AnyConnect 4.2.x および Splunk 経由の Cisco Network Visibility Module のインストールと設定

目次

概要

このドキュメントでは、Cisco AnyConnect Network Visibility Module (NVM) を、エンドユーザ システム上で AnyConnect 4.2.x 以降を使用してインストールおよび設定する方法を説明します。

Cisco AnyConnect NVM は、セキュリティ分析を展開するための手段として使用されます。 NVM により組織は、そのネットワーク上にあるエンドポイントやユーザの行動を表示し、オンプレミスとオフプレミスの両方にあるエンドポイントからのフローを、ユーザ、アプリケーション、デバイス、ロケーション、および接続先などの追加のコンテキストとともに収集できるようになります。

この TechNote で取り上げているのは、Splunk を使用した AnyConnect NVM の設定例です。

前提条件

要件

次の項目に関する知識が推奨されます。

- NVM を備えた AnyConnect 4.2.01022 以降
- AnyConnect APEX ライセンス
- ASDM 7.5.1 以降

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco AnyConnect Security Mobility Client 4.2 以降
- Cisco AnyConnect Profile Editor
- Cisco 適応型セキュリティ アプライアンス（ASA）バージョン 9.5.2
- Cisco Adaptive Security Device Manager（ASDM）バージョン 7.5.1
- Splunk Enterprise 6.3
- コレクタのデバイスとしての Ubuntu 14.04.3 LTS

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

Cisco AnyConnect セキュア モビリティ クライアント

Cisco AnyConnect は、企業を保護する各種のセキュリティ サービスを提供する統合エージェントです。 AnyConnect は、最も一般的には企業 VPN クライアントとして使用されていますが、企業セキュリティのさまざまな面に対応する追加モジュールもサポートしています。 この追加モジュールにより、ポスチャ アセスメント、Web セキュリティ、マルウェア保護、ネットワーク可視性などのセキュリティ機能が有効になります。

この TechNote は、Network Visibility Module（NVM）に関するものです。この機能は Cisco AnyConnect と統合されており、管理者はこれを使用してエンドポイント アプリケーションの使

用状況をモニタできます。

Cisco AnyConnect の詳細については、次を参照してください。

『Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.3』

Internet Protocol Flow Information Export (IPFIX)

IPFIX は、アカウンティング/監査/セキュリティなどの多様な目的のために IP フロー情報をエクスポートする際の標準を定義する、IETF プロトコルです。 IPFIX は Cisco NetFlow プロトコル v9 を基本にしています。ただし直接的な互換性はありません。

Cisco vzFlow は、IPFIX プロトコルに基づいて拡張されたプロトコル仕様です。 IPFIX には、AC NVM の一部として収集できるすべてのパラメータをサポートする、十分な標準情報要素はありません。 Cisco vzFlow プロトコルは IPFIX 標準を拡張し、新しい情報要素を定義します。さらに、IPFIX データのエクスポートのために AC NVM により使用される標準セットの IPFIX テンプレートを定義します。

IPFIX の詳細については、rfc5101、rfc7011、rfc7012、rfc7013、rfc7014、rfc7015 を参照してください。

IPFIX コレクタ

コレクタは、IPFIX データを受信して保存するサーバです。 これはそのデータを Splunk にフィードします。 たとえば、Lancope

シスコは、自社製の IPFIX コレクタも提供しています。

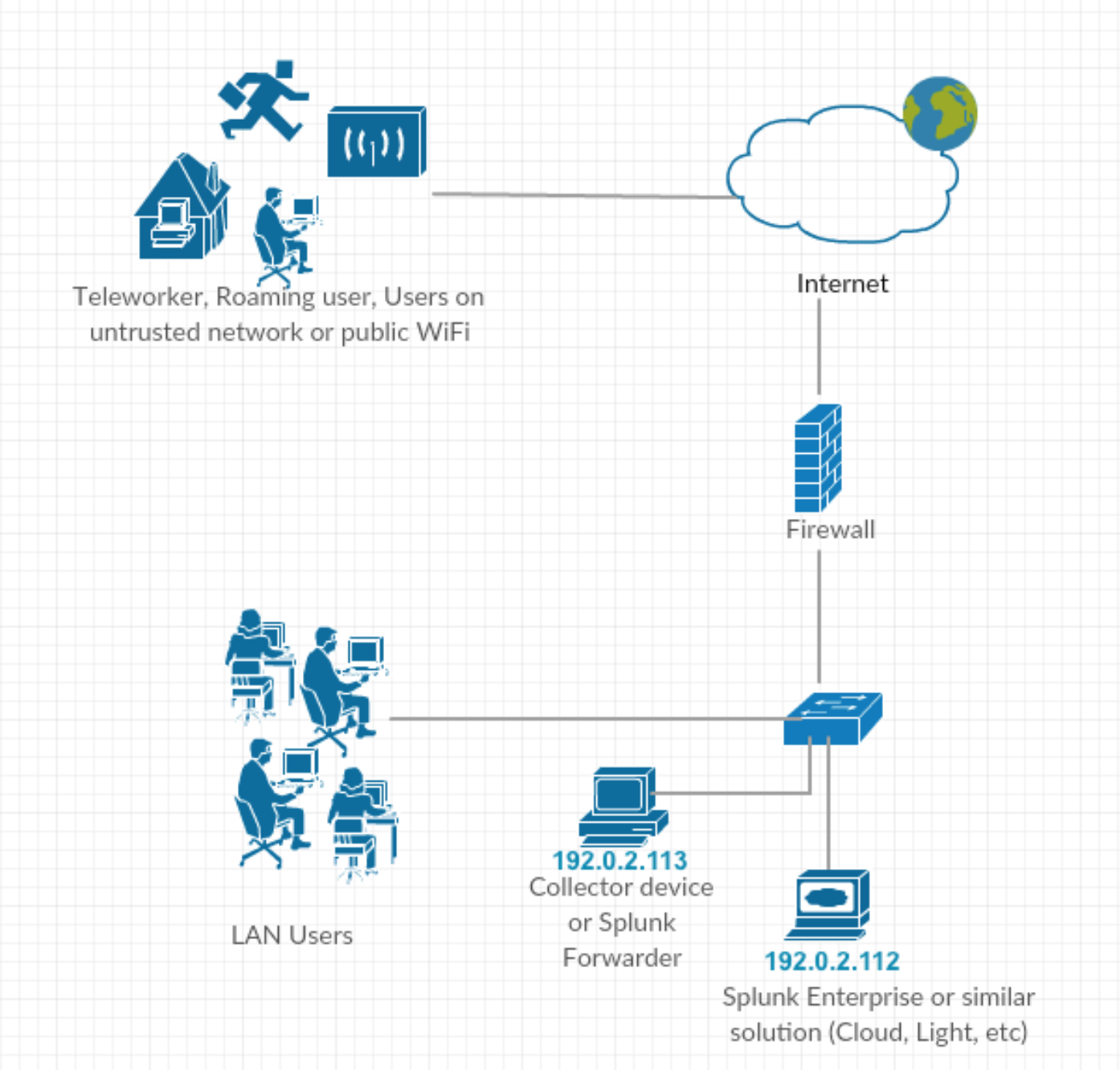
Splunk

Splunk は、診断データを収集して分析し、IT インフラストラクチャに関する意味深い情報を提供する強力なツールです。 これは管理者がネットワークのヘルスを把握するために重要なデータを収集する、ワンストップのロケーションです。

シスコは Splunk を所有または保守しているわけではありませんが、シスコは Cisco AnyConnect NVM App for Splunk を提供しています。

Splunk の詳細については、その Web サイトを参照してください。

トポロジ



この TechNote の IP アドレスの表記法：

コレクタ IP アドレス： 192.0.2.123

Splunk IP アドレス： 192.0.2.113

設定

このセクションでは、Cisco NVM コンポーネントの設定について説明します。

AnyConnect NVM クライアント プロファイル

AnyConnect NVM 設定は、コレクタ IP アドレスやポート番号に関する情報を含む XML ファイルに、そのほかの情報とともに保存されます。 コレクタ IP アドレスとポート番号は、NVM クライアント プロファイルで正しく設定される必要があります。

NVM モジュールを正しく操作するには、XML ファイルがこのディレクトリ内に置かれている必要があります。

- Windows 7 以降の場合： **%%ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM**
- Mac OS X の場合： **//opt/cisco/anyconnect/nvm**

プロファイルが Cisco ASA または Identity Services Engine（ISE）に存在している場合、AnyConnect NVM 展開とともに自動展開されます。

XML プロファイルの例：

```
<?xml version="1.0" encoding="UTF-8"?>
-<NVMProfile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="NVMProfile.xsd">
-<CollectorConfiguration>
<CollectorIP>192.0.2.123</CollectorIP>
<Port>2055</Port>
</CollectorConfiguration>
<Anonymize>false</Anonymize>
<CollectionMode>all</CollectionMode>
</NVMProfile>
```

NVM プロファイルは、次の 2 つのツールを使用して作成できます。

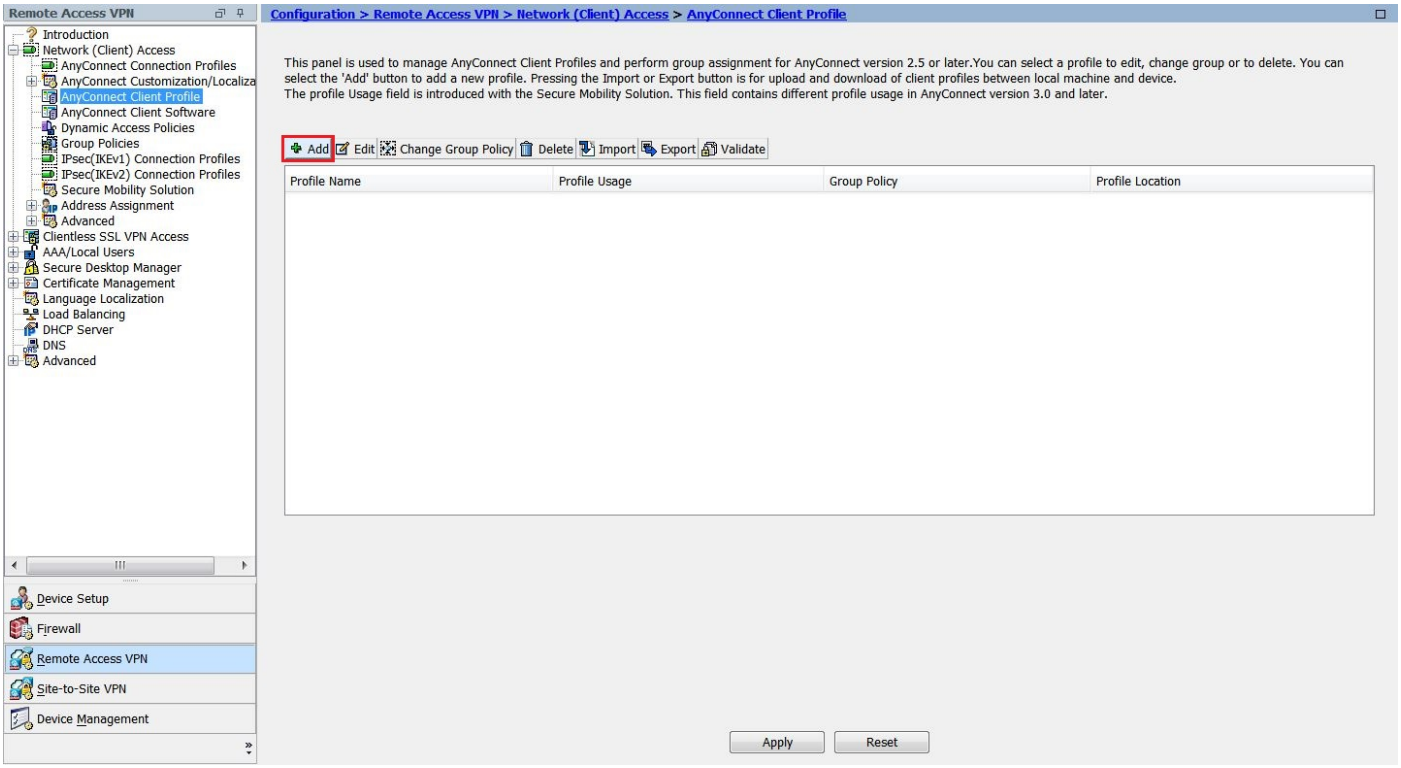
- Cisco ASDM
- AnyConnect プロファイル エディタ

ASDM を介した NVM クライアント プロファイルの設定

この方式は、AnyConnect NVM が Cisco ASA を介して展開される場合に推奨されます。

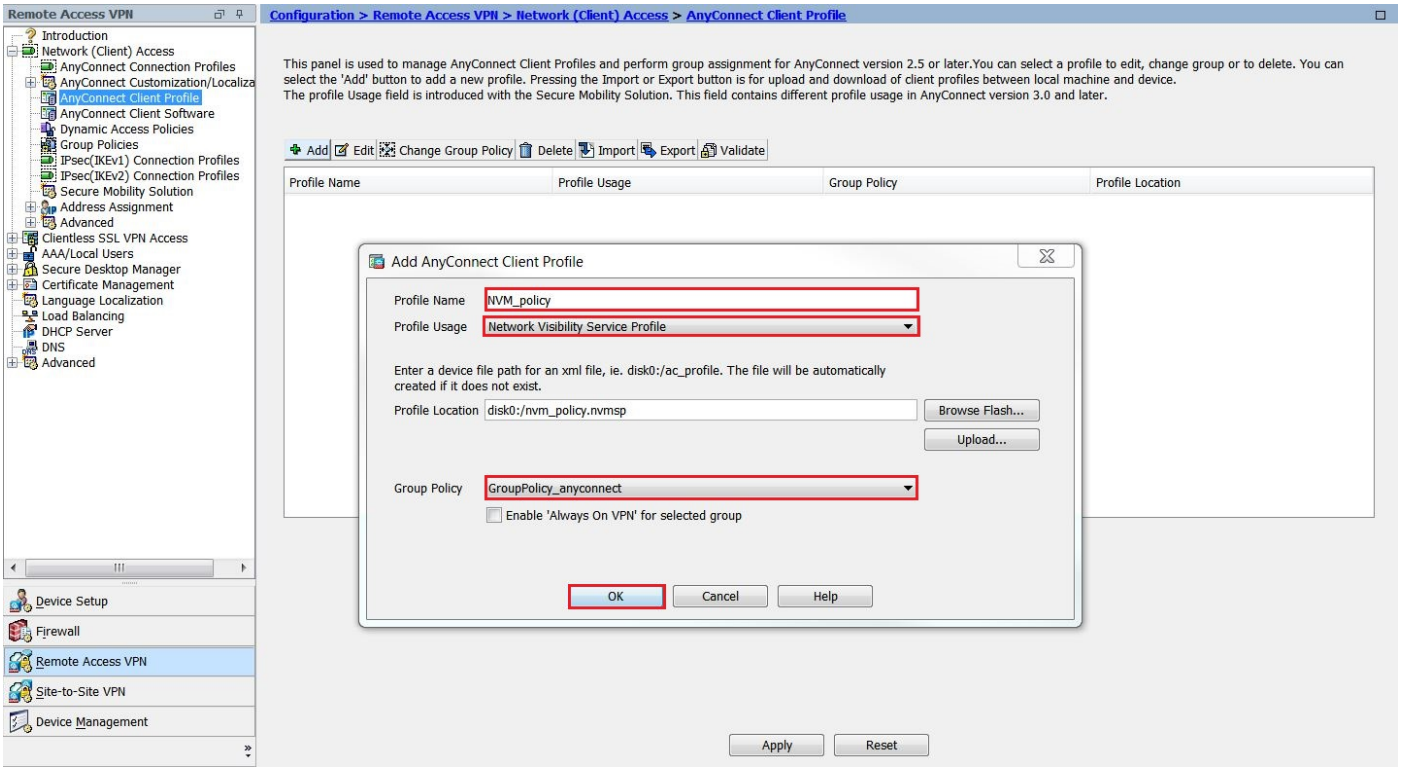
1. [Configuration] > [Remove Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile]の順に移動します。

