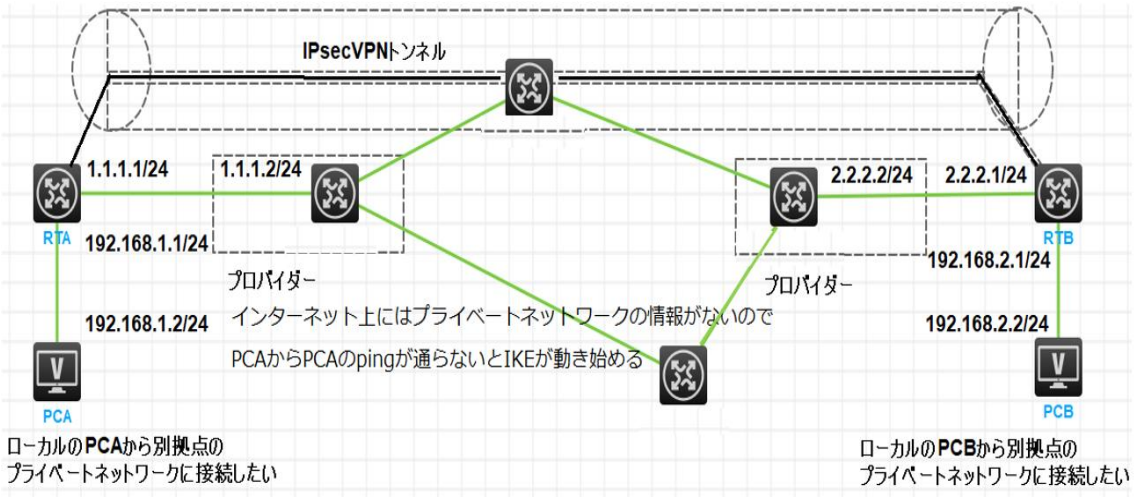
IPsecVPN の設定(IKE main モード)

実習内容と目標

このラボでは以下のことを学びます：

- IPsec で IKE メインモード、事前共有鍵認証方式を習得します。

ネットワーク図



以下がこの実習でクラウドをシュミレートするために SWA を配置。上の図から分かるように、SWA(クラウド上)は RTA と RTB のプライベートネットワーク(192.168.1.0, 192.168.2.0 の情報は持っていません)。

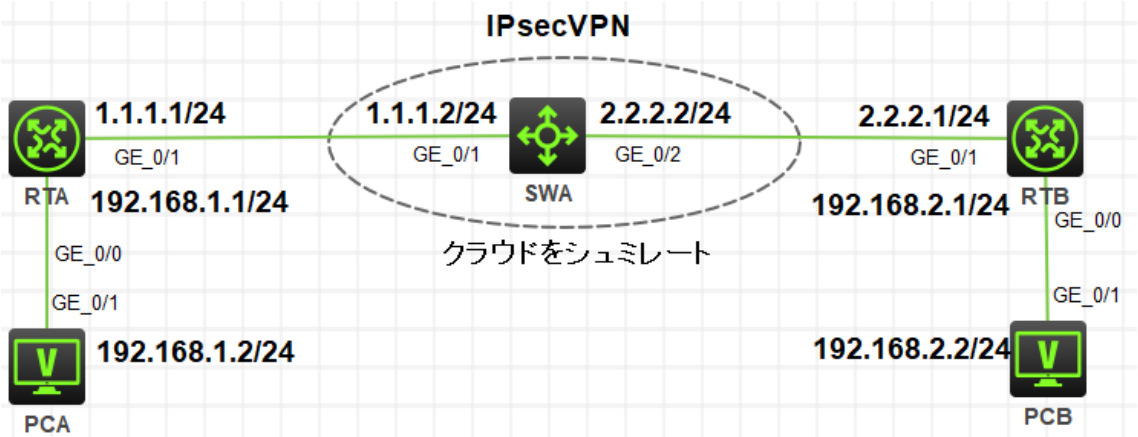


図 4.1 実習ネットワーク

実習装置

本実験に必要な主な設備機材 実験装置名前とモデル番号	バージョン	数量	特記事項
MSR36-20	Version7.1	2	ルーター
S5820V2	Version7.1	1	スイッチ
PC	Windows 7	2	ホスト
ネットワークケーブルの接続	--	4	ストレートケーブル

