Prime Infrastructure Packet Capture Procedures

Document ID: 118840

Contributed by Ram Krishnamoorthy, Cisco TAC Engineer.
Mar 16, 2015

Contents

Introduction

This document describes the use of the ***tcpdump*** CLI command in order to capture the desired packets from a Cisco Prime Infrastructure (PI) server.

Use the tcpdump Command

This section provides examples that illustrate the way in which the ***tcpdump*** command is used.

```
nms-pi/admin# tech dumptcp ?
  <0-3>  Gigabit Ethernet interface number
```

The output of the ***show interface*** command provides precise information about the interface name and number that is currently in use.

```
nms-pi/admin# tech dumptcp 0 ?
count Specify a max package count, default is continuous (no limit)
<cr> Carriage return.
```

Note: You can can indicate the specific package count in the previous command. If you do not indicate a specific package count, a continuous capture is run with no limit.

```
nms-pi/admin# tech dumptcp 0 | ?
 Output modifier commands:
 begin Begin with line that matches
 count Count the number of lines in the output
 end End with line that matches
 exclude Exclude lines that match
 include Include lines that match
 last Display last few lines of the output

nms-pi/admin# tech dumptcp 0 > test-capture.pcap
```

Note: It is easiest to save the file, and then review it. In this example, the server saves the file in the root of the directory structure. In order to view the files, enter the ***dir*** command.

Copy the Captured Files to an Outside Location

Here are two examples that illustrate the manner in which captured files are copied to a location that is outside of the server:

- In this example, the capture file is copied to an FTP server with an IP address of ***1.2.3.4***:

  ```
  copy disk:/test-capture.pcap ftp://1.2.3.4/
  ```
- In this example, the capture file is copied to a TFTP server with an IP address ***5.6.7.8***:

  ```
  copy disk:/test-capture.pcap tftp://5.6.7.8/
  ```

Capture Packets as a Root User

If you desire more granular captures, log into the CLI as a *root* user after you have logged in as an *admin* user.

```
test$ ssh admin@12.13.14.15
Password:
nms-pi/admin#
nms-pi/admin# root
Enter root password :
Starting root bash shell ...
ade # su -
[root@nms-pi~]#
```

Example Root User Captures

Here are three examples of captures that are taken by a root user:

- In this example, all of the packets that are destined to port ***162*** on the PI server are captured:

  ```
  [root@nms-pi~]# tcpdump -i eth0 -s0 -n dst port 162
  ```
- In this example, all of the packets that are destined to port ***9991*** are captured and written to a file called ***test.pcap*** in the ***/localdisk/ftp/*** directory:

  ```
  [root@nms-pi~]# tcpdump -w /localdisk/ftp/test.pcap -s0 -n dst port 9991
  ```
- In this example, any packets with a source IP address of ***1.1.1.1*** are captured:

  ```
  [root@nms-pi~]# tcpdump -n src host 1.1.1.1
  ```

Updated: Mar 16, 2015 Document ID: 118840