**Cisco Firepower NGFW Object** (similar to ASA)

* Objects are containers used throughout the Cisco Firepower NGFW configuration.

**Types of objects** we can create

* ACP: Network object, port object, security zone object, URL object, geolocation
* NAT: Network object, port object, security zone
* We can define object groups to group (Network object, port object, vlan object, url objects)

**Cisco Firepower NGFW NAT (Similar to ASA NAT)**

**Cisco Firepower prefilter**

* Prefilter policy is the first line of a defense inside the Cisco ASA engine which can be used to protect your network from undesired traffic.

Two reasons to use prefilter policies:

* Improves performance of Cisco Firepower NGFW system by blocking traffic early or exempting traffic from further (Snort) inspection, based on simple Layer 3 and Layer 4 conditions.
* Provide inspection for encapsulated traffic based on tunnel endpoints and encapsulation type (GRE, IP in IP; IP version 6 in IP)

Prefilter policy consists of these action and condition rules:

**Condition rules**

* For prefilter rules: security zones, source and destination IP addresses, VLAN, and protocols or ports.
* For tunnel rules: security zones, tunnel endpoints, VLAN, encapsulation type or port.

**Actions** that are available when configuring prefilter rules:

* **Block:** discard traffic without further inspection.
* **Fastpath:** permits traffic without sending the traffic to Snort inspection.
* **Analyze:** sends traffic to further (Snort) inspection, based on configured ACP rules.

**Access Control Policies**

ACP is the central part of configuring firewall functionality and is used to:

* Allow or block traffic based on simple or more sophisticated traffic characteristics.
* Send traffic to further analyses to IPS or file policy for inspection of malicious traffic.
* Make decisions whether to log traffic as connection events.
* Manage security intelligence, SSL decryption, authentication, and other advanced firewall and IPS settings.

ACP Components

The ACP can be divided into the following components:

* **Rules:** Rules are how you match on traffic conditions. These are matched in a top-down fashion.
* **Prefilter policy:** Allows traffic to be fastpathed (bypass all inspection) or dropped prior to any other inspection.
* **Default action:** If no rules match the traffic, the traffic matches here.
* **Security intelligence:** Prevents traffic from entering the access control policy by filtering based on reputation of IP addresses, URLs, and DNS names.

**ACP rules components**

* **Name:** used to uniquely identify a rule.
* **Conditions:** identify the type of traffic that the rule handles
* **Action:** Each rule must have an action associated with it.
* **IPS and file policy inspection settings:** Influence if traffic will be sent for further analyses to IPS policy to detect malicious traffic or to file policy to detect prohibited files or malware-infected files.
* **Connection logging settings:** Determine if traffic will be logged as connection events.

**ACP Rules Name and Conditions**

When configuring ACP conditions you can choose from the following:

* **Zones:** traffic that entering or leaving a device via an interface in a specific security zone. A security zone is a logical grouping of one or more interfaces according to your deployment and security policies.
* **OSI Layer 2 to Layer 4 parameters:** VLAN (only in case of IPS/IDS deployment), source and destination IP address or its geolocation, protocol, and source and destination port.
* **OSI Layer 7 parameters:** 
  1. Applications: match traffic by the application detected in a session. You can control access to individual applications, or filter access according to basic characteristics: type, risk, business relevance, categories, and tags.
  2. URLs: Matches traffic by the URL requested in the session. You can control access to individual websites, use lists and feeds, or filter access based on a site's general classification and risk level.
* **Miscellaneous parameters:**
  1. Users identity and realm: matches traffic by the user or realm involved in the session. Requires identity policy to be configured which specified how to authenticate users to determine their identity.
  2. Identity Services Engine (ISE) attributes: match traffic based on Cisco ISE scalable group tags (SGTs).
* Rules that use port conditions and do not require further processing (for example, with block action), are implemented inside the ASA engine.
* Rules that use application condition need to be sent to the Snort engine, regardless whether additional inspection is needed, to determine the type of application, based on configured application detectors inside Snort.
* Port conditions use port objects instead of port numbers themselves. Eve

**ACP rules actions**

* **Allow:** allows matching traffic to pass. However, depending on your requirements, you can perform further inspection to inspect network traffic before it reaches its destination. Traffic is also subject to security intelligence and network discovery.
* **Trust:** allows traffic to pass without further inspection of any kind, including network discovery.
* **Block and block with reset:** deny traffic without further inspection of any kind. Block with reset also resets the connection.
* **Interactive block and block with reset:** deny traffic without further inspection of any kind. Block with reset rule also resets the connection. For HTTP traffic, when the system blocks a web request, a user can override the default browser or server page with a custom page that explains that the connection was denied. The system calls this custom page an HTTP response page.
* **Monitor:** does not affect traffic flow, matching traffic is only logged and neither permitted nor denied
* The default action determines how the system handles traffic that is not matched by any ACP rule. The default action can block or trust all traffic without further inspection, inspect traffic for intrusions based on IPS policies, or allow traffic and collect network discovery data.

