No NetFlow traffic captured

Problem

NetFlow export is started on the devices but there is no NetFlow traffic in the application.

Solution

NetFlow traffic may not show due to several reasons:

- Firewall and access lists are blocking netflow packets
- Collection port is not opened
- Collection port has already being used by a different application
- Bad netflow exporter configuration
- Aggregation filter is filtering out the traffic
- License has expired
- NetFlow packets are being dropped

To determine the cause and solution please do the following:

General steps:

Go to System tab in the application

a. check the Packets chart (netflow packets that the application collected)
   i. f there are no UDP packets received go to steps 1 to 2.
   ii. if there are dropped packets restart Tomcat service for temporary quick fix and go to step 1c to resolve the core problem
b. check Flows chart:
   i. if there are no flows this means that no netflow data is received by the application, go to steps 1 to 2.
   ii. if all flows are unlicensed, your license is invalid or expired - contact us for resolving this
   iii. if all flows are filtered, go to blocked URL > Settings > NetFlow Settings > Aggregation filtering and remove the filter rejecting all flow
   iv. if all flows are dropped, try restarting the tomcat service and contact us if the problem persists
c. check Performance chart:
   i. if Heap utilisation is high try adding more RAM to Tomcat and PostgreSQL services (consult Post installation steps)
   ii. if DB write time is high try adding more CPU cores to the server
   iii. if you are not sure what to do contact us at support@netvizura.com

Linux:

1. Check if NetFlow data is received by the server
    a. in command shell on the server execute `tcpdump port 2055` command - you should see steady stream of packets received by the server (2055 is the default NetFlow port)
        i. if there is no netflow packets check your firewalls, access lists to enable packets to be received by NetVizura server;
    b. in command shell on the server execute `watch -n1 "ls -l /var/lib/netvizura/flow/temp"` - after several seconds you should see that `tmp.bin` file size is increasing
        i. if `tmp.bin` file size is not increasing, but `tcpdump` shows that netflow packets are reaching the server check your local firewall configuration (usually iptables) or NetVizura NetFlow Collection port (see below).
2. Check if Collection port on the server is open and that NetVizura is listening on that port
    a. Check that firewall is allowing packets on NetFlow port (the default is 2055)
        i. Execute command `service iptables status` to view firewall configuration. There has to be a line present which is allowing traffic on NetFlow port (2055)
    b. Check that NetVizura is listening on NetFlow port
        i. Execute command `netstat -noap | grep 2055` and verify that there is a line present similar to following:

```
                    udp        0      0 :::
2055                       :::
*                                      28004/java
off (0.00/0/0)
```

        It is important that *java* process is the one that occupied NetFlow port - not some other process. If some other process already occupied NetFlow port you need to reconfigure that other process to use a different port.
    c. Check that Collection port is accessible outside the NetVizura server

        i. on a remote host execute command `nmap netvizura_ip_address -sU -p 2055` where netvizura_ip_address is the address of NetVizura server. In the output of the command you should see that the port is open.
3. Check netflow exporter configuration
    a. Check if netflow device is configured to send netflows to the NetVizura server IP address and collection port
        i. Collection port in NetVizura application can be set in blocked URL > Settings > NetFlow Settings > Configuration
        ii. Default Collection port is 2055
    b. Try installing a netflow generator and set it to export data to the NetVizura server
        i. if there is traffic on the chart then netflow exporter configuration is not good
        ii. if there is no traffic on the chart, check if the traffic is being blocked (access lists, firewalls)

Windows:

> ⚠ Using an administrator account on Windows is recommended.

1. Check if NetFlow data is received by the server
   a. You should determine if server receives steady stream of packets at 2055 port (2055 is the default NetFlow port) with some packet analyzer for windows (wireshark, windump, etc)
      i. if there is no netflow packets check your firewalls, access lists to enable packets to be received by NetVizura server;
   b. In C:\Program Files\NetVizura\flow\temp after several seconds you should see that `tmp.bin` file size is increasing (This is default location for NetVizura NetFlow installation)
      i. if `tmp.bin` file size is not increasing, but packet analyzer shows that netflow packets are reaching the server, check your local firewall configuration or NetVizura NetFlow Collection port (see below).
2. Check if Collection port on the server is open and that NetVizura is listening on that port (the default is 2055)
   a. Check that firewall is allowing packets on NetFlow port (the default is 2055)
   b. Check that NetVizura is listening on NetFlow port
   i. In Windows Command Prompt or PowerShell execute the following command: `netstat -noab` and verify that Tomcat process is the one that occupied NetFlow port 2055. If some other process already occupied NetFlow port you need to reconfigure that other process to use a different port.
   c. Check that Collection port is accessible outside the NetVizura server
      i. on a remote host execute command `nmap -sU netvizura_ip_address -p 2055` where netvizura_ip_address is the address of NetVizura server. In the output of the command you should see that the port is open.
3. Check netflow exporter configuration
   a. Check if netflow device is configured to send netflows to the NetVizura server IP address and collection port
      i. Collection port in NetVizura application can be set in blocked URL > Settings > NetFlow Settings > Configuration
      ii. Default Collection port is 2055
   b. Try installing a netflow generator and set it to export data to the NetVizura server
      i. if there is traffic on the chart then netflow exporter configuration is not good
      ii. if there is no traffic on the chart, check if the traffic is being blocked (access lists, firewalls)