配置從ASA和FTD到Microsoft Azure的基於策略和基於路由的VPN

目錄

簡介

本文檔介紹思科ASA與思科安全防火牆和Microsoft Azure雲服務之間的VPN的概念和配置。

概念

VPN加密域

IPSec允許參與VPN隧道的IP地址範圍。使用本地流量選擇器和遠端流量選擇器定義加密域，以指定IPSec捕獲和加密的本地和遠端子網範圍。定義VPN加密域的方法有兩種：基於路由或基於策略的流量選擇器。

基於路由：
加密域設定為允許任何進入IPSec隧道的流量。IPSec本地和遠端流量選擇器設定為0.0.0.0。這意味著路由到IPSec隧道的所有流量都會被加密，無論源/目標子網如何。

Cisco Adaptive Security Appliance(ASA)在9.8版及更高版本中支援使用虛擬隧道介面(VTI)的基於路由的VPN。

由FMC（Firepower管理中心）管理的Cisco安全防火牆或Firepower威脅防禦(FTD)支援使用6.7版及更高版本中的VTI的基於路由的VPN。

基於策略：

加密域設定為只加密源和目標的特定IP範圍。基於策略的本地流量選擇器和遠端流量選擇器標識要通過IPSec加密的流量。

ASA支援8.2版及更高版本中的基於策略的VPN以及加密對映。

Microsoft Azure通過模擬的基於策略的流量選擇器支援基於路由、基於策略或基於路由的流量。Azure當前限制你可以根據所選的VPN方法配置的網際網路金鑰交換(IKE)版本。基於路由需要IKEv2，基於策略需要IKEv1。這意味著如果使用IKEv2，則必須在Azure中選擇基於路由並且ASA必須使用VTI，但是如果ASA由於代碼版本而僅支援加密對映，則必須將Azure配置為使用基於策略的流量選擇器進行基於路由的流量選擇。這是通過PowerShell指令碼部署在Azure門戶中完成的，以實現Microsoft呼叫UsePolicyBasedTrafficSelectors的選項，如下所述：https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps。

要從ASA和FTD配置角度進行總結：

- 對於使用加密對映配置的ASA/FTD，必須使用UsePolicyBasedTrafficSelectors為基於策略的VPN或基於路由的Azure。
- 對於配置了VTI的ASA，必須將Azure配置為基於路由的VPN。
- 若是FTD，請在此處找到有關如何設定VTI的進一步資訊；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

必要條件

需求

思科建議您瞭解以下主題：

- 對於在ASA上使用VTI的IKEv2基於路由的VPN:ASA代碼版本9.8(1)或更高版本。（必須為基於路由的VPN配置Azure。）
- 對於在ASA和FTD上使用加密對映的IKEv1基於策略的VPN:ASA代碼版本8.2或更高版本以及FTD 6.2.0或更高版本。（必須為基於策略的VPN配置Azure。）
- 對於在具有基於策略的流量選擇器的ASA上使用加密對映的IKEv2基於路由的VPN:使用加密對映配置的ASA代碼版本8.2或更高版本。（必須使用UsePolicyBasedTrafficSelectors為基於路由的VPN配置Azure。）
- 瞭解FMC的FTD管理和配置。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

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

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

完成配置步驟。選擇配置IKEv1、使用VTI的IKEv2路由或使用基於策略的流量選擇器（ASA上的加密對映）的IKEv2路由。

ASA上的IKEv1配置

對於從ASA到Azure的站點到站點IKEv1 VPN，請執行下一個ASA配置。確保在Azure門戶中配置基於策略的隧道。在此示例中，在ASA上使用加密對映。

有關ASA配置資訊的完整IKEv1，請參閱思科文檔。

步驟1.在外部介面上啟用IKEv1。

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

步驟2.建立IKEv1策略，該策略定義用於雜湊、身份驗證、Diffie-Hellman組、生存期和加密的演算法/方法。

> **附註**：所列的第1階段IKEv1屬性是根據此公開的Microsoft文檔盡力提供的。有關進一步說明，請聯絡Microsoft Azure支援。

```
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
```

步驟3.在IPsec屬性下建立隧道組，並配置對等IP地址和隧道預共用金鑰。

```
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
```

步驟4.建立一個訪問清單，定義要加密和隧道化的流量。在本示例中，感興趣的流量是來自從10.2.2.0子網到10.1.1.0的隧道的流量。如果站點之間涉及多個子網，則該流量可以包含多個條目。

在8.4及更高版本中，可以建立用作網路、子網、主機IP地址或多個對象的容器的對象或對象組。建立兩個具有本地和遠端子網的對象，並將它們用於加密訪問控制清單(ACL)和網路地址轉換(NAT)語句。

```
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
```

步驟5.配置轉換集(TS)，其中必須包含關鍵字**IKEv1**.在遠端也必須建立相同的TS。

> **附註**：所列的第2階段IKEv1屬性是根據此公開的Microsoft文檔盡力提供的。有關進一步說明，請聯絡Microsoft Azure支援。

```
Cisco-ASA(config)#crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac
```

步驟6.配置加密對映並將其應用於具有以下元件的外部介面：
·對等IP地址
·包含相關流量的已定義存取清單
·TS
·該配置未設定完全轉發保密(PFS)，因為公開的Azure文檔說，Azure中的IKEv1已禁用PFS。可通過使用以下配置啟用可選PFS設定，該設定建立用於保護資料的新Diffie-Hellman金鑰對（在第2階段啟動之前，兩端必須啟用PFS）： **crypto map outside_map 20 set pfs .**
·設定的第2階段IPSec生命週期基於公開可用的Azure文檔。如需進一步說明，請聯絡Microsoft Azure支援。

```
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
```

步驟7.確保VPN流量不受任何其他NAT規則的約束。建立NAT豁免規則：

```
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
```

> **注意**：使用多個子網時，您必須建立包含所有源子網和目標子網的對象組，並在NAT規則中使用它們。

```
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 9.8(1)或更高版本上基於IKEv2路由的VTI

對於基於ASA代碼的站點到站點IKEv2路由VPN，請遵循以下配置。確保Azure配置為基於路由的VPN，並且不要在Azure門戶中配置UsePolicyBasedTrafficSelectors。ASA上配置了VTI。

有關完整的ASA VTI配置資訊，請參閱思科文檔。

步驟1.在外部介面上啟用IKEv2:

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

步驟2.新增IKEv2第1階段策略。

> **注意**:Microsoft發佈的資訊與Azure使用的特定IKEv2第1階段加密、完整性和生存期屬性衝突。列出的屬性是根據此公開的Microsoft文檔盡力提供的。此處將顯示與Microsoft的IKEv2屬性衝突的資訊。如需進一步說明，請聯絡Microsoft Azure支援。

```
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
```

步驟3.新增IKEv2階段2 IPsec方案。指定加密IPsec中的安全引數 **ikev2 ipsec-proposal** 配置模式：

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}
通訊協定esp完整性{md5 | sha-1 | sha-256 | sha-384 | sha-512 | null}

> **附註**：Microsoft發佈的資訊與Azure使用的特定第2階段IPSec加密和完整性屬性衝突。列出的屬性是根據此公開的Microsoft文檔盡力提供的。此處將顯示與Microsoft的第2階段IPSec屬性衝突的資訊。如需進一步說明，請聯絡Microsoft Azure支援。

```
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
```

步驟4.新增指定：

- 之前配置的ikev2第2階段IPSec建議書
- 階段2 IPSec生存期（可選）（以秒和/或千位元組為單位）
- PFS組（可選）

> **附註**：Microsoft發佈的資訊與Azure使用的特定第2階段IPSec生存期和PFS屬性衝突。列出的屬性是根據此公開的Microsoft文檔盡力提供的。此處將顯示與Microsoft的第2階段IPSec屬性衝突的資訊。如需進一步說明，請聯絡Microsoft Azure支援。

```
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
```

步驟5.在IPsec屬性下建立隧道組，並配置對等IP地址和IKEv2本地和遠端隧道預共用金鑰：

```
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
```

步驟6.建立指定：

- 新的隧道介面編號：interface tunnel [number]
- 新的隧道介面名稱：nameif [name]
- 隧道介面上不存在的IP地址：ip address [ip-address] [mask]
- VPN在本地終止的隧道源介面：tunnel source interface [int-name]
- Azure網關IP地址：隧道目標[Azure Public IP]
- IPSec IPv4模式：通道模式ipsec ipv4
- 用於此VTI的IPSec配置檔案：隧道保護ipsec配置檔案[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
```

步驟7.建立靜態路由以將流量指向隧道。要新增靜態路由，請輸入以下命令：
route if_name dest_ip mask gateway_ip [distance]

其 **dest_ip** 和 **mask** 是Azure雲中目標網路的IP地址，例如10.0.0.0/24。gateway_ip必須是隧道介面子網上的任何IP地址（存在或不存在），例如169.254.0.2。此gateway_ip的目的是將流量指向隧道介面，但特定網關IP本身並不重要。

