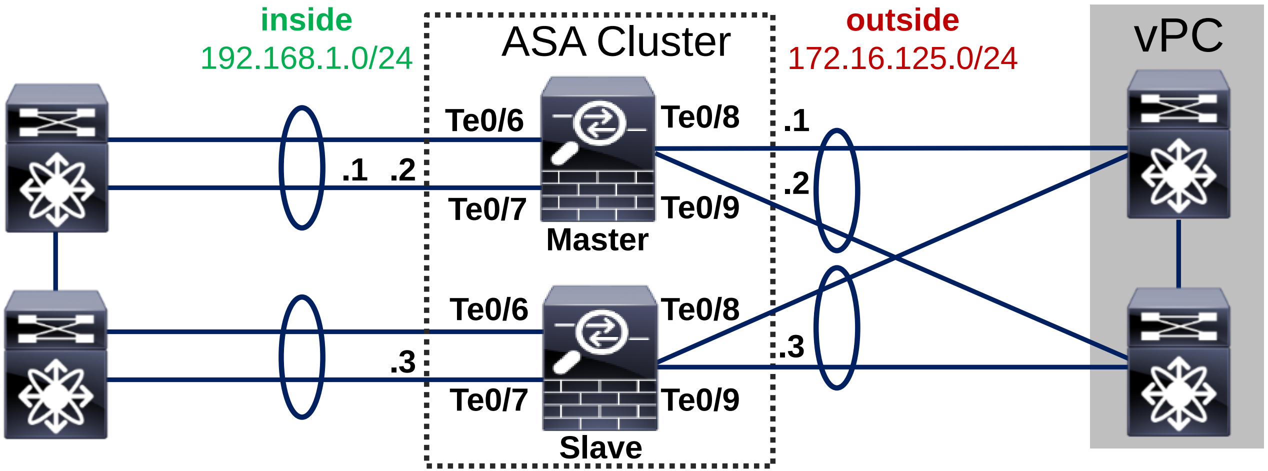
```
asa(config)# cluster group DC_ASA
asa(cfg-cluster)# clacp static-port-priority
```

  - Disable LACP Graceful Convergence and Adaptive Hash on adjacent NX-OS
- Supervisor bundles data and CCL interfaces on Firepower 4100 and 9300
  - Spanned Etherchannel only with up to 32 active total (up to 16 per chassis) links
  - Disable only Adaptive Hash on adjacent NX-OS
- Always configure virtual MAC for each data Etherchannel to avoid instability
- cLACP assumes a Spanned Etherchannel connects to one logical switch
  - LACP actor IDs between member ports are not strictly enforced, allowing creativity

Reference

Individual Interface Mode

- Not supported on Firepower 4100 or 9300; routed ASA only elsewhere
- Master owns virtual IP on data interfaces for management purposes only
- All members get data interface IPs from the pools in the order of admission
- Per-unit Etherchannel support up to 16 members



Reference

Traffic Load Balancing in Individual Mode

- Each unit has a separate IP/MAC address pair on its data interfaces
  - Traffic load-balancing is not as seamless as with Spanned Etherchannel mode
- Policy Based Routing (PBR) with route maps is very static by definition
  - Simple per-flow hashing or more elaborate distribution using ACLs
  - Difficult to direct return connections with NAT/PAT
  - Must use SLA with Object Tracking to detect unit addition and removal
  - Nexus Intelligent Traffic Director (ITD) simplifies configuration process
- Dynamic routing with Equal Cost Multi Path (ECMP)
  - Per-flow hashing with no static configuration
  - Easier to detect member addition and removal
  - Preferred approach with some convergence caveats

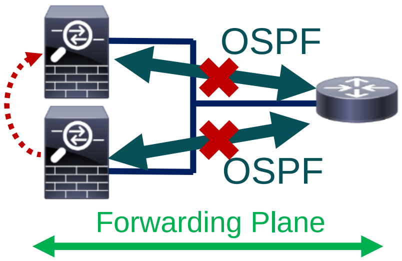
Dynamic Routing

- Master unit runs dynamic routing in Spanned Etherchannel mode
  - RIP, EIGRP, OSPFv2, OSPFv3, BGP-4 (IPv4 and IPv6), PIM
  - Routing and ARP tables are synchronized to other members, like in failover
  - Possible external convergence impact only on Master failure
- Each member forms independent adjacencies in Individual mode
  - Same protocols as in Spanned Etherchannel, but multicast data is centralized
  - Higher overall processing impact from maintaining separate routing tables
  - Slower external convergence on any member failure

Non Stop Forwarding (NSF)

- Routing Information Base (RIB) is replicated in Spanned Etherchannel mode
  - Master establishes dynamic routing adjacencies and keeps Slaves up-to-date
  - When Master fails, the cluster continues traffic forwarding based on RIB
  - New Master re-establishes the dynamic routing adjacencies and updates the RIB
  - Adjacent routers flush routes and cause momentary traffic blackholing
- Non Stop Forwarding (NSF) and Graceful Restart (GR) avoid blackholing

1. Cluster Master fails; new Master initiates adjacency with the peer router indicating that traffic forwarding should continue.



2. Router re-establishes adjacency with Master while retaining the stale routes; these routes are refreshed when the adjacency reestablishes.

3. Primary Route Processor undergoes a restart, signals the peer cluster to continue forwarding while the backup re-establishes adjacencies.

4. FTD/ASA cluster continues normal traffic forwarding until the primary RP restarts or the backup takes over or the timeout expires.

Reference

NSF and GR Configuration on ASA

- Feature has to be enabled on all adjacent devices to work
- Use Cisco with all Cisco peers (default) or IETF NSF for third-party in OSPFv2

```
router ospf 1
 nsf cisco enforce-global
nsf cisco helper
```

(Optional) Disable NSF if any adjacent device is

(Default) Help other NSF devices restart gracefully.

```
router ospf 1
 nsf ietf restart-interval 260
 nsf ietf helper strict-lsa-checking
```

Default graceful restart time is 120 seconds.

(Optional) Helper aborts peer's NSF restart on impactful LSA changes

- Common Graceful Restart configuration for OSPFv3

```
router ospf 1
 graceful-restart restart-interval 180
 graceful-restart helper strict-lsa-checking
```

- BGPv4 Graceful Restart is enabled globally and configured for each neighbor

```
! System Context
router bgp 65001
 bgp graceful-restart restart-time 180 stalepath-time 720
! Context A
router bgp 65001
 address-family ipv4 unicast
  neighbor 192.168.1.101 ha-mode graceful-restart
```

Default maximum wait time for a restarting peer is 120 seconds.

Default wait time before flushing routes toward a GR capable peer is 360 seconds.

Enable GR for each neighbor.

cisco Live!

Reference

Faster Dynamic Routing Convergence on ASA

- Reduce protocol timers on **all adjacent segments** to improve convergence
  - OSPF timers **must** match between peers
  - **Do not** lower dead interval in Spanned Etherchannel mode with NSF/GR
- **ASA 9.1 and earlier** software uses higher minimum timers

```
asa(config)# interface GigabitEthernet0/0
asa(config-if)# ospf hello-interval 1
asa(config-if)# ospf dead-interval 3
asa(config-if)# router ospf 1
asa(config-router)# timers spf 1 1
```

Generate OSPF hello packets every 1 second

Declare neighbor dead with no hello packets for 3 seconds

Delay before and between SPF calculations for 1 second

- **ASA 9.2(1)+** provides faster convergence

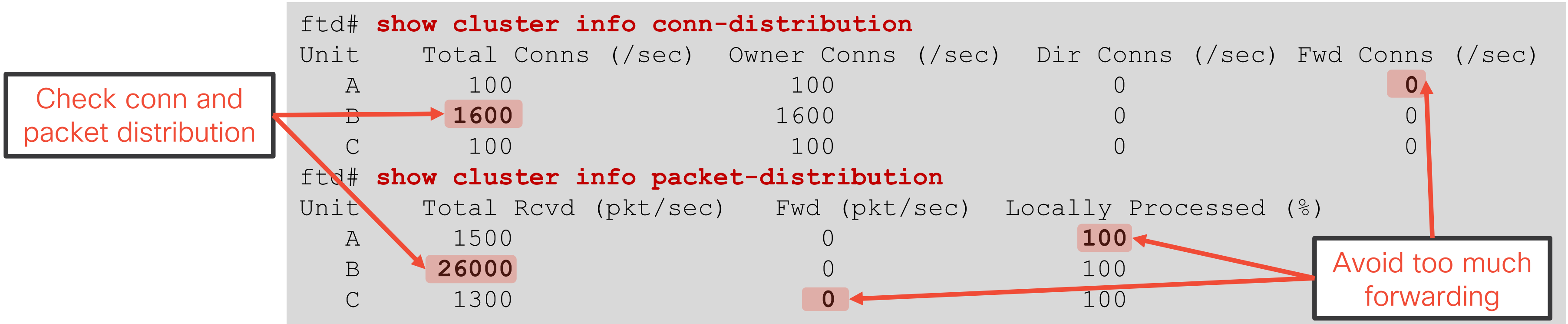
```
asa(config)# interface GigabitEthernet0/0
asa(config-if)# ospf dead-interval minimal hello-multiplier 3
asa(config-if)# router ospf 1
asa(config-router)# timers throttle spf 500 1000 5000
```

Generate 3 OSPF FastHello packets per second; 1 second to detect a dead neighbor

Delay SPF calculation by 500 ms, delay between calculations for 1 second and no more than 5 seconds

Verifying Load Distribution

- Uneven Owner connection distribution implies a load-balancing issue
  - Use a more granular Etherchannel hashing algorithm on connected switches
- High Forwarder connection count implies flow asymmetry
  - Always match Etherchannel hashing algorithms between all connected switches
  - Cannot avoid asymmetry with NAT/PAT



```
ftd# show cluster info conn-distribution
Unit     Total Conns (/sec)   Owner Conns (/sec)   Dir Conns (/sec)  Fwd Conns (/sec)
   A          100                   100                  0                  0
   B         1600                  1600                  0                  0
   C          100                   100                  0                  0
ftd# show cluster info packet-distribution
Unit     Total Rcvd (pkt/sec)    Fwd (pkt/sec)   Locally Processed (%)
   A         1500                      0               100
   B        26000                      0               100
   C         1300                      0               100
```

Check conn and packet distribution

Avoid too much forwarding

Cluster Management

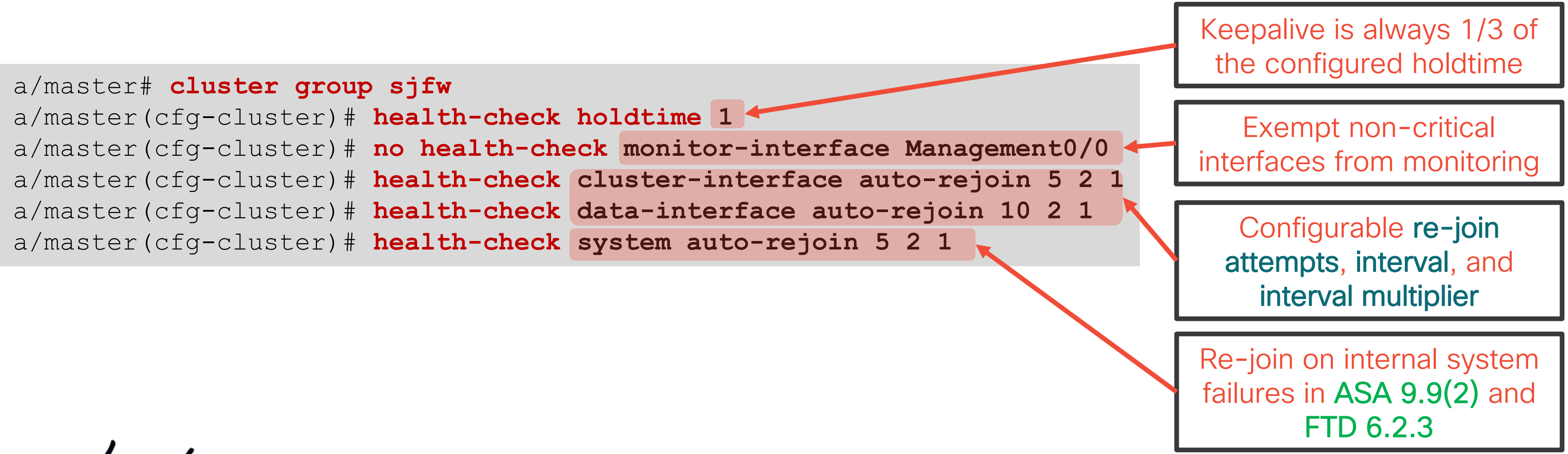
- Dedicated management interface is required on FTD and preferred on ASA
  - SNMP typically requires per-unit IP, syslog/NSEL can share IP on a data interface
  - management-only allows MAC/IP pools in Spanned Etherchannel mode on ASA
- A regular data interface can be used for managing an ASA cluster in-band
  - Connecting to cluster data interface IP always reaches the master
- Use cluster exec for non-configuration commands on some/all members

```
asa/master# cluster exec show version | include Serial
A(LOCAL):*************************************************************
Serial Number: JAF1434AERL

B:********************************************************************
Serial Number: JAF1511ABFT
```

Health Monitoring

- A unit shuts down all data interfaces and disables clustering on CCL failure
- Each member generates keepalives on CCL every 1 second by default
  - Master removes a unit from the cluster after 3 missed keepalives (holdtime)
  - Member leaves cluster if its interface/SSP is down and another member has it up
  - Rejoin attempted 3 times (after 5, 10, 20 minutes), then the unit disables clustering



```
a/master# cluster group sjfw
a/master(cfg-cluster)# health-check holdtime 1
a/master(cfg-cluster)# no health-check monitor-interface Management0/0
a/master(cfg-cluster)# health-check cluster-interface auto-rejoin 5 2 1
a/master(cfg-cluster)# health-check data-interface auto-rejoin 10 2 1
a/master(cfg-cluster)# health-check system auto-rejoin 5 2 1
```

Keepalive is always 1/3 of the configured holdtime

Exempt non-critical interfaces from monitoring

Configurable re-join attempts, interval, and interval multiplier

Re-join on internal system failures in ASA 9.9(2) and FTD 6.2.3

Configuring Clustering

Preparation Checklist for ASA Appliances

- Get serial console access to all future cluster members
- Clear the existing configuration and configure appropriate boot images
- Switch to the multiple-context mode if desired
- Install Cluster (ASA5580/5585-X) and matching 3DES/10GE I/O licenses
- Designate a dedicated management interface (same on all members)
- Designate one or more physical interfaces per unit for CCL
- Assign an isolated subnet for CCL on a separate switch or VDC
- Configure jumbo-frame reservation command and reload each ASA
- Pick Spanned Etherchannel or Individual interface mode for entire cluster

Reference

Setting Interface Mode on ASA Appliances

- Use cluster interface-mode command before configuring clustering
  - The running configuration is checked for incompatible commands
  - Interface mode setting is stored outside of the startup configuration
  - Use show cluster interface-mode to check current mode
  - Use no cluster interface-mode to return to standalone mode
- Clearing interface configuration and reloading each ASA is recommended
  - You can display the list of conflicts and resolve them manually

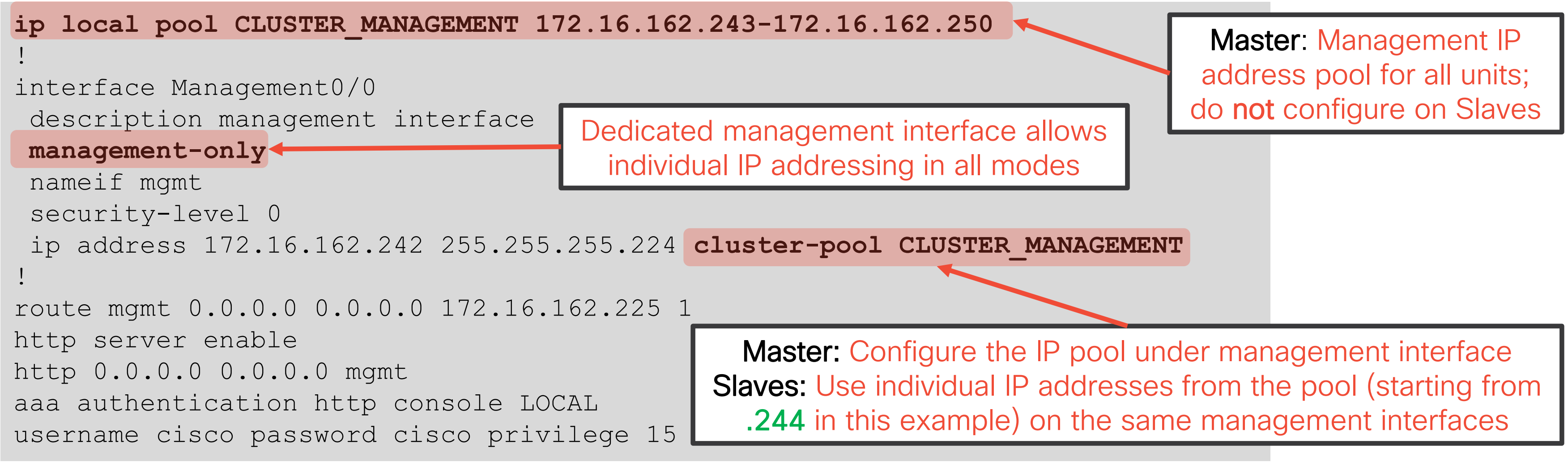
```
asa(config)# cluster interface-mode spanned check-details
ERROR: Please modify the following configuration elements that are incompatible with
'spanned' interface-mode.
 - Interface Gi0/0 is not a span-cluster port-channel interface, Gi0/0(outside) cannot
be used as data interface when cluster interface-mode is 'spanned'.
```

  - It is not recommended to bypass the check and force the mode change

Reference

Management Access to ASA Appliances

- ASDM High Availability and Scalability Wizard simplifies deployment
  - Only set the interface mode on Master, then add Slaves automatically over HTTPS
  - Requires basic management connectivity to all members



```
ip local pool CLUSTER_MANAGEMENT 172.16.162.243-172.16.162.250
!
interface Management0/0
 description management interface
 management-only
 nameif mgmt
 security-level 0
 ip address 172.16.162.242 255.255.255.224 cluster-pool CLUSTER_MANAGEMENT
!
route mgmt 0.0.0.0 0.0.0.0 172.16.162.225 1
http server enable
http 0.0.0.0 0.0.0.0 mgmt
aaa authentication http console LOCAL
username cisco password cisco privilege 15
```

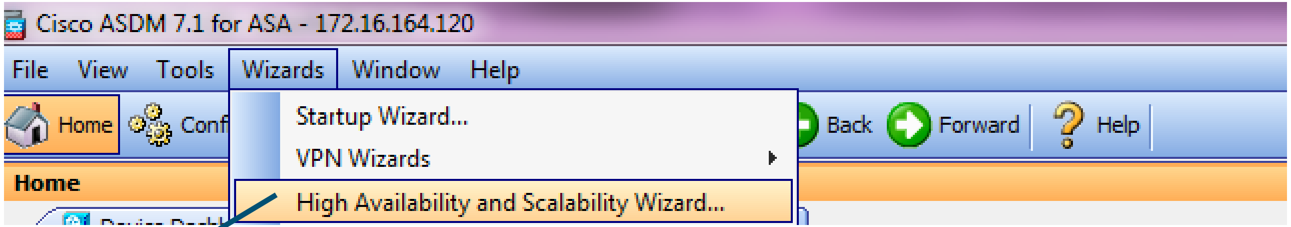
Master: Management IP address pool for all units; do **not** configure on Slaves

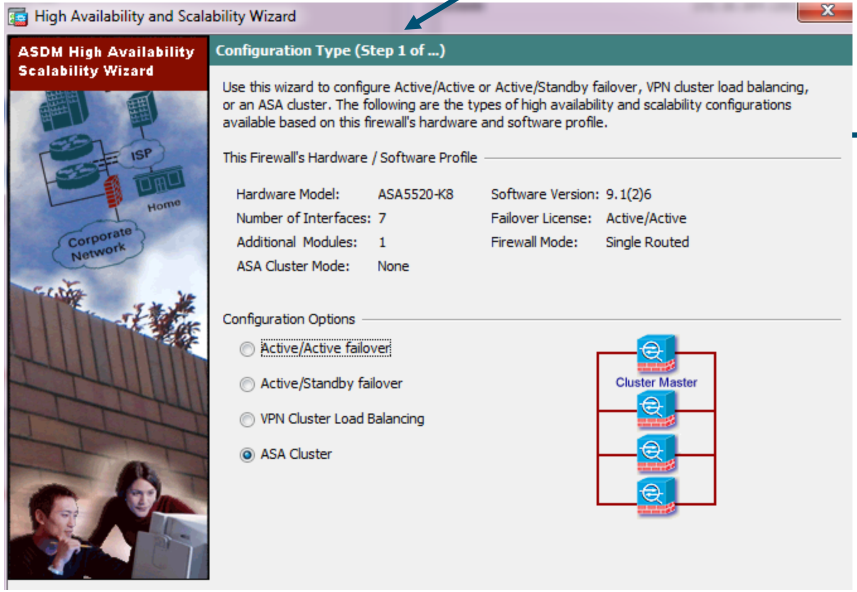
Dedicated management interface allows individual IP addressing in all modes

Master: Configure the IP pool under management interface
Slaves: Use individual IP addresses from the pool (starting from .244 in this example) on the same management interfaces

Reference

ASDM Wizard




High Availability and Scalability Wizard
ASDM High Availability Scalability Wizard
ISP
Home
Corporate Network

Configuration Type (Step 1 of ...)

