

ASAおよびFTDからMicrosoft AzureへのポリシーベースおよびルートベースのVPNの設定

内容

[概要](#)

[コンセプト](#)

[VPN暗号化ドメイン](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ASAでのIKEv1の設定](#)

[ASAコード9.8\(1\)以降での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](#)

[トラブルシューティング](#)

[IKEv1](#)

[IKEv2](#)

概要

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。

コンセプト

VPN暗号化ドメイン

IPSecでVPNトンネルに参加できるIPアドレス範囲。暗号化ドメインは、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を使用して定義され、IPSecでキャプチャおよび暗号化す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には、次の2つの方法があります。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。

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のトラフィックセレクタは0.0.0.0に設定されます。これは、IPSecトンネルにルーティングされるすべてのトラフィックが、送信元/宛先サブネットに関係なく暗号化されることを意味します。

Cisco適応型セキュリティアプライアンス(ASA)は、バージョン9.8以降の仮想トンネルインターフェイス(VTI)を使用して、ルートベースのVPNをサポートします。

FMC(Firepower Management Center)によって管理される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をサポートしません。

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範囲のみを暗号化するように設定されています。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を介して暗号化するトラフィックを識別します。

ASAは、バージョン8.2以降で暗号マップを使用するポリシーベースのVPNをサポートします。

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、選択したVPN方式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。つまり、IKEv2を使用する場合、Azureのルートベースを選択し、ASAでVTIを使用する必要がありますが、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を構成する必要があります。これは、PowerShellスクリプトの展開を使用してAzureポータルで実行され、次に説明するように、MicrosoftがUsePolicyBasedTrafficSelectorsを呼び出すオプションを実装します。

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps> にアクセスしてください。

ASAとFTDの設定の観点から要約すると、次のようになります。

- 暗号マップを使用して設定された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に設定する必要があります。
- VTIで設定されたASAでは、AzureをルートベースVPN用に設定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、次を参照してください。
https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/firepower_threat_defense_site_to_site_vpns.html#concept_ccj_p4r_cmb

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用に構成する必要があります)。
- ASAおよびFTDでクリプトマップを使用する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 (AzureはポリシーベースVPN用に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 : 暗号マップが設定されたASAコードバージョン8.2以降。
(Azureは、UsePolicyBasedTrafficSelectorsを使用するルートベースVPN用に構成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。

- Cisco ASA
- Microsoft Azure
- Cisco FTD
- Cisco FMC

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、初期（デフォルト）設定の状態から起動しています。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。

設定

設定手順を実行します。IKEv1、VTIに基づくIKEv2ルートベース、またはUse Policy-Based Traffic Selectors (ASAのクリプトマップ) に基づく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については、次のASA設定に従ってください。Azureポータルでポリシーベースのトンネルを構成してください。この例では、ASAで暗号マップを使用します。

ASAの設定情報の詳細については、[このCiscoドキュメント](#)を参照してください。

ステップ1：外部インターフェイスでIKEv1を有効にします。

```
Cisco-ASA(config)#crypto ikev1 enable outside
```

手順2：ハッシュ、認証、Diffie-Hellmanグループ、ライフタイム、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：記載されているフェーズ1のIKEv1属性は、この公開されているMicrosoftのドキュメントから**[ベストエフォートを提供します](#)**。詳細については、Microsoft Azureサポートにお問い合わせください。

```
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 2
Cisco-ASA(config-ikev1-policy)#lifetime 28800
```

ステップ3:IPsec属性の下に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。

```
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
```

ステップ4：暗号化および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。この例で対象となるトラフィックは、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している場合は、このトラフィックに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、crypto Access Control List (ACL; 暗号アクセスコントロールリスト) とNetwork Address Translation (NAT; ネットワークアドレス変換) の両方のステートメントに使用します。

```
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
```

ステップ5：キーワードを含むトランスフォームセット(TS)を設定します。IKEv1. 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：記載されているフェーズ2のIKEv1属性は、この公開されているMicrosoftのドキュメントから[ベストエフォートで提供されます](#)。詳細については、Microsoft Azureサポートにお問い合わせください。

```
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

- ・ピアIPアドレス
- ・対象のトラフィックを含む定義済みアクセスリスト
- ・TS
- ・この構成ではPerfect Forward Secrecy (PFS)が設定されません。これは、一般に公開されている[Azureのドキュメント](#)で、AzureのIKEv1に対してPFSが無効にされているためです。データを保護するために使用される新しいDiffie-Hellmanキーのペアを作成するオプションのPFS設定(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る)は、次の設定を使用して有効にできます。 `crypto map outside_map 20 set pfs` .
- ・フェーズ2のIPSecライフタイムセットは、一般に公開されている[Azureドキュメントに基づいています](#)。詳細については、Microsoft Azureサポートにお問い合わせください。

```
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
```

ステップ7:VPNトラフィックが他のNATルールの対象に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。

```
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 no-proxy-arp route-lookup
```

注：複数のサブネットを使用する場合は、すべての送信元および宛先サブネットを含む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。

```
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
```

ASAコード9.8(1)以降でのVTIを使用したIKEv2ルートベース

ASAコードでのサイト間IKEv2ルートベースVPNの場合は、次の設定に従います。AzureがルートベースVPN用に構成されていることを確認してください。また、AzureポータルでUsePolicyBasedTrafficSelectorsを構成しないでください。VTIがASAで設定されている。

ASA VTIの設定情報の詳細については、[このCiscoドキュメント](#)を参照してください。

ステップ1：外部インターフェイスでIKEv2を有効にします。

