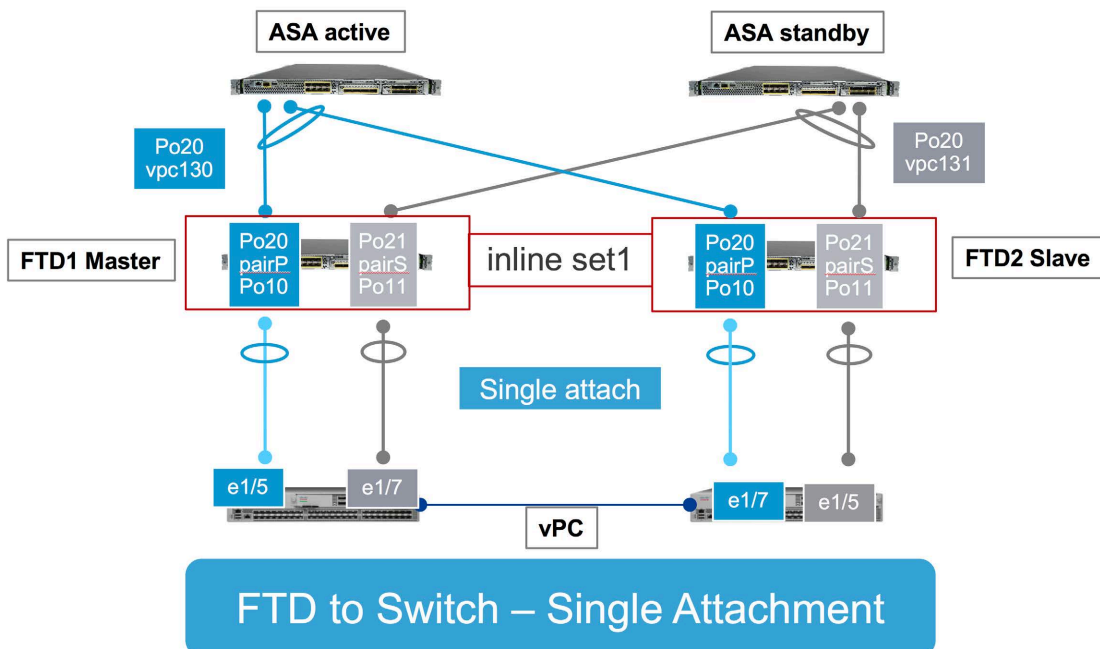
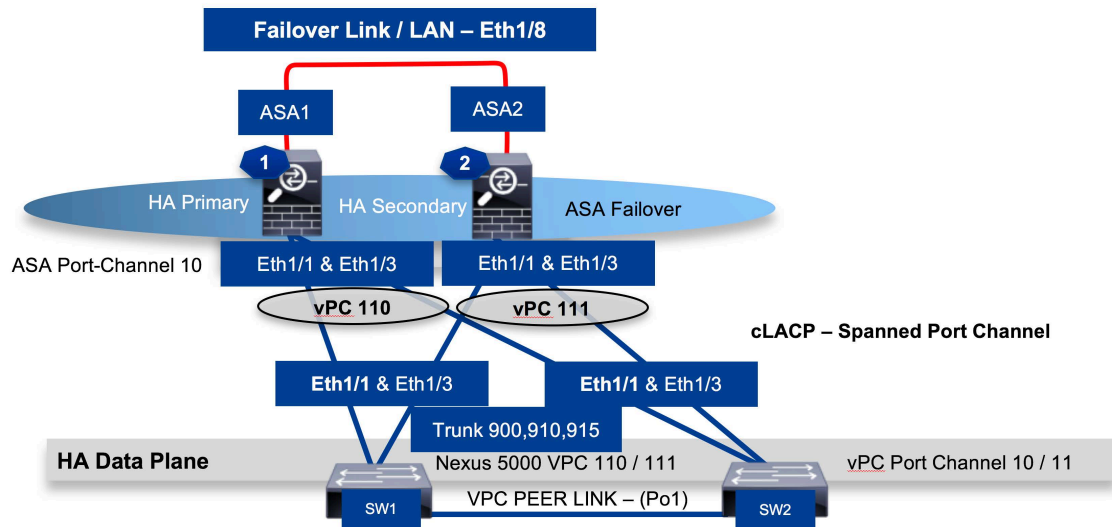


FTD App Cluster NGIPS with ASA App Failover

Design Overview



FPR4100-FTD1-master

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

FTD1

CONSOLE MGMT USB Network Module 1: 1, 3, 5, 7, 2, 4, 6, 8. Network Module 2: Empty. Network Module 3: Empty.

