

# セキュアクライアントAnyConnect VPNの強化対策の実装

## 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](#)

[コンセプト](#)

[Cisco Secure Firewallでのクライアントのセキュリティ強化策：](#)

[ロギングとsyslog IDを使用した攻撃の特定](#)

[攻撃の検証](#)

[FMCの設定例](#)

[DefaultWEBVPNGroupおよびDefaultRAGroup接続プロファイルでのAAA認証の無効化](#)

[DefaultWEBVPNGroupおよびDefaultRAGroupでホストスキャン/セキュアファイアウォールポスチャを無効にする（オプション）](#)

[グループエイリアスの無効化とグループURLの有効化](#)

[証明書マッピング](#)

[IPsec-IKEv2](#)

[ASAの設定例](#)

[DefaultWEBVPNGroupおよびDefaultRAGroup接続プロファイルでのAAA認証の無効化](#)

[DefaultWEBVPNGroupおよびDefaultRAGroupでホストスキャン/セキュアファイアウォールポスチャを無効にする（オプション）](#)

[グループエイリアスの無効化とグループURLの有効化](#)

[証明書マッピング](#)

[IPsec-IKEv2](#)

[結論](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、リモートアクセスVPN実装のセキュリティを向上させ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。

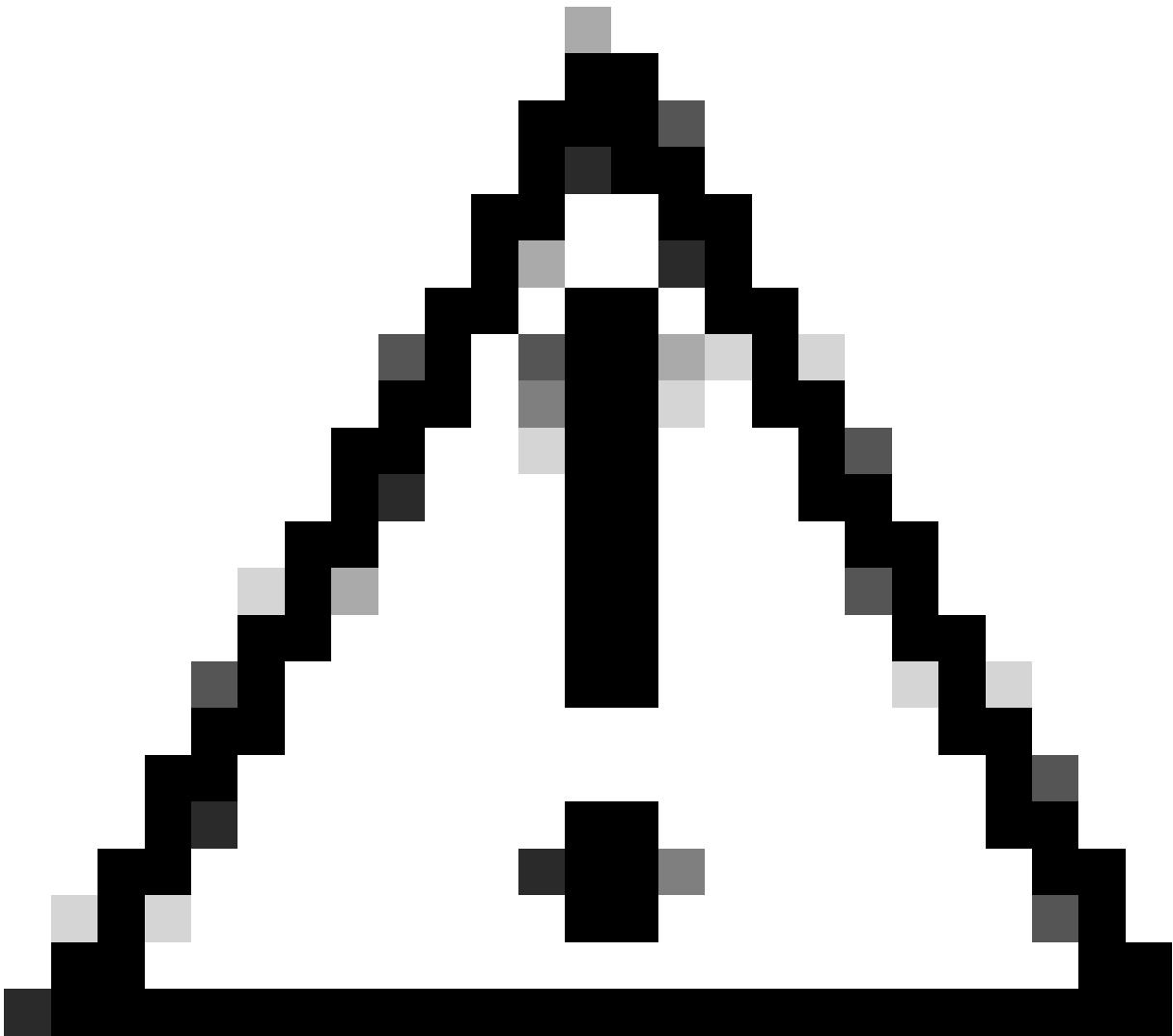
- Cisco Secure Client AnyConnect VPN』を参照してください。
- ASA/FTDリモートアクセス設定。

## 使用するコンポーネント

ベストプラクティスガイドは、次のハードウェアとソフトウェアのバージョンに基づいています。

- Cisco ASA 9.x
- Firepower Threat Defense(FTD)7.x/FMC 7.x

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。



注意：このドキュメントには、Firepowerデバイスマネージャ(FDM)の手順は含まれていません。FDMは、DefaultWEBVPNGroupの認証方式の変更のみをサポートします。コン

---

トロールプレーンACL、またはFDM UIのリモートアクセスVPNの「グローバル設定」セクションのカスタムポートを使用してください。必要に応じて、Cisco Technical Assistance Center(TAC)に連絡し、サポートを依頼してください。

---

## 背景説明

このドキュメントの目的は、Cisco Secure Client AnyConnect VPNの設定が、サイバーセキュリティ攻撃が一般的に見られる現代の世界におけるセキュリティのベストプラクティスに準拠していることを確認することです。

総当たり攻撃では通常、ユーザ名とパスワードの組み合わせを使用してリソースへのアクセスを繰り返し試みます。攻撃者は、インターネットブラウザ、セキュアクライアントユーザインターフェイス、またはその他のツールを使用して、複数のユーザ名とパスワードを入力し、それらがAAAデータベース内の正当な組み合わせと一致することを望んでいます。認証にAAAを使用する場合、接続を確立するために必要であるため、エンドユーザはユーザ名とパスワードを入力する必要があります。同時に、ユーザがクレデンシャルを入力するまで、ユーザを確認しません。本質的に、これにより攻撃者は次のシナリオを利用できます。

1. Cisco Secure Firewallの公開された完全修飾ドメイン名 (特に接続プロファイルでグループエイリアスを使用する場合) :
  - 攻撃者がVPNファイアウォールのFQDNを検出した場合、ブルートフォースアタックを開始するグループエイリアスを使用してトンネルグループを選択するオプションがあります。
2. AAAまたはローカルデータベースで設定されたデフォルト接続プロファイル :
  - 攻撃者は、VPNファイアウォールのFQDNを見つけると、AAAサーバまたはローカルデータベースに対してブルートフォースアタックを試みることができます。これは、グループエイリアスが指定されていない場合でも、FQDNへの接続がデフォルト接続プロファイルに到達するために発生します。
3. ファイアウォールまたはAAAサーバでのリソース枯渇 :
  - 攻撃者は、大量の認証要求を送信し、Denial of Service (DoS ; サービス拒否) 状態を発生させることで、AAAサーバまたはファイアウォールリソースに過大な負荷を与える可能性があります。

## コンセプト

グループエイリアス :

- ファイアウォールが接続プロファイルを参照するための代替名。ファイアウォールへの接続を開始した後、ユーザが選択できるように、これらの名前がセキュアクライアントUIのドロップダウンメニューに表示されます。group-aliasesを削除すると、セキュアクライアントUIのドロップダウン機能が削除されます。

グループURL:

- 着信接続が目的の接続プロファイルに直接マッピングされるように、接続プロファイルに連付けることができるURL。ユーザがセキュアクライアントUIで完全なURLを入力するか、XMLプロファイルでURLを「表示名」と統合してユーザにURLを表示しないようにできるため、ドロップダウン機能はありません。

ここで異なるのは、グループエイリアスを実装する場合、ユーザが接続 to vpn\_gateway.example.comを開始し、エイリアスを表示して接続プロファイルへのドライブを選択する点です。グループURLを使用すると、ユーザは vpn\_gateway.example.com/example\_groupへの接続を開始し、ドロップダウンメニューの必要やオプションなしで接続プロファイルに直接接続できます。

## Cisco Secure Firewallでのクライアントのセキュリティ強化策：

これらの方式は、正当なユーザを適切なトンネルグループや接続プロファイルにマッピングする一方で、悪意のある可能性のあるユーザをトラップトンネルグループに送信します。このトラップトンネルグループは、ユーザ名とパスワードの組み合わせを許可しないように設定されています。すべての組み合わせを実装する必要はありませんが、グループエイリアスを無効にし、DefaultWEBVPNGroupおよびDefaultRAGroupの認証方式を変更することで、推奨事項が効果的に機能するようになります。