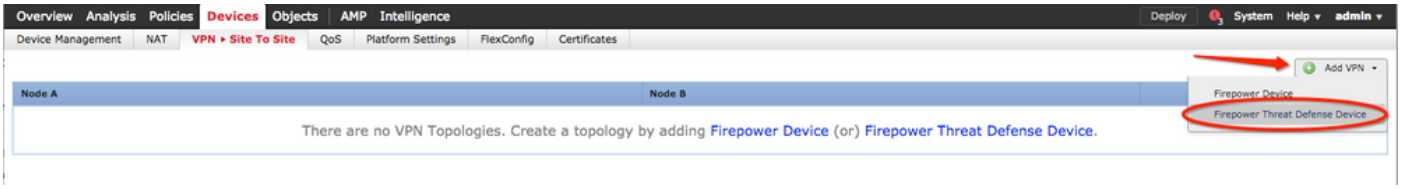
```
Cisco-ASA(config)#route vti 10.0.0.0 255.255.255.0 169.254.0.2
```

FTD上的IKEv1組態

對於從FTD到Azure的站點到站點IKEv1 VPN，您需要先將FTD裝置註冊到FMC。

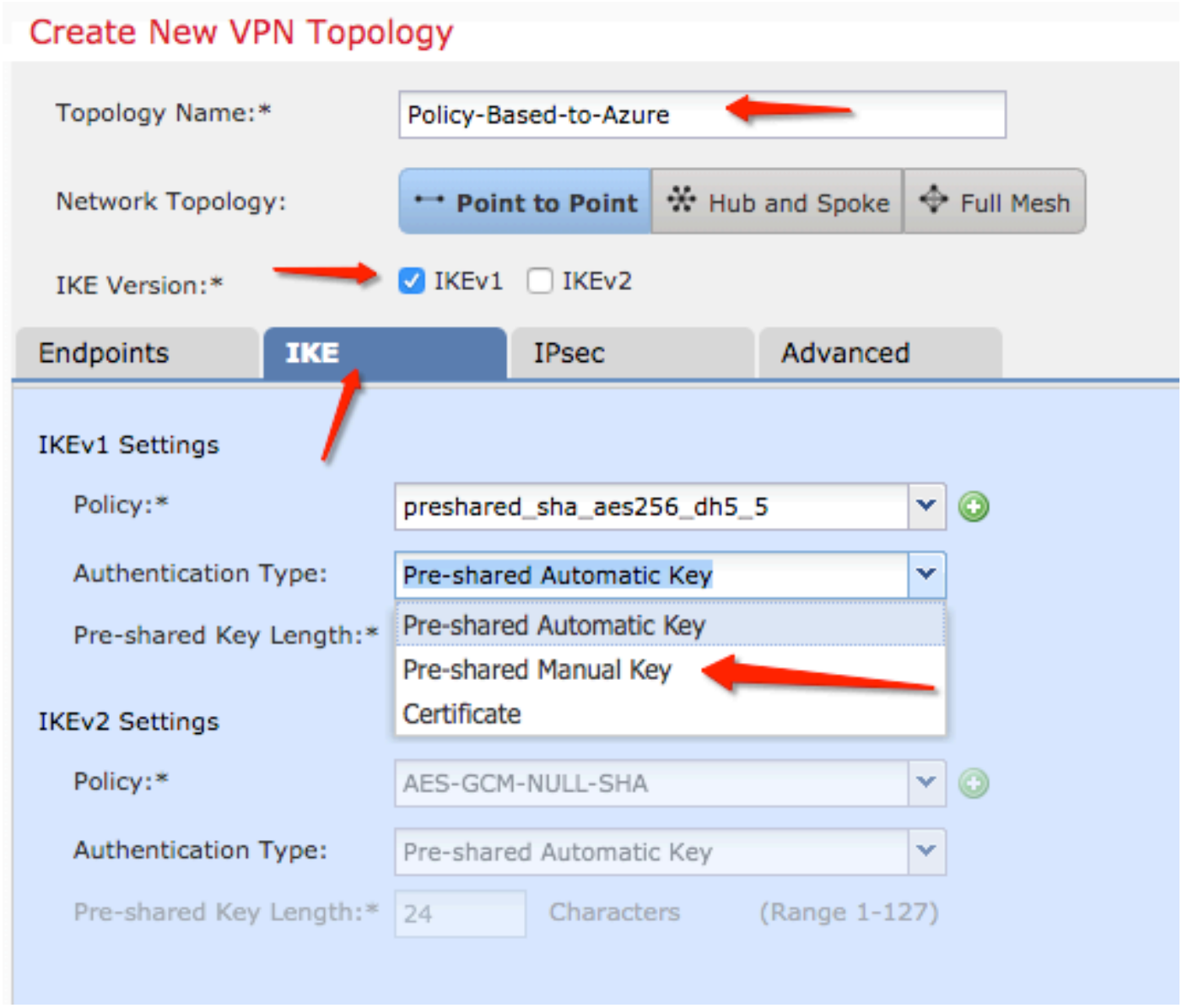
步驟1.建立站點到站點策略。導航至 **FMC dashboard > Devices > VPN > Site to Site**.

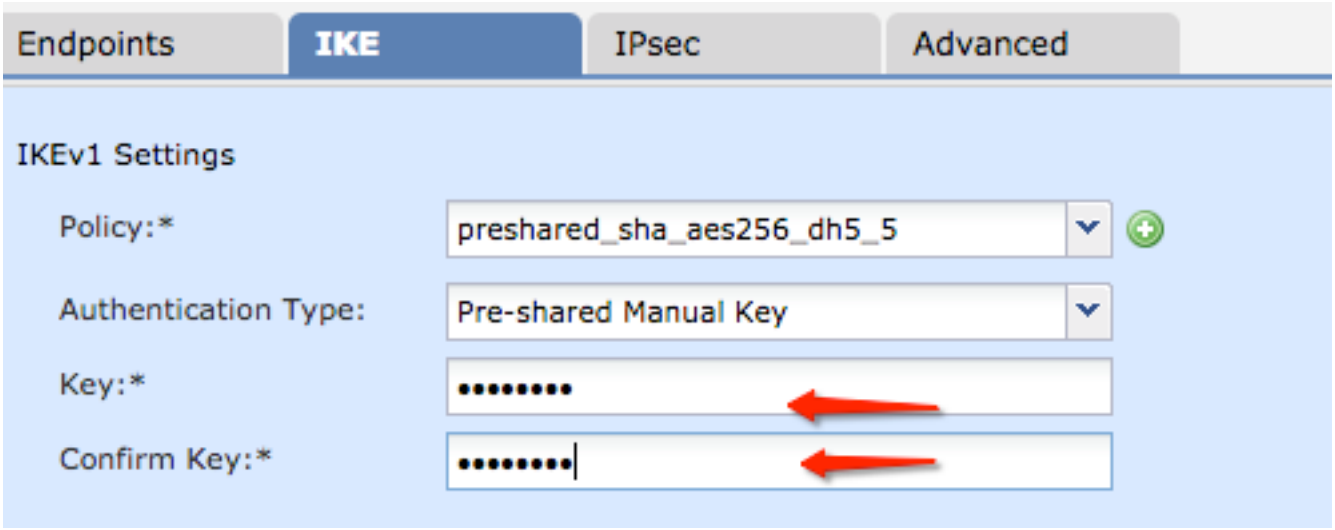
步驟2.建立新策略。按一下 **Add VPN** 下拉選單並選擇 **Firepower Threat Defense device .**