2. [Add] をクリックします。

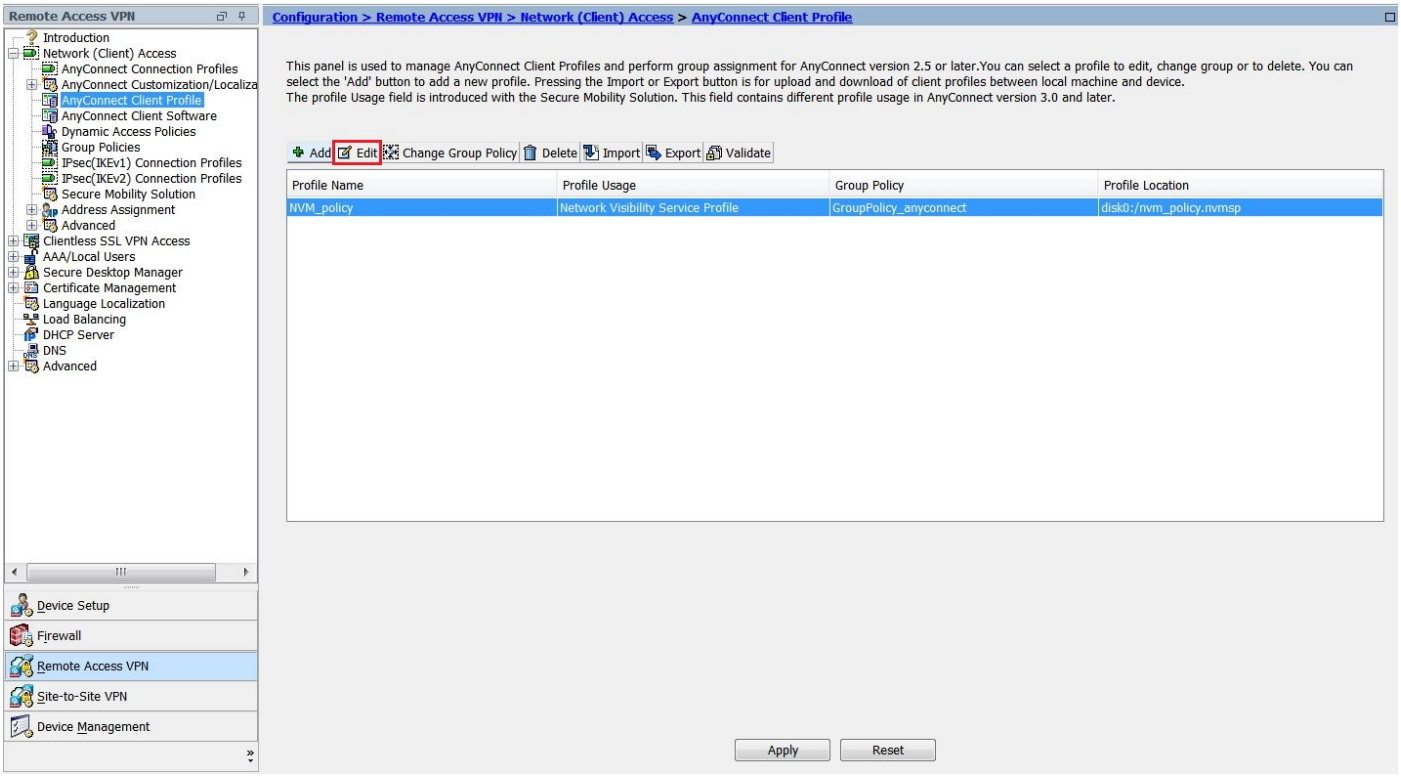


3. プロファイルの名前を入力します。 [Profile Usage]で、[Network Visibility Service Profile] を選択します。

4. AnyConnect ユーザが使用するグループ ポリシーにこれを割り当てます。 [OK] をクリックします。

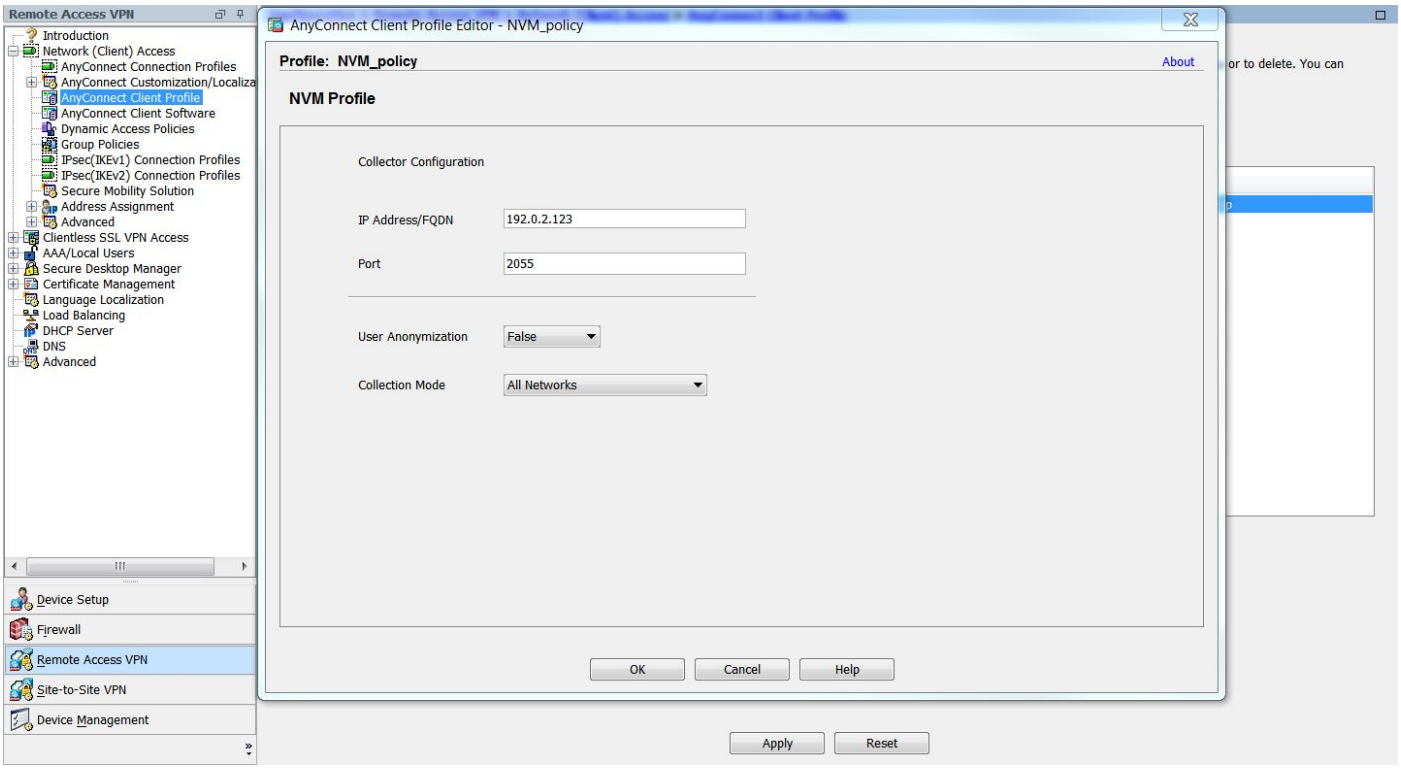


5. 新しいポリシーが作成されました。 [編集（Edit）]をクリックします。



6. コレクタ IP アドレスとポート番号に関する情報を入力します。 [OK] をクリックします。

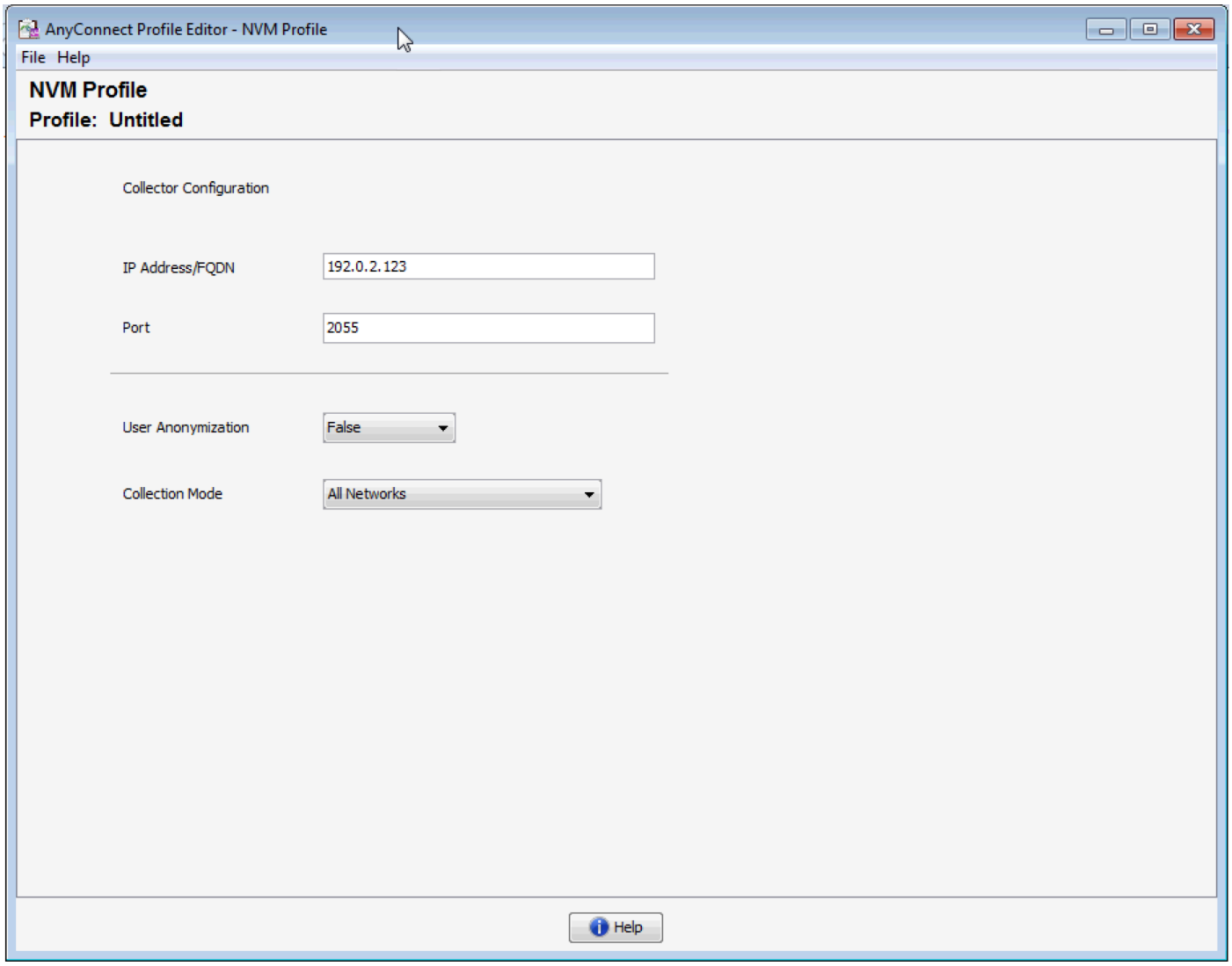
7. [Apply] をクリックします。



AnyConnect プロファイル エディタでの NVM クライアント プロファイルの設定

これは Cisco.com で使用できるスタンドアロン ツールです。 この方式は、AnyConnect NVM が Cisco ISE を介して展開される場合に推奨されます。 このツールを使用して作成された NVM プロファイルは、Cisco ISE にアップロードするか、またはエンドポイントに直接コピーできます

