Securing Networks with

Cisco FTD

Chapter 9

Prefilter Policy

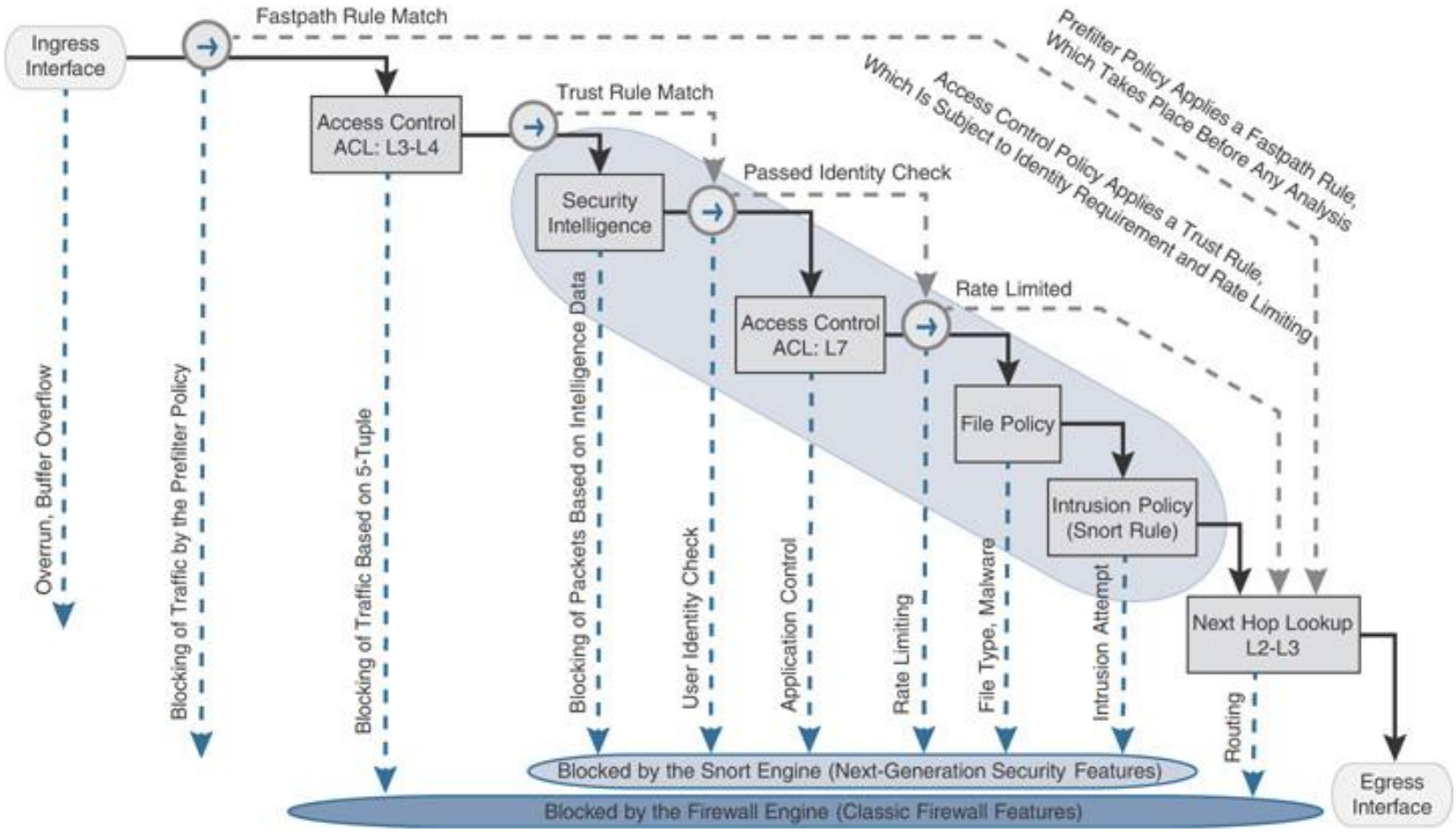
Mohsen Kheradmand

The objectives of this chapter are to learn about

- Configuration and deployment of prefilter policy
- Differences between prefilter policy and access control policy
- Different ways to bypass deep packet inspection
- Inspection of encapsulated traffic

Prefilter Policy: Rules and Actions

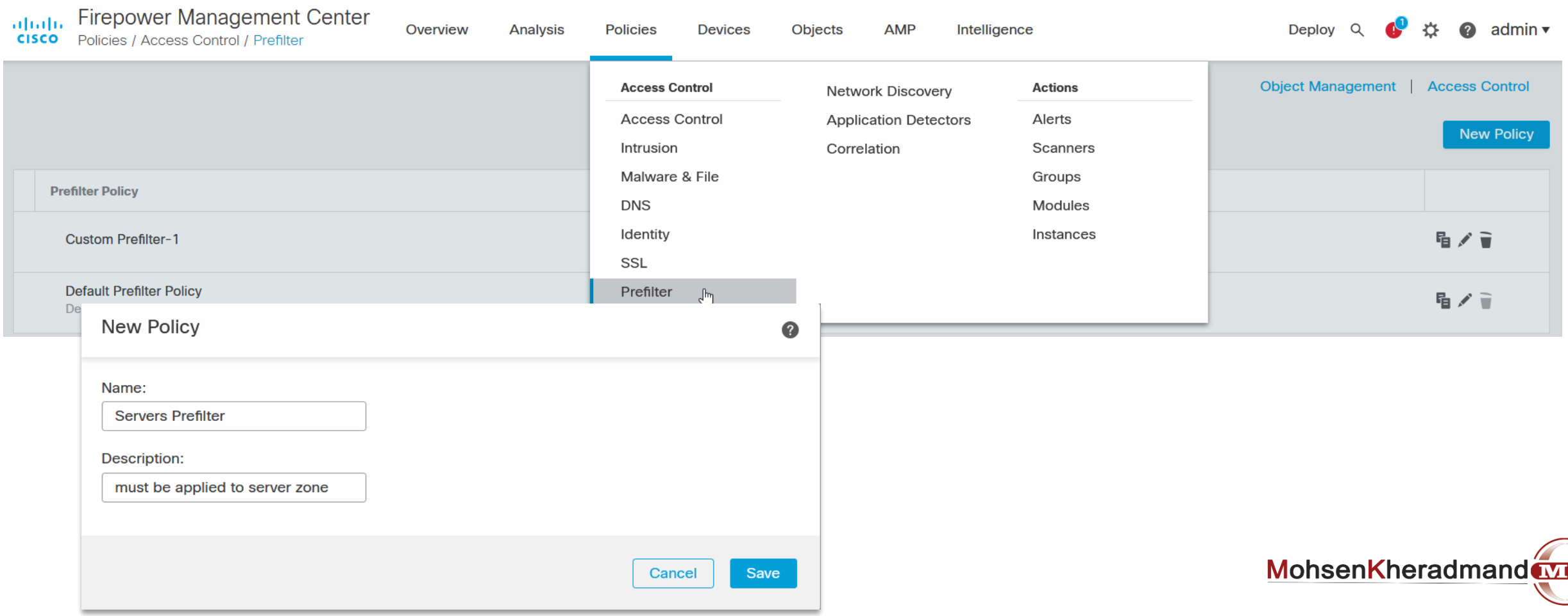
- A prefilter policy acts on traffic earlier and faster than the access control policy
- Prefilter Rule Can Filter Traffic Based on Interface, Network, VLAN, and Port



