

FDMによって管理されるFTDでのリモート・アクセスVPNの構成

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[ライセンス](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[FTDでのライセンスの確認](#)

[保護されたネットワークの定義](#)

[ローカル ユーザの作成](#)

[証明書の追加](#)

[リモートアクセスVPNの設定](#)

[確認](#)

[トラブルシューティング](#)

[AnyConnectクライアントの問題](#)

[初期接続の問題](#)

[トラフィック固有の問題](#)

はじめに

このドキュメントでは、バージョン6.5.0以降を実行するオンボックスマネージャFDMによって管理されるFTD上のRA VPNの展開を設定する方法について説明します。

前提条件

要件

シスコでは、Firepower Device Manager(FDM)でのリモートアクセス仮想プライベートネットワーク(RA VPN)の設定に関する知識があることを推奨します。

ライセンス

- Firepower脅威対策(FTD)がスマートライセンスポータルに登録され、エクスポート制御機能が有効になっている (RA VPN設定タブを有効にするために)
- 有効なAnyConnectライセンス (APEX、Plus、またはVPN-Only)

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いています。

- バージョン6.5.0-115が稼働するCisco FTD
- Cisco AnyConnect セキュア モビリティ クライアント バージョン 4.7.01076

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

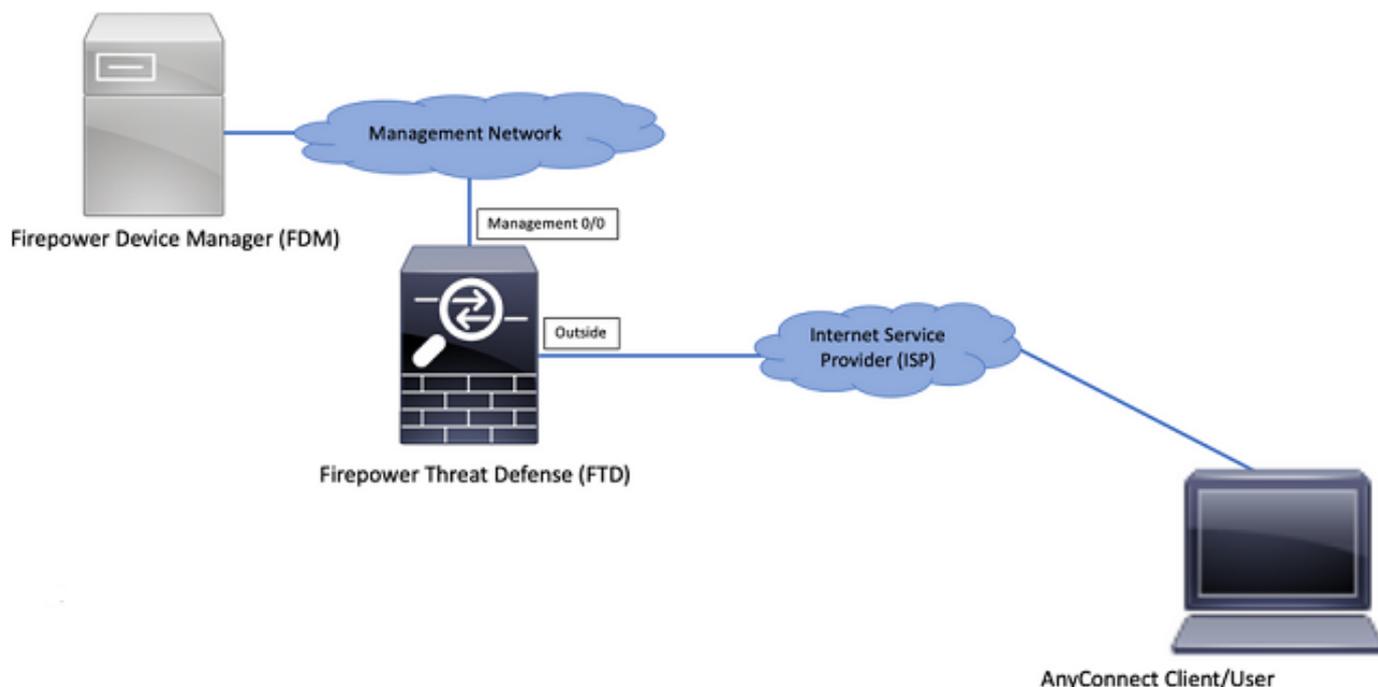
背景説明

FDMを使用したFTDの設定では、同じインターフェイスから管理にアクセスしている間に、外部インターフェイスを使用してAnyConnectクライアントの接続を確立しようとするると困難が生じます。これは、FDMの既知の制限です。この問題については、機能拡張要求[CSCvm76499](#)が提起されています。

設定

ネットワーク図

ローカルを使用したAnyConnectクライアント認証。



FTDでのライセンスの確認

ステップ 1：図に示すように、デバイスがスマートライセンスに登録されていることを確認します。

The screenshot displays the Cisco Firepower Device Manager interface for a device named 'firepower'. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device: firepower'. The main header shows the device model 'Cisco Firepower Threat Defense for VMWa...', software version '6.5.0-115', VDB '309.0', and rule update '2019-08-12-001-vrt'. A 'High Availability' status is shown as 'Not Configured' with a 'CONFIGURE' button.

