



# Настройка клиента EzVPN Cisco на IOS Cisco с концентратором VPN 3000

---

## Содержание

### Введение

#### Предварительные условия

- Требования
- Используемые компоненты
- Условные обозначения

#### Настройка концентратора VPN 3000

- Задача
- Схема сети
- Пошаговые инструкции
- Конфигурация маршрутизатора

#### Проверка

##### Устранение неполадок

- Команды устранения неполадок
- Выходные данные команд отладки
- Дополнительные команды show в Cisco IOS для устранения неполадок
- Отладка концентратора VPN 3000
- Возможные проблемы

##### Дополнительные сведения

---

## Введение

В этом документе описаны процедуры, необходимые для настройки маршрутизатора Cisco IOS® в качестве EzVPN в NEM (режиме расширения сети) для подключения к концентратору Cisco VPN 3000. EzVPN Phase II (фаза II) снабжен новой функцией поддержки базовой конфигурации NAT (преобразование сетевых адресов). EzVPN Phase II основана на протоколе Unity (ПО VPN-клиент). Удаленное устройство всегда является инициатором IPsec-туннеля. Однако IKE (обмен ключами в Интернете) и предложения IPsec невозможно настроить в EzVPN-клиенте. VPN-клиент согласовывает предложения с сервером.

Информацию о настройке IPsec между PIX/ASA 7.x и маршрутизатором Cisco 871 с помощью Easy VPN см. в Примеры конфигурации с PIX/ASA 7.x Easy VPN с ASA 5500 в качестве сервера и Cisco 871 в качестве Easy VPN Remote.

Информацию о настройке IPsec между аппаратным клиентом Cisco IOS® Easy VPN Remote и сервером PIX Easy VPN см. в Примеры конфигурации аппаратного клиента IOS Easy VPN Remote на сервере PIX Easy VPN.

Информацию о настройке маршрутизатора Cisco 7200 в качестве EzVPN и маршрутизатора Cisco 871 в качестве Easy VPN Remote см. в Примеры конфигурации сервера 7200 Easy VPN в 871 Easy VPN Remote.

## Предварительные условия

### Требования

Перед применением данной конфигурации убедитесь, что маршрутизатор Cisco IOS поддерживает функцию EzVPN Phase II и имеет возможность подключения по IP со сквозными соединениями для создания IPsec-туннеля.

### Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного и аппаратного обеспечения:

- ПО Cisco IOS версии 12.2(8)YJ (EzVPN Phase II)
- Концентратор VPN 3000 версии 3.6.x
- Маршрутизатор Cisco 1700

Данные для документа были получены в специально созданных лабораторных условиях. Все устройства, используемые в этом документе, были запущены с чистой (заданной по умолчанию) конфигурацией. Если ваша сеть работает в реальных условиях, убедитесь, что вы понимаете потенциальное воздействие каждой команды.

**Примечание.** Данная конфигурация была проверена с помощью маршрутизатора Cisco 3640 с ПО Cisco IOS версии 12.4(8) и концентратора VPN 3000 версии 4.7.x

## Условные обозначения

Более подробные сведения о применяемых в документе обозначениях см. в документе Условные обозначения, используемые в технической документации Cisco.

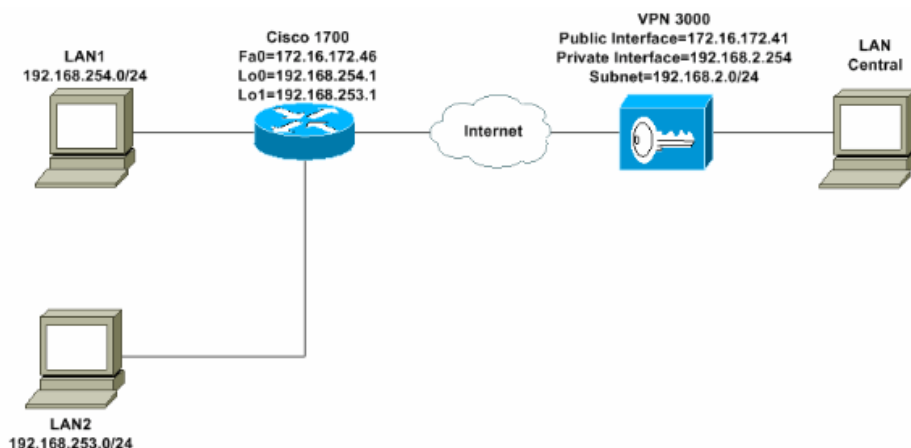
## Настройка концентратора VPN 3000

### Задача

В этом разделе представлена информация, необходимая для настройки концентратора VPN 3000.

