ASAおよびFTDからMS AzureへのポリシーおよびルートベースのVPN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

バックグラウンド情報

- コンセプト
  - VPN暗号化ドメイン

設定

- ASAでのIKEv1の設定
- ASAコード9.8(1)以降のVTIを使用したIKEv2ルートベース
- FTDでのIKEv1の設定
- ポリシーベースのトラフィックセレクタを使用したIKEv2ルートベース

確認

- フェーズ 1
- フェーズ 2

トラブルシュート

- IKEv1
- IKEv2

はじめに

このドキュメントでは、Cisco ASAとCisco Secure FirewallおよびMicrosoft Azureクラウドサービス間のVPNの概念と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。

- ASAでVTIを使用するIKEv2ルートベースVPNの場合：ASAコードバージョン9.8(1)以降

（Azureはルートベースvpn用に設定する必要があります）
- ASAおよびFTDで暗号マップを使用するIKEv1ポリシーベースVPNの場合：ASAコードバージョン8.2以降およびFTD 6.2.0以降（ポリシーベースVPN用にAzureを設定する必要があります）。
- ポリシーベースのトラフィックセレクタを使用してASA上でクリプトマップを使用するIKEv2ルートベースVPNの場合：クリプトマップで設定されたASAコードバージョン8.2以降（Azureは、UsePolicyBasedTrafficSelectorsを使用してルートベースVPN用に設定する必要があります）。
- FTDの管理と設定に関するFMCの知識。

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。

- シスコFTD
- シスコFMC
- Microsoft Azure
- ASA 9.18.4.22を実行するCisco ASAv

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、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。

バックグラウンド情報

コンセプト

VPN暗号化ドメイン

IPSecのIPアドレス範囲により、VPNトンネルに参加できます。 暗号化ドメインは、ローカルトラフィックおよびリモートトラフィックセレクタを使用して定義され、IPSecによってキャプチャおよび暗号化されるローカルおよびリモートサブネット範囲を指定します。

VPN暗号化ドメインを定義する方法には、ルートベースとポリシーベースの2つのトラフィックセレクタがあります。

ルートベース：
暗号化ドメインは、IPSecトンネルに入るすべてのトラフィックを許可するように設定されます。IPSecローカルおよびリモートトラフィックセレクタは0.0.0.0に設定されます。つまり、IPSecトンネルにルーティングされるトラフィックは、送信元/宛先サブネットに関係なく暗号化されます。

Cisco適応型セキュリティアプライアンス(ASA)では、バージョン9.8以降で仮想トンネルインターフェイス(VTI)を使用したルートベースのVPNがサポートされています。

Firepower Management Center(FMC)で管理されるCisco Secure FirewallまたはFirepower Threat Defense(FTD)は、バージョン6.7以降のVTIを使用したルートベースのVPNをサポートします。

ポリシーベース：

暗号化ドメインは、送信元と宛先の両方について、特定のIP範囲だけを暗号化するように設定されます。 ポリシーベースのローカルトラフィックセレクタとリモートトラフィックセレクタは、IPSec経由で暗号化するトラフィックを特定します。

ASAは、バージョン8.2以降でクリプトマップを使用するポリシーベースVPNをサポートしています。

Microsoft Azureは、シミュレートされたポリシーベースのトラフィックセレクタを使用して、ルートベース、ポリシーベース、またはルートベースをサポートします。Azureは現在、VPNで選択された方法に基づいて構成できるインターネットキーエクスチェンジ(IKE)のバージョンを制限しています。 ルートベースにはIKEv2が必要で、ポリシーベースにはIKEv1が必要です。 IKEv2を使用する場合は、Azureのルートベースを選択する必要があり、ASAはVTIを使用する必要があります。

コードバージョンが原因でASAが暗号マップのみをサポートする場合は、ポリシーベースのトラフィックセレクタを使用してルートベース用にAzureを設定する必要があります。これは、MicrosoftがUsePolicyBasedTrafficSelectorsを呼び出すオプションを実装するために、PowerShellスクリプトを使用してAzureポータルで行われます。このオプションについては、「VPNゲートウェイを複数のオンプレミスのポリシーベースVPNデバイスに接続する」を参照してください。

ASAとFTDの設定の観点からまとめるには、次の手順を実行します。

- VTIを使用して構成されたASAでは、AzureをルートベースのVPN用に構成する必要があり

ます。
- FTDの場合、VTIの設定方法の詳細については、『Firepower Management Centerコンフィギュレーションガイド、バージョン6.7』を参照してください。
- 暗号マップを使用して構成されたASA/FTDの場合、AzureはポリシーベースのVPNまたはUsePolicyBasedTrafficSelectorsを使用したルートベースのVPN用に構成する必要があります。

設定

設定手順を実行します。IKEv1、VTIを使用したIKEv2ルートベース、またはポリシーベースのトラフィックセレクタ（ASA上のクリプトマップ）を使用したIKEv2ルートベースのいずれかを設定します。

ASAでのIKEv1の設定

ASAからAzureへのサイト間IKEv1 VPNでは、次のASA設定を実装します。Azureポータルでポリシーベースのトンネルを構成していることを確認してください。この例では、ASAでクリプトマップを使用しています。

ASAでのIKEv1の詳細な設定情報については、『ASAvでASDMまたはCLIを使用してIKEv1のIPsecサイトツーサイトトンネルを設定する』を参照してください。

---

1. 外部インターフェイスでIKEv1を有効にします。

<#root>

```
Cisco-ASA(config)#

crypto ikev1 enable outside
```

---

2. ハッシュ、認証、Diffie-Hellmanグループ、有効期間、および暗号化に使用するアルゴリズムとメソッドを定義するIKEv1ポリシーを作成します。

注：リストされているフェーズ1のIKEv1属性は、『VPNデバイスと、サイト間VPNゲート

ウェイ接続用のIPsec/IKEパラメータ』からの属性です。詳細については、Microsoft Azureサポートにお問い合わせください。

<#root>

```
Cisco-ASA(config)#

crypto ikev1 policy 1



Cisco-ASA(config-ikev1-policy)#

authentication pre-share


Cisco-ASA(config-ikev1-policy)#

encryption aes


Cisco-ASA(config-ikev1-policy)#

hash sha


Cisco-ASA(config-ikev1-policy)#

group 14


Cisco-ASA(config-ikev1-policy)#

lifetime 28800
```

3. IPsec属性でトンネルグループを作成し、ピアIPアドレスとトンネル事前共有キーを設定します。

<#root>

```
Cisco-ASA(config)#

tunnel-group 192.168.1.1 type ipsec-l2l
```

```
Cisco-ASA(config)#

tunnel-group 192.168.1.1 ipsec-attributes


Cisco-ASA(config-tunnel-ipsec)#

ikev1 pre-shared-key cisco
```

---

4. 暗号化してトンネリングするトラフィックを定義するアクセスリストを作成します。

この例では、対象のトラフィックは10.2.2.0サブネットから10.1.1.0へのトンネルからのものです。 サイト間に複数のサブネットが関係する場合は、複数のエントリを含めることができます。

バージョン8.4以降では、ネットワーク、サブネット、ホストIPアドレス、または複数のオブジェクトのコンテナとして機能するオブジェクトまたはオブジェクトグループを作成できます。ローカルサブネットとリモートサブネットを持つ2つのオブジェクトを作成し、それらを暗号アクセスコントロールリスト(ACL)文とネットワークアドレス変換(NAT)文の両方に使用します。

```
<#root>
Cisco-ASA(config)#

object network 10.2.2.0_24


Cisco-ASA(config-network-object)#

subnet 10.2.2.0 255.255.255.0


Cisco-ASA(config)#

object network 10.1.1.0_24


Cisco-ASA(config-network-object)#

subnet 10.1.1.0 255.255.255.0


Cisco-ASA(config)#
```

```
access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24
```

---

5. キーワードIKEv1を含むトランスフォームセット(TS)を設定します。 リモートエンドでも同じTSを作成する必要があります。

注：上記のフェーズ2のIKEv1属性は、『サイト間VPNゲートウェイ接続用のVPNデバイスとIPsec/IKEパラメータ』で参照できます。詳細については、Microsoft Azureサポートにお問い合わせください。

```
<#root>

Cisco-ASA(config)#

crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac
```

ステップ 6暗号マップを設定し、次のコンポーネントを含む外部インターフェイスに適用します。

- TSです。
- ピアのIPアドレス
- 対象のトラフィックを含む定義済みのアクセスリスト。
- この設定では、Perfect Forward Secrecy（PFS；完全転送秘密）は設定されません。「VPN Devices and IPsec/IKE Parameters for Site-to-Site VPN Gateway Connections」では、AzureのIKEv1ではPFSが無効であると記述されています。

オプションのPFS設定では、データの保護に使用されるDiffie-Hellmanキーの新しいペアが作成されます（フェーズ2が起動する前に、両側でPFSが有効になっている必要があります）。 この設定を有効にするには、crypto map outside_map 20 set pfsコマンドを実行します。

- フェーズ2のIPSecライフタイムは、VPNデバイスと、サイト間VPNゲートウェイ接続用のIPsec/IKEパラメータに基づいて設定されます。詳細については、Microsoft Azureサポートにお問い合わせください。

```
<#root>

Cisco-ASA(config)#
```

```
crypto map outside_map 20 match address 100

Cisco-ASA(config)#
crypto map outside_map 20 set peer 192.168.1.1

Cisco-ASA(config)#
crypto map outside_map 20 set ikev1 transform-set myset

Cisco-ASA(config)#
crypto map outside_map 20 set security-association lifetime seconds 3600

Cisco-ASA(config)#
crypto map outside_map 20 set security-association lifetime kilobytes 102400000
Cisco-ASA(config)#
crypto map outside_map interface outside
```

---

7. VPNトラフィックが他のNATルールの対象となっていないことを確認します。 NAT除外ルールを作成します。

```
<#root>
Cisco-ASA(config)#
nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination static 10.1.1.0_24 10.1.1.0_24
```

注：複数のサブネットを使用する場合は、すべての送信元サブネットと宛先サブネットでオブジェクトグループを作成し、NATルールで使用する必要があります。

```
<#root>
Cisco-ASA(config)#
```

```
object-group network 10.x.x.x_SOURCE

Cisco-ASA(config-network-object-group)#
network-object 10.4.4.0 255.255.255.0

Cisco-ASA(config-network-object-group)#
network-object 10.2.2.0 255.255.255.0


Cisco-ASA(config)#
object network 10.x.x.x_DESTINATION

Cisco-ASA(config-network-object-group)#
network-object 10.3.3.0 255.255.255.0

Cisco-ASA(config-network-object-group)#
network-object 10.1.1.0 255.255.255.0


Cisco-ASA(config)#
nat (inside,outside) 1 source static 10.x.x.x_SOURCE 10.x.x.x_SOURCE destination static 10.x.x.x_DESTINA
```

