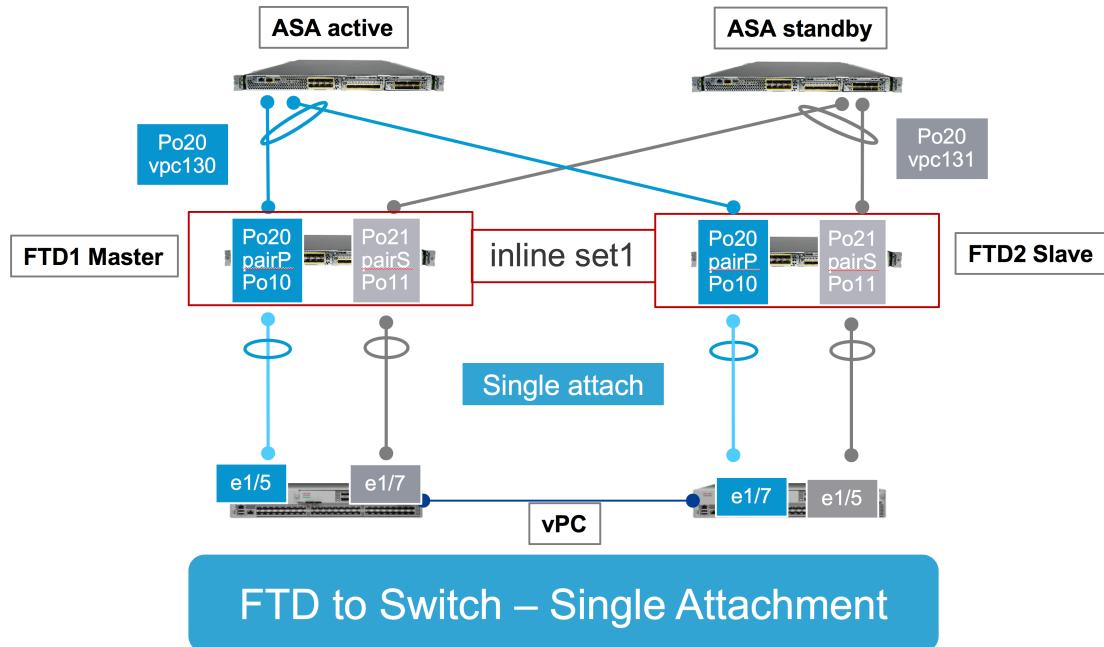
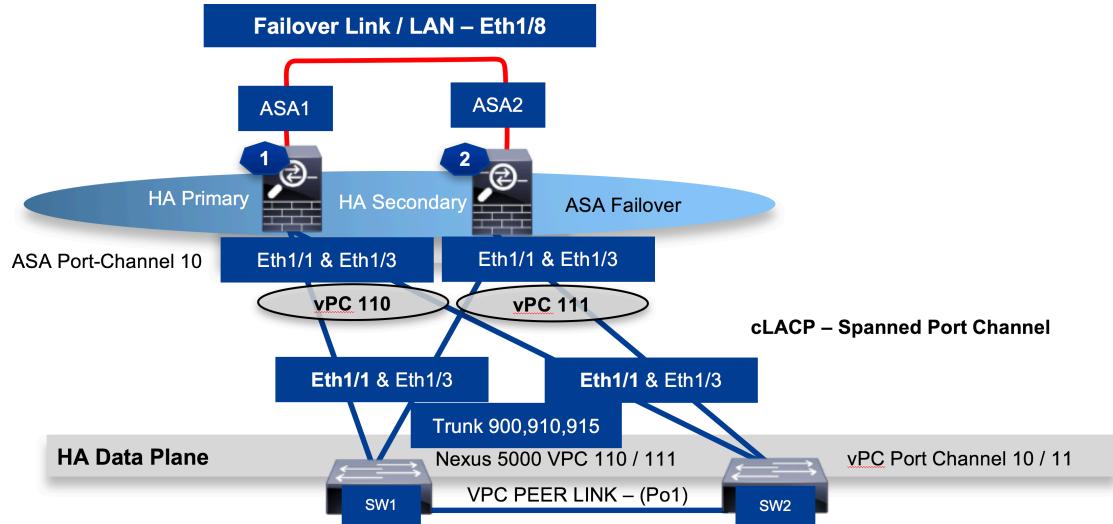


# FTD App Cluster NGIPS with ASA App Failover

## Design Overview



## FPR4100-FTD1-master

Overview **Interfaces** Logical Devices Security Engine Platform Settings System Tools

**FTD1**

All Interfaces	Hardware Bypass	Add Port Channel						
Interface	Type	Admin Speed	Operational Speed	Application	Admin Duplex	Auto Negotiation	Operation State	Admin State
MGMT	Management							
Port-channel10	data	SW1-vpc130	10gbps	10gbps	FTD	Full Duplex	no	up
Ethernet1/1								up
Port-channel11	data	SW1-vpc131	10gbps	10gbps	FTD	Full Duplex	no	up
Ethernet1/3								up
Port-channel20	data	ASA1-Po20	10gbps	10gbps	FTD	Full Duplex	no	up
Ethernet1/5								up
Port-channel21	data	ASA2-vPo21	10gbps	10gbps	FTD	Full Duplex	no	up
Ethernet1/6								up
Port-channel48	cluster	CCL	10gbps	10gbps	FTD	Full Duplex	no	up
Ethernet1/2								up
Ethernet1/4								up
Ethernet1/7	mgmt		1gbps	1gbps	FTD	Full Duplex	no	up
Ethernet1/8	data		10gbps	10gbps		Full Duplex	no	up

