

# Exemplo de configuração de VPN ASA com cenários sobrepostos

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Tradução em ambos os endpoints VPN](#)

[ASA 1](#)

[Criar os objetos necessários para as sub-redes em uso](#)

[Configurar a instrução NAT](#)

[Configurar a ACL de criptografia com as sub-redes traduzidas](#)

[Configuração de criptografia relevante](#)

[ASA 2](#)

[Criar os objetos necessários para as sub-redes em uso](#)

[Configurar a instrução NAT](#)

[Configurar a ACL de criptografia com as sub-redes traduzidas](#)

[Configuração de criptografia relevante](#)

[Verificar](#)

[ASA 1](#)

[ASA 2](#)

[Topologia de hub e spoke com spokes sobrepostos](#)

[ASA1](#)

[Criar os objetos necessários para as sub-redes em uso](#)

[Criar instruções manuais para traduzir:](#)

[Configurar a ACL de criptografia com as sub-redes traduzidas](#)

[Configuração de criptografia relevante](#)

[ASA2 \(SPOKE1\)](#)

[Configure a ACL de criptografia indo para a sub-rede convertida \(10.20.20.0 /24\)](#)

[Configuração de criptografia relevante](#)

[R1 \(SPOKE2\)](#)

[Configure a ACL de criptografia indo para a sub-rede convertida \(10.30.30.0 /24\)](#)

[Configuração de criptografia relevante](#)

[Verificar](#)

[ASA 1](#)

[ASA2 \(SPOKE1\)](#)

[R1 \(SPOKE2\)](#)

[Troubleshoot](#)

[Cancele associações de segurança](#)

[Revisar a configuração do NAT](#)

## Introduction

Este documento descreve as etapas usadas para converter o tráfego VPN que viaja através de um túnel IPsec de LAN para LAN (L2L) entre dois Adaptive Security Appliances (ASA) em cenários sobrepostos e também a Port Address Translation (PAT), o tráfego da Internet.

## Prerequisites

### Requirements

Certifique-se de ter configurado o Cisco Adaptive Security Appliance com endereços IP nas interfaces e ter conectividade básica antes de prosseguir com este exemplo de configuração.

### Componentes Utilizados

As informações aqui são baseadas nesta versão de software:

- Cisco Adaptive Security Appliance Software versão 8.3 e posterior.

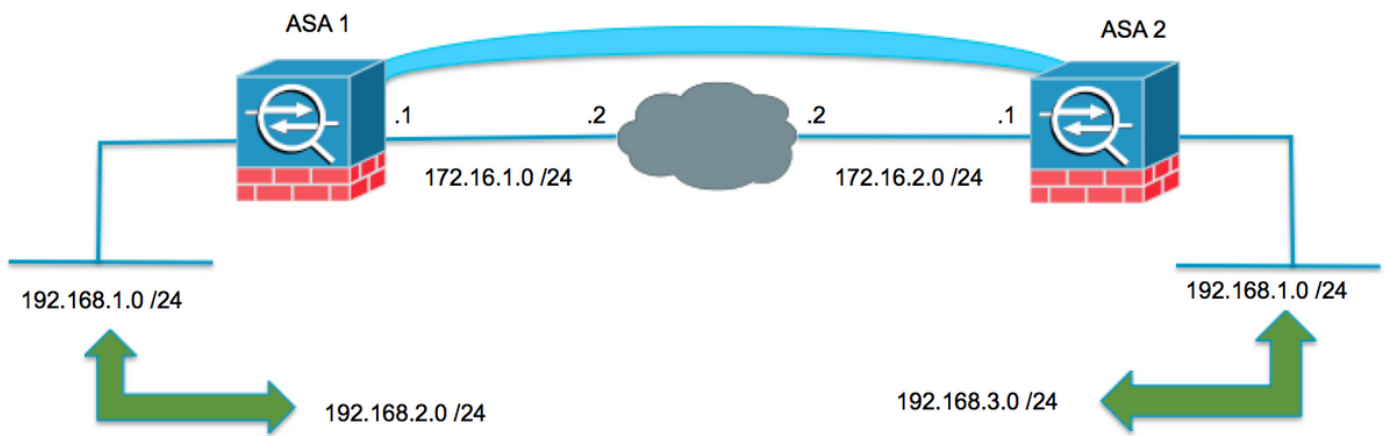
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Informações de Apoio

Cada dispositivo tem uma rede privada protegida por trás dela. Em cenários de sobreposição, a comunicação através da VPN nunca acontece porque os pacotes nunca deixam a sub-rede local, já que o tráfego é enviado para um endereço IP da mesma sub-rede. Isso pode ser realizado com a Network Address Translation (NAT), conforme explicado nas seções a seguir.

## Tradução em ambos os endpoints VPN

Quando as redes protegidas por VPN se sobrepõem e a configuração pode ser modificada em ambos os endpoints; O NAT pode ser usado para converter a rede local em uma sub-rede diferente ao ir para a sub-rede traduzida remota.



## ASA 1

Criar os objetos necessários para as sub-redes em uso

```
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
```

Configurar a instrução NAT

Crie uma instrução manual para converter a rede local em uma sub-rede diferente somente ao ir para a sub-rede remota (também traduzida)

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

Configurar a ACL de criptografia com as sub-redes traduzidas

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

Configuração de criptografia relevante

```
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

### Criar os objetos necessários para as sub-redes em uso

```
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
```

### Configurar a instrução NAT

Crie uma instrução manual para converter a rede local em uma sub-rede diferente somente ao ir para a sub-rede remota (também traduzida)

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

### Configurar a ACL de criptografia com as sub-redes traduzidas

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

### Configuração de criptografia relevante

```
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
```

## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

## 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 SAs

ASA1(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)
```

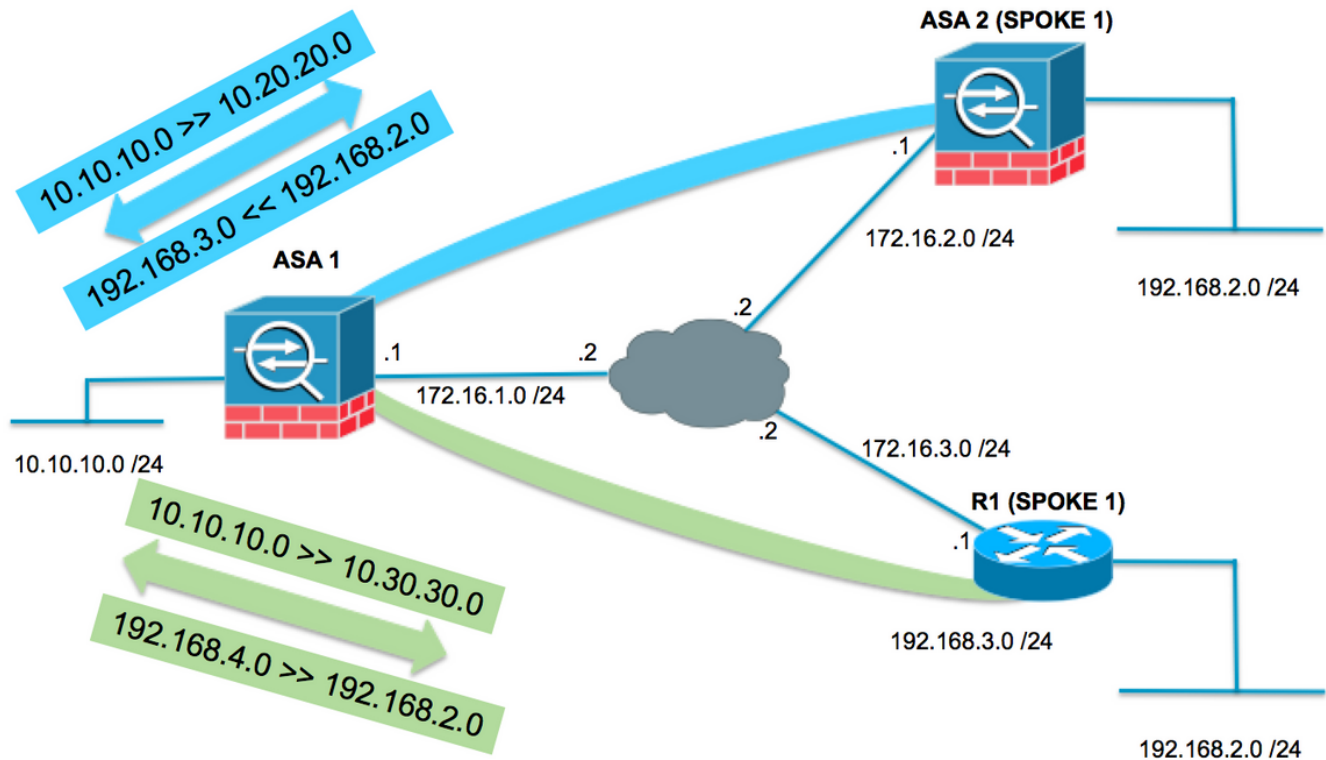
```
IV size: 16 bytes
```

```
replay detection support: Y
```

Anti replay bitmap:  
0x00000000 0x00000001

## Topologia de hub e spoke com spokes sobrepostos

Na topologia a seguir, ambos os spokes têm a mesma sub-rede que precisa ser protegida pelo túnel IPsec em direção ao Hub. Para facilitar o gerenciamento nos spokes, a configuração de NAT para solucionar o problema de sobreposição é executada somente no hub.



### ASA1

Criar os objetos necessários para as sub-redes em uso

```
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
```

Criar instruções manuais para traduzir:

- A rede local 10.10.10.0 /24 a 10.20.20.0 /24 ao ir para o SPOKE1 (192.168.2.0 /24).
- A rede SPOKE1 192.168.2.0 /24 a 192.168.3.0 /24 quando chega a 10.20.20.0 /24.
- A rede local 10.10.10.0 /24 a 10.30.30.0 /24 ao ir para o SPOKE3 (192.168.2.0 /24).
- A rede SPOKE2 192.168.2.0 /24 a 192.168.4.0 /24 quando chega a 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
```

## Configurar a ACL de criptografia com as sub-redes traduzidas

```
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
```

## Configuração de criptografia relevante

```
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)

### Configure a ACL de criptografia indo para a sub-rede convertida (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
```

## Configuração de criptografia relevante

```
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)

### Configure a ACL de criptografia indo para a sub-rede convertida (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
```

### Configuração de criptografia relevante

```
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
```

## Verificar

### 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 SAs

```
ASA1(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 0x0000003FF
```

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)

```
R31show 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 SA
```

```
R1#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:
```

## Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

### Cancele associações de segurança

Ao solucionar problemas, certifique-se de limpar as SAs existentes após fazer uma alteração. No modo privilegiado do PIX, use estes comandos:

- **clear crypto ipsec sa** - Exclui as SAs IPsec ativas.
- **clear crypto isakmp sa** - Exclui as SAs IKE ativas.

### Revisar a configuração do NAT

- **show nat detail** - Exibe a configuração de NAT com os objetos / grupos de objetos expandidos

## Comandos para Troubleshooting

Use esta seção para confirmar se a sua configuração funciona corretamente.

O Cisco CLI Analyzer (somente clientes registrados) aceita alguns comandos show. Use o Cisco CLI Analyzer para visualizar uma análise da saída do comando show.

**Note:** Consulte [Informações Importantes sobre Comandos de Depuração](#) e [Solução de Problemas de Segurança IP - Entendendo e Usando Comandos de Depuração](#) antes de usar comandos **debug**.

- **debug crypto isakmp** – Exibe as negociações IPsec da Fase 2.
- **debug crypto isakmp** – Exibe as negociações ISAKMP da Fase 1.

## Informações Relacionadas

- [Guia de configuração do NAT](#)
- [Soluções de problemas mais comuns para VPN IPsec de acesso remoto e L2L](#)
- [Negociação IPsec/Protocolos IKE](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)