- 接続プロファイル設定でグループエイリアスを無効にしてグループURLのみを使用すると、適切なFQDNを持つクライアントだけが接続を開始できるため、攻撃者が簡単に検出して選択することのない特定のFQDNを使用できます。たとえば、vpn\_gateway.example.com/example\_groupはvpn\_gateway.example.comよりも攻撃者にとって発見が困難です。
- DefaultWEBVPNGroupおよびDefaultRAGroupでAAA認証を無効にし、証明書認証を設定します。これにより、ローカルデータベースまたはAAAサーバに対するブルートフォースを回避できます。このシナリオの攻撃者は、接続試行時に即時エラーを表示されます。認証は証明書に基づいているため、ユーザ名またはパスワードのフィールドはありません。そのため、総当たり攻撃は停止されます。もう1つのオプションは、悪意のある要求のシンクホールを作成するためのサポート設定のないAAAサーバを作成することです。
- 接続プロファイルに証明書マッピングを使用します。これにより、クライアントデバイス上の証明書から受信した属性に基づいて、着信接続を特定の接続プロファイルにマッピングできます。適切な証明書を持つユーザは正しくマッピングされますが、マッピング基準に失敗した攻撃者はDefaultWEBVPNGroupに送信されます。
- SSLの代わりにIKEv2-IPSecを使用すると、トンネルグループはXMLプロファイル内の特定のユーザグループマッピングに依存します。エンドユーザマシンにこのXMLがないと、ユーザはデフォルトのトンネルグループに自動的に送信されます。

---

注：グループエイリアス機能の詳細については、『[ASA VPNコンフィギュレーションガイド](#)』と『表1』を参照してください。SSL VPNの接続プロファイル属性』を参照してください。

---

## ロギングとsyslog IDを使用した攻撃の特定

総当たり攻撃は、リモートアクセスVPNを侵害する主要な方法であり、脆弱なパスワードを悪用して不正なエントリを取得します。ロギングの利用とsyslogの評価によって攻撃の兆候を認識する方法を知ることは非常に重要です。異常なボリュームに遭遇した場合に攻撃を示す可能性がある一般的なsyslog IDは次のとおりです。

%ASA-6-113015

<#root>

%ASA-6-113015

: AAA user authentication Rejected : reason = User was not found : local database : user = admin : user

%ASA-6-113005

<#root>

%ASA-6-113005

: AAA user authentication Rejected : reason = Unspecified : server = x.x.x.x : user = \*\*\*\*\* : user IP =

%ASA-6-716039

<#root>

%ASA-6-716039

: Group <DfltGrpPolicy> User <admin> IP <x.x.x.x> Authentication: rejected, Session Type: WebVPN

ユーザ名は、ASAでno logging hide usernameコマンドが設定されるまで、常に非表示になります

。

---

注：有効なユーザが生成されたか、または悪意のあるIPによって認識された場合、これは情報を提供しますが、ユーザ名がログに表示されるので注意してください。

---

Cisco ASAロギング：

[Secure ASA Firewallユーザガイド](#)

『Cisco Secure Firewall ASAシリーズCLIコンフィギュレーションガイド』の「[ロギング](#)」の章

Cisco FTDロギング：

[FMCを介してFTDにロギングを設定](#)

『Cisco Secure Firewall Management Center Device Configuration Guide』の「Platform Settings」の章の「[Configure Syslog](#)」の項

[Firepower Device Manager\(FDM\)でのsyslogの設定と確認](#)

『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「System Settings」の章の「[Configuring System Logging Settings](#)」の項

## 攻撃の検証

これを確認するには、ASAまたはFTDのコマンドラインインターフェイス(CLI)にログインして show aaa-server コマンドを実行し、設定されたAAAサーバのいずれかに対して試行された認証要求と拒否された認証要求の数が異常でないかどうかを調べます。

```
<#root>
```

```
ciscoasa#
```

```
show aaa-server
```

```
Server Group: LOCAL - - - - - >>>> Sprays against the LOCAL database
Server Protocol: Local database
Server Address: None
Server port: None
Server status: ACTIVE, Last transaction at 16:46:01 UTC Fri Mar 22 2024
Number of pending requests 0
Average round trip time 0ms
Number of authentication requests 8473575 - - - - - >>>> Unusual increments
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 0
Number of rejects 8473574 - - - - - >>>> Unusual increments
```

```
<#root>
```

```
ciscoasa#
```

```
show aaa-server
```

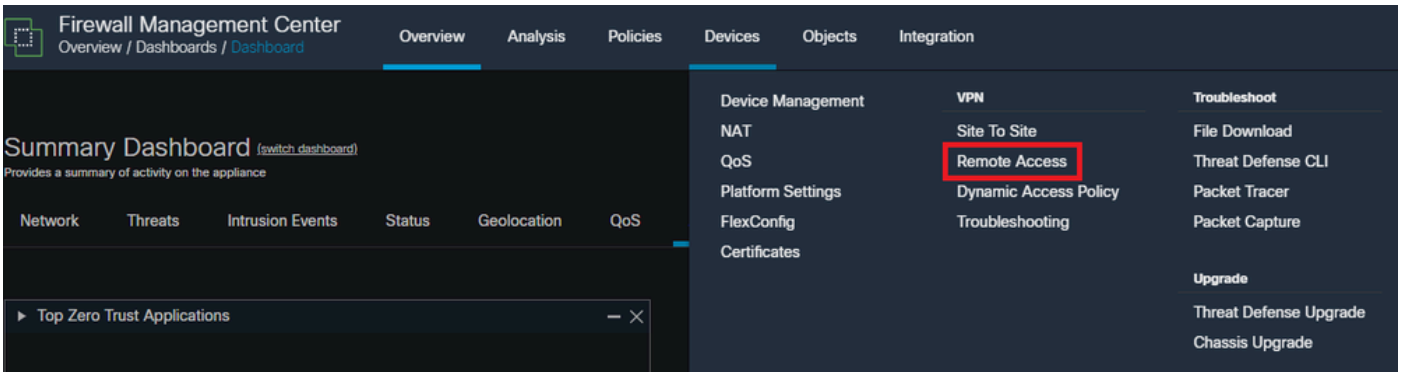
```
Server Group: LDAP-SERVER - - - - - >>>> Sprays against the LDAP server
Server Protocol: ldap
Server Hostname: ldap-server.example.com
Server Address: 10.10.10.10
Server port: 636
Server status: ACTIVE, Last transaction at unknown
Number of pending requests 0
Average round trip time 0ms
Number of authentication requests 2228536 - - - - - >>>> Unusual increments
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 1312
Number of rejects 2225363 - - - - - >>>> Unusual increments
Number of challenges 0
Number of malformed responses 0
Number of bad authenticators 0
Number of timeouts 1
Number of unrecognized responses 0
```



# FMCの設定例

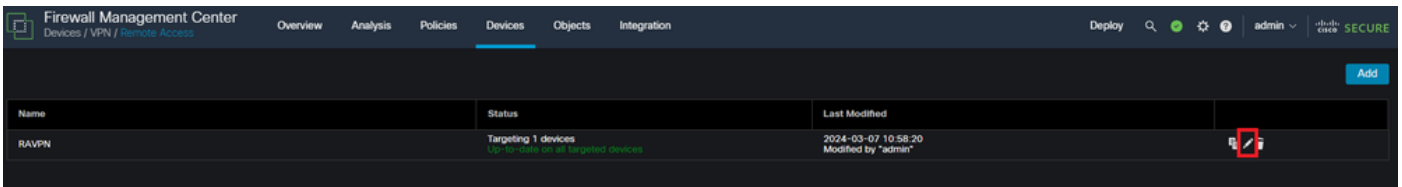
## DefaultWEBVPNGroupおよびDefaultRAGroup接続プロファイルでのAAA認証の無効化

Devices > Remote Accessの順に移動します。



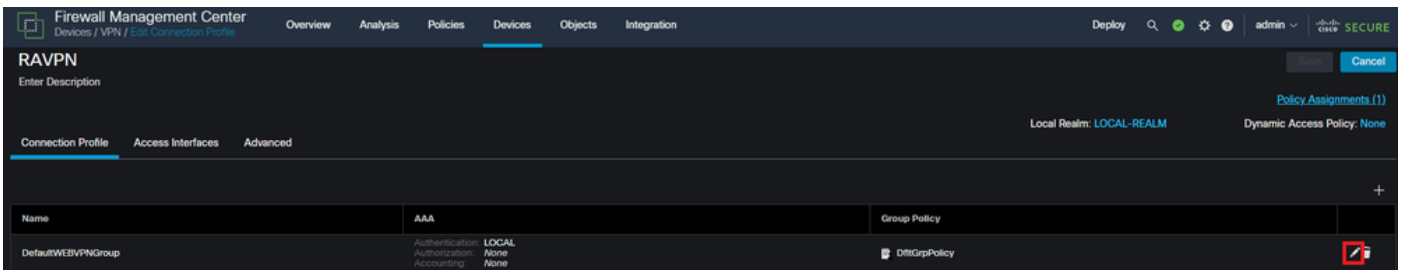
が、リモートアクセスVPNポリシー設定に移動するためにFMC GUIをナビゲートしていることを示します。

既存のリモートアクセスVPNポリシーを編集し、「DefaultRAGroup」という名前の接続プロファイルを作成します。



FMC UIでリモートアクセスVPNポリシーを編集する方法を表示します。

「DefaultWEBVPNGroup」および「DefaultRAGroup」という名前の接続プロファイルを編集します。



FMC UI内でDefaultWEBVPNGroupを編集する方法を表示します。

AAAタブに移動し、Authentication Methodドロップダウンを選択します。Client Certificate Onlyを選択し、Saveを選択します。

## Edit Connection Profile

Connection Profile:\* DefaultWEBVPNGroup

Group Policy:\* DfltGrpPolicy +  
[Edit Group Policy](#)

Client Address Assignment   **AAA**   Aliases

### Authentication

Authentication Method: Client Certificate Only ▼  
 Enable multiple certificate authentication

▶ Map username from client certificate

### Authorization

Authorization Server: ▼  
 Allow connection only if user exists in authorization database

### Accounting

Accounting Server: ▼

[Cancel](#) [Save](#)

FMC UI内のDefaultWEBVPNGroupに対してのみ、認証方式をクライアント証明書に変更します。

DefaultRAGroupを編集し、AAAタブに移動して、Authentication Methodドロップダウンを選択します。'Client Certificate Only'を選択し、Saveを選択します。

