PIX 6.x: пример конфигурации простого VPN-туннеля PIX-PIX

Перевод выполнен профессиональным переводчиком

Перевод выполнен профессиональным переводчиком

***Интерактивный*: В данном документе содержится анализ конкретного устройства Cisco.**

Содержание

Введение

Эта конфигурация позволяет двум брандмауэрам Cisco Secure PIX поддерживать простой туннель частной виртуальной сети (VPN) из PIX в PIX через Интернет или любую публичную сеть, которая использует IP-безопасность (IPSec). IPSec - это комбинация открытых стандартов, которые обеспечивают конфиденциальность и целостность данных и проверку их происхождения между равноправными узлами IPSec.

Подробнее для оборудования Cisco Security под управлением программного обеспечения версии 7.x см. "PIX/ASA 7.x: пример конфигурации простого VPN-туннеля PIX-to-PIX".

Предварительные условия

Требования

Для данного документа нет особых требований.

Используемые компоненты

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

- Брандмауэр Cisco Secure PIX 515E с программным обеспечением версии 6.3(5)
- Брандмауэр Cisco Secure PIX 515E с программным обеспечением версии 6.3(5)

Условные обозначения

См. Технические советы Cisco. Условные обозначения для получения дополнительной информации об условных обозначениях в документах.

Общие сведения

Процесс согласования IPSec можно разделить на пять шагов, в которые входят два этапа обмена ключами в Интернете (IKE).

1. Туннель IPSec инициирован содержательным трафиком. Трафик считается содержательным при передаче между двумя одноранговыми узлами IPsec.
2. На втором этапе обмена ключами (IKE) для равноправных узлов IPSec выполняется согласование установленной политики сопоставлений безопасности (SA) IKE. По завершении аутентификации равноправных пользователей создается защищенный туннель с применением протокола ISAKMP (Протокол управления ключами Ассоциации безопасности Интернет).
3. На втором этапе IKE для равноправных узлов IPSec выполняется согласование SA IPSec с применением аутентификации и защищенного туннеля. Согласование общей политики определяет то, как будет установлен туннель IPSec.
4. Туннель IPSec создан, и данные передаются между узлами IPSec на основании параметров IPSec, настроенных в наборах преобразования IPSec.
5. Разъединение туннеля IPSec выполняется при удалении SA IPSec или по истечении срока их действия.

Примечание: согласование IPSec между двумя PIX не работает, если SA на обеих фазах IKE не совпадают на равноправных узлах.

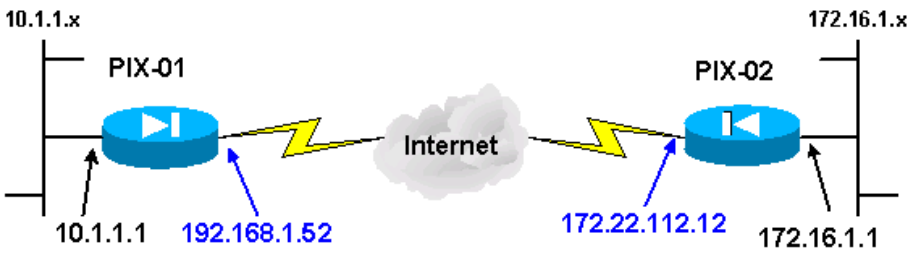
Настройка

В этом разделе приводятся сведения о настройке функций, описанных в данном документе.

Примечание: для поиска дополнительной информации о командах, упоминаемых в данном документе, используйте средство Command Lookup Tool (только для зарегистрированных заказчиков).

Схема сети

В данном документе используется следующая схема сети:



Примечание: схемы IP-адресации, которые использованы в данной конфигурации, нельзя применять в Интернете. Это адреса RFC 1918 , которые использовались в лабораторной среде.

Конфигурация IKE и IPSec

Конфигурация IPSec на каждом PIX должна изменяться только при внесении сведений об одноранговом устройстве и соглашения об именовании для криптокарт и наборов преобразования. Конфигурацию можно проверить с помощью команд **write terminal** или **show**. Соответствующие команды: **show isakmp**, **show isakmp policy**, **show access-list**, **show crypto IPSec transform-set** и **show crypto map**. Подробнее см. "Справочник по командам брандмауэра Cisco Secure PIX".

Для настройки IPSec выполните следующие действия:

1. Настройте IKE для предварительно разрешенных для общего доступа ключей
2. Настройте IPSec
3. Настройте Network Address Translation (NAT)
4. Настройте системные параметры PIX

Настройка IKE для предварительно разрешенных для общего доступа ключей

Задайте команду **isakmp enable**, чтобы включить IKE на конечных интерфейсах IPSec. В этом сценарии внешний интерфейс является конечным интерфейсом IPSec обоих PIX. IKE настроен на обоих PIX. Следующие команды показывают только PIX-01.

```
isakmp enable outside
```

Необходимо определить также политику IKE, которые используются во время согласований IKE. Для этого задайте команду **isakmp policy**. При задании этой команды необходимо назначить уровень приоритета так, чтобы политики определялись уникально. В этом случае политике будет назначен высочайший приоритет - 1. Политика также настраивается на использование предварительно разрешенного для общего доступа ключа, алгоритма хэширования MD5 для аутентификации данных, DES для Encapsulating Security Payload (ESP) и группы 1 Диффи-Хельмана. Указывается также использование срока действия SA.

```
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
```

Конфигурацию IKE можно проверить с помощью команды **show isakmp policy**:

```
PIX-01#show isakmp policy
Protection suite of priority 1
encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm: Message Digest 5
authentication method: Pre-Shared Key
Diffie-Hellman group: #1 (768 bit)
lifetime: 1000 seconds, no volume limit
Default protection suite
encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm: Secure Hash Standard
authentication method: Rivest-Shamir-Adleman Signature
Diffie-Hellman group: #1 (768 bit)
lifetime: 86400 seconds, no volume limit
```

В конце задайте команду **isakmp key**, чтобы настроить предварительно разрешенный для общего доступа ключ и назначить адрес однорангового узла. Предварительно разрешенные для общего доступа ключи одноранговых узлов IPSec должны совпадать. Адреса

различаются, что зависит от IP-адреса удаленного однорангового узла.

```
isakmp key ********** address 172.22.112.12 netmask 255.255.255.255
PIX-01#
```

Политику можно проверить с помощью команд **write terminal** и **show isakmp**:

```
PIX-01#show isakmp
isakmp enable outside
isakmp key ********** address 172.22.112.12 netmask 255.255.255.255
isakmp identity address
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
```

Настройка IPSec

IPSec инициируется, когда один из PIX получает трафик, предназначенный для внутренней сети другого PIX. Данный трафик считается содержательным трафиком, для которого требуется защита по протоколу IPSec. Список доступа используется для определения того, какой трафик инициирует соглашения IKE и IPSec. Этот список доступа разрешает трафик, который должен отправляться из сети 10.1.1.x через туннель IPSec в сеть 172.16.1.x. Список доступа в конфигурации противоположного PIX является зеркальным отражением этого списка. Это подходит для PIX-01.

```
access-list 101 permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0
```

Набор преобразования IPSec определяет политику безопасности, которую одноранговые узлы используют для защиты потока данных. Преобразование IPSec определяется через использование команды **crypto IPSec transform-set**. Необходимо выбрать уникальное имя для настройки преобразования, а для определения протоколов безопасности IPSec можно выбрать до трех преобразований. В этой конфигурации используются только два преобразования: **esp-hmac-md5** и **esp-des**.

```
crypto IPSec transform-set chevelle esp-des esp-md5-hmac
```

С помощью криптокарт осуществляется настройка сопоставлений IPSec SA для зашифрованного трафика. Для создания криптокарты необходимо назначить имя карты и номер последовательности. Затем определяются параметры криптокарты. Показанная криптокарта "transam" использует алгоритм IKE для установления защищенных соединений по протоколу IPSec, шифрует все, что совпадает со списком доступа 101, и использует набор преобразований **chevelle** для применения своей политики безопасности к трафику.

```
crypto map transam 1 IPSec-isakmp
crypto map transam 1 match address 101
crypto map transam 1 set peer 172.22.112.12
crypto map transam 1 set transform-set chevelle
```

После задания криптокарты примените ее к интерфейсу. Следует выбрать конечный интерфейс IPSec.

```
crypto map transam interface outside
```

Для проверки атрибутов криптокарты задайте команду **show crypto map**.

```
PIX-01#show crypto map

Crypto Map: "transam" interfaces: { outside }

Crypto Map "transam" 1 IPSec-isakmp
Peer = 172.22.112.12
access-list 101 permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255
Current peer: 172.22.112.12
Security association lifetime: 4608000 kilobytes/28800 seconds
PFS (Y/N): N
Transform sets={ chevelle, }
```

Настройка NAT

Эта команда указывает PIX не применять NAT ни к какому трафику, который считается содержательным для IPSec. Таким образом, весь трафик, который совпадает с инструкцией команды **access-list**, исключается из работы служб NAT.

```
access-list NoNAT permit ip 10.1.1.0 255.255.255.0
172.16.1.0 255.255.255.0
nat (inside) 0 access-list NoNAT
```

Настройка системных параметров PIX

Поскольку все входные сеансы должны быть явно разрешены списком доступа или каналом передачи данных, команда **sysopt connection permit-IPSec** используется для разрешения всех внутренних аутентифицированных шифрованных сеансов IPSec. В случае трафика, защищенного IPSec, дополнительная проверка канала может быть избыточной и стать причиной сбоя создания туннеля. Команда **sysopt** меняет различные характеристики безопасности и конфигурации брандмауэра PIX.

```
sysopt connection permit-IPSec
```

Конфигурации

Если у вас есть выходные данные команды **write terminal** с устройства Cisco, для отображения потенциальных проблем и средств их решения можно использовать Output Interpreter (только для зарегистрированных заказчиков). Для использования утилиты Output Interpreter (только для зарегистрированных заказчиков) необходимо выполнить вход в систему и разрешить использование сценариев JavaScript.

PIX-01 на 192.68.1.52
PIX версии 6.3 (5) interface ethernet0 auto interface ethernet1 auto nameif ethernet0 outside security0 nameif ethernet1 inside security100 enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname PIX-01 fixup protocol dns maximum-length 512 fixup protocol ftp 21 fixup protocol h323 h225 1720 fixup protocol h323 ras 1718-1719 fixup protocol http 80 fixup protocol rsh 514 fixup protocol rtsp 554 fixup protocol sip 5060 fixup protocol sip udp 5060 fixup protocol skinny 2000

```
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names

!--- Определяет целевой трафик, защищенный туннелем IPSec.


access-list 101 permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0

!--- Не применяйте NAT для трафика к другому брандмауэру PIX Firewall.


access-list NoNAT permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500

!--- Устанавливает внешний адрес на брандмауэре PIX.


ip address outside 192.168.1.52 255.255.255.0

!--- Устанавливает внутренний адрес на брандмауэре PIX.


ip address inside 10.1.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
pdm history enable
arp timeout 14400

!--- Эта команда указывает PIX не применять NAT ни к какому трафику,
!--- признанному содержательным для IPSec.

nat (inside) 0 access-list NoNAT

!--- Устанавливает маршрут по умолчанию для шлюза по умолчанию.

route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable

!--- Разрешает трафику проходить через брандмауэр PIX
!--- и не требует дополнительного канала
!--- или инструкций списка доступа для разрешения трафика IPSec.

sysopt connection permit-IPSec

!--- Фаза 2 IKE:
!--- Набор преобразования IPSec "chevelle" использует esp-md5-hmac
!--- для обеспечения аутентификации данных.


crypto IPSec transform-set chevelle esp-des esp-md5-hmac

!--- Криптокарты настраивают SA для трафика IPSec.
!--- Показывает, что IKE используется для установления SA IPSec.

crypto map transam 1 IPSec-isakmp

!--- Назначает содержательный трафик для узла 172.22.112.12.
```

```
crypto map transam 1 match address 101

!--- Устанавливает одноранговый узел IPSec.

crypto map transam 1 set peer 172.22.112.12

!--- Устанавливает, что набор преобразований IPSec "chevelle"
!--- нужно использовать с записью криптокарты "transam".

crypto map transam 1 set transform-set chevelle

!--- Назначает криптокарту transam-интерфейсу.

crypto map transam interface outside

!--- Фаза 1 IKE:
!--- Включает IKE на интерфейсе, используемом для окончания туннеля IPSec

isakmp enable outside

!--- Устанавливает ISAKMP-подлинность одноранговой узла и
!--- предварительно разрешенный для совместного использования ключ для одноранговых узлов IPSec.
!--- Тот же самый предварительно разрешенный для совместного использования ключ
!--- должен быть настроен на узлах IPSec для аутентификации IKE.

isakmp key ******** address 172.22.112.12 netmask 255.255.255.255

!--- PIX использует метод IP-адреса
!--- для подлинности IKE в согласования IKE.

isakmp identity address

!--- Политика ISAKMP определяет набор параметров,
!--- которые используются для согласований IKE.
!--- Если эти параметры не установлены, используются параметры по умолчанию.
!--- Команда show isakmp policy показывает отличия
!--- политики по умолчанию и настроенной политики.

isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
arp timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

PIX-02 на 172.22.112.12

```
PIX версии 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX-02
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names

!--- Определяет целевой трафик, защищенный туннелем IPSec.


access-list 101 permit ip 172.16.1.0 255.255.255.0 10.1.1.0 255.255.255.0
```

```
!--- Не используйте NAT для передачи данных к другому брандмауэру PIX Firewall.

access-list NoNAT permit ip 172.16.1.0 255.255.255.0 10.1.1.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500

!--- Устанавливает внешний адрес на брандмауэре PIX.

ip address outside 172.22.112.12 255.255.255.0

!--- Устанавливает внутренний адрес на брандмауэре PIX.

ip address inside 172.16.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
pdm history enable
arp timeout 14400

!--- Эта команда указывает PIX не применять NAT ни к какому трафику,
!--- признанному содержательным для IPSec.

nat (inside) 0 access-list NoNAT

!--- Устанавливает маршрут по умолчанию для шлюза по умолчанию.

route outside 0.0.0.0 0.0.0.0 172.22.112.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable

!--- Разрешает трафику проходить через брандмауэр PIX
!--- и не требует дополнительного канала
!--- или инструкций списка доступа для разрешения трафика IPSec.

sysopt connection permit-IPSec

!--- Фаза 2 IKE:
!--- Набор преобразований IPSec определяет согласованную политику безопасности,
!--- которую одноранговые узлы используют для защиты потока данных.
!--- Набор преобразования IPSec "toyota" использует заголовок аутентификации hmac-md5
!--- и инкапсулирует полезную нагрузку с помощью des.

crypto IPSec transform-set toyota esp-des esp-md5-hmac

!--- Криптокарты настраивают SA для трафика IPSec.
!--- Показывает, что IKE используется для установления SA IPSec.

crypto map bmw 1 IPSec-isakmp

!--- Назначает содержательный трафик для узла 192.168.1.52.

crypto map bmw 1 match address 101

!--- Устанавливает одноранговый узел IPSec.

crypto map bmw 1 set peer 192.168.1.52

!--- Устанавливает, что набор преобразований IPSec "toyota"
!--- нужно использовать с записью криптокарты "bmw".

crypto map bmw 1 set transform-set toyota
```

```
!--- Назначает криптокарту bmw-интерфейсу.

crypto map bmw interface outside

!--- Фаза 1 IKE:
!--- Включает IKE на интерфейсе, используемом для окончания туннеля IPSec.

isakmp enable outside

!--- Устанавливает ISAKMP-подлинность одноранговой узла и
!--- предварительно разрешенный для совместного использования ключ для одноранговых узлов IPSec.
!--- Тот же самый предварительно разрешенный для совместного использования ключ
!--- должен быть настроен на узлах IPSec для аутентификации IKE.

isakmp key ******** address 192.168.1.52 netmask 255.255.255.255

!--- PIX использует метод IP-адреса
!--- для подлинности IKE в согласования IKE.

isakmp identity address

!--- Политика ISAKMP определяет набор параметров,
!--- которые используются для согласований IKE.
!--- Если эти параметры не установлены, используются параметры по умолчанию.

isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
arp timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

Проверка

В данном разделе содержатся сведения о проверке работы конфигурации.

Отдельные команды **show** поддерживаются средством Output Interpreter Tool (только для зарегистрированных пользователей), которое позволяет просматривать выходные данные команды **show**.

- **show crypto IPSec sa** — эта команда показывает текущий статус SA IPSec, она полезна для определения того, шифруется трафик, или нет.
- **show crypto isakmp sa** — эта команда показывает текущий статус SA IKE.

Команды show PIX-01

Команды show PIX-01

```
PIX-01#show crypto IPSec sa
interface: внешний
Crypto map tag: transam, local addr. 192.168.1.52

local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
current_peer: 172.22.112.12
PERMIT, flags={origin_is_acl,}

!--- Проверяет, с ошибками или без отправляются и принимаются
!--- зашифрованные пакеты.

#pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
```

```
#send errors 2, #recv errors 0

local crypto endpt.: 192.168.1.52, remote crypto endpt.: 172.22.112.12
path mtu 1500, IPSec overhead 56, media mtu 1500
current outbound spi: 6f09cbf1

!--- Показывает установленные входящие SA.

inbound esp sas:
spi: 0x70be0c04(1891503108)
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: transam
sa timing: remaining key lifetime (k/sec): (4607999/28430)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:

!--- Показывает установленные выходящие SA.

outbound ESP sas:
spi: 0x6f09cbf1(1862913009)
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: transam
sa timing: remaining key lifetime (k/sec): (4607999/28430)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound ESP sas:



!--- ISAKMP SA находится в состоянии покоя (QM_IDLE), когда существует.
!--- ISAKMP SA находится в состоянии ожидания. ISAKMP SA аутентифицирован своим одноранговым узлом
!--- и может быть использован для последующих изменений Quick Mode.

PIX-01#show crypto isakmp sa
    dst             src          state      pending        created
172.22.112.12    192.168.1.52    QM_IDLE        0        1Maui-PIX-01#
```

Команды show PIX-02

Команды show PIX-02

```
PIX-02#show crypto IPSec sa

interface: внешний
Crypto map tag: bmw, local addr. 172.22.112.12

local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
current_peer: 192.168.1.52
PERMIT, flags={origin_is_acl,}

!--- Проверяет, с ошибками или без отправляются и принимаются
!--- зашифрованные пакеты.

#pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. Failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.22.112.12, remote crypto endpt.: 192.168.1.52
path mtu 1500, IPSec overhead 56, media mtu 1500
current outbound spi: 70be0c04

!--- Показывает установленные входящие SA.

Inbound ESP sas:
spi: 0x6f09cbf1(1862913009)
transform: esp-des esp-md5-hmac
```

```
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: bmw
sa timing: remaining key lifetime (k/sec): (4607999/28097)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound PCP sas:

!--- Показывает установленные выходящие SA.

Outbound ESP sas:
spi: 0x70be0c04(1891503108)
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: bmw
sa timing: remaining key lifetime (k/sec): (4607999/28097)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound ESP sas:



!--- ISAKMP SA находится в состоянии покоя (QM_IDLE), когда существует.
!--- ISAKMP SA находится в состоянии ожидания. ISAKMP SA аутентифицирован своим одноранговым узлом
!--- и может быть использован для последующих изменений Quick Mode.

PIX-02#show crypto isakmp sa
    dst             src          state      pending        created
172.22.112.12    192.168.1.52    QM_IDLE        0       PIX-02#
```

Внутренний интерфейс PIX не может быть эхотестирован на предмет формирования 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
```

Поиск и устранение неисправностей

В данном разделе описывается процесс устранения неполадок конфигурации.

Команды поиска и устранения неисправностей

Примечание: Команды **clear** должны использоваться в режиме конфигурации.

- **clear crypto IPSec sa** — эта команда перезапускает SA IPSec после безуспешных попыток согласования VPN-туннеля.
- **clear crypto isakmp sa** — эта команда перезапускает SA ISAKMP после безуспешных попыток согласования VPN-туннеля.

Примечание: перед использованием команд отладки обратитесь к документу "Важные сведения о командах отладки".

- **debug crypto IPSec** — эта показывает, договаривается ли клиент об IPSec-части соединения VPN.
- **debug crypto isakmp** — эта команда показывает, договариваются ли одноранговые узлы об ISAKMP-части соединения VPN.

После завершения соединения его можно проверить с помощью команд **show**.

Дополнительные сведения

- **Страница поддержки PIX**
- **Документация для брандмауэра PIX**
- **Справочник по командам PIX**
- **Документы RFC**
- **Страница поддержки сопоставления IPsec и протокола IKE**
- **Техническая поддержка и документация - Cisco Systems**

Дата генерации PDF файла: Jan 05, 2010

---

http://www.cisco.com/support/RU/customer/content/9/92072/38.shtml

---