

セキュアファイアウォールでのセキュアクライアントVPN管理トンネルの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[制限事項](#)

[設定](#)

[コンフィギュレーション](#)

[ステップ 1: AnyConnect管理VPNプロファイルの作成](#)

[ステップ 2: AnyConnect VPNプロファイルの作成](#)

[ステップ 3: AnyConnect管理VPNプロファイルおよびAnyConnect VPNプロファイルのFMCへのアップロード](#)

[ステップ 4: グループポリシーの作成](#)

[ステップ 5: 新しいAnyConnect設定の作成](#)

[手順 6: URLオブジェクトの作成](#)

[手順 7: URLエイリアスの定義](#)

[確認](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、Cisco FMCによって管理されるセキュアファイアウォールの脅威対策でセキュアクライアントVPN管理トンネルを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco AnyConnect Profile Editor
- Firewall Management Center(FMC)によるSSL AnyConnectの設定
- クライアント証明書認証

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。

- Cisco Firewall Threat Defense(FTD)バージョン6.7.0 (ビルド65)

- Cisco FMCバージョン6.7.0 (ビルド65)
- Windows 10マシンにインストールされたCisco AnyConnect 4.9.01095

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

この例では、Secure Sockets Layer(SSL)を使用して、FTDとWindows 10クライアントの間にバーチャルプライベートネットワーク(VPN)を作成します。

リリース6.7以降、Cisco FTDはAnyConnect管理トンネルの設定をサポートしています。この修正により、以前にオープンされた拡張要求Cisco Bug ID [CSCvs78215](#)が修正されます。

AnyConnect Management機能を使用すると、エンドポイントの起動が完了した直後にVPNトンネルを作成できます。ユーザがAnyConnectアプリを手動で起動する必要はありません。システムの電源が入るとすぐに、AnyConnect VPNエージェントサービスが管理VPN機能を検出し、AnyConnect管理VPNプロファイルのサーバリストで定義されているホストエントリを使用してAnyConnectセッションを開始します。

制限事項

- クライアント証明書認証のみがサポートされます。
- Windowsクライアントでは、マシン証明書ストアのみがサポートされます。
- Cisco Firepower Device Manager(FDM)ではサポートされていません。Cisco Bug ID [CSCvx90058](#)。
- Linuxクライアントではサポートされません。

すべての制限事項については、『[Cisco Secure Client管理者ガイドリリース5](#)』を参照してください。

設定

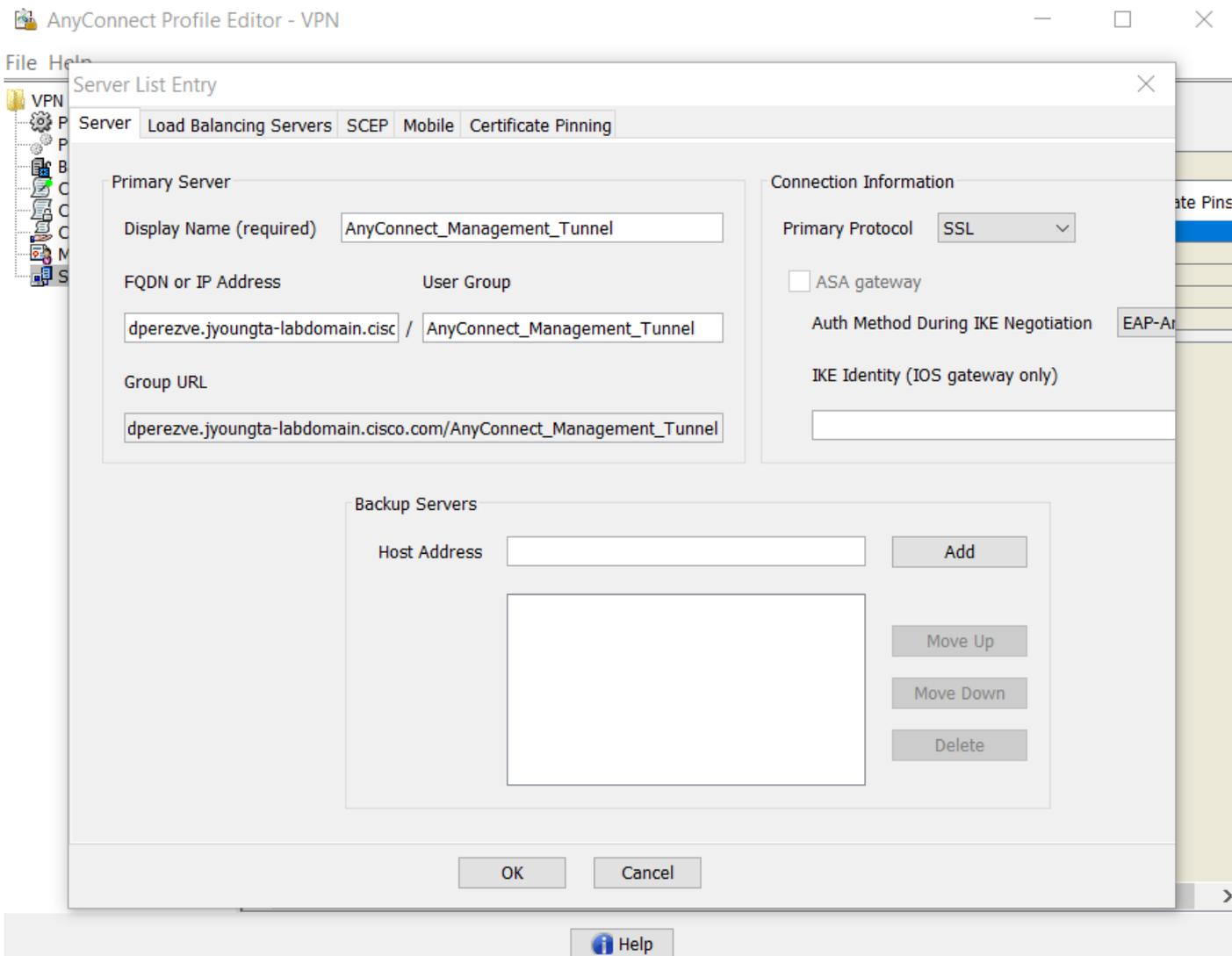
コンフィギュレーション

ステップ 1 : AnyConnect管理VPNプロファイルの作成

AnyConnect管理VPNプロファイルを作成するには、AnyConnectプロファイルエディタを開きます。管理プロファイルには、エンドポイントのブートアップ後にVPNトンネルを確立するために使用されるすべての設定が含まれています。