実習手順

タスク 1:それぞれの装置に IP アドレスを設定する

この実習では RTA と RTB 間 IKE 認証による IPsec トンネルの接続をどのようにするかを示します。そして、どのようにフェーズ 1 でメインモードを使い、事前共有鍵認証を行う IKE を設定するかを示します。

手順 1:両 PC に IP アドレス、ゲートウェイアドレスを設定する

PC、ルーター、そしてスイッチを図 4-1 のように接続します。そして、スイッチには VLAN 2 を作成し、VLAN 2 に GE1/0/2 を追加します。

<H3C>system-view

System View: return to User View with Ctrl+Z.

[H3C]sysname SWA

[SWA]vlan 2

[SWA-vlan2]port GigabitEthernet 1/0/2

[SWA-vlan2]quit

アドレスおよびデフォルトゲートウェイは表 3-1 に従って設定します。RTA を PCA のデフォルトゲートウェイに、RTB を PCB のデフォルトゲートウェイに設定します。

表 3-1 IP アドレス割り当て

装置	**インターフェイス**	**IP アドレス**	**ゲートウェイ**
RTA	G0/0	192.168.1.1/24	-
	G0/1	1.1.1.1/24	-
RTB	G0/0	192.168.2.1/24	-

	G0/1	2.2.2.1/24	-
SWA	VLAN 1	1.1.1.2/24	
	VLAN 2	2.2.2.2/24	
PCA		192.168.1.2/24	192.168.1.1/24
PCB		192.168.2.2/24	192.168.2.1/24

手順 2: ルーティングプロトコルを設定する

RTA, RTB, SWA に以下のように OSPF を設定します。

```
[RTA] ospf 1
[RTA-ospf-1]area 0
[RTA-ospf-1-area-0.0.0.0]network 1.1.1.0 0.0.0.255
[RTA-ospf-1-area-0.0.0.0]quit
[RTA-ospf-1]quit

[SWA]ospf 1
[SWA-ospf-1]area 0
[SWA-ospf-1-area-0.0.0.0]network 1.1.1.0 0.0.0.255
[SWA-ospf-1-area-0.0.0.0]network 2.2.2.0 0.0.0.255
[SWA-ospf-1-area-0.0.0.0]quit
[SWA-ospf-1]quit

[RTB]ospf 1
[RTB-ospf-1]area 0
[RTB-ospf-1-area-0.0.0.0]network 2.2.2.0 0.0.0.255
[RTB-ospf-1-area-0.0.0.0]quit
[RTB-ospf-1]quit
```

上記のように設定後、SWA は公共ネットワークをシミュレートしていて、公共ネットワークルートのみ保存しています。これはサブネット 192.168.1.0/24 と 192.168.2.0/24 へのルートを持っていません。なぜならば、OSPF エリア PCA と PCB に接続されているルーターインタフェースへのルートを含んでいません。

各ルーターでリモートプライベートネットワークへのスタティックルートを以下のように設定します。

```
[RTA]ip route-static 192.168.2.0 255.255.255.0 1.1.1.2
[RTB]ip route-static 192.168.1.0 255.255.255.0 2.2.2.2
```