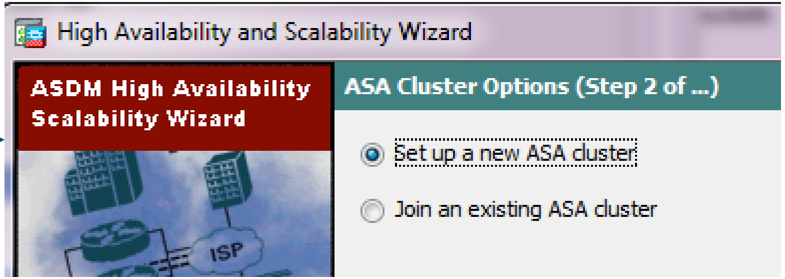
Use this wizard to configure Active/Active or Active/Standby failover, VPN cluster load balancing, or an ASA cluster. The following are the types of high availability and scalability configurations available based on this firewall's hardware and software profile.

This Firewall's Hardware / Software Profile

Hardware Model: ASA5520-K8
Number of Interfaces: 7
Additional Modules: 1
ASA Cluster Mode: None
Software Version: 9.1(2)6
Failover License: Active/Active
Firewall Mode: Single Routed

Configuration Options

○ Active/Active failover
○ Active/Standby failover
○ VPN Cluster Load Balancing
● ASA Cluster


High Availability and Scalability Wizard
ASDM High Availability Scalability Wizard
ISP

ASA Cluster Options (Step 2 of ...)

● Set up a new ASA cluster
○ Join an existing ASA cluster

Fully configure Master in 4 easy steps, then have ASDM add Slaves one by one over basic HTTPS management connection.

... or use good old CLI ;-)

Reference

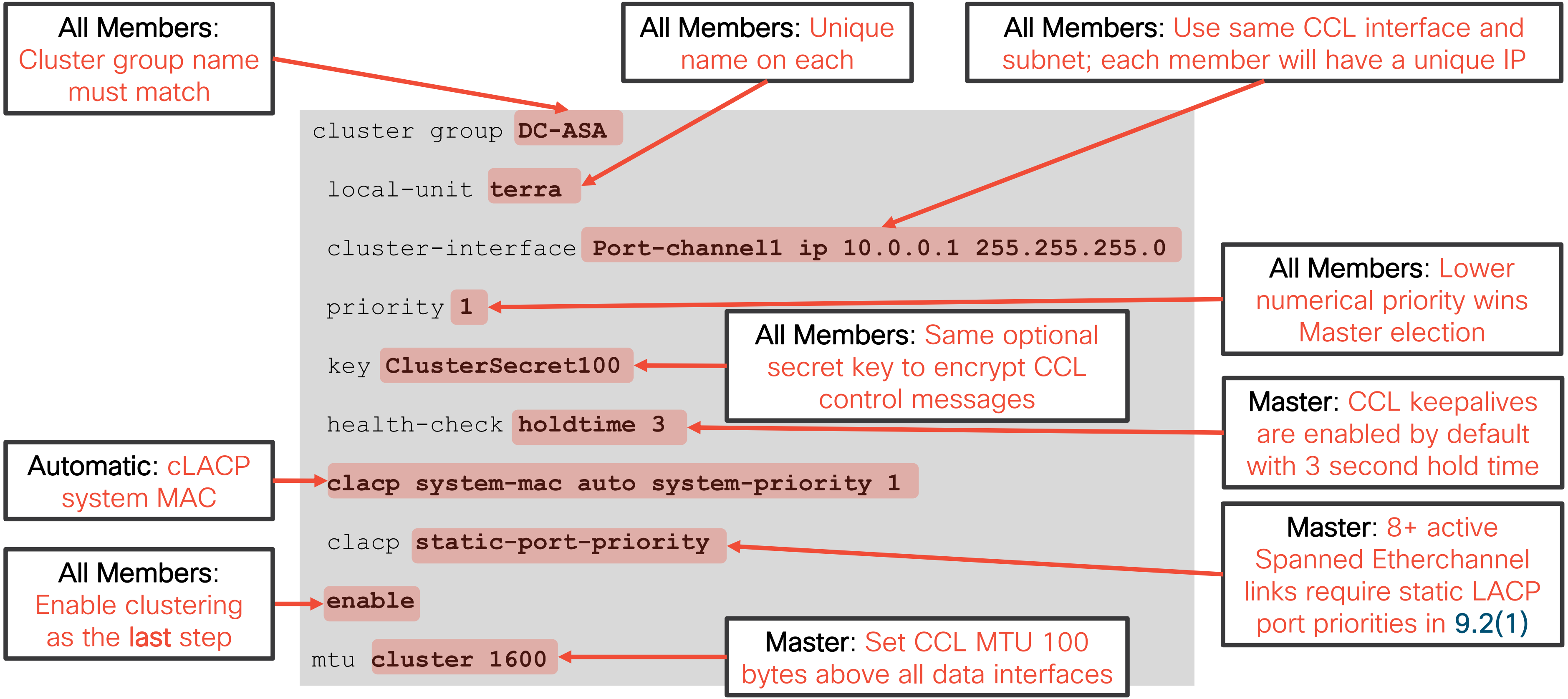
ASA CLI: CCL Etherchannel

- Create an Etherchannel interface for CCL on each member separately
  - Same physical interface members across all units
  - Use LACP for quicker failure detection or static on mode for less complexity
  - Use system context in the multiple-context mode
  - Connect one physical interface to each logical switch in VSS/vPC

```
ciscoasa(config)# interface TenGigabitEthernet 0/6
ciscoasa(config-if)# channel-group 1 mode on
INFO: security-level, delay and IP address are cleared on TenGigabitEthernet0/6.
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface TenGigabitEthernet 0/7
ciscoasa(config-if)# channel-group 1 mode on
INFO: security-level, delay and IP address are cleared on TenGigabitEthernet0/7.
ciscoasa(config-if)# no shutdown
```

Reference

ASA CLI: Cluster Group



```
cluster group DC-ASA
 local-unit terra
 cluster-interface Port-channel1 ip 10.0.0.1 255.255.255.0
 priority 1
 key ClusterSecret100
 health-check holdtime 3
 clacp system-mac auto system-priority 1
 clacp static-port-priority
 enable
mtu cluster 1600
```

All Members: Cluster group name must match

All Members: Unique name on each

All Members: Use same CCL interface and subnet; each member will have a unique IP

All Members: Lower numerical priority wins Master election

All Members: Same optional secret key to encrypt CCL control messages

Master: CCL keepalives are enabled by default with 3 second hold time

Automatic: cLACP system MAC

Master: 8+ active Spanned Etherchannel links require static LACP port priorities in 9.2(1)

All Members: Enable clustering as the last step

Master: Set CCL MTU 100 bytes above all data interfaces

Reference

ASA CLI: Data Interfaces on Master

Spanned Etherchannel Mode

```
interface TenGigabitEthernet0/8
 channel-group 20 mode active
interface TenGigabitEthernet0/9
 channel-group 20 mode active
interface Port-channel20
 port-channel span-cluster
 mac-address 0001.000a.0001
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
```

Up to 32 ports with cLACP in 9.2(1)

Spanned Etherchannel bundles ports across entire cluster

Virtual MAC is required for Etherchannel stability

Single virtual IP for all members

Individual Mode

```
ip local pool INSIDE 10.1.1.2-10.1.1.17
interface TenGigabitEthernet0/8
 channel-group 20 mode active
interface TenGigabitEthernet0/9
 channel-group 20 mode active
interface Port-channel20
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0 cluster-pool INSIDE
```

Every member bundles a separate Etherchannel

Up to 16 ports with LACP in 9.2(1)

Traffic load-balanced to each member based on individually assigned IP addresses from the pool

Virtual IP is owned by Master for management only

Reference

ASA CLI: Adding Slave Units

- Verify that the Master is operational before adding Slave members

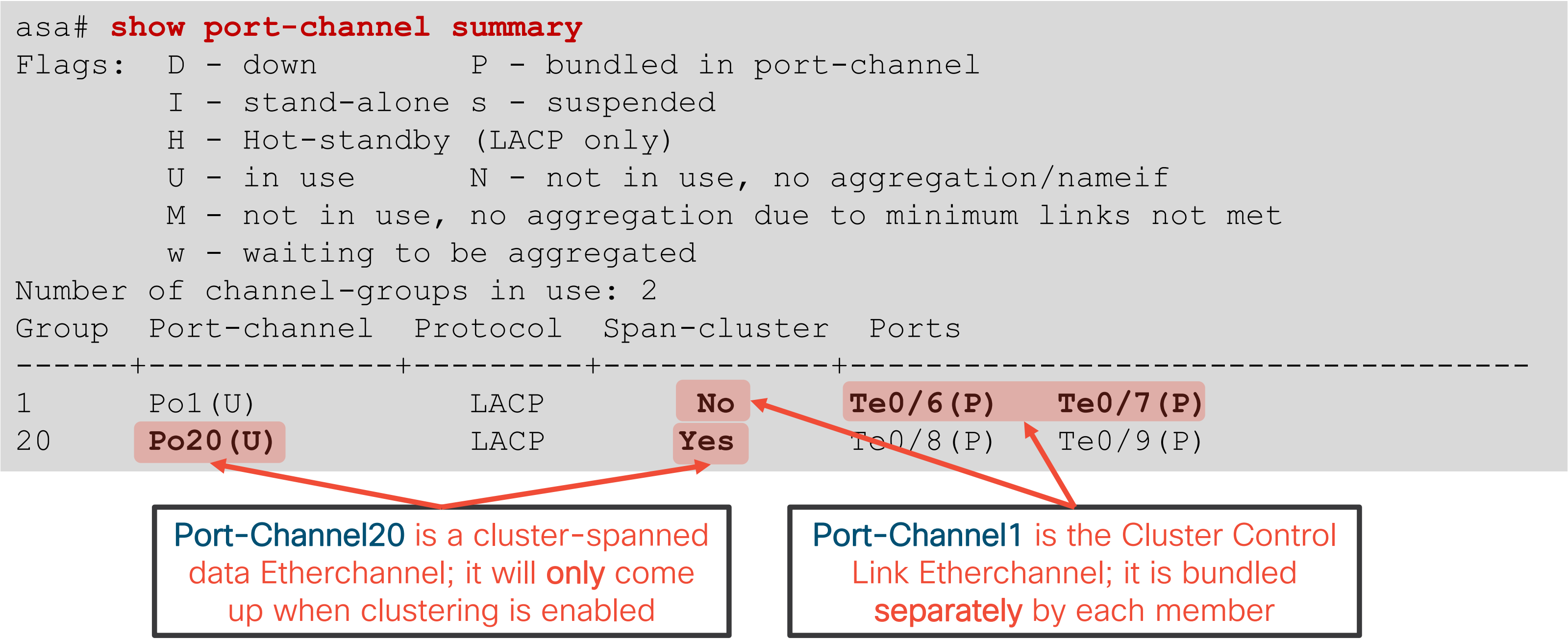
```
asa# show cluster info
Cluster DC-ASA: On
    Interface mode: spanned
    This is “terra" in state MASTER
        ID          : 1
        Version     : 9.1(3)
        Serial No.: JAF1511ABFT
        CCL IP      : 10.0.0.1
        CCL MAC     : 5475.d05b.26f2
        Last join : 17:20:24 UTC Sep 26 2013
        Last leave: N/A
```

- Add one Slave at a time by configuring the cluster group

```
cluster group DC-ASA
 local-unit sirius
 cluster-interface Port-channel1 ip 10.0.0.2 255.255.255.0
 priority 100
 key ClusterSecret100
 enable
```

ASA: Spanned Etherchannel Verification

- Each cluster member shows only local Etherchannel member ports



```
asa# show port-channel summary
Flags:  D - down          P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        U - in use        N - not in use, no aggregation/nameif
        M - not in use, no aggregation due to minimum links not met
        w - waiting to be aggregated
Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
------+-------------+---------+------------+------------------------------------
1      Po1(U)           LACP          No      Te0/6(P)    Te0/7(P)
20     Po20(U)          LACP         Yes      Te0/8(P)    Te0/9(P)
```

Port-Channel20 is a cluster-spanned data Etherchannel; it will **only** come up when clustering is enabled

Port-Channel1 is the Cluster Control Link Etherchannel; it is bundled **separately** by each member

Reference

Clustering on Firepower 4100 and 9300

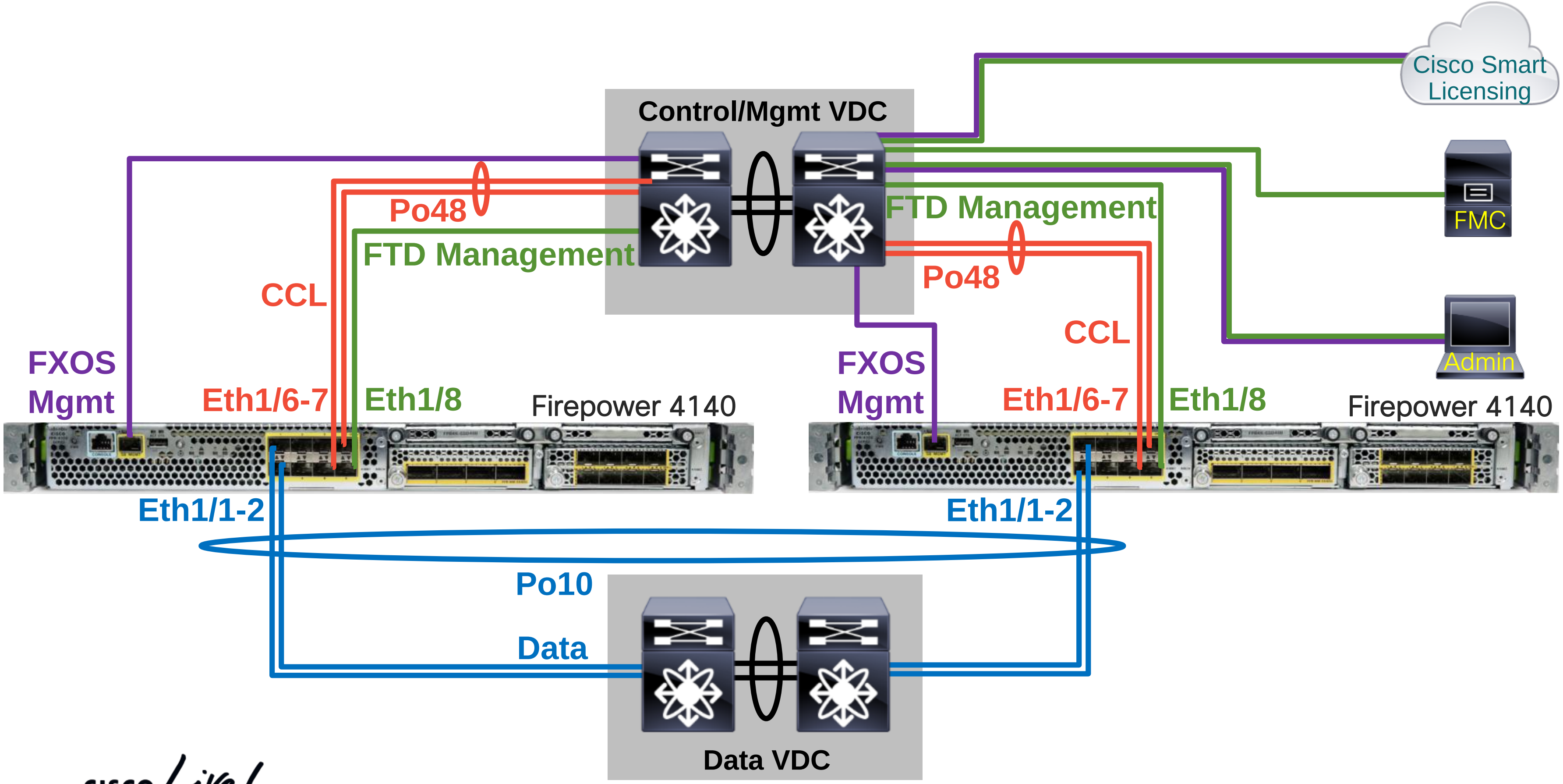
- Only Spanned Etherchannel interface mode is supported
- Supervisor pushes cluster configuration during logical device deployment
    - Site ID for inter-site clustering is optional
    - Firewall context mode and TLS/SSL ciphers are replicated in ASA
- Remote flow backup for N+1 chassis fault tolerance on Firepower 9300
- Module- and chassis-level overflow warning syslogs

```
%ASA-6-748008: CPU load 80% of module 1 in chassis 1 (unit-1-1) exceeds overflow
protection threshold CPU 75%. System may be oversubscribed on member failure.
%ASA-6-748009: Memory load 80% of chassis 1 exceeds overflow protection threshold
memory 78%. System may be oversubscribed on chassis failure.
```

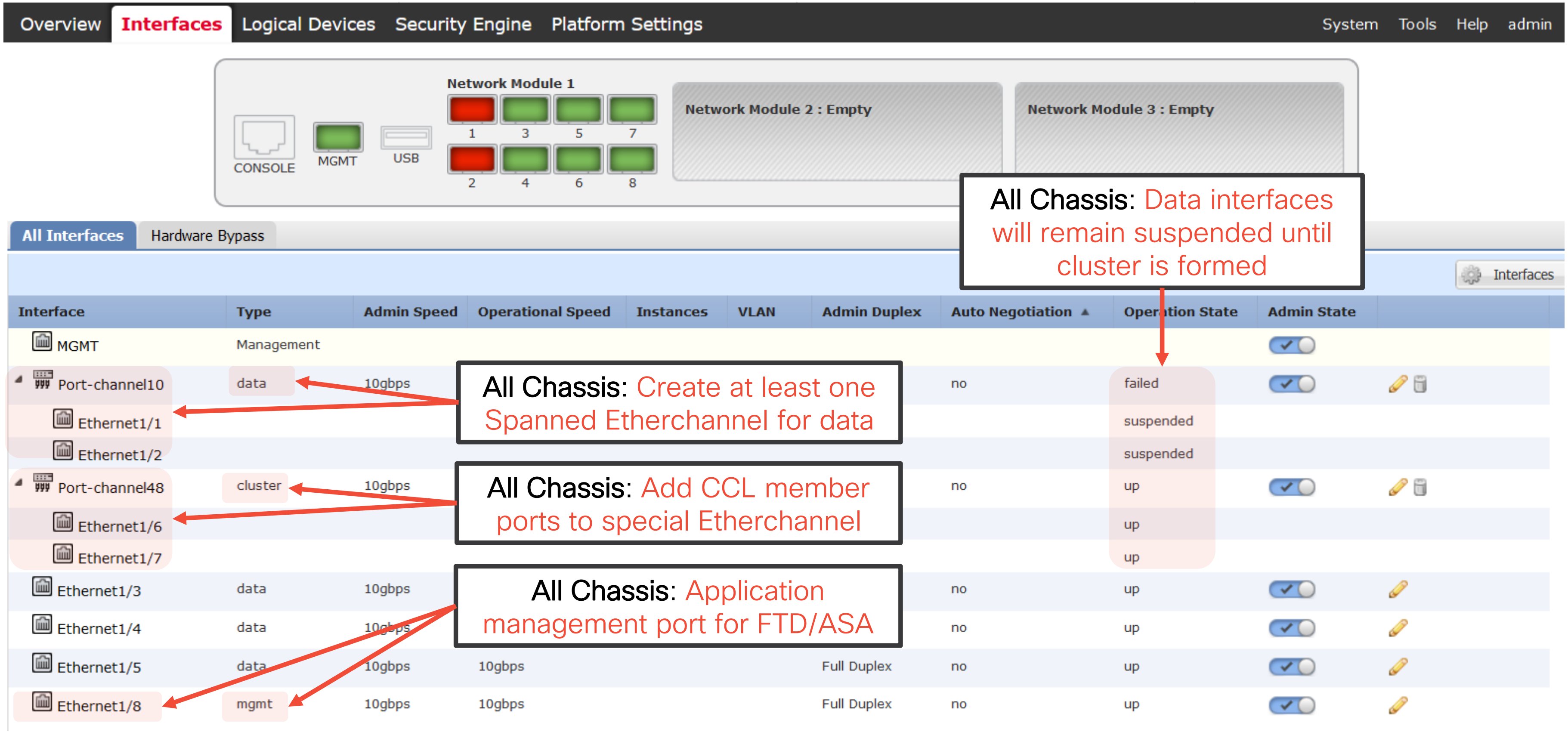
Preparation Checklist for Firepower Appliances

