NetFlow Overview

Introduction

NetFlow is a protocol for exporting metrics for IP traffic flows. NetFlow data is sent from a flow exporter to a flow collector. Services and applications that serve as NetFlow collectors are designed to receive the NetFlow data sent from exporters, aggregate the information, and provide data visualization and exploration toolsets.

Exporting NetFlow data about traffic on an MX or Z-Series network can be useful in a variety of scenarios, including the following:

- **Mixed Meraki & Cisco Deployments** - NetFlow is supported within Cisco IOS on a large number of Cisco products. NetFlow can subsequently be used to aggregate traffic data for both Cisco IOS and Meraki MX/Z-Series devices at a given location.

- **Traffic analysis across a large number of Dashboard networks and organizations** - The Cisco Meraki Dashboard provides a large suite of traffic analysis information and summary reports across multiple networks or for an entire Dashboard organization. In some cases, customers may have a very large number of managed networks, also distributed across many distinct Dashboard organizations. In this use case, Dashboard networks across a wide number of different Dashboard organizations can export NetFlow data to a common server for centralized traffic analysis and monitoring within a network operations center.

NOTE: Netflow is also supported on a subset of MS series switches. Please refer to the following documentation for more information: [MS NetFlow and Encrypted Traffic Analytics](#)

Meraki Implementation

There have been several different versions of NetFlow introduced since its original inception. All MX models and Z-Series operate using NetFlow version 9.

NetFlow Export Scope

The MX can only export NetFlow data for traffic that hits the CPU, specifically traffic that is NAT’ed or routed. If traffic is hardware switched (i.e. within the same VLAN), then the MX won’t see the needed information to send any NetFlow updates on it.

Templates

One of the new NetFlow version 9 features is the use of templates. In NetFlow v9 the NetFlow exporter sends a schema outlining the fields that will be included in subsequent NetFlow flow updates. Data fields that an MX or Z-Series will export via NetFlow are:

- **IP_SRC_ADDR**
  - IPv4 source address

- **IP_DST_ADDR**
• IPv4 destination address

• **L4_SRC_PORT**
  ◦ TCP/UDP source port number i.e.: FTP, Telnet, or equivalent

• **L4_DST_PORT**
  ◦ TCP/UDP destination port number i.e.: FTP, Telnet, or equivalent

• **BYTES**
  ◦ Incoming counter with length N x 8 bits for the number of bytes associated with an IP Flow.

• **OUT_BYTES**
  ◦ Outgoing counter with length N x 8 bits for the number of bytes associated with an IP Flow.

• **PKTS**
  ◦ Incoming counter with length N x 8 bits for the number of packets associated with an IP Flow.

• **OUT_PKTS**
  ◦ Outgoing counter with length N x 8 bits for the number of packets associated with an IP Flow.

• **PROTOCOL**
  ◦ IP protocol byte

The fields exported are based on the [NetFlow Version 9 Flow-Record Format](#). The following image shows an example packet capture of a NetFlow Template:
Flow Updates

NetFlow updates for a given flow are sent periodically as data becomes available. The maximum frequency in which an update will be sent for a single flow is 3 seconds. These updates are also batched together when possible to try to minimize the traffic footprint.

The following image shows example contents of multiple flow updates in a single packet:

```
Flowset 1
  Flowset Id: Data Template (v9) (0)
  Flowset Length: 44
  Template (id = 5206, count = 9)
    Template Id: 5206
    Field Count: 9
      Field (1/9): IP_SRC_ADDR
        Type: IP_SRC_ADDR (8)
        Length: 4
      Field (2/9): IP_DST_ADDR
        Type: IP_DST_ADDR (12)
        Length: 4
      Field (3/9): L4_SRC_PORT
        Type: L4_SRC_PORT (7)
        Length: 2
      Field (4/9): L4_DST_PORT
        Type: L4_DST_PORT (11)
        Length: 2
      Field (5/9): BYTES
        Type: BYTES (1)
        Length: 4
      Field (6/9): OUTBYTES
        Type: OUTBYTES (23)
        Length: 4
      Field (7/9): PKTS
        Type: PKTS (2)
        Length: 4
      Field (8/9): OUT_PKTS
        Type: OUT_PKTS (24)
        Length: 4
      Field (9/9): PROTOCOL
        Type: PROTOCOL (4)
        Length: 1
```
Dashboard Configuration

NetFlow can be configured in Dashboard on the Network-wide > Configure > General page. NetFlow configuration settings are found under the Reporting header, with the following options:

- **NetFlow traffic reporting**
  - A drop-down menu to enable or disable NetFlow functionality

- **NetFlow collector IP**
  - This configuration option only appears if NetFlow traffic reporting is set to "Enabled: send netflow traffic statistics"
  - Used to configure the IPv4 address of the NetFlow collector

- **NetFlow collector port**
  - This configuration option only appears if NetFlow traffic reporting is set to "Enabled: send netflow traffic statistics"
  - Used to configure the UDP port that the NetFlow collector will be listening on

NetFlow data can be exported to a collector on the LAN of an MX, across a site-to-site VPN connection, or over the public Internet.
NetFlow Collector Configuration

The current Meraki-specific requirements for NetFlow are as follows:

- Dashboard must be configured to communicate with a NetFlow collector, not a flow exporter.
- The collector must support NetFlow version 9.

There are a number of server options available for NetFlow collection. Cisco Meraki recommends configuring an "ELK" stack, referring to a combination of the services ElasticSearch, LogStash, and Kibana to provide parsing, data storage, and visualization.

Please refer to your NetFlow collector's documentation for configuration specifics, this article provides an example ELK stack configuration.

Troubleshooting

In some circumstances, a NetFlow collector may not receive NetFlow updates. To mitigate this, the following troubleshooting steps are recommended:

Verify the Configuration

Check the configured NetFlow collector IP and NetFlow collector port configured in Dashboard (Network-wide > Configure > General). Ensure that the IP address and port number entered in Dashboard match the current IPv4 address of the NetFlow collector, and the current UDP port the NetFlow collector is listening on.

Verify Connectivity

If the communication path between an MX/Z-Series and the NetFlow collector is not operational, the collector may not receive NetFlow updates. If the NetFlow collector is configured to respond to ICMP messages, a ping test to the NetFlow collector's IP address from the Ping Live Tool (Security & SD-WAN/Teleworker Gateway > Monitor > Appliance Status) will verify IP connectivity between the MX/Z-Series and the NetFlow collector. If the ping test fails, it is recommended to perform the same test with another client device.

Verify NetFlow Traffic

If the MX/Z-Series can send traffic to the collector but NetFlow data is still not populating, verify that NetFlow traffic is flowing as expected.

To confirm that the MX or Z-Series is sending NetFlow traffic, take a packet capture on the appropriate interface. It is recommended to set the output to "Download .pcap file (for Wireshark)."

In the packet capture, we would expect to see periodic UDP traffic sent to the configured NetFlow collector IP and port.

If the NetFlow collector is across a Non-Meraki VPN tunnel, it will not be possible to decrypt the ESP traffic to view the NetFlow updates directly.
If NetFlow updates are being sent from the MX or Z-Series to the correct IP address and port for the NetFlow collector, it is also recommended to perform a packet capture on the NetFlow collector. If the NetFlow collector is not receiving the updates sent from the MX or Z-Series, any hops between the MX or Z-Series and NetFlow collector should be investigated to ensure that NetFlow updates are not being dropped or routed incorrectly. This could occur if a firewall between the two devices is not configured correctly.

**Additional Notes**

Please consider the following additional notes when using NetFlow.

**Wireshark and NetFlow Traffic**

In many cases, Wireshark will not be able to natively render the NetFlow payload:

<table>
<thead>
<tr>
<th>User Datagram Protocol, Src Port: 5557 (5557), Dst Port: 9995 (9995)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Port: 5557 (5557)</td>
</tr>
<tr>
<td>Destination Port: 9995 (9995)</td>
</tr>
<tr>
<td>Length: 90</td>
</tr>
<tr>
<td>Checksum: 0x8832 [validation disabled]</td>
</tr>
<tr>
<td>[Stream index: 1]</td>
</tr>
<tr>
<td>Data (82 bytes)</td>
</tr>
<tr>
<td>Data: 00090002112dacb055f2883600003be0000000001456003e...</td>
</tr>
<tr>
<td>[Length: 82]</td>
</tr>
</tbody>
</table>

If Wireshark does not render the payload as NetFlow data, a small configuration change of Wireshark will be needed. This can be achieved using the following steps:

1. Within the packet capture, find a NetFlow packet (as identified based on the source and destination IP/port).
2. Once this is selected, click on the Analyze menu option at the top of the Wireshark window and select "Decode As..."
3. From the Decode As window, click in the column on the right-hand side.
4. Once selected, type "cflow"
   - The list should already move based on the characters input.
5. Then, select CFLOW, click Apply, and then click OK.
Wireshark will now correctly interpret this data as NetFlow data.

**Note on SolarWinds NTA**

SolarWinds NTA ignores NetFlow packets that do not contain either an SNMP ingress or egress interface index. The MX supports export of an SNMP ingress or egress interface index via NetFlow.