Устранение наиболее распространенных неполадок удаленных VPN-подключений и VPN-туннелей ЛВС-ЛВС на базе протокола IPSec

Содержание

Введение

В этом документе описываются стандартные решения проблем VPN-подключений на базе протокола IPsec. Эти решения были разработаны непосредственно в ходе выполнения запросов на обслуживание, полученных и обработанных службой технической поддержки Cisco. Многие из этих решений могут быть реализованы до выполнения детальной диагностики VPN-соединения IPsec. В результате этот документ представлен в качестве контрольного списка распространенных процедур, которые необходимо попробовать выполнить до устранения неполадок в соединении и вызова службы технической поддержки Cisco.

Если необходимы документы с примерами для VPN типа "сеть-сеть" и VPN удаленного доступа, см. разделы *VPN-подключения удаленного доступа, VPN-туннели "сеть-сеть" (ЛВС-ЛВС) на базе PIX, VPN-туннели "сеть-сеть" (ЛВС-ЛВС) на базе ПО IOS)* и *VPN-туннели "сеть-сеть" (ЛВС-ЛВС) на базе VPN3000* документа Примеры и технические примечания к настройке.

Примечание: Хотя в этом документе приведены примеры по использованию маршрутизаторов и устройств защиты, практически все эти концепции можно также применить для концентраторов VPN 3000.

Примечание: Описание работы наиболее распространенных команд отладки, используемых для устранения неполадок в работе IPsec для ПО Cisco IOS® и PIX, см. в документе Устранение неполадок протокола IPsec - общие сведения и использование команд отладки.

Примечание: Любые команды, используемые в этом документе, можно найти с помощью средства поиска команд Command Lookup(только для зарегистрированных клиентов).

 **Предупреждение:** Использование многих решений, представленных в настоящем документе, может привести к временной потере возможности VPN-подключения IPsec на устройстве. При применении этих решений рекомендуется соблюдать осторожность и требования политики контроля изменений.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с содержанием следующих разделов.

- Настройка IPsec VPN на устройствах Cisco:
    - Устройства защиты Cisco PIX серии 500
    - Устройства защиты Cisco ASA серии 5500
    - Маршрутизаторы Cisco IOS®
    - Концентраторы семейства VPN 3000 (необязательно)

Используемые компоненты

Сведения, содержащиеся в данных документах, касаются следующих версий программного и аппаратного обеспечения:

- Устройства защиты Cisco серии ASA 5500
- Устройства защиты Cisco серии PIX 500
- Cisco IOS

Сведения в этом документе были получены в результате тестирования приборов в специфической лабораторной среде. Все устройства, используемые в этом документе, запускались с чистой конфигурацией (конфигурацией по умолчанию). Если ваша сеть работает в реальных условиях, убедитесь, что вы понимаете потенциальное воздействие каждой команды.

Условные обозначения

Более подробные сведения о применяемых в документе обозначениях см. в документе Cisco Technical Tips Conventions (Условные обозначения, используемые в технической документации Cisco).

Проблема: сбой в работе настройки IPSec VPN

Недавно настроенное или измененное решение IPsec VPN не функционирует.

Текущая конфигурация IPsec VPN более не функционирует.

Решения

В этом разделе описываются решения наиболее распространенных проблем с IPsec VPN. Хотя порядок, в котором перечислены решения, не имеет особого значения, список можно использовать в качестве контрольного списка для проверки или тестирования до выполнения детальной диагностики и вызова TAC. Все эти решения получены в процессе обработки запросов к службе TAC и использовались для устранения неполадок на стороне клиентов.

Примечание: Некоторые из этих команд были перемещены на вторую строку из-за нехватки пространства.

Включение обхода NAT (проблема #1 RA VPN)

NAT-Traversal, или NAT-T, обеспечивает трафику VPN возможность прохождения через устройства NAT или PAT, таких как маршрутизатор Linksys SOHO. Если функция NAT-T не включена, часто возникает видимость стабильного подключения VPN-клиентов к PIX или ASA, однако при этом они не могут получить доступ к внутренней сети за устройством защиты.

Примечание: В IOS 12.2(13)T и более поздних версиях NAT-T по умолчанию включен в IOS.

Ниже приведена команда для включения NAT-T на устройстве защиты Cisco. Значение 20 в этом примере означает период сообщения/запроса keepalive (заданный по умолчанию).

PIX/ASA версия 7.1 и более ранние

```
pix(config)#isakmp nat-traversal 20
```

PIX/ASA версия 7.2 и более поздние

```
securityappliance(config)#crypto isakmp nat-traversal 20
```

Примечание: Эта команда используется и для PIX 6.x, и для PIX/ASA 7.x.

Примечание: Важно разрешить использование протокола UDP 4500 для портов NAT-T, UDP 500, TCP 10000 ESP путем настройки ACL, поскольку PIX/ASA функционирует как устройство NAT . Для получения дополнительных сведений о настройке ACL в PIX/ASA см. документ Настройка туннеля IPsec через брандмауэр с преобразованием сетевых адресов.

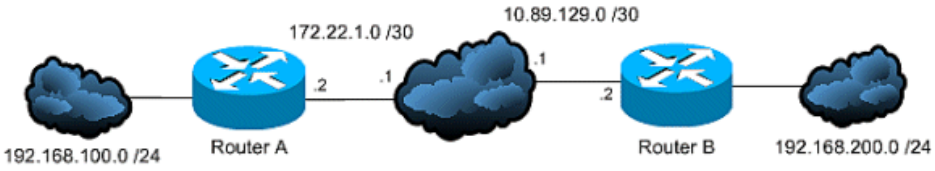
Концентратор VPN

Выберите **Configuration > Tunneling и Security >IPSEC >NAT Transparency > Enable: *IPsec over NAT-T*** , чтобы отключить NAT-T на концентраторе VPN.

Примечание: NAT-T также обеспечивает возможность одновременного подключения нескольких VPN-клиентов с использованием устройства PAT к любому головному узлу, независимо от того, является ли таким узлом PIX, маршрутизатор или концентратор.

Правильная проверка возможности подключения

При идеальных условиях возможность VPN-подключения тестируется с устройств за оконечными точками, выполняющих шифрование. При этом многие пользователи могут проверить возможность VPN-подключения, выполнив команду **ping** на устройствах, выполняющих шифрование. Команда **ping** вполне подходит для выполнения этой задачи, однако важно отправить эту команду с соответствующего интерфейса. Если источник **ping** выбран неправильно, может отобразиться сбой VPN-подключения, тогда как в действительности подключение было успешно установлено. Рассмотрим для примера следующий вариант:



Маршрутизатор A с ACL шифрования

```
access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
```

Маршрутизатор B с ACL шифрования

```
access-list 110 permit ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255
```

В этой ситуации команда **ping** должна быть отправлена из "внутренней" сети за одним из маршрутизаторов. Причина в том, что ACL шифрования настроены только для шифрования трафика с использованием этих исходных адресов. Команда **ping** , отправленная с внешнего интерфейса (со стороны Интернета) одного из маршрутизаторов, не шифруется. Используйте расширенные параметры команды **ping** в привилегированном режиме EXEC для отправки команды ping от "внутреннего" интерфейса маршрутизатора:

```
routerA#ping
Protocol [ip]:
Target IP address: 192.168.200.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
   Source address or interface: 192.168.100.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.100.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Представьте, что маршрутизаторы на этой схеме заменили устройствами защиты PIX или ASA. Команда **ping** , используемая для тестирования возможности подключения, может быть также отправлена с внутреннего интерфейса с помощью ключевого слова **inside** :

```
securityappliance#ping inside 192.168.200.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Примечание: Не рекомендуется выбирать внутренний интерфейс устройства защиты в качестве целевого объекта команды **ping**. Если необходимо выбрать внутренний интерфейс в качестве целевого объекта команды **ping**, необходимо включить **management-access** для этого интерфейса, иначе устройство не сможет ответить.

```
securityappliance(config)#management-access inside
```

Включение ISAKMP

Если отсутствует указание на использование VPN-туннеля IPsec, причина может заключаться в том, что ISAKMP не был активирован. Убедитесь, что для всех устройств включена поддержка ISAKMP. Используйте одну из этих команд, чтобы включить на устройствах поддержку ISAKMP:

- Cisco IOS

```
router(config)#crypto isakmp enable
```

- Cisco PIX 7.1 и более ранние версии (замените **outside** на необходимый интерфейс)

```
pix(config)#isakmp enable outside
```

- Cisco PIX/ASA 7.2(1) и более поздние версии (замените **outside** на необходимый интерфейс)

```
securityappliance(config)#crypto isakmp enable outside
```

Включение/отключение безопасной пересылки (PFS)

При согласовании IPsec безопасная пересылка (PFS) позволяет гарантировать отсутствие связи нового ключа шифрования со всеми предыдущими ключами. Необходимо включить или отключить PFS для обеих конечных точек туннеля; в противном случае не удастся создать IPsec-туннель ЛВС-ЛВС на маршрутизаторе PIX/ASA/IOS.

PIX/ASA:

По умолчанию безопасная пересылка (PFS)отключена. Чтобы включить PFS воспользуйтесь командой **pfs** с ключевым словом enable (в режиме настройки групповой политики). Чтобы отключить PFS, введите ключевое слово disable.

```
hostname(config-group-policy)#pfs {enable | disable}
```

Чтобы удалить атрибут PFS из текущей конфигурации, введите эту команду с ключом "no". Групповая политика может наследовать значение PFS из другой групповой политики. Введите эту команду с ключом "no", чтобы предотвратить наследование значения.

```
hostname(config-group-policy)#no pfs
```

Маршрутизатор IOS:

Чтобы указать, что протокол IPsec должен запрашивать PFS при запросе новых сопоставлений безопасности для текущей записи криптокарты либо что IPsec должен запрашивать PFS при получении запросов на новые сопоставления безопасности, используйте команду **set pfs** в режиме настройки криптокарты. Если необходимо, чтобы IPsec не запрашивал PFS, используйте эту команду с ключом "no". По умолчанию PFS не запрашивается. Если при использовании этой команды группа не указана, по умолчанию будет использоваться group1.

```
set pfs [group1 | group2]
no set pfs
```

Для команды set pfs:

- group1 — указывает, что во время нового обмена ключами по схеме Диффи-Хеллмана следует использовать 768-битную группу Диффи-Хеллмана по простому модулю.
- group2 — указывает, что во время нового обмена ключами по схеме Диффи-Хеллмана следует использовать 1024-битную группу Диффи-Хеллмана по простому модулю.

Пример:

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#set pfs group2
```

Очистка предыдущих и существующих сопоставлений безопасности (туннелей)

Если это сообщение об ошибке возникает на маршрутизаторе IOS, проблема заключается в истечении срока или очистке SA. Удаленный туннель конечного устройства не распознает данные об использовании устаревшего SA для отправки пакета (не пакета создания SA). При создании нового сопоставления безопасности выполняется возобновление связи, поэтому необходимо инициировать передачу *содержательного* трафика по туннелю для создания нового сопоставления безопасности и повторного создания туннеля.

```
%CRYPTO-4-IKMP_NO_SA: IKE message from x.x.x.x  has no SA
```

Очистка сопоставлений безопасности ISKAMP (этап I) и IPsec (этап II) - это самый простой и чаще всего оптимальный способ решения проблем с IPsec VPN.

При очистке SA часто устраняется большое количество сообщений об ошибках и сбоев без необходимости проведения диагностики. Хотя этот метод можно легко использовать в любой ситуации, практически всегда необходимо выполнение требования по очистке сопоставлений безопасности после изменений или добавлений к текущей конфигурации IPsec VPN. Более того, хотя поддерживается возможность очистки только определенного сопоставления безопасности, наибольшими преимуществами можно воспользоваться при глобальной очистке SA на устройстве.

Примечание: После очистки сопоставлений безопасности может возникнуть необходимость в отправке трафика по туннелю для их повторной установки.

 **Предупреждение:** Если не указать нужные для очистки сопоставления безопасности, перечисленные здесь команды могут привести к очистке всех сопоставлений безопасности устройства. Соблюдайте осторожность, если используются другие туннели IPsec VPN.

1. До очистки сопоставлений безопасности их необходимо просмотреть

    1. **Cisco IOS**

```
router#show crypto isakmp sa
router#show crypto ipsec sa
```

    2. **Cisco PIX/ASA Security Appliance**

```
securityappliance#show crypto isakmp sa
securityappliance#show crypto ipsec sa
```

    Примечание: Для Cisco PIX 6.x и PIX/ASA 7.x используются эти же команды

2. Очистка сопоставлений безопасности. Каждую команду можно ввести как показано (выделение полужирным шрифтом), или ввести с указанными для них параметрами.

    1. **Cisco IOS**

        1. **ISAKMP (Этап I)**

```
router#clear crypto isakmp ?
 <0 - 32766>  connection id of SA
 <cr>
```

        2. **IPsec (Этап II)**

```
router#clear crypto sa ?
 counters  Reset the SA counters
 map       Clear all SAs for a given crypto map
 peer      Clear all SAs for a given crypto peer
 spi       Clear SA by SPI
 <cr>
```

    2. **Cisco PIX/ASA Security Appliance**

        1. **ISAKMP (Этап I)**

```
securityappliance#clear crypto isakmp sa
```

        2. **IPsec (Этап II)**

```
security appliance#clear crypto ipsec sa ?

 counters  Clear IPsec SA counters
 entry     Clear IPsec SAs by entry
 map       Clear IPsec SAs by map
 peer      Clear IPsec SA by peer
 <cr>
```

Проверка жизненного цикла ISAKMP

Если при использовании туннеля ЛВС-ЛВС часто происходят разрывы соединений, проблема может заключаться в меньшем, чем нужно, значении жизненного цикла, настроенного в SA ISAKMP.

По умолчанию задается значение, равное 86400 секундам или 24 часам. Как правило, если указан более короткий жизненный цикл, то при этом обеспечивается более безопасное согласование ISAKMP (до определенного предела), но при заданном более коротком жизненном цикле устройство защиты быстрее настраивает будущие сопоставления безопасности IPsec.

Совпадение выбирается в тех случаях, когда обе политики двух одноранговых узлов содержат одинаковые значения шифрования, хеша, аутентификации и параметра Диффи-Хеллмана, а также когда в политике удаленного узла указывается значение жизненного цикла, меньшее или равное аналогичному значению сравниваемой политики. Если значения жизненного цикла не идентичны, используется меньшее значение жизненного цикла из политики удаленного узла. Если не удается найти приемлемых совпадений, IKE отклоняет согласование и сопоставление безопасности по протоколу IKE не устанавливается.

Укажите значение для жизненного цикла SA. В этих примерах задается значение. равное 4 часам (14400 секундам). Значение по умолчанию составляет 86400 секунд (24 часов).

PIX/ASA

```
hostname(config)#isakmp policy 2 lifetime  14400
```

Маршрутизатор IOS

```
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#lifetime 86400
```

Включите или отключите запросы keepalive ISAKMP

Настройка запросов keepalive ISAKMP позволяет предотвратить периодические разрывы VPN-соединений удаленного доступа или ЛВС-ЛВС, к которым относятся соединения на базе VPN-клиентов, VPN-туннели и туннели, соединение по которым разрывается по истечении заданного времени неактивности. Эта функция обеспечивает для конечной точки туннеля возможность отслеживания постоянного присутствия удаленного узла и отправки отчетов о собственном присутствии этому узлу. Если узел не отвечает на запросы, конечная точка удаляет соединение. Для обеспечения поддержки запросов keepalive для ISAKMP необходимо, чтобы их поддерживали обе конечные точки VPN.

- Настройте в IOS поддержку запросов keepalive ISAKMP с помощью этой команды:

```
router(config)#crypto isakmp keepalive 15
```

- Используйте эти команды для настройки запросов keepalive ISAKMP для устройств защиты PIX/ASA:
  - Cisco PIX 6.x

```
pix(config)#isakmp keepalive 15
```

  - В Cisco PIX/ASA 7.x и более поздних версиях для группы туннелей с именем **10.165.205.222**

```
securityappliance(config)#tunnel-group 10.165.205.222
  ipsec-attributes

securityappliance(config-tunnel-ipsec)#isakmp keepalive
```

```
threshold 15 retry 10
```

В определенных ситуациях для разрешения проблемы необходимо отключить эту функцию (например в случаях, когда VPN-клиент находится за брандмауэром, предотвращающим передачу DPD-пакетов).

В Cisco PIX/ASA 7.x и более поздних версиях для группы туннелей с именем **10.165.205.222**

Отключает включенную в IKE по умолчанию обработку запросов keepalive.

```
securityappliance(config)#tunnel-group 10.165.205.222
  ipsec-attributes

securityappliance(config-tunnel-ipsec)#isakmp keepalive
     disable
```

Отключение запросов keepalive для VPN-клиента 4.x Cisco

Выберите **%System Root% > Program Files > Cisco Systems >VPN-клиент > Profiles** на клиентском ПК, в работе которого произошел сбой, чтобы отключить запросы keepalive, и при необходимости измените **файл PCF** для данного соединения.

Замените **'ForceKeepAlives=0'** (по умолчанию) на **'ForceKeepAlives=1'**.

Повторно введите или восстановите предварительные ключи

Во многих случаях причиной нерабочего состояния VPN-туннеля IPsec может быть простая опечатка. Например, на устройствах защиты предварительные ключи после ввода скрываются. Из-за этого невозможно увидеть, правильно ли вводится ключ.**Убедитесь, что для всех конечных точек VPN предварительные ключи введены правильно.** Повторно введите ключ, чтобы убедиться, что это правильный ключ; это простое решение позволяет избежать детального устранения неполадок.

В VPN удаленного доступа убедитесь, что в VPN-клиенте Cisco введены действительные имя группы и предварительный ключ. Эта ошибка может возникнуть, если имя группы/предварительный ключ, указанные для VPN-клиента и головного устройства, не совпадают.

```
1 12:41:51.900 02/18/06 Sev=Warning/3 IKE/0xE3000056
The received HASH payload cannot be verified 2 12:41:51.900 02/18/06 Sev=Warning/2 IKE/0xE300007D
Hash verification failed
```

Предварительный ключ также можно восстановить без внесения изменений в конфигурацию устройства защиты PIX/ASA. См. PIX/ASA 7.x и более поздние версии: восстановление предварительного ключа.

 **Предупреждение:** При удалении команд шифрования возникает высокая вероятность отключения одного или всех VPN-туннелей. Соблюдайте осторожность при работе с этими командами и просмотрите политику контроля изменений до выполнения следующих действий.

- Используйте эти команды для удаления и повторного ввода предварительного ключа **secretkey** для узла **10.0.0.1** или группы **vpngroup** в IOS:
    - Cisco VPN (ЛВС-ЛВС)

```
router(config)#no crypto isakmp key secretkey
  address 10.0.0.1
router(config)#crypto isakmp key secretkey
  address 10.0.0.1
```

    - Cisco VPN (удаленные подключения)

```
router(config)#crypto isakmp client configuration
  group vpngroup
router(config-isakmp-group)#no key secretkey
router(config-isakmp-group)#key secretkey
```

- Используйте эти команды для удаления и повторного ввода **secretkey** для узла **10.0.0.1** на устройстве защиты PIX/ASA:
  - Cisco PIX 6.x

```
pix(config)#no isakmp key secretkey address 10.0.0.1
pix(config)#isakmp key secretkey address 10.0.0.1
```

  - Cisco PIX/ASA 7.x и более поздние версии

```
securityappliance(config)#tunnel-group 10.0.0.1
  ipsec-attributes
securityappliance(config-tunnel-ipsec)#no pre-shared-key
securityappliance(config-tunnel-ipsec)#pre-shared-key
  secretkey
```

Удаление и замена криптокарт

Если после очистки сопоставления безопасности проблема с IPsec VPN не устраняется, удалите и замените соответствующую криптокарту для устранения более широкого круга проблем.

 **Предупреждение:** При удалении криптокарты из интерфейса происходит **полное** отключение всех туннелей IPsec, связанных с этой криптокартой. Будьте внимательны при выполнении этих действий и, прежде чем продолжать, выполните все требования политики контроля изменений, используемой в вашей организации.

- Чтобы удалить и заменить криптокарту в IOS, воспользуйтесь следующими командами:

  Начните с удаления криптокарты из интерфейса. Используйте ключ "no" для команды **crypto map** .

```
router(config-if)#no crypto map mymap
```

  Продолжите использование ключа **no** для удаления всей криптокарты.

```
router(config)#no crypto map mymap 10
```

  Замените криптокарту в интерфейсе Ethernet0/0 для узла **10.0.0.1**. В этом примере показана настройка криптокарты с минимальными требованиями:

```
router(config)#crypto map mymap 10 ipsec-isakmp
router(config-crypto-map)#match address 101
router(config-crypto-map)#set transform-set mySET
router(config-crypto-map)#set peer 10.0.0.1
router(config-crypto-map)#exit
router(config)#interface ethernet0/0
router(config-if)#crypto map mymap
```

- Используйте эти команды для удаления и замены криптокарты в PIX или ASA:

Начните с удаления криптокарты из интерфейса. Используйте ключ "no" для команды **crypto map** .

```
securityappliance(config)#no crypto map mymap interface outside
```

Продолжите использование ключа **no** для удаления других команд криптокарты.

```
securityappliance(config)#no crypto map mymap 10 match
  address 101
securityappliance(config)#no crypto map mymap set
  transform-set mySET
securityappliance(config)#no crypto map mymap set
  peer 10.0.0.1
```

Замена криптокарты для узла **10.0.0.1**. В этом примере показана настройка криптокарты с минимальными требованиями:

```
securityappliance(config)#crypto map mymap 10 ipsec-isakmp
securityappliance(config)#crypto map mymap 10
  match address 101
securityappliance(config)#crypto map mymap 10 set
  transform-set mySET
securityappliance(config)#crypto map mymap 10 set
  peer 10.0.0.1
securityappliance(config)#crypto map mymap interface outside
```

Убедитесь в наличии команд sysopt (только для PIX/ASA)

Команды **sysopt connection permit-ipsec** и **sysopt connection permit-vpn** обеспечивают для пакетов от туннеля IPsec и соответствующей полезной нагрузки возможность прохождения ACL интерфейса на устройстве защиты. Если эти команды не включены, то в работе туннелей IPsec, завершающихся на устройстве защиты, вероятнее всего, произойдет сбой.

В ПО Security Appliance версии 7.0 и более ранних версиях соответствующей для этой ситуации командой sysopt является **sysopt connection permit-ipsec**.

В ПО Security Appliance версии 7.1(1) и более ранних версиях соответствующей для этой ситуации командой sysopt является **sysopt connection permit-vpn**.

В PIX 6.x это функциональность по умолчанию **отключена**. В PIX/ASA 7.0(1) и более поздних версиях эта функция **включена** по умолчанию. Используйте следующие команды show, что определить, поддерживаются ли соответствующие команды **sysopt** на вашем устройстве:

1. Cisco PIX 6.x

```
pix# show sysopt
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
no sysopt uauth allow-http-cache
no sysopt connection permit-ipsec
     !--- sysopt connection permit-ipsec is disabled

no sysopt connection permit-pptp
no sysopt connection permit-l2tp
no sysopt ipsec pl-compatible
```

2. Cisco PIX/ASA 7.x

```
securityappliance# show running-config sysopt
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt connection permit-vpn
     !--- sysopt connection permit-vpn is enabled
!--- This device is running 7.2(2)
```

Используйте следующие команды для включения необходимых команд **sysopt** для вашего устройства:

- Cisco PIX 6.x и PIX/ASA 7.0

```
pix(config)#sysopt connection permit-ipsec
```

- Cisco PIX/ASA версии 7.1(1) или более поздней

```
securityappliance(config)#sysopt connection permit-vpn
```

Проверьте идентификатор ISAKMP

Если в работе VPN-туннелей IPsec произошел сбой при согласовании IKE, причина сбоя может заключаться в PIX или в том, что один узел не может распознать идентификатор другого узла. Если два узла используют IKE для настройки сопоставлений безопасности IPsec , каждый узел отправляет идентификатор ISAKMP удаленному узлу. Он отправляет или IP-адрес, или имя сервера, в зависимости от настройки идентификатора ISAKMP каждого параметра. По умолчанию идентификатор ISAKMP брандмауэра PIX настраивается на IP-адрес. Как правило, настройка устройства защиты и идентификаторов его узлов выполняется с использованием одного метода для избежания возникновения сбоев при согласовании IKE.

Чтобы настроить отправку идентификатора этапа 2 узлу, используйте **команду isakmp identity** в глобальном режиме конфигурации

```
isakmp identity address
!--- If the RA or L2L (site-to-site) VPN tunnels connect with pre-shared
key as authentication type
```

ИЛИ

```
isakmp identity hostname
!--- If the RA or L2L (site-to-site) VPN tunnels connect with digital
certificate as authentication type
```

Проверьте время ожидания простоя

Если для времени ожидания простоя задано значение 30 минут (по умолчанию), это означает, что туннель отбрасывается после 30 минут без прохождения трафика. Клиент VPN отключается через 30 минут независимо от настроек времени ожидания простоя и возникает ошибка `PEER_DELETE-IKE_DELETE_UNSPECIFIED`.

Если необходимо, чтобы туннель всегда находился в рабочем состоянии, измените настройки и задайте параметр **неограниченное**,

чтобы избежать отбрасывания туннелей:

PIX/ASA версия 7.x и более поздние

```
group-policy DfltGrpPolicy attributes
vpn-idle-timeout none
```

Маршрутизатор IOS

Для настройки таймера ожидания IPsec SA используйте команду **crypto ipsec security-association idle-time** в режиме глобальной настройки или в режиме конфигурирования криптокарты. По умолчанию таймеры ожидания IPsec SA отключены.

```
crypto ipsec security-association idle-time
seconds
```

Время в *секундах*, которое таймер ожидания предоставляет неактивному узлу для поддержания сопоставления безопасности. Допустимые значения аргумента времени в секундах - в диапазоне от 60 до 86400.

Убедитесь, что указаны правильные ACL

В стандартной конфигурации IPsec VPN используются два списка доступа. Один список доступа используется для освобождения трафика, предназначенного для VPN-туннеля от процесса NAT. В другом списке доступа определяется трафик для шифрования; сюда относится ACL шифрования в конфигурациях ЛВС-ЛВС и раздельное туннелирование ACL в конфигурациях удаленного доступа. В случае неправильной настройки или отсутствия этих ACL поддерживается только одно направление трафика в VPN-туннеле, при этом также может сложиться ситуация, при которой трафик не сможет проходить через туннель.

Убедитесь, что настроены все списки доступа, необходимые для завершения настройки IPsec VPN и что в этих списках определен соответствующий тип трафика. В списке содержатся указания для проверки, если предполагается, что ACL является причиной проблемы в работе IPsec VPN.

- Убедитесь,что в списке контроля доступа (ACL) без трансляции сетевых адресов и в ACL криптокарты указан верный трафик.
- Если используется несколько VPN-туннелей и ACL шифрования, убедитесь, что эти списки доступа не перекрывают друг друга.
- Не используйте ACL дважды. Даже если в списке контроля доступа (ACL) без трансляции сетевых адресов и в ACL шифрования указан один и тот же трафик, необходимо использовать два различных списка доступа.
- Убедитесь,что устройство настроено для использования списка контроля доступа без трансляции сетевых адресов. Для маршрутизаторов это означает использование команды **route-map** . Для модулей PIX или ASA, это означает использование команды **nat (0)** . Список контроля доступа без трансляции сетевых адресов необходим для конфигураций удаленного доступа или ЛВС-ЛВС.
    - В этом случае маршрутизатор IOS настраивается для освобождения трафика, передаваемого между **192.168.100.0 /24** и **192.168.200.0 /24** или **192.168.1.0 /24** от NAT. Трафик, передаваемый в другие точки назначения, обрабатывается с помощью перегрузки NAT:

```
access-list 110 deny ip 192.168.100.0 0.0.0.255
  192.168.200.0 0.0.0.255
access-list 110 deny ip 192.168.100.0 0.0.0.255
  192.168.1.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255 any

route-map nonat permit 10
 match ip address 110

ip nat inside source route-map nonat interface FastEthernet0/0 overload
```

- В этом случае PIX настраивается для освобождения трафика, передаваемого между **192.168.100.0 /24** и **192.168.200.0 /24** или **192.168.1.0 /24** от NAT. Например, весь остальной трафик обрабатывается с использованием перегрузки NAT:

```
access-list noNAT extended permit ip 192.168.100.0
  255.255.255.0 192.168.200.0 255.255.255.0
access-list noNAT extended permit ip 192.168.100.0
  255.255.255.0 192.168.1.0 255.255.255.0

nat (inside) 0 access-list noNAT
nat (inside) 1 0.0.0.0 0.0.0.0

global (outside) 1 interface
```

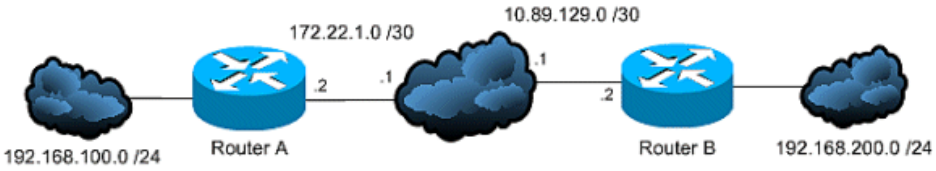
Примечание: Списки контроля доступа без трансляции сетевых адресов могут использоваться только для IP-адресов или IP-сетей, упомянутых в примерах (access-list noNAT), и должны совпадать с ACL шифрования. Списки контроля доступа без трансляции сетевых адресов не применяются для номеров портов (например 23, 25 и т.д.).

Примечание: Пример неправильной конфигурации:

```
access-list noNAT extended permit ip 192.168.100.0
  255.255.255.0 192.168.200.0 255.255.255.0 eq 25
```

- Убедитесь,что ACL не направлены в обратную сторону и имеют правильный тип.

- Список контроля доступа без трансляции сетевых адресов и список контроля доступа криптокарты для конфигураций ЛВС-ЛВС должны быть записаны с точки зрения устройства, на котором настроен список. Это означает, что ACL должны **зеркально** отражать друг друга. В этом примере настроен туннель ЛВС-ЛВС между **192.168.100.0 /24** и **192.168.200.0 /24**.



Маршрутизатор A с ACL шифрования

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
  192.168.200.0 0.0.0.255
```

Маршрутизатор B с ACL шифрования

```
access-list 110 permit ip 192.168.200.0 0.0.0.255
  192.168.100.0 0.0.0.255
```

Примечание: Эта же концепция применяется для устройств защиты PIX и ASA, хотя такие примеры и не включены в данный документ.

- Настройки списков управления доступом для раздельного туннелирования и конфигураций удаленного доступа должны включать **стандартные** списки доступа, разрешающие передачу трафика для сетей, доступ к которым необходим для VPN-клиентов.

Примечание: В расширенном списке доступа использование параметра **'any'** в исходных настройках списка управлением доступом для раздельного туннелирования аналогично отключению раздельного туннелирования. Используйте только исходные сети в расширенном списке управления доступом для раздельного туннелирования.

Примечание: Пример правильной конфигурации:

```
access-list 140 permit ip 10.1.0.0 0.0.255.255 10.18.0.0 0.0.255.255
```

Примечание: Пример неправильной конфигурации:

```
access-list 140 permit ip any 10.18.0.0 0.0.255.255
```

- Cisco IOS

```
router(config)#access-list 10 permit ip 192.168.100.0
router(config)#crypto isakmp client configuration group MYGROUP
router(config-isakmp-group)#acl 10
```

- Cisco PIX 6.x

```
pix(config)#access-list 10 permit 192.168.100.0
  255.255.255.0
pix(config)#vpngroup MYGROUP split-tunnel 10
```

- Cisco PIX/ASA 7.x

```
securityappliance(config)#access-list 10 standard
  permit 192.168.100.0 255.255.255.0
securityappliance(config)#group-policy MYPOLICY internal
securityappliance(config)#group-policy MYPOLICY attributes
securityappliance(config-group-policy)#split-tunnel-policy
  tunnelspecified
securityappliance(config-group-policy)#split-tunnel-network-list
  value 10
```

Проверьте политики ISAKMP

Если туннель IPsec не находится в рабочем состоянии, убедитесь, что политики ISAKMP соответствуют удаленным узлам. Эта политика ISAKMP применима как для VPN-конфигураций IPsec "сеть-сеть" (ЛВС-ЛВС), так и для IPsec VPN удаленного доступа.

Если VPN-клиенты Cisco или VPN типа "сеть-сеть" не могут установить туннель к удаленному устройству, убедитесь, что **два узла содержат одни и те же значения шифрования, хеша, аутентификации и параметра Диффи-Хеллмана,** а также убедитесь, что в политике удаленных узлов для жизненного цикла указано значение, меньшее или равное аналогичному значению в политике, отправленной инициатором. Если значения жизненных циклов не совпадают, то устройство защиты использует меньшее значение. Если не удается найти приемлемых совпадений, ISAKMP отклонит согласование и SA не будет установлено.

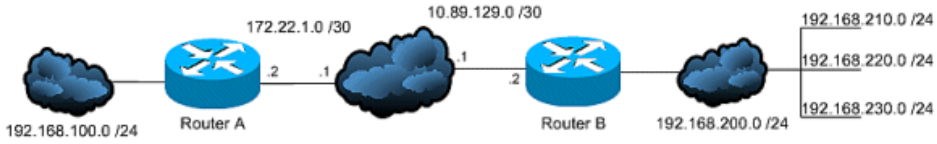
Примечание: С политикой ISAKMP и набором для преобразования, используемыми в PIX/ASA, VPN-клиент Cisco не может применять политику, комбинирующую DES и SHA. При использовании DES необходимо применить MD5 для алгоритма хеширования или можно воспользоваться другими комбинациями: 3DES и SHA или 3DES и MD5.

Убедитесь, что маршрутизация настроена правильно

Маршрутизация — это важная часть любого развертывания IPsec VPN. Убедитесь, что для устройств шифрования, таких как маршрутизаторы и устройства защиты PIX или ASA предоставлены правильные данные маршрутизации для передачи трафика по туннелю VPN. Более того, если за устройством шлюза существуют другие маршрутизаторы, убедитесь, что для этих маршрутизаторов настроены параметры связи с туннелем и предоставлены данные о сетях на другой стороне.

Одним из ключевых компонентов маршрутизации при развертывании VPN является функция обратного ввода трафика (RRI). RRI размещает динамические записи для удаленных сетей или VPN-клиентов в таблице маршрутизации шлюза VPN. Эти маршруты используются для устройства, на котором они установлены, а также для других устройств в сети, поскольку маршруты, установленные RRI, можно перераспределить с помощью такого протокола маршрутизации, как EIGRP или OSPF.

- При использовании конфигурации ЛВС-ЛВС важно настроить для каждой конечной точки маршруты к сети, для которых предполагается выполнять шифрование трафика. В этом примере для Маршрутизатора A необходимо настроить маршруты к сетям за Маршрутизатором B через **10.89.129.2**. Маршрутизатор B должен иметь схожий маршрут к **192.168.100.0 /24**:



  - Первый способ предоставления каждому маршрутизатору соответствующих маршрутов заключается в настройке статических маршрутов для каждой сети назначения. Например, для Маршрутизатора A можно настроить следующие инструкции маршрутов:

```
ip route 0.0.0.0 0.0.0.0 172.22.1.1
ip route 192.168.200.0 255.255.255.0 10.89.129.2
ip route 192.168.210.0 255.255.255.0 10.89.129.2
ip route 192.168.220.0 255.255.255.0 10.89.129.2
ip route 192.168.230.0 255.255.255.0 10.89.129.2
```

    Если Маршрутизатор A был заменен PIX или ASA, то конфигурация может выглядеть следующим образом:

```
route outside 0.0.0.0 0.0.0.0 172.22.1.1
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
```

  - Если за каждой конечной точкой существует большое количество сетей, конфигурацию статических маршрутов трудно обслуживать. Вместо этого рекомендуется использовать внесение обратного маршрута в соответствии с приведенным описанием. RRI помещает в таблицу маршрутизации маршруты для всех удаленных сетей, указанных в ACL шифрования. Например, ACL шифрования и криптокарта Маршрутизатора A может выглядеть следующим образом:

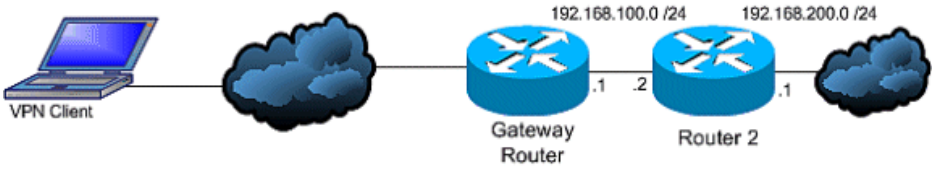
```
access-list 110 permit ip 192.168.100.0 0.0.0.255
  192.168.200.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
  192.168.210.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
  192.168.220.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
  192.168.230.0 0.0.0.255

crypto map myMAP 10 ipsec-isakmp
set peer 10.89.129.2
 reverse-route
set transform-set mySET
match address 110
```

    Если Маршрутизатор A был заменен PIX или ASA, то конфигурация может выглядеть следующим образом:

```
access-list cryptoACL extended permit ip 192.168.100.0
  255.255.255.0 192.168.200.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
  255.255.255.0 192.168.210.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
  255.255.255.0 192.168.220.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
  255.255.255.0 192.168.230.0 255.255.255.0
```

```
crypto map myMAP 10 match address cryptoACL
crypto map myMAP 10 set peer 10.89.129.2
crypto map myMAP 10 set transform-set mySET
crypto map mymap 10 set reverse-route
```

- В конфигурации удаленного доступа изменения маршрутизации не всегда являются обязательными. Однако если за шлюзом VPN или средством Security Appliance имеются другие маршрутизаторы, эти маршрутизаторы должны каким-то образом получить данные о пути к VPN-клиентам. В этом примере для VPN-клиентов были указаны адреса в диапазоне **10.0.0.0 /24** при подключении.



Если между шлюзом и другим маршрутизатором(ами) не используется протокол маршрутизации, то для маршрутизаторов, таких как Маршрутизатор 2, можно использовать статические маршруты:

```
ip route 10.0.0.0 255.255.255.0 192.168.100.1
```

Если между шлюзом и другими маршрутизаторами используется протокол маршрутизации, такой как EIGRP или OSPF, рекомендуется использовать внесение обратного маршрута в соответствии с приведенным описанием. RRI автоматически добавляет маршруты для VPN-клиента к таблице маршрутизации шлюза. После этого эти маршруты можно распределить для других маршрутизаторов в сети.

  - Маршрутизатор IOS Cisco:

```
crypto dynamic-map dynMAP 10
set transform-set mySET
 reverse-route

crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

  - Cisco PIX или ASA Security Appliance:

```
crypto dynamic-map dynMAP 10 set transform-set mySET
crypto dynamic-map dynMAP 10 set reverse-route

crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

Примечание: Проблема с маршрутизацией возникает в том случае, когда происходит перекрытие пула IP-адресов, назначенных для VPN-клиентов, с внутренними сетями головного устройства. Для получения дополнительных сведений см. раздел Перекрытие в частных сетях.

Убедитесь,что задан правильный набор для преобразования

Убедитесь, что для шифрования и хеширования IPsec используются одни и те же алгоритмы. Для получения дополнительных сведений см. справочник команд руководства по настройке Cisco Security Appliance.

Примечание: С политикой ISAKMP и набором для преобразования, используемыми в PIX/ASA, VPN-клиент Cisco не может применять политику, комбинирующую DES и SHA. При использовании DES необходимо применить MD5 для алгоритма хеширования или можно воспользоваться другими комбинациями: 3DES и SHA или 3DES и MD5.

Проверьте порядковые номера и имя криптокарты

Если статические и динамические узлы настроены на одной криптокарте, то порядок записей криптокарты имеет первостепенное значение. Последовательный номер записи динамической криптокарты **должен** превышать номера всех других статических записей криптокарты. Если значение нумерации статических записей превышает значение нумерации динамической записи, при соединении с этими узлами произойдет ошибка.

Ниже приведен пример криптокарты с правильной нумерацией, содержащей статическую запись и динамическую запись. Обратите внимание, что динамическая запись имеет более высокий порядковый номер и оставлено место для добавления дополнительных статических записей:

```
crypto dynamic-map cisco 20 set transform-set myset
crypto map mymap 10 match address 100
crypto map mymap 10 set peer 172.16.77.10
crypto map mymap 10 set transform-set myset
crypto map mymap interface outside
crypto map mymap 60000 ipsec-isakmp dynamic cisco
```

Примечание: Имена криптокарт интерпретируются с учетом регистра символов.

Примечание: Убедитесь, что криптокарта используется в соответствующем интерфейсе, в котором начинается/заканчивается туннель IPsec.

В ситуациях, в которых туннели VPN заканчиваются в одном и том же интерфейсе, необходимо создать криптокарту с этим же именем (в одном интерфейсе может содержаться только одна криптокарта), но с другим порядковым номером. Это же условие также должно соблюдаться для маршрутизатора, PIX и ASA.

Для получения дополнительных сведений о PIX-конфигурации концентратора для той же криптокарты с другими порядковыми номерами на том же интерфейсе см. документ Настройка IPsec между концентратором и удаленными PIX с VPN-клиентом и расширенной аутентификацией. Также см. PIX/ASA 7.X : добавление нового туннеля или предоставление удаленного доступа к существующему VPN-туннелю ЛВС-ЛВС для получения дополнительных сведений о настройке криптокарт для различных вариантов использования VPN-подключений удаленного доступа и ЛВС-ЛВС.

Убедитесь, что указан правильный IP-адрес узла.

Для настройки VPN-туннеля IPsec ЛВС-ЛВС на базе PIX/ASA Security Appliance 7.x необходимо указать **<имя>**группы туннелей в качестве **IP-адреса удаленного узла** (удаленного конца туннеля) в команде **tunnel-group <name>type ipsec-l2l** для создания и управления базой данных записей о соединениях IPsec. В командах **имени группы туннелей** и **заданного адреса криптокарты** должен быть указан один и тот же IP-адрес. При настройке VPN с ASDM имена группы туннелей назначаются автоматически для правильного IP-адреса узла.

В конфигурации VPN-туннеля IPsec ЛВС-ЛВС на базе PIX 6.x IP-адрес противоположного узла (удаленного конца туннеля) должен совпадать с адресом в команде **isakmp key address** и в команде **set peer** в криптокарте для успешного создания VPN-соединения IPsec.

Отключение XAUTH для узлов соединений ЛВС-ЛВС

Если туннель ЛВС-ЛВС и VPN-туннель удаленного доступа настроены на одной криптокарте, на другой узел туннеля ЛВС-ЛВС будет отправлен запрос о данных XAUTH и в работе туннеля произойдет сбой.

Примечание: Эта проблема может возникнуть только при использовании Cisco IOS и PIX 6.x., тогда как PIX/ASA 7.x не затрагивается, поскольку в ней используются группы туннелей.

Используйте команду **no-xauth** при вводе ключа isakmp, чтобы устройство не отправляло запрос о данных XAUTH на узел (имя пользователя и пароль). Это ключевое слово отключает XAUTH для статичных узлов IPsec. Аналогичную команду введите на устройстве, на котором VPN-подключения удаленного доступа и ЛВС-ЛВС настроены на той же самой криптокарте:

```
router(config)# crypto isakmp key cisco123 address
  172.22.1.164 no-xauth
```

Если PIX/ASA 7.x выступает в роли сервера Easy VPN Server, клиент Easy VPN не может подключиться к головному узлу из-за проблемы с Xauth. Отключите в PIX/ASA аутентификацию пользователей для устранения этой проблемы следующим образом:

```
ASA(config)#tunnel-group example-group type ipsec-ra
ASA(config)#tunnel-group example-group ipsec-attributes
ASA(config-tunnel-ipsec)#isakmp ikev1-user-authentication none
```

См. раздел Прочие этого документа для получения дополнительных сведений о команде **isakmp ikev1-user-authentication** .

Проблема: пользователь с использованием удаленного доступа подключается к VPN и не имеет другого доступа к ресурсам

Пользователи удаленного доступа после подключения к VPN не имеют возможности подключения к Интернет.

Пользователи удаленного доступа не имеют доступа к ресурсам, расположенным за другими сетями VPN на этом же устройстве.

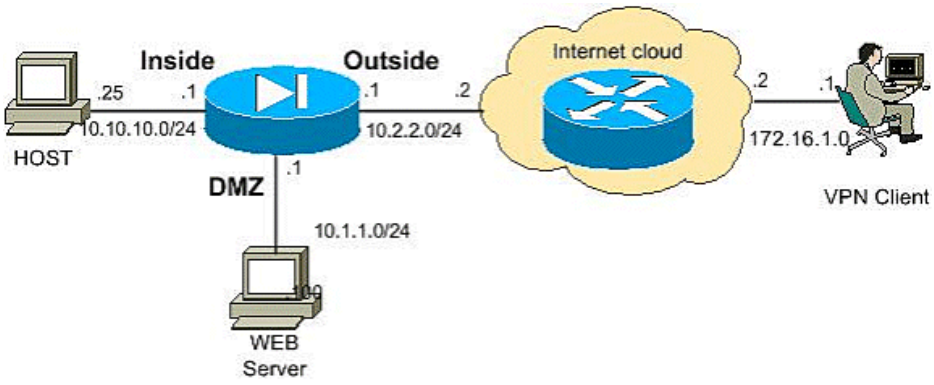
Пользователи удаленного доступа имеют доступ только к локальной сети.

Решения

Не удается получить доступ к серверам в DMZ

После того, как VPN-клиент установил туннель IPsec с использованием головного устройства VPN (маршрутизатор PIX/ASA/IOS), пользователи VPN-клиента получают доступ к ресурсам внутренней сети (10.10.10.0/24), но не имеют доступа к сети DMZ (10.1.1.0/24).
.

Схема 1 :



Убедитесь, что конфигурация NO NAT (без трансляции сетевых адресов) разделенного туннелирования добавлена в головном устройстве в сети DMZ.

Пример 1:

ASA/PIX
ciscoasa#**show running-config** *!--- Split tunnel for the* ***inside network*** *access*

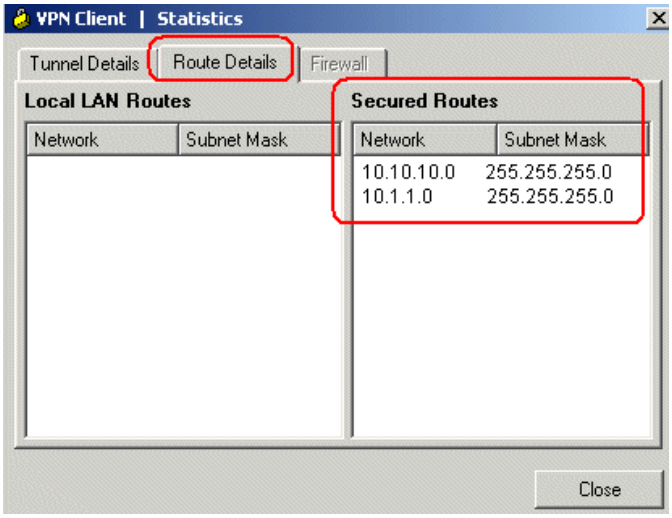
```
access-list vpnusers_spitTunnelAcl permit ip 10.10.10.0 255.255.0.0 any

!--- Split tunnel for the DMZ network access

access-list vpnusers_spitTunnelAcl permit ip 10.1.1.0 255.255.0.0 any

!--- Create a pool of addresses from which IP addresses are assigned
!--- dynamically to the remote VPN Clients.

ip local pool vpnclient 192.168.1.1-192.168.1.5

!--- This access list is used for a nat zero command that prevents
!--- traffic which matches the access list from undergoing NAT.

!--- No Nat for the DMZ network.


access-list nonat-dmz permit ip  10.1.1.0 255.255.255.0  192.168.1.0 255.255.255.0

!--- No Nat for the Inside network.

access-list nonat-in permit ip  10.10.10.0 255.255.255.0  192.168.1.0 255.255.255.0

!--- NAT 0 prevents NAT for networks specified in the ACL nonat

.
nat (DMZ) 0 access-list nonat-dmz
nat (inside) 0 access-list nonat-in
```

После добавления новой записи в настройке NAT необходимо очистить преобразование сетевых адресов.

```
Clear xlate
Clear local
```

Проверьте:

Если были настроены параметры туннеля, перейдите в **Cisco VPN Клиент** и выберите **Состояние > Маршрутизация данных,** чтобы проверить, что защищенные маршруты отображаются для сети DMZ и внутренней сети.



См. PIX/ASA 7.x: пример настройки доступа к почтовому серверу в DMZ о настройке брандмауэра PIX для обеспечения доступа к почтовому серверу, расположенному в сети демилитаризованной зоны (DMZ).

См. PIX/ASA 7.x: добавление нового туннеля или предоставление удаленного доступа к существующему VPN-туннелю ЛВС-ЛВС для ознакомления с инструкциями по прохождению всех необходимых этапов для добавления нового VPN-туннеля или удаленного VPN-доступа к существующей VPN-конфигурации ЛВС-ЛВС.

См. PIX/ASA 7.x: пример конфигурации для разрешения раздельного туннелирования для VPN-клиентов в ASA для ознакомления с

пошаговыми инструкциями по предоставлению доступа в Интернет для VPN-клиентов при их туннелировании через Cisco ASA Security Appliance серии 5500.

См. PIX/ASA Пример настройки аутентификации 7.x и VPN-клиент 4.x Cisco в Windows 2003 IAS RADIUS (в Active Directory) для настройки удаленного доступа для соединений с VPN между VPN-клиентом Cisco (4.x для Windows) и PIX Security Appliance 7.x серии 500.

VPN-клиентам не удается отправить запрос DNS

Если после настройки туннеля VPN-клиентам не удается отправить запрос DNS, проблема может заключаться в конфигурации DNS-сервера на головном устройстве (ASA/PIX). Также следует проверить возможность соединения между VPN-клиентами и DNS-сервером. Параметры DNS-сервер должны быть заданы в групповой политике и применены в групповой политике в общих атрибутах группы туннелей, например:

```
   !--- Create the group policy named vpn3000 and
!--- specify the DNS server IP address(172.16.1.1)
!--- and the domain name(cisco.com) in the group policy.

   group-policy vpn3000 internal
group-policy vpn3000 attributes
dns-server value 172.16.1.1
default-domain value cisco.com
   !--- Associate the group policy(vpn3000) to the tunnel group
!--- using the default-group-policy.

   tunnel-group vpn3000 general-attributes
default-group-policy vpn3000
```

Раздельное туннелирование

Раздельное туннелирование позволяет IPsec-клиентам, использующим удаленный доступ, условно направлять по туннелю IPsec в зашифрованном виде или напрямую пересылать пакеты интерфейсу сети в формате открытого текста и в дешифрованном виде, после чего они направляются в точку назначения. Раздельное туннелирование отключается в соответствии с настройками по умолчанию, а именно в соответствии с трафиком `tunnelall`.

```
   split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}
```

Чтобы просмотреть примеры настройки раздельного туннелирования см. следующее:

- PIX/ASA 7.x: пример настройки для обеспечения раздельного туннелирования для VPN-клиентов в ASA
- Маршрутизатор пример настройки для обеспечения возможности для VPN-клиентов подключения к IPsec и Интернет с помощью раздельного туннелирования

Прикрепление

Эту функцию можно использовать для входящего в интерфейс трафика VPN, который после этого направляется из этого интерфейса. Например, если имеется концентратор и оконечная сеть VPN, в которой устройствами защиты являются концентраторы, а удаленные сети VPN являются оконечными, для обеспечения взаимодействия между оконечными устройствами трафик должен переходить к устройству защиты, а затем к другому оконечному устройству.

Используйте команду **same-security-traffic** для обеспечения входа и выхода из одного интерфейса для трафика.

```
securityappliance(config)# same-security-traffic permit intra-interface
```

Доступ к локальной сети

Пользователи удаленного доступа подключаются к VPN и имеют доступ только к локальной сети.

Для просмотра более подробного примера настройки см. PIX/ASA 7.x: обеспечение доступа к локальной сети для VPN-клиентов.

Перекрытие в частных сетях

Если не удается получить доступ к внутренней сети после настройки туннеля, проверьте IP-адрес, назначенный VPN-клиенту, перекрывающему внутреннюю сеть за головным устройством.

Необходимо всегда проверять, относятся ли IP-адреса в пуле для VPN-клиентов и внутренняя сеть головного устройства к различным сетям. Можно назначить одну основную сеть с различными подсетями, но при этом вероятно периодическое возникновение проблем с маршрутизацией.

Для просмотра дополнительных примеров см. схема 1 и пример 1 в разделе "Невозможно получить доступ к сервером в демилитаризованной зоне".

Проблема: более чем трем пользователям VPN-клиентов не удается подключиться к PIX/ASA

Только три VPN-клиента могут подключиться к ASA/PIX; при подключении четвертого клиента происходит ошибка. При ошибке отображается следующее сообщение об ошибке:

```
Безопасное VPN-подключение разрывается локальным клиентом. Причина 413: не удалось выполнить аутентификацию пользователя.
```

Решения

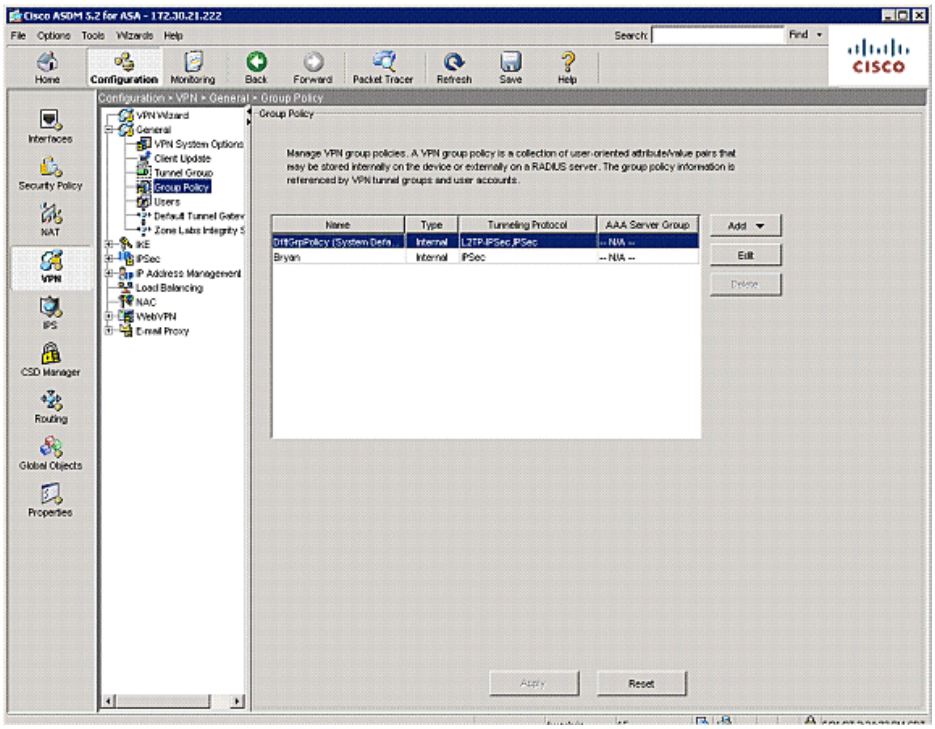
В большинстве случаев эта проблема связана с настройкой попыток одновременного входа в групповой политике. Для получения дополнительных сведений см. раздел Настройка групповых политик Выбранные процедуры настройки ASDM VPN для Cisco ASA серии 5500, версия 5.2.

Попытки одновременного входа

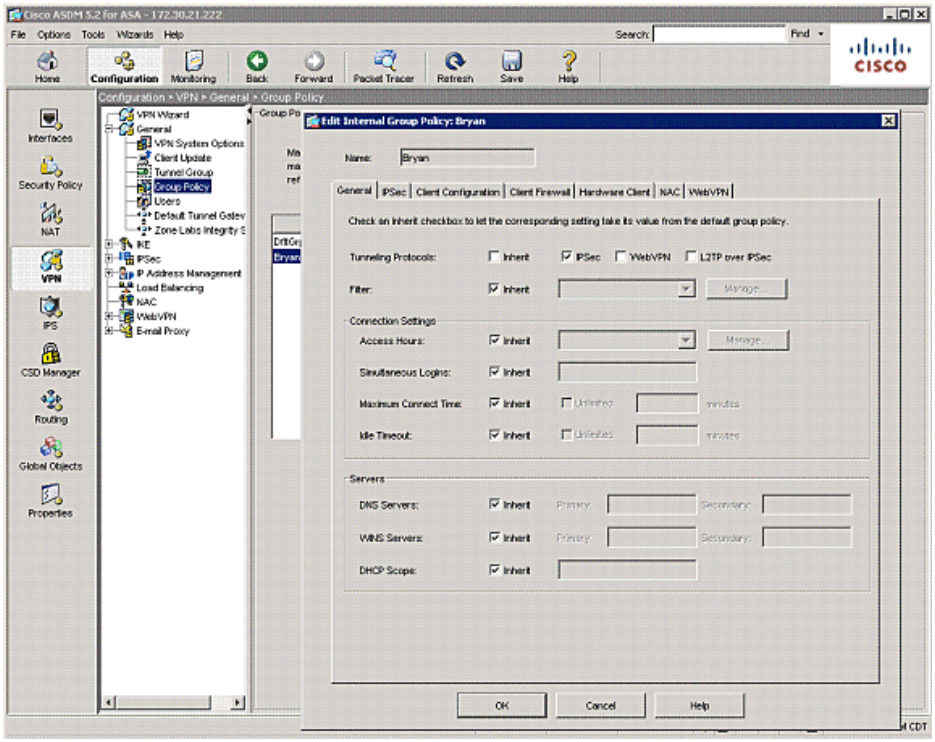
Если в ASDM установлен флажок **"Наследовать"**, то для пользователя будет поддерживаться только то количество попыток одновременного входа, которое задано по умолчанию. По умолчанию значение для попыток одновременного входа устанавливается равным трем.

Для устранения этой проблемы увеличьте значение попыток одновременного входа.

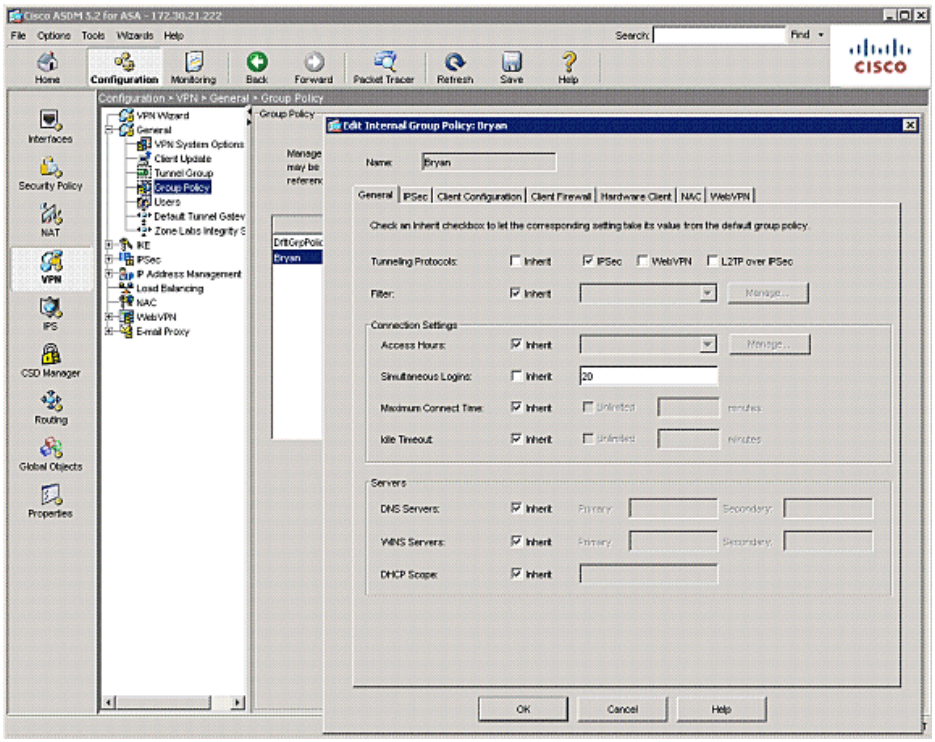
Запустите ASDM и перейдите в **Настройка > VPN > Групповая политика**.



Выберите необходимую **Группу** и щелкните кнопку **Правка**.



На вкладке **"Общие"** снимите флажок **"Наследовать"** для **"Попытки одновременного входа"** в **"Настройки соединения"**. Выберите соответствующее значение в поле .



Примечание: Минимальным допустимым значением для этого поля является 0. При использовании этого значения отключается возможность входа и запрещается доступ для пользователей.

Настройте ASA/PIX с помощью интерфейса командной строки

Выполните эти шаги, чтобы задать необходимое значение для количества попыток одновременного входа. В этом примере для этого параметра было выбрано значение, равное 20.

```
ciscoasa(config)#group-policy Bryan attributes
ciscoasa(config-group-policy)#vpn-simultaneous-logins 20
```

Для получения дополнительных сведений об этой команде, см. Справочник команд Cisco Security Appliance, версия 7.2.

Проблема: не удается запустить сеанс или приложение, а также медленная передача данных после организации туннеля

После установки туннеля IPsec не устанавливается сеанс или связь с приложением.

Решение

Используйте команду **ping** для проверки работы сети или проверьте доступность сервера приложений из сети пользователя. Может возникнуть проблема с максимальным размером сегмента (MSS) временных пакетов, проходящих через маршрутизатор или устройство PIX/ASA, такие проблемы особенно часто возникают при использовании сегментов с установленным битом SYN.

Маршрутизатор для Cisco IOS

Чтобы устранить эту проблему, выполните следующие действия:

Измените значение MSS во внешнем интерфейсе (интерфейс туннеля) маршрутизатора. Чтобы задать значение MSS, выполните следующие действия:

```
Router>enable
Router#configure terminal
Router(config)#interface ethernet0/1
      Router(config-if)#ip tcp adjust-mss 1300

Router(config-if)#end
```

В этих сообщениях показываются выходные данные отладки максимального размера сегмента TCP:

```
      Router#debug ip tcp transactions

Sep 5 18:42:46.247: TCP0: state was LISTEN -> SYNRCVD [23 -> 10.0.1.1(38437)]
Sep 5 18:42:46.247: TCP: tcb 32290C0 connection to 10.0.1.1:38437, peer MSS 1300, MSS is
1300
Sep 5 18:42:46.247: TCP: sending SYN, seq 580539401, ack 6015751
Sep 5 18:42:46.247: TCP0: Connection to 10.0.1.1:38437, advertising MSS 1300
Sep 5 18:42:46.251: TCP0: state was SYNRCVD -> ESTAB [23 -> 10.0.1.1(38437)]
```

Значение MSS будет изменено на 1300 для маршрутизатора в соответствии с настройками.

Дополнительные сведения см. в PIX/ASA 7.x и IOS: фрагментация VPN.

PIX/ASA 7.X

Возникает проблема со стабильным доступом в Интернет или медленной передачей данных при использовании туннеля, поскольку отображается сообщение об ошибке о размере MTU и возникают проблемы с MSS; чтобы устранить проблему, см. следующие документы:

PIX/ASA 7.x и IOS: VPN фрагментация

PIX/ASA Выпуск 7.0: Превышено допустимое значение MSS - HTTP-клиенты не могут просматривать определенные веб- узлы

Проблема: невозможно инициировать туннель VPN из ASA/PIX

Невозможно инициировать VPN-туннель из интерфейса ASA/PIX, а после установки туннеля не удается воспользоваться командой ping с удаленного конца туннеля для "прозвона" внутреннего интерфейса ASA/PIX.

Решение

Невозможно применить для внутреннего интерфейса PIX команду ping с другого конца туннеля. Чтобы разрешить эту проблему, настройте команду **management-access** в режиме глобального конфигурирования.

```
PIX-02(config)#management-access inside

PIX-02(config)#show management-access
management-access inside
```

Прочее

При переводе настройки VPN из PIX/ASA, на котором запущена версия 7.0.x, в другое устройство защиты, на котором запущена версия 7.2.x, отображается следующее сообщение об ошибке:

```
ERROR: The authentication-server-group none command has been deprecated.
The "isakmp ikev1-user-authentication none" command in the ipsec-attributes should be used
instead.
```

Команда **authentication-server-group** более не поддерживается в версии 7.2(1) и более поздних версиях. Эта команда была исключена и перемещена в режим настройки tunnel-group general-attributes.

См. раздел isakmp ikev1-user-authentication справочника по командам для получения дополнительных сведений об этой команде.

Дополнительные сведения

- **PIX/ASA Выпуск 7.0: Превышено допустимое значение MSS - HTTP-клиенты не могут просматривать определенные веб-узлы**
- **PIX/ASA 7.x и IOS: VPN фрагментация**
- **Устройства Cisco ASA Security Appliance серии 5500**
- **Cisco Серия PIX 500 Security Appliance**
- **Протоколы согласования IPsec/IKE**
- **Концентраторы семейства Cisco VPN 3000**
- **Cisco Systems — техническая поддержка и документация**

Дата генерации PDF файла: Jan 05, 2010

---

http://www.cisco.com/support/RU/customer/content/10/105401/common_ipsec_trouble.shtml

---