上記設定完了後、RTA, RTB, SWA のルーティングテーブルを表示します。

[RTA]display ip routing-table

Destinations : 18 Routes : 18

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.0/24	Direct	0	0	1.1.1.1	GE0/1
1.1.1.0/32	Direct	0	0	1.1.1.1	GE0/1
1.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.255/32	Direct	0	0	1.1.1.1	GE0/1
2.2.2.0/24	O_INTRA	10	2	1.1.1.2	GE0/1
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.0/24	Direct	0	0	192.168.1.1	GE0/0
192.168.1.0/32	Direct	0	0	192.168.1.1	GE0/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.255/32	Direct	0	0	192.168.1.1	GE0/0
192.168.2.0/24	Static	60	0	1.1.1.2	GE0/1
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

<SWA>display ip routing-table

Destinations : 16 Routes : 16

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.0/24	Direct	0	0	1.1.1.2	Vlan1
1.1.1.0/32	Direct	0	0	1.1.1.2	Vlan1
1.1.1.2/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.255/32	Direct	0	0	1.1.1.2	Vlan1
2.2.2.0/24	Direct	0	0	2.2.2.2	Vlan2
2.2.2.0/32	Direct	0	0	2.2.2.2	Vlan2
2.2.2.2/32	Direct	0	0	127.0.0.1	InLoop0
2.2.2.255/32	Direct	0	0	2.2.2.2	Vlan2

127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

[RTB]display ip routing-table

Destinations : 18 Routes : 18

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.0/24	O_INTRA	10	2	2.2.2.2	GE0/1
2.2.2.0/24	Direct	0	0	2.2.2.1	GE0/1
2.2.2.0/32	Direct	0	0	2.2.2.1	GE0/1
2.2.2.1/32	Direct	0	0	127.0.0.1	InLoop0
2.2.2.255/32	Direct	0	0	2.2.2.1	GE0/1
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.0/24	Static	60	0	2.2.2.2	GE0/1
192.168.2.0/24	Direct	0	0	192.168.2.1	GE0/0
192.168.2.0/32	Direct	0	0	192.168.2.1	GE0/0
192.168.2.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.2.255/32	Direct	0	0	192.168.2.1	GE0/0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

この結果は、SWA のルーティングテーブルにはプライベートネットワークへのルートを持っていないことを表しています。

以下のように、PCA と PCB 間の接続を確認します。

<PCA>ping 192.168.2.2

Ping 192.168.2.2 (192.168.2.2): 56 data bytes, press CTRL_C to break

Request time out

Request time out

Request time out

Request time out

Request time out

この結果は、PCA は PCB に ping できないことを表しています。この結果の理由は SWA が PCB へのルートを持っていないからです。

手順 3：IKE プロポーザルを設定する

[RTA]ike proposal 1

[RTA-ike-proposal-1]authentication-method pre-share

[RTA-ike-proposal-1]authentication-algorithm md5

[RTA-ike-proposal-1]encryption-algorithm 3des-cbc

[RTA-ike-proposal-1]quit

[RTB]ike proposal 1

[RTB-ike-proposal-1]authentication-method pre-share

[RTB-ike-proposal-1]authentication-algorithm md5

[RTB-ike-proposal-1]encryption-algorithm 3des-cbc

[RTB-ike-proposal-1]quit

手順 4：IKE keychain を設定する

[RTA]ike keychain keychain1

[RTA-ike-keychain-keychain1]pre-shared-key address 2.2.2.1 255.255.255.0 key simple h3c

[RTA-ike-keychain-keychain1]quit

[RTB]ike keychain keychain1

[RTB-ike-keychain-keychain1]pre-shared-key address 1.1.1.1 255.255.255.0 key simple h3c

[RTB-ike-keychain-keychain1]quit

手順 5：IKE profile を設定する

Pre-shared key を使う

[RTA]ike profile profile1

[RTA-ike-profile-profile1]local-identity address 1.1.1.1

[RTA-ike-profile-profile1]match remote identity address 2.2.2.1 255.255.255.0

[RTA-ike-profile-profile1]keychain keychain1

```
[RTA-ike-profile-profile1]proposal 1
[RTA-ike-profile-profile1]quit

[RTB]ike profile profile1
[RTB-ike-profile-profile1]local-identity address 2.2.2.1
[RTB-ike-profile-profile1]match remote identity address 1.1.1.1 255.255.255.0
[RTB-ike-profile-profile1]keychain keychain1
[RTB-ike-profile-profile1]proposal 1
[RTB-ike-profile-profile1]quit
```

