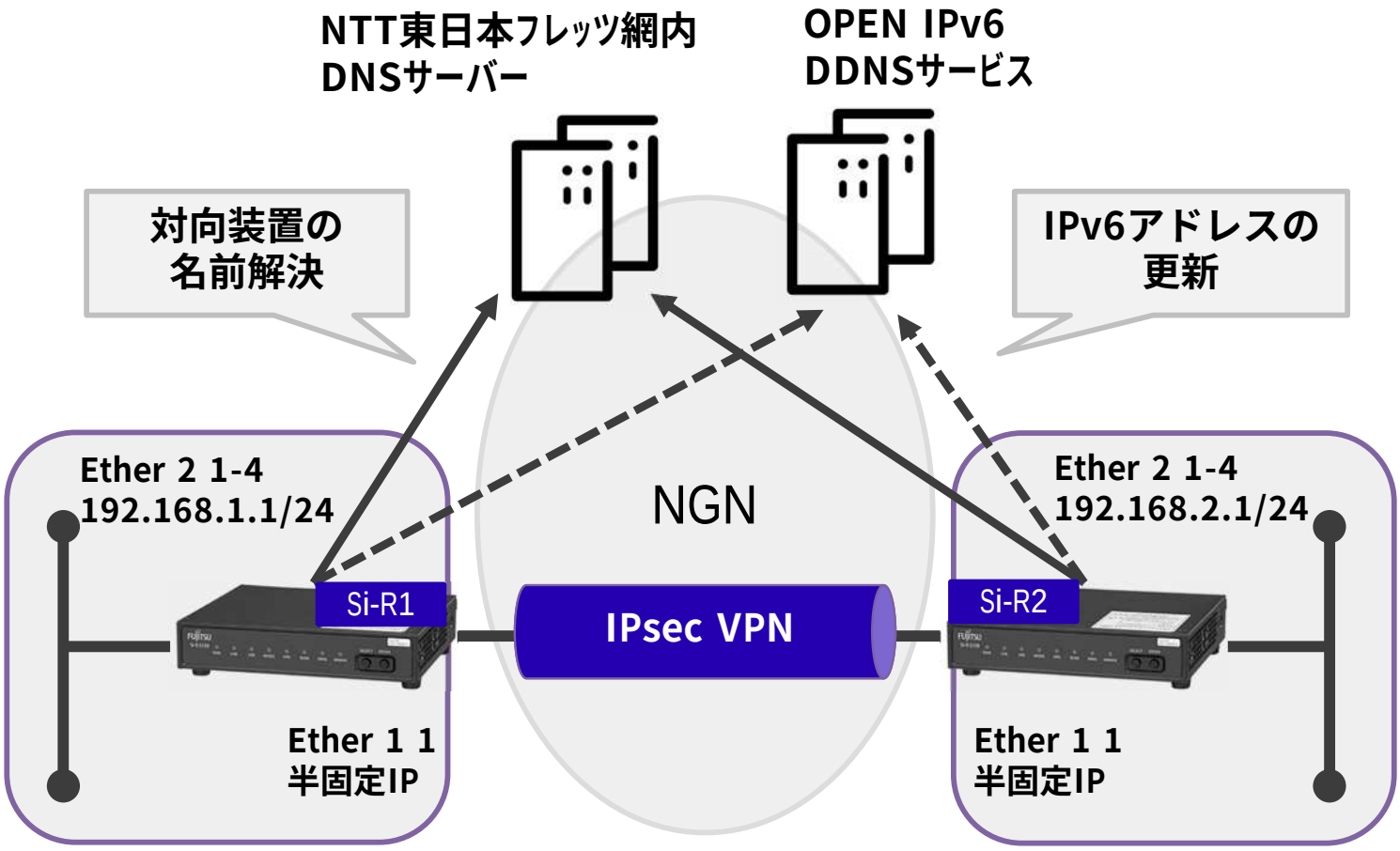
【OPEN IPv6 ダイナミックDNSと連携したVPN拠点間接続】

IPv6 IPoE方式(ひかり電話契約なし）で拠点間を接続する設定例です。

フレッツ 光ネクストのフレッツ・v6オプションを利用して、 NGN網内折り返しで拠点間をVPN接続します。
IPv6 IPoE方式（ひかり電話契約なし）の場合、/64のプレフィックスをひとつ配布されますが、このプレフィックスは半固定になります。「OPEN IPv6 ダイナミック DNS for フレッツ・光ネクスト」と連携することで、配布されるプレフィックスが変更されても、自動でIPsecを再接続することが可能です。なお、「OPEN IPv6 ダイナミック DNS for フレッツ・光ネクスト」をご利用するにあたって、ホームページ上で事前に登録が必要です。