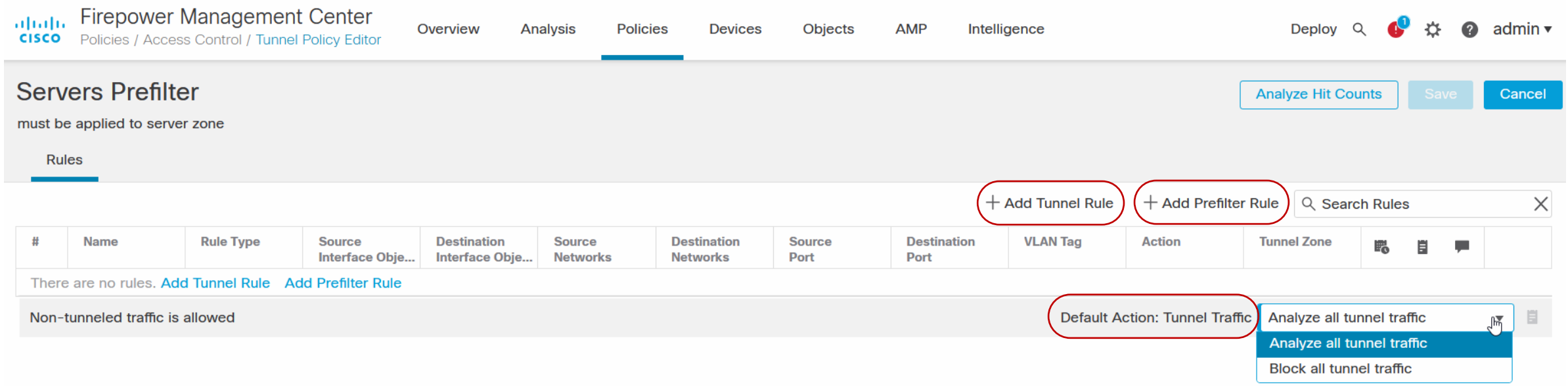
Potential Reasons for a Packet Drop by a Threat Defense

Prefilter Policy: Configuration

- Policies > Prefilter > New Policy
- Enter a name for new policy (or description) and save it



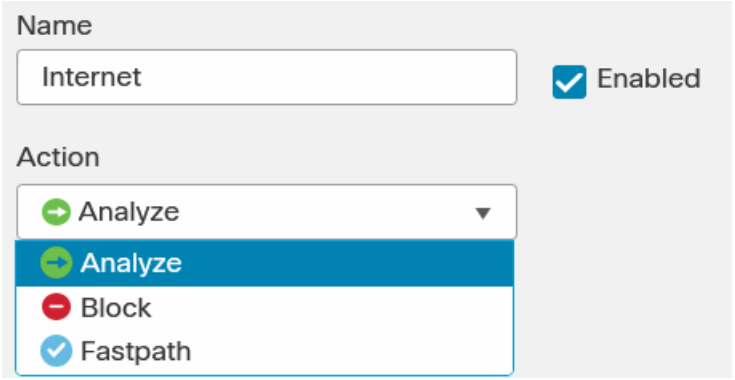
Prefilter Policy: Configuration



There are three ways to assign an action to the traffic:

- Tunnel rule
  Filters tunnel traffic that is encapsulated by an additional IP header (i.e. : GRE, IP-in-IP, and IPv6-in-IP)
- Prefilter rule
  Filter traffic based on basic networking constraints (IP address, port number ,VLAN tag, and interface)
- Default action
  - Act on a traffic that is not matched to Tunnel rules (it is applicable only for tunnel traffic

Prefilter Policy: Configuration



Both a tunnel rule and prefilter rule offer three types of actions:

- **Analyze**
  - Allows a threat defense to perform further analysis on matching traffic
  - Inspected and controlled by access control policies, intrusion policies, and malware and file policies
- **Block**
  - This action blocks matching traffic immediately
  - No further inspection is performed by any policy
- **Fastpath**
  - This action bypasses any further security analysis
  - The matching traffic is no longer subject to rate limit and identity requirements

Bypassing Deep Packet Inspection

Secure Firewall offers two types of rule actions to bypass deep packet inspection :

➢ Fastpath action:

- A prefilter rule with the Fastpath action, bypass the traffic before a packet reaches the firewall engine and Snort engine