手順 6：ACL を設定する

両ルーターがサブネット 192.168.1.0/24 と 192.168.2.0/24 との間のトラフィックを認識できるように ACL を設定します。

```
[RTA]acl advanced 3000
[RTA-acl-ipv4-adv-3000]rule 0 permit ip source 192.168.1.0 0.0.0.255 destination
 192.168.2.0 0.0.0.255
[RTA-acl-ipv4-adv-3000]quit

[RTB]acl advanced 3000
[RTB-acl-ipv4-adv-3000]rule 0 permit ip source 192.168.2.0 0.0.0.255 destination
 192.168.1.0 0.0.0.255
[RTB-acl-ipv4-adv-3000]quit
```

手順 7：IPsec proposal を設定する

```
[RTA]ipsec transform-set trans1
[RTA-ipsec-transform-set-trans1]esp authentication-algorithm sha1
[RTA-ipsec-transform-set-trans1]esp encryption-algorithm aes-cbc-128
[RTA-ipsec-transform-set-trans1]quit

[RTB]ipsec transform-set trans1
[RTB-ipsec-transform-set-trans1]esp authentication-algorithm sha1
[RTB-ipsec-transform-set-trans1]esp encryption-algorithm aes-cbc-128
[RTB-ipsec-transform-set-trans1]quit
```

手順 8: IPsec policy の設定と適用

両ルーターにおいて、IPsec policy の設定と隣接する装置と接続されている物理インタフェースにそれを適用する。

```
[RTA]ipsec policy policy1 1 isakmp
[RTA-ipsec-policy-isakmp-policy1-1]remote-address 2.2.2.1
[RTA-ipsec-policy-isakmp-policy1-1]security acl 3000
[RTA-ipsec-policy-isakmp-policy1-1]transform-set trans1
[RTA-ipsec-policy-isakmp-policy1-1]ike-profile profile1
[RTA-ipsec-policy-isakmp-policy1-1]quit
[RTA]interface GigabitEthernet 0/1
[RTA-GigabitEthernet0/1]ipsec apply policy policy1
[RTA-GigabitEthernet0/1]quit

[RTB]ipsec policy policy1 1 isakmp
RTB-ipsec-policy-isakmp-policy1-1]remote-address 1.1.1.1
RTB-ipsec-policy-isakmp-policy1-1]security acl 3000
[RTB-ipsec-policy-isakmp-policy1-1]transform-set trans1
[RTB-ipsec-policy-isakmp-policy1-1]ike-profile profile1
[RTB-ipsec-policy-isakmp-policy1-1]quit
[RTB]interface GigabitEthernet 0/1
[RTB-GigabitEthernet0/1]ipsec apply policy policy1
[RTB-GigabitEthernet0/1]quit
```

