

**Cisco Firepower Threat Defense**

* Unified software that includes cisco ASA features, legacy firePOWER Services, and new features.
* can be deployed on cisco firepower 1000 series, 2100 series, 4100 series, 9000 series appliances to provide to provide NGFW
* can be run on cisco unified computing system (UCS) E-series blades installed on cisco ISR routers
* cisco firepower 1000 series: NGFW that run FTD and features designed for small business and home. We have 1010, 1120, 1140
* cisco firepower 2100 series: uses for many cases, including internet edge and data center. Models: 2110, 2120, 2130, 2140.
* cisco firepower 4100 series. There are seven models at the time
* cisco firepower 9300 series appliances are deigned for very large enterprises or services providers
* Cisco FTD for ISR is supported on the following platforms: cisco ISR G2 Series: 2911, 2921, 2951, 3925, 3945, 3925E; Cisco ISR 4000 Series: 4331, 4351, 4451, 4351, 4451, 4321, 4431

**Surveying the Cisco Firepower Management Center**

* Cisco FTD devices, Cisco firepower NGIPS devices and cisco ASA firepower modules can be managed by the FMC
* When we add a managed device to the cisco FMC, we must provide an IP address of the managed device along with a registration key for authentication. Cisco FMC and the managed device use the registration key and a NAT ID to authenticate and authorize for initial registration

**Exploring the cisco firepower Device Manager FDM**

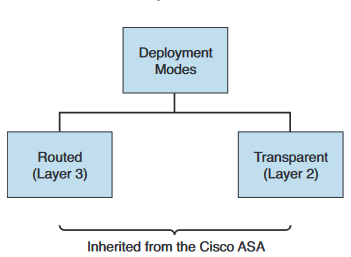
* It is used to configure small cisco FTD deployment
* To access FDM, you just need to point your browser at the firewall in order to configure and manage the device

**Cisco Defense Orchestrator CDO**

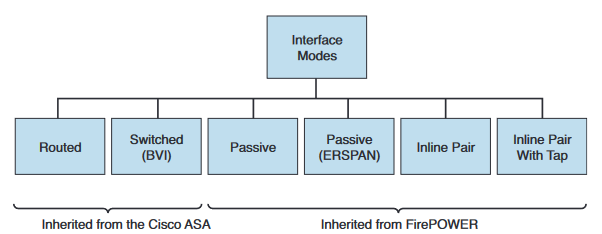
* Solutions that allow you to manage your firewalls from the cloud.
* Allows you to analyze access control policies and objects to identify errors and inconsistencies
* Can also manage and analyze cisco FTD, virtual firewall in AWS, Meraki security devices

**Cisco FTD Deployment Modes**

* Two modes of configuration: routed and transparent
  + **Transparent mode**: in same subnet
  + **Routed:** between different subnets

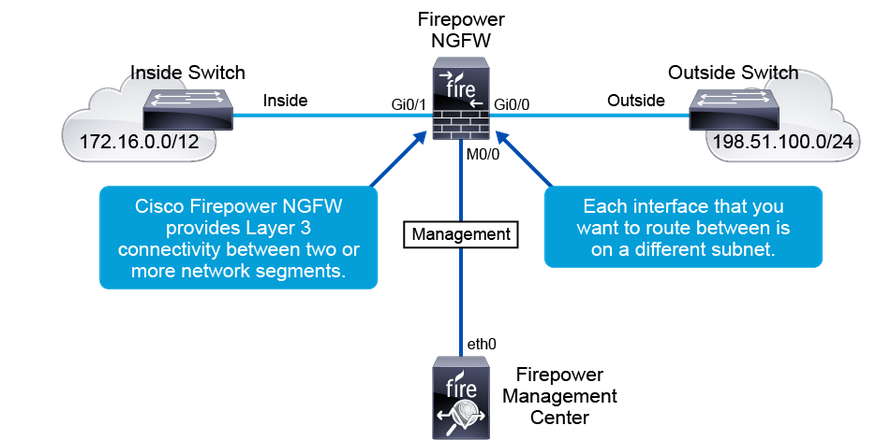


* **Cisco FTD Interfaces Modes**
* Optionally, specific interfaces can be configured for use as IDS or IPS
* **IDS mode**:
  + inline tap interface mode
  + passive interface mode
  + encapsulated remote switched port analyzer (ERSPAN) interface mode
* IPS mode: inline pair

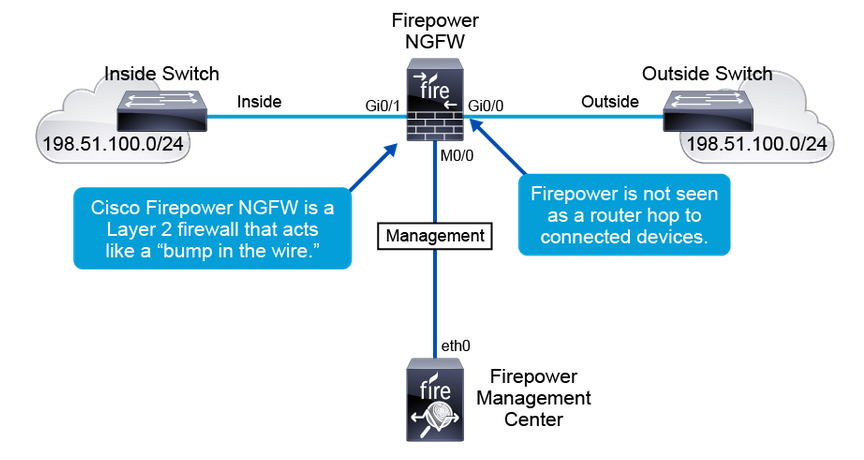


* IPS mode is supported both in routed and transparent deployment modes.
* Intrusion Detection System (IDS) mode in inline tap or passive interface mode is supported in both routed and transparent firewall deployment modes.
* IDS mode in Encapsulated Remote Switched Port Analyzer (ERSPAN) interface mode is supported in transparent firewall deployment mode.

