

Configuración del Túnel VPN Sitio a Sitio Basado en Ruta en FTD Administrado por FMC

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Límites y Restricciones](#)

[Pasos de configuración en FMC](#)

[Verificación](#)

[Desde la GUI de FMC](#)

[Desde CLI de FTD](#)

Introducción

Este documento describe cómo configurar un túnel VPN de sitio a sitio basado en una ruta estática en Firepower Threat Defense administrado por Firepower Management Center.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica de cómo funciona un túnel VPN.
- Comprender cómo navegar por el FMC.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Cisco Firepower Management Center (FMC) versión 6.7.0
- Cisco Firepower Threat Defense (FTD) versión 6.7.0

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.

Antecedentes

La VPN basada en rutas permite la determinación del tráfico interesante que se debe cifrar o enviar a través del túnel VPN, y utiliza el ruteo del tráfico en lugar de la política/lista de acceso como en la VPN basada en políticas o en mapas criptográficos. El dominio de cifrado está configurado para permitir el tráfico que entra en el túnel IPsec. Los selectores de tráfico local y remoto IPsec están configurados en 0.0.0.0/0.0.0.0. Esto significa que todo el tráfico enrutado en el túnel IPsec se cifra independientemente de la subred de origen/destino.

Este documento se centra en la configuración de la Interfaz de Túnel Virtual Estática (SVTI). Para obtener información sobre la configuración de la interfaz de túnel virtual dinámico (DVTI) en Secure Firewall, consulte este [documento](#).

Límites y Restricciones


Estas son las limitaciones y restricciones conocidas para túneles basados en ruta en FTD:

- Sólo admite IPsec. GRE no es compatible.
- Solo admite interfaces IPv4, así como IPv4, redes protegidas o carga útil de VPN (sin compatibilidad con IPv6).
- El ruteo estático y solamente el protocolo de ruteo dinámico BGP se soporta para las interfaces VTI que clasifican el tráfico para VPN (No soporta otros protocolos como OSPF, RIP, y así sucesivamente).
- Sólo se admiten 100 VTI por interfaz.
- VTI no es compatible con un clúster de FTD.
- VTI no es compatible con estas políticas:
 - QoS
 - NAT
 - Configuración de la plataforma


Estos algoritmos ya no son compatibles con la versión 6.7.0 del FMC/FTD para los nuevos túneles VPN (FMC admite todos los cifrados eliminados para gestionar el FTD < 6.7):

- 3DES, DES y el cifrado NULL no son compatibles con la directiva IKE.
- Los grupos DH 1, 2 y 24 no son compatibles con la directiva IKE y la propuesta IPsec.

- La política IKE no admite la integridad MD5.
- PRF MD5 no es compatible con la política IKE.
- Los algoritmos de cifrado DES, 3DES, AES-GMAC, AES-GMAC-192 y AES-GMAC-256 no son compatibles con la propuesta IPSec.

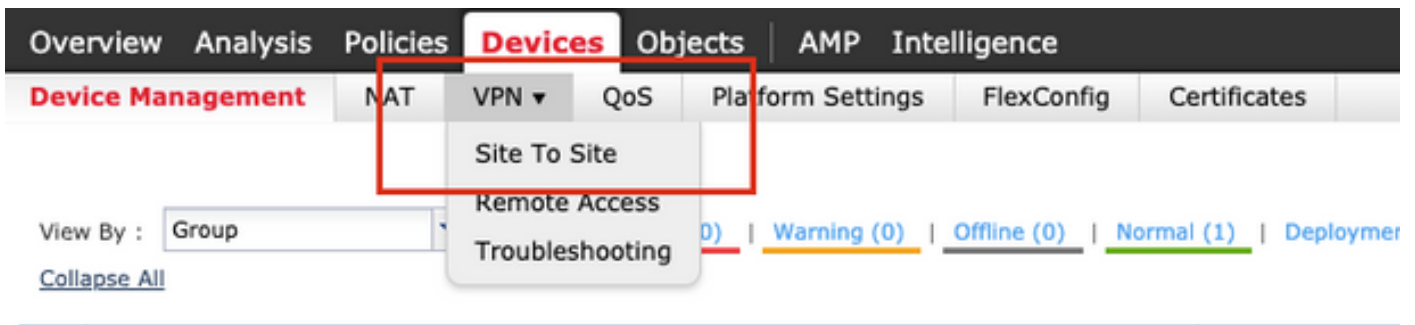
 Nota: Esto se aplica tanto a los túneles VPN basados en políticas como a las rutas entre sitios. Para actualizar un FTD antiguo a 6.7 desde FMC, se activa una comprobación de validación previa que advierte al usuario de los cambios que pertenecen a los cifrados eliminados que bloquean la actualización.

FTD 6.7 gestionado mediante FMC 6.7	Configuración disponible	Túnel VPN de sitio a sitio
Instalación nueva	Cifras débiles disponibles pero que no se pueden utilizar para configurar el dispositivo FTD 6.7.	Cifras débiles disponibles pero que no se pueden utilizar para configurar el dispositivo FTD 6.7.
Actualización: FTD solo configurado con cifrados débiles	Actualización desde FMC 6.7 UI, una comprobación previa a la validación muestra un error. La actualización se bloquea hasta que se vuelva a configurar.	Después de la actualización de FTD, y suponga que el peer no ha cambiado su configuración, entonces el túnel se termina.
Actualización: FTD solo se configura con algunas cifras débiles y algunas cifradas fuertes	Actualización desde FMC 6.7 UI, una comprobación previa a la validación muestra un error. La actualización se bloquea hasta que se vuelva a configurar.	Después de la actualización de FTD, y asuma que el peer tiene cifrados fuertes, luego el túnel se restablece.
Actualización: país de clase C (no dispone de una licencia criptográfica segura)	Permitir DES está permitido	Permitir DES está permitido

