ASDM 6.4: Túnel del VPN de sitio a sitio con el ejemplo de configuración IKEv2

Contenido

Introducción

Este documento describe cómo configurar un túnel VPN de sitio a sitio entre dos Cisco Adaptive Security Appliances (ASA) mediante la versión 2 del Intercambio de claves de Internet (IKE). Describe los pasos que se han seguido para configurar el túnel VPN mediante un Asistente de GUI de Adaptive Security Device Manager (ASDM).

prerrequisitos

Requisitos

Aseegurese que Cisco ASA se ha configurado con las configuraciones básicas.

Componentes Utilizados

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

- Dispositivos de seguridad adaptable Cisco ASA de la serie 5500 que funciona con la versión de software 8.4 y posterior
- Versión 6.4 y posterior del software ASDM de Cisco

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

IKEv2, es una mejora al protocolo existente IKEv1 que incluye estas ventajas:

- Menos intercambios del mensaje entre los pares IKE
- Métodos de autenticación unidireccional
- Soporte incorporado para el Dead Peer Detection (DPD) y el NAT-Traversal
- Uso del Protocolo de Autenticación Extensible (EAP) para la autenticación
- Elimina el riesgo de ataques simples DOS usando los Cookie antiobstrucción

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

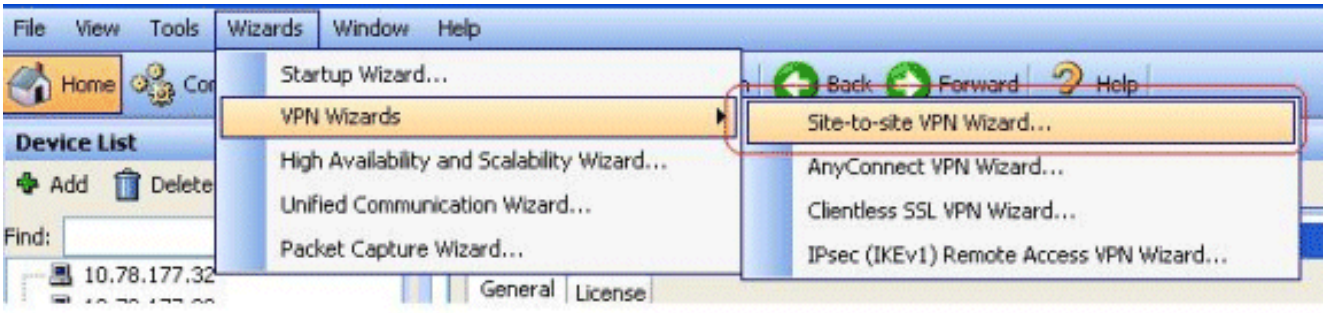
Este documento muestra la configuración del túnel del VPN de sitio a sitio en HQ-ASA. Lo mismo se podían seguir que un espejo en el BQ-ASA.

Configuración de ASDM en HQ-ASA

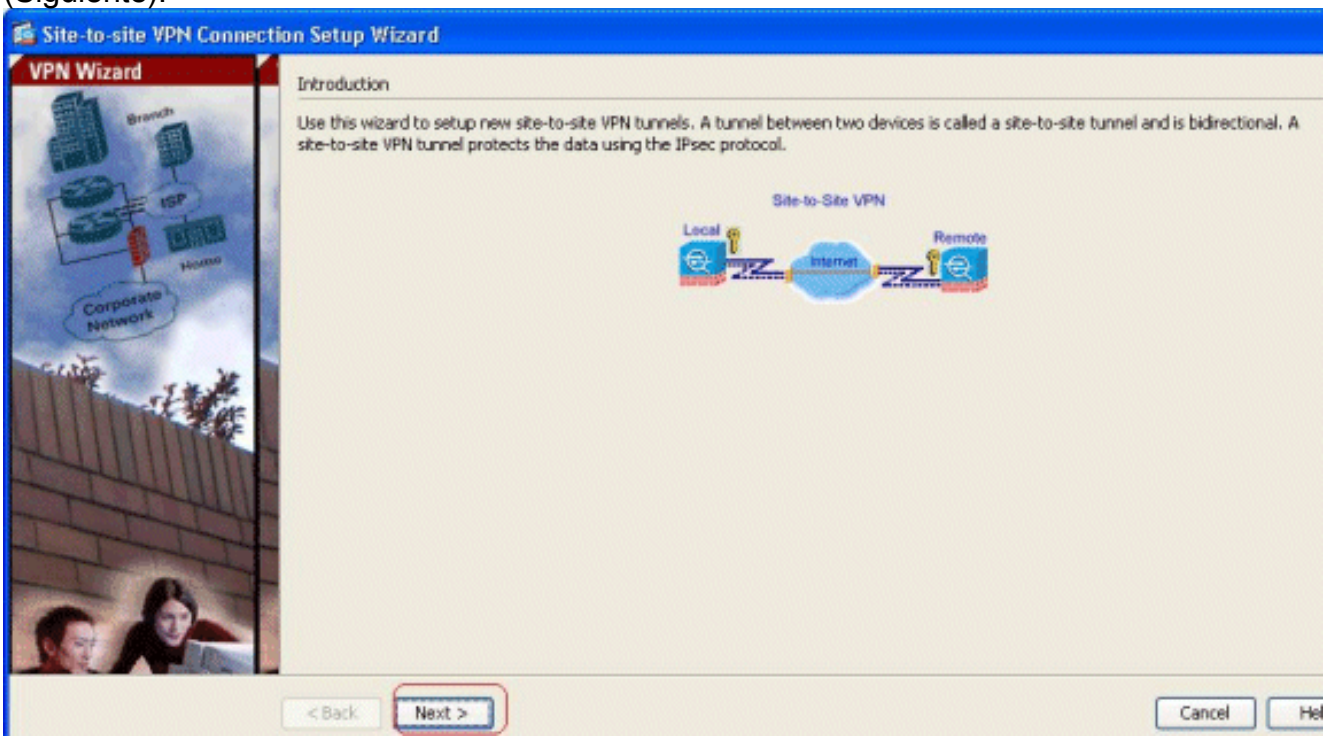
Este túnel VPN se podía configurar usando un Asisitente fácil de usar GUI.

