配置从ASA和FTD到MS Azure的基于策略和路由的VPN

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- 概念
  - VPN加密域

配置

- ASA上的IKEv1配置
- 基于IKEv2路由且在ASA代码9.8(1)或更高版本上具有VTI
- FTD上的IKEv1配置
- 使用基于策略的流量选择器的IKEv2基于路由

验证

- 第 1 阶段
- 第 2 阶段

故障排除

- IKEv1
- IKEv2

简介

本文档介绍思科ASA与思科安全防火墙和Microsoft Azure云服务之间的VPN的概念和配置。

先决条件

要求

Cisco 建议您了解以下主题：

- 对于在ASA上使用VTI的IKEv2基于路由的VPN:ASA代码版本9.8(1)或更高版本（必须为基于路由的VPN配置Azure。）

- 对于ASA和FTD上使用加密映射的基于IKEv1策略的VPN:ASA代码版本8.2或更高版本以及FTD 6.2.0或更高版本（必须为基于策略的VPN配置Azure。）
- 对于在具有基于策略的流量选择器的ASA上使用加密映射的IKEv2基于路由的VPN:使用加密映射配置ASA代码版本8.2或更高版本（必须使用UsePolicyBasedTrafficSelectors为基于路由的VPN配置Azure。）
- 了解FMC的FTD管理和配置。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科FTD
- 思科FMC
- Microsoft Azure
- 运行ASA 9.18.4.22的Cisco ASAv

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

概念

VPN加密域

使用IPSec的IP地址范围允许其参与VPN隧道。使用本地流量和远程流量选择器定义加密域，以指定IPSec捕获和加密的本地和远程子网范围。

定义VPN加密域有两种方法：基于路由或基于策略的流量选择器：

基于路由：
加密域设置为允许任何进入IPSec隧道的流量。IPSec本地和远程流量选择器设置为0.0.0.0。这意味着任何路由到IPSec隧道的流量都会被加密，而不考虑源/目标子网。

思科自适应安全设备(ASA)支持使用版本9.8及更高版本中的虚拟隧道接口(VTI)的基于路由的VPN。

由Firepower管理中心(FMC)管理的思科安全防火墙或Firepower威胁防御(FTD)支持使用版本6.7及更高版本的VTI的基于路由的VPN。

基于策略：

加密域设置为只加密源和目标的特定IP范围。基于策略的本地流量选择器和远程流量选择器标识要通过IPSec加密的流量。

ASA支持8.2版及更高版本中带加密映射的基于策略的VPN。

Microsoft Azure通过模拟的基于策略的流量选择器支持基于路由、基于策略或基于路由的流量。Azure当前限制您可以根据VPN所选方法配置的Internet密钥交换(IKE)版本。基于路由需要IKEv2，基于策略需要IKEv1。如果使用IKEv2，则必须选择Azure中基于路由且ASA必须使用VTI。

如果ASA由于代码版本而仅支持加密映射，则必须使用基于策略的流量选择器将Azure配置为基于路由。这在Azure门户中通过PowerShell脚本部署完成，以实现Microsoft调用UsePolicyBasedTrafficSelectors的选项，您可以参考该选项：将VPN网关连接到多个本地基于策略的VPN设备。

要从ASA和FTD配置角度进行总结，请执行以下操作：

- 对于配置了VTI的ASA，必须为基于路由的VPN配置Azure。
- 对于FTD，有关如何配置VTI的详细信息，请访问此处；Firepower管理中心配置指南，版本6.7
- 对于使用加密映射配置的ASA/FTD，必须使用UsePolicyBasedTrafficSelectors为基于策略的VPN或基于路由的Azure进行配置。

配置

完成配置步骤。选择配置IKEv1、使用VTI的IKEv2路由或使用基于策略的流量选择器的IKEv2路由（ASA上的加密映射）。

ASA上的IKEv1配置

对于从ASA到Azure的站点到站点IKEv1 VPN，实施下一个ASA配置。确保在Azure门户中配置基于策略的隧道。在本示例中，加密映射用于ASA。

参考在ASAv上使用ASDM或CLI配置IKEv1 IPsec站点到站点隧道，以获取ASA配置信息的完整IKEv1。

1.在外部接口上启用IKEv1。

<#root>

```
Cisco-ASA(config)#

crypto ikev1 enable outside
```

2.创建IKEv1策略，该策略定义用于散列、身份验证、Diffie-Hellman组、生存期和加密的算法/方法。

注意：列出的第1阶段IKEv1属性来自VPN设备和站点到站点VPN网关连接的IPsec/IKE参数。有关进一步说明，请联系Microsoft Azure支持。

<#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.在IPsec属性下创建隧道组，并配置对等IP地址和隧道预共享密钥。

```
<#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.创建访问列表，定义要加密和隧道化的流量。

在本例中，相关流量来自从10.2.2.0子网到10.1.1.0的隧道。如果站点之间涉及多个子网，则该流量可以包含多个条目。

在版本8.4及更高版本中，可以创建用作网络、子网、主机IP地址或多个对象的容器的对象或对象组。创建两个具有本地和远程子网的对象，并将它们同时用于加密访问控制列表(ACL)和网络地址转换(NAT)语句。

<#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.配置转换集(TS)，该转换集必须包含关键字IKEv1。在远程端也必须创建相同的TS。

注意：可以从站点到站点VPN网关连接的VPN设备和IPsec/IKE参数中引用列出的第2阶段IKEv1属性。有关进一步说明，请联系Microsoft Azure支持。

<#root>

```
Cisco-ASA(config)#

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

步骤6.配置加密映射并将其应用到外部接口，外部接口具有以下组件：

- TS。
- 对等IP地址。
- 包含相关流量的已定义访问列表。

- 配置未设置完全转发保密(PFS)。站点到站点VPN网关连接的VPN设备和IPsec/IKE参数状态在Azure中对IKEv1禁用PFS。

可选的PFS设置创建用于保护数据的新Diffie-Hellman密钥对（在第2阶段启动之前，两端必须启用PFS。）可以通过运行此命令启用此设置：crypto map outside_map 20 set pfs。

- 第2阶段IPSec生命期设置基于站点到站点VPN网关连接的VPN设备和IPsec/IKE参数。有关进一步说明，请联系Microsoft Azure支持。

<#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.确保VPN流量不受任何其他NAT规则的约束。创建NAT免除规则:

<#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
```

注意：当使用多个子网时，您必须创建包含所有源和目标子网的对象组，并在NAT规则中使用它们。

```
<#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
```

基于IKEv2路由且在ASA代码9.8(1)或更高版本上具有VTI

对于基于ASA代码的站点到站点IKEv2路由VPN，请使用此配置。确保Azure已配置为基于路由的VPN，并且未在Azure门户中配置UsePolicyBasedTrafficSelectors。ASA上配置了VTI。

参考CLI手册3:Cisco ASA系列VPN CLI配置指南9.8,获取完整的ASA VTI配置信息。

1.在外部接口上启用IKEv2:

```
<#root>

Cisco-ASA(config)#

crypto ikev2 enable outside
```

2.添加IKEv2第1阶段策略。

> 注意:Microsoft发布的信息与Azure使用的特定IKEv2第1阶段加密、完整性和生命周期属性冲突。列出的属性来自VPN设备和站点到站点VPN网关连接的IPsec/IKE参数。与Microsoft的IKEv2属性冲突的信息是Sample Configuration:Cisco ASA设备（IKEv2/无BGP）。 有关进一步说明，请联系Microsoft Azure支持。

```
<#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.添加IKEv2第2阶段IPsec提议。在crypto IPsec ikev2 ipsec-proposal配置模式下指定安全参数：

