FutureNet NXR,WXR 設定例集

IPsec 編

Ver 1.5.0

センチュリー・システムズ株式会社

目次

はじめに

- FutureNet はセンチュリー・システムズ株式会社の登録商標です。
- 本書に記載されている会社名，製品名は、各社の商標および登録商標です。
- 本ガイドは、以下の FutureNet NXR,WXR 製品に対応しております。
  NXR-120/C,NXR-125/CX,NXR-130/C,NXR-155/C-WM,NXR-155/C-XW,NXR-155/C-L,
  NXR-230/C,NXR-350/C,NXR-1200,WXR-250
- 本書の内容の一部または全部を無断で転載することを禁止しています。
- 本書の内容については、将来予告なしに変更することがあります。
- 本書の内容については万全を期しておりますが、ご不審な点や誤り、記載漏れ等お気づきの点がありましたらお手数ですが、ご一報下さいますようお願い致します。
- 本書は FutureNet NXR-120/C, NXR-125/CX の以下のバージョンをベースに作成しております。
  1 章 FutureNet NXR-120/C Ver5.22.2
  ※1-6 は FutureNet NXR-120/C Ver5.24.1C
  1-8 は FutureNet NXR-120/C Ver5.22.5
  1-9 は FutureNet NXR-120/C Ver5.24.1C, FutureNet NXR-125/CX Ver5.25.1
  2 章 FutureNet NXR-120/C Ver5.24.1C
  ※2-9,10 は FutureNet NXR-120/C Ver5.24.1C, FutureNet NXR-125/CX Ver5.25.1
  3 章 FutureNet NXR-120/C Ver5.22.2
  ※3-4 は FutureNet NXR-120/C Ver5.22.5
  4 章 FutureNet NXR-120/C Ver5.24.1C
  ※4-2 は FutureNet NXR-125/CX Ver5.25.2
  各種機能において、ご使用されている製品およびファームウェアのバージョンによっては、一部機能,コマンドおよび設定画面が異なっている場合もありますので、その場合は各製品のユーザーズガイドを参考に適宜読みかえてご参照および設定を行って下さい。
- Route Based IPsec 機能は各製品で本機能が実装されているバージョンでのみ利用可能です。
- 本バージョンでは IPv4 のみを対象とし、IPv6 設定に関しては本バージョンでは記載しておりません。
- 設定した内容の復帰(流し込み)を行う場合は、CLI では「copy」コマンド,GUI では設定の復帰を行う必要があります。
- モバイル通信端末をご利用頂く場合で契約内容が従量制またはそれに準ずる場合、大量のデータ通信を行うと利用料が高額になりますので、ご注意下さい。
- 本書を利用し運用した結果発生した問題に関しましては、責任を負いかねますのでご了承下さい。

改版履歴

Version	更新内容
1.0.0	初版
1.1.0	設定例を NXR-120/C Ver5.22.2 ベースに変更 第 3 章 L2TP/IPsec 設定追加 IPsec 接続確認方法更新 L2TP/IPsec 接続確認方法追加 設定例 show config 形式サンプル追加 FutureNet サポートデスクへのお問い合わせページ更新
1.2.0	スマートフォンとの L2TP/IPsec FQDN 接続設定例追加
1.3.0	FQDN での IPsec 接続設定例追加
1.4.0	第 2 章を NXR-120/C Ver5.24.1C ベースに変更 センタ経由拠点間通信設定例追加 IPsec 冗長化設定例追加 第 4 章 Virtual Private Cloud(VPC)設定追加
1.5.0	Windows Azure 接続設定例追加 L2TP/IPsec 設定を一部更新

NXR,WXR シリーズの IPsec 機能

NXR シリーズでは、一部のファームウェアバージョンから WXR シリーズはリリース当初から 2 種類の IPsec 接続方式をサポートしています。XR シリーズなど従来からサポートしている方式を Policy Based IPsec、NXR シリーズで一部のファームウェアバージョンから新規に追加された方式を Route based IPsec と呼びます。
この設定例では Policy Based IPsec,Route based IPsec それぞれの設定例を掲載しています。

・Policy Based IPsec

NXR,WXR シリーズの Policy Based IPsec とはルーティングテーブルに関係なく IPsec アクセスリストで設定したポリシにマッチしたパケットは全て ESP 化の対象とします。これによりポリシーにマッチしないパケットはルーティングテーブルに従ってフォワーディングされます。
また IPsec で ESP 化されるパケットに対してのフィルタリングや NAT(システム NAT 設定は除く)を行うことはできません。

・Route Based IPsec

従来の Policy Based IPsec の場合はルーティングテーブルに関係なく IPsec アクセスリストで設定したポリシにマッチしたパケットは全て ESP 化の対象としました。
そのため IPsec で ESP 化されるパケットに対してのフィルタリングや NAT(システム NAT 設定は除く)を行うことはできません。
これに対して Route Based IPsec では IPsec アクセスリストで設定したポリシにマッチしたパケットを ESP 化の対象とするのではなく、トンネルインタフェースに対するルート設定によって ESP 化するかどうかが決定されます。※トンネルインタフェース設定にて IPsec モードを指定する必要があります。
トンネルインタフェースでは Policy Based IPsec 利用時とは異なり、主に以下のことが可能となります。

- IP フィルタリング(静的フィルタリング,ステートフルパケットインスペクション(SPI))
- NAT(送信元 NAT(SNAT),宛先 NAT(DNAT),IP マスカレード)
- OSPF などの経路制御

※上記は Policy Based IPsec 利用時でも GRE(IPIP) over IPsec を利用することにより可能。

Route Based IPsec 機能は NXR シリーズ,WXR シリーズ全製品で利用することができます。
※2014 年 3 月現在

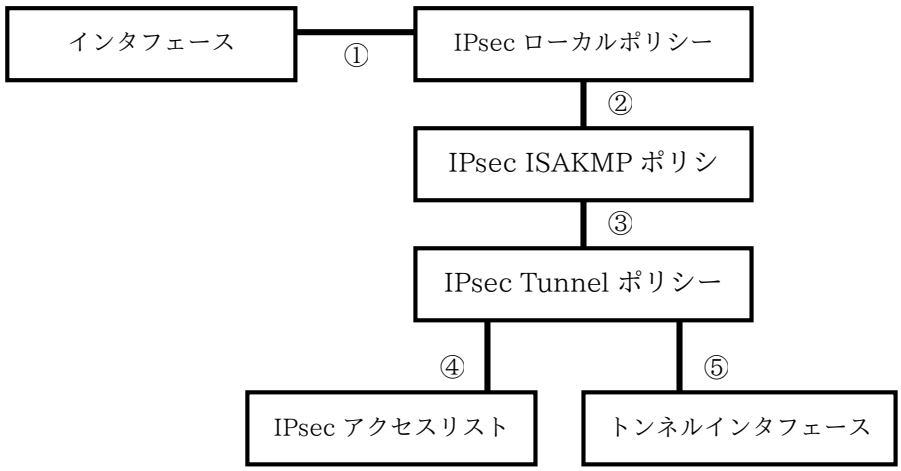
・Policy Based IPsec と Route Based IPsec の機能比較

Policy Based IPsec,Route Based IPsec それぞれの方式を利用した時に利用可能な機能の比較を以下に示します。

機能名	Policy Based IPsec	Route Based IPsec
Set route	○	×
ルーティングによるハンドリング	×	○
policy-ignore	○	× (無効に設定してください)
NAT	△ (SYSTEM NAT で一部対応可能)	○
フィルタリング	×	○
ルーティングプロトコル (OSPF/RIPv1/v2)	×	○
DF bit が 1 のパケットの 強制フラグメント	○	○
プレ/ポストフラグメントの選択	× (ポストフラグメントのみ可能)	○
アウターヘッダのカスタマイズ	×	○
IPv6 ポリシーany の利用	×	○
バランシング	×	○(ECMP により可能) ※Equal Cost Multi Path
QoS	×	○

・NXR,WXR シリーズの IPsec 設定の関連付け

NXR,WXR シリーズで IPsec 設定を行う場合、以下のような関連付けが必要となります。



IPsec を設定する際には上記関連づけが適切に行われていないと、IPsec 接続以前に IPsec 機能が起動しません。ですので IPsec を設定する際には上記を意識した設定を行う必要があります。
そして各設定の関連づけを行う際、どのような設定をする必要があるか以下に示します。
※以下の数字は上記図の数字に対応

①インタフェース設定で IPsec ローカルポリシー設定を指定する場合は、以下のコマンドを設定します。
ipsec policy N (N はローカルポリシー番号)

②IPsec ISAKMP ポリシー設定で IPsec ローカルポリシー設定を指定する場合は、以下のコマンドを設定します。
local policy N (N はローカルポリシー番号)

③IPsec トンネルポリシー設定で IPsec ISAKMP ポリシー設定を指定する場合は、以下のコマンドを設定します。
set key-exchange isakmp N (N は ISAKMP ポリシー番号)

④IPsec トンネルポリシー設定で IPsec アクセスリストを指定する場合は、以下のコマンドを設定します。
match address WORD (WORD は IPsec アクセスリストのアクセスリスト名)

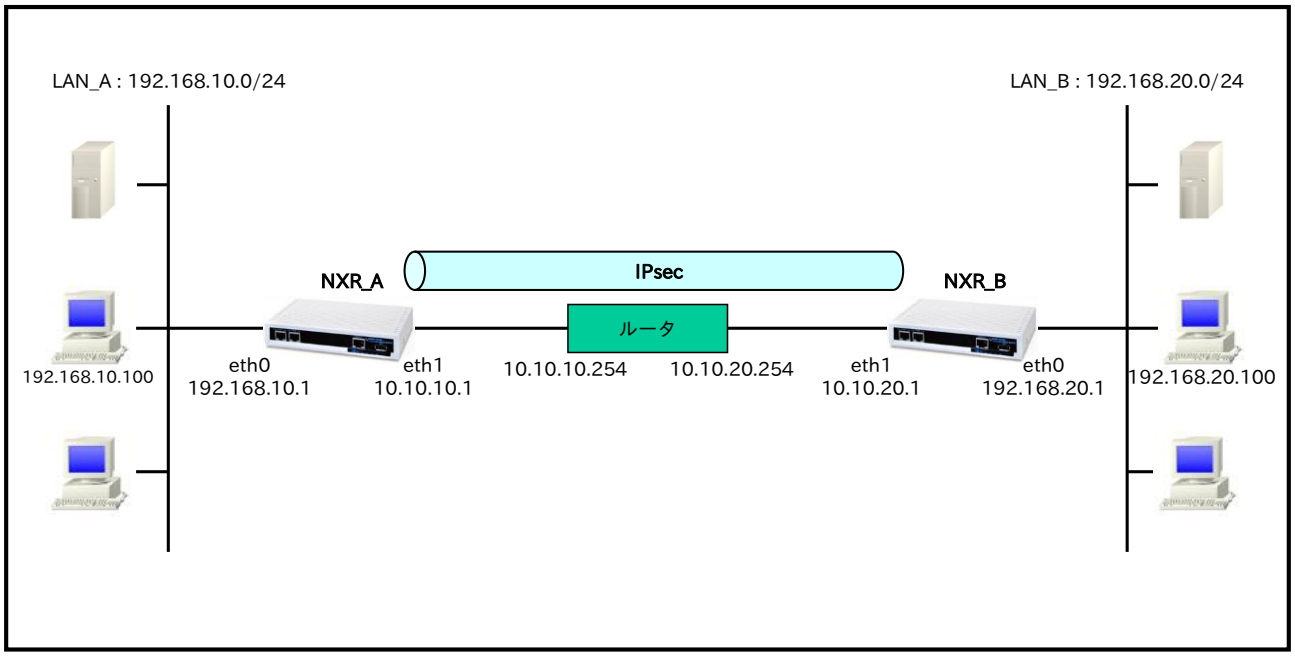
⑤トンネルインタフェース設定で IPsec トンネルポリシー設定を指定する場合は、以下のコマンドを設定します。(Route Based IPsec のみ)
tunnel protection ipsec policy N (N は IPsec トンネルポリシー番号)
※その他にトンネルインタフェースを IPsec で使用する場合は以下のコマンドが必要です。
tunnel mode ipsec ipv4

1. Policy Based IPsec 設定

1-1. 固定 IP アドレスでの接続設定例(MainMode の利用)

LAN_A 192.168.10.0/24 と LAN_B 192.168.20.0/24 のネットワークにある NXR_A,NXR_B 間で IPsec トンネルを構築し LAN 間通信を可能にします。
IPsec を使用するルータの WAN 側 IP アドレスはともに固定 IP アドレスになります。

【 構成図 】



- IPsec を利用する上で ISAKMP ポリシー,トンネルポリシー設定でそれぞれ以下のようなプロポーザルを設定する必要があります。
  ※プロポーザルのデフォルト値に関しては各製品のユーザーズガイドをご参照下さい。
  この設定例では ISAKMP ポリシー(フェーズ 1)で利用するプロポーザルは以下のとおりです。

認証アルゴリズム	SHA-1
暗号化アルゴリズム	AES-128
Diffie-Hellman(DH)グループ	Group5
対向の認証方式	事前共有鍵(Pre-Shared Key)
ネゴシエーションモード	Main
ライフタイム	10800(s)

  この設定例ではトンネルポリシー(フェーズ 2)で利用するプロポーザルは以下のとおりです。

認証アルゴリズム	SHA1-HMAC
暗号化アルゴリズム	AES128
Diffie-Hellman(DH)グループ	Group5
ライフタイム	3600(s)

- 事前共有鍵は対向機器と同一のもの(ここでは ipseckey)を設定する必要があります。

【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 0.0.0.0/0 10.10.10.254
NXR_A(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode main
NXR_A(config-ipsec-isakmp)#remote address ip 10.10.20.1
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address LAN_B
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#ip address 10.10.10.1/24
NXR_A(config-if)#ipsec policy 1
NXR_A(config-if)#exit
NXR_A(config)#fast-forwarding enable
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 0.0.0.0/0 10.10.20.254
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address 10.10.20.1/24
NXR_B(config-if)#ipsec policy 1
NXR_B(config-if)#exit
NXR_B(config)#fast-forwarding enable
NXR_B(config)#exit
NXR_B#save config
```

【 設定例解説 】

〔NXR_A の設定〕

1. <ホスト名の設定>

```
nxr120(config)#hostname NXR_A
```

ホスト名を NXR_A と設定します。

2. <LAN 側(ethernet0)インタフェース設定>

```
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
```

LAN 側(ethernet0)インタフェースの IP アドレスとして 192.168.10.1/24 を設定します。

3. <スタティックルート設定>

```
NXR_A(config)#ip route 0.0.0.0/0 10.10.10.254
```

デフォルトルートを設定します。ゲートウェイアドレスは上位ルータの IP アドレスを設定します。

4. <IPsec アクセスリスト設定>

```
NXR_A(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
```

IPsec アクセスリスト名を LAN_B とし送信元 IP アドレス 192.168.10.0/24,宛先 IP アドレス 192.168.20.0/24 を設定します。Policy Based IPsec では IPsec アクセスリストで設定したルールに基づき IPsec で ESP 化するかどうかが決定されます。よってここで設定した送信元,宛先 IP アドレスにマッチしたパケットが IPsec のカプセル化対象となります。

5. <IPsec ローカルポリシー設定>

```
NXR_A(config)#ipsec local policy 1
```

IPsec ローカルポリシー1 を設定します。

```
NXR_A(config-ipsec-local)#address ip
```

IPsec トンネルの送信元 IP アドレスを設定します。この IP アドレスにはインタフェース設定で ipsec policy 1 と指定したインタフェースの IP アドレスが自動的に設定されます。

6. <IPsec ISAKMP ポリシー設定>

```
NXR_A(config)#ipsec isakmp policy 1
```

NXR_B との IPsec 接続で使用する ISAKMP ポリシー1 を設定します。

```
NXR_A(config-ipsec-isakmp)#description NXR_B
```

ISAKMP ポリシー1 の説明として NXR_B を設定します。

```
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey
```

認証方式として pre-share(事前共有鍵) を選択し事前共有鍵 ipseckey を設定します。なおこの設定は対向の NXR と同じ値を設定する必要があります。

```
NXR_A(config-ipsec-isakmp)#hash sha1
```

認証アルゴリズムとして sha1 を設定します。

```
NXR_A(config-ipsec-isakmp)#encryption aes128
```

暗号化アルゴリズムとして aes128 を設定します。

```
NXR_A(config-ipsec-isakmp)#group 5
```

Diffie-Hellman(DH)グループとして group 5 を設定します。

```
NXR_A(config-ipsec-isakmp)#lifetime 10800
```

ISAKMP SA のライフタイムとして 10800 秒を設定します。

```
NXR_A(config-ipsec-isakmp)#isakmp-mode main
```

フェーズ 1 のネゴシエーションモードとしてここでは IPsec を使用するルータの WAN 側 IP アドレスがともに固定 IP アドレスのためメインモードを設定します。

```
NXR_A(config-ipsec-isakmp)#remote address ip 10.10.20.1
```

対向の NXR の WAN 側 IP アドレスを設定します。ここでは対向の NXR の WAN 側 IP アドレス 10.10.20.1 を設定します。

```
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic restart
```

IKE KeepAlive(DPD)を設定します。ここでは 30 秒間隔で 3 回リトライを行い keepalive 失敗時に SA を削除し IKE のネゴシエーションを開始するよう設定します。

DPD(Dead Peer Detection)は ISAKMP SA を監視する機能で対向の NXR の WAN 側で障害が発生した場合などにそれを検知し、現在利用している SA を削除したり SA を削除して再ネゴシエーションを行ったりするなどの機能があります。なお DPD は常に定期的に送信されるわけではなく対向の NXR より IPsec パケットを受信している場合は DPD パケットの送信は行われません。

```
NXR_A(config-ipsec-isakmp)#local policy 1
```

関連づけを行う IPsec ローカルポリシーとして IPsec ローカルポリシー1 を設定します。

7. <IPsec トンネルポリシー設定>

```
NXR_A(config)#ipsec tunnel policy 1
```

NXR_B との IPsec 接続で使用するトンネルポリシー1 を設定します。

```
NXR_A(config-ipsec-tunnel)#description NXR_B
```

トンネルポリシー1 の説明として NXR_B を設定します。

```
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
```

IPsec ポリシーのネゴシエーションモードはネゴシエーションを自ら開始したり、逆にいかなる場合も自らネゴシエーションを開始しないという設定が可能です。

ここではネゴシエーションモードを auto に設定します。これによりこちらからネゴシエーションを開始することができます。

```
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
```

IPsec トンネルポリシーで使用するトランスフォーム(プロポーザル)を設定します。

ここでは暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1 を設定します。

```
NXR_A(config-ipsec-tunnel)#set pfs group5
```

PFS(Perfect Forward Secrecy)の設定とそれに伴う DH グループを設定します。

ここでは PFS を有効とし、かつ DH グループとして group5 を設定します。

```
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
```

IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
```

関連づけを行う ISAKMP ポリシーとして ISAKMP ポリシー1 を設定します。

```
NXR_A(config-ipsec-tunnel)#match address LAN_B
```

IPsec アクセスリストとして LAN_B を設定します。

8. <WAN 側(ethernet1)インタフェース設定>

```
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#ip address 10.10.10.1/24
```

WAN 側(ethernet1)インタフェースの IP アドレスとして 10.10.10.1/24 を設定します。

```
NXR_A(config-if)#ipsec policy 1
```

IPsec トンネルのエンドポイントとなるため IPsec ローカルポリシー1 を設定します。

9. <ファストフォワーディングの有効化>

```
NXR_A(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(☞) ファストフォワーディングの詳細および利用時の制約については、NXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

〔NXR_B の設定〕

1. <ホスト名の設定>

```
nxr120(config)#hostname NXR_B
```

ホスト名を NXR_B と設定します。

2. <LAN 側(ethernet0)インタフェース設定>

```
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
```

LAN 側(ethernet0)インタフェースの IP アドレスとして 192.168.20.1/24 を設定します。

3. <スタティックルート設定>

```
NXR_B(config)#ip route 0.0.0.0/0 10.10.20.254
```

デフォルトルートを設定します。ゲートウェイアドレスは上位ルータの IP アドレスを設定します。

4. <IPsec アクセスリスト設定>

```
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
```

IPsec アクセスリスト名を LAN_A とし送信元 IP アドレス 192.168.20.0/24,宛先 IP アドレス 192.168.10.0/24 を設定します。

5. <IPsec ローカルポリシー設定>

```
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
```

IPsec ローカルポリシー1 で IPsec トンネルの送信元 IP アドレスを設定します。

6. <IPsec ISAKMP ポリシー設定>

```
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey
```

NXR_A との IPsec 接続で使用する ISAKMP ポリシー1 を設定します。
ISAKMP ポリシー1 の説明として NXR_A、認証方式として pre-share(事前共有鍵)を選択し事前共有鍵 ipseckey を設定します。

```
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
```

認証アルゴリズムとして sha1、暗号化アルゴリズムとして aes128、Diffie-Hellman(DH)グループとして group 5、ISAKMP SA のライフタイムとして 10800 秒、フェーズ 1 のネゴシエーションモードとしてメインモードを設定します。

```
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
```

NXR_A の WAN 側 IP アドレス 10.10.10.1、IKE KeepAlive(DPD)を監視間隔 30 秒,リトライ回数 3 回とし keepalive 失敗時に SA を削除し IKE のネゴシエーションを開始するよう設定します。
そして IPsec ローカルポリシー1 と関連づけを行います。

7. <IPsec トンネルポリシー設定>

```
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
```

NXR_A との IPsec 接続で使用するトンネルポリシー1 を設定します。
IPsec トンネルポリシー1 の説明として NXR_A、ネゴシエーションモードとして auto を設定します。

```
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして LAN_A を設定します。

8. <WAN 側(ethernet1)インタフェース設定>

```
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address 10.10.20.1/24
NXR_B(config-if)#ipsec policy 1
```

WAN 側(ethernet1)インタフェースの IP アドレスとして 10.10.20.1/24 を設定します。

また IPsec トンネルのエンドポイントとなるため IPsec ローカルポリシー1 を設定します。

9. <ファストフォワーディングの有効化>

```
NXR_B(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。

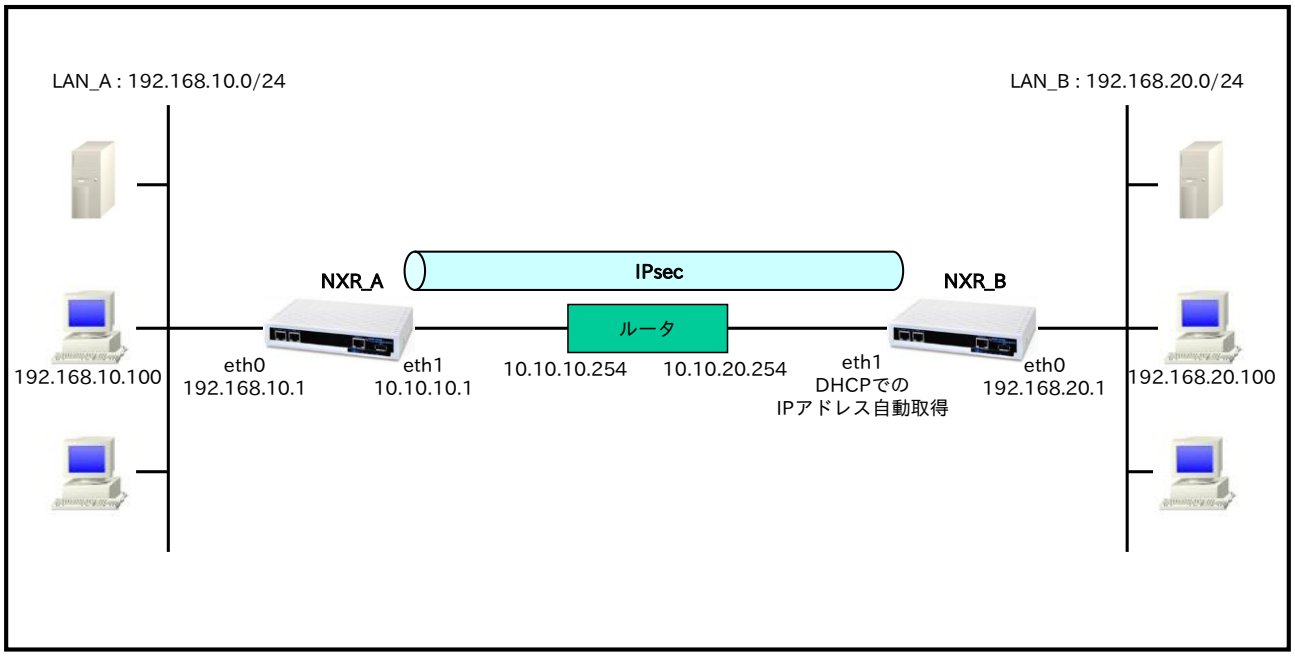
【 パソコンの設定例 】

	LAN A のパソコン	LAN B のパソコン
IP アドレス	192.168.10.100	192.168.20.100
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1

1-2. 動的 IP アドレスでの接続設定例(AggressiveMode の利用)

NXR の WAN 側 IP アドレスが接続のたびに変わる動的 IP アドレス環境でも IPsec を利用することが可能です。なおこの設定例では固定 IP-動的 IP での接続を想定しています。動的 IP 同士での接続は 1-8. FQDN での IPsec 接続設定例をご参照ください。

【 構成図 】



- ここでは IPsec トンネル構築に際し動的 IP アドレスの NXR からネゴシエーションを開始します。
- IPsec を利用する上で ISAKMP ポリシー,トンネルポリシー設定で以下のようなプロポーザルを設定する必要があります。
  ※プロポーザルのデフォルト値に関しては各製品のユーザーズガイドをご参照下さい。
  この設定例では ISAKMP ポリシー(フェーズ 1)で利用するプロポーザルは以下のとおりです。

認証アルゴリズム	SHA-1
暗号化アルゴリズム	AES-128
Diffie-Hellman(DH)グループ	Group5
対向の認証方式	事前共有鍵(Pre-Shared Key)
ネゴシエーションモード	Aggressive
ライフタイム	10800(s)

この設定例ではトンネルポリシー(フェーズ 2)で利用するプロポーザルは以下のとおりです。

認証アルゴリズム	SHA1-HMAC
暗号化アルゴリズム	AES128
Diffie-Hellman(DH)グループ	Group5
ライフタイム	3600(s)

- 事前共有鍵は対向機器と同一のもの(ここでは ipseckey)を設定する必要があります。
- この構成では NXR_B の WAN 側 IP アドレスが動的 IP アドレスのため IP アドレスを ID として利用することができません。そのため NXR_A では ISAKMP ポリシー設定で remote identity を NXR_B では IPsec ローカルポリシー設定で self-identity を設定します。

  (☞) identity は IKE のネゴシエーション時に NXR を識別するのに使用します。
  そのため self-identity は対向の NXR の remote identity と設定を合わせる必要があります。

【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 0.0.0.0/0 10.10.10.254
NXR_A(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A(config-ipsec-isakmp)#remote address ip any
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrb
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address LAN_B
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#ip address 10.10.10.1/24
NXR_A(config-if)#ipsec policy 1
NXR_A(config-if)#exit
NXR_A(config)#fast-forwarding enable
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address dhcp
NXR_B(config-if)#ipsec policy 1
NXR_B(config-if)#exit
NXR_B(config)#fast-forwarding enable
NXR_B(config)#exit
NXR_B#save config
```

【 設定例解説 】

〔NXR_A の設定〕

1. <ホスト名の設定>

```
nxr120(config)#hostname NXR_A
```

ホスト名を NXR_A と設定します。

2. <LAN 側(ethernet0)インタフェース設定>

```
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
```

LAN 側(ethernet0)インタフェースの IP アドレスとして 192.168.10.1/24 を設定します。

3. <スタティックルート設定>

```
NXR_A(config)#ip route 0.0.0.0/0 10.10.10.254
```

デフォルトルートを設定します。ゲートウェイアドレスは上位ルータの IP アドレスを設定します。

4. <IPsec アクセスリスト設定>

```
NXR_A(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
```

IPsec アクセスリスト名を LAN_B とし送信元 IP アドレス 192.168.10.0/24,宛先 IP アドレス 192.168.20.0/24 を設定します。Policy Based IPsec では IPsec アクセスリストで設定したルールに基づき IPsec で ESP 化するかどうかが決定されます。よってここで設定した送信元,宛先 IP アドレスにマッチしたパケットが IPsec のカプセル化対象となります。

5. <IPsec ローカルポリシー設定>

```
NXR_A(config)#ipsec local policy 1
```

IPsec ローカルポリシー1 を設定します。

```
NXR_A(config-ipsec-local)#address ip
```

IPsec トンネルの送信元 IP アドレスを指定します。この IP アドレスはインタフェース設定で ipsec policy 1 と指定したインタフェースの IP アドレスが自動的に設定されます。

6. <IPsec ISAKMP ポリシー設定>

```
NXR_A(config)#ipsec isakmp policy 1
```

NXR_B との IPsec 接続で使用する ISAKMP ポリシー1 を設定します。

```
NXR_A(config-ipsec-isakmp)#description NXR_B
```

ISAKMP ポリシー1 の説明として NXR_B を設定します。

```
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey
```

認証方式として pre-share(事前共有鍵) を選択し事前共有鍵 ipseckey を設定します。なおこの設定は対向の NXR と同じ値を設定する必要があります。

```
NXR_A(config-ipsec-isakmp)#hash sha1
```

認証アルゴリズムとして sha1 を設定します。

```
NXR_A(config-ipsec-isakmp)#encryption aes128
```

暗号化アルゴリズムとして aes128 を設定します。

```
NXR_A(config-ipsec-isakmp)#group 5
```

Diffie-Hellman(DH)グループとして group 5 を設定します。

```
NXR_A(config-ipsec-isakmp)#lifetime 10800
```

ISAKMP SA のライフタイムとして 10800 秒を設定します。

```
NXR_A(config-ipsec-isakmp)#isakmp-mode aggressive
```

フェーズ 1 のネゴシエーションモードとして IPsec を使用するルータの WAN 側 IP アドレスが片側動的 IP アドレスのためアグレッシブモードを設定します。

```
NXR_A(config-ipsec-isakmp)#remote address ip any
```

対向の NXR の WAN 側 IP アドレスを設定します。ここでは対向の NXR の WAN 側 IP アドレスが動的 IP アドレスのため any を設定します。

```
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrb
```

対向の NXR の identity を設定します。ここでは ID として FQDN 方式で nxrb と設定します。
本設定が必要な理由は対向の NXR の WAN 側 IP アドレスが動的 IP アドレスのため IP アドレスを ID として利用することができないためです。

```
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic clear
```

IKE KeepAlive(DPD)を設定します。ここでは監視を 30 秒間隔で 3 回リトライを行い keepalive 失敗時に SA を削除するよう設定します。
DPD(Dead Peer Detection)は ISAKMP SA を監視する機能で対向 SG の WAN 側で障害が発生した場合などにそれを検知し、現在利用している SA を削除したり SA を削除して再ネゴシエーションを行ったりするなどの機能があります。なお DPD は常に定期的に送信されるわけではなく対向の NXR より IPsec パケットを受信している場合は DPD パケットの送信は行われません。

```
NXR_A(config-ipsec-isakmp)#local policy 1
```

関連づけを行う IPsec ローカルポリシーとして IPsec ローカルポリシー1 を設定します。

7. <IPsec トンネルポリシー設定>

```
NXR_A(config)#ipsec tunnel policy 1
```

NXR_B との IPsec 接続で使用するトンネルポリシー1 を設定します。

```
NXR_A(config-ipsec-tunnel)#description NXR_B
```

トンネルポリシー1 の説明として NXR_B を設定します。

```
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
```

IPsec ポリシーのネゴシエーションモードはネゴシエーションを自ら開始したり、逆にいかなる場合も自らネゴシエーションを開始しないという設定が可能です。
ここではネゴシエーションモードを responder に設定します。これによりこちらからいかなる場合(Rekey を含む)においてもネゴシエーションを開始することはありません。

```
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
```

IPsec トンネルポリシーで使用するトランスフォーム(プロポーザル)を設定します。
ここでは暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1 を設定します。

```
NXR_A(config-ipsec-tunnel)#set pfs group5
```

PFS(Perfect Forward Secrecy)の設定とそれに伴う DH グループを設定します。
ここでは PFS を有効とし、かつ DH グループとして group5 を設定します。

```
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
```

IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
```

関連づけを行う ISAKMP ポリシーとして ISAKMP ポリシー1 を設定します。

```
NXR_A(config-ipsec-tunnel)#match address LAN_B
```

IPsec アクセスリストとして LAN_B を設定します。

8. <WAN 側(ethernet1)インタフェース設定>

```
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#ip address 10.10.10.1/24
```

WAN 側(ethernet1)インタフェースの IP アドレスとして 10.10.10.1/24 を設定します。

```
NXR_A(config-if)#ipsec policy 1
```

IPsec トンネルのエンドポイントとなるため IPsec ローカルポリシー1 を設定します。

9. <ファストフォワーディングの有効化>

```
NXR_A(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(☞) ファストフォワーディングの詳細および利用時の制約については、NXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

〔NXR_B の設定〕

1. <ホスト名の設定>

```
nxr120(config)#hostname NXR_B
```

ホスト名を NXR_B と設定します。

2. <LAN 側(ethernet0)インタフェース設定>

```
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
```

LAN 側(ethernet0)インタフェースの IP アドレスとして 192.168.20.1/24 を設定します。

3. <IPsec アクセスリスト設定>

```
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
```

IPsec アクセスリスト名を LAN_A とし送信元 IP アドレス 192.168.20.0/24,宛先 IP アドレス 192.168.10.0/24 を設定します。

4. <IPsec ローカルポリシー設定>

```
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
```

IPsec ローカルポリシー1 で IPsec トンネルの送信元 IP アドレスを設定します。

```
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
```

本装置の identity を設定します。ここでは ID として FQDN 方式で nxrb と設定します。
本設定が必要な理由は WAN 側 IP アドレスが動的 IP アドレスのため対向の NXR で本装置の IP アドレスを ID として設定しておくことができないためです。

5. <IPsec ISAKMP ポリシー設定>

```
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey
```

NXR_A との IPsec 接続で使用する ISAKMP ポリシー1 を設定します。
ISAKMP ポリシー1 の説明として NXR_A、認証方式として pre-share(事前共有鍵)を選択し事前共有鍵 ipseckey を設定します。

```
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
```

認証アルゴリズムとして sha1、暗号化アルゴリズムとして aes128，Diffie-Hellman(DH)グループとして group 5、ISAKMP SA のライフタイムとして 10800 秒、フェーズ 1 のネゴシエーションモードとしてアグレッシブモードを設定します。

```
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
```

NXR_A の WAN 側 IP アドレス 10.10.10.1、IKE KeepAlive(DPD)を監視間隔 30 秒,リトライ回数 3 回とし keepalive 失敗時に SA を削除し IKE のネゴシエーションを開始するよう設定します。
そして IPsec ローカルポリシー1 と関連づけを行います。

6. <IPsec トンネルポリシー設定>

```
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
```

NXR_A との IPsec 接続で使用するトンネルポリシー1 を設定します。
IPsec トンネルポリシー1 の説明として NXR_A、ネゴシエーションモードとして auto を設定します。

```
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして LAN_A を設定します。

7. <WAN 側(ethernet1)インタフェース設定>

```
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address dhcp
NXR_B(config-if)#ipsec policy 1
```

WAN 側(ethernet1)インタフェースの IP アドレスが動的 IP のため DHCP クライアントとして動作するように設定します。

また IPsec トンネルのエンドポイントとなるため IPsec ローカルポリシー1 を設定します。

8. <ファストフォワーディングの有効化>

```
NXR_B(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。

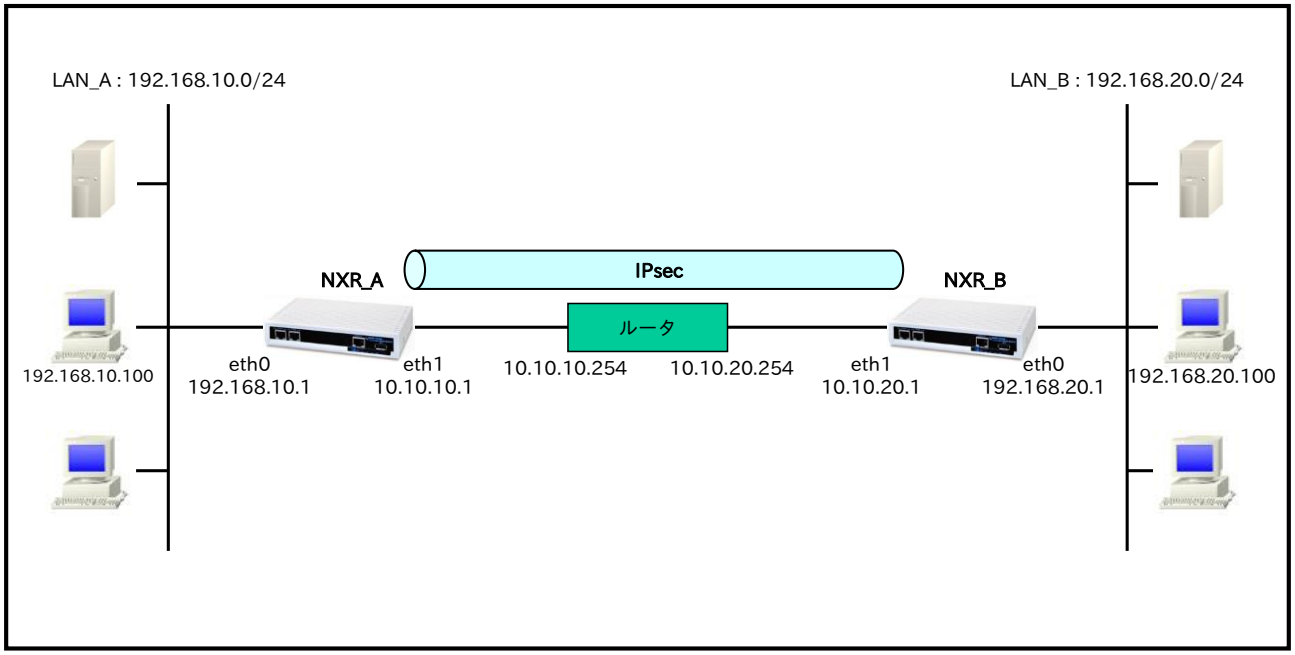
【 パソコンの設定例 】

	LAN A のパソコン	LAN B のパソコン
IP アドレス	192.168.10.100	192.168.20.100
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1

1-3. RSA 公開鍵暗号方式での接続設定例

IKE のフェーズ 1 で対向の NXR の認証に RSA 公開鍵暗号方式を利用することができます。RSA 公開鍵暗号方式を利用する場合は IKE のフェーズ 1 でメインモードを使用する必要があります。

【 構成図 】



- 公開鍵は対向の NXR の ISAKMP ポリシー設定で使用しますので各 NXR の ISAKMP ポリシー設定前までに公開鍵を作成しておく必要があります。
- RSA 公開鍵暗号方式を利用する場合は各 NXR の IPsec ローカルポリシー設定,ISAKMP ポリシー設定で identity 設定が必須になります。
- この設定例では ISAKMP ポリシー(フェーズ 1)で利用するプロポーザルは以下のとおりです。

認証アルゴリズム	SHA-1
暗号化アルゴリズム	AES-128
Diffie-Hellman(DH)グループ	Group5
対向の認証方式	事前共有鍵(Pre-Shared Key)
ネゴシエーションモード	Main
ライフタイム	10800(s)

- この設定例ではトンネルポリシー(フェーズ 2)で利用するプロポーザルは以下のとおりです。

認証アルゴリズム	SHA1-HMAC
暗号化アルゴリズム	AES128
Diffie-Hellman(DH)グループ	Group5
ライフタイム	3600(s)

【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 0.0.0.0/0 10.10.10.254
NXR_A(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
NXR_A(config)#ipsec generate rsa-sig-key 1024
RSA-SIG KEY generating...
NXR_A(config)#exit
NXR_A#show ipsec rsa-pub-key
RSA public key :
0sAQNe9Ghb4CNEaJuIIy67aSxECLJDHhvndH1opuMs6P8yGiTNlcGeSOQ8XEy8iYTst2bv022XUxSt37RhOR
5lRiY1i83TXkQZbhnJDCNJv+rtX/aro745MbJ9auXT1L5tda4C54S7SELboAtU28sD3si0OwlzLWtE7yRUqLP4Z
iiNMw==
NXR_A#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#self-identity fqdn nxra
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication rsa-sig 0sAQOx8kE6uhZTvWMikunsy3uK5/7jIkTXsCjQpgo4B+
X64UAVeuxFQZ3KG3bzyjmyCbpkt0xEiU+v1kF4AOAOXoDfgND+KAdEky/YWqQYzMuuuu2uy/K6E9JA24N
ACufuqMqgGSXc51fJ/6V5Qi9YtVd7TWBkZQSZJJADBHs/YyYD9Q==
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode main
NXR_A(config-ipsec-isakmp)#remote address ip 10.10.20.1
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrb
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address LAN_B
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#ip address 10.10.10.1/24
NXR_A(config-if)#ipsec policy 1
NXR_A(config-if)#exit
NXR_A(config)#fast-forwarding enable
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 0.0.0.0/0 10.10.20.254
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
NXR_B(config)#ipsec generate rsa-sig-key 1024
RSA-SIG KEY generating...
NXR_B(config)#exit
NXR_B#show ipsec rsa-pub-key
RSA public key :
0sAQOx8kE6uhZTvWMikunsy3uK5/7jIkTXsCjQpgo4B+X64UAVeuxFQZ3KG3bzyjmyCbpkt0xEiU+v1kF4AO
AOXoDfgND+KAdEky/YWqQYzMuuuu2uy/K6E9JA24NACufuqMqgGSXc51fJ/6V5Qi9YtVd7TWBkZQSZJJAD
BHs/YyYD9Q==
NXR_B#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication rsa-sig 0sAQNe9Ghb4CNEaJuIIy67aSxECLJDHhvndH1opuMs
6P8yGiTNlcGeSOQ8XEy8iYTst2bv022XUxSt37RhOR5lRiY1i83TXkQZbhnJDCNJv+rtX/aro745MbJ9auXT1L5
tda4C54S7SELboAtU28sD3si0OwlzLWtE7yRUqLP4ZiiNMw==
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#remote identity fqdn nxra
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address 10.10.20.1/24
NXR_B(config-if)#ipsec policy 1
NXR_B(config-if)#exit
NXR_B(config)#fast-forwarding enable
NXR_B(config)#exit
NXR_B#save config
```

【 設定例解説 】

〔NXR_A の設定〕

1. <ホスト名の設定>

```
nxr120(config)#hostname NXR_A
```

ホスト名を NXR_A と設定します。

2. <LAN 側(ethernet0)インタフェース設定>

```
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
```

LAN 側(ethernet0)インタフェースの IP アドレスとして 192.168.10.1/24 を設定します。

3. <スタティックルート設定>

```
NXR_A(config)#ip route 0.0.0.0/0 10.10.10.254
```

デフォルトルートを設定します。ゲートウェイアドレスは上位ルータの IP アドレスを設定します。

4. <IPsec アクセスリスト設定>

```
NXR_A(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
```

IPsec アクセスリスト名を LAN_B とし送信元 IP アドレス 192.168.10.0/24,宛先 IP アドレス 192.168.20.0/24 を設定します。Policy Based IPsec では IPsec アクセスリストで設定したルールに基づき IPsec で ESP 化するかどうかが決定されます。よってここで設定した送信元,宛先 IP アドレスにマッチしたパケットが IPsec のカプセル化対象となります。

5. <RSA Signature Key の作成>

```
NXR_A(config)#ipsec generate rsa-sig-key 1024
```

IPsec の認証で使用する RSA Signature Key を作成します。ここでは 1024bit で作成します。

6. <RSA 公開鍵の確認>

```
NXR_A#show ipsec rsa-pub-key
RSA public key :
0sAQNe9Ghb4CNEaJuIIy67aSxECLJDHhvndH1opuMs6P8yGiTNlcGeSOQ8XEy8iYTst2bv022XUxSt37RhOR
5lRiY1i83TXkQZbhnJDCNJv+rtX/aro745MbJ9auXT1L5tda4C54S7SELboAtU28sD3si0OwlzLWtE7yRUqLP4Z
iiNMw==
```

作成した RSA 公開鍵を確認します。ここで表示された公開鍵は対向の NXR の IPsec ISAKMP ポリシー設定で使用します。

7. <IPsec ローカルポリシー設定>

```
NXR_A(config)#ipsec local policy 1
```

IPsec ローカルポリシー1 を設定します。

```
NXR_A(config-ipsec-local)#address ip
```

IPsec トンネルの送信元 IP アドレスを設定します。この IP アドレスにはインタフェース設定で ipsec policy 1 と指定したインタフェースの IP アドレスが自動的に設定されます。

```
NXR_A(config-ipsec-local)#self-identity fqdn nxra
```

本装置の identity を設定します。ここでは ID として FQDN 方式で nxra と設定します。
RSA 公開鍵暗号方式を利用する場合は、identity 設定が必須になります。

8. <IPsec ISAKMP ポリシー設定>

```
NXR_A(config)#ipsec isakmp policy 1
```

NXR_B との IPsec 接続で使用する ISAKMP ポリシー1 を設定します。

```
NXR_A(config-ipsec-isakmp)#description NXR_B
```

ISAKMP ポリシー1 の説明として NXR_B を設定します。

```
NXR_A(config-ipsec-isakmp)#authentication rsa-sig 0sAQOx8kE6uhZTvWMikunsy3uK5/7jIkTX sCjQpgo4B+
X64UAVeuxFQZ3KG3bzyjmyCbpkt0xEiU+v1kF4AOAOXoDfgND+KAdEky/YWqQYzMuuuu2uy/K6E9JA24NAC
ufuqMqgGSXc51fJ/6V5Qi9YtVd7TWBkZQSZJJADBHs/YyYD9Q==
```

認証方式として rsa-sig(公開鍵暗号方式)を選択し NXR_B で作成した公開鍵を設定します。この設定の前までに対向の NXR の公開鍵は作成しておく必要があります。

```
NXR_A(config-ipsec-isakmp)#hash sha1
```

認証アルゴリズムとして sha1 を設定します。

```
NXR_A(config-ipsec-isakmp)#encryption aes128
```

暗号化アルゴリズムとして aes128 を設定します。

```
NXR_A(config-ipsec-isakmp)#group 5
```

Diffie-Hellman(DH)グループとして group 5 を設定します。

```
NXR_A(config-ipsec-isakmp)#lifetime 10800
```

ISAKMP SA のライフタイムとして 10800 秒を設定します。

```
NXR_A(config-ipsec-isakmp)#isakmp-mode main
```

フェーズ 1 のネゴシエーションモードを設定します。RSA 公開鍵暗号方式を利用する場合はメインモードを使用する必要があります。

```
NXR_A(config-ipsec-isakmp)#remote address ip 10.10.20.1
```

対向の NXR の WAN 側 IP アドレスを設定します。ここでは対向の NXR の WAN 側 IP アドレス 10.10.20.1 を設定します。

```
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrb
```

対向の NXR の identity を設定します。ここでは ID として FQDN 方式で nxrb と設定します。

```
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic restart
```

IKE KeepAlive(DPD)を設定します。ここでは 30 秒間隔で 3 回リトライを行い keepalive 失敗時に SA を削除し IKE のネゴシエーションを開始するよう設定します。

DPD(Dead Peer Detection)は ISAKMP SA を監視する機能で対向の NXR の WAN 側で障害が発生した場合などにそれを検知し、現在利用している SA を削除したり SA を削除して再ネゴシエーションを行ったりするなどの機能があります。なお DPD は常に定期的に送信されるわけではなく対向の NXR より IPsec パケットを受信している場合は DPD パケットの送信は行われません。

```
NXR_A(config-ipsec-isakmp)#local policy 1
```

関連づけを行う IPsec ローカルポリシーとして IPsec ローカルポリシー1 を設定します。

9. <IPsec トンネルポリシー設定>

```
NXR_A(config)#ipsec tunnel policy 1
```

NXR_B との IPsec 接続で使用するトンネルポリシー1 を設定します。

```
NXR_A(config-ipsec-tunnel)#description NXR_B
```

トンネルポリシー1 の説明として NXR_B を設定します。

```
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
```

IPsec ポリシーのネゴシエーションモードはネゴシエーションを自ら開始したり、逆にいかなる場合も自らネゴシエーションを開始しないという設定が可能です。
ここではネゴシエーションモードを auto に設定します。これによりこちらからネゴシエーションを開始することができます。

```
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
```

IPsec トンネルポリシーで使用するトランスフォーム(プロポーザル)を設定します。
ここでは暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1 を設定します。

```
NXR_A(config-ipsec-tunnel)#set pfs group5
```

PFS(Perfect Forward Secrecy)の設定とそれに伴う DH グループを設定します。
ここでは PFS を有効とし、かつ DH グループとして group5 を設定します。

```
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
```

IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
```

関連づけを行う ISAKMP ポリシーとして ISAKMP ポリシー1 を設定します。

```
NXR_A(config-ipsec-tunnel)#match address LAN_B
```

IPsec アクセスリストとして LAN_B を設定します。

10. <WAN 側(ethernet1)インタフェース設定>

```
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#ip address 10.10.10.1/24
```

WAN 側(ethernet1)インタフェースの IP アドレスとして 10.10.10.1/24 を設定します。

```
NXR_A(config-if)#ipsec policy 1
```

IPsec トンネルのエンドポイントとなるため IPsec ローカルポリシー1 を設定します。

11. <ファストフォワーディングの有効化>

```
NXR_A(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(☞) ファストフォワーディングの詳細および利用時の制約については、NXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

〔NXR_B の設定〕

1. <ホスト名の設定>

```
nxr120(config)#hostname NXR_B
```

ホスト名を NXR_B と設定します。

2. <LAN 側(ethernet0)インタフェース設定>

```
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
```

LAN 側(ethernet0)インタフェースの IP アドレスとして 192.168.20.1/24 を設定します。

3. <スタティックルート設定>

```
NXR_B(config)#ip route 0.0.0.0/0 10.10.20.254
```

デフォルトルートを設定します。ゲートウェイアドレスは上位ルータの IP アドレスを設定します。

4. <IPsec アクセスリスト設定>

```
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
```

IPsec アクセスリスト名を LAN_A とし送信元 IP アドレス 192.168.20.0/24,宛先 IP アドレス 192.168.10.0/24 を設定します。

5. <RSA Signature Key の作成>

```
NXR_B(config)#ipsec generate rsa-sig-key 1024
```

IPsec の認証で使用する RSA Signature Key を作成します。ここでは 1024bit で作成します。

6. <RSA 公開鍵の確認>

```
NXR_B#show ipsec rsa-pub-key
RSA public key :
0sAQOx8kE6uhZTvWMikunsy3uK5/7jIkTXsCjQpgo4B+X64UAVeuxFQZ3KG3bzyjmyCbpkt0xEiU+v1kF4AO
AOXoDfgND+KAdEky/YWqQYzMuuuu2uy/K6E9JA24NACufuqMqgGSXc51fJ/6V5Qi9YtVd7TWBkZQSZJJAD
BHs/YyYD9Q==
```

作成した RSA 公開鍵を確認します。ここで表示された公開鍵は対向の NXR の IPsec ISAKMP ポリシー設定で使用します。

7. <IPsec ローカルポリシー設定>

```
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
```

IPsec ローカルポリシー1 で IPsec トンネルの送信元 IP アドレスを設定します。

```
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
```

本装置の identity を設定します。ここでは ID として FQDN 方式で nxrb と設定します。

8. <IPsec ISAKMP ポリシー設定>

```
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication rsa-sig 0sAQNe9Ghb4CNEaJuIIy67aSxECLJDHhvndH1opuMs
6P8yGiTNlcGeSOQ8XEy8iYTst2bv022XUxSt37RhOR5lRiY1i83TXkQZbhnJDCNJv+rtX/aro745MbJ9auXT1L5td
a4C54S7SELboAtU28sD3si0OwlzLWtE7yRUqLP4ZiiNMw==
```

NXR_A との IPsec 接続で使用する ISAKMP ポリシー1 を設定します。

ISAKMP ポリシー1 の説明として NXR_A、認証方式として rsa-sig(公開鍵暗号方式)を選択し NXR_A で作成した公開鍵を設定します。

```
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
```

認証アルゴリズムとして sha1、暗号化アルゴリズムとして aes128、Diffie-Hellman(DH)グループとして group 5、ISAKMP SA のライフタイムとして 10800 秒、フェーズ 1 のネゴシエーションモードとしてメインモードを設定します。

```
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#remote identity fqdn nxra
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
```

NXR_A の WAN 側 IP アドレス 10.10.10.1、identity として FQDN 方式で nxra、IKE KeepAlive(DPD)を監視間隔 30 秒,リトライ回数 3 回とし keepalive 失敗時に SA を削除し IKE のネゴシエーションを開始するよう設定します。

そして IPsec ローカルポリシー1 と関連づけを行います。

9. <IPsec トンネルポリシー設定>

```
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
```

NXR_A との IPsec 接続で使用するトンネルポリシー1 を設定します。

IPsec トンネルポリシー1 の説明として NXR_A、ネゴシエーションモードとして auto を設定します。

```
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして LAN_A を設定します。

10. <WAN 側(ethernet1)インタフェース設定>

```
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address 10.10.20.1/24
NXR_B(config-if)#ipsec policy 1
```

