

# How to Determine Traffic Handled by a Specific Snort Instance

## Contents

[Introduction](#)  
[Prerequisites](#)  
[Requirements](#)  
[Components Used](#)  
[Configure](#)  
[Configurations](#)  
[Verify](#)  
[Troubleshoot](#)

## Introduction

This document describes how to determine the traffic that is being handled by a specific snort instance. This detail is very useful while troubleshooting high CPU utilization on a specific snort instance.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of Firepower Technology

### Components Used

The information in this document is based on these software and hardware versions:

- Firepower Management Center 6.X and above
- Applicable to all managed devices which include Firepower Threat Defense, Firepower Modules, and Firepower Sensors

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, make sure that you understand the potential impact of any command.

## Configure

### Configurations

Login to the Firepower Management Center with administration privileges.

Once the login is successful, navigate to **Analysis > Search**, as shown in the image:

The screenshot shows the Firepower Management Center's Analysis > Search interface. The top navigation bar includes Overview, Analysis (which is selected), Policies, Devices, Objects, AMP, and Intelligence, along with Deploy and a checkmark icon. Below the navigation is a toolbar with Context Explorer, Connections, Intrusions, Files, Hosts, Users, Vulnerabilities, Correlation, Custom, Lookup, and a Save/Save As New/Search button. On the left, a sidebar titled 'Sections' lists General Information, Networking, Geolocation, Device, SSL, Application, URL, Netflow, and QoS. Under 'Device', the 'Device' section is selected, showing fields for Device\*, Ingress Interface, Egress Interface, and Ingress / Egress Interface, all set to 's1p1'. The 'SSL' section contains fields for SSL, SSL Status, SSL Flow Error, SSL Actual Action, SSL Expected Action, SSL Failure Reason, SSL Certificate Status, SSL Version, SSL Cipher Suite, SSL Policy, SSL Rule, SSL Session ID, SSL Ticket ID, SSL Flow Flags, SSL Flow Messages, SSL Certificate Fingerprint, and SSL Subject Common Name, with values like 'yes, no', 'Decrypt, Success, Block, Failure', and 'SSLv3.0, TLS'. A 'Device' dropdown at the top left is set to 'Connection Events'. The main search area is titled '(unnamed search)' with a 'Private' checkbox, 'Save', 'Save As New', and 'Search' buttons. The search results table is currently empty.

Ensure that the **Connection Events** table is chosen from the drop down and then select the **Device** from the section. Enter values for the Device field and Snort Instance ID (0 to N, the number of snort instances depend on the managed device), as shown in the image:

This screenshot shows the same interface as the previous one, but with different search criteria. The 'Device' dropdown is now set to 'Connection Events'. In the 'Device' section of the search form, the 'Device\*' field is set to 'FTD', and the 'Snort Instance ID' field is set to '2'. The rest of the interface remains the same, including the sidebar sections and the search results table.

Once the values are entered, click **Search** and the result would be connection events that are triggered by the specific snort instance.

**Note:** If managed device is Firepower Threat Defense, you can determine the snort instances using FTD CLISH mode.

```
> show asp inspect-dp snort
SNORT Inspect Instance Status Info Id Pid Cpu-Usage Conns Segs/Pkts Status tot (usr | sys) -- --
--- ----- ----- ----- 0 5266 0% ( 0%| 0%) 0 0 READY 1 5268 0% ( 0%| 0%) 0 0 READY
0%| 0%) 0 0 READY 2 5267 0% ( 0%| 0%) 0 0 READY 3 5270 0% ( 0%| 0%) 0 0 READY 4 5269 0% ( 0%|
0%) 0 0 READY
```

**Note:** If the managed device is Firepower Module or Firepower Sensor, you can determine the snort instances using the expert mode and Linux based **top** command.

```
admin@firepower:~$ top
PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+   COMMAND
5247 root      20   0 15248 1272  932 S    0  0.0    0:03.05 top
5264 root      1  -19 1685m 461m 17m S    0  2.9    1:05.26 snort
```

## Verify

There is currently no verification procedure available for this configuration.

## Troubleshoot

There is currently no specific troubleshooting information available for this configuration.