

# Configurar L2TP sobre IPsec entre o Windows 8 PC e o ASA usando chave pré-compartilhada

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Restrições](#)

[Componentes Utilizados](#)

[Conventions](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração completa do túnel](#)

[Configuração do ASA usando o Adaptive Security Device Manager \(ASDM\)](#)

[Configuração do ASA usando CLI](#)

[Configuração do cliente L2TP/IPsec do Windows 8](#)

[Configuração de túnel dividido](#)

[Configuração do ASA](#)

[Configuração no cliente L2TP/IPsec](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve como configurar o L2TP (Layer 2 Tunneling Protocol) sobre IPsec usando a chave pré-compartilhada entre o Cisco Adaptive Security Appliance (ASA) e o cliente nativo do Windows 8.

A segurança L2TP sobre Internet Protocol (IPsec) oferece a capacidade de implantar e administrar uma solução de VPN (Virtual Private Network) L2TP em conjunto com os serviços de VPN IPsec e firewall em uma única plataforma.

## Prerequisites

## Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conectividade IP da máquina cliente para o ASA. Para testar a conectividade, tente fazer ping no endereço IP do ASA do endpoint do cliente e vice-versa
- Certifique-se de que a porta UDP 500 e 4500 e o protocolo ESP (Encapsulating Security

Payload) não estejam bloqueados em nenhum lugar ao longo do caminho da conexão

## Restrições

- L2TP sobre IPsec suporta apenas IKEv1. IKEv2 não é suportado.
- O L2TP com IPsec no ASA permite que o LNS interopere com clientes VPN nativos integrados em sistemas operacionais como Windows, MAC OS X, Android e Cisco IOS. Somente L2TP com IPsec é suportado, o L2TP nativo não é suportado no ASA.
- A duração mínima da associação de segurança IPsec suportada pelo cliente Windows é de 300 segundos. Se o tempo de vida do ASA for definido para menos de 300 segundos, o cliente Windows o ignorará e o substituirá por uma vida útil de 300 segundos.
- O ASA só suporta as autenticações PPP (Point-to-Point Protocol), PAP (Password Authentication Protocol Protocolo de Autenticação de Senha) e CHAP (Challenge-Handshake Authentication Protocol Protocolo de Autenticação de Handshake de Desafio) da Microsoft, versões 1 e 2, no banco de dados local. O EAP (Extensible Authentication Protocol) e o CHAP são executados por servidores de autenticação de proxy. Portanto, se um usuário remoto pertencer a um grupo de túneis configurado com os comandos **authentication eap-proxy** ou **authentication chap**, e o ASA estiver configurado para usar o banco de dados local, esse usuário não poderá se conectar.

Tipos de autenticação PPP suportados

As conexões L2TP sobre IPsec no ASA suportam somente os tipos de autenticação PPP mostrados na Tabela

### *Suporte de servidor AAA e tipos de autenticação PPP*

Tipo de servidor AAA	Tipos de autenticação PPP suportados
LOCAL	PAP, MSCHAPv1, MSCHAPv2
RADIUS	PAP, CHAP, MSCHAPv1, MSCHAPv2, EAP-Proxy
TACACS+	PAP, CHAP, MSCHAPv1
LDAP	PAP
NT	PAP
Kerberos	PAP
SDI	SDI

Características do tipo de autenticação do PPP

Palavra-chave	Tipo de autenticação	Características
chap	CHAP	Em resposta ao desafio do servidor, o cliente retorna o [desafio mais senha] criptografado com um nome de usuário em texto claro. Esse protocolo é mais seguro que o PAP, mas não criptografa dados.
eap-proxy	EAP	Habilita o EAP, que permite que o Security Appliance faça proxy do processo de autenticação PPP para um servidor de autenticação RADIUS externo.
ms-chap-v1	Microsoft CHAP, Versão 1	Semelhante ao CHAP, mas mais seguro porque o servidor armazena e compara somente senhas criptografadas em vez de senhas em texto claro como no CHAP. Esse protocolo também gera uma chave para a criptografia de dados pelo MPPE.
ms-chap-v2	Microsoft CHAP, Versão, 2	
pap	PAP	Passa o nome de usuário e a senha em texto claro durante a autenticação e não é seguro.

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 5515 Series ASA que executa a versão de software 9.4(1)
- Cliente L2TP/IPSec (Windows 8)

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Produtos Relacionados

Essa configuração também pode ser usada com o Cisco ASA 5500 Series Security Appliance 8.3(1) ou posterior.

## Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos

## Informações de Apoio

O L2TP (Layer 2 Tunneling Protocol) é um protocolo de tunelamento de VPN que permite que os clientes remotos usem a rede IP pública para se comunicarem com segurança com servidores de rede corporativa privados. O L2TP usa PPP sobre UDP (porta 1701) para fazer o túnel dos dados.

O protocolo L2TP é baseado no modelo cliente/servidor. A função é dividida entre o Servidor de Rede L2TP (LNS) e o Concentrador de Acesso L2TP (LAC). O LNS normalmente é executado em um gateway de rede, como o ASA, nesse caso, enquanto o LAC pode ser um NAS (Network Access Server, servidor de acesso à rede) de discagem ou um dispositivo de endpoint com um cliente L2TP em pacote, como Microsoft Windows, Apple iPhone ou Android.

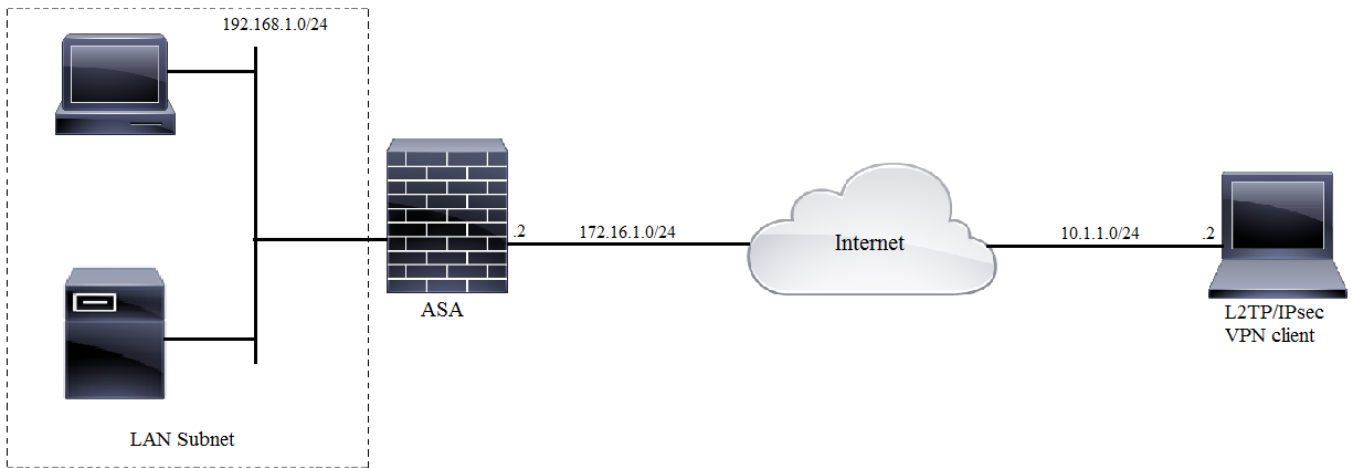
## Configurar

Esta seção apresenta as informações para configurar os recursos descritos neste documento.

**Note:** Use a ferramenta [Command Lookup Tool \(apenas para clientes registrados\) para obter mais informações sobre os comandos usados neste documento.](#)

**Note:** Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São endereços RFC 1918 que foram usados em um ambiente de laboratório.

## Diagrama de Rede

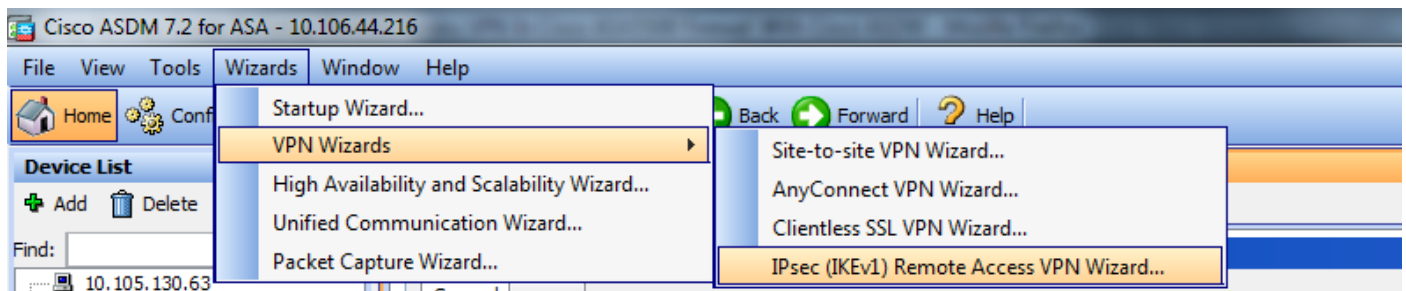


## Configuração completa do túnel

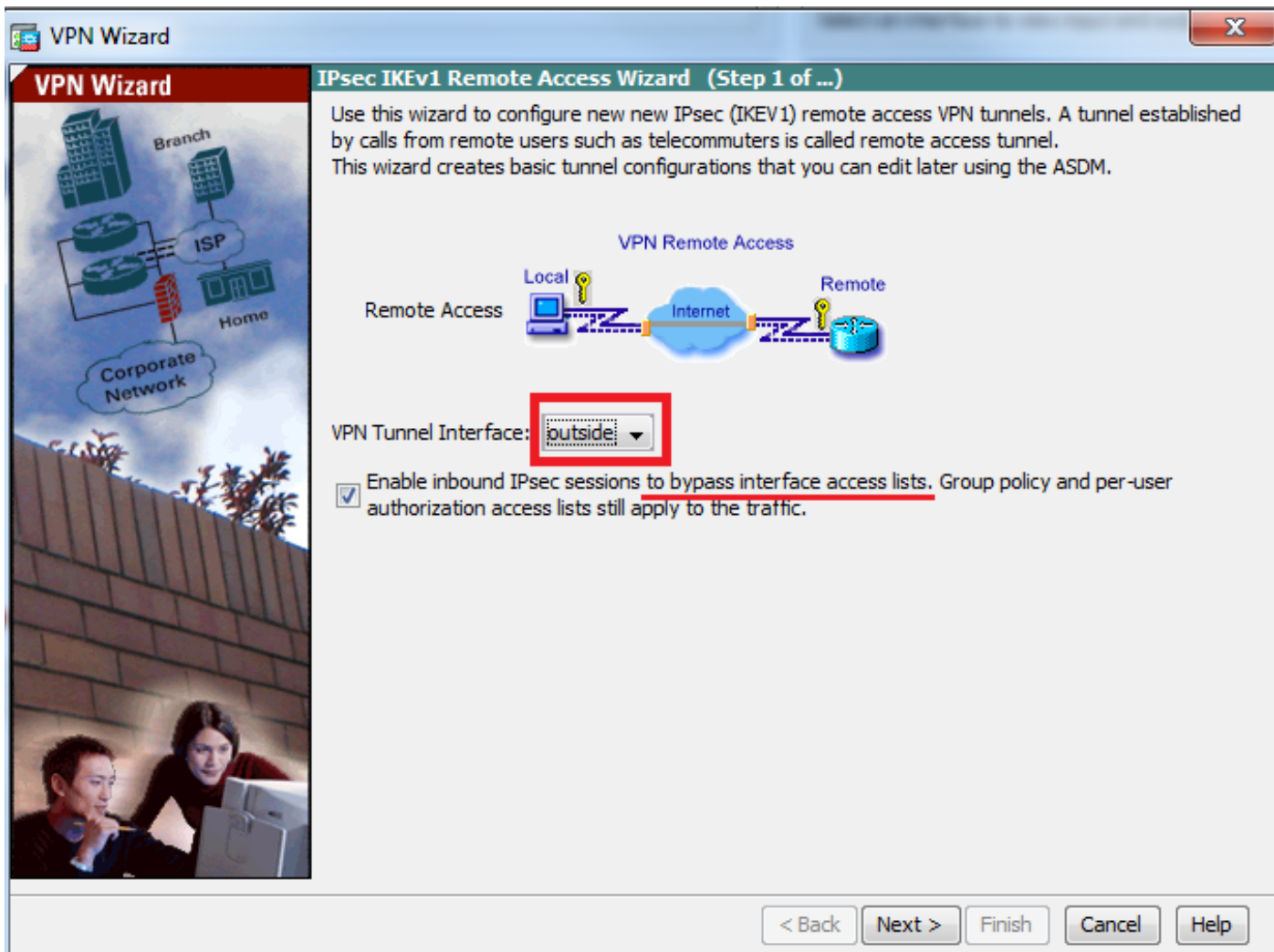
### Configuração do ASA usando o Adaptive Security Device Manager (ASDM)

Conclua estes passos:

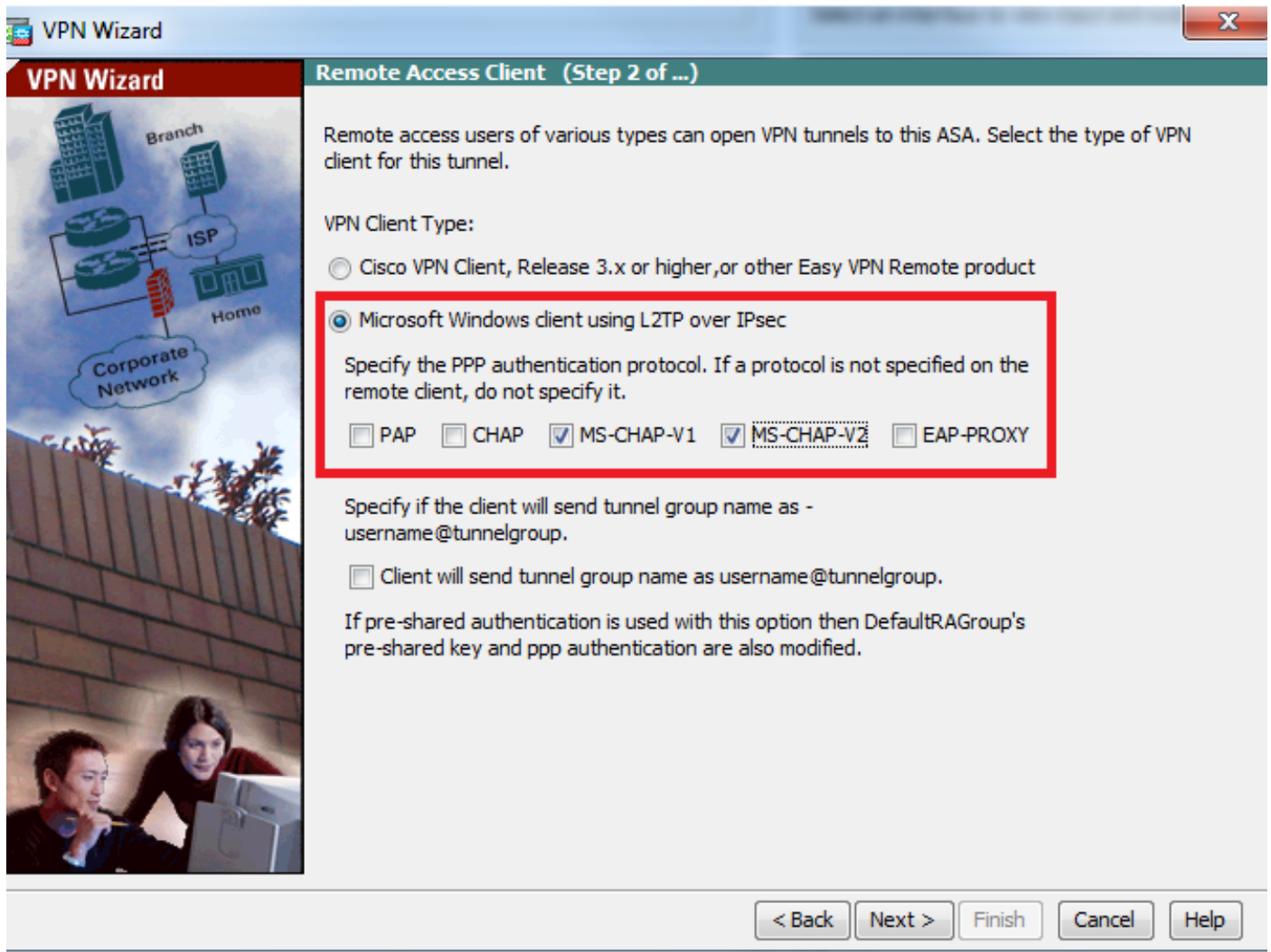
Etapa 1. Faça login no ASDM e navegue até **Assistentes > Assistentes VPN > Assistente de VPN de acesso remoto IKEv1 (Ipsec)**.



