Logical Firewall for Highly Resilient Networks

Scalable and Resilient NGFW Designs with Cisco Firepower Appliances

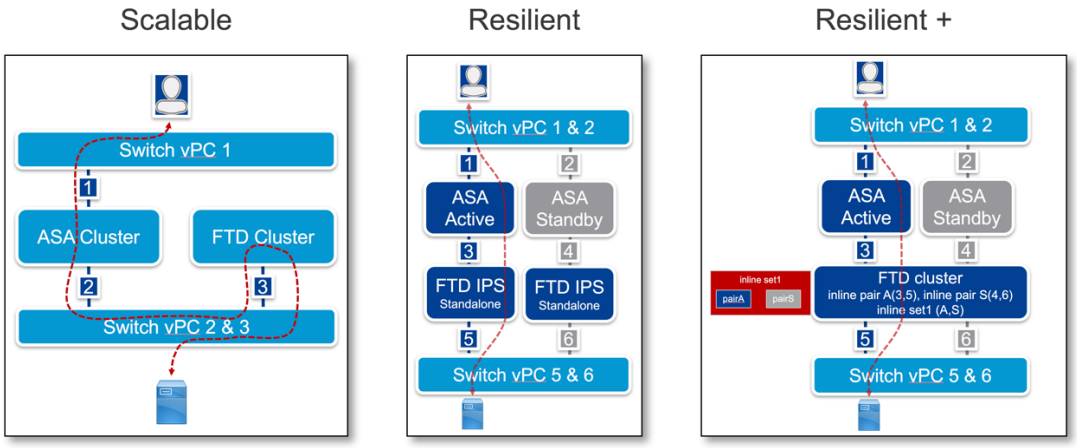
Introduction

Cisco Firepower 9300 and 4100 Series appliances offer fully integrated threat defense solutions with the ability to separate the firewall from next generation intrusion prevention (NGIPS) and advanced malware protection (AMP) capabilities based on security need. The flexibility to run either ASA or FTD (Firepower Threat Defense) software on the Firepower appliances, extends multiple benefits to customers:

- Organizations that have strict administrative boundaries between threat and network operation teams, can separate hardware and software by function.
- Customer networks with multiple security vendors can use the latest hardware and choose the capabilities they require: traditional stateful inspection firewalling, NGIPS, AMP, etc. In the future as their needs change, the same Firepower appliances can be updated to support different features or all features in a single appliance.
- Firepower 9300 and 4100 appliances offer resiliency and scalability through both ASA and FTD software clustering. Expanding network needs can be supported with our scalable security solutions, combining up to 16 physical appliances into one entity, easily managed as one single logical traditional firewall or NGIPS or NGFW.
- Customers running ASA5585-X with FirePOWER services (ASA software and FirePOWER features running within a single appliance) can upgrade to Firepower 4100 40G speeds, while maintaining the same 4RU footprint. Using the ASA and FTD software, new Firepower 9300 and 4100 Series appliances in resilient designs can achieve the same or better capabilities as compared to ASA5585-X.

This document provides technical details on the wiring and configuring of both ASA and FTD based Firepower (FPR) 4100 Series appliances.

There are three primary designs that can be used with ASA and FTD software, running on their dedicated FPR4100s:



1. **Scalable NGFW design** – solution that can elastically grow in scale (throughput, Connections per Second (CPS), etc.)
    a. Two or more ASA based devices in cluster mode with multiple contexts in either Routed (L3FW) or Transparent (L2FW) mode.
    b. Two or more FTD based devices run in cluster mode with transparent mode BVIs (Bridge-Groups) and NGFW and AMP features applied to match ASA contexts.

Using clustering, scalable design allows us to size each application (ASA and FTD) independently according to the throughput requirements. Further, each application has its own fault tolerance domain, where failure of an ASA unit inside a cluster would not affect FTD packet flow or capacity.

2. **Resilient NGFW design** – solution is comparable to ASA 5585-X appliance with FirePOWER services from a functionality perspective
    a. Two ASA based devices in failover configuration run multiple contexts in either Routed (L3FW) or Transparent (L2FW) mode. Failover Active/Active can equally be deployed.
    b. Two standalone FTD based devices run in NGIPS mode, inline pairing ASA port-channels.

Resilient design offers a well-tested traditional IPS deployment model that is simplest to implement. It is most similar to ASA with FirePOWER services from behavior and configuration perspective.

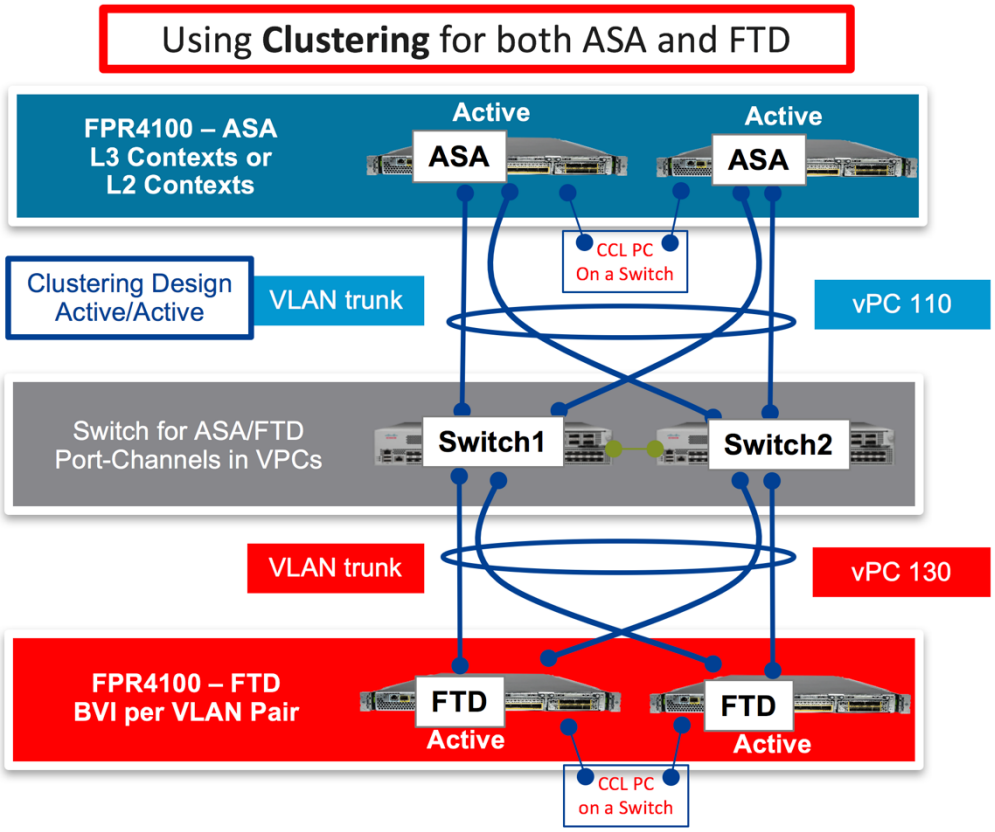
3. **Resilient+ NGFW Design Extension** – an extension to the Resilient design that places FTD based devices into a cluster where each cluster member is directly connected to the primary ASA based device with a virtual port channel and to the secondary ASA with a different virtual port channel.

Resilient+ improves on the resilient design by allowing FTD units to cluster and load-share NGIPS/AMP inspection. FTD inspection capacity can be sized to match the throughput requirements

by adding additional FTD units into the cluster. Lastly, similar to scalable design, FTD Access Control Policies are fully stateful.

Scalable NGFW Design

To enable scale, we can use a cluster of 4100's running ASA software code in front of a cluster of 4100's running FTD code. Each cluster started as a pair of devices to eliminate asymmetry in any deployment. Each cluster can be expanded to the limits of the respective clustering mechanism (16 units in most cases).



ASA Application

The ASA spanned Etherchannel cluster is setup in L3 Routed mode, where each cluster member responds to the same virtual IP address and mac address allowing the switch to use vPC to combine them into one firewall.

When starting a cluster deployment, the first step is to ensure that the switch being used and the code running on it supports clustering. This can be critical and if it isn't supported than it can cause many problems such as both ASA's thinking they are master. Refer to below link for supported devices for ASA clustering.

http://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asamatrx.html - pgfId-137822

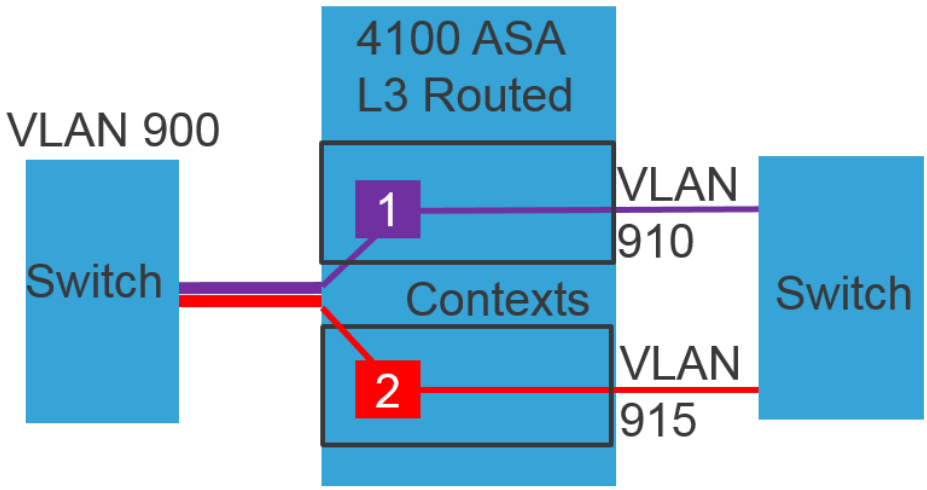
On FPR4100's, FXOS is used to provision an ASA app and its membership in the cluster. For detailed review of this setup, refer to below collection of videos on this setup:

YouTube link: http://cs.co/asa-on-firepower

YouTube link: http://cs.co/ftd-on-firepower

When setting up the cluster in FXOS, refrain from filling in the site id field, unless you know you need it for multi-site DC deployments.