## Edit Connection Profile

Connection Profile:\*

Group Policy:\*  +

[Edit Group Policy](#)

Client Address Assignment

**AAA**

Aliases

### Authentication

Authentication Method:

Enable multiple certificate authentication

▶ Map username from client certificate

### Authorization

Authorization Server:

Allow connection only if user exists in authorization database

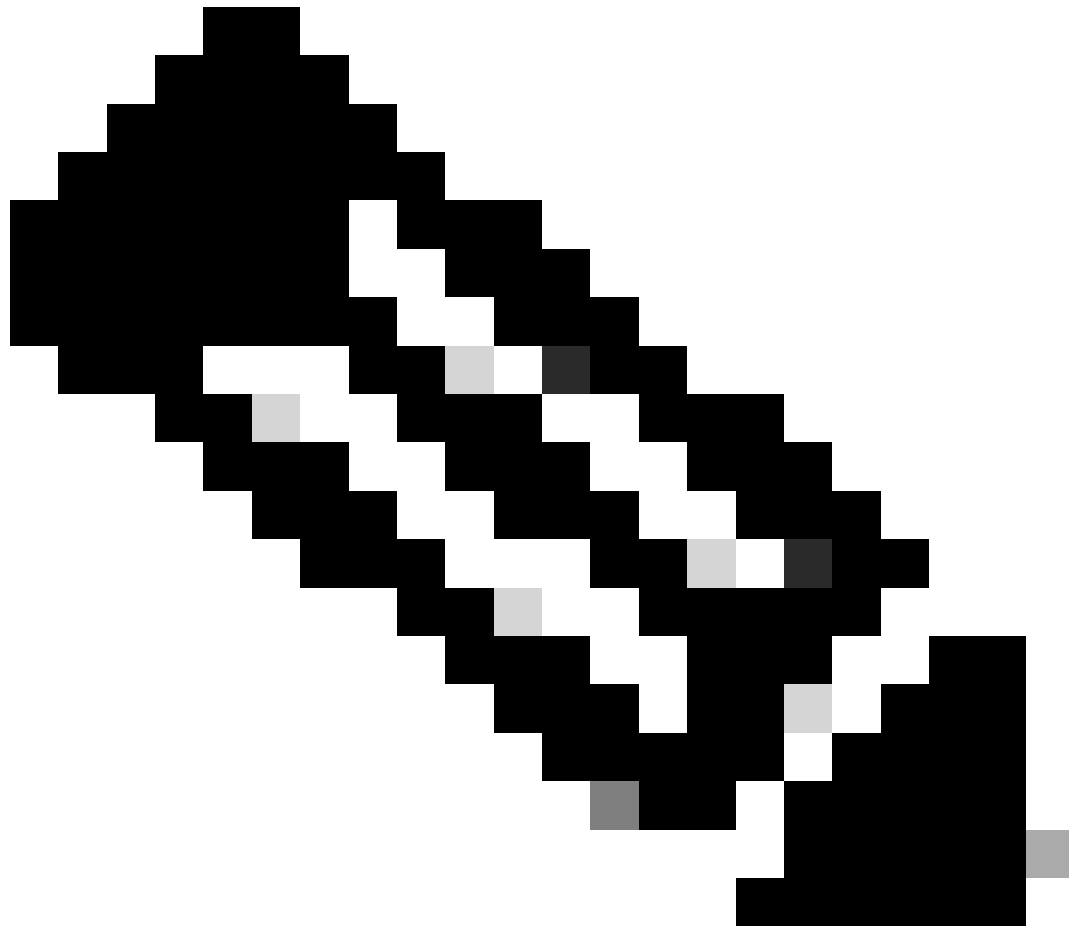
### Accounting

Accounting Server:

Cancel

Save

FMC UI内のDefaultRAGroupに対してだけ、認証方式をクライアント証明書に変更します。



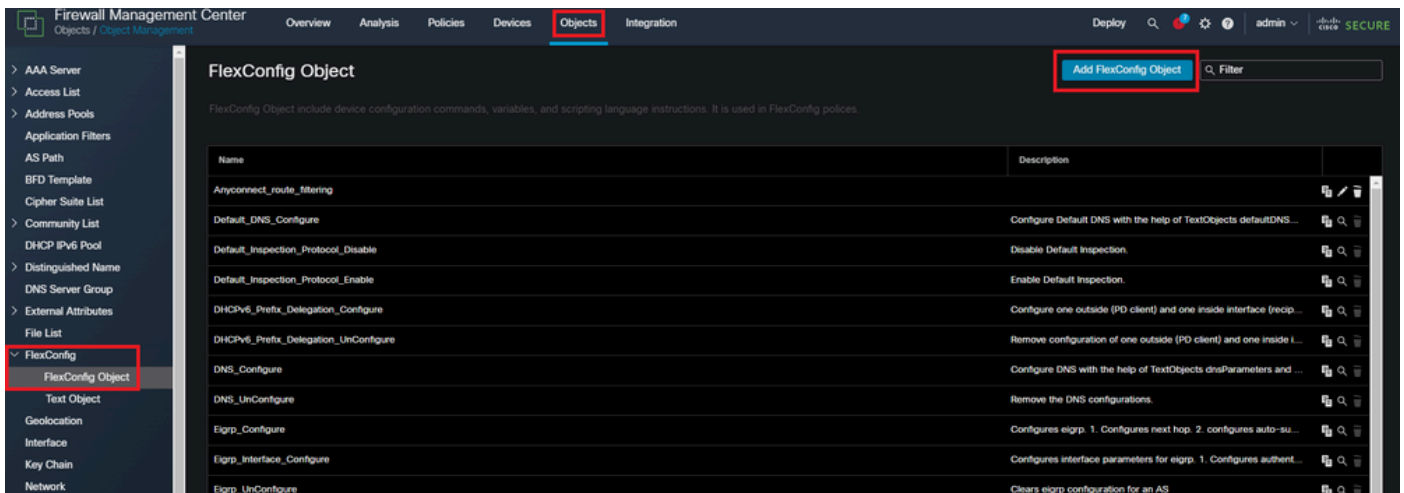
注：認証方式は、シンクホールAAAサーバにすることもできます。この方法を使用すると、AAAサーバの設定が誤って設定され、実際には要求が処理されません。変更を保存するには、「Client Address Assignment」タブでVPNプールを定義する必要もあります。

---

## DefaultWEBVPNGroupおよびDefaultRAGroupでホストスキャン/セキュアファイアウォールポスチャを無効にする（オプション）

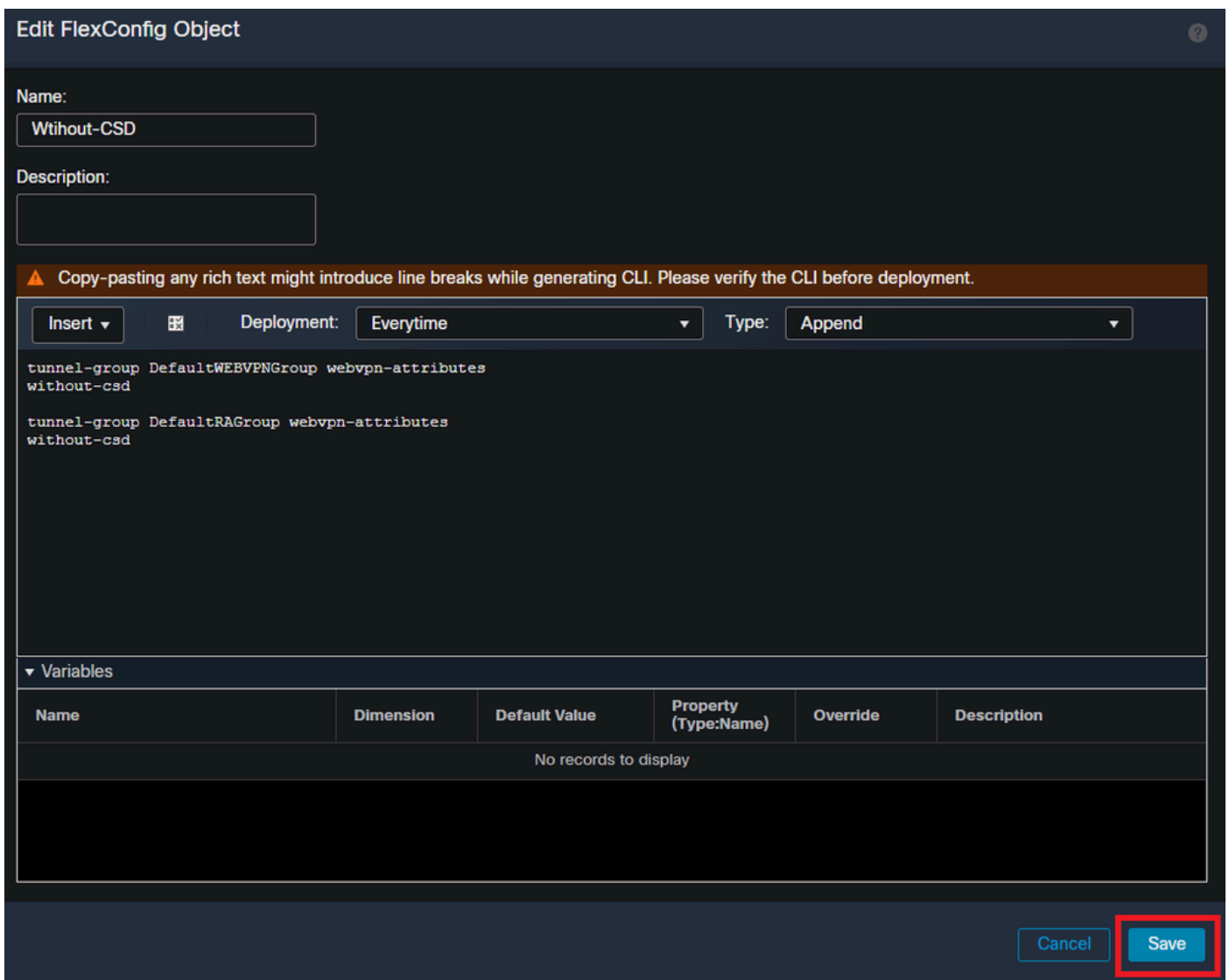
これは、環境内にホストスキャン/セキュアファイアウォールポスチャがある場合にのみ必要です。このステップにより、攻撃者はエンドポイントスキャンプロセスによってファイアウォールのリソース使用率を上げることができなくなります。FMCでこれを実現するには、without-csdコマンドを使用してFlexConfigオブジェクトを作成し、エンドポイントスキャン機能を無効にします。