```
Cisco-ASA(config)#crypto ikev2 enable outside
```

手順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、および有効期間の属性に関して競合する情報を公開しています。記載されている属性は、この公開されているMicrosoftのドキュメント[からベストエフォートで提供されています](#)。MicrosoftのIKEv2属性と競合する情報が表示され**ません**。詳細については、Microsoft Azureサポートにお問い合わせください。

```
Cisco-ASA(config)#crypto ikev2 policy 1
Cisco-ASA(config-ikev2-policy)#encryption aes
Cisco-ASA(config-ikev2-policy)#integrity sha
Cisco-ASA(config-ikev2-policy)#group 2
Cisco-ASA(config-ikev2-policy)#lifetime seconds 28800
```

ステップ3:IKEv2フェーズ2のIPsecプロポーザルを追加します。暗号化IPsecのセキュリティパラメータを指定します `ikev2 ipsec-proposal ip inspect` コマンドを使用して、一連の:

```
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。記載されている属性は、この公開されているMicrosoftのドキュメント [からベストエフォートで提供されています](#)。Microsoftのフェーズ2 IPsec属性と競合する情報が [表示されます](#)。詳細については、Microsoft Azureサポートにお問い合わせください。

```
Cisco-ASA(config)#crypto ipsec ikev2 ipsec-proposal SET1
Cisco-ASA(config-ipsec-proposal)#protocol esp encryption aes
Cisco-ASA(config-ipsec-proposal)#protocol esp integrity sha-1
```

ステップ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) (秒単位またはキロバイト)
- PFSグループ (オプション)

注: Microsoftは、Azureが使用する特定のフェーズ2 IPsecライフタイムとPFS属性に関して競合する情報を公開しています。記載されている属性は、この公開されているMicrosoftのドキュメント [からベストエフォートで提供されています](#)。Microsoftのフェーズ2 IPsec属性と競合する情報が [表示されます](#)。詳細については、Microsoft Azureサポートにお問い合わせください。

```
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
```

ステップ5:IPsec属性の下に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。

```
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
```

ステップ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 [名前]`
- トンネルインターフェイス上に存在しないIPアドレス: `ip address [ip-address] [mask]`
- VPNがローカルで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]

```
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
```

ステップ7：トラフィックをトンネルに向ける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、次のコマンドを入力します。

```
route if_name dest_ip mask gateway_ip [distance]
```