WAN 側(ethernet1)インタフェースの IP アドレスとして 10.10.20.1/24 を設定します。

また IPsec トンネルのエンドポイントとなるため IPsec ローカルポリシー1 を設定します。

11. <ファストフォワーディングの有効化>

```
NXR_B(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。

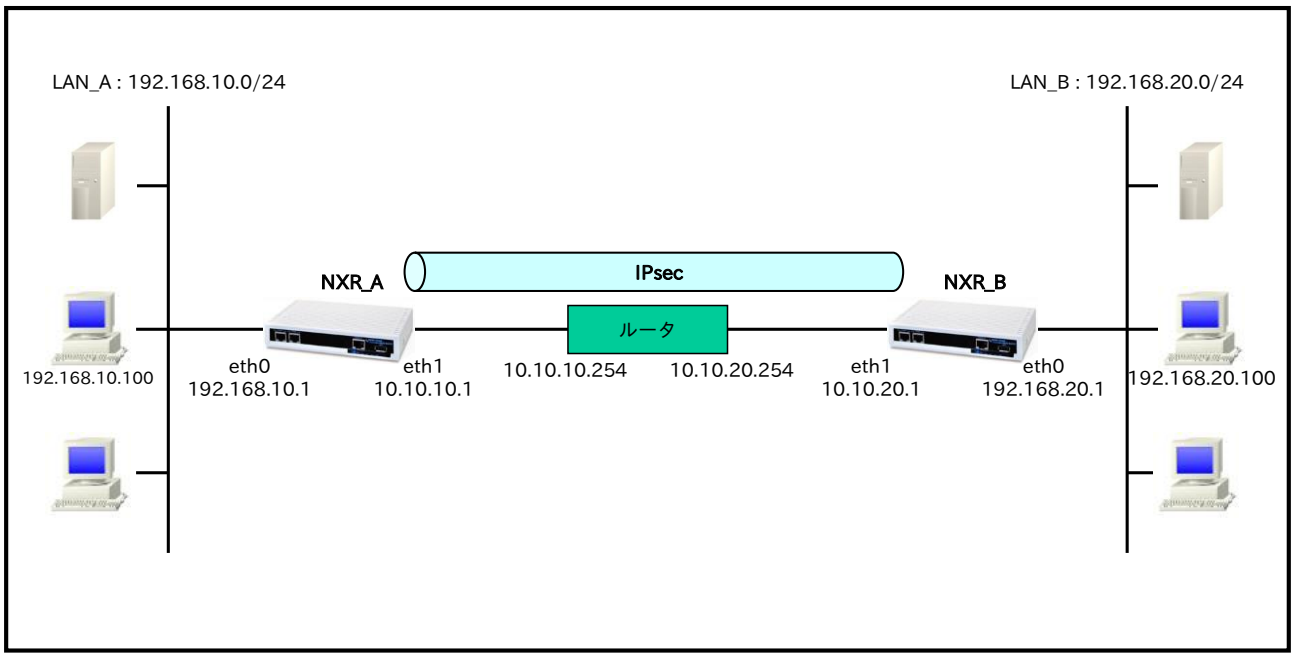
【 パソコンの設定例 】

	LAN A のパソコン	LAN B のパソコン
IP アドレス	192.168.10.100	192.168.20.100
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1

1-4. X.509(デジタル署名認証)方式での接続設定例

IKE フェーズ 1 で対向の NXR との認証に X.509(デジタル署名認証)方式を利用することができます。
認証で利用する証明書や鍵は FutureNet RA シリーズや別途 CA 等で事前に用意しておく必要があります(NXR では証明書の発行を行うことはできません)。また X.509 方式を利用する場合は IKE フェーズ 1 でメインモードを使用する必要があります。

【 構成図 】



- X.509 方式を利用する場合はフェーズ 1 でメインモードを選択する必要があります。
- X.509 で必要となる証明書や鍵は NXR シリーズでは発行をすることができませんので FutureNet RA シリーズで発行するか、別途 CA 等で用意しておく必要があります。
- 各種証明書は FTP および SSH によるインポートが可能です。この設定例では FTP サーバからのインポートを行います。
- 証明書を保管しているサーバを 192.168.10.10,192.168.20.10 とします。
- サーバにはそれぞれ NXR_A,NXR_B のルータで使用する証明書として以下の証明書が保管されています。

192.168.10.10 のサーバ		192.168.20.10 のサーバ	
証明書名	ファイル名	証明書名	ファイル名
CA 証明書	nxrCA.pem	CA 証明書	nxrCA.pem
CRL	nxrCRL.pem	CRL	nxrCRL.pem
NXR_A 用証明書	nxraCert.pem	NXR_B 用証明書	nxrbCert.pem
NXR_A 用秘密鍵	nxraKey.pem	NXR_B 用秘密鍵	nxrbKey.pem

ここでは各証明書の拡張子として pem を使用します。

(☞) 各証明書は DER または PEM フォーマットでなくてはなりません。
なおどのフォーマットの証明書かどうかはファイルの拡張子で自動的に判断されます。
よって PEM の場合は pem,DER の場合は der また cer の拡張子でなければなりません。
なおシングル DES で暗号化された鍵ファイルは使用することができません。

・ この設定例では ISAKMP ポリシー(フェーズ 1)で利用するプロポーザルは以下のとおりです。

認証アルゴリズム	SHA-1
暗号化アルゴリズム	AES-128
Diffie-Hellman(DH)グループ	Group5
対向の認証方式	事前共有鍵(Pre-Shared Key)
ネゴシエーションモード	Main
ライフタイム	10800(s)

・ この設定例ではトンネルポリシー(フェーズ 2)で利用するプロポーザルは以下のとおりです。

認証アルゴリズム	ESP-SHA1-HMAC
暗号化アルゴリズム	ESP-AES128
Diffie-Hellman(DH)グループ	Group5
ライフタイム	3600(s)

【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 0.0.0.0/0 10.10.10.254
NXR_A(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
NXR_A(config)#ipsec x509 enable
NXR_A(config)#ipsec x509 ca-certificate nxr ftp://192.168.10.10/nxrCA.pem
NXR_A(config)#ipsec x509 crl nxr ftp://192.168.10.10/nxrCRL.pem
NXR_A(config)#ipsec x509 certificate nxra ftp://192.168.10.10/nxraCert.pem
NXR_A(config)#ipsec x509 private-key nxra key ftp://192.168.10.10/nxraKey.pem
NXR_A(config)#ipsec x509 private-key nxra password nxrapass
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#x509 certificate nxra
NXR_A(config-ipsec-local)#self-identity dn /C=JP/CN=nxra/E=nxra@example.com
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication rsa-sig
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode main
NXR_A(config-ipsec-isakmp)#remote address ip 10.10.20.1
NXR_A(config-ipsec-isakmp)#remote identity dn /C=JP/CN=nxrb/E=nxrb@example.com
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address LAN_B
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#ip address 10.10.10.1/24
NXR_A(config-if)#ipsec policy 1
NXR_A(config-if)#exit
NXR_A(config)#fast-forwarding enable
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 0.0.0.0/0 10.10.20.254
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
NXR_B(config)#ipsec x509 enable
NXR_B(config)#ipsec x509 ca-certificate nxr ftp://192.168.20.10/nxrCA.pem
NXR_B(config)#ipsec x509 crl nxr ftp://192.168.20.10/nxrCRL.pem
NXR_B(config)#ipsec x509 certificate nxrb ftp://192.168.20.10/nxrbCert.pem
NXR_B(config)#ipsec x509 private-key nxrb key ftp://192.168.20.10/nxrbKey.pem
NXR_B(config)#ipsec x509 private-key nxrb password nxrbpass
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#x509 certificate nxrb
NXR_B(config-ipsec-local)#self-identity dn /C=JP/CN=nxrb/E=nxrb@example.com
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication rsa-sig
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#remote identity dn /C=JP/CN=nxra/E=nxra@example.com
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address 10.10.20.1/24
NXR_B(config-if)#ipsec policy 1
NXR_B(config-if)#exit
NXR_B(config)#fast-forwarding enable
NXR_B(config)#exit
NXR_B#save config
```

【 設定例解説 】

〔NXR_A の設定〕

1. <ホスト名の設定>

```
nxr120(config)#hostname NXR_A
```

ホスト名を NXR_A と設定します。

2. <LAN 側(ethernet0)インタフェース設定>

```
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
```

LAN 側(ethernet0)インタフェースの IP アドレスとして 192.168.10.1/24 を設定します。

3. <スタティックルート設定>

```
NXR_A(config)#ip route 0.0.0.0/0 10.10.10.254
```

デフォルトルートを設定します。ゲートウェイアドレスは上位ルータの IP アドレスを設定します。

4. <IPsec アクセスリスト設定>

```
NXR_A(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
```

IPsec アクセスリスト名を LAN_B とし送信元 IP アドレス 192.168.10.0/24,宛先 IP アドレス 192.168.20.0/24 を設定します。Policy Based IPsec では IPsec アクセスリストで設定したルールに基づき IPsec で ESP 化するかどうかが決定されます。よってここで設定した送信元,宛先 IP アドレスにマッチしたパケットが IPsec のカプセル化対象となります。

5. <X.509 の有効化>

```
NXR_A(config)#ipsec x509 enable
```

X.509 機能を有効にします。

6. <CA 証明書の設定>

```
NXR_A(config)#ipsec x509 ca-certificate nxr ftp://192.168.10.10/nxrCA.pem
```

FTP サーバ 192.168.10.10 にある CA 証明書ファイル nxrCA.pem をインポートします。

7. <CRL の設定>

```
NXR_A(config)#ipsec x509 crl nxr ftp://192.168.10.10/nxrCRL.pem
```

FTP サーバ 192.168.10.10 にある CRL ファイル nxrCRL.pem をインポートします。

8. <NXR_A 用公開鍵証明書の設定>

```
NXR_A(config)#ipsec x509 certificate nxra ftp://192.168.10.10/nxraCert.pem
```

FTP サーバ 192.168.10.10 にある NXR_A 用公開鍵証明書ファイル nxraCert.pem をインポートします。

9. <NXR_A 用秘密鍵の設定>

```
NXR_A(config)#ipsec x509 private-key nxra key ftp://192.168.10.10/nxraKey.pem
```

FTP サーバ 192.168.10.10 にある NXR_A 用秘密鍵ファイル nxraKey.pem をインポートします。

10. <NXR_A 用秘密鍵パスフレーズの設定>

```
NXR_A(config)#ipsec x509 private-key nxra password nxrapass
```

NXR_A 用秘密鍵のパスフレーズである nxrapass を設定します。

(☞) パスフレーズを暗号化する場合は hidden オプションを設定します。

11. <IPsec ローカルポリシー設定>

```
NXR_A(config)#ipsec local policy 1
```

IPsec ローカルポリシー1 を設定します。

```
NXR_A(config-ipsec-local)#address ip
```

IPsec トンネルの送信元 IP アドレスを設定します。この IP アドレスにはインタフェース設定で ipsec policy 1 と指定したインタフェースの IP アドレスが自動的に設定されます。

```
NXR_A(config-ipsec-local)#x509 certificate nxra
```

X.509 で利用する証明書を指定します。ここでは 8. <NXR_A 用公開鍵証明書の設定>で設定した certificate name nxra を設定します。

```
NXR_A(config-ipsec-local)#self-identity dn /C=JP/CN=nxra/E=nxra@example.com
```

本装置の identity を設定します。ここでは/C=JP/CN=nxra/E=nxra@example.com を設定します。

X.509 では機器の identity は DN(Distinguished Name)方式で設定する必要があります。よって設定前に証明書の DN または subject 等をご確認下さい。

なお X.509 を利用する場合は identity 設定は必須になります。

12. <IPsec ISAKMP ポリシー設定>

```
NXR_A(config)#ipsec isakmp policy 1
```

NXR_B との IPsec 接続で使用する ISAKMP ポリシー1 を設定します。

```
NXR_A(config-ipsec-isakmp)#description NXR_B
```

ISAKMP ポリシー1 の説明として NXR_B を設定します。

```
NXR_A(config-ipsec-isakmp)#authentication rsa-sig
```

認証方式として X.509 を利用する場合は rsa-sig を選択します。

```
NXR_A(config-ipsec-isakmp)#hash sha1
```

認証アルゴリズムとして sha1 を設定します。

```
NXR_A(config-ipsec-isakmp)#encryption aes128
```

暗号化アルゴリズムとして aes128 を設定します。

```
NXR_A(config-ipsec-isakmp)#group 5
```

Diffie-Hellman(DH)グループとして group 5 を設定します。

```
NXR_A(config-ipsec-isakmp)#lifetime 10800
```
ISAKMP SA のライフタイムとして 10800 秒を設定します。

```
NXR_A(config-ipsec-isakmp)#isakmp-mode main
```
フェーズ 1 のネゴシエーションモードを設定します。X.509 を利用する場合はメインモードを使用する必要があります。

```
NXR_A(config-ipsec-isakmp)#remote address ip 10.10.20.1
```
対向の NXR の WAN 側 IP アドレスを設定します。ここでは対向の NXR の WAN 側 IP アドレス 10.10.20.1 を設定します。

```
NXR_A(config-ipsec-isakmp)#remote identity dn /C=JP/CN=nxrb/E=nxrb@example.com
```
対向の NXR の identity を設定します。
ここでは/C=JP/CN=nxrb/E=nxrb@example.com を設定します。
対向の NXR の identity に関しても DN(Distinguished Name)方式で設定しますので、設定前に対向の NXR の証明書の DN または subject 等をご確認下さい。
なお X.509 を利用する場合は、identity 設定は必須になります。

```
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic restart
```
IKE KeepAlive(DPD)を設定します。ここでは 30 秒間隔で 3 回リトライを行い keepalive 失敗時に SA を削除し IKE のネゴシエーションを開始するよう設定します。
DPD(Dead Peer Detection)は ISAKMP SA を監視する機能で対向の NXR の WAN 側で障害が発生した場合などにそれを検知し、現在利用している SA を削除したり SA を削除して再ネゴシエーションを行ったりするなどの機能があります。なお DPD は常に定期的に送信されるわけではなく対向の NXR より IPsec パケットを受信している場合は DPD パケットの送信は行われません。

```
NXR_A(config-ipsec-isakmp)#local policy 1
```
関連づけを行う IPsec ローカルポリシーとして IPsec ローカルポリシー1 を設定します。

13. <IPsec トンネルポリシー設定>

```
NXR_A(config)#ipsec tunnel policy 1
```
NXR_B との IPsec 接続で使用するトンネルポリシー1 を設定します。

```
NXR_A(config-ipsec-tunnel)#description NXR_B
```
トンネルポリシー1 の説明として NXR_B を設定します。

```
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
```
IPsec ポリシーのネゴシエーションモードはネゴシエーションを自ら開始したり、逆にいかなる場合も自らネゴシエーションを開始しないという設定が可能です。
ここではネゴシエーションモードを auto に設定します。これによりこちらからネゴシエーションを開始することができます。

```
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
```

IPsec トンネルポリシーで使用するトランスフォーム(プロポーザル)を設定します。

ここでは暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1 を設定します。

```
NXR_A(config-ipsec-tunnel)#set pfs group5
```

PFS(Perfect Forward Secrecy)の設定とそれに伴う DH グループを設定します。

ここでは PFS を有効とし、かつ DH グループとして group5 を設定します。

```
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
```

IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
```

関連づけを行う ISAKMP ポリシーとして ISAKMP ポリシー1 を設定します。

```
NXR_A(config-ipsec-tunnel)#match address LAN_B
```

IPsec アクセスリストとして LAN_B を設定します。

14. <WAN 側(ethernet1)インタフェース設定>

```
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#ip address 10.10.10.1/24
```

WAN 側(ethernet1)インタフェースの IP アドレスとして 10.10.10.1/24 を設定します。

```
NXR_A(config-if)#ipsec policy 1
```

IPsec トンネルのエンドポイントとなるため IPsec ローカルポリシー1 を設定します。

15. <ファストフォワーディングの有効化>

```
NXR_A(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(☞) ファストフォワーディングの詳細および利用時の制約については、NXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

〔NXR_B の設定〕

1. <ホスト名の設定>

```
nxr120(config)#hostname NXR_B
```

ホスト名を NXR_B と設定します。

2. <LAN 側(ethernet0)インタフェース設定>

```
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
```

LAN 側(ethernet0)インタフェースの IP アドレスとして 192.168.20.1/24 を設定します。

3. <スタティックルート設定>

```
NXR_B(config)#ip route 0.0.0.0/0 10.10.20.254
```

デフォルトルートを設定します。ゲートウェイアドレスは上位ルータの IP アドレスを設定します。

4. <IPsec アクセスリスト設定>

```
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
```

IPsec アクセスリスト名を LAN_A とし送信元 IP アドレス 192.168.20.0/24,宛先 IP アドレス 192.168.10.0/24 を設定します。

5. <X.509 の有効化および証明書等の設定>

```
NXR_B(config)#ipsec x509 enable
NXR_B(config)#ipsec x509 ca-certificate nxr ftp://192.168.20.10/nxrCA.pem
NXR_B(config)#ipsec x509 crl nxr ftp://192.168.20.10/nxrCRL.pem
NXR_B(config)#ipsec x509 certificate nxrb ftp://192.168.20.10/nxrbCert.pem
NXR_B(config)#ipsec x509 private-key nxrb key ftp://192.168.20.10/nxrbKey.pem
NXR_B(config)#ipsec x509 private-key nxrb password nxrbpass
```

X.509 機能を有効にし、各証明書や秘密鍵等のインポートおよび秘密鍵に対するパスフレーズを設定します。インポートによる設定は NXR_A と同等ですので、詳細は 5. <X.509 の有効化>、6. <CA 証明書の設定>、7. <CRL の設定>、8. <NXR_A 用公開鍵証明書の設定>、9. <NXR_A 用秘密鍵の設定>、10. <NXR_A 用秘密鍵パスフレーズの設定>をご参照下さい。

6. <IPsec ローカルポリシー設定>

```
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#x509 certificate nxrb
```

IPsec ローカルポリシー1 で IPsec トンネルの送信元 IP アドレスを設定します。
また X.509 で利用する証明書を指定します。ここでは 5. X.509 の有効化および証明書等の設定で設定した certificate name nxrb を設定します。

```
NXR_B(config-ipsec-local)#self-identity dn /C=JP/CN=nxrb/E=nxrb@example.com
```

本装置の identity を設定します。ここでは/C=JP/CN=nxrb/E=nxrb@example.com を設定します。

7. <IPsec ISAKMP ポリシー設定>

```
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication rsa-sig
```

NXR_A との IPsec 接続で使用する ISAKMP ポリシー1 を設定します。ISAKMP ポリシー1 の説明として NXR_A、認証方式として X.509 を利用する場合は rsa-sig を選択します。

```
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
```

認証アルゴリズムとして sha1、暗号化アルゴリズムとして aes128、Diffie-Hellman(DH)グループとして group 5、ISAKMP SA のライフタイムとして 10800 秒、フェーズ 1 のネゴシエーションモードとしてメ

インモードを設定します。

```
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#remote identity dn /C=JP/CN=nxra/E=nxra@example.com
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
```

NXR_A の WAN 側 IP アドレス 10.10.10.1、対向の NXR の identity として /C=JP/CN=nxra/E=nxra@example.com、IKE KeepAlive(DPD)を監視間隔 30 秒,リトライ回数 3 回とし keepalive 失敗時に SA を削除し IKE のネゴシエーションを開始するよう設定します。
そして IPsec ローカルポリシー1 と関連づけを行います。

8. <IPsec トンネルポリシー設定>

```
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
```

NXR_A との IPsec 接続で使用するトンネルポリシー1 を設定します。
IPsec トンネルポリシー1 の説明として NXR_A、ネゴシエーションモードとして auto を設定します。

```
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして LAN_A を設定します。

9. <WAN 側(ethernet1)インタフェース設定>

```
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address 10.10.20.1/24
NXR_B(config-if)#ipsec policy 1
```

WAN 側(ethernet1)インタフェースの IP アドレスとして 10.10.20.1/24 を設定します。
また IPsec トンネルのエンドポイントとなるため IPsec ローカルポリシー1 を設定します。

10. <ファストフォワーディングの有効化>

```
NXR_B(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。

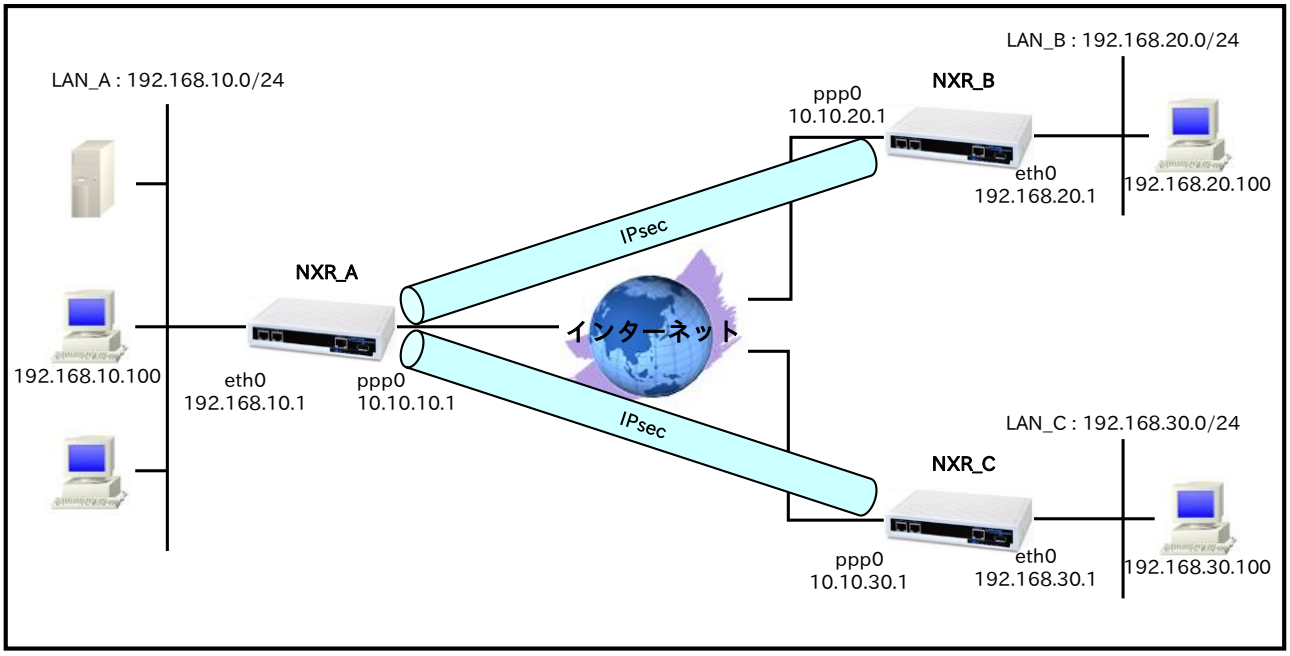
【 パソコンの設定例 】

	LAN A のパソコン	LAN B のパソコン
IP アドレス	192.168.10.100	192.168.20.100
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1

1-5. PPPoE を利用した IPsec 接続設定例

PPPoE 上でも IPsec を利用することは可能です。ここではフェーズ 1 で NXR_A(センタ) － NXR_B(拠点)間はメインモードを NXR_A(センタ) － NXR_C(拠点)間はアグレッシブモードを利用して接続しています。なお本設定例では IPsec 経由での拠点間通信は行いません。
またここでは各拠点からのインターネットアクセスを可能にするために、フィルタ設定(SPI),NAT 設定(IP マスカレード),DNS 設定を行います。

【 構成図 】



- NXR_A⇔NXR_B 間はメインモード(事前共有鍵は ipseckey1),NXR_A⇔NXR_C 間はアグレッシブモード(事前共有鍵は ipseckey2)を利用します。
- この設定例では IPsec 経由での拠点間通信は行いません。
- 各拠点からのインターネットアクセスを可能にするため NAT 設定(IP マスカレード)やフィルタ設定(SPI)および DNS 設定を行います。

【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 0.0.0.0/0 ppp 0
NXR_A(config)#ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
NXR_A(config)#ip access-list ppp0_in permit any 10.10.10.1 50
NXR_A(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
NXR_A(config)#ipsec access-list LAN_C ip 192.168.10.0/24 192.168.30.0/24
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode main
NXR_A(config-ipsec-isakmp)#remote address ip 10.10.20.1
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address LAN_B
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#ipsec isakmp policy 2
NXR_A(config-ipsec-isakmp)#description NXR_C
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A(config-ipsec-isakmp)#remote address ip any
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrc
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 2
NXR_A(config-ipsec-tunnel)#description NXR_C
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 2
NXR_A(config-ipsec-tunnel)#match address LAN_C
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface ppp 0
NXR_A(config-ppp)#ip address 10.10.10.1/32
NXR_A(config-ppp)#ip masquerade
```

```
NXR_A(config-ppp)#ip access-group in ppp0_in
NXR_A(config-ppp)#ip spi-filter
NXR_A(config-ppp)#ip tcp adjust-mss auto
NXR_A(config-ppp)#no ip redirects
NXR_A(config-ppp)#ppp username test1@example.jp password test1pass
NXR_A(config-ppp)#ipsec policy 1
NXR_A(config-ppp)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#no ip address
NXR_A(config-if)#pppoe-client ppp 0
NXR_A(config-if)#exit
NXR_A(config)#dns
NXR_A(config-dns)#service enable
NXR_A(config-dns)#exit
NXR_A(config)#fast-forwarding enable
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 0.0.0.0/0 ppp 0
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 udp 500 500
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 50
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface ppp 0
NXR_B(config-ppp)#ip address 10.10.20.1/32
NXR_B(config-ppp)#ip masquerade
NXR_B(config-ppp)#ip access-group in ppp0_in
NXR_B(config-ppp)#ip spi-filter
NXR_B(config-ppp)#ip tcp adjust-mss auto
NXR_B(config-ppp)#no ip redirects
NXR_B(config-ppp)#ppp username test2@example.jp password test2pass
NXR_B(config-ppp)#ipsec policy 1
```

```
NXR_B(config-ppp)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#no ip address
NXR_B(config-if)#pppoe-client ppp 0
NXR_B(config-if)#exit
NXR_B(config)#dns
NXR_B(config-dns)#service enable
NXR_B(config-dns)#exit
NXR_B(config)#fast-forwarding enable
NXR_B(config)#exit
NXR_B#save config
```

〔NXR_C の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_C
NXR_C(config)#interface ethernet 0
NXR_C(config-if)#ip address 192.168.30.1/24
NXR_C(config-if)#exit
NXR_C(config)#ip route 0.0.0.0/0 ppp 0
NXR_C(config)#ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
NXR_C(config)#ip access-list ppp0_in permit 10.10.10.1 any 50
NXR_C(config)#ipsec access-list LAN_A ip 192.168.30.0/24 192.168.10.0/24
NXR_C(config)#ipsec local policy 1
NXR_C(config-ipsec-local)#address ip
NXR_C(config-ipsec-local)#self-identity fqdn nxrc
NXR_C(config-ipsec-local)#exit
NXR_C(config)#ipsec isakmp policy 1
NXR_C(config-ipsec-isakmp)#description NXR_A
NXR_C(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR_C(config-ipsec-isakmp)#hash sha1
NXR_C(config-ipsec-isakmp)#encryption aes128
NXR_C(config-ipsec-isakmp)#group 5
NXR_C(config-ipsec-isakmp)#lifetime 10800
NXR_C(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_C(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_C(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_C(config-ipsec-isakmp)#local policy 1
NXR_C(config-ipsec-isakmp)#exit
NXR_C(config)#ipsec tunnel policy 1
NXR_C(config-ipsec-tunnel)#description NXR_A
NXR_C(config-ipsec-tunnel)#negotiation-mode auto
NXR_C(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_C(config-ipsec-tunnel)#set pfs group5
NXR_C(config-ipsec-tunnel)#set sa lifetime 3600
NXR_C(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_C(config-ipsec-tunnel)#match address LAN_A
NXR_C(config-ipsec-tunnel)#exit
NXR_C(config)#interface ppp 0
NXR_C(config-ppp)#ip address negotiated
NXR_C(config-ppp)#ip masquerade
NXR_C(config-ppp)#ip access-group in ppp0_in
NXR_C(config-ppp)#ip spi-filter
NXR_C(config-ppp)#ip tcp adjust-mss auto
NXR_C(config-ppp)#no ip redirects
NXR_C(config-ppp)#ppp username test3@example.jp password test3pass
NXR_C(config-ppp)#ipsec policy 1
NXR_C(config-ppp)#exit
NXR_C(config)#interface ethernet 1
NXR_C(config-if)#no ip address
NXR_C(config-if)#pppoe-client ppp 0
NXR_C(config-if)#exit
```

```
NXR_C(config)#dns
NXR_C(config-dns)#service enable
NXR_C(config-dns)#exit
NXR_C(config)#fast-forwarding enable
NXR_C(config)#exit
NXR_C#save config
```

【 設定例解説 】

〔NXR_A の設定〕

1. <ホスト名の設定>

```
nxr120(config)#hostname NXR_A
```

ホスト名に NXR_A を設定します。

2. <LAN 側(ethernet0)インタフェース設定>

```
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
```

LAN 側(ethernet0)インタフェースの IP アドレスとして 192.168.10.1/24 を設定します。

3. <スタティックルート設定>

```
NXR_A(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。なおゲートウェイとして ppp0 インタフェースを指定します。

4. <IP アクセスリスト設定>

```
NXR_A(config)#ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
NXR_A(config)#ip access-list ppp0_in permit any 10.10.10.1 50
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を ppp0_in とします。

一行目は宛先 IP アドレス 10.10.10.1,送信元 UDP ポート番号 500,宛先 UDP ポート番号 500 のパケットを許可する設定です。

二行目は宛先 IP アドレス 10.10.10.1,プロトコル番号 50(ESP)のパケットを許可する設定です。

なおこの IP アクセスリスト設定は ppp0 インタフェース設定で登録します。

(☞) IP アクセスリストを設定しただけではフィルタとして有効にはなりません。フィルタリングしたいインタフェースでの登録が必要になります。

(☞) UDP ポート 500 番およびプロトコル番号 50(ESP)は IPsec のネゴシエーションおよび通信で使用します。

5. <IPsec アクセスリスト設定>

```
NXR_A(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
NXR_A(config)#ipsec access-list LAN_C ip 192.168.10.0/24 192.168.30.0/24
```

一行目は IPsec アクセスリスト名を LAN_B とし送信元 IP アドレス 192.168.10.0/24,宛先 IP アドレス 192.168.20.0/24 を設定します。

二行目は IPsec アクセスリスト名を LAN_C とし、送信元 IP アドレス 192.168.10.0/24,宛先 IP アドレス

192.168.30.0/24 を設定します。
Policy Based IPsec では IPsec アクセスリストで設定したルールに基づき IPsec で ESP 化するかどうかが決定されます。よってここで設定した送信元,宛先 IP アドレスにマッチしたパケットが IPsec のカプセル化対象となります。

6. <IPsec ローカルポリシー設定>

```
NXR_A(config)#ipsec local policy 1
```

IPsec ローカルポリシー1 を設定します。

```
NXR_A(config-ipsec-local)#address ip
```

IPsec トンネルの送信元 IP アドレスを指定します。この IP アドレスはインタフェース設定で ipsec policy 1 と指定したインタフェースの IP アドレスが自動的に設定されます。

7. <IPsec ISAKMP ポリシー1 設定>

```
NXR_A(config)#ipsec isakmp policy 1
```

NXR_B との IPsec 接続で使用する ISAKMP ポリシー1 を設定します。

```
NXR_A(config-ipsec-isakmp)#description NXR_B
```

ISAKMP ポリシー1 の説明として NXR_B を設定します。

```
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey1
```

認証方式として pre-share(事前共有鍵) を選択し事前共有鍵 ipseckey1 を設定します。なおこの設定は対向の NXR と同じ値を設定する必要があります。

```
NXR_A(config-ipsec-isakmp)#hash sha1
```

認証アルゴリズムとして sha1 を設定します。

```
NXR_A(config-ipsec-isakmp)#encryption aes128
```

暗号化アルゴリズムとして aes128 を設定します。

```
NXR_A(config-ipsec-isakmp)#group 5
```

Diffie-Hellman(DH)グループとして group 5 を設定します。

```
NXR_A(config-ipsec-isakmp)#lifetime 10800
```

ISAKMP SA のライフタイムとして 10800 秒を設定します。

```
NXR_A(config-ipsec-isakmp)#isakmp-mode main
```

フェーズ 1 のネゴシエーションモードとしてここでは IPsec を使用するルータの WAN 側 IP アドレスがともに固定 IP アドレスのためメインモードを設定します。

```
NXR_A(config-ipsec-isakmp)#remote address ip 10.10.20.1
```

対向の NXR の WAN 側 IP アドレスを設定します。ここでは対向の NXR_B の WAN 側 IP アドレス

10.10.20.1 を設定します。

```
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic restart
```

IKE KeepAlive(DPD)を設定します。ここでは 30 秒間隔で 3 回リトライを行い keepalive 失敗時に SA を削除し IKE のネゴシエーションを開始するよう設定します。

DPD(Dead Peer Detection)は ISAKMP SA を監視する機能で対向の NXR の WAN 側で障害が発生した場合などにそれを検知し、現在利用している SA を削除したり SA を削除して再ネゴシエーションを行ったりするなどの機能があります。なお DPD は常に定期的に送信されるわけではなく対向の NXR より IPsec パケットを受信している場合は DPD パケットの送信は行われません。

```
NXR_A(config-ipsec-isakmp)#local policy 1
```

関連づけを行う IPsec ローカルポリシーとして IPsec ローカルポリシー1 を設定します。

8. <IPsec トンネルポリシー1 設定>

```
NXR_A(config)#ipsec tunnel policy 1
```

NXR_B との IPsec 接続で使用するトンネルポリシー1 を設定します。

```
NXR_A(config-ipsec-tunnel)#description NXR_B
```

トンネルポリシー1 の説明として NXR_B を設定します。

```
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
```

IPsec ポリシーのネゴシエーションモードはネゴシエーションを自ら開始したり、逆にいかなる場合も自らネゴシエーションを開始しないという設定が可能です。

ここではネゴシエーションモードを auto に設定します。これによりこちらからネゴシエーションを開始することができます。

```
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
```

IPsec トンネルポリシーで使用するトランスフォーム(プロポーザル)を設定します。

ここでは暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1 を設定します。

```
NXR_A(config-ipsec-tunnel)#set pfs group5
```

PFS(Perfect Forward Secrecy)の設定とそれに伴う DH グループを設定します。

ここでは PFS を有効とし、かつ DH グループとして group5 を設定します。

```
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
```

IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
```

関連づけを行う ISAKMP ポリシーとして ISAKMP ポリシー1 を設定します。

```
NXR_A(config-ipsec-tunnel)#match address LAN_B
```

IPsec アクセスリストとして LAN_B を設定します。

9. <IPsec ISAKMP ポリシー2 設定>

```
NXR_A(config)#ipsec isakmp policy 2
```

NXR_C との IPsec 接続で使用する ISAKMP ポリシー2 を設定します。

```
NXR_A(config-ipsec-isakmp)#description NXR_C
```

ISAKMP ポリシー2 の説明として NXR_C を設定します。

```
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey2
```

認証方式として pre-share(事前共有鍵) を選択し事前共有鍵 ipseckey2 を設定します。

```
NXR_A(config-ipsec-isakmp)#hash sha1
```

認証アルゴリズムとして sha1 を設定します。

```
NXR_A(config-ipsec-isakmp)#encryption aes128
```

暗号化アルゴリズムとして aes128 を設定します。

```
NXR_A(config-ipsec-isakmp)#group 5
```

Diffie-Hellman(DH)グループとして group 5 を設定します。

```
NXR_A(config-ipsec-isakmp)#lifetime 10800
```

ISAKMP SA のライフタイムとして 10800 秒を設定します。

```
NXR_A(config-ipsec-isakmp)#isakmp-mode aggressive
```

フェーズ 1 のネゴシエーションモードとして IPsec を使用するルータの WAN 側 IP アドレスが片側動的 IP アドレスのためアグレッシブモードを設定します。

```
NXR_A(config-ipsec-isakmp)#remote address ip any
```

対向の NXR の WAN 側 IP アドレスを設定します。ここでは対向の NXR_C の WAN 側 IP アドレスが動的 IP アドレスのため any を設定します。

```
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrc
```

対向の NXR の identity を設定します。ここでは ID として FQDN 方式で nxrc と設定します。
本設定が必要な理由は対向の NXR_C の WAN 側 IP アドレスが動的 IP アドレスのため IP アドレスを ID として利用することができないためです。

```
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic clear
```

IKE KeepAlive(DPD)を設定します。ここでは監視を 30 秒間隔で 3 回リトライを行い keepalive 失敗時に SA を削除するよう設定します。

```
NXR_A(config-ipsec-isakmp)#local policy 1
```

関連づけを行う IPsec ローカルポリシーとして IPsec ローカルポリシー1 を設定します。

10. <IPsec トンネルポリシー2 設定>

```
NXR_A(config)#ipsec tunnel policy 2
```

NXR_C との IPsec 接続で使用するトンネルポリシー2 を設定します。

```
NXR_A(config-ipsec-tunnel)#description NXR_C
```

トンネルポリシー2 の説明として NXR_C と設定します。

```
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
```

IPsec ポリシーのネゴシエーションモードはネゴシエーションを自ら開始したり、逆にいかなる場合も自らネゴシエーションを開始しないという設定が可能です。

ここではネゴシエーションモードを responder に設定します。これによりこちらからいかなる場合(Rekey を含む)においてもネゴシエーションを開始することはありません。

```
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
```

IPsec トンネルポリシーで使用するトランスフォーム(プロポーザル)を設定します。

ここでは暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1 を設定します。

```
NXR_A(config-ipsec-tunnel)#set pfs group5
```

PFS(Perfect Forward Secrecy)の設定とそれに伴う DH グループを設定します。

ここでは PFS を有効とし、かつ DH グループとして group5 を設定します。

```
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
```

IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 2
```

関連づけを行う ISAKMP ポリシーとして ISAKMP ポリシー2 を設定します。

```
NXR_A(config-ipsec-tunnel)#match address LAN_C
```

IPsec アクセスリストとして LAN_C を設定します。

11. <WAN 側(ppp0)インタフェース設定>

```
NXR_A(config)#interface ppp 0
NXR_A(config-ppp)#ip address 10.10.10.1/32
```

WAN 側(ppp0)インタフェースを設定します。

IP アドレスとして固定 IP アドレス 10.10.10.1/32 を設定します。

```
NXR_A(config-ppp)#ip masquerade
NXR_A(config-ppp)#ip access-group in ppp0_in
NXR_A(config-ppp)#ip spi-filter
NXR_A(config-ppp)#ip tcp adjust-mss auto
NXR_A(config-ppp)#no ip redirects
```

IP マスカレードを有効、IP アクセスリスト ppp0_in を in フィルタに適用、ステートフルパケットインスペクションを有効に設定します。

また TCP MSS の調整機能をオート、ICMP リダイレクト機能を無効に設定します。

```
NXR_A(config-ppp)#ppp username test1@example.jp password test1pass
NXR_A(config-ppp)#ipsec policy 1
```

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

また IPsec トンネルのエンドポイントとなるため IPsec ローカルポリシー1 を設定します。

12. <ethernet1 インタフェース設定>

```
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#no ip address
NXR_A(config-if)#pppoe-client ppp 0
```

ethernet1 インタフェースで、ppp0 インタフェースを PPPoE クライアントとして使用できるよう設定します。

13. <DNS 設定>

```
NXR_A(config)#dns
NXR_A(config-dns)#service enable
```

DNS 設定で DNS サービスを有効にします。

14. <ファストフォワーディングの有効化>

```
NXR_A(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(☞) ファストフォワーディングの詳細および利用時の制約については、NXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

〔NXR_B の設定〕

1. <ホスト名の設定>

```
nxr120(config)#hostname NXR_B
```

ホスト名に NXR_B を設定します。

2. <LAN 側(ethernet0)インタフェース設定>

```
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
```

LAN 側(ethernet0)インタフェースの IP アドレスとして 192.168.20.1/24 を設定します。

3. <スタティックルート設定>

```
NXR_B(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。なおゲートウェイとして ppp0 インタフェースを指定します。

4. <IP アクセスリスト設定>

```
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 udp 500 500
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 50
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を ppp0_in とします。

一行目は送信元 IP アドレス 10.10.10.1,宛先 IP アドレス 10.10.20.1,送信元 UDP ポート番号 500,宛先 UDP ポート番号 500 のパケットを許可する設定です。

二行目は送信元 IP アドレス 10.10.10.1,宛先 IP アドレス 10.10.20.1,プロトコル番号 50(ESP)のパケットを許可する設定です。

この IP アクセスリスト設定は ppp0 インタフェース設定で登録します。

(☞) UDP ポート 500 番およびプロトコル番号 50(ESP)は IPsec のネゴシエーションおよび通信で使用します。

5. <IPsec アクセスリスト設定>

```
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
```

IPsec アクセスリスト名を LAN_A とし送信元 IP アドレス 192.168.20.0/24,宛先 IP アドレス 192.168.10.0/24 を設定します。

6. <IPsec ローカルポリシー設定>

```
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
```

IPsec ローカルポリシー1 で IPsec トンネルの送信元 IP アドレスを設定します。

7. <IPsec ISAKMP ポリシー設定>

```
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey1
```

NXR_A との IPsec 接続で使用する ISAKMP ポリシー1 を設定します。

ISAKMP ポリシー1 の説明として NXR_A、認証方式として pre-share(事前共有鍵)を選択し事前共有鍵 ipseckey1 を設定します。

```
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
```

認証アルゴリズムとして sha1、暗号化アルゴリズムとして aes128、Diffie-Hellman(DH)グループとして group 5、ISAKMP SA のライフタイムとして 10800 秒、フェーズ 1 のネゴシエーションモードとしてメインモードを設定します。

```
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
```

NXR_A の WAN 側 IP アドレス 10.10.10.1、IKE KeepAlive(DPD)を監視間隔 30 秒,リトライ回数 3 回と

し keepalive 失敗時に SA を削除し IKE のネゴシエーションを開始するよう設定します。
そして IPsec ローカルポリシー1 と関連づけを行います。

8. <IPsec トンネルポリシー設定>

```
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
```

NXR_A との IPsec 接続で使用するトンネルポリシー1 を設定します。
IPsec トンネルポリシー1 の説明として NXR_A、ネゴシエーションモードとして auto を設定します。

```
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして LAN_A を設定します。

9. <WAN 側(ppp0)インタフェース設定>

```
NXR_B(config)#interface ppp 0
NXR_B(config-ppp)#ip address 10.10.20.1/32
```

WAN 側(ppp0)インタフェースを設定します。
IP アドレスとして固定 IP アドレス 10.10.20.1/32 を設定します。

```
NXR_B(config-ppp)#ip masquerade
NXR_B(config-ppp)#ip access-group in ppp0_in
NXR_B(config-ppp)#ip spi-filter
NXR_B(config-ppp)#ip tcp adjust-mss auto
NXR_B(config-ppp)#no ip redirects
```

IP マスカレードを有効、IP アクセスリスト ppp0_in を in フィルタに適用、ステートフルパケットインスペクションを有効に設定します。
また TCP MSS の調整機能をオート、ICMP リダイレクト機能を無効に設定します。

```
NXR_B(config-ppp)#ppp username test2@example.jp password test2pass
NXR_B(config-ppp)#ipsec policy 1
```

PPPoE 接続で使用するユーザ ID とパスワードを設定します。
また IPsec トンネルのエンドポイントとなるため IPsec ローカルポリシー1 を設定します。

10. <ethernet1 インタフェース設定>

```
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#no ip address
NXR_B(config-if)#pppoe-client ppp 0
```

ethernet1 インタフェースで、ppp0 インタフェースを PPPoE クライアントとして使用できるよう設定します。

11. <DNS 設定>

```
NXR_B(config)#dns
NXR_B(config-dns)#service enable
```

DNS 設定で DNS サービスを有効にします。

12. <ファストフォワーディングの有効化>

```
NXR_B(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。

〔NXR_C の設定〕

1. <ホスト名の設定>

```
nxr120(config)#hostname NXR_C
```

ホスト名に NXR_C を設定します。

2. <LAN 側(ethernet0)インタフェース設定>

```
NXR_C(config)#interface ethernet 0
NXR_C(config-if)#ip address 192.168.30.1/24
```

LAN 側(ethernet0)インタフェースの IP アドレスとして 192.168.30.1/24 を設定します。

3. <スタティックルート設定>

```
NXR_C(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。なおゲートウェイとして ppp0 インタフェースを指定します。

4. <IP アクセスリスト設定>

```
NXR_C(config)#ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
NXR_C(config)#ip access-list ppp0_in permit 10.10.10.1 any 50
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を ppp0_in とします。

一行目は送信元 IP アドレス 10.10.10.1,送信元 UDP ポート番号 500,宛先 UDP ポート番号 500 のパケットを許可する設定です。

二行目は送信元 IP アドレス 10.10.10.1,プロトコル番号 50(ESP)のパケットを許可する設定です。

この IP アクセスリスト設定は ppp0 インタフェース設定で登録します。

(☞) UDP ポート 500 番およびプロトコル番号 50(ESP)は IPsec のネゴシエーションおよび通信で使用します。

5. <IPsec アクセスリスト設定>

```
NXR_C(config)#ipsec access-list LAN_A ip 192.168.30.0/24 192.168.10.0/24
```

IPsec アクセスリスト名を LAN_A とし送信元 IP アドレス 192.168.30.0/24,宛先 IP アドレス 192.168.10.0/24 を設定します。

6. <IPsec ローカルポリシー設定>

```
NXR_C(config)#ipsec local policy 1
NXR_C(config-ipsec-local)#address ip
```

IPsec ローカルポリシー1 で IPsec トンネルの送信元 IP アドレスを設定します。

```
NXR_C(config-ipsec-local)#self-identity fqdn nxrc
```

本装置の identity を設定します。ここでは ID として FQDN 方式で nxrc と設定します。
本設定が必要な理由は WAN 側 IP アドレスが動的 IP アドレスのため対向の NXR_A で本装置の IP アドレスを ID として設定しておくことができないためです。

7. <IPsec ISAKMP ポリシー設定>

```
NXR_C(config)#ipsec isakmp policy 1
NXR_C(config-ipsec-isakmp)#description NXR_A
NXR_C(config-ipsec-isakmp)#authentication pre-share ipseckey2
```

ISAKMP ポリシー1 の説明として NXR_A、認証方式として pre-share(事前共有鍵)を選択し事前共有鍵 ipseckey2 を設定します。

```
NXR_C(config-ipsec-isakmp)#hash sha1
NXR_C(config-ipsec-isakmp)#encryption aes128
NXR_C(config-ipsec-isakmp)#group 5
NXR_C(config-ipsec-isakmp)#lifetime 10800
NXR_C(config-ipsec-isakmp)#isakmp-mode aggressive
```

認証アルゴリズムとして sha1、暗号化アルゴリズムとして aes128、Diffie-Hellman(DH)グループとして group 5、ISAKMP SA のライフタイムとして 10800 秒、フェーズ 1 のネゴシエーションモードとしてアグレッシブモードを設定します。

```
NXR_C(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_C(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_C(config-ipsec-isakmp)#local policy 1
```

NXR_A の WAN 側 IP アドレス 10.10.10.1、IKE KeepAlive(DPD)を監視間隔 30 秒,リトライ回数 3 回とし keepalive 失敗時に SA を削除し IKE のネゴシエーションを開始するよう設定します。
そして IPsec ローカルポリシー1 と関連づけを行います。

8. <IPsec トンネルポリシー設定>

```
NXR_C(config)#ipsec tunnel policy 1
NXR_C(config-ipsec-tunnel)#description NXR_A
NXR_C(config-ipsec-tunnel)#negotiation-mode auto
```

IPsec トンネルポリシー1 の説明として NXR_A、ネゴシエーションモードとして auto を設定します。

```
NXR_C(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_C(config-ipsec-tunnel)#set pfs group5
NXR_C(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_C(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_C(config-ipsec-tunnel)#match address LAN_A
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして LAN_A を設定します。

9. <WAN 側(ppp0)インタフェース設定>

```
NXR_C(config)#interface ppp 0
NXR_C(config-ppp)#ip address negotiated
```

WAN 側(ppp0)インタフェースを設定します。

IP アドレスとして動的 IP アドレスの場合は negotiated を設定します。

```
NXR_C(config-ppp)#ip masquerade
NXR_C(config-ppp)#ip access-group in ppp0_in
NXR_C(config-ppp)#ip spi-filter
NXR_C(config-ppp)#ip tcp adjust-mss auto
NXR_C(config-ppp)#no ip redirects
```

IP マスカレードを有効、IP アクセスリスト ppp0_in を in フィルタに適用、ステートフルパケットインスペクションを有効に設定します。

また TCP MSS の調整機能をオート、ICMP リダイレクト機能を無効に設定します。

```
NXR_C(config-ppp)#ppp username test3@example.jp password test3pass
NXR_C(config-ppp)#ipsec policy 1
```

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

また IPsec トンネルのエンドポイントとなるため IPsec ローカルポリシー1 を設定します。

10. <ethernet1 インタフェース設定>

```
NXR_C(config)#interface ethernet 1
NXR_C(config-if)#no ip address
NXR_C(config-if)#pppoe-client ppp 0
```

ethernet1 インタフェースで、ppp0 インタフェースを PPPoE クライアントとして使用できるよう設定します。

11. <DNS 設定>

```
NXR_C(config)#dns
NXR_C(config-dns)#service enable
```

DNS 設定で DNS サービスを有効にします。

12. <ファストフォワーディングの有効化>

```
NXR_C(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。

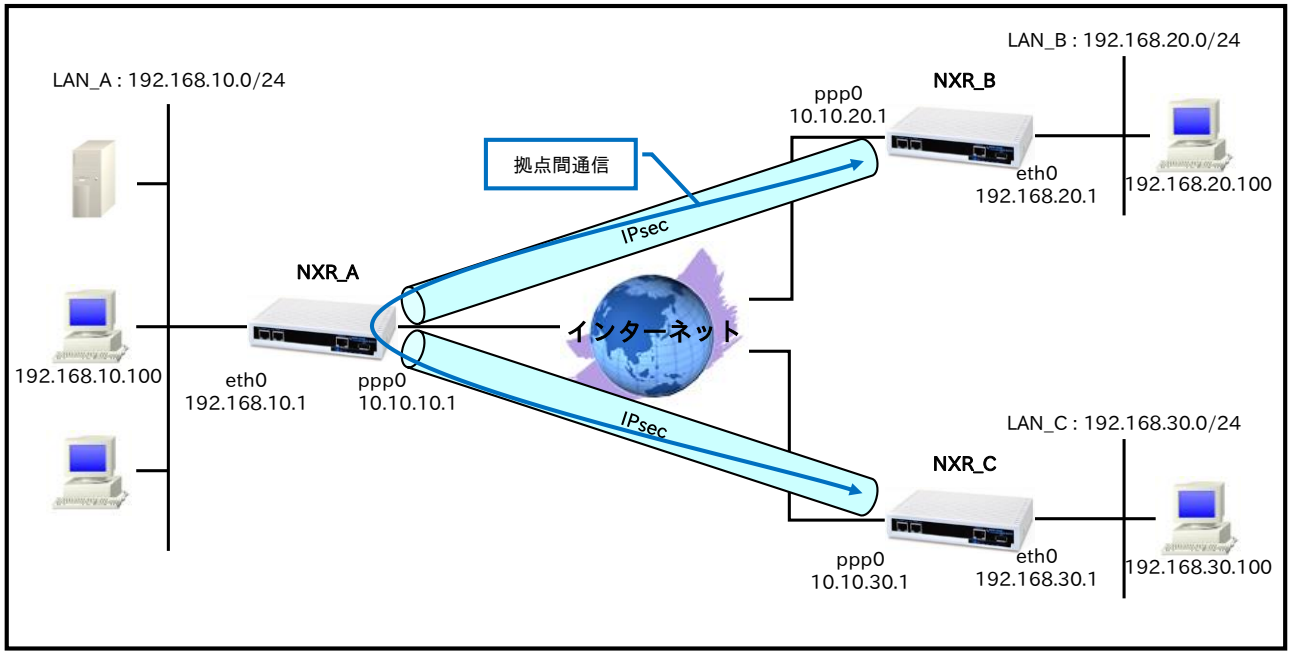
【 パソコンの設定例 】

	LAN A のパソコン	LAN B のパソコン	LAN C のパソコン
IP アドレス	192.168.10.100	192.168.20.100	192.168.30.100
サブネットマスク	255.255.255.0	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1	192.168.30.1
DNS サーバ	192.168.10.1	192.168.20.1	192.168.30.1

1-6. センタ経由拠点間通信設定例

1-5.PPPoE を利用した IPsec 接続設定例では拠点間の IPsec 経由での通信は行えませんでしたが、この設定例ではセンタ経由での拠点間通信を実現します。

【 構成図 】



- NXR_A⇔NXR_B 間はメインモード(事前共有鍵は ipseckey1),NXR_A⇔NXR_C 間はアグレッシブモード(事前共有鍵は ipseckey2)を利用します。
- 拠点間通信を実現するためセンタ,拠点で IPsec アクセスリストを以下のように設定します。

		送信元 IP アドレス	宛先 IP アドレス
NXR_A(センタ)	NXR_B 向け	192.168.0.0/16	192.168.20.0/24
	NXR_C 向け	192.168.0.0/16	192.168.30.0/24
NXR_B(拠点)	NXR_A 向け	192.168.20.0/24	192.168.0.0/16
NXR_C(拠点)	NXR_A 向け	192.168.30.0/24	192.168.0.0/16

- NXR_B,C の LAN 側ネットワークからルータの LAN 側インタフェースへのアクセスを可能にするために LAN 側インタフェースで IPsec ポリシーのチェックを無効にしています。
- 各拠点からのインターネットアクセスを可能にするため NAT 設定(IP マスカレード)やフィルタ設定(SPI)および DNS 設定を行います。

【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 0.0.0.0/0 ppp 0
NXR_A(config)#ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
NXR_A(config)#ip access-list ppp0_in permit any 10.10.10.1 50
NXR_A(config)#ipsec access-list LAN_B ip 192.168.0.0/16 192.168.20.0/24
NXR_A(config)#ipsec access-list LAN_C ip 192.168.0.0/16 192.168.30.0/24
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode main
NXR_A(config-ipsec-isakmp)#remote address ip 10.10.20.1
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address LAN_B
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#ipsec isakmp policy 2
NXR_A(config-ipsec-isakmp)#description NXR_C
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A(config-ipsec-isakmp)#remote address ip any
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrc
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 2
NXR_A(config-ipsec-tunnel)#description NXR_C
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 2
NXR_A(config-ipsec-tunnel)#match address LAN_C
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface ppp 0
NXR_A(config-ppp)#ip address 10.10.10.1/32
NXR_A(config-ppp)#ip masquerade
```

```
NXR_A(config-ppp)#ip access-group in ppp0_in
NXR_A(config-ppp)#ip spi-filter
NXR_A(config-ppp)#ip tcp adjust-mss auto
NXR_A(config-ppp)#no ip redirects
NXR_A(config-ppp)#ppp username test1@example.jp password test1pass
NXR_A(config-ppp)#ipsec policy 1
NXR_A(config-ppp)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#no ip address
NXR_A(config-if)#pppoe-client ppp 0
NXR_A(config-if)#exit
NXR_A(config)#dns
NXR_A(config-dns)#service enable
NXR_A(config-dns)#exit
NXR_A(config)#fast-forwarding enable
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#ipsec policy-ignore
NXR_B(config-if)#exit
NXR_B(config)#ip route 0.0.0.0/0 ppp 0
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 udp 500 500
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 50
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.0.0/16
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface ppp 0
NXR_B(config-ppp)#ip address 10.10.20.1/32
NXR_B(config-ppp)#ip masquerade
NXR_B(config-ppp)#ip access-group in ppp0_in
NXR_B(config-ppp)#ip spi-filter
NXR_B(config-ppp)#ip tcp adjust-mss auto
NXR_B(config-ppp)#no ip redirects
NXR_B(config-ppp)#ppp username test2@example.jp password test2pass
```

```
NXR_B(config-ppp)#ipsec policy 1
NXR_B(config-ppp)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#no ip address
NXR_B(config-if)#pppoe-client ppp 0
NXR_B(config-if)#exit
NXR_B(config)#dns
NXR_B(config-dns)#service enable
NXR_B(config-dns)#exit
NXR_B(config)#fast-forwarding enable
NXR_B(config)#exit
NXR_B#save config
```