この例では、完全修飾ドメイン名(FQDN)dperezve.jyoungta-labdomain.cisco.comを指すサーバリストエントリが定義され、プライマリプロトコルとしてSSLが選択されます。サーバリストを追加するには、サーバリストに移動し、追加ボタンを選択します。必須フィールドに入力し、変更

を保存します。



管理VPNプロファイルには、サーバリストに加えて、次の必須設定が含まれている必要があります。

- AutomaticCertSelectionをtrueに設定する必要があります。
- AutoReconnectをtrueに設定する必要があります。
- AutoReconnectBehaviorをReconnectAfterResume用に構成する必要があります。
- AutoUpdateをfalseに設定する必要があります。
- BlockUntrustedServersをtrueに設定する必要があります。
- CertificateStoreをMachineStore用に構成する必要があります。
- CertificateStoreOverrideをtrueに設定する必要があります。
- EnableAutomaticServerSelectionをfalseに設定する必要があります。
- EnableScriptingをfalseに設定する必要があります。
- RetainVPNOnLogoffはtrueに設定する必要があります。

AnyConnect Profile Editorで、Preferences(Part 1)に移動し、次のように設定を調整します。

File Help

Preferences (Part 1)
Profile: ...nnect -FTD-Lab1.XML Profile\AnyConnect_Management_Tunnel.xml

Use Start Before Logon User Controllable

Show Pre-Connect Message

Certificate Store

Windows **Machine** ▾

macOS All ▾

Certificate Store Override

Auto Connect On Start User Controllable

Minimize On Connect User Controllable

Local Lan Access User Controllable

Disable Captive Portal Detection User Controllable

Auto Reconnect User Controllable

Auto Reconnect Behavior

ReconnectAfterResume ▾ User Controllable

Auto Update User Controllable

RSA Secure ID Integration

Automatic ▾ User Controllable

Windows Logon Enforcement

SingleLocalLogon ▾

Windows VPN Establishment

AllowRemoteUsers ▾

Help

次に、Preferences(Part 2)に移動し、Disable Automatic Certificate Selectionオプションのチェックマークを外します。

Preferences (Part 2)
Profile: ...nnect -FTD-Lab1.XML ProfileAnyConnect_Management_Tunnel.xml

Disable Automatic Certificate Selection User Controllable

Proxy Settings: Native User Controllable

Public Proxv Server Address:

Note: Enter public Proxv Server address and Port here. Example:10.86.125.33:8080

Allow Local Proxy Connections

Enable Optimal Gateway Selection User Controllable

Suspension Time Threshold (hours): 4

Performance Improvement Threshold (%): 20

Automatic VPN Policy

Trusted Network Policy: Disconnect

Untrusted Network Policy: Connect

Trusted DNS Domains:

Trusted DNS Servers:

Note: adding all DNS servers in use is recommended with Trusted Network Detection

Trusted Servers @ https://<server>[:<port>]

https://

ステップ 2 : AnyConnect VPNプロファイルの作成

管理VPNプロファイルに加えて、通常のAnyConnect VPNプロファイルを設定する必要があります。AnyConnect VPNプロファイルは、最初の接続試行で使用されます。このセッション中に、管理VPNプロファイルがFTDからダウンロードされます。

AnyConnect VPNプロファイルを作成するには、AnyConnect Profile Editorを使用します。この場合、両方のファイルに同じ設定が含まれているため、同じ手順を実行できます。

