

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 known attacks and intrusions are already encoded in the signatures
- Can not detect Zero-Day attack

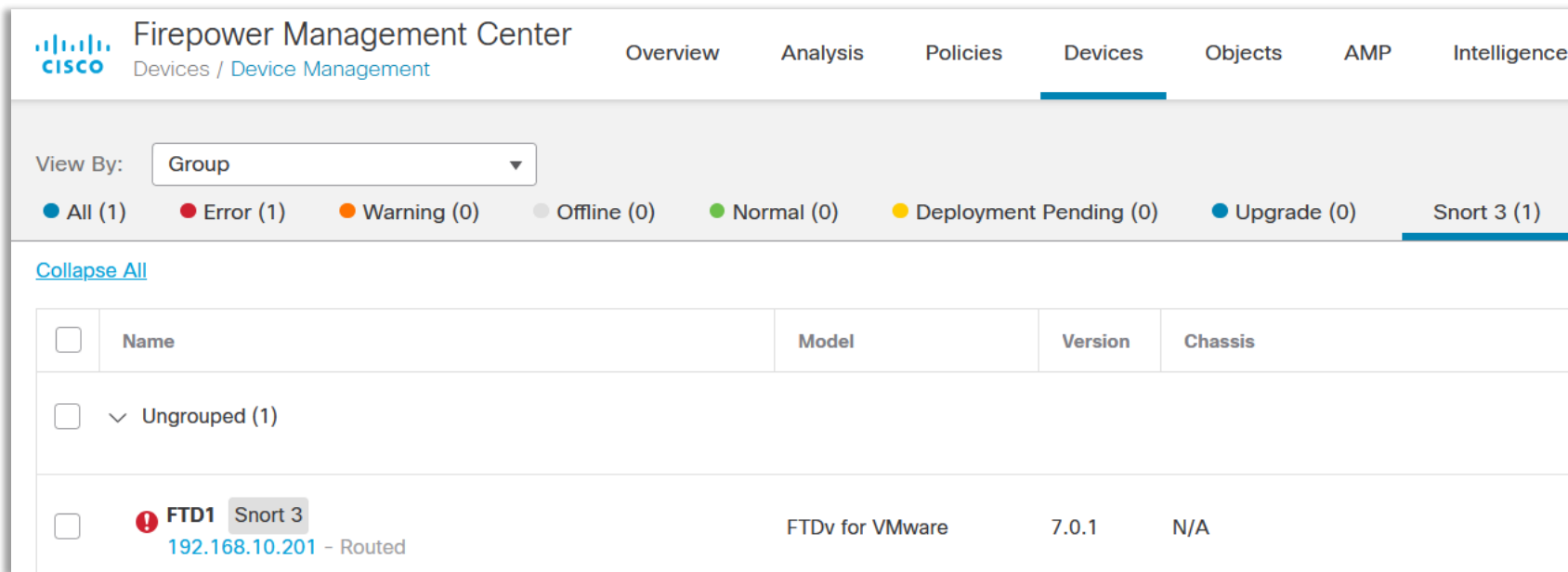
Anomaly based detection

- 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.



Firepower Management Center
Devices / Device Management

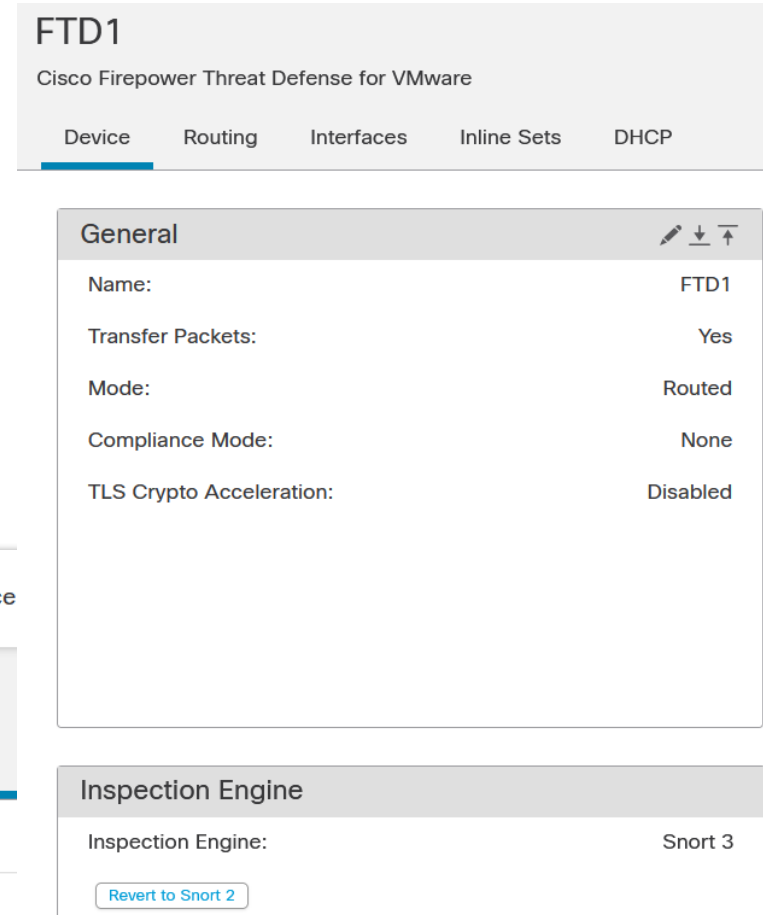
Overview Analysis Policies **Devices** Objects AMP Intelligence

View By: Group

All (1) Error (1) Warning (0) Offline (0) Normal (0) Deployment Pending (0) Upgrade (0) **Snort 3 (1)**

[Collapse All](#)

☐	Name	Model	Version	Chassis
☐	Ungrouped (1)			
☐	FTD1 Snort 3 192.168.10.201 - Routed	FTDv for VMware	7.0.1	N/A



FTD1
Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP

General

Name: FTD1

Transfer Packets: Yes

Mode: Routed

Compliance Mode: None

TLS Crypto Acceleration: Disabled

Inspection Engine

Inspection Engine: Snort 3

[Revert to Snort 2](#)

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

Add Rule?

Name

☒ Enabled

Insert

into Mandatory

Action

→ Allow



Time Range

None

+

Zones

Networks

VLAN Tags

 Users

Applications

Ports

URLs

Dynamic Attributes

Inspection

Logging

Comments

Intrusion Policy

Connectivity Over Security

Variable Set

Default Set



File Policy

None



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.

