# IPsec の設定

# Agenda

- IPsec の基本設定
  - crypto map
  - ipsec profile
  - VTI over ipsec

# IPsec の基本設定 ～crypto map～

Step1, isakmp policy を設定

```
VPN-RT1(config)#crypto isakmp policy 10
VPN-RT1(config-isakmp)# encryption aes
VPN-RT1(config-isakmp)# hash sha256
VPN-RT1(config-isakmp)# authentication pre-share
VPN-RT1(config-isakmp)# group 5
VPN-RT1(config-isakmp)# lifetime 1000

VPN-RT2(config)#crypto isakmp policy 10
VPN-RT2(config-isakmp)# encryption aes
VPN-RT2(config-isakmp)# hash sha256
VPN-RT2(config-isakmp)# authentication pre-share
VPN-RT2(config-isakmp)# group 5
VPN-RT2(config-isakmp)# lifetime 1000
```

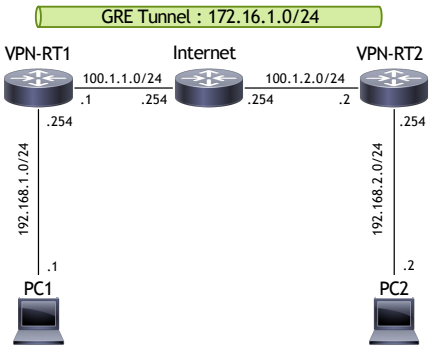
Step2, pre-shared key を設定

```
VPN-RT1(config)#crypto isakmp key cisco address 100.1.2.2

VPN-RT2(config)#crypto isakmp key cisco address 100.1.1.1
```

Step3, 設定確認

```
VPN-RT1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:     AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:           Secure Hash Standard 2 (256 bit)
        authentication method:    Pre-Shared Key
        Diffie-Hellman group:     #5 (1536 bit)
        lifetime:           1000 seconds, no volume limit
!
VPN-RT1#show crypto isakmp key
Keyring      Hostname/Address                          Preshared Key

default      100.1.2.2                                 cisco
```

| | |
|---|---|
| 暗号化アルゴリズム | AES |
| ハッシュアルゴリズム | SHA256 |
| 認証方式 | Pre-Shared Key (cisco) |
| DH group | 5 |
| Life time / duration | 1,000 sec |




IPsec を設定するにあたり、記載のパラメータで ISAKMP SA を確立するものとする。

Step1 で isakmp policy を定義し、各パラメータを定義していく。
また、 preshared-key は step2 で peer のアドレスと共に指定する。

```
Step4, transform-set を設定
VPN-RT1(config)#crypto ipsec transform-set AES-SHA esp-aes esp-sha256-hmac
VPN-RT1(cfg-crypto-trans)# mode transport

VPN-RT2(config)#crypto ipsec transform-set AES-SHA esp-aes esp-sha256-hmac
VPN-RT2(cfg-crypto-trans)# mode transport
```

```
Step5, 設定確認
VPN-RT1#show crypto ipsec transform-set AES-SHA
{ esp-aes esp-sha256-hmac  }
   will negotiate = { Transport,  },
```

