vEdgeとCisco IOS®間のサイト間LAN間IPSec

内容

概要

このドキュメントでは、Virtual Routing and Forwarding(VRF)が設定されたCisco IOS®デバイス間のvEdge上のtransport-vpnにおける事前共有キー設定を使用したIPSec IKEv1サイト間VPNについて説明します。また、vEdgeルータとAmazon Virtual Port Channel(vPC)（カスタマーゲートウェイ）の間でIPSecを設定するためのリファレンスとしても使用できます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- IKEv1
- IPSec プロトコル

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 18.2以降のソフトウェアを搭載したvEdgeルータ
- Cisco IOS®-XEルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

vEdgeルータ

```
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
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

1.ピアのリモートアドレスが到達可能であることを確認します。

```
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. Cisco IOS®-XEルータでIPSec phase1インターネットキーエクスチェンジ(IKE)が確立されているかどうかを確認します。状態は「QM_IDLE」である必要があります。

```
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ルータでIPSecフェーズ2が確立されているかどうかを確認し、両方のサイトで「pkts encaps」および「kts decaps」カウンタが増加していることを確認します。

```
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フェーズ1および2のセッションがvEdgeでも確立されているかどうかを確認します。状態は「IKE_UP_IPSEC_UP」である必要があります。

```
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ルータで見られた一致カウンタとともに、txおよびrxカウンタが両方向で増加するかどうかを確認します。

```
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
```

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

Cisco IOS®/IOS®-XEのIPSecトラブルシューティングガイドについては、次を参照してください。

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

関連情報

- Amazon VPC 「カスタマーゲートウェイ」の詳細：https://docs.aws.amazon.com/en_us/vpc/latest/adminguide/Introduction.html
- **テクニカル サポートとドキュメント – Cisco Systems**

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。