Configuración de VPN de sitio a sitio en FTD administrado por FDM

Contenido

Introducción

Este documento describe cómo configurar VPN de sitio a sitio en Firepower Threat Defense (FTD) administrado por FirePower Device Manager (FDM).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica de VPN
- Experiencia con FDN
- Experiencia con la línea de comandos del dispositivo de seguridad adaptable (ASA)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- FTD 6.5 de Cisco
- ASA 9.10(1)32
- IKEv2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

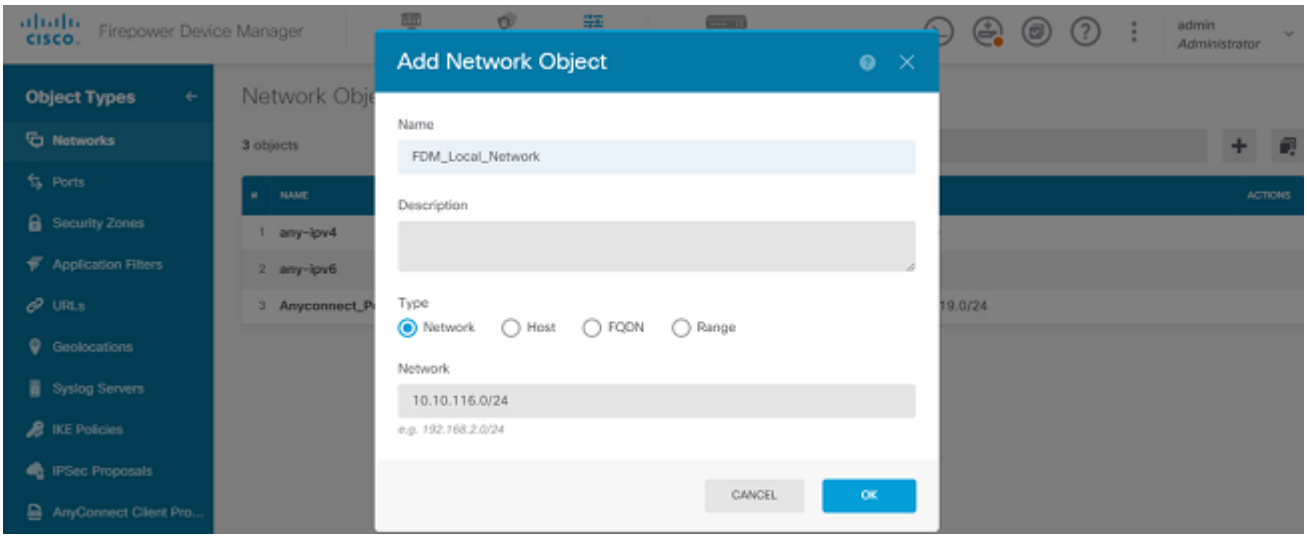
Configurar

Comience con la configuración en FTD con FDM.

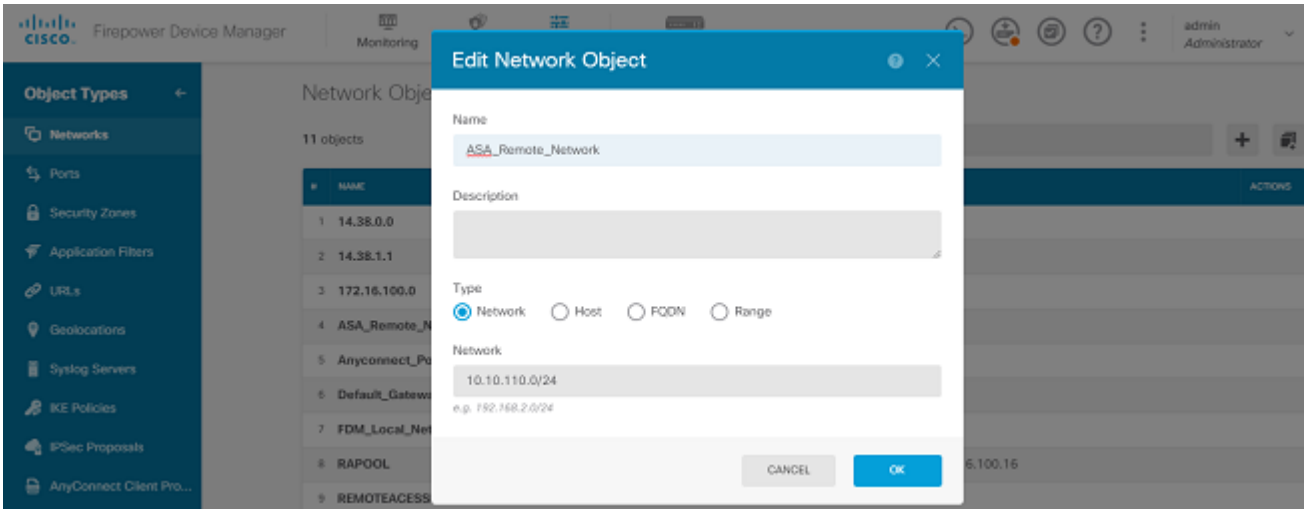
Definición de redes protegidas

Vaya a **Objetos > Redes > Agregar nueva red**.