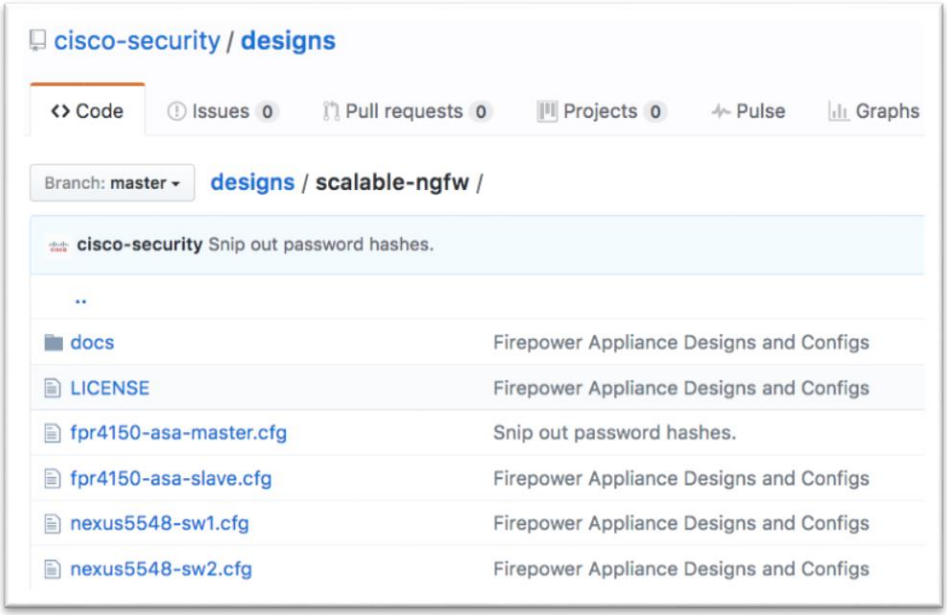
The port-channels that were setup in FXOS as trunk ports carry both the outside and any inside or DMZ VLANs. In the case shown below, the outside VLAN was 900 and used the 10.10.10.0/24 subnet. The ASA cluster was setup with 2 contexts, con1 and con2, each with an IP address in the shared outside subnet. Each has a unique inside interface on a different VLAN, 910 or 915. If there were DMZ interfaces, you could create an additional trunked interface on each context.



ASA (master and slave) units and Nexus5548 Switches in vPC Configuration can be found at:

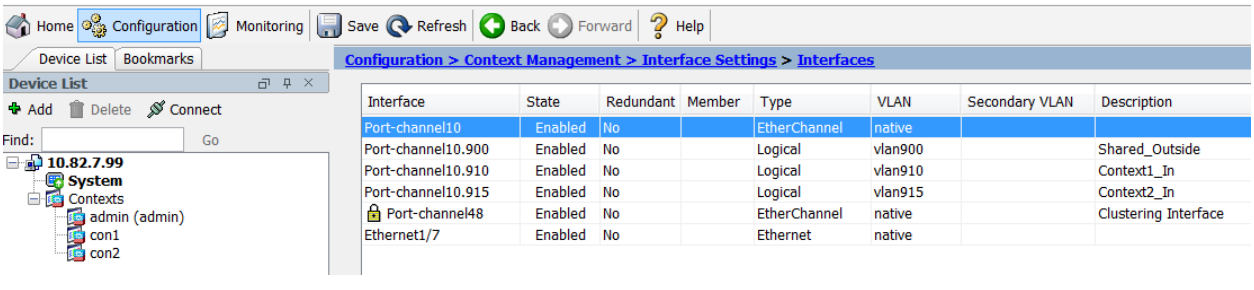
https://github.com/cisco-security/designs/tree/master/scalable-ngfw

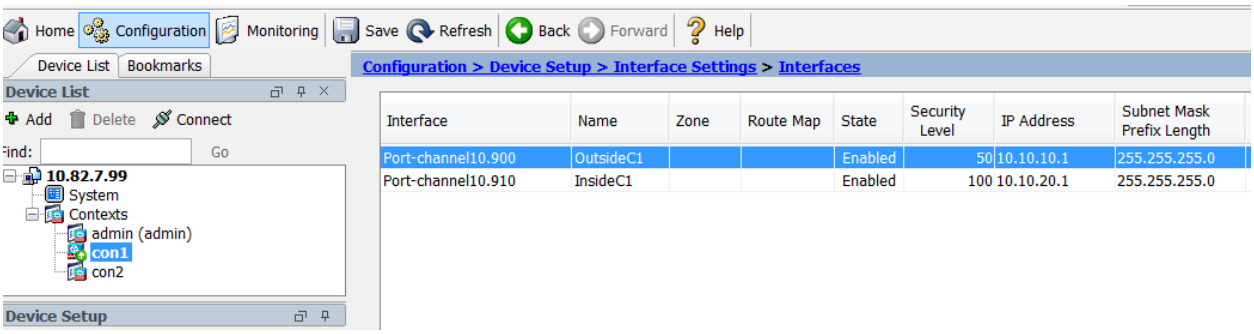
fpr4150-asa-master.cfg contains system, admin, con1, and con2 context configurations. Inside system context, data-link port-channel VLAN sub-interfaces are assigned to appropriate user contexts.

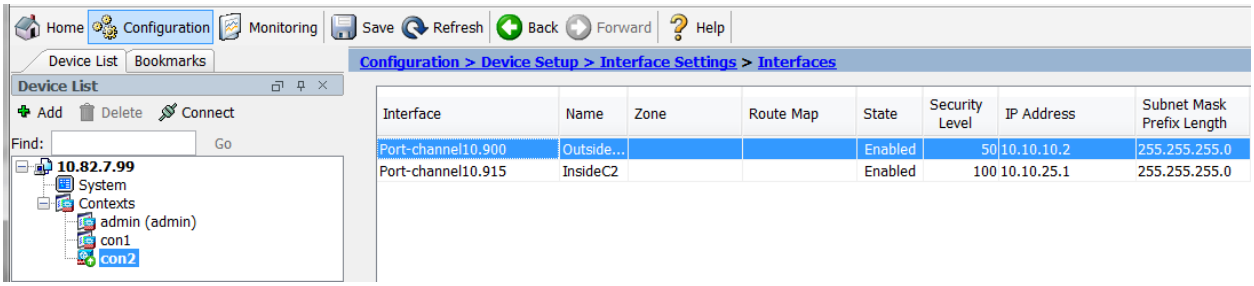


Policy for each context is built as normal in ASA. Normal ASA context rules apply and each context contains all the appropriate rules to control the traffic flowing through that context. Interfaces are assigned to each context from the admin context. VLAN 900 is shared on both contexts as the outside network.

See below ASDM screenshots of System, con1, and con2 context interfaces.