「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(たとえば、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。

```
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に事前に登録しておく必要があります。

ステップ1：サイト間ポリシーを作成します。次に移動します。FMC dashboard > Devices > VPN > Site to Site.



ステップ2：新しいポリシーを作成します。をクリックします。Add VPN ドロップダウンメニューから Firepower Threat Defense device .



ステップ3: Create new VPN Topology ウィンドウで、Topology Nameをチェックし、IKEv1 Protocolチェックボックスをオンにし、IKE tab.この例では、事前共有キーを認証方式として使用します。

をクリックします。Authentication Type ドロップダウンメニューを選択し、Pre-shared manual key .手動の事前共有キーを Key と Confirm Key テキストフィールド。

Create New VPN Topology


Topology Name:*

Network Topology: Point to Point Hub and Spoke Full Mesh


IKE Version:* IKEv1 IKEv2

Endpoints **IKE** IPsec Advanced


IKEv1 Settings

Policy:* 

Authentication Type:

Pre-shared Key Length:*
 

IKEv2 Settings


Policy:* 

Authentication Type:


Pre-shared Key Length:* Characters (Range 1-127)


Endpoints **IKE** IPsec Advanced

IKEv1 Settings

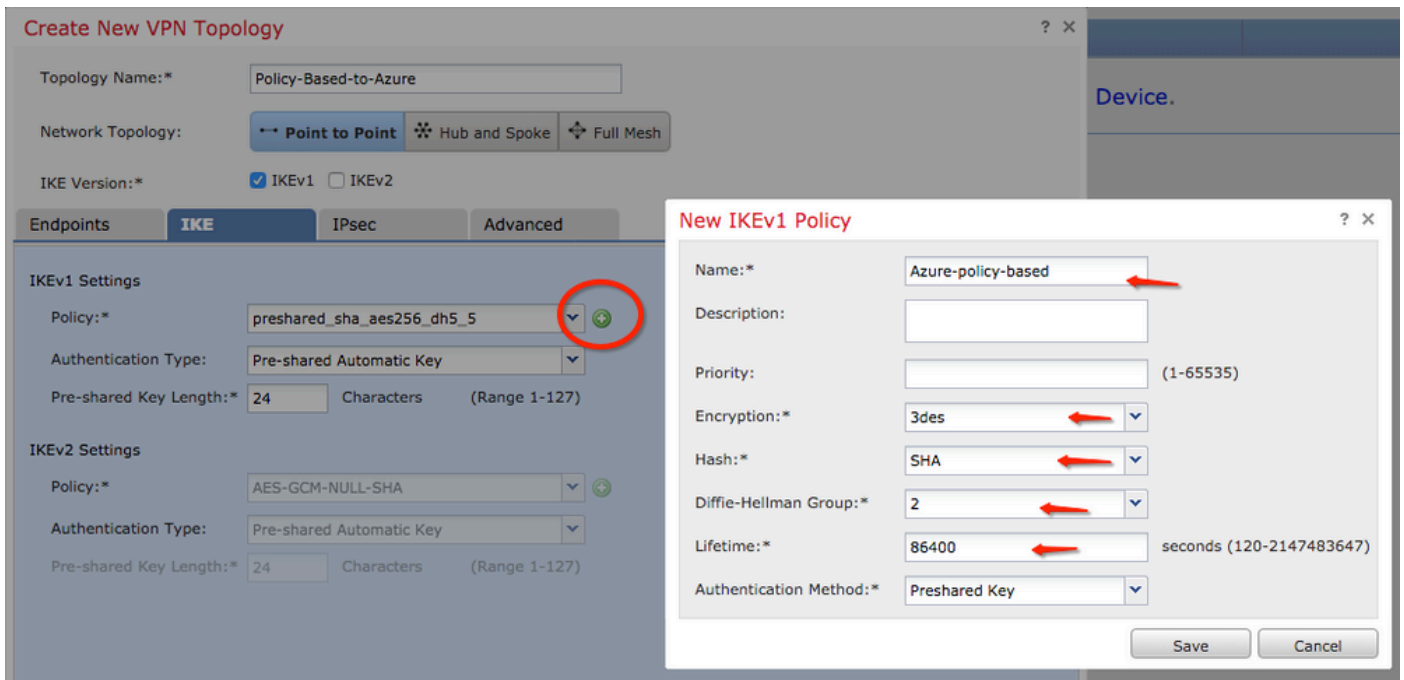
Policy:* 

Authentication Type:

Key:* 

Confirm Key:* 