➢ Trust action

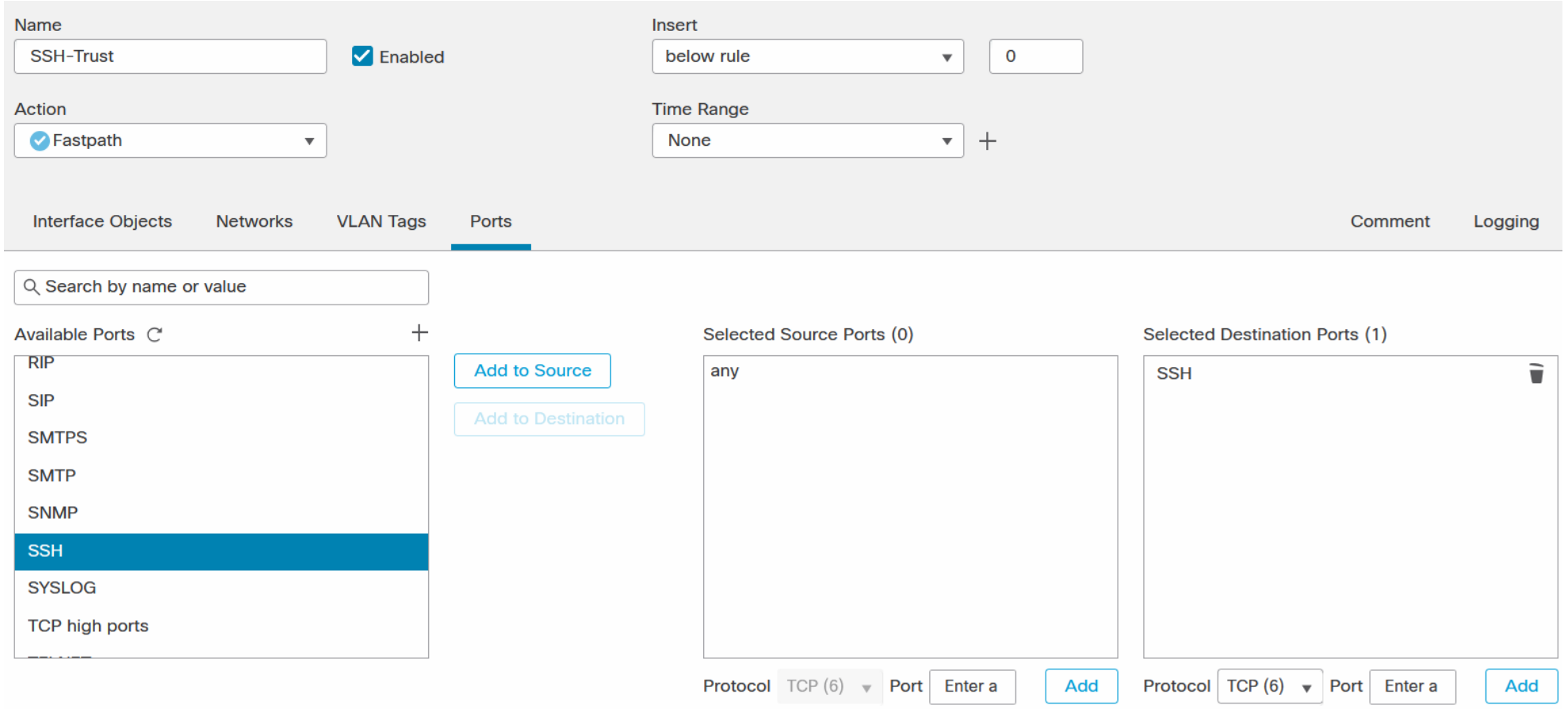
- An access control rule with the Trust action allows a threat defense to bypass deep packet inspection
- Trusted traffic checks for identity and quality of service (QoS) requirements as configured in their respective policies
- Access control policy rules offer more filtering capability. i.e. you can filter traffic based on applications, URLs, users, ….

Prefilter Policy: Configuration

➢ In this example we need to allow management traffic pass via SSH and HTTPS (without deep inspection)

1) Add Prefilter Rule

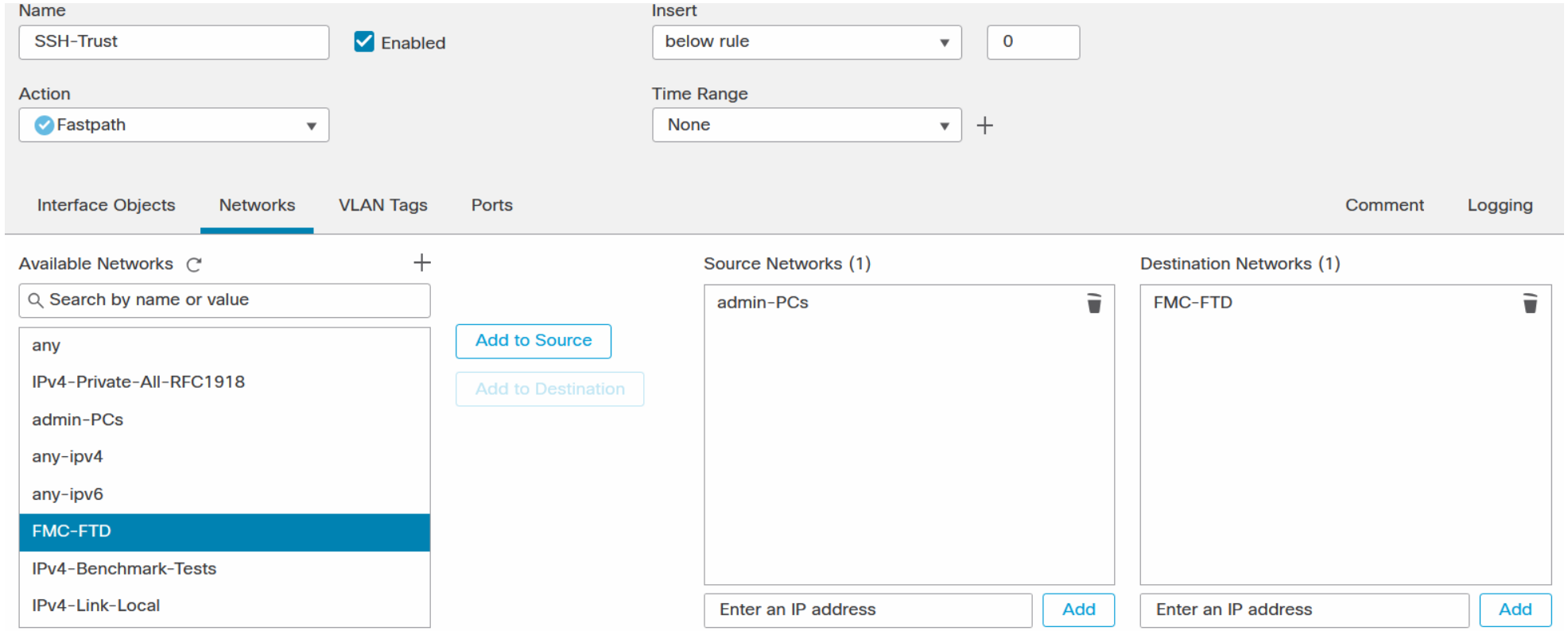
- Type a name for rule
- Action = Fastpath
- Destination port= SSH