- Set up and cable identical Firepower chassis and modules for the cluster
- Ensure over-the-network Supervisor management access
- Bring up Firepower Management Center for FTD
- Generate device token and enable Smart Licensing on chassis and/or FMC
- Delete all pre-existing logical devices from the chassis
- Download application images for FTD or ASA
- Designate a dedicated application management interface (one per chassis)
- Designate one or more physical interfaces per chassis for CCL
- Assign an isolated subnet for CCL on a separate switch or VDC

Sample FTD Cluster Deployment Topology



Chassis Manager: Interface Configuration



Interface	Type	Admin Speed	Operational Speed	Instances	VLAN	Admin Duplex	Auto Negotiation ▲	Operation State	Admin State	
MGMT	Management								✓	
Port-channel10	data	10gbps					no	failed	✓	✎ 🗑
Ethernet1/1								suspended		
Ethernet1/2								suspended		
Port-channel48	cluster	10gbps					no	up	✓	✎ 🗑
Ethernet1/6								up		
Ethernet1/7								up		
Ethernet1/3	data	10gbps					no	up	✓	✎
Ethernet1/4	data	10gbps					no	up	✓	✎
Ethernet1/5	data	10gbps	10gbps			Full Duplex	no	up	✓	✎
Ethernet1/8	mgmt	10gbps	10gbps			Full Duplex	no	up	✓	✎

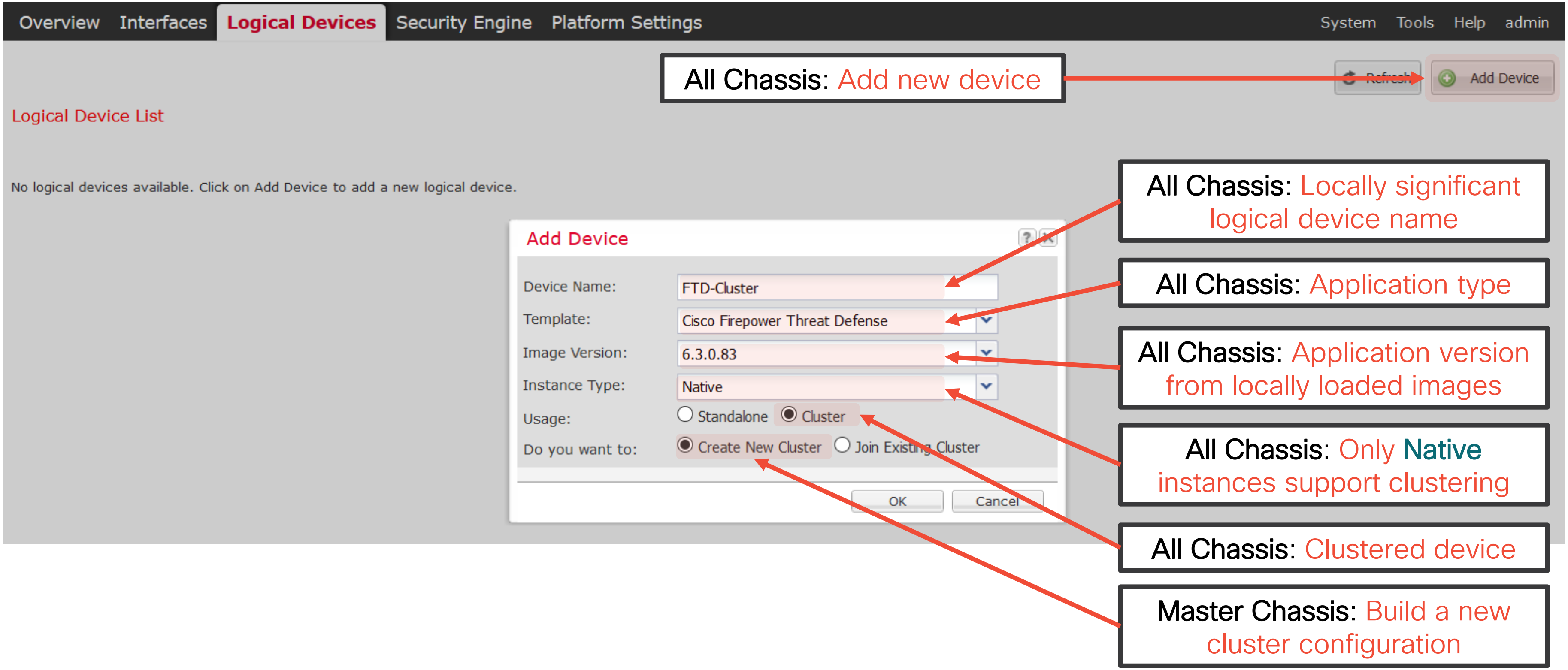
All Chassis: Data interfaces will remain suspended until cluster is formed

All Chassis: Create at least one Spanned Etherchannel for data

All Chassis: Add CCL member ports to special Etherchannel

All Chassis: Application management port for FTD/ASA

Chassis Manager: Add Logical Device



Logical Device List

No logical devices available. Click on Add Device to add a new logical device.

Add Device

Device Name: FTD-Cluster

Template: Cisco Firepower Threat Defense

Image Version: 6.3.0.83

Instance Type: Native

Usage: ○ Standalone ● Cluster

Do you want to: ● Create New Cluster ○ Join Existing Cluster

All Chassis: Add new device

All Chassis: Locally significant logical device name

All Chassis: Application type

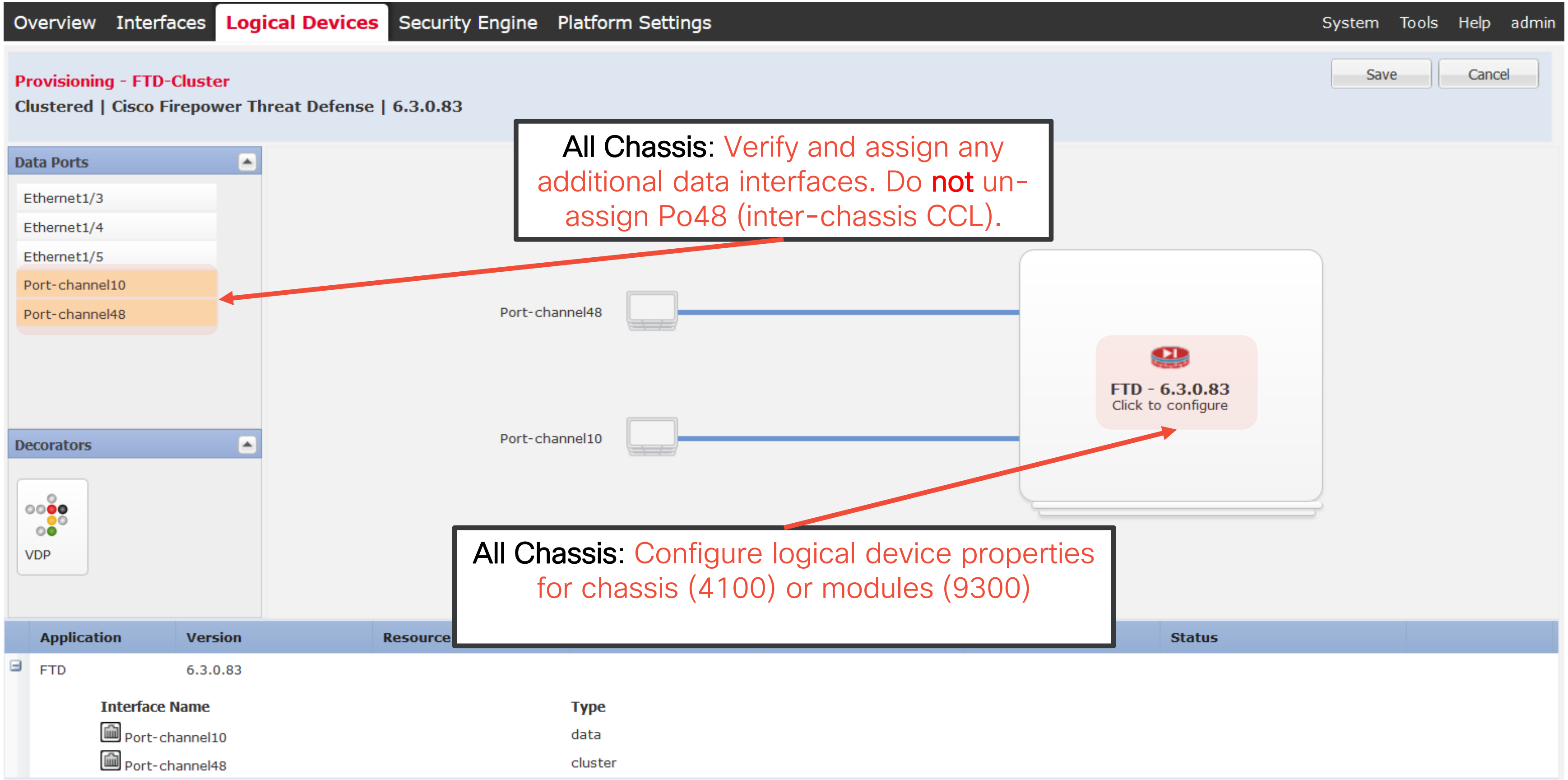
All Chassis: Application version from locally loaded images

All Chassis: Only Native instances support clustering

All Chassis: Clustered device

Master Chassis: Build a new cluster configuration

Chassis Manager: FTD Interface Assignment



Provisioning - FTD-Cluster

Clustered | Cisco Firepower Threat Defense | 6.3.0.83

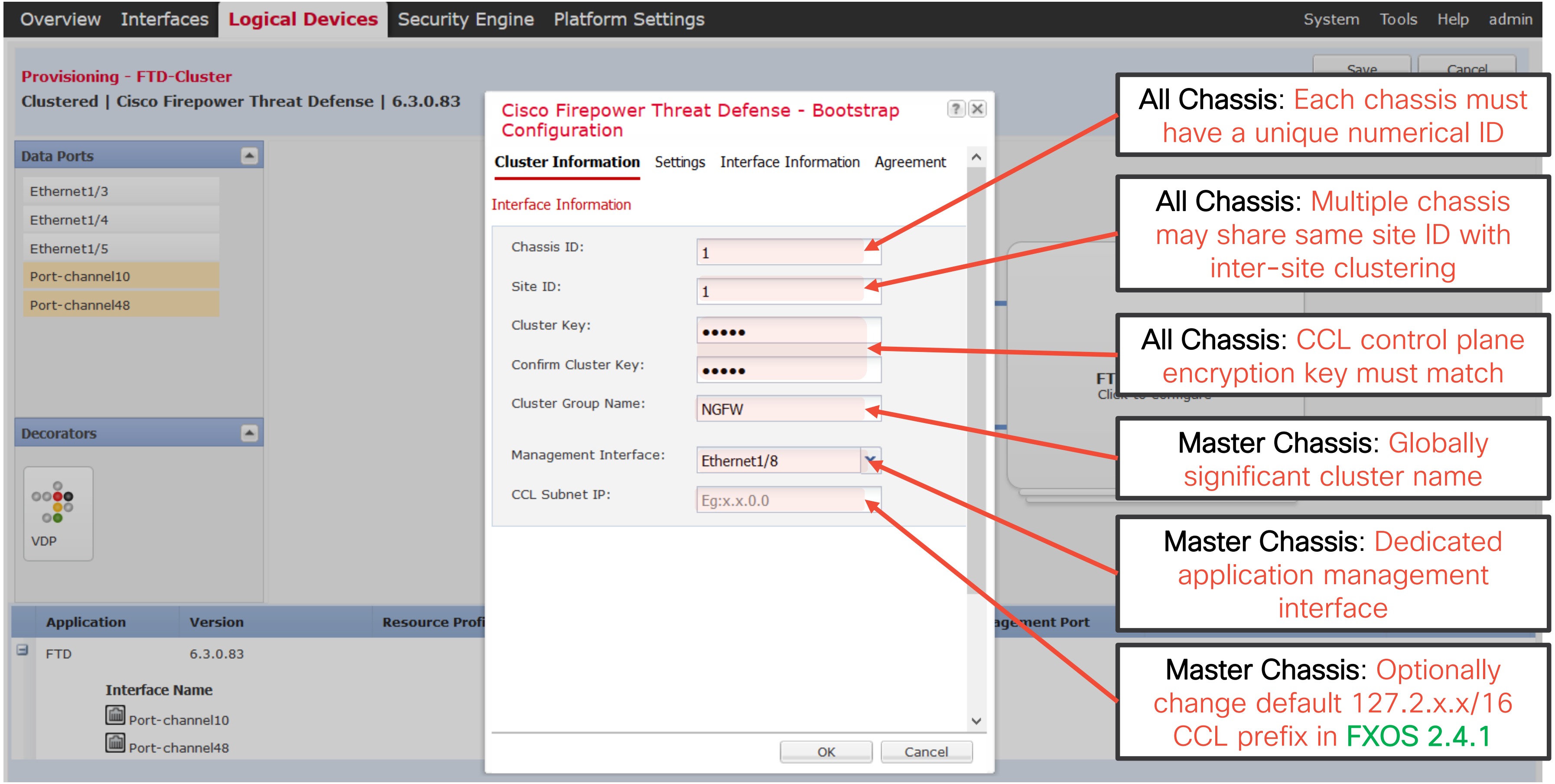
All Chassis: Verify and assign any additional data interfaces. Do **not** un-assign Po48 (inter-chassis CCL).

All Chassis: Configure logical device properties for chassis (4100) or modules (9300)

Application	Version	Resource	Status
FTD	6.3.0.83		

Interface Name	Type
Port-channel10	data
Port-channel48	cluster

Chassis Manager: FTD Cluster Bootstrap



Cisco Firepower Threat Defense - Bootstrap Configuration

Cluster Information | Settings | Interface Information | Agreement

Interface Information

Chassis ID: 1

Site ID: 1

Cluster Key: •••••

Confirm Cluster Key: •••••

Cluster Group Name: NGFW

Management Interface: Ethernet1/8

CCL Subnet IP: Eg:x.x.0.0

OK | Cancel

All Chassis: Each chassis must have a unique numerical ID

All Chassis: Multiple chassis may share same site ID with inter-site clustering

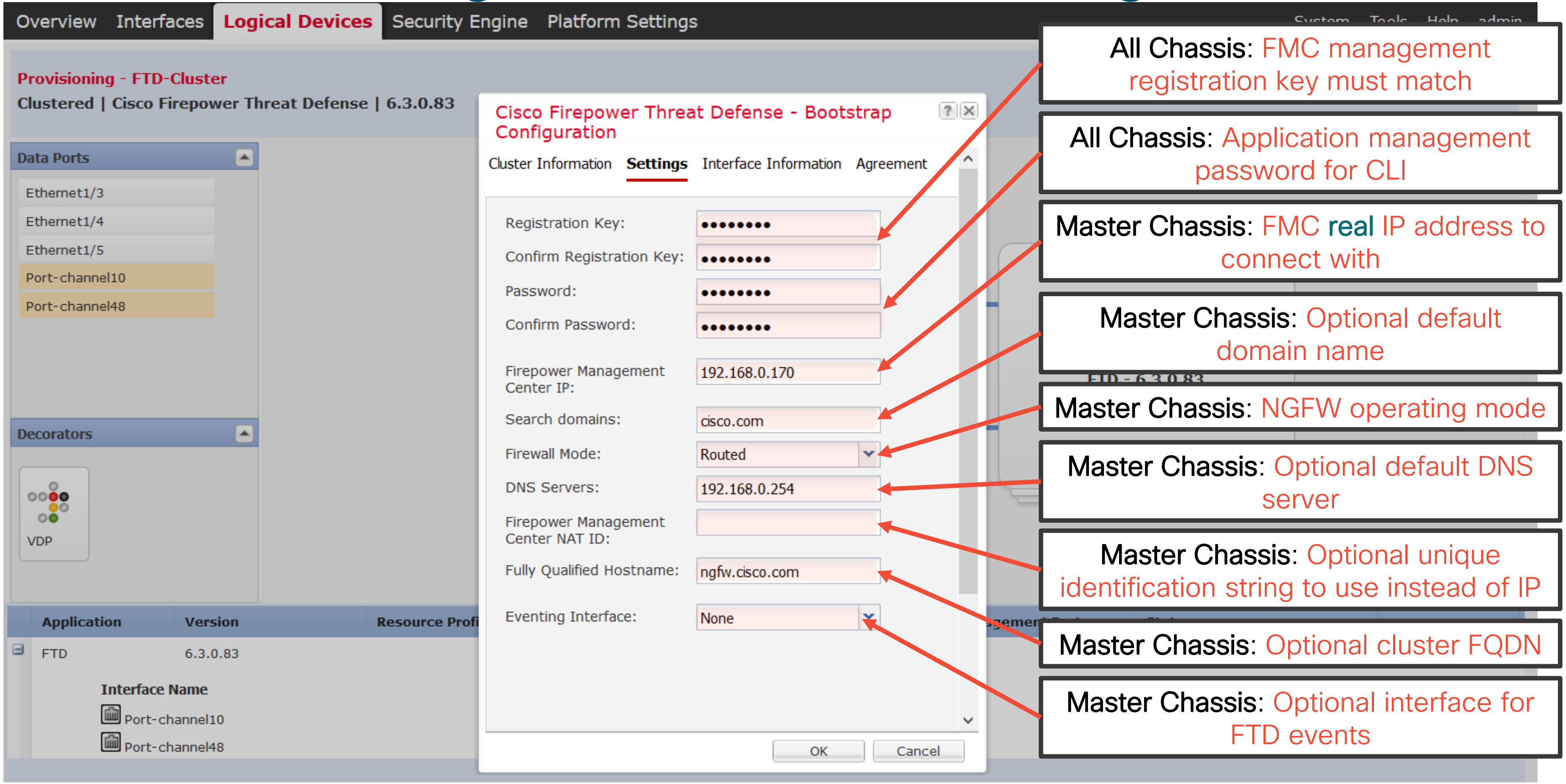
All Chassis: CCL control plane encryption key must match

Master Chassis: Globally significant cluster name

Master Chassis: Dedicated application management interface

Master Chassis: Optionally change default 127.2.x.x/16 CCL prefix in FXOS 2.4.1

Chassis Manager: FTD Device Settings



Provisioning - FTD-Cluster
Clustered | Cisco Firepower Threat Defense | 6.3.0.83

Cisco Firepower Threat Defense - Bootstrap Configuration

Cluster Information | **Settings** | Interface Information | Agreement

Registration Key:	••••••••
Confirm Registration Key:	••••••••
Password:	••••••••
Confirm Password:	••••••••
Firepower Management Center IP:	192.168.0.170
Search domains:	cisco.com
Firewall Mode:	Routed
DNS Servers:	192.168.0.254
Firepower Management Center NAT ID:	
Fully Qualified Hostname:	ngfw.cisco.com
Eventing Interface:	None