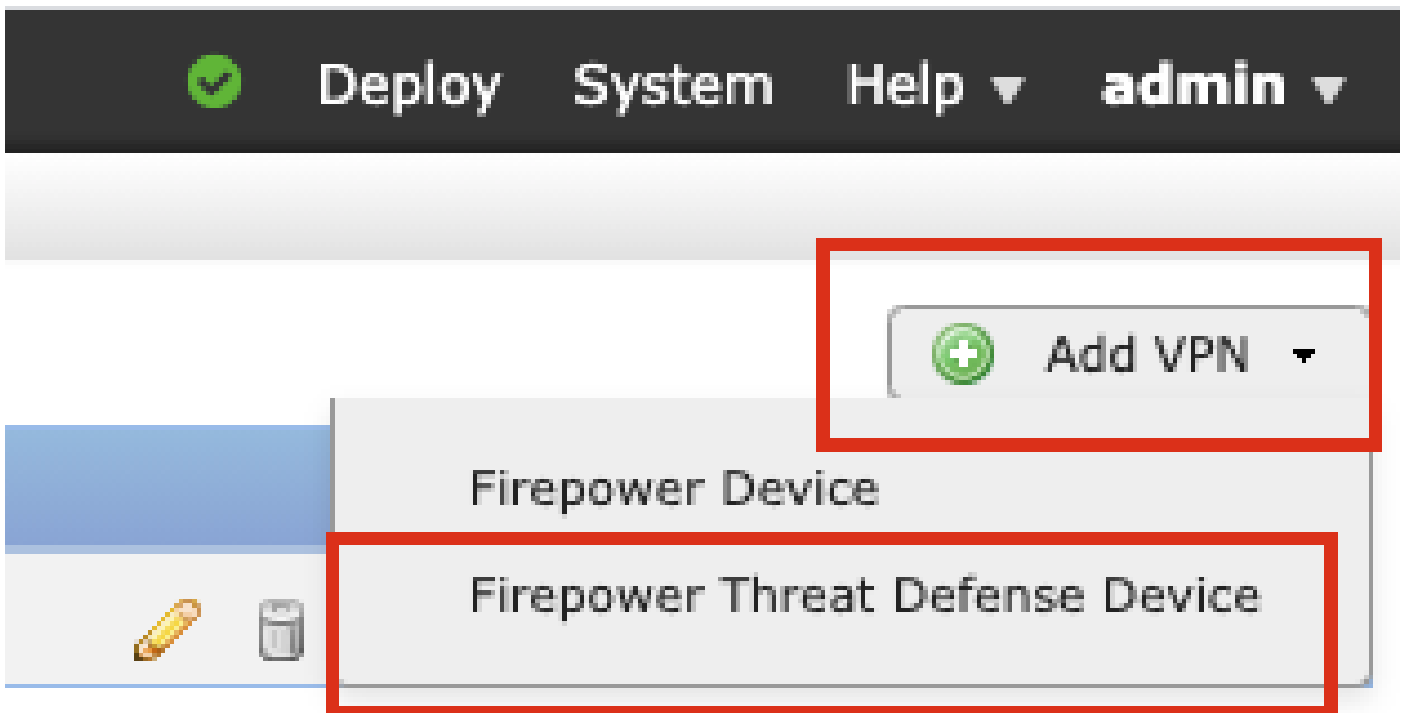
 Nota: No se necesitan licencias adicionales, la VPN basada en ruta se puede configurar en los modos con licencia y de evaluación. Sin cumplimiento de cifrado (funciones de exportación controladas habilitadas), sólo DES se puede utilizar como algoritmo de cifrado.

Pasos de configuración en FMC

Paso 1. Vaya a Dispositivos >VPN >Sitio a sitio.



Paso 2. Haga clic en Add VPN, y elija Firepower Threat Defence Device, como se muestra en la imagen.



Paso 3. Proporcione un nombre de topología y seleccione el tipo de VPN como basado en ruta (VTI). Elija la versión IKE.

A efectos de esta demostración, se entenderá por:

Nombre de topología: VTI-ASA

Versión IKE: IKEv2

Topology Name:*

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

IKE Version:* IKEv1 IKEv2

Paso 4. Elija el Dispositivo en el que debe configurarse el túnel, Puede elegir agregar una nueva Interfaz de plantilla virtual (haga clic en el icono +), o seleccione una de la lista que existe.

Endpoints | IKE | IPsec | Advanced

Node A

Device:*

Virtual Tunnel Interface:* [Edit VTI](#)

Tunnel Source IP is Private

Connection Type:*

Tunnel IP Address :
Tunnel Source Interface :
Tunnel Source Interface IP :

Node B

Device:*

Virtual Tunnel Interface:* [Edit VTI](#)

Tunnel Source IP is Private

Connection Type:*

Tunnel IP Address :
Tunnel Source Interface :
Tunnel Source Interface IP :

Paso 5. Defina los parámetros de la nueva interfaz de túnel virtual. Click OK.

A efectos de esta demostración, se entenderá por:

Nombre: VTI-ASA

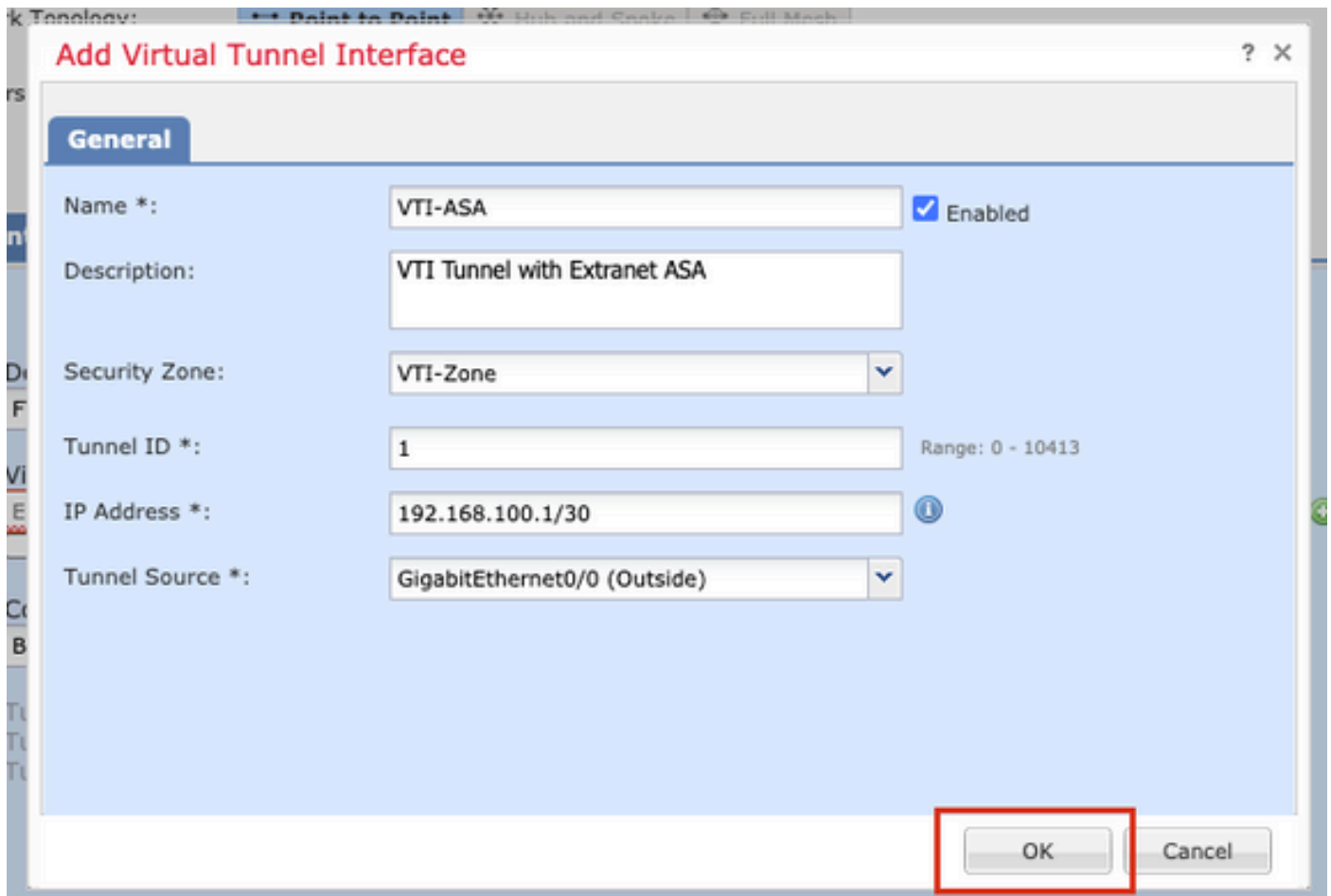
Descripción (opcional): Túnel VTI con Extranet ASA

Zona de seguridad: VTI-Zone

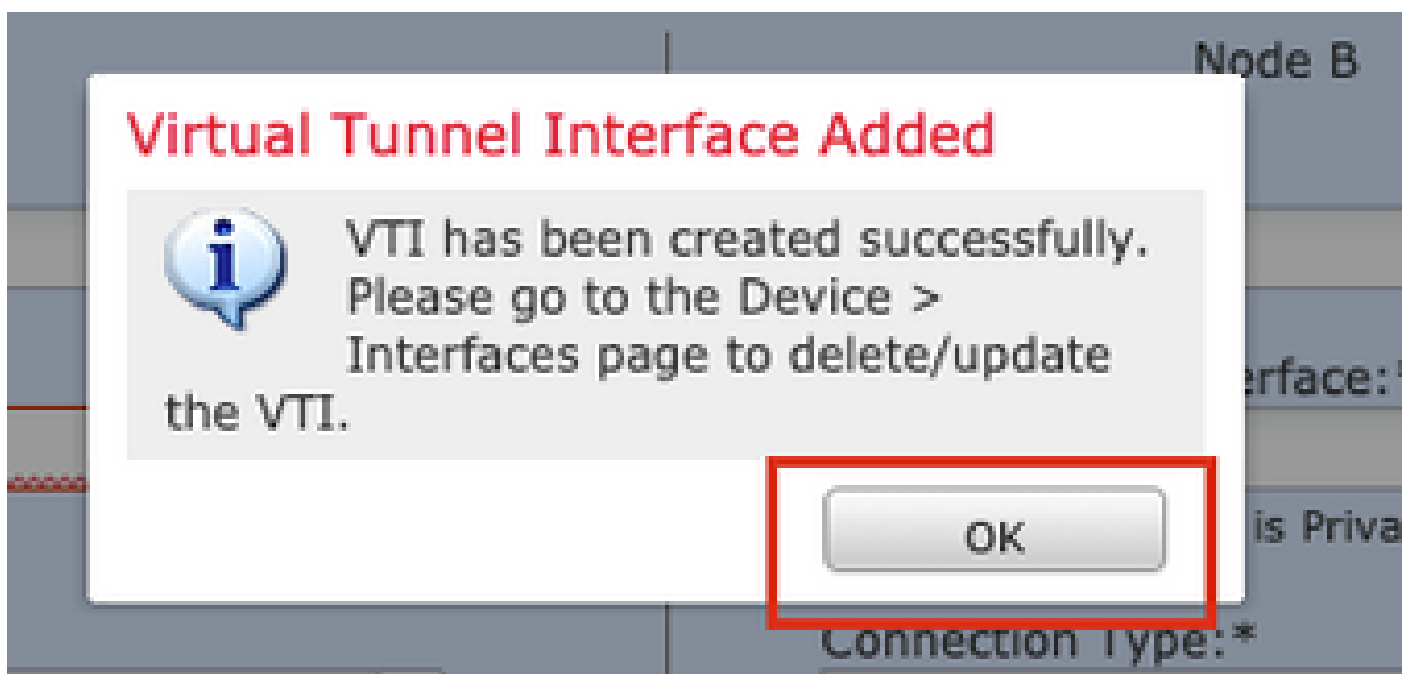
ID de túnel: 1

Dirección IP: 192.168.100.1/30

Fuente del túnel: GigabitEthernet0/0 (exterior)



Paso 6. Haga clic en OK en la ventana emergente que indica que se ha creado el nuevo VTI.



Paso 7. Elija el VTI recién creado o un VTI que exista en Virtual Tunnel Interface. Proporcione la información para el Nodo B (que es el dispositivo par).

A efectos de esta demostración, se entenderá por:

Dispositivo: Extranet

Nombre del dispositivo: ASA-Peer

Dirección IP del terminal: 10.106.67.252

Create New VPN Topology

Topology Name: *

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

IKE Version: * IKEv1 IKEv2

Endpoints | IKE | IPsec | Advanced

Node A

Device: *

Virtual Tunnel Interface: *

Tunnel Source IP is Private

Connection Type: *

Tunnel IP Address : 192.168.100.1
Tunnel Source Interface : Outside
Tunnel Source Interface IP : 10.197.224.90

Additional Configuration ⓘ
Route traffic to the VTI : [Routing Policy](#)
Permit VPN traffic : [AC Policy](#)

Node B


Device: *

Device Name: *

Endpoint IP Address: *

Paso 8. Vaya a la pestaña IKE. Puede optar por utilizar una directiva predefinida o hacer clic en el botón + situado junto a la pestaña Directiva y crear una nueva.

IKEv2 Settings

Policy:* AES-GCM-NULL-SHA-LATEST 

Authentication Type: Pre-shared Automatic Key

Pre-shared Key Length:* 24 Characters (Range 1-127)

Paso 9. (Opcional, si crea una nueva política IKEv2.) Proporcione un nombre para la política y seleccione los algoritmos que se utilizarán en la política. Click Save.