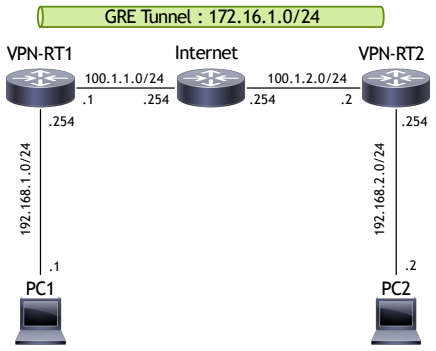
```
Step6, ACL を設定
VPN-RT1(config)#access-list 100 permit gre host 100.1.1.1 host 100.1.2.2

VPN-RT2(config)# access-list 100 permit gre host 100.1.2.2 host 100.1.1.1
```

```
Step7, IPsec Life time / duration を設定
VPN-RT1(config)#crypto ipsec security-association lifetime seconds 1000

VPN-RT2(config)#crypto ipsec security-association lifetime seconds 1000
```

```
Step8, crypto map の設定
VPN-RT1(config)#crypto map GRE-OVER-IPSEC 10 ipsec-isakmp
VPN-RT1(config-crypto-map)# set peer 100.1.2.2
VPN-RT1(config-crypto-map)# set transform-set AES-SHA
VPN-RT1(config-crypto-map)# match address 100

VPN-RT2(config)#crypto map GRE-OVER-IPSEC 10 ipsec-isakmp
VPN-RT2(config-crypto-map)# set peer 100.1.1.1
VPN-RT2(config-crypto-map)# set transform-set AES-SHA
VPN-RT2(config-crypto-map)# match address 100
```

```
Step9, 設定確認
VPN-RT1#show crypto map
Crypto Map IPv4 "GRE-OVER-IPSEC" 10 ipsec-isakmp
        Peer = 100.1.2.2
        Extended IP access list 100
            access-list 100 permit gre host 100.1.1.1 host 100.1.2.2
        Security association lifetime: 4608000 kilobytes/1000 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                AES-SHA:  { esp-aes esp-sha256-hmac  } ,
        }
        Interfaces using crypto map GRE-OVER-IPSEC:
        Interfaces using crypto map NiStTeSt1:
```

| | |
|---|---|
| セキュリティプロトコル | ESP |
| Life time / duration | 1,000 sec |
| カプセル化モード | transport |
| 暗号化アルゴリズム | AES |
| ハッシュアルゴリズム | SHA256 |
| DH group | N/A |




IPsec を設定するにあたり、 記載のパラメータで IPsec SA を確立するものとする。
まずは transform-set を定義する。今回は 「AES-SHA」 という名前を指定し、暗号化アルゴリズム、ハッシュアルゴリズム、カプセル化モードを定義する。

続いて、 IPsec の対象とするトラフィックを ACL で指定する。
今回は GRE over IPsec とするため、 GRE でカプセル化された後のトラフィックが IPsec の対象となる。

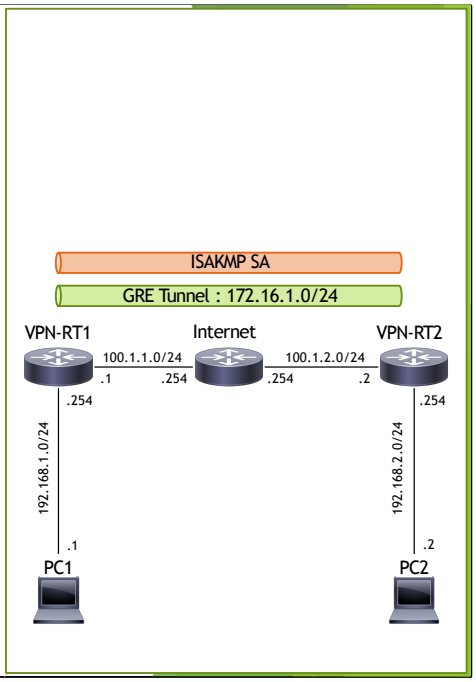
続いて、 IPsec SA の Life time / duration を定義する。
その後、 crypto map を定義し、対向 VPN 装置と適用する transform-set 、ACL の紐付けを行う。

```
Step10, crypto map を I/F に適用
VPN-RT1(config-if)#crypto map GRE-OVER-IPSEC

VPN-RT2(config-if)#crypto map GRE-OVER-IPSEC
```

```
Step11, 設定確認
VPN-RT1#show crypto map
Crypto Map IPv4 "GRE-OVER-IPSEC" 10 ipsec-isakmp
        Peer = 100.1.2.2
        Extended IP access list 100
            access-list 100 permit gre host 100.1.1.1 host 100.1.2.2
        Current peer: 100.1.2.2
        Security association lifetime: 4608000 kilobytes/1000 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                AES-SHA:  { esp-aes esp-sha256-hmac  } ,
        }
        Interfaces using crypto map GRE-OVER-IPSEC:
                Ethernet1/0

        Interfaces using crypto map NiStTeSt1:
```

```
Step12, PC1 から PC2 に ping を実行
PC1#ping 192.168.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 5/7/10 ms
```

```
Step13, isakmp sa の確認
VPN-RT1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
100.1.2.2       100.1.1.1       QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA

VPN-RT2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
100.1.2.2       100.1.1.1       QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA
```