✓ It means traffic destined to SSH port are trusted and not inspected

Prefilter Policy: Configuration

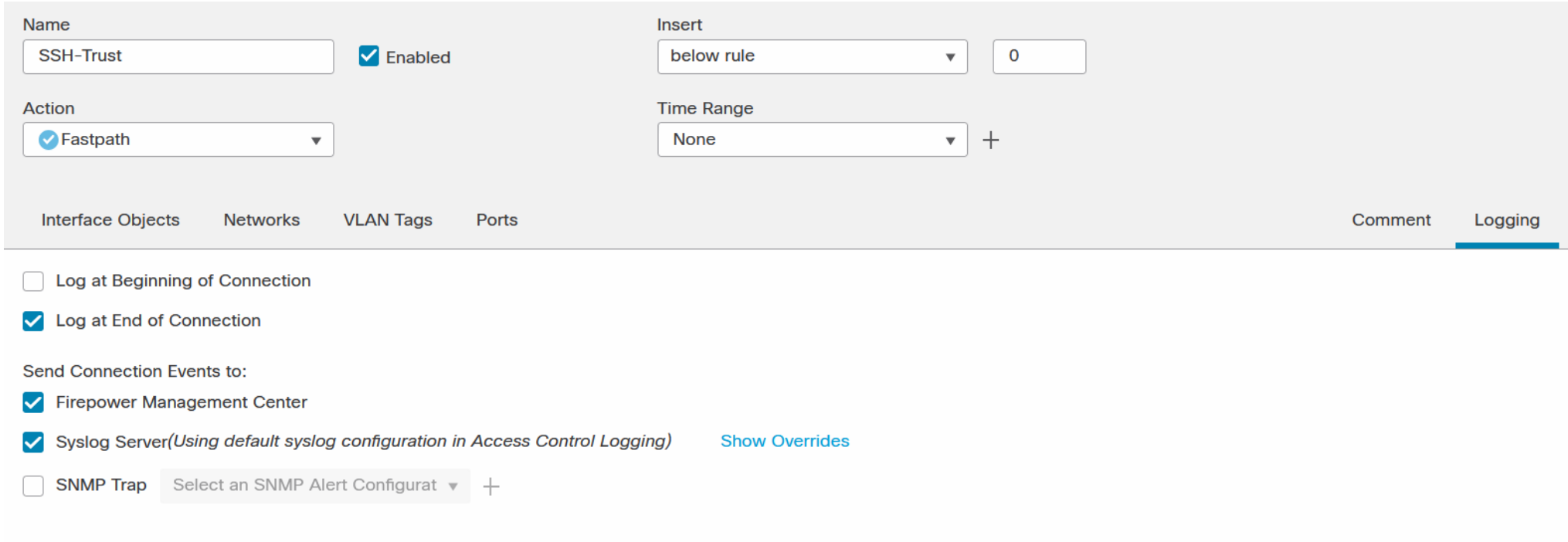
1) Add Prefilter Rule



- Optionally you can Select source and destination traffic and add to source/destination network

Prefilter Policy: Configuration

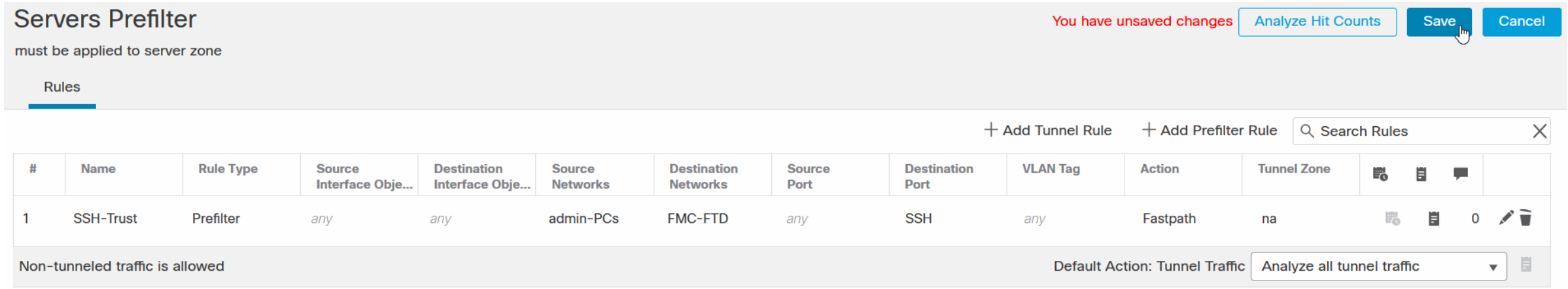
1) Add Prefilter Rule



- Optionally, enable logging to enable the FTD to send logs of matched traffic to FMC

Prefilter Policy: Configuration

Finally click Add



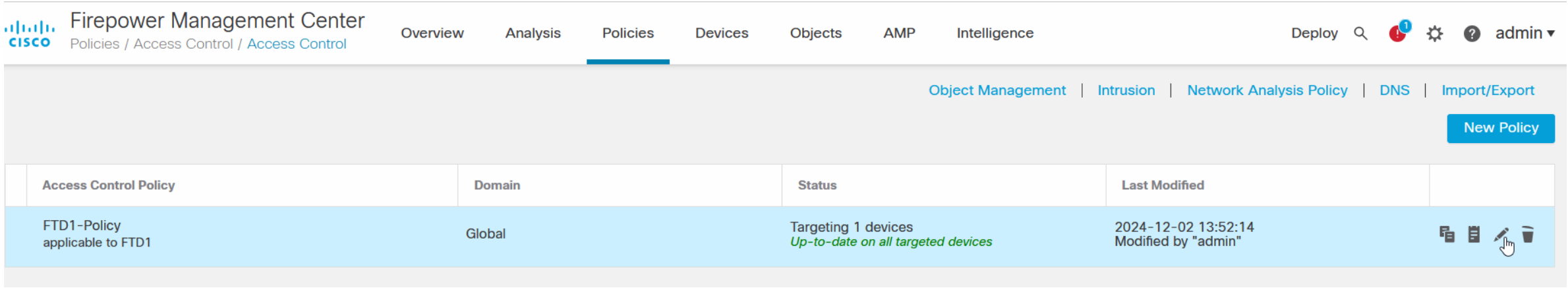
- Leave the Default Action Tunnel Traffic to Analyze all tunnel traffic
- Click save

- Note : Do not deploy a new prefilter policy at this stage.(next section , invoke this prefilter to access control policy)

Prefilter Policy: Configuration

2) Invoking a Prefilter Policy into an Access Control Policy

- Policies > Access Control > Access Control

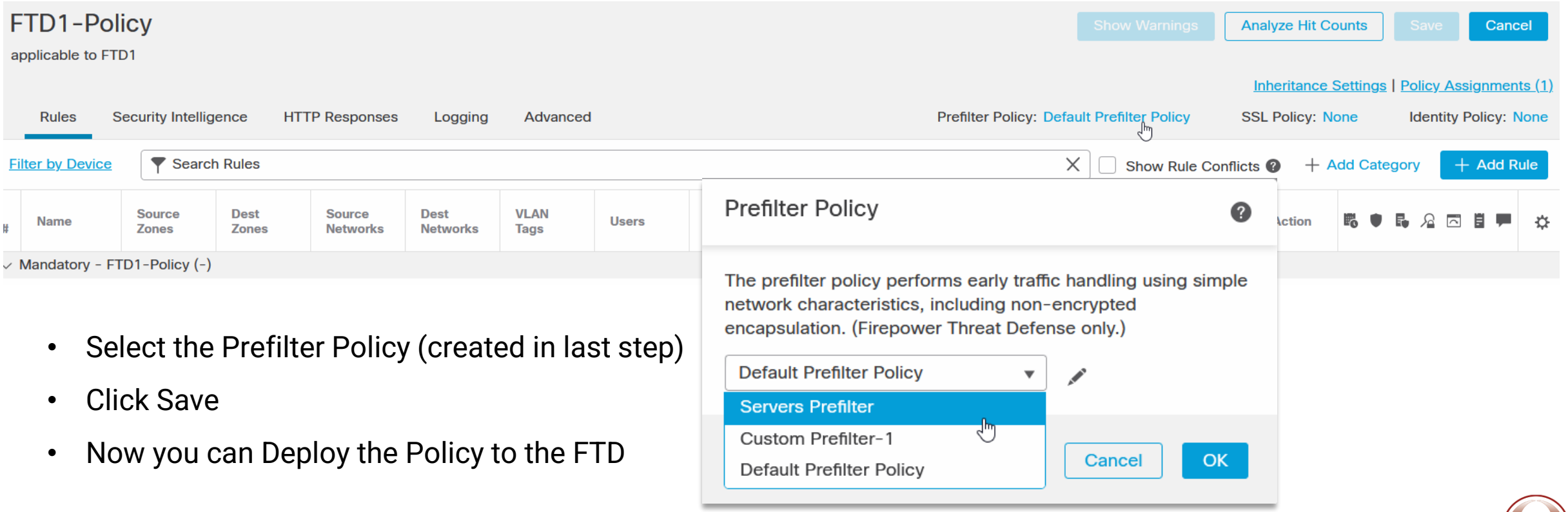


- Edit desired Access control policy

Prefilter Policy: Configuration

2) Invoking a Prefilter Policy into an Access Control Policy

- Click the Default Prefilter Policy to change it

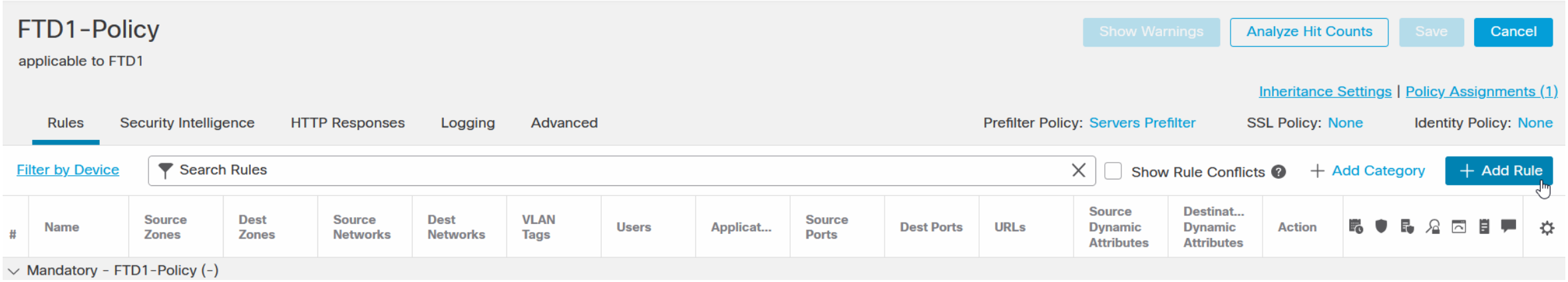


- Select the Prefilter Policy (created in last step)
- Click Save
- Now you can Deploy the Policy to the FTD