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}



注意：Microsoft发布的信息与Azure使用的特定第2阶段IPSec加密和完整性属性冲突。列出的属性来自VPN设备和站点到站点VPN网关连接的IPsec/IKE参数。与Microsoft的第2阶段IPSec属性冲突的信息是Sample Configuration:Cisco ASA设备（IKEv2/无BGP）。 有关进一步说明，请联系Microsoft Azure支持。

```
<#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.添加指定以下内容的IPSec配置文件：

- 之前配置的ikev2第2阶段IPSec提议。
- 第2阶段IPSec生命期（可选）（以秒和/或千字节为单位）。
- PFS组（可选）

注意：Microsoft发布的信息与Azure使用的特定第2阶段IPSec生命周期和PFS属性冲突。列出的属性来自基于路由的VPN IPsec安全关联（IKE快速模式SA）产品。与Microsoft的第2阶段IPSec属性冲突的信息是Sample Configuration:Cisco ASA设备（IKEv2/无BGP）。 有关进一步说明，请联系Microsoft Azure支持。

<#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.在IPsec属性下创建隧道组，并配置对等IP地址和IKEv2本地和远程隧道预共享密钥：

<#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.创建指定以下内容的VTI:

- 新的隧道接口编号：interface tunnel [number]
- 新的隧道接口名称：nameif [name]
- 隧道接口上不存在的IP地址：ip address [ip-address] [mask]
- VPN在本地终止的隧道源接口：tunnel source interface [int-name]
- Azure网关IP地址：隧道目标[Azure Public IP]
- IPSec IPv4模式隧道模式IPSec IPv4
- 用于此VTI的IPSec配置文件：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.创建将流量指向隧道的静态路由。要添加静态路由，请运行以下命令：
route if_name dest_ip mask gateway_ip [distance]

dest_ip和mask是Azure云中目标网络的IP地址，例如10.0.0.0/24。gateway_ip必须是隧道接口子网上的任何IP地址（存在或不存在），例如169.254.0.2。此gateway_ip的目的是将流量指向隧道接口，但是，特定网关IP本身并不重要。