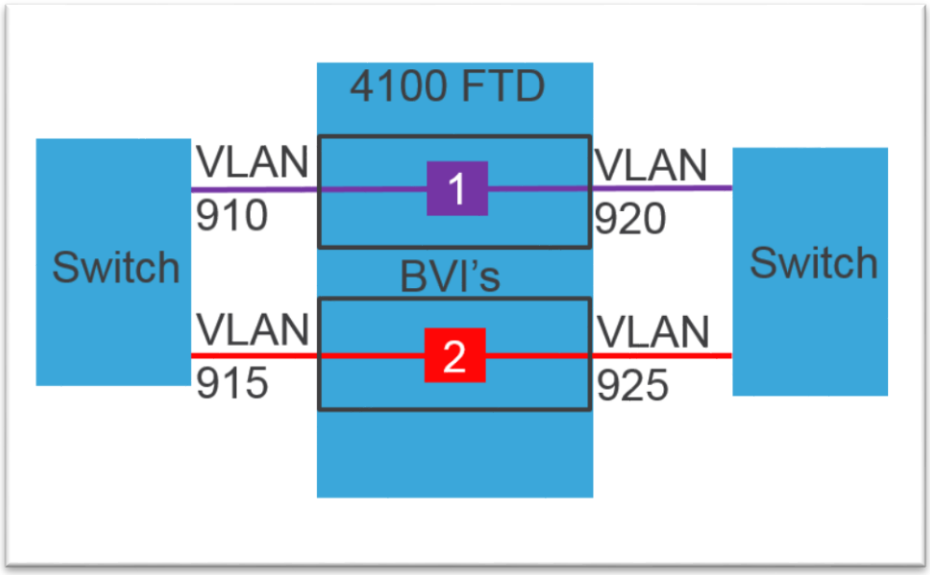






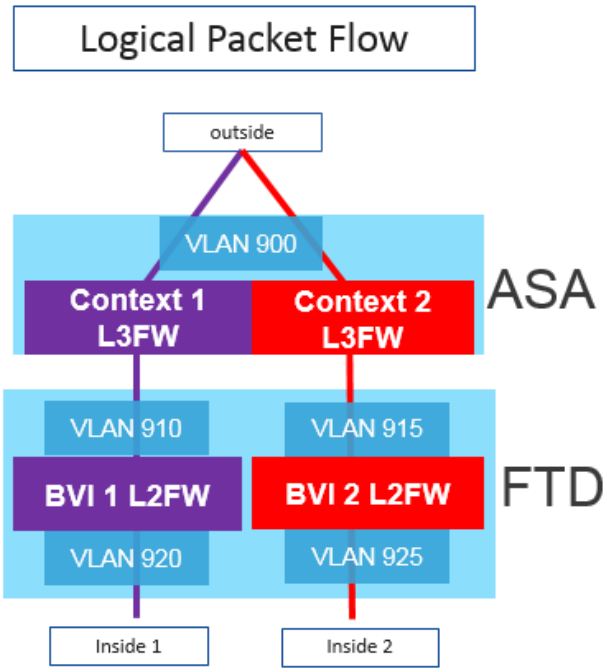
FTD

Once the packets come back to the switch, an additional set of port-channeled interfaces pick the packets up on VLAN 910 and 915 and bring them to the NGFW cluster. Two Firepower4150s are setup in a cluster mode running FTD software in L2 Transparent mode with BVIs. In FTD, we created a subinterface on the port-channel for every VLAN, 910, 915, 920, and 925. We then paired up the subinterfaces into BVIs, 910 to 920 and 915 to 925.

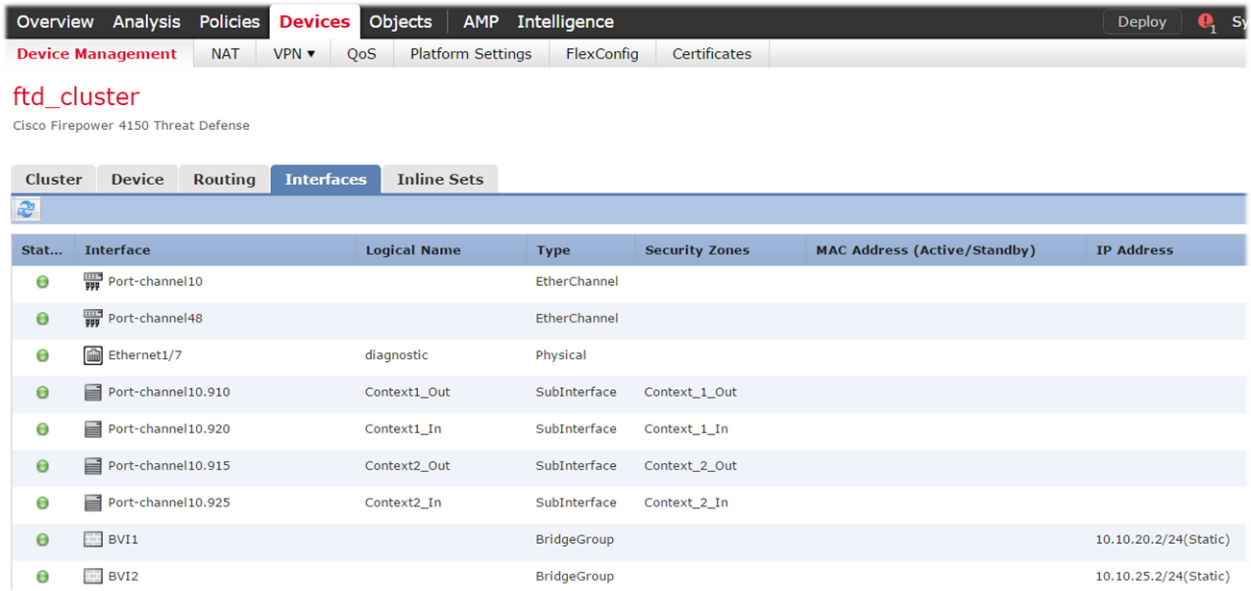


Before FTD enables a multi-context feature in its upcoming releases, we can use existing FTD functionality to isolate traffic and policies. Using BVIs in FTD transparent mode keeps the traffic flowing only between interfaces assigned to the same bridge-group. Packets that enter on an interface assign to BVI 1 should exit only on BVI 1 and the same for any BVI being used. This accomplishes FTD traffic isolation, matching the contexts in ASA. If we had three contexts on the ASA, that simply use outside and inside interfaces, we would create three BVIs to handle the packet flow through FTD. Similarly, if we had additional interfaces on ASA context, like a DMZ, we would need to add additional BVIs for each

egress interface in that context. See below logical diagram which shows how we match up the 2 ASA contexts with the 2 FTD BVIs.

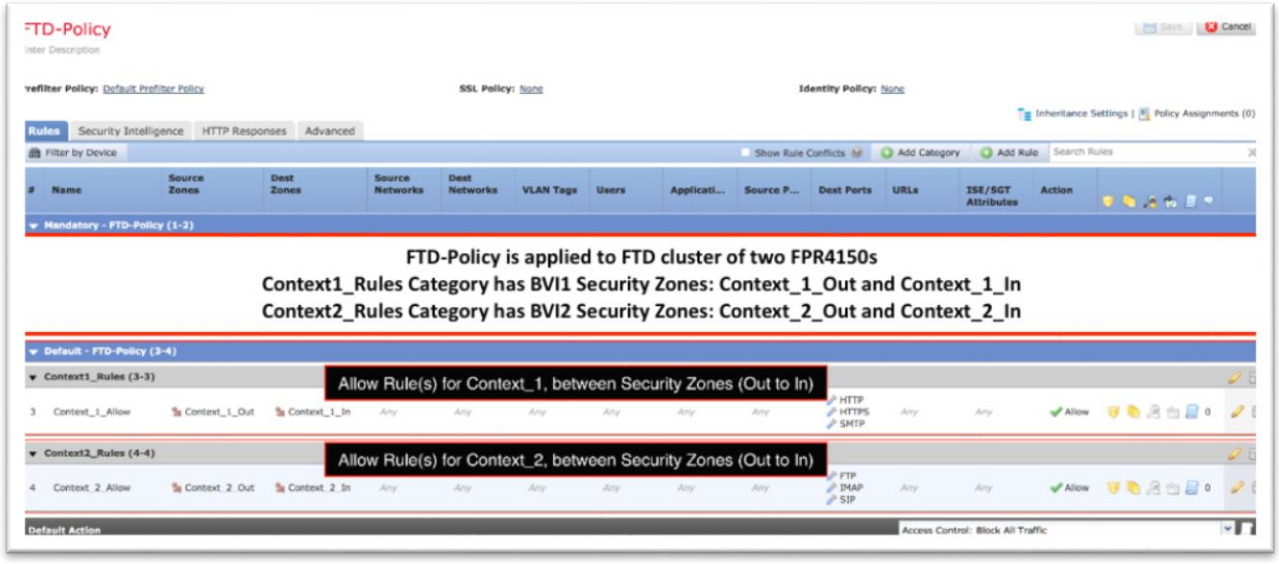


Additional controls in terms of policies can be imposed by using security zones and their assignment into dedicated ACP rules for each BVI. If we define a security zone per BVI sub-interface, we can then build policy rules that are specific to the BVIs. The following FMC screenshot shows assignment of security zones to their appropriate BVI port-channel sub-interface.

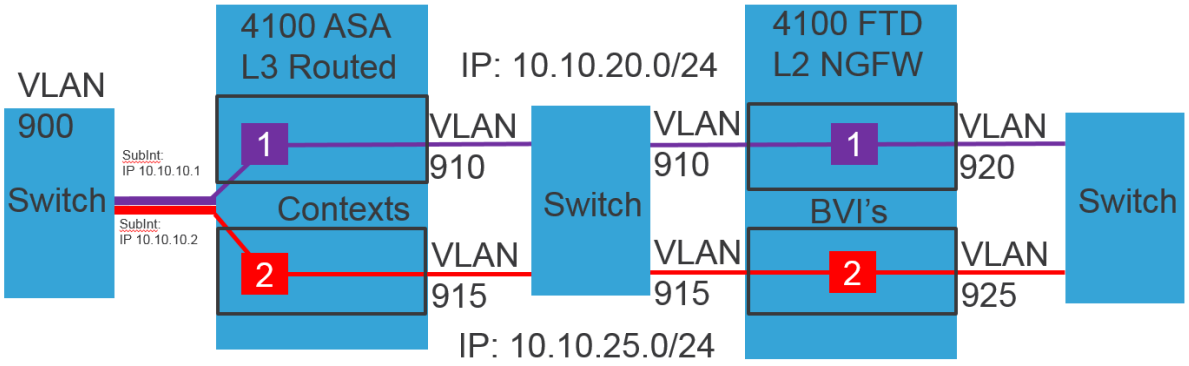


Stat...	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
	Port-channel10		EtherChannel			
	Port-channel48		EtherChannel			
	Ethernet1/7	diagnostic	Physical			
	Port-channel10.910	Context1_Out	SubInterface	Context_1_Out		
	Port-channel10.920	Context1_In	SubInterface	Context_1_In		
	Port-channel10.915	Context2_Out	SubInterface	Context_2_Out		
	Port-channel10.925	Context2_In	SubInterface	Context_2_In		
	BVI1		BridgeGroup			10.10.20.2/24(Static)
	BVI2		BridgeGroup			10.10.25.2/24(Static)

Using this approach, we can build an FMC policy where the configuration for one ASA context/FTD BVI is grouped in a category and separated from the configuration for any other context/BVI. Below FMC screenshot shows how we separate rules into BVI1 and BVI2 categories.