ステップ4：新しいISAKMPポリシーまたはフェーズ1パラメータを作成して設定します。同じウィンドウで、 **green plus button** 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、目的の[Encryption]、[Hash]、[Diffie-Hellman Group]、[Lifetime]、および[Authentication Method]を選択して、 **Save** .



ステップ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。次に移動します。IPsec タブ、選択 Static IPv6の Crypto Map Type チェックボックスにマークを付けます。ポリシーの横の [レポート (Report)] edit pencil アイコン IKEV1 IPsec Proposals ユーティリティは Transform Sets オプション.

Create New VPN Topology

Topology Name:*

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints | IKE | **IPsec** | Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode:

Transform Sets:

IKEv1 IPsec Proposals*	IKEv2 IPsec Proposals
<input type="text" value="tunnel_aes256_sha"/>	<input type="text" value="AES-GCM"/>

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

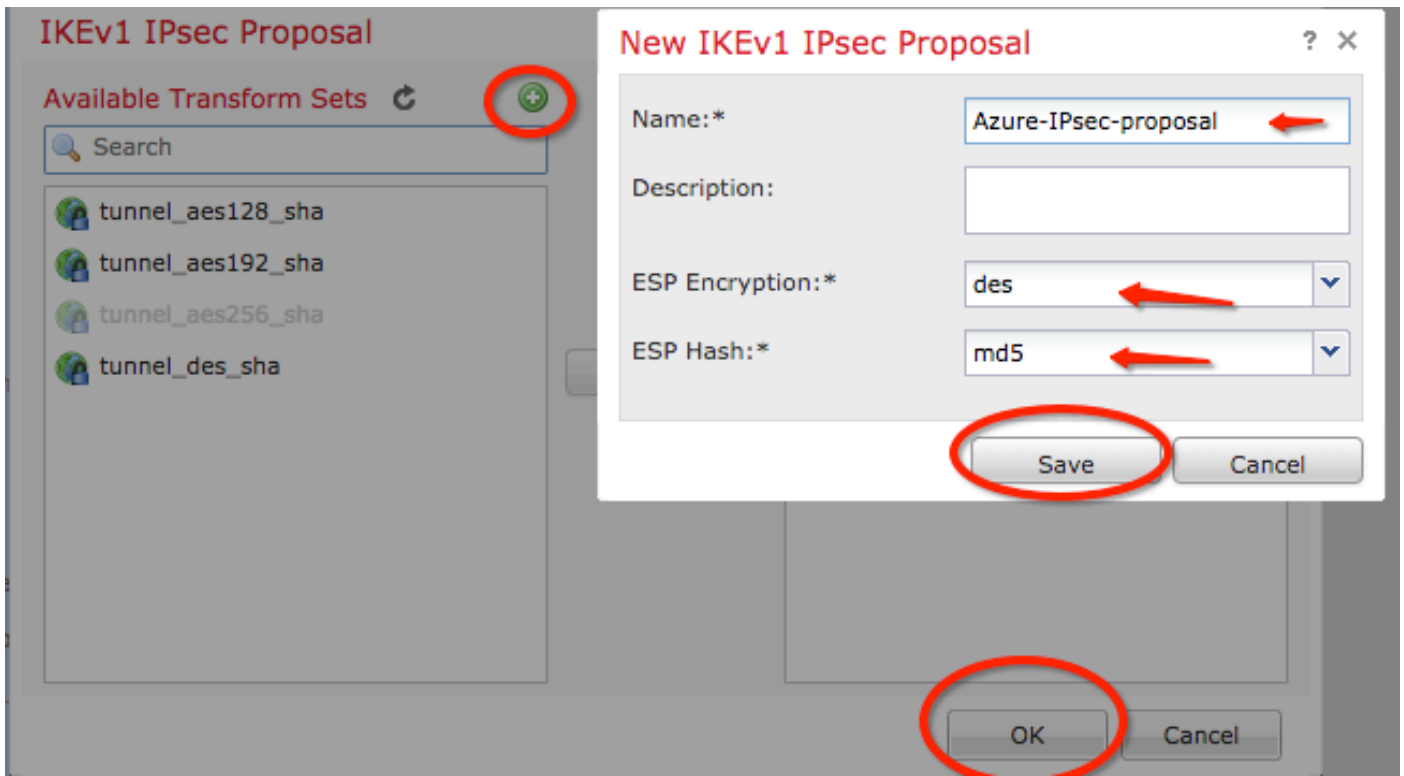
Modulus Group:

Lifetime Duration*: Seconds (Range 120-2147483647)

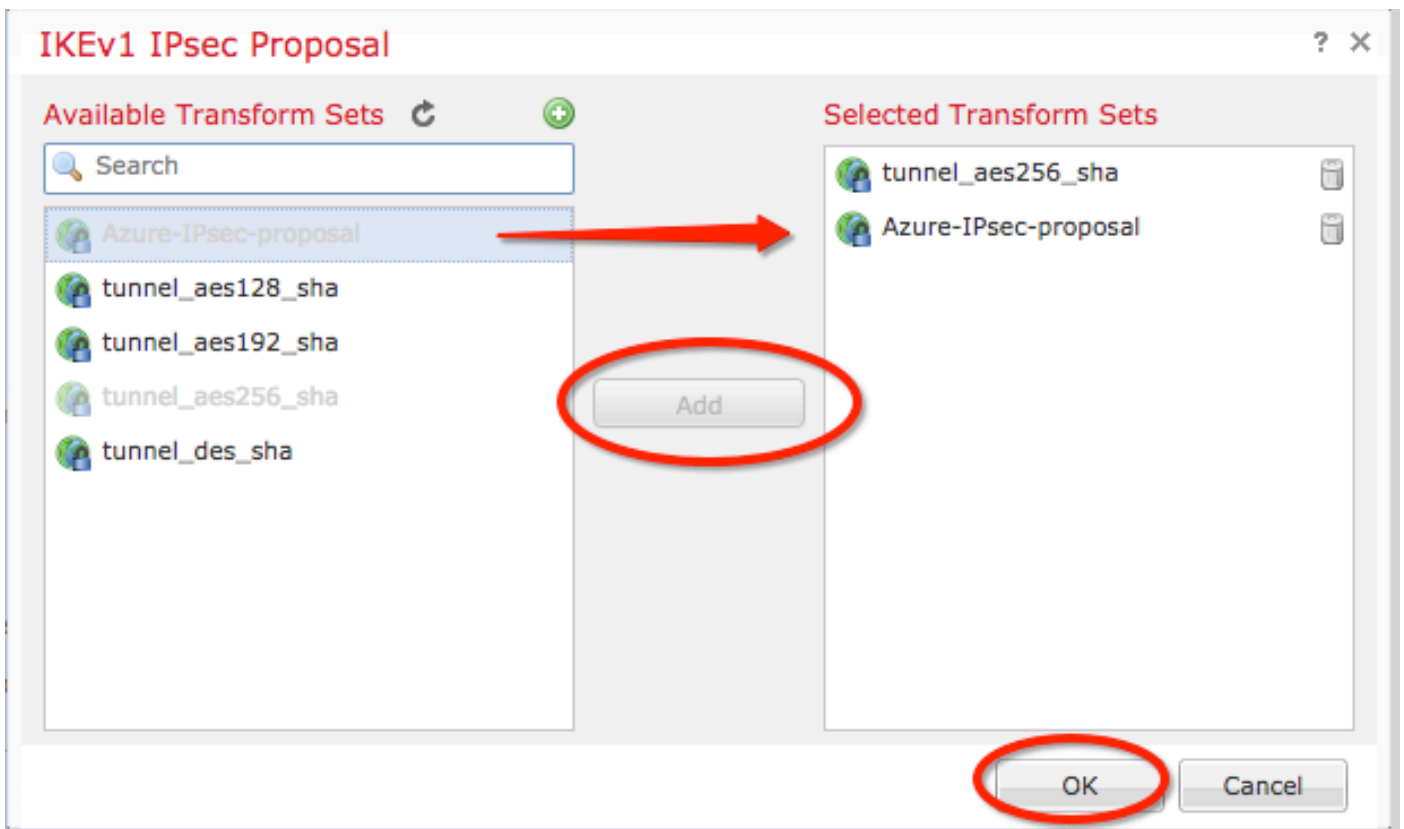
Lifetime Size: Kbytes (Range 10-2147483647)

ESPv3 Settings

ステップ6：新しいIPsecプロポーザルを作成します。Cisco IOSソフトウェア IKEv1 IPsec Proposal ウィンドウで、green plus button をクリックします。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 .