Firepower Management Center

Policies / Access Control / Intrusion / Intrusion Policies

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy Search 5 ? admin

Intrusion Policies Network Analysis Policies

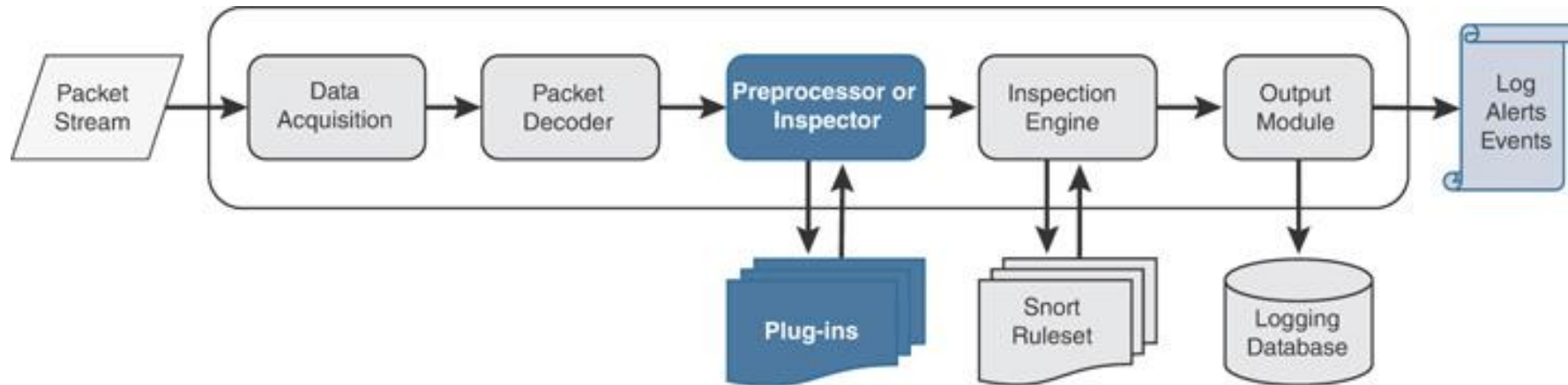
Show Snort 3 Sync status Search by Intrusion Policy, Description, or Base Policy All IPS Rules IPS Mapping Compare Policies Create Policy

Intrusion Policy	Description	Base Policy	Usage Information
mk	Connectivity Over Security	Connectivity Over Security	No Access Control Policy No Device Snort 2 Version Snort 3 Version

