Troubleshoot AnyConnect Network Visibility Module Telemetry Ingest Issues in Secure Network Analytics

Contents

Introduction

This document describes the procedure to troubleshoot Network Visibility Module (NVM) telemetry ingest issues in Secure Network Analytics (SNA).

Prerequisites

- Cisco SNA knowledge
- Cisco AnyConnect knowledge

Configuration Guides

- Secure Network Analytics Endpoint License and Network Visibility Module (NVM) Configuration Guide
- Cisco AnyConnect Administrator Guide Network Visibility Module, Release 4.10

Requirements

- SNA Manager and Flow Collector in version 7.3.2 or newer
- SNA Endpoint License
- Cisco AnyConnect with Network Visibility Module 4.3 or newer

Components Used

- SNA Manager and Flow Collect version 7.4.0 and Endpoint License
- Cisco AnyConnect 4.10.03104 with VPN and Network Visibility Module
- Windows 10 Virtual machine
- Wireshark software

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Troubleshoot Process

SNA Configuration

Verify Licensing

Ensure that the Smart Licensing Virtual Account that the SNA Manager is registered to, has the Endpoint Licenses.

Verify NVM Telemetry Ingest

To confirm if the SNA Flow Collector receives and inserts NVM telemetry from the endpoints proceed as follows:

1. Log in to the Flow Collector via SSH or console with **root** credentials.

2. Run the **grep 'NVM records this period:' /lancope/var/sw/today/logs/sw.log** command.

3. From the returned output, confirm if the Flow Collector ingests NVM records and inserts them into the database.

```
ao-fc01-cds:~# grep 'NVM records this period:' /lancope/var/sw/today/logs/sw.log
04:00:01 I-pro-t: NVM records this period: received 0 at 0 rps, inserted 0 at 0 rps, discarded 0
04:05:00 I-pro-t: NVM records this period: received 0 at 0 rps, inserted 0 at 0 rps, discarded 0
04:10:00 I-pro-t: NVM records this period: received 0 at 0 rps, inserted 0 at 0 rps, discarded 0
04:15:00 I-pro-t: NVM records this period: received 0 at 0 rps, inserted 0 at 0 rps, discarded 0
```

From this output it seems that the Flow Collector has not received any NVM records at all, however you must confirm if it is configured to listen for NVM telemetry.

Verify if the Flow Collector is configured to listen for NVM telemetry

1. Log in to the Flow Collector Admin User Interface (UI).

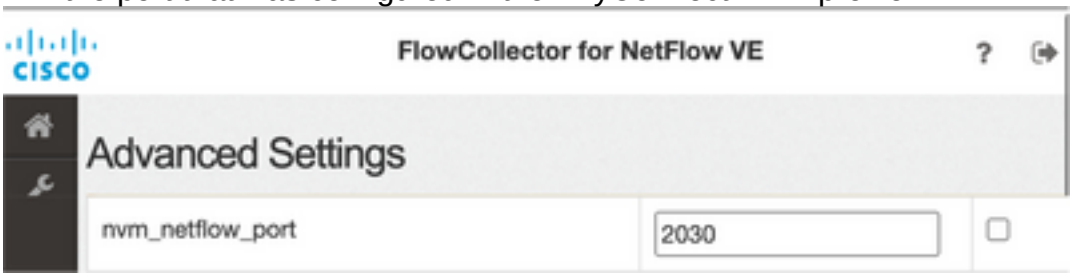
2. Navigate to to **Support > Advanced Settings**.

3. Ensure the required attributes are configured correctly:

SNA Version 7.3.2 or 7.4.0

==========

- Locate the **nvm_netflow_port** attribute and verify the configured value. This must match with the port that was configured in the AnyConnect NVM profile.



