

ESET Tech Center

Knowledgebase > Diagnostics > Using tcpdump on a Virtual Appliance

Using tcpdump on a Virtual Appliance

Steef | ESET Nederland - 2023-08-14 - Comments (0) - Diagnostics

When troubleshooting network related issues on a virtual appliance/linux machine, tcpdump is the linux equivalent of wireshark.

To install tcpdump:

Enter the following command in the terminal of the appliance to install tcpdump:

```
yum install tcpdump
```

Confirm the installation with "y"

```
=====  
Installing:  
tcpdump          x86_64          14:4.9.2-3.e17          base          421 k  
Transaction Summary  
=====  
Install 1 Package  
  
Total download size: 421 k  
Installed size: 1.0 M  
Is this ok [y/d/N]: y  
Downloading packages:  
tcpdump-4.9.2-3.e17.x86_64.rpm          | 421 kB    00:10  
Running transaction check  
Running transaction test  
Transaction test succeeded  
Running transaction  
  Installing : 14:tcpdump-4.9.2-3.e17.x86_64          1/1  
  Verifying  : 14:tcpdump-4.9.2-3.e17.x86_64          1/1  
  
Installed:  
tcpdump.x86_64 14:4.9.2-3.e17  
  
Complete!
```

Use the following command to capture and save the packets in a file:

```
tcpdump -vv -w FILENAME.pcap -i any
```

Reproduce the issue, so it is captured in the tcpdump log.

To cancel the capture press:

```
Ctrl + c
```

To compress the output file:

```
tar -cvzf FILENAME.tar.gz FILENAME.pcap
```

Please send the compressed output file: FILENAME.tar.gz to [ESET Support](#).

Related Content

- [Create a full memory dump of a VMware virtual machine](#)
- [How do I generate a memory dump manually?](#)
- [How to create a Wireshark log](#)
- [Run the Info_get.command on a Linux machine and send the logs to ESET Technical Support](#)
- [How do I use ESET Log Collector?](#)