ASAコード9.8(1)以降のVTIを使用したIKEv2ルートベース

ASAコードのサイト間IKEv2ルートベースVPNの場合は、次の設定を使用します。Azureがルートベースの VPN用に構成されていることを確認し、Azureポータルで UsePolicyBasedTrafficSelectorsを構成していないことを確認してください。VTIがASAで設定されます。

ASA VTIの全設定情報については、『CLIブック3:Cisco ASAシリーズVPN CLIコンフィギュレーションガイド9.8』を参照してください。

---

1. OutsideインターフェイスでIKEv2を有効にします。

```
<#root>

Cisco-ASA(config)#

crypto ikev2 enable outside
```

---

2. IKEv2フェーズ1ポリシーを追加します。

注: Microsoftは、Azureで使用される特定のIKEv2フェーズ1暗号化、整合性、およびライフタイム属性と競合する情報を公開しています。リストされている属性は、VPNデバイスと、サイト間VPNゲートウェイ接続用のIPsec/IKEパラメータからの属性です。MicrosoftのIKEv2属性と競合する情報は、「Cisco ASAデバイス(IKEv2/no BGP)の設定例」です。 詳細については、Microsoft Azureサポートにお問い合わせください。

```
<#root>

Cisco-ASA(config)#

crypto ikev2 policy 1

Cisco-ASA(config-ikev2-policy)#

encryption aes-256

Cisco-ASA(config-ikev2-policy)#

integrity sha256

Cisco-ASA(config-ikev2-policy)#

group 14

Cisco-ASA(config-ikev2-policy)#

lifetime seconds 28800
```

---

3. IKEv2 Phase 2 IPsecプロポーザルを追加します。crypto IPsec ikev2 ipsec-proposalコンフィギュレーションモードでセキュリティパラメータを指定します。

protocol esp encryption {des | 3des | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 | null}
protocol esp integrity {md5 | sha-1 | sha-256 | sha-384 | sha-512 | null}

注：Microsoftは、Azureで使用される特定のフェーズ2 IPSec暗号化および整合性の属性に関して競合する情報を公開しています。リストされている属性は、VPNデバイスと、サイト間VPNゲートウェイ接続用のIPsec/IKEパラメータからの属性です。Microsoftからのフェーズ2 IPSec属性と競合する情報は、設定例：Cisco ASAデバイス(IKEv2/no BGP)です。 詳細については、Microsoft Azureサポートにお問い合わせください。

<#root>

```
Cisco-ASA(config)#

crypto ipsec ikev2 ipsec-proposal SET1


Cisco-ASA(config-ipsec-proposal)#

protocol esp encryption aes-256


Cisco-ASA(config-ipsec-proposal)#

protocol esp integrity sha-256
```

---

4. 次を指定するIPSecプロファイルを追加します。

- 以前に設定したikev2フェーズ2 IPSecプロポーザル。
- フェーズ2のIPSecライフタイム（オプション）を秒単位またはキロバイト単位（あるいはその両方）で指定します。
- PFSグループ（オプション）

注：Microsoftは、Azureで使用される特定のフェーズ2 IPSecライフタイムおよびPFS属性に関して競合する情報を公開しています。示されている属性は、『ルートベースのVPN IPSecセキュリティアソシエーション（IKEクイックモードSA）提供』からの引用です。Microsoftからのフェーズ2 IPSec属性と競合する情報は、設定例：Cisco ASAデバイス(IKEv2/no BGP)です。 詳細については、Microsoft Azureサポートにお問い合わせください。

<#root>

```
Cisco-ASA(config)#
crypto ipsec profile PROFILE1

Cisco-ASA(config-ipsec-profile)#
set ikev2 ipsec-proposal SET1

Cisco-ASA(config-ipsec-profile)#
set security-association lifetime seconds 27000

Cisco-ASA(config-ipsec-profile)#
set security-association lifetime kilobytes unlimited

Cisco-ASA(config-ipsec-profile)#
set pfs none
```

---

5. IPsec属性でトンネルグループを作成し、ピアIPアドレスとIKEv2ローカルおよびリモートトンネル事前共有キーを設定します。

```
<#root>
Cisco-ASA(config)#
tunnel-group 192.168.1.1 type ipsec-l2l

Cisco-ASA(config)#
tunnel-group 192.168.1.1 ipsec-attributes

Cisco-ASA(config-tunnel-ipsec)#
ikev2 local-authentication pre-shared-key cisco

Cisco-ASA(config-tunnel-ipsec)#
ikev2 remote-authentication pre-shared-key cisco
```

---

6. 次を指定するVTIを作成します。

- 新しいトンネルインターフェイス番号：interface tunnel [number]
- 新しいトンネルインターフェイス名：nameif [name]
- トンネルインターフェイスに存在しないIPアドレス：ip address [ip-address] [mask]
- VPNがローカルに終端するトンネル送信元インターフェイス：tunnel source interface [int-name]
- AzureゲートウェイのIPアドレス：トンネルの宛先[AzureパブリックIP]
- IPSec IPv4モード：tunnel mode ipsec ipv4
- このVTIに使用するIPSecプロファイル：tunnel protection ipsec profile [profile-name]

<#root>

```
Cisco-ASA(config)#

interface tunnel 100

Cisco-ASA(config-if)#

nameif vti

Cisco-ASA(config-if)#

ip address 169.254.0.1 255.255.255.252

Cisco-ASA(config-if)#

tunnel source interface outside

Cisco-ASA(config-if)#

tunnel destination [Azure Public IP]

Cisco-ASA(config-if)#

tunnel mode ipsec ipv4

Cisco-ASA(config-if)#

tunnel protection ipsec profile PROFILE1
```

---

7. トラフィックをトンネルに向かわせるためのスタティックルートを作成します。スタティックルートを追加するには、次のコマンドを実行します。

route if_name dest_ip mask gateway_ip [距離]

dest_ipとmaskは、Azureクラウド内の宛先ネットワークのIPアドレスです（例：10.0.0.0/24）。gateway_ipは、トンネルインターフェイスサブネット上の任意のIPアドレス（169.254.0.2など）である必要があります。このgateway_ipの目的は、トラフィックをトンネルインターフェイスに向けることですが、特定のゲートウェイIP自体は重要ではありません。

<#root>

```
Cisco-ASA(config)#

route vti 10.0.0.0 255.255.255.0 169.254.0.2
```

FTDでのIKEv1の設定

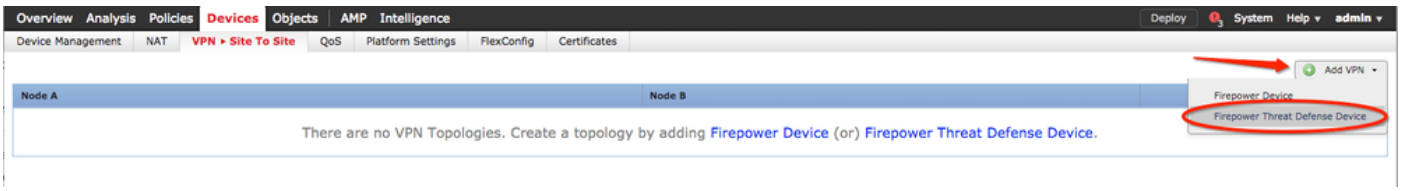
FTDからAzureへのサイト間IKEv1 VPNの場合、FTDデバイスをFMCに登録しておく必要があります。

---

1. サイト間ポリシーを作成します。FMCダッシュボード>デバイス> VPN >サイト間に移動します。

---

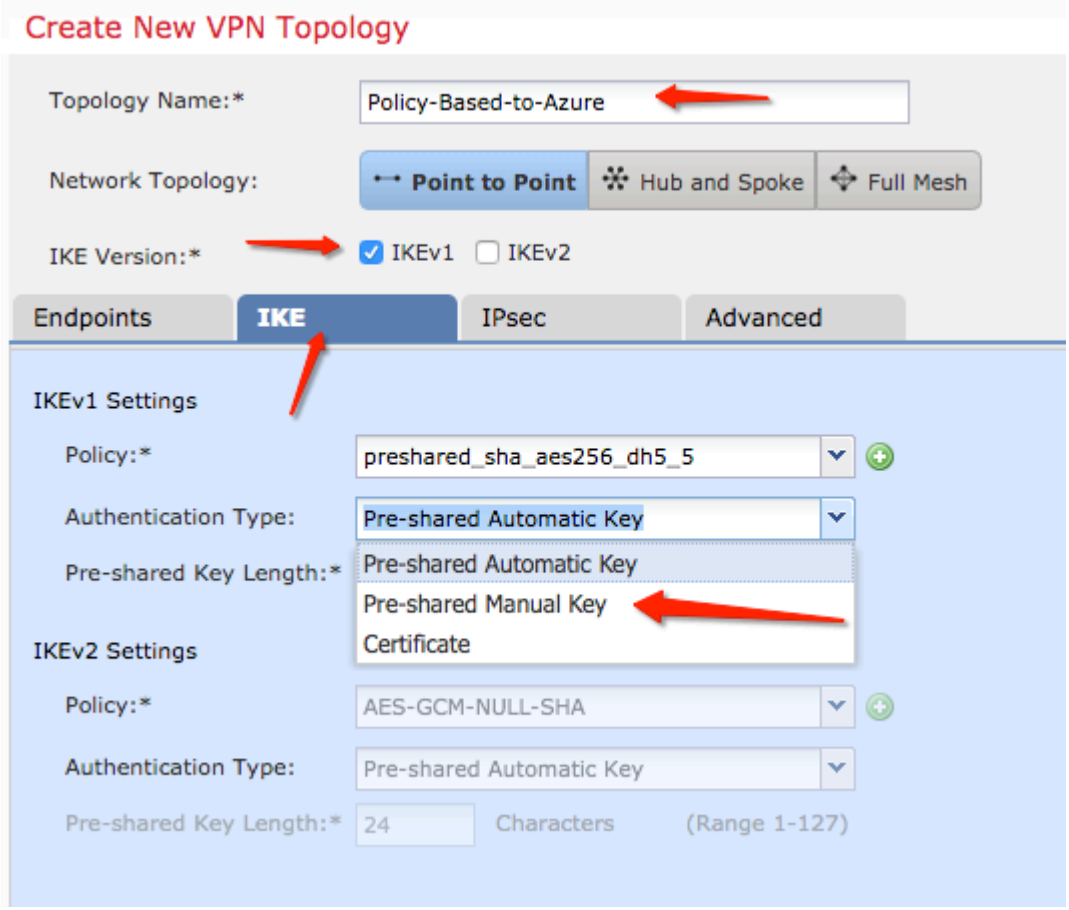
2. 新しいポリシーを作成します。Add VPNドロップダウンメニューをクリックし、Firepower Threat Defense Deviceを選択します。

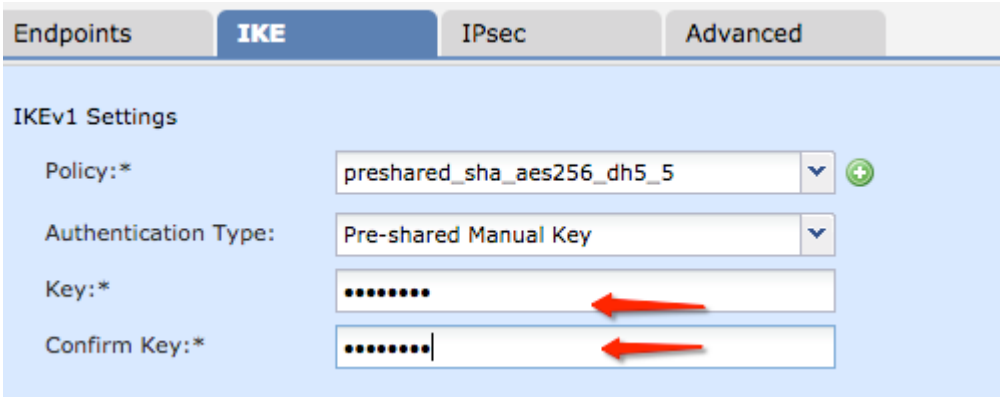


---

3. Create new VPN Topologyウィンドウで、Topology Nameを指定し、IKEV1 protocolチェック

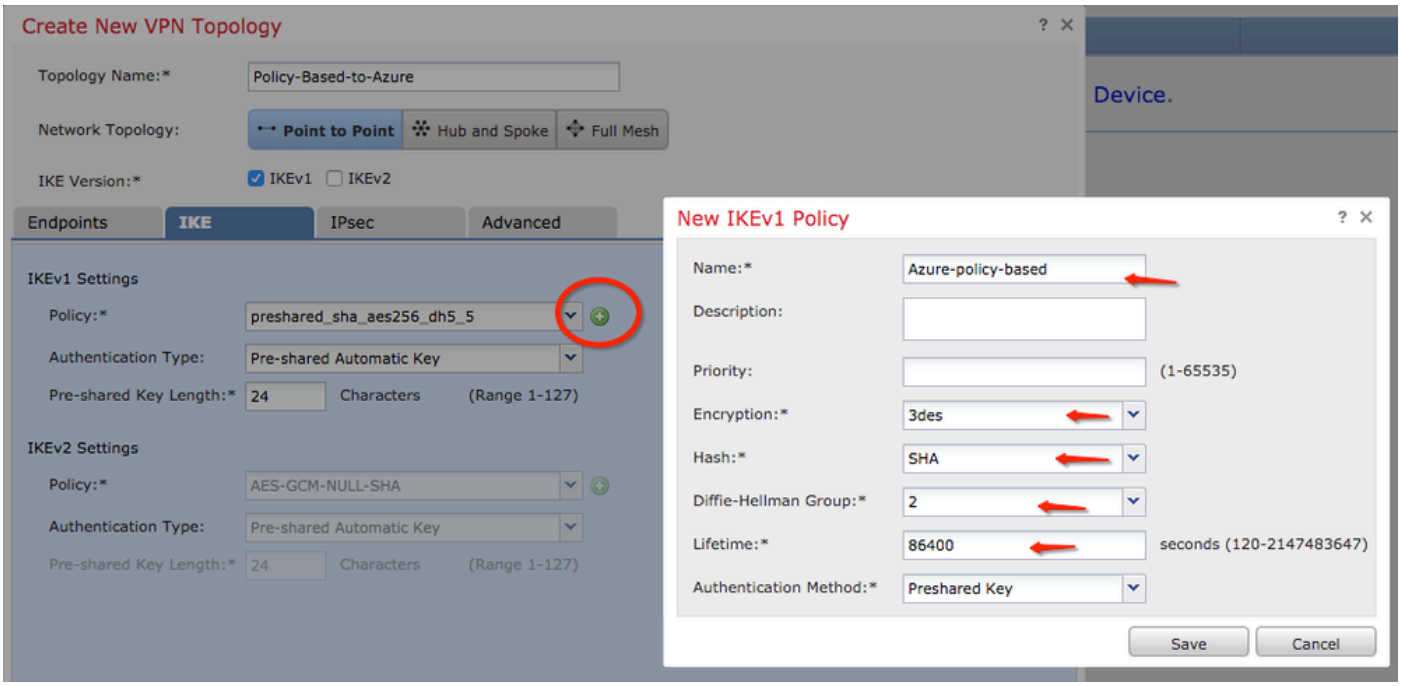
ボックスにチェックマークを入れて、IKEタブをクリックします。この例では、認証方式として事前共有キーが使用されます。Authentication Typeドロップダウンメニューをクリックし、Pre-shared Manual Keyを選択します。KeyおよびConfirm Keyテキストフィールドに手動事前共有キーを入力します。





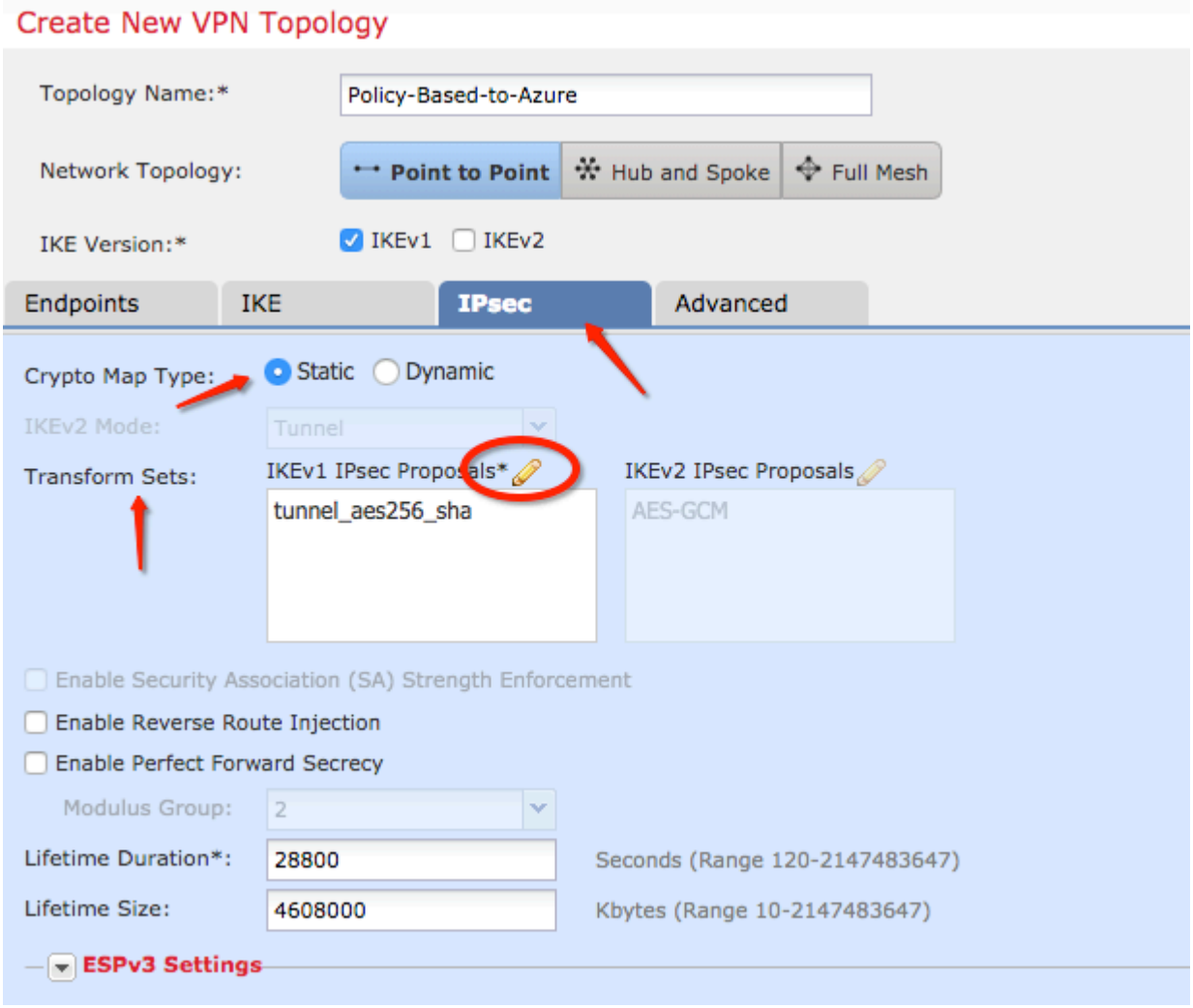
---

4. 新しいポリシーを作成して、ISAKMPポリシーまたはフェーズ1パラメータを設定します。同じウィンドウで、緑色の+ボタンをクリックして新しいISAKMPポリシーを追加します。ポリシーの名前を指定し、必要なEncryption、Hash、Diffie-Hellman Group、Lifetime、およびAuthentication Methodを選択し、Saveをクリックします。



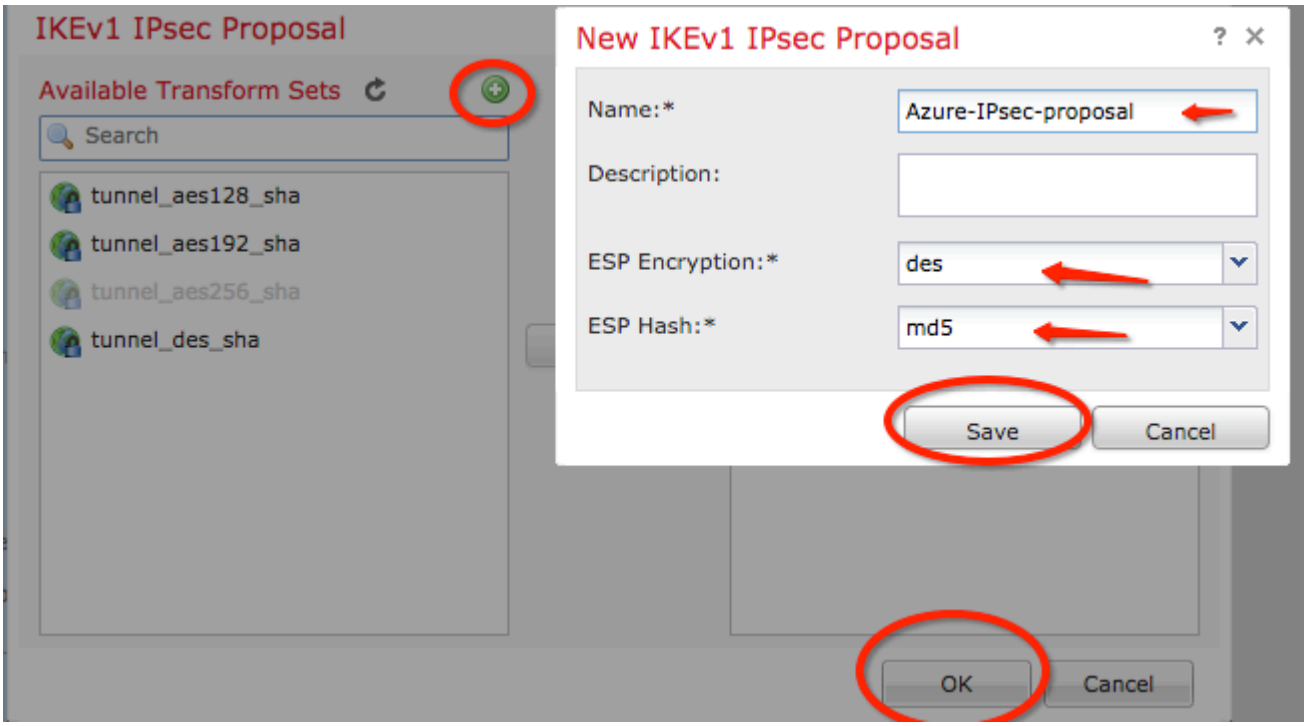
---

5. IPSecポリシーまたはフェーズ2パラメータを設定します。IPsecタブに移動し、Crypto Map TypeチェックボックスでStaticを選択します。Transform SetsオプションでIKEV1 IPSec Proposalsのedit pencilアイコンをクリックします。



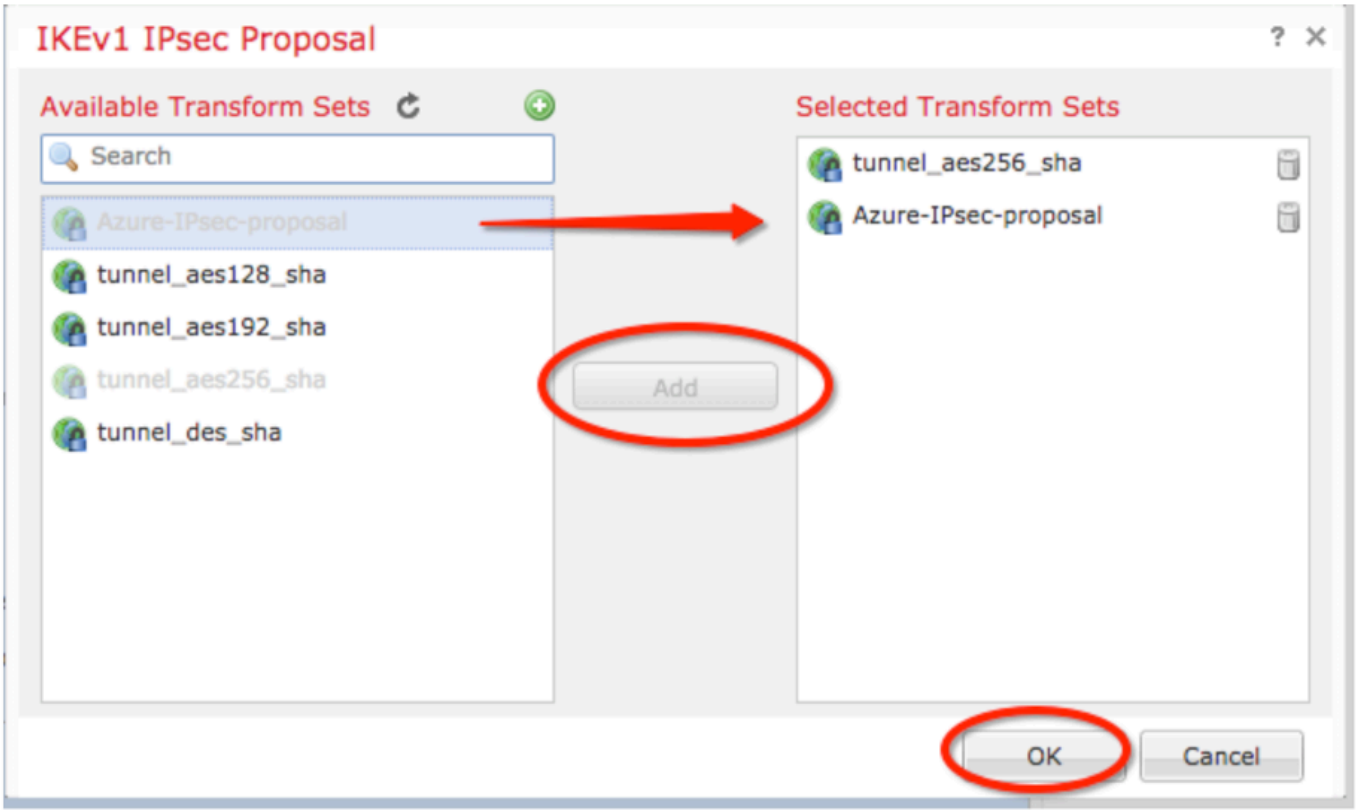
---

6. 新しいIPSecプロポーザルを作成します。IKEv1 IPSec Proposalウィンドウで、緑色の+ボタンをクリックして新しいプロポーザルを追加します。ポリシーの名前と、ESP暗号化およびESPハッシュアルゴリズムに必要なパラメータを指定し、Saveをクリックします。



