Настройка IPSec между концентратором и удаленными PIX с VPN-клиентом и расширенной аутентификацией

Содержание

Введение

Этот документ показывает конфигурацию IPSec, которая включает и функцию шлюз-шлюз и функцию удаленного пользователя. С помощью расширенной аутентификации (Xauth) устройства происходит удостоверение подлинности устройства предварительным ключом, а аутентификация пользователя осуществляется путем ввода имени пользователя и пароля.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Версия 6.3 (3) межсетевого экрана PIX
- Версия клиентской части Cisco VPN 3.5

- Cisco Secure ACS для версии Windows 2.6

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.

Общие сведения

В этом примере есть туннель между шлюзами IPSec от удаленного PIX до хаба PIX. Этот туннель шифрует трафик от сети 10.48.67.x позади удаленного PIX к сети 10.48.66.x позади межсетевого экрана (PIX) концентратора. ПК в Интернете может сформировать Туннель IPSec через межсетевой экран (PIX) концентратора к сети 10.48.66. x.

Чтобы использовать функциональную возможность Xauth, вы сначала должны установить свой основной сервер аутентификации, авторизации и учета (AAA). Используйте команду **crypto map client authentication**, чтобы сказать Межсетевому экрану PIX использовать Xauth (RADIUS/TACACS + имя пользователя и пароль) проблема во время Фазы 1 Протокола IKE для аутентификации IKE. Если Xauth отказывает, сопоставление безопасности IKE не установлено. Задайте то же название AAA-сервера в рамках командного оператора **crypto map client authentication**, который задан в командном операторе **aaa-server**. Удаленный пользователь должен выполнить Версию клиентской части Cisco VPN 3. x. или позже.

Примечание: Cisco рекомендует использовать Cisco VPN Client 3.5.x или позже. Клиент VPN 1.1 не работает с этой конфигурацией и вне области этого документа.

Примечание: 3.6 и позднее Cisco VPN Client не поддерживает набор преобразований des/sha.

Если восстанавливать конфигурацию без Xauth не требуется, используйте команду no crypto map client authentication. Функция Xauth не включена по умолчанию.

Примечание: Технология шифрования подлежит экспортному контролю. Это - ваша обязанность знать законы, отнесенные к экспорту технологии шифрования. См. домашнюю страницу Бюро экспортной администрации для получения дополнительной информации. Пошлите Электронное письмо export@cisco.com, если у вас есть какие-либо вопросы, отнесенные к экспортному контролю.

Примечание: В Версии 5.3 Межсетевого экрана PIX и позже, были представлены порты RADIUS с изменяемой конфигурацией. Некоторые серверы RADIUS используют порты RADIUS, отличные от 1645 или 1646 (обычно 1812 или 1813). В PIX 5.3 и позже, Проверка подлинности RADIUS и порты учета могут быть изменены на кроме по умолчанию 1645/1646 использующий эти команды:

```
aaa-server radius-authport #
aaa-server radius-acctport #
```

