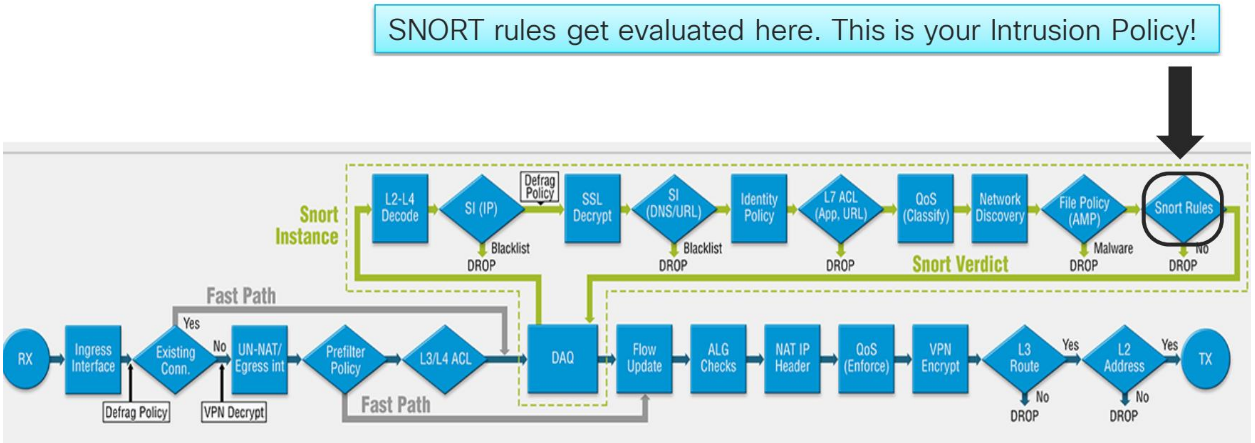
Intrusion Policies:

- An intrusion is any activity like Malware that is designed to compromise your data security.
- An intrusion is somebody attempting to break into or misuse your system or the Network.
- Intrusion can be defined any set of actions that attempt to compromise CIA of resources.
- Intrusion Policy is where setup and configure your Intrusion Prevention/Detection policies.
- The Cisco Firepower Intrusion Policies enable Intrusion Prevention System (IPS) functions.
- These policies are a collection of SNORT rules and they are evaluated against traffic flows.
- Cisco Firepower Threat Defense uses the SNORT engine to perform deep packet inspection.
- In Cisco FTD SNORT is a pattern matching regex engine, it will look for patterns in the traffic.
- In the Cisco Firepower FTD each SNORT rule is a regex string that matches a known attack.
- FTD Intrusion Policies enable IPS functions, these policies are collection of SNORT rules.
- These collection of SNORT rules in Cisco Firepower FTD are evaluated against traffic flows.
- There are several default policies, so you do not need to know details about each rule.
- It is based on Snort & like other similar systems it is signature-based protection mechanism.
- Out of the box the Cisco FTD Firepower comes with a number of pre-defined base policies.
- There are several default policies, so you don’t need to know the details about each rule.
- In Cisco Firepower FTD the Intrusion policies are linked to Access Control Policies (ACPs).
- More rules enabled more performance is impacted, but more security secure you have.
- Each Intrusion Policy can use its own Base Policy & you can have multiple Intrusion Policies.
- Intrusion Prevention system helps organizations in identifying malicious traffic and blocks it.
- IPS technology can be deployed in-line to monitor incoming traffic and inspect that traffic.
- Intrusion rule is a set of keywords & arguments that system uses to detect vulnerabilities.
- Intrusion rule is uses to detect vulnerabilities attempts to exploit vulnerabilities on network.
- System analyzes network traffic compares packets against conditions specified in each rule.
- If the packet data matches all the conditions specified in an intrusion rule, the rule triggers.
- If a rule is an alert rule, it generates an intrusion event, if it is pass rule, it ignores the traffic.
- For drop rule in an inline deployment, the system drops the packet and generates an event.
- Can view and evaluate intrusion events from Firepower Management Center web interface.
- In Cisco Firepower Threat Defense (FTD) Intrusion Policies (IPS) Manage your Snort Rules.

