Exemplo de configuração de ASA para ASA de IKEv1/IPsec dinâmico para estático

Contents

Introduction

Este documento descreve como permitir que o Adaptive Security Appliance (ASA) aceite conexões VPN IPsec site-to-site dinâmicas de qualquer peer dinâmico (ASA neste caso). Como mostra o Diagrama de Rede neste documento, o túnel IPsec é estabelecido quando o túnel é iniciado somente a partir da extremidade do Remote-ASA. O Central-ASA não pode iniciar um túnel VPN devido à configuração dinâmica do IPsec. O endereço IP do Remote-ASA é desconhecido.

Configure o Central-ASA para aceitar dinamicamente conexões de um endereço IP curinga (0.0.0.0/0) e de uma chave pré-compartilhada curinga. O Remote-ASA é, então, configurado para criptografar o tráfego das sub-redes local para o Central-ASA, conforme especificado pela lista de acesso de criptografia. Ambos os lados executam a isenção de NAT (Network Address Translation Conversão de Endereço de Rede) para ignorar o NAT para o tráfego IPsec.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no software Cisco ASA (5510 e 5520) Firewall versão 9.x e posterior.

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

> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

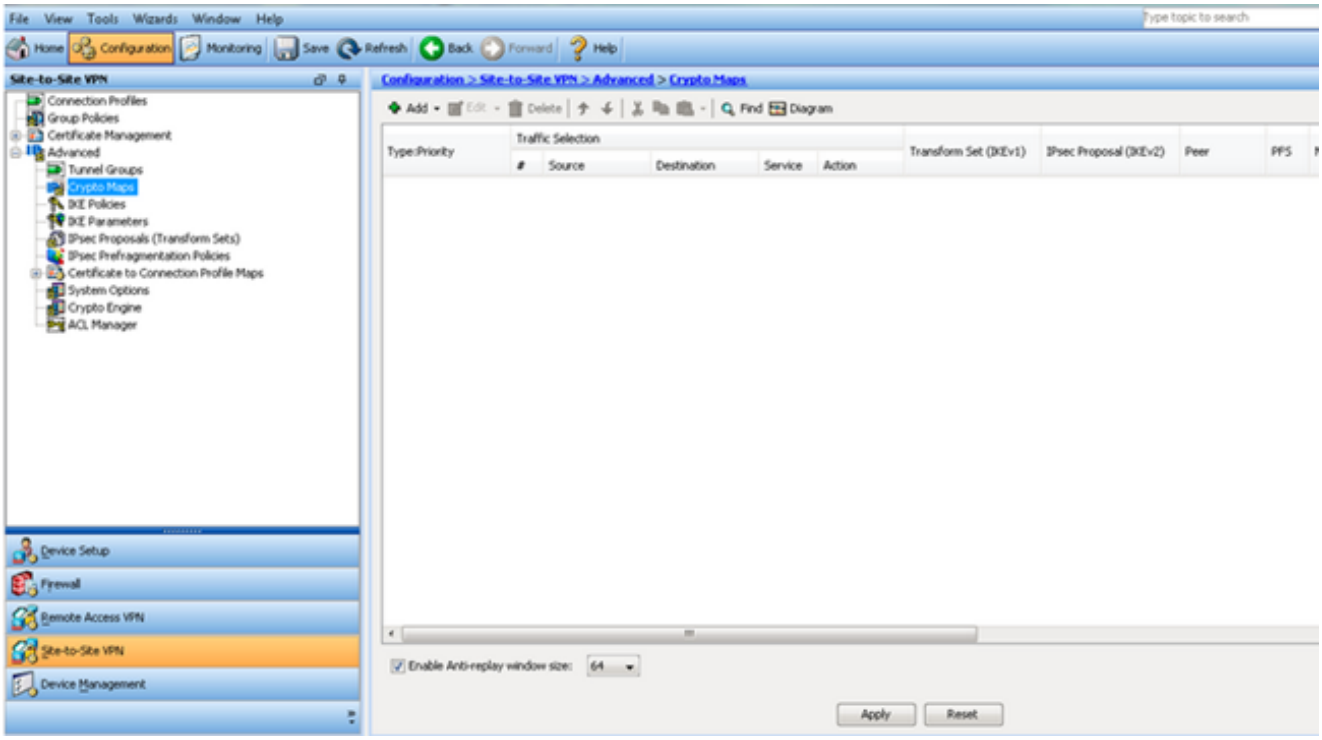
Diagrama de Rede

Configuração do ASDM

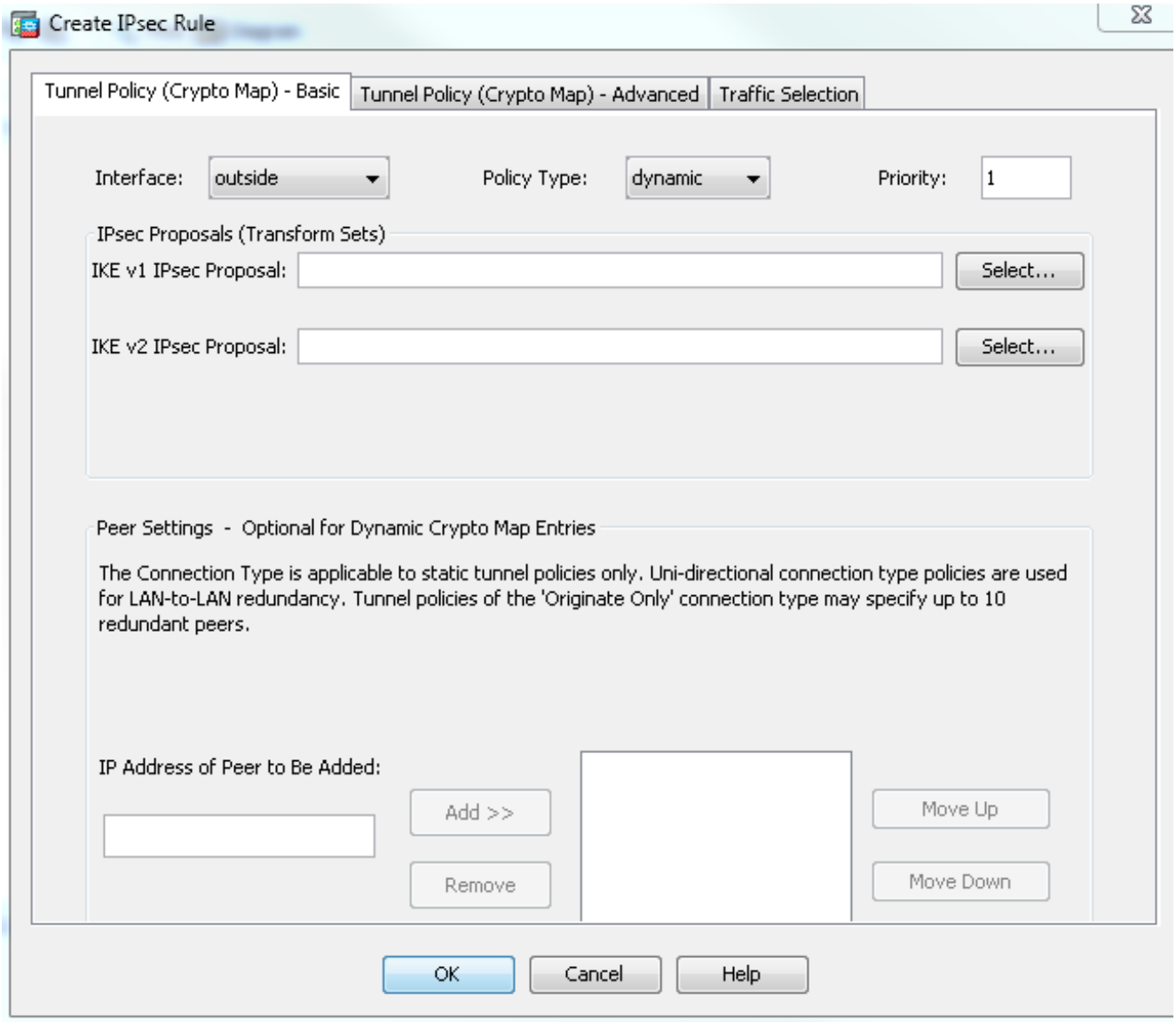
Central-ASA (Peer estático)

Em um ASA com um endereço IP estático, configure a VPN de forma que aceite conexões dinâmicas de um peer desconhecido enquanto ela autentica o peer usando uma chave pré-compartilhada IKEv1:

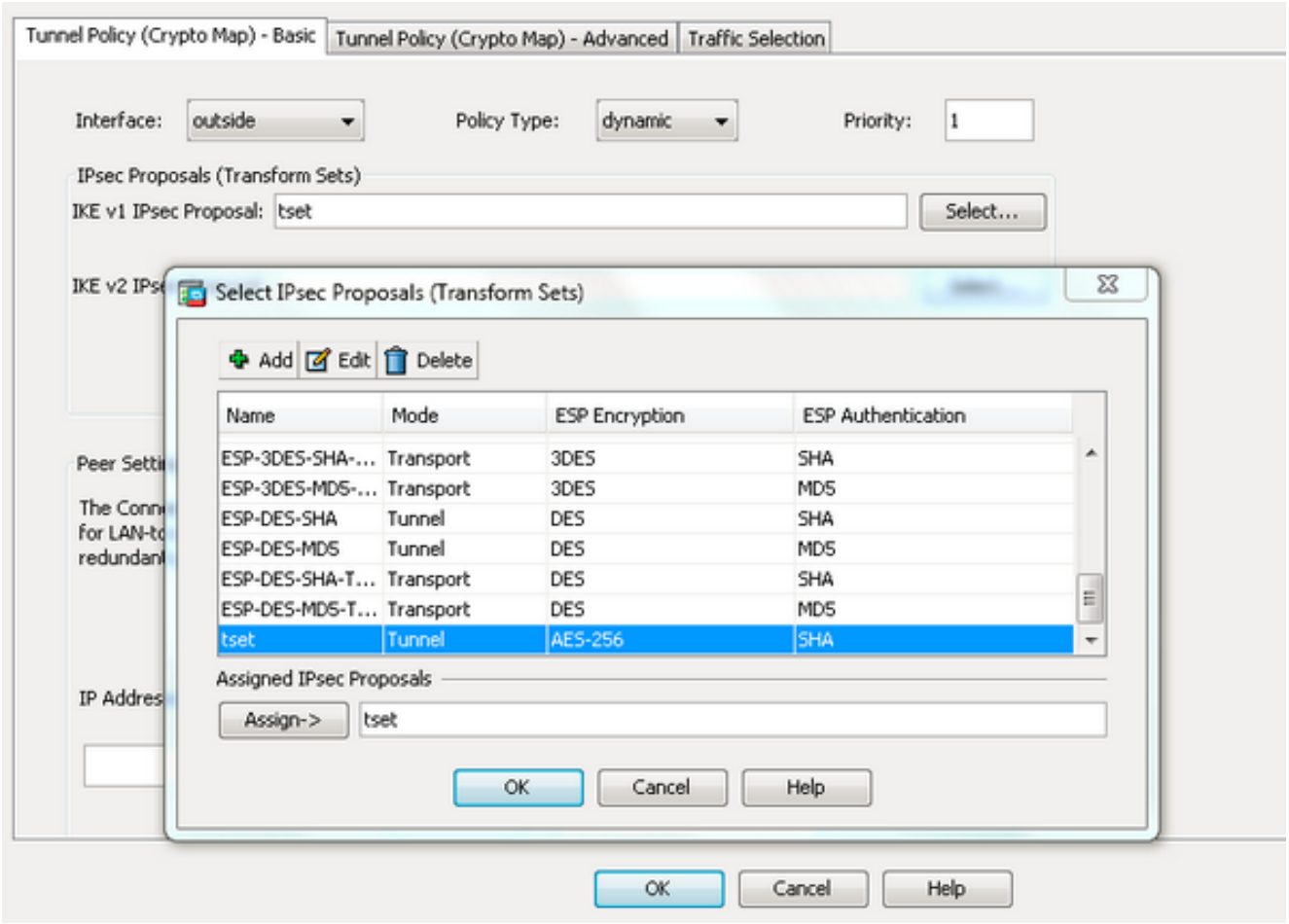
1. Escolha **Configuration > Site-to-Site VPN > Advanced > Crypto Maps.** A janela exibe a lista de entradas do mapa de criptografia que já estão em vigor (se houver). Como o ASA não sabe qual é o endereço IP do peer, para que o ASA aceite a conexão configure o **mapa dinâmico** com um conjunto de transformação correspondente (Proposta de IPsec). Clique em
Add.



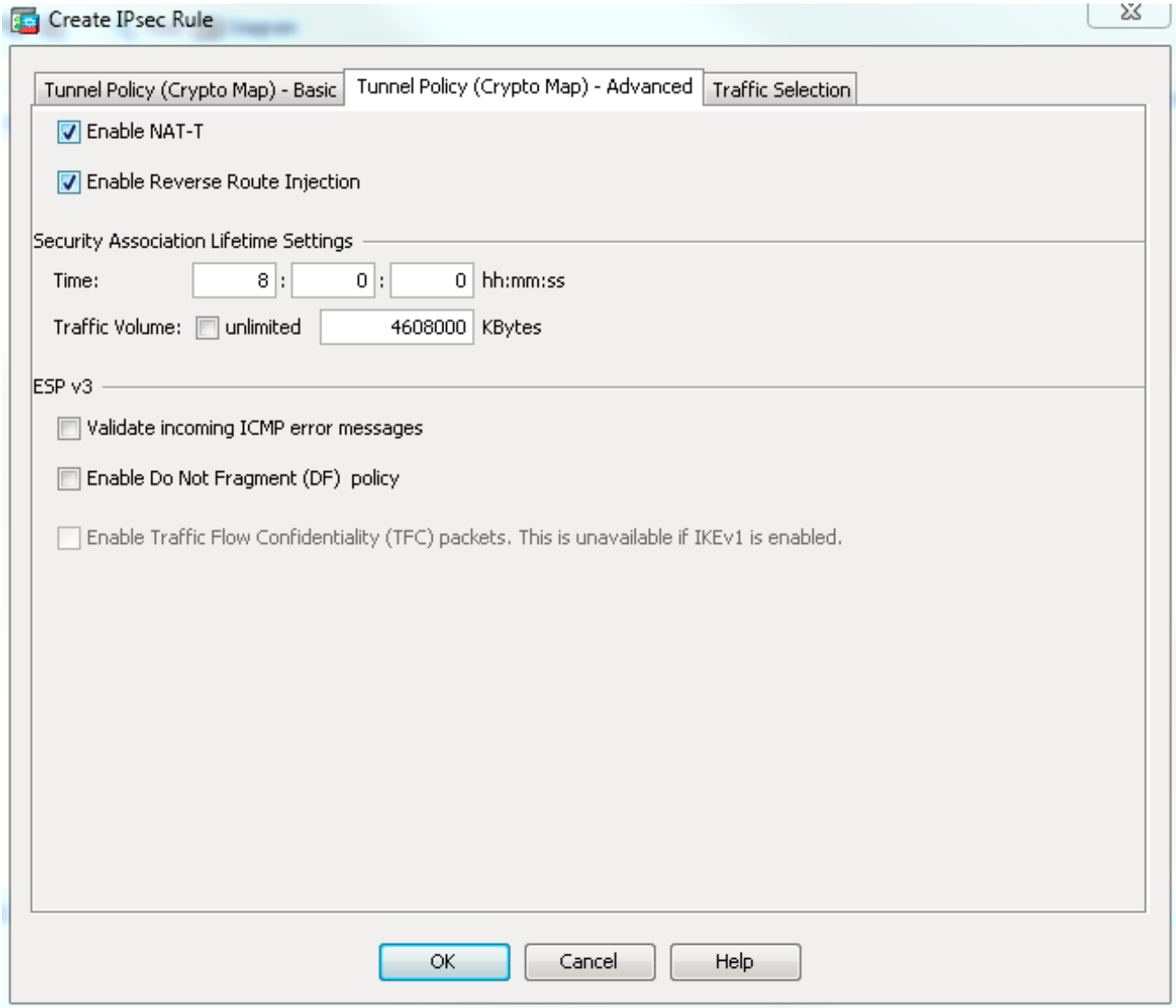
2. Na janela Create IPsec Rule, na guia Tunnel Policy (Crypto Map) - Basic, escolha **outside** na lista suspensa Interface e **dynamic** na lista suspensa Policy Type. No campo Prioridade, atribua a prioridade para essa entrada caso haja várias entradas em Mapa dinâmico. Em seguida, clique em **Selecionar** ao lado do campo Proposta IPsec IKE v1 para selecionar a proposta
IPsec.



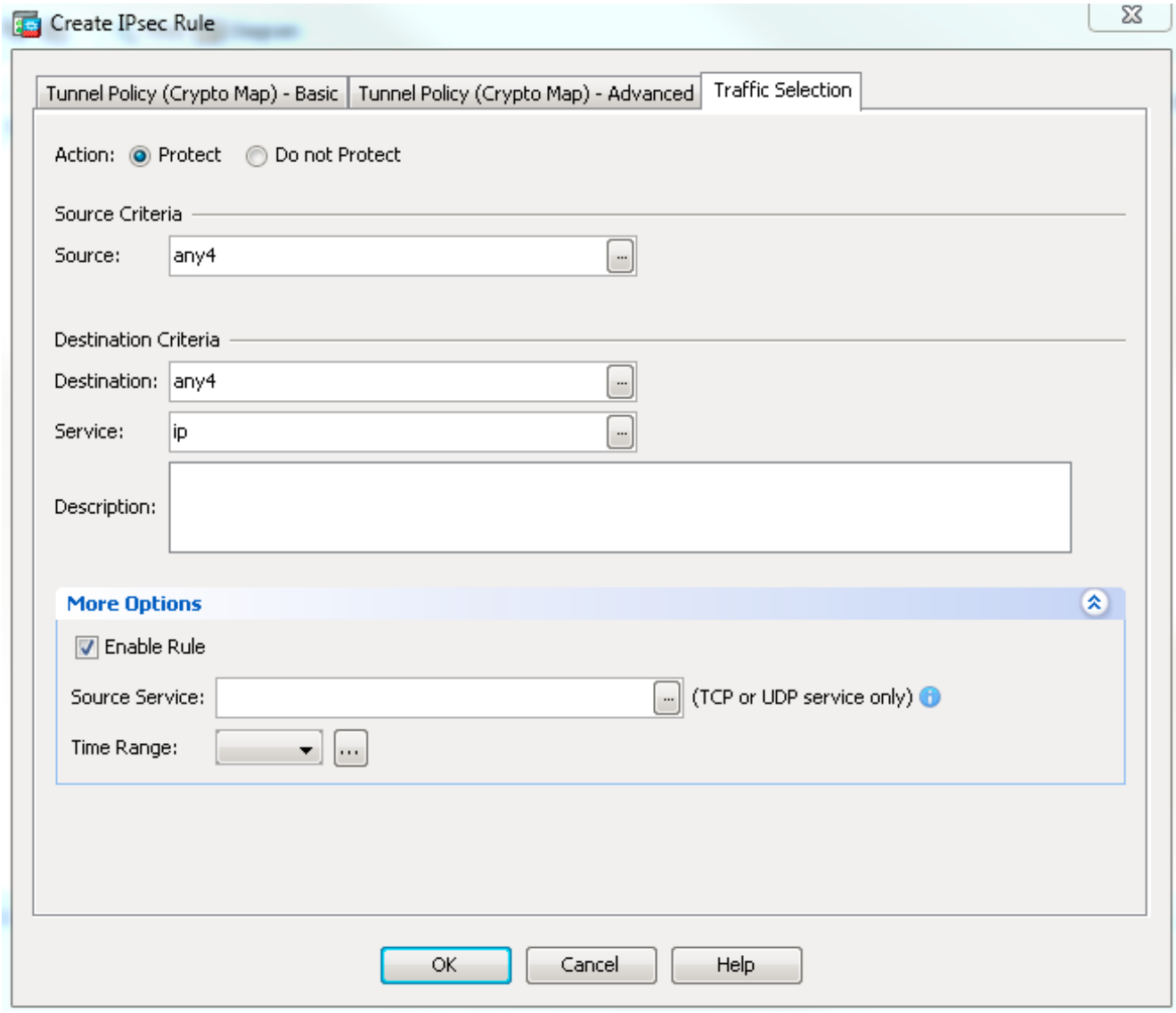
3. Quando a caixa de diálogo Selecionar propostas de IPsec (Conjuntos de transformações) for aberta, escolha entre as propostas de IPsec atuais ou clique em **Adicionar** para criar uma nova e usar a mesma. Clique em **OK** quando terminar.

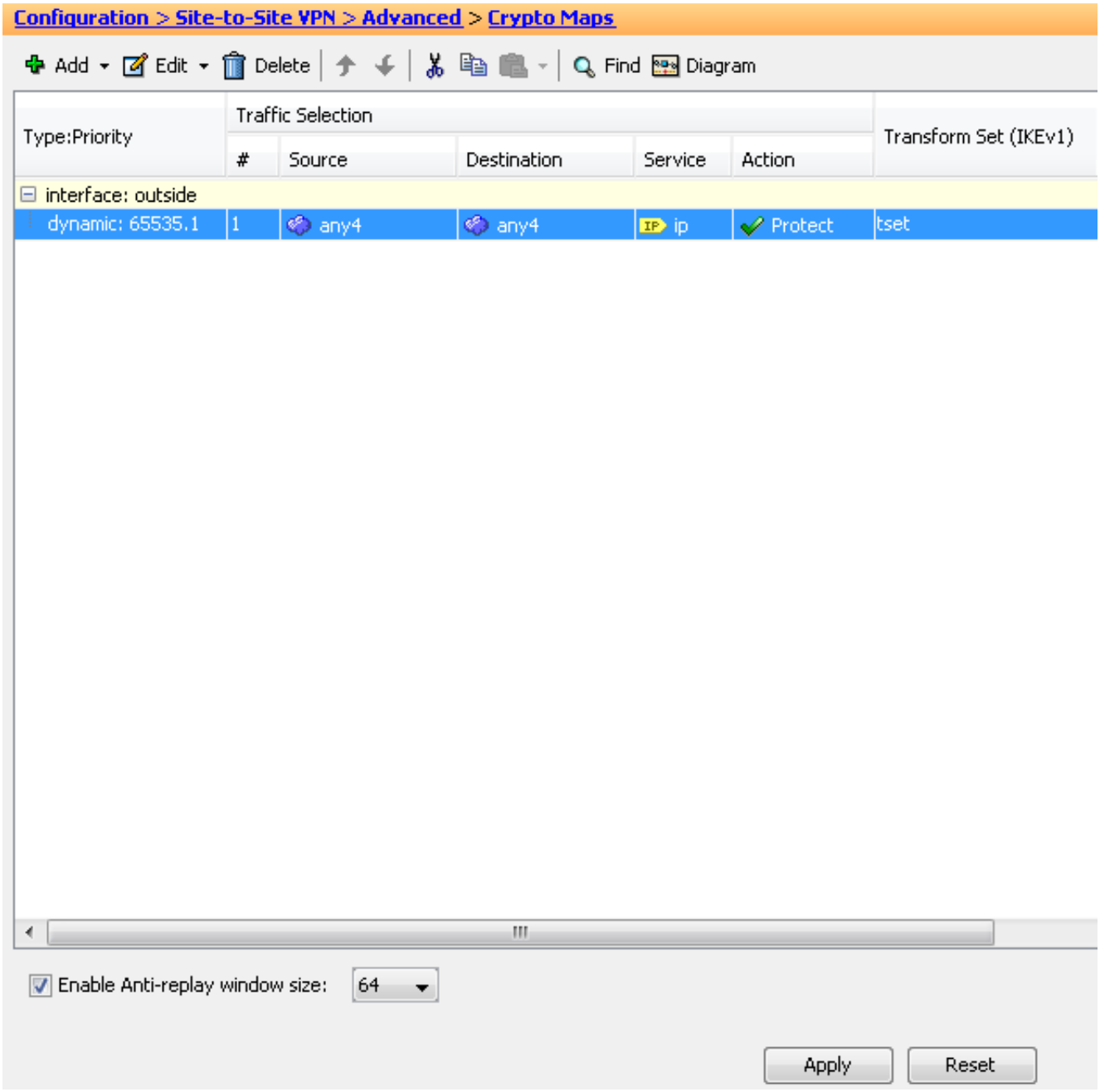


4. Na guia Tunnel Policy (Crypto Map)-Advanced (Política de túnel (Mapa de criptografia)-Advanced), marque a caixa de seleção **Enable NAT-T (Habilitar NAT-T)** (necessária se um dos pares estiver atrás de um dispositivo NAT) e a caixa de seleção **Enable Reverse Route Inject (Habilitar injeção de rota reversa)**. Quando o túnel VPN é ativado para o peer dinâmico, o ASA instala uma rota dinâmica para a rede VPN remota negociada que aponta para a interface
VPN.



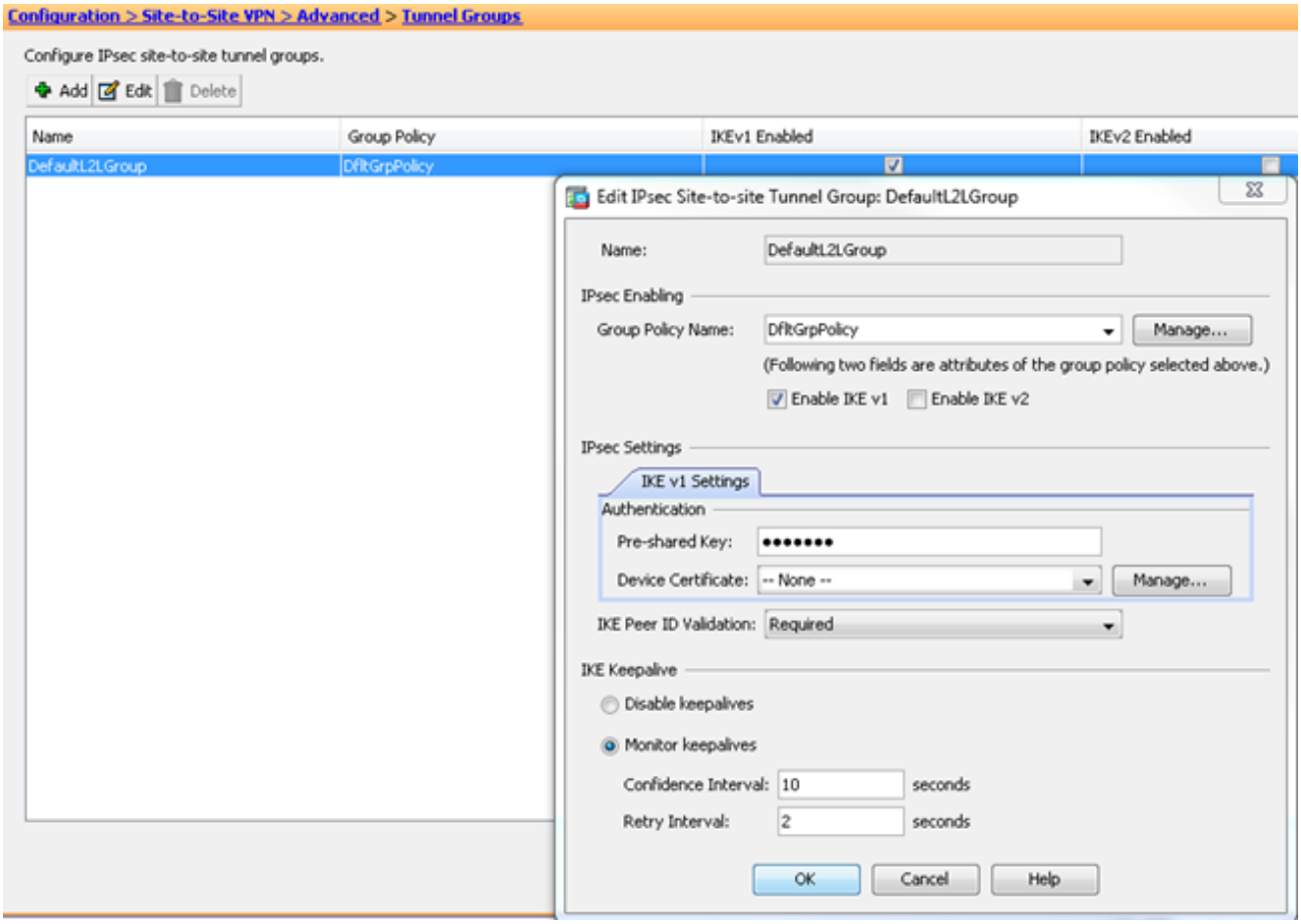
Opcionalmente, na guia Seleção de tráfego, você também pode definir o tráfego de VPN interessante para o peer dinâmico e clicar em
OK.


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:
OK
Cancel
Help



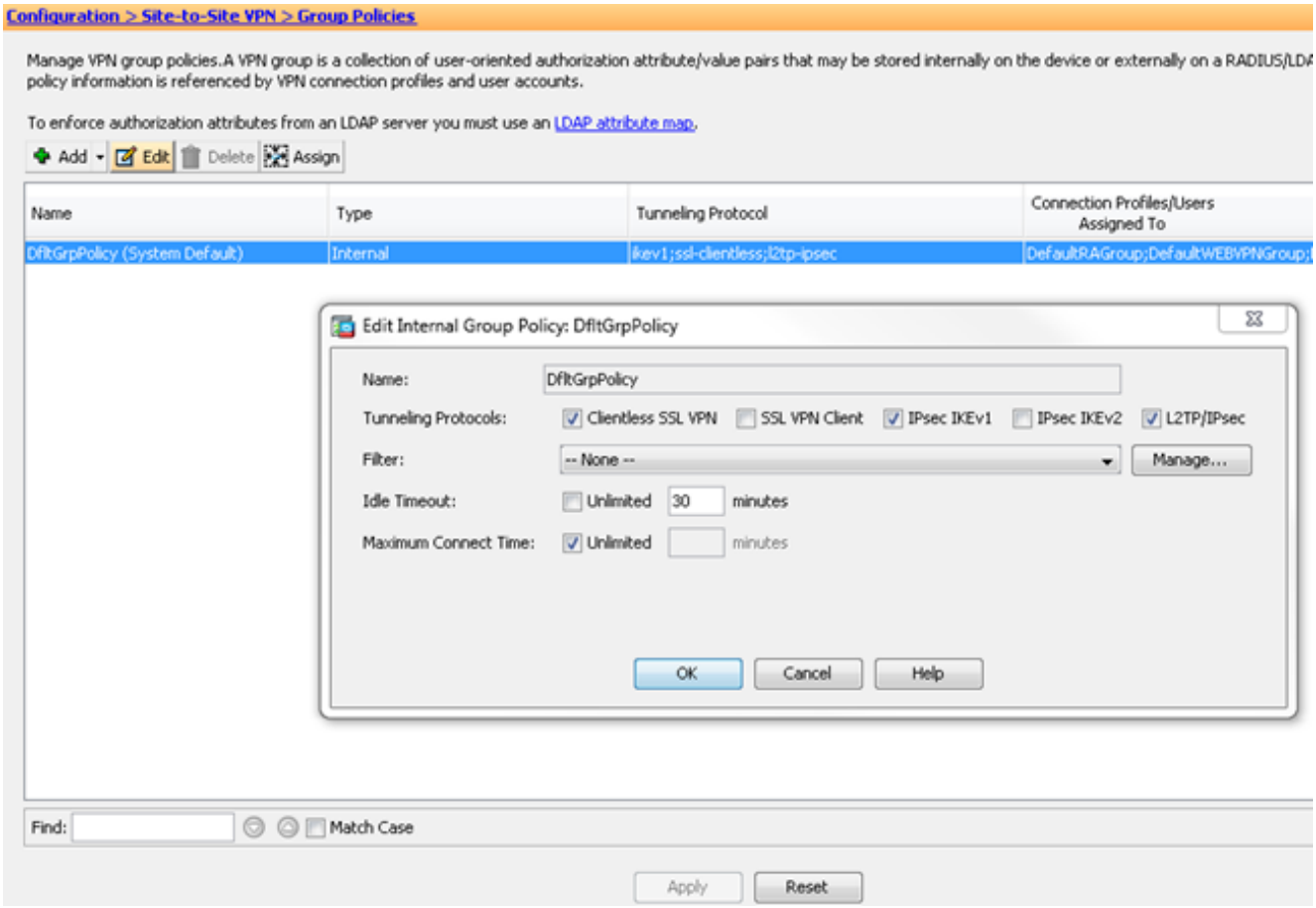
Como mencionado anteriormente, como o ASA não tem nenhuma informação sobre o endereço IP do peer dinâmico remoto, a solicitação de conexão desconhecida fica no DefaultL2LGroup que existe no ASA por padrão. Para que a autenticação seja bem-sucedida, a chave pré-compartilhada (cisco123 neste exemplo) configurada no peer remoto precisa corresponder a uma em DefaultL2LGroup.

5. Escolha **Configuration > Site-to-Site VPN > Advanced > Tunnel Groups**, selecione **DefaultL2LGgroup**, clique em **Edit** e configure a chave pré-compartilhada desejada. Clique em **OK** quando
terminar.

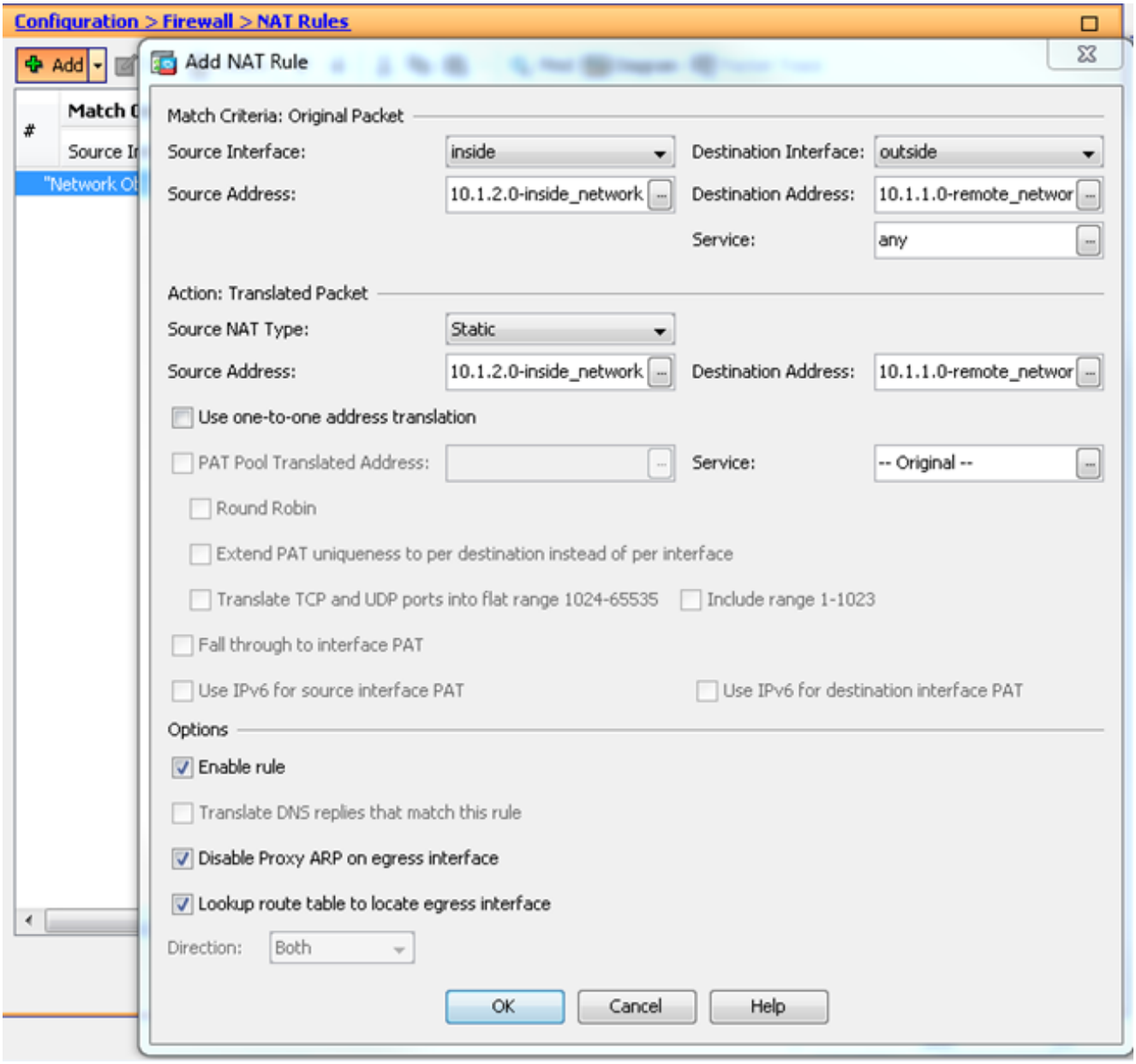


Note: Isso cria uma chave pré-compartilhada curinga no peer estático (Central-ASA). Qualquer dispositivo/peer que conheça essa chave pré-compartilhada e suas propostas correspondentes podem estabelecer com êxito um túnel VPN e acessar recursos por VPN. Certifique-se de que esta chave pré-desenhada não é partilhada com entidades desconhecidas e não é fácil de adivinhar.

6. Escolha **Configuration > Site-to-Site VPN > Group Policies** e selecione a política de grupo de sua escolha (política de grupo padrão neste caso). Clique em **Editar** e edite a política de grupo na caixa de diálogo Editar política interna de grupo. Clique em **OK** quando terminar.

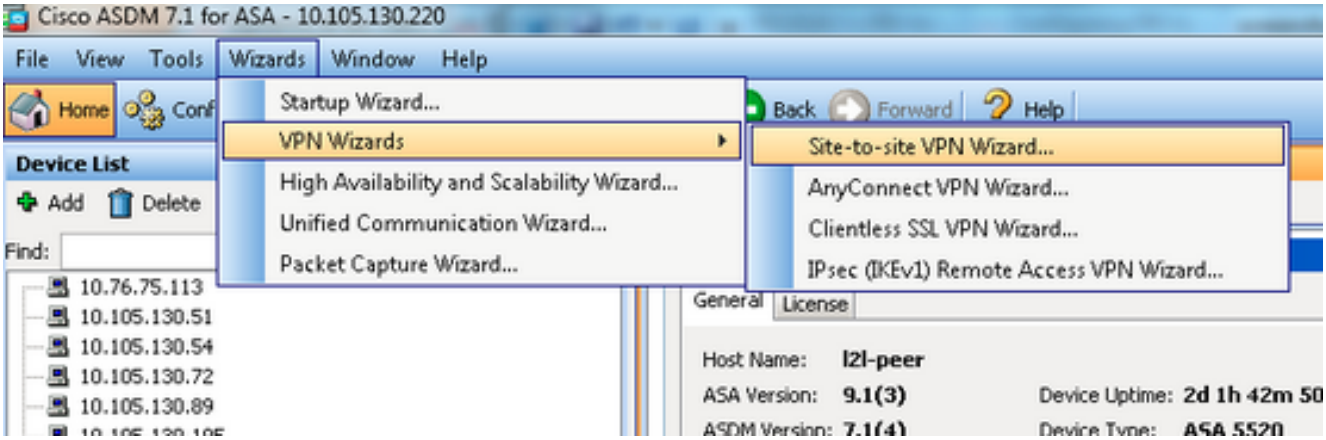


7. Escolha **Configuration > Firewall > NAT Rules** e, na janela Add Nat Rule, configure uma regra no nat (NAT-EXEMPT) para tráfego VPN. Clique em **OK** quando terminar.

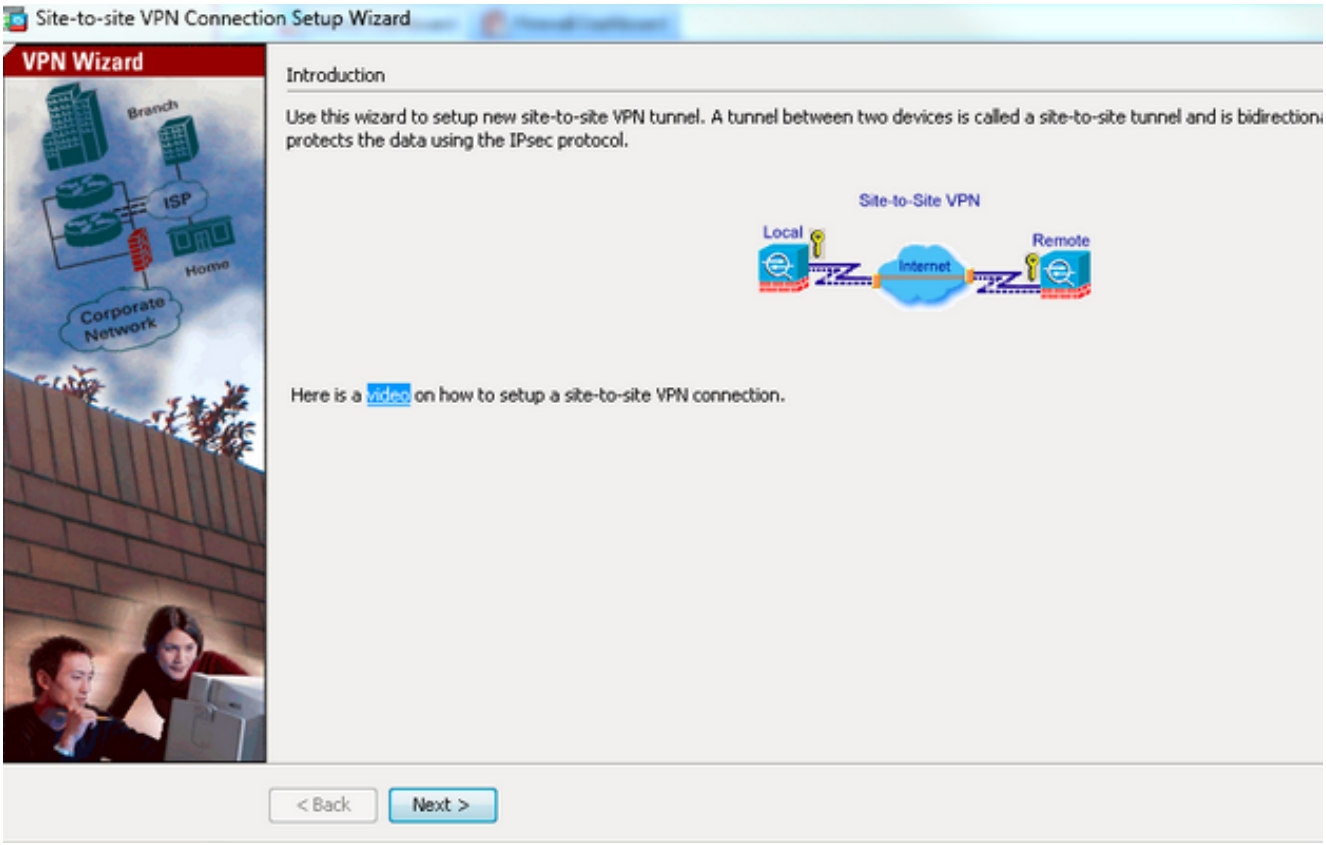


Remote-ASA (Peer dinâmico)

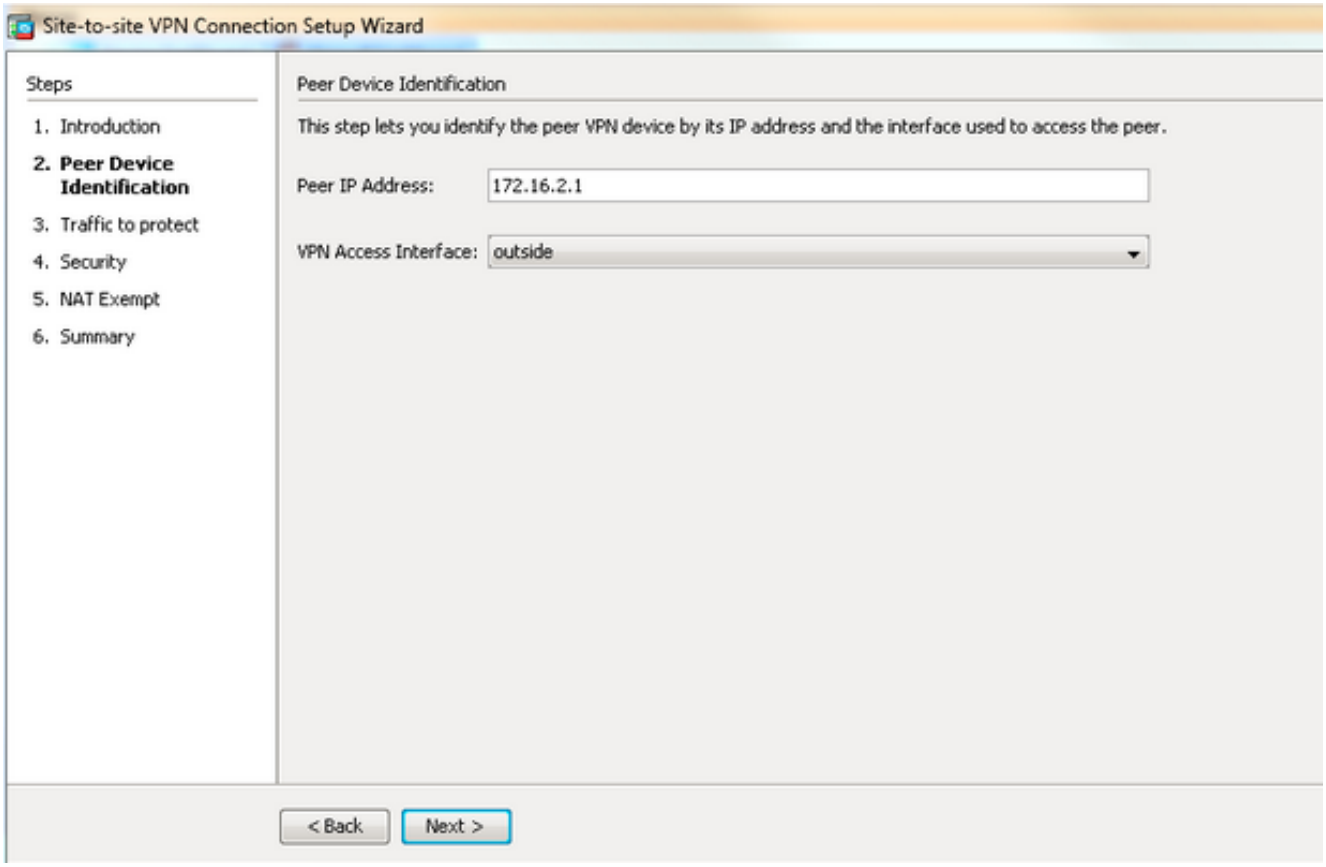
1. Escolha **Assistentes > Assistentes VPN > Assistente de VPN Site a Site** assim que o aplicativo ASDM se conectar ao ASA.



2. Clique em Next.

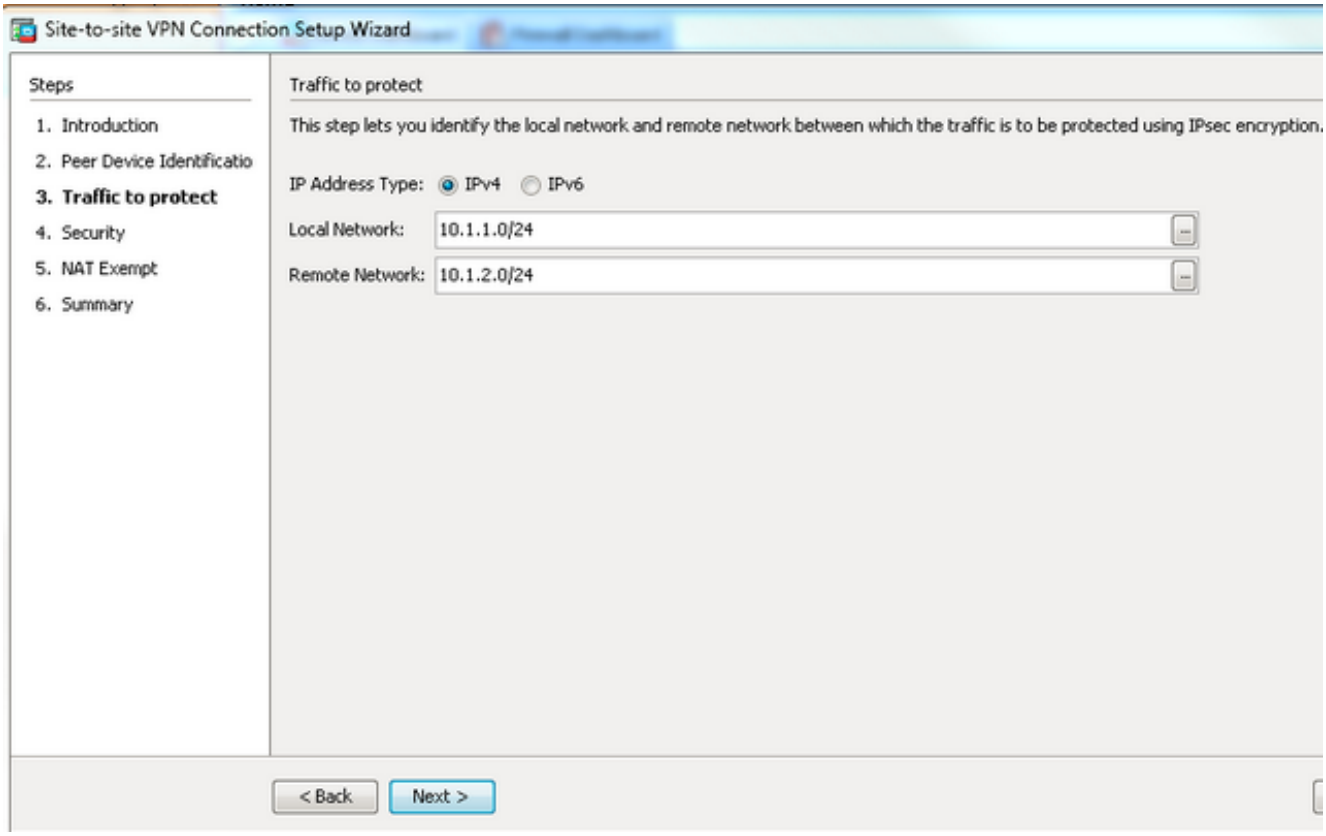


3. Escolha **fora** da lista suspensa VPN Access Interface para especificar o endereço IP externo do peer remoto. Selecione a interface (**WAN)** em que o mapa de criptografia é aplicado. Clique em
Next.

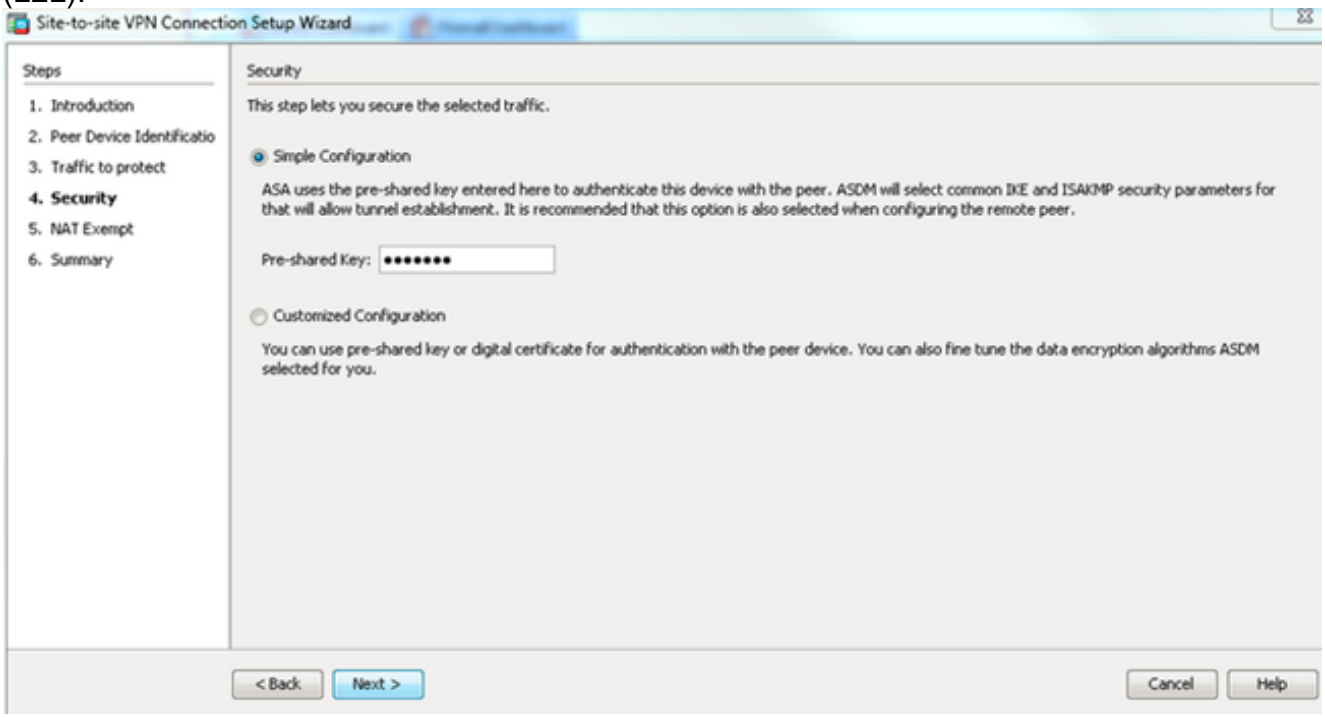


4. Especifique os hosts/redes que devem ter permissão para passar pelo túnel VPN. Nesta etapa, você precisa fornecer as redes locais e as redes remotas para o túnel VPN. Clique nos botões ao lado dos campos Rede local e Rede remota e escolha o endereço conforme o requisito. Clique em **Avançar** quando

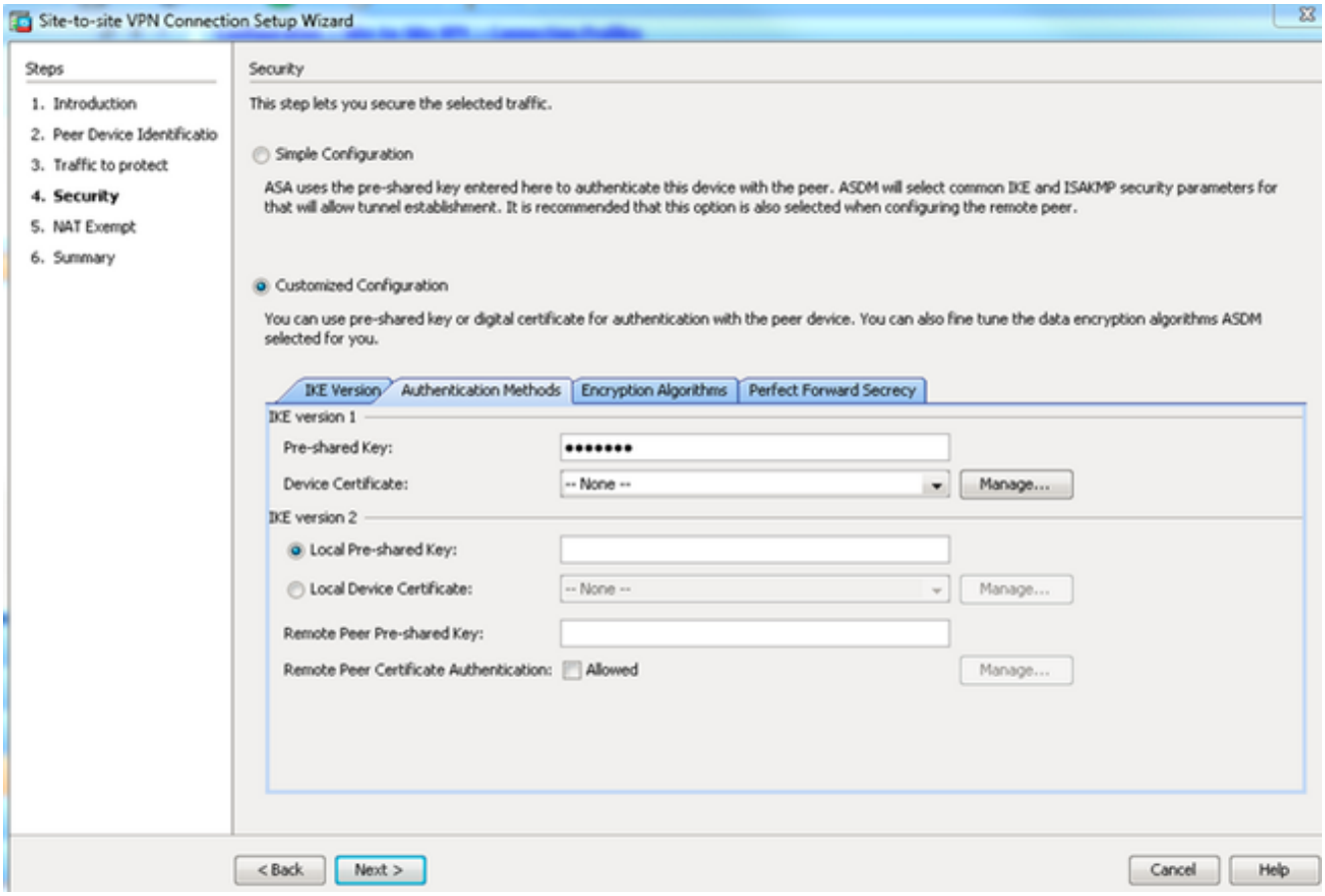
terminar.



5. Insira as informações de autenticação a serem usadas, que é a chave pré-compartilhada neste exemplo. A chave pré-compartilhada usada neste exemplo é cisco123. O nome do grupo de túnel é o endereço IP do peer remoto por padrão se você configurar a VPN LAN-to-LAN
(L2L).

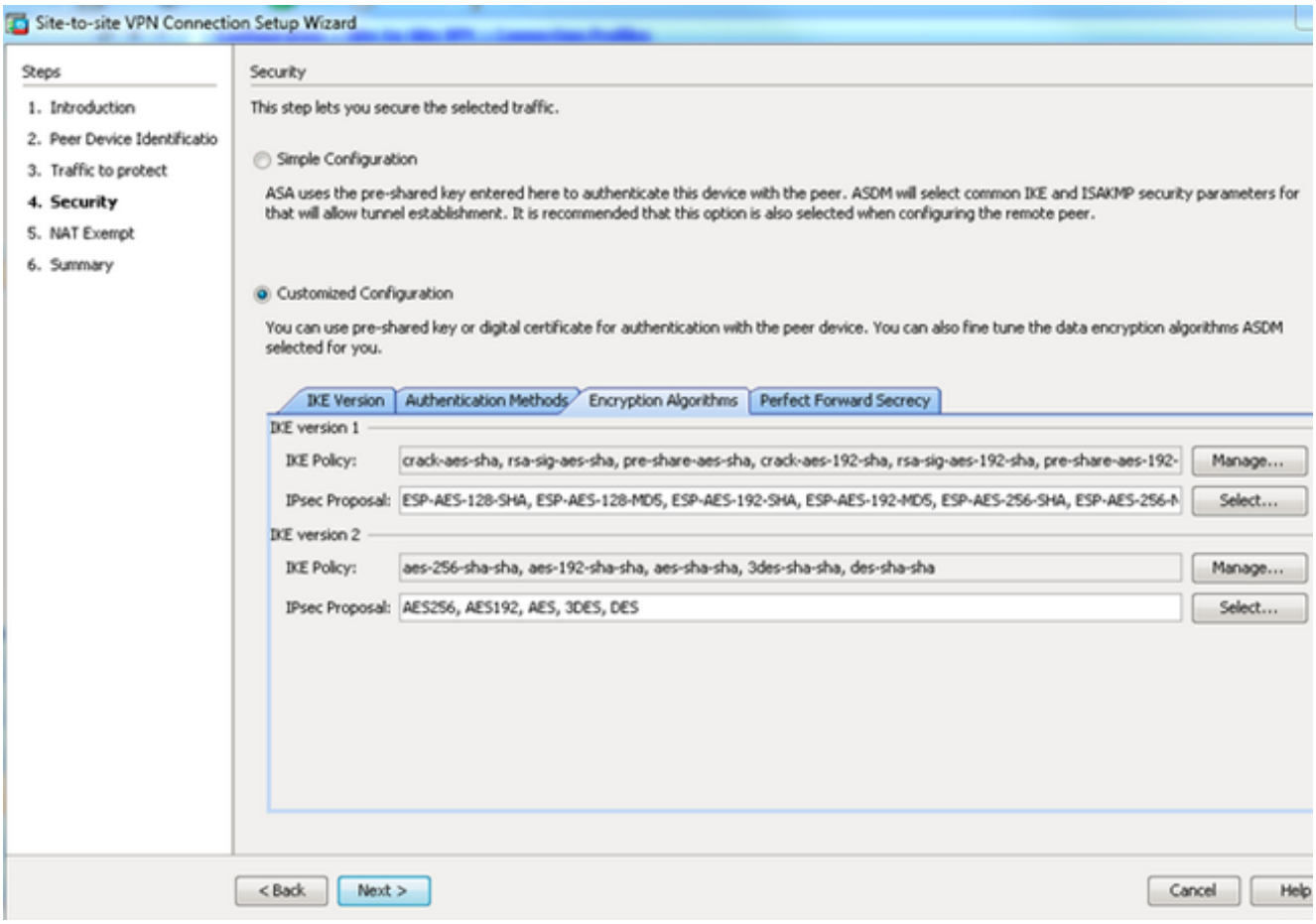


OUVocê pode personalizar a configuração para incluir a política IKE e IPsec de sua escolha. Deve haver pelo menos uma política correspondente entre os correspondentes:Na guia Métodos de autenticação, insira a chave pré-compartilhada IKE versão 1 no campo Chave pré-compartilhada. Neste exemplo, é
cisco123.



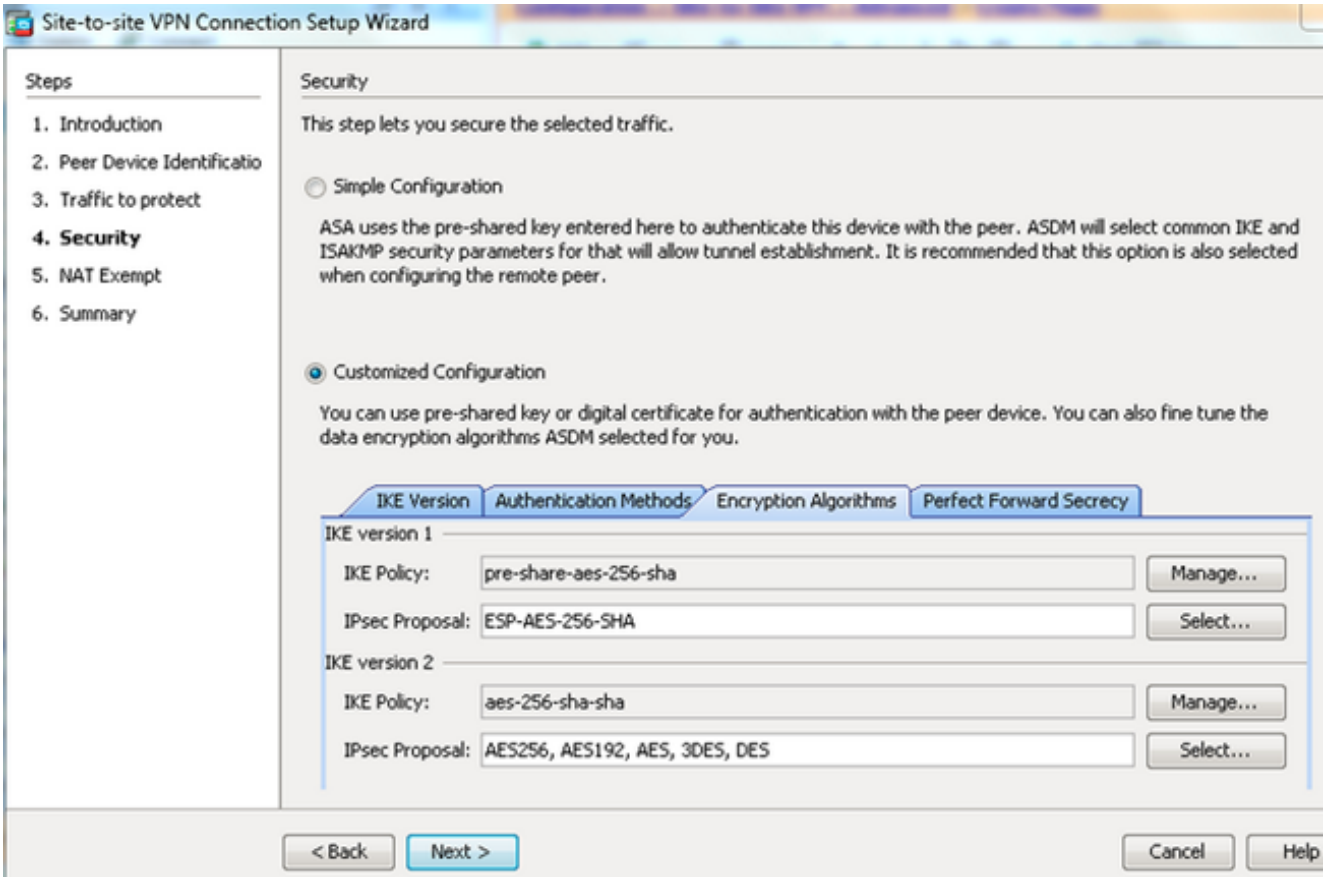
Clique na guia **Encryption Algorithms (Algoritmos de criptografia)**.

6. Clique em **Gerenciar** ao lado do campo Diretiva IKE, clique em **Adicionar** e configure uma política IKE personalizada (fase-1). Clique em **OK** quando terminar.

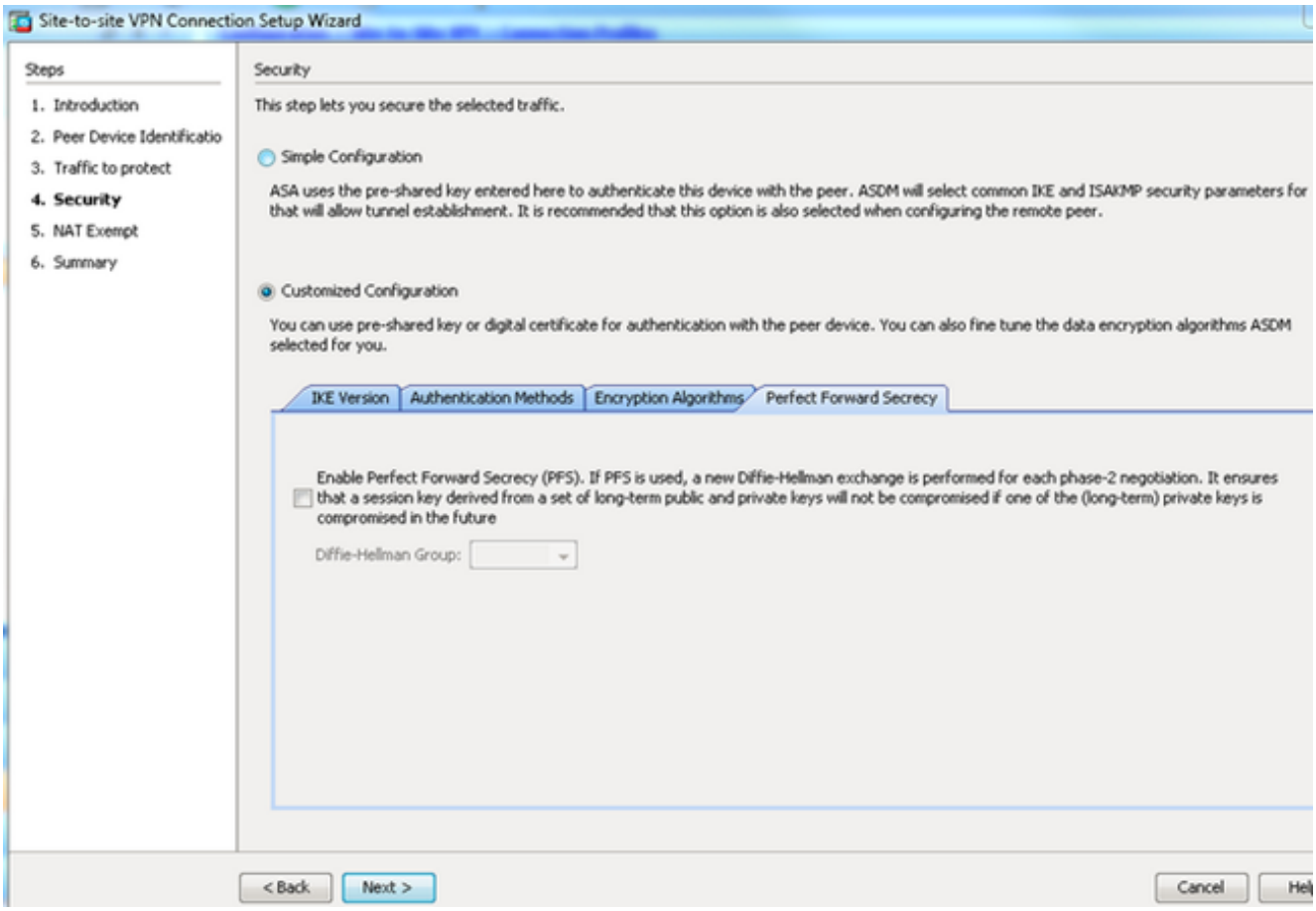


7. Clique em **Selecionar** ao lado do campo Proposta de IPsec e selecione a Proposta de IPsec

desejada. Clique em **Avançar** quando terminar.

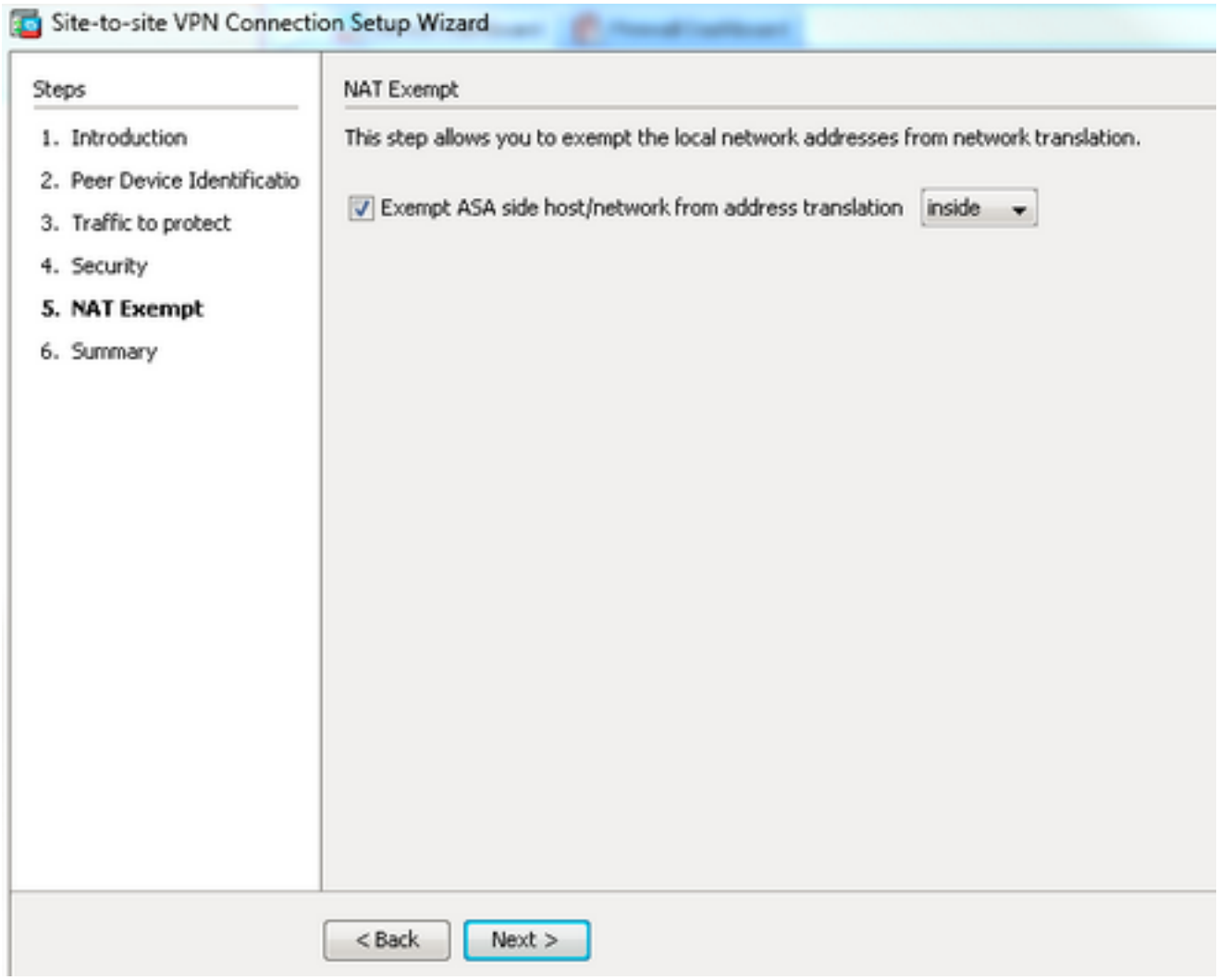


Opcionalmente, você pode ir até a guia Perfect Forward Secsecret e marcar a caixa de seleção **Enable Perfect Forward Secsecret (PFS)**. Clique em **Avançar** quando terminar.

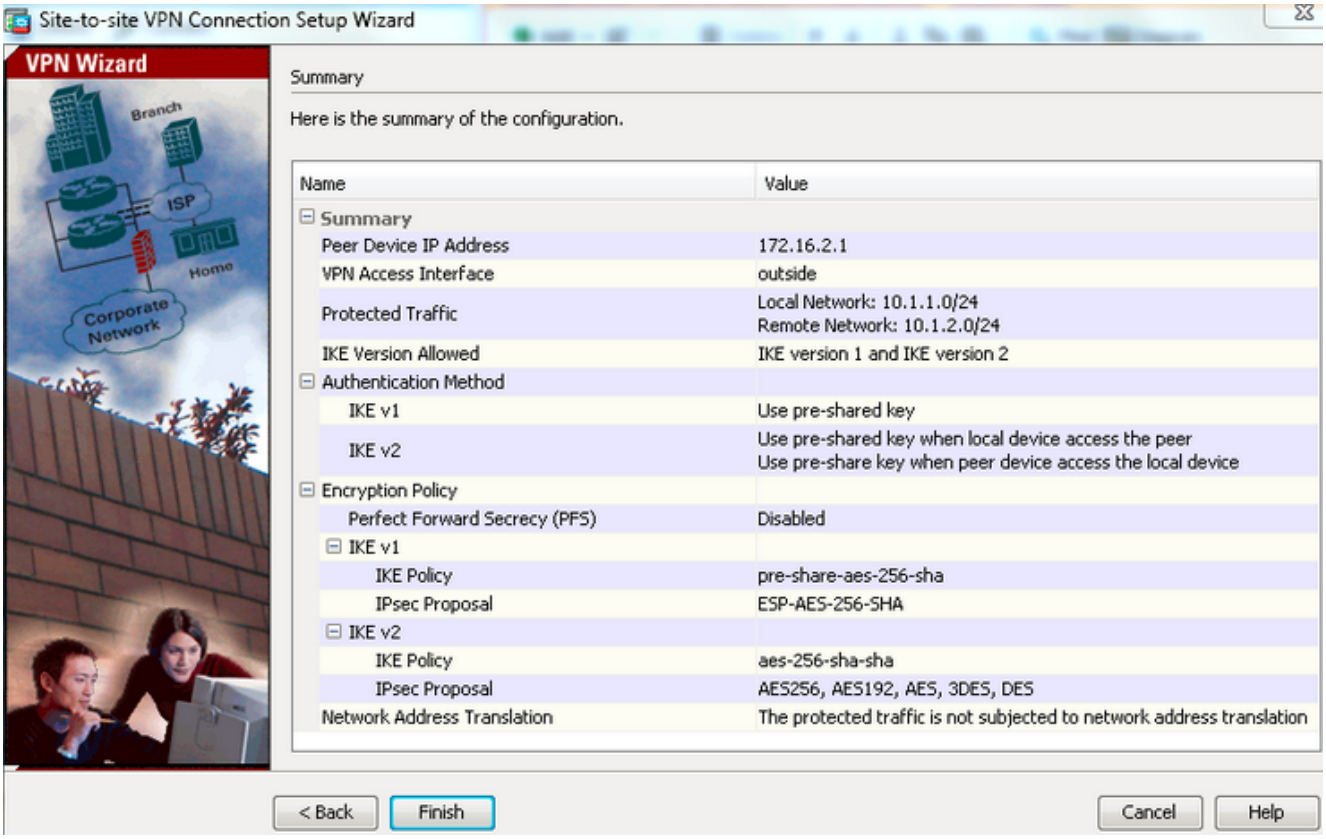


8. Marque a caixa de seleção **Isentar host/rede do lado ASA da conversão de endereço** para

impedir o tráfego do túnel do início da Conversão de endereço de rede. Escolha **local ou interno** na lista suspensa para definir a interface onde a rede local pode ser alcançada. Clique em
Next.



9. O ASDM exibe um resumo da VPN recém-configurada. Verifique e clique em **Concluir**.



Configuração de CLI

Configuração do ASA central (peer estático)

1. Configure uma regra NO-NAT/ NAT-EXEMPT para tráfego VPN como mostrado neste exemplo:

```
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 a chave pré-compartilhada em DefaultL2LGroup para autenticar qualquer peer Dynamic-L2L remoto:

```
tunnel-group DefaultL2LGroup ipsec-attributes
 ikev1 pre-shared-key cisco123
```

3. Defina a política de fase 2/ISAKMP:

```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
```

4. Defina o conjunto de transformações da fase 2/política de IPsec:

```
crypto ipsec ikev1 transform-set tset esp-aes-256 esp-sha-hmac
```

5. Configure o mapa dinâmico com estes parâmetros: Conjunto de transformação necessárioHabilitar RRP (Reverse Route Inject, injeção de rota reversa), que permite que o Security Appliance aprenda informações de roteamento 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. Vincule o mapa dinâmico ao mapa de criptografia, aplique o mapa de criptografia e ative ISAKMP/IKEv1 na interface externa:

```
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map

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

Remote-ASA (Peer dinâmico)

1. Configure uma regra de isenção de NAT para tráfego 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 um grupo de túneis para um par de VPN estático e chave pré-compartilhada.

```
tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
ikev1 pre-shared-key cisco123
```

3. Defina a política de FASE-1/ISAKMP:

```
crypto ikev1 policy 10
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
```

4. Defina um conjunto de transformação da fase 2/política de IPsec:

```
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
```

5. Configure uma lista de acesso que defina o tráfego/rede de VPN interessante:

```
access-list outside_cryptomap extended permit ip object
10.1.1.0-inside_network object 10.1.2.0-remote_network
```

6. Configure o mapa de criptografia estático com estes parâmetros: Crypto/VPN access-listEndereço IP do peer IPsec remotoConjunto de transformação necessário

```
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 o mapa de criptografia e ative ISAKMP/IKEv1 na interface externa:

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

Verificar

Use esta seção para confirmar se a configuração funciona corretamente.

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

- **show crypto isakmp sa** - Exibe todas as Associações de Segurança IKE (SAs) atuais em um peer.

- **show crypto ipsec sa** - Exibe todas as SAs IPsec atuais.

Esta seção mostra um exemplo de saída de verificação para os dois ASAs.

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

Esta seção disponibiliza informações para a solução de problemas de configuração.

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

Note: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug.**

Use estes comandos da forma mostrada:

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

> **Caution**: O comando **clear crypto isakmp sa** é invasivo, pois limpa todos os túneis VPN ativos.

No software PIX/ASA versão 8.0(3) e posterior, um SA IKE individual pode ser limpo usando o comando **clear crypto isakmp sa** *<peer ip address>*. Nas versões de software anteriores à 8.0(3), use o comando **vpn-sessiondb logoff tunnel-group** *<tunnel-group-name>* para limpar SAs de IKE e IPsec para um único 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
```

Depurações usadas:

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

Remote-ASA (iniciador)

Insira este comando **packet-tracer** para iniciar o 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)
```

Central-ASA (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
```

Informações Relacionadas

- Referências de comandos do Cisco ASA Series
- Página de Suporte de Negociação IPSec/Protocolos IKE
- Solicitações de Comentários (RFCs)
- Suporte técnico e documentação - Cisco System