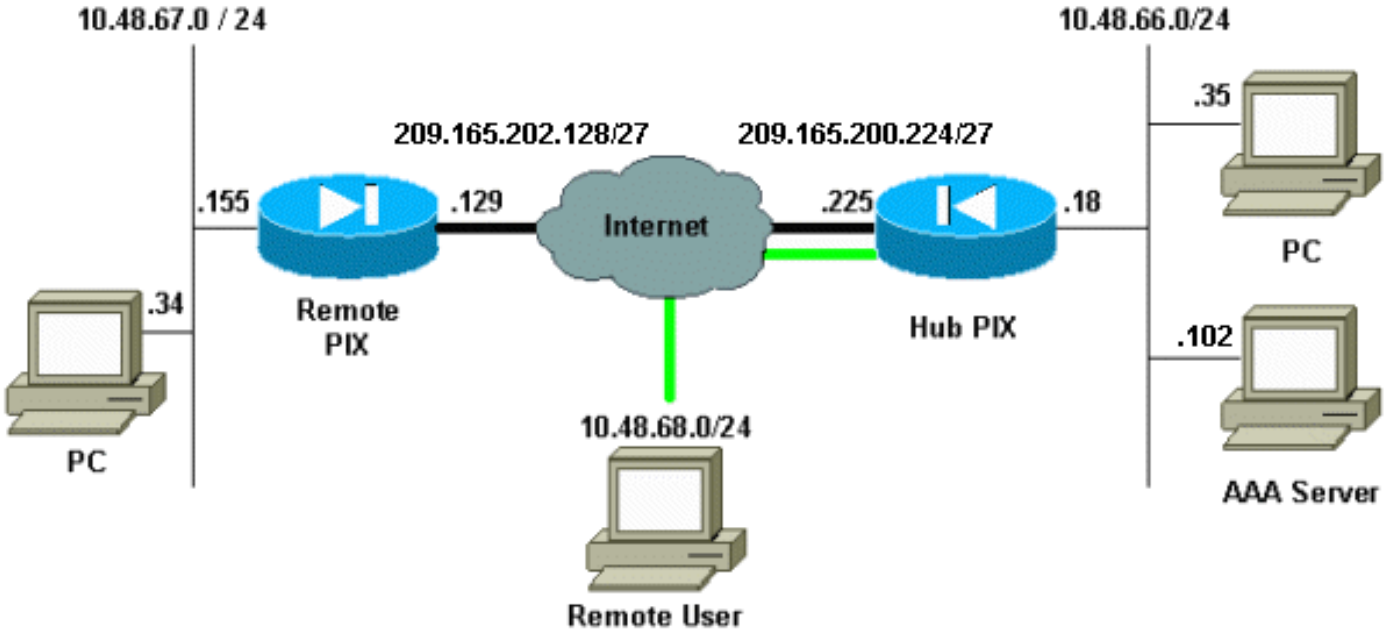
Настройка

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

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

Эта схема использует зеленые и черные жирные линии для указания на VPN-туннели.



Конфигурации

Эти конфигурации используются в данном документе.

- МЕЖСЕТЕВОЙ ЭКРАН (PIX) КОНЦЕНТРАТОРА
- Удаленный PIX

Примечание: Для примера в этом документе IP-адрес сервера VPN 209.165.200.225, имя группы является "vpn3000", и пароль группы является Cisco.

Конфигурация PIX концентратора
PIX Version 6.3(3) interface ethernet0 auto interface ethernet1 auto nameif ethernet0 outside security0 nameif ethernet1 inside security100 enable password OnTrBUG1Tp0edmkr encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname hubfixup 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
!--- Include traffic in the encryption process. access-
list 101 permit ip 10.48.66.0 255.255.255.0 10.48.67.0
255.255.255.0
!--- Accept traffic from the Network Address Translation
(NAT) process
access-list nonat permit ip 10.48.66.0 255.255.255.0
10.48.67.0 255.255.255.0
access-list nonat permit ip 10.48.66.0 255.255.255.0
10.48.68.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
ip address outside 209.165.200.225 255.255.255.224
ip address inside 10.48.66.18 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool mypool 10.48.68.1-10.48.68.254
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
global (outside) 1 209.16.200.230-209.16.200.240 netmask
255.255.255.224
global (outside) 1 209.16.200.241
!--- Except traffic from the NAT process. nat (inside) 0
access-list nonat
nat (inside) 1 10.48.66.0 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 209.165.200.226 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 uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
aaa-server mytacacs protocol tacacs+
aaa-server mytacacs (inside) host 10.48.66.102 cisco
timeout 5
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
!--- Use the crypto-map sequence 10 command for PIX to
PIX.

crypto map mymap 10 ipsec-isakmp
crypto map mymap 10 match address 101
crypto map mymap 10 set peer 209.165.202.129
```

```
crypto map mymap 10 set transform-set myset
!--- Use the crypto-map sequence 20 command for PIX to
VPN Client.

crypto map mymap 20 ipsec-isakmp dynamic dynmap
crypto map mymap client authentication mytacacs
crypto map mymap interface outside
isakmp enable outside
isakmp key ******** address 209.165.202.129 netmask
255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
!--- ISAKMP policy for VPN Client that runs 3.x code
needs to be DH group 2. isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!--- IPsec group configuration for VPN Client. vpngroup
vpn3000 address-pool mypool
vpngroup vpn3000 dns-server 10.48.66.129
vpngroup vpn3000 wins-server 10.48.66.129
vpngroup vpn3000 default-domain cisco.com
vpngroup vpn3000 idle-time 1800
vpngroup vpn3000 password ********
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:7293dd9fc7c58ff5d65f042dd6ddbe13
: end
```

Удаленная конфигурация PIX

```
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 100basetx
interface ethernet2 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
enable password OnTrBUG1Tp0edmkr encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname remote
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
access-list 101 permit ip 10.48.67.0 255.255.255.0
10.48.66.0 255.255.255.0
!--- Accept traffic from the NAT process. access-list
nonat permit ip 10.48.67.0 255.255.255.0 10.48.66.0
255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
```

