Verify a custom SID list from Firepower sensors using CLI and FMC GUI

Introduction

This document describes how to get a custom SID list from Firepower Threat Defense (FTD) or FirePOWER module using CLI and FMC GUI. SID information can be found on FMC GUI if you navigate to ***Objects > Intrusion Rules***. In some cases, to get a list of available SIDs from the CLI is necessary.

Prerequisites

Requirements

Cisco recommends that you know these topics:

- Cisco Firepower Threat Defense (FTD)
- Cisco ASA with FirePOWER Services
- Cisco Firepower Management Center (FMC)
- Linux basic knowledge

Components Used

The information in this document is based on the following software version:

- Firepower Management Center 6.6.0
- Firepower Threat Defense 6.4.0.9
- FirePOWER module 6.2.3.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

An ***intrusion rule*** is a set of keywords and arguments that the system uses to detect attempts to exploit vulnerabilities on your network. As the system analyzes network traffic, it compares packets against the conditions specified in each rule. If the packet data matches all the conditions specified in a rule, the rule triggers. If a rule is an alert rule, it generates an intrusion event. If it is a pass rule, it ignores the traffic. For a drop rule in an inline deployment, the system drops the packet and generates an event. You can view and evaluate intrusion events from the Firepower Management Center web console.

The Firepower System provides two types of intrusion rules: ***shared object rules*** and ***standard text rules***. The Cisco Talos Security Intelligence and Research Group (Talos) can use shared object rules to detect attacks against vulnerabilities in ways that traditional standard text rules cannot. It is not possible to create shared object rules. When intrusion rules are written on your

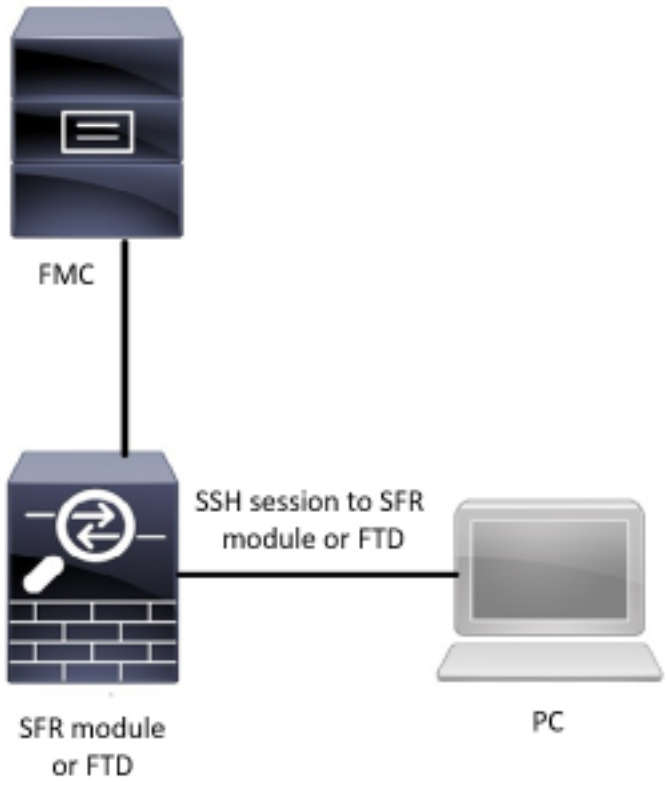
own, standard text rule must be created. Custom standard text rules to tune the types of events you are likely to see. By writing rules and specifying the rule's event message, you can more easily identify traffic that indicates attacks and policy evasions.

When you enable a custom standard text rule in a custom intrusion policy, keep in mind that some rule keywords and arguments require that traffic first be decoded or preprocessed in a certain way.

A ***custom local rule*** on a Firepower System is a custom standard Snort rule that you import in an ASCII text file format from a local machine. A Firepower System allows you to import local rules using the web interface. The steps to import local rules are very straightforward. However, to write an optimal local rule, a user requires in-depth knowledge of Snort and networking protocols.