Now we can review our scaling NGFW design, with ASA contexts and FTD BVIs applied to independent traffic paths. See below diagram of the logical packet flow:



Hosts and services on either VLAN 920 or 925 can talk to the outside world on VLAN 900 and beyond and have a L3/L4 policy built in an ASA context and zone-based FTD policy for application, content and threat related protections. This scalable NGFW solution enforces traffic isolation between contexts/BVIs, and allows FTD policy separation by using security zones and FMC ACP categories.

Testing

Scalable NGFW design was tested in a variety of simulated failure scenarios. This could be testing the failure of a single port and a group of ports connecting a device to the switch. Both data and cluster

control link ports were tested. Then we proceed to test traffic impact of device failures, either switch, FPR4150-ASA or FPR4150-FTD. The failures were tested using a variety of test flows including TCP, UDP, and ICMP. In each case, high-availability built into clustering and vPC features guarantied connection survival and quick recovery. All failure tests are captured in a collection of videos found here:

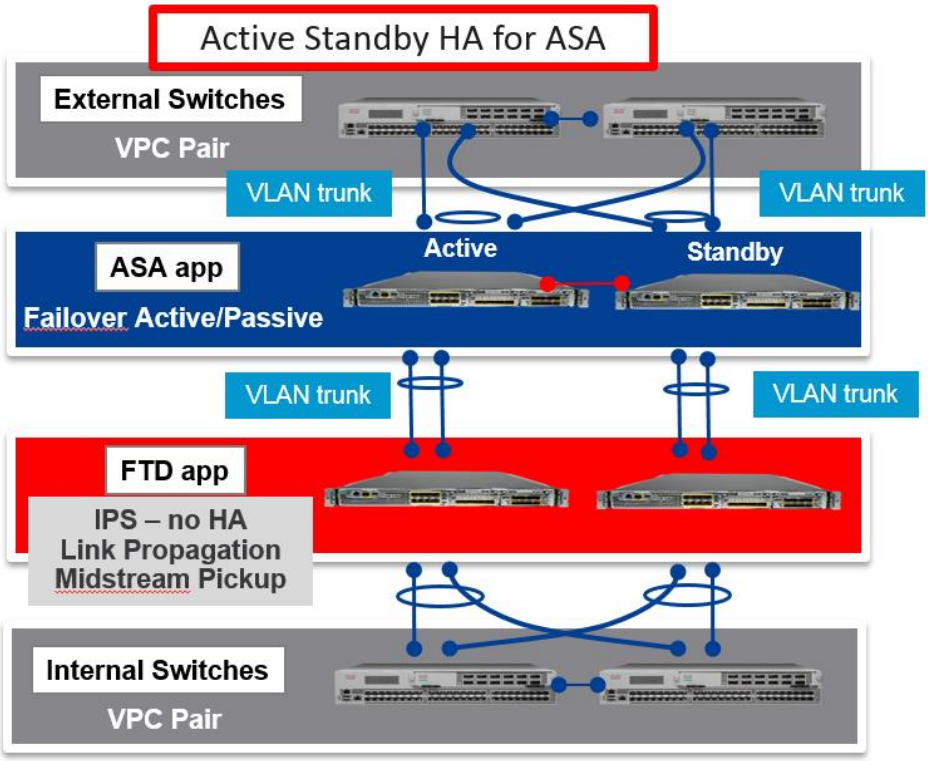
YouTube link: http://cs.co/asa-on-firepower

YouTube link: http://cs.co/ftd-on-firepower

Because ASA devices were setup as a cluster and FTD devices were clustered, each test that impacted the path of an active flow of packets resulted in either the switch or device moving packets to another port in a port channel without impact. If the port channel was completely down for the device, then the flow was moved to the other device in the cluster. In either case, ASA or FTD, changing the packet flow through one cluster because of a failure didn't change the path through the other cluster, which was the expected result of two independent clusters.

Resilient NGFW Design

To enable resilience, a pair of 4100's running ASA code are deployed in Active Standby HA. Behind each ASA, directly connected to the ASA, sits a 4100 running FTD deployed in interface pairing mode (NGIPS style deployment).

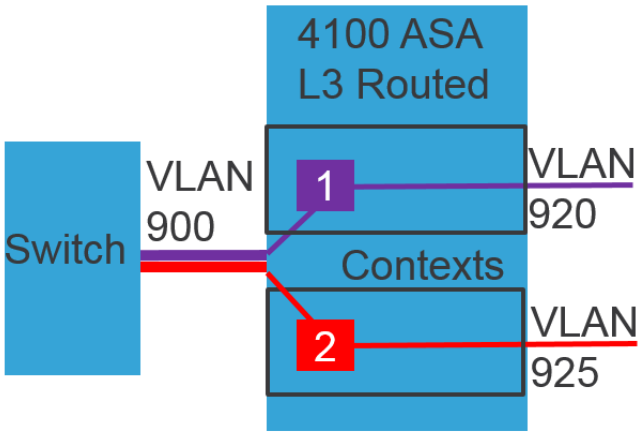


ASA Application

The ASA Active Standby HA pair is setup in L3 Routed mode. The active ASA has the active IP and Active MAC and the standby box has the standby IP and MAC.

On FPR4100's, FXOS is used to provision the ASA app, but as opposed to clustering, HA is not configured within FXOS.

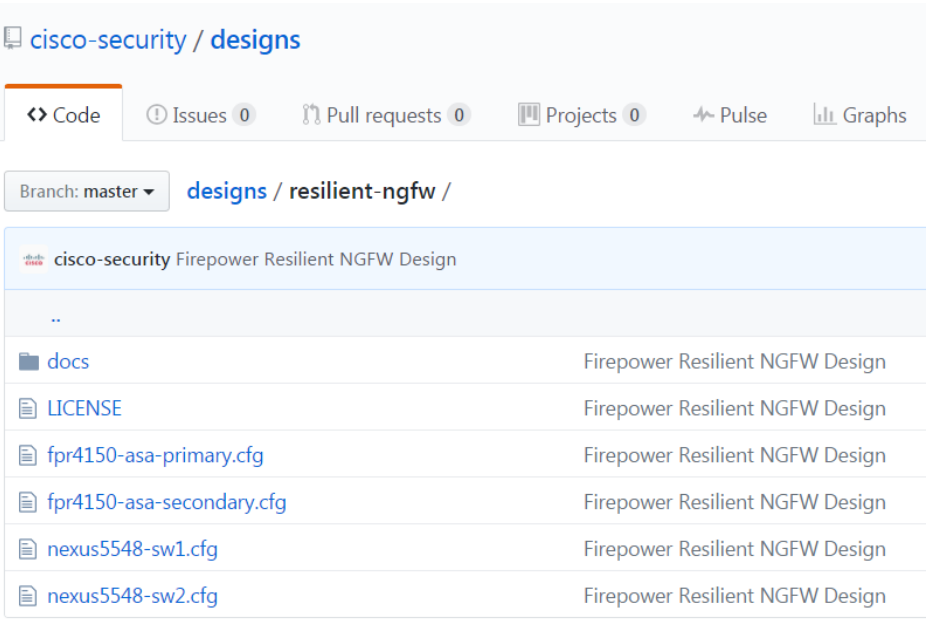
An outside port channel, Po10 was setup with the outside VLAN 900. The ASA was setup in multi context mode, Con1 and Con2, and each context shares the outside interface and has a unique IP address assigned to it. An inside port channel, Po30, was created to connect directly to the 4100 running FTD. This port channel has 2 VLANs assigned to it, 920 and 925. Each context on the ASA is assigned one of the VLANs and has an IP address on the subnet on that VLAN.



ASA (Active and Standby) units and Nexus5548 Switches in vPC Configuration can be found at:

https://github.com/cisco-security/designs/tree/master/resilient-ngfw

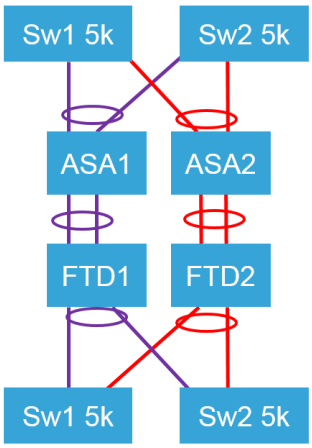
fpr4150-asa-primary.cfg contains system, admin, con1, and con2 context configurations. Inside system context, data-link port-channel VLAN sub-interfaces are assigned to appropriate user contexts.



