Network Visibility Module

About Network Visibility Module

Because users are increasingly operating on unmanaged devices, enterprise administrators have less visibility into what is going on inside and outside of the network. The Network Visibility Module (NVM) collects rich flow context from an endpoint on or off premise and provides visibility into network connected devices and user behaviors when coupled with a Cisco solution such as Stealthwatch, or a third-party solution such as Splunk. The enterprise administrator can then do capacity and service planning, auditing, compliance, and security analytics. NVM provides the following services:

- Monitors application use to enable better informed improvements (expanded IPFIX collector elements in VzFlow protocol specification) in network design.
- Classifies logical groups of applications, users, or endpoints.
- Finds potential anomalies to help track enterprise assets and plan migration activities.

This feature allows you to choose whether you want the telemetry targeted as opposed to whole infrastructure deployment. The NVM collects the endpoint telemetry for better visibility into the following:

- The device—the endpoint, irrespective of its location
- The user—the one logged into the endpoint
- The application—what generates the traffic
- The location—the network location the traffic was generated on
- The destination—the actual FQDN to which this traffic was intended

When on a trusted network, AnyConnect NVM exports the flow records to a collector such as Cisco Stealthwatch or a third-party vendor such as LiveAction, which performs the file analysis and provides a UI interface. Another third-party vendor such as Splunk may also provide a UI interface to see the reports. Since

most enterprise IT administrator want to build their own visualization templates with the data, we provide some sample base templates through a Splunk app plugin.

NVM on Desktop AnyConnect

Historically, a flow collector provided the ability to collect IP network traffic as it enters or exits an interface of a switch or a router. It could determine the source of congestion in the network, the path of flow, but not much else. With NVM on the endpoint, the flow is augmented by rich endpoint context such as type of device, the user, the application, etc. This makes the flow records more actionable depending on the capabilities of the collection platform. The exported data provided with NVM which is sent via IPFIX is compatible with Cisco NetFlow collectors as well as other 3rd party flow collection platforms such as Splunk, IBM Qradar, LiveAction. Please see platform-specific integration documentation for additional information, For example, Splunk integration is available via https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/200600-Install-and-Configure-Cisco-Network-Visi.html.

If you choose to install the Network Visibility Module, the About screen of the AnyConnect Secure Mobility Client UI lists it as installed. No other indication exists on the AnyConnect UI when NVM is running.

An AnyConnect profile for NVM gets pushed from the ISE or ASA headend if this feature is enabled. On the ISE headend, you can use the standalone profile editor, generate the NVM service profile XML, upload it to ISE, and map it against the new NVM module, just as you do with Web Security, Network Access Manager, and such. On the ASA headend, you can use either the standalone or ASDM profile editor.

NVM gets notified when the VPN state changes to connected and when the endpoint is in a trusted network.

How to Use NVM

You can use NVM for the following scenarios:

- To audit a user's network history for potential exfiltration after a security incident occurred.
- To see how system or adminstrative rights impact what network connected processes are running on a user's machine.
- To get a list of all devices running a legacy OS.
- To determine what application in your network is running the highest network bandwidth.
- To determine how many versions of Firefox are being used in your network.
- To determine what percentage of Chrome.exe connections are IPv6 in your network.

NVM Profile Editor

In the profile editor, configure the IP/FQDN of the collector server and whether data will be anonymized or not. You can create a custom Data Collection Policy to have more control over the anonymization of the data shared with the collector.

Network Visibility Module can establish connection with a single stack IPv4 with an IPv4 address, a single stack IPv6 with an IPv6 address, or a dual stack IPv4/IPv6 to the IP address as preferred by the OS.

Note The Network Visibility Module sends flow information only when it is on the trusted network. By default, no data is collected. Data is collected only when configured as such in the profile, and the data continues to be collected when the endpoint is connected. If collection is done on an untrusted network, it is cached and sent when the endpoint is on a trusted network. NVM uses the TND feature of VPN to learn if the endpoint is in a trusted network. Also, if VPN is in a connected state, then the endpoint is considered to be on the trusted network, and the flow information is sent. The NVM-specific system logs show TND use. Refer to AnyConnect Profile Editor, Preferences (Part 2) for information about setting the TND parameter.

