

vEdge와 Cisco IOS 간의 사이트 대 사이트 LAN 대 LAN IPSec®

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[vEdge 라우터](#)

[Cisco IOS®-XE](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 VRF(Virtual Routing and Forwarding)가 구성된 Cisco IOS® 디바이스 간 vEdge의 transport-vpn에서 사전 공유 키 구성을 사용하는 IPSec IKEv1 Site-to-Site VPN에 대해 설명합니다. 또한 vEdge 라우터와 Amazon vPC(Virtual Port Channel)(고객 게이트웨이) 간에 IPSec을 구성하기 위한 참조로 사용할 수 있습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- IKEv1
- IPSec 프로토콜

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- vEdge 라우터(18.2 소프트웨어 이상)
- Cisco IOS®-XE 라우터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

vEdge 라우터

```
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

```

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

1. 피어의 원격 주소에 연결할 수 있는지 확인합니다.

```

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. IPSec Phase1 IKE(Internet Key Exchange)가 Cisco IOS®-XE 라우터에 설정되어 있는지 확인합니다. 상태는 "QM_IDLE"이어야 합니다.

```

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. Cisco IOS®-XE 라우터에서 IPSec 2단계가 설정되었는지 확인하고 두 사이트에서 "pkts encaps" 및 "kts decaps" 카운터가 증가했는지 확인합니다.

```

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. IPsec 1단계 및 2단계 세션이 vEdge에서도 설정되었는지 확인합니다. 상태는 "IKE_UP_IPSEC_UP"이어야 합니다.

```
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. Cisco IOS®-XE 라우터에서 확인한 일치하는 카운터와 함께 tx 및 rx 카운터가 양방향으로 증가하는지 확인합니다.

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

TCP	TUNNEL	SOURCE	DEST	SYSTEM	LOCAL	REMOTE	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							

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

Cisco IOS®/IOS®-XE에 대한 IPsec 문제 해결 가이드는 다음을 참조하십시오.

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

관련 정보

- Amazon VPC "Customer Gateway"에 대한 자세한 정보:
https://docs.aws.amazon.com/en_us/vpc/latest/adminguide/Introduction.html
- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.