**Cisco Next-Generation Firewalls and Cisco Next Generation Intrusion Prevent Systems**

Cisco ASA with FirePOWER services available on the cisco ASA 5500-X Series, ASA 5585-X Adaptive Security Appliances; Firepower Threat Defense (FTD), and Cisco Advanced Malware (AMP) provide a security solution that helps discover threats and enforce and harden/\* - policies before an attack takes place

NGIPSs, Email Security, Web security Appliance with AMP help you to detect, block and defend against attacks that have already taken place

**NGIPSs**

**IPSs** were traditionally used in network infrastructures to protect against known security threats

IPSs suffer from certain shortcomings

* They are sometimes not very effective and may be ignored
* They often need to be operated in conjunction with other products or tools (firewalls, analytics, and correlation tools)
* Their operation costs and the operating resources they need are high
* They can leave infrastructure imperfectly covered against attackers

Supplement legacy IPS functionality with more capabilities such as:

* **Application awareness and control:** provides visibility into Layer 7 applications and can protect against Layer 7 threats
* **Content awareness of the information traversing the infrastructure**
* **Contextual awareness** (helps better understand alerts and automatically deduce comprehensive information about the events taking place
* **Host and user awareness**

**Most important capabilities of cisco NGIPS**

* **Threat containment and remediation**: Cisco Firepower NGIPS provides protection  
  against known and new threats. Its features include file analysis, packet- and flow-  
  based inspection, and vulnerability assessment.  
  ■ **Application visibility**: Cisco Firepower NGIPS offers deep inspection and control of  
  application-specific information for better efficacy.  
  ■ **Identity management**: NGIPS policies can be enforced by using contextual user  
  information.  
  ■ **Security automation**: Cisco Firepower NGIPS includes automated event impact  
  assessment and policy tuning.  
  ■ **Logging and traceability management**: This can be used in retrospective analysis.  
  ■ **High availability and stacking**: Cisco Firepower NGIPS provides redundancy and  
  performance by leveraging multiple devices.  
  ■ **Network behavioral analysis**: Key behavioral indicators and threat scores help analysts  
  prioritize and recover from attacks.  
  ■ **Access control and segmentation**: Access policies can be applied to separate traffic  
  profiles in the network.  
  ■ **Real-time contextual awareness**: NGIPS discovers and provides information about  
  applications, users, devices, operating systems, vulnerabilities, services, processes,  
  files, and threat data related to IT environments.

**Cisco IOS Zone-Based Firewall (ZBFW)**

* It is another firewall solution.
* It is a stateful firewall used in Cisco IOS devices
* Successor of the legacy IOS firewall or the context-Based Access Control (CBAC)
* Include features that are not available in CBAC (included the assignment of the router interfaces to different security zones to control IP traffic
* Zone-based firewalls can also be implemented in an SD-WAN solution
* In SD-WAN configuration, zone deployments and configurations include the following components:
  + **Source zone:** group of VPNs where the data traffic flows originate (vpn can be part of only one Source zone)
  + **Destination zone**: group of VPNs where the data traffic flows terminate (vpn can be part of only one Destination zone)
  + **Firewall policy**: security policy, that defines the conditions that the data traffic flow from the source zone must match to allow the flow to continue to the destination zone (firewall policies can match IP prefixes, IP ports, the protocols TCP, UDP, and ICMP and applications)
  + **Zone pair**: a container that associates a source zone with a destination zone and applies a firewall policy to traffic that flows between the two zones
  + **Matching flows** that are accepted can be processed in two different ways:
    - **Inspect**: the packet’s header can be inspected to determine its source address and port
    - **Pass**: the packet can pass to the destination zone without the packet’s header being inspected at all
* In ZBFW deployment a zone must be configured before interfaces can be assigned to the zone
* An interface can be assigned to only one security zone
* All traffic to and from given interface in a device with ZBFW configured is implicitly blocked when the interface is assigned to a zone; except traffic to and from other interfaces in the same zone
* Pass, inspect, and drop can only be applied between two zones

**Deployment Modes of Network Security Solutions and Architectures that provides Firewall capabilities**

**Inline Pair**

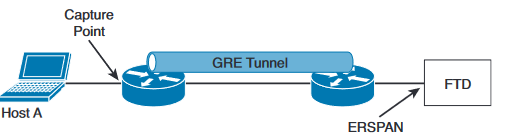
* Inline is used for prevention and inline devices can be placed between two assets that communicate (ex: between a switch and a router) to block and mitigate threats
* Two interfaces of the device are used in an inline pair for traffic to enter and exit the device after being inspected
* It offers two more modes of operation: routed (devices operates at layer 3) and switched (transparent modes, it uses two interfaces in a vlan pair and bridges them together)
* Disadvantage of inline interfaces: all traffic is dropped in the event of a software failure or a loss of power

**Passive/ monitoring mode**

* Mode where the cisco NGFW or NGIPS device does not usually prevent attacks
* The device uses one interface to silently inspect traffic and identify malicious activity without interrupting traffic flow
* Usually connected to a switch’s span port, a mirrored port
* Device doesn’t block traffic
* Supported in routed or transparent deployment modes

**Passive with ERSPAN mode**

* Supported only in routed deployment mode
* You can configure one physical interface operating ad a sniffer



**Cisco ASA Application inspection**

* Stateful inspection engine keeps information about each connection traversing the security appliance’s interface and makes sure they are valid
* Stateful application inspection examines not only the packet header but also the contents of packet up through the application layer
* Cisco ASA provides MPF (Modular Policy Framework) to provide application security or perform QoS functions
* MPF offers a consistent and flexible way to configure the cisco ASA application inspection

)

**Cisco NGIPS Preprocessors (incompris)**

**Cisco Advanced Malware Protection (AMP)**

* Cisco solutions that enable you to detect and block malware, continuously analyze for malware, and get retrospective alerts.
* We have AMP for endpoint and AMP for network
* Cisco AMP for network: provides continuously analysis and tracking of files and also retrospective security so that a security administrator can take action during and after an attack
* **ThreatGRID:** security company that provides cloud-based and on premises malware analysis solutions

**Cisco AMP features:**

* **file reputation:** AMP allows you to analyze files inline and block or apply policies
* **File sandboxing**: AMP allows you to analyze unknown files to understand true file behaviour
* **File retrospection**: AMP allows you to continue to analyze files for changing threat level

**Architecture of AMP: three main components**

* **AMP cloud:** contains many different analysis tools and technologies to detect malware in files, including the Threat Grid analysis solution
* **AMP client connectors:** include AMP for networks and AMP for Endpoint
* **Threat Intelligence sources:**
* **Snort, clamAV and Immunet AV open-source communities** contributes threat information daily
* **Talos**: team of leading threat researchers that contributes to the threat information ecosystem of Cisco security products
* **ThreatGRID**