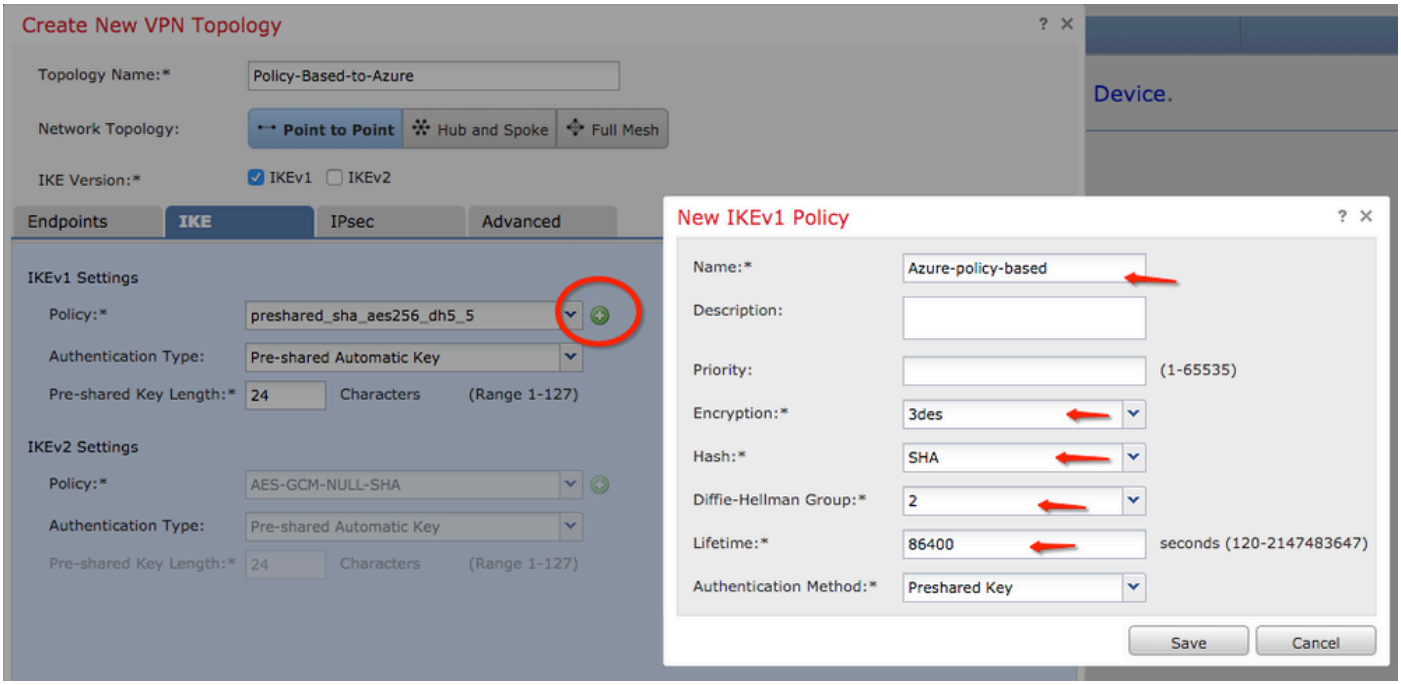
步驟3.在 **Create new VPN Topology** 視窗，指定您的 **Topology Name**，請檢視 **IKEV1** 協定覈取方塊，然後點選 **IKE** 頁籤。在本示例中，預共用金鑰用作身份驗證方法。

按一下 **Authentication Type** 下拉選單，然後選擇 **Pre-shared manual key** .在 **Key** 和**Confirm Key** 文本欄位。

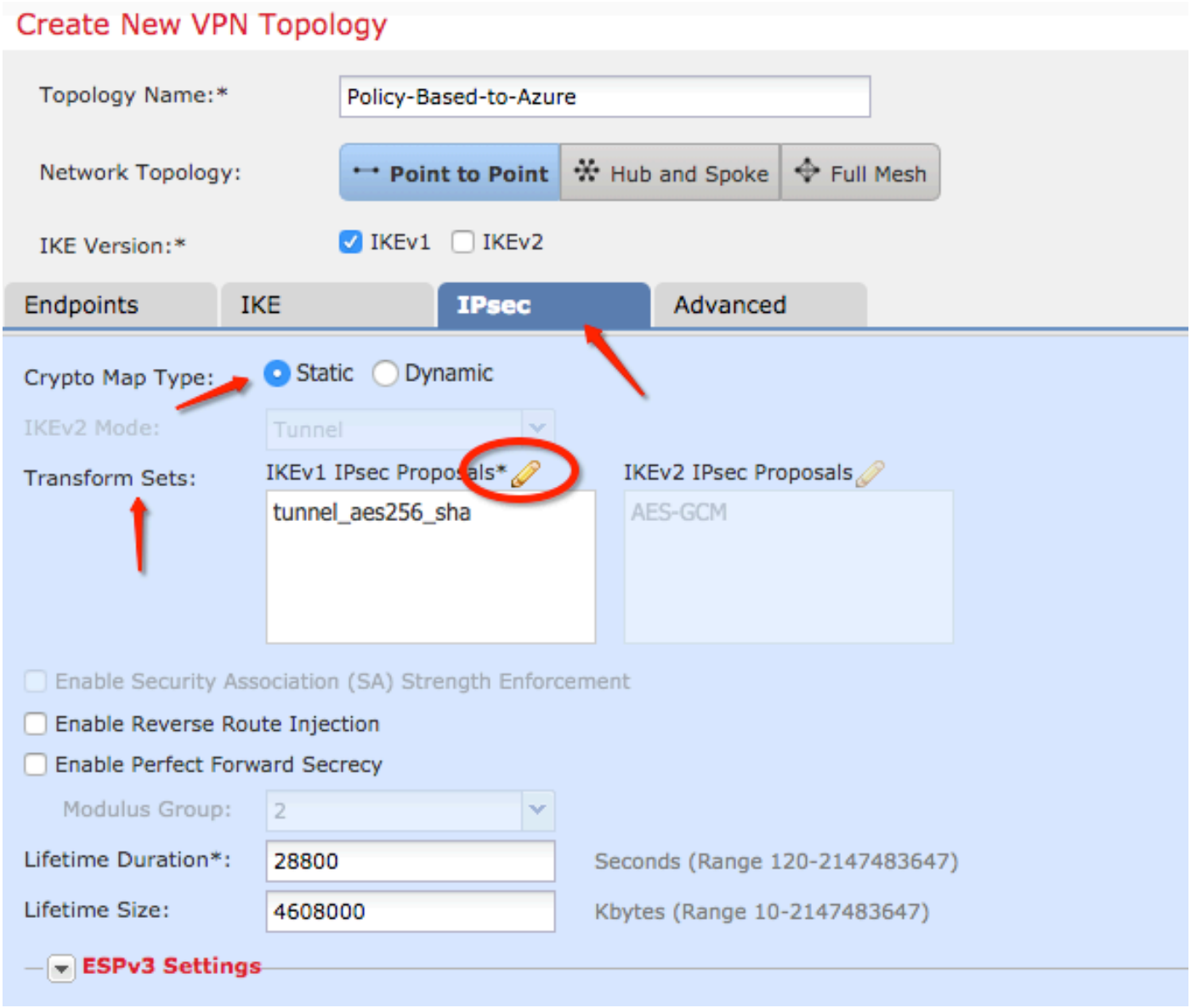




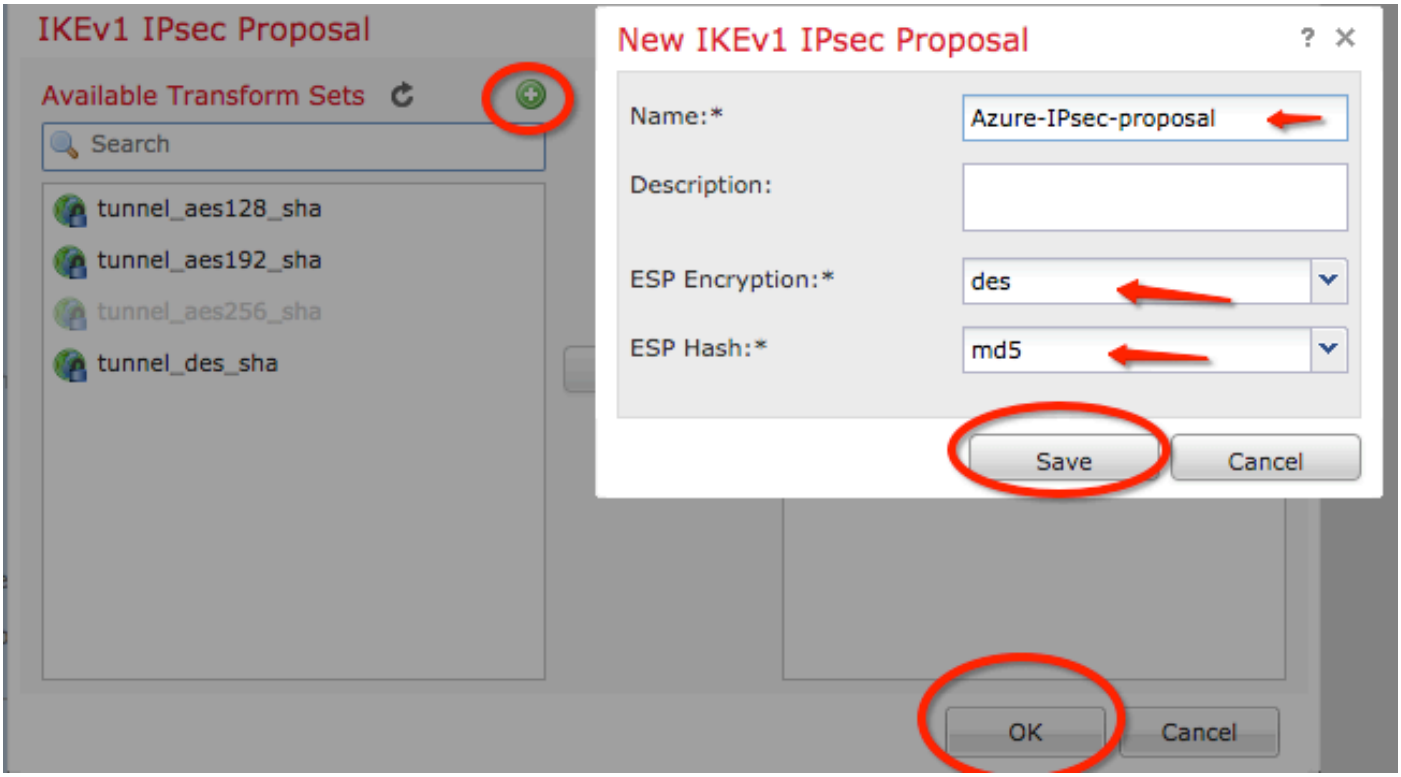
步驟4.通過建立一個新引數來配置ISAKMP策略或階段1引數。在同一視窗中，按一下 **green plus button** 新增新的ISAKMP策略。指定策略名稱並選擇所需的加密、雜湊、Diffie-Hellman組、生存期和身份驗證方法，然後按一下 **Save** .