。



AnyConnect プロファイル エディタの詳細については、以下を参照してください。

AnyConnect プロファイル エディタ

Cisco ASA 上での Web 展開の設定

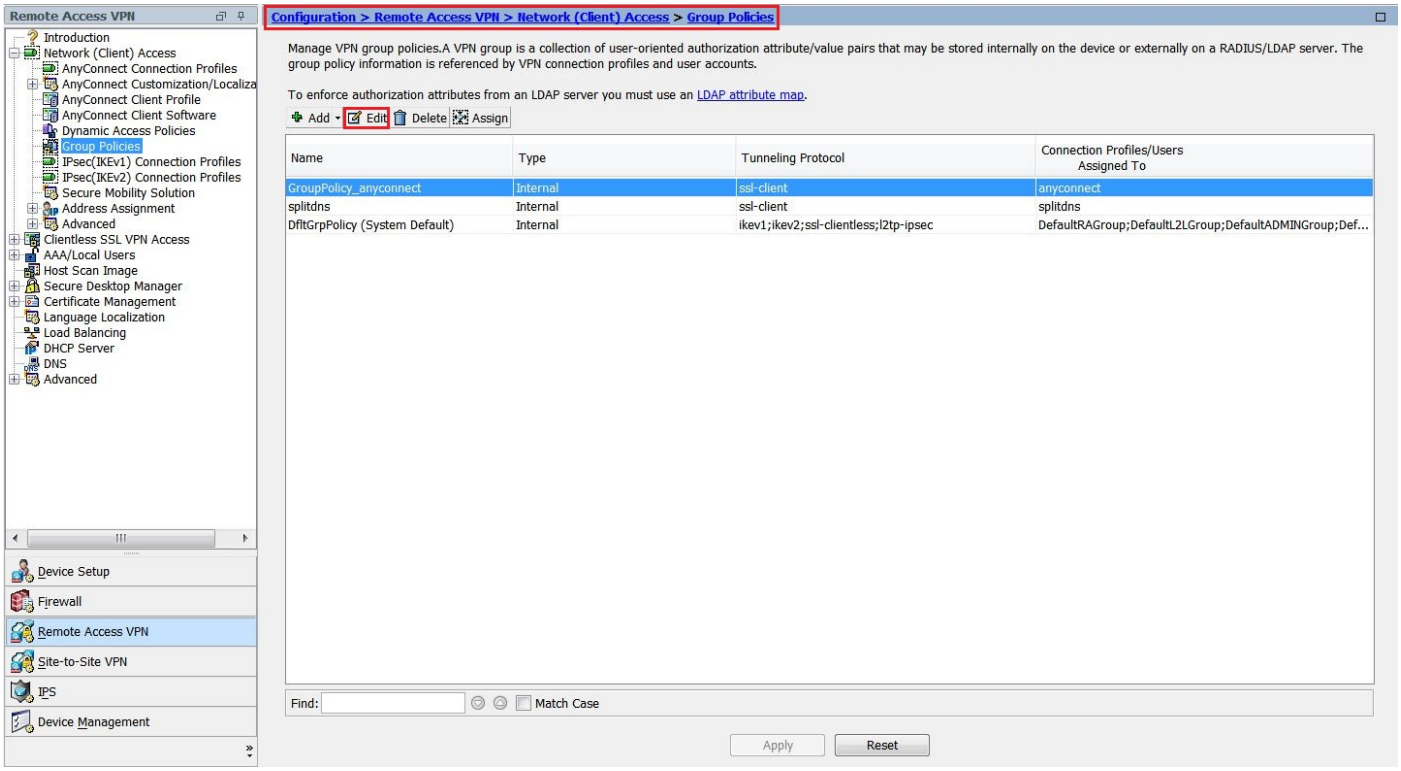
この TechNote は、AnyConnect が ASA 上にすでに設定済みであり、NVM モジュール設定のみ追加が必要であると想定しています。 ASA AnyConnect の設定の詳細については、以下を参照してください。

ASDM ブック 3： Cisco ASA シリーズ VPN ASDM コンフィギュレーション ガイド 7.5

Cisco ASA 上で AnyConnect NVM モジュールを有効にするには、次の手順を実行します。

1. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies]を選択します。

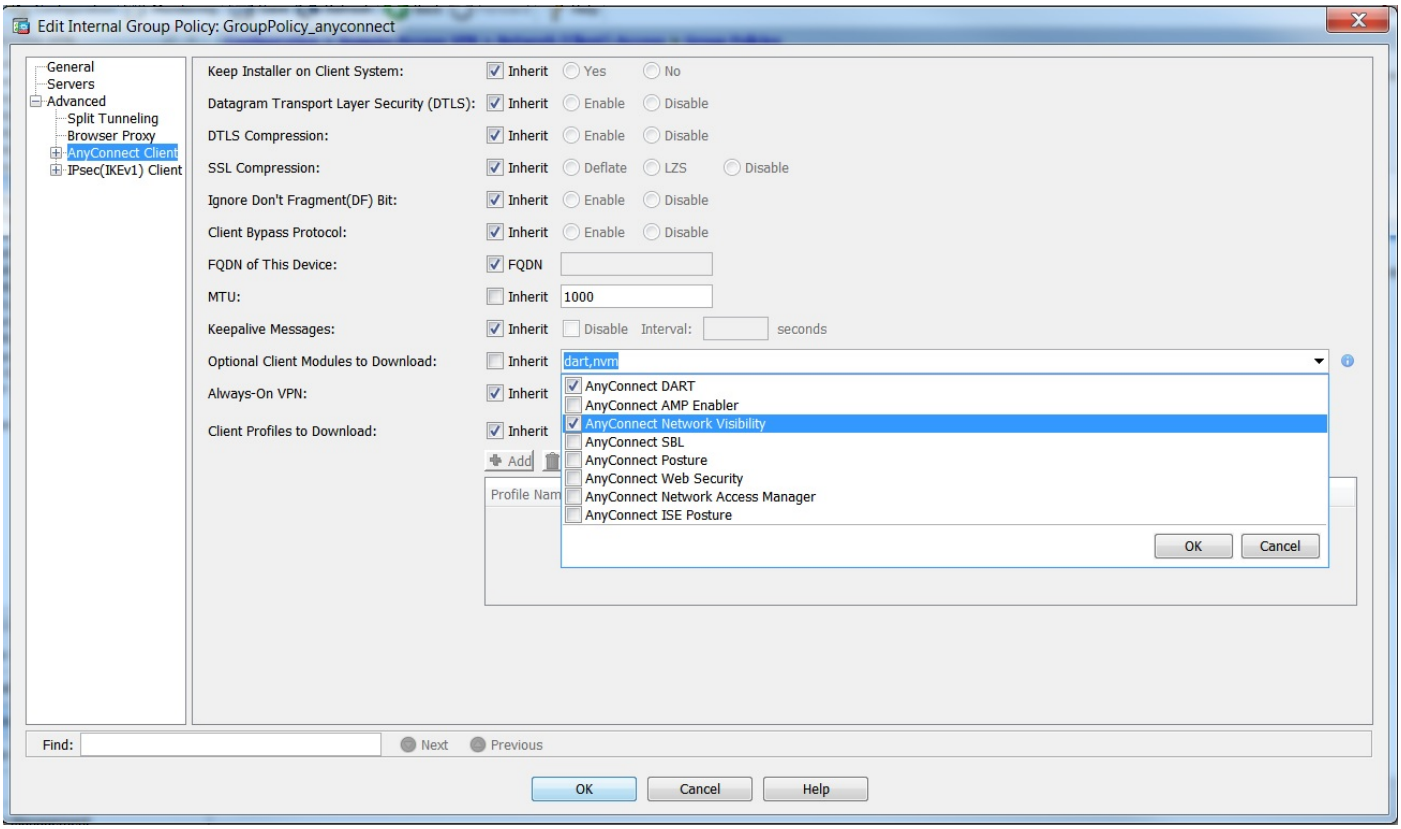
2. 関連グループ ポリシーを選択し、[Edit]をクリックします。



3. グループ ポリシー ポップアップ内で、[Advanced] > [AnyConnect Client]を選択します。

4. [Optional Client Modules to Download]を展開し、[AnyConnect Network Visibility] を選択します。

5. [OK]をクリックし、変更を適用します。



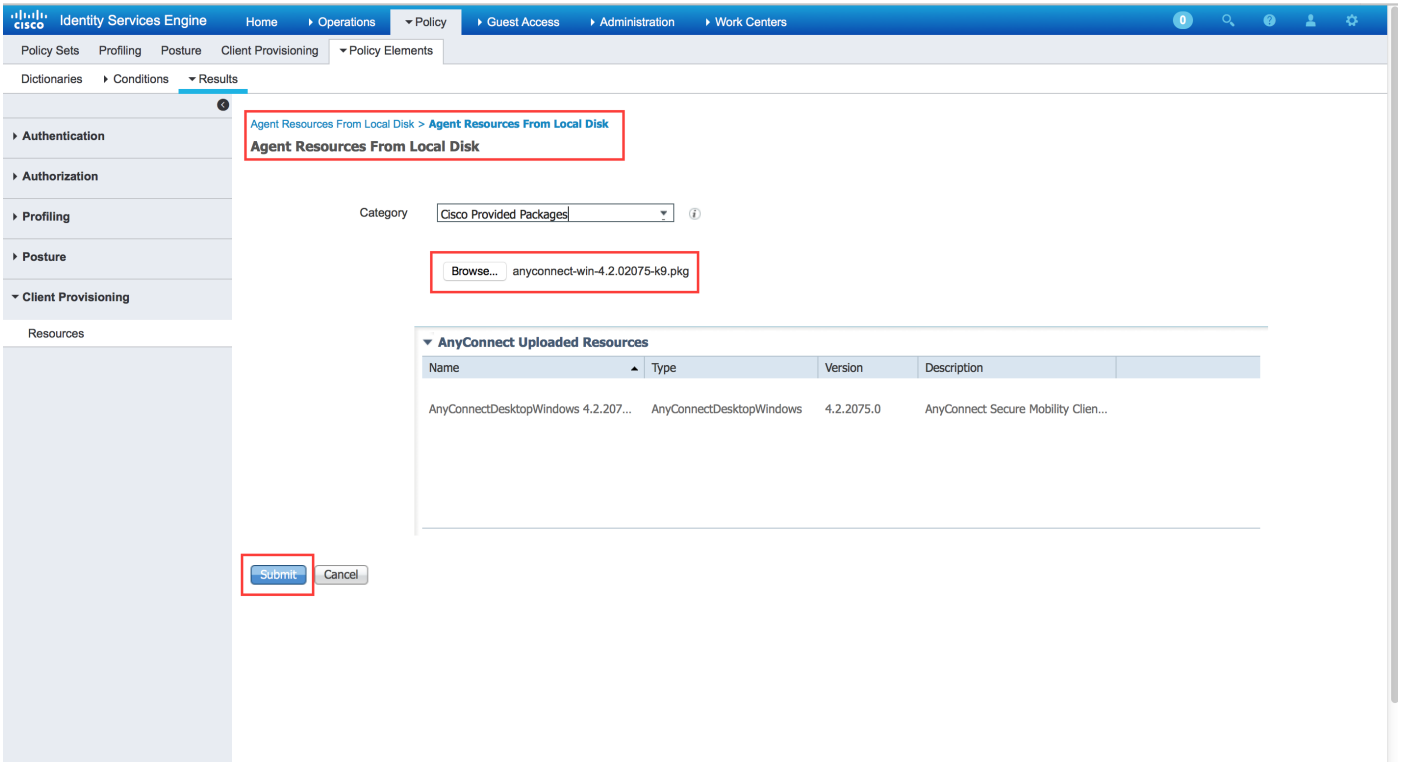
Cisco ISE 上での Web 展開の設定

- Cisco ISE を AnyConnect Web 展開用に設定するには、次の手順を実行します。

- Cisco ISE GUI で、[Policy] > [Policy Elements] > [Results]を選択します。
- [Client Provisioning]を展開して [Resources] を表示し、[Resources] を選択します。

AnyConnect イメージの追加

[Add] > [Agent Resources]を選択し、AnyConnect パッケージ ファイルをアップロードします。



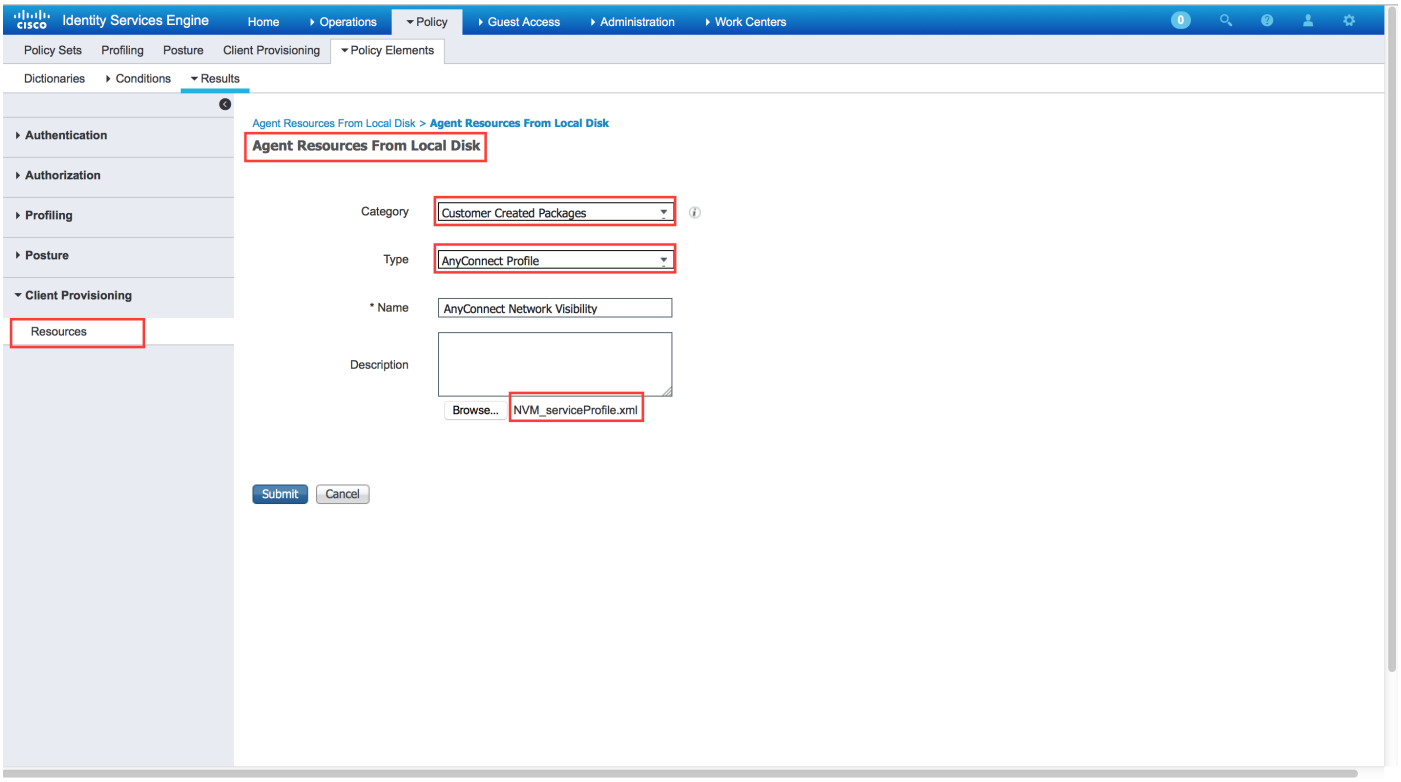
ポップアップでパッケージのハッシュを確認します。

ファイルハッシュは、Cisco.com ダウンロード ページで照会するか、またはサードパーティ製ツールを使用して確認できます。

複数の AnyConnect イメージを追加するには、この手順を繰り返すことができます（Mac OSX および Linux OS の場合）。

AnyConnect NVM プロファイルの追加：

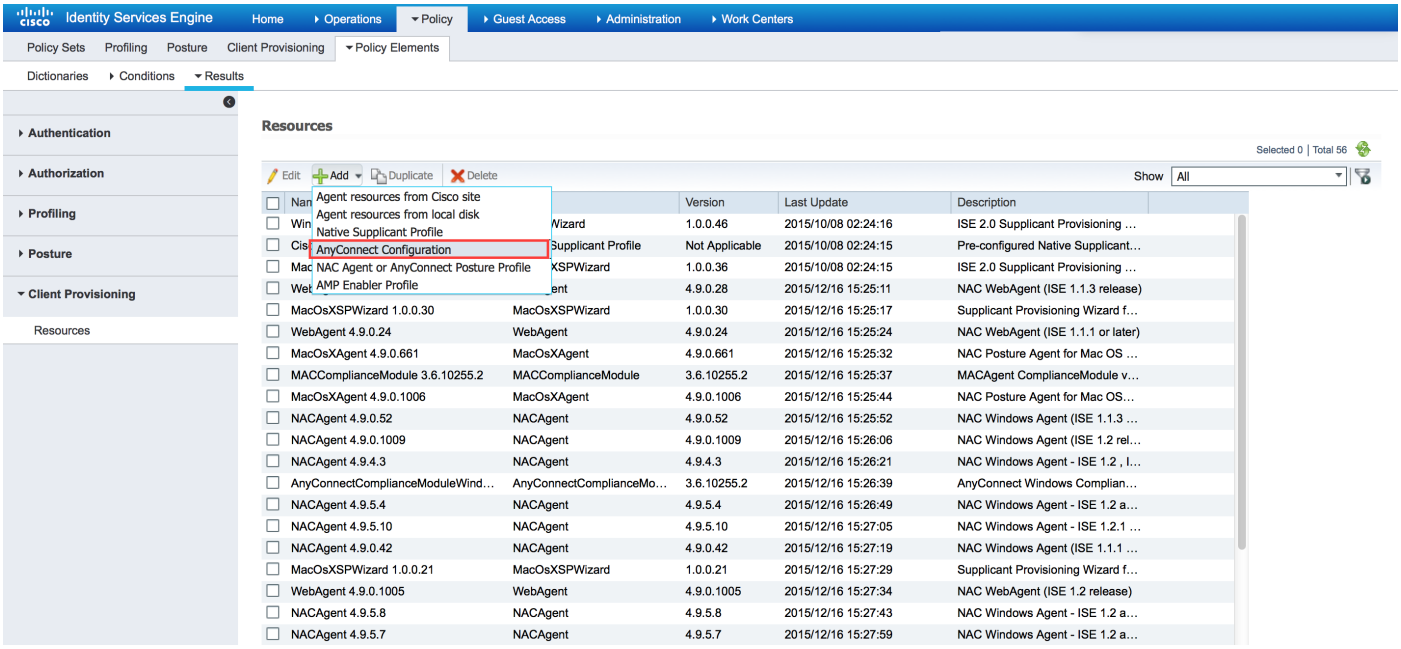
[Add] > [Agent Resources]を選択し、NVM クライアント プロファイルをアップロードします。