> **Warning**: Make sure you use a controlled network environment to test any intrusion rules that you write before you use the rules in a production environment. Poorly written intrusion rules may seriously affect the performance of the system

Network Diagram



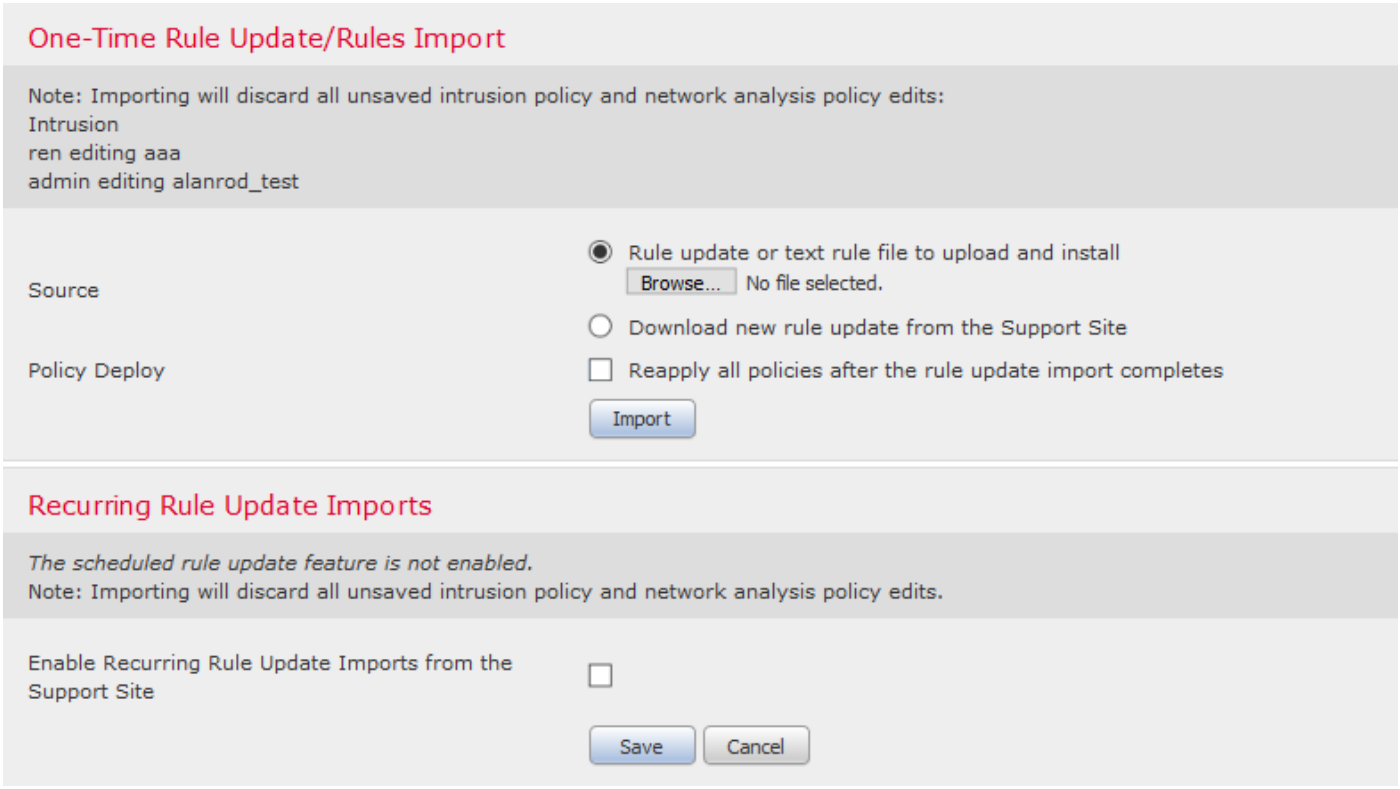
Configure

Import Local Rules

Before you begin, you need to make sure the rules listed on your custom file do not contain any special characters. The rule importer requires all custom rules to be imported using ASCII or UTF-8 encoding. The procedure shown below explains how to import local standard text rules from a local machine.