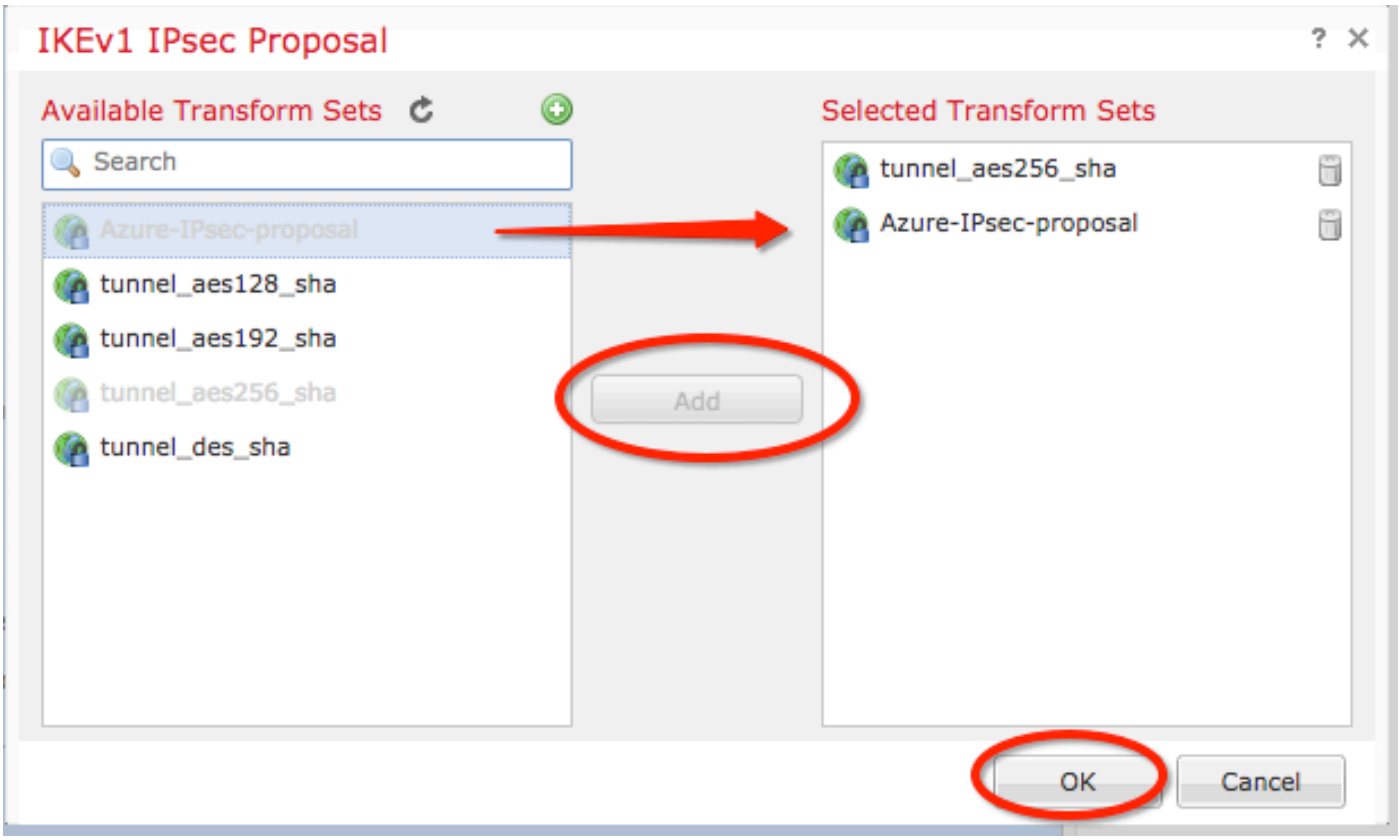
步驟5.配置IPsec策略或階段2引數。導航至 **IPsec** 頁籤，選擇 **Static** 在 **Crypto Map Type** 覈取方塊。按一下 **edit pencil** 圖示 **IKEV1 IPsec Proposals** 在 **Transform Sets** 選項。



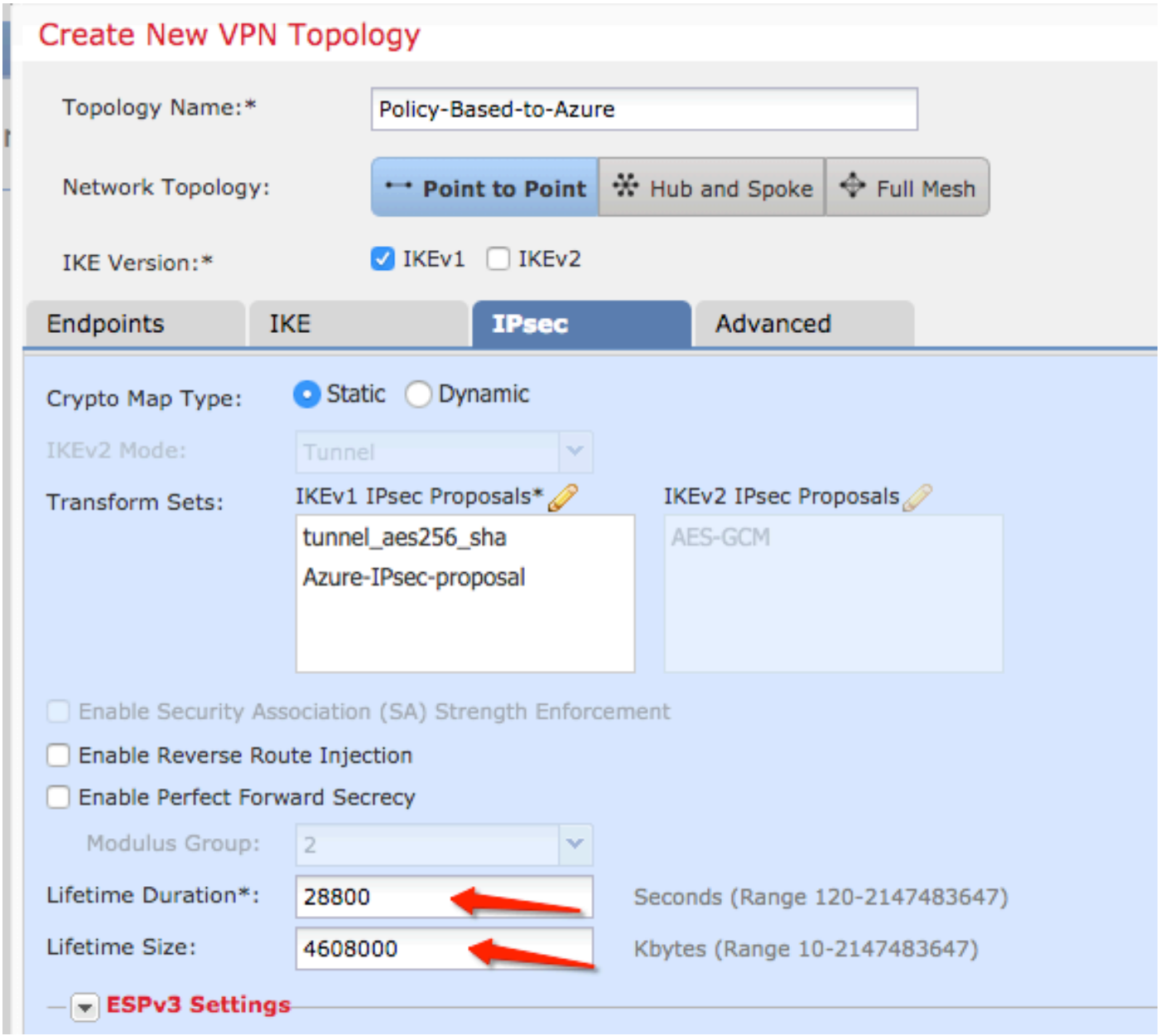
步驟6.建立新的IPsec方案。在 **IKEv1 IPSec Proposal** 視窗中，按一下 **green plus button** 以新增一個新節點。為ESP加密和ESP雜湊演算法指定策略名稱及其所需引數，然後按一下 **Save** .