Routed Mode



Transparent mode



Cisco Firepower NGFW IPS inline

**High Availability**

two high availability options:

* **Failover:** When two identical devices are bundled together to cover up each other in case of a failure.
* **Clustering:** When two or more devices are bundled together to not only work during a failure but also to improve throughput and connection limits. This option is a successor of failover, because it delivers high availability and scalability at the same time.

**Active-Standby failover**

* **The standby FTD** (in example) does not actively pass traffic
* When a fails occurs, the active FTD device (FTD) fails over to the standby device, which then become active
* We have the **failover link and the stateful failover links** between the two units
* Recommendation: using the sale unterface on both devices in a failover or a stateful link, confguring two separate interface on each of the devices (one for failover, another for stateful link
* Sateful link: is used to pass connection state information
* Devices constantly communicate over the failover lonk to determinate the operating status of each device
* Information being exchanged over the failover link : firewall state (active/standby), hello messages (keepalives), network link status, Mac address exchange, configuration and synchronization

**Requirement for failover configurations**

* Two participant devices must be configured in the same firewall mode (ex: routed or transparent), be running the same software version, same domain or group on the cisco FMC, must have same NTP configuration
* DCHP or PPPoE must not be configured on any their interfaces
* Same licenses
* Two participant devices must be running the same software version

**Clustering**

* It lets **you group cisco FTD units together as a single logical device**
* Supported on the cisco firepower 9300, 4100 series
* Goal: increased throughput and redundancy of multiples devices
* We have a **cluster-control link** for unit-to-unit communication. Both data and control traffic are sent over the cluster control link
* FTD cluster members work together sharing the security policy and traffic flows
* One FTD is **the master units** and it handles all management and centralized function; and all other cluster members are considered **slave units**
* The master is either the first unit joining the cluster or based on a configured priority
* All configurations are performing on the master unit only and it is replicated to the others units
* A new master is elected only upon a departure of the existing one
* All cluster participant should be connected to a single management network

**Cisco Firepower NGFW appliance virtualization overview**

Install multiple cisco FTD logical devices on a single appliance

**Cisco Firepower NGFW Packet Processing and Policies**

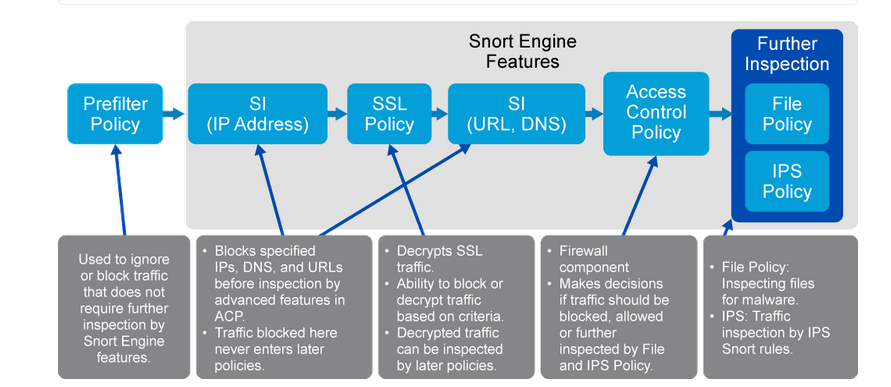
Cisco FTD software on cisco firepower NGFW consists of two main engines:

* **ASA (LINA) engine**: responsible for traffic handling and filtering. Functions like ip routing, Layer3/4 ACL filtering, NAT, VPN are performed by the LINA engine
* **Snort engine:** handles traffic inspection; functions like security intelligence, IPS, Advanced Malware Protection (AMP) and cisco URL filtering. It focused on layer 7 functionality

**Policies available in snort engine**

* **Security intelligence**: is used to ignore or block traffic that does not require further inspection by snort engine feature
* **DNS Name System DNS policy:** monitor DNS requests that originate behind the NGFW. When an internal PC sends out a DNS request for a malicious domain the NGFW intercepts the DNS request and blocked it.
* **Access policy:** central firewall component of firepower. ACP inspect traffic up to layer 7 and this is where access rules are configured
* **File policies**: provide inspection capabilities for individual files in the payloads of network traffic. File policies are used to provide file control and malware protection. Files can also be sent to the Threat Grid, for dynamic malware inspection.
* **Intrusion policies**: along with ACPs and Network Analysis Policies, provide NGIPS features for deep-packet inspection.
* **SSL policy:** can be used to inspect incoming SSL traffic to your internal servers, and it can also be used to inspect outgoing SSL traffic to servers on the internet.

Resume



**Additional policy**

* **Network discovery policies:** are used to discover network applications, users, and hosts in the environment.
* **Correlation policy:** is used to automatically trigger some alerts or responses when a specific event meets certain configured criteria
* **Identity policies:** assign identity to users who connect through an NGFW device

**Cisco Firepower NGFW Policy Relationships**

* Access Control Policy is a central part of policy configuration, as other policies need to be attached to ACP to take effect:
* Prefilter, SSL, identity, and DNS policies need to be attached globally to the ACP.
* IPS and file policies are attached per ACP rules.

**Cisco Firepower deployment**

The deployment action distributes these configuration components:

* Access control policies and all associated policies: DNS, file, identity, intrusion, network analysis, SSL
* Any associated rule configurations and objects associated with a policy to be deployed
* Intrusion rule updates
* Device and interface configurations
* Platform settings
* VPN deployments
* Network discovery policy
* NAT policies
* Quality of service (QoS) policy