〔NXR_C の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_C
NXR_C(config)#interface ethernet 0
NXR_C(config-if)#ip address 192.168.30.1/24
NXR_C(config-if)#ipsec policy-ignore
NXR_C(config-if)#exit
NXR_C(config)#ip route 0.0.0.0/0 ppp 0
NXR_C(config)#ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
NXR_C(config)#ip access-list ppp0_in permit 10.10.10.1 any 50
NXR_C(config)#ipsec access-list LAN_A ip 192.168.30.0/24 192.168.0.0/16
NXR_C(config)#ipsec local policy 1
NXR_C(config-ipsec-local)#address ip
NXR_C(config-ipsec-local)#self-identity fqdn nxrc
NXR_C(config-ipsec-local)#exit
NXR_C(config)#ipsec isakmp policy 1
NXR_C(config-ipsec-isakmp)#description NXR_A
NXR_C(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR_C(config-ipsec-isakmp)#hash sha1
NXR_C(config-ipsec-isakmp)#encryption aes128
NXR_C(config-ipsec-isakmp)#group 5
NXR_C(config-ipsec-isakmp)#lifetime 10800
NXR_C(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_C(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_C(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_C(config-ipsec-isakmp)#local policy 1
NXR_C(config-ipsec-isakmp)#exit
NXR_C(config)#ipsec tunnel policy 1
NXR_C(config-ipsec-tunnel)#description NXR_A
NXR_C(config-ipsec-tunnel)#negotiation-mode auto
NXR_C(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_C(config-ipsec-tunnel)#set pfs group5
NXR_C(config-ipsec-tunnel)#set sa lifetime 3600
NXR_C(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_C(config-ipsec-tunnel)#match address LAN_A
NXR_C(config-ipsec-tunnel)#exit
NXR_C(config)#interface ppp 0
NXR_C(config-ppp)#ip address negotiated
NXR_C(config-ppp)#ip masquerade
NXR_C(config-ppp)#ip access-group in ppp0_in
NXR_C(config-ppp)#ip spi-filter
NXR_C(config-ppp)#ip tcp adjust-mss auto
NXR_C(config-ppp)#no ip redirects
NXR_C(config-ppp)#ppp username test3@example.jp password test3pass
NXR_C(config-ppp)#ipsec policy 1
NXR_C(config-ppp)#exit
NXR_C(config)#interface ethernet 1
NXR_C(config-if)#no ip address
```

```
NXR_C(config-if)#pppoe-client ppp 0
NXR_C(config-if)#exit
NXR_C(config)#dns
NXR_C(config-dns)#service enable
NXR_C(config-dns)#exit
NXR_C(config)#fast-forwarding enable
NXR_C(config)#exit
NXR_C#save config
```

【 設定例解説 】

〔NXR_A の設定〕

(☞) ここに記載のない設定項目は 1-5. PPPoE を利用した IPsec 接続設定例の〔NXR_A の設定〕が参考になりますので、そちらをご参照下さい。

1. <IPsec アクセスリスト設定>

```
NXR_A(config)#ipsec access-list LAN_B ip 192.168.0.0/16 192.168.20.0/24
NXR_A(config)#ipsec access-list LAN_C ip 192.168.0.0/16 192.168.30.0/24
```

一行目は IPsec アクセスリスト名を LAN_B とし送信元 IP アドレス 192.168.0.0/16,宛先 IP アドレス 192.168.20.0/24 を設定します。

二行目は IPsec アクセスリスト名を LAN_C とし、送信元 IP アドレス 192.168.0.0/16,宛先 IP アドレス 192.168.30.0/24 を設定します。

Policy Based IPsec では IPsec アクセスリストで設定したルールに基づき IPsec で ESP 化するかどうかが決定されます。よってここで設定した送信元,宛先 IP アドレスにマッチしたパケットが IPsec のカプセル化対象となります。

(☞) 設定例内の各拠点のネットワークアドレスを包括する 192.168.0.0/16 を送信元 IP アドレスで指定することにより、LAN_A,LAN_B,LAN_C 内の IP アドレスを送信元とするパケットを各拠点に転送することができます。

〔NXR_B の設定〕

(☞) ここに記載のない設定項目は 1-5. PPPoE を利用した IPsec 接続設定例の〔NXR_B の設定〕が参考になりますので、そちらをご参照下さい。

1. <LAN 側(ethernet0)インタフェース設定>

```
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
```

LAN 側(ethernet0)インタフェースの IP アドレスに 192.168.20.1/24 を設定します。

```
NXR_B(config-if)#ipsec policy-ignore
```

IPsec ポリシーのチェックを行わないよう設定します。

LAN 側インタフェースへの通信が IPsec アクセスリストにマッチしている場合、この設定を行うことで LAN 側インタフェースの IP アドレスに対して通信が可能となります。

2. <IPsec アクセスリスト設定>

```
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.0.0/16
```

IPsec アクセスリスト名を LAN_A とし送信元 IP アドレス 192.168.20.0/24,宛先 IP アドレス 192.168.0.0/16 を設定します。

(☞) 設定例内の各拠点のネットワークアドレスを包括する 192.168.0.0/16 を宛先 IP アドレスで指定することにより、LAN_A,LAN_C 内の IP アドレスを宛先とするパケットを NXR_A に転送することができます。

〔NXR_C の設定〕

(☞) ここに記載のない設定項目は 1-5. PPPoE を利用した IPsec 接続設定例の〔NXR_C の設定〕が参考になりますので、そちらをご参照下さい。

1. <LAN 側(ethernet0)インタフェース設定>

```
NXR_C(config)#interface ethernet 0
NXR_C(config-if)#ip address 192.168.30.1/24
```

LAN 側(ethernet0)インタフェースの IP アドレスに 192.168.30.1/24 を設定します。

```
NXR_C(config-if)#ipsec policy-ignore
```

IPsec ポリシーのチェックを行わないよう設定します。

2. <IPsec アクセスリスト設定>

```
NXR_C(config)#ipsec access-list LAN_A ip 192.168.30.0/24 192.168.0.0/16
```

IPsec アクセスリスト名を LAN_A とし送信元 IP アドレス 192.168.30.0/24,宛先 IP アドレス 192.168.0.0/16 を設定します。

(☞) 設定例内の各拠点のネットワークアドレスを包括する 192.168.0.0/16 を宛先 IP アドレスで指定することにより、LAN_A,LAN_B 内の IP アドレスを宛先とするパケットを NXR_A に転送することができます。

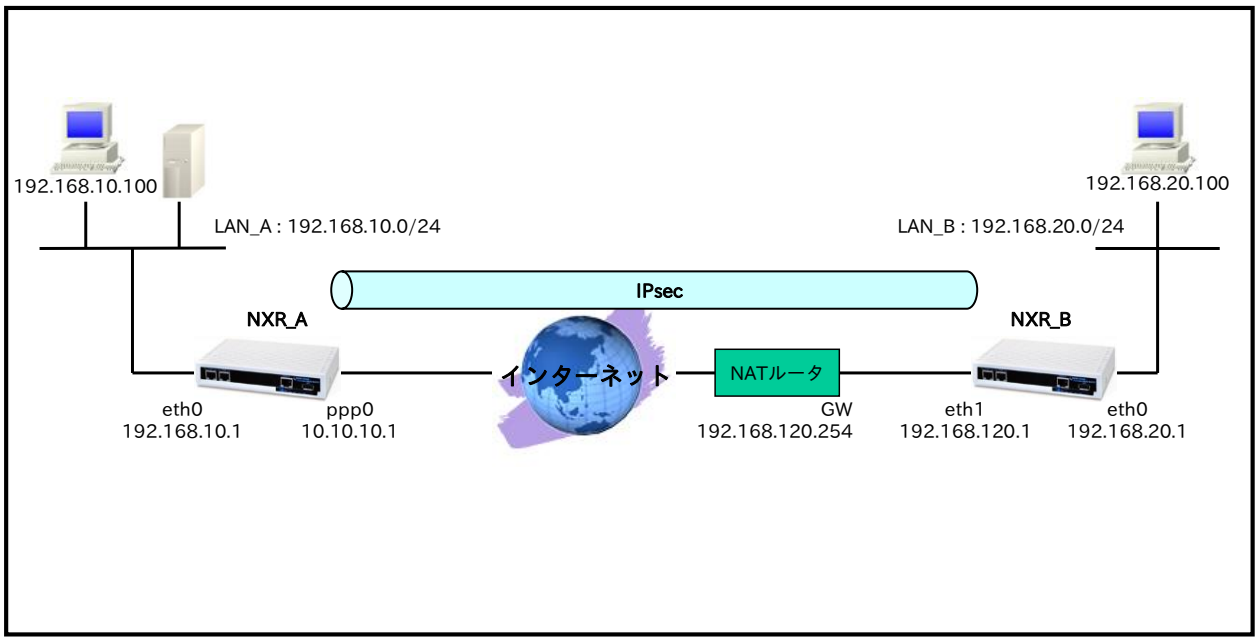
【 パソコンの設定例 】

	LAN A のパソコン	LAN B のパソコン	LAN C のパソコン
IP アドレス	192.168.10.100	192.168.20.100	192.168.30.100
サブネットマスク	255.255.255.0	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1	192.168.30.1
DNS サーバ	192.168.10.1	192.168.20.1	192.168.30.1

1-7. IPsec NAT トラバーサル接続設定例

NXR がプライベートネットワーク内にあるなどグローバル IP アドレスを保持できないような環境で同一拠点にグローバル IP アドレスを保持している NAPT ルータがある場合、このルータを経由して NXR では NAT トラバーサルという方法で IPsec を利用できます。

【 構成図 】



- NAPT ルータが存在する場合、NXR_B から送信された IKE のネゴシエーションパケット中の送信元ポートは変換されてしまうケースがあります。そのため NAT トラバーサルでは NXR_A と NXR_B の間で NAPT ルータの自動検出を行います。
- NAT トラバーサルでのネゴシエーションが完了した場合、実際の通信は ESP パケットではなく UDP パケットとなります(ESP パケットを UDP でカプセル化する形となります)。
- NAT トラバーサルの通信で利用しているセッション情報を NAPT ルータで維持させるために NXR では NAT トラバーサルキープアライブパケットを定期的に送信します。
- NAT トラバーサルを利用する場合は NAT トラバーサル機能を有効にする必要があります。
- この構成では NXR_B の WAN 側 IP アドレスがプライベート IP アドレスのため IP アドレスを ID として利用せずに、NXR_A では ISAKMP ポリシー設定で remote identity を NXR_B では IPsec ローカルポリシー設定で self-identity を設定します。

  (☞) identity は IKE のネゴシエーション時に NXR を識別するのに使用します。
  そのため self-identity は対向の NXR の remote identity と設定を合わせる必要があります。
- 各拠点からのインターネットアクセスを可能にするために NAT 設定(IP マスカレード)やフィルタ設定(SPI)および DNS 設定を行います。

  ※NAPT ルータはインターネットアクセスおよび NXR_B へのルート設定が完了済みとします。

【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 0.0.0.0/0 ppp 0
NXR_A(config)#ip access-list ppp0_in permit any 10.10.10.1 udp any 500
NXR_A(config)#ip access-list ppp0_in permit any 10.10.10.1 udp any 4500
NXR_A(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
NXR_A(config)#ipsec nat-traversal enable
% restart ipsec service to take affect.
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A(config-ipsec-isakmp)#remote address ip any
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrb
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address LAN_B
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface ppp 0
NXR_A(config-ppp)#ip address 10.10.10.1/32
NXR_A(config-ppp)#ip masquerade
NXR_A(config-ppp)#ip access-group in ppp0_in
NXR_A(config-ppp)#ip spi-filter
NXR_A(config-ppp)#ip tcp adjust-mss auto
NXR_A(config-ppp)#no ip redirects
NXR_A(config-ppp)#ppp username test1@example.jp password test1pass
NXR_A(config-ppp)#ipsec policy 1
NXR_A(config-ppp)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#no ip address
NXR_A(config-if)#pppoe-client ppp 0
NXR_A(config-if)#exit
NXR_A(config)#dns
NXR_A(config-dns)#service enable
NXR_A(config-dns)#exit
NXR_A(config)#fast-forwarding enable
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 0.0.0.0/0 192.168.120.254
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
NXR_B(config)#ipsec nat-traversal enable
% restart ipsec service to take affect.
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address 192.168.120.1/24
NXR_B(config-if)#ipsec policy 1
NXR_B(config-if)#exit
NXR_B(config)#dns
NXR_B(config-dns)#service enable
NXR_B(config-dns)#address 192.168.120.254
NXR_B(config-dns)#exit
NXR_B(config)#fast-forwarding enable
NXR_B(config)#exit
NXR_B#save config
```

【 設定例解説 】

〔NXR_A の設定〕

1. <ホスト名の設定>

```
nxr120(config)#hostname NXR_A
```

ホスト名を NXR_A と設定します。

2. <LAN 側(ethernet0)インタフェース設定>

```
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
```

LAN 側(ethernet0)インタフェースの IPv4 アドレスに 192.168.10.1/24 を設定します。

3. <スタティックルート設定>

```
NXR_A(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。なおゲートウェイとして ppp0 インタフェースを指定します。

4. <IP アクセスリスト設定>

```
NXR_A(config)#ip access-list ppp0_in permit any 10.10.10.1 udp any 500
NXR_A(config)#ip access-list ppp0_in permit any 10.10.10.1 udp any 4500
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を ppp0_in とします。

一行目は宛先 IP アドレス 10.10.10.1,宛先 UDP ポート番号 500 のパケットを許可する設定です。

二行目は宛先 IP アドレス 10.10.10.1,宛先 UDP ポート番号 4500 のパケットを許可する設定です。

この IP アクセスリスト設定は ppp0 インタフェース設定で登録します。

(☞) IP アクセスリストを設定しただけではフィルタとして有効にはなりません。フィルタリングしたいインタフェースでの登録が必要になります。

(☞) NAT トラバーサルでは、UDP ポート 500 番および UDP ポート番号 4500 は IPsec のネゴシエーションおよび通信で使用します。

5. <IPsec アクセスリスト設定>

```
NXR_A(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
```

IPsec アクセスリスト名を LAN_B とし送信元 IP アドレス 192.168.10.0/24,宛先 IP アドレス 192.168.20.0/24 を設定します。Policy Based IPsec では IPsec アクセスリストで設定したルールに基づき IPsec で ESP 化するかどうかが決定されます。よってここで設定した送信元,宛先 IP アドレスにマッチしたパケットが IPsec のカプセル化対象となります。

6. <IPsec NAT トラバーサル設定>

```
NXR_A(config)#ipsec nat-traversal enable
```

NAT トラバーサルを有効にします。

7. <IPsec ローカルポリシー設定>

```
NXR_A(config)#ipsec local policy 1
```

IPsec ローカルポリシー1 を設定します。

```
NXR_A(config-ipsec-local)#address ip
```

IPsec トンネルの送信元 IP アドレスを指定します。この IP アドレスはインタフェース設定で ipsec policy 1 と指定したインタフェースの IP アドレスが自動的に設定されます。

8. <IPsec ISAKMP ポリシー設定>

```
NXR_A(config)#ipsec isakmp policy 1
```

NXR_B との IPsec 接続で使用する ISAKMP ポリシー1 を設定します。

```
NXR_A(config-ipsec-isakmp)#description NXR_B
```

ISAKMP ポリシー1 の説明として NXR_B を設定します。

```
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey
```

認証方式として pre-share(事前共有鍵) を選択し事前共有鍵 ipseckey を設定します。なおこの設定は対向の NXR と同じ値を設定する必要があります。

```
NXR_A(config-ipsec-isakmp)#hash sha1
```

認証アルゴリズムとして sha1 を設定します。

```
NXR_A(config-ipsec-isakmp)#encryption aes128
```

暗号化アルゴリズムとして aes128 を設定します。

```
NXR_A(config-ipsec-isakmp)#group 5
```

Diffie-Hellman(DH)グループとして group 5 を設定します。

```
NXR_A(config-ipsec-isakmp)#lifetime 10800
```

ISAKMP SA のライフタイムとして 10800 秒を設定します。

```
NXR_A(config-ipsec-isakmp)#isakmp-mode aggressive
```

フェーズ 1 のネゴシエーションモードとして IPsec を使用するルータの WAN 側 IP アドレスがプライベート IP アドレスのためアグレッシブモードを設定します。

```
NXR_A(config-ipsec-isakmp)#remote address ip any
```

対向の NXR の WAN 側 IP アドレスを設定します。ここでは対向の NXR_B の WAN 側 IP アドレスがプライベート IP アドレスのため any を設定します。

```
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrb
```

対向の NXR の identity を設定します。ここでは ID として FQDN 方式で nxrb と設定します。
本設定が必要な理由は対向の NXR_B の WAN 側 IP アドレスがプライベート IP アドレスのためです。

```
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic clear
```

IKE KeepAlive(DPD)を設定します。ここでは監視を 30 秒間隔で 3 回リトライを行い keepalive 失敗時に

SA を削除するよう設定します。
DPD(Dead Peer Detection)は ISAKMP SA を監視する機能で対向 SG の WAN 側で障害が発生した場合などにそれを検知し、現在利用している SA を削除したり SA を削除して再ネゴシエーションを行ったりするなどの機能があります。なお DPD は常に定期的に送信されるわけではなく対向の NXR より IPsec パケットを受信している場合は DPD パケットの送信は行われません。

```
NXR_A(config-ipsec-isakmp)#local policy 1
```
関連づけを行う IPsec ローカルポリシーとして IPsec ローカルポリシー1 を設定します。

9. <IPsec トンネルポリシー設定>

```
NXR_A(config)#ipsec tunnel policy 1
```
NXR_B との IPsec 接続で使用するトンネルポリシー1 を設定します。

```
NXR_A(config-ipsec-tunnel)#description NXR_B
```
トンネルポリシー1 の説明として NXR_B を設定します。

```
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
```
IPsec ポリシーのネゴシエーションモードはネゴシエーションを自ら開始したり、逆にいかなる場合も自らネゴシエーションを開始しないという設定が可能です。
ここではネゴシエーションモードを responder に設定します。これによりこちらからいかなる場合(Rekey を含む)においてもネゴシエーションを開始することはありません。

```
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
```
IPsec トンネルポリシーで使用するトランスフォーム(プロポーザル)を設定します。
ここでは暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1 を設定します。

```
NXR_A(config-ipsec-tunnel)#set pfs group5
```
PFS(Perfect Forward Secrecy)の設定とそれに伴う DH グループを設定します。
ここでは PFS を有効とし、かつ DH グループとして group5 を設定します。

```
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
```
IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
```
関連づけを行う ISAKMP ポリシーとして ISAKMP ポリシー1 を設定します。

```
NXR_A(config-ipsec-tunnel)#match address LAN_B
```
IPsec アクセスリストとして LAN_B を設定します。

10. <WAN 側(ppp0)インタフェース設定>

```
NXR_A(config)#interface ppp 0
NXR_A(config-ppp)#ip address 10.10.10.1/32
```

WAN 側(ppp0)インタフェースを設定します。

IP アドレスとして固定 IP アドレス 10.10.10.1/32 を設定します。

```
NXR_A(config-ppp)#ip masquerade
NXR_A(config-ppp)#ip access-group in ppp0_in
NXR_A(config-ppp)#ip spi-filter
NXR_A(config-ppp)#ip tcp adjust-mss auto
NXR_A(config-ppp)#no ip redirects
```

IP マスカレードを有効、IP アクセスリスト ppp0_in を in フィルタに適用、ステートフルパケットインスペクションを有効に設定します。

また TCP MSS の調整機能をオート、ICMP リダイレクト機能を無効に設定します。

```
NXR_A(config-ppp)#ppp username test1@example.jp password test1pass
NXR_A(config-ppp)#ipsec policy 1
```

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

また IPsec トンネルのエンドポイントとなるため IPsec ローカルポリシー1 を設定します。

11. <ethernet1 インタフェース設定>

```
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#no ip address
NXR_A(config-if)#pppoe-client ppp 0
```

ethernet1 インタフェースで、ppp0 インタフェースを PPPoE クライアントとして使用できるよう設定します。

12. <DNS 設定>

```
NXR_A(config)#dns
NXR_A(dns-config)#service enable
```

DNS 設定で DNS サービスを有効にします。

13. <ファストフォワーディングの有効化>

```
NXR_A(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(☞) ファストフォワーディングの詳細および利用時の制約については、NXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

〔NXR_B の設定〕

1. <ホスト名の設定>

```
nxr120(config)#hostname NXR_B
```

ホスト名に NXR_B を設定します。

2. <LAN 側(ethernet0)インタフェース設定>

```
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
```

LAN 側(ethernet0)インタフェースの IP アドレスに 192.168.20.1/24 を設定します。

3. <スタティックルート設定>

```
NXR_B(config)#ip route 0.0.0.0/0 192.168.120.254
```

デフォルトルートを設定します。(ゲートウェイアドレスは上位の NAPT ルータの IP アドレス)

4. <IPsec アクセスリスト設定>

```
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
```

IPsec アクセスリスト名を LAN_A とし送信元 IP アドレス 192.168.20.0/24,宛先 IP アドレス 192.168.10.0/24 を設定します。

5. <IPsec NAT トラバーサルの有効化>

```
NXR_B(config)#ipsec nat-traversal enable
```

NAT トラバーサルを有効にします。

6. <IPsec ローカルポリシー設定>

```
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
```

IPsec ローカルポリシー1 で IPsec トンネルの送信元 IP アドレスを設定します。

```
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
```

本装置の identity を設定します。ここでは ID として FQDN 方式で nxrb と設定します。

7. <IPsec ISAKMP ポリシー設定>

```
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey
```

NXR_A との IPsec 接続で使用する ISAKMP ポリシー1 を設定します。
ISAKMP ポリシー1 の説明として NXR_A、認証方式として pre-share(事前共有鍵)を選択し事前共有鍵 ipseckey を設定します。

```
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
```

認証アルゴリズムとして sha1、暗号化アルゴリズムとして aes128、Diffie-Hellman(DH)グループとして group 5、ISAKMP SA のライフタイムとして 10800 秒、フェーズ 1 のネゴシエーションモードとしてアグレッシブモードを設定します。

```
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
```

NXR_A の WAN 側 IP アドレス 10.10.10.1、IKE KeepAlive(DPD)を監視間隔 30 秒,リトライ回数 3 回とし keepalive 失敗時に SA を削除し IKE のネゴシエーションを開始するよう設定します。

そして IPsec ローカルポリシー1 と関連づけを行います。

8. <IPsec トンネルポリシー設定>

```
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
```

NXR_A との IPsec 接続で使用するトンネルポリシー1 を設定します。

IPsec トンネルポリシー1 の説明として NXR_A、ネゴシエーションモードとして auto を設定します。

```
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして LAN_A を設定します。

9. <WAN 側(ethernet1)インタフェース設定>

```
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address 192.168.120.1/24
NXR_B(config-if)#ipsec policy 1
```

WAN 側(ethernet1)インタフェースの IPv4 アドレスとして 10.10.20.1/24 を設定します。

また IPsec トンネルのエンドポイントとなるため IPsec ローカルポリシー1 を設定します。

10. <DNS 設定>

```
NXR_B(config)#dns
NXR_B(config-dns)#service enable
```

DNS 設定で DNS サービスを有効にします。

```
NXR_B(config-dns)#address 192.168.120.254
```

DNS サーバアドレスとして上位の NAT ルータの 192.168.120.254 を設定します。

11. <ファストフォワーディングの有効化>

```
NXR_B(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。

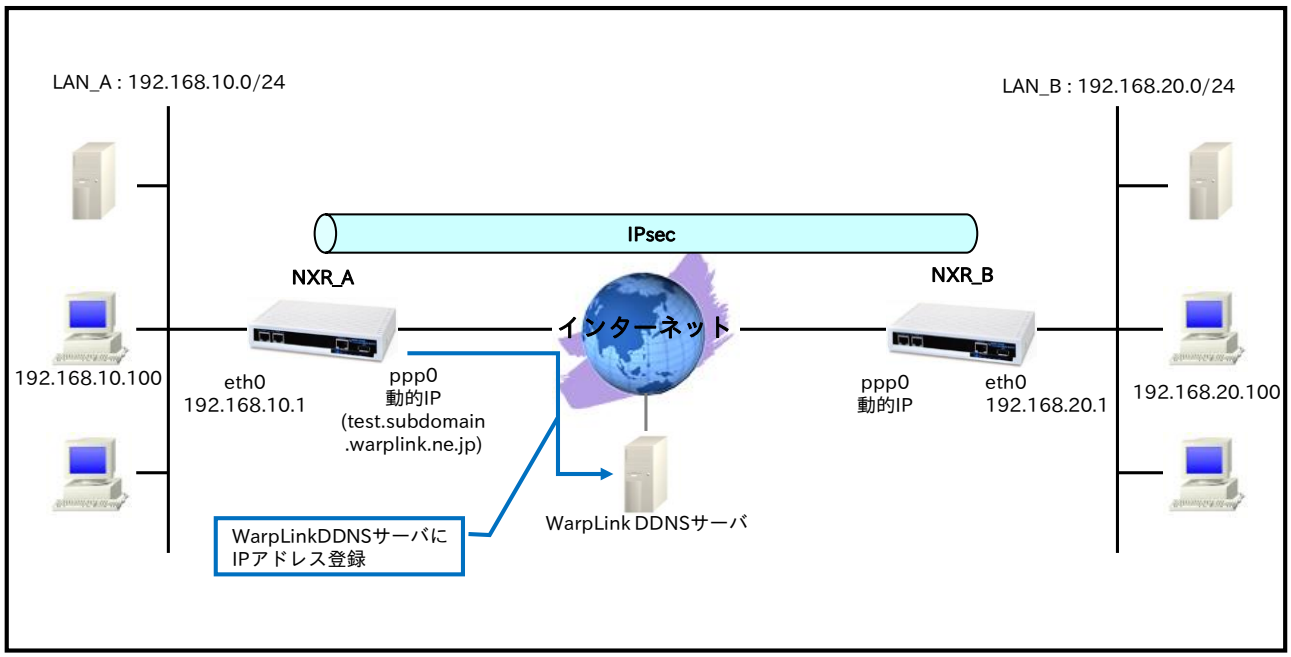
【 パソコンの設定例 】

	LAN A のパソコン	LAN B のパソコン
IP アドレス	192.168.10.100	192.168.20.100
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1
DNS サーバ	192.168.10.1	192.168.20.1

1-8. FQDN での IPsec 接続設定例

この設定例では、ダイナミック DNS を利用してアドレス不定の NXR 同士で IPsec 接続による通信を行います。ダイナミック DNS を利用することで、NXR の WAN 側 IP アドレスが不定のみの環境でも IPsec による VPN を利用できます。
ここではダイナミック DNS サービスに弊社が提供している WarpLinkDDNS サービスを使用します。

【 構成図 】



- NXR で WarpLink 機能を設定し WarpLinkDDNS サービスを動作させます。

  (☞) WarpLinkDDNS サービスは弊社が提供している有償の DDNS サービスとなります。
  詳細は下記 URL からご確認下さい。
  http://www.warplink.ne.jp/ddns/index.html

- NXR_A は自身の IP アドレスを WarpLinkDDNS サーバに登録します。NXR_B は WarpLinkDDNS サーバに登録されている NXR_A の FQDN を設定します。そして FQDN の名前解決後 IPsec 接続を開始します。

  (☞) 設定した FQDN の名前解決後に IPsec 接続を開始します。よって名前解決ができない場合、IPsec 接続を開始することができませんのでご注意ください。
  なお両拠点ルータで WarpLinkDDNS サービスを動作させることで両拠点ルータから IPsec 接続を開始することが可能になり、片側で WarpLinkDDNS サービスを動作させる場合に比べ再接続性の向上が期待できます。

【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 0.0.0.0/0 ppp 0
NXR_A(config)#ip access-list ppp0_in permit any any udp 500 500
NXR_A(config)#ip access-list ppp0_in permit any any 50
NXR_A(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A(config-ipsec-isakmp)#remote address ip any
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrb
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address LAN_B
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface ppp 0
NXR_A(config-ppp)#ip address negotiated
NXR_A(config-ppp)#ip masquerade
NXR_A(config-ppp)#ip access-group in ppp0_in
NXR_A(config-ppp)#ip spi-filter
NXR_A(config-ppp)#ip tcp adjust-mss auto
NXR_A(config-ppp)#no ip redirects
NXR_A(config-ppp)#ppp username test1@example.jp password test1pass
NXR_A(config-ppp)#ipsec policy 1
NXR_A(config-ppp)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#no ip address
NXR_A(config-if)#pppoe-client ppp 0
NXR_A(config-if)#exit
NXR_A(config)#warplink
NXR_A(config-warplink)#service enable
NXR_A(config-warplink)#account username warplinksample password warplinksamplepass
NXR_A(config-warplink)#exit
NXR_A(config)#dns
NXR_A(config-dns)#service enable
NXR_A(config-dns)#exit
NXR_A(config)#fast-forwarding enable
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 0.0.0.0/0 ppp 0
NXR_B(config)#ip access-list ppp0_in permit any any udp 500 500
NXR_B(config)#ip access-list ppp0_in permit any any 50
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_B(config-ipsec-isakmp)#remote address ip test.subdomain.warplink.ne.jp
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface ppp 0
NXR_B(config-ppp)#ip address negotiated
NXR_B(config-ppp)#ip masquerade
NXR_B(config-ppp)#ip access-group in ppp0_in
NXR_B(config-ppp)#ip spi-filter
NXR_B(config-ppp)#ip tcp adjust-mss auto
NXR_B(config-ppp)#no ip redirects
NXR_B(config-ppp)#ppp username test2@example.jp password test2pass
NXR_B(config-ppp)#ipsec policy 1
NXR_B(config-ppp)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#no ip address
NXR_B(config-if)#pppoe-client ppp 0
NXR_B(config-if)#exit
NXR_B(config)#dns
NXR_B(config-dns)#service enable
NXR_B(config-dns)#exit
NXR_B(config)#fast-forwarding enable
NXR_B(config)#exit
NXR_B#save config
```

【 設定例解説 】

〔NXR_A の設定〕

1. <ホスト名の設定>

```
nxr120(config)#hostname NXR_A
```

ホスト名に NXR_A を設定します。

2. <LAN 側(ethernet0)インタフェース設定>

```
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
```

LAN 側(ethernet0)インタフェースの IP アドレスとして 192.168.10.1/24 を設定します。

3. <スタティックルート設定>

```
NXR_A(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。なおゲートウェイとして ppp0 インタフェースを指定します。

4. <IP アクセスリスト設定>

```
NXR_A(config)#ip access-list ppp0_in permit any any udp 500 500
NXR_A(config)#ip access-list ppp0_in permit any any 50
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を ppp0_in とします。

一行目は送信元 UDP ポート番号 500,宛先 UDP ポート番号 500 のパケットを許可する設定です。

二行目はプロトコル番号 50(ESP)のパケットを許可する設定です。

なおこの IP アクセスリスト設定は ppp0 インタフェース設定で登録します。

(☞) IP アクセスリストを設定しただけではフィルタとして有効にはなりません。フィルタリングしたいインタフェースでの登録が必要になります。

(☞) UDP ポート 500 番およびプロトコル番号 50(ESP)は IPsec のネゴシエーションおよび通信で使用します。

5. <IPsec アクセスリスト設定>

```
NXR_A(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
```

IPsec アクセスリスト名を LAN_B とし送信元 IP アドレス 192.168.10.0/24,宛先 IP アドレス 192.168.20.0/24 を設定します。Policy Based IPsec では IPsec アクセスリストで設定したルールに基づき IPsec で ESP 化するかどうかが決定されます。よってここで設定した送信元,宛先 IP アドレスにマッチしたパケットが IPsec のカプセル化対象となります。

6. <IPsec ローカルポリシー設定>

```
NXR_A(config)#ipsec local policy 1
```

IPsec ローカルポリシー1 を設定します。

```
NXR_A(config-ipsec-local)#address ip
```

IPsec トンネルの送信元 IP アドレスを指定します。この IP アドレスはインタフェース設定で ipsec policy 1 と指定したインタフェースの IP アドレスが自動的に設定されます。

7. <IPsec ISAKMP ポリシー設定>

```
NXR_A(config)#ipsec isakmp policy 1
```

NXR_B との IPsec 接続で使用する ISAKMP ポリシー1 を設定します。

```
NXR_A(config-ipsec-isakmp)#description NXR_B
```

ISAKMP ポリシー1 の説明として NXR_B を設定します。

```
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey1
```

認証方式として pre-share(事前共有鍵)を選択し事前共有鍵 ipseckey1 を設定します。なおこの設定は対向の NXR_B と同じ値を設定する必要があります。

```
NXR_A(config-ipsec-isakmp)#hash sha1
```

認証アルゴリズムとして sha1 を設定します。

```
NXR_A(config-ipsec-isakmp)#encryption aes128
```

暗号化アルゴリズムとして aes128 を設定します。

```
NXR_A(config-ipsec-isakmp)#group 5
```

Diffie-Hellman(DH)グループとして group 5 を設定します。

```
NXR_A(config-ipsec-isakmp)#lifetime 10800
```

ISAKMP SA のライフタイムとして 10800 秒を設定します。

```
NXR_A(config-ipsec-isakmp)#isakmp-mode aggressive
```

フェーズ 1 のネゴシエーションモードとして IPsec を使用するルータの WAN 側 IP アドレスが動的 IP アドレスのためアグレッシブモードを設定します。

```
NXR_A(config-ipsec-isakmp)#remote address ip any
```

対向の NXR の WAN 側 IP アドレスを設定します。ここでは対向の NXR_B の WAN 側 IP アドレスが動的 IP アドレスのため any を設定します。

```
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrb
```

対向の NXR の identity を設定します。ここでは ID として FQDN 方式で nxrb と設定します。
本設定が必要な理由は対向の NXR_B の WAN 側 IP アドレスが動的 IP アドレスのため IP アドレスを ID として利用することができないためです。

```
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic clear
```

IKE KeepAlive(DPD)を設定します。ここでは監視を 30 秒間隔で 3 回リトライを行い keepalive 失敗時に SA を削除するよう設定します。
DPD(Dead Peer Detection)は ISAKMP SA を監視する機能で対向 SG の WAN 側で障害が発生した場合などにそれを検知し、現在利用している SA を削除したり SA を削除して再ネゴシエーションを行ったりする

などの機能があります。なお DPD は常に定期的に送信されるわけではなく対向の NXR より IPsec パケットを受信している場合は DPD パケットの送信は行われません。

```
NXR_A(config-ipsec-isakmp)#local policy 1
```

関連づけを行う IPsec ローカルポリシーとして IPsec ローカルポリシー1 を設定します。

8. <IPsec トンネルポリシー設定>

```
NXR_A(config)#ipsec tunnel policy 1
```

NXR_B との IPsec 接続で使用するトンネルポリシー1 を設定します。

```
NXR_A(config-ipsec-tunnel)#description NXR_B
```

トンネルポリシー1 の説明として NXR_B を設定します。

```
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
```

IPsec ポリシーのネゴシエーションモードはネゴシエーションを自ら開始したり、逆にいかなる場合も自らネゴシエーションを開始しないという設定が可能です。
ここではネゴシエーションモードを responder に設定します。これによりこちらからいかなる場合(Rekey を含む)においてもネゴシエーションを開始することはありません。

```
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
```

IPsec トンネルポリシーで使用するトランスフォーム(プロポーザル)を設定します。
ここでは暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1 を設定します。

```
NXR_A(config-ipsec-tunnel)#set pfs group5
```

PFS(Perfect Forward Secrecy)の設定とそれに伴う DH グループを設定します。
ここでは PFS を有効とし、かつ DH グループとして group5 を設定します。

```
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
```

IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
```

関連づけを行う ISAKMP ポリシーとして ISAKMP ポリシー1 を設定します。

```
NXR_A(config-ipsec-tunnel)#match address LAN_B
```

IPsec アクセスリストとして LAN_B を設定します。

9. <WAN 側(ppp0)インタフェース設定>

```
NXR_A(config)#interface ppp 0
NXR_A(config-ppp)#ip address negotiated
```

WAN 側(ppp0)インタフェースを設定します。
IP アドレスとして動的 IP アドレスの場合は negotiated を設定します。

```
NXR_A(config-ppp)#ip masquerade
NXR_A(config-ppp)#ip access-group in ppp0_in
NXR_A(config-ppp)#ip spi-filter
NXR_A(config-ppp)#ip tcp adjust-mss auto
NXR_A(config-ppp)#no ip redirects
```

IP マスカレードを有効、IP アクセスリスト ppp0_in を in フィルタに適用、ステートフルパケットインスペクションを有効に設定します。

また TCP MSS の調整機能をオート、ICMP リダイレクト機能を無効に設定します。

```
NXR_A(config-ppp)#ppp username test1@example.jp password test1pass
NXR_A(config-ppp)#ipsec policy 1
```

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

また IPsec トンネルのエンドポイントとなるため IPsec ローカルポリシー1 を設定します。

10. <ethernet1 インタフェース設定>

```
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#no ip address
NXR_A(config-if)#pppoe-client ppp 0
```

ethernet1 インタフェースで、ppp0 インタフェースを PPPoE クライアントとして使用できるよう設定します。

11. <WarpLink 設定>

```
NXR_A(config)#warplink
NXR_A(config-warplink)#service enable
```

WarpLink 設定で WarpLink サービスを有効にします。

```
NXR_A(config-warplink)#account username warplinksample password warplinksamplepass
```

WarpLink サービスで使用するユーザ ID,パスワードを設定します。ここでは WarpLink サービスのユーザ ID を warplinksample、パスワードを warplinksamplepass とします。

12. <DNS 設定>

```
NXR_A(config)#dns
NXR_A(config-dns)#service enable
```

DNS 設定で DNS サービスを有効にします。

13. <ファストフォワーディングの有効化>

```
NXR_A(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(☞) ファストフォワーディングの詳細および利用時の制約については、NXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

〔NXR_B の設定〕

1. <ホスト名の設定>

```
nxr120(config)#hostname NXR_B
```

ホスト名に NXR_B を設定します。

2. <LAN 側(ethernet0)インタフェース設定>

```
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
```

LAN 側(ethernet0)インタフェースの IP アドレスとして 192.168.20.1/24 を設定します。

3. <スタティックルート設定>

```
NXR_B(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。なおゲートウェイとして ppp0 インタフェースを指定します。

4. <IP アクセスリスト設定>

```
NXR_B(config)#ip access-list ppp0_in permit any any udp 500 500
NXR_B(config)#ip access-list ppp0_in permit any any 50
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を ppp0_in とします。

一行目は送信元 UDP ポート番号 500,宛先 UDP ポート番号 500 のパケットを許可する設定です。

二行目はプロトコル番号 50(ESP)のパケットを許可する設定です。

この IP アクセスリスト設定は ppp0 インタフェース設定で登録します。

(☞) UDP ポート 500 番およびプロトコル番号 50(ESP)は IPsec のネゴシエーションおよび通信で使用します。

5. <IPsec アクセスリスト設定>

```
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
```

IPsec アクセスリスト名を LAN_A とし送信元 IP アドレス 192.168.20.0/24,宛先 IP アドレス 192.168.10.0/24 を設定します。

6. <IPsec ローカルポリシー設定>

```
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
```

IPsec ローカルポリシー1 で IPsec トンネルの送信元 IP アドレスを設定します。

```
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
```

本装置の identity を設定します。ここでは ID として FQDN 方式で nxrb と設定します。

本設定が必要な理由は WAN 側 IP アドレスが動的 IP アドレスのため対向の NXR_A で本装置の IP アドレスを ID として設定しておくことができないためです。

7. <IPsec ISAKMP ポリシー設定>

```
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey1
```

ISAKMP ポリシー1 の説明として NXR_A、認証方式として pre-share(事前共有鍵)を選択し事前共有鍵 ipseckey1 を設定します。

```
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
```

認証アルゴリズムとして sha1、暗号化アルゴリズムとして aes128、Diffie-Hellman(DH)グループとして group 5、ISAKMP SA のライフタイムとして 10800 秒、フェーズ 1 のネゴシエーションモードとしてアグレッシブモードを設定します。

```
NXR_B(config-ipsec-isakmp)#remote address ip test.subdomain.warplink.ne.jp
```

対向ルータ NXR_A の FQDN を設定します。ここでは NXR_A の FQDN として test.subdomain.warplink.ne.jp を設定します。

```
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
```

IKE KeepAlive(DPD)を監視間隔 30 秒,リトライ回数 3 回とし keepalive 失敗時に SA を削除し IKE のネゴシエーションを開始するよう設定します。
そして IPsec ローカルポリシー1 と関連づけを行います。

8. <IPsec トンネルポリシー設定>

```
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
```

NXR_A との IPsec 接続で使用するトンネルポリシー1 を設定します。
IPsec トンネルポリシー1 の説明として NXR_A、ネゴシエーションモードとして auto を設定します。

```
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして LAN_A を設定します。

9. <WAN 側(ppp0)インタフェース設定>

```
NXR_B(config)#interface ppp 0
NXR_B(config-ppp)#ip address negotiated
```

WAN 側(ppp0)インタフェースを設定します。

IP アドレスとして動的 IP アドレスの場合は negotiated を設定します。

```
NXR_B(config-ppp)#ip masquerade
NXR_B(config-ppp)#ip access-group in ppp0_in
NXR_B(config-ppp)#ip spi-filter
NXR_B(config-ppp)#ip tcp adjust-mss auto
NXR_B(config-ppp)#no ip redirects
```

IP マスカレードを有効、IP アクセスリスト ppp0_in を in フィルタに適用、ステートフルパケットインスペクションを有効に設定します。

また TCP MSS の調整機能をオート、ICMP リダイレクト機能を無効に設定します。

```
NXR_B(config-ppp)#ppp username test2@example.jp password test2pass
NXR_B(config-ppp)#ipsec policy 1
```

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

また IPsec トンネルのエンドポイントとなるため IPsec ローカルポリシー1 を設定します。

10. <ethernet1 インタフェース設定>

```
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#no ip address
NXR_B(config-if)#pppoe-client ppp 0
```

ethernet1 インタフェースで、ppp0 インタフェースを PPPoE クライアントとして使用できるよう設定します。

11. <DNS 設定>

```
NXR_B(config)#dns
NXR_B(config-dns)#service enable
```

DNS 設定で DNS サービスを有効にします。

12. <ファストフォワーディングの有効化>

```
NXR_B(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。

【 パソコンの設定例 】

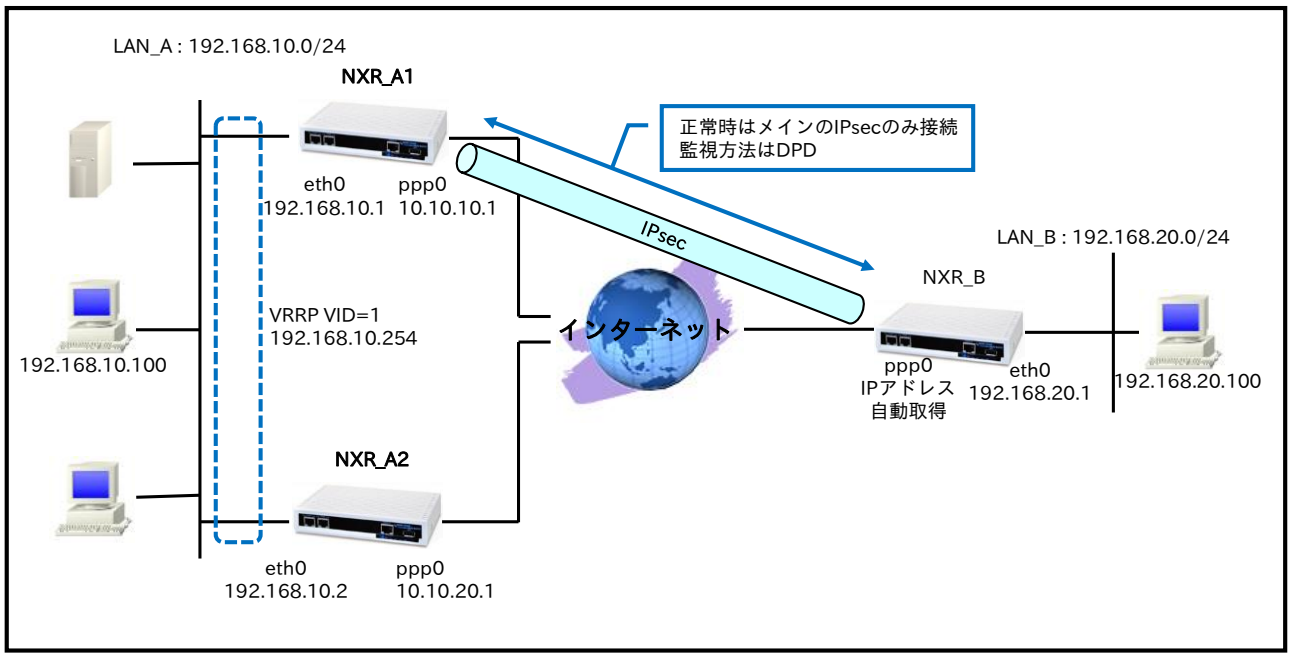
	LAN A のパソコン	LAN B のパソコン
IP アドレス	192.168.10.100	192.168.20.100
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1
DNS サーバ	192.168.10.1	192.168.20.1

1-9. 冗長化設定(backup policy の利用)

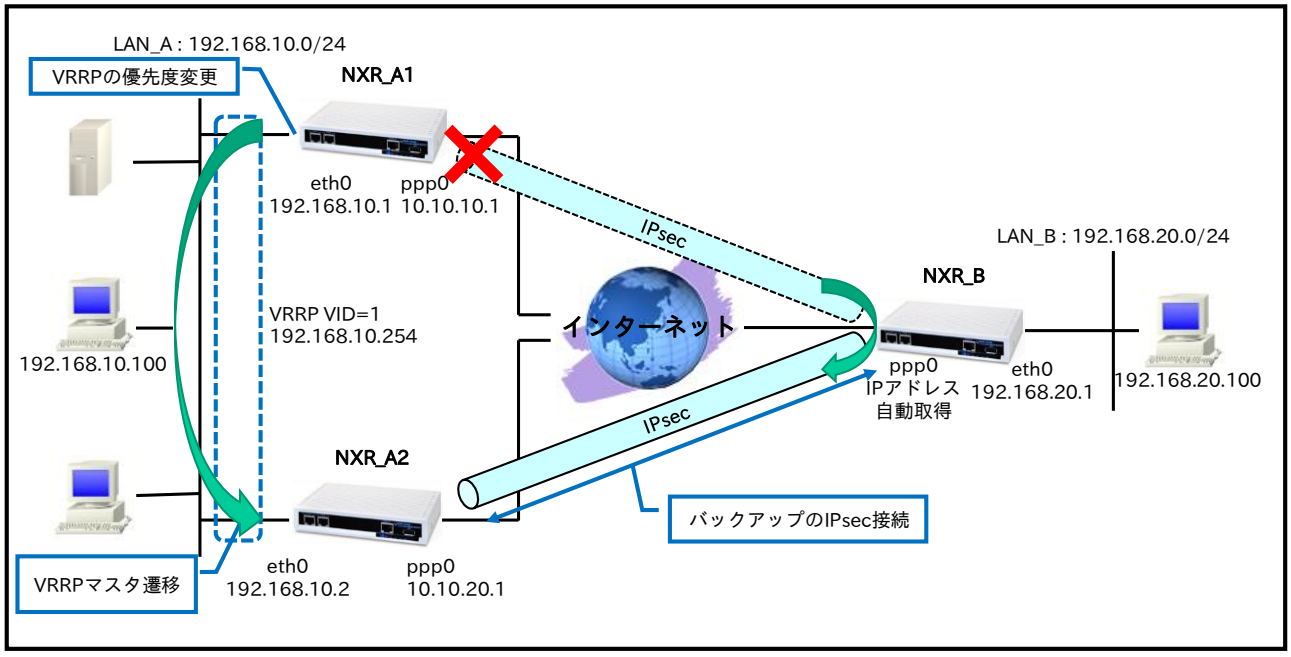
センタ側で回線と機器の冗長化を行う設定例です。
正常時 NXR_A1⇔NXR_B 間で IPsec トンネル経由で通信を行い、センタ側での障害検出時 NXR_A2⇔NXR_B 間の通信に切り替えます。

【 構成図 】

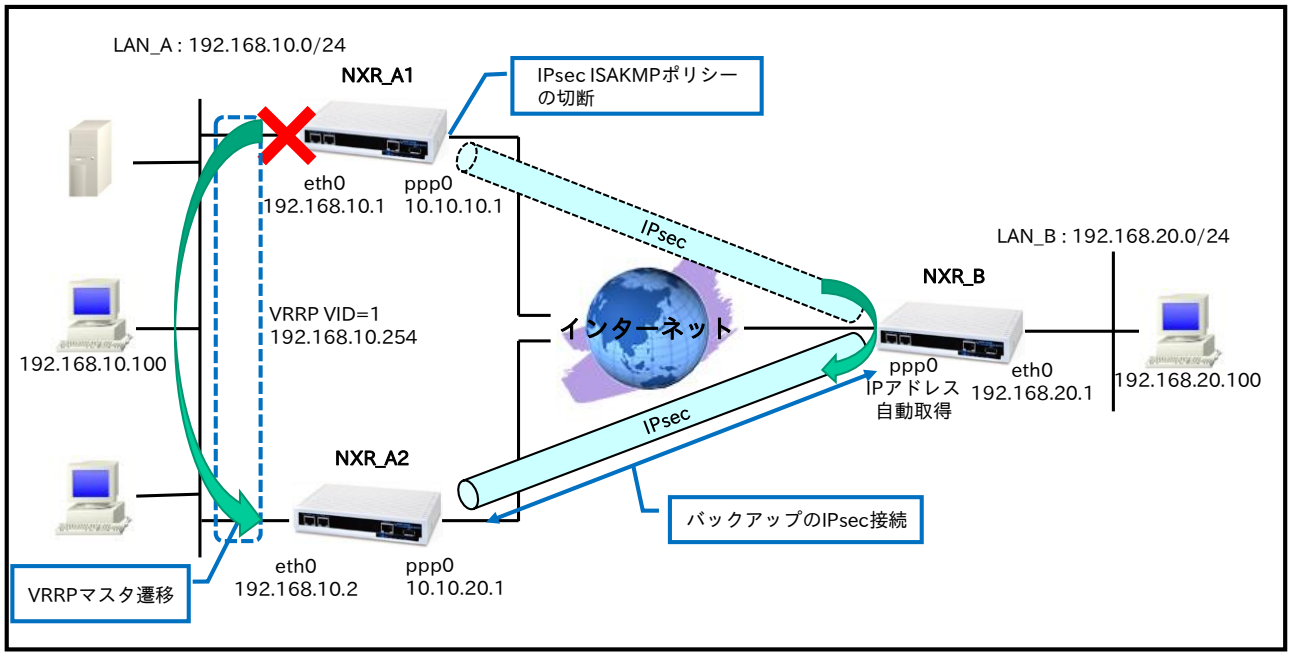
<正常時>



<NXR_A1 ppp0 インタフェースリンクダウン時>



<NXR_A1 ethernet0 インタフェースリンクダウン時>



- NXR_A1,A2 では以下の条件で VRRP を動作させます。

	NXR_A1	NXR_A2
グループ ID	1	
IP アドレス	192.168.10.254	
プライオリティ	254	100
プリエンプト	有効	
アドバタイズ間隔	5	
ネットワークイベントによる障害検知後のプライオリティ	50	−

- 本設定例では IPsecSA 確立時に IPsec ルートを有効化する設定を行います。
- NXR_A2,B では IPsec ルート無効時に、カプセル化対象のパケットをルータから出力しないようにするためゲートウェイを null インタフェースとしたルートを設定します。
- NXR_A1 では ppp0 インタフェースリンクダウンによる WAN 側障害検知時、ネットワークイベントにて VRRP の優先度を変更します。また ethernet0 インタフェースリンクダウンに LAN 側障害検知時、ネットワークイベントにて IPsecISAKMP ポリシーの切断を行います。そして WAN 側での経路障害など IPsec 未確立時に、LAN_B 宛のパケットを NXR_A2 に転送するためのルートを設定します。なお、その際ルートのディスタンス値は IPsec ルートよりも大きい値を設定します。
- NXR_B では DPD で監視を行い NXR_A1 との IPsec 未確立時に NXR_A2 に対して IPsec のネゴシエーションを行います。

(☞) 本設定例では backup policy 機能により冗長化を実現します。

【 設定例 】

〔NXR_A1 の設定〕

```
nxr125#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr125(config)#hostname NXR_A1
NXR_A1(config)#track 1 interface ppp 0 initial-timeout 30
NXR_A1(config)#track 2 interface ethernet 0
NXR_A1(config)#interface ethernet 0
NXR_A1(config-if)#ip address 192.168.10.1/24
NXR_A1(config-if)#no ip redirects
NXR_A1(config-if)#vrrp ip 1 address 192.168.10.254
NXR_A1(config-if)#vrrp ip 1 priority 254
NXR_A1(config-if)#vrrp ip 1 preempt
NXR_A1(config-if)#vrrp ip 1 timers advertise 5
NXR_A1(config-if)#vrrp ip 1 netevent 1 priority 50
NXR_A1(config-if)#exit
NXR_A1(config)#ip route 192.168.20.0/24 192.168.10.2 10
NXR_A1(config)#ip route 0.0.0.0/0 ppp 0
NXR_A1(config)#ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
NXR_A1(config)#ip access-list ppp0_in permit any 10.10.10.1 50
NXR_A1(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
NXR_A1(config)#ipsec local policy 1
NXR_A1(config-ipsec-local)#address ip
NXR_A1(config-ipsec-local)#exit
NXR_A1(config)#ipsec isakmp policy 1
NXR_A1(config-ipsec-isakmp)#description NXR_B
NXR_A1(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR_A1(config-ipsec-isakmp)#hash sha1
NXR_A1(config-ipsec-isakmp)#encryption aes128
NXR_A1(config-ipsec-isakmp)#group 5
NXR_A1(config-ipsec-isakmp)#lifetime 10800
NXR_A1(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A1(config-ipsec-isakmp)#remote address ip any
NXR_A1(config-ipsec-isakmp)#remote identity fqdn nxrb
NXR_A1(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A1(config-ipsec-isakmp)#local policy 1
NXR_A1(config-ipsec-isakmp)#netevent 2 disconnect
NXR_A1(config-ipsec-isakmp)#exit
NXR_A1(config)#ipsec tunnel policy 1
NXR_A1(config-ipsec-tunnel)#description NXR_B
NXR_A1(config-ipsec-tunnel)#negotiation-mode responder
NXR_A1(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A1(config-ipsec-tunnel)#set pfs group5
NXR_A1(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A1(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A1(config-ipsec-tunnel)#match address LAN_B
NXR_A1(config-ipsec-tunnel)#set route
NXR_A1(config-ipsec-tunnel)#set priority 1
NXR_A1(config-ipsec-tunnel)#exit
NXR_A1(config)#interface ppp 0
NXR_A1(config-ppp)#ip address 10.10.10.1/32
NXR_A1(config-ppp)#ip masquerade
NXR_A1(config-ppp)#ip access-group in ppp0_in
NXR_A1(config-ppp)#ip spi-filter
NXR_A1(config-ppp)#ip tcp adjust-mss auto
NXR_A1(config-ppp)#no ip redirects
NXR_A1(config-ppp)#ppp username test1@example.jp password test1pass
NXR_A1(config-ppp)#ipsec policy 1
NXR_A1(config-ppp)#exit
NXR_A1(config)#interface ethernet 1
NXR_A1(config-if)#no ip address
NXR_A1(config-if)#pppoe-client ppp 0
```