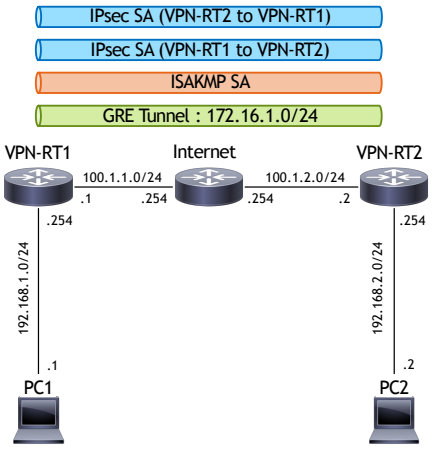

最後に定義した crypto map を 物理 I/F に適用する。
ここでは、 GRE packet が送信される Internet 向けの I/F に適用している。

crypto map を用いる場合、 IPsec の対象となる通信が発生すると ISAKMP SA と IPsec SA の確立が行われる。
そのため、 PC1 から PC2 に ping を実行する。

すると、 ping をトリガーとして ISAKMP SA と IPsec SA が確立し、 ping による通信は暗号化される。

まずは確立した ISAKMP SA を show command で確認する。
VPN-RT1 と VPN-RT2 で ISAKMP SA が確立していることがわかる。

```
Step14, IPsec SA の確認
VPN-RT1#show crypto ipsec sa

interface: Ethernet1/0
    Crypto map tag: GRE-OVER-IPSEC, local addr 100.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (100.1.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (100.1.2.2/255.255.255.255/47/0)
   current_peer 100.1.2.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #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.: 100.1.1.1, remote crypto endpt.: 100.1.2.2
     plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet1/0
     current outbound spi: 0x7D57AB9F(2102897567)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x46A76EEF(1185378031)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Transport, }
        conn id: 1, flow_id: SW:1, sibling_flags 80004000, crypto map: GRE-OVER-IPSEC
        sa timing: remaining key lifetime (k/sec): (4199053/601)
        IV size: 16 bytes
        replay detection support: Y
        ecn bit support: Y status: off
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x7D57AB9F(2102897567)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Transport, }
        conn id: 2, flow_id: SW:2, sibling_flags 80004000, crypto map: GRE-OVER-IPSEC
        sa timing: remaining key lifetime (k/sec): (4199053/601)
        IV size: 16 bytes
        replay detection support: Y
        ecn bit support: Y status: off
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

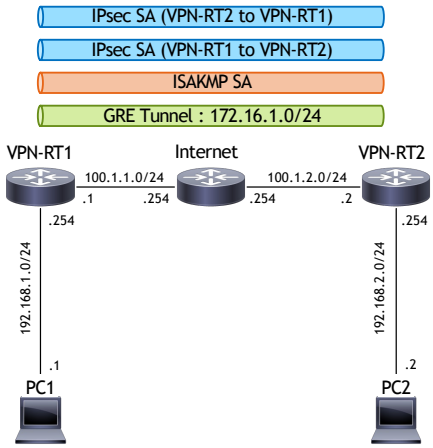



続いて、 IPsec SA を確認する。
VPN-RT1 から見ると、 ”100.1.2.2 (VPN-RT2)” に対して peer が設定されており、 inbound esp と outbound esp の 2つの SA が確立されていることがわかる。

また、 ping の実行例から 「.!!!!」 と4発が通信に成功しており、 #pkt encaps , decaps などが4つ count up している。

そして、今回は ESP のみを使用しているが、 ESP と AH の両方を使用する場合は inbound ah と outbound ah も表示され、4つの SA が確立されることとなる。

