ISEでのIKEv2によるFTDへのAnyConnect VPNの設定

内容

はじめに

このドキュメントでは、FMCによって管理されるFTDでのIKEv2およびISE認証を使用したリモートアクセスVPN(RVPN)の基本設定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。

- 基本的なVPN、TLS、およびインターネットキーエクスチェンジバージョン2(IKEv2)
- 基本認証、許可、アカウンティング(AAA)およびRADIUS
- Firepower Management Center(FMC)の使用経験

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Cisco Firepower Threat Defense(FTD)7.2.0
- Cisco FMC 7.2.0
- AnyConnect 4.10.07073
- Cisco ISE 3.1

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

IKEv2とSecure Sockets Layer(SSL)はどちらも、特にVPNのコンテキストでセキュアな接続を確立するために使用されるプロトコルです。IKEv2は、強力な暗号化方式と認証方式を提供し、VPN接続に高レベルのセキュリティを提供します。

このドキュメントでは、Transport Layer Security(TLS)とIKEv2を使用するためにリモートアクセスVPNを可能にするFTDバージョン7.2.0以降の設定例を示します。Cisco AnyConnectはクライアントとして使用でき、複数のプラットフォームでサポートされています。

設定

1. SSL証明書のインポート

証明書は、AnyConnectが設定されている場合に不可欠です。

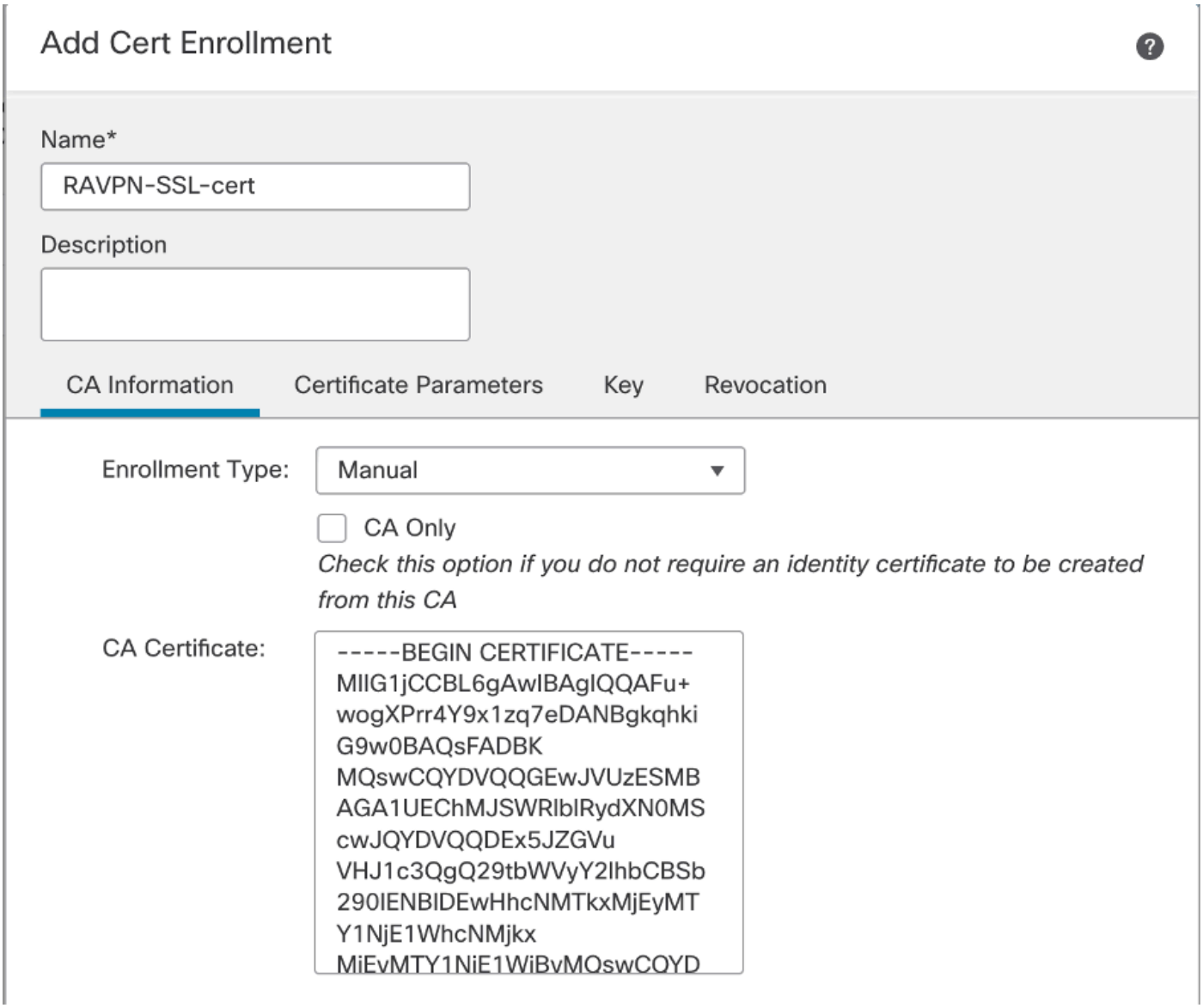
証明書の手動登録には制限があります。
1. FTDでは、証明書署名要求(CSR)を生成する前に認証局(CA)証明書が必要です。
2. CSRが外部で生成される場合、PKCS12の別の方法が使用されます。

FTDアプライアンスで証明書を取得する方法はいくつかありますが、安全で簡単な方法は、CSRを作成し、CAによって署名してもらうことです。その方法を次に示します。

1. Objects > Object Management > PKI > Cert Enrollmentに移動し、Add Cert Enrollmentをクリックします。

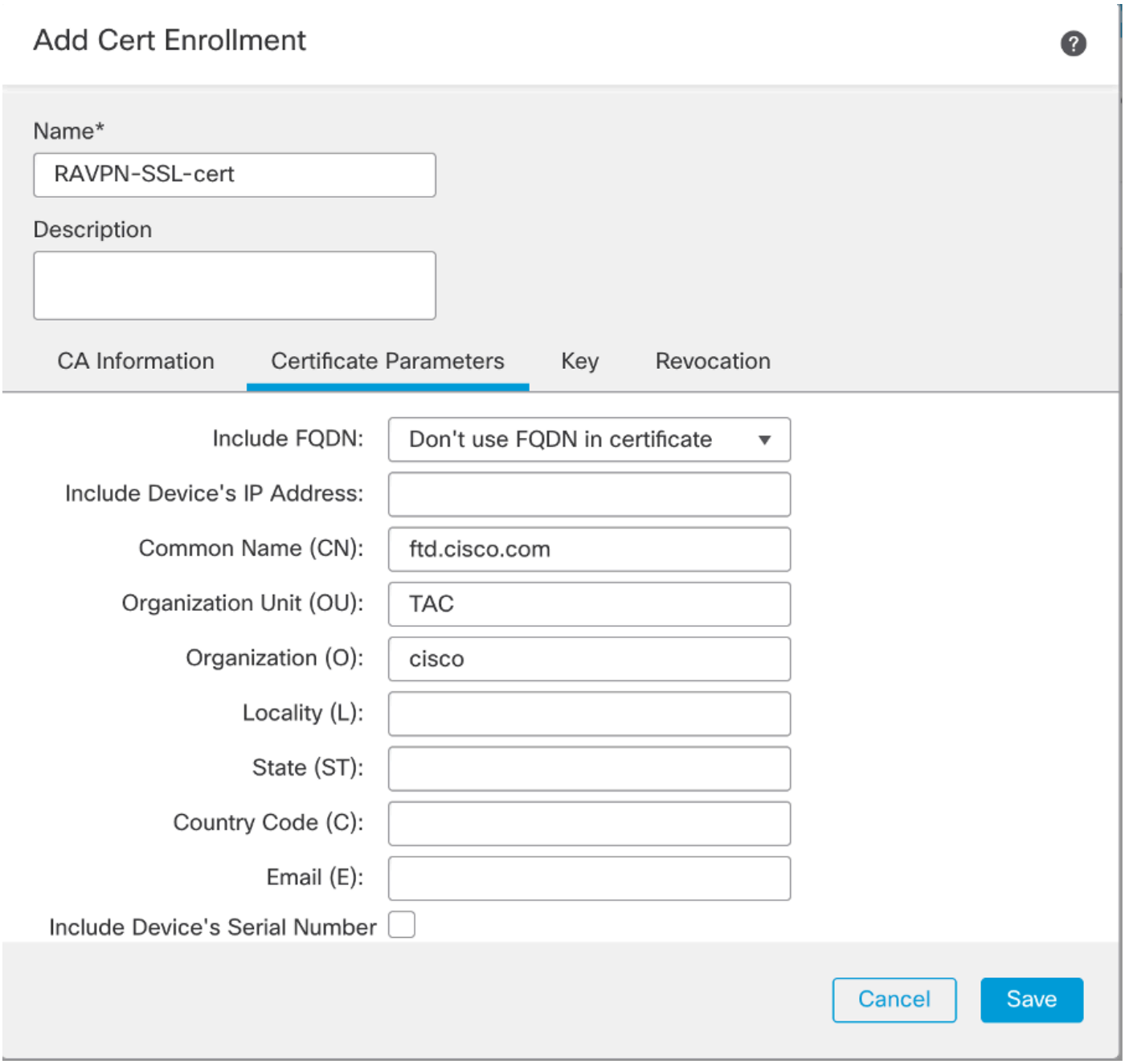
2. トラストポイント名RAVPN-SSL-certを入力します。

3. CA Informationタブで、登録タイプとしてManualを選択し、図に示すようにCA証明書を貼り付けます。



*FMC:CA*証明書

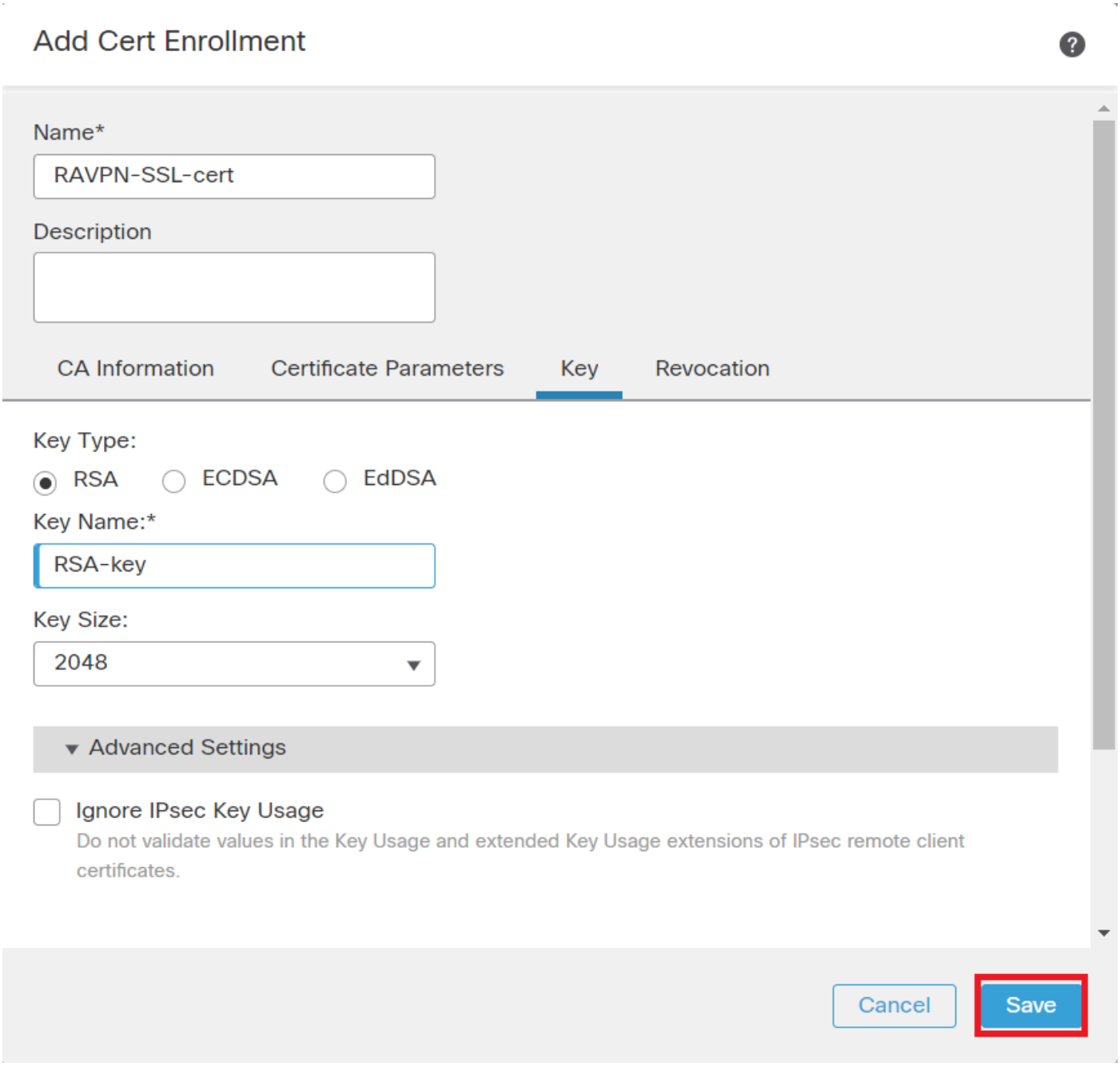
4.「Certificate Parameters」で、サブジェクト名を入力します。例：



