

Конфигурация Router-to-Router LAN-to-LAN туннеля с маршрутизатором, иницирующим агрессивный режим IKE

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Общие сведения](#)

[Настройка](#)

[Схема сети](#)

[Конфигурации](#)

[Проверка](#)

[Устранение неполадок](#)

[Команды для устранения неполадок](#)

[Выходные данные отладки маршрутизатора RouterA](#)

[Дополнительные сведения](#)

Введение

В выпуске ПО Cisco IOS® 12.2 (8) T введены функции маршрутизатора для иницирования обмена ключами между сетями (IKE) в агрессивном режиме. Для получения дополнительной информации посмотрите Идентификатор ошибки [CSCdt30808 \(только зарегистрированные клиенты\)](#) в Bug Toolkit. Ранее маршрутизатор мог ответить на запрос согласования туннеля в агрессивном режиме, но никогда не мог иницировать его самостоятельно.

Предварительные условия

Требования

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

Сведения в этом документе основаны на версиях оборудования и программного обеспечения, указанных ниже.

- Cisco IOS 12.2 (8) T использовался на обоих маршрутизаторах, невзирая на то, что необязательно иметь его на принимающем маршрутизаторе.

Примечание: Эта конфигурация была протестирована с Release 12.2 программного обеспечения Cisco IOS (13) T1. Все аспекты конфигурации остаются теми же самыми.

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Условные обозначения

[Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.](#)

Общие сведения

Примечание: Новые команды интерфейса командной строки (CLI) следующие:

- `crypto isakmp peer <адрес <x. x. x. x> | <name> имени хоста>`
- `set aggressive-mode client-endpoint <fqdn <name> | ipv4 address <x. x. x. x> | пользовательский-fqdn <name>>`
- `<password> set aggressive-mode password`

В приведенном ниже примере конфигурации маршрутизаторы RouterA и RouterB соединены туннелем между локальными сетями. Маршрутизатор A всегда будет маршрутизатором, иницирующим туннель, и в этом примере он настроен инициировать в агрессивном режиме. Маршрутизатор B просто использует динамическую криптокарту для приема параметров туннеля от маршрутизатора A, хотя для него также может применяться стандартная конфигурация туннеля между локальными сетями (LAN-to-LAN).

Примечание: В данном примере RouterB не должен выполнять программное обеспечение Cisco IOS версии 12.2(8)T для принятия параметров туннеля от RouterA. Как показано выше, маршрутизаторы всегда принимали запрос агрессивного режима, однако они никогда не могут запустить его.

Настройка

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

Примечание: [Поиск дополнительной информации о командах в данном документе можно выполнить с помощью средства "Command Lookup" \(Поиск команд\) \(только для зарегистрированных клиентов\).](#)

Схема сети

В данном документе используется сетевая установка, показанная на следующей схеме.

1.1.1.1/24 Loopback0

14.38.69.70



RouterA

2.2.2.2/24 Loopback0

14.38.69.71



RouterB

14.38.69.0/16

Tunnel

Конфигурации

Эти конфигурации используются в данном документе:

- [Маршрутизатор A](#)
- [Маршрутизатор B](#)

Маршрутизатор A

```
Building configuration...

Current configuration : 1253 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!
!
memory-size iomem 10
ip subnet-zero
!
!
!
!
crypto isakmp policy 1
  hash md5
  authentication pre-share
crypto isakmp keepalive 30 5
!
crypto isakmp peer address 14.38.69.71
  set aggressive-mode password cisco123
  set aggressive-mode client-endpoint ipv4-address
14.38.69.70
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map mymap 1 ipsec-isakmp
  set peer 14.38.69.71
  set transform-set myset
  match address 100
!
!
!
interface Loopback0
  ip address 1.1.1.1 255.255.255.0
!
interface Ethernet0/0
```

```
ip address 14.38.69.70 255.255.0.0
half-duplex
crypto map mymap
!
interface BRI0/0
no ip address
shutdown
!
interface Ethernet0/1
no ip address
shutdown
half-duplex
!
ip classless
ip route 0.0.0.0 0.0.0.0 14.38.69.71
ip http server
!
!
access-list 100 permit ip 1.1.1.0 0.0.0.255 2.2.2.0
0.0.0.255
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
login
!
!
end
```

Маршрутизатор В

```
Building configuration...

Current configuration : 1147 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterB
!
!
ip subnet-zero
!
!
!
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 14.38.69.70
crypto isakmp keepalive 30 5
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
```

```
!  
crypto dynamic-map mymap 10  
  set transform-set myset  
!  
!  
crypto map mainmap 1 ipsec-isakmp dynamic mymap  
!  
!  
!  
interface Loopback0  
  ip address 2.2.2.2 255.255.255.0  
!  
interface FastEthernet0/0  
  ip address 14.38.69.71 255.255.0.0  
  duplex auto  
  speed auto  
  crypto map mainmap  
!  
interface Serial0/0  
  no ip address  
  shutdown  
  no fair-queue  
!  
interface FastEthernet0/1  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 14.38.69.70  
no ip http server  
!  
!  
call rsvp-sync  
!  
!  
mgcp profile default  
!  
dial-peer cor custom  
!  
!  
line con 0  
  exec-timeout 0 0  
  speed 115200  
line aux 0  
line vty 0 4  
  login  
!  
!  
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.

- команда `show crypto ipsec sa` – отображает связи безопасности, соответствующие второму этапу.
- команда `show crypto isakmp sa` в ТБ отображает сопоставления безопасности, соответствующие первому этапу

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Примечание: Прежде чем применять команды отладки, ознакомьтесь с разделом "Важные сведения о командах отладки".

- команда `debug crypto ipsec` отображает согласование IPsec на втором этапе.
- `debug crypto isakmp` – вывод данных о согласовании ISAKMP в фазе 1.
- "debug crypto engine" - отображается зашифрованный трафик.

Выходные данные отладки маршрутизатора RouterA

```
00:08:26: IPSEC(sa_request): ,
(key eng. msg.) OUTBOUND local= 14.38.69.70, remote= 14.38.69.71,
  local_proxy= 1.1.1.0/255.255.255.0/0/0 (type=4),
  remote_proxy= 2.2.2.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-3des esp-md5-hmac ,
  lifedur= 3600s and 4608000kb,
  spi= 0x4B68058A(1265108362), conn_id= 0, keysize= 0, flags= 0x400C
00:08:26: ISAKMP: received ke message (1/1)
00:08:26: ISAKMP: local port 500, remote port 500
00:08:26: ISAKMP (0:1): SA has tunnel attributes set.
00:08:26: ISAKMP (0:1): SA is doing unknown authentication!
00:08:26: ISAKMP (1): ID payload
  next-payload : 13
  type          : 1
  protocol      : 17
  port          : 500
  length        : 8
00:08:26: ISAKMP (1): Total payload length: 12
00:08:26: ISAKMP (0:1): Input = IKE_MSG_FROM_IPSEC, IKE_SA_REQ_AM
Old State = IKE_READY New State = IKE_I_AM1

00:08:26: ISAKMP (0:1): beginning Aggressive Mode exchange
00:08:26: ISAKMP (0:1): sending packet to 14.38.69.71 (I) AG_INIT_EXCH...
Success rate is 0 percent (0/5)
vpn-2611a1#
00:08:36: ISAKMP (0:1): retransmitting phase 1 AG_INIT_EXCH...
00:08:36: ISAKMP (0:1): incrementing error counter on sa: retransmit phase 1
00:08:36: ISAKMP (0:1): retransmitting phase 1 AG_INIT_EXCH
00:08:36: ISAKMP (0:1): sending packet to 14.38.69.71 (I) AG_INIT_EXCH
00:08:37: ISAKMP (0:1): received packet from 14.38.69.71 (I) AG_INIT_EXCH
00:08:37: ISAKMP (0:1): processing SA payload. message ID = 0
00:08:37: ISAKMP (0:1): SA using tunnel password as pre-shared key.
00:08:37: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
00:08:37: ISAKMP:          encryption DES-CBC
00:08:37: ISAKMP:          hash MD5
00:08:37: ISAKMP:          default group 1
```

```
00:08:37: ISAKMP:      auth pre-share
00:08:37: ISAKMP:      life type in seconds
00:08:37: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
00:08:37: ISAKMP (0:1): atts are acceptable. Next payload is 0
00:08:37: ISAKMP (0:1): processing vendor id payload
00:08:37: ISAKMP (0:1): vendor ID is Unity
00:08:37: ISAKMP (0:1): processing vendor id payload
00:08:37: ISAKMP (0:1): vendor ID is DPD
00:08:37: ISAKMP (0:1): processing vendor id payload
00:08:37: ISAKMP (0:1): speaking to another IOS box!
00:08:37: ISAKMP (0:1): processing vendor id payload
00:08:37: ISAKMP (0:1): processing KE payload. message ID = 0
00:08:37: ISAKMP (0:1): processing ID payload. message ID = 0
00:08:37: ISAKMP (0:1): processing NONCE payload. message ID = 0
00:08:37: ISAKMP (0:1): SA using tunnel password as pre-shared key.
00:08:37: ISAKMP (0:1): SKEYID state generated
00:08:37: ISAKMP (0:1): processing HASH payload. message ID = 0
00:08:37: ISAKMP (0:1): SA has been authenticated with 14.38.69.71
00:08:37: ISAKMP (0:1): IKE_DPD is enabled, initializing timers
00:08:37: ISAKMP: Locking DPD struct 0x82702444
      from crypto_ikmp_dpd_ike_init, count 1
00:08:37: ISAKMP (0:1): sending packet to 14.38.69.71 (I) QM_IDLE
00:08:37: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_I_AM1  New State = IKE_P1_COMPLETE

00:08:37: IPSEC(key_engine): got a queue event...
00:08:37: IPsec: Key engine got KEYENG_IKMP_MORE_SAS message
00:08:37: ISAKMP: received ke message (6/1)
00:08:37: ISAKMP: received KEYENG_IKMP_MORE_SAS message
00:08:37: ISAKMP (0:1): sending packet to 14.38.69.71 (I) QM_IDLE
00:08:37: ISAKMP (0:1): purging node -1844394438
00:08:37: ISAKMP (0:1): Sending initial contact.

00:08:37: ISAKMP (0:1): received packet from 14.38.69.71 (I) QM_IDLE
00:08:37: ISAKMP (0:1): processing HASH payload. message ID = 133381228
00:08:37: ISAKMP (0:1): processing NOTIFY RESPONDER_LIFETIME protocol 1
      spi 0, message ID = 133381228, sa = 82701CDC
00:08:37: ISAKMP (0:1): processing responder lifetime
00:08:37: ISAKMP (0:1): deleting node 133381228 error
      FALSE reason "informational (in) state 1"
00:08:37: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_INFO_NOTIFY
Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

00:08:38: ISAKMP: quick mode timer expired.
00:08:38: ISAKMP (0:1): src 14.38.69.70 dst 14.38.69.71
00:08:38: ISAKMP (0:1): beginning Quick Mode exchange, M-ID of -1119238561
00:08:38: ISAKMP (0:1): sending packet to 14.38.69.71 (I) QM_IDLE
00:08:38: ISAKMP (0:1): Node -1119238561, Input = IKE_MESG_INTERNAL,
      IKE_INIT_QM Old State = IKE_QM_READY  New State = IKE_QM_I_QM1

00:08:38: ISAKMP (0:1): received packet from 14.38.69.71 (I) QM_IDLE
00:08:38: ISAKMP (0:1): processing HASH payload. message ID = -1119238561
00:08:38: ISAKMP (0:1): processing SA payload. message ID = -1119238561
00:08:38: ISAKMP (0:1): Checking IPsec proposal 1
00:08:38: ISAKMP: transform 1, ESP_3DES
00:08:38: ISAKMP:   attributes in transform:
00:08:38: ISAKMP:     encaps is 1
00:08:38: ISAKMP:     SA life type in seconds
00:08:38: ISAKMP:     SA life duration (basic) of 3600
00:08:38: ISAKMP:     SA life type in kilobytes
00:08:38: ISAKMP:     SA life duration (VPI) of  0x0 0x46 0x50 0x0
00:08:38: ISAKMP:     authenticator is HMAC-MD5
00:08:38: ISAKMP (0:1): atts are acceptable.
00:08:38: IPSEC(validate_proposal_request): proposal part #1,
```

```

(key eng. msg.) INBOUND local= 14.38.69.70, remote= 14.38.69.71,
  local_proxy= 1.1.1.0/255.255.255.0/0/0 (type=4),
  remote_proxy= 2.2.2.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-3des esp-md5-hmac ,
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
00:08:38: ISAKMP (0:1): processing NONCE payload. message ID = -1119238561
00:08:38: ISAKMP (0:1): processing ID payload. message ID = -1119238561
00:08:38: ISAKMP (0:1): processing ID payload. message ID = -1119238561
00:08:38: ISAKMP (0:1): Creating IPsec SAs
00:08:38:      inbound SA from 14.38.69.71 to 14.38.69.70
      (proxy 2.2.2.0 to 1.1.1.0)
00:08:38:      has spi 0x4B68058A and conn_id 2000 and flags 4
00:08:38:      lifetime of 3600 seconds
00:08:38:      lifetime of 4608000 kilobytes
00:08:38:      outbound SA from 14.38.69.70 to 14.38.69.71
      (proxy 1.1.1.0 to 2.2.2.0)
00:08:38:      has spi 1503230765 and conn_id 2001 and flags C
00:08:38:      lifetime of 3600 seconds
00:08:38:      lifetime of 4608000 kilobytes
00:08:38: ISAKMP (0:1): sending packet to 14.38.69.71 (I) QM_IDLE
00:08:38: ISAKMP (0:1): deleting node -1119238561 error FALSE reason ""
00:08:38: ISAKMP (0:1): Node -1119238561, Input = IKE_MSG_FROM_PEER,
      IKE_QM_EXCH Old State = IKE_QM_I_QM1
      New State = IKE_QM_PHASE2_COMPLETE

00:08:38: IPSEC(key_engine): got a queue event...
00:08:38: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 14.38.69.70, remote= 14.38.69.71,
  local_proxy= 1.1.1.0/255.255.255.0/0/0 (type=4),
  remote_proxy= 2.2.2.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-3des esp-md5-hmac ,
  lifedur= 3600s and 4608000kb,
  spi= 0x4B68058A(1265108362), conn_id= 2000, keysize= 0, flags= 0x4
00:08:38: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 14.38.69.70, remote= 14.38.69.71,
  local_proxy= 1.1.1.0/255.255.255.0/0/0 (type=4),
  remote_proxy= 2.2.2.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-3des esp-md5-hmac ,
  lifedur= 3600s and 4608000kb,
  spi= 0x59997B2D(1503230765), conn_id= 2001, keysize= 0, flags= 0xC
00:08:38: IPSEC(create_sa): sa created,
(sa) sa_dest= 14.38.69.70, sa_prot= 50,
  sa_spi= 0x4B68058A(1265108362),
  sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2000
00:08:38: IPSEC(create_sa): sa created,
(sa) sa_dest= 14.38.69.71, sa_prot= 50,
  sa_spi= 0x59997B2D(1503230765),
  sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2001
00:08:38: ISAKMP: received ke message (7/1)
00:08:38: ISAKMP: DPD received kei with flags 0x10
00:08:38: ISAKMP: Locking DPD struct 0x82702444 from
  crypto_ikmp_dpd_handle_kei_mess, count 2

```

[Дополнительные сведения](#)

- [Страница поддержки IPsec](#)
- [Техническая поддержка - Cisco Systems](#)