```
Step15, IPsec SA の確認
VPN-RT2#show crypto ipsec sa

interface: Ethernet1/0
    Crypto map tag: GRE-OVER-IPSEC, local addr 100.1.2.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (100.1.2.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (100.1.1.1/255.255.255.255/47/0)
   current_peer 100.1.1.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #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.: 100.1.2.2, remote crypto endpt.: 100.1.1.1
     plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet1/0
     current outbound spi: 0x3753E9B9(928246201)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x66022149D(1711412381)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Transport, }
        conn id: 3, flow_id: SW:3, sibling_flags 80000000, crypto map: GRE-OVER-IPSEC
        sa timing: remaining key lifetime (k/sec): (4219431/440)
        IV size: 16 bytes
        replay detection support: Y
        ecn bit support: Y status: off
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x3753E9B9(928246201)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Transport, }
        conn id: 4, flow_id: SW:4, sibling_flags 80000000, crypto map: GRE-OVER-IPSEC
        sa timing: remaining key lifetime (k/sec): (4219431/440)
        IV size: 16 bytes
        replay detection support: Y
        ecn bit support: Y status: off
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```




VPN-RT2 でも同様に確認が可能。

# IPsec の基本設定 ～ipsec profile～

Step1, isakmp policy を設定

```
VPN-RT1(config)#crypto isakmp policy 10
VPN-RT1(config-isakmp)# encryption aes
VPN-RT1(config-isakmp)# hash sha256
VPN-RT1(config-isakmp)# authentication pre-share
VPN-RT1(config-isakmp)# group 5
VPN-RT1(config-isakmp)# lifetime 1000

VPN-RT2(config)#crypto isakmp policy 10
VPN-RT2(config-isakmp)# encryption aes
VPN-RT2(config-isakmp)# hash sha256
VPN-RT2(config-isakmp)# authentication pre-share
VPN-RT2(config-isakmp)# group 5
VPN-RT2(config-isakmp)# lifetime 1000
```

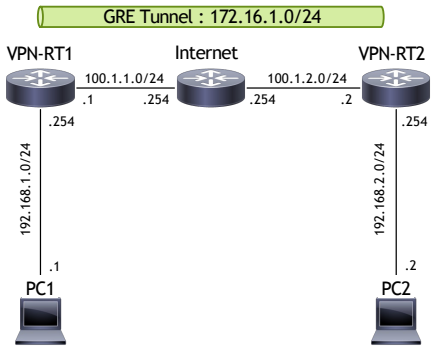
Step2, pre-shared key を設定

```
VPN-RT1(config)#crypto isakmp key cisco address 100.1.2.2

VPN-RT2(config)#crypto isakmp key cisco address 100.1.2.2
```

Step3, 設定確認

```
VPN-RT1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:     AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:           Secure Hash Standard 2 (256 bit)
        authentication method:    Pre-Shared Key
        Diffie-Hellman group:     #5 (1536 bit)
        lifetime:           1000 seconds, no volume limit
!
VPN-RT1#show crypto isakmp key
Keyring      Hostname/Address                          Preshared Key

default      100.1.2.2                                 cisco
```

| | |
|---|---|
| 暗号化アルゴリズム | AES |
| ハッシュアルゴリズム | SHA256 |
| 認証方式 | Pre-Shared Key (cisco) |
| DH group | 5 |
| Life time / duration | 1,000 sec |




crypto map ではなく ipsec profile を用いる場合、 ISAKMP SA に関しては設定差分なし。

```
Step4, transform-set を設定
VPN-RT1(config)#crypto ipsec transform-set AES-SHA esp-aes esp-sha256-hmac
VPN-RT1(cfg-crypto-trans)# mode transport

VPN-RT2(config)#crypto ipsec transform-set AES-SHA esp-aes esp-sha256-hmac
VPN-RT2(cfg-crypto-trans)# mode transport
```