```
NXR_A1(config-if)#exit
NXR_A1(config)#dns
NXR_A1(config-dns)#service enable
NXR_A1(config-dns)#exit
NXR_A1(config)#fast-forwarding enable
NXR_A1(config)#exit
NXR_A1#save config
```

〔NXR_A2 の設定〕

```
nxr125#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr125(config)#hostname NXR_A2
NXR_A2(config)#interface ethernet 0
NXR_A2(config-if)#ip address 192.168.10.2/24
NXR_A2(config-if)#no ip redirects
NXR_A2(config-if)#vrrp ip 1 address 192.168.10.254
NXR_A2(config-if)#vrrp ip 1 priority 100
NXR_A2(config-if)#vrrp ip 1 preempt
NXR_A2(config-if)#vrrp ip 1 timers advertise 5
NXR_A2(config-if)#exit
NXR_A2(config)#ip route 192.168.20.0/24 null 254
NXR_A2(config)#ip route 0.0.0.0/0 ppp 0
NXR_A2(config)#ip access-list ppp0_in permit any 10.10.20.1 udp 500 500
NXR_A2(config)#ip access-list ppp0_in permit any 10.10.20.1 50
NXR_A2(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
NXR_A2(config)#ipsec local policy 1
NXR_A2(config-ipsec-local)#address ip
NXR_A2(config-ipsec-local)#exit
NXR_A2(config)#ipsec isakmp policy 1
NXR_A2(config-ipsec-isakmp)#description NXR_B
NXR_A2(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR_A2(config-ipsec-isakmp)#hash sha1
NXR_A2(config-ipsec-isakmp)#encryption aes128
NXR_A2(config-ipsec-isakmp)#group 5
NXR_A2(config-ipsec-isakmp)#lifetime 10800
NXR_A2(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A2(config-ipsec-isakmp)#remote address ip any
NXR_A2(config-ipsec-isakmp)#remote identity fqdn nxrb
NXR_A2(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A2(config-ipsec-isakmp)#local policy 1
NXR_A2(config-ipsec-isakmp)#exit
NXR_A2(config)#ipsec tunnel policy 1
NXR_A2(config-ipsec-tunnel)#description NXR_B
NXR_A2(config-ipsec-tunnel)#negotiation-mode responder
NXR_A2(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A2(config-ipsec-tunnel)#set pfs group5
NXR_A2(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A2(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A2(config-ipsec-tunnel)#match address LAN_B
NXR_A2(config-ipsec-tunnel)#set route
NXR_A2(config-ipsec-tunnel)#set priority 1
NXR_A2(config-ipsec-tunnel)#exit
NXR_A2(config)#interface ppp 0
NXR_A2(config-ppp)#ip address 10.10.20.1/32
NXR_A2(config-ppp)#ip masquerade
NXR_A2(config-ppp)#ip access-group in ppp0_in
NXR_A2(config-ppp)#ip spi-filter
NXR_A2(config-ppp)#ip tcp adjust-mss auto
NXR_A2(config-ppp)#no ip redirects
NXR_A2(config-ppp)#ppp username test2@example.jp password test2pass
NXR_A2(config-ppp)#ipsec policy 1
NXR_A2(config-ppp)#exit
```

```
NXR_A2(config)#interface ethernet 1
NXR_A2(config-if)#no ip address
NXR_A2(config-if)#pppoe-client ppp 0
NXR_A2(config-if)#exit
NXR_A2(config)#dns
NXR_A2(config-dns)#service enable
NXR_A2(config-dns)#exit
NXR_A2(config)#fast-forwarding enable
NXR_A2(config)#exit
NXR_A2#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 192.168.10.0/24 null 254
NXR_B(config)#ip route 0.0.0.0/0 ppp 0
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 any 50
NXR_B(config)#ip access-list ppp0_in permit 10.10.20.1 any udp 500 500
NXR_B(config)#ip access-list ppp0_in permit 10.10.20.1 any 50
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A1
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#backup policy 2
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A1
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
NXR_B(config-ipsec-tunnel)#set route
NXR_B(config-ipsec-tunnel)#set priority 1
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#ipsec isakmp policy 2
NXR_B(config-ipsec-isakmp)#description NXR_A2
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.20.1
```

```
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 2
NXR_B(config-ipsec-tunnel)#description NXR_A2
NXR_B(config-ipsec-tunnel)#negotiation-mode manual
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 2
NXR_B(config-ipsec-tunnel)#match address LAN_A
NXR_B(config-ipsec-tunnel)#set route
NXR_B(config-ipsec-tunnel)#set priority 10
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface ppp 0
NXR_B(config-ppp)#ip address negotiated
NXR_B(config-ppp)#ip masquerade
NXR_B(config-ppp)#ip access-group in ppp0_in
NXR_B(config-ppp)#ip spi-filter
NXR_B(config-ppp)#ip tcp adjust-mss auto
NXR_B(config-ppp)#no ip redirects
NXR_B(config-ppp)#ppp username test3@example.jp password test3pass
NXR_B(config-ppp)#ipsec policy 1
NXR_B(config-ppp)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#no ip address
NXR_B(config-if)#pppoe-client ppp 0
NXR_B(config-if)#exit
NXR_B(config)#dns
NXR_B(config-dns)#service enable
NXR_B(config-dns)#exit
NXR_B(config)#fast-forwarding enable
NXR_B(config)#exit
NXR_B#save config
```

【 設定例解説 】

〔NXR_A1 の設定〕

1. <ホスト名の設定>

```
nxr125(config)#hostname NXR_A1
```

ホスト名に NXR_A1 を設定します。

2. <トラック設定(リンク監視)>

```
NXR_A1(config)#track 1 interface ppp 0 initial-timeout 30
```

トラック No.1 に ppp0 インタフェースのリンク監視設定を登録します。

なおイニシャルタイムアウトを 30 秒に設定します。これはインタフェースのリンク監視設定時、初期のトラック状態はイニット(init)で ppp0 インタフェースがリンクアップ状態と判断するとトラックはアップ状態となりますが、ppp0 インタフェースがリンクダウン状態の場合トラックはダウン状態にはなりません。そのため設定したタイムアウト時間が経過した場合にトラックをダウン状態にするためイニシャルタイムアウトを設定します。

```
NXR_A1(config)#track 2 interface ethernet 0
```

トラック No.2 に ethernet0 インタフェースのリンク監視設定を登録します。

3. <LAN 側(ethernet0)インタフェース設定>

```
NXR_A1(config)#interface ethernet 0
NXR_A1(config-if)#ip address 192.168.10.1/24
```

LAN 側(ethernet0)インタフェースの IP アドレスとして 192.168.10.1/24 を設定します。

```
NXR_A1(config-if)#no ip redirects
```

ICMP リダイレクト機能を無効に設定します。

```
NXR_A1(config-if)#vrrp ip 1 address 192.168.10.254
```

VRRP の仮想 IP アドレスとして 192.168.10.254 を設定します。

```
NXR_A1(config-if)#vrrp ip 1 priority 254
```

VRRP のプライオリティとして 254 を設定します。

```
NXR_A1(config-if)#vrrp ip 1 preempt
```

VRRP のプリエンプトを有効にします。

プリエンプトが有効の場合プライオリティの最も高いルータが常にマスタールータとなります。

```
NXR_A1(config-if)#vrrp ip 1 timers advertise 5
```

VRRP アドバタイズの送信間隔を 5 秒に設定します。

```
NXR_A1(config-if)#vrrp ip 1 netevent 1 priority 50
```

ネットワークイベントを設定します。

この設定は track コマンドで指定した監視方法で障害を検知した場合、検知後 NXR で実行する動作を指定したものです。ここでは track 1 コマンドで指定した ppp0 インタフェースのリンク監視で障害(リンクダウン)を検知した場合、VRRP のプライオリティを 50 に変更します。

4. <スタティックルート設定>

```
NXR_A1(config)#ip route 192.168.20.0/24 192.168.10.2 10
```

LAN_B 向け 192.168.20.0/24 のルートを設定します。なおゲートウェイアドレスは 192.168.10.2 を設定します。またこのルートのディスタンス値として 10 を設定します。

(☞) IPsec SA 未確立時に NXR_A1 で受信した宛先 IP アドレス 192.168.20.0/24 のパケットをバックアップルータである NXR_A2 経由で拠点に転送するための設定です。

```
NXR_A1(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。なおゲートウェイとして ppp0 インタフェースを指定します。

5. <IP アクセスリスト設定>

```
NXR_A1(config)#ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
NXR_A1(config)#ip access-list ppp0_in permit any 10.10.10.1 50
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を ppp0_in とします。

一行目は宛先 IP アドレス 10.10.10.1,送信元 UDP ポート番号 500,宛先 UDP ポート番号 500 のパケットを許可する設定です。
二行目は宛先 IP アドレス 10.10.10.1,プロトコル番号 50(ESP)のパケットを許可する設定です。
なおこの IP アクセスリスト設定は ppp0 インタフェース設定で登録します。

(☞) IP アクセスリストを設定しただけではフィルタとして有効にはなりません。フィルタリングしたいインタフェースでの登録が必要になります。

(☞) UDP ポート 500 番およびプロトコル番号 50(ESP)は IPsec のネゴシエーションおよび通信で使用します。

6. <IPsec アクセスリスト設定>

```
NXR_A1(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
```

IPsec アクセスリスト名を LAN_B とし送信元 IP アドレス 192.168.10.0/24,宛先 IP アドレス 192.168.20.0/24 を設定します。Policy Based IPsec では IPsec アクセスリストで設定したルールに基づき IPsec で ESP 化するかどうかが決定されます。よってここで設定した送信元,宛先 IP アドレスにマッチしたパケットが IPsec のカプセル化対象となります。

7. <IPsec ローカルポリシー設定>

```
NXR_A1(config)#ipsec local policy 1
NXR_A1(config-ipsec-local)#address ip
```

IPsec ローカルポリシー1 で IPsec トンネルの送信元 IP アドレスを設定します。

8. <IPsec ISAKMP ポリシー設定>

```
NXR_A1(config)#ipsec isakmp policy 1
NXR_A1(config-ipsec-isakmp)#description NXR_B
NXR_A1(config-ipsec-isakmp)#authentication pre-share ipseckey1
```

NXR_B との IPsec 接続で使用する ISAKMP ポリシー1 を設定します。
ISAKMP ポリシー1 の説明として NXR_B、認証方式として pre-share(事前共有鍵)を選択し事前共有鍵 ipseckey1 を設定します。

```
NXR_A1(config-ipsec-isakmp)#hash sha1
NXR_A1(config-ipsec-isakmp)#encryption aes128
NXR_A1(config-ipsec-isakmp)#group 5
NXR_A1(config-ipsec-isakmp)#lifetime 10800
NXR_A1(config-ipsec-isakmp)#isakmp-mode aggressive
```

認証アルゴリズムとして sha1、暗号化アルゴリズムとして aes128，Diffie-Hellman(DH)グループとして group 5、ISAKMP SA のライフタイムとして 10800 秒、フェーズ 1 のネゴシエーションモードとしてアグレッシブモードを設定します。

```
NXR_A1(config-ipsec-isakmp)#remote address ip any
NXR_A1(config-ipsec-isakmp)#remote identity fqdn nxrb
NXR_A1(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A1(config-ipsec-isakmp)#local policy 1
```

NXR_B の WAN 側 IP アドレスが動的 IP アドレスのためリモートアドレスを any、identity として FQDN 方式で nxrb、IKE KeepAlive(DPD)を監視間隔 30 秒,リトライ回数 3 回とし keepalive 失敗時に SA を削

除するよう設定します。
そして IPsec ローカルポリシー1 と関連づけを行います。

```
NXR_A1(config-ipsec-isakmp)#netevent 2 disconnect
```

ネットワークイベントとして track 2 コマンドで指定した ethernet0 インタフェースのリンク監視で障害(リンクダウン)を検知した場合、IPsec トンネル 1 の削除を行います。

9. <IPsec トンネルポリシー設定>

```
NXR_A1(config)#ipsec tunnel policy 1
NXR_A1(config-ipsec-tunnel)#description NXR_B
NXR_A1(config-ipsec-tunnel)#negotiation-mode responder
```

NXR_B との IPsec 接続で使用するトンネルポリシー1 を設定します。IPsec トンネルポリシー1 の説明として NXR_B、ネゴシエーションモードとして responder を設定します。

```
NXR_A1(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A1(config-ipsec-tunnel)#set pfs group5
NXR_A1(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_A1(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A1(config-ipsec-tunnel)#match address LAN_B
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして LAN_B を設定します。

```
NXR_A1(config-ipsec-tunnel)#set route
NXR_A1(config-ipsec-tunnel)#set priority 1
```

IPsec アクセスリストで設定した宛先のプリフィックスをルーティングテーブルに追加します。
また IPsec トンネルポリシーのプライオリティを設定します。この IPsec トンネルポリシーはメインとなるためプライオリティを 1 に設定します。なおこのプライオリティはルーティングテーブルに追加時にディスタンス値としても利用されます。

10. <WAN 側(ppp0)インタフェース設定>

```
NXR_A1(config)#interface ppp 0
NXR_A1(config-ppp)#ip address 10.10.10.1/32
```

WAN 側(ppp0)インタフェースを設定します。
IP アドレスとして固定 IP アドレス 10.10.10.1/32 を設定します。

```
NXR_A1(config-ppp)#ip masquerade
NXR_A1(config-ppp)#ip access-group in ppp0_in
NXR_A1(config-ppp)#ip spi-filter
NXR_A1(config-ppp)#ip tcp adjust-mss auto
NXR_A1(config-ppp)#no ip redirects
```

IP マスカレードを有効、IP アクセスリスト ppp0_in を in フィルタに適用、ステートフルパケットインスペクションを有効に設定します。
また TCP MSS の調整機能をオート、ICMP リダイレクト機能を無効に設定します。

```
NXR_A1(config-ppp)#ppp username test1@example.jp password test1pass
NXR_A1(config-ppp)#ipsec policy 1
```

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

また IPsec トンネルのエンドポイントとなるため IPsec ローカルポリシー1 を設定します。

11. <ethernet1 インタフェース設定>

```
NXR_A1(config)#interface ethernet 1
NXR_A1(config-if)#no ip address
NXR_A1(config-if)#pppoe-client ppp 0
```

ethernet1 インタフェースで、ppp0 インタフェースを PPPoE クライアントとして使用できるよう設定します。

12. <DNS 設定>

```
NXR_A1(config)#dns
NXR_A1(config-dns)#service enable
```

DNS 設定で DNS サービスを有効にします。

13. <ファストフォワーディングの有効化>

```
NXR_A1(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(☞) ファストフォワーディングの詳細および利用時の制約については、NXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

〔NXR_A2 の設定〕

1. <ホスト名の設定>

```
nxr125(config)#hostname NXR_A2
```

ホスト名に NXR_A2 を設定します。

2. <LAN 側(ethernet0)インタフェース設定>

```
NXR_A2(config)#interface ethernet 0
NXR_A2(config-if)#ip address 192.168.10.2/24
```

LAN 側(ethernet0)インタフェースの IP アドレスとして 192.168.10.2/24 を設定します。

```
NXR_A2(config-if)#no ip redirects
```

ICMP リダイレクト機能を無効に設定します。

```
NXR_A2(config-if)#vrrp ip 1 address 192.168.10.254
```

VRRP の仮想 IP アドレスとして 192.168.10.254 を設定します。

```
NXR_A2(config-if)#vrrp ip 1 priority 100
```

VRRP のプライオリティとして 100 を設定します。

```
NXR_A2(config-if)#vrrp ip 1 preempt
```

VRRP のプリエンプトを有効にします。

```
NXR_A2(config-if)#vrrp ip 1 timers advertise 5
```

VRRP アドバタイズの送信間隔を 5 秒に設定します。

3. <スタティックルート設定>

```
NXR_A2(config)#ip route 192.168.20.0/24 null 254
```

LAN_B 向け 192.168.20.0/24 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

(☞) null インタフェースを出力インタフェースとして設定した場合、パケットが出力されることはありません(ドロップされます)。よってパケット出力を行う場合は null インタフェースよりもディスタンス値が小さいルートを設定する必要があります。

```
NXR_A2(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。なおゲートウェイとして ppp0 インタフェースを指定します。

4. <IP アクセスリスト設定>

```
NXR_A2(config)#ip access-list ppp0_in permit any 10.10.20.1 udp 500 500
NXR_A2(config)#ip access-list ppp0_in permit any 10.10.20.1 50
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を ppp0_in とします。

一行目は宛先 IP アドレス 10.10.20.1,送信元 UDP ポート番号 500,宛先 UDP ポート番号 500 のパケットを許可する設定です。

二行目は宛先 IP アドレス 10.10.20.1,プロトコル番号 50(ESP)のパケットを許可する設定です。

なおこの IP アクセスリスト設定は ppp0 インタフェース設定で登録します。

(☞) UDP ポート 500 番およびプロトコル番号 50(ESP)は IPsec のネゴシエーションおよび通信で使用します。

5. <IPsec アクセスリスト設定>

```
NXR_A2(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
```

IPsec アクセスリスト名を LAN_B とし送信元 IP アドレス 192.168.10.0/24,宛先 IP アドレス 192.168.20.0/24 を設定します。

6. <IPsec ローカルポリシー設定>

```
NXR_A2(config)#ipsec local policy 1
NXR_A2(config-ipsec-local)#address ip
```

IPsec ローカルポリシー1 で IPsec トンネルの送信元 IP アドレスを設定します。

7. <IPsec ISAKMP ポリシー設定>

```
NXR_A2(config)#ipsec isakmp policy 1
NXR_A2(config-ipsec-isakmp)#description NXR_B
NXR_A2(config-ipsec-isakmp)#authentication pre-share ipseckey2
```

NXR_B との IPsec 接続で使用する ISAKMP ポリシー1 を設定します。

ISAKMP ポリシー1 の説明として NXR_B、認証方式として pre-share(事前共有鍵)を選択し事前共有鍵 ipseckey2 を設定します。

```
NXR_A2(config-ipsec-isakmp)#hash sha1
NXR_A2(config-ipsec-isakmp)#encryption aes128
NXR_A2(config-ipsec-isakmp)#group 5
NXR_A2(config-ipsec-isakmp)#lifetime 10800
NXR_A2(config-ipsec-isakmp)#isakmp-mode aggressive
```

認証アルゴリズムとして sha1、暗号化アルゴリズムとして aes128，Diffie-Hellman(DH)グループとして group 5、ISAKMP SA のライフタイムとして 10800 秒、フェーズ 1 のネゴシエーションモードとしてアグレッシブモードを設定します。

```
NXR_A2(config-ipsec-isakmp)#remote address ip any
NXR_A2(config-ipsec-isakmp)#remote identity fqdn nxrb
NXR_A2(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A2(config-ipsec-isakmp)#local policy 1
```

NXR_B の WAN 側 IP アドレスが動的 IP アドレスのためリモートアドレスを any、identity として FQDN 方式で nxrb、IKE KeepAlive(DPD)を監視間隔 30 秒,リトライ回数 3 回とし keepalive 失敗時に SA を削除するよう設定します。

そして IPsec ローカルポリシー1 と関連づけを行います。

8. <IPsec トンネルポリシー設定>

```
NXR_A2(config)#ipsec tunnel policy 1
NXR_A2(config-ipsec-tunnel)#description NXR_B
NXR_A2(config-ipsec-tunnel)#negotiation-mode responder
```

NXR_B との IPsec 接続で使用するトンネルポリシー1 を設定します。IPsec トンネルポリシー1 の説明として NXR_B、ネゴシエーションモードとして responder を設定します。

```
NXR_A2(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A2(config-ipsec-tunnel)#set pfs group5
NXR_A2(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_A2(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A2(config-ipsec-tunnel)#match address LAN_B
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして LAN_B を設定します。

```
NXR_A2(config-ipsec-tunnel)#set route
NXR_A2(config-ipsec-tunnel)#set priority 1
```

IPsec アクセスリストで設定した宛先のプリフィックスをルーティングテーブルに追加します。

また IPsec トンネルポリシーのプライオリティを設定します。この IPsec トンネルポリシーはメインとなる

ためプライオリティを 1 に設定します。なおこのプライオリティはルーティングテーブルに追加時にディスタンス値としても利用されます。

9. <WAN 側(ppp0)インタフェース設定>

```
NXR_A2(config)#interface ppp 0
NXR_A2(config-ppp)#ip address 10.10.20.1/32
```

WAN 側(ppp0)インタフェースを設定します。

IP アドレスとして固定 IP アドレス 10.10.20.1/32 を設定します。

```
NXR_A2(config-ppp)#ip masquerade
NXR_A2(config-ppp)#ip access-group in ppp0_in
NXR_A2(config-ppp)#ip spi-filter
NXR_A2(config-ppp)#ip tcp adjust-mss auto
NXR_A2(config-ppp)#no ip redirects
```

IP マスカレードを有効、IP アクセスリスト ppp0_in を in フィルタに適用、ステートフルパケットインスペクションを有効に設定します。

また TCP MSS の調整機能をオート、ICMP リダイレクト機能を無効に設定します。

```
NXR_A2(config-ppp)#ppp username test2@example.jp password test2pass
NXR_A2(config-ppp)#ipsec policy 1
```

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

また IPsec トンネルのエンドポイントとなるため IPsec ローカルポリシー1 を設定します。

10. <ethernet1 インタフェース設定>

```
NXR_A2(config)#interface ethernet 1
NXR_A2(config-if)#no ip address
NXR_A2(config-if)#pppoe-client ppp 0
```

ethernet1 インタフェースで、ppp0 インタフェースを PPPoE クライアントとして使用できるよう設定します。

11. <DNS 設定>

```
NXR_A2(config)#dns
NXR_A2(config-dns)#service enable
```

DNS 設定で DNS サービスを有効にします。

12. <ファストフォワーディングの有効化>

```
NXR_A2(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。

〔NXR_B の設定〕

1. <ホスト名の設定>

```
nxr120(config)#hostname NXR_B
```

ホスト名に NXR_B を設定します。

2. <LAN 側(ethernet0)インタフェース設定>

```
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
```

LAN 側(ethernet0)インタフェースの IP アドレスとして 192.168.20.1/24 を設定します。

3. <スタティックルート設定>

```
NXR_B(config)#ip route 192.168.10.0/24 null 254
```

LAN_A 向け 192.168.10.0/24 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

```
NXR_B(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。なおゲートウェイとして ppp0 インタフェースを指定します。

4. <IP アクセスリスト設定>

```
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 any 50
NXR_B(config)#ip access-list ppp0_in permit 10.10.20.1 any udp 500 500
NXR_B(config)#ip access-list ppp0_in permit 10.10.20.1 any 50
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を ppp0_in とします。

一行目は宛先 IP アドレス 10.10.10.1,送信元 UDP ポート番号 500,宛先 UDP ポート番号 500 のパケットを許可する設定です。

二行目は宛先 IP アドレス 10.10.10.1,プロトコル番号 50(ESP)のパケットを許可する設定です。

三行目は宛先 IP アドレス 10.10.20.1,送信元 UDP ポート番号 500,宛先 UDP ポート番号 500 のパケットを許可する設定です。

四行目は宛先 IP アドレス 10.10.20.1,プロトコル番号 50(ESP)のパケットを許可する設定です。

なおこの IP アクセスリスト設定は ppp0 インタフェース設定で登録します。

(☞) UDP ポート 500 番およびプロトコル番号 50(ESP)は IPsec のネゴシエーションおよび通信で使用します。

5. <IPsec アクセスリスト設定>

```
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
```

IPsec アクセスリスト名を LAN_A とし送信元 IP アドレス 192.168.20.0/24,宛先 IP アドレス 192.168.10.0/24 を設定します。

6. <IPsec ローカルポリシー設定>

```
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
```

IPsec ローカルポリシー1 で IPsec トンネルの送信元 IP アドレスを設定します。

また本装置の identity として FQDN 方式で nxrb と設定します。

7. <IPsec ISAKMP ポリシー1 設定>

```
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A1
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey1
```

NXR_A1 との IPsec 接続で使用する ISAKMP ポリシー1 を設定します。

ISAKMP ポリシー1 の説明として NXR_A1、認証方式として pre-share(事前共有鍵)を選択し事前共有鍵 ipseckey1 を設定します。

```
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
```

認証アルゴリズムとして sha1、暗号化アルゴリズムとして aes128，Diffie-Hellman(DH)グループとして group 5、ISAKMP SA のライフタイムとして 10800 秒、フェーズ 1 のネゴシエーションモードとしてアグレッシブモードを設定します。

```
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
```

NXR_A1 の WAN 側 IP アドレス 10.10.10.1、IKE KeepAlive(DPD)を監視間隔 30 秒,リトライ回数 3 回とし keepalive 失敗時に SA を削除し IKE のネゴシエーションを開始するよう設定します。

そして IPsec ローカルポリシー1 と関連づけを行います。

```
NXR_B(config-ipsec-isakmp)#backup policy 2
```

バックアップポリシーを設定します。この設定は DPD で障害を検出した場合に指定した ISAKMP ポリシのネゴシエーションを開始します。ここではバックアップポリシーとして 2 を設定します。

8. <IPsec トンネルポリシー1 設定>

```
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A1
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
```

NXR_A1 との IPsec 接続で使用するトンネルポリシー11 を設定します。

IPsec トンネルポリシー1 の説明として NXR_A1、ネゴシエーションモードとして auto を設定します。

```
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして LAN_A を設定します。

```
NXR_B(config-ipsec-tunnel)#set route
NXR_B(config-ipsec-tunnel)#set priority 1
```

IPsec アクセスリストで設定した宛先のプリフィックスをルーティングテーブルに追加します。
また IPsec トンネルポリシーのプライオリティを設定します。この IPsec トンネルポリシーはメインとなるためプライオリティを 1 に設定します。なおこのプライオリティはルーティングテーブルに追加時にディスタンス値としても利用されます。

9. <IPsec ISAKMP ポリシー2 設定>

```
NXR_B(config)#ipsec isakmp policy 2
NXR_B(config-ipsec-isakmp)#description NXR_A2
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey2
```

NXR_A2 との IPsec 接続で使用する ISAKMP ポリシー2 を設定します。
ISAKMP ポリシー2 の説明として NXR_A2、認証方式として pre-share(事前共有鍵)を選択し事前共有鍵 ipseckey2 を設定します。

```
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
```

認証アルゴリズムとして sha1、暗号化アルゴリズムとして aes128，Diffie-Hellman(DH)グループとして group 5、ISAKMP SA のライフタイムとして 10800 秒、フェーズ 1 のネゴシエーションモードとしてアグレッシブモードを設定します。

```
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.20.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
```

NXR_A2 の WAN 側 IP アドレス 10.10.20.1、IKE KeepAlive(DPD)を監視間隔 30 秒,リトライ回数 3 回とし keepalive 失敗時に SA を削除し IKE のネゴシエーションを開始するよう設定します。
そして IPsec ローカルポリシー1 と関連づけを行います。

10. <IPsec トンネルポリシー2 設定>

```
NXR_B(config)#ipsec tunnel policy 2
NXR_B(config-ipsec-tunnel)#description NXR_A2
NXR_B(config-ipsec-tunnel)#negotiation-mode manual
```

NXR_A2 との IPsec 接続で使用するトンネルポリシー2 を設定します。
IPsec トンネルポリシー2 の説明として NXR_A2、ネゴシエーションモードとして manual を設定します。
なおバックアップポリシー利用時、バックアップとなる IPsec トンネルポリシーではネゴシエーションモードを manual に設定する必要があります。

```
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 2
NXR_B(config-ipsec-tunnel)#match address LAN_A
```

ISAKMP ポリシー2 と関連づけを行い、IPsec アクセスリストとして LAN_A を設定します。

```
NXR_B(config-ipsec-tunnel)#set route
NXR_B(config-ipsec-tunnel)#set priority 10
```

IPsec アクセスリストで設定した宛先のプリフィックスをルーティングテーブルに追加します。

また IPsec トンネルポリシーのプライオリティを設定します。この IPsec トンネルポリシーはバックアップとなるためプライオリティを 10 に設定します。

11. <WAN 側(ppp0)インタフェース設定>

```
NXR_B(config)#interface ppp 0
NXR_B(config-ppp)#ip address negotiated
```

WAN 側(ppp0)インタフェースを設定します。

IP アドレスとして動的 IP アドレスの場合は negotiated を設定します。

```
NXR_B(config-ppp)#ip masquerade
NXR_B(config-ppp)#ip access-group in ppp0_in
NXR_B(config-ppp)#ip spi-filter
NXR_B(config-ppp)#ip tcp adjust-mss auto
NXR_B(config-ppp)#no ip redirects
```

IP マスカレードを有効、IP アクセスリスト ppp0_in を in フィルタに適用、ステートフルパケットインスペクションを有効に設定します。

また TCP MSS の調整機能をオート、ICMP リダイレクト機能を無効に設定します。

```
NXR_B(config-ppp)#ppp username test3@example.jp password test3pass
NXR_B(config-ppp)#ipsec policy 1
```

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

また IPsec トンネルのエンドポイントとなるため IPsec ローカルポリシー1 を設定します。

12. <ethernet1 インタフェース設定>

```
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#no ip address
NXR_B(config-if)#pppoe-client ppp 0
```

ethernet1 インタフェースで、ppp0 インタフェースを PPPoE クライアントとして使用できるよう設定します。

13. <DNS 設定>

```
NXR_B(config)#dns
NXR_B(config-dns)#service enable
```

DNS 設定で DNS サービスを有効にします。

14. <ファストフォワーディングの有効化>

```
NXR_B(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。

【 パソコンの設定例 】

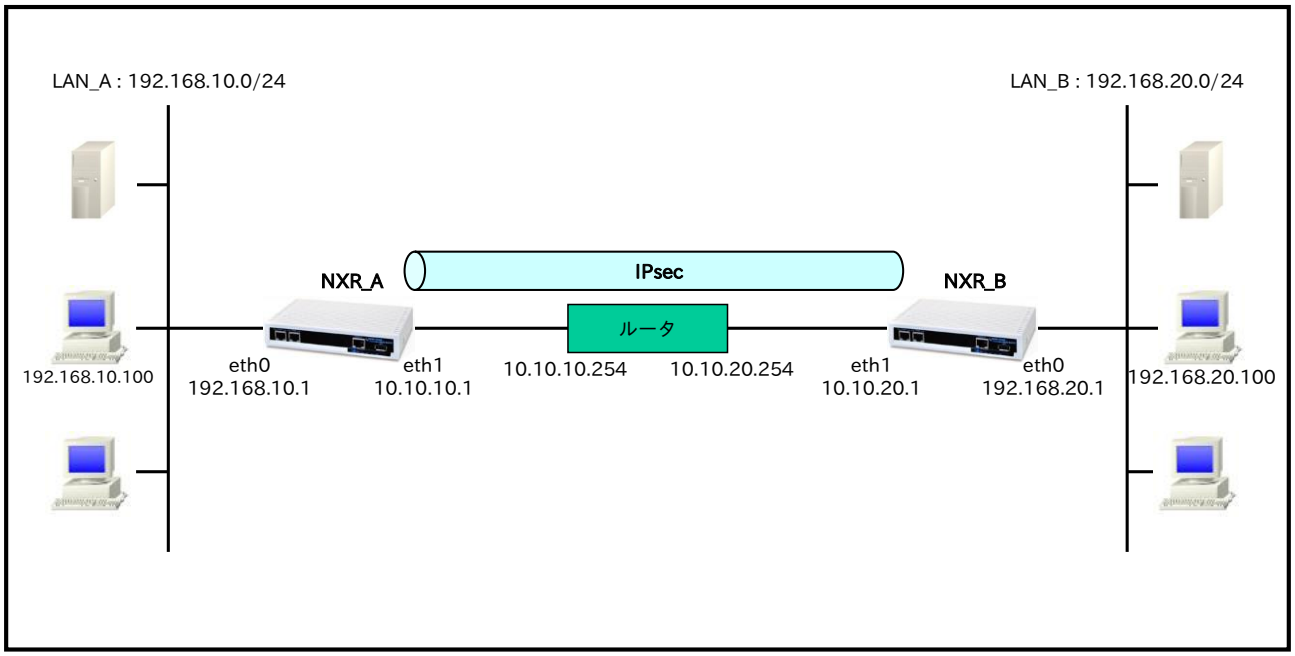
	LAN A のパソコン	LAN B のパソコン
IP アドレス	192.168.10.100	192.168.20.100
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.254	192.168.20.1
DNS サーバ	192.168.10.1	192.168.20.1
	192.168.10.2	

2. Route Based IPsec 設定

2-1. 固定 IP アドレスでの接続設定例(MainMode の利用)

LAN_A 192.168.10.0/24 と LAN_B 192.168.20.0/24 のネットワークにある NXR_A,NXR_B 間で IPsec トンネルを構築し、LAN 間通信を可能にします。IPsec を使用するルータの WAN 側 IP アドレスはともに固定 IP アドレスになります。

【 構成図 】



- Route Based IPsec は Policy Based IPsec での設定に対し以下の設定を追加する必要があります。
  - ・トンネルインタフェース設定
  - ・ルート設定(スタティックルート設定,RIPv1/v2,OSPF,BGP)
- 1-1. 固定 IP アドレスでの接続設定例(MainMode の利用)の内容も一部参考になりますのでご参照下さい。

【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1 1
NXR_A(config)#ip route 192.168.20.0/24 null 254
NXR_A(config)#ip route 0.0.0.0/0 10.10.10.254
NXR_A(config)#ipsec access-list ipsec_acl ip any any
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode main
NXR_A(config-ipsec-isakmp)#remote address ip 10.10.20.1
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address ipsec_acl
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
NXR_A(config-tunnel)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#ip address 10.10.10.1/24
NXR_A(config-if)#ipsec policy 1
NXR_A(config-if)#exit
NXR_A(config)#fast-forwarding enable
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1 1
NXR_B(config)#ip route 192.168.10.0/24 null 254
NXR_B(config)#ip route 0.0.0.0/0 10.10.20.254
NXR_B(config)#ipsec access-list ipsec_acl ip any any
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
NXR_B(config-tunnel)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address 10.10.20.1/24
NXR_B(config-if)#ipsec policy 1
NXR_B(config-if)#exit
NXR_B(config)#fast-forwarding enable
NXR_B(config)#exit
NXR_B#save config
```

【 設定例解説 】

〔NXR_A の設定〕

(☞) ここに記載のない設定項目は 1-1. 固定 IP アドレスでの接続設定例(MainMode の利用)の〔NXR_A の設定〕が参考になりますので、そちらをご参照下さい。

1. <スタティックルート設定>

```
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1 1
```

LAN_B 向け 192.168.20.0/24 のルートを設定します。なおゲートウェイインタフェースは tunnel 1 を設定します。またこのルートのディスタンス値として 1 を設定します。

(☞) これは IPsec で使用するスタティックルートであり、ここで設定した宛先 IP アドレスにマッチしたパケットが IPsec のカプセル化対象となります。なおゲートウェイアドレスは IPsec で使用するトンネルインタフェースを設定します。

```
NXR_A(config)#ip route 192.168.20.0/24 null 254
```

LAN_B 向け 192.168.20.0/24 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

(☞) null インタフェースを出力インタフェースとして設定した場合、パケットが出力されることはありません(ドロップされます)。よってパケット出力を行う場合は null インタフェースよりもディスタンス値が小さいルートを設定する必要があります。

2. <IPsec アクセスリスト設定>

```
NXR_A(config)#ipsec access-list ipsec_acl ip any any
```

IPsec アクセスリスト名を ipsec_acl とし、送信元 IP アドレス,宛先 IP アドレスに any を設定します。
Policy Based IPsec では IPsec アクセスリストで設定したルールに基づき IPsec で ESP 化するかどうかが決定されましたが、Route Based IPsec では IPsec アクセスリストは IKE フェーズ 2 の ID としてのみ使用します。

(☞) Route Based IPsec で ESP 化するか否かは IPsec アクセスリストではなくトンネルインタフェースをゲートウェイとするルート設定の有無で決まります。

3. <IPsec トンネルポリシー設定>

```
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
```

NXR_B との IPsec 接続で使用するトンネルポリシー1 を設定します。
IPsec トンネルポリシー1 の説明として NXR_B、ネゴシエーションモードとして auto を設定します。

```
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address ipsec_acl
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

4. <トンネルインタフェース設定>

```
NXR_A(config)#interface tunnel 1
```

トンネル 1 インタフェースを設定します。

```
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
```

トンネルインタフェースで使用するトンネルモードを設定します。

トンネルインタフェースを Route Based IPsec で使用する場合は ipsec ipv4 と設定します。

```
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
```

使用する IPsec トンネルポリシーを設定します。

ここでは IPsec トンネルポリシー1 と関連づけを行います。

(☞) IPsec ローカルポリシーではありませんのでご注意下さい。

```
NXR_A(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

〔NXR_B の設定〕

(☞) ここに記載のない設定項目は 1-1. 固定 IP アドレスでの接続設定例(MainMode の利用)の〔NXR_B の設定〕が参考になりますので、そちらをご参照下さい。

1.<スタティックルート設定>

```
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1 1
```

LAN_A 向け 192.168.10.0/24 のルートを設定します。なおゲートウェイインタフェースは tunnel 1 を設定します。またこのルートのディスタンス値として 1 を設定します。

```
NXR_B(config)#ip route 192.168.10.0/24 null 254
```

LAN_A 向け 192.168.10.0/24 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

2. <IPsec アクセスリスト設定>

```
NXR_B(config)#ipsec access-list ipsec_acl ip any any
```

IPsec アクセスリスト名を ipsec_acl とし、送信元 IP アドレス,宛先 IP アドレスに any を設定します。

3. <IPsec トンネルポリシー設定>

```
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
```

NXR_A との IPsec 接続で使用するトンネルポリシー1 を設定します。

IPsec トンネルポリシー1 の説明として NXR_A、ネゴシエーションモードとして auto を設定します。

```
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

4. <トンネルインタフェース設定>

```
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
```

トンネル 1 インタフェースでトンネルモードを ipsec ipv4、使用するトンネルポリシーとして 1 を設定します。また TCP MSS の調整機能をオートに設定します。

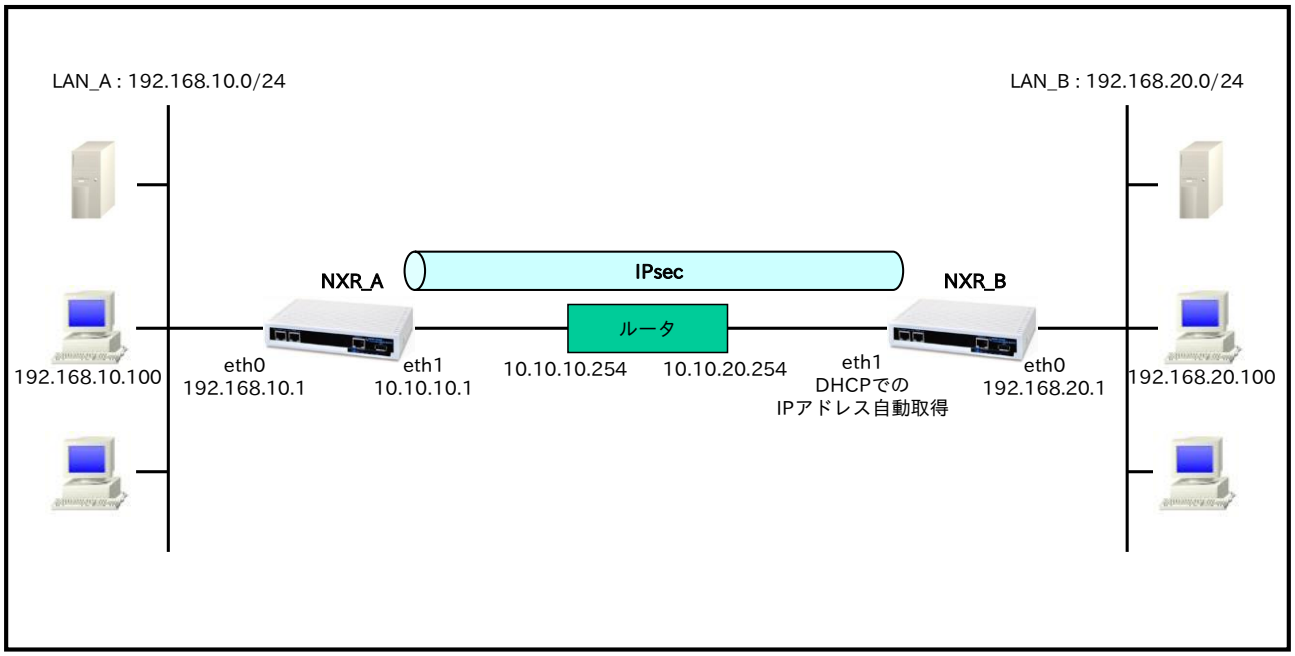
【 パソコンの設定例 】

	LAN A のパソコン	LAN B のパソコン
IP アドレス	192.168.10.100	192.168.20.100
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1

2-2. 動的 IP アドレスでの接続設定例(AggressiveMode の利用)

NXR の WAN 側 IP アドレスが接続のたびに変わる動的 IP アドレス環境でも IPsec を利用することが可能です。なおこの設定例では固定 IP-動的 IP での接続を想定しています。動的 IP 同士での接続は 2-8. FQDN での IPsec 接続設定例をご参照ください。

【 構成図 】



- Route Based IPsec は Policy Based IPsec での設定に対し以下の設定を追加する必要があります。
  - ・トンネルインタフェース設定
  - ・ルート設定(スタティックルート設定,RIPv1/v2,OSPF,BGP)
- 1-2. 動的 IP アドレスでの接続設定例(AggressiveMode の利用)の内容も一部参考になりますので、ご参照下さい。

【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1 1
NXR_A(config)#ip route 192.168.20.0/24 null 254
NXR_A(config)#ip route 0.0.0.0/0 10.10.10.254
NXR_A(config)#ipsec access-list ipsec_acl ip any any
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A(config-ipsec-isakmp)#remote address ip any
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrb
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address ipsec_acl
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
NXR_A(config-tunnel)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#ip address 10.10.10.1/24
NXR_A(config-if)#ipsec policy 1
NXR_A(config-if)#exit
NXR_A(config)#fast-forwarding enable
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1 1
NXR_B(config)#ip route 192.168.10.0/24 null 254
NXR_B(config)#ipsec access-list ipsec_acl ip any any
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
NXR_B(config-tunnel)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address dhcp
NXR_B(config-if)#ipsec policy 1
NXR_B(config-if)#exit
NXR_B(config)#fast-forwarding enable
NXR_B(config)#exit
NXR_B#save config
```

【 設定例解説 】

〔NXR_A の設定〕

(☞) ここに記載のない設定項目は 1-2. 動的 IP アドレスでの接続設定例(AggressiveMode の利用)の〔NXR_A の設定〕が参考になりますので、そちらをご参照下さい。

1. <スタティックルート設定>

```
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1 1
```

LAN_B 向け 192.168.20.0/24 のルートを設定します。なおゲートウェイインタフェースは tunnel 1 を設定します。またこのルートのディスタンス値として 1 を設定します。

(☞) これは IPsec で使用するスタティックルートであり、ここで設定した宛先 IP アドレスにマッチしたパケットが IPsec のカプセル化対象となります。なおゲートウェイアドレスは IPsec で使用するトンネルインタフェースを設定します。

```
NXR_A(config)#ip route 192.168.20.0/24 null 254
```

LAN_B 向け 192.168.20.0/24 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

(☞) null インタフェースを出力インタフェースとして設定した場合、パケットが出力されることはありません(ドロップされます)。よってパケット出力を行う場合は null インタフェースよりもディスタンス値が小さいルートを設定する必要があります。

2. <IPsec アクセスリスト設定>

```
NXR_A(config)#ipsec access-list ipsec_acl ip any any
```

IPsec アクセスリスト名を ipsec_acl とし、送信元 IP アドレス,宛先 IP アドレスに any を設定します。Policy Based IPsec では IPsec アクセスリストで設定したルールに基づき IPsec で ESP 化するかどうかが決定されましたが、Route Based IPsec では IPsec アクセスリストは IKE フェーズ 2 の ID としてのみ使用します。

(☞) Route Based IPsec で ESP 化するか否かは IPsec アクセスリストではなくトンネルインタフェースをゲートウェイとするルート設定の有無で決まります。

3. <IPsec トンネルポリシー設定>

```
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
```

NXR_B との IPsec 接続で使用するトンネルポリシー1 を設定します。IPsec トンネルポリシー1 の説明として NXR_B、ネゴシエーションモードとして responder を設定します。

```
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address ipsec_acl
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

4. <トンネルインタフェース設定>

```
NXR_A(config)#interface tunnel 1
```

トンネル 1 インタフェースを設定します。

```
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
```

トンネルインタフェースで使用するトンネルモードを設定します。

トンネルインタフェースを Route Based IPsec で使用する場合は ipsec ipv4 と設定します。

```
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
```

使用する IPsec トンネルポリシーを設定します。

ここでは IPsec トンネルポリシー1 と関連づけを行います。

(☞) IPsec ローカルポリシーではありませんのでご注意下さい。

```
NXR_A(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

〔NXR_B の設定〕

(☞) ここに記載のない設定項目は 1-2. 動的 IP アドレスでの接続設定例(AggressiveMode の利用)の〔NXR_B の設定〕が参考になりますので、そちらをご参照下さい。

1. <スタティックルート設定>

```
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1 1
```

LAN_A 向け 192.168.10.0/24 のルートを設定します。なおゲートウェイインタフェースは tunnel 1 を設定します。またこのルートのディスタンス値として 1 を設定します。

```
NXR_B(config)#ip route 192.168.10.0/24 null 254
```

LAN_A 向け 192.168.10.0/24 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

2. <IPsec アクセスリスト設定>

```
NXR_B(config)#ipsec access-list ipsec_acl ip any any
```

IPsec アクセスリスト名を ipsec_acl とし、送信元 IP アドレス,宛先 IP アドレスに any を設定します。

3. <IPsec トンネルポリシー設定>

```
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
```

NXR_A との IPsec 接続で使用するトンネルポリシー1 を設定します。

IPsec トンネルポリシー1 の説明として NXR_A、ネゴシエーションモードとして auto を設定します。

```
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

4. <トンネルインタフェース設定>

```
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
```

トンネル 1 インタフェースでトンネルモードを ipsec ipv4、使用するトンネルポリシーとして 1 を設定します。また TCP MSS の調整機能をオートに設定します。

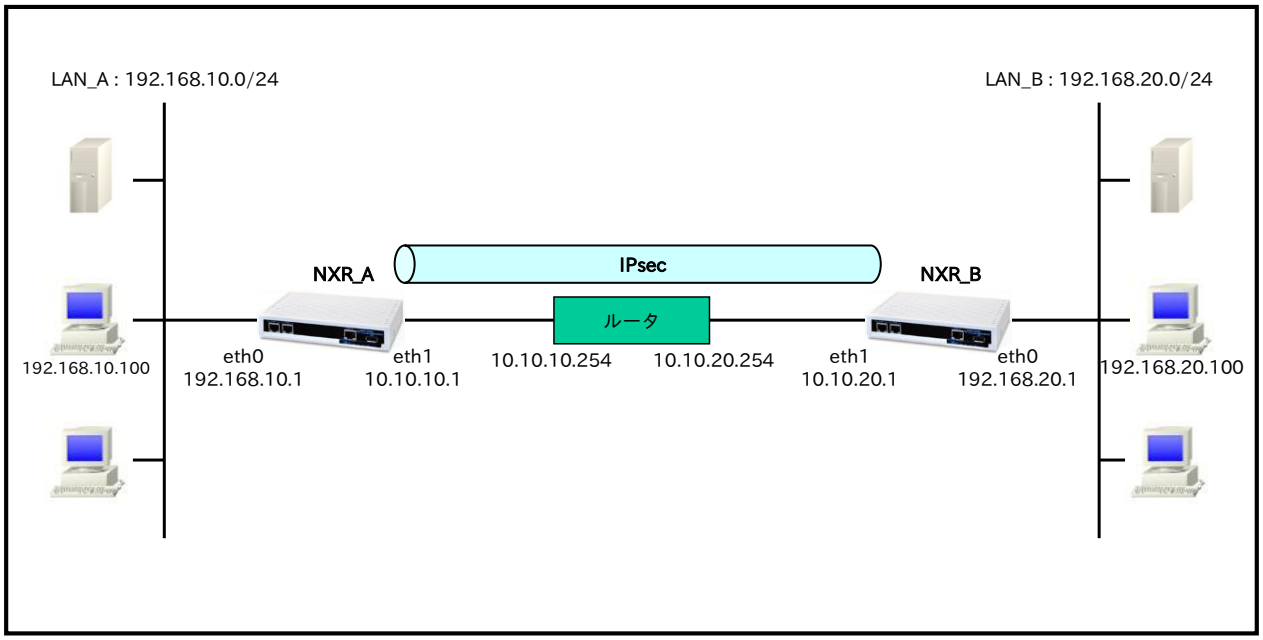
【 パソコンの設定例 】

	LAN A のパソコン	LAN B のパソコン
IP アドレス	192.168.10.100	192.168.20.100
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1

2-3. RSA 公開鍵暗号方式での接続設定例

IKE のフェーズ 1 で対向の NXR の認証に RSA 公開鍵暗号方式を利用することができます。RSA 公開鍵暗号方式を利用する場合は IKE のフェーズ 1 でメインモードを使用する必要があります。

【 構成図 】



- Route Based IPsec は Policy Based IPsec での設定に対し以下の設定を追加する必要があります。
  - ・トンネルインタフェース設定
  - ・ルート設定(スタティックルート設定,RIPv1/v2,OSPF,BGP)
- 1-3. RSA 公開鍵暗号方式での接続設定例の内容も参考になりますのでご参照下さい。

【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1 1
NXR_A(config)#ip route 192.168.20.0/24 null 254
NXR_A(config)#ip route 0.0.0.0/0 10.10.10.254
NXR_A(config)#ipsec access-list ipsec_acl ip any any
NXR_A(config)#ipsec generate rsa-sig-key 1024
RSA-SIG KEY generating...
NXR_A(config)#exit
NXR_A#show ipsec rsa-pub-key
RSA public key :
0sAQNe9Ghb4CNEaJuIIy67aSxECLJDHhvndH1opuMs6P8yGiTNlcGeSOQ8XEy8iYTst2bv022XUxSt37RhOR
5lRiY1i83TXkQZbhnJDCNJv+rtX/aro745MbJ9auXT1L5tda4C54S7SELboAtU28sD3si0OwlzLWtE7yRUqLP4Z
iiNMw==
NXR_A#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#self-identity fqdn nxra
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication rsa-sig 0sAQOx8kE6uhZTvWMikunsy3uK5/7jIkTX sCjQpgo
4B+X64UAVeuxFQZ3KG3bzyjmyCbpkt0xEiU+v1kF4AOAOXoDfgND+KAdEky/YWqQYzMuuuu2uy/K6E9JA
24NACufuqMqgGSXc51fJ/6V5Qi9YtVd7TWBkZQSZJJADBHs/YyYD9Q==
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode main
NXR_A(config-ipsec-isakmp)#remote address ip 10.10.20.1
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrb
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address ipsec_acl
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
NXR_A(config-tunnel)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#ip address 10.10.10.1/24
NXR_A(config-if)#ipsec policy 1
NXR_A(config-if)#exit
NXR_A(config)#fast-forwarding enable
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1 1
NXR_B(config)#ip route 192.168.10.0/24 null 254
NXR_B(config)#ip route 0.0.0.0/0 10.10.20.254
NXR_B(config)#ipsec access-list ipsec_acl ip any any
NXR_B(config)#ipsec generate rsa-sig-key 1024
RSA-SIG KEY generating...
NXR_B(config)#exit
NXR_B#show ipsec rsa-pub-key
RSA public key :
0sAQOx8kE6uhZTvWMikunsy3uK5/7jIkTXsCjQpgo4B+X64UAVeuxFQZ3KG3bzyjmyCbpkt0xEiU+v1kF4AO
AOXoDfgND+KAdEky/YWqQYzMuuuu2uy/K6E9JA24NACufuqMqgGSXc51fJ/6V5Qi9YtVd7TWBkZQSZJJAD
BHs/YyYD9Q==
NXR_B#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication rsa-sig 0sAQNe9Ghb4CNEaJuIIy67aSxECLJDHhvndH1opu
Ms6P8yGiTNlcGeSOQ8XEy8iYTst2bv022XUxSt37RhOR5lRiY1i83TXkQZbhnJDCNJv+rtX/aro745MbJ9auXT
1L5tda4C54S7SELboAtU28sD3si0OwlzLWtE7yRUqLP4ZiiNMw==
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#remote identity fqdn nxra
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
NXR_B(config-tunnel)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address 10.10.20.1/24
NXR_B(config-if)#ipsec policy 1
NXR_B(config-if)#exit
NXR_B(config)#fast-forwarding enable
NXR_B(config)#exit
NXR_B#save config
```

【 設定例解説 】

〔NXR_A の設定〕

(☞) ここに記載のない設定項目は 1-3. RSA 公開鍵暗号方式での接続設定例の〔NXR_A の設定〕が参考になりますので、そちらをご参照下さい。

1. <スタティックルート設定>

```
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1 1
```

LAN_B 向け 192.168.20.0/24 のルートを設定します。なおゲートウェイインタフェースは tunnel 1 を設定します。またこのルートのディスタンス値として 1 を設定します。

(☞) これは IPsec で使用するスタティックルートであり、ここで設定した宛先 IP アドレスにマッチしたパケットが IPsec のカプセル化対象となります。なおゲートウェイアドレスは IPsec で使用するトンネルインタフェースを設定します。

```
NXR_A(config)#ip route 192.168.20.0/24 null 254
```

LAN_B 向け 192.168.20.0/24 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

(☞) null インタフェースを出力インタフェースとして設定した場合、パケットが出力されることはありません(ドロップされます)。よってパケット出力を行う場合は null インタフェースよりもディスタンス値が小さいルートを設定する必要があります。

2. <IPsec アクセスリスト設定>

```
NXR_A(config)#ipsec access-list ipsec_acl ip any any
```

IPsec アクセスリスト名を ipsec_acl とし、送信元 IP アドレス,宛先 IP アドレスに any を設定します。

Policy Based IPsec では IPsec アクセスリストで設定したルールに基づき IPsec で ESP 化するかどうかが決定されましたが、Route Based IPsec では IPsec アクセスリストは IKE フェーズ 2 の ID としてのみ使用します。

(☞) Route Based IPsec で ESP 化するか否かは IPsec アクセスリストではなくトンネルインタフェースをゲートウェイとするルート設定の有無で決まります。

3. <IPsec トンネルポリシー設定>

```
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
```

NXR_B との IPsec 接続で使用するトンネルポリシー1 を設定します。

IPsec トンネルポリシー1 の説明として NXR_B、ネゴシエーションモードとして auto を設定します。

```
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address ipsec_acl
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

4. <トンネルインタフェース設定>