Step 1. Access the **Import Rules** tab by navigating to **Objects > Intrusion Rules > Import**

Rules. The **Rule Updates** page appears as shown in the image below:



Step 2. Select **Rule update or text rule file to upload and install** and click **Browse** to select the custom rule file

> **Note**: All uploaded rules are saved in the **local rule** category

Step 3. Click **Import**. The rule file is imported

> **Note**: The Firepower Systems do not use the new rule set for inspection. To activate a local rule, you need to enable it in the Intrusion Policy, and then apply the policy.

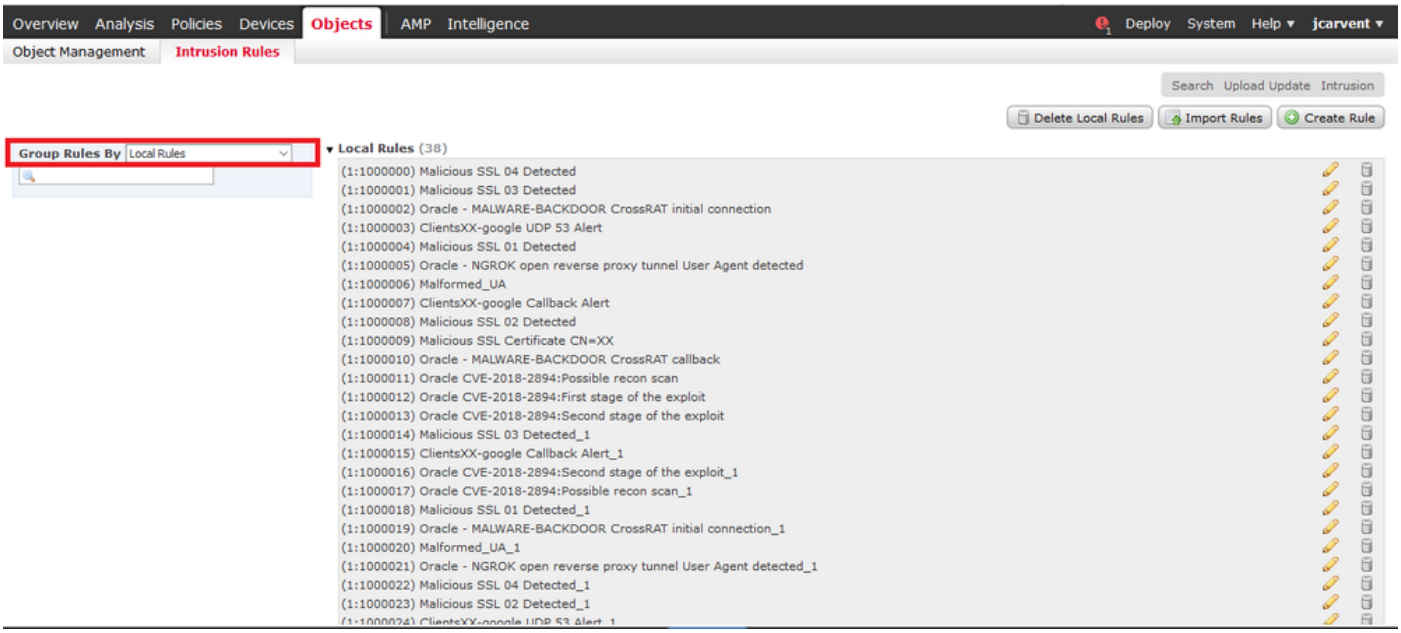
Verify

From FMC GUI

1. View local rules imported from FMC GUI

Step 1. Navigate to **Objects > Intrusion Rules**

Step 2. Select **Local Rules** from **Group Rules**



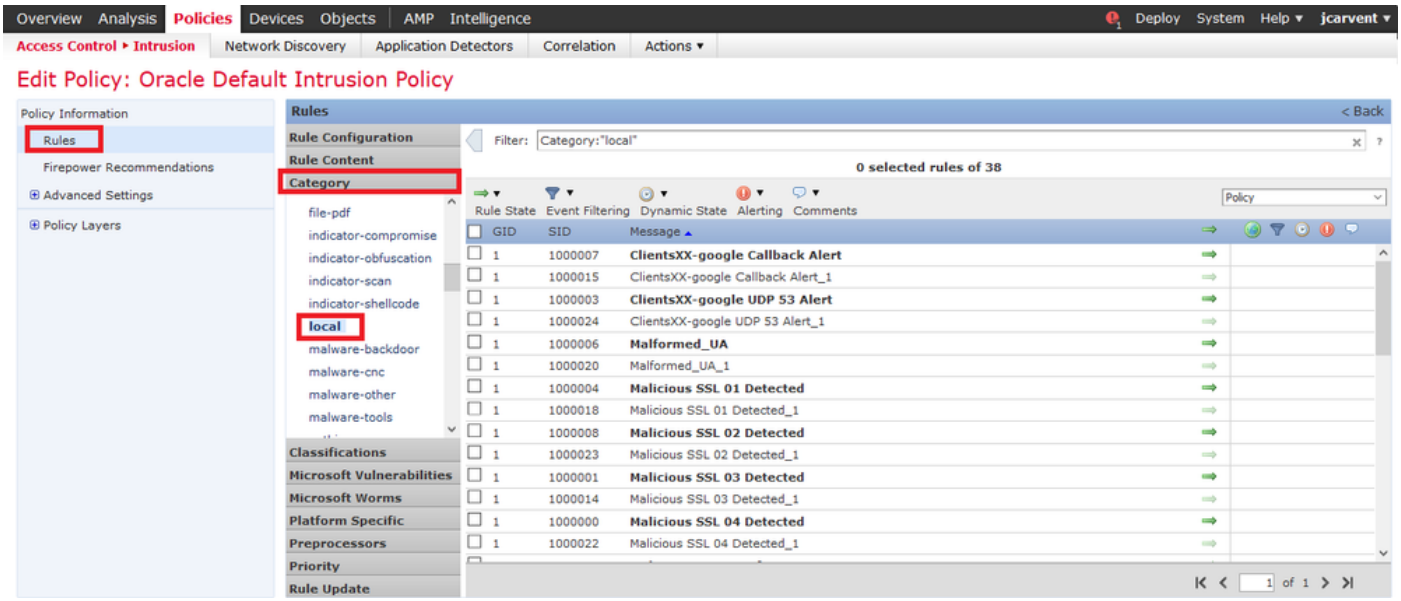
By default, the Firepower System sets the local rules in a disabled state. These local rules must manually set the state of local rules before you can use them in your intrusion policy.