```
mtu intf2 1500
ip address outside 209.165.202.129 255.255.255.224
ip address inside 10.48.67.155 255.255.255.0
no ip address intf2
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
no failover ip address intf2
pdm history enable
arp timeout 14400
global (outside) 1 209.16.202.135-209.16.202.145 netmask
255.255.255.224
global (outside) 1 209.16.202.146
!--- Except traffic from the NAT process. nat (inside) 0
access-list nonat
nat (inside) 1 10.48.0.0 255.255.255.0 0 0
nat (inside) 1 10.48.67.0 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 209.165.202.130 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 uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto map mymap 10 ipsec-isakmp
!--- Include traffic in the encryption process. crypto
map mymap 10 match address 101
crypto map mymap 10 set peer 209.165.200.225
crypto map mymap 10 set transform-set myset
crypto map mymap interface outside
isakmp enable outside
isakmp key ******** address 209.165.200.225 netmask
255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:13ef4d29384c65c2cd968b5d9396f6e8
: end
```

См. раздел "Конфигураций" PIX Настройки к PIX и Клиенту VPN 3.x для получения дальнейшей информации о том, как установить Клиент VPN. Кроме того, обратитесь к тому, Как Добавить Аутентификацию AAA (проверка подлинности, авторизация и учет) (Xauth) к

PIX IPSEC 5.2 и Позже для дополнительных сведений о конфигурации Аутентификации AAA (проверка подлинности, авторизация и учет) к PIX IPSEC.

Проверка

В данном разделе содержатся сведения для проверки правильности конфигурации.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

- **команда show crypto isakmp sa отображает сопоставления безопасности (SA), соответствующие первому этапу.**
- **show crypto ipsec sa - Отображение набора обеспечения мер безопасности фазы 2.**

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Следующие команды отладки необходимо выполнять на обоих (одноранговых) маршрутизаторах IPSec. Связи безопасности должны быть очищены на обоих одноранговых узлах.

- **"debug crypto isakmp" - отображаются ошибки, возникающие в фазе 1.**
- **"debug crypto ipsec" – отображает ошибки в фазе 2.**
- **debug crypto engine– выводит информацию о криптографическом модуле.**
- **команда clear crypto isakmp sa—удаляет сопоставления безопасности, соответствующие этапу 1.**
- **clear crypto ipsec sa—Очищает ассоциации связи в фазе 2.**
- **debug radius [сеанс | все | имя пользователя]** — Доступный в PIX 6.2, эта команда регистрирует информацию о сеанса RADIUS и атрибуты передаваемых и полученных Пакетов RADIUS.
- **debug tacacs [session|user <user_name>]** — Доступный в PIX 6.3, эта команда регистрирует информацию о TACACS.
- **debug aaa [authentification|authorization|accounting|internal] - доступна в PIX 6.3, показывает информацию подсистемы AAA.**

Методы отладки PIX на концентраторе

Примечание: Знайте, что иногда, когда согласование IPsec успешно, не, все отладки показывают на PIX идентификатору ошибки Cisco CSCdu84168 (только зарегистрированные клиенты), который является копией внутреннего идентификатора ошибки Cisco CSCdt31745 (только зарегистрированные клиенты). Это еще не решено с записи этого документа.

Примечание: Иногда IPSEC VPN от Клиентов VPN может не завершиться на PIX. Для решения этого вопроса гарантируйте, что клиентский компьютер не имеет никаких межсетевых экранов. Если межсетевые экраны присутствуют, проверьте, отключен ли порт 500 и 4500 UDP. Если это верно, включите IPSec по TCP или разблокируйте порты UDP.

Отладка динамического туннеля IPSec между концентратором и удаленными межсетевыми экранами (PIX)

```
crypto_isakmp_process_block:src:209.165.202.129,
dest:209.165.200.225 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225
spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing vendor id payload

ISAKMP (0): received xauth v6 vendor id

ISAKMP (0): processing vendor id payload

ISAKMP (0): remote peer supports dead peer detection

ISAKMP (0): processing vendor id payload

ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to another IOS box!

return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225
spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): SA has been authenticated

ISAKMP: Created a peer struct for 209.165.202.129, peer port 62465
ISAKMP (0): ID payload
        next-payload : 8
```

```
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
VPN Peer: ISAKMP: Added new peer: ip:209.165.202.129/500 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:209.165.202.129/500 Ref cnt incremented to:1
Total VPN Peers:1
crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225
spt:500 dpt:500
ISAKMP (0): processing NOTIFY payload 24578 protocol 1
        spi 0, message ID = 863921625
ISAKMP (0): processing notify INITIAL_CONTACTIPSEC(key_engine):
got a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 209.165.202.129

return status is IKMP_NO_ERR_NO_TRANS
crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225
spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 2542705093

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (basic) of 28800
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:      authenticator is HMAC-MD5
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 209.165.200.225, src= 209.165.202.129,
    dest_proxy= 10.48.66.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.48.67.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 2542705093