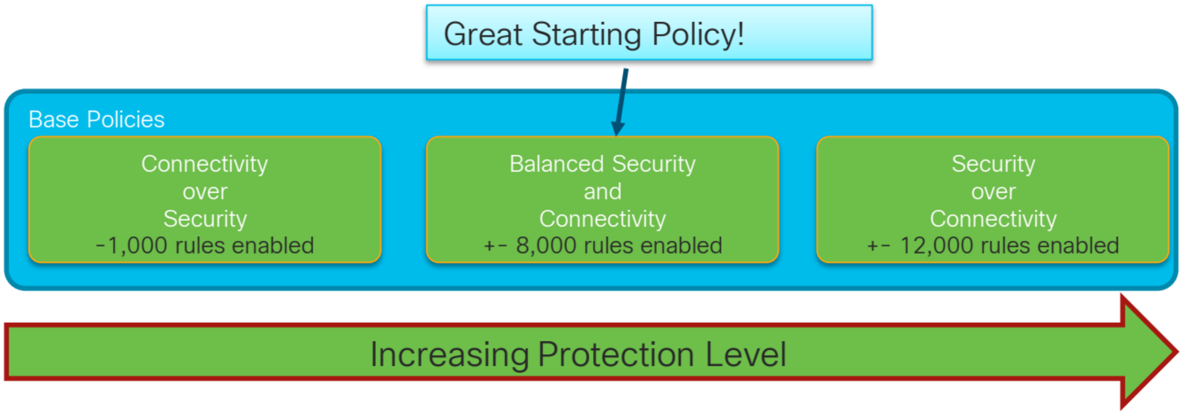


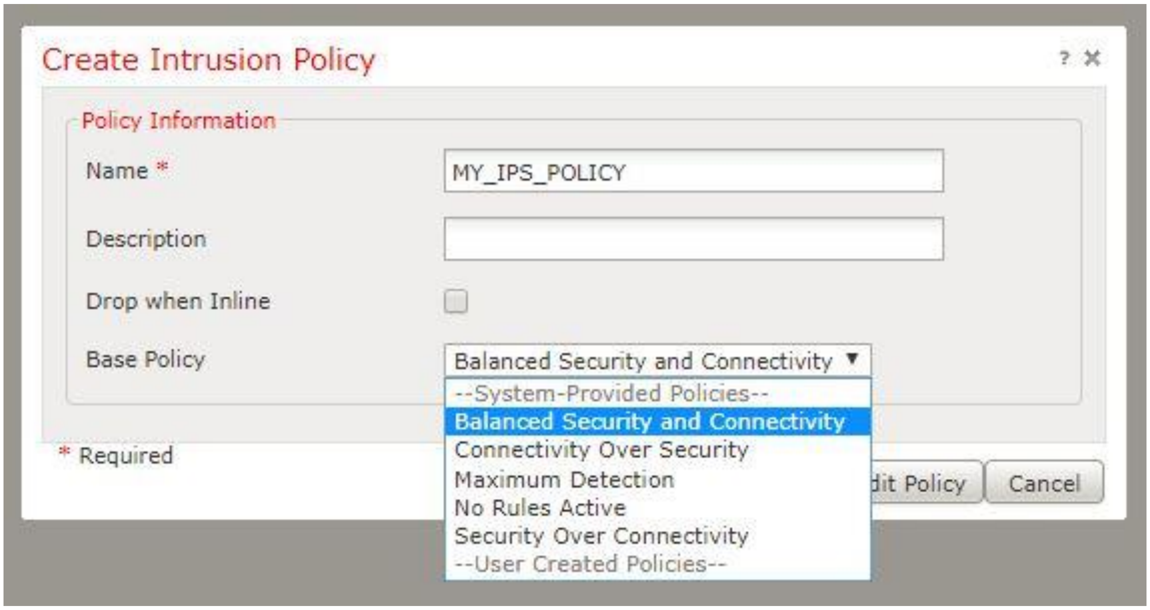
SNORT rules get evaluated here. This is your Intrusion Policy!

Default Policies:

- There are several policies that FMC uses by default, which are regularly updated by Cisco.
- They can be used as a base policy when creating your own policies in the Cisco Firepower.
- You can also create, custom policies are deployed as layers, to create a policy hierarchy.
- These custom policies in Cisco FTD Firepower are policy at the bottom is the Base Layer.

Default Policies	Description
Balanced Security and Connectivity	This policy is designed to balance overall network performance with network infrastructure security and appropriate for most networks.
Connectivity over Security	Used when connectivity is more important. Only the most critical rules are enabled. Select this policy if you want to apply some intrusion protection but you are fairly confident in the security of your network.
Security over Connectivity	When connectivity is the secondary concern. Enables most rules. May result in higher false positives. Enables more signatures & catch more.
Maximum detection	Every rule is turned on & will likely result in false positives. Best to only use this for labs and testing. Provide maximum detection of attacks.
No Rules Active	All rules are disabled. Would generally only be used as a template.