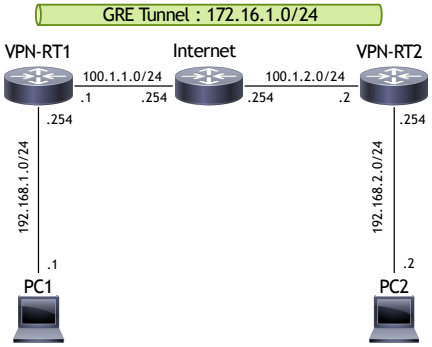
```
Step5, 設定確認
VPN-RT1#show crypto ipsec transform-set AES-SHA
{ esp-aes esp-sha256-hmac  }
   will negotiate = { Transport,  },
```

```
Step6, IPsec Life time / duration を設定
VPN-RT1(config)#crypto ipsec security-association lifetime seconds 1000

VPN-RT2(config)#crypto ipsec security-association lifetime seconds 1000
```

```
Step7, ipsec profile の設定
VPN-RT1(config)#crypto ipsec profile IPSEC_PROFILE
VPN-RT1(ipsec-profile)#set transform-set AES-SHA

VPN-RT2(config)#crypto ipsec profile IPSEC_PROFILE
VPN-RT2(ipsec-profile)#set transform-set AES-SHA
```

```
Step8, 設定確認
VPN-RT1#show crypto ipsec profile
IPSEC profile IPSEC_PROFILE
        Security association lifetime: 4608000 kilobytes/1000 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                AES-SHA:  { esp-aes esp-sha256-hmac  } ,
        }

IPSEC profile default
        Security association lifetime: 4608000 kilobytes/1000 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                default:  { esp-aes esp-sha-hmac  } ,
        }
```

| | |
|---|---|
| セキュリティプロトコル | ESP |
| Life time / duration | 1,000 sec |
| カプセル化モード | transport |
| 暗号化アルゴリズム | AES |
| ハッシュアルゴリズム | SHA256 |
| DH group | N/A |

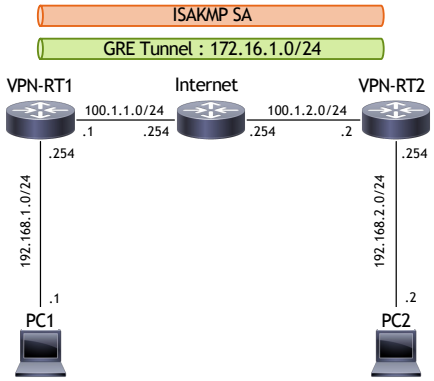



IPsec SA に関する設定を行う際、 ipsec profile を用いる場合は ACL が不要となる。
また、ipsec profile では crypto map と異なり transform-set の紐付けのみ行う。

```
Step9, crypto map を tunnel I/F に適用
VPN-RT1(config-if)#tunnel protection ipsec profile IPSEC_PROFILE

VPN-RT2(config-if)#tunnel protection ipsec profile IPSEC_PROFILE
```

```
Step10, isakmp sa の確認
VPN-RT1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
100.1.1.1       100.1.2.2       QM_IDLE           1001 ACTIVE
100.1.2.2       100.1.1.1       QM_IDLE           1002 ACTIVE

IPv6 Crypto ISAKMP SA


VPN-RT2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
100.1.1.1       100.1.2.2       QM_IDLE           1001 ACTIVE
100.1.2.2       100.1.1.1       QM_IDLE           1002 ACTIVE

IPv6 Crypto ISAKMP SA
```





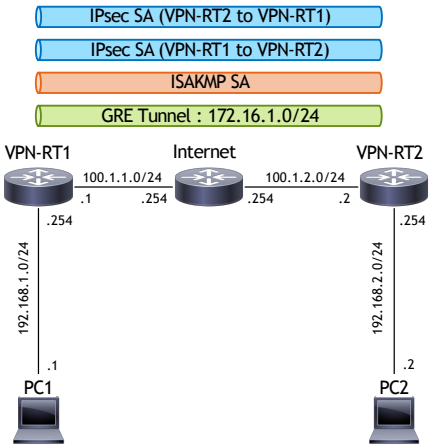

最後に定義した ipsec profile を Tunnel I/F に適用する。
ここでは、GRE Tunnel の I/F に適用している。

また、 ipsec profile では profile を tunnel I/F に適用した時点で ISAKMP SA , IPSEC SA が確立される。

まずは確立した ISAKMP SA を show command で確認する。
VPN-RT1 と VPN-RT2 で ISAKMP SA が確立していることがわかる。

※ipsec profile を適用することで各 IPsec 装置から ISAKMP SA が開始されるため、 IPsec SA が2本確立されている。

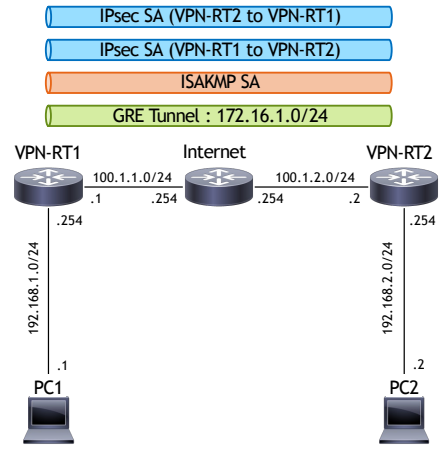
```
Step11, IPsec SA の確認
VPN-RT1#show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 100.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (100.1.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (100.1.2.2/255.255.255.255/47/0)
   current_peer 100.1.2.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #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.: 100.1.1.1, remote crypto endpt.: 100.1.2.2
     plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet1/0
     current outbound spi: 0x9F2F4D76(2670677366)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x57BEA7BD(1472112573)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Transport, }
        conn id: 1, flow_id: SW:1, sibling_flags 80004000, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4608000/942)
        IV size: 16 bytes
        replay detection support: Y
        ecn bit support: Y status: off
        Status: ACTIVE(ACTIVE)
      spi: 0x80B5E11C(2159403292)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Transport, }
        conn id: 3, flow_id: SW:3, sibling_flags 80000000, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4305641/944)
        IV size: 16 bytes
        replay detection support: Y
        ecn bit support: Y status: off
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:
```




続いて、 IPsec SA を確認する。
VPN-RT1 から見ると、 ”100.1.2.2 (VPN-RT2)” に対して peer が設定されており、 inbound esp と outbound esp の SA が確立されていることがわかる。

※ISAKMP SA と同じ理由で、 SA は in/out で2つずつ生成されている。

```
Step11, IPsec SA の確認
VPN-RT1#show crypto ipsec sa

…
 outbound esp sas:
      spi: 0xC1ED74D9(3253564633)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Transport, }
        conn id: 2, flow_id: SW:2, sibling_flags 80004000, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4608000/942)
        IV size: 16 bytes
        replay detection support: Y
        ecn bit support: Y status: off
        Status: ACTIVE(ACTIVE)
      spi: 0x9F2F4D76(2670677366)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Transport, }
        conn id: 4, flow_id: SW:4, sibling_flags 80000000, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4305641/944)
        IV size: 16 bytes
        replay detection support: Y
        ecn bit support: Y status: off
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```




続いて、 IPsec SA を確認する。
VPN-RT1 から見ると、 ”100.1.2.2 (VPN-RT2)” に対して peer が設定されており、 inbound esp と outbound esp の SA が確立されていることがわかる。

※ISAKMP SA と同じ理由で、 SA は in/out で2つずつ生成されている。

# IPsec の基本設定 ～VTI over IPsec～

Step1, isakmp policy を設定

```
VPN-RT1(config)#crypto isakmp policy 10
VPN-RT1(config-isakmp)# encryption aes
VPN-RT1(config-isakmp)# hash sha256
VPN-RT1(config-isakmp)# authentication pre-share
VPN-RT1(config-isakmp)# group 5
VPN-RT1(config-isakmp)# lifetime 1000

VPN-RT2(config)#crypto isakmp policy 10
VPN-RT2(config-isakmp)# encryption aes
VPN-RT2(config-isakmp)# hash sha256
VPN-RT2(config-isakmp)# authentication pre-share
VPN-RT2(config-isakmp)# group 5
VPN-RT2(config-isakmp)# lifetime 1000
```

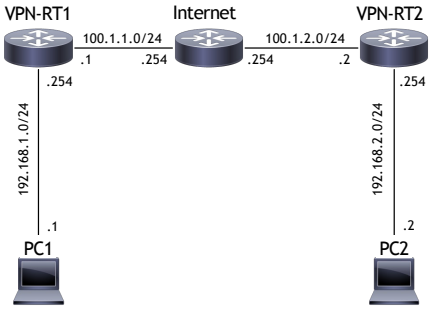
Step2, pre-shared key を設定

```
VPN-RT1(config)#crypto isakmp key cisco address 100.1.2.2

VPN-RT2(config)#crypto isakmp key cisco address 100.1.2.2
```

Step3, 設定確認

```
VPN-RT1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:     AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:           Secure Hash Standard 2 (256 bit)
        authentication method:    Pre-Shared Key
        Diffie-Hellman group:     #5 (1536 bit)
        lifetime:           1000 seconds, no volume limit
!
VPN-RT1#show crypto isakmp key
Keyring      Hostname/Address                          Preshared Key

default      100.1.2.2                                 cisco
```

| | |
|---|---|
| 暗号化アルゴリズム | AES |
| ハッシュアルゴリズム | SHA256 |
| 認証方式 | Pre-Shared Key (cisco) |
| DH group | 5 |
| Life time / duration | 1,000 sec |




GRE を使用せずに、 Tunnel mode を IPsec とすることでも IPsec VPN を構築することが可能となる。
この場合も、 ISAKMP SA に関する設定は差異がない。

```
Step4, transform-set を設定
VPN-RT1(config)#crypto ipsec transform-set AES-SHA esp-aes esp-sha256-hmac
VPN-RT1(cfg-crypto-trans)# mode tunnel

VPN-RT2(config)#crypto ipsec transform-set AES-SHA esp-aes esp-sha256-hmac
VPN-RT2(cfg-crypto-trans)# mode tunnel
```

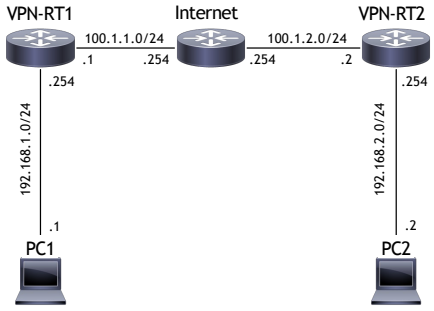
```
Step5, 設定確認
VPN-RT1#show crypto ipsec transform-set AES-SHA
{ esp-aes esp-sha256-hmac  }
   will negotiate = { Tunnel,  },
```

```
Step6, IPsec Life time / duration を設定
VPN-RT1(config)#crypto ipsec security-association lifetime seconds 1000

VPN-RT2(config)#crypto ipsec security-association lifetime seconds 1000
```

```
Step7, ipsec profile の設定
VPN-RT1(config)#crypto ipsec profile IPSEC_PROFILE
VPN-RT1(ipsec-profile)#set transform-set AES-SHA

VPN-RT2(config)#crypto ipsec profile IPSEC_PROFILE
VPN-RT2(ipsec-profile)#set transform-set AES-SHA
```

```
Step8, 設定確認
VPN-RT1#show crypto ipsec profile
IPSEC profile IPSEC_PROFILE
        Security association lifetime: 4608000 kilobytes/1000 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                AES-SHA:  { esp-aes esp-sha256-hmac  } ,
        }

IPSEC profile default
        Security association lifetime: 4608000 kilobytes/1000 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                default:  { esp-aes esp-sha-hmac  } ,
        }
```

| | |
|---|---|
| セキュリティプロトコル | ESP |
| Life time / duration | 1,000 sec |
| カプセル化モード | tunnel |
| 暗号化アルゴリズム | AES |
| ハッシュアルゴリズム | SHA256 |
| DH group | N/A |

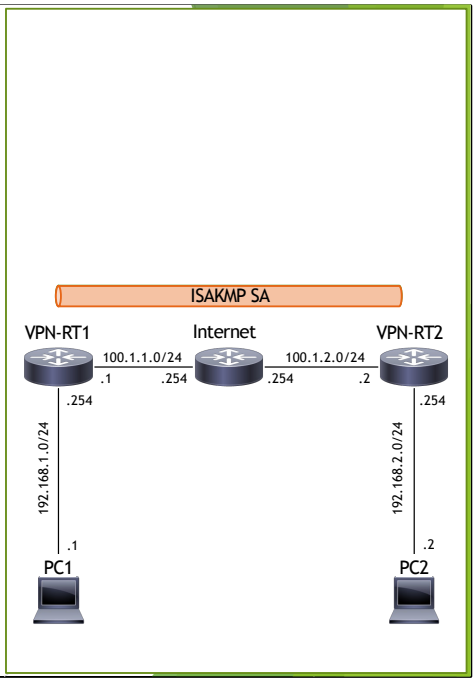



VTI over IPsec の場合、 GRE は使用せずに IPsec として IP header を付与する。
そのため、 tunnel mode は transport ではなく tunnel を指定する。

```
Step9, Tunnel I/F (IPsec) を設定
VPN-RT1(config)#interface tunnel 0
VPN-RT1(config-if)#ip address 172.16.1.1 255.255.255.0
VPN-RT1(config-if)#tunnel source Ethernet1/0
VPN-RT1(config-if)#tunnel destination 100.1.2.2
VPN-RT1(config-if)#tunnel mode ipsec ipv4
VPN-RT1(config-if)#tunnel protection ipsec profile IPSEC_PROFILE

VPN-RT2(config)#interface tunnel 0
VPN-RT2(config-if)#ip address 172.16.1.2 255.255.255.0
VPN-RT2(config-if)#tunnel source Ethernet1/0
VPN-RT2(config-if)#tunnel destination 100.1.1.1
VPN-RT2(config-if)#tunnel mode ipsec ipv4
VPN-RT2(config-if)#tunnel protection ipsec profile IPSEC_PROFILE
```

```
Step10, tunnel I/F の確認
VPN-RT1#show interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 172.16.1.1/24
  MTU 17878 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 100.1.1.1 (Ethernet1/0), destination 100.1.2.2
   Tunnel Subblocks:
      src-track:
         Tunnel0 source tracking subblock associated with Ethernet1/0
          Set of tunnels with source Ethernet1/0, 1 member (includes iterators), on interface <OK>
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1438 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "IPSEC_PROFILE")
```

```
Step11, isakmp sa の確認
VPN-RT1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
100.1.1.1       100.1.2.2       QM_IDLE           1001 ACTIVE
100.1.2.2       100.1.1.1       QM_IDLE           1002 ACTIVE

IPv6 Crypto ISAKMP SA

VPN-RT2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
100.1.1.1       100.1.2.2       QM_IDLE           1001 ACTIVE
100.1.2.2       100.1.1.1       QM_IDLE           1002 ACTIVE

IPv6 Crypto ISAKMP SA
```

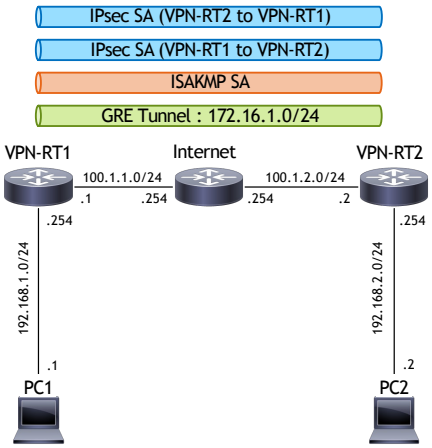



VTI over IPsec では、 Tunnel mode を 「ipsec ipv4」 とし、 ipsec profile を適用する。
また、 ipsec profile では profile を tunnel I/F に適用した時点で ISAKMP SA , IPSEC SA が確立される。

まずは確立した ISAKMP SA を show command で確認する。
VPN-RT1 と VPN-RT2 で ISAKMP SA が確立していることがわかる。

※ipsec profile を適用することで各 IPsec 装置から ISAKMP SA が開始されるため、 IPsec SA が2本確立されている。

```
Step11, IPsec SA の確認
VPN-RT1#show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 100.1.1.1

   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 100.1.2.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #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.: 100.1.1.1, remote crypto endpt.: 100.1.2.2
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet1/0
     current outbound spi: 0x8A78B9A7(2323167655)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x6A7C3A28(1786526251)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Tunnel, }
        conn id: 5, flow_id: SW:5, sibling_flags 80000040, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4324236/669)
        IV size: 16 bytes
        replay detection support: Y
        ecn bit support: Y status: off
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x8A78B9A7(2323167655)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Tunnel, }
        conn id: 6, flow_id: SW:6, sibling_flags 80000040, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4324236/669)
        IV size: 16 bytes
        replay detection support: Y
        ecn bit support: Y status: off
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```




続いて、 IPsec SA を確認する。
VPN-RT1 から見ると、 ”100.1.2.2 (VPN-RT2)” に対して peer が設定されており、 inbound esp と outbound esp の 2つの SA が確立されていることがわかる。