ISAKMP (0): processing ID payload. message ID = 2542705093
ISAKMP (0): ID_IPV4_ADDR_SUBNET src 10.48.67.0/255.255.255.0 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 2542705093
ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 10.48.66.0/255.255.255.0 prot 0 port 0
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0x858c841a(2240578586) for SA
        from 209.165.202.129 to 209.165.200.225 for prot 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225
spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPSec SAs
        inbound SA from 209.165.202.129 to 209.165.200.225
```

```
        (proxy 10.48.67.0 to 10.48.66.0)
        has spi 2240578586 and conn_id 3 and flags 4
        lifetime of 28800 seconds
        lifetime of 4608000 kilobytes
        outbound SA from 209.165.200.225 to 209.165.202.129
        (proxy  10.48.66.0 to 10.48.67.0)
        has spi 681010504 and conn_id 4 and flags 4
        lifetime of 28800 seconds
        lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 209.165.200.225, src= 209.165.202.129,
    dest_proxy= 10.48.66.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.48.67.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0x858c841a(2240578586), conn_id= 3, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 209.165.200.225, dest= 209.165.202.129,
    src_proxy= 10.48.66.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.48.67.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0x28976548(681010504), conn_id= 4, keysize= 0, flags= 0x4

VPN Peer: IPSEC: Peer ip:209.165.202.129/500
Ref cnt incremented to:2 Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:209.165.202.129/500
Ref cnt incremented to:3 Total VPN Peers:1
return status is IKMP_NO_ERROR
```

Отладки, когда вы подключаете клиент VPN с МЕЖСЕТЕВЫМ ЭКРАНОМ (PIX) КОНЦЕНТРАТОРА

```
crypto_isakmp_process_block:src:209.165.202.129,
dest:209.165.200.225 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225
spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing vendor id payload

ISAKMP (0): received xauth v6 vendor id

ISAKMP (0): processing vendor id payload

ISAKMP (0): remote peer supports dead peer detection

ISAKMP (0): processing vendor id payload
```

```
ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to another IOS box!

return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225
spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): SA has been authenticated

ISAKMP: Created a peer struct for 209.165.202.129, peer port 62465
ISAKMP (0): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
VPN Peer: ISAKMP: Added new peer: ip:209.165.202.129/500 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:209.165.202.129/500 Ref cnt incremented to:1
Total VPN Peers:1
crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225
spt:500 dpt:500
ISAKMP (0): processing NOTIFY payload 24578 protocol 1
        spi 0, message ID = 863921625
ISAKMP (0): processing notify INITIAL_CONTACTIPSEC(key_engine):
got a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 209.165.202.129

return status is IKMP_NO_ERR_NO_TRANS
crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225
spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 2542705093

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (basic) of 28800
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:      authenticator is HMAC-MD5
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 209.165.200.225, src= 209.165.202.129,
    dest_proxy= 10.48.66.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.48.67.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 2542705093
```

```
ISAKMP (0): processing ID payload. message ID = 2542705093
ISAKMP (0): ID_IPV4_ADDR_SUBNET src 10.48.67.0/255.255.255.0 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 2542705093
ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 10.48.66.0/255.255.255.0 prot 0 port 0
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0x858c841a(2240578586) for SA
        from 209.165.202.129 to 209.165.200.225 for prot 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225
spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPSec SAs
        inbound SA from 209.165.202.129 to 209.165.200.225
        (proxy 10.48.67.0 to 10.48.66.0)
        has spi 2240578586 and conn_id 3 and flags 4
        lifetime of 28800 seconds
        lifetime of 4608000 kilobytes
        outbound SA from 209.165.200.225 to 209.165.202.129
        (proxy  10.48.66.0 to 10.48.67.0)
        has spi 681010504 and conn_id 4 and flags 4
        lifetime of 28800 seconds
        lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 209.165.200.225, src= 209.165.202.129,
    dest_proxy= 10.48.66.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.48.67.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0x858c841a(2240578586), conn_id= 3, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 209.165.200.225, dest= 209.165.202.129,
    src_proxy= 10.48.66.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.48.67.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0x28976548(681010504), conn_id= 4, keysize= 0, flags= 0x4

VPN Peer: IPSEC: Peer ip:209.165.202.129/500
Ref cnt incremented to:2 Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:209.165.202.129/500
Ref cnt incremented to:3 Total VPN Peers:1
return status is IKMP_NO_ERROR
```

Дополнительные сведения

- Страница технической поддержки протоколов согласования IPSec и IKE
- Страница поддержки Cisco Secure ACS для Windows
- Справочник по командам PIX
- Страница поддержки PIX
- TACACS+ в документации по IOS
- Страница поддержки TACACS+
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация