Устранение наиболее распространенных проблем удаленных VPN-подключений и VPN-туннелей LAN — LAN 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 предоставляет чек-листа общих процедур для попытки, прежде чем вы начнете устранять неполадки техническая поддержка Cisco вызова и соединение.

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: Даже при том, что примеры конфигурации в этом документе для использования на маршрутизаторах и устройствах безопасности, почти все эти понятия также применимы к концентратору 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: ASA/PIX не передаст многоадресный трафик по VPN-туннелям IPSec.

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

% Warning: 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 конфигурацией IPSec VPN на этих устройствах Cisco:

- Устройства защиты Cisco PIX серии 500
- Устройства защиты Cisco ASA серии 5500
- Маршрутизаторы Cisco IOS
- Концентраторы Cisco VPN серии 3000 *(Необязательно)*

Используемые компоненты

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

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

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Конфигурация IPSec VPN не работает

Проблема

Недавно настроенное или модифицированное решение для IPSec VPN не работает.

Текущая конфигурация IPSec VPN больше не работает.

Решения

Этот раздел содержит решения наиболее распространенных проблем 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.

- Включите прохождение NAT (#1 вопрос сетей VPN RA)
- Тестовое подключение должным образом
- Включение ISAKMP
- Включение/отключение безопасной пересылки (PFS)
- Очистите старые или существующие сопоставления безопасности (туннели)
- Проверьте время существования ISAKMP
- Включите или отключите пакеты Keepalive ISAKMP
- Повторно введите или восстановите предварительные общие ключи
- Несогласованный предварительный общий ключ
- Удалите и повторно примените криптокарты
- Проверьте, что Команды sysopt присутствуют (Только PIX/ASA)
- Проверьте ISAKMP - идентичность
- Проверьте Простаивающий / Превышение времени ожидания сеанса
- Проверьте, что ACL Корректны и Связаны к Криптокарте
- Проверьте политику ISAKMP
- Проверьте, что Маршрутизация Корректна
- Проверьте, что Transform-Set Корректен
- Проверьте порядковые номера криптокарты и название
- Проверьте, что IP - адрес адресуемой точки Корректен
- Проверьте туннельную группу и имена групп
- Отключите XAUTH для узлов L2L
- Исчерпываемый пул VPN
- Проблемы с задержкой для трафика клиента VPN

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

Включите прохождение NAT (#1 вопрос сетей VPN RA)

Прохождение NAT или NAT-T позволяют трафику VPN проходить через NAT или устройства PAT, такие как Маршрутизатор Soho Linksys. 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.

Если вы не включаете NAT-T в Устройстве NAT/PAT, можно получить сообщение об ошибках `regular translation creation failed for protocol 50 src inside:10.0.1.26 dst outside:10.9.69.4` в PIX/ASA.

Точно так же, если вы неспособны сделать одновременный вход в систему от того же IP-адреса, сообщение об ошибках `Secure VPN connection terminated locally by client. Reason 412: The remote peer is no longer responding.` появляется. Включите NAT-T в устройстве VPN головного узла для решения этой ошибки.

Примечание: С Cisco IOS Software Release 12.2 (13) T и позднее NAT-T включен по умолчанию в Cisco IOS.

Вот команда для включения NAT-T на Cisco Security Appliance. 20 в данном примере являются временем поддержки активности (по умолчанию).

PIX/ASA 7.1 и ранее

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

PIX/ASA 7.2 (1) и последующие версии

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

Клиенты должны модифицироваться также для него для работы.

В Cisco VPN Client выберите к **Соединениям** и нажмите **Modify**. Это открывает новое окно, где необходимо выбрать **Вкладку Передача**. Под этой вкладкой предпочтите **Enable Transparent Tunneling** и **IPSec по** кнопке с зависимой фиксацией **UDP (NAT / PAT)**. Затем нажмите **Save** и протестируйте соединение.

Примечание: Эта команда является тем же и для PIX 6.x и для PIX/ASA 7. x.

Примечание: Важно позволить UDP 4500 для NAT-T, UDP 500 и ESP портов конфигурацией ACL, потому что PIX/ASA действует как устройство NAT. См. Настройку Туннель IPSec через Межсетевой экран с NAT для получения дополнительной информации для узнавания больше о конфигурации списков управления доступом (ACL) в PIX/ASA.

VPN-концентратор

Выберите **Configuration> Tunneling и Security> IPSEC> NAT Transparency> Enable:** ***IPsec по NAT-T*** для включения NAT-T на Концентраторе VPN.

Примечание: NAT-T также позволяет множественным клиентам VPN для соединения через устройство PAT в то же время к любому головному узлу, является ли это PIX, маршрутизатором или Концентратором.

Тестовое подключение должным образом

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 **эхо-запрос** должен быть получен от "внутренней" сети позади любого маршрутизатора. 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 опции **команды ping** в привилегированном режиме EXEC для определения источника эхо-запроса 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 = ½/4 ms
```

Представьте, что маршрутизаторы на этой схеме заменили устройствами защиты PIX или ASA. **Эхо-запрос**, используемый для тестирования подключения, может также быть получен от внутреннего интерфейса с **внутренним** ключевым словом:

```
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
```

Примечание: Когда проблема существует с подключением, даже фаза 1 VPN не подходит. На ASA, если подключение отказывает, выходные данные SA подобны данному примеру, который указывает возможно на неправильную конфигурацию криптографического однорангового узла и/или неправильную конфигурацию Предложения ISAKMP:

```
Router#show crypto isakmp sa 1 IKE Peer: XX.XX.XX.XX Type : L2L Role : initiator Rekey : no
State : MM_WAIT_MSG2
```

Примечание: Состояние могло быть от MM_WAIT_MSG2 до MM_WAIT_MSG5, который обозначает сбой заинтересованного обмена состояния в основном режиме (MM).

Примечание: Выходные данные Crypto SA, когда фаза 1 подключена, подобны данному примеру:

```
Router#show crypto isakmp sa 1 IKE Peer: XX.XX.XX.XX Type : L2L Role : initiator Rekey : no
State : MM_ACTIVE
```

Включение ISAKMP

Если отсутствует указание на использование VPN-туннеля IPsec, причина может заключаться в том, что ISAKMP не был активирован. Убедитесь, что вы включили ISAKMP на своих устройствах. 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`

Можно также получить эту ошибку при включении ISAKMP на внешнем интерфейсе:

```
UDP: ERROR - socket <unknown> 62465 in used
ERROR: IkeReceiverInit, unable to bind to port
```

Причина ошибки может состоять в том, что Клиент позади ASA/ПИ получает PAT'd к порту 500 udp, прежде чем isakmp сможет быть включен на интерфейсе. Как только та трансляция PAT удалена (clear xlate), isakmp в состоянии быть включенным.

Примечание: Всегда удостоверяйтесь, что UDP 500 и 4500 номеров портов

зарезервированы для согласования соединений ISAKMP с узлом.

Примечание: Когда ISAKMP не включен на интерфейсе, клиент VPN показывает сообщение об ошибках, подобное этому сообщению:

```
Secure VPN connection terminated locally by client.
Reason 412: The remote peer is no longer responding
```

Примечание: Для решения этой ошибки включите ISAKMP на крипто-интерфейсе Шлюза VPN.

Включение/отключение безопасной пересылки (PFS)

При согласовании IPsec безопасная пересылка (PFS) позволяет гарантировать отсутствие связи нового ключа шифрования со всеми предыдущими ключами. Или включите или отключите безопасную пересылку (PFS) на обоих равноправные пользователи туннеля; иначе, LAN-LAN (L2L) Туннель IPSec не установлен в PIX/ASA/МАРШРУТИЗАТОРЕ IOS.

PIX/ASA:

По умолчанию безопасная пересылка (PFS)отключена. **Для включения PFS используйте команду 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 для безопасной пересылки (PFS) от 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 никакая группа не задана с этой командой, group1 используется в качестве по умолчанию.

```
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 IPsec должен использовать 1024-разрядный Диффи-Хеллман главная группа модуля, когда выполнен новый Обмен Диффи-Хеллмана.

Пример:

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

Примечание: Безопасная пересылка (Perfect Forward Secrecy, PFS) является составляющей

собственность Cisco и не поддерживается на устройствах стороннего производителя.

Очистите старые или существующие сопоставления безопасности (туннели)

Если это сообщение об ошибках происходит в Маршрутизаторе IOS, проблема состоит в том, что SA или истек или был очищен. Удаленный туннель конечного устройства не распознает данные об использовании устаревшего SA для отправки пакета (не пакета создания SA). Когда новый SA будет установлен, резюме связи, поэтому инициируйте *представляющий интерес трафик* через туннель, чтобы создать новый SA и восстановить туннель.

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

При очистке ISAKMP (Фаза I) и IPsec (Этап 2) сопоставления безопасности (SA) это является самым простым и часто лучшее решение решить проблемы IPSec VPN.

При очистке SA можно часто решать большое разнообразие сообщений об ошибках и странного поведения без потребности устранить неполадки. В то время как этот способ может легко использоваться в любой ситуации, это - почти всегда требование для очистки SA после того, как вы изменяетесь или добавляете 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: Как только Сопоставления безопасности были очищены, может быть необходимо передать трафик через туннель для восстанавливания их.

% Warning: Пока вы не задаете, какие сопоставления безопасности очиститься, команды, перечисленные здесь, могут очистить все сопоставления безопасности на устройстве. Соблюдайте осторожность, если используются другие туннели IPsec VPN.

1. До очистки сопоставлений безопасности их необходимо просмотреть**Cisco IOS**`router#show crypto isakmp sa router#show crypto ipsec sa` **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 ассоциаций безопасности. Каждая команда может быть введена как показано полужирным или введена с вариантами, показавшими с ними.**Cisco IOSISAKMP (фаза I)**`router#clear crypto isakmp ? <0 - 32766> connection id of SA <cr>`**IPsec (этап 2)**`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>`**Cisco PIX/ASA Security ApplianceISAKMP (фаза I)**`securityappliance#clear crypto isakmp sa` **IPsec (этап 2)**`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>`

Проверьте время существования ISAKMP

Если пользователи часто разъединяются через туннель L2L, проблемой может быть меньший срок действия, настроенный в ISAKMP SA. Если какое-либо несоответствие происходит во времени существования ISAKMP, можно получить **%PIX|ASA-5-713092: Группа = x. x. x. x, IP = x. x. x. x, Сбой во время смены ключа фазы 1 пытается из-за** сообщения **ошибки коллизии** в PIX/ASA. Для FWSM можно получить сообщение об ошибках

`%FWSM-5-713092: Group = x.x.x.x, IP = x.x.x.x, Failure during phase 1 rekeying attempt due to collision`. Настройте то же значение в обоих узлы для решения проблемы его.

По умолчанию составляет 86,400 секунд или 24 часа. Как правило более короткий срок действия предоставляет более безопасные согласования ISAKMP (в какой-то степени), но с более короткими сроками службы устройство безопасности устанавливает будущие контексты безопасности IPSec более быстро.

Соответствие сделано, когда обе политики от двух узлов содержит то же шифрование, хэш, аутентификацию и значения параметра Диффи-Хеллмана, и когда политика удаленного узла задает срок действия, меньше чем или равный сроку действия в сравненной политике. Если сроки службы не идентичны, более короткий срок действия — от политики удаленного узла — используется. Если никакое приемлемое соответствие не найдено, IKE отказывается от согласования, и IKE SA не установлена.

Задайте срок действия SA. Данные примеры устанавливают срок действия 4 часов (14400 секунд). По умолчанию составляет 86400 секунд (24 часа).

PIX/ASA

`hostname(config)#`**`isakmp policy 2 lifetime 14400`**
Маршрутизатор IOS

`R2(config)#`**`crypto isakmp policy 10`** `R2(config-isakmp)#`**`lifetime 86400`**
Если максимальный настроенный срок действия превышен, вы получаете это сообщение об ошибках, когда завершено VPN-подключение:

`Secure VPN Connection terminated locally by the Client. Reason 426: Maximum Configured Lifetime Exceeded` Превышен настроенный максимальный срок существования.

Для решения этого сообщения об ошибках установите *пожизненное* значение в *0* для установки срока действия сопоставления безопасности IKE к бесконечности. VPN всегда будет соединением и не завершится.

`hostname(config)#isakmp policy 2 lifetime 0`
Можно также **отключить re-xauth в групповой политике** для решения вопроса.

Включите или отключите пакеты Keepalive ISAKMP

При настройке пакетов Keepalive ISAKMP это помогает предотвращать спорадически отброшенный LAN-LAN или VPN для удаленного доступа, который включает клиенты VPN, туннели и туннели, которые отброшены после периода бездействия. Эта функция позволяет оконечной точке туннеля контролировать продолжительное присутствие удаленного узла и сообщить о его собственном присутствии тому узлу. Если узел становится безразличным, оконечная точка удаляет соединение. Для пакетов Keepalive ISAKMP для работы обе оконечных точки VPN должны поддержать их.

- Настройте пакеты Keepalive ISAKMP в Cisco IOS с этой командой:`router(config)#`**`crypto isakmp keepalive 15`**
- Используйте эти команды для настройки пакетов Keepalive ISAKMP на Устройствах безопасности PIX/ASA:Cisco PIX 6.x`pix(config)#`**`isakmp keepalive 15`** PIX/ASA Cisco 7.x и позже, для туннельной группы назвал **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 некоторых ситуациях необходимо отключить эту опцию для решения проблемы, например, если Клиент VPN находится позади Межсетевого экрана, который предотвращает пакеты DPD.PIX/ASA Cisco 7.x и позже, для туннельной группы назвал **10.165.205.222**Отключает обработку сообщения поддержки активности IKE, которая включена по умолчанию.`securityappliance(config)#`**`tunnel-group 10.165.205.222 ipsec-attributes`** `securityappliance(config-tunnel-ipsec)#`**`isakmp keepalive disable`** **Отключите поддержку активности для Cisco VPN Client 4. x**Выберите**> Program Files % Root %System> Cisco Systems> VPN Client> Профили** на Клиентском компьютере, который испытывает проблему, чтобы отключить сообщение поддержки активности IKE и отредактировать **файл PCF**, когда это применимо, для соединения.**Измените 'ForceKeepAlives=0' (по умолчанию) на 'ForceKeepAlives=1'.**

Примечание: Пакеты Keepalive являются составляющей собственность Cisco и не поддерживаются устройствами стороннего производителя.

Повторно введите или восстановите предварительные общие ключи

Во многих случаях, когда VPN-туннель IPSec не подходит, простая опечатка может быть виновата. Например, на устройстве безопасности, предварительные общие ключи становятся скрытыми, как только они введены. Эта путаница лишает возможности видеть, является ли ключ неправильным. **Убедитесь, что вы ввели любые предварительные общие ключи правильно в каждую оконечную точку VPN.** Повторно введите ключ, чтобы быть уверенными, что это корректно; это - простое решение, которое может помочь избегать всестороннего устранения проблем.

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
3      14:37:50.562  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
4      14:37:50.593  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
5      14:44:15.937  10/05/06  Sev=Warning/2 IKE/0xA3000067
Received Unexpected InitialContact Notify (PLMgrNotify:888)
6      14:44:36.578  10/05/06  Sev=Warning/3 IKE/0xE3000056
The received HASH payload cannot be verified
7      14:44:36.593  10/05/06  Sev=Warning/2 IKE/0xE300007D
Hash verification failed... may be configured with invalid group password.
8      14:44:36.609  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
9      14:44:36.640  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
```

Можно также восстановить предварительный общий ключ без любых изменений конфигурации на устройстве безопасности PIX/ASA. Подробное описание настройки сети VPN на базе IPSec между двумя узлами в устройстве защиты Cisco с версией ПО 7.x см. в документе PIX/ASA 7.x: Восстановление общего ключа.

% Warning: 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, чтобы удалить и повторно ввести предварительный общий ключ **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` VPN для удаленного доступа Cisco`router(config)#crypto isakmp client configuration group vpngroup router(config-isakmp-group)#no key secretkey router(config-isakmp-group)#key secretkey`
- Используйте эти команды, чтобы удалить и повторно ввести предварительный общий ключ **secretkey** для узла **10.0.0.1** на Устройствах безопасности 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`

Несогласованный предварительный общий ключ

Инициирование VPN-туннеля разъединено. Эта проблема могла бы произойти из-за несогласованного предварительного общего ключа во время согласований фазы I.

Сообщение **MM_WAIT_MSG_6** в **команде show crypto isakmp sa** указывает на несогласованный предварительный общий ключ как показано в данном примере:

```
ASA#show crypto isakmp sa Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 1 IKE Peer: 10.7.13.20 Type : L2L Role : initiator Rekey : no State : MM_WAIT_MSG_6
```

Для решения этого вопроса повторно введите предварительный общий ключ в обоих устройствах; предварительный общий ключ должен быть уникальным и совпасться. Посмотрите Повторно вводят или Восстанавливают Предварительные общие ключи для получения дополнительной информации.

Удалите и повторно примените криптокарты

Когда вы очищаете сопоставления безопасности, и это не решает вопрос IPSec VPN, удаляет и повторно применяет соответствующую криптокарту для решения большого разнообразия проблем, которое включает неустойчивое отбрасывание VPN-туннеля и сбой некоторых узлов VPN для подъема.

% Warning: При удалении криптокарты из интерфейса это **определенно** переводит в нерабочее состояние любые Туннели IPSec, привязанные к той криптокарте. Выполните эти действия с осторожностью и рассмотрите политику управления изменениями своей организации перед переходом.

- Используйте эти команды, чтобы удалить и заменить криптокарту в Cisco IOS:Начните с удаления криптокарты из интерфейса. Не используйте форму команды **криптокарты**.`router(config-if)#no crypto map mymap` Продолжите не использовать форму для удаления всей криптокарты.`router(config)#no crypto map mymap 10` Замените криптокарту на интерфейсном 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, чтобы удалить и заменить криптокарту на PIX или ASA:Начните с удаления криптокарты из интерфейса. Не используйте форму команды **криптокарты**.`securityappliance(config)#`**`no crypto map mymap interface outside`** Продолжите не использовать форму 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`** Замените криптокарту 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`**

Примечание: Если вы удаляете и повторно применяете криптокарту, это также решает проблему с подключением, если был изменен IP-адрес головного узла.

Проверьте, что Команды sysopt присутствуют (Только PIX/ASA)

Sysopt connection permit-ipsec команд и **sysopt connection permit-vpn** позволяют пакетам из Туннеля IPSec и их информационных наполнений обходить интерфейсные ACL на устройстве безопасности. Туннели IPSec, которые завершены на устройстве безопасности, вероятно, откажут, если не будет выполнена одна из этих команд.

В Версии программного обеспечения 7.0 Устройства безопасности и ранее, соответствующая команда sysopt для этой ситуации является **sysopt connection permit-ipsec**.

В Версии программного обеспечения 7.1 (1) Устройства безопасности и позже, соответствующая команда sysopt для этой ситуации является **sysopt connection permit-vpn**.

В PIX 6.x, эта функциональность **отключена** по умолчанию. С PIX/ASA 7.0 (1) и позже, эта функциональность **добавлена** по умолчанию. Используйте эти команды показа, чтобы определить, включена ли соответствующая **команда sysopt** на вашем устройстве:

- 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`
- Cisco – PIX/ASA 7.x`securityappliance#` **`show running-config all 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 эти команды для включения корректной **команды sysopt** для устройства:

- PIX Cisco 6.x и PIX/ASA 7.0`pix(config)#`**`sysopt connection permit-ipsec`**
- Cisco PIX/ASA 7.1 (1) и позже`securityappliance(config)#`**`sysopt connection permit-vpn`**

Примечание: Если вы не хотите использовать **команду sysopt connection**, то необходимо явно разрешить необходимый трафик, который является представляющим интерес

трафиком от источника до назначения, например, от LAN удаленного устройства к LAN локального устройства и "порта 500 UDP" для внешнего интерфейса удаленного устройства к внешнему интерфейсу локального устройства, во внешнем ACL.

Проверьте ISAKMP - идентичность

Если VPN-туннель IPSec отказал в Ike согласование, сбой может произойти или из-за PIX или из-за неспособности его узла распознать идентичность его узла. Когда два узла используют IKE для установления Сопоставлений безопасности IPSec, каждый узел передает свой ISAKMP - идентичность к удаленному узлу. Это передает или свой IP-адрес или имя хоста, зависящее от того, как каждому установили его ISAKMP - идентичность. По умолчанию ISAKMP - идентичность модуля Межсетевого экрана PIX установлен в IP-адрес. Как правило заставьте устройство безопасности и личности его узлов таким же образом избегать сбоя Ike согласование.

Чтобы заставить ID Фазы 2 передаваться узлу, используйте **команду identity isakmp** в режиме глобальной конфигурации

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

Или

```
crypto isakmp identity auto
!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with ISAKMP negotiation by
connection type; IP address for !--- preshared key or cert DN for certificate authentication.
```

Или

```
crypto isakmp identity hostname
!--- Uses the fully-qualified domain name of !--- the host exchanging ISAKMP identity
information (default). !--- This name comprises the hostname and the domain name.
```

VPN-туннель не в состоянии подходить после движущейся конфигурации от PIX до ASA с помощью программного средства миграции конфигурации PIX/ASA; эти сообщения появляются в журнале:

```
[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, Stale PeerTblEntry found, removing! [IKEv1]: Group =
x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match! [IKEv1]: Group =
x.x.x.x, IP = x.x.x.x, construct_ipsec_delete(): No SPI to identify Phase 2 SA! [IKEv1]: Group =
x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match!
```

Эта проблема происходит, так как PIX по умолчанию собирается определить соединение как **имя хоста**, где ASA определяет как **IP**. Для решения этого вопроса используйте **команду crypto isakmp identity** в режиме глобальной конфигурации как показано ниже:

```
crypto isakmp identity hostname !--- Use the fully-qualified domain name of !--- the host
exchanging ISAKMP identity information (default). !--- This name comprises the hostname and the
domain name.
```

Когда вы получаете сообщение об ошибках `Received an un-encrypted INVALID_COOKIE`, выполняете **команду crypto isakmp identity address** для решения вопроса.

Примечание: Команда identity isakmp осуждалась от версии программного обеспечения 7.2 (1). См. Справочник по командам Cisco Security Appliance, Версия 7.2 для получения дополнительной информации.

Проверьте Простаивающий / Превышение времени ожидания сеанса

Если время простоя установлено в 30 минут (по умолчанию), это означает, что это отбрасывает туннель после того, как 30 минут "no traffic" (нета трафика) проходят через него. Клиент VPN разъединен после 30 минут независимо от значения времени простоя и встречается с ошибкой `PEER_DELETE-IKE_DELETE_UNSPECIFIED`.

Настройте **время простоя** и **превышение времени ожидания сеанса** как **ни один** для создания туннеля всегда, и так, чтобы туннель никогда не был отброшен даже когда с помощью устройств стороннего производителя.

PIX/ASA 7.x и более поздние

Введите **команду vpn-idle-timeout** в режим конфигурации групповой политики или в режим конфигурации имени пользователя для настройки пользовательского периода ожидания:

```
hostname(config)#group-policy DfltGrpPolicy attributes hostname(config-group-policy)#vpn-idle-timeout none
```

Настройте максимальное количество времени для VPN-подключений с **командой vpn-session-timeout** в режиме конфигурации групповой политики или в режиме конфигурации имени пользователя:

```
hostname(config)#group-policy DfltGrpPolicy attributes hostname(config-group-policy)#vpn-session-timeout none
```

Примечание: Когда у вас есть **туннель - все** настроенные, вы не должны настраивать **idle-timeout**, потому что даже при настройке времени простоя VPN это не будет работать, потому что весь трафик проходит туннель (так как туннель - все настроено). Поэтому представляющий интерес трафик (или даже трафик, генерируемый ПК), будет содержательным и не позволит Idle-timeout войти в действие.

Маршрутизатор с ПО Cisco IOS

Используйте **команду crypto ipsec security-association idle-time** в режиме глобальной конфигурации или режиме конфигурации криптокарты для настройки счетчика простоя контекста безопасности IPSec. Контекстом безопасности IPSec по умолчанию счетчики простоя отключены.

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

Время находится в *секундах*, которые счетчик простоя позволяет неактивному узлу поддерживать SA. Допустимые значения для секундного аргумента колеблются от 60 до 86400.

Проверьте, что ACL Корректны и Связаны к Криптокарте

В стандартной конфигурации IPsec VPN используются два списка доступа. Один список используется для исключения трафика, направленного в туннель VPN, из процесса NAT. Другой список доступа определяет трафик для шифрования; он включает в себя список шифрования ACL в настройке ЛВС-ЛВС или список раздельного туннелирования в конфигурации удаленного доступа. Если эти списки доступа неправильно настроены или отсутствуют, трафик может идти по туннелю VPN только в одном направлении или может вообще не проходить через туннель.

Примечание: Удостоверьтесь, что связали крипто-ACL с криптокартой при помощи команды адреса соответствия криптокарты в режиме глобальной конфигурации.

Убедитесь, что все списки доступа, необходимые для конфигурации IPsec VPN, настроены и что эти списки определяют правильный трафик. В списке далее описаны простые способы проверки в тех случаях, когда подозревается, что причина проблем с IPsec VPN в списке доступа.

- Убедитесь, что в исключении NAT и списках доступа шифрования ACL указан правильный трафик.
- Если имеется несколько туннелей VPN и списков шифрования ACL, убедитесь, что эти списки не пересекаются.**Примечание:** На концентраторе VPN вы могли бы видеть журнал как это:`Tunnel Rejected: IKE peer does not match remote peer as defined in L2L policy`Во избежание этого сообщения и для внедрения туннеля, удостоверьтесь, что Crypto ACLS не накладывается, и тот же представляющий интерес трафик не используется никаким другим настроенным VPN-туннелем.
- 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.
- Для конфигурации удаленного доступа не используйте access-list для представляющего интерес трафика с динамической криптокартой. Это может заставить клиент VPN быть неспособным соединиться с головным устройством. При ошибочной настройке крипто-ACL для VPN для удаленного доступа можно получить сообщение об ошибках `%ASA-3-713042: IKE Initiator unable to find policy: Intf 2`.**Примечание:** Если это - туннель от узла к узлу VPN, удостоверьтесь, что совпали со списком доступа с узлом. Они должны быть в обратном порядке на узле.См. PIX/ASA 7.x и Cisco VPN Client 4.x с Windows 2003 IAS RADIUS (Против Active Directory) Пример Конфигурации аутентификации для примера конфигурации, который показывает, как установить соединение VPN для удаленного доступа между Cisco VPN Client и PIX/ASA.
- Убедитесь, что конфигурация устройства позволяет использовать ACL исключения NAT. **Для маршрутизаторов это означает использование команды route-map. Для PIX или ASA это означает использование команды nat (0).** Список ACL исключения NAT необходимо для конфигураций ЛВС-ЛВС и удаленного доступа.Здесь, маршрутизатор IOS настроен для освобождения трафика, который передается между **192.168.100.0 / 24** и **192.168.200.0 / 24** или **192.168.1.0 / 24** от NAT. Трафик, предназначенный для где-либо еще, подвергается перегрузке 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
```
Здесь, PIX настроен для освобождения трафика, который передается между **192.168.100.0 / 24** и **192.168.200.0 / 24** или **192.168.1.0 / 24** от NAT. Например, весь другой трафик подвергается перегрузке 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:** ACL освобождения NAT

работают только с IP-адресом или IP - сетями, такими как те примеры, упомянутые (access-list noNAT), и должны быть идентичны ACL криптокарты. ACL освобождения NAT не работают с номерами портов (например, 23, 25, и т.д.).**Примечание:** В среде VoIP, куда голосовые вызовы между сетями передаются через VPN, не работают голосовые вызовы, если должным образом не настроены ACL NAT 0. Прежде, чем идти глубоко посредством Устранения проблем VoIP, предложено проверить статус возможности VPN - подключения, потому что проблема могла быть с неверной конфигурацией освобожденных ACL NAT.**Примечание:** Если существует неверная конфигурация в освобождении NAT (nat 0) ACL, можно получить сообщение об ошибках как показано.`%PIX-3-305005: **No translation group** found for icmp src outside:192.168.100.41 dst inside:192.168.200.253 (type 8, code 0) %ASA-3-305005: No translation group found for udp src Outside:x.x.x.x/p dst Inside:y.y.y.y/p`**Примечание: Неправильный пример:**`access-list noNAT extended permit ip 192.168.100.0 255.255.255.0 192.168.200.0 255.255.255.0 **eq 25**` Если освобождение NAT (nat 0) не работает, то попытайтесь удалить его и выполнить **команду NAT 0** для него для работы.

- Удостоверьтесь, что ваши ACL не назад и что они - нужный тип.Крипто-и ACL освобождения NAT для конфигураций LAN-to-LAN должен быть записан с точки зрения устройства, на котором настроен ACL. Это означает, что ACL должны **отразить** 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:** Несмотря на то, что это не проиллюстрировано здесь, это то же понятие применяется к PIX и Устройствам обеспечения безопасности ASA, также.В PIX/ASA ACL разделения туннеля для конфигураций Удаленного доступа должны быть **стандартными списками доступа**, которые разрешают трафик к сети, к которой клиенты VPN должны обратиться. Маршрутизаторы IOS могут использовать расширенный список ACL для разделения туннеля.**Примечание:** В расширенном списке доступа, для использования **'любого'** в источнике в ACL разделенного туннелирования подобно для отключения разделенного туннелирования. Используйте только исходные сети в расширенном списке ACL для разделенного туннелирования.**Примечание: Корректный пример:**`access-list 140 permit ip **10.1.0.0 0.0.255.255** 10.18.0.0 0.0.255.255` **Примечание: Неправильный пример:**`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**`

Если НИКАКОЙ ACL NAT не неправильно сконфигурирован или не настроен на ASA, эта ошибка происходит в ASA 8.3:

```
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection for udp
src outside: x.x.x.x/xxxxx dst inside:x.x.x.x/xx denied due to NAT reverse path failure
```

Для решения этого вопроса проверьте, что конфигурация корректна, или реконфигурируйте, если параметры настройки являются неправильными.

Конфигурация освобождения NAT в версии ASA 8.3 для туннеля VPN типа «узел-узел»:

Сквозное VPN-соединение должно быть установлено между HOASA и BOASA с обоими ASA с помощью версии 8.3. Конфигурация освобождения NAT на HOASA выглядит подобной этому:

```
object network obj-local
subnet 192.168.100.0 255.255.255.0
object network obj-remote
subnet 192.168.200.0 255.255.255.0
nat (inside,outside) 1 source static obj-local obj-local destination static obj-remote objremote
```

Проверьте политику ISAKMP

Если Туннель IPSec не подключен UP, проверьте, что Политика ISAKMP совпадает с удаленными узлами. 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 сроки службы не идентичны, устройство безопасности использует более короткий срок действия. Если никакое приемлемое соответствие не существует, ISAKMP отказывается от согласования, и SA не установлен.

```
"Error: Unable to remove Peer TblEntry, Removing peer from peer table
failed, no match!"
```

Вот подробное сообщение журнала:

```
4|Mar 24 2010 10:21:50|713903: IP = X.X.X.X, Error: Unable to remove PeerTblEntry
3|Mar 24 2010 10:21:50|713902: IP = X.X.X.X, Removing peer from peer table failed,
no match!
3|Mar 24 2010 10:21:50|713048: IP = X.X.X.X, Error processing payload: Payload ID: 1
4|Mar 24 2010 10:21:49|713903: IP = X.X.X.X, Information Exchange processing failed
5|Mar 24 2010 10:21:49|713904: IP = X.X.X.X, Received an un-encrypted
NO_PROPOSAL_CHOSEN notify message, dropping
```

Это сообщение обычно появляется из-за несогласованной Политики ISAKMP или недостающего оператора NAT 0.

Кроме того, это сообщение появляется:

```
Error Message    %PIX|ASA-6-713219: Queueing KEY-ACQUIRE messages to be processed when
P1 SA is complete.
```

Это сообщение указывает, что сообщения Фазы 2 ставятся в очередь после того, как Фаза 1 завершает. Это сообщение об ошибках могло бы произойти из-за одной из этих причин:

- Не сочетайтесь синфазно на любом из узлов
- ACL блокирует узлы от завершения фазы 1

Это сообщение обычно появляется после `Removing peer from peer table failed, no match! .`

Если Cisco VPN Client неспособен подключить устройство головного узла, проблемой может быть несоответствие ПОЛИТИКИ ISAKMP. Устройство головного узла должно совпасть с одним из Предложений ike Cisco VPN Client.

Примечание: Для Политики ISAKMP и Команды IPsec transform set, которая используется на PIX/ASA, клиент Cisco VPN не может использовать политику с комбинацией 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, что Маршрутизация Корректна

Маршрутизация — это важная часть любого развертывания IPsec VPN. Убедитесь, что ваши устройства шифрования, такие как маршрутизаторы и PIX или Устройства обеспечения безопасности ASA имеют информацию о соответствующей маршрутизации для передачи трафика по VPN-туннелю. Кроме того, если другие маршрутизаторы существуют позади вашего устройства шлюза, быть уверенными, что те маршрутизаторы знают, как достигнуть туннеля и что сети с другой стороны.

Одним основным компонентом маршрутизации в развертывании VPN является Включение ввода обратной маршрутизации (RRI). RRI размещает динамические записи для удаленных сетей или клиентов VPN в таблице маршрутизации Шлюза VPN. Эти маршруты полезны для устройства, на котором они установлены, а также к другим устройствам в сети, потому что маршруты, установленные RRI, могут быть перераспределены через протокол маршрутизации, такой как EIGRP или OSPF.

- В конфигурации LAN-to-LAN для каждой оконечной точки важно иметь маршрут или маршруты к сетям, для которых это, как предполагается, шифрует трафик. В данном примере Необходимая вещь маршрутизатора направляет к сетям позади маршрутизатора B до **10.89.129.2**. Маршрутизатор B должен иметь подобный маршрут к **192.168.100.0 / 24**:Первый способ гарантировать, что каждый маршрутизатор знает соответствующий маршрут (маршруты), состоит в том, чтобы настроить статические маршруты для каждой сети назначения. Например, маршрутизатору A можно было настроить эти инструкции маршрута:`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, конфигурация может быть похожей на это:`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 большое число сетей существует позади каждой оконечной точки, конфигурация статических маршрутов становится трудной поддержать. 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, крипто-ACL и криптокарта маршрутизатора A могут быть похожими на это:`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, конфигурация может быть похожей на это:
```
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 необходимы. 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 данном примере предположите, что клиентам VPN дают адреса в диапазоне **10.0.0.0 / 24**, когда они соединяются.Если никакой протокол маршрутизации не используется между шлюзом и другим маршрутизатором (маршрутизаторами), статические маршруты могут использоваться на маршрутизаторах, таких как маршрутизатор 2:
```
ip route 10.0.0.0 255.255.255.0 192.168.100.1
```
Если протокол маршрутизации, такой как EIGRP или OSPF используется между шлюзом и другими маршрутизаторами, рекомендуется, чтобы Включение ввода обратной маршрутизации использовалось, как описано. RRI автоматически добавляет маршруты для клиента VPN к таблице маршрутизации шлюза. Эти маршруты могут тогда быть распределены другим маршрутизаторам в сети.Маршрутизатор с ПО Cisco IOS:
```
crypto dynamic-map
dynMAP 10
 set transform-set mySET
 reverse-route crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```
PIX Cisco или устройство обеспечения безопасности ASA:
```
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: Если пул IP-адресов, назначенных для клиентов VPN, является наложениями с внутренними сетями устройства головного узла, проблема маршрутизации происходит. Для получения дополнительной информации обратитесь к разделу Наложений частной сети.

Проверьте, что Transform-Set Корректен

Удостоверьтесь, что IP - безопасное шифрование и алгоритмы хэширования, которые будут использоваться набором преобразований на обоих концах, являются тем же. См. раздел Справочника по командам руководства по конфигурации Cisco Security Appliance для получения дополнительной информации.

Примечание: Для Политики ISAKMP и Команды IPsec transform set, которая используется на PIX/ASA, клиент Cisco VPN не может использовать политику с комбинацией 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 Криптокарты и Название и также что

Криптокарта применена в правильном интерфейсе, в котором Туннель IPSec запускают/заканчивают

Если статические и динамические узлы настроены на той же криптокарте, заказ элементов криптокарты очень важен. Порядковый номер записи динамической криптокарты **должен быть** выше, чем все другие записи статической криптокарты. Если статические записи пронумерованы выше, чем динамическая запись, соединения с теми узлами, сбой и отладки как показано появляются.

```
IKEv1]: Group = x.x.x.x, IP = x.x.x.x, QM FSM error (P2 struct &0x49ba5a0, mess id 0xcd600011)!
[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match!
```

Примечание: Только одна Динамическая криптокарта позволена для каждого интерфейса в Устройстве безопасности.

Вот пример должным образом пронумерованной криптокарты, которая содержит статическую запись и динамическую запись. Обратите внимание на то, что динамическая запись имеет самый высокий порядковый номер, и комнату покинули добавить дополнительные статические записи:

```
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 криптокарты учитывают регистр.

Примечание: Это сообщение об ошибках может также быть замечено, когда динамическая крипто-последовательность человека не корректна, который заставляет узел поражать неправильную криптокарту, и также несогласованным крипто-списком доступа, который определяет представляющий интерес трафик: `%ASA-3-713042: IKE, :`

В сценариях, где множественные VPN-туннели, которые будут завершены в том же интерфейсе, мы должны создать криптокарту с тем же названием (только одна криптокарта позволена для интерфейса), но с номером другой последовательности. Это сохраняется 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. Точно так же обратитесь к PIX/ASA 7. X: Добавьте Новый Туннель или Удаленный доступ к Существующей VPN L2L для получения дополнительной информации для узнавания больше о конфигурации криптокарты и для L2L и для сценариев VPN для удаленного доступа.

Проверьте, что IP - адрес адресуемой точки Корректен

Для Устройства безопасности PIX/ASA 7.x LAN-LAN (L2L) конфигурация IPSec VPN, необходимо задать **<name>** туннельной группы как **theRemote IP - адрес адресуемой точки** (удаленный туннельный конец) в **команде tunnel-group <name> type ipsec-l2l** для создания и управления базы данных записей о подключениях для IPsec. IP - адрес адресуемой точки должен совпасть в **имени группы туннелей** и **командах Crypto map set address**. При настройке VPN с ASDM она генерировала имя группы туннелей автоматически с

правильным IP - адресом адресуемым точки. Если IP - адрес адресуемой точки не настроен должным образом, журналы могут содержать это сообщение, которое может быть решено правильной конфигурацией **IP - адреса адресуемого точки**.

```
[IKEv1]: Group = DefaultL2LGroup, IP = x.x.x.x,
ERROR, had problems decrypting packet, probably due to mismatched pre-shared key. Aborting
```

В PIX 6.x LAN-LAN (L2L) конфигурация IPSec VPN, IP - адрес адресуемой точки (удаленный туннельный конец) должен совпасть **с основным адресом isakmp** и **командой set peer** в криптокарте для успешного соединения IPSec VPN.

Когда IP - адрес адресуемой точки не был настроен должным образом на крипте - настройке ASA, ASA не в состоянии установить VPN-туннель и "зависает" на этапе *MM_WAIT_MSG4* только. Для решения этого вопроса исправьте IP - адрес адресуемой точки в конфигурации.

Когда VPN-туннель "зависает" в в состоянии MM_WAIT_MSG4, вот выходные данные **команды show crypto isakmp sa**.

```
hostname#show crypto isakmp sa 1 IKE Peer: XX.XX.XX.XX Type : L2L Role : initiator Rekey : no
State : MM_WAIT_MSG4
```

Проверьте туннельную группу и имена групп

```
%PIX|ASA-3-713206: Tunnel Rejected: Conflicting protocols specified by
tunnel-group and group-policy
```

Сообщение появляется, когда туннель отброшен, потому что позволенный туннель, заданный в групповой политике, другой, чем позволенный туннель в конфигурации туннельной группы.

```
group-policy hf_group_policy attributes
  vpn-tunnel-protocol l2tp-ipsec

username hfremote attributes
  vpn-tunnel-protocol l2tp-ipsec
```

Both lines should read: `vpn-tunnel-protocol ipsec l2tp-ipsec`

Уже включите IPSec В политике Группы по умолчанию к Существующие протоколы В Политике Группы по умолчанию.

```
group-policy DfltGrpPolicy attributes
   vpn-tunnel-protocol L2TP-IPSec IPSec webvpn
```

Отключите XAUTH для узлов L2L

Если туннель между локальными сетями (LAN-to-LAN) и туннель VPN для удаленного доступа настроены на той же криптокарте, узлу LAN-LAN предлагают для получения информации о XAUTH и сбоев туннеля между локальными сетями (LAN-to-LAN) с ***"CONF_XAUTH"*** в выходных данных **команды show crypto isakmp sa**.

Вот пример выходных данных SA:

```
Router#show crypto isakmp sa IPv4 Crypto ISAKMP SA dst src state conn-id slot status X.X.X.X
Y.Y.Y.Y CONF_XAUTH 10223 0 ACTIVE X.X.X.X Z.Z.Z.Z CONF_XAUTH 10197 0 ACTIVE
```

Примечание: Эта проблема только применяется к Cisco IOS и PIX 6. x. тогда как на PIX/ASA 7.x не влияет эта проблема, так как это использует туннельные группы.

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 статических узлов IPsec. Введите команду, подобную этому на устройстве, которое имеет и L2L и VPN RA, настроенную на той же криптокарте:

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

В сценарии, где PIX/ASA 7.x действия как Сервер Easy VPN, клиент Easy VPN неспособен соединиться с головным узлом из-за проблемы Xauth. Отключите проверку подлинности пользователя в PIX/ASA для решения вопроса как показано:

```
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
```

Посмотрите Раздел прочих сведений этого документа для знания больше о **команде isakmp ikev1-user-authentication**.

Исчерпываемый пул VPN

Когда диапазон IP-адресов, назначенных на пул VPN, не достаточен, можно расширить доступность IP-адресов двумя способами:

1. Удалите существующий диапазон и определите новый диапазон.
   Например:
   ```
   CiscoASA(config)#no ip local pool testvpnpool 10.76.41.1-10.76.41.254
   CiscoASA(config)#ip local pool testvpnpool 10.76.41.1-10.76.42.254
   ```
2. Когда изолированные подсети должны быть добавлены к пулу VPN, можно определить два отдельных пула VPN и затем задать их в заказе под "атрибутами туннельной группы". Например:
   ```
   CiscoASA(config)#ip local pool testvpnpoolAB 10.76.41.1-10.76.42.254
   CiscoASA(config)#ip local pool testvpnpoolCD 10.76.45.1-10.76.45.254
   CiscoASA(config)#tunnel-group test type remote-access CiscoASA(config)#tunnel-group test
   general-attributes CiscoASA(config-tunnel-general)#address-pool (inside) testvpnpoolAB
   testvpnpoolCD CiscoASA(config-tunnel-general)#exit
   ```

Заказ, в котором вы задаете пулы, очень важен, потому что ASA выделяет адреса от этих пулов в заказе, в котором пулы появляются в этой команде.

Примечание: Параметры настройки пулов адресов в команде пулов адресов групповой политики всегда отвергают параметры настройки локального пула в команде пула адресов туннельной группы.

Проблемы с задержкой для трафика клиента VPN

Когда существуют проблемы задержки по VPN-подключению, проверяют следующее для решения этого:

1. Проверьте, может ли MSS пакета быть уменьшен далее.
2. Если IPsec/tcp используется вместо IPsec/udp, то настройте поток vpn заповедника.
3. Повторно загрузите Cisco ASA.

Клиенты VPN Неспособны Соединиться с ASA/PIX

Проблема

Когда Xauth используется с сервером RADIUS, клиенты Cisco VPN неспособны

аутентифицироваться.

Решение

Проблема может состоять в том, что xauth испытывает таймаут. Увеличьте значение таймаута для AAA-сервера для решения этого вопроса.

Пример:

```
Hostname(config)#aaa-server test protocol radius hostname(config-aaa-server-group)#aaa-server test host 10.2.3.4 hostname(config-aaa-server-host)#timeout 10
```

Проблема

Когда Xauth используется с сервером RADIUS, клиенты Cisco VPN неспособны аутентифицироваться.

Решение

Первоначально, удостоверьтесь, что аутентификация работает должным образом. Для сужения проблемы сначала проверьте аутентификацию с локальной базой данных на ASA.

```
tunnel-group tggroup general-attributes
              authentication-server-group none
              authentication-server-group LOCAL
        exit
```

Если это хорошо работает, то проблема должна быть отнесена к Конфигурации сервера RADIUS.

Проверьте подключение сервера RADIUS от ASA. Если эхо-запрос работает без какой-либо проблемы, то проверьте Связанную с радиусом конфигурацию на ASA и конфигурацию базы данных на сервере RADIUS.

Вы могли использовать **команду debug radius** для устранения проблем связанных проблем радиуса. Для **выходных данных radius примера отладки** обратитесь к этому Примеру выходных данных.

Примечание: Перед использованием **команды отладки** на ASA обратитесь к этой документации: Предупреждающее сообщение.

Соединение Отбрасываний Клиента VPN Часто на Первой Попытке или "VPN-подключении безопасности, завершенном узлом. Причина 433". или "Безопасное VPN-подключение, завершенное Одноранговой Причиной 433: (Причина, Не Указанная Узлом)"

Проблема

Пользователи Клиента Cisco VPN могли бы получить эту ошибку, когда они делают попытку соединения с устройством VPN головного узла.

"*Клиент VPN часто отбрасывает соединение на первой попытке*" или "*VPN-подключении безопасности, завершенном узлом. Причина 433*". или "*Безопасное VPN-подключение, завершенное Одноранговой Причиной 433: (Причина, Не Указанная Узлом)*" или "*Предпринятый для присвоения сети или адреса широковещательного IP, удаляя (x. x. x. x) от пула*"

Решение 1

Проблема могла бы быть с присвоением пула IP или через ASA/PIX, сервер RADIUS, сервер DHCP или через сервер RADIUS, действующий как сервер DHCP. Используйте **команду debug crypto**, чтобы проверить, что маска подсети и IP-адреса корректны. Кроме того, проверьте, что пул не включает сетевой адрес и широковещательный адрес. Серверы RADIUS должны быть в состоянии назначить надлежащие IP-адреса на клиентов.

Решение 2

Эта проблема также происходит из-за сбоя расширенной проверки подлинности. Необходимо проверить AAA-сервер для устранения проблем этой ошибки. Проверка пароля проверки подлинности сервера на Сервере и клиенте и повторная загрузка AAA-сервера могли бы решить этот вопрос.

Решение 3

Другой обходной путь для этой проблемы должен отключить опцию обнаружения угрозы. Время от времени, когда существуют множественные повторные передачи для других неполных Сопоставлений безопасности (SA), ASA с активированной опцией обнаружения угрозы думает, что атака сканирования происходит, и порты VPN отмечены как основной преступник. Попытайтесь отключить опцию обнаружения угрозы, поскольку это может вызвать много издержек на обработке ASA. Используйте эти команды для отключения обнаружения угрозы:

```
no threat-detection basic-threat
no threat-detection scanning-threat shun
no threat-detection statistics
no threat-detection rate
```

Для получения дополнительной информации об этой функции, обратитесь к Обнаружению Угрозы.

Примечание: Это может использоваться в качестве обходного пути, чтобы проверить, исправляет ли это актуальную проблему. Удостоверьтесь, что отключение обнаружения угрозы на Cisco ASA фактически ставит под угрозу несколько характеристик безопасности, таких как смягчение Попыток Сканирования, DoS с Недопустимым SPI, пакеты, которые отказывают Контроль приложения и Неполные Сеансы.

Решение 4

Когда набор преобразований должным образом не настроен, эта проблема также происходит. Правильная конфигурация набора преобразований решает вопрос.

Удаленный доступ и пользовательское подключение EZVPN к

VPN, но не могут обратиться к внешним ресурсам

Проблема

У пользователей удаленного доступа нет интернет-соединения, как только они соединяются с VPN.

Пользователи удаленного доступа не могут обратиться к ресурсам, расположенным позади других VPN на том же устройстве.

Пользователи удаленного доступа могут обратиться только к локальной сети.

Решения

Попробуйте эти решения для решения этого вопроса:

- Неспособный обратиться к серверам в DMZ
- Клиенты VPN, неспособные решить DNS
- Разделение туннеля — Неспособный обратиться к Интернету или исключенным сетям
- Прикрепление
- Доступ к локальной сети
- Наложения частной сети

Неспособный обратиться к серверам в DMZ

Как только клиент VPN установлен Туннель IPSec с устройством головного узла VPN (PIX/ASA/МАРШРУТИЗАТОР IOS), Пользователи VPN-клиента в состоянии обратиться к Внутренней сети (10.10.10.0/24) ресурсы, но они неспособны обратиться к сети DMZ (10.1.1.0/24).

Схема

Проверьте, что Разделение туннеля, НИКАКАЯ конфигурация NAT не добавлена в устройстве головного узла для доступа к ресурсам в сети DMZ.

Пример

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
```

Конфигурация версии ASA 8.3:

Эта конфигурация показывает, как настроить освобождение NAT для сети DMZ, чтобы позволить пользователям VPN обратиться к сети DMZ:

```
object network obj-dmz
subnet 10.1.1.0 255.255.255.0
object network obj-vpnpool
subnet 192.168.1.0 255.255.255.0
nat (inside,dmz) 1 source static obj-dmz obj-dmz destination static obj-vpnpool obj-vpnpool
```

После добавления новой записи для конфигурации NAT очистите преобразование NAT.

```
Clear xlate
Clear local
```

Проверка:

Если туннель был установлен, переходит **к Cisco VPN Client** и выбирает **Status> Route Details**, чтобы проверить, что защищенные маршруты показывают и для DMZ и для Внутренних сетей.

Подробное описание настройки сети VPN на базе IPSec между двумя узлами в устройстве защиты Cisco с версией ПО 7.x см. в документе PIX/ASA 7.x: Доступ Почтового сервера на Примере Конфигурации DMZ для получения дополнительной информации о том, как установить Межсетевой экран PIX для доступа к почтовому серверу, расположился в сети Demilitarized Zone (DMZ).

Подробное описание настройки сети VPN на базе IPSec между двумя узлами в устройстве защиты Cisco с версией ПО 7.x см. в документе PIX/ASA 7.x: Добавьте Новый Туннель или Удаленный доступ к Существующей VPN L2L для обеспечения шагов, требуемых добавить новый VPN-туннель или VPN для удаленного доступа к конфигурации VPN L2L, которая уже существует.

Подробное описание настройки сети VPN на базе IPSec между двумя узлами в устройстве защиты Cisco с версией ПО 7.x см. в документе PIX/ASA 7.x: Позвольте Разделенное туннелирование для Клиентов VPN на Примере конфигурации ASA для обеспечения пошаговых инструкций о том, как предоставить доступ Клиентов VPN к Интернету, в то время как они туннелированы в устройство адаптивной защиты Cisco (ASA) Устройство безопасности серии 5500.

См. PIX/ASA 7.x и Cisco VPN Client 4.x с Windows 2003 IAS RADIUS (Против Active Directory) Пример Конфигурации аутентификации для получения дополнительной информации о том, как установить соединение VPN для удаленного доступа между Cisco VPN Client (4.x для Windows) и устройством защиты PIX 500 Series 7. x.

Клиенты VPN, неспособные решить DNS

После того, как туннель был установлен, если Клиенты VPN неспособны решить DNS, проблемой может быть конфигурация Сервера DNS в устройстве головного узла (ASA/PIX). Также проверьте подключение между Клиентами VPN и Сервером DNS. Конфигурация

Сервера DNS должна быть настроена под групповой политикой и применена под групповая политика в туннельной группе общие атрибуты; пример:

```
!--- 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
```

Клиенты VPN, неспособные подключить внутренние серверы по имени

Клиент VPN неспособен пропинговать хосты или серверы удаленной внутренней сети или внутренней сети головного узла по имени. Необходимо включить split-dns, настраивают на ASA для решения этого вопроса.

Разделение туннеля — Неспособный обратиться к Интернету или исключенным сетям

Разделенное туннелирование позволяет Клиентам IPSEC удаленного доступа условно прямые пакеты по Туннелю IPSec в зашифрованной форме или прямые пакеты к сетевому интерфейсу в форме открытого текста, дешифрованной, где они тогда маршрутизируются к конечному назначению. Раздельное туннелирование отключено по умолчанию, который является трафиком `tunnelall`.

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

Примечание: Опция ***excludespecified*** поддерживается только для клиентов Cisco VPN, не Клиентов EzVPN.

```
ciscoasa(config-group-policy)#split-tunnel-policy excludespecified
```

См. эти документы для примеров подробной конфигурации раздельного туннелирования:

- PIX/ASA 7.X : Пример конфигурации устройства ASA, разрешающей раздельное туннелирование для VPN-клиентов
- Пример конфигурации маршрутизатора, разрешающего VPN-клиентам подключаться к узлам по протоколу IPsec и к сети Интернет, с использованием раздельного туннелирования
- Пример настройки расщепления туннелей для клиентов VPN на концентраторе VPN 3000

Прикрепление

Эта функция полезна для трафика VPN, который входит по интерфейсу и маршрутизируется на выход из этого же 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 конфигурацию **same-security-traffic**, чтобы позволить трафику вводить и выходить из того же интерфейса.

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

Доступ к локальной сети

Пользователи удаленного доступа соединяются с VPN и в состоянии соединиться с локальной сетью только.

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

Наложения частной сети

Проблема

Если вы неспособны обратиться к внутренней сети после установки туннеля, проверьте IP-адрес, назначенный на клиент VPN, который накладывается на внутреннюю сеть позади устройства головного узла.

Решение

Всегда удостоверяйтесь, что IP-адреса в пуле, который будет назначен для клиентов VPN, внутренней сети устройства головного узла и внутренней сети Клиента VPN, должны быть в других сетях. Можно назначить ту же крупную сеть с другими подсетями, но иногда происходят проблемы маршрутизации.

Для дальнейших примеров см. *Схему* и *Пример* Неспособного для Доступа к Серверам в разделе DMZ.

Неспособный подключить больше чем Трех пользователей VPN-клиента

Проблема

Только три клиента VPN могут соединиться с ASA/PIX; соединение для четвертых клиентских сбоев. После сбоя отображено это сообщение об ошибках:

```
Secure VPN Connection terminated locally by the client.
 Reason 413: User Authentication failed.tunnel rejected; the maximum tunnel count has been
reached
```

Решения

В большинстве случаев эта проблема отнесена к одновременному значению входа в систему в групповой политике и максимальном session-limit.

Попробуйте эти решения для решения этого вопроса:

- Настройте одновременные входы в систему
- Настройка ASA/PIX в интерфейсе командной строки
- Настройте концентратор, настраивают концентратор

Для получения дополнительных сведений см. раздел Настройка групповых политик Выбранные процедуры настройки ASDM VPN для Cisco ASA серии 5500, версия 5.2.

Настройте одновременные входы в систему

Если флажок **Inherit** в ASDM проверен, только число по умолчанию одновременных входов в систему позволено для пользователя. Значение по умолчанию для одновременных входов в систему равняется трем.

Для решения этого вопроса увеличьте стоимость для одновременных входов в систему.

1. ASDM запуска и затем перешел к **Конфигурации> VPN> Групповая политика**.
2. Выберите соответствующую **Группу** и нажмите **кнопку Edit**.
3. Однажды во **Вкладке Общие**, отмените флажок **Inherit** для **Одновременных Входов в систему** при **Настройках соединения**. Выберите соответствующее значение в поле.**Примечание:** Минимальное значение для этого поля 0, который отключает вход в систему и предотвращает пользовательский доступ.**Примечание:** При регистрации в использование той же учетной записи пользователя от другого ПК текущий сеанс (соединение, установленное от другого ПК с помощью той же учетной записи пользователя), завершен, и новый сеанс установлен. Это - поведение по умолчанию и независимо к VPN одновременные входы в систему.

Настройка ASA/PIX в интерфейсе командной строки

Выполните эти шаги для настройки необходимого номера одновременных входов в систему. В данном примере, 20 был выбран в качестве желаемого значения.

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

Для узнавания больше об этой команде обратитесь к Справочнику по командам Cisco Security Appliance, Версии 7.2.

Используйте **команду vpn-sessiondb max-session-limit** в режиме глобальной конфигурации для ограничения сеансов VPN минимальным значением, чем устройство безопасности позволяет. Используйте версию `no` этой команды для удаления предела сеанса. Используйте команду снова для перезаписи текущего параметра.

```
vpn-sessiondb max-session-limit {session-limit}
```

Данный пример показывает, как установить максимальный предел сеанса VPN 450:

```
hostname#vpn-sessiondb max-session-limit 450
```

Настройте концентратор

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

Решение

Выполните эти шаги для настройки необходимого номера одновременных входов в систему. Можно также попытаться установить Одновременные Входы в систему в 5 для этого SA:

Choose Configuration> User Management> Groups> Modify 10.19.187.229> Общий> Одновременные Входы в систему и изменяет количество входов в систему к **5**.

Неспособный Инициировать Сеанс или Приложение и Медленную Передачу после Установки туннеля

Проблема

После установления Туннеля IPSec, приложения или сеанса не инициирует через туннель.

Решения

Используйте команду ping для проверки работы сети или проверьте доступность сервера приложений из сети пользователя. Это может быть проблема с Maximum Segment Size (MSS) для переходных пакетов, которые пересекают маршрутизатор или устройство PIX/ASA, в частности сегменты TCP с установленным битом SYN.

Маршрутизатор Cisco IOS — изменяет значение MSS во внешнем интерфейсе (туннельный интерфейс конца) маршрутизатора

Выполните эти команды для изменения значения MSS во внешнем интерфейсе (туннельный интерфейс конца) маршрутизатора:

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

Эти сообщения показывают выходные данные отладки для TCP MSS:

```
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)]
```

MSS отрегулирован к 1300 на маршрутизаторе согласно конфигурации.

Для получения дополнительной информации обратитесь к PIX/ASA 7.x и IOS: Фрагментация VPN.

PIX/ASA 7. X — см. Документацию PIX/ASA

Существует неспособность обратиться к Интернету должным образом или медленной передаче через туннель, потому что это дает сообщение об ошибках максимального размера передаваемого блока данных и проблемы MSS. См. эти документы для решения вопроса:

- PIX/ASA 7.x и IOS: Фрагментация VPN
- Проблема PIX/ASA 7.0: Превышено допустимое значение MSS — HTTP-клиенты не могут просматривать определенные веб-узлы

Неспособный инициировать VPN-туннель от ASA/PIX

Проблема

Вы неспособны инициировать VPN-туннель от интерфейса ASA/PIX, и после того, как установка туннеля, Клиент/VPN удаленного конца будет неспособен пропинговать внутренний интерфейс ASA/PIX на VPN-туннеле. Например, pn клиент может быть неспособен инициировать SSH или соединение HTTP к Внутреннему интерфейсу ASA по VPN-туннелю.

Решение

Внутренний интерфейс PIX не может быть пропингован от другого конца туннеля, пока **команда management-access** не настроена в режиме глобальной конфигурации.

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

Примечание: Эта команда также помогает в инициировании ssh или соединения http с внутренним интерфейсом ASA через VPN-туннель.

Примечание: Эта информация сохраняется для интерфейса DMZ также. Например, если вы хотите пропинговать интерфейс DMZ PIX/ASA или хотеть инициировать туннель от интерфейса DMZ, тогда **команда management-access DMZ** требуется.

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

Примечание: Если клиент VPN неспособен соединиться, то удостоверьтесь ESP, и порты UDP открыты, однако если те порты не открыты, тогда пытаются соединиться на TCP 10000 с выбором этого порта при записи подключения VPN Client. Щелчок правой кнопкой **модифицирует> вкладка Передача> IPsec по TCP**. См. PIX/ASA 7.x для Поддержки IPsec по TCP на любом Примере Конфигурации порта для получения дополнительной информации о IPsec по TCP.

Неспособный передать трафик через VPN-туннель

Проблема

Вы неспособны передать трафик через VPN-туннель.

Решение

Эта проблема происходит из-за проблемы, описанной в идентификаторе ошибки Cisco CSCtb53186 (только зарегистрированные клиенты). Для решения этого вопроса повторно загрузите ASA. См. дефект для получения дополнительной информации.

Когда пакеты ESP заблокированы, эта проблема могла бы также произойти. Для решения этого вопроса, реконфигурировав VPN-туннель.

Когда данные не зашифрованы, но только дешифрованы по VPN-туннелю как показано в этих выходных данных, эта проблема могла бы произойти:

```
ASA# sh crypto ipsec sa peer x.x.x.x
peer address: y.y.y.y
    Crypto map tag: IPSec_map, seq num: 37, local addr: x.x.x.x
```

```
      access-list test permit ip host xx.xx.xx.xx host yy.yy.yy.yy
      local ident (addr/mask/prot/port): (xx.xx.xx.xx/255.255.255.255/0/0)
      remote ident (addr/mask/prot/port): (yy.yy.yy.yy/255.255.255.255/0/0)
      current_peer: y.y.y.y

     #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0 #pkts decaps: 393, #pkts decrypt: 393,
#pkts verify: 393 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts comp
failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments
created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #send
errors: 0, #recv errors: 0
```

Для решения этого вопроса проверьте придерживающееся:

1. И если крипто-соответствие access-lists с удаленным узлом, что access-lists NAT 0 корректен.
2. Если маршрутизация корректна, и трафик действительно поражает внешний интерфейс, проходящий внутри. Пример выходных данных показывает, что расшифровка сделана, но не происходит шифрование.
3. Если команда connection-vpn разрешения на sysopt была настроена на ASA. Если не настроенный, настройте эту команду, потому что она позволяет ASA освобождать ЗАШИФРОВАННЫЙ/ТРАФИК VPN от интерфейсной проверки ACL.

Резервный узел Настройки для vpn туннелирует на той же криптокарте

Проблема

Вы хотите использовать узлы множественного резервирования для одиночного туннеля vpn.

Решение

Множественные одноранговые телефонные соединения Настройки эквивалентны обеспечению списка нейтрализации. Для каждого туннеля устройство безопасности пытается выполнить согласование с первым узлом в списке.

Если тот узел не отвечает, устройство безопасности прокладывает себе путь вниз список, пока или узел не отвечает или в списке больше нет узлов.

ASA нужно настроить криптокарту уже как основную адресуемую точку. Вторичный узел мог быть добавлен после основного.

Конфигурация данного примера показывает основную адресуемую точку как X.X.X.X и резервный узел как Y.Y.Y.Y:

```
ASA(config)#crypto map mymap 10 set peer X.X.X.X Y.Y.Y.Y
```

Для получения дополнительной информации обратитесь к одноранговому разделу набора Криптокарты в *Справочнике по командам Cisco Security Appliance, Версии 8.0*.

Отключите/Перезапустите VPN-туннель

Проблема

Чтобы временно отключить VPN-туннель и перезапустить сервис, завершите процедуру, описанную в этом разделе.

Решение

Используйте **команду crypto map interface** в режиме глобальной конфигурации для удаления ранее определенного набора криптокарты к интерфейсу. Используйте **эту команду с параметром no** для удаления набора криптокарты из интерфейса.

```
hostname(config)#no crypto map map-name interface interface-name
```

Эта команда удаляет набор криптокарты к любому интерфейсу устройства активной безопасности, и сделайте VPN-туннель IPSec неактивным в том интерфейсе.

Для перезапуска Туннеля IPSec на интерфейсе необходимо назначить набор криптокарты на интерфейс, прежде чем тот интерфейс сможет предоставить Сервисы IPSec.

```
hostname(config)#crypto map map-name interface interface-name
```

Некоторые Туннели, не Зашифрованные

Проблема

Когда очень большой номер туннелей настроен на Шлюзе VPN, некоторые туннели не передают трафик. ASA не получает зашифрованные пакеты для тех туннелей.

Решение

Эта проблема происходит, потому что ASA не в состоянии передавать зашифрованные пакеты через туннели. Двойные правила шифрования созданы в таблице ASP. Это - известная неполадка и идентификатор ошибки, CSCtb53186 (только зарегистрированные клиенты) был подан для рассмотрения этой проблемы. Для решения, этот вопрос, или повторно загружают ASA или обновляют программное обеспечение к версии, в которой исправлена эта ошибка.

Ошибка: - %ASA-5-713904: Группа = DefaultRAGroup, IP = x. x. x. x, Клиент использует неподдерживаемый Режим транзакции v2 версия. Туннель завершился.

Проблема

Сообщение об ошибках `%ASA-5-713904: Group = DefaultRAGroup, IP = 99.246.144.186, Client is using an unsupported Transaction Mode v2 version.Tunnel terminated` появляется.

Решение

Причина для сообщения об ошибках `Transaction Mode v2` состоит в том, что ASA поддерживает только Настройку режима IKE V6 а не старая версия режима V2. Используйте Настройку режима IKE версия V6 для решения этой ошибки.

Ошибка: - %ASA-6-722036: Пользователь группы клиентов Группы xxxx IP x. x. x. x Передающий большой пакет 1220 (порог 1206)

Проблема

Сообщение об ошибках `%ASA-6-722036: Group < client-group > User < xxxx > IP < x.x.x.x> Transmitting large packet 1220 (threshold 1206)` появляется в журналах ASA. Что это регистрирует средства и как это может быть решено?

Решение

Это сообщение журнала сообщает, что большой пакет был передан клиенту. Источник пакета не знает о MTU клиента. Это может также произойти из-за сжатия несжимаемых данных. Обходной путь должен выключить сжатие SVC со сжатием обращения к операционной системе ни один команда, которая решает вопрос.

Ошибка: Группа сервера аутентификации ни один команда была осуждена

Проблема

Если вы передаете конфигурацию VPN от PIX/ASA, который выполняет Версию 7.0.x к другому устройству безопасности, которое выполняется 7.2.x, вы получаете это сообщение об ошибках:

```
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.
```

Решение

Команда authentication-server-group больше не поддерживается в 7.2 (1) и позже. Эта команда осуждалась и переместилась в режим конфигурации общих атрибутов туннельной группы.

См. раздел ikev1-проверка-подлинности-пользователи isakmp Справочника по командам для получения дополнительной информации об этой команде.

Сообщение об ошибках, когда QoS Включено в одном Конце VPN-туннеля

Проблема

При включении QoS в одном конце VPN-туннеля вы могли бы получить это сообщение об ошибках:

```
IPSEC: Received an ESP packet (SPI= 0xDB6E5A60, sequence number= 0x7F9F) from
```

`10.18.7.11 (user= ghufhi) to 172.16.29.23 that failed anti-replay checking`

Решение

Когда один конец туннеля делает QoS, это сообщение обычно вызывается. Когда пакет обнаружен как не то, чтобы работать, это происходит. Можно отключить QoS для остановки этого, но оно может быть проигнорировано, пока трафик в состоянии пересечь туннель.

% Warning: элемент криптокарты будет неполным

Проблема

При выполнении **команды crypto map mymap 20 ipsec-isakmp** вы могли бы получить эту ошибку:

`% Warning:`

Пример:

`ciscoasa(config)#`**`crypto map mymap 20 ipsec-isakmp WARNING: crypto map entry will be incomplete`**

Решение

Это - обычное предупреждение при определении новой криптокарты, напоминание, что параметры, такие как access-list (адрес соответствия), набор преобразований и адрес партнера (peer) должны быть настроены, прежде чем это сможет работать. Это также обычно, который первая линия, которую вы вводите для определения криптокарты не показывает в конфигурации.

Ошибка: - %ASA-4-400024: IDS:2151 Большой пакет ICMP от к на интерфейсе снаружи

Проблема

Неспособный передать большой ping - пакет через туннель vpn. Когда мы пытаемся передать большие ping - пакеты, мы получаем ошибку `%ASA-4-400024: IDS:2151 Large ICMP packet from to on interface outside`

Решение

Отключите подписи 2150 и 2151 для решения этого вопроса. Как только подписи отключены, эхо-запрос хорошо работает.

Используйте эти команды для отключения подписей:

ASA (config) **#ip контрольная подпись 2151 отключает**

ASA (config) **#ip контрольная подпись 2150 отключает**

Ошибка: - %PIX|ASA-4-402119: IPSec: Полученный пакет

протокола (SPI=spi, порядковый номер = seq_num) от remote_IP (имя пользователя) к local_IP, который отказал проверку антивоспроизведения.

Проблема

Я получил эту ошибку в сообщениях журнала ASA:

```
: - %PIX|ASA-4-402119: IPSec:    (SPI=spi,    = seq_num)  remote_IP ( )  local_IP,     .
```

Решение

Для решения этой ошибки используйте команду crypto ipsec security-association replay window-size для варьирования размера окна.

```
hostname(config)#crypto ipsec security-association replay window-size 1024
```

Примечание: Cisco рекомендует использовать полные 1024 размера окна для устранения любых проблем антивоспроизведения.

Сообщение об ошибках - %PIX|ASA-4-407001: Запретите трафик для local-host interface_name:inside_address, ограничение лицензии номера превысило

Проблема

Немного хостов неспособны соединиться с Интернетом, и это сообщение об ошибках появляется в системном журнале:

```
Error Message - %PIX|ASA-4-407001: Deny traffic for local-host interface_name:inside_address,
license limit of number exceeded
```

Решение

Когда количество пользователей превышает пользовательский предел используемой лицензии, это сообщение об ошибках получено. Эта ошибка может быть решена путем обновления лицензии на более высокое количество пользователей. Лицензия пользователя может включать 50, 100, или неограниченные пользователи как требуется.

Сообщение об ошибках - %VPN_HW-4-PACKET_ERROR:

Проблема

Сообщение об ошибках `Error Message - %VPN_HW-4-PACKET_ERROR:` указывает, что не соответствуют пакету ESP с HMAC, полученным маршрутизатором. Эта ошибка могла бы быть вызвана этими проблемами:

- Дефектная VPN модуль H/W

- Поврежденный пакет ESP

Решение

Для решения этого сообщения об ошибках:

- Проигнорируйте сообщения об ошибках, пока нет нарушение трафика.
- Если существует нарушение трафика, замените модуль.

: Команда отклонила: удалите крипто-соединение между VLAN XXXX и XXXX, сначала.

Проблема

Когда вы пытаетесь добавить позволенный VLAN на магистральном порте на коммутаторе, это сообщение об ошибках появляется: `Command rejected: delete crypto connection between VLAN XXXX and VLAN XXXX, first..`

Граничный транк глобальной сети (WAN) не может модифицироваться для разрешения дополнительных VLAN. Т.е. вы неспособны добавить VLAN в транке SPA IPSEC VPN.

Эта команда отклонена, потому что разрешение ее приведет к крипто-VLAN связанного интерфейса, которая принадлежит позволенному списку VLAN интерфейса, который излагает потенциальное нарушение Безопасности IPsec. Обратите внимание на то, что это поведение применяется ко всем магистральным портам.

Решение

Вместо команды `no switchport trunk allowed vlan (vlanlist)` используйте команду `switchport trunk allowed vlan none` или команду `"switchport trunk allowed vlan remove (vlanlist)"`.

Сообщение об ошибках - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Отбрасывание пакета - опция Invalid Window Scale для сеанса x. x. x. x: 27331 к x. x. x. x: 23 [Инициатор (отмечают 0, разлагают на множители 0), Респондент (отмечают 1, разлагают на множители 2)]

Проблема

Эта ошибка происходит, когда вы пробуете к telnet от устройства на дальнем конце VPN-туннеля или когда вы пробуете к telnet от самого маршрутизатора:

```
Error Message - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Dropping packet - Invalid Window Scale option for session x.x.x.x:27331 to x.x.x.x:23 [Initiator(flag 0,factor 0) Responder (flag 1, factor 2)]
```

Решение

Лицензия пользователя может включать 50, 100, или неограниченные пользователи как требуется. Масштабирование окна было добавлено для учета быстрой передачи данных на длинных толстых сетях (LFN). Это, как правило, соединения с очень высокой пропускной способностью, но также и большая задержка. Сети со спутниковыми подключениями являются одним примером LFN, так как соединения Satellite всегда имеют высокие задержки распространения, но, как правило, имеют высокую пропускную способность. К окну enable, масштабирующемуся для поддержки LFNs, размер окна TCP должен быть больше чем 65,535. Это сообщение об ошибках может быть решено путем увеличения размера окна TCP, чтобы быть больше чем 65,535.

%ASA-5-305013: Асимметричные правила NAT совпали для форварда и реверса. Обновите эту проблему потоки

Проблема

Это сообщение об ошибках появляется, как только подходит VPN-туннель:

```
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse . Please update this issue
flows
```

Решение

Для решения этого вопроса если не о том же интерфейсе как хост с помощью NAT, используйте сопоставленный адрес вместо фактического адреса для соединения с хостом. Кроме того, включите **команду inspect**, если приложение встраивает IP-адрес.

%PIX|ASA-5-713068: Полученная неподпрограмма Уведомляет сообщение: notify_type

Проблема

Если VPN-туннель не в состоянии подходить, это сообщение об ошибках появляется:

```
%PIX|ASA-5-713068: Received non-routine Notify message: notify_type
```

Решение

Это сообщение происходит из-за неверной конфигурации (т.е. когда политика или ACL не настроены, чтобы быть тем же на узлах). Как только с политикой и ACL совпадают, туннель подходит без любой проблемы.

%ASA-5-720012: (Вторичный VPN) Отказавший для обновления данных времени выполнения аварийного переключения IPSec на резервном модуле (или) %ASA-6-

720012: (модуль VPN), Отказавший для обновления данных времени выполнения аварийного переключения IPsec на резервном модуле

Проблема

Когда вы пытаетесь обновить устройство адаптивной защиты Cisco (ASA), одно из этих сообщений об ошибках появляется:

```
%ASA-5-720012: (VPN-Secondary) Failed to update IPSec failover runtime data on the standby unit.

%ASA-6-720012: (VPN-unit) Failed to update IPsec failover runtime data on the standby unit.
```

Решение

Эти сообщения об ошибках являются информативными ошибками. Сообщения не влияют на функциональность ASA или VPN.

Эти сообщения появляются, когда подсистема аварийного переключения VPN не может обновить Связанные с ipsec данные во время выполнения, потому что соответствующий Туннель IPSec был удален на резервном модуле. Для решения их выполните **команду wr standby** на активном модуле.

Два дефекта были поданы для адресации к этому поведению и обновлению к версии программного обеспечения ASA, где исправлены эти ошибки. См. идентификаторы ошибок Cisco CSCtj58420 (только зарегистрированные клиенты) и CSCtn56517 (только зарегистрированные клиенты) для получения дополнительной информации.

Ошибка: - %ASA-3-713063: Адрес партнера (peer) IKE, не настроенный для назначения 0.0.0.0

Проблема

Сообщение об ошибках `%ASA-3-713063: IKE Peer address not configured for destination 0.0.0.0` появляется, и туннель не в состоянии подходить.

Решение

Когда адрес партнера (peer) IKE не настроен для туннеля L2L, это сообщение появляется. Эта ошибка может быть решена путем изменения порядкового номера криптокарты, затем удаления и повторного применения криптокарты.

Ошибка: %ASA-3-752006: Туннельный Менеджер был не в состоянии диспетчеризировать сообщение KEY_ACQUIRE.

Проблема

Сообщение об ошибках `%ASA-3-752006: Tunnel Manager failed to dispatch a KEY_ACQUIRE message.Probable mis-configuration of the crypto map or tunnel-group."` зарегистрировано на Cisco ASA.

Решение

Это сообщение об ошибках может быть вызвано неверной конфигурацией криптокарты или туннельной группы. Гарантируйте, что оба настроены должным образом. Для получения дополнительной информации об этом сообщении об ошибках, обратитесь к Ошибке 752006.

Вот некоторые корректирующие действия:

- Удалите крипто-ACL (например, привязанный к динамической схеме).
- Удалите неиспользованную связанную конфигурацию IKEv2, если таковые имеются.
- Проверьте, что крипто-ACL совпал должным образом.
- Удалите двойные записи access-list, если таковые имеются.

Ошибка: %ASA-4-402116: IPSec: Полученный пакет ESP (SPI = 0x99554D4E, порядковый номер = 0x9E) от XX.XX.XX.XX (user = XX.XX.XX.XX) к YY.YY.YY.YY

В настройке Туннеля VPN между локальными сетями эта ошибка получена на одном конечном ASA:

```
The decapsulated inner packet doesn't match the negotiated policy in the SA.

The packet specifies its destination as 10.32.77.67, its source as 10.105.30.1, and its protocol as icmp.

The SA specifies its local proxy as 10.32.77.67/255.255.255.255/ip/0 and its remote_proxy as 10.105.42.192/255.255.255.224/ip/0.
```

Решение

Необходимо проверить access-lists представляющего интерес трафика, определенный на обоих концах VPN-туннеля. Оба должны совпасть как точные зеркальные образы.

Подведенный для запуска 64-разрядного установщика BA для включения виртуального адаптера из-за ошибки 0xffffffff

Проблема

Когда AnyConnect не в состоянии соединяться, сообщение журнала `Failed to launch 64-bit VA installer to enable the virtual adapter due to error 0xffffffff` получено.

Решение

Для устранения указанной неполадки выполните следующие действия:

1. Перейдите **к Системе> интернет-менеджмент Связи> интернет-параметры настройки Связи** и удостоверьтесь, что **Выключают Автоматическое Обновление Корневых сертификатов**, отключен.
2. Если это отключено, то отключите всю **Административную** часть **Шаблона** GPO, назначенного на машину, на которую влияют, и тест снова.

См. Выключают Автоматическое Обновление Корневых сертификатов для получения дополнительной информации.

Ошибка 5: Отсутствует имя хоста для этого подключения. Невозможно установить VPN-подключение.

Проблема

Сообщение об ошибках `Error 5: No hostname exists for this connection entry. Unable to make VPN connection` получено во время новой установки ПК.

Решение

Эта проблема происходит из-за идентификатора ошибки Cisco CSCso94244 (только зарегистрированные клиенты). Для получения дополнительных сведений обратитесь к документации по данной ошибке.

Cisco VPN Client не работает с картой данных на Windows 7

Проблема

Cisco VPN Client не работает с картой данных на Windows 7.

Решение

Cisco VPN Client, установленный на Windows 7, не работает с соединениями 3G, так как карты данных не поддерживаются на клиентах VPN, установленных на машине Windows 7.

Предупреждающее сообщение: "Функциональные возможности VPN могут не работать вообще"

Проблема

При попытке включить isakmp на внешнем интерфейсе ASA, получено это предупреждающее сообщение:

```
ASA(config)# crypto isakmp enable outside
WARNING, system is running low on memory.  Performance may start to degrade.
VPN functionality may not work at all.
```

На этом этапе обратитесь к ASA через ssh. HTTPS остановлен, и на других клиентов SSL также влияют.

Решение

Эта проблема происходит из-за требований к памяти другими модулями, такими как регистратор и крипто-. Удостоверьтесь, что у вас нет **команды logging queue 0**. Это делает набор размера очереди к 8192, и распределение памяти поднимается.

В платформах, таких как ASA5505 и ASA5510, это распределение памяти склоняется к памяти - исчерпали ресурсы другие модули (IKE и и т.д.). Идентификатор ошибки Cisco CSCtb58989 (только зарегистрированные клиенты) был зарегистрирован для адресации к подобному типу поведения. Для решения этого настройте logging queue к меньшему значению, такой как 512.

Ошибка Заполнения IPSec

Проблема

Это сообщение об ошибках получено:

```
%PIX|ASA-3-402130: CRYPTO: Received an ESP packet (SPI =
 0xXXXXXXX, sequence number= 0xXXXX) from x.x.x.x (user= user) to y.y.y.y with
 incorrect IPsec padding
```

Решение

Проблема происходит, потому что IPSEC VPN выполняет согласование без алгоритма хеширования. Пакетное хеширование гарантирует проверку целостности для канала ESP. Поэтому без хеширования, неправильна сформированные пакет приняты необнаруженные Cisco ASA, и это пытается дешифровать эти пакеты. Однако, потому что эти пакеты неправильно сформированы, ASA находит дефекты при дешифровании пакета. Это вызывает сообщения об ошибках заполнения, которые замечены.

Рекомендация состоит в том, чтобы включать алгоритм хэширования в набор преобразований для VPN и гарантировать, что ссылка между узлами имеет минимальный пакетный дефект.

Время задержки Тишины в эфире по удаленным телефонам узла

Проблема

Время задержки тишины в эфире испытано по удаленным телефонам узла. Как устранить эту проблему?

Решение

Отключите облегченную и проверку SIP для решения этой проблемы:

```
asa(config)# no inspect sip asa(config)# no inspect skinny
```

VPN-туннель разъединен после каждых 18 часов

Проблема

VPN-туннель разъединен после каждых 18 часов даже при том, что срок действия установлен в течение 24 часов.

Решение

Срок действия является максимальным временем, SA может использоваться для смены ключа. Значение, которое вы вводите в конфигурацию как срок действия, является другим с повторно вводить времени SA. Поэтому необходимо выполнить согласование о новом SA (или пара SA в случае IPsec), прежде чем истечет текущий. Повторно вводить время должно всегда быть меньшим, чем срок действия для получения возможности множественных попыток в случае, если первые повторно вводят сбои попытки. RFC не задают, как вычислить повторно вводить время. Это оставляют усмотрению лиц, осуществляющих внедрение. Поэтому время будет варьироваться в зависимости от используемой платформы, который версия программного обеспечения, и т.д.

Некоторые реализации могут использовать случайный фактор для вычисления повторно вводить таймера. Например, если ASA инициирует туннель, то это обычно, который это повторно введет в 64800 секунд = 75% из 86400. Если маршрутизатор инициирует, то ASA может ждать дольше, чтобы дать узлу больше времени для инициирования повторно введения. Таким образом это обычно, что сеанс VPN разъединен каждые 18 часов для использования другого ключа для согласования VPN. Это не должно вызывать отбрасывание VPN или проблему.

Трафик не поддержан после того, как LAN в туннель LAN пересмотрена

Проблема

Трафик не поддержан после того, как LAN в туннель LAN пересмотрена.

Решение

ASA контролирует каждое соединение, которое проходит через него и поддерживает запись в ее таблице состояний согласно функции контроля приложения. Подробные данные зашифрованного потока данных, которые проходят через VPN, поддержаны в форме базы данных сопоставления безопасности (SA). Для LAN к VPN-подключениям LAN это поддерживает два других трафика. Каждый - зашифрованный поток данных между Шлюзами VPN. Другой трафик между сетевым ресурсом позади Шлюза VPN и конечным пользователем позади другого конца. Когда VPN завершена, подробные данные потока для этого определенного SA удалены. Однако запись таблицы состояний, поддержанная ASA для этого TCP - подключения, становится устаревшей ни из-за какого действия, которое препятствует загрузке. Это означает, что ASA все еще сохранит TCP - подключение для того отдельного потока, в то время как завершается пользовательское приложение. Однако TCP - подключения станут случайными и в конечном счете таймаут после того, как истечет таймер простоя TCP.

Эта проблема была решена путем представления функции под названием Туннелировавшие Потоки Персистентного IPSec. Новая команда, потоки vpn заповедника

соединения sysopt, была интегрирована в Cisco ASA для сохранения информации о таблице состояний на пересмотре VPN-туннеля. По умолчанию эта команда отключена. Когда VPN L2L восстановится с разрушения и восстановит туннель, путем включения этого Cisco ASA поддержит сведения таблицы состояния TCP.

Сообщение об ошибках сообщает, что Пропускная способность достигла Крипто-функциональности

Проблема

Это сообщение об ошибках получено на маршрутизаторе серии 2900:

```
: 20  10:51:29: %CERM-4-TX_BW_LIMIT:     Tx 85000 /  -  securityk9   .
```

Решение

Это - известная неполадка, которая происходит из-за строгих рекомендаций, выполненных Правительством США. Согласно этому, securityk9 лицензия может только позволить шифрованию полезной нагрузки до скоростей близко к 90 Мбит/с и ограничить количество зашифрованных сеансов туннелей/TLS к устройству. Для получения дополнительной информации о крипто-ограничениях экспорта, обратитесь к Cisco ISR G2 SEC и HSEC Лицензирование.

В случае устройств Cisco это получено, чтобы быть однонаправленным трафиком на меньше чем 85 Мбит/с в или из маршрутизатора ISR G2 с двунаправленным общим количеством 170 Мбит/с. Это требование просит Cisco 1900, 2900 и 3900 платформ ISR G2. Эта команда помогает вам в просмотре этих ограничений:

```
Router#show platform cerm-information Crypto Export Restrictions Manager(CERM) Information: CERM
functionality: ENABLED ---------------------------------------------------------------- Resource
Maximum Limit Available ---------------------------------------------------------------- Tx
Bandwidth(in kbps) 85000 85000 Rx Bandwidth(in kbps) 85000 85000 Number of tunnels 225 225
Number of TLS sessions 1000 1000 ---Output truncated----
```

Существует дефект, поданный для адресации к этому поведению. См. идентификатор ошибки Cisco CSCtu24534 (только зарегистрированные клиенты) для получения дополнительной информации.

Во избежание этой проблемы необходимо купить лицензию HSECK9. "hseck9" характеристика лицензирования предоставляет улучшенной функциональности шифрования полезной нагрузки увеличенное количество VPN-туннеля и безопасные речевые сеансы. Для получения дополнительной информации о лицензировании комплекта маршрутизаторов ISR Cisco, обратитесь к Активации ПО.

Проблема: Даже если входящий трафик расшифровки работает, исходящий трафик шифрования в Туннеле IPSec может отказать.

Решение

Эта проблема наблюдалась относительно IP - безопасного соединения после того, как множитель повторно вводит, но триггерное условие не ясно. Присутствие этой проблемы может быть установлено путем проверки выходных данных **команды show asp drop** и проверки, что контекст VPN С истекшим сроком противостоит увеличениям для каждого передаваемого исходящего пакета. См. идентификатор ошибки Cisco CSCtd36473 (только зарегистрированные клиенты) для получения дополнительной информации.

Прочее

Сообщение AG_INIT_EXCH Появляется в Выходных данных Команд "show crypto isakmp sa" и "отладки"

Если туннель не становится инициируемым, сообщение `AG_INIT_EXCH` появляется в выходных данных **команды show crypto isakmp sa** и в **выходных данных отладки** также. Если порт udp 500 заблокирован на пути, причина может произойти из-за не сочетающейся политики ISAKMP или.

Сообщение отладки "Получило сообщение IPC во время недопустимого состояния", Появляется

Это сообщение является информационным сообщением и не имеет никакого отношения к разъединению VPN-туннеля.

Дополнительные сведения

- Проблема PIX/ASA 7.0: Превышено допустимое значение MSS — HTTP-клиенты не могут просматривать определенные веб-узлы
- PIX/ASA 7.x и IOS: Фрагментация VPN
- Устройства обеспечения безопасности Cisco ASA серии 5500
- Cisco PIX 500 Series Security Appliances
- Согласование IPsec/Протоколы IKE
- Cisco VPN 3000 Series Concentrators
- Cisco Systems – техническая поддержка и документация