The central diagram illustrates the device's network configuration, showing an 'Inside Network' connected to the device via interface 'o/1'. The device has three interfaces: 'o/0', 'o/1', and 'o/2'. It is also connected to an 'ISP/WAN/Gateway' and an 'Internet' cloud. Services like 'DNS Server', 'NTP Server', and 'Smart License' are shown as configured.

The main content area is a grid of configuration tiles:

- Interfaces:** Connected, Enabled 3 of 4. [View All Interfaces](#)
- Smart License:** Registered. [View Configuration](#) (highlighted with a red box)
- Routing:** There are no routes yet. [Create the first static route](#)
- Updates:** Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds. [View Configuration](#)
- Backup and Restore:** [View Configuration](#)
- Troubleshoot:** No files created yet. [REQUEST FILE TO BE CREATED](#)
- System Settings:** Management Access, Logging Settings, DHCP Server, DNS Server, Management Interface, Hostname, NTP, Cloud Services, Reboot/Shutdown, Traffic Settings, URL Filtering Preferences.
- Site-to-Site VPN:** There are no connections yet. [View Configuration](#)
- Remote Access VPN:** Requires RA VPN license. No connections | 1 Group Policy. [View Configuration](#)
- Advanced Configuration:** Includes: FlexConfig, Smart CLI. [View Configuration](#)
- Device Administration:** Audit Events, Deployment History, Download Configuration. [View Configuration](#)

ステップ 2：次の図に示すように、デバイスでAnyConnectライセンスが有効になっていることを確認します。

Device Summary
Smart License

CONNECTED SUFFICIENT LICENSE
Last sync: 04 Apr 2020 02:10 PM
Next sync: 04 Apr 2020 02:20 PM
Go to Cloud Services

SUBSCRIPTION LICENSES INCLUDED

Threat ENABLE

Disabled by user

This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies that control files based on file type.

Includes: Intrusion Policy

Malware ENABLE

Disabled by user

This License allows you to perform Cisco Advanced Malware Protection (AMP) with AMP for Firepower and AMP Threat Grid. You must have this license to apply file policies that detect and block malware in files transmitted over your network.

Includes: File Policy

URL License ENABLE

Disabled by user

This license allows you to control web access based on URL categories and reputations, rather than by individual URL alone. You must have this license to deploy access rules that filter web traffic based on category and reputation.

Includes: URL Reputation

RA VPN License Type: APEX AND PLUS DISABLE

Enabled

Please select the license type that you purchased to enable remote access VPN. Note that Firepower Device Manager does not support any of the advanced features covered by the Apex license.

Includes: RA-VPN

PERPETUAL LICENSES INCLUDED

Base License ENABLED ALWAYS

Enabled

ステップ3：図に示すように、トークンでエクスポート制御の機能が有効になっていることを確認します。

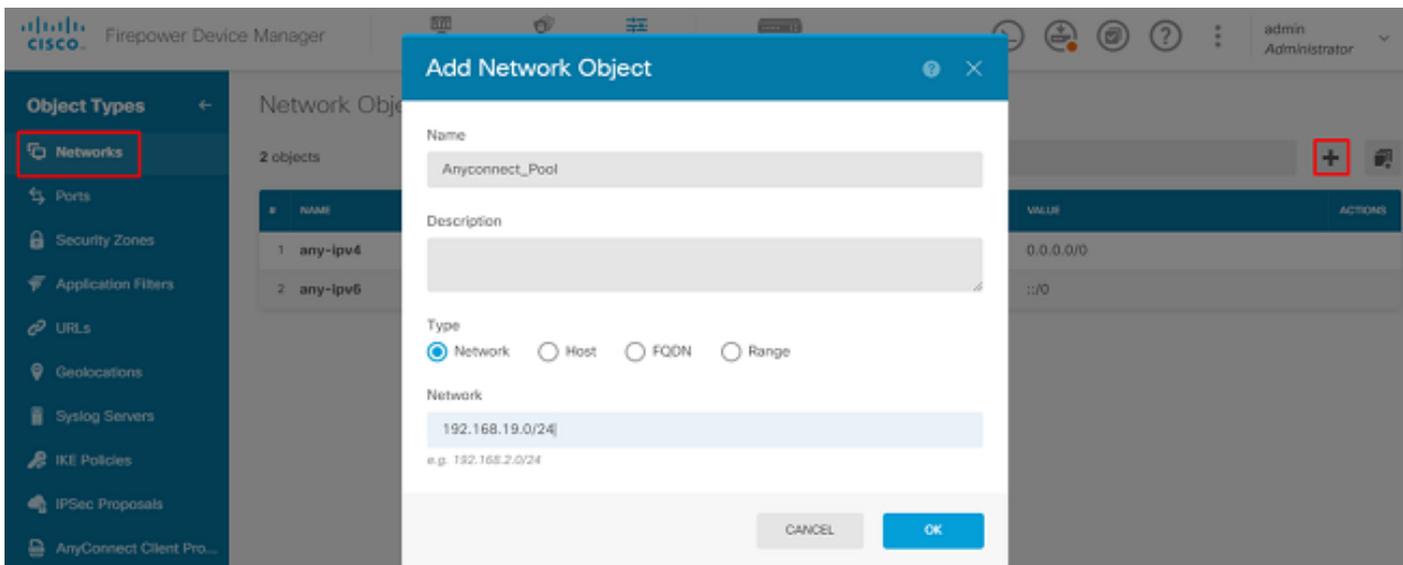
Device Summary
Smart License

CONNECTED SUFFICIENT LICENSE
Last sync: 04 Apr 2020 02:10 PM
Next sync: 04 Apr 2020 02:20 PM