Complete estos pasos:

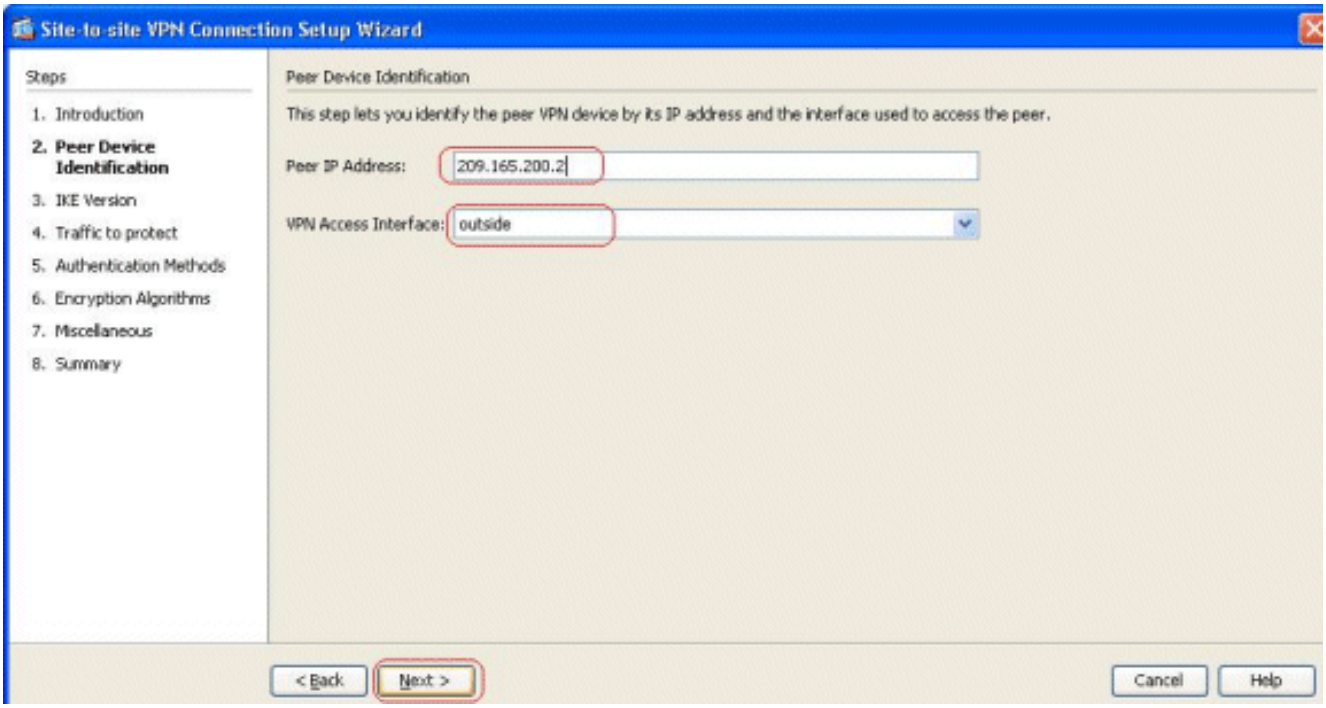
1. Inicie sesión al ASDM, y vaya a los **Asisitente >** a los **Asistentes VPN >** al **Asisitente del VPN de sitio a sitio**.



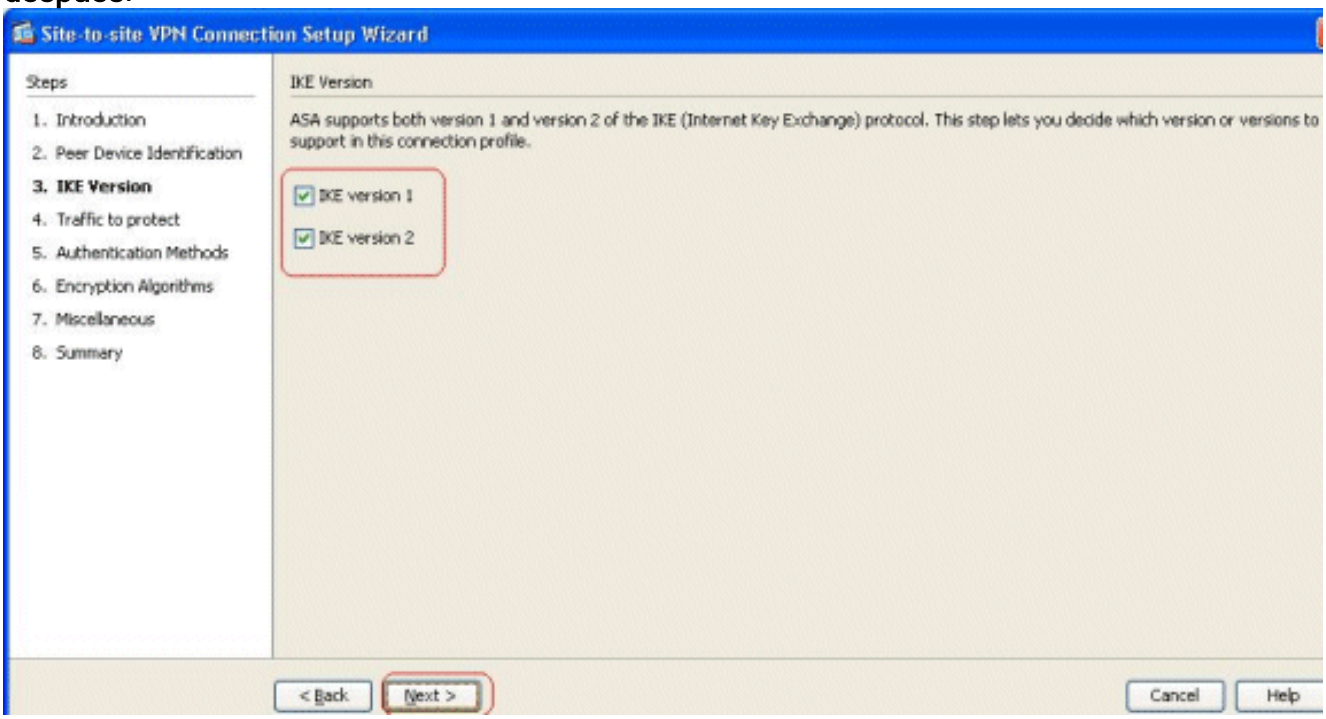
2. Una ventana de la configuración de conexión del VPN de sitio a sitio aparece. Haga clic en Next (Siguiente).



