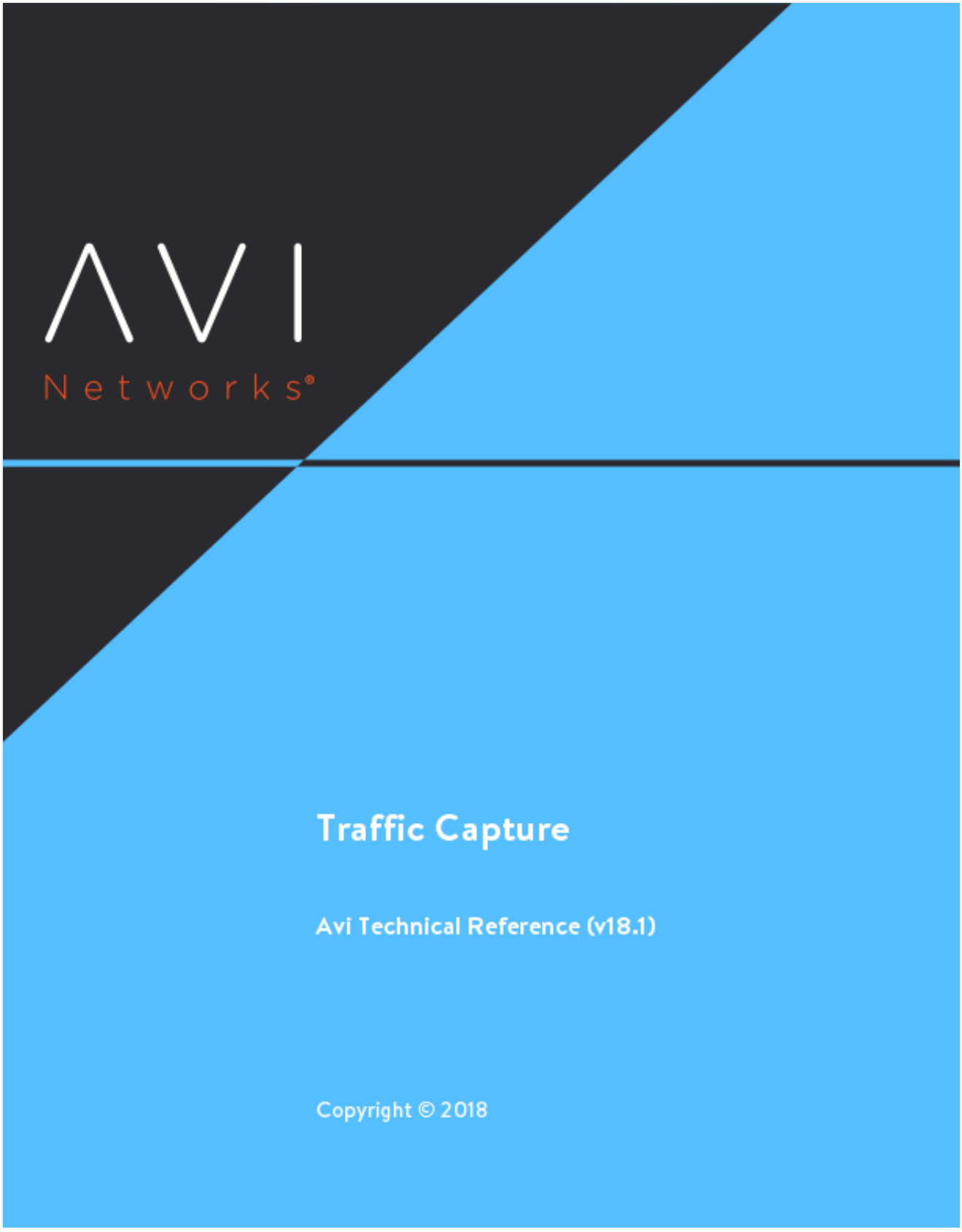


Traffic Capture

Avi Technical Reference (v18.1)

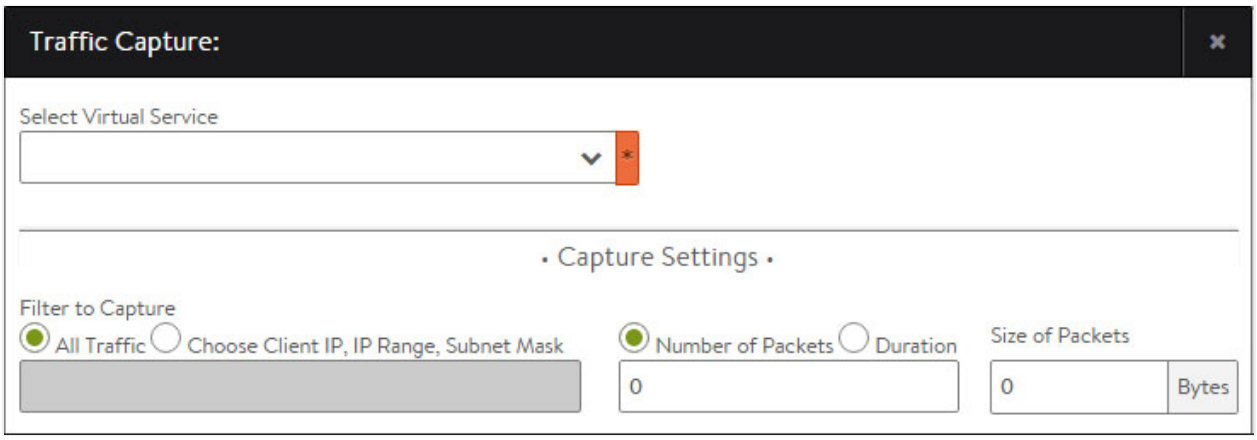
Traffic Capture

view online

Most troubleshooting of connection or traffic data may be done quickly via virtual services logs. However, some troubleshooting may require full visibility into the packet transmission. Vantage provides a packet capture feature, which runs TCPdump against a designated virtual service. The packet capture is done on all Service Engines that may be hosting the VS, then collated into the completed capture.

Capture Configuration

The Capture Configuration section shows the parameters defined for any captures that are currently in progress. To begin a new capture, select the blue pencil icon on the right of the box.



- Select Virtual Service: The capture is executed against traffic for a virtual service. The capture includes both the client-to-SE and SE-to-server sides of the connection. It will automatically be performed on all SEs handling traffic for the virtual service.
- All Traffic: By default, all traffic is captured. Adding an optional filter will enable IP based filtering based on a single IP address 10.1.1.1, a space separated list, a range 10.1.1.1-10.1.1.255, or a subnet mask 10.1.1.1/24. This IP could be either the client or the server of the connection.
- Number of Packets / Duration: It is highly recommended to set a limit to the duration of the capture. This limit may be either the max number of packets to receive, or the duration of time, in minutes. Once the limit has been reached, the capture will terminate and be sent to the Controller for processing and should be available shortly after.
- Size of Packets: Set the number of bytes to capture per packet. This is similar to the snaplen option in TCPdump.

When the capture is started, the Capture Configuration section indicates the progress of the capture. Once the capture is complete, it may still take a few minutes for the new capture to show up in the Completed Captures, as the Controller may need to collate data from multiple SEs and format the data, which is output as a pcap file.

Note: By default, packet captures do not include Service Engine health monitors. This can be enabled via the CLI.

Completed Captures

Once a traffic capture has completed, it will show in the Completed Captures table. This table shows the date, virtual service name and size. The far right column of the table contains an export icon, which allows administrators to download the pcap file. This file type can be viewed by common traffic capture utilities such as Wireshark.

Traffic Capture Via CLI

To provide packet captures via the CLI, log into the Vantage shell as normal. Then enter the packet capture sub-mode for the desired virtual service:

```
<strong>debug virtualservice Test-VS</strong>
Updating an existing object. Currently, the object is:
+-------+--------------------+
| Field | Value              |
+-------+--------------------+
| uuid  | virtualservice-0-1 |
| name  | Test-VS            |
+-------+--------------------+
```

Parameters may be defined for the packet capture. By default, the capture is performed within the context of the selected Virtual Service. It is also performed on all Service Engines that are handling the VS traffic, and includes the packets from the client and server side of the SE.

`capture_params duration`	Time, in minutes. Default is unlimited.
`capture_params num_pkts`	Maximum number of packets to collect. Default is unlimited.
`capture_params pkt_size`	Packet size, or snap length, to capture. Default is unlimited.
`debug_ip addrs`	IP4 Address format
`debug_ip prefixes`	IP4 Prefix format
`debug_vs_hm_include`	Include health monitor packets in the capture
`debug_vs_hm_none`	This default omits health monitor packets from the capture
`debug_vs_hm_only`	Only capture health monitor packets

The `debug_ip` command enters a sub-mode. This allows multiple IP addresses or IP subnets to be entered (omit the `debug_ip` for subsequent entries). Save to commit the desired IPs and return to the previous menu.

> *Warning: By default, no maximum packets or duration of time to be captured are defined. It is recommended to include a maximum packet capture as shown in the following example. Without a limit, the capture will run until filling the Service Engine disk, potentially disrupting service.*

Specify parameters, including the max number of packets to capture:

```
<strong>capture_params num_pkts 1000</strong>
<strong>debug_ip addrs 10.10.10.10</strong>
debug_ip > <strong>save</strong>
```

Begin capturing based on the previously configured parameters:

```
capture
save
```

```
+----------------+--------------------+
| Field          | Value              |
+----------------+--------------------+
| uuid           | virtualservice-0-1 |
| name           | Test-VS            |
| debug_ip       |                    |
|   addrs[1]     | 10.10.10.10        |
| capture        | True               |
| capture_params |                    |
|   duration     | 0 mins             |
|   num_pkts     | 1000               |
+----------------+--------------------+
```

Re-enter the packet capture sub-mode and stop an ongoing packet capture:

```
<strong>debug virtualservice Test-VS</strong>
debugvirtualservice> <strong>no capture</strong>
debugvirtualservice> <strong>save</strong>
```

Export the packet capture to a remote system that can view it via a tool such as TCPdump or Wireshark:

```
<strong>show debug virtualservice Test-VS capture</strong>
Please specify the destination directory: <strong>/tmp</strong>
Downloaded the attachment to /tmp/vs_virtualservice.20141205_192033.pcap
<strong>bash</strong>
root@Avi-CTRL:~# <strong>scp /tmp/vs_virtualservice.192033.pcap user@10.1.1.1:/tmp</strong>
```