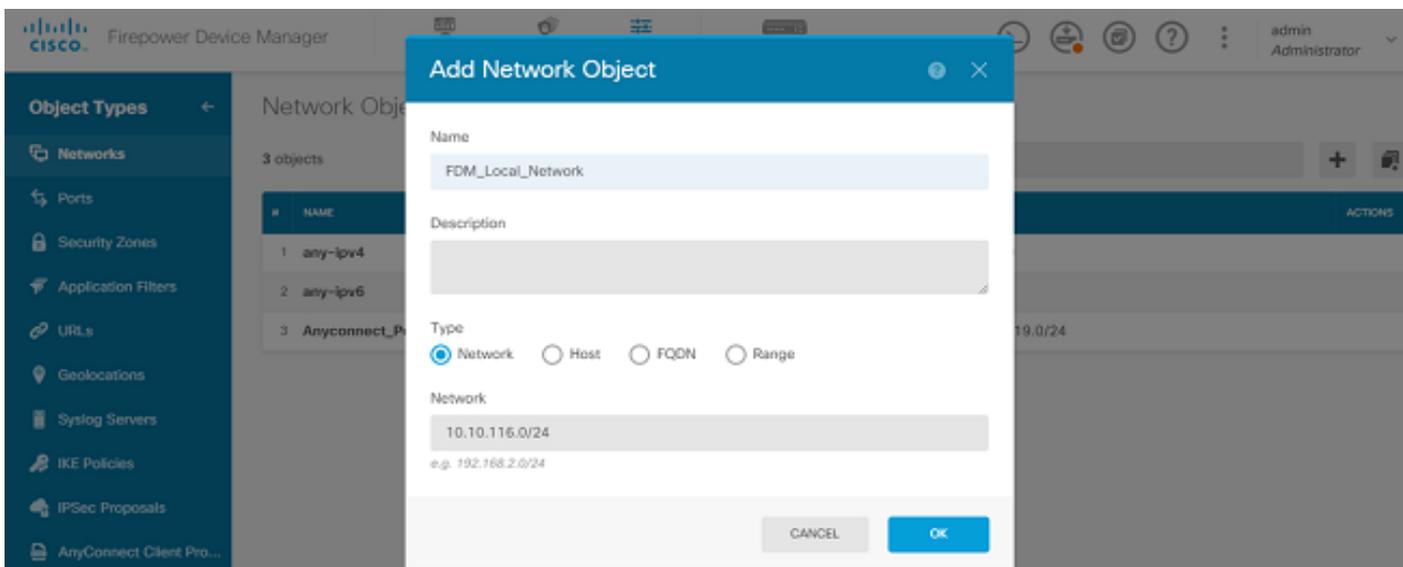
Assigned Virtual Account: SEC TAC
Export-controlled features: Enabled
Go to [Cisco Smart Software Manager](#).

保護されたネットワークの定義

移動先 Objects > Networks > Add new Network を参照。FDM GUIからVPNプールとLANネットワークを構成します。図に示すように、AnyConnectユーザへのローカルアドレス割り当てに使用するVPNプールを作成します。

