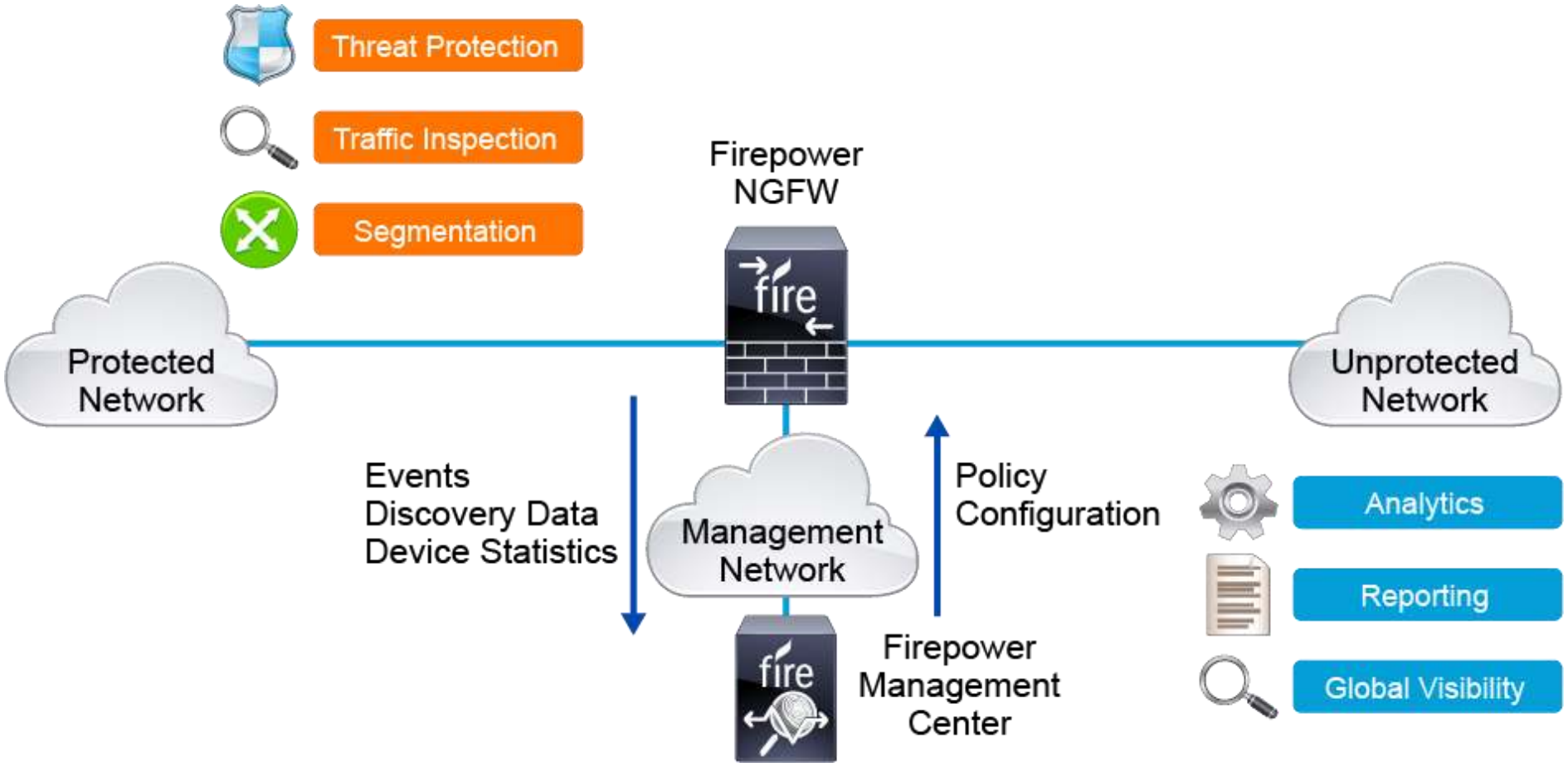
06- Cisco Firepower Next-Generation Firewall

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Cisco Firepower NGFW Deployments

- Cisco Firepower NGFW is the Cisco next generation network security appliance, offering NGFW services such as Cisco URL Filtering, application control and visibility, advanced malware protection, and so on.
- It also offers Intrusion Prevention System (IPS) services in a single agile platform.
- The Cisco Firepower NGFW runs a unified image of Cisco FTD and Cisco ASA code to offer all the NGFW services and IPS services from Cisco Firepower plus features such as NAT, VPNs, and so on from the ASA.

Cisco Firepower NGFW Deployments (cont.)



Cisco Firepower NGFW Deployments (cont.)

- Managed by using the central Cisco Firepower Management Center (FMC), cloud-based Cisco Defense Orchestrator (CDO), or the local Cisco Firepower Device Manager (FDM).
- Cisco FMC provides deep analytic capabilities and **application programming interface (API)** integration that is not provided by the Cisco FDM.
- Both Cisco Firepower NGFW and Cisco FMC can be **physical** or **virtual** appliances.
- Cisco Firepower NGFW Virtual (NGFWv) and Cisco FMC are available for Amazon Web Services (AWS), Kernel-based Virtual Machine (KVM), Microsoft Azure, and VMware vSphere environments.
- Physical or virtual FMCs can manage virtual or physical Cisco Firepower NGFW appliances.

Cisco Firepower NGFW Deployments (cont.)

- Cisco FMC can be used to manage the Cisco FTD system.
- Cisco FMC is a purpose-built network appliance that provides a centralized management console and database repository for your Cisco Firepower deployment.
- You can monitor the information that your devices report, and assess and control the overall activity that occurs on your network.
- Cisco FMC also controls the network management features on your devices: switching, routing, NAT, VPN, and so on.

Cisco Firepower NGFW Deployments (cont.)

- You need to **register** the Cisco Firepower NGFW with Cisco FMC.
- After the communication channel is set up between the Cisco FMC and Cisco Firepower NGFW, basic information is exchanged between the two appliances.
- If you change the policy configuration on Cisco FMC for a managed device, that policy change does not take effect until you **deploy** that policy (known as a deploy or apply).
- You can deploy the policy immediately or later.

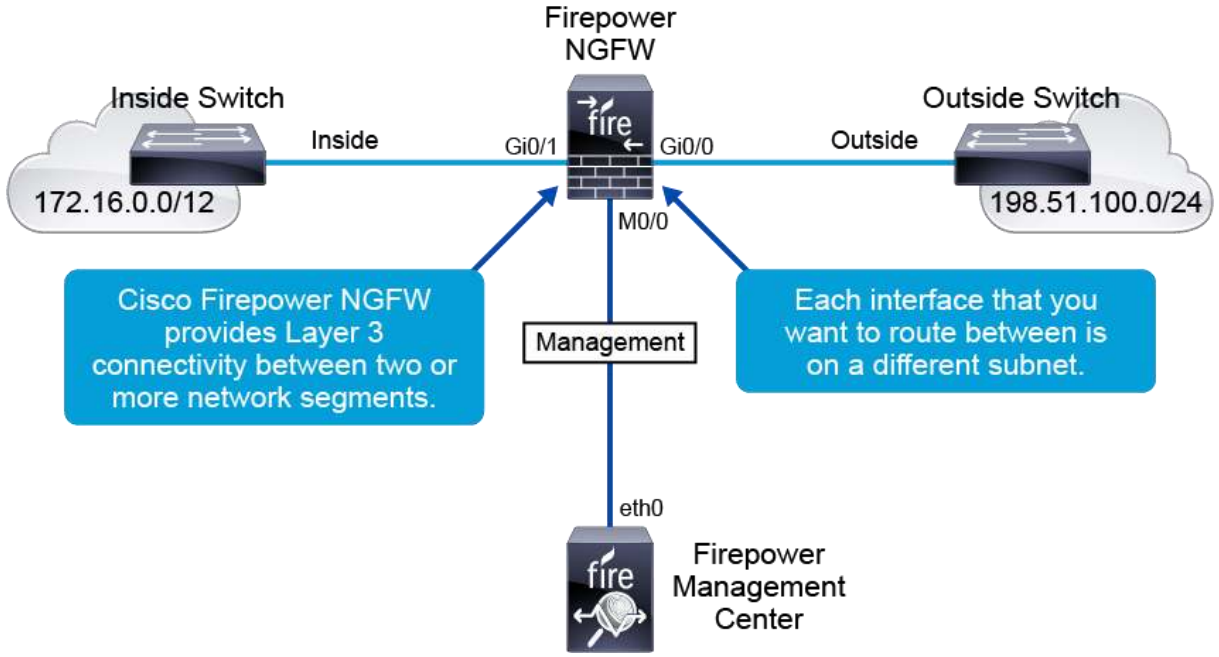
Cisco Firepower NGFW Deployments (cont.)

- Cisco Firepower NGFW can be deployed in a **routed** or **transparent** NGFW mode, or in a **inline** or **passive** IPS mode:

  - The Cisco Firepower NGFW supports two platform-wide firewall modes (routed or transparent) and several interface modes.
  - The default firewall mode is routed. You can change the firewall mode using the **configure firewall { routed | transparent }** CLI command.
  - 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.

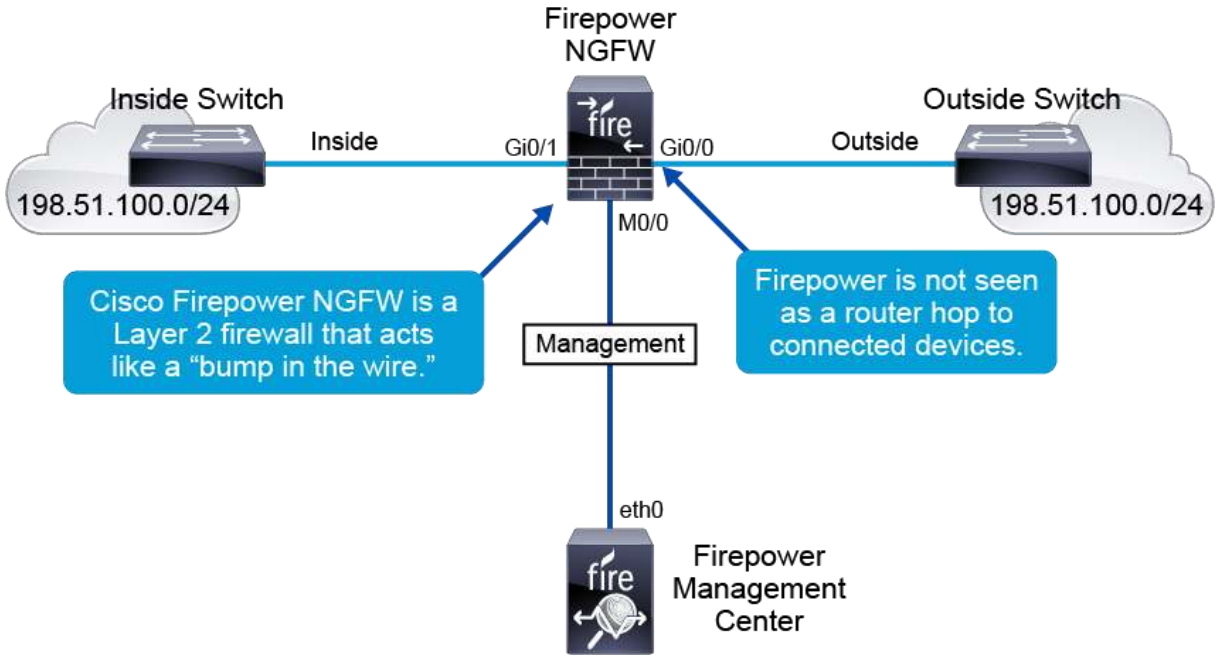
Cisco Firepower NGFW Deployments (cont.)

- **Cisco Firepower NGFW Routed Mode**
  - In routed mode, the Cisco Firepower NGFW provides Layer 3 connectivity between two or more network segments, the Cisco FTD device is considered to be a router hop in the network. Each interface that you want to route between is on a different subnet.



