ASA 5500-to-ASA Dynamic-to-Static IKEv1/IPsec Configuratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe de Adaptieve security applicatie (ASA) ingeschakeld kan worden om dynamische IPsec site-to-site VPN-verbindingen te accepteren van elk dynamisch peer (ASA in dit geval). Zoals het netwerkdiagram in dit document toont, wordt de IPsec-tunnel gevestigd wanneer de tunnel van het Afstandsbediening-kanaal wordt geïnitieerd. Central-ASA kan geen VPN-tunnel initiëren vanwege de dynamische configuratie van IPsec. Het IP-adres van Remote-ASA is onbekend.

Configureer Centraal-ASA om dynamisch verbindingen te accepteren van een wild-kaart IP adres (0.0.0.0/0) en een pre-gedeelde sleutel met een wild-kaart. Remote-ASA is dan geconfigureerd om het verkeer te versleutelen van lokale naar Centraal-ASA subnetten zoals gespecificeerd door de crypto toegangslijst. Beide partijen verlenen NAT-vrijstelling (Network Address Translation) om NAT te omzeilen voor IPsec-verkeer.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

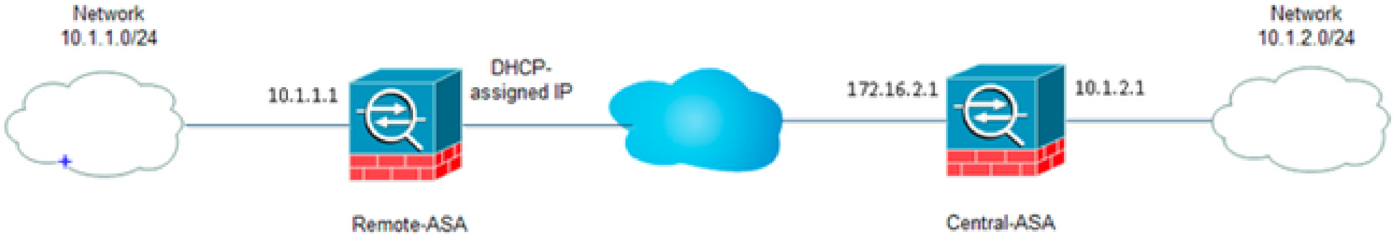
De informatie in dit document is gebaseerd op Cisco ASA (5510 en 5520) Firewallsoftwarerelease 9.x en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

> Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

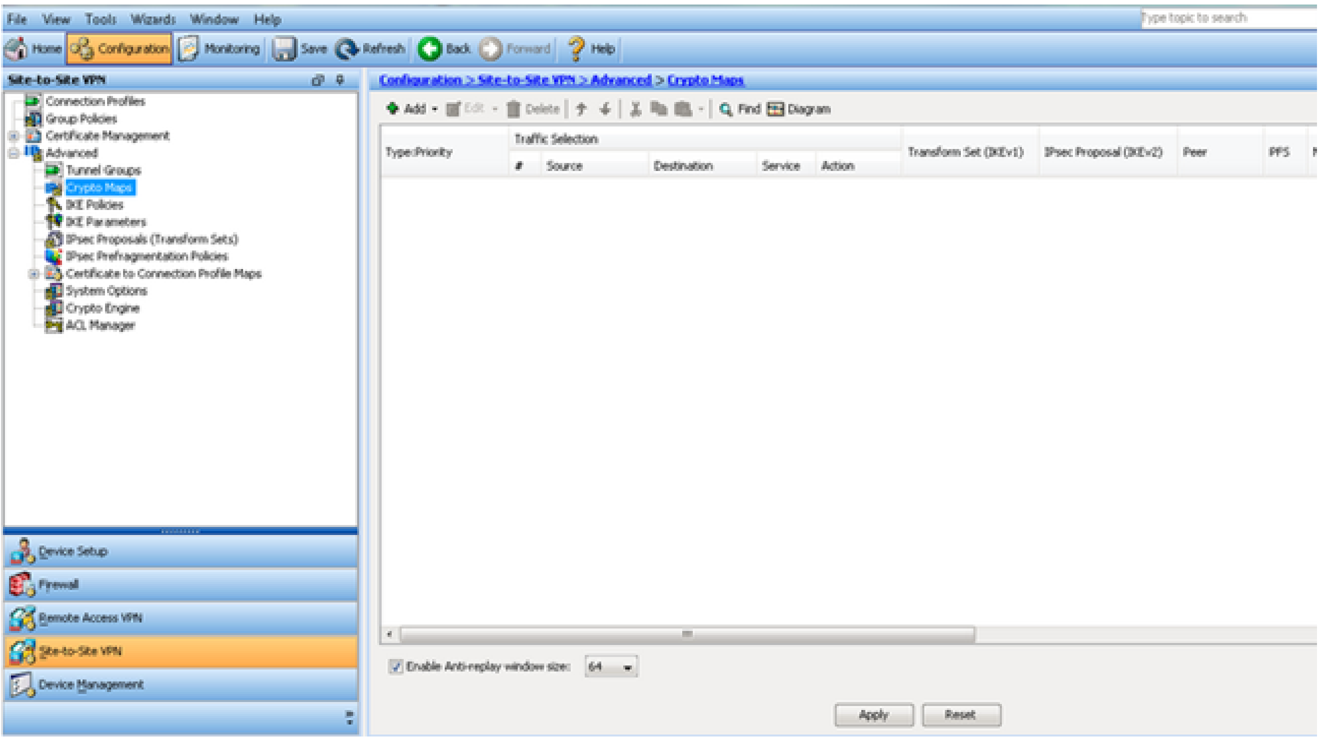


ASDM-configuratie

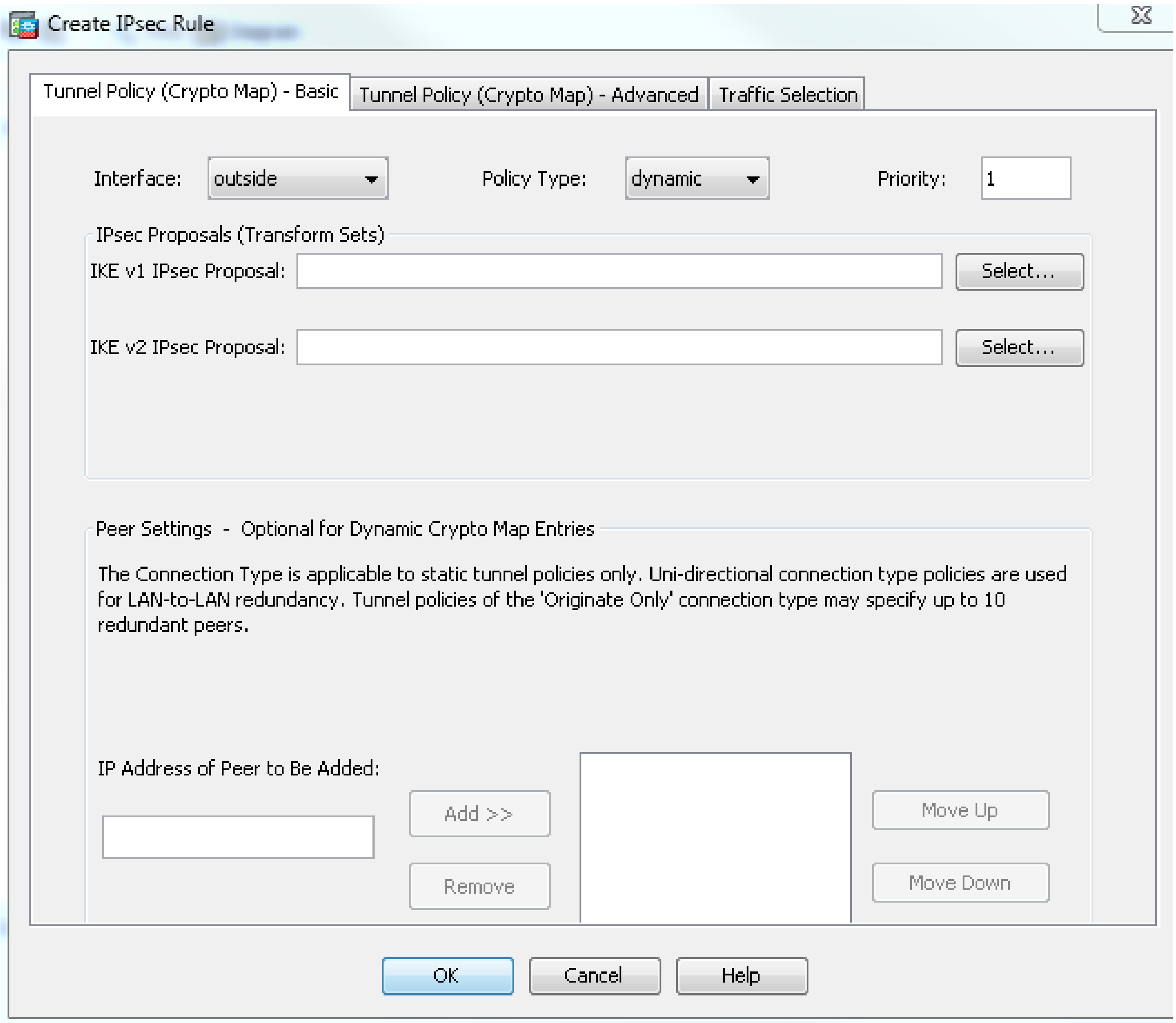
Centraal-ASA (statische peer)

Op een ASA met een Statisch IP-adres, stel VPN op dusdanige wijze in dat het dynamische verbindingen van een onbekend peer accepteert terwijl het de peer nog steeds authentiek maakt met behulp van een IKEv1 Pre-Shared Key:

1. Kies **Configuration > Site-to-Site VPN > Advanced > Crypto Maps.** Het venster toont de lijst van crypto kaart ingangen die reeds op zijn plaats zijn (als er). Aangezien ASA niet weet wat het Peer IP-adres is, moet ASA de verbinding **Dynamic-Map** accepteren met een andere transformatie-set (IPsec Proposal). Klik op **Toevoegen**.



2. In het venster Create IPsec Rule, van het tabblad Tunnel Beleid (Crypto Map) - het tabblad Basis, kiest u **buiten** van de vervolgkeuzelijst Interface en **dynamisch** van de vervolgkeuzelijst Beleidstype. In het veld Prioriteit de prioriteit voor deze ingang toewijzen voor het geval er meerdere items zijn onder Dynamische-Kaart. Klik vervolgens op **Selecteer** naast het veld IKE v1 IPsec-voorstel om het IPsec-voorstel te selecteren.