FMC:Certificate Parameters（証明書パラメータ）

5. Key タブで、キー・タイプを選択し、名前とビット・サイズを指定します。RSAでは、2048ビットが最小です。

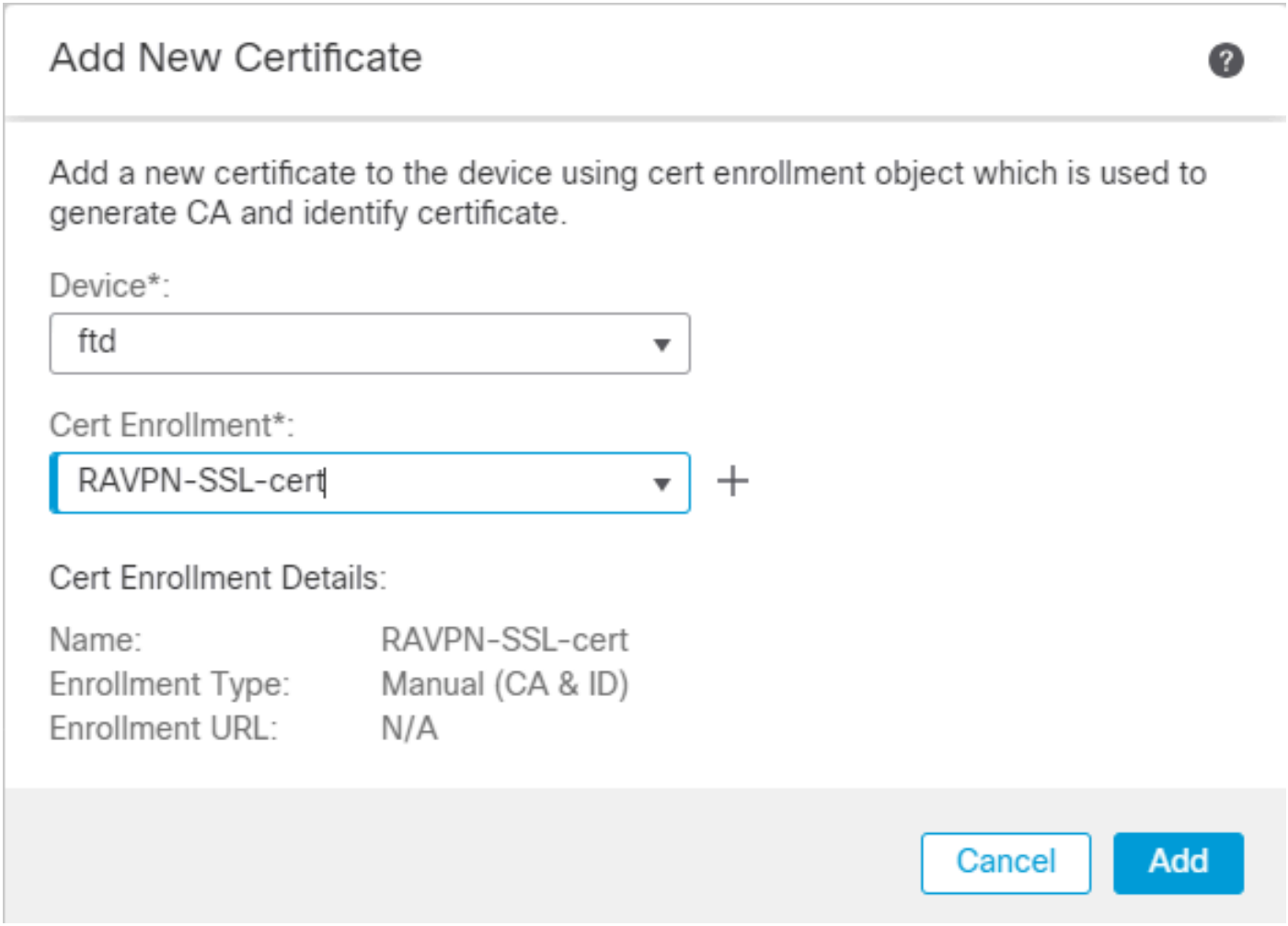
6. Saveをクリックします。



FMC:Certificate Key（証明書キー）

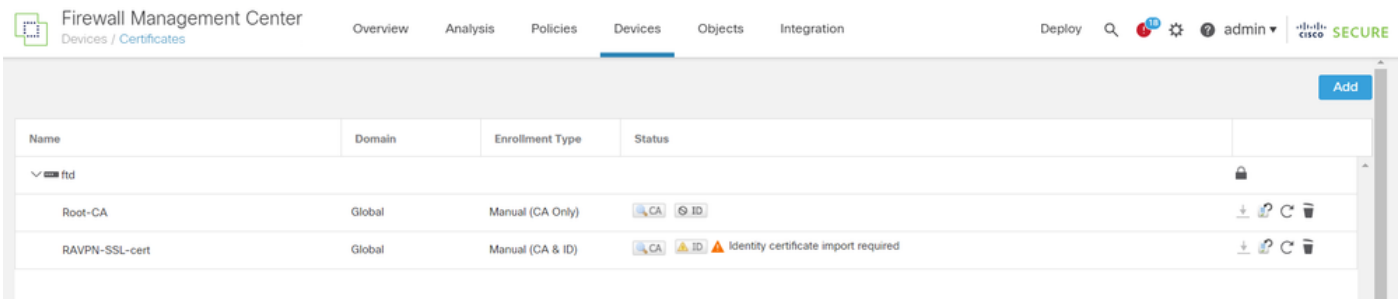
7. Devices > Certificates > Add > New Certificateに移動します。

8. Deviceを選択します。Cert Enrollmentで、作成したトラストポイントを選択し、図に示すようAddにクリックします。

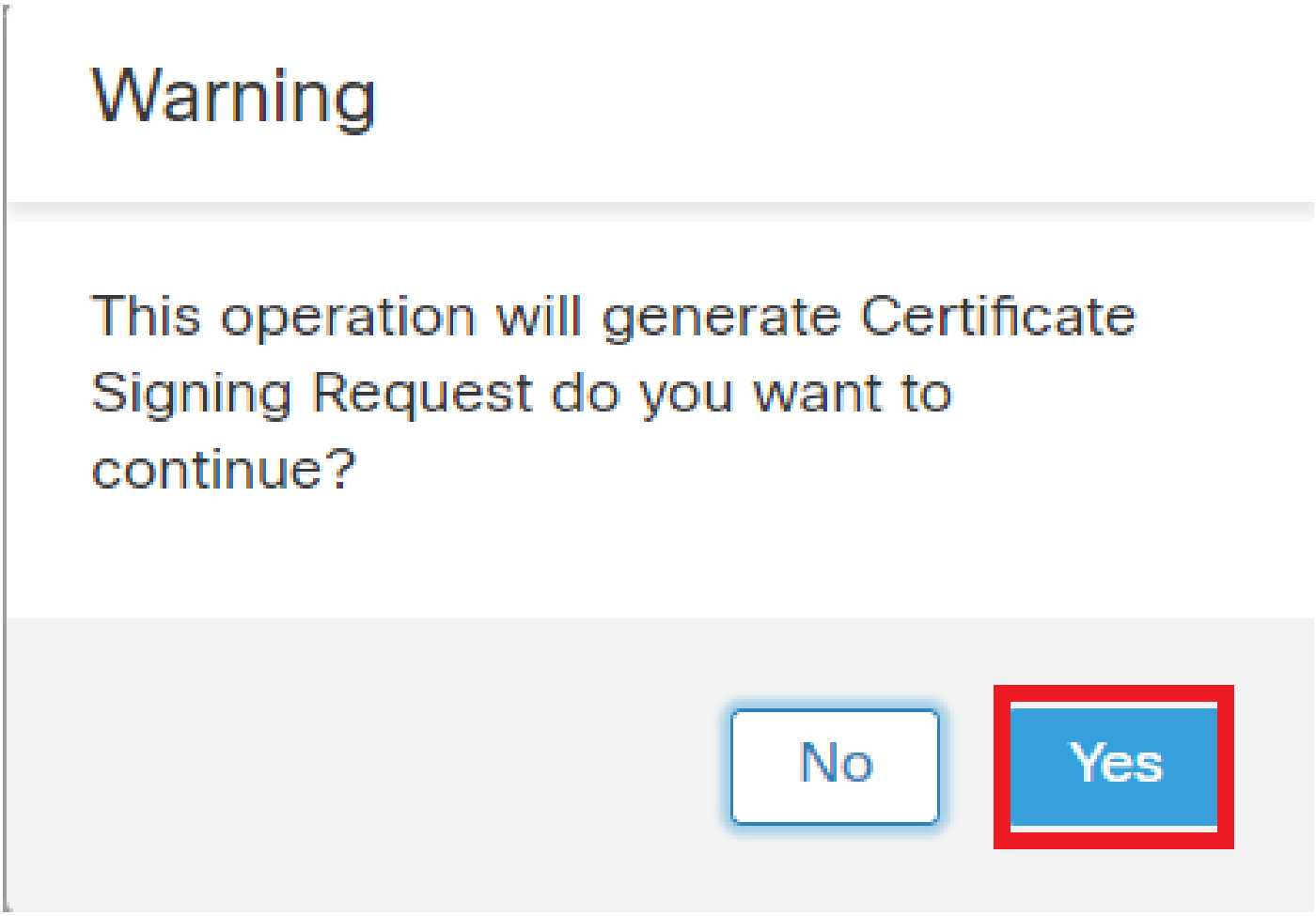


*FMC:FTD*への証明書の登録

9.「ID」をクリックし、CSRを生成するためのプロンプトが表示されたら、「Yes」を選択します。



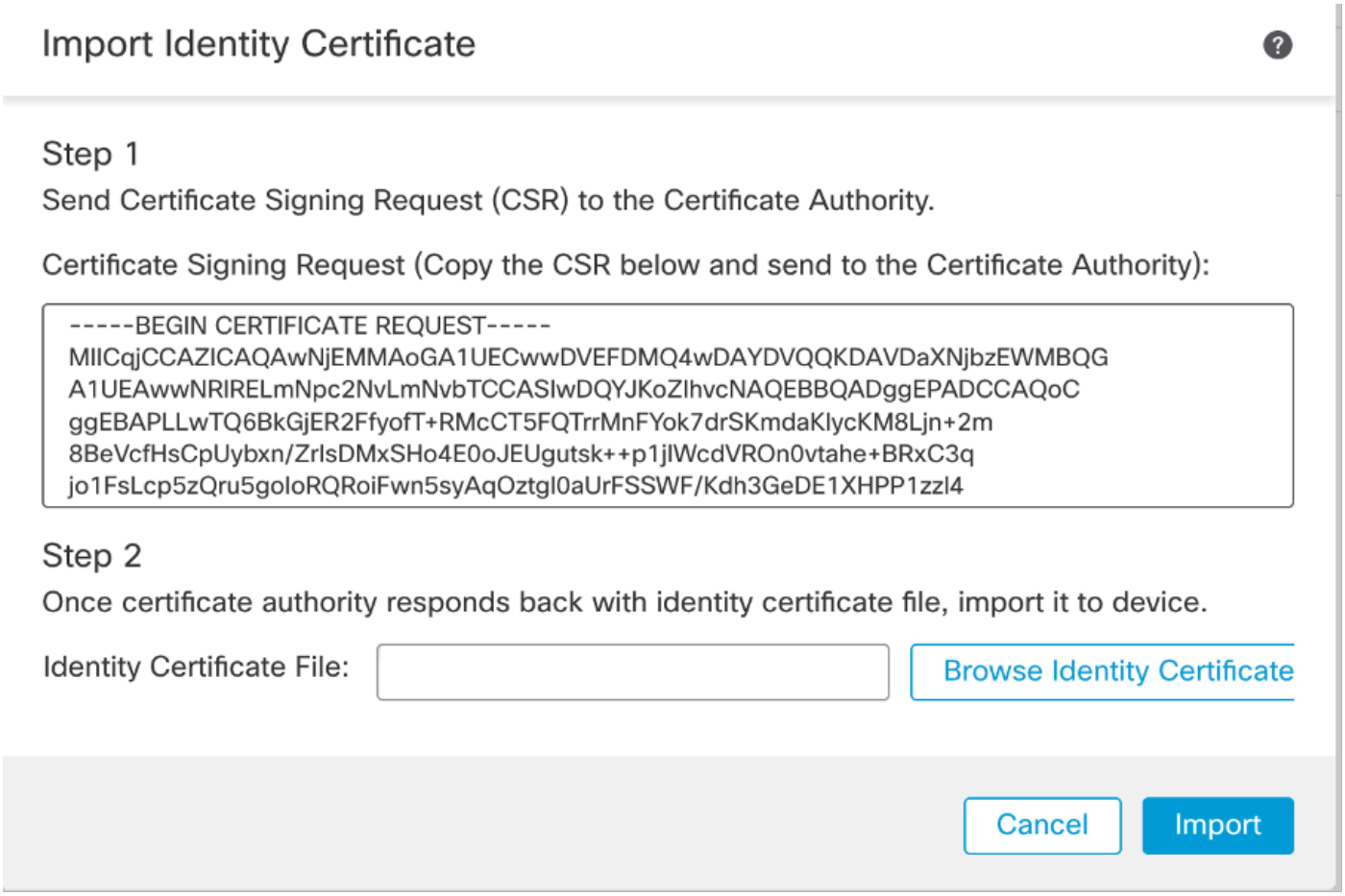
FMC:Certificate CA Enrolled（証明書*CA*登録済み）



FMC:CSRの生成

10. CSRが生成されます。CSRは、ID証明書を取得するためにCAと共有できます。

11. Base64形式のCAからID証明書を受信したら、図のようにBrowse Identity CertificateおよびImportをクリックしてディスクから選択します。



*FMC:ID*証明書のインポート

12. インポートが成功すると、トラストポイントは次のように表示されRAVPN-SSL-certます。

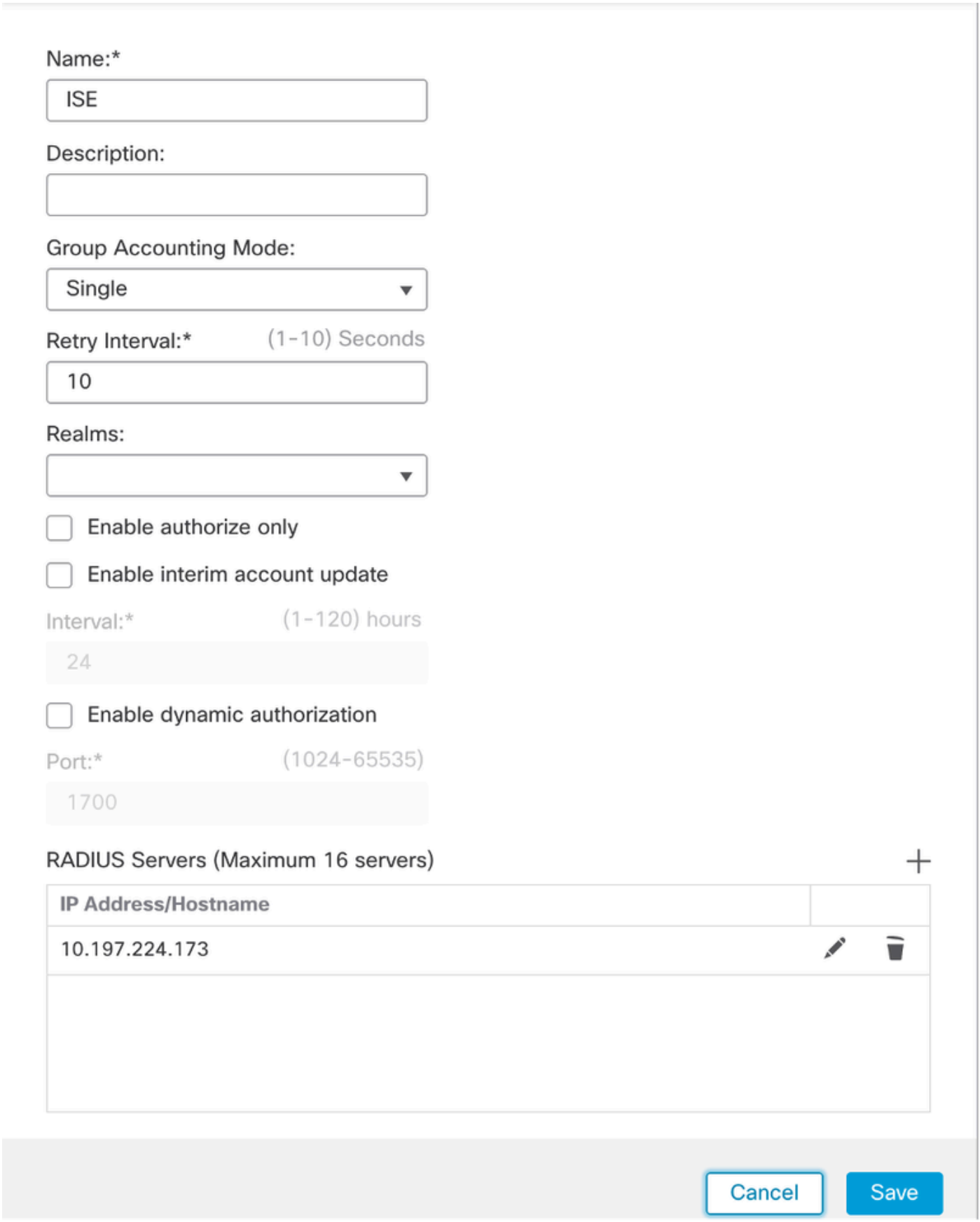
FMC:Trustpoint Enrollment Successful（トラストポイント登録成功）