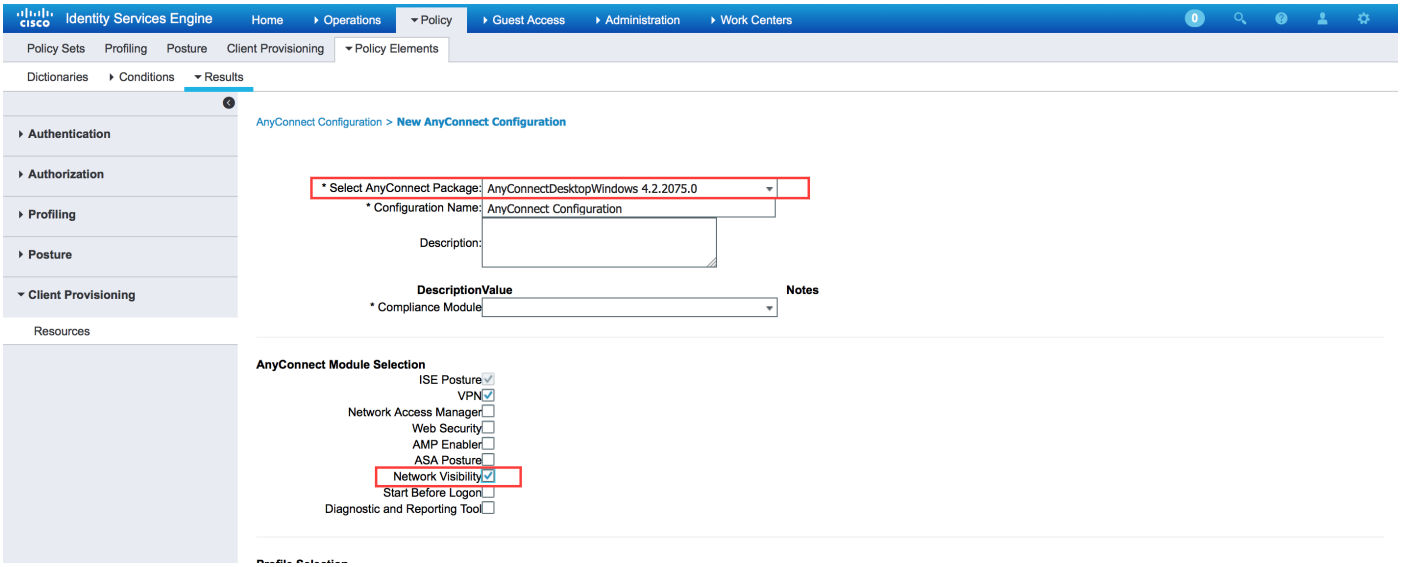
AnyConnect 設定ファイルの追加：

[Add]> **[AnyConnect Configuration]** の順にクリックします。

前のステップでアップロードしたパッケージを選択します。



[AnyConnect Module Selection]内の [NVM] を、必要なポリシーとともに有効にします。



上のセクションでは、AnyConnect Client モジュール、プロファイル、カスタマイズ/言語パッケージ、および Opswat パッケージを有効にしました。

Cisco ISE 上の Web 展開設定に関する詳細情報については、以下を参照してください。

[AnyConnect の Web 展開]

信頼ネットワーク検出

NVM は、信頼ネットワーク内にある場合にのみフロー情報を送信します。 これはエンドポイントが信頼ネットワーク内にあるかどうかを調べるために、AnyConnect クライアントの TND 機能を使用します。 TND は、エンドポイントが信頼ネットワーク内にあるかどうかを判断するために、DNS/ドメイン情報を使用します。 VPN は、接続されると、信頼ネットワーク内にあると見なされ、フロー情報はコレクタに送信されます。

TND は、NVM が正しく機能するために、正しく設定される必要があります。 TND 設定の詳細については、次を参照してください。

[信頼ネットワーク検出の設定]

展開

AnyConnect NVM ソリューションの展開には、次の手順が関係しています。

1. Cisco ASA/ISE 上での AnyConnect NVM の設定

2. IPFIX コレクタ コンポーネントの設定

3. Cisco NVM アプリケーションでの Splunk のセットアップ

ステップ 1：Cisco ASA/ISE 上での AnyConnect NVM の設定

この手順は、「設定」のセクションで詳しく扱われています。

NVM を Cisco ISE/ASA 上で設定すると、クライアント エンドポイントに自動展開できます。

手順 2：IPFIX コレクタ コンポーネントの設定

コレクタ コンポーネントはエンドポイントからすべての IPFIX データを収集して変換し、それを Splunk アプリケーションに転送します。 さまざまなサードパーティのコレクタ ツールを利用できますが、Cisco NVM は IPFIX を理解するすべてのコレクタと互換性があります。 この TechNote では、64 ビット Linux 上で稼働するシスコ製のコレクタ ツールを使用します。 CentOS および Ubuntu 設定スクリプトは、Splunk アプリケーションに含まれています。 CentOS のインストール スクリプトおよび設定ファイルは、Fedora や Redhat のディストリビューションでも使用できます。 コレクタは、スタンドアロン 64 ビット Linux システム、または 64 ビット Linux 上で稼働する Splunk Forwarder のいずれかの上で実行する必要があります。

コレクタをインストールするには、APP_DIR/appserver/addon/ ディレクトリにある CiscoNVMCollector_TA.tar ファイル内のアプリケーションを、インストールを予定しているシステムにコピーする必要があります。

この TechNote では、Splunk は E: ドライブの Windows ワークステーションにインストールされます。 ドライブにします。

CiscoNVMCollector_TA.tar ファイルは、以下のディレクトリ内にあります。

```
E:\Program Files\Splunk\etc\apps\CiscoNVM\appserver\addon\
```

コレクタのインストールを予定しているシステム上で tar ファイルを抽出し、スーパー ユーザ権限で install.sh スクリプトを実行します。 install.sh スクリプトを実行する前に、.tar バンドル内の $PLATFORM$_README ファイルを読むことをお勧めします。 $PLATFORM$_README ファイルには、install.sh スクリプトを実行する前に確認および（必要であれば）変更が求められる、関連する構成設定についての情報が記載されています。

Ubuntu サーバ上のコレクタのディレクトリ：

```
root@ubuntu-splunkcollector:~/Downloads/CiscoNVMCollector_TA$ ls
acnvmcollector   CENTOS_README                  libboost_log.so.1.57.0
acnvmcollectord  install_centos.sh              libboost_system.so.1.57.0
acnvm.conf       install.sh                     libboost_thread.so.1.57.0
acnvm.conf~      install_ubuntu.sh              UBUNTU_README
acnvm.service    libboost_filesystem.so.1.57.0
root@ubuntu-splunkcollector:~/Downloads/CiscoNVMCollector_TA$
```

情報は、構成ファイル（acnvm.conf）内で設定する必要があります。

1. Splunk インスタンスの IP アドレスとリスニング ポート。

2. コレクタ（着信 IPFIX データ）のリスニング ポート。

フローごとのデータ ポート、エンドポイント ID データ ポート、およびコレクタ ポートは、設定ファイル内でデフォルト設定に事前設定されています。 デフォルト以外のポートを使用する場合は、これらの値を必ず変更します。

この情報は、設定ファイル（acnvm.conf）に追加されます。

```
  GNU nano 2.2.6                          File: acnvm.conf

{
```

```
"syslog_server_ip" : "192.0.2.113",
"syslog_flowdata_server_port" : 20519,
"syslog_sysdata_server_port" : 20520,
"netflow_collector_port" : 2055,
"log_level" : 7
}
```

