Securing Networks with

Cisco FTD

Chapter 13

Network Analysis and Intrusion Policies

Mohsen Kheradmand

Cisco Firepower IPS Rules Fundamental

- 2 main methods that IPS detects intrusions

Signature based detection

- Detects based on signature of all knows attacks and intrusions are already encoded in the signatures
- Can not detect Zero-Day attack

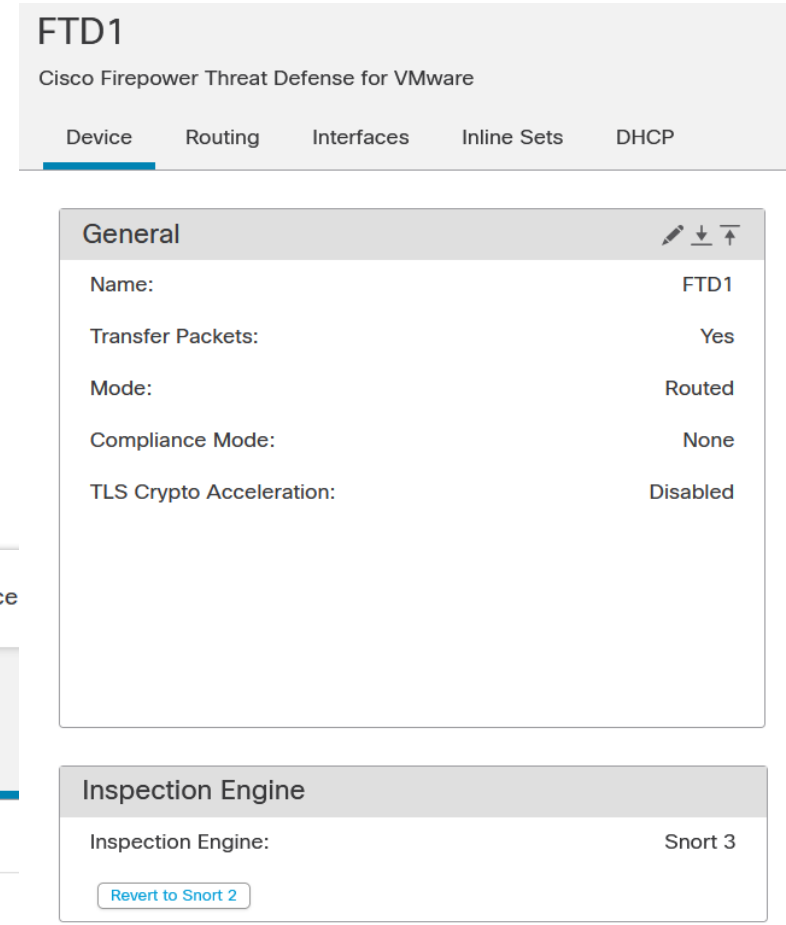
Anomaly based detection

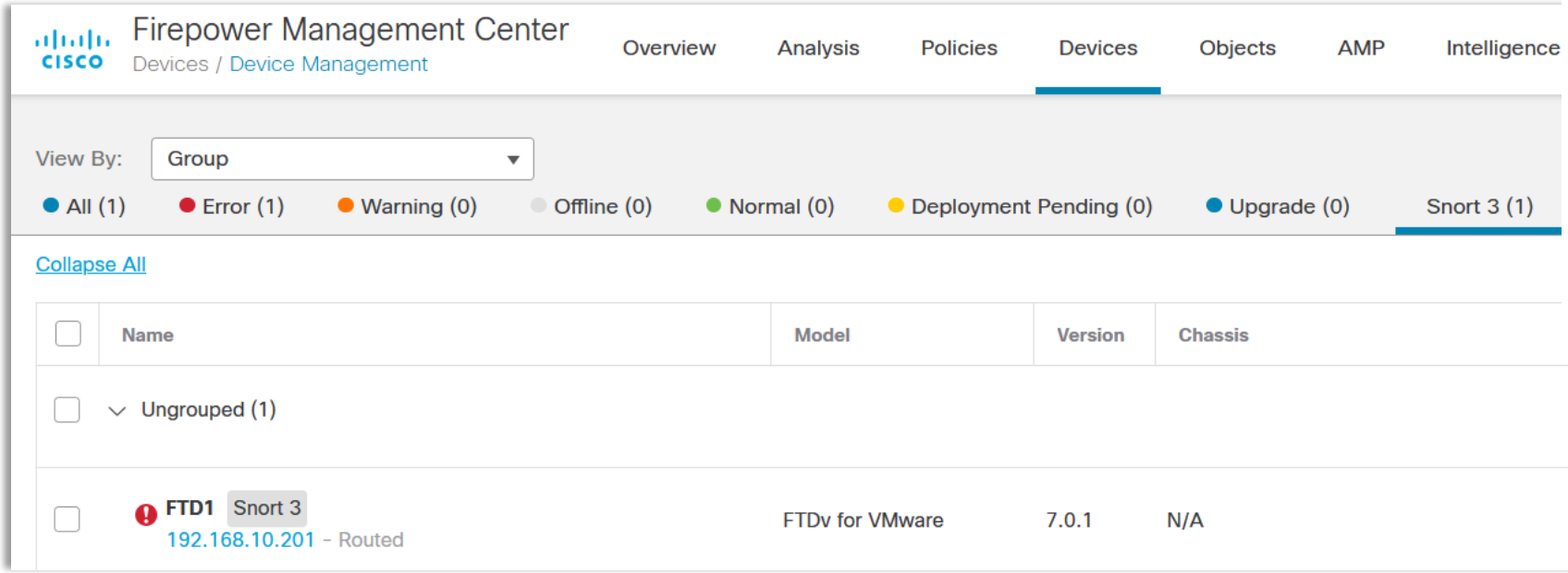
- In this method, Firepower is always learning and updating normal traffic pattern.
- Any traffic violating normal profiled pattern is assumed to be anomaly
- Can detect zero-based attack but has mostly false positive. (normal traffic incorrectly labeled as intrusion traffic)

Cisco Firepower IPS Rules Fundamental

Cisco Firepower IPS and Snort

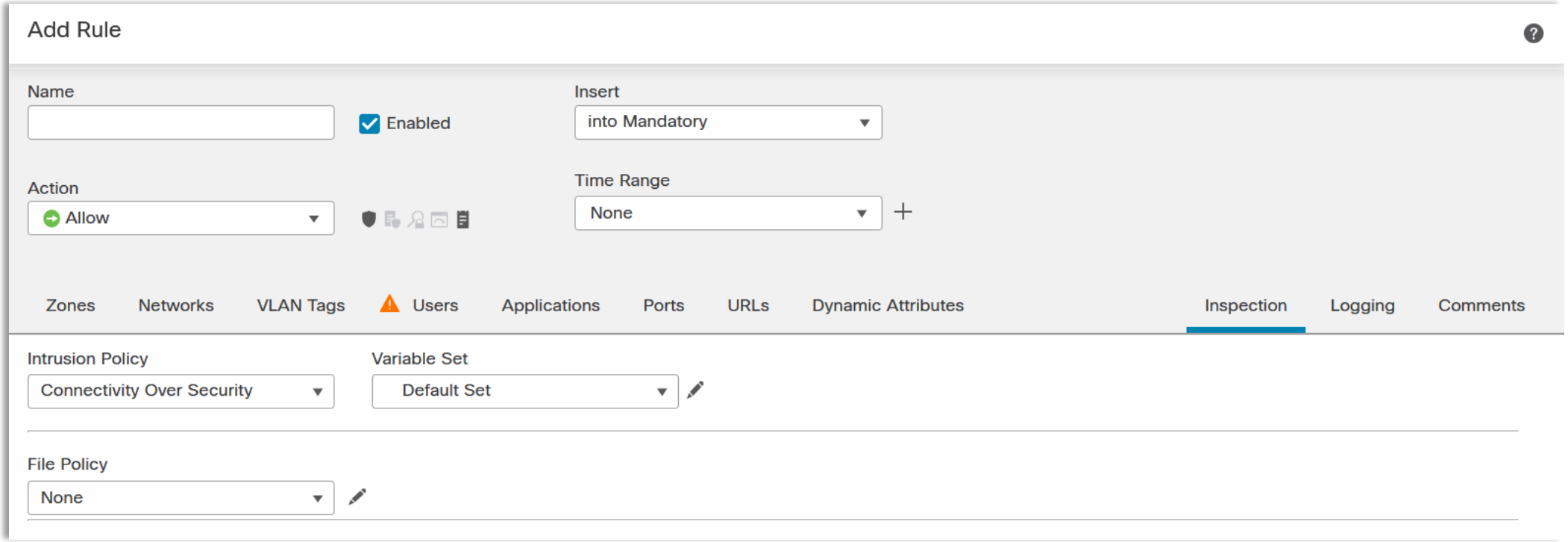
- Cisco Firepower IPS rules are based on open source Snort IDS software
- Before Firepower version 6.7, Snort version 2 and after Firepower version 6.7, Snort version 3 is used
- Snort Version 2 and Snort Version 3 are not compatible.
- There is a snort convertor feature in new firepower versions to change snort rules from version 2 to version 3.





Snort

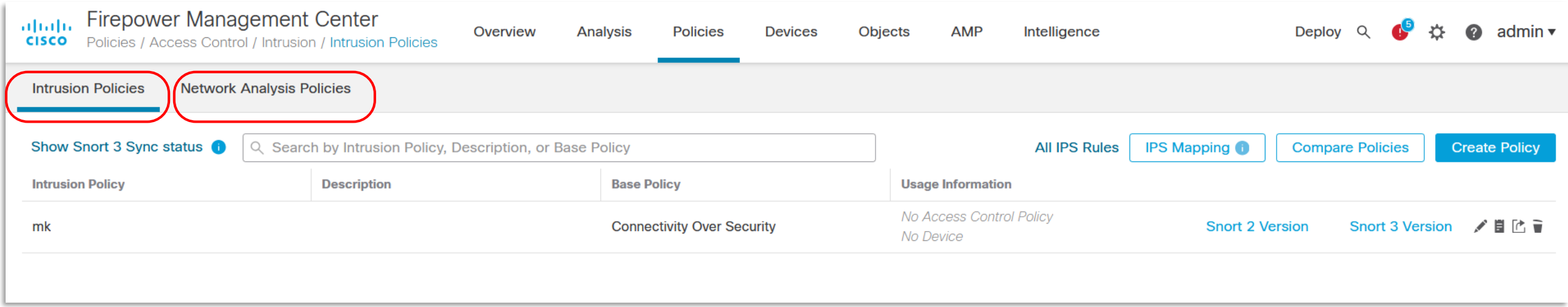
- The IDS/IPS is powered by Snort
- Snort rules sniff network packets, detect malicious activities, generate alerts for users, or block any harmful packets
- A Snort rule is also known as an intrusion rule
- Intrusion rule has two policies: an intrusion policy and a network analysis policy



Simple Options to Select the Built-in Intrusion Policy

Snort policy components

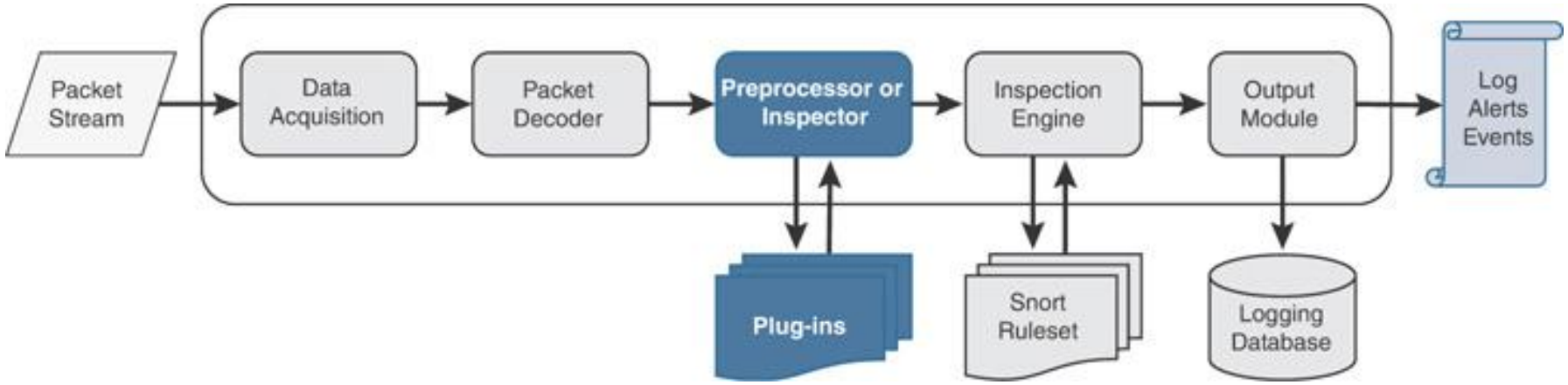
- **Network analysis policy** : works with inspectors (in Snort 3) and preprocessors (in Snort 2) to normalize traffic.
- **Intrusion policy** : performs deep packet inspection.