手順 9: 設定を確認する

```
[RTA]display ike proposal
  Priority Authentication Authentication Encryption    Diffie-Hellman Duration
                     method          algorithm       algorithm           group          (seconds)
------------------------------------------------------------------------------
  1             PRE-SHARED-KEY       MD5             3DES-CBC       Group 1             86400
  default    PRE-SHARED-KEY       SHA1            DES-CBC        Group 1             86400

[RTA]display ipsec transform-set
IPsec transform set: trans1
   State: complete
```

```
  Encapsulation mode: tunnel
  ESN: Disabled
  PFS:
  Transform: ESP
  ESP protocol:
    Integrity: SHA1
    Encryption: AES-CBC-128

[RTA]display ipsec policy
-----------------------------------------
IPsec Policy: policy1
Interface: GigabitEthernet0/1
-----------------------------------------

  ----------------------------
  Sequence number: 1
  Mode: ISAKMP
  ----------------------------
  Traffic Flow Confidentiality: Disabled
  Security data flow: 3000
  Selector mode: standard
  Local address:
  Remote address: 2.2.2.1
  Transform set:    tran1
  IKE profile: profile1
  IKEv2 profile:
  SA duration(time based): 3600 seconds
  SA duration(traffic based): 1843200 kilobytes
  SA idle time:

[RTB]display ike proposal
 Priority Authentication Authentication Encryption    Diffie-Hellman Duration
                  method           algorithm       algorithm           group          (seconds)
-------------------------------------------------------------------------------
 1            PRE-SHARED-KEY        MD5             3DES-CBC       Group 1            86400
 default   PRE-SHARED-KEY        SHA1            DES-CBC        Group 1            86400
```

```
[RTB]display ipsec transform-set
IPsec transform set: trans1
   State: complete
   Encapsulation mode: tunnel
   ESN: Disabled
   PFS:
   Transform: ESP
   ESP protocol:
      Integrity: SHA1
      Encryption: AES-CBC-128

[RTB]display ipsec policy
-------------------------------------------
IPsec Policy: policy1
Interface: GigabitEthernet0/1
-------------------------------------------

   ----------------------------
   Sequence number: 1
   Mode: ISAKMP
   ----------------------------
   Traffic Flow Confidentiality: Disabled
   Security data flow: 3000
   Selector mode: standard
   Local address:
   Remote address: 1.1.1.1
   Transform set:    trans1
   IKE profile: profile1
   IKEv2 profile:
   SA duration(time based): 3600 seconds
   SA duration(traffic based): 1843200 kilobytes
   SA idle time:
```

手順 10:トンネルが確立されていて稼働しているかを確認する

PCA から PCB に ping して両 PC 間の接続を確認します。

```
<PCA>ping 192.168.2.2
```

Ping 192.168.2.2 (192.168.2.2): 56 data bytes, press CTRL_C to break
Request time out
56 bytes from 192.168.2.2: icmp_seq=1 ttl=253 time=2.000 ms
56 bytes from 192.168.2.2: icmp_seq=2 ttl=253 time=9.000 ms
56 bytes from 192.168.2.2: icmp_seq=3 ttl=253 time=2.000 ms
56 bytes from 192.168.2.2: icmp_seq=4 ttl=253 time=4.000 ms

出力は、最初の ICMP エコー要求がタイムアウトになり、他のすべての要求はタイムアウトしなかったことを示しています。 最初の要求がタイムアウトする前に IPsec SAs が使用できなかったため、最初の要求は破棄されました。 最初のリクエストが IKE ネゴシエーションをトリガーし、次に予想される IPsec SAs が推定され、後続のすべてのリクエストが IPsec トンネルを介して宛先に配信されました。

RTA と RTB の IPsec と IKE 情報を表示します。
<RTA>display ike sa
<RTA>display ike sa
Connection-ID Remote Flag DOI
---
2 2.2.2.1 RD IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY

<RTA>display ike sa verbose
<RTA>display ike sa verbose

Connection ID: 2
Outside VPN:
Inside VPN:
Profile: profile1
Transmitting entity: Initiator

