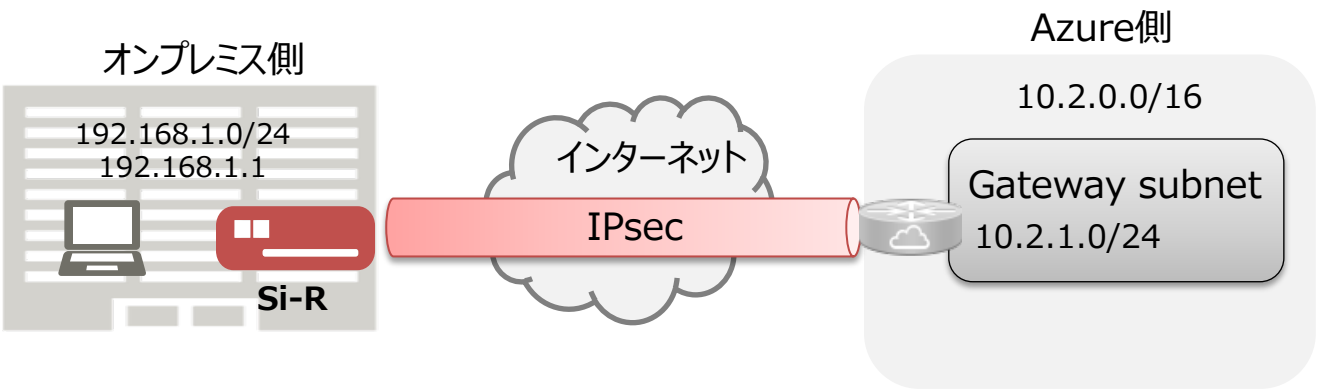
技術情報：Si-R Gシリーズ設定例
「Microsoft Azure」との接続（ルートベースIPsec）

Si-R Gシリーズで「Microsoft Azure」ルートベースIPsec接続する場合の設定例です。

Azure VPNゲートウェイ接続用のVPNデバイスとして、Microsoft社様と富士通共同でSi-R Gシリーズの検証を実施いたしました。
検証済みのVPNデバイスとデバイス構成ガイド
https://docs.microsoft.com/ja-jp/azure/vpn-gateway/vpn-gateway-about-vpn-devices

[対象機種と版数]
Si-R Gシリーズ　V20.14以降
Si-R Gシリーズ　V04.12以降

[設定内容]
・Si-R Gのether 1 1をWAN側、ether 2 1-4をLAN側とします。
・WAN側は、PPPoEで固定グローバルアドレスが1つ割り当てられるとします。
・Si-RLAN側に192.168.1.1/24を割り当てるとします。
・Azure側では、10.2.0.0/16の仮想ネットワークの中に、ゲートウェイサブネット10.2.1.0/24が存在するとします。
・IPv4 over IPv4 IPsec tunnelで拠点を接続します。



オンプレミス側ネットワーク

項目	環境情報
接続メディア	FTTHなど
接続プロトコル	PPPoE
WAN	固定グローバルアドレス(xxx.xxx.xxx.xxx)
LAN	192.168.1.0/24

オンプレミス側ネットワークでは、Si-RでPPPoE(アドレス固定)を行います。
固定のアドレスを使用して、Azureネットワークに対して、IPsec接続を動作させます。

Microsoft Azure側ネットワーク

サブネット名	アドレス範囲
Gateway subnet	10.2.1.0/24

Microsoft Azure 仮想ネットワークでは、10.2.0.0/16のアドレス空間の中に、1つのサブネットが存在します。

Copyright 2022 FUJITSU LIMITED

オンプレミス(Si-R)での設定
本章では、Microsoft AzureとIPsec接続するためのSi-Rの設定について解説します。

Azure側の設定については以下を参照ください。
https://docs.microsoft.com/ja-jp/azure/vpn-gateway/tutorial-site-to-site-portal
チュートリアル:Azure Portal でサイト間接続を作成する

IPsec設定項目
IPsec設定値については、以下のような内容になります。
Azure側のIPsec/IKEポリシー「規定」で設定される最優先パラメータ、かつSi-Rがサポートしているパラメータを指定しています。本パラメータ以外の設定を行う場合は、Azure側で「カスタム」に変更し、Si-Rと一致するパラメータを設定してください。

IKEフェーズ1

項目	設定値
自側トンネルエンドポイントアドレス	xxx.xxx.xxx.xxx
相手側トンネルエンドポイントアドレス	yyy.yyy.yyy.yyy ポータルサイトより確認
lan側ローカルアドレス	192.168.1.1/24
暗号情報	aes-cbc-256
認証(ハッシュ)情報	hmac-sha1
DHグループ	group 2(modp1024)
PRF(疑似乱数関数)	hmac-sha1
IKE SA有効時間	8h
NAT-TRAVERSAL	on
DPD	on
IKEセッション共有鍵	test ポータルサイトに設定した値を使用

IKEフェーズ2

項目	設定値
IPsec情報のセキュリティプロトコル	esp
暗号情報	aes-cbc-256
認証(ハッシュ)情報	hmac-sha1
IPsec SA 有効時間	1h
DHグループ	off
ESN(拡張シーケンス番号)	disable
IPsec対象範囲(送信元)	any
IPsec対象範囲(宛先)	any

Copyright 2022 FUJITSU LIMITED

config
configの全体像としては以下のような内容になります。
configは大きく分けて、etherポート定義、lan定義、PPPoE定義、IPsec定義に分けられます。それぞれについて順を追って説明していきます。

```
ether 1 1 vlan untag 1
ether 2 1-4 vlan untag 2
lan 1 ip address 192.168.1.1/24 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@isp pass@isp
remote 0 ap 0 keep connect
remote 0 ppp ipcp vjcomp disable
remote 0 ip address local xxx.xxx.xxx.xxx
remote 0 ip route 0 default 1 1
remote 0 ip nat mode multi any 1 5m
remote 0 ip nat static 0 xxx.xxx.xxx.xxx any xxx.xxx.xxx.xxx any 50
remote 0 ip nat static 1 xxx.xxx.xxx.xxx 500 xxx.xxx.xxx.xxx 500 17
remote 0 ip nat static 2 xxx.xxx.xxx.xxx 4500 xxx.xxx.xxx.xxx 4500 17
remote 0 ip msschange 1414
remote 1 name Azure
remote 1 ap 0 name IPsec
remote 1 ap 0 datalink type ipsec
remote 1 ap 0 keep connect
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-sha1
remote 1 ap 0 ipsec ike lifetime 1h
remote 1 ap 0 ipsec ike esn disable
remote 1 ap 0 ike local-idtype address
remote 1 ap 0 ike remote-idtype address
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-sha1
remote 1 ap 0 ike proposal 0 pfs modp1024
remote 1 ap 0 ike proposal 0 prf hmac-sha1
remote 1 ap 0 ike proposal 0 lifetime 8h
remote 1 ap 0 ike nat-traversal use on
remote 1 ap 0 ike dpd use on
remote 1 ap 0 tunnel local xxx.xxx.xxx.xxx
remote 1 ap 0 tunnel remote yyy.yyy.yyy.yyy
remote 1 ip route 0 10.2.0.0/16 1 1
remote 1 ip msschange 1350
syslog pri error,warn,info
syslog facility 23
time zone 0900
consoleinfo autologout 8h
telnetinfo autologout 5m
terminal charset SJIS
```


Copyright 2022 FUJITSU LIMITED

etherポートの設定
各etherポートにVLAN(untag)を割り当てます。これは、後のlan定義や、PPPoEの定義と結びつきます。

```
ether 1 1 vlan untag 1
ether 2 1-4 vlan untag 2
```

wan側のポートに対してvlan 1を、lan側のポートに対してvlan 2を設定します。

PPPoEの設定
WAN側にPPPoEの設定をします。PPPoEの送出先としてvlan 1(ether 1 1)を指定します。

```
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@isp pass@isp
remote 0 ap 0 keep connect
remote 0 ppp ipcp vjcomp disable
remote 0 ip address local xxx.xxx.xxx.xxx
remote 0 ip msschange 1414
```

項目	設定値
ID(PPPoE)	id@isp
PASS(PPPoE)	pass@isp

mtu値、mss値については回線により異なります。回線側にご確認ください。

```
remote 0 ip route 0 default 1 1
```

PPPoEのインタフェースに対してデフォルトルートを設定します。

ファイアウォールの設定
PPPoEの定義にファイアウォールの設定を追加します。

```
remote 0 ip nat mode multi any 1 5m
remote 0 ip nat static 0 xxx.xxx.xxx.xxx any xxx.xxx.xxx.xxx any 50
remote 0 ip nat static 1 xxx.xxx.xxx.xxx 500 xxx.xxx.xxx.xxx 500 17
remote 0 ip nat static 2 xxx.xxx.xxx.xxx 4500 xxx.xxx.xxx.xxx 4500 17
```

mode multiの設定により、NAPTの設定が有効になります。
IPsec/IKEパススルーの設定を行います。

lan側アドレスの設定
lan側のアドレスを192.168.1.1/24に設定します。このlanインタフェースはvlan 2の物理ポートと結びつきます。

```
lan 1 ip address 192.168.1.1/24 3
lan 1 vlan 2
```


Copyright 2022 FUJITSU LIMITED

IPsecの設定
まず、設定するインタフェースをIPsecができるようにするため、インタフェースの転送方式、IPsecタイプを設定します。
IPsecを常時接続に設定します。

```
remote 1 name Azure
remote 1 ap 0 name IPsec
remote 1 ap 0 datalink type ipsec
remote 1 ap 0 keep connect
```

IKEフェーズ1
IPsec設定項目：IKEフェーズ1表にて提示した内容を設定します。

```
remote 1 ap 0 ike local-idtype address
remote 1 ap 0 ike remote-idtype address
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-sha1
remote 1 ap 0 ike proposal 0 pfs modp1024
remote 1 ap 0 ike proposal 0 prf hmac-sha1
remote 1 ap 0 ike proposal 0 lifetime 8h
remote 1 ap 0 ike nat-traversal use on
remote 1 ap 0 ike dpd use on
remote 1 ap 0 tunnel local xxx.xxx.xxx.xxx
remote 1 ap 0 tunnel remote yyy.yyy.yyy.yyy
```

事前共有鍵(ike shared key)、相手側トンネルエンドポイント(tunnel remote)については、Microsoft Azureポータルサイトにて確認した内容を設定します。
lifetimeは、Azure側の値を超えないように設定してください。

IKEフェーズ2
IPsec設定項目：IKEフェーズ２表にて提示した内容を設定します。

```
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-sha1
remote 1 ap 0 ipsec ike lifetime 1h
remote 1 ap 0 ipsec ike esn disable
```

lifetimeは、Azure側の値を超えないように設定してください。
本設定例は、IPsec(IKEフェーズ2)のPFSグループはoff設定になってます。PFSグループの設定を行う場合、以下設定を追加ください。
例） remote 1 ap 0 ipsec ike pfs modp1024

Copyright 2022 FUJITSU LIMITED

その他
ルート設定、MSS値の設定をします。このMSS値はカプセル化の方式によって変わります。今回は1350を設定します。

```
remote 1 ip route 0 10.2.0.0/16 1 1
remote 1 ip msschange 1350
syslog pri error,warn,info
syslog facility 23
time zone 0900
consoleinfo autologout 8h
telnetinfo autologout 5m
terminal charset SJIS
```

Azure内の仮想サーバ等、ICMPに応答する装置（Azureの仮想ネットワークゲートウェイ宛は不可）がある場合は、接続先セッション監視の設定を追加することを推奨します。
例） remote 1 ap 0 sessionwatch address 192.168.1.1 a.a.a.a
（a.a.a.a→仮想サーバなど）

以上で設定が完了です。
最後に設定をsaveして再起動します。

```
save
reset
```


Copyright 2022 FUJITSU LIMITED

Si-Rを接続し、少し時間がたってからshow access-pointコマンドを実行して確認してください。正常にIPsecが確立できていれば下記のような結果が得られます。

```
#show access-point
remote 1 ap 0                 : Azure.IPsec
  status                      : connected
    since                     : Jul 4 11:41:29 2022
  speed                       : not available
    send traffic              : not available
    receive traffic           : not available
  type                        : IPsec/IKE
    IKE Version               : 2
    IKE SA                    : established
    IPsec SA                  : established
```

IKE SA,IPsec SAともにestablished、status connectedとなっていれば接続ができています。

Copyright 2022 FUJITSU LIMITED