IPSec de LAN para LAN de site a site entre vEdge e Cisco IOS®

Contents

Introduction

Este documento descreve a VPN site a site IPSec IKEv1 com configuração de chaves pré-compartilhadas em transport-vpn no vEdge entre o dispositivo Cisco IOS® com Virtual Routing and Forwarding (VRF) configurado. Ele também pode ser usado como referência para configurar o IPSec entre o roteador vEdge e o Amazon Virtual Port Channel (vPC) (gateway do cliente).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- IKEv1
- Protocolos IPSec

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Roteador vEdge com software 18.2 ou mais recente
- Roteador 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Roteador 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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

1. Certifique-se de que o endereço remoto do peer esteja acessível:

```
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. Verifique se a fase IPSec1 Internet Key Exchange (IKE) está estabelecida no roteador Cisco IOS®-XE. O estado deve 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 se a fase 2 do IPSec está estabelecida no roteador Cisco IOS®-XE e certifique-se de que os contadores "pkts encaps" e "kts decaps" aumentem em ambos os 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. Verifique se as sessões das fases 1 e 2 do IPSec também estão estabelecidas no vEdge. O Estado deve 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 se os contadores tx e rx aumentam em ambas as direções junto com os contadores correspondentes que foram vistos no roteador Cisco IOS®-XE.

```
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
```

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Para obter o guia de Troubleshooting de IPSec no Cisco IOS®/IOS®-XE, consulte:

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

Informações Relacionadas

- Mais informações sobre o Amazon VPC "Gateway do cliente": https://docs.aws.amazon.com/en_us/vpc/latest/adminguide/Introduction.html
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.