[対象機種と版数]

- Si-R Gシリーズ V20.53以降



Copyright 2023 FUJITSU LIMITED

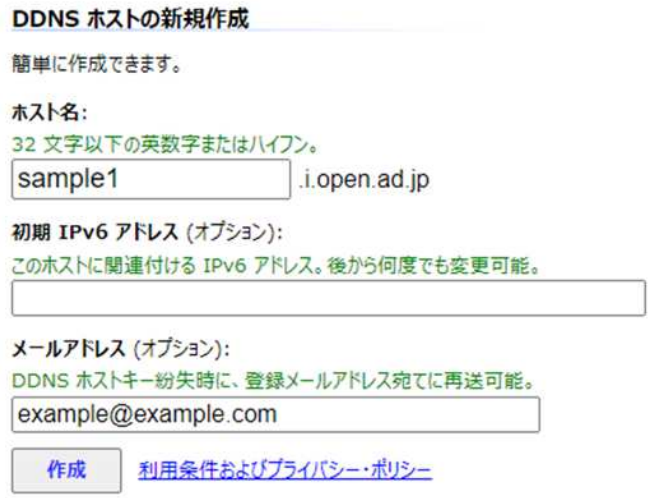
[設定内容]

- Si-Rのether 1 1をWAN側、ether 2 1-をLAN側とします。
- WAN側は、IPoEで/64のアドレス空間が割り当てられるとします。
- LAN側に192.168.1.1/24、192.168.2.1/24をそれぞれ割り当てるとします。
- DDNSサービスに対してアドレスを自動更新する設定をします。
    - 接続先セッション監視機能を活用し、専用更新ホストに対して定期的にpingを送信することで、DDNSホスト名のIPv6アドレスを更新することができる。
- IPv4 over IPv6 IPsec(IKEv2)トンネルで拠点間を接続します。

[DDNSサービス]

OPEN IPv6 DDNSサービスをご利用いただくには以下のURLより登録が必要です。
https://i.open.ad.jp/

上部メニューより 「DDNSホスト一覧・新規作成」 > 「DDNS ホストの新規作成」を選択します。



各拠点のSi-Rに割り当てるをホスト名を作成します。
ホスト名とメールアドレス(任意)を入力し、「作成」を押してください。拠点数の分だけホスト名が必要です。

ホストを作成するとホストキー情報等が表示されます。
なお、ホスト名(FQDN)と専用更新アドレスはSi-Rの構成定義で使用します。

※OPEN IPv6ダイナミックDNS for フレッツ・光ネクストはソフトイーサ株式会社が提供するサービスです。
弊社ではサービスのサポートはしておりません。

Copyright 2023 FUJITSU LIMITED

[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。

- sample1.i.open.ad.jpにはSi-R1で使用するホスト名(FQDN)を設定してください。
- update-0123456789abcdefff.i.open.ad.jpにはSi-R1で使用する専用更新ホスト名を設定してください。
- sample2.i.open.ad.jpにはSi-R2で使用するホスト名(FQDN)を設定してください。
- update-fffedcba9876543210.i.open.ad.jpにはSi-R2で使用する専用更新ホスト名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。