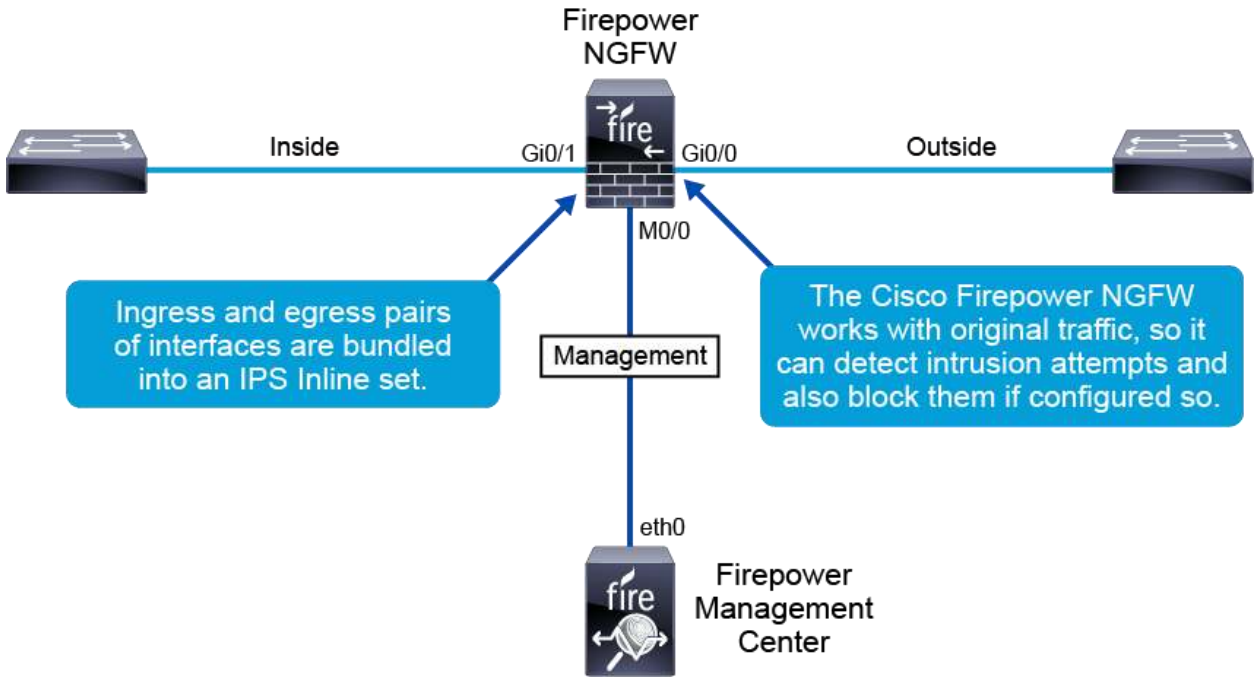
Cisco Firepower NGFW Deployments (cont.)

- **Cisco Firepower NGFW Transparent Mode**
  - A transparent firewall, is a Layer 2 firewall that acts like a "bump in the wire," and is not seen as a router hop to connected devices. However, like any other firewall, access between interfaces is controlled, and all of the usual firewall checks are in place.



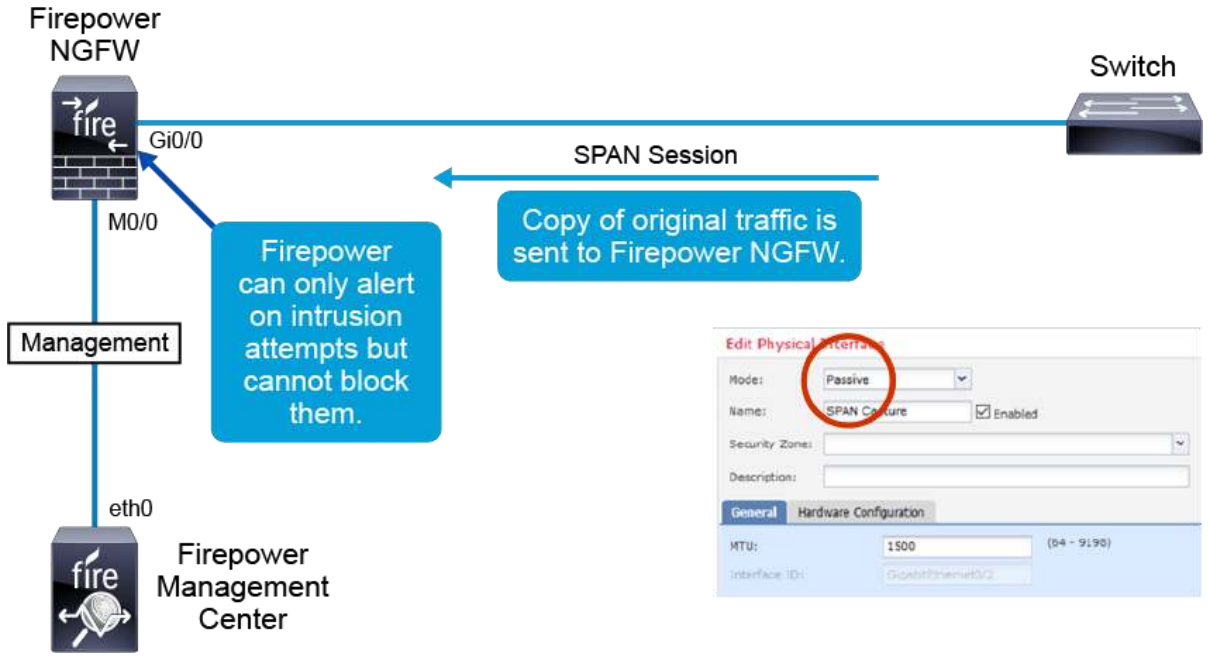
Cisco Firepower NGFW Deployments (cont.)

- **Cisco Firepower NGFW IPS Inline Mode**
  - In IPS inline mode, ingress and egress pairs of interfaces are bundled into an IPS inline set. An IPS sits inline, and all traffic inspected must pass through the IPS to reach its destination.



Cisco Firepower NGFW Deployments (cont.)

- **Cisco Firepower NGFW IDS Passive Mode**
  - In a Cisco Firepower IDS passive mode, you deploy the Cisco Firepower NGFW out-of-band from the flow of network traffic, it monitors traffic flowing across a network by using a Switched Port Analyzer (SPAN) or mirror port.

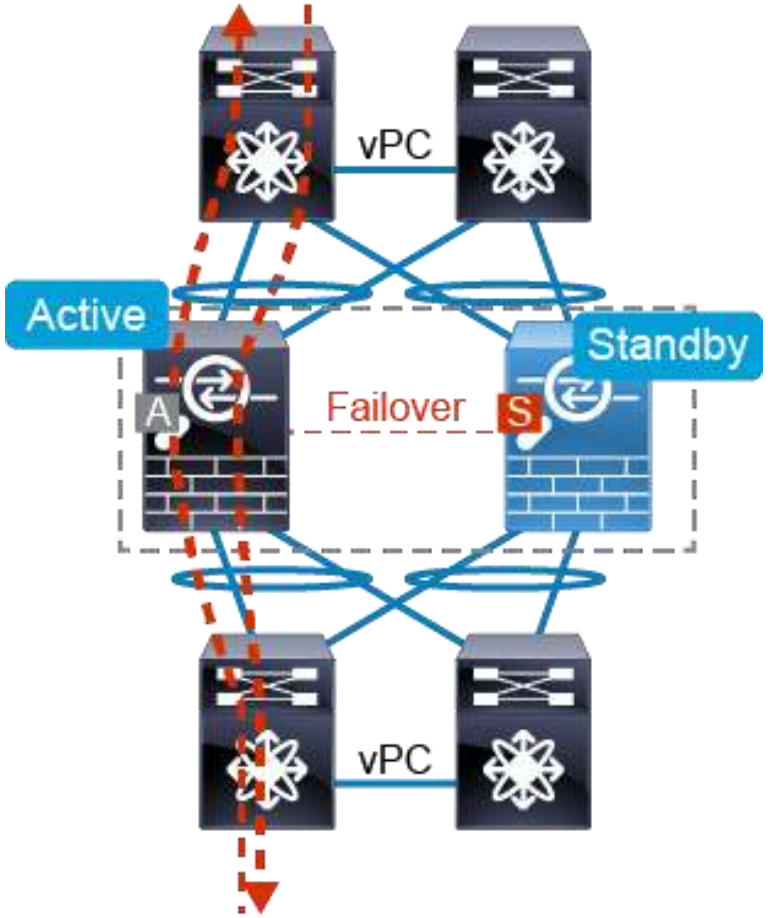


Cisco Firepower NGFW Deployments (cont.)

- **Cisco Firepower NGFW High Availability**
  - The Cisco Firepower NGFW supports both failover and clustering high-availability features that provide device-level redundancy.

- **With Cisco FTD operating system you have 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.

Cisco Firepower NGFW Deployments (cont.)



Cisco Firepower NGFW Deployments (cont.)

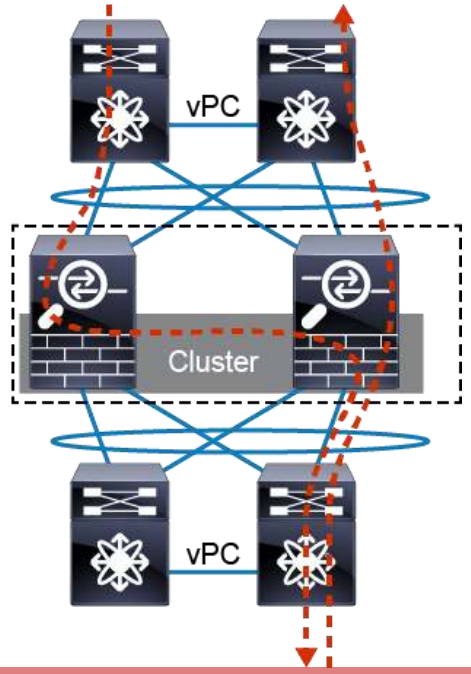
- Configuring high availability, also called failover, ***requires two identical Cisco FTD devices*** connected to each other through a dedicated failover link and, optionally, a state link.
- Cisco FTD supports active/standby failover, where one unit is the active unit and passes traffic.
- The standby unit does not actively pass traffic, but synchronizes configuration and other state information from the active unit.
- When a failover occurs, the active unit fails over to the standby unit, which then becomes active.

Cisco Firepower NGFW Deployments (cont.)

- The health of the active unit (hardware, interfaces, software, and environmental status) is monitored to determine if specific failover conditions are met.
- If those conditions are met, failover occurs.
- Failover delivers high availability rather than scalability.
- In failover, you are limited to two Cisco Firepower devices running Cisco FTD operating system.
- Clustering on the other hand lets you group multiple Cisco FTD units together as a single logical device.

Cisco Firepower NGFW Deployments (cont.)

- Clustering preserves the benefits of failover and implements scalability:
  - All member are managed as a single entity.
  - Connection states are preserved after a single member failure.
  - Scaling of throughput and maximum concurrent connections.



Cisco Firepower NGFW Deployments (cont.)

- **Cisco Firepower NGFW Appliance Virtualization**

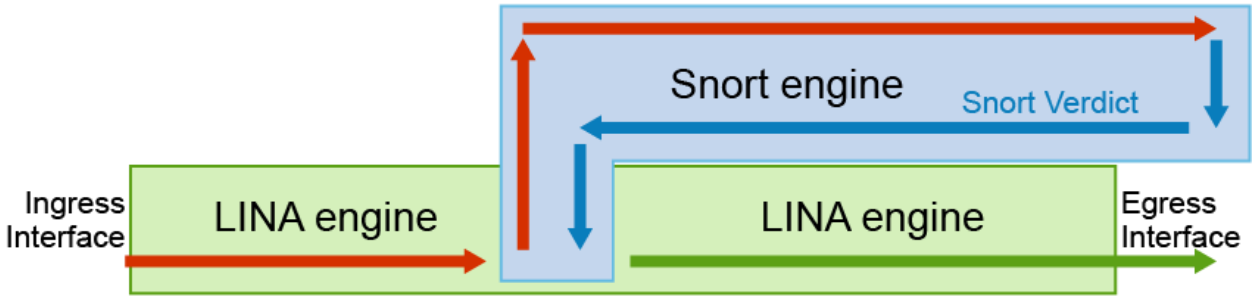
  - Cisco Firepower multi-instance feature was introduced in Cisco FTD version 6.3.
  - Instances are fully independent and fault-isolated and one NGFW instance cannot impact another's resources.
  - Traffic and management processing is completely separated between instances.
  - CPU, memory, and disk resources are dedicated to an instance at provision.
  - Once created, each instance operates within Cisco FMC like a separate device.
  - With multi-instance, each firewall instance is contained to its resources so no cross-impact on either management or data planes can take place.

Cisco Firepower NGFW Deployments (cont.)

- **Cisco Firepower NGFW Appliance Virtualization (cont.)**
  - With multi-instance support, administrators can create and run multiple independent instances of the Cisco FTD Software on the same hardware appliance.
  - Multi-instance is supported on the Cisco Firepower 4100 Series and the Cisco Firepower 9300 Series appliances.
  - Each instance of Cisco FTD running on the hardware appliance has dedicated hardware resources, thus providing the benefit of guaranteed performance per instance and also the benefit that one instance cannot affect the performance of another instance.

Cisco Firepower NGFW Packet Processing and Policies

- It is very important to understand how a packet is processed by the Cisco Firepower device.
- There are *many different types of policies* available on Cisco Firepower NGFW and the way these policies are configured affects the packet processing procedure.
- The Cisco FTD software on Cisco Firepower NGFW consists of two main engines, the **LINA (or ASA) engine** and the **Snort (Cisco Firepower) engine**.



Cisco Firepower NGFW Packet Processing and Policies (cont.)