Interface: outside

Policy Type: dynamic

Priority: 1

IPsec Proposals (Transform Sets)

IKE v1 IPsec Proposal:

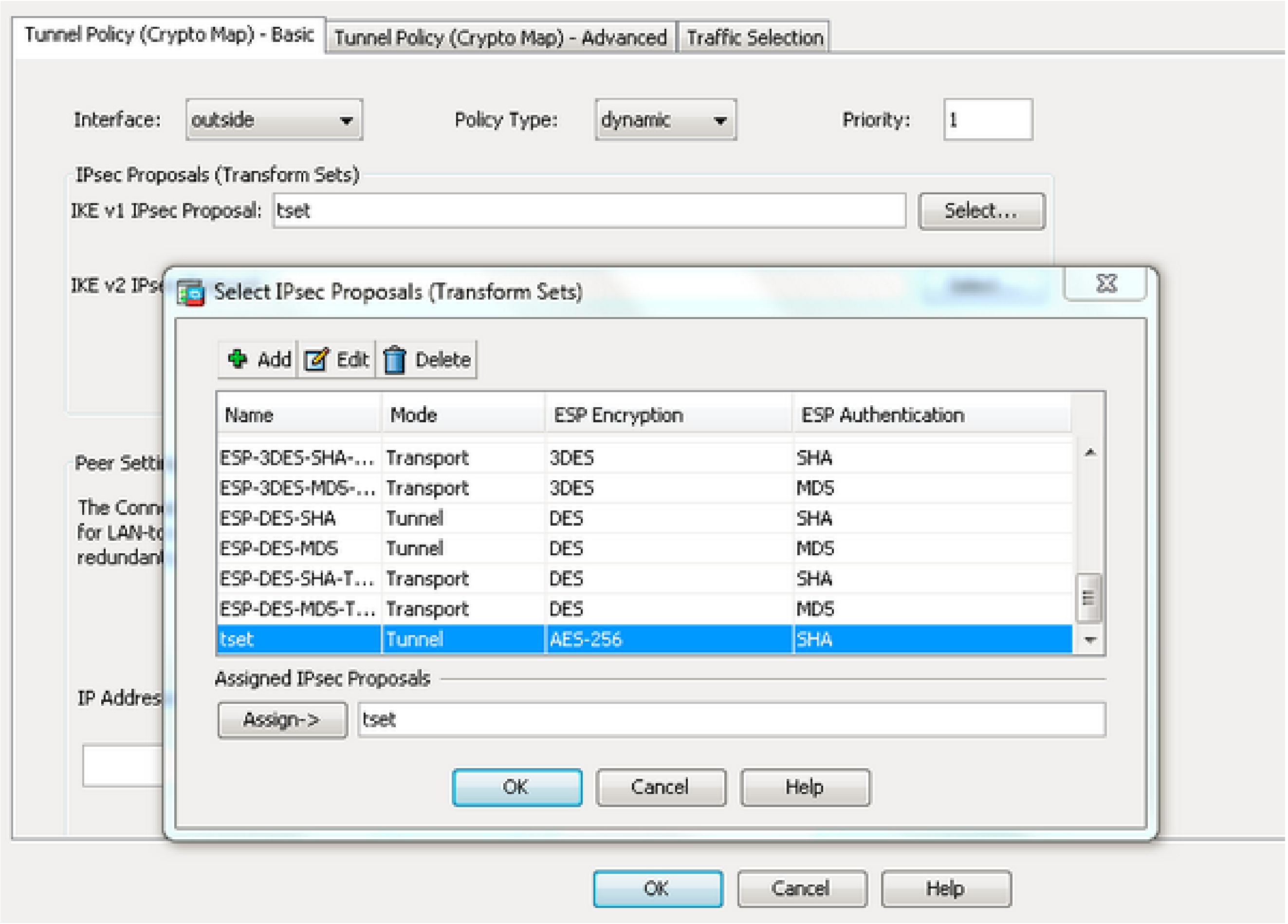
IKE v2 IPsec Proposal:

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. Wanneer het dialoogvenster IPsec-voorstellen selecteren (Instellen omzetten) wordt geopend, kiest u uit de huidige IPsec-voorstellen of klikt u op **Toevoegen** om er een nieuwe te maken en hetzelfde te gebruiken. Klik op **OK** wanneer u klaar bent.



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: tset

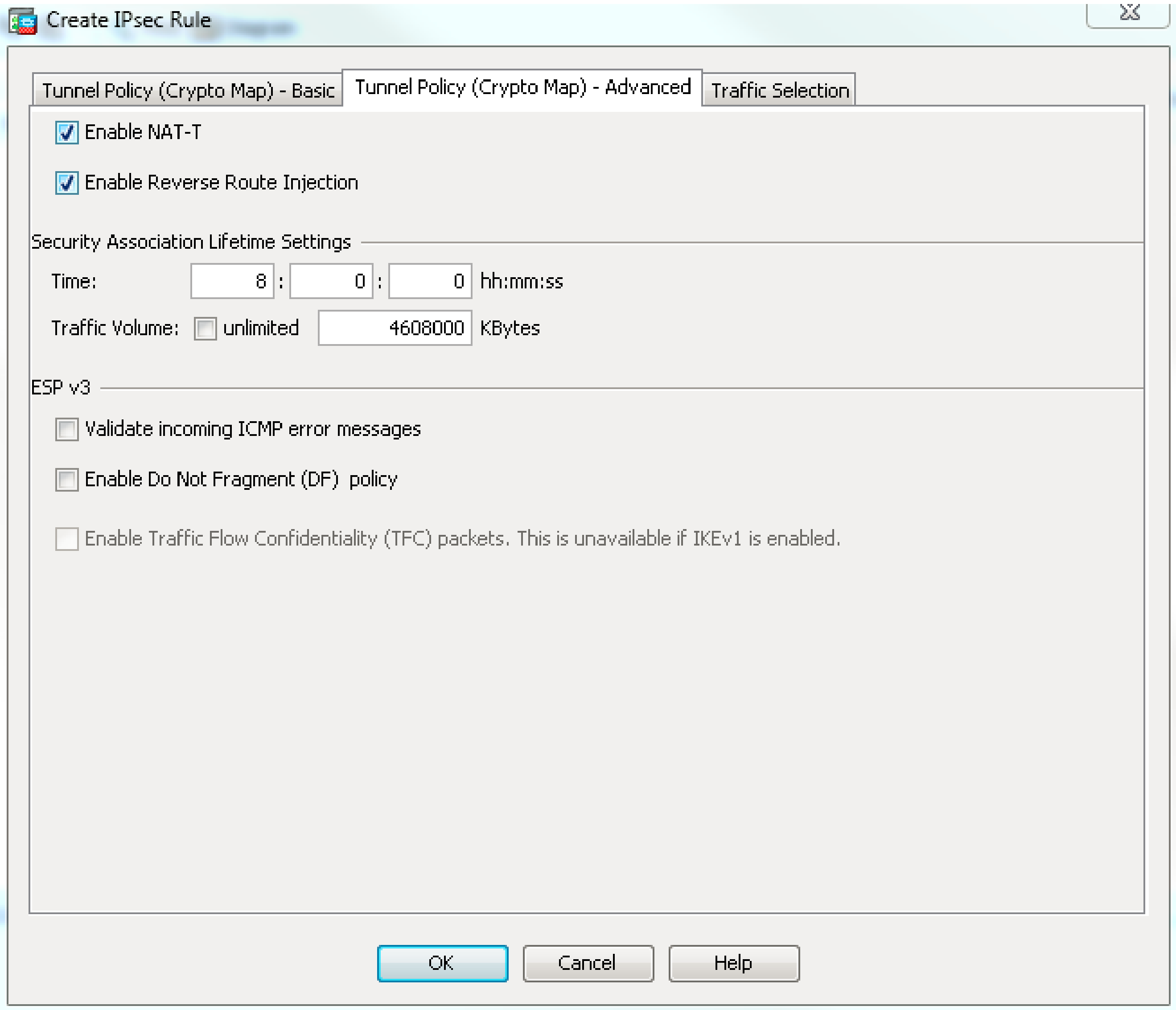
Select...
IKE v2 IPs
Peer Setti
The Conn
for LAN-to
redundan
IP Addres
Select IPsec Proposals (Transform Sets)
Add
Edit
Delete

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

Assign-> tset

4. Vanuit het tabblad Geavanceerd van Tunnel beleid (Crypto Map) controleert u het vakje **NAT-T** inschakelen (verplicht als een van de gelijken achter een NAT-apparaat staat) en het vakje **Routeinjectie inschakelen**. Wanneer de VPN-tunnel voor de dynamische peer verschijnt, installeert ASA een dynamische route voor het onderhandeld externe VPN-netwerk dat naar de VPN-interface
wijst.

 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

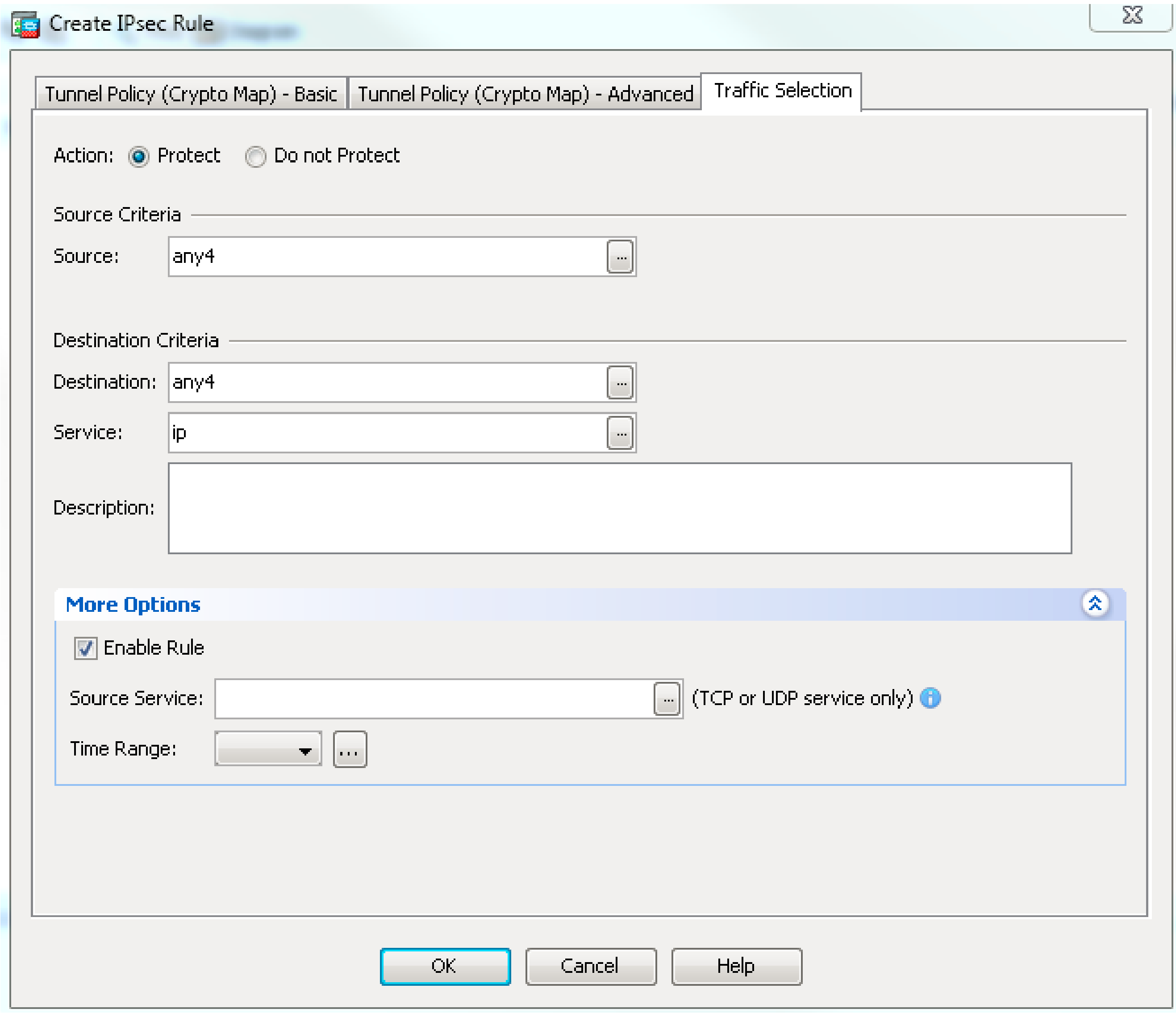
ESP v3

□ Validate incoming ICMP error messages

□ Enable Do Not Fragment (DF) policy

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

Optioneel kunt u in het tabblad Verkeerselectie ook het interessante VPN-verkeer voor de dynamische peer definiëren en op **OK**
klikken.



