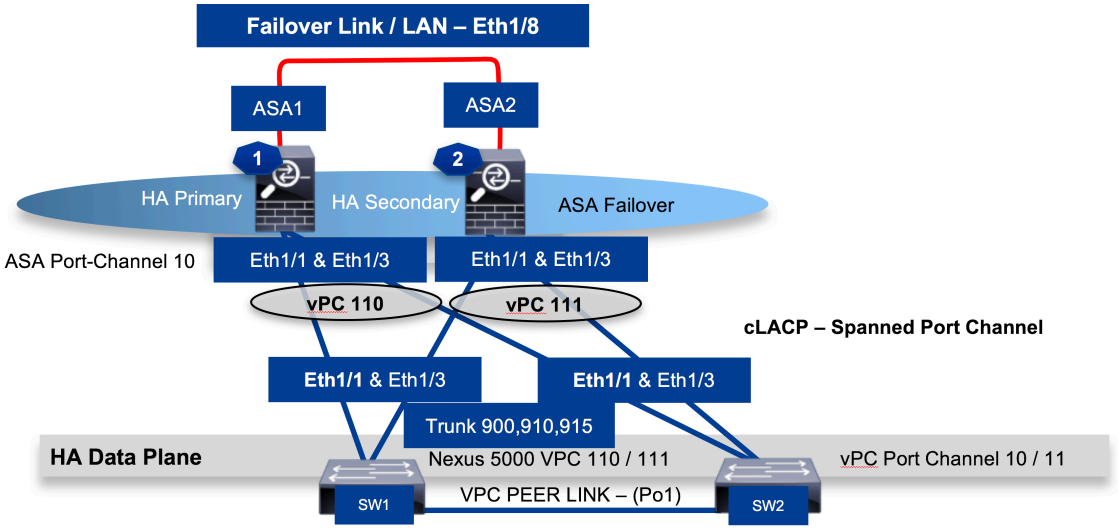
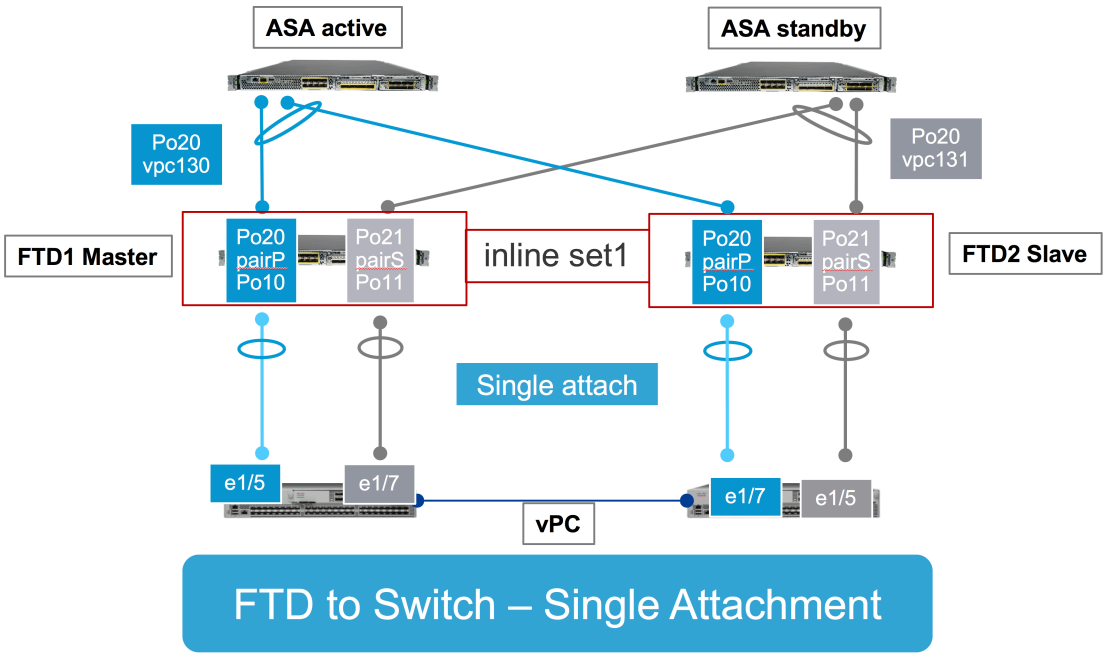