2. Enable a local rule from Intrusion Policy

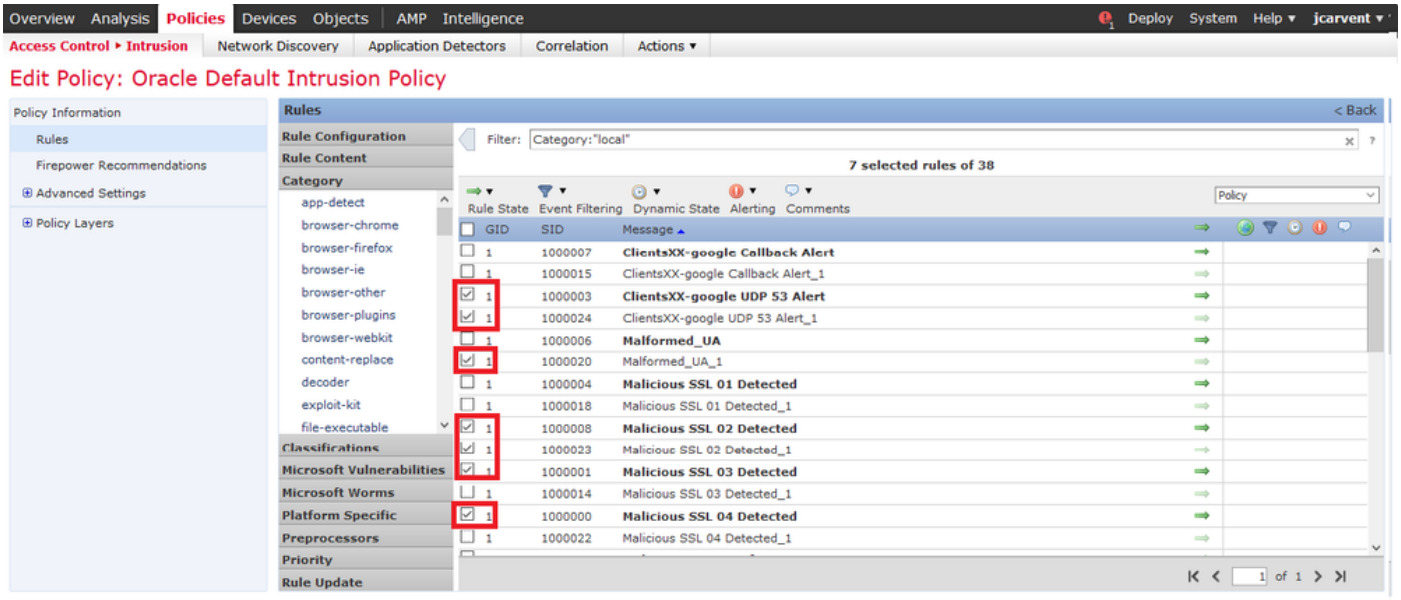
Step 1. Navigate to Policy Editor page under **Policies** > **Intrusion** > **Intrusion Policy**

Step 2. Select **Rules** in the left panel

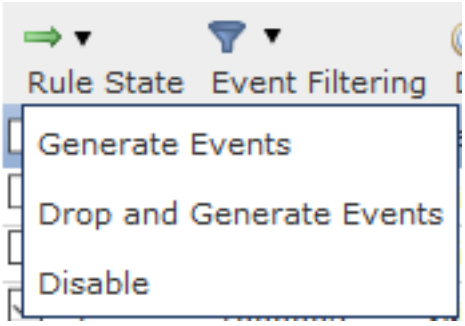
Step 3. Under the **Category**, select **local.** All of the local rules should appear if available:



Step 4. Select the desired local rules:



Step 5. After selecting the desired local rules, select a state from **Rule State**



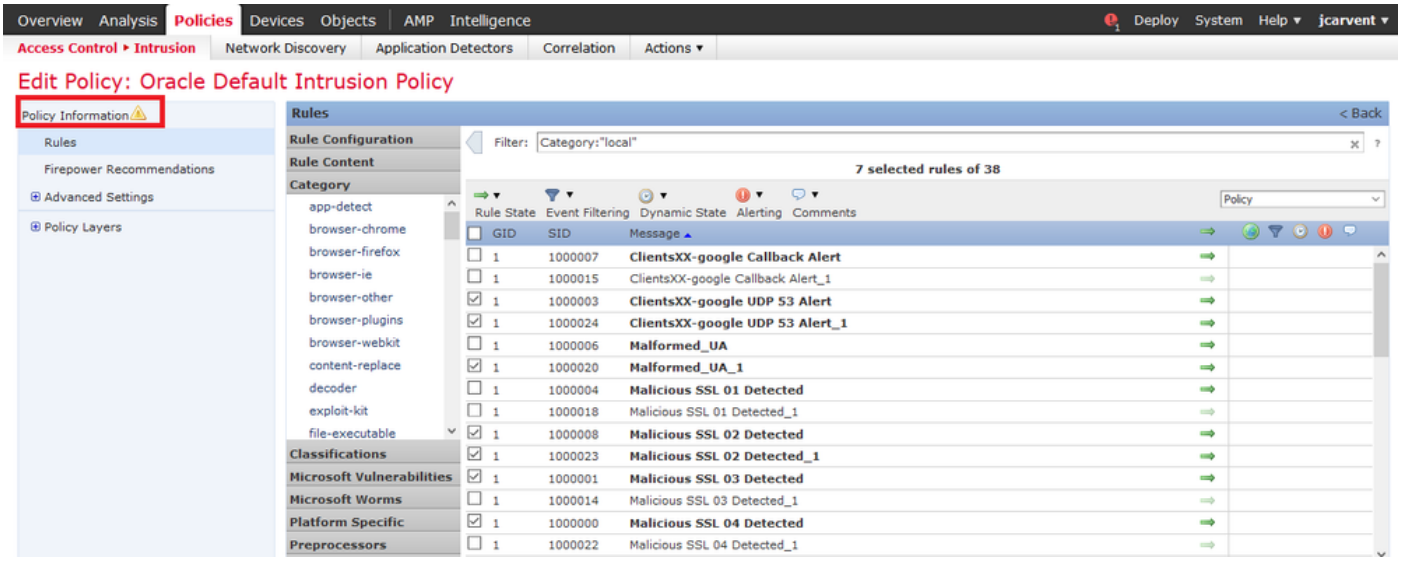
The following options are available:

- Generate Events: Enable the rule and generate an event

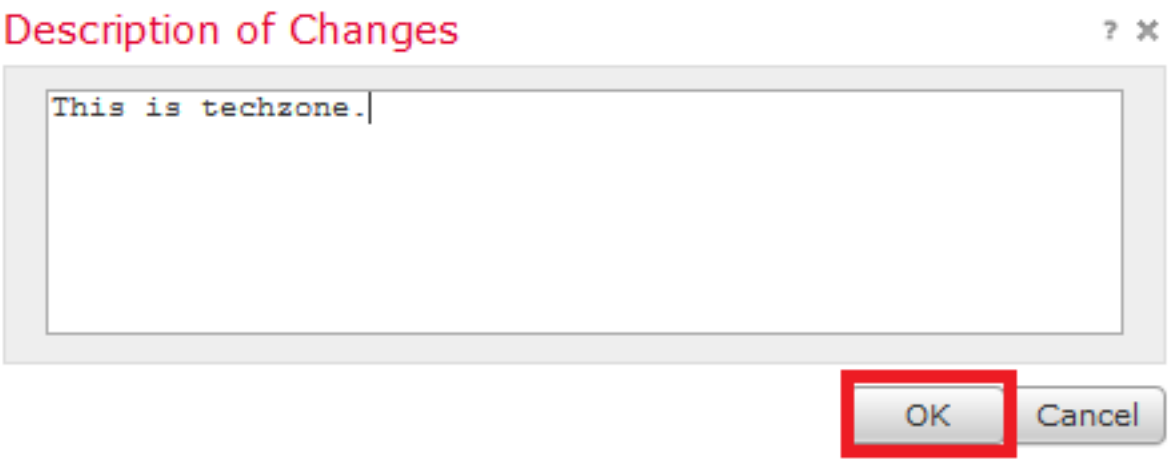
- Drop and Generate Events: Enable the rule, drop the traffic, and generate an event

- Disable: No enable the rule, no events

Step 6. Once the rule state is selected, click on the **Policy Information option on the left panel**



Step 7. Select the **Commit Changes** button and provide a brief description of changes. Click on **OK** later. The Intrusion Policy is validated.



> **Note**: The policy validation fails if you enable an imported local rule that uses the deprecated threshold keyword in combination with the intrusion event thresholding feature in an intrusion policy.

Step 8. Deploy the changes

From FTD or SFR module CLI

1. View the local rules imported from FTD or SFR module CLI

Step 1. Establish an SSH or CLI session from your SFR module or FTD

Step 2. Navigate to expert mode

```
> expert
admin@firepower:~$
```

Step 3. Get administrator privileges

```
admin@firepower:~$ sudo su -
```

Step 4. Type your password

```
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
```

Step 5. Navigate to **/ngfw/var/sf/detection_engines/UUID/intrusion/**

```
root@firepower:/home/admin# cd /ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-
2369c038cbc9/intrusion/
root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
```

> **Note**: If you are using SFR module, do not use /ngfw/var/sf/detection_engines/*/intrusion path. Insted use **/var/sf/detection_engines/*/intrusion**

Step 6. Introduce the following command

```
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
```

Refer to the image below as a working example:

```
root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
sid:1000008
sid:1000023
sid:1000007
sid:1000035
sid:1000004
sid:1000000
...
```

This will list the customer SID list that is enabled by the FTD or SFR module.

Troubleshoot

Step 1. Make sure SSH session is established to SFR module or FTD, from FMC detection_engines is not listed

Step 2. The command grep -Eo "sid:*([0-9]{1,8})" */*local.rules only will work under intrusion directory, the command cannot be used from another directory

Step 3. Use the command grep -Eo "sid:*([0-9]{1,8})" */*.rules in order to get a complete SID list from all categories

Best Practices for Importing Local Intrusion Rules

Observe the guidelines when importing a local rule file:

- The rules importer requires that all custom rules are imported in a plain text file encoded in ASCII or UTF-8
- The text file name can include alphanumeric characters, spaces, and no special characters other than underscore (_), period (.), and dash (-)
- The system imports local rules preceded with a single pound character (#), but they are flagged as deleted
- The system imports local rules preceded with a single pound character (#) and does not import local rules preceded with two-pound characters (##)
- Rules cannot contain any escape characters
- You do not have to specify a Generator ID (GID) when importing a local rule. If you do, specify only GID 1 for a standard text rule
- When importing a rule for the first time, do *not* specify a Snort ID (SID) or revision number. This avoids collisions with SIDs of other rules, including deleted rules. The system will automatically assign the rule the next available custom rule SID of 1000000 or greater, and a revision number of 1
- If you must import rules with SIDs, the SIDs must be unique numbers between 1,000,000 and 9,999,999

- In a multidomain deployment, the system assigns SIDs to imported rules from a shared pool used by all domains on the Firepower Management Center. If multiple administrators are importing local rules at the same time, SIDs within an individual domain might appear to be non-sequential, because the system assigned the intervening numbers in the sequence to another domain
- When importing an updated version of a local rule you have previously imported, or when reinstating a local rule you have deleted, you ***must*** include the SID assigned by the system and a revision number greater than the current revision number. You can determine the revision number for a current or deleted rule by editing the rule

  Note: The system automatically increments the revision number when you delete a local rule; this is a device that allows you to reinstate local rules. All deleted local rules are moved from the local rule category to the deleted rule category.

- Import local rules on the primary Firepower Management Center in a high availability pair to avoid SID numbering issues
- The import fails if a rule contains any of the following:A SID is greater than 2147483647A list of source or destination ports that is longer than 64 characters
- Policy validation fails if you enable an imported local rule that uses the deprecated ***threshold*** keyword in combination with the intrusion event thresholding feature in an intrusion policy
- All imported local rules are automatically saved in the local rule category
- The system always sets local rules that you import to the disabled rule state. You must manually set the state of local rules before you can use them in your intrusion policy

Related Information

Here are some documents for reference related to snort SID:

Update Intrusion Rules

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/System_Software_Updates.html#ID-2259-00000356

The Intrusion Rules Editor

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/the_intrusion_rules_editor.html