■ Si-R1設定例

```
ether 1 1 vlan untag 1
ether 2 1-4 vlan untag 2
lan 0 ipv6 use on
lan 0 ipv6 address 0 auto
lan 0 ipv6 ra mode recv
lan 0 ipv6 ra recv prefix-mode routers
lan 0 ipv6 filter 0 pass acl 10 in
lan 0 ipv6 filter 1 pass acl 11 in
lan 0 ipv6 filter 2 pass acl 12 in
lan 0 ipv6 filter 3 pass acl 13 in
lan 0 ipv6 filter default spi 5m
lan 0 ipv6 dhcp service client
lan 0 ipv6 dhcp client option na off
lan 0 vlan 1
lan 1 ip address 192.168.1.1/24 3
lan 1 vlan 2
remote 0 name DDNS
remote 0 ap 0 name ping
remote 0 ap 0 datalink type overlap
remote 0 ap 0 overlap to lan 0
remote 0 ap 0 overlap nexthop6 ra
remote 0 ap 0 sessionwatch address ra@lan0 update-0123456789abcdefff.i.open.ad.jp
remote 0 ap 0 sessionwatch interval 1m 5m 15s 1s
remote 0 ipv6 use on
remote 1 name VPN
remote 1 ap 0 name sir2
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 ike local-idtype fqdn
remote 1 ap 0 ike remote-idtype fqdn
remote 1 ap 0 ike name local sample1.i.open.ad.jp
remote 1 ap 0 ike name remote sample2.i.open.ad.jp
remote 1 ap 0 ike shared key text test
```


Copyright 2023 FUJITSU LIMITED

```
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 initial connect
remote 1 ap 0 ike dpd use on
remote 1 ap 0 tunnel local sample1.i.open.ad.jp
remote 1 ap 0 tunnel remote sample2.i.open.ad.jp
remote 1 ap 0 sessionwatch address 192.168.1.1 192.168.2.1
remote 1 ip route 0 192.168.2.0/24 1 1
remote 1 ip msschange 1400
acl 10 description v6_dhcp
acl 10 ipv6 any any 17 any
acl 10 udp 547 546
acl 11 description v6_icmp
acl 11 ipv6 any any 58 any
acl 12 description v6_ike
acl 12 ipv6 any any 17 any
acl 12 udp 500 500
acl 13 description v6_esp
acl 13 ipv6 any any 50 any
syslog facility 23
time zone 0900
resource system vlan 4084-4094
consoleinfo autologout 8h
telnetinfo autologout 5m
terminal charset SJIS
```


Copyright 2023 FUJITSU LIMITED

■ Si-R2設定

```
ether 1 1 vlan untag 1
ether 2 1 vlan untag 2
ether 2 2 vlan untag 2
ether 2 3 vlan untag 2
ether 2 4 vlan untag 2
lan 0 ipv6 use on
lan 0 ipv6 address 0 auto
lan 0 ipv6 ra mode recv
lan 0 ipv6 ra recv prefix-mode routers
lan 0 ipv6 filter 0 pass acl 10 in
lan 0 ipv6 filter 1 pass acl 11 in
lan 0 ipv6 filter 2 pass acl 12 in
lan 0 ipv6 filter 3 pass acl 13 in
lan 0 ipv6 filter default spi 5m
lan 0 ipv6 dhcp service client
lan 0 ipv6 dhcp client option na off
lan 0 vlan 1
lan 1 ip address 192.168.2.1/24 3
lan 1 vlan 2
remote 0 name DDNS
remote 0 ap 0 name ping6
remote 0 ap 0 datalink type overlap
remote 0 ap 0 overlap to lan 0
remote 0 ap 0 overlap nexthop6 ra
remote 0 ap 0 sessionwatch address ra@lan0 update-fffedcba9876543210.i.open.ad.jp
remote 0 ap 0 sessionwatch interval 1m 5m 15s 1s
remote 0 ipv6 use on
remote 1 name VPN
remote 1 ap 0 name sir1
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 ike local-idtype fqdn
remote 1 ap 0 ike remote-idtype fqdn
remote 1 ap 0 ike name local sample2.i.open.ad.jp
remote 1 ap 0 ike name remote sample1.i.open.ad.jp
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 initial connect
remote 1 ap 0 ike dpd use on
remote 1 ap 0 tunnel local sample2.i.open.ad.jp
remote 1 ap 0 tunnel remote sample1.i.open.ad.jp
remote 1 ap 0 sessionwatch address 192.168.2.1 192.168.1.1
```


Copyright 2023 FUJITSU LIMITED

```
remote 1 ip route 0 192.168.1.0/24 1 1
remote 1 ip msschange 1400
acl 10 description v6_dhcp
acl 10 ipv6 any any 17 any
acl 10 udp 547 546
acl 11 description v6_icmp
acl 11 ipv6 any any 58 any
acl 12 description v6_ike
acl 12 ipv6 any any 17 any
acl 12 udp 500 500
acl 13 description v6_esp
acl 13 ipv6 any any 50 any
syslog facility 23
time zone 0900
proxydns domain 0 any * any dhcp lan0
resource system vlan 4089-4094
consoleinfo autologout 8h
telnetinfo autologout 5m
terminal charset SJIS
```


Copyright 2023 FUJITSU LIMITED

[解説]

■ Si-R1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 0 ipv6 use on
WAN側インターフェースでIPv6を有効にします。

lan 0 ipv6 address 0 auto
WAN側インターフェースのIPv6アドレスを自動設定にします。

lan 0 ipv6 ra mode recv
RAメッセージの受信機能を有効にします。

lan 0 ipv6 ra recv prefix-mode routers
RAメッセージ受信によりプレフィックスが変更された場合、アドレス切替を行うように設定します。

lan 0 ipv6 filter 0 pass acl 10 in
lan 0 ipv6 filter 1 pass acl 11 in
lan 0 ipv6 filter 2 pass acl 12 in
lan 0 ipv6 filter 3 pass acl 13 in
WAN側インターフェースにACLの設定を適用します。

lan 0 ipv6 filter default spi 5m
ACLに一致しなかったパケットに対してSPIを動作させます。

lan 0 ipv6 dhcp service client
WAN側インターフェースに対して、IPv6 DHCPクライアント機能を有効にします。

lan 0 ipv6 dhcp client option na off
IPv6 DHCP クライアントのIPv6 アドレス要求をoffに設定します。

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

lan 1 ip address 192.168.1.1/24 3
LAN側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。

Copyright 2023 FUJITSU LIMITED

remote 0 name DDNS
DDNSアドレス更新のための接続先セッション監視用overlapインターフェースの名前(任意)を設定します。

remote 0 ap 0 name ping
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 overlap
パケット転送方法としてoverlapを設定します。

remote 0 ap 0 overlap to lan 0
パケットの送出先をWAN側インターフェースに設定します。

remote 0 ap 0 overlap nexthop6 ra
パケットの転送先としてRAメッセージ送信元アドレスを設定します。

remote 0 ap 0 sessionwatch address ra@lan0 update-0123456789abcdefff.i.open.ad.jp
接続先セッション監視の設定をします。
- ICMP ECHOパケットの送信元として、RAで取得してアドレスを設定します。
- ICMP ECHOパケットの送信先として、DDNSホスト名の「専用更新ホスト名」を設定します。

remote 0 ap 0 sessionwatch interval 1m 5m 15s 1s
ICMP ECHOパケットの送信間隔を設定します。

remote 0 ipv6 use on
IPv6アドレスを有効にします。

remote 1 name VPN
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 sir1
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。

Copyright 2023 FUJITSU LIMITED

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 fqdn
IKEv2情報の相手装置IDタイプをFQDNに設定します。

remote 1 ap 0 ike name local sample1.i.open.ad.jp
IKEv2情報の自装置IDとしてSi-R1のDDNSホスト名（FQDN）を設定します。

remote 1 ap 0 ike name remote sample2.i.open.ad.jp
IKEv2情報の相手装置IDとしてSi-R2のDDNSホスト名（FQDN）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 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 tunnel local sample1.i.open.ad.jp
IPsecトンネルの送信元アドレスとしてSi-R1のDDNSホスト名（FQDN）を設定をします。

remote 1 ap 0 tunnel remote sample2.i.open.ad.jp
IPsecトンネルの送信元アドレスとしてSi-R2のDDNSホスト名（FQDN）を設定をします。

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

remote 1 ip route 0 192.168.2.0/24 1 1
Si-R2のLAN側ネットワークへのスタティックルートを設定します。

remote 1 ip msschange 1400
トンネルインタフェースのMSS値を1400に書き換えます。

Copyright 2023 FUJITSU LIMITED

acl 10 description v6_dhcp
acl 10 ipv6 any any 17 any
acl 10 udp 547 546
ACLでDHCPv6の設定をします。

acl 11 description v6_icmp
acl 11 ipv6 any any 58 any
ACLでICMPv6の設定をします。

acl 12 description v6_ike
acl 12 ipv6 any any 17 any
acl 12 udp 500 500
acl 13 description v6_esp
acl 13 ipv6 any any 50 any
ACLでIPsec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。

Copyright 2023 FUJITSU LIMITED

■ Si-R2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 0 ipv6 use on
WAN側インターフェースでIPv6を有効にします。

lan 0 ipv6 address 0 auto
WAN側インターフェースのIPv6アドレスを自動設定にします。

lan 0 ipv6 ra mode recv
RAメッセージの受信機能を有効にします。

lan 0 ipv6 ra recv prefix-mode routers
RAメッセージ受信によりプレフィックスが変更された場合、アドレス切替を行うように設定します。

lan 0 ipv6 filter 0 pass acl 10 in
lan 0 ipv6 filter 1 pass acl 11 in
lan 0 ipv6 filter 2 pass acl 12 in
lan 0 ipv6 filter 3 pass acl 13 in
WAN側インターフェースにACLの設定を適用します。

lan 0 ipv6 filter default spi 5m
ACLに一致しなかったパケットに対してSPIを動作させます。

lan 0 ipv6 dhcp service client
WAN側インターフェースに対して、IPv6 DHCPクライアント機能を有効にします。

lan 0 ipv6 dhcp client option na off
IPv6 DHCP クライアントのIPv6 アドレス要求をoffに設定します。

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

lan 1 ip address 192.168.2.1/24 3
LAN側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 DDNS
DDNSアドレス更新のための接続先セッション監視用overlapインターフェースの名前(任意)を設定します。

remote 0 ap 0 name ping
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。

Copyright 2023 FUJITSU LIMITED

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

remote 0 ap 0 overlap to lan 0
パケットの送出先をWAN側インターフェースに設定します。

remote 0 ap 0 overlap nexthop6 ra
パケットの転送先としてRAメッセージ送信元アドレスを設定します。

remote 0 ap 0 sessionwatch address ra@lan0 update-fffedcba9876543210.i.open.ad.jp
接続先セッション監視の設定をします。
- ICMP ECHOパケットの送信元として、RAで取得してアドレスを設定します。
- ICMP ECHOパケットの送信先として、DDNSホスト名の「専用更新ホスト名」を設定します。

remote 0 ap 0 sessionwatch interval 1m 5m 15s 1s
ICMP ECHOパケットの送信間隔を設定します。

remote 0 ipv6 use on
IPv6アドレスを有効にします。

remote 1 name VPN
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 sir1
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 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 fqdn
IKEv2情報の相手装置IDタイプをFQDNに設定します。

Copyright 2023 FUJITSU LIMITED

remote 1 ap 0 ike name local sample2.i.open.ad.jp
IKEv2情報の自装置IDとしてSi-R2のDDNSホスト名（FQDN）を設定します。

remote 1 ap 0 ike name remote sample1.i.open.ad.jp
IKEv2情報の相手装置IDとしてSi-R1のDDNSホスト名（FQDN）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 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 tunnel local sample2.i.open.ad.jp
IPsecトンネルの送信元アドレスとしてSi-R2のDDNSホスト名（FQDN）を設定をします。

remote 1 ap 0 tunnel remote sample1.i.open.ad.jp
IPsecトンネルの送信元アドレスとしてSi-R1のDDNSホスト名（FQDN）を設定をします。

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 0 192.168.1.0/24 1 1
Si-R1のLAN側ネットワークへのスタティックルートを設定します。

remote 1 ip msschange 1400
トンネルインタフェースのMSS値を1400に書き換えます。

Copyright 2023 FUJITSU LIMITED

acl 10 description v6_dhcp
acl 10 ipv6 any any 17 any
acl 10 udp 547 546
ACLでDHCPv6の設定をします。

acl 11 description v6_icmp
acl 11 ipv6 any any 58 any
ACLでICMPv6の設定をします。

acl 12 description v6_ike
acl 12 ipv6 any any 17 any
acl 12 udp 500 500
acl 13 description v6_esp
acl 13 ipv6 any any 50 any
ACLでIPsec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。

Copyright 2023 FUJITSU LIMITED