A efectos de esta demostración, se entenderá por:

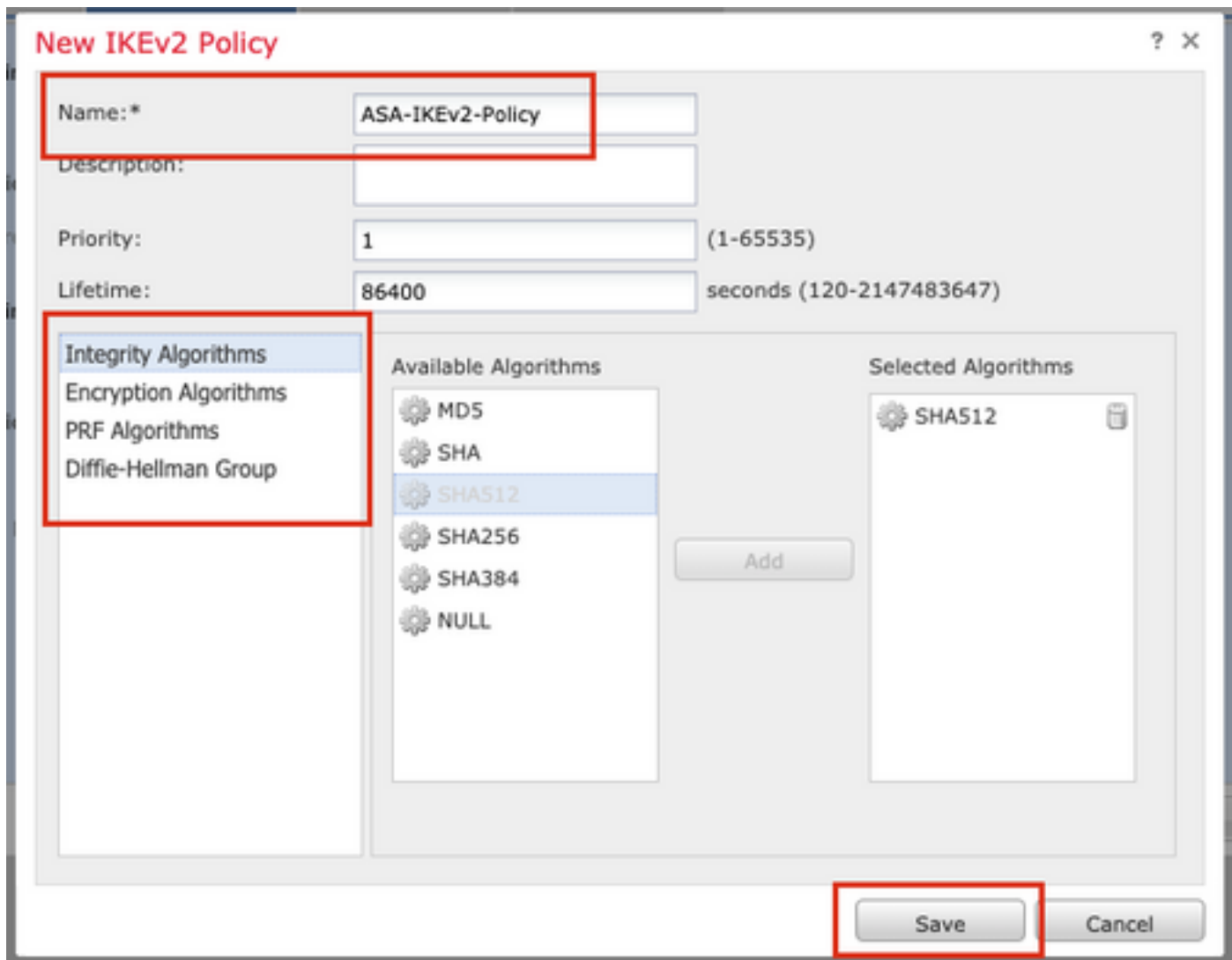
Nombre: ASA-IKEv2-Policy

Algoritmos de integridad: SHA-512

Algoritmos de cifrado: AES-256

Algoritmos PRF: SHA-512

Grupo Diffie-Hellman: 21



Paso 10. Elija el recién creado o la Política que existe. Seleccione el Tipo de autenticación. Si se utiliza una clave manual precompartida, especifíquela en los cuadros Key y Confirm Key.

A efectos de esta demostración, se entenderá por:

Política: ASA-IKEv2-Policy

Tipo de autenticación: clave manual previamente compartida

Clave: cisco123

Confirmar clave: cisco123

Endpoints **IKE** IPsec Advanced

IKEv1 Settings

Policy:* preshared_sha_aes256_dh14_3 [v] [⊕]

Authentication Type: Pre-shared Automatic Key [v]

Pre-shared Key Length:* 24 Characters (Range 1-127)

IKEv2 Settings


Policy:* ASA-IKEv2-Policy [v] [⊕]

Authentication Type: Pre-shared Manual Key [v]

Key:* [.....]

Confirm Key:* [.....]

Enforce hex-based pre-shared key only



 Nota: Si ambos terminales están registrados en el mismo FMC, también se puede utilizar la opción de clave automática precompartida.

Paso 11. Vaya a la pestaña IPsec. Puede optar por utilizar una propuesta IPsec IKEv2 predefinida o crear una nueva. Haga clic en el botón Editar situado junto a la ficha Propuesta IKEv2 IPsec.

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel [v]

Transform Sets:

IKEv1 IPsec Proposals  IKEv2 IPsec Proposals* 

tunnel_aes256_sha AES-GCM

Enable Security Association (SA) Strength Enforcement

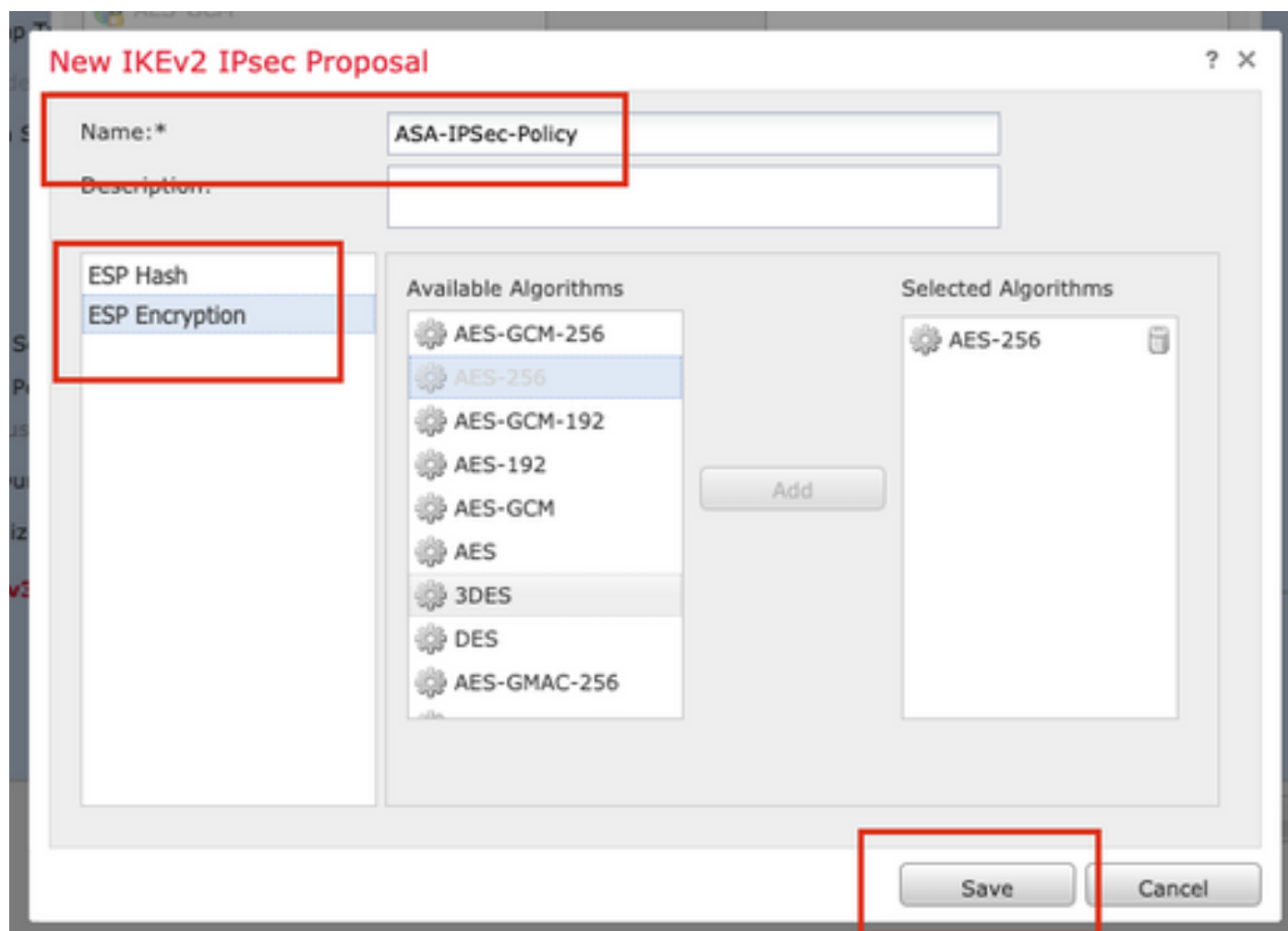
Paso 12. (Opcional, si crea una nueva propuesta IKEv2 IPsec.) Proporcione un nombre para la propuesta y seleccione los algoritmos que se utilizarán en la propuesta. Click Save.

A efectos de esta demostración, se entenderá por:

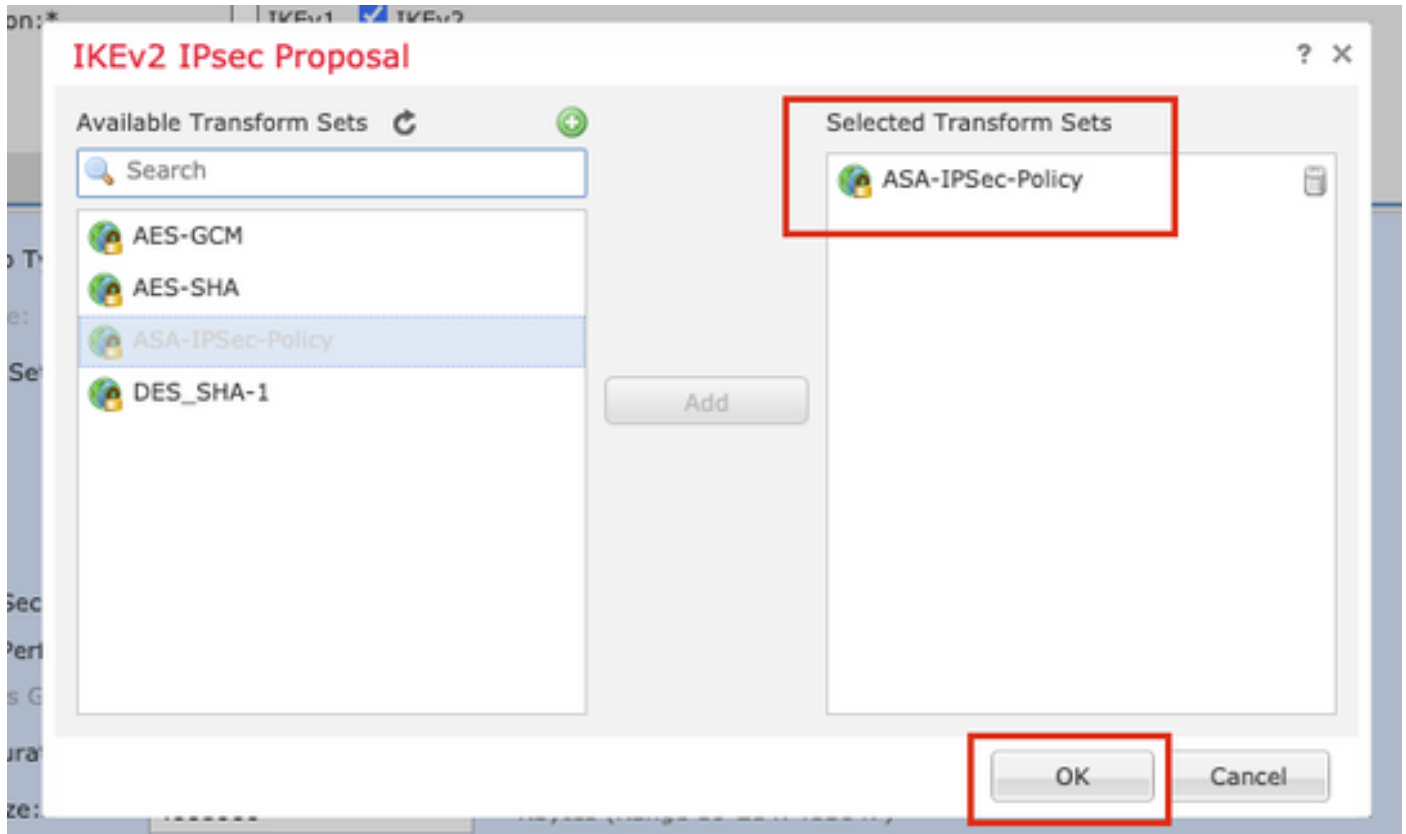
Nombre: ASA-IPSec-Policy

Hash ESP: SHA-512

Cifrado ESP: AES-256



Paso 13. Elija la Propuesta o la Propuesta recién creada que exista en la lista de propuestas disponibles. Click OK.