Objects > Object Management > FlexConfig Object > Add FlexConfig Objectの順に移動します。



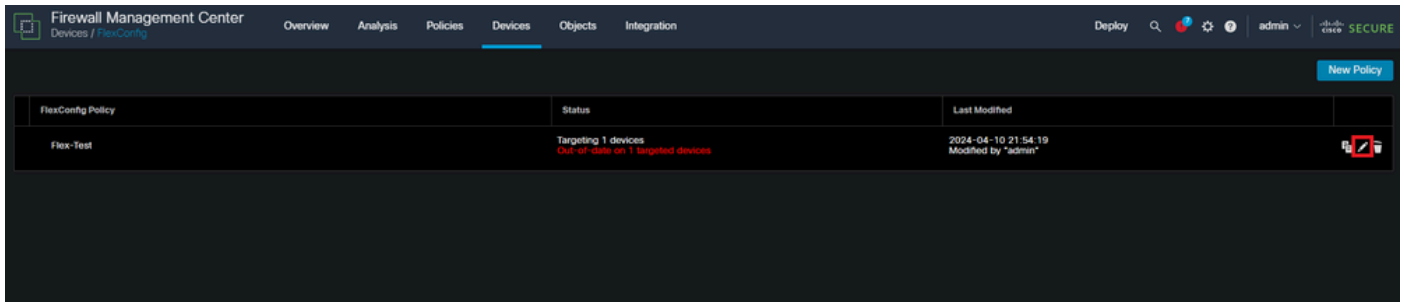
FMC UIでFlexConfigオブジェクトを作成する。

FlexConfigオブジェクトに名前を付け、タイプがAppendのデプロイメントをEverytimeに設定します。次に、表示されたとおりに構文を入力し、オブジェクトを保存します。



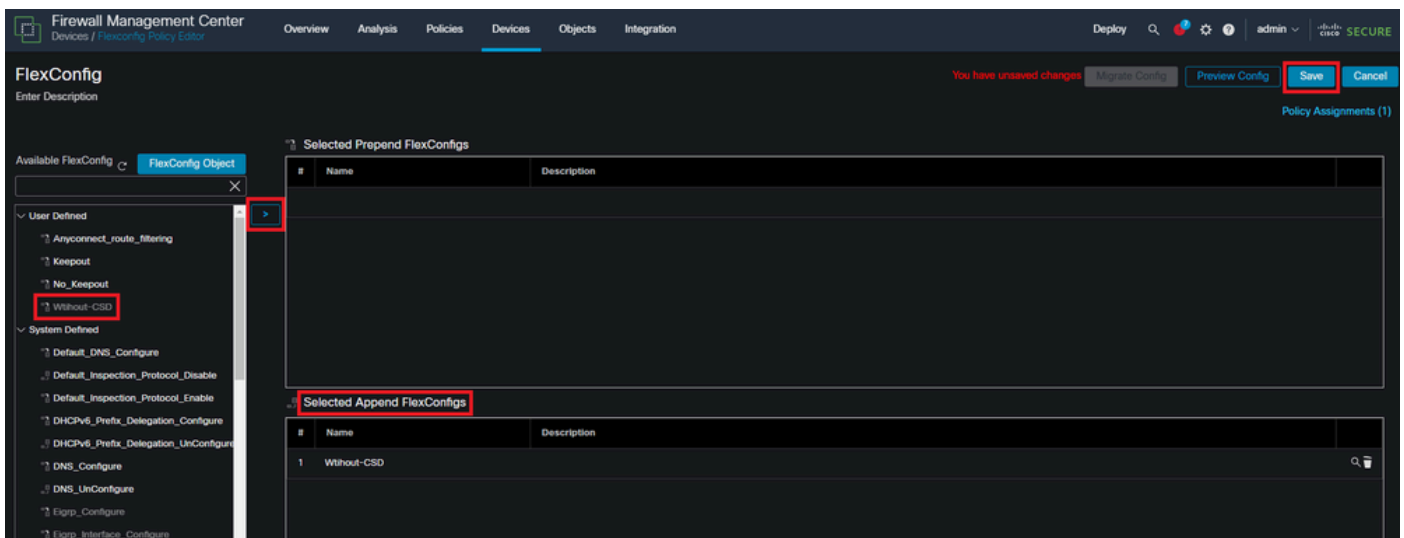
'without-csd'でFlexConfigオブジェクトを作成しています

Devices > FlexConfigの順に移動し、PencilをクリックしてFlexConfigポリシーを編集します。



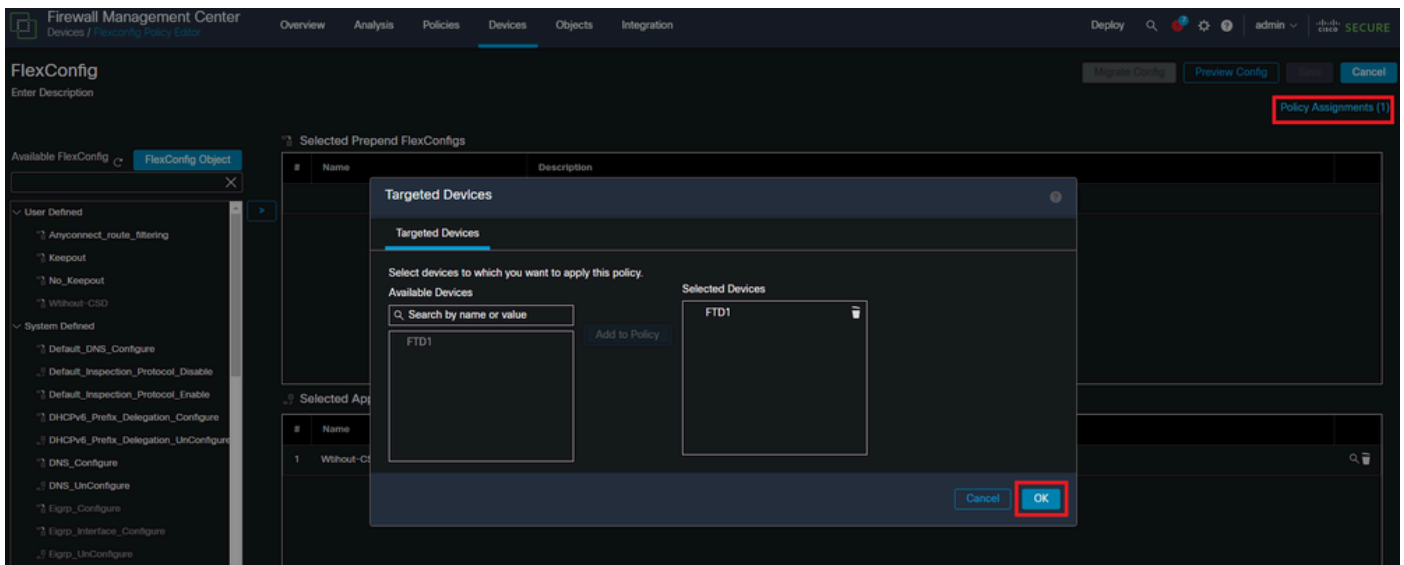
FMC内でFlexConfigポリシーを編集します。

「ユーザー定義」セクションで作成したオブジェクトを検索します。次に、矢印を選択して、Selected Append FlexConfigsに追加します。最後に、Saveを選択してFlexConfigポリシーを保存します。



FlexConfigオブジェクトをFlexConfigポリシーにアタッチします。

Policy Assignmentsを選択して、このFlexConfigポリシーを適用するFTDを選択してから、OKを選択します。これが新しいFlexConfigの割り当てである場合は、再度Saveを選択して、変更を適用します。導入後の検証



FlexConfigポリシーをFirePOWERデバイスに割り当てます。

FTD CLIに入り、DefaultWEBVPNGroupおよびDefaultRAGroupに対してshow run tunnel-groupコマンドを発行します。without-csdが設定に含まれていることを確認します。

```
<#root>
```

```
FTD72#
```

```
show run tunnel-group DefaultRAGroup
```

```
tunnel-group DefaultRAGroup general-attributes  
address-pool TEST-POOL  
tunnel-group DefaultRAGroup webvpn-attributes  
authentication certificate
```

```
without-csd
```

```
FTD72#
```

```
show run tunnel-group DefaultWEBVPNGroup
```

```
tunnel-group DefaultWEBVPNGroup general-attributes  
address-pool TEST-POOL  
tunnel-group DefaultWEBVPNGroup webvpn-attributes  
authentication certificate
```

```
without-csd
```

## グループエイリアスの無効化とグループURLの有効化

接続プロファイルに移動し、「エイリアス」タブを選択します。グループエイリアスを無効また

は削除し、プラス(+)アイコンをクリックしてURLエイリアスを追加します。

**Edit Connection Profile**

Connection Profile:\* LDAP-TG

Group Policy:\* DfltGrpPolicy +  
[Edit Group Policy](#)

Client Address Assignment   AAA   **Aliases**

**Alias Names:**  
Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off for display. +

Name	Status	
LDAP	Disabled	

**URL Alias:**  
Configure the list of URL alias which your endpoints can select on web access. If users choose the following URLs, system will automatically log them in via this connection profile. +

URL	Status	
-----	--------	--

FMCのUIでトンネルグループのgroup-aliasオプションを無効にする

URLエイリアスのオブジェクト名を設定し、URLのファイアウォールのFQDNまたはIPアドレスを入力し、続いて接続プロファイルを関連付ける名前を入力します。この例では、「aaaldap」を選択します。FQDNを取得した攻撃者が完全なURLを推測する可能性が低いいため、不明瞭なほど、安全性が高くなります。終了したら、Saveを選択します。



# Edit URL Objects



## Name

LDAP-ALIAS

## Description

## URL

https://ftd1 [redacted] .com/aaalda|

Allow Overrides

Cancel

Save

FMC UI内でのURLエイリアスオブジェクトの作成

ドロップダウンからURLエイリアスを選択し、Enabledボックスにチェックマークを入れて、OKを選択します。

# Add URL Alias



URL Alias:

LDAP-ALIAS



Enabled

Cancel

OK

URLエイリアスがFMC UI内で有効になっていることを確認します。

group-aliasが削除されているか無効になっているかを確認し、URL Aliasが有効になっていることを確認して、Saveを選択します。


## Edit Connection Profile

Connection Profile:\* LDAP-TG

Group Policy:\* DfltGrpPolicy [Edit Group Policy](#)


Client Address Assignment   AAA   **Aliases**

Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off for display.