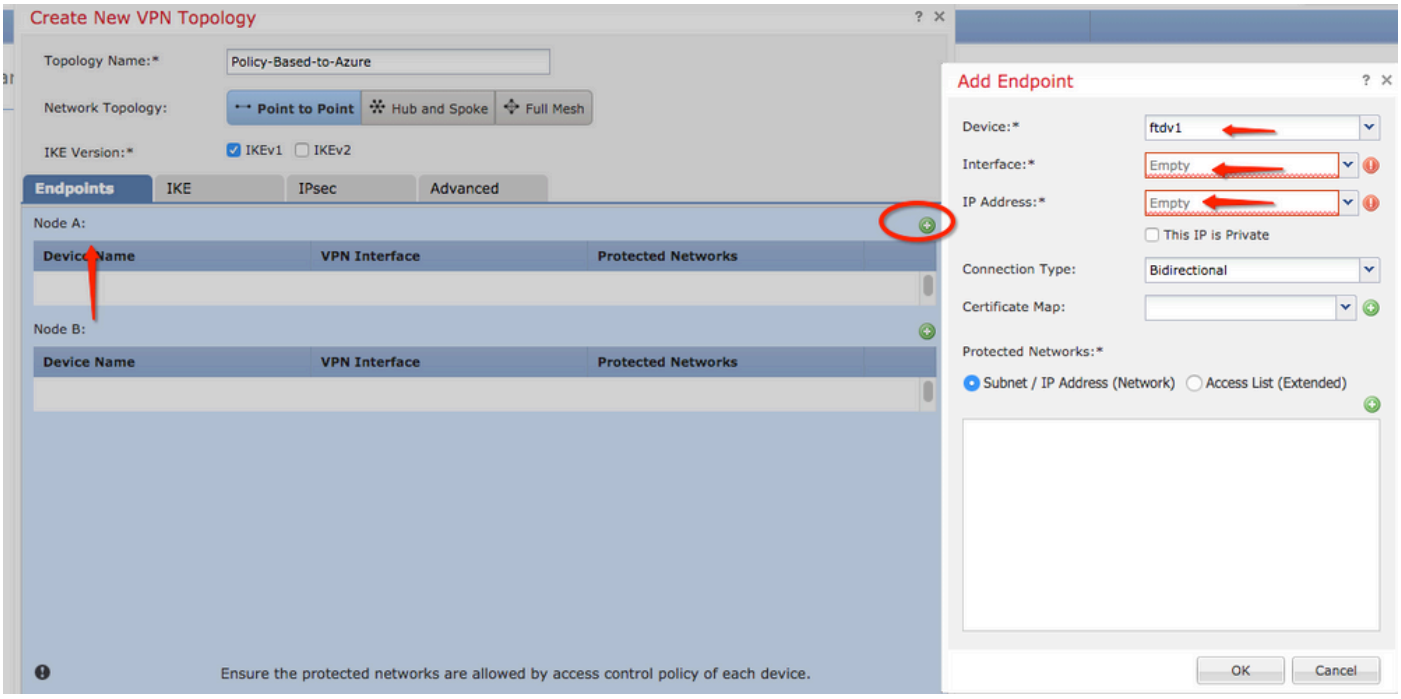
步驟7. 在 **IKEV1 IPsec Proposal** 視窗中，將新IPsec策略新增到 **Selected Transform Sets** 部分並按一下 **OK** .



步驟8.返回 **IPSec** 頁籤中，配置所需的生存期持續時間和大小。



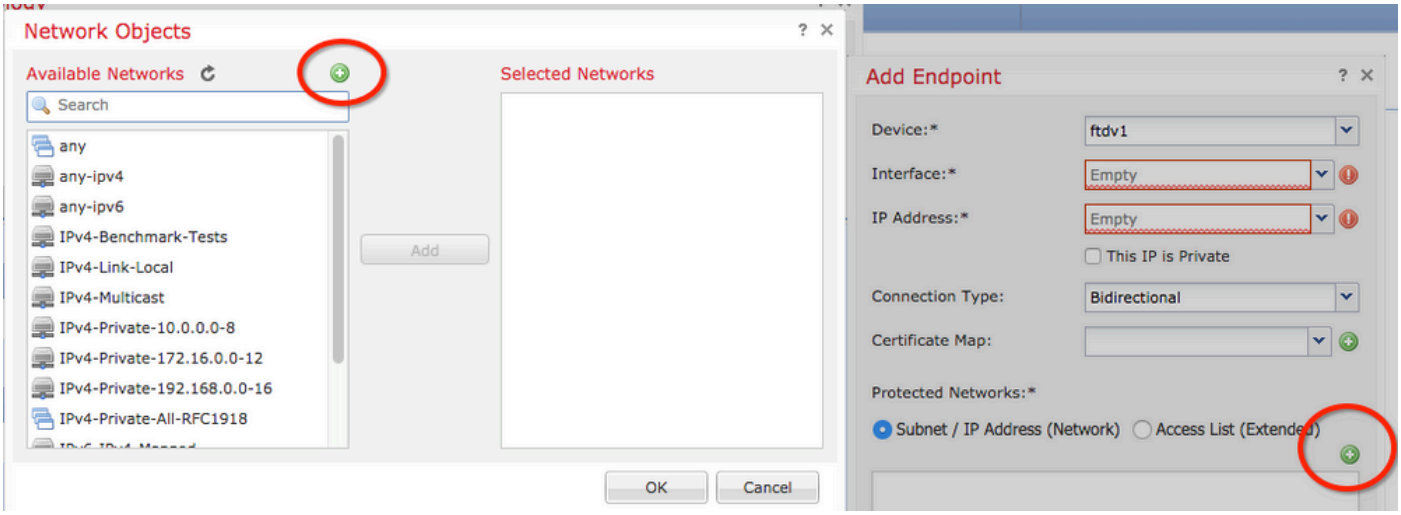
步驟9.選擇加密域/流量選擇器/受保護網路。導航至 **Endpoints** 頁籤。在 **Node A** 部分按一下 **green plus button** 以新增一個新節點。在此範例中，節點A用作FTD的本地子網。



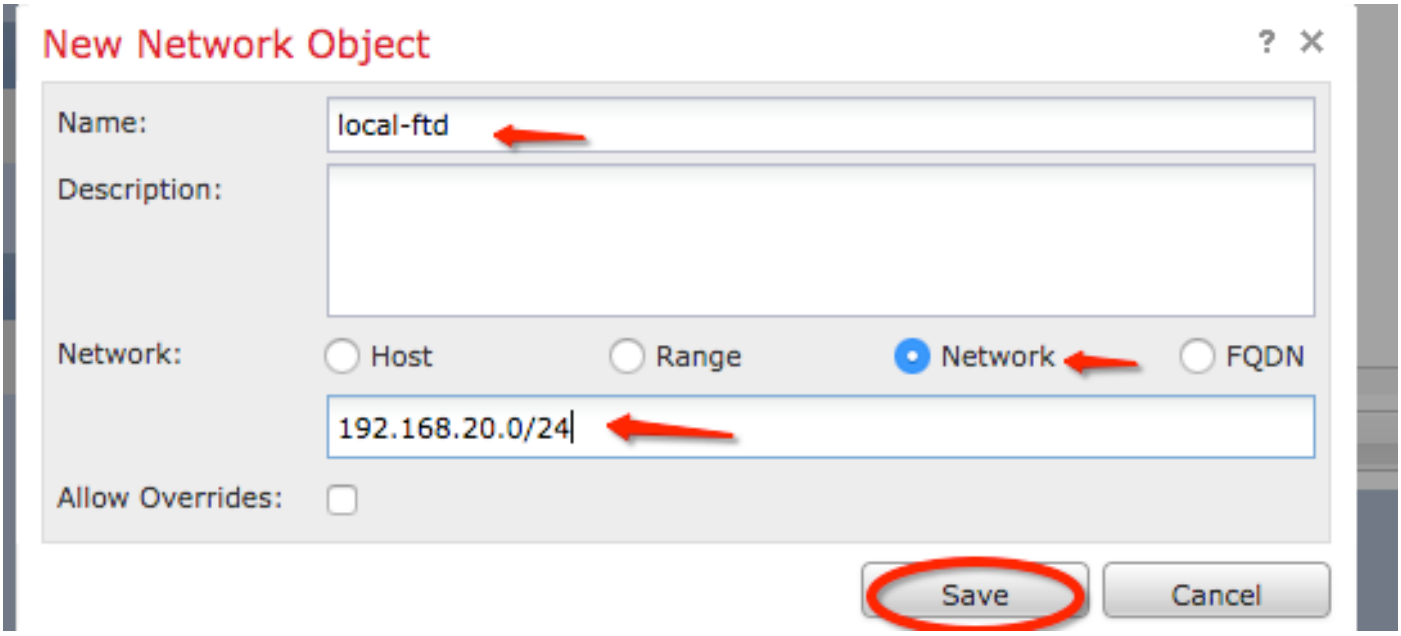
步驟10.在 **Add Endpoint** 視窗中，指定要在 **Device** 下拉選單及其要使用的物理介面和IP地址。

