【YAMAHAルーターとのインターネットVPN(IPsec IKEv2)】

インターネットVPN(IPsec IKEv2)でセンター(YAMAHA RTX830) ― 拠点(Si-R G)間を接続する設定例です。

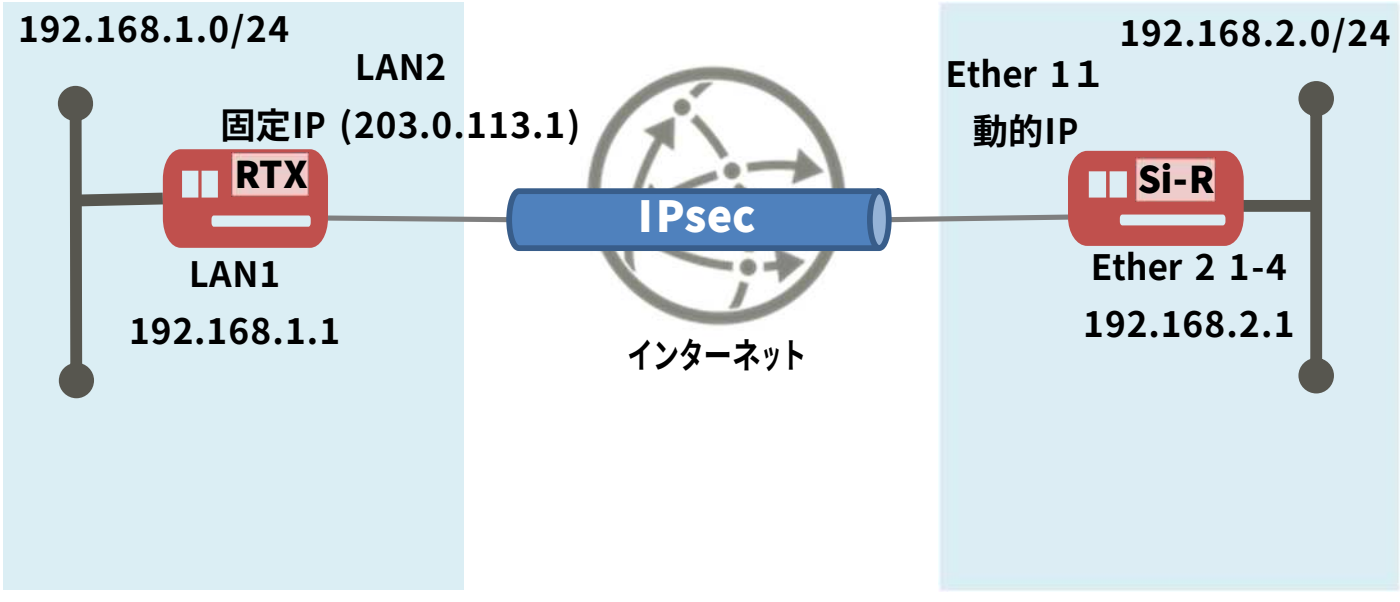
センター(RTX830)はPPPoE 固定1IP回線、拠点(Si-R G120)はPPPoE 動的IP回線を使用し、センター拠点間をIPsec(IKEv2)で接続します。
※本設定例は、弊社で独自に接続試験を行った結果を元に作成しております。

[対象機種と版数]

- Si-R Gシリーズ V20.52以降
- YAMAHA RTX830 Rev.15.02.29

[設定内容]

- RTX830のlan2をWAN側、lan1をLAN側とします。
- Si-R G120のether 1 1をWAN側、ether 2 1-8をLAN側とします。
- RTX830のLAN側に192.168.1.1/24を割り当てます。
- Si-RのLAN側に192.168.2.1/24を割り当てます。
- RTX830にはプロバイダより203.0.113.1の固定IPアドレスが割りてられるものとします。
- インターネットVPN(IPsec IKEv2)でセンター拠点間を接続します。



[設定]

以下の設定例を、コピー&ペーストでご利用いただくことができます。

- id-a@ispにはRTX830のISPのIDを設定してください。
- pwd-a@ispにはRTX830のISPのパスワードを設定してください。
- id-b@ispにはSi-RのISPのIDを設定してください。
- pwd-b@ispにはSi-RのISPのパスワードを設定してください。
- kyoten1にはSi-RのIPsecのID（装置識別情報）を設定してください。
- testにはIPsec共通鍵を設定してください。

■ RTX830設定例

```
ip route default gateway pp 1
ip route 192.168.2.0/24 gateway tunnel 1
ip lan1 address 192.168.1.1/24
pp select 1
 pp always-on on
 pppoe use lan2
 pp auth accept pap chap
 pp auth myname id-a@isp pwd-a@isp
 ppp lcp mru on 1454
 ppp ccp type none
 ip pp address 203.0.113.1/32
 ip pp mtu 1454
 ip pp nat descriptor 1
 pp enable 1
tunnel select 1
 ipsec tunnel 101
  ipsec sa policy 101 1 esp
  ipsec ike version 1 2
  ipsec ike duration child-sa 1 3600
  ipsec ike duration ike-sa 1 28800
  ipsec ike keepalive use 1 on dpd 10 6
  ipsec ike local address 1 192.168.1.1
  ipsec ike local name 1 203.0.113.1 ipv4-addr
  ipsec ike pre-shared-key 1 text test
  ipsec ike remote address 1 any
  ipsec ike remote name 1 kyoten1 fqdn
 ip tunnel tcp mss limit auto
 tunnel enable 1
nat descriptor type 1 masquerade
nat descriptor address outer 1 203.0.113.1
nat descriptor masquerade static 1 1 192.168.1.1 udp 500
nat descriptor masquerade static 1 2 192.168.1.1 esp
ipsec auto refresh on
```

■ Si-R G120設定

```
ether 1 1 vlan untag 1
ether 2 1-4 vlan untag 2
lan 1 ip address 192.168.2.1/24 3
lan 1 vlan 2
remote 0 name PPPoE
remote 0 mtu 1454
remote 0 ap 0 name PPPoE
remote 0 ap 0 datalink bind vlan 1
remote 0 ap 0 ppp auth send id-b@isp pwd-b@isp
remote 0 ap 0 keep connect
remote 0 ppp ipcp vjcomp disable
remote 0 ip route 0 203.0.113.1/32 1 1
remote 0 ip nat mode multi any 1 5m
remote 0 ip nat static 0 192.168.2.1 500 any 500 17
remote 0 ip nat static 1 192.168.2.1 any any any 50
remote 0 ip msschange 1414
remote 1 name RTX
remote 1 ap 0 name RTX
remote 1 ap 0 datalink type ipsec
remote 1 ap 0 ipsec type ikev2
remote 1 ap 0 ipsec ike protocol esp
remote 1 ap 0 ipsec ike encrypt aes-cbc-256
remote 1 ap 0 ipsec ike auth hmac-sha256
remote 1 ap 0 ipsec ike pfs modp2048
remote 1 ap 0 ipsec ike lifetime 1h
remote 1 ap 0 ipsec ike esn disable
remote 1 ap 0 ike local-idtype fqdn
remote 1 ap 0 ike remote-idtype address
remote 1 ap 0 ike name local kyoten1
remote 1 ap 0 ike shared key text test
remote 1 ap 0 ike proposal 0 encrypt aes-cbc-256
remote 1 ap 0 ike proposal 0 hash hmac-sha256
remote 1 ap 0 ike proposal 0 pfs modp2048
remote 1 ap 0 ike proposal 0 prf hmac-sha256
remote 1 ap 0 ike proposal 0 lifetime 8h
remote 1 ap 0 ike remote-id-send enable
remote 1 ap 0 ike initial connect
remote 1 ap 0 ike dpd use on
remote 1 ap 0 ike dpd retry 1s 6
remote 1 ap 0 tunnel remote 203.0.113.1
remote 1 ap 0 sessionwatch address 192.168.2.1 192.168.1.1
remote 1 ip route 0 default 1 1
remote 1 ip msschange 1350
syslog facility 23
time zone 0900
resource system vlan 4089-4094
consoleinfo autologout 8h
telnetinfo autologout 5m
terminal charset SJIS
```

[解説]

■ RTX830設定解説

ip route default gateway pp 1
デフォルトルートをpp1向きに設定します。

ip route 192.168.2.0/24 gateway tunnel 1
拠点側LANへのルートをtunnel1向きに設定します。

ip lan1 address 192.168.1.1/24
lan1にIPアドレスを設定します。

pp select 1
pp1インターフェースの設定を行います。

pp always-on on
常時接続の設定をします。

pppoe use lan2
lan2側(WAN側)に対してPPPoE を使用するよう設定します。

pp auth accept pap chap
pap chapによる認証情報を設定します。

pp auth myname id-a@isp pwd-a@isp
インターネット用プロバイダの認証ID、パスワードを設定します。

ppp lcp mru on 1454
LCP のネゴシエーションでMaximum-Receive-Unit オプションを使用し、パケットの最大長を制限します。

ppp ccp type none
圧縮機能はPPPoE では使用できません。none に設定する必要があります。

ip pp address 203.0.113.1/32
プロバイダから割り当てられたIPアドレスを設定します。

ip pp mtu 1454
フレッツ光ネクストではMTU長を1454byteに設定します。

ip pp nat descriptor 1
NATディスクリプターを割り当てます。

pp enable 1
pp1インターフェースを有効化します。

tunnel select 1
tunnel1インターフェースの設定を行います。

ipsec tunnel 101
tunnel1インターフェースで使用するSAのポリシーを設定します。

ipsec sa policy 101 1 esp
SAのポリシーを定義します。自動鍵交換用IPsec情報を以下のように設定します。
- セキュリティプロトコル：ESP(暗号)

ipsec ike duration child-sa 1 3600
自動鍵交換用IPsec情報のSA 有効時間を1時間に設定します。

ipsec ike duration ike-sa 1 28800
IKEv2情報のSA 有効時間を8時間に設定します。

ipsec ike keepalive use 1 on dpd 10 6
DPD監視の設定をします。

ipsec ike local address 1 192.168.1.1
IPSecトンネルの送信元アドレスの設定をします。

ipsec ike local name 1 203.0.113.1 ipv4-addr
IKEv2情報の自装置識IDを設定します。

ipsec ike pre-shared-key 1 text test
IKEv2セッション確立時の共有鍵（Pre-shared key）を設定します。

ipsec ike remote address 1 any
相手装置のアドレスをanyに設定します。

ipsec ike remote name 1 kyoten1 fqdn
IKEv2情報の相手置識IDを設定します。

ip tunnel tcp mss limit auto
MSS書き換えを設定します。

tunnel enable 1
tunnel1インターフェースを有効化します。

nat descriptor type 1 masquerade
NATディスクリプターを定義します。

nat descriptor address outer 1 203.0.113.1
NATの外側IPアドレスを設定します。

nat descriptor masquerade static 1 1 192.168.1.1 udp 500
nat descriptor masquerade static 1 2 192.168.1.1 esp
スタティックNATにより、IKEパケットとESPパケットを通す設定をします。

ipsec auto refresh on
SAを自動更新するように設定します。

■ Si-R G120設定解説

ether 1 1 vlan untag 1
Ether 1 1インタフェースにVLAN1を割り当てます。

ether 2 1-4 vlan untag 2
Ether 2 1-4インタフェースにVLAN1を割り当てます。

lan 1 ip address 192.168.2.1/24 3
LAN1側にIPアドレスを設定します。

lan 1 vlan 2
VLAN ID とlan 定義番号の関連付けを行います。

remote 0 name PPPoE
インターネット接続用インターフェースに名前(任意)を設定します。

remote 0 mtu 1454
フレッツ光ネクストではMTU長を1464byteに設定します。

remote 0 ap 0 name PPPoE
アクセスポイントの名前（任意、remote nameと同じでも可）を設定します。

remote 0 ap 0 datalink bind vlan 1
VLAN IDとremote定義番号の関連付けを行います。

remote 0 ap 0 ppp auth send id-b@isp pwd-b@isp
インターネット用プロバイダーの認証ID、パスワードを設定します。

remote 0 ap 0 keep connect
インターネットへ常時接続します。

remote 0 ppp ipcp vjcomp disable
VJヘッダー圧縮を使用しない設定にします。

remote 0 ip route 0 203.0.113.1/32 1 1
センターへのスタティックルートを設定します。

remote 0 ip nat mode multi any 1 5m
マルチNATを設定します。

remote 0 ip nat static 0 192.168.2.1 500 any 500 17
スタティックNATにより、IKEパケットを通す設定をします。

remote 0 ip nat static 1 192.168.2.1 any any any 50
スタティックNATにより、ESPパケットを通す設定をします。

remote 0 ip msschange 1414
MSS書き換えを設定します。

remote 1 name RTX
IPsecインターフェースの名前(任意)を設定します。

remote 1 ap 0 name RTX
アクセスポイントの名前（任意、remote nameと同じでも可）を設定します。

remote 1 ap 0 datalink type ipsec
パケット転送方法としてIPsecを設定します。

remote 1 ap 0 ipsec type ikev2
IPsec情報のタイプにIPsec自動鍵交換(IKE Version2)を設定します。

remote 1 ap 0 ipsec ike protocol esp
自動鍵交換用IPsec情報のセキュリティプロトコルにESP（暗号）を設定します。

remote 1 ap 0 ipsec ike encrypt aes-cbc-256
自動鍵交換用IPsec情報の暗号情報にAES256を設定します。

remote 1 ap 0 ipsec ike auth hmac-sha256
自動鍵交換用IPsec情報の認証情報にSHA256を設定します。

remote 1 ap 0 ipsec ike pfs modp2048
自動鍵交換用IPsec情報のPFS使用時のDH（Diffie-Hellman）グループにmodp2048を設定します。

remote 1 ap 0 ipsec ike lifetime 1h
自動鍵交換用IPsec情報のSA 有効時間を1時間に設定します。

remote 1 ap 0 ipsec ike esn disable
ENS(拡張シーケンス番号）を使用しないように設定します。

remote 1 ap 0 ike local-idtype fqdn
IKEv2情報の自装置IDタイプをFQDNに設定します。

remote 1 ap 0 ike remote-idtype address
IKEv2情報の相手装置IDタイプをアドレスに設定します。

remote 1 ap 0 ike name local kyoten1
IKEv2情報の自装置識IDを設定します。

remote 1 ap 0 ike shared key text test
IKEv2セッション確立時の共有鍵（Pre-shared key）を設定します。

remote 1 ap 0 ike proposal 0 encrypt aes-cbc-256
IKEv2セッション用暗号情報の暗号アルゴリズムにAES256を設定します。

remote 1 ap 0 ike proposal 0 hash hmac-sha256
IKEv2セッション用認証(ハッシュ)情報をSHA256に設定します。

remote 1 ap 0 ike proposal 0 pfs modp2048
IKEv2セッション用DH(Diffie-Hellman)グループにmodp2048を設定します。

remote 1 ap 0 ike proposal 0 prf hmac-sha256
IKEv2セッション用PRF(Pseudo Random Function)にSHA256を設定します。

remote 1 ap 0 ike proposal 0 lifetime 8h
IKEv2情報のSA 有効時間を8時間に設定します。

remote 1 ap 0 ike remote-id-send enable
IKEv2情報の相手装置ID送信を有効に設定します。

remote 1 ap 0 ike initial connect
対象回線の接続またはIPsec 対象パケットの送信を契機として、IPsec/IKE SAの確立動作を開始しするように設定します。

remote 1 ap 0 ike dpd use on
DPD(Dead Pear Detection)を有効に設定します。

remote 1 ap 0 ike dpd retry 1s 6
DPDの再送時間/回数の設定をします。

remote 1 ap 0 tunnel remote 203.0.113.1
IPsecトンネルの送信先アドレスとしてセンターのアドレスを設定します。

remote 1 ap 0 sessionwatch address 192.168.2.1 192.168.1.1
接続先セッション監視の設定をします。
192.168.2.1：ICMP ECHOパケットの送信元IPアドレスです。
192.168.1.1：ICMP ECHOパケットの宛先IPアドレスです。

remote 1 ip route 0 default 1 1
センター向きにデフォルトルートを設定します。

remote 1 ip msschange 1350
MSS書き換えの設定をします。

syslog facility 23
システムログ情報の出力対象ファシリティの設定をします。通常はこのままで構いません。

time zone 0900
タイムゾーンを設定します。通常はこのままで構いません。

resource system vlan 4089-4094
装置内部資源として予約するVLAN IDを設定します。通常はこのままで構いません。

consoleinfo autologout 8h
telnetinfo autologout 5m
シリアルコンソール、TELNETコネクションの入出力がない場合のコネクション切断時間を設定します。
通常はこの値で構いません。

terminal charset SJIS
ターミナルで使用する漢字コードをShift JISコードに設定します。