- **Access control policy** : filters specific network traffic and applies the network analysis and intrusion policies to it

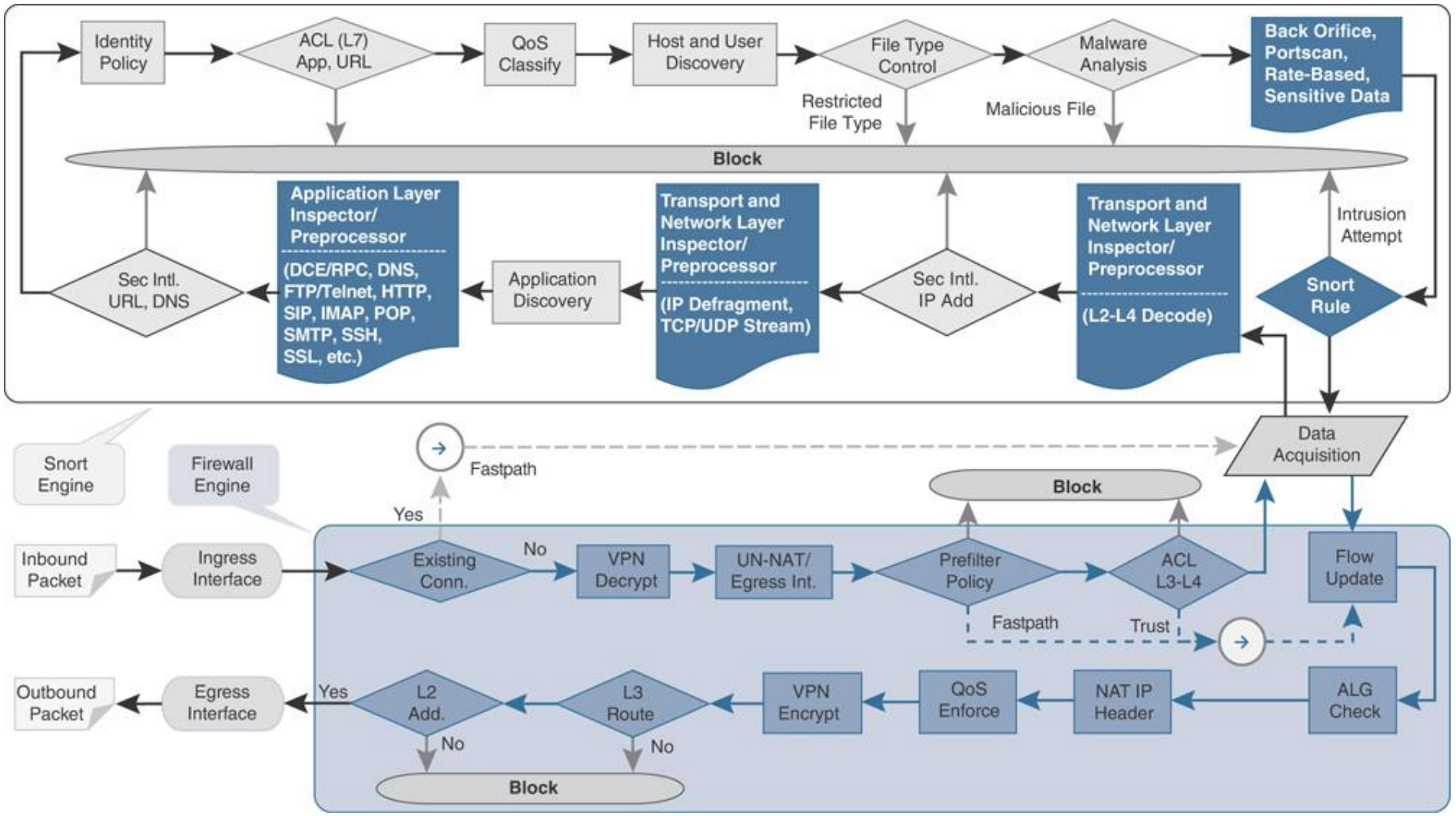
Network Analysis Policy

- Before deep packet inspection, the Snort engine decodes a packet into a standard format that a Snort rule can analyze easily
- This component is called a **preprocessor** (in Snort 2) or an **inspector** (in Snort 3)
- The Snort engine uses them in multiple phases to decode and normalize traffic
- Snort has many protocol-specific preprocessors or inspectors
- They can identify anomalies of packets, detect evasion techniques, or drop inconsistent packets



- Network Analysis Policy occurs after Security Intelligence and SSL decryption, but before access control or intrusion policy

Network Analysis Policy



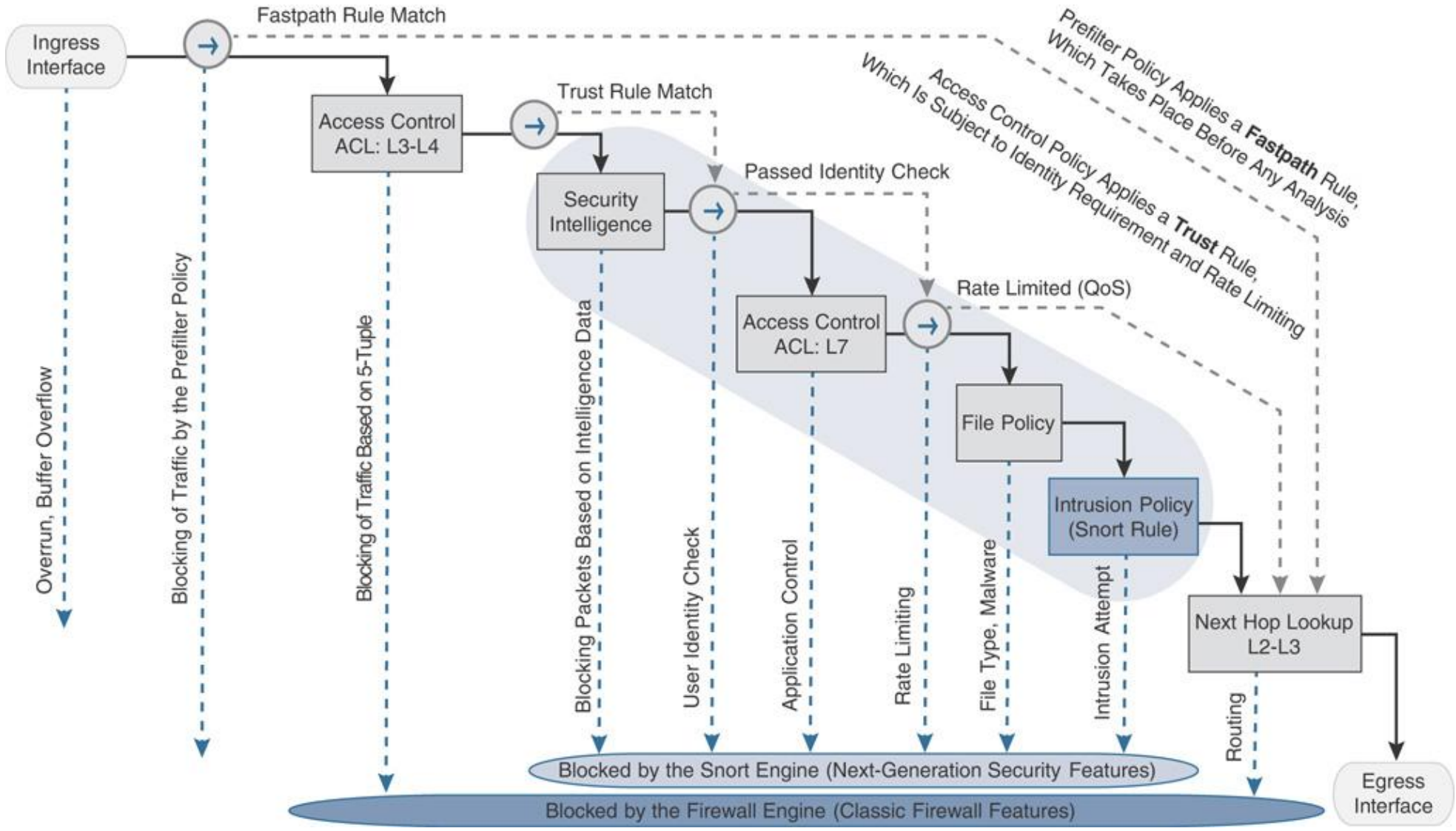
Network Analysis Policy Components Acting in Multiple Phases

MohsenKheradmand MK

Intrusion Policy

- An intrusion policy allows you to enable, disable, or set a rule state for matching traffic
- After decoding and normalizing a packet, the threat defense uses the intrusion rules to perform deep packet inspection
- An intrusion rule is written based on Snort rule syntax and contains the signature of a specific vulnerability
- Secure Firewall supports Snort rules from various sources :
  - Standard text rules:
    - Written by The Cisco Talos in cleartext format. The Snort detection engine uses them to analyze packets.
  - Shared object (SO) rules:
    - Written by The Cisco Talos in the C programming language
  - Preprocessor rules:
    - Created by The Snort development team (use to control alerts that come from the preprocessors)
  - Local rules:
    - Custom Snort rules (using the built-in rule editor or by importing rules written in a plaintext file)
    - If you obtain Snort rules from a third party, the system considers them to be local rules as well.

Intrusion Policy



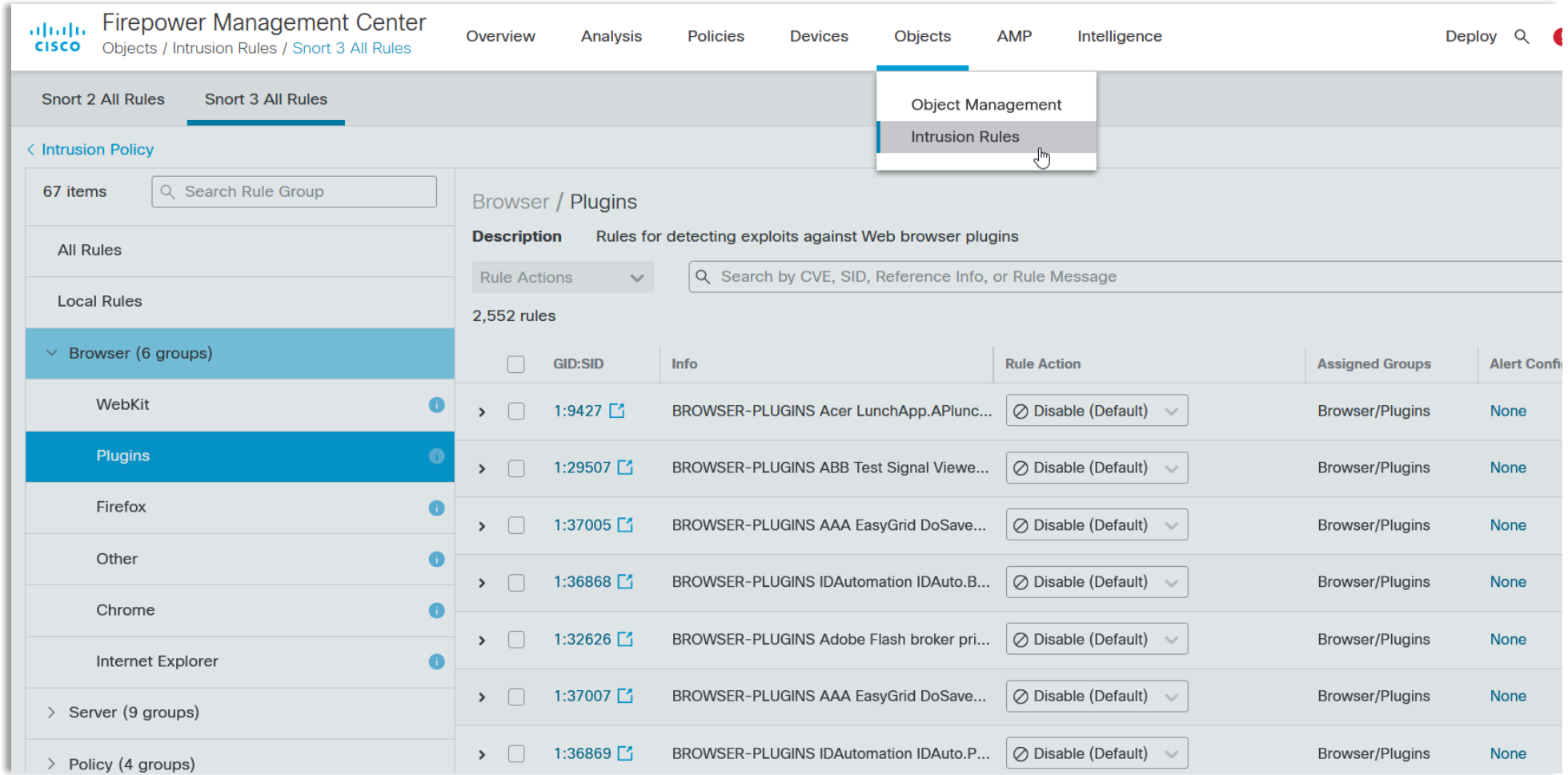
Intrusion Policy

Snort uses a unique generator ID (GID) and Snort rule ID (SID) to identify a rule

Type of Rule	Identification Number
Standard text rule	GID is 1 SID is lower than 1,000,000.
Shared object rule	GID is 3
Preprocessor rule	GID can be anything other than 1–3.
Local rule	SID is 1,000,000 or higher.

Intrusion Policy

- In **Objects > Intrusion Rules** , you can check all Firepower IPS rules (Snort version 2 or version 3 format)



Intrusion Policy

- System-Provided Variable Sets
  - A Snort rule supports variables to represent the source and destination IP addresses and port numbers
  - It helps to deploy Snort rules in any network without modifying the original rule
  - Secure Firewall comes with many default variables.
  - The purposes of the system-provided variables are apparent in their names.
    - For instance:

      $HOME_NET, $EXTERNAL_NET:
      - $HOME_NET includes the internal network resources that you need to protect.
      - $EXTERNAL_NET specifies the external network that you are not responsible to protect

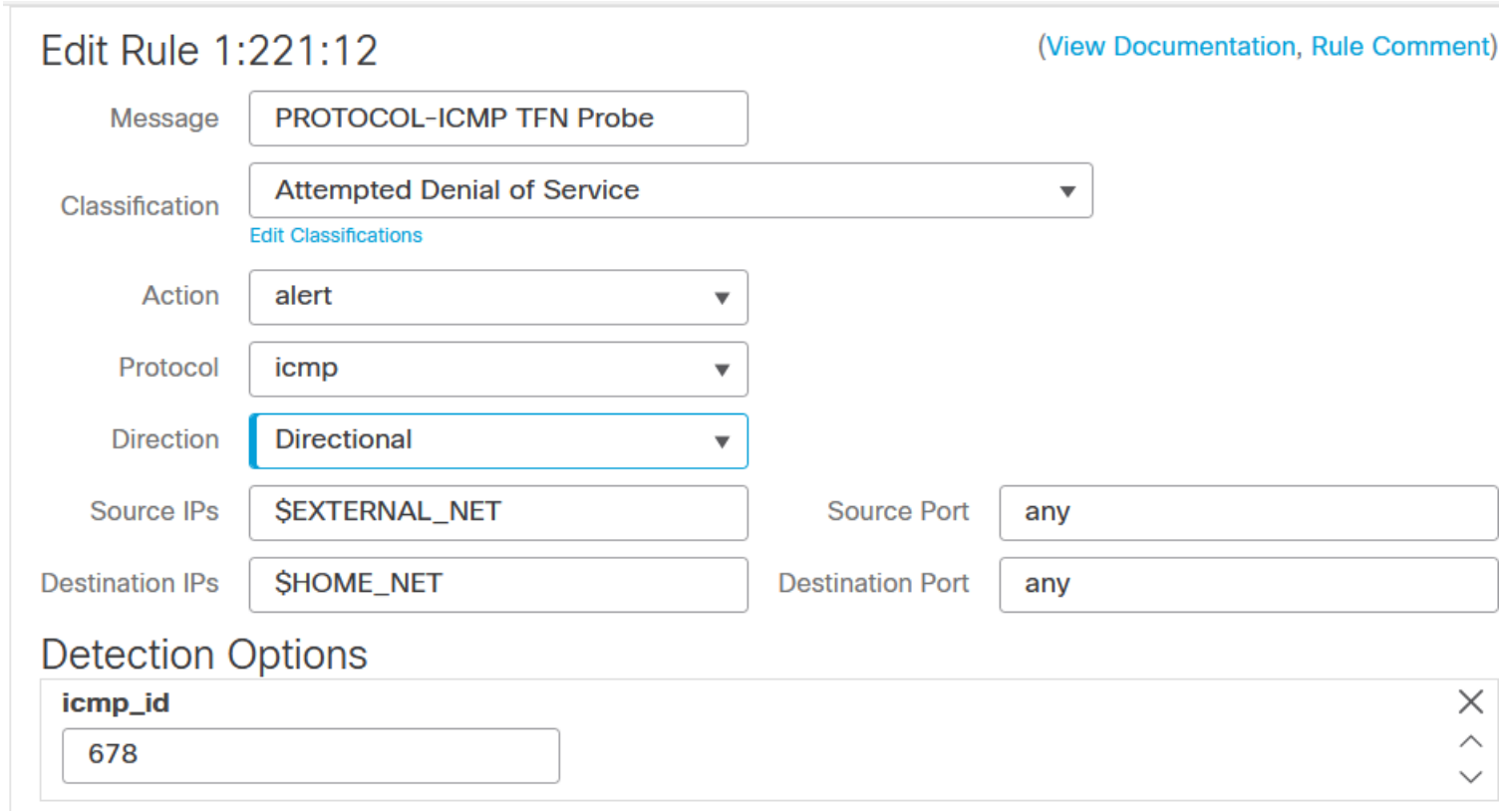
      $HTTP_SERVERS, $DNS_SERVERS:
      - These names are used to define the static IP addresses of the web servers and domain name servers.

      $FTP_PORTS, $HTTP_PORTS:
      - These names are used to define the port numbers of the FTP servers and web servers

Intrusion Policy

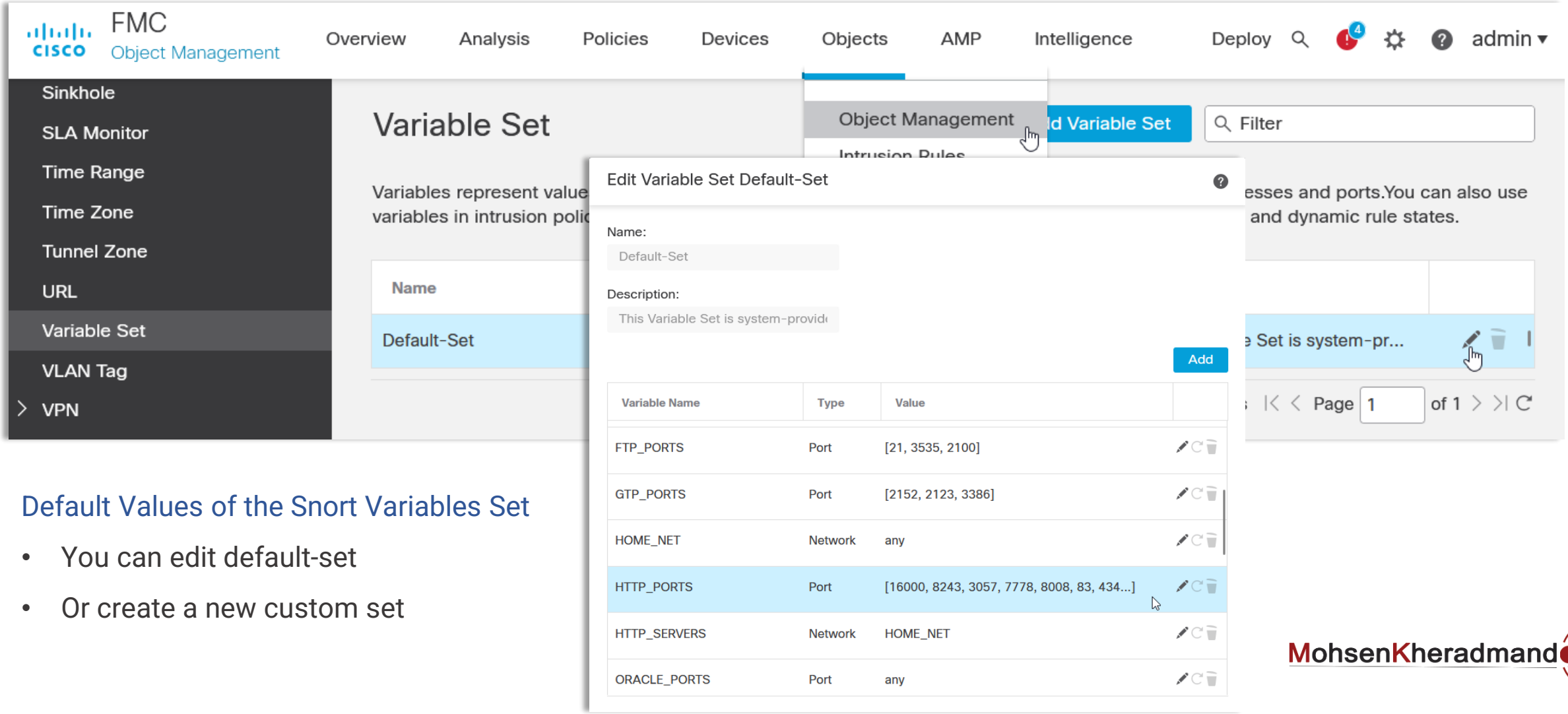
- System-Provided Variable Sets

Example :



Intrusion Policy

- System-Provided Variable Sets



Default Values of the Snort Variables Set

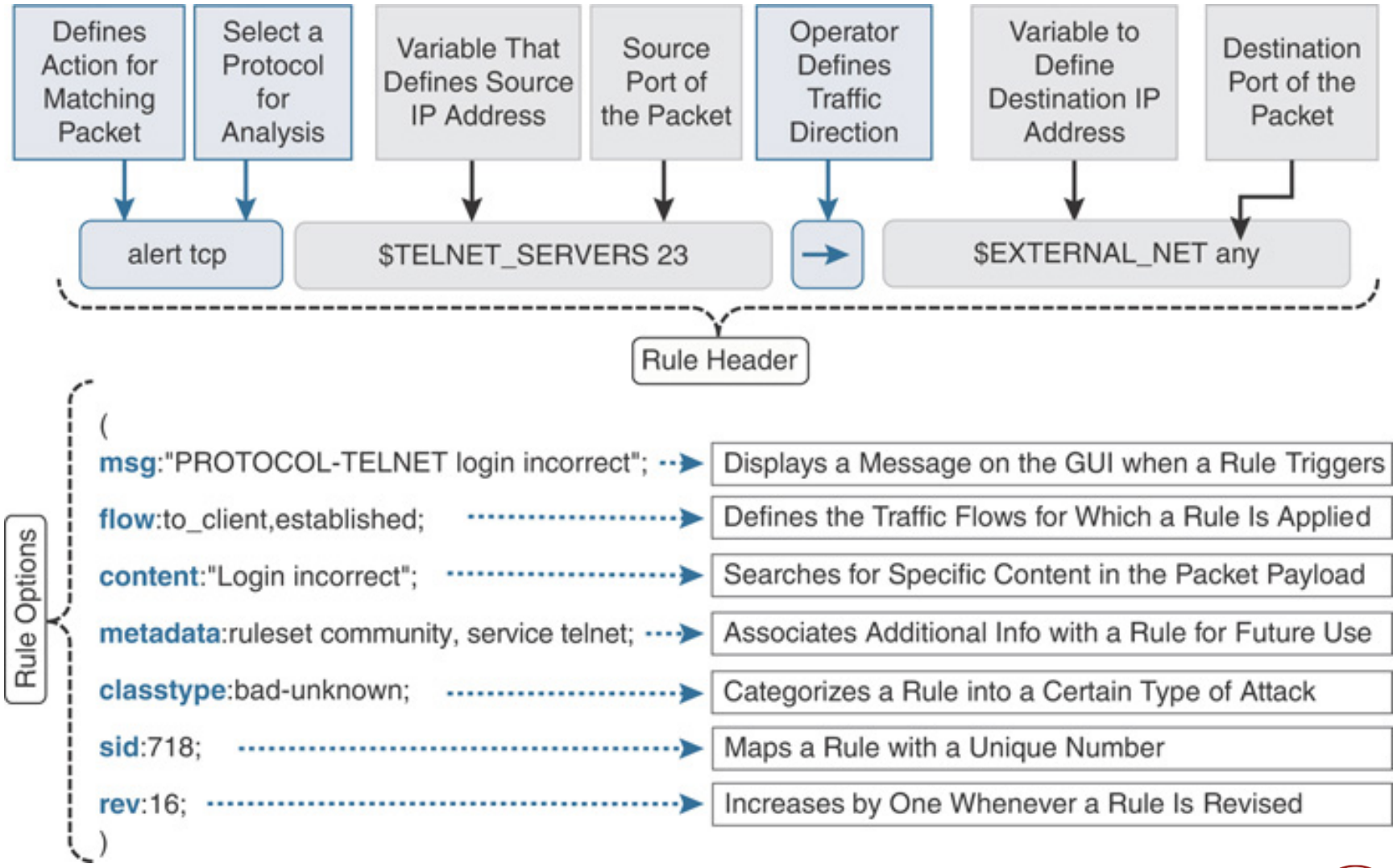
- You can edit default-set
- Or create a new custom set

MohsenKheradmand MK

Intrusion Policy

- System-Provided Variable Sets

Sample :
Snort rule 1:718 , demonstrate the operation of an intrusion policy



Intrusion Policy

- System-Provided Base Policies

Secure Firewall software comes with several preconfigured network analysis and intrusion policies.

You can deploy one of them directly, or use one as a baseline for your custom intrusion policy:

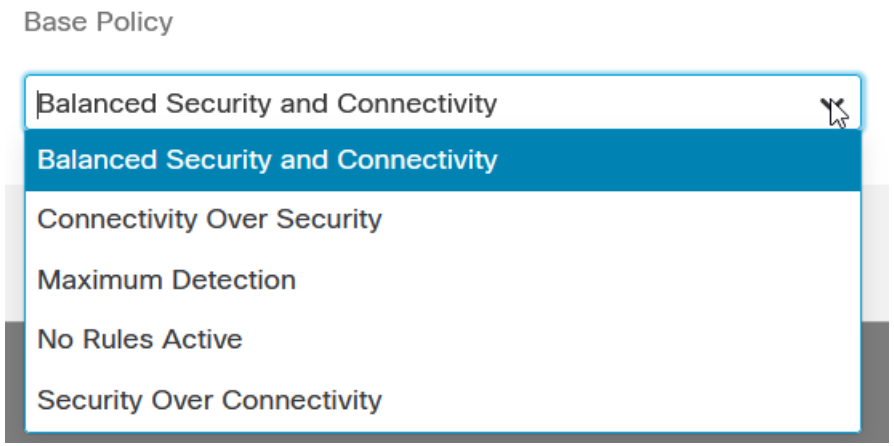
- **Balanced Security and Connectivity:**
  - This policy address the critical vulnerabilities while maintaining system performance
- **Connectivity over Security:**
  - This policy Prioritizes connection speed by reducing the detection of older or less critical vulnerabilities.
- **Security over Connectivity**:
  - Prioritizes network security over connectivity by more rules to drop offending traffic over the other default policies.
- **Maximum Detection**:
  - In this policy , Security has supreme priority over business continuity.
  - Users may experience latency, and a threat defense may drop some legitimate traffic.
- **No Rules Active**
  - Create an empty intrusion policy with all the intrusion rules disabled

Intrusion Policy

- System-Provided Base Policies

Cisco uses the Common Vulnerability Scoring System (CVSS) score to determine whether a rule should be enabled in a system-provided policy

Intrusion Policy	CVSS Score	Age of Vulnerability
Connectivity over Security	10	Current year plus two prior years
Balanced Security and Connectivity	9 or higher	Current year plus two prior years
Security over Connectivity	8 or higher	Current year plus three prior years
Maximum Detection	7/5 or higher	All the years since 2005



Intrusion Policy

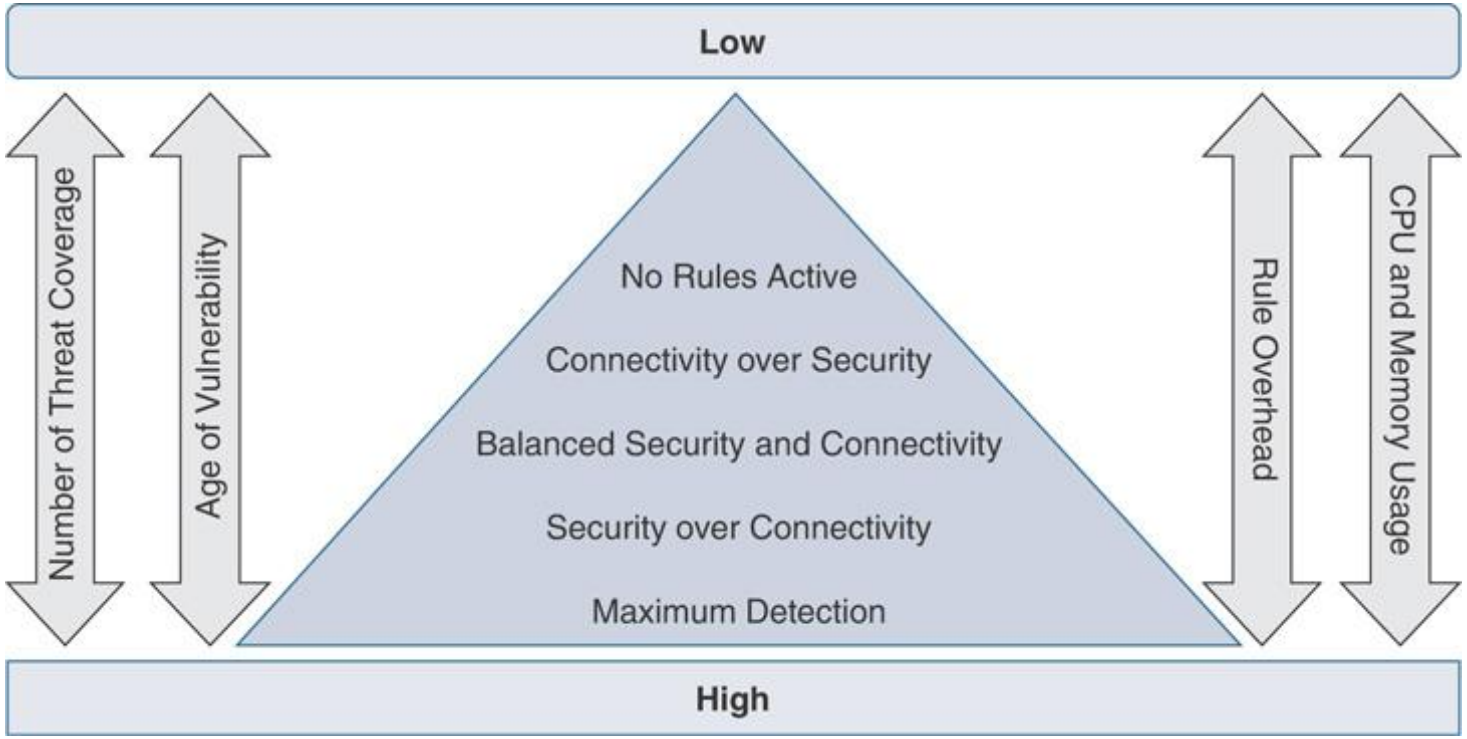
- System-Provided Base Policies

  - Cisco releases rule updates periodically
  - Latest ruleset can be downloaded automatically from the cloud and install it by a scheduled task in FMC
  - You can also manually download a rule update file and upload it to the FMC for installation
  - Each rule update comes with a unique ruleset
  - The *Maximum Detection policy* and *Security over Connectivity policy* have more intrusion rules than the others

Intrusion Policy

- System-Provided Base Policies

Differences Between the System-Provided Policies , Coverages, and Processing Overheads

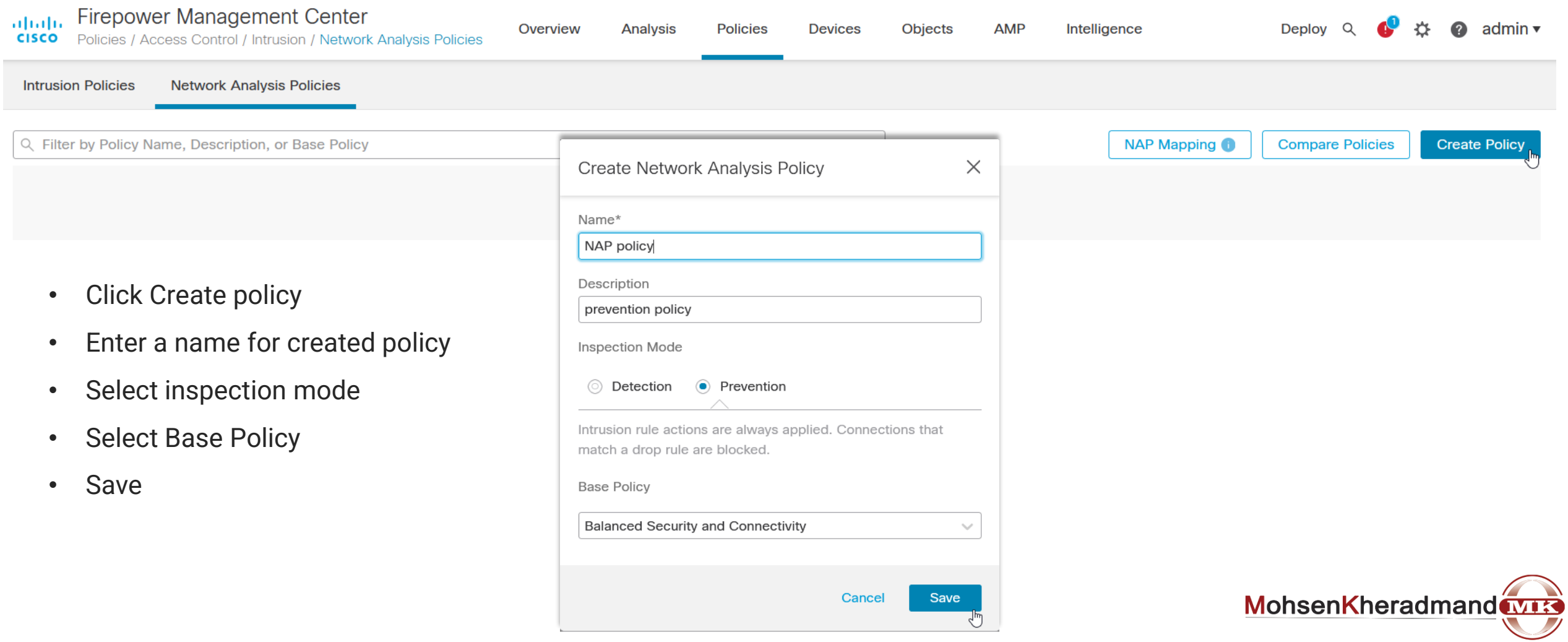


Tips:

- Cisco releases rule updates periodically
- Latest ruleset can be downloaded automatically from the cloud and install it by a scheduled task in FMC
- You can also manually download a rule update file and upload it to the FMC for installation
- Each rule update comes with a unique ruleset
- The *Maximum Detection policy* and *Security over Connectivity policy* have more intrusion rules than the others

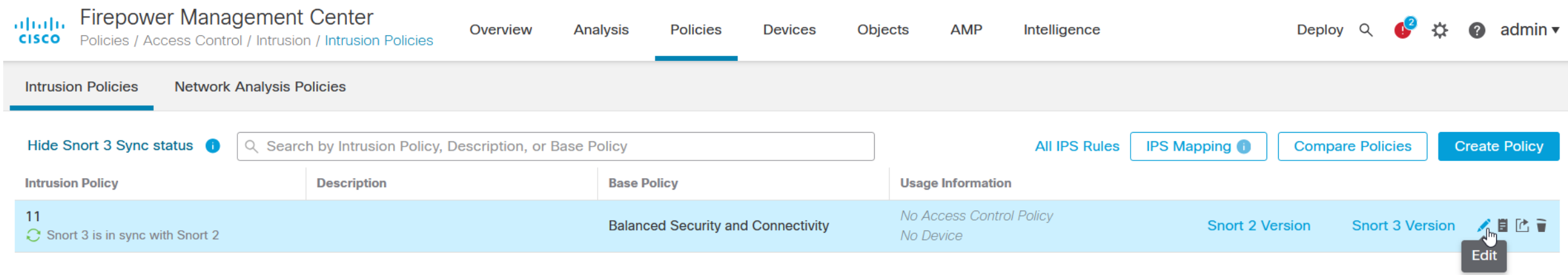
Configuring a Network Analysis Policy

- Policies > Access Control > Intrusion >> Network Analysis Policies tab



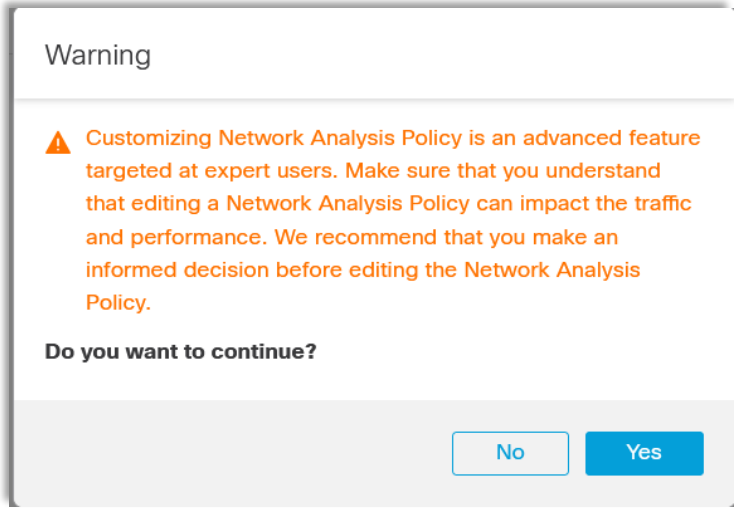
- Click Create policy
- Enter a name for created policy
- Select inspection mode
- Select Base Policy
- Save

Configuring a Network Analysis Policy



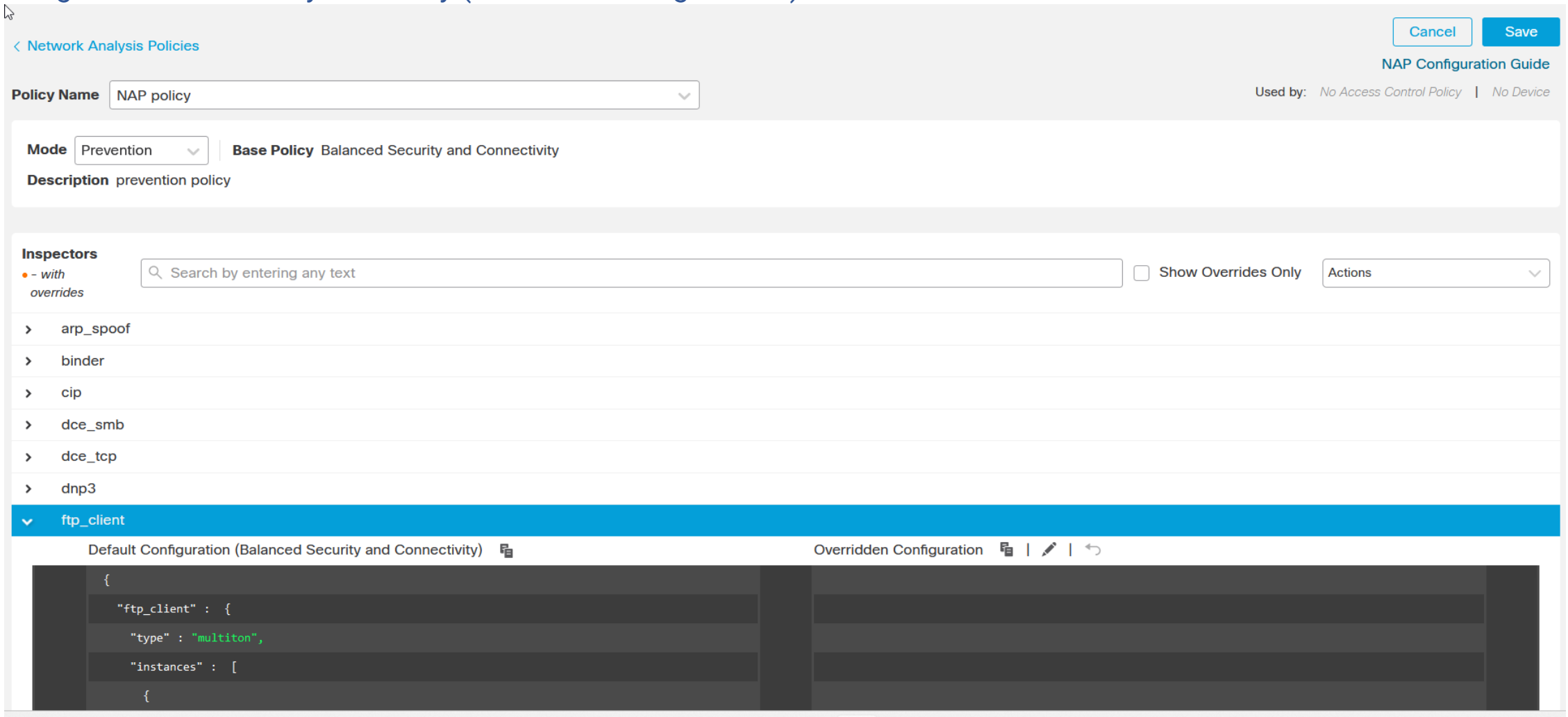
You can edit policy rules but :

- A network analysis policy is an advanced feature
- Misconfiguration of policy can impact the traffic flow and system performance
- Only expert users should modify its settings when necessary
- When you click Edit , a warning message will be shown



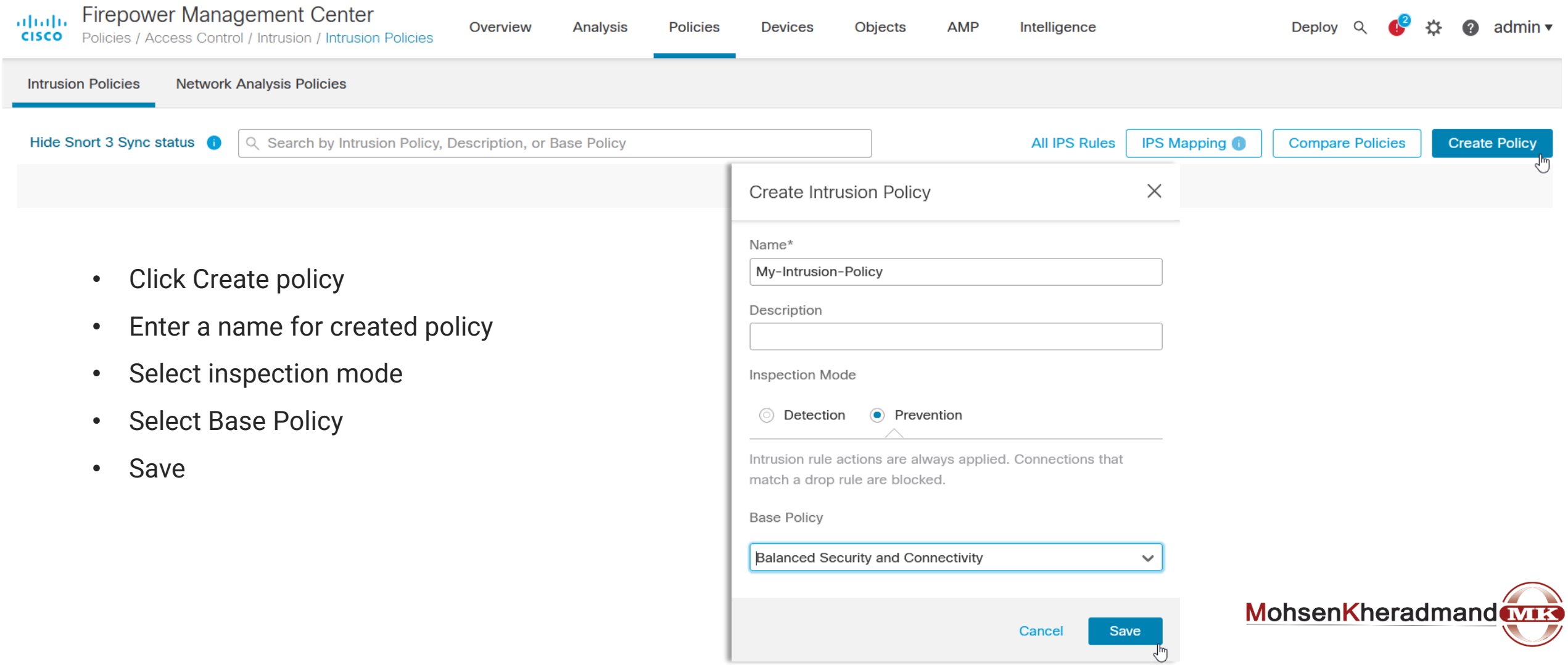
Configuring a Network Analysis Policy

Editing the Network Analyses Policy (advanced configuration)



Configuring an Intrusion Policy

- Policies > Access Control > Intrusion >> Intrusion Policies tab



- Click Create policy
- Enter a name for created policy
- Select inspection mode
- Select Base Policy
- Save

Configuring an Intrusion Policy

➢ Intrusion Rule Recommendations

- Intrusion rule recommendations enables you to optimize the ruleset in your intrusion policy

  By this feature :

  >The FTD analyzes your network discovery data

  >> Correlates them with any associated vulnerabilities in the Vulnerability Database

  >>> and recommends intrusion rules that are relevant only to your network environment

- You should use intrusion rule recommendations after the majority of the hosts in your network are discovered
- The intrusion rule recommendations feature is disabled, by default

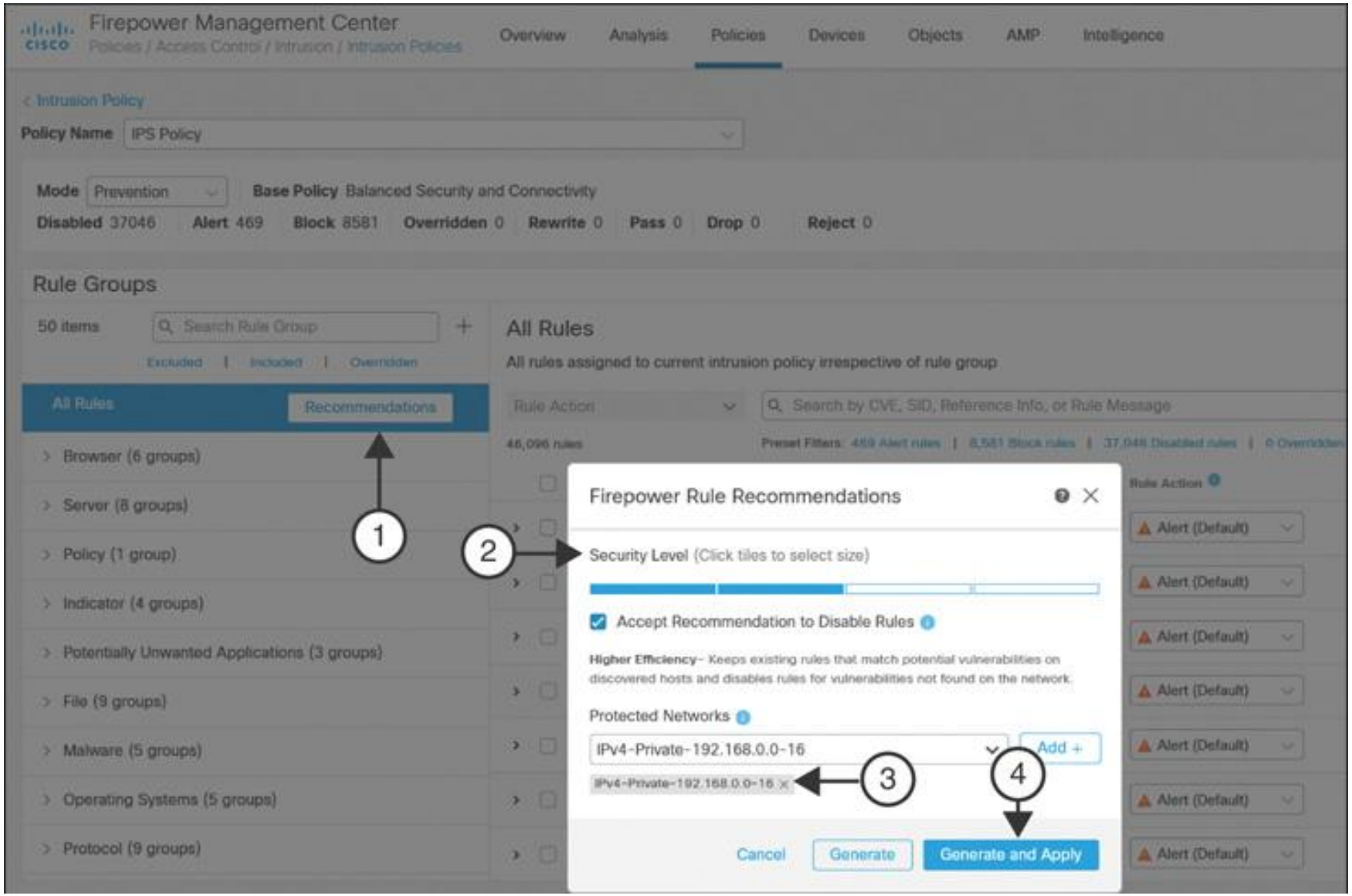
Configuring an Intrusion Policy

- Intrusion Rule Recommendations

Rule Recommendations Setup

Based on the Snort **3** Editor

1) Click recommendation
2) Select Security Level
3) Add desired Protected network
4) Click Generate and Apply



! Snort 3 recommendation was introduced in software version 7.1.

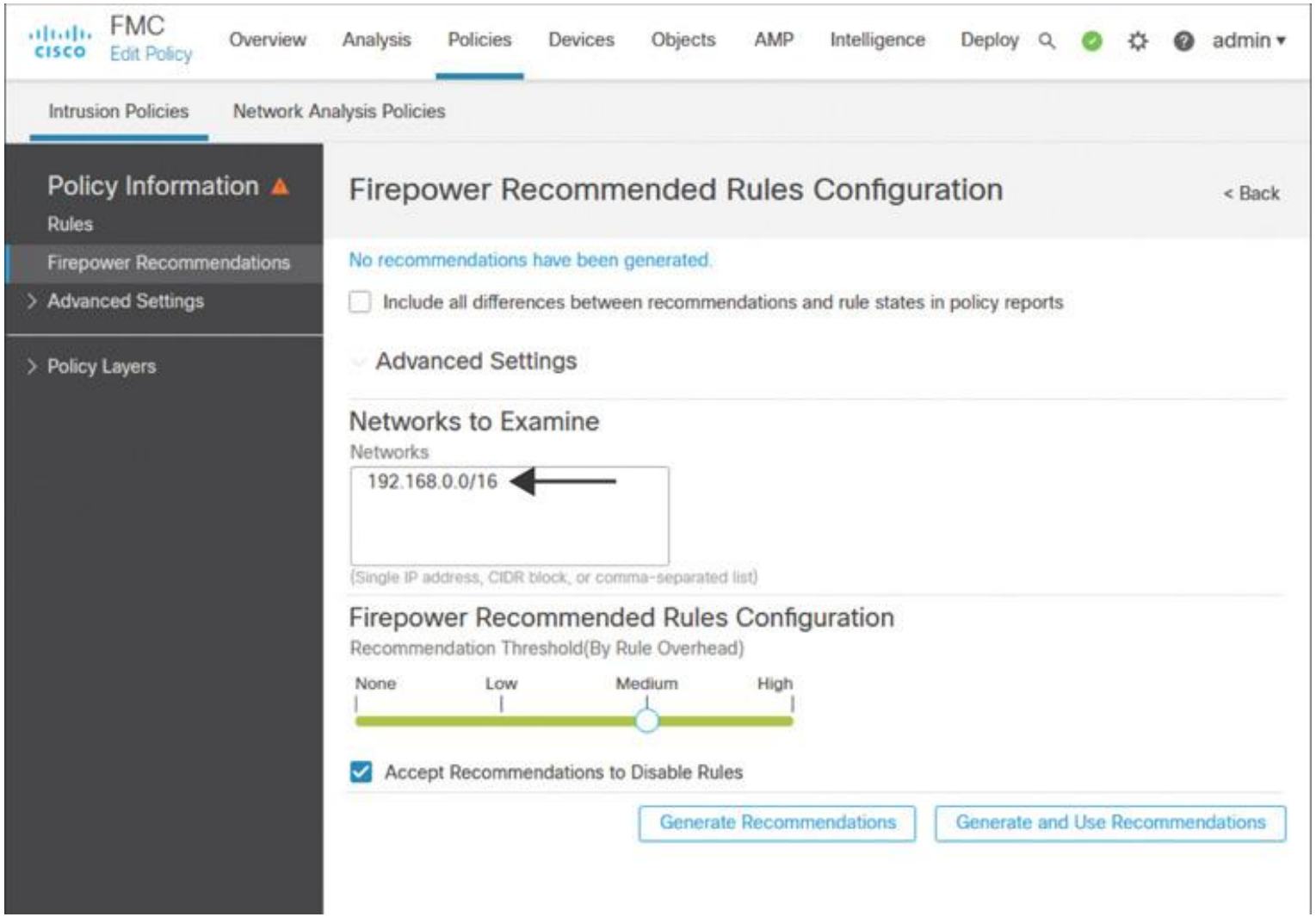
Configuring an Intrusion Policy

➢ Intrusion Rule Recommendations

Rule Recommendations Setup

Based on the Snort **2** Editor

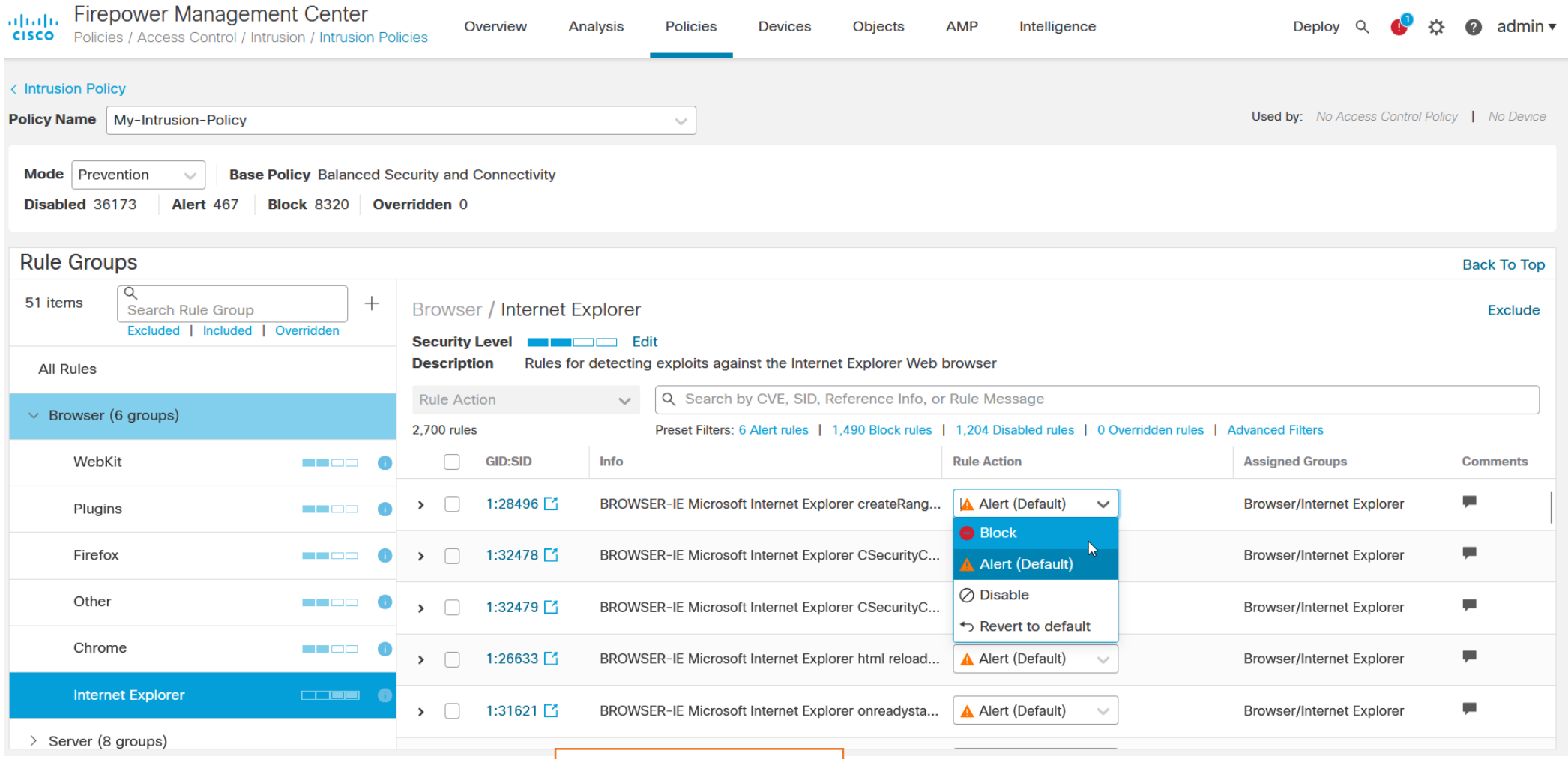
1) Click Snort 2 rule editor
2) Click Firepower Recommendation
3) Enter the network that you want to protect with the intrusion policy
4) Select Recommendation threshold
5) Click Generate or Generate and Use
6) go to the Policy Information page
7) save the changes by clicking the Commit Changes



Note : Higher Threshold = higher processing overhead

Configuring an Intrusion Policy

➢ Enabling or Disabling an Intrusion Rule



Snort **3** editor

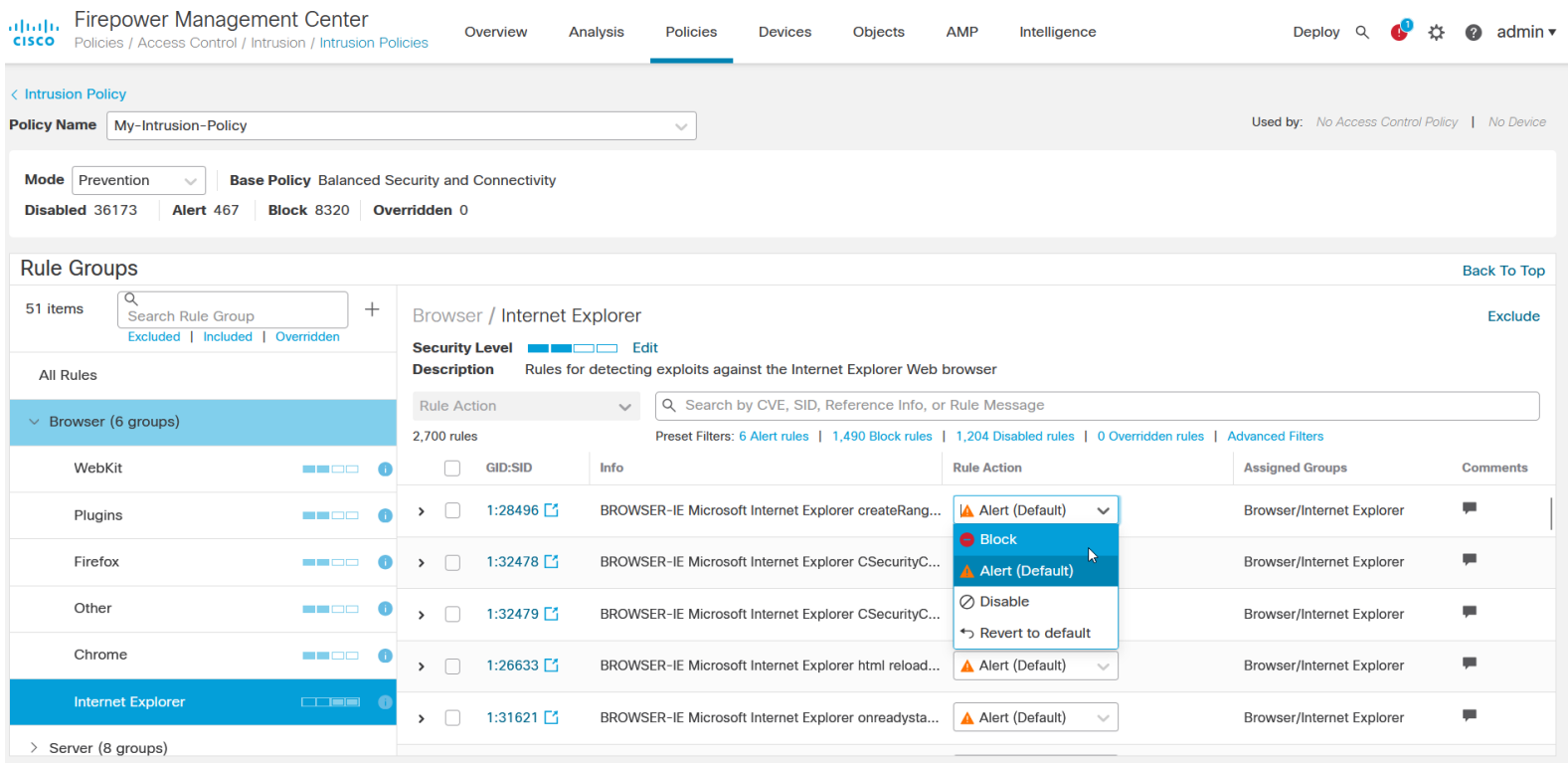
MohsenKheradmand MK

Configuring an Intrusion Policy

➢ Enabling or Disabling an Intrusion Rule

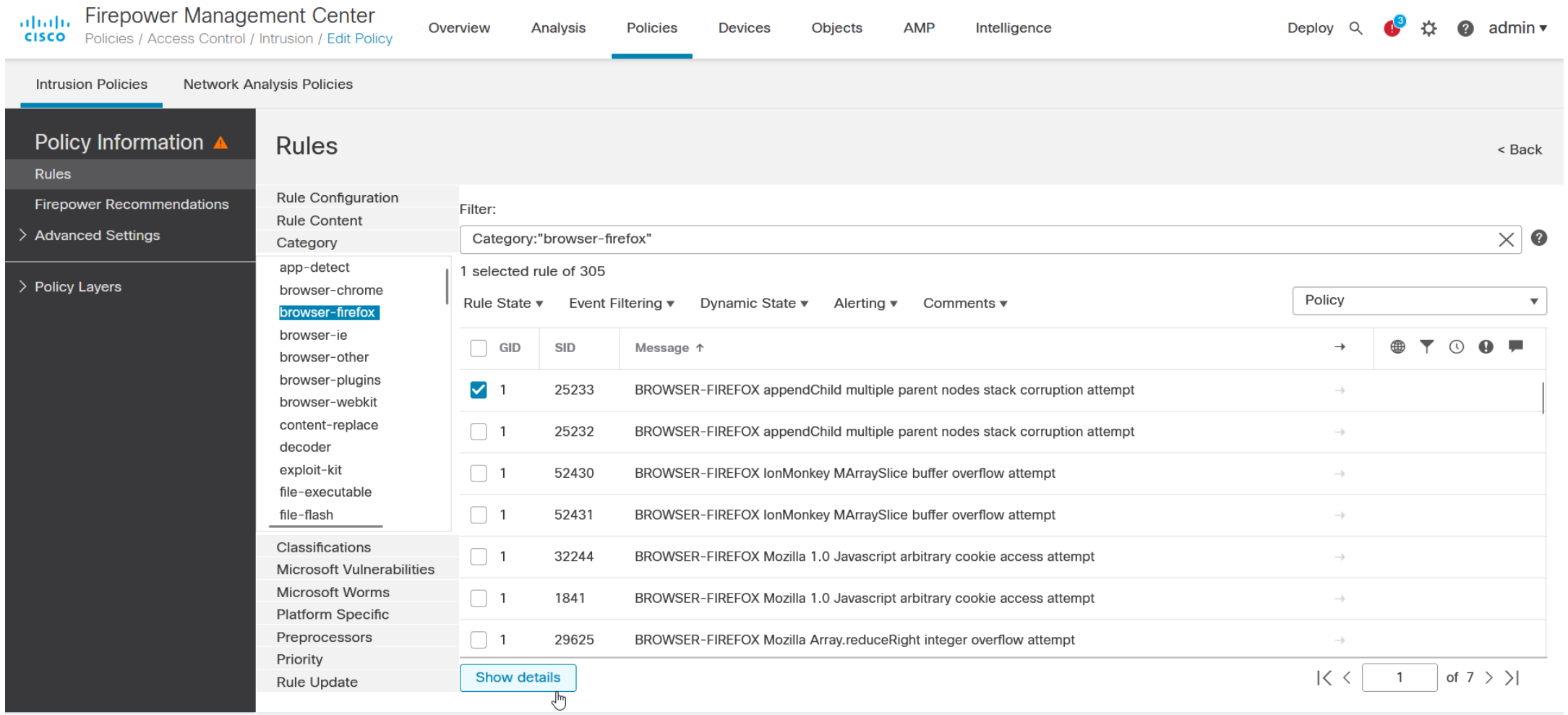
- There are thousands of intrusion rules in FTD (many of them are enables and many are disabled

1) Click Snort 3 rule editor
2) from the Rule Groups select your group
3) Select Rule Action of the desired Rule
4) No need to save any change



Configuring an Intrusion Policy

➢ Enabling or Disabling an Intrusion Rule



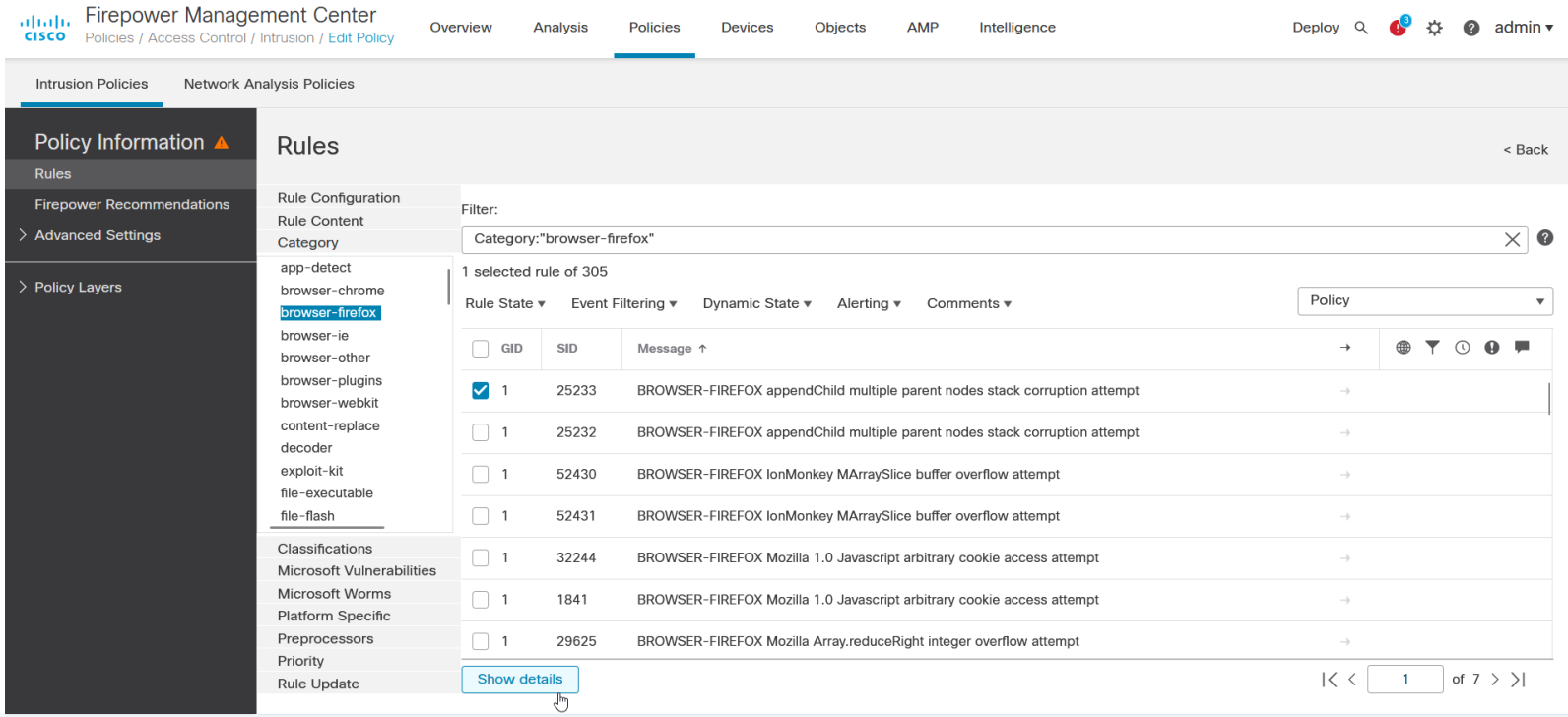
Snort **2** editor

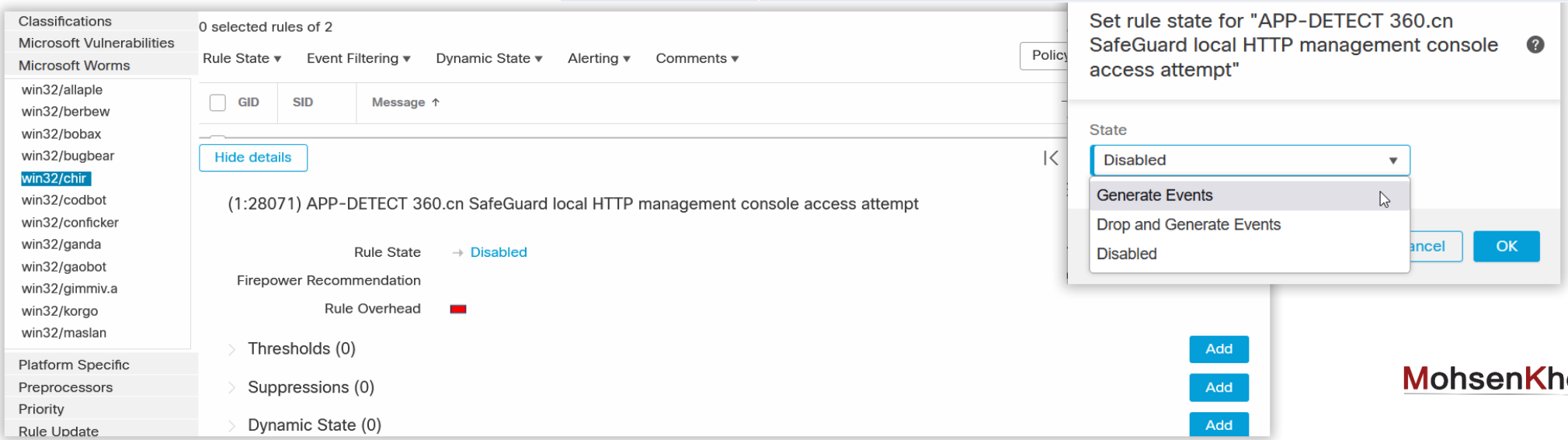
Intrusion Rule

Configuring an Intrusion Policy

➢ Enabling or Disabling an Intrusion Rule

1) Click Snort 2 rule editor
2) Click Rule
3) Select your desired Rule
4) Click Show Details
5) Change Rule State or other settings



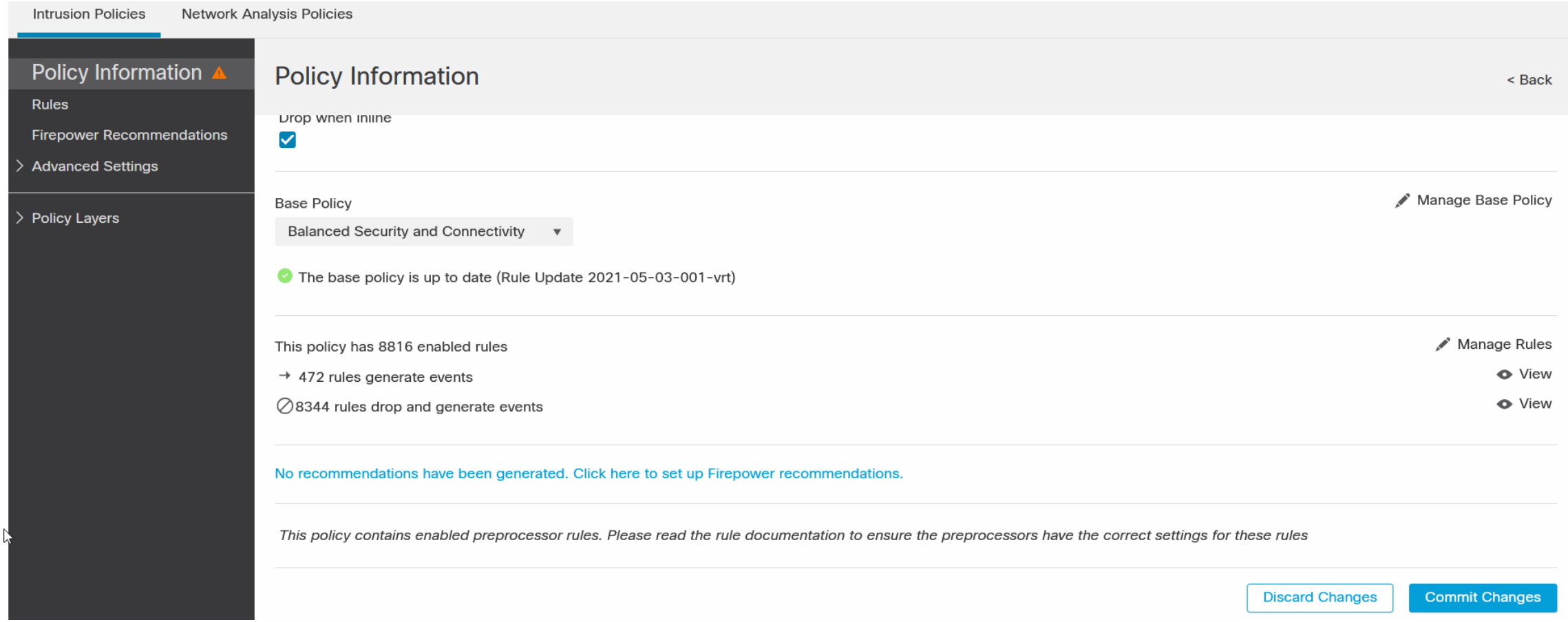


MohsenKheradmand MK

Configuring an Intrusion Policy

➢ Enabling or Disabling an Intrusion Rule

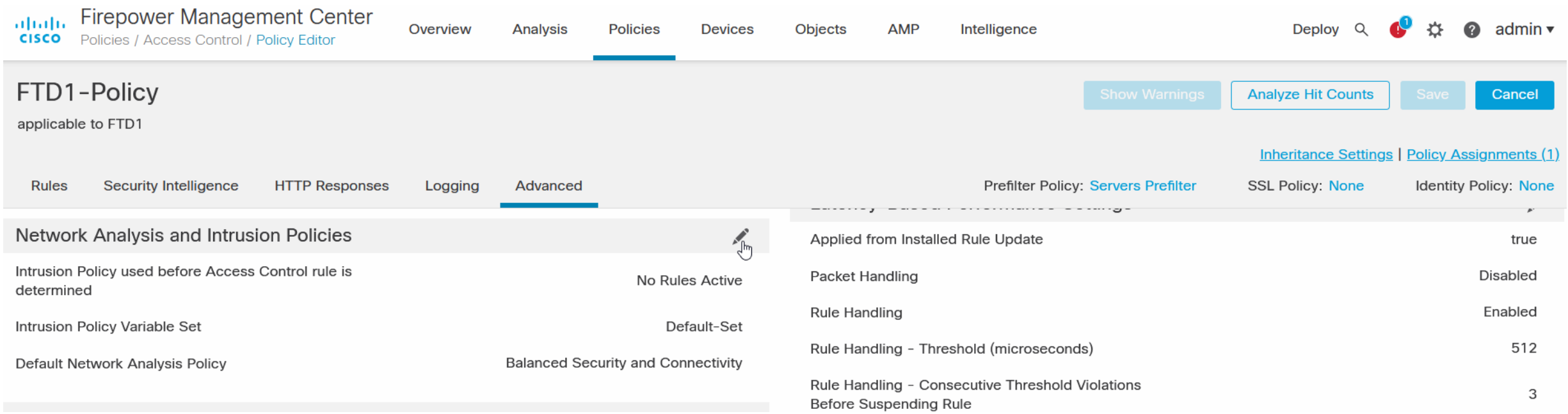
- Finally , Go to the Policy Information page. save any changes by clicking the **Commit Changes** button



MohsenKheradmand MK

Policy Deployment

- Policies > Access Control > Access Control
- Create a new Policy or edit existing Policy
- Click Advanced
- Network Analysis and Intrusion Policies > click edit

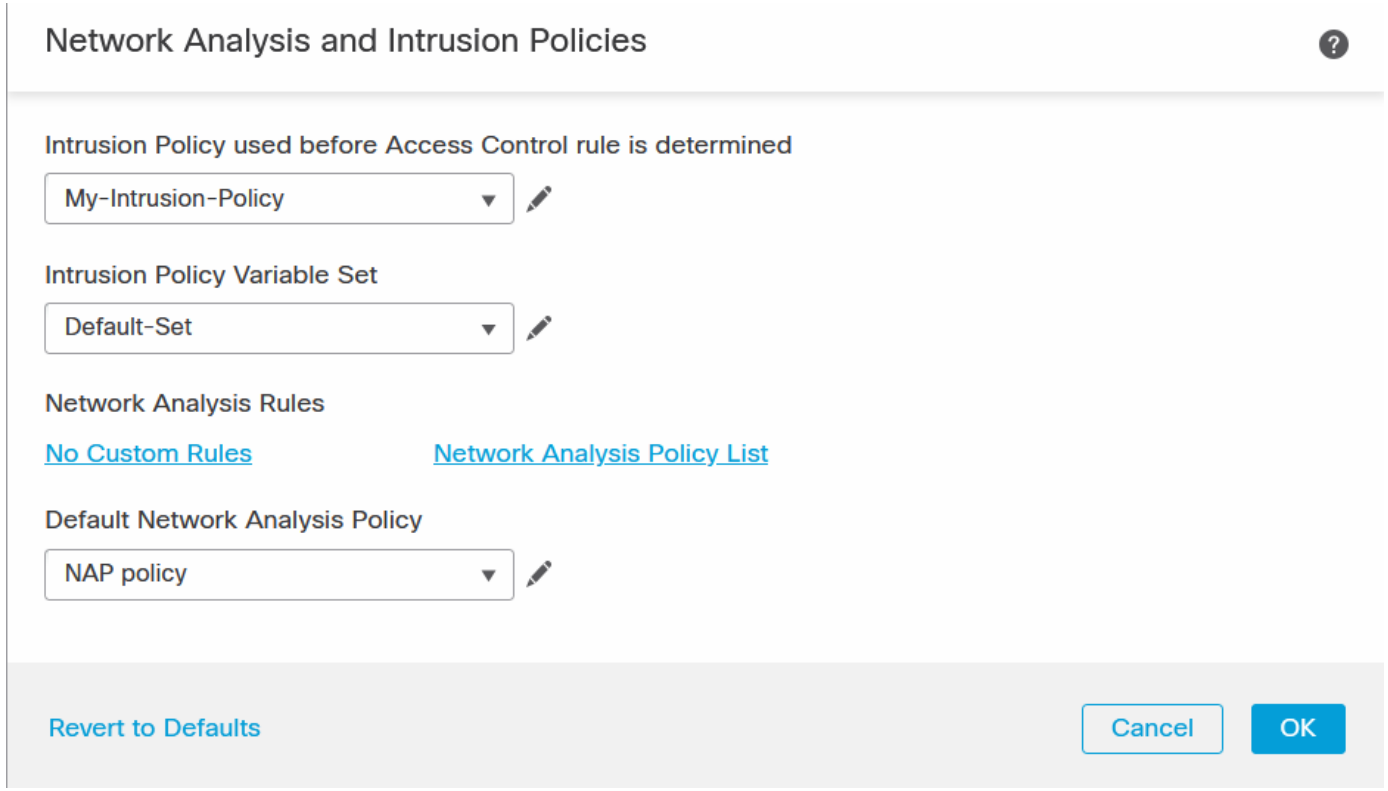


Policy Deployment

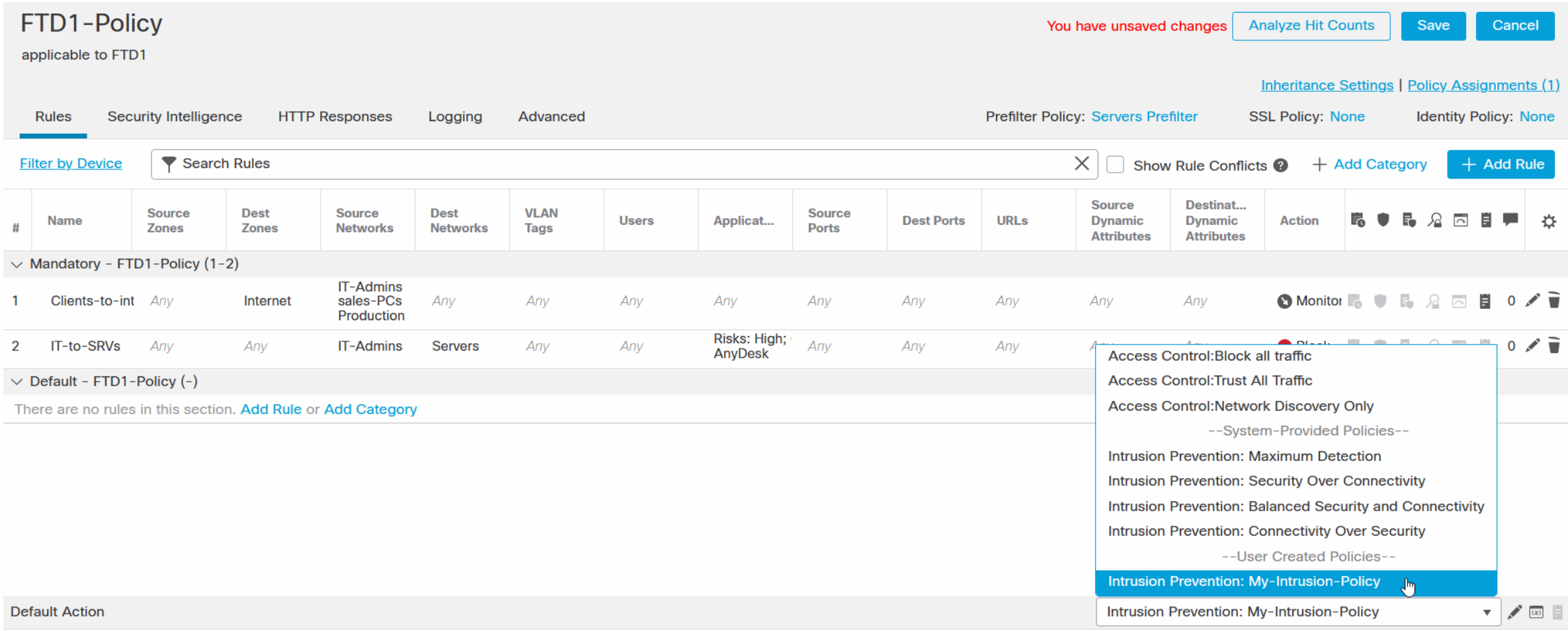
Edit Network Analysis and Intrusion Policies

- Select the Intrusion Policy that you have created
- Select Variable Set (can be leave default)
- Select Analysis Policy that you have created
- Click Ok

- Note : you can use custom Analysis Rule or edit the existing in this windows



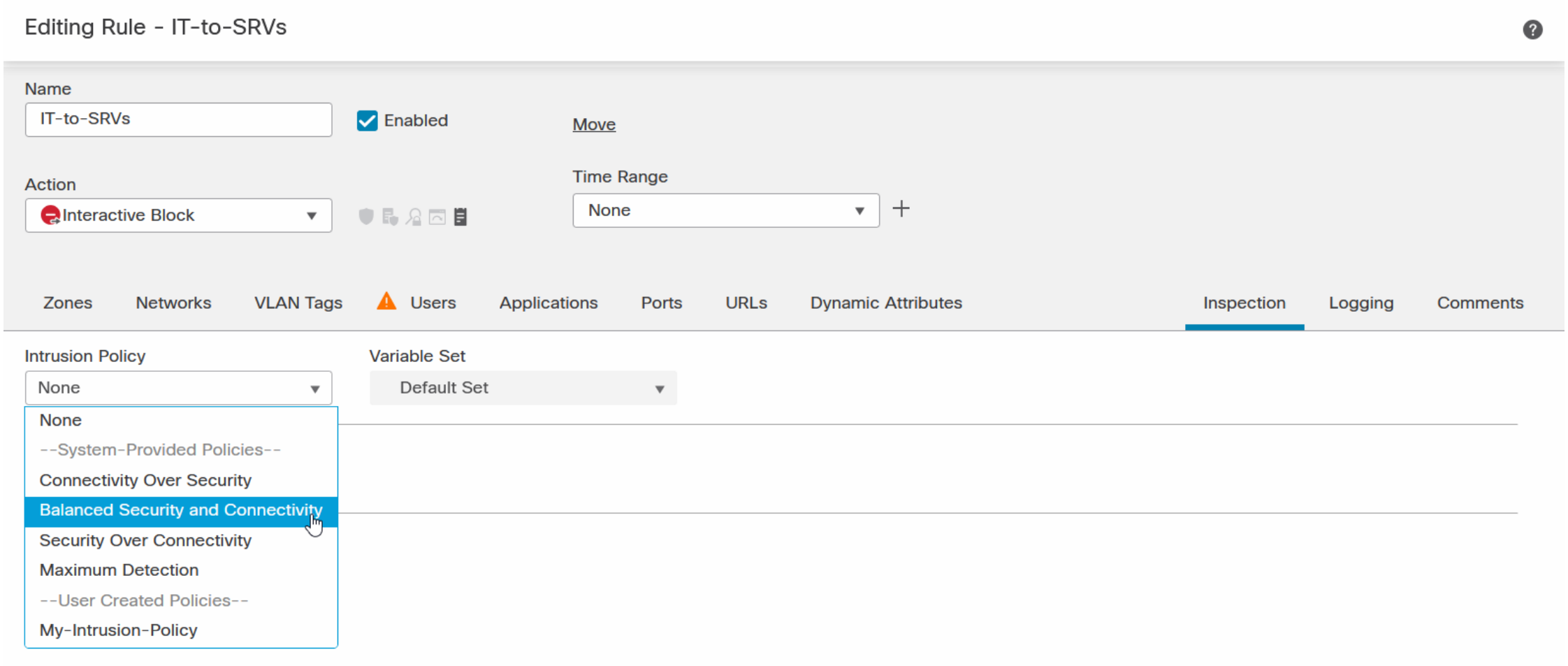
Policy Deployment



- For any traffic that does not match any access control rule, select a system provided or custom intrusion policy as the default action

Policy Deployment

- You can also set an inspection policy per access control rule

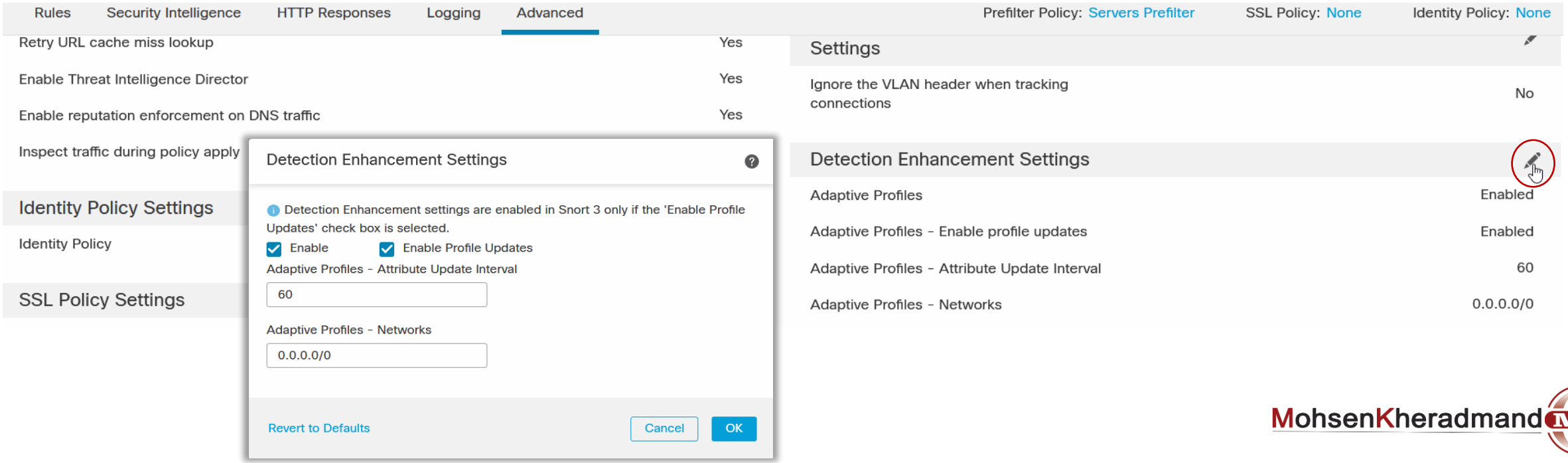


- Note : the Intrusion Policy can be specified only by Allow action or interactive block

Intrusion Rule

➢ Intrusion Policy Recommendations

- If you want to match and filter packets based on 5-tuple , use ACP or Prefilter than Intrusion Policy
- Select the "*Balanced Security and Connectivity policy*" as the base policy when you create a new network analysis policy and intrusion policy (better performance)
- Use the intrusion rule recommendations feature within the intrusion policy
- Enhance detection by selecting both advanced options : Adaptive Profiles and Enable Profile Update