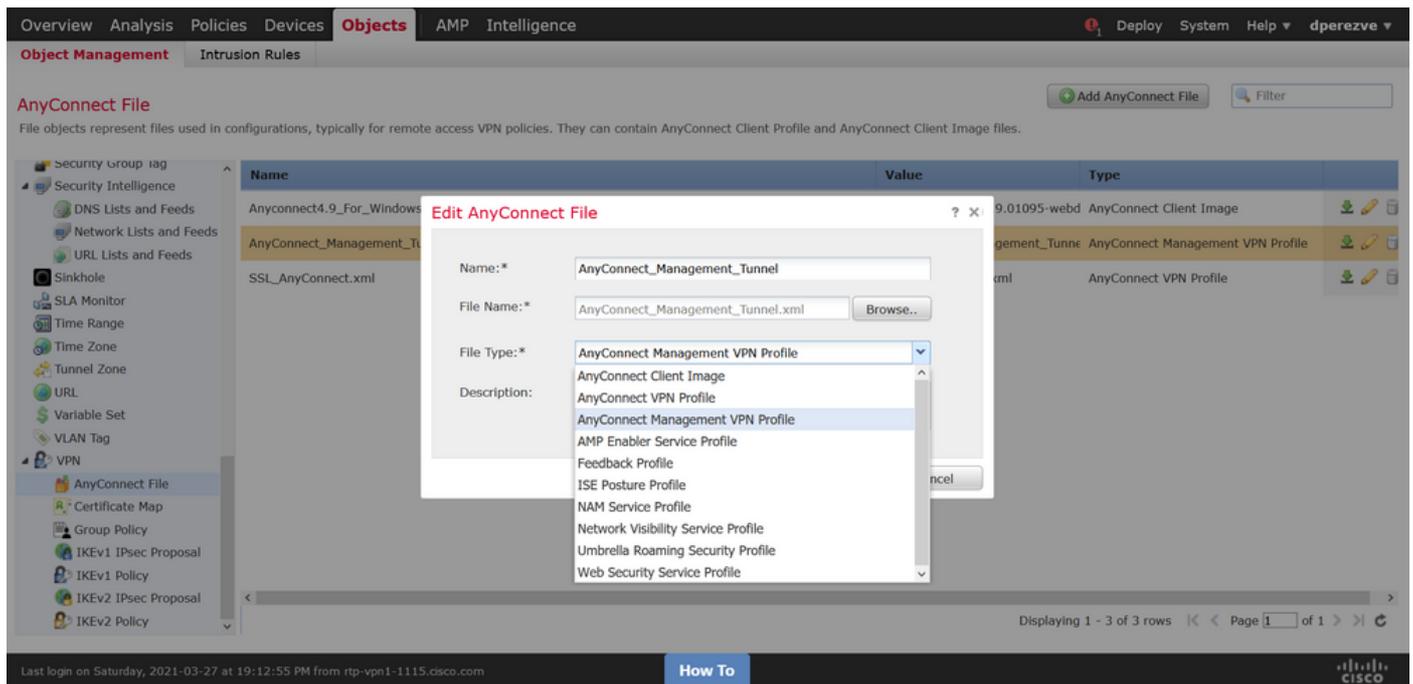
ステップ 3 : AnyConnect管理VPNプロファイルおよびAnyConnect VPNプロファイルのFMCへのアップロード

プロファイルが作成されたら、次の手順でプロファイルをAnyConnectファイルオブジェクトとしてFMCにアップロードします。

新しいAnyConnect Management VPN ProfileをFMCにアップロードするには、Objects > Object Managementの順に移動し、目次からVPNオプションを選択してから、Add AnyConnect Fileボタンを選択します。

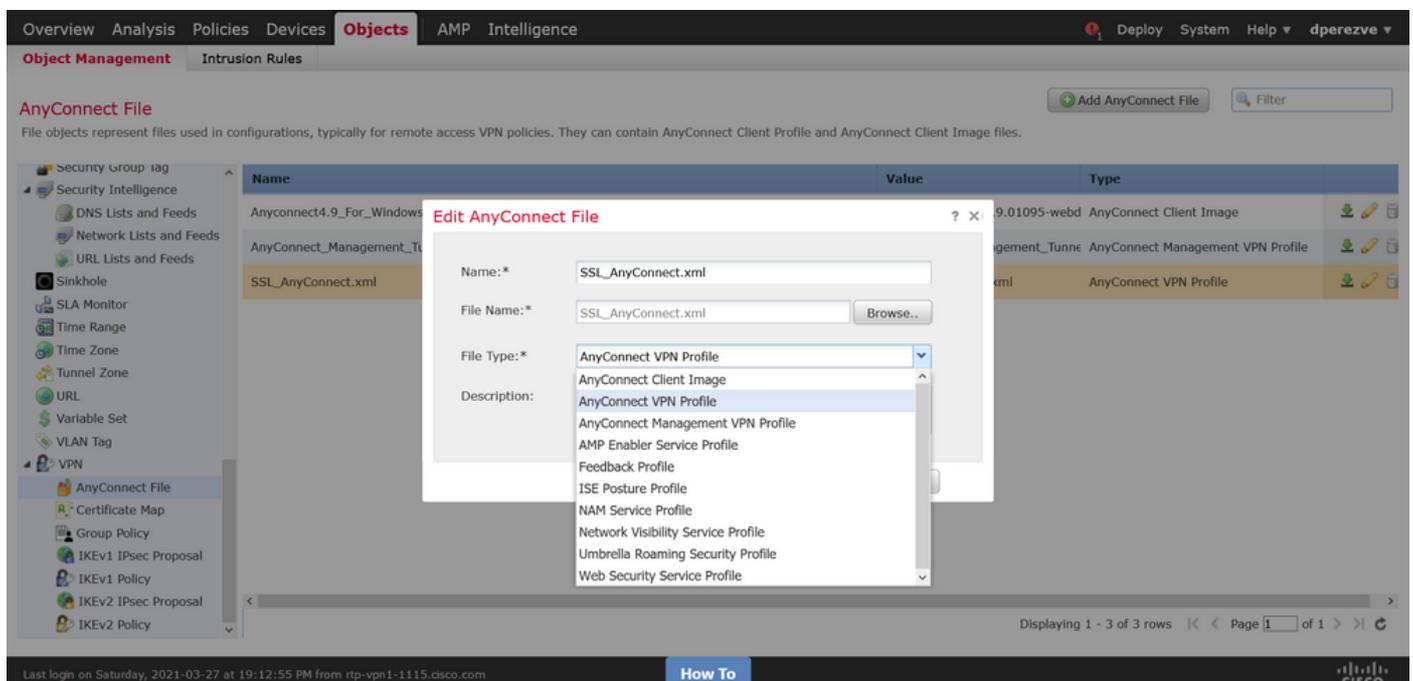
ファイルの名前を指定します。ファイルタイプとしてAnyConnect Management VPN Profileを選

押し、オブジェクトを保存します。



AnyConnect VPNプロファイルをアップロードするには、再度Objects > Object Managementに移動し、目次からVPNオプションを選択してから、Add AnyConnect Fileボタンを選択します。

