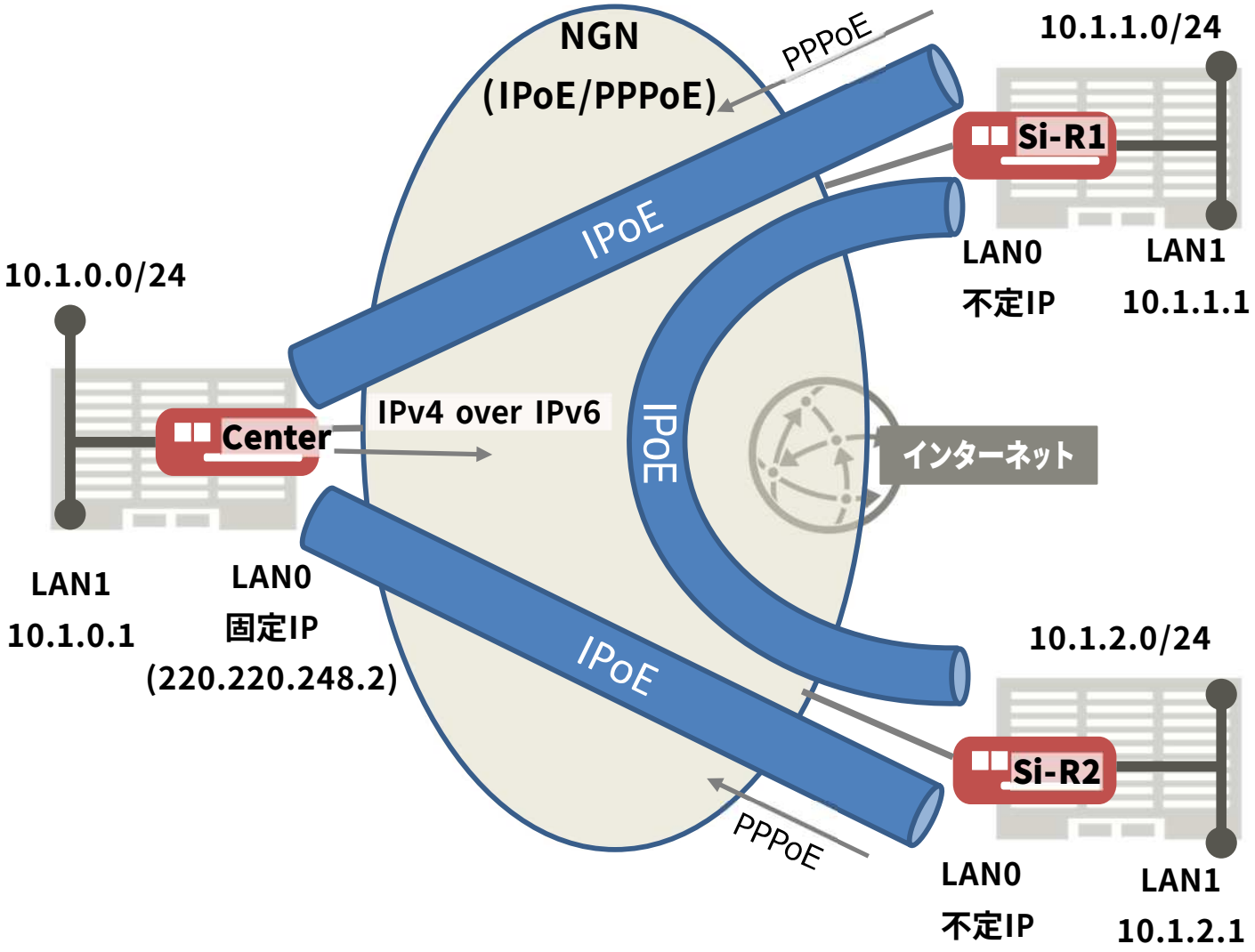
技術情報：Si-R Gシリーズ設定例
（NTT東日本 / NTT西日本フレッツ光ネクスト）

動的VPN機能を利用し、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。
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。動的VPN設定を行うことで、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。
各拠点間の通信も直接IPsecを張ることが可能になるため、センタールータの負荷軽減が可能です。
また、拠点追加時も自拠点を追加するのみで他拠点の設定変更は不要です。

※IPv4パケットをIPv6ヘッダでカプセリング(IPv4 over IPv6 IPsec tunnel)

[対象機種と版数]
・Si-R Gシリーズ V20.15以降

[設定内容]
・Si-RのLAN0側をWAN側、LAN1側を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。
・WAN側は、PPPoE(IPv4)、IPoE(IPv6)を利用します。
・IPoE(IPv4 over IPv6 IPsec tunnel)で拠点間のデータ通信を行います。
・PPPoE(IPv4)でセンター～拠点間の動的VPN制御通信を行います。
・センタールータは、動的VPNのサーバ機能を動作させ、拠点ルータは動的VPNのクライアント機能を動作させます。
・センターのPPPoE(IPv4)は220.220.248.2(固定IPアドレス)を割り当てます。
・Si-RのLAN側に10.1.0.1/24、 10.1.1.1/24 、 10.1.2.1/24を割り当てます。



[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。
・ id-a@ispにはISPのIDを設定してください。
・ pwd-a@ispにはISPのパスワードを設定してください。
・ id-b@ispにはISPのIDを設定してください。
・ pwd-b@ispにはISPのパスワードを設定してください。
・ id-c@ispにはISPのIDを設定してください。
・ pwd-c@ispにはISPのパスワードを設定してください。
・ tmp-key にはtemplate用のIPsec鍵を設定してください。

Center設定事例

```
ether 1 1 vlan untag 1
ether 1 2 use off
ether 2 1 vlan untag 2-8
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 trafficclass 0 any any any any any any 0
lan 0 ipv6 dhcp service client
lan 0 ipv6 dhcp client option na off
lan 0 ipv6 in-policy 0 policy-group 0
lan 0 vlan 1
lan 1 ip address 10.1.0.1/24 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-a@isp pw-a@isp
remote 0 ap 0 keep connect
remote 0 ppp ipcp vjcomp disable
remote 0 ip address local 220.220.248.2
remote 0 ip route 0 default 1 1
remote 0 ip nat mode multi 220.220.248.2 1 5m
remote 0 ip nat static 0 10.1.0.1 5070 220.220.248.2 5070 17
remote 0 ip msschange 1414
remote 3 name null
remote 3 ap 0 name null
remote 3 ap 0 datalink type discard
template 0 name dvpn
template 0 idle 20m
template 0 interface pool 10 90
template 0 datalink type ipsec
template 0 combine use dvpn
template 0 ip msschange 1300
template 0 ipv6 use on
template 0 dvpn client 0
```

```
template 0 ipsec ike protocol esp
template 0 ipsec ike encrypt aes-cbc-256
template 0 ipsec ike auth hmac-sha512
template 0 ipsec ike pfs modp2048
template 0 ipsec ike newsa responder off 0
template 0 ike shared key text tmp-key
template 0 ike proposal 0 encrypt aes-cbc-256
template 0 ike proposal 0 hash hmac-sha512
template 0 ike proposal 0 pfs modp2048
template 0 tunnel local ra@lan0
template 0 sessionwatch address 10.1.0.1
template 0 sessionwatch interval 1m
dvpn server use on
dvpn server domain fuji
dvpn server auth use on
dvpn client 0 server 0 address 220.220.248.2 5070
dvpn client 0 server 0 auth FUJI-0000 FUJI-0000
dvpn client 0 expire register 10m
dvpn client 0 expire session 30m
dvpn client 0 ua 10.1.0.1
dvpn client 0 domain fuji
dvpn client 0 localnet 0 0.0.0.0/0 on
dvpn client 0 localid FUJI-0000
dvpn client 0 interface lan 0 ra
routemanage ip ecmp mode hash
acl 10 description v6_ESP
acl 10 ipv6 any any 50 any
acl 11 description v6_ISAKMP
acl 11 ipv6 any any 17 any
acl 11 udp 500 500
acl 12 description SIP_Cli
acl 12 ipv6 any any 17 any
acl 12 udp 5070 5070
acl 13 description v6_dhcp
acl 13 ipv6 any any 17 any
acl 13 udp 547 546
acl 14 description v6_icmp
acl 14 ipv6 any any 58 any
acl 15 description v6_DNS
acl 15 ipv6 any any 17 any
acl 15 udp 53 any
acl 16 description v6_IP-in-IP
acl 16 ipv6 any any 4 any
acl 17 description v6_any
acl 17 ipv6 any any any any
```

```
policy-group 0 pattern 0 unmatch acl 10
policy-group 0 pattern 1 unmatch acl 11
policy-group 0 pattern 2 unmatch acl 12
policy-group 0 pattern 3 unmatch acl 13
policy-group 0 pattern 4 unmatch acl 14
policy-group 0 pattern 5 unmatch acl 15
policy-group 0 pattern 6 unmatch acl 16
policy-group 0 pattern 7 match acl 17
policy-group 0 interface rmt3
aaa 0 name dvpnserver
aaa 0 user 0 id FUJI-0000
aaa 0 user 0 password FUJI-0000
aaa 0 user 1 id FUJI-0001
aaa 0 user 1 password FUJI-0001
aaa 0 user 2 id FUJI-0002
aaa 0 user 2 password FUJI-0002
aaa 0 user 3 id FUJI-0003
aaa 0 user 3 password FUJI-0003
aaa 0 user 4 id FUJI-0004
aaa 0 user 4 password FUJI-0004
aaa 0 user 5 id FUJI-0005
aaa 0 user 5 password FUJI-0005
syslog facility 23
time auto server 0::0 dhcp
time zone 0900
consoleinfo autologout 15m
telnetinfo autologout 5m
loopback ip address 0 10.1.0.1
terminal charset SJIS
```

Si-R_1設定事例

```
ether 1 1 vlan untag 1
ether 1 2 use off
ether 2 1 vlan untag 2-8
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 trafficclass 0 any any any any any any 0
lan 0 ipv6 dhcp service client
lan 0 ipv6 dhcp client option na off
lan 0 ipv6 in-policy 0 policy-group 0
lan 0 vlan 1
lan 1 ip address 10.1.1.1/24 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-b@isp pw-b@isp
remote 0 ap 0 keep connect
remote 0 ppp ipcp vjcomp disable
remote 0 ip route 0 220.220.248.2/32 1 1
remote 0 ip nat mode multi any 1 5m
remote 0 ip nat static 0 10.1.4.254 5070 any 5070 17
remote 0 ip msschange 1414
remote 1 name dvpn
remote 1 ap 0 name center
remote 1 ap 0 datalink type ipsec
remote 1 ap 0 keep connect
remote 1 ap 0 dvpn client 0
remote 1 ap 0 dvpn remotenet 0 0.0.0.0/0 on
remote 1 ap 0 ipsec type dvpn
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-sha512
remote 1 ap 0 ipsec ike pfs modp2048
remote 1 ap 0 ike shared key text sir2-key
remote 1 ap 0 ike proposal 0 encrypt aes-cbc-256
remote 1 ap 0 ike proposal 0 hash hmac-sha512
remote 1 ap 0 ike proposal 0 pfs modp2048
remote 1 ap 0 ike initial connect
remote 1 ap 0 tunnel local ra@lan0
remote 1 ap 0 sessionwatch address 10.1.1.1 10.1.0.1
remote 1 ap 0 sessionwatch interval 20s 1m 40s 5s
remote 1 ap 1 datalink type discard
remote 1 ip route 0 default 1 1
remote 1 ip msschange 1300
remote 1 ip dvpn 0 autoignore
remote 1 ip dvpn 1 invite acl 20 24 0
remote 1 ip dvpn 2 invite acl 21 24 0
remote 1 ip dvpn 3 invite acl 22 24 0
```

```
remote 3 name null
remote 3 ap 0 name null
remote 3 ap 0 datalink type discard
template 0 name dvpn
template 0 idle 20m
template 0 interface pool 10 90
template 0 datalink type ipsec
template 0 combine use dvpn
template 0 ip msschange 1300
template 0 ipv6 use on
template 0 dvpn client 0
template 0 ipsec ike protocol esp
template 0 ipsec ike encrypt aes-cbc-256
template 0 ipsec ike auth hmac-sha512
template 0 ipsec ike pfs modp2048
template 0 ipsec ike newsa responder off 0
template 0 ike shared key text tmp-key
template 0 ike proposal 0 encrypt aes-cbc-256
template 0 ike proposal 0 hash hmac-sha512
template 0 ike proposal 0 pfs modp2048
template 0 tunnel local ra@lan0
template 0 sessionwatch address 10.1.1.1
template 0 sessionwatch interval 1m
dvpn client 0 server 0 address 220.220.248.2 5070
dvpn client 0 server 0 auth FUJI-0001 FUJI-0001
dvpn client 0 expire register 10m
dvpn client 0 expire session 30m
dvpn client 0 ua 10.1.1.1
dvpn client 0 domain fuji
dvpn client 0 localnet 0 10.1.1.0/24 on
dvpn client 0 localid FUJI-0001
dvpn client 0 interface lan 0 ra
routemanage ip ecmp mode hash
acl 10 description v6_ESP
acl 10 ipv6 any any 50 any
acl 11 description v6_ISAKMP
acl 11 ipv6 any any 17 any
acl 11 udp 500 500
acl 12 description SIP_Cli
acl 12 ipv6 any any 17 any
acl 12 udp 5070 5070
acl 13 description v6_dhcp
acl 13 ipv6 any any 17 any
acl 13 udp 547 546
acl 14 description v6_icmp
acl 14 ipv6 any any 58 any
acl 15 description v6_DNS
acl 15 ipv6 any any 17 any
acl 15 udp 53 any
acl 16 description v6_IP-in-IP
acl 16 ipv6 any any 4 any
acl 17 description v6_any
acl 17 ipv6 any any any any
acl 20 ip any 192.168.0.0/16 any any
acl 21 ip any 172.16.0.0/12 any any
acl 22 ip any 10.0.0.0/8 any any
```

```
policy-group 0 pattern 0 unmatch acl 10
policy-group 0 pattern 1 unmatch acl 11
policy-group 0 pattern 2 unmatch acl 12
policy-group 0 pattern 3 unmatch acl 13
policy-group 0 pattern 4 unmatch acl 14
policy-group 0 pattern 5 unmatch acl 15
policy-group 0 pattern 6 unmatch acl 16
policy-group 0 pattern 7 match acl 17
policy-group 0 interface rmt3
syslog facility 23
time auto server 0::0 dhcp
time zone 0900
consoleinfo autologout 15m
telnetinfo autologout 5m
loopback ip address 0 10.1.1.1
terminal charset SJIS
```

Si-R_2設定事例

```
ether 1 1 vlan untag 1
ether 1 2 use off
ether 2 1 vlan untag 2-8
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 trafficclass 0 any any any any any any 0
lan 0 ipv6 dhcp service client
lan 0 ipv6 dhcp client option na off
lan 0 ipv6 in-policy 0 policy-group 0
lan 0 vlan 1
lan 1 ip address 10.1.2.1/24 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-c@isp pw-c@isp
remote 0 ap 0 keep connect
remote 0 ppp ipcp vjcomp disable
remote 0 ip route 0 220.220.248.2/32 1 1
remote 0 ip nat mode multi any 1 5m
remote 0 ip nat static 0 10.1.4.254 5070 any 5070 17
remote 0 ip msschange 1414
remote 1 name dvpn
remote 1 ap 0 name center
remote 1 ap 0 datalink type ipsec
remote 1 ap 0 keep connect
remote 1 ap 0 dvpn client 0
remote 1 ap 0 dvpn remotenet 0 0.0.0.0/0 on
remote 1 ap 0 ipsec type dvpn
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-sha512
remote 1 ap 0 ipsec ike pfs modp2048
remote 1 ap 0 ike shared key text sir3-key
remote 1 ap 0 ike proposal 0 encrypt aes-cbc-256
remote 1 ap 0 ike proposal 0 hash hmac-sha512
remote 1 ap 0 ike proposal 0 pfs modp2048
remote 1 ap 0 ike initial connect
remote 1 ap 0 tunnel local ra@lan0
remote 1 ap 0 sessionwatch address 10.1.2.1 10.1.0.1
remote 1 ap 0 sessionwatch interval 20s 1m 40s 5s
remote 1 ap 1 datalink type discard
remote 1 ip route 0 default 1 1
remote 1 ip msschange 1300
remote 1 ip dvpn 0 autoignore
remote 1 ip dvpn 1 invite acl 20 24 0
remote 1 ip dvpn 2 invite acl 21 24 0
remote 1 ip dvpn 3 invite acl 22 24 0
```

```
remote 3 name null
remote 3 ap 0 name null
remote 3 ap 0 datalink type discard
template 0 name dvpn
template 0 idle 20m
template 0 interface pool 10 90
template 0 datalink type ipsec
template 0 combine use dvpn
template 0 ip msschange 1300
template 0 ipv6 use on
template 0 dvpn client 0
template 0 ipsec ike protocol esp
template 0 ipsec ike encrypt aes-cbc-256
template 0 ipsec ike auth hmac-sha512
template 0 ipsec ike pfs modp2048
template 0 ipsec ike newsa responder off 0
template 0 ike shared key text tmp-key
template 0 ike proposal 0 encrypt aes-cbc-256
template 0 ike proposal 0 hash hmac-sha512
template 0 ike proposal 0 pfs modp2048
template 0 tunnel local ra@lan0
template 0 sessionwatch address 10.1.2.1
template 0 sessionwatch interval 1m
dvpn client 0 server 0 address 220.220.248.2 5070
dvpn client 0 server 0 auth FUJI-0002 FUJI-0002
dvpn client 0 expire register 10m
dvpn client 0 expire session 30m
dvpn client 0 ua 10.1.2.1
dvpn client 0 domain fuji
dvpn client 0 localnet 0 10.1.2.0/24 on
dvpn client 0 localid FUJI-0002
dvpn client 0 interface lan 0 ra
routemanage ip ecmp mode hash
acl 10 description v6_ESP
acl 10 ipv6 any any 50 any
acl 11 description v6_ISAKMP
acl 11 ipv6 any any 17 any
acl 11 udp 500 500
acl 12 description SIP_Cli
acl 12 ipv6 any any 17 any
acl 12 udp 5070 5070
acl 13 description v6_dhcp
acl 13 ipv6 any any 17 any
acl 13 udp 547 546
acl 14 description v6_icmp
acl 14 ipv6 any any 58 any
acl 15 description v6_DNS
acl 15 ipv6 any any 17 any
acl 15 udp 53 any
acl 16 description v6_IP-in-IP
acl 16 ipv6 any any 4 any
acl 17 description v6_any
acl 17 ipv6 any any any any
acl 20 ip any 192.168.0.0/16 any any
acl 21 ip any 172.16.0.0/12 any any
acl 22 ip any 10.0.0.0/8 any any
```

```
policy-group 0 pattern 0 unmatch acl 10
policy-group 0 pattern 1 unmatch acl 11
policy-group 0 pattern 2 unmatch acl 12
policy-group 0 pattern 3 unmatch acl 13
policy-group 0 pattern 4 unmatch acl 14
policy-group 0 pattern 5 unmatch acl 15
policy-group 0 pattern 6 unmatch acl 16
policy-group 0 pattern 7 match acl 17
policy-group 0 interface rmt3
syslog facility 23
time auto server 0::0 dhcp
time zone 0900
consoleinfo autologout 15m
telnetinfo autologout 5m
loopback ip address 0 10.1.2.1
terminal charset SJIS
```

[解説]

Center設定解説

ether 1 1 vlan untag 1
ether1 1ポートをTag なしVLAN1に設定します。

ether 1 2 use off
ether 1 2ポートを無効にします。

ether 2 1 vlan untag 2-8
ether2 1-8ポートをTag なしVLAN2に設定します。

lan 0 ipv6 use on
WAN側インタフェースでIPv6機能を有効にします。

lan 0 ipv6 address 0 auto
WAN側インタフェースでIPv6アドレスを設定します。

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 trafficclass 0 any any any any any any 0
Traffic Class 値書き換え条件を設定します。

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 アドレス要求を無効にします。

lan 0 ipv6 in-policy 0 policy-group 0
Ingress ポリシールーティングを設定します。

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 10.1.0.1/24 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 PPPoE
PPPoEインターフェースの名前（任意）を設定します。

remote 0 mtu 1454
MTU長を1454byte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
 # インターネット向けパケットの転送先をvlan1インターフェースに設定します。

remote 0 ap 0 ppp auth send id-a@isp pw-a@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 address local 220.220.248.2
#WAN側IPアドレスを設定します。

remote 0 ip route 0 default 1 1
 # WAN側インターフェースにデフォルトルートを設定します。
 # ・default：インターネット側のIPアドレスです。
 # ・1：metric値です。通常は1のままで構いません。
 # ・1：distance値です。

remote 0 ip nat mode multi 220.220.248.2 1 5m
 # マルチNATの設定をします。

remote 0 ip nat static 0 10.1.0.1 5070 220.220.248.2 5070 17
 # スタティックNATにより、パケットを通す設定をします。

remote 0 ip msschange 1414
 # MSS値に1414byteを設定します。

remote 3 name null
 # 相手ネットワーク名称を設定します。

remote 3 ap 0 name null
 # 接続先の名称を設定します。

remote 3 ap 0 datalink type discard
 # パケット転送方法を設定します。

template 0 name dvpn
 # ダイナミックVPN用インターフェースの名前（任意）を設定します。

template 0 idle 20m
 # 無通信監視タイマを20分に設定します。

template 0 interface pool 10 90
 # 動的VPNインターフェースで使用する開始remoteインターフェース番号/インターフェース数を設定します。
 # （既に使用しているremoteインターフェース定義番号は使用できません。）
 # 10：ダイナミックVPNで使用する開始remoteインターフェース番号です。
 # 90：ダイナミックVPNで使用するremoteインターフェース数です。

template 0 datalink type ipsec
 # IPsec使用の設定をします。

template 0 combine use dvpn
 # ダイナミックVPN使用の設定をします。

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

template 0 ipv6 use on
 # IPv6 機能を有効化します。

template 0 dvpn client 0
 # 動的VPN 接続で使用するクライアント情報を設定します。

template 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。

template 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。

template 0 ipsec ike auth hmac-sha512
 # 自動鍵交換用IPsec情報の認証情報にSHA512を設定します。

template 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。

template 0 ipsec ike newsa responder off 0
 # 自動鍵交換用IPsec 情報のNew SA Responder(更新時間／更新データ量)を設定します。

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

template 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ビットを設定します。

template 0 ike proposal 0 hash hmac-sha512
 # IKE セッション用認証（ハッシュ）情報にSHA512を設定します。

template 0 ike proposal 0 pfs modp2048
 # IKE セッション用DH(Diffie-Hellman)グループを2048に設定します。

template 0 tunnel local ra@lan0
 # IPsecトンネルの送信元アドレスを設定します。

template 0 sessionwatch address 10.1.0.1
 # 接続先セッション監視の送信元IPアドレスを設定します。

template 0 sessionwatch interval 1m
 # 接続先セッション監視の送信間隔を設定します。

dvpn server use on
 # ダイナミックVPNサーバを起動します。

dvpn server domain fuji
 # ダイナミックVPNサーバのドメイン名を設定します。

dvpn server auth use on
 # ダイナミックVPNサーバのの認証を有効にします。

dvpn client 0 server 0 address 220.220.248.2 5070
 # 動的VPN サーバのアドレス、ポート番号を設定します。
 # ・220.220.248.2：動的VPNサーバのアドレス。
 # ・5070：ポート番号。

dvpn client 0 server 0 auth FUJI-0000 FUJI-0000
 # 動的VPN サーバの認証情報を設定します。1

dvpn client 0 expire register 10m
 # 動的VPN の情報有効期間を10分に設定します。

dvpn client 0 expire session 30m
 # 動的VPN のセッション更新間隔を30分に設定します。

dvpn client 0 ua 10.1.0.1
 # 動的VPN クライアントのアドレスを設定します。

dvpn client 0 domain fuji
 # 動的VPN ドメイン名を設定します。

dvpn client 0 localnet 0 0.0.0.0/0 on
 # 動的VPN で接続する自側ネットワークを設定します。
 # ・0.0.0.0/0：自側ネットワーク
 # ・on：自側ユーザID を生成して動的VPN サーバに登録します。

dvpn client 0 localid FUJI-0000
 # 動的VPN サーバに登録する自側ユーザIDを設定します。

dvpn client 0 interface lan 0 ra
 # PN 通信で利用するインタフェースを設定します。

routemanage ip ecmp mode hash
 # IPv4 ルーティングのECMPを設定します。

```
acl 10 description v6_ESP
acl 10 ipv6 any any 50 any
acl 11 description v6_ISAKMP
acl 11 ipv6 any any 17 any
acl 11 udp 500 500
acl 12 description SIP_Cli
acl 12 ipv6 any any 17 any
acl 12 udp 5070 5070
acl 13 description v6_dhcp
acl 13 ipv6 any any 17 any
acl 13 udp 547 546
acl 14 description v6_icmp
acl 14 ipv6 any any 58 any
acl 15 description v6_DNS
acl 15 ipv6 any any 17 any
acl 15 udp 53 any
acl 16 description v6_IP-in-IP
acl 16 ipv6 any any 4 any
acl 17 description v6_any
acl 17 ipv6 any any any any
# IPv6通信時のフィルタを設定します。

policy-group 0 pattern 0 unmatch acl 10
policy-group 0 pattern 1 unmatch acl 11
policy-group 0 pattern 2 unmatch acl 12
policy-group 0 pattern 3 unmatch acl 13
policy-group 0 pattern 4 unmatch acl 14
policy-group 0 pattern 5 unmatch acl 15
policy-group 0 pattern 6 unmatch acl 16
policy-group 0 pattern 7 match acl 17
policy-group 0 interface rmt3
# ポリシールール一致パターンを設定します。

aaa 0 name dvpnserver
# 認証のグループ名を設定します。

aaa 0 user 0 id FUJI-0000
aaa 0 user 0 password FUJI-0000
aaa 0 user 1 id FUJI-0001
aaa 0 user 1 password FUJI-0001
aaa 0 user 2 id FUJI-0002
aaa 0 user 2 password FUJI-0002
aaa 0 user 3 id FUJI-0003
aaa 0 user 3 password FUJI-0003
aaa 0 user 4 id FUJI-0004
aaa 0 user 4 password FUJI-0004
aaa 0 user 5 id FUJI-0005
aaa 0 user 5 password FUJI-0005
# ダイナミックVPNの認証ID、パスワードを設定します。
# user 3～5は予備用とします。
```

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の設定をします。通常はこの値で構いません。

time auto server 0::0 dhcp
＃ DHCP サーバが広報する時刻提供サーバに従います。

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 15m
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。

loopback ip address 0 10.1.0.1
＃ 接続先セッション監視のエンドポイントをloopbackアドレスに設定します。

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。

Si-R_1設定解説

ether 1 1 vlan untag 1
 # ether1 1ポートをTag なしVLAN1に設定します。

ether 1 2 use off
 # ether 1 2ポートを無効にします。

ether 2 1 vlan untag 2-8
 # ether2 1-8ポートをTag なしVLAN2に設定します。

lan 0 ipv6 use on
 # WAN側インタフェースでIPv6機能を有効にします。

lan 0 ipv6 address 0 auto
 # WAN側インタフェースでIPv6アドレスを設定します。

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 trafficclass 0 any any any any any any 0
 # Traffic Class 値書き換え条件を設定します。

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 アドレス要求を無効にします。

lan 0 ipv6 in-policy 0 policy-group 0
 # Ingress ポリシールーティングを設定します。

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 10.1.1.1/24 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。

remote 0 name PPPoE
 # PPPoEインターフェースの名前（任意）を設定します。

remote 0 mtu 1454
 # MTU長を1454byte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
 # インターネット向けパケットの転送先をvlan1インターフェースに設定します。

remote 0 ap 0 ppp auth send id-b@isp pw-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 0 220.220.248.2/32 1 1
 # WAN側インターフェースにデフォルトルートを設定します。
 # ・220.220.248.2/32 : WAN側のIPアドレスです。
 # ・1 : metric値です。通常は1のままで構いません。
 # ・1 : distance値です。

remote 0 ip nat mode multi any 1 5m
 # マルチNATの設定をします。

remote 0 ip nat static 0 10.1.4.254 5070 any 5070 17
 # スタティックNATにより、パケットを通す設定をします。

remote 0 ip msschange 1414
 # MSS値に1414byteを設定します。

remote 1 name dvpn
 # 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 center
 # 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 keep connect
 # 常時接続します。

remote 1 ap 0 dvpn client 0
 # 動的VPN 接続で使用するクライアント情報を設定します。

remote 1 ap 0 dvpn remotenet 0 0.0.0.0/0 on
 # 動的VPN で接続する相手側ネットワークを設定する。
 # ・0.0.0.0/0：相手側ネットワークの設定をします。0.0.0.0/0はデフォルトルート。
 # ・on：invite条件一致時のテンプレート使用の可否。

remote 1 ap 0 ipsec type dvpn
 # 動的VPN でIPsec 使用の設定をします。

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ビットを設定します。

remote 1 ap 0 ipsec ike auth hmac-sha512
 # 自動鍵交換用IPsec情報の認証情報にSHA512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 ike shared key text sir2-key
 # IKE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
 # IKEセッション用暗号情報の暗号アルゴリズムにAES256ビットを設定します。

remote 1 ap 0 ike proposal 0 hash hmac-sha512
 # IKEセッション用の認証情報にSHA512を設定します。

remote 1 ap 0 ike proposal 0 pfs modp2048
 # IKE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 ike initial connect
 # IKE ネゴシエーション開始動作の設定をします。

remote 1 ap 0 tunnel local ra@lan0
 # トンネル利用時の自側のトンネルエンドポイントアドレスを設定します。

remote 1 ap 0 sessionwatch address 10.1.1.1 10.1.0.1
 # 接続先セッション監視の設定をします。
 # ・10.1.1.1 : ICMP ECHOパケットの送信元IPアドレスです。
 # ・10.1.0.1 : ICMP ECHOパケットの宛先IPアドレスです。

remote 1 ap 0 sessionwatch interval 20s 1m 40s 5s
 # 接続先セッション監視のインターバルの設定をします。

remote 1 ap 1 datalink type discard
 # パケット転送方法を設定します。

remote 1 ip route 0 default 1 1
 # デフォルトルートを設定します。

remote 1 ip msschange 1300
 # MSS 書き換えの設定をします。

remote 1 ip dvpn 0 autoignore
remote 1 ip dvpn 1 invite acl 20 24 0
remote 1 ip dvpn 2 invite acl 21 24 0
remote 1 ip dvpn 3 invite acl 22 24 0
 # 動的VPN の接続契機となるIPv4 パケットの検出条件を設定します。

remote 3 name null
 # 相手ネットワーク名称を設定します。

remote 3 ap 0 name null
 # 接続先の名称を設定します。

remote 3 ap 0 datalink type discard
 # パケット転送方法を設定します。

template 0 name dvpn
 # ダイナミックVPN用インターフェースの名前（任意）を設定します。

template 0 idle 20m
 # 無通信監視タイマを20分に設定します。

template 0 interface pool 10 90
 # 動的VPNインターフェースで使用する開始remoteインターフェース番号/インターフェース数を設定します。
 # （既に使用しているremoteインターフェース定義番号は使用できません。）
 # 10：ダイナミックVPNで使用する開始remoteインターフェース番号です。
 # 90：ダイナミックVPNで使用するremoteインターフェース数です。

template 0 datalink type ipsec
 # IPsec使用の設定をします。

template 0 combine use dvpn
 # ダイナミックVPN使用の設定をします。

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

template 0 ipv6 use on
 # IPv6 機能を有効化します。

template 0 dvpn client 0
 # 動的VPN 接続で使用するクライアント情報を設定します。

template 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。

template 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。

template 0 ipsec ike auth hmac-sha512
 # 自動鍵交換用IPsec情報の認証情報にSHA512を設定します。

template 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。

template 0 ipsec ike newsa responder off 0
 # 自動鍵交換用IPsec 情報のNew SA Responder(更新時間／更新データ量)を設定します。

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

template 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ビットを設定します。

template 0 ike proposal 0 hash hmac-sha512
 # IKE セッション用認証（ハッシュ）情報にSHA512を設定します。

template 0 ike proposal 0 pfs modp2048
 # IKE セッション用DH(Diffie-Hellman)グループを2048に設定します。

template 0 tunnel local ra@lan0
 # IPsecトンネルの送信元アドレスを設定します。

template 0 sessionwatch address 10.1.1.1
 # 接続先セッション監視の送信元IPアドレスを設定します。

template 0 sessionwatch interval 1m
 # 接続先セッション監視の送信間隔を設定します。

dvpn client 0 server 0 address 220.220.248.2 5070
 # 動的VPN サーバのアドレス、ポート番号を設定します。
 # ・220.220.248.2：動的VPNサーバのアドレス。
 # ・5070：ポート番号。

dvpn client 0 server 0 auth FUJI-0001 FUJI-0001
 # 動的VPN サーバの認証情報を設定します。1

dvpn client 0 expire register 10m
 # 動的VPN の情報有効期間を10分に設定します。

dvpn client 0 expire session 30m
 # 動的VPN のセッション更新間隔を30分に設定します。

dvpn client 0 ua 10.1.1.1
 # 動的VPN クライアントのアドレスを設定します。

dvpn client 0 domain fuji
 # 動的VPN ドメイン名を設定します。

dvpn client 0 localnet 0 10.1.1.0/24 on
 # 動的VPN で接続する自側ネットワークを設定します。
 # ・10.1.1.0/24：自側ネットワーク
 # ・on：自側ユーザID を生成して動的VPN サーバに登録します。

dvpn client 0 localid FUJI-0001
 # 動的VPN サーバに登録する自側ユーザIDを設定します。

dvpn client 0 interface lan 0 ra
 # PN 通信で利用するインタフェースを設定します。

routemanage ip ecmp mode hash
 # IPv4 ルーティングのECMPを設定します。

```
acl 10 description v6_ESP
acl 10 ipv6 any any 50 any
acl 11 description v6_ISAKMP
acl 11 ipv6 any any 17 any
acl 11 udp 500 500
acl 12 description SIP_Cli
acl 12 ipv6 any any 17 any
acl 12 udp 5070 5070
acl 13 description v6_dhcp
acl 13 ipv6 any any 17 any
acl 13 udp 547 546
acl 14 description v6_icmp
acl 14 ipv6 any any 58 any
acl 15 description v6_DNS
acl 15 ipv6 any any 17 any
acl 15 udp 53 any
acl 16 description v6_IP-in-IP
acl 16 ipv6 any any 4 any
acl 17 description v6_any
acl 17 ipv6 any any any any
# IPv6通信時のフィルタを設定します。

acl 20 ip any 192.168.0.0/16 any any
acl 21 ip any 172.16.0.0/12 any any
acl 22 ip any 10.0.0.0/8 any any
# 動的VPN の接続契機となるIPv4 パケットの検出条件を設定します。

policy-group 0 pattern 0 unmatch acl 10
policy-group 0 pattern 1 unmatch acl 11
policy-group 0 pattern 2 unmatch acl 12
policy-group 0 pattern 3 unmatch acl 13
policy-group 0 pattern 4 unmatch acl 14
policy-group 0 pattern 5 unmatch acl 15
policy-group 0 pattern 6 unmatch acl 16
policy-group 0 pattern 7 match acl 17
policy-group 0 interface rmt3
# ポリシールール一致パターンを設定します。

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の設定をします。通常はこの値で構いません。

time auto server 0::0 dhcp
# DHCP サーバが広報する時刻提供サーバに従います。

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 15m
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。

loopback ip address 0 10.1.1.1
# 接続先セッション監視のエンドポイントをloopbackアドレスに設定します。

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。
```

Si-R_2設定解説

ether 1 1 vlan untag 1
 # ether1 1ポートをTag なしVLAN1に設定します。

ether 1 2 use off
 # ether 1 2ポートを無効にします。

ether 2 1 vlan untag 2-8
 # ether2 1-8ポートをTag なしVLAN2に設定します。

lan 0 ipv6 use on
 # WAN側インタフェースでIPv6機能を有効にします。

lan 0 ipv6 address 0 auto
 # WAN側インタフェースでIPv6アドレスを設定します。

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 trafficclass 0 any any any any any any 0
 # Traffic Class 値書き換え条件を設定します。

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 アドレス要求を無効にします。

lan 0 ipv6 in-policy 0 policy-group 0
 # Ingress ポリシールーティングを設定します。

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 10.1.2.1/24 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 PPPoE
 # PPPoEインターフェースの名前（任意）を設定します。

remote 0 mtu 1454
 # MTU長を1454byte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
 # インターネット向けパケットの転送先をvlan1インターフェースに設定します。

remote 0 ap 0 ppp auth send id-c@isp pw-c@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 0 220.220.248.2/32 1 1
 # WAN側インターフェースにデフォルトルートを設定します。
 # ・220.220.248.2/32 : WAN側のIPアドレスです。
 # ・1 : metric値です。通常は1のままで構いません。
 # ・1 : distance値です。

remote 0 ip nat mode multi any 1 5m
 # マルチNATの設定をします。

remote 0 ip nat static 0 10.1.4.254 5070 any 5070 17
 # スタティックNATにより、パケットを通す設定をします。

remote 0 ip msschange 1414
 # MSS値に1414byteを設定します。

remote 1 name dvpn
 # 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 center
 # 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 keep connect
 # 常時接続します。

remote 1 ap 0 dvpn client 0
 # 動的VPN 接続で使用するクライアント情報を設定します。

remote 1 ap 0 dvpn remotenet 0 0.0.0.0/0 on
 # 動的VPN で接続する相手側ネットワークを設定する。
 # ・0.0.0.0/0：相手側ネットワークの設定をします。0.0.0.0/0はデフォルトルート。
 # ・on：invite条件一致時のテンプレート使用の可否。

remote 1 ap 0 ipsec type dvpn
 # 動的VPN でIPsec 使用の設定をします。

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ビットを設定します。

remote 1 ap 0 ipsec ike auth hmac-sha512
 # 自動鍵交換用IPsec情報の認証情報にSHA512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 ike shared key text sir3-key
 # IKE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
 # IKEセッション用暗号情報の暗号アルゴリズムにAES256ビットを設定します。

remote 1 ap 0 ike proposal 0 hash hmac-sha512
 # IKEセッション用の認証情報にSHA512を設定します。

remote 1 ap 0 ike proposal 0 pfs modp2048
 # IKE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 ike initial connect
 # IKE ネゴシエーション開始動作の設定をします。

remote 1 ap 0 tunnel local ra@lan0
 # トンネル利用時の自側のトンネルエンドポイントアドレスを設定します。

remote 1 ap 0 sessionwatch address 10.1.2.1 10.1.0.1
 # 接続先セッション監視の設定をします。
 # ・10.1.2.1 : ICMP ECHOパケットの送信元IPアドレスです。
 # ・10.1.0.1 : ICMP ECHOパケットの宛先IPアドレスです。

remote 1 ap 0 sessionwatch interval 20s 1m 40s 5s
 # 接続先セッション監視のインターバルの設定をします。

remote 1 ap 1 datalink type discard
 # パケット転送方法を設定します。

remote 1 ip route 0 default 1 1
 # デフォルトルートを設定します。

remote 1 ip msschange 1300
 # MSS 書き換えの設定をします。

remote 1 ip dvpn 0 autoignore
remote 1 ip dvpn 1 invite acl 20 24 0
remote 1 ip dvpn 2 invite acl 21 24 0
remote 1 ip dvpn 3 invite acl 22 24 0
 # 動的VPN の接続契機となるIPv4 パケットの検出条件を設定します。

remote 3 name null
 # 相手ネットワーク名称を設定します。

remote 3 ap 0 name null
 # 接続先の名称を設定します。

remote 3 ap 0 datalink type discard
 # パケット転送方法を設定します。

template 0 name dvpn
 # ダイナミックVPN用インターフェースの名前（任意）を設定します。

template 0 idle 20m
 # 無通信監視タイマを20分に設定します。

template 0 interface pool 10 90
 # 動的VPNインターフェースで使用する開始remoteインターフェース番号/インターフェース数を設定します。
 # （既に使用しているremoteインターフェース定義番号は使用できません。）
 # 10：ダイナミックVPNで使用する開始remoteインターフェース番号です。
 # 90：ダイナミックVPNで使用するremoteインターフェース数です。

template 0 datalink type ipsec
 # IPsec使用の設定をします。

template 0 combine use dvpn
 # ダイナミックVPN使用の設定をします。

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

template 0 ipv6 use on
 # IPv6 機能を有効化します。

template 0 dvpn client 0
 # 動的VPN 接続で使用するクライアント情報を設定します。

template 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。

template 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。

template 0 ipsec ike auth hmac-sha512
 # 自動鍵交換用IPsec情報の認証情報にSHA512を設定します。

template 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。

template 0 ipsec ike newsa responder off 0
 # 自動鍵交換用IPsec 情報のNew SA Responder(更新時間／更新データ量)を設定します。

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

template 0 ike proposal 0 encrypt aes-cbc-256
 # IKEｾｯｼｮﾝ用暗号情報の暗号ｱﾙｺﾞﾘｽﾞﾑにAES256ﾋﾞｯﾄを設定します。

template 0 ike proposal 0 hash hmac-sha512
 # IKE ｾｯｼｮﾝ用認証（ﾊｯｼｭ）情報にSHA512を設定します。

template 0 ike proposal 0 pfs modp2048
 # IKE ｾｯｼｮﾝ用DH(Diffie-Hellman)ｸﾞﾙｰﾌﾟを2048に設定します。

template 0 tunnel local ra@lan0
 # IPsecﾄﾝﾈﾙの送信元ｱﾄﾞﾚｽを設定します。

template 0 sessionwatch address 10.1.2.1
 # 接続先ｾｯｼｮﾝ監視の送信元IPｱﾄﾞﾚｽを設定します。

template 0 sessionwatch interval 1m
 # 接続先ｾｯｼｮﾝ監視の送信間隔を設定します。

dvpn client 0 server 0 address 220.220.248.2 5070
 # 動的VPN サーバのアドレス、ポート番号を設定します。
 # ・220.220.248.2：動的VPNサーバのアドレス。
 # ・5070：ポート番号。

dvpn client 0 server 0 auth FUJI-0002 FUJI-0002
 # 動的VPN サーバの認証情報を設定します。1

dvpn client 0 expire register 10m
 # 動的VPN の情報有効期間を10分に設定します。

dvpn client 0 expire session 30m
 # 動的VPN のｾｯｼｮﾝ更新間隔を30分に設定します。

dvpn client 0 ua 10.1.2.1
 # 動的VPN クライアントのアドレスを設定します。

dvpn client 0 domain fuji
 # 動的VPN ドメイン名を設定します。

dvpn client 0 localnet 0 10.1.2.0/24 on
 # 動的VPN で接続する自側ﾈｯﾄﾜｰｸを設定します。
 # ・10.1.2.0/24：自側ﾈｯﾄﾜｰｸ
 # ・on：自側ユーザID を生成して動的VPN サーバに登録します。

dvpn client 0 localid FUJI-0002
 # 動的VPN サーバに登録する自側ユーザIDを設定します。

dvpn client 0 interface lan 0 ra
 # PN 通信で利用するｲﾝﾀﾌｪｰｽを設定します。

routemanage ip ecmp mode hash
 # IPv4 ﾙｰﾃｨﾝｸﾞのECMPを設定します。

```
acl 10 description v6_ESP
acl 10 ipv6 any any 50 any
acl 11 description v6_ISAKMP
acl 11 ipv6 any any 17 any
acl 11 udp 500 500
acl 12 description SIP_Cli
acl 12 ipv6 any any 17 any
acl 12 udp 5070 5070
acl 13 description v6_dhcp
acl 13 ipv6 any any 17 any
acl 13 udp 547 546
acl 14 description v6_icmp
acl 14 ipv6 any any 58 any
acl 15 description v6_DNS
acl 15 ipv6 any any 17 any
acl 15 udp 53 any
acl 16 description v6_IP-in-IP
acl 16 ipv6 any any 4 any
acl 17 description v6_any
acl 17 ipv6 any any any any
# IPv6通信時のフィルタを設定します。

acl 20 ip any 192.168.0.0/16 any any
acl 21 ip any 172.16.0.0/12 any any
acl 22 ip any 10.0.0.0/8 any any
# 動的VPN の接続契機となるIPv4 パケットの検出条件を設定します。

policy-group 0 pattern 0 unmatch acl 10
policy-group 0 pattern 1 unmatch acl 11
policy-group 0 pattern 2 unmatch acl 12
policy-group 0 pattern 3 unmatch acl 13
policy-group 0 pattern 4 unmatch acl 14
policy-group 0 pattern 5 unmatch acl 15
policy-group 0 pattern 6 unmatch acl 16
policy-group 0 pattern 7 match acl 17
policy-group 0 interface rmt3
# ポリシールール一致パターンを設定します。

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の設定をします。通常はこの値で構いません。

time auto server 0::0 dhcp
# DHCP サーバが広報する時刻提供サーバに従います。

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 15m
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。

loopback ip address 0 10.1.2.1
# 接続先セッション監視のエンドポイントをloopbackアドレスに設定します。

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。
```