

# Site-to-Site LAN to LAN IPSec Between vEdge and Cisco IOS®

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[vEdge Router](#)

[Cisco IOS®-XE](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

## Introduction

This document describes IPSec IKEv1 site-to-site VPN with pre-shared keys configuration in transport-vpn on vEdge between Cisco IOS® device with Virtual Routing and Forwarding (VRF) configured. It can also be used as a reference in order to configure IPSec between vEdge router and Amazon Virtual Port Channel (vPC) (customer gateway).

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- IKEv1
- IPSec Protocols

### Components Used

The information in this document is based on these software and hardware versions:

- vEdge Router with 18.2 Software or newer
- Cisco IOS®-XE Router

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, ensure that you understand the potential impact of any command.

# Configure

## vEdge Router

```
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

```

## Verify

Use this section in order to confirm that your configuration works properly.

### 1. Ensure that the remote address of peer is reachable:

```

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. Check if IPsec phase1 Internet Key Exchange (IKE) is established on Cisco IOS®-XE router. The state should be "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. Check if IPsec phase 2 is established on Cisco IOS®-XE router and ensure that "pkts encaps" and "kts decaps" counters increase on both sites:

```

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. Check if IPsec phase 1 and 2 sessions are established on vEdge as well. The State should be "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. Check if tx- and rx- counters increase in both directions along with the matching counters that were seen on Cisco IOS®-XE router.

```
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

This section provides information you can use in order to troubleshoot your configuration.

For IPsec troubleshooting guide on Cisco IOS®/IOS®-XE, refer to this:

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

## Related Information

- More information about 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)
- [Technical Support & Documentation - Cisco Systems](#)