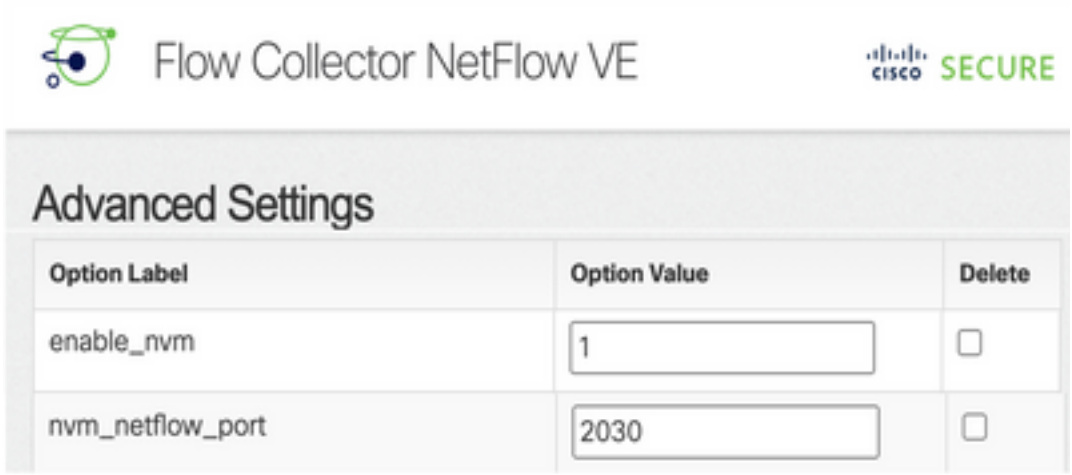
Note: Ensure that the configured port is a non-reserved port and is not 2055, 514 or 8514. If the configured value is "0" the feature is disabled.

Note: If a field is not shown, scroll to the bottom of the page. Click the **Add New Option** field. For more information about advanced settings on the Flow Collector, refer to the Advanced Settings online help topic.

SNA Version 7.4.1

==========

- Locate the **nvm_netflow_port** attribute and verify the configured value. This must match with the port that was configured in the AnyConnect NVM profile.
- Locate the **enable_nvm** attribute and ensure that the value is set to **1**, otherwise the feature is disabled.



Note: Ensure that the configured port is a non-reserved port and is not 2055, 514 or 8514.

Note: If a field is not shown, scroll to the bottom of the page. Click the **Add New Option**

field. For more information about advanced settings on the Flow Collector, refer to the Advanced Settings online help topic.

4. Once the advanced settings on the Flow Collector have been configured correctly, verify if the telemetry is now ingested, with the same procedure as as described in the **Verify NVM Telemetry Ingest** section.

5. If the configuration of the endpoint with AnyConnect NVM and the settings on the Flow Collector are correct, the **sw.log** file must reflect it:

```
ao-fc01-cds:~# grep 'NVM records this period:' /lancope/var/sw/today/logs/sw.log
04:35:00 I-pro-t: NVM records this period: received 78 at 0 rps, inserted 78 at 0 rps, discarded
0
04:40:00 I-pro-t: NVM records this period: received 66 at 0 rps, inserted 66 at 0 rps, discarded
0
04:45:00 I-pro-t: NVM records this period: received 91 at 0 rps, inserted 91 at 0 rps, discarded
0
04:50:00 I-pro-t: NVM records this period: received 80 at 0 rps, inserted 80 at 0 rps, discarded
0
```

6. If the Flow Collector still does not ingest NVM records, verify if the collector receives the packets on the interface and, in any case, ensure that the configuration of the endpoints is correct.

Endpoint Configuration

You can deploy AnyConnect NVM in one of two ways: a) with the AnyConnect package or b) with the Standalone NVM package (on AnyConnect desktop only).

The required configuration is the same for both deployments, the difference resides in the configuration of Trusted Network Detection.