Local IP: 1.1.1.1
Local ID type: IPV4_ADDR
Local ID: 1.1.1.1

Remote IP: 2.2.2.1

```
    Remote ID type: IPV4_ADDR
    Remote ID: 2.2.2.1

    Authentication-method: PRE-SHARED-KEY
    Authentication-algorithm: MD5
    Encryption-algorithm: 3DES-CBC

    Life duration(sec): 86400
    Remaining key duration(sec): 85632
    Exchange-mode: Main
    Diffie-Hellman group: Group 1
    NAT traversal: Not detected

    Extend authentication: Disabled
    Assigned IP address:

<RTA>display ipsec sa
<RTA>display ipsec sa
-------------------------------
Interface: GigabitEthernet0/1
-------------------------------

  -----------------------------
  IPsec policy: policy1
  Sequence number: 1
  Mode: ISAKMP
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Path MTU: 1428
    Tunnel:
        local    address: 1.1.1.1
```

```
    remote address: 2.2.2.1
  Flow:
    sour addr: 192.168.1.0/255.255.255.0    port: 0    protocol: ip
    dest addr: 192.168.2.0/255.255.255.0    port: 0    protocol: ip

  [Inbound ESP SAs]
    SPI: 2415685184 (0x8ffc6e40)
    Connection ID: 12884901889
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/2777
    Max received sequence-number: 4
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for NAT traversal: N
    Status: Active

  [Outbound ESP SAs]
    SPI: 3646540216 (0xd959c9b8)
    Connection ID: 12884901888
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/2777
    Max sent sequence-number: 4
    UDP encapsulation used for NAT traversal: N
    Status: Active

<RTB>display ike sa
<RTB>display ike sa
  Connection-ID     Remote                Flag          DOI
-------------------------------------------------------------------
  2                 1.1.1.1               RD            IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY

<RTB>display ike sa verbose
```

```
<RTB>display ike sa verbose
    ---------------------------------------------
    Connection ID: 2
    Outside VPN:
    Inside VPN:
    Profile: profile1
    Transmitting entity: Responder
    ---------------------------------------------
    Local IP: 2.2.2.1
    Local ID type: IPV4_ADDR
    Local ID: 2.2.2.1

    Remote IP: 1.1.1.1
    Remote ID type: IPV4_ADDR
    Remote ID: 1.1.1.1

    Authentication-method: PRE-SHARED-KEY
    Authentication-algorithm: MD5
    Encryption-algorithm: 3DES-CBC

    Life duration(sec): 86400
    Remaining key duration(sec): 85506
    Exchange-mode: Main
    Diffie-Hellman group: Group 1
    NAT traversal: Not detected

    Extend authentication: Disabled
    Assigned IP address:

<RTB>display ipsec sa
<RTB>display ipsec sa
------------------------------
Interface: GigabitEthernet0/1
------------------------------

  ----------------------------
```

IPsec policy: policy1

Sequence number: 1

Mode: ISAKMP

Tunnel id: 0

Encapsulation mode: tunnel

Perfect Forward Secrecy:

Inside VPN:

Extended Sequence Numbers enable: N

Traffic Flow Confidentiality enable: N

Path MTU: 1428

Tunnel:

local address: 2.2.2.1

remote address: 1.1.1.1

Flow:

sour addr: 192.168.2.0/255.255.255.0 port: 0 protocol: ip

dest addr: 192.168.1.0/255.255.255.0 port: 0 protocol: ip

[Inbound ESP SAs]

SPI: 1971329230 (0x758018ce)

Connection ID: 4294967296

Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1

SA duration (kilobytes/sec): 1843200/3600

SA remaining duration (kilobytes/sec): 1843199/2592

Max received sequence-number: 4

Anti-replay check enable: Y

Anti-replay window size: 64

UDP encapsulation used for NAT traversal: N

Status: Active

[Outbound ESP SAs]

SPI: 316893198 (0x12e3680e)