## ACP Rules Further Inspections

For traffic that is allowed you have two options for further inspection:

* **IPS policy:** uses intrusion rules to examine packets for threats.
* **File and malware policy:** allows to detect and block certain filetypes or examine files for malware.

## ACP Rules Logging

As a Cisco Firepower NGFW device monitors traffic generated by the hosts on your network, the device can generate logs of the connections that they detect and send those logs to Cisco FMC, syslog server or to the Simple Network Management Protocol (SNMP) trap receiver.

**Cisco firepower NGFW Security Intelligence**

* Security Intelligence block traffic based on ip addresses, urls, dns names that have a known bad reputation
* First line of defense which acts before any other snort policies

Security intelligence places traffic into two categories or container.

Traffic is compared against IP addresses and URLs inside these two containers.

* **Blacklist:**
  + For traffic that is considered malicious.
  + Matching traffic is blocked or monitored. For blocked traffic no further inspection is performed.
* **Whitelist:**
  + Used to override objects that appear in blacklist.
  + Whitelist matches do not generate events.
  + Matching traffic continues along the Cisco Firepower NGFW processing pipeline.

**Security Intelligence Object**

Inside a whitelist or blacklist the following objects can be used:

* **Feed objects:** By default, the system comes with a security intelligence feed provided by Cisco which provides IP addresses and URLs with bad reputation. This feed is constantly updated and provides protection from observed malicious activity.
* **List objects:** Lists are manually created by administrators in a form of text file and contain a static list of IP addresses and URLs names with bad reputation.
* **General network or URL objects and groups:** These are static objects or object groups you create inside Cisco FMC object manager and can also be used as objects in other policies, such as in access control policy rules.
* **Global whitelist/blacklist:** These are initially empty and can be populated by an administrator from connection events.

Another building block of security intelligence: is a **DNS policy**

* which performs filtering of DNS traffic based on requested DNS names
* DNS policy uses a whitelist and blacklist categories, which also use feed and list objects and global whitelist and blacklist to define good or bad DNS names.

**Cisco Firepower Discovery**

* + It is the process of collecting information about hosts and users in your environment.
  + You should define the network ranges that you want to protect in the network discovery policy. Any detected IP is identified as a host, and a host profile is created for that system.
  + A host profile is a collection of information about a host, such as operating system, open ports, connections detected, and so on.
  + data collected about hosts, applications, operating systems, services, users, and vulnerabilities is used throughout the system for analysis and automation of security protection

**Host profiles**

* + A host profile provides a complete view of all the information that the system has gathered about a single host. The information can be:
    - IP address of the host.
    - The operating system running on a host.
    - The servers running on a host.
    - The clients and web applications running on a host.
    - The protocols running on a host.
    - The IOC tags on a host.
    - The VLAN tags on a host.
    - The last 24 hours of user activity on your network.
    - The most recent malware events for a host.
    - The vulnerabilities associated with a host.
    - The Nmap scan results for a host (Nmap discovers operating systems and services on hosts.).
  + **Vulnerabilties in host profile:** The Vulnerabilities sections of the host profile list the vulnerabilities that affect that host. These vulnerabilities are based on the operating system, servers, and applications that the system detected on the host.

**Cisco Firepower IPS Policies**

* system's last line of defense before traffic is allowed to its destination.
* Cisco delivers several intrusion policies with the Firepower system
* Policies are designed by the cisco Talos Security Intelligence and Research Group (you can not modify these policies but you can change the action to take for a given rule)
* Intrusion detection: generally, refers to the process of passively analyzing network for potential intrusions and storing attack data for security analysis
* Intrusion prevention: includes the concept of instrusion detection but adds ability to block or alter malicious traffic as it travels across your network

Variables

* Used to representing networks and port (for example the inside network is represented by the variable $HOME\_NET)
* Two types of variables:
* Systems default variables (preconfigured) : $HOME\_NET, $HOME\_EXTERNAL\_NET, $HTTPS\_SERVERS…
* Policy variables that override default variables (used in specific policies)

Platform setting policy: it is a policies that shared a set of parameters that define the aspects of cisco firepower device that are likely to be similar to other managed devices.

Cisco Firepower Malware and files policies

* Cisco Firepower gives you means to detect the movement of files in your networks and to take appropriate action
* Cisco Firepower NGFW offers file type detection feature which can detect or block files based on file type.
* Cisco Firepower also offers Malware detection feature which can detect or block malicious files
* **Cisco Advanced Malware Protection (AMP):** enable you to detect and block malware, continuously analyze for malware, and get retrospective alerts.