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

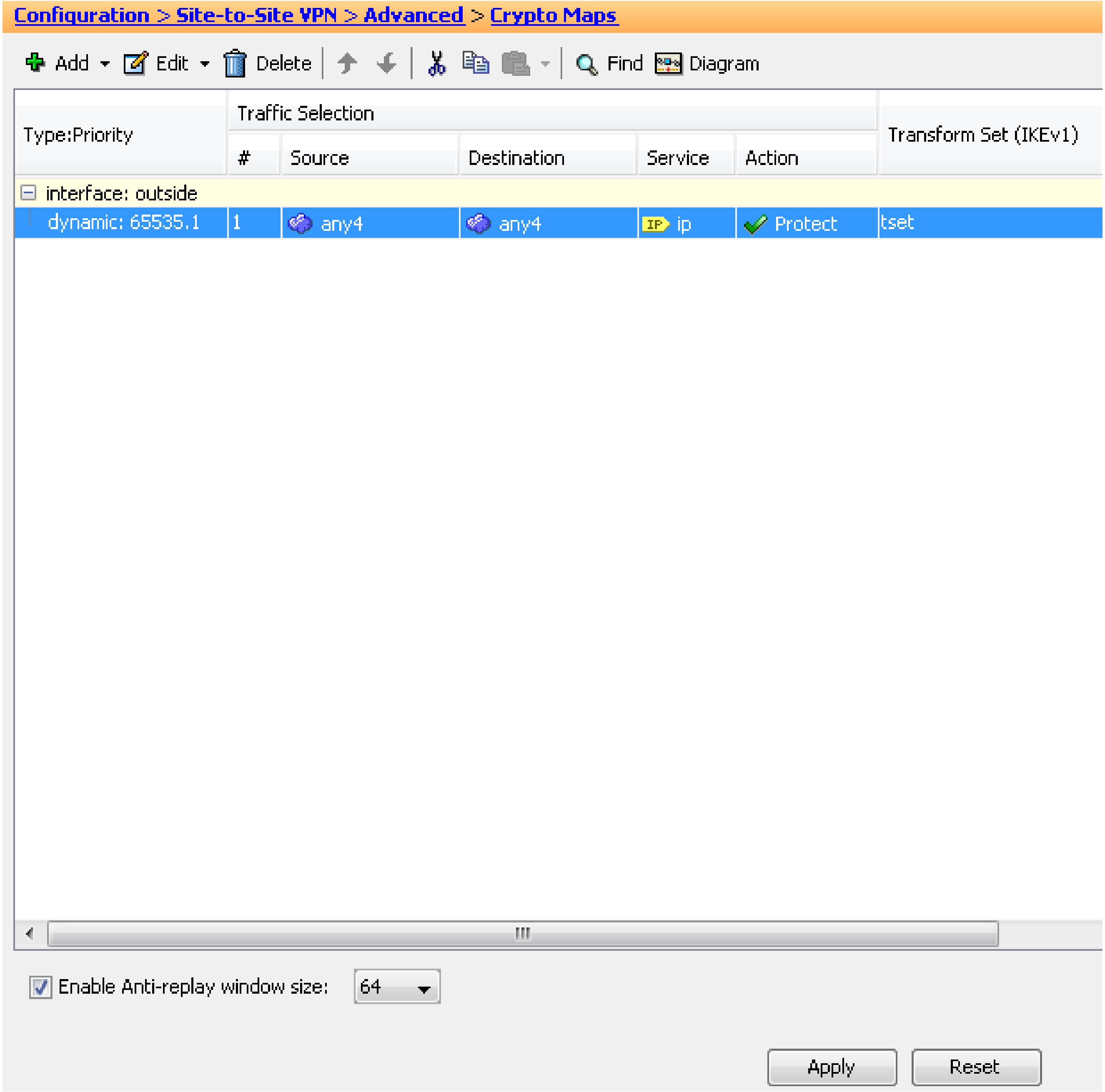
Description:

More Options

☑ Enable Rule

Source Service: (TCP or UDP service only)

Time Range:

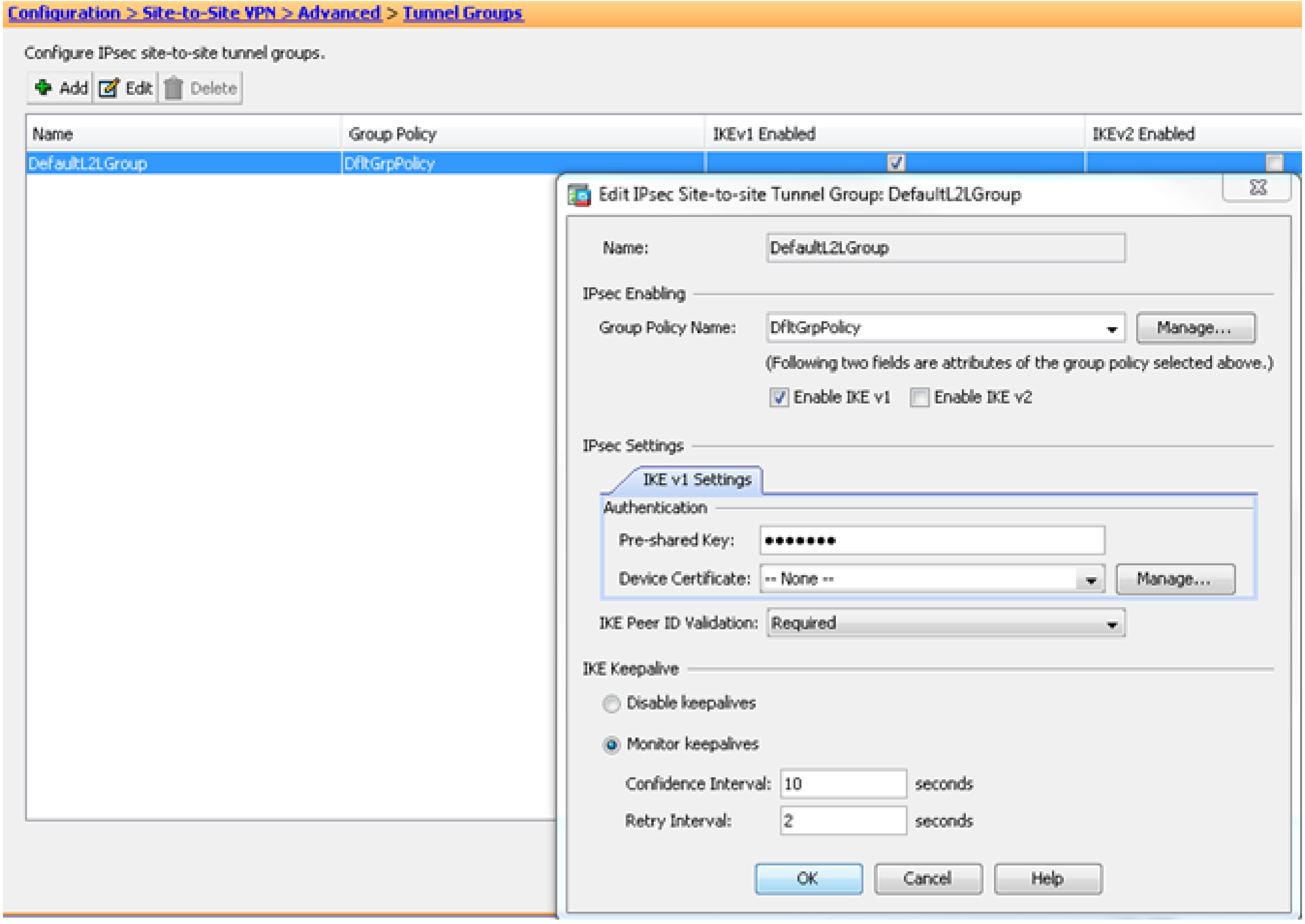


Type:Priority	Traffic Selection					Transform Set (IKEv1)
	#	Source	Destination	Service	Action	
⊟ interface: outside						
dynamic: 65535.1	1	any4	any4	ip	✓ Protect	tset

☑ Enable Anti-replay window size: 64

Zoals eerder vermeld, aangezien ASA geen informatie heeft over het externe dynamische peer IP-adres, landt het onbekende verbindingsverzoek onder DefaultL2LGroup dat standaard op ASA bestaat. Om verificatie te laten slagen moet de vooraf gedeelde toets (cisco123 in dit voorbeeld) die op de externe peer is ingesteld, overeenkomen met één bij DefaultL2LGgroup.

5. Kies **Configuratie > Site-to-Site VPN > Geavanceerd > Tunnelgroepen**, selecteer **DefaultL2LG**, klik op **Bewerken** en stel de gewenste voorgedeelde toets in. Klik op **OK** als u klaar
bent.