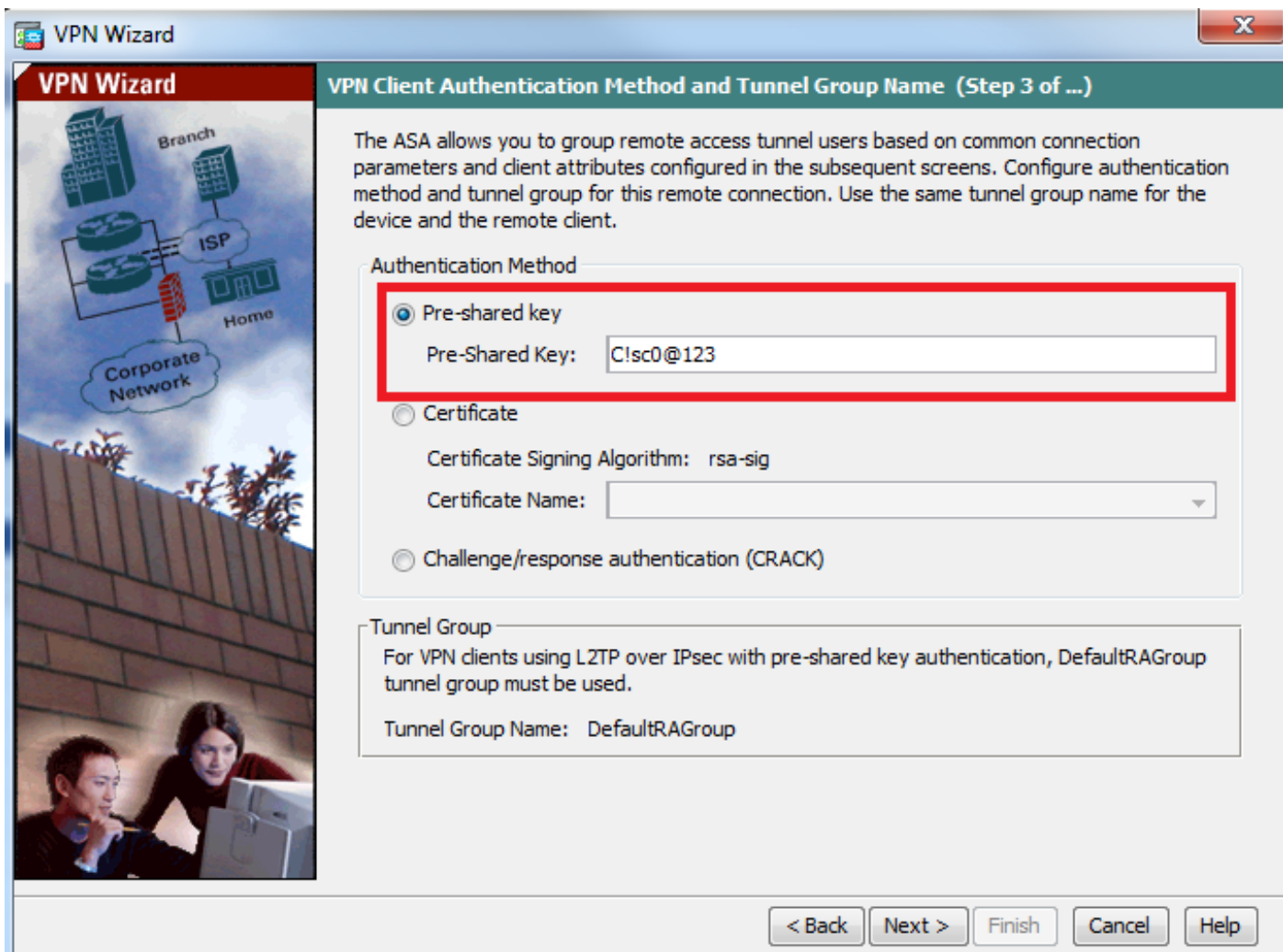
Etapa 2. Uma janela de configuração da VPN de acesso remoto é exibida. Na lista suspensa, escolha a interface na qual o túnel VPN deve ser terminado. Neste exemplo, a interface externa está conectada à WAN e, portanto, terminando túneis VPN nesta interface. Mantenha a caixa **Habilitar sessões IPsec de entrada para ignorar listas de acesso de interface**. A política de grupo e as listas de acesso de autorização por usuário ainda se aplicam ao tráfego verificado, de modo que a nova lista de acesso não precisa ser configurada na interface externa para permitir que os clientes acessem recursos internos. Clique em Next.



Etapa 3. Como mostrado nesta imagem, escolha o tipo de cliente como **cliente Microsoft Windows usando L2TP sobre IPsec e MS-CHAP-V1 e MS-CHAP-V2** como protocolo de autenticação PPP, pois PAP não é seguro e outros tipos de autenticação não são suportados com o banco de dados LOCAL como servidor de autenticação e clique em **Avançar**.

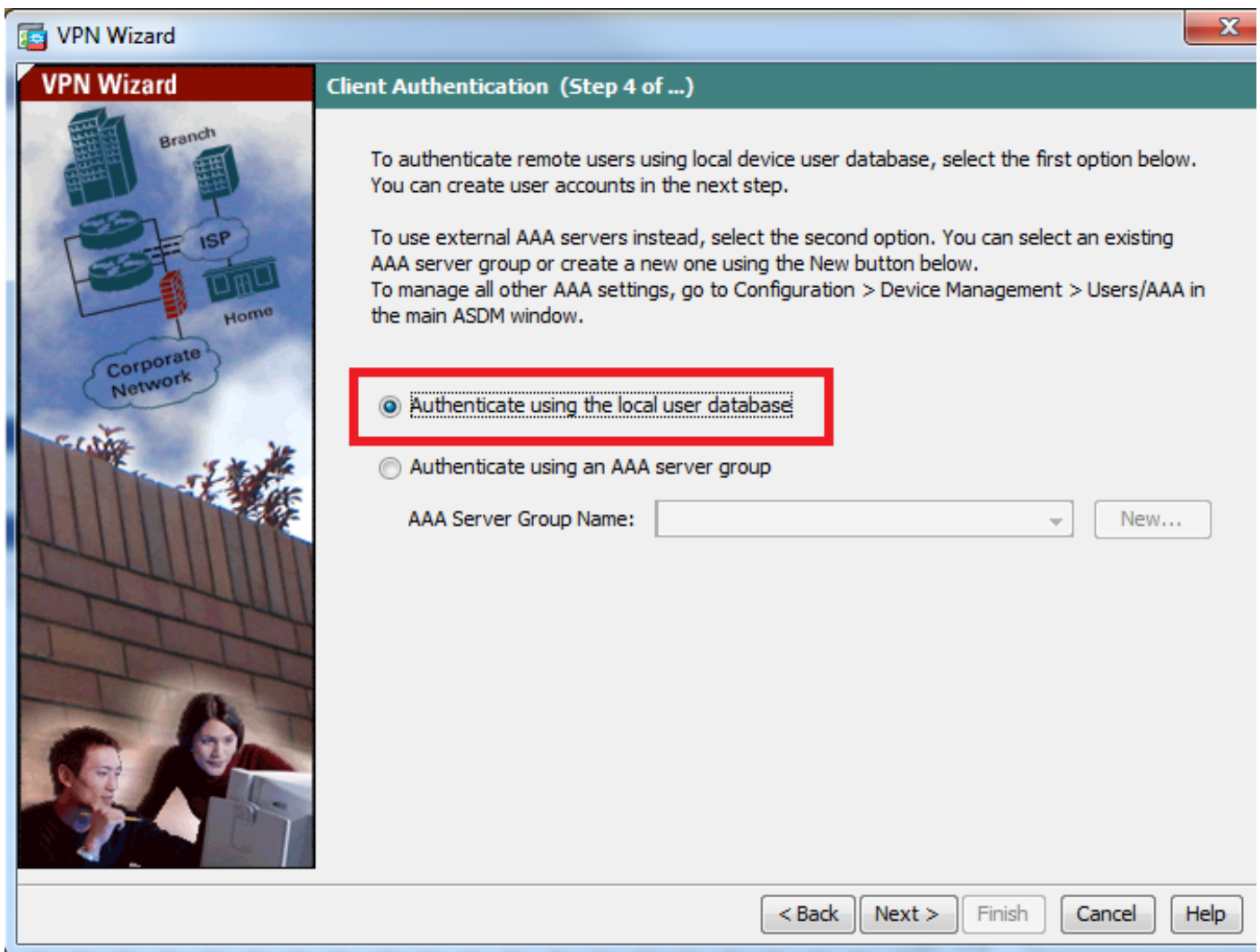


Etapa 4. Escolha o método de autenticação como **Pre-shared-key** e digite a chave pré-compartilhada que deve ser a mesma no lado do cliente e clique em **Next**, como mostrado nesta imagem.



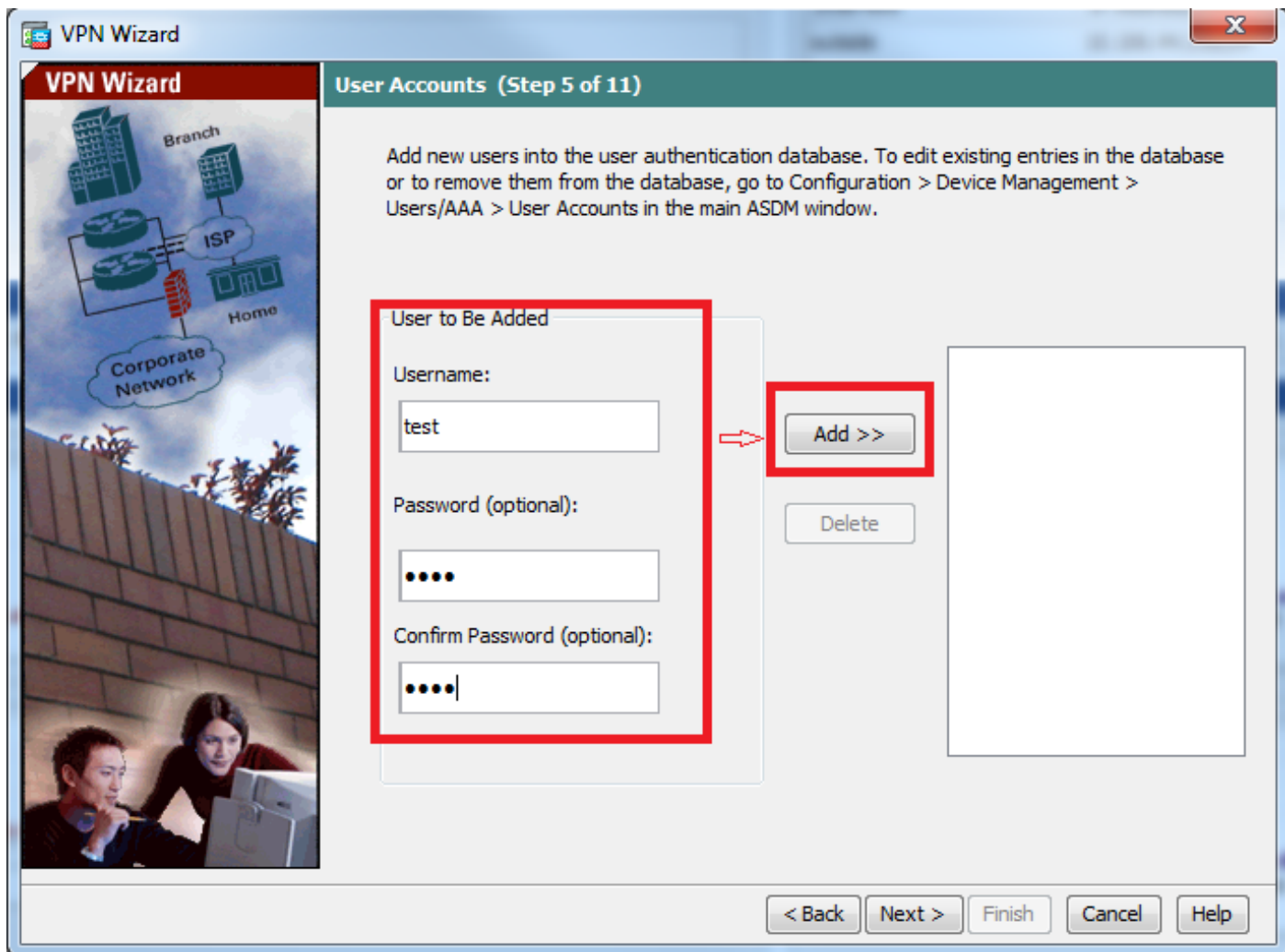
Etapa 5. Especifique um método para autenticar usuários que tentam conexões L2TP sobre IPsec. Um servidor de autenticação AAA externo ou seu próprio banco de dados local podem ser usados. Escolha **Autenticar usando o banco de dados de usuário local** se quiser autenticar os clientes em relação ao banco de dados local do ASA e clique em **Avançar**.

**Note:** Consulte [Configurar a autenticação RADIUS para usuários de VPN](#) para autenticar os usuários usando o servidor AAA externo.

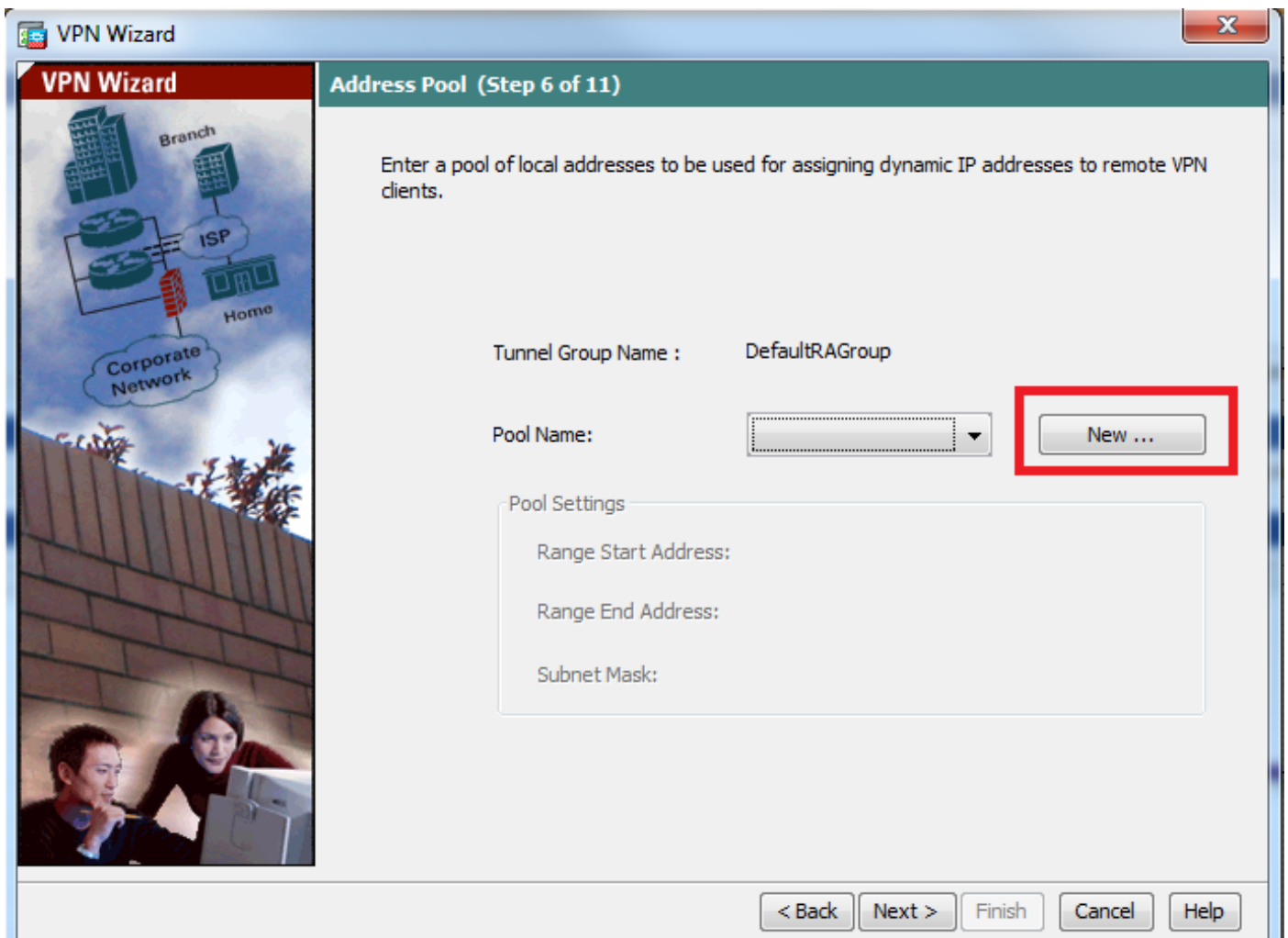


Etapa 6. Para adicionar novos usuários ao banco de dados local para autenticação de usuário, insira o nome de usuário e a senha e clique em **ADD** ou então as contas de usuário existentes no banco de dados podem ser usadas, como mostrado nesta imagem. Clique em Next.



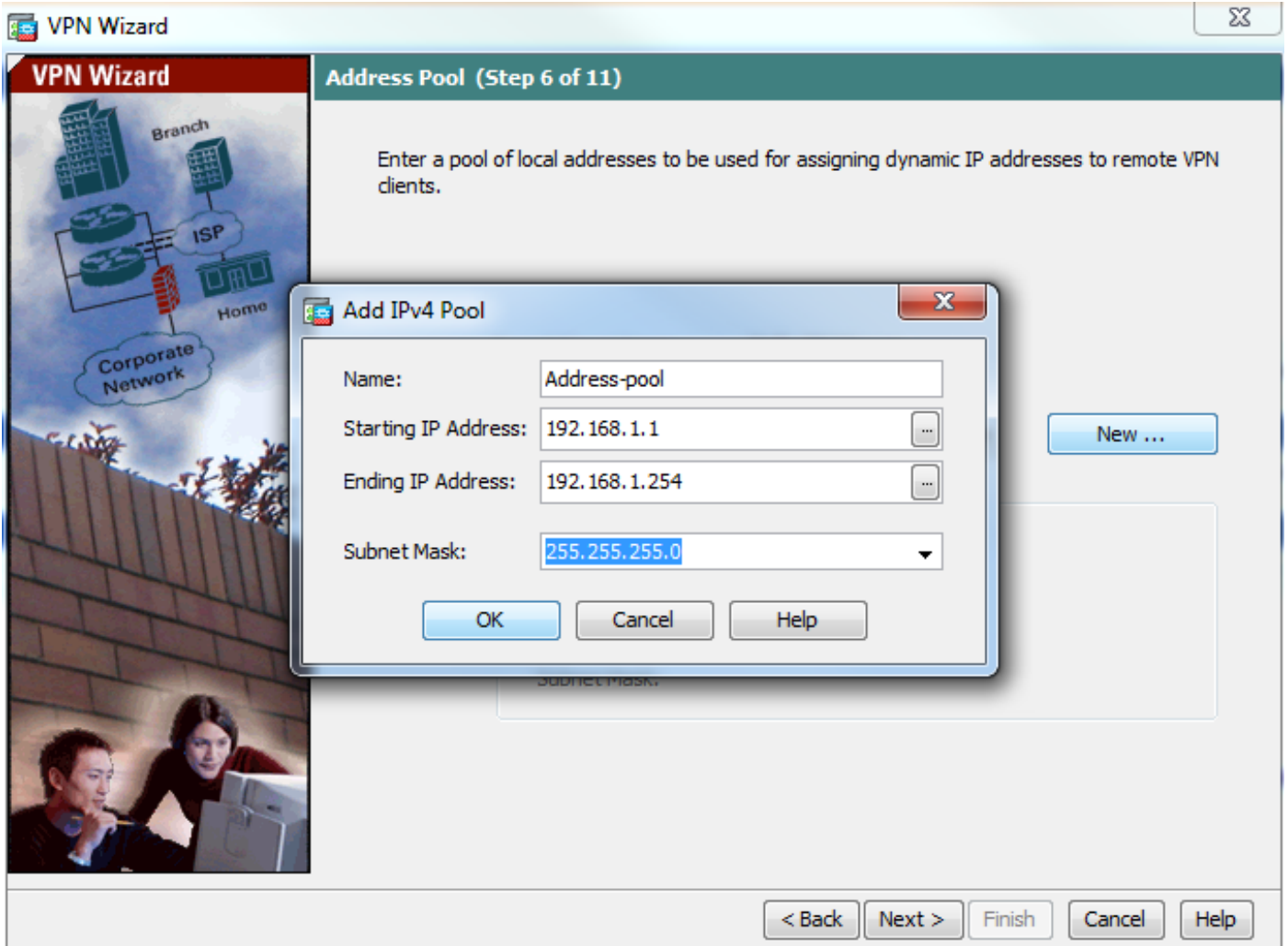


Passo 7. Na lista suspensa, escolha o pool de endereços a ser usado para atribuir endereços IP aos clientes. Para criar um novo pool de endereços, clique em **Novo**, como mostrado nesta imagem.

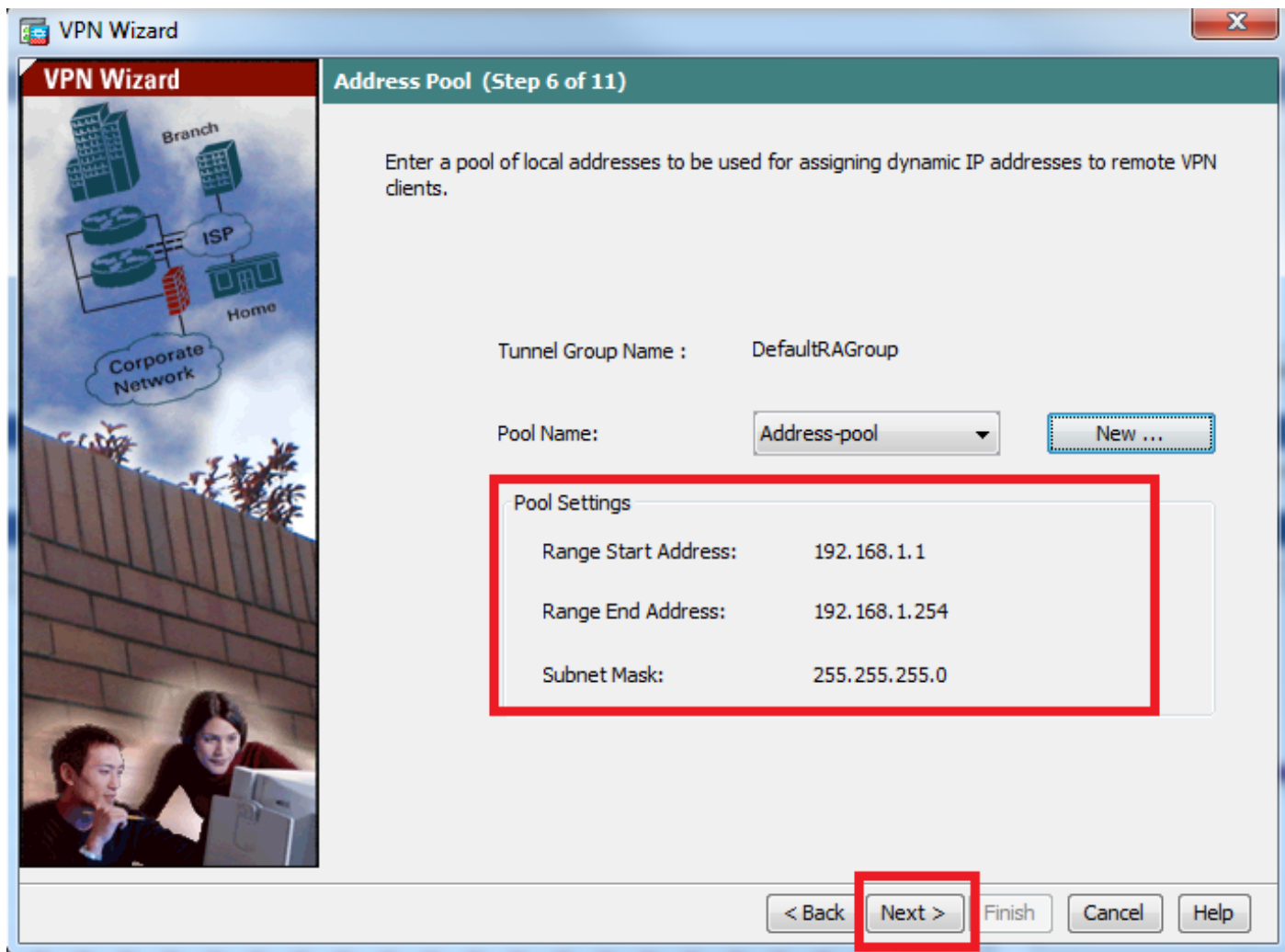


Etapa 8. A caixa de diálogo **Add IPv4 Pool** é exibida.

1. Digite o nome do novo pool de endereços IP.
2. Insira os endereços IP inicial e final.
3. Insira a máscara de sub-rede e clique em **OK**.



Etapa 9. Verifique as configurações do pool e clique em **Avançar**.



Etapa 10. Configure os atributos a serem enviados aos clientes ou deixe-os em branco e clique em **Avançar**.

VPN Wizard

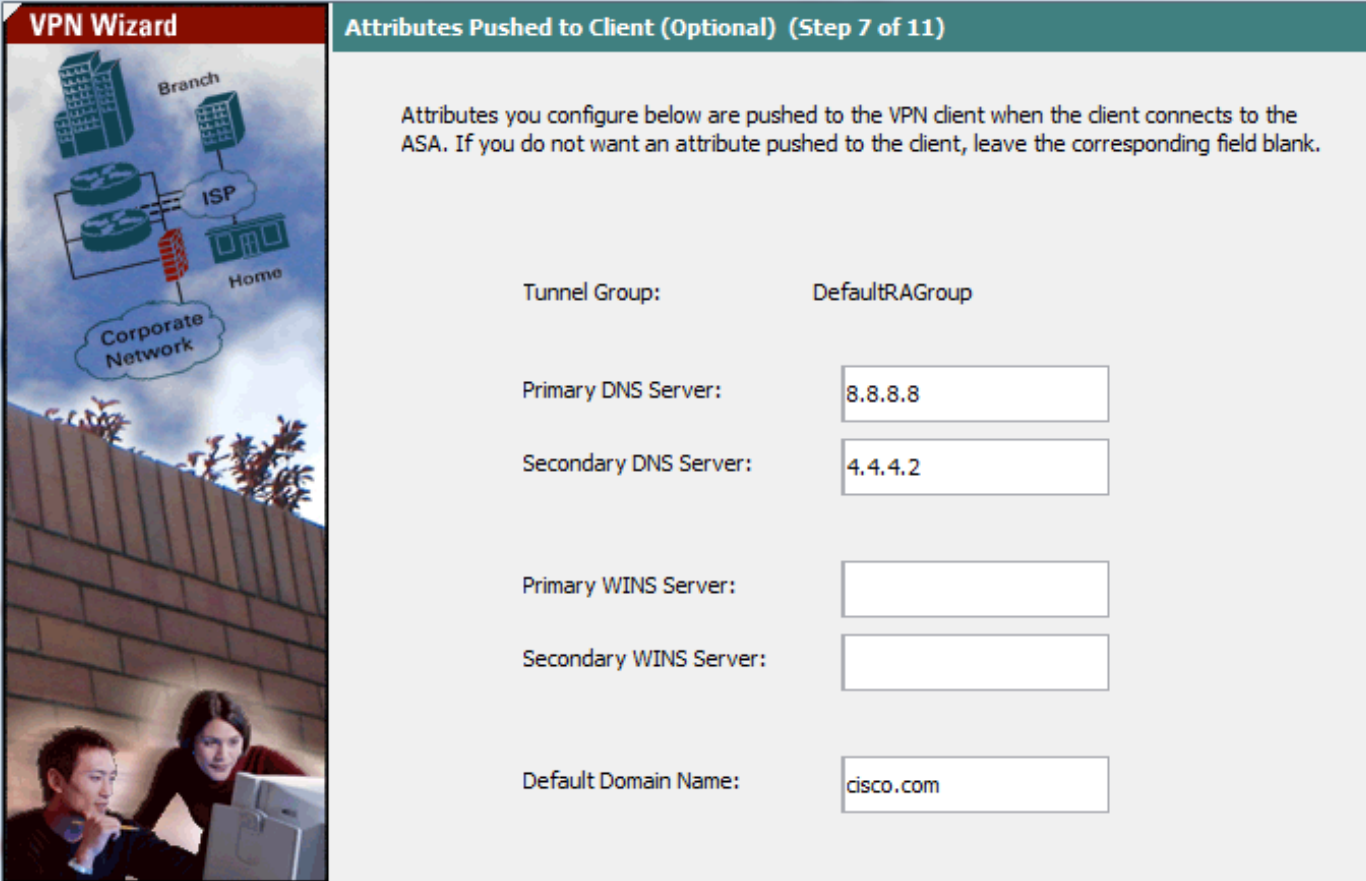
### VPN Wizard

#### Attributes Pushed to Client (Optional) (Step 7 of 11)

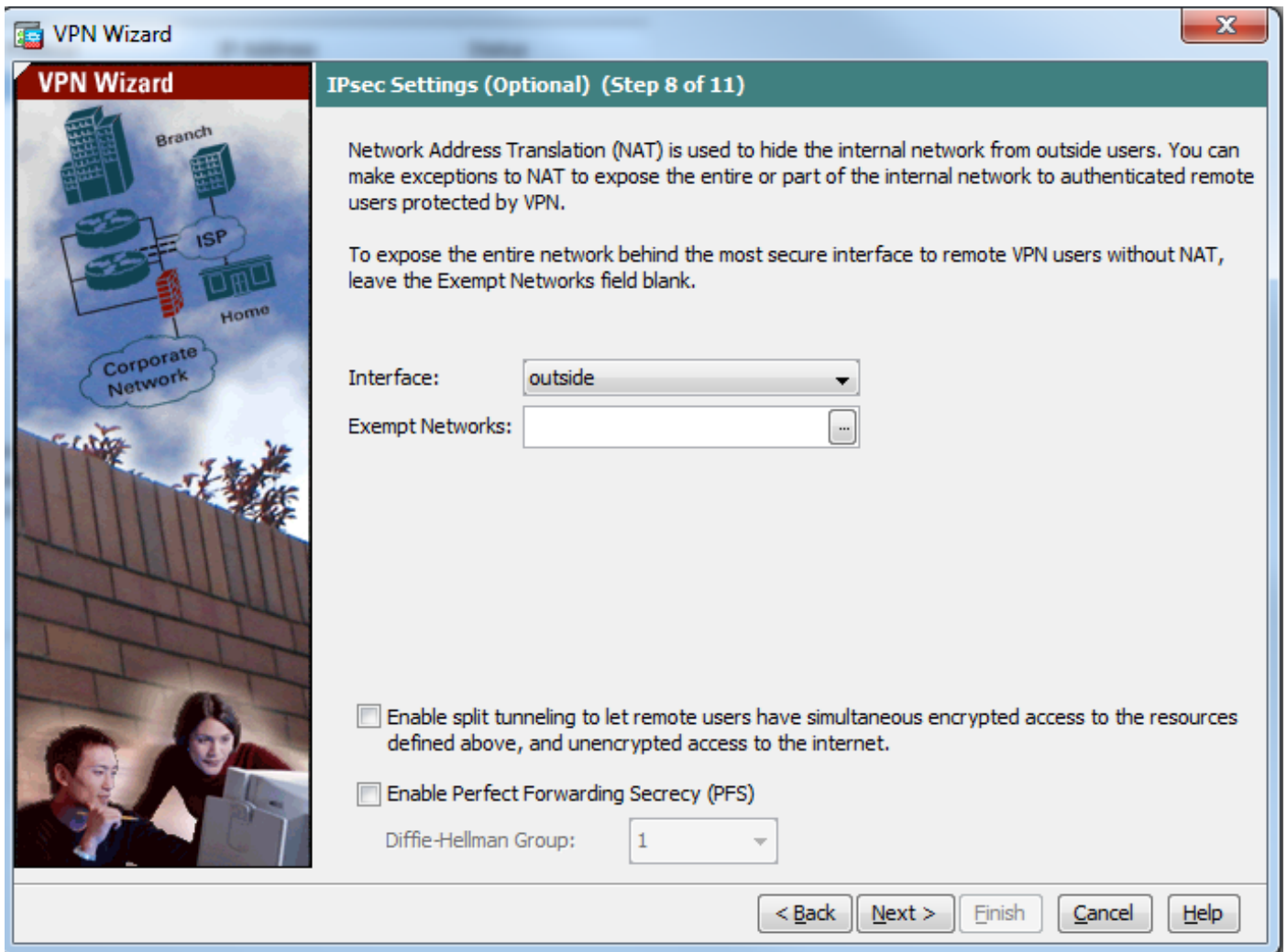
Attributes you configure below are pushed to the VPN client when the client connects to the ASA. If you do not want an attribute pushed to the client, leave the corresponding field blank.

Tunnel Group:	DefaultRAGroup
Primary DNS Server:	<input type="text" value="8.8.8.8"/>
Secondary DNS Server:	<input type="text" value="4.4.4.2"/>
Primary WINS Server:	<input type="text"/>
Secondary WINS Server:	<input type="text"/>
Default Domain Name:	<input type="text" value="cisco.com"/>

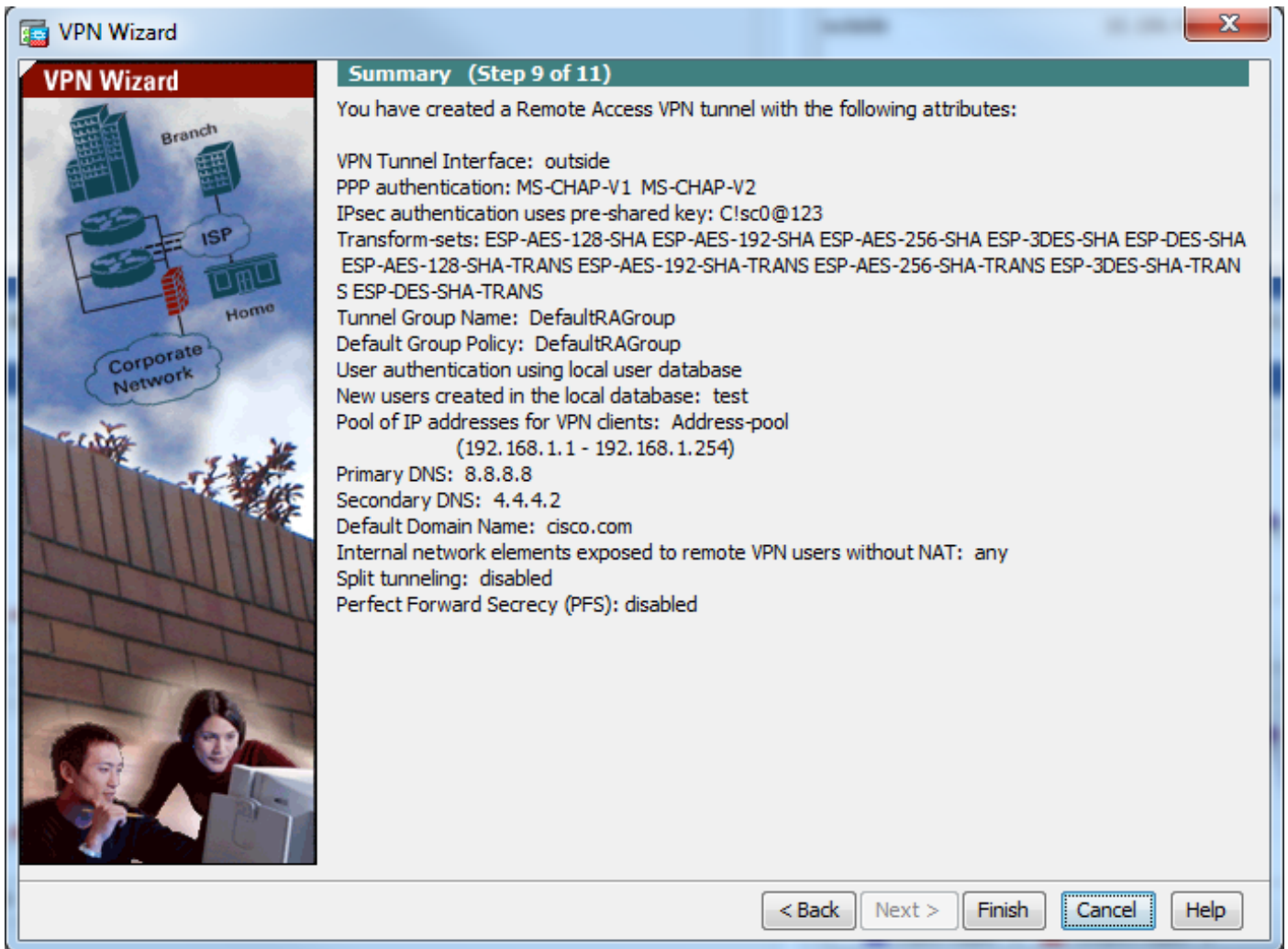
< Back   Next >   Finish   Cancel   Help



Etapa 11: Certifique-se de que a caixa **Ativar segredo de encaminhamento perfeito (PFS)** esteja desmarcada, uma vez que algumas plataformas cliente não suportam este recurso. **Habilite o tunelamento dividido para permitir que usuários remotos tenham acesso criptografado simultâneo aos recursos definidos acima, e o acesso não criptografado à caixa de Internet está desmarcado**, o que significa que o tunelamento completo está habilitado no qual todo o tráfego (incluindo o tráfego de Internet) da máquina cliente será enviado para o ASA pelo túnel VPN. Clique em Next.



Etapa 12. Revise as informações de resumo e clique em **Concluir**.



## Configuração do ASA usando CLI

**Etapa 1. Configure os parâmetros da política IKE Fase 1.**

Essa política é usada para proteger o tráfego de controle entre os peers (isto é, ela protege a chave pré-compartilhada e as negociações da fase 2)

```
ciscoasa(config)#crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)#authentication pre-share
ciscoasa(config-ikev1-policy)#encryption 3des
ciscoasa(config-ikev1-policy)#hash sha
ciscoasa(config-ikev1-policy)#group 2
ciscoasa(config-ikev1-policy)#lifetime 86400
ciscoasa(config-ikev1-policy)#exit
```

**Etapa 2. Configure Transform-set.**

Contém parâmetros de política IKE Fase 2 que são usados para proteger o tráfego de dados. Como o cliente Windows L2TP/IPsec usa o modo de transporte IPsec, defina o modo de transporte. O padrão é o modo túnel

```
ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac
ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport
```

**Etapa 3. Configure o mapa dinâmico.**

À medida que os clientes do Windows recebem o endereço IP dinâmico do ISP ou do servidor

DHCP local (exemplo de modem), o ASA não está ciente do endereço IP do peer e isso coloca um problema na configuração de um peer estático na extremidade do ASA. Portanto, a configuração de criptografia dinâmica deve ser abordada, na qual todos os parâmetros não são necessariamente definidos e os parâmetros ausentes são aprendidos dinamicamente posteriormente, como resultado da negociação de IPsec do cliente.

```
ciscoasa(config)#crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set TRANS-ESP-3DES-SHA
```

**Etapa 4. Vincule o mapa dinâmico ao mapa de criptografia estático e aplique o mapa de criptografia e ative o IKEv1 na interface externa**

O mapa de criptografia dinâmico não pode ser aplicado em uma interface e, portanto, vinculá-lo ao mapa de criptografia estático. Os conjuntos de criptografia dinâmicos devem ser os mapas de criptografia de prioridade mais baixa no conjunto de mapas de criptografia (ou seja, eles devem ter os números de sequência mais altos) para que o ASA avalie outros mapas de criptografia primeiro. Ele examina o mapa de criptografia dinâmico definido somente quando as outras entradas do mapa (estático) não correspondem.

```
ciscoasa(config)#crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
ciscoasa(config)#crypto map outside_map interface outside
ciscoasa(config)#crypto ikev1 enable outside
```

**Etapa 5. Criar pool de endereços IP**

Crie um pool de endereços dos quais os endereços IP são atribuídos dinamicamente aos VPN Clients remotos. Ignore esta etapa para usar o pool existente no ASA.

```
ciscoasa(config)#ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0
```

**Etapa 6. Configurar política de grupo**

Identificar a política de grupo como interna, o que significa que os atributos são extraídos do banco de dados local.

```
ciscoasa(config)#group-policy L2TP-VPN internal
```

**Note:** As conexões L2TP/IPsec podem ser configuradas com a política de grupo padrão (DfltGrpPolicy) ou com uma política de grupo definida pelo usuário. Em ambos os casos, a política de grupo deve ser configurada para usar o protocolo de tunelamento L2TP/IPsec. configure l2tp-ipsec no atributo do protocolo VPN na política de grupo padrão que será herdada para a política de grupo definida pelo usuário se o atributo do protocolo vpn não estiver configurado nela.

Configurar atributos como o protocolo de túnel vpn (no nosso caso, é l2tp-ipsec), nome de domínio, endereço IP do servidor DNS e WINS e novas contas de usuário

```
ciscoasa(config)#group-policy L2TP-VPN attributes
ciscoasa(config-group-policy)#dns-server value 8.8.8.8 4.4.4.2
ciscoasa(config-group-policy)#vpn-tunnel-protocol l2tp-ipsec
ciscoasa(config-group-policy)#default-domain value cisco.com
```

Configure nomes de usuário e senhas no dispositivo além de usar AAA. Se o usuário for um cliente L2TP que usa o Microsoft CHAP versão 1 ou versão 2 e o ASA estiver configurado para se autenticar no banco de dados local, a palavra-chave mschap deverá ser incluída. Por exemplo, nome de usuário <nome de usuário> senha <senha> mschap.



```
ciscoasa(config-group-policy)# username test password test mschap
```

#### Passo 7. Configure tunnel-group

Crie um grupo de túneis com o comando **tunnel-group** e especifique o nome do pool de endereços local usado para alocar o endereço IP ao cliente. Se o método de autenticação for pre-shared-key, o nome do grupo de túneis deve ser DefaultRAGroup, pois não há opção no cliente para especificar o grupo de túneis e, portanto, ele aterrissa somente no grupo de túneis padrão. Vincule a política de grupo ao grupo de túneis usando o comando default-group-policy

```
ciscoasa(config)#tunnel-group DefaultRAGroup general-attributes
ciscoasa(config-tunnel-general)#address-pool Address-pool
ciscoasa(config-tunnel-general)#default-group-policy L2TP-VPN
ciscoasa(config-tunnel-general)#exit
```

**Note:** O perfil de conexão padrão (grupo de túnel), DefaultRAGroup deve ser configurado, se a autenticação com base em chave pré-compartilhada for executada. Se a autenticação baseada em certificado for executada, um perfil de conexão definido pelo usuário poderá ser escolhido com base nos identificadores de certificado

Use o comando **tunnel-group ipsec-attribute** para entrar no modo de configuração de atributo ipsec para definir a chave pré-compartilhada.

```
ciscoasa(config)# tunnel-group DefaultRAGroup ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev1 pre-shared-key C!sc0@l23
ciscoasa(config-tunnel-ipsec)#exit
```

Configure o protocolo de autenticação PPP com o comando **authentication type** do modo tunnel group ppp-attribute. Desative o CHAP que está ativado por padrão, pois não é suportado se o servidor AAA estiver configurado como banco de dados local.

```
ciscoasa(config)#tunnel-group DefaultRAGroup ppp-attributes
ciscoasa(config-ppp)#no authentication chap
ciscoasa(config-ppp)#authentication ms-chap-v2
ciscoasa(config-ppp)#exit
```

#### Etapa 8. Configurar isenção de NAT

Configure o NAT-Isenção para que os clientes possam acessar recursos internos conectados às interfaces internas (neste exemplo, os recursos internos são conectados à interface interna).

```
ciscoasa(config)#object network L2TP-Pool
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)#exit
ciscoasa(config)# nat (inside,outside) source static any any destination static L2TP-Pool L2TP-
Pool no-proxy-arp route-lookup
```

#### Exemplo de configuração completa

```
crypto ikev1 policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
exit
```

```
crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport

crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set TRANS-ESP-3DES-SHA

crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface outside
crypto ikev1 enable outside

ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0

group-policy L2TP-VPN internal
group-policy L2TP-VPN attributes
vpn-tunnel-protocol l2tp-ipsec
default-domain value cisco.com
username test password test mschap
exit

tunnel-group DefaultRAGroup general-attributes
address-pool Address-pool
default-group-policy L2TP-VPN
exit

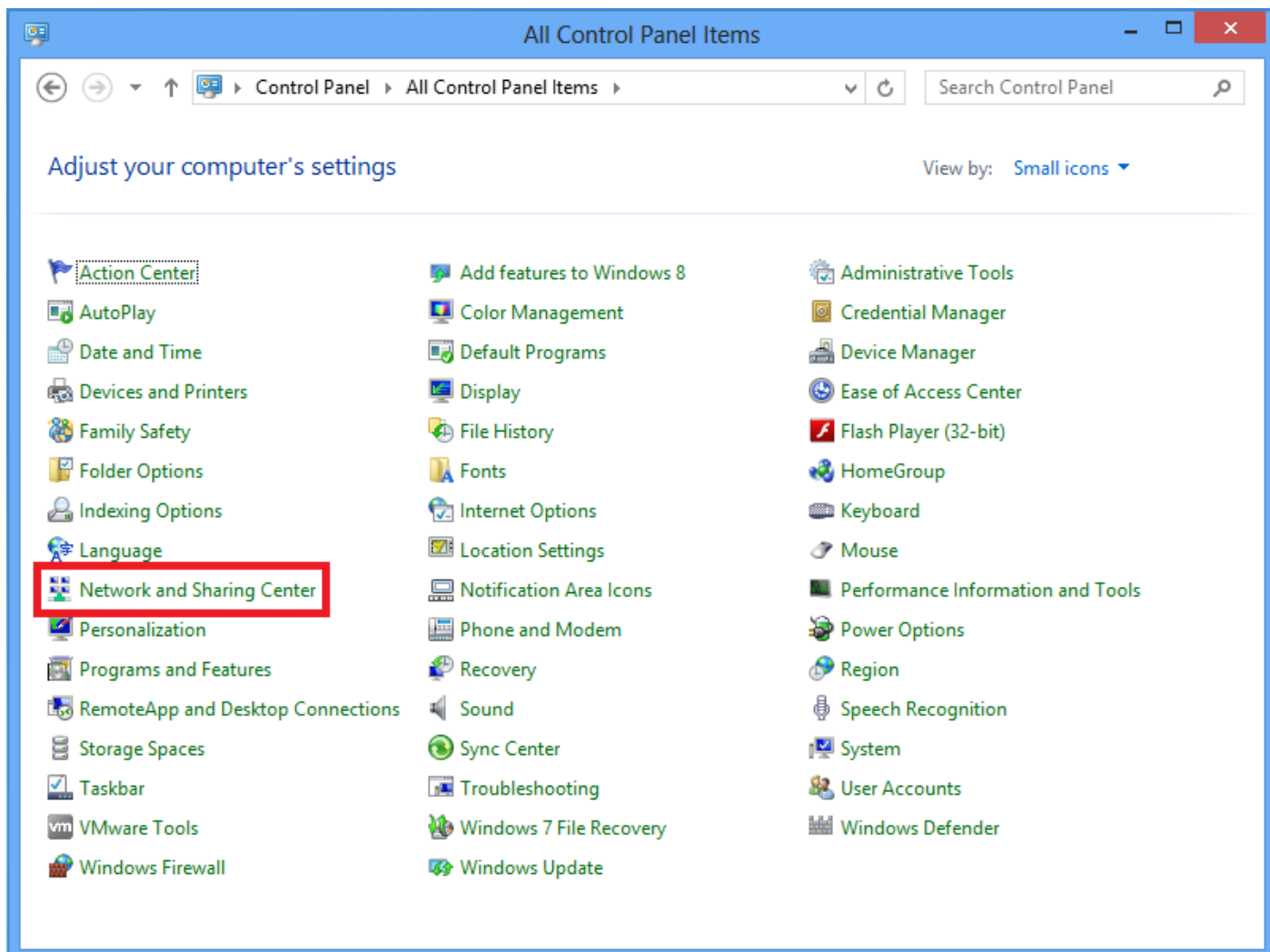
tunnel-group DefaultRAGroup ipsec-attributes
ikev1 pre-shared-key C!sc0@123
exit

tunnel-group DefaultRAGroup ppp-attributes
no authentication chap
authentication ms-chap-v2
exit

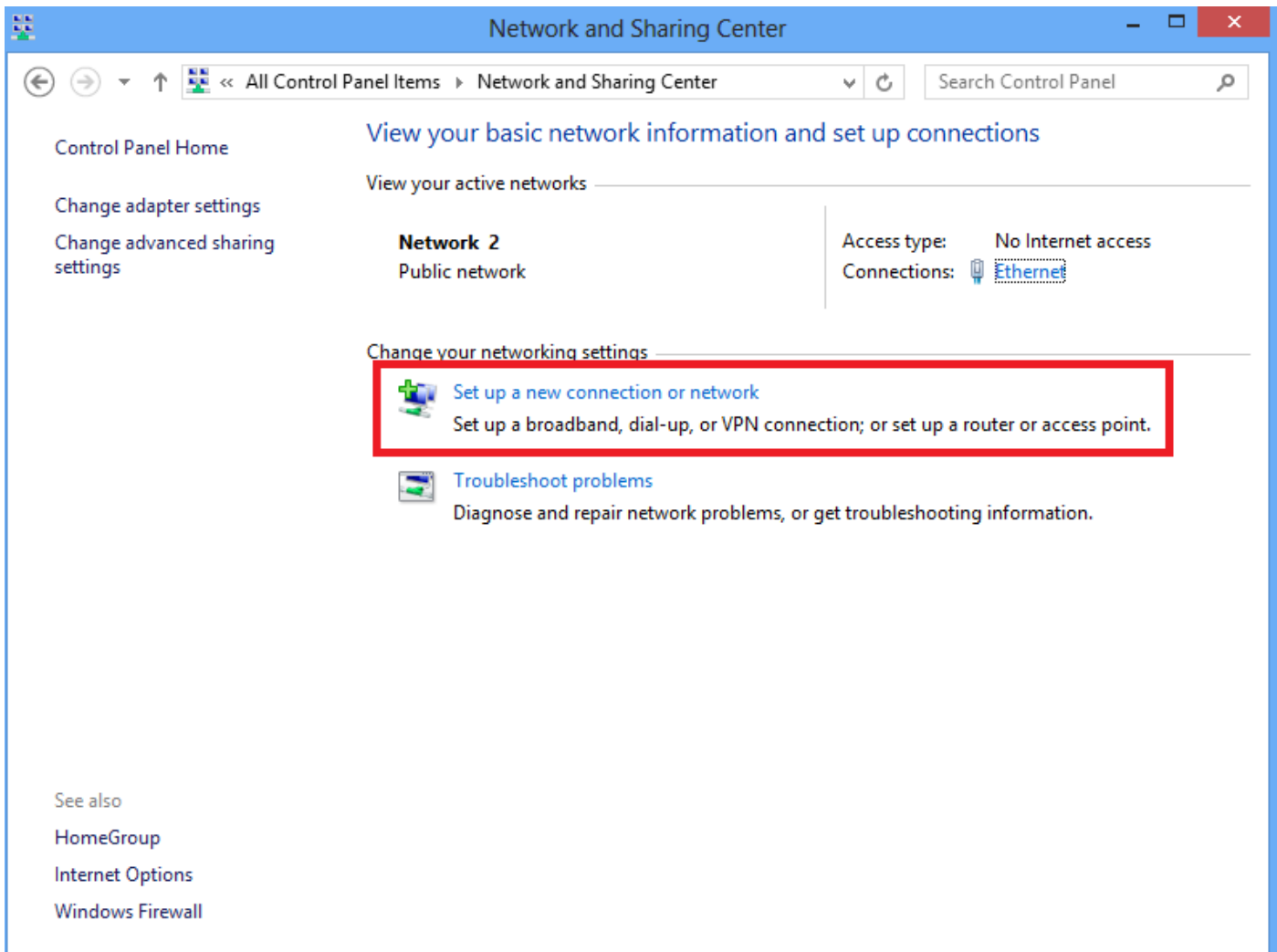
object network L2TP-Pool
subnet 192.168.1.0 255.255.255.0
exit
nat(inside,outside) source static any any destination static L2TP-Pool L2TP-Pool no-proxy-arp
route-lookup
```

## Configuração do cliente L2TP/IPsec do Windows 8

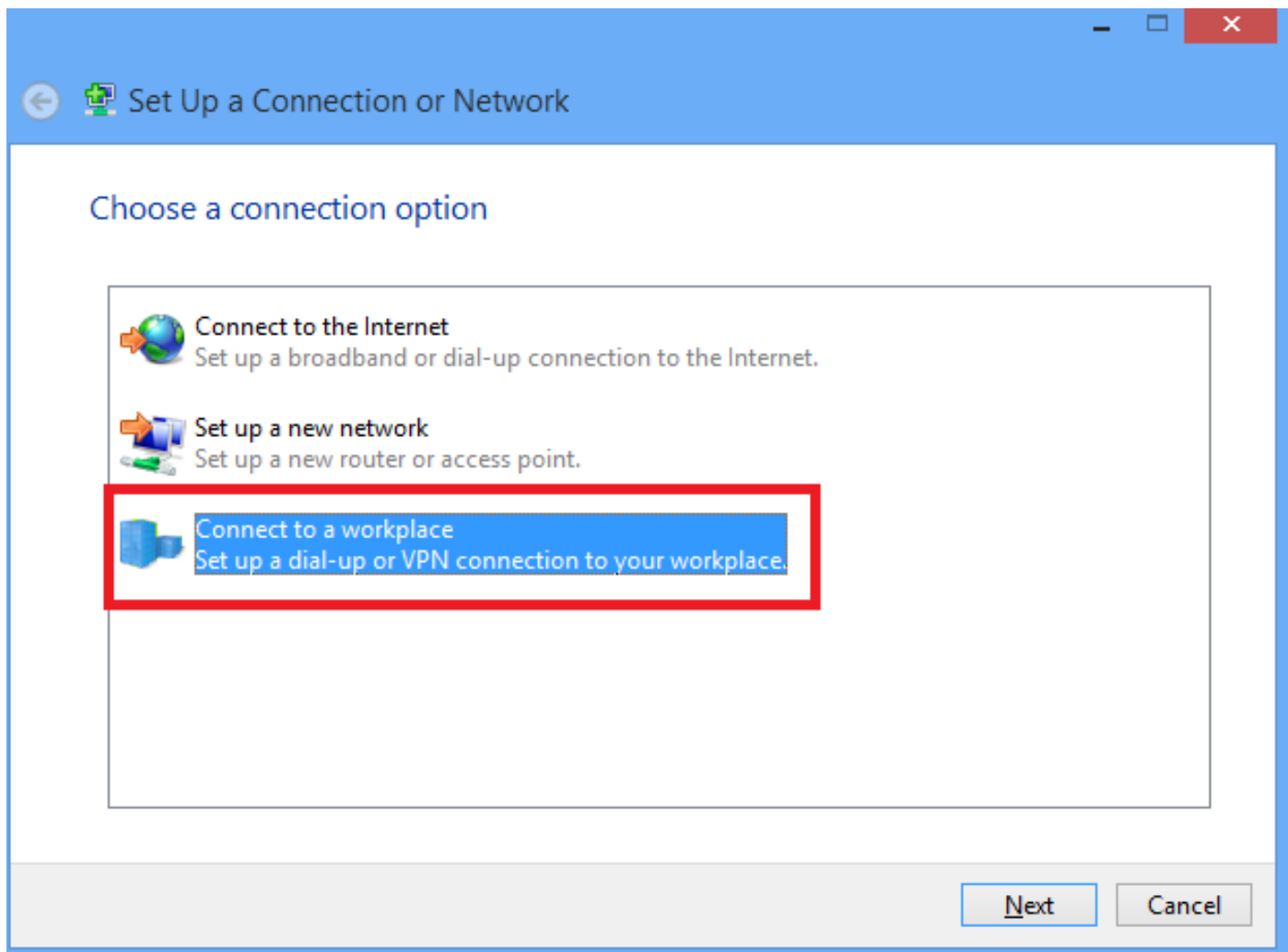
1. Abra o painel de controle e selecione Central de redes e compartilhamento.



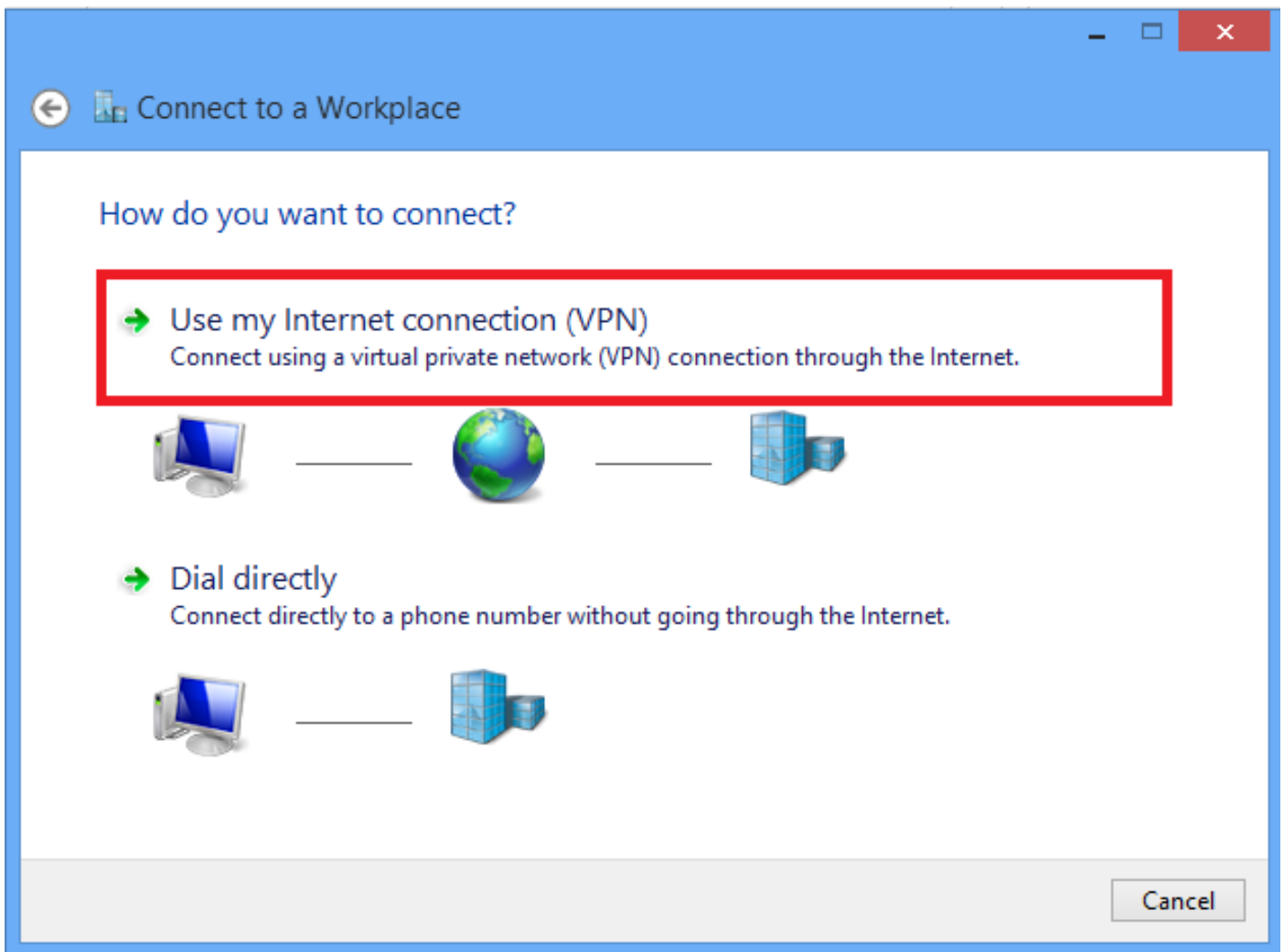
2. Escolha **Configurar uma nova conexão ou uma nova opção de rede**.



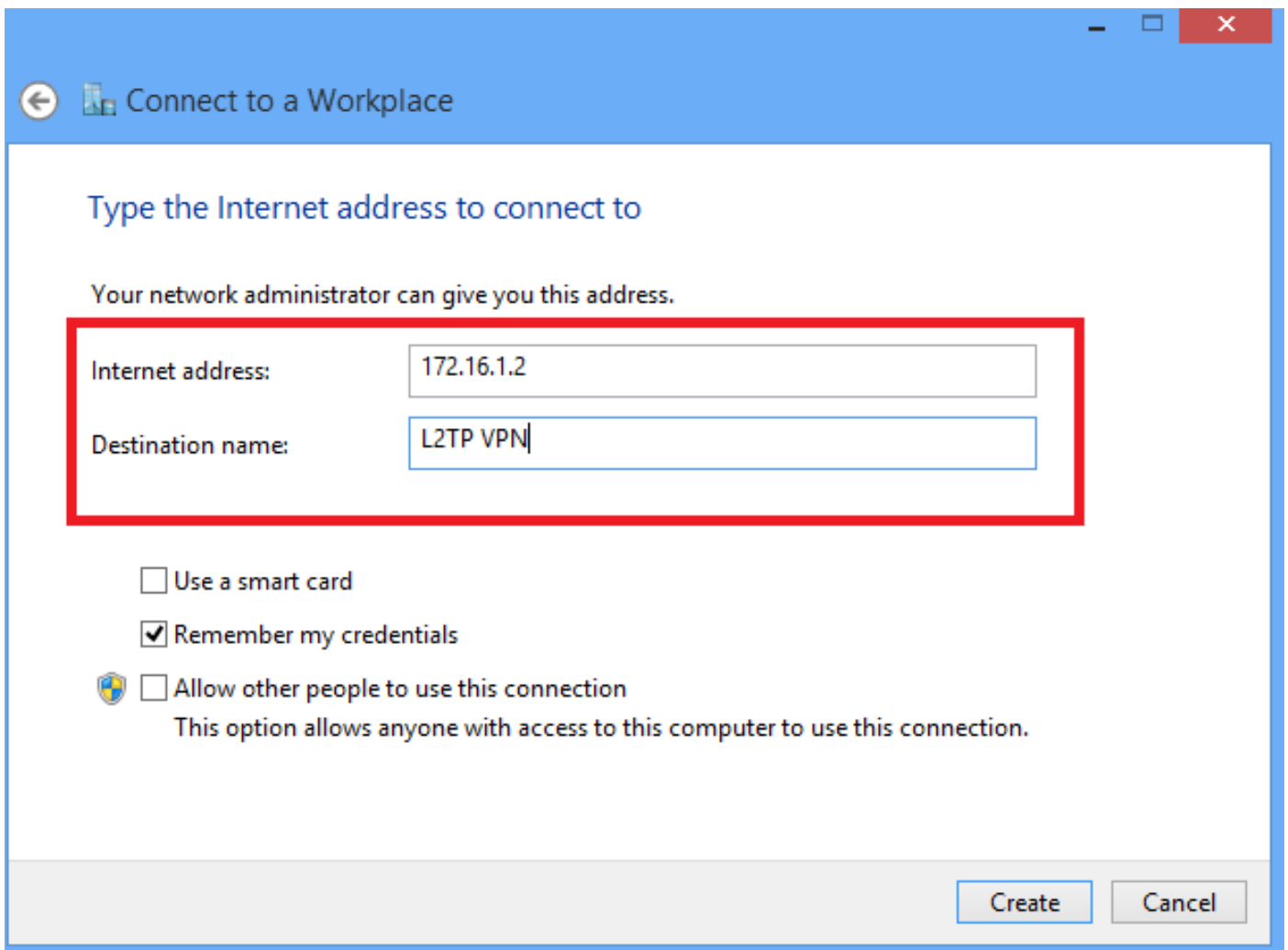
3. Escolha **Conectar-se a uma opção de local de trabalho** e clique em **Avançar**.



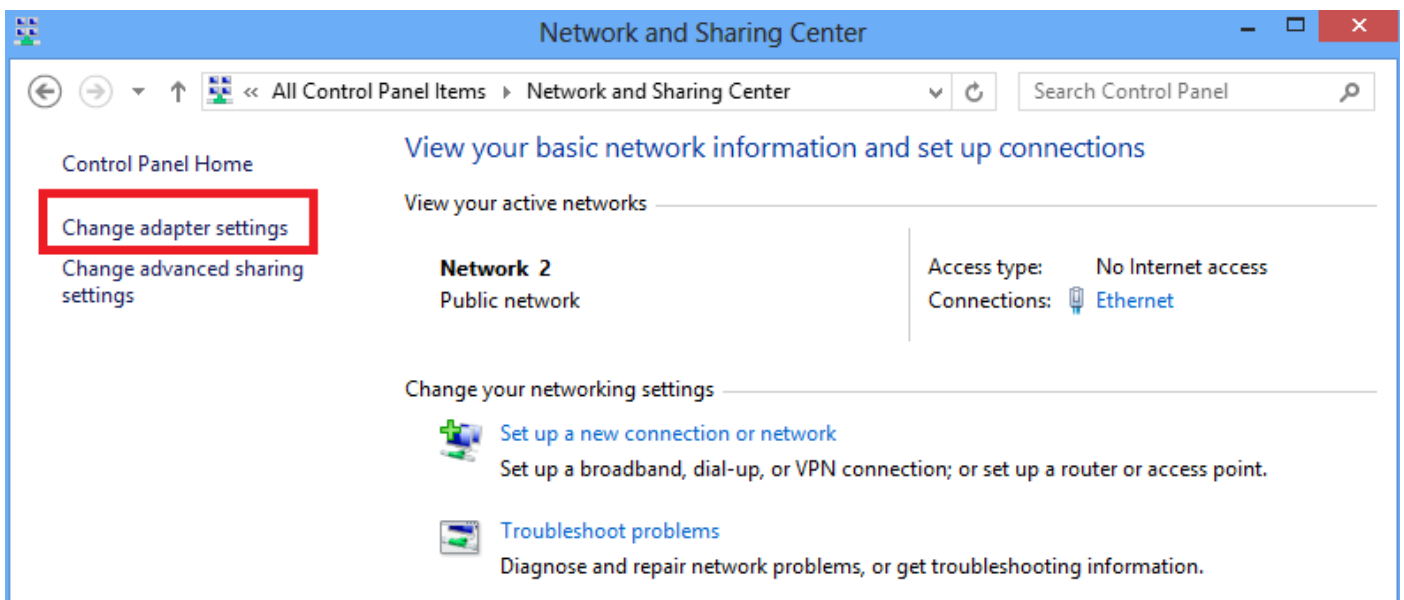
4. Clique na opção **Usar minha conexão com a Internet (VPN)**.



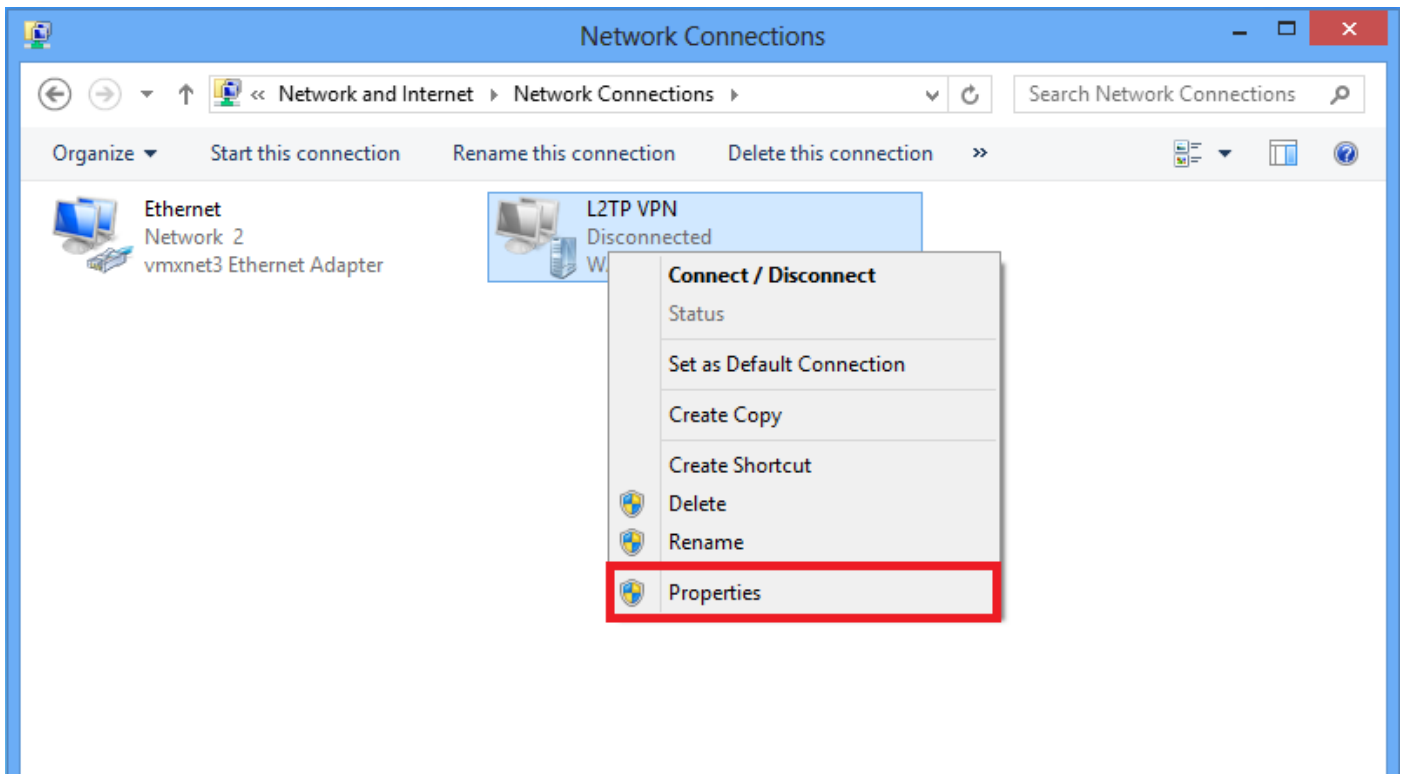
5. Insira o endereço IP da interface WAN ou FQDN do ASA e qualquer nome para o adaptador VPN que seja significativo localmente e clique em **Criar**.



6. No Centro de Rede e Compartilhamento, escolha a opção **Alterar configurações do adaptador** no painel esquerdo da janela.

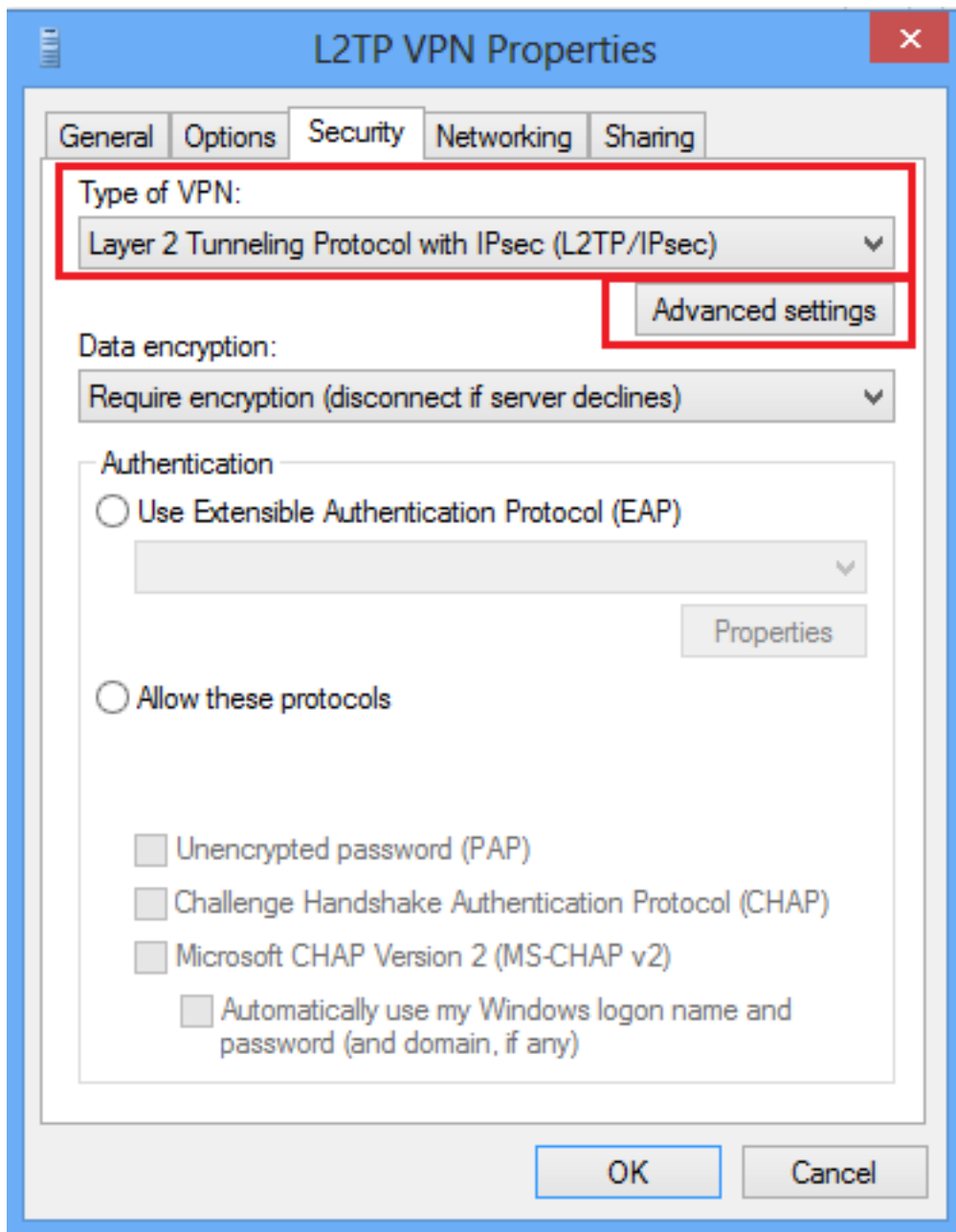


7. Clique com o botão direito do mouse no adaptador recém-criado para L2TP VPN e escolha **Propriedades**.

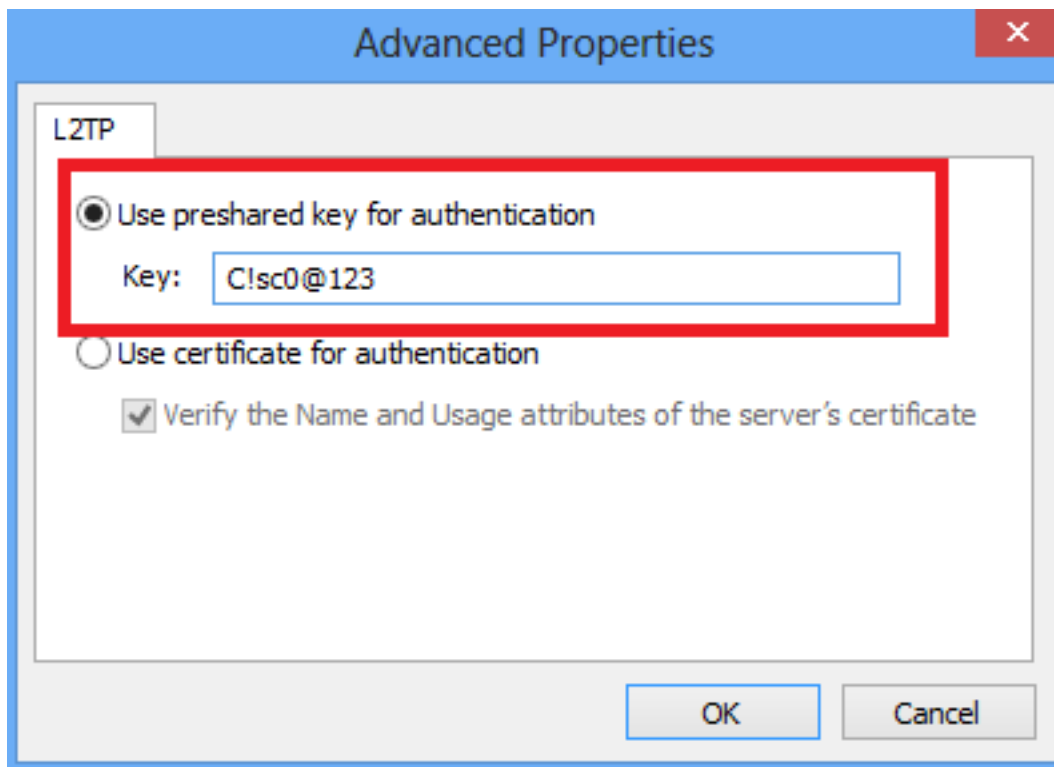


8. Navegue até a guia **Segurança**, escolha o Tipo de VPN como **Protocolo de Tunelamento de Camada 2 com IPsec (L2TP/IPsec)** e clique em **Configurações avançadas**.

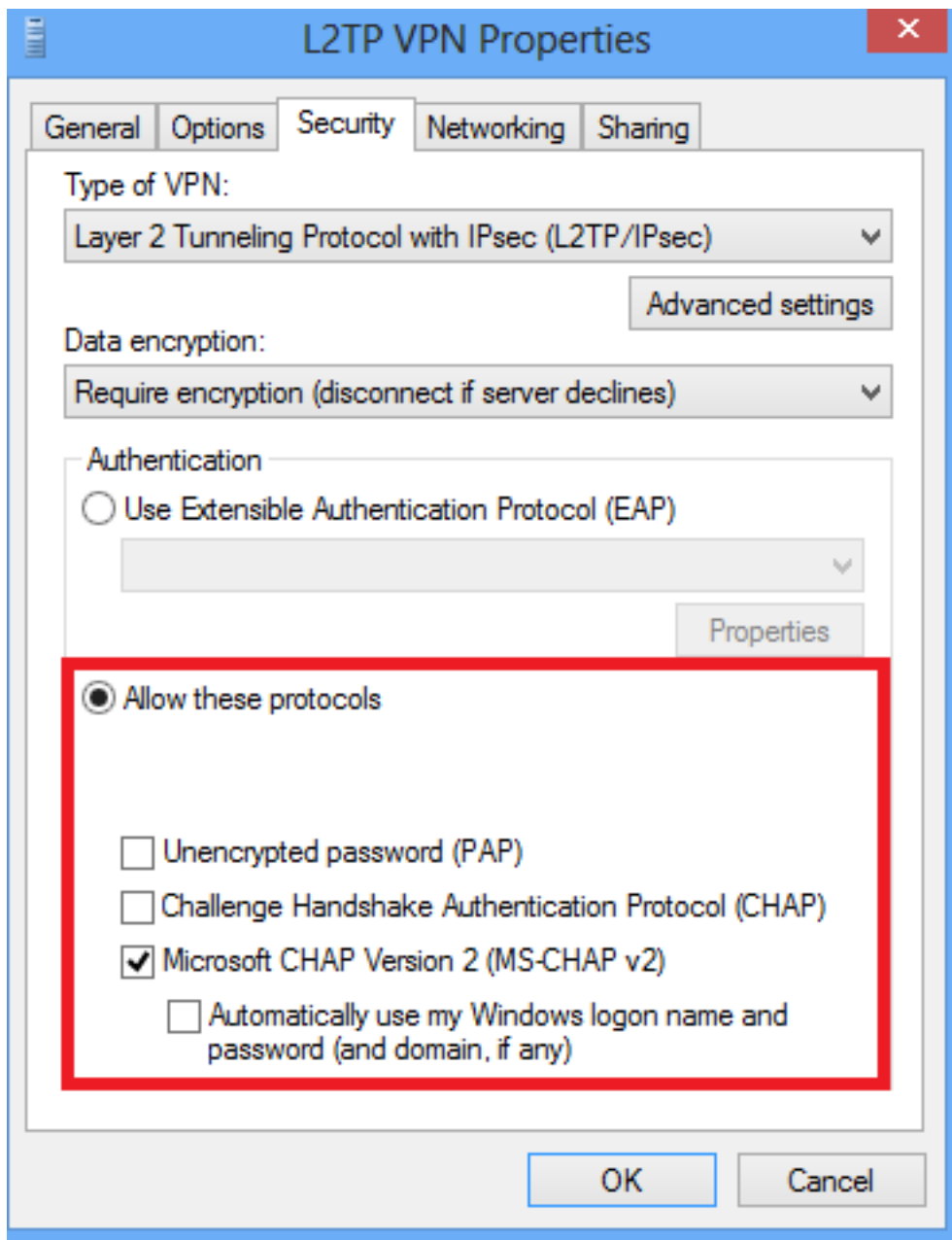




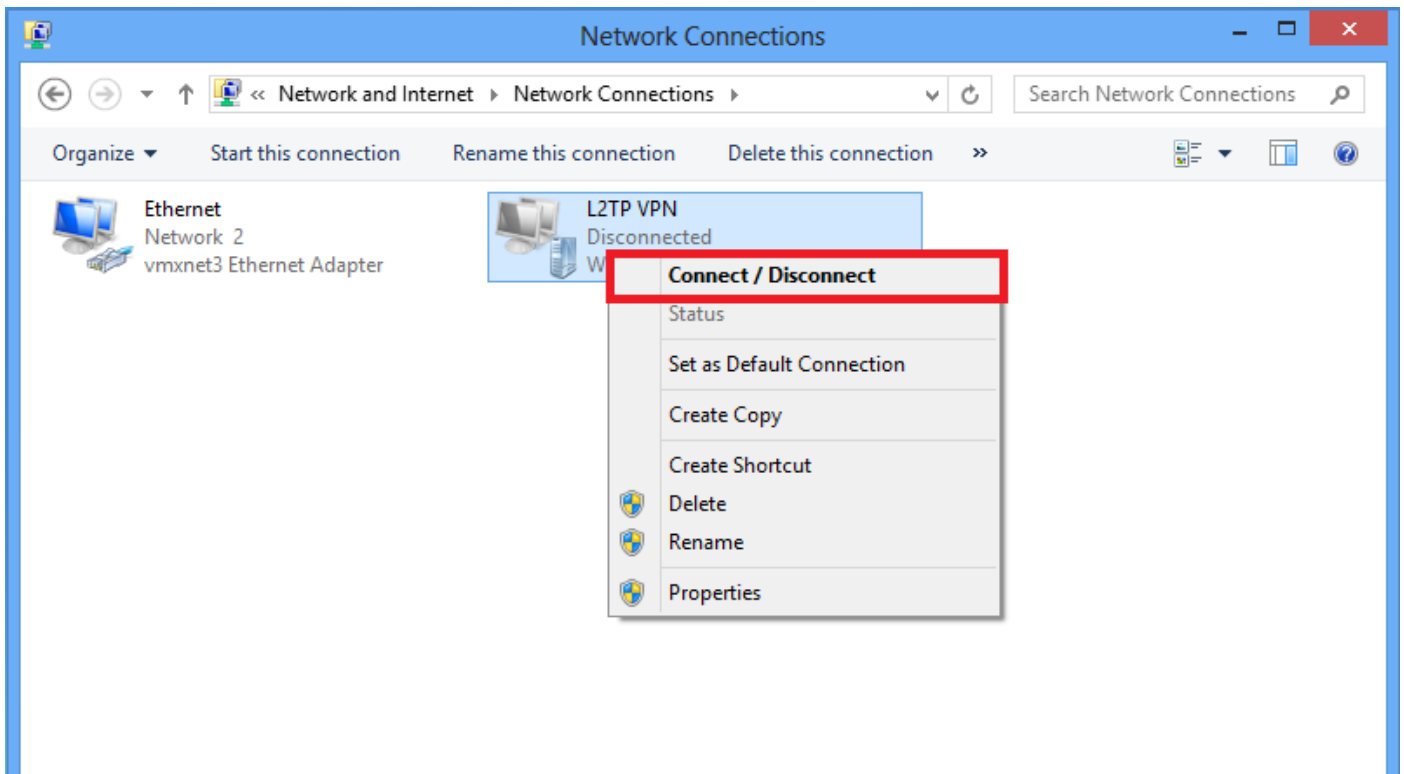
9. Digite a chave pré-compartilhada como a mesma mencionada no grupo de túneis **DefaultRAGgroup** e clique em **OK**. Neste exemplo, C!sc0@123 é usado como a chave pré-compartilhada.



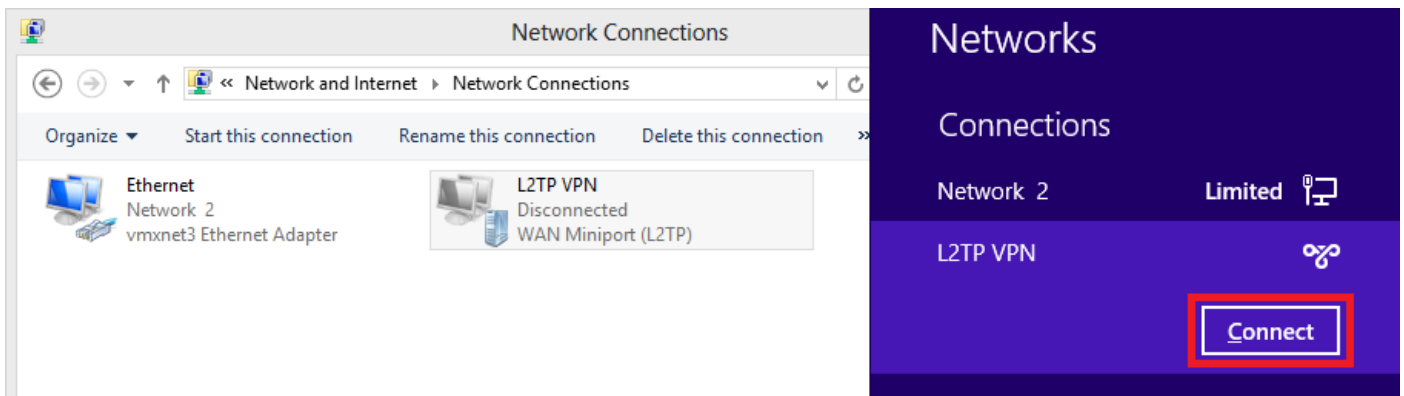
10. Escolha o método de autenticação como Permitir esses protocolos e certifique-se de que apenas a caixa de seleção "Microsoft CHAP Versão 2 (MS-CHAP v2)" esteja marcada e clique em OK.



11. Em conexões de rede, clique com o botão direito do mouse no adaptador L2TP VPN e escolha **Connect/Disconnect**.



12. O ícone Redes aparecerá e clique em **Conectar** na conexão VPN L2TP.



13. Digite as credenciais do usuário e clique em **OK**.

# ← Networks

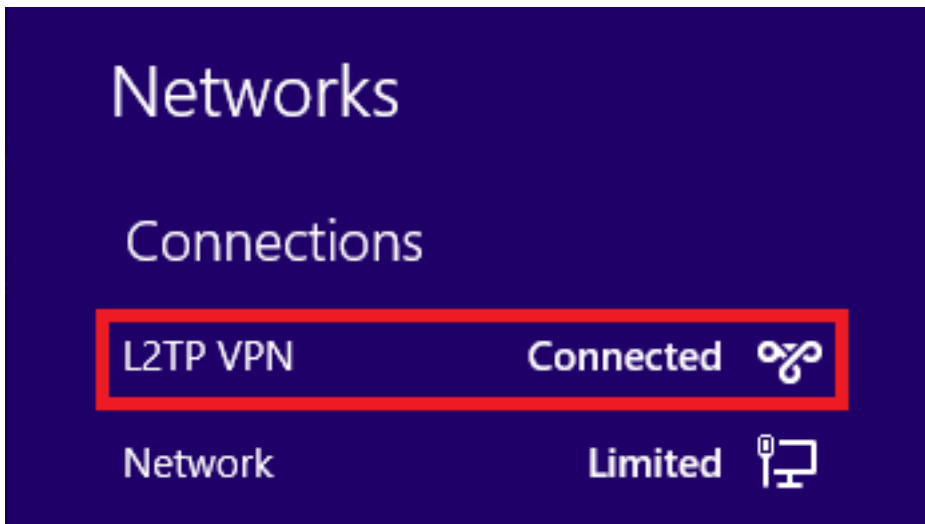
Connecting to 172.16.1.2

## Network Authentication



Domain:

Se os parâmetros necessários forem correspondentes em ambas as extremidades, a conexão L2TP/IPsec será estabelecida.



## Configuração de túnel dividido

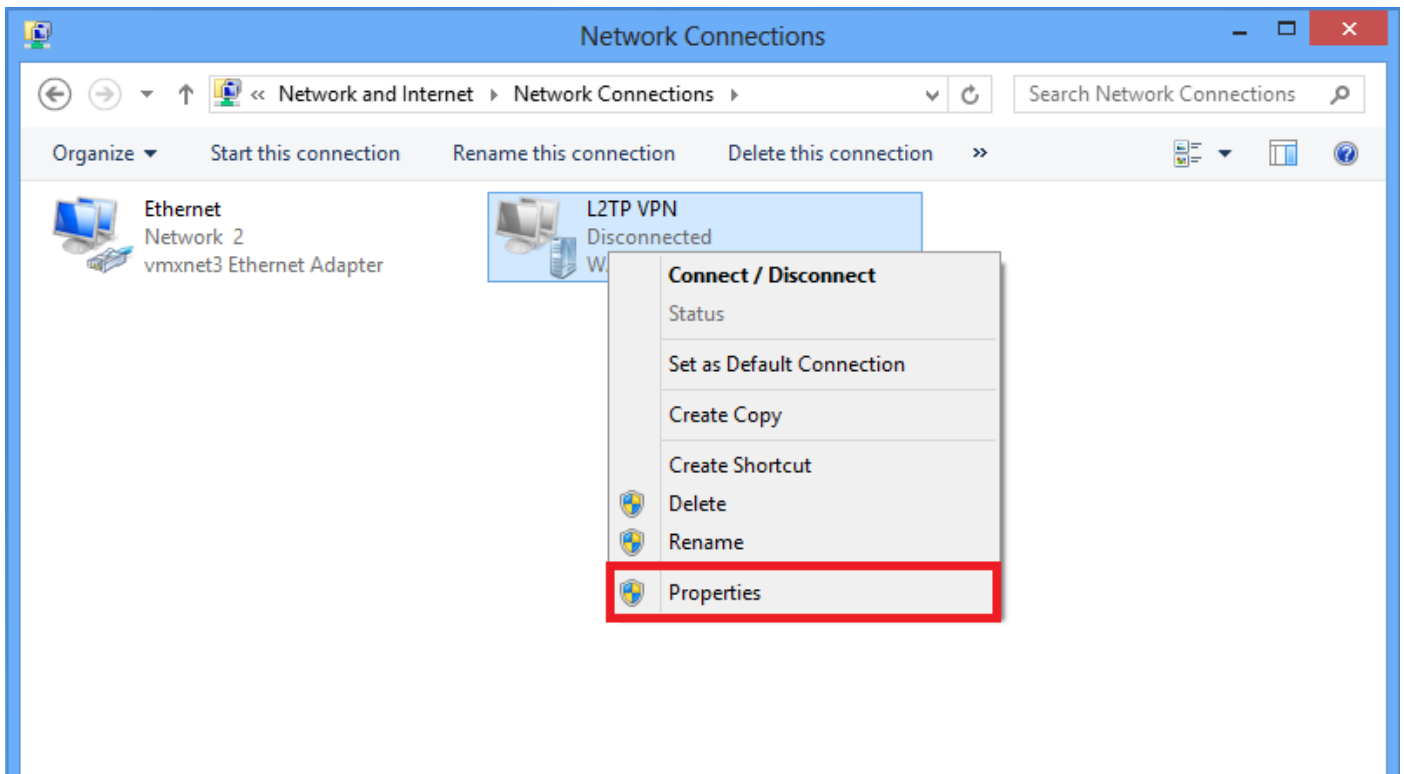
O túnel dividido é um recurso que você pode usar para definir o tráfego para as sub-redes ou os hosts que devem ser criptografados. Isso envolve a configuração de uma ACL (Access Control List, lista de controle de acesso) associada a esse recurso. O tráfego para as sub-redes ou hosts definidos nessa ACL é criptografado sobre o túnel a partir da extremidade do cliente, e as rotas para essas sub-redes são instaladas na tabela de roteamento do PC. O ASA intercepta a mensagem DHCPINFORM de um cliente e responde com a máscara de sub-rede, o nome de domínio e as rotas estáticas sem classe.

## Configuração do ASA

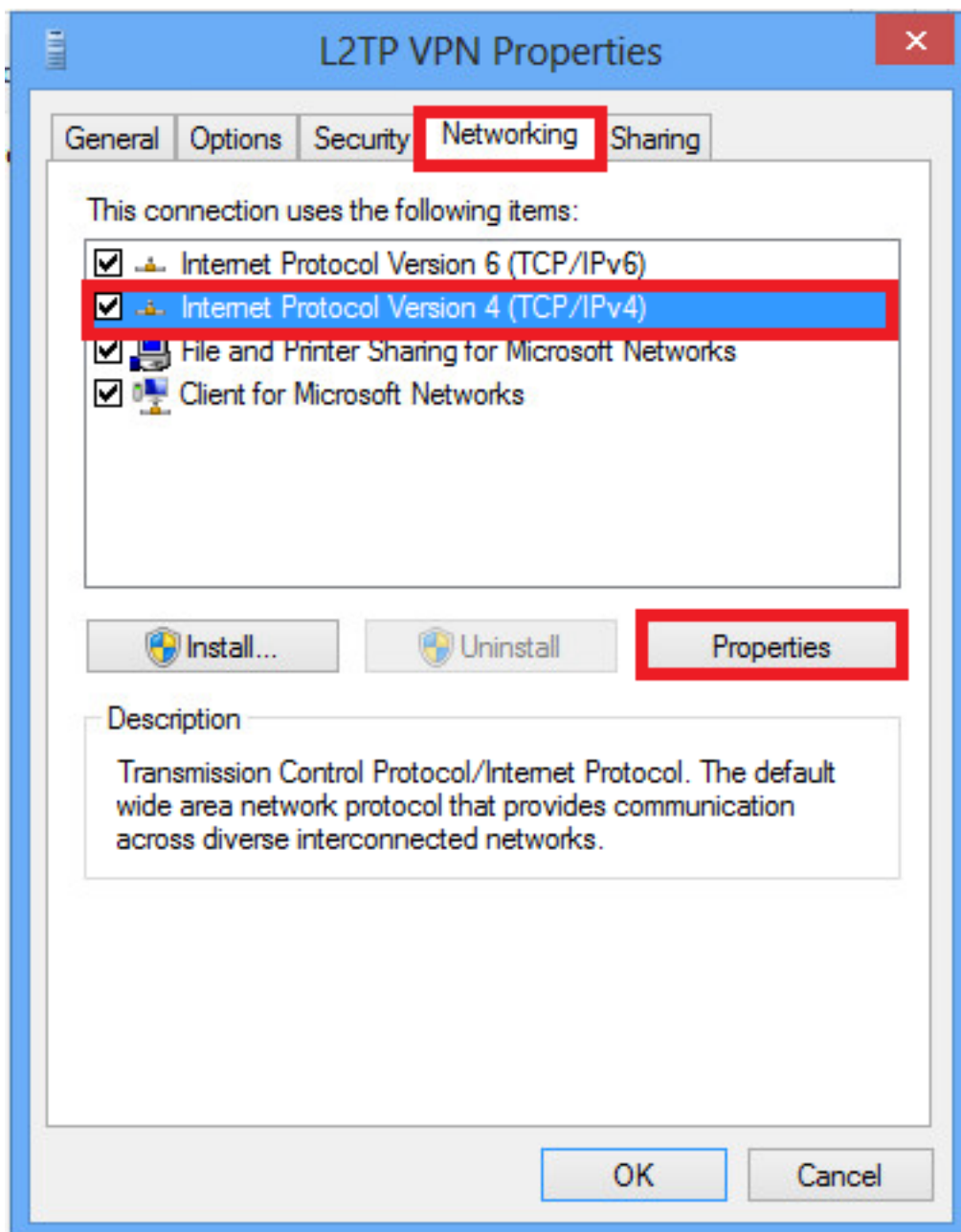
```
ciscoasa(config)# access-list SPLIT standard permit 10.1.1.0 255.255.255.0  
  
ciscoasa(config)# group-policy DefaultRAGroup attributes  
ciscoasa(config-group-policy)# split-tunnel-policy tunnelspecified  
ciscoasa(config-group-policy)# split-tunnel-network-list value SPLIT  
ciscoasa(config-group-policy)# intercept-dhcp 255.255.255.255 enable
```

## Configuração no cliente L2TP/IPsec

1. Clique com o botão direito do mouse no adaptador L2TP VPN e escolha **Propriedades**.

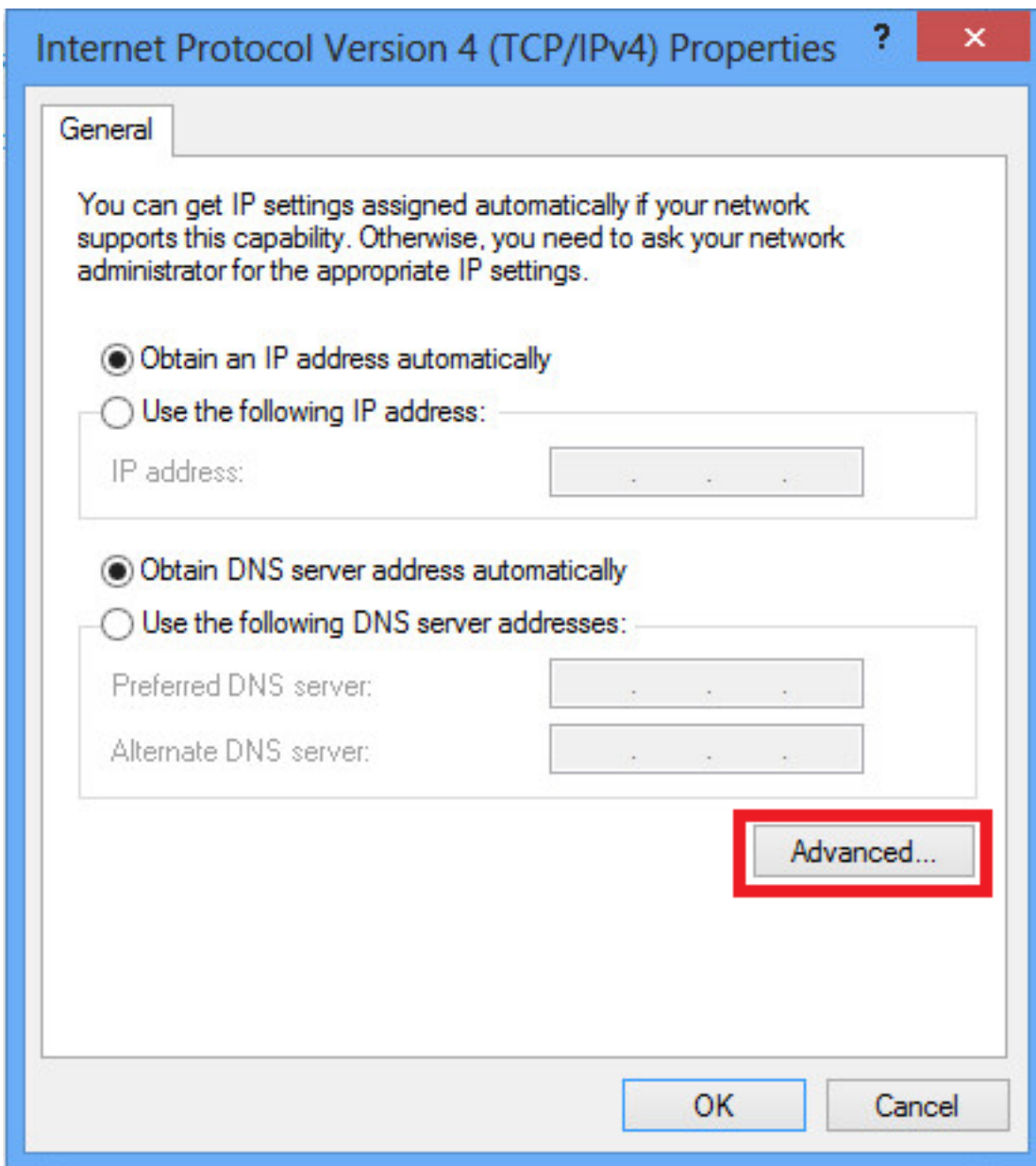


2. Navegue até a guia Rede, escolha Protocolo de Internet Versão 4 (TCP/IPv4) e clique em **Propriedades**.

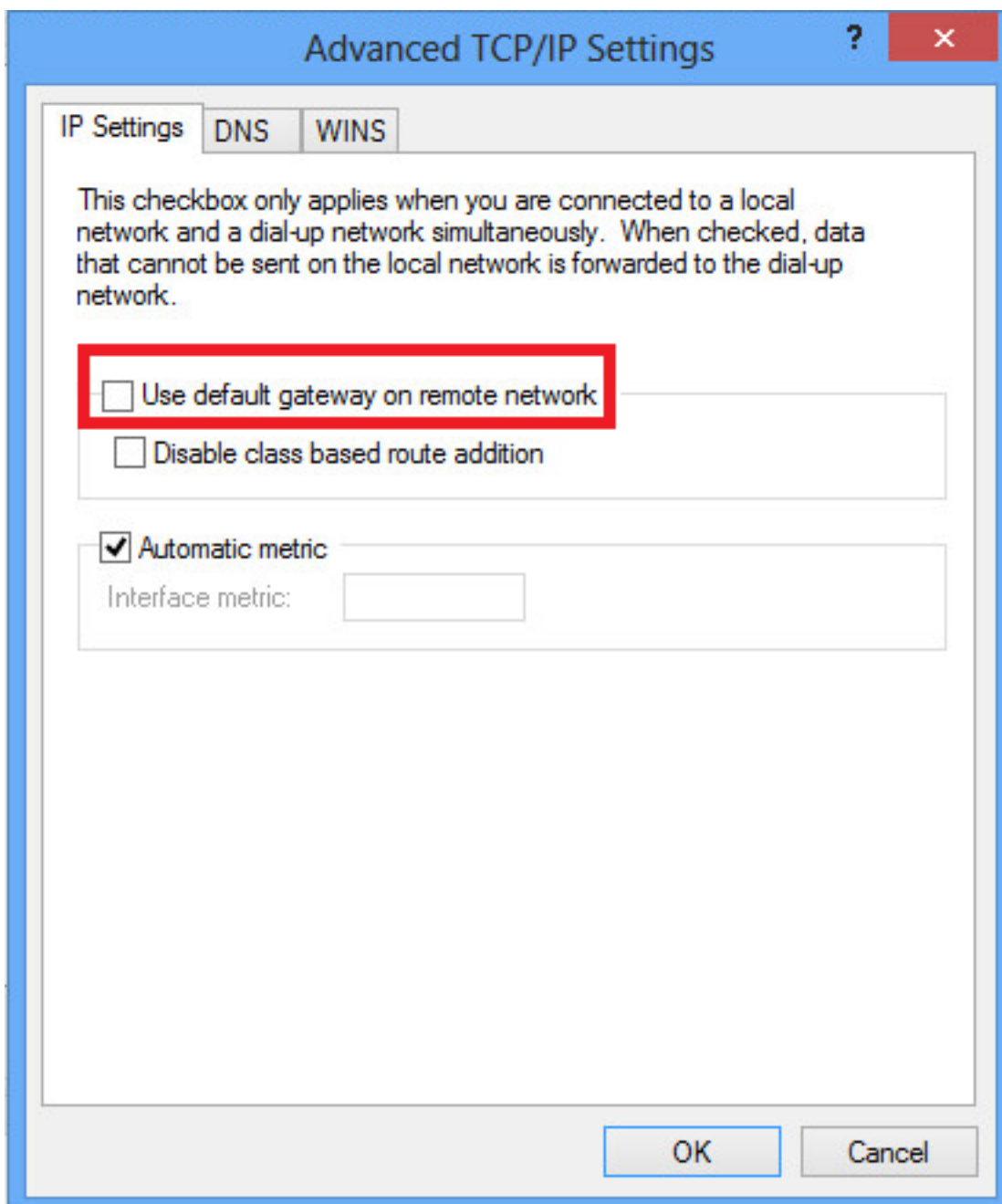


3. Clique na opção **Avançado**.





4. Desmarque **Usar gateway padrão** na opção de rede remota e clique em **OK**.



## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

**Note:** 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 ikev1 sa` - Mostra todas as SAs IKE atuais em um peer.

```
ciscoasa# show crypto ikev1 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:

### 10.1.1.2

Type : user                    Role : responder  
Rekey : no

**State : MM\_ACTIVE**

- **show crypto ipsec sa** - Mostra todas as SAs IPsec atuais em um peer.

```
ciscoasa# show crypto ipsec sa
interface: outside
Crypto map tag:
```

#### **outside\_dyn\_map**

, seq num: 10, local addr: 172.16.1.2

local ident (addr/mask/prot/port): (172.16.1.2/255.255.255.255/

#### **17/1701**

)  
remote ident (addr/mask/prot/port): (10.1.1.2/255.255.255.255/

#### **17/1701**

)

**current\_peer: 10.1.1.2, username: test**

**dynamic allocated peer ip: 192.168.1.1**

dynamic allocated peer ip(ipv6): 0.0.0.0

**#pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29**

**#pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118**

#pkts compressed: 0, #pkts decompressed: 0  
#pkts not compressed: 29, #pkts comp failed: 0, #pkts decomp failed: 0  
#post-frag successes: 0, #post-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.: 172.16.1.2/0, remote crypto endpt.: 10.1.1.2/0
path mtu 1500, ipsec overhead 58(36), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: E8AF927A
current inbound spi : 71F346AB
```

```
inbound esp sas:
spi: 0x71F346AB (1911768747)
  transform: esp-3des esp-sha-hmac no compression
  in use settings = {RA, Transport, IKEv1, }
  slot: 0, conn_id: 4096, crypto-map: outside_dyn_map
  sa timing: remaining key lifetime (kB/sec): (237303/3541)
  IV size: 8 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000003
```

```
outbound esp sas:
spi: 0xE8AF927A (3903820410)
  transform: esp-3des esp-sha-hmac no compression
  in use settings = {RA, Transport, IKEv1, }
  slot: 0, conn_id: 4096, crypto-map: outside_dyn_map
  sa timing: remaining key lifetime (kB/sec): (237303/3541)
  IV size: 8 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001
```

- show vpn-sessiondb detail ra-ikev1-ipsec filter protocol l2tpOverIpSec - Mostra informações detalhadas sobre conexões L2TP sobre IPsec.

```
ciscoasa# show vpn-sessiondb detail ra-ikev1-ipsec filter protocol l2tpOverIpSec
```

```
Session Type: IKEv1 IPsec Detailed
```

**Username : test**

Index : 1

**Assigned IP : 192.168.1.1                      Public IP : 10.1.1.2**

```
Protocol : IKEv1 IPsec L2TPOverIPsec
License : Other VPN
Encryption : IKEv1: (1)3DES IPsec: (1)3DES L2TPOverIPsec: (1)none
Hashing : IKEv1: (1)SHA1 IPsec: (1)SHA1 L2TPOverIPsec: (1)none
Bytes Tx : 1574 Bytes Rx : 12752
Pkts Tx : 29 Pkts Rx : 118
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

**Group Policy : L2TP-VPN                      Tunnel Group : DefaultRAGroup**

Login Time : 23:32:48 UTC Sat May 16 2015

Duration : 0h:04m:05s  
Inactivity : 0h:00m:00s  
VLAN Mapping : N/A VLAN : none  
Audt Sess ID : 0a6a2577000010005557d3a0  
Security Grp : none

IKEv1 Tunnels: 1  
IPsec Tunnels: 1  
L2TPOverIPsec Tunnels: 1

**IKEv1:**

Tunnel ID : 1.1  
UDP Src Port : 500 UDP Dst Port : 500  
IKE Neg Mode : Main Auth Mode : preSharedKeys  
Encryption : 3DES Hashing : SHA1  
Rekey Int (T): 28800 Seconds Rekey Left(T): 28555 Seconds  
D/H Group : 2  
Filter Name :

**IPsec:**

Tunnel ID : 1.2  
Local Addr : 172.16.1.2/255.255.255.255/17/1701  
Remote Addr : 10.1.1.2/255.255.255.255/17/1701  
Encryption : 3DES Hashing : SHA1  
Encapsulation: Transport  
Rekey Int (T): 3600 Seconds Rekey Left(T): 3576 Seconds  
Rekey Int (D): 250000 K-Bytes Rekey Left(D): 250000 K-Bytes  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
Bytes Tx : 1574 Bytes Rx : 12752  
Pkts Tx : 29 Pkts Rx : 118

**L2TPOverIPsec:**

Tunnel ID : 1.3

**Username : test**

**Assigned IP : 192.168.1.1**

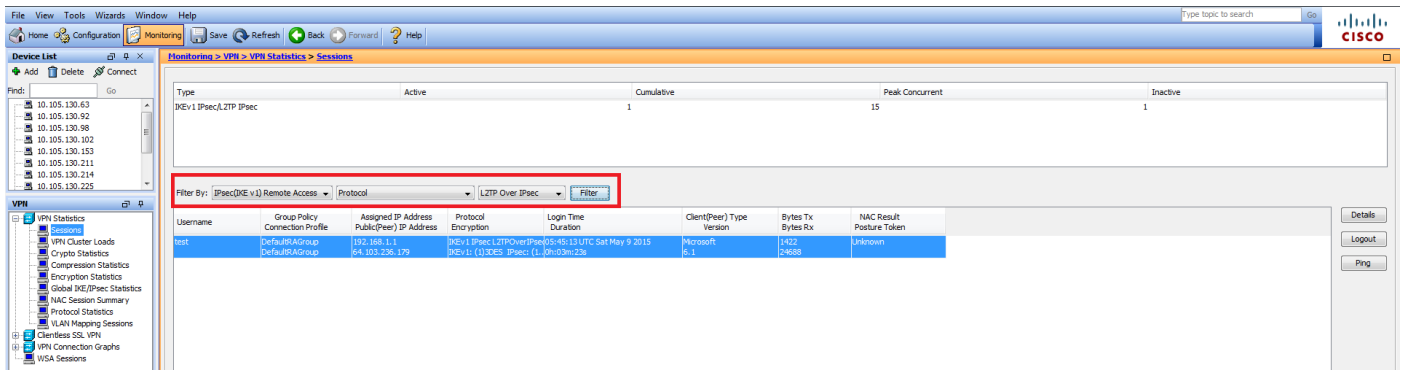
**Public IP : 10.1.1.2**

Encryption : none Hashing : none

**Auth Mode : msCHAPV2**

Idle Time Out: 30 Minutes                      Idle TO Left : 27 Minutes  
Client OS : Microsoft  
Client OS Ver: 6.2  
Bytes Tx : 475                                      Bytes Rx : 9093  
Pkts Tx : 18                                        Pkts Rx : 105

No ASDM, em **Monitoring > VPN > VPN Statistics > Sessions**, as informações gerais sobre a sessão VPN podem ser vistas. As sessões L2TP sobre IPsec podem ser filtradas por **acesso remoto IPsec (IKEv1) > Protocolo > L2TP sobre IPsec**.



## Troubleshoot

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

**Note:** Consulte [Informações Importantes sobre Comandos de Depuração antes de usar comandos debug](#).

**Caution:** No ASA, você pode definir vários níveis de depuração; por padrão, o nível 1 é usado. Se você alterar o nível de depuração, a verbosidade das depurações pode aumentar. Faça isso com cuidado, especialmente em ambientes de produção!

Use os seguintes **comandos debug com cuidado** para solucionar problemas com o túnel VPN

- **debug crypto ikev1** - exibe informações de depuração sobre IKE
- **debug crypto ipsec** - exibe informações de depuração sobre IPsec

Esta é a saída de depuração para uma conexão L2TP sobre IPsec bem-sucedida:

```
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NONE (0) total length : 408
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing SA payload
May 18 04:17:18 [IKEv1]Phase 1 failure: Mismatched attribute types for class Group
Description: Rcv'd: Unknown Cfg'd: Group 2
May 18 04:17:18 [IKEv1]Phase 1 failure: Mismatched attribute types for class Group
Description: Rcv'd: Unknown Cfg'd: Group 2
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Oakley proposal is acceptable
```

May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal RFC VID  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal ver 02 VID  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received Fragmentation VID  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing IKE SA payload  
May 18 04:17:18 [IKEv1]Phase 1 failure: Mismatched attribute types for class Group  
Description: Rcv'd: Unknown Cfg'd: Group 2  
May 18 04:17:18 [IKEv1]Phase 1 failure: Mismatched attribute types for class Group  
Description: Rcv'd: Unknown Cfg'd: Group 2  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2,

### **IKE SA Proposal # 1, Transform # 5 acceptable Matches global IKE entry # 2**

May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ISAKMP SA payload  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Traversal VID ver RFC payload  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Fragmentation VID + extended capabilities payload  
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE\_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 124  
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500  
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE\_DECODE RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 260  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ke payload  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ISA\_KE payload  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing nonce payload  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ke payload  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing nonce payload  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Cisco Unity VID payload  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing xauth V6 VID payload  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send IOS VID  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Constructing ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing VID payload  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload  
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash  
May 18 04:17:18 [IKEv1]IP = 10.1.1.2,

### **Connection landed on tunnel\_group DefaultRAGroup**

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating keys for Responder...  
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, 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  
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500  
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE\_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + NONE (0) total length : 64

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload  
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID\_IPV4\_ADDR ID received 10.1.1.2  
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload  
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP  
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

**Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device**

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Connection landed on tunnel\_group DefaultRAGroup  
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing ID payload  
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing hash payload  
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP  
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing dpd vid payload  
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE\_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total length : 84  
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

#### **PHASE 1 COMPLETED**

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alive type for this connection: None  
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alives configured on but peer does not support keep-alives (type = None)  
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P1 rekey timer: 21600 seconds.  
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500  
May 18 04:17:18 [IKEv1 DECODE]IP = 10.1.1.2, IKE Responder starting QM: msg id = 00000001  
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE\_DECODE RECEIVED Message (msgid=1) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 300  
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload  
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing SA payload  
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing nonce payload  
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload  
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID\_IPV4\_ADDR ID received 10.1.1.2  
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

**Received remote Proxy Host data in ID Payload: Address 10.1.1.2, Protocol 17, Port 1701**

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload  
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID\_IPV4\_ADDR ID received 172.16.1.2  
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

**Received local Proxy Host data in ID Payload: Address 172.16.1.2, Protocol 17, Port 1701**

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

**L2TP/IPSec session detected.**

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, QM IsRekeyed old sa not found by addr  
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

**Static Crypto Map check, map outside\_dyn\_map, seq = 10 is a successful match**



May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Remote Peer configured for crypto map: outside\_dyn\_map  
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing IPsec SA payload  
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, I

**IPsec SA Proposal # 2, Transform # 1 acceptable**

Matches global IPsec SA entry # 10

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE: requesting SPI!

IPSEC: New embryonic SA created @ 0x00007ffff13ab260,

SCB: 0xE1C00540,

Direction: inbound

SPI : 0x7AD72E0D

Session ID: 0x00001000

VPIF num : 0x00000002

Tunnel type: ra

Protocol : esp

Lifetime : 240 seconds

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got SPI from key engine: SPI = 0x7ad72e0d

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, oakley constructing quick mode

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing blank hash payload

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPsec SA payload

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPsec nonce payload

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing proxy ID

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2,

**Transmitting Proxy Id:**

**Remote host: 10.1.1.2 Protocol 17 Port 1701**

**Local host: 172.16.1.2 Protocol 17 Port 1701**

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing qm hash payload

May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Responder sending 2nd QM pkt: msg id = 00000001

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE\_DECODE SENDING Message (msgid=1) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 160

May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE\_DECODE RECEIVED Message (msgid=1) with payloads : HDR + HASH (8) + NONE (0) total length : 52

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, loading all IPSEC SAs

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key!

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for crypto map outside\_dyn\_map 10 matching ACL Unknown: returned cs\_id=e148a8b0;

encrypt\_rule=00000000; tunnelFlow\_rule=00000000

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key!

IPSEC: New embryonic SA created @ 0x00007ffffelc75c00,  
SCB: 0xE13ABD20,  
Direction: outbound  
SPI : 0x8C14FD70  
Session ID: 0x00001000  
VPIF num : 0x00000002  
Tunnel type: ra  
Protocol : esp  
Lifetime : 240 seconds

IPSEC: Completed host OBSA update, SPI 0x8C14FD70

IPSEC: Creating outbound VPN context, SPI 0x8C14FD70

Flags: 0x00000205  
SA : 0x00007ffffelc75c00  
SPI : 0x8C14FD70  
MTU : 1500 bytes  
VCID : 0x00000000  
Peer : 0x00000000  
SCB : 0x0AC609F9  
Channel: 0x00007ffffed817200

IPSEC: Completed outbound VPN context, SPI 0x8C14FD70

VPN handle: 0x000000000000028d4

IPSEC: New outbound encrypt rule, SPI 0x8C14FD70

Src addr: 172.16.1.2  
Src mask: 255.255.255.255  
Dst addr: 10.1.1.2  
Dst mask: 255.255.255.255

#### **Src ports**

**Upper: 1701**

**Lower: 1701**

Op : equal

#### **Dst ports**

**Upper: 1701**

**Lower: 1701**

Op : equal

**Protocol: 17**

```
Use protocol: true
SPI: 0x00000000
Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x8C14FD70
  Rule ID: 0x00007ffffe1c763d0
IPSEC: New outbound permit rule, SPI 0x8C14FD70
  Src addr: 172.16.1.2
  Src mask: 255.255.255.255
  Dst addr: 10.1.1.2
  Dst mask: 255.255.255.255
  Src ports
    Upper: 0
    Lower: 0
    Op   : ignore
  Dst ports
    Upper: 0
    Lower: 0
    Op   : ignore
  Protocol: 50
  Use protocol: true
  SPI: 0x8C14FD70
  Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x8C14FD70
  Rule ID: 0x00007ffffe1c76a00
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for
crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0;
encrypt_rule=00000000; tunnelFlow_rule=00000000
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, Security negotiation complete for
User () Responder, Inbound SPI = 0x7ad72e0d, Outbound SPI = 0x8c14fd70
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got a KEY_ADD msg for
SA: SPI = 0x8c14fd70
IPSEC: New embryonic SA created @ 0x00007ffffe13ab260,
  SCB: 0xE1C00540,
  Direction: inbound
  SPI       : 0x7AD72E0D
  Session ID: 0x00001000
  VPIF num  : 0x00000002
  Tunnel type: ra
  Protocol   : esp
  Lifetime   : 240 seconds
IPSEC: Completed host IBSA update, SPI 0x7AD72E0D
IPSEC: Creating inbound VPN context, SPI 0x7AD72E0D
  Flags: 0x00000206
  SA   : 0x00007ffffe13ab260
  SPI  : 0x7AD72E0D
  MTU  : 0 bytes
  VCID : 0x00000000
  Peer : 0x000028D4
  SCB  : 0x0AC5BD5B
  Channel: 0x00007ffffe817200
IPSEC: Completed inbound VPN context, SPI 0x7AD72E0D
  VPN handle: 0x0000000000004174
IPSEC: Updating outbound VPN context 0x000028D4, SPI 0x8C14FD70
  Flags: 0x00000205
  SA   : 0x00007ffffe1c75c00
  SPI  : 0x8C14FD70
  MTU  : 1500 bytes
  VCID : 0x00000000
  Peer : 0x00004174
  SCB  : 0x0AC609F9
```

Channel: 0x00007ffffed817200  
IPSEC: Completed outbound VPN context, SPI 0x8C14FD70  
VPN handle: 0x00000000000028d4  
IPSEC: Completed outbound inner rule, SPI 0x8C14FD70  
Rule ID: 0x00007ffffelc763d0  
IPSEC: Completed outbound outer SPD rule, SPI 0x8C14FD70  
Rule ID: 0x00007ffffelc76a00  
IPSEC: New inbound tunnel flow rule, SPI 0x7AD72E0D  
Src addr: 10.1.1.2  
Src mask: 255.255.255.255  
Dst addr: 172.16.1.2  
Dst mask: 255.255.255.255  
Src ports  
Upper: 1701  
Lower: 1701  
Op : equal  
Dst ports  
Upper: 1701  
Lower: 1701  
Op : equal  
Protocol: 17  
Use protocol: true  
SPI: 0x00000000  
Use SPI: false  
IPSEC: Completed inbound tunnel flow rule, SPI 0x7AD72E0D  
Rule ID: 0x00007ffffel3aba90  
IPSEC: New inbound decrypt rule, SPI 0x7AD72E0D  
Src addr: 10.1.1.2  
Src mask: 255.255.255.255  
Dst addr: 172.16.1.2  
Dst mask: 255.255.255.255  
Src ports  
Upper: 0  
Lower: 0  
Op : ignore  
Dst ports  
Upper: 0  
Lower: 0  
Op : ignore  
Protocol: 50  
Use protocol: true  
SPI: 0x7AD72E0D  
Use SPI: true  
IPSEC: Completed inbound decrypt rule, SPI 0x7AD72E0D  
Rule ID: 0x00007ffffelc77420  
IPSEC: New inbound permit rule, SPI 0x7AD72E0D  
Src addr: 10.1.1.2  
Src mask: 255.255.255.255  
Dst addr: 172.16.1.2  
Dst mask: 255.255.255.255  
Src ports  
Upper: 0  
Lower: 0  
Op : ignore  
Dst ports  
Upper: 0  
Lower: 0  
Op : ignore  
Protocol: 50  
Use protocol: true  
SPI: 0x7AD72E0D  
Use SPI: true  
IPSEC: Completed inbound permit rule, SPI 0x7AD72E0D  
Rule ID: 0x00007ffffel3abb80

```
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Pitcher: received  
KEY_UPDATE, spi 0x7ad72e0d  
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P2 rekey timer:  
3420 seconds.  
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,
```

## PHASE 2 COMPLETED

```
(msgid=00000001)  
May 18 04:17:18 [IKEv1]IKEQM_Active() Add L2TP classification rules: ip <10.1.1.2> mask  
<0xFFFFFFFF> port <1701>  
May 18 04:17:21 [IKEv1]Group = DefaultRAGroup,
```

**Username = test, IP = 10.1.1.2, Adding static route for client address: 192.168.1.1**

Alguns dos erros comumente vistos relacionados à VPN no cliente Windows são mostrados nesta tabela

Código de erro	Solução possível
691	Verifique se o nome de usuário e a senha inseridos estão corretos
789,835	Certifique-se de que a chave pré-compartilhada configurada na máquina cliente seja a mesma no ASA
800	1. Verifique se o tipo de VPN está definido como "Layer 2 Tunneling Protocol (L2TP)" 2. Verifique se a chave pré-compartilhada foi configurada corretamente
809	Certifique-se de que a porta UDP 500, 4500 (caso o cliente ou o servidor esteja por trás do dispositivo NAT) e que o tráfego ESP não foi bloqueado

## Informações Relacionadas

- [Dispositivos de segurança adaptáveis Cisco ASA 5500 Series](#)
- [Soluções de problemas mais comuns para VPN IPsec de acesso remoto e L2L](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)