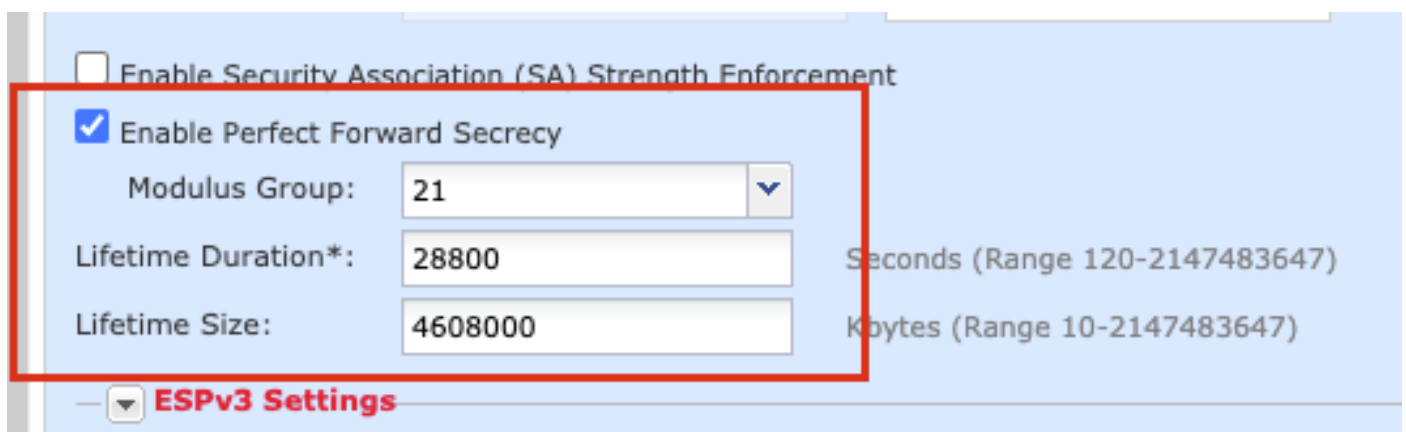
Paso 14. (Opcional) Elija la configuración Perfect Forward Secrecy. Configuración de la duración y el tamaño de la vida útil de IPsec.

A efectos de esta demostración, se entenderá por:

Confidencialidad directa perfecta: grupo de módulos 21

Duración de la vida útil: 28800 (Predeterminado)

Tamaño de vida útil: 4608000 (predeterminado)



Paso 15. Compruebe los parámetros configurados. Haga clic en Save, como se muestra en esta imagen.

Topology Name:*

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

IKE Version:* IKEv1 IKEv2

Endpoints IKE **IPsec** Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode:

Transform Sets:

IKEv1 IPsec Proposals	IKEv2 IPsec Proposals*
tunnel_aes256_sha	ASA-IPSec-Policy

Enable Security Association (SA) Strength Enforcement

Enable Perfect Forward Secrecy


Modulus Group:

Lifetime Duration*: Seconds (Range 120-2147483647)

Lifetime Size: Kbytes (Range 10-2147483647)

ESPv3 Settings

Paso 16. Configure la política de control de acceso. Vaya a Políticas > Control de acceso > Control de acceso. Edite la política aplicada al FTD.

 Nota: sysopt connection permit-vpn no funciona con túneles VPN basados en ruta. Las reglas de control de acceso deben configurarse para las zonas IN-> OUT y OUT -> IN.

Proporcione las Zonas de Origen y las Zonas de Destino en la pestaña Zonas .

Proporcione Redes de origen, Redes de destino en la pestaña Redes. Haga clic en Add (Agregar).

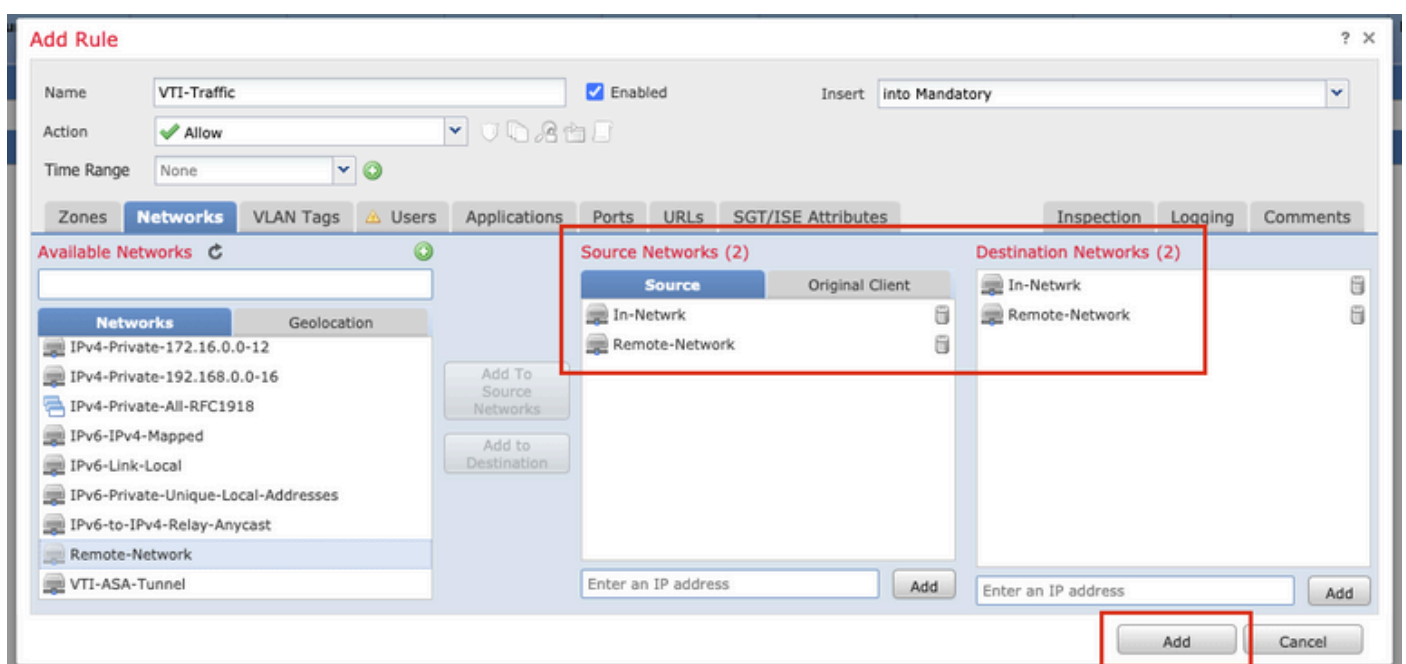
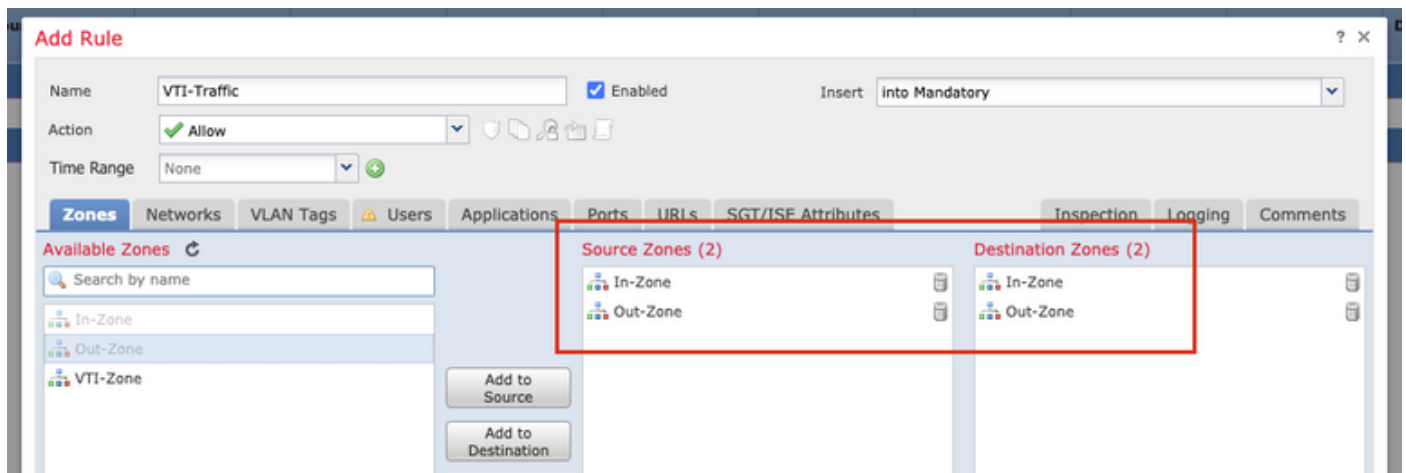
A efectos de esta demostración, se entenderá por:

Zonas de origen: zona interna y zona externa

Zonas de destino: zona externa e interna

Redes de origen: en red y red remota

Redes de destino: redes remotas e internas



Paso 17. Agregue el ruteo sobre el túnel VTI. Vaya a Devices > Device Management. Edite el dispositivo en el que está configurado el túnel VTI.

Vaya a Static Route en la pestaña Routing. Haga clic en Agregar ruta.

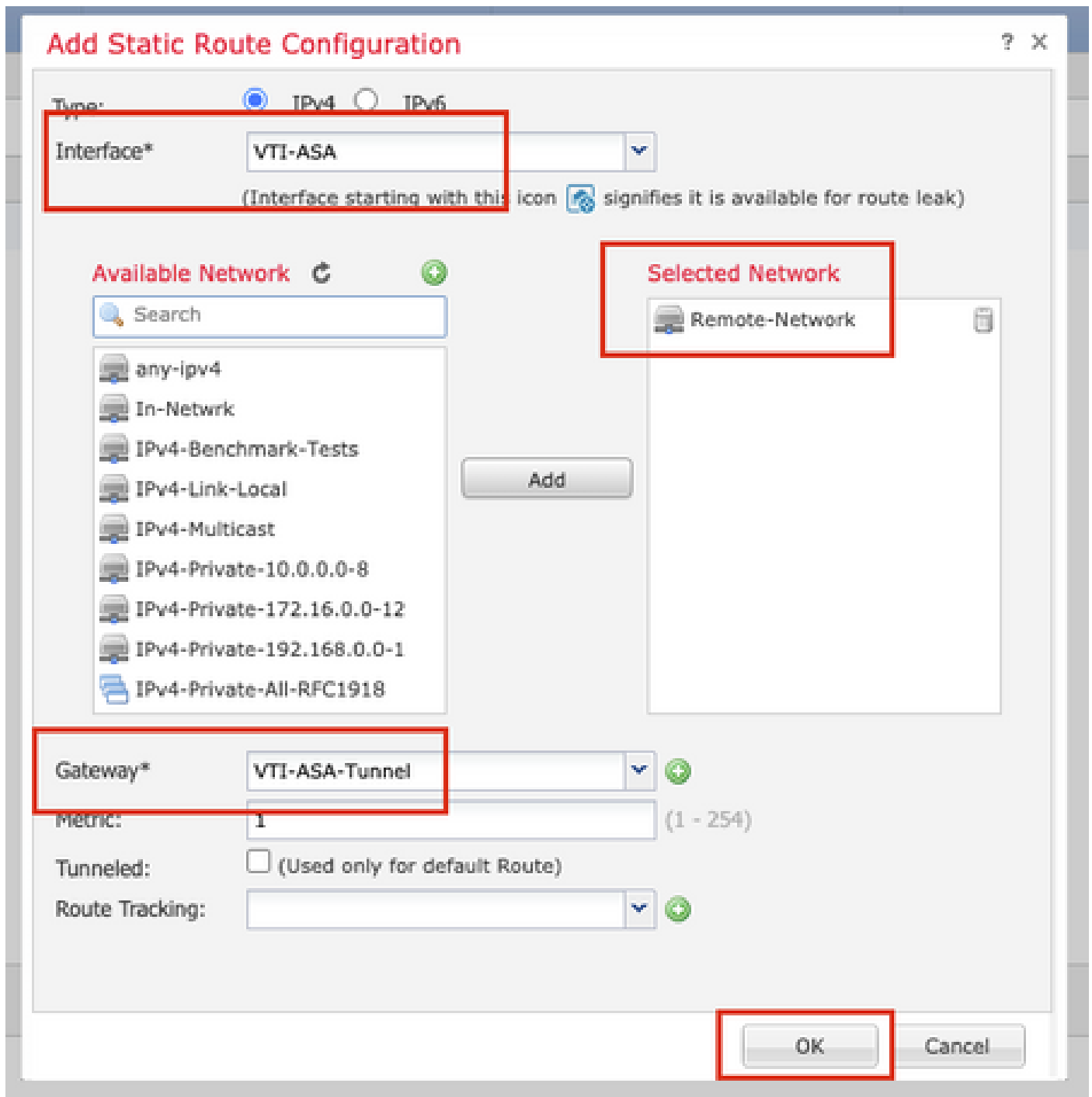
Proporcione la interfaz, elija la red, proporcione la puerta de enlace. Click OK.

A efectos de esta demostración, se entenderá por:

Interfaz: VTI-ASA

Red: Red remota

Puerta de enlace: Túnel VTI-ASA



Paso 18. Vaya a Deploy > Deployment. Elija el FTD en el que debe implementarse la configuración y haga clic en Deploy.

Configuración enviada a la CLI de FTD después de una implementación correcta:

```
<#root>
```

```
crypto ikev2 policy 1
```

```
encryption aes-256  
integrity sha512  
group 21  
prf sha512  
lifetime seconds 86400
```

```

crypto ikev2 enable Outside

crypto ipsec ikev2 ipsec-proposal CSM_IP_1

    protocol esp encryption aes-256
    protocol esp integrity sha-512

crypto ipsec profile FMC_IPSEC_PROFILE_1

    set ikev2 ipsec-proposal CSM_IP_1
    set pfs group21

group-policy .DefaultS2SGroupPolicy internal
group-policy .DefaultS2SGroupPolicy attributes
    vpn-idle-timeout 30
    vpn-idle-timeout alert-interval 1
    vpn-session-timeout none
    vpn-session-timeout alert-interval 1
    vpn-filter none
    vpn-tunnel-protocol ikev1 ikev2

tunnel-group 10.106.67.252 type ipsec-l2l
tunnel-group 10.106.67.252 general-attributes
    default-group-policy .DefaultS2SGroupPolicy
tunnel-group 10.106.67.252 ipsec-attributes
    ikev2 remote-authentication pre-shared-key *****
    ikev2 local-authentication pre-shared-key *****

interface Tunnel1

    description VTI Tunnel with Extranet ASA
    nameif VTI-ASA

    ip address 192.168.100.1 255.255.255.252
    tunnel source interface Outside
    tunnel destination 10.106.67.252
    tunnel mode ipsec ipv4

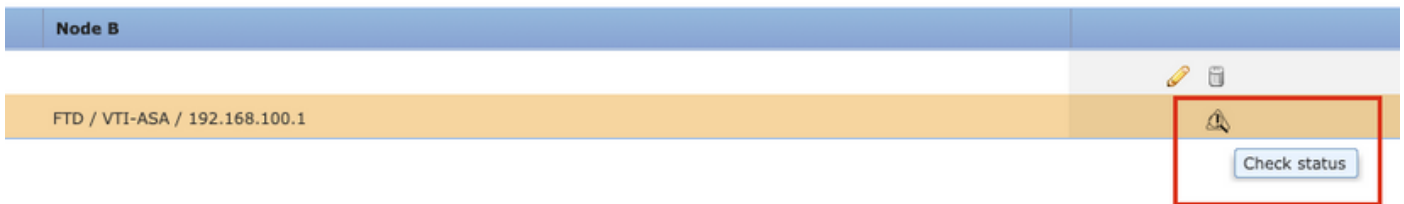
    tunnel protection ipsec profile FMC_IPSEC_PROFILE_1

```

Verificación

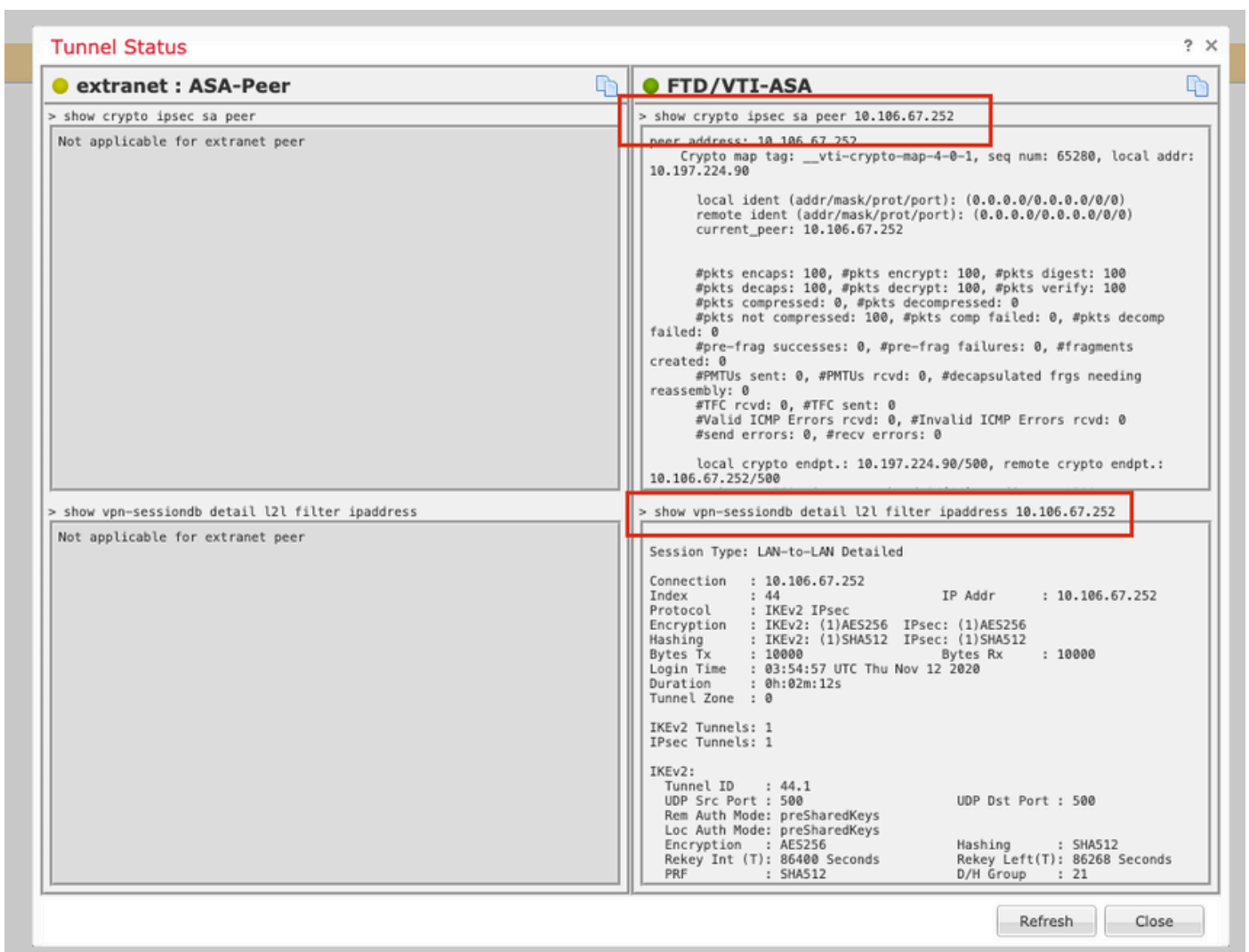
Desde la GUI de FMC

Haga clic en la opción Check Status para monitorear el estado en vivo del túnel VPN desde la propia GUI



Esto incluye estos comandos tomados de la CLI de FTD:

- show crypto ipsec sa peer <Peer IP Address>
- show vpn-sessiondb detail l2l filter ipaddress <Peer IP Address>



Desde CLI de FTD

Estos comandos se pueden utilizar desde la CLI de FTD para ver la configuración y el estado de los túneles VPN.

```
show running-config crypto
show running-config nat
```

```
show running-config route
show crypto ikev1 sa detailed
show crypto ikev2 sa detailed
show crypto ipsec sa detailed
show vpn-sessiondb detail 121
```

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).