Настройка преобразования маршрутизатор - VPN Client, режима конфигурации, шаблона общего ключа с помощью NAT

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

Выпуск программного обеспечения Cisco IOS® 12.0.7T или выше.

Оборудование, поддерживающее данные редакции ПО.

VPN-клиент CiscoSecure 1.0/10A или 1.1 (показывается, соответственно, как 2.0.7/E или 2.1.12, см. **Help > About** [Справка > О программе])

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе в действующей сети необходимо понимать последствия выполнения любой команды.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Настройка

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

Примечание. Для поиска дополнительных сведений о командах, описываемых в данном документе, используйте средство поиска команд (только для зарегистрированных заказчиков).

Схема сети

В этом документе используются настройки сети, показанные на данной диаграмме:

Варианты конфигураций

В настоящем документе используются следующие конфигурации.

Клиент VPN

Маршрутизатор

Конфигурация клиента VPN

Конфигурация маршрутизатора

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
enable secret 5 $1$v5OP$mPuiEQn8ULa8hVMYVOV1D.
enable password ww
!
ip subnet-zero
!
cns event-service server
!
!--- IKE configuration.  crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0
crypto isakmp client configuration address-pool local
ourpool
!
!--- IPSec configuration. crypto ipsec transform-set
trans1 esp-des esp-md5-hmac
!
crypto dynamic-map dynmap 10
set transform-set trans1
!
crypto map intmap client configuration address initiate
crypto map intmap client configuration address respond
crypto map intmap 10 ipsec-isakmp dynamic dynmap
 !
 interface Ethernet0
ip address 201.70.32.101 255.255.255.0
 no ip directed-broadcast
ip nat outside
no ip route-cache
no ip mroute-cache
 crypto map intmap
 !
interface Serial1
ip address 10.2.2.1 255.255.255.0
no ip directed-broadcast
ip nat inside
!
 ip local pool ourpool 10.2.1.1 10.2.1.254
ip nat pool outsidepool 201.70.32.150 201.70.32.160
netmask 255.255.255.0
!--- Except the private network to private network
traffic !--- from the NAT process. ip nat inside source
route-map nonat pool outsidepool
 ip classless
ip route 0.0.0.0 0.0.0.0 201.70.32.1
```

```
no ip http server
!--- Except the private network to private network
traffic !--- from the NAT process. access-list 101 deny
ip 10.2.2.0 0.0.0.255 10.2.1.0 0.0.0.255 access-list 101
permit ip 10.2.2.0 0.0.0.255 any route-map nonat permit
10 match ip address 101 ! line con 0 transport input
none line aux 0 line vty 0 4 password ww login ! end
```

Проверка

В данном разделе содержатся сведения о проверке работы конфигурации.

Некоторые команды **show** поддерживаются интерпретатором выходных данных (доступен только для зарегистрированных заказчиков); интерпретатор позволяет просматривать анализ выходных данных команды **show**.

show crypto engine connections active – отображает зашифрованные и расшифрованные пакеты.

show crypto ipsec sa – отображает ассоциации безопасности, соответствующие второму этапу.

show crypto isakmp sa – отображает ассоциации безопасности, соответствующие первому этапу.

Поиск и устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Примечание. Прежде чем применять команды отладки (**debug**), ознакомьтесь с разделом Важные сведения о командах отладки.

Следующие команды отладки необходимо выполнять на обоих (одноранговых) маршрутизаторах IPSec. Удаление ассоциаций безопасности должно быть выполнено на обоих соединениях.

debug crypto ipsec – отображает процесс согласования по протоколу IPSec на этапе 2.

debug crypto isakmp – отображает процесс согласования по протоколу ISAKMP на этапе 1.

debug crypto engine – отображает зашифрованный трафик.

clear crypto isakmp – удаляет ассоциации безопасности, соответствующие первому этапу.

clear crypto sa – удаляет ассоциации безопасности, соответствующие второму этапу.

Пример отладочных выходных данных

Отладочные данные маршрутизатора

