

Use Packet Capture Procedures on Firepower Device

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Steps to Capture Packets](#)

[Copy a Pcap File](#)

Introduction

This document describes how to use the **tcpdump** command in order to capture packets that are seen by a network interface of your Firepower device.

Prerequisites


Requirements

Cisco recommends that you have knowledge of the Cisco Firepower device and the virtual device models.

Components Used

This document is not restricted to specific software and hardware versions. It uses Berkeley Packet Filter (BPF) syntax.

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.

 **Warning:** If you run **tcpdump** command on a production system, it can impact network performance.

Steps to Capture Packets

Log in to the CLI of your Firepower device.

In versions 6.1 and later, enter **capture-traffic**. For example,

```
<#root>
```

```
> capture-traffic
```

Please choose domain to capture traffic from:
0 - eth0
1 - Default Inline Set (Interfaces s2p1, s2p2)

In versions 6.0.x.x and earlier, enter **system support capture-traffic**. For example,

```
<#root>
```


```
> system support capture-traffic
```

Please choose domain to capture traffic from:
0 - eth0
1 - Default Inline Set (Interfaces s2p1, s2p2)

After you make a selection, you are prompted for options:

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:


In order to capture sufficient data from the packets, it is necessary to use the **-s** option in order to set the snaplength correctly. The snaplength can be set to a value that matches the configured maximum transmission unit (MTU) value of the Interface Set configuration, which defaults to 1518.

 **Warning:** When you capture traffic to the screen, it can degrade the performance of system and network. Cisco recommends that you use the **-w <filename>** option with **tcpdump** command. It captures the packets to a file. If you run the command without the **-w** option, press the **Ctrl-C** key combination in order to exit.

Example of **-w <filename>** option:

```
<#root>
```

```
-w capture.pcap -s 1518
```

 **Caution:** Do not use any path elements when you specify the packet capture (pcap) filename. You must specify only the pcap filename to be created in the appliance.

If it is desirable to capture a limited number of packets, you can use the **-c <packets> flag** in order to specify the number of packets to capture. For example, in order to capture exactly 5000 packets:

```
<#root>
```

```
-w capture.pcap -s 1518 -c 5000
```

Additionally, a BPF filter can be added at the end of the command in order to limit which packets are captured. For example, in order to limit the packet capture to 5000 packets with a source or destination IP address of 192.0.2.1, you could use these options:

```
<#root>
```

```
-w capture.pcap -s 1518 -c 5000 host 192.0.2.1
```

When you capture traffic that is virtual LAN (VLAN) tagged, you must specify the VLAN with the BPF syntax. Otherwise, the pcap does not contain any of the VLAN tagged packets. For example, this example limits the capture to traffic that is VLAN tagged from 192.0.2.1:


```
<#root>
```

```
-w capture.pcap -s 1518 -c 5000 vlan and host 192.0.2.1
```

If you are unsure if traffic is VLAN tagged, this syntax could be used in order to capture traffic from 192.0.2.1 which is and is not VLAN tagged:

```
<#root>
```

```
-w capture.pcap -s 1518 -c 5000 'host 192.0.2.1 or (vlan and host 192.0.2.1)'
```

 **Note:** In the previous example, the parentheses are needed so that the or does not only apply to vlan. The single quotes are then needed in order to prevent any possible misinterpretation of the parentheses by the shell.

Specification of a VLAN tag captures all VLAN traffic that matches the rest of your BPF. However, if you want to capture a specific VLAN tag, you can specify which VLAN tag you would like to capture like so:

```
<#root>
```

```
-w capture.pcap -s 1518 -c 5000 vlan 1 and host 192.0.2.1
```

After you specify the desired options and press **Enter**, tcpdump begins to capture traffic.

 **Tip:** If the -c option was not used, press the **Ctrl-C** key combination in order to stop the capture.

Once you stop the capture, you receive confirmation. For example:

```
<#root>
```

```
Please specify tcpdump options desired.
```

(or enter '?' for a list of supported options)

Options:

```
-w capture.pcap -s 1518 -c 5000 host 192.0.2.1
```

Cleaning up.

Done.


Copy a Pcap File

In order to copy a pcap file from a FirePOWER appliance to another system which accepts inbound SSH connections, use this command:

```
<#root>
```

```
> system file secure-copy hostname username destination_directory pcap_file
```

After you press **Enter**, you are prompted for the password to the remote system. The file can be copied across the network.

 **Note:** In this example, the hostname refers to the name or IP address of the target remote host, the username specifies the name of the user on the remote host, the destination_directory specifies the destination path on the remote host, and the pcap_file specifies the local pcap file for transfer.