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

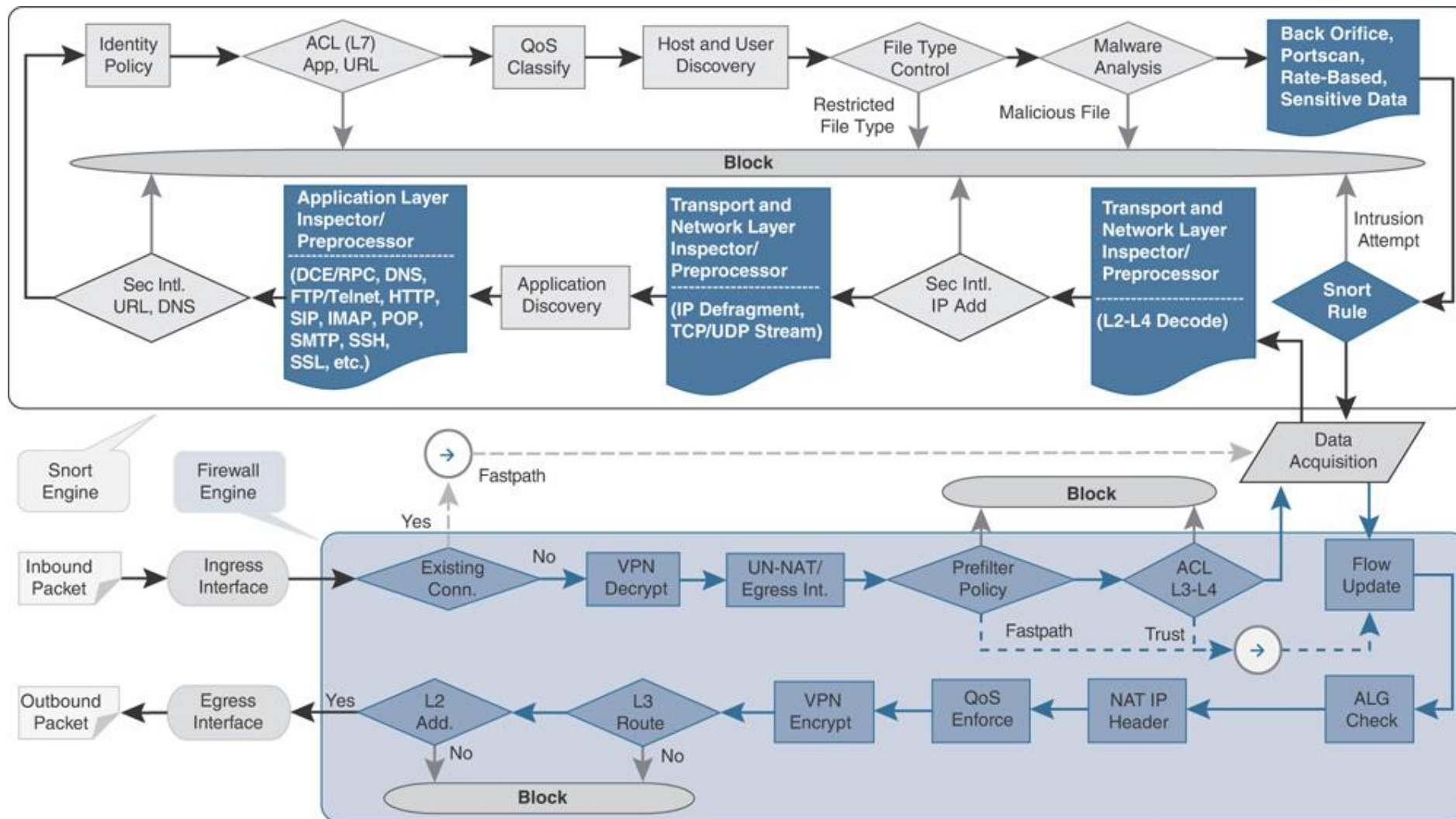
Network Analysis Policy

- 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

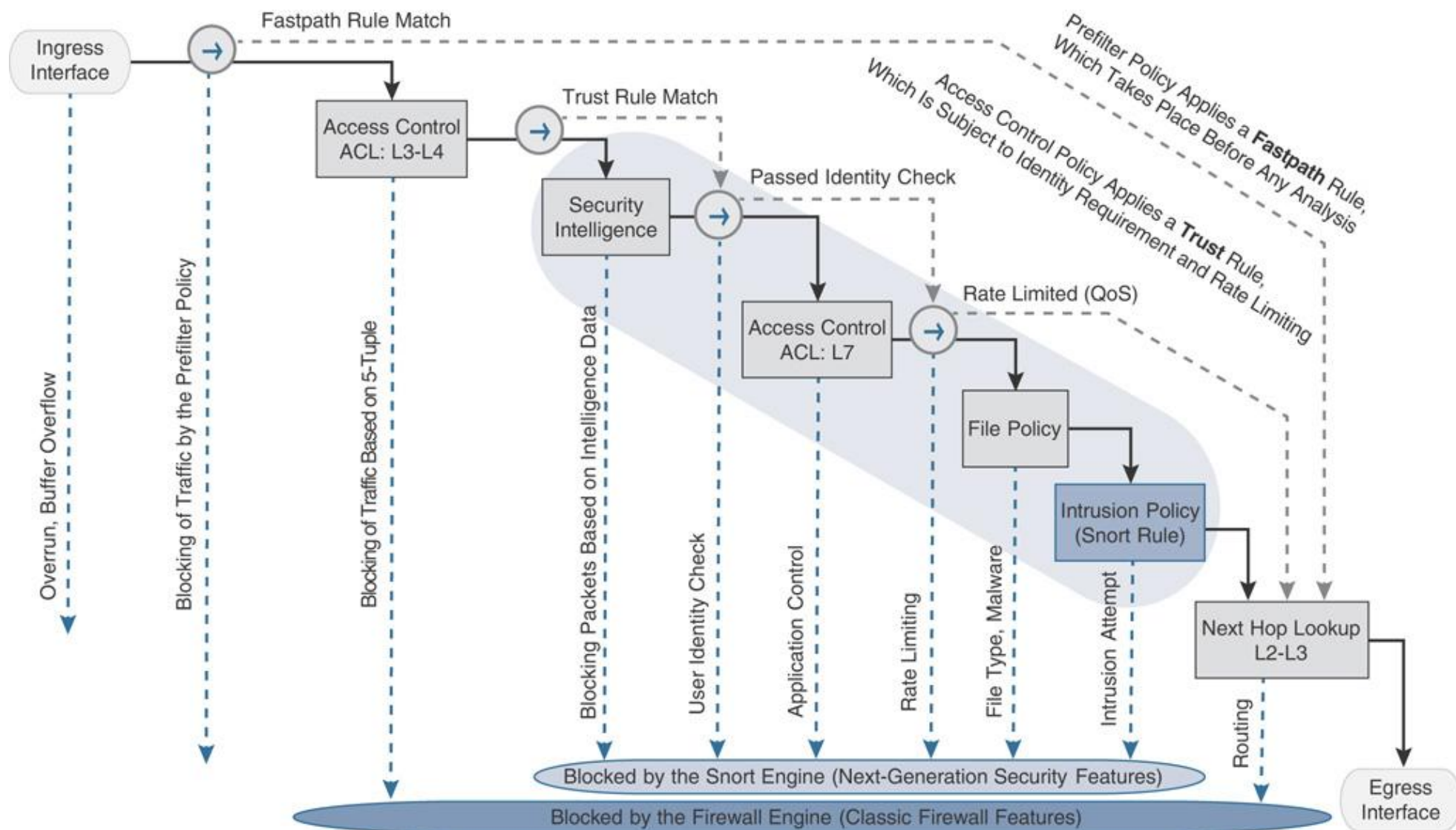


Network Analysis Policy Components Acting in Multiple Phases

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)

The screenshot shows the Cisco Firepower Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Objects' tab is selected, and a dropdown menu is open, showing 'Object Management' and 'Intrusion Rules'. The 'Intrusion Rules' page is displayed, showing a list of rules for 'Browser / Plugins'. The page includes a search bar, a table of rules, and a sidebar with navigation options.

Browser / Plugins

Description Rules for detecting exploits against Web browser plugins

Rule Actions Search by CVE, SID, Reference Info, or Rule Message

2,552 rules

	GID:SID	Info	Rule Action	Assigned Groups	Alert Config
> ☐	1:9427	BROWSER-PLUGINS Acer LunchApp.APlunc...	Disable (Default)	Browser/Plugins	None
> ☐	1:29507	BROWSER-PLUGINS ABB Test Signal Viewe...	Disable (Default)	Browser/Plugins	None
> ☐	1:37005	BROWSER-PLUGINS AAA EasyGrid DoSave...	Disable (Default)	Browser/Plugins	None
> ☐	1:36868	BROWSER-PLUGINS IDAutomation IDAuto.B...	Disable (Default)	Browser/Plugins	None
> ☐	1:32626	BROWSER-PLUGINS Adobe Flash broker pri...	Disable (Default)	Browser/Plugins	None
> ☐	1:37007	BROWSER-PLUGINS AAA EasyGrid DoSave...	Disable (Default)	Browser/Plugins	None
> ☐	1:36869	BROWSER-PLUGINS IDAutomation IDAuto.P...	Disable (Default)	Browser/Plugins	None

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 :

Edit Rule 1:221:12

[\(View Documentation, Rule Comment\)](#)

Message

PROTOCOL-ICMP TFN Probe

Classification

Attempted Denial of Service

[Edit Classifications](#)

Action

alert

Protocol

icmp

Direction

Directional

Source IPs

\$EXTERNAL_NET

Source Port

any

Destination IPs

\$HOME_NET

Destination Port

any

Detection Options

icmp_id

678

✕

^

v

Intrusion Policy

- System-Provided Variable Sets

Variable Set

Variables represent values used in intrusion policies.

Name
Default-Set

Edit Variable Set Default-Set

Name: Default-Set

Description: This Variable Set is system-provided.

Variable Name	Type	Value
FTP_PORTS	Port	[21, 3535, 2100]
GTP_PORTS	Port	[2152, 2123, 3386]
HOME_NET	Network	any
HTTP_PORTS	Port	[16000, 8243, 3057, 7778, 8008, 83, 434...]
HTTP_SERVERS	Network	HOME_NET
ORACLE_PORTS	Port	any

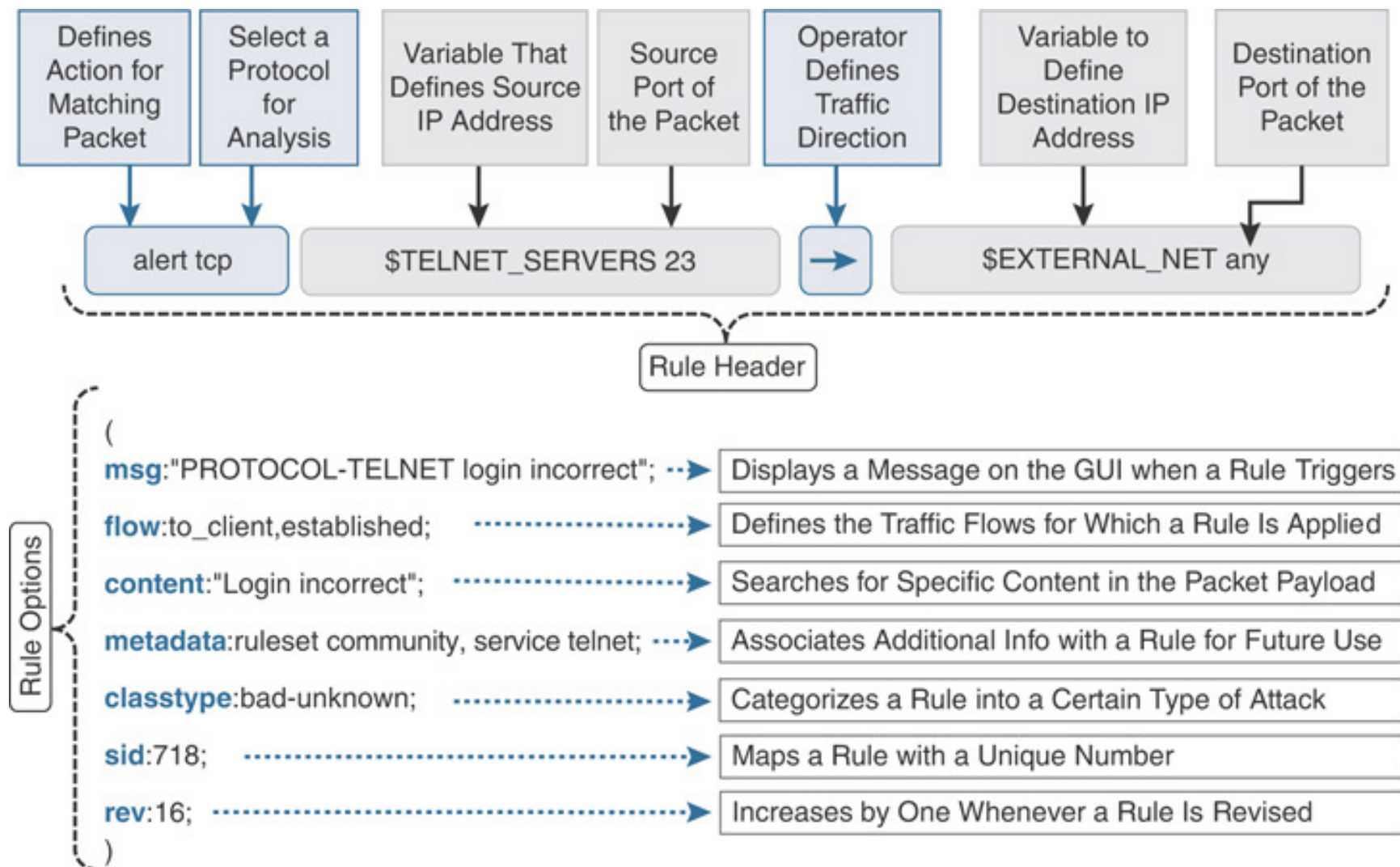
Default Values of the Snort Variables Set