手順 7 : Cisco IOSソフトウェア IKEV1 IPsec Proposal ウィンドウで、新しいIPsecポリシーを Selected Transform Sets セクションをクリック OK .



ステップ8: IPsec タブをクリックして、目的のライフタイム期間とサイズを設定します。

Create New VPN Topology

Topology Name:* Policy-Based-to-Azure

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

IPsec Endpoints IKE Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals* IKEv2 IPsec Proposals

tunnel_aes256_sha
Azure-IPsec-proposal

AES-GCM

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

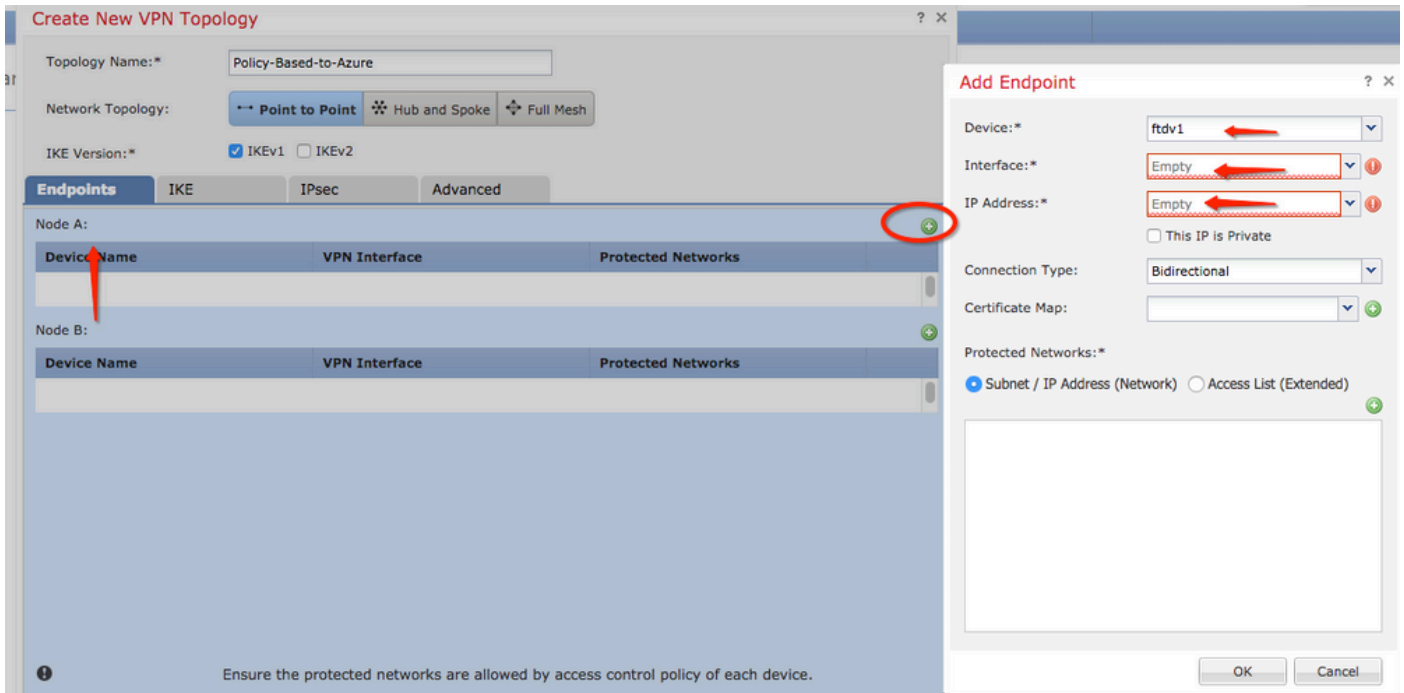
Modulus Group: 2

Lifetime Duration*: 28800 Seconds (Range 120-2147483647)

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

ESPv3 Settings

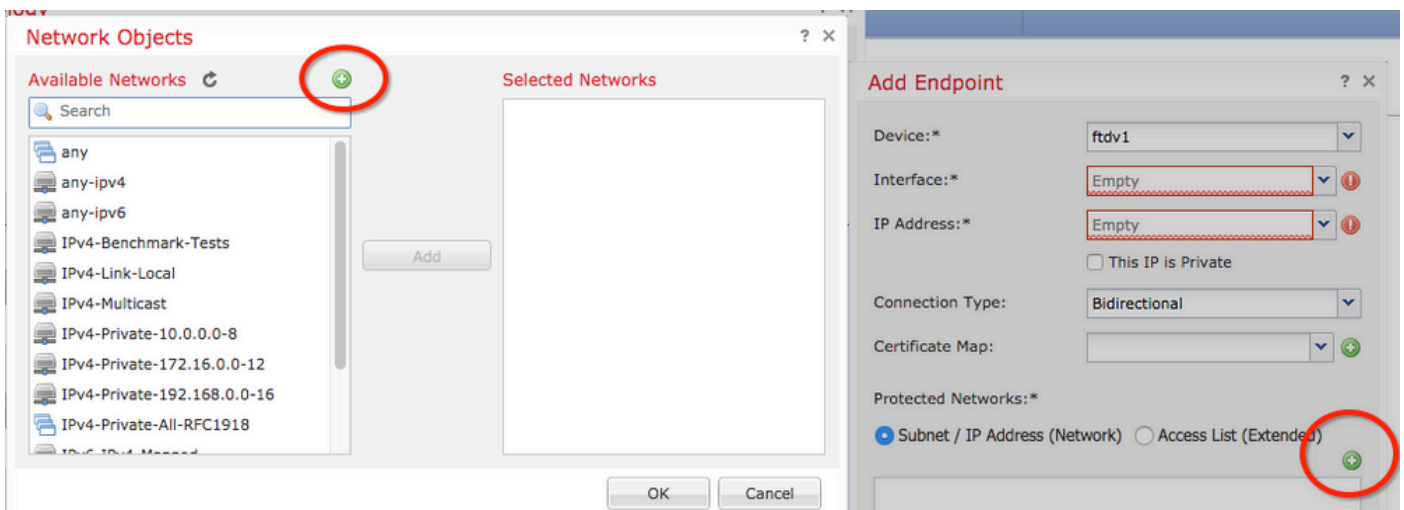
ステップ9:[Encryption Domain/Traffic Selectors/Protected Networks]を選択します。次に移動します。 Endpoints tab.Cisco IOSソフトウェア Node A セクション green plus button をクリックします。この例では、ノードAがFTDへのローカルサブネットとして使用されています。



ステップ10: Add Endpoint ウィンドウで使用するFTDを Device 使用する物理インターフェイスとIPアドレスとともにドロップダウンします。

ステップ11: ローカルトラフィックセクタを指定するには、 Protected Networks オプションを選択し、 green plus button 新しいオブジェクトを作成します。

ステップ12. Network Objects ウィンドウで、 green plus button の横に Available Networks 新しいローカルトラフィックセクタオブジェクトを作成するテキスト。



ステップ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 .