All Interfaces Hardware Bypass

Interface	Type	Admin Speed	Operational Speed	Application	Admin Duplex	Auto Negotiation	Operation State	Admin State
MGMT	Management							<input checked="" type="checkbox"/>
Port-channel10	data	SW1-vpc130	10gbps	10gbps	FTD	Full Duplex	no	up
Ethernet1/1	data	SW1-vpc131	10gbps	10gbps	FTD	Full Duplex	no	up
Port-channel11	data	SW1-vpc131	10gbps	10gbps	FTD	Full Duplex	no	up
Ethernet1/3	data	ASA1-Po20	10gbps	10gbps	FTD	Full Duplex	no	up
Port-channel20	data	ASA1-Po20	10gbps	10gbps	FTD	Full Duplex	no	up
Ethernet1/5	data	ASA1-Po20	10gbps	10gbps	FTD	Full Duplex	no	up
Port-channel21	data	ASA1-Po20	10gbps	10gbps	FTD	Full Duplex	no	up
Ethernet1/6	data	ASA1-Po20	10gbps	10gbps	FTD	Full Duplex	no	up
Port-channel48	cluster	CCL	10gbps	10gbps	FTD	Full Duplex	no	up
Ethernet1/2	data							up
Ethernet1/4	data							up
Ethernet1/7	mgmt		1gbps	1gbps	FTD	Full Duplex	no	up
Ethernet1/8	data		10gbps	10gbps	FTD	Full Duplex	no	up

FPR4100-FTD2-slave

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

FTD2

CONSOLE MGMT USB Network Module 1: 1, 3, 5, 7, 2, 4, 6, 8. Network Module 2: Empty. Network Module 3: Empty.

All Interfaces Hardware Bypass

Interface	Type	Admin Speed	Operational Speed	Application	Admin Duplex	Auto Negotiation	Operation State	Admin State
MGMT	Management							<input checked="" type="checkbox"/>
Port-channel10	data	SW2-vpc130	10gbps	10gbps	FTD	Full Duplex	no	up
Ethernet1/1	data	SW2-vpc131	10gbps	10gbps	FTD	Full Duplex	no	up
Port-channel11	data	SW2-vpc131	10gbps	10gbps	FTD	Full Duplex	no	up
Ethernet1/3	data	ASA1-Po20	10gbps	10gbps	FTD	Full Duplex	no	up
Port-channel20	data	ASA1-Po20	10gbps	10gbps	FTD	Full Duplex	no	up
Ethernet1/5	data	ASA1-Po20	10gbps	10gbps	FTD	Full Duplex	no	up
Port-channel21	data	ASA1-Po20	10gbps	10gbps	FTD	Full Duplex	no	up
Ethernet1/6	data	ASA1-Po20	10gbps	10gbps	FTD	Full Duplex	no	up
Port-channel48	cluster	CCL	10gbps	10gbps	FTD	Full Duplex	no	up
Ethernet1/2	data							up
Ethernet1/4	data							up
Ethernet1/7	mgmt		1gbps	1gbps	FTD	Full Duplex	no	up
Ethernet1/8	data		10gbps	10gbps	FTD	Full Duplex	no	up

FMC Configuration

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

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

OverviewAnalysisPolicies**Devices**ObjectsAMPIntelligence

Device ManagementNATVPNQoSPlatform SettingsFlexConfigCertificates

DeploySystemHelpaciadmin

FTDClusterCisco Firepower 4150 Threat Defense

ClusterDeviceRouting**Interfaces**Inline Sets

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

OverviewAnalysisPolicies**Devices**ObjectsAMPIntelligence

Device ManagementNATVPNQoSPlatform SettingsFlexConfigCertificates

FTDClusterCisco Firepower 4150 Threat Defense

ClusterDeviceRouting**Interfaces**Inline Sets

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

OverviewAnalysis**Policies**DevicesObjectsAMPIntelligence

Access ControlAccess ControlNetwork DiscoveryApplication DetectorsCorrelationActions

DeploySystemHelpaciadmin

NGIPS_Policy

Prefilter Policy: Default Prefilter PolicySSL Policy: NoneIdentity Policy: None

Inheritance SettingsPolicy Assignments (1)

RulesSecurity IntelligenceHTTP ResponsesAdvanced

Filter by DeviceShow Rule ConflictsAdd CategoryAdd RuleSearch Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	TSE/SGT Attributes	Action
Mandatory - NGIPS_Policy (1-7)													
Inside_1 (1-4)													
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
Inside_2 (5-7)													
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 ActionAccess Control: Block All Traffic													