Contents

Introduction

This document describes how packet captures can be taken from the Jabber Guest Server.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- The Jabber Guest must have access to Internet to download the package.
- WinSCP software installed on the PC to collect the captures.

Components Used

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

- Jabber Guest versions 10.5 and 10.6
- WinSCP software

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.

Problem: How Packet Captures can be taken from Jabber Guest Server?

Solution

Step 1.

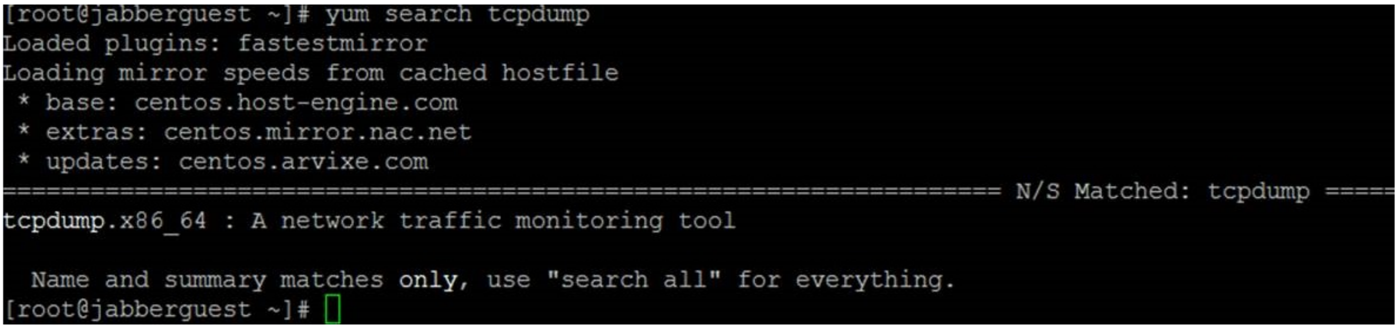
The Jabber Guest server must have access to Internet, for it to download the package from the Internet. In case a web proxy is used, follow the procedure to allow CentOS on Jabber Guest to use the web proxy to download the package.

Refer to the link https://www.centos.org/docs/5/html/yum/sn-yum-proxy-server.html to follow the procedure.

After making sure that the Jabber Guest Server can download the package, proceed to Step 2.

Step 2.

Log in to the Jabber Guest server using Secure Socket Host (SSH) root credentials and run the **yum search tcpdump** command to find the latest version of tcpdump.

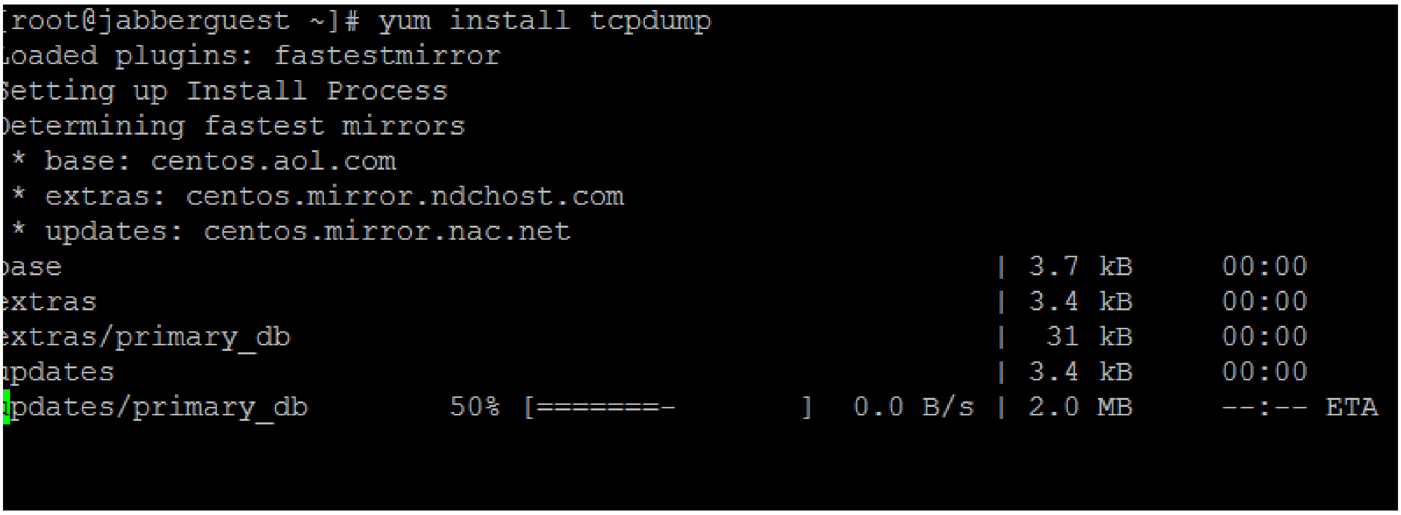


```
[root@jabberguest ~]# yum search tcpdump
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: centos.host-engine.com
 * extras: centos.mirror.nac.net
 * updates: centos.arvixe.com
==================================================================== N/S Matched: tcpdump =====
tcpdump.x86_64 : A network traffic monitoring tool

  Name and summary matches only, use "search all" for everything.
[root@jabberguest ~]# 
```

Step 3.