步驟11.要指定本地流量選擇器，請導航到 **Protected Networks** ，然後按一下 **green plus button** 建立新對象。

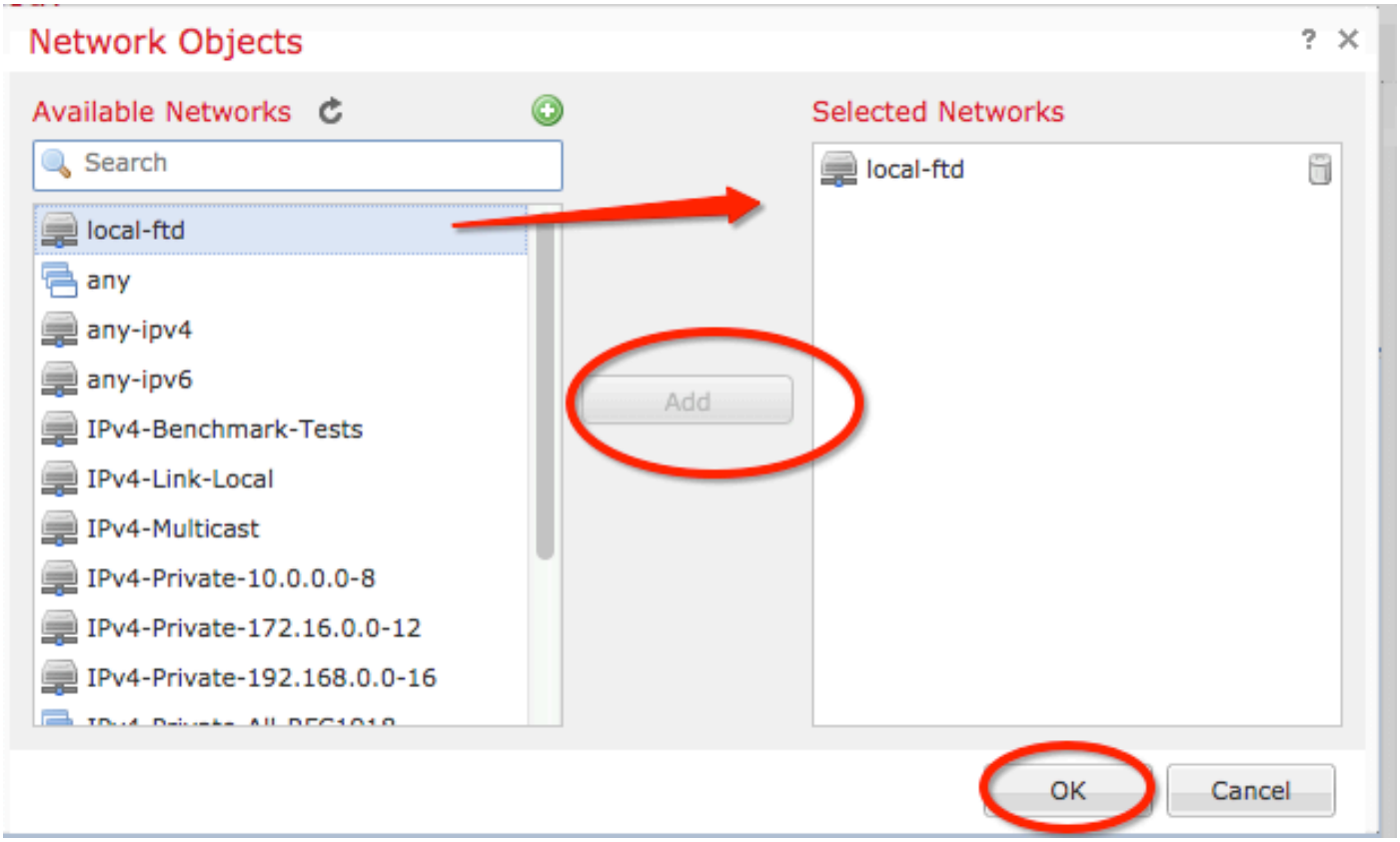
步驟12.在 **Network Objects** 視窗中，按一下 **green plus button** 在 **Available Networks** 用於建立新的本地流量選擇器對象的文本。



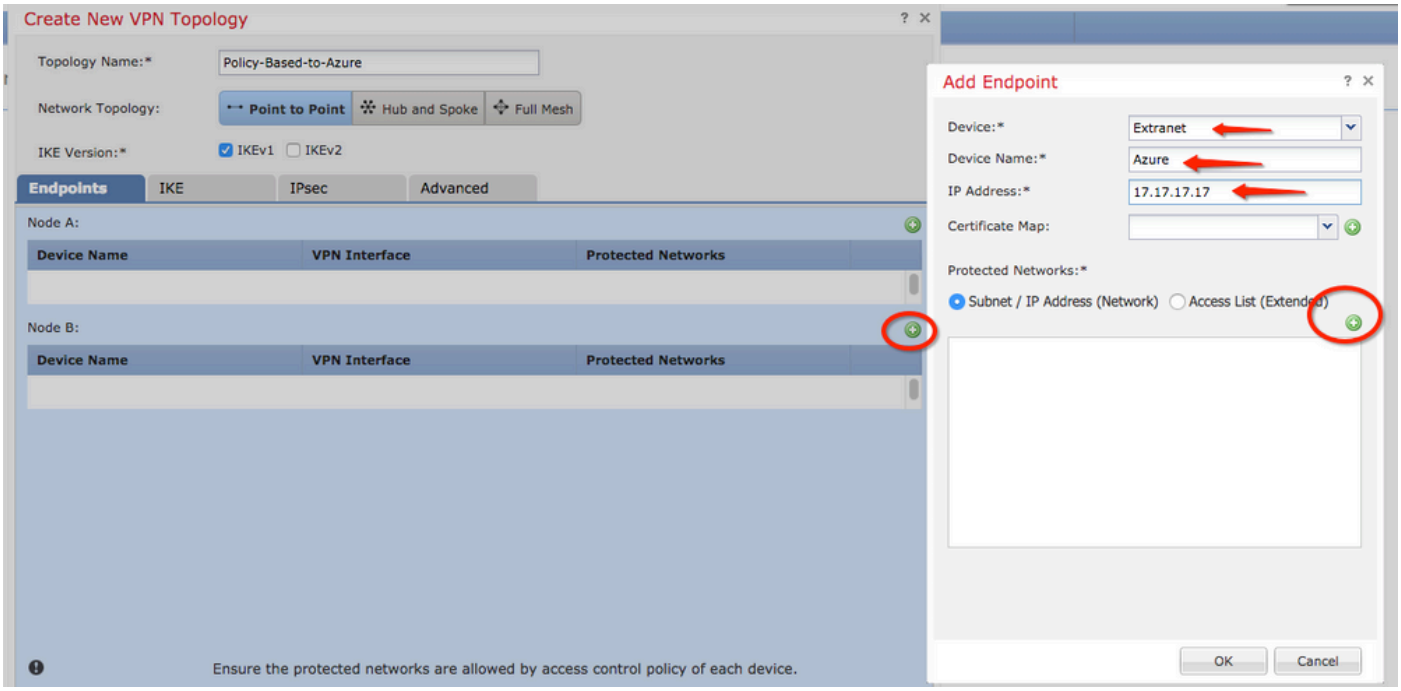
步驟13.在 **New Network Object** 視窗中，指定對象的名稱，並相應地選擇主機/網路/範圍/FQDN。然後，按一下 **Save** .