- **Desktop** or **Mobile**—Determines whether you are setting up NVM on a desktop or mobile device. **Desktop** is the default.
- **Collector Configuration**
  - **IP Address/FQDN**—Specifies the IPv4 or IPv6 IP address/FQDN that will be used as the collector.
  - **Port**—Specifies at which port number the collector is listening.
- **Aggregation Interval**—You can customize the NVM timer to define when Cisco nvzFlow exports the data. Specify at what interval the value will be exported so that the collector environment is not overrun. The default is 5 seconds.
- **Throttle Rate**—Throttling controls at what rate to send data from the cache to the collector so that the end user is minimally impacted. You can apply throttling on both real time and cached data, as long as there is cached data. Enter the throttle rate in Kbps. The default is 500 Kbps.

  The cached data is exported after this fixed period of time. Enter 0 to disable this feature.
- **Collection Mode**—Specify when data from the endpoint should be collected by choosing **collection mode is off, trusted network only, untrusted network only, or all networks.**
- **Collection Criteria**—Control collection of data in the following ways: You can reduce unnecessary broadcasts during data collection so that you have only relevant data to analyze. By default, broadcast and multicast packet collection are turned off so that less time is spent on back-end resources. You must click the check box to enable collection for broadcast and multicast packets and to filter the data.
  - **Broadcast packets** and **Multicast packets**—By default, and for efficiency, broadcast and multicast packet collection are turned off. You must click the check box to enable collection for broadcast and multicast packets and to filter the data.
- **Data Collection Policy**—You can add data collection policies and associate them with a network type or connectivity scenario. You can apply one policy to VPN and another to non-VPN traffic since multiple interfaces can be active at the same time.

  When you click Add, the Data Collection Policy window appears. Keep these guidelines in mind when creating policies:
  - By default, all fields are reported and collected if no policy is created or associated with a network type.
  - Each data collection policy must be associated with at least one network type, but you cannot have two policies for the same network type.

- The policy with the more specific network type takes precedence. For example, since VPN is part of the trusted network, a policy containing VPN as a network type takes precedence over a policy which has trusted as the network specified.
- You can only create a data collection policy for the network that applies based on the collection mode chosen. For example, if the **Collection Mode** is set to **Trusted Network Only**, you cannot create a **Data Collection Policy** for an **Untrusted Network Type**.
- If a profile from an earlier AnyConnect release is opened in a later AnyConnect release profile editor, it automatically converts the profile to the newer release, adding a data collection policy for all networks that excludes the same fields as were anonymized previously.
- **Name**—Specify a name for the policy you are creating.

- **Network Type**—Determine the collection mode, or the network to which a data collection policy should apply, by choosing VPN, trusted, or untrusted. If you choose trusted, the policy applies to the VPN case as well.
- **Include/Exclude**
  - **Type**—Determine what fields you want to **Include** or **Exclude** in the data collection policy. The default is **Exclude**, all fields not checked are collected, and no fields are checked.
  - **Fields**—Determine which fields will be part of your data collection policy. Based on the network type and the fields included/excluded, NVM collects the appropriate data on the endpoint.

    See Collection Parameters for NVM, on page 4 for details.

Save the profile as `NVM_ServiceProfile.xml`. You must save the profile with this exact name or NVM fails to collect and send data.

Collection Parameters for NVM

The following parameters are collected at the endpoint and exported to the collector:

- Flow Details:
  - Source IP—IP address of endpoint
  - Source Port—Port of endpoint from where connection is being made
  - Destination IP—IP address of host
  - Destination Port—Port that host endpoint is trying to connect to
- Destination hostname—Actual fqdn/hostname that resolved to the destination IP on the endpoint
- DNS suffix—DNS suffix configured on the interface associated with the flow on the endpoint
- Interface Index
- Interface Name
- Interface Type
- Interface UID

- L4ByteCountIn—Total number of incoming bytes (payload only, not including L4 headers) on that flow at Layer 4
- L4ByteCountOut—Total number of outgoing bytes (payload only, not including L4 headers) on that flow at Layer 4
- LoggedInUser
- Module Hash List
- Module Name List
- OS Edition
- OS name
- OS version
- Parent Process Account—Authority/Username of the parent of the process associated with the flow.
- Parent Process Hash— SHA256 hash of the process image of the parent process associated with the flow
- Parent Process Name—Name of the parent of the process associated with the flow
- Process Account—Authority/Username of the process associated with the flow
- Process Hash—SHA256 hash of the process image associated with the flow
- Process Name—Name of the process associated with the flow
- System Manufacturer
- System Type—x86 or x64
- UDID—Universally Unique Identifier. Uniquely identifies the endpoint corresponding to each flow
- VirtualStationName

Data Privacy

Any NVM data stored on the disk is obfuscated. If the device is restarted, data is lost.

Customer Feedback Module Gives NVM Status

Part of the Customer Feedback Module collection provides data about whether NVM is installed or not, the number of flows per day, and the DB size.