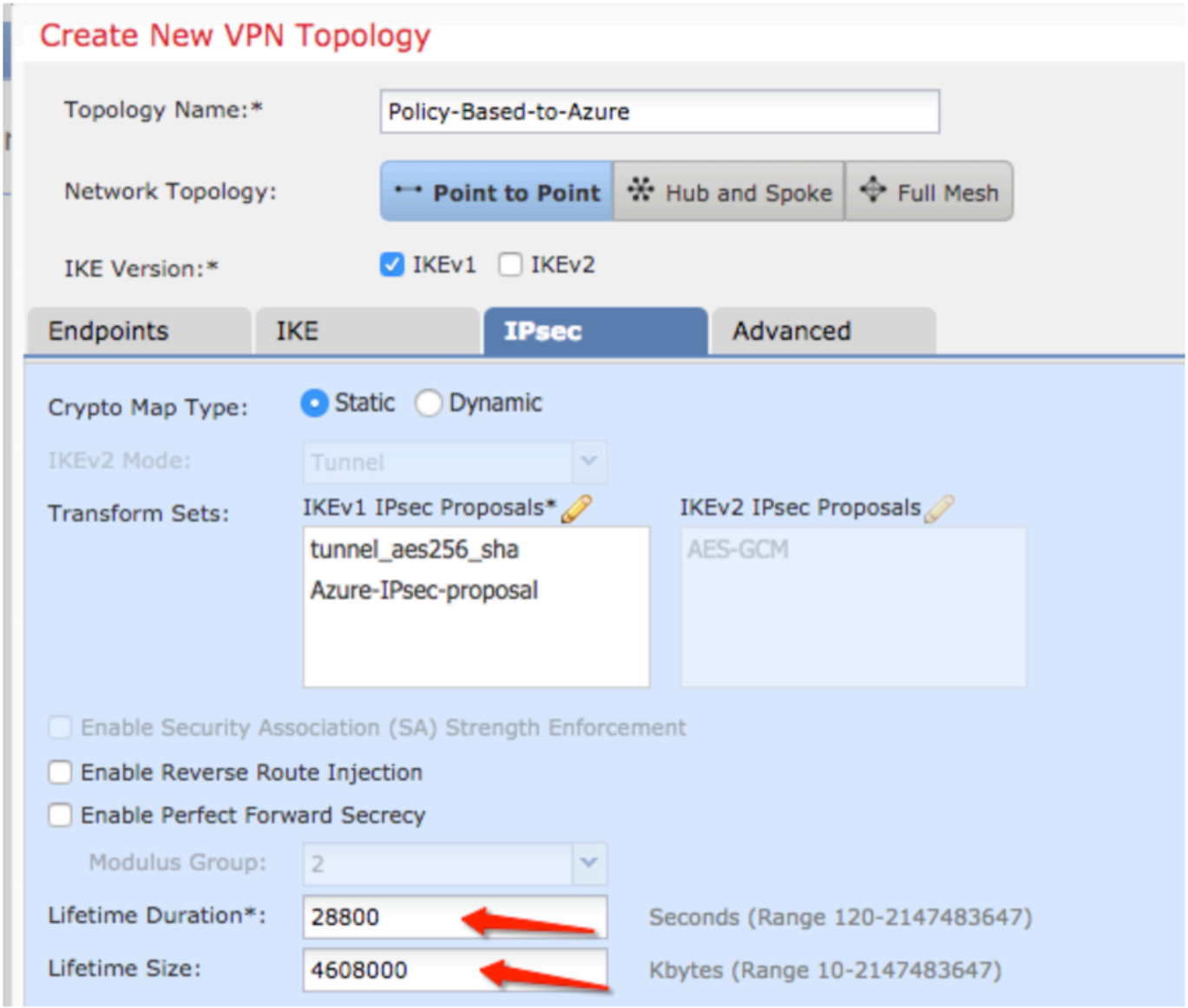
---

7. IKEV1 IPsec Proposalウィンドウで、新しいIPsecポリシーをSelected Transform Setsセクションに追加し、OKをクリックします。



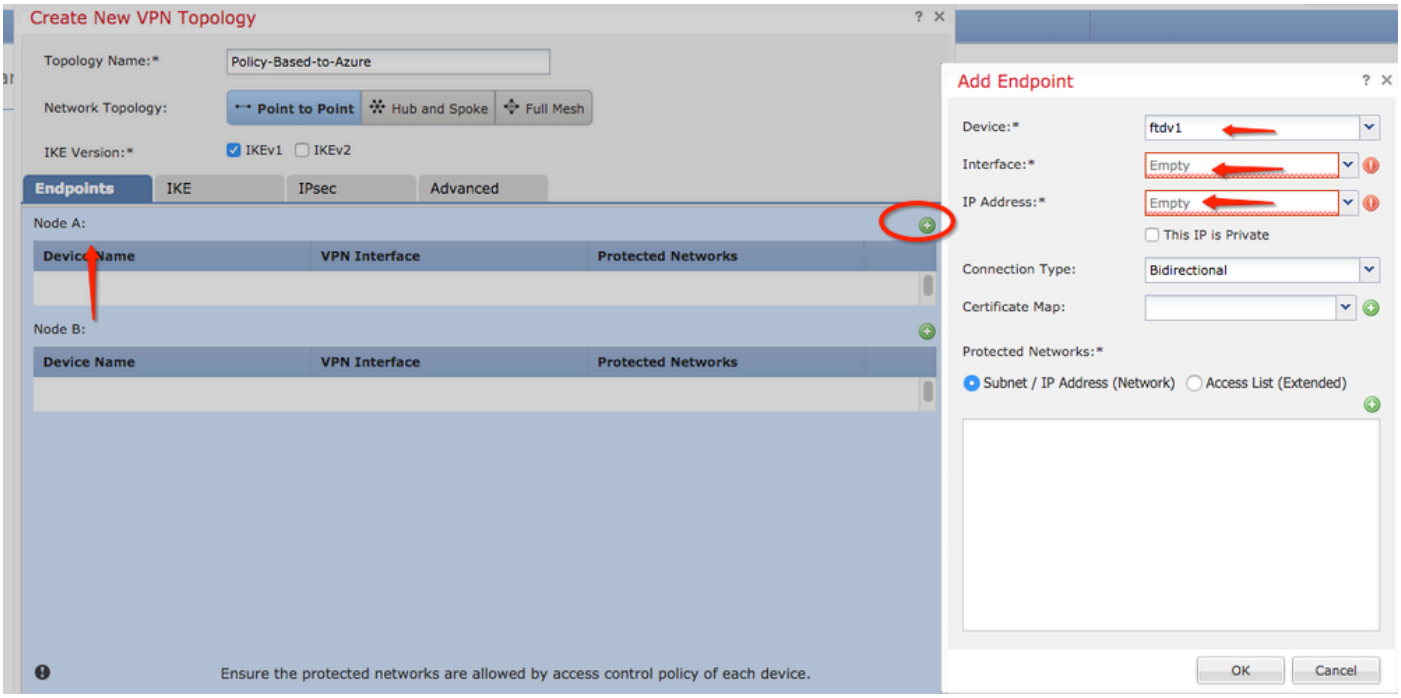
---

8. IPSecタブに戻り、目的のライフタイム期間とサイズを設定します。



---

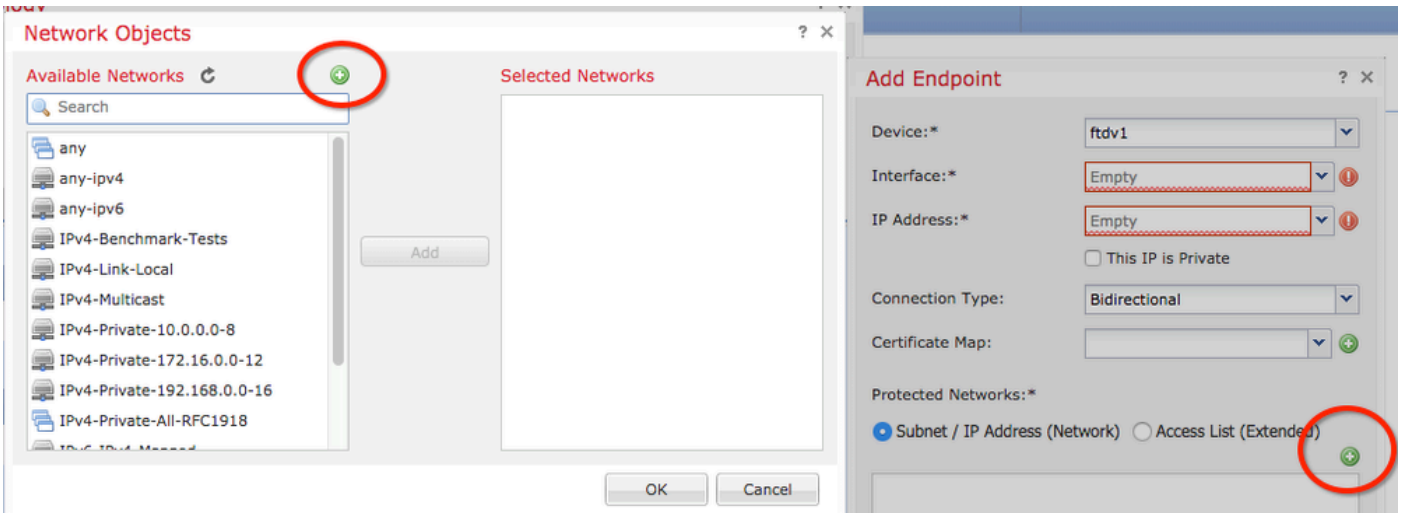
9. 暗号化ドメイン/トラフィックセレクタ/保護されたネットワークを選択します。Endpointsタブに移動します。ノードAで緑色の+ボタンをクリックして、新しいノードを追加します。この例では、ノードAがFTDへのローカルサブネットとして使用されています。



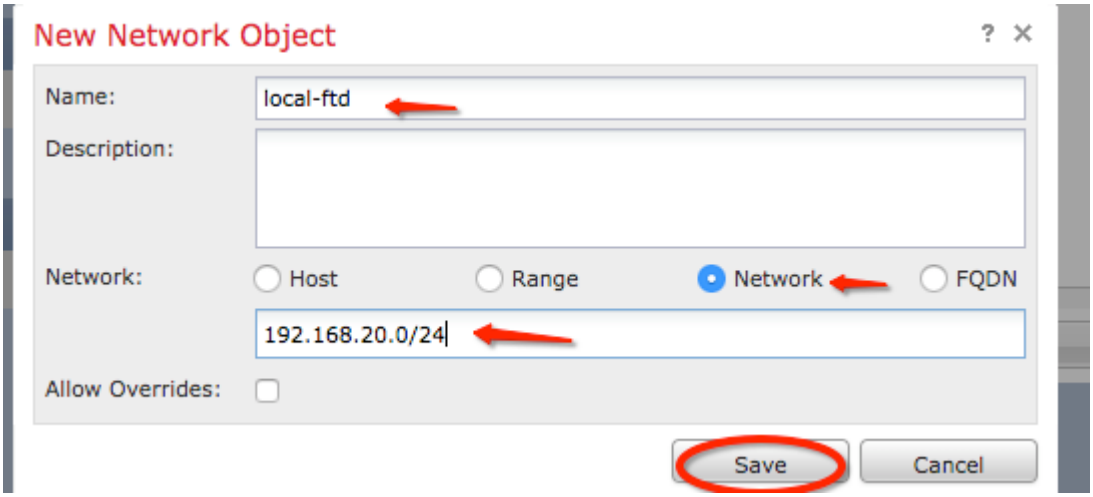
10. Add EndpointウィンドウのDeviceドロップダウンで、使用するFTDを、物理インターフェイスおよび使用するIPアドレスとともに指定します。

11. ローカルトラフィックセレクタを指定するには、Protected Networks オプションに移動し、緑色の+ボタンをクリックして新しいオブジェクトを作成します。

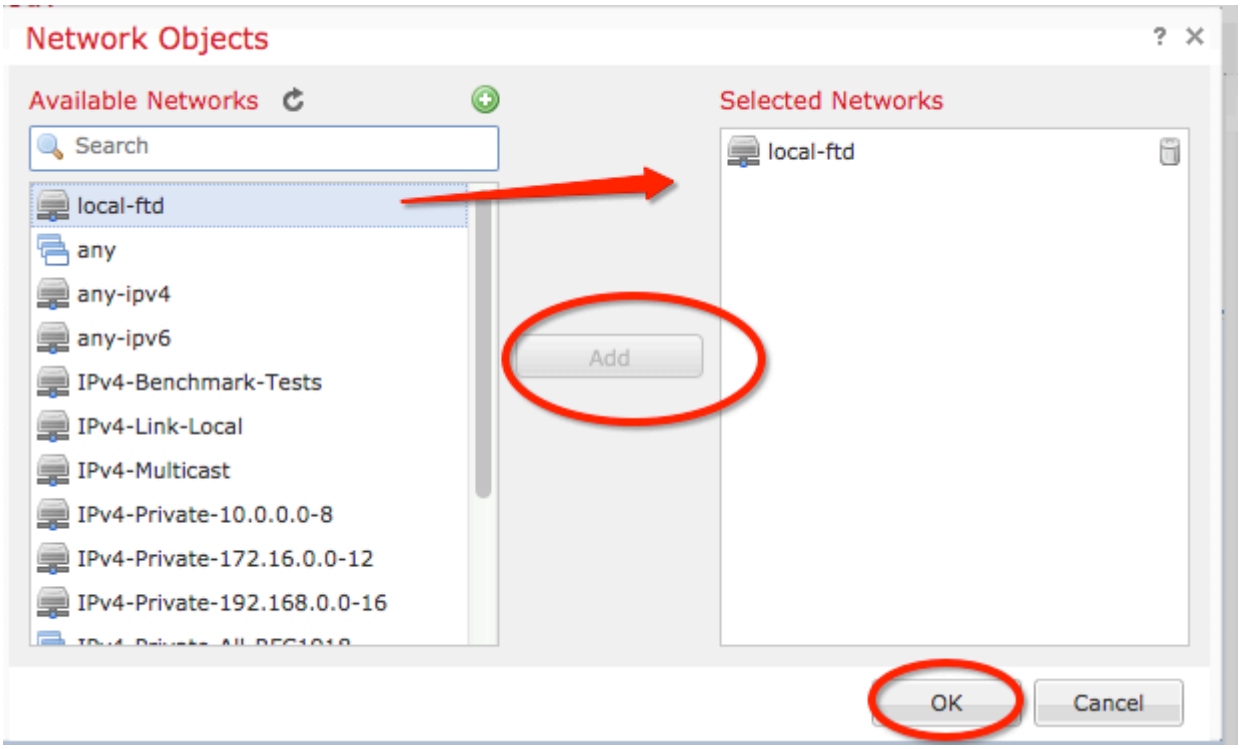
12. Network Objectsウィンドウで、Available Networksテキストの横にある緑色の+ボタンをクリックして、新しいローカルトラフィックセレクタオブジェクトを作成します。