Connection ID: 4294967297

Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1

SA duration (kilobytes/sec): 1843200/3600

SA remaining duration (kilobytes/sec): 1843199/2592

```
      Max sent sequence-number: 4
      UDP encapsulation used for NAT traversal: N
      Status: Active

----------------------------
IPsec policy: policy1
Sequence number: 1
Mode: ISAKMP
----------------------------
   Tunnel id: 0
   Encapsulation mode: tunnel
   Perfect Forward Secrecy:
   Inside VPN:
   Extended Sequence Numbers enable: N
   Traffic Flow Confidentiality enable: N
   Path MTU: 1428
   Tunnel:
        local   address: 2.2.2.1
        remote address: 1.1.1.1
   Flow:
        sour addr: 192.168.2.0/255.255.255.0    port: 0    protocol: ip
        dest addr: 192.168.1.0/255.255.255.0    port: 0    protocol: ip

   [Inbound ESP SAs]
     SPI: 3646540216 (0xd959c9b8)
     Connection ID: 4294967298
     Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
     SA duration (kilobytes/sec): 1843200/3600
     SA remaining duration (kilobytes/sec): 1843199/2677
     Max received sequence-number: 4
     Anti-replay check enable: Y
     Anti-replay window size: 64
     UDP encapsulation used for NAT traversal: N
     Status: Active

   [Outbound ESP SAs]
```

SPI: 2415685184 (0x8ffc6e40)
Connection ID: 4294967299
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/2677
Max sent sequence-number: 4
UDP encapsulation used for NAT traversal: N
Status: Active

出力は、期待される ISAKMP SA と IOsec SAs がすべて確立されたことを示しています。 RTA のインバウンド SA の SPI は RTB のアウトバウンド SA の SPI と一致し、RTA のアウトバウンド SA の SPI は RTA のインバウンド SA の SPI と一致します。 SAs は、同じ認証アルゴリズムと暗号化アルゴリズムを使用します。

手順 11：IPsec の動作を監視する

存在する全ての IPsec SA と ISAKMP SA をクリアする。
<RTA>reset ike sa
<RTA>reset ipsec sa

<RTB>reset ike sa
<RTB>reset ipsec sa

デバッグを有効にします。
<RTA>terminal monitor
The current terminal is enabled to display logs.
<RTA>terminal debugging
The current terminal is enabled to display debugging logs.
<RTA>debugging ike packet
<RTA>debugging ipsec packet

IPsec トンネルを確立するために PCA から PCB へ ping します。
<PCA>ping 192.168.2.2
Ping 192.168.2.2 (192.168.2.2): 56 data bytes, press CTRL_C to break
Request time out
56 bytes from 192.168.2.2: icmp_seq=1 ttl=253 time=2.000 ms
56 bytes from 192.168.2.2: icmp_seq=2 ttl=253 time=9.000 ms

56 bytes from 192.168.2.2: icmp_seq=3 ttl=253 time=2.000 ms
56 bytes from 192.168.2.2: icmp_seq=4 ttl=253 time=4.000 ms

デバッギング情報確認し、分析します。
<RTA>*Dec 27 10:59:36:781 2021 RTA IPSEC/7/PACKET:
Failed to find SA by SP, SP Index = 0, SP Convert-Seq = 65536.
*Dec 27 10:59:36:781 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Encryption algorithm is 3DES-CBC.
*Dec 27 10:59:36:781 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Hash algorithm is HMAC-MD5.
*Dec 27 10:59:36:781 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
DH group 1.
*Dec 27 10:59:36:781 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Authentication method is Pre-shared key.
*Dec 27 10:59:36:781 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Lifetime type is in seconds.
*Dec 27 10:59:36:781 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Life duration is 86400.
*Dec 27 10:59:36:781 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct transform payload for transform 1.
*Dec 27 10:59:36:781 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Constructed SA payload.
*Dec 27 10:59:36:781 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct NAT-T rfc3947 vendor ID payload.
*Dec 27 10:59:36:781 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct NAT-T draft3 vendor ID payload.
*Dec 27 10:59:36:782 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct NAT-T draft2 vendor ID payload.
*Dec 27 10:59:36:782 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct NAT-T draft1 vendor ID payload.
*Dec 27 10:59:36:782 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct XAUTH draft6 vendor ID payload.
*Dec 27 10:59:36:782 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Sending packet to 2.2.2.1 remote port 500, local port 500.
*Dec 27 10:59:36:782 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