Great Starting Policy!
Base Policies
Connectivity over Security -1,000 rules enabled
Balanced Security and Connectivity +- 8,000 rules enabled
Security over Connectivity +- 12,000 rules enabled
Increasing Protection Level



Create Intrusion Policy

Policy Information

Name * MY_IPS_POLICY

Description

Drop when Inline □

Base Policy: Balanced Security and Connectivity ▼

--System-Provided Policies--
Balanced Security and Connectivity
Connectivity Over Security
Maximum Detection
No Rules Active
Security Over Connectivity
--User Created Policies--
* Required
dit Policy
Cancel

To help you expedite a deployment, Firepower software comes with several preconfigured network analysis policies and intrusion policies. You can use one of the following systems provided policies as the default security policy for your network or as a baseline for a custom security policy

Connectivity Over Security:

This policy is built for organizations where connectivity (being able to get to all resources) takes precedence over network infrastructure security. The intrusion policy enables far fewer rules than those enabled in the Security over Connectivity policy. Only the most critical rules that block traffic are enabled. Select this policy if you want to apply some intrusion protection but you are fairly confident in the security of your network. This policy prioritizes connection speed while maintaining detection of a few critical vulnerabilities.

Balanced Security and Connectivity:

This policy is designed to balance overall network performance with network infrastructure security. This policy is appropriate for most networks. Select this policy for most situations where you want to apply intrusion prevention. Cisco Talos recommends this policy for the best system performance without compromising the detection of the latest critical vulnerabilities.

Security Over Connectivity:

This policy is built for organizations where network infrastructure security takes precedence over user convenience. The intrusion policy enables numerous network anomaly intrusion rules that could alert on or drop legitimate traffic. Select this policy when security is paramount or for traffic that is high risk. Security has higher priority than connection speed and reachability.

Maximum Detection:

This policy is built for organizations where network infrastructure security is given even more emphasis than is given by the Security Over Connectivity policy, with the potential for even greater operational impact. For example, the intrusion policy enables rules in a large number of threat categories including malware, exploit kit, old and common vulnerabilities, and known in-the-wild exploits. If you select this policy, carefully evaluate whether too much legitimate traffic is being dropped. Maximum Detection is not typical for production networks. Security has supreme priority over business continuity.

Variable Sets:

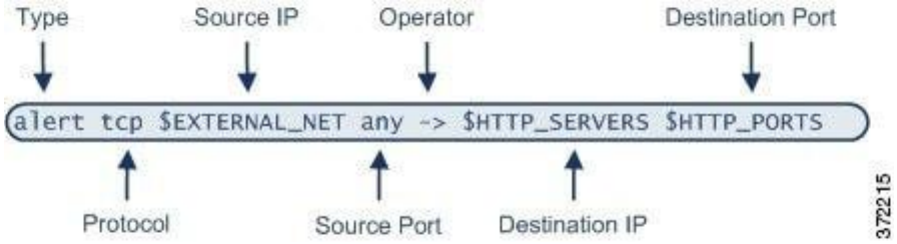
The variable sets represent commonly used values in the intrusion rules to identify source and destination IP addresses and ports. SNORT uses a set of internal variables. These specify details like inside and outside networks, special ports, and so on. The HOME_NET variable in the variable set is the "protected" networks. You can create multiple variable sets to apply to separate intrusion policies. Variables are useful, as values can be set or changed in a global area. This means that there is no need to edit individual SNORT rules. In Firepower, a global list of variables is a Variable Set. FMC comes with a default variable set. It's recommended to change these values to represent your network. You should create your own set and change that, rather than modifying the default set. There are many variables in FMC. Below is a table of the common variables that you should consider changing. If nothing else, change $HOME_NET variable. The Default-Set object is available out of the box. Create a new variable set by clicking the Add Variable Set button.

Variable	Usage	Default Value	Notes
$HOME_NET	Specifies the protected network	any	Add trusted networks in here
$EXTERNAL_NET	Specifies the outside network	any	Add $HOME_NET as an exclusion here
$SIP_SERVERS	Define SIP Servers	HOME_NET	A list of IPs
$SMTP_SERVERS	Define SMTP Servers	HOME_NET	A list of IPs
$SNMP_SERVERS	Define SNMP Servers	HOME_NET	A list of IPs
$SQL_SERVERS	Define SQL Servers	HOME_NET	A list of IPs
$SSH_SERVERS	Define SSH Servers	HOME_NET	A list of IPs
$TELNET_SERVERS	Define Telnet Servers	HOME_NET	A list of IPs
$FTP_PORTS	Ports that FTP runs on	21, 2100, 3535	Only change if non-default ports are needed
$HTTP_PORTS	Ports that HTTP runs on	Many ports	Only change if non-default ports are needed
$ORACLE_PORTS	Ports that Oracle databases run on	any	Only change if non-default ports are needed
$SSH_PORTS	Ports that are used for SSH	22	Only change if non-default ports are needed

To find the Variable sets, navigate to Objects > Object Management. Click Variable Sets at the right, a default Variable Sets named Default-Set is pre-defined, Edit the Default-Set Variable Sets. Notice that the values $HOME_NET and $EXTERNAL_NET. These are variables. SNORT uses these variables to represent the protected and the unprotected networks. It's best practice to change these values to represent your network. You should create your own Variable Set or than modifying the default set. Edit EXTERNAL_NET.

The Intrusion Rule Header:

Every standard text rule and shared object rule has a rule header containing parameters and arguments. The following illustrates parts of a rule header:



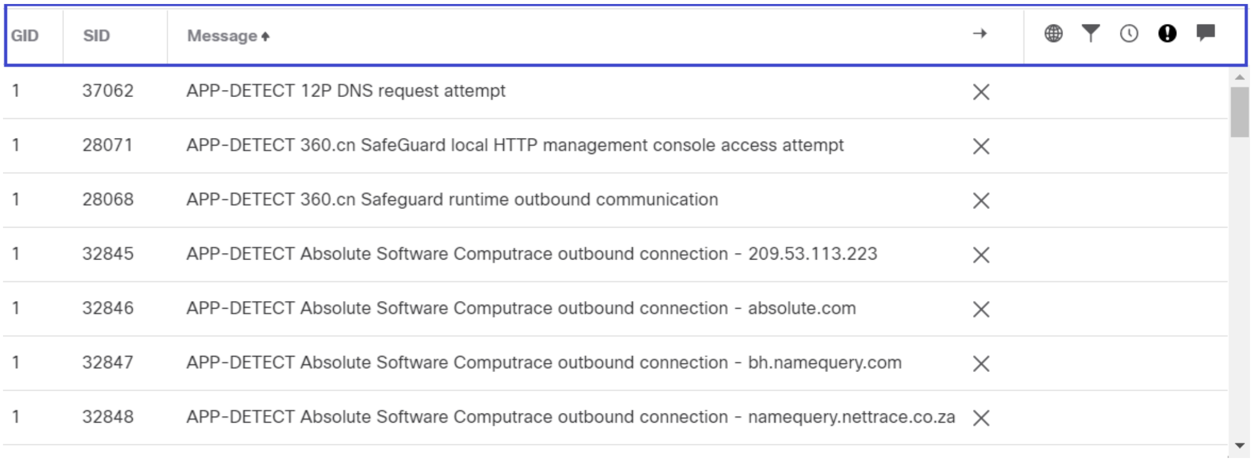
```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
```

Component	Example Value	This Value
Action	alert	Generates an intrusion event when triggered.
Protocol	tcp	Tests TCP traffic only.
Source IP Address	$EXTERNAL_NET	Tests traffic coming from any host that is not on your internal network.
Source Ports	any	Tests traffic coming from any port on the originating host.
Operator	->	Tests external traffic (destined for the web servers on your network).
Destination IP Address	$HTTP_SERVERS	Tests traffic to be delivered to any host specified as a web server on your internal network.
Destination Ports	$HTTP_PORTS	Tests traffic delivered to an HTTP port on your internal network.

Intrusion Rules Page Columns:

The Intrusion Rules page uses the same icons in its menu bar and column headers.