步驟14.將對象新增到 **Selected Networks** 部分 **Network Objects** 視窗並按一下 **OK** .按一下 **OK** 在 **Add Endpoint** 視窗。

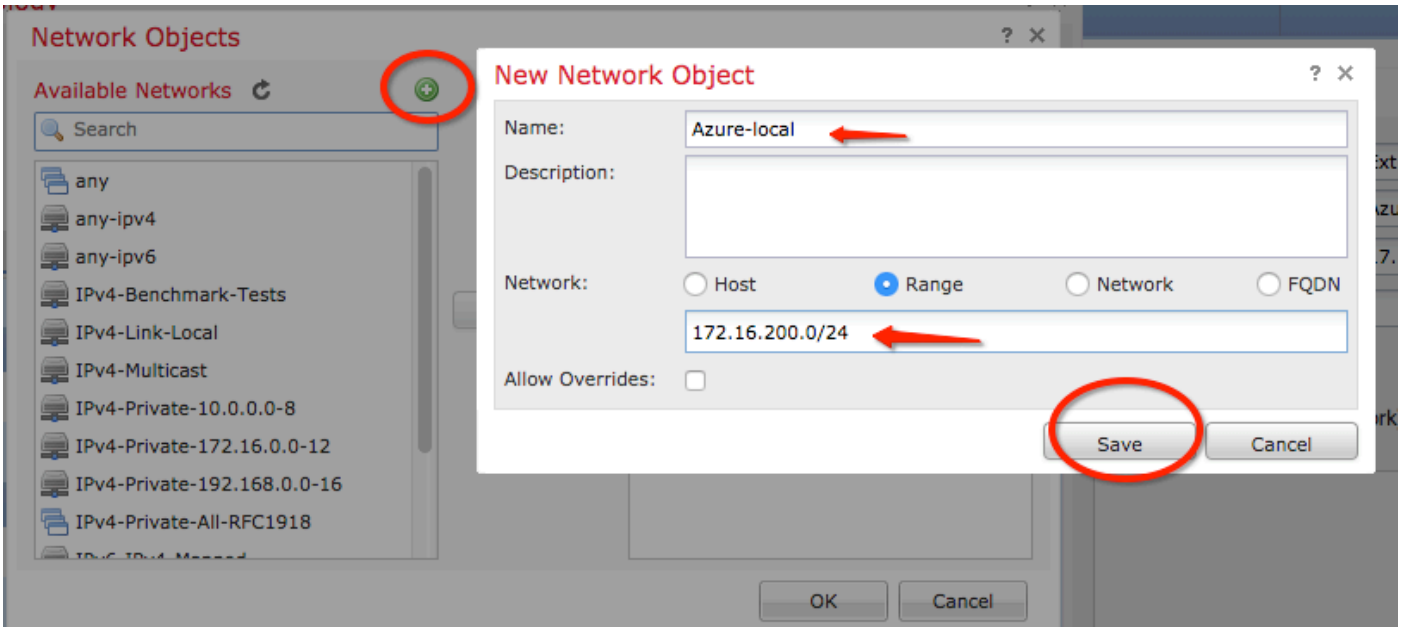


步驟15.定義節點B終結點，在此示例中，該終結點是Azure終結點。在 **Create New VPN Topology** 視窗，導航至 **Node B** ，然後按一下 **green plus button** 新增遠端終端流量選擇器。指定 **Extranet** 對於不是由與節點A相同的FMC管理的所有VPN對等端點。鍵入裝置的名稱（僅在本地有效）及其IP地址。

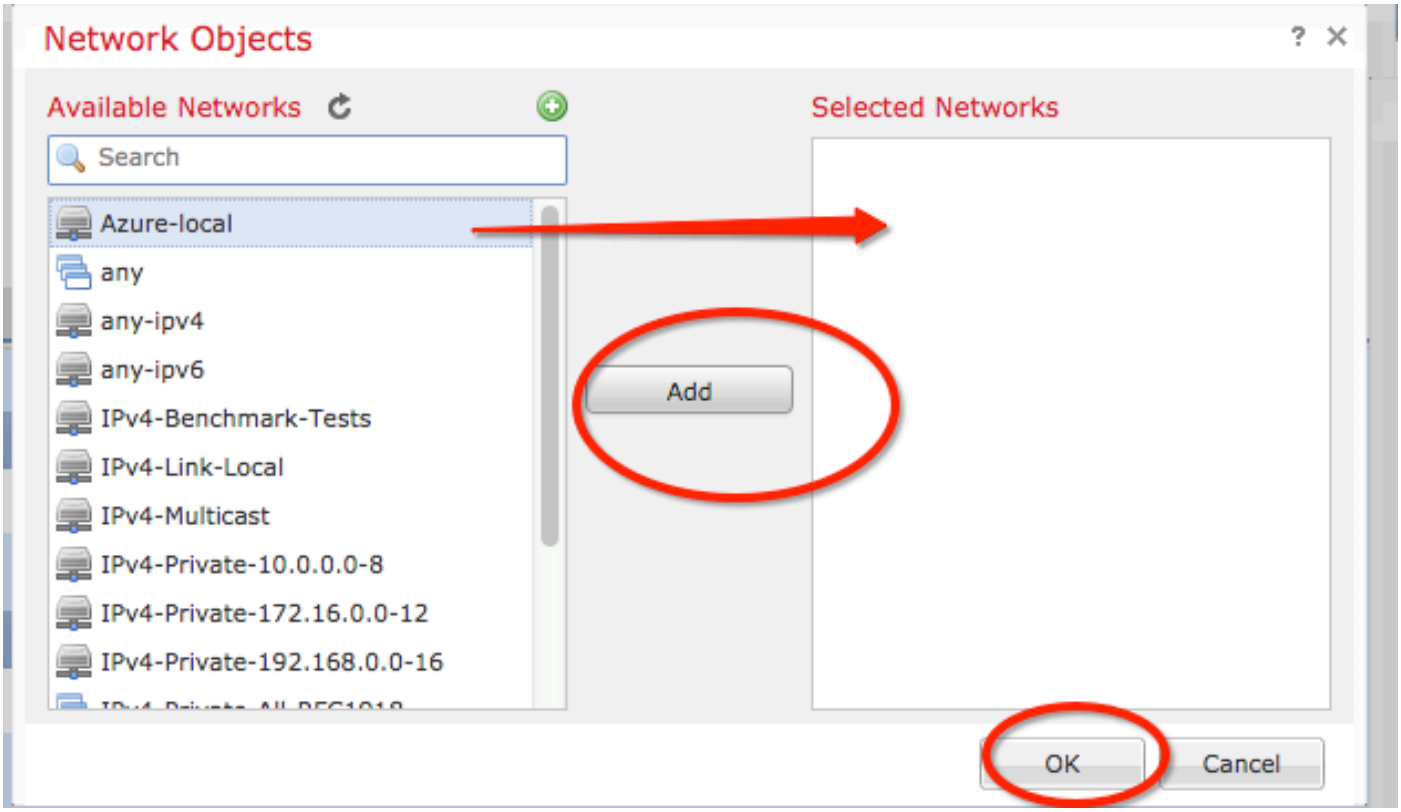


步驟16.建立遠端流量選擇器對象。導航至 **Protected Networks** ，然後按一下 **green plus button** 新增新對象。

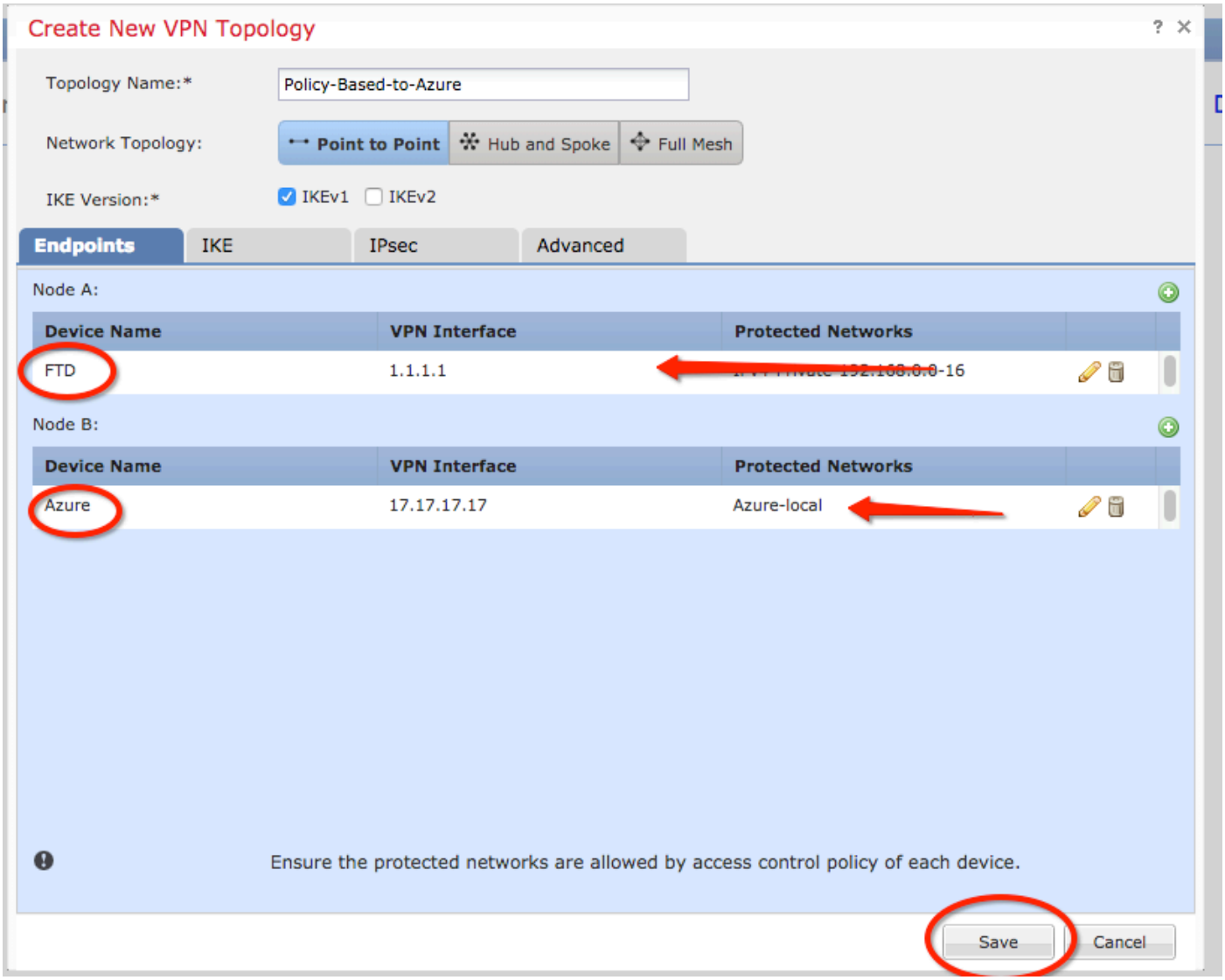
步驟17.在 **Network Objects** 視窗中，按一下 **green plus button** 在 **Available Networks** 建立新對象的文本。在 **New Network Object** 視窗中，指定對象的名稱，並相應地選擇主機/範圍/網路/FQDN，然後按一下 **Save** .