### Схема сети

В этом документе используются настройки сети, показанные на данной схеме. Интерфейсы обратной петли используются как внутренние подсети, а FastEthernet 0 по умолчанию для Интернет.

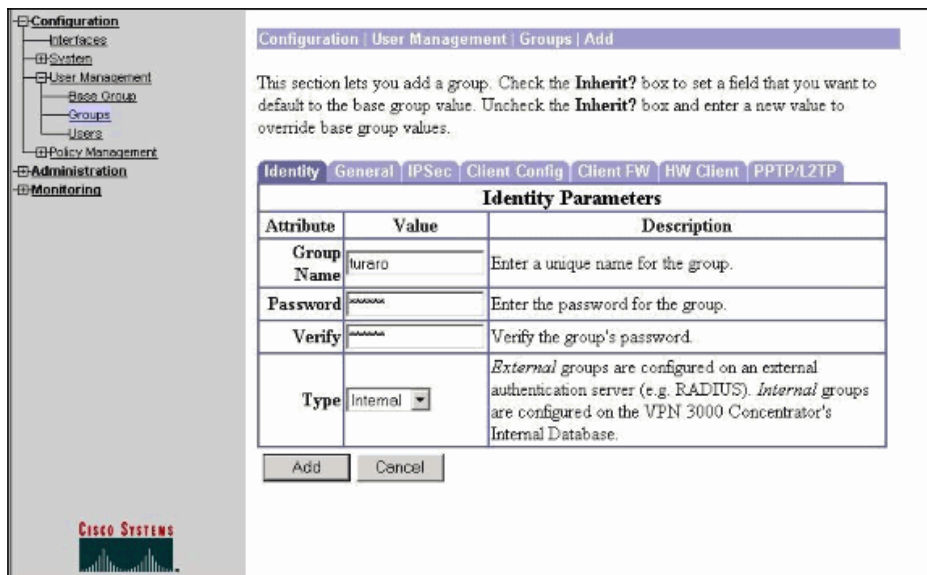


## Пошаговые инструкции

Выполните следующие шаги.

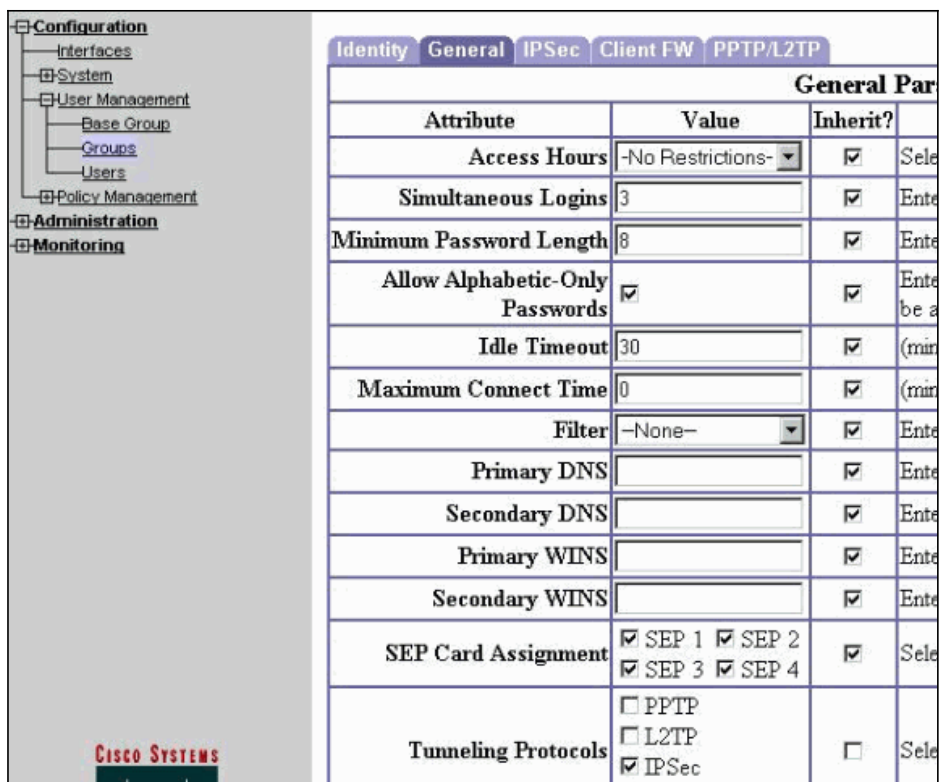
1. Чтобы настроить IPsec-группу для пользователей, выберите **Configuration > User Management > Groups > Add** и укажите имя группы и пароль.

В данном примере используется имя группы **turaro** и пароль **tululo**.

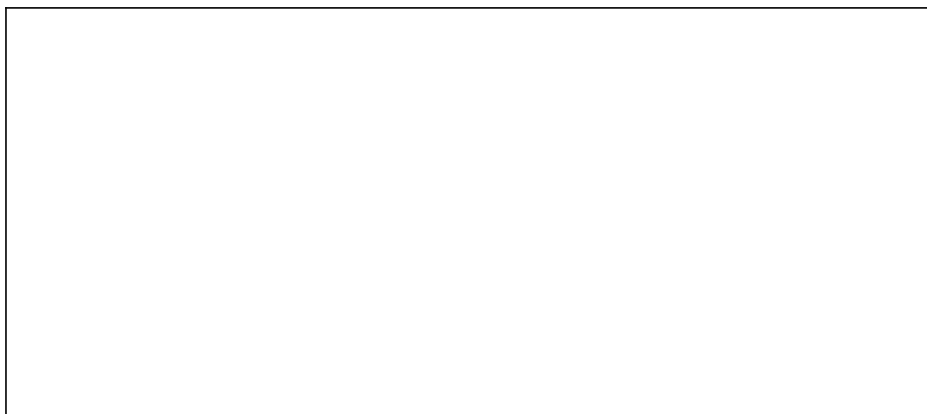


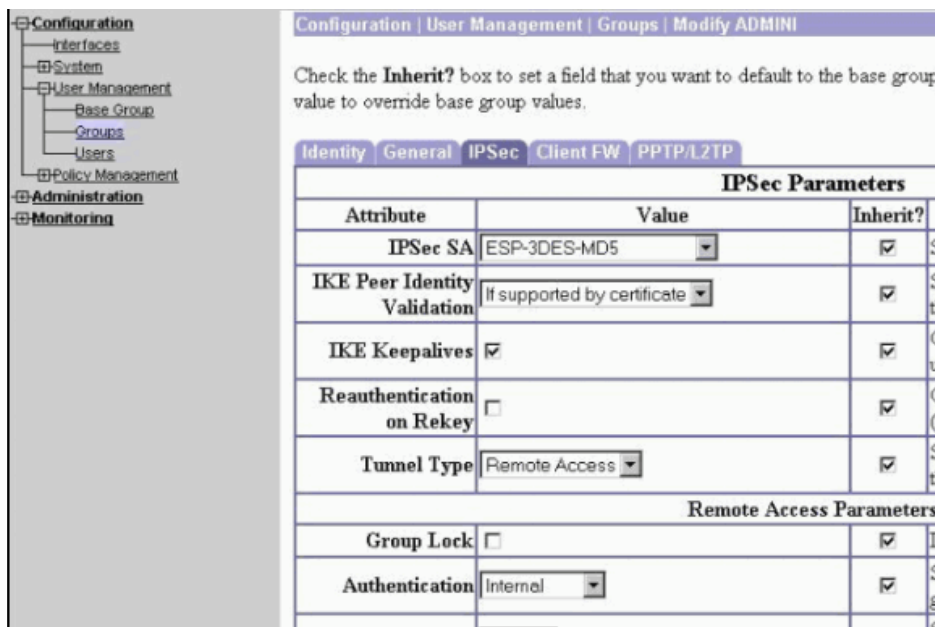
- Чтобы включить IPsec и отключить PPTP (протокол туннелирования "точка-точка") и L2TP (протокол туннелирования уровня 2), выберите **Configuration > User Management > Groups > turaro > General**.

Сделайте выбор и нажмите **Apply**.



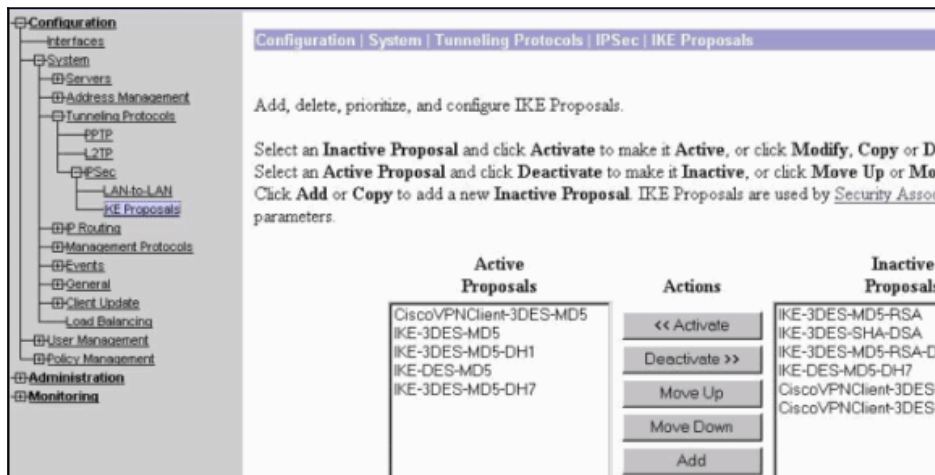
- Для расширенной аутентификации (Xauth) установите значение аутентификации **Internal**, для типа туннеля – **Remote Access** и для IPsec SA – **ESP-3DES-MD5**.





4. Для проверки, что Cisco VPN-клиент (CiscoVPNClient-3DES-MD5) находится в списке Active Proposals для IKE (фаза 1), выберите **Configuration > System > Tunneling Protocols > IPsec > IKE Proposals**.

**Примечание.** Процесс проверки, что Cisco VPN-клиент находится в списке Active Proposals для IKE (фаза 1) для концентратора VPN версии 4.1.x будет отличаться. Выберите **Configuration > Tunneling and Security > IPsec > IKE Proposals**.



5. Проверьте соответствие по безопасности IPsec (SA).

На шаге 3 для SA IPsec устанавливается значение ESP-3DES-MD5. При необходимости можно создать новое, но убедитесь, что для группы используется правильное SA IPsec. Для используемого SA IPsec необходимо отключить PFS (безопасная пересылка). Установите Cisco VPN-клиент в качестве предложения IKE, выбрав **Configuration > Policy Management > Traffic Management > SAs**. Введите имя SA в текстовом поле и сделайте соответствующий выбор, как показано ниже.

**Примечание.** При выборе стандартного SA этот и следующий шаги являются необязательными. Если клиент имеет динамически назначенный IP-адрес, необходимо в текстовом поле равнорангового узла IKE использовать 0.0.0.0. Проверьте, что предложение IKE установлено в **CiscoVPNClient-3DES-MD5**, как показано в данном примере.



Configuration | Policy Management | Traffic Management | Security Associations | Modify

Modify a configured Security Association.

SA Name  Specify the name of this Security Association (S

Inheritance  Select the granularity of this SA.

---

**IPSec Parameters**

Authentication Algorithm  Select the packet authentication algorithm to use

Encryption Algorithm  Select the ESP encryption algorithm to use.

Encapsulation Mode  Select the Encapsulation Mode for this SA.

Perfect Forward Secrecy  Select the use of Perfect Forward Secrecy.

Lifetime Measurement  Select the lifetime measurement of the IPSec ke

Data Lifetime  Specify the data lifetime in kilobytes (KB).

Time Lifetime  Specify the time lifetime in seconds.

---

**IKE Parameters**

IKE Peer  Specify the IKE Peer for a LAN-to-LAN IPSec

Negotiation Mode  Select the IKE Negotiation mode to use.

Digital Certificate  Select the Digital Certificate to use.

Certificate Transmission  Entire certificate chain Choose how to send the digital certificate to the

Identity certificate only

IKE Proposal  Select the IKE Proposal to use as IKE initiator.

6. Не устанавливайте флажок *Allow the networks in the list to bypass the tunnel*. Поскольку осуществляется поддержка раздельного туннелирования, а функция обхода не поддерживается функцией EzVPN-клиент.

|  |                                  |  |
|--|----------------------------------|--|
| <ul style="list-style-type: none"> <li>Configuration</li> <li>  Interfaces</li> <li>  System</li> <li>  User Management           <ul style="list-style-type: none"> <li>Base Group</li> <li>Groups</li> <li>Users</li> </ul> </li> <li>  Policy Management</li> <li>Administration</li> <li>Monitoring</li> </ul> | Banner                           | <input checked="" type="checkbox"/>  |
|  | Allow Password Storage on Client | <input type="checkbox"/>   |
|  | Split Tunneling Policy           | <input checked="" type="radio"/> Tunnel everything<br><input type="checkbox"/> Allow the networks in list to bypass the tunnel<br><input type="radio"/> Only tunnel networks in list |
|  | Split Tunneling Network List     | <input type="text" value="-None-"/>  |

7. Чтобы добавить пользователя, выберите **Configuration > User Management > Users**. Укажите имя пользователя и пароль, внесите его в группу и нажмите **Add**.

Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity | General | IPSec | PPTP/L2TP

| Identity Parameters |                                     |   |
|---------------------|-------------------------------------|---|
| Attribute           | Value                               | Description   |
| Username            | <input type="text" value="podma"/>  | Enter a unique username.  |
| Password            | <input type="password"/>            | Enter the user's password. The password must satisfy the group password requirements. |
| Verify              | <input type="password"/>            | Verify the user's password.   |
| Group               | <input type="text" value="turaro"/> | Enter the group to which this user belongs.   |
| IP Address          | <input type="text"/>                | Enter the IP address assigned to this user.   |
| Subnet Mask         | <input type="text"/>                | Enter the subnet mask assigned to this user.  |

CISCO SYSTEMS

8. Выберите **Administration > Admin Sessions** и проверьте подключение пользователя. В режиме NEM, концентратор VPN не

назначает IP-адреса из пула.

**Примечание.** При выборе стандартного SA этот шаг является необязательным.

| 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<br>Public IP Address | Group    | Protocol<br>Encryption | Login Time<br>Duration     | Client Type<br>Version | Bytes Tx<br>Bytes Rx | Actions        |  |
| Cisco_MAE              | 192.168.253.0<br>172.16.172.46           | turaro   | IPSec<br>3DES-168      | Mar 31 18:32:23<br>0:02:50 | N/A<br>N/A             | 301320<br>301320     | [Logout] [Log] |  |
| Management Sessions    |  |          |                        |                            |                        |                      |                | [ LAN-to-LAN Sessions   Remote Access Sessions ] |
| Administrator          | IP Address                               | Protocol | Encryption             | Login Time                 | Duration               | Actions              |                |  |
| admin                  | 171.69.89.5                              | HTTP     | None                   | Mar 31 18:35:01            | 0:00:12                | [Logout] [Ping]      |                |  |

9. Чтобы сохранить конфигурацию, нажмите значок **Save Needed** или **Save**.

## Конфигурация маршрутизатора

### Результат show version

```
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)  
!  
!--- Укажите имя конфигурации,  
!--- которая будет назначена для интерфейса.  
  
crypto ipsec client ezvpn SJVPN  
!--- Управление туннелем; по умолчанию установлен автоматический режим.  
  
connect auto  
!--- Имя группы и пароль должны совпадать с указанными для концентратора VPN.  
  
group turaro key tululo  
!--- Режим, выбранный в качестве расширения сети.  
  
mode network-extension  
!--- Конечный узел туннеля (IP-адрес публичного интерфейса концентратора VPN).  
  
peer 172.16.172.41  
!  
interface Loopback0  
ip address 192.168.254.1 255.255.255.0  
!--- Настройте интерфейс обратной связи  
!--- в качестве внутреннего интерфейса.  
  
ip nat inside  
!--- Указывает имя конфигурации Cisco EzVPN Remote,  
!--- которая назначается для внутреннего интерфейса.  
  
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
!--- Настройте интерфейс FastEthernet
!--- в качестве внешнего интерфейса.

  ip nat outside
!--- Указывает имя конфигурации Cisco EzVPN Remote,
!--- которое назначается для первого внешнего интерфейса, поскольку
!--- outside интерфейс для интерфейса не указан.
!--- По умолчанию установлен outside.

  crypto ipsec client ezvpn SJVPN
!
!--- Укажите параметр overload с помощью команды ip nat
!--- в режиме глобальной конфигурации, чтобы включить
!--- преобразование сетевых адресов (NAT) адреса внутреннего источника,
!--- что позволит нескольким ПК использовать один IP-адрес.

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

```

## Проверка

Используйте этот раздел для проверки правильной работы конфигурации.

Средство Интерпретатор выходных данных (только для зарегистрированных клиентов) (OIT) поддерживает некоторые команды **show**. Используйте OIT для просмотра анализа выходных данных команды **show**.

После настройки обоих устройств, маршрутизатор Cisco 3640 пытается установить VPN-туннель путем соединения с VPN-концентратором, автоматически используя IP-адрес однорангового узла. После обмена начальными параметрами ISAKMP, маршрутизатор отображает данное сообщение:

```

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

```

Необходимо ввести команду **crypto ipsec client ezvpn xauth**, которая запрашивает имя пользователя и пароль. Они должны совпадать с именем пользователя и паролем, указанных для концентратора VPN (шаг 7). После согласования имени пользователя и пароля на обоих равноправных узлах, согласуются остальные параметры и включается IPsec VPN-туннель.

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

```
EZVPN: crypto ipsec client ezvpn xauth
```

```
!--- Введите команду crypto ipsec client ezvpn xauth.
```

```
crypto ipsec client ezvpn xauth
```

```
Enter Username and Password.: padma
```

```
Password: : password
```

## Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

### Команды устранения неполадок

Некоторые команды **show** поддерживаются Интерпретатором выходных данных (только для зарегистрированных клиентов), что позволяет просматривать анализ выходных данных команды **show**.

**Примечание.** Перед использованием команд **debug** ознакомьтесь со статьей [Важная информация о командах отладки](#).

- **debug crypto ipsec client ezvpn** – отображает сведения о конфигурации и выполнении функции EzVPN-клиент.
- **debug crypto ipsec** – отображает данные отладки подключений IPsec.
- **debug crypto isakmp** – отображает данные отладки подключений IPsec и первый набор атрибутов, отклоняемых из-за несовместимости на обоих концах.
- **show debug** – отображает состояние каждого параметра отладки.

### Выходные данные команд отладки

После ввода команды **crypto ipsec client ezvpn SJVPN** EzVPN-клиент выполняет попытку соединения с сервером. При изменении команды **connect manual** в группе конфигурации, введите команду **crypto ipsec client ezvpn connect SJVPN** для начала обмена предложениями с сервером.

```
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

!--- Фаза 1 (ISAKMP) завершена.

4d05h: ISAKMP: received ke message (6/1)

4d05h: ISAKMP: received KEYENG_IKMP_MORE_SAS message

4d05h: ISAKMP: set new node -857862190 to CONF_XAUTH
!--- Иницируйте расширенную аутентификацию.

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

!--- Введите команду crypto ipsec client ezvpn xauth.

crypto ipsec client ezvpn xauth

Enter Username and Password.: padma

Password: : password

!--- Маршрутизатор запросит имя пользователя и пароль,
!--- указанные для сервера.

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, используемый на входящем 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, используемый на исходящем 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

```

## Дополнительные команды show в Cisco IOS для устранения неполадок

```

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:

## Очистка активного туннеля

Очистить туннели можно с помощью следующих команд:

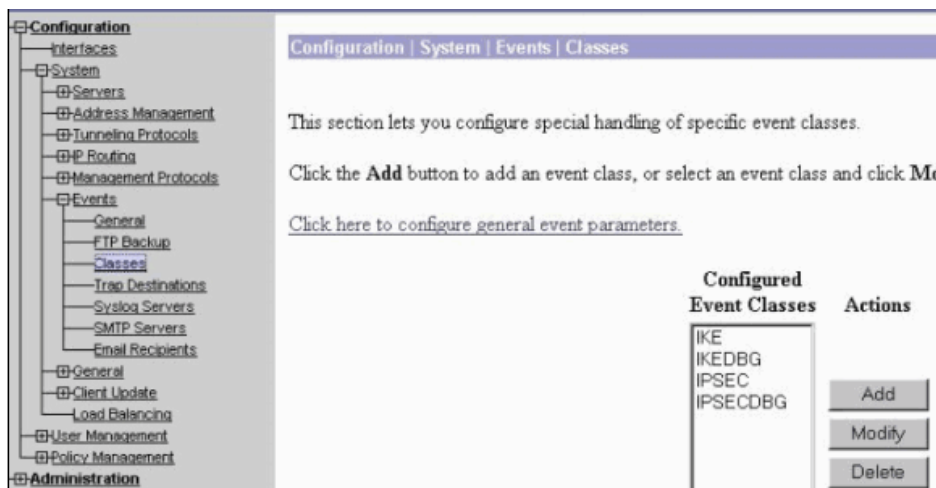
- **clear crypto isakmp**
- **clear crypto sa**
- **clear crypto ipsec client ezvpn**

**Примечание.** Возможно использование VPN-концентратора для окончания сеанса, для этого выберите **Administration > Admin Sessions**, выберите пользователя в **Remote Access Session** и нажмите **logout**.

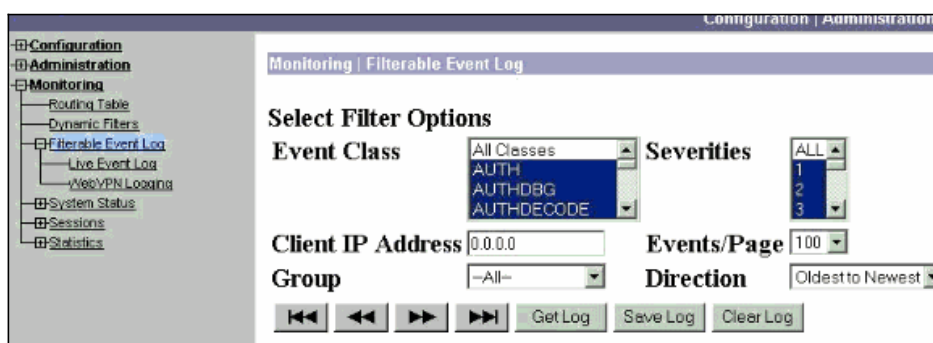
## Отладка концентратора VPN 3000

Чтобы включить эту отладку, при наличии сбоев соединения, выберите **Configuration > System > Events > Classes**. Если созданные классы не помогают определить проблему, можно добавить другие классы.





Чтобы просмотреть журнал текущих событий в памяти, фильтруемый по классам событий, важности, IP-адресам и т. д., выберите **Monitoring > Filterable Event log**.



Чтобы просмотреть статистику протокола IPsec, выберите **Monitoring > Statistics > IPsec**. Это окно отображает статистику активности IPsec, включая текущие IPsec-туннели в VPN-концентраторе, с момента последней загрузки или сброса. Эта статистика соответствует проекту IETF для MIB по IPsec Flow Monitoring. Окно **Monitoring > Sessions > Detail** также отображает данные 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     |  |      |

## Возможные проблемы

- Маршрутизатор Cisco IOS зависает в состоянии AG\_INIT\_EXCH. При устранении неисправности включите отладку IPsec и ISAKMP с помощью следующих команд:
  - debug crypto ipsec
  - debug crypto isakmp
  - debug crypto ezvpn



Маршрутизатор Cisco IOS отображает следующее:

```
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
```

Для концентратора VPN 3000 требуется функция Xauth. Однако, выбранное предложение не поддерживает Xauth. Проверьте, что указана внутренняя аутентификация для Xauth. Включите внутреннюю аутентификацию и установите режим аутентификации для предложений IKE в **Preshared Keys (Xauth)**, как на предыдущем снимке экрана. Чтобы изменить предложение, нажмите **Modify**.

- Неверный пароль:

В маршрутизаторе Cisco IOS сообщение **Invalid Password** не отображается. Для концентратора VPN может отобразиться сообщение **Received unexpected event EV\_ACTIVATE\_NEW\_SA in state AM\_TM\_INIT\_XAUTH** (Получено непредвиденное событие EV\_ACTIVATE\_NEW\_SA в состоянии AM\_TM\_INIT\_XAUTH).

Проверьте правильность пароля.

- Неправильное имя пользователя:

Для маршрутизатора Cisco IOS отображается информация, аналогичная информации при вводе неправильного пароля. Для концентратора VPN отображается следующее **Authentication rejected: Reason = User was not found** (Аутентификация отклонена: Причина = Пользователь не найден).

## Дополнительные сведения

- [Страница поддержки концентратора VPN Cisco серии 3000](#)
- [Cisco Easy VPN Remote Phase II](#)
- [Страница поддержки клиента Cisco VPN 3000](#)
- [Страница поддержки согласования IPsec/протоколов IKE](#)
- [Cisco Systems — техническая поддержка и документация](#)

---

© 1992-2010 Cisco Systems, Inc. Все права защищены.

---

Дата генерации PDF файла: Jan 05, 2010

---

[http://www.cisco.com/support/RU/customer/content/10/107614/vpn\\_ios\\_ezvpn.shtml](http://www.cisco.com/support/RU/customer/content/10/107614/vpn_ios_ezvpn.shtml)

---