```
<#root>

Cisco-ASA(config)#

route vti 10.0.0.0 255.255.255.0 169.254.0.2
```

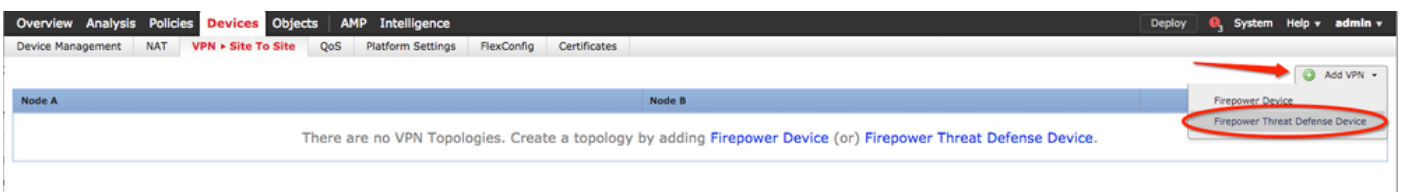
FTD上的IKEv1配置

对于从FTD到Azure的站点到站点IKEv1 VPN，您必须事先将FTD设备注册到FMC。

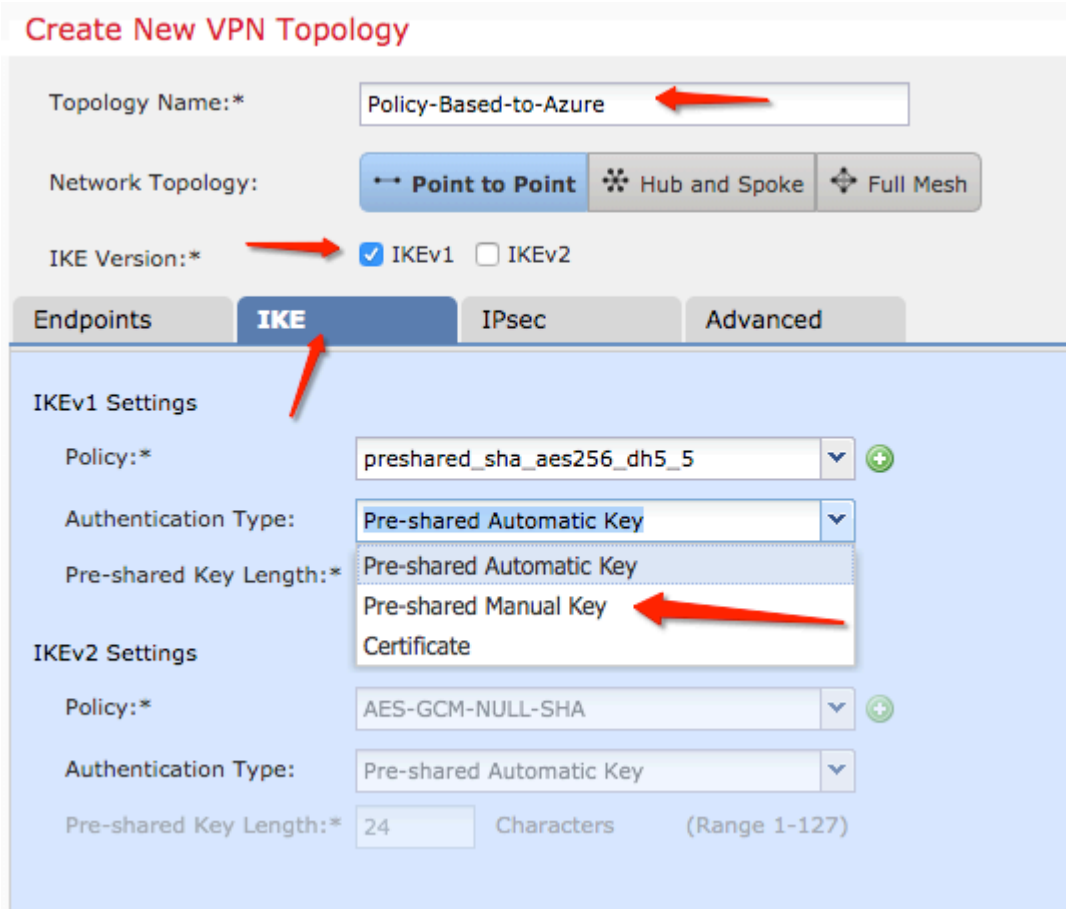
1.创建站点到站点策略。导航到FMC控制面板>设备> VPN >站点到站点.

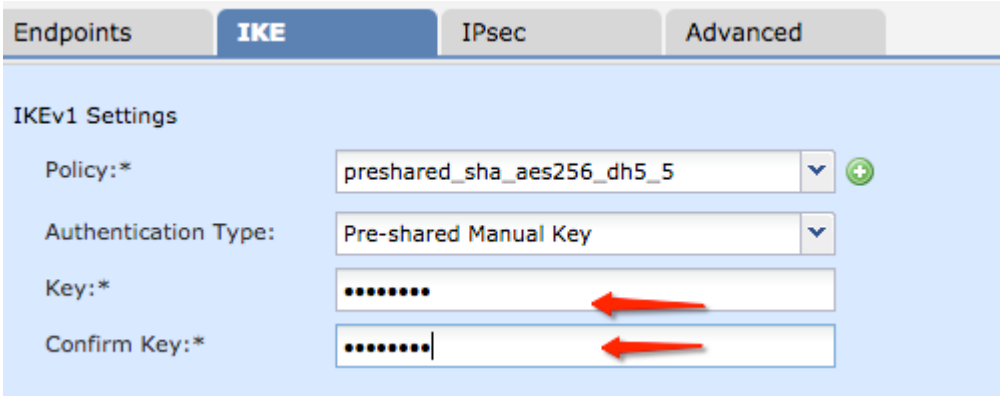


2.创建新策略。单击Add VPN下拉菜单，然后选择Firepower Threat Defense Device。

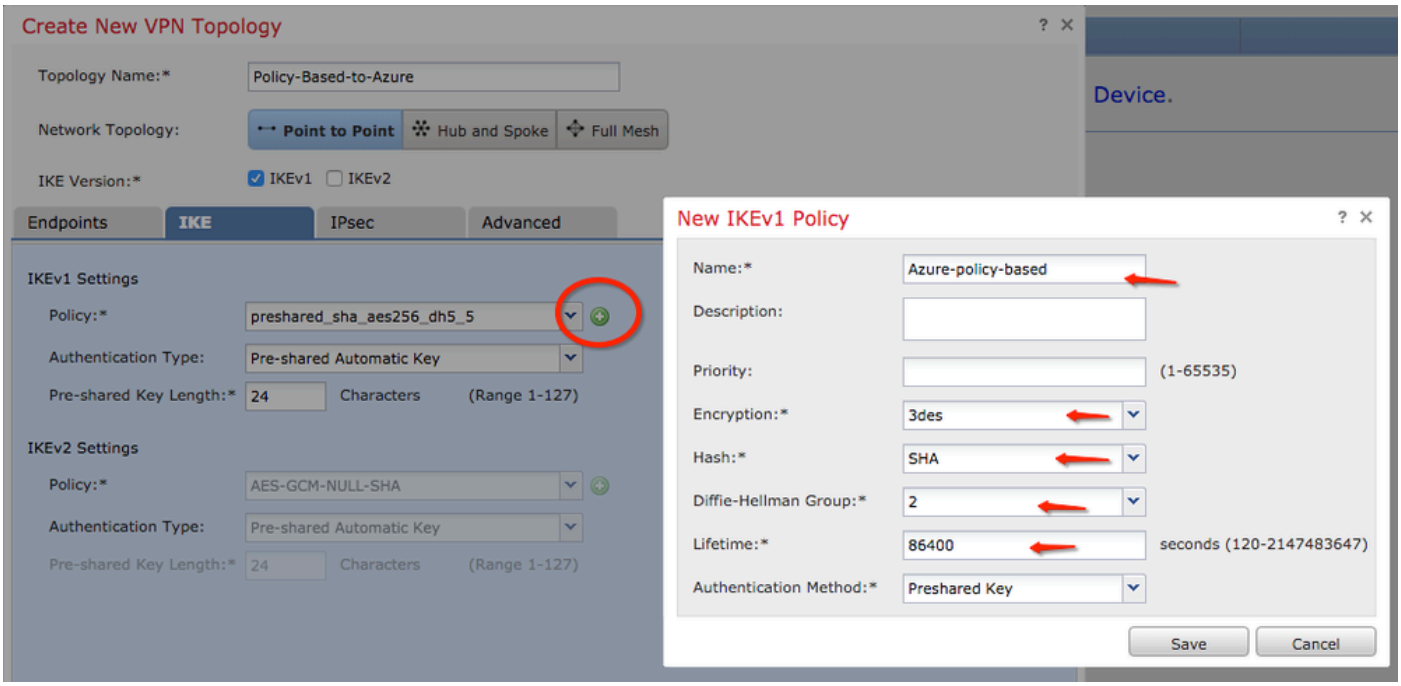


3.在Create new VPN Topology窗口中，指定Topology Name，选中IKEV1协议复选框，然后单击IKE选项卡。在本示例中，预共享密钥用作身份验证方法。单击Authentication Type下拉菜单，然后选择Pre-shared Manual Key。在Key和Confirm Key文本字段中键入手动预共享密钥。