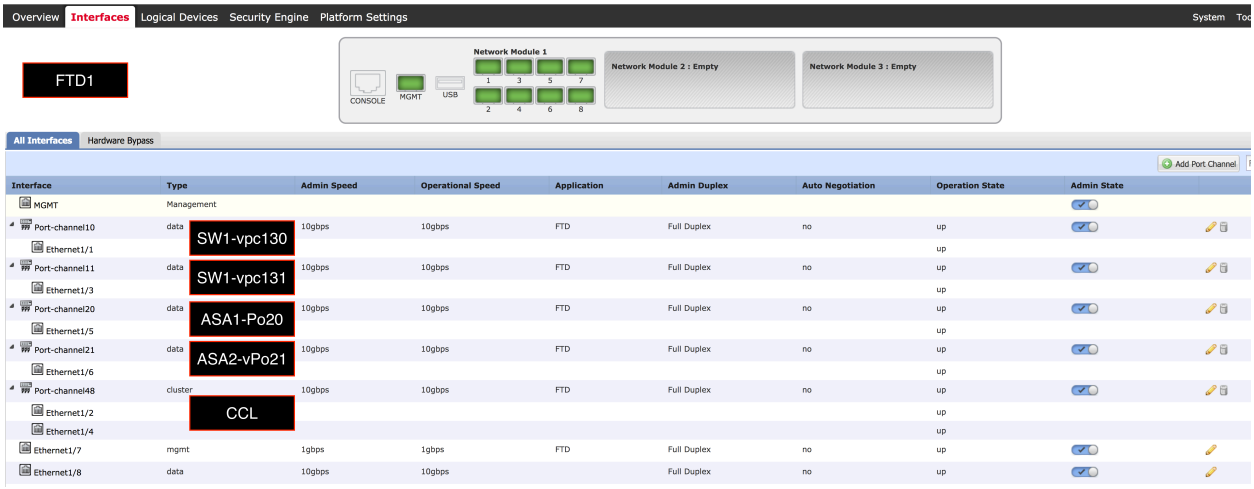
FTD App Cluster NGIPS with ASA App Failover