Application	Version	Resource Profi
FTD	6.3.0.83	

Interface Name
Port-channel10
Port-channel48

All Chassis: FMC management registration key must match

All Chassis: Application management password for CLI

Master Chassis: FMC real IP address to connect with

Master Chassis: Optional default domain name

Master Chassis: NGFW operating mode

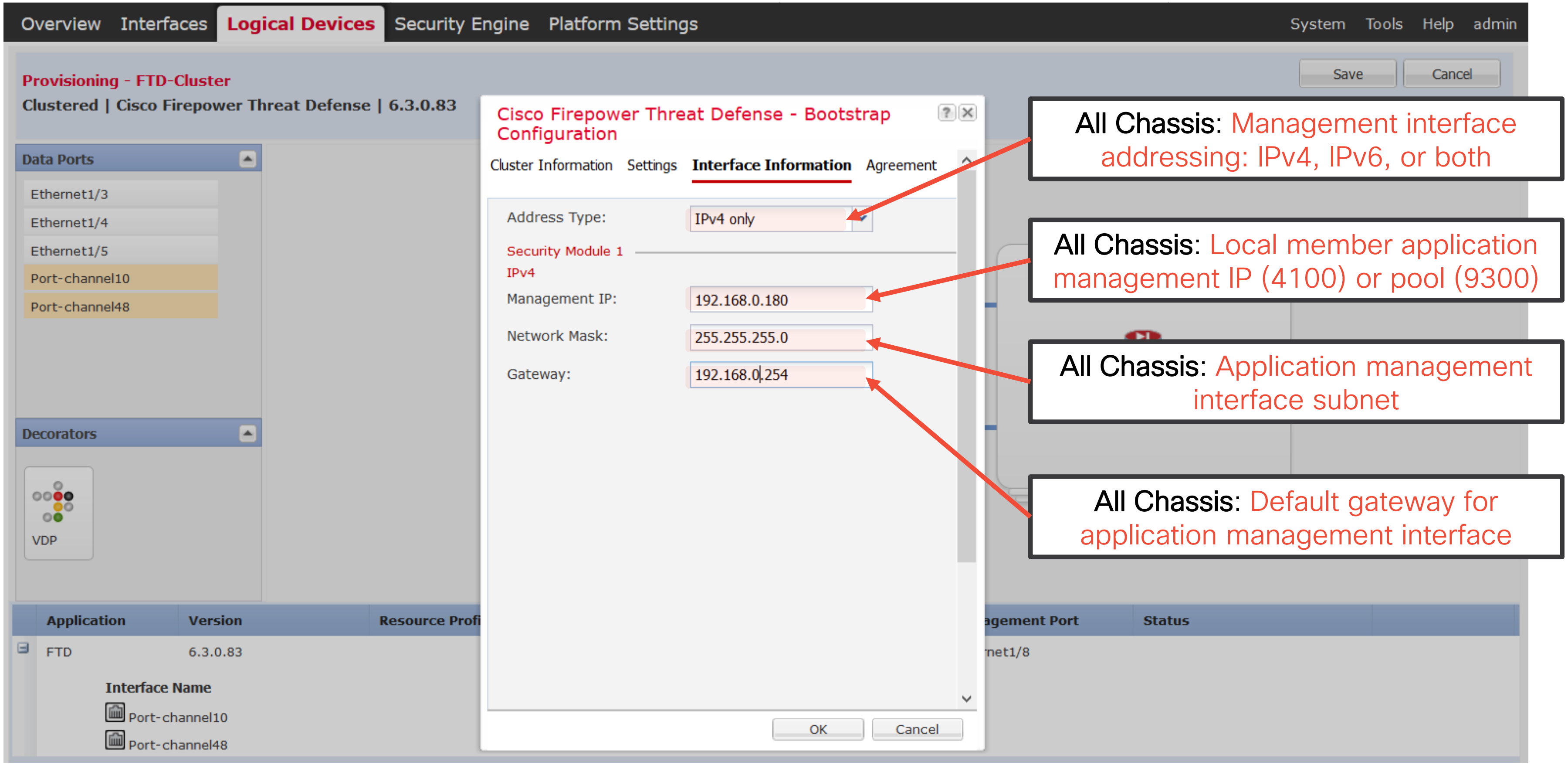
Master Chassis: Optional default DNS server

Master Chassis: Optional unique identification string to use instead of IP

Master Chassis: Optional cluster FQDN

Master Chassis: Optional interface for FTD events

Chassis Manager: FTD Management Interface



Provisioning - FTD-Cluster

Clustered | Cisco Firepower Threat Defense | 6.3.0.83

Cisco Firepower Threat Defense - Bootstrap Configuration

Cluster Information | Settings | **Interface Information** | Agreement

Address Type: IPv4 only

Security Module 1

IPv4

Management IP: 192.168.0.180

Network Mask: 255.255.255.0

Gateway: 192.168.0.254

OK | Cancel

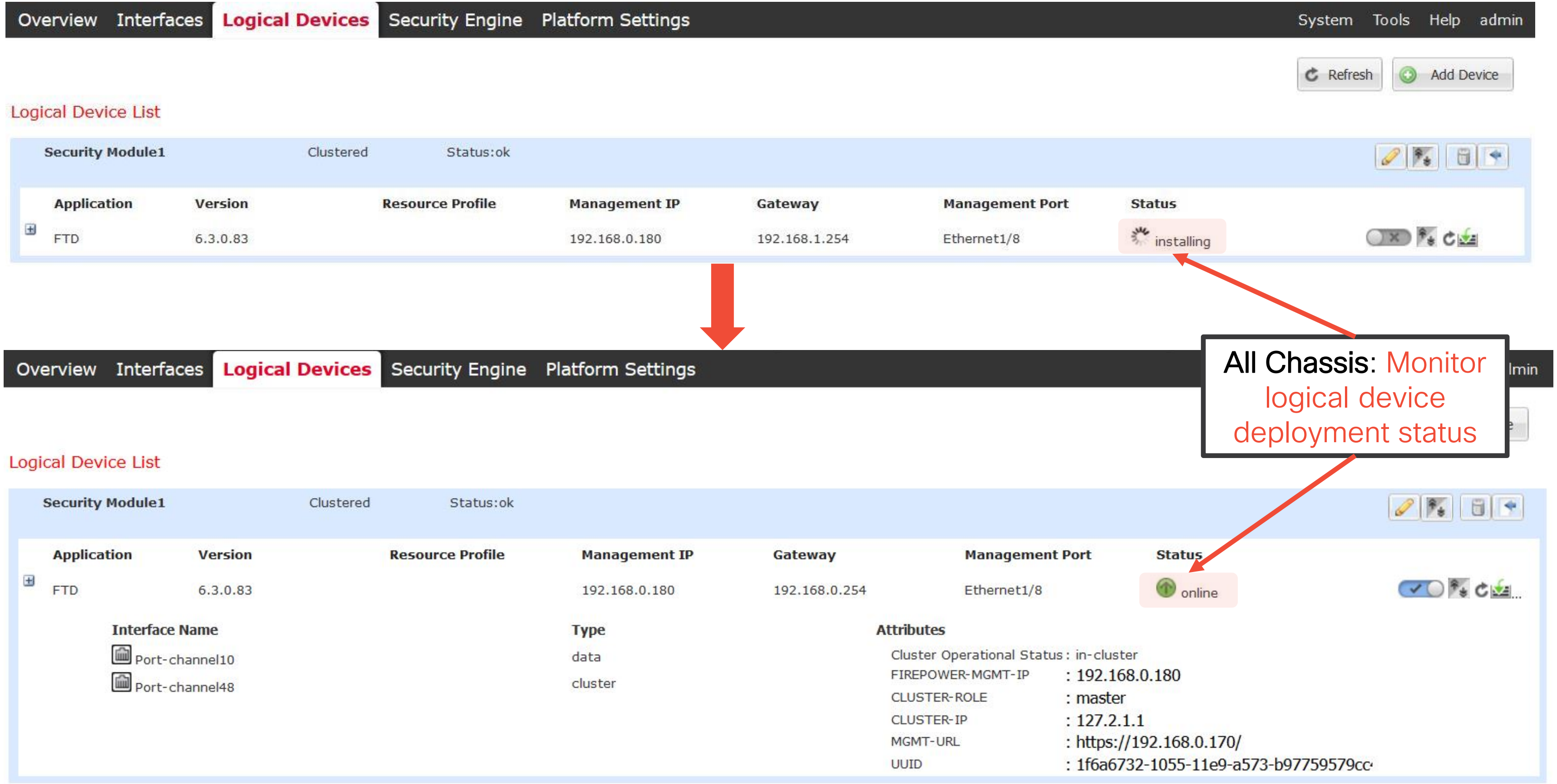
All Chassis: Management interface addressing: IPv4, IPv6, or both

All Chassis: Local member application management IP (4100) or pool (9300)

All Chassis: Application management interface subnet

All Chassis: Default gateway for application management interface

Chassis Manager: FTD Device Installation



Logical Device List

Security Module1 Clustered Status:ok

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	6.3.0.83		192.168.0.180	192.168.1.254	Ethernet1/8	installing

Logical Device List

Security Module1 Clustered Status:ok

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	6.3.0.83		192.168.0.180	192.168.0.254	Ethernet1/8	online

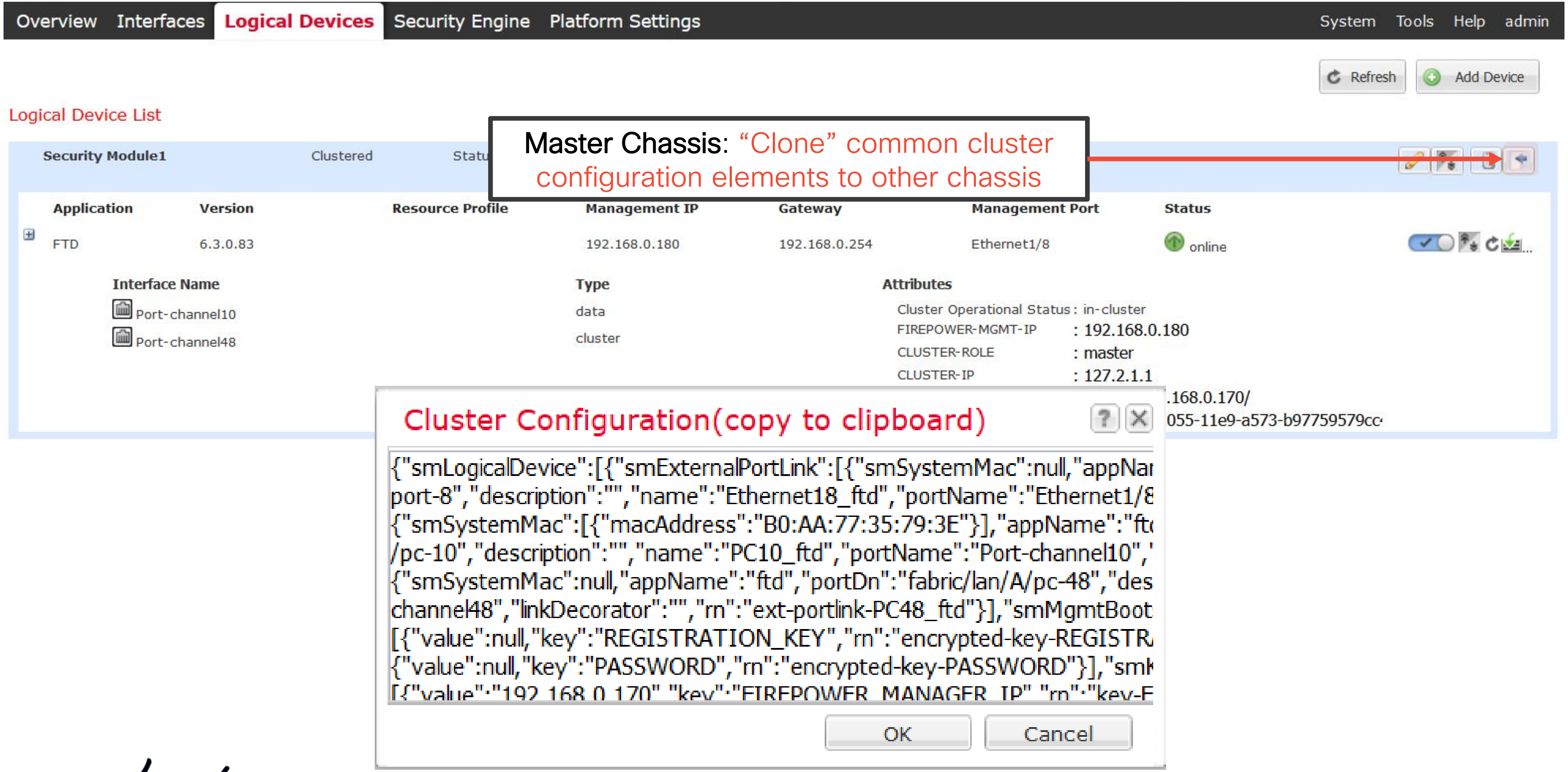
Interface Name	Type
Port-channel10	data
Port-channel48	cluster

Attributes

Cluster Operational Status	: in-cluster
FIREPOWER-MGMT-IP	: 192.168.0.180
CLUSTER-ROLE	: master
CLUSTER-IP	: 127.2.1.1
MGMT-URL	: https://192.168.0.170/
UUID	: 1f6a6732-1055-11e9-a573-b97759579cc

All Chassis: Monitor logical device deployment status

Chassis Manager: Export Cluster Configuration



Master Chassis: “Clone” common cluster configuration elements to other chassis

Logical Device List

Security Module1 Clustered Statu

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	6.3.0.83		192.168.0.180	192.168.0.254	Ethernet1/8	online

Interface Name	Type
Port-channel10	data
Port-channel48	cluster

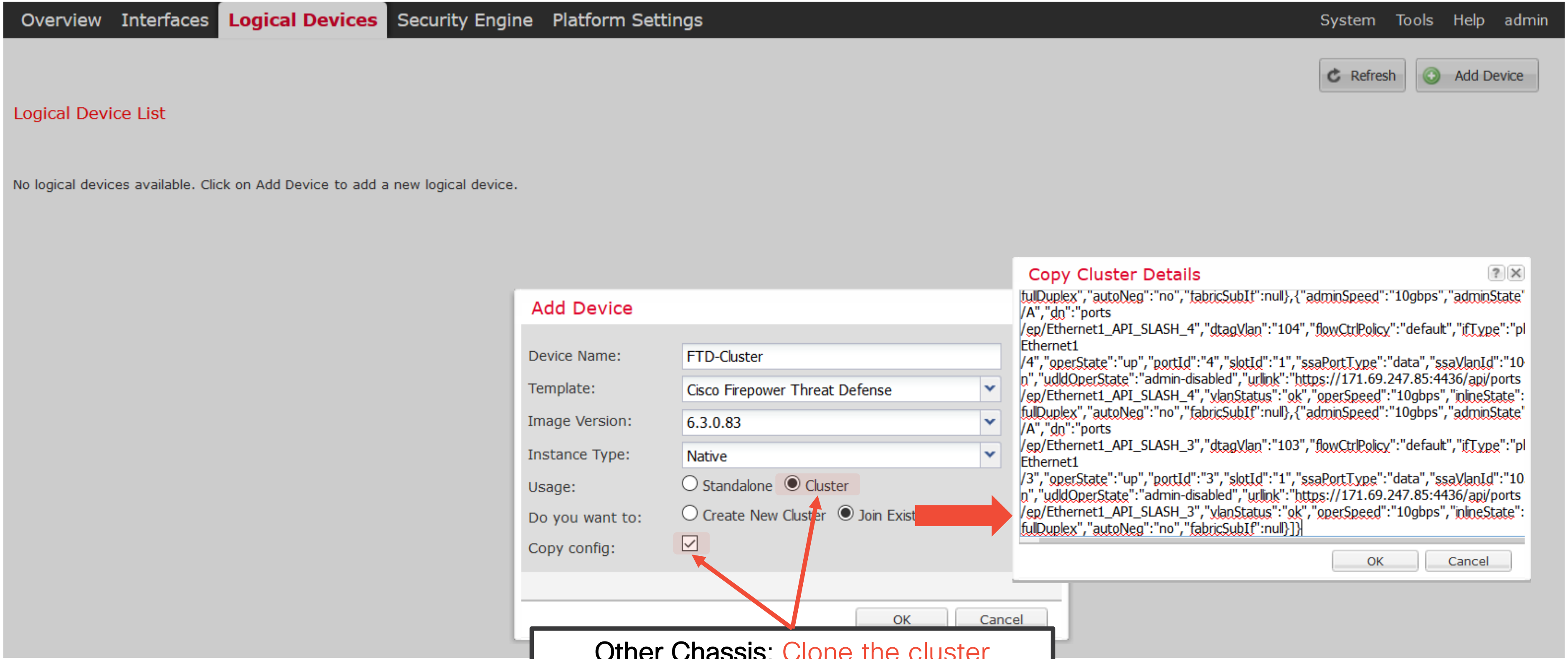
Attributes

Cluster Operational Status : in-cluster
FIREPOWER-MGMT-IP : 192.168.0.180
CLUSTER-ROLE : master
CLUSTER-IP : 127.2.1.1
.168.0.170/
055-11e9-a573-b97759579cc

Cluster Configuration(copy to clipboard)

{"smLogicalDevice":[{"smExternalPortLink":[{"smSystemMac":null,"appNar
port-8","description":"","name":"Ethernet18_ftd","portName":"Ethernet1/8
{"smSystemMac":[{"macAddress":"B0:AA:77:35:79:3E"}],"appName":"ftc
/pc-10","description":"","name":"PC10_ftd","portName":"Port-channel10",'
{"smSystemMac":null,"appName":"ftd","portDn":"fabric/lan/A/pc-48","des
channel48","linkDecorator":"","rn":"ext-portlink-PC48_ftd"}],"smMgmtBoot
[{"value":null,"key":"REGISTRATION_KEY","rn":"encrypted-key-REGISTR
{"value":null,"key":"PASSWORD","rn":"encrypted-key-PASSWORD"}],"smk
[{"value":"192.168.0.170","key":"FIREPOWER_MANAGER_IP","rn":"key-F

Chassis Manager: Adding Chassis to Cluster



Logical Device List

No logical devices available. Click on Add Device to add a new logical device.

Add Device

Device Name:	FTD-Cluster
Template:	Cisco Firepower Threat Defense
Image Version:	6.3.0.83
Instance Type:	Native
Usage:	○ Standalone ● Cluster
Do you want to:	○ Create New Cluster ● Join Exist
Copy config:	☑

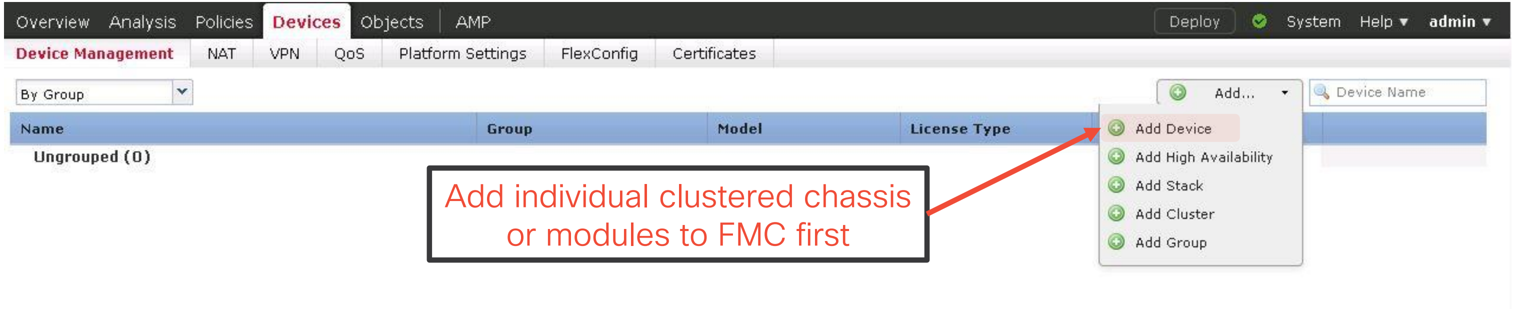
Copy Cluster Details

```
fullDuplex","autoNeg":"no","fabricSubIf":null},{"adminSpeed":"10gbps","adminState'
/A","dn":"ports
/ep/Ethernet1_API_SLASH_4","dtagVlan":"104","flowCtrlPolicy":"default","ifType":"pl
Ethernet1
/4","operState":"up","portId":"4","slotId":"1","ssaPortType":"data","ssaVlanId":"10
n","udldOperState":"admin-disabled","urllink":"https://171.69.247.85:4436/api/ports
/ep/Ethernet1_API_SLASH_4","vlanStatus":"ok","operSpeed":"10gbps","inlineState":
fullDuplex","autoNeg":"no","fabricSubIf":null},{"adminSpeed":"10gbps","adminState'
/A","dn":"ports
/ep/Ethernet1_API_SLASH_3","dtagVlan":"103","flowCtrlPolicy":"default","ifType":"pl
Ethernet1
/3","operState":"up","portId":"3","slotId":"1","ssaPortType":"data","ssaVlanId":"10
n","udldOperState":"admin-disabled","urllink":"https://171.69.247.85:4436/api/ports
/ep/Ethernet1_API_SLASH_3","vlanStatus":"ok","operSpeed":"10gbps","inlineState":
fullDuplex","autoNeg":"no","fabricSubIf":null}]}
```

Other Chassis: Clone the cluster configuration from master chassis when adding a new chassis

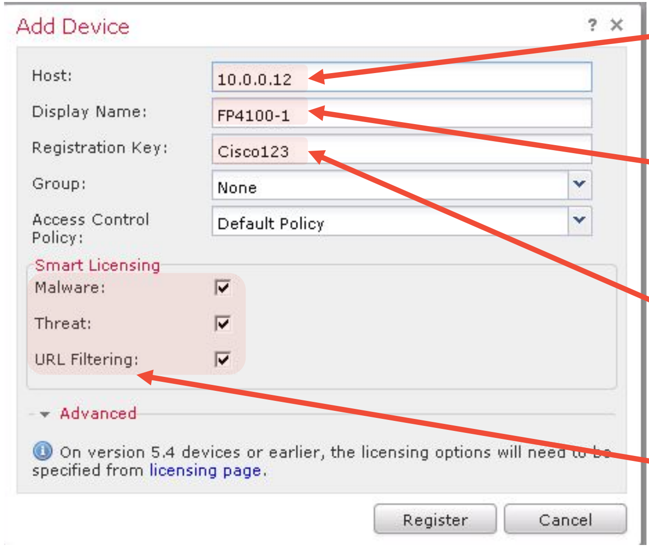
Reference

Before FMC 6.3: Add Individual Cluster Members



Overview Analysis Policies Devices Objects AMP
Deploy System Help ▾ admin ▾
Device Management NAT VPN QoS Platform Settings FlexConfig Certificates
By Group
Add...
Device Name
Name Group Model License Type
Ungrouped (0)
Add Device
Add High Availability
Add Stack
Add Cluster
Add Group

Add individual clustered chassis or modules to FMC first



Add Device

Host:	10.0.0.12
Display Name:	FP4100-1
Registration Key:	Cisco123
Group:	None
Access Control Policy:	Default Policy

Smart Licensing

Malware:	☑
Threat:	☑
URL Filtering:	☑

▾ Advanced

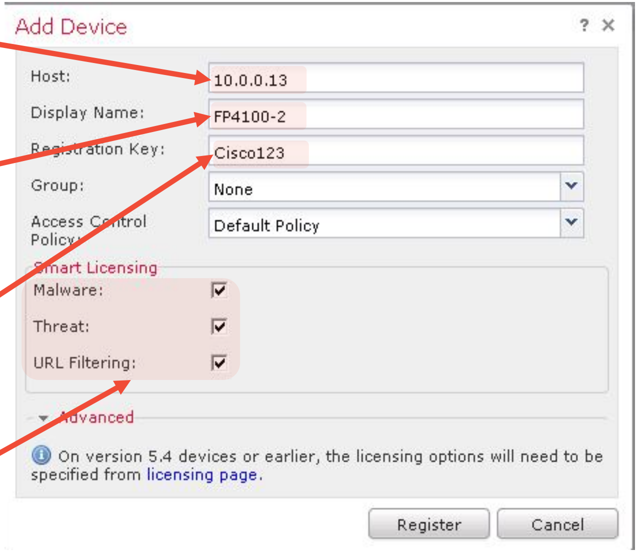
On version 5.4 devices or earlier, the licensing options will need to be specified from licensing page.

All Chassis/Modules: FTD application management IP

All Chassis/Modules: Unique display name in FMC

All Chassis: FMC registration key **must** match logical device configuration

All Chassis/Modules: Feature licenses must match across entire cluster



Add Device

Host:	10.0.0.13
Display Name:	FP4100-2
Registration Key:	Cisco123
Group:	None
Access Control Policy:	Default Policy

Smart Licensing

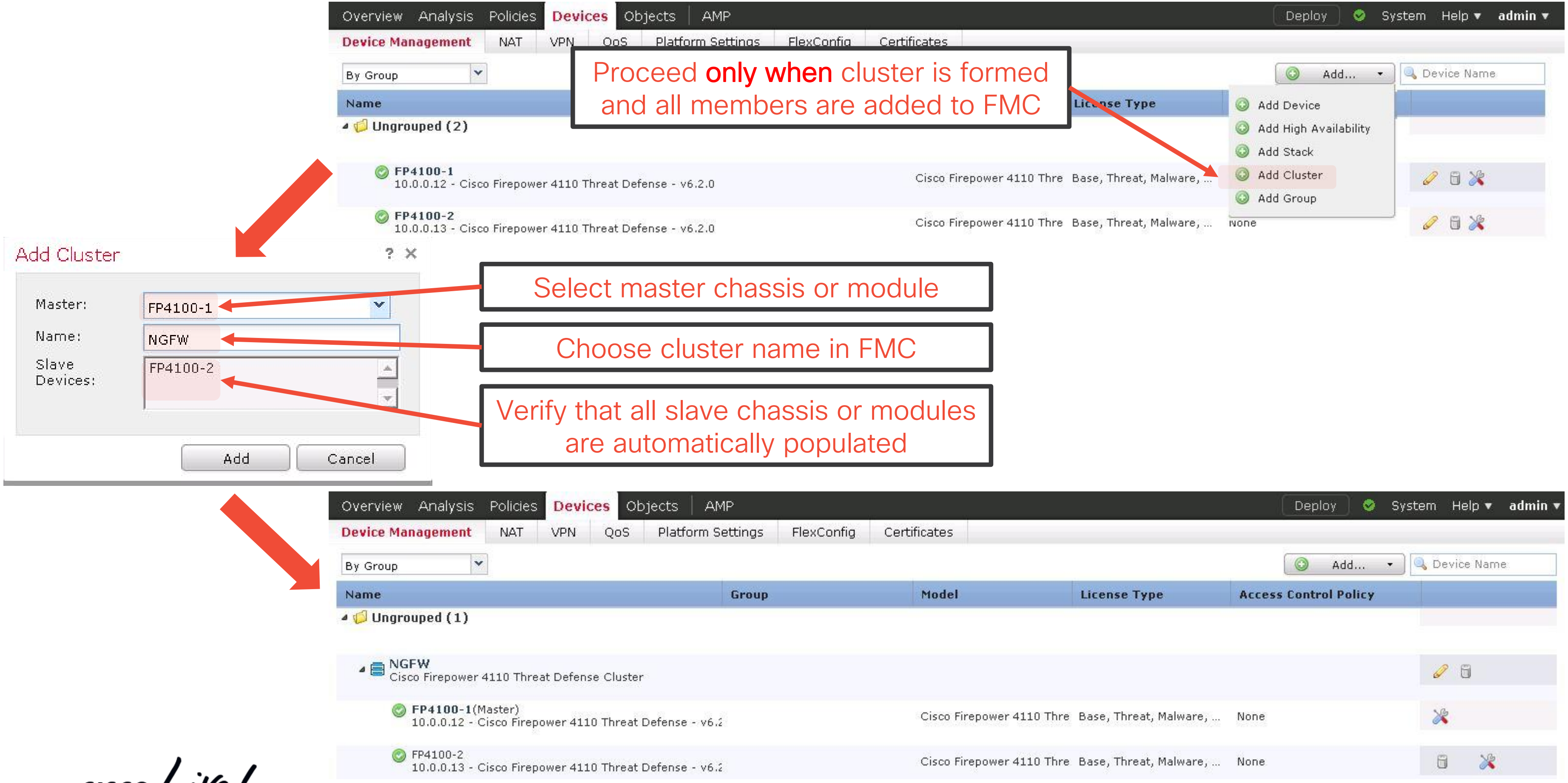
Malware:	☑
Threat:	☑
URL Filtering:	☑

▾ Advanced

On version 5.4 devices or earlier, the licensing options will need to be specified from licensing page.

Reference

Before FMC 6.3: Add Cluster



Overview Analysis Policies **Devices** Objects AMP — Deploy — System Help ▾ admin ▾

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

By Group — Add... — Device Name

Add Device
Add High Availability
Add Stack
Add Cluster
Add Group

Name	Model	License Type	
Ungrouped (2)			
FP4100-1 10.0.0.12 - Cisco Firepower 4110 Threat Defense - v6.2.0	Cisco Firepower 4110 Thre	Base, Threat, Malware, ...	
FP4100-2 10.0.0.13 - Cisco Firepower 4110 Threat Defense - v6.2.0	Cisco Firepower 4110 Thre	Base, Threat, Malware, ...	None

Proceed **only when** cluster is formed and all members are added to FMC

Add Cluster

Master:	FP4100-1
Name:	NGFW
Slave Devices:	FP4100-2

Add Cancel

Select master chassis or module

Choose cluster name in FMC

Verify that all slave chassis or modules are automatically populated

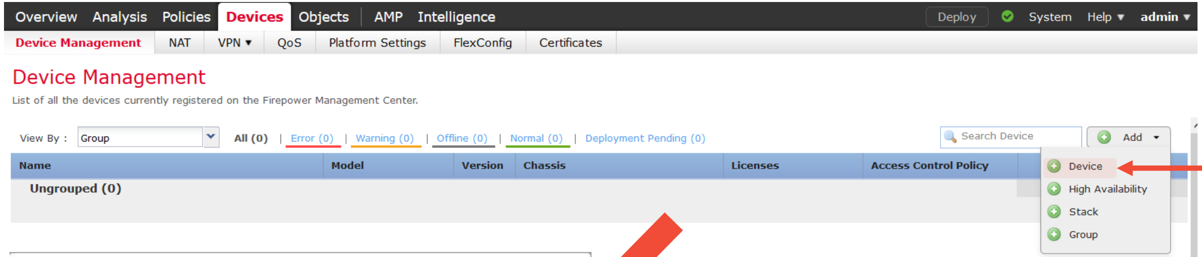
Overview Analysis Policies **Devices** Objects AMP — Deploy — System Help ▾ admin ▾

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

By Group — Add... — Device Name

Name	Group	Model	License Type	Access Control Policy
Ungrouped (1)				
NGFW Cisco Firepower 4110 Threat Defense Cluster				
FP4100-1(Master) 10.0.0.12 - Cisco Firepower 4110 Threat Defense - v6.2		Cisco Firepower 4110 Thre	Base, Threat, Malware, ...	None
FP4100-2 10.0.0.13 - Cisco Firepower 4110 Threat Defense - v6.2		Cisco Firepower 4110 Thre	Base, Threat, Malware, ...	None

FMC 6.3: Add Entire Cluster



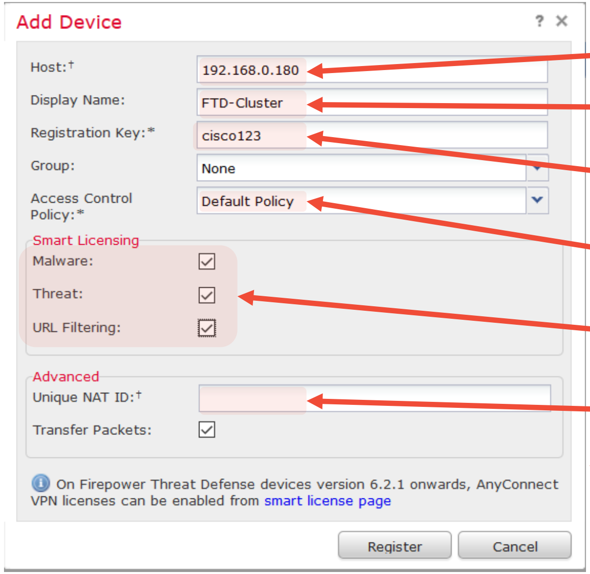
Device Management

List of all the devices currently registered on the Firepower Management Center.

View By : Group | All (0) | Error (0) | Warning (0) | Offline (0) | Normal (0) | Deployment Pending (0)

Name	Model	Version	Chassis	Licenses	Access Control Policy
Ungrouped (0)					

Add **master** unit **only**, other cluster members are discovered automatically



Add Device

Host:†	192.168.0.180
Display Name:	FTD-Cluster
Registration Key:*	cisco123
Group:	None
Access Control Policy:*	Default Policy

Smart Licensing

Malware:	☑
Threat:	☑
URL Filtering:	☑

Advanced

Unique NAT ID:†	
Transfer Packets:	☑

On Firepower Threat Defense devices version 6.2.1 onwards, AnyConnect VPN licenses can be enabled from smart license page

FTD application **real** management IP

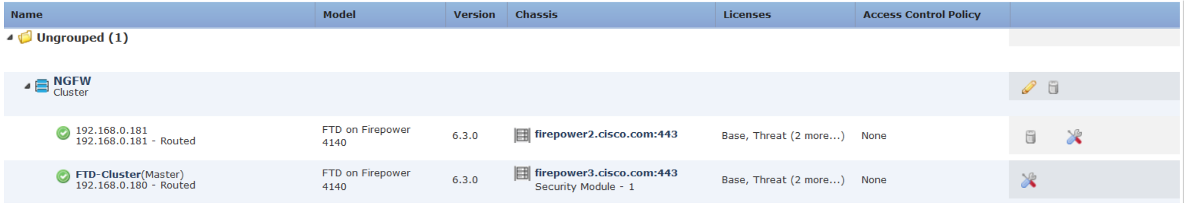
Master unit unique display name in FMC

FMC registration key must match logical device configuration across all members

Must assign a default **Main Access Control Policy**

Feature licenses must match across entire cluster

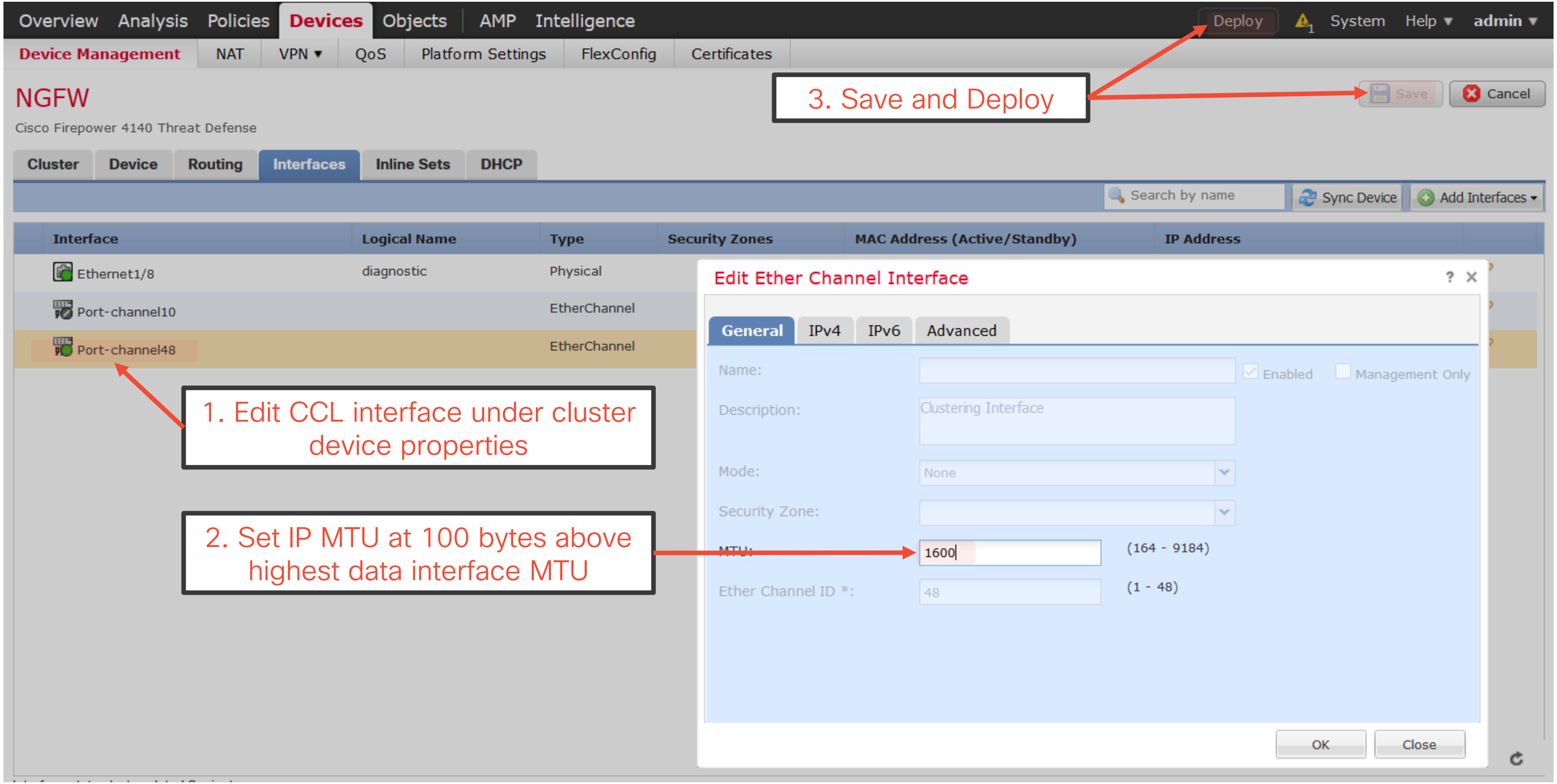
Optional matching identification string to use instead of IP



Name	Model	Version	Chassis	Licenses	Access Control Policy
Ungrouped (1)					
NGFW Cluster					
192.168.0.181 192.168.0.181 - Routed	FTD on Firepower 4140	6.3.0	firepower2.cisco.com:443	Base, Threat (2 more...)	None
FTD-Cluster(Master) 192.168.0.180 - Routed	FTD on Firepower 4140	6.3.0	firepower3.cisco.com:443 Security Module - 1	Base, Threat (2 more...)	None

cisco Live!

FMC: Change CCL MTU Settings



NGFW

Cisco Firepower 4140 Threat Defense

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Ethernet1/8	diagnostic	Physical			
Port-channel10		EtherChannel			
Port-channel48		EtherChannel			

Edit Ether Channel Interface

Name:

☑ Enabled □ Management Only

Description: Clustering Interface

Mode: None

Security Zone:

MTU: 1600 (164 - 9184)

Ether Channel ID *: 48 (1 - 48)

1. Edit CCL interface under cluster device properties

2. Set IP MTU at 100 bytes above highest data interface MTU

3. Save and Deploy

Monitoring and Troubleshooting Clustering

- show cluster command group displays aggregated statistics
  - show cluster history helps to understand state transitions and failure reasons
  - show cluster cpu helps to check CPU utilization across cluster
- show cluster info command group displays cluster subsystem information
  - show cluster info health helps to monitor aggregated unit health data
  - show cluster info loadbalance relates to optional Conn Rebalance feature
  - show cluster info trace shows cluster state machine debug data for Cisco TAC
- Leverage syslog messages to understand failure reasons

```
%ASA-3-747022: Clustering: Asking slave unit terra to quit because it failed interface health
check 3 times (last failure on Port-channel1), rejoin will be attempted after 20 min.
```

  - Use logging device-id to identity reporting members for connection events

Multi-Site Clustering

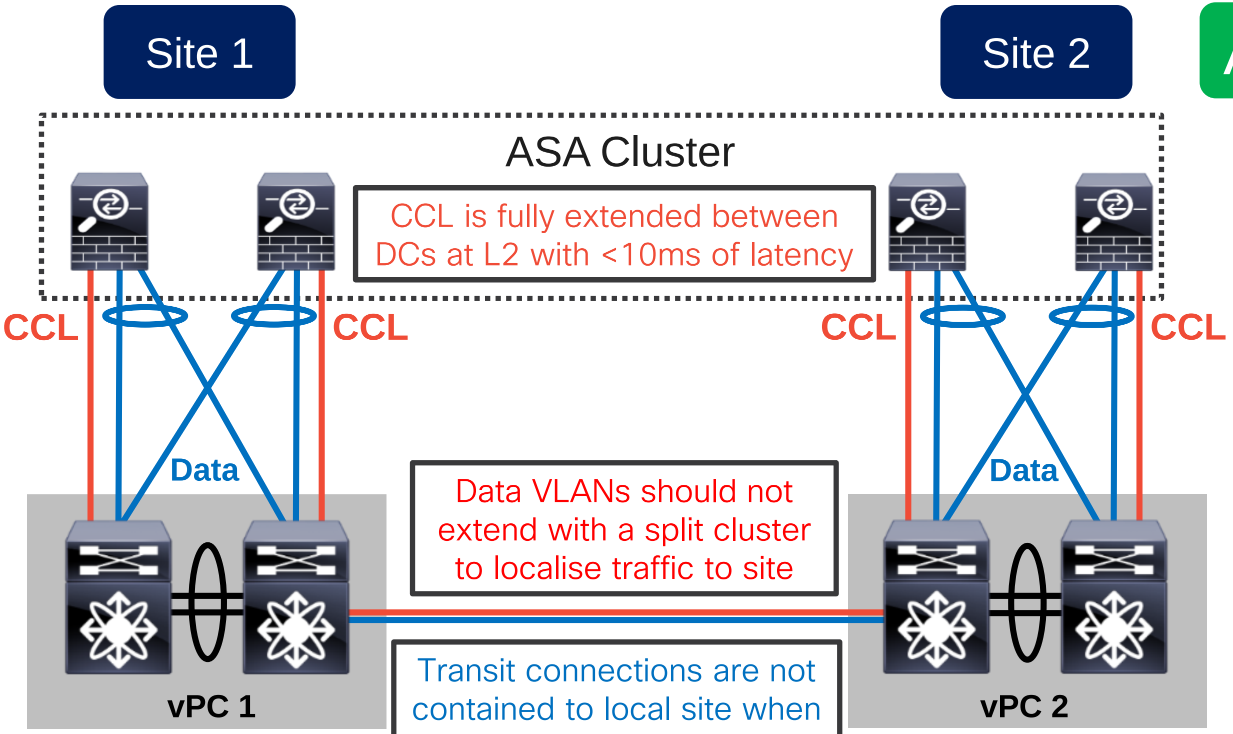
Inter Data Center (DC) Clustering

- Clustering assumes, but not requires data interface adjacency at Layer 2
- Geographically separated clusters supported in ASA 9.1(4)+
  - “Dark Media” CCL with up to 10ms of one-way latency and no packet loss
  - Routed firewall in Individual interface mode only
- ASA 9.2(1) extends inter-DC clustering to Spanned Etherchannel mode
  - Transparent firewall only
  - Routed firewall support presented design challenges
- ASA 9.5(1) adds inter-DC Spanned Etherchannel clustering in routed mode
- FTD 6.2 adds NGFW inter-site clustering through FlexConfig only
- ACI 3.2 Anycast Services for routed ASA and FTD clusters with Multi-Pod

Reference

Split or Single Individual Mode Cluster

ASA 9.2(1)



CCL is fully extended between DCs at L2 with <10ms of latency

Data interfaces connect to local switch pair only

Data VLANs should not extend with a split cluster to localise traffic to site

Transit connections are not contained to local site when extending data VLANs

Local vPC/VSS pairs at each site

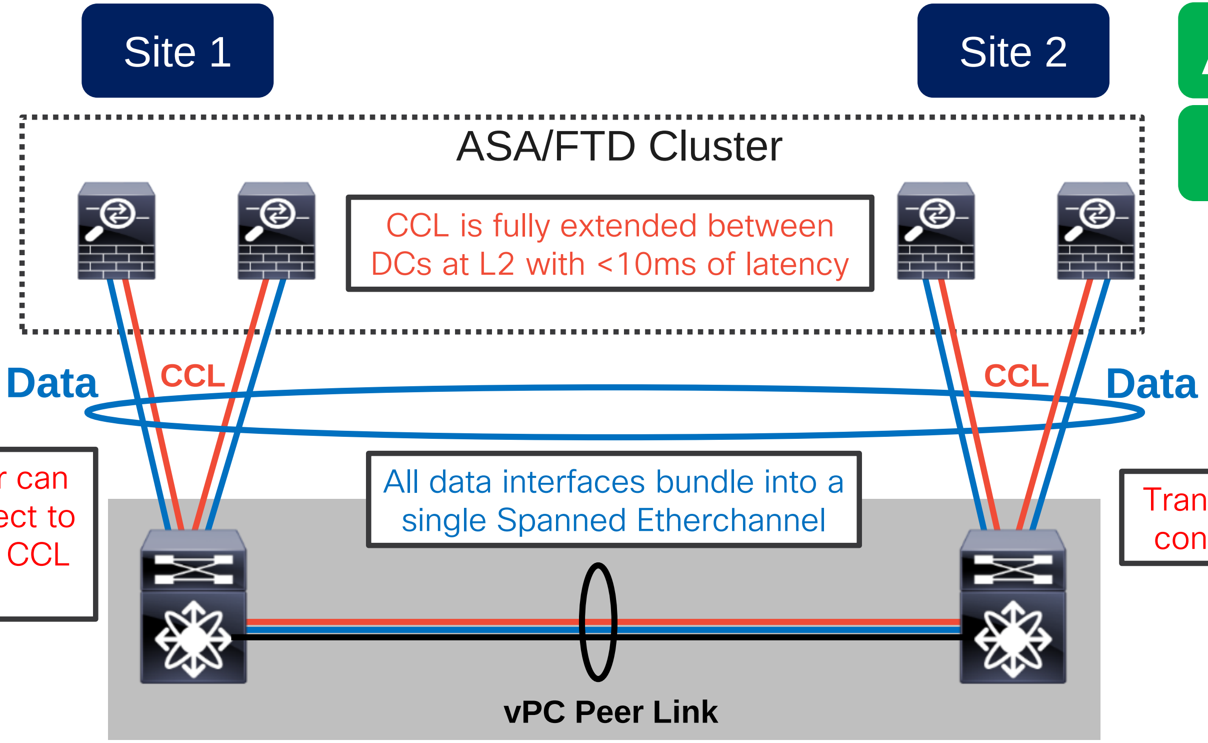
Local vPC/VSS pairs at each site

Reference

Extended Spanned Etherchannel Cluster

ASA 9.1(4)

FTD 6.2



CCL is fully extended between DCs at L2 with <10ms of latency

Each cluster member can single- or dual-connect to the VSS/vPC pair for CCL and Data

All data interfaces bundle into a single Spanned Etherchannel

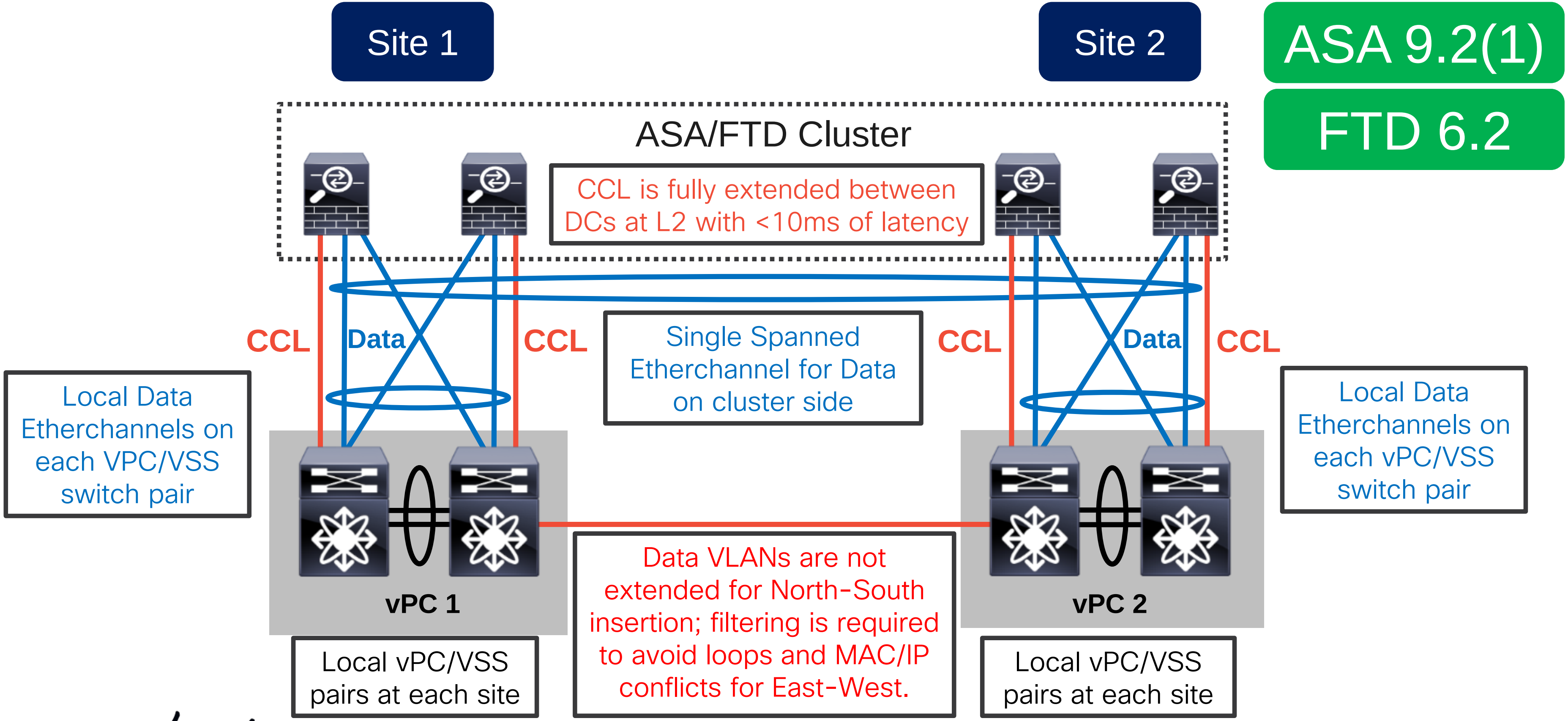
Transit connections are not contained to the local site

vPC logical switch pair is stretched across sites

Split Spanned Etherchannel Cluster

ASA 9.2(1)

FTD 6.2



CCL is fully extended between DCs at L2 with <10ms of latency

Single Spanned Etherchannel for Data on cluster side

Local Data Etherchannels on each VPC/VSS switch pair

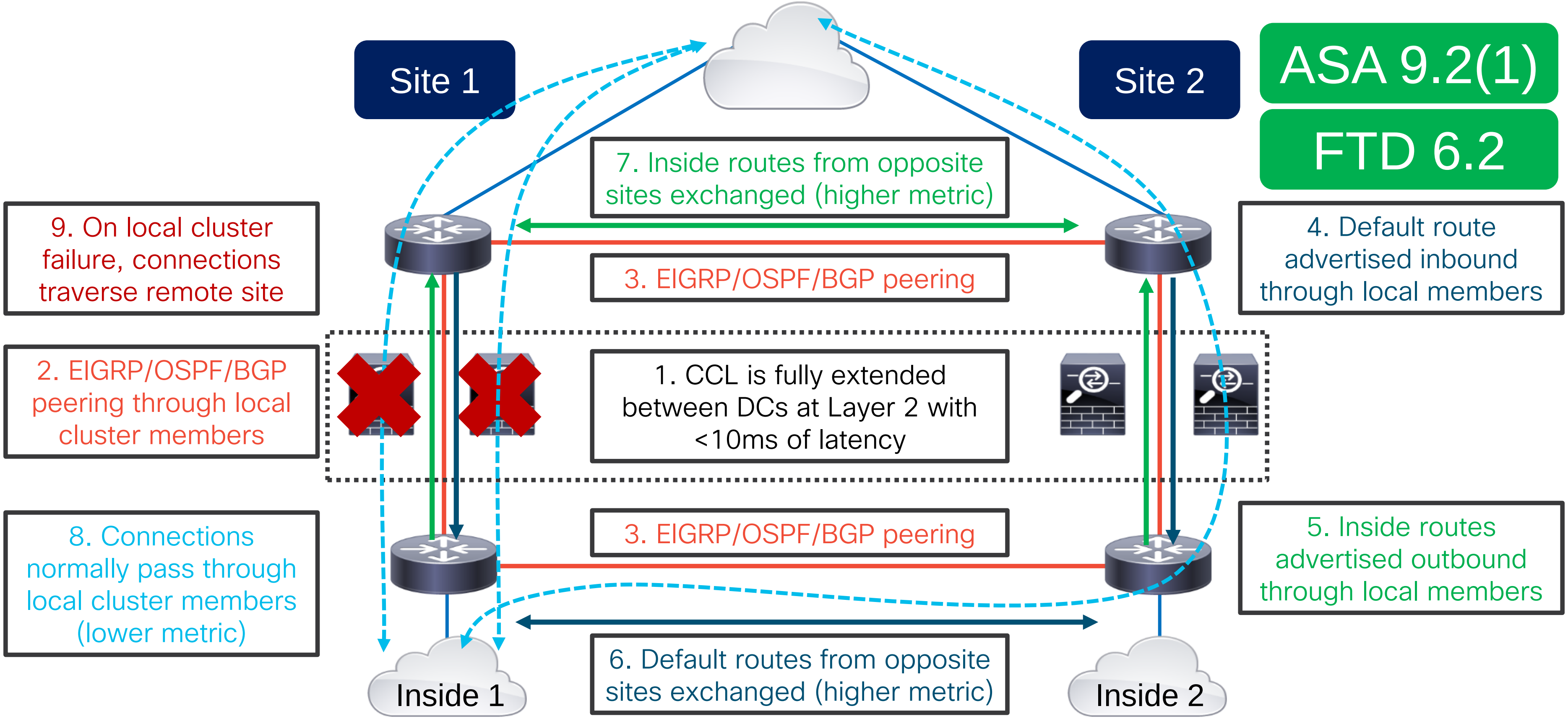
Local Data Etherchannels on each vPC/VSS switch pair

Local vPC/VSS pairs at each site

Local vPC/VSS pairs at each site

Data VLANs are not extended for North-South insertion; filtering is required to avoid loops and MAC/IP conflicts for East-West.

North-South (NS) Inter DC Cluster



ASA 9.2(1)

FTD 6.2

1. CCL is fully extended between DCs at Layer 2 with <10ms of latency

2. EIGRP/OSPF/BGP peering through local cluster members

3. EIGRP/OSPF/BGP peering

3. EIGRP/OSPF/BGP peering

4. Default route advertised inbound through local members

5. Inside routes advertised outbound through local members

6. Default routes from opposite sites exchanged (higher metric)

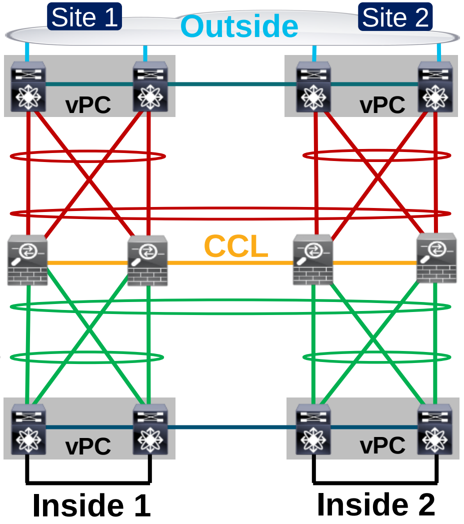
7. Inside routes from opposite sites exchanged (higher metric)

8. Connections normally pass through local cluster members (lower metric)

9. On local cluster failure, connections traverse remote site

Example: NS Split Spanned Etherchannel Cluster

- A vPC pair of Nexus switches at each site
  - Split Spanned Etherchannel cluster in transparent mode
  - Separate Etherchannel to local cluster members per vPC pair
  - VRF sandwich "through" the cluster with static PBR and SLA
- Non-overlapping inside subnets between sites
  - Mirrored SVI MAC addresses between two cluster transit VLANs
  - Dual-homed cluster members on each vPC pair localize traffic
  - Inter-site Layer 3 links (higher cost) to re-route traffic on failure
  - Bi-directional connection symmetry without NAT
  - Inbound asymmetry only between same-site members with NAT

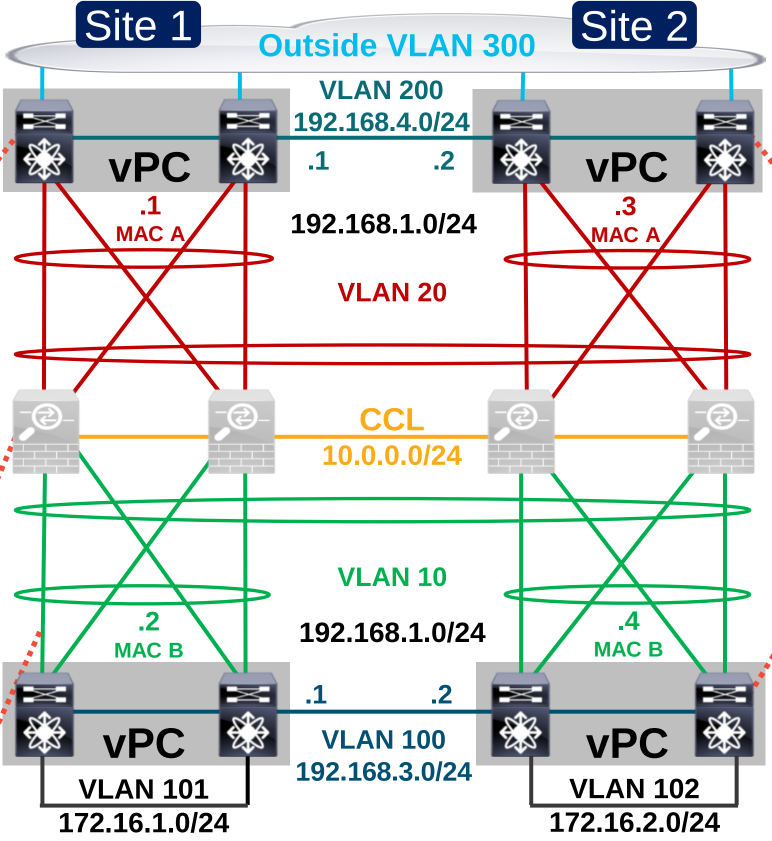


NS Split Spanned Cluster Configuration

```
ip sla 1
 icmp-echo 192.168.1.2
ip sla schedule 1 life forever start-
 time now
track 1 ip sla 1 reachability
ip access-list PBR
   permit ip any 172.16.1.0 255.255.255.0
route-map PBR
 match ip address PBR
 set ip next-hop verify-availability
   192.168.1.2 track 1
 set ip next-hop 192.168.4.2
interface Vlan300
 ip policy route-map PBR
```

```
interface Port-Channel10.10
 vlan 10
 nameif FW-inside
 bridge-group 1
interface Port-Channel10.20
 vlan 20
 nameif FW-outside
 bridge-group 1
```

```
interface Ethernet3/1
 channel-group 1 mode active
interface Ethernet3/2
 channel-group 1 mode active
interface Port-Channel1
 switchport trunk allowed vlans 10,20
 vpc 10
```



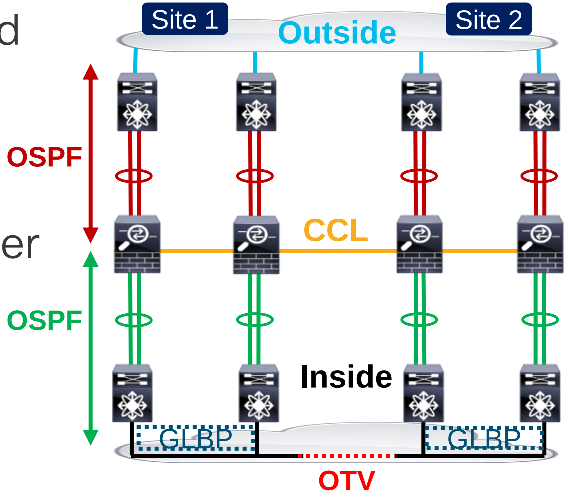
```
ip sla 1
 icmp-echo 192.168.1.4
ip sla schedule 1 life forever start-
 time now
track 1 ip sla 1 reachability
ip access-list PBR
   permit ip any 172.16.2.0 255.255.255.0
route-map PBR
 match ip address PBR
 set ip next-hop verify-availability
   192.168.1.4 track 1
 set ip next-hop 192.168.4.1
interface Vlan300
 ip policy route-map PBR
```

```
ip sla 1
 icmp-echo 192.168.1.3
ip sla schedule 1 life forever start-
 time now
track 1 ip sla 1 reachability
ip access-list PBR
   permit ip any any
route-map PBR
 match ip address PBR
 set ip next-hop verify-availability
   192.168.1.3 track 1
 set ip next-hop 192.168.3.1
interface Vlan102
 ip policy route-map PBR
```

Reference

Example: NS Split Individual Mode Cluster

- A pair of standalone (non-vPC) Nexus switches at each site
  - One Individual mode cluster unit per switch, single attached
  - Routed firewall-on-a-stick VRF sandwich with OSPF
- Inside VLAN is fully extended between sites with OTV
  - Each pair of switches uses localized GLBP as first hop router
  - GLBP traffic is blocked between sites
  - OSPF allows re-routing in case of local cluster unit failure
- Traffic symmetry is achievable without NAT
  - Outbound connections use the directly attached cluster member
  - Inbound traffic requires LISP to eliminate tromboning due to ECMP

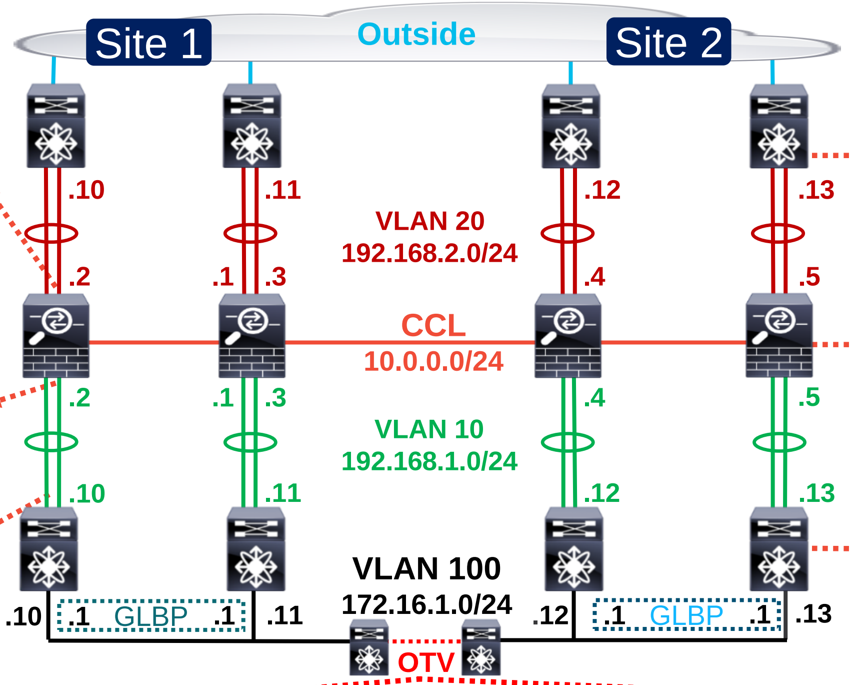


NS Split Individual Cluster Configuration

```
ip local pool OUTSIDE 192.168.2.2-
 192.168.2.17
interface Port-Channel10.20
 vlan 20
 nameif FW-outside
 ip address 192.168.2.1 255.255.255.0
  cluster-pool OUTSIDE
```

```
ip local pool OUTSIDE 192.168.1.2-
 192.168.1.17
interface Port-Channel10.10
 vlan 10
 nameif FW-inside
 ip address 192.168.1.1 255.255.255.0
  cluster-pool INSIDE
```

```
interface Ethernet3/1
 channel-group 1 mode active
interface Ethernet3/2
 channel-group 1 mode active
interface Port-Channel1
 switchport trunk allowed vlans 10,20
```



```
interface Vlan20
 vrf member OUTSIDE
 ip address 192.168.2.13/24
 ip router ospf 1 area 0.0.0.0
```

```
router ospf 1
 network 0.0.0.0 0.0.0.0 area
  0.0.0.0
```

```
interface Vlan10
 vrf member INSIDE
 ip address 192.168.1.13/24
 ip router ospf 2 area 0.0.0.0
interface Vlan100
 vrf member INSIDE
 ip router ospf 2 area 0.0.0.0
```

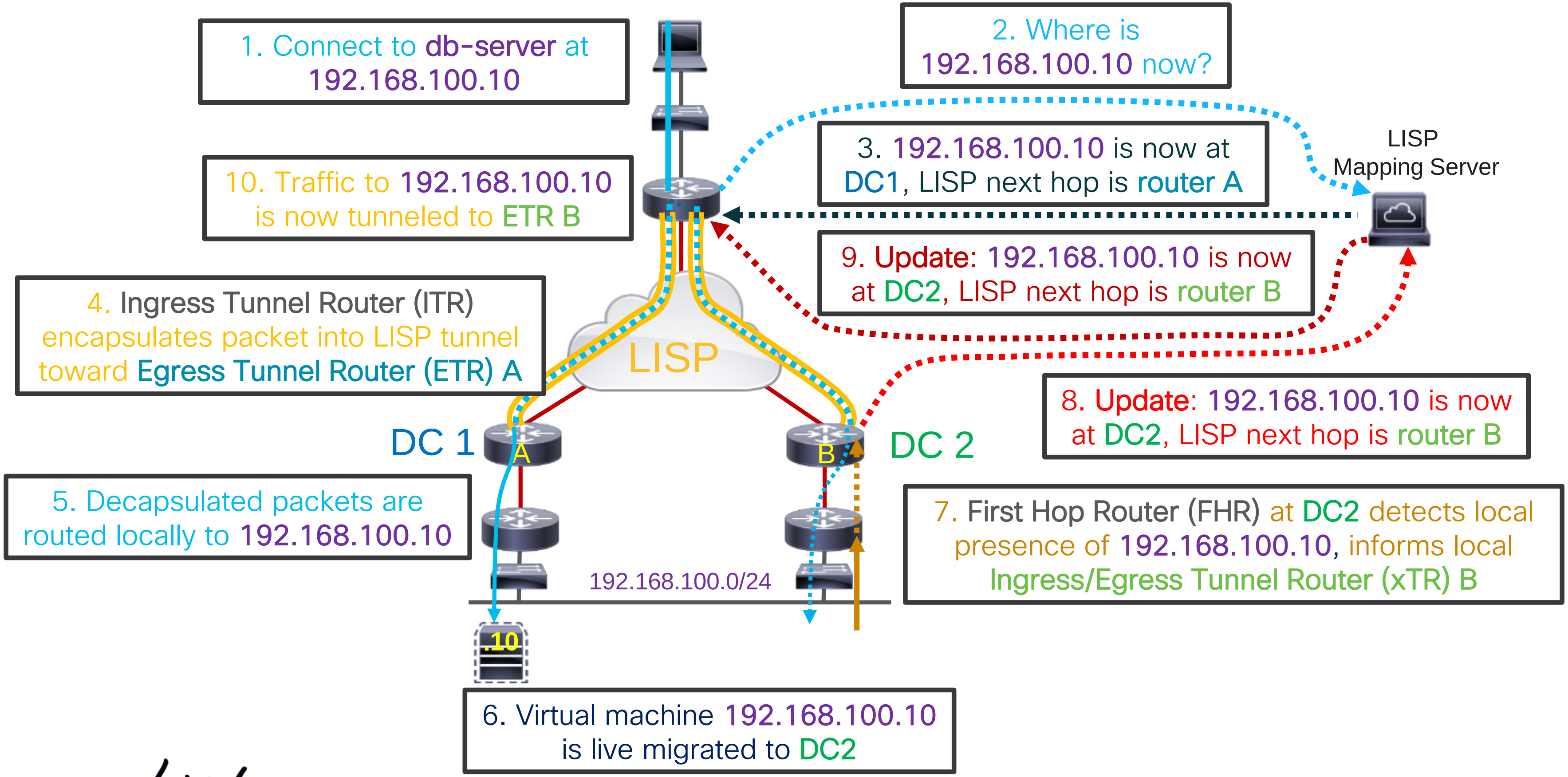
```
mac-list GLBP_FILTER seq 10 deny 0007.b400.0000 ffff.ffff.0000
mac-list GLBP_FILTER seq 20 permit 0000.0000.0000 0000.0000.0000
otv-isis default
 vpn Overlay1
  redistribute filter route-map GLBP_FILTER
```

OTV MAC Filter for GLBP

```
ip access-list NON_GLBP
 10 deny udp any 224.0.0.102/32 eq 3222
 20 permit ip any any
vlan access-map FILTER 10
 match ip address NON_GLBP
 action forward
vlan filter FILTER vlan-list 100
```

GLBP VLAN Filter

Locator/Identifier Separation Protocol (LISP)



1. Connect to db-server at 192.168.100.10

2. Where is 192.168.100.10 now?

3. 192.168.100.10 is now at DC1, LISP next hop is router A

4. Ingress Tunnel Router (ITR) encapsulates packet into LISP tunnel toward Egress Tunnel Router (ETR) A

5. Decapsulated packets are routed locally to 192.168.100.10

6. Virtual machine 192.168.100.10 is live migrated to DC2

7. First Hop Router (FHR) at DC2 detects local presence of 192.168.100.10, informs local Ingress/Egress Tunnel Router (xTR) B

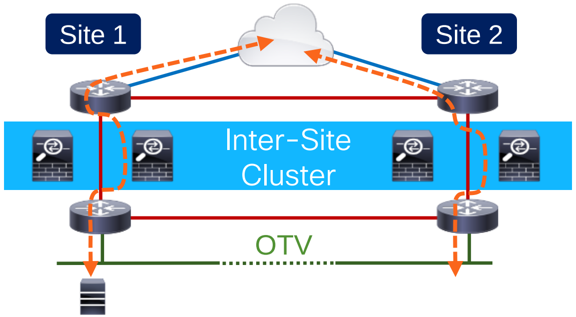
8. Update: 192.168.100.10 is now at DC2, LISP next hop is router B

9. Update: 192.168.100.10 is now at DC2, LISP next hop is router B

10. Traffic to 192.168.100.10 is now tunneled to ETR B

Dynamic Owner Reassignment with LISP

- Move flow ownership with Virtual Machines
  - Only supported with North-South clustering
  - Based on inspection of LISP FHR→xTR updates



```
access-list MOBILITY_APP permit tcp any any eq 8443
class-map MOBILITY_APP
 match access-list MOBILITY_APP

cluster group DC-ASA
 site-id 2

policy-map global_policy
 class inspection_default
  inspect lisp
 class MOBILITY_APP
  cluster flow-mobility lisp
```

Select specific applications or flows that are eligible for owner reassignment

Up to 8 sites in a single cluster

UDP/4342 traffic is inspected for LISP by default

Other triggers for owner reassignment will be added in the future

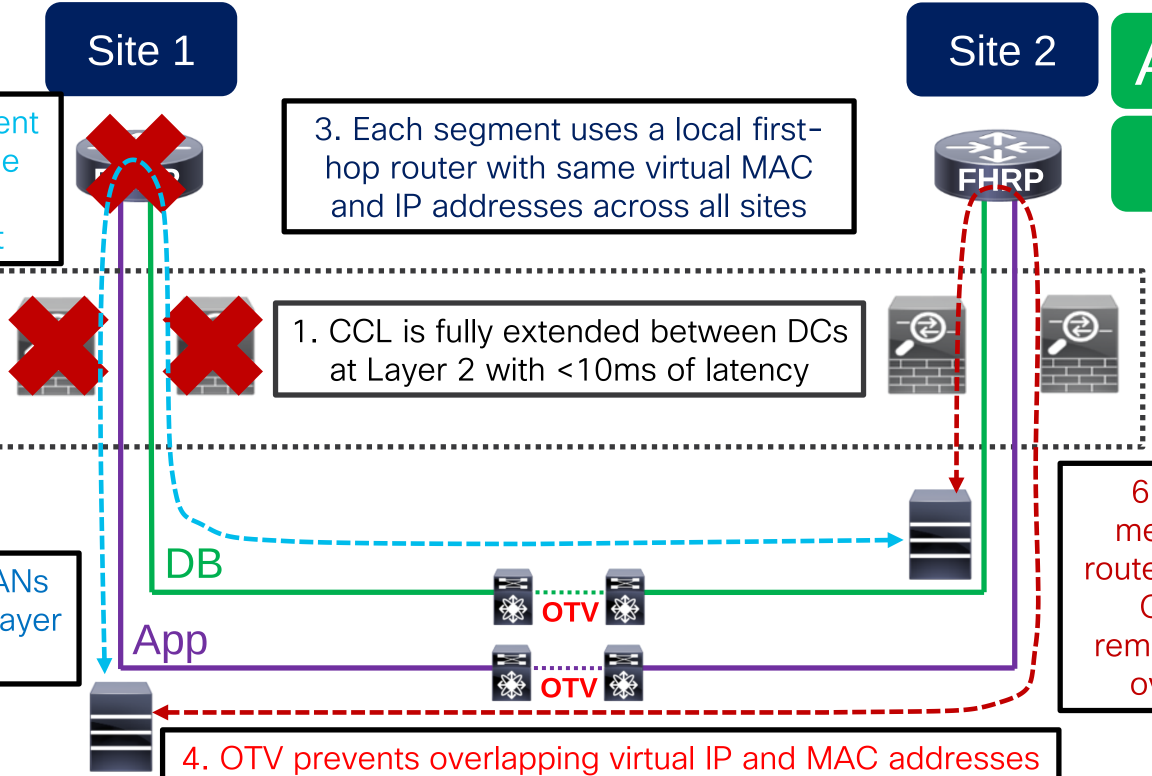
Reference

Transparent East-West (EW) Inter DC Cluster

Not recommended due to OTV filtering complexity; use Routed East-West insertion instead.

ASA 9.3(2)

FTD 6.2



1. CCL is fully extended between DCs at Layer 2 with <10ms of latency

2. Protected data VLANs are fully extended at Layer 2 between sites

3. Each segment uses a local first-hop router with same virtual MAC and IP addresses across all sites

4. OTV prevents overlapping virtual IP and MAC addresses of the first-hop routers from leaking between sites

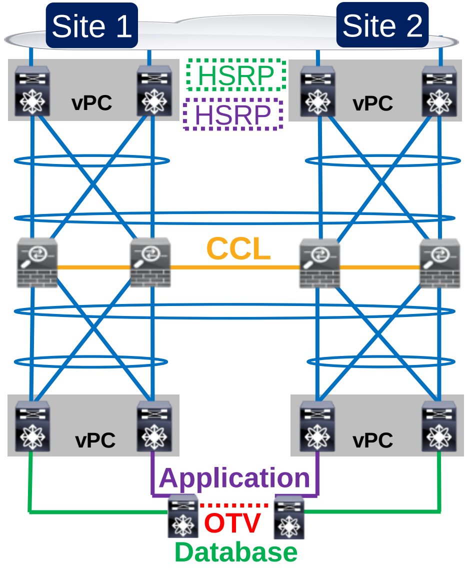
5. ASA cluster in transparent mode inserts between the endpoints and first-hop router on each segment

6. If all local cluster members or first-hop routers fail at a given site, OTV filter must be removed manually to fail over to another site

Reference

Example: EW Transparent Spanned Cluster

- A vPC pair of Nexus switches at each site
  - Transparent Split Spanned Etherchannel cluster in to separate internal segments
  - Separate Etherchannel to local cluster members per vPC pair
  - Passing firewall twice between segments is acceptable
- Internal VLANs are fully extended between sites with OTV
  - Each site uses localized HSRP as first hop router
  - HSRP traffic is blocked between sites
  - Upstream SVI/HSRP MAC statically bound to outside on cluster
  - Full Layer 2 reachability from each router to remote site
  - Must manually remove OTV filters on full upstream path failure
- Must implement LISP to avoid excessive flow redirection

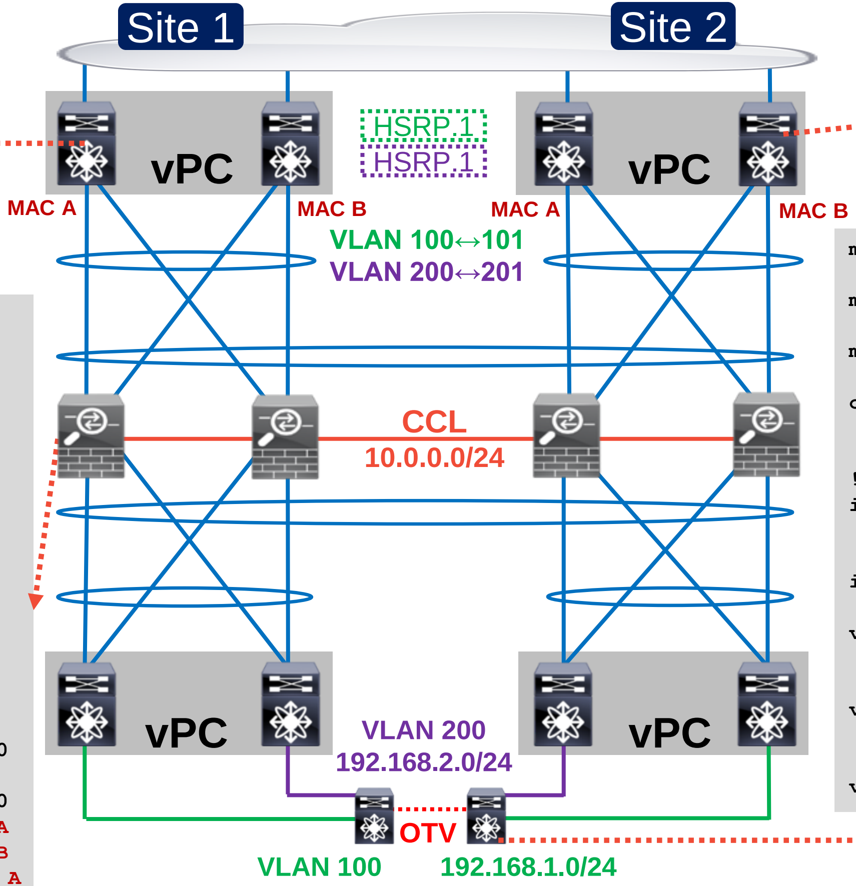


Reference

EW Transparent Spanned Cluster Configuration

```
interface Vlan101
 ip address 192.168.1.2/24
 hsrp 10
  preempt
  ip 192.168.1.1
interface Vlan201
 ip address 192.168.2.2/24
 hsrp 20
  preempt
  ip 192.168.2.1
```

```
interface Port-Channel10.100
 vlan 100
 nameif DB-inside
 bridge-group 1
interface Port-Channel10.101
 vlan 101
 nameif DB-outside
 bridge-group 1
interface Port-Channel10.200
 vlan 200
 nameif App-inside
 bridge-group 2
interface Port-Channel10.201
 vlan 201
 nameif App-outside
 bridge-group 2
interface BVI1
 ip address 192.168.1.4 255.255.255.0
interface BVI2
 ip address 192.168.2.4 255.255.255.0
mac-address-table static DB-outside A
mac-address-table static DB-outside B
mac-address-table static App-outside A
mac-address-table static App-outside B
```



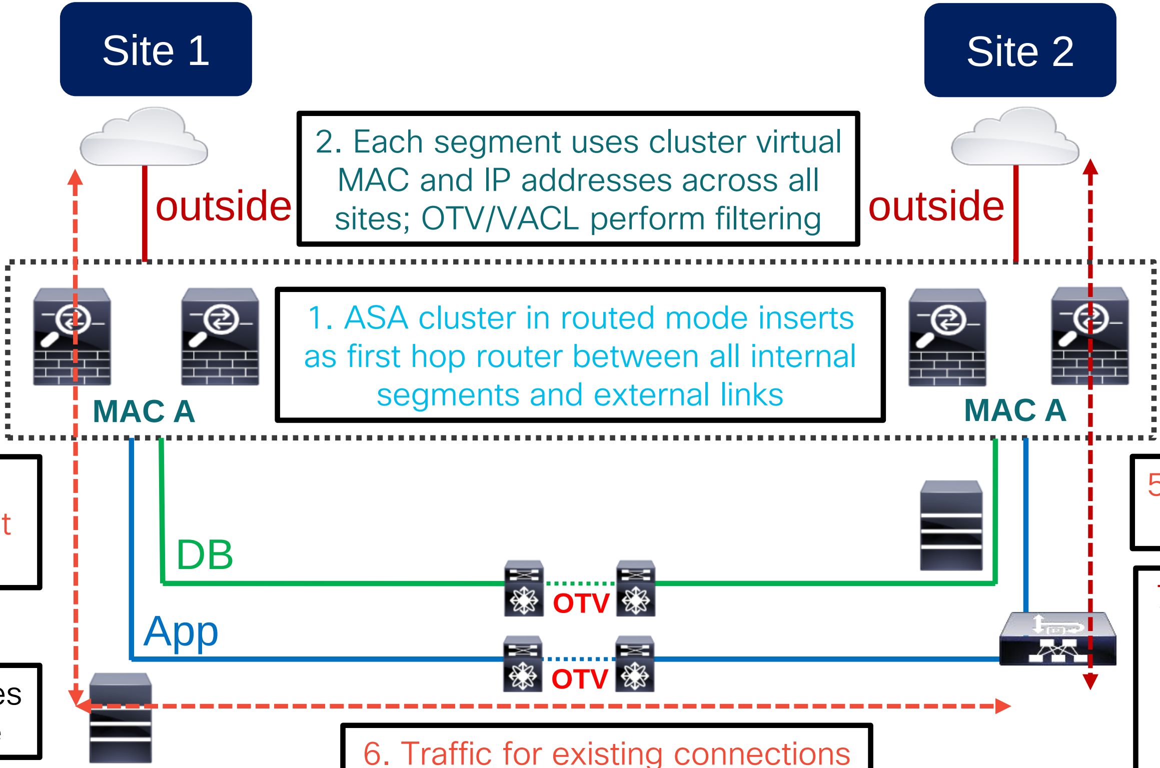
```
interface Vlan101
 ip address 192.168.1.3/24
 hsrp 10
  ip 192.168.1.1
interface Vlan201
 ip address 192.168.2.3/24
 hsrp 20
  ip 192.168.2.1
```

```
mac-list HSRP_MAC seq 10 deny
    0000.0c07.ac00 ffff.ffff.ff00
mac-list HSRP_MAC seq 20 deny
    0000.0c9f.f000 ffff.ffff.ff00
mac-list HSRP_MAC seq 30 permit
    0000.0000.0000 0000.0000.0000
otv-isis default
 vpn Overlay1
  redistribute filter route-map HSRP_MAC
!
ip access-list HSRP_TRAFFIC
 10 permit udp any 224.0.0.2/32 eq 1985
 20 permit udp any 224.0.0.102/32 eq 1985
ip access-list ALL
 10 permit ip any any
vlan access-map HSRP_FILTER 10
 match ip address HSRP_TRAFFIC
 action drop
vlan access-map HSRP_FILTER 20
 match ip address ALL
 action forward
vlan filter HSRP_FILTER vlan-list 100, 200
```

Routed East-West (EW) Inter DC Cluster

ASA 9.5(1)

FTD 6.2



1. ASA cluster in routed mode inserts as first hop router between all internal segments and external links

2. Each segment uses cluster virtual MAC and IP addresses across all sites; OTV/VACL perform filtering

3. Connections establish locally at each site

4. VM live-migrates to a different site

5. New connections establish locally through new site

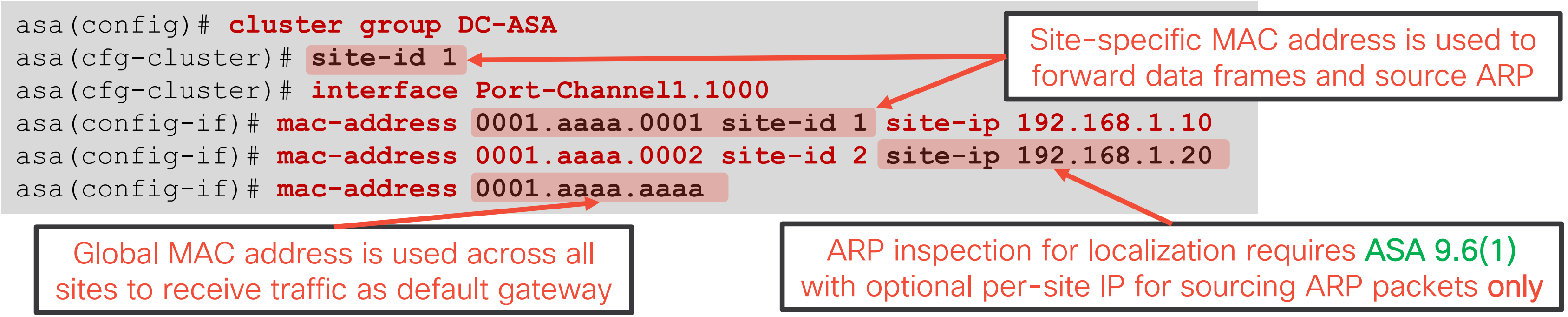
6. Traffic for existing connections traverses the original owner and uses extended data subnet

7. **PROBLEM**: Access switch at new site sees MAC A flapping between local and OTV ports

SOLUTION: Per-site MAC addresses in ASA 9.5(1)

Per-Site MAC Addresses

- Routed Spanned Etherchannel cluster extends MAC addresses in 9.5(1)
  - Global interface MAC address is used to receive and source frames by default
  - Per-site MAC addresses can be used to source frames on extended segments



```
asa(config)# cluster group DC-ASA
asa(cfg-cluster)# site-id 1
asa(cfg-cluster)# interface Port-Channel1.1000
asa(config-if)# mac-address 0001.aaaa.0001 site-id 1 site-ip 192.168.1.10
asa(config-if)# mac-address 0001.aaaa.0002 site-id 2 site-ip 192.168.1.20
asa(config-if)# mac-address 0001.aaaa.aaaa
```

Site-specific MAC address is used to forward data frames and source ARP

Global MAC address is used across all sites to receive traffic as default gateway

ARP inspection for localization requires ASA 9.6(1) with optional per-site IP for sourcing ARP packets **only**

- Dynamic routing is centralized, but **possible** with a shared outside segment
- Global MAC address localization is required by OTV or similar mechanisms

OTV Silent Host Problem

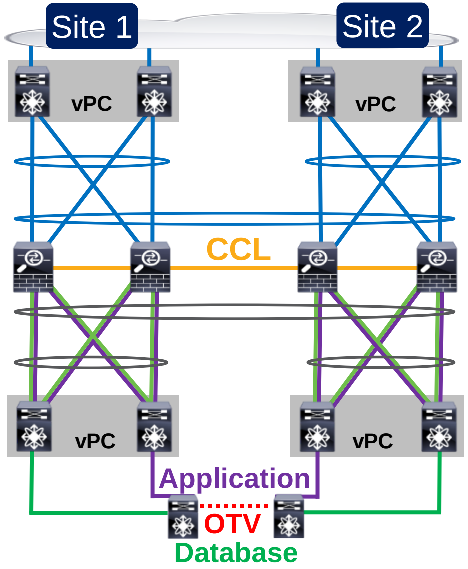
- OTV suppresses unicast flooding for unknown MAC addresses by default
  - Hosts that mostly generate local traffic quickly become unreachable across OTV
  - Recommended to set ARP timeout below MAC address table timeout
- ASA 9.8(3) and FTD 6.2.2.2 replicate ARP replies to all sites
  - Refresh MAC table entries in OTV to partially combat the Silent Host problem
- Cluster global MAC becomes a silent host when per-site MAC is used
  - ASA 9.12(1) and FTD 6.4 generate a periodic GARP for global MAC/IP

```
asa(cfg-cluster)# site-periodic-garp interval 280
```

One unit at each site generates a GARP at this frequency in seconds; default is 280

Example: EW Routed Spanned Cluster

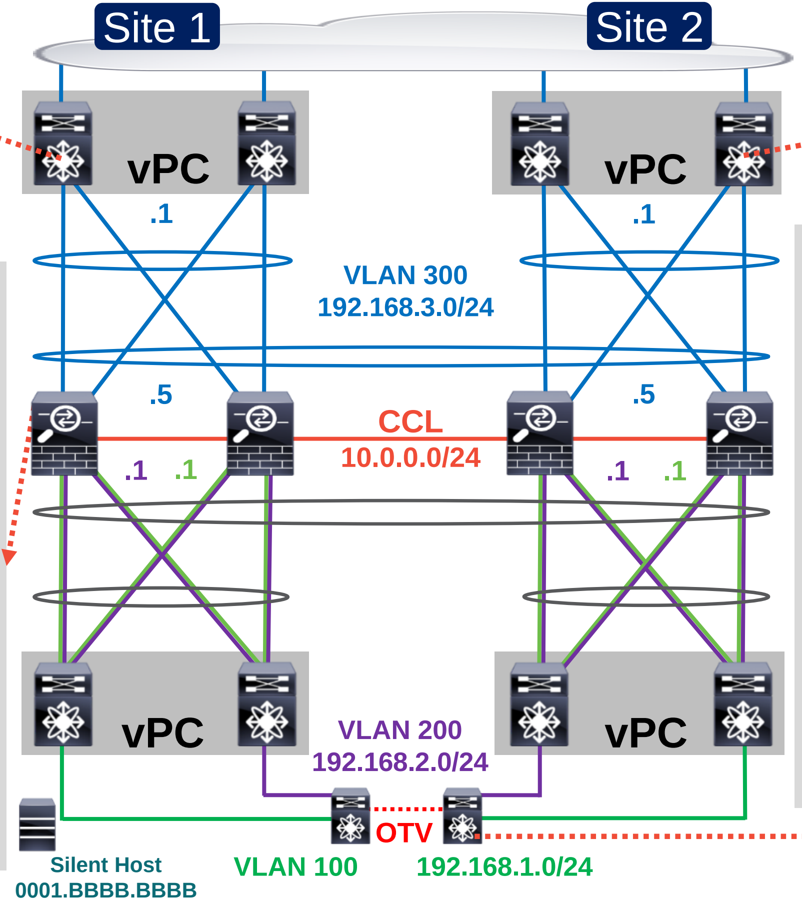
- A vPC pair of Nexus switches at each site
  - Split Spanned Etherchannel cluster in routed mode to separate internal segments
  - Separate Etherchannel to local cluster members per vPC pair
  - Static routing between distribution and core is acceptable
- Internal VLANs are fully extended between sites with OTV
  - Each site uses localized cluster as first hop router
  - Traffic to and from global cluster MAC is blocked between sites
  - Nexus F2 line cards allow VACL filtering without ARP Inspection
  - Must manually remove OTV filters on full upstream path failure
  - One silent host with a very long ARP timeout at site 1



EW Routed Spanned Cluster Configuration

```
interface Vlan300
 ip address 192.168.3.2/24
hsrp 10
  preempt
  ip 192.168.3.1
ip route 192.168.1.0/24 192.168.3.5
ip route 192.168.2.0/24 192.168.3.5
```

```
cluster-group DC-ASA
 site-id 1
interface Port-Channel10
 port-channel span-cluster
 mac-address 0001.aaaa.aaaa
interface Port-Channel10.100
 vlan 100
 nameif DB
 ip address 192.168.1.1 255.255.255.0
 mac-address 0001.aa01.0001 site-id 1
 mac-address 0001.aa01.0002 site-id 2
interface Port-Channel10.200
 vlan 200
 nameif App
 ip address 192.168.2.1 255.255.255.0
 mac-address 0001.aa02.0001 site-id 1
 mac-address 0001.aa02.0002 site-id 2
interface Port-Channel10.300
 vlan 300
 nameif outside
 ip address 192.168.3.5 255.255.255.0
route outside 0.0.0.0 0.0.0.0
          192.168.3.1
```



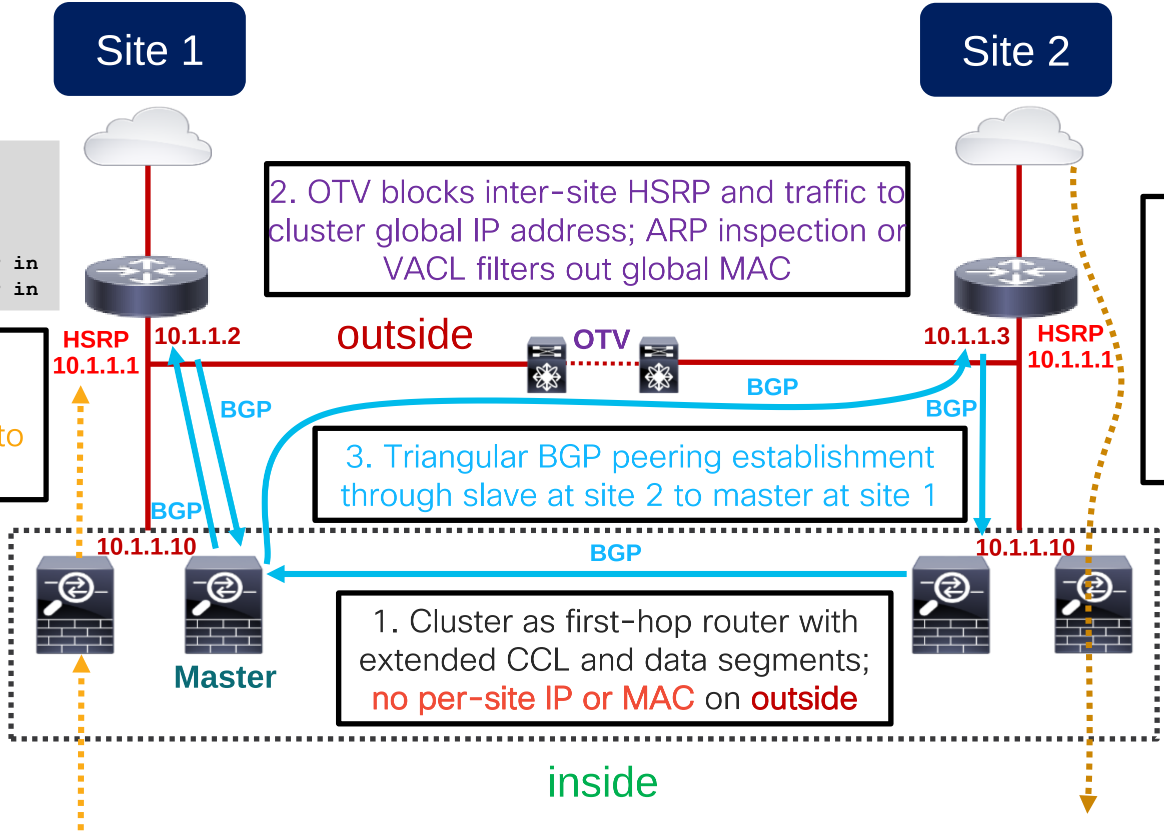
```
interface Vlan300
 ip address 192.168.3.3/24
hsrp 10
  ip 192.168.3.1
ip route 192.168.1.0/24 192.168.3.5
ip route 192.168.2.0/24 192.168.3.5
```

```
mac-list GMAC_FILTER seq 10 deny
       0001.aaaa.aaaa ffff.ffff.ffff
mac-list GMAC_FILTER seq 20 permit
       0000.0000.0000 0000.0000.0000
otv-isis default
 vpn Overlay1
  redistribute filter route-map GMAC_FILTER
!
mac access-list GMAC_TRAFFIC
 10 permit 0001.aaaa.aaaa 0000.0000.0000 any
 20 permit any 0001.aaaa.aaaa 0000.0000.0000
mac access-list ALL
 10 permit any any
vlan access-map FILTER 10
 match mac address GMAC_TRAFFIC
 action drop
vlan access-map FILTER 20
 match mac address ALL
 action forward
vlan filter FILTER vlan-list 100, 200
!
otv flood mac 0001.bbbb.bbbb vlan 100
```

EW Routed Cluster with Upstream BGP

```
route-map NHOP permit 10
 set ip next-hop 10.1.1.1
router bgp 65000
 address-family ipv4 unicast
  neighbor 10.1.1.2 route-map NHOP in
  neighbor 10.1.1.3 route-map NHOP in
```

5. Outbound connections require cluster to rewrite upstream BGP next-hop IP to HSRP address



2. OTV blocks inter-site HSRP and traffic to cluster global IP address; ARP inspection or VACL filters out global MAC

3. Triangular BGP peering establishment through slave at site 2 to master at site 1

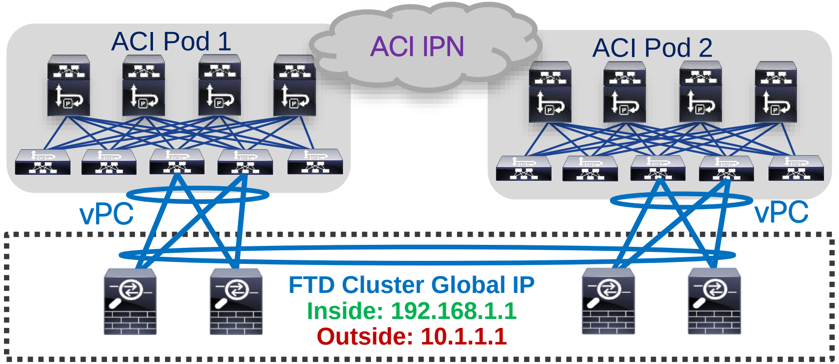
1. Cluster as first-hop router with extended CCL and data segments; no per-site IP or MAC on outside

4. Inbound connections traverse local cluster members via global cluster next-hop IP 10.1.1.10

Inter DC Cluster with ACI Anycast Services

- Routed ASA or FTD as first-hop gateway or PBR node in ACI Multipod
  - Split Spanned Etherchannel insertion with each pod as a separate vPC
- Cluster global interface IP/MAC are configured as Anycast gateways
  - No need for per-site IP/MAC addresses or FTD FlexConfig
  - ACI always directs outgoing traffic to closest cluster member group in local pod
  - Automatic switchover to next closest cluster group with no manual filters on failure

ACI Anycast Service IP: 192.168.1.1, 10.1.1.1



Workloads in Pod 2 direct traffic toward 192.168.1.1 and 10.1.1.1 through local cluster members only; switch to Pod 1 cluster members if no local ones are available

Director Localization and Site Redundancy

- Flow Director selection logic is not site-aware by default
  - A flow owned at one site may select Flow Director at a different site
  - Excessive inter-site traffic on CCL for director lookups is expensive
- Director Localization can be enabled to create two Directors

```
asa(cfg-cluster)# site-id 1
asa(cfg-cluster)# director-localization
```

  - Local Director is at the same site as Flow Owner, primary lookup path

```
TCP outside 85.2.2.123:22 inside 85.2.1.122:58772, idle 0:00:07, bytes 0, flags yl
```

  - Global Director is at a different site from Flow Owner, backup lookup path
  - Lookups for NAT/PAT, IP fragments, or SCTP inspected flows are not localized
- Site Redundancy adds a Director at remote site in ASA 9.9 and FTD 6.2.3

```
asa(cfg-cluster)# site-redundancy
```

Closing Remarks

Clustering Best Practices

- Use a validated switch or verify documented requirements
- Leverage LACP Etherchannel for CCL and dual-connect to VSS/vPC
  - Match the data forwarding capacity of each member
  - Set CCL MTU to 100 bytes above all data interfaces and no less than 1400 bytes
- Speed up switching and routing convergence
  - Enable Spanning Tree Portfast on CCL and data interfaces
  - Use NSF/GR or lower dead interval and SPF throttle timers on cluster and peers
- Reduce asymmetry to increase scale
  - Use firewall-on-a-stick in Spanned Etherchannel mode for best load distribution
  - Minimize centralized features and NAT/PAT

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

cisco Live!

Continue your education

- Demos in the Cisco campus
- Walk-in labs
- Meet the engineer 1:1 meetings
- Related sessions

Thank you

You make **possible**