

# IPSec de LAN a LAN de sitio a sitio entre vEdge y Cisco IOS®

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Router vEdge](#)

[Cisco IOS® XE](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

## Introducción

Este documento describe la VPN de sitio a sitio IPSec IKEv1 con configuración de claves previamente compartidas en transport-vpn en vEdge entre dispositivos Cisco IOS® con Virtual Routing and Forwarding (VRF) configurado. También se puede utilizar como referencia para configurar IPSec entre el router vEdge y Amazon Virtual Port Channel (vPC) (gateway del cliente).

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- IKEv1
- Protocolos IPSec

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Router vEdge con software 18.2 o posterior
- Router Cisco IOS®-XE

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

# Configurar

## Router vEdge

```
vpn 0
!
interface ge0/1
 ip address 192.168.103.7/24
!
 no shutdown
!
interface ipsec1
 ip address 10.0.0.2/30
 tunnel-source-interface ge0/1
 tunnel-destination 192.168.103.130
 ike
  version 1
  mode main
  rekey 14400
  cipher-suite aes128-cbc-sha1
  group 2
  authentication-type
  pre-shared-key
    pre-shared-secret $8$qzBthmnUSTMs54lxyHYZXVcnyCwENxJGcxRQT09X6SI=
    local-id 192.168.103.7
    remote-id 192.168.103.130
!
!
!
 ipsec
  rekey 3600
  replay-window 512
  cipher-suite aes256-cbc-sha1
  perfect-forward-secrecy group-2
!
 no shutdown
!
vpn 1
 ip ipsec-route 0.0.0.0/0 vpn 0 interface ipsec1
```

## Cisco IOS® XE

```
crypto keyring KR vrf vedge2_vrf
 pre-shared-key address 0.0.0.0 0.0.0.0 key test
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
crypto isakmp profile IKE_PROFILE
 keyring KR
 self-identity address
 match identity address 0.0.0.0 vedge2_vrf
crypto ipsec transform-set TSET esp-aes 256 esp-sha-hmac
 mode tunnel
crypto ipsec profile IPSEC_PROFILE
 set transform-set TSET
 set pfs group2
 set isakmp-profile IKE_PROFILE
!
```

```

interface Tunnel1
 ip address 10.0.0.1 255.255.255.252
 description "*** IPSec tunnel ***"
 tunnel source 192.168.103.130
 tunnel mode ipsec ipv4
 tunnel destination 192.168.103.7
 tunnel vrf vedge2_vrf
 tunnel protection ipsec profile IPSEC_PROFILE isakmp-profile IKE_PROFILE
!
interface GigabitEthernet4
 description "*** vEdge2 ***"
 ip vrf forwarding vedge2_vrf
 ip address 192.168.103.130 255.255.255.0 secondary

```

## Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

1. Asegúrese de que la dirección remota del par sea accesible:

```

csr1000v2#ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms

```

2. Compruebe si IPsec phase1 Internet Key Exchange (IKE) está establecido en el router Cisco IOS®-XE. El estado debe ser "QM\_IDLE":

```

csr1000v2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
192.168.103.130 192.168.103.7 QM_IDLE          1004 ACTIVE

IPv6 Crypto ISAKMP SA

```

3. Verifique si la fase 2 de IPsec está establecida en el router Cisco IOS®-XE y asegúrese de que los contadores "pkts encaps" y "pkts decaps" aumenten en ambos sitios:

```

csr1000v2#show crypto ipsec sa

interface: Tunnel1
  Crypto map tag: Tunnel1-head-0, local addr 192.168.103.130

protected vrf: (none)
local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 192.168.103.7 port 4500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 12, #pkts encrypt: 12, #pkts digest: 12
  #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.: 192.168.103.130, remote crypto endpt.: 192.168.103.7
plaintext mtu 1422, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet4
current outbound spi: 0xFFB55(1047381)
PFS (Y/N): Y, DH group: group2
```

```
inbound esp sas:
spi: 0x2658A80C(643344396)
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel UDP-Encaps, }
conn id: 2023, flow_id: CSR:23, sibling_flags FFFFFFFF80004048, crypto map: Tunnel1-
head-0
sa timing: remaining key lifetime (k/sec): (4608000/1811)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
spi: 0xFFB55(1047381)
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel UDP-Encaps, }
conn id: 2024, flow_id: CSR:24, sibling_flags FFFFFFFF80004048, crypto map: Tunnel1-
head-0
sa timing: remaining key lifetime (k/sec): (4608000/1811)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

**4. Compruebe también si las sesiones de fase 1 y 2 de IPsec se han establecido en vEdge. El estado debe ser "IKE\_UP\_IPSEC\_UP".**

```
vedge4# show ipsec ike sessions
ipsec ike sessions 0 ipsec1
version          1
source-ip        192.168.103.7
source-port      4500
dest-ip          192.168.103.130
dest-port        4500
initiator-spi    8012038bc7cf1e09
responder-spi    29db204a8784ff02
cipher-suite     aes128-cbc-sha1
dh-group         "2 (MODP-1024)"
state            IKE_UP_IPSEC_UP
uptime           0:01:55:30
```

```
vedge4# show ipsec ike outbound-connections SOURCE SOURCE DEST DEST CIPHER EXT IP PORT IP PORT
SPI SUITE KEY HASH TUNNEL MTU SEQ -----
-----
```

```
192.168.103.7 4500 192.168.103.130 4500 643344396 aes256-cbc-sha1 ****ba9b 1418 no
```

**5. Verifique si los contadores tx y rx aumentan en ambas direcciones junto con los contadores coincidentes que se vieron en el router Cisco IOS®-XE.**

```
vedge4# show tunnel statistics dest-ip 192.168.103.130
```

```

TCP
TUNNEL
MSS
PROTOCOL SOURCE IP DEST IP PORT PORT IP COLOR COLOR MTU tx-pkts
tx-octets rx-pkts rx-octets ADJUST
-----
ipsec 192.168.103.7 192.168.103.130 4500 4500 - - - 1418 10
1900 11 2038 1334

```

## Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Para obtener la guía de resolución de problemas de IPsec en Cisco IOS®/IOS®-XE, consulte lo siguiente:

<https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html>

## Información Relacionada

- Más información sobre Amazon VPC "Customer Gateway":  
[https://docs.aws.amazon.com/en\\_us/vpc/latest/adminguide/Introduction.html](https://docs.aws.amazon.com/en_us/vpc/latest/adminguide/Introduction.html)
- [Soporte Técnico y Documentación - Cisco Systems](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).