Design Overview

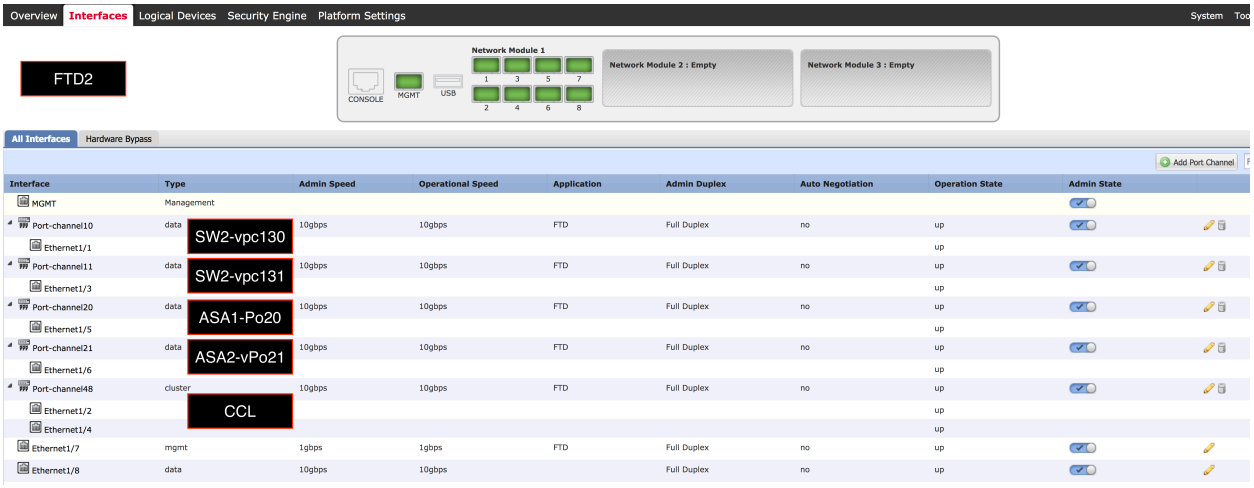




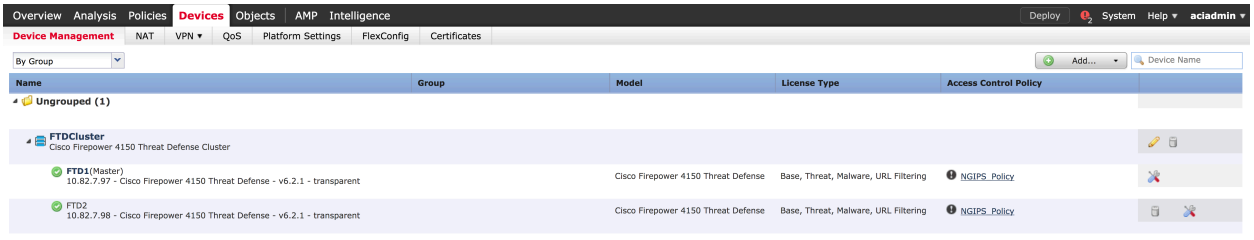
FPR4100-FTD1-master

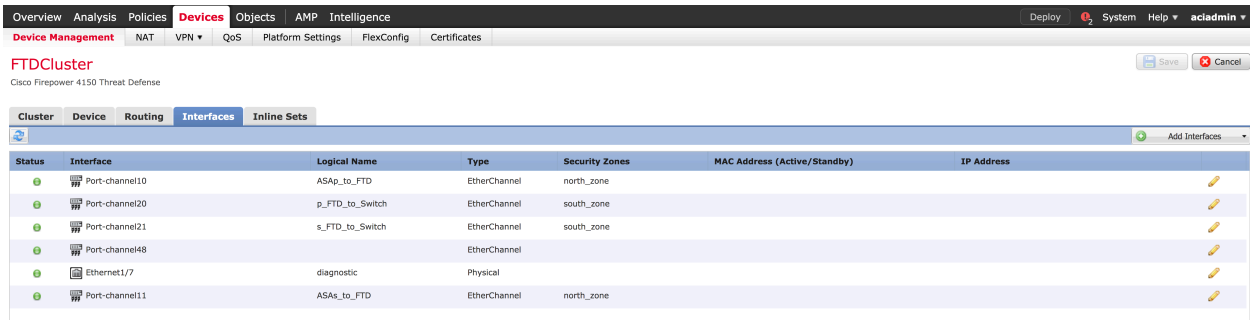


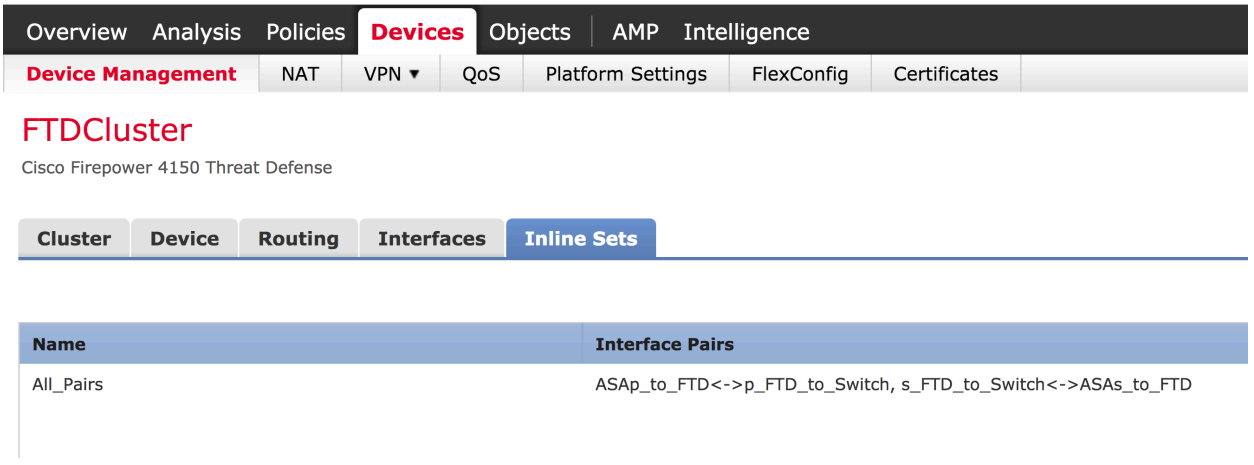
FPR4100-FTD2-slave

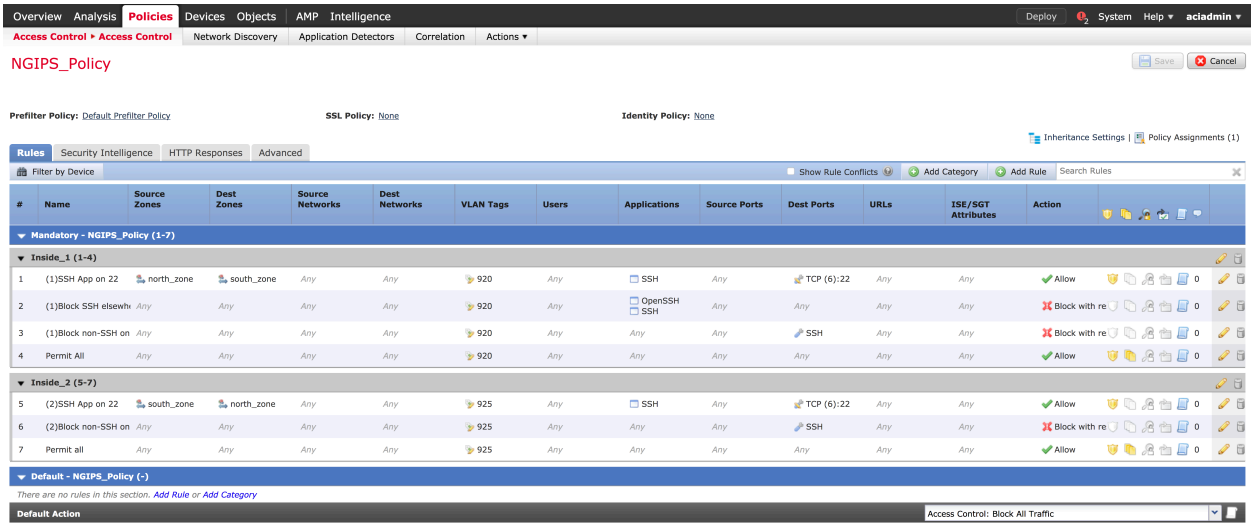


FMC Configuration




Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help aciadmin
Device Management NAT VPN QoS Platform Settings FlexConfig Certificates
FTDCluster
Cisco Firepower 4150 Threat Defense
Save Cancel
Cluster Device Routing Interfaces Inline Sets
Add Interfaces
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


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
Deploy System Help aciadmin
Access Control ▸ Access Control Network Discovery Application Detectors Correlation Actions
NGIPS_Policy
Save Cancel
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
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 elsewh Any Any Any Any 920 Any OpenSSH SSH Any Any Any Any Block with re
3 (1)Block non-SSH on Any Any Any Any 920 Any Any Any SSH 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 Any Any SSH 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