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

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

Base Policy

Balanced Security and Connectivity

Balanced Security and Connectivity

Connectivity Over Security

Maximum Detection

No Rules Active

Security Over Connectivity

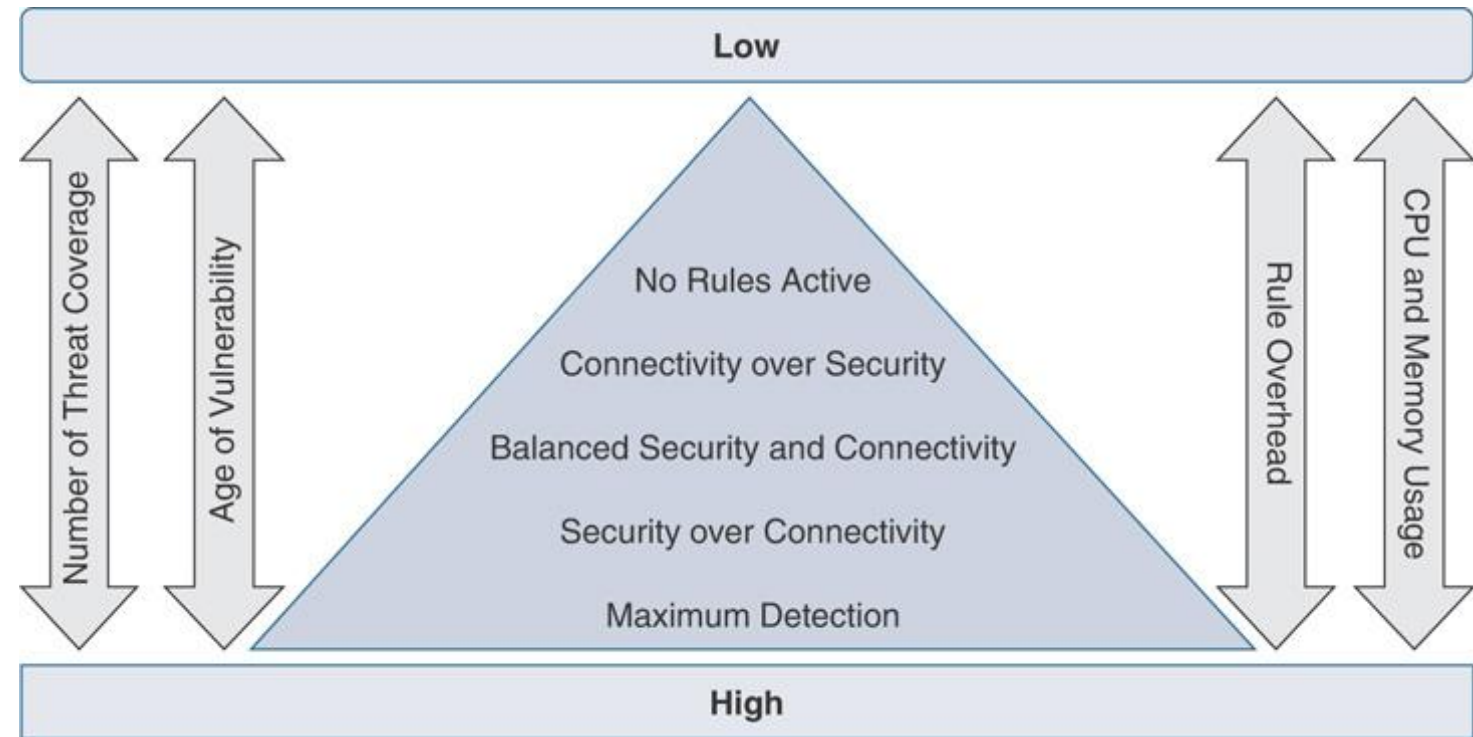
Intrusion Policy

- 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

Firepower Management Center

Policies / Access Control / Intrusion / Network Analysis Policies

Overview Analysis Policies Devices Objects AMP Intelligence Deploy ? admin

Intrusion Policies Network Analysis Policies

Filter by Policy Name, Description, or Base Policy

NAP Mapping Compare Policies Create Policy

Create Network Analysis Policy

Name*
NAP policy

Description
prevention policy

Inspection Mode
☐ Detection ☒ Prevention

Intrusion rule actions are always applied. Connections that match a drop rule are blocked.

Base Policy
Balanced Security and Connectivity

Cancel Save

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

Configuring a Network Analysis Policy

Firepower Management Center
Policies / Access Control / Intrusion / Intrusion Policies

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy 🔍 2 ⚙️ ? admin ▾

Intrusion Policies Network Analysis Policies

Hide Snort 3 Sync status ⓘ 🔍 Search by Intrusion Policy, Description, or Base Policy All IPS Rules IPS Mapping ⓘ Compare Policies Create Policy

Intrusion Policy	Description	Base Policy	Usage Information	
11 🔄 Snort 3 is in sync with Snort 2		Balanced Security and Connectivity	No Access Control Policy No Device	Snort 2 Version Snort 3 Version  Edit

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

Warning

⚠️ Customizing Network Analysis Policy is an advanced feature targeted at expert users. Make sure that you understand that editing a Network Analysis Policy can impact the traffic and performance. We recommend that you make an informed decision before editing the Network Analysis Policy.

Do you want to continue?

No Yes

Configuring a Network Analysis Policy

Editing the Network Analyses Policy (advanced configuration)

[< Network Analysis Policies](#)

CancelSave

NAP Configuration Guide

Used by: No Access Control Policy | No Device

Policy NameNAP policy

ModePreventionBase PolicyBalanced Security and Connectivity

Descriptionprevention policy

Inspectors

– with overrides

Search by entering any text

Show Overrides Only

Actions

arp_spoof

binder

cip

dce_smb

dce_tcp

dnp3

ftp_client

Default Configuration (Balanced Security and Connectivity)

Overridden Configuration

```
{
  "ftp_client" : {
    "type" : "multiton",
    "instances" : [
      {
```

Configuring an Intrusion Policy

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

The screenshot shows the Cisco Firepower Management Center interface. The top navigation bar includes the Cisco logo, the title 'Firepower Management Center', and a breadcrumb trail: 'Policies / Access Control / Intrusion / Intrusion Policies'. The main navigation tabs are 'Overview', 'Analysis', 'Policies' (which is selected), 'Devices', 'Objects', 'AMP', and 'Intelligence'. On the right side of the navigation bar are links for 'Deploy', a search icon, a notification icon with a '2', a settings gear, a help icon, and a user profile 'admin'. Below the navigation bar, there are two sub-tabs: 'Intrusion Policies' (selected) and 'Network Analysis Policies'. A search bar is present with the placeholder text 'Search by Intrusion Policy, Description, or Base Policy'. To the right of the search bar are three buttons: 'All IPS Rules', 'IPS Mapping' (with an information icon), and 'Compare Policies'. On the far right is a prominent blue 'Create Policy' button. A modal dialog box titled 'Create Intrusion Policy' is open in the foreground. It contains the following fields and options: 'Name*' with the value 'My-Intrusion-Policy'; 'Description' (empty); 'Inspection Mode' with radio buttons for 'Detection' and 'Prevention' (selected); a note stating 'Intrusion rule actions are always applied. Connections that match a drop rule are blocked.'; and 'Base Policy' with a dropdown menu showing 'Balanced Security and Connectivity'. At the bottom of the dialog are 'Cancel' and 'Save' buttons.

- 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

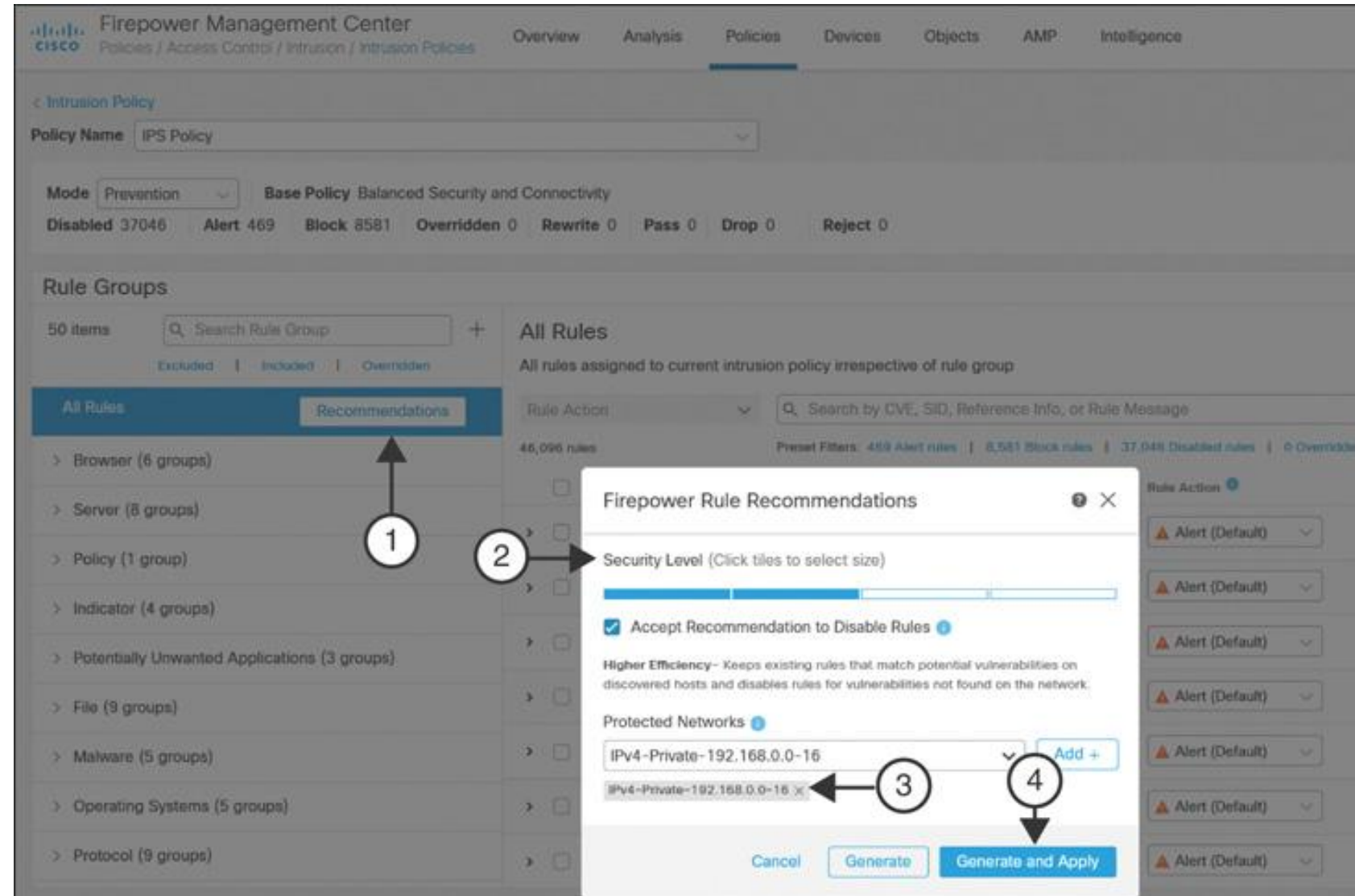
- You should use intrusion rule recommendations after the majority of the hosts in your network are discovered
- The intrusion rule recommendations feature is disabled, by default

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

The screenshot displays the Cisco FMC interface for configuring intrusion rules. The top navigation bar includes links for Overview, Analysis, Policies, Devices, Objects, AMP, Intelligence, and Deploy. The left sidebar shows the 'Policy Information' menu with 'Rules' and 'Firepower Recommendations' highlighted. The main panel is titled 'Firepower Recommended Rules Configuration' and contains the following elements:

- A message: 'No recommendations have been generated.'
- An unchecked checkbox: 'Include all differences between recommendations and rule states in policy reports'.
- An expanded 'Advanced Settings' section.
- A 'Networks to Examine' section with an input field containing '192.168.0.0/16' and a note: '(Single IP address, CIDR block, or comma-separated list)'.
- A 'Firepower Recommended Rules Configuration' section with a 'Recommendation Threshold (By Rule Overhead)' slider. The slider has markers for None, Low, Medium, and High, with the current setting at Medium.
- An unchecked checkbox: 'Accept Recommendations to Disable Rules'.
- Two buttons at the bottom: 'Generate Recommendations' and 'Generate and Use Recommendations'.

Note : Higher Threshold = higher processing overhead

➤ Enabling or Disabling an Intrusion Rule

Snort 3 editor

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

The screenshot displays the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes links for Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The 'Policies' tab is active, showing the 'Intrusion Policy' configuration page. The policy name is 'My-Intrusion-Policy'. The mode is set to 'Prevention' and the base policy is 'Balanced Security and Connectivity'. The policy status shows 36173 Disabled, 467 Alert, 8320 Block, and 0 Overridden rules.

The 'Rule Groups' section on the left lists 51 items, including 'Browser (6 groups)' and 'Internet Explorer'. The 'Browser / Internet Explorer' group is selected, showing 2,700 rules. A search bar is available to filter rules by CVE, SID, Reference Info, or Rule Message. The 'Rule Action' dropdown menu is open, showing options: Alert (Default), Block, Alert (Default), Disable, and Revert to default. The 'Assigned Groups' column shows 'Browser/Internet Explorer' for all rules.

Rule Action	Assigned Groups	Comments
Alert (Default)	Browser/Internet Explorer	
Block	Browser/Internet Explorer	
Alert (Default)	Browser/Internet Explorer	
Disable	Browser/Internet Explorer	
Revert to default	Browser/Internet Explorer	
Alert (Default)	Browser/Internet Explorer	
Alert (Default)	Browser/Internet Explorer	

Configuring an Intrusion Policy

➤ Enabling or Disabling an Intrusion Rule

Firepower Management Center

Policies / Access Control / Intrusion / Edit Policy

Overview Analysis Policies Devices Objects AMP Intelligence Deploy 🔍 ⚙️ ? admin ▼

Intrusion Policies Network Analysis Policies

Policy Information ▲
Rules
Firepower Recommendations
> Advanced Settings

> Policy Layers

Rules

[< Back](#)

Rule Configuration
 Rule Content
 Category
 app-detect
 browser-chrome
browser-firefox
 browser-ie
 browser-other
 browser-plugins
 browser-webkit
 content-replace
 decoder
 exploit-kit
 file-executable
 file-flash
 Classifications
 Microsoft Vulnerabilities
 Microsoft Worms
 Platform Specific
 Preprocessors
 Priority
 Rule Update

Filter:

1 selected rule of 305

Rule State ▼ Event Filtering ▼ Dynamic State ▼ Alerting ▼ Comments ▼
Policy ▼

☐	GID	SID	Message ↑	
☒	1	25233	BROWSER-FIREFOX appendChild multiple parent nodes stack corruption attempt	→
☐	1	25232	BROWSER-FIREFOX appendChild multiple parent nodes stack corruption attempt	→
☐	1	52430	BROWSER-FIREFOX IonMonkey MArraySlice buffer overflow attempt	→
☐	1	52431	BROWSER-FIREFOX IonMonkey MArraySlice buffer overflow attempt	→
☐	1	32244	BROWSER-FIREFOX Mozilla 1.0 Javascript arbitrary cookie access attempt	→
☐	1	1841	BROWSER-FIREFOX Mozilla 1.0 Javascript arbitrary cookie access attempt	→
☐	1	29625	BROWSER-FIREFOX Mozilla Array.reduceRight integer overflow attempt	→

|< <

1

of 7 >> |

[Show details](#)

Snort 2 editor

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

Firepower Management Center
Policies / Access Control / Intrusion / Edit Policy

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy 🔍 ⚙️ ? admin ▾

Intrusion Policies Network Analysis Policies

Policy Information ▲

Rules

Firepower Recommendations

Advanced Settings

Policy Layers

Rules

Rule Configuration

Rule Content

Category

app-detect

browser-chrome

browser-firefox

browser-ie

browser-other

browser-plugins

browser-webkit

content-replace

decoder

exploit-kit

file-executable

file-flash

Classifications

Microsoft Vulnerabilities

Microsoft Worms

Platform Specific

Preprocessors

Priority

Rule Update

Filter:

Category: "browser-firefox"

1 selected rule of 305

Rule State ▼ Event Filtering ▼ Dynamic State ▼ Alerting ▼ Comments ▼

Policy

☐	GID	SID	Message ↑	→	🌐	🔍	🕒	🚨	💬
☒	1	25233	BROWSER-FIREFOX appendChild multiple parent nodes stack corruption attempt	→					
☐	1	25232	BROWSER-FIREFOX appendChild multiple parent nodes stack corruption attempt	→					
☐	1	52430	BROWSER-FIREFOX IonMonkey MArraySlice buffer overflow attempt	→					
☐	1	52431	BROWSER-FIREFOX IonMonkey MArraySlice buffer overflow attempt	→					
☐	1	32244	BROWSER-FIREFOX Mozilla 1.0 Javascript arbitrary cookie access attempt	→					
☐	1	1841	BROWSER-FIREFOX Mozilla 1.0 Javascript arbitrary cookie access attempt	→					
☐	1	29625	BROWSER-FIREFOX Mozilla Array.reduceRight integer overflow attempt	→					

Show details

1 of 7

Classifications

Microsoft Vulnerabilities

Microsoft Worms

win32/allapple

win32/berbew

win32/bobax

win32/bugbear

win32/chir

win32/codbot

win32/conficker

win32/ganda

win32/gaobot

win32/gimmiv.a

win32/korgo

win32/maslan

Platform Specific

Preprocessors

Priority

Rule Update

0 selected rules of 2

Rule State ▼ Event Filtering ▼ Dynamic State ▼ Alerting ▼ Comments ▼

Hide details

(1:28071) APP-DETECT 360.cn SafeGuard local HTTP management console access attempt

Rule State → Disabled

Firepower Recommendation

Rule Overhead

Thresholds (0)

Suppressions (0)

Dynamic State (0)

Set rule state for "APP-DETECT 360.cn SafeGuard local HTTP management console access attempt"

State

Disabled

Generate Events

Drop and Generate Events

Disabled

Cancel OK

Add

Add

Add

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

The screenshot shows a web interface for configuring intrusion policies. At the top, there are two tabs: "Intrusion Policies" (selected) and "Network Analysis Policies". On the left, a dark sidebar contains a menu with "Policy Information" (highlighted with an orange triangle), "Rules", "Firepower Recommendations", "> Advanced Settings", and "> Policy Layers". The main content area is titled "Policy Information" and includes a "< Back" link in the top right. The settings shown are: "Drop when inline" with a checked checkbox; "Base Policy" set to "Balanced Security and Connectivity" with a dropdown arrow and a "Manage Base Policy" link; a green status message "The base policy is up to date (Rule Update 2021-05-03-001-vrt)"; a summary stating "This policy has 8816 enabled rules" with details "→ 472 rules generate events" and "○ 8344 rules drop and generate events", each with a "View" link; a blue link "No recommendations have been generated. Click here to set up Firepower recommendations."; and a note "This policy contains enabled preprocessor rules. Please read the rule documentation to ensure the preprocessors have the correct settings for these rules". At the bottom right, there are two buttons: "Discard Changes" and "Commit Changes".

Policy Deployment

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

 Firepower Management Center
Policies / Access Control / Policy Editor

OverviewAnalysisPoliciesDevicesObjectsAMPIntelligence

Deploy 🔍    admin ▼

FTD1-Policy

applicable to FTD1

Show WarningsAnalyze Hit CountsSaveCancel

[Inheritance Settings](#) | [Policy Assignments \(1\)](#)

RulesSecurity IntelligenceHTTP ResponsesLoggingAdvanced

Prefilter Policy: Servers PrefilterSSL Policy: NoneIdentity Policy: None

Network Analysis and Intrusion Policies

Intrusion Policy used before Access Control rule is determined

Intrusion Policy Variable Set

Default Network Analysis Policy

No Rules Active

Default-Set

Balanced Security and Connectivity

Applied from Installed Rule Update

Packet Handling

Rule Handling

Rule Handling - Threshold (microseconds)

Rule Handling - Consecutive Threshold Violations Before Suspending Rule

true

Disabled

Enabled

512

3

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

Network Analysis and Intrusion Policies

Intrusion Policy used before Access Control rule is determined

My-Intrusion-Policy

Intrusion Policy Variable Set

Default-Set

Network Analysis Rules

[No Custom Rules](#) [Network Analysis Policy List](#)

Default Network Analysis Policy

NAP policy

[Revert to Defaults](#) [Cancel](#) [OK](#)

Policy Deployment

FTD1-Policy

applicable to FTD1

You have unsaved changes

Analyze Hit Counts

Save

Cancel

Inheritance Settings

Policy Assignments (1)

Rules

Security Intelligence

HTTP Responses

Logging

Advanced

Prefilter Policy: Servers Prefilter

SSL Policy: None

Identity Policy: None

Filter by Device

Search Rules

Show Rule Conflicts

Add Category

Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destinat... Dynamic Attributes	Action	
Mandatory - FTD1-Policy (1-2)															
1	Clients-to-int	Any	Internet	IT-Admins sales-PCs Production	Any	Any	Any	Any	Any	Any	Any	Any	Any	Monitor	
2	IT-to-SRVs	Any	Any	IT-Admins	Servers	Any	Any	Risks: High; AnyDesk	Any	Any	Any				
Default - FTD1-Policy (-)															
There are no rules in this section. Add Rule or Add Category															

Default Action

Access Control:Block all traffic

Access Control:Trust All Traffic

Access Control:Network Discovery Only

--System-Provided Policies--

Intrusion Prevention: Maximum Detection

Intrusion Prevention: Security Over Connectivity

Intrusion Prevention: Balanced Security and Connectivity

Intrusion Prevention: Connectivity Over Security

--User Created Policies--

Intrusion Prevention: My-Intrusion-Policy

Intrusion Prevention: My-Intrusion-Policy

- 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

Editing Rule - IT-to-SRVs ?

Name: ☒ Enabled [Move](#)

Action: Time Range: +

Zones Networks VLAN Tags Users Applications Ports URLs Dynamic Attributes **Inspection** Logging Comments

Intrusion Policy: Variable Set:

None
--System-Provided Policies--
Connectivity Over Security
Balanced Security and Connectivity
Security Over Connectivity
Maximum Detection
--User Created Policies--
My-Intrusion-Policy

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

➤ 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

The screenshot displays a configuration interface with a top navigation bar and a main content area. The top bar includes tabs for 'Rules', 'Security Intelligence', 'HTTP Responses', 'Logging', and 'Advanced' (which is selected). To the right of the tabs, there are policy settings: 'Prefilter Policy: Servers Prefilter', 'SSL Policy: None', and 'Identity Policy: None'. The main content area is divided into two sections. On the left, under the 'Advanced' tab, there is a table with the following rows: 'Retry URL cache miss lookup' (Yes), 'Enable Threat Intelligence Director' (Yes), 'Enable reputation enforcement on DNS traffic' (Yes), and 'Inspect traffic during policy apply'. Below this table are three expandable sections: 'Identity Policy Settings' (containing 'Identity Policy'), 'SSL Policy Settings', and 'Detection Enhancement Settings' (which is currently open as a dialog box). The 'Detection Enhancement Settings' dialog box contains the following information: a note stating 'Detection Enhancement settings are enabled in Snort 3 only if the 'Enable Profile Updates' check box is selected.', two checked checkboxes for 'Enable' and 'Enable Profile Updates', a text input field for 'Adaptive Profiles - Attribute Update Interval' with the value '60', and another text input field for 'Adaptive Profiles - Networks' with the value '0.0.0.0/0'. At the bottom of the dialog are buttons for 'Revert to Defaults', 'Cancel', and 'OK'. On the right side of the main content area, there is a 'Settings' section with a pencil icon, followed by a table with the following rows: 'Ignore the VLAN header when tracking connections' (No), 'Adaptive Profiles' (Enabled), 'Adaptive Profiles - Enable profile updates' (Enabled), 'Adaptive Profiles - Attribute Update Interval' (60), and 'Adaptive Profiles - Networks' (0.0.0.0/0). A red circle with a pencil icon is drawn around the 'Adaptive Profiles' row in this table.

Rules	Security Intelligence	HTTP Responses	Logging	Advanced	Prefilter Policy: Servers Prefilter	SSL Policy: None	Identity Policy: None
Retry URL cache miss lookup				Yes			
Enable Threat Intelligence Director				Yes			
Enable reputation enforcement on DNS traffic				Yes			
Inspect traffic during policy apply							

Identity Policy Settings

Identity Policy

SSL Policy Settings

Detection Enhancement Settings

ⓘ Detection Enhancement settings are enabled in Snort 3 only if the 'Enable Profile Updates' check box is selected.

☒ Enable ☒ Enable Profile Updates

Adaptive Profiles - Attribute Update Interval

Adaptive Profiles - Networks

[Revert to Defaults](#) [Cancel](#) [OK](#)

Settings

✎

Ignore the VLAN header when tracking connections No

Detection Enhancement Settings

✎

Adaptive Profiles Enabled

Adaptive Profiles - Enable profile updates Enabled

Adaptive Profiles - Attribute Update Interval 60

Adaptive Profiles - Networks 0.0.0.0/0

➤ Intrusion Policy Recommendations

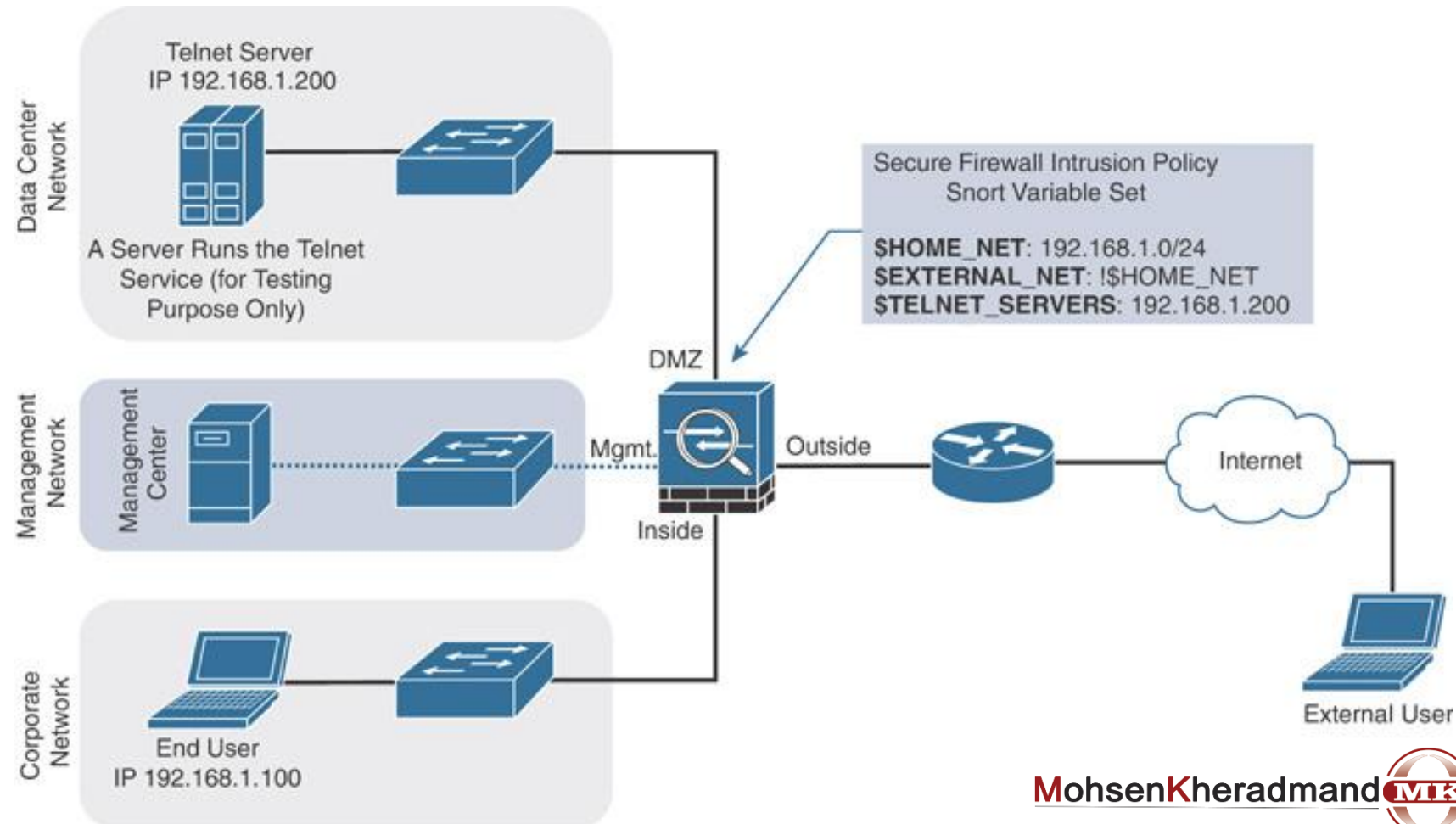
- If you want to match and filter packets based on 5-tuple , use ACP or Prefilter than Intrusion Policy
- Select the “*Balanced Security and Connectivity policy*” as the base policy when you create a new network analysis policy and intrusion policy (better performance)
- Use the intrusion rule recommendations 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

Connection Events (switch workflow)

No Search Constraints (Edit Search)

Connections with Application Details Table View of Connection Events

Jump to...

	First Packet x	Action x	Reason x	Initiator IP x	Responder IP x	Source Port / ICMP Type x	Destination Port / ICMP Code x	Intrusion Events x
▼	☐ 2021-12-25 15:33:44	Allow		192.168.1.100	192.168.1.200	36146 / tcp	23 (telnet) / tcp	
▼	☐ 2021-12-25 15:25:01	Allow		192.168.1.100	192.168.1.200	36144 / tcp	23 (telnet) / tcp	
▼	☐ 2021-12-25 15:17:36	Block	Intrusion Block	192.168.1.100	192.168.1.200	36142 / tcp	23 (telnet) / tcp	
▼	☐ 2021-12-25 15:16:00	Allow		192.168.1.100	192.168.1.200	36140 / tcp	23 (telnet) / tcp	

Page 1 of 1 Displaying rows 1-4 of 4 rows

View View All

Rule Action: Block
Interface Mode: Inline
Inspection Mode: Prevention

Rule Action: Block
Interface Mode: Inline-Tap
Inspection Mode: Prevention

The first connection was allowed. No intrusion event was generated for it, because the user was able to log in successfully.

Rule Action: Block
Interface Mode: Inline
Inspection Mode: Detection

Intrusion Rule

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

1 No intrusion event was generated for the first connection because the user was able to log in successfully.

Rule Action: Block
Interface Mode: Inline-Tap
Inspection Mode: Prevention

	Time x	Inline Result x	Source IP x	Destination IP x	Message x	Count
▼	2021-12-25 15:33:44	Would have dropped	192.168.1.200	192.168.1.100	PROTOCOL-TELNET login incorrect (1:718:16)	1
▼	2021-12-25 15:25:01	Would have dropped	192.168.1.200	192.168.1.100	PROTOCOL-TELNET login incorrect (1:718:16)	1
▼	2021-12-25 15:17:36	Dropped	192.168.1.200	192.168.1.100	PROTOCOL-TELNET login incorrect (1:718:16)	1

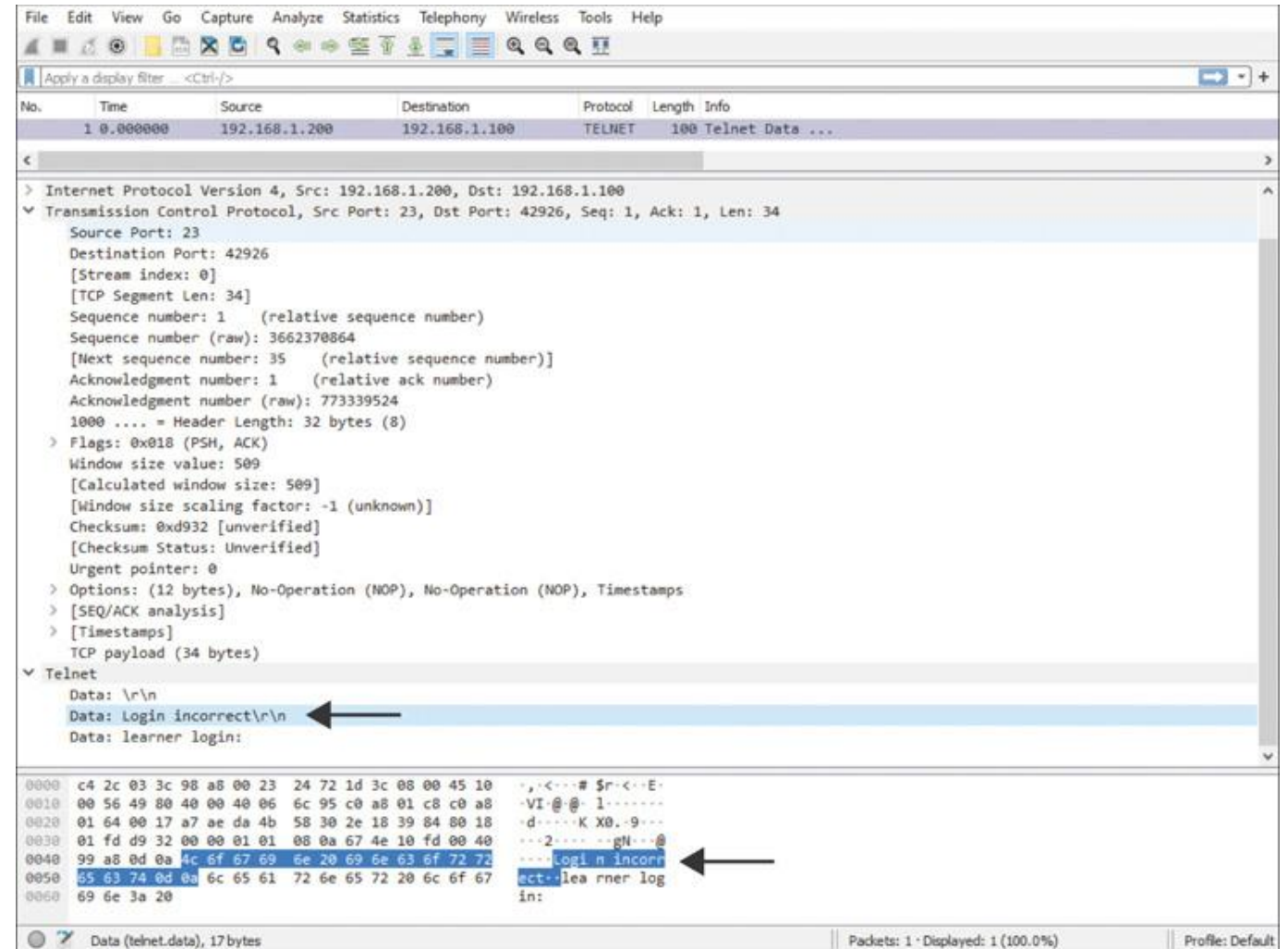
Rule Action: Block
Interface Mode: Inline
Inspection Mode: Prevention

Rule Action: Block
Interface Mode: Inline
Inspection Mode: Detection

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