3. Especifique el IP Address de Peer y la interfaz de acceso VPN. Haga clic en Next (Siguiente).

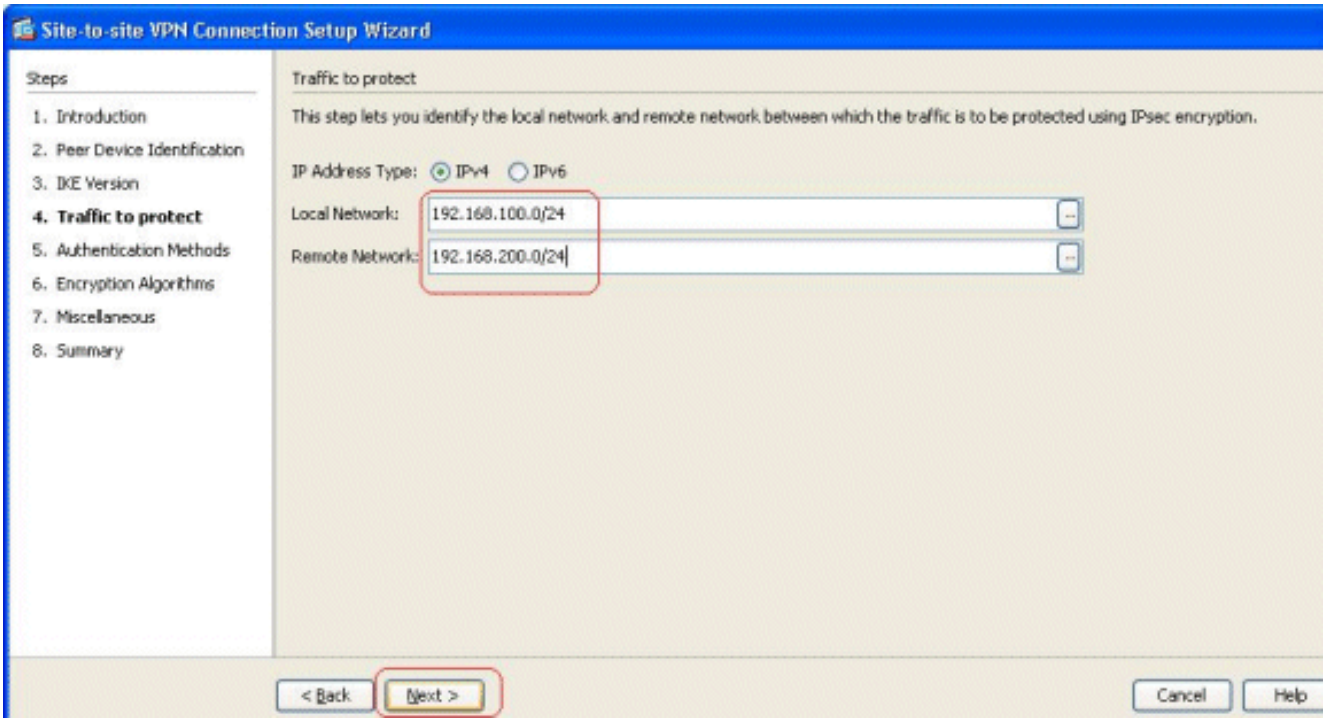


4. Seleccione ambas versiones IKE, y haga clic **después**.

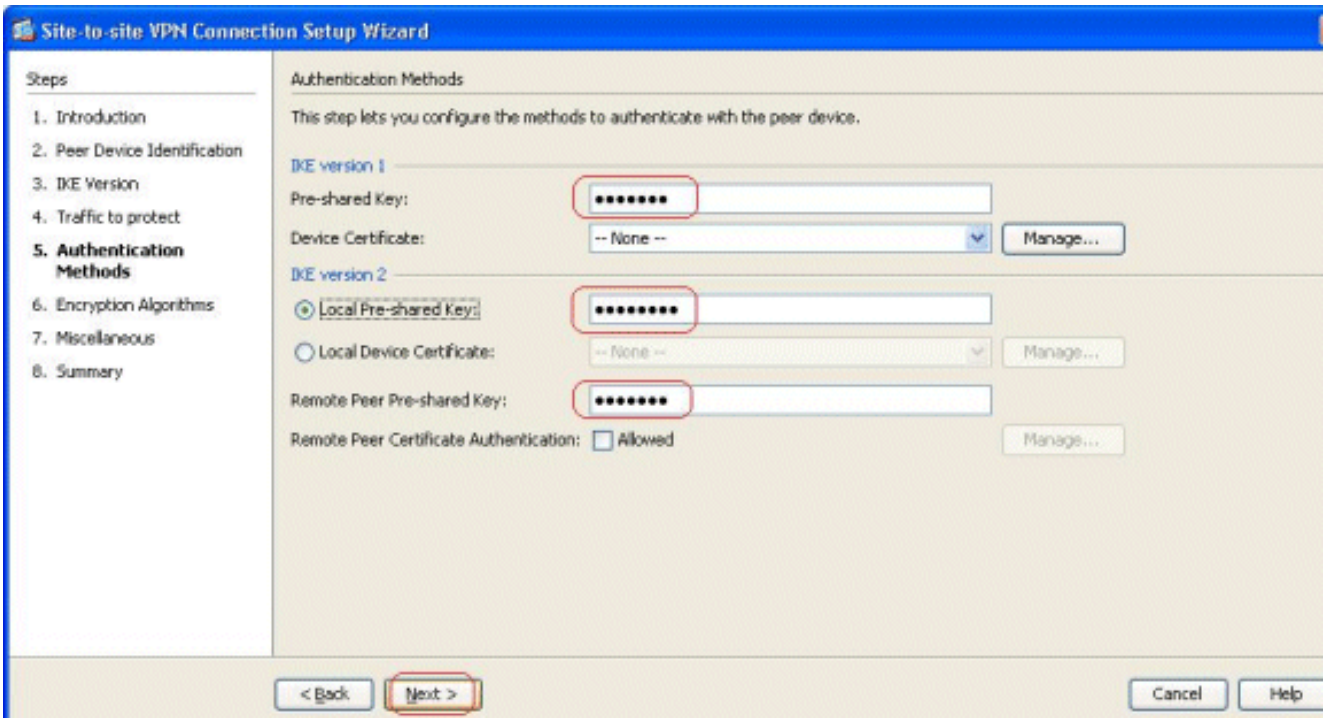


Nota: Ambas versiones del IKE se configuran aquí porque el iniciador podría tener un respaldo de IKEv2 a IKEv1 cuando IKEv2 falla.

