

EzVPN com o NEM no IOS Router com exemplo de configuração do VPN 3000 concentrator

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar o VPN 3000 Concentrator](#)

[Tarefa](#)

[Diagrama de Rede](#)

[Instruções passo a passo](#)

[Configuração do roteador](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Saída dos comandos Debug](#)

[Comandos cisco ios show relacionados para pesquisar defeitos](#)

[Debug de VPN 3000 Concentrator](#)

[que pode dar errado](#)

[Informações Relacionadas](#)

Introdução

Este documento explica o procedimento que você deve utilizar para configurar um roteador Cisco IOS® como um EzVPN no [Network Extension Mode \(NEM\)](#) para se conectar a um Cisco VPN 3000 Concentrator. Uma característica nova da fase II do EzVPN é o apoio de uma configuração da tradução de endereços da rede básica (NAT). A fase II do EzVPN é derivada do protocolo de Unity (software do cliente VPN). O dispositivo remoto é sempre o iniciador do túnel de IPsec. Contudo, as propostas do Internet Key Exchange (IKE) e do IPsec não são configuráveis no cliente ezvpn. O cliente VPN negocia propostas com o server.

Para configurar o IPsec entre um PIX/ASA 7.x e um roteador Cisco 871 utilizando o Easy VPN, consulte [Exemplo de Configuração Remota de um PIX/ASA 7.x Easy VPN com um ASA 5500 como Servidor e um Cisco 871 como o Easy VPN](#).

Para configurar o IPsec entre o Cisco IOS® Easy VPN Remote Hardware Client e o PIX Easy VPN Server, consulte [Exemplo de Configuração de um IOS Easy VPN Remote Hardware Client para um PIX Easy VPN Server](#).

Para configurar um Cisco 7200 Router como um EzVPN e o Cisco 871 Router como o Easy VPN

Remote, consulte [Exemplo de Configuração Remota de um 7200 Easy VPN Server para 871 Easy VPN](#).

Pré-requisitos

Requisitos

Antes de tentar esta configuração, verifique se o roteador Cisco IOS oferece suporte ao [recurso EzVPN Fase II](#) e possui conectividade IP fim a fim para estabelecer o túnel IPsec.

Componentes Utilizados

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

- Cisco IOS Software Release 12.2(8)YJ (fase II do EzVPN)
- VPN 3000 concentrator 3.6.x
- Cisco 1700 Router

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Note: Esta configuração foi testada recentemente com um Cisco 3640 Router com Cisco IOS Software Release 12.4(8) e a versão do VPN 3000 concentrator 4.7.x.

Convenções

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

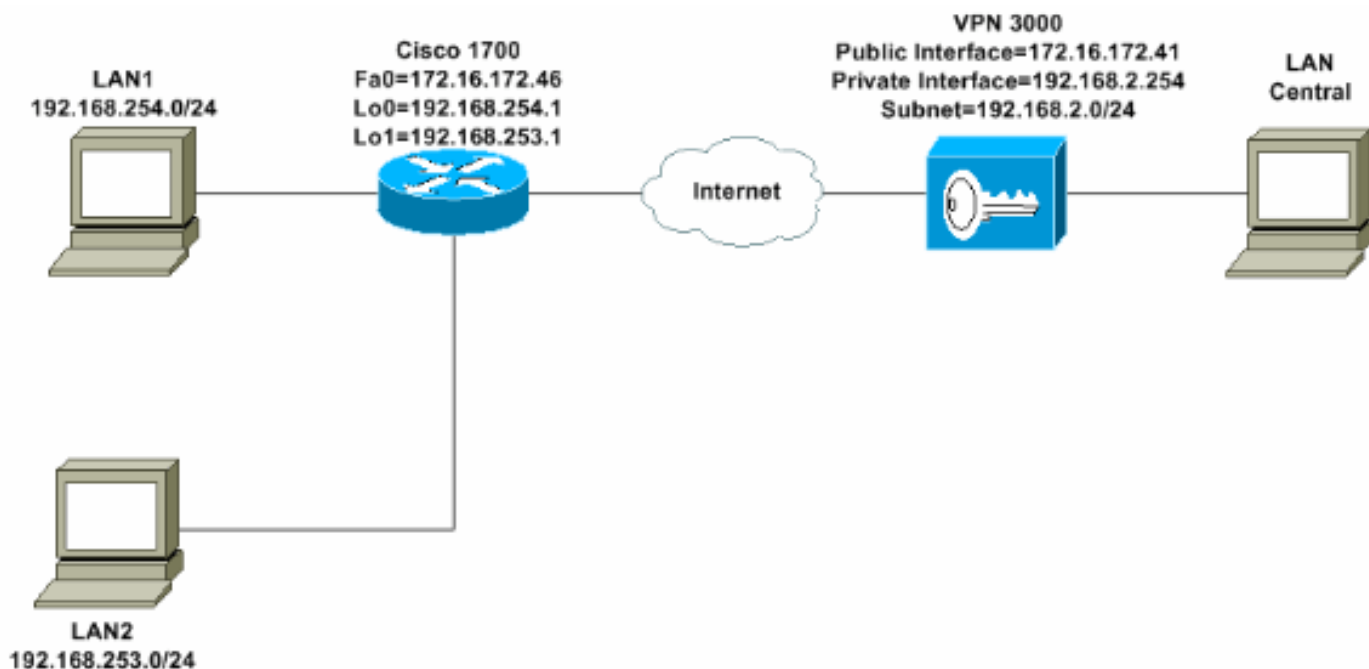
Configurar o VPN 3000 Concentrator

Tarefa

Nesta seção, você é apresentado com a informação para configurar o VPN 3000 concentrator.

Diagrama de Rede

Este documento utiliza a configuração de rede mostrada neste diagrama. As interfaces de loopback são usadas como sub-redes internas, e o FastEthernet 0 é o padrão ao Internet.



[Instruções passo a passo](#)

Conclua estes passos:

1. Selecione **Configuration > User Management > Groups > Add** e defina um nome e uma senha de grupo para configurar um grupo de IPsec para os usuários. Este exemplo usa o nome de grupo **turaro** com senha/verificação **tululo**.

The screenshot shows the Cisco configuration interface. On the left is a navigation tree with the following items: Configuration, Interfaces, System, User Management (Base Group, Groups, Users), Policy Management, Administration, and Monitoring. The main area displays the 'Configuration | User Management | Groups | Add' dialog. The dialog contains the following text: 'This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.' Below this text are several tabs: Identity, General, IPsec, Client Config, Client FW, HW Client, and PPTP/L2TP. The 'Identity Parameters' table is shown with the following data:

Attribute	Value	Description
Group Name	turaro	Enter a unique name for the group.
Password	*****	Enter the password for the group.
Verify	*****	Verify the group's password.
Type	Internal	<i>External groups</i> are configured on an external authentication server (e.g. RADIUS). <i>Internal groups</i> are configured on the VPN 3000 Concentrator's Internal Database.

At the bottom of the dialog are 'Add' and 'Cancel' buttons. The Cisco Systems logo is visible in the bottom left corner of the interface.

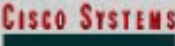
2. Selecione **Configuration > User Management > Groups > turaro > General** para habilitar o IPsec e desabilitar o Point-to-Point Tunneling Protocol (PPTP) e o Layer 2 Tunnel Protocol (L2TP). Faça suas seleções e clique em **Apply**.

- [-] Configuration
 - Interfaces
 - [-] System
 - [-] User Management
 - Base Group
 - Groups
 - Users
 - [-] Policy Management
- [-] Administration
- [-] Monitoring

Identity
General
IPSec
Client FW
PPTP/L2TP

General Par

Attribute	Value	Inherit?	
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Sele
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Ente
Minimum Password Length	8	<input checked="" type="checkbox"/>	Ente
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Ente be a
Idle Timeout	30	<input checked="" type="checkbox"/>	(min
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(min
Filter	-None-	<input checked="" type="checkbox"/>	Ente
Primary DNS		<input checked="" type="checkbox"/>	Ente
Secondary DNS		<input checked="" type="checkbox"/>	Ente
Primary WINS		<input checked="" type="checkbox"/>	Ente
Secondary WINS		<input checked="" type="checkbox"/>	Ente
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	<input checked="" type="checkbox"/>	Sele
Tunneling Protocols	<input type="checkbox"/> PPTP <input type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPSec	<input type="checkbox"/>	Sele



3. Defina Authentication como **Internal** para Extended Authentication (Xauth) e certifique-se de que Tunnel Type seja **Remote Access** e IPSec SA seja **ESP-3DES-MD5**.

Configuration | User Management | Groups | Modify ADMINI

Check the **Inherit?** box to set a field that you want to default to the base group value to override base group values.

Identity General **IPSec** Client FW PPTP/L2TP

IPSec Parameters

Attribute	Value	Inherit?
IPSec SA	ESP-3DES-MD5	<input checked="" type="checkbox"/>
IKE Peer Identity Validation	If supported by certificate	<input checked="" type="checkbox"/>
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Reauthentication on Rekey	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Tunnel Type	Remote Access	<input checked="" type="checkbox"/>

Remote Access Parameters

Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Authentication	Internal	<input checked="" type="checkbox"/>

4. Selecione **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals** para se certificar de que o Cisco VPN Client (CiscoVPNClient-3DES-MD5) esteja em Active Proposals for IKE (Fase 1). **Note:** Do concentrador VPN 4.1.x, o procedimento é diferente para assegurar-se de que o Cisco VPN Client esteja na lista de propósitos ativo para IKE (fase 1). Selecione **Configuration > Tunneling and Security > IPSec > IKE Proposals**.

Configuration | System | Tunneling Protocols | IPSec | IKE Proposals

Add, delete, prioritize, and configure IKE Proposals.

Select an **Inactive Proposal** and click **Activate** to make it **Active**, or click **Modify**, **Copy** or **Delete**. Select an **Active Proposal** and click **Deactivate** to make it **Inactive**, or click **Move Up** or **Move Down**. Click **Add** or **Copy** to add a new **Inactive Proposal**. IKE Proposals are used by **Security Associations** parameters.

Active Proposals	Actions	Inactive Proposals
CiscoVPNClient-3DES-MD5 IKE-3DES-MD5 IKE-3DES-MD5-DH1 IKE-DES-MD5 IKE-3DES-MD5-DH7	<< Activate Deactivate >> Move Up Move Down Add	IKE-3DES-MD5-RSA IKE-3DES-SHA-DSA IKE-3DES-MD5-RSA-D IKE-DES-MD5-DH7 CiscoVPNClient-3DES CiscoVPNClient-3DES

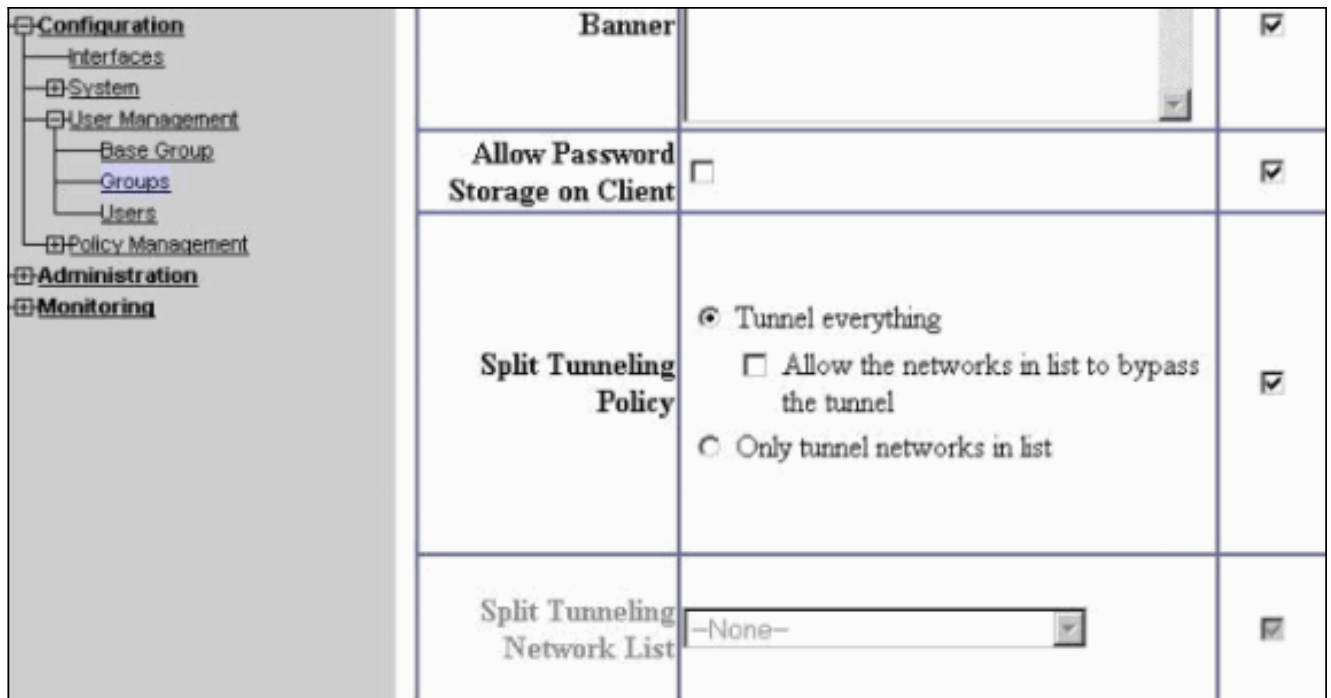
5. Verifique sua associação de segurança IPsec (SA). No passo 3, sua IPsec SA é ESP-3DES-MD5. Você pode criar uma nova se desejar, mas certifique-se de utilizar a IPsec SA correta no seu grupo. Você deve desabilitar o discrição perfeita adiante (PFS) para IPsec SA que você usa. Selecione o Cisco VPN Client como a proposta para o IKE ao escolher **Configuration > Policy Management > Traffic Management > SAs**. Datilografe o nome SA na

caixa de texto e faça as seleções apropriadas como mostrado aqui:

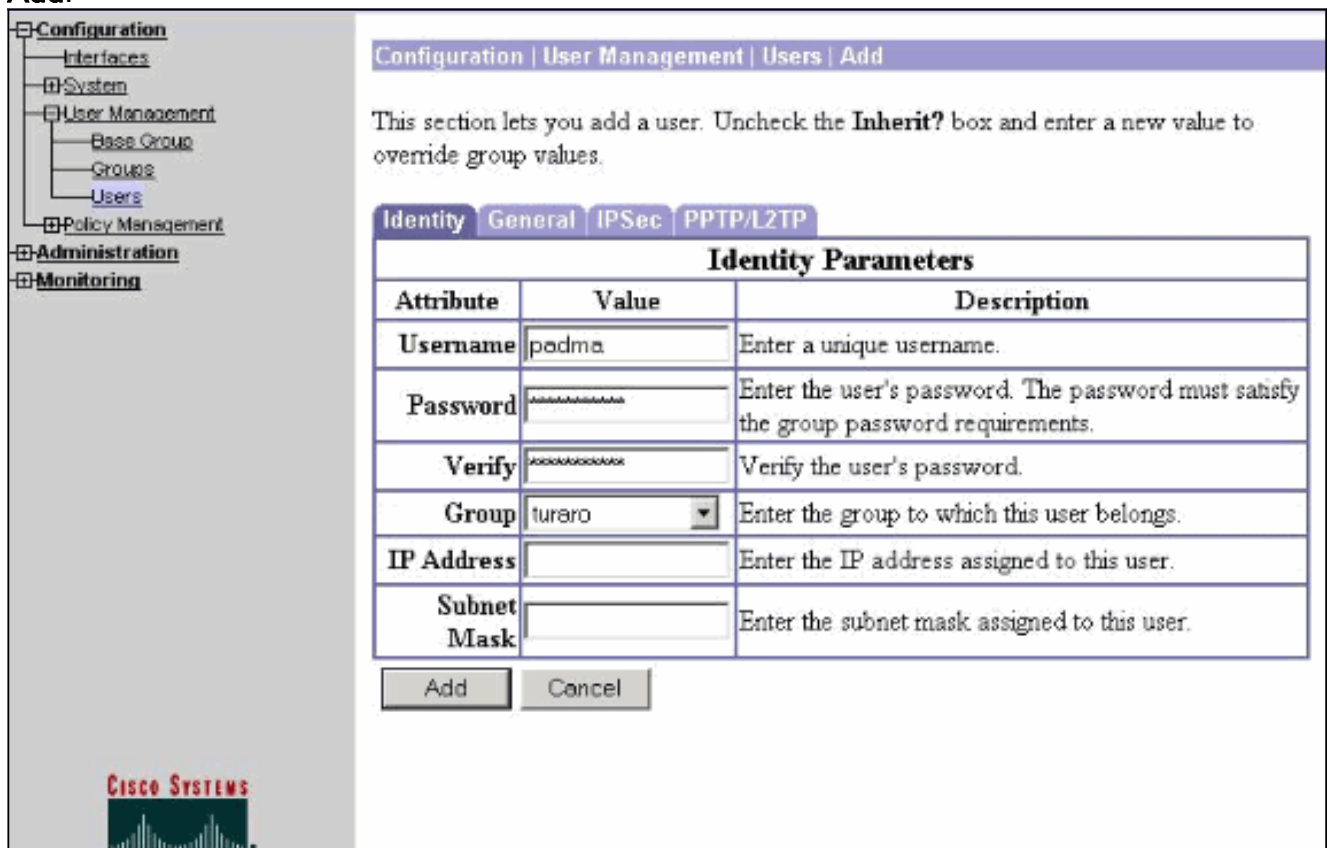
Configuration Policy Management Traffic Management Security Associations Modify		
Modify a configured Security Association.		
SA Name	<input type="text" value="ESP-3DES-MD5"/>	Specify the name of this Security Association (S
Inheritance	<input type="text" value="From Rule"/>	Select the granularity of this SA.
IPSec Parameters		
Authentication Algorithm	<input type="text" value="ESP/MD5/HMAC-128"/>	Select the packet authentication algorithm to use
Encryption Algorithm	<input type="text" value="3DES-168"/>	Select the ESP encryption algorithm to use.
Encapsulation Mode	<input type="text" value="Tunnel"/>	Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy	<input type="text" value="Disabled"/>	Select the use of Perfect Forward Secrecy.
Lifetime Measurement	<input type="text" value="Time"/>	Select the lifetime measurement of the IPSec ke
Data Lifetime	<input type="text" value="10000"/>	Specify the data lifetime in kilobytes (KB).
Time Lifetime	<input type="text" value="28800"/>	Specify the time lifetime in seconds.
IKE Parameters		
IKE Peer	<input type="text" value="0.0.0.0"/>	Specify the IKE Peer for a LAN-to-LAN IPSec
Negotiation Mode	<input type="text" value="Aggressive"/>	Select the IKE Negotiation mode to use.
Digital Certificate	<input type="text" value="None (Use Preshared Keys)"/>	Select the Digital Certificate to use.
Certificate Transmission	<input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only	Choose how to send the digital certificate to the
IKE Proposal	<input type="text" value="CiscoVPNClient-3DES-MD5"/>	Select the IKE Proposal to use as IKE initiator.

Note: Esta etapa e a próxima etapa são opcionais se você prefere escolher um SA predefinido. Se seu cliente tem dinamicamente um endereço IP atribuído, use 0.0.0.0 na caixa de texto do par IKE. Certifique-se de que a IKE Proposal esteja configurada como **CiscoVPNClient-3DES-MD5** conforme mostrado neste exemplo.

6. Você não deve clicar em *Allow the networks in the list to bypass the tunnel*. A razão é que o Split Tunneling está apoiado, mas a característica do desvio não é apoiada com os recursos de cliente ezvpn.



7. Selecione **Configuration > User Management > Users** para adicionar um usuário. Defina um nome de usuário e a senha, atribua a um grupo e clique em **Add**.



8. Selecione **Administration > Admin Sessions** e verifique se o usuário está conectado. No NEM, o concentrador VPN não atribui um endereço IP de Um ou Mais Servidores Cisco ICM NT do pool. **Note:** Esta etapa é opcional se você prefere escolher um SA predefinido.

LAN-to-LAN Sessions				[Remote Access Sessions Management Sessions]				
Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx	Actions
No LAN-to-LAN Sessions								
Remote Access Sessions				[LAN-to-LAN Sessions Management Sessions]				
Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	Actions	
Cisco_MAE	192.168.253.0 172.16.172.46	turaro	IPSec 3DES-168	Mar 31 18:32:23 0:02:50	N/A N/A	301320 301320	[Logout Ping]	
Management Sessions				[LAN-to-LAN Sessions Remote Access Sessions]				
Administrator	IP Address	Protocol	Encryption	Login Time	Duration	Actions		
adman	171.69.89.5	HTTP	None	Mar 31 18:35:01	0:00:12	[Logout Ping]		

9. Clique nos ícones **Save Needed** ou **Save** para salvar a configuração.

Configuração do roteador

mostre saídas de versão

show version

```
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-BK9NO3R2SY7-M), Version 12.2(8)YJ,
EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
```

```
1721-1(ADSL) uptime is 4 days, 5 hours, 33 minutes
System returned to ROM by reload
System image file is "flash:c1700-bk9no3r2sy7-mz.122-8.YJ.bin"
cisco 1721 (MPC860P) processor (revision 0x100) with 88474K/9830K bytes
16384K bytes of processor board System flash (Read/Write)
```

1721-1

```
1721-1(ADSL)#show run
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1721-1(ADSL)
!
!--- Specify the configuration name !--- to be assigned
to the interface. crypto ipsec client ezvpn SJVPN
!--- Tunnel control; automatic is the default. connect
auto
!--- The group name and password should be the same as
given in the VPN Concentrator. group turaro key tululo
!--- The mode that is chosen as the network extension.
mode network-extension
!--- The tunnel peer end (VPN Concentrator public
interface IP address). peer 172.16.172.41
!
interface Loopback0
 ip address 192.168.254.1 255.255.255.0
!--- Configure the Loopback interface !--- as the inside
interface. ip nat inside
!--- Specifies the Cisco EzVPN Remote configuration name
!--- to be assigned to the inside interface.
```



```

crypto ipsec client ezvpn SJVPN inside
!
interface Loopback1
 ip address 192.168.253.1 255.255.255.0
 ip nat inside
 crypto ipsec client ezvpn SJVPN inside
!
interface FastEthernet0
 ip address 172.16.172.46 255.255.255.240
 !--- Configure the FastEthernet interface !--- as the
 outside interface. ip nat outside
 !--- Specifies the Cisco EzVPN Remote configuration name
 !--- to be assigned to the first outside interface,
 because !--- outside is not specified for the interface.
 !--- The default is outside.

 crypto ipsec client ezvpn SJVPN
!
 !--- Specify the overload option with the ip nat command
 !--- in global configuration mode in order to enable !--
 - Network Address Translation (NAT) of the inside source
 address !--- so that multiple PCs can use the single IP
 address.

 ip nat inside source route-map EZVPN interface
 FastEthernet0 overload
 ip classless
 ip route 0.0.0.0 0.0.0.0 172.16.172.41
!
 access-list 177 deny ip 192.168.254.0 0.0.0.255
 192.168.2.0 0.0.0.255
 access-list 177 deny ip 192.168.253.0 0.0.0.255
 192.168.2.0 0.0.0.255
 access-list 177 permit ip 192.168.253.0 0.0.0.255 any
 access-list 177 permit ip 192.168.254.0 0.0.0.255 any
!
 route-map EZVPN permit 10
  match ip address 177
!
!
 line con 0
 line aux 0
 line vty 0 4
  password cisco
  login
!
 no scheduler allocate
end

```

Verificar

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

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Uma vez que você configura ambos os dispositivos, o Cisco 3640 Router tenta estabelecer o túnel VPN contactando o concentrador VPN que usa automaticamente o endereço IP do peer. Depois que os parâmetros ISAKMP iniciais são trocados, o roteador indica esta mensagem:

Pending XAuth Request, Please enter the following command: **crypto ipsec client ezvpn xauth**

É necessário inserir o comando **crypto ipsec client ezvpn xauth**, o qual solicitará um nome de usuário e uma senha. Isto deve combinar o nome de usuário e senha configurado no concentrador VPN (etapa 7). Uma vez que o nome de usuário e senha é concordado por ambos os pares, o resto dos parâmetros está concordado e o túnel do IPsec VPN vem acima.

EZVPN(SJVPN): Pending XAuth Request, Please enter the following command:

EZVPN: crypto ipsec client ezvpn xauth

!--- Enter the crypto ipsec client ezvpn xauth command.

crypto ipsec client ezvpn xauth

Enter Username and Password.: **padma**

Password: : **password**

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos para Troubleshooting

A [Output Interpreter Tool \(somente clientes registrados\)](#) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

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

- **debug crypto ipsec client ezvpn** — Exibe informações que mostram a configuração e a implementação do recurso EzVPN Client.
- **debug crypto ipsec** — Exibe informações de depuração sobre conexões de IPsec.
- **debug crypto isakmp** — Exibe informações de depuração sobre conexões de IPsec e mostra o primeiro conjunto de atributos negados devido a incompatibilidades em ambas as extremidades.
- **show debug** — Exibe o estado de cada opção de depuração.

Saída dos comandos Debug

Assim que você inscrever o comando **crypto ipsec client ezvpn SJVPN**, o cliente ezvpn tenta conectar ao server. Se você alterar o comando **connect manual** na configuração de grupo, insira o comando **crypto ipsec client ezvpn connect SJVPN** para iniciar a troca de propostas com o servidor.

4d05h: ISAKMP (0:3): beginning Aggressive Mode exchange
4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) AG_INIT_EXCH
4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) AG_INIT_EXCH
4d05h: ISAKMP (0:3): processing SA payload. message ID = 0
4d05h: ISAKMP (0:3): processing ID payload. message ID = 0
4d05h: ISAKMP (0:3): processing vendor id payload
4d05h: ISAKMP (0:3): vendor ID is Unity
4d05h: ISAKMP (0:3): processing vendor id payload
4d05h: ISAKMP (0:3): vendor ID seems Unity/DPD but bad major
4d05h: ISAKMP (0:3): vendor ID is XAUTH
4d05h: ISAKMP (0:3): processing vendor id payload
4d05h: ISAKMP (0:3): vendor ID is DPD
4d05h: ISAKMP (0:3) local preshared key found
4d05h: ISAKMP (0:3) Authentication by xauth preshared
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65527 policy
4d05h: ISAKMP: encryption 3DES-CBC
4d05h: ISAKMP: hash MD5
4d05h: ISAKMP: default group 2
4d05h: ISAKMP: auth XAUTHInitPreShared
4d05h: ISAKMP: life type in seconds
4d05h: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): Encryption algorithm offered does not match policy!
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65528 policy
4d05h: ISAKMP: encryption 3DES-CBC
4d05h: ISAKMP: hash MD5
4d05h: ISAKMP: default group 2
4d05h: ISAKMP: auth XAUTHInitPreShared
4d05h: ISAKMP: life type in seconds
4d05h: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): Encryption algorithm offered does not match policy!
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65529 policy
4d05h: ISAKMP: encryption 3DES-CBC
4d05h: ISAKMP: hash MD5
4d05h: ISAKMP: default group 2
4d05h: ISAKMP: auth XAUTHInitPreShared
4d05h: ISAKMP: life type in seconds
4d05h: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): Encryption algorithm offered does not match policy!
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65530 policy
4d05h: ISAKMP: encryption 3DES-CBC
4d05h: ISAKMP: hash MD5
4d05h: ISAKMP: default group 2
4d05h: ISAKMP: auth XAUTHInitPreShared
4d05h: ISAKMP: life type in seconds
4d05h: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): Encryption algorithm offered does not match policy!
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65531 policy
4d05h: ISAKMP: encryption 3DES-CBC
4d05h: ISAKMP: hash MD5
4d05h: ISAKMP: default group 2
4d05h: ISAKMP: auth XAUTHInitPreShared
4d05h: ISAKMP: life type in seconds
4d05h: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): Hash algorithm offered does not match policy!
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65532 policy
4d05h: ISAKMP: encryption 3DES-CBC
4d05h: ISAKMP: hash MD5
4d05h: ISAKMP: default group 2
4d05h: ISAKMP: auth XAUTHInitPreShared

4d05h: ISAKMP: life type in seconds
4d05h: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): **atts are acceptable.** Next payload is 0
4d05h: ISAKMP (0:3): processing KE payload. message ID = 0
4d05h: ISAKMP (0:3): processing NONCE payload. message ID = 0
4d05h: ISAKMP (0:3): SKEYID state generated
4d05h: ISAKMP (0:3): processing HASH payload. message ID = 0
4d05h: ISAKMP (0:3): **SA has been authenticated with 172.16.172.41**
4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) AG_INIT_EXCH
4d05h: ISAKMP (0:3): Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_I_AM1 New State = IKE_P1_COMPLETE

4d05h: IPSEC(key_engine): got a queue event...

4d05h: IPsec: Key engine got KEYENG_IKMP_MORE_SAS message

4d05h: ISAKMP (0:3): Need XAUTH

4d05h: ISAKMP (0:3): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE

Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

!--- Phase 1 (ISAKMP) is complete. 4d05h: ISAKMP: received ke message (6/1) 4d05h: ISAKMP: received KEYENG_IKMP_MORE_SAS message 4d05h: ISAKMP: set new node -857862190 to CONF_XAUTH *!--- Initiate extended authentication.* 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP (0:3): purging node -857862190 4d05h: ISAKMP (0:3): Sending initial contact. 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP: set new node -1898481791 to CONF_XAUTH 4d05h: ISAKMP (0:3): processing transaction payload from 172.16.172.41. message ID = -1898481791 4d05h: ISAKMP: Config payload REQUEST 4d05h: ISAKMP (0:3): checking request: 4d05h: ISAKMP: XAUTH_TYPE_V2 4d05h: ISAKMP: XAUTH_USER_NAME_V2 4d05h: ISAKMP: XAUTH_USER_PASSWORD_V2 4d05h: ISAKMP: XAUTH_MESSAGE_V2 4d05h: ISAKMP (0:3): Xauth process request 4d05h: ISAKMP (0:3): Input = IKE_MSG_FROM_PEER, IKE_CFG_REQUEST Old State = IKE_P1_COMPLETE New State = IKE_XAUTH_REPLY_AWAIT 4d05h: EZVPN(SJVPN): Current State: READY 4d05h: EZVPN(SJVPN): Event: XAUTH_REQUEST 4d05h: EZVPN(SJVPN): ezvpn_xauth_request 4d05h: EZVPN(SJVPN): ezvpn_parse_xauth_msg 4d05h: EZVPN: Attributes sent in xauth request message: 4d05h: XAUTH_TYPE_V2(SJVPN): 0 4d05h: XAUTH_USER_NAME_V2(SJVPN): 4d05h: XAUTH_USER_PASSWORD_V2(SJVPN): 4d05h: XAUTH_MESSAGE_V2(SJVPN) <Enter Username and Password.> 4d05h: EZVPN(SJVPN): New State: XAUTH_REQ 4d05h: ISAKMP (0:3): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE Old State = IKE_XAUTH_REPLY_AWAIT New State = IKE_XAUTH_REPLY_AWAIT 4d05h: EZVPN(SJVPN): Pending XAuth Request, Please enter the following command: 4d05h: EZVPN: **crypto ipsec client ezvpn xauth**

!--- Enter the crypto ipsec client ezvpn xauth command.

crypto ipsec client ezvpn xauth

Enter Username and Password.: **padma**

Password: : **password**

!--- The router requests your username and password that is !--- configured on the server. 4d05h: EZVPN(SJVPN): Current State: XAUTH_REQ 4d05h: EZVPN(SJVPN): Event: XAUTH_PROMPTING 4d05h: EZVPN(SJVPN): New State: XAUTH_PROMPT 1721-1(ADSL)# 4d05h: EZVPN(SJVPN): Current State: XAUTH_PROMPT 4d05h: EZVPN(SJVPN): Event: XAUTH_REQ_INFO_READY 4d05h: EZVPN(SJVPN): ezvpn_xauth_reply 4d05h: XAUTH_TYPE_V2(SJVPN): 0 4d05h: XAUTH_USER_NAME_V2(SJVPN): Cisco_MAE 4d05h: XAUTH_USER_PASSWORD_V2(SJVPN): <omitted> 4d05h: EZVPN(SJVPN): New State: XAUTH_REPLIED 4d05h: xauth-type: 0 4d05h: username: Cisco_MAE 4d05h: password: <omitted> 4d05h: message <Enter Username and Password.> 4d05h: ISAKMP (0:3): responding to peer config from 172.16.172.41. ID = -1898481791 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP (0:3): deleting node -1898481791 error FALSE reason "done with xauth request/reply exchange" 4d05h: ISAKMP (0:3): Input = IKE_MSG_INTERNAL, IKE_XAUTH_REPLY_ATTR Old State = IKE_XAUTH_REPLY_AWAIT New State = IKE_XAUTH_REPLY_SENT 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP: set new node -1602220489 to CONF_XAUTH 4d05h: ISAKMP (0:3): processing transaction payload from 172.16.172.41. message ID = -1602220489 4d05h:

ISAKMP: Config payload SET 4d05h: ISAKMP (0:3): Xauth process set, status = 1 4d05h: ISAKMP (0:3): checking SET: 4d05h: ISAKMP: XAUTH_STATUS_V2 XAUTH-OK 4d05h: ISAKMP (0:3): attributes sent in message: 4d05h: Status: 1 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP (0:3): deleting node -1602220489 error FALSE reason "" 4d05h: ISAKMP (0:3): Input = IKE_MSG_FROM_PEER, IKE_CFG_SET Old State = IKE_XAUTH_REPLY_SENT New State = IKE_P1_COMPLETE 4d05h: EZVPN(SJVPN): Current State: XAUTH_REPLIED 4d05h: EZVPN(SJVPN): Event: XAUTH_STATUS 4d05h: EZVPN(SJVPN): New State: READY 4d05h: ISAKMP (0:3): Need config/address 4d05h: ISAKMP (0:3): Need config/address 4d05h: ISAKMP: set new node 486952690 to CONF_ADDR 4d05h: ISAKMP (0:3): initiating peer config to 172.16.172.41. ID = 486952690 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) CONF_ADDR 4d05h: ISAKMP (0:3): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_MODE_REQ_SENT 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) CONF_ADDR 4d05h: ISAKMP (0:3): processing transaction payload from 172.16.172.41. message ID = 486952690 4d05h: ISAKMP: Config payload REPLY 4d05h: ISAKMP(0:3) process config reply 4d05h: ISAKMP (0:3): deleting node 486952690 error FALSE reason "done with transaction" 4d05h: ISAKMP (0:3): Input = IKE_MSG_FROM_PEER, IKE_CFG_REPLY Old State = IKE_CONFIG_MODE_REQ_SENT New State = IKE_P1_COMPLETE 4d05h: EZVPN(SJVPN): Current State: READY 4d05h: EZVPN(SJVPN): Event: MODE_CONFIG_REPLY 4d05h: EZVPN(SJVPN): ezvpn_mode_config 4d05h: EZVPN(SJVPN): ezvpn_parse_mode_config_msg 4d05h: EZVPN: Attributes sent in message 4d05h: ip_ifnat_modified: old_if 0, new_if 2 4d05h: ip_ifnat_modified: old_if 0, new_if 2 4d05h: ip_ifnat_modified: old_if 1, new_if 2 4d05h: EZVPN(SJVPN): New State: SS_OPEN 4d05h: ISAKMP (0:3): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-sha-hmac , lifedur= 2147483s and 4608000kb, spi= 0xE6DB9372(3873149810), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 2147483s and 4608000kb, spi= 0x3C77C53D(1014482237), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 2147483s and 4608000kb, spi= 0x79BB8DF4(2042334708), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 2147483s and 4608000kb, spi= 0x19C3A5B2(432252338), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: ISAKMP: received ke message (1/4) 4d05h: ISAKMP: set new node 0 to QM_IDLE 4d05h: EZVPN(SJVPN): Current State: SS_OPEN 4d05h: EZVPN(SJVPN): Event: SOCKET_READY 4d05h: EZVPN(SJVPN): No state change 4d05h: ISAKMP (0:3): sitting IDLE. Starting QM immediately (QM_IDLE) 4d05h: ISAKMP (0:3): beginning Quick Mode exchange, M-ID of -1494477527 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-sha-hmac , lifedur= 2147483s and 4608000kb, spi= 0xB18CF11E(2978803998), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 2147483s and 4608000kb, spi= 0xA8C469EC(2831444460), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 2147483s and 4608000kb, spi= 0xBC5AD5EE(3160069614), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 2147483s and 4608000kb, spi= 0x8C34C692(2352268946), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): Node -1494477527, Input = IKE_MSG_INTERNAL, IKE_INIT_QM Old State = IKE_QM_READY New State = IKE_QM_I_QM1 4d05h: ISAKMP: received ke message (1/4) 4d05h: ISAKMP: set new node 0 to QM_IDLE 4d05h: ISAKMP (0:3): sitting IDLE. Starting QM immediately (QM_IDLE) 4d05h: ISAKMP (0:3): beginning Quick Mode exchange, M-ID of -1102788797 4d05h: EZVPN(SJVPN): Current State: SS_OPEN 4d05h: EZVPN(SJVPN): Event: SOCKET_READY 4d05h: EZVPN(SJVPN): No state change 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): Node -1102788797, Input = IKE_MSG_INTERNAL,

IKE_INIT_QM Old State = IKE_QM_READY New State = IKE_QM_I_QM1 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP: set new node 733055375 to QM_IDLE 4d05h: ISAKMP (0:3): processing HASH payload. message ID = 733055375 4d05h: ISAKMP (0:3): processing NOTIFY RESPONDER_LIFETIME protocol 1 spi 0, message ID = 733055375, sa = 820ABFA0 4d05h: ISAKMP (0:3): processing responder lifetime 4d05h: ISAKMP (0:3): start processing isakmp responder lifetime 4d05h: ISAKMP (0:3): restart ike sa timer to 86400 secs 4d05h: ISAKMP (0:3): deleting node 733055375 error FALSE reason "informational (in) state 1" 4d05h: ISAKMP (0:3): Input = IKE_MSG_FROM_PEER, IKE_INFO_NOTIFY Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): processing HASH payload. message ID = -1494477527 4d05h: ISAKMP (0:3): processing SA payload. message ID = -1494477527 4d05h: ISAKMP (0:3): Checking IPsec proposal 1 4d05h: ISAKMP: transform 1, ESP_3DES 4d05h: ISAKMP: attributes in transform: 4d05h: ISAKMP: SA life type in seconds 4d05h: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9B 4d05h: ISAKMP: SA life type in kilobytes 4d05h: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 4d05h: ISAKMP: encaps is 1 4d05h: ISAKMP: authenticator is HMAC-MD5 4d05h: ISAKMP (0:3): atts are acceptable. 4d05h: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 4d05h: ISAKMP (0:3): processing NONCE payload. message ID = -1494477527 4d05h: ISAKMP (0:3): processing ID payload. message ID = -1494477527 4d05h: ISAKMP (0:3): processing ID payload. message ID = -1494477527 4d05h: ISAKMP (0:3): processing NOTIFY RESPONDER_LIFETIME protocol 3 spi 1344958901, message ID = -1494477527, sa = 820ABFA0 4d05h: ISAKMP (0:3): processing responder lifetime 4d05h: ISAKMP (3): responder lifetime of 28800s 4d05h: ISAKMP (3): responder lifetime of 0kb 4d05h: ISAKMP (0:3): Creating IPsec SAs 4d05h: inbound SA from 172.16.172.41 to 172.16.172.46 (proxy 0.0.0.0 to 192.168.254.0) 4d05h: has spi 0x3C77C53D and conn_id 2000 and flags 4 4d05h: lifetime of 28800 seconds 4d05h: outbound SA from 172.16.172.46 to 172.16.172.41 (proxy 192.168.254.0 to 0.0.0.0) 4d05h: has spi 1344958901 and conn_id 2001 and flags C 4d05h: lifetime of 28800 seconds 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): deleting node -1494477527 error FALSE reason "" 4d05h: ISAKMP (0:3): Node -1494477527, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): processing HASH payload. message ID = -1102788797 4d05h: ISAKMP (0:3): processing SA payload. message ID = -1102788797 4d05h: ISAKMP (0:3): Checking IPsec proposal 1 4d05h: ISAKMP: transform 1, ESP_3DES 4d05h: ISAKMP: attributes in transform: 4d05h: ISAKMP: SA life type in seconds 4d05h: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9B 4d05h: ISAKMP: SA life type in kilobytes 4d05h: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 4d05h: ISAKMP: encaps is 1 4d05h: ISAKMP: authenticator is HMAC-MD5 4d05h: ISAKMP (0:3): atts are acceptable. 4d05h: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 4d05h: ISAKMP (0:3): processing NONCE payload. message ID = -1102788797 4d05h: ISAKMP (0:3): processing ID payload. message ID = -1102788797 4d05h: ISAKMP (0:3): processing ID payload. message ID = -1102788797 4d05h: ISAKMP (0:3): processing NOTIFY RESPONDER_LIFETIME protocol 3 spi 653862918, message ID = -1102788797, sa = 820ABFA0 4d05h: ISAKMP (0:3): processing responder lifetime 4d05h: ISAKMP (3): responder lifetime of 28800s 4d05h: ISAKMP (3): responder lifetime of 0kb 4d05h: IPSEC(key_engine): got a queue event... 4d05h: IPSEC(initialize_sas): , (key eng. msg.) INBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 28800s and 0kb, spi= 0x3C77C53D(1014482237), conn_id= 2000, keysize= 0, flags= 0x4 4d05h: IPSEC(initialize_sas): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= **192.168.254.0**/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 28800s and 0kb, spi= 0x502A71B5(1344958901), conn_id= 2001, keysize= 0, flags= 0xC 4d05h: IPSEC(create_sa): sa created, (sa) sa_dest= 172.16.172.46, sa_prot= 50, sa_spi= **0x3C77C53D(1014482237)**,
!--- SPI that is used on inbound SA. sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2000 4d05h: IPSEC(create_sa): sa created, (sa) sa_dest= 172.16.172.41, sa_prot= 50, sa_spi= **0x502A71B5(1344958901)**,
!--- SPI that is used on outbound SA. sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2001 4d05h:


```

ISAKMP (0:3): Creating IPsec SAs 4d05h: inbound SA from 172.16.172.41 to 172.16.172.46 (proxy
0.0.0.0 to 192.168.253.0) 4d05h: has spi 0xA8C469EC and conn_id 2002 and flags 4 4d05h: lifetime
of 28800 seconds 4d05h: outbound SA from 172.16.172.46 to 172.16.172.41 (proxy 192.168.253.0 to
0.0.0.0 ) 4d05h: has spi 653862918 and conn_id 2003 and flags C 4d05h: lifetime of 28800 seconds
4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): deleting
node -1102788797 error FALSE reason "" 4d05h: ISAKMP (0:3): Node -1102788797, Input =
IKE_MSG_FROM_PEER, IKE_QM_EXCH Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE
4d05h: ISAKMP: received ke message (4/1) 4d05h: ISAKMP: Locking CONFIG struct 0x81F433A4 for
crypto_ikmp_config_handle_kei_mess, count 3 4d05h: EZVPN(SJVPN): Current State: SS_OPEN 4d05h:
EZVPN(SJVPN): Event: MTU_CHANGED 4d05h: EZVPN(SJVPN): No state change 4d05h: IPSEC(key_engine):
got a queue event... 4d05h: IPSEC(initialize_sas): , (key eng. msg.) INBOUND local=
172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4),
remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 28800s and 0kb, spi= 0xA8C469EC(2831444460), conn_id= 2002, keysize= 0, flags= 0x4
4d05h: IPSEC(initialize_sas): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote=
172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4),
remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 28800s and 0kb,
    spi= 0x26F92806(653862918), conn_id= 2003, keysize= 0, flags= 0xC
4d05h: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.16.172.46, sa_prot= 50,
    sa_spi= 0xA8C469EC(2831444460),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2002
4d05h: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.16.172.41, sa_prot= 50,
    sa_spi= 0x26F92806(653862918),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2003
4d05h: ISAKMP: received ke message (4/1)
4d05h: ISAKMP: Locking CONFIG struct 0x81F433A4 for
    crypto_ikmp_config_handle_kei_mess, count 4
4d05h: EZVPN(SJVPN): Current State: SS_OPEN
4d05h: EZVPN(SJVPN): Event: SOCKET_UP
4d05h: ezvpn_socket_up
4d05h: EZVPN(SJVPN): New State: IPSEC_ACTIVE
4d05h: EZVPN(SJVPN): Current State: IPSEC_ACTIVE
4d05h: EZVPN(SJVPN): Event: MTU_CHANGED
4d05h: EZVPN(SJVPN): No state change
4d05h: EZVPN(SJVPN): Current State: IPSEC_ACTIVE
4d05h: EZVPN(SJVPN): Event: SOCKET_UP
4d05h: ezvpn_socket_up
4d05h: EZVPN(SJVPN): No state change

```

[Comandos cisco ios show relacionados para pesquisar defeitos](#)

```
1721-1(ADSL)#show crypto ipsec client ezvpn
```

```

Tunnel name : SJVPN
Inside interface list: Loopback0, Loopback1,
Outside interface: FastEthernet0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP

```

```
1721-1(ADSL)#show crypto isakmp sa
```

dst	src	state	conn-id	slot
172.16.172.41	172.16.172.46	QM_IDLE	3	0

```
1721-1(ADSL)#show crypto ipsec sa
```

```

interface: FastEthernet0
Crypto map tag: FastEthernet0-head-0, local addr. 172.16.172.46
local ident (addr/mask/prot/port): (192.168.253.0/255.255.255.0/0/0)

```

remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

current_peer: **172.16.172.41**

PERMIT, flags={origin_is_acl,}

#pkts encaps: 100, #pkts **encrypt: 100**, #pkts digest 100

#pkts decaps: 100, #pkts **decrypt: 100**, #pkts verify 100

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 172.16.172.46, remote crypto endpt.: 172.16.172.41

path mtu 1500, media mtu 1500

current outbound spi: 26F92806

inbound esp sas:

spi: **0xA8C469EC(2831444460)**

transform: esp-3des esp-md5-hmac ,

in use settings = {Tunnel, }

slot: 0, conn id: 2002, flow_id: 3, crypto map: FastEthernet0-head-0

sa timing: remaining key lifetime (k/sec): (4607848/28656)

IV size: 8 bytes

replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: **0x26F92806(653862918)**

transform: esp-3des esp-md5-hmac ,

in use settings = {Tunnel, }

slot: 0, conn id: 2003, flow_id: 4, crypto map: FastEthernet0-head-0

sa timing: remaining key lifetime (k/sec): (4607848/28647)

IV size: 8 bytes

replay detection support: Y

outbound ah sas:

outbound pcp sas:

local ident (addr/mask/prot/port): (**192.168.254.0**/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

current_peer: **172.16.172.41**

PERMIT, flags={origin_is_acl,}

#pkts encaps: 105, #pkts **encrypt: 105**, #pkts digest 105

#pkts decaps: 105, #pkts **decrypt: 105**, #pkts verify 105

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 172.16.172.46, remote crypto endpt.: 172.16.172.41

path mtu 1500, media mtu 1500

current outbound spi: 502A71B5

inbound esp sas:

spi: **0x3C77C53D(1014482237)**

transform: esp-3des esp-md5-hmac ,

in use settings = {Tunnel, }

slot: 0, conn id: 2000, flow_id: 1, crypto map: FastEthernet0-head-0

sa timing: remaining key lifetime (k/sec): (4607847/28644)

IV size: 8 bytes

replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:

```
spi: 0x502A71B5(1344958901)
  transform: esp-3des esp-md5-hmac ,
  in use settings =(Tunnel, )
  slot: 0, conn id: 2001, flow_id: 2, crypto map: FastEthernet0-head-0
  sa timing: remaining key lifetime (k/sec): (4607847/28644)
  IV size: 8 bytes
  replay detection support: Y
```

outbound ah sas:

outbound pcp sas:

[Cancele um túnel ativo](#)

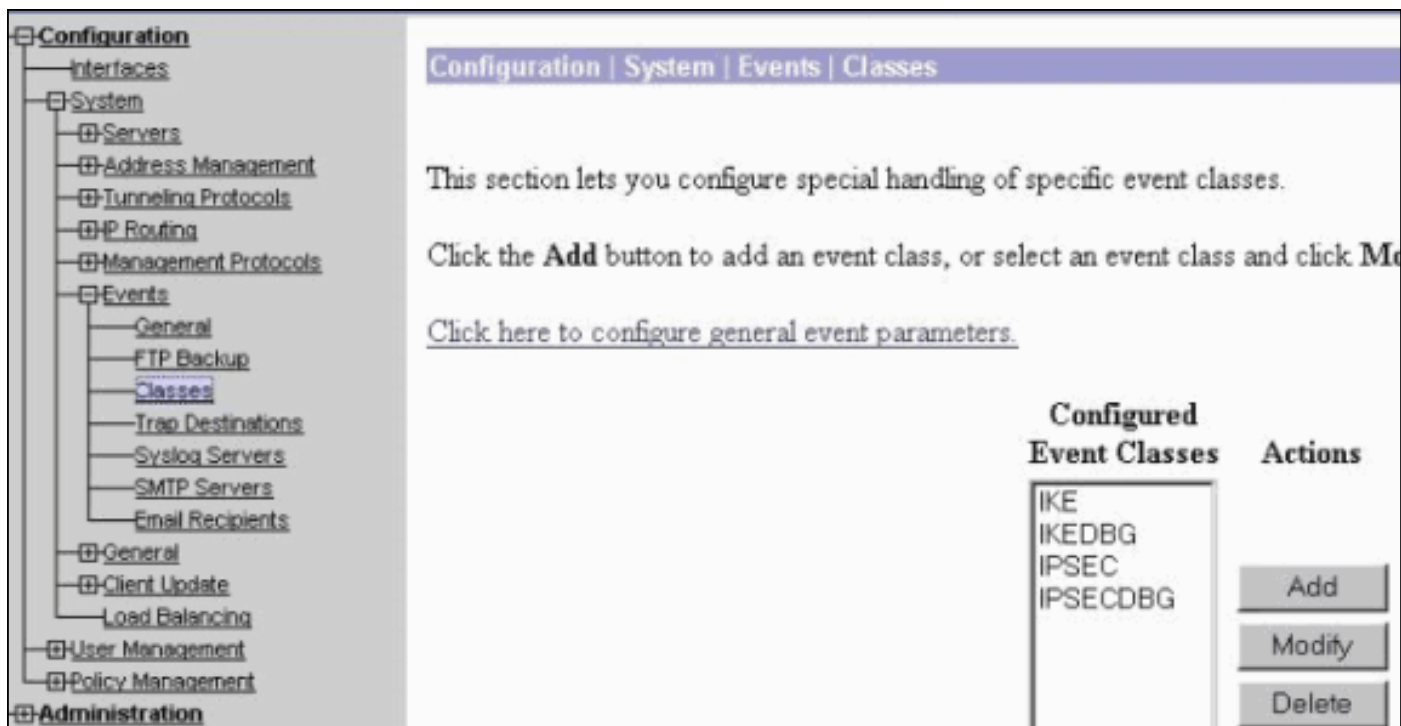
Você pode cancelar os túneis com estes comandos:

- cancele o isakmp cripto
- cancele o sa cripto
- cancele o EzVPN do cliente de IPSec de criptografia

Note: Você pode usar o concentrador VPN a fim logout da sessão quando você escolhe a **administração > sessões de administrador**, seleciona o usuário na **sessão de acesso remota** e clica a **saída**.

[Debug de VPN 3000 Concentrator](#)

Selecione **Configuration > System > Events > Classes** para habilitar essa depuração caso haja falhas de eventos de conexão. Você pode sempre adicionar mais classes se essas mostradas não o ajudam a identificar o problema.



Para acessar o log de eventos atual na memória, o qual pode ser filtrado por classe de eventos, severidade, endereço IP e assim por diante, selecione **Monitoring > Filterable Event log**.



Para exibir as estatísticas do protocolo IPsec, selecione **Monitoring > Statistics > IPSec**. Essa janela exibe estatísticas da atividade do IPsec (incluindo os túneis IPsec atuais) no VPN Concentrator desde que ele foi reinicializado ou redefinido pela última vez. Estas estatísticas conformam-se ao esboço de IETF para o fluxo do IPsec que monitora o MIB. A janela **Monitoring > Sessions > Detail** também exibe dados do IPsec.

IKE (Phase 1) Statistics		IPsec (Phase 2) Statistics	
Active Tunnels	1	Active Tunnels	2
Total Tunnels	122	Total Tunnels	362
Received Bytes	2057442	Received Bytes	0
Sent Bytes	332256	Sent Bytes	1400
Received Packets	3041	Received Packets	0
Sent Packets	2128	Sent Packets	5
Received Packets Dropped	1334	Received Packets Dropped	0
Sent Packets Dropped	0	Received Packets Dropped (Anti-Replay)	0
Received Notifies	15	Sent Packets Dropped	0
Sent Notifies	254	Inbound Authentications	0
Received Phase-2 Exchanges	362		

[que pode dar errado](#)

- O roteador do Cisco IOS obtém colado no estado AG_INIT_EXCH. Quando você pesquisar defeitos, gire sobre o IPsec e o ISAKMP debuga com estes comandos: [debug crypto ipsecdebug crypto isakmpdebug crypto ezvpn](#) No Cisco IOS roteador, você vê este:

```

1721-1(ADSL)#show crypto ipsec client ezvpn
Tunnel name : SJVPN
Inside interface list: Loopback0, Loopback1,
Outside interface: FastEthernet0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
1721-1(ADSL)#show crypto isakmp sa

      dst      src      state      conn-id  slot
172.16.172.41  172.16.172.46  QM_IDLE          3        0

1721-1(ADSL)#show crypto ipsec sa

interface: FastEthernet0
  Crypto map tag: FastEthernet0-head-0, local addr. 172.16.172.46
  local ident (addr/mask/prot/port): (192.168.253.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

current_peer: 172.16.172.41
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 100, #pkts encrypt: 100, #pkts digest 100
  #pkts decaps: 100, #pkts decrypt: 100, #pkts verify 100
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 172.16.172.46, remote crypto endpt.: 172.16.172.41
  path mtu 1500, media mtu 1500
  current outbound spi: 26F92806

```

inbound esp sas:

spi: **0xA8C469EC(2831444460)**
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2002, flow_id: 3, crypto map: FastEthernet0-head-0
sa timing: remaining key lifetime (k/sec): (4607848/28656)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: **0x26F92806(653862918)**
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2003, flow_id: 4, crypto map: FastEthernet0-head-0
sa timing: remaining key lifetime (k/sec): (4607848/28647)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas:

local ident (addr/mask/prot/port): (192.168.254.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

current_peer: **172.16.172.41**

PERMIT, flags={origin_is_acl,}

#pkts encaps: 105, #pkts **encrypt: 105**, #pkts digest 105

#pkts decaps: 105, #pkts **decrypt: 105**, #pkts verify 105

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 172.16.172.46, remote crypto endpt.: 172.16.172.41

path mtu 1500, media mtu 1500

current outbound spi: 502A71B5

inbound esp sas:

spi: **0x3C77C53D(1014482237)**
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2000, flow_id: 1, crypto map: FastEthernet0-head-0
sa timing: remaining key lifetime (k/sec): (4607847/28644)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: **0x502A71B5(1344958901)**
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: FastEthernet0-head-0
sa timing: remaining key lifetime (k/sec): (4607847/28644)
IV size: 8 bytes

replay detection support: Y

outbound ah sas:

outbound pcp sas:

No VPN 3000 concentrator, o Xauth é exigido. Contudo, a proposta selecionada não apoia o Xauth. Verifique se [internal authentication for Xauth](#) foi especificado. Habilite a autenticação interna e certifique-se que as propostas IKE tenham o modo de autenticação configurado para **Preshared Keys (Xauth)**, como na [captura de tela](#) anterior. Clique em **Modify** para editar a proposta.

- A senha está incorreta. Você não verá a mensagem **Invalid Password** no roteador Cisco IOS. No VPN Concentrator, você deverá ver **Received unexpected event EV_ACTIVATE_NEW_SA in state AM_TM_INIT_XAUTH**. Assegure-se de que a sua senha esteja correta.
- O username está incorreto. No roteador do Cisco IOS você vê debugar similar a este se você tem a senha errada. No VPN Concentrator você verá **Authentication rejected: Reason = User was not found**.

[Informações Relacionadas](#)

- [Página de suporte do Cisco VPN 3000 Series Concentrator](#)
- [Fase remota II do Cisco Easy VPN](#)
- [Página de suporte ao cliente do Cisco VPN 3000 Series](#)
- [Página de Suporte de Negociação IPSec/Protocolos IKE](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)