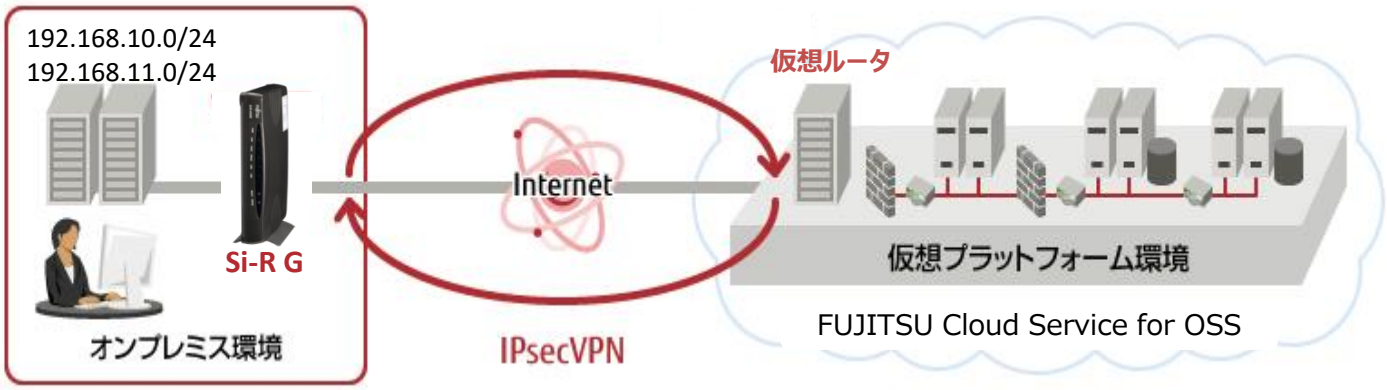
技術情報：Si-R/Si-R brinシリーズ設定例

「FUJITSU Cloud Service for OSS」との接続

Si-R Gシリーズで「FUJITSU Cloud Service for OSS」とIPsec接続する場合の設定例です。



[対象機種と版数]

Si-R Gシリーズ V2.13以降

[設定内容]

・Si-R Gのether 2 1-4 をLAN側とします。

・Si-R GのLAN側に192.168.10.1/24を割り当るとします。

・オンプレミス側ネットワーク
オンプレミス側ネットワークでは、固定のアドレスを使用して、FUJITSU Cloud Service for OSSネットワークに対して、IPsec接続を動作させます。

項目	設定値
接続メディア	FTTH/ADSLなど
VPN装置 グローバルIPアドレス	xxx.xxx.xxx.xxx/xx
VPN装置 ゲートウェイアドレス（ISP側）	xxx.xxx.xxx.xxz
VPN装置 ローカルIPアドレス	192.168.10.1/24

・FUJITSU Cloud Service for OSS側ネットワーク
オンプレミス側とFUJITSU Cloud Service for OSS側でのIPsec により、IPsec トンネルを介して、オンプレミスからFUJITSU Cloud Service for OSS側の仮想システムネットワークに対して通信を　することが可能となります。

項目	設定値
仮想ルータ グローバルIPアドレス	yyy.yyy.yyy.yyy
仮想ルータ ローカルIPアドレス	192.168.0.1/24
仮想サーバ IPアドレス	192.168.0.4

[FUJITSU Cloud Service for OSSの設定]

FUJITSU Cloud Service for OSSは、サービスポータル/APIを利用し、仮想リソースを配備・利用いただけるサービスです。
FUJITSU Cloud Service for OSSのIPsec VPNゲートウェイの設定につきましては、以下サイトを参照ください
http://jp.fujitsu.com/solutions/cloud/for_OSS/

オンプレミス環境のVPN装置（Si-R G）とfor OSSのIPsec VPNゲートウェイに設定する値は以下の通りです。

・IKE フェーズ1

項目	設定値	【for OSS設定範囲】 備考
IKE version	IKEv1	【IKEv1】 対向装置で同一値に設定
認証方式	事前共有鍵（pre-shared key）方式 認証鍵：secret	【事前共有鍵（pre-shared key）方式】 対向装置で同一値に設定
暗号情報	aes-cbc-256	【aes-cbc-128/192/256】 セキュリティ強度の高いものを選択 対向装置で同一値に設定
認証(ハッシュ)情報	hmac-sha1	【hmac-sha1】 対向装置で同一値に設定
DHグループ	group 14(modp2048)	【group 2/5/14】 セキュリティ強度の高いものを選択 対向装置で同一値に設定
モード	メインモード	【メインモード】 対向装置で同一値に設定
IKE SA有効時間	86400秒	【60～86400秒】 一般的な値に設定 対向装置で合わせることを推奨
keep alive （DPD）	無通信監視時間：10 秒 DPDアクション：restart（for OSS側設定） DPD検出タイムアウト：30秒（for OSS 側設定）	一般的な値に設定 対向装置で合わせることを推奨
イニシエータモード	bi-directional（for OSS側設定）	【bi-directional, response-only】 一般的な値に設定

・IKE フェーズ2

項目	設定値	【for OSS設定範囲】 備考
IPsec情報の セキュリティプロトコル	ESP	【ESP】 対向装置で同一値に設定
暗号情報	aes-cbc-256	【aes-cbc-128/192/256】 セキュリティ強度の高いものを選択 対向装置で同一値に設定
認証(ハッシュ)情報	hmac-sha1	【hmac-sha1】 対向装置で同一値に設定
DHグループ	group 14(modp2048)	【group 2/5/14】 セキュリティ強度の高いものを選択 対向装置で同一値に設定
モード	クイックモード	対向装置で同一値に設定
対象範囲 （range）	オンプレミス側：192.168.10.0/24(※1) 192.168.11.0/24(※1) for OSS側：192.168.0.0/24	対向装置で自側/相手側を反対に設定
IPsec SA有効時間	28800秒	【60～86400秒】 一般的な値に設定 対向装置で合わせることを推奨

※1 オンプレミス側の利用ネットワーク例。設定はオンプレミス側のアドレスレンジが自由に利用できるように考慮。
VPN装置 ：相手側レンジ（192.168.0.0/24）、自側レンジ（any）
仮想ルータ：相手側レンジ（0.0.0.0/0）、自側レンジ（192.168.0.0/24）

[設定例]

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。

Si-R G設定例

```
ether 1 1 vlan untag 1
ether 2 1-4 vlan untag 2
lan 0 ip address xxx.xxx.xxx.xxx/xx 3
lan 0 ip route 0 default xxx.xxx.xxx.xxz 1 1
lan 0 ip nat mode multi xxx.xxx.xxx.xxx 1 5m
lan 0 ip nat static 0 xxx.xxx.xxx.xxx any xxx.xxx.xxx.xxx any 50
lan 0 ip nat static 1 xxx.xxx.xxx.xxx 500 xxx.xxx.xxx.xxx 500 17
lan 0 ip nat static 2 xxx.xxx.xxx.xxx 22 xxx.xxx.xxx.xxx 22 6
lan 0 vlan 1
lan 2 ip address 192.168.10.1/24 3
lan 2 ip route 0 192.168.11.0/24 192.168.10.254 1 1
lan 2 vlan 2
remote 0 name OSS
remote 0 ap 0 name ipsec01
remote 0 ap 0 datalink type ipsec
remote 0 ap 0 keep connect
remote 0 ap 0 ipsec type ike
remote 0 ap 0 ipsec ike protocol esp
remote 0 ap 0 ipsec ike range any4 192.168.0.0/24
remote 0 ap 0 ipsec ike encrypt aes-cbc-256
remote 0 ap 0 ipsec ike auth hmac-sha1
remote 0 ap 0 ipsec ike pfs modp2048
remote 0 ap 0 ike shared key text secret
remote 0 ap 0 ike proposal 0 encrypt aes-cbc-256
remote 0 ap 0 ike proposal 0 hash hmac-sha1
remote 0 ap 0 ike proposal 0 pfs modp2048
remote 0 ap 0 ike initial connect
remote 0 ap 0 ike dpd use on
remote 0 ap 0 tunnel local xxx.xxx.xxx.xxx
remote 0 ap 0 tunnel remote yyy.yyy.yyy.yyy
remote 0 ap 0 sessionwatch address 192.168.10.1 192.168.0.4
remote 0 ip route 0 192.168.0.0/24 1 1
remote 0 ip msschange 1300
syslog pri error,warn,info
syslog facility 23
time zone 0900
consoleinfo autologout 8h
telnetinfo autologout 5m
terminal charset SJIS
```

[解説]

Si-R_G設定解説

ether 1 1 vlan untag 1
 ポートをTag なしVLAN1に設定します。

ether 2 1-4 vlan untag 2
 ポートをTag なしVLAN2に設定します。

lan 0 ip address xxx.xxx.xxx.xxx/xx 3
 WAN側IPアドレス（ISPより割当）を設定します。
 xxx.xxx.xxx.xxx/xx: WAN側のIPアドレス/マスクです。
 3 :ブロードキャストアドレスのタイプです。通常は3で構いません。

lan 0 ip route 0 default xxx.xxx.xxx.xxz 1 1
 FUJITSU Cloud Service for OSSへのスタティックルートを設定します。
 xxx.xxx.xxx.xxz ：ISP側ゲートウェイアドレスです。
 1：metric値です。通常は1で構いません。
 1：distance値です。通常は1で構いません。

lan 0 ip nat mode multi xxx.xxx.xxx.xxx 1 5m
 マルチNATの設定をします。

lan 0 ip nat static 0 xxx.xxx.xxx.xxx any xxx.xxx.xxx.xxx any 50
lan 0 ip nat static 1 xxx.xxx.xxx.xxx 500 xxx.xxx.xxx.xxx 500 17
lan 0 ip nat static 2 xxx.xxx.xxx.xxx 22 xxx.xxx.xxx.xxx 22 6
 スタティックNATにより、IKE,ESP,SSHパケットを通す設定をします。

lan 0 vlan 1
 VLAN ID とlan 定義番号の関連付けを行います。
 LAN0にTag なしVLAN1を設定します。

lan 2 ip address 192.168.10.1/24 3
 LAN側IPアドレスを設定します。
 192.168.10.1/24: LAN側のIPアドレス/マスクです。
 3 :ブロードキャストアドレスのタイプです。通常は3で構いません。

lan 2 ip route 0 192.168.11.0/24 192.168.10.254 1 1
 LAN側のスタティックルートを設定します。
 192.168.10.254 ：192.168.11.0/24のゲートウェイアドレスです。
 1：metric値です。通常は1で構いません。
 1：distance値です。通常は1で構いません。

lan 2 vlan 2
 VLAN ID とlan 定義番号の関連付けを行います。
 LAN2にTag なしVLAN2を設定します。

remote 0 name OSS
IPsecインタフェースの名前(任意)を設定します。

remote 0 ap 0 name ipsec01
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 type ipsec
パケット転送方法としてIPsecを設定します。

remote 0 ap 0 keep connect
常時接続します。

remote 0 ap 0 ipsec type ike
IPsec情報タイプにIPsec自動鍵交換を設定します。

remote 0 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 0 ap 0 ipsec ike range any4 192.168.0.0/24
自動鍵交換用IPsec 情報の対象範囲を設定します。
any4 : 送信元IPv4パケットを全てIPsec 対象とします。
192.168.0.0/24 : IPsec 対象となる宛先IPアドレス/マスクです。

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

remote 0 ap 0 ipsec ike auth hmac-sha1
自動鍵交換用IPsec情報の認証情報にSHA1を設定します。

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

remote 0 ap 0 ike proposal 0 encrypt aes-cbc-256
IKE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 0 ap 0 ike proposal 0 hash hmac-sha1
IKEセッション用認証情報にSHA1を設定します。

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

remote 0 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ます。

remote 0 ap 0 ike dpd use on
IKE でDPD を利用する設定を行います。

remote 0 ap 0 tunnel local xxx.xxx.xxx.xxx
IPsecトンネルの送信元アドレスの設定をします。

remote 0 ap 0 tunnel remote yyy.yyy.yyy.yyy
IPsecトンネルのあて先アドレスの設定をします。

remote 0 ap 0 sessionwatch address 192.168.10.1 192.168.0.4
接続先セッション監視の設定をします。
・192.168.10.1：ICMP ECHOパケットの送信元IPアドレスです。
・192.168.0.4：ICMP ECHOパケットの宛先IPアドレス（監視サーバ）です。

remote 0 ip route 0 192.168.0.0/24 1 1
FUJITSU Cloud Service for OSSへのスタティックルートを設定します。
192.168.0.0/24 :FUJITSU Cloud Service for OSS側ネットワークです。
1：metric値です。通常は1で構いません。
1：distance値です。通常は1で構いません。

remote 0 ip msschange 1300
MSS値に1300byteを設定します。

syslog pri error,warn,info
syslog facility 23
システムログ情報の出力情報／出力対象ファシリティを設定します。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。

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
このままで構いません。

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。

[IPsec確立確認方法]

オンプレミス側（Si-R Gシリーズ）での接続状況確認方法を示します。

1.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。
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。

```
Si-R G100(config)# show access-point
remote 0 ap 0      : ipsec01
  status           : connected
    since          : Nov 26 11:26:40 2015
  speed            : not available
    send traffic   : not available
    receive traffic : not available
  type             : IPsec/IKE
    IKE Version    : 1
    exchange type  : main
    IKE SA         : established
    IPsec SA       : established
```