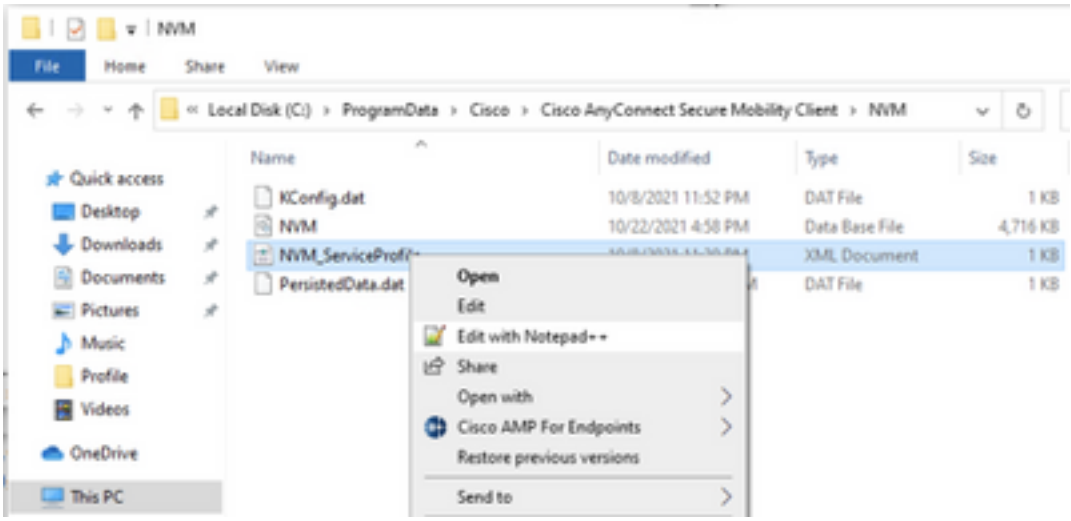
Verify NVM Profile

Locate the NVM Profile used by the endpoint and confirm the **Collector Configuration** settings.

NVM Profile Location:

- Windows: **%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM**
- Mac: **/opt/cisco/anyconnect/nvm**

Note: The name of the NVM profile must be **NVM_ServiceProfile**, otherwise Network Visibility Module fails to collect and send data.



The content of the NVM profile depends on your configuration, however the elements of the profile that are relevant for SNA are marked in bold. Ensure to review the notes after the NVM profile example:

<?xml version="1.0" encoding="UTF-8"?> <NVMProfile xsi:noNamespaceSchemaLocation="NVMProfile.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"> <ProfileVersion>2</ProfileVersion> <CollectorConfiguration>
<CollectorIP>10.1.0.250</CollectorIP>
<Port>2030</Port>
<Secure>false</Secure>
</CollectorConfiguration>
<TemplateReportInterval>5</TemplateReportInterval>
<AggInterval>5</AggInterval>
<ThrottleRate>500</ThrottleRate>
<CollectionMode>all</CollectionMode>
<CollectionCriteria>
<Broadcast>false</Broadcast>
<Multicast>false</Multicast>
</CollectionCriteria>
<DataCollectionPolicy>
</DataCollectionPolicy>
</NVMProfile>

Note: Ensure that the **configured port is a non-reserved port and is not 2055, 514 or 8514**. The configured port in this profile needs to be the same as the one configured on the Flow Collector.

Note: Ensure that if the NVM Profile has the **Secure** XML element, it is set to **false**, otherwise the flows are sent encrypted with DTLS and the Flow collector is not able to process them.

Verify Trusted Network Detection (TND) settings

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 to the collector when the endpoint is on a trusted network. The Secure Network Analytics Flow Collector needs to have additional configuration for it to process cached flows (See Configure the Flow Collector for Off-Network Cached Flows for the needed configuration).

Trusted Network state can be determined by the TND feature of VPN (configured in the VPN Profile) or by the TND configuration in the NVM profile:

TND configuration in VPN Profile

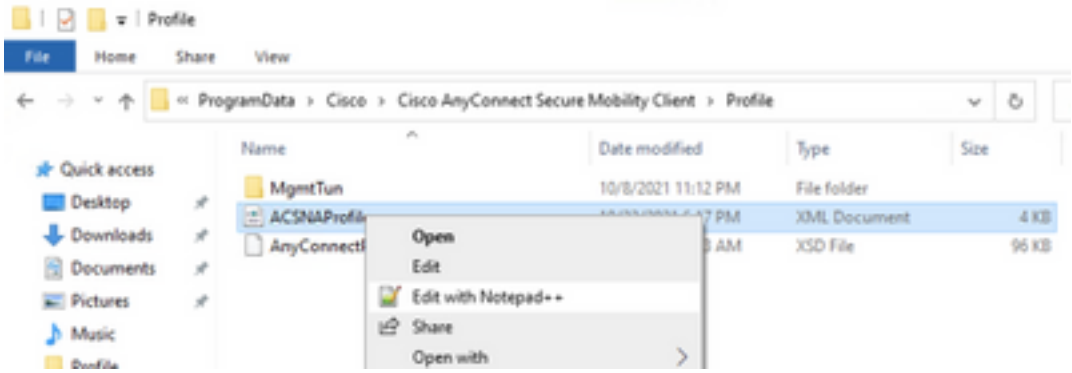
> **Note**: This is not an option for NVM Standalone deployments.

1. Locate the VPN Profile used by the endpoint and confirm the configured **Automatic VPN Policy** settings

VPN Profile Location:

- Windows: **%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile**
- Mac: **/opt/cisco/anyconnect/profile**

In this example the VPN profile is named **ACSNAProfile**.



2. Edit the profile with a text editor and locate the **AutomaticVPNPolicy** element. Ensure that the configured policy is correct for successful detection of the Trusted Network. In this case:

```
...
<AutomaticVPNPolicy>true
<TrustedDNSDomains>*.cisco.local</TrustedDNSDomains>
<TrustedNetworkPolicy>DoNothing</TrustedNetworkPolicy>
<UntrustedNetworkPolicy>Connect</UntrustedNetworkPolicy>
<AlwaysOn>false
</AlwaysOn>
</AutomaticVPNPolicy>
```

> **Note**: For NVM relevance: if both the Trusted Network Policy and Untrusted Network Policy are set to Do Nothing, Trusted Network Detection from the VPN Profile gets disabled.

TND configuration in NVM Profile

Locate the NVM Profile used by the endpoint and confirm that the configured **Trusted Server List** settings are correct.

NVM Profile Location:

- Windows: **%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM**
- Mac: **/opt/cisco/anyconnect/nvm**

```
...
<TrustedServerList> <TrustedServer> <ServerAddress>10.64.0.32</ServerAddress>
<ServerPort>443</ServerPort>
<CertificateHash>C6EF32AAAAAAAAAA26C4BB6829AD2809B5175C9437A7D085A31FA60000000000</CertificateHa
sh>
</TrustedServer>
</TrustedServerList>
</NVMProfile>
```

> **Note**: An SSL probe is sent to the configured trusted headend, which responds with a certificate, if reachable. The thumbprint (SHA-256 hash) is then extracted and matched against the hash set in the profile editor. A successful match signifies that the endpoint is in a trusted network; however, if the headend is unreachable, or if the certificate hash does not match, then the endpoint is considered to be in an untrusted network.

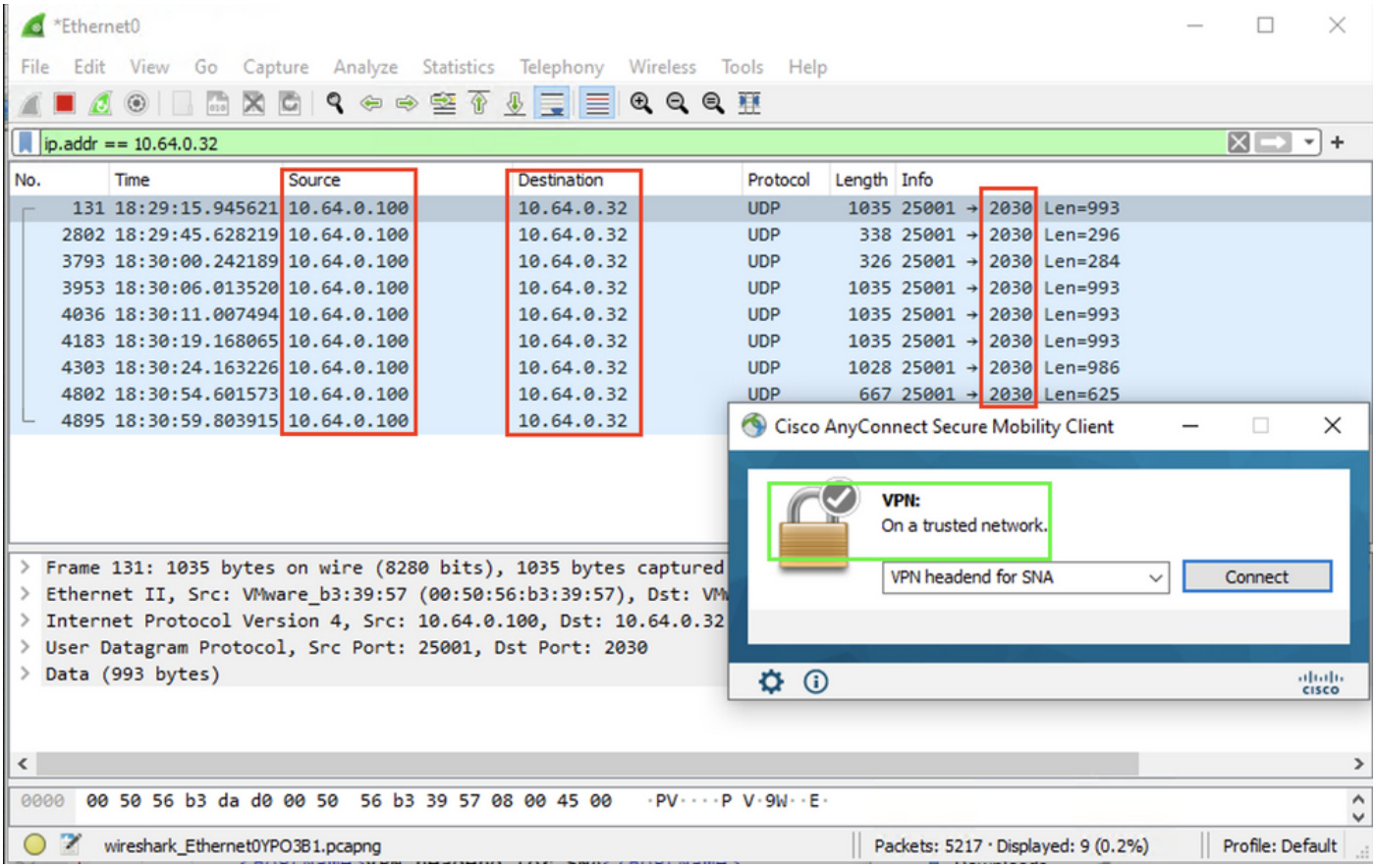
> **Note**: Trusted servers behind proxies are not supported.

Collect packet captures

You can collect a packet capture on the Endpoint network adapter to verify that flows are sent to the Flow Collector.

a. If the Endpoint is on a Trusted Network but NOT connected to VPN the capture must be enabled on the physical network adapter.

In this case, the Anyconnect Client indicates that the endpoint is on a Trusted Network, which means that the flows are sent to the configured Flow Collector over the configured port through the Physical Network Adapter of the endpoint, as we can see in the AnyConnect Window and the Wireshark window displayed next.

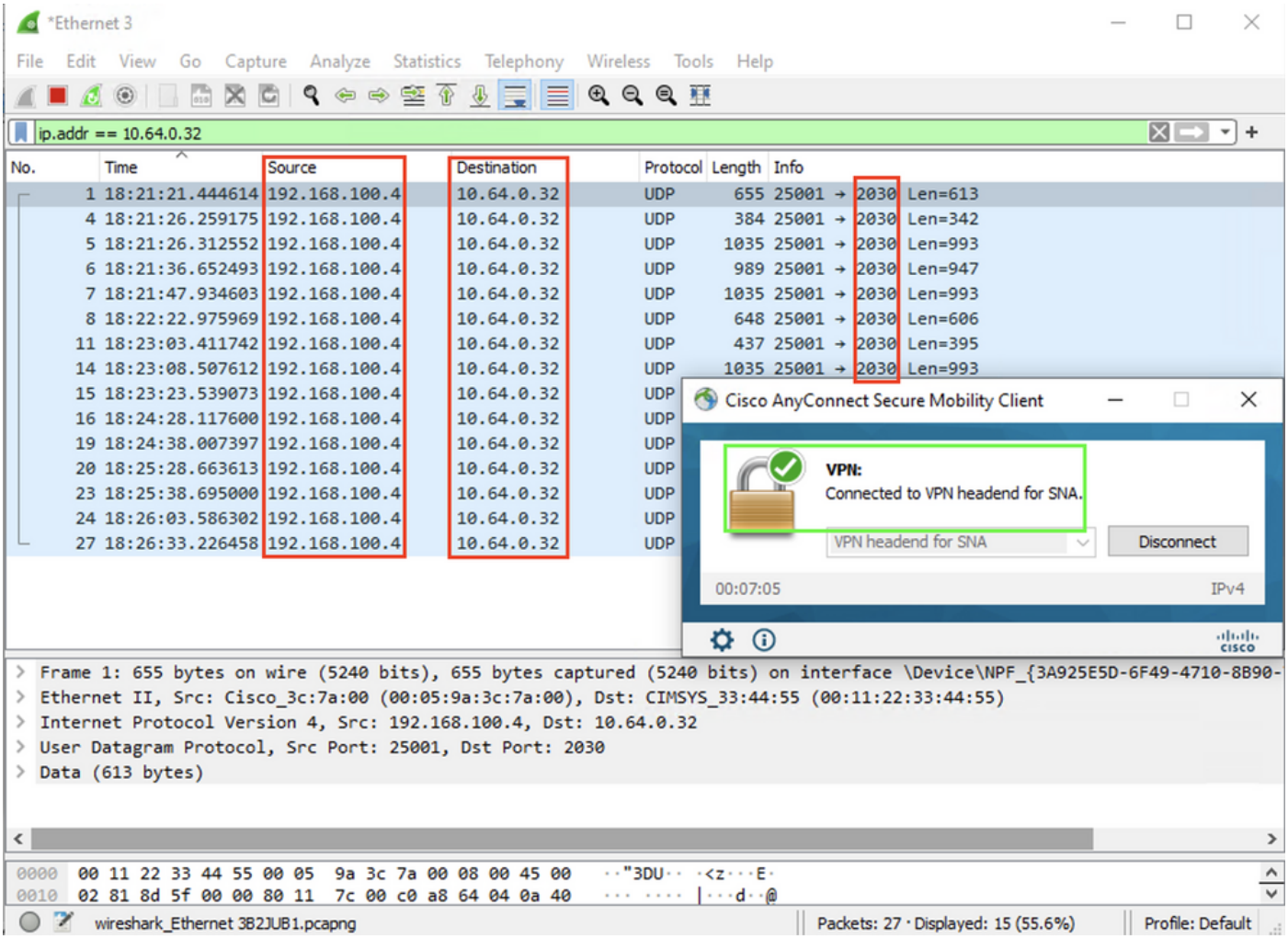


b. If the Endpoint is connected to AnyConnect VPN it is automatically considered to be on the Trusted Network, therefore the capture must be enabled on the Virtual Network Adapter.