2. RADIUSサーバの設定

2.1. FMCでのFTDの管理

1. Objects > Object Management > RADIUS Server Group > Add RADIUS Server Groupに移動します。

2. 名前を入力しISE、「+」をクリックしてRADIUSサーバーを追加します。

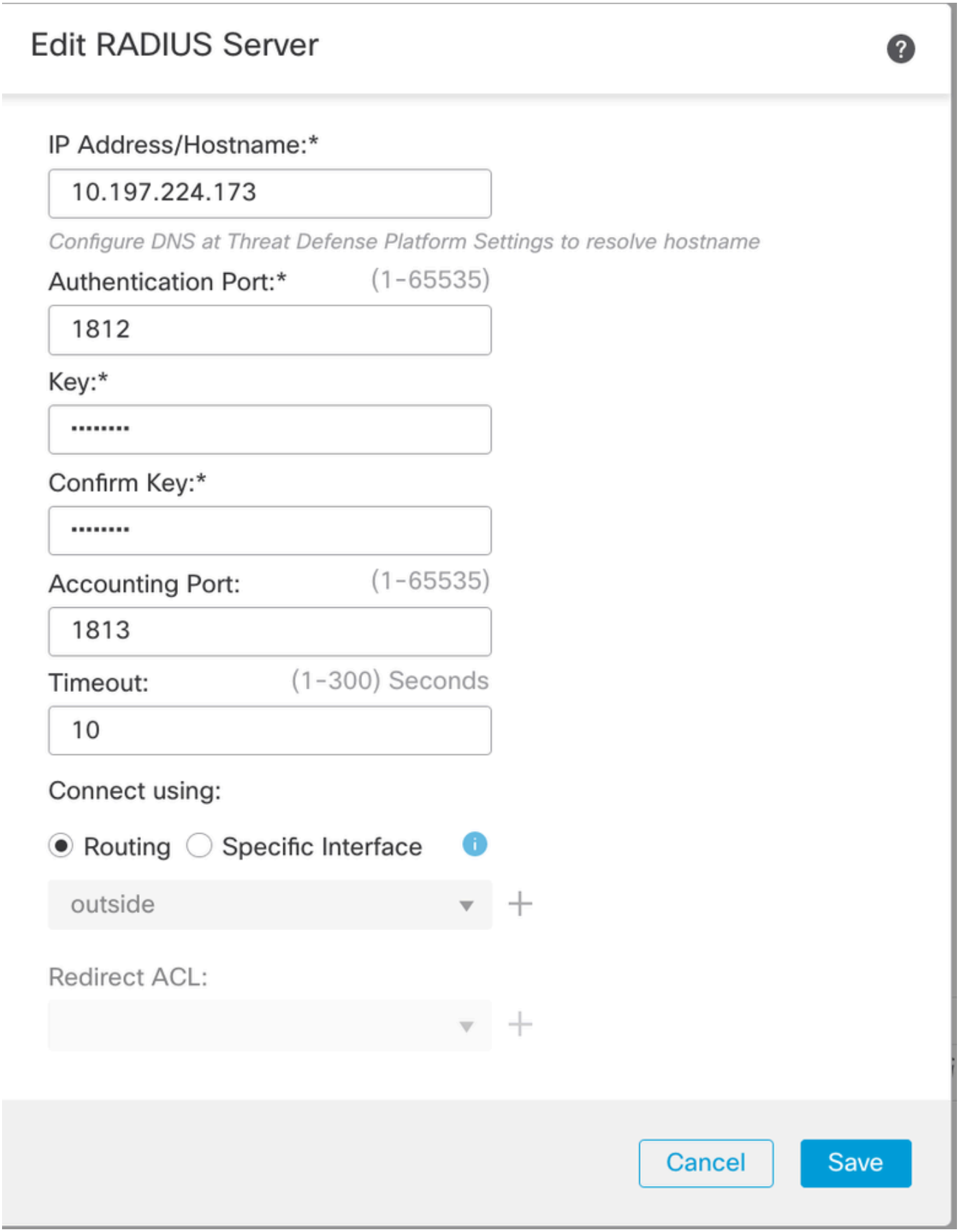


*FMC:Radius*サーバの設定

3. ISE RadiusサーバのIPアドレスを、ISEサーバと同じ共有秘密（キー）とともに指定します。

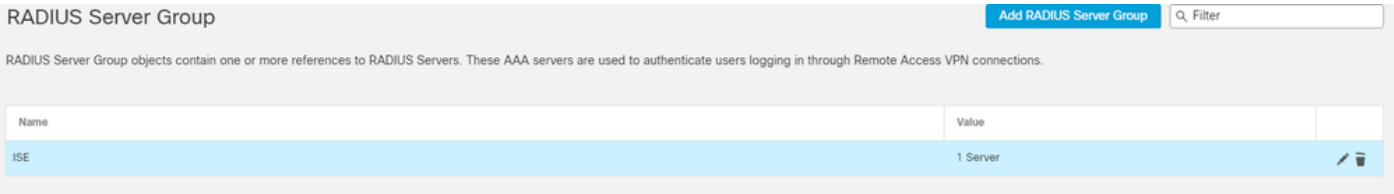
4. FTDがISEサーバと通信するために使用するRouting またはSpecific Interfaceのいずれかを選択します。

5.図に示すよSave うにクリックします。



FMC:ISEサーバ

6. 保存されたサーバは、図に示すようにRADIUS Server Group の下に追加されます。



FMC:RADIUS Server Group（RADIUSサーバグループ）

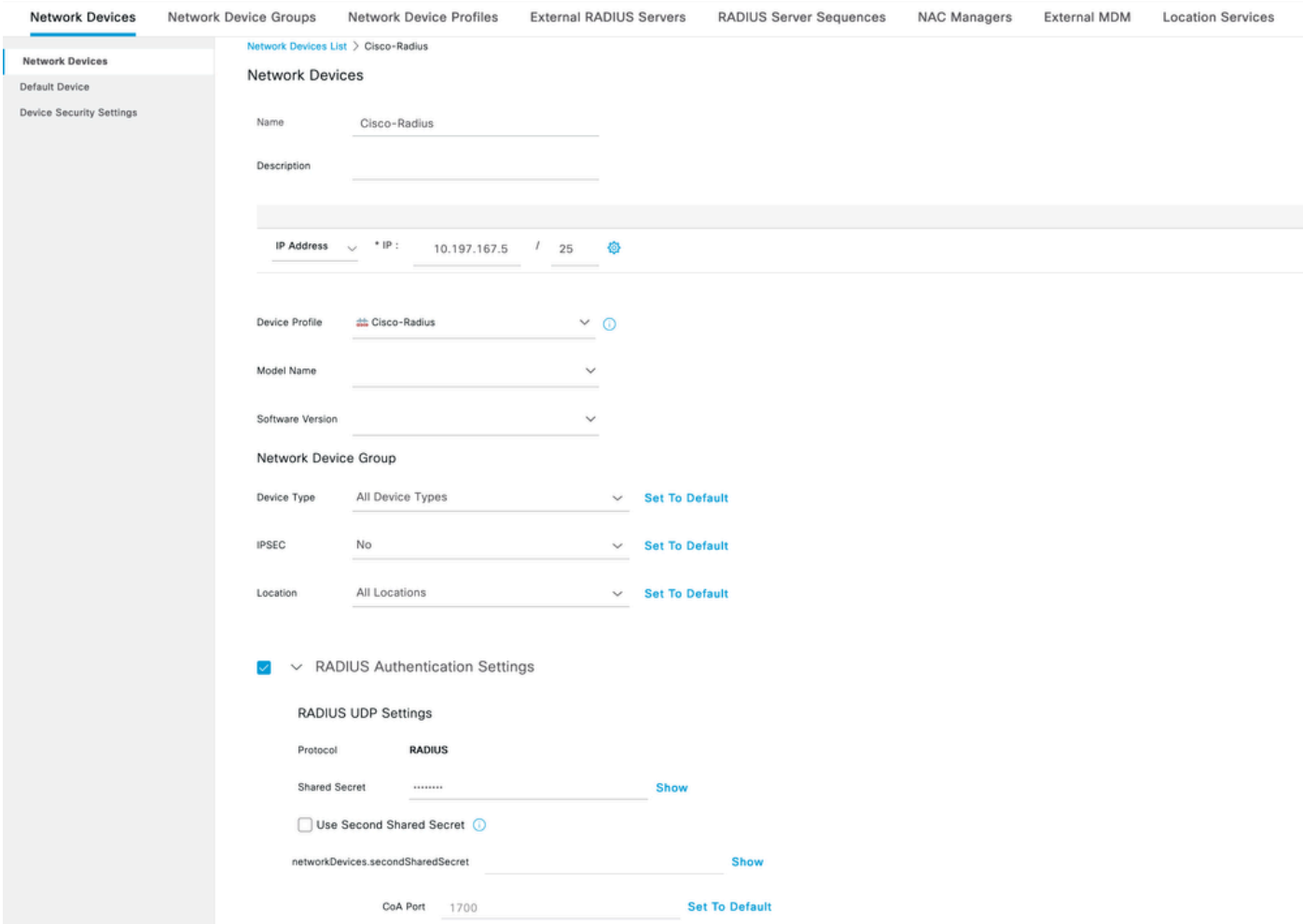
2.2. ISEでのFTDの管理

1. Network Devices に移動し、Addをクリックします。

2. サーバの「Cisco-Radius」名と、FTD通信インターフェイスであるRADIUSクライアントIP Addressの「Cisco-Radius」名を入力します。

3. Radius Authentication Settingsで、Shared Secretを追加します。

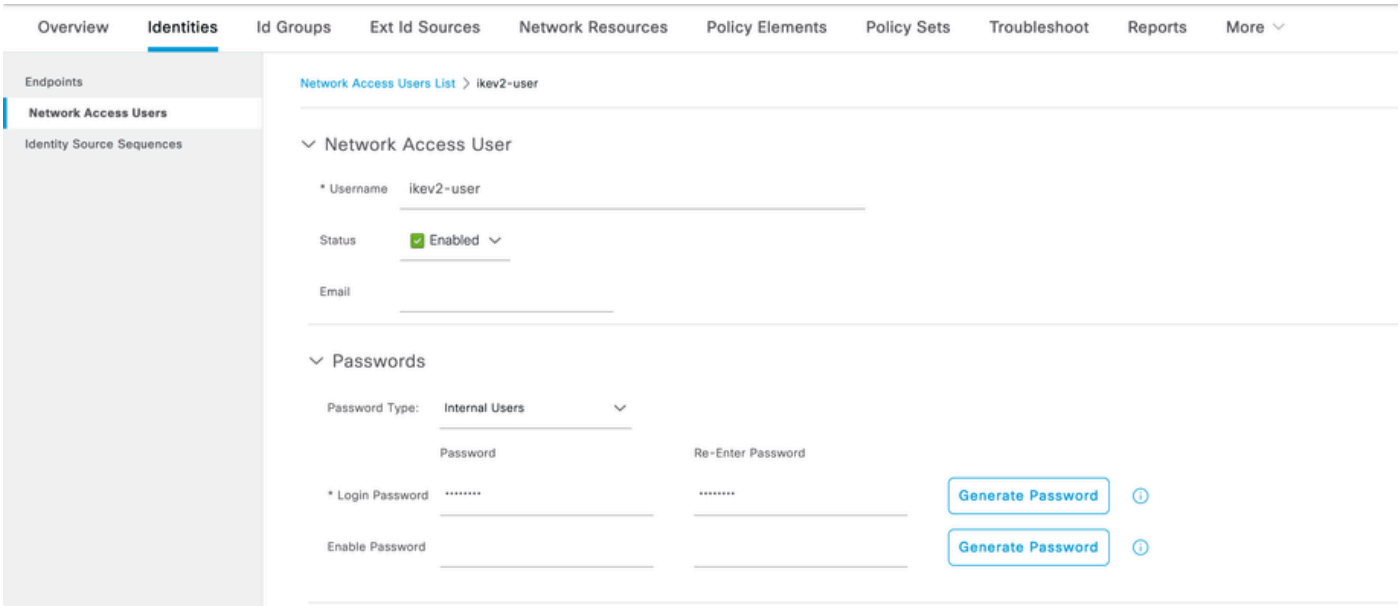
4. 「Save」をクリックします。



ISE:Network Devices（ネットワークデバイス）

5. ユーザを作成するには、Network Access > Identities > Network Access Usersに移動して、をクリックし Addます。

6. 必要に応じて、UsernameandLoginパスワードを作成します。



ISE – ユーザ

7. 基本ポリシーを設定するために、Policy > Policy Sets > Default > Authentication Policy > Defaultに移動し、All_User_ID_Storesを選択します。

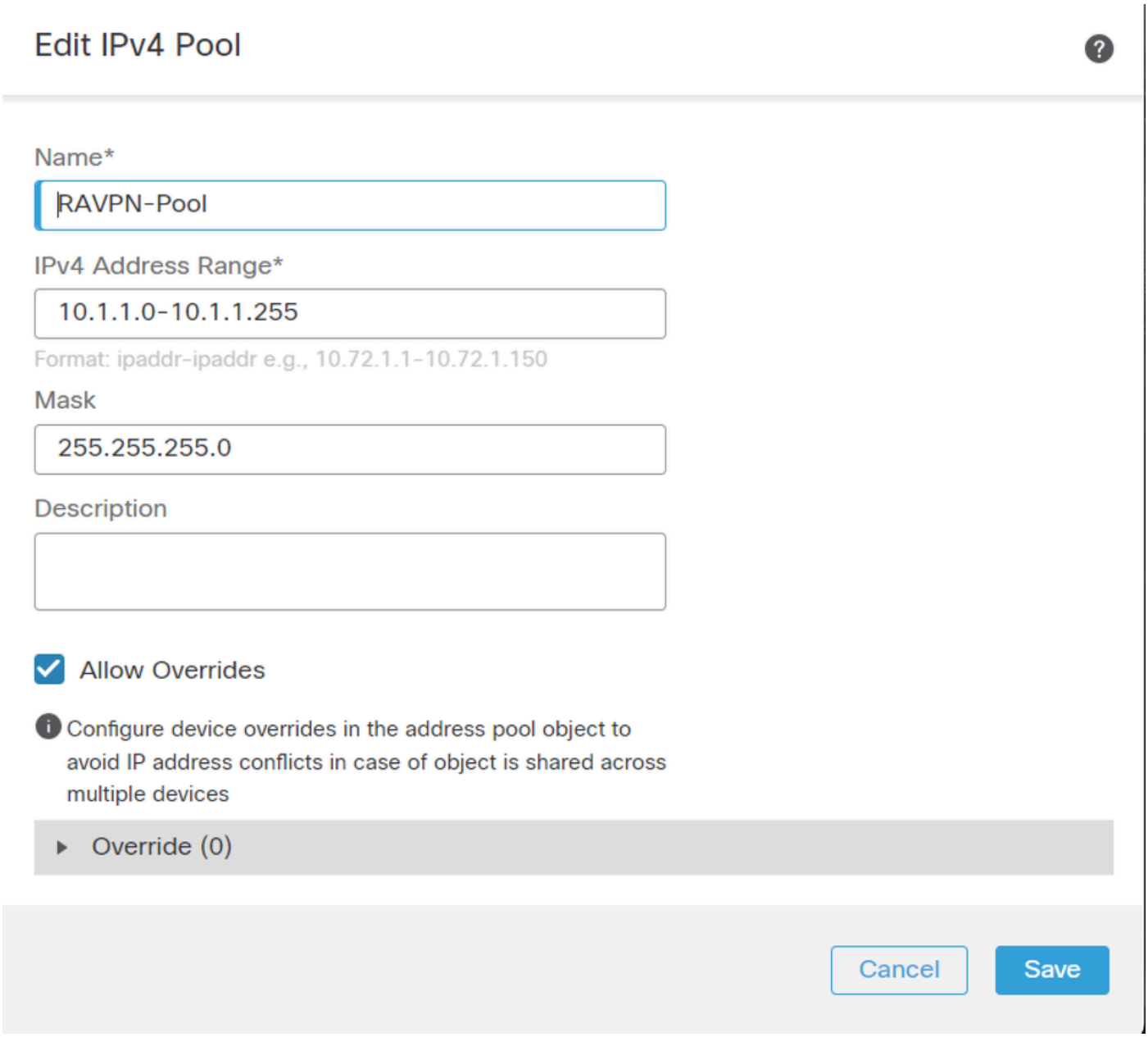
8.図に示すように、Policy > Policy Sets > Default > Authorization Policy > Basic_Authenticated_Access, に移動しPermitAccessて選択します。

ISE:Authentication Policy（認証ポリシー）

ISE:Authorization Policy（認可ポリシー）

3. FMC上のVPNユーザ用のアドレスプールの作成

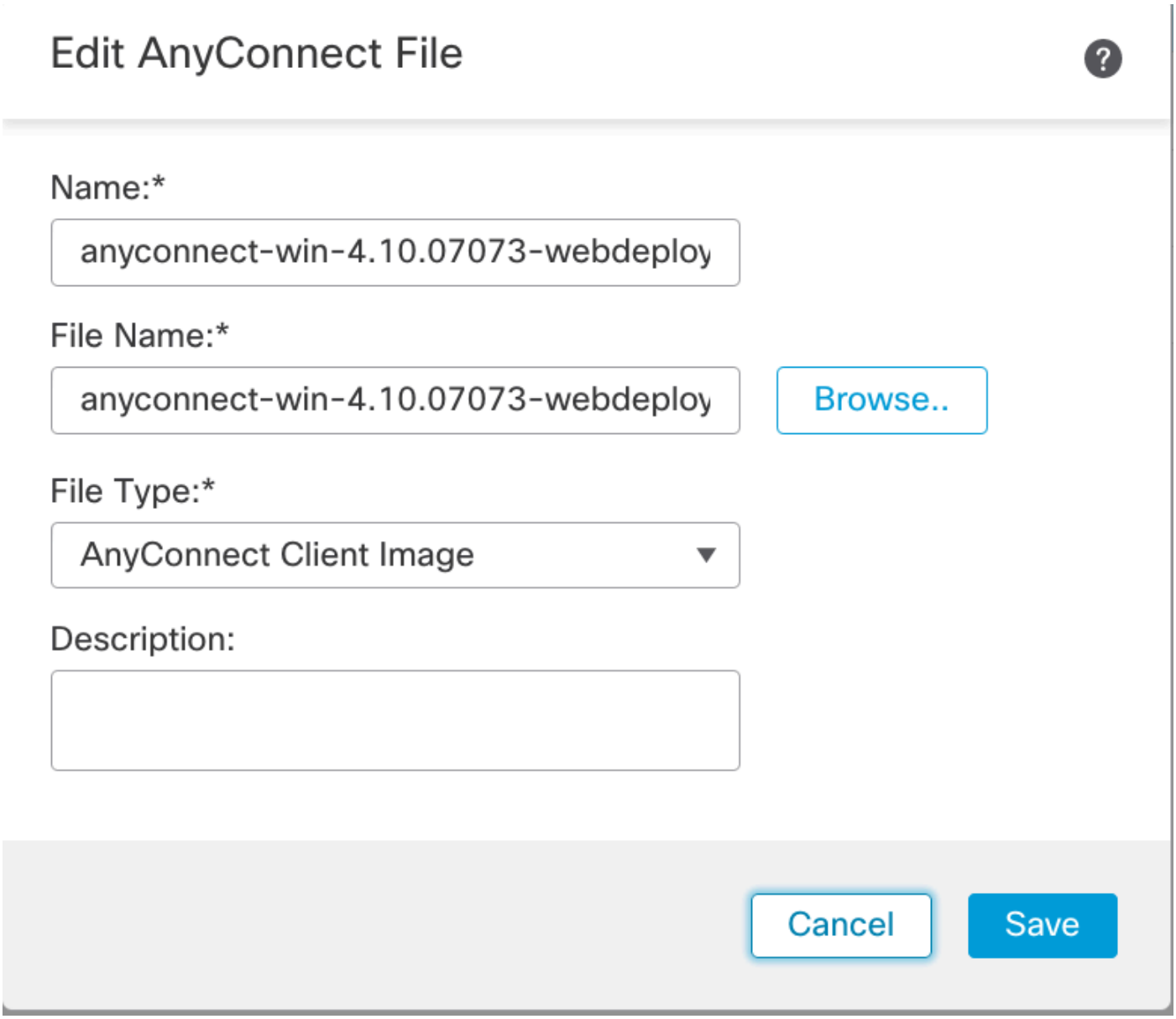
1. Objects > Object Management > Address Pools > Add IPv4 Poolsに移動します。
2. 名前RAVPN-Poolとアドレス範囲を入力します。マスクはオプションです。
3. **Save**をクリックします。



FMC:Address Pool（アドレスプール）

4. AnyConnectイメージのアップロード

1. Objects > Object Management > VPN > AnyConnect File > Add AnyConnect Fileに移動します。
2. 名前を入力しanyconnect-win-4.10.07073-webdeployをクリックして、ディスクBrowse から**Anyconnect**ファイルを選択し、図に示すようにクリックSave します。



*FMC:Anyconnect*クライアントイメージ

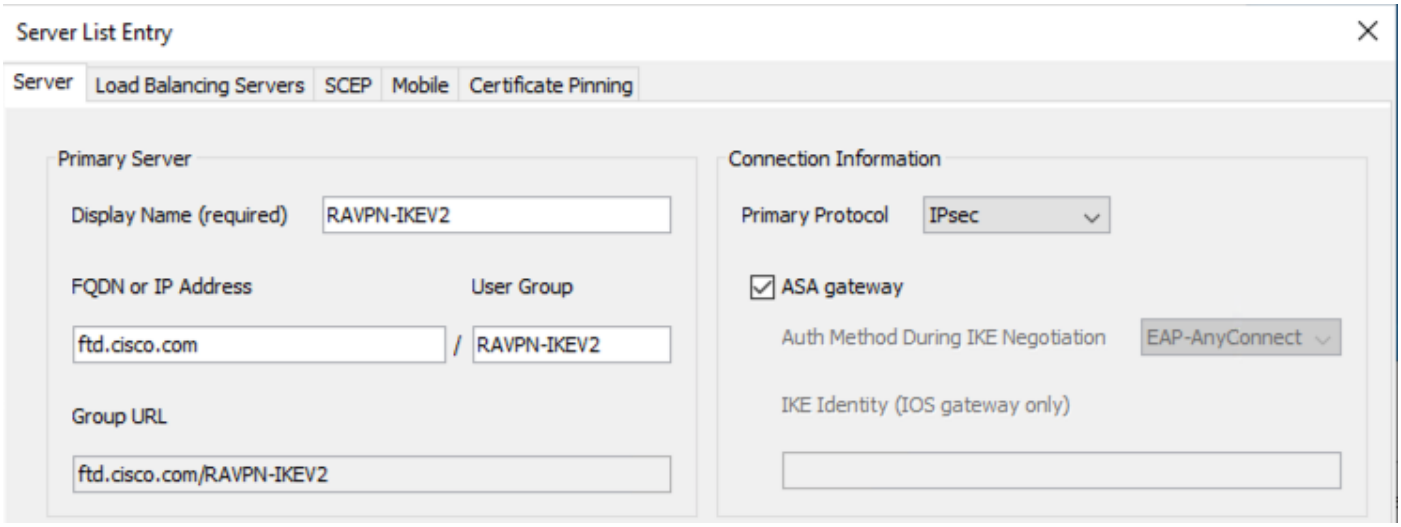
5. XMLプロファイルの作成

5.1.プロファイルエディタ

1. プロファイルエディタをsoftware.cisco.comからダウンロードして開きます。
2. **Server List** > **Add**...に移動します。

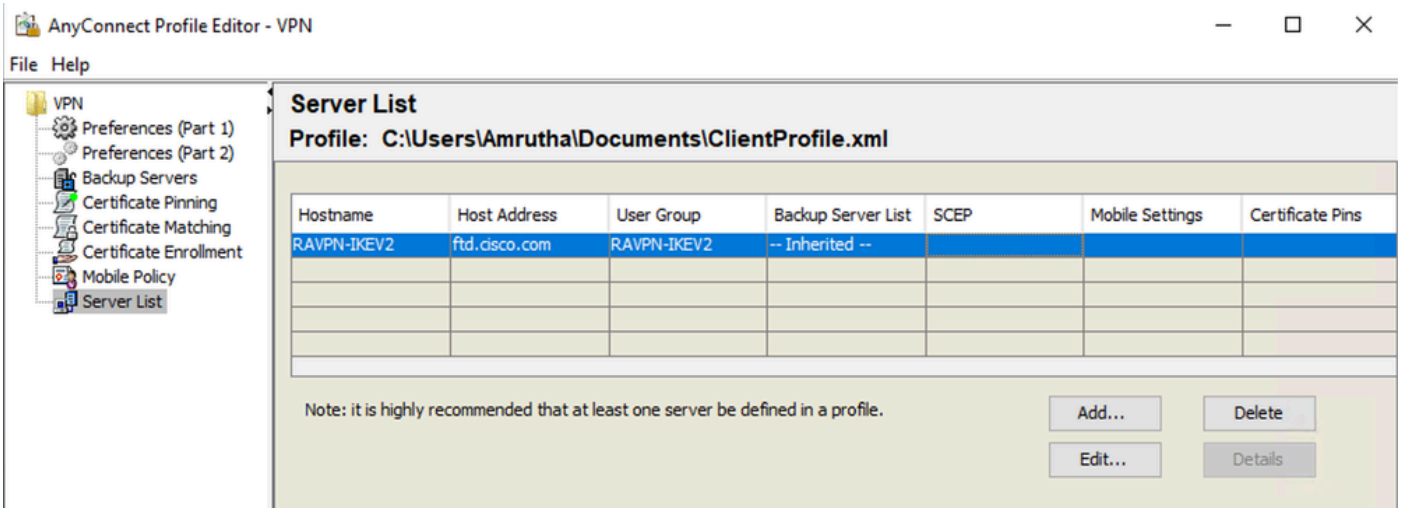
3. 表示名RAVPN-IKEV2FQDN および**ユーザー・グループ**（別名）を入力します。

4.図に示すように、プライマリ・プロトコル IPsec , asclick**Ok** を選択します。



プロファイルエディタ – サーバーリスト

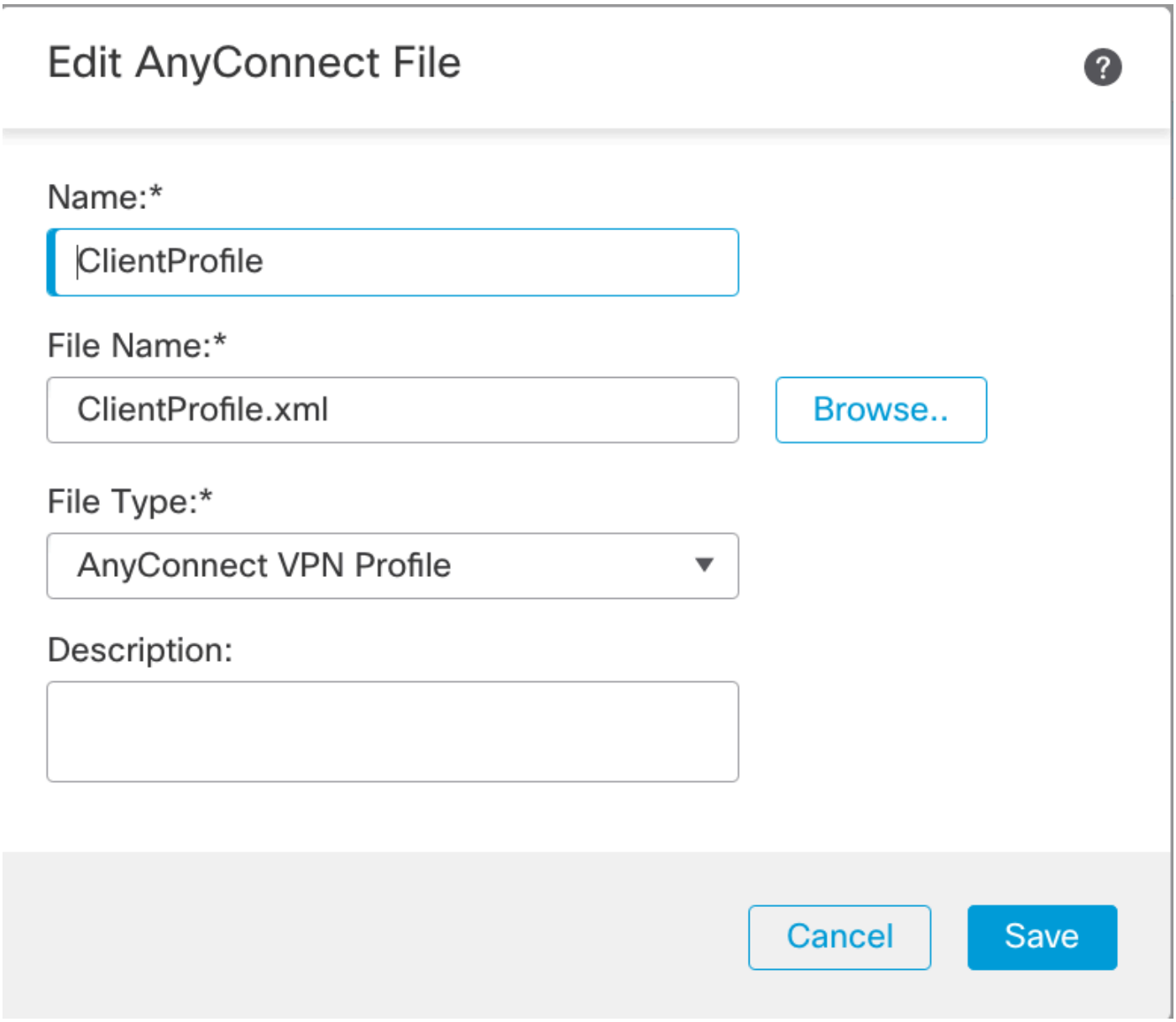
5. サーバー・リストが追加されます。ClientProfile.xmlとして保存します。



プロファイルエディタ – *ClientProfile.xml*

5.2. **FMC上**

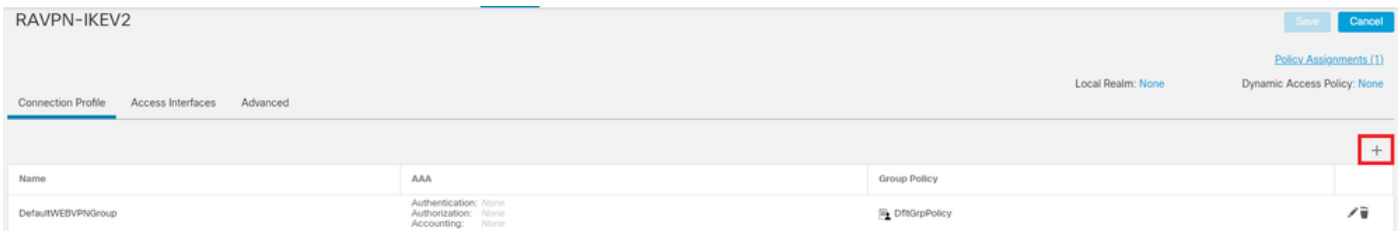
1. Objects > Object Management > VPN > AnyConnect File > Add AnyConnect Fileに移動します。
2. 名前を入力ClientProfileし、をクリックBrowse して、ディスクからファイルを選択ClientProfile.xmlします。
3. 「**Save** 」をクリックします。



FMC:Anyconnect VPNプロファイル

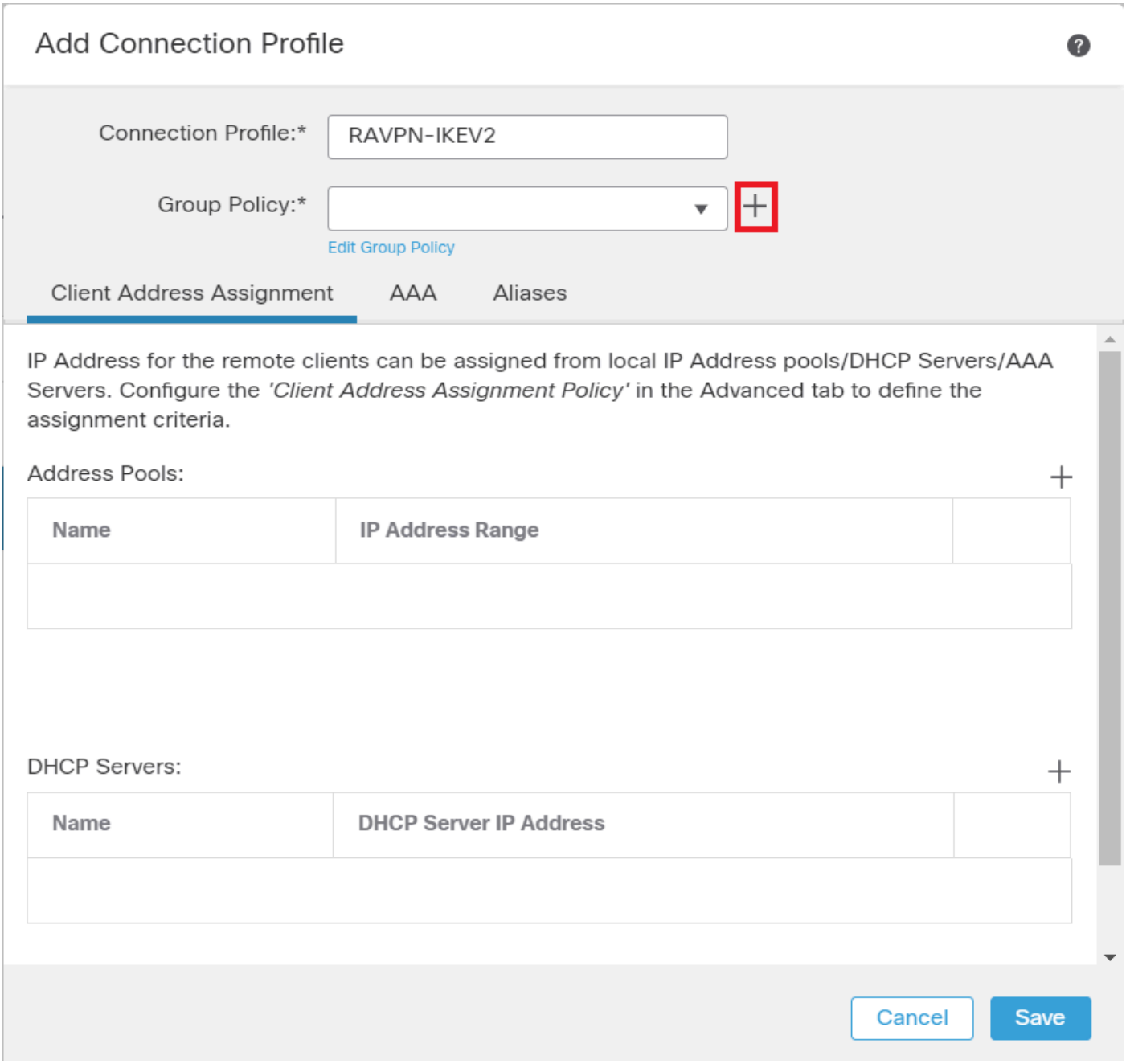
6. リモートアクセスの設定

1.図に示すように、接続プロファイルを追加するために、Devices > VPN > Remote Accessに移動し、+をクリックします。



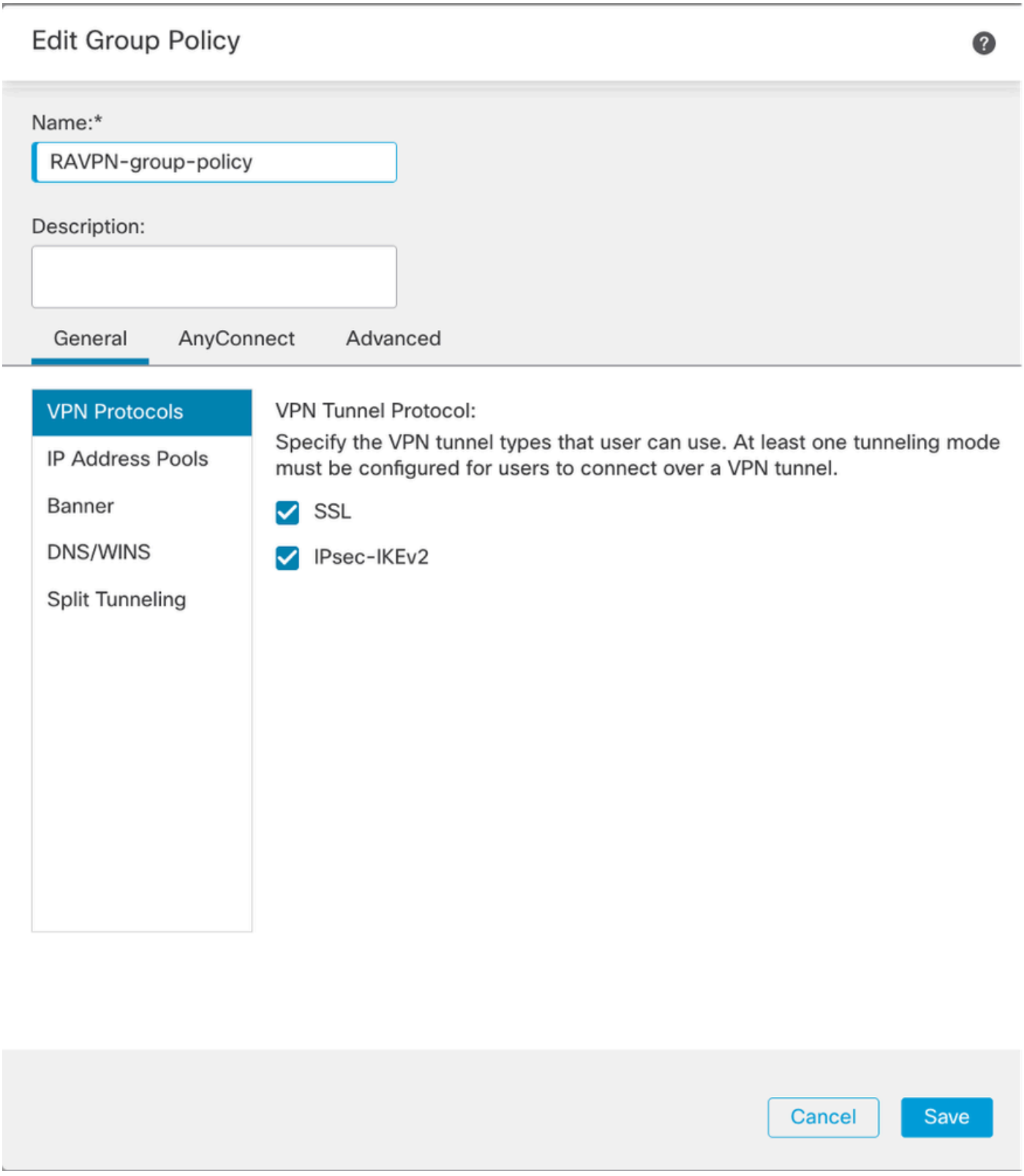
FMC:Remote Access Connection Profile（リモートアクセス接続プロファイル）

2. 接続プロファイル名を入力RAVPN-IKEV2し、図に示すように+**Group Policy**をクリックしてグループポリシーを作成します。



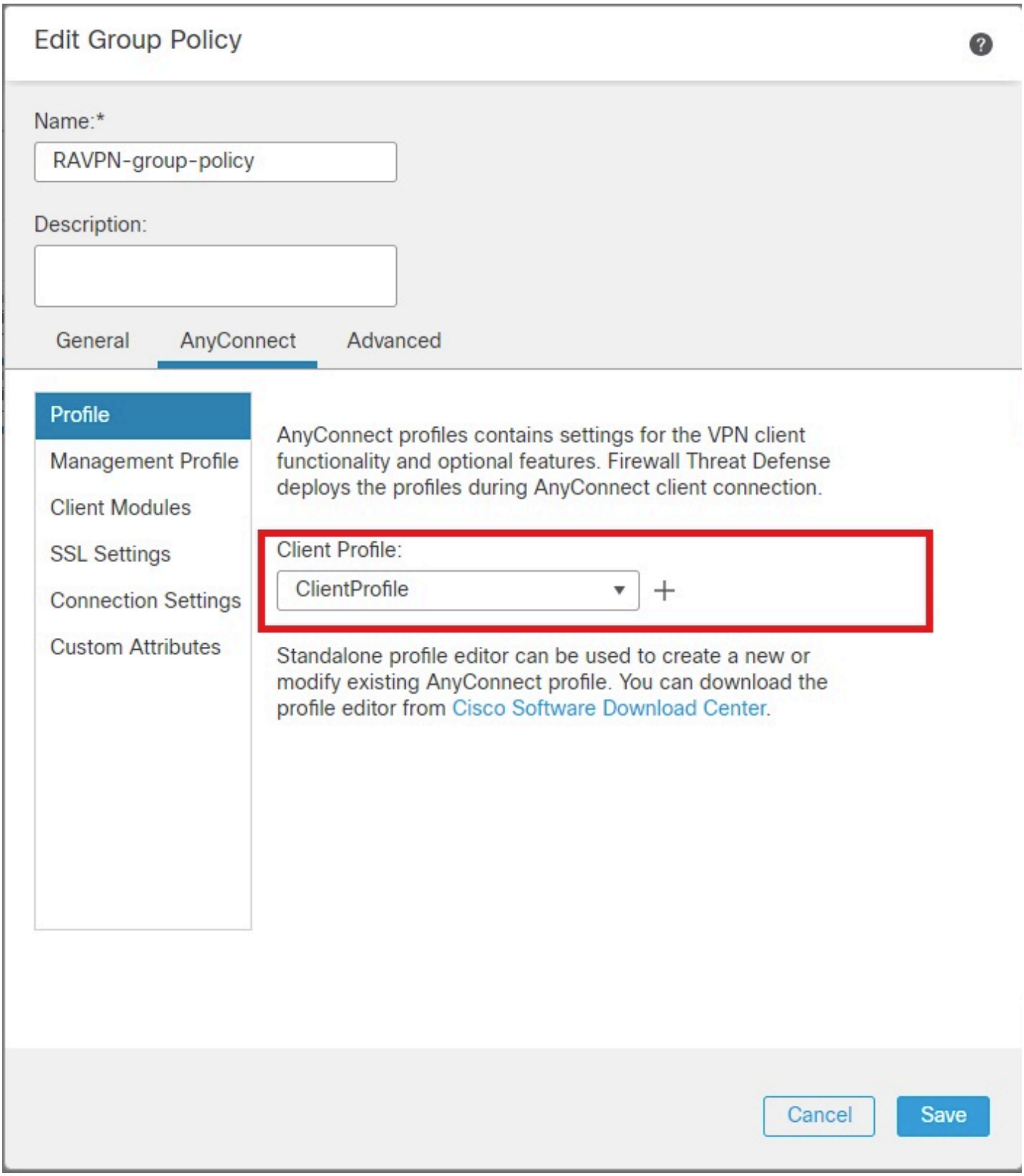
FMC:Group Policy（グループポリシー）

3. 名前を入力しRAVPN-group-policy、図に示すようにVPNプロトコル **SSL and IPsec-IKEv2** を選択します。



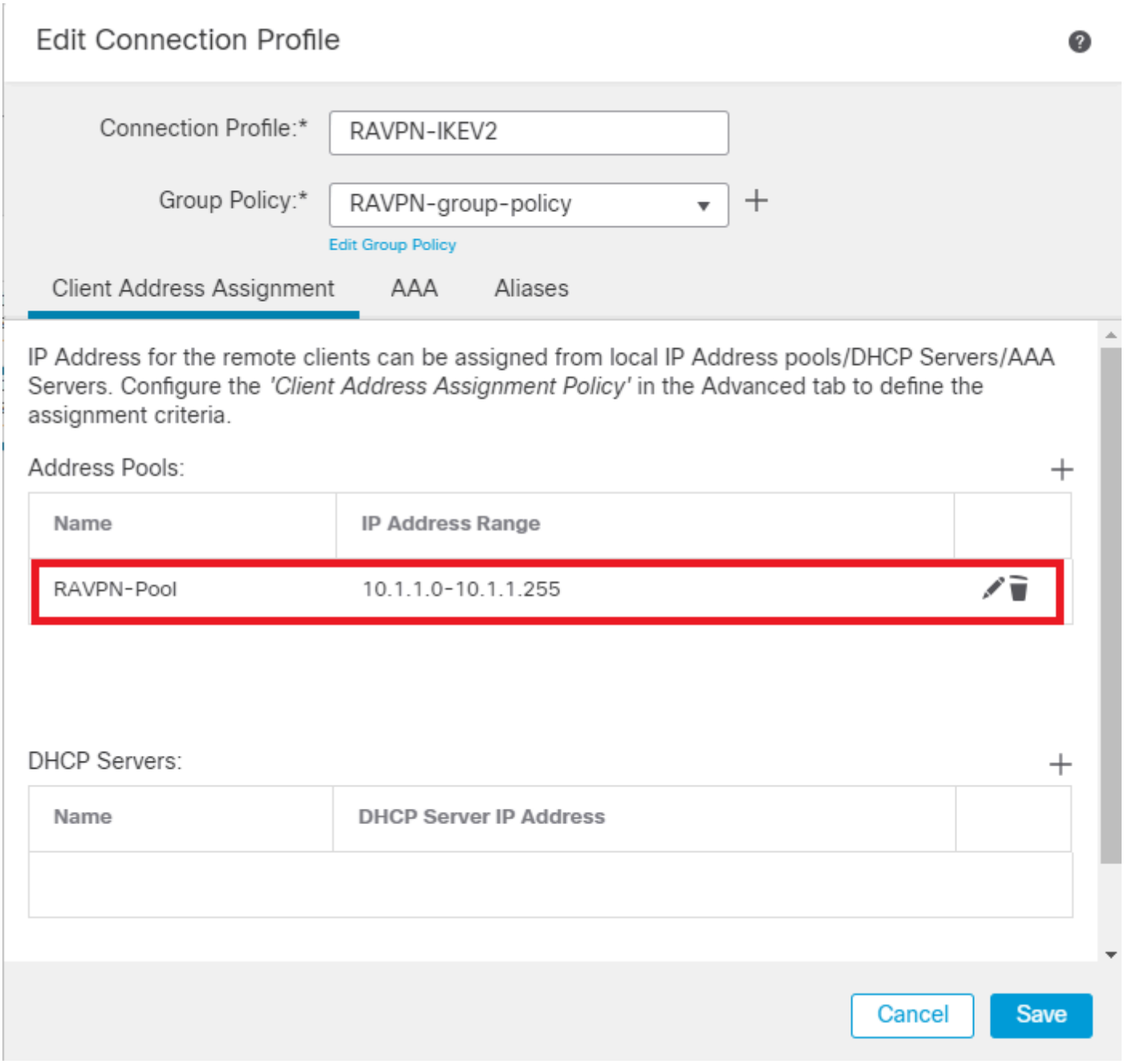
FMC:VPNプロトコル

4.AnyConnect > Profileの下で、ドロップダウンからXMLプロファイルClientProfileを選択し、図に示すよSaveうにクリックします。



FMC:Anyconnectプロファイル

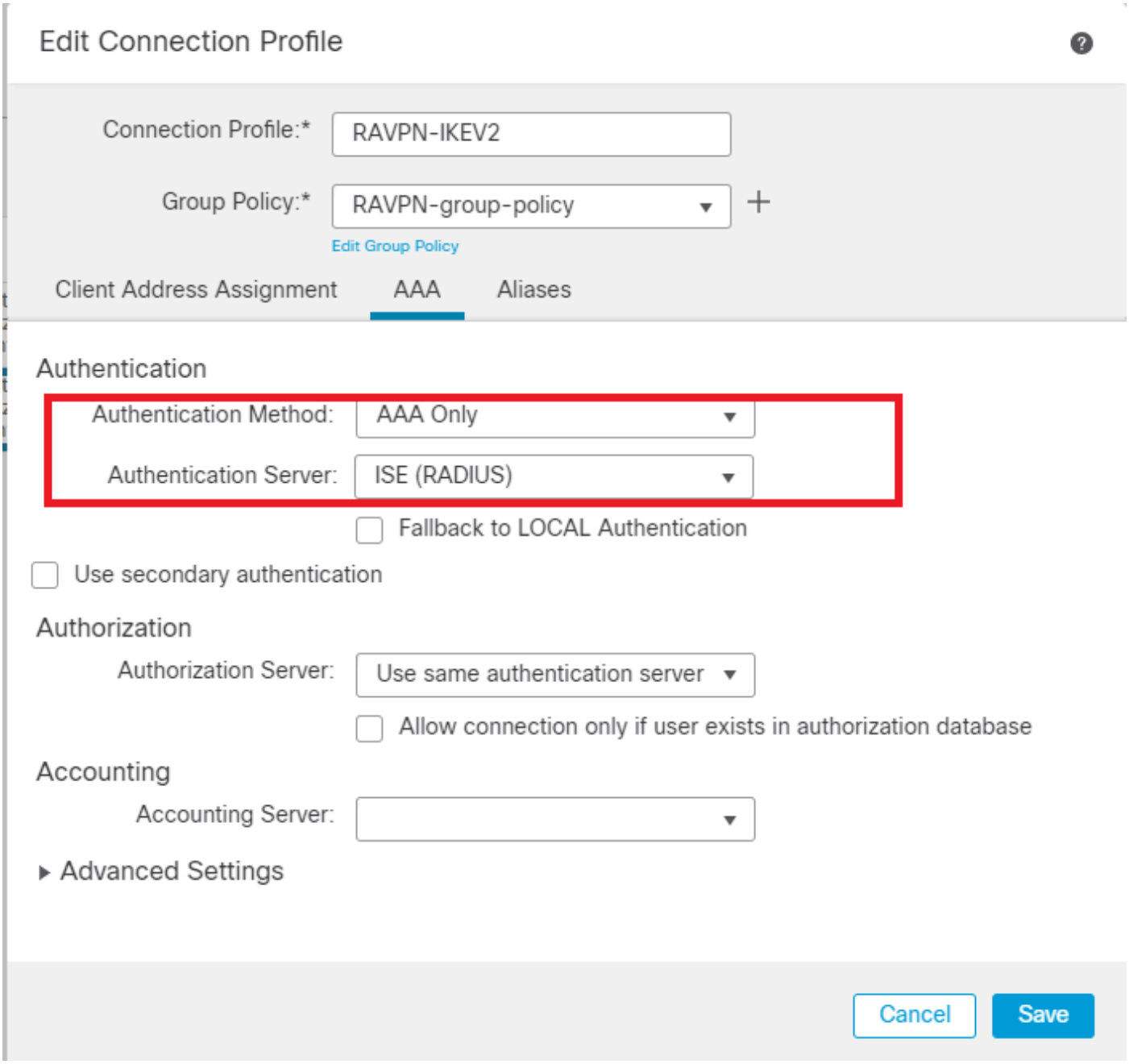
5. 「+ as shown in the image」をクリックしてアドレス・プールRAVPN-Poolを追加します。



FMC:Client Address Assignment（クライアントアドレス割り当て）

6. AAA > Authentication Methodに移動し、AAA Onlyを選択します。

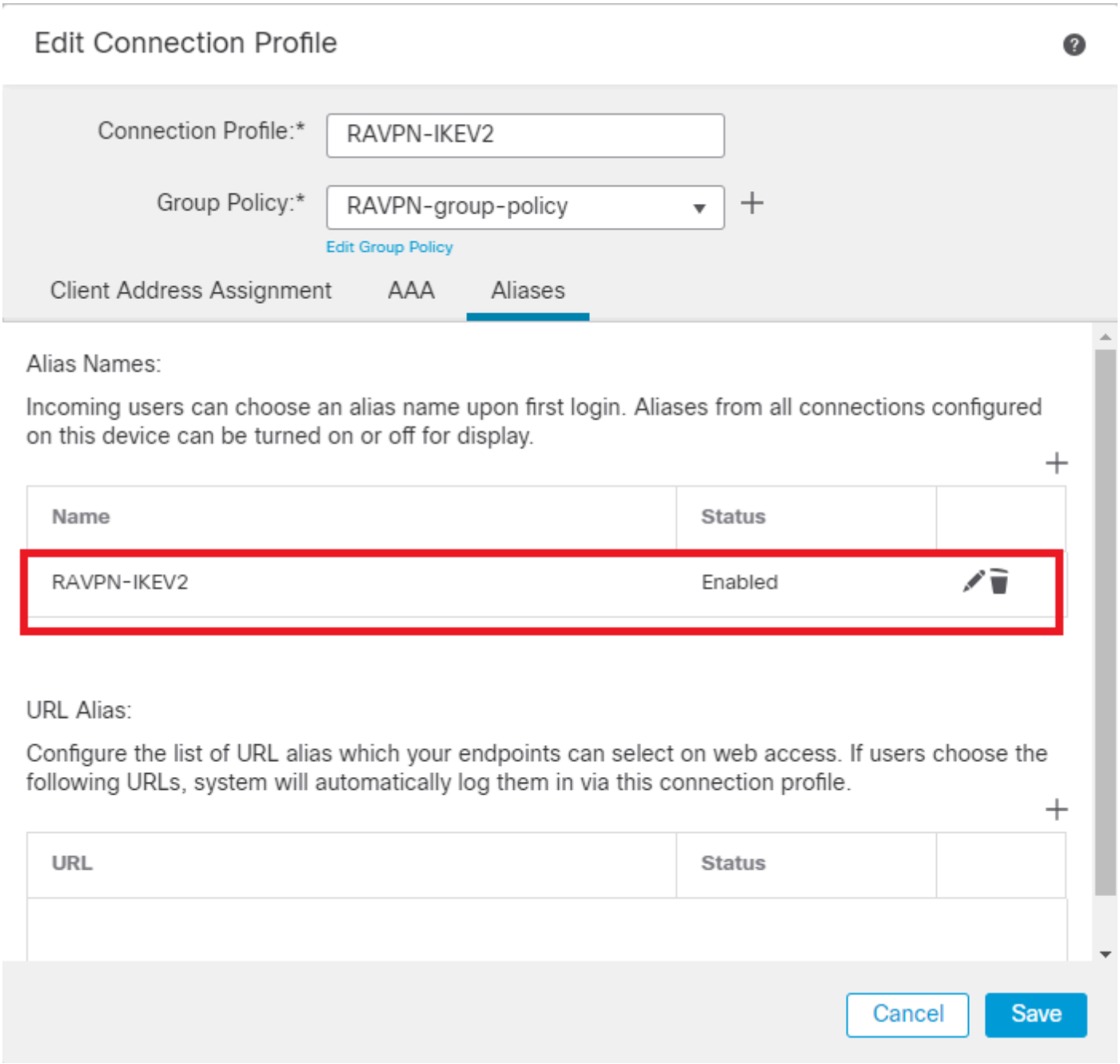
7. Authentication ServerISE (RADIUS) として選択します。



FMC:AAA認証

8. Aliases に移動し、エイリアス名を入力します。RAVPN-IKEV2は、ClientProfile.xmlでユーザグループとして使用されます。

9. Saveをクリックします。

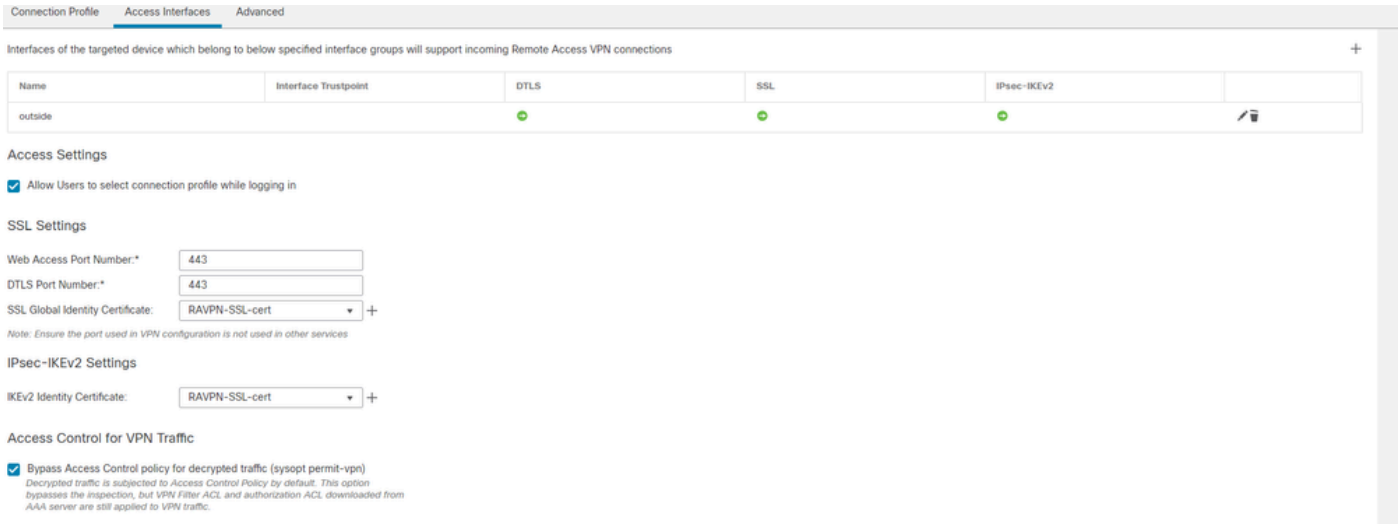


FMC：エイリアス

10. Access Interfacesに移動し、RAVPN IKEv2を有効にする必要があるインターフェイスを選択します。

11. SSLとIKEv2の両方のID証明書を選択します。

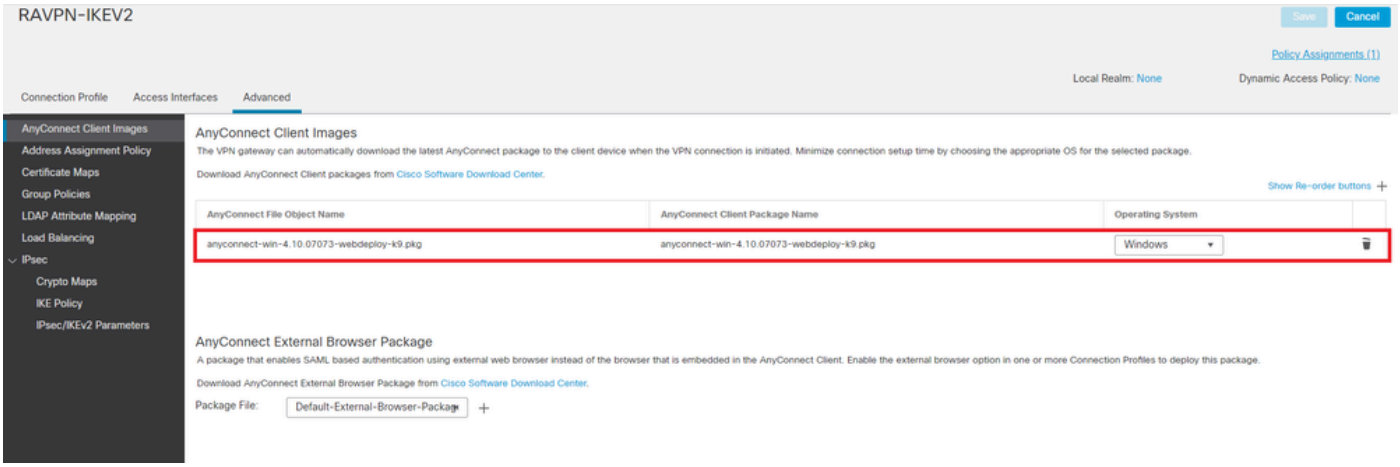
12. Saveをクリックします。



FMC：アクセスインターフェイス

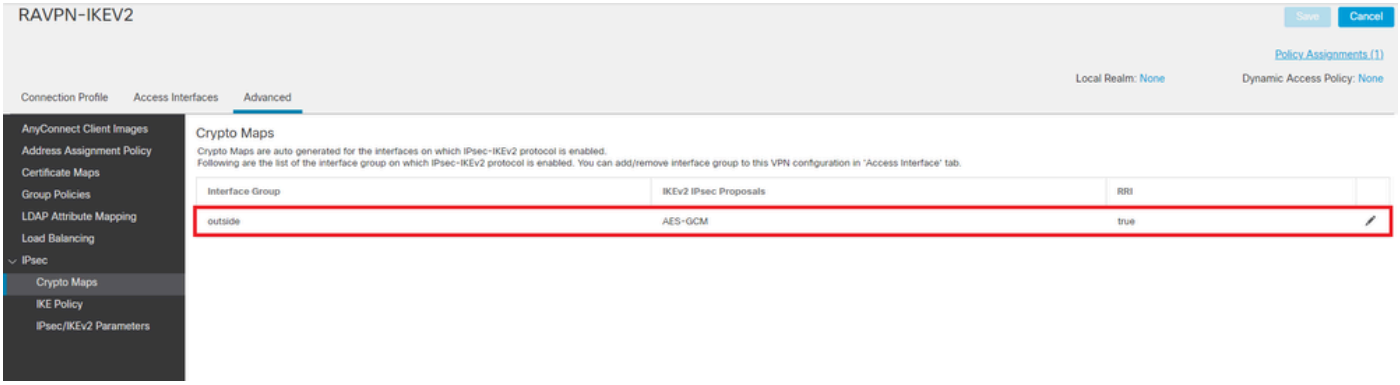
13. Advanced に移動します。

14. +をクリックして、Anyconnectクライアントイメージを追加します。



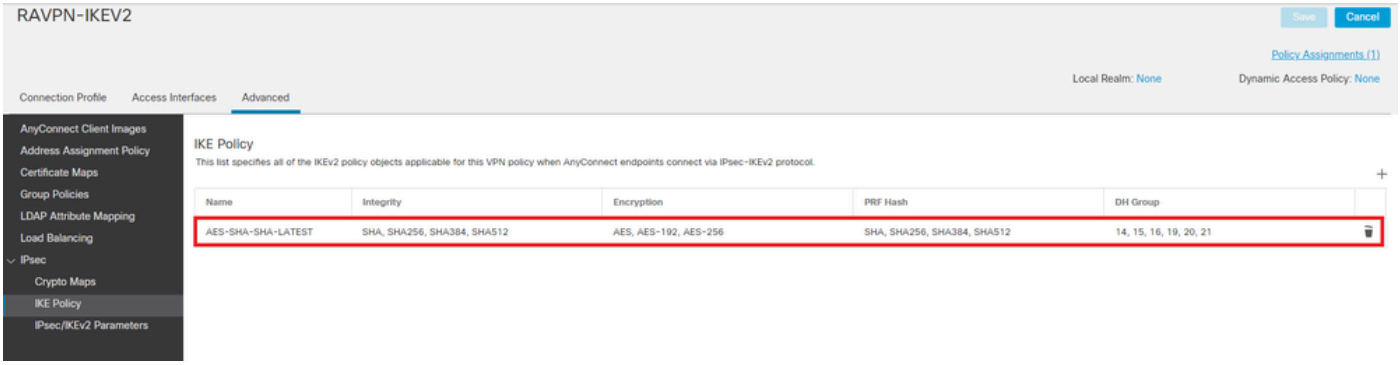
*FMC:Anyconnect*クライアントパッケージ

15. の下にIPsec、図に示すようにCrypto Maps、を追加します。



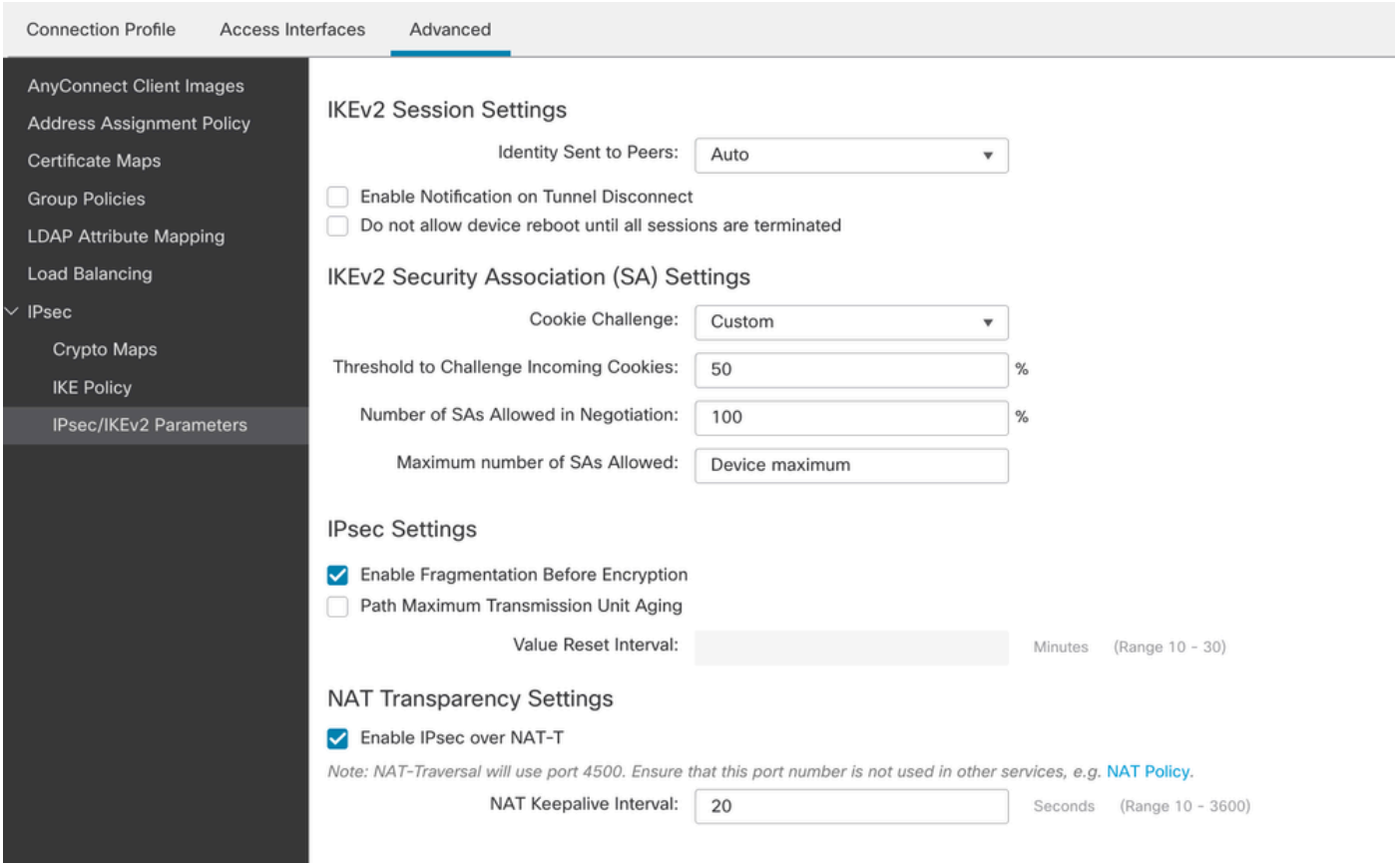
FMC：暗号マップ

16.「IPsec 」で、「+」をクリックしIKE Policy てを追加します。



FMC:IKEポリシー

17. IPsec で、IPsec/IKEv2 Parametersを追加します。



FMC:IPsec/IKEv2パラメータ

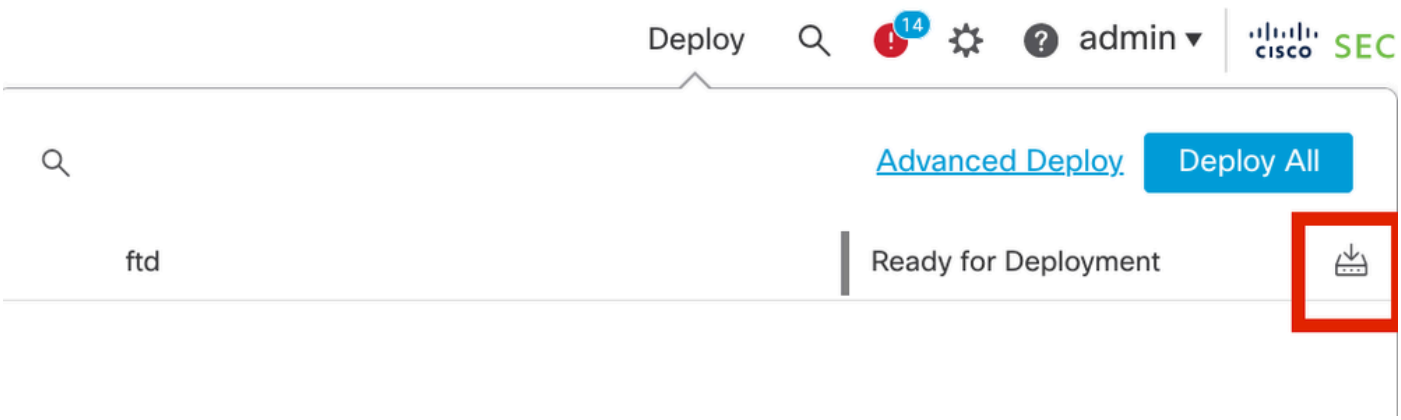
18. Connection Profileの下に、新しいプロファイルRAVPN-IKEV2が作成されます。

19.図に示すようにクSaveリックします。

FMC

：接続プロファイル*RAVPN-IKEV2*

20. 設定を展開します。



*FMC:FTD*の導入

7. Anyconnectプロファイルの設定

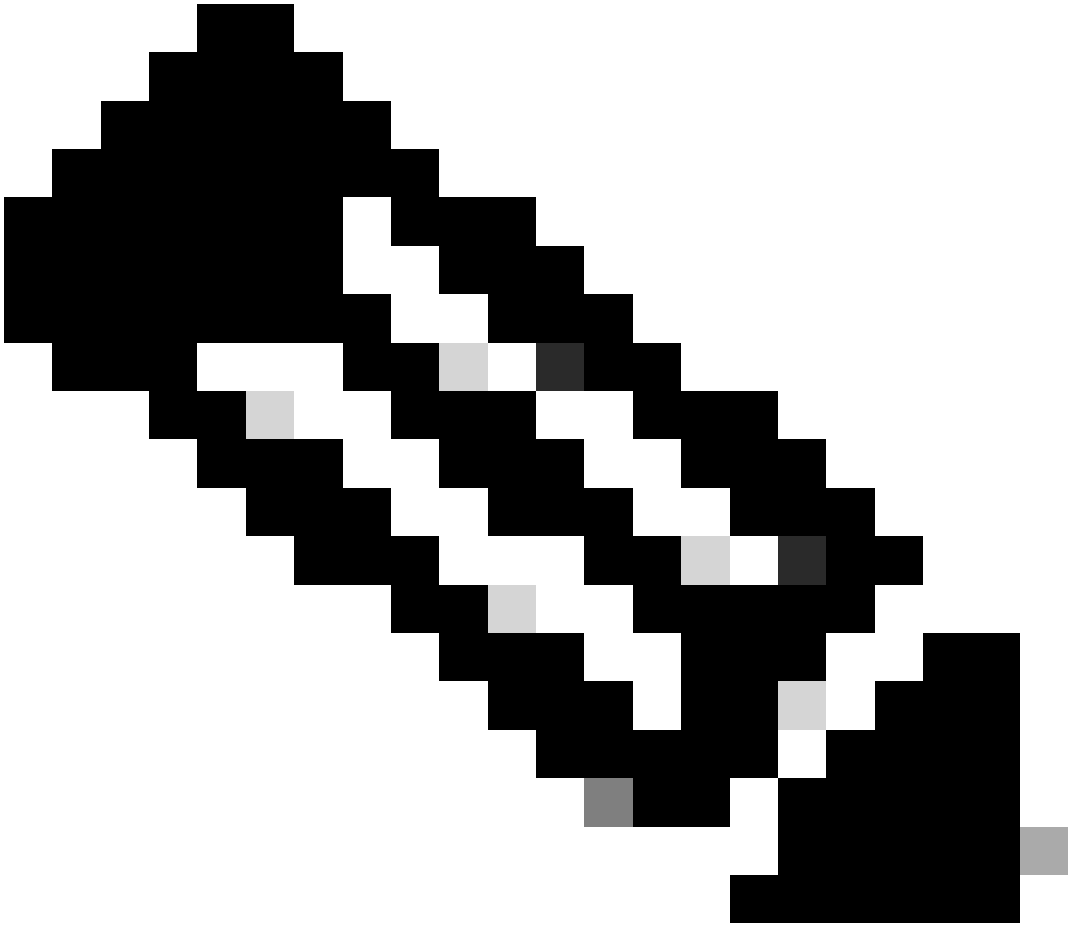
PC上のプロファイル（以下に保存） C:\ProgramData\Cisco\Cisco Anyconnect Secure Mobility Client\Profile .

<#root>

<?xml version="1.0" encoding="UTF-8"?> <AnyConnectProfile xmlns="http://schemas[dot]xmlsoap<dot>org/encoding/" xmlns:xsi="http://www[dot]w3

<HostName>RAVPN-IKEV2</HostName> <HostAddress>ftd.cisco.com</HostAddress> <UserGroup>RAVPN-IKEV2</UserG

</HostEntry> </ServerList> </AnyConnectProfile>



注：クライアントプロファイルがすべてのユーザのPCにダウンロードされたら、グループポリシーでトンネリングプロトコルとしてSSLクライアントをディセーブルにすることを推奨します。これにより、ユーザはIKEv2/IPsecトンネリングプロトコルを使用して排他的に接続できます。

確認

このセクションを使用して、設定が正しく動作していることを確認できます。

1. 最初の接続では、FQDN/IPを使用して、ユーザのPCからAnyConnect経由でSSL接続を確立します。
2. SSLプロトコルが無効で、前の手順を実行できない場合、クライアントプロファイルClientProfile.xmlがパスの下のPC上に存在することを確認します(PCがSSLプロトコルを使用していない場合は、SSLプロトコルを使用しますC:\ProgramData\Cisco\Cisco

Anyconnect Secure Mobility Client\Profile)。

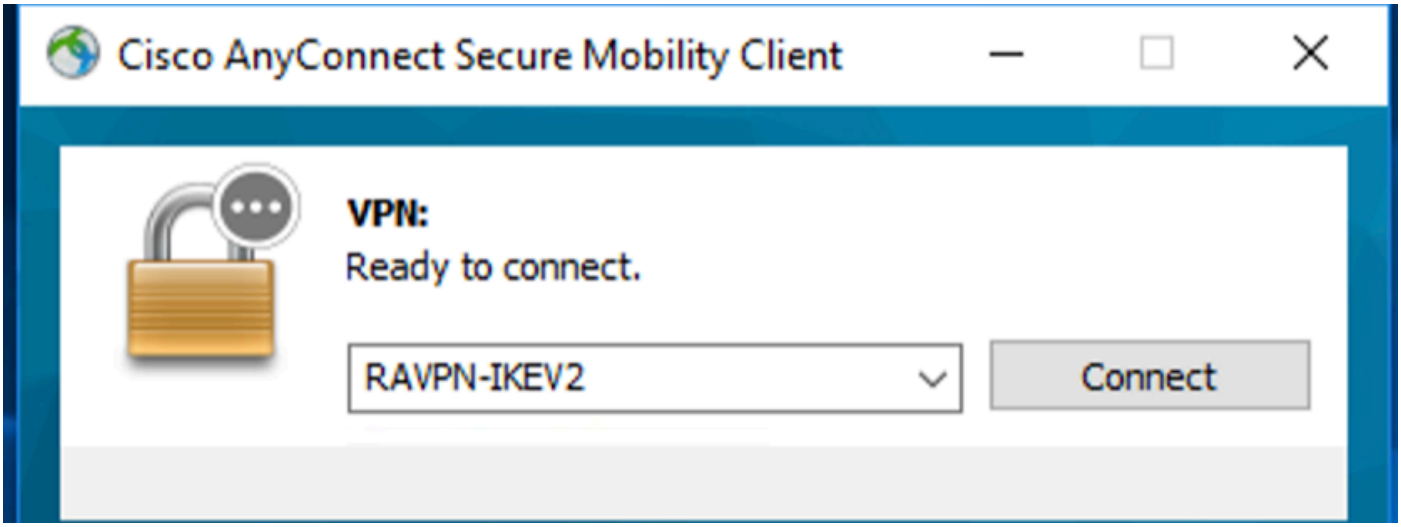
3. プロンプトが表示されたら、認証用のユーザ名とパスワードを入力します。

4. 認証に成功すると、クライアントプロファイルがユーザのPCにダウンロードされます。

5. Anyconnectを切断します。

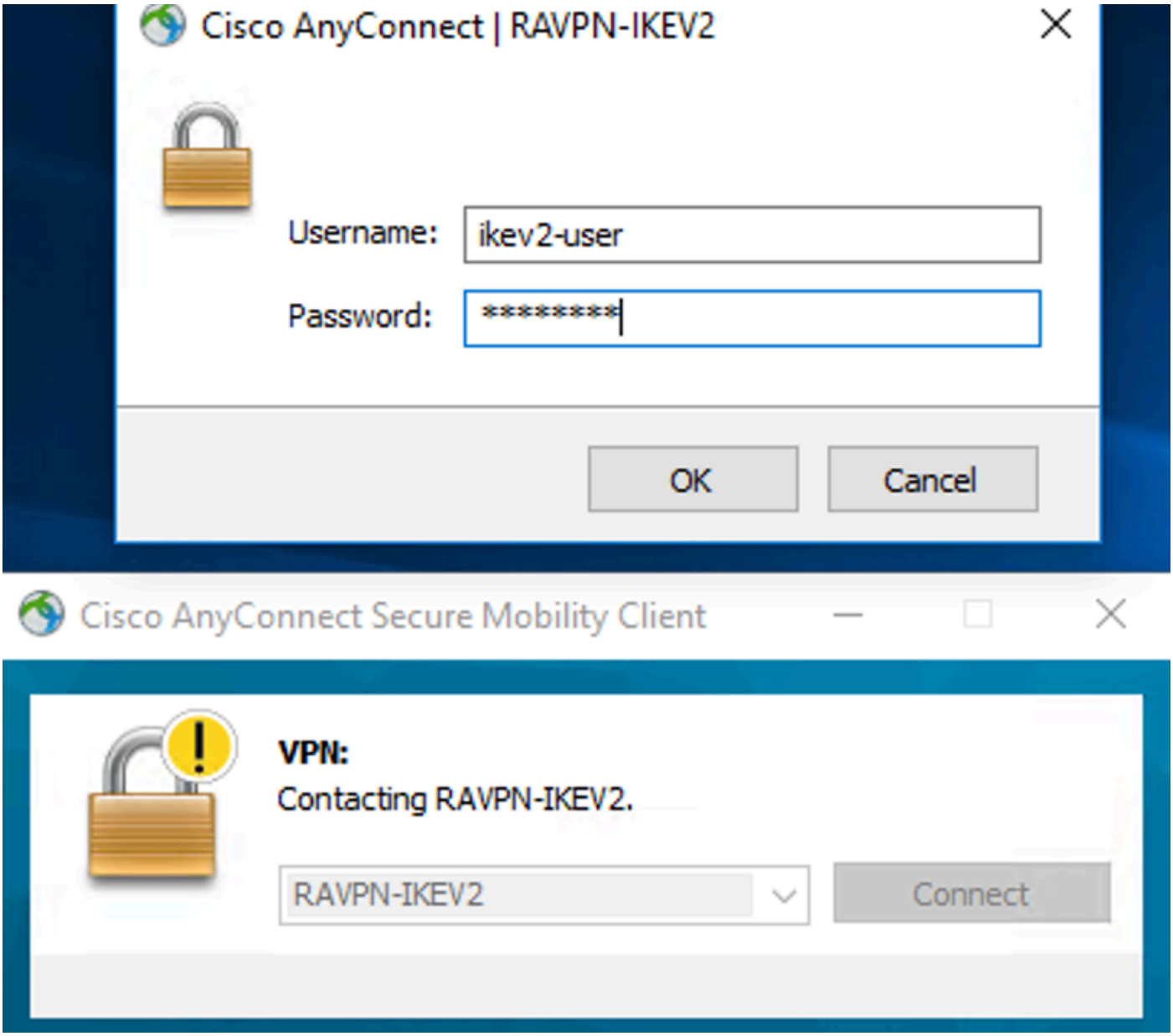
6. プロファイルをダウンロードしたら、IKEv2/IPsecを使用してAnyconnectに接続するために、クライアントプロファイル**RAVPN-IKEV2** に示されているホスト名をドロップダウンから選択します。

7. Connectをクリックします。



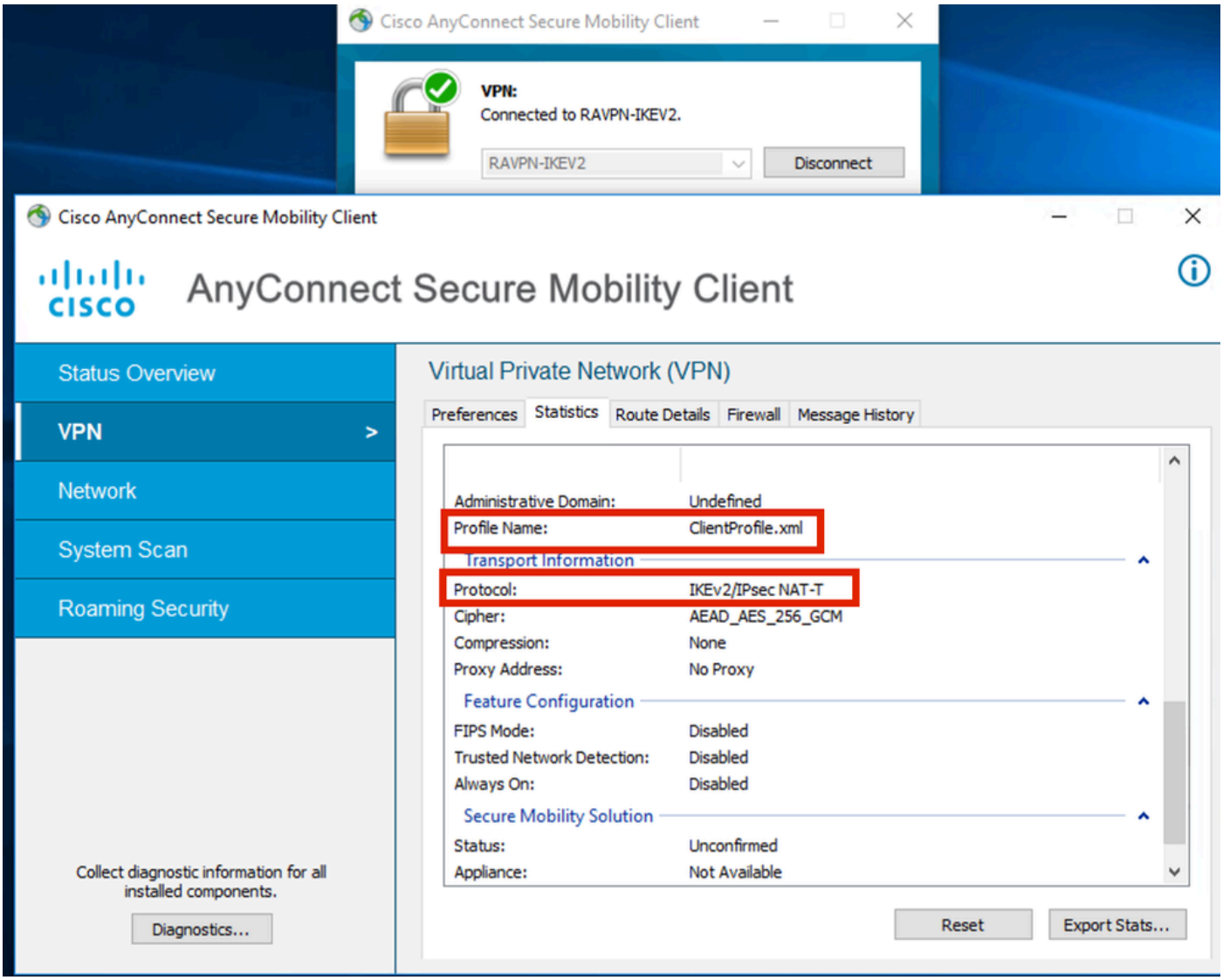
*Anyconnect*ドロップダウン

8. ISEサーバ上で作成された認証用のユーザ名とパスワードを入力します。



*Anyconnect*接続

9. 接続後に使用するプロファイルとプロトコル(IKEv2/IPsec)を確認します。



*Anyconnect*接続

FTD CLI出力：

```
<#root>
```

```
firepower# show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect

Username : ikev2-user                   Index        : 9
Assigned IP  : 10.1.1.1                 Public IP    : 10.106.55.22
Protocol     : IKEv2 IPsecOverNatT AnyConnect-Parent
License      : AnyConnect Premium
Encryption   : IKEv2: (1)AES256 IPsecOverNatT: (1)AES-GCM-256 AnyConnect-Parent: (1)none
```

```
Hashing      : IKEv2: (1)SHA512 IPsecOverNatT: (1)none AnyConnect-Parent: (1)none
Bytes Tx     : 450                          Bytes Rx     : 656
Pkts Tx      : 6                            Pkts Rx      : 8
Pkts Tx Drop : 0                            Pkts Rx Drop : 0
Group Policy : RAVPN-group-policy           Tunnel Group : RAVPN-IKEV2
Login Time   : 07:14:08 UTC Thu Jan 4 2024
Duration     : 0h:00m:08s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                           VLAN         : none
Audt Sess ID : 0ac5e205000090006596618c
Security Grp : none                          Tunnel Zone  : 0

IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1

AnyConnect-Parent:
Tunnel ID    : 9.1
Public IP    : 10.106.55.22
Encryption.  : none.                         Hashing     : none

Auth Mode    : userPassword
Idle Time out: 30 Minutes                    Idle TO Left : 29 Minutes
Client OS    : win
Client OS Ver: 10.0.15063
Client Type  : AnyConnect
Client Ver   : 4.10.07073

IKEv2:
Tunnel ID : 9.2
UDP Src Port : 65220                          UDP Dst Port : 4500
Rem Auth Mode: userPassword
Loc Auth Mode: rsaCertificate
Encryption   : AES256                          Hashing      : SHA512
Rekey Int (T): 86400 Seconds                   Rekey Left(T): 86391 Seconds
PRF : SHA512                                   D/H Group    : 19
Filter Name  :
Client OS    : Windows Client                  Type         : AnyConnect

IPsecOverNatT:
Tunnel ID    : 9.3
Local Addr   : 0.0.0.0/0.0.0.0/0/0
Remote Addr  : 10.1.1.1/255.255.255.255/0/0
Encryption   : AES-GCM-256                     Hashing       : none
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds                   Rekey Left(T) : 28791 Seconds
Idle Time Out: 30 Minutes                      Idle TO Left  : 29 Minutes
Bytes Tx     : 450 Bytes                       Rx            : 656
Pkts Tx      : 6                               Pkts Rx       : 8
```

```
firepower# show crypto ikev2 sa
```

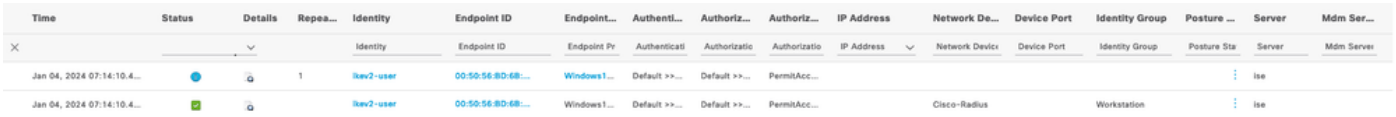
```
IKEv2 SAs:

Session-id:6, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                          Remote                                          fvrf/ivrf
16530741  10.197.167.5/4500              10.106.55.22/65220
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:19, Auth sign: RSA, Auth verify: EAP
Life/Active Time: 86400/17 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 10.1.1.1/0 - 10.1.1.1/65535
ESP spi in/out: 0x6f7efd61/0xded2cbc8
```

```
firepower# show crypto ipsec sa
```

```
interface: Outside
    Crypto map tag: CSM_Outside_map_dynamic, seq num: 30000, local addr: 10.197.167.5

      Protected vrf:
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.1.1.1/255.255.255.255/0/0)
      current_peer: 10.106.55.22, username: ikev2-user
      dynamic allocated peer ip: 10.1.1.1
      dynamic allocated peer ip(ipv6): 0.0.0.0

      #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 6
      #pkts decaps: 8, #pkts decrypt: 8, #pkts verify: 8
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.197.167.5/4500, remote crypto endpt.: 10.106.55.22/65220
      path mtu 1468, ipsec overhead 62(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: DED2CBC8
      current inbound spi : 6F7EFD61

  inbound esp sas:
     spi: 0x6F7EFD61 (1870593377)
     SA State: active
     transform: esp-aes-gcm-256 esp-null-hmac no compression
     in use settings ={RA, Tunnel, NAT-T-Encaps, IKEv2, }
     slot: 0, conn_id: 9, crypto-map: CSM_Outside_map_dynamic
     sa timing: remaining key lifetime (sec): 28723
     IV size: 8 bytes
     replay detection support: Y
     Anti replay bitmap:
```

```
     0x00000000 0x000001FF

  outbound esp sas:
    spi: 0xDED2CBC8 (3738356680)
    SA State: active
    transform: esp-aes-gcm-256 esp-null-hmac no compression
    in use settings ={RA, Tunnel, NAT-T-Encaps, IKEv2, }
    slot: 0, conn_id: 9, crypto-map: CSM_Outside_map_dynamic
    sa timing: remaining key lifetime (sec): 28723
    IV size: 8 bytes
    replay detection support: Y
    Anti replay bitmap:
    0x00000000 0x00000001
```

ISEログ：



ISE：ライブログ

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

```
debug radius all
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
```

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。