对LAN IPSec的站点到站点LAN在vEdge和Cisco IOS®之间;

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[配置](#)
[vEdge路由器](#)
[思科 IOS®-XE](#)
[验证](#)
[故障排除](#)
[相关信息](#)

简介

本文在vEdge的传输VPN描述与预共享密钥配置的IPSec IKEv1 Site to Site VPN在(VRF)之间被配置的Cisco IOS设备用虚拟路由和转发。它可能也用于，参考为了配置在vEdge路由器和亚马逊虚拟端口信道(vPC) (用户网关)之间的IPSec。

先决条件

要求

Cisco 建议您了解以下主题：

- IKEv1
- IPsec 协议

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 有18.2软件的vEdge路由器或更新
- Cisco IOS XE路由器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

vEdge路由器

```
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
```

思科 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
```

验证

使用本部分可确认配置能否正常运行。

1. 保证对等体的远端地址可及的：

```
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. 检查IPSec phase1 Internet Key Exchange (IKE)是否在Cisco IOS XE路由器设立。状态应该是“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. 检查IPSec第2阶段是否在Cisco IOS XE路由器设立并且保证“pkts encaps”和“kts decap”计数器在两个站点增加：

```
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. 检查IPSec阶段1和2会话是否在vEdge建立。状态应该是“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. 检查tx-和RX计数器是否增加两个方向与在Cisco IOS XE路由器被看到的匹配计数器一起。

```
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
```

故障排除

本部分提供了可用于对配置进行故障排除的信息。

关于在Cisco IOS/IOS®-XE的IPSec故障排除指南，请参见此：

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

相关信息

- 关于亚马逊VPC “用户网关”的更多信息
  ： https://docs.aws.amazon.com/en_us/vpc/latest/adminguide/Introduction.html
- **技术支持和文档 - Cisco Systems**