Capture tcpdump to a ramdisk (for 4750 and 7000 series only)

Information

Article Number 000001567

Goal Capture packets on an EdgeMarc / EdgeProtect for off-line analysis. Capture raw packets in a manner that a 3rd-party tool, such as Ethereal / Wireshark, can decode and display as a protocol trace.

Solution (last updated: 2/29/2016)

The following are steps to creating a ramdisk, perform a tcpdump, and upload the resulting pcap file(s):

Step 1 - Creating ramdisk:

- Log in to CLI
- Type: `mkdir /var/ramdisk`
- Type: `mount -t tmpfs tmpfs /var/ramdisk -o size=8000k`
- Type: `cd /var/ramdisk`

NOTE: Failure to mount the ramdisk may cause phone registration issues or instability issues with the EdgeMarc.
You may be writing the files to the filesystem itself and filing the available disk space on the router.

Step 2 - Initiate tcpdump

See: Using the tcpdump command for details on using the tcpdump command.

[The commands below apply to the EdgeProtect / EdgeMarc 4750 and 7000 Series running VOS 14.1.0 or higher]

[For ALL other platforms, please refer to Capture tcpdump to a ramdisk]

Running tcpdump commands and capturing to a file

To capture (only) SIP signaling on a single interface, without closing the CLI (ssh) session, as an example, type:

```
# tcpdump -i eth0 -s0 port 5060 -w /var/ramdisk/eth0.pcap
```

To end the capture, press `ctrl-c`

OR

To run the same command in the background, type:

```
# nohup tcpdump -i eth0 -s0 port 5060 -w /var/ramdisk/eth0.pcap &
```

To end the capture(s), type:

killall tcpdump

Other examples:

(SIP and RTP)

To capture (only) SIP signaling on both interfaces simultaneously to two separate files (from one SSH window), as an example, type:

```
# nohup tcpdump -i eth0 -s0 port 5060 -w /var/ramdisk/eth0.pcap & nohup
tcpdump -i eth1 -s0 port 5060 -w /var/ramdisk/eth1.pcap &
```

- `eth1, is the WAN interface`
- `eth0, is the LAN interface`
  (if you are using VLANS, substitute eth0 with the vlan that the ALG is listening to - example eth0.100)

To capture RTP traffic (UDP) on both interfaces simultaneously to two separates files (from one SSH window), as an example, type:

```
# nohup tcpdump -i eth0 -s0 udp -w /var/ramdisk/eth0.pcap & nohup
tcpdump -i eth1 -s0 udp -w /var/ramdisk/eth1.pcap &
```

To capture (only) SIP signaling both interfaces simultaneously to a single file (from one SSH window), as an example, type:

```
# nohup tcpdump -i any port 5060 -s 0 -w /var/ramdisk/any.pcap &
```

- `this command is used to capture SIP signaling when the SIP-UA (FXS), SIP-GW (FXO) or PRI port on the EdgeMarc is involved in the call`

To capture RTP traffic (UDP) on all interfaces simultaneously to a single file, type

```
# nohup tcpdump -i any udp -s 0 -w /var/ramdisk/any.pcap &
```

Note:
The "&" characters will background the capture tasks.
To end the capture, type: `killall tcpdump`

(H.323 / video-conferencing traffic)

To capture H323 registration signaling on any interface, simultaneously to a single file (from one SSH window), as an example, type:

nohup tcpdump -ni any -s0 port 1719 -w /var/ramdisk/h323_reg_any.pcap &

To capture H323 registration signaling on both interface, simultaneously to two separate files (from one SSH window), as an example, type:

nohup tcpdump -ni eth0 -s0 port 1719 -w /var/ramdisk/H323_reg_eth0.pcap & nohup tcpdump -ni eth1 -s0 port 1719 -w /var/ramdisk/H323_reg_eth1.pcap &

- eth1, is the WAN interface
- eth0, is the LAN interface
  (if you are using VLANS, substitute eth0 with the vlan that the ALG is listening to - example eth0.100)

To capture H323 registration and setup signaling on any interface, simultaneously to a single file (from one SSH window), as an example, type:
nohup tcpdump -ni any -s0 port 1719 or port 1720 -w /var/ramdisk/H323_setup_any.pcap &

To capture H323 registration and setup signaling on both interface, simultaneously to a two separate files (from one SSH window), as an example, type:
nohup tcpdump -ni eth0 -s0 port 1719 or port 1720 -w /var/ramdisk/H323_eth0.pcap & nohup tcpdump -ni eth1 -s0 port 1719 or port 1720 -w /var/ramdisk/H323_eth1.pcap &

- The "&" characters will background the capture tasks.
- To end the capture, type: killall tcpdump

Step 3 - Upload to a PC for analysis

Use WinSCP, FTP or inband Z-modem to download the capture(s) from the ramdisk

ftp

- Type: `ftp` *`public_ftp_server`*
- Type: `lcd /var/ramdisk`
- Type: `mput *.pcap`

z-modem

See: EdgeMarc: lsz Command Support for details on inband z-modem transfer.

- SSH/Telnet to CLI using a zmodem-capable application, such as windows Hyperterm
- Type: cd /var/ramdisk
- Type: lsz *.pcap

Last Modified Date 2/29/2016 9:06 PM

Copyright © 2016. All Rights Reserved. www.edgewaternetworks.com