ファイルの名前を指定しますが、ここではファイルタイプとしてAnyConnect VPN Profileを選択し、新しいオブジェクトを保存します。



プロファイルをオブジェクトリストに追加し、AnyConnect Management VPN ProfileおよびAnyConnect VPN Profileとしてそれぞれマークする必要があります。

The screenshot shows the Cisco FTD Object Manager interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Objects' tab is active, and the 'Object Management' section is selected. A sidebar on the left lists various object categories, with 'VPN' expanded to show 'AnyConnect File'. The main area displays a table of AnyConnect File objects:

Name	Value	Type
Anyconnect4.9_For_Windows	anyconnect-win-4.9.01095-webd	AnyConnect Client Image
AnyConnect_Management_Tunnel	AnyConnect_Management_Tunnel	AnyConnect Management VPN Profile
SSL_AnyConnect.xml	SSL_AnyConnect.xml	AnyConnect VPN Profile

At the bottom of the interface, there is a 'How To' button and a Cisco logo.

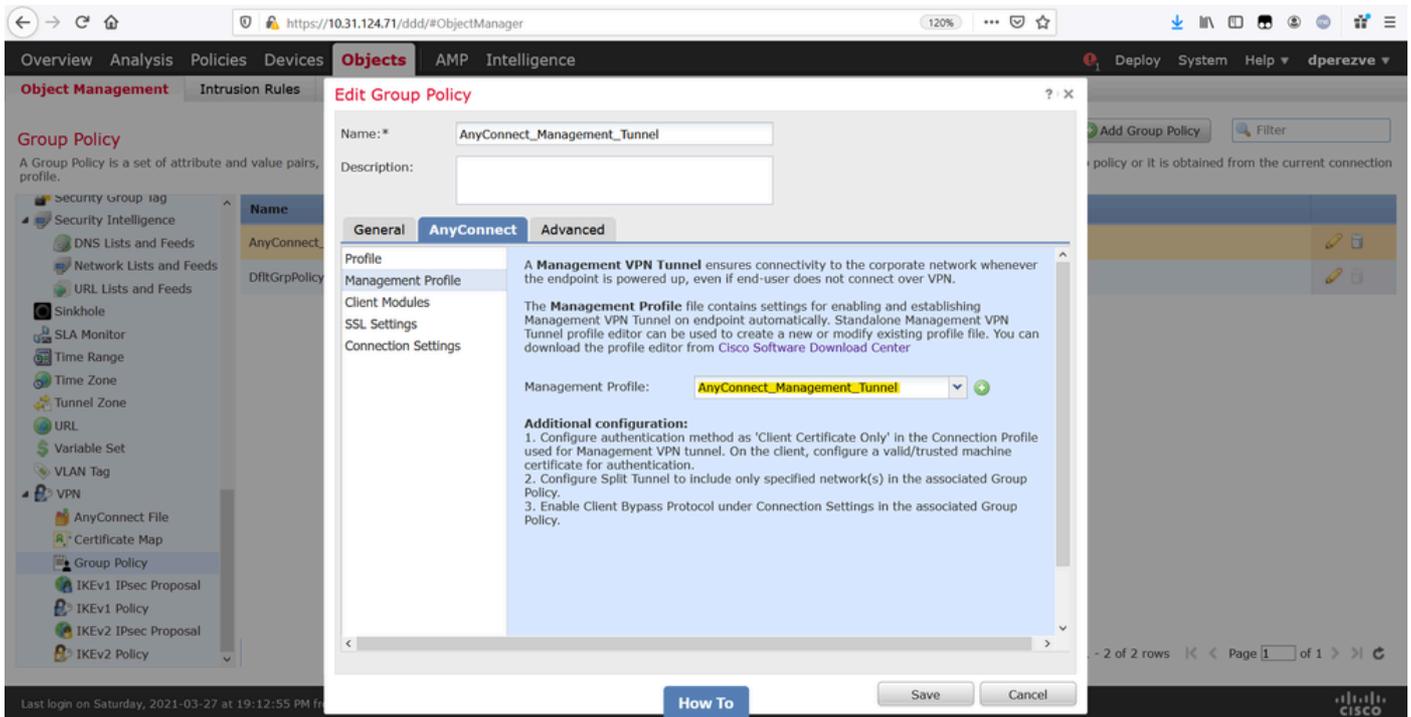
ステップ 4 : グループポリシーの作成

新しいグループポリシーを作成するには、Objects > Object Managementに移動し、目次からVPNオプションを選択してから、Group Policyを選択し、Add Group Policyボタンをクリックします。