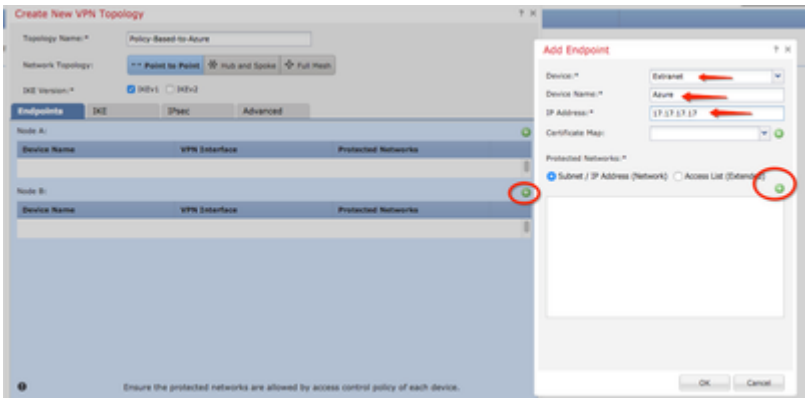
13. New Network Objectウィンドウで、オブジェクトの名前を指定し、それに応じてhost/network/range/FQDNを選択します。次に、Saveをクリックします。



14. オブジェクトをNetwork ObjectsウィンドウのSelected Networksセクションに追加し、OKをクリックします。 Add Endpointウィンドウで OKをクリックします。



15. ノードB（この例ではAzureエンドポイント）を定義します。Create New VPN Topologyウィンドウで、Node Bセクションに移動し、緑色の+ボタンをクリックしてリモートエンドポイントトラフィックセレクタを追加します。ノードAと同じFMCで管理されていないすべてのVPNピアエンドポイントにExtranetを指定します。デバイスの名前（ローカルでのみ有効）とIPアドレスを入力します。

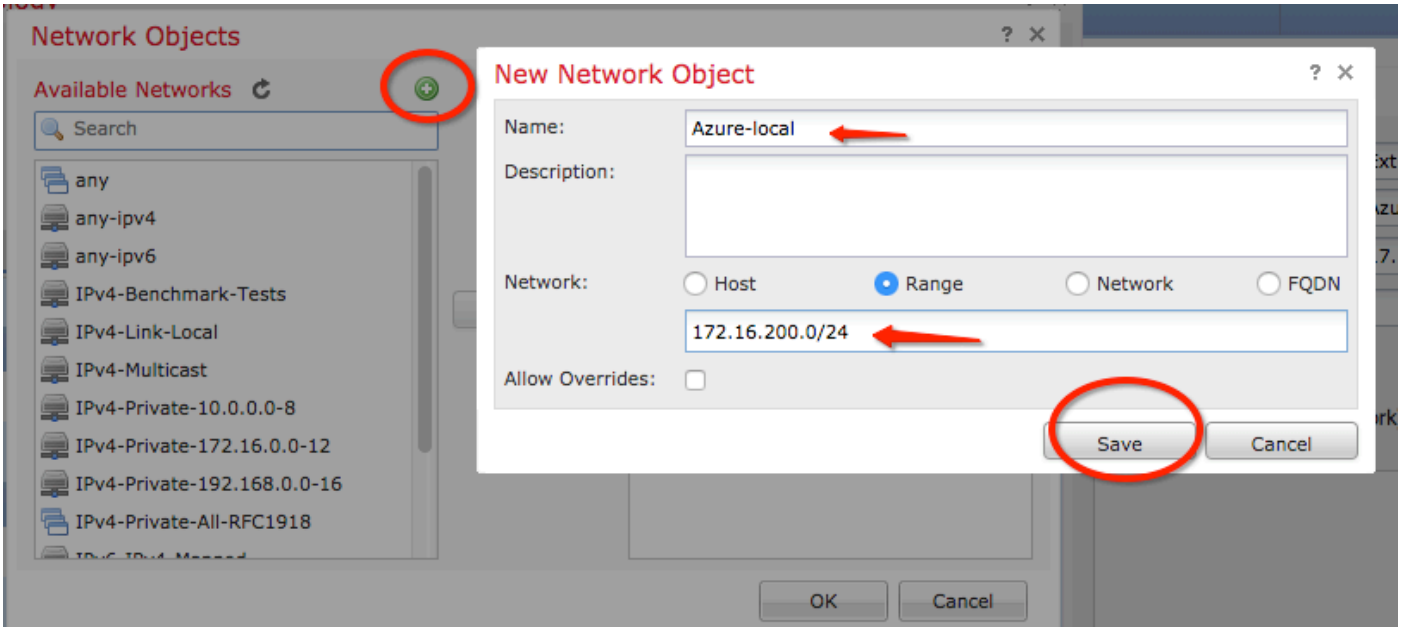


---

16. リモートトラフィックセレクタオブジェクトを作成します。Protected Networks セクションに移動し、緑色の+ボタンをクリックして新しいオブジェクトを追加します。

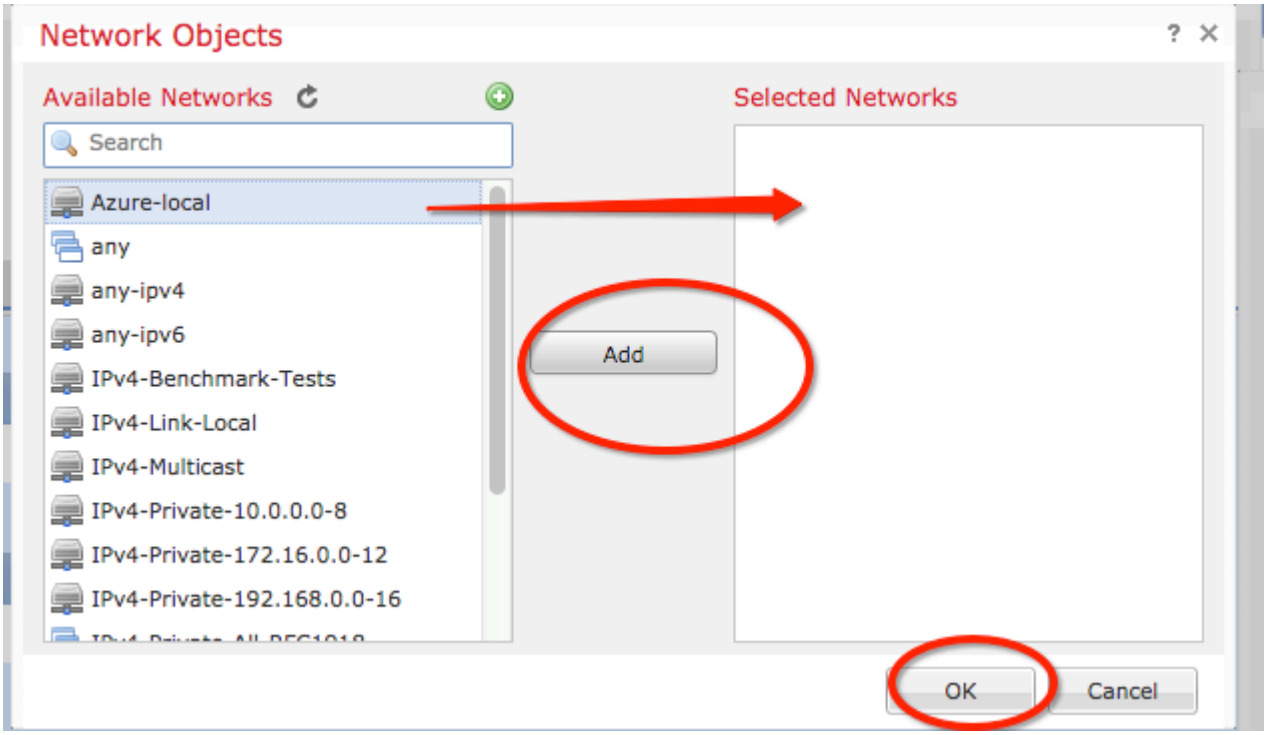
---

17. 「Network Objects」ウィンドウで、「Available Networks」テキストの横にある緑色の「+」ボタンをクリックして、新しいオブジェクトを作成します。New Network Objectウィンドウで、オブジェクトの名前を指定し、それに応じてhost/range/network/FQDNを選択し、Saveをクリックします。