5. Especifique la red local y la red remota para cifrar y esté pasado el tráfico entre estas redes a través del túnel VPN. Haga clic en Next (Siguiente).



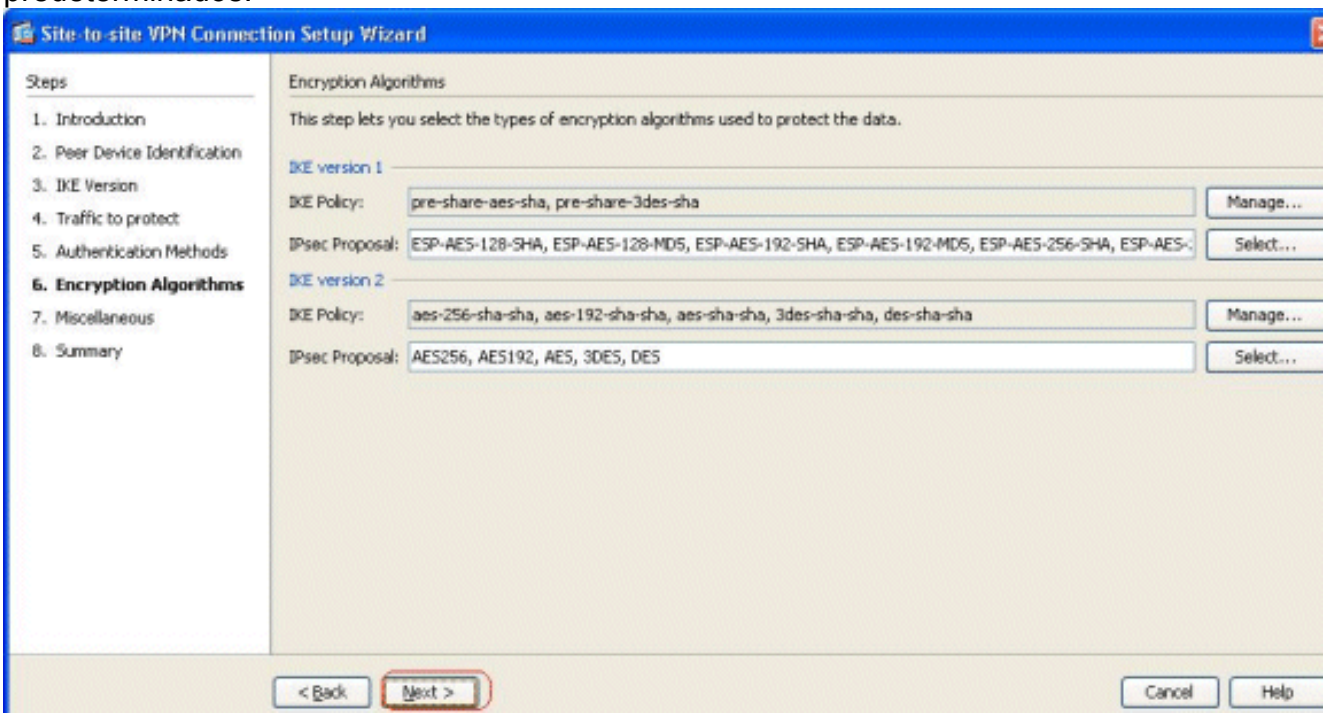
6. Especifique las claves previamente compartidas para ambas versiones del IKE.



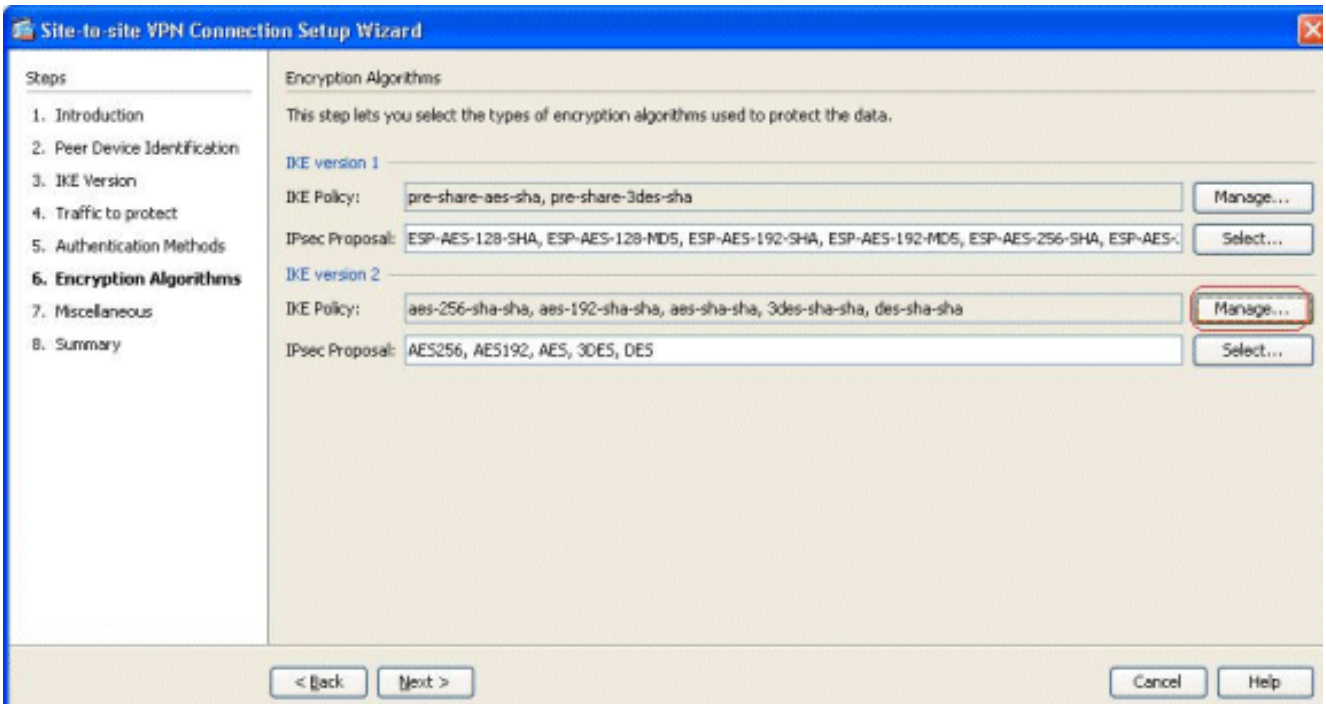
La diferencia principal entre las mentiras de las versiones 1 y 2 IKE en términos de método de autentificación que permiten. IKEv1 permite solamente un tipo de autenticación en ambos extremos VPN (es decir, clave previamente compartida o certificado). Sin embargo, IKEv2 permite que los métodos de autentificación asimétricos sean configurados (es decir, autenticación de la clave previamente compartida para el terminal original, pero autenticación certificada para el respondedor) usando el local separado y la autenticación remota CLI.Además, usted puede tener diversas claves previamente compartidas en los ambos extremos. La clave previamente compartida local en el extremo HQ-ASA se convierte en la clave previamente compartida remota en el extremo BQ-ASA. Asimismo, la clave previamente compartida remota en el extremo HQ-ASA se convierte en la clave previamente compartida local en el extremo BQ-ASA.

7. Especifique los algoritmos de encripción para ambas versiones 1 y 2. IKE. Aquí, se validan

los valores predeterminados:

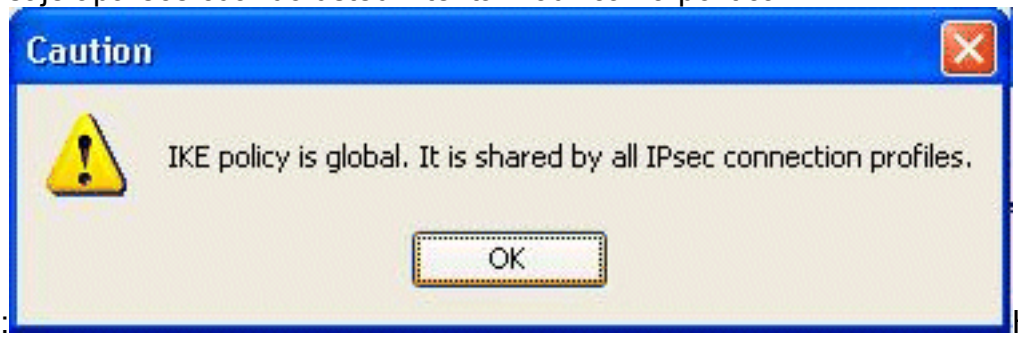


8. El tecleo **maneja…** para modificar la política IKE.



Nota: La política IKE en IKEv2 es sinónima a la **política isakmp** en IKEv1.**La oferta del IPSec** en IKEv2 es sinónima a la **transformación fijada** en IKEv1.

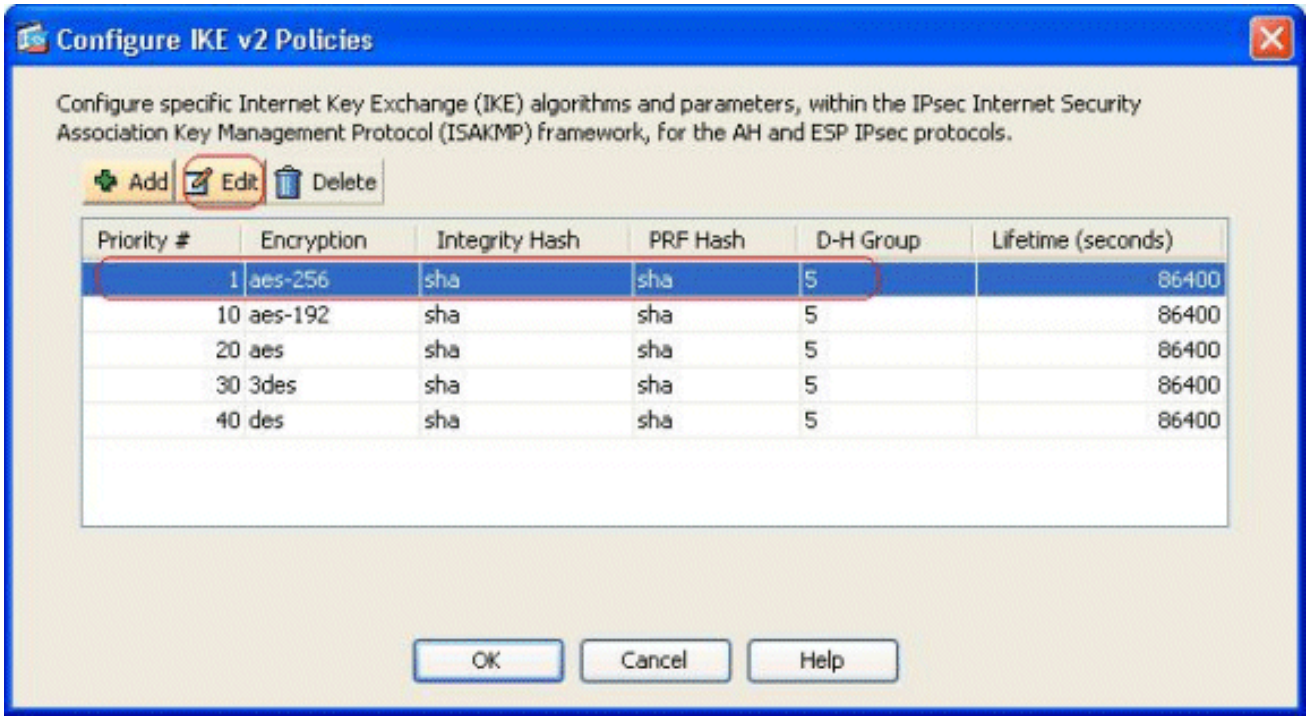
9. Este mensaje aparece cuando usted intenta modificar la política existente:



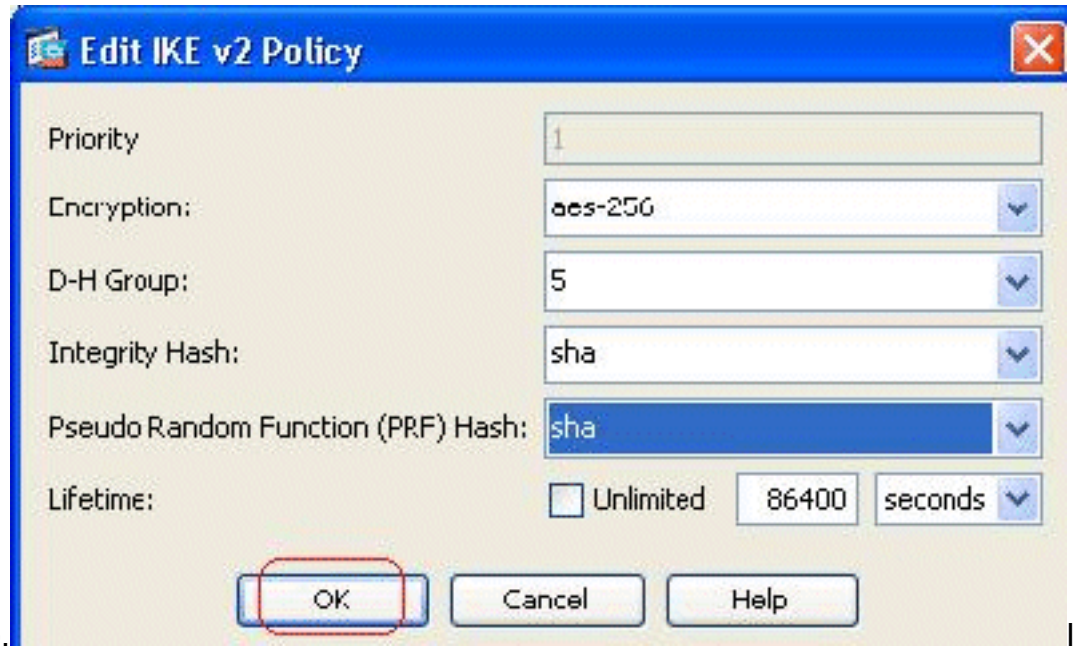
Haga Click

en OK para proceder.

10. Seleccione la política IKE especificada, y el tecleo **edita**.

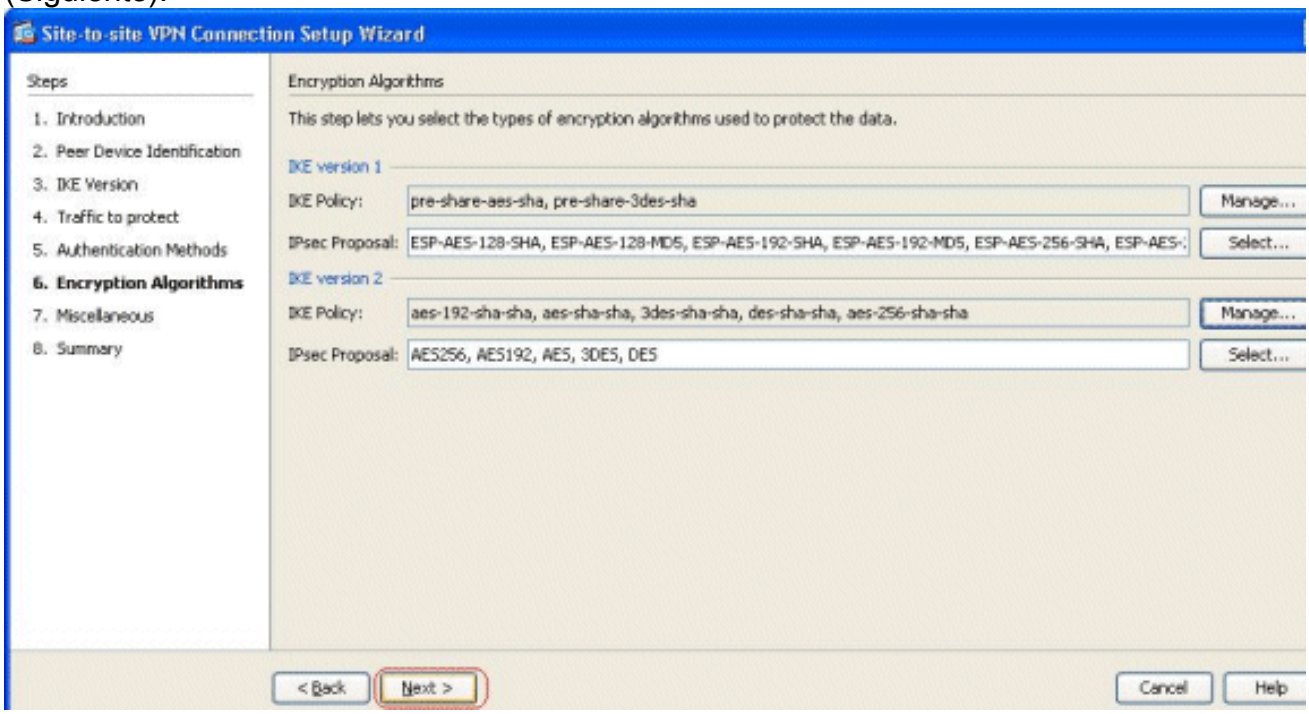


11. Usted puede modificar los parámetros tales como prioridad, cifrado, grupo del D-H, hash de la integridad, los valores de hash PRF, y de curso de la vida. Haga Click en OK cuando está acabado.

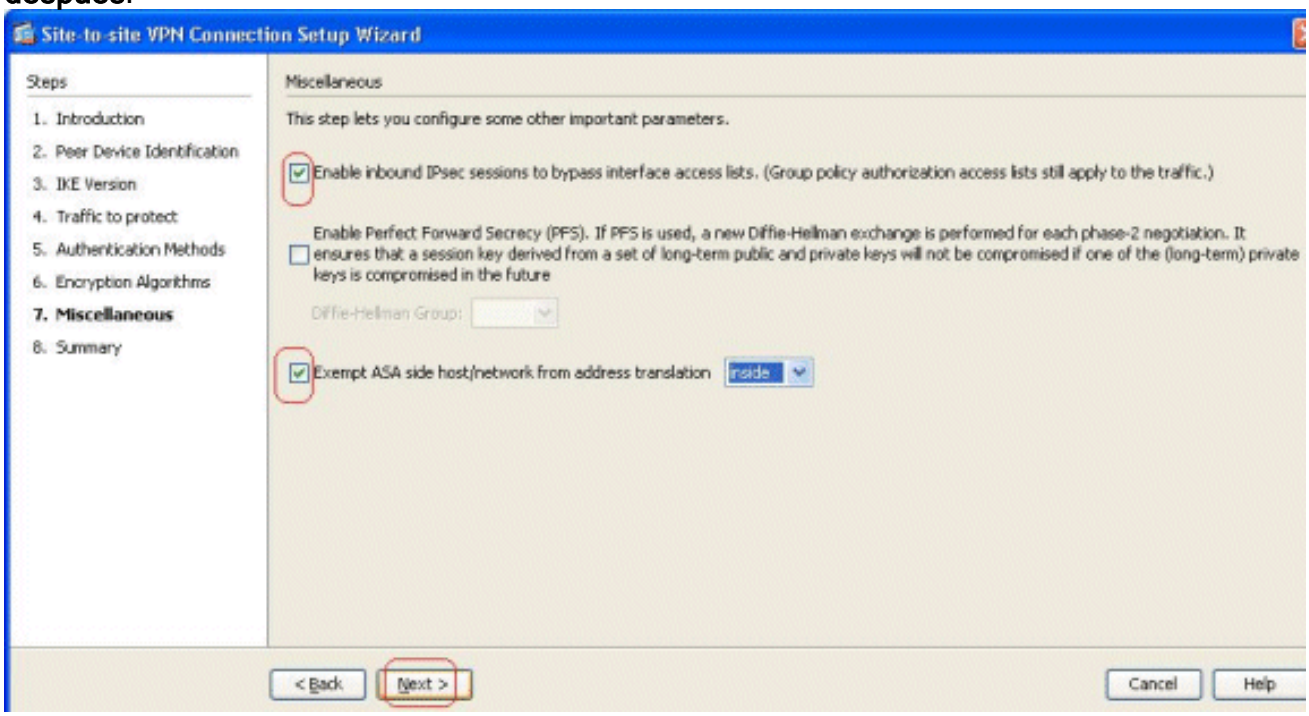


IKEv2 permite para que el algoritmo de la integridad sea negociado por separado del pseudo algoritmo al azar de la función (PRF). Esto se podía configurar en la política IKE con las opciones disponibles actuales que eran SHA-1 o MD5.Usted no puede modificar los parámetros de la oferta del IPSec que se definen por abandono. Tecleo **selecto** al lado del campo de la oferta del IPSec para agregar los nuevos parámetros. La diferencia principal entre IKEv1 e IKEv2, en términos de ofertas del IPSec, es que IKEv1 valida la transformación fijada en términos de combinaciones de cifrado y de algoritmos de autenticación. IKEv2 valida los parámetros del cifrado y de la integridad individualmente, y finalmente hace todo el posible O combinaciones de éstos. Usted podría ver éstos en el extremo de este Asisitente, en la diapositiva sumaria.

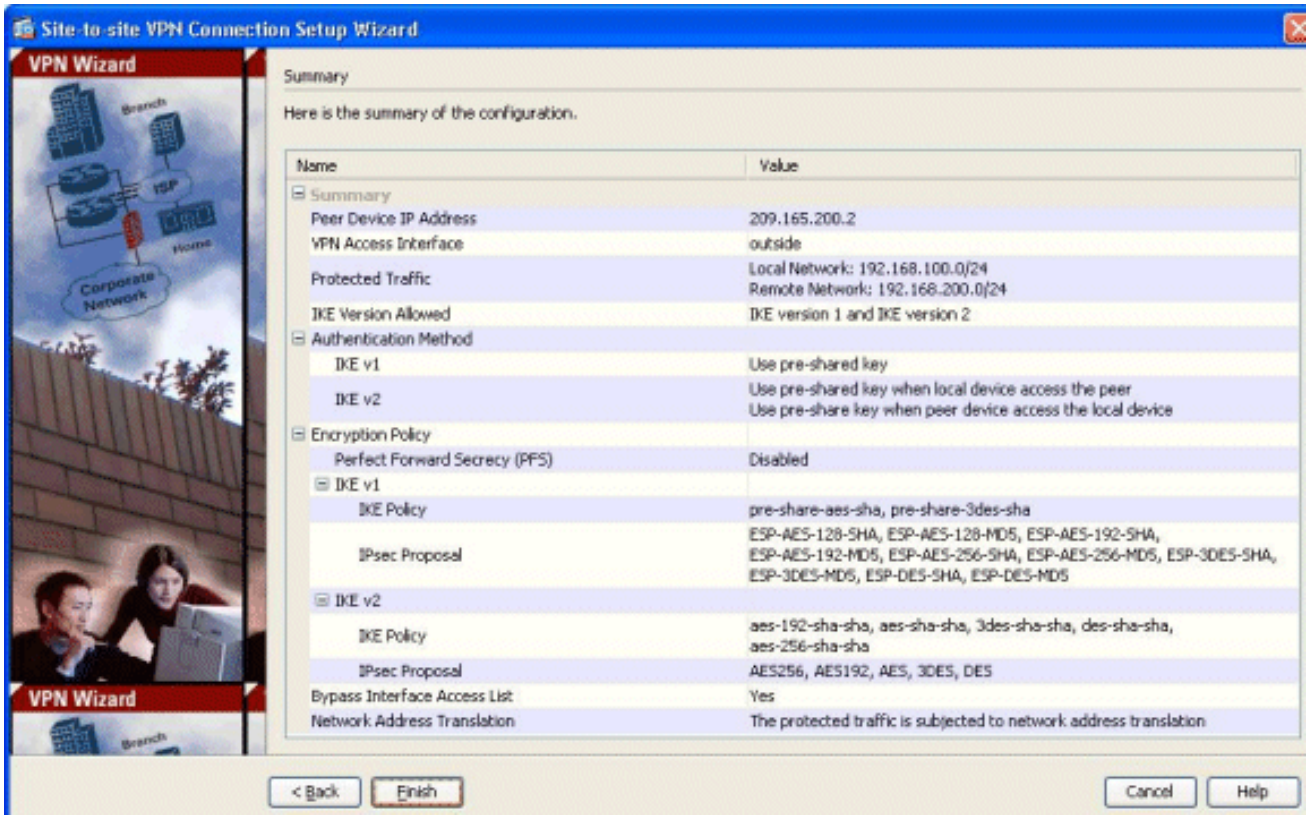
12. Haga clic en Next (Siguiente).



13. Especifique los detalles, tales como exención de NAT, PFS, y desviar de la interfaz ACL. Elija **después**.



14. Un resumen de la configuración se puede considerar aquí:



Clic en Finalizar para completar al Asisitente del túnel del VPN de sitio a sitio. Un perfil de la nueva conexión se crea con los parámetros configurados.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- muestre ikev2 crypto sa - Visualiza IKEv2 la base de datos tiempo de ejecución SA.
- muestre el detalle l2l de VPN-sessiondb - Visualiza la información sobre las sesiones del VPN de sitio a sitio.

Troubleshooting

Comandos para resolución de problemas

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- debug crypto ikev2 - Mensajes del **debug de las** demostraciones para IKEv2.

Información Relacionada

- Soporte técnico de los dispositivos de las 5500 Series de Cisco ASA
- Soporte Técnico y Documentación - Cisco Systems