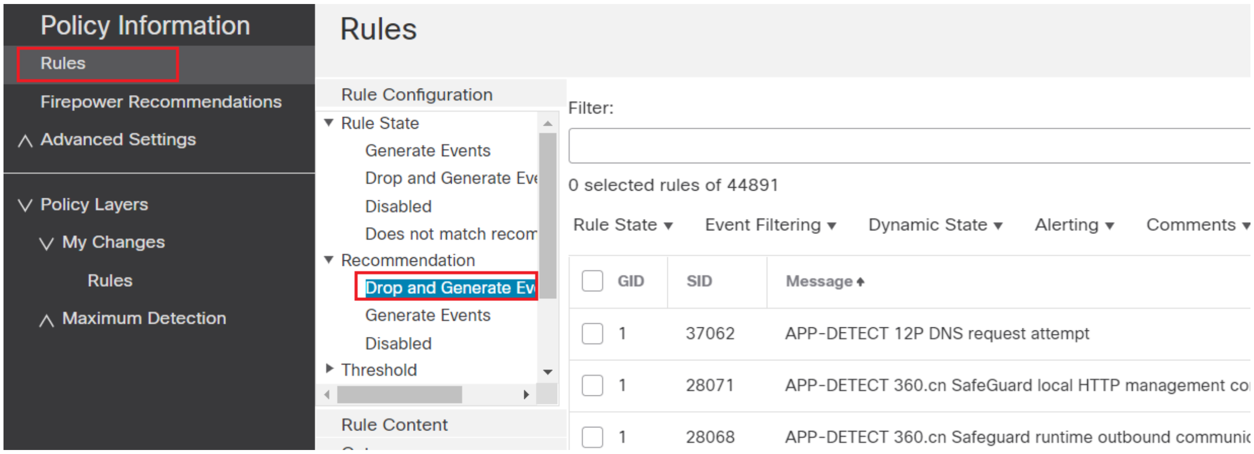
Heading	Description
GID	Integer that indicates the Generator ID (GID) for the rule.
SID	Integer that indicates the Snort ID (SID), which acts a unique identifier for the rule. For custom rules, the SID is 1000000 or higher.
Message	Message included in events generated by this rule, which also acts as the name of the rule.
➡	The rule state for the rule: Drop and generate events (✖) Generate events (➡) Disabled (➡) The icon for a disabled rule is a dimmed version of the icon for a rule that is set to generate events without dropping traffic.
🌐	Firepower recommended rule state for the rule.
▼	Event filter, including event thresholds and event suppression, applied to the rule.
🕒	Dynamic rule state for the rule, which goes into effect if specified rate anomalies occur.
❗	Alerts configured for the rule (currently SNMP alerts only).
💬	Comments added to the rule.



GID	SID	Message ↑	→	🌐	▼	🕒	❗	💬
1	37062	APP-DETECT 12P DNS request attempt	✕					
1	28071	APP-DETECT 360.cn SafeGuard local HTTP management console access attempt	✕					
1	28068	APP-DETECT 360.cn Safeguard runtime outbound communication	✕					
1	32845	APP-DETECT Absolute Software Computrace outbound connection - 209.53.113.223	✕					
1	32846	APP-DETECT Absolute Software Computrace outbound connection - absolute.com	✕					
1	32847	APP-DETECT Absolute Software Computrace outbound connection - bh.namequery.com	✕					
1	32848	APP-DETECT Absolute Software Computrace outbound connection - namequery.nettrace.co.za	✕					

Intrusion Rule Configuration Filters:

You can filter the rules listed in the Rules page by several rule configuration settings. For example, if you want to view the set of rules whose rule state does not match the recommended rule state, you can filter on rule state by selecting Does not match recommendation.

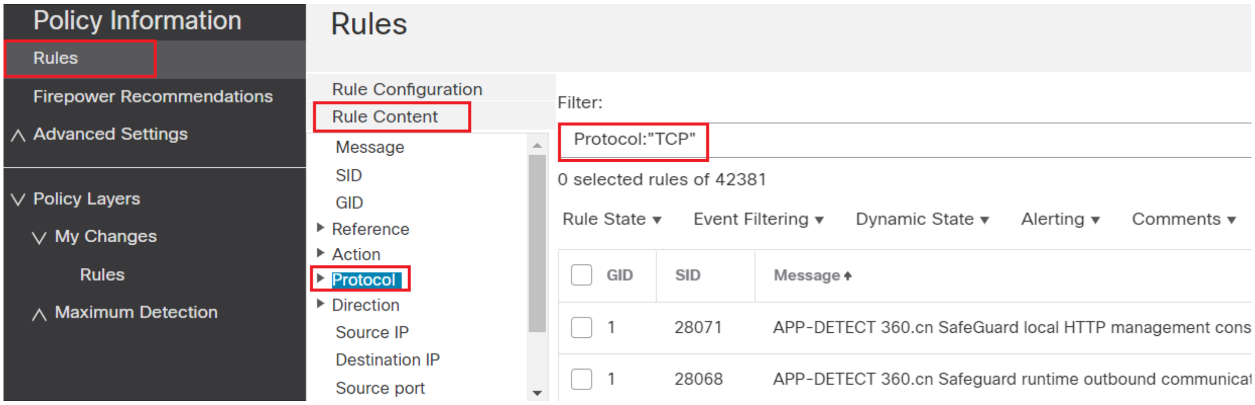


0 selected rules of 44891

□	GID	SID	Message ▲
□	1	37062	APP-DETECT 12P DNS request attempt
□	1	28071	APP-DETECT 360.cn SafeGuard local HTTP management co
□	1	28068	APP-DETECT 360.cn Safeguard runtime outbound communic

Intrusion Rule Content Filters:

You can filter the rules listed in the Rules page by several rule content items. For example, you can quickly retrieve a rule by searching for the rule's SID. You can also find all rules that inspect traffic going to a specific protocol.