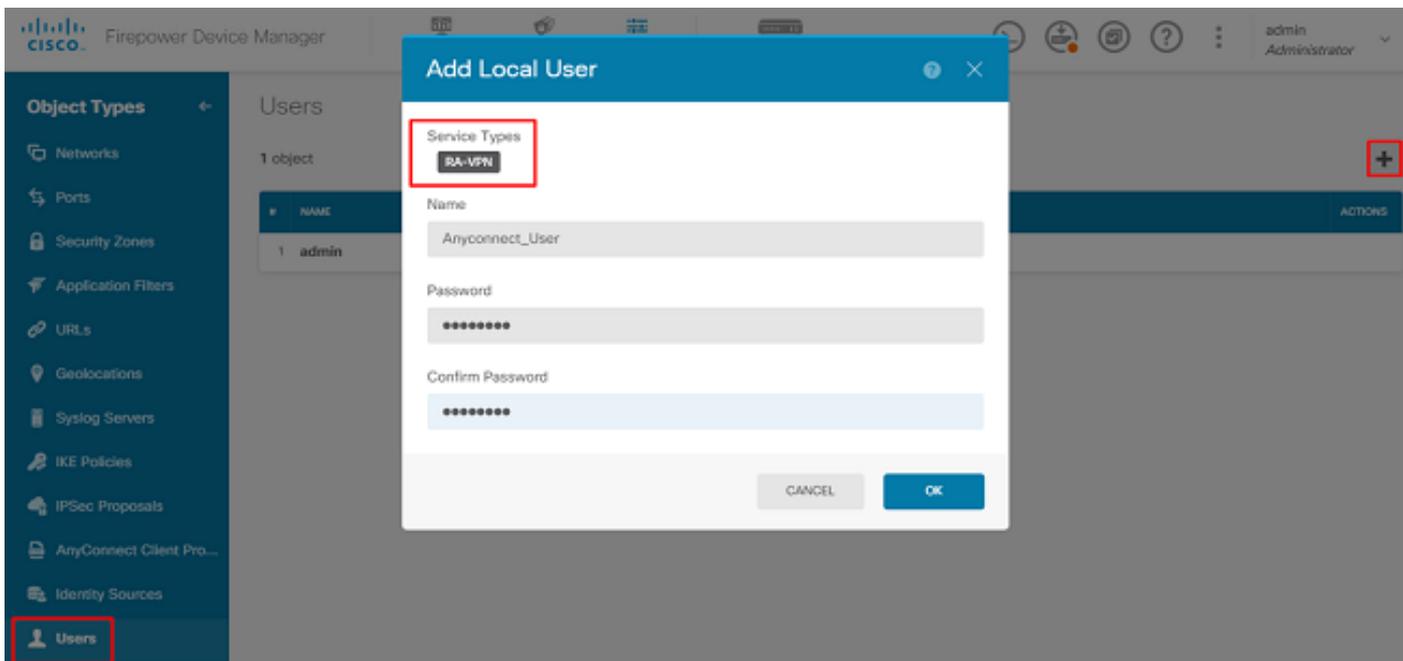


図に示すように、FDMデバイスの背後にあるローカル・ネットワークのオブジェクトを作成します：



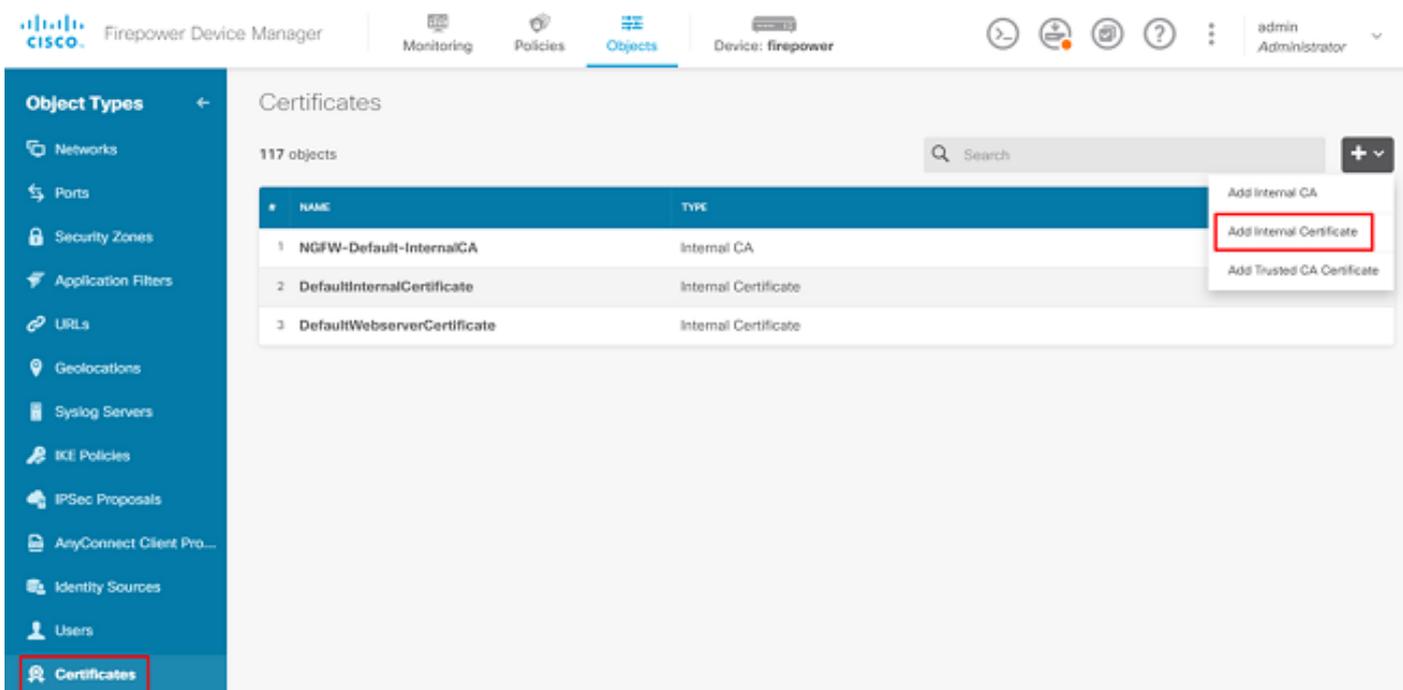
ローカル ユーザの作成

移動先 [Objects > Users > Add User](#) を参照。Anyconnect経由でFTDに接続するVPNローカルユーザを追加します。次の図に示すように、ローカルユーザを作成します。



証明書の追加

移動先 Objects > Certificates > Add Internal Certificate を参照。図に示すように、証明書を設定します。



図に示すように、証明書と秘密キーの両方をアップロードします。



Choose the type of internal certificate you want to create



Upload Certificate and Key

Create a certificate from existing files.
PEM and DER files are supported.