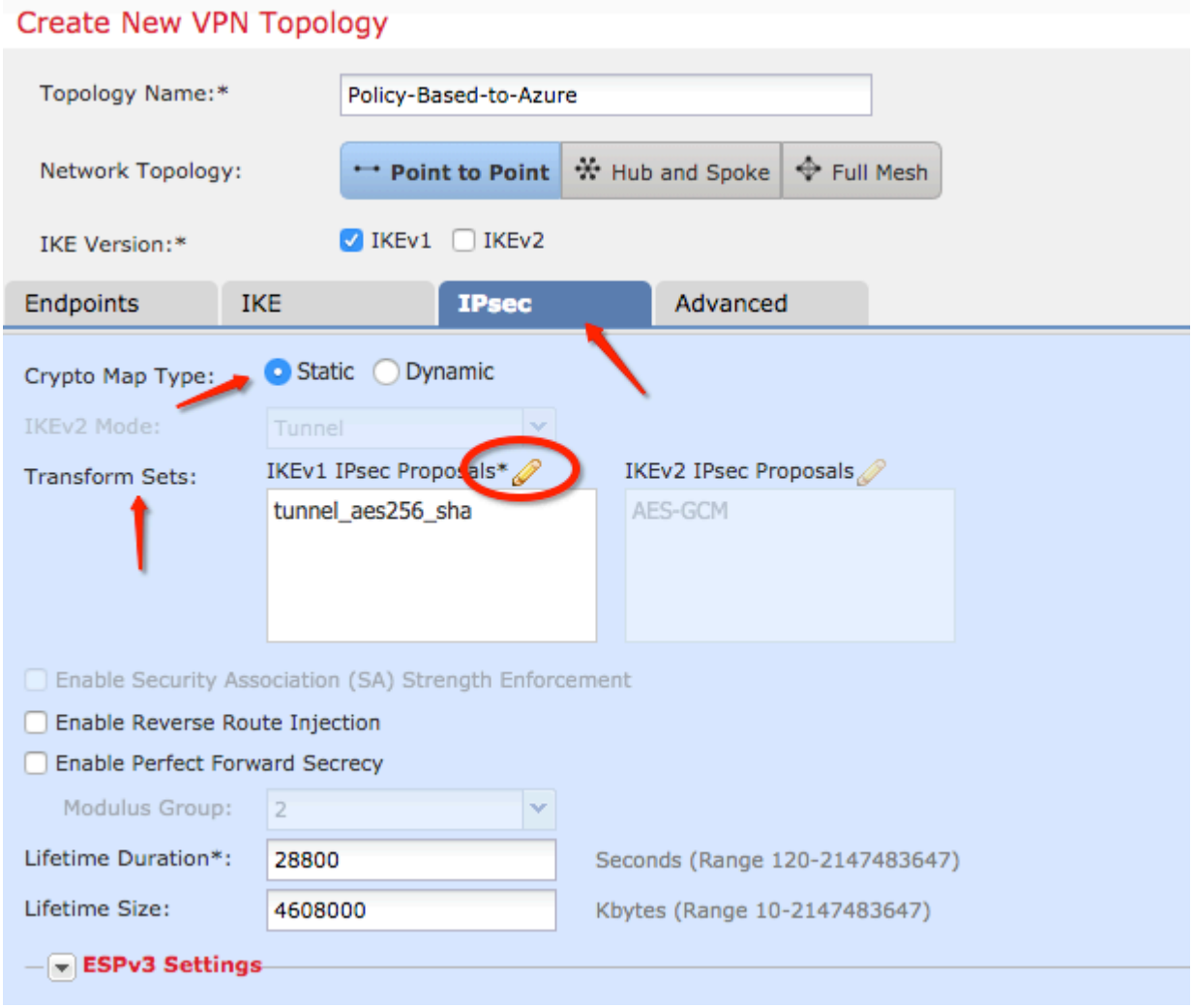




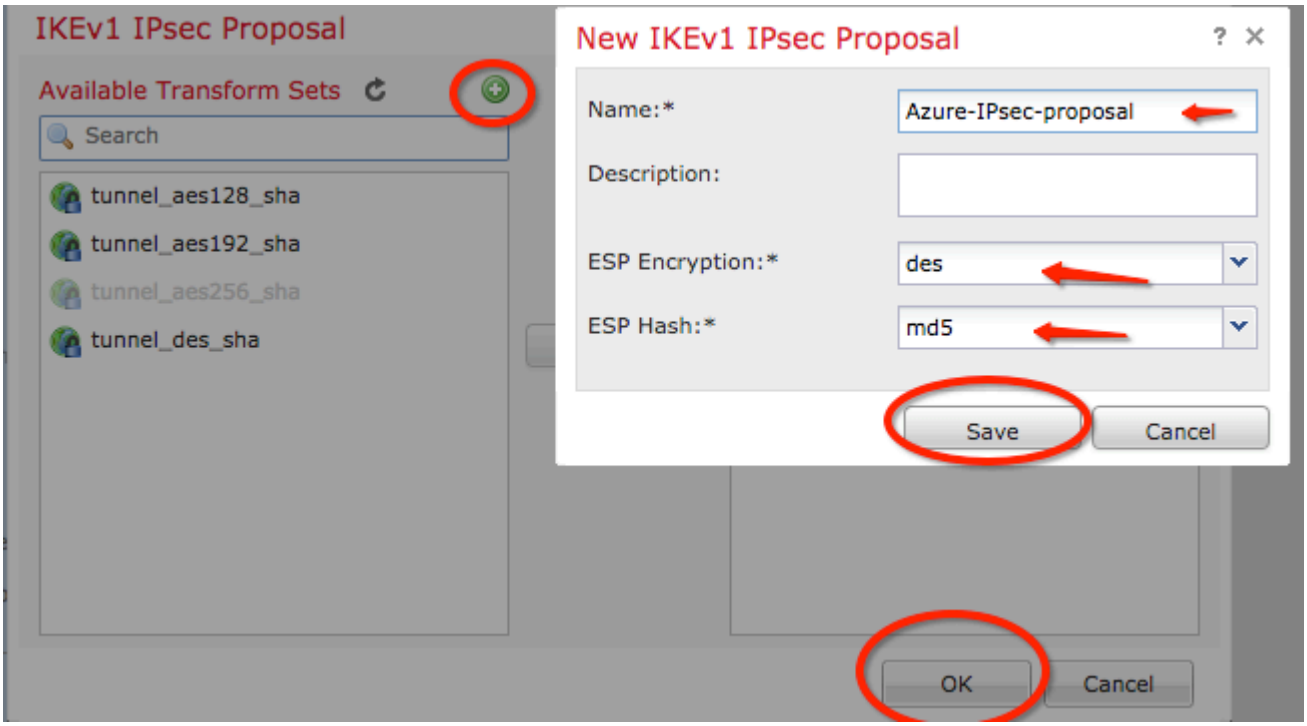
4.通过创建一个新参数来配置ISAKMP策略或第1阶段参数。在同一窗口中，单击绿色+按钮以添加新的ISAKMP策略。指定策略名称，并选择所需的加密(Encryption)、哈希(Hash)、Diffie-Hellman组(Diffie-Hellman Group)、生存期(Lifetime)和身份验证方法(Authentication Method)，然后单击保存(Save)。



5.配置IPsec策略或第2阶段参数。导航到IPsec选项卡，在Crypto Map Type复选框中选择Static。在转换集选项的IKEV1 IPsec提议中，点击编辑铅笔图标。

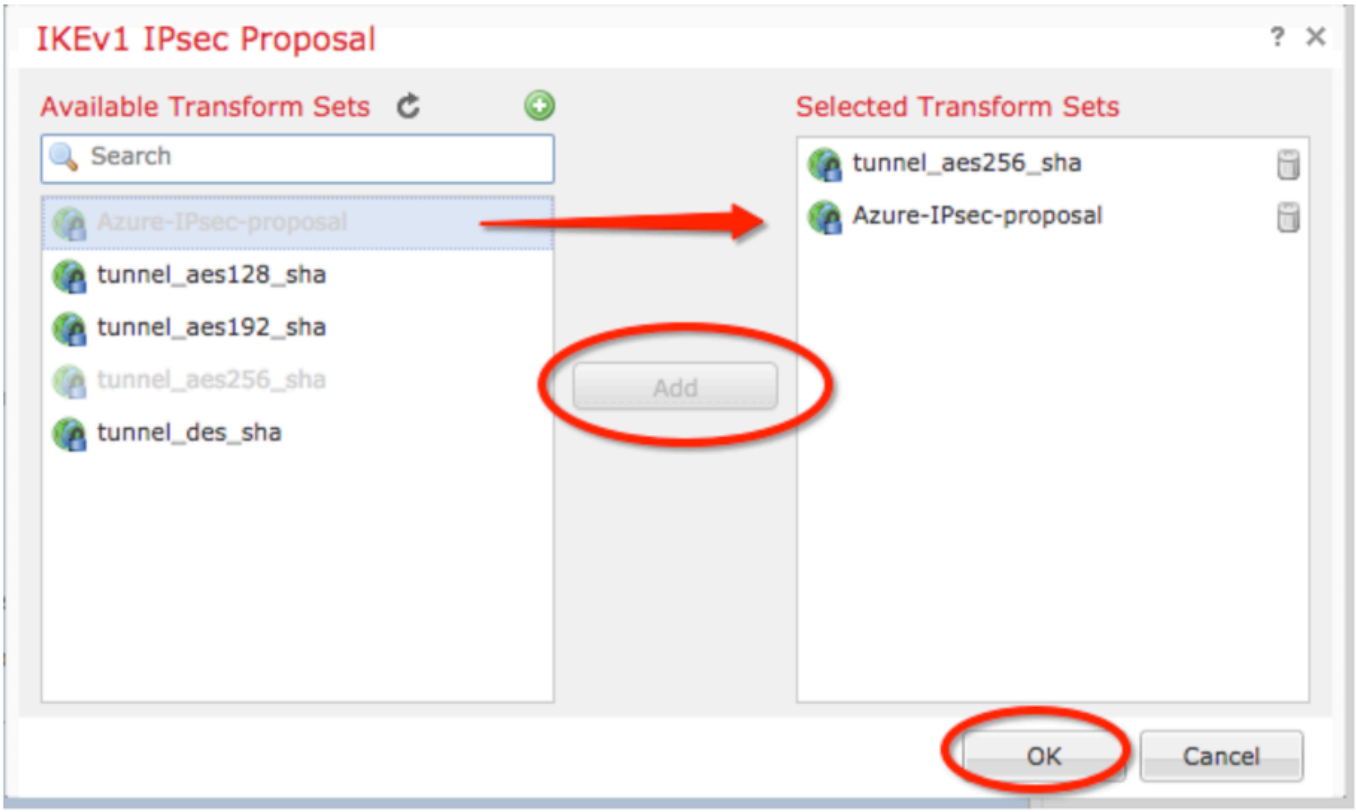


6.创建新的IPsec提议。在IKEv1 IPSec Proposal窗口中，单击绿色+按钮以添加新的。为ESP加密和ESP散列算法指定策略名称及其所需参数，然后单击Save。

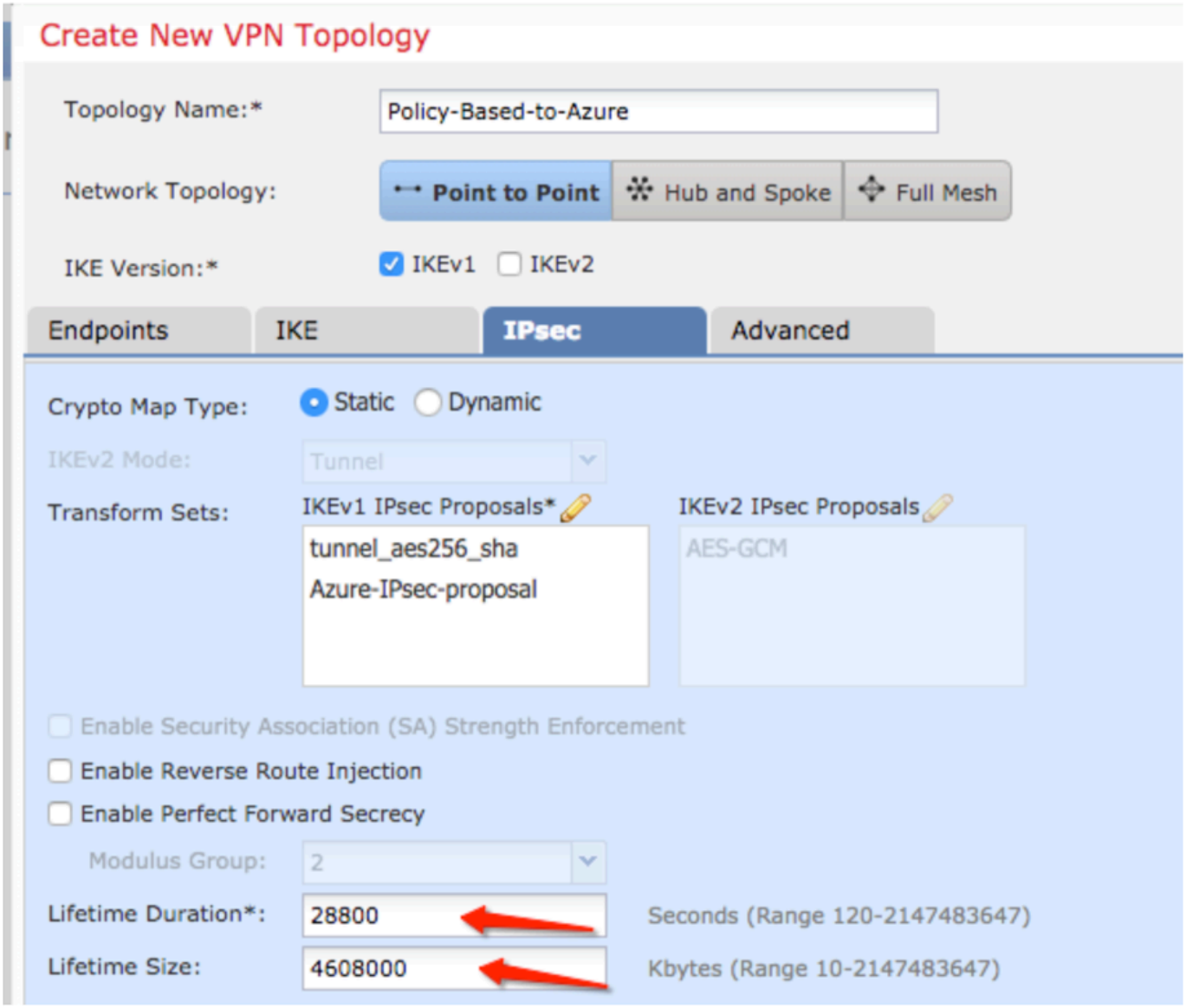


---

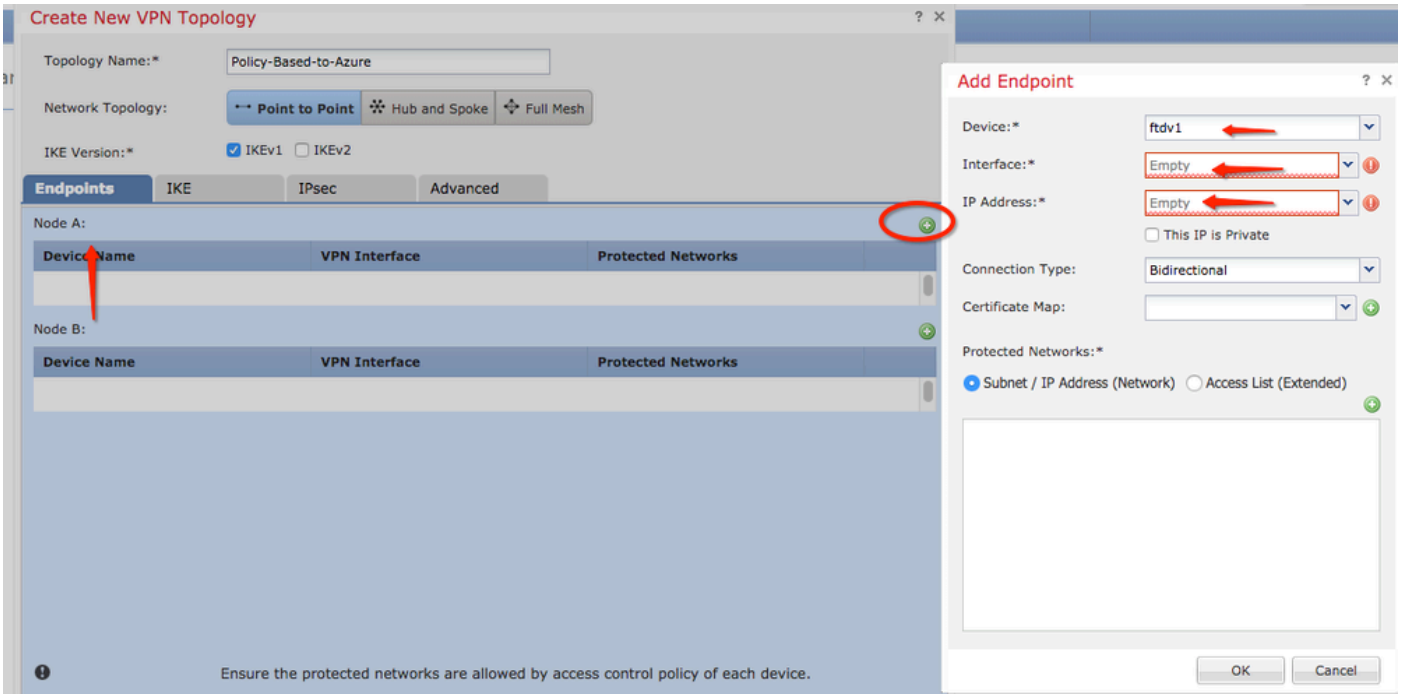
7. 在IKEV1 IPsec Proposal窗口中，将新IPsec策略添加到Selected Transform Sets部分，然后单击OK。



8.返回IPSec选项卡，配置所需的生存期持续时间和大小。



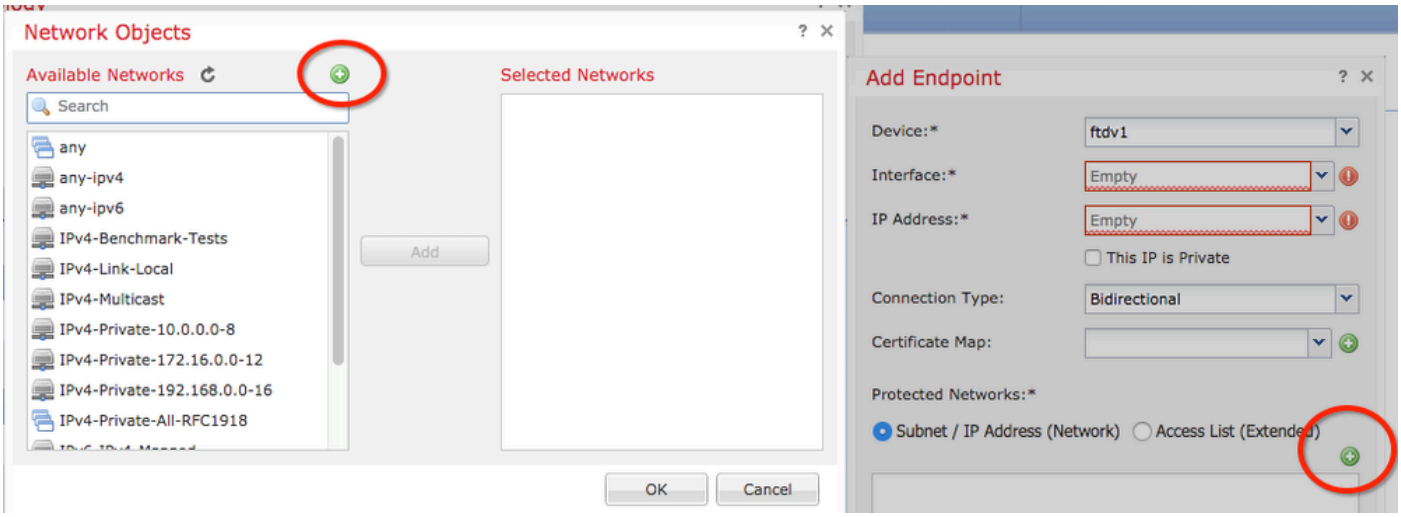
9.选择加密域/流量选择器/受保护的网络。导航到终端选项卡。在节点A上，点green + button击以添加新节点。在本示例中，节点A用作FTD的本地子网。



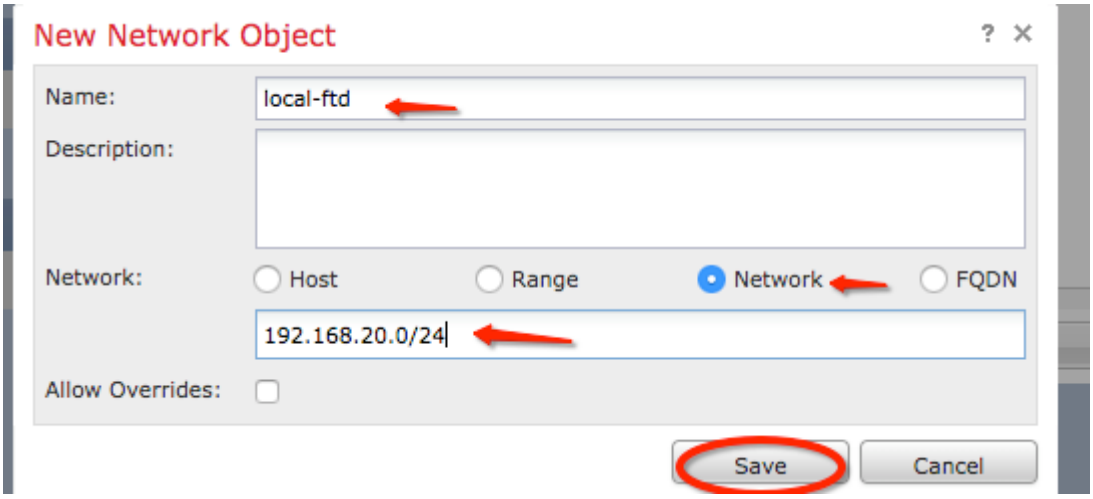
10.在Add Endpoint窗口中，指定要在Device下拉列表上使用的FTD以及要使用的物理接口和IP地址。

11.要指定本地流量选择器，请导航到受保护网络选项，然后单击绿色+按钮以创建新对象。

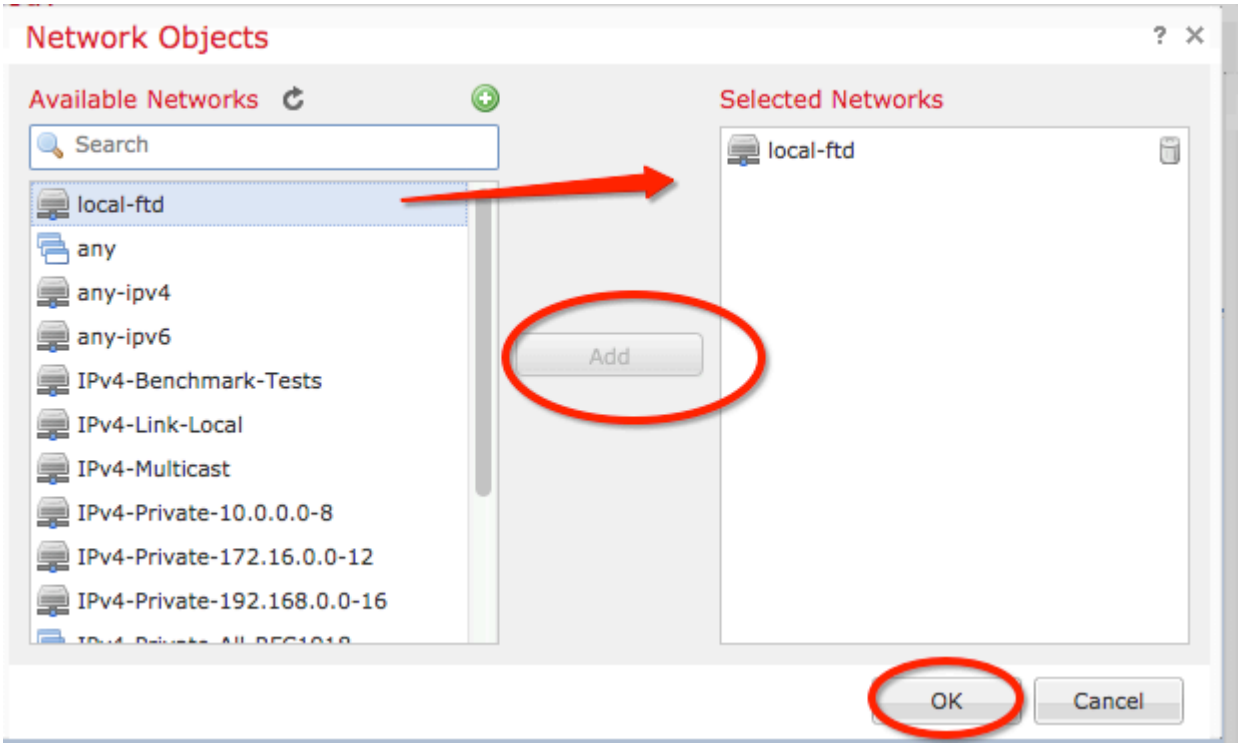
12.在网络对象窗口中，单击可用网络文本旁的绿色+按钮，以创建新的本地流量选择器对象。



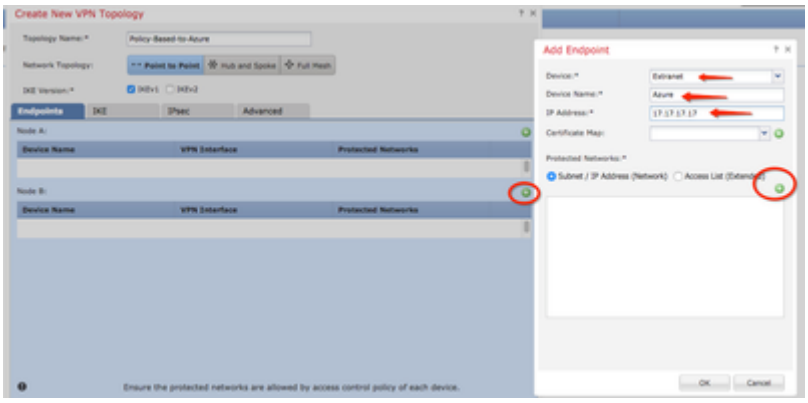
13.在New Network Object窗口中，指定对象的名称并相应选择；主机/网络/范围/FQDN。然后，单击Save。



14.将对象添加到“网络对象”窗口的“选定的网络”部分，然后单击确定。在“添加终端”窗口上，单击确定。

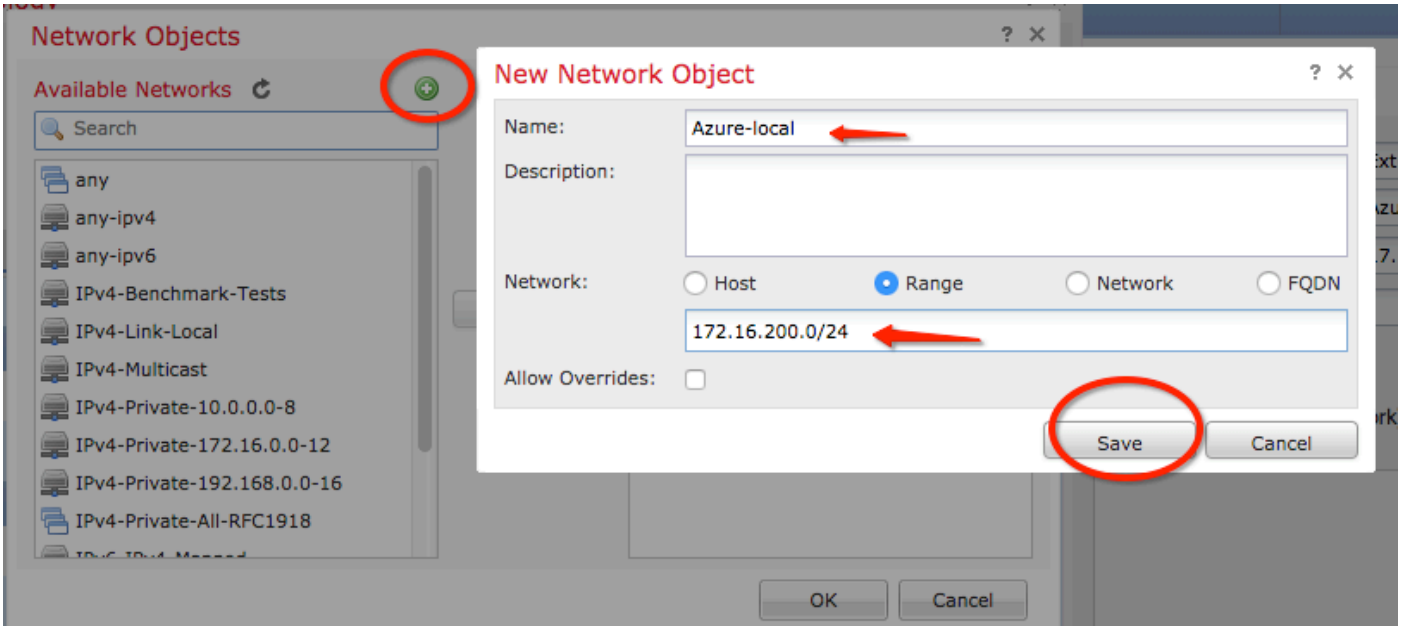


15.定义节点B，在本示例中，节点是Azure终结点。在Create New VPN Topology窗口中，导航到Node B部分并单击绿色+按钮以添加远程终端流量选择器。为并非由与节点A相同的FMC管理的所有VPN对等终端指定Extranet。键入设备的名称（仅在本地有效）及其IP地址。

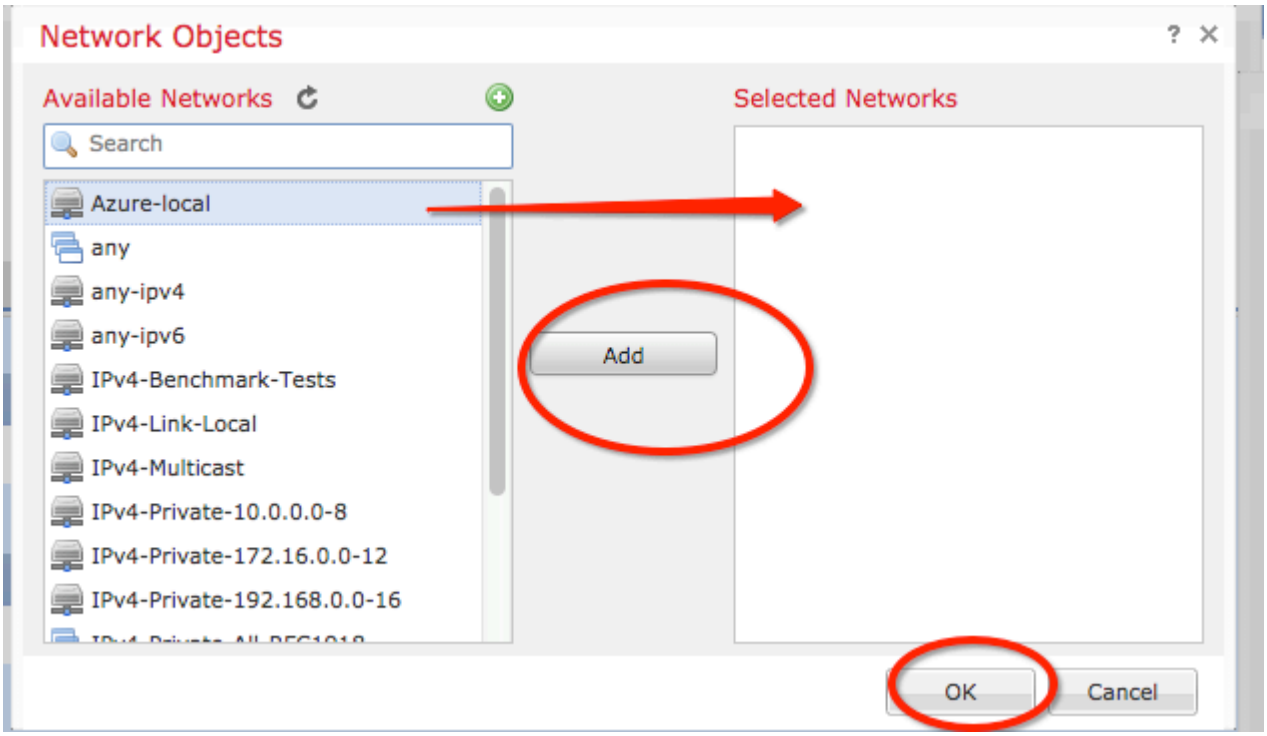


16.创建远程流量选择器对象。导航到受保护网络部分，然后单击绿色+按钮添加新对象。

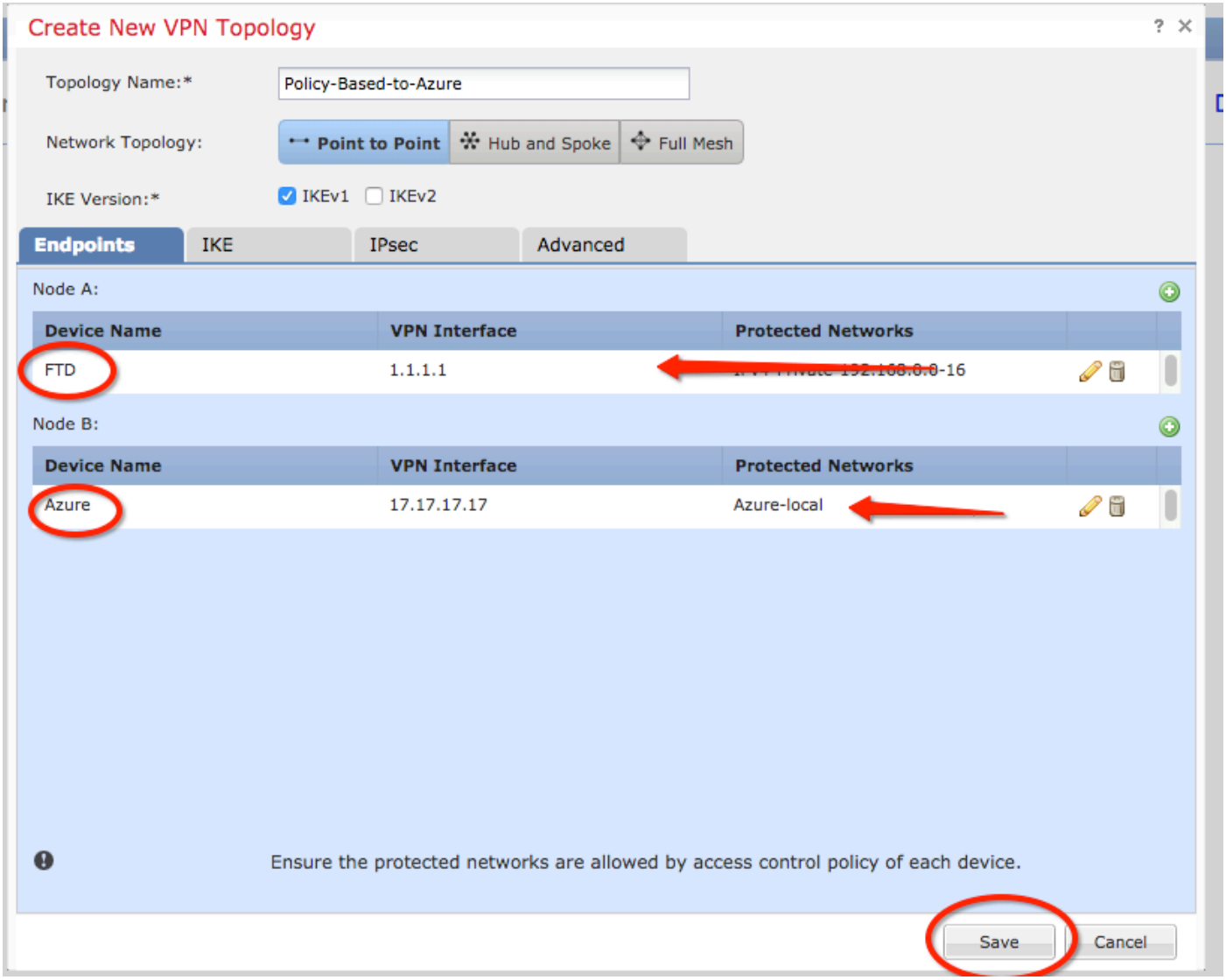
17.在网络对象窗口中，单击可用网络文本旁的绿色+按钮以创建新对象。在New Network Object窗口中，指定对象的名称并相应选择；host/range/network/FQDN，然后单击Save。



18.返回Network Objects窗口，将新的远程对象添加到Selected Networks部分，然后单击OK。在Add Endpoint窗口中单击OK。



19.在Create New VPN Topology窗口中，您现在可以看到两个节点都有其正确的流量选择器/受保护的网络。Click Save.



20.在FMC控制面板上，点击右上方窗格中的Deploy，选择FTD设备，然后点击Deploy。

21.在CLI上，VPN配置与ASA设备的配置看起来相同。

使用基于策略的流量选择器的IKEv2基于路由

对于具有加密映射的ASA上的站点到站点IKEv2 VPN，请使用此配置。确保Azure已配置为基于路由的VPN，并且必须使用PowerShell在Azure门户中配置UsePolicyBasedTrafficSelector。

从Microsoft将VPN网关连接到多个本地基于策略的VPN设备介绍UsePolicyBasedTrafficSelector与基于路由的Azure VPN模式的配置。如果不完成此步骤，由于从Azure接收的流量选择器不匹配，具有加密映射的ASA无法建立连接。

参考CLI手册3:Cisco ASA系列VPN CLI配置指南，9.8，用于包含加密映射配置信息的完整ASA IKEv2。

1.在外部接口上启用IKEv2:

<#root>

```
Cisco-ASA(config)#

crypto ikev2 enable outside
```

2.添加IKEv2第1阶段策略。

注意:Microsoft发布的信息与Azure使用的IKEv2第1阶段加密、完整性和生命周期属性冲突。列出的属性来自VPN设备和站点到站点VPN网关连接的IPsec/IKE参数。来自Microsoft的IKEv2属性信息冲突Sample Configuration:Cisco ASA设备（IKEv2/无BGP）。 如需进一步说明，请联系Microsoft Azure支持。

<#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.在IPsec属性下创建隧道组，并配置对等IP地址和IKEv2本地和远程隧道预共享密钥：

<#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.创建访问列表，定义要加密和隧道化的流量。在本示例中，相关流量是来自从10.2.2.0子网到10.1.1.0的隧道的流量。如果站点之间涉及多个子网，则该流量可以包含多个条目。

在版本8.4及更高版本中，可以创建用作网络、子网、主机IP地址或多个对象的容器的对象或对象组。创建两个具有本地和远程子网的对象，并将它们同时用于加密ACL和NAT语句。

<#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.添加IKEv2第2阶段IPsec提议。在crypto IPsec ikev2 ipsec-proposal配置模式下指定安全参数：

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}

注意:Microsoft已发布的信息与Azure使用的第2阶段IPSec加密和完整性属性冲突。列出的属性来自基于路由的VPN IPsec安全关联（IKE快速模式SA）产品。Microsoft提供的第2阶段IPSec属性信息冲突Sample Configuration:Cisco ASA设备（IKEv2/无BGP）。 如需进一步说明，请联系Microsoft Azure支持。

<#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.配置加密映射并将其应用于外部接口，该接口包含以下组件：

·对等IP地址。
·包含相关流量的已定义访问列表。
· IKEv2第2阶段IPSec提议。
·第2阶段IPSec生存期（以秒为单位）。
·可选的完全向前保密(PFS)设置，创建用于保护数据的新Diffie-Hellman密钥对（在第2阶段出现之前，两端都必须启用PFS。）

Microsoft已发布的信息与Azure使用的第2阶段IPSec生命周期和PFS属性冲突。

列出的属性来自基于路由的VPN IPsec安全关联（IKE快速模式SA）产品。

Microsoft提供的第2阶段IPSec属性信息冲突Sample Configuration:Cisco ASA设备（IKEv2/无BGP）。 有关进一步说明，请联系Microsoft Azure支持。

<#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.确保VPN流量不受任何其他NAT规则的约束。创建NAT免除规则：

<#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
```

注意：当使用多个子网时，您必须创建包含所有源和目标子网的对象组，并在NAT规则中使用它们。

<#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
```

验证

在ASA和Azure网关上完成配置后，Azure将启动VPN隧道。您可以使用以下命令验证隧道构建是否正确：

第 1 阶段

验证是否已建立第1阶段安全关联(SA):

接下来，显示从UDP端口500上的本地外部接口IP 192.168.1.2构建到远程目标IP 192.168.2.2的IKEv2 SA。还有一个有效的子SA，为要流经的加密流量而构建。

<#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
```

在本示例中，IKEv1 SA是以ASA作为发起方构建的，其对等IP 192.168.2.2的剩余有效期为86388秒：

<#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
```

第 2 阶段

验证第2阶段IPSec安全关联是否与show crypto ipsec sa peer [peer-ip]建立：

<#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
```

通过IPSec SA发送四个数据包，接收四个数据包，且没有错误。一个带有SPI 0x9B60EDC5的入站SA和一个带有SPI 0x8E7A2E12的出站SA按预期安装。

您还可以通过检查vpn-sessiondb l2l条目来验证通过隧道的数据传递：

<#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
```

字节Tx:和字节数Rx:显示通过IPSec SA发送和接收的数据计数器。

故障排除

1.验证ASA在发往Azure专用网络的内部接口上收到发往VPN的流量。要进行测试，可以从内部客户端配置连续ping，并在ASA上配置数据包捕获以验证是否已收到数据包：

---

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
```

- 如果发现来自Azure的应答流量，则正确构建VPN并发送/接收流量。
- 如果源流量不存在，请验证发件人是否正确路由到ASA。
- 如果发现源流量，但来自Azure的回复流量不存在，请继续验证原因。

2.验证ASA内部接口上接收的流量已由ASA正确处理并路由到VPN:

模拟ICMP回应请求：

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

---

请参阅完整的Packet Tracer使用指南使用Packet Tracer排除访问故障

<#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=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
```

NAT免除流量（转换不生效）。 验证VPN流量上未发生NAT转换。此外，验证output-interface是否正确，它必须是应用加密映射的物理接口或虚拟隧道接口。

确保未看到任何访问列表丢弃。如果VPN阶段显示ENCRYPT:ALLOW，隧道已建立，您可以看到安装了封装的IPSec SA。

2.1.如果加密：在Packet Tracer中可以看到ALLOW。

- 使用show crypto ipsec sa验证是否已安装IPsec SA并加密流量。
- 您可以在外部接口上执行捕获，以验证加密数据包是从ASA发送的，加密响应是从Azure接收的。

2.2.如果在Packet Tracer中看到ENCRYPT:DROP。

- VPN隧道尚未建立，但正在协商。这是首次启用隧道时的预期条件。运行debugs以查看隧道协商过程并确定故障发生位置及发生情况。

验证IKE的正确版本已触发并且IKE通用进程未显示相关错误：

<#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.
```

如果启动VPN流量时未看到ike-common调试输出，这意味着流量在到达加密进程之前被丢弃，或者未在设备上启用crypto ikev1/ikev2。仔细检查加密配置和数据包丢弃。

如果ike-common调试显示加密进程已触发，请调试IKE配置的版本以查看隧道协商消息并确定使用Azure建立隧道时失败的位置。

IKEv1

请参阅完整的ikev1调试过程和分析：ASA IPsec和IKE调试（IKEv1主模式）故障排除TechNote。

<#root>

```
Cisco-ASA#

debug crypto ikev1 127


Cisco-ASA#
```

```
debug crypto ipsec 127
```

IKEv2

请参阅完整的ikev2调试过程和分析：对具有PSK的站点到站点VPN使用ASA IKEv2调试

<#root>

```
Cisco-ASA#

debug crypto ikev2 platform 127

Cisco-ASA#

debug crypto ikev2 protocol 127

Cisco-ASA#

debug crypto ipsec 127
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。