Run the **yum install tcpdump** command to install the tcpdump package on the Jabber Guest Server.



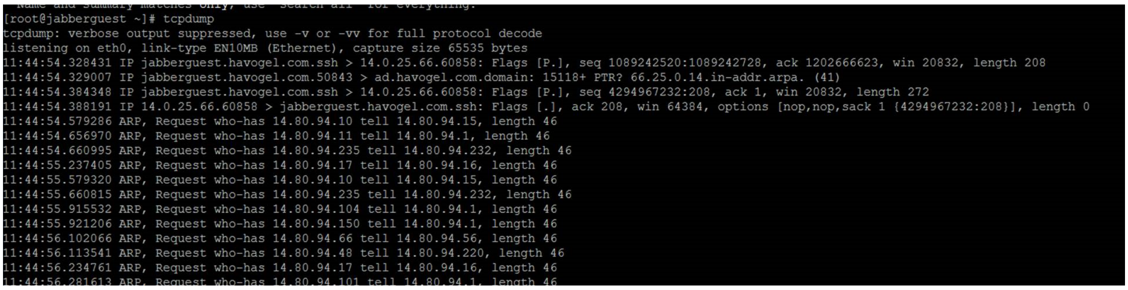
```
[root@jabberguest ~]# yum install tcpdump
Loaded plugins: fastestmirror
Setting up Install Process
Determining fastest mirrors
 * base: centos.aol.com
 * extras: centos.mirror.ndchost.com
 * updates: centos.mirror.nac.net
base                                                         | 3.7 kB     00:00
extras                                                       | 3.4 kB     00:00
extras/primary_db                                            |  31 kB     00:00
updates                                                      | 3.4 kB     00:00
updates/primary_db          50% [=======-        ]  0.0 B/s | 2.0 MB     --:-- ETA
```

Step 4.

You are sent through several prompts. Enter **y** on every component to verify each prompt.

Step 5.

Tcpdump is now available again for packet captures from the Jabber Guest Server.



```
  Name and summary matches only, use "search all" for everything.
[root@jabberguest ~]# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
11:44:54.328431 IP jabberguest.havogel.com.ssh > 14.0.25.66.60858: Flags [P.], seq 1089242520:1089242728, ack 1202666623, win 20832, length 208
11:44:54.329007 IP jabberguest.havogel.com.50843 > ad.havogel.com.domain: 15118+ PTR? 66.25.0.14.in-addr.arpa. (41)
11:44:54.384348 IP jabberguest.havogel.com.ssh > 14.0.25.66.60858: Flags [P.], seq 4294967232:208, ack 1, win 20832, length 272
11:44:54.388191 IP 14.0.25.66.60858 > jabberguest.havogel.com.ssh: Flags [.], ack 208, win 64384, options [nop,nop,sack 1 {4294967232:208}], length 0
11:44:54.579286 ARP, Request who-has 14.80.94.10 tell 14.80.94.15, length 46
11:44:54.656970 ARP, Request who-has 14.80.94.11 tell 14.80.94.1, length 46
11:44:54.660995 ARP, Request who-has 14.80.94.235 tell 14.80.94.232, length 46
11:44:55.237405 ARP, Request who-has 14.80.94.17 tell 14.80.94.16, length 46
11:44:55.579320 ARP, Request who-has 14.80.94.10 tell 14.80.94.15, length 46
11:44:55.660815 ARP, Request who-has 14.80.94.235 tell 14.80.94.232, length 46
11:44:55.915532 ARP, Request who-has 14.80.94.104 tell 14.80.94.1, length 46
11:44:55.921206 ARP, Request who-has 14.80.94.150 tell 14.80.94.1, length 46
11:44:56.102066 ARP, Request who-has 14.80.94.66 tell 14.80.94.56, length 46
11:44:56.113541 ARP, Request who-has 14.80.94.48 tell 14.80.94.220, length 46
11:44:56.234761 ARP, Request who-has 14.80.94.17 tell 14.80.94.16, length 46
11:44:56.281613 ARP, Request who-has 14.80.94.101 tell 14.80.94.1, length 46
```

You can run the tcpdump and write the capture on a .pcap file using the **tcpdump -w TAC.pcap** command.

Step 6.

You can collect the files from the Jabber Guest Server with WinSCP. An enhancement on the product to take the packet captures from the web GUI is opened and is tracked under:

https://tools.cisco.com/bugsearch/bug/CSCuu99856/?reffering_site=dumpcr