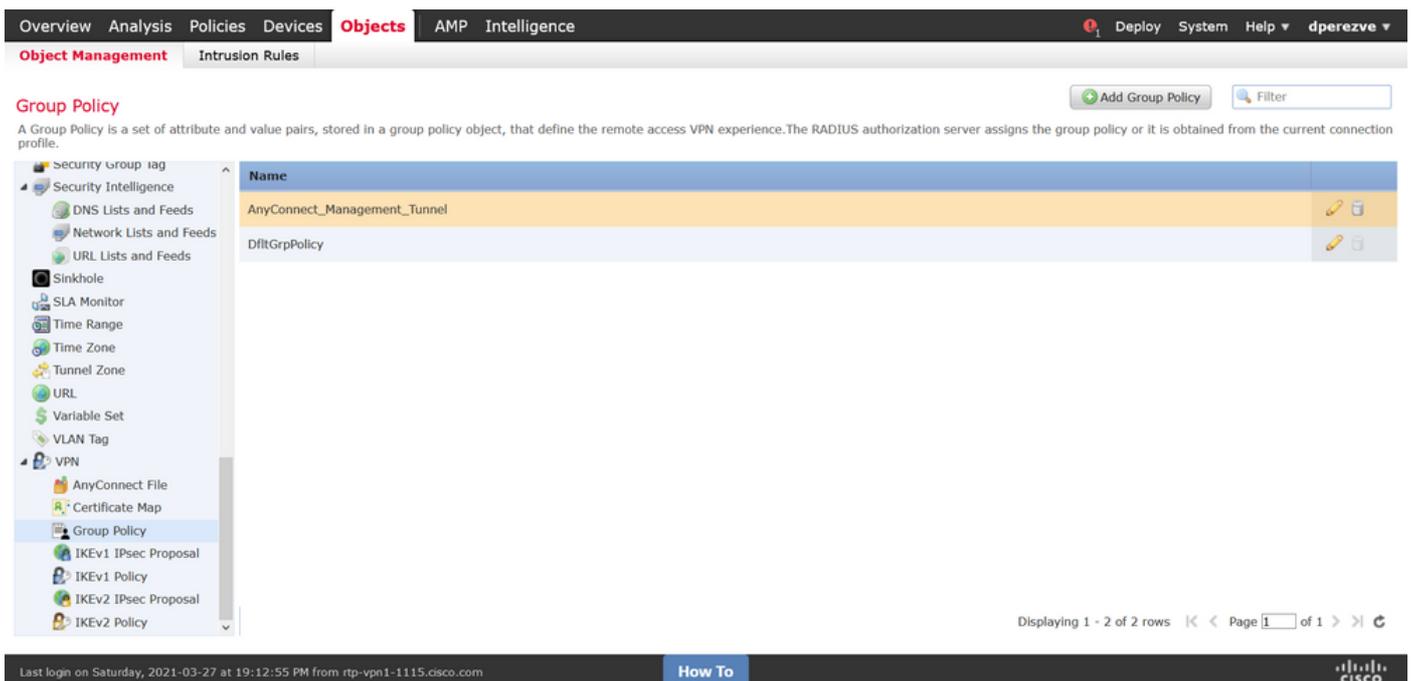
Add Group Policyウィンドウが開いたら、名前を割り当て、AnyConnectプールを定義し、AnyConnectタブを開きます。Profileに移動し、Client Profileドロップダウンメニューで通常のAnyConnect VPNプロファイルを表すオブジェクトを選択します。

The screenshot shows the 'Edit Group Policy' dialog box in the Cisco FTD interface. The dialog has a 'Name' field containing 'AnyConnect_Management_Tunnel' and a 'Description' field. Below these are three tabs: 'General', 'AnyConnect', and 'Advanced'. The 'AnyConnect' tab is selected, showing a 'Profile' section with a 'Client Profile' dropdown menu set to 'SSL_AnyConnect.xml'. The dialog also includes 'Save' and 'Cancel' buttons at the bottom.

次に、Management Profileタブに移動し、Management ProfileドロップダウンメニューでManagement VPN Profileを含むオブジェクトを選択します。



変更を保存して、新しいオブジェクトを既存のグループポリシーに追加します。



ステップ 5 : 新しいAnyConnect設定の作成

FMCでのSSL AnyConnectの設定は、4つの異なる手順で構成されます。AnyConnectを設定するには、Devices > VPN > Remote Accessの順に選択し、Addボタンを選択します。これにより、リモートアクセスVPNポリシーウィザードが開きます。

Policy Assignmentタブで、手元にあるFTDデバイスを選択し、接続プロファイルの名前を定義して、SSLチェックボックスをオンにします。

The screenshot shows the 'Remote Access VPN Policy Wizard' in the Cisco ICM interface. The navigation bar indicates the current step is '2 Connection Profile'. The main content area is titled 'Targeted Devices and Protocols'. It includes a 'Name:*' field with the value 'AnyConnect_Management_Tunnel' and an empty 'Description:' field. Under 'VPN Protocols', the 'SSL' checkbox is checked, and 'IPsec-IKEv2' is unchecked. The 'Targeted Devices' section shows two columns: 'Available Devices' with a search bar and a list containing 'ftdv-dperezve' and 'ftdv-fejimene', and 'Selected Devices' with 'ftdv-dperezve'. A 'Before You Start' sidebar on the right provides instructions on authentication servers, client packages, and device interfaces. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons, and a footer with the Cisco logo and a 'How To' link.

Connection Profileで、認証方式としてClient Certificate Onlyを選択します。これは、この機能でサポートされる唯一の認証です。

The screenshot shows the 'Remote Access VPN Policy Wizard' in the Cisco ICM interface, now at step '4 Access & Certificate'. The 'Connection Profile' section shows the name 'AnyConnect_Management_Profile'. The 'Authentication, Authorization & Accounting (AAA)' section is active, with 'Authentication Method' set to 'Client Certificate Only'. The 'Username From Certificate' dropdown is open, showing options: 'AAA Only', 'SAML', 'Client Certificate Only', and 'Client Certificate & AAA'. The 'Authorization Server' and 'Accounting Server' fields are empty. The 'Client Address Assignment' section has three unchecked checkboxes: 'Use AAA Server (Realm or RADIUS only)', 'Use DHCP Servers', and 'Use IP Address Pools'. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons, and a footer with the Cisco logo and a 'How To' link.

次に、ステップ3で作成したグループポリシーオブジェクトをGroup Policyドロップダウンで選択します。

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help dperezve

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 **AnyConnect** 4 Access & Certificate 5 Summary

Authorization Server: (Realm or RADIUS)

Accounting Server: (RADIUS)

Client Address Assignment:
 Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only) i

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools:

IPv6 Address Pools:

Group Policy:
 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.

Group Policy:* +

^

v

Back Next Cancel

Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com How To

AnyConnectタブで、エンドポイントのオペレーティングシステム(OS)に応じてAnyConnect File Objectを選択します。

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help dperezve

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 **AnyConnect** 4 Access & Certificate 5 Summary

AAA

AnyConnect Client Image
 The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#). Show Re-order buttons +

<input checked="" type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	Anyconnect4.9_For_Windows	anyconnect-win-4.9.01095-webdeploy-k9.pkg	Windows <input type="text" value="Windows"/>

Back Next Cancel

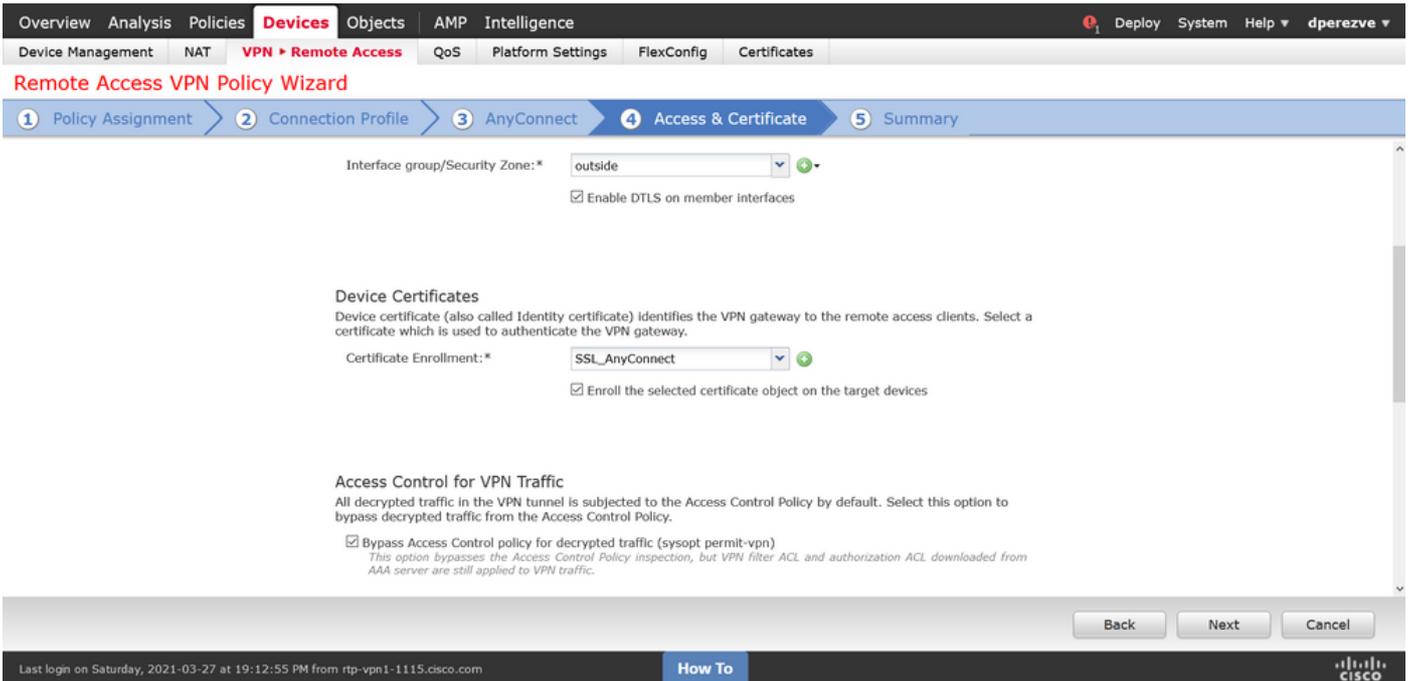
Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com How To

Access & Certificateで、FTDがWindowsクライアントに対してそのIDをプローブするために使用する必要がある証明書を指定します。

注：ユーザは管理VPN機能を使用する際にAnyConnectアプリケーションと対話できないため、証明書は完全に信頼されている必要があり、警告メッセージを表示してはなりません。

注：証明書の検証エラーを防ぐには、証明書のサブジェクト名に含まれる共通名(CN)フィールドが、XMLプロファイルのサーバリスト (ステップ1およびステップ2) で定義されて

 いるFQDNと一致する必要があります。



Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help dperezve

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Interface group/Security Zone:* Enable DTLS on member interfaces

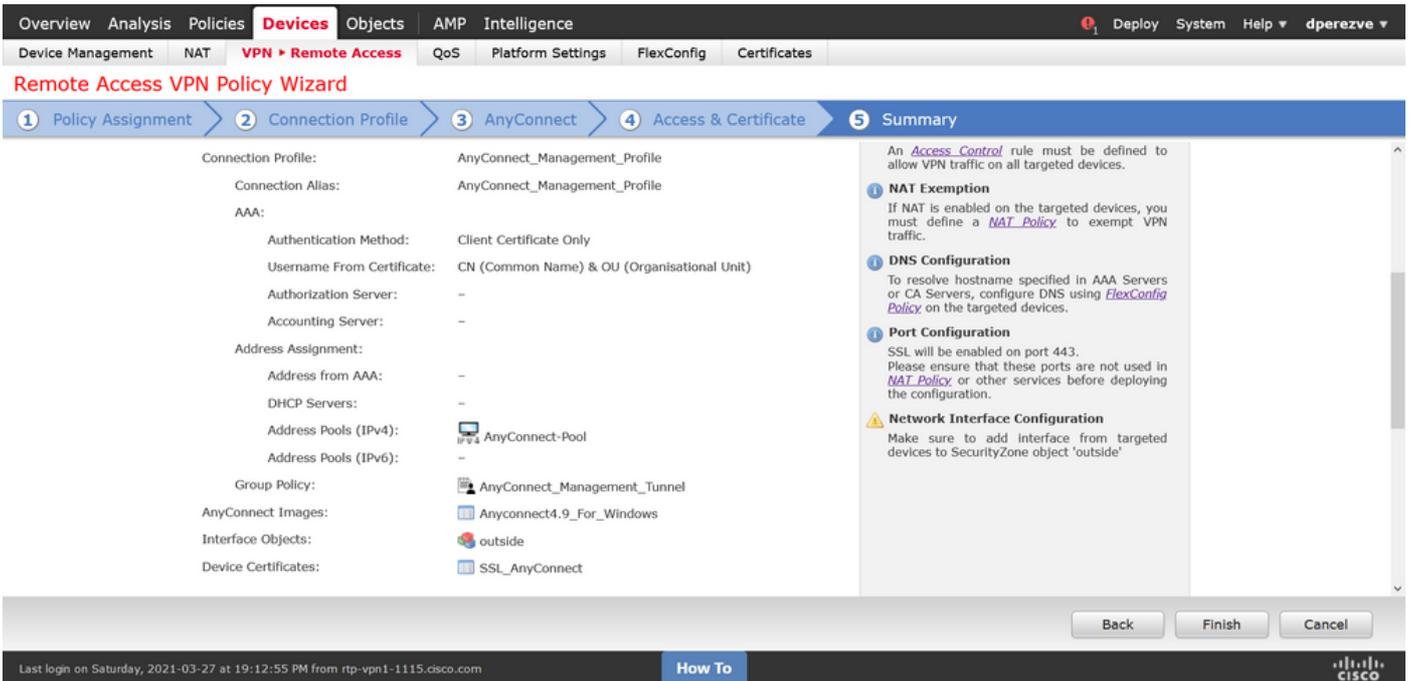
Device Certificates
Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.
Certificate Enrollment:* Enroll the selected certificate object on the target devices

Access Control for VPN Traffic
All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.
 Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Back Next Cancel

Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com [How To](#) 

最後に、SummaryタブでFinishボタンを選択して、新しいAnyConnect設定を追加します。



Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help dperezve

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Connection Profile: AnyConnect_Management_Profile
Connection Alias: AnyConnect_Management_Profile
AAA:
Authentication Method: Client Certificate Only
Username From Certificate: CN (Common Name) & OU (Organisational Unit)
Authorization Server: -
Accounting Server: -
Address Assignment:
Address from AAA: -
DHCP Servers: -
Address Pools (IPv4):  AnyConnect-Pool
Address Pools (IPv6): -
Group Policy:  AnyConnect_Management_Tunnel
AnyConnect Images:  Anyconnect4.9_For_Windows
Interface Objects:  outside
Device Certificates:  SSL_AnyConnect

An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.

NAT Exemption
If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.

DNS Configuration
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.

Port Configuration
SSL will be enabled on port 443. Please ensure that these ports are not used in [NAT Policy](#) or other services before deploying the configuration.

Network Interface Configuration
Make sure to add interface from targeted devices to SecurityZone object 'outside'

Back Finish Cancel

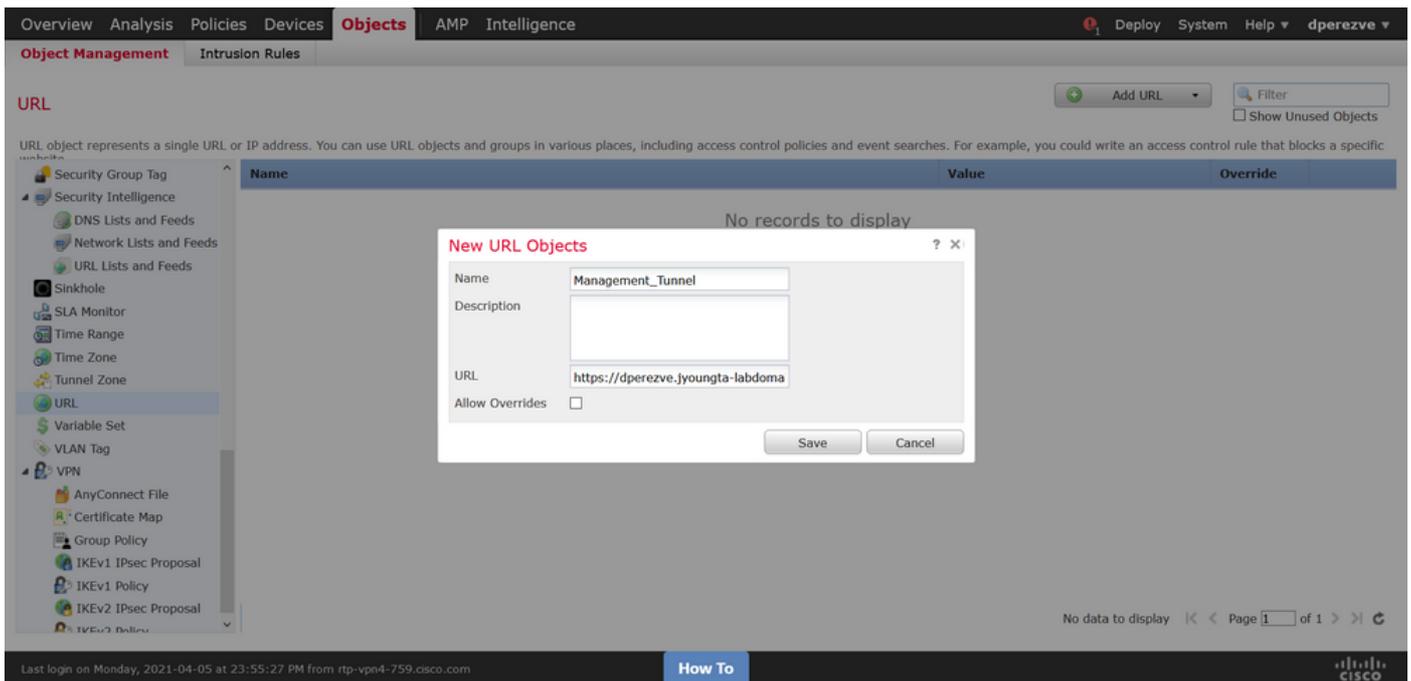
Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com [How To](#) 

手順 6 : URLオブジェクトの作成

Objects > Object Managementの順に移動し、目次からURLを選択します。次に、Add URLドロップダウンでAdd Objectを選択します。

オブジェクトの名前を指定し、管理VPNプロファイルサーバリスト (ステップ2) で指定したのと同じFQDN/ユーザグループを使用してURLを定義します。この例では、URLは dperezve.jyoungta-labdomain.cisco.com/AnyConnect_Management_Tunnelである必要があります

o

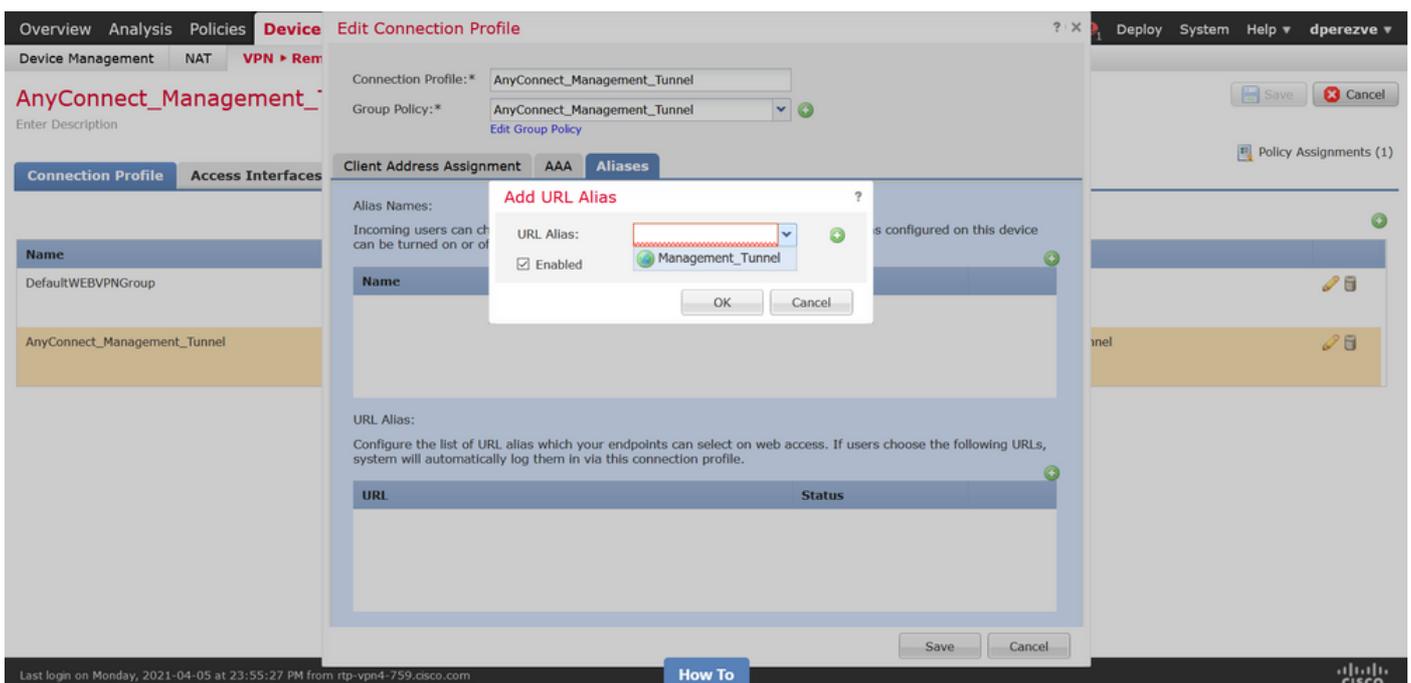


変更を保存して、オブジェクトをオブジェクトリストに追加します。

手順 7 : URLエイリアスの定義

AnyConnect設定でURLエイリアスを有効にするには、Devices > VPN > Remote Accessの順に移動し、鉛筆アイコンをクリックして編集します。

次に、Connection Profileタブで手元の設定を選択し、Aliasesに移動してAddボタンをクリックし、URL AliasドロップダウンでURL Objectを選択します (図1の矢印Aを参照)。Enabledチェックボックスがオンになっていることを確認します。



変更を保存し、FTDに設定を展開します。

確認

導入が完了したら、AnyConnect VPNプロファイルを使用した最初の手動AnyConnect接続が必要です。この接続中に、管理VPNプロファイルがFTDからダウンロードされ、C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTunに保存されます。この時点から、ユーザの操作なしで、管理VPNプロファイルを介して後続の接続を開始する必要があります。

トラブルシューティング

証明書検証エラーの場合：

- 認証局(CA)のルート証明書がFTDにインストールされていることを確認します。
- 同じCAによって署名されたID証明書がWindowsマシンのストアにインストールされていることを確認してください。
- CNフィールドが証明書に含まれており、管理VPNプロファイルのサーバリストで定義されているFQDNおよびURLエイリアスで定義されているFQDNと同じであることを確認します。

開始されていない管理トンネルの場合：

- 管理VPNプロファイルがダウンロードされ、C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTunに保存されていることを確認します。
- 管理VPNプロファイルの名前がVpnMgmtTunProfile.xmlであることを確認します。

接続の問題については、DARTバンドルを収集し、詳細な調査を行うためにCisco TACにお問い合わせください。

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。