Self-Signed Certificate

Create a new certificate that is signed
by the device.

証明書とキーは、次の図に示すように、コピーアンドペーストまたは各ファイルのアップロードボタンでアップロードできます。

Add Internal Certificate



Name

Anyconnect_Certificate

SERVER CERTIFICATE (USER AGENT)

Paste certificate, or choose file:

UPLOAD CERTIFICATE

The supported formats are: PEM, DER.

```
wkM7QqtRuyzBzGhnoSebJkP/Hiky/Q+r6UrYSnv++UJSrg777/9NgonwTpLI/8/J
idGSN0b/ic6iPh2aGpB1Lra3MGCL1pJaRqxq3+1yBDsfVFCaKT9wWcnUveQd6LZp
k+iaN+V24yOj3vCJILihtxwdllqeSs8F8XdaL4LQObcTfZ/3YNBWqvwV2TL
-----END CERTIFICATE-----
```

CERTIFICATE KEY

Paste key, or choose file:

UPLOAD KEY

The supported formats are: PEM, DER.

```
QzYPpjCgYEAqJ9nlk8sfPfmotyOwprlBEdwMMDeKLX3KDY58jviv1/8a/wsX+uz
3A7VQn6gA6ISWHgxHdmqYnD38P6kCuK/hQMUCqdIKUITXkh0ZpglQbfW2lJ0VD4M
gKugRI5t0Zva5j+bQ5q0f8D/mtYYTBf8JGqqEfSju0Zsy2ifWtsbJrE=
-----END RSA PRIVATE KEY-----
```

CANCEL

OK

リモートアクセスVPNの設定

移動先 [Remote Access VPN > Create Connection Profile](#) を参照。図に示すように、FDMでRA VPNウィザードを移動します。

Firepower Device Manager

Monitoring Policies Objects Device: firepower

Model: Cisco Firepower Threat Defense for VMWa... Software: 6.5.0-115 VDB: 309.0 Rule Update: 2019-08-12-001-vrt High Availability: Not Configured

Interfaces: Connected, Enabled 3 of 4. View All Interfaces

Smart License: Registered. View Configuration

Site-to-Site VPN: There are no connections yet. View Configuration

Remote Access VPN: Configured, No connections | 1 Group Policy. View Configuration

Advanced Configuration: Includes: FlexConfig, Smart CLI. View Configuration

System Settings: Management Access, Logging Settings, DHCP Server, DNS Server, Management Interface, Hostname, NTP, Cloud Services, Reboot/Shutdown, Traffic Settings, URL Filtering Preferences

Device Administration: Audit Events, Deployment History, Download Configuration. View Configuration

Firepower Device Manager

Monitoring Policies Objects Device: firepower

RA VPN

Connection Profiles

Group Policies

Device Summary: Remote Access VPN Connection Profiles

Search

+	NAME	AAA	GROUP POLICY	ACTIONS
There are no Remote Access Connections yet. Start by creating the first Connection.				

CREATE CONNECTION PROFILE

図に示すように、接続プロファイルを作成し、設定を開始します。

Connection and Client Configuration

Specify how to authenticate remote users and the AnyConnect clients they can use to connect to the inside network.

Connection Profile Name

This name is configured as a connection alias, it can be used to connect to the VPN gateway

Anyconnect

Group Alias

Anyconnect

[Add Group Alias](#)

Group URL

[Add Group URL](#)

図に示すように、認証方式を選択します。このガイドでは、ローカル認証を使用します。

Primary Identity Source

Authentication Type

AAA Only Client Certificate Only AAA and Client Certificate

Primary Identity Source for User Authentication

LocalIdentitySource

Fallback Local Identity Source

Please Select Local Identity Source

Strip Identity Source server from username

Strip Group from Username

Secondary Identity Source

Secondary Identity Source for User Authentication

Please Select Identity Source

Advanced

Authorization Server

Please select

Accounting Server

Please select

次のいずれかを選択します Anyconnect_Pool 図に示すオブジェクト :

Client Address Pool Assignment

IPv4 Address Pool

Endpoints are provided an address from this pool



Anyconnect_Pool

IPv6 Address Pool

Endpoints are provided an address from this pool



DHCP Servers



CANCEL

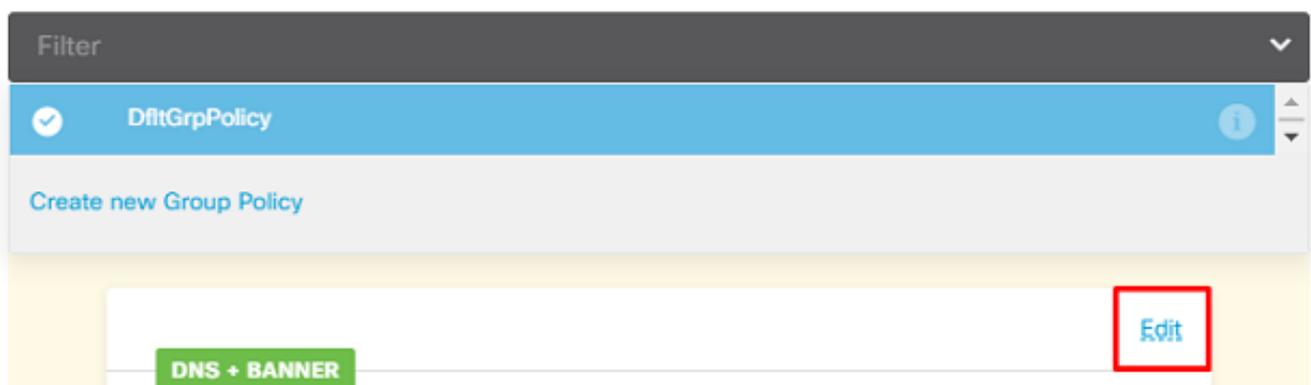
NEXT

デフォルトのグループポリシーの要約が次のページに表示されます。新しいグループポリシーは、ドロップダウンをクリックして次のオプションを選択すると作成できます [Create a new Group Policy](#) を参照。このガイドでは、デフォルトのグループポリシーが使用されます。図に示すように、ポリシーの上部にある編集オプションを選択します。

Remote User Experience

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

View Group Policy



グループポリシーで、スプリットトンネリングを追加します。これにより、Anyconnectに接続されたユーザは、Anyconnectクライアントを介して内部FTDネットワーク宛てのトラフィックのみを送信し、他のすべてのトラフィックは図に示すようにユーザのISP接続から送信されます。

Corporate Resources (Split Tunneling)

IPv4 Split Tunneling

Allow specified traffic over tunnel ▼

IPv6 Split Tunneling

Allow all traffic over tunnel ▼

IPv4 Split Tunneling Networks

+

FDM_Local_Network

次のページで、Anyconnect_Certificate 「証明書」セクションに追加されました。次に、FTDがAnyConnect接続をリッスンするインターフェイスを選択します。復号化されたトラフィックのBypass Access Controlポリシー(sysopt permit-vpn)。このコマンドは、sysopt permit-vpn が選択されていません。次の図に示すように、Anyconnectクライアントからのトラフィックが内部ネットワークにアクセスできるようにするアクセスコントロールポリシーを作成する必要があります。

Global Settings

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

Certificate of Device Identity

Anyconnect_Certificate ▼

Outside Interface

outside (GigabitEthernet0/0) ▼

Fully-qualified Domain Name for the Outside Interface

e.g. ravpn.example.com

Access Control for VPN Traffic

Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

NAT免除は、Policies > NAT または、ウィザードで自動的に設定することもできます。図に示すように、Anyconnectクライアントがアクセスするために必要な内部インターフェイスとネットワークを選択します。

NAT Exempt



Inside Interfaces

The interfaces through which remote access VPN users can connect to the internal networks



inside (GigabitEthernet0/1)

Inside Networks

The internal networks remote access VPN users are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.



FDM_Local_Network

図に示すように、ユーザが接続できる各オペレーティングシステム(Windows/Mac/Linux)の Anyconnectパッケージを選択します。

AnyConnect Package

If a user does not already have the right AnyConnect package installed, the system will launch the AnyConnect installer when the client authenticates for the first time. The user can then install the package from the system.

You can download AnyConnect packages from software.cisco.com. You must have the necessary AnyConnect software license.

Packages

UPLOAD PACKAGE

Windows: anyconnect-win-4.7.04056-webdeploy-k9.pkg

BACK

NEXT

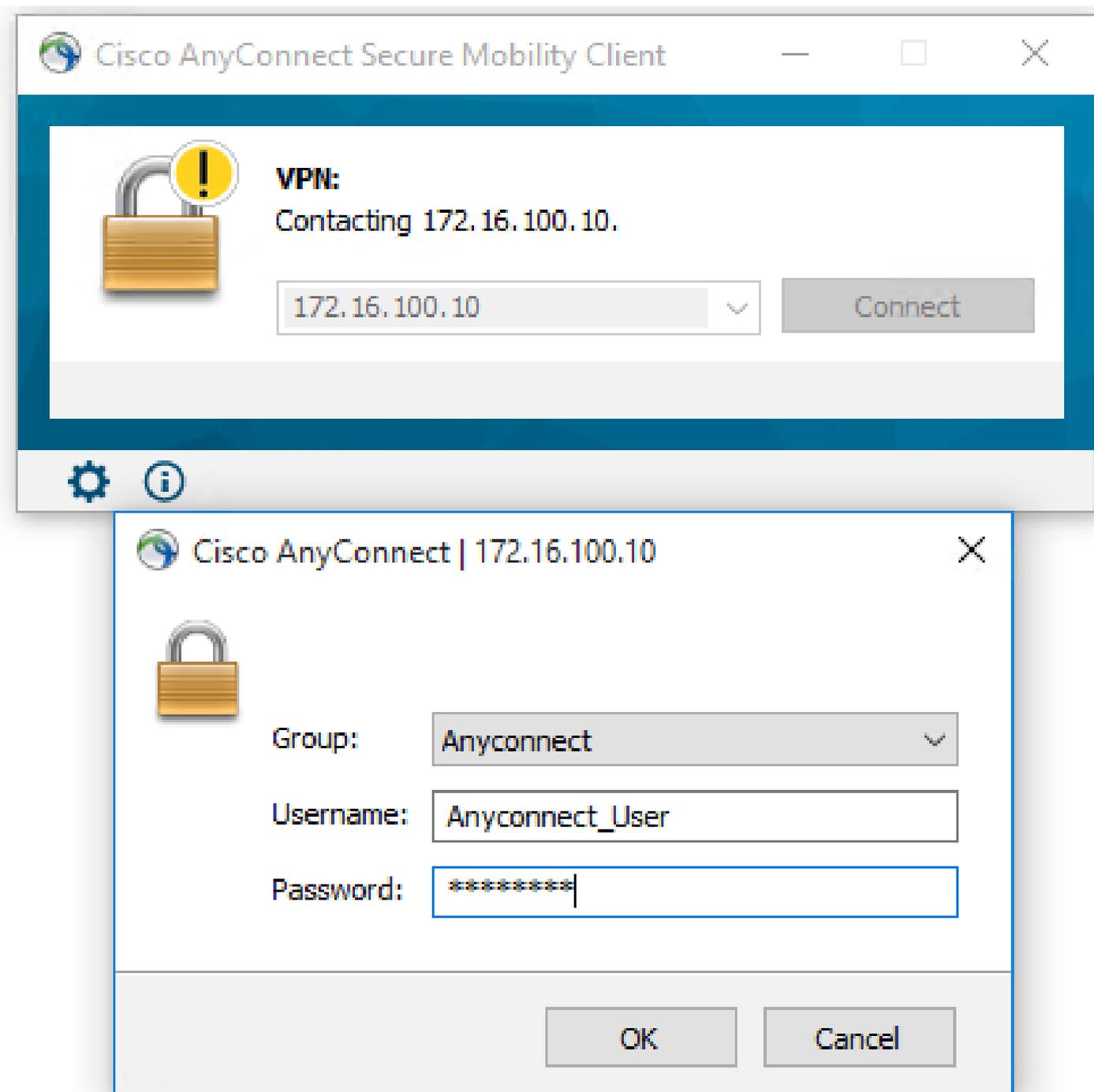
最後のページには、設定全体の概要が表示されます。正しいパラメータが設定されていることを確認し、Finishボタンを押して新しい設定を導入します。

