

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Настройка](#)

[Схема сети](#)

[Конфигурации](#)

[Проверка](#)

[выходные данные команды show с туннелями вверх](#)

[Устранение неполадок](#)

[Команды для устранения неполадок](#)

[Дополнительные сведения](#)

Введение

Обычные конфигурации IPSec неспособны передавать протоколы маршрутизации, такие как EIGRP и OSPF или отличный от IP трафик, например сетевые протоколы IPX, AppleTalk и т.д. Этот документ иллюстрирует, как организовать передачу между разными сетями, используя протокол маршрутизации и трафик не по протоколу IP с IPSec. Этот способ использует общую инкапсуляцию маршрутов для достижения этой цели.

Предварительные условия

Требования

Прежде чем использовать эту конфигурацию, убедитесь, что выполняются следующие требования:

- Удостоверьтесь, что туннель работает перед применением криптокарт.
- Крипто-потребность списка доступа иметь GRE как протокол для разрешения: хост х . х . х . х gre разрешения access-list 101 размещает у.у.у.у х . х . х = <tunnel_source> у.у.у.у = <tunnel_destination>
- Используйте IP - адреса обратной связи для определения узлов Протокола IKE и точки начала туннеля и назначения туннеля для улучшения доступности.
- Для обсуждения возможных проблем Максимального размера передаваемого блока данных (MTU) обратитесь к [Регулировке IP MTU, TCP MSS И PMTUD на Windows и Sun Systems](#).

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного

обеспечения и оборудования:

- Версии 12.1.8 и 12.2.1 программного обеспечения Cisco IOS

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 Технические рекомендации Cisco. Условные обозначения.](#)

Настройка

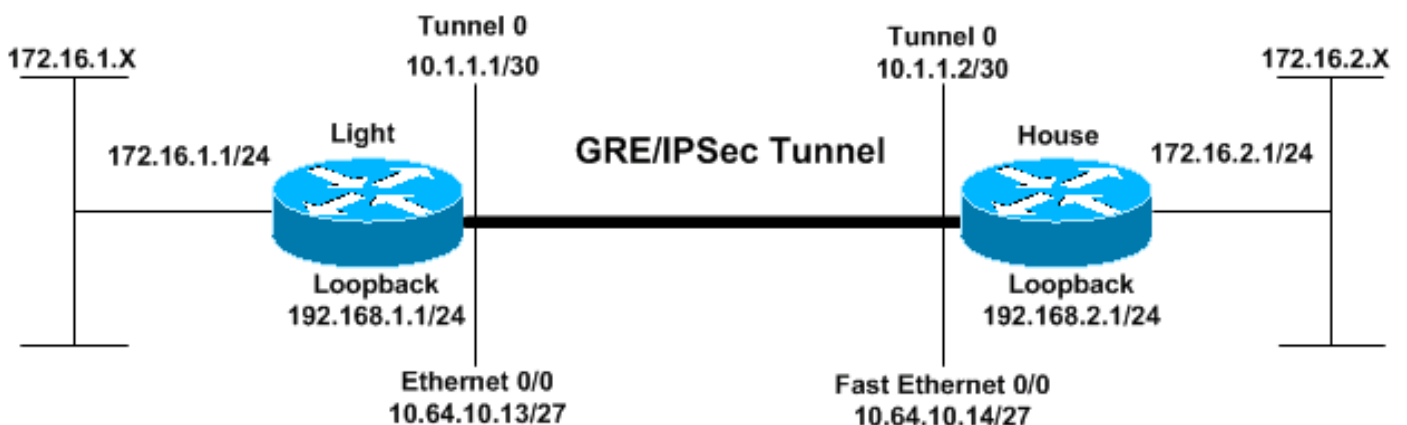
В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

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

Примечания по конфигурации IOS: С кодами Cisco IOS Software Release 12.2 (13) T и позднее (выше пронумерованные коды T-train, программное обеспечение Cisco IOS версии 12.3 и коды следующих версий) настроенный IPSec "криптокарта" только должен быть применен к физическому интерфейсу. Это больше не требуется, чтобы быть примененным на Туннельный интерфейс GRE. Наличие "криптокарты" на медосмотре и туннельном интерфейсе, когда вы используете программное обеспечение Cisco IOS версии 12.2. (13) T и коды следующих версий все еще работают. Однако это настоятельно рекомендовано для применения его только на физический интерфейс.

Схема сети

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



Конфигурации

- [Свет](#)
- [House](#)

CBET

```
Current configuration:!  
version 12.2  
no service single-slot-reload-enableservice timestamps debug uptimeservice  
timestamps log uptimeno service password-encryption!  
hostname Light!  
logging rate-limit console 10  
except errors!  
ip subnet-zero!  
no ip finger!  
no ip dhcp-client network-discovery  
ipx routing 00e0.b06a.40fc!  
!---  
IKE policies.crypto isakmp policy 25hash  
md5authentication pre-sharecrypto isakmp key cisco123  
address 192.168.2.1!  
!--- IPsec policies.crypto ipsec  
transform-set WWW esp-des esp-md5-hmac mode  
transport!  
crypto map GRE local-address Loopback0  
crypto map GRE 50 ipsec-isakmp set peer 192.168.2.1  
set transform-set WWW  
!--- What to encrypt?  
match address 101!  
call rsvp-sync!  
fax interface-type modemmta receive  
maximum-recipients 0!  
interface Loopback0  
ip address 192.168.1.1 255.255.255.0!  
interface Tunnel0  
ip address 10.1.1.1 255.255.255.252  
ip mtu 1440  
ipx network CC  
tunnel source Loopback0  
tunnel destination 192.168.2.1  
crypto map GRE!  
interface FastEthernet0/0  
ip address 10.64.10.13 255.255.255.224  
no ip route-cacheno ip mroute-cached  
duplex autospeed auto  
crypto map GRE!  
interface FastEthernet0/1  
ip address 172.16.1.1 255.255.255.0  
duplex autospeed auto  
ipx network AA! router eigrp 10  
network 10.1.1.0 0.0.0.3  
network 172.16.1.0 0.0.0.255  
network 192.168.1.0 no auto-summary  
no eigrp log-neighbor-changes!  
ip kerberos source-interface any  
ip classless  
ip route 192.168.2.0 255.255.255.0 10.64.10.14  
ip http server!  
!--- What to encrypt?  
access-list 101 permit gre host 192.168.1.1 host 192.168.2.1!  
dial-peer cor custom!  
line con 0  
transport input nonline aux 0  
line vty 0 4  
login!  
end  
Light#
```

House

```
Current configuration:  
version 12.1  
service timestamps debug uptimeservice timestamps log uptimeno service  
password-encryption!  
hostname House!  
ip subnet-zero!  
ipx routing 00e0.b06a.4114!  
!--- IKE policies.crypto isakmp policy 25hash  
md5authentication pre-sharecrypto isakmp key cisco123  
address 192.168.1.1 !  
!--- IPsec policies.crypto ipsec transform-set WWW esp-des esp-md5-hmac  
mode transport!  
crypto map GRE local-address Loopback0  
crypto map GRE 50 ipsec-isakmp set peer 192.168.1.1  
set transform-set WWW  
!--- What to encrypt?  
match address 101!  
interface Loopback0  
ip address 192.168.2.1 255.255.255.0!  
interface Tunnel0  
ip address 10.1.1.2 255.255.255.252  
ip mtu 1440  
ipx network CC  
tunnel source Loopback0  
tunnel destination 192.168.1.1  
crypto map GRE!  
interface FastEthernet0/0  
ip address 10.64.10.14 255.255.255.224  
no ip route-cacheno ip mroute-cached  
duplex autospeed auto  
crypto map GRE!  
interface FastEthernet0/1  
ip address 172.16.2.1 255.255.255.0  
duplex autospeed auto  
ipx network BB!  
interface FastEthernet4/0  
no ip address  
shutdown  
duplex autospeed auto!  
router eigrp 10  
network 10.1.1.0 0.0.0.3  
network 172.16.2.0 0.0.0.255  
network 192.168.2.0 no auto-summary  
no eigrp log-neighbor-changes!  
ip classless  
ip route 192.168.1.0 255.255.255.0 10.64.10.13  
ip http server!  
!--- What to encrypt?  
access-list 101 permit gre host 192.168.2.1 host 192.168.1.1!  
line con 0  
line aux 0  
line vty 0 4  
login!  
end  
House#
```

Проверка

В данном разделе содержатся сведения о проверке работы конфигурации.

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

- **show crypto engine connections active** в Ъ отображение зашифрованных и дешифрованных пакетов между узлами IPsec.
- команда **show crypto isakmp sa** отображает сопоставления безопасности (SA), соответствующие первому этапу.
- **show crypto ipsec sa** - Отображение набора обеспечения мер безопасности фазы 2.
- **show ipx route [network] [default] [detailed]?** Показывает содержание таблицы маршрутизации IPX.

ВЫХОДНЫЕ ДАННЫЕ КОМАНДЫ show с туннелями вверх

```
Light#show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area      N1 - OSPF NSSA external
type 1, N2 - OSPF NSSA external type 2      E1 - OSPF external type 1, E2 - OSPF external type
2, E - EGP      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR      P - periodic downloaded static
routeGateway of last resort is not set      172.16.0.0/24 is subnetted, 2 subnetsC
172.16.1.0 is directly connected, FastEthernet0/1D      172.16.2.0 [90/297246976] via 10.1.1.2,
00:00:31, Tunnel0      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masksC      10.1.1.0/30 is
directly connected, Tunnel0C      10.64.10.0/27 is directly connected, FastEthernet0/0C
192.168.1.0/24 is directly connected, Loopback0S      192.168.2.0/24 [1/0] via
10.64.10.14Light#ping      Protocol [ip]: Target IP address: 172.16.2.1Repeat count [5]:
Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: ySource address or
interface: 172.16.1.1Type of service [0]: Set DF bit in IP header? [no]: Validate reply data?
[no]: Data pattern [0xABCD]: Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of
sizes [n]: Type escape sequence to abort.Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout
is 2 seconds:!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4
msLight#House#show ip routeCodes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area      N1 - OSPF NSSA
external type 1, N2 - OSPF NSSA external type 2      E1 - OSPF external type 1, E2 - OSPF
external type 2, E - EGP      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area      * - candidate default, U - per-user static route, o - ODR      P - periodic
downloaded static routeGateway of last resort is not set      172.16.0.0/24 is subnetted, 2
subnetsD      172.16.1.0 [90/297246976] via 10.1.1.1, 00:00:36, Tunnel0C      172.16.2.0 is
directly connected, FastEthernet0/1      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masksC
10.1.1.0/30 is directly connected, Tunnel0C      10.64.10.0/27 is directly connected,
FastEthernet0/0S      192.168.1.0/24 [1/0] via 10.64.10.13C      192.168.2.0/24 is directly
connected, Loopback0House#ping Protocol [ip]: Target IP address: 172.16.1.1Repeat count [5]:
Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: ySource address or
interface: 172.16.2.1Type of service [0]: Set DF bit in IP header? [no]: Validate reply data?
[no]: Data pattern [0xABCD]: Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of
sizes [n]: Type escape sequence to abort.Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout
is 2 seconds:!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 msLight#show
ipx routeCodes: C - Connected primary network,      c - Connected secondary network      S -
Static, F - Floating static, L - Local (internal), W - IPXWAN      R - RIP, E - EIGRP, N -
NLSP, X - External, A - Aggregate      s - seconds, u - uses, U - Per-user static3 Total IPX
routes. Up to 1 parallel paths and 16 hops allowed.No default route known.C      AA (NOVELL-
ETHER), Fa0/1C      CC (TUNNEL),      Tu0R      BB [151/01] via
CC.00e0.b06a.4114,      17s, Tu0House#show ipx routeCodes: C - Connected primary network,      c -
```

```

Connected secondary network      S - Static, F - Floating static, L - Local (internal), W -
IPXWAN      R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate      s - seconds, u -
uses, U - Per-user static3 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.No
default route known.C      BB (NOVELL-ETHER), Fa0/1C      CC (TUNNEL),      Tu0R
AA [151/01] via      CC.00e0.b06a.40fc, 59s, Tu0Light#ping ipx BB.0004.9af2.8261Type escape
sequence to abort.Sending 5, 100-byte IPX Novell Echoes to BB.0004.9af2.8261, timeout is 2
second:!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 msHouse#ping ipx
AA.0004.9af2.8181 Type escape sequence to abort.Sending 5, 100-byte IPX Novell Echoes to
AA.0004.9af2.8181, timeout is 2 second:!!!!Success rate is 100 percent (5/5), round-trip
min/avg/max = 1/2/4 msLight#show crypto isa sa      dst      src      state      conn-
id      slot192.168.2.1      192.168.1.1      QM_IDLE      1      0192.168.1.1      192.168.2.1
QM_IDLE      2      0House#show crypto isa sa      dst      src      state
conn-id      slot192.168.1.1      192.168.2.1      QM_IDLE      1      0192.168.2.1
192.168.1.1      QM_IDLE      2      0Light#show crypto engine connections active ID
Interface      IP-Address      State Algorithm      Encrypt Decrypt 1 <none>
<none>      set      HMAC_MD5+DES_56_CB      0      0 2 <none>      <none>
set      HMAC_MD5+DES_56_CB      0      02000 FastEthernet0/0 10.64.10.13      set
HMAC_MD5+DES_56_CB      0      1612001 FastEthernet0/0 10.64.10.13      set
HMAC_MD5+DES_56_CB      161      02002 FastEthernet0/0 10.64.10.13      set
HMAC_MD5+DES_56_CB      0      02003 FastEthernet0/0 10.64.10.13      set
HMAC_MD5+DES_56_CB      0      02004 FastEthernet0/0 10.64.10.13      set
HMAC_MD5+DES_56_CB      0      02005 FastEthernet0/0 10.64.10.13      set
HMAC_MD5+DES_56_CB      0      0House#show crypto engine connections active ID Interface
IP-Address      State Algorithm      Encrypt Decrypt 1 <none>      <none>
set      HMAC_MD5+DES_56_CB      0      0 2 <none>      <none>      set
HMAC_MD5+DES_56_CB      0      02000 FastEthernet0/0 10.64.10.14      set
HMAC_MD5+DES_56_CB      0      1592001 FastEthernet0/0 10.64.10.14      set
HMAC_MD5+DES_56_CB      159      02002 FastEthernet0/0 10.64.10.14      set
HMAC_MD5+DES_56_CB      0      02003 FastEthernet0/0 10.64.10.14      set
HMAC_MD5+DES_56_CB      0      02004 FastEthernet0/0 10.64.10.14      set
HMAC_MD5+DES_56_CB      0      02005 FastEthernet0/0 10.64.10.14      set
HMAC_MD5+DES_56_CB      0      0House#show crypto ipsec sa detail interface: Tunnel0
Crypto map tag: GRE, local addr. 192.168.2.1 local ident (addr/mask/prot/port):
(192.168.2.1/255.255.255.255/47/0) remote ident (addr/mask/prot/port):
(192.168.1.1/255.255.255.255/47/0) current_peer: 192.168.1.1 PERMIT,
flags={origin_is_acl,transport_parent,} #pkts encaps: 192, #pkts encrypt: 192, #pkts digest
192 #pkts decaps: 190, #pkts decrypt: 190, #pkts verify 190 #pkts compressed: 0, #pkts
decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#pkts no sa (send) 12, #pkts invalid sa (rcv) 0 #pkts encaps failed (send) 0, #pkts decaps
failed (rcv) 0 #pkts invalid prot (recv) 0, #pkts verify failed: 0 #pkts invalid identity
(recv) 0, #pkts invalid len (rcv) 0 #pkts replay rollover (send): 0, #pkts replay rollover
(rcv) 0 ##pkts replay failed (rcv): 0 #pkts internal err (send): 0, #pkts internal err
(recv) 0 local crypto endpt.: 192.168.2.1, remote crypto endpt.: 192.168.1.1 path mtu
1514, media mtu 1514 current outbound spi: 1FA721CA inbound esp sas: spi:
0xEE52531(249898289) transform: esp-des esp-md5-hmac , in use settings
={Transport, } slot: 0, conn id: 2000, flow_id: 1, crypto map: GRE sa timing:
remaining key lifetime (k/sec): (4607961/2797) IV size: 8 bytes replay detection
support: Y spi: 0xFEE24F3(267265267) transform: esp-des esp-md5-hmac , in use
settings ={Transport, } slot: 0, conn id: 2002, flow_id: 3, crypto map: GRE sa
timing: remaining key lifetime (k/sec): (4608000/2826) IV size: 8 bytes replay
detection support: Y spi: 0x19240817(421791767) transform: esp-des esp-md5-hmac ,
in use settings ={Transport, } slot: 0, conn id: 2004, flow_id: 5, crypto map: GRE
sa timing: remaining key lifetime (k/sec): (4608000/2759) IV size: 8 bytes replay
detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas:
spi: 0x1FA721CA(531046858) transform: esp-des esp-md5-hmac , in use settings
={Transport, } slot: 0, conn id: 2001, flow_id: 2, crypto map: GRE sa timing:
remaining key lifetime (k/sec): (4607972/2797) IV size: 8 bytes replay detection
support: Y spi: 0x12B10EB0(313593520) transform: esp-des esp-md5-hmac , in
use settings ={Transport, } slot: 0, conn id: 2003, flow_id: 4, crypto map: GRE sa
timing: remaining key lifetime (k/sec): (4608000/2826) IV size: 8 bytes replay
detection support: Y spi: 0x1A700242(443548226) transform: esp-des esp-md5-hmac ,
in use settings ={Transport, } slot: 0, conn id: 2005, flow_id: 6, crypto map: GRE
sa timing: remaining key lifetime (k/sec): (4608000/2759) IV size: 8 bytes replay
detection support: Y outbound ah sas: outbound pcp sas: local ident

```

```

(addr/mask/prot/port): (192.168.2.1/255.255.255.255/0/0)  remote ident (addr/mask/prot/port):
(192.168.1.1/255.255.255.255/0/0)  current_peer: 192.168.1.1  PERMIT,
flags={transport_parent,}  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0  #pkts decaps:
0, #pkts decrypt: 0, #pkts verify 0  #pkts compressed: 0, #pkts decompressed: 0  #pkts not
compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0  #pkts no sa (send) 0, #pkts
invalid sa (rcv) 0  #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0  #pkts invalid
prot (recv) 0, #pkts verify failed: 0  #pkts invalid identity (recv) 0, #pkts invalid len
(rcv) 0  #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0  ##pkts replay
failed (rcv): 0  #pkts internal err (send): 0, #pkts internal err (recv) 0  local crypto
endpt.: 192.168.2.1, remote crypto endpt.: 192.168.1.1  path mtu 1514, media mtu 1514
current outbound spi: 0  inbound esp sas:  inbound ah sas:  inbound pcp sas:
outbound esp sas:  outbound ah sas:  outbound pcp sas:interface: FastEthernet0/0  Crypto
map tag: GRE, local addr. 192.168.2.1  local ident (addr/mask/prot/port):
(192.168.2.1/255.255.255.255/47/0)  remote ident (addr/mask/prot/port):
(192.168.1.1/255.255.255.255/47/0)  current_peer: 192.168.1.1  PERMIT,
flags={origin_is_acl,transport_parent,}  #pkts encaps: 193, #pkts encrypt: 193, #pkts digest
193  #pkts decaps: 192, #pkts decrypt: 192, #pkts verify 192  #pkts compressed: 0, #pkts
decompressed: 0  #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#pkts no sa (send) 12, #pkts invalid sa (rcv) 0  #pkts encaps failed (send) 0, #pkts decaps
failed (rcv) 0  #pkts invalid prot (recv) 0, #pkts verify failed: 0  #pkts invalid identity
(recv) 0, #pkts invalid len (rcv) 0  #pkts replay rollover (send): 0, #pkts replay rollover
(rcv) 0  ##pkts replay failed (rcv): 0  #pkts internal err (send): 0, #pkts internal err
(recv) 0  local crypto endpt.: 192.168.2.1, remote crypto endpt.: 192.168.1.1  path mtu
1514, media mtu 1514  current outbound spi: 1FA721CA  inbound esp sas:  spi:
0xEE52531(249898289)  transform: esp-des esp-md5-hmac ,  in use settings
={Transport, }  slot: 0, conn id: 2000, flow_id: 1, crypto map: GRE  sa timing:
remaining key lifetime (k/sec): (4607961/2789)  IV size: 8 bytes  replay detection
support: Y  spi: 0xFEE24F3(267265267)  transform: esp-des esp-md5-hmac ,  in use
settings ={Transport, }  slot: 0, conn id: 2002, flow_id: 3, crypto map: GRE  sa
timing: remaining key lifetime (k/sec): (4608000/2817)  IV size: 8 bytes  replay
detection support: Y  spi: 0x19240817(421791767)  transform: esp-des esp-md5-hmac ,
in use settings ={Transport, }  slot: 0, conn id: 2004, flow_id: 5, crypto map: GRE
sa timing: remaining key lifetime (k/sec): (4608000/2750)  IV size: 8 bytes  replay
detection support: Y  inbound ah sas:  inbound pcp sas:  outbound esp sas:  spi:
0x1FA721CA(531046858)  transform: esp-des esp-md5-hmac ,  in use settings
={Transport, }  slot: 0, conn id: 2001, flow_id: 2, crypto map: GRE  sa timing:
remaining key lifetime (k/sec): (4607972/2789)  IV size: 8 bytes  replay detection
support: Y  spi: 0x12B10EB0(313593520)  transform: esp-des esp-md5-hmac ,  in
use settings ={Transport, }  slot: 0, conn id: 2003, flow_id: 4, crypto map: GRE  sa
timing: remaining key lifetime (k/sec): (4608000/2817)  IV size: 8 bytes  replay
detection support: Y  spi: 0x1A700242(443548226)  transform: esp-des esp-md5-hmac ,
in use settings ={Transport, }  slot: 0, conn id: 2005, flow_id: 6, crypto map: GRE
sa timing: remaining key lifetime (k/sec): (4608000/2750)  IV size: 8 bytes  replay
detection support: Y  outbound ah sas:  outbound pcp sas:  local ident
(addr/mask/prot/port): (192.168.2.1/255.255.255.255/0/0)  remote ident (addr/mask/prot/port):
(192.168.1.1/255.255.255.255/0/0)  current_peer: 192.168.1.1  PERMIT,
flags={transport_parent,}  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0  #pkts decaps:
0, #pkts decrypt: 0, #pkts verify 0  #pkts compressed: 0, #pkts decompressed: 0  #pkts not
compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0  #pkts no sa (send) 0, #pkts
invalid sa (rcv) 0  #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0  #pkts invalid
prot (recv) 0, #pkts verify failed: 0  #pkts invalid identity (recv) 0, #pkts invalid len
(rcv) 0  #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0  ##pkts replay
failed (rcv): 0  #pkts internal err (send): 0, #pkts internal err (recv) 0  local crypto
endpt.: 192.168.2.1, remote crypto endpt.: 192.168.1.1  path mtu 1514, media mtu 1514
current outbound spi: 0  inbound esp sas:  inbound ah sas:  inbound pcp sas:
outbound esp sas:  outbound ah sas:  outbound pcp sas:

```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

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

Примечание:

- "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.
- *debug ip your routing protocol?* Отображает информацию о транзакциях маршрутизации вашего протокола маршрутизации.
- идентификатор соединения clear crypto connection [слот | rsm | vip]? Завершает в настоящее время происходящий зашифрованный сеанс. Зашифрованные сеансы обычно завершаются когда времена сеанса. Для получения значения connection-id используйте команду show crypto cisco connections.
- clear crypto isakmp —Очищает связи безопасности в фазе 1.
- clear crypto sa – удаляет связи безопасности, соответствующие второму этапу.

[Дополнительные сведения](#)

- [Страница поддержки IPsec](#)
- [Введение в шифрование IPsec](#)
- [Настройка параметров сетевой безопасности IPsec Network Security](#)
- [Настройка протокола защищенного обмена ключами IKE](#)
- [Средство поиска команд только для зарегистрированных пользователей\)](#)
- [Техническая поддержка - Cisco Systems](#)