```
NXR_A(config)#interface tunnel 1
```

トンネル 1 インタフェースを設定します。

```
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
```

トンネルインタフェースで使用するトンネルモードを設定します。

トンネルインタフェースを Route Based IPsec で使用する場合は ipsec ipv4 と設定します。

```
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
```

使用する IPsec トンネルポリシーを設定します。

ここでは IPsec トンネルポリシー1 と関連づけを行います。

(☞) IPsec ローカルポリシーではありませんのでご注意下さい。

```
NXR_A(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

〔NXR_B の設定〕

(☞) ここに記載のない設定項目は 1-3. RSA 公開鍵暗号方式での接続設定例の〔NXR_B の設定〕が参考になりますので、そちらをご参照下さい。

1. <スタティックルート設定>

```
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1 1
```

LAN_A 向け 192.168.10.0/24 のルートを設定します。なおゲートウェイインタフェースは tunnel 1 を設定します。またこのルートのディスタンス値として 1 を設定します。

```
NXR_B(config)#ip route 192.168.10.0/24 null 254
```

LAN_A 向け 192.168.10.0/24 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

2. <IPsec アクセスリスト設定>

```
NXR_B(config)#ipsec access-list ipsec_acl ip any any
```

IPsec アクセスリスト名を ipsec_acl とし、送信元 IP アドレス,宛先 IP アドレスに any を設定します。

3. <IPsec トンネルポリシー設定>

```
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
```

NXR_A との IPsec 接続で使用するトンネルポリシー1 を設定します。

IPsec トンネルポリシー1 の説明として NXR_A、ネゴシエーションモードとして auto を設定します。

```
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

4. <トンネルインタフェース設定>

```
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
```

トンネル 1 インタフェースでトンネルモードを ipsec ipv4、使用するトンネルポリシーとして 1 を設定します。また TCP MSS の調整機能をオートに設定します。

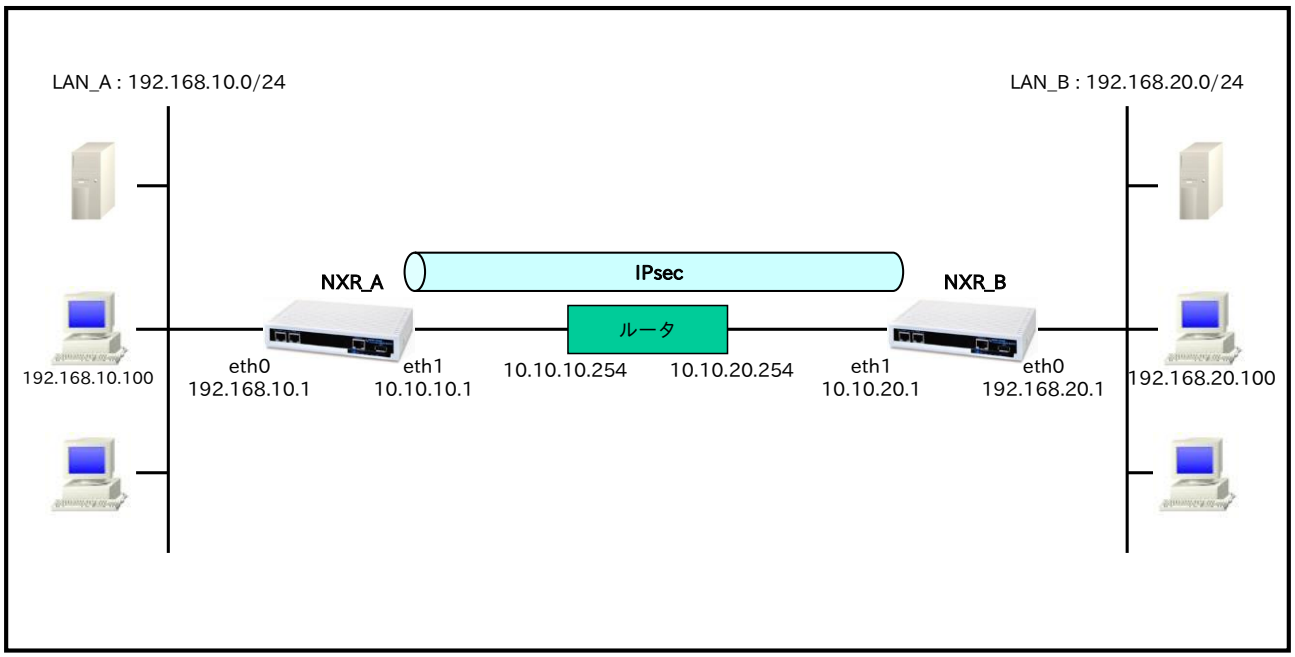
【 パソコンの設定例 】

	LAN A のパソコン	LAN B のパソコン
IP アドレス	192.168.10.100	192.168.20.100
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1

2-4. X.509(デジタル署名認証)方式での接続設定例

IKE のフェーズ 1 で対向の NXR の認証に X.509(デジタル署名認証)方式を利用することができます。認証で利用する証明書や鍵は FutureNet RA シリーズや別途 CA 等で事前に用意しておく必要があります(NXR では証明書の発行を行うことはできません)。X.509 方式を利用する場合は IKE のフェーズ 1 でメインモードを使用する必要があります。

【 構成図 】



- Route Based IPsec は Policy Based IPsec での設定に対し以下の設定を追加する必要があります。
  - ・トンネルインタフェース設定
  - ・ルート設定(スタティックルート設定,RIPv1/v2,OSPF,BGP)
- 1-4. X.509(デジタル署名認証)方式での接続設定例の内容も参考になりますのでご参照下さい。

【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1 1
NXR_A(config)#ip route 192.168.20.0/24 null 254
NXR_A(config)#ip route 0.0.0.0/0 10.10.10.254
NXR_A(config)#ipsec access-list ipsec_acl ip any any
NXR_A(config)#ipsec x509 enable
NXR_A(config)#ipsec x509 ca-certificate nxr ftp://192.168.10.10/nxrCA.pem
NXR_A(config)#ipsec x509 crl nxr ftp://192.168.10.10/nxrCRL.pem
NXR_A(config)#ipsec x509 certificate nxra ftp://192.168.10.10/nxraCert.pem
NXR_A(config)#ipsec x509 private-key nxra key ftp://192.168.10.10/nxraKey.pem
NXR_A(config)#ipsec x509 private-key nxra password nxrapass
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#x509 certificate nxra
NXR_A(config-ipsec-local)#self-identity dn /C=JP/CN=nxra/E=nxra@example.com
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication rsa-sig
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode main
NXR_A(config-ipsec-isakmp)#remote address ip 10.10.20.1
NXR_A(config-ipsec-isakmp)#remote identity dn /C=JP/CN=nxrb/E=nxrb@example.com
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address ipsec_acl
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
NXR_A(config-tunnel)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#ip address 10.10.10.1/24
NXR_A(config-if)#ipsec policy 1
NXR_A(config-if)#exit
NXR_A(config)#fast-forwarding enable
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1 1
NXR_B(config)#ip route 192.168.10.0/24 null 254
NXR_B(config)#ip route 0.0.0.0/0 10.10.20.254
NXR_B(config)#ipsec access-list ipsec_acl ip any any
NXR_B(config)#ipsec x509 enable
NXR_B(config)#ipsec x509 ca-certificate nxr ftp://192.168.20.10/nxrCA.pem
NXR_B(config)#ipsec x509 crl nxr ftp://192.168.20.10/nxrCRL.pem
NXR_B(config)#ipsec x509 certificate nxrb ftp://192.168.20.10/nxrbCert.pem
NXR_B(config)#ipsec x509 private-key nxrb key ftp://192.168.20.10/nxrbKey.pem
NXR_B(config)#ipsec x509 private-key nxrb password nxrbpass
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#x509 certificate nxrb
NXR_B(config-ipsec-local)#self-identity dn /C=JP/CN=nxrb/E=nxrb@example.com
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication rsa-sig
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#remote identity dn /C=JP/CN=nxra/E=nxra@example.com
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
NXR_B(config-tunnel)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address 10.10.20.1/24
NXR_B(config-if)#ipsec policy 1
NXR_B(config-if)#exit
NXR_B(config)#fast-forwarding enable
NXR_B(config)#exit
NXR_B#save config
```

【 設定例解説 】

〔NXR_A の設定〕

(☞) ここに記載のない設定項目は 1-4. X.509(デジタル署名認証)方式での接続設定例の〔NXR_A の設定〕が参考になりますので、そちらをご参照下さい。

1. <スタティックルート設定>

```
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1 1
```

LAN_B 向け 192.168.20.0/24 のルートを設定します。なおゲートウェイインタフェースは tunnel 1 を設定します。またこのルートのディスタンス値として 1 を設定します。

(☞) これは IPsec で使用するスタティックルートであり、ここで設定した宛先 IP アドレスにマッチしたパケットが IPsec のカプセル化対象となります。なおゲートウェイアドレスは IPsec で使用するトンネルインタフェースを設定します。

```
NXR_A(config)#ip route 192.168.20.0/24 null 254
```

LAN_B 向け 192.168.20.0/24 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

(☞) null インタフェースを出力インタフェースとして設定した場合、パケットが出力されることはありません(ドロップされます)。よってパケット出力を行う場合は null インタフェースよりもディスタンス値が小さいルートを設定する必要があります。

2. <IPsec アクセスリスト設定>

```
NXR_A(config)#ipsec access-list ipsec_acl ip any any
```

IPsec アクセスリスト名を ipsec_acl とし、送信元 IP アドレス,宛先 IP アドレスに any を設定します。

Policy Based IPsec では IPsec アクセスリストで設定したルールに基づき IPsec で ESP 化するかどうかが決定されましたが、Route Based IPsec では IPsec アクセスリストは IKE フェーズ 2 の ID としてのみ使用します。

(☞) Route Based IPsec で ESP 化するか否かは IPsec アクセスリストではなくトンネルインタフェースをゲートウェイとするルート設定の有無で決まります。

3. <IPsec トンネルポリシー設定>

```
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
```

NXR_B との IPsec 接続で使用するトンネルポリシー1 を設定します。

IPsec トンネルポリシー1 の説明として NXR_B、ネゴシエーションモードとして auto を設定します。

```
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address ipsec_acl
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

4. <トンネルインタフェース設定>

```
NXR_A(config)#interface tunnel 1
```

トンネル 1 インタフェースを設定します。

```
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
```

トンネルインタフェースで使用するトンネルモードを設定します。

トンネルインタフェースを Route Based IPsec で使用する場合は ipsec ipv4 と設定します。

```
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
```

使用する IPsec トンネルポリシーを設定します。

ここでは IPsec トンネルポリシー1 と関連づけを行います。

(☞) IPsec ローカルポリシーではありませんのでご注意下さい。

```
NXR_A(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

〔NXR_B の設定〕

(☞) ここに記載のない設定項目は 1-4. X.509(デジタル署名認証)方式での接続設定例の〔NXR_B の設定〕が参考になりますので、そちらをご参照下さい。

1. <スタティックルート設定>

```
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1 1
```

LAN_A 向け 192.168.10.0/24 のルートを設定します。なおゲートウェイインタフェースは tunnel 1 を設定します。またこのルートのディスタンス値として 1 を設定します。

```
NXR_B(config)#ip route 192.168.10.0/24 null 254
```

LAN_A 向け 192.168.10.0/24 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

2. <IPsec アクセスリスト設定>

```
NXR_B(config)#ipsec access-list ipsec_acl ip any any
```

IPsec アクセスリスト名を ipsec_acl とし、送信元 IP アドレス,宛先 IP アドレスに any を設定します。

3. <IPsec トンネルポリシー設定>

```
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
```

NXR_A との IPsec 接続で使用するトンネルポリシー1 を設定します。

IPsec トンネルポリシー1 の説明として NXR_A、ネゴシエーションモードとして auto を設定します。

```
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

4. <トンネルインタフェース設定>

```
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
```

トンネル 1 インタフェースでトンネルモードを ipsec ipv4、使用するトンネルポリシーとして 1 を設定します。また TCP MSS の調整機能をオートに設定します。

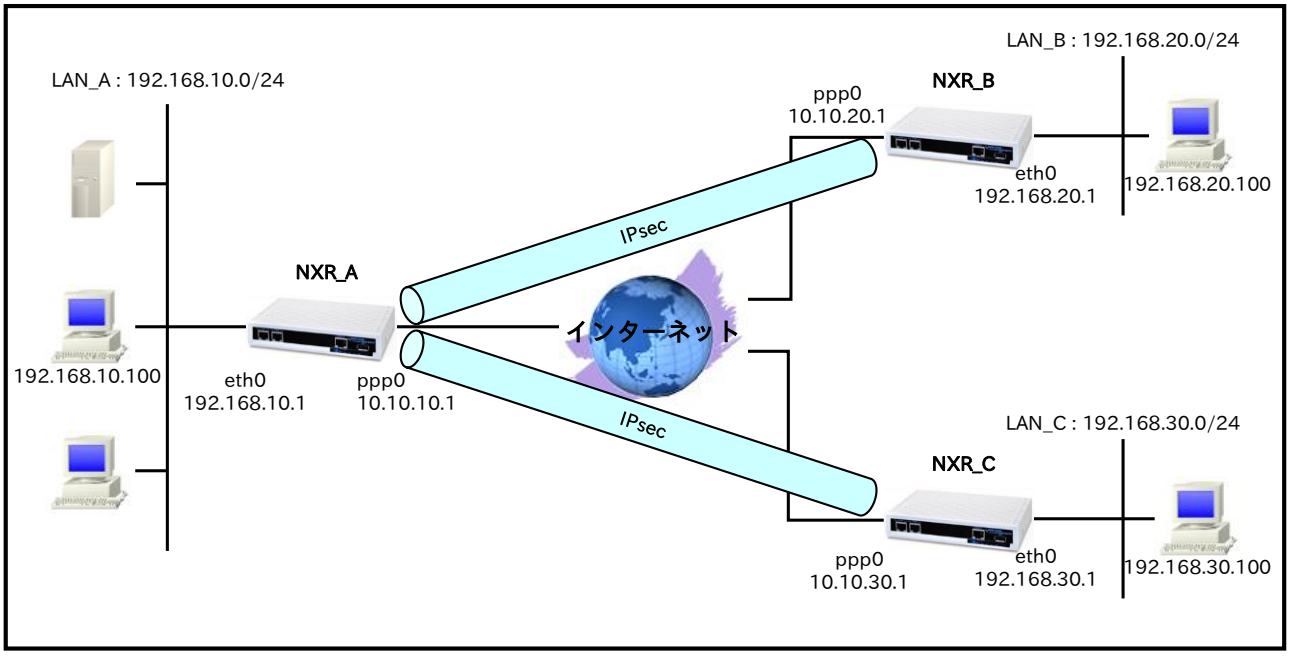
【 パソコンの設定例 】

	LAN A のパソコン	LAN B のパソコン
IP アドレス	192.168.10.100	192.168.20.100
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1

2-5. PPPoE を利用した IPsec 接続設定例

PPPoE 上でも IPsec を利用することは可能です。ここではフェーズ 1 で NXR_A(センタ)－NXR_B(拠点)間はメインモードを NXR_A(センタ)－NXR_C(拠点)間はアグレッシブモードを利用して接続しています。
なお、この設定例では IPsec 経由での拠点間通信は行いません。
また、ここでは各拠点からのインターネットアクセスを可能にするためにフィルタ設定(SPI),NAT 設定(IP マスカレード),DNS 設定を行っています。

【 構成図 】



- Route Based IPsec は Policy Based IPsec での設定に対し以下の設定を追加する必要があります。
  - ・トンネルインタフェース設定
  - ・ルート設定(スタティックルート設定,RIPv1/v2,OSPF,BGP)
- この設定例では IPsec 経由での拠点間通信は行いません。
- この設定例では ipsec priority-ignore 機能を使用します。この機能に対応していないファームウェアをご利用頂いている場合は、同じフェーズ 2 の ID を持つ IPsec SA を同時に複数個確立することができません。そのため設定例のように同一の IPsec アクセスリストを複数の IPsec トンネルポリシーに適用した場合 IPsec SA を複数同時に確立することができませんので、各 IPsec トンネルポリシー毎に異なるルールの IPsec アクセスリストを設定する必要があります。
- 各拠点からのインターネットアクセスを可能にするために、NAT 設定(IP マスカレード)やフィルタ設定(SPI)および DNS 設定を行っています。
- 1-5. PPPoE を利用した IPsec 接続設定例の内容も参考になりますのでご参照下さい。

【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1 1
NXR_A(config)#ip route 192.168.30.0/24 tunnel 2 1
NXR_A(config)#ip route 192.168.20.0/24 null 254
NXR_A(config)#ip route 192.168.30.0/24 null 254
NXR_A(config)#ip route 0.0.0.0/0 ppp 0
NXR_A(config)#ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
NXR_A(config)#ip access-list ppp0_in permit any 10.10.10.1 50
NXR_A(config)#ipsec access-list ipsec_acl ip any any
NXR_A(config)#ipsec priority-ignore enable
% restart ipsec service to take affect.
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode main
NXR_A(config-ipsec-isakmp)#remote address ip 10.10.20.1
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address ipsec_acl
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
NXR_A(config-tunnel)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#ipsec isakmp policy 2
NXR_A(config-ipsec-isakmp)#description NXR_C
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A(config-ipsec-isakmp)#remote address ip any
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrc
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 2
NXR_A(config-ipsec-tunnel)#description NXR_C
```

```
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 2
NXR_A(config-ipsec-tunnel)#match address ipsec_acl
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 2
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 2
NXR_A(config-tunnel)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#interface ppp 0
NXR_A(config-ppp)#ip address 10.10.10.1/32
NXR_A(config-ppp)#ip masquerade
NXR_A(config-ppp)#ip access-group in ppp0_in
NXR_A(config-ppp)#ip spi-filter
NXR_A(config-ppp)#ip tcp adjust-mss auto
NXR_A(config-ppp)#no ip redirects
NXR_A(config-ppp)#ppp username test1@example.jp password test1pass
NXR_A(config-ppp)#ipsec policy 1
NXR_A(config-ppp)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#no ip address
NXR_A(config-if)#pppoe-client ppp 0
NXR_A(config-if)#exit
NXR_A(config)#dns
NXR_A(config-dns)#service enable
NXR_A(config-dns)#exit
NXR_A(config)#fast-forwarding enable
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1 1
NXR_B(config)#ip route 192.168.10.0/24 null 254
NXR_B(config)#ip route 0.0.0.0/0 ppp 0
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 udp 500 500
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 50
NXR_B(config)#ipsec access-list ipsec_acl ip any any
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
```

```
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
NXR_B(config-tunnel)#exit
NXR_B(config)#interface ppp 0
NXR_B(config-ppp)#ip address 10.10.20.1/32
NXR_B(config-ppp)#ip masquerade
NXR_B(config-ppp)#ip access-group in ppp0_in
NXR_B(config-ppp)#ip spi-filter
NXR_B(config-ppp)#ip tcp adjust-mss auto
NXR_B(config-ppp)#no ip redirects
NXR_B(config-ppp)#ppp username test2@example.jp password test2pass
NXR_B(config-ppp)#ipsec policy 1
NXR_B(config-ppp)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#no ip address
NXR_B(config-if)#pppoe-client ppp 0
NXR_B(config-if)#exit
NXR_B(config)#dns
NXR_B(config-dns)#service enable
NXR_B(config-dns)#exit
NXR_B(config)#fast-forwarding enable
NXR_B(config)#exit
NXR_B#save config
```

〔NXR_C の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_C
NXR_C(config)#interface ethernet 0
NXR_C(config-if)#ip address 192.168.30.1/24
NXR_C(config-if)#exit
NXR_C(config)#ip route 192.168.10.0/24 tunnel 1 1
NXR_C(config)#ip route 192.168.10.0/24 null 254
NXR_C(config)#ip route 0.0.0.0/0 ppp 0
NXR_C(config)#ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
NXR_C(config)#ip access-list ppp0_in permit 10.10.10.1 any 50
NXR_C(config)#ipsec access-list ipsec_acl ip any any
NXR_C(config)#ipsec local policy 1
NXR_C(config-ipsec-local)#address ip
NXR_C(config-ipsec-local)#self-identity fqdn nxrc
NXR_C(config-ipsec-local)#exit
NXR_C(config)#ipsec isakmp policy 1
NXR_C(config-ipsec-isakmp)#description NXR_A
NXR_C(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR_C(config-ipsec-isakmp)#hash sha1
NXR_C(config-ipsec-isakmp)#encryption aes128
NXR_C(config-ipsec-isakmp)#group 5
NXR_C(config-ipsec-isakmp)#lifetime 10800
NXR_C(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_C(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_C(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_C(config-ipsec-isakmp)#local policy 1
```

```
NXR_C(config-ipsec-isakmp)#exit
NXR_C(config)#ipsec tunnel policy 1
NXR_C(config-ipsec-tunnel)#description NXR_A
NXR_C(config-ipsec-tunnel)#negotiation-mode auto
NXR_C(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_C(config-ipsec-tunnel)#set pfs group5
NXR_C(config-ipsec-tunnel)#set sa lifetime 3600
NXR_C(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_C(config-ipsec-tunnel)#match address ipsec_acl
NXR_C(config-ipsec-tunnel)#exit
NXR_C(config)#interface tunnel 1
NXR_C(config-tunnel)#tunnel mode ipsec ipv4
NXR_C(config-tunnel)#tunnel protection ipsec policy 1
NXR_C(config-tunnel)#ip tcp adjust-mss auto
NXR_C(config-tunnel)#exit
NXR_C(config)#interface ppp 0
NXR_C(config-ppp)#ip address negotiated
NXR_C(config-ppp)#ip masquerade
NXR_C(config-ppp)#ip access-group in ppp0_in
NXR_C(config-ppp)#ip spi-filter
NXR_C(config-ppp)#ip tcp adjust-mss auto
NXR_C(config-ppp)#no ip redirects
NXR_C(config-ppp)#ppp username test3@example.jp password test3pass
NXR_C(config-ppp)#ipsec policy 1
NXR_C(config-ppp)#exit
NXR_C(config)#interface ethernet 1
NXR_C(config-if)#no ip address
NXR_C(config-if)#pppoe-client ppp 0
NXR_C(config-if)#exit
NXR_C(config)#dns
NXR_C(config-dns)#service enable
NXR_C(config-dns)#exit
NXR_C(config)#fast-forwarding enable
NXR_C(config)#exit
NXR_C#save config
```

【 設定例解説 】

〔NXR_A の設定〕

(☞) ここに記載のない設定項目は 1-5. PPPoE を利用した IPsec 接続設定例の〔NXR_A の設定〕が参考になりますので、そちらをご参照下さい。

1. <スタティックルート設定>

```
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1 1
NXR_A(config)#ip route 192.168.30.0/24 tunnel 2 1
```

一行目は LAN_B 向け 192.168.20.0/24 のルートを設定します。なおゲートウェイインタフェースは tunnel 1 を設定します。またこのルートのディスタンス値として 1 を設定します。

二行目は LAN_C 向け 192.168.30.0/24 のルートを設定します。なおゲートウェイインタフェースは tunnel 2 を設定します。またこのルートのディスタンス値として 1 を設定します。

(☞) これは IPsec で使用するスタティックルートであり、ここで設定した宛先 IP アドレスにマッチしたパケットが IPsec のカプセル化対象となります。なおゲートウェイアドレスは IPsec で使用するトンネルインタフェースを設定します。

```
NXR_A(config)#ip route 192.168.20.0/24 null 254
NXR_A(config)#ip route 192.168.30.0/24 null 254
```

一行目は LAN_B 向け 192.168.20.0/24 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。
二行目は LAN_C 向け 192.168.30.0/24 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

(☞) null インタフェースを出力インタフェースとして設定した場合、パケットが出力されることはありません(ドロップされます)。よってパケット出力を行う場合は null インタフェースよりもディスタンス値が小さいルートを設定する必要があります。

2. <IPsec アクセスリスト設定>

```
NXR_A(config)#ipsec access-list ipsec_acl ip any any
```

IPsec アクセスリスト名を ipsec_acl とし、送信元 IP アドレス,宛先 IP アドレスに any を設定します。
Policy Based IPsec では IPsec アクセスリストで設定したルールに基づき IPsec で ESP 化するかどうかが決定されましたが、Route Based IPsec では IPsec アクセスリストは IKE フェーズ 2 の ID としてのみ使用します。

(☞) Route Based IPsec で ESP 化するか否かは IPsec アクセスリストではなくトンネルインタフェースをゲートウェイとするルート設定の有無で決まります。

3. <IPsec priority-ignore 設定>

```
NXR_A(config)#ipsec priority-ignore enable
```

ipsec priority-ignore を有効に設定します。
これはプライオリティによる IPsec SA の優先度を無効にする設定です。
Route based IPsec ではフェーズ 2 の ID を IPsec SA を確立するための ID としてのみ使用します。そのためプライオリティによる冗長化設定などを利用しない場合は、本設定を有効にすることによって同じフェーズ 2 の ID を持つ IPsec SA を複数個同時に確立することができます。

(☞) この機能に対応していないファームウェアをご利用頂いている場合は、同じフェーズ 2 の ID を持つ IPsec SA を同時に複数個確立することができません。そのため設定例のように同一の IPsec アクセスリストを複数の IPsec トンネルポリシーに適用した場合 IPsec SA を複数同時に確立することができませんので、各 IPsec トンネルポリシー毎に異なるルールの IPsec アクセスリストを設定する必要があります。

4. <IPsec トンネルポリシー1 設定>

```
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
```

NXR_B との IPsec 接続で使用するトンネルポリシー1 を設定します。
IPsec トンネルポリシー1 の説明として NXR_B、ネゴシエーションモードとして auto を設定します。

```
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address ipsec_acl
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

5. <トンネル 1 インタフェース設定>

```
NXR_A(config)#interface tunnel 1
```

トンネル 1 インタフェースを設定します。

```
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
```

トンネルインタフェースで使用するトンネルモードを設定します。

トンネルインタフェースを Route Based IPsec で使用する場合は ipsec ipv4 と設定します。

```
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
```

使用する IPsec トンネルポリシーを設定します。

ここでは IPsec トンネルポリシー1 と関連づけを行います。

(☞) IPsec ローカルポリシーではありませんのでご注意下さい。

```
NXR_A(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

6. <IPsec トンネルポリシー2 設定>

```
NXR_A(config)#ipsec tunnel policy 2
NXR_A(config-ipsec-tunnel)#description NXR_C
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
```

NXR_C との IPsec 接続で使用するトンネルポリシー2 を設定します。IPsec トンネルポリシー2 の説明として NXR_C、ネゴシエーションモードとして responder を設定します。

```
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 2
NXR_A(config-ipsec-tunnel)#match address ipsec_acl
```

ISAKMP ポリシー 2 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

7. <トンネル 2 インタフェース設定>

```
NXR_A(config)#interface tunnel 2
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 2
NXR_A(config-tunnel)#ip tcp adjust-mss auto
```

トンネル 2 インタフェースでトンネルモードを ipsec ipv4、使用するトンネルポリシーとして 2 を設定します。また TCP MSS の調整機能をオートに設定します。

〔NXR_B の設定〕

(☞) ここに記載のない設定項目は 1-5. PPPoE を利用した IPsec 接続設定例の〔NXR_B の設定〕が参考になりますので、そちらをご参照下さい。

1. <スタティックルート設定>

```
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1 1
```

LAN_A 向け 192.168.10.0/24 のルートを設定します。なおゲートウェイインタフェースは tunnel 1 を設定します。またこのルートのディスタンス値として 1 を設定します。

```
NXR_B(config)#ip route 192.168.10.0/24 null 254
```

LAN_A 向け 192.168.10.0/24 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

2. <IPsec アクセスリスト設定>

```
NXR_B(config)#ipsec access-list ipsec_acl ip any any
```

IPsec アクセスリスト名を ipsec_acl とし、送信元 IP アドレス,宛先 IP アドレスに any を設定します。

3. <IPsec トンネルポリシー設定>

```
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
```

NXR_A との IPsec 接続で使用するトンネルポリシー1 を設定します。

IPsec トンネルポリシー1 の説明として NXR_A、ネゴシエーションモードとして auto を設定します。

```
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

4. <トンネルインタフェース設定>

```
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
```

トンネル 1 インタフェースでトンネルモードを ipsec ipv4、使用するトンネルポリシーとして 1 を設定します。また TCP MSS の調整機能をオートに設定します。

〔NXR_C の設定〕

(☞) ここに記載のない設定項目は 1-5. PPPoE を利用した IPsec 接続設定例の〔NXR_C の設定〕が参考になりますので、そちらをご参照下さい。

1. <スタティックルート設定>

```
NXR_C(config)#ip route 192.168.10.0/24 tunnel 1 1
```

LAN_A 向け 192.168.10.0/24 のルートを設定します。なおゲートウェイインタフェースは tunnel 1 を設定します。またこのルートのディスタンス値として 1 を設定します。

```
NXR_C(config)#ip route 192.168.10.0/24 null 254
```

LAN_A 向け 192.168.10.0/24 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

2. <IPsec アクセスリスト設定>

```
NXR_C(config)#ipsec access-list ipsec_acl ip any any
```

IPsec アクセスリスト名を ipsec_acl とし、送信元 IP アドレス,宛先 IP アドレスに any を設定します。

3. <IPsec トンネルポリシー設定>

```
NXR_C(config)#ipsec tunnel policy 1
NXR_C(config-ipsec-tunnel)#description NXR_A
NXR_C(config-ipsec-tunnel)#negotiation-mode auto
```

NXR_A との IPsec 接続で使用するトンネルポリシー1 を設定します。

IPsec トンネルポリシー1 の説明として NXR_A、ネゴシエーションモードとして auto を設定します。

```
NXR_C(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_C(config-ipsec-tunnel)#set pfs group5
NXR_C(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_C(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_C(config-ipsec-tunnel)#match address ipsec_acl
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

4. ＜トンネルインタフェース設定＞

```
NXR_C(config)#interface tunnel 1
NXR_C(config-tunnel)#tunnel mode ipsec ipv4
NXR_C(config-tunnel)#tunnel protection ipsec policy 1
NXR_C(config-tunnel)#ip tcp adjust-mss auto
```

トンネル 1 インタフェースでトンネルモードを ipsec ipv4、使用するトンネルポリシーとして 1 を設定します。また TCP MSS の調整機能をオートに設定します。

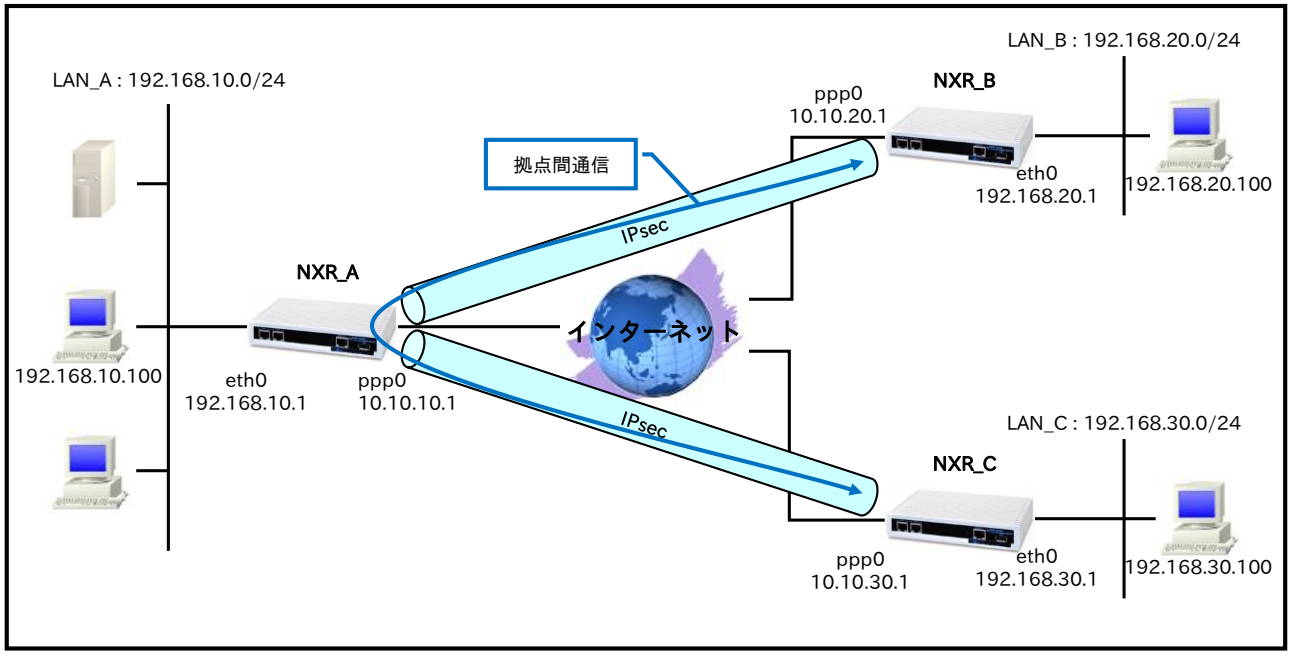
【 パソコンの設定例 】

	LAN A のパソコン	LAN B のパソコン	LAN C のパソコン
IP アドレス	192.168.10.100	192.168.20.100	192.168.30.100
サブネットマスク	255.255.255.0	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1	192.168.30.1
DNS サーバ	192.168.10.1	192.168.20.1	192.168.30.1

2-6. センタ経由拠点間通信設定例

2-5.PPPoE を利用した IPsec 接続設定例では拠点間の IPsec 経由での通信は行えませんでしたが、この設定例ではセンタ経由での拠点間通信を実現します。

【 構成図 】



- Route Based IPsec は Policy Based IPsec での設定に対し以下の設定を追加する必要があります。
  - ・トンネルインタフェース設定
  - ・ルート設定(スタティックルート設定,RIPv1/v2,OSPF,BGP)
- 拠点間通信を実現するためセンタ,拠点で以下のルートを設定します。

		宛先 IP アドレス
NXR_A(センタ)	NXR_B 向け	192.168.20.0/24
	NXR_C 向け	192.168.30.0/24
NXR_B(拠点)	NXR_A,C 向け	192.168.0.0/16
NXR_C(拠点)	NXR_A,B 向け	192.168.0.0/16

- この設定例では ipsec priority-ignore 機能を使用します。この機能に対応していないファームウェアをご利用頂いている場合は、同じフェーズ 2 の ID を持つ IPsec SA を同時に複数個確立することができません。そのため設定例のように同一の IPsec アクセスリストを複数の IPsec トンネルポリシーに適用した場合 IPsec SA を複数同時に確立することができませんので、各 IPsec トンネルポリシー毎に異なるルールの IPsec アクセスリストを設定する必要があります。
- 各拠点からのインターネットアクセスを可能にするために、NAT 設定(IP マスカレード)やフィルタ設定(SPI)および DNS 設定を行っています。
- 1-6. センタ経由拠点間通信設定例の内容も参考になりますのでご参照下さい。

【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1 1
NXR_A(config)#ip route 192.168.30.0/24 tunnel 2 1
NXR_A(config)#ip route 192.168.20.0/24 null 254
NXR_A(config)#ip route 192.168.30.0/24 null 254
NXR_A(config)#ip route 0.0.0.0/0 ppp 0
NXR_A(config)#ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
NXR_A(config)#ip access-list ppp0_in permit any 10.10.10.1 50
NXR_A(config)#ipsec access-list ipsec_acl ip any any
NXR_A(config)#ipsec priority-ignore enable
% restart ipsec service to take affect.
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode main
NXR_A(config-ipsec-isakmp)#remote address ip 10.10.20.1
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address ipsec_acl
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
NXR_A(config-tunnel)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#ipsec isakmp policy 2
NXR_A(config-ipsec-isakmp)#description NXR_C
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A(config-ipsec-isakmp)#remote address ip any
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrc
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
```

```
NXR_A(config)#ipsec tunnel policy 2
NXR_A(config-ipsec-tunnel)#description NXR_C
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 2
NXR_A(config-ipsec-tunnel)#match address ipsec_acl
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 2
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 2
NXR_A(config-tunnel)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#interface ppp 0
NXR_A(config-ppp)#ip address 10.10.10.1/32
NXR_A(config-ppp)#ip masquerade
NXR_A(config-ppp)#ip access-group in ppp0_in
NXR_A(config-ppp)#ip spi-filter
NXR_A(config-ppp)#ip tcp adjust-mss auto
NXR_A(config-ppp)#no ip redirects
NXR_A(config-ppp)#ppp username test1@example.jp password test1pass
NXR_A(config-ppp)#ipsec policy 1
NXR_A(config-ppp)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#no ip address
NXR_A(config-if)#pppoe-client ppp 0
NXR_A(config-if)#exit
NXR_A(config)#dns
NXR_A(config-dns)#service enable
NXR_A(config-dns)#exit
NXR_A(config)#fast-forwarding enable
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 192.168.0.0/16 tunnel 1 1
NXR_B(config)#ip route 192.168.0.0/16 null 254
NXR_B(config)#ip route 0.0.0.0/0 ppp 0
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 udp 500 500
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 50
NXR_B(config)#ipsec access-list ipsec_acl ip any any
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
```

```
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
NXR_B(config-tunnel)#exit
NXR_B(config)#interface ppp 0
NXR_B(config-ppp)#ip address 10.10.20.1/32
NXR_B(config-ppp)#ip masquerade
NXR_B(config-ppp)#ip access-group in ppp0_in
NXR_B(config-ppp)#ip spi-filter
NXR_B(config-ppp)#ip tcp adjust-mss auto
NXR_B(config-ppp)#no ip redirects
NXR_B(config-ppp)#ppp username test2@example.jp password test2pass
NXR_B(config-ppp)#ipsec policy 1
NXR_B(config-ppp)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#no ip address
NXR_B(config-if)#pppoe-client ppp 0
NXR_B(config-if)#exit
NXR_B(config)#dns
NXR_B(config-dns)#service enable
NXR_B(config-dns)#exit
NXR_B(config)#fast-forwarding enable
NXR_B(config)#exit
NXR_B#save config
```

〔NXR_C の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_C
NXR_C(config)#interface ethernet 0
NXR_C(config-if)#ip address 192.168.30.1/24
NXR_C(config-if)#exit
NXR_C(config)#ip route 192.168.0.0/16 tunnel 1 1
NXR_C(config)#ip route 192.168.0.0/16 null 254
NXR_C(config)#ip route 0.0.0.0/0 ppp 0
NXR_C(config)#ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
NXR_C(config)#ip access-list ppp0_in permit 10.10.10.1 any 50
NXR_C(config)#ipsec access-list ipsec_acl ip any any
NXR_C(config)#ipsec local policy 1
NXR_C(config-ipsec-local)#address ip
NXR_C(config-ipsec-local)#self-identity fqdn nxrc
NXR_C(config-ipsec-local)#exit
NXR_C(config)#ipsec isakmp policy 1
NXR_C(config-ipsec-isakmp)#description NXR_A
NXR_C(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR_C(config-ipsec-isakmp)#hash sha1
NXR_C(config-ipsec-isakmp)#encryption aes128
NXR_C(config-ipsec-isakmp)#group 5
NXR_C(config-ipsec-isakmp)#lifetime 10800
NXR_C(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_C(config-ipsec-isakmp)#remote address ip 10.10.10.1
```

```
NXR_C(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_C(config-ipsec-isakmp)#local policy 1
NXR_C(config-ipsec-isakmp)#exit
NXR_C(config)#ipsec tunnel policy 1
NXR_C(config-ipsec-tunnel)#description NXR_A
NXR_C(config-ipsec-tunnel)#negotiation-mode auto
NXR_C(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_C(config-ipsec-tunnel)#set pfs group5
NXR_C(config-ipsec-tunnel)#set sa lifetime 3600
NXR_C(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_C(config-ipsec-tunnel)#match address ipsec_acl
NXR_C(config-ipsec-tunnel)#exit
NXR_C(config)#interface tunnel 1
NXR_C(config-tunnel)#tunnel mode ipsec ipv4
NXR_C(config-tunnel)#tunnel protection ipsec policy 1
NXR_C(config-tunnel)#ip tcp adjust-mss auto
NXR_C(config-tunnel)#exit
NXR_C(config)#interface ppp 0
NXR_C(config-ppp)#ip address negotiated
NXR_C(config-ppp)#ip masquerade
NXR_C(config-ppp)#ip access-group in ppp0_in
NXR_C(config-ppp)#ip spi-filter
NXR_C(config-ppp)#ip tcp adjust-mss auto
NXR_C(config-ppp)#no ip redirects
NXR_C(config-ppp)#ppp username test3@example.jp password test3pass
NXR_C(config-ppp)#ipsec policy 1
NXR_C(config-ppp)#exit
NXR_C(config)#interface ethernet 1
NXR_C(config-if)#no ip address
NXR_C(config-if)#pppoe-client ppp 0
NXR_C(config-if)#exit
NXR_C(config)#dns
NXR_C(config-dns)#service enable
NXR_C(config-dns)#exit
NXR_C(config)#fast-forwarding enable
NXR_C(config)#exit
NXR_C#save config
```

【 設定例解説 】

〔NXR_A の設定〕

(☞) NXR_A の設定は 2-5. PPPoE を利用した IPsec 接続設定例の〔NXR_A の設定〕と同一となりますので、そちらをご参照下さい。

〔NXR_B の設定〕

(☞) ここに記載のない設定項目は 2-5. PPPoE を利用した IPsec 接続設定例の〔NXR_B の設定〕が参考になりますので、そちらをご参照下さい。

1. <スタティックルート設定>

```
NXR_B(config)#ip route 192.168.0.0/16 tunnel 1 1
```

192.168.0.0/16 のルートを設定します。なおゲートウェイインタフェースは tunnel 1 を設定します。またこのルートのディスタンス値として 1 を設定します。これにより設定例内の各拠点のネットワークアドレスを包括する 192.168.0.0/16 を宛先 IP アドレスで指定することにより、LAN_A,LAN_C 内の IP アドレスを

送信元とするパケットを各拠点に転送することができます。

```
NXR_B(config)#ip route 192.168.0.0/16 null 254
```

192.168.0.0/16 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

〔NXR_C の設定〕

(☞) ここに記載のない設定項目は 2-5. PPPoE を利用した IPsec 接続設定例の〔NXR_C の設定〕が参考になりますので、そちらをご参照下さい。

1. <スタティックルート設定>

```
NXR_C(config)#ip route 192.168.0.0/16 tunnel 1 1
```

192.168.0.0/16 のルートを設定します。なおゲートウェイインタフェースは tunnel 1 を設定します。またこのルートのディスタンス値として 1 を設定します。これにより設定例内の各拠点のネットワークアドレスを包括する 192.168.0.0/16 を宛先 IP アドレスで指定することにより、LAN_A,LAN_B 内の IP アドレスを送信元とするパケットを各拠点に転送することができます。

```
NXR_C(config)#ip route 192.168.0.0/16 null 254
```

192.168.0.0/16 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

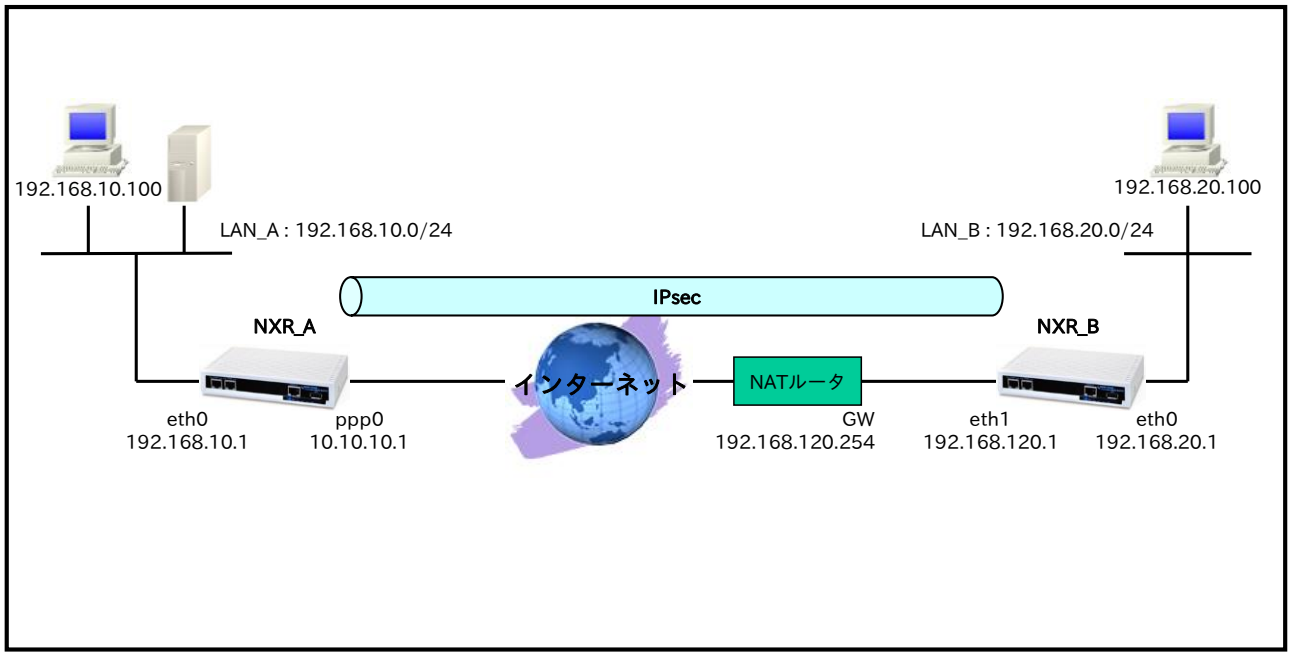
【 パソコンの設定例 】

	LAN A のパソコン	LAN B のパソコン	LAN C のパソコン
IP アドレス	192.168.10.100	192.168.20.100	192.168.30.100
サブネットマスク	255.255.255.0	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1	192.168.30.1
DNS サーバ	192.168.10.1	192.168.20.1	192.168.30.1

2-7. IPsec NAT トラバーサル接続設定例

NXR がプライベートネットワーク内にあるなどグローバル IP アドレスを保持できないような環境で、同一拠点にグローバル IP アドレスを保持している NAPT ルータがある場合、このルータを経由して NXR では NAT トラバーサルという方法で IPsec を利用できます。

【 構成図 】



- Route Based IPsec は Policy Based IPsec での設定に対し以下の設定を追加する必要があります。
  - ・トンネルインタフェース設定
  - ・ルート設定(スタティックルート設定,RIPv1/v2,OSPF,BGP)
- 1-7. IPsec NAT トラバーサル接続設定例の内容も参考になりますのでご参照下さい。
- 各拠点からのインターネットアクセスを可能にするために NAT 設定(IP マスカレード)やフィルタ設定(SPI)および DNS 設定を行っています

【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1 1
NXR_A(config)#ip route 192.168.20.0/24 null 254
NXR_A(config)#ip route 0.0.0.0/0 ppp 0
NXR_A(config)#ip access-list ppp0_in permit any 10.10.10.1 udp any 500
NXR_A(config)#ip access-list ppp0_in permit any 10.10.10.1 udp any 4500
NXR_A(config)#ipsec access-list ipsec_acl ip any any
NXR_A(config)#ipsec nat-traversal enable
% restart ipsec service to take affect.
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A(config-ipsec-isakmp)#remote address ip any
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrb
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address ipsec_acl
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
NXR_A(config-tunnel)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#interface ppp 0
NXR_A(config-ppp)#ip address 10.10.10.1/32
NXR_A(config-ppp)#ip masquerade
NXR_A(config-ppp)#ip access-group in ppp0_in
NXR_A(config-ppp)#ip spi-filter
NXR_A(config-ppp)#ip tcp adjust-mss auto
NXR_A(config-ppp)#no ip redirects
NXR_A(config-ppp)#ppp username test1@example.jp password test1pass
NXR_A(config-ppp)#ipsec policy 1
NXR_A(config-ppp)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#no ip address
NXR_A(config-if)#pppoe-client ppp 0
NXR_A(config-if)#exit
NXR_A(config)#dns
NXR_A(config-dns)#service enable
```

```
NXR_A(config-dns)#exit
NXR_A(config)#fast-forwarding enable
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1 1
NXR_B(config)#ip route 192.168.10.0/24 null 254
NXR_B(config)#ip route 0.0.0.0/0 192.168.120.254
NXR_B(config)#ipsec access-list ipsec_acl ip any any
NXR_B(config)#ipsec nat-traversal enable
% restart ipsec service to take affect.
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
NXR_B(config-tunnel)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address 192.168.120.1/24
NXR_B(config-if)#ipsec policy 1
NXR_B(config-if)#exit
NXR_B(config)#dns
NXR_B(config-dns)#service enable
NXR_B(config-dns)#address 192.168.120.254
NXR_B(config-dns)#exit
NXR_B(config)#fast-forwarding enable
NXR_B(config)#exit
NXR_B#save config
```

【 設定例解説 】

〔NXR_A の設定〕

(☞) ここに記載のない設定項目は 1-7. IPsec NAT トラバーサル接続設定例の〔NXR_A の設定〕が参考になりますので、そちらをご参照下さい。

1. <スタティックルート設定>

```
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1 1
```

LAN_B 向け 192.168.20.0/24 のルートを設定します。なおゲートウェイインタフェースは tunnel 1 を設定します。またこのルートのディスタンス値として 1 を設定します。

(☞) これは IPsec で使用するスタティックルートであり、ここで設定した宛先 IP アドレスにマッチしたパケットが IPsec のカプセル化対象となります。なおゲートウェイアドレスは IPsec で使用するトンネルインタフェースを設定します。

```
NXR_A(config)#ip route 192.168.20.0/24 null 254
```

LAN_B 向け 192.168.20.0/24 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

(☞) null インタフェースを出力インタフェースとして設定した場合、パケットが出力されることはありません(ドロップされます)。よってパケット出力を行う場合は null インタフェースよりもディスタンス値が小さいルートを設定する必要があります。

2. <IPsec アクセスリスト設定>

```
NXR_A(config)#ipsec access-list ipsec_acl ip any any
```

IPsec アクセスリスト名を ipsec_acl とし、送信元 IP アドレス,宛先 IP アドレスに any を設定します。
Policy Based IPsec では IPsec アクセスリストで設定したルールに基づき IPsec で ESP 化するかどうかが決定されましたが、Route Based IPsec では IPsec アクセスリストは IKE フェーズ 2 の ID としてのみ使用します。

(☞) Route Based IPsec で ESP 化するか否かは IPsec アクセスリストではなくトンネルインタフェースをゲートウェイとするルート設定の有無で決まります。

3. <IPsec トンネルポリシー設定>

```
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
```

NXR_B との IPsec 接続で使用するトンネルポリシー1 を設定します。IPsec トンネルポリシー1 の説明として NXR_B、ネゴシエーションモードとして responder を設定します。

```
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address ipsec_acl
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

4. <トンネルインタフェース設定>

```
NXR_A(config)#interface tunnel 1
```

トンネル 1 インタフェースを設定します。

```
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
```

トンネルインタフェースで使用するトンネルモードを設定します。

トンネルインタフェースを Route Based IPsec で使用する場合は ipsec ipv4 と設定します。

```
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
```

使用する IPsec トンネルポリシーを設定します。

ここでは IPsec トンネルポリシー1 と関連づけを行います。

(☞) IPsec ローカルポリシーではありませんのでご注意下さい。

```
NXR_A(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

〔NXR_B の設定〕

(☞) ここに記載のない設定項目は 1-7. IPsec NAT トラバーサル接続設定例の〔NXR_B の設定〕が参考になりますので、そちらをご参照下さい。

1. <スタティックルート設定>

```
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1 1
```

LAN_A 向け 192.168.10.0/24 のルートを設定します。なおゲートウェイインタフェースは tunnel 1 を設定します。またこのルートのディスタンス値として 1 を設定します。

```
NXR_B(config)#ip route 192.168.10.0/24 null 254
```

LAN_A 向け 192.168.10.0/24 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

2. <IPsec アクセスリスト設定>

```
NXR_B(config)#ipsec access-list ipsec_acl ip any any
```

IPsec アクセスリスト名を ipsec_acl とし、送信元 IP アドレス,宛先 IP アドレスに any を設定します。

3. <IPsec トンネルポリシー設定>

```
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
```

NXR_A との IPsec 接続で使用するトンネルポリシー1 を設定します。

IPsec トンネルポリシー1 の説明として NXR_A、ネゴシエーションモードとして auto を設定します。

```
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

4. <トンネルインタフェース設定>

```
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
```

トンネル 1 インタフェースでトンネルモードを ipsec ipv4、使用するトンネルポリシーとして 1 を設定します。また TCP MSS の調整機能をオートに設定します。

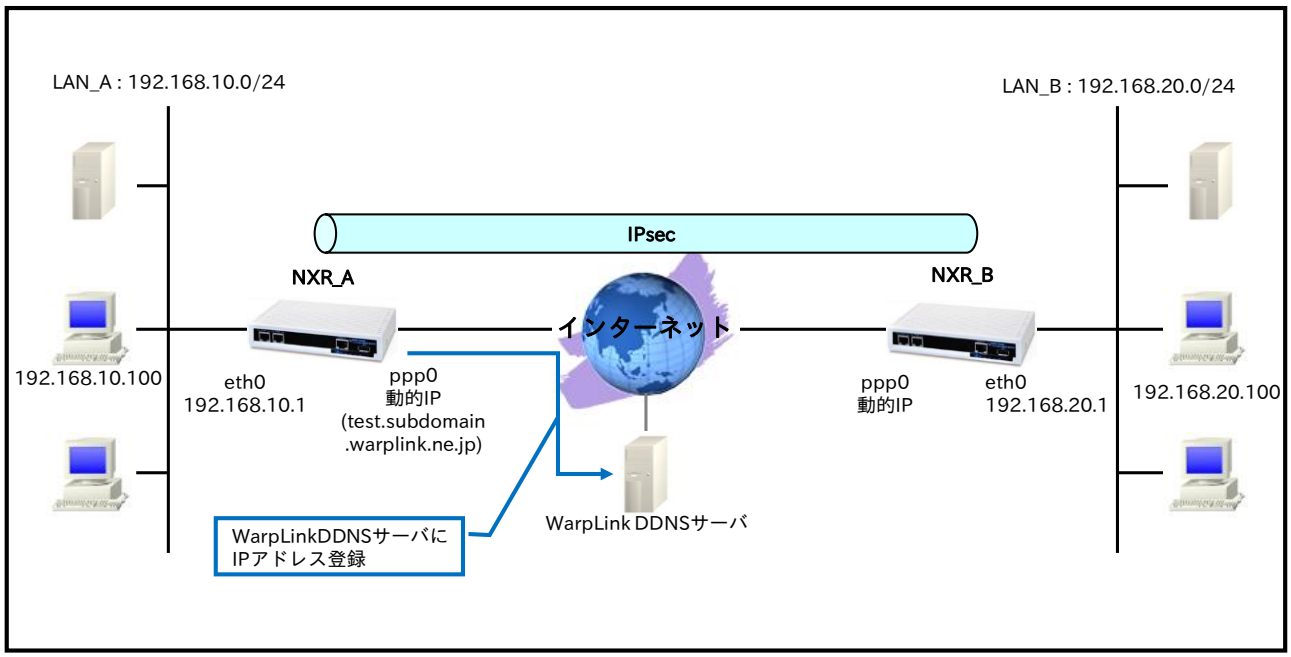
【 パソコンの設定例 】

	LAN A のパソコン	LAN B のパソコン
IP アドレス	192.168.10.100	192.168.20.100
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1
DNS サーバ	192.168.10.1	192.168.20.1

2-8. FQDN での IPsec 接続設定例

この設定例では、ダイナミック DNS を利用してアドレス不定の NXR 同士で IPsec 接続による通信を行います。ダイナミック DNS を利用することで NXR の WAN 側 IP アドレスが不定のみの環境でも IPsec による VPN を利用できます。
ここではダイナミック DNS サービスに弊社が提供している WarpLinkDDNS サービスを使用します。

【 構成図 】



- NXR で WarpLink 機能を設定し WarpLinkDDNS サービスを動作させます。
  (☞) WarpLinkDDNS サービスは弊社が提供している有償の DDNS サービスとなります。
  詳細は下記 URL からご確認下さい。
  http://www.warplink.ne.jp/ddns/index.html
- NXR_A は自身の IP アドレスを WarpLinkDDNS サーバに登録します。NXR_B は WarpLinkDDNS サーバに登録されている NXR_A の FQDN を設定します。そして FQDN の名前解決後 IPsec 接続を開始します。
  (☞) 設定した FQDN の名前解決後に IPsec 接続を開始します。よって名前解決ができない場合 IPsec 接続を開始することができませんのでご注意ください。
  なお両拠点ルータで WarpLinkDDNS サービスを動作させることで両拠点ルータから IPsec 接続を開始することが可能になり、片側で WarpLinkDDNS サービスを動作させる場合に比べ再接続性の向上が期待できます。
- 1-8. FQDN での IPsec 接続設定例の内容も参考になりますのでご参照下さい。

【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1 1
NXR_A(config)#ip route 192.168.20.0/24 null 254
NXR_A(config)#ip route 0.0.0.0/0 ppp 0
NXR_A(config)#ip access-list ppp0_in permit any any udp 500 500
NXR_A(config)#ip access-list ppp0_in permit any any 50
NXR_A(config)#ipsec access-list ipsec_acl ip any any
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A(config-ipsec-isakmp)#remote address ip any
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrb
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address ipsec_acl
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
NXR_A(config-tunnel)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#interface ppp 0
NXR_A(config-ppp)#ip address negotiated
NXR_A(config-ppp)#ip masquerade
NXR_A(config-ppp)#ip access-group in ppp0_in
NXR_A(config-ppp)#ip spi-filter
NXR_A(config-ppp)#ip tcp adjust-mss auto
NXR_A(config-ppp)#no ip redirects
NXR_A(config-ppp)#ppp username test1@example.jp password test1pass
NXR_A(config-ppp)#ipsec policy 1
NXR_A(config-ppp)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#no ip address
NXR_A(config-if)#pppoe-client ppp 0
NXR_A(config-if)#exit
NXR_A(config)#warplink
NXR_A(config-warplink)#service enable
NXR_A(config-warplink)#account username warplinksample password warplinksamplepass
NXR_A(config-warplink)#exit
```

```
NXR_A(config)#dns
NXR_A(config-dns)#service enable
NXR_A(config-dns)#exit
NXR_A(config)#fast-forwarding enable
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1 1
NXR_B(config)#ip route 192.168.10.0/24 null 254
NXR_B(config)#ip route 0.0.0.0/0 ppp 0
NXR_B(config)#ip access-list ppp0_in permit any any udp 500 500
NXR_B(config)#ip access-list ppp0_in permit any any 50
NXR_B(config)#ipsec access-list ipsec_acl ip any any
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_B(config-ipsec-isakmp)#remote address ip test.subdomain.warplink.ne.jp
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
NXR_B(config-tunnel)#exit
NXR_B(config)#interface ppp 0
NXR_B(config-ppp)#ip address negotiated
NXR_B(config-ppp)#ip masquerade
NXR_B(config-ppp)#ip access-group in ppp0_in
NXR_B(config-ppp)#ip spi-filter
NXR_B(config-ppp)#ip tcp adjust-mss auto
NXR_B(config-ppp)#no ip redirects
NXR_B(config-ppp)#ppp username test2@example.jp password test2pass
NXR_B(config-ppp)#ipsec policy 1
NXR_B(config-ppp)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#no ip address
```

```
NXR_B(config-if)#pppoe-client ppp 0
NXR_B(config-if)#exit
NXR_B(config)#dns
NXR_B(config-dns)#service enable
NXR_B(config-dns)#exit
NXR_B(config)#fast-forwarding enable
NXR_B(config)#exit
NXR_B#save config
```

【 設定例解説 】

〔NXR_A の設定〕

(☞) ここに記載のない設定項目は 1-8. FQDN での IPsec 接続設定例の〔NXR_A の設定〕が参考になりますので、そちらをご参照下さい。

1. <スタティックルート設定>

```
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1 1
```

LAN_B 向け 192.168.20.0/24 のルートを設定します。なおゲートウェイインタフェースは tunnel 1 を設定します。またこのルートのディスタンス値として 1 を設定します。

(☞) これは IPsec で使用するスタティックルートであり、ここで設定した宛先 IP アドレスにマッチしたパケットが IPsec のカプセル化対象となります。なおゲートウェイアドレスは IPsec で使用するトンネルインタフェースを設定します。

```
NXR_A(config)#ip route 192.168.20.0/24 null 254
```

LAN_B 向け 192.168.20.0/24 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

(☞) null インタフェースを出力インタフェースとして設定した場合、パケットが出力されることはありません(ドロップされます)。よってパケット出力を行う場合は null インタフェースよりもディスタンス値が小さいルートを設定する必要があります。

2. <IPsec アクセスリスト設定>

```
NXR_A(config)#ipsec access-list ipsec_acl ip any any
```

IPsec アクセスリスト名を ipsec_acl とし、送信元 IP アドレス,宛先 IP アドレスに any を設定します。
Policy Based IPsec では IPsec アクセスリストで設定したルールに基づき IPsec で ESP 化するかどうかが決定されましたが、Route Based IPsec では IPsec アクセスリストは IKE フェーズ 2 の ID としてのみ使用します。

(☞) Route Based IPsec で ESP 化するか否かは IPsec アクセスリストではなくトンネルインタフェースをゲートウェイとするルート設定の有無で決まります。

3. <IPsec トンネルポリシー設定>

```
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
```

NXR_B との IPsec 接続で使用するトンネルポリシー1 を設定します。IPsec トンネルポリシー1 の説明と

して NXR_B、ネゴシエーションモードとして responder を設定します。

```
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address ipsec_acl
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

4. <トンネルインタフェース設定>

```
NXR_A(config)#interface tunnel 1
```

トンネル 1 インタフェースを設定します。

```
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
```

トンネルインタフェースで使用するトンネルモードを設定します。

トンネルインタフェースを Route Based IPsec で使用する場合は ipsec ipv4 と設定します。

```
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
```

使用する IPsec トンネルポリシーを設定します。

ここでは IPsec トンネルポリシー1 と関連づけを行います。

(☞) IPsec ローカルポリシーではありませんのでご注意下さい。

```
NXR_A(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

〔NXR_B の設定〕

(☞) ここに記載のない設定項目は 1-8. FQDN での IPsec 接続設定例の

〔NXR_B の設定〕が参考になりますので、そちらをご参照下さい。

1. <スタティックルート設定>

```
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1 1
```

LAN_A 向け 192.168.10.0/24 のルートを設定します。なおゲートウェイインタフェースは tunnel 1 を設定します。またこのルートのディスタンス値として 1 を設定します。

```
NXR_B(config)#ip route 192.168.10.0/24 null 254
```

LAN_A 向け 192.168.10.0/24 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

2. <IPsec アクセスリスト設定>

```
NXR_B(config)#ipsec access-list ipsec_acl ip any any
```

IPsec アクセスリスト名を ipsec_acl とし、送信元 IP アドレス,宛先 IP アドレスに any を設定します。

3. <IPsec トンネルポリシー設定>

```
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
```

NXR_A との IPsec 接続で使用するトンネルポリシー1 を設定します。

IPsec トンネルポリシー1 の説明として NXR_A、ネゴシエーションモードとして auto を設定します。

```
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

4. ＜トンネルインタフェース設定＞

```
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
```

トンネル 1 インタフェースでトンネルモードを ipsec ipv4、使用するトンネルポリシーとして 1 を設定します。また TCP MSS の調整機能をオートに設定します。

【 パソコンの設定例 】

	LAN A のパソコン	LAN B のパソコン
IP アドレス	192.168.10.100	192.168.20.100

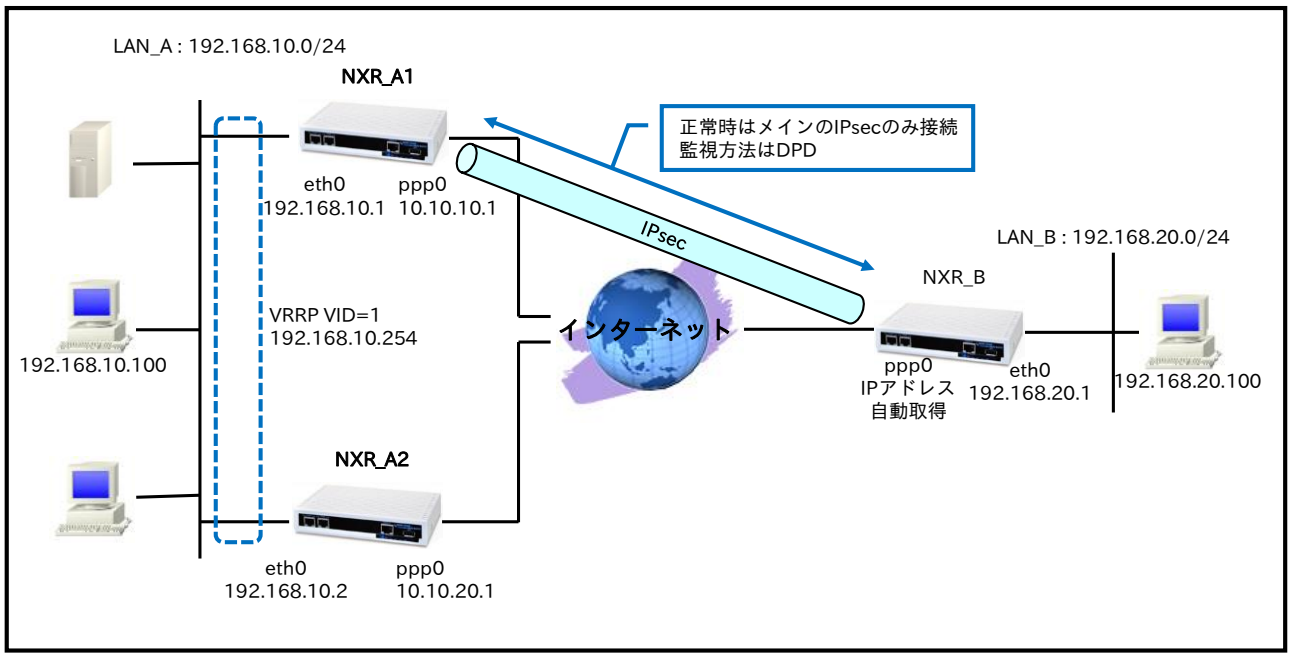
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1
DNS サーバ	192.168.10.1	192.168.20.1

2-9. 冗長化設定 1 (backup policy の利用)

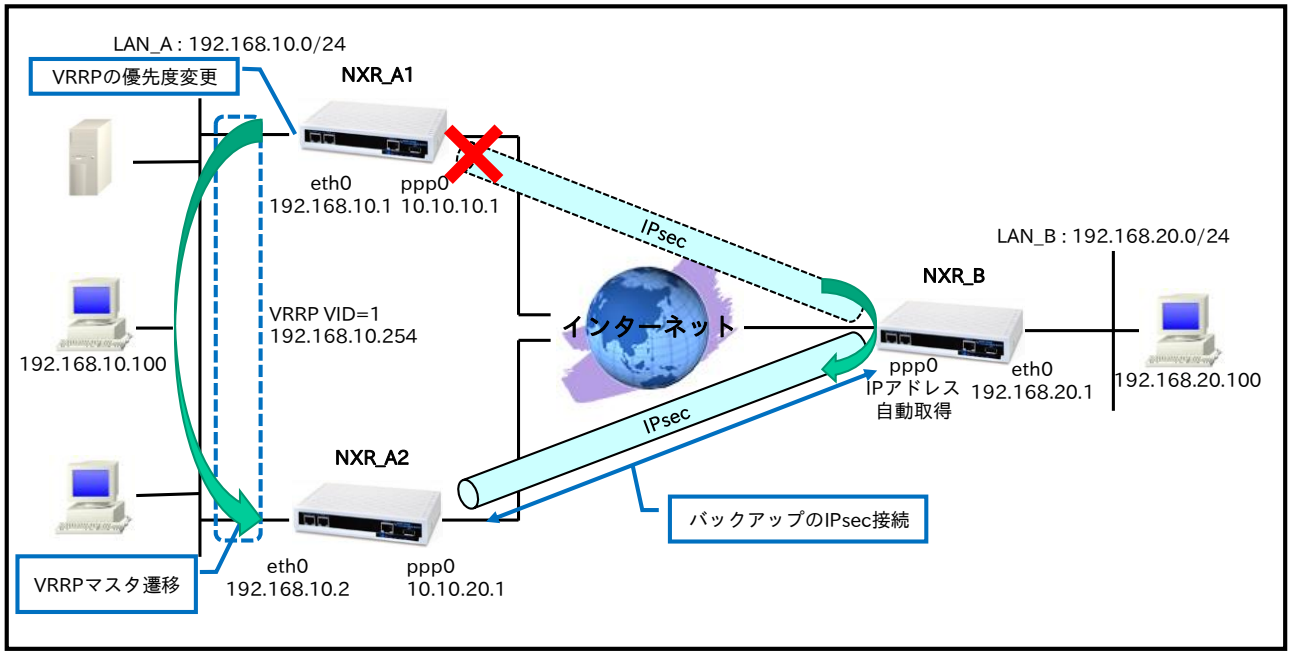
センタ側で回線と機器の冗長化を行う設定例です。
正常時 NXR_A1⇔NXR_B 間で IPsec トンネル経由で通信を行い、センタ側での障害検出時 NXR_A2⇔NXR_B 間の通信に切り替えます。

【 構成図 】

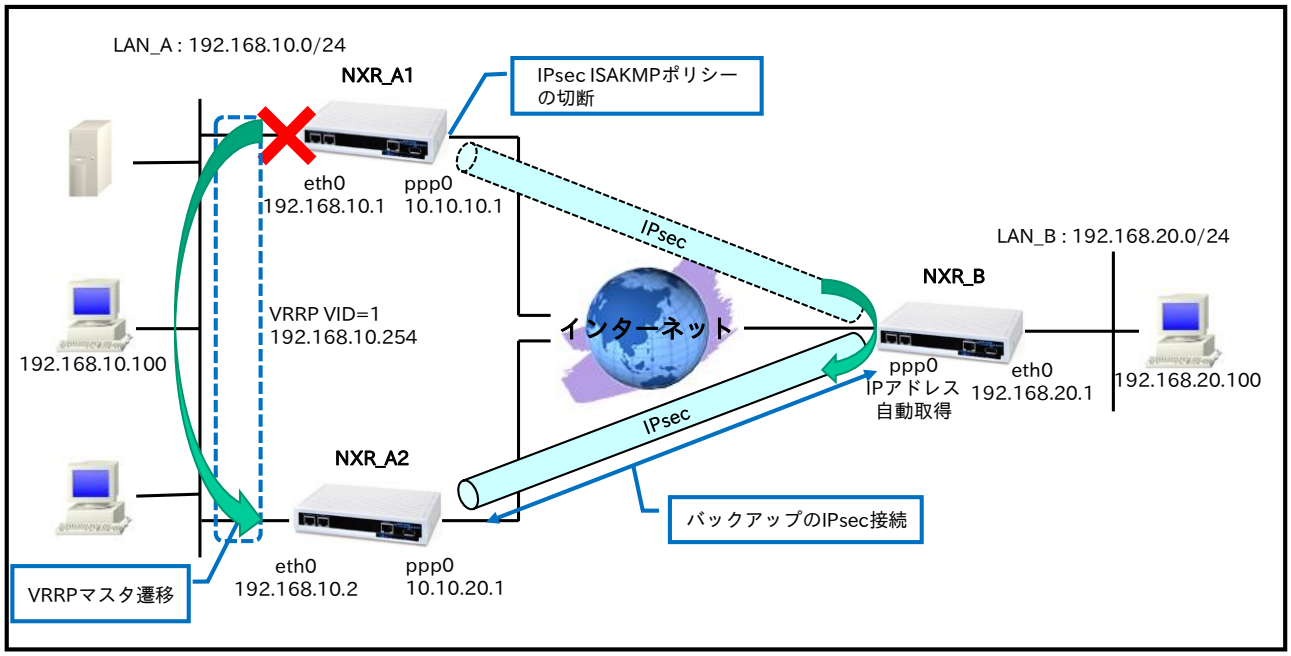
<正常時>



<NXR_A1 ppp0 インタフェースリンクダウン時>



<NXR_A1 ethernet0 インタフェースリンクダウン時>



- NXR_A1,A2 では以下の条件で VRRP を動作させます。

	NXR_A1	NXR_A2
グループ ID	1	
IP アドレス	192.168.10.254	
プライオリティ	254	100
プリエンプト	有効	
アドバタイズ間隔	5	
ネットワークイベントによる障害検知後のプライオリティ	50	−

- NXR_A2,B では IPsec ルート無効時に、カプセル化対象のパケットをルータから出力しないようにするためゲートウェイを null インタフェースとしたルートを設定します。
- NXR_A1 では ppp0 インタフェースリンクダウンによる WAN 側障害検知時に、ネットワークイベントにて VRRP の優先度を変更します。また ethernet0 インタフェースリンクダウンに LAN 側障害検知時に、ネットワークイベントにて IPsecISAKMP ポリシーの切断を行います。そして WAN 側での経路障害など IPsec 未確立時に LAN_B 宛のパケットを NXR_A2 に転送するためのルートを設定します。なおその際ルートのディスタンス値は IPsec ルートよりも大きい値を設定します。
- NXR_B では DPD で監視を行い NXR_A1 との IPsec 未確立時に NXR_A2 に対して IPsec のネゴシエーションを行います。

(☞) 本設定例では backup policy 機能により、冗長化を実現します。

【 設定例 】

〔NXR_A1 の設定〕

```
nxr125#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr125(config)#hostname NXR_A1
NXR_A1(config)#track 1 interface ppp 0 initial-timeout 30
NXR_A1(config)#track 2 interface ethernet 0
NXR_A1(config)#interface ethernet 0
NXR_A1(config-if)#ip address 192.168.10.1/24
NXR_A1(config-if)#no ip redirects
NXR_A1(config-if)#vrrp ip 1 address 192.168.10.254
NXR_A1(config-if)#vrrp ip 1 priority 254
NXR_A1(config-if)#vrrp ip 1 preempt
NXR_A1(config-if)#vrrp ip 1 timers advertise 5
NXR_A1(config-if)#vrrp ip 1 netevent 1 priority 50
NXR_A1(config-if)#exit
NXR_A1(config)#ip route 192.168.20.0/24 tunnel 1 1
NXR_A1(config)#ip route 192.168.20.0/24 192.168.10.2 10
NXR_A1(config)#ip route 0.0.0.0/0 ppp 0
NXR_A1(config)#ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
NXR_A1(config)#ip access-list ppp0_in permit any 10.10.10.1 50
NXR_A1(config)#ipsec access-list ipsec_acl ip any any
NXR_A1(config)#ipsec local policy 1
NXR_A1(config-ipsec-local)#address ip
NXR_A1(config-ipsec-local)#exit
NXR_A1(config)#ipsec isakmp policy 1
NXR_A1(config-ipsec-isakmp)#description NXR_B
NXR_A1(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR_A1(config-ipsec-isakmp)#hash sha1
NXR_A1(config-ipsec-isakmp)#encryption aes128
NXR_A1(config-ipsec-isakmp)#group 5
NXR_A1(config-ipsec-isakmp)#lifetime 10800
NXR_A1(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A1(config-ipsec-isakmp)#remote address ip any
NXR_A1(config-ipsec-isakmp)#remote identity fqdn nxrb
NXR_A1(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A1(config-ipsec-isakmp)#local policy 1
NXR_A1(config-ipsec-isakmp)#netevent 2 disconnect
NXR_A1(config-ipsec-isakmp)#exit
NXR_A1(config)#ipsec tunnel policy 1
NXR_A1(config-ipsec-tunnel)#description NXR_B
NXR_A1(config-ipsec-tunnel)#negotiation-mode responder
NXR_A1(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A1(config-ipsec-tunnel)#set pfs group5
NXR_A1(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A1(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A1(config-ipsec-tunnel)#match address ipsec_acl
NXR_A1(config-ipsec-tunnel)#exit
NXR_A1(config)#interface tunnel 1
NXR_A1(config-tunnel)#tunnel mode ipsec ipv4
NXR_A1(config-tunnel)#tunnel protection ipsec policy 1
NXR_A1(config-tunnel)#ip tcp adjust-mss auto
NXR_A1(config-tunnel)#exit
NXR_A1(config)#interface ppp 0
NXR_A1(config-ppp)#ip address 10.10.10.1/32
NXR_A1(config-ppp)#ip masquerade
NXR_A1(config-ppp)#ip access-group in ppp0_in
NXR_A1(config-ppp)#ip spi-filter
NXR_A1(config-ppp)#ip tcp adjust-mss auto
NXR_A1(config-ppp)#no ip redirects
NXR_A1(config-ppp)#ppp username test1@example.jp password test1pass
NXR_A1(config-ppp)#ipsec policy 1
```

```
NXR_A1(config-ppp)#exit
NXR_A1(config)#interface ethernet 1
NXR_A1(config-if)#no ip address
NXR_A1(config-if)#pppoe-client ppp 0
NXR_A1(config-if)#exit
NXR_A1(config)#dns
NXR_A1(config-dns)#service enable
NXR_A1(config-dns)#exit
NXR_A1(config)#fast-forwarding enable
NXR_A1(config)#exit
NXR_A1#save config
```

〔NXR_A2 の設定〕

```
nxr125#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr125(config)#hostname NXR_A2
NXR_A2(config)#interface ethernet 0
NXR_A2(config-if)#ip address 192.168.10.2/24
NXR_A2(config-if)#no ip redirects
NXR_A2(config-if)#vrrp ip 1 address 192.168.10.254
NXR_A2(config-if)#vrrp ip 1 priority 100
NXR_A2(config-if)#vrrp ip 1 preempt
NXR_A2(config-if)#vrrp ip 1 timers advertise 5
NXR_A2(config-if)#exit
NXR_A2(config)#ip route 192.168.20.0/24 tunnel 1 1
NXR_A2(config)#ip route 192.168.20.0/24 null 254
NXR_A2(config)#ip route 0.0.0.0/0 ppp 0
NXR_A2(config)#ip access-list ppp0_in permit any 10.10.20.1 udp 500 500
NXR_A2(config)#ip access-list ppp0_in permit any 10.10.20.1 50
NXR_A2(config)#ipsec access-list ipsec_acl ip any any
NXR_A2(config)#ipsec local policy 1
NXR_A2(config-ipsec-local)#address ip
NXR_A2(config-ipsec-local)#exit
NXR_A2(config)#ipsec isakmp policy 1
NXR_A2(config-ipsec-isakmp)#description NXR_B
NXR_A2(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR_A2(config-ipsec-isakmp)#hash sha1
NXR_A2(config-ipsec-isakmp)#encryption aes128
NXR_A2(config-ipsec-isakmp)#group 5
NXR_A2(config-ipsec-isakmp)#lifetime 10800
NXR_A2(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A2(config-ipsec-isakmp)#remote address ip any
NXR_A2(config-ipsec-isakmp)#remote identity fqdn nxrb
NXR_A2(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A2(config-ipsec-isakmp)#local policy 1
NXR_A2(config-ipsec-isakmp)#exit
NXR_A2(config)#ipsec tunnel policy 1
NXR_A2(config-ipsec-tunnel)#description NXR_B
NXR_A2(config-ipsec-tunnel)#negotiation-mode responder
NXR_A2(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A2(config-ipsec-tunnel)#set pfs group5
NXR_A2(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A2(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A2(config-ipsec-tunnel)#match address ipsec_acl
NXR_A2(config-ipsec-tunnel)#exit
NXR_A2(config)#interface tunnel 1
NXR_A2(config-tunnel)#tunnel mode ipsec ipv4
NXR_A2(config-tunnel)#tunnel protection ipsec policy 1
NXR_A2(config-tunnel)#ip tcp adjust-mss auto
NXR_A2(config-tunnel)#exit
NXR_A2(config)#interface ppp 0
NXR_A2(config-ppp)#ip address 10.10.20.1/32
```

```
NXR_A2(config-ppp)#ip masquerade
NXR_A2(config-ppp)#ip access-group in ppp0_in
NXR_A2(config-ppp)#ip spi-filter
NXR_A2(config-ppp)#ip tcp adjust-mss auto
NXR_A2(config-ppp)#no ip redirects
NXR_A2(config-ppp)#ppp username test2@example.jp password test2pass
NXR_A2(config-ppp)#ipsec policy 1
NXR_A2(config-ppp)#exit
NXR_A2(config)#interface ethernet 1
NXR_A2(config-if)#no ip address
NXR_A2(config-if)#pppoe-client ppp 0
NXR_A2(config-if)#exit
NXR_A2(config)#dns
NXR_A2(config-dns)#service enable
NXR_A2(config-dns)#exit
NXR_A2(config)#fast-forwarding enable
NXR_A2(config)#exit
NXR_A2#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1 1
NXR_B(config)#ip route 192.168.10.0/24 tunnel 2 10
NXR_B(config)#ip route 192.168.10.0/24 null 254
NXR_B(config)#ip route 0.0.0.0/0 ppp 0
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 any 50
NXR_B(config)#ip access-list ppp0_in permit 10.10.20.1 any udp 500 500
NXR_B(config)#ip access-list ppp0_in permit 10.10.20.1 any 50
NXR_B(config)#ipsec access-list ipsec_acl ip any any
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A1
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#backup policy 2
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A1
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
NXR_B(config-ipsec-tunnel)#set priority 1
NXR_B(config-ipsec-tunnel)#exit
```

```
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
NXR_B(config-tunnel)#exit
NXR_B(config)#ipsec isakmp policy 2
NXR_B(config-ipsec-isakmp)#description NXR_A2
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.20.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 2
NXR_B(config-ipsec-tunnel)#description NXR_A2
NXR_B(config-ipsec-tunnel)#negotiation-mode manual
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 2
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
NXR_B(config-ipsec-tunnel)#set priority 10
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface tunnel 2
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 2
NXR_B(config-tunnel)#ip tcp adjust-mss auto
NXR_B(config-tunnel)#exit
NXR_B(config)#interface ppp 0
NXR_B(config-ppp)#ip address negotiated
NXR_B(config-ppp)#ip masquerade
NXR_B(config-ppp)#ip access-group in ppp0_in
NXR_B(config-ppp)#ip spi-filter
NXR_B(config-ppp)#ip tcp adjust-mss auto
NXR_B(config-ppp)#no ip redirects
NXR_B(config-ppp)#ppp username test3@example.jp password test3pass
NXR_B(config-ppp)#ipsec policy 1
NXR_B(config-ppp)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#no ip address
NXR_B(config-if)#pppoe-client ppp 0
NXR_B(config-if)#exit
NXR_B(config)#dns
NXR_B(config-dns)#service enable
NXR_B(config-dns)#exit
NXR_B(config)#fast-forwarding enable
NXR_B(config)#exit
NXR_B#save config
```

【 設定例解説 】

〔NXR_A1 の設定〕

(☞) ここに記載のない設定項目は 1-9. 冗長化設定の〔NXR_A1 の設定〕が参考になりますので、そちらをご参照下さい。

1. <スタティックルート設定>

```
NXR_A1(config)#ip route 192.168.20.0/24 tunnel 1 1
```

LAN_B 向け 192.168.20.0/24 のルートを設定します。なおゲートウェイインタフェースは tunnel 1 を設定します。またこのルートのディスタンス値として 1 を設定します。

(☞) これは IPsec で使用するスタティックルートであり、ここで設定した宛先 IP アドレスにマッチしたパケットが IPsec のカプセル化対象となります。なおゲートウェイアドレスは IPsec で使用するトンネルインタフェースを設定します。

2. <IPsec アクセスリスト設定>

```
NXR_A1(config)#ipsec access-list ipsec_acl ip any any
```

IPsec アクセスリスト名を ipsec_acl とし、送信元 IP アドレス,宛先 IP アドレスに any を設定します。Policy Based IPsec では IPsec アクセスリストで設定したルールに基づき IPsec で ESP 化するかどうかが決定されましたが、Route Based IPsec では IPsec アクセスリストは IKE フェーズ 2 の ID としてのみ使用します。

(☞) Route Based IPsec で ESP 化するか否かは IPsec アクセスリストではなくトンネルインタフェースをゲートウェイとするルート設定の有無で決まります。

3. <IPsec トンネルポリシー設定>

```
NXR_A1(config)#ipsec tunnel policy 1
NXR_A1(config-ipsec-tunnel)#description NXR_B
NXR_A1(config-ipsec-tunnel)#negotiation-mode responder
```

NXR_B との IPsec 接続で使用するトンネルポリシー1 を設定します。IPsec トンネルポリシー1 の説明として NXR_B、ネゴシエーションモードとして responder を設定します。

```
NXR_A1(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A1(config-ipsec-tunnel)#set pfs group5
NXR_A1(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_A1(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A1(config-ipsec-tunnel)#match address ipsec_acl
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

4. <トンネルインタフェース設定>

```
NXR_A1(config)#interface tunnel 1
```

トンネル 1 インタフェースを設定します。

```
NXR_A1(config-tunnel)#tunnel mode ipsec ipv4
```

トンネルインタフェースで使用するトンネルモードを設定します。

トンネルインタフェースを Route Based IPsec で使用する場合は ipsec ipv4 と設定します。

```
NXR_A1(config-tunnel)#tunnel protection ipsec policy 1
```

使用する IPsec トンネルポリシーを設定します。

ここでは IPsec トンネルポリシー1 と関連づけを行います。

(☞) IPsec ローカルポリシーではありませんのでご注意下さい。

```
NXR_A1(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

〔NXR_A2 の設定〕

(☞) ここに記載のない設定項目は 1-9. 冗長化設定の〔NXR_A2 の設定〕が参考になりますので、そちらをご参照下さい。

1. <スタティックルート設定>

```
NXR_A2(config)#ip route 192.168.20.0/24 tunnel 1 1
```

LAN_A 向け 192.168.10.0/24 のルートを設定します。なおゲートウェイインタフェースは tunnel 1 を設定します。またこのルートのディスタンス値として 1 を設定します。

```
NXR_A2(config)#ip route 192.168.20.0/24 null 254
```

LAN_A 向け 192.168.10.0/24 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

(☞) null インタフェースを出力インタフェースとして設定した場合、パケットが出力されることはありません(ドロップされます)。よってパケット出力を行う場合は null インタフェースよりもディスタンス値が小さいルートを設定する必要があります。

2. <IPsec アクセスリスト設定>

```
NXR_A2(config)#ipsec access-list ipsec_acl ip any any
```

IPsec アクセスリスト名を ipsec_acl とし、送信元 IP アドレス,宛先 IP アドレスに any を設定します。

3. <IPsec トンネルポリシー設定>

```
NXR_A2(config)#ipsec tunnel policy 1
NXR_A2(config-ipsec-tunnel)#description NXR_B
NXR_A2(config-ipsec-tunnel)#negotiation-mode responder
```

NXR_B との IPsec 接続で使用するトンネルポリシー1 を設定します。IPsec トンネルポリシー1 の説明として NXR_B、ネゴシエーションモードとして responder を設定します。

```
NXR_A2(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A2(config-ipsec-tunnel)#set pfs group5
NXR_A2(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_A2(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A2(config-ipsec-tunnel)#match address ipsec_acl
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

4. <トンネルインタフェース設定>

```
NXR_A2(config)#interface tunnel 1
NXR_A2(config-tunnel)#tunnel mode ipsec ipv4
NXR_A2(config-tunnel)#tunnel protection ipsec policy 1
NXR_A2(config-tunnel)#ip tcp adjust-mss auto
```

トンネル 1 インタフェースでトンネルモードを ipsec ipv4、使用するトンネルポリシーとして 1 を設定します。また TCP MSS の調整機能をオートに設定します。

〔NXR_B の設定〕

(☞) ここに記載のない設定項目は 1-9. 冗長化設定の〔NXR_B の設定〕が参考になりますので、そちらをご参照下さい。

1. <スタティックルート設定>

```
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1 1
NXR_B(config)#ip route 192.168.10.0/24 tunnel 2 10
```

一行目は LAN_B 向け 192.168.10.0/24 のルートを設定します。なおゲートウェイインタフェースは tunnel 1 を設定します。またこのルートのディスタンス値として 1 を設定します。
二行目は LAN_C 向け 192.168.10.0/24 のルートを設定します。なおゲートウェイインタフェースは tunnel 2 を設定します。またこのルートのディスタンス値として 10 を設定します。

```
NXR_B(config)#ip route 192.168.10.0/24 null 254
```

LAN_B 向け 192.168.10.0/24 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

2. <IPsec アクセスリスト設定>

```
NXR_B(config)#ipsec access-list ipsec_acl ip any any
```

IPsec アクセスリスト名を ipsec_acl とし、送信元 IP アドレス,宛先 IP アドレスに any を設定します。

3. <IPsec トンネルポリシー1 設定>

```
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A1
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
```

NXR_A1 との IPsec 接続で使用するトンネルポリシー1 を設定します。

IPsec トンネルポリシー1 の説明として NXR_A1、ネゴシエーションモードとして auto を設定します。

```
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

4. <トンネル 1 インタフェース設定>

```
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
```

トンネル 1 インタフェースでトンネルモードを ipsec ipv4、使用するトンネルポリシーとして 1 を設定します。また TCP MSS の調整機能をオートに設定します。

5. <IPsec トンネルポリシー2 設定>

```
NXR_B(config)#ipsec tunnel policy 2
NXR_B(config-ipsec-tunnel)#description NXR_A2
NXR_B(config-ipsec-tunnel)#negotiation-mode manual
```

NXR_A2 との IPsec 接続で使用するトンネルポリシー2 を設定します。

IPsec トンネルポリシー2 の説明として NXR_A2、ネゴシエーションモードとして manual を設定します。

```
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 2
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
NXR_B(config-ipsec-tunnel)#set priority 10
```

ISAKMP ポリシー2 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

またプライオリティを 10 に設定します。

6. <トンネル 2 インタフェース設定>

```
NXR_B(config)#interface tunnel 2
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 2
NXR_B(config-tunnel)#ip tcp adjust-mss auto
```

トンネル 2 インタフェースでトンネルモードを ipsec ipv4、使用するトンネルポリシーとして 2 を設定します。また TCP MSS の調整機能をオートに設定します。

【 パソコンの設定例 】

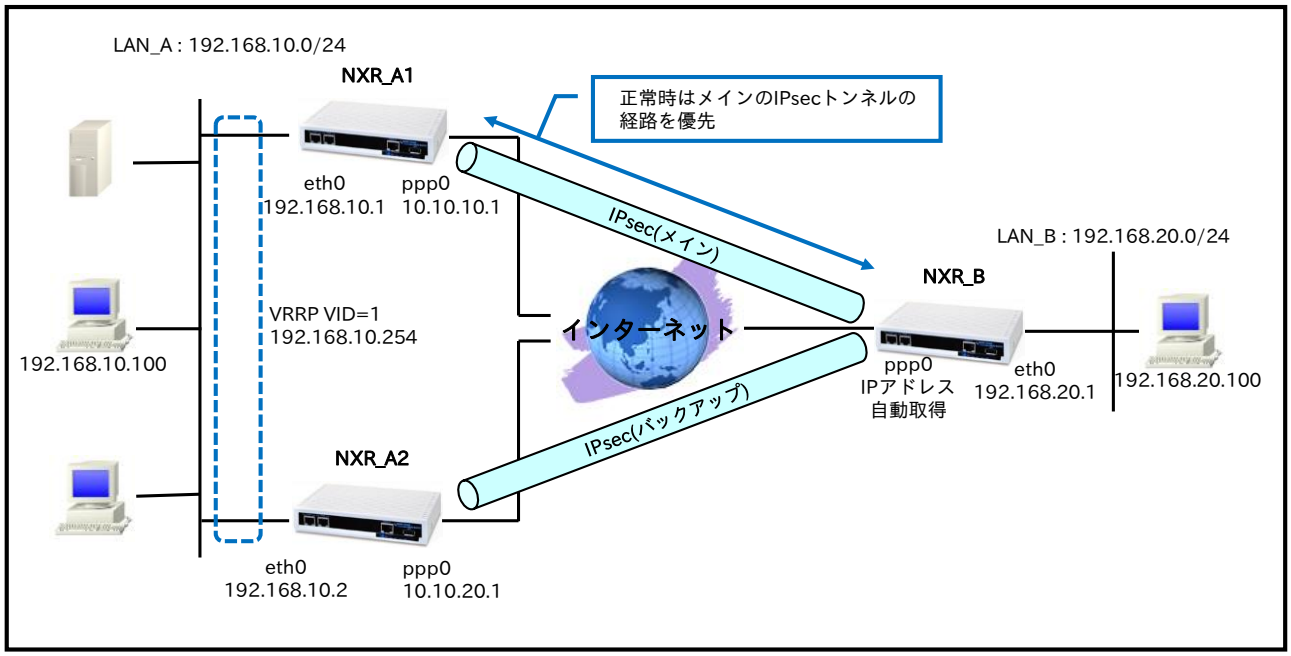
	LAN A のパソコン	LAN B のパソコン
IP アドレス	192.168.10.100	192.168.20.100
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.254	192.168.20.1
DNS サーバ	192.168.10.1	192.168.20.1
	192.168.10.2	

2-10. 冗長化設定 2 (IPsec 同時接続)

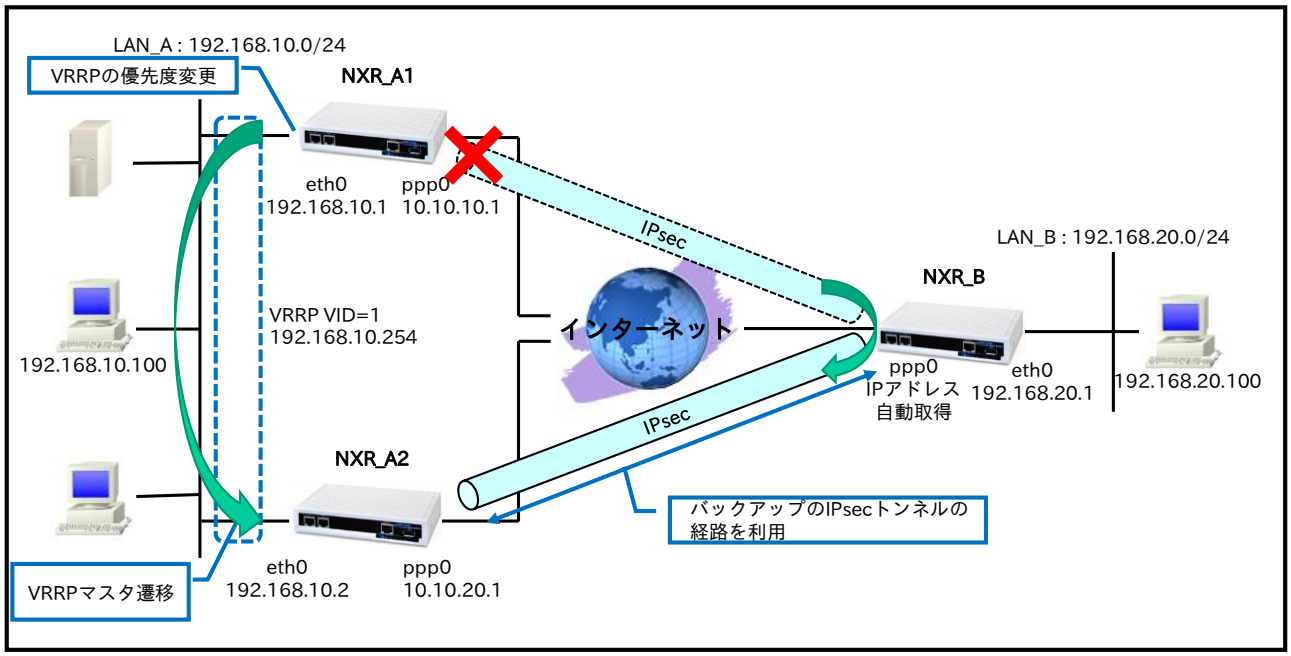
センタ側で回線と機器の冗長化を行う設定例です。2-9. 冗長化設定 1 (backup policy の利用)と異なり、NXR_B では NXR_A1,A2 と IPsecSA を確立しておき障害検出時ルートによる切り替えを行います。

【 構成図 】

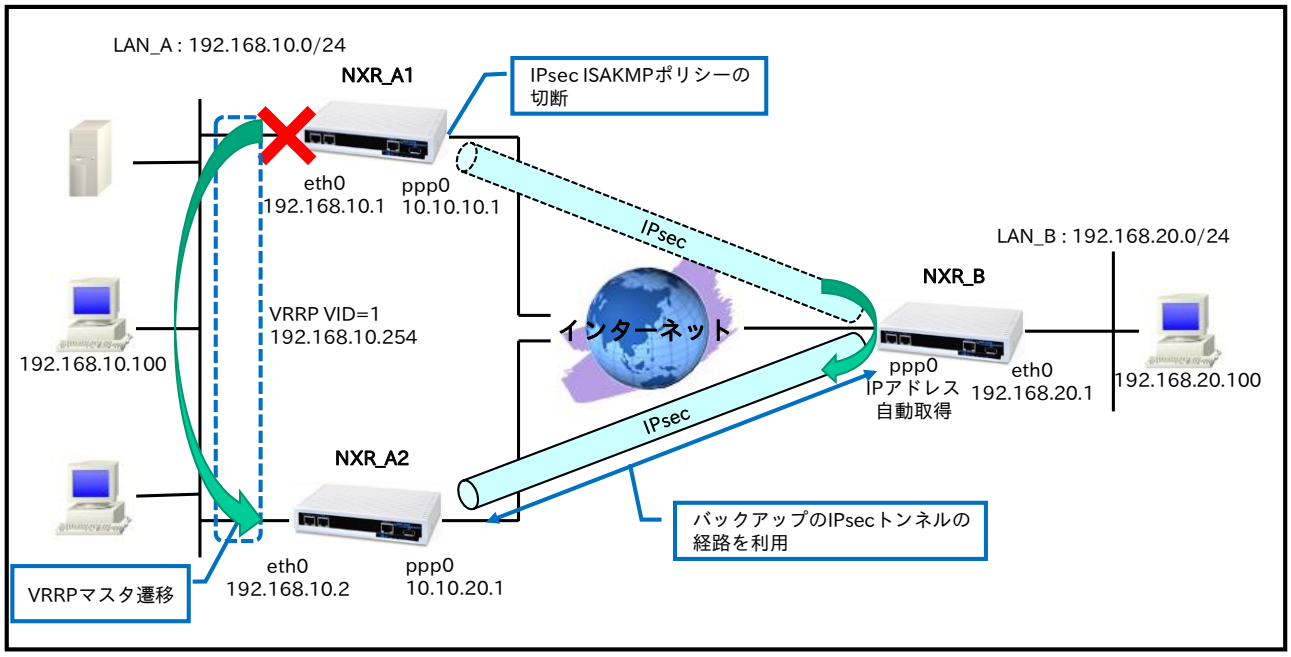
<正常時>



<NXR_A1 ppp0 インタフェースリンクダウン時>



<NXR_A1 ethernet0 インタフェースリンクダウン時>



- NXR_A1,A2 では以下の条件で VRRP を動作させます。

	NXR_A1	NXR_A2
グループ ID	1	
IP アドレス	192.168.10.254	
プライオリティ	254	100
プリエンプト	有効	
アドバタイズ間隔	5	
ネットワークイベントによる障害検知後のプライオリティ	50	−

- NXR_A2,B では IPsec ルート無効時に、カプセル化対象のパケットをルータから出力しないようにするためゲートウェイを null インタフェースとしたルートを設定します。
- NXR_A1 では ppp0 インタフェースリンクダウンによる WAN 側障害検知時に、ネットワークイベントにて VRRP の優先度を変更します。また ethernet0 インタフェースリンクダウンに LAN 側障害検知時に、ネットワークイベントにて IPsec ISAKMP ポリシーの切断を行います。そして WAN 側での経路障害など IPsec 未確立時に LAN_B 宛のパケットを NXR_A2 に転送するためのルートを設定します。なおその際ルートのディスタンス値は IPsec ルートよりも大きい値を設定します。
- NXR_B では NXR_A1,A2 に対して同時に IPsec を確立する設定を行います。また経路の切り替えを行うために NXR_A1 側の IPsec ルートに対して NXR_A2 側の IPsec ルートのディスタンス値をより大きい値に設定することで正常時は NXR_A1 経由、NXR__A1 での障害時は NXR_A2 経由となるようにします。

  (☞) 本設定例ではスタティックルートのディスタンス値の重み付けにより冗長化を実現します。
- この設定例では ipsec priority-ignore 機能を使用します。この機能に対応していないファームウェア

をご利用頂いている場合は、同じフェーズ 2 の ID を持つ IPsec SA を同時に複数個確立することができません。そのため設定例のように同一の IPsec アクセスリストを複数の IPsec トンネルポリシーに適用した場合 IPsec SA を複数同時に確立することができませんので、各 IPsec トンネルポリシー毎に異なるルールの IPsec アクセスリストを設定する必要があります。

【 設定例 】

〔NXR_A1 の設定〕

```
nxr125#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr125(config)#hostname NXR_A1
NXR_A1(config)#track 1 interface ppp 0 initial-timeout 30
NXR_A1(config)#track 2 interface ethernet 0
NXR_A1(config)#interface ethernet 0
NXR_A1(config-if)#ip address 192.168.10.1/24
NXR_A1(config-if)#no ip redirects
NXR_A1(config-if)#vrrp ip 1 address 192.168.10.254
NXR_A1(config-if)#vrrp ip 1 priority 254
NXR_A1(config-if)#vrrp ip 1 preempt
NXR_A1(config-if)#vrrp ip 1 timers advertise 5
NXR_A1(config-if)#vrrp ip 1 netevent 1 priority 50
NXR_A1(config-if)#exit
NXR_A1(config)#ip route 192.168.20.0/24 tunnel 1 1
NXR_A1(config)#ip route 192.168.20.0/24 192.168.10.2 10
NXR_A1(config)#ip route 0.0.0.0/0 ppp 0
NXR_A1(config)#ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
NXR_A1(config)#ip access-list ppp0_in permit any 10.10.10.1 50
NXR_A1(config)#ipsec access-list ipsec_acl ip any any
NXR_A1(config)#ipsec local policy 1
NXR_A1(config-ipsec-local)#address ip
NXR_A1(config-ipsec-local)#exit
NXR_A1(config)#ipsec isakmp policy 1
NXR_A1(config-ipsec-isakmp)#description NXR_B
NXR_A1(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR_A1(config-ipsec-isakmp)#hash sha1
NXR_A1(config-ipsec-isakmp)#encryption aes128
NXR_A1(config-ipsec-isakmp)#group 5
NXR_A1(config-ipsec-isakmp)#lifetime 10800
NXR_A1(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A1(config-ipsec-isakmp)#remote address ip any
NXR_A1(config-ipsec-isakmp)#remote identity fqdn nxrb
NXR_A1(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A1(config-ipsec-isakmp)#local policy 1
NXR_A1(config-ipsec-isakmp)#netevent 2 disconnect
NXR_A1(config-ipsec-isakmp)#exit
NXR_A1(config)#ipsec tunnel policy 1
NXR_A1(config-ipsec-tunnel)#description NXR_B
NXR_A1(config-ipsec-tunnel)#negotiation-mode responder
NXR_A1(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A1(config-ipsec-tunnel)#set pfs group5
NXR_A1(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A1(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A1(config-ipsec-tunnel)#match address ipsec_acl
NXR_A1(config-ipsec-tunnel)#exit
NXR_A1(config)#interface tunnel 1
NXR_A1(config-tunnel)#tunnel mode ipsec ipv4
NXR_A1(config-tunnel)#tunnel protection ipsec policy 1
NXR_A1(config-tunnel)#ip tcp adjust-mss auto
```

```
NXR_A1(config-tunnel)#exit
NXR_A1(config)#interface ppp 0
NXR_A1(config-ppp)#ip address 10.10.10.1/32
NXR_A1(config-ppp)#ip masquerade
NXR_A1(config-ppp)#ip access-group in ppp0_in
NXR_A1(config-ppp)#ip spi-filter
NXR_A1(config-ppp)#ip tcp adjust-mss auto
NXR_A1(config-ppp)#no ip redirects
NXR_A1(config-ppp)#ppp username test1@example.jp password test1pass
NXR_A1(config-ppp)#ipsec policy 1
NXR_A1(config-ppp)#exit
NXR_A1(config)#interface ethernet 1
NXR_A1(config-if)#no ip address
NXR_A1(config-if)#pppoe-client ppp 0
NXR_A1(config-if)#exit
NXR_A1(config)#dns
NXR_A1(config-dns)#service enable
NXR_A1(config-dns)#exit
NXR_A1(config)#fast-forwarding enable
NXR_A1(config)#exit
NXR_A1#save config
```

〔NXR_A2 の設定〕

```
nxr125#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr125(config)#hostname NXR_A2
NXR_A2(config)#interface ethernet 0
NXR_A2(config-if)#ip address 192.168.10.2/24
NXR_A2(config-if)#no ip redirects
NXR_A2(config-if)#vrrp ip 1 address 192.168.10.254
NXR_A2(config-if)#vrrp ip 1 priority 100
NXR_A2(config-if)#vrrp ip 1 preempt
NXR_A2(config-if)#vrrp ip 1 timers advertise 5
NXR_A2(config-if)#exit
NXR_A2(config)#ip route 192.168.20.0/24 tunnel 1 1
NXR_A2(config)#ip route 192.168.20.0/24 null 254
NXR_A2(config)#ip route 0.0.0.0/0 ppp 0
NXR_A2(config)#ip access-list ppp0_in permit any 10.10.20.1 udp 500 500
NXR_A2(config)#ip access-list ppp0_in permit any 10.10.20.1 50
NXR_A2(config)#ipsec access-list ipsec_acl ip any any
NXR_A2(config)#ipsec local policy 1
NXR_A2(config-ipsec-local)#address ip
NXR_A2(config-ipsec-local)#exit
NXR_A2(config)#ipsec isakmp policy 1
NXR_A2(config-ipsec-isakmp)#description NXR_B
NXR_A2(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR_A2(config-ipsec-isakmp)#hash sha1
NXR_A2(config-ipsec-isakmp)#encryption aes128
NXR_A2(config-ipsec-isakmp)#group 5
NXR_A2(config-ipsec-isakmp)#lifetime 10800
NXR_A2(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A2(config-ipsec-isakmp)#remote address ip any
NXR_A2(config-ipsec-isakmp)#remote identity fqdn nxrb
NXR_A2(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A2(config-ipsec-isakmp)#local policy 1
NXR_A2(config-ipsec-isakmp)#exit
NXR_A2(config)#ipsec tunnel policy 1
NXR_A2(config-ipsec-tunnel)#description NXR_B
NXR_A2(config-ipsec-tunnel)#negotiation-mode responder
NXR_A2(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A2(config-ipsec-tunnel)#set pfs group5
NXR_A2(config-ipsec-tunnel)#set sa lifetime 3600
```

```
NXR_A2(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A2(config-ipsec-tunnel)#match address ipsec_acl
NXR_A2(config-ipsec-tunnel)#exit
NXR_A2(config)#interface tunnel 1
NXR_A2(config-tunnel)#tunnel mode ipsec ipv4
NXR_A2(config-tunnel)#tunnel protection ipsec policy 1
NXR_A2(config-tunnel)#ip tcp adjust-mss auto
NXR_A2(config-tunnel)#exit
NXR_A2(config)#interface ppp 0
NXR_A2(config-ppp)#ip address 10.10.20.1/32
NXR_A2(config-ppp)#ip masquerade
NXR_A2(config-ppp)#ip access-group in ppp0_in
NXR_A2(config-ppp)#ip spi-filter
NXR_A2(config-ppp)#ip tcp adjust-mss auto
NXR_A2(config-ppp)#no ip redirects
NXR_A2(config-ppp)#ppp username test2@example.jp password test2pass
NXR_A2(config-ppp)#ipsec policy 1
NXR_A2(config-ppp)#exit
NXR_A2(config)#interface ethernet 1
NXR_A2(config-if)#no ip address
NXR_A2(config-if)#pppoe-client ppp 0
NXR_A2(config-if)#exit
NXR_A2(config)#dns
NXR_A2(config-dns)#service enable
NXR_A2(config-dns)#exit
NXR_A2(config)#fast-forwarding enable
NXR_A2(config)#exit
NXR_A2#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1 1
NXR_B(config)#ip route 192.168.10.0/24 tunnel 2 10
NXR_B(config)#ip route 192.168.10.0/24 null 254
NXR_B(config)#ip route 0.0.0.0/0 ppp 0
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 any 50
NXR_B(config)#ip access-list ppp0_in permit 10.10.20.1 any udp 500 500
NXR_B(config)#ip access-list ppp0_in permit 10.10.20.1 any 50
NXR_B(config)#ipsec access-list ipsec_acl ip any any
NXR_B(config)#ipsec priority-ignore enable
% restart ipsec service to take affect.
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A1
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A1
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
NXR_B(config-ipsec-tunnel)#set priority 1
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
NXR_B(config-tunnel)#exit
NXR_B(config)#ipsec isakmp policy 2
NXR_B(config-ipsec-isakmp)#description NXR_A2
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.20.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 2
```

```
NXR_B(config-ipsec-tunnel)#description NXR_A2
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 2
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface tunnel 2
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 2
NXR_B(config-tunnel)#ip tcp adjust-mss auto
NXR_B(config-tunnel)#exit
NXR_B(config)#interface ppp 0
NXR_B(config-ppp)#ip address negotiated
NXR_B(config-ppp)#ip masquerade
NXR_B(config-ppp)#ip access-group in ppp0_in
NXR_B(config-ppp)#ip spi-filter
NXR_B(config-ppp)#ip tcp adjust-mss auto
NXR_B(config-ppp)#no ip redirects
NXR_B(config-ppp)#ppp username test3@example.jp password test3pass
NXR_B(config-ppp)#ipsec policy 1
NXR_B(config-ppp)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#no ip address
NXR_B(config-if)#pppoe-client ppp 0
NXR_B(config-if)#exit
NXR_B(config)#dns
NXR_B(config-dns)#service enable
NXR_B(config-dns)#exit
NXR_B(config)#fast-forwarding enable
NXR_B(config)#exit
NXR_B#save config
```

【 設定例解説 】

〔NXR_A1 の設定〕

(☞) NXR_A1 の設定は 2-9. 冗長化設定 1(backupSA の利用)の〔NXR_A1 の設定〕と同一となりますので、そちらをご参照下さい。

〔NXR_A2 の設定〕

(☞) NXR_A2 の設定は 2-9. 冗長化設定 1(backupSA の利用)の〔NXR_A2 の設定〕が参考になりますので、そちらをご参照下さい。

〔NXR_B の設定〕

(☞) ここに記載のない設定項目は 2-9. 冗長化設定 1(backupSA の利用)の〔NXR_B の設定〕が参考になりますので、そちらをご参照下さい。

1. <IPsec priority-ignore 設定>

```
NXR_B(config)#ipsec priority-ignore enable
```

ipsec priority-ignore を有効に設定します。

これはプライオリティによる IPsec SA の優先度を無効にする設定です。

Route based IPsec ではフェーズ 2 の ID を IPsec SA を確立するための ID としてのみ使用します。そのためプライオリティによる冗長化設定などを利用しない場合は、本設定を有効にすることによって同じフェーズ 2 の ID を持つ IPsec SA を複数個同時に確立することができます。

(☞) この機能に対応していないファームウェアをご利用頂いている場合は、同じフェーズ 2 の ID を持つ IPsec SA を同時に複数個確立することができません。そのため設定例のように同一の IPsec アクセスリストを複数の IPsec トンネルポリシーに適用した場合 IPsec SA を複数同時に確立することができませんので、各 IPsec トンネルポリシー毎に異なるルールの IPsec アクセスリストを設定する必要があります。

2. <IPsec ISAKMP ポリシー1 設定>

```
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A1
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey1
```

NXR_A1 との IPsec 接続で使用する ISAKMP ポリシー1 を設定します。

ISAKMP ポリシー1 の説明として NXR_A1、認証方式として pre-share(事前共有鍵)を選択し事前共有鍵 ipseckey1 を設定します。

```
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
```

認証アルゴリズムとして sha1、暗号化アルゴリズムとして aes128、Diffie-Hellman(DH)グループとして group 5、ISAKMP SA のライフタイムとして 10800 秒、フェーズ 1 のネゴシエーションモードとしてアグレッシブモードを設定します。

```
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
```

NXR_A1 の WAN 側 IP アドレス 10.10.10.1、IKE KeepAlive(DPD)を監視間隔 30 秒,リトライ回数 3 回とし keepalive 失敗時に SA を削除し IKE のネゴシエーションを開始するよう設定します。

そして IPsec ローカルポリシー 1 と関連づけを行います。

3. <IPsec トンネルポリシー2 設定>

```
NXR_B(config)#ipsec tunnel policy 2
NXR_B(config-ipsec-tunnel)#description NXR_A2
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
```

NXR_A2 との IPsec 接続で使用するトンネルポリシー2 を設定します。

IPsec トンネルポリシー2 の説明として NXR_A2、ネゴシエーションモードとして auto を設定します。

```
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 2
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
```

ISAKMP ポリシー2 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

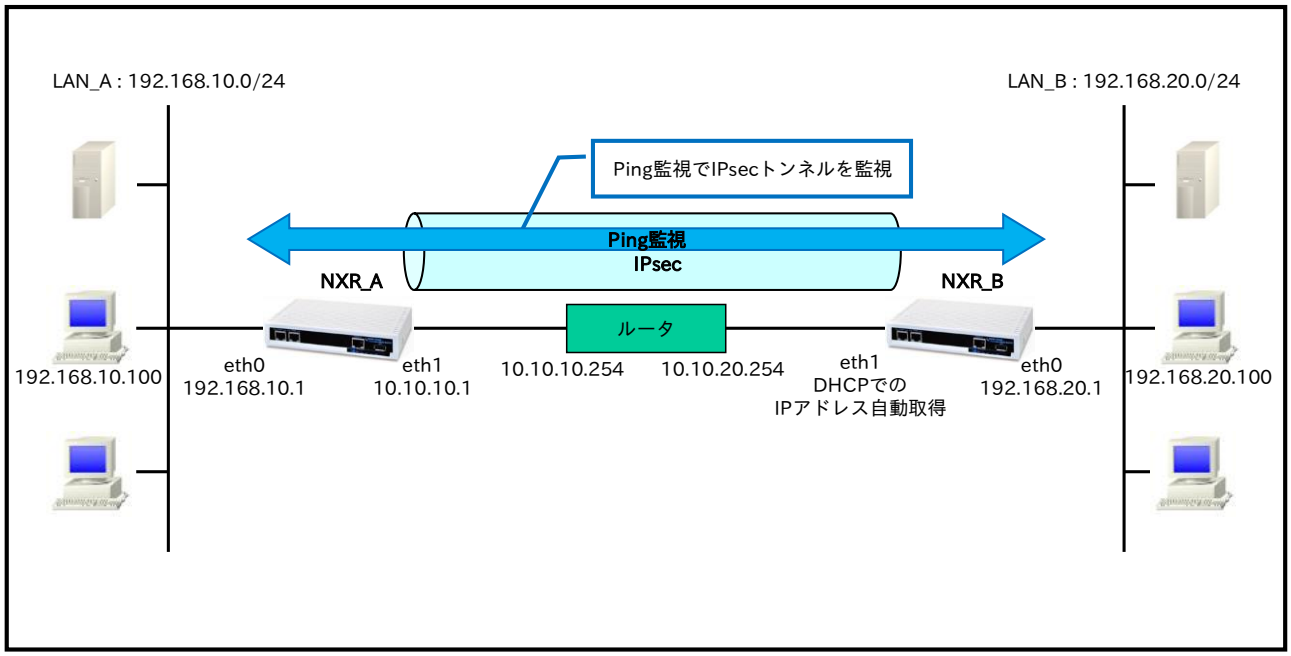
【 パソコンの設定例 】

	LAN A のパソコン	LAN B のパソコン
IP アドレス	192.168.10.100	192.168.20.100
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.254	192.168.20.1
DNS サーバ	192.168.10.1	192.168.20.1
	192.168.10.2	

2-11. ネットワークイベント機能で IPsec トンネルを監視

NXR シリーズではネットワークイベントという機能があり、これはある監視対象の状態変化を検知した際に指定された動作を行うという機能です。この機能を利用して Ping 監視を行い Ping による障害検知後 IPsec を再接続します。

【 構成図 】



- Ping 監視機能で指定した宛先(192.168.10.1)に対して指定した時間間隔,リトライ回数監視を行い障害を検知できるようにします。ここでは 10 秒間隔で監視を行い、3 回リトライしても応答が得られない場合は障害発生と判断します。

  (☞) ネットワークイベント機能で監視を行う場合、障害を検知していない場合はステータスは up となり障害を検知した場合は down となります。
- Ping 監視で障害を検知した場合に IPsec トンネルの再接続を行えるよう IPsec ISAKMP ポリシー設定内の netevent で reconnect を設定します。
- 2-2. 動的 IP アドレスでの接続設定例(AggressiveMode の利用)の内容も参考になりますのでご参照下さい。

【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface  179thernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1 1
NXR_A(config)#ip route 192.168.20.0/24 null 254
NXR_A(config)#ip route 0.0.0.0/0 10.10.10.254
NXR_A(config)#ipsec access-list ipsec_acl ip any any
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A(config-ipsec-isakmp)#remote address ip any
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrb
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address ipsec_acl
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
NXR_A(config-tunnel)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#interface  179thernet 1
NXR_A(config-if)#ip address 10.10.10.1/24
NXR_A(config-if)#ipsec policy 1
NXR_A(config-if)#exit
NXR_A(config)#fast-forwarding enable
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface  180thernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1 1
NXR_B(config)#ip route 192.168.10.0/24 null 254
NXR_B(config)#track 1 ip reachability 192.168.10.1 interface tunnel 1 10 3
NXR_B(config)#ipsec access-list ipsec_acl ip any any
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#netevent 1 reconnect
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
NXR_B(config-tunnel)#exit
NXR_B(config)#interface  180thernet 1
NXR_B(config-if)#ip address dhcp
NXR_B(config-if)#ipsec policy 1
NXR_B(config-if)#exit
NXR_B(config)#fast-forwarding enable
NXR_B(config)#exit
NXR_B#save config
```

【 設定例解説 】

〔NXR_A の設定〕

(☞) 設定項目は 2-2. 動的 IP アドレスでの接続設定例(AggressiveMode の利用)の〔NXR_A の設定〕が参考になりますので、そちらをご参照下さい。

〔NXR_B の設定〕

(☞) ここに記載のない設定項目は 2-2. 動的 IP アドレスでの接続設定例(AggressiveMode の利用)の〔NXR_B の設定〕が参考になりますので、そちらをご参照下さい。

1. <トラック設定(Ping 監視)>

```
NXR_B(config)#track 1 ip reachability 192.168.10.1 interface tunnel 1 10 3
```

トラック No.1 に Ping 監視設定を登録します。

宛先 IP アドレスを 192.168.10.1(NXR_A の ethernet0 インタフェースの IP アドレス)とし出力インタフェースを tunnel1 インタフェースとします。

(☞) インタフェース名を指定した場合はそのインタフェースの IP アドレスが監視パケットの送信元 IP アドレスとなります。なおトンネルインタフェースの IP アドレス設定が no ip address の場合は ifindex が小さいインタフェース(lo 除く)の IP アドレスが使用されます。通常は ethernet0 インタフェースの IP アドレスが使用されます。

送信間隔 10 秒で 3 回リトライを行い、応答が得られない場合はダウン状態に遷移します。

2. <IPsec ISAKMP ポリシー設定>

```
NXR_B(config-ipsec-isakmp)#netevent 1 reconnect
```

ネットワークイベントとして track 1 コマンドで指定した Ping 監視で障害を検知した場合、IPsec トンネル 1 の再接続を行います。

(☞) ネットワークイベントで IPsec を指定する場合は IKE 単位での指定となるため IPsec tunnel ポリシー設定ではなく IPsec ISAKMP ポリシー設定になります。

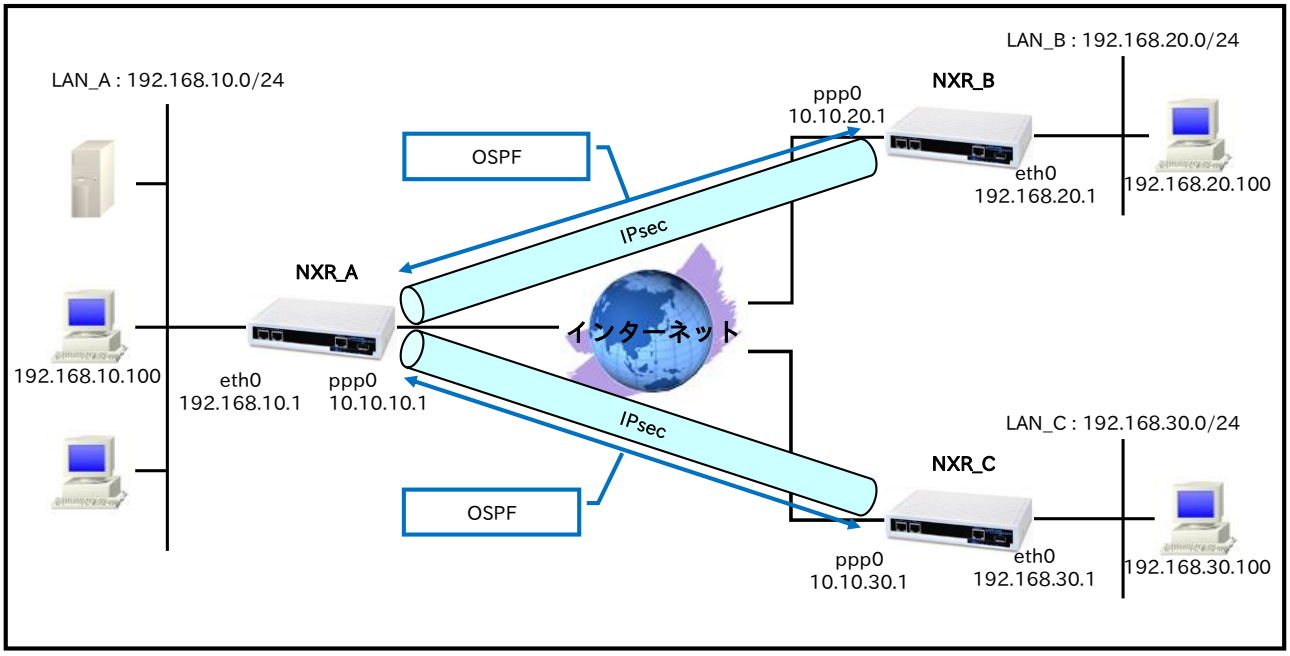
【 パソコンの設定例 】

	LAN A のパソコン	LAN B のパソコン
IP アドレス	192.168.10.100	192.168.20.100
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1

2-12. IPsec トンネルでダイナミックルーティング(OSPF)を利用する

Route Based IPsec では Policy Based IPsec と異なり、IPsec のみで OSPF を利用することが可能です。
ここでは NXR_A 経由で IPsec での拠点間通信を行います。

【 構成図 】



- トンネルインタフェースで OSPF のパケットを送受信するためにはトンネルインタフェースに IP アドレスを設定する必要があります。
- トンネルインタフェースにおいて OSPF を使用する場合、ネットワークタイプは Point to Point となります。
- 各拠点からのインターネットアクセスを可能にするために NAT 設定(IP マスカレード)やフィルタ設定(SPI)および DNS 設定を行っています。
- 2-5. PPPoE を利用した IPsec 接続設定例の内容も参考になりますのでご参照下さい。

【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface  183thernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#router ospf
NXR_A(config-router)#router-id 172.31.0.1
NXR_A(config-router)#network 192.168.10.0/24 area 0
NXR_A(config-router)#passive-interface  183thernet 0
NXR_A(config-router)#exit
NXR_A(config)#ip route 192.168.0.0/16 null 254
NXR_A(config)#ip route 0.0.0.0/0 ppp 0
NXR_A(config)#ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
NXR_A(config)#ip access-list ppp0_in permit any 10.10.10.1 50
NXR_A(config)#ipsec access-list ipsec_acl ip any any
NXR_A(config)#ipsec priority-ignore enable
% restart ipsec service to take affect.
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode main
NXR_A(config-ipsec-isakmp)#remote address ip 10.10.20.1
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address ipsec_acl
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 1
NXR_A(config-tunnel)#ip address 192.168.10.1/32
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
NXR_A(config-tunnel)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#ipsec isakmp policy 2
NXR_A(config-ipsec-isakmp)#description NXR_C
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A(config-ipsec-isakmp)#remote address ip any
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrc
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A(config-ipsec-isakmp)#local policy 1
```

```
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 2
NXR_A(config-ipsec-tunnel)#description NXR_C
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 2
NXR_A(config-ipsec-tunnel)#match address ipsec_acl
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 2
NXR_A(config-tunnel)#ip address 192.168.10.1/32
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 2
NXR_A(config-tunnel)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#interface ppp 0
NXR_A(config-ppp)#ip address 10.10.10.1/32
NXR_A(config-ppp)#ip masquerade
NXR_A(config-ppp)#ip access-group in ppp0_in
NXR_A(config-ppp)#ip spi-filter
NXR_A(config-ppp)#ip tcp adjust-mss auto
NXR_A(config-ppp)#no ip redirects
NXR_A(config-ppp)#ppp username test1@example.jp password test1pass
NXR_A(config-ppp)#ipsec policy 1
NXR_A(config-ppp)#exit
NXR_A(config)#interface  184thernet 1
NXR_A(config-if)#no ip address
NXR_A(config-if)#pppoe-client ppp 0
NXR_A(config-if)#exit
NXR_A(config)#dns
NXR_A(config-dns)#service enable
NXR_A(config-dns)#exit
NXR_A(config)#fast-forwarding enable
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface  184thernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#router ospf
NXR_B(config-router)#router-id 172.31.0.2
NXR_B(config-router)#network 192.168.20.0/24 area 0
NXR_B(config-router)#passive-interface  184thernet 0
NXR_B(config-router)#exit
NXR_B(config)#ip route 192.168.0.0/16 null 254
NXR_B(config)#ip route 0.0.0.0/0 ppp 0
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 udp 500 500
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 50
NXR_B(config)#ipsec access-list ipsec_acl ip any any
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
```

```
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#ip address 192.168.20.1/32
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
NXR_B(config-tunnel)#exit
NXR_B(config)#interface ppp 0
NXR_B(config-ppp)#ip address 10.10.20.1/32
NXR_B(config-ppp)#ip masquerade
NXR_B(config-ppp)#ip access-group in ppp0_in
NXR_B(config-ppp)#ip spi-filter
NXR_B(config-ppp)#ip tcp adjust-mss auto
NXR_B(config-ppp)#no ip redirects
NXR_B(config-ppp)#ppp username test2@example.jp password test2pass
NXR_B(config-ppp)#ipsec policy 1
NXR_B(config-ppp)#exit
NXR_B(config)#interface  185thernet 1
NXR_B(config-if)#no ip address
NXR_B(config-if)#pppoe-client ppp 0
NXR_B(config-if)#exit
NXR_B(config)#dns
NXR_B(config-dns)#service enable
NXR_B(config-dns)#exit
NXR_B(config)#fast-forwarding enable
NXR_B(config)#exit
NXR_B#save config
```

〔NXR_C の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_C
NXR_C(config)#interface  185thernet 0
NXR_C(config-if)#ip address 192.168.30.1/24
NXR_C(config-if)#exit
NXR_C(config)#router ospf
NXR_C(config-router)#router-id 172.31.0.3
NXR_C(config-router)#network 192.168.30.0/24 area 0
NXR_C(config-router)#passive-interface  185thernet 0
NXR_C(config-router)#exit
NXR_C(config)#ip route 192.168.0.0/16 null 254
NXR_C(config)#ip route 0.0.0.0/0 ppp 0
NXR_C(config)#ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
NXR_C(config)#ip access-list ppp0_in permit 10.10.10.1 any 50
NXR_C(config)#ipsec access-list ipsec_acl ip any any
NXR_C(config)#ipsec local policy 1
NXR_C(config-ipsec-local)#address ip
```

```
NXR_C(config-ipsec-local)#self-identity fqdn nxrc
NXR_C(config-ipsec-local)#exit
NXR_C(config)#ipsec isakmp policy 1
NXR_C(config-ipsec-isakmp)#description NXR_A
NXR_C(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR_C(config-ipsec-isakmp)#hash sha1
NXR_C(config-ipsec-isakmp)#encryption aes128
NXR_C(config-ipsec-isakmp)#group 5
NXR_C(config-ipsec-isakmp)#lifetime 10800
NXR_C(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_C(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_C(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_C(config-ipsec-isakmp)#local policy 1
NXR_C(config-ipsec-isakmp)#exit
NXR_C(config)#ipsec tunnel policy 1
NXR_C(config-ipsec-tunnel)#description NXR_A
NXR_C(config-ipsec-tunnel)#negotiation-mode auto
NXR_C(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_C(config-ipsec-tunnel)#set pfs group5
NXR_C(config-ipsec-tunnel)#set sa lifetime 3600
NXR_C(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_C(config-ipsec-tunnel)#match address ipsec_acl
NXR_C(config-ipsec-tunnel)#exit
NXR_C(config)#interface tunnel 1
NXR_C(config-tunnel)#ip address 192.168.30.1/32
NXR_C(config-tunnel)#tunnel mode ipsec ipv4
NXR_C(config-tunnel)#tunnel protection ipsec policy 1
NXR_C(config-tunnel)#ip tcp adjust-mss auto
NXR_C(config-tunnel)#exit
NXR_C(config)#interface ppp 0
NXR_C(config-ppp)#ip address negotiated
NXR_C(config-ppp)#ip masquerade
NXR_C(config-ppp)#ip access-group in ppp0_in
NXR_C(config-ppp)#ip spi-filter
NXR_C(config-ppp)#ip tcp adjust-mss auto
NXR_C(config-ppp)#no ip redirects
NXR_C(config-ppp)#ppp username test3@example.jp password test3pass
NXR_C(config-ppp)#ipsec policy 1
NXR_C(config-ppp)#exit
NXR_C(config)#interface  186thernet 1
NXR_C(config-if)#no ip address
NXR_C(config-if)#pppoe-client ppp 0
NXR_C(config-if)#exit
NXR_C(config)#dns
NXR_C(config-dns)#service enable
NXR_C(config-dns)#exit
NXR_C(config)#fast-forwarding enable
NXR_C(config)#exit
NXR_C#save config
```

【 設定例解説 】

〔NXR_A の設定〕

(☞) ここに記載のない設定項目は 2-5. PPPoE を利用した IPsec 接続設定例の〔NXR_A の設定〕が参考になりますので、そちらをご参照下さい。

1. <OSPF 設定>

```
NXR_A(config)#router ospf
```

OSPF を設定します。

```
NXR_A(config-router)#router-id 172.31.0.1
```

OSPF のルータ ID として 172.31.0.1 を設定します。

```
NXR_A(config-router)#network 192.168.10.0/24 area 0
```

OSPF のエリアおよびそのエリアに所属するネットワークを設定します。

ここではネットワークとして 192.168.10.0/24、エリアを 0 と設定します。

これにより 192.168.10.0/24 のネットワークに属するインタフェースでエリア 0 として OSPF パケットのやりとりができるようになります。

```
NXR_A(config-router)#passive-interface  187thernet 0
```

パッシブインタフェースとして ethernet0 を設定します。

パッシブインタフェースを設定することでそのインタフェースで不要な OSPF パケットの送信を止めることができます。

2. <スタティックルート設定>

```
NXR_A(config)#ip route 192.168.0.0/16 null 254
```

192.168.0.0/16 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

(☞) null インタフェースを出力インタフェースとして設定した場合、パケットが出力されることはありません(ドロップされます)。よってパケット出力を行う場合は null インタフェースよりもディスタンス値が小さいルートを設定する必要があります。

これにより OSPF で作成した LAN_B,LAN_C 宛のルートがない場合、パケットはドロップされます。

3. <トンネル 1 インタフェース設定>

```
NXR_A(config)#interface tunnel 1
```

トンネル 1 インタフェースを設定します。

```
NXR_A(config-tunnel)#ip address 192.168.10.1/32
```

トンネル 1 インタフェースの IP アドレスに 192.168.10.1/32 を設定します。

これによりトンネルインタフェースで OSPF パケットのやりとりができるようになります。

(☞) LAN(ethernet0 インタフェース)側と同一のネットワークに属する IP アドレスになり、サブネットマスクは/32 で設定します。

```
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
```

トンネルインタフェースで使用するトンネルモードを設定します。

トンネルインタフェースを Route Based IPsec で使用する場合は ipsec ipv4 と設定します。

```
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
```

使用する IPsec トンネルポリシーを設定します。

ここでは IPsec トンネルポリシー1 と関連づけを行います。

(☞) IPsec ローカルポリシーではありませんのでご注意下さい。

```
NXR_A(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

4. <トンネル 2 インタフェース設定>

```
NXR_A(config)#interface tunnel 2
NXR_A(config-tunnel)#ip address 192.168.10.1/32
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 2
NXR_A(config-tunnel)#ip tcp adjust-mss auto
```

トンネル 2 インタフェースで IP アドレス 192.168.10.1/32、トンネルモードを ipsec ipv4、使用するトンネルポリシーとして 2 を設定します。また TCP MSS の調整機能をオートに設定します。

〔NXR_B の設定〕

(☞) ここに記載のない設定項目は 2-5. PPPoE を利用した IPsec 接続設定例の〔NXR_B の設定〕が参考になりますので、そちらをご参照下さい。

1. <OSPF 設定>

```
NXR_B(config)#router ospf
NXR_B(config-router)#router-id 172.31.0.2
NXR_B(config-router)#network 192.168.20.0/24 area 0
NXR_B(config-router)#passive-interface  188thernet 0
```

OSPF 設定でルータ ID として 172.31.0.2、ネットワークとして 192.168.20.0/24、エリアを 0、パッシブインタフェースとして ethernet0 を設定します。

2. <スタティックルート設定>

```
NXR_B(config)#ip route 192.168.0.0/16 null 254
```

192.168.0.0/16 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

これにより OSPF で作成した LAN_A,LAN_C 宛のルートがない場合、パケットはドロップされます。

3. <トンネルインタフェース設定>

```
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#ip address 192.168.20.1/32
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
```

トンネル 1 インタフェースで IP アドレス 192.168.20.1/32、トンネルモードを ipsec ipv4、使用するトンネルポリシーとして 1 を設定します。また TCP MSS の調整機能をオートに設定します。

〔NXR_C の設定〕

(☞) ここに記載のない設定項目は 2-5. PPPoE を利用した IPsec 接続設定例の〔NXR_C の設定〕が参考になりますので、そちらをご参照下さい。

1. <OSPF 設定>

```
NXR_C(config)#router ospf
NXR_C(config-router)#router-id 172.31.0.3
NXR_C(config-router)#network 192.168.30.0/24 area 0
NXR_C(config-router)#passive-interface  189thernet 0
```

OSPF 設定でルータ ID として 172.31.0.3、ネットワークとして 192.168.30.0/24、エリアを 0、パッシブインタフェースとして ethernet0 を設定します。

2. <スタティックルート設定>

```
NXR_C(config)#ip route 192.168.0.0/16 null 254
```

192.168.0.0/16 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

これにより OSPF で作成した LAN_A,LAN_B 宛のルートがない場合、パケットはドロップされます。

3. <トンネル 1 インタフェース設定>

```
NXR_C(config)#interface tunnel 1
NXR_C(config-tunnel)#ip address 192.168.30.1/32
NXR_C(config-tunnel)#tunnel mode ipsec ipv4
NXR_C(config-tunnel)#tunnel protection ipsec policy 1
NXR_C(config-tunnel)#ip tcp adjust-mss auto
```

トンネル 1 インタフェースで IP アドレス 192.168.30.1/32、トンネルモードを ipsec ipv4、使用するトンネルポリシーとして 1 を設定します。また TCP MSS の調整機能をオートに設定します。

【 パソコンの設定例 】

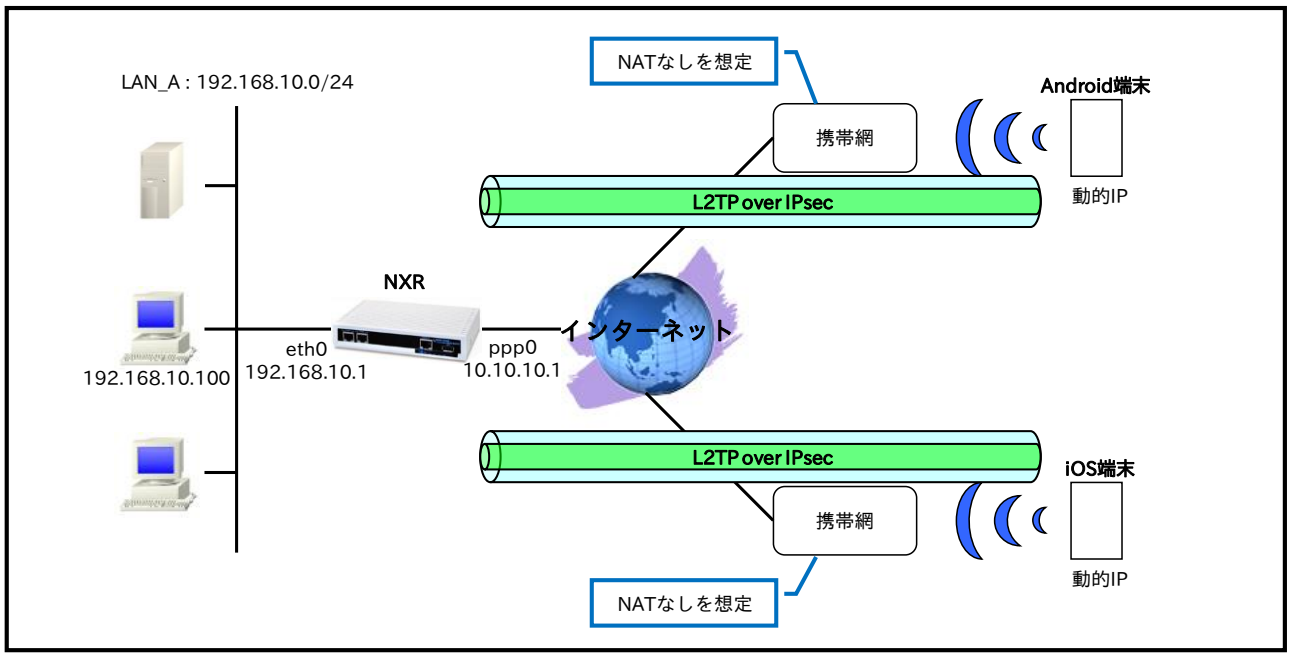
	LAN A のパソコン	LAN B のパソコン	LAN C のパソコン
IP アドレス	192.168.10.100	192.168.20.100	192.168.30.100
サブネットマスク	255.255.255.0	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1	192.168.30.1
DNS サーバ	192.168.10.1	192.168.20.1	192.168.30.1

3. L2TP/IPsec 設定

3-1. スマートフォンとの L2TP/IPsec 接続設定例

Android や iOS のスマートフォンに搭載されている L2TP/IPsec の VPN 機能を利用することで、NXR と VPN 接続することが可能です。なお、この設定例では IPsec で事前共有鍵を利用して接続を行います。
また、本設定例では携帯網で NAT されないことを想定しています。キャリアグレード NAT により携帯網側で NAT される可能性がある場合は 3-3. スマートフォンとの L2TP/IPsec NAT トラバーサル接続設定例をご参照ください。
なお、この設定例は弊社独自の検証結果を元に作成しております。よって、Android や iOS のスマートフォンとの接続を保証するものではありません。

【 構成図 】



- L2TP/IPsec を設定する場合は大きく分けて以下の設定が必要となります。
  - IPsec 設定
  - L2TP 設定
  - virtual-template インタフェース設定
  -アクセスサーバ(RAS)設定
- IPsec はトランスポートモードを使用し L2TP パケットを暗号化します。
- L2TPv2 の LNS 機能による着信では virtual-template インタフェースを使用します。
- 接続してきたスマートフォンには IP アドレスプールより IP アドレスを割り当てます。この設定例では 2 台に IP アドレスを割り当てるため IP アドレスを 2 つ設定し、かつユーザ ID 毎に指定した IP アドレスを割り当てます。

【 設定例 】

〔NXR の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR
NXR(config)#interface ethernet 0
NXR(config-if)#ip address 192.168.10.1/24
NXR(config-if)#exit
NXR(config)#ip route 0.0.0.0/0 ppp 0
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 50
NXR(config)#ipsec local policy 1
NXR(config-ipsec-local)#address ip
NXR(config-ipsec-local)#exit
NXR(config)#ipsec isakmp policy 1
NXR(config-ipsec-isakmp)#description smartphone
NXR(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR(config-ipsec-isakmp)#hash sha1
NXR(config-ipsec-isakmp)#encryption aes128
NXR(config-ipsec-isakmp)#group 5
NXR(config-ipsec-isakmp)#lifetime 86400
NXR(config-ipsec-isakmp)#isakmp-mode main
NXR(config-ipsec-isakmp)#remote address ip any
NXR(config-ipsec-isakmp)#local policy 1
NXR(config-ipsec-isakmp)#exit
NXR(config)#ipsec tunnel policy 1
NXR(config-ipsec-tunnel)#description smartphone
NXR(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR(config-ipsec-tunnel)#no set pfs
NXR(config-ipsec-tunnel)#set sa lifetime 28800
NXR(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR(config-ipsec-tunnel)#match protocol l2tp-smartphone
NXR(config-ipsec-tunnel)#exit
NXR(config)#ppp account username android01 password android01pass
NXR(config)#ppp account username ios01 password ios01pass
NXR(config)#ppp account username test1@example.jp password test1pass
NXR(config)#access-server profile 0
NXR(config-ras)#ppp username android01 ip 172.16.0.10
NXR(config-ras)#exit
NXR(config)#access-server profile 1
NXR(config-ras)#ppp username ios01 ip 172.16.0.11
NXR(config-ras)#exit
NXR(config)#ip local pool smartphoneip address 172.16.0.10 172.16.0.11
NXR(config)#interface virtual-template 0
NXR(config-if-vt)#ip address 172.16.0.1/32
NXR(config-if-vt)#ip tcp adjust-mss auto
NXR(config-if-vt)#no ip redirects
NXR(config-if-vt)#no ip rebound
NXR(config-if-vt)#peer ip pool smartphoneip
NXR(config-if-vt)#exit
NXR(config)#l2tp udp source-port 1701
NXR(config)#l2tp 1
NXR(config-l2tp)#tunnel address any ipsec
NXR(config-l2tp)#tunnel mode lns
NXR(config-l2tp)#tunnel virtual-template 0
NXR(config-l2tp)#exit
% Restarting l2tp service. Please wait.....
NXR(config)#interface ppp 0
NXR(config-ppp)#ip address 10.10.10.1/32
NXR(config-ppp)#ip masquerade
NXR(config-ppp)#ip access-group in ppp0_in
NXR(config-ppp)#ip spi-filter
```

```
NXR(config-ppp)#ip tcp adjust-mss auto
NXR(config-ppp)#no ip redirects
NXR(config-ppp)#ppp username test1@example.jp
NXR(config-ppp)#ipsec policy 1
NXR(config-ppp)#exit
NXR(config)#interface ethernet 1
NXR(config-if)#no ip address
NXR(config-if)#pppoe-client ppp 0
NXR(config-if)#exit
NXR(config)#dns
NXR(config-dns)#service enable
NXR(config-dns)#exit
NXR(config)#fast-forwarding enable
NXR(config)#exit
NXR#save config
```

【 設定例解説 】

〔NXR の設定〕

1. <ホスト名の設定>

```
nxr120(config)#hostname NXR
```

ホスト名に NXR を設定します。

2. <LAN 側(ethernet0)インタフェース設定>

```
NXR(config)#interface ethernet 0
NXR(config-if)#ip address 192.168.10.1/24
```

LAN 側(ethernet0)インタフェースの IP アドレスとして 192.168.10.1/24 を設定します。

3. <スタティックルート設定>

```
NXR(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。なおゲートウェイとして ppp0 インタフェースを指定します。

4. <IP アクセスリスト設定>

```
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 50
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を ppp0_in とします。

一行目は宛先 IP アドレス 10.10.10.1,送信元 UDP ポート番号 500,宛先 UDP ポート番号 500 のパケットを許可する設定です。

二行目は宛先 IP アドレス 10.10.10.1,プロトコル番号 50(ESP)のパケットを許可する設定です。

なお、この IP アクセスリスト設定は ppp0 インタフェース設定で登録します。

(☞) IP アクセスリストを設定しただけではフィルタとして有効にはなりません。フィルタリングしたいインタフェースでの登録が必要になります。

(☞) UDP ポート 500 番およびプロトコル番号 50(ESP)は IPsec のネゴシエーションおよび通信で使用します。

5. <IPsec ローカルポリシー設定>

```
NXR(config)#ipsec local policy 1
NXR(config-ipsec-local)#address ip
```

IPsec ローカルポリシー1 で IPsec トンネルの送信元 IP アドレスを設定します。

6. <IPsec ISAKMP ポリシー設定>

```
NXR(config)#ipsec isakmp policy 1
NXR(config-ipsec-isakmp)#description smartphone
NXR(config-ipsec-isakmp)#authentication pre-share ipseckey
```

スマートフォンとの IPsec 接続で使用する ISAKMP ポリシー1 を設定します。

ISAKMP ポリシー1 の説明として smartphone、認証方式として pre-share(事前共有鍵)を選択し事前共有鍵 ipseckey を設定します。

```
NXR(config-ipsec-isakmp)#hash sha1
NXR(config-ipsec-isakmp)#encryption aes128
NXR(config-ipsec-isakmp)#group 5
NXR(config-ipsec-isakmp)#lifetime 86400
NXR(config-ipsec-isakmp)#isakmp-mode main
```

認証アルゴリズムとして sha1、暗号化アルゴリズムとして aes128、Diffie-Hellman(DH)グループとして group 5、ISAKMP SA のライフタイムとして 86400 秒、フェーズ 1 のネゴシエーションモードとしてメインモードを設定します。

```
NXR(config-ipsec-isakmp)#remote address ip any
NXR(config-ipsec-isakmp)#local policy 1
```

スマートフォンが動的 IP アドレスのためリモートアドレスを any と設定します。

そして IPsec ローカルポリシー1 と関連づけを行います。

7. <IPsec トンネルポリシー設定>

```
NXR(config)#ipsec tunnel policy 1
NXR(config-ipsec-tunnel)#description smartphone
```

スマートフォンとの IPsec 接続で使用するトンネルポリシー1 を設定します。

IPsec トンネルポリシー1 の説明として smartphone と設定します。

```
NXR(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR(config-ipsec-tunnel)#no set pfs
NXR(config-ipsec-tunnel)#set sa lifetime 28800
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を無効、IPsec SA のライフタイムとして 28800 秒を設定します。

```
NXR(config-ipsec-tunnel)#set key-exchange isakmp 1
```

ISAKMP ポリシー1 と関連づけを行います。

```
NXR(config-ipsec-tunnel)#match protocol l2tp-smartphone
```

スマートフォンとの間で L2TPv2 over IPsec 接続する際に設定します。この設定を有効にすると下記の設定が有効となり、IPsec 接続を行う際に自動設定されます。

・protocol-mode → transport

・negotiation-mode → responder

・IPsec セレクタ → 以下のように自動設定されます。

ID ペイロード	NXR 側	スマートフォン側
IPv4 アドレス	host	host
プロトコル	UDP	UDP
ポート番号	1701	any(どのポートでも受け付ける)

8. <PPP アカウント設定>

```
NXR(config)#ppp account username android01 password android01pass
NXR(config)#ppp account username ios01 password ios01pass
```

PPP のアカウントを設定します。

ここでは L2TPv2 の LNS 機能による着信時のユーザ ID,パスワードを設定します。

(☞) ここで設定したアカウントはアクセスサーバ設定で利用します。

```
NXR(config)#ppp account username test1@example.jp password test1pass
```

ここでは ppp0 インタフェースで使用するユーザ名,パスワードを設定します。

(☞) ここで設定したアカウントは ppp0 インタフェースの設定で利用します。

9. <アクセスサーバ(RAS)プロファイル 0 設定>

```
NXR(config)#access-server profile 0
```

アクセスサーバプロファイル 0 を設定します。

```
NXR(config-ras)#ppp username android01 ip 172.16.0.10
```

ユーザ名 android01 に 172.16.0.10 の IP アドレスを割り当てるよう設定します。

10. <アクセスサーバ(RAS)プロファイル 1 設定>

```
NXR(config)#access-server profile 1
```

アクセスサーバプロファイル 1 を設定します。

```
NXR(config-ras)#ppp username ios01 ip 172.16.0.11
```

ユーザ名 ios01 に 172.16.0.11 の IP アドレスを割り当てるよう設定します。

11. <IP アドレスプール設定>

```
NXR(config)#ip local pool smartphoneip address 172.16.0.10 172.16.0.11
```

IP アドレスプールを設定します。

ここでは IP アドレスプール名を smartphoneip としスマートフォンに割り当てる 172.16.0.10～

172.16.0.11 の IP アドレスを設定します。

12. <virtual-template 0 インタフェース設定>

```
NXR(config)#interface virtual-template 0
```

virtual-template 0 インタフェースを設定します。

virtual-template インタフェースは仮想的なインタフェースであり実際に作成されるわけではありません。

virtual-template インタフェースを使用するとコールを受けた際に PPP のクローンを作成し、本ノードの設定内容を当該 PPP に適用します。なお PPP クローンのインタフェース番号は、本装置が自動的に割り当てます。

```
NXR(config-if-vt)#ip address 172.16.0.1/32
```

virtual-template インタフェースの IP アドレスに 172.16.0.1/32 を設定します。

```
NXR(config-if-vt)#ip tcp adjust-mss auto
NXR(config-if-vt)#no ip redirects
NXR(config-if-vt)#no ip rebound
```

TCP MSS の調整機能をオート、ICMP リダイレクト機能を無効、IP リバウンド機能を無効に設定します。

```
NXR(config-if-vt)#peer ip pool smartphoneip
```

使用する IP アドレスプールを設定します。

ここではアクセスサーバ設定で設定した IP アドレスプール名 smartphoneip を設定します。

13. <L2TPv2 設定>

```
NXR(config)#l2tp udp source-port 1701
```

L2TPv2 で使用する送信元ポートを 1701 に設定します。

```
NXR(config)#l2tp 1
```

スマートフォンとの接続で使用する L2TP1 を設定します。

```
NXR(config-l2tp)#tunnel mode lns
```

L2TPv2 のトンネルモードを設定します。ここでは LNS を指定します。

```
NXR(config-l2tp)#tunnel address any ipsec
```

接続先に IP アドレスとして any を設定します。

また any 指定時にバインドするプロトコルとして IPsec を指定します。これにより IPsec SA の確立したクライアントからの接続のみ許可します。

```
NXR(config-l2tp)#tunnel virtual-template 0
```

LNS 利用時に使用する virtual-template 0 インタフェースを設定します。

14. <WAN 側(ppp0)インタフェース設定>

```
NXR(config)#interface ppp 0
NXR(config-ppp)#ip address 10.10.10.1/32
```

WAN 側(ppp0)インタフェースを設定します。

IP アドレスを 10.10.10.1/32 に設定します。

```
NXR(config-ppp)#ip masquerade
NXR(config-ppp)#ip access-group in ppp0_in
NXR(config-ppp)#ip spi-filter
NXR(config-ppp)#ip tcp adjust-mss auto
NXR(config-ppp)#no ip redirects
```

IP マスカレードを有効、IP アクセスリスト ppp0_in を in フィルタに適用、ステートフルパケットインスペクションを有効に設定します。

また TCP MSS の調整機能をオート、ICMP リダイレクト機能を無効に設定します。

```
NXR(config-ppp)#ppp username test1@example.jp
NXR(config-ppp)#ipsec policy 1
```

PPPoE 接続で使用するユーザ ID を設定します。

ここでは PPP アカウント設定で作成した test1@example.jp を設定します。

また IPsec トンネルのエンドポイントとなるため、IPsec ローカルポリシー1 を設定します。

15. <ethernet1 インタフェース設定>

```
NXR(config)#interface ethernet 1
NXR(config-if)#no ip address
NXR(config-if)#pppoe-client ppp 0
```

ethernet1 インタフェースで、ppp0 インタフェースを PPPoE クライアントとして使用できるよう設定します。

16. <DNS 設定>

```
NXR(config)#dns
NXR(config-dns)#service enable
```

DNS 設定で DNS サービスを有効にします。

17. <ファストフォワーディングの有効化>

```
NXR(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(☞) ファストフォワーディングの詳細および利用時の制約については、NXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

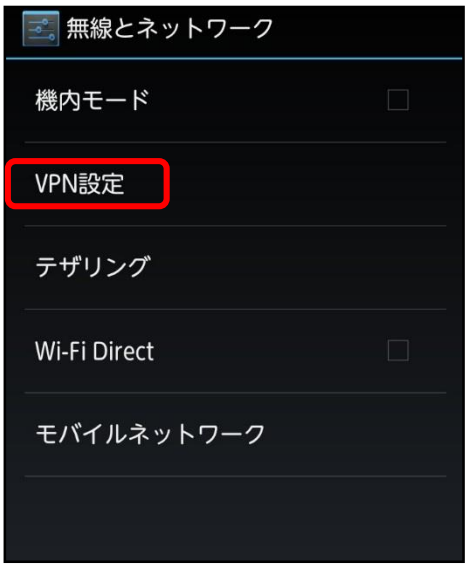
【 スマートフォン設定例 】

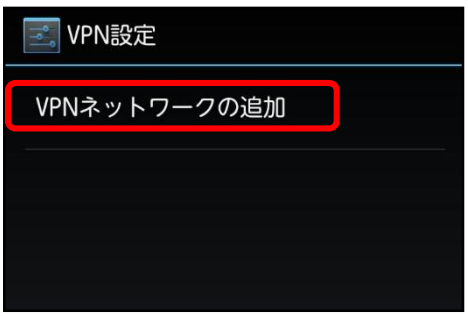
〔Android の設定〕

(☞) ここで記載した設定はあくまで一例ですので、ご利用頂いている Android 端末によって設定が異なる場合があります。設定の詳細はご利用中の Android 端末の取扱説明書等をご確認下さい。

(☞) 本設定例は Android 端末との接続性を保証するものではありません。
ご利用頂く際には十分な検証を行った上でのご利用をお願い致します。

1. メニュー画面から「設定」をタップします。
2. 設定画面で「無線とネットワーク」をタップします。
3. 無線とネットワーク画面で「VPN 設定」をタップします。
4. VPN 設定画面で「VPN ネットワークの追加」をタップします。

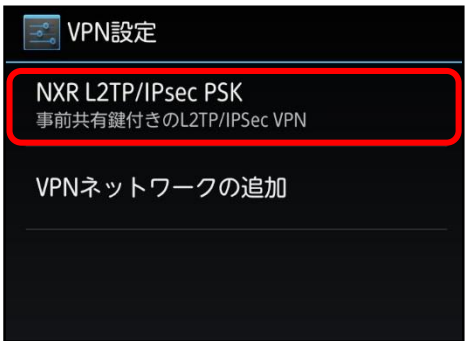




5. VPN ネットワークの編集で次の各項目を設定し保存します。

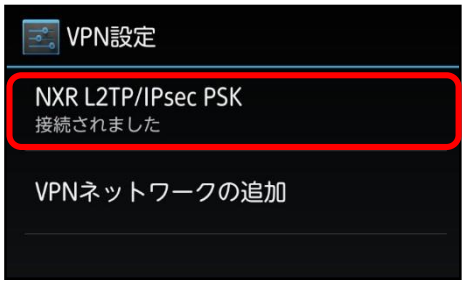
	設定項目	設定値	備考
①	名前	NXR L2TP/IPsec PSK	任意の名称を設定します
②	タイプ	L2TP/IPSec PSK	
③	サーバーアドレス	10.10.10.1	NXR の WAN 側 IP アドレスを設定します
④	L2TP セキュリティ保護	(未使用)	本設定例では使用していません
⑤	IPSec ID	(未使用)	本設定例では使用していません
⑥	IPSec 事前共有鍵	ipseckey	NXR で設定した事前共有鍵を設定します
⑦	詳細オプションを表示する	無効	

6. 設定保存後、VPN 名「NXR L2TP/IPsec PSK」が作成されますので、作成した「NXR L2TP/IPsec PSK」をタップします。



7. ユーザ名とパスワードの入力画面が表示されますので、L2TP/IPsec 用に設定した PPP のユーザ名とパスワードを入力し、接続をタップすると VPN 接続を開始します。

8. 接続が完了(成功)すると VPN 名の下に「接続されました」と表示されます。

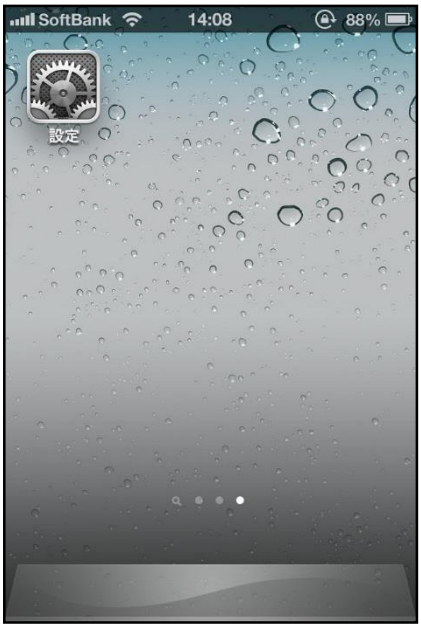


〔iOS の設定〕

(☞) ここで記載した設定はあくまで一例ですので、ご利用頂いている iOS 端末によって設定が異なる場合があります。設定の詳細はご利用中の iOS 端末の取扱説明書等をご確認下さい。

(☞) 本設定例は iOS 端末との接続性を保証するものではありません。
ご利用頂く際には十分な検証を行った上でのご利用をお願い致します。

1. ホーム画面から「設定」をタップします。
2. 設定画面で「一般」をタップします。



3. 一般画面で「VPN」をタップします。
4. VPN 画面で「VPN 構成を追加…」をタップします。

※この例では「test」という設定が定義されているところに VPN 設定を追加します。

5. 構成を追加画面で「L2TP」を選択し以下の各項目を設定し保存します。

	設定項目	設定値	備考
①	説明	NXR L2TP/IPsec PSK	任意の名称を設定します
②	サーバ	10.10.10.1	NXR の WAN 側 IP アドレスを設定します
③	アカウント	ios01	PPP 認証で使用するアカウントを設定します
④	RSA SecurID	オフ	－
⑤	パスワード	ios01pass	PPP 認証で使用するパスワードを設定します
⑥	シークレット	ipseckey	NXR で設定した事前共有鍵を設定します
⑦	すべての信号を送信	オン	－
⑧	プロキシ	オフ	－

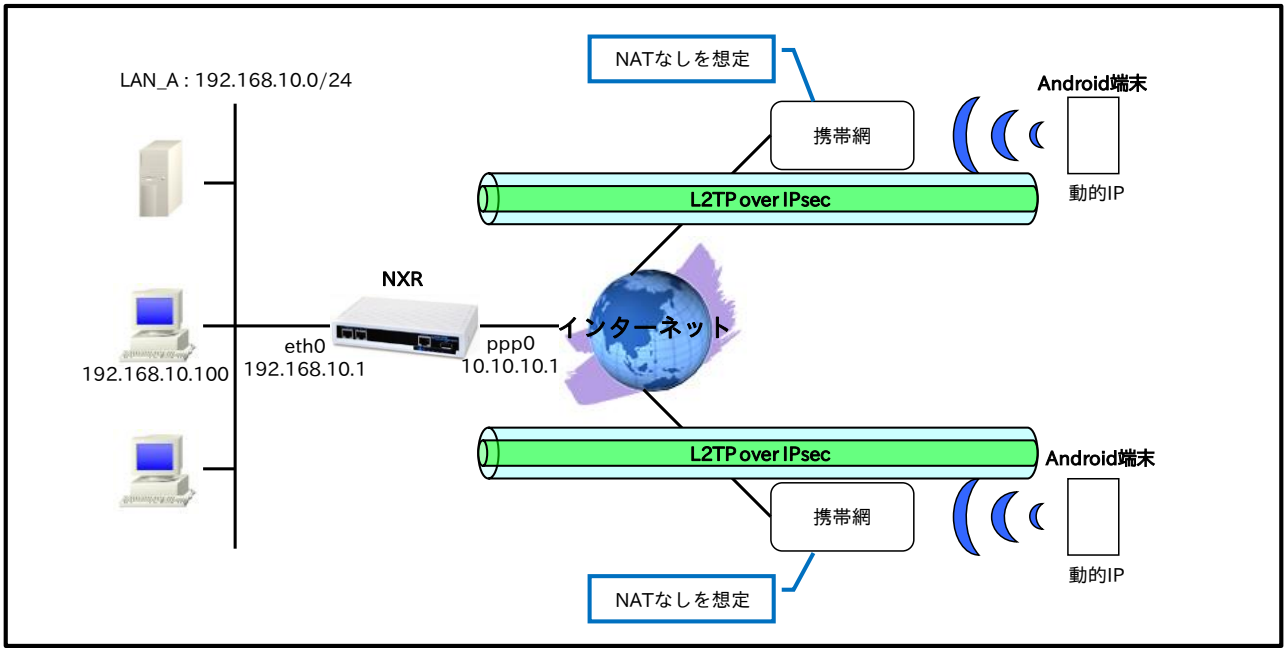
6. VPN 構成「NXR L2TP/IPsec PSK」が作成されますので、チェックがついていることを確認します。
   チェックがついていない場合は作成した VPN 構成をタップします。
   そして VPN をオンにし VPN 接続を開始します。
7. VPN 接続完了後は以下のような画面が表示されます。

なお、「状況」をタップすることで IP アドレスなどの VPN 接続情報が表示されます。

3-2. スマートフォンとの L2TP/IPsec 接続設定例(CRT)

この設定例では Android 端末で IPsec で認証に証明書を利用して L2TP/IPsec 接続を行います。なお、キャリアグレード NAT により携帯網側で NAT される可能性がある場合は 3-3. スマートフォンとの L2TP/IPsec NAT トラバーサル接続設定例も参考になりますので、合わせてご参照ください。
また、この設定例は弊社独自の検証結果を元に作成しております。よって、Android のスマートフォンとの接続を保証するものではありません。

【 構成図 】



- 接続してきたスマートフォンには IP アドレスプールより IP アドレスを割り当てます。この設定例では 2 台に IP アドレスを割り当てるため IP アドレスを 2 つ設定し、かつユーザ ID 毎に指定した IP アドレスを割り当てます。
- X.509 で必要となる証明書や鍵は NXR シリーズでは発行をすることができませんので、FutureNet RA シリーズで発行するか、別途 CA 等で用意しておく必要があります。
- 各種証明書は、NXR では FTP などでインポートが可能です。この設定例では FTP サーバからのインポートを行います。証明書を保管しているサーバを 192.168.10.10 とし、サーバには以下の証明書が保管されているものとします。

192.168.10.10 のサーバ	
証明書名	ファイル名
CA 証明書	nxrCA.pem
CRL	nxrCRL.pem
NXR 用証明書	nxrCert.pem
NXR 用秘密鍵	nxrKey.pem

ここでは各証明書の拡張子として pem を使用します。

(☞) 各証明書は DER または PEM フォーマットでなくてはなりません。なおどのフォーマットの証明書かどうかはファイルの拡張子で自動的に判断されます。よって PEM の場合は pem,DER の場合は der また cer の拡張子でなければなりません。
なおシングル DES で暗号化された鍵ファイルは使用することができません。

・ Android では、SD カードのルートディレクトリへのコピーで証明書をインポートすることができます。証明書のインポートについてはご利用機器のマニュアル等をご参照下さい。

【 設定例 】

〔NXR の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR
NXR(config)#interface ethernet 0
NXR(config-if)#ip address 192.168.10.1/24
NXR(config-if)#exit
NXR(config)#ip route 0.0.0.0/0 ppp 0
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 50
NXR(config)#ipsec x509 enable
NXR(config)#ipsec x509 ca-certificate nxrCA ftp://192.168.10.10/nxrCA.pem
NXR(config)#ipsec x509 crl nxrCA ftp://192.168.10.10/nxrCRL.pem
NXR(config)#ipsec x509 certificate nxr ftp://192.168.10.10/nxrCert.pem
NXR(config)#ipsec x509 private-key nxr key ftp://192.168.10.10/nxrKey.pem
NXR(config)#ipsec x509 private-key nxr password nxrpass
NXR(config)#ipsec local policy 1
NXR(config-ipsec-local)#address ip
NXR(config-ipsec-local)#x509 certificate nxr
NXR(config-ipsec-local)#exit
NXR(config)#ipsec isakmp policy 1
NXR(config-ipsec-isakmp)#description smartphone1
NXR(config-ipsec-isakmp)#authentication rsa-sig
NXR(config-ipsec-isakmp)#hash sha1
NXR(config-ipsec-isakmp)#encryption aes128
NXR(config-ipsec-isakmp)#group 5
NXR(config-ipsec-isakmp)#lifetime 86400
NXR(config-ipsec-isakmp)#isakmp-mode main
NXR(config-ipsec-isakmp)#remote address ip any
NXR(config-ipsec-isakmp)#remote identity dn C=JP,CN=smartphone1,E=smartphone@example.com
NXR(config-ipsec-isakmp)#local policy 1
NXR(config-ipsec-isakmp)#exit
NXR(config)#ipsec tunnel policy 1
NXR(config-ipsec-tunnel)#description smartphone
NXR(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR(config-ipsec-tunnel)#no set pfs
NXR(config-ipsec-tunnel)#set sa lifetime 28800
NXR(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR(config-ipsec-tunnel)#match protocol l2tp-smartphone
NXR(config-ipsec-tunnel)#exit
NXR(config)#ipsec isakmp policy 2
NXR(config-ipsec-isakmp)#description smartphone2
NXR(config-ipsec-isakmp)#authentication rsa-sig
NXR(config-ipsec-isakmp)#hash sha1
NXR(config-ipsec-isakmp)#encryption aes128
NXR(config-ipsec-isakmp)#group 5
```

```
NXR(config-ipsec-isakmp)#lifetime 86400
NXR(config-ipsec-isakmp)#isakmp-mode main
NXR(config-ipsec-isakmp)#remote address ip any
NXR(config-ipsec-isakmp)#remote identity dn C=JP,CN=smartphone2,E=smartphone@example.com
NXR(config-ipsec-isakmp)#local policy 1
NXR(config-ipsec-isakmp)#exit
NXR(config)#ipsec tunnel policy 2
NXR(config-ipsec-tunnel)#description smartphone
NXR(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR(config-ipsec-tunnel)#no set pfs
NXR(config-ipsec-tunnel)#set sa lifetime 28800
NXR(config-ipsec-tunnel)#set key-exchange isakmp 2
NXR(config-ipsec-tunnel)#match protocol l2tp-smartphone
NXR(config-ipsec-tunnel)#exit
NXR(config)#ppp account username android01 password android01pass
NXR(config)#ppp account username android02 password android02pass
NXR(config)#ppp account username test1@example.jp password test1pass
NXR(config)#access-server profile 0
NXR(config-ras)#ppp username android01 ip 172.16.0.10
NXR(config-ras)#exit
NXR(config)#access-server profile 1
NXR(config-ras)#ppp username android02 ip 172.16.0.11
NXR(config-ras)#exit
NXR(config)#ip local pool smartphoneip address 172.16.0.10 172.16.0.11
NXR(config)#interface virtual-template 0
NXR(config-if-vt)#ip address 172.16.0.1/32
NXR(config-if-vt)#ip tcp adjust-mss auto
NXR(config-if-vt)#no ip redirects
NXR(config-if-vt)#no ip rebound
NXR(config-if-vt)#peer ip pool smartphoneip
NXR(config-if-vt)#exit
NXR(config)#l2tp udp source-port 1701
NXR(config)#l2tp 1
NXR(config-l2tp)#tunnel address any ipsec
NXR(config-l2tp)#tunnel mode lns
NXR(config-l2tp)#tunnel virtual-template 0
NXR(config-l2tp)#exit
% Restarting l2tp service. Please wait.....
NXR(config)#interface ppp 0
NXR(config-ppp)#ip address 10.10.10.1/32
NXR(config-ppp)#ip masquerade
NXR(config-ppp)#ip access-group in ppp0_in
NXR(config-ppp)#ip spi-filter
NXR(config-ppp)#ip tcp adjust-mss auto
NXR(config-ppp)#no ip redirects
NXR(config-ppp)#ppp username test1@example.jp
NXR(config-ppp)#ipsec policy 1
NXR(config-ppp)#exit
NXR(config)#interface ethernet 1
NXR(config-if)#no ip address
NXR(config-if)#pppoe-client ppp 0
NXR(config-if)#exit
NXR(config)#dns
NXR(config-dns)#service enable
NXR(config-dns)#exit
NXR(config)#fast-forwarding enable
NXR(config)#exit
NXR#save config
```

【 設定例解説 】

〔NXR の設定〕

(☞) ここに記載のない設定項目は 3-1. スマートフォンとの L2TP/IPsec 接続設定例が参考になりますので、そちらをご参照下さい。

1. <X.509 の有効化>

```
NXR(config)#ipsec x509 enable
```

X.509 機能を有効にします。

2. <CA 証明書の設定>

```
NXR(config)#ipsec x509 ca-certificate nxrCA ftp://192.168.10.10/nxrCA.pem
```

FTP サーバ 192.168.10.10 にある CA 証明書ファイル nxrCA.pem をインポートします。

3. <CRL の設定>

```
NXR(config)#ipsec x509 crl nxrCA ftp://192.168.10.10/nxrCRL.pem
```

FTP サーバ 192.168.10.10 にある CRL ファイル nxrCRL.pem をインポートします。

4. <NXR 用公開鍵証明書の設定>

```
NXR(config)#ipsec x509 certificate nxr ftp://192.168.10.10/nxrCert.pem
```

FTP サーバ 192.168.10.10 にある NXR 用公開鍵証明書ファイル nxrCert.pem をインポートします。

5. <NXR 用秘密鍵の設定>

```
NXR(config)#ipsec x509 private-key nxr key ftp://192.168.10.10/nxrKey.pem
```

FTP サーバ 192.168.10.10 にある NXR 用秘密鍵ファイル nxrKey.pem をインポートします。

6. <NXR 用秘密鍵パスフレーズの設定>

```
NXR(config)#ipsec x509 private-key nxr password nxrpass
```

NXR 用秘密鍵のパスフレーズである nxrpass を設定します。

(☞) パスフレーズを暗号化する場合は hidden オプションを設定します。

7. <IPsec ローカルポリシー設定>

```
NXR(config)#ipsec local policy 1
NXR(config-ipsec-local)#address ip
```

IPsec ローカルポリシー1 で IPsec トンネルの送信元 IP アドレスを設定します。

```
NXR(config-ipsec-local)#x509 certificate nxr
```

X.509 で利用する証明書を指定します。ここでは 4. NXR 用公開鍵証明書の設定で設定した certificate name nxr を設定します。

8. <IPsec ISAKMP ポリシー1 設定>

```
NXR(config)#ipsec isakmp policy 1
NXR(config-ipsec-isakmp)#description smartphone
NXR(config-ipsec-isakmp)#authentication rsa-sig
```

スマートフォン 1 との IPsec 接続で使用する ISAKMP ポリシー1 を設定します。
ISAKMP ポリシー1 の説明として smartphone、認証方式として X.509 を利用する場合は rsa-sig を設定します。

```
NXR(config-ipsec-isakmp)#hash sha1
NXR(config-ipsec-isakmp)#encryption aes128
NXR(config-ipsec-isakmp)#group 5
NXR(config-ipsec-isakmp)#lifetime 86400
NXR(config-ipsec-isakmp)#isakmp-mode main
```

認証アルゴリズムとして sha1、暗号化アルゴリズムとして aes128、Diffie-Hellman(DH)グループとして group 5、ISAKMP SA のライフタイムとして 86400 秒、フェーズ 1 のネゴシエーションモードとしてメインモードを設定します。

```
NXR(config-ipsec-isakmp)#remote address ip any
NXR(config-ipsec-isakmp)#remote identity dn C=JP,CN=smartphone1,E=smartphone@example.com
NXR(config-ipsec-isakmp)#local policy 1
```

スマートフォンが動的 IP アドレスのためリモートアドレスを any と設定します。
対向のスマートフォンの identity に関しては DN(Distinguished Name)方式で設定しますので、設定前に対向スマートフォンの証明書の DN または subject 等をご確認下さい。
なお X.509 を利用する場合は、identity 設定は必須になります。
そして IPsec ローカルポリシー1 と関連づけを行います。

9. <IPsec ISAKMP ポリシー2 設定>

```
NXR(config)#ipsec isakmp policy 2
NXR(config-ipsec-isakmp)#description smartphone
NXR(config-ipsec-isakmp)#authentication rsa-sig
```

スマートフォン 2 との IPsec 接続で使用する ISAKMP ポリシー2 を設定します。
ISAKMP ポリシー2 の説明として smartphone、認証方式として X.509 を利用する場合は rsa-sig を設定します。

```
NXR(config-ipsec-isakmp)#hash sha1
NXR(config-ipsec-isakmp)#encryption aes128
NXR(config-ipsec-isakmp)#group 5
NXR(config-ipsec-isakmp)#lifetime 86400
NXR(config-ipsec-isakmp)#isakmp-mode main
```

認証アルゴリズムとして sha1、暗号化アルゴリズムとして aes128、Diffie-Hellman(DH)グループとして group 5、ISAKMP SA のライフタイムとして 86400 秒、フェーズ 1 のネゴシエーションモードとしてメインモードを設定します。

```
NXR(config-ipsec-isakmp)#remote address ip any
NXR(config-ipsec-isakmp)#remote identity dn C=JP,CN=smartphone2,E=smartphone@example.com
NXR(config-ipsec-isakmp)#local policy 1
```

スマートフォンが動的 IP アドレスのためリモートアドレスを any と設定します。
対向のスマートフォンの identity に関しては DN(Distinguished Name)方式で設定しますので、設定前に対向スマートフォンの証明書の DN または subject 等をご確認下さい。
そして IPsec ローカルポリシー1 と関連づけを行います。

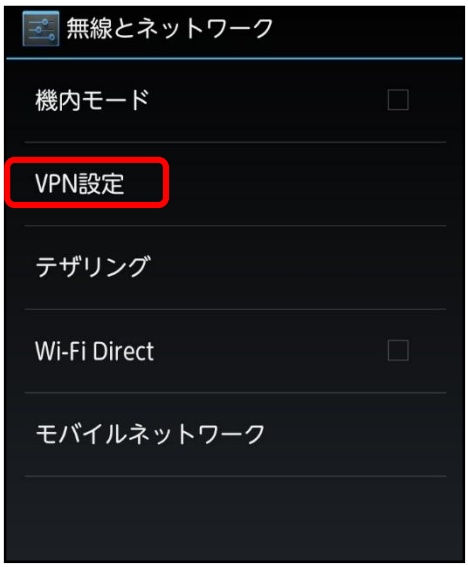
【 スマートフォン設定例 】

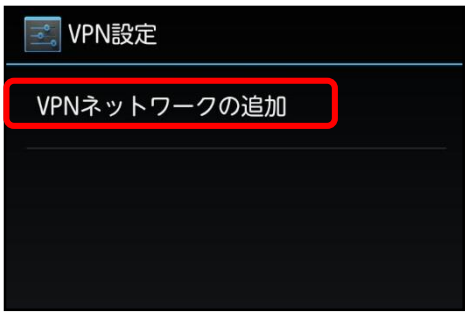
〔Android の設定〕

(☞) ここで記載した設定はあくまで一例ですので、ご利用頂いている Android 端末によって設定が異なる場合があります。設定の詳細はご利用中の Android 端末の取扱説明書等をご確認下さい。
また、証明書は SD カードのルートディレクトリにコピーします。なお、この設定例では証明書はすでにインポート済みとします。

(☞) 本設定例は Android 端末との接続性を保証するものではありません。
ご利用頂く際には十分な検証を行った上でのご利用をお願い致します。

1. メニュー画面から「設定」をタップします。
2. 設定画面で「無線とネットワーク」をタップします。
3. 無線とネットワーク画面で「VPN 設定」をタップします。
4. VPN 設定画面で「VPN ネットワークの追加」をタップします。

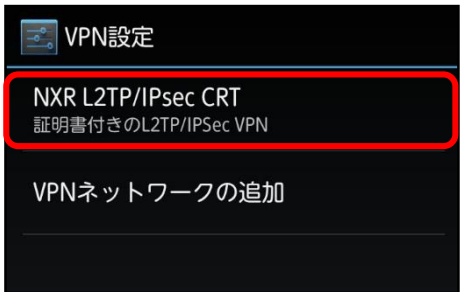




5. VPN ネットワークの編集で次の各項目を設定し保存します。

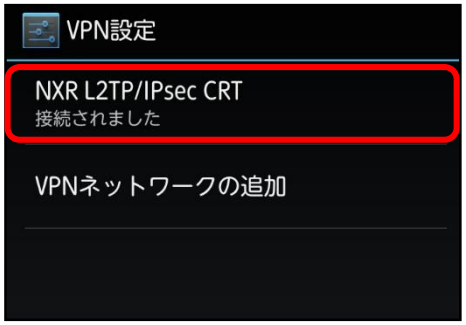
	設定項目	設定値	備考
①	名前	NXR L2TP/IPsec CRT	任意の名称を設定します
②	タイプ	L2TP/IPSec RSA	
③	サーバーアドレス	10.10.10.1	NXR の WAN 側 IP アドレスを設定します
④	L2TP セキュリティ保護	(未使用)	本設定例では使用していません
⑤	IPSec ユーザー証明書	nxr L2TP/IPsec	インポートした証明書を選択します
⑥	IPSecCA 証明書	nxr L2TP/IPsec	インポートした証明書を選択します
⑦	IPSec サーバー証明書	(サーバーから受信)	
⑧	詳細オプションを表示する	無効	

6. VPN 名「NXR L2TP/IPsec CRT」が作成されますので、作成した「NXR L2TP/IPsec CRT」をタップします。



7. ユーザ名とパスワードの入力画面が表示されますので、L2TP/IPsec 用に設定した PPP のユーザ名とパスワードを入力し、接続をタップすると VPN 接続を開始します。

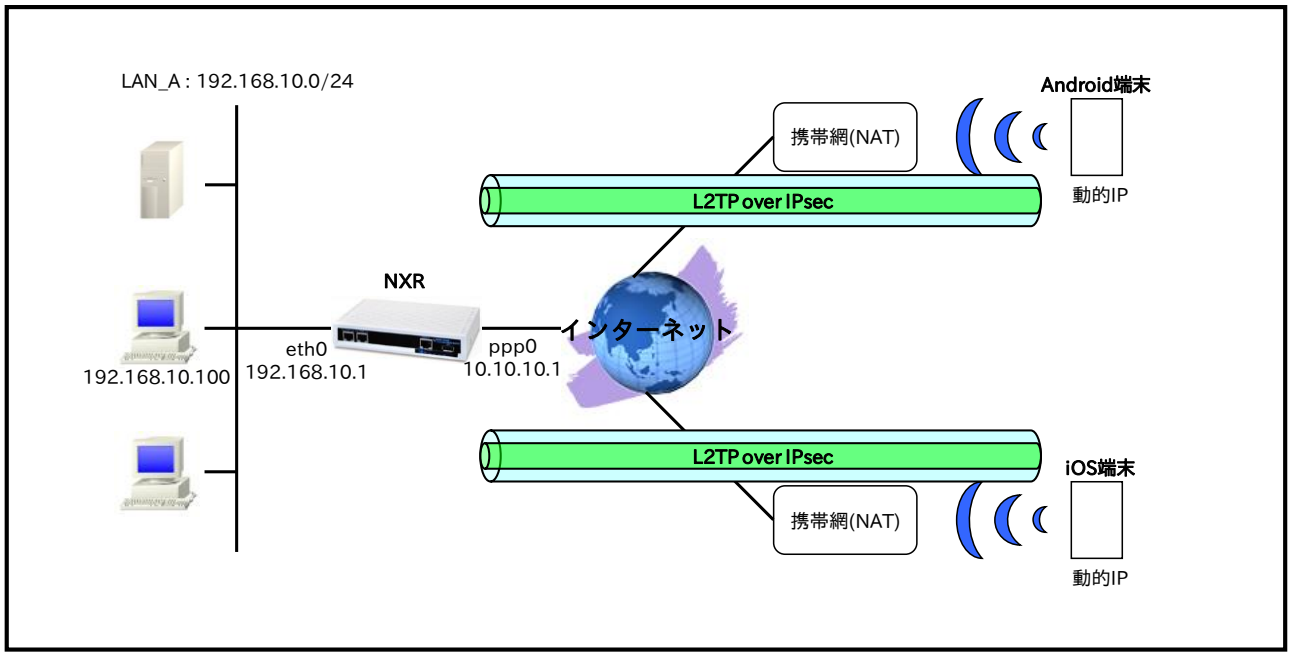
8. 接続が完了(成功)すると VPN 名の下に「接続されました」と表示されます。



3-3. スマートフォンとの L2TP/IPsec NAT トラバーサル接続設定例

Android や iOS のスマートフォンが NAT 環境下にある場合に NXR と L2TP/IPsec 接続する設定例です。携帯網を利用している場合やグローバル IP アドレスが割り当てられないようなケース(キャリアグレード NAT)では、本設定例のような設定をする必要があります。なお、この設定例では IPsec で事前共有鍵を利用して接続を行います。
なお、この設定例は弊社独自の検証結果を元に作成しております。よって、Android や iOS のスマートフォンとの接続を保証するものではありません。

【 構成図 】



- 接続してきたスマートフォンには IP アドレスプールより IP アドレスを割り当てます。この設定例では 2 台分の IP アドレスを設定します。また、接続してきた端末のユーザ ID に対して IP アドレスプールの範囲内から動的に IP アドレスを割り当てます。
- IP アドレスプールの範囲は NXR の LAN 側ネットワーク内のアドレスとするため virtual-template 0 インタフェースでプロキシ ARP を有効にします。

【 設定例 】

〔NXR の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR
NXR(config)#interface ethernet 0
NXR(config-if)#ip address 192.168.10.1/24
NXR(config-if)#exit
NXR(config)#ip route 0.0.0.0/0 ppp 0
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 udp any 500
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 udp any 4500
NXR(config)#ipsec nat-traversal enable
% restart ipsec service to take affect.
NXR(config)#ipsec local policy 1
NXR(config-ipsec-local)#address ip
NXR(config-ipsec-local)#exit
NXR(config)#ipsec isakmp policy 1
NXR(config-ipsec-isakmp)#description smartphone
NXR(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR(config-ipsec-isakmp)#hash sha1
NXR(config-ipsec-isakmp)#encryption aes128
NXR(config-ipsec-isakmp)#group 5
NXR(config-ipsec-isakmp)#lifetime 86400
NXR(config-ipsec-isakmp)#isakmp-mode main
NXR(config-ipsec-isakmp)#remote address ip any
NXR(config-ipsec-isakmp)#local policy 1
NXR(config-ipsec-isakmp)#exit
NXR(config)#ipsec tunnel policy 1
NXR(config-ipsec-tunnel)#description smartphone
NXR(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR(config-ipsec-tunnel)#no set pfs
NXR(config-ipsec-tunnel)#set sa lifetime 28800
NXR(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR(config-ipsec-tunnel)#match protocol l2tp-smartphone nat-traversal
NXR(config-ipsec-tunnel)#exit
NXR(config)#ppp account username android01 password android01pass
NXR(config)#ppp account username ios01 password ios01pass
NXR(config)#ppp account username test1@example.jp password test1pass
NXR(config)#ip local pool smartphoneip address 192.168.10.10 192.168.10.11
NXR(config)#interface virtual-template 0
NXR(config-if-vt)#ip address 192.168.10.1/32
NXR(config-if-vt)#ip tcp adjust-mss auto
NXR(config-if-vt)#no ip redirects
NXR(config-if-vt)#no ip rebound
NXR(config-if-vt)#peer ip pool smartphoneip
NXR(config-if-vt)#peer ip proxy-arp
NXR(config-if-vt)#exit
NXR(config)#l2tp udp source-port 1701
NXR(config)#l2tp 1
NXR(config-l2tp)#tunnel address any ipsec
NXR(config-l2tp)#tunnel mode lns
NXR(config-l2tp)#tunnel virtual-template 0
NXR(config-l2tp)#exit
% Restarting l2tp service. Please wait.....
NXR(config)#interface ppp 0
NXR(config-ppp)#ip address 10.10.10.1/32
NXR(config-ppp)#ip masquerade
NXR(config-ppp)#ip access-group in ppp0_in
NXR(config-ppp)#ip spi-filter
NXR(config-ppp)#ip tcp adjust-mss auto
NXR(config-ppp)#no ip redirects
NXR(config-ppp)#ppp username test1@example.jp
```

```
NXR(config-ppp)#ipsec policy 1
NXR(config-ppp)#exit
NXR(config)#interface ethernet 1
NXR(config-if)#no ip address
NXR(config-if)#pppoe-client ppp 0
NXR(config-if)#exit
NXR(config)#dns
NXR(config-dns)#service enable
NXR(config-dns)#exit
NXR(config)#fast-forwarding enable
NXR(config)#exit
NXR#save config
```

【 設定例解説 】

〔NXR の設定〕

1. <ホスト名の設定>

```
nxr120(config)#hostname NXR
```

ホスト名に NXR を設定します。

2. <LAN 側(ethernet0)インタフェース設定>

```
NXR(config)#interface ethernet 0
NXR(config-if)#ip address 192.168.10.1/24
```

LAN 側(ethernet0)インタフェースの IP アドレスとして 192.168.10.1/24 を設定します。

3. <スタティックルート設定>

```
NXR(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。なおゲートウェイとして ppp0 インタフェースを指定します。

4. <IP アクセスリスト設定>

```
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 udp any 500
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 udp any 4500
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を ppp0_in とします。

一行目は宛先 IP アドレス 10.10.10.1,宛先 UDP ポート番号 500 のパケットを許可する設定です。

二行目は宛先 IP アドレス 10.10.10.1,宛先 UDP ポート番号 4500 のパケットを許可する設定です。

なお、この IP アクセスリスト設定は ppp0 インタフェース設定で登録します。

(☞) IP アクセスリストを設定しただけではフィルタとして有効にはなりません。フィルタリングしたいインタフェースでの登録が必要になります。

(☞) UDP ポート 500 番および 4500 番は IPsec NAT トラバーサルのネゴシエーションおよび通信で使用します。

5. <IPsec NAT トラバーサルの有効化>

```
NXR(config)#ipsec nat-traversal enable
```

NAT トラバーサルを有効にします。

6. <IPsec ローカルポリシー設定>

```
NXR(config)#ipsec local policy 1
NXR(config-ipsec-local)#address ip
```

IPsec ローカルポリシー1 で IPsec トンネルの送信元 IP アドレスを設定します。

7. <IPsec ISAKMP ポリシー設定>

```
NXR(config)#ipsec isakmp policy 1
NXR(config-ipsec-isakmp)#description smartphone
NXR(config-ipsec-isakmp)#authentication pre-share ipseckey
```

スマートフォンとの IPsec 接続で使用する ISAKMP ポリシー1 を設定します。

ISAKMP ポリシー1 の説明として smartphone、認証方式として pre-share(事前共有鍵)を選択し事前共有鍵 ipseckey を設定します。

```
NXR(config-ipsec-isakmp)#hash sha1
NXR(config-ipsec-isakmp)#encryption aes128
NXR(config-ipsec-isakmp)#group 5
NXR(config-ipsec-isakmp)#lifetime 86400
NXR(config-ipsec-isakmp)#isakmp-mode main
```

認証アルゴリズムとして sha1、暗号化アルゴリズムとして aes128，Diffie-Hellman(DH)グループとして group 5、ISAKMP SA のライフタイムとして 86400 秒、フェーズ 1 のネゴシエーションモードとしてメインモードを設定します。

```
NXR(config-ipsec-isakmp)#remote address ip any
NXR(config-ipsec-isakmp)#local policy 1
```

スマートフォンが動的 IP アドレスのためリモートアドレスを any と設定します。

そして IPsec ローカルポリシー1 と関連づけを行います。

8. <IPsec トンネルポリシー設定>

```
NXR(config)#ipsec tunnel policy 1
NXR(config-ipsec-tunnel)#description smartphone
```

スマートフォンとの IPsec 接続で使用するトンネルポリシー1 を設定します。

IPsec トンネルポリシー1 の説明として smartphone と設定します。

```
NXR(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR(config-ipsec-tunnel)#no set pfs
NXR(config-ipsec-tunnel)#set sa lifetime 28800
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を無効、IPsec SA のライフタイムとして 28800 秒を設定します。

```
NXR(config-ipsec-tunnel)#set key-exchange isakmp 1
```

ISAKMP ポリシー1 と関連づけを行います。

```
NXR(config-ipsec-tunnel)#match protocol l2tp-smartphone nat-traversal
```

スマートフォンとの間で L2TPv2 over IPsec 接続する際に設定します。この設定を有効にすると下記の設

定が有効となり、IPsec 接続を行う際に自動設定されます。

・protocol-mode → transport

・negotiation-mode → responder

・IPsec セレクタ → 以下のように自動設定します。また NAT トラバーサル有効時は NAT 配下のどのアドレスからの接続も受け付けます。

ID ペイロード	NXR 側	スマートフォン側
IPv4 アドレス	host	host
プロトコル	UDP	UDP
ポート番号	1701	any(どのポートでも受け付ける)

9. <PPP アカウント設定>

```
NXR(config)#ppp account username android01 password android01pass
NXR(config)#ppp account username ios01 password ios01pass
```

PPP のアカウントを設定します。

ここでは L2TPv2 の LNS 機能による着信時のユーザ ID,パスワードを設定します。

(☞) ここで設定したアカウントはアクセスサーバ設定で利用します。

```
NXR(config)#ppp account username test1@example.jp password test1pass
```

ここでは ppp0 インタフェースで使用するユーザ名,パスワードを設定します。

(☞) ここで設定したアカウントは ppp0 インタフェースの設定で利用します。

10. <IP アドレスプール設定>

```
NXR(config)#ip local pool smartphoneip address 192.168.10.10 192.168.10.11
```

IP アドレスプールを設定します。

ここでは IP アドレスプール名を smartphoneip としスマートフォンに割り当てる 192.168.10.10～192.168.10.11 の IP アドレスを設定します。

11. <virtual-template 0 インタフェース設定>

```
NXR(config)#interface virtual-template 0
```

virtual-template0 インタフェースを設定します。

virtual-template インタフェースは仮想的なインタフェースであり、実際に作成されるわけではありません。virtual-template インタフェースを使用するとコールを受けた際に PPP のクローンを作成し、本ノードの設定内容を当該 PPP に適用します。なお PPP クローンのインタフェース番号は、本装置が自動的に割り当てます。

```
NXR(config-if-vt)#ip address 192.168.10.1/32
```

virtual-template インタフェースの IP アドレスに 192.168.10.1/32 を設定します。

```
NXR(config-if-vt)#ip tcp adjust-mss auto
NXR(config-if-vt)#no ip redirects
NXR(config-if-vt)#no ip rebound
```

TCP MSS の調整機能をオート、ICMP リダイレクト機能を無効、IP リバウンド機能を無効に設定します。

```
NXR(config-if-vt)#peer ip pool smartphoneip
```

使用する IP アドレスプールを設定します。

ここではアクセスサーバ設定で設定した IP アドレスプール名 smartphoneip を設定します。

```
NXR(config-if-vt)#peer ip proxy-arp
```

プロキシ ARP を設定します。

12. <L2TPv2 設定>

```
NXR(config)#l2tp udp source-port 1701
```

L2TPv2 で使用する送信元ポートを 1701 に設定します。

```
NXR(config)#l2tp 1
```

スマートフォンとの接続で使用する L2TP1 を設定します。

```
NXR(config-l2tp)#tunnel mode lns
```

L2TPv2 のトンネルモードを設定します。ここでは LNS を指定します。

```
NXR(config-l2tp)#tunnel address any ipsec
```

接続先に IP アドレスとして any を設定します。

また any 指定時にバインドするプロトコルとして IPsec を指定します。これにより IPsec SA の確立したクライアントからの接続のみを許可します。

```
NXR(config-l2tp)#tunnel virtual-template 0
```

LNS 利用時に使用する virtual-template 0 インタフェースを設定します。

13. <WAN 側(ppp0)インタフェース設定>

```
NXR(config)#interface ppp 0
NXR(config-ppp)#ip address 10.10.10.1/32
```

WAN 側(ppp0)インタフェースを設定します。

IP アドレスを 10.10.10.1/32 に設定します。

```
NXR(config-ppp)#ip masquerade
NXR(config-ppp)#ip access-group in ppp0_in
NXR(config-ppp)#ip spi-filter
NXR(config-ppp)#ip tcp adjust-mss auto
NXR(config-ppp)#no ip redirects
```

IP マスカレードを有効、IP アクセスリスト ppp0_in を in フィルタに適用、ステートフルパケットインスペクションを有効に設定します。

また TCP MSS の調整機能をオート、ICMP リダイレクト機能を無効に設定します。

```
NXR(config-ppp)#ppp username test1@example.jp
NXR(config-ppp)#ipsec policy 1
```

PPPoE 接続で使用するユーザ ID を設定します。

ここでは PPP アカウント設定で作成した test1@example.jp を設定します。

また IPsec トンネルのエンドポイントとなるため IPsec ローカルポリシー1 を設定します。

14. <ethernet1 インタフェース設定>

```
NXR(config)#interface ethernet 1
NXR(config-if)#no ip address
NXR(config-if)#pppoe-client ppp 0
```

ethernet1 インタフェースで、ppp0 インタフェースを PPPoE クライアントとして使用できるよう設定します。

15. <DNS 設定>

```
NXR(config)#dns
NXR(config-dns)#service enable
```

DNS 設定で DNS サービスを有効にします。

16. <ファストフォワーディングの有効化>

```
NXR(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(☞) ファストフォワーディングの詳細および利用時の制約については、NXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

【 スマートフォン設定例 】

〔Android の設定〕

設定は、3-1. スマートフォンとの L2TP/IPsec 接続設定例の〔Android の設定〕と同一ですので、そちらをご参照下さい。

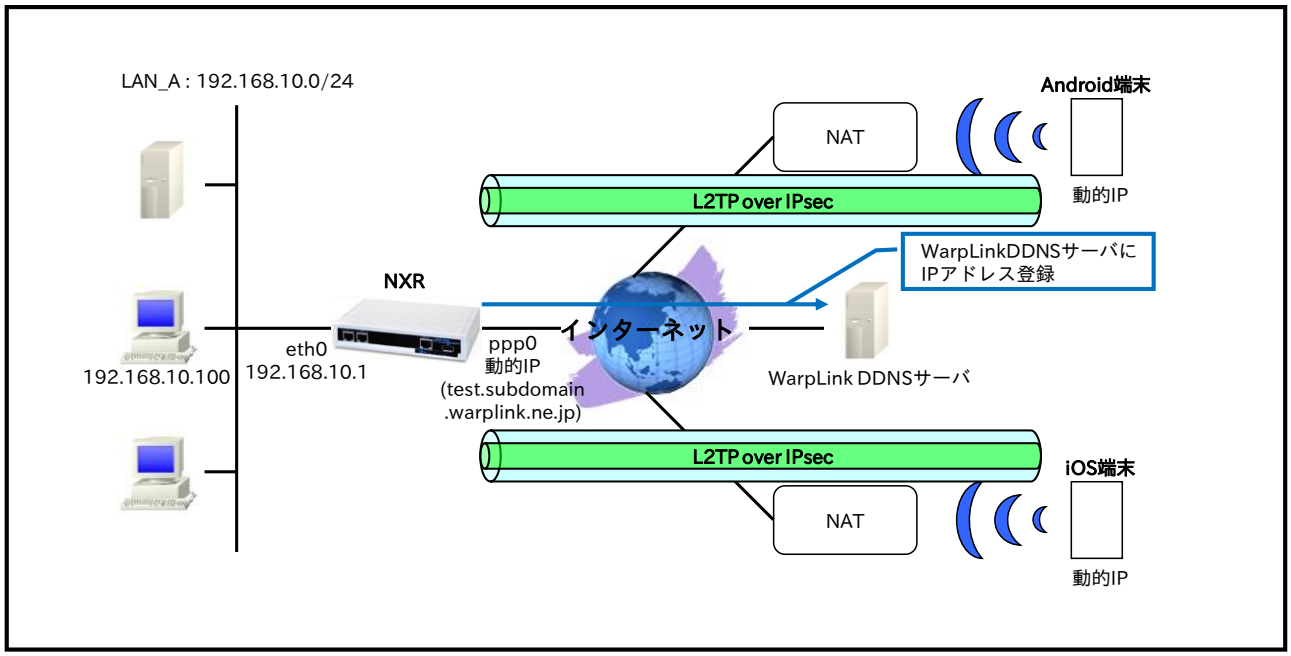
〔iOS の設定〕

設定は、3-1. スマートフォンとの L2TP/IPsec 接続設定例の〔iOS の設定〕と同一ですので、そちらをご参照下さい。

3-4. スマートフォンとの L2TP/IPsec FQDN 接続設定例

この設定例では、ダイナミック DNS を利用してアドレス不定の NXR と Android や iOS のスマートフォンで L2TP/IPsec による通信を行います。ダイナミック DNS を利用することで NXR の WAN 側 IP アドレスが不定の環境でも L2TP/IPsec を利用できます。
ここではダイナミック DNS サービスに弊社が提供している WarpLinkDDNS サービスを使用します。
なお、この設定例は弊社独自の検証結果を元に作成しております。よって、Android や iOS のスマートフォンとの接続を保証するものではありません。

【 構成図 】



- NXR で WarpLink 機能を設定し、WarpLinkDDNS サービスを動作させます。
  (☞) WarpLinkDDNS サービスは弊社が提供している有償の DDNS サービスとなります。
  詳細は下記 URL からご確認下さい。
  http://www.warplink.ne.jp/ddns/index.html
- NXR は自身の IP アドレスを WarpLinkDDNS サーバに登録します。そしてスマートフォンは WarpLinkDDNS サーバに登録されている NXR の FQDN を設定し、その FQDN を DNS サーバに問い合わせし L2TP/IPsec 接続します。
- 3-3. スマートフォンとの L2TP/IPsec NAT トラバーサル接続設定例の内容も参考になりますのでご参照下さい。

【 設定例 】

〔NXR の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR
NXR(config)#interface ethernet 0
NXR(config-if)#ip address 192.168.10.1/24
NXR(config-if)#exit
NXR(config)#ip route 0.0.0.0/0 ppp 0
NXR(config)#ip access-list ppp0_in permit any any udp any 500
NXR(config)#ip access-list ppp0_in permit any any udp any 4500
NXR(config)#ipsec nat-traversal enable
% restart ipsec service to take affect.
NXR(config)#ipsec local policy 1
NXR(config-ipsec-local)#address ip
NXR(config-ipsec-local)#exit
NXR(config)#ipsec isakmp policy 1
NXR(config-ipsec-isakmp)#description smartphone
NXR(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR(config-ipsec-isakmp)#hash sha1
NXR(config-ipsec-isakmp)#encryption aes128
NXR(config-ipsec-isakmp)#group 5
NXR(config-ipsec-isakmp)#lifetime 86400
NXR(config-ipsec-isakmp)#isakmp-mode main
NXR(config-ipsec-isakmp)#remote address ip any
NXR(config-ipsec-isakmp)#local policy 1
NXR(config-ipsec-isakmp)#exit
NXR(config)#ipsec tunnel policy 1
NXR(config-ipsec-tunnel)#description smartphone
NXR(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR(config-ipsec-tunnel)#no set pfs
NXR(config-ipsec-tunnel)#set sa lifetime 28800
NXR(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR(config-ipsec-tunnel)#match protocol l2tp-smartphone nat-traversal
NXR(config-ipsec-tunnel)#exit
NXR(config)#ppp account username android01 password android01pass
NXR(config)#ppp account username ios01 password ios01pass
NXR(config)#ppp account username test1@example.jp password test1pass
NXR(config)#ip local pool smartphoneip address 192.168.10.10 192.168.10.11
NXR(config)#interface virtual-template 0
NXR(config-if-vt)#ip address 192.168.10.1/32
NXR(config-if-vt)#ip tcp adjust-mss auto
NXR(config-if-vt)#no ip redirects
NXR(config-if-vt)#no ip rebound
NXR(config-if-vt)#peer ip pool smartphoneip
NXR(config-if-vt)#peer ip proxy-arp
NXR(config-if-vt)#exit
NXR(config)#l2tp udp source-port 1701
NXR(config)#l2tp 1
NXR(config-l2tp)#tunnel address any ipsec
NXR(config-l2tp)#tunnel mode lns
NXR(config-l2tp)#tunnel virtual-template 0
NXR(config-l2tp)#exit
% Restarting l2tp service. Please wait.....
NXR(config)#interface ppp 0
NXR(config-ppp)#ip address negotiated
NXR(config-ppp)#ip masquerade
NXR(config-ppp)#ip access-group in ppp0_in
NXR(config-ppp)#ip spi-filter
NXR(config-ppp)#ip tcp adjust-mss auto
NXR(config-ppp)#no ip redirects
NXR(config-ppp)#ppp username test1@example.jp
```

```
NXR(config-ppp)#ipsec policy 1
NXR(config-ppp)#exit
NXR(config)#interface ethernet 1
NXR(config-if)#no ip address
NXR(config-if)#pppoe-client ppp 0
NXR(config-if)#exit
NXR(config)#warplink
NXR(config-warplink)#service enable
NXR(config-warplink)#account username warplinksample password warplinksamplepass
NXR(config-warplink)#exit
NXR(config)#dns
NXR(config-dns)#service enable
NXR(config-dns)#exit
NXR(config)#fast-forwarding enable
NXR(config)#exit
NXR#save config
```

【 設定例解説 】

〔NXR の設定〕

(☞) ここに記載のない設定項目は 3-3. スマートフォンとの L2TP/IPsec NAT トラバーサル接続設定例が参考になりますので、そちらをご参照下さい。

1. <IP アクセスリスト設定>

```
NXR(config)#ip access-list ppp0_in permit any any udp any 500
NXR(config)#ip access-list ppp0_in permit any any udp any 4500
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を ppp0_in とします。

一行目は宛先 UDP ポート番号 500 のパケットを許可する設定です。

二行目は宛先 UDP ポート番号 4500 のパケットを許可する設定です。

なお、この IP アクセスリスト設定は ppp0 インタフェース設定で登録します。

(☞) IP アクセスリストを設定しただけではフィルタとして有効にはなりません。フィルタリングしたいインタフェースでの登録が必要になります。

(☞) UDP ポート 500 番および 4500 番は IPsec NAT トラバーサルのネゴシエーションおよび通信で使用します。

2. <WAN 側(ppp0)インタフェース設定>

```
NXR(config)#interface ppp 0
NXR(config-ppp)#ip address negotiated
```

WAN 側(ppp0)インタフェースを設定します。

IP アドレスとして動的 IP アドレスの場合は negotiated を設定します。

```
NXR(config-ppp)#ip masquerade
NXR(config-ppp)#ip access-group in ppp0_in
NXR(config-ppp)#ip spi-filter
NXR(config-ppp)#ip tcp adjust-mss auto
NXR(config-ppp)#no ip redirects
```

IP マスカレードを有効、IP アクセスリスト ppp0_in を in フィルタに適用、ステートフルパケットインス

ペクションを有効に設定します。

また TCP MSS の調整機能をオート、ICMP リダイレクト機能を無効に設定します。

```
NXR(config-ppp)#ppp username test1@example.jp
NXR(config-ppp)#ipsec policy 1
```

PPPoE 接続で使用するユーザ ID を設定します。

また IPsec ローカルポリシー1 を適用します。

3. <WarpLink 設定>

```
NXR(config)#warplink
NXR(config-warplink)#service enable
```

WarpLink 設定で WarpLink サービスを有効にします。

```
NXR(config-warplink)#account username warplinksample password warplinksamplepass
```

WarpLink サービスで使用するユーザ ID,パスワードを設定します。ここでは WarpLink サービスのユーザ ID を warplinksample、パスワードを warplinksamplepass とします。

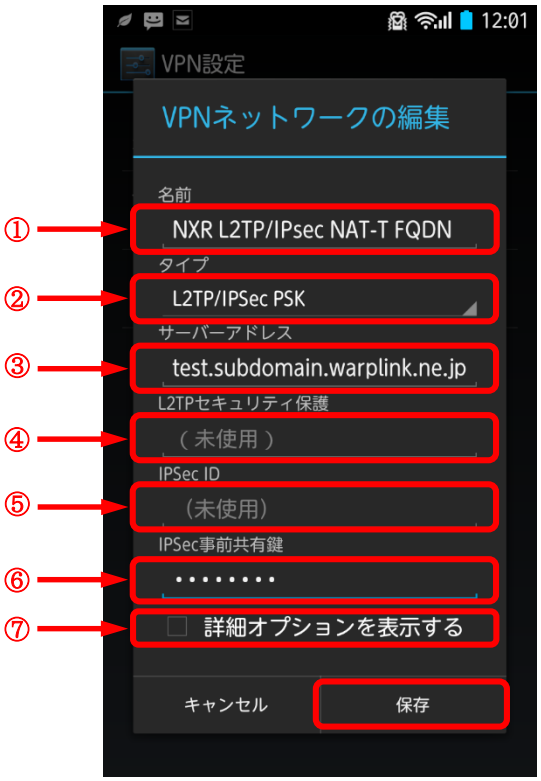
【 スマートフォン設定例 】

〔Android の設定〕

(☞) ここに記載のない設定項目は 3-1. スマートフォンとの L2TP/IPsec 接続設定例の〔Android の設定〕が参考になりますので、そちらをご参照下さい。

(☞) 本設定例は Android 端末との接続性を保証するものではありません。
ご利用頂く際には十分な検証を行った上でのご利用をお願い致します。

VPN ネットワークの編集で以下の各項目を設定し保存します。



	設定項目	設定値	備考
①	名前	NXR L2TP/IPsec PSK	任意の名称を設定します
②	タイプ	L2TP/IPSec PSK	
③	サーバーアドレス	test.subdomain.warplink.ne.jp	NXR の FQDN を設定します
④	L2TP セキュリティ保護	(未使用)	本設定例では使用していません
⑤	IPSec ID	(未使用)	本設定例では使用していません
⑥	IPSec 事前共有鍵	ipseckey	NXR で設定した事前共有鍵を設定します
⑦	詳細オプションを表示する	無効	

〔iOS の設定〕

(☞) ここに記載のない設定項目は 3-1. スマートフォンとの L2TP/IPsec 接続設定例の〔iOS の設定〕が参考になりますので、そちらをご参照下さい。

(☞) 本設定例は iOS 端末との接続性を保証するものではありません。
ご利用頂く際には十分な検証を行った上でのご利用をお願い致します。

構成を追加画面で「L2TP」を選択し以下の各項目を設定し保存します。

	設定項目	設定値	備考
①	説明	NXR L2TP/IPsec PSK	任意の名称を設定します
②	サーバ	test.subdomain.warplink.ne.jp	NXR の FQDN を設定します
③	アカウント	ios01	PPP 認証で使用するアカウントを設定します
④	RSA SecurID	オフ	－
⑤	パスワード	ios01pass	PPP 認証で使用するパスワードを設定します
⑥	シークレット	ipseckey	NXR で設定した事前共有鍵を設定します
⑦	すべての信号を送信	オン	－
⑧	プロキシ	オフ	－

なお、L2TP/IPsec の接続状況は「状況」をタップすることで確認できます。


SoftBank
VPN
15:19
56%
VPN
状況
サーバ test.subdomain.warplink.ne.jp
接続時間
2:19
接続先
192.168.10.1
IPアドレス
192.168.10.10

4. Virtual Private Cloud(VPC)設定

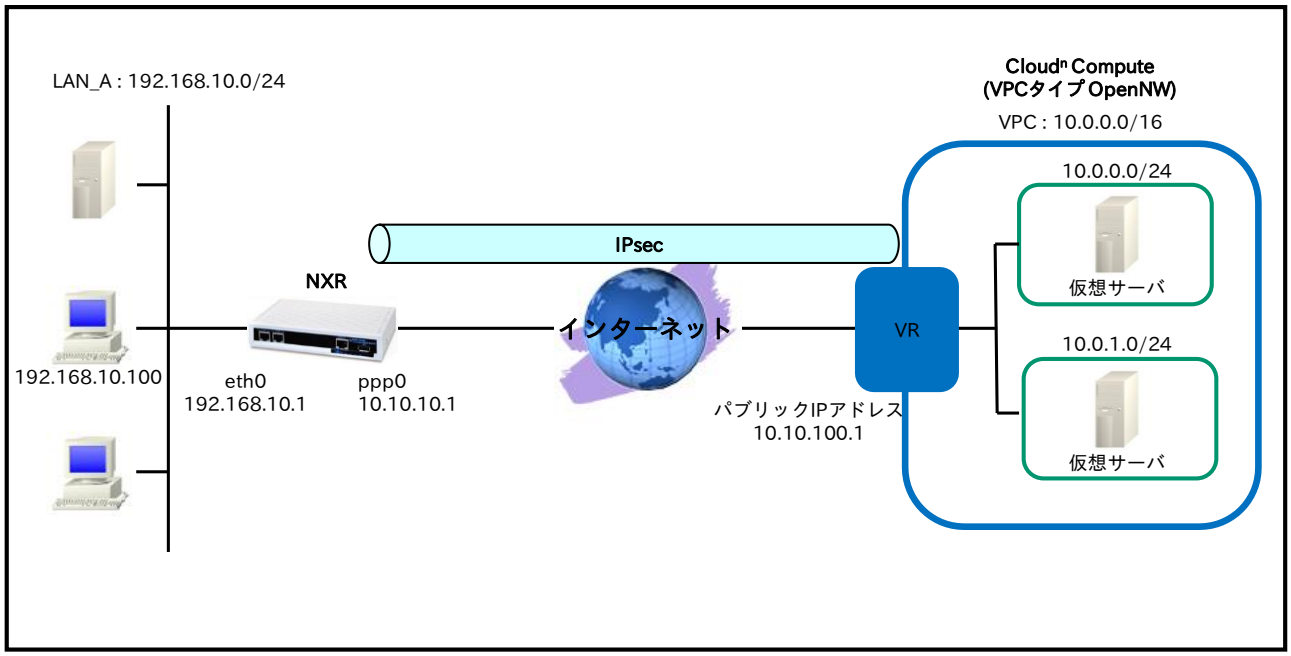
4-1. Cloud^{n} Compute(VPC タイプ OpenNW)接続設定例

「Cloud^{n} Compute(VPC タイプ OpenNW)」(以下 Cloud^{n})は NTT コミュニケーションズ社が提供するクラウド上に論理的なプライベートネットワーク(Virtual Private Cloud)を構築し、その中に Cloud^{n} の仮想サーバーを設置するサービスです。なお、この設定例は弊社独自の検証結果を元に作成しております。よって、Cloud^{n} の仮想ネットワークとの接続を保証するものではありません。

※Cloud^{n} Compute(VPC タイプ OpenNW)に関する情報は下記 URL をご参照ください。

http://www.ntt.com/cloudn/data/server3.html

【 構成図 】



- 本設定例では NXR で Route Based IPsec 設定を行います。
- Cloud^{n} と接続する上で ISAKMP ポリシー(フェーズ１)で以下のプロポーザルを設定します。

認証アルゴリズム	SHA-1
暗号化アルゴリズム	AES-128
Diffie-Hellman(DH)グループ	Group5
対向の認証方式	事前共有鍵(Pre-Shared Key)
ネゴシエーションモード	Main
ライフタイム	10800(s)

トンネルポリシー(フェーズ２)で以下のプロポーザルを設定します。

認証アルゴリズム	SHA1-HMAC
暗号化アルゴリズム	AES128
Diffie-Hellman(DH)グループ	Group5
ライフタイム	3600(s)

・ Cloud^{n} 側の設定については操作マニュアル等をご参照ください。

【 設定例 】

〔NXR の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR
NXR(config)#interface ethernet 0
NXR(config-if)#ip address 192.168.10.1/24
NXR(config-if)#exit
NXR(config)#ip route 10.0.0.0/16 tunnel 1 1
NXR(config)#ip route 10.0.0.0/16 null 254
NXR(config)#ip route 0.0.0.0/0 ppp 0
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 50
NXR(config)#ipsec access-list ipsec_acl ip 192.168.10.0/24 10.0.0.0/16
NXR(config)#ipsec local policy 1
NXR(config-ipsec-local)#address ip
NXR(config-ipsec-local)#exit
NXR(config)#ipsec isakmp policy 1
NXR(config-ipsec-isakmp)#description Cloudn
NXR(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR(config-ipsec-isakmp)#hash sha1
NXR(config-ipsec-isakmp)#encryption aes128
NXR(config-ipsec-isakmp)#group 5
NXR(config-ipsec-isakmp)#lifetime 10800
NXR(config-ipsec-isakmp)#isakmp-mode main
NXR(config-ipsec-isakmp)#remote address ip 10.10.100.1
NXR(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR(config-ipsec-isakmp)#local policy 1
NXR(config-ipsec-isakmp)#exit
NXR(config)#ipsec tunnel policy 1
NXR(config-ipsec-tunnel)#description Cloudn
NXR(config-ipsec-tunnel)#negotiation-mode auto
NXR(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR(config-ipsec-tunnel)#set pfs group5
NXR(config-ipsec-tunnel)#set sa lifetime 3600
NXR(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR(config-ipsec-tunnel)#match address ipsec_acl
NXR(config-ipsec-tunnel)#exit
NXR(config)#interface tunnel 1
NXR(config-tunnel)#tunnel mode ipsec ipv4
NXR(config-tunnel)#tunnel protection ipsec policy 1
NXR(config-tunnel)#ip tcp adjust-mss auto
NXR(config-tunnel)#exit
NXR(config)#interface ppp 0
NXR(config-ppp)#ip address 10.10.10.1/32
NXR(config-ppp)#ip masquerade
NXR(config-ppp)#ip access-group in ppp0_in
NXR(config-ppp)#ip spi-filter
NXR(config-ppp)#ip tcp adjust-mss auto
NXR(config-ppp)#no ip redirects
NXR(config-ppp)#ppp username test1@example.jp password test1pass
NXR(config-ppp)#ipsec policy 1
NXR(config-ppp)#exit
NXR(config)#interface ethernet 1
NXR(config-if)#no ip address
NXR(config-if)#pppoe-client ppp 0
NXR(config-if)#exit
NXR(config)#dns
NXR(config-dns)#service enable
```

```
NXR(config-dns)#exit
NXR(config)#fast-forwarding enable
NXR(config)#exit
NXR#save config
```

【 設定例解説 】

〔NXR の設定〕

1. <ホスト名の設定>

```
nxr120(config)#hostname NXR
```

ホスト名に NXR を設定します。

2. <LAN 側(ethernet0)インタフェース設定>

```
NXR(config)#interface ethernet 0
NXR(config-if)#ip address 192.168.10.1/24
```

LAN 側(ethernet0)インタフェースの IP アドレスに 192.168.10.1/24 を設定します。

3. <スタティックルート設定>

```
NXR(config)#ip route 10.0.0.0/16 tunnel 1 1
```

Cloud[n] の VPC 向け 10.0.0.0/16 のルートを設定します。なお、ゲートウェイインタフェースは tunnel 1 を設定します。また、このルートのディスタンス値として 1 を設定します。

(☞) これは IPsec で使用するスタティックルートであり、ここで設定した宛先 IP アドレスにマッチしたパケットが IPsec のカプセル化対象となります。なおゲートウェイアドレスは IPsec で使用するトンネルインタフェースを設定します。

```
NXR(config)#ip route 10.0.0.0/16 null 254
```

Cloud[n] の VPC 向け 10.0.0.0/16 のルートを設定します。ただし、ゲートウェイインタフェースは null を設定します。また、このルートのディスタンス値として 254 を設定します。

(☞) null インタフェースを出力インタフェースとして設定した場合、パケットが出力されることはありません(ドロップされます)。よってパケット出力を行う場合は null インタフェースよりもディスタンス値が小さいルートを設定する必要があります。

```
NXR_B(config)#ip route 0.0.0.0/0 ppp 0
```

デフォルトルートを設定します。なおゲートウェイとして ppp0 インタフェースを指定します。

4. <IP アクセスリスト設定>

```
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 50
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を ppp0_in とします。

一行目は宛先 IP アドレス 10.10.10.1,送信元 UDP ポート番号 500,宛先 UDP ポート番号 500 のパケットを許可する設定です。

二行目は宛先 IP アドレス 10.10.10.1,プロトコル番号 50(ESP)のパケットを許可する設定です。

この IP アクセスリスト設定は ppp0 インタフェース設定で登録します。

(☞) UDP ポート 500 番およびプロトコル番号 50(ESP)は IPsec のネゴシエーションおよび通信で使用します。

5. <IPsec アクセスリスト設定>

```
NXR(config)#ipsec access-list ipsec_acl ip 192.168.10.0/24 10.0.0.0/16
```

IPsec アクセスリスト名を ipsec_acl とし、送信元 IP アドレス 192.168.10.0/24,宛先 IP アドレス 10.0.0.0/16 を設定します。

(☞) NXR 同士の Route Based IPsec 接続では送信元 IP アドレス,宛先 IP アドレスに any を使用しました。しかし Cloud[n] との接続のためには上記のようなネットワークを指定した IPsec アクセスリストが必要となります。

6. <IPsec ローカルポリシー設定>

```
NXR(config)#ipsec local policy 1
NXR(config-ipsec-local)#address ip
```

IPsec ローカルポリシー1 で IPsec トンネルの送信元 IP アドレスを設定します。

7. <IPsec ISAKMP ポリシー設定>

```
NXR(config)#ipsec isakmp policy 1
NXR(config-ipsec-isakmp)#description Cloudn
NXR(config-ipsec-isakmp)#authentication pre-share ipseckey
```

Cloud[n] との IPsec 接続で使用する ISAKMP ポリシー1 を設定します。
ISAKMP ポリシー1 の説明として Cloudn、認証方式として pre-share(事前共有鍵)を選択し事前共有鍵 ipseckey を設定します。

```
NXR(config-ipsec-isakmp)#hash sha1
NXR(config-ipsec-isakmp)#encryption aes128
NXR(config-ipsec-isakmp)#group 5
NXR(config-ipsec-isakmp)#lifetime 10800
NXR(config-ipsec-isakmp)#isakmp-mode main
```

認証アルゴリズムとして sha1、暗号化アルゴリズムとして aes128、Diffie-Hellman(DH)グループとして group 5、ISAKMP SA のライフタイムとして 10800 秒、フェーズ 1 のネゴシエーションモードとしてメインモードを設定します。

(☞) Cloud[n] との接続にはメインモードである必要があります。(2014 年 1 月現在)

```
NXR(config-ipsec-isakmp)#remote address ip 10.10.100.1
NXR(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR(config-ipsec-isakmp)#local policy 1
```

Cloud[n] の WAN 側 IP アドレス 10.10.100.1、IKE KeepAlive(DPD)を監視間隔 30 秒,リトライ回数 3 回とし keepalive 失敗時に SA を削除し IKE のネゴシエーションを開始するよう設定します。
そして IPsec ローカルポリシー1 と関連づけを行います。

8. <IPsec トンネルポリシー設定>

```
NXR(config)#ipsec tunnel policy 1
NXR(config-ipsec-tunnel)#description Cloudn
NXR(config-ipsec-tunnel)#negotiation-mode auto
```

Cloud[n]との IPsec 接続で使用するトンネルポリシー1 を設定します。

IