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

Содержание

Введение

Эта конфигурация позволяет двум межсетевым экранам 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 этого документа отсутствуют особые требования.

Используемые компоненты

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

- Cisco Secure PIX 515E Межсетевой экран с версией программного обеспечения 6.3 (5)
- Cisco Secure PIX 515E Межсетевой экран с версией программного обеспечения 6.3 (5)

Условные обозначения

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

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 пользователей протокола IPSec выполняется согласование установленной политики сопоставлений безопасности (SA) IKE. По завершении аутентификации одноранговых узлов создается защищенный туннель с применением протокола ISAKMP.
3. На втором этапе обмена ключами (IKE) одноранговые узлы IPsec используют проверенный и безопасный туннель для согласования преобразований IPSec SA. 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 сопоставлений безопасности (IPSec SA) или по истечении срока их действия.

Примечание: Если SA на обеих из фаз IKE не совпадают на узлах, согласование IPsec между двумя PIXs отказывает.

Настройка

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

Примечание: Используйте Средство поиска команд Command Lookup Tool (только зарегистрированные клиенты) для получения дополнительной информации о командах, используемых в этом документе.

Схема сети

Этот документ использует эту схему сети:

Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией 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 общих ключей
2. Настройте IPSec
3. Настройте сетевую переадресацию (NAT)
4. Настройте параметры системы PIX

Настройте IKE для общих ключей

Выполните **команду enable isakmp** для включения IKE на Оконечных 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 или 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
```

Настройте IPSec

IPSec инициируется, когда один из PIXs получает трафик, который предназначен для другой внутренней сети 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 говорит PIX не NAT, который любой трафик считал как содержательный 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
```

Настройте параметры системы PIX

Поскольку все входящие сеансы должны быть явно разрешены списком доступа или conduit, команда **sysopt connection permit-IPSec** используется, чтобы разрешить, чтобы все входящие подключения IPSec аутентифицировали сеансы с шифрованием. 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

При наличии исходящих данных команды write terminal от устройства Cisco для отображения потенциальных проблем и исправлений можно использовать Output Interpreter (только для зарегистрированных клиентов). 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 Version 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
!--- Defines interesting traffic that is protected by
the IPSec tunnel. access-list 101 permit ip 10.1.1.0
255.255.255.0 172.16.1.0 255.255.255.0
!--- Do not perform NAT for traffic to other 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
!--- Sets the outside address on the PIX Firewall. ip
address outside 192.168.1.52 255.255.255.0
!--- Sets the inside address on the PIX Firewall. 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
!--- This command tells the PIX not to NAT any traffic
!--- deemed interesting for IPSec. nat (inside) 0
access-list NoNAT
!--- Sets the default route to the default gateway.
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
!--- Allows IPSec traffic to pass through the PIX
Firewall !--- and does not require an additional conduit
!--- or access-list statements to permit IPSec traffic.
sysopt connection permit-IPSec
!--- IKE Phase 2: !--- The IPSec transform-set
"chevelle" uses esp-md5-hmac to provide !--- data
```

```
authentication.

crypto IPSec transform-set chevelle esp-des esp-md5-hmac
!--- Crypto maps set up the SAs for IPSec traffic. !---
Indicates that IKE is used to establish IPSec SAs.
crypto map transam 1 IPSec-isakmp
!--- Assigns interesting traffic to peer 172.22.112.12.
crypto map transam 1 match address 101
!--- Sets the IPSec peer. crypto map transam 1 set peer
172.22.112.12
!--- Sets the IPSec transform set "chevelle" !--- to be
used with the crypto map entry "transam". crypto map
transam 1 set transform-set chevelle
!--- Assigns the crypto map transam to the interface.
crypto map transam interface outside
!--- IKE Phase 1: !--- Enables IKE on the interface used
to terminate the IPSec tunnel

isakmp enable outside
!--- Sets the ISAKMP identity of the peer and !--- sets
the pre-shared key between the IPSec peers. !--- The
same preshared key must be configured on the !--- IPSec
peers for IKE authentication. isakmp key ********
address 172.22.112.12 netmask 255.255.255.255
!--- The PIX uses the IP address method by default !---
for the IKE identity in the IKE negotiations. isakmp
identity address
!--- The ISAKMP policy defines the set of parameters !--
- that are used for IKE negotiations. !--- If these
parameters are not set, the default parameters are used.
!--- The show isakmp policy command shows the
differences in !--- the default and configured policy.

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
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

PIX-02 в 172.22.112.12

```
PIX Version 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
!--- Defines interesting traffic that is protected by
the IPSec tunnel. access-list 101 permit ip 172.16.1.0
255.255.255.0 10.1.1.0 255.255.255.0
!--- Do not perform NAT for traffic to other 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
!--- Sets the outside address on the PIX Firewall. ip
address outside 172.22.112.12 255.255.255.0
!--- Sets the inside address on the PIX Firewall. 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
!--- This command tells the PIX not to NAT any traffic
!--- deemed interesting for IPSec. nat (inside) 0
access-list NoNAT
!--- Sets the default route to the default gateway.
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
!--- Allows IPSec traffic to pass through the PIX
Firewall !--- and does not require an additional conduit
!--- or access-list statements to permit IPSec traffic.
sysopt connection permit-IPSec
!--- IKE Phase 2:  !--- The IPSec transform set defines
the negotiated security policy !--- that the peers use
to protect the data flow. !--- The IPSec transform-set
"toyota" uses hmac-md5 authentication header !--- and
encapsulates the payload with des.
```

```
crypto IPSec transform-set toyota esp-des esp-md5-hmac
!--- Crypto maps set up the SAs for IPSec traffic. !---
Indicates that IKE is used to establish IPSec SAs.
crypto map bmw 1 IPSec-isakmp
!--- Assigns interesting traffic to peer 192.168.1.52.
crypto map bmw 1 match address 101
!--- Sets IPSec peer. crypto map bmw 1 set peer
192.168.1.52
!--- Sets the IPSec transform set "toyota" !--- to be
used with the crypto map entry "bmw". crypto map bmw 1
set transform-set toyota
!--- Assigns the crypto map bmw to the interface. crypto
map bmw interface outside
!--- IKE Phase 1: !--- Enables IKE on the interface used
to terminate IPSec tunnel.

isakmp enable outside
!--- Sets the ISAKMP identity of the peer and !--- sets
the preshared key between the IPSec peers. !--- The same
preshared key must be configured on the !--- IPSec peers
for IKE authentication. isakmp key ******** address
192.168.1.52 netmask 255.255.255.255
!--- The PIX uses the IP address method by default !---
for the IKE identity in the IKE negotiations. isakmp
identity address
!--- The ISAKMP policy defines the set of parameters !--
- that are used for IKE negotiations. !--- If these
parameters are not set, the default parameters are used.
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
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

Проверка

В этом разделе содержатся сведения, которые помогают убедиться в надлежащей работе конфигурации.

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

- **show crypto ipsec sa** Если трафик шифруется, эта команда отображает текущий статус КОНТЕКСТОВ БЕЗОПАСНОСТИ IPSEC и полезна в определении.
- **show crypto isakmp sa** команда показывает текущее состояние SA IKE.

Команды PIX-01 show

Команды PIX-01 show
PIX-01#**show crypto IPSec sa** interface: **outside**

```
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,}
!--- This verifies that encrypted packets are being sent
!--- and received without any errors. #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
!--- Shows inbound SAs that are established. 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:
!--- Shows outbound SAs that are established. 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 PCP sas:

!--- The ISAKMP SA is in the quiescent state (QM_IDLE)
when it exists. !--- The ISAKMP SA is idle. The ISAKMP
SA remains authenticated with its !--- peer and can be
used for subsequent Quick Mode exchanges. 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 PIX-02 show

Команды PIX-02 show

```
PIX-02#show crypto IPSec sa

interface: outside
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,}
!--- This verifies that encrypted packets are !--- being
sent and recede without any errors. #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
!--- Shows inbound SAs that are established. 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:
!--- Shows outbound SAs that are established. 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 PCP sas:

!--- The ISAKMP SA is in the quiescent state (QM_IDLE)
when it exists. !--- The ISAKMP SA is idle. The ISAKMP
SA remains authenticated with its !--- peer and can be
used for subsequent Quick Mode exchanges. 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
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Примечание: Команды clear должны быть выполнены в режиме конфигурации.

- **clear crypto IPSec sa** — Эта команда перезагружает КОНТЕКСТЫ БЕЗОПАСНОСТИ IPSEC после неудачных попыток для согласования о VPN-туннеле.
- **clear crypto isakmp sa** — Эта команда перезагружает SA ISAKMP после неудачных попыток для согласования о VPN-туннеле.

Примечание: Обратитесь к документу Важная информация о командах отладки, прежде чем использовать команды debug.

- **debug crypto ipsec** команда показывает, выполняет ли клиент согласование о Части IPSec VPN-подключения.
- **debug crypto isakmp** команда показывает, выполняют ли узлы согласование о части ISAKMP VPN-подключения.

После завершения соединения его можно проверить с помощью команд show.

Дополнительные сведения

- Страница поддержки PIX
- Справочник по командам PIX
- Запрос на комментарии (RFC)
- Страница поддержки IPsec Negotiation/IKE
- Cisco Systems – техническая поддержка и документация