```
Apr 18 15:17:59: ISAKMP (4): received packet from
    201.70.32.82 (R) MM_NO_STATE
Apr 18 15:17:59: ISAKMP (4): received packet from
    201.70.32.82 (R) MM_NO_STATE
Apr 18 15:18:03: ISAKMP (0): received packet from
    201.70.32.82 (N) NEW SA
Apr 18 15:18:03: ISAKMP (0:5): processing SA payload.
    message ID = 0
Apr 18 15:18:03: ISAKMP (0:5): Checking ISAKMP transform
1
    against priority 1 policy
Apr 18 15:18:03: ISAKMP:      encryption DES-CBC
Apr 18 15:18:03: ISAKMP:      hash MD5
Apr 18 15:18:03: ISAKMP:      default group 1
Apr 18 15:18:03: ISAKMP:      auth pre-share
Apr 18 15:18:03: ISAKMP (0:5): atts are acceptable.
    Next payload is 0
Apr 18 15:18:03: CryptoEngine0: generate alg parameter
Apr 18 15:18:05: CRYPTO_ENGINE: Dh phase 1 status: 0
Apr 18 15:18:05: CRYPTO_ENGINE: Dh phase 1 status: 0
Apr 18 15:18:05: ISAKMP (0:5): SA is doing pre-shared
    key authentication
Apr 18 15:18:05: ISAKMP (5): SA is doing pre-shared
    key authentication using id type ID_IPV4_ADDR
Apr 18 15:18:05: ISAKMP (5): sending packet to
    201.70.32.82 (R) MM_SA_SETUP
Apr 18 15:18:05: ISAKMP (5): received packet from
    201.70.32.82 (R) MM_SA_SETUP
Apr 18 15:18:05: ISAKMP (0:5): processing KE payload.
    message ID = 0
Apr 18 15:18:05: CryptoEngine0: generate alg parameter
Apr 18 15:18:05: CRYPTO_ENGINE: Dh phase 1 status: 0
Apr 18 15:18:05: CRYPTO_ENGINE: Dh phase 1 status: 0
Apr 18 15:18:05: ISAKMP (0:5): SA is doing pre-shared
    key authentication
Apr 18 15:18:05: ISAKMP (5): SA is doing pre-shared
    key authentication using id
type ID_IPV4_ADDR
Apr 18 15:18:05: ISAKMP (5): sending packet to
    201.70.32.82 (R) MM_SA_SETUP
Apr 18 15:18:05: ISAKMP (5): received packet from
    201.70.32.82 (R) MM_SA_SETUP
Apr 18 15:18:05: ISAKMP (0:5): processing KE payload.
    message ID = 0
Apr 18 15:18:05: CryptoEngine0: generate alg parameter
Apr 18 15:18:07: ISAKMP (0:5): processing NONCE payload.
    message ID = 0
Apr 18 15:18:07: CryptoEngine0: create ISAKMP SKEYID for
    conn id 5
Apr 18 15:18:07: ISAKMP (0:5): SKEYID state generated
Apr 18 15:18:07: ISAKMP (0:5): processing vendor id
payload
Apr 18 15:18:07: ISAKMP (0:5): processing vendor id
payload
Apr 18 15:18:07: ISAKMP (5): sending packet to
201.70.32.82
```

```
    (R) MM_KEY_EXCH
Apr 18 15:18:07: ISAKMP (0:4): purging SA.
Apr 18 15:18:07: ISAKMP (0:4): purging node -1412157317
Apr 18 15:18:07: ISAKMP (0:4): purging node 1875403554
Apr 18 15:18:07: CryptoEngine0: delete connection 4
Apr 18 15:18:08: ISAKMP (5): received packet from
    201.70.32.82 (R) MM_KEY_EXCH
Apr 18 15:18:08: ISAKMP (0:5): processing ID payload.
    message ID = 0
Apr 18 15:18:08: ISAKMP (0:5): processing HASH payload.
    message ID = 0
Apr 18 15:18:08: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:08: ISAKMP (5): processing NOTIFY payload
    24578 protocol 1 spi 0, message ID = 0
Apr 18 15:18:08: ISAKMP (0:5): SA has been authenticated
    with 201.70.32.82
Apr 18 15:18:08: ISAKMP (5): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
Apr 18 15:18:08: ISAKMP (5): Total payload length: 12
Apr 18 15:18:08: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:08: CryptoEngine0: clear dh number
    for conn id 1
Apr 18 15:18:08: ISAKMP (5): sending packet to
    201.70.32.82 (R) QM_IDLE
Apr 18 15:18:08: ISAKMP (5): received packet from
    201.70.32.82 (R) QM_IDLE
Apr 18 15:18:08: ISAKMP (0:5): Locking struct 14D0DC
    on allocation
Apr 18 15:18:08: ISAKMP (0:5): allocating address
    10.2.1.1
Apr 18 15:18:08: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:08: ISAKMP (0:5): initiating peer config to
    201.70.32.82. message ID = 1226793520
Apr 18 15:18:08: ISAKMP (5): sending packet to
201.70.32.82
    (R) QM_IDLE
Apr 18 15:18:09: ISAKMP (5): received packet from
201.70.32.82
    (R) QM_IDLE
Apr 18 15:18:09: ISAKMP (0:5): processing transaction
payload
    from 201.70.32.82. message ID = 1226793520
Apr 18 15:18:09: ISAKMP: recieved config from
201.70.32.82   .
Apr 18 15:18:09: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:09: ISAKMP:     Config payload type: 4
Apr 18 15:18:09: ISAKMP (0:5): peer accepted the
address!
Apr 18 15:18:09: ISAKMP (0:5): adding static route for
10.2.1.1
Apr 18 15:18:09: ISAKMP (0:5): deleting node 1226793520
Apr 18 15:18:09: CryptoEngine0: generate hmac context
for
    conn id 5
Apr 18 15:18:09: ISAKMP (0:5): processing SA payload.
    message ID = -617682048
```

```
Apr 18 15:18:09: ISAKMP (0:5): Checking IPSec proposal 1
Apr 18 15:18:09: ISAKMP: transform 1, ESP_DES
Apr 18 15:18:09: ISAKMP:   attributes in transform:
Apr 18 15:18:09: ISAKMP:      authenticator is HMAC-MD5
Apr 18 15:18:09: ISAKMP:      encaps is 1
Apr 18 15:18:09: validate proposal 0
Apr 18 15:18:09: ISAKMP (0:5): atts are acceptable.
Apr 18 15:18:09: IPSEC(validate_proposal_request):
    proposal part #1, (key eng. msg.) dest=
201.70.32.101,
    src= 201.70.32.82, dest_proxy=
10.2.2.0/255.255.255.0/0/0
    (type=4), src_proxy= 10.2.1.1/255.255.255.255/0/0
(type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0,
keysize= 0,
    flags= 0x4
Apr 18 15:18:09: validate proposal request 0
Apr 18 15:18:09: ISAKMP (0:5): processing NONCE payload.
    message ID = -617682048
Apr 18 15:18:09: ISAKMP (0:5): processing ID payload.
    message ID = -617682048
Apr 18 15:18:09: ISAKMP (5): ID_IPV4_ADDR src 10.2.1.1
    prot 0 port 0
Apr 18 15:18:09: ISAKMP (0:5): processing ID payload.
    message ID = -617682048
Apr 18 15:18:09: ISAKMP (5): ID_IPV4_ADDR_SUBNET dst
    10.2.2.0/255.255.255.0 prot 0 port 0
Apr 18 15:18:09: IPSEC(key_engine): got a queue event...
Apr 18 15:18:09: IPSEC(spi_response): getting spi
    153684796 for SA from 201.70.32.82    to
201.70.32.101
    for prot 3
Apr 18 15:18:09: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:09: ISAKMP (5): sending packet to
201.70.32.82
    (R) QM_IDLE
Apr 18 15:18:09: ISAKMP (5): received packet from
201.70.32.82
    (R) QM_IDLE
Apr 18 15:18:09: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:09: ISAKMP (0:5): processing SA payload.
    message ID = -1078114754
Apr 18 15:18:09: ISAKMP (0:5): Checking IPSec proposal 1
Apr 18 15:18:10: ISAKMP: transform 1, ESP_DES
Apr 18 15:18:10: ISAKMP:   attributes in transform:
Apr 18 15:18:10: ISAKMP:      authenticator is HMAC-MD5
Apr 18 15:18:10: ISAKMP:      encaps is 1
Apr 18 15:18:10: validate proposal 0
Apr 18 15:18:10: ISAKMP (0:5): atts are acceptable.
Apr 18 15:18:10: IPSEC(validate_proposal_request):
    proposal part #1, (key eng. msg.) dest=
201.70.32.101,
    src= 201.70.32.82, dest_proxy=
10.2.2.0/255.255.255.0/0/0
    (type=4), src_proxy= 10.2.1.1/255.255.255.255/0/0
(type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0,
keysize= 0,
    flags= 0x4
```

```
Apr 18 15:18:10: validate proposal request 0
Apr 18 15:18:10: ISAKMP (0:5): processing NONCE payload.
    message ID = -1078114754
Apr 18 15:18:10: ISAKMP (0:5): processing ID payload.
    message ID = -1078114754
Apr 18 15:18:10: ISAKMP (5): ID_IPV4_ADDR src 10.2.1.1
    prot 0 port 0
Apr 18 15:18:10: ISAKMP (0:5): processing ID payload.
    message ID = -1078114754
Apr 18 15:18:10: ISAKMP (5): ID_IPV4_ADDR_SUBNET dst
    10.2.2.0/255.255.255.0 prot 0 port 0
Apr 18 15:18:10: IPSEC(key_engine): got a queue event...
Apr 18 15:18:10: IPSEC(spi_response): getting spi
224008976
    for SA from 201.70.32.82    to 201.70.32.101
    for prot 3
Apr 18 15:18:10: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:10: ISAKMP (5): sending packet to
201.70.32.82
    (R) QM_IDLE
Apr 18 15:18:10: ISAKMP (5): received packet from
201.70.32.82
    (R) QM_IDLE
Apr 18 15:18:10: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:10: ipsec allocate flow 0
Apr 18 15:18:10: ipsec allocate flow 0
Apr 18 15:18:10: ISAKMP (0:5): Creating IPSec SAs
Apr 18 15:18:10:         inbound SA from 201.70.32.82
    to 201.70.32.101   (proxy 10.2.1.1        to
10.2.2.0)
Apr 18 15:18:10:         has spi 224008976 and conn_id
2000
    and flags 4
Apr 18 15:18:10:         outbound SA from 201.70.32.101
    to 201.70.32.82    (proxy 10.2.2.0        to
10.2.1.1)
Apr 18 15:18:10:         has spi -1084694986 and conn_id
2001
    and flags 4
Apr 18 15:18:10: ISAKMP (0:5): deleting node -1078114754
Apr 18 15:18:10: IPSEC(key_engine): got a queue event...
Apr 18 15:18:10: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 201.70.32.101, src=
201.70.32.82,
    dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.2.1.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xD5A1B10(224008976), conn_id= 2000, keysize=
0,
    flags= 0x4
Apr 18 15:18:10: IPSEC(initialize_sas): ,
  (key eng. msg.) src= 201.70.32.101, dest=
201.70.32.82,
    src_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.2.1.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xBF58DE36(3210272310), conn_id= 2001, keysize=
0,
    flags= 0x4
Apr 18 15:18:10: IPSEC(create_sa): sa created,
```

```
  (sa) sa_dest= 201.70.32.101, sa_prot= 50,
    sa_spi= 0xD5A1B10(224008976),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2000
Apr 18 15:18:10: IPSEC(create_sa): sa created,
  (sa) sa_dest= 201.70.32.82, sa_prot= 50,
    sa_spi= 0xBF58DE36(3210272310),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001
Apr 18 15:18:10: ISAKMP: Locking struct 14D0DC for IPSEC
Apr 18 15:18:24: ISAKMP (0:5): retransmitting
    phase 2 -617682048 ...
Apr 18 15:18:24: ISAKMP (5): sending packet to
201.70.32.82
    (R) QM_IDLE

Router#show crypto ipsec
Apr 18 15:18:39: ISAKMP (0:5): retransmitting
    phase 2 -617682048 ...
Apr 18 15:18:39: ISAKMP (5): sending packet to
201.70.32.82
    (R) QM_IDLE      sa

interface: Ethernet0
    Crypto map tag: intmap, local addr. 201.70.32.101

   local  ident (addr/mask/prot/port):
   (10.2.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port):
   (10.2.1.1/255.255.255.255/0/0)
   current_peer: 201.70.32.82
     PERMIT, flags={}
    #pkts encaps: 7, #pkts encrypt: 7, #pkts digest 7
    #pkts decaps: 7, #pkts decrypt: 7, #pkts verify 7
    #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.: 201.70.32.101, remote
     crypto endpt.: 201.70.32.82
     path mtu 1500, media mtu 1500
     current outbound spi: BF58DE36

     inbound esp sas:
      spi: 0xD5A1B10(224008976)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1,
        crypto map: intmap
        sa timing: remaining key lifetime
       (k/sec): (4607999/3500)
        IV size: 8 bytes
        replay detection support: Y


     inbound ah sas:


     inbound pcp sas:


     outbound esp sas:
      spi: 0xBF58DE36(3210272310)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
```

```
        slot: 0, conn id: 2001, flow_id: 2,
     crypto map: intmap
        sa timing: remaining key lifetime
        (k/sec): (4607999/3500)
        IV size: 8 bytes
        replay detection support: Y


     outbound ah sas:

     outbound pcp sas:

Router#sho crypto engine connections active

  ID Interface       IP-Address      State  Algorithm
Encrypt  Decrypt
   5                     set    HMAC_MD5+DES_56_CB
0        0
2000 Ethernet0       201.70.32.101   set
HMAC_MD5+DES_56_CB  0        7
2001 Ethernet0       201.70.32.101   set
HMAC_MD5+DES_56_CB  7        0
Crypto adjacency count : Lock: 0, Unlock: 0
```

Сведения о клиенте VPN

```
Apr 18 15:17:59: ISAKMP (4): received packet from
    201.70.32.82 (R) MM_NO_STATE
Apr 18 15:17:59: ISAKMP (4): received packet from
    201.70.32.82 (R) MM_NO_STATE
Apr 18 15:18:03: ISAKMP (0): received packet from
    201.70.32.82 (N) NEW SA
Apr 18 15:18:03: ISAKMP (0:5): processing SA payload.
    message ID = 0
Apr 18 15:18:03: ISAKMP (0:5): Checking ISAKMP transform
1
    against priority 1 policy
Apr 18 15:18:03: ISAKMP:      encryption DES-CBC
Apr 18 15:18:03: ISAKMP:      hash MD5
Apr 18 15:18:03: ISAKMP:      default group 1
Apr 18 15:18:03: ISAKMP:      auth pre-share
Apr 18 15:18:03: ISAKMP (0:5): atts are acceptable.
    Next payload is 0
Apr 18 15:18:03: CryptoEngine0: generate alg parameter
Apr 18 15:18:05: CRYPTO_ENGINE: Dh phase 1 status: 0
Apr 18 15:18:05: CRYPTO_ENGINE: Dh phase 1 status: 0
Apr 18 15:18:05: ISAKMP (0:5): SA is doing pre-shared
    key authentication
Apr 18 15:18:05: ISAKMP (5): SA is doing pre-shared
    key authentication using id type ID_IPV4_ADDR
Apr 18 15:18:05: ISAKMP (5): sending packet to
    201.70.32.82 (R) MM_SA_SETUP
Apr 18 15:18:05: ISAKMP (5): received packet from
    201.70.32.82 (R) MM_SA_SETUP
Apr 18 15:18:05: ISAKMP (0:5): processing KE payload.
    message ID = 0
Apr 18 15:18:05: CryptoEngine0: generate alg parameter
Apr 18 15:18:05: CRYPTO_ENGINE: Dh phase 1 status: 0
Apr 18 15:18:05: CRYPTO_ENGINE: Dh phase 1 status: 0
Apr 18 15:18:05: ISAKMP (0:5): SA is doing pre-shared
    key authentication
Apr 18 15:18:05: ISAKMP (5): SA is doing pre-shared
    key authentication using id
type ID_IPV4_ADDR
Apr 18 15:18:05: ISAKMP (5): sending packet to
```

```
    201.70.32.82 (R) MM_SA_SETUP
Apr 18 15:18:05: ISAKMP (5): received packet from
    201.70.32.82 (R) MM_SA_SETUP
Apr 18 15:18:05: ISAKMP (0:5): processing KE payload.
    message ID = 0
Apr 18 15:18:05: CryptoEngine0: generate alg parameter
Apr 18 15:18:07: ISAKMP (0:5): processing NONCE payload.
    message ID = 0
Apr 18 15:18:07: CryptoEngine0: create ISAKMP SKEYID for
    conn id 5
Apr 18 15:18:07: ISAKMP (0:5): SKEYID state generated
Apr 18 15:18:07: ISAKMP (0:5): processing vendor id
payload
Apr 18 15:18:07: ISAKMP (0:5): processing vendor id
payload
Apr 18 15:18:07: ISAKMP (5): sending packet to
201.70.32.82
    (R) MM_KEY_EXCH
Apr 18 15:18:07: ISAKMP (0:4): purging SA.
Apr 18 15:18:07: ISAKMP (0:4): purging node -1412157317
Apr 18 15:18:07: ISAKMP (0:4): purging node 1875403554
Apr 18 15:18:07: CryptoEngine0: delete connection 4
Apr 18 15:18:08: ISAKMP (5): received packet from
    201.70.32.82 (R) MM_KEY_EXCH
Apr 18 15:18:08: ISAKMP (0:5): processing ID payload.
    message ID = 0
Apr 18 15:18:08: ISAKMP (0:5): processing HASH payload.
    message ID = 0
Apr 18 15:18:08: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:08: ISAKMP (5): processing NOTIFY payload
    24578 protocol 1 spi 0, message ID = 0
Apr 18 15:18:08: ISAKMP (0:5): SA has been authenticated
    with 201.70.32.82
Apr 18 15:18:08: ISAKMP (5): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
Apr 18 15:18:08: ISAKMP (5): Total payload length: 12
Apr 18 15:18:08: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:08: CryptoEngine0: clear dh number
    for conn id 1
Apr 18 15:18:08: ISAKMP (5): sending packet to
    201.70.32.82 (R) QM_IDLE
Apr 18 15:18:08: ISAKMP (5): received packet from
    201.70.32.82 (R) QM_IDLE
Apr 18 15:18:08: ISAKMP (0:5): Locking struct 14D0DC
    on allocation
Apr 18 15:18:08: ISAKMP (0:5): allocating address
    10.2.1.1
Apr 18 15:18:08: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:08: ISAKMP (0:5): initiating peer config to
    201.70.32.82. message ID = 1226793520
Apr 18 15:18:08: ISAKMP (5): sending packet to
201.70.32.82
    (R) QM_IDLE
Apr 18 15:18:09: ISAKMP (5): received packet from
201.70.32.82
    (R) QM_IDLE
Apr 18 15:18:09: ISAKMP (0:5): processing transaction
```

```
payload
    from 201.70.32.82. message ID = 1226793520
Apr 18 15:18:09: ISAKMP: recieved config from
201.70.32.82   .
Apr 18 15:18:09: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:09: ISAKMP:     Config payload type: 4
Apr 18 15:18:09: ISAKMP (0:5): peer accepted the
address!
Apr 18 15:18:09: ISAKMP (0:5): adding static route for
10.2.1.1
Apr 18 15:18:09: ISAKMP (0:5): deleting node 1226793520
Apr 18 15:18:09: CryptoEngine0: generate hmac context
for
    conn id 5
Apr 18 15:18:09: ISAKMP (0:5): processing SA payload.
    message ID = -617682048
Apr 18 15:18:09: ISAKMP (0:5): Checking IPSec proposal 1
Apr 18 15:18:09: ISAKMP: transform 1, ESP_DES
Apr 18 15:18:09: ISAKMP:   attributes in transform:
Apr 18 15:18:09: ISAKMP:      authenticator is HMAC-MD5
Apr 18 15:18:09: ISAKMP:      encaps is 1
Apr 18 15:18:09: validate proposal 0
Apr 18 15:18:09: ISAKMP (0:5): atts are acceptable.
Apr 18 15:18:09: IPSEC(validate_proposal_request):
    proposal part #1, (key eng. msg.) dest=
201.70.32.101,
    src= 201.70.32.82, dest_proxy=
10.2.2.0/255.255.255.0/0/0
    (type=4), src_proxy= 10.2.1.1/255.255.255.255/0/0
(type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0,
keysize= 0,
    flags= 0x4
Apr 18 15:18:09: validate proposal request 0
Apr 18 15:18:09: ISAKMP (0:5): processing NONCE payload.
    message ID = -617682048
Apr 18 15:18:09: ISAKMP (0:5): processing ID payload.
    message ID = -617682048
Apr 18 15:18:09: ISAKMP (5): ID_IPV4_ADDR src 10.2.1.1
    prot 0 port 0
Apr 18 15:18:09: ISAKMP (0:5): processing ID payload.
    message ID = -617682048
Apr 18 15:18:09: ISAKMP (5): ID_IPV4_ADDR_SUBNET dst
    10.2.2.0/255.255.255.0 prot 0 port 0
Apr 18 15:18:09: IPSEC(key_engine): got a queue event...
Apr 18 15:18:09: IPSEC(spi_response): getting spi
    153684796 for SA from 201.70.32.82    to
201.70.32.101
    for prot 3
Apr 18 15:18:09: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:09: ISAKMP (5): sending packet to
201.70.32.82
    (R) QM_IDLE
Apr 18 15:18:09: ISAKMP (5): received packet from
201.70.32.82
    (R) QM_IDLE
Apr 18 15:18:09: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:09: ISAKMP (0:5): processing SA payload.
    message ID = -1078114754
Apr 18 15:18:09: ISAKMP (0:5): Checking IPSec proposal 1
```

```
Apr 18 15:18:10: ISAKMP: transform 1, ESP_DES
Apr 18 15:18:10: ISAKMP:   attributes in transform:
Apr 18 15:18:10: ISAKMP:      authenticator is HMAC-MD5
Apr 18 15:18:10: ISAKMP:      encaps is 1
Apr 18 15:18:10: validate proposal 0
Apr 18 15:18:10: ISAKMP (0:5): atts are acceptable.
Apr 18 15:18:10: IPSEC(validate_proposal_request):
    proposal part #1, (key eng. msg.) dest=
201.70.32.101,
    src= 201.70.32.82, dest_proxy=
10.2.2.0/255.255.255.0/0/0
    (type=4), src_proxy= 10.2.1.1/255.255.255.255/0/0
(type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0,
keysize= 0,
    flags= 0x4
Apr 18 15:18:10: validate proposal request 0
Apr 18 15:18:10: ISAKMP (0:5): processing NONCE payload.
    message ID = -1078114754
Apr 18 15:18:10: ISAKMP (0:5): processing ID payload.
    message ID = -1078114754
Apr 18 15:18:10: ISAKMP (5): ID_IPV4_ADDR src 10.2.1.1
    prot 0 port 0
Apr 18 15:18:10: ISAKMP (0:5): processing ID payload.
    message ID = -1078114754
Apr 18 15:18:10: ISAKMP (5): ID_IPV4_ADDR_SUBNET dst
    10.2.2.0/255.255.255.0 prot 0 port 0
Apr 18 15:18:10: IPSEC(key_engine): got a queue event...
Apr 18 15:18:10: IPSEC(spi_response): getting spi
224008976
    for SA from 201.70.32.82    to 201.70.32.101
    for prot 3
Apr 18 15:18:10: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:10: ISAKMP (5): sending packet to
201.70.32.82
    (R) QM_IDLE
Apr 18 15:18:10: ISAKMP (5): received packet from
201.70.32.82
    (R) QM_IDLE
Apr 18 15:18:10: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:10: ipsec allocate flow 0
Apr 18 15:18:10: ipsec allocate flow 0
Apr 18 15:18:10: ISAKMP (0:5): Creating IPSec SAs
Apr 18 15:18:10:         inbound SA from 201.70.32.82
    to 201.70.32.101   (proxy 10.2.1.1        to
10.2.2.0)
Apr 18 15:18:10:         has spi 224008976 and conn_id
2000
    and flags 4
Apr 18 15:18:10:         outbound SA from 201.70.32.101
    to 201.70.32.82    (proxy 10.2.2.0        to
10.2.1.1)
Apr 18 15:18:10:         has spi -1084694986 and conn_id
2001
    and flags 4
Apr 18 15:18:10: ISAKMP (0:5): deleting node -1078114754
Apr 18 15:18:10: IPSEC(key_engine): got a queue event...
Apr 18 15:18:10: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 201.70.32.101, src=
201.70.32.82,
    dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
```

```
    src_proxy= 10.2.1.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xD5A1B10(224008976), conn_id= 2000, keysize=
0,
    flags= 0x4
Apr 18 15:18:10: IPSEC(initialize_sas): ,
  (key eng. msg.) src= 201.70.32.101, dest=
201.70.32.82,
    src_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.2.1.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xBF58DE36(3210272310), conn_id= 2001, keysize=
0,
    flags= 0x4
Apr 18 15:18:10: IPSEC(create_sa): sa created,
  (sa) sa_dest= 201.70.32.101, sa_prot= 50,
    sa_spi= 0xD5A1B10(224008976),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2000
Apr 18 15:18:10: IPSEC(create_sa): sa created,
  (sa) sa_dest= 201.70.32.82, sa_prot= 50,
    sa_spi= 0xBF58DE36(3210272310),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001
Apr 18 15:18:10: ISAKMP: Locking struct 14D0DC for IPSEC
Apr 18 15:18:24: ISAKMP (0:5): retransmitting
    phase 2 -617682048 ...
Apr 18 15:18:24: ISAKMP (5): sending packet to
201.70.32.82
    (R) QM_IDLE

Router#show crypto ipsec
Apr 18 15:18:39: ISAKMP (0:5): retransmitting
    phase 2 -617682048 ...
Apr 18 15:18:39: ISAKMP (5): sending packet to
201.70.32.82
    (R) QM_IDLE      sa

interface: Ethernet0
    Crypto map tag: intmap, local addr. 201.70.32.101

   local  ident (addr/mask/prot/port):
   (10.2.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port):
   (10.2.1.1/255.255.255.255/0/0)
   current_peer: 201.70.32.82
     PERMIT, flags={}
    #pkts encaps: 7, #pkts encrypt: 7, #pkts digest 7
    #pkts decaps: 7, #pkts decrypt: 7, #pkts verify 7
    #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.: 201.70.32.101, remote
     crypto endpt.: 201.70.32.82
     path mtu 1500, media mtu 1500
     current outbound spi: BF58DE36

     inbound esp sas:
      spi: 0xD5A1B10(224008976)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1,
```

```
        crypto map: intmap
        sa timing: remaining key lifetime
       (k/sec): (4607999/3500)
        IV size: 8 bytes
        replay detection support: Y


     inbound ah sas:


     inbound pcp sas:


     outbound esp sas:
      spi: 0xBF58DE36(3210272310)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2,
     crypto map: intmap
        sa timing: remaining key lifetime
        (k/sec): (4607999/3500)
        IV size: 8 bytes
        replay detection support: Y


     outbound ah sas:

     outbound pcp sas:

Router#sho crypto engine connections active

  ID Interface       IP-Address      State  Algorithm
Encrypt  Decrypt
   5                     set    HMAC_MD5+DES_56_CB
0        0
2000 Ethernet0       201.70.32.101   set
HMAC_MD5+DES_56_CB  0        7
2001 Ethernet0       201.70.32.101   set
HMAC_MD5+DES_56_CB  7        0
Crypto adjacency count : Lock: 0, Unlock: 0
```

Дополнительные сведения

- Настройка параметров сетевой безопасности IPSec
- Настройка протокола защищенного обмена ключами IKE
- Введение в протокол IPSec
- Страницы поддержки продуктов с IP Security (IPSec)
- Техническая поддержка — Cisco Systems