

# IPsec entre dois IOS Router com exemplo de configuração das redes privadas de sobreposição

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

## [Introdução](#)

Este documento descreve como configurar o roteador do Cisco IOS em um IPsec local a local VPN com endereços de rede privada de sobreposição atrás dos gateways de VPN.

## [Pré-requisitos](#)

### [Requisitos](#)

Não existem requisitos específicos para este documento.

### [Componentes Utilizados](#)

A informação neste documento é baseada nos Cisco IOS 3640 Router que executam a versão de software 12.4.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

### [Convenções](#)

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

## [Configurar](#)

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

**Nota:** Use a [Command Lookup Tool \(somente clientes registrados\)](#) para obter mais informações sobre os comandos usados nesta seção.

## [Diagrama de Rede](#)

Este documento utiliza a seguinte configuração de rede:

**Nota:** Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços da RFC1918 que foram usados em um ambiente de laboratório.

O Private\_LAN1 e Private\_LAN2 têm uma sub-rede IP de 192.168.1.0/24. Isto simula o espaço de endereço sobreposto atrás de cada lado do túnel de IPsec.

Neste exemplo, o roteador do Site\_A executa uma tradução bidirecional de modo que as duas LAN privadas possam se comunicar sobre o túnel de IPsec. A tradução significa que o Private\_LAN1 “vê” Private\_LAN2 como 10.10.10.0/24 através do túnel de IPsec, e Private\_LAN2 “vê” o Private\_LAN1 como 10.5.5.0/24 através do túnel de IPsec.

## [Configurações](#)

Este documento utiliza as seguintes configurações:

- [Configuração de SDM do roteador do Site\\_A](#)
- [Configuração de CLI do roteador do Site\\_A](#)
- [Configuração de roteador do Site\\_B](#)

### [Configuração de SDM do roteador do Site\\_A](#)

**Nota:** Este documento supõe que o roteador está configurado com configurações básicas como a configuração da interface, etc. Refira a [configuração de roteador básico usando o SDM](#) para mais informação.

### **Configuração de NAT**

Termine estas etapas a fim usar o NAT para configurar o SDM no roteador do Site\_A:

1. Escolha **configuram > NAT > editam a configuração de NAT**, e clicam **relações designadas NAT** a fim definir confiado e interfaces não confiável como mostrado.
2. Clique em **OK**.
3. O clique **adiciona** a fim configurar do interior a tradução NAT ao sentido exterior como

mostrado.

4. Clique em **OK**.
5. Mais uma vez, o clique **adiciona** a fim configurar como mostrado a tradução NAT da parte externa ao sentido interno.
6. Clique em **OK**.**Nota:** Está aqui a configuração de CLI equivalente:

## Configuração de VPN

Termine estas etapas a fim usar o VPN para configurar o SDM no roteador do Site\_A:

1. Escolha **configuram > componentes VPN > VPN > Add >IKE > de políticas de IKE** a fim definir as políticas de IKE segundo as indicações desta imagem.
2. Clique em **OK**.**Nota:** Está aqui a configuração de CLI equivalente:
3. Escolha **configuram > componentes VPN > VPN > Add >IKE > de chaves pré-compartilhada** a fim ajustar o valor de chave pré-compartilhada com endereço IP do peer.
4. Clique em **OK**.**Nota:** Está aqui a configuração de CLI equivalente:
5. Escolha **configuram > VPN > componentes > IPsec VPN > transformam o > Add dos grupos** a fim criar um *myset* ajustado da transformação segundo as indicações desta imagem.
6. Clique em **OK**.**Nota:** Está aqui a configuração de CLI equivalente:
7. Escolha **configuram > VPN > de componentes > de IPsec > do IPsec de Rules(ACLs) VPN > Add** a fim criar um Access Control List(ACL) crypto *101*.
8. Clique em **OK**.**Nota:** Está aqui a configuração de CLI equivalente:
9. Escolha **configuram > VPN > de componentes > de IPsec > de políticas de IPsec VPN > Add em** oder para criar o *mymap* do mapa do crypto segundo as indicações desta imagem.
10. Clique em **Add**.Clique o **tab geral** e retenha as configurações padrão.Clique a aba da **informação de peer** a fim adicionar o endereço IP do peer 172.16.1.2.Clique a aba dos **grupos da transformação** a fim selecionar desejado transformam *myset* ajustado.Clique a aba da **regra do IPsec** a fim selecionar o ACL 101 crypto existente.Clique em **OK**.**Nota:** Está aqui a configuração de CLI equivalente:
11. Escolha **configuram > VPN > VPN de Site-para-Site > editam o > Add do VPN de Site-para-Site** a fim aplicar o *mymap* do crypto map ao Ethernet0/0 da relação.
12. Clique em **OK**.**Nota:** Está aqui a configuração de CLI equivalente:

## Configuração de CLI do roteador do Site\_A

### Roteador do Site\_A

```
Site_A#show running-config
*Sep 25 21:15:58.954: %SYS-5-CONFIG_I: Configured from
console by console
Building configuration...

Current configuration : 1545 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Site_A
!
boot-start-marker
boot-end-marker
!
```

```

!
no aaa new-model
!
resource policy
!
!
!
ip cef
!
!
crypto isakmp policy 10
  hash md5
  authentication pre-share
!--- Defines ISAKMP policy. crypto isakmp key 6 L2L12345
address 172.16.1.2 255.255.255.0

!--- Defines pre-shared secret used for IKE
authentication !! crypto ipsec transform-set myset esp-
des esp-md5-hmac
!--- Defines IPSec encryption and authentication
algorithms. ! crypto map mymap 10 ipsec-isakmp
  set peer 172.16.1.2
  set transform-set myset
  match address 101
!--- Defines crypto map. !!!! interface Loopback0 ip
address 192.168.1.1 255.255.255.0 ip nat inside
  ip virtual-reassembly
!
interface Ethernet0/0
  ip address 10.1.1.2 255.255.255.0
  ip nat outside
  ip virtual-reassembly
  half-duplex
  crypto map mymap
!--- Apply crypto map on the outside interface. !! !---
Output Suppressed ! ip http server no ip http secure-
server ! ip route 0.0.0.0 0.0.0.0 10.1.1.1
!
ip nat inside source static network 192.168.1.0 10.5.5.0
/24

!--- Static translation defined to translate
Private_LAN1 !--- from 192.168.1.0/24 to 10.5.5.0/24. !-
-- Note that this translation is used for both !--- VPN
and Internet traffic from Private_LAN1. !--- A routable
global IP address range, or an extra NAT !--- at the ISP
router (in front of Site_A router), is !--- required if
Private_LAN1 also needs internal access. ip nat outside
source static network 192.168.1.0 10.10.10.0 /24

!--- Static translation defined to translate
Private_LAN2 !--- from 192.168.1.0/24 to 10.10.10.0/24.
! access-list 101 permit ip 10.5.5.0 0.0.0.255
192.168.1.0 0.0.0.255

!--- Defines IPSec interesting traffic. !--- Note that
the host behind Site_A router communicates !--- to
Private_LAN2 using 10.10.10.0/24. !--- When the packets
arrive at the Site_A router, they are first !---
translated to 192.168.1.0/24 and then encrypted by
IPSec. !! control-plane !! line con 0 line aux 0 line
vty 0 4 !! end Site_A#

```

## Configuração de CLI do roteador do Site\_B

### Roteador do Site\_B

```
Site_B#show running-config
Building configuration...

Current configuration : 939 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Site_B
!
!
ip subnet-zero
!
!
crypto isakmp policy 10
  hash md5
  authentication pre-share
crypto isakmp key L2L12345 address 10.1.1.2
255.255.255.0
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap 10 ipsec-isakmp
  set peer 10.1.1.2
  set transform-set myset
  match address 101
!
!
!
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet1
 ip address 172.16.1.2 255.255.255.0
  crypto map mymap
!
!--- Output Suppressed ! ip classless ip route 0.0.0.0
0.0.0.0 172.16.1.1
ip http server
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 10.5.5.0
0.0.0.255
!
line con 0
line aux 0
line vty 0 4
!
end

Site_B#
```

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **mostre isakmp cripto sa** — Indica todas as associações de segurança atuais do Internet Key Exchange (IKE) (SA) em um par. `Site_A#show crypto isakmp sa`

```
dst          src          state          conn-id slot status
172.16.1.2   10.1.1.2     QM_IDLE       1      0 ACTIVE
```

- **mostre o detalhe cripto isakmp sa** — Indica os detalhes de todo o IKE atual SA em um par. `Site_A#show crypto isakmp sa detail`

```
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
```

```
C-id Local          Remote          I-VRF          Status Encr Hash Auth DH Lifetime
Cap.
1     10.1.1.2         172.16.1.2     ACTIVE des  md5  psk  1  23:59:42
```

```
Connection-id:Engine-id = 1:1(software)
```

- **mostre IPsec cripto sa** — Indica os ajustes usados por SA atuais. `Site_A#show crypto ipsec sa`

```
interface: Ethernet0/0
  Crypto map tag: mymap, local addr 10.1.1.2

protected vrf: (none)
local ident (addr/mask/prot/port): (10.5.5.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
current_peer 172.16.1.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 2
#pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 2
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 3, #recv errors 0

local crypto endpt.: 10.1.1.2, remote crypto endpt.: 172.16.1.2
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0x1A9CDC0A(446487562)

inbound esp sas:
  spi: 0x99C7BA58(2580003416)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2002, flow_id: SW:2, crypto map: mymap
    sa timing: remaining key lifetime (k/sec): (4478520/3336)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x1A9CDC0A(446487562)
    transform: esp-des esp-md5-hmac ,
```

```
in use settings ={Tunnel, }
conn id: 2001, flow_id: SW:1, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4478520/3335)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

outbound ah sas:

outbound pcp sas:

Site\_A#

- **mostre a IP traduções nat** — Indica a informação do slot de tradução. Site\_A#**show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
---	---	---	10.10.10.1	192.168.1.1
---	---	---	10.10.10.0	192.168.1.0
---	10.5.5.1	192.168.1.1	---	---
---	10.5.5.0	192.168.1.0	---	---

- **show ip nat statistics** — Indica a informação estática sobre a tradução. Site\_A#**show ip nat statistics**

Total active translations: 4 (2 static, 2 dynamic; 0 extended)

Outside interfaces:

Ethernet0/0

Inside interfaces:

Loopback0

Hits: 42 Misses: 2

CEF Translated packets: 13, CEF Punted packets: 0

Expired translations: 7

Dynamic mappings:

Queued Packets: 0

Site\_A#

- Termine estas etapas a fim verificar a conexão: No SDM, escolha **ferramentas > sibilo** a fim estabelecer o túnel do IPsec VPN com o IP da fonte como 192.168.1.1 e o IP de destino como 10.10.10.1. Clique o **túnel do teste** a fim verificar o túnel do IPsec VPN é estabelecido segundo as indicações desta imagem. Clique em Iniciar.

## Troubleshooting

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

```
Site_A#debug ip packet
```

```
IP packet debugging is on
```

```
Site_A#ping
```

```
Protocol [ip]:
```

```
Target IP address: 10.10.10.1
```

```
Repeat count [5]:
```

```
Datagram size [100]:
```

```
Timeout in seconds [2]:
```

```
Extended commands [n]: y
```

```
Source address or interface: 192.168.1.1
```

```
Type 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 10.10.10.1, timeout is 2 seconds:
```

```
Packet sent with a source address of 192.168.1.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/45/52 ms
Site_A#
*Sep 30 18:08:10.601: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), routed via FIB
*Sep 30 18:08:10.601: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending
*Sep 30 18:08:10.641: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB
*Sep 30 18:08:10.641: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rcvd 4
*Sep 30 18:08:10.645: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), routed via FIB
*Sep 30 18:08:10.645: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending
*Sep 30 18:08:10.685: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB
*Sep 30 18:08:10.685: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rcvd 4
*Sep 30 18:08:10.685: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), routed via FIB
*Sep 30 18:08:10.689: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending
*Sep 30 18:08:10.729: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB
*Sep 30 18:08:10.729: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rcvd 4
*Sep 30 18:08:10.729: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), routed via FIB
*Sep 30 18:08:10.729: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending
*Sep 30 18:08:10.769: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB
*Sep 30 18:08:10.769: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rcvd 4
*Sep 30 18:08:10.773: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), routed via FIB
*Sep 30 18:08:10.773: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending
*Sep 30 18:08:10.813: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB
*Sep 30 18:08:10.813: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rcvd 4
```

## [Informações Relacionadas](#)

- [Soluções de Troubleshooting Mais Comuns de VPN IPsec L2L e de Acesso Remoto](#)
- [IPsec entre ASA/PIX e Cisco VPN 3000 Concentrador com exemplo de configuração das redes privadas de sobreposição](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)