Set up NetFlow sources for NTA

Overview

This article describes how to set up a device to export NetFlow data to NTA. As a feature to facilitate traffic analysis on Cisco IOS-enabled devices, NetFlow begins its work at the network device itself. Any device that is NetFlow-enabled, in order to communicate the traffic related data it is holding about that device, must be configured to send, push, or export that data to specific collection targets.

Orion NTA collects NetFlow data (by default, on port 2055) only if a network device is specifically configured to send to it. As a NetFlow collector, Orion NTA can receive exported NetFlow version 5 data and NetFlow version 9 data that includes all fields of the NetFlow version 5 template. After it collects NetFlow traffic data, Orion NTA analyzes device bandwidth usage in terms of the source and destination endpoints of conversations reflected in the traffic.

Environment

All NTA versions

Steps

Verify the following for NTA to correctly process NetFlow data and relevant traffic statistics:

- Each device must be configured to export NetFlow data to Orion NTA.
- Each device that exports NetFlow data to Orion NTA must be monitored in Orion NPM.
- Traffic from a device that is not monitored in Orion NPM is only displayed in aggregate as traffic from unmonitored devices. If the device is set up to export data to Orion NTA, but is unmonitored in NPM, the collector may receive the data without being able to meaningfully analyze it.
- The specific interface through which a device exports NetFlow data must be monitored in Orion NPM, and the index number for this interface in the Orion database (interface table) must match the index number in the collected flow data.

Perform the following steps:

1. Log in to the network device.
2. Use the following commands to enable NetFlow on a Cisco device:
   ```
   ip flow-export source
   ```
ip flow-export version 5
ip flow-export destination 2055
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
snmp-server ifindex persist


For information on enabling NetFlow on Cisco ASA devices, consult this SolarWinds article that provides an example NetFlow Config - Cisco ASA.

Otherwise, consult the following examples depending on your device. If your network is device is of a different vendor, consult that vendor's documentation:

- Foundry sFlow Configuration
- Extreme sFlow Configuration
- HP sFlow Configuration

3. Verify that your device and its NetFlow exporting interface are being monitored in Orion.

4. To verify that a device is exporting data as expected, use a packet capture tool, such as Wireshark, to search for packets sent from the network device to the Orion server.

To verify that the IP address of the exporting interface on the network device is the one being monitored in Orion:

1. Open a CLI and log in to the network device.
2. Enter `show run` to display the running configuration on the device.
3. Scroll to the lines where the export source interface is defined. For example, ip flow-export source Ethernet0/0.
4. To discover the IP address of this interface, enter `show run int Ethernet0/0`. You should be able to see that the interface IP address is being monitored in the Orion server.

In the NetFlow module in the Orion Web Console, you should see NetFlow-enabled nodes listed in the NetFlow Sources resource.

Disclaimer: Please note, any content posted herein is provided as a suggestion or recommendation to you for your internal use. This is not part of the SolarWinds software or documentation that you purchased from SolarWinds, and the information set forth herein may come from third parties. Your organization should internally review and assess to what extent, if any, such custom scripts or recommendations will be incorporated into your environment. You elect to use third-party content at your own risk, and you will be solely responsible for the incorporation of the same, if any.