Collect Expressway Packet Captures from the CLI

Contents

Introduction

This document describes how to collect a packet capture from the CLI of an Expressway or Video Communication Server (VCS) with the Tcpdump feature.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Expressway or Cisco VCS
- Tcpdump

Components Used

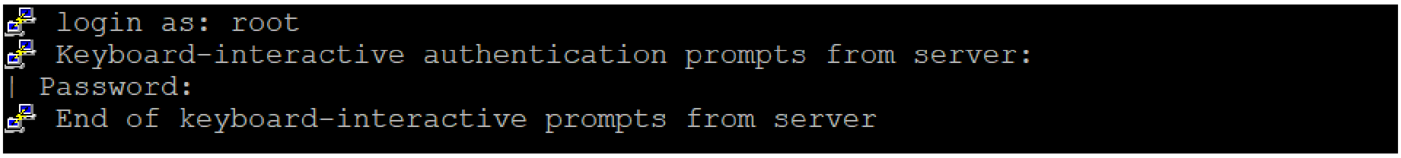
This document is not restricted to specific software and hardware versions.

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.

Packet Capture Process

Verify Disk Space Usage and Capture Location

1. Log in to the Expressway CLI with the root user and associated password.



```
login as: root
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
```

Expressway Root Login

2. Use the command to verify the disk space usage to ensure there is sufficient space for the packet capture to be stored.

```
df /mnt/harddisk
```

3. Create a new directory for the capture to be stored with the command.

```
mkdir /mnt/harddisk/capture
```

4. Navigate to the newly created directory.

```
cd /mnt/harddisk/capture
```

Capture Options

The packet capture can be configured using the Tcpdump feature with various options. The command captures packets on any interface and writes to a file named Newcapture. You can specify any desired file name and options.

```
tcpdump -i any -w Newcapture
```

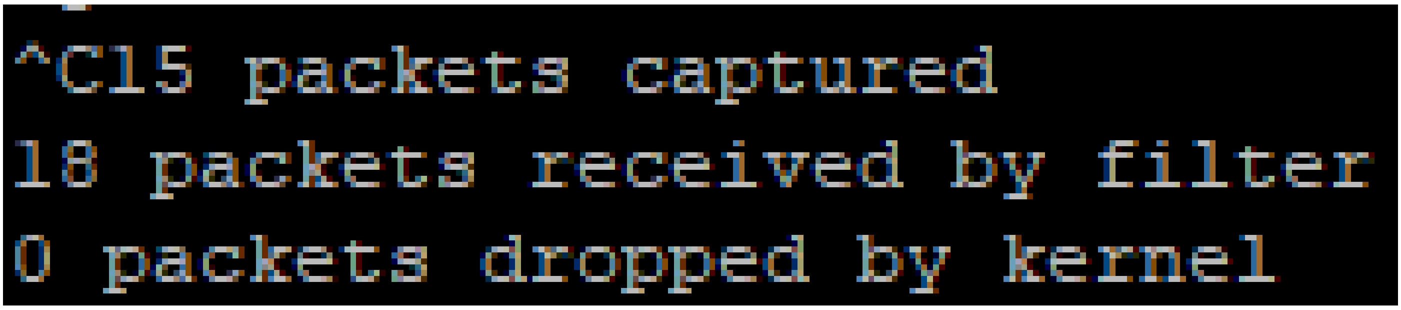
Additional options are described in the Tcpdump Manpage.

Start and Collect the Capture

1. Start a new packet capture using the command. The options used in the command captures packets on the Ethernet 0 interface, showing the full packet, and writing to a file named Newcapture.

```
tcpdump -i eth0 -s 0 -w Newcapture
```

2. Once the desired packets have been captured, stop the capture by pressing the Control button plus the C button at the same time on the keyboard.



```
^C15 packets captured
18 packets received by filter
0 packets dropped by kernel
```

Expressway Command Line

3. Use a Secure File Transfer Protocol (SFTP) client to transfer the file from the capture directory to the local computer.

4. Remove the newly created directory and packet capture file with the command.

```
rm -r /mnt/harddisk/capture
```

Related Information

- Tcpdump Manpage