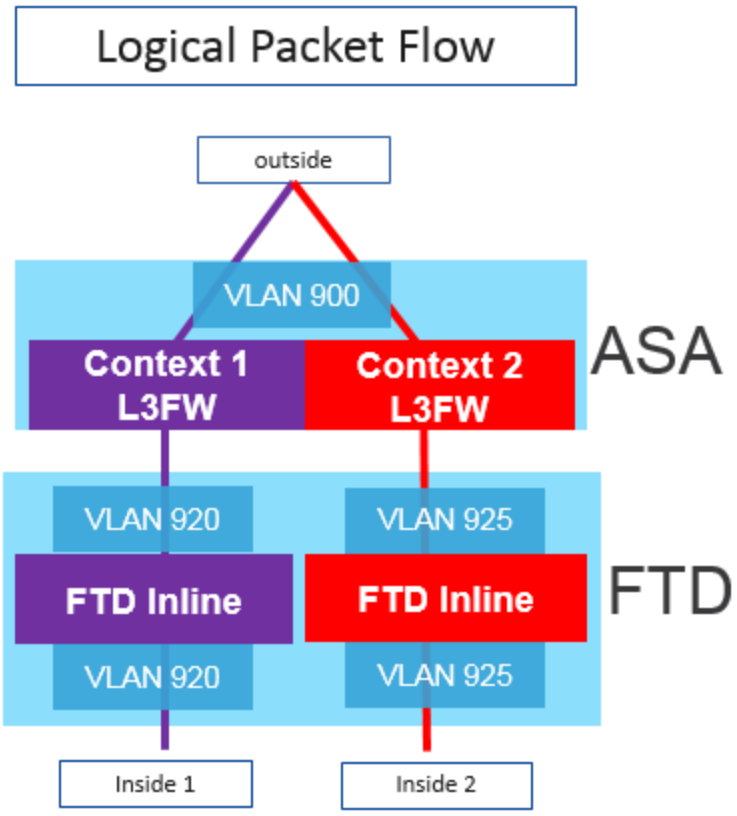
Policy for each context is built as normal in ASA. Normal ASA context rules apply and each context contains all the appropriate rules to control the traffic flowing through that context. Interfaces are assigned to each context from the admin context. VLAN 900 is shared on both contexts as the outside network.

FTD Application

Because the interfaces from ASA go directly to FTD, the setup for FTD in interface pairing mode is a bit different than a standard IPS appliance creating interface pairs. ASA requires that the 2 ports leaving the port channel to the FTD device be a port channel because they are a logical interface. Because FXOS handles all port channel duties, these get created on both ASA and FTD 4100's.



The result is that ASA passes traffic off on trunk port carrying VLAN's 920 and 925 and because these trunk ports are going through interface paired ports on FTD, they are not modified and exit FTD on the same VLANs they entered on. Interface pairing ensures traffic segregation because the flow of packets is unaltered and remain on the VLANs they entered on without any ability to have them put on different VLANs.



Since we are deploying FTD in interface pairing mode, we need to have two 'interfaces' to pair together. In this case, we use two logical interfaces: the port channel to ASA and the port channel to the inside switch.

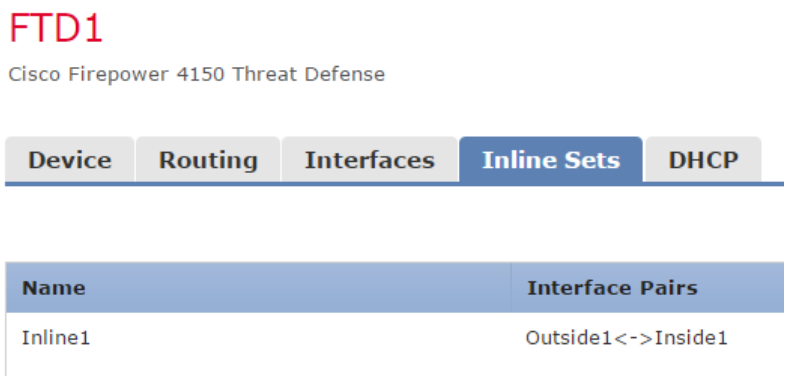
FTD1

Cisco Firepower 4150 Threat Defense

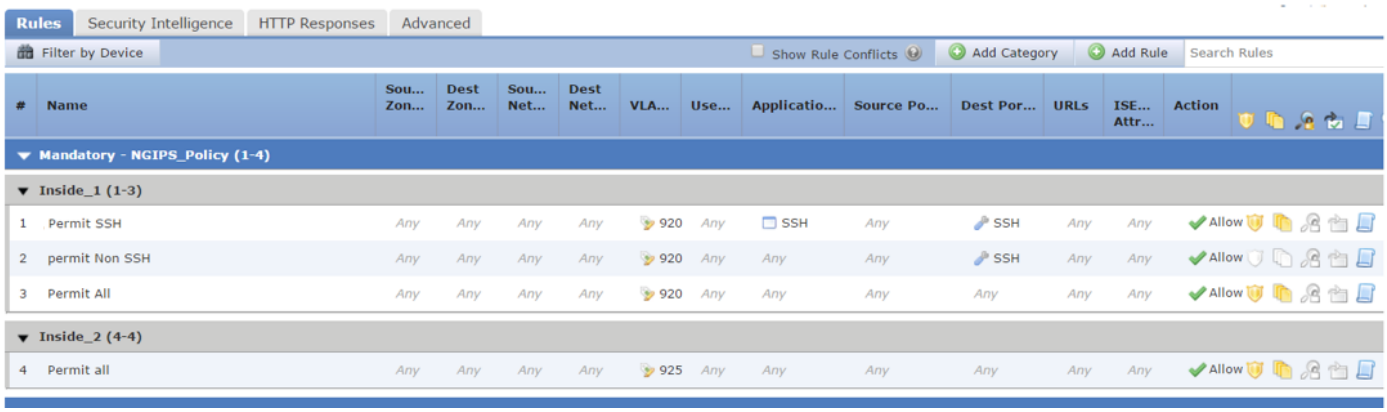
Device | Routing | Interfaces | Inline Sets | DHCP

Stat...	Interface	Logical Name	Type
	Port-channel10	Outside1	EtherChannel
	Port-channel20	Inside1	EtherChannel
	Ethernet1/7	diagnostic	Physical

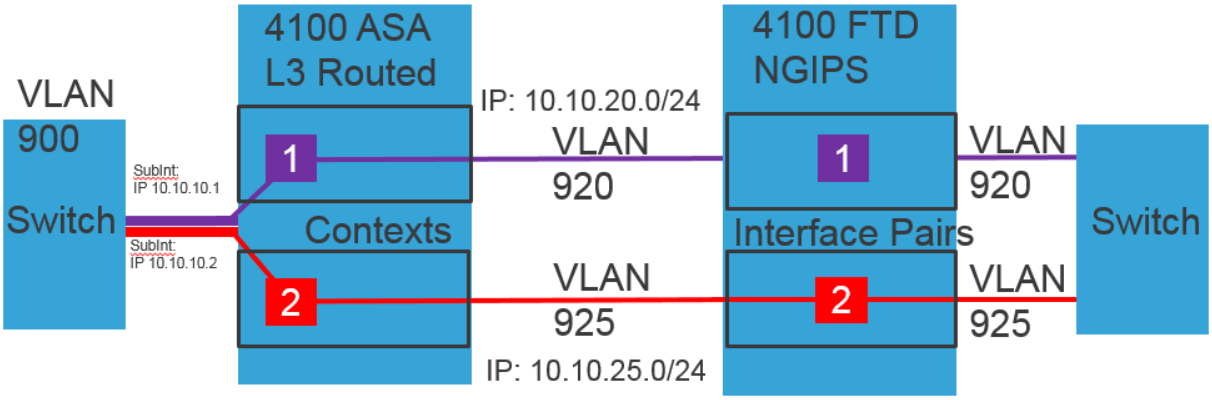
In the Inline Set area, we pair up the two port channels, Outside1 and Inside1 to form Inline1.



Since we have a trunk port going through FTD where the vlans do not change, we apply differentiated policy using the VLAN id. Traffic that belongs to inside1 uses VLAN id 920 and traffic that belongs to Inside2 uses VLAN id 925 so any rule created specifically for one or the other simply needs to include the VLAN id in the rule for it to be specific to one or the other.



Reviewing the Resilient NGFW Design with ASA contexts and FTD interface pairs enforcing independent traffic paths. The logical packet flow is documented below:



Hosts and services on either VLAN 920 or 925 can talk to the outside world on VLAN 900 and beyond and have a L3/L4 policy built in an ASA context and VLAN based FTD policy for application, content and threat related protections. This resilient NGFW solution enforces traffic isolation between contexts/VLANs, and allows FTD policy separation by using VLANs and FMC ACP categories.

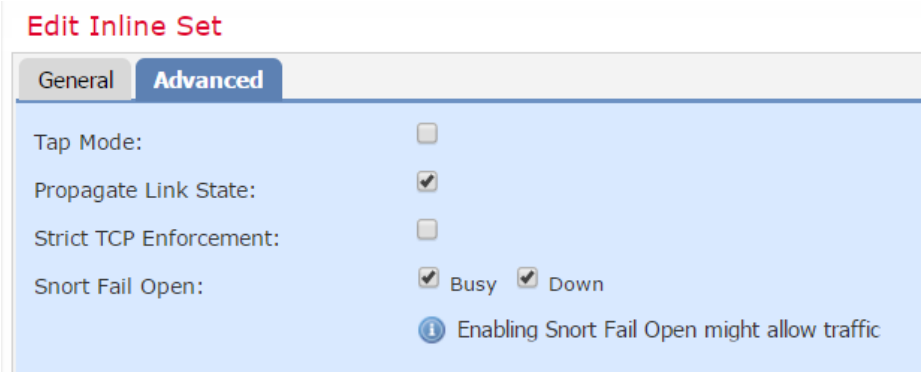
Testing

The Resilient NGFW design was tested in a variety of simulated failure scenarios. This could be testing the failure of a single port and a group of ports connecting a device to the switch. Then we proceeded to test traffic impact of device failures, either switch, FPR4150-ASA or FPR4150-FTD. The failures were tested using a variety of test flows including TCP, UDP, and ICMP. In each case, high-availability built into ASA HA and vPC features guarantied connection survival and quick recovery. All failure tests are captured in a collection of videos found here:

YouTube link: http://cs.co/asa-on-firepower

YouTube link: http://cs.co/ftd-on-firepower

Because ASA devices were setup in active standby HA using port channels and these port channels were configured through the FTD inline pairs, each test that impacted the path of an active flow of packets resulted in either the switch or device moving packets to another port in a port channel without impact. Because FTD interface pairs were assigned to an inline set, a feature called Propagate Link State was enabled. In a normal inline set with 2 interfaces linked together as one, this tells FTD that if link on one interface goes down, FTD should bring link on the other interface down. Because in this design, FTD uses a port channel on both sides and sets up the inline pair using these two ports channels, if both ports in the port channel went down, then FTD would bring the other port channel down.

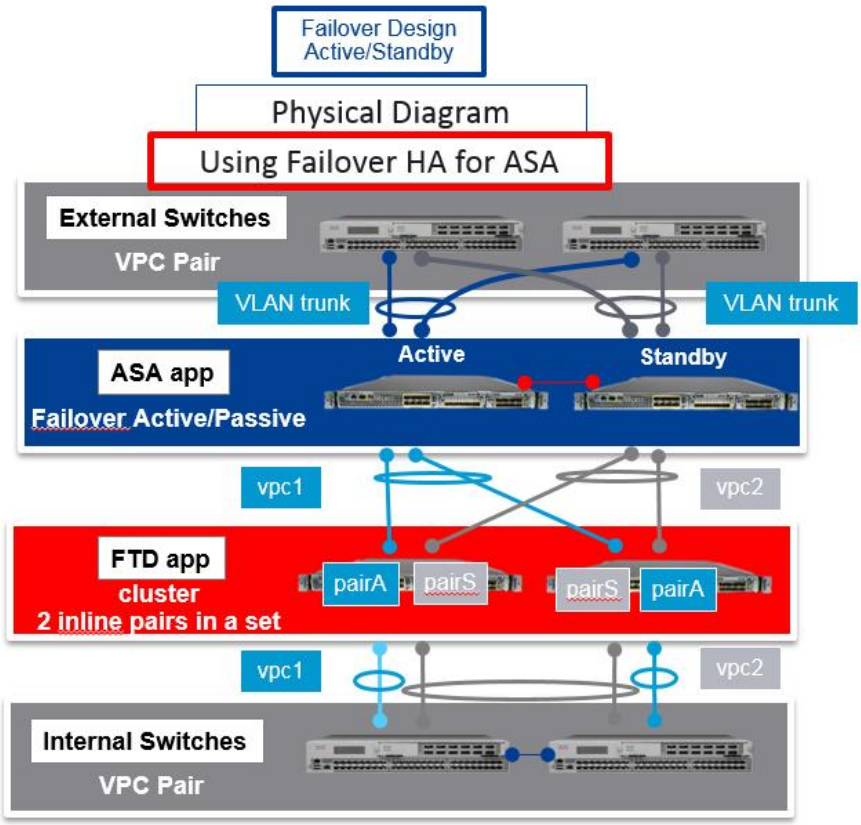


Because ASA was setup for HA, it controlled what path was used traffic. This guarantees traffic symmetry because packets are allowed to move through only the active ASA. If the port channel on FTD inside went down, then link state was propagated to the other side of ASA bringing those links down which told ASA to failover to the backup device. Because FTD devices were independent (identical to Firepower Service modules in an ASA 5585), there was no state shared between them. This was required because if HA was configured it was possible to get the active device for ASA out of synch with the active device for FTD which resulted in no traffic passing. To allow this, one would need to separate ASA failover from FTD failover by inserting a switch in between. But because in this design no HA was configured between FTD devices and no state was shared, the FTD device would use mid-session pickup for any flow that got moved to FTD in mid-stream. This is an attempt to pick up state and if possible start analyzing traffic for IPS policy.

This does not apply to access control policy including application control. So if you are using application policy to, for example, identify SSH application traffic on TCP port 22 (normal SSH port) and allow it, and then block all other traffic on port 22 as the policy example earlier illustrates. On ASA failover, where traffic flows are pushed through the backup FTD box, any flow on port 22 will not be able to get identified and will get denied and need to be restarted. This would apply to any flow where application identification is required for permission. But as previously stated, this is identical behavior to the Firepower services module.

Resilient+ NGFW Design

Similar to the Resilient design, a pair of 4100's running ASA code are deployed in Active Standby HA. Behind the ASAs, directly connected to each ASA, sits a cluster of 4100s running FTD deployed in interface pairing mode (NGIPS style deployment).

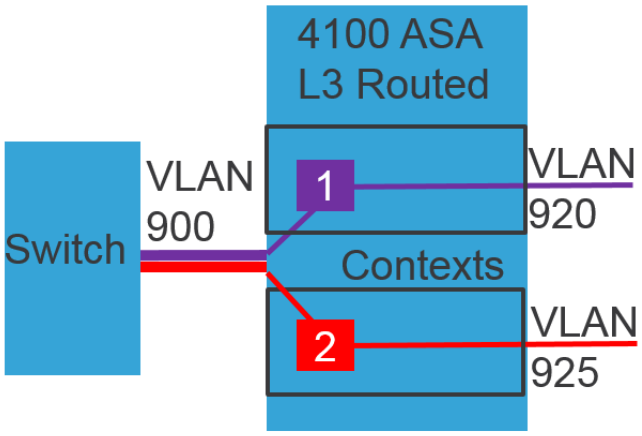


ASA Application

The ASA Active Standby HA pair is setup in L3 Routed mode. The active ASA has the active IP and Active MAC and the standby box has the standby IP and MAC.

On FPR4100's, FXOS is used to provision the ASA app, but as opposed to clustering, HA is not configured within FXOS.

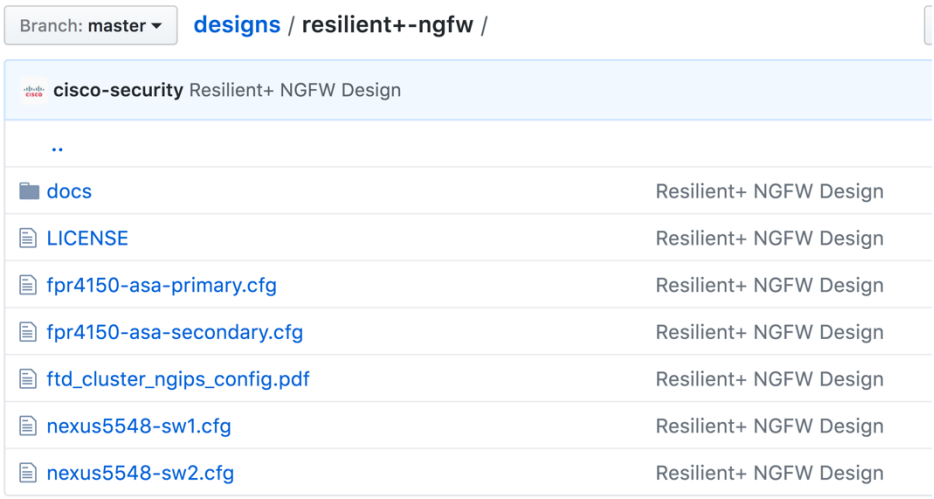
An outside port channel, Po10 was setup with the outside VLAN 900. The ASA was setup in multi context mode, Con1 and Con2, and each context shares the outside interface and has a unique IP address assigned to it. An inside port channel, Po30, was created to connect directly to the 4100 cluster running FTD. This port channel has 2 VLANs assigned to it, 920 and 925. Each context on the ASA is assigned one of the VLANs and has an IP address on the subnet on that VLAN.



ASA (Active and Standby) units and Nexus5548 Switches in vPC Configuration can be found at:

https://github.com/cisco-security/designs/tree/master/resilient+-ngfw

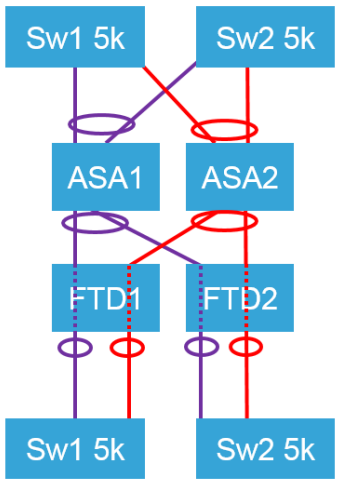
fpr4150-asa-primary.cfg contains system, admin, con1, and con2 context configurations. Inside system context, data-link port-channel VLAN sub-interfaces are assigned to appropriate user contexts.



Policy for each context is built as normal in ASA. Normal ASA context rules apply and each context contains all the appropriate rules to control the traffic flowing through that context. Interfaces are assigned to each context from the admin context. VLAN 900 is shared on both contexts as the outside network.

FTD Application

In the Resilient design, the port channel from each ASA went to a single directly attached FTD device. The primary change in the resilient plus design is that the port channel from ASA goes to each member of the FTD cluster. The Primary ASA uses a port channel to each member of the FTD cluster as a primary path (Purple). The secondary ASA uses a similar port channel to each FTD cluster member (red path).



Because ASA is in active standby HA, either all packets will traverse the purple path, or in the case of a failover, all packets would then be moved to the red path. In any case, because both ASA and FTD are deployed with state sharing all flows are handled statefully. The port channel to the cluster allows the active ASA to send all of the traffic headed inbound to be load balanced across all the FTD instances in the cluster.

In this specific deployment, each interface from the primary ASA to FTD is put into port channel 10, and the interfaces from the secondary ASA are put into port channel 11 coming into FTD.

FTDCluster

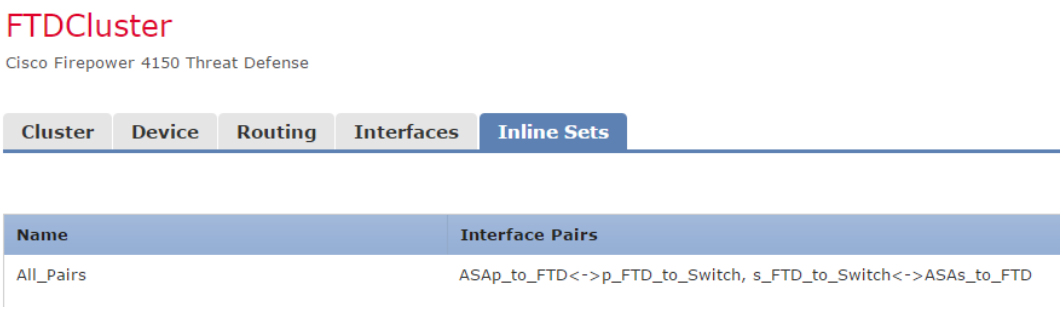
Cisco Firepower 4150 Threat Defense

Cluster | Device | Routing | Interfaces | Inline Sets

Status	Interface	Logical Name	Type
	Port-channel10	ASAp_to_FTD	EtherChannel
	Port-channel20	p_FTD_to_Switch	EtherChannel
	Port-channel21	s_FTD_to_Switch	EtherChannel
	Port-channel48		EtherChannel
	Ethernet1/7	diagnostic	Physical
	Port-channel11	ASAs_to_FTD	EtherChannel

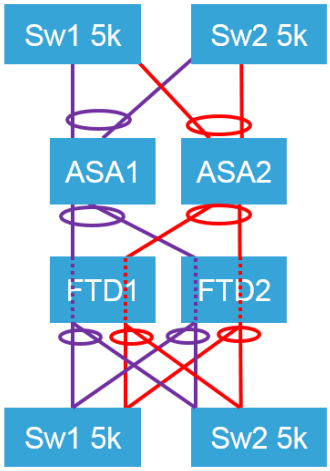
On the inside of the cluster, each FTD has a port channel to the switch below, primary path is port channel 20, standby is port channel 21.

Then in FMC, an Inline Set is created that pairs Port channel 10 and 20 (Primary path) and 11 and 21 (standby path) and puts both inline pairs into the same inline set. This allows any flow that gets moved to the backup ASA that comes across the FTD to be analyzed



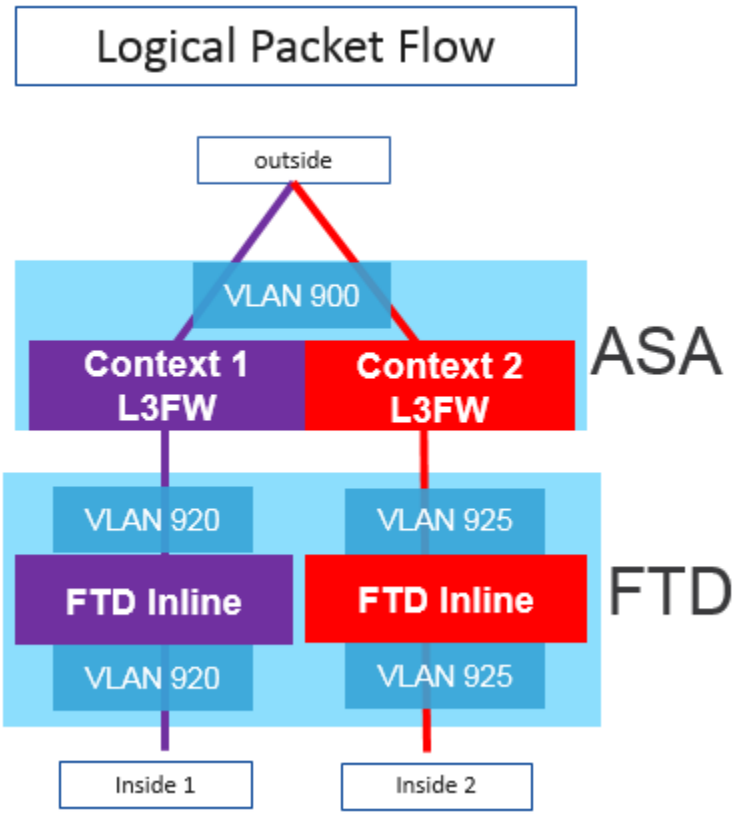
In this example, we attached each FTD to only one switch. If a switch goes down, it will take down the FTD it attaches to forcing traffic through the other switch's attached FTD, but not causing an ASA failover event.

If this is a problem, or if there were more than 2 FTDs (a true performance based cluster), you could add an interface to each port channel going to the switches (20 and 21) to dual attach each FTD to the switches. Doing so creates an interesting "interface" pairing where a port channel containing a single physical interface on the top of FTD is paired up with a port channel that contains 2 physical interfaces on the bottom. The bottom port channel is only considered to be down when both interfaces are down. This increases resilience and availability at the cost of physical interfaces on FTD.

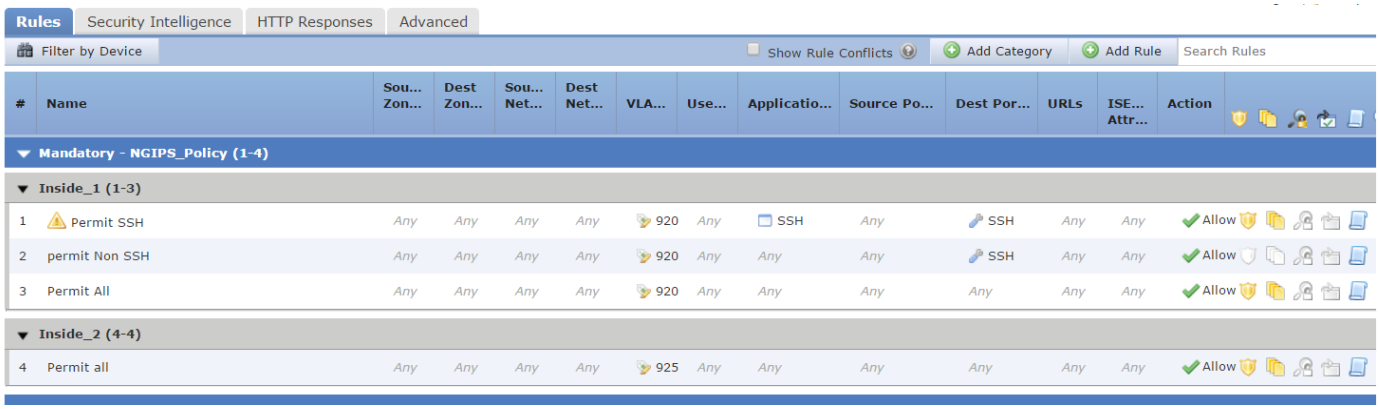


The end result is that ASA passes traffic off on a trunk port carrying VLAN's 920 and 925 and because these trunk ports are going through interface paired ports on FTD, they are not modified and exit FTD on

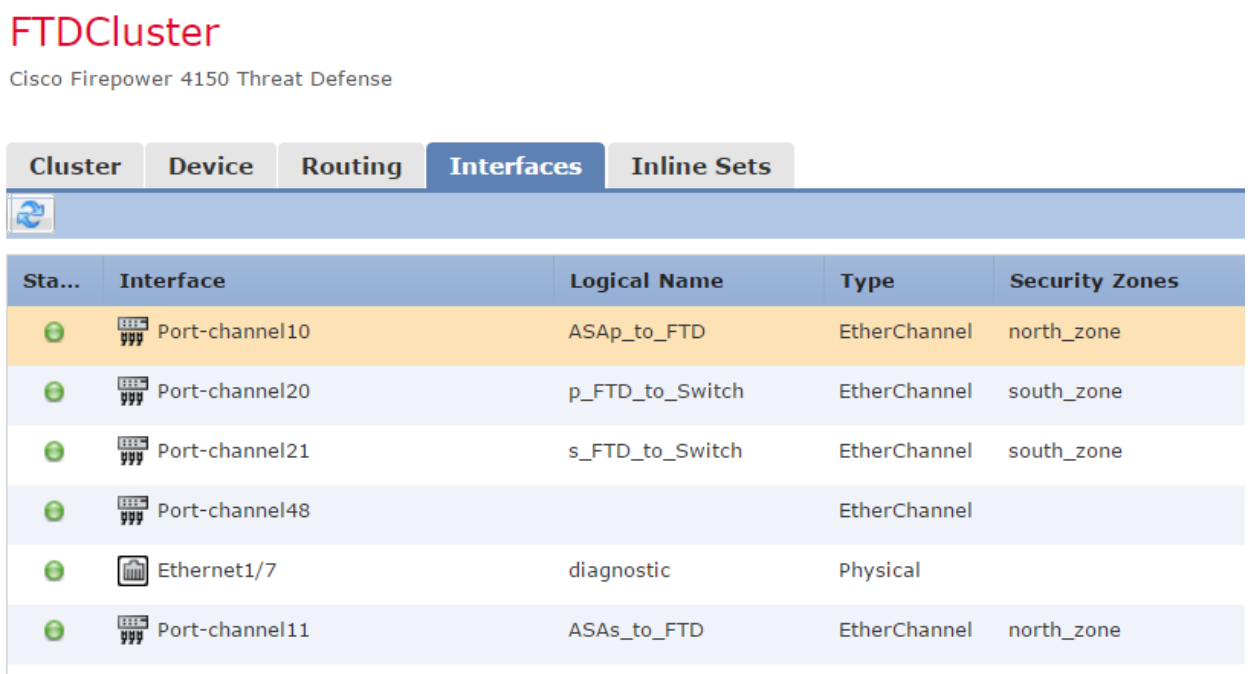
the same VLANs they entered on. Interface pairing ensures traffic segregation because the flow of packets is unaltered and remains on the VLANs they entered on without any ability to have them put on different VLANs.



Since we have a trunk port going through FTD where the VLANs do not change, we apply differentiated policy using the VLAN id. Traffic that belongs to inside1 uses VLAN id 920 and traffic that belongs to Inside2 uses VLAN id 925 so any rule created specifically for one or the other simply needs to include the VLAN id in the rule for it to be specific to one or the other.

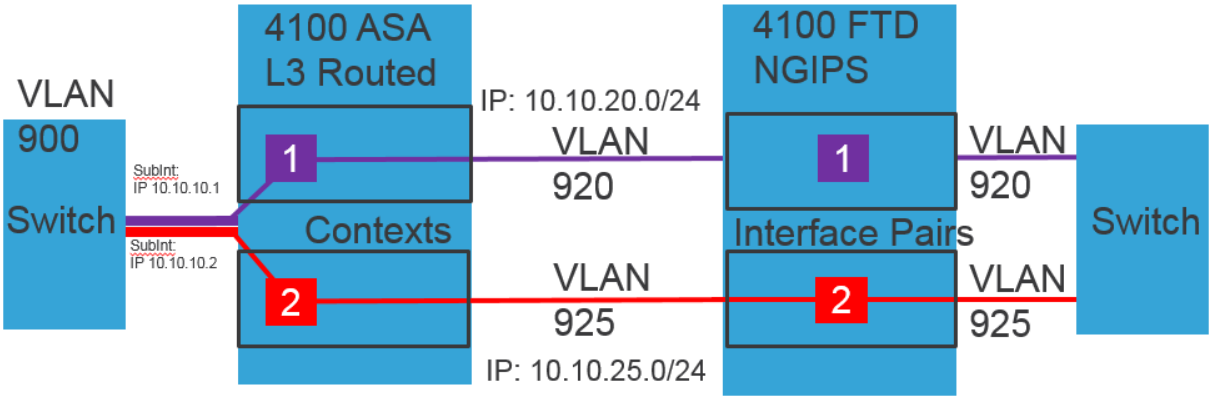


Zones can be used to provide an additional layer of functionality by allowing inbound or outbound policies. By creating a North Zone with the port channels from ASA to FTD and a South Zone with port channels from FTD to Switch, one can enforce directionality on policy allowing the admin to create policies specific to traffic coming from outside to inside vs traffic going from inside to outside.



After creating the zones, we can use the zones in our policy to differentiate direction north to south or south to north.

Reviewing the Resilient+ NGFW Design with Active Standby ASA contexts and FTD clustered interface pairs enforcing independent traffic paths and differentiated policy. The logical packet flow is documented below:



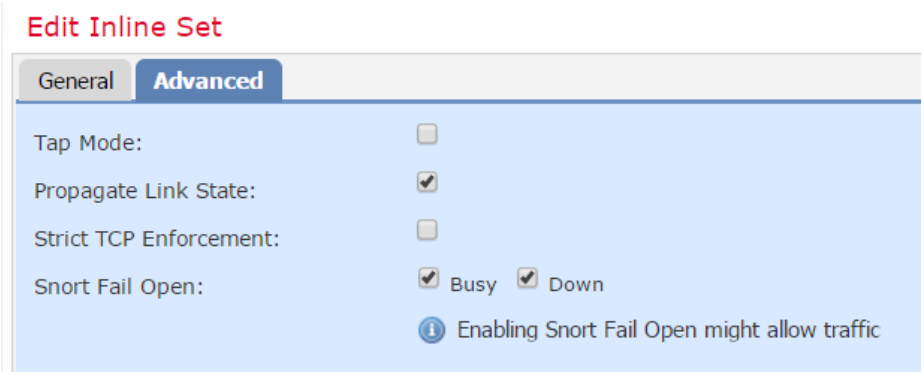
Hosts and services on either VLAN 920 or 925 can talk to the outside world on VLAN 900 and beyond and have a L3/L4 policy built in an ASA context and VLAN based FTD policy for application, content and threat related protections. This Resilient+ NGFW solution enforces traffic isolation between contexts/VLANs, and allows FTD policy separation by using VLANs and FMC ACP categories.

Testing

The Resilient+ NGFW design was tested in a variety of simulated failure scenarios. This could be testing the failure of a single port and a group of ports connecting a device to the switch. Then we proceeded to test traffic impact of device failures, either switch, FPR4150-ASA or FPR4150-FTD. The failures were tested using a variety of test flows including TCP, UDP, and ICMP. In each case, high-availability built into ASA HA, or FTD Clustering and vPC features guarantied connection survival and quick recovery. All failure tests are captured in a collection of videos found here:

YouTube: http://cs.co/ftd-on-firepower

Because ASA devices were setup in active standby HA using port channels and these port channels were configured through the FTD inline pairs, each test that impacted the path of an active flow of packets resulted in either the switch or device moving packets to another port in a port channel without impact. Because FTD interface pairs were assigned to an inline set, a feature called Propagate Link State was enabled. In a normal inline set with 2 interfaces linked together as one, this tells FTD that if link on one interface goes down, FTD should bring link on the other interface down. Because in this design, FTD uses a port channel on both sides and sets up the inline pair using these two ports channels, if all ports in the port channel went down, the port channel itself is deemed to be down, then FTD would bring the other port channel down.



Because ASA was setup for HA, it controlled what path was used traffic. This guarantees traffic symmetry because packets are allowed to move through only the active ASA. Because each ASA was ether channeled to each FTD in the cluster, the traffic from ASA to the inside will be load split across the available FTD units. This allows full horizontal scaling of security services allowing a user to deploy devices to meet the load depending on security features enable.

If the port channel on FTD inside went down, then link state was propagated to the other side to ASA bringing those links down which told ASA to failover to the backup device. Because FTD devices were deployed in a cluster and state is shared between them (different from Firepower services modules), any time a flow was moved from one FTD device to another because of FTD failure, the move was accomplished statefully without forcing the flow to restart. This applies not only to L3/L4 access control policy but application based policy as well.

References

Scalable NGFW Design Videos:

Scalable NGFW Design Chalk Talk: https://youtu.be/fpIL2xmvyqY

FPR4100 FTD App Cluster: (1) Overview: https://youtu.be/lANuLtEIS-Q

FPR4100 FTD App Cluster: (2) Data Link Resiliency: https://youtu.be/YhPhhZ5MV1Q

FPR4100 FTD App Cluster: (3) Control Link Resiliency: https://youtu.be/nhCe3TS2qds

FPR4100 FTD App Cluster: (4) Unit Loss Resiliency: https://youtu.be/xdmWoXA4wyc

FPR4100 FTD App Cluster: (5) Switch Loss Resiliency: https://youtu.be/BE0qgksJbQM

FPR4100 ASA App Cluster: (1) Overview: https://youtu.be/7XODTR3vP8E

FPR4100 ASA App Cluster: (2) Data and CCL Resiliency: https://youtu.be/V6w6dPY9nO8

FPR4100 ASA App Cluster: (3) ASA Unit Resiliency: https://youtu.be/OvbS_qyw1w8

Resilient NGFW Design Videos:

Resilient NGFW Design Chalk Talk: https://youtu.be/1ZrMbhd6xbU

FPR4100 ASA App Failover + FTD NGIPS (1) Overview: https://youtu.be/qqMzcSS31as

FPR4100 ASA App Failover + FTD NGIPS (2) Link resiliency: https://youtu.be/dVSa8lJImnI

FPR4100 ASA App Failover + FTD NGIPS (3) Appliance Resiliency: https://youtu.be/3tlMsNAxT84

Resilient+ NGFW Design Videos:

Resilient Plus NGFW Design Chalk Talk: https://youtu.be/vH63K_LwnQk

FPR4100 FTD App Cluster NGIPS with ASA App Failover (1) Overview: https://youtu.be/-2AQt4ZxwmU

FPR4100 FTD Cluster NGIPS with ASA HA (2) Data Link Resiliency: https://youtu.be/hngtZNNsyM0

FPR4100 FTD Cluster NGIPS with ASA HA: (3) Unit & Switch Resiliency: https://youtu.be/U4fK0i3gKiw