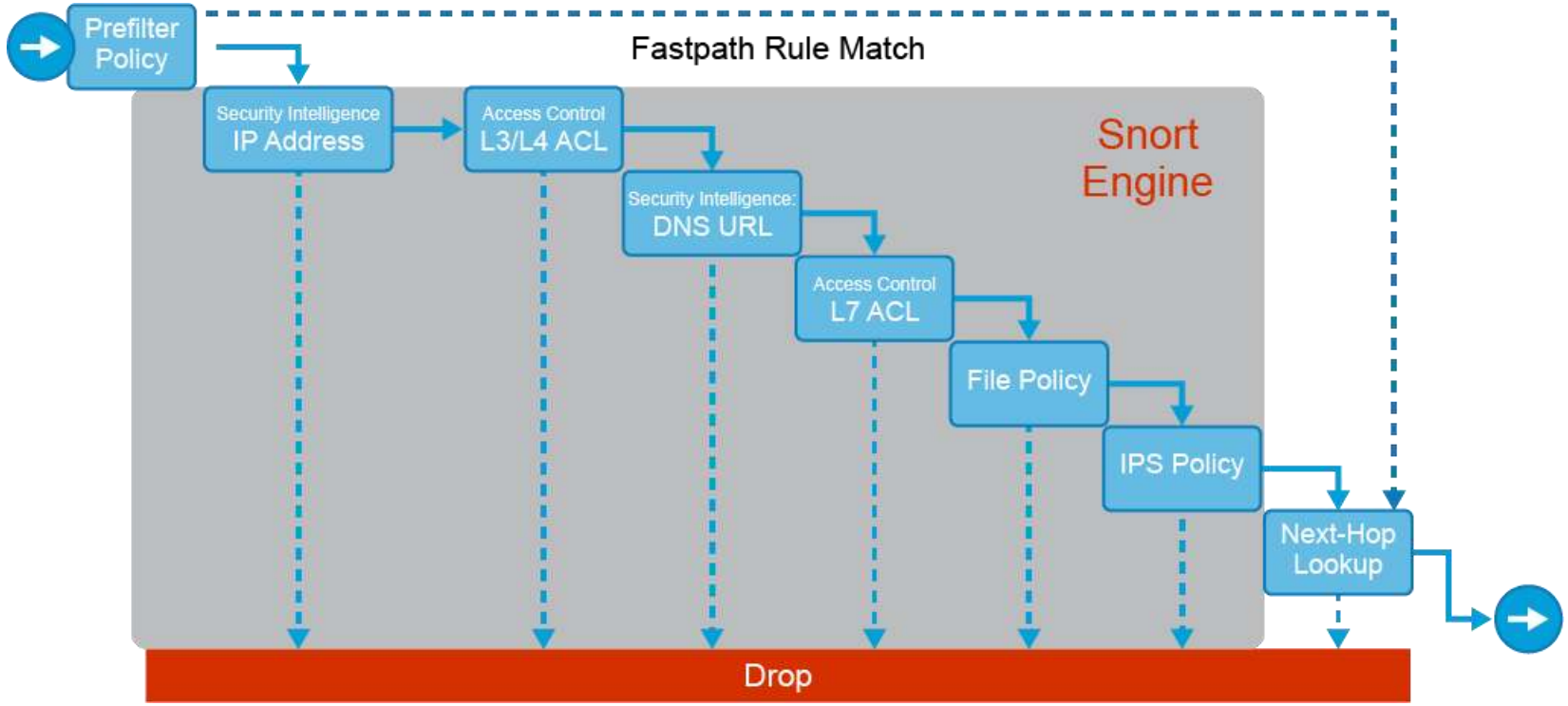
- The **LINA engine** is the base ASA firewall engine, responsible for traffic handling and filtering.
- Functions like IP routing, Layer 3/Layer 4 ACL filtering, NAT, and VPN, are performed by the LINA engine.
- The **Snort engine** handles traffic inspection—functions like security intelligence, IPS, Advanced Malware Protection (AMP), and Cisco URL Filtering that require inspection or modification beyond the Layer 3/Layer 4 header, are also handled by the Snort engine.

Cisco Firepower NGFW Packet Processing and Policies (cont.)

- Traffic arriving at a Cisco Firepower NGFW interface is processed by the LINA engine.
- If the traffic matches a profile that requires deeper inspection, the traffic is sent to the Snort engine.
- If the Snort engine returns a disposition of Safe or Benign, then the traffic is returned to the LINA engine for egress processing.

Cisco Firepower NGFW Packet Processing and Policies (cont.)

- For Cisco Firepower appliances that are managed through a central Cisco FMC, the different security policies are configured through several flexible policy options.

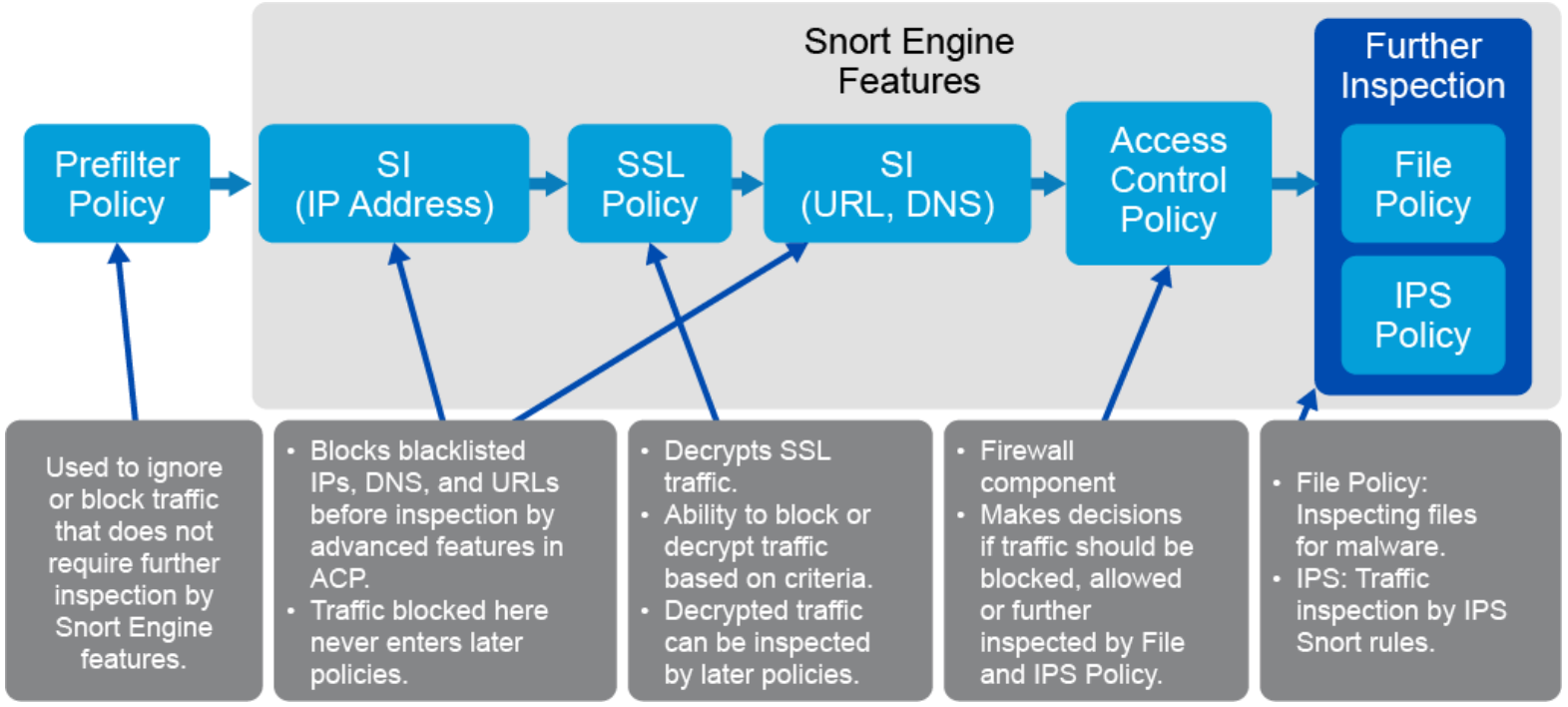


Cisco Firepower NGFW Packet Processing and Policies (cont.)

- Any of these policies mentioned above can drop the traffic according to the settings in respective policies.
- The packet processed in a sequence.
- For example, if traffic is blocked by IP address-based security intelligence feature, the packet never gets processed by the ACP, file policy, or IPS policy.
- On the other hand, packet is never processed by the file policy or IPS policy, if the packet gets blocked by the ACP rule.

Cisco Firepower NGFW Packet Processing and Policies (cont.)

- On the Cisco Firepower NGFW physical platforms, SSL decryption is performed in hardware instead of software for much higher SSL decryption performance.



Configure Cisco Firepower with FDM

LAB

Cisco Firepower NGFW Objects

- Cisco FMC uses objects in various areas of your Cisco Firepower System.
- Prior to configuring different policies in Cisco Firepower, you can define certain objects that are used to label a variable, or number of variables, of a similar type.
- These objects will be referenced later in the implementation process.
- Objects are used throughout the system, with the most common use in ACP.
- Objects are containers used throughout the Cisco Firepower NGFW configuration.
- Objects are reusable configurations that associate a name with a value. When you want to use that value, use the named object instead.

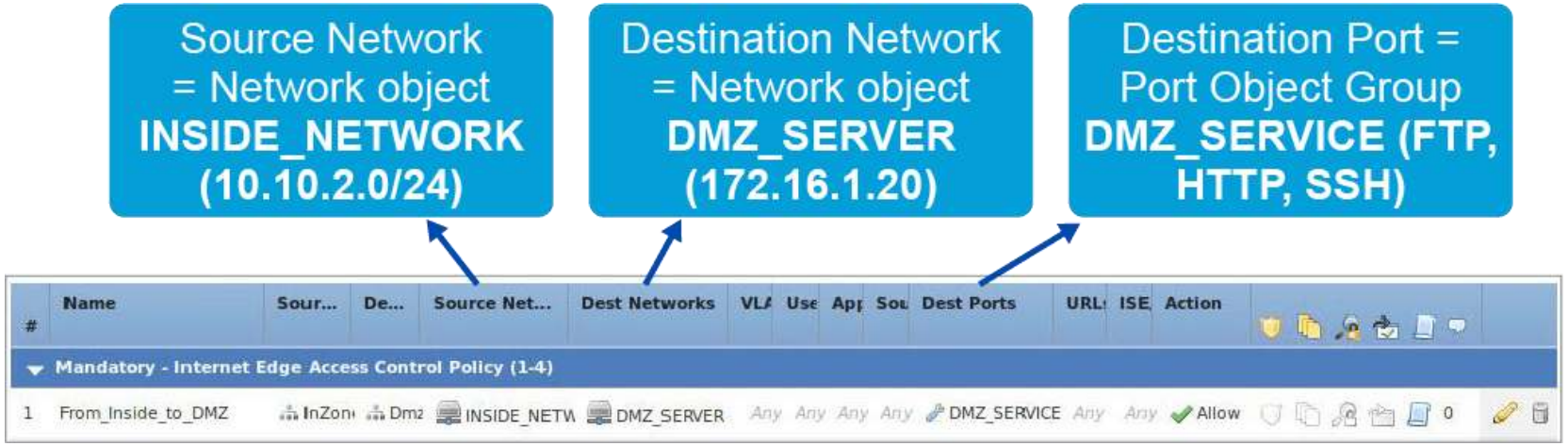
Cisco Firepower NGFW Objects (cont.)

- You can use the object manager in the Cisco FMC's GUI to create and manage objects and object groups.

- Objects are then linked to your policies, and therefore, the proceeding applies:
  - Usually you can also create objects as required directly within the policy (ACP for example).
  - Editing an object used in a policy will require a re-apply of that ACP.
  - You cannot delete an object that is used in a policy.

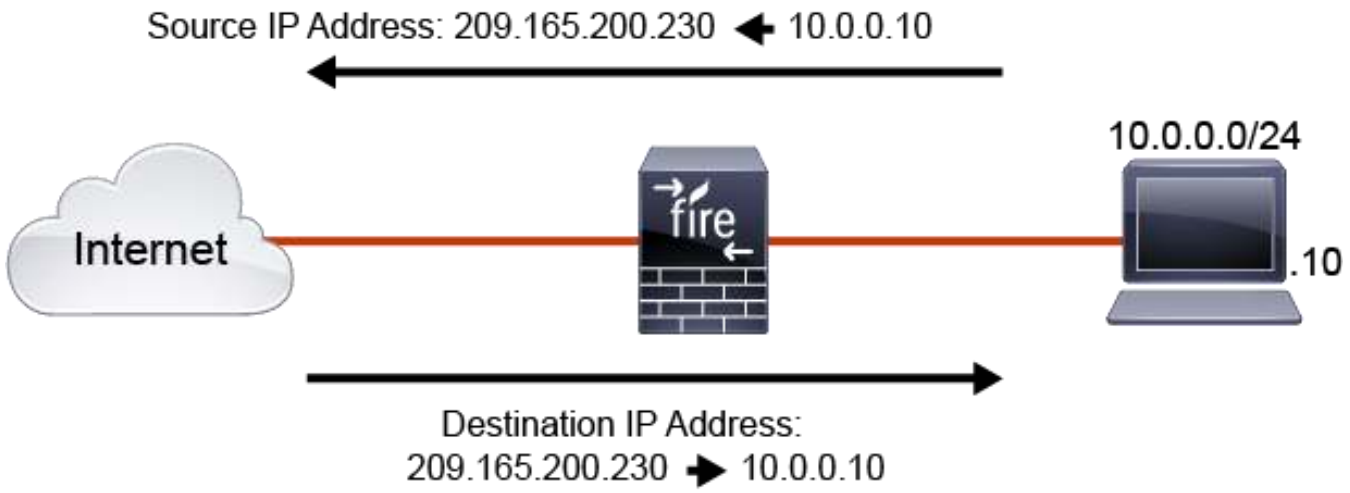
Cisco Firepower NGFW Objects (cont.)