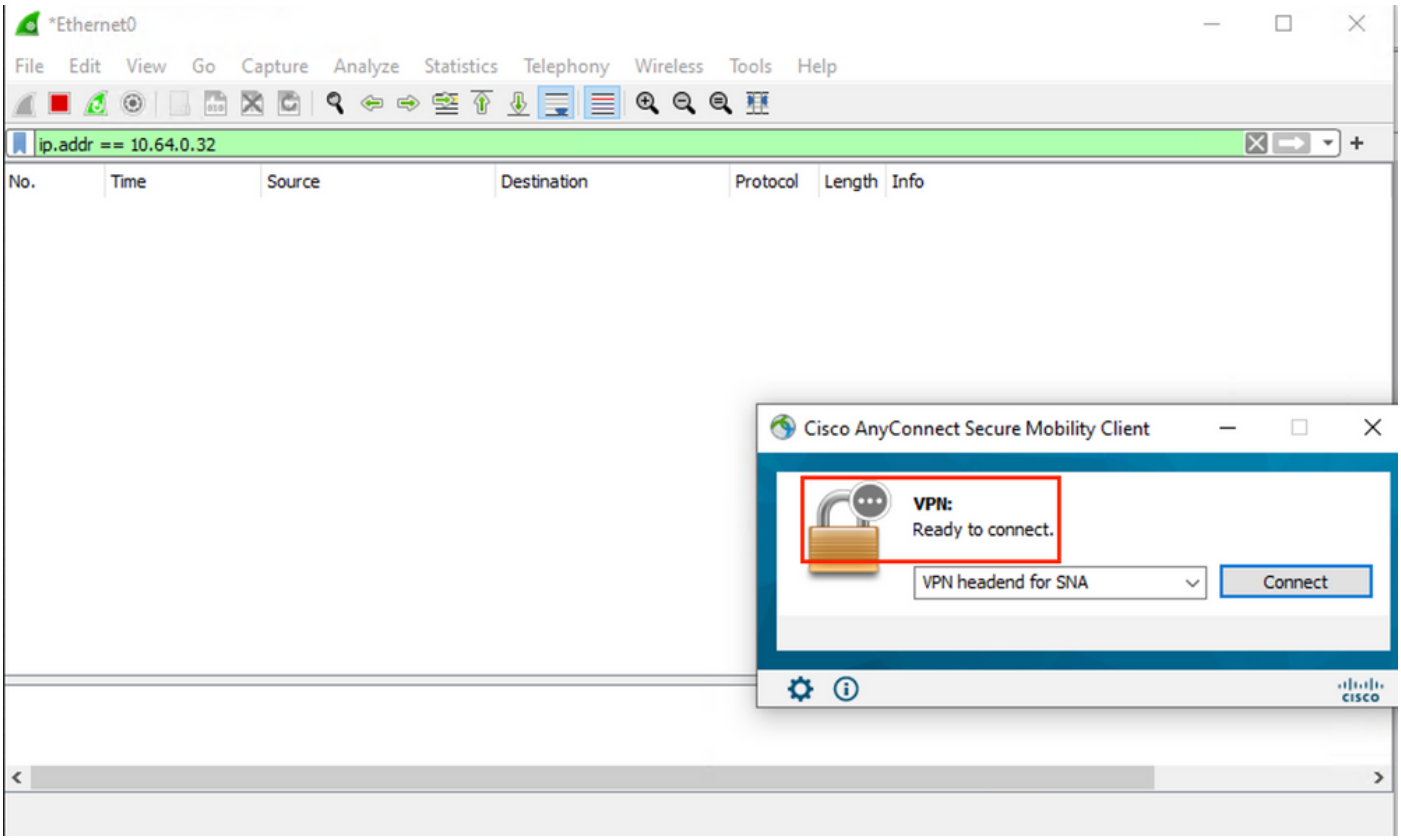
> **Note**: If the VPN module is installed and TND is configured in the Network Visibility Module profile, then Network Visibility Module performs trusted network detection even inside the VPN network.

The AnyConnect Client indicates that the endpoint is connected to VPN, which means that the flows are sent to the configured Flow Collector over the configured port through the Virtual Network Adapter of the endpoint (VPN Tunnel), as we can see in the AnyConnect Window and the Wireshark window displayed next.

> **Note**: The Split Tunnel configuration of the VPN Profile the Endpoint is connected to must include the IP address of the Flow Collector, otherwise the flows are not sent across the VPN tunnel.



c. If the Endpoint is not on a Trusted Network, flows are not sent to the Flow Collector.



Related Defects

There are currently two known defects that can impact the NVM telemetry ingest process on Secure Network Analytics:

- FC Engine cannot ingest NVM telemetry on eth1. See Cisco bug ID CSCwb84013
- Flow Collector not inserting NVM records from AnyConnect version 4.10.04071 or above. See Cisco bug ID CSCwb91824

Related Information

- For additional assistance, please contact Technical Assistance Center (TAC). A valid support contract is required: Cisco Worldwide Support Contacts.
- You can also visit the Cisco Security Analytics Community here.
- Technical Support & Documentation - Cisco Systems