步驟18.返回 **Network Objects** 視窗，將新的遠端對象新增到 **Selected Networks** 部分並按一下 **OK** .按一下 **Ok** 在 **Add Endpoint** 視窗。



步驟19.在 **Create New VPN Topology** 視窗現在可以看到兩個節點及其正確的流量選擇器/受保護網路。按一下 **Save** .



步驟20.在FMC控制面板上，按一下 **Deploy** 在右上角窗格中，選擇FTD裝置，然後按一下 **Deploy** .

步驟21.在命令列介面上，VPN配置與ASA裝置的配置相同。

使用基於策略的流量選擇器的IKEv2基於路由

對於使用加密對映的ASA上的站點到站點IKEv2 VPN，請遵循以下配置。確保Azure配置為基於路由的VPN，並且必須使用PowerShell在Azure門戶中配置UsePolicyBasedTrafficSelector。

來自Microsoft的本文檔介紹了與基於路由的Azure VPN模式結合使用的UsePolicyBasedTrafficSelector的配置。如果不完成此步驟，由於從Azure接收的流量選擇器不匹配，具有加密對映的ASA無法建立連線。

有關完整的ASA IKEv2（包含加密對映配置資訊）的資訊，請參閱此思科文檔。

步驟1.在外部介面上啟用IKEv2:

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

步驟2.新增IKEv2第1階段策略。

注意:Microsoft發佈的資訊與Azure使用的特定IKEv2第1階段加密、完整性和生存期屬性衝突。列出的屬性是根據此公開的Microsoft文檔盡力提供的。此處可看到來自Microsoft的IKEv2屬性信息衝突。有關進一步說明，請聯絡Microsoft Azure支援。

```
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
```

步驟3.在IPsec屬性下建立隧道組，並配置對等IP地址和IKEv2本地和遠端隧道預共用金鑰：

```
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
```

步驟4.建立一個訪問清單，定義要加密和隧道化的流量。在本示例中，感興趣的流量是來自從10.2.2.0子網到10.1.1.0的隧道的流量。如果站點之間涉及多個子網，則該流量可以包含多個條目。

在8.4及更高版本中，可以建立用作網路、子網、主機IP地址或多個對象的容器的對象或對象組。建立兩個具有本地和遠端子網的對象，並將它們用於加密ACL和NAT語句。

```
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
```

步驟5.新增IKEv2階段2 IPsec建議。在加密IPsec ikev2 ipsec建議配置模式下指定安全引數：

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}
通訊協定esp完整性{md5 | sha-1 | sha-256 | sha-384 | sha-512 | null}

注意:Microsoft發佈的資訊與Azure使用的特定第2階段IPSec加密和完整性屬性衝突。列出的屬性是根據此公開的Microsoft文檔盡力提供的。Microsoft提供的第2階段IPSec屬性資訊，此處可以看到。有關進一步說明，請聯絡Microsoft Azure支援。

```
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
```

步驟6.配置加密對映並將其應用於包含以下元件的外部介面：
·對等IP地址
·包含相關流量的已定義存取清單
·IKEv2第2階段IPSec提案
·第2階段IPSec生存期（以秒為單位）

·可選的完全向前保密(PFS)設定，該設定建立一個新的Diffie-Hellman金鑰對，用於保護資料（在第2階段啟動之前，兩端必須啟用PFS）

Microsoft發佈的資訊與Azure使用的特定第2階段IPSec生存期和PFS屬性衝突。

列出的屬性盡最大努力來自 此公開的Microsoft文檔.

Microsoft提供的第2階段IPSec屬性資訊，此處可以看到。有關進一步說明，請聯絡Microsoft Azure支援。

```
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
```

步驟8.確保VPN流量不受任何其他NAT規則的約束。建立NAT豁免規則：

```
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
```

> **注意**：使用多個子網時，您必須建立包含所有源子網和目標子網的對象組，並在NAT規則中使用它們。

```
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
```

驗證

在ASA和Azure網關上完成配置後，Azure將啟動VPN隧道。您可以使用以下命令驗證通道建立是否正確：

第1階段

驗證是否已建立第1階段安全關聯(SA):

IKEv2

接下來，顯示從UDP埠500上的本地外部介面IP 192.168.1.2構建到遠端目標IP 192.168.2.2的IKEv2 SA。還有一個為加密流量流經而建立的有效子SA。

```
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
```

此處顯示的是以ASA作為發起方構建的對等IP 192.168.2.2且剩餘生存時間為86388秒的IKEv1 SA。

```
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
```

第2階段

驗證IPSec第2階段安全關聯已與 **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
```

通過IPSec SA傳送四個資料包，接收四個資料包，沒有錯誤。一個帶有SPI 0x9B60EDC5的入站SA和一個帶有SPI 0x8E7A2E12的出站SA按預期安裝。

您還可以檢查是否資料通過隧道 **vpn-sessiondb l2l** 條目：

```
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
```

位元組Tx:和Bytes Rx:顯示通過IPSec SA傳送和接收的資料計數器。

疑難排解

步驟1.驗證ASA在發往Azure專用網路的內部介面上接收到VPN流量。要測試，您可以從內部客戶端配置連續ping，並在ASA上配置資料包捕獲以驗證是否收到該資料包：

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
```

如果看到來自Azure的回覆流量，則正確構建VPN並傳送/接收流量。

如果源流量不存在，請驗證您的傳送者是否正確路由到ASA。

如果發現源流量，但來自Azure的回覆流量不存在，則繼續驗證原因。

步驟2.驗證ASA內部介面上接收的流量是否正確由ASA處理並路由到VPN:

模擬ICMP回應請求：
packet-tracer input [inside-interface-name] icmp [inside-host-ip] 8 0 [azure-host-ip] detail

完整的Packet Tracer使用指南可在此處找到：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=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
```

請注意，NAT將免除流量（無轉換生效）。 驗證VPN流量上是否未進行NAT轉換。

此外，請驗證 **output-interface** 正確 — 它必須是應用加密對映的物理介面或虛擬隧道介面。

確保未看到任何存取清單捨棄專案。

如果VPN階段顯示 **ENCRYPT: ALLOW** 中，隧道已構建，您可以看到安裝了encaps的IPSec SA。

步驟2.1.如果 **ENCRYPT: ALLOW** 可在packet tracer中看到。

驗證是否已安裝IPsec SA並使用 **show crypto ipsec sa** .

您可以在外部介面上執行捕獲，以驗證加密資料包是從ASA傳送的，還是從Azure接收加密響應。

步驟2.2.如果 **ENCRYPT:DROP** 可在packet tracer中看到。

VPN隧道尚未建立，但正在協商。這是您首次開啟通道時的預期情況。運行debugs以檢視隧道協商過程並確定故障發生位置和原因。

首先，驗證觸發的IKE版本是否正確以及ike通用進程是否顯示相關錯誤：

```
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.
```

如果在啟動VPN流量時未看到ike-common調試輸出，則這意味著流量在到達加密進程之前被丟棄，或者該盒上未啟用加密ikev1/ikev2。仔細檢查加密配置和資料包丟棄。

如果ike-common調試顯示已觸發加密進程，請調試IKE配置的版本以檢視隧道協商消息並確定使用Azure構建隧道時失敗的位置。

IKEv1

可以在此處找到完整的ikev1調試過程和分析。

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

IKEv2

可以在此處找到完整的ikev2調試過程和分析。

```
Cisco-ASA#debug crypto ikev2 platform 127
Cisco-ASA#debug crypto ikev2 protocol 127
Cisco-ASA#debug crypto ipsec 127
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。