Ejemplo de Configuración de IKEv1/IPsec Dinámico a Estático de ASA a ASA

Contenido

Introducción

Este documento describe cómo habilitar Adaptive Security Appliance (ASA) para que acepte conexiones VPN dinámicas IPsec de sitio a sitio desde cualquier peer dinámico (ASA en este caso). Como muestra el Diagrama de red en este documento, el túnel IPsec se establece cuando el túnel se inicia solamente desde el extremo Remote-ASA. El ASA central no puede iniciar un túnel VPN debido a la configuración IPsec dinámica. Se desconoce la dirección IP de Remote-ASA.

Configure Central-ASA para aceptar dinámicamente las conexiones de una dirección IP comodín (0.0.0.0/0) y una clave previamente compartida comodín. A continuación, el ASA remoto se configura para cifrar el tráfico de las subredes de ASA local a Central según lo especificado por la lista de acceso crypto. Ambos lados realizan la exención de traducción de direcciones de red (NAT) para eludir la NAT para el tráfico IPsec.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

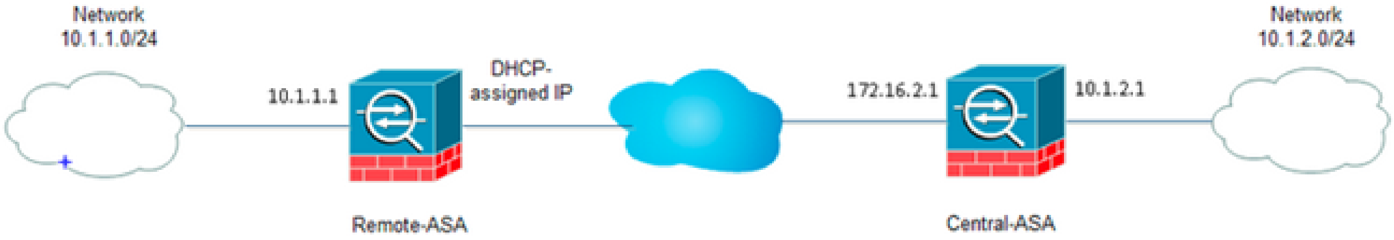
La información de este documento se basa en el software de firewall Cisco ASA (5510 y 5520) versión 9.x y posteriores.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

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

Diagrama de la red

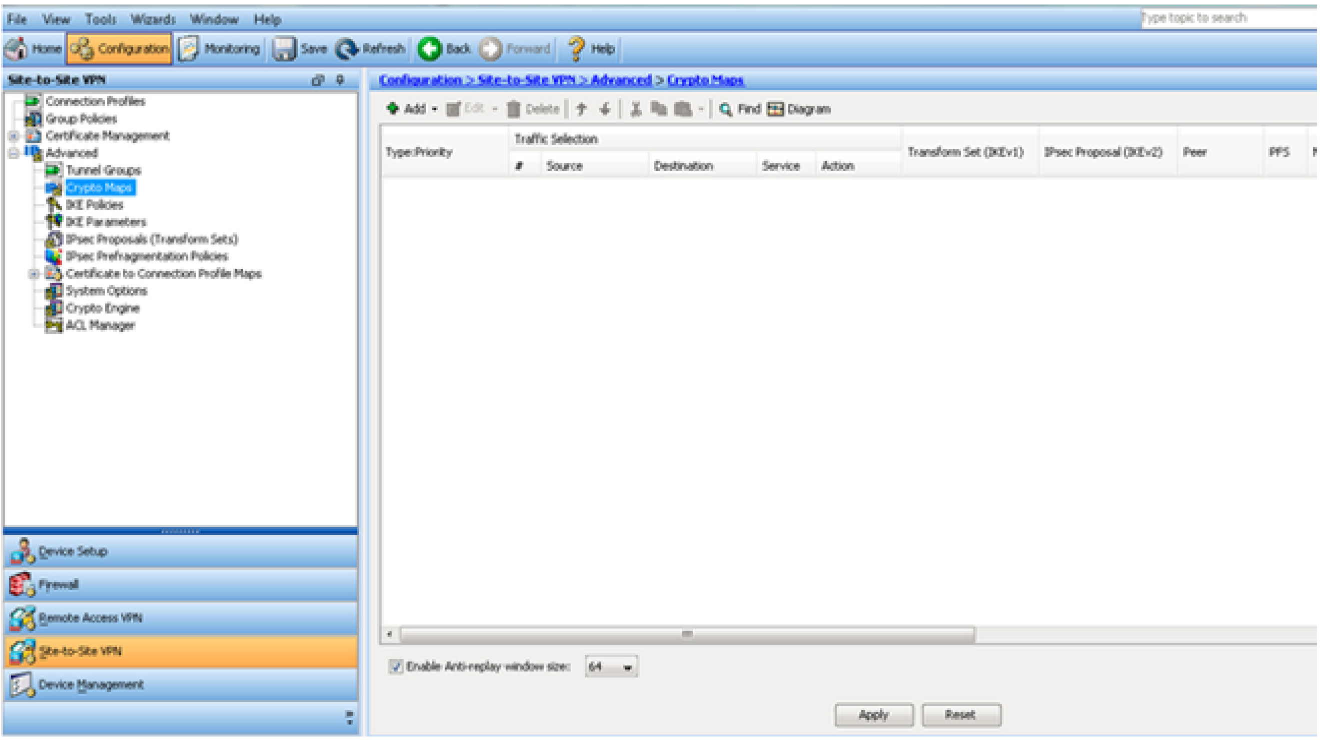


Configuración de ASDM

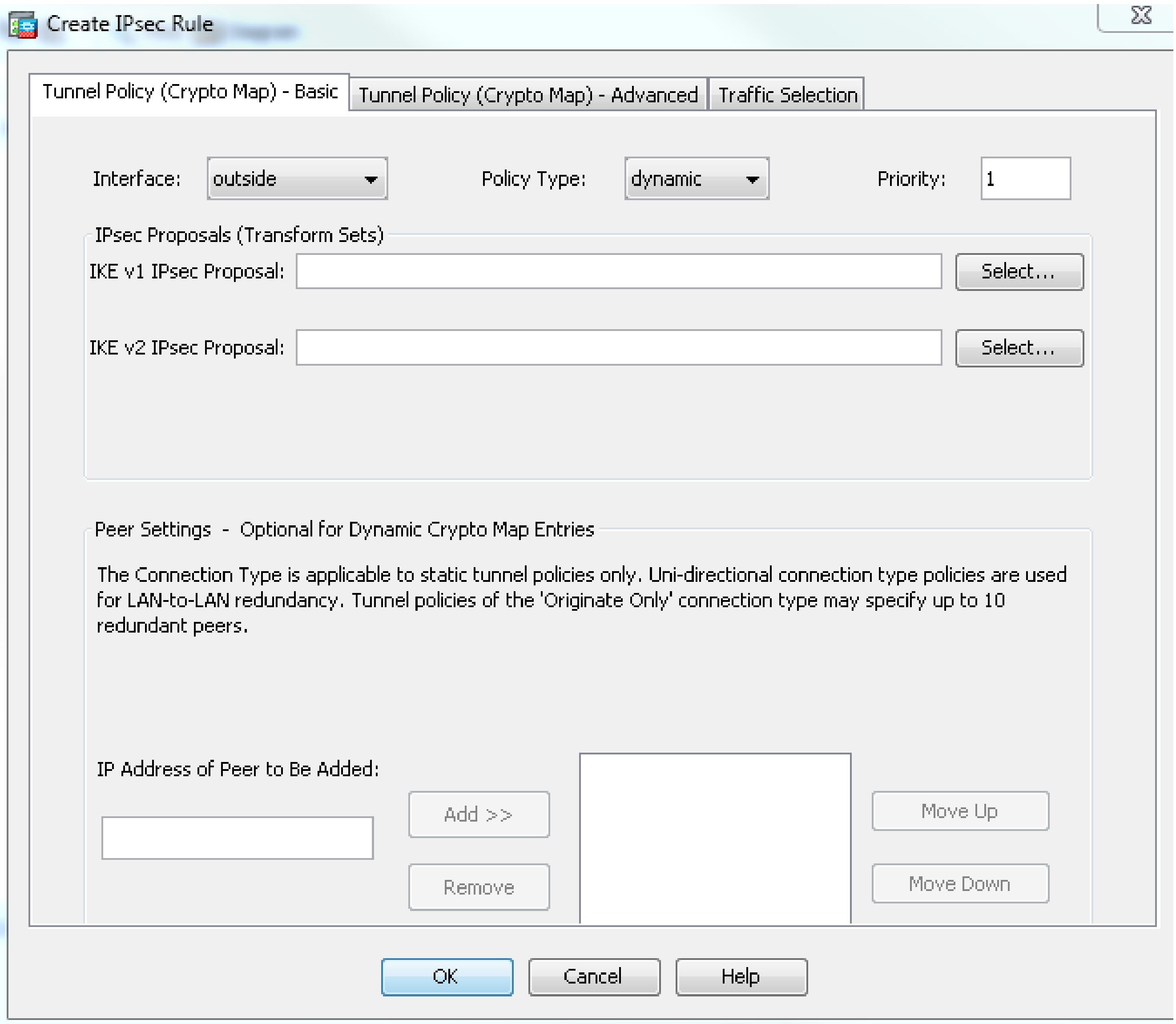
ASA central (par estático)

En un ASA con una dirección IP estática, configure la VPN de tal manera que acepte conexiones dinámicas de un par desconocido mientras aún autentica el par usando una clave previamente compartida IKEv1:

1. Elija **Configuration > Site-to-Site VPN > Advanced > Crypto Maps.** La ventana muestra la lista de entradas de mapa criptográfico que ya están en su lugar (si hay alguna). Dado que ASA no sabe cuál es la dirección IP del par, para que ASA acepte la conexión, configure **Dynamic-map** con un conjunto de transformación coincidente (Propuesta IPsec). Haga clic en Add
(Agregar).


File View Tools Wizards Window Help
Type topic to search
Home Configuration Monitoring Save Refresh Back Forward Help
Site-to-Site VPN
Connection Profiles
Group Policies
Certificate Management
Advanced
Tunnel Groups
Crypto Maps
IKE Policies
IKE Parameters
IPsec Proposals (Transform Sets)
IPsec Prefragmentation Policies
Certificate to Connection Profile Maps
System Options
Crypto Engine
ACL Manager
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Site-to-Site VPN > Advanced > Crypto Maps
Add Edit Delete Find Diagram
Type:Priority
Traffic Selection
# Source Destination Service Action
Transform Set (IKEv1)
IPsec Proposal (IKEv2)
Peer
PFS
Enable Anti-replay window size: 64
Apply
Reset

2. En la ventana Create IPsec Rule (Crear regla IPsec), en la ficha Tunnel Policy (Mapa criptográfico) - Basic (Política de túnel), elija **outside** de la lista desplegable Interface y **dynamic** de la lista desplegable Policy Type (Tipo de política). En el campo Prioridad, asigne la prioridad para esta entrada en caso de que haya varias entradas en Mapa dinámico. A continuación, haga clic en **Seleccionar** junto al campo Propuesta IPsec IKE v1 para seleccionar la propuesta IPSec.


Create IPsec Rule
Tunnel Policy (Crypto Map) - Basic
Tunnel Policy (Crypto Map) - Advanced
Traffic Selection

Interface: outside

Policy Type: dynamic

Priority: 1

IPsec Proposals (Transform Sets)

IKE v1 IPsec Proposal:

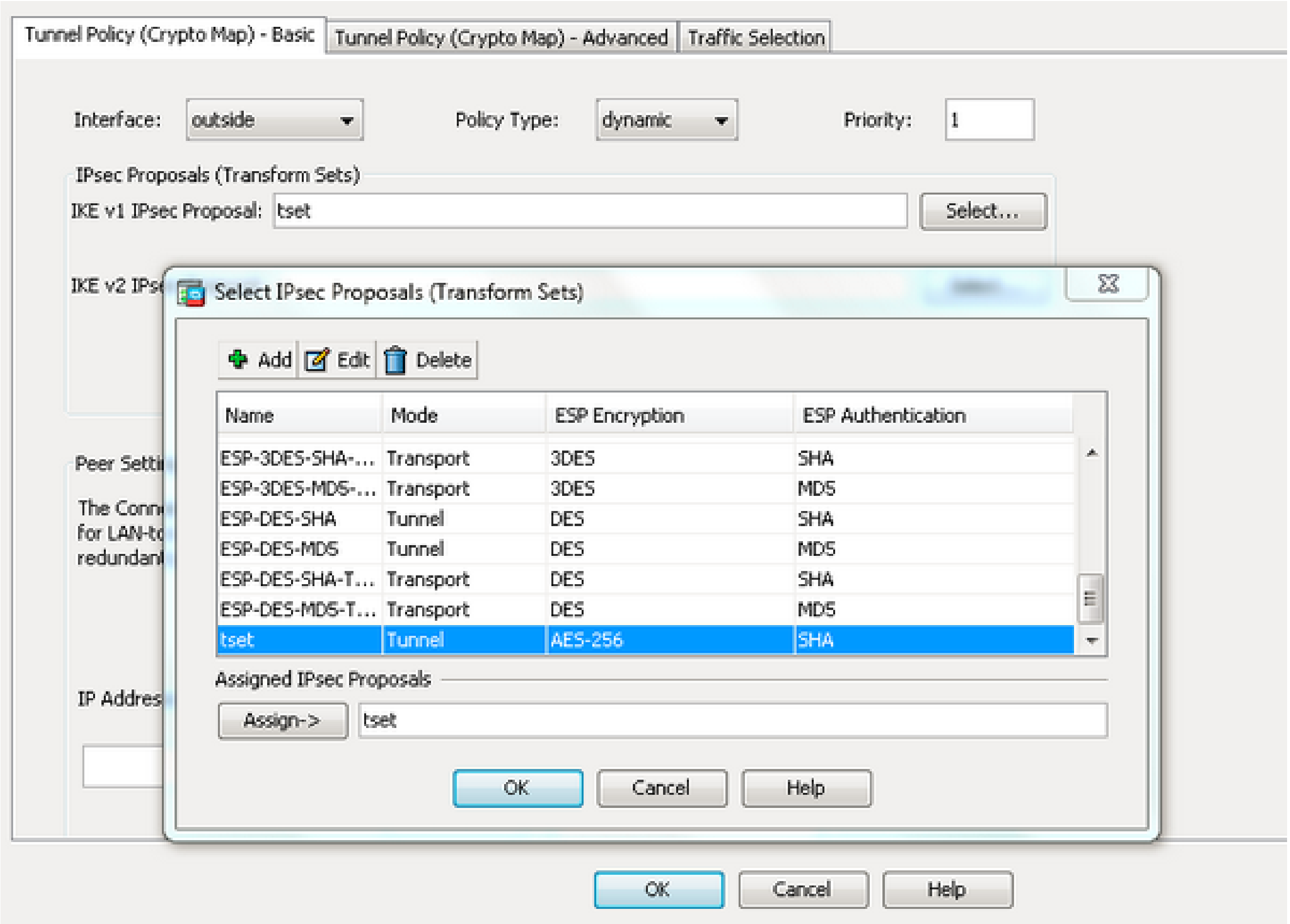
IKE v2 IPsec Proposal:

Peer Settings - Optional for Dynamic Crypto Map Entries

The Connection Type is applicable to static tunnel policies only. Uni-directional connection type policies are used for LAN-to-LAN redundancy. Tunnel policies of the 'Originate Only' connection type may specify up to 10 redundant peers.

IP Address of Peer to Be Added:

3. Cuando se abre el cuadro de diálogo Seleccionar propuestas de IPSec (Conjuntos de transformación), elija entre las propuestas de IPSec actuales o haga clic en **Agregar** para crear una nueva y utilizar la misma. Haga clic en **Aceptar** cuando haya terminado.



Interface: outside

Policy Type: dynamic

Priority: 1

IPsec Proposals (Transform Sets)

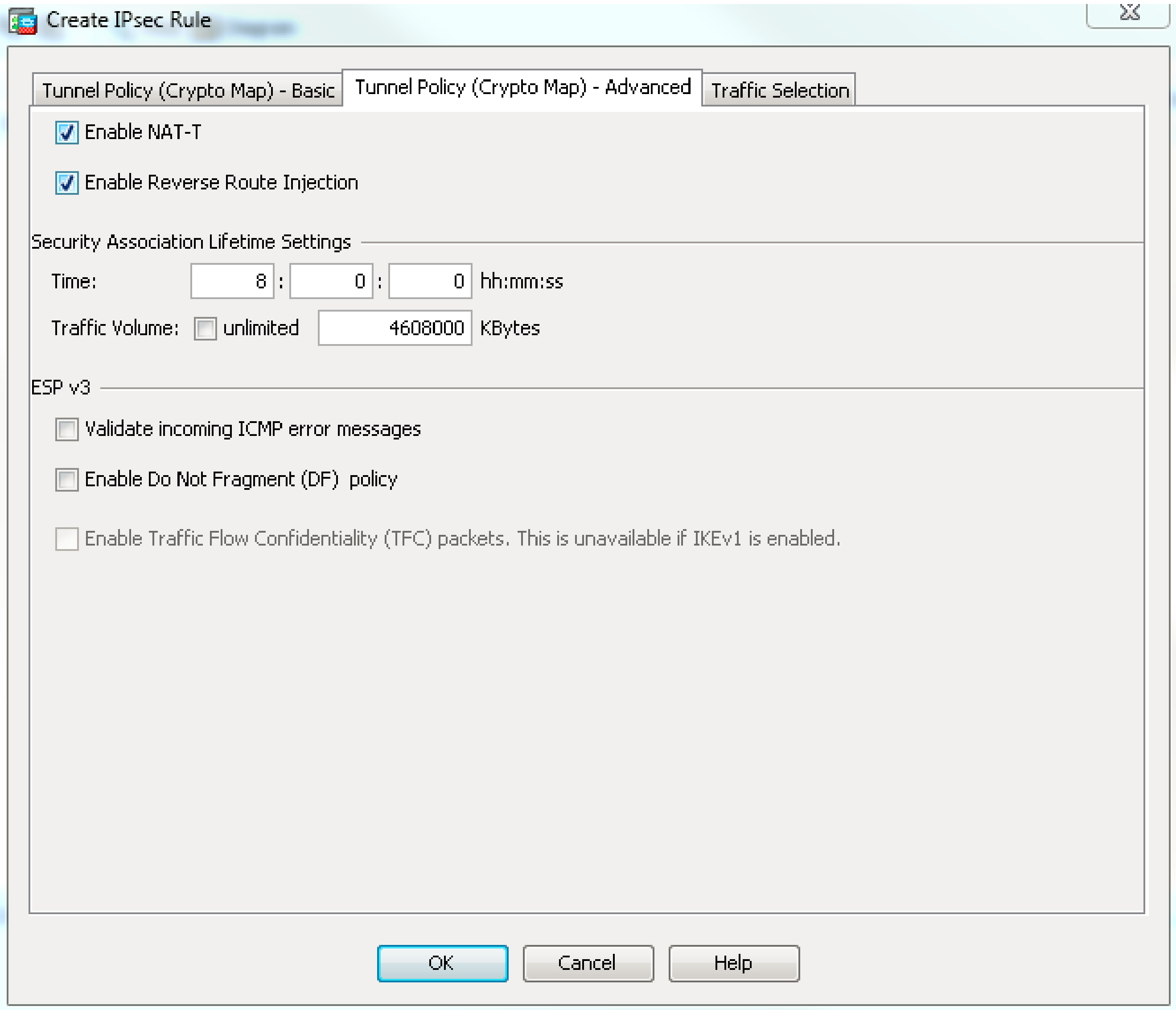
IKE v1 IPsec Proposal: tset

Name	Mode	ESP Encryption	ESP Authentication
ESP-3DES-SHA-...	Transport	3DES	SHA
ESP-3DES-MD5-...	Transport	3DES	MD5
ESP-DES-SHA	Tunnel	DES	SHA
ESP-DES-MD5	Tunnel	DES	MD5
ESP-DES-SHA-T...	Transport	DES	SHA
ESP-DES-MD5-T...	Transport	DES	MD5
tset	Tunnel	AES-256	SHA

Assigned IPsec Proposals

tset

4. En la ficha Tunnel Policy (Crypto Map)-Advanced (Política de túnel [Mapa criptográfico]), marque la casilla de verificación **Enable NAT-T** (Habilitar NAT-T si cualquiera de los pares está detrás de un dispositivo NAT) y la casilla de verificación **Enable Reverse Route Injection** (Habilitar inyección de ruta inversa). Cuando el túnel VPN se activa para el par dinámico, ASA instala una ruta dinámica para la red VPN remota negociada que apunta a la interfaz VPN.



Create IPsec Rule

Tunnel Policy (Crypto Map) - Basic
Tunnel Policy (Crypto Map) - Advanced
Traffic Selection

☑ Enable NAT-T

☑ Enable Reverse Route Injection

Security Association Lifetime Settings

Time: 8 : 0 : 0 hh:mm:ss

Traffic Volume: □ unlimited 4608000 KBytes

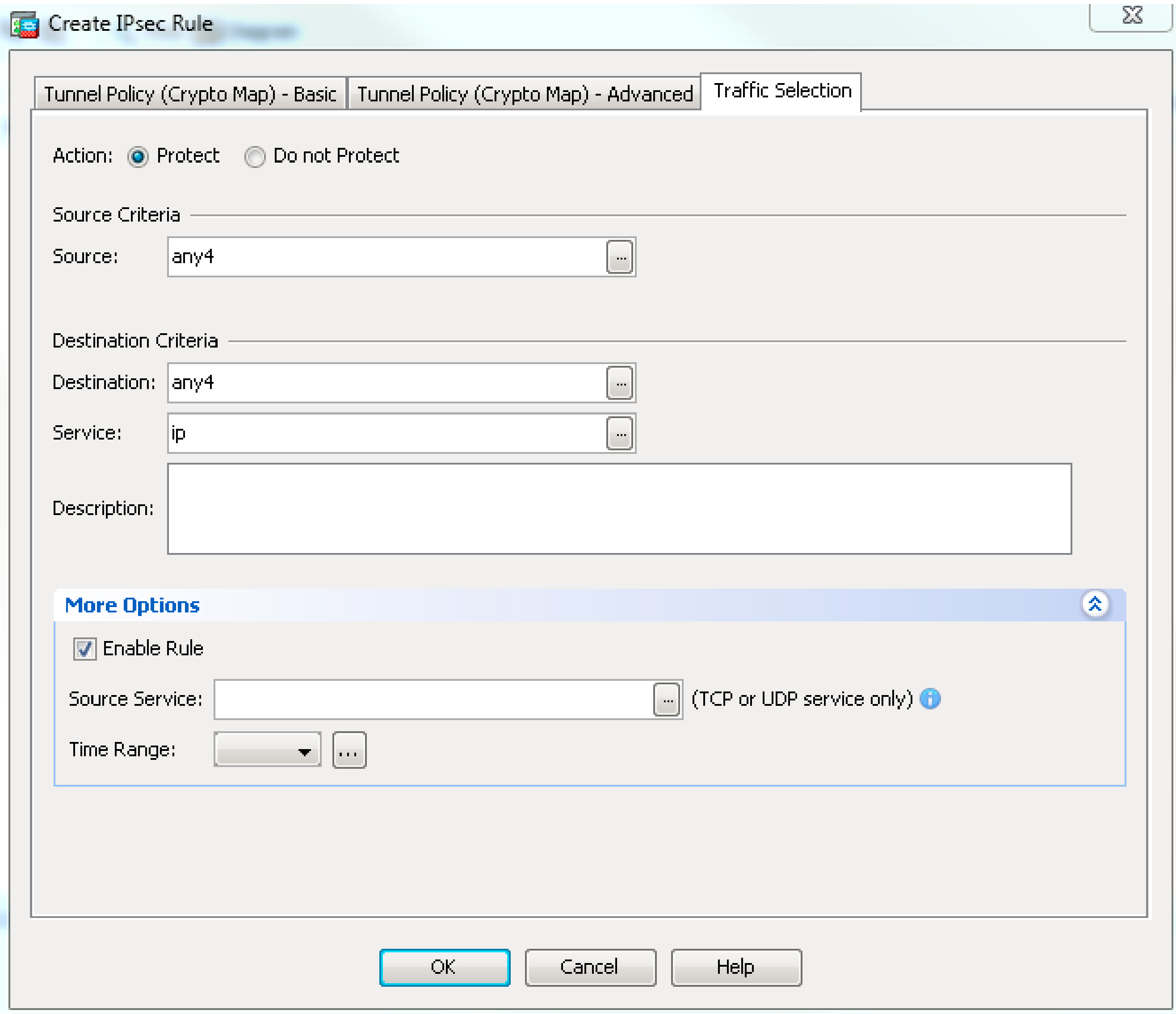
ESP v3

□ Validate incoming ICMP error messages

□ Enable Do Not Fragment (DF) policy

□ Enable Traffic Flow Confidentiality (TFC) packets. This is unavailable if IKEv1 is enabled.

Opcionalmente, en la pestaña Selección de tráfico también puede definir el tráfico de VPN interesante para el par dinámico y hacer clic en
Aceptar.



Create IPsec Rule

Tunnel Policy (Crypto Map) - Basic
Tunnel Policy (Crypto Map) - Advanced
Traffic Selection

Action: ● Protect ○ Do not Protect

Source Criteria

Source: any4

Destination Criteria

Destination: any4

Service: ip

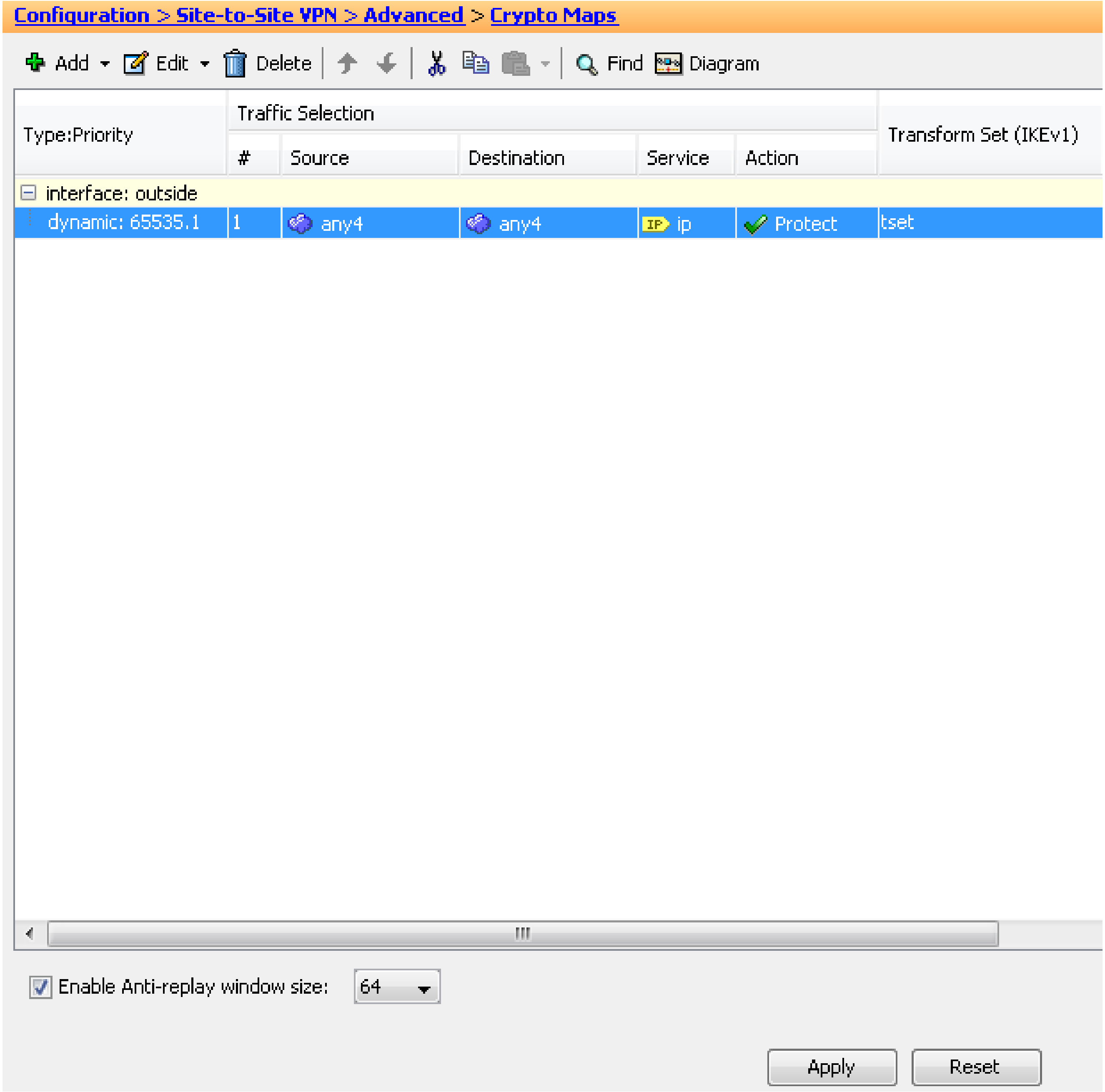
Description:

More Options

☑ Enable Rule

Source Service: (TCP or UDP service only)

Time Range:



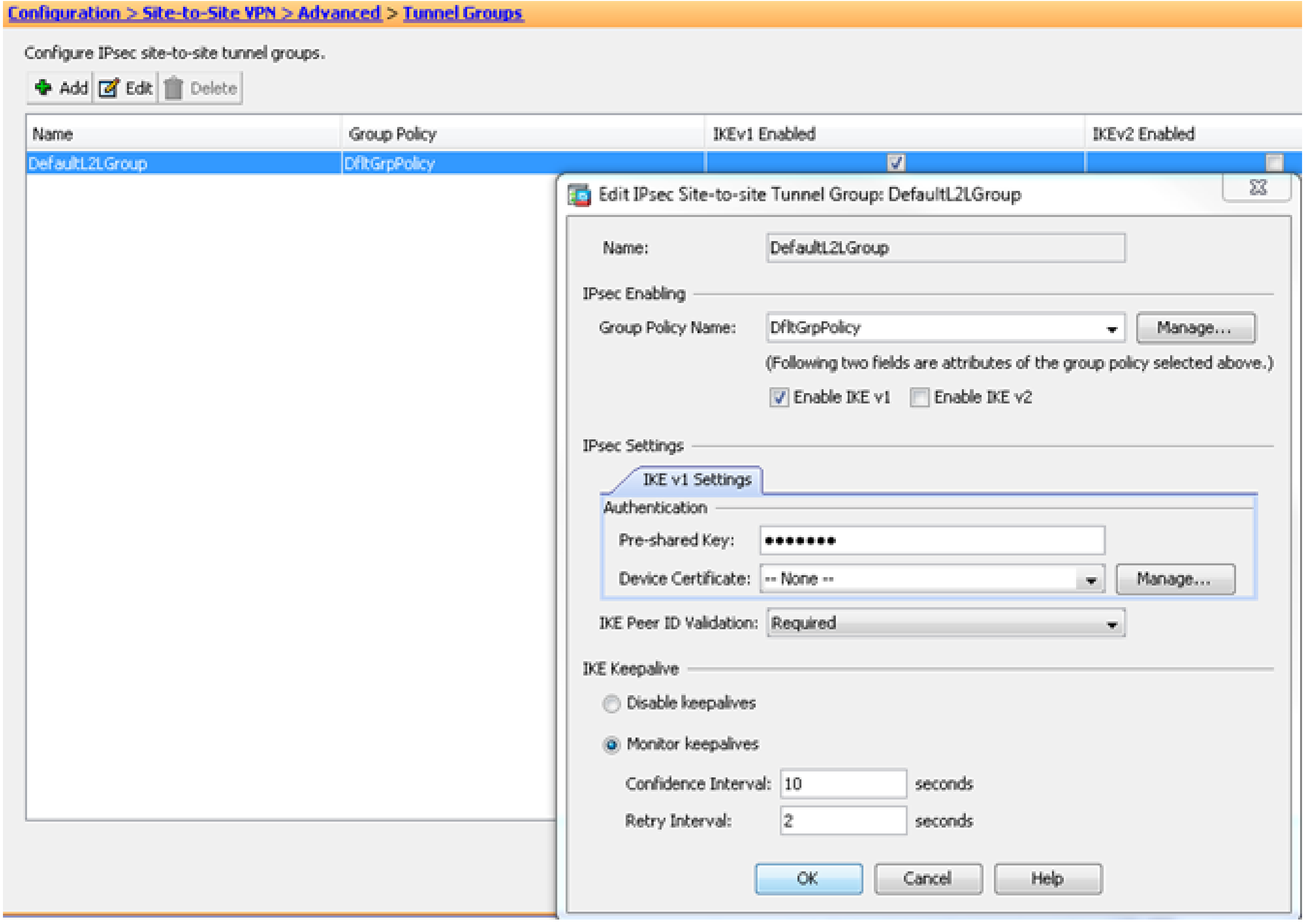
Configuration > Site-to-Site VPN > Advanced > Crypto Maps

Type:Priority	Traffic Selection					Transform Set (IKEv1)
	#	Source	Destination	Service	Action	
interface: outside						
dynamic: 65535.1	1	any4	any4	ip	✓ Protect	tset

☑ Enable Anti-replay window size: 64

Como se mencionó anteriormente, dado que ASA no tiene ninguna información sobre la dirección IP dinámica de peer remota, la solicitud de conexión desconocida se encuentra bajo DefaultL2LGroup que existe en ASA de forma predeterminada. Para que la autenticación suceda a la clave previamente compartida (cisco123 en este ejemplo) configurada en el par remoto debe coincidir con una en DefaultL2LGroup.

5. Elija **Configuration > Site-to-Site VPN > Advanced > Tunnel Groups**, seleccione **DefaultL2LGroup**, haga clic en **Edit** y configure la clave previamente compartida deseada. Haga clic en **Aceptar** cuando haya terminado.



Configuration > Site-to-Site VPN > Advanced > Tunnel Groups

Configure IPsec site-to-site tunnel groups.

Name	Group Policy	IKEv1 Enabled	IKEv2 Enabled
DefaultL2LGroup	DfltGrpPolicy	☑	□

Edit IPsec Site-to-site Tunnel Group: DefaultL2LGroup

Name: DefaultL2LGroup

IPsec Enabling

Group Policy Name: DfltGrpPolicy

(Following two fields are attributes of the group policy selected above.)

☑ Enable IKE v1 □ Enable IKE v2

IPsec Settings

IKE v1 Settings

Authentication

Pre-shared Key: •••••••

Device Certificate: -- None --

IKE Peer ID Validation: Required

IKE Keepalive

○ Disable keepalives

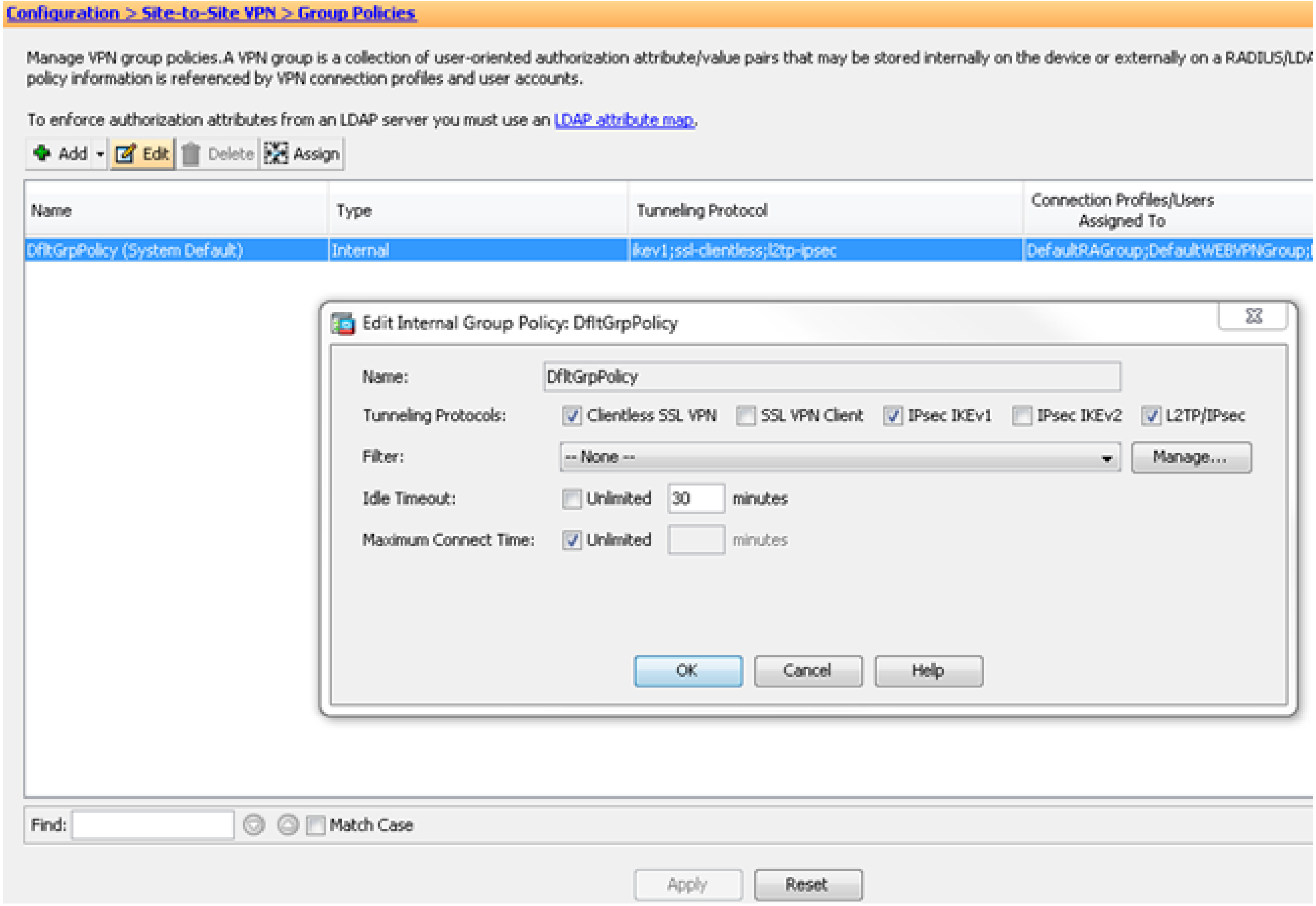
● Monitor keepalives

Confidence Interval: 10 seconds

Retry Interval: 2 seconds

Nota: Esto crea una clave previamente compartida comodín en el par estático (Central-ASA). Cualquier dispositivo/par que conozca esta clave previamente compartida y sus propuestas coincidentes pueden establecer con éxito un túnel VPN y acceder a los recursos a través de VPN. Asegúrese de que esta clave predefinida no se comparte con entidades desconocidas y no es fácil de adivinar.

6. Elija **Configuration** > **Site-to-Site VPN** > **Group Policies** y seleccione la política de grupo que elija (la política de grupo predeterminada en este caso). Haga clic en **Editar** y edite la política de grupo en el cuadro de diálogo Editar política de grupo interna. Haga clic en **Aceptar** cuando haya terminado.



Configuration > Site-to-Site VPN > Group Policies

Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDA
policy information is referenced by VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
DfltGrpPolicy (System Default)	Internal	ikev1;ssl-clientless;l2tp-ipsec	DefaultRAGroup;DefaultWEBVPNGroup;

Edit Internal Group Policy: DfltGrpPolicy

Name: DfltGrpPolicy

Tunneling Protocols: ☑ Clientless SSL VPN ☐ SSL VPN Client ☑ IPsec IKEv1 ☐ IPsec IKEv2 ☑ L2TP/IPsec

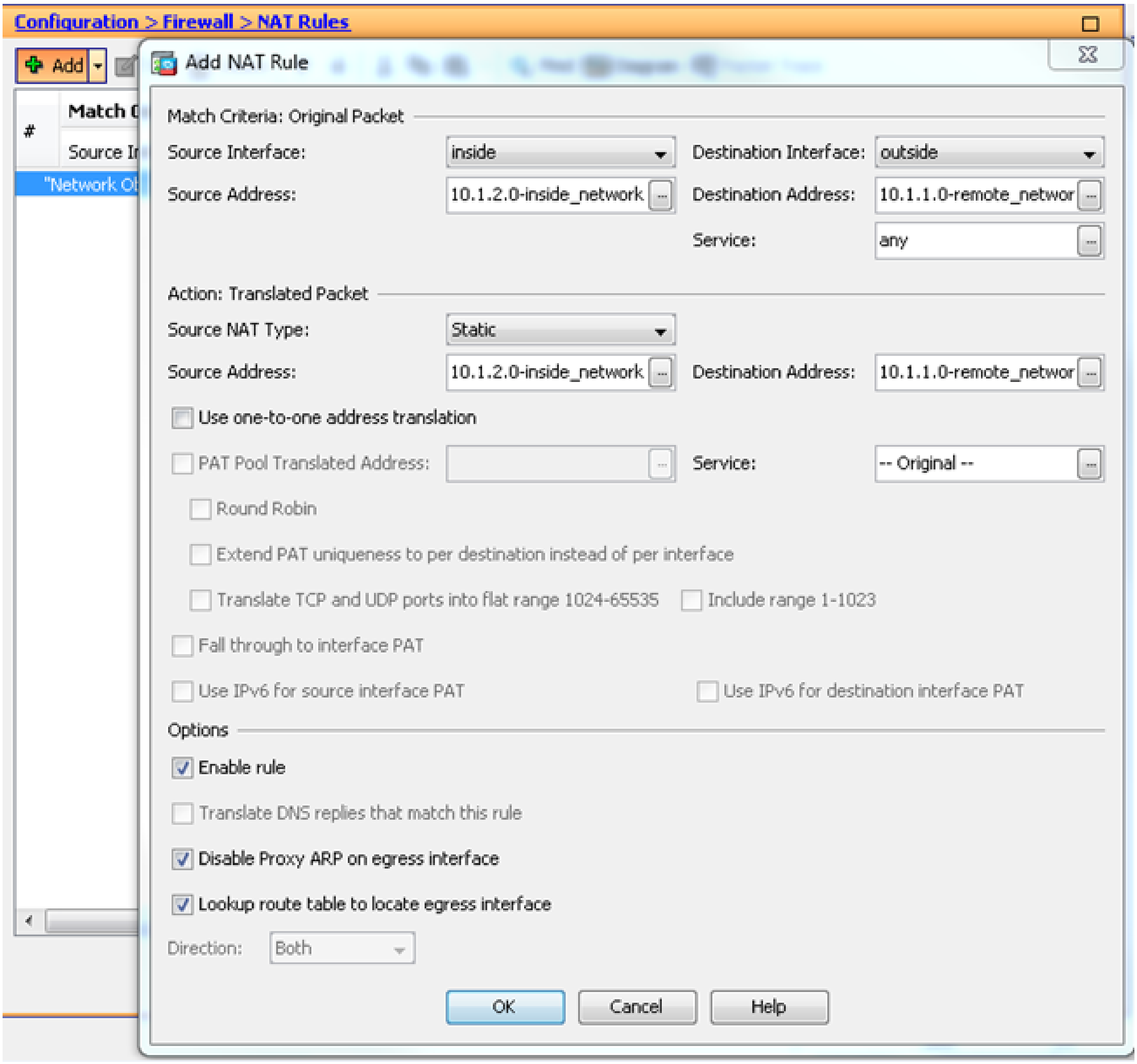
Filter: -- None --

Idle Timeout: ☐ Unlimited 30 minutes

Maximum Connect Time: ☑ Unlimited minutes

Find: ☐ Match Case

7. Elija **Configuration** > **Firewall** > **NAT Rules** y en la ventana Add Nat Rule , configure una regla no nat (NAT-EXEMPT) para el tráfico VPN. Haga clic en **Aceptar** cuando haya terminado.



Configuration > Firewall > NAT Rules

Add NAT Rule

Match Criteria: Original Packet

Source Interface: inside

Destination Interface: outside

Source Address: 10.1.2.0-inside_network

Destination Address: 10.1.1.0-remote_networ

Service: any

Action: Translated Packet

Source NAT Type: Static

Source Address: 10.1.2.0-inside_network

Destination Address: 10.1.1.0-remote_networ

□ Use one-to-one address translation

□ PAT Pool Translated Address:

Service: -- Original --

□ Round Robin

□ Extend PAT uniqueness to per destination instead of per interface

□ Translate TCP and UDP ports into flat range 1024-65535 □ Include range 1-1023

□ Fall through to interface PAT

□ Use IPv6 for source interface PAT □ Use IPv6 for destination interface PAT

Options

☑ Enable rule

□ Translate DNS replies that match this rule

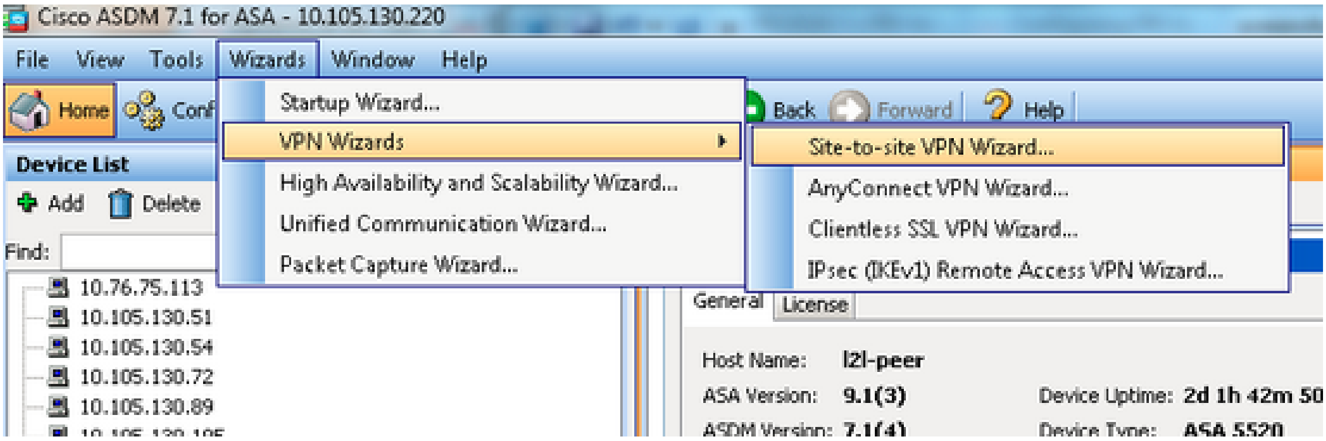
☑ Disable Proxy ARP on egress interface

☑ Lookup route table to locate egress interface

Direction: Both

ASA remoto (par dinámico)

1. Elija **Wizards > VPN Wizards > Site-to-site VPN Wizard** una vez que la aplicación ASDM se conecte al ASA.



Cisco ASDM 7.1 for ASA - 10.105.130.220

Host Name: l2l-peer

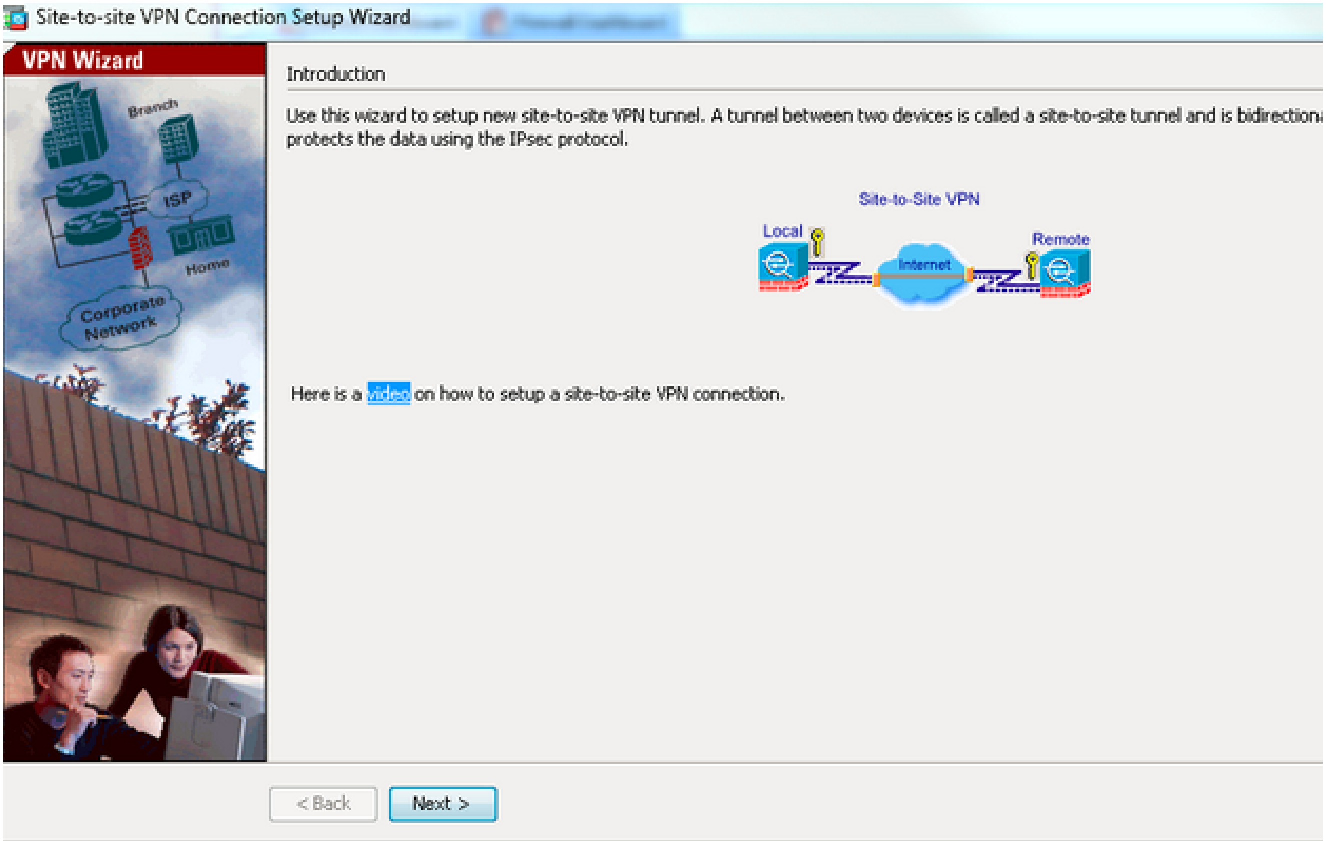
ASA Version: 9.1(3)

Device Uptime: 2d 1h 42m 50

ASDM Version: 7.1(4)

Device Type: ASA 5520

2. Haga clic en Next (Siguiente).



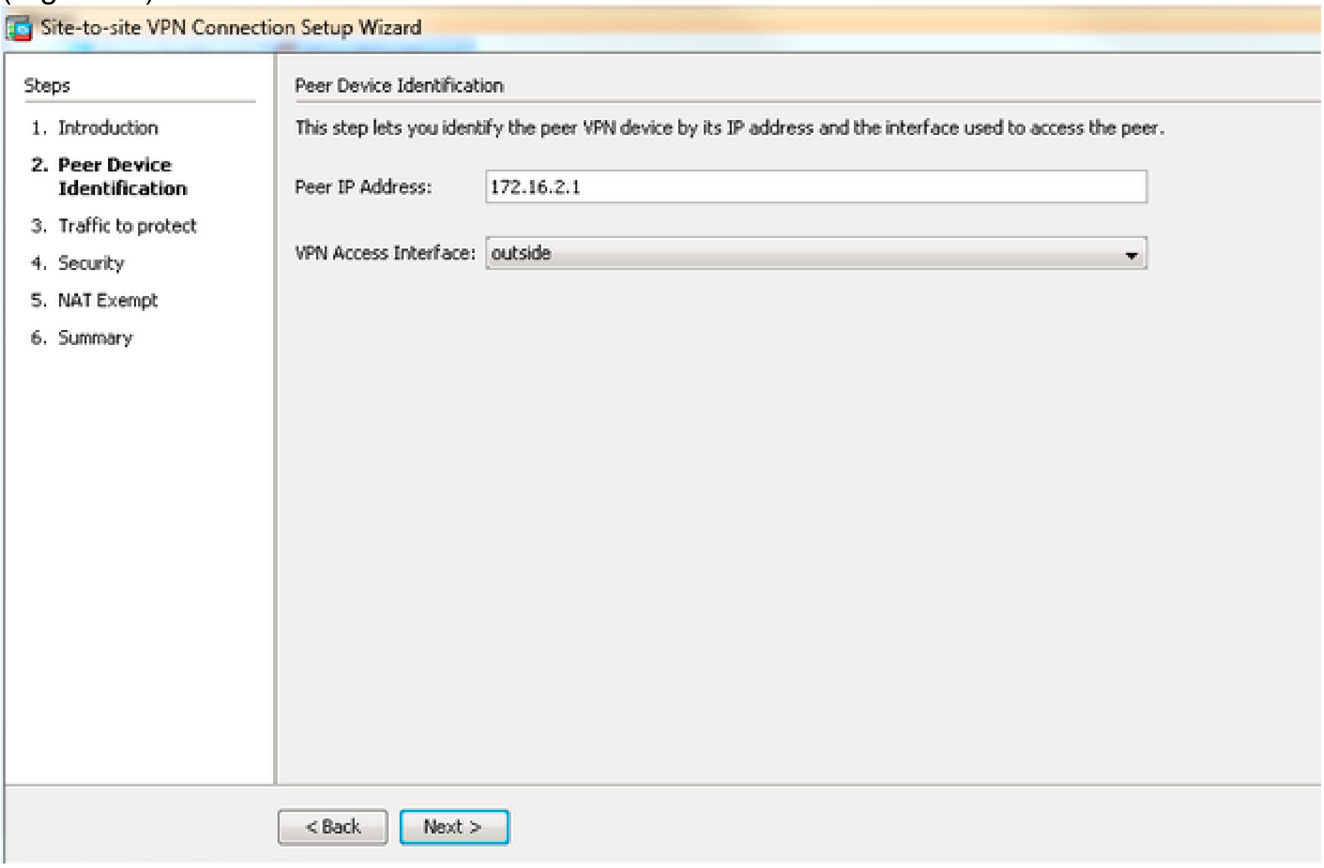
Site-to-site VPN Connection Setup Wizard

Introduction

Use this wizard to setup new site-to-site VPN tunnel. A tunnel between two devices is called a site-to-site tunnel and is bidirectiona
protects the data using the IPsec protocol.

Here is a video on how to setup a site-to-site VPN connection.

3. Elija **outside** en la lista desplegable VPN Access Interface para especificar la dirección IP externa del par remoto. Seleccione la interfaz (**WAN)** donde se aplica el mapa criptográfico. Haga clic en Next
   (Siguiente).



Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. **Peer Device Identification**
3. Traffic to protect
4. Security
5. NAT Exempt
6. Summary

Peer Device Identification

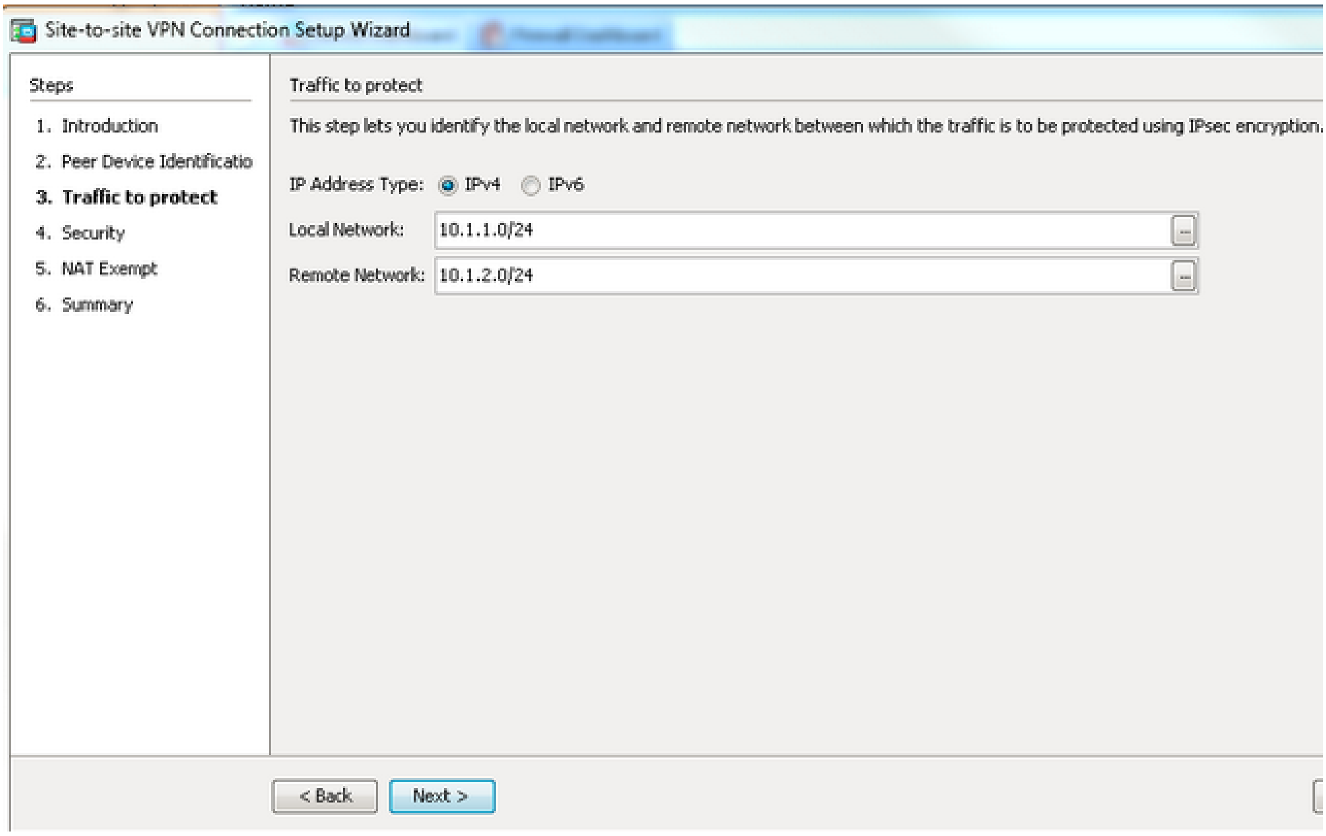
This step lets you identify the peer VPN device by its IP address and the interface used to access the peer.

Peer IP Address: 172.16.2.1

VPN Access Interface: outside

4. Especifique los hosts/redes a los que se debe permitir el paso a través del túnel VPN. En este paso, debe proporcionar las Redes Locales y Redes Remotas para el Túnel VPN. Haga clic en los botones situados junto a los campos Red local y Red remota y elija la dirección según sea necesario. Haga clic en **Siguiente** cuando haya

terminado.



Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. Peer Device Identificatio
3. **Traffic to protect**
4. Security
5. NAT Exempt
6. Summary

Traffic to protect

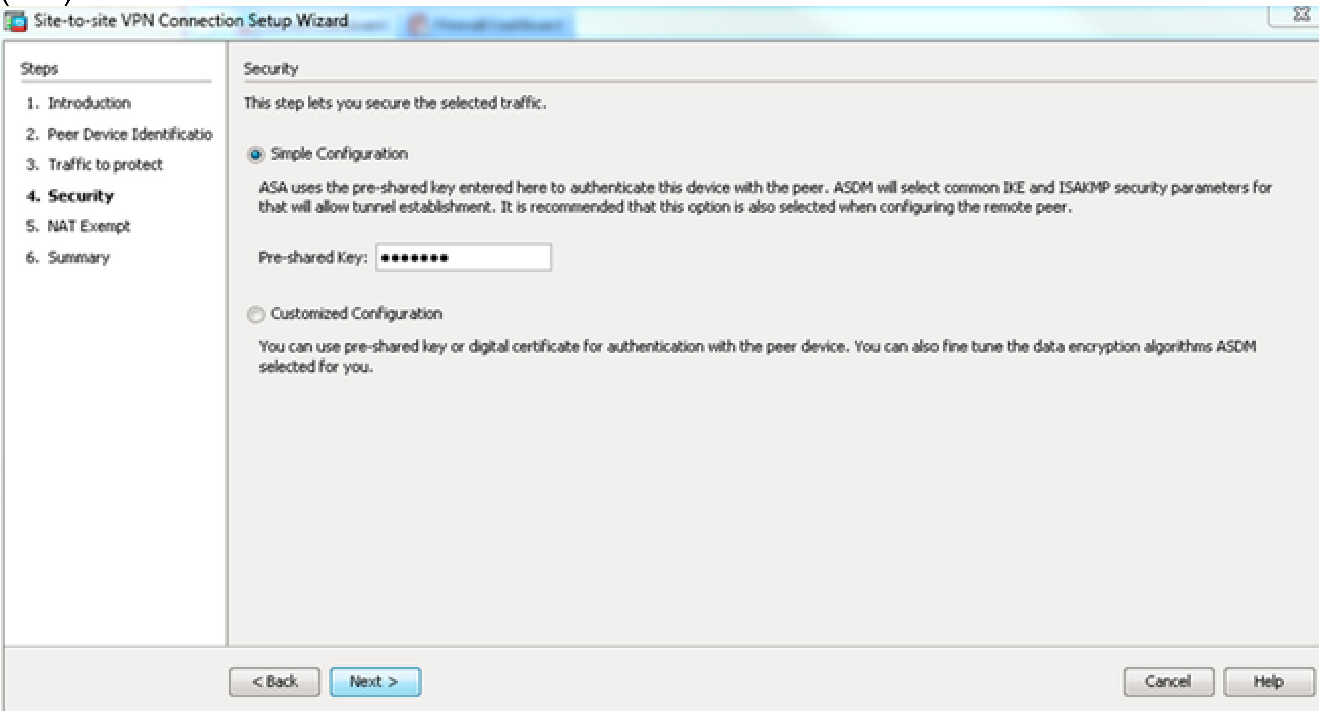
This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption.

IP Address Type: ● IPv4 ○ IPv6

Local Network: 10.1.1.0/24

Remote Network: 10.1.2.0/24

5. Introduzca la información de autenticación que se utilizará, que es una clave previamente compartida en este ejemplo. La clave previamente compartida utilizada en este ejemplo es cisco123. El nombre del grupo de túnel es la dirección IP del par remoto de forma predeterminada si configura VPN de LAN a LAN (L2L).



Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. Peer Device Identificatio
3. Traffic to protect
4. **Security**
5. NAT Exempt
6. Summary

Security

This step lets you secure the selected traffic.

● Simple Configuration

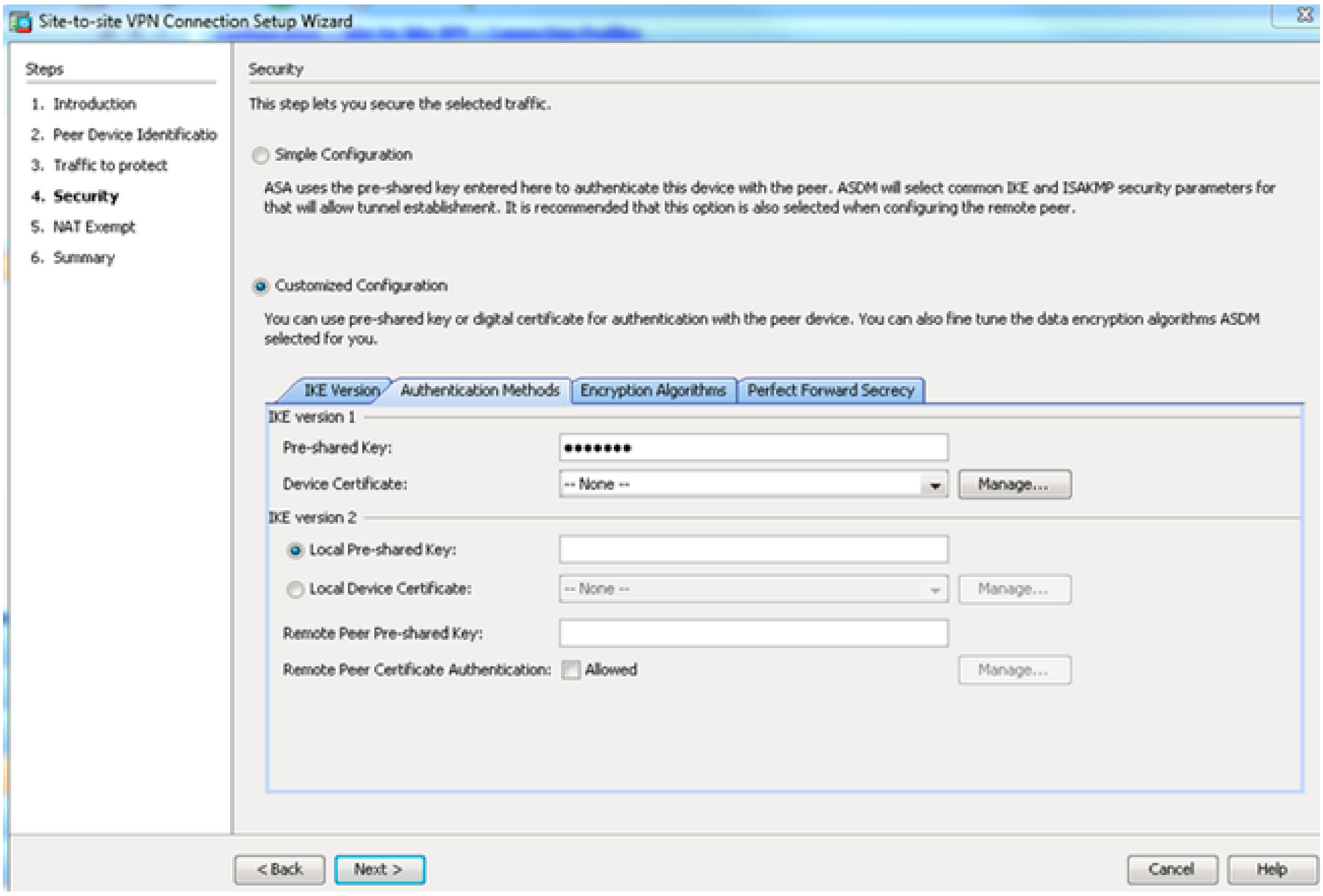
ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.

Pre-shared Key: ••••••••

○ Customized Configuration

You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.

OPuede personalizar la configuración para incluir la política IKE e IPsec de su elección. Debe haber al menos una política de coincidencia entre los pares:En la ficha Métodos de autenticación, introduzca la clave previamente compartida IKE versión 1 en el campo Clave previamente compartida. En este ejemplo, es **cisco123**.



Security

This step lets you secure the selected traffic.

○ Simple Configuration

ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.

● Customized Configuration

You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.

IKE version 1

Pre-shared Key: •••••••

Device Certificate: -- None --

IKE version 2

● Local Pre-shared Key:

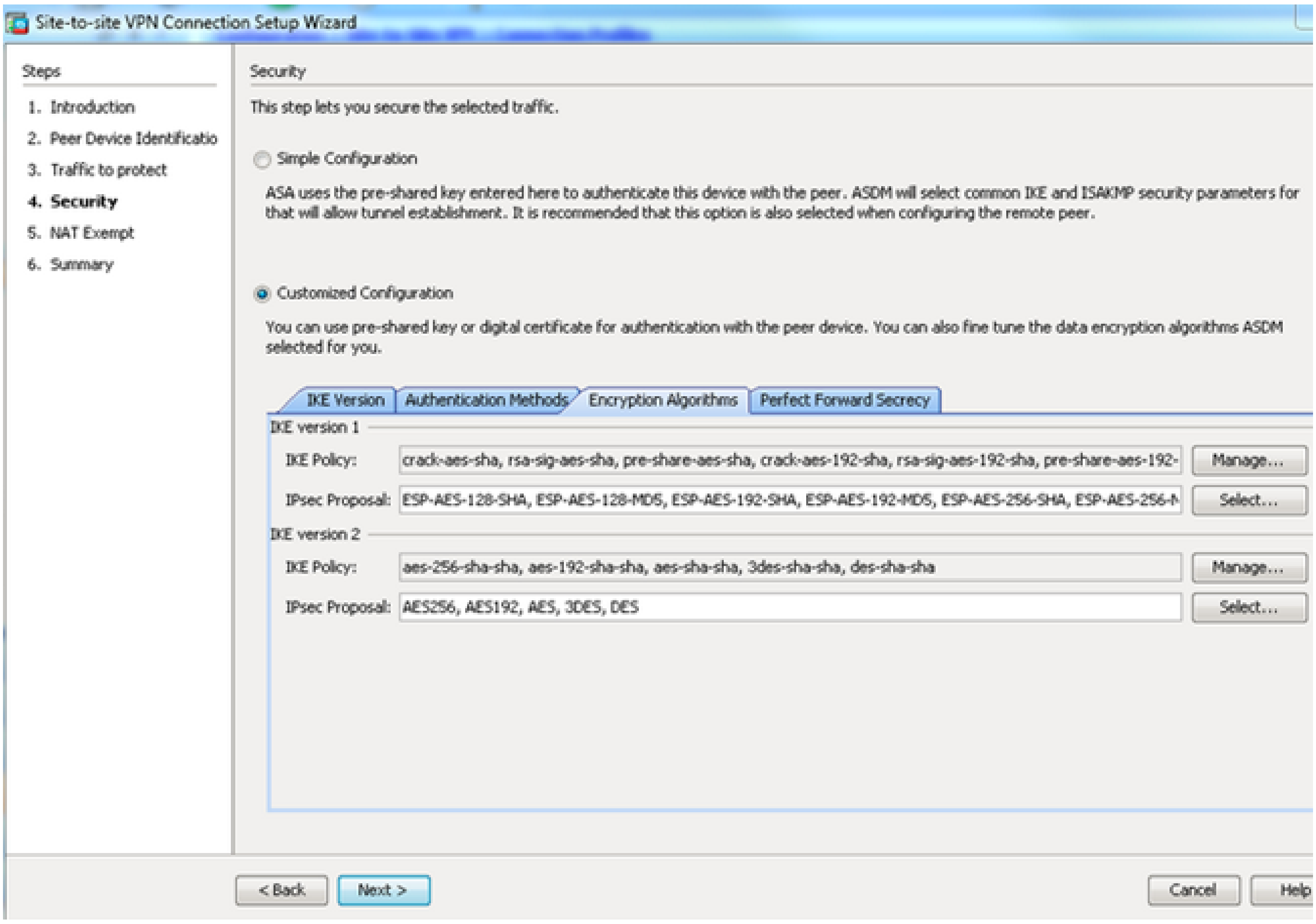
○ Local Device Certificate: -- None --

Remote Peer Pre-shared Key:

Remote Peer Certificate Authentication: □ Allowed

Haga clic en la pestaña **Algoritmos de cifrado**.

6. Haga clic en **Administrar** junto al campo IKE Policy, haga clic en **Agregar** y configure una política IKE personalizada (fase 1). Haga clic en **Aceptar** cuando haya terminado.



Security

This step lets you secure the selected traffic.

○ Simple Configuration

ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.

● Customized Configuration

You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.

IKE version 1

IKE Policy: crack-aes-sha, rsa-sig-aes-sha, pre-share-aes-sha, crack-aes-192-sha, rsa-sig-aes-192-sha, pre-share-aes-192-

IPsec Proposal: ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5, ESP-AES-256-SHA, ESP-AES-256-M

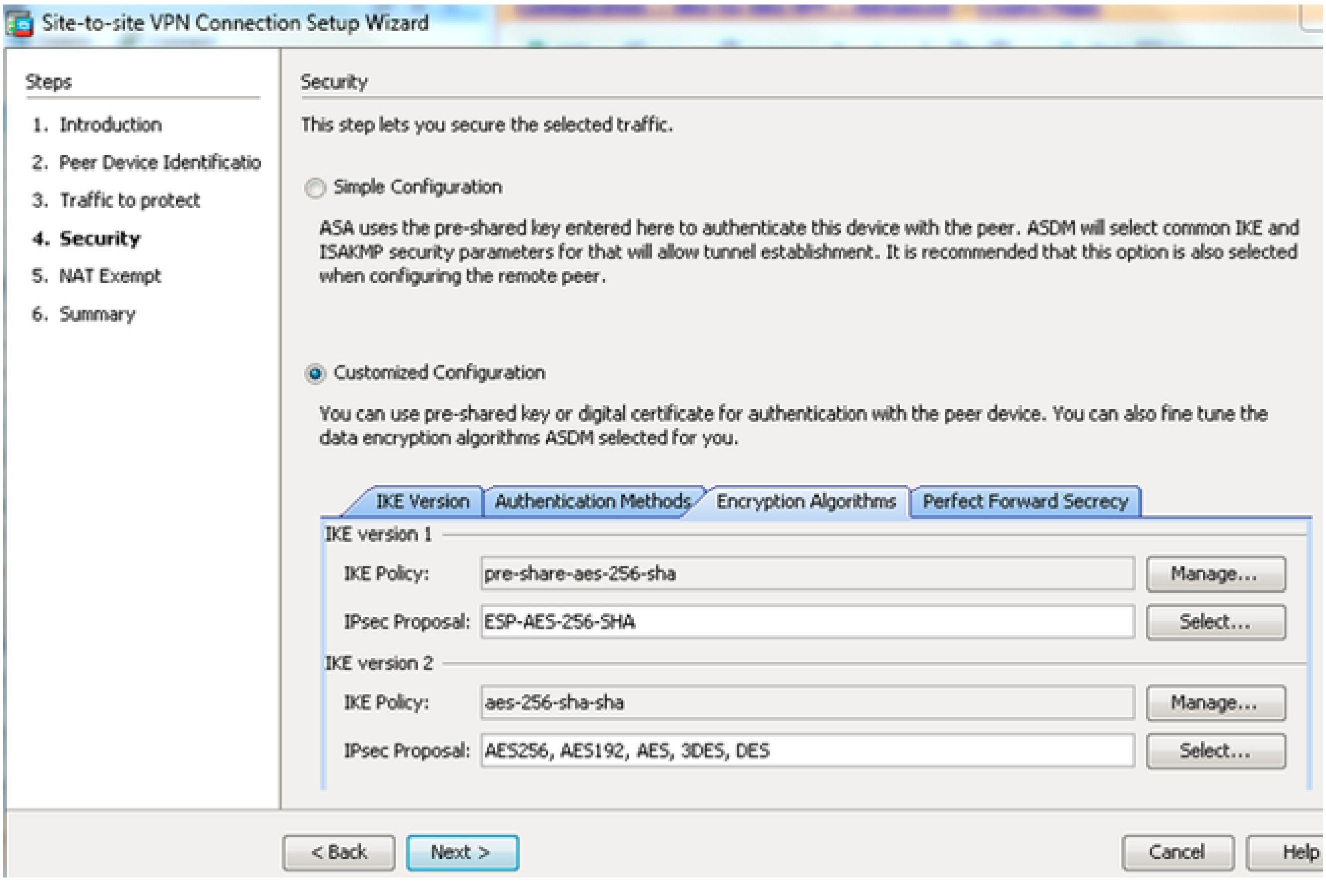
IKE version 2

IKE Policy: aes-256-sha-sha, aes-192-sha-sha, aes-sha-sha, 3des-sha-sha, des-sha-sha

IPsec Proposal: AES256, AES192, AES, 3DES, DES

7. Haga clic en **Seleccionar** junto al campo Propuesta de IPSec y seleccione la propuesta de

IPSec deseada. Haga clic en **Siguiente** cuando haya terminado.



Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. Peer Device Identificatio
3. Traffic to protect
4. **Security**
5. NAT Exempt
6. Summary

Security

This step lets you secure the selected traffic.

○ Simple Configuration

ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.

● Customized Configuration

You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.

IKE version 1

IKE Policy: pre-share-aes-256-sha

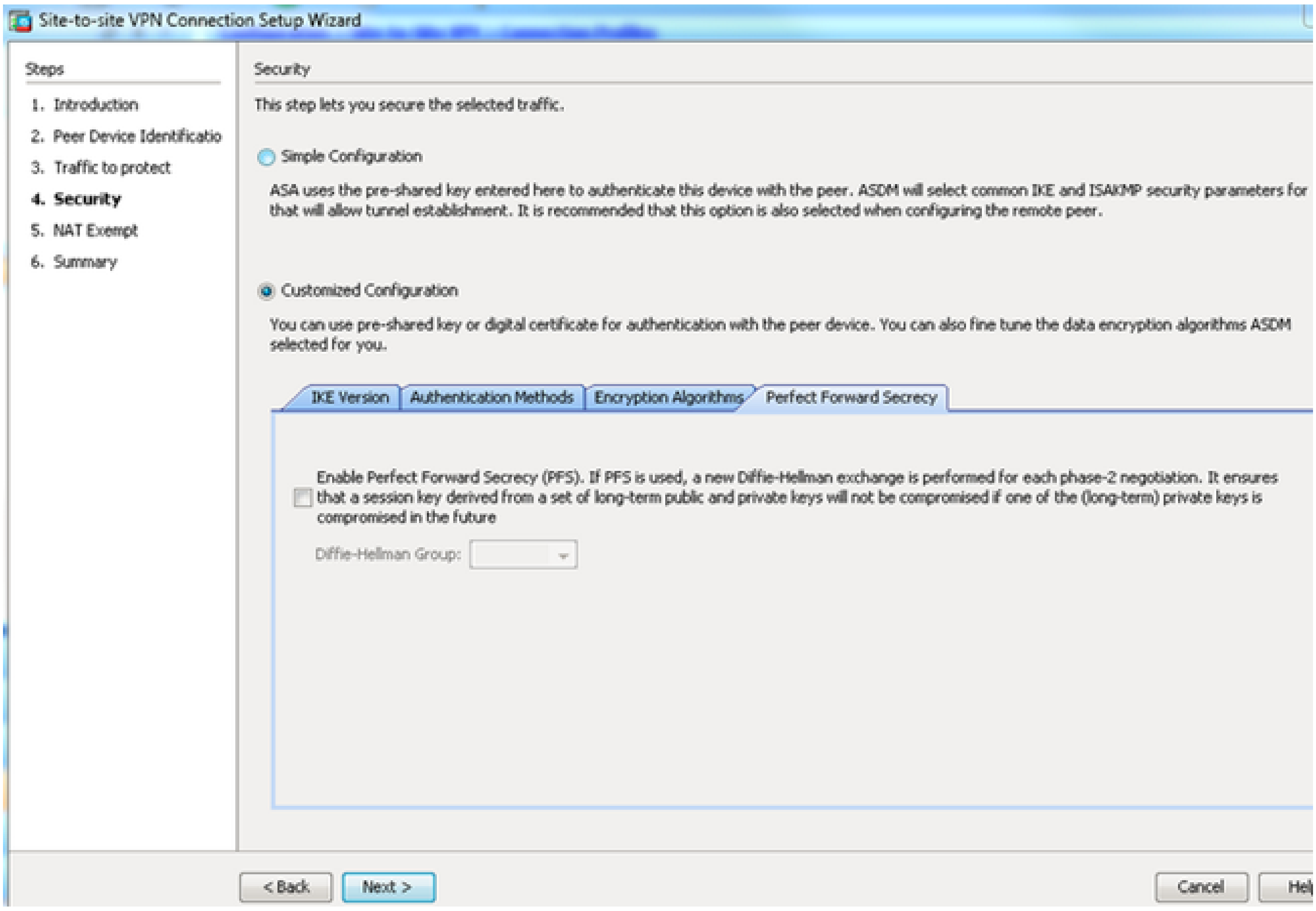
IPsec Proposal: ESP-AES-256-SHA

IKE version 2

IKE Policy: aes-256-sha-sha

IPsec Proposal: AES256, AES192, AES, 3DES, DES

Opcionalmente, puede ir a la ficha Perfect Forward Secrecy (Confidencialidad directa perfecta) y marcar la casilla de verificación **Enable Perfect Forward Secrecy (PFS)**. Haga clic en **Siguiente** cuando haya terminado.



Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. Peer Device Identificatio
3. Traffic to protect
4. **Security**
5. NAT Exempt
6. Summary

Security

This step lets you secure the selected traffic.

○ Simple Configuration

ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.

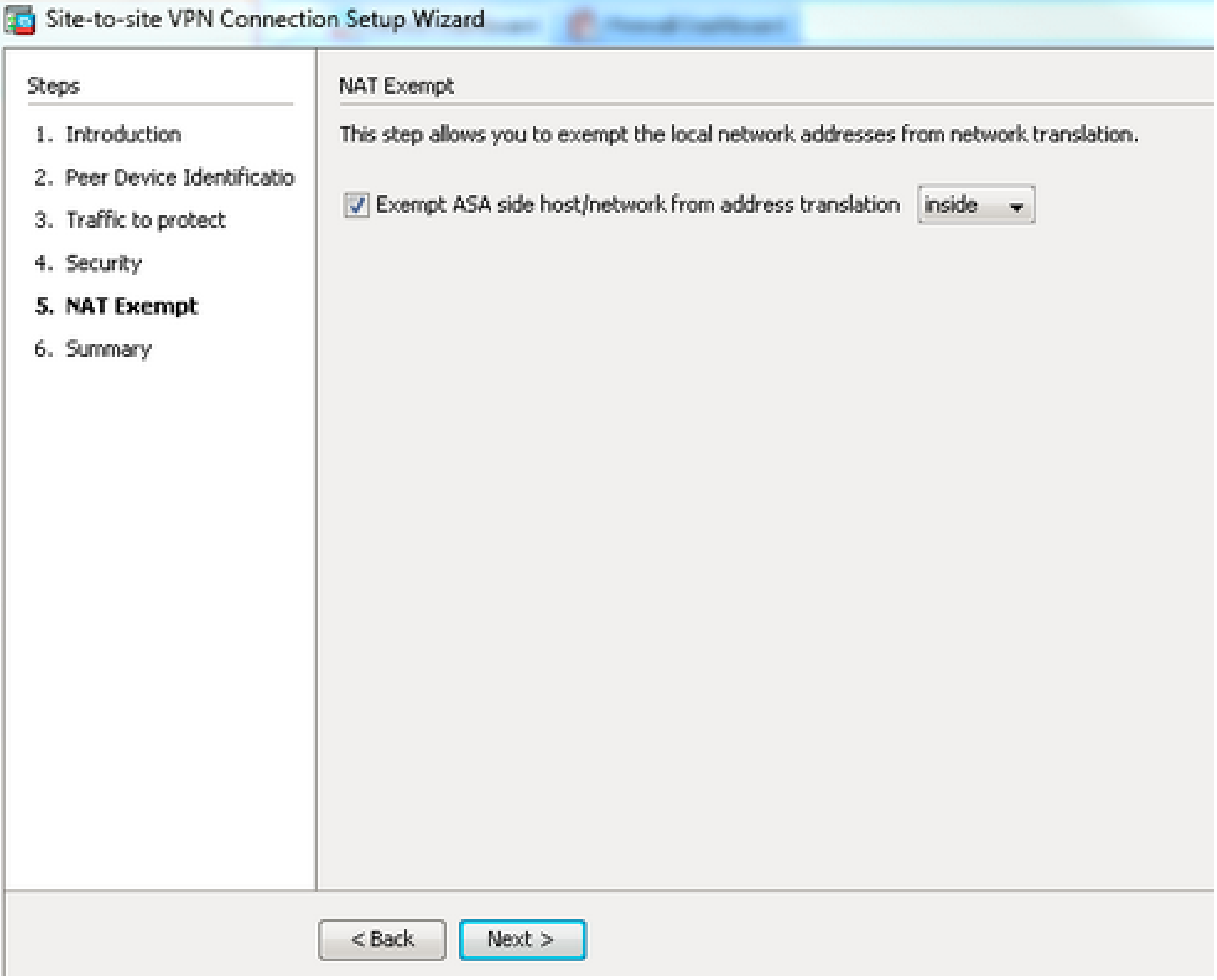
● Customized Configuration

You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.

□ Enable Perfect Forward Secrecy (PFS). If PFS is used, a new Diffie-Hellman exchange is performed for each phase-2 negotiation. It ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the (long-term) private keys is compromised in the future

Diffie-Hellman Group:

8. Marque la casilla de verificación **Exempt ASA side host/network from address translation** para evitar que el tráfico del túnel comience el inicio de la Traducción de Dirección de Red. Elija **local o interno** de la lista desplegable para establecer la interfaz donde se puede alcanzar la red local. Haga clic en Next
   (Siguiente).



Site-to-site VPN Connection Setup Wizard

Steps

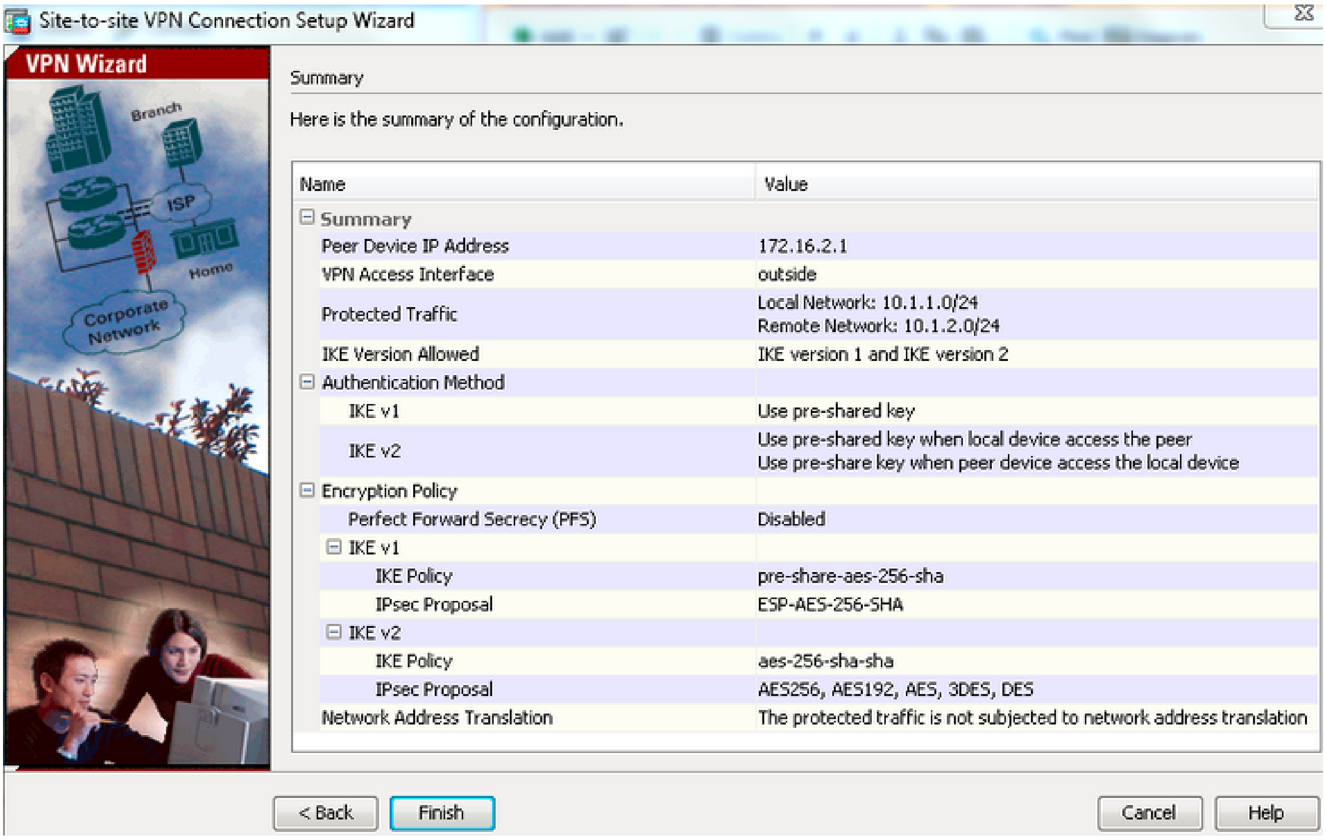
1. Introduction
2. Peer Device Identificatio
3. Traffic to protect
4. Security
5. **NAT Exempt**
6. Summary

NAT Exempt

This step allows you to exempt the local network addresses from network translation.

☑ Exempt ASA side host/network from address translation: inside

9. ASDM muestra un resumen de la VPN que se acaba de configurar. Verifique y haga clic en **Finalizar**.



Summary

Here is the summary of the configuration.

Name	Value
Summary	
Peer Device IP Address	172.16.2.1
VPN Access Interface	outside
Protected Traffic	Local Network: 10.1.1.0/24 Remote Network: 10.1.2.0/24
IKE Version Allowed	IKE version 1 and IKE version 2
Authentication Method	
IKE v1	Use pre-shared key
IKE v2	Use pre-shared key when local device access the peer Use pre-share key when peer device access the local device
Encryption Policy	
Perfect Forward Secrecy (PFS)	Disabled
IKE v1	
IKE Policy	pre-share-aes-256-sha
IPsec Proposal	ESP-AES-256-SHA
IKE v2	
IKE Policy	aes-256-sha-sha
IPsec Proposal	AES256, AES192, AES, 3DES, DES
Network Address Translation	The protected traffic is not subjected to network address translation

Configuración de CLI

Configuración de ASA central (par estático)

1. Configure una regla NO-NAT/ NAT-EXEMPT para el tráfico VPN como muestra este ejemplo:
```
object network 10.1.1.0-remote_network
subnet 10.1.1.0 255.255.255.0

object network 10.1.2.0-inside_network
 subnet 10.1.2.0 255.255.255.0

nat (inside,outside) source static 10.1.2.0-inside_network 10.1.2.0-inside_network
destination static 10.1.1.0-remote_network 10.1.1.0-remote_network
no-proxy-arp route-lookup
```
2. Configure la clave previamente compartida bajo DefaultL2LGroup para autenticar cualquier peer dinámico-L2L-remoto:
```
tunnel-group DefaultL2LGroup ipsec-attributes
 ikev1 pre-shared-key cisco123
```
3. Defina la política ISAKMP/fase 2:
```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
```
4. Defina la política IPSec/conjunto de transformación de fase 2:
```
crypto ipsec ikev1 transform-set tset esp-aes-256 esp-sha-hmac
```
5. Configure el mapa dinámico con estos parámetros: Conjunto de transformación necesarioHabilitar la inyección de ruta inversa (RRI), que permite al dispositivo de seguridad aprender información de routing para clientes conectados (opcional)

```
crypto dynamic-map outside_dyn_map 1 set ikev1 transform-set tset
crypto dynamic-map outside_dyn_map 1 set reverse-route
```

6. Enlazar el mapa dinámico al mapa crypto, aplicar el mapa crypto y habilitar ISAKMP/IKEv1 en la interfaz exterior:
   ```
   crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map

   crypto map outside_map interface outside
   crypto ikev1 enable outside
   ```

ASA remoto (par dinámico)

1. Configure una regla de exención de NAT para el tráfico VPN:
   ```
   object network 10.1.1.0-inside_network
   subnet 10.1.1.0 255.255.255.0

   object network 10.1.2.0-remote_network
   subnet 10.1.2.0 255.255.255.0

   nat (inside,outside) source static 10.1.1.0-inside_network 10.1.1.0-inside_network
   destination static 10.1.2.0-remote_network 10.1.2.0-remote_network
   no-proxy-arp route-lookup
   ```
2. Configure un grupo de túnel para un peer VPN estático y una clave previamente compartida.
   ```
   tunnel-group 172.16.2.1 type ipsec-l2l
   tunnel-group 172.16.2.1 ipsec-attributes
   ikev1 pre-shared-key cisco123
   ```
3. Defina la política PHASE-1/ISAKMP:
   ```
   crypto ikev1 policy 10
   authentication pre-share
   encryption aes-256
   hash sha
   group 2
   lifetime 86400
   ```
4. Defina un conjunto de transformación/política IPSec de fase 2:
   ```
   crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
   ```
5. Configure una lista de acceso que defina el tráfico/red VPN interesante:
   ```
   access-list outside_cryptomap extended permit ip object
   10.1.1.0-inside_network object 10.1.2.0-remote_network
   ```
6. Configure el mapa crypto estático con estos parámetros: Lista de acceso de criptografía/VPNDirección IP de peer IPsec remotaConjunto de transformación necesario
   ```
   crypto map outside_map 1 match address outside_cryptomap
   crypto map outside_map 1 set peer 172.16.2.1
   crypto map outside_map 1 set ikev1 transform-set ESP-AES-256-SHA
   ```
7. Aplique el mapa crypto y habilite ISAKMP/IKEv1 en la interfaz exterior:
   ```
   crypto map outside_map interface outside
   crypto ikev1 enable outside
   ```

Verificación

Utilice esta sección para confirmar que la configuración funciona correctamente.

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

- **show crypto isakmp sa**: muestra todas las asociaciones de seguridad (SA) IKE actuales en un par.

- **show crypto ipsec sa** - Muestra todas las SA IPsec actuales.

Esta sección muestra la verificación de ejemplo para los dos ASA.

ASA central

```
Central-ASA#show crypto isakmp sa

  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: 172.16.1.1
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE

    Central-ASA# show crypto ipsec sa
interface: outside
    Crypto map tag: outside_dyn_map, seq num: 1, local addr: 172.16.2.1

        local ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
      current_peer: 172.16.1.1

        #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.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
      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: 30D071C0
      current inbound spi : 38DA6E51

      inbound esp sas:
      spi: 0x38DA6E51 (953839185)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
         sa timing: remaining key lifetime (kB/sec): (3914999/28588)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x0000001F
    outbound esp sas:
      spi: 0x30D071C0 (818966976)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
         sa timing: remaining key lifetime (kB/sec): (3914999/28588)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

ASA remoto

```
Remote-ASA#show crypto isakmp sa

  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: 172.16.2.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE

  Remote-ASA#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1

        access-list outside_cryptomap extended permit ip 10.1.1.0
255.255.255.0 10.1.2.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
      current_peer: 172.16.2.1

        #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.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0
      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: 38DA6E51
      current inbound spi : 30D071C0

      inbound esp sas:
      spi: 0x30D071C0 (818966976)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 8192, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4373999/28676)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x0000001F
    outbound esp sas:
      spi: 0x38DA6E51 (953839185)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 8192, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4373999/28676)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

Troubleshoot

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

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

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

Utilice estos comandos como se muestra a continuación:

```
clear crypto ikev1 sa <peer IP address>
Clears the Phase 1 SA for a specific peer.
```

> **Precaución:** El comando **clear crypto isakmp sa** es intrusivo ya que borra todos los túneles VPN activos.

En la versión 8.0(3) y posteriores del software PIX/ASA, se puede despejar una SA IKE individual usando el comando **clear crypto isakmp sa** *<peer ip address>*. En las versiones de software anteriores a 8.0(3), utilice el comando **vpn-sessiondb logoff tunnel-group** *<tunnel-group-name>* para borrar las SAs IKE e IPsec para un solo túnel.

```
Remote-ASA#vpn-sessiondb logoff tunnel-group 172.16.2.1
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions from TunnelGroup "172.16.2.1" logged off : 1

clear crypto ipsec sa peer <peer IP address>
!!! Clears the required Phase 2 SA for specific peer.
debug crypto condition peer < Peer address>
!!! Set IPsec/ISAKMP debug filters.
debug crypto isakmp sa <debug level>
!!! Provides debug details of ISAKMP SA negotiation.
debug crypto ipsec sa <debug level>
!!! Provides debug details of IPsec SA negotiations
undebug all
!!! To stop the debugs
```

Depuraciones utilizadas:

```
debug cry condition peer <remote peer public IP>
debug cry ikev1 127
debug cry ipsec 127
```

Remote-ASA (iniciador)

Ingrese este comando **packet-tracer** para iniciar el túnel:

```
Remote-ASA#packet-tracer input inside icmp 10.1.1.10 8 0 10.1.2.10 detailed

IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
Jan 19 22:00:06 [IKEv1 DEBUG]Pitcher: received a key acquire message, spi 0x0
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple:
Prot=1, saddr=10.1.1.10, sport=0, daddr=10.1.2.10, dport=0
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE Initiator: New Phase 1, Intf
inside, IKE Peer 172.16.2.1 local Proxy Address 10.1.1.0, remote Proxy Address
10.1.2.0, Crypto map (outside_map)
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0)
total length : 132
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
<skipped>...
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +
NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
Automatic NAT Detection Status: Remote end is NOT behind a NAT device
This end is NOT behind a NAT device
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128)
+ VENDOR (13) + NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR ID received 172.16.2.1
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1,
Oakley begin quick mode
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1, PHASE 1 COMPLETED


Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1, IKE Initiator
starting QM: msg id = c45c7b30
:
.
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, Transmitting Proxy Id:
 Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0
 Remote subnet: 10.1.2.0 Mask 255.255.255.0 Protocol 0 Port 0
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE
(10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
```

```
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) +
ID (5) + ID (5) + NONE (0) total length : 172
:
.
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.2.0--255.255.255.0
:
.
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
Security negotiation complete for LAN-to-LAN Group (172.16.2.1)
Initiator, Inbound SPI = 0x30d071c0, Outbound SPI = 0x38da6e51
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 76
:
.
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
PHASE 2 COMPLETED (msgid=c45c7b30)
```

ASA central (Respondedor)

```
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length
:
132
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, Connection landed on tunnel_group
DefaultL2LGroup
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
Generating keys for Responder...
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) +
VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) +
NONE (0) total length : 304
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8)
+ IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96
Jan 20 12:42:35 [IKEv1 DECODE]Group = DefaultL2LGroup, IP = 172.16.1.1,
ID_IPV4_ADDR ID received172.16.1.1
:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) +
VENDOR (13) + NONE (0) total length : 96
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, PHASE 1 COMPLETED
:
```

```
.
Jan 20 12:42:35 [IKEv1 DECODE]IP = 172.16.1.1, IKE Responder starting QM:
msg id = c45c7b30
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE
RECEIVED Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) +
NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Received remote
IP Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0,
Protocol 0, Port 0:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup,
IP = 172.16.1.1, Received local
IP Proxy Subnet data in ID Payload: Address 10.1.2.0, Mask 255.255.255.0,
Protocol 0, Port 0Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup,
IP = 172.16.1.1, processing notify payload
Jan 20 12:42:35 [IKEv1] Group = DefaultL2LGroup, IP = 172.16.1.1, QM
IsRekeyed old sa not found by addr
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Static Crypto Map
check, map outside_dyn_map, seq = 1 is a successful match
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, IKE
Remote Peer configured for crypto map: outside_dyn_map
:
.
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
Transmitting Proxy Id:  Remote subnet: 10.1.1.0  Mask 255.255.255.0 Protocol 0  Port 0
Local subnet: 10.1.2.0 mask 255.255.255.0 Protocol 0 Port 0:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=c45c7b30)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE
(0) total length : 172 Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED
Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 52:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Security
negotiation complete for LAN-to-LAN Group (DefaultL2LGroup) Responder,
Inbound SPI = 0x38da6e51, Outbound SPI = 0x30d071c0:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1,
PHASE 2 COMPLETED (msgid=c45c7b30)
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Adding static
route for L2L peer coming in on a dynamic map. address: 10.1.1.0, mask: 255.255.255.0
```

Información Relacionada

- Referencias de Comandos de Cisco ASA Series
- Página de Soporte de IPSec Negotiation/IKE Protocols
- Solicitudes de Comentarios (RFC)
- Soporte técnico y documentación - Cisco System