詳細については、次のサイトを参照してください。

https://splunkbase.splunk.com/app/2992/#/documentation

手順 3：Cisco NVM アプリケーションでの Splunk のセットアップ

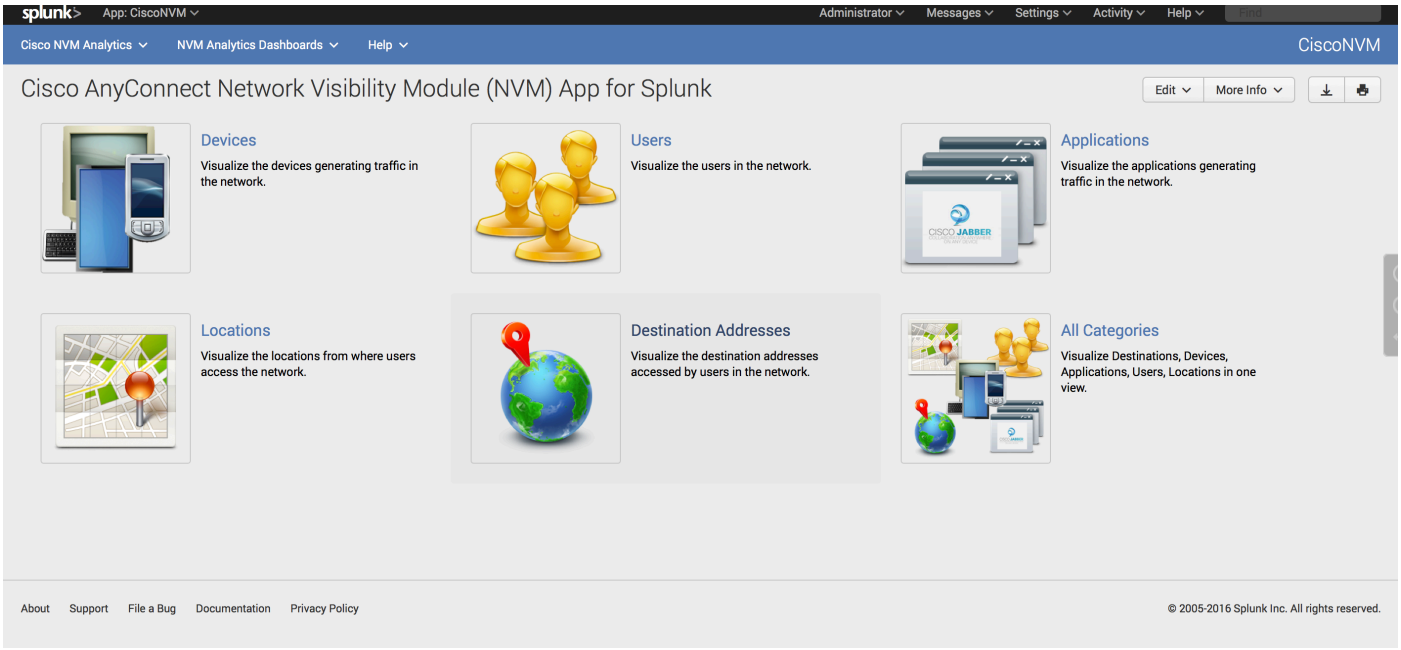
Cisco AnyConnect NVM App for Splunk は、Splunkbase 上で使用できます。 このアプリケーションは、事前定義レポートやダッシュボードで、有用なレポートによるエンドポイントからの IPFIX（nvzFlow）データを使用するために役立ちます。また、ユーザとエンドポイントの動作を相関させます。

Splunkbase 上での Cisco NVM アプリケーションのリンク：

https://splunkbase.splunk.com/app/2992/

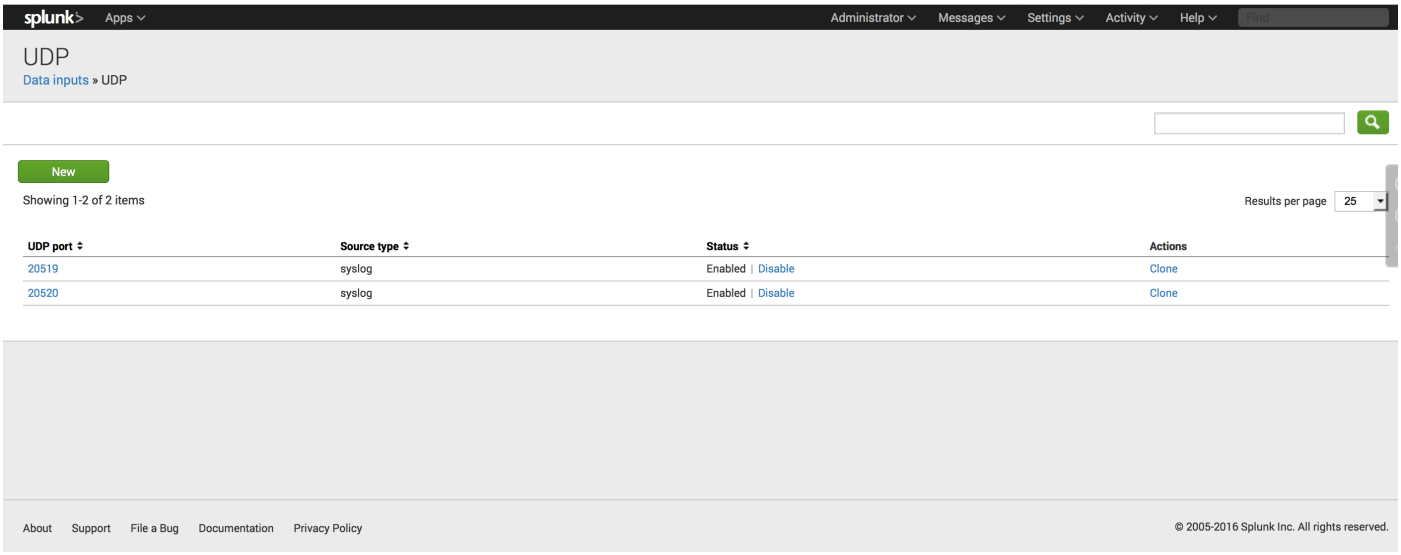
インストール：

[Splunk] > [Apps]と選択し、Splunkbase からダウンロードしたかまたは [Apps] セクション内で検索した **tar.gz** ファイルをインストールします。



デフォルトでは、Splunk はフローごとのデータおよびエンドポイント ID データの 2 つのデータ入力フィードを、UDP ポート 20519 および 20520 でそれぞれ受け取ります。 コレクタ コンポーネントは、デフォルトではこれらのポートでフィードを送信します。 Splunk ではデフォルトのポートは変更できます。しかし、コレクタ設定では同じポートを指定する必要があります（手順 2 を参照）。

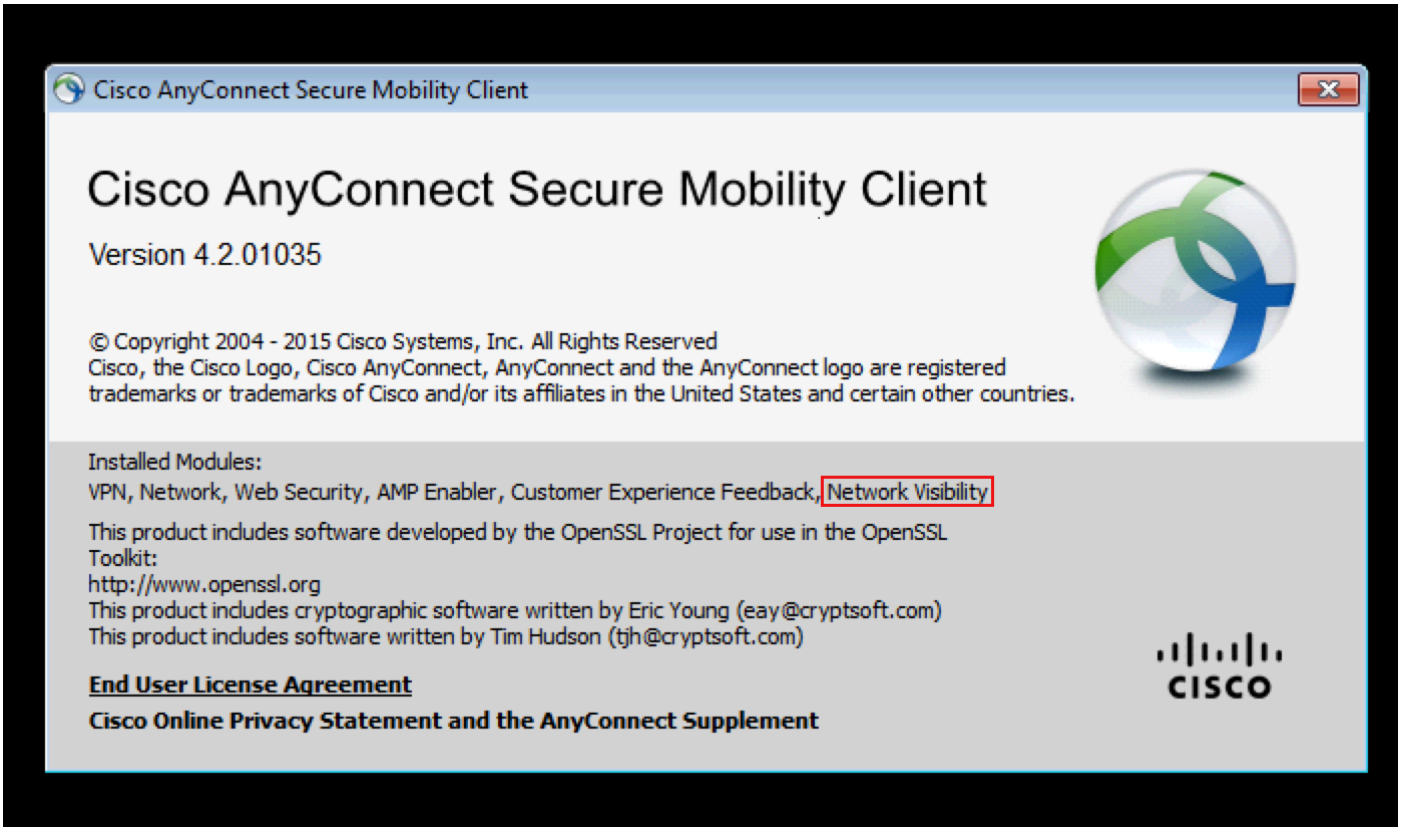
デフォルトのポートを変更するには、[Splunk] > [Settings] > [Data Input] > [UDP]を選択します。