- When you configure ACP rule you can define matching criteria for the rule, such as source network, destination network, destination port, and many more.
- In the example FTP, HTTP, and SSH traffic should be allowed from the inside network to the DMZ Server.



Cisco Firepower NGFW NAT

- The NAT technology was developed primarily to overcome IP Version 4 (IPv4) addressing problems that occurred with the expansion of the internet.
- NAT is required to translate private (local) IPv4 addresses into public (global) routable IPv4 addresses.



Cisco Firepower NGFW NAT (cont.)

- Cisco Firepower NGFW can implement NAT with two types in a similar way as on the Cisco ASA appliance:

  - **Auto NAT:** All NAT rules that are configured as a parameter of a network object are considered to be auto NAT rules. This is a quick and easy way to configure NAT for a network object.

  - **Manual NAT:** lets you identify both real and mapped source and destination IP address in a single rule. Specifying both the source and destination addresses lets you implement policy NAT by specifying that traffic from one source going to one destination will use different translation than traffic going from the same source to different destination.

Cisco Firepower NGFW NAT (cont.)

- Inside the policy, you configure NAT rules. Rules are divided into three sections as shown in the next figure:

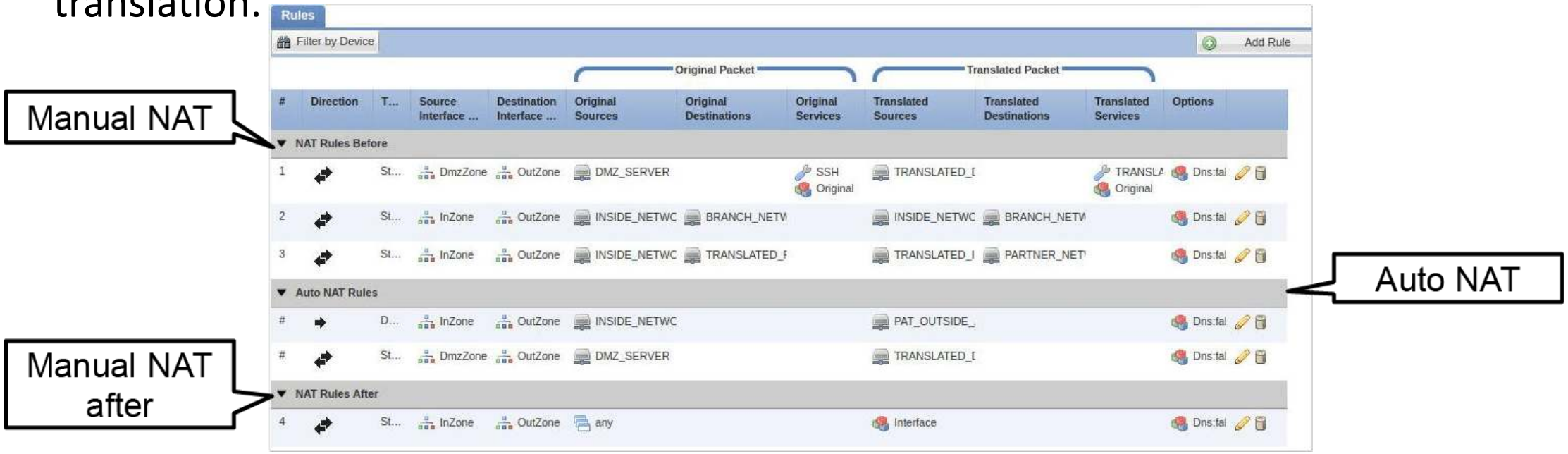
  - **NAT Rules Before:** This section is most commonly used to implement twice NAT, policy NAT, or NAT exceptions.

  - **Auto NAT Rules:** This section is most commonly used to implement simple rules for dynamic NAT or PAT and static NAT.

  - **NAT Rules After:** This rules are commonly used to implement catch-all scenario where previously non-matched traffic matched a default translation rule.

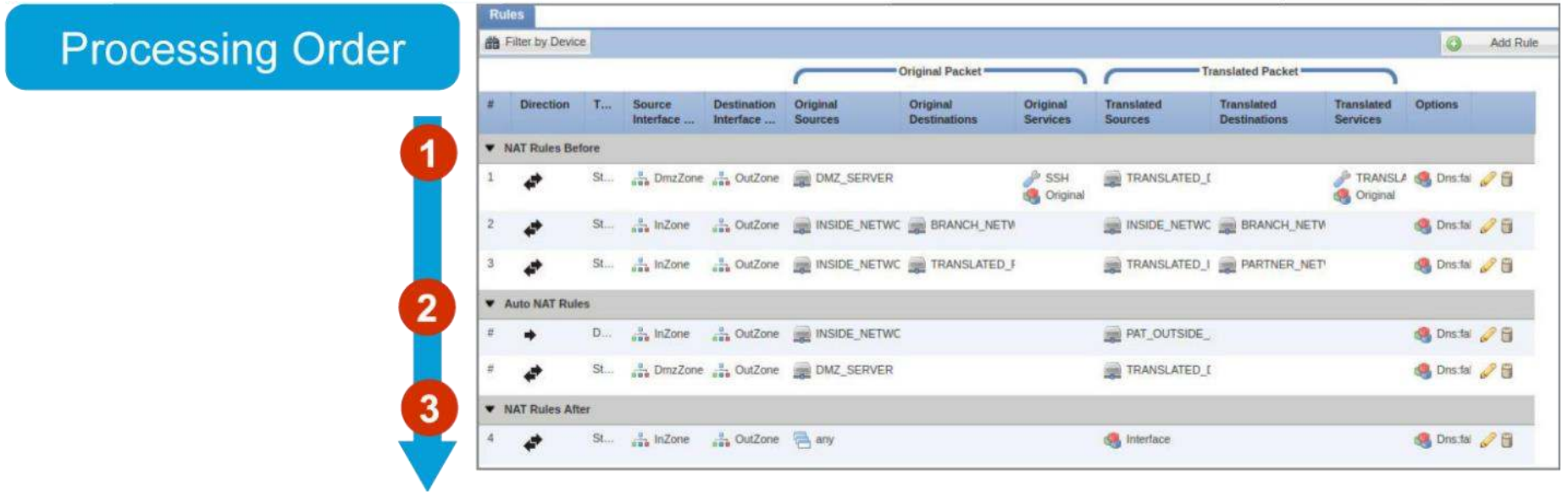
Cisco Firepower NGFW NAT (cont.)

- The Cisco Firepower NGFW appliance uses the entire NAT table to find a match when a packet needs to be translated.
- When no translation is found in the NAT table, the packet is forwarded without a translation.



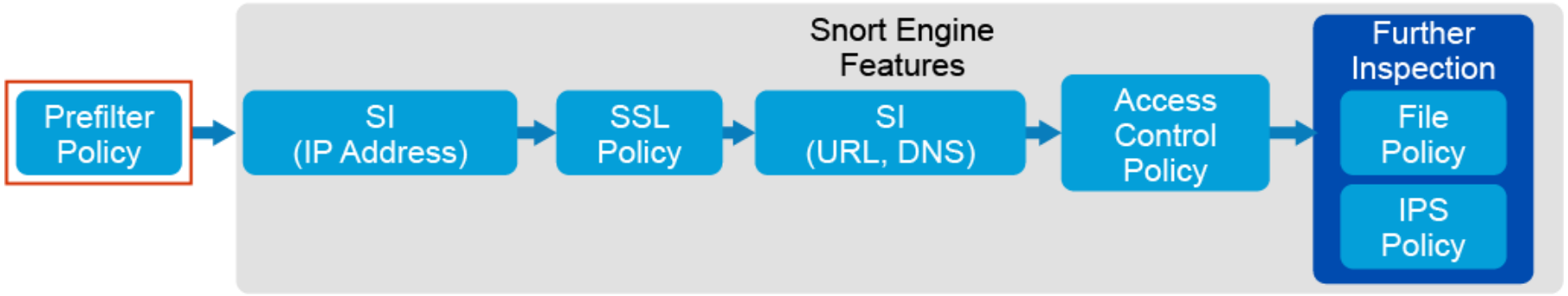
Cisco Firepower NGFW NAT (cont.)

- Auto NAT and manual NAT rules are stored in a single table that is divided into three sections.
- Section 1 rules are applied first, then section 2, and finally section 3, until a match is found. For example, if a match is found in section 1, sections 2 and 3 are not evaluated.



Cisco Firepower NGFW Prefilter Policies

- Traffic arriving at Cisco Firepower NGFW device is processed by Cisco ASA and Snort engine.
- 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.



Cisco Firepower NGFW Prefilter Policies (cont.)

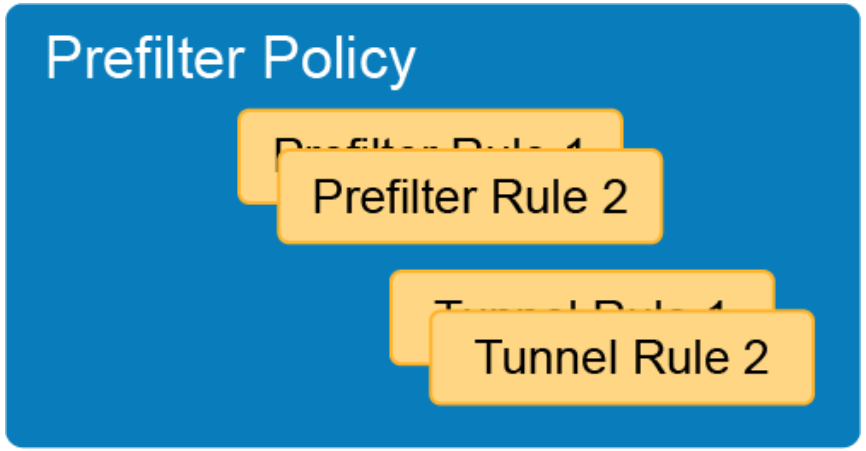
- **There are two reasons to use prefilter policies:**

1. 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.

2. Provide inspection for tunneled traffic based on tunnel endpoints, IP addresses, and encapsulation types.

Cisco Firepower NGFW Prefilter Policies (cont.)

- Prefilter policy consists of rules that are evaluated using the top-bottom approach.
- Each rule consists of simple conditions and associated actions.

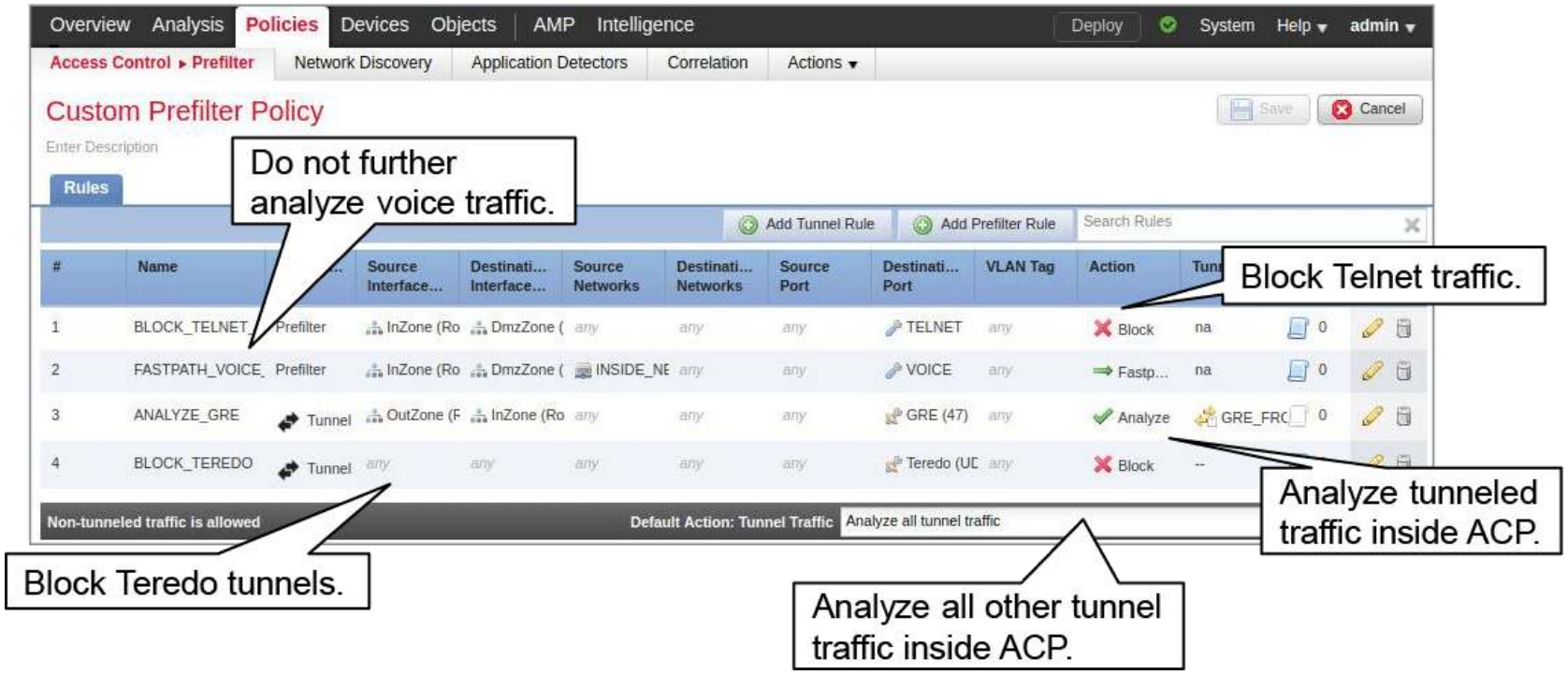


Cisco Firepower NGFW Prefilter Policies (cont.)