Name	Status	
LDAP	<b>Disabled</b>	

URL Alias:

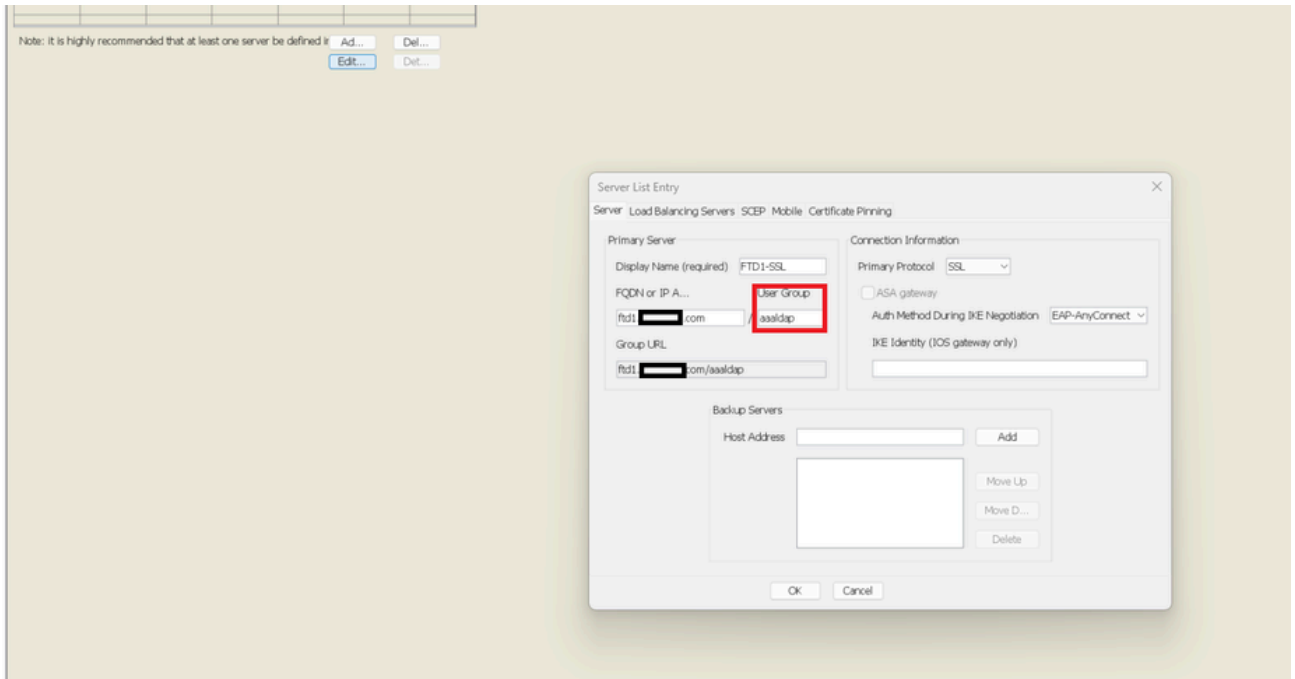
Configure the list of URL alias which your endpoints can select on web access. If users choose the following URLs, system will automatically log them in via this connection profile.

URL	Status	
LDAP-ALIAS (https://ftd1 [redacted] com/aaaldap)	<b>Enabled</b>	

[Cancel](#) [Save](#)

FMCのUIでトンネルグループのURLエイリアスオプションを有効にする

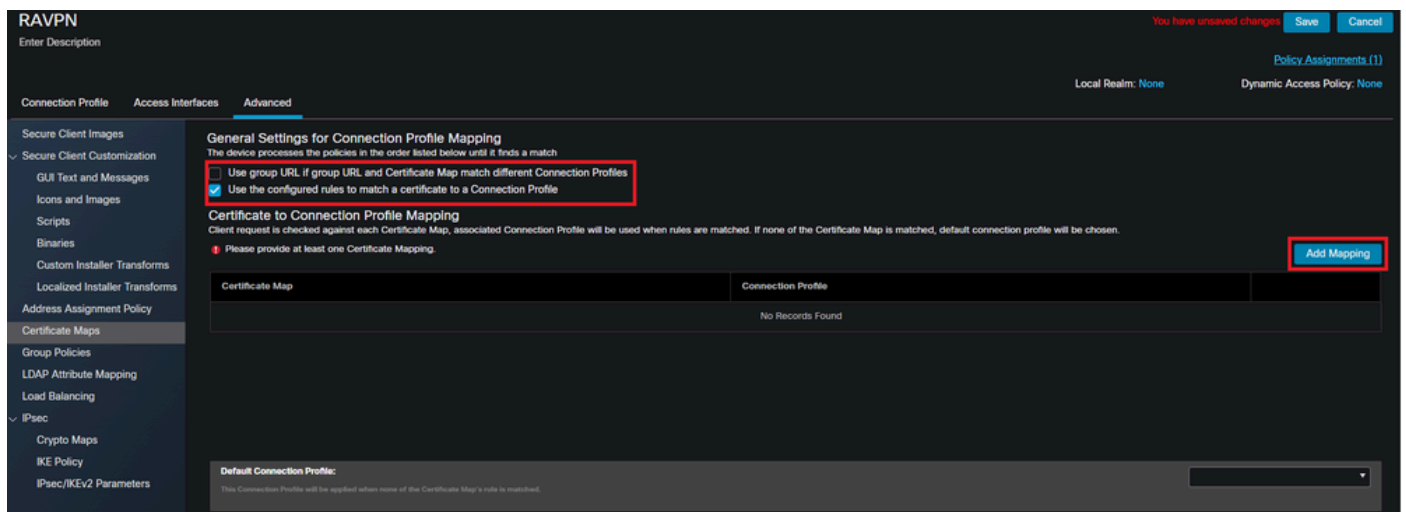
必要に応じて、URLエイリアスをXMLの一部としてプッシュすることもできます。これは、VPNプロファイルエディタまたはASAプロファイルエディタを使用してXMLを編集することで実現されます。これを行うには、Server Listタブに移動し、SSLを使用する場合はUser Groupフィールドが接続プロファイルのURLエイリアスと一致することを確認します。IKEv2では、User Groupフィールドが接続プロファイルの正確な名前と一致することを確認します。



SSL接続用のURLエイリアスを持つようにXMLプロファイルを編集します。

## 証明書マッピング

リモートアクセスVPNポリシー内のAdvancedタブに移動します。基本設定に基づいて一般設定オプションを選択します。選択したら、Add Mappingを選択します。



FMC UI内でAdvancedタブに移動して、FMC UI内に証明書マップオブジェクトを作成します。

証明書マップオブジェクトに名前を付け、Add Ruleを選択します。このルールでは、ユーザを特定の接続プロファイルにマッピングするために識別する証明書のプロパティを定義します。終了したら、OKを選択してからSaveを選択します。

## Add Certificate Map



Map Name\*:

Certificate-Map-CN

Mapping Rule

Add Rule

Configure the certificate matching rule

#	Field	Component	Operator	Value
1	Subject ▼	CN (Common Name) ▼	Equals ▼	customvalue

OK

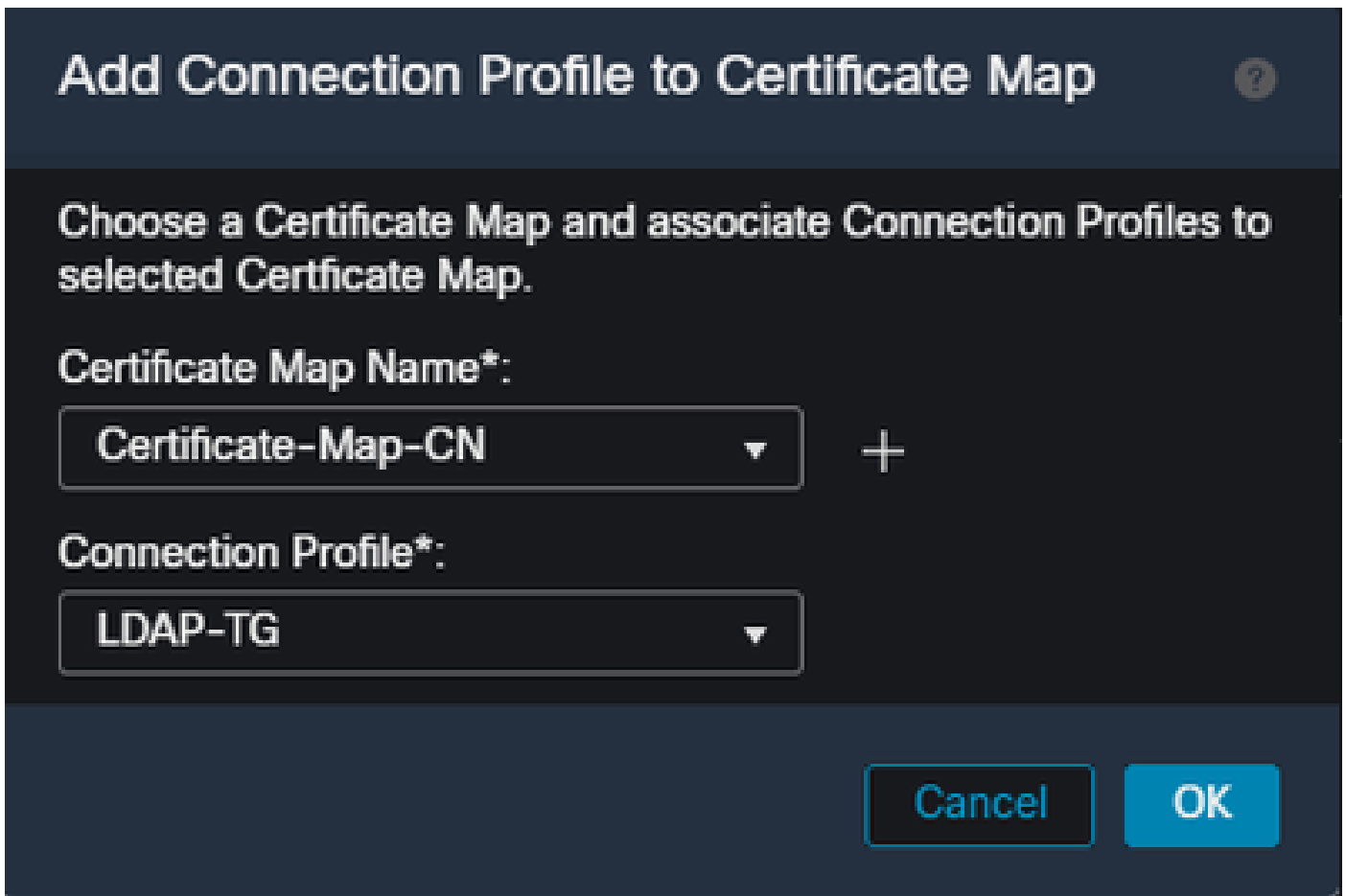
Cancel

Cancel

Save

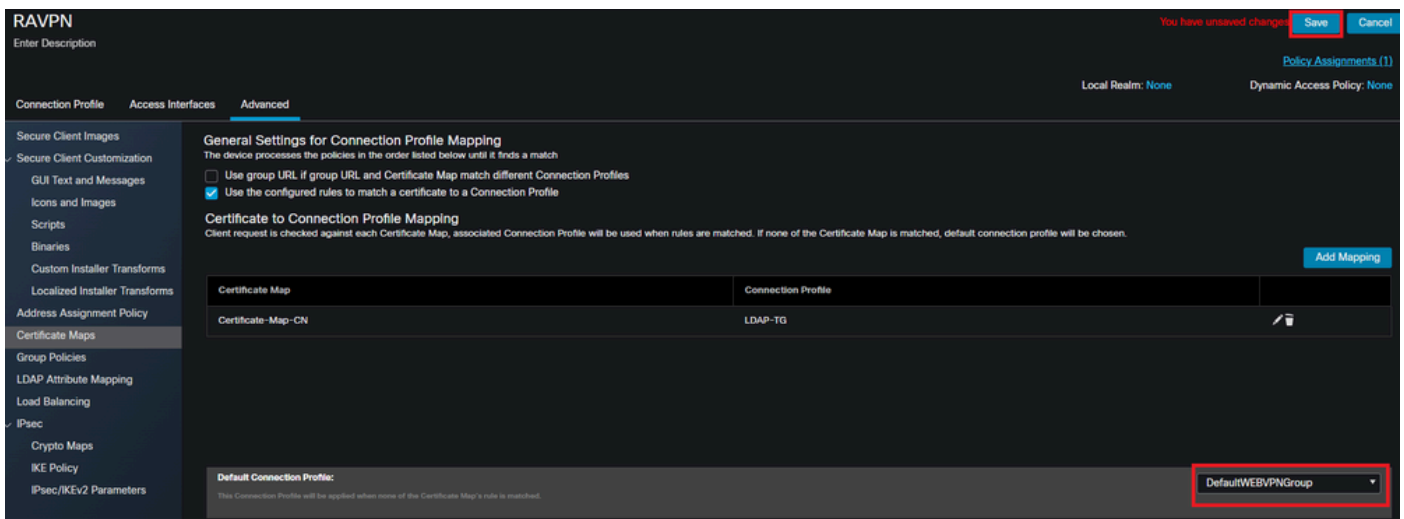
証明書マップを作成し、FMCのUIでマップの基準を追加します。

ドロップダウンから、証明書マップオブジェクトと、証明書マップを関連付ける接続プロファイルを選択します。次にOKを選択します。



証明書マップオブジェクトをFMC UI内の目的のトンネルグループに関連付けます。

ユーザがマッピングに失敗するとDefaultWEBVPNGroupに送信されるように、デフォルト接続プロファイルがDefaultWEBVPNGroupとして設定されていることを確認します。完了したら、Saveを選択して、変更を適用します。



証明書マッピングのデフォルト接続プロファイルをFMC UI内のDefaultWEBVPNGroupに変更します。

## IPsec-IKEv2

目的のIPsec-IKEv2接続プロファイルを選択し、Edit Group Policyに移動します。

## Edit Connection Profile

Connection Profile:\* IKEV2

Group Policy:\* IKEV2-IPSEC +

[Edit Group Policy](#)

**Client Address Assignment**   AAA   Aliases

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the 'Client Address Assignment Policy' in the Advanced tab to define the assignment criteria.

Address Pools: +

Name	IP Address Range	
AnyConnect_Pool	10.50.50.1-10.50.50.6	

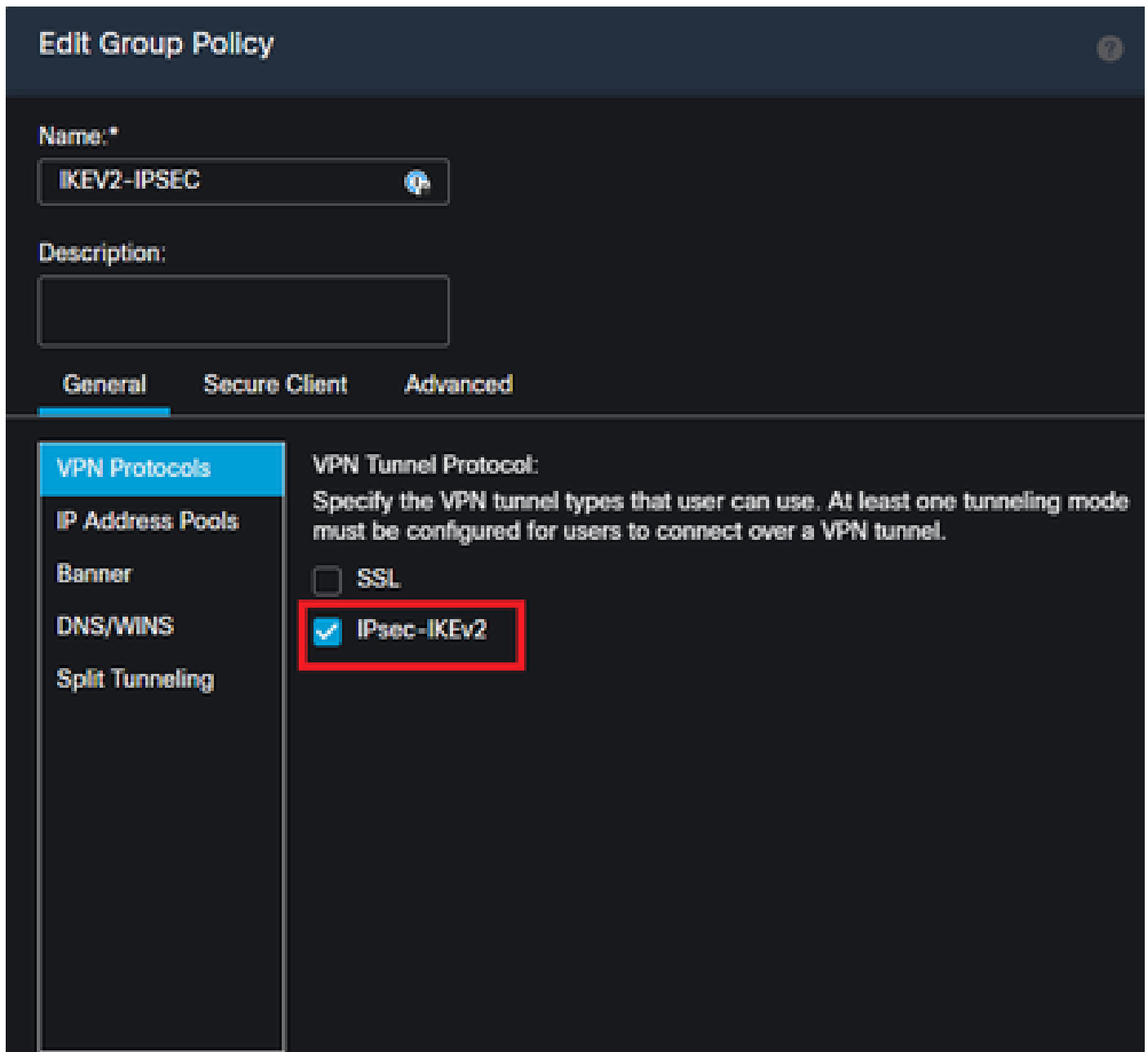
DHCP Servers: +

Name	DHCP Server IP Address	

[Cancel](#) [Save](#)

