在有VPN 3000集中器的IOS路由器上，带NEM的EzVPN配置示例

目录

简介

本文解释您使用为了配置Cisco IOS路由器作为在网络扩展模式(NEM)的一EzVPN连接到Cisco VPN 3000集中器的步骤。一个新的EzVPN第II阶段功能是一基本网络地址转换(NAT)配置的支持。EzVPN第II阶段从Unity协议(VPN客户端软件)派生。远程设备总是IPSec隧道的发起者。然而，Internet Key Exchange (IKE)和IPsec建议不是可配置在EzVPN客户端。VPN客户端协商建议用服务器。

要使用 Easy VPN 在 PIX/ASA 7.x 和 Cisco 871 路由器之间配置 IPsec，请参阅将 ASA 5500 用作服务器，将 Cisco 871 用作 Easy VPN Remote 的 PIX/ASA 7.x Easy VPN 配置示例。

要在 Cisco IOS Easy VPN Remote Hardware Client 和 PIX Easy VPN 服务器之间配置 IPsec，请参阅 IOS Easy VPN Remote Hardware Client 到 PIX Easy VPN 服务器配置示例。

要将 Cisco 7200 路由器配置为 EzVPN 并将 Cisco 871 路由器配置为 Easy VPN Remote，请参阅 7200 Easy VPN 服务器到 871 Easy VPN Remote 配置示例。

先决条件

要求

在您尝试此配置检查前Cisco IOS路由器支持EzVPN第II阶段功能，并且有与设立IPSec隧道的端到端连接的IP连通性。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS软件版本12.2(8)YJ (EzVPN相位II)
- VPN 3000集中器3.6.x
- Cisco 1700 路由器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

注意： 此配置用有Cisco IOS软件版本12.4(8)和VPN 3000集中器4.7.x版本的一个Cisco 3640路由器最近测试。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置VPN 3000集中器

任务

在此部分，您提交以信息配置VPN 3000集中器。

网络图

本文档使用此图所示的网络设置。回环接口使用作为内部子网，并且FastEthernet0是默认到互联网。

逐步指导

完成这些步骤：

1. 选择**Configuration > User Management > Groups > Add**并且定义组名和密码为了配置用户的一个IPSec组。此示例以密码使用组名**turaro**/验证**tululo**。
2. 选择**Configuration > User Management > Groups** >启用**IPSec**和禁用点对点隧道协议(PPTP)和Layer2隧道协议的**turaro** >General (L2TP)。做您的选择并且单击**应用**。
3. 设置验证对**内部**扩展认证的并且保证隧道类型是**远程访问，**并且IPSec SA是**ESP-3DES-MD5**。
4. 选择**Configuration > System > Tunneling Protocols > IPSec > IKE Proposals**为了确保，Cisco VPN Client (CiscoVPNClient-3DES-MD5)是在IKE的(相位1)有效建议。**注意：** 从VPN集中器4.1.x，步骤为保证是不同的Cisco VPN Client是在有效建议列表IKE的(相位1)。选择**Configuration>建立隧道和安全> IPSec > IKE Proposals。**
5. 验证您的IPSec安全关联(SA)。在步骤3您的IPsec SA是ESP-3DES-MD5。如果希望，但是确

保您使用在您的组的正确IPsec SA您能创建新的。您应该禁用您使用的IPsec的SA完整转发安全性(PFS)。选择Cisco VPN Client作为IKE建议通过选择**Configuration > Policy Management > Traffic Management > SAS**。键入在文本框的SA名称并且做适当的选择如显示此处：**注意**：如果喜欢选择预定义的SA，此步骤和下一步可选。如果您的客户端动态地有一个指定的IP地址，请使用0.0.0.0在IKE对等体文本框。make保证IKE建议设置为**CiscoVPNClient-3DES-MD5**，当此示例显示。

6. 您不能单击*允许在列表的网络绕过通道*。原因是支持分割隧道，但是旁路功能不支持与EzVPN客户端功能。
7. 选择**Configuration > User Management** > Users为了添加用户。定义用户名和密码，分配它到组，并且单击**添加**。
8. 选择**Administration > Admin塞申斯**并且检查用户连接。在NEM中， VPN集中器不分配从池的一个IP地址。**注意：** 如果喜欢选择预定义的SA，此步骤可选。
9. 点击**"Save"需要的**或**Save图标**为了保存配置。

路由器配置

show version输出

```
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
```

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

一旦配置两个设备，使用对端IP地址， Cisco 3640路由器尝试通过自动联系VPN集中器设置VPN通道。在交换最初的 ISAKMP 参数后，路由器显示以下消息：

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

您必须输入提示您输入用户名和口令的 **crypto ipsec client ezvpn xauth** 命令。这应该匹配在VPN集中器配置的用户名和密码(步骤7)。一旦用户名和密码由两对等体同意，参数的其余同意，并且IPSec VPN通道出来。

```
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
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

注意： 发出 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **debug crypto ipsec client ezvpn** —显示显示EzVPN客户端功能的配置和实施的信息。
- **debug crypto ipsec** - 显示有关 IPsec 连接的调试信息。
- **debug crypto isakmp** - 显示有关 IPsec 连接的调试信息，并显示由于两端不兼容而被拒绝的第一组属性。
- **show debug** —显示每个调试选项的状态。

从调试指令的输出

当您输入**crypto ipsec client ezvpn SJVPN命令**， EzVPN客户端尝试连接到服务器。如果更改**connect manual命令**在组配置下，请输入**crypto ipsec client ezvpn connect SJVPN命令**启动建议交换到服务器。

```
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_MESG_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_MESG_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_MESG_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_MESG_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_MESG_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_MESG_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_MESG_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_MESG_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_MESG_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_MESG_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_MESG_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_MESG_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_MESG_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_MESG_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
```

相关Cisco IOS显示排除故障的命令

```
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:
```

清除活动通道

您能清除通道用这些命令：

- clear crypto isakmp
- clear crypto sa
- clear crypto ipsec client ezvpn

注意： 当您在**远程访问会话**上选择**Administration > Admin塞申斯**，选择用户并且点击**注销时，**您能使用VPN集中器为了注销会话。

VPN 3000 集中器调试

如果有事件连接故障，请选择**Configuration > System > Events > Classes**为了启用此调试。如果显示的那个不帮助您识别问题，您能总是添加更多类。

为了查看时事登录内存，可过滤由事件类，严重性， IP地址，等等，选择**Monitoring > Filterable Event Log**。

为了查看IPSec协议的统计信息，选择**Monitoring > Statistics > IPSec。**因为它是为时启动的或重置，此窗口表示IPsec活动的统计信息，包括当前IPSec隧道，在VPN集中器。这些统计信息依照监控

MIB的IPsec流的IETF草案。**Monitoring > Sessions > Detail**窗口也表示IPsec数据。

可能出现的错误

- Cisco IOS路由器陷在AG_INIT_EXCH状态。当您排除故障时，请用这些命令打开IPsec和ISAKMP调试：**debug crypto ipsecdebug crypto isakmpdebug crypto EzVPN**在Cisco IOS路由器上，您看到此：

```
5d16h: ISAKMP (0:9): beginning Aggressive Mode exchange
5d16h: ISAKMP (0:9): sending packet to 10.48.66.115 (I) AG_INIT_EXCH
5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH...
5d16h: ISAKMP (0:9): incrementing error counter on sa: retransmit phase 1
5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH
5d16h: ISAKMP (0:9): sending packet to 10.48.66.115 (I) AG_INIT_EXCH
5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH...
5d16h: ISAKMP (0:9): incrementing error counter on sa: retransmit phase 1
5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH
5d16h: ISAKMP (0:9): sending packet to 10.48.66.115 (I) AG_INIT_EXCH
5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH...
5d16h: ISAKMP (0:9): incrementing error counter on sa: retransmit phase 1
5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH
5d16h: ISAKMP (0:9): sending packet to 10.48.66.115 (I) AG_INIT_EXCH
```

  在VPN 3000集中器上，Xauth要求。然而，选定建议不支持Xauth。验证Xauth的内部验证指定。启用内部验证并且保证IKE建议有认证模式设置为**预共享密匙(Xauth)**，正如在上一个屏幕画面。点击**修改**为了编辑建议。
- 密码不正确。您看不到在Cisco IOS路由器的**无效密码**消息。在VPN集中器上，您也许发现**在状态AM_TM_INIT_XAUTH的已接收意外事件EV_ACTIVATE_NEW_SA**。保证您的密码正确。
- 用户名不正确。在Cisco IOS路由器上，如果有错误的密码，您看到调试类似于此。在VPN集中器上您看到**拒绝的验证：未找到原因=用户**。

相关信息

- Cisco VPN 3000 系列集中器支持页
- Cisco Easy VPN Remote第II阶段
- Cisco VPN 3000 系列客户端支持页
- IPsec 协商/IKE 协议支持页
- 技术支持和文档 - Cisco Systems