## FPR4100-FTD2-slave

Overview **Interfaces** Logical Devices Security Engine Platform Settings System Tools

**FTD2**

All Interfaces	Hardware Bypass	Add Port Channel						
Interface	Type	Admin Speed	Operational Speed	Application	Admin Duplex	Auto Negotiation	Operation State	Admin State
MGMT	Management							
Port-channel10	data	SW2-vpc130	10gbps	10gbps	FTD	Full Duplex	no	up
Ethernet1/1								up
Port-channel11	data	SW2-vpc131	10gbps	10gbps	FTD	Full Duplex	no	up
Ethernet1/3								up
Port-channel20	data	ASA1-Po20	10gbps	10gbps	FTD	Full Duplex	no	up
Ethernet1/5								up
Port-channel21	data	ASA2-vPo21	10gbps	10gbps	FTD	Full Duplex	no	up
Ethernet1/6								up
Port-channel48	cluster	CCL	10gbps	10gbps	FTD	Full Duplex	no	up
Ethernet1/2								up
Ethernet1/4								up
Ethernet1/7	mgmt		1gbps	1gbps	FTD	Full Duplex	no	up
Ethernet1/8	data		10gbps	10gbps		Full Duplex	no	up

## FMC Configuration

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help aciadmin

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

By Group Add... Device Name

Name	Group	Model	License Type	Access Control Policy
Ungrouped (1)				
FTDCluster Cisco Firepower 4150 Threat Defense Cluster				
FTD1(Master) 10.82.7.97 - Cisco Firepower 4150 Threat Defense - v6.2.1 - transparent		Cisco Firepower 4150 Threat Defense	Base, Threat, Malware, URL Filtering	NGIPS_Policy
FTD2 10.82.7.98 - Cisco Firepower 4150 Threat Defense - v6.2.1 - transparent		Cisco Firepower 4150 Threat Defense	Base, Threat, Malware, URL Filtering	NGIPS_Policy

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN ▾ QoS Platform Settings FlexConfig Certificates

**FTDCluster**  
Cisco Firepower 4150 Threat Defense

**Interfaces**

Status	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Up	Port-channel10	ASAp_to_FTD	EtherChannel	north_zone		
Up	Port-channel20	p_FTD_to_Switch	EtherChannel	south_zone		
Up	Port-channel21	s_FTD_to_Switch	EtherChannel	south_zone		
Up	Port-channel48		EtherChannel			
Up	Ethernet1/7	diagnostic	Physical			
Up	Port-channel11	ASAs_to_FTD	EtherChannel	north_zone		

Overview Analysis Policies **Devices** Objects | AMP Intelligence

Device Management NAT VPN ▾ QoS Platform Settings FlexConfig Certificates

## FTDCluster

Cisco Firepower 4150 Threat Defense

**Cluster Device Routing Interfaces **Inline Sets****

Name	Interface Pairs
All_Pairs	ASAp_to_FTD<->p_FTD_to_Switch, s_FTD_to_Switch<->ASAs_to_FTD

Overview Analysis **Policies** Devices Objects AMP Intelligence

Access Control ▾ Access Control

Network Discovery Application Detectors Correlation Actions ▾

**NGIPS\_Policy**

Prefilter Policy: Default Prefilter Policy SSL Policy: None Identity Policy: None

Inheritance Settings | Policy Assignments (1)

**Rules** Security Intelligence HTTP Responses Advanced

Filter by Device Show Rule Conflicts Add Category Add Rule Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	ISE/SGT Attributes	Action
1	(1)SSH App on 22	north_zone	south_zone	Any	Any	920	Any	SSH	Any	TCP (6):22	Any	Any	Allow
2	(1)Block SSH elsewhere	Any	Any	Any	Any	920	Any	OpenSSH	Any	Any	Any	Any	Block with re
3	(1)Block non-SSH on	Any	Any	Any	Any	920	Any	SSH	Any	Any	Any	Any	Block with re
4	Permit All	Any	Any	Any	Any	920	Any	Any	Any	Any	Any	Any	Allow
5	(2)SSH App on 22	south_zone	north_zone	Any	Any	925	Any	SSH	Any	TCP (6):22	Any	Any	Allow
6	(2)Block non-SSH on	Any	Any	Any	Any	925	Any	SSH	Any	Any	Any	Any	Block with re
7	Permit all	Any	Any	Any	Any	925	Any	Any	Any	Any	Any	Any	Allow

Default - NGIPS\_Policy (-)  
There are no rules in this section. Add Rule or Add Category

Default Action Access Control: Block All Traffic