確認

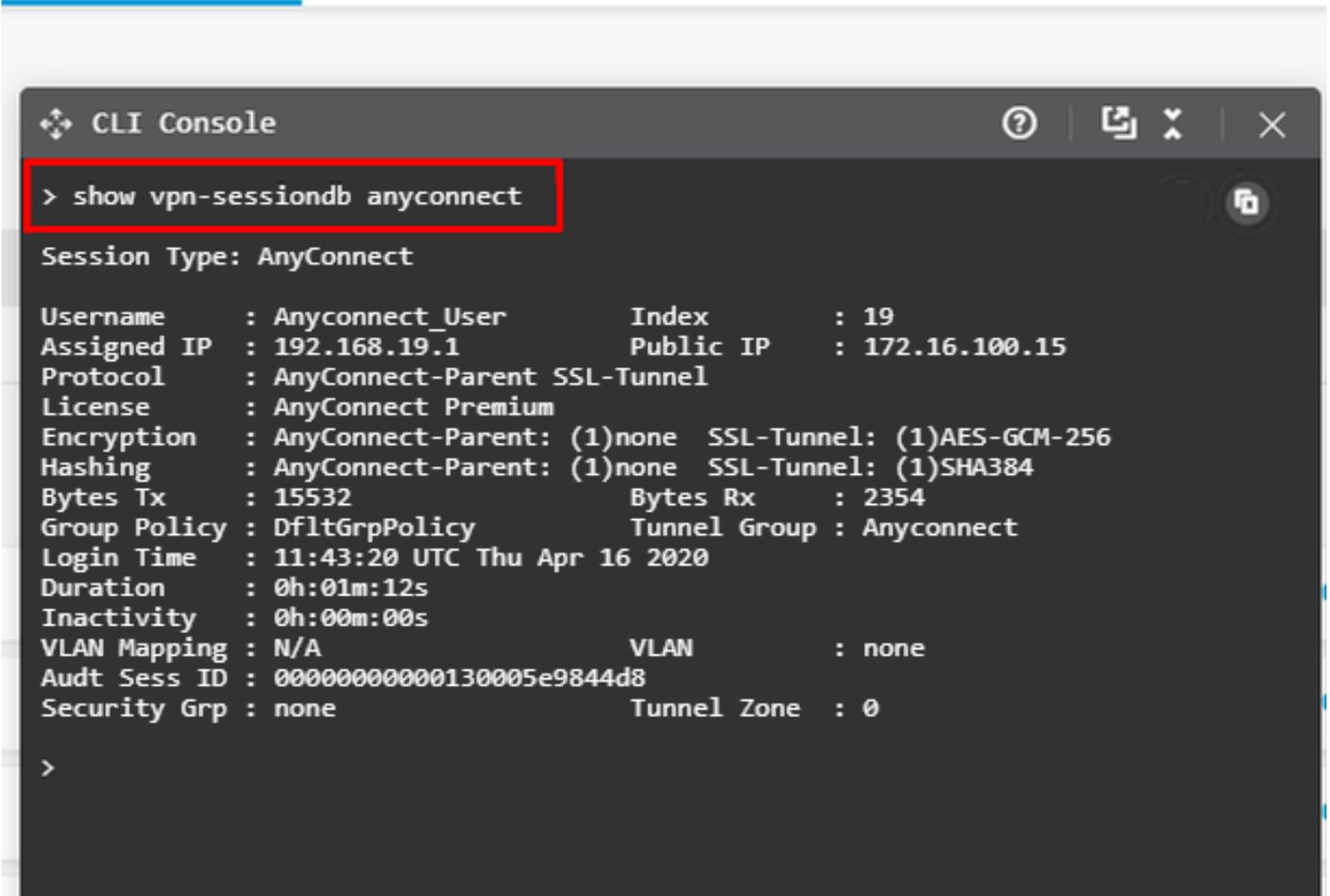
ここでは、設定が正常に機能しているかどうかを確認します。

設定を展開したら、接続を試みます。FTDの外部IPに解決されるFQDNがある場合は、それを Anyconnect接続ボックスに入力します。この例では、FTDの外部IPアドレスが使用されます。図に示すように、FDMのオブジェクト・セクションで作成されたユーザー名/パスワードを使用しま

す。



FDM 6.5.0の時点では、FDM GUIを使用してAnyconnectユーザを監視する方法はありません。唯一のオプションは、CLIを介してAnyconnectユーザをモニタすることです。FDM GUIのCLIコンソールを使用して、ユーザーが接続されていることを確認することもできます。次のコマンドを使用します。 Show vpn-sessiondb anyconnect.



同じコマンドをCLIから直接実行できます。

```
> show vpn-sessiondb anyconnect
```

```
Session Type: AnyConnect
```

```
Username      : Anyconnect_User      Index      : 15
Assigned IP   : 192.168.19.1         Public IP  : 172.16.100.15
Protocol      : AnyConnect-Parent SSL-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384
Bytes Tx      : 38830                Bytes Rx   : 172
Group Policy  : DfltGrpPolicy        Tunnel Group : Anyconnect
Login Time    : 01:08:10 UTC Thu Apr 9 2020
Duration      : 0h:00m:53s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                  VLAN       : none
Audt Sess ID  : 000000000000f0005e8e757a
Security Grp  : none                  Tunnel Zone : 0
```

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を説明します。

ユーザがSSLを使用してFTDに接続できない場合は、次の手順を実行してSSLネゴシエーションの問題を切り分けます。

1. FTDの外部のIPアドレスにユーザのコンピュータからpingが通ることを確認します。
2. TCPスリーウェイハンドシェイクが成功しているかどうかを確認するには、外部スニファを使用します。

AnyConnectクライアントの問題

このセクションでは、AnyConnect VPN Clientに関する最も一般的な2つの問題をトラブルシューティングするためのガイドラインを示します。AnyConnectクライアントのトラブルシューティングガイドについては、『[AnyConnect VPN Client Troubleshooting Guide](#)』を参照してください。

初期接続の問題

ユーザに初期接続の問題がある場合は、debugを有効にします `webvpn` FTDでAnyConnectを使用して、デバッグメッセージを分析します。デバッグはFTDのCLIで実行する必要があります。次のコマンドを使用します。 `debug webvpn anyconnect 255`を参照。

AnyConnectからログを取得するために、クライアントマシンからDARTバンドルを収集します。DARTバンドルの収集方法については、『[DARTバンドルの収集](#)』を参照してください。

トラフィック固有の問題

接続が成功しても、トラフィックがSSL VPNトンネルで失敗する場合は、クライアントのトラフィック統計情報を調べて、トラフィックがクライアントで送受信されていることを確認します。クライアントの詳細な統計情報は、AnyConnectのすべてのバージョンで利用できます。クライアントがトラフィックの送受信を示している場合は、FTDで送受信されたトラフィックを確認します。FTDがフィルタを適用している場合、フィルタ名が表示され、トラフィックがドロップされているかどうかを確認するためにACLエントリを調べることができます。ユーザが経験する一般的なトラフィックの問題は次のとおりです。

- FTDのルーティングの問題：内部ネットワークが、割り当てられたIPアドレスとVPNクライアントにパケットをルーティングして戻すことができません。
- トラフィックをブロックするアクセスコントロールリスト
- VPNトラフィックに対するネットワークアドレス変換(NAT)がバイパスされていない

FDMによって管理されるFTDでのリモートアクセスVPNの詳細については、[FDMによって管理されるリモートアクセスFTD](#)の完全なコンフィギュレーションガイドを参照してください。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。