Configure los objetos para las redes LAN desde la GUI de FDM. Cree un objeto para la red local detrás del dispositivo FDM, como se muestra en la imagen.



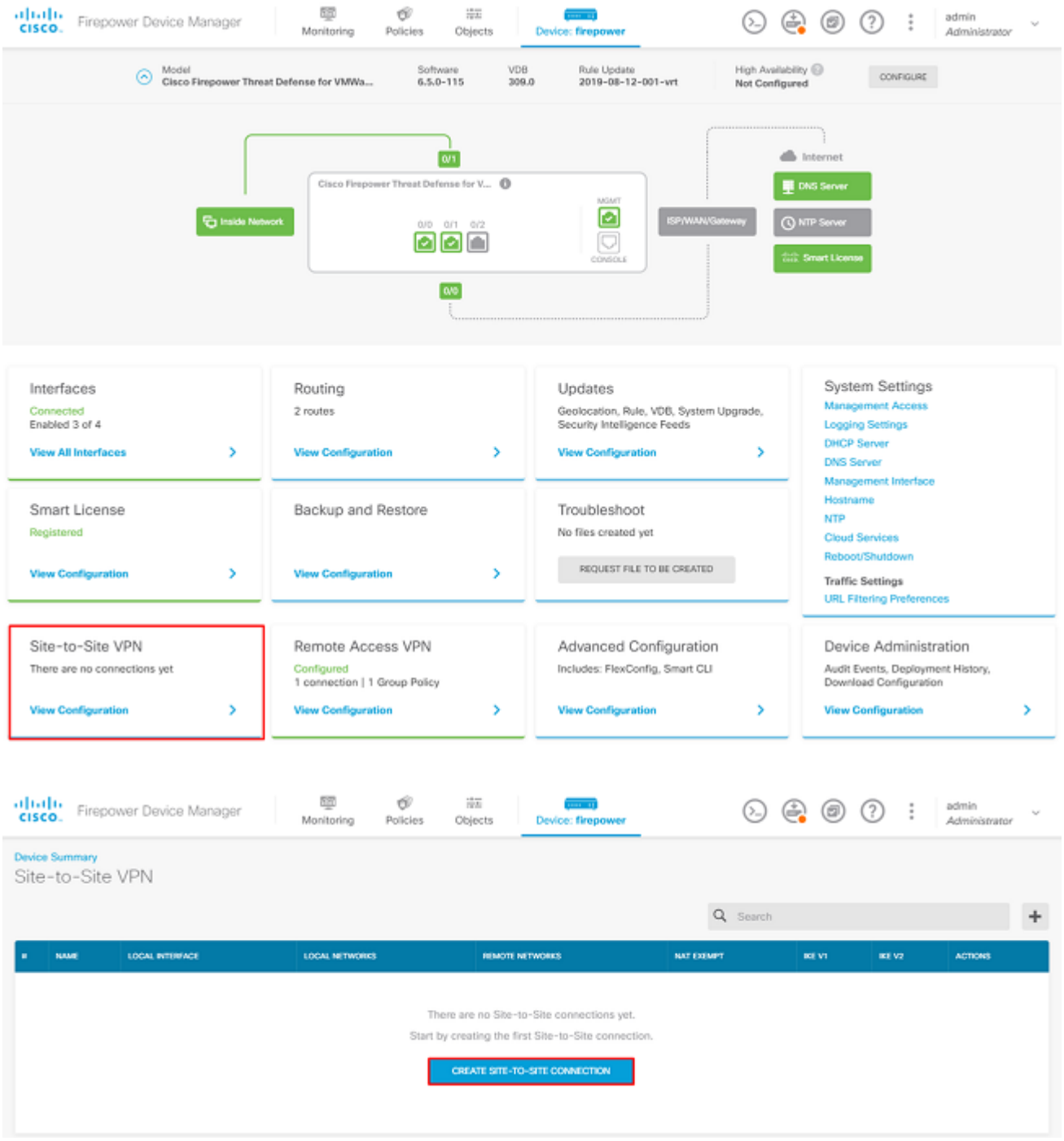
Cree un objeto para la red remota detrás del dispositivo ASA como se muestra en la imagen.



Configuración de VPN de sitio a sitio

Vaya a **VPN de sitio a sitio > Crear conexión de sitio a sitio**.

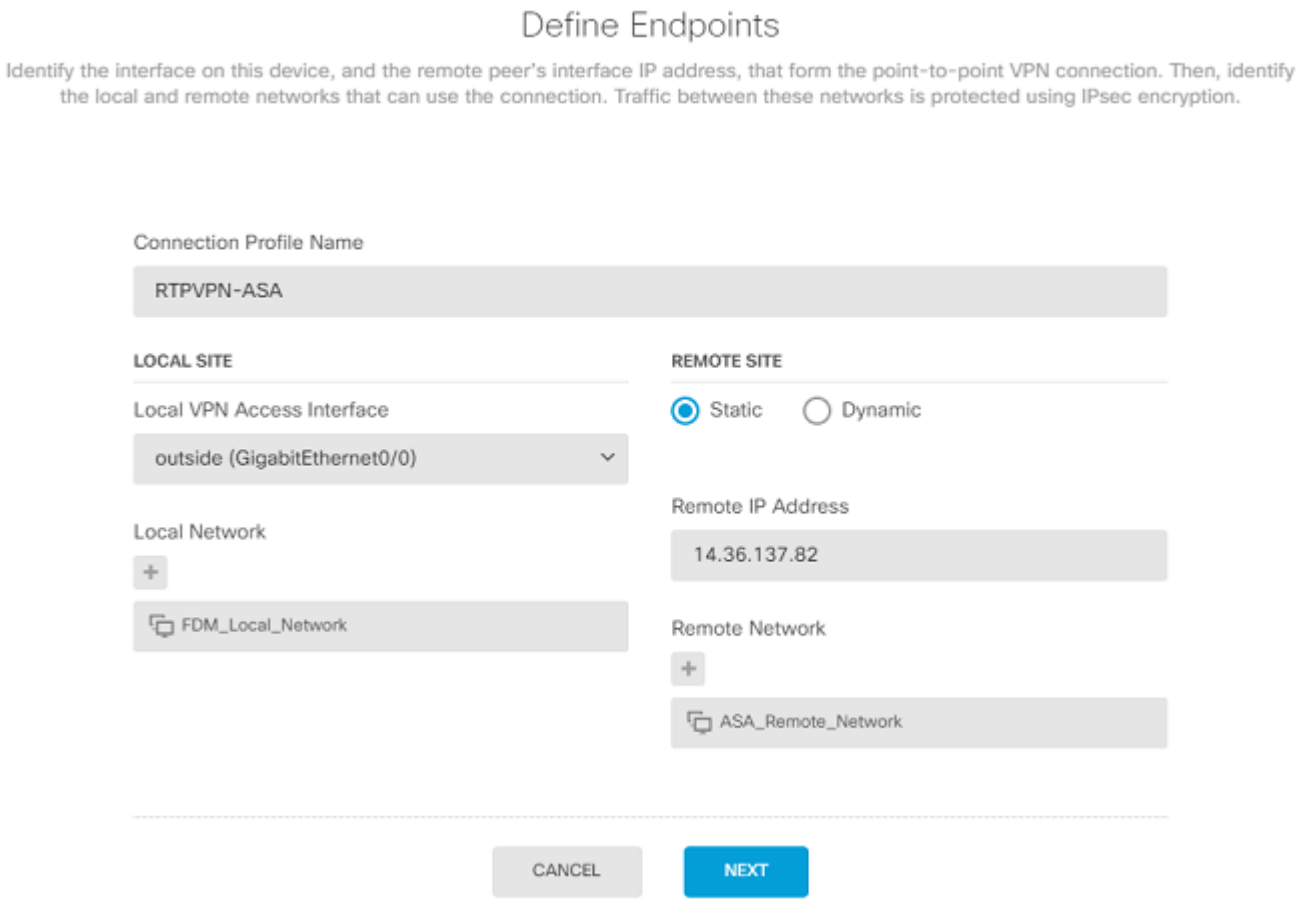
Vaya al asistente de sitio a sitio en FDM, como se muestra en la imagen.