- The following actions are available when configuring prefilter rules:
  - **Block:** discard traffic without further inspection.
  - **Fastpath:** permits traffic without sending the traffic to Snort inspection. On certain Cisco Firepower platforms, fastpathed flows are eligible for flow offload functionality where traffic is switched inside a network interface card.
  - **Analyze:** sends traffic to further (Snort) inspection, based on configured ACP rules.

Cisco Firepower NGFW Prefilter Policies (cont.)

- **Prefilter Policies Use Case**



Cisco Firepower NGFW Prefilter Policies (cont.)

- The policy consists of four rules:

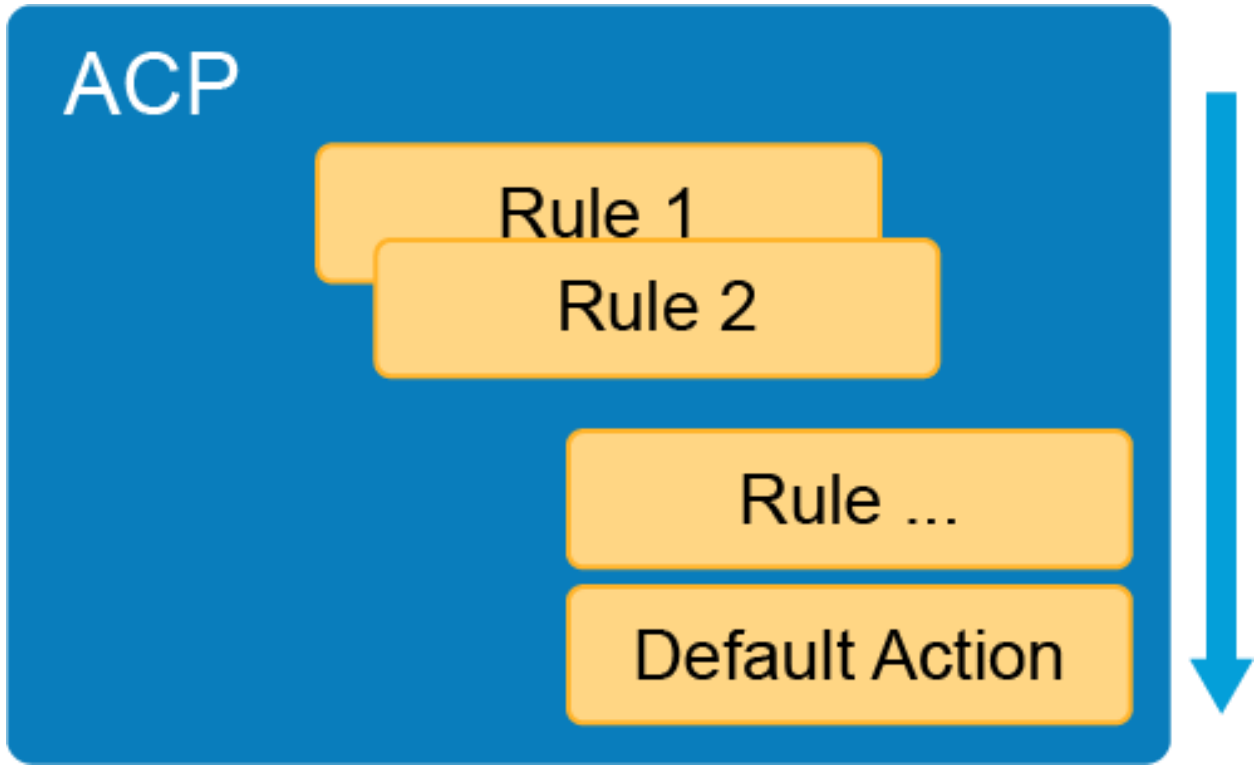
1. The first rule is the prefilter rule and blocks Telnet traffic from InZone going to DmzZone, based on destination TCP port. Note that a TELNET object does not represent the application, but is rather a port object, representing TCP port 23.
2. The second rule is prefilter rule and allows voice traffic from InZone going to DmzZone, based on destination UDP ports. The traffic is fastpathed, thus skipping all Snort inspections.
3. The third rule is the tunnel rule and matches GRE traffic. Traffic is sent for further analyses to ACP, where it could be matched based on inner header and inspected using Snort inspection.
4. The last rule is the tunnel rule and immediately blocks Teredo IPv6 tunnels.

Cisco Firepower NGFW Access Control Policies

- Access control is a hierarchical policy-based feature that allows you to specify, inspect, and log network traffic.
- Each managed Cisco Firepower NGFW device is assigned one ACP.
- 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.

Cisco Firepower NGFW Access Control Policies (cont.)

- The ACP consists of rules that are processed using top-down, first match approach.



Cisco Firepower NGFW Access Control Policies (cont.)

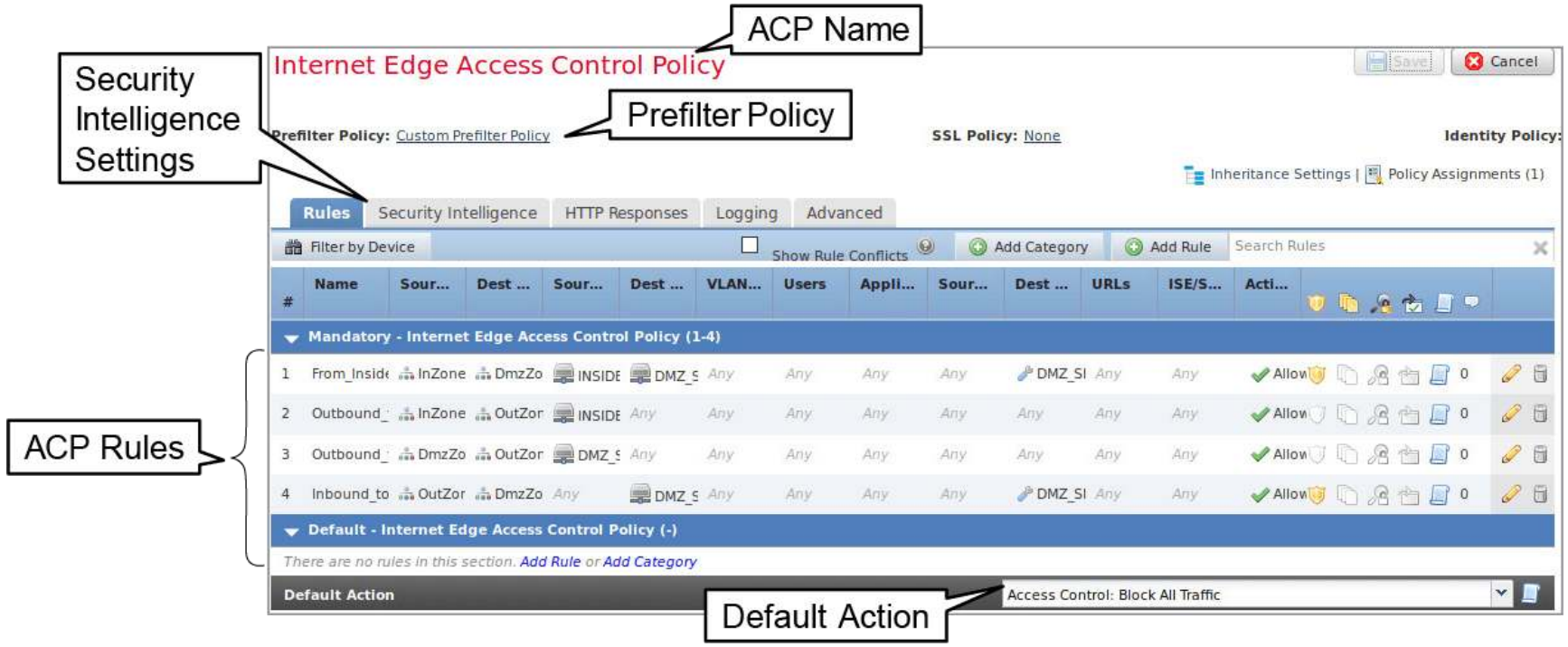
- When traffic matches configured conditions inside a rule, the ACP applies the configured action for that rule, which can generally allow, block, or send traffic to further analyses.
- If traffic matches no rules, then the system applies the action defined in the default action of the ACP.
- **The only exception** to the first match rule is **monitor action**, which only logs traffic, and continues matching against the subsequent ACP rules.

Cisco Firepower NGFW Access Control Policies (cont.)

- A Cisco Firepower NGFW device must have an ACP applied to perform operations, and only one ACP can be applied to a device at any given time.
- However, it is typical to create many ACPs to manage changed environments.
- ACPs use hierarchical implementation that can be used for multitenancy.
- ACPs can be nested, where descendant ACP inherits rules and settings from its direct parent policy.

Cisco Firepower NGFW Access Control Policies (cont.)

- Traffic requires an ACP to proceed through the system.
- Each ACP has a name that allows unique identification inside the system.



Cisco Firepower NGFW Access Control Policies (cont.)

ACP Rules

- The next figure shows ACP rule components.

Cisco Firepower NGFW Access Control Policies (cont.)

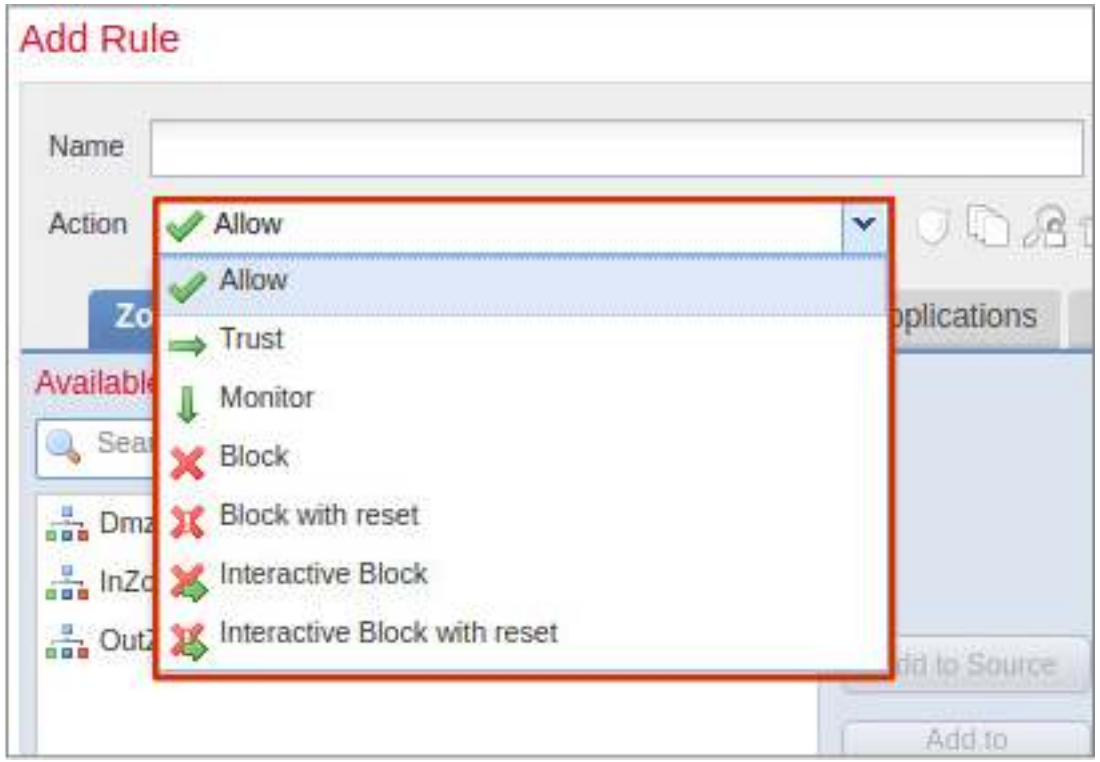
- Each ACP rule consists of:

  - **Name:** used to uniquely identify a rule.
  - **Conditions:** identify the type of traffic that the rule handles. A rule can have multiple conditions. Traffic must match all the conditions in the rule for the rule to apply to traffic.
  - **Action:** Each rule must have an action associated with it. The action specifies what happens with traffic that matched a rule.
  - **IPS and file policy inspection settings:** Influence if traffic will be sent for furter 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.