MohsenKheradmand MK

➢ Intrusion Policy Recommendations

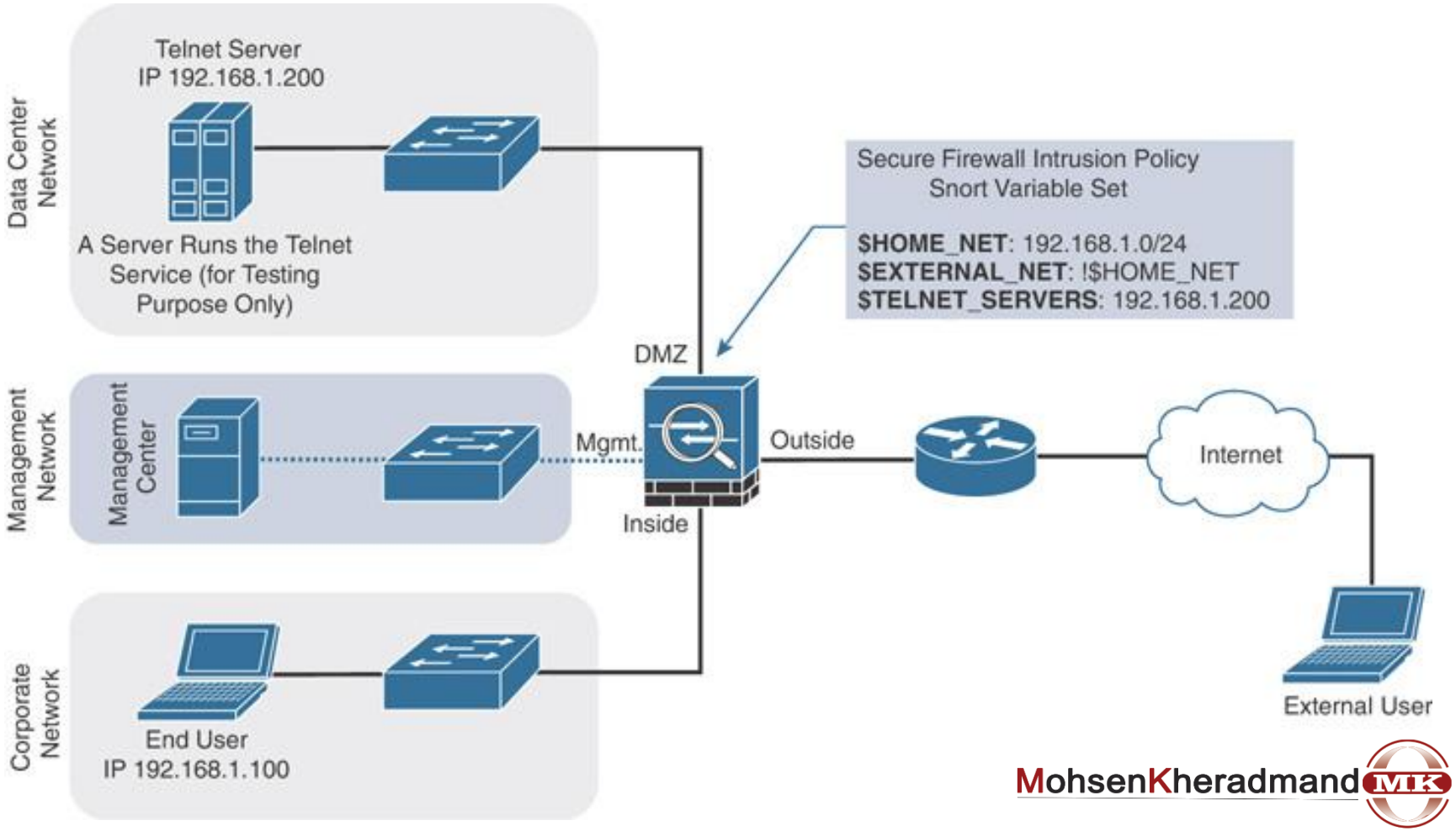
- If you want to match and filter packets based on 5-tuple , use ACP or Prefilter than Intrusion Policy
- Select the "*Balanced Security and Connectivity policy*" as the base policy when you create a new network analysis policy and intrusion policy (better performance)
- Use the intrusion rule recommendations feature within the intrusion policy
- Enhance detection by selecting both advanced options : Adaptive Profiles and Enable Profile Update
- For IPS deployment , use the ingress and egress interfaces as an inline interface pair (inside an inline set)
- For IDS deployment , deploy the FTD in inline tap mode instead of in passive mode (can switch to inline mode faster)
- In Passive mode , ensure that Adaptive Profiles option is enabled
  (Policies > Access control > Advanced >Detection Enhancement Settings > Adaptive Profiles)
  It enables the FTD to adapt intrusion rules dynamically based on the metadata of the service, client application, and host traffic.
- In firewall mode , better to select Routed mode , (however , you can use transparency or a bump in the wire, by using inline mode like transparent mode which has less configuration overhead)

Verification

- If the traffic carry a signature of any vulnerability, the FTD trigger an intrusion alert for it
- In IPS mode , FTD would block and in IDS (inline-tap or Passive mode) , FTD generates an alert

Example :

- Using simple Snort rule 1:718
- External user wants to telnet to internal network
- If you enter incorrect credentials, the server sends the Login incorrect message
- And the FTD blocks Any subsequent connection attempts via telnet

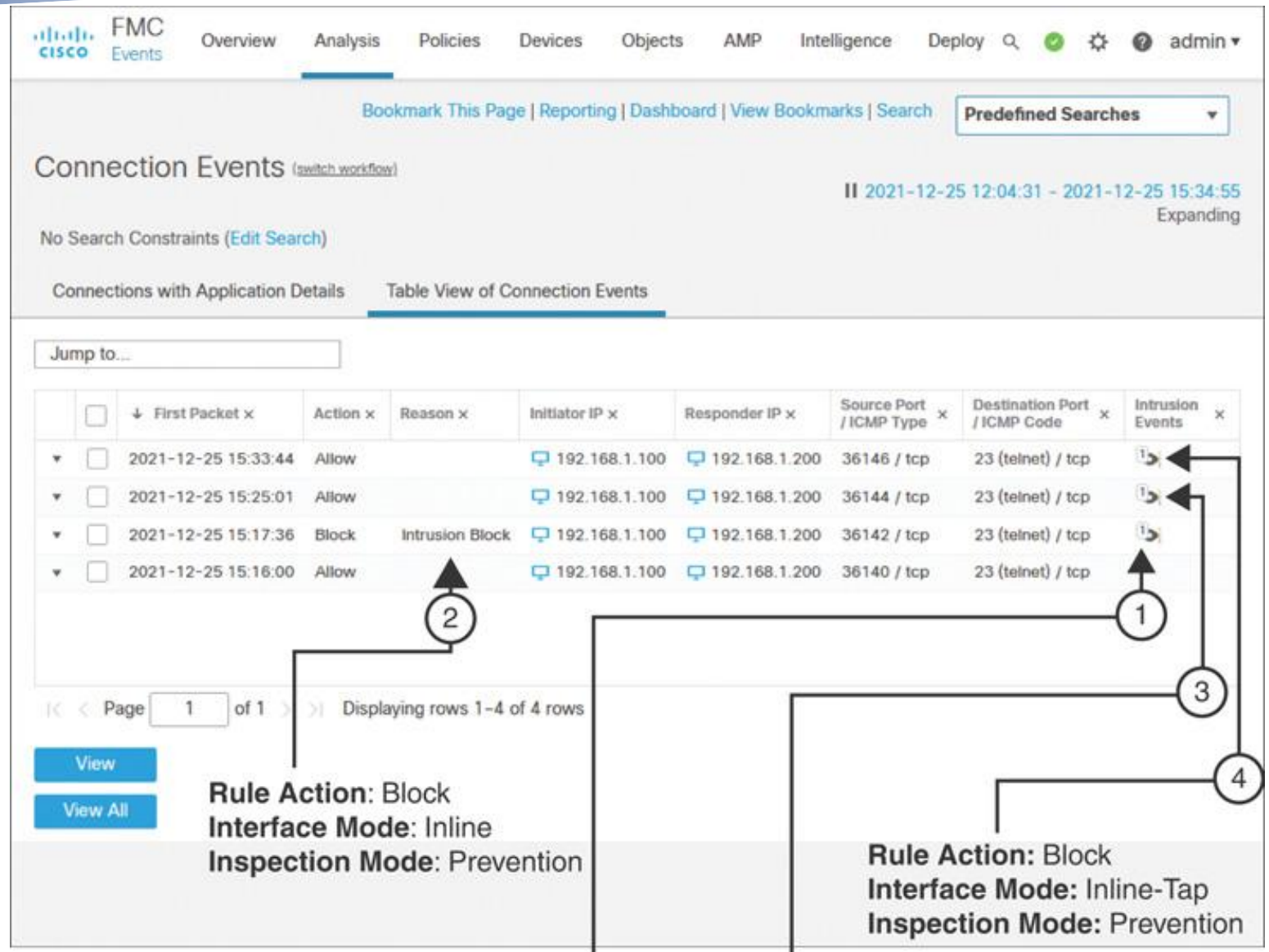


Verification

There is 2 method to check events

- Connection Events page
- Intrusion Events page

Analysis > Connections > Events



MohsenKheradmand MK

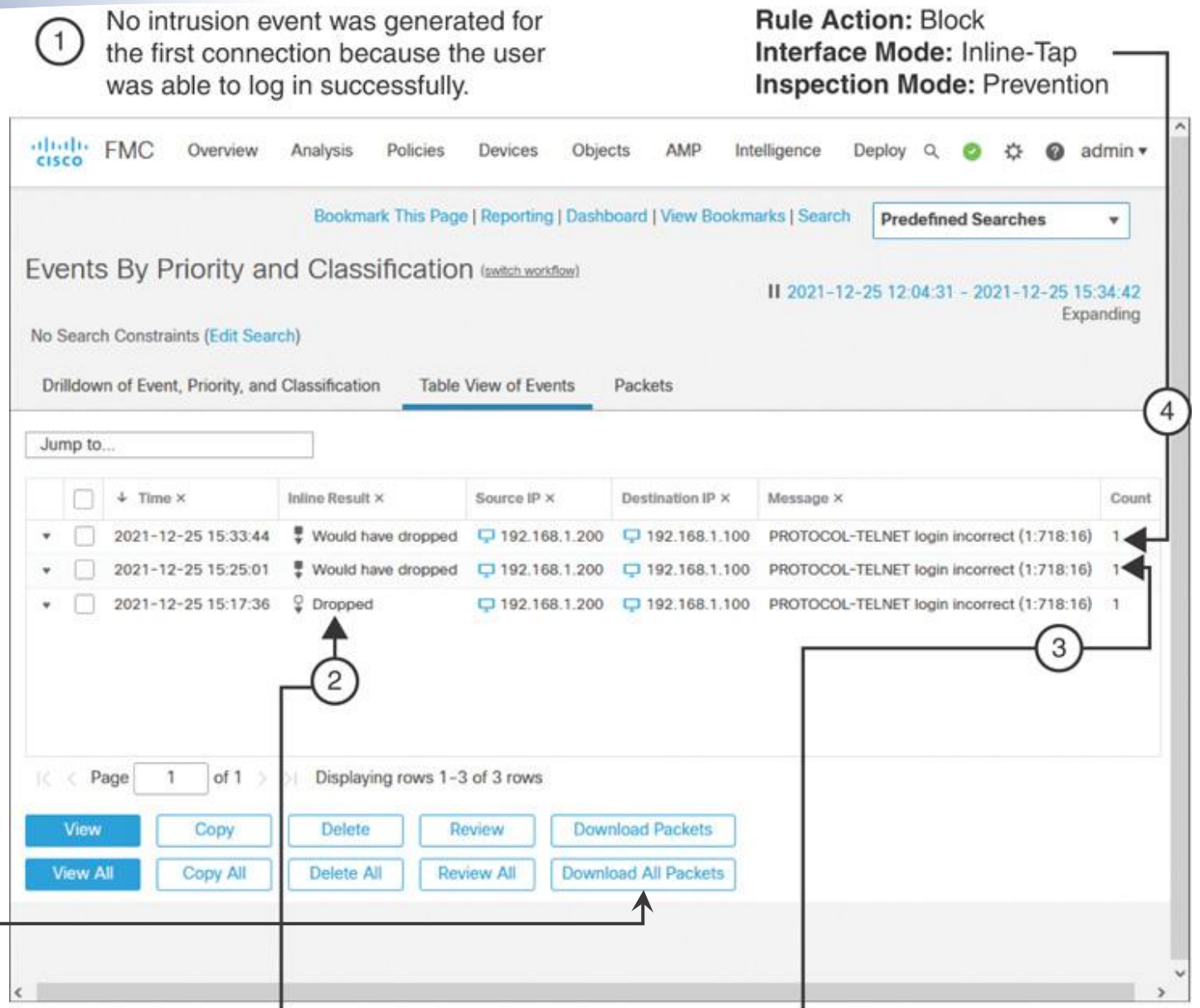
Verification

There is 2 method to check events

- Connection Events page
- Intrusion Events page

Analysis > Intrusions > Events

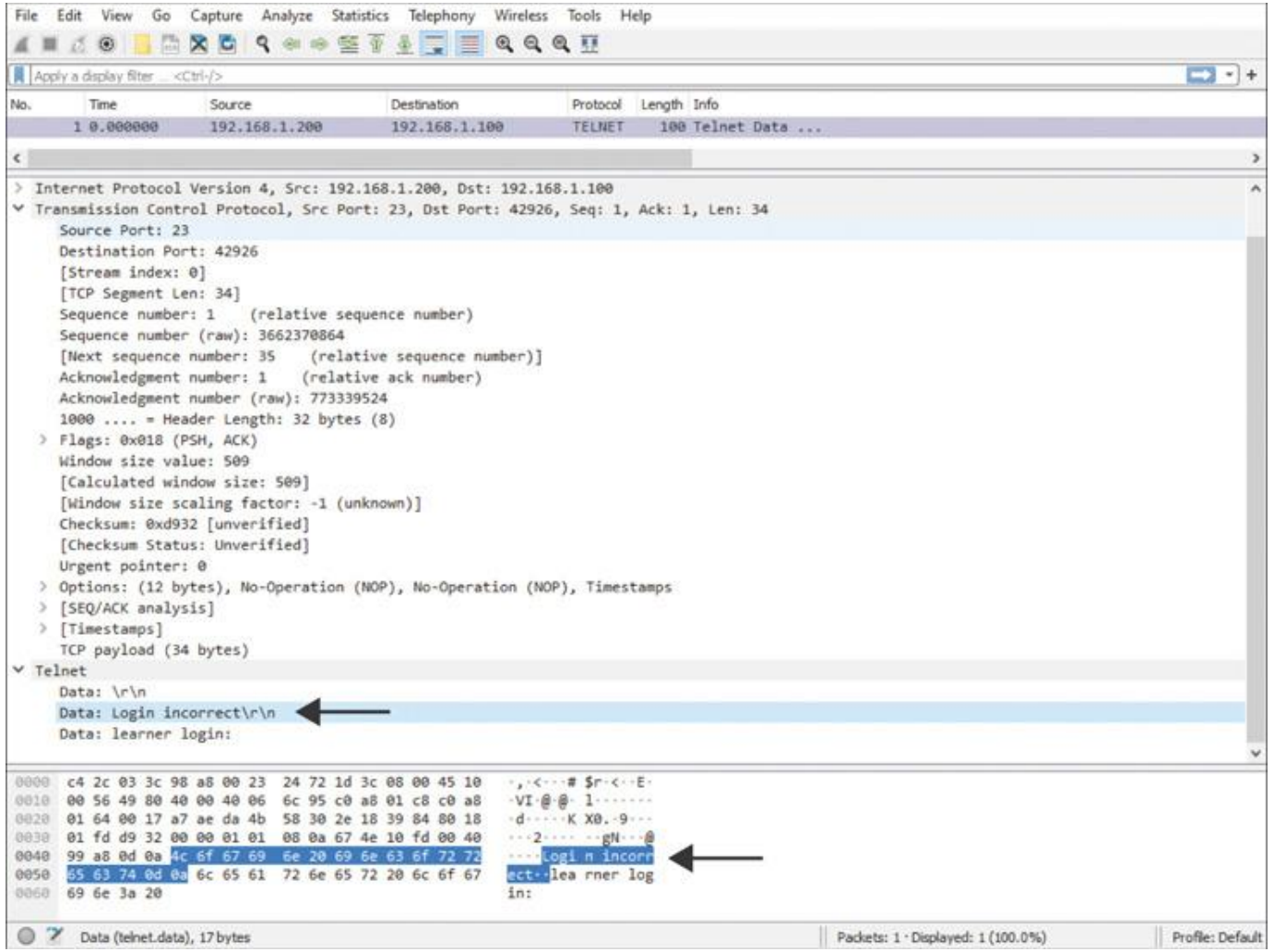
You can also download the packet that triggered as an intrusion event for using in offline analysis third-party software like Wireshark



MohsenKheradmand MK

Verification

The packets are saved in .**pcap** file format which is supported by most packet analyzer tools



Verification

- The Intrusion Events dashboard
- summary of all the intrusion activities