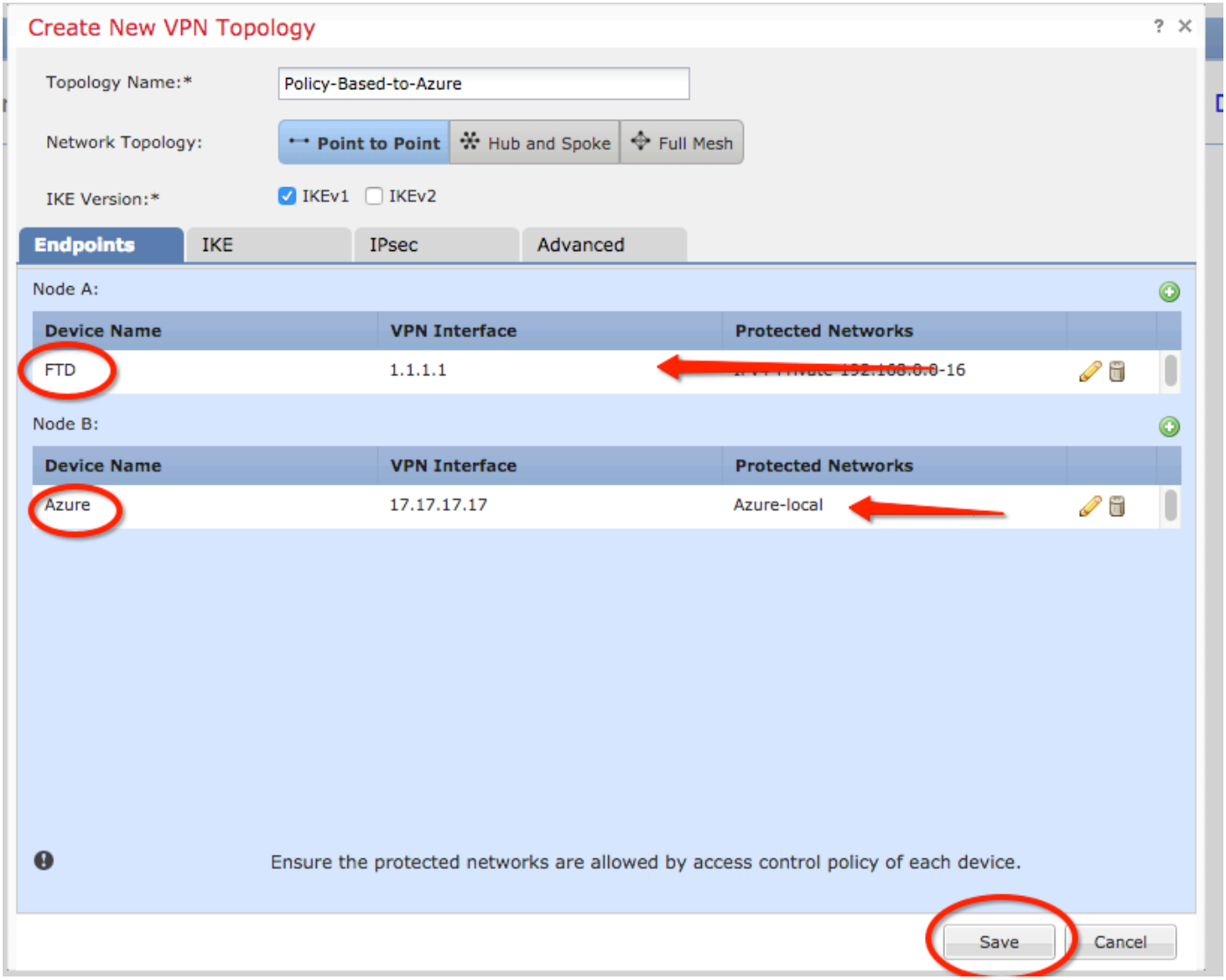
---

18. Network Objectsウィンドウに戻り、新しいリモートオブジェクトをSelected Networks セクションに追加して、OKをクリックします。Add Endpointウィンドウで OKをクリックします。



---

19. Create New VPN Topology ウィンドウで、両方のノードが正しいトラフィックセレクタまたは保護されたネットワークとともに表示されます。[Save] をクリックします。



---

20. FMCダッシュボードの右上のペインでDeployをクリックし、FTDデバイスを選択して、Deployをクリックします。

---

21. CLIでは、VPN設定はASAデバイスの設定と同じように表示されます。

ポリシーベースのトラフィックセレクタを使用したIKEv2ルートベース

暗号マップを使用するASAのサイト間IKEv2 VPNの場合は、次の設定を使用します。Azureがルートベースの VPN用に構成されていることを確認し、PowerShellを使用して UsePolicyBasedTrafficSelectorsをAzureポータルで構成する必要があります。

「Microsoftからの複数のオンプレミスのポリシーベースVPNデバイスへのVPNゲートウェイの接

続」では、UsePolicyBasedTrafficSelectorsとルートベースのAzure VPNモードの組み合わせの設定について説明しています。この手順を完了しないと、Azureから受信したトラフィックセレクタの不一致が原因で、暗号マップを含むASAは接続を確立できません。

暗号マップを使用したASA IKEv2の設定情報については、『CLIブック3:Cisco ASAシリーズVPN CLIコンフィギュレーションガイド9.8』を参照してください。

---

1. OutsideインターフェイスでIKEv2を有効にします。

```
<#root>

Cisco-ASA(config)#

crypto ikev2 enable outside
```

---

2. IKEv2フェーズ1ポリシーを追加します。

注: Microsoftは、Azureで使用されるIKEv2フェーズ1の暗号化、整合性、およびライフタイム属性と競合する情報を公開しています。リストされている属性は、VPNデバイスと、サイト間VPNゲートウェイ接続用のIPsec/IKEパラメータからの属性です。競合するMicrosoftからのIKEv2属性情報は、「Cisco ASAデバイス（IKEv2/BGPなし）」の設定例です。 詳細については、Microsoft Azureサポートにお問い合わせください。

```
<#root>

Cisco-ASA(config)#

crypto ikev2 policy 1


Cisco-ASA(config-ikev2-policy)#

encryption aes-256

Cisco-ASA(config-ikev2-policy)#

integrity sha256

Cisco-ASA(config-ikev2-policy)#
```

```
group 14

Cisco-ASA(config-ikev2-policy)#

lifetime seconds 28800
```

---

3. IPsec属性でトンネルグループを作成し、ピアIPアドレスとIKEv2ローカルおよびリモートトンネル事前共有キーを設定します。

```
<#root>

Cisco-ASA(config)#

tunnel-group 192.168.1.1 type ipsec-l2l


Cisco-ASA(config)#

tunnel-group 192.168.1.1 ipsec-attributes


Cisco-ASA(config-tunnel-ipsec)#

ikev2 local-authentication pre-shared-key cisco


Cisco-ASA(config-tunnel-ipsec)#

ikev2 remote-authentication pre-shared-key cisco
```

---

4. 暗号化してトンネリングするトラフィックを定義するアクセスリストを作成します。この例では、対象のトラフィックは、10.2.2.0サブネットから10.1.1.0に送信されたトンネルからのトラフィックです。サイト間に複数のサブネットが関係する場合は、複数のエントリを含めることができます。

バージョン8.4以降では、ネットワーク、サブネット、ホストIPアドレス、または複数のオブジェクトのコンテナとして機能するオブジェクトまたはオブジェクトグループを作成できます。ローカルとリモートのサブネットを持つ2つのオブジェクトを作成し、クリプトACLとNAT文の両方に使用します。

```
<#root>

Cisco-ASA(config)#

object network 10.2.2.0_24


Cisco-ASA(config-network-object)#

subnet 10.2.2.0 255.255.255.0


Cisco-ASA(config)#

object network 10.1.1.0_24


Cisco-ASA(config-network-object)#

subnet 10.1.1.0 255.255.255.0



Cisco-ASA(config)#

access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24
```

---

5. IKEv2 Phase 2 IPsecプロポーザルを追加します。crypto IPsec ikev2 ipsec-proposalコンフィギュレーションモードでセキュリティパラメータを指定します。

protocol esp encryption {des | 3des | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 | null}
protocol esp integrity {md5 | sha-1 | sha-256 | sha-384 | sha-512 | null}

注: Microsoftは、Azureで使用されるフェーズ2 IPSec暗号化および整合性の属性と競合する情報を公開しました。示されている属性は、『ルートベースのVPN IPSecセキュリティアソシエーション（IKEクイックモードSA）提供』からの引用です。競合するMicrosoftからのフェーズ2 IPSec属性情報は、「Cisco ASAデバイス(IKEv2/no BGP)」の設定例です。 詳細については、Microsoft Azureサポートにお問い合わせください。

```
<#root>

Cisco-ASA(config)#
```

```
crypto ipsec ikev2 ipsec-proposal SET1

Cisco-ASA(config-ipsec-proposal)#

protocol esp encryption aes-256

Cisco-ASA(config-ipsec-proposal)#

protocol esp integrity sha-256
```

---

6. 暗号マップを設定し、次のコンポーネントを含む外部インターフェイスに適用します。

・ ピアIPアドレス。
・ 対象のトラフィックを含む定義済みのアクセスリスト。
・ IKEv2フェーズ2 IPSecプロポーザル。
・ フェーズ2のIPSecライフタイム（秒単位）。
・ オプションのPFS(Perfect Forward Secrecy)設定。データの保護に使用されるDiffie-Hellmanキーの新しいペアを作成します（フェーズ2が起動する前に、両側でPFSが有効になっている必要があります）。

Microsoftは、Azureで使用されるフェーズ2 IPSecの有効期間およびPFS属性と競合する情報を公開しました。

示されている属性は、『ルートベースのVPN IPSecセキュリティアソシエーション（IKEクイックモードSA）提供』からの引用です。

競合するMicrosoftからのフェーズ2 IPSec属性情報は、「Cisco ASAデバイス(IKEv2/no BGP)」の設定例です。 詳細については、Microsoft Azureサポートにお問い合わせください。

<#root>

```
Cisco-ASA(config)#

crypto map outside_map 20 match address 100

Cisco-ASA(config)#

crypto map outside_map 20 set peer 192.168.1.1
```

```
Cisco-ASA(config)#

crypto map outside_map 20 set ikev2 ipsec-proposal myset


Cisco-ASA(config)#

crypto map outside_map 20 set security-association lifetime seconds 27000


Cisco-ASA(config)#

crypto map outside_map 20 set security-association lifetime kilobytes unlimited

Cisco-ASA(config)#

crypto map outside_map 20 set pfs none

Cisco-ASA(config)#

crypto map outside_map interface outside
```

---

8. VPNトラフィックが他のNATルールの対象となっていないことを確認します。 NAT除外ルールを作成します。

```
<#root>

Cisco-ASA(config)#

nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination static 10.1.1.0_24 10.1.1.0_24
```

注：複数のサブネットを使用する場合は、すべての送信元サブネットと宛先サブネットでオブジェクトグループを作成し、NATルールで使用する必要があります。

```
<#root>

Cisco-ASA(config)#

object-group  network 10.x.x.x_SOURCE


Cisco-ASA(config-network-object-group)#
```

```
network-object  10.4.4.0 255.255.255.0

Cisco-ASA(config-network-object-group)#
network-object  10.2.2.0 255.255.255.0


Cisco-ASA(config)#
object network 10.x.x.x_DESTINATION

Cisco-ASA(config-network-object-group)#
network-object  10.3.3.0 255.255.255.0

Cisco-ASA(config-network-object-group)#
network-object  10.1.1.0 255.255.255.0


Cisco-ASA(config)#
nat (inside,outside) 1 source static 10.x.x.x_SOURCE 10.x.x.x_SOURCE destination

static 10.x.x.x_DESTINATION  10.x.x.x_DESTINATION no-proxy-arp route-lookup
```

確認

ASAとAzureゲートウェイの両方で構成が完了すると、AzureはVPNトンネルを開始します。次のコマンドを使用して、トンネルが正しく構築されていることを確認できます。

フェーズ 1

Phase 1セキュリティアソシエーション(SA)が作成されたことを確認します。

次に、UDPポート500上のローカル外部インターフェイスIP 192.168.1.2からリモート宛先IP

192.168.2.2に構築されたIKEv2 SAが示されます。また、暗号化されたトラフィックが通過するように構築された有効な子SAもあります。

<#root>

```
    Cisco-ASA#

 show crypto ikev2 sa


IKEv2 SAs:

Session-id:44615, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                                 Remote
  3208253 192.168.1.2/500                                       192.168.2.2/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/142 sec
*-->Child sa: local selector  192.168.0.0/0 - 192.168.0.255/65535
          remote selector 192.168.3.0/0 - 192.168.3.255/65535
          ESP spi in/out: 0x9b60edc5/0x8e7a2e12
```

この例では、IKEv1 SAはASAを使用してピアIP 192.168.2.2に対する発信側として構築され、残りのライフタイムは86388秒です。

<#root>

```
    Cisco-ASA#

 sh crypto ikev1 sa detail


IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 192.168.2.2
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
    Encrypt : aes             Hash    : SHA
    Auth    : preshared       Lifetime: 86400
    Lifetime Remaining: 86388
```

フェーズ 2

フェーズ2のIPSecセキュリティアソシエーションがshow crypto ipsec sa peer [peer-ip]を使用して構築されていることを確認します。

<#root>

```
Cisco-ASA#

 show crypto ipsec sa peer 192.168.2.2



peer address: 192.168.2.2
 Crypto map tag: outside, seq num: 10, local addr: 192.168.1.2

 access-list VPN extended permit ip 192.168.0.0 255.255.255.0 192.168.3.0 255.255.255.0
 local ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)
 remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
 current_peer: 192.168.2.2


 #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
 #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 4, #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.: 192.168.1.2/500, remote crypto endpt.: 192.168.2.2/500
 path mtu 1500, ipsec overhead 74(44), media mtu 1500
 PMTU time remaining (sec): 0, DF policy: copy-df
 ICMP error validation: disabled, TFC packets: disabled
 current outbound spi: 8E7A2E12
 current inbound spi : 9B60EDC5

 inbound esp sas:
 spi: 0x9B60EDC5 (2606820805)
 SA State: active
 transform: esp-aes-256 esp-sha256-hmac no compression
 in use settings ={L2L, Tunnel, IKEv2, }
 slot: 0, conn_id: 182743040, crypto-map: outside
 sa timing: remaining key lifetime (kB/sec): (4193279/28522)
 IV size: 16 bytes
 replay detection support: Y
 Anti replay bitmap:
 0x00000000 0x0000001F

 outbound esp sas:
 spi: 0x8E7A2E12 (2390371858)
 SA State: active
 transform: esp-aes-256 esp-sha256-hmac no compression
 in use settings ={L2L, Tunnel, IKEv2, }
 slot: 0, conn_id: 182743040, crypto-map: outside
 sa timing: remaining key lifetime (kB/sec): (3962879/28522)
 IV size: 16 bytes
 replay detection support: Y
 Anti replay bitmap:
 0x00000000 0x00000001
```

4つのパケットが送信され、4つはエラーなしでIPSec SAを介して受信されます。SPI 0x9B60EDC5を使用した着信SAが1つと、SPI 0x8E7A2E12を使用した発信SAが1つ正常にインストールされています。

また、vpn-sessiondb l2lエントリのチェックを通じて、トンネルを通過するデータを確認することもできます。

<#root>

```
Cisco-ASA#

show vpn-sessiondb l2l



Session Type: LAN-to-LAN

Connection : 192.168.2.2
Index : 44615 IP Addr : 192.168.2.2
Protocol : IKEv2 IPsec
Encryption : IKEv2: (1)AES256 IPsec: (1)AES256
Hashing : IKEv2: (1)SHA256 IPsec: (1)SHA256
Bytes Tx : 400 Bytes Rx : 400
Login Time : 18:32:54 UTC Tue Mar 13 2018
Duration : 0h:05m:22s
```

バイトTx：およびバイトRx:IPSec SAを介した送受信データカウンタを表示します。

トラブルシュート

1. VPNのトラフィックが、内部インターフェイス上のAzureプライベートネットワーク宛てのASAによって受信されることを確認します。テストするには、内部クライアントからの連続pingを設定し、ASAでパケットキャプチャを設定して受信されたことを確認します。

---

capture [cap-name] interface [if-name] match [protocol] [src-ip] [src-mask] [dest-ip] [dest-mask]

show capture [cap-name]

<#root>

```
Cisco-ASA#

capture inside interface inside match ip host [local-host] host [remote-host]


Cisco-ASA#

show capture inside


2 packets captured

   1: 18:50:42.835863       192.168.0.2 > 192.168.3.2: icmp: echo request
   2: 18:50:42.839128       192.168.3.2 > 192.168.0.2: icmp: echo reply
2 packets shown
```

- Azureからの応答トラフィックが表示される場合、VPNは適切に構築され、トラフィックを送受信します。
- 送信元トラフィックがない場合は、送信者がASAに適切にルーティングしていることを確認します。
- 送信元トラフィックは見られるものの、Azureからの応答トラフィックがない場合は、その理由を引き続き確認します。

---

2. ASA内部インターフェイスで受信したトラフィックがASAで適切に処理され、VPNにルーティングされていることを確認します。

ICMPエコー要求をシミュレートするには、次の手順を実行します。

packet-tracer input [inside-interface-name] icmp [inside-host-ip] 8 0 [azure-host-ip]詳細

詳細なパケットトレーサの使用ガイドライン「パケットトレーサを使用したアクセス問題のトラブルシューティング」を参照してください。

<#root>

```
Cisco-ASA#

 packet-tracer input inside icmp 192.168.0.2 8 0 192.168.3.2 detail
```

```
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7f6c19afb0a0, priority=13, domain=capture, deny=false
        hits=3, user_data=0x7f6c19afb9b0, cs_id=0x0, l3_type=0x0
        src mac=0000.0000.0000, mask=0000.0000.0000
        dst mac=0000.0000.0000, mask=0000.0000.0000
        input_ifc=inside, output_ifc=any

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7f6c195971f0, priority=1, domain=permit, deny=false
        hits=32, user_data=0x0, cs_id=0x0, l3_type=0x8
        src mac=0000.0000.0000, mask=0000.0000.0000
        dst mac=0000.0000.0000, mask=0100.0000.0000
        input_ifc=inside, output_ifc=any

Phase: 3
Type:


ROUTE-LOOKUP


Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.1.1


using egress ifc  outside



Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7f6c192502900, priority=0, domain=nat-per-session, deny=true
        hits=41, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=any, output_ifc=any

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
 Forward Flow based lookup yields rule:
 in  id=0x7f6c1987c120, priority=0, domain=inspect-ip-options, deny=true
        hits=26, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=inside, output_ifc=any

Phase: 6
Type: QOS
Subtype:
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7f6c19a60280, priority=70, domain=qos-per-class, deny=false
        hits=30, user_data=0x7f6c19a5c030, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=any, output_ifc=any

Phase: 7
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7f6c1983ab50, priority=66, domain=inspect-icmp-error, deny=false
        hits=27, user_data=0x7f6c1987afc0, cs_id=0x0, use_real_addr, flags=0x0, protocol=1
        src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, tag=any, dscp=0x0
        input_ifc=inside, output_ifc=any

Phase: 8
Type:

VPN


Subtype: encrypt
Result:

ALLOW


Config:
Additional Information:
 Forward Flow based lookup yields rule:
 out id=0x7f6c19afe1a0, priority=70, domain=encrypt, deny=false
        hits=2, user_data=0x13134, cs_id=0x7f6c19349670, reverse, flags=0x0, protocol=0
        src ip/id=192.168.0.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=192.168.3.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=any, output_ifc=outside

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 43, packet dispatched to next module
Module information for forward flow ...
```

```
snp_fp_tracer_drop
snp_fp_inspect_ip_options
snp_fp_inspect_icmp
snp_fp_adjacency
snp_fp_encrypt
snp_fp_fragment
snp_ifc_stat

Module information for reverse flow ...

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

NATはトラフィックを除外します（変換は行われません）。 VPNトラフィックでNAT変換が発生しないことを確認します。 また、output-interfaceが正しいことを確認します。これは、暗号マップが適用されている物理インターフェイス、または仮想トンネルインターフェイスである必要があります。

アクセスリストのドロップが発生していないことを確認します。 VPNフェーズでENCRYPT: ALLOWと表示された場合、トンネルはすでに構築されており、encapsを使用してインストールされたIPSec SAを確認できます。

2.1.パケットトレーサに「ENCRYPT: ALLOW」が表示される場合

- IPSec SAがインストールされていることを確認し、show crypto ipsec saを使用してトラフィックを暗号化します。
- 外部インターフェイスでキャプチャを実行して、暗号化されたパケットがASAから送信され、暗号化された応答がAzureから受信されることを確認できます。

2.2. ENCRYPT:DROPがパケットトレーサで見られる場合。

- VPNトンネルはまだ確立されていませんが、ネゴシエーション中です。これは、最初にトンネルを起動したときに予期される状態です。デバッグを実行してトンネルネゴシエーションプロセスを表示し、障害が発生した場所と障害が発生した場合を特定します。

正しいバージョンのIKEがトリガーされ、ike-commonプロセスに関連するエラーが表示されてい

ないことを確認します。

<#root>

```
Cisco-ASA#
```

debug crypto ike-common 255

```
Cisco-ASA# Mar 13 18:58:14 [IKE COMMON DEBUG]Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1.
```

VPNトラフィックの開始時にike-common debug出力が表示されない場合、これはトラフィックが暗号化プロセスに到達する前にドロップされるか、ボックスでcrypto ikev1/ikev2が有効でないことを意味します。暗号設定とパケットドロップを再確認します。

ike-commonデバッグで暗号化プロセスがトリガーされたことが示された場合、IKE構成バージョンをデバッグしてトンネルネゴシエーションメッセージを表示し、Azureを使用したトンネル構築でエラーが発生した場所を特定します。

IKEv1

ikev1デバッグの完全な手順と分析「ASA IPsecおよびIKEデバッグ（IKEv1メインモード）トラブルシューティングテクニカルノート」を参照してください。

<#root>

```
Cisco-ASA#
```

debug crypto ikev1 127

```
Cisco-ASA#
```

debug crypto ipsec 127

IKEv2

完全なikev2デバッグ手順と分析「PSKによるサイト間VPNのためのASA IKEv2デバッグの使用」

を参照してください。

<#root>

Cisco-ASA#

debug crypto ikev2 platform 127

Cisco-ASA#

debug crypto ikev2 protocol 127

Cisco-ASA#

debug crypto ipsec 127

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。