New Network Object

? X

Name: ←

Description:

Network: Host Range Network ← FQDN

←

Allow Overrides:

ステップ14 : オブジェクトを Selected Networks セクション Network Objects ウィンドウを開き、OK .クリック OK IPv6の Add Endpoint です。

Network Objects

? X

Available Networks

Search

- local-ftd ←
- any
- any-ipv4
- any-ipv6
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12
- IPv4-Private-192.168.0.0-16
- IPv4-Private-All-RFC1918

Selected Networks

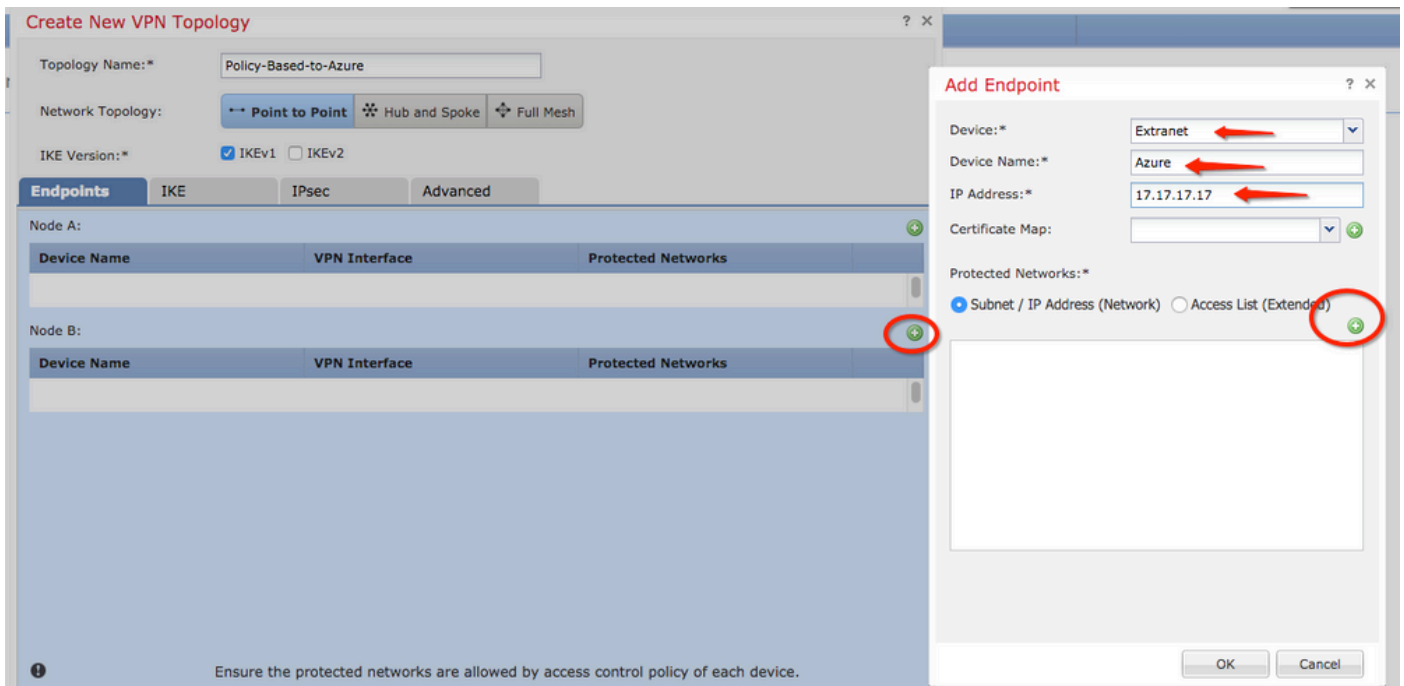
local-ftd

Add

OK

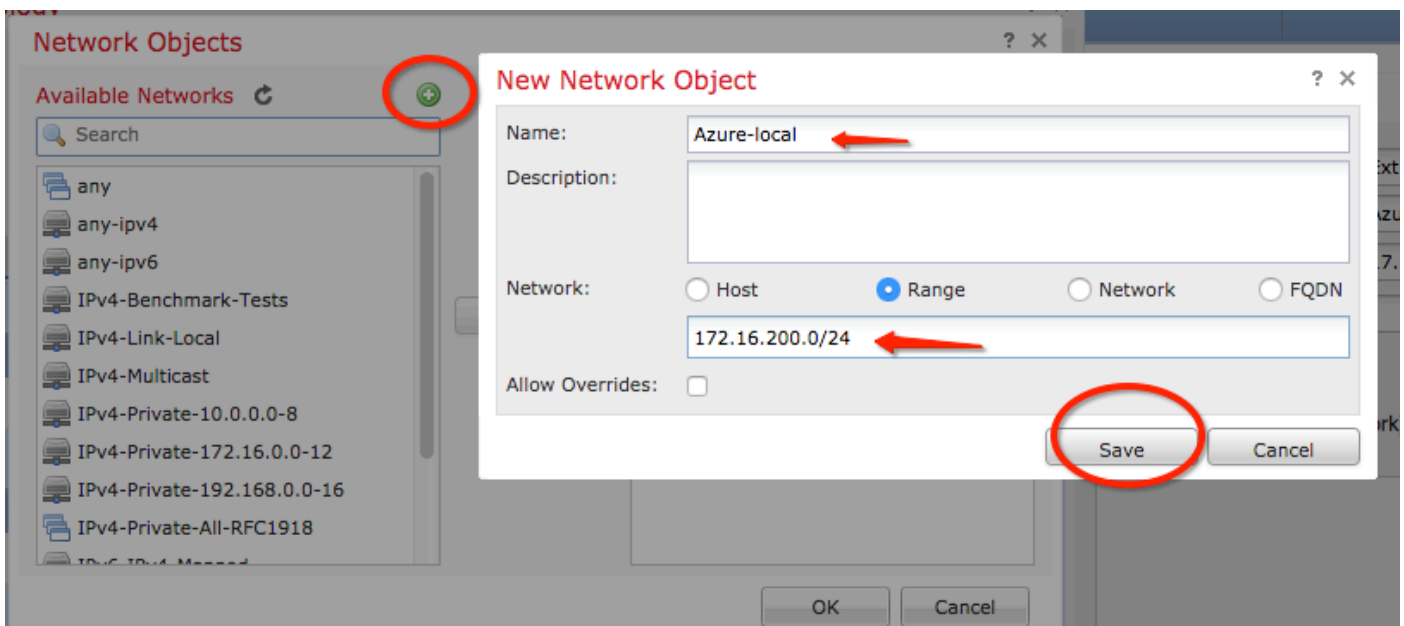
Cancel

手順15 : ノードBのエンドポイント (この例ではAzureエンドポイント) を定義します。Cisco IOSソフトウェア Create New VPN Topology ウィンドウで、 Node B セクションをクリックし、 green plus button 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。このインスタンスの Extranet 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ついて、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。

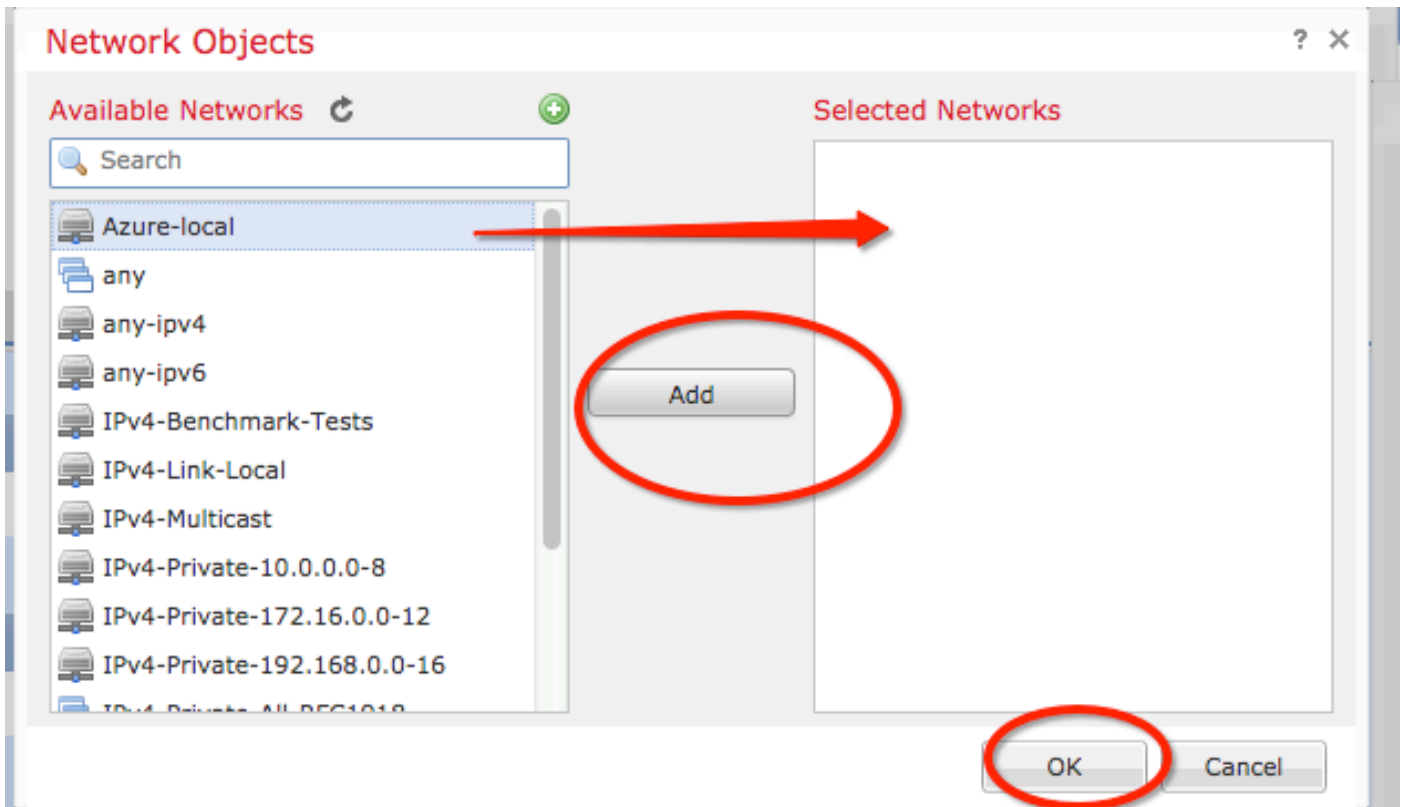


ステップ16：リモートトラフィックセクタオブジェクトを作成します。次に移動します。
Protected Networks セクションをクリックし、 green plus button 新しいオブジェクトを追加します。

ステップ17: Network Objects ウィンドウで、 green plus button の横に Available Networks 新しいオブジェクトを作成するテキスト。Cisco IOSソフトウェア 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を選択して、 Save .