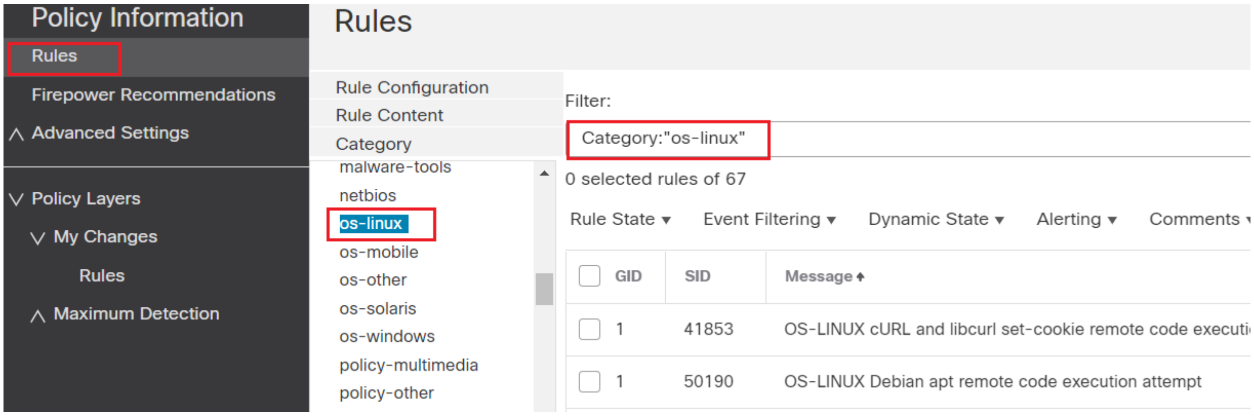
Filter: Protocol:"TCP"

0 selected rules of 42381

□	GID	SID	Message ▲
□	1	28071	APP-DETECT 360.cn SafeGuard local HTTP management cons
□	1	28068	APP-DETECT 360.cn Safeguard runtime outbound communicat

Intrusion Rule Categories:

The Firepower System places rules in categories based on the type of traffic the rule detects. On the Rules page, you can filter by rule category, so you can set a rule attribute for all rules in a category. For example, if you do not have Linux hosts on your network, you could filter by the os-linux category, then disable all the rules showing to disable the entire os-linux category. You can hover your pointer over a category name to display the number of rules in that category.



Filter: Category:"os-linux"

0 selected rules of 67

	GID	SID	Message
□	1	41853	OS-LINUX cURL and libcurl set-cookie remote code executi
□	1	50190	OS-LINUX Debian apt remote code execution attempt

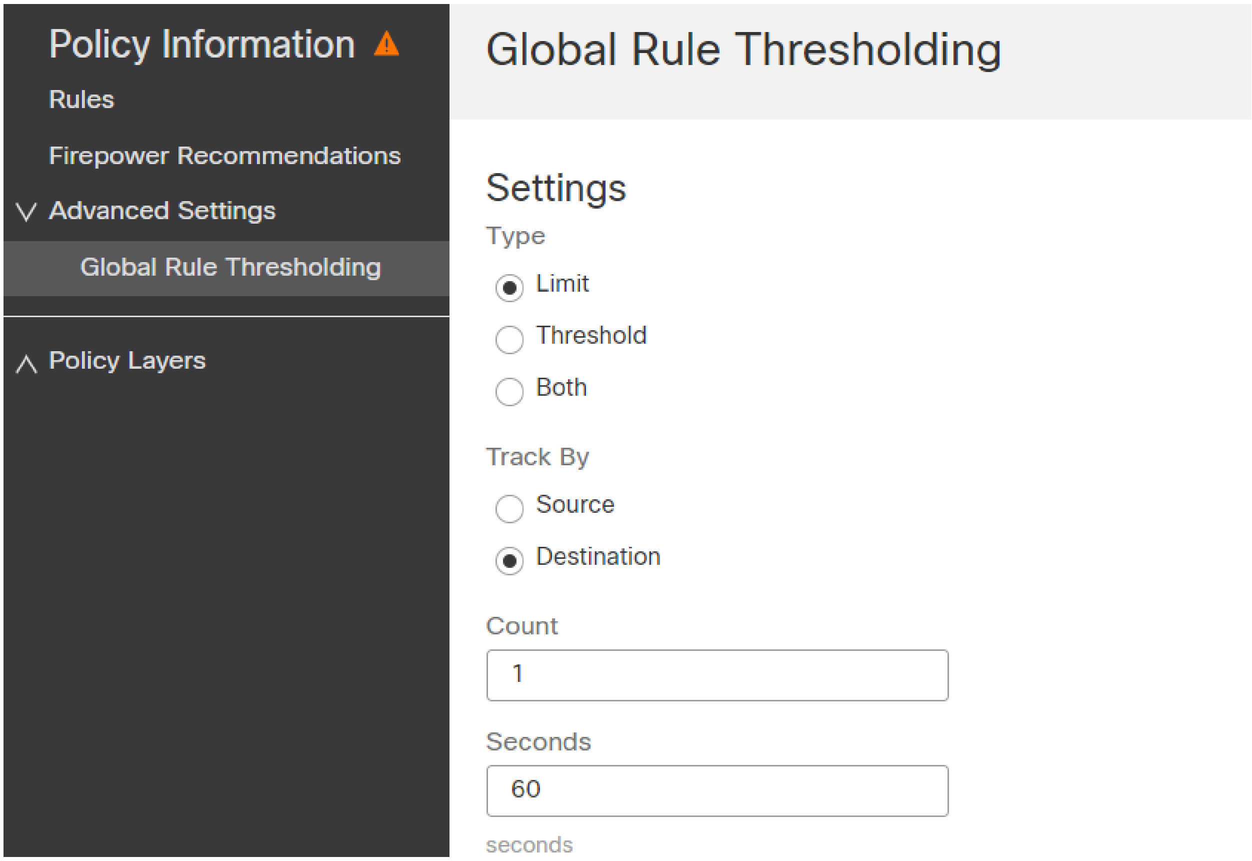
Recommendation Feature:

Use the Firepower Recommendations feature within the intrusion policy. This feature can incorporate the network discovery data to determine the intrusion rules that are related to the operating systems, services, and applications running in a network. Click the Generate and Use Recommendations button. This button appears if FMC did not generate any recommendation before. If a recommendation has already been generated, you will see different buttons, whose labels are self-explanatory, such as Update Recommendations, Do Not Use Recommendations, and so on.

Global Rule Thresholding Options:

The global rule threshold sets limits for event logging by an intrusion policy. You can set a global rule threshold across all traffic to limit how often the policy logs events from a specific source or destination and displays those events per specified time period. You can also set thresholds per shared object rule, standard text rule, or preprocessor rule in the policy. When you set a global threshold, that threshold applies for each rule in the policy that does not have an overriding specific threshold. Thresholds can prevent you from being overwhelmed with a large number of events. Every intrusion policy contains a default global rule threshold that applies by default to all intrusion rules and preprocessor rules. This default threshold limits the number of events on traffic going to a destination to one event per 60 seconds. The default values for global rule thresholding options are:

Type — Limit,
Track By — Destination,
Count — 1
Seconds — 60



Policy Information ⚠

Rules

Firepower Recommendations

∨ Advanced Settings

Global Rule Thresholding

∧ Policy Layers

Global Rule Thresholding

Settings

Type

● Limit

○ Threshold

○ Both

Track By

○ Source

● Destination

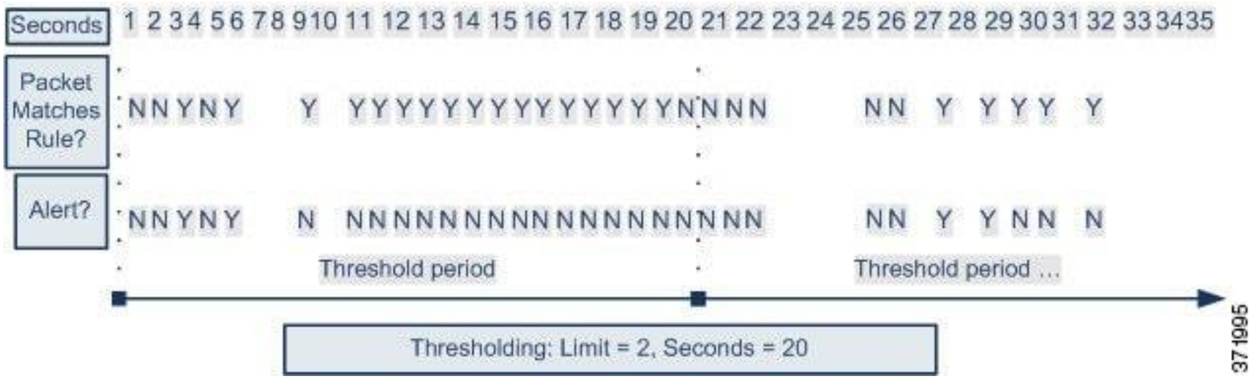
Count

1

Seconds

60

seconds



Advanced Settings:

Specific Threat Detection:

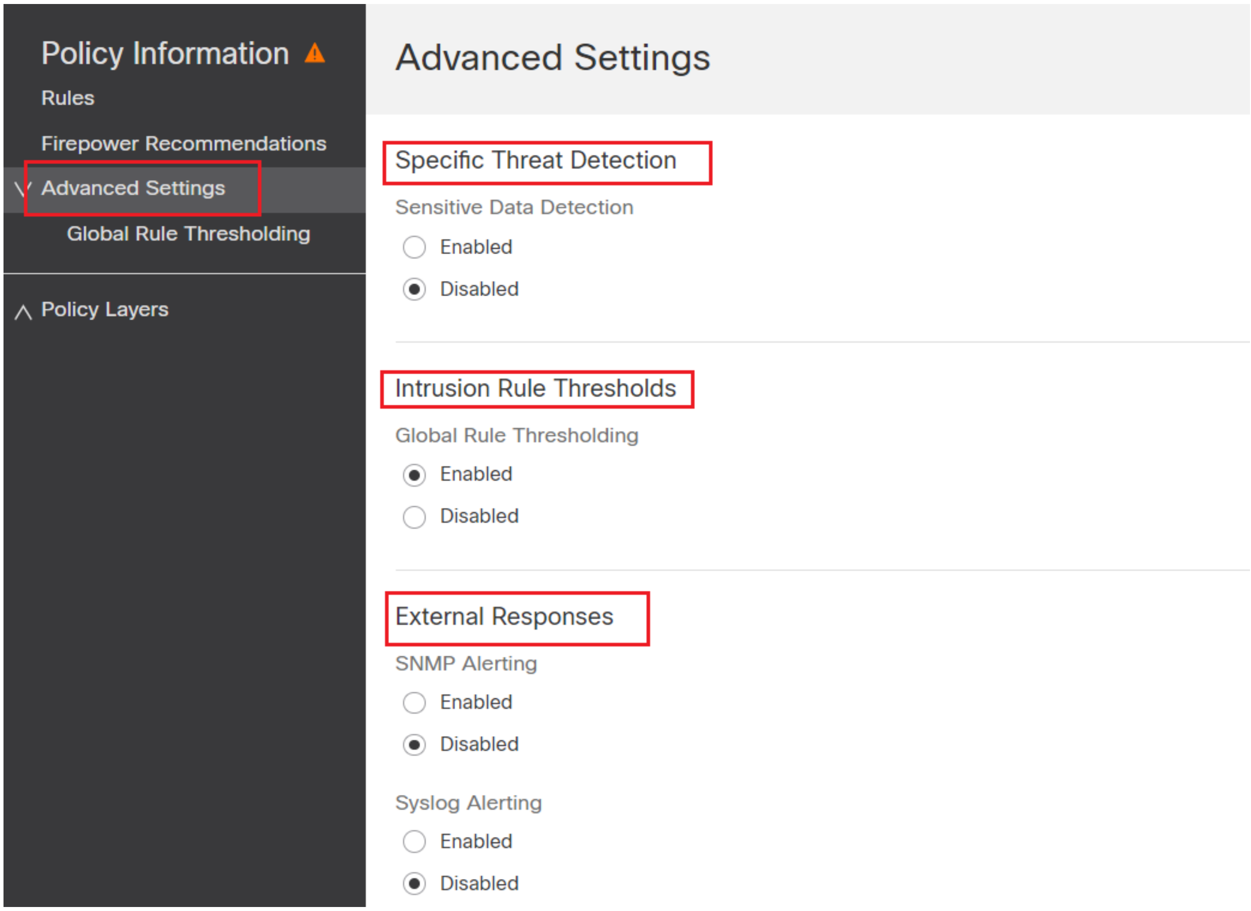
The sensitive data preprocessor detects sensitive data such as credit card numbers and Social Security numbers in ASCII text.

Intrusion Rule Thresholds:

Global rule thresholding can prevent your system from being overwhelmed with a large number of events by allowing you to use thresholds to limit the number of times the system logs and displays intrusion events.

External Responses:

You can enable logging to system log (syslog) facilities or send event data to an SNMP trap server. Per policy, you can specify intrusion event notification limits, set up intrusion event notification to external logging facilities, and configure external responses to intrusion events.



Advanced Settings

Specific Threat Detection

Sensitive Data Detection

○ Enabled

● Disabled

Intrusion Rule Thresholds

Global Rule Thresholding

● Enabled

○ Disabled

External Responses

SNMP Alerting

○ Enabled

● Disabled

Syslog Alerting

○ Enabled

● Disabled