確認

AnyConnect NVM インストールの検証

インストールが成功したら、Network Visibility Module が、AnyConnect Secure Mobility クライアントの**情報セクション**内にある [Installed Modules] にリストされます。



また、nvm サービスがエンドポイント上で実行しており、プロファイルが要求されたディレクトリ内にあることを確認します。

コレクタの実行中ステータスの確認

コレクタのステータスが実行中であることを確認します。 これにより、コレクタがエンドポイントから常時 IPFIX/cflow を受信していることを確認できます。

```
  GNU nano 2.2.6                                File: acnvm.conf

{
"syslog_server_ip" : "192.0.2.113",
"syslog_flowdata_server_port" : 20519,
"syslog_sysdata_server_port" : 20520,
"netflow_collector_port" : 2055,
"log_level" : 7
}
```

Splunk の検証

Splunk と関連サービスが実行していることを確認します。 Splunk のトラブルシューティングに関する資料については、Splunk の Web サイトを参照してください。

トラブルシューティング

パケット フロー

1. IPFIX パケットは、AnyConnect NVM モジュールによってクライアント エンドポイントで生成されます。

2. クライアント エンドポイントは、IPFIX パケットをコレクタ IP アドレスに転送します。

3. コレクタは情報を収集して、Splunk に転送します。

4. コレクタは、トラフィックを Splunk に、次の 2 つの異なるストリームで送信します。 つまり、フローごとのデータと、エンドポイント ID データです。

すべてのトラフィックは UDP ベースであり、トラフィックの確認はありません。

トラフィックのデフォルト ポート：

IPFIX データ　　2055

フローごとのデータ 20519

フローごとのデータ 20520

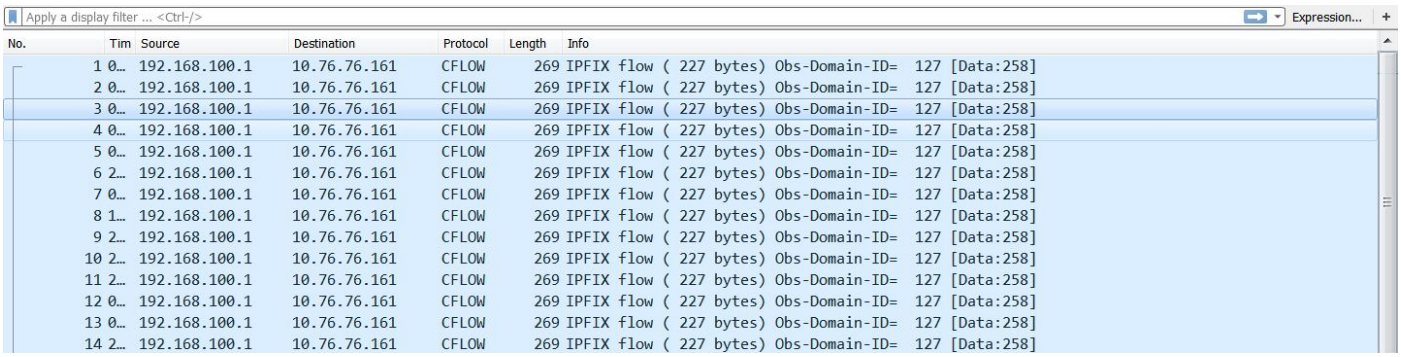
NVM モジュールは IPFIX データをキャッシュに入れ、信頼ネットワーク内であればそれをコレクタに送信します。 これは、ラップトップが社内ネットワーク（on-prem）に接続されているか、または VPN を介して接続されているかのいずれかの場合に実行されます。

基本的なトラブルシューティング ステップ

- クライアント エンドポイントとコレクタとの間のネットワーク接続を確認します。
- コレクタと Splunk との間のネットワーク接続を確認します。
- NVM がクライアント エンドポイントに正しくインストールされていることを確認します。
- IPFIX トラフィックが生成されているかどうかを確認するには、エンドポイントにキャプチ

ャを適用します。
- IPFIX トラフィックを受信しているかどうか、およびトラフィックを Splunk に転送しているかどうかを確認するために、コレクタにキャプチャを適用します。
- トラフィックを受信しているかどうかを確認するには、Splunk にキャプチャを適用します。

Wireshark に表示される IPFIX トラフィック：



信頼ネットワーク検出（TND）

NVM は、TND に依存して、エンドポイントが信頼ネットワーク内にあるときを検出します。TND 設定が誤っている場合、NVM の問題が発生する原因になります。

TND は DHCP を介して受け取る情報に基づいて動作します。 ドメイン名および DNS サーバ。DNS サーバまたはドメイン名（あるいはその両方）が設定値と一致する場合、ネットワークは信頼できると見なされます。

NVM がトラフィックをコレクタに転送しない場合、TND に問題がある可能性があります。

フロー テンプレート

IPFIX フロー テンプレートは、IPFIX 通信の開始時にコレクタに送信されます。 これらのテンプレートは、コレクタが IPFIX データの意味を解明するために役立ちます。 この情報がコレクタに送信されないと、コレクタは IPFIX データを収集できません。 これにより、データ コレクションに関する問題が発生します。

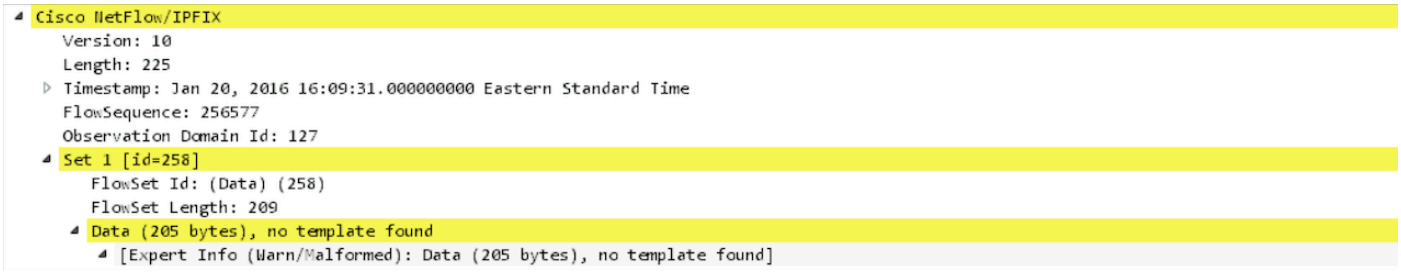
このような問題は、コレクタが後から設定された場合や、IPFIX の最初の数パケットがネットワークでドロップする場合（VPN では一般的）に見られます。 これを軽減するには、次のイベントの 1 つが必要です。

1. NVM クライアント プロファイルに変更がある。
2. ネットワーク変更イベントがある。
3. nvmagent サービスが再起動する。
4. エンドポイントがリブート/再起動する。

この問題は、エンドポイントをリブートするか、VPN を再接続することで回復できる可能性があります。

この問題は、エンドポイントのパケット キャプチャ内の **no template found**、またはコレクタ ログ内の **no templates for flowset** を確認することで特定できます。

パケット キャプチャ



コレクタ ログ：

```
  GNU nano 2.2.6                                File: acnvm.conf

{
"syslog_server_ip" : "192.0.2.113",
"syslog_flowdata_server_port" : 20519,
"syslog_sysdata_server_port" : 20520,
"netflow_collector_port" : 2055,
"log_level" : 7
}
```

Recommended Release

シスコは常に、使用時または更新時に最新ソフトウェア バージョンの AnyConnect を選択するように推奨しています。 AnyConnect のバージョンを選択するときは、最新の 4.2.x または 4.3.x クライアントを使用してください。 これにより各 NVM に最新の拡張と不具合の修正が提供され、最近の変更は Microsoft コード署名証明書の適用により緩和されます。 詳細については、こちらをご覧ください。

関連する不具合

1. CSCva21660：acnvmagent.exe*32 プロセスの AnyConnect NVM ハンドル/リーク

関連リンク

1. Cisco AnyConnect Network Visibility（NVM）App for Splunk：https://splunkbase.splunk.com/app/2992/
2. Splunk コレクタのセットアップおよびコレクタ スクリプトのインストールに関する Splunk の資料： https://splunkbase.splunk.com/app/2992/#/documentation
3. 『Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.3』
4. AnyConnect 4.3 のリリース ノート