ステップ18: Network Objects ウィンドウで、新しいリモートオブジェクトを Selected Networks セクションとクリック OK .クリック ok IPv6の Add Endpoint です。



ステップ19: Create New VPN Topology ウィンドウ両方のノードに正しいトラフィックセレクタと保護されたネットワークが表示されます。クリック **Save** .

Create New VPN Topology

Topology Name:*

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints | IKE | IPsec | Advanced

Node A:

Device Name	VPN Interface	Protected Networks
FTD	1.1.1.1	1.1.1.1 Private 192.168.0.0-16

Node B:

Device Name	VPN Interface	Protected Networks
Azure	17.17.17.17	Azure-local

Ensure the protected networks are allowed by access control policy of each device.

ステップ20:FMCダッシュボードで、 **Deploy** 右上のペインでFTDデバイスを選択し、 **Deploy** .

ステップ21 : コマンドラインインターフェイスでは、VPN設定はASAデバイスの設定と同じです。

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でのサイト間IKEv2 VPNの場合は、次の設定に従います。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によるこのドキュメント](#)では、UsePolicyBasedTrafficSelectorsとルートベースのAzure VPNモードの組み合わせについて説明します。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、クリプトマップを使用したASAは接続を確立できません。

暗号マップの設定情報を含む完全なASA IKEv2については、[このCiscoドキュメント](#)を参照してください。

ステップ1 : 外部インターフェイスでIKEv2を有効にします。

```
Cisco-ASA(config)#crypto ikev2 enable outside
```

手順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、および有効期間の属性に関して競合する情報を公開しています。記載されている属性は、この公開されているMicrosoftのドキュメントからベストエフォートで提供されています。競合が表示されるMicrosoftからのIKEv2属性情報。詳細については、Microsoft Azureサポートにお問い合わせください。

```
Cisco-ASA(config)#crypto ikev2 policy 1
Cisco-ASA(config-ikev2-policy)#encryption aes
Cisco-ASA(config-ikev2-policy)#integrity sha
Cisco-ASA(config-ikev2-policy)#group 2
Cisco-ASA(config-ikev2-policy)#lifetime seconds 28800
```

ステップ3:IPsec属性の下に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。

```
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
```

ステップ4:暗号化および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。この例で対象となるトラフィックは、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している場合は、このトラフィックに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。

```
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
```

ステップ5:IKEv2フェーズ2の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。記載されている属性は、この公開されているMicrosoftのドキュメントからベストエフォートで提供されています。競合が発生したMicrosoftからのフェーズ2 IPsec属性情報が表示されます。詳細については、Microsoft Azureサポートにお問い合わせください。

```
Cisco-ASA(config)#crypto ipsec ikev2 ipsec-proposal SET1
Cisco-ASA(config-ipsec-proposal)#protocol esp encryption aes
Cisco-ASA(config-ipsec-proposal)#protocol esp integrity sha-1
```

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

- ・ピアIPアドレス
- ・対象のトラフィックを含む定義済みアクセスリスト
- ・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)
- ・オプションのPFS(Perfect Forward Secrecy)設定。データを保護するために使用される新しいDiffie-Hellmanキーのペアを作成します (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が使用する特定のフェーズ2 IPsecライフタイムとPFS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、次の場所からベストエフォートで提供されます。 [この公開されているMicrosoftドキュメント](#)。

競合が発生したMicrosoftからのフェーズ2 IPsec属性情報が表示されます。詳細については、Microsoft Azureサポートにお問い合わせください。

```
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
```

ステップ8:VPNトラフィックが他のNATルールの対象に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。

```
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 no-proxy-arp route-lookup
```

注: 複数のサブネットを使用する場合は、すべての送信元および宛先サブネットを含む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。

```
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設定が完了すると、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

フェーズ1の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。

IKEv2

次に、UDPポート500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を示します。また、暗号化されたトラフィックがフローオーバーするように構築された有効な子SAもあります。

```
Cisco-ASA# show crypto ikev2 sa
```

IKEv2 SAs:

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

```
Tunnel-id Local Remote
Status Role
3208253 192.168.1.2/500 192.168.2.2/500
READY INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:5, 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、ASAを使用してピアIP 192.168.2.2に対するイニシエータとして構築され、残りのライフタイムが86388秒のIKEv1 SAを示しています。

```
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].

```
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-sha-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-sha-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つがエラーなしでIPSec SAを介して受信されます。SPI 0x9B60EDC5を持つ1つのインバウンドSAと、SPI 0x8E7A2E12を持つ1つのアウトバウンドSAが予想どおりにインストールされます。

データがトンネルを通過することを確認するには、 vpn-sessiondb l2l entries:

```
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)SHA1 IPsec: (1)SHA1
Bytes Tx : 400 Bytes Rx : 400
Login Time : 18:32:54 UTC Tue Mar 13 2018
Duration : 0h:05m:22s

バイトTx:バイトRx:IPSec SA上の送受信されたデータカウンタを表示します。

トラブルシュート

手順1:VPNのトラフィックが、Azureプライベートネットワーク宛ての内部インターフェイス上のASAで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]
```

```
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に正しく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表示されるが、Azureからの応答トラフィックが存在しない場合は、続行して理由を確認します。

ステップ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によって適切に処理され、VPNにルーティングされ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 :

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

packet-tracerの使用に関するガイドラインの詳細は、次を参照してください。

<https://community.cisco.com/443/t5/security-knowledge-base/troubleshooting-access-problems-using-packet-tracer/ta-p/3114976>

```
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=0x7f6c19250290, 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=0x7f6c19afela0, 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` が正しい場合：クリプトマップが適用されている物理インターフェイスか、仮想トンネルインターフェイスのいずれかである必要があります。

アクセスリストドロップが発生していないことを確認します。

VPNフェーズが `ENCRYPT: ALLOW` トンネルはすでに構築されており、`encaps` でインストールされた IPsec SAを確認できます。

ステップ2.1. `ENCRYPT: ALLOW packet-tracer`で確認できます。

IPsec SAがインストールされ、IPsec SAを使用してトラフィックが暗号化されていることを `show crypto ipsec sa` .

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から受信されたことを確認できます。

ステップ2.2. `ENCRYPT:DROP packet-tracer`で確認できます。

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の発生を特定します。

まず、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。

```
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. Map Tag = outside. Map Sequence Number = 10.
```

VPNトラフィックの開始時に`ike-common`デバッグ出力が表示されない場合は、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`が有効になってい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は、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`の完全なデバッグ手順と分析については、[ここ](#)を参照してください。

```
Cisco-ASA#debug crypto ikev1 127
Cisco-ASA#debug crypto ipsec 127
```

IKEv2

`ikev2`の完全なデバッグ手順と分析については、[ここ](#)を参照してください。

```
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。