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

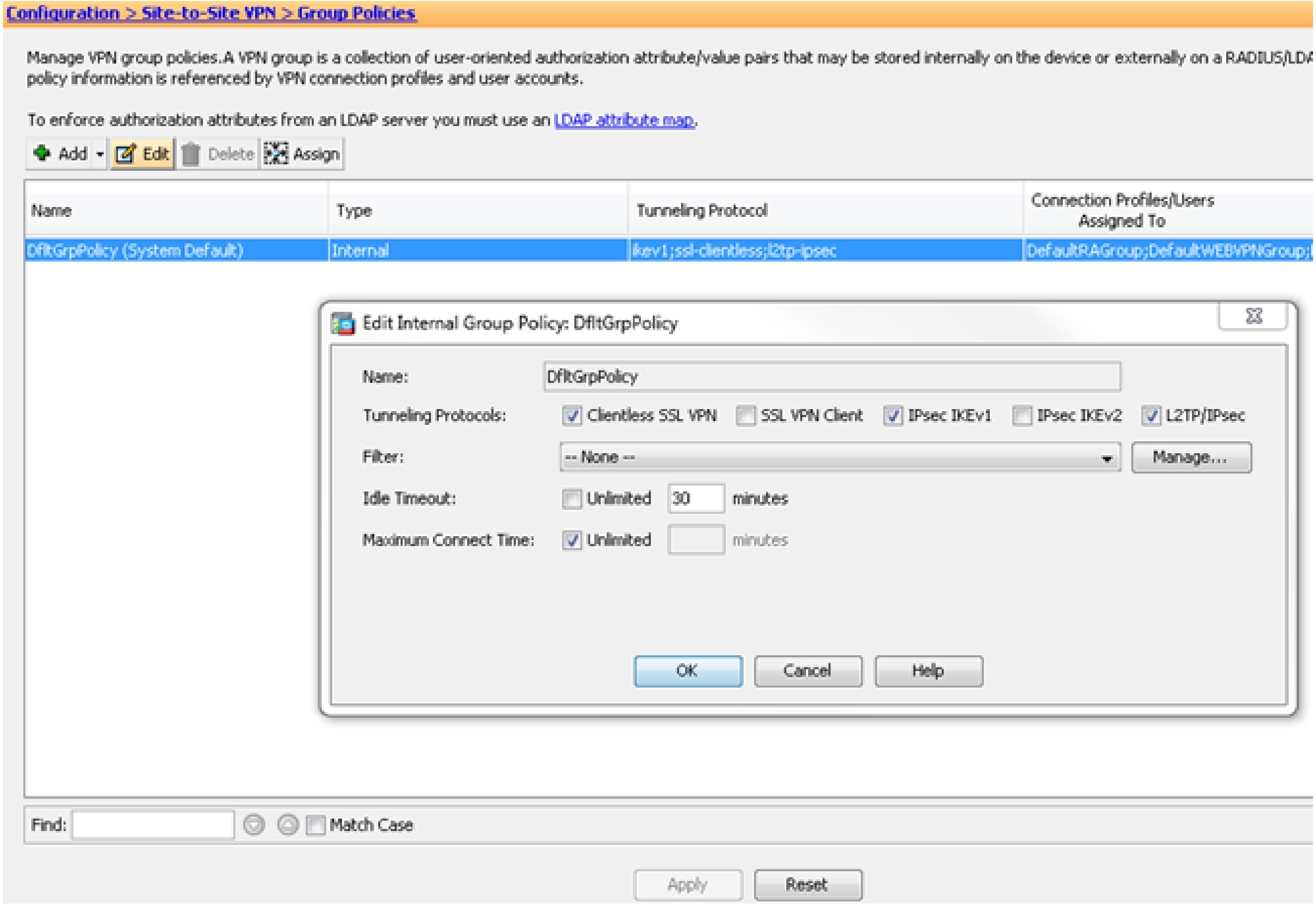
● Monitor keepalives

Confidence Interval: 10 seconds

Retry Interval: 2 seconds

Opmerking: Dit creëert een pre-gedeelde sleutel van de statische peer (Centraal-ASA). Elk apparaat/peer die deze vooraf gedeelde sleutel en zijn aanpassingsvoorstellen kent kan met succes een VPN-tunnel en toegangsbronnen via VPN creëren. Zorg ervoor dat deze pre-skared toets niet gedeeld wordt met onbekende entiteiten en niet makkelijk te raden is.

6. Kies **Configuration** > **Site-to-Site VPN** > **Groepsbeleid** en selecteer het groepsbeleid van uw keuze (in dit geval de standaardinstelling groepsbeleid). Klik op **Bewerken** en bewerk het groepsbeleid in het dialoogvenster Intern groepsbeleid bewerken. Klik op **OK** wanneer u klaar bent.



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

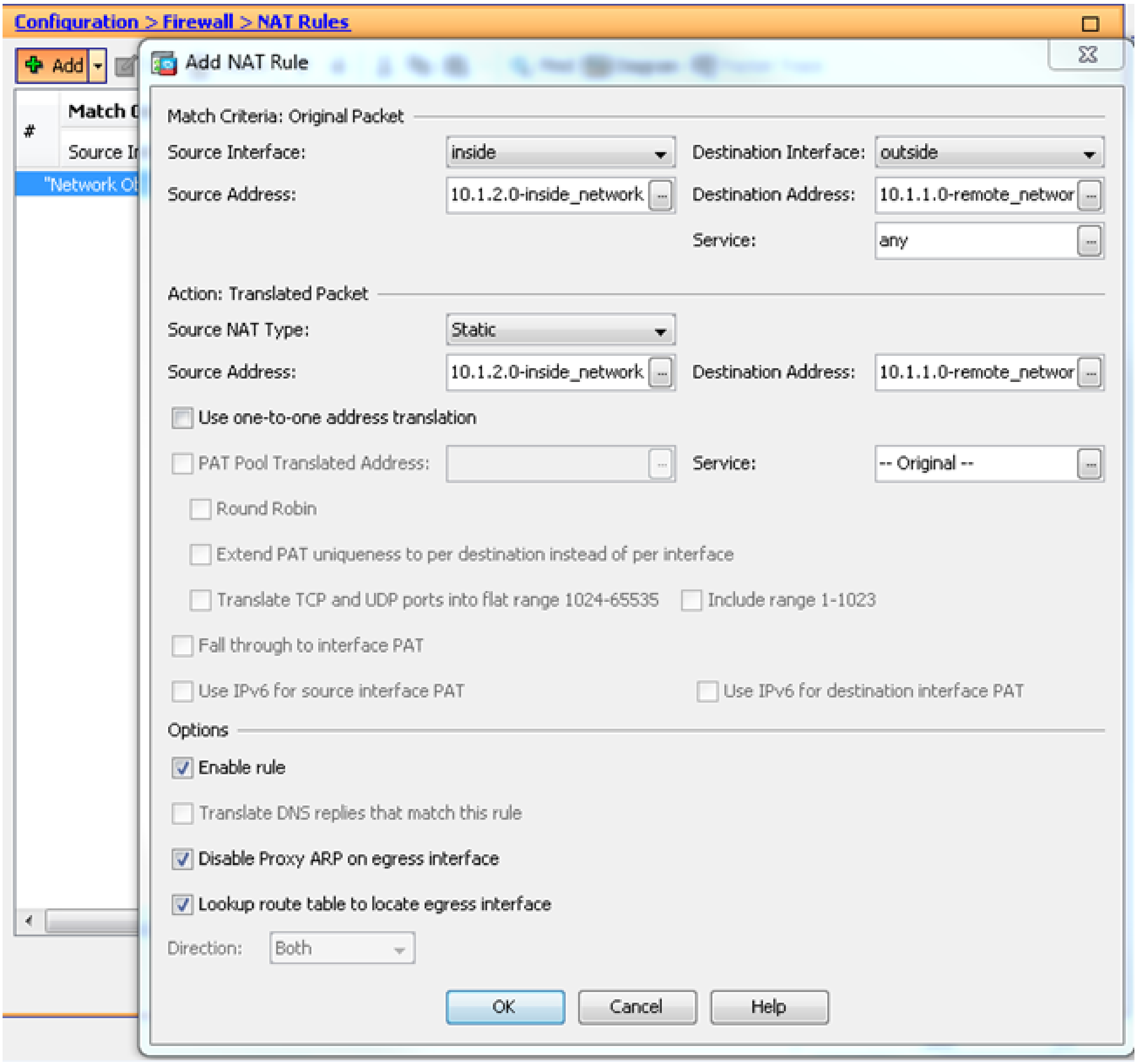
Tunneling Protocols: ☑ Clientless SSL VPN ☐ SSL VPN Client ☑ IPsec IKEv1 ☐ IPsec IKEv2 ☑ L2TP/IPsec

Filter: -- None --

Idle Timeout: ☐ Unlimited 30 minutes

Maximum Connect Time: ☑ Unlimited minutes

7. Kies **Configuration** > **Firewall** > **NAT-regels** en kies in het venster Add Nat Rule een no-nee-regel (NAT-EXEMPT) voor VPN-verkeer. Klik op **OK** wanneer u klaar bent.



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

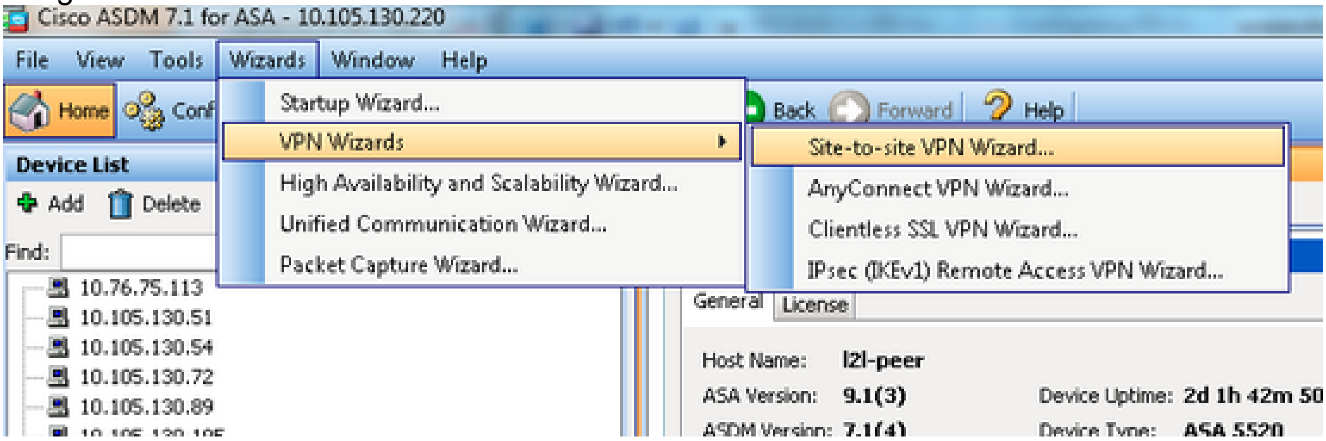
☑ Disable Proxy ARP on egress interface

☑ Lookup route table to locate egress interface

Direction: Both

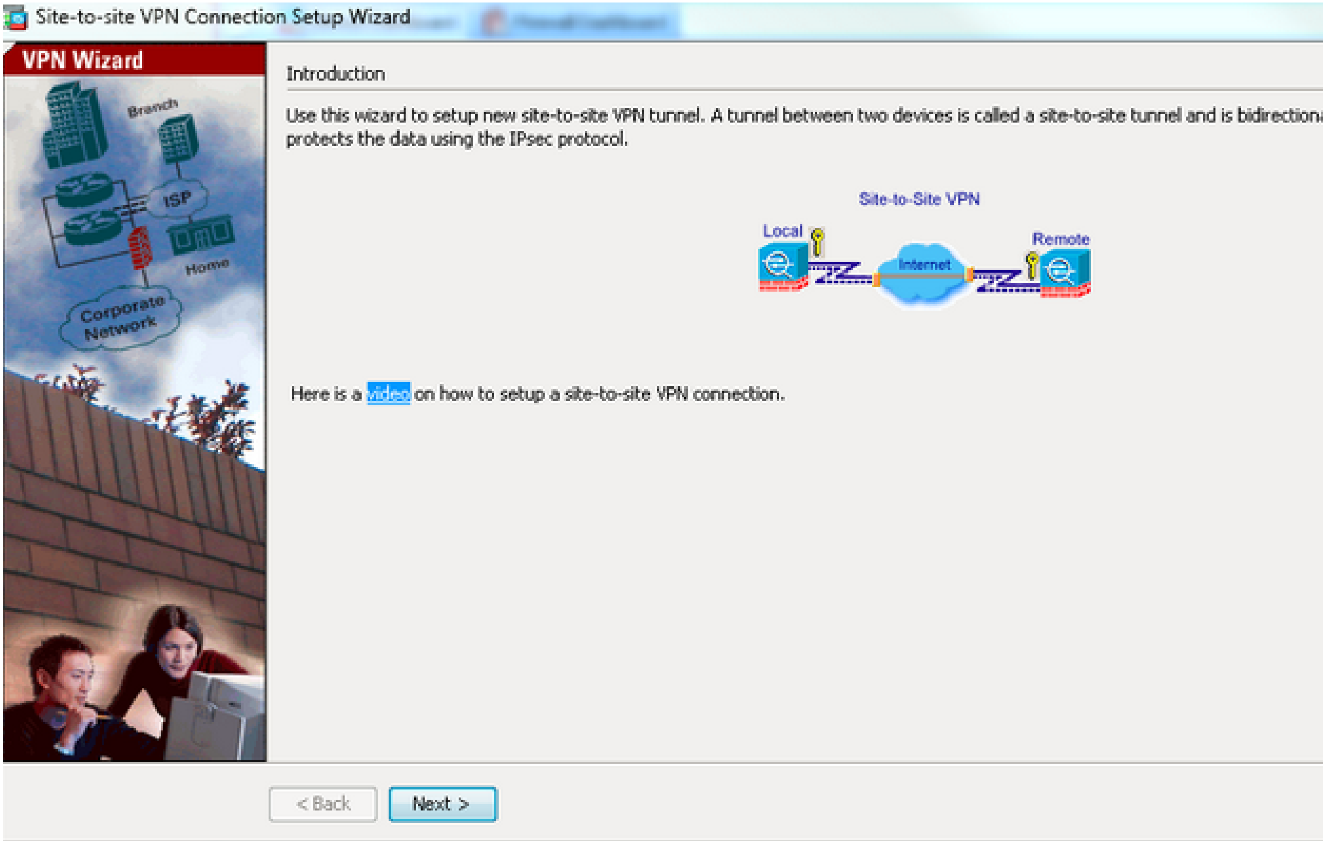
Remote-ASA (dynamische peer)

1. Kies **Wizard > VPN Wizard > Site-to-site VPN Wizard** nadat de ASDM-toepassing op de ASA is
aangesloten.



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. Klik op
Volgende.



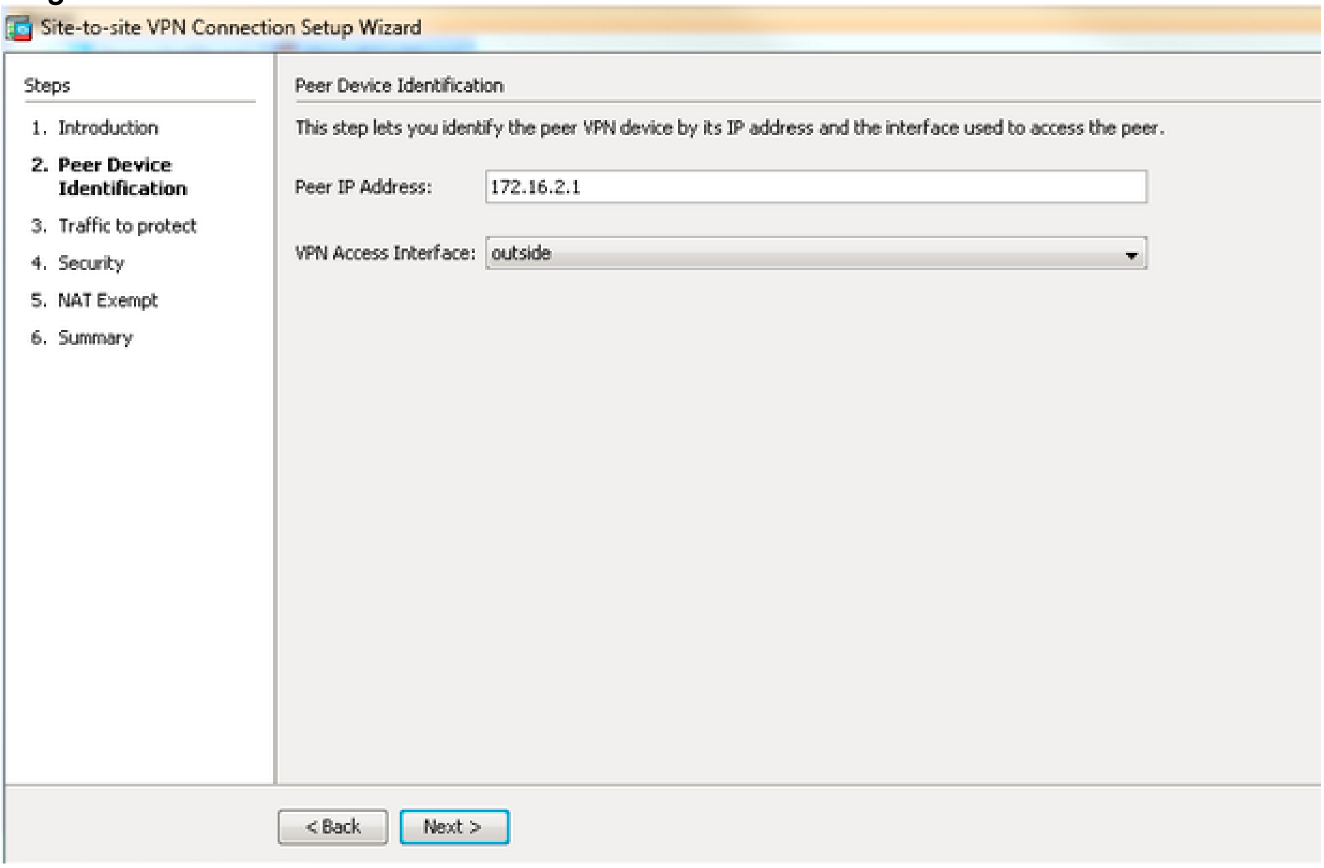
Site-to-site VPN Connection Setup Wizard

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. Kies **buiten** van de vervolgkeuzelijst VPN-toegangsinterface om het externe IP-adres van de externe peer te specificeren. Selecteer de interface (**WAN)** waar de crypto-map wordt toegepast. Klik op
Volgende.



Site-to-site VPN Connection Setup Wizard

Peer Device Identification

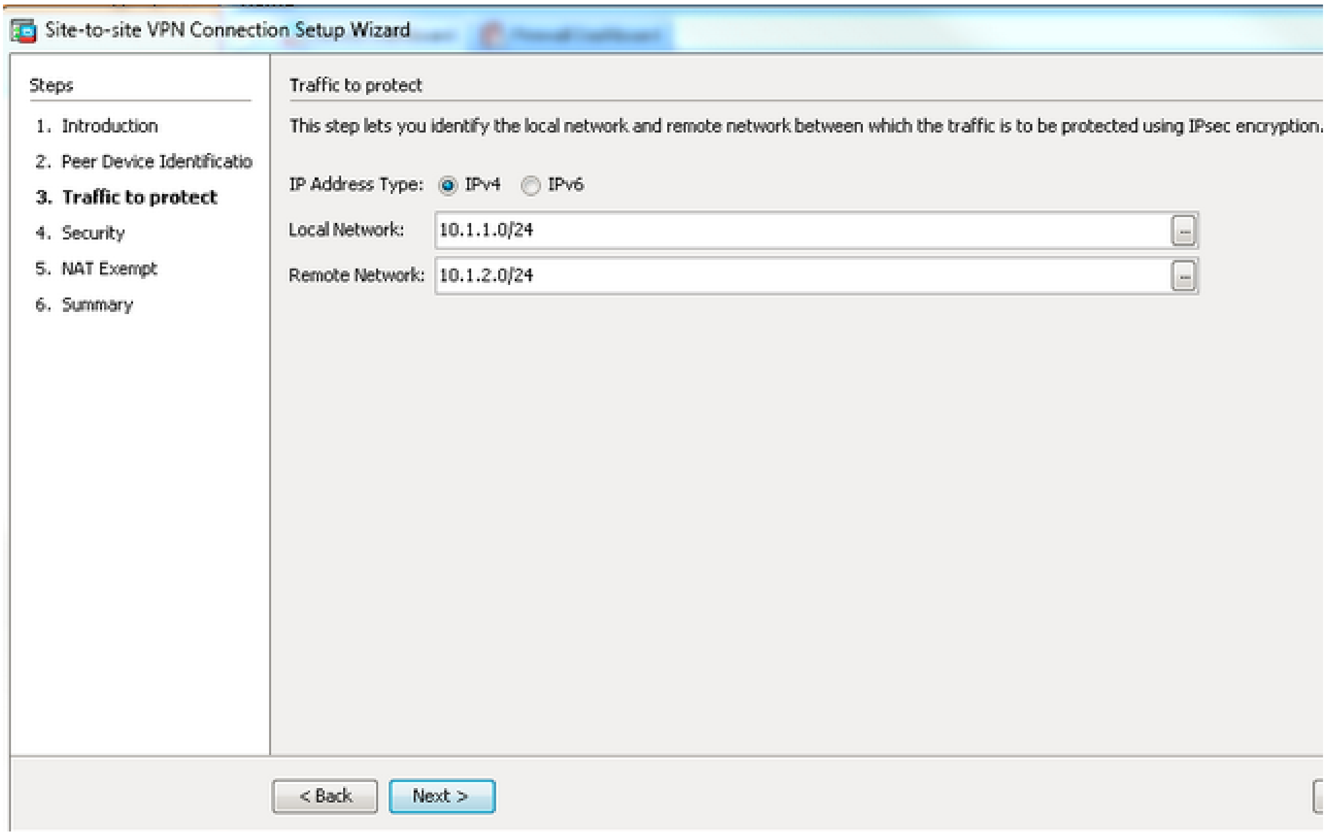
This step lets you identify the peer VPN device by its IP address and the interface used to access the peer.

Peer IP Address: 172.16.2.1

VPN Access Interface: outside

4. Specificeer de hosts/netwerken die moeten worden toegestaan door de VPN-tunnel te gaan. In deze stap moet u de lokale netwerken en Remote-netwerken voor de VPN-tunnelleiding bieden. Klik op de knoppen naast de velden Local Network en Remote Network en kies het adres naar behoefte. Klik op **Volgende** als u klaar

bent.


Site-to-site VPN Connection Setup Wizard

Traffic to protect

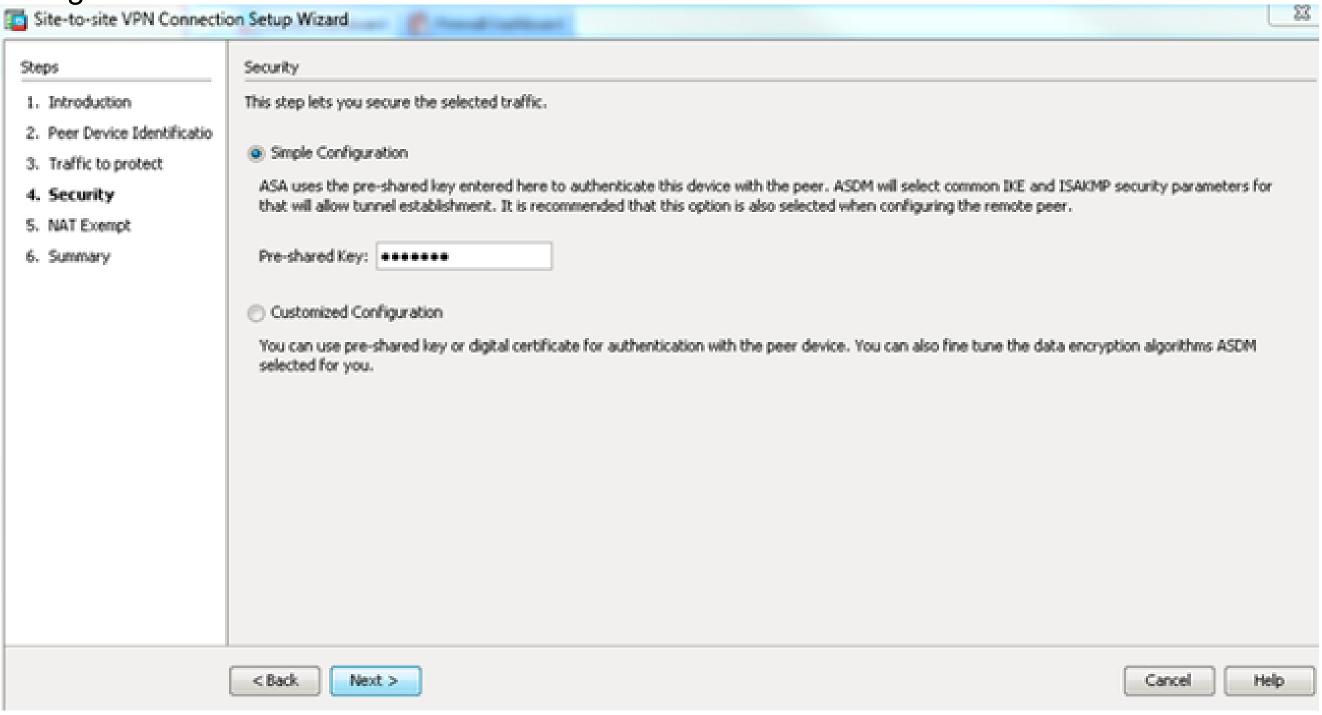
This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption.

IP Address Type: ● IPv4 ○ IPv6

Local Network: 10.1.1.0/24

Remote Network: 10.1.2.0/24

5. Voer de te gebruiken authenticatie-informatie in, die vooraf gedeeld wordt in dit voorbeeld. De pre-gedeelde sleutel die in dit voorbeeld wordt gebruikt is Cisco123. De naam van de Tunnel Groep is het verre peer IP adres standaard als u LAN-to-LAN (L2L) VPN configureren.


Site-to-site VPN Connection Setup Wizard

Security

This step lets you secure the selected traffic.

● Simple Configuration

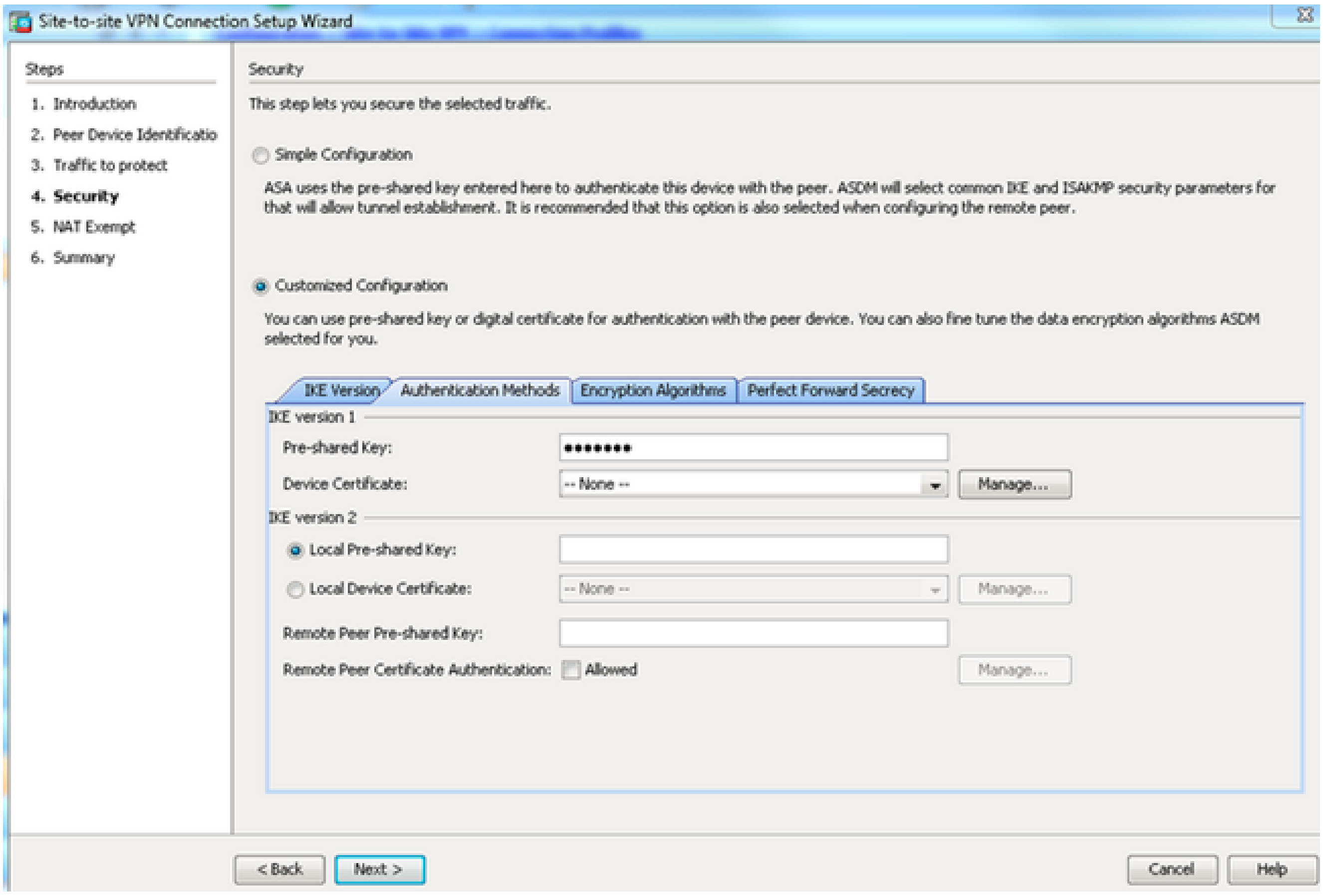
ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.

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.

OFU kunt de configuratie aanpassen om het IKE- en IPsec-beleid van uw keuze te omvatten. Er moet ten minste één overeenstemmend beleid tussen de verschillende partijen bestaan:Typ in het tabblad Verificatiemethoden de vooraf gedeelde sleutel van IKE, versie 1, in het veld Voorgedeelde sleutel. In dit voorbeeld is het
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:

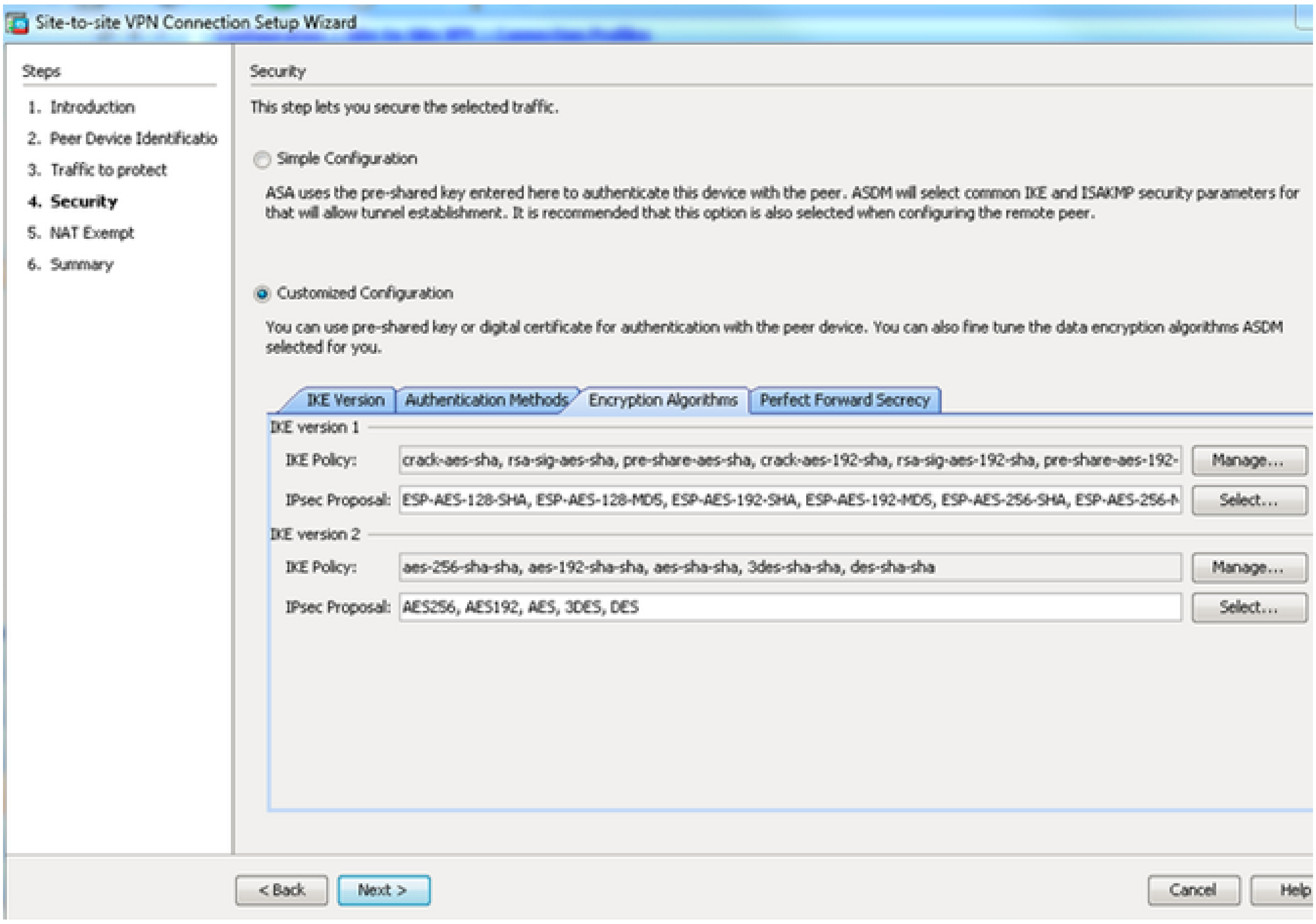
○ Local Device Certificate: -- None --

Remote Peer Pre-shared Key:

Remote Peer Certificate Authentication: □ Allowed

Klik op het tabblad **Encryption Algorithms**.

6. Klik op **Manager** naast het veld IKE-beleid op **Toevoegen** en stel een aangepast IKE-beleid in **(**fase-1**)**. Klik op **OK** wanneer u klaar bent.



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

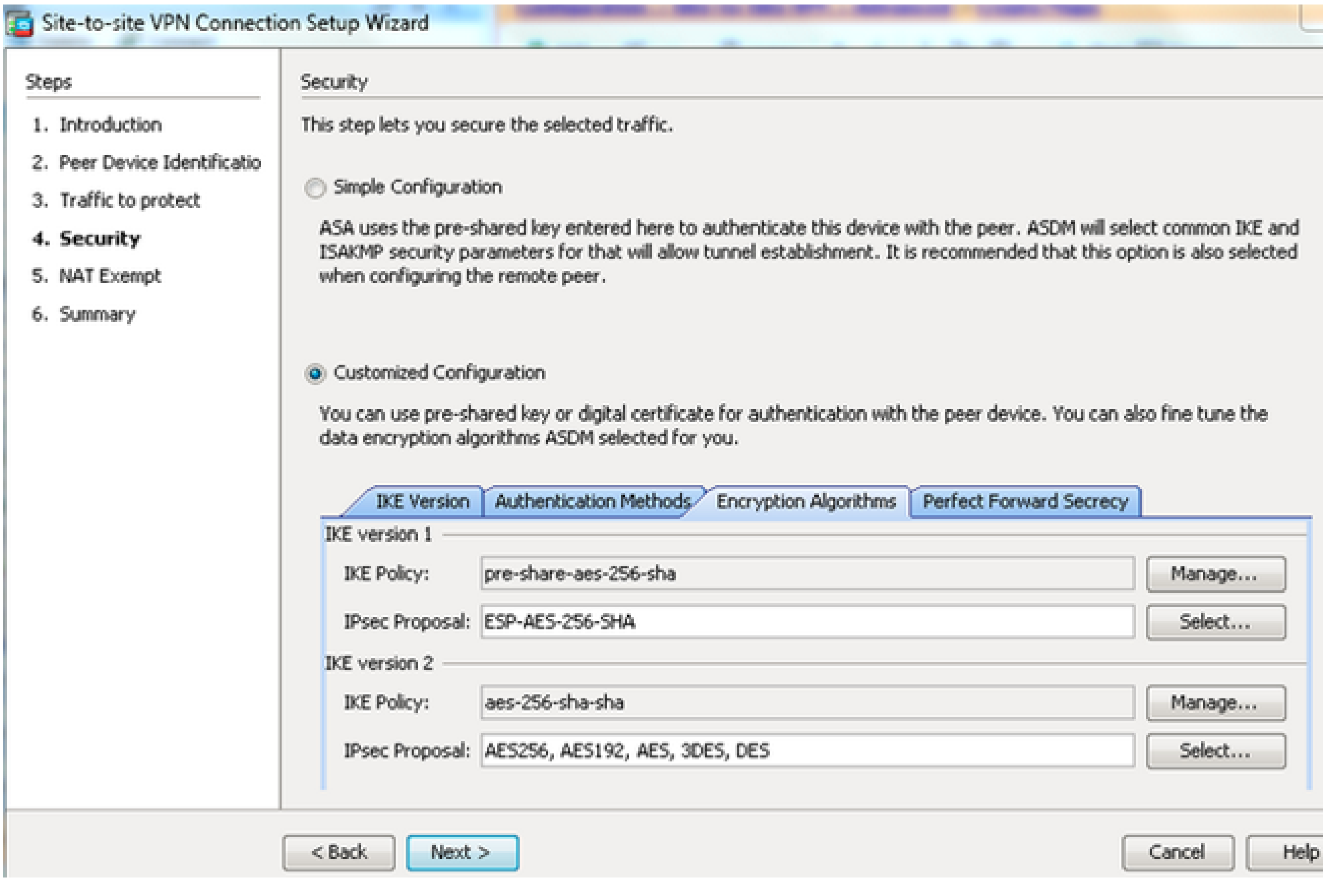
IKE version 2

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. Klik op **Selecteer** naast het veld IPsec Proposal en selecteer het gewenste IPsec Proposal.

Klik op **Volgende** als u klaar bent.



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

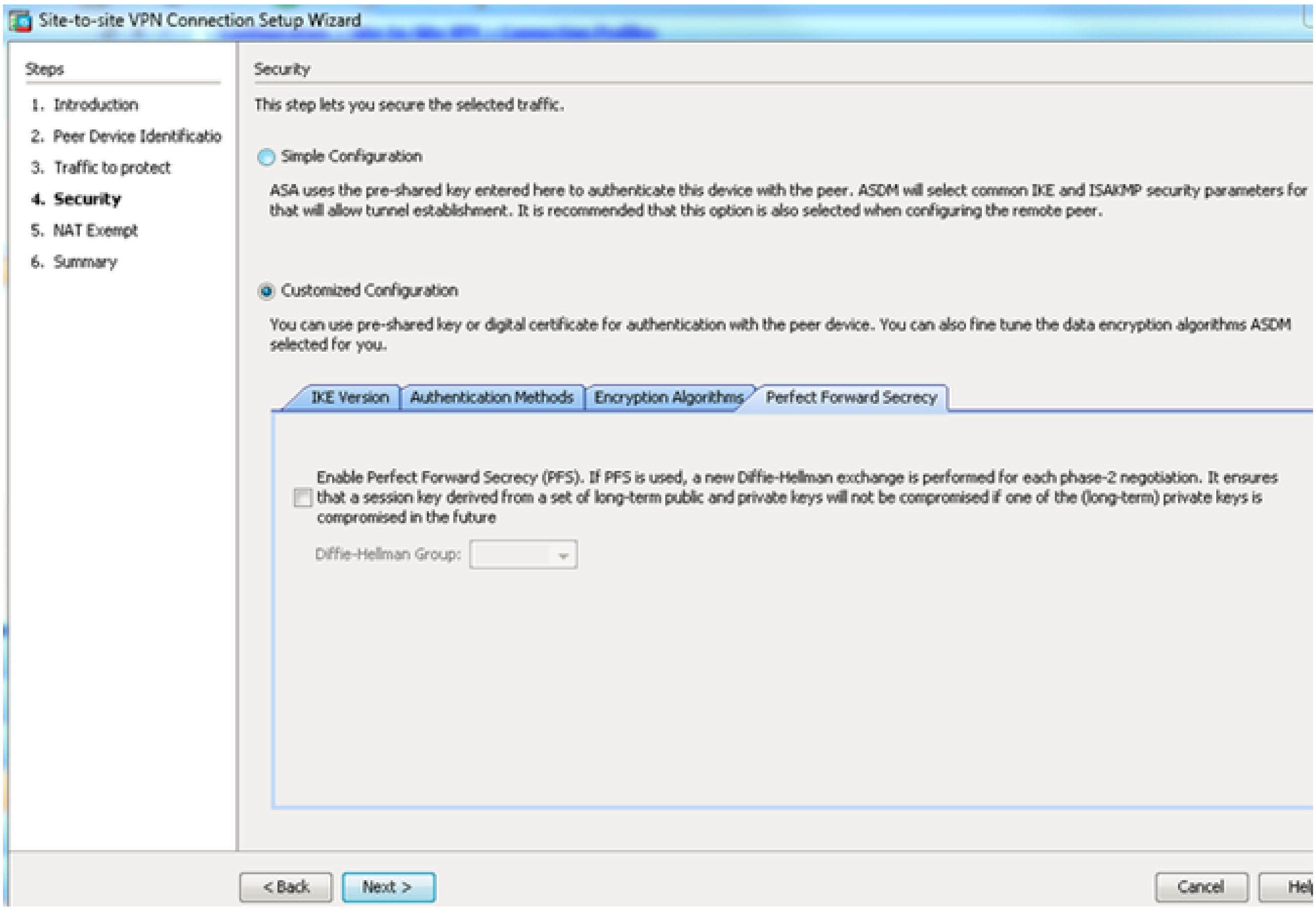
IPsec Proposal: ESP-AES-256-SHA

IKE version 2

IKE Policy: aes-256-sha-sha

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

U kunt naar het tabblad Perfect Forward Security gaan en het vakje **Enable Perfect Forward Security (PFS)** controleren. Klik op **Volgende** als u klaar bent.



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

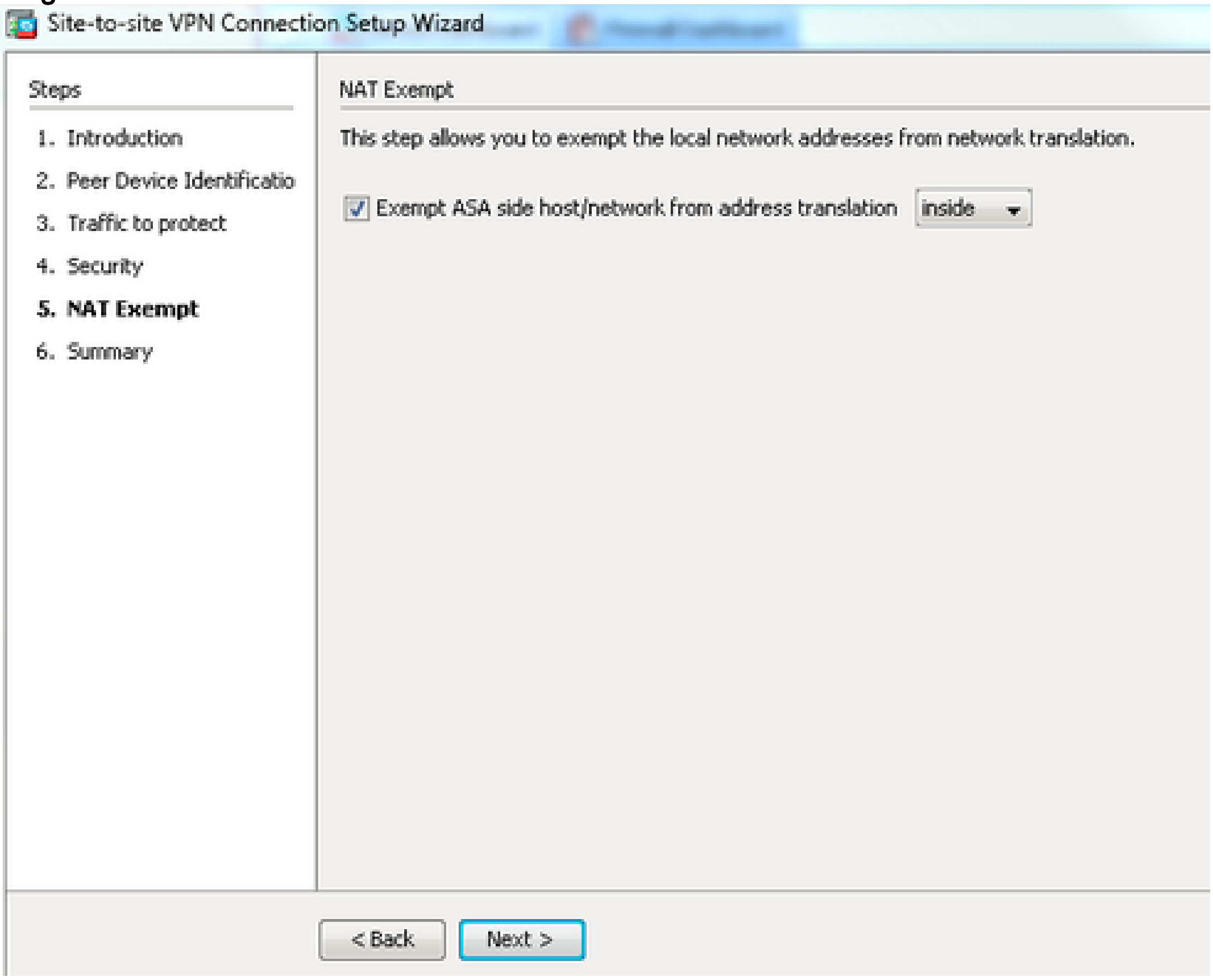
You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.

□ 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. Controleer de **vrijgestelde ASA side host/network van het** aanvinkvakje **van adresvertaling**

om het tunnelverkeer vanaf het begin van de netwerkadresomzetting te voorkomen. Kies **lokaal of binnen** in de vervolgkeuzelijst om de interface in te stellen waar het lokale netwerk bereikbaar is. Klik op **Volgende.**

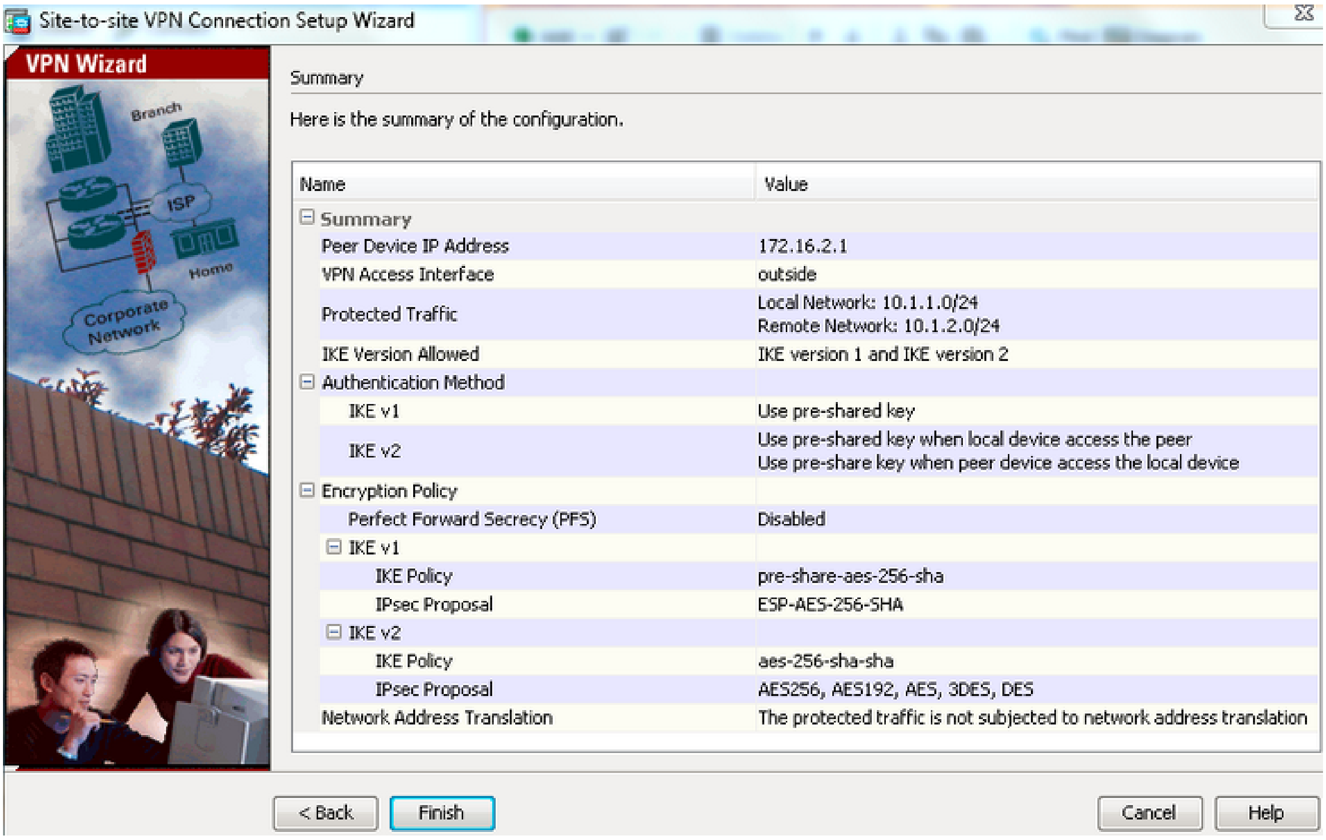


NAT Exempt

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

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

9. ASDM geeft een samenvatting van de zojuist geconfigureerd VPN-software weer. Controleer en klik op **Voltooien**.



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

CLI-configuratie

Configuratie Central ASA (statische peer)

1. Configureer een NO-NAT/NAT-EXEMPT regel voor VPN-verkeer zoals dit voorbeeld aangeeft:
```
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. Configureer de voorgedeelde toets onder DefaultL2LGgroup om elke externe Dynamic-L2L-peer te controleren:
```
tunnel-group DefaultL2LGroup ipsec-attributes
 ikev1 pre-shared-key cisco123
```
3. Het fase-2/ISAKMP-beleid definiëren:
```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
```
4. Defineer het fase-2 transformatie set/IPsec-beleid:
```
crypto ipsec ikev1 transform-set tset esp-aes-256 esp-sha-hmac
```
5. Configureer de dynamische kaart met deze parameters: Vereiste transformatieToegang voor omgekeerde routeinjectie (RI), waardoor de security applicatie kan leren voor het verzenden van informatie voor verbonden klanten (optioneel)

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

6. Bind de dynamische kaart aan de crypto kaart, pas de crypto kaart toe en laat ISAKMP/IKEv1 op de buiteninterface toe:
   ```
   crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map

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

Remote-ASA (dynamische peer)

1. Configureer een NAT-vrijstellingsregel voor VPN-verkeer:
   ```
   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. Configureer een tunnelgroep voor een statische VPN-peer en een vooraf gedeelde sleutel.
   ```
   tunnel-group 172.16.2.1 type ipsec-l2l
   tunnel-group 172.16.2.1 ipsec-attributes
   ikev1 pre-shared-key cisco123
   ```
3. Definieer FASE-1/ISAKMP-beleid:
   ```
   crypto ikev1 policy 10
   authentication pre-share
   encryption aes-256
   hash sha
   group 2
   lifetime 86400
   ```
4. Defineert een fase-2 transformatie set/IPsec beleid:
   ```
   crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
   ```
5. Configureer een toegangslijst die interessant VPN-verkeer/netwerk definieert:
   ```
   access-list outside_cryptomap extended permit ip object
   10.1.1.0-inside_network object 10.1.2.0-remote_network
   ```
6. Configuratie van statische crypto kaart met deze parameters: Toegangslijst van Crypto/VPNRemote IPsec peer-IP-adresVereiste transformatie
   ```
   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. Pas de crypto kaart toe en laat ISAKMP/IKEv1 op de buiteninterface toe:
   ```
   crypto map outside_map interface outside
   crypto ikev1 enable outside
   ```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met **show.** Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

- **Laat crypto isakmp sa** - displays alle huidige IKE Security Associations (SA's) bij een peer zien.

- **Laat crypto ipsec sa** - displays alle huidige IPsec SA's zien.

In deze paragraaf wordt een voorbeeld van verificatie voor de twee ASA's gegeven.

Centraal-ASA

```
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
```

Remote-ASA

```
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
```

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met **show.** Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

Opmerking: Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met **debug opgeeft.**

Gebruik deze opdrachten zoals wordt weergegeven:

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

> **Voorzichtig:** De **duidelijke crypto isakmp sa** opdracht is opdringerig omdat deze alle actieve VPN-tunnels reinigt.

In PIX/ASA software release 8.0(3) en hoger kan een individuele IKE SA worden gewist met behulp van de **duidelijke crypto isakmp als** *<peer ip-adres>*opdracht. In softwarereleases eerder dan 8.0(3), gebruikt u de **vpn-sessionetuning tunnelgroep** *<tunnel-group-name>*opdracht om IKE en IPsec SA's te wissen voor één tunnel.

```
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
```

Gebruikte debugs:

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

Remote-ASA (Initiator)

Typ deze opdracht **pakkettracer** om de tunnel te openen:

```
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)
```

Centraal-ASA (Responder)

```
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
```

Gerelateerde informatie

- Cisco ASA Series Series Opdrachtreferenties
- Ondersteuning van IPsec-onderhandeling/IKE-protocollen
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie - Cisco-systeem