IPsecVPN の設定(IKE aggressive 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 アグレッシブモード、事前共有鍵認証方式を習得します。
  このラボタスクでは、IKE ネゴシエーションを介して RTA と RTB の間に IPsec トンネルを確立する方法と、フェーズ 1 でアグレッシブモード(VPN の対向の IP アドレスが動的に設定される環境ではアグレッシブモード)を使用するように IKE を構成する方法を示します。

ネットワーク図

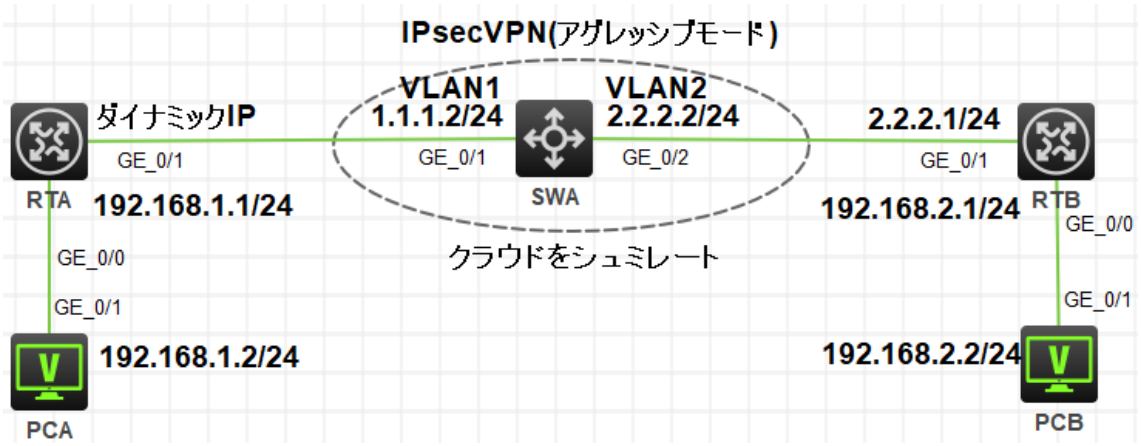

図 4.1 実習ネットワーク

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

手順 1：IP アドレスを設定する

表 3-3 にように IP アドレスを割り当てます。PCA のデフォルトゲートウェイとして RTA、そして PCB のデフォルトゲートウェイを RTB と設定します。

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

表 3-3 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	ダイナミックに IP アドレスを取得	-
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

SWA, RTB に以下のように OSPF を設定します。

[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。

ルーターB 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。
[RTB]ip route-static 192.168.1.0 255.255.255.0 2.2.2.2

手順 3: 公共のネットワーク接続を設定します

[SWA]dhcp enable
[SWA]dhcp server ip-pool 1
[SWA-dhcp-pool-1]network 1.1.1.0 mask 255.255.255.0
[SWA-dhcp-pool-1]gateway-list 1.1.1.2
[SWA-dhcp-pool-1]quit

[RTA]interface GigabitEthernet 0/1
[RTA-GigabitEthernet0/1]ip address dhcp-alloc
[RTA-GigabitEthernet0/1]quit

RTA のルーティング情報を表示します。この結果は RTA が IP アドレスとデフォルトルートを取得していることを表しています。
[RTA]display ip routing-table
Destinations : 17 Routes : 17

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/0	Static	70	0	1.1.1.2	GE0/1
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
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
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

PCA から PCB へ ping します。PCA が何もプライベートネットワークへのルートを持っていないため、PCB への ping はできません。

```
<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
```

手順 4：IKE Proposal を設定します

```
[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 5：IKE identify を設定します

[RTA]ike identity fqdn rta

[RTB]ike identity fqdn rtb

手順 6：IKE keychain を設定します

[RTA]ike keychain keychain1

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

[RTA-ike-keychain-keychain1]quit

[RTB]ike keychain keychain1

[RTB-ike-keychain-keychain1]pre-shared-key hostname rta key simple h3c

[RTB-ike-keychain-keychain1]quit

手順 7：IKE Profile を設定します

[RTA]ike profile profile1

[RTA-ike-profile-profile1]exchange-mode aggressive

[RTA-ike-profile-profile1]match remote identity fqdn rtb

[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]exchange-mode aggressive

[RTB-ike-profile-profile1]match remote identity fqdn rta

[RTB-ike-profile-profile1]keychain keychain1

[RTB-ike-profile-profile1]proposal 1

[RTB-ike-profile-profile1]quit

手順 8：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 9：IPsec Proposal を設定します

[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 10：IPsec Policy を設定して適用します

両方のルーターで IPsec Policy を設定し、それを隣接する装置に接続されているインタフェースへ適用します。
[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

応答者としての RTB は、対抗側の IP アドレスを取得できないため、テンプレートとして構成する必要があります。
[RTB]ipsec policy-template template1 1
[RTB-ipsec-policy-template-template1-1]security acl 3000

[RTB-ipsec-policy-template-template1-1]transform-set trans1
[RTB-ipsec-policy-template-template1-1]ike-profile profile1
[RTB-ipsec-policy-template-template1-1]quit
[RTB]ipsec policy policy1 1 isakmp template template1
[RTB]interface GigabitEthernet 0/1
[RTB-GigabitEthernet0/1]ipsec apply policy policy1
[RTB-GigabitEthernet0/1]quit

手順 11: 設定を確認します

RTA と RTB で display コマンドを使い設定情報を表示します。

```
<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:    trans1
  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 policy-template
-------------------------------------------
IPsec Policy Template: template1
-------------------------------------------

  ----------------------------
  Sequence number: 1
  ----------------------------
  Traffic Flow Confidentiality: Disabled
  Security data flow : 3000
  Selector mode: standard
  Local address:
  IKE profile: profile1
  IKEv2 profile:
  Remote address:
```

Transform set: trans1

IPsec SA local duration(time based):

IPsec SA local duration(traffic based):

SA idle time:

[RTB]display ipsec policy

IPsec Policy: policy1

Interface: GigabitEthernet0/1

Sequence number: 1

Mode: Template

Policy template name: template1

手順 12:トンネルが確立されていて稼働しているかを確認します

PCA から PCB に ping して両方の PC 間の接続性を確認します。

<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=1.000 ms

56 bytes from 192.168.2.2: icmp_seq=3 ttl=253 time=1.000 ms

56 bytes from 192.168.2.2: icmp_seq=4 ttl=253 time=1.000 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。 最初のリクエストがタイムアウトする前に IPsec SAs が利用できなかったためです。 最初の要求は破棄され、後続のすべての要求は 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

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

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

    Local IP: 1.1.1.1
    Local ID type: FQDN
    Local ID: rta

    Remote IP: 2.2.2.1
    Remote ID type: FQDN
    Remote ID: rtb

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

    Life duration(sec): 86400
    Remaining key duration(sec): 86080
    Exchange-mode: Aggressive
    Diffie-Hellman group: Group 1
    NAT traversal: Not detected
    Extend authentication: Disabled
    Assigned IP address:
この出力結果は IKE がアグレッシブモードでの認証をしたことを表しています。
<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: 3943816766 (0xeb11de3e)
    Connection ID: 12884901888
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3269
    Max received sequence-number: 9
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for NAT traversal: N
    Status: Active

  [Outbound ESP SAs]
    SPI: 2248163441 (0x86004071)
    Connection ID: 4294967297
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 1843200/3600
```

```
    SA remaining duration (kilobytes/sec): 1843199/3269
    Max sent sequence-number: 9
    UDP encapsulation used for NAT traversal: N
    Status: Active

<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
  ----------------------------------------------
  Connection ID: 2
  Outside VPN:
  Inside VPN:
  Profile: profile1
  Transmitting entity: Responder
  ----------------------------------------------
  Local IP: 2.2.2.1
  Local ID type: FQDN
  Local ID: rtb

  Remote IP: 1.1.1.1
  Remote ID type: FQDN
  Remote ID: rta

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

  Life duration(sec): 86400
  Remaining key duration(sec): 85645
  Exchange-mode: Aggressive
  Diffie-Hellman group: Group 1
```

NAT traversal: Not detected

Extend authentication: Disabled
Assigned IP address:

この出力結果は ISAKMP SA がアグレッシブモードで認証されたことを表しています。

```
<RTB>display ipsec sa
-------------------------------
Interface: GigabitEthernet0/1
-------------------------------
  -----------------------------
  IPsec policy: policy1
  Sequence number: 1
  Mode: Template
  -----------------------------
    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: 2248163441 (0x86004071)
      Connection ID: 4294967296
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/2792
      Max received sequence-number: 9
      Anti-replay check enable: Y
      Anti-replay window size: 64
```

UDP encapsulation used for NAT traversal: N
Status: Active

[Outbound ESP SAs]
SPI: 3943816766 (0xeb11de3e)
Connection ID: 4294967297
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/2792
Max sent sequence-number: 9
UDP encapsulation used for NAT traversal: N
Status: Active

手順 13：IPsec の操作を監視します

存在する全ての IPsec SAs と ISAKMP SAs をクリアします。

```
<RTA>reset ike sa
<RTA>reset ipsec sa

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

デバッギングを有効にします

```
<RTA>debugging ike packet
<RTA>debugging ipsec packet
```

IPsec トンネルを確立するのをトリガーするために 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=5.000 ms
56 bytes from 192.168.2.2: icmp_seq=2 ttl=253 time=4.000 ms
56 bytes from 192.168.2.2: icmp_seq=3 ttl=253 time=3.000 ms
56 bytes from 192.168.2.2: icmp_seq=4 ttl=253 time=3.000 ms
```

デバッギング情報確認し、分析します。

```
<RTA>*Dec 27 17:41:06:235 2021 RTA IPSEC/7/PACKET:
```

Failed to find SA by SP, SP Index = 0, SP Convert-Seq = 65536.
*Dec 27 17:41:06:235 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 17:41:06:235 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 17:41:06:235 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
DH group 1.
*Dec 27 17:41:06:235 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 17:41:06:235 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 17:41:06:235 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Life duration is 86400.
*Dec 27 17:41:06:235 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 17:41:06:235 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Constructed SA payload.
*Dec 27 17:41:06:241 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct KE payload.
*Dec 27 17:41:06:242 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct NONCE payload.
*Dec 27 17:41:06:242 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Local ID type: FQDN (2).
*Dec 27 17:41:06:242 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Local ID value: rta.
*Dec 27 17:41:06:242 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct ID payload.
*Dec 27 17:41:06:242 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 17:41:06:242 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 17:41:06:242 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 17:41:06:242 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 17:41:06:242 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 17:41:06:242 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 17:41:06:242 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 17:41:06:242 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
I-Cookie: bcded72f665242bf
R-Cookie: 0000000000000000
next payload: SA
version: ISAKMP Version 1.0
exchange mode: Aggressive
flags:
message ID: 0
length: 328
*Dec 27 17:41:06:242 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Sending an IPv4 packet.
*Dec 27 17:41:06:251 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 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
I-Cookie: bcded72f665242bf
R-Cookie: f74c3eafc3262c64
next payload: SA
version: ISAKMP Version 1.0
exchange mode: Aggressive
flags:
message ID: 0
length: 328
*Dec 27 17:41:06:251 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 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received ISAKMP Key Exchange Payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received ISAKMP Nonce Payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received ISAKMP Identification Payload.
*Dec 27 17:41:06:251 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 17:41:06:251 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 17:41:06:251 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 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received ISAKMP NAT-D Payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received ISAKMP NAT-D Payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received ISAKMP Hash Payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Process NONCE payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Process KE payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Process ID payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Peer ID type: FQDN (2).
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Peer ID value: FQDN rtb.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Process SA payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Check ISAKMP transform 1.
*Dec 27 17:41:06:251 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 17:41:06:251 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 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
  DH group is 1.
*Dec 27 17:41:06:251 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 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
  Lifetime type is 1.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

Life duration is 86400.

*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Attributes is acceptable.

*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Process vendor ID payload.

*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received 2 NAT-D payload.

*Dec 27 17:41:06:256 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Verify HASH payload.

*Dec 27 17:41:06:256 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
HASH:
df75edf4 8f4bc628 a283abd1 b255633c

*Dec 27 17:41:06:256 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct NAT-D payload.

*Dec 27 17:41:06:256 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
HASH:
6a243a4a 79b85851 5372998f fdbfa6a1

*Dec 27 17:41:06:256 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct authentication by pre-shared-key.

*Dec 27 17:41:06:256 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct INITIAL-CONTACT payload.

*Dec 27 17:41:06:256 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Encrypt the packet.

*Dec 27 17:41:06:256 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 17:41:06:256 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
I-Cookie: bcded72f665242bf
R-Cookie: f74c3eafc3262c64
next payload: NAT-D
version: ISAKMP Version 1.0
exchange mode: Aggressive
flags: ENCRYPT
message ID: 0
length: 116

*Dec 27 17:41:06:256 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

構成ファイル

- RTA

```
#
 sysname RTA
#
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 dhcp-alloc
 ipsec apply policy policy1
#
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 identity fqdn rta
#
ike profile profile1
 keychain keychain1
 exchange-mode aggressive
 match remote identity fqdn rtb
 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
  #
  vlan 1
  #
  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-template template1 1
  transform-set trans1
  security acl 3000
  ike-profile profile1
  #
  ipsec policy policy1 1 isakmp template template1
  #
  ike identity fqdn rtb

```
#
ike profile profile1
 keychain keychain1
 exchange-mode aggressive
 match remote identity fqdn rta
 proposal 1
#
ike proposal 1
 encryption-algorithm 3des-cbc
 authentication-algorithm md5
#
ike keychain keychain1
 pre-shared-key hostname rta 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
#
 dhcp enable
#
vlan 1
#
vlan 2
#
dhcp server ip-pool 1
 gateway-list 1.1.1.2
 network 1.1.1.0 mask 255.255.255.0
#
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
 #
```