FMC UI内でグループポリシーを編集します。

Generalタブで、VPN Protocolsセクションに移動し、IPsec-IKEv2ボックスにチェックマークが付いていることを確認します。



FMC UIのグループポリシー内でIPsec-IKEv2を有効にします。

VPNプロファイルエディタまたはASAプロファイルエディタで、Server Listタブに移動します。ユーザグループ名は、ファイアウォール上の接続プロファイル名と完全に一致している必要があります。この例では、IKEV2は接続プロファイル/ユーザグループ名です。プライマリプロトコルがIPsecとして設定されている。の「表示名」は、この接続プロファイルへの接続を確立するときに、セキュアクライアントUIでユーザに表示されます。



Server List Entry

Server Load Balancing Servers SCEP Mobile Certificate Pinning

Primary Server

Display Name (required) FTD1-IPSEC

FQDN or IP A... User Group

ftd1[redacted].com / IKEV2

Group URL

Connection Information

Primary Protocol IPsec

ASA gateway

Auth Method During IKE Negotiation EAP-AnyConnect

IKE Identity (IOS gateway only)

Backup Servers

Host Address [ ] Add

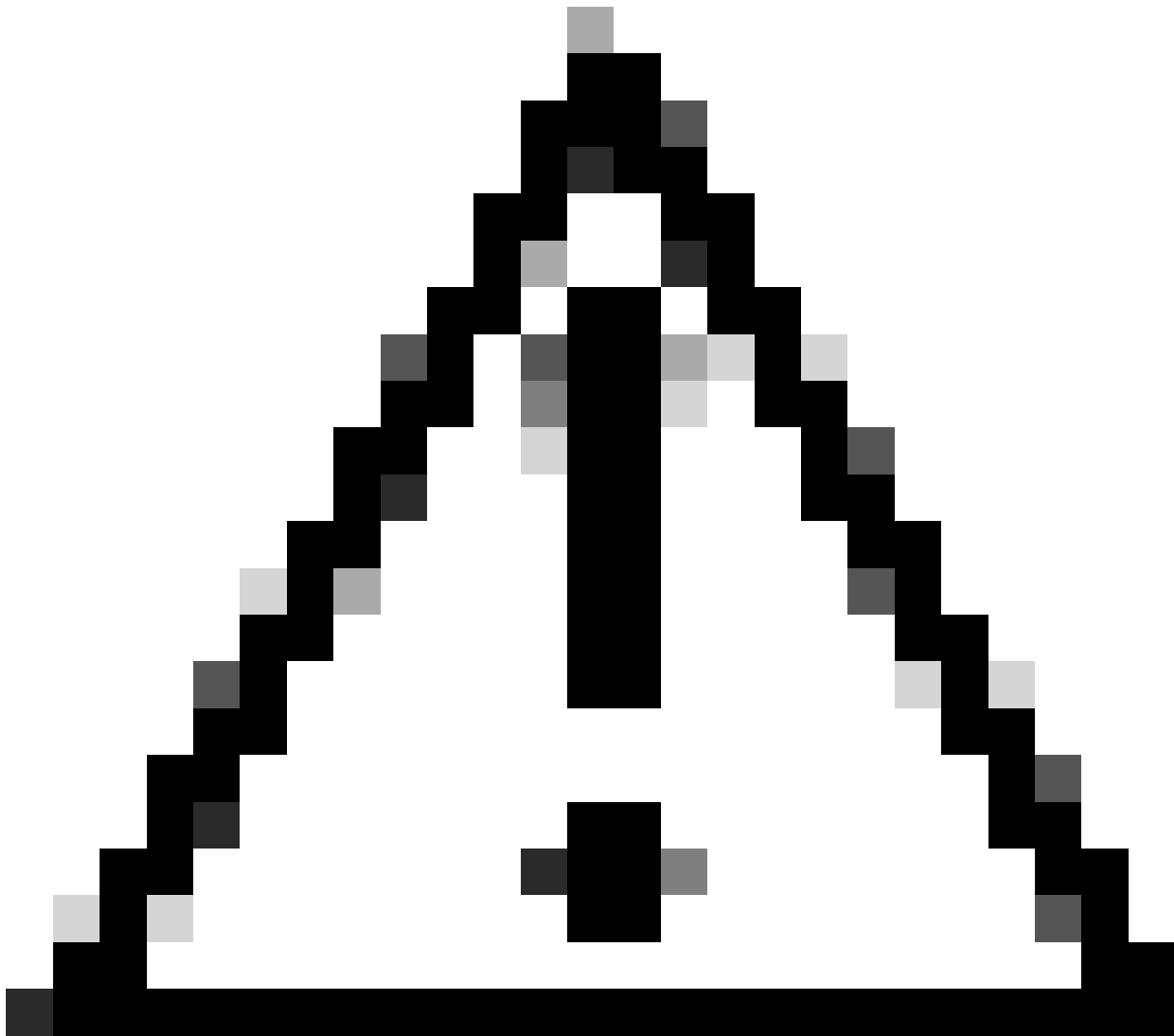
[ ] Move Up

[ ] Move D...

[ ] Delete

OK Cancel

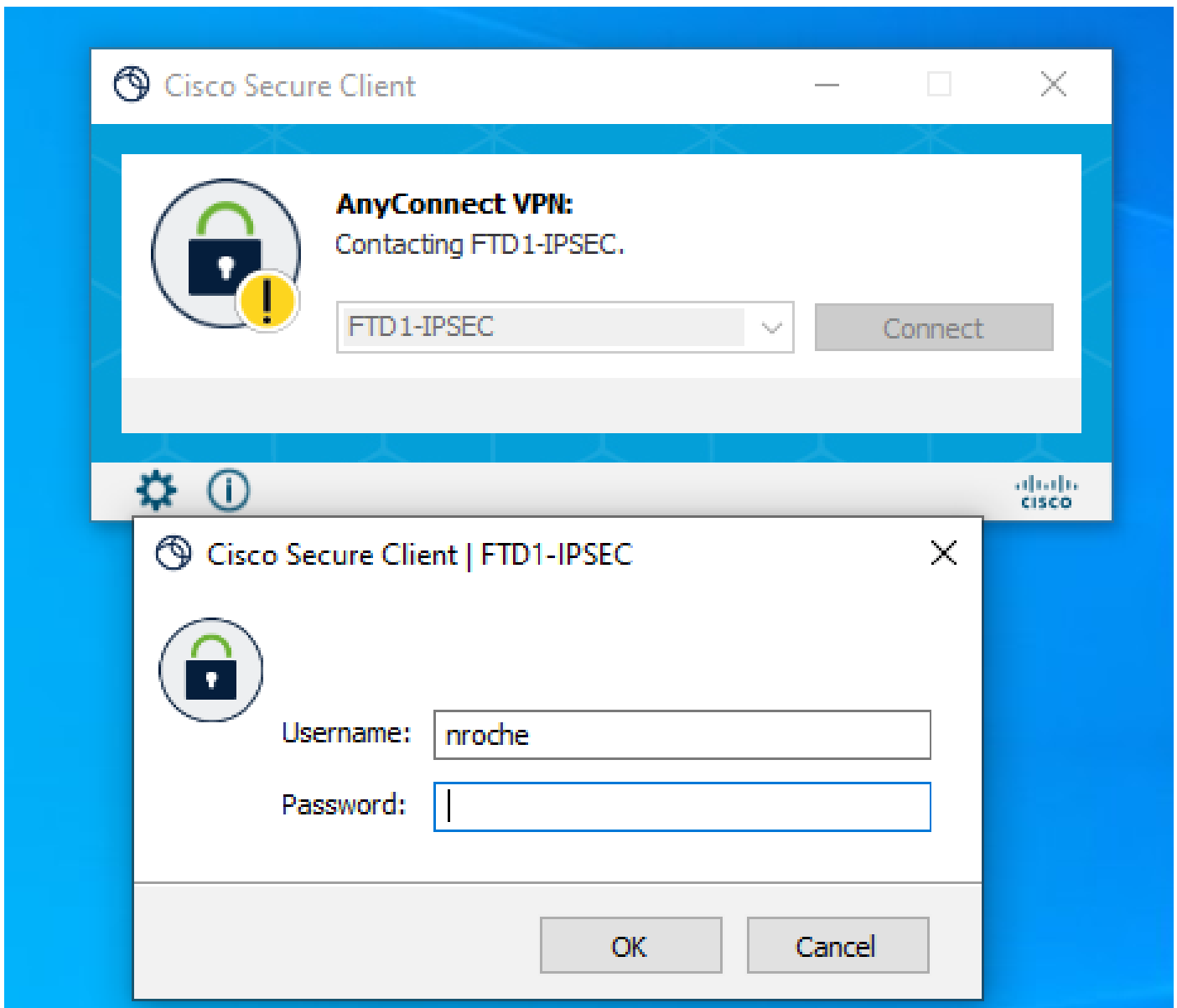
プライマリプロトコルがIPsecで、ユーザグループが接続プロファイル名と一致するようにXMLプロファイルを編集します。



注意：ファイアウォールからクライアントにXMLプロファイルをプッシュするには、SSL接続が必要です。IKEV2-IPsecのみを使用している場合、XMLプロファイルはアウトオブバンド方式でクライアントにプッシュする必要があります。

---

XMLプロファイルをクライアントにプッシュすると、セキュアクライアントはXMLプロファイルのユーザグループを使用して、IKEV2-IPsec接続プロファイルに接続します。



IPsec-IKEv2 RAVPN接続のセキュアクライアントUIビュー。

## ASAの設定例

DefaultWEBVPNGroupおよびDefaultRAGroup接続プロファイルでのAAA認証の無効化

tunnel-group DefaultWEBVPNGroupにwebvpn-attributesセクションを入力し、証明書ベースとして認証を指定します。DefaultRAGroupに対してこのプロセスを繰り返します。これらのデフォルトの接続プロファイルを使用するユーザは、認証用の証明書を提示することを強制され、ユーザ名とパスワードのクレデンシャルを入力する機会はありません。

```
ASA# configure terminal
ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes
ASA(config-tunnel-webvpn)# authentication certificate
```

```
ASA# configure terminal
```

```
ASA(config)# tunnel-group DefaultRAGroup webvpn-attributes
ASA(config-tunnel-webvpn)# authentication certificate
```

## DefaultWEBVPNGroupおよびDefaultRAGroupでホストスキャン/セキュアファイアウォールポスチャを無効にする ( オプション )

これは、環境内にホストスキャン/セキュアファイアウォールポスチャがある場合にのみ必要です。このステップにより、攻撃者はエンドポイントスキャンプロセスによってファイアウォールのリソース使用率を上げることができなくなります。DefaultWEBVPNGroup、DefaultRAGroup、および接続プロファイルのwebvpn-attributesセクションに入り、without-csdを実装して、エンドポイントスキャン機能を無効にします。

```
ASA# configure terminal
ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes
ASA(config-tunnel-webvpn)# without-csd
```

```
ASA# configure terminal
ASA(config)# tunnel-group DefaultRAGroup webvpn-attributes
ASA(config-tunnel-webvpn)# without-csd
```

## グループエイリアスの無効化とグループURLの有効化

ユーザが接続するトンネルグループを入力します。既存のグループエイリアスがある場合は、無効にするか、削除します。この例では無効になっています。これが完了したら、RAVPN終端インターフェイスのFQDNまたはIPアドレスを使用してグループURLを作成します。グループURLの末尾の名前は分かりにくい必要があります。VPN、AAA、RADIUS、LDAPなどの一般的な値は、攻撃者がFQDNを取得する際に完全なURLを推測しやすくなるため、使用しないでください。代わりに、トンネルグループの識別に役立つ内部的に有意な名前を使用します。

```
ASA# configure terminal
ASA(config)# tunnel-group NAME webvpn-attributes
ASA(config-tunnel-webvpn)# group-alias NAME disable
ASA(config-tunnel-webvpn)# group-url https://FQDN/name enable
```

## 証明書マッピング

グローバルコンフィギュレーションモードで、証明書マップを作成し、名前とシーケンス番号を割り当てます。次に、マッピングを利用するためにユーザが照合する必要があるルールを定義します。この例では、ユーザは「customvalue」と等しい共通名の値の基準に一致する必要があります。次に、webvpn設定を入力し、目的のトンネルグループに証明書マップを適用します。完了したら、DefaultWEBVPNGroupを入力し、証明書マッピングに失敗したユーザのデフォルトをこ

のトンネルグループにします。ユーザがマッピングに失敗すると、DefaultWEBVPNGroupにリダイレクトされます。DefaultWEBVPNGroupに証明書認証が設定されている場合、ユーザはユーザ名またはパスワードのクレデンシャルを渡すオプションを使用できません。

```
ASA(config)# crypto ca certificate map NAME 1
ASA(config-ca-cert-map)# subject-name attr cn eq customvalue

ASA(config)# webvpn
ASA(config-webvpn)# certificate-group-map NAME 1 TG-NAME

ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes
ASA(config-tunnel-webvpn)# tunnel-group-map default-group
```

## IPsec-IKEv2

グローバルコンフィギュレーションモードから、既存のグループポリシーを編集したり、新しいグループポリシーを作成して、そのグループポリシーの属性を入力したりできます。属性セクションに移動したら、IKEv2を唯一のVPNトンネルプロトコルとして有効にします。このグループポリシーが、IPsec-IKEv2リモートアクセスVPN接続に使用されるトンネルグループに関連付けられていることを確認します。FMCの手順と同様に、VPNプロファイルエディタまたはASAプロファイルエディタを使用してXMLプロファイルを編集し、User GroupフィールドをASAのトンネルグループの名前に一致するように変更し、プロトコルをIPsecに変更する必要があります。

```
ASA# configure terminal
ASA(config)# group-policy GP-NAME internal
ASA(config)# group-policy GP-NAME attributes
ASA(config-group-policy)# vpn-tunnel-protocol ikev2

ASA(config)# tunnel-group TG-NAME general-attributes
ASA(config-tunnel-general)# default-group-policy GP-NAME
```

VPNプロファイルエディタまたはASAプロファイルエディタで、Server Listタブに移動します。ユーザグループ名は、ファイアウォール上の接続プロファイル名と完全に一致する必要があります。プライマリプロトコルがIPsecとして設定されている。表示名は、この接続プロファイルへの接続を確立するときに、セキュアクライアントUIでユーザに表示されます。

Server List Entry

Server Load Balancing Servers SCEP Mobile Certificate Pinning

Primary Server

Display Name (required) ASA-IPsec

FQDN or IP A... User Group

FQDN TG-NAME

Group URL

FQDN/TG-NAME

Connection Information

Primary Protocol IPsec

ASA gateway

Auth Method During IKE Negotiation EAP-AnyConnect

IKE Identity (IOS gateway only)

Backup Servers

Host Address

Add

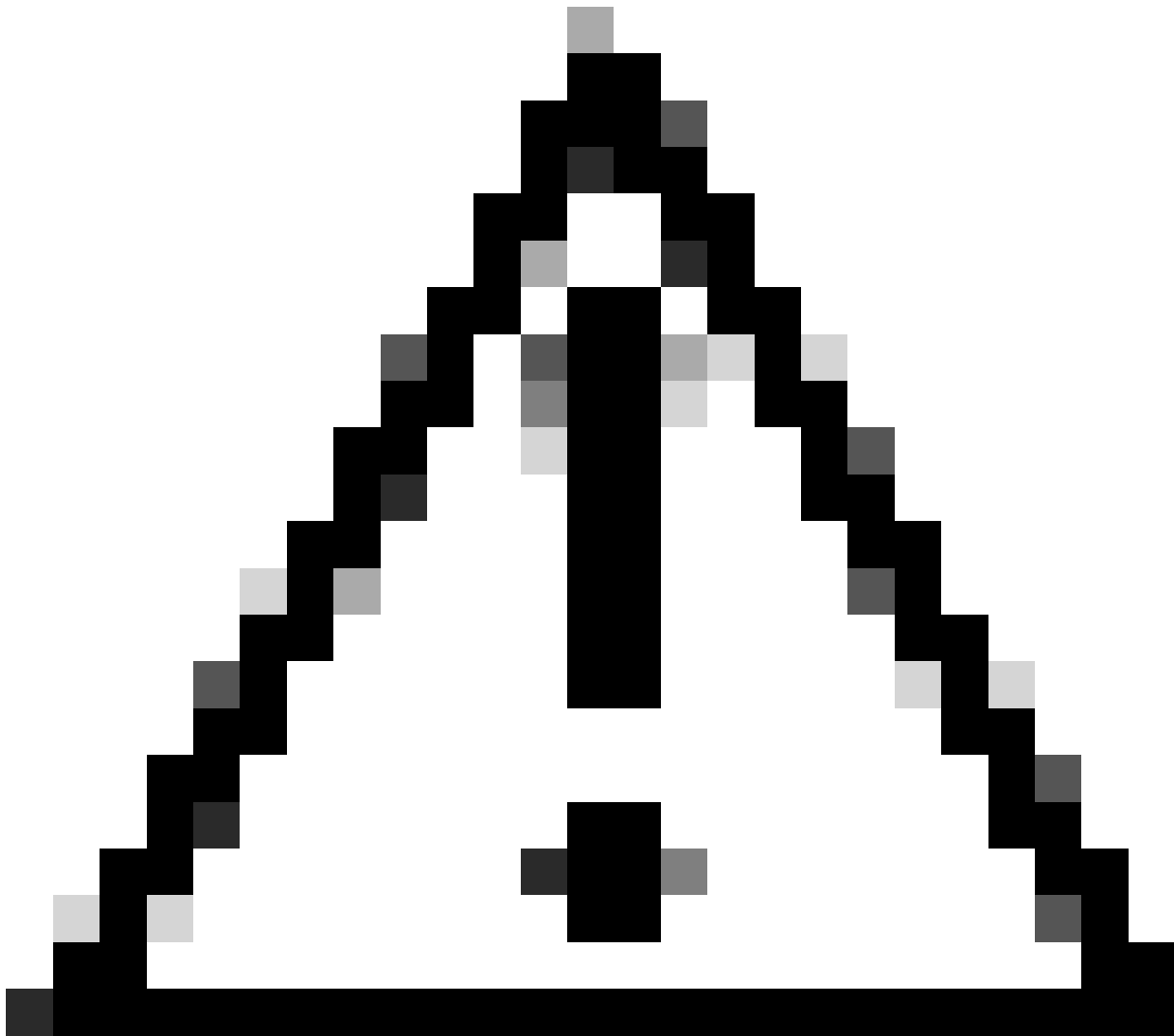
Move Up

Move D...

Delete

OK Cancel

プライマリプロトコル名がIPsecで、ユーザグループ名がIPsec-IKEv2 RAVPN接続用ASAのトンネルグループ名と一致するように、XMLプロファイルを編集します。



注意：ファイアウォールからクライアントにXMLプロファイルをプッシュするには、SSL接続が必要です。IKEV2-IPsecのみを使用している場合、XMLプロファイルはアウトオブバンド方式でクライアントにプッシュする必要があります。

---

## 結論

要約すると、このドキュメントの強化策の目的は、攻撃者がDefaultWEBVPNGroupとDefaultRAGroupに強制されている間に、正当なユーザをカスタム接続プロファイルにマッピングすることです。最適化された設定では、2つのデフォルトの接続プロファイルに正規のカスタムAAAサーバ設定はありません。また、グループエイリアスを削除すると、ファイアウォールのFQDNまたはパブリックIPアドレスに移動するときにドロップダウンの表示が削除されるため、攻撃者がカスタム接続プロファイルを簡単に識別できなくなります。

## 関連情報

[シスコテクニカルサポートとダウンロード](#)

[パスワードスプレー攻撃](#)

[不正アクセスの脆弱性2023年9月](#)

[ASA設定ガイド](#)

[EMC/FDM構成ガイド](#)



## 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。