I-Cookie: d5f7180aa563cf61
R-Cookie: 0000000000000000
next payload: SA
version: ISAKMP Version 1.0
exchange mode: Main
flags:
message ID: 0
length: 176
*Dec 27 10:59:36:782 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Sending an IPv4 packet.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received packet from 2.2.2.1 source port 500 destination port 500.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

I-Cookie: d5f7180aa563cf61
R-Cookie: 535bbbeaca951ab0
next payload: SA
version: ISAKMP Version 1.0
exchange mode: Main
flags:
message ID: 0
length: 116
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received ISAKMP Security Association Payload.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received ISAKMP Vendor ID Payload.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received ISAKMP Vendor ID Payload.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Process SA payload.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Check ISAKMP transform 1.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Encryption algorithm is 3DES-CBC.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
HASH algorithm is HMAC-MD5.

*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
DH group is 1.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Authentication method is Pre-shared key.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Lifetime type is 1.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Life duration is 86400.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Attributes is acceptable.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Process vendor ID payload.
*Dec 27 10:59:36:788 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct KE payload.
*Dec 27 10:59:36:789 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct NONCE payload.
*Dec 27 10:59:36:789 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct NAT-D payload.
*Dec 27 10:59:36:789 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct DPD vendor ID payload.
*Dec 27 10:59:36:789 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Sending packet to 2.2.2.1 remote port 500, local port 500.
*Dec 27 10:59:36:789 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

I-Cookie: d5f7180aa563cf61
R-Cookie: 535bbbeaca951ab0
next payload: KE
version: ISAKMP Version 1.0
exchange mode: Main
flags:
message ID: 0
length: 208

構成ファイル

- RTA
  #

```
 sysname RTA
#
ospf 1
 area 0.0.0.0
  network 1.1.1.0 0.0.0.255
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 1.1.1.1 255.255.255.0
 ipsec apply policy policy1
#
 ip route-static 192.168.2.0 24 1.1.1.2
#
acl advanced 3000
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
#
ipsec transform-set trans1
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm sha1
#
ipsec policy policy1 1 isakmp
 transform-set trans1
 security acl 3000
 remote-address 2.2.2.1
 ike-profile profile1
#
ike profile profile1
 keychain keychain1
 local-identity address 1.1.1.1
 match remote identity address 2.2.2.1 255.255.255.0
 proposal 1
#
```

```
ike proposal 1
  encryption-algorithm 3des-cbc
  authentication-algorithm md5
#
ike keychain keychain1
  pre-shared-key address 2.2.2.1 255.255.255.0 key simple h3c
 #
```

- RTB

```
#
 sysname RTB
#
ospf 1
 area 0.0.0.0
  network 2.2.2.0 0.0.0.255
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 2.2.2.1 255.255.255.0
 ipsec apply policy policy1
#
 ip route-static 192.168.1.0 24 2.2.2.2
#
acl advanced 3000
 rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
ipsec transform-set trans1
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm sha1
#
ipsec policy policy1 1 isakmp
 transform-set trans1
 security acl 3000
 remote-address 1.1.1.1
 ike-profile profile1
#
ike profile profile1
 keychain keychain1
 local-identity address 2.2.2.1
 match remote identity address 1.1.1.1 255.255.255.0
```

```
 proposal 1
#
ike proposal 1
 encryption-algorithm 3des-cbc
 authentication-algorithm md5
#
ike keychain keychain1
 pre-shared-key address 1.1.1.1 255.255.255.0 key simple h3c
#
```

- SWA

```
#
 sysname SWA
#
ospf 1
 area 0.0.0.0
  network 1.1.1.0 0.0.0.255
  network 2.2.2.0 0.0.0.255
#
vlan 1
#
vlan 2
#
interface Vlan-interface1
 ip address 1.1.1.2 255.255.255.0
#
interface Vlan-interface2
 ip address 2.2.2.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
```