Cisco Firepower NGFW Access Control Policies (cont.)

ACP Rules Actions

- Each rule that is created, must have an action associated with it.



Cisco Firepower NGFW Access Control Policies (cont.)

- The previous figure shows available 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. Based on configured conditions, the system may also skip security intelligence checks.
  - **Block and block with reset:** deny traffic without further inspection of any kind. Block with reset also resets the connection.

Cisco Firepower NGFW Access Control Policies (cont.)

- The previous figure shows available actions (cont.)

  - **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. Rather, traffic is matched against additional rules to determine whether to allow or block it.

Cisco Firepower NGFW Access Control Policies (cont.)

- 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.

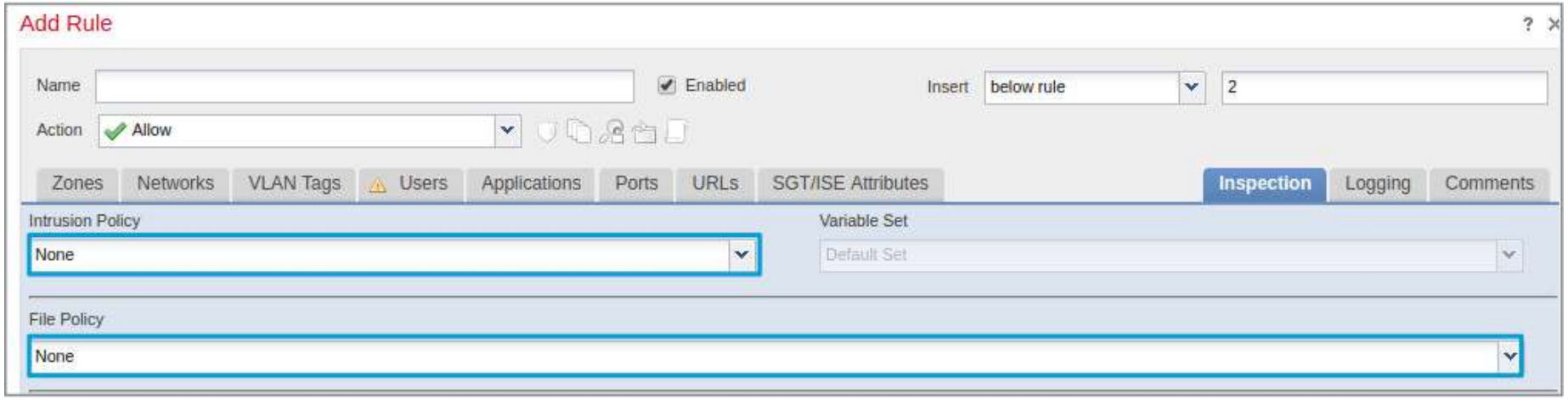
Cisco Firepower NGFW Access Control Policies (cont.)

ACP Rules Further Inspections

- For traffic that is allowed (either through allow or interactive block action) you have two options for further inspection:
  - **IPS policy:** uses intrusion rules (also known as Snort rules) to examine packets for threats.
  - **File and malware policy:** allows to detect and block certain filetypes or examine files for malware.

Cisco Firepower NGFW Access Control Policies (cont.)

- The next figure shows that IPS and the file policy for a rule are configured under the Inspection tab when editing or adding an ACP rule.



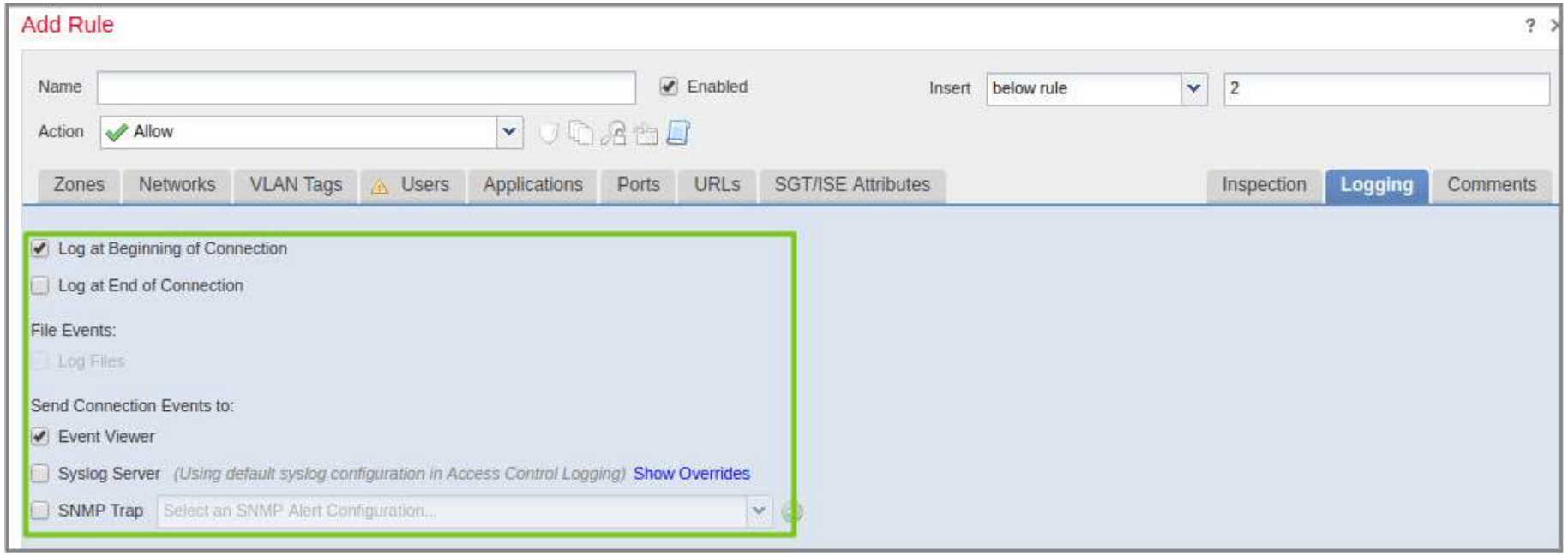
Cisco Firepower NGFW Access Control Policies (cont.)

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.
- Settings inside ACP give you granular control over which connections you log, when you log them, and where you store the data.
- Usually, you can log a connection at its beginning or its end, or both.
- When you log a connection, the system generates a connection event.

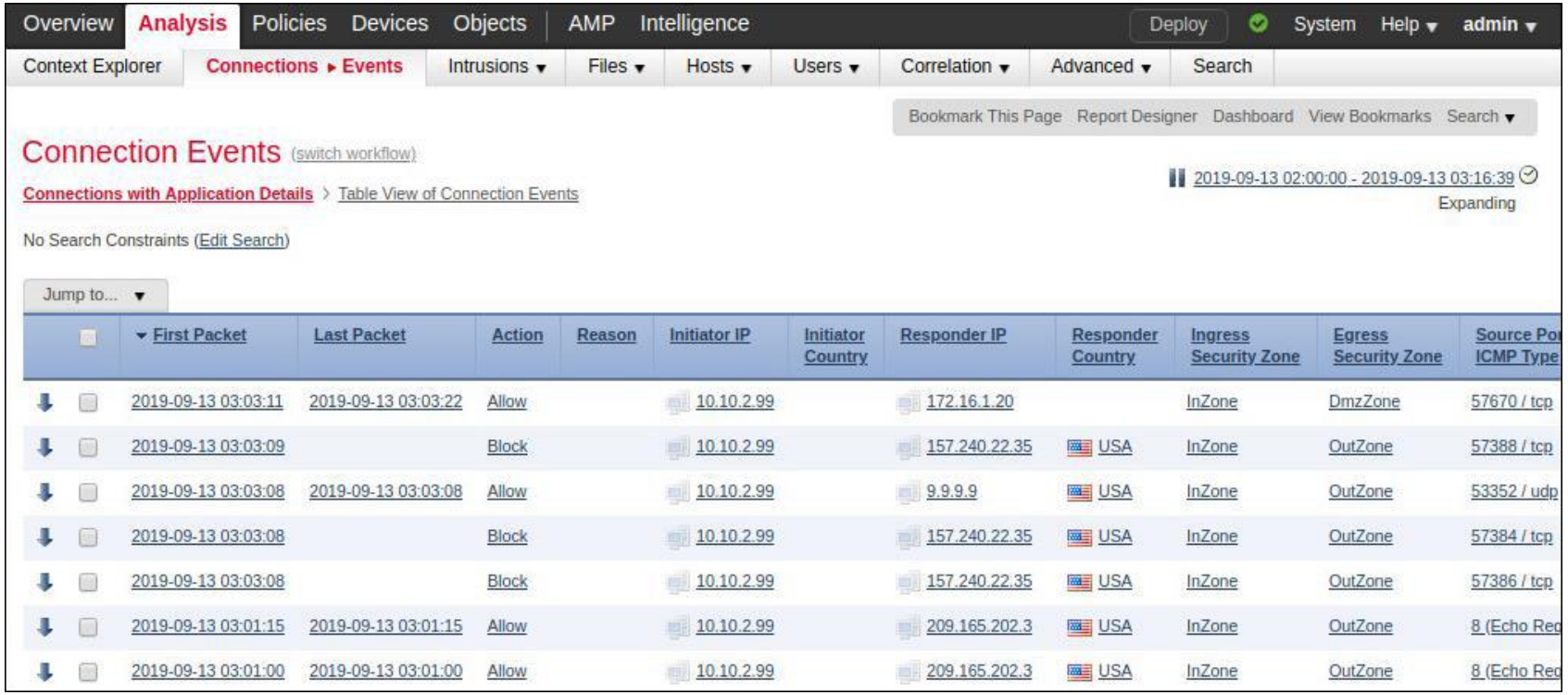
Cisco Firepower NGFW Access Control Policies (cont.)

- You can configure logging settings for each ACP rule as shown in the next figure.



Cisco Firepower NGFW Access Control Policies (cont.)

- Connection events contain data about the monitored connections, The figure shows how connection events look like inside Cisco FMC.

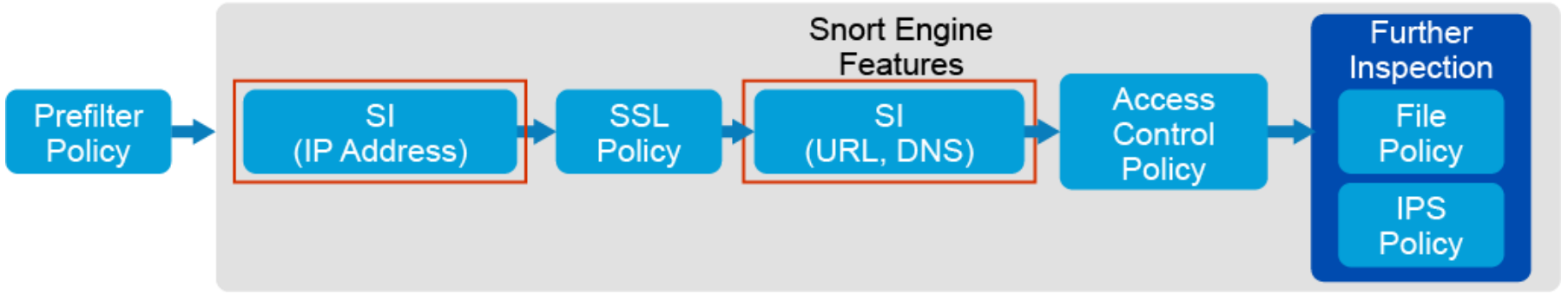


Cisco Firepower NGFW Security Intelligence

- As a first line of defense against malicious traffic, the Cisco Firepower NGFW device uses the security intelligence feature, which allows you to immediately blacklist (block) connections, based on the latest reputation intelligence, removing the need for a more resource-intensive, in-depth analysis.
- Security intelligence functionality also generates special events, called security intelligence events, when a connection matches a blacklisted object.
- Security intelligence works by matching traffic against a whitelist and a blacklist and blocking traffic to or from IP addresses, URLs, or DNS that are on the blacklist.

Cisco Firepower NGFW Security Intelligence (cont.)

- The figure shows where in the Cisco Firepower NGFW processing pipeline security intelligence takes place.
- Filtering based on IP addresses takes place immediately after prefilter policies and as a first step inside an ACP.
- In case of filtering based on URLs or DNS names, system first performs SSL decryption, since requested URLs may be sent inside an encrypted SSL session.



Cisco Firepower NGFW Security Intelligence (cont.)

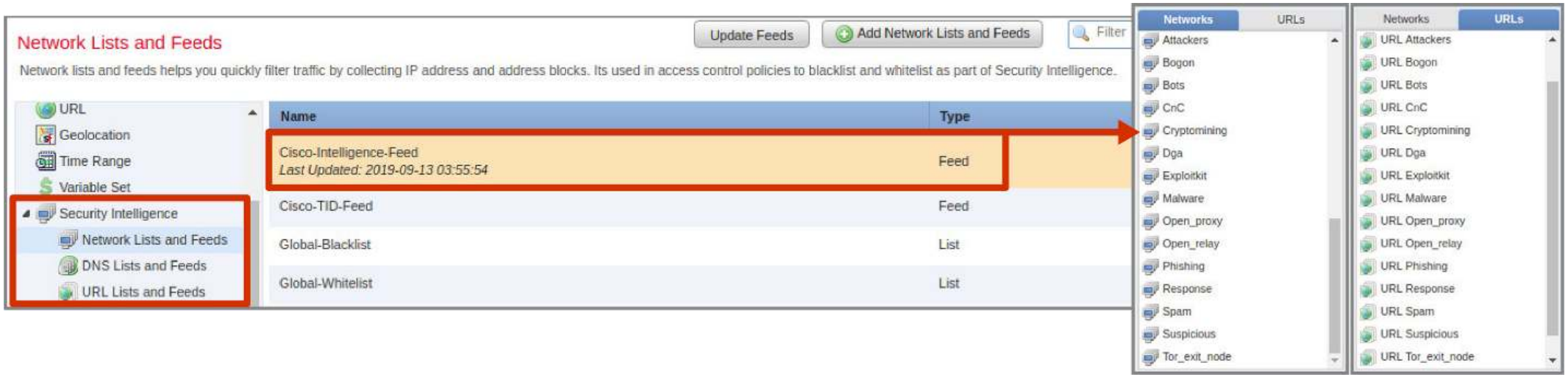
- Security intelligence blacklist and whitelist objects are managed in inside Cisco FMC object manager.
- Security intelligence places traffic into two categories:

  - Blacklist:
    - For traffic that is considered malicious.
    - Matching traffic is blocked or monitored. For blocked traffic no further inspection is performed.

  - Whitelists:
    - Used to override objects that appear in blacklist.
    - Whitelist matches do not generate events.

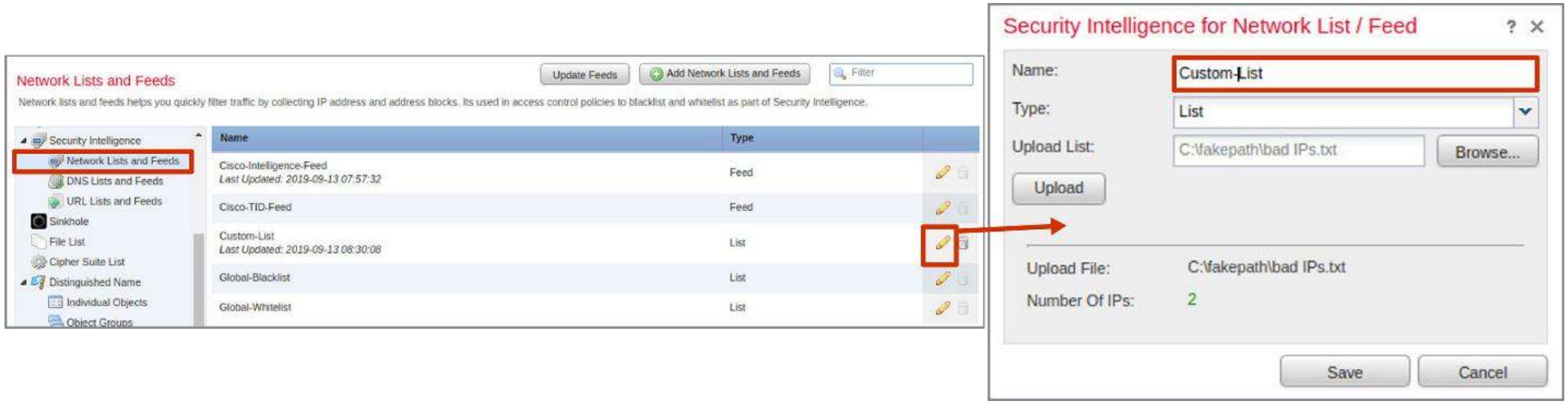
Cisco Firepower NGFW Security Intelligence (cont.)

- Security intelligence feed provides an automatic way to download updates to your objects.



Cisco Firepower NGFW Security Intelligence (cont.)

- The previous figure shows how to upload a list file to Cisco FMC.



Cisco Firepower NGFW Security Intelligence (cont.)

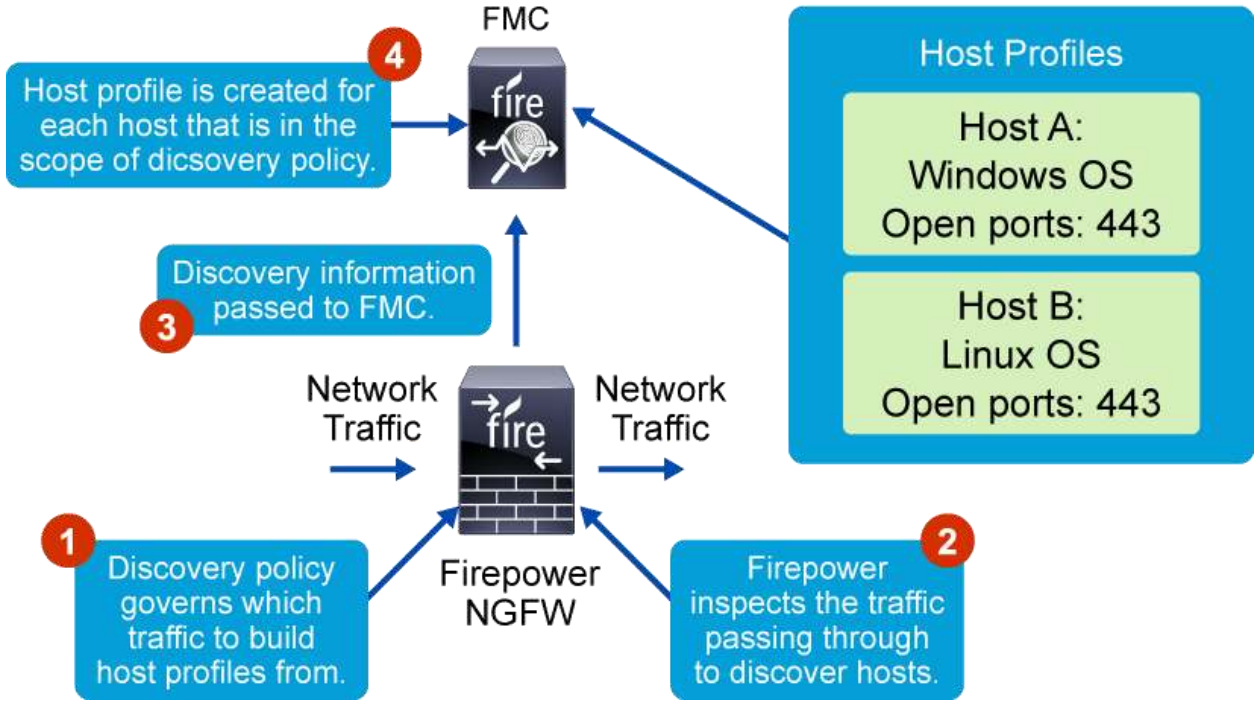
- With the *Whitelist Now* and *Backlist Now* options, which are available from the events view, by right-clicking and IP address, URL, or a DNS name, you can immediately take action on entries by adding them to the global lists.

Cisco Firepower NGFW Discovery Policies

- Cisco Firepower Discovery is the process of collecting information about hosts and users in your environment.
- Cisco Firepower inspects the traffic passing through the Cisco Firepower NGFW to discover both users and hosts. Hosts are discovered by configuring a discovery policy.
- Discovery is an integral part of the Cisco Firepower System.
- The data collected about hosts, applications, operating systems, services, users, and vulnerabilities is used throughout the system for analysis and automation of security protection:

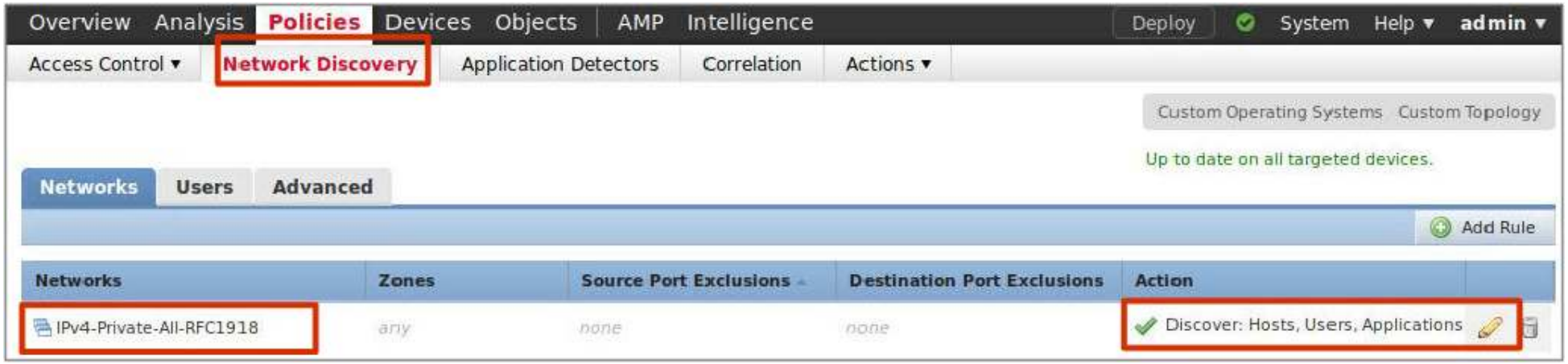
Cisco Firepower NGFW Discovery Policies (cont.)

- The network discovery policy is how you manage your discovery information.
- Upon initial setup, the network discovery policy is not configured to perform host discovery.



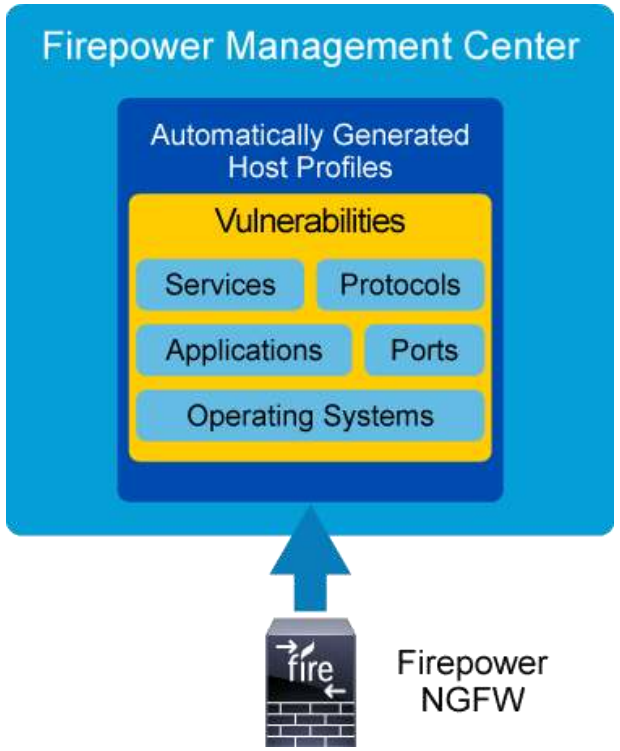
Cisco Firepower NGFW Discovery Policies (cont.)

- You create rules in the discovery policy to define what is to be discovered in your network and what will not be discovered.
- For example, you can define private IP address ranges only to be discovered.
- This way, the system does not automatically build host profiles on traffic that exists on the internet, outside your network.



Cisco Firepower NGFW Discovery Policies (cont.)

- A host profile provides a complete view of all the information that the system has gathered about a single host.



Cisco Firepower NGFW Discovery Policies (cont.)

- Host profiles can also provide you with the following information:
  - 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.

Cisco Firepower NGFW Discovery Policies (cont.)

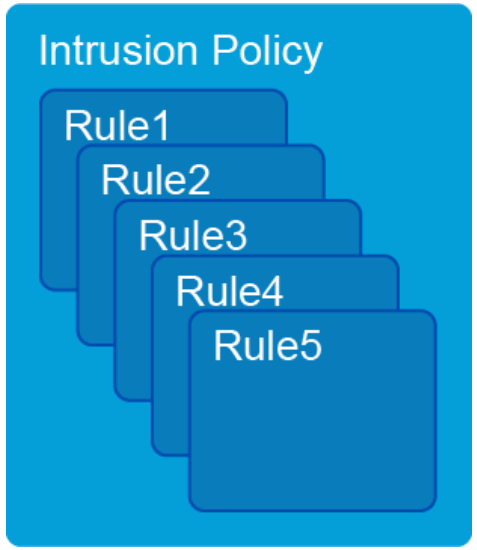
- Vulnerabilities are automatically assigned to a host based on the operating system, applications, and services seen on the discovered host.
- For example, Cisco Firepower NGFW detects Windows 7 on the host.
- This information on operating system will be added to the operating system section of the host profile, along with any vulnerabilities associated to that version of Windows 7.
- Vulnerabilities for your host profiles come from the Vulnerability Database (VDB) in the Cisco Firepower System and are automatically populated based on what is detected on that host.

Cisco Firepower NGFW Discovery Policies (cont.)

- 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 NGFW IPS Policies

- Intrusion policies are defined sets of intrusion detection and prevention configurations that inspect traffic for security violations and can block or alter malicious traffic.
- Intrusion policies are invoked by your ACP and are the system's last line of defense before traffic is allowed to its destination.



Cisco Firepower NGFW IPS Policies (cont.)

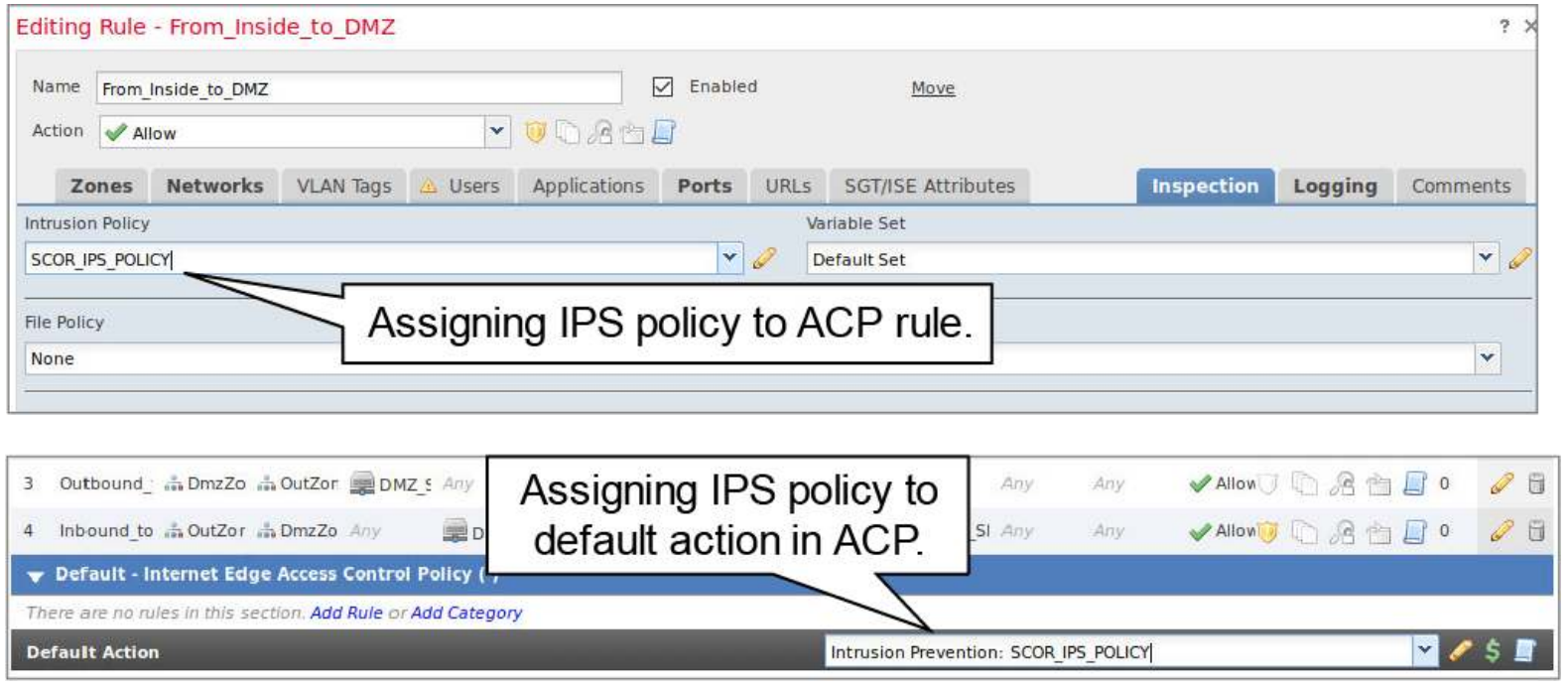
- Snort is free, open-source software that acts as a network intrusion detection system.
- Cisco Firepower technology is based on this software.
- An intrusion rule, also known as a Snort rule, is a specified set of keywords and arguments that the system uses to detect attempts to exploit vulnerabilities in your network.
- As the system analyzes network traffic, it compares packets against the conditions specified in each rule, and triggers the rule if the data packet meets all the conditions specified in the rule.

Cisco Firepower NGFW IPS Policies (cont.)

- Snort rules can be created by anyone.
- Snort is a free, open-source system.
- You have the option to create your own Snort rules and import them into the Cisco FMC.
- The Cisco Firepower System is shipped with all available Snort rules that are regularly updated by Cisco Talos.

Cisco Firepower NGFW IPS Policies (cont.)

- After you configure IPS policies, you need to assign IPS policy to ACP.
- An intrusion policy can be assigned to an individual access policy rule or to the default action.



Cisco Firepower NGFW IPS Policies (cont.)

- When the Cisco Firepower System identifies a possible intrusion, it generates an intrusion event, which is a record of the date, time, the type of exploit, and contextual information about the source of the attack and its target.

Cisco Firepower NGFW Malware and File Policies

- Cisco Firepower gives you means to detect the movement of files in your networks and to take appropriate action.
- For example, office documents that are exchanged between users in internal network segments may be part of normal collaboration between co-workers, but documents that are sent to outsiders can indicate sensitive data leakage.
- With the file detection feature, you can choose to simply be alerted, or you can block the file and prevent it from leaving the enterprise.

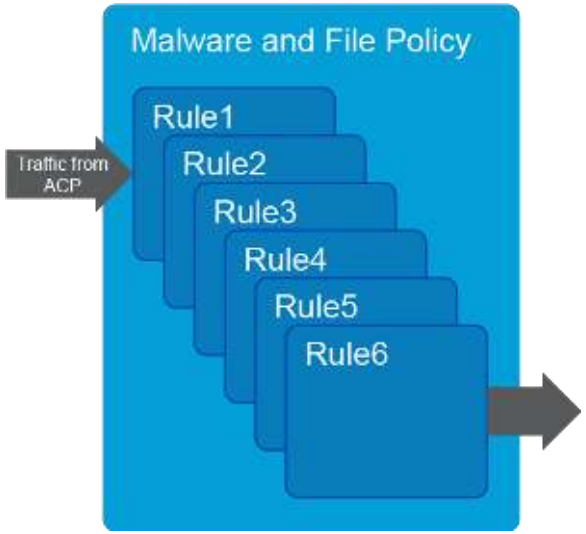
Cisco Firepower NGFW Malware and File Policies (cont.)

- Cisco Firepower NGFW offers file type detection feature which can detect or block files based on file type.
- Example of using this feature is blocking all PDF files leaving your enterprise (the system does not look for malicious content when using this feature).

Cisco Firepower NGFW Malware and File Policies (cont.)

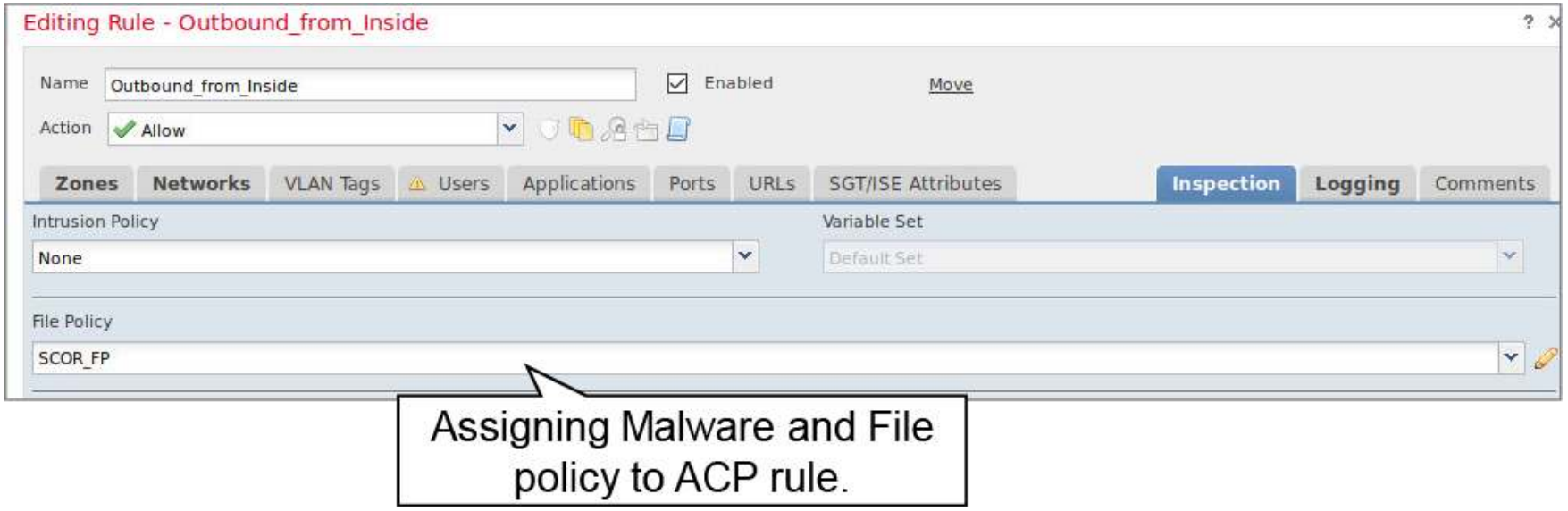
Malware and File Policy Rules

- A malware and file policy is a set of configurations that the system uses to perform malware detection and file control, as part of your overall access control configuration. This association ensures that before the system passes a file in traffic that matches an access control rule's conditions, it first inspects the file.



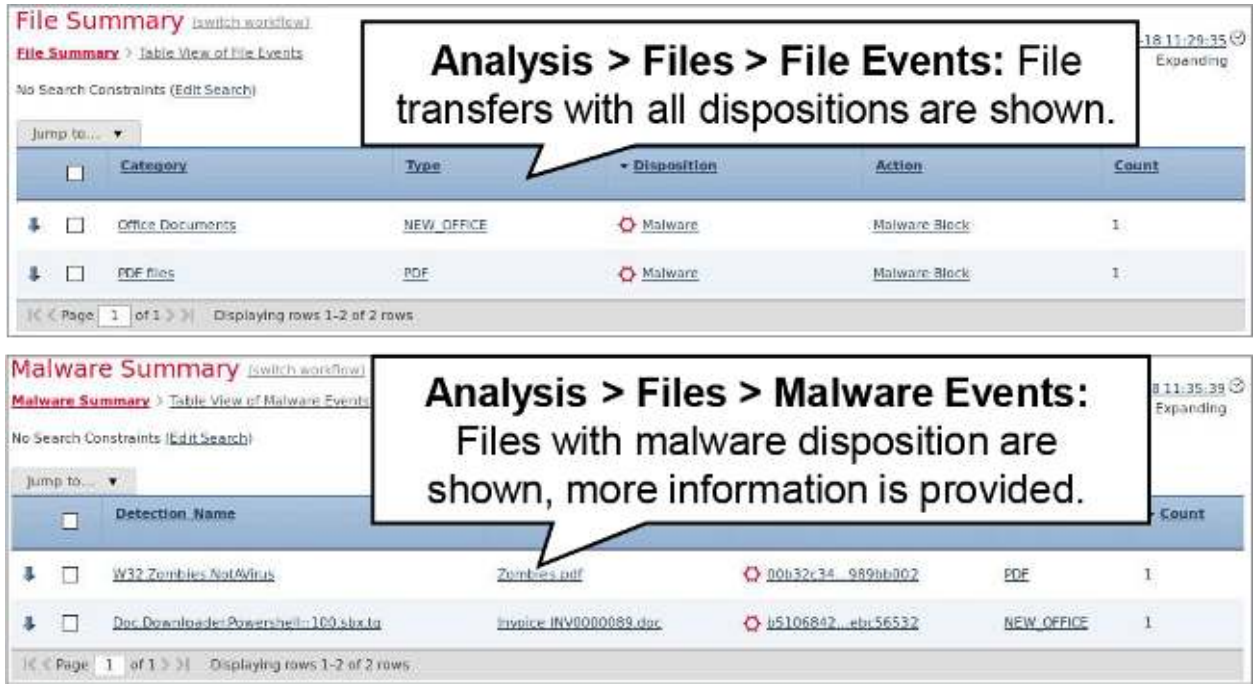
Cisco Firepower NGFW Malware and File Policies (cont.)

- After you configure Malware and file policy, you need to assign file and Malware policy to ACP rule.
- Malware and file policy can be assigned to an individual access policy rules only, it is not possible to assign Malware and file policy to the default action of the ACP.



Cisco Firepower NGFW Malware and File Policies (cont.)

- There are two menus in the Cisco FMC GUI where you can see events related to malware and file policy:



Configure Cisco Firepower with FMC

LAB