Trust Rule via Access Control Policy

- ✓ As I mentioned in the last step we want to allow HTTPS traffic to pass through as well , without deep inspection
- ✓ But other facilities like : Security Intelligence data, application fingerprints, URL filtering, user identities are needed

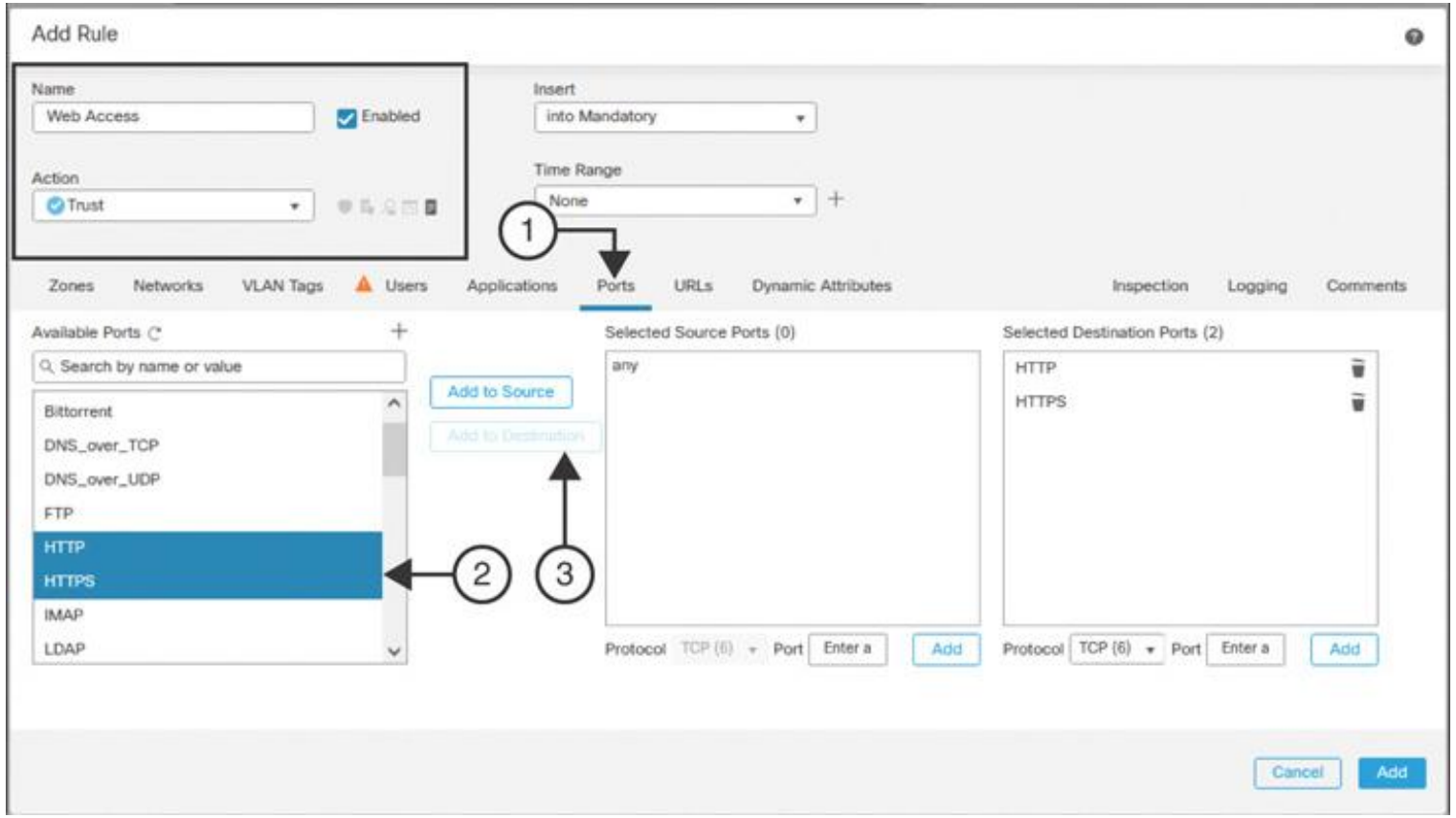
- Policies > Access Control > Access Control.



- Click Add Rule

Trust Rule via Access Control Policy

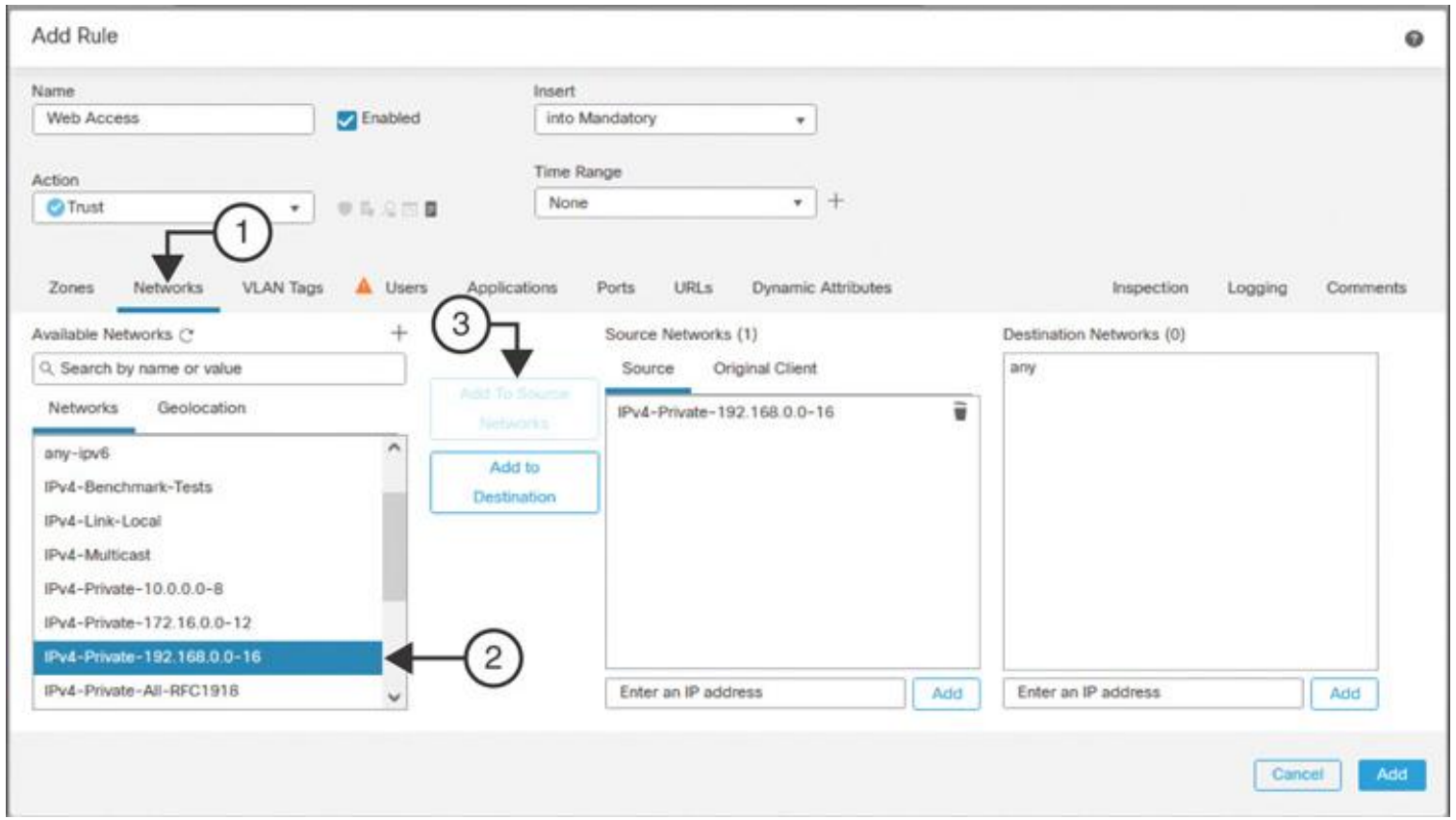
- Enter a name for Rule
- Action = trust
- Select HTTP/HTTPS ports
- Add selected ports to destination ports



Trust Rule via Access Control Policy

You can also :

- Select the source traffic and Add to source network



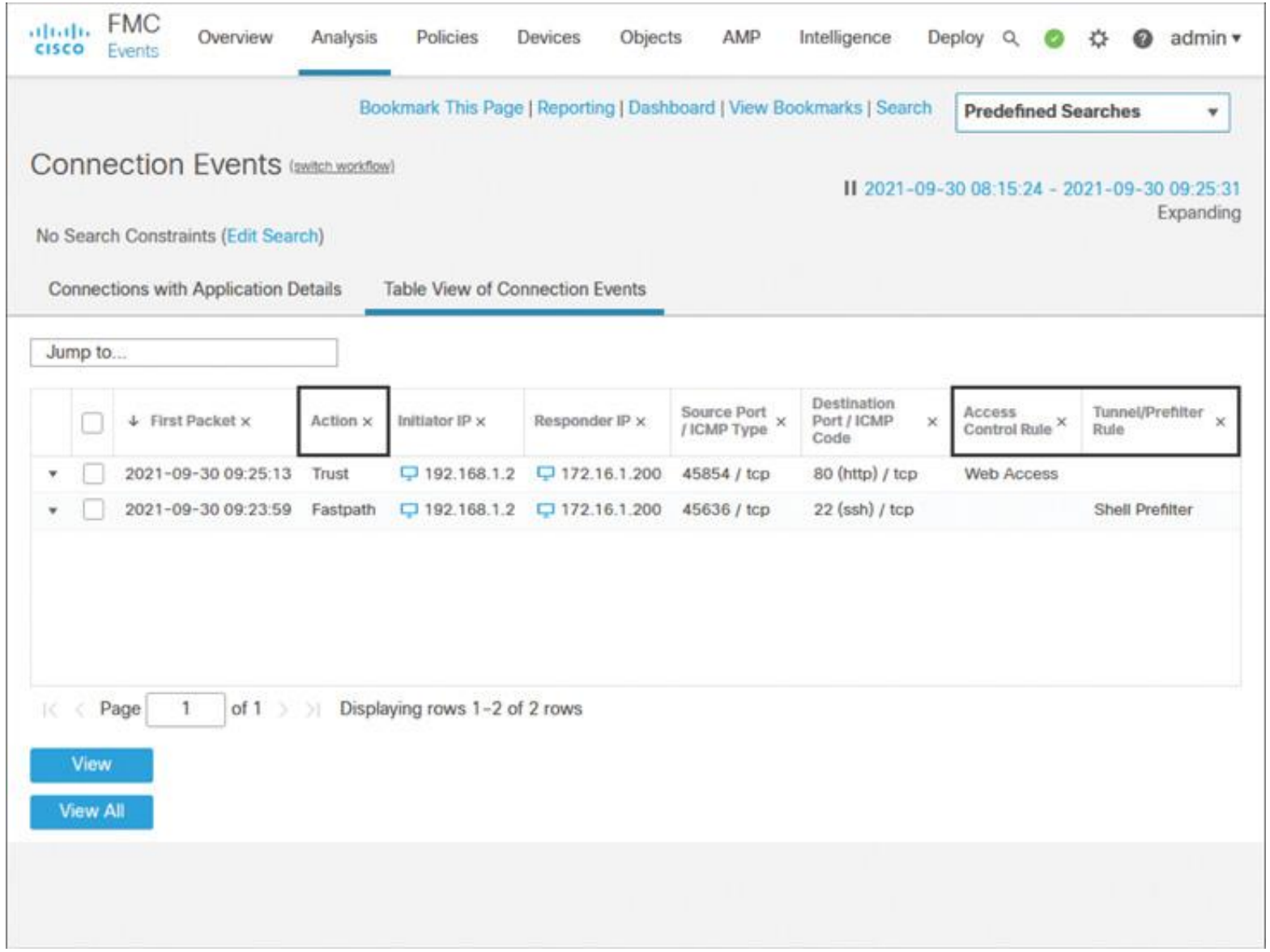
Finally :

- Add
- Click Save
- And Deploy the policy to FTD

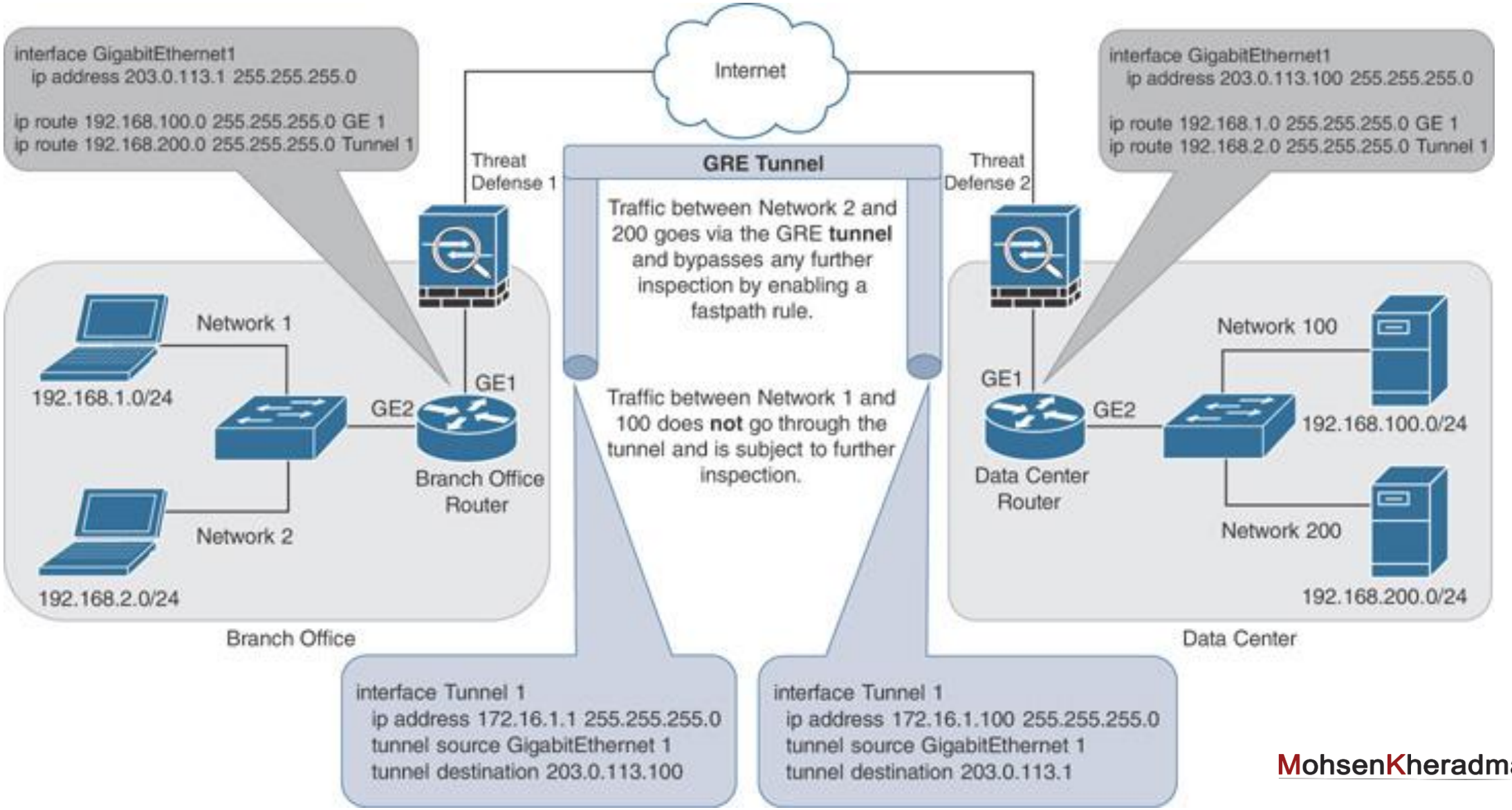
Verification

Verify the actions of prefilter and access control rules on live traffic

Analysis > Connections > Events

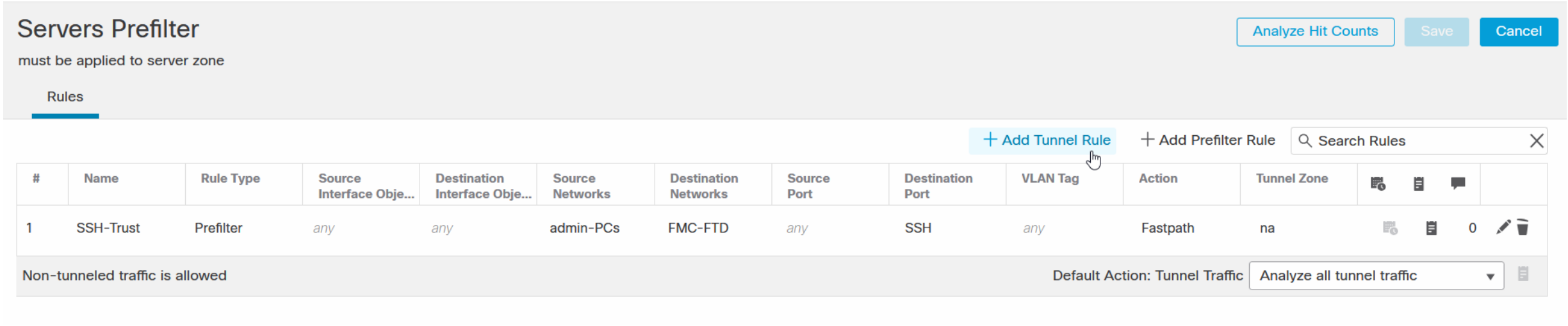


Managing Encapsulated Traffic inspection



Managing Encapsulated Traffic inspection

Click Prefilter policy > edit



Click Add Tunnel Rule

Managing Encapsulated Traffic inspection