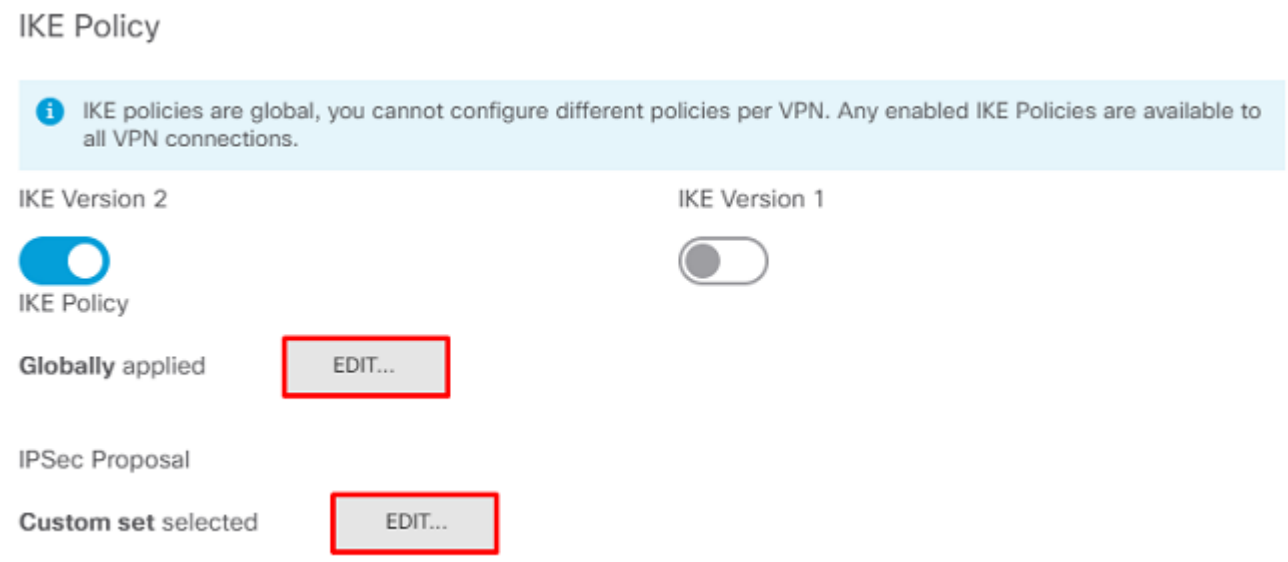
Dé a la conexión de sitio a sitio un nombre de perfil de conexión que se pueda identificar fácilmente.

Elija la interfaz externa correcta para el FTD y, a continuación, elija la red local que debe cifrarse en la VPN de sitio a sitio.

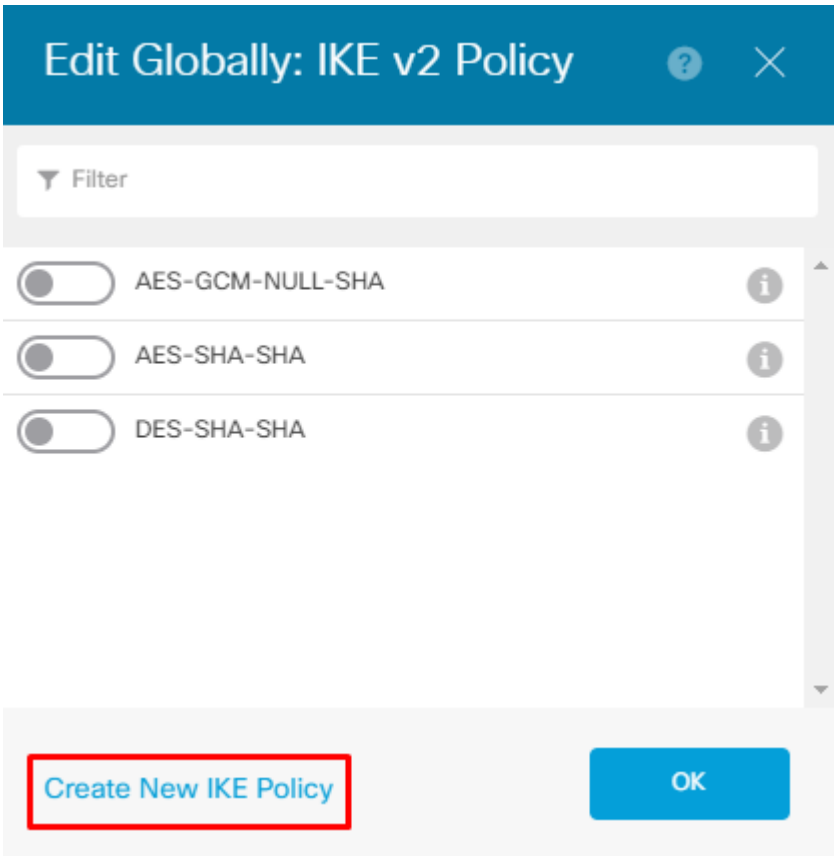
Establezca la interfaz pública del par remoto. A continuación, elija la red de peers remotos que está cifrada a través de la VPN de sitio a sitio, como se muestra en la imagen.



En la página siguiente, seleccione el botón **Edit** para establecer los parámetros de Intercambio de claves de Internet (IKE), como se muestra en la imagen.

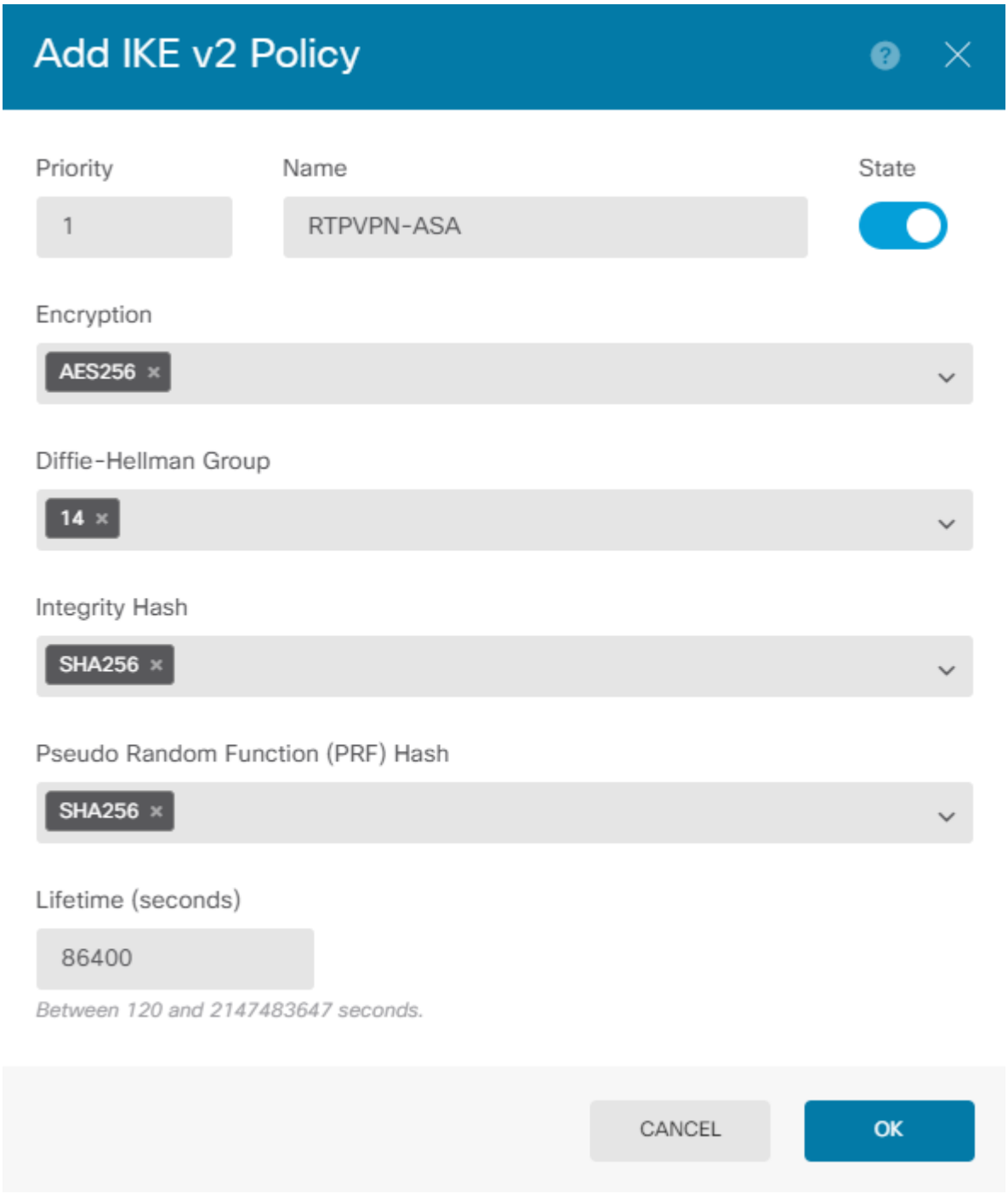


Elija el botón **Create New IKE Policy** como se muestra en la imagen.

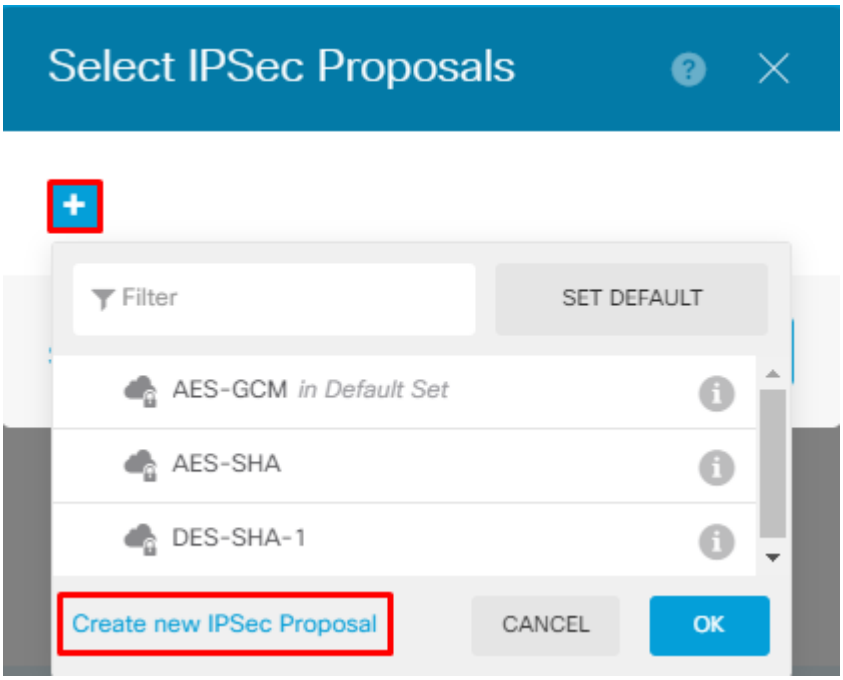


Esta guía utiliza estos parámetros para el intercambio inicial IKEv2:

Cifrado AES-256
Integridad SHA256
Grupo DH 14
PRF SHA256



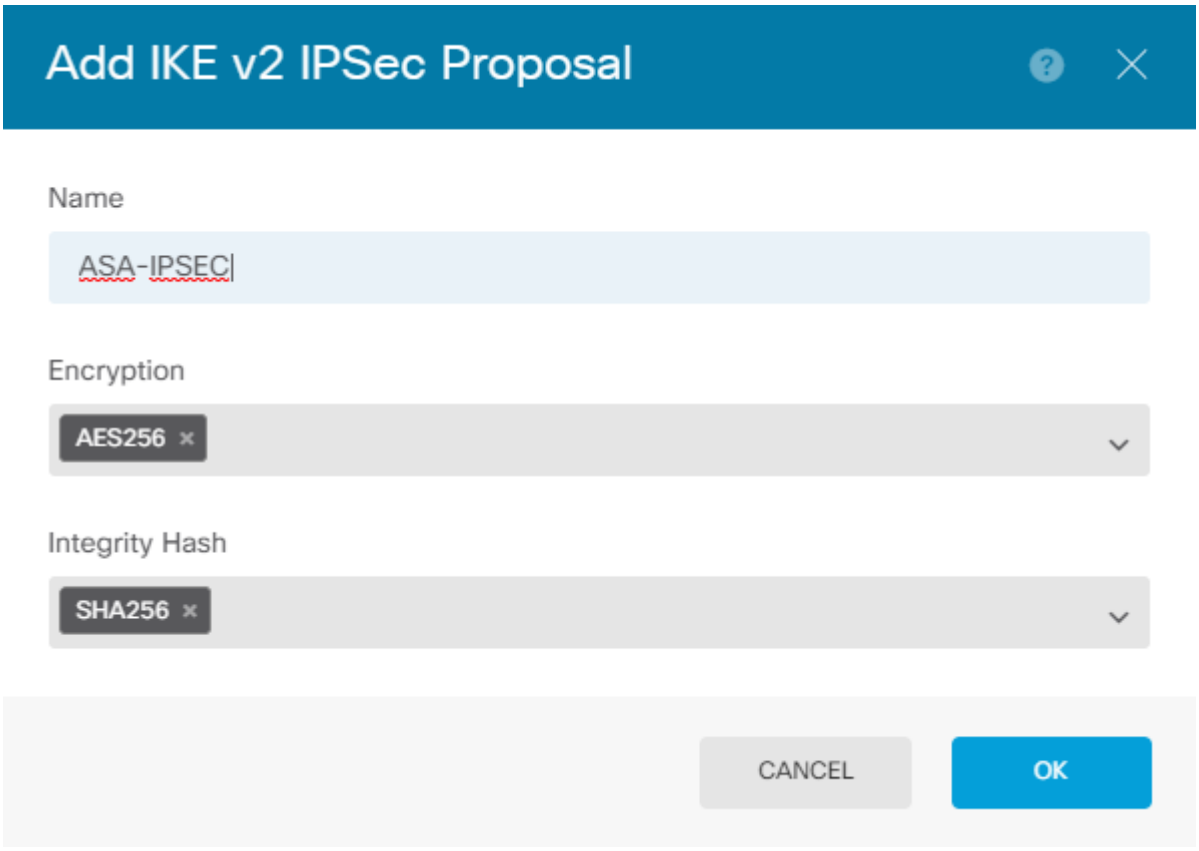
Una vez de vuelta en la página principal, elija el botón **Edit** para la propuesta IPSec. Cree una nueva propuesta IPSec como se muestra en la imagen.



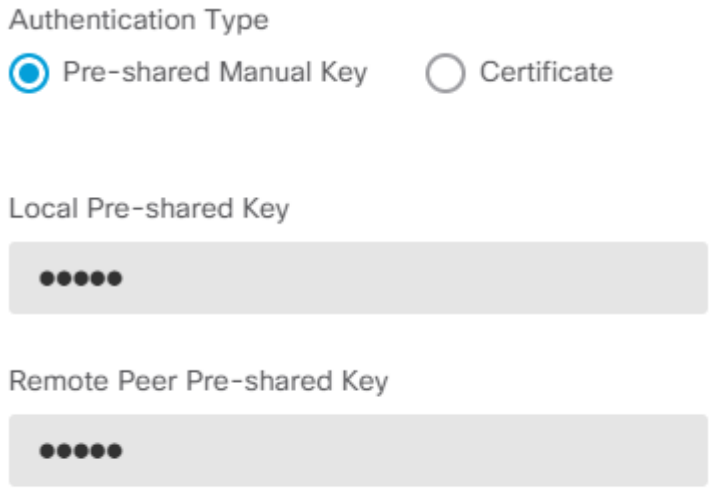
Esta guía utiliza estos parámetros para IPSec:

Cifrado AES-256

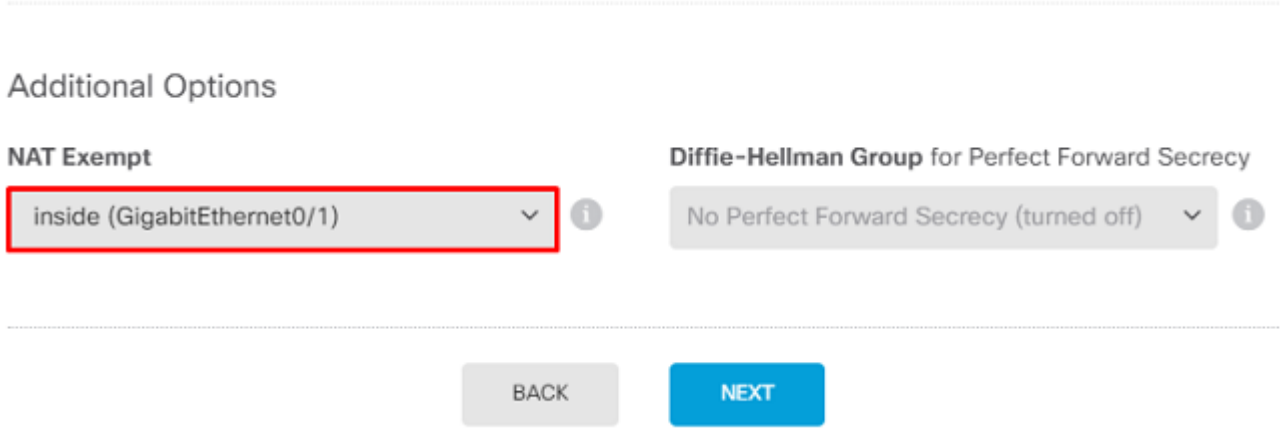
Integridad SHA256



Establezca la autenticación en clave previamente compartida e introduzca la clave previamente compartida (PSK) que se utiliza en ambos extremos. En esta guía, se utiliza la PSK de Cisco como se muestra en la imagen.



Establezca la interfaz NAT Exempt interna. Si hay varias interfaces internas que se utilizan, se debe crear una regla de exención de NAT manual en **Políticas > NAT**.



En la última página, se muestra un resumen de la conexión de sitio a sitio. Asegúrese de que se han seleccionado las direcciones IP correctas y de que se han utilizado los parámetros de encriptación adecuados. A continuación, pulse el botón Finish (Finalizar). Implemente la nueva VPN de sitio a sitio.

La configuración de ASA se completa con el uso de la CLI.

Configuración de ASA

1. Habilite IKEv2 en la interfaz externa del ASA:

```
Crypto ikev2 enable outside
```

2. Cree la política IKEv2 que define los mismos parámetros configurados en el FTD:

```
Crypto ikev2 policy 1
 Encryption aes-256
 Integrity sha256
 Group 14
 Prf sha256
 Lifetime seconds 86400
```

3. Cree una política de grupo que permita el protocolo IKEv2:

```
Group-policy FDM_GP internal
Group-policy FDM_GP attributes
Vpn-tunnel-protocol ikev2
```

4. Cree un grupo de túnel para la dirección IP pública de FTD del par. Haga referencia a la política de grupo y especifique la clave previamente compartida:

```
Tunnel-group 172.16.100.10 type ipsec-l2l
Tunnel-group 172.16.100.10 general-attributes
 Default-group-policy FDM_GP
Tunnel-group 172.16.100.10 ipsec-attributes
 ikev2 local-authentication pre-shared-key cisco
 ikev2 remote-authentication pre-shared-key cisco
```

5. Cree una lista de acceso que defina el tráfico que se va a cifrar: (FTDSubnet 10.10.116.0/24) (ASASubnet 10.10.110.0/24):

```
Object network FDMSubnet
 Subnet 10.10.116.0 255.255.255.0
Object network ASASubnet
 Subnet 10.10.110.0 255.255.255.0
Access-list ASAtoFTD extended permit ip object ASASubnet object FTDSubnet
```

6. Cree una propuesta IKEv2 IPsec que haga referencia a los algoritmos especificados en el FTD:

```
Crypto ipsec ikev2 ipsec-proposal FDM
 Protocol esp encryption aes-256
```

```
Protocol esp integrity sha-256
```

7. Cree una entrada de mapa criptográfico que una la configuración:

```
Crypto map outside_map 20 set peer 172.16.100.10
Crypto map outside_map 20 match address ASAtoFTD
Crypto map outside_map 20 set ikev2 ipsec-proposal FTD
Crypto map outside_map 20 interface outside
```

8. Cree una declaración de exención de NAT que evite que el firewall NATTED el tráfico VPN:

```
Nat (inside,outside) 1 source static ASASubnet ASASubnet destination static FDMSubnet FDMSubnet
no-proxy-arp route-lookup
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Intente iniciar el tráfico a través del túnel VPN. Con acceso a la línea de comandos del ASA o FTD, esto se puede hacer con el comando packet tracer. Cuando utiliza el comando packet-tracer para activar el túnel VPN, se debe ejecutar dos veces para verificar si el túnel aparece. La primera vez que se ejecuta el comando, el túnel VPN está inactivo, por lo que el comando packet-tracer falla con el cifrado VPN DROP. No utilice la dirección IP interna del firewall como dirección IP de origen en el rastreador de paquetes, ya que esto siempre falla.

```
firepower# packet-tracer input inside icmp 10.10.116.10 8 0 10.10.110.10

Phase: 9
Type: VPN
Subtype: encrypt
Result: DROP
Config:
Additional Information:
```

```
firepower# packet-tracer input inside icmp 10.10.116.10 8 0 10.10.110.10

Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 172.16.100.1 using egress ifc outside

Phase: 2
```

```
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source static |s2sAclSrcNwgV4|c9911223-779d-11ea-9c1b-5ddd47126971 |s2sAclSrcNwgV4|
Additional Information:
NAT divert to egress interface outside
Untranslate 10.10.110.10/0 to 10.10.110.10/0

Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group NGFW_ONBOX_ACL global
access-list NGFW_ONBOX_ACL advanced trust object-group |acSvcg-268435457 ifc inside any ifc outside any
access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy
access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule
object-group service |acSvcg-268435457
service-object ip
Additional Information:

Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static |s2sAclSrcNwgV4|c9911223-779d-11ea-9c1b-5ddd47126971 |s2sAclSrcNwgV4|
Additional Information:
Static translate 10.10.116.10/0 to 10.10.116.10/0

Phase: 9
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:

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

Para monitorear el estado del túnel, navegue hasta la CLI del FTD o ASA.

Desde la CLI de FTD, verifique la fase 1 y la fase 2 con el comando **show crypto ikev2 sa**.

```
> show crypto ikev2 sa

IKEv2 SAs:

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

Tunnel-id Local                                         Remote
```

```
  3821043 172.16.100.10/500                                   192.168.200.10/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/1150 sec
Child sa: local selector  10.10.116.0/0 - 10.10.116.255/65535
          remote selector 10.10.110.0/0 - 10.10.110.255/65535
          ESP spi in/out: 0x7398dcbd/0x2303b0c0
```

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Problemas de conectividad inicial

Al crear una VPN, hay dos lados que negocian el túnel. Por lo tanto, es mejor obtener ambos lados de la conversación cuando se resuelve cualquier tipo de falla de túnel. Una guía detallada sobre cómo depurar túneles IKEv2 se puede encontrar aquí: Cómo depurar VPN IKEv2

La causa más común de fallas de túnel es un problema de conectividad. La mejor manera de determinar esto es tomar capturas de paquetes en el dispositivo.

Utilice este comando para tomar capturas de paquetes en el dispositivo:

```
Capture capout interface outside match ip host 172.16.100.10 host 192.168.200.10
```

Una vez que la captura esté en su lugar, intente enviar tráfico a través de la VPN y verifique si hay tráfico bidireccional en la captura de paquetes.

Revise la captura de paquetes con el comando **show cap capout**.

```
firepower# show cap capout

4 packets captured

   1: 01:21:06.763983       172.16.100.10.500 > 192.168.200.10.500:  udp 574
   2: 01:21:06.769415       192.168.200.10.500 > 172.16.100.10.500:  udp 619
   3: 01:21:06.770666       172.16.100.10.500 > 192.168.200.10.500:  udp 288
   4: 01:21:06.773748       192.168.200.10.500 > 172.16.100.10.500:  udp 256
```

Problemas Específicos Del Tráfico

Los problemas comunes de tráfico que experimentan los usuarios son:

- Problemas de ruteo detrás del FTD - la red interna no puede rutear paquetes de vuelta a las direcciones

IP asignadas y a los clientes VPN.
- Listas de control de acceso que bloquean el tráfico.
- La traducción de direcciones de red (NAT) no se omite para el tráfico VPN.

Información Relacionada

Para obtener más información sobre las VPN de sitio a sitio en el FTD gestionado por FDM, puede encontrar la guía de configuración completa aquí.

- Guía de configuración de FDM Administrado por FDM.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).