

# Пример конфигурации VPN ASA с перекрывающимися сценариями

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Общие сведения](#)

[Трансляция на обеих Оконечных точках VPN](#)

[ASA 1](#)

[Создайте необходимые объекты для подсетей в использовании](#)

[Настройте выражение NAT](#)

[Настройте крипто-ACL с транслированными подсетями](#)

[Соответствующее крипто - настройка](#)

[ASA 2](#)

[Создайте необходимые объекты для подсетей в использовании](#)

[Настройте выражение NAT](#)

[Настройте крипто-ACL с транслированными подсетями](#)

[Соответствующее крипто - настройка](#)

[Проверка](#)

[ASA 1](#)

[ASA 2](#)

[Топология звезды с перекрывающимися спицами](#)

[ASA1](#)

[Создайте необходимые объекты для подсетей в использовании](#)

[Создайте ручные операторы для перевода:](#)

[Настройте крипто-ACL с транслированными подсетями](#)

[Соответствующее крипто - настройка](#)

[ASA2 \(SPOKE1\)](#)

[Настройте крипто-ACL, переходящий к транслированной подсети \(10.20.20.0 / 24\)](#)

[Соответствующее крипто - настройка](#)

[R1 \(SPOKE2\)](#)

[Настройте крипто-ACL, переходящий к транслированной подсети \(10.30.30.0 / 24\)](#)

[Соответствующее крипто - настройка](#)

[Проверка](#)

[ASA 1](#)

[ASA2 \(SPOKE1\)](#)

[R1 \(SPOKE2\)](#)

[Устранение неполадок](#)

[Очистка ассоциаций безопасности](#)

[Конфигурация NAT анализа](#)

[Команды для устранения неполадок](#)

[Дополнительные сведения](#)

## Введение

Этот документ описывает шаги, используемые для перевода трафика VPN, который перемещается по LAN-LAN (L2L) Туннель IPSec между двумя Устройствами адаптивной защиты (ASA) в перекрывающихся сценариях и также Преобразовании адресов портов (PAT) интернет-трафик.

## Предварительные условия

### Требования

Удостоверьтесь, что вы настроили устройство адаптивной защиты Cisco с IP-адресами на интерфейсах и имеете основное подключение перед переходом этот пример конфигурации.

### Используемые компоненты

Сведения в этом документе основываются на этой версии программного обеспечения:

- Версия программного обеспечения 8.3 Устройства адаптивной защиты Cisco и позже.

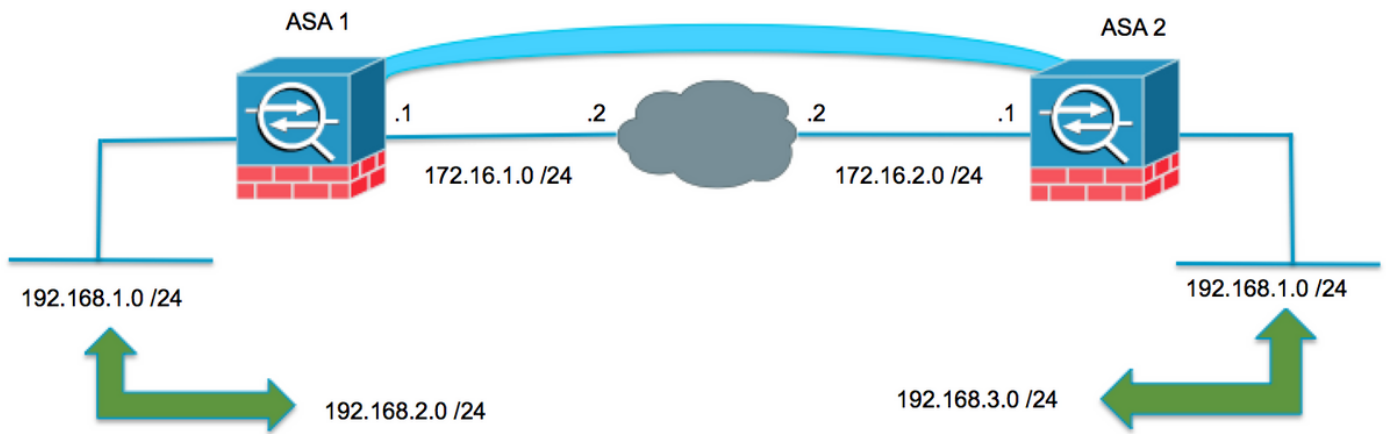
Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

## Общие сведения

Каждое устройство имеет частное, защищенную сеть позади него. В перекрывающихся сценариях никогда не происходит связь через VPN, потому что пакеты никогда не оставляют локальную подсеть, так как трафик передается IP-адресу той же подсети. Это может быть выполнено с Технологией NAT, как объяснено в следующих разделах.

## Трансляция на обеих Оконечных точках VPN

Когда наложение защищенных сетей VPN и конфигурация могут модифицироваться на обеих оконечных точках; NAT может использоваться для перевода локальной сети в другую подсеть, переходя к удаленной транслированной подсети.



## ASA 1

### Создайте необходимые объекты для подсетей в использовании

```
object network LOCAL
  subnet 192.168.1.0 255.255.255.0
object network XLATED-LOCAL
  subnet 192.168.2.0 255.255.255.0
object network XLATED-REMOTE
  subnet 192.168.3.0 255.255.255.0
```

### Настройте выражение NAT

Создайте ручной оператор для перевода локальной сети в другую подсеть только, переходя к удаленной подсети (также преобразованный)

```
nat (inside,outside) source static LOCAL XLATED-LOCAL destination static XLATED-REMOTE XLATED-REMOTE
```

### Настройте крипто-ACL с транслированными подсетями

```
access-list VPN-TRAFFIC extended permit ip object XLATED-LOCAL object XLATED-REMOTE
```

### Соответствующее крипто - настройка

```
crypto ikev1 enable outside
crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400
```

```
crypto ipsec ikev1 transform-set AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-TRAFFIC
crypto map MYMAP 10 set peer 172.16.2.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside
```

```
tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK
```

## ASA 2

## Создайте необходимые объекты для подсетей в использовании

```
object network LOCAL
  subnet 192.168.1.0 255.255.255.0
object network XLATED-LOCAL
  subnet 192.168.3.0 255.255.255.0
object network XLATED-REMOTE
  subnet 192.168.2.0 255.255.255.0
```

## Настройте выражение NAT

Создайте ручной оператор для перевода локальной сети в другую подсеть только, переходя к удаленной подсети (также преобразованный)

```
nat (inside,outside) source static LOCAL XLATED-LOCAL destination static XLATED-REMOTE XLATED-REMOTE
```

## Настройте крипто-ACL с транслированными подсетями

```
access-list VPN-TRAFFIC extended permit ip object XLATED-LOCAL object XLATED-REMOTE Rele
```

## Соответствующее крипто - настройка

```
crypto ikev1 enable outside
crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400
```

```
crypto ipsec ikev1 transform-set AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-TRAFFIC
crypto map MYMAP 10 set peer 172.16.1.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside
```

```
tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK
```

## Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

## ASA 1

```
ASA1(config)# sh cry isa sa
```

```
IKEv1 SAs:
```

```
  Active SA: 1
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
```

```
1  IKE Peer: 172.16.2.1
   Type    : L2L                Role    : initiator
   Rekey   : no                 State   : MM_ACTIVE
```

```
There are no IKEv2 SAsASA1(config)# show crypto ipsec sa
```

```

interface: outside
  Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.1.1

  access-list VPN-TRAFFIC extended permit ip 192.168.2.0 255.255.255.0 192.168.3.0
  255.255.255.0
  local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
  current_peer: 172.16.2.1

  #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
  #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #TFC rcvd: 0, #TFC sent: 0
  #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
  #send errors: 0, #recv errors: 0

  local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0
  path mtu 1500, ipsec overhead 74(44), media mtu 1500
  PMTU time remaining (sec): 0, DF policy: copy-df
  ICMP error validation: disabled, TFC packets: disabled
  current outbound spi: F90C149A
  current inbound spi : 6CE656C7

inbound esp sas:
  spi: 0x6CE656C7 (1827034823)
  transform: esp-aes-256 esp-sha-hmac no compression
  in use settings = {L2L, Tunnel, IKEv1, }
  slot: 0, conn_id: 16384, crypto-map: MYMAP
  sa timing: remaining key lifetime (kB/sec): (3914999/28768)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x000003FF

outbound esp sas:
  spi: 0xF90C149A (4178318490)
  transform: esp-aes-256 esp-sha-hmac no compression
  in use settings = {L2L, Tunnel, IKEv1, }
  slot: 0, conn_id: 16384, crypto-map: MYMAP
  sa timing: remaining key lifetime (kB/sec): (3914999/28768)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001

```

## ASA 2

```
ASA2(config)# show crypto isa sa
```

```
IKEv1 SAs:
```

```

Active SA: 1
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 172.16.1.1
   Type    : L2L                Role    : responder
   Rekey   : no                 State   : MM_ACTIVE

```

```

There are no IKEv2 SAs
ASA2(config)# show crypto ipsec sa
interface: outside

```

Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.2.1

```
access-list VPN-TRAFFIC extended permit ip 192.168.3.0 255.255.255.0 192.168.2.0
255.255.255.0
```

```
local ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer: 172.16.1.1
```

```
#pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 6CE656C7
current inbound spi : F90C149A
```

inbound esp sas:

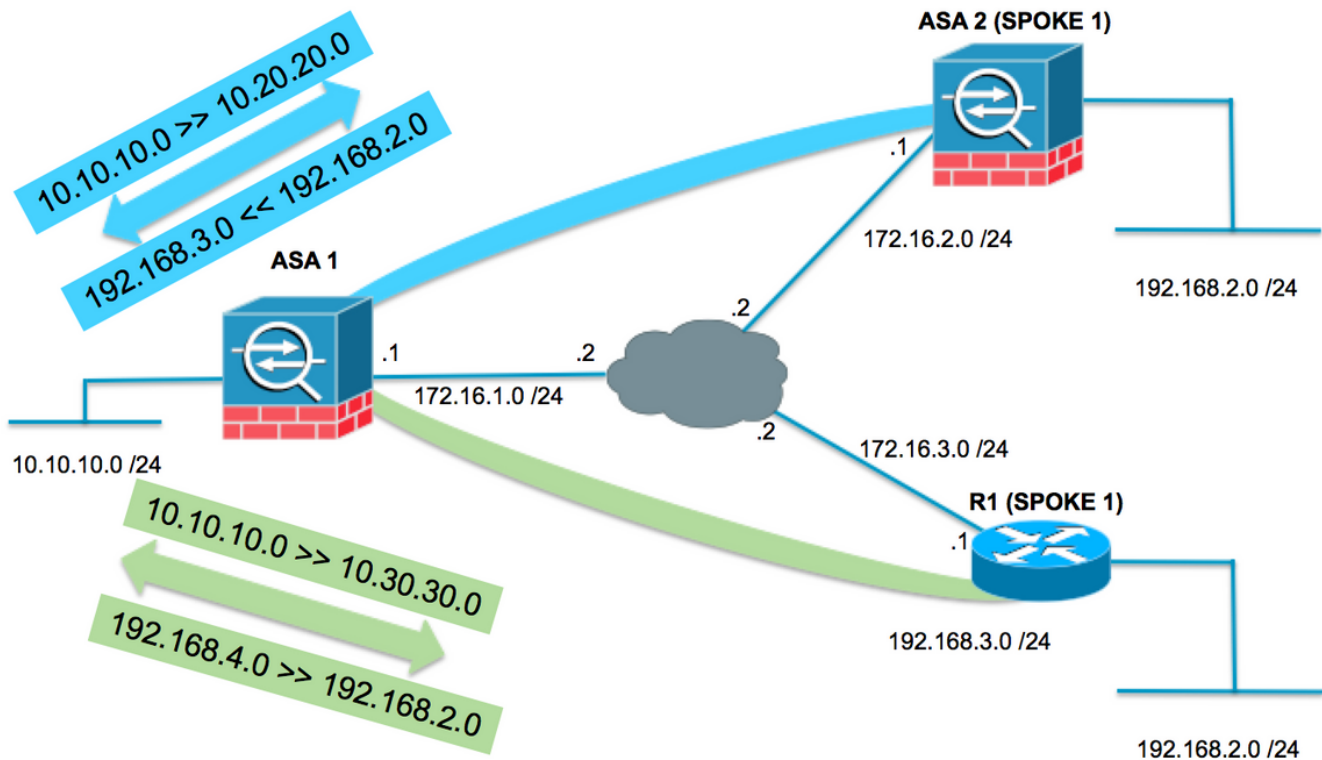
```
spi: 0xF90C149A (4178318490)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 12288, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (4373999/28684)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x000003FF
```

outbound esp sas:

```
spi: 0x6CE656C7 (1827034823)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 12288, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (4373999/28683)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

## Топология звезды с перекрывающимися спицами

В нумерующей страницы топологии оба луча имеют ту же подсеть, которая должна быть защищена по Туннелю IPsec к Концентратору. Для упрощения управления на лучах, конфигурация NAT для обхода перекрывающейся проблемы выполнена на Концентраторе только.



## ASA1

### Создайте необходимые объекты для подсетей в использовании

```
object network LOCAL
  subnet 10.10.10.0 255.255.255.0
object network SPOKES-NETWORK
  subnet 192.168.2.0 255.255.255.0
object network LOCAL-XLATE-TO-SPOKE1
  subnet 10.20.20.0 255.255.255.0
object network LOCAL-XLATE-TO-SPOKE2
  subnet 10.30.30.0 255.255.255.0
object network REMOTE-XLATE-SPOKE1
  subnet 192.168.3.0 255.255.255.0
object network REMOTE-XLATE-SPOKE2
  subnet 192.168.4.0 255.255.255.0
```

### Создайте ручные операторы для перевода:

- Локальная сеть 10.10.10.0 / 24 к 10.20.20.0 / 24, переходя к SPOKE1 (192.168.2.0 / 24).
- Сеть SPOKE1 192.168.2.0 / 24 к 192.168.3.0 / 24, доходя до 10.20.20.0 / 24.
- Локальная сеть 10.10.10.0 / 24 к 10.30.30.0 / 24, переходя к SPOKE3 (192.168.2.0 / 24).
- Сеть SPOKE2 192.168.2.0 / 24 к 192.168.4.0 / 24, доходя до 10.30.30.0 / 24.

```
nat (inside,outside) source static LOCAL LOCAL-XLATE-SPOKE1 destination static REMOTE-XLATE-SPOKE1 SPOKES-NETWORK
nat (inside,outside) source static LOCAL LOCAL-XLATE-SPOKE2 destination static REMOTE-XLATE-SPOKE2 SPOKES-NETWORK
```

### Настройте крипто-ACL с транслированными подсетями

```
access-list VPN-to-SPOKE1 extended permit ip object LOCAL-XLATE-SPOKE1 object SPOKES-NETWORKS
```

```
access-list VPN-to-SPOKE2 extended permit ip object LOCAL-XLATE-SPOKE2 object SPOKES-NETWORKS
```

## Соответствующее крипто - настройка

```
crypto ikev1 enable outside
crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400

crypto ipsec ikev1 transform-set AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-to-SPOKE1
crypto map MYMAP 10 set peer 172.16.2.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP 20 match address VPN-to-SPOKE2
crypto map MYMAP 20 set peer 172.16.3.1
crypto map MYMAP 20 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside

tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK
tunnel-group 172.16.3.1 type ipsec-l2l
tunnel-group 172.16.3.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK
```

## ASA2 (SPOKE1)

### Настройте крипто-ACL, переходящий к транслированной подсети (10.20.20.0 / 24)

```
access-list VPN-TRAFFIC extended permit ip 192.168.2.0 255.255.255.0 10.20.20.0 255.255.255.0
```

## Соответствующее крипто - настройка

```
crypto ikev1 enable outside
crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400

crypto ipsec ikev1 transform-set esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-TRAFFIC
crypto map MYMAP 10 set peer 172.16.1.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside

tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK
```

## R1 (SPOKE2)

### Настройте крипто-ACL, переходящий к транслированной подсети (10.30.30.0 / 24)

```
ip access-list extended VPN-TRAFFIC
  permit ip 192.168.2.0 0.0.0.255 10.30.30.0 0.0.0.255
```



## Соответствующее крипто - настройка

```
crypto isakmp policy 1
  encr aes 256
  authentication pre-share
  group 2

crypto isakmp key secure_PSK address 172.16.1.1

crypto ipsec transform-set AES256-SHA esp-aes 256 esp-sha-hmac
mode tunnel

crypto map MYMAP 10 ipsec-isakmp
  set peer 172.16.1.1
  set transform-set AES256-SHA
  match address VPN-TRAFFIC

interface GigabitEthernet0/1
  ip address 172.16.3.1 255.255.255.0
  duplex auto
  speed auto
  media-type rj45
  crypto map MYMAP
```

## Проверка

### ASA 1

```
ASA1(config)# show crypto isakmp sa
```

IKEv1 SAs:

```
Active SA: 2
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 2
```

```
1 IKE Peer: 172.16.3.1
  Type      : L2L           Role      : responder
  Rekey     : no           State     : MM_ACTIVE
2 IKE Peer: 172.16.2.1
  Type      : L2L           Role      : responder
  Rekey     : no           State     : MM_ACTIVE
```

```
There are no IKEv2 SAsASA1(config)# show crypto ipsec sa
```

interface: outside

```
Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.1.1
```

```
access-list VPN-to-SPOKE1 extended permit ip 10.20.20.0 255.255.255.0 192.168.2.0
255.255.255.0
```

```
local ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer: 172.16.2.1
```

```
#pkts encaps: 10, #pkts encrypt: 9, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 9, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
```

#send errors: 0, #recv errors: 0

local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0  
path mtu 1500, ipsec overhead 74(44), media mtu 1500  
PMTU time remaining (sec): 0, DF policy: copy-df  
ICMP error validation: disabled, TFC packets: disabled  
current outbound spi: 79384296  
current inbound spi : 2189BF7A

inbound esp sas:

spi: 0x2189BF7A (562675578)  
transform: esp-aes-256 esp-sha-hmac no compression  
in use settings ={L2L, Tunnel, IKEv1, }  
slot: 0, conn\_id: 12288, crypto-map: MYMAP  
sa timing: remaining key lifetime (kB/sec): (3914999/28618)  
IV size: 16 bytes  
replay detection support: Y  
Anti replay bitmap:  
0x00000000 0x000003FF

outbound esp sas:

spi: 0x79384296 (2033730198)  
transform: esp-aes-256 esp-sha-hmac no compression  
in use settings ={L2L, Tunnel, IKEv1, }  
slot: 0, conn\_id: 12288, crypto-map: MYMAP  
sa timing: remaining key lifetime (kB/sec): (3914999/28618)  
IV size: 16 bytes  
replay detection support: Y  
Anti replay bitmap:  
0x00000000 0x00000001

Crypto map tag: MYMAP, seq num: 20, local addr: 172.16.1.1

access-list VPN-to-SPOKE2 extended permit ip 10.30.30.0 255.255.255.0 192.168.2.0  
255.255.255.0

local ident (addr/mask/prot/port): (10.30.30.0/255.255.255.0/0/0)  
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)  
current\_peer: 172.16.3.1

#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10  
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10  
#pkts compressed: 0, #pkts decompressed: 0  
#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0  
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0  
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0  
#TFC rcvd: 0, #TFC sent: 0  
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0  
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.3.1/0  
path mtu 1500, ipsec overhead 74(44), media mtu 1500  
PMTU time remaining (sec): 0, DF policy: copy-df  
ICMP error validation: disabled, TFC packets: disabled  
current outbound spi: 65FDF4F5  
current inbound spi : 05B7155D

inbound esp sas:

spi: 0x05B7155D (95884637)  
transform: esp-aes-256 esp-sha-hmac no compression  
in use settings ={L2L, Tunnel, IKEv1, }  
slot: 0, conn\_id: 8192, crypto-map: MYMAP  
sa timing: remaining key lifetime (kB/sec): (3914999/2883)  
IV size: 16 bytes  
replay detection support: Y

```
Anti replay bitmap:
0x00000000 0x0000001F
outbound esp sas:
spi: 0x65FDF4F5 (1711142133)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (3914999/2883)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

## ASA2 (SPOKE1)

```
ASA2(config)# show crypto isakmp sa
```

```
IKEv1 SAs:
```

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
```

```
1 IKE Peer: 172.16.1.1
Type      : L2L           Role      : initiator
Rekey     : no           State     : MM_ACTIVE
```

```
There are no IKEv2 SAs
ASA2(config)# show crypto ipsec sa
interface: outside
```

```
Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.2.1

access-list VPN-TRAFFIC extended permit ip 192.168.2.0 255.255.255.0 10.20.20.0
255.255.255.0
local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
current_peer: 172.16.1.1

#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 2189BF7A
current inbound spi : 79384296
```

```
inbound esp sas:
```

```
spi: 0x79384296 (2033730198)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (4373999/28494)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
```

```
0x00000000 0x000003FF
outbound esp sas:
spi: 0x2189BF7A (562675578)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (4373999/28494)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

## R1 (SPOKE2)

```
R3lshow crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
```

dst	src	state	conn-id	status
172.16.1.1	172.16.3.1	QM_IDLE	1001	ACTIVE

```
IPv6 Crypto ISAKMP SARl#show crypto ipsec sa
```

```
interface: GigabitEthernet0/1
```

```
Crypto map tag: MYMAP, local addr 172.16.3.1
```

```
protected vrf: (none)
```

```
local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
```

```
remote ident (addr/mask/prot/port): (10.30.30.0/255.255.255.0/0/0)
```

```
current_peer 172.16.1.1 port 500
```

```
PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
```

```
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 172.16.3.1, remote crypto endpt.: 172.16.1.1
```

```
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
```

```
current outbound spi: 0x5B7155D(95884637)
```

```
PFS (Y/N): N, DH group: none
```

```
inbound esp sas:
```

```
spi: 0x65FDF4F5(1711142133)
```

```
transform: esp-256-aes esp-sha-hmac ,
```

```
in use settings ={Tunnel, }
```

```
conn id: 1, flow_id: SW:1, sibling_flags 80004040, crypto map: MYMAP
```

```
sa timing: remaining key lifetime (k/sec): (4188495/2652)
```

```
IV size: 16 bytes
```

```
replay detection support: Y
```

```
Status: ACTIVE(ACTIVE)
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
```

```
spi: 0x5B7155D(95884637)
```

```
transform: esp-256-aes esp-sha-hmac ,
```

```
in use settings ={Tunnel, }
```

```
conn id: 2, flow_id: SW:2, sibling_flags 80004040, crypto map: MYMAP
```

```
sa timing: remaining key lifetime (k/sec): (4188495/2652)
```

```
IV size: 16 bytes
```

```
replay detection support: Y
```

```
Status: ACTIVE(ACTIVE)
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

## Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

### Очистка ассоциаций безопасности

Когда вы устраняете неполадки, убедитесь очистить существующие SA после внесения изменения. В привилегированном режиме PIX используйте следующие команды:

- `clear [crypto] ipsec sa`— удаляет все активные ассоциации безопасности IPSec.
- `clear crypto isakmp sa`— удаляет активные ассоциации безопасности IKE.

### Конфигурация NAT анализа

- **покажите, что туземная подробность** - Отображает конфигурацию NAT с объектом (объектами) / расширенный object-group

### Команды для устранения неполадок

Этот раздел позволяет убедиться, что конфигурация работает правильно.

[Cisco CLI Анализатор \(только зарегистрированные клиенты\)](#) поддерживает некоторые команды `show`. Используйте Cisco CLI Анализатор для просматривания аналитику выходных данных команды `show`.

**Примечание:** См. [раздел Важные сведения о командах отладки](#) и [Устранение проблем системы безопасности IP - Понимание и Использование команд отладки](#) перед использованием команд отладки.

- `debug crypto ipsec` – отображает согласования IPSec на Этапе 2.
- `debug crypto isakmp` – отображает согласования ISAKMP на 1-м этапе.

## Дополнительные сведения

- [Руководство конфигурации NAT](#)
- [Устранение наиболее распространенных проблем удаленных VPN-подключений и VPN-туннелей LAN — LAN на базе протокола IPSec](#)
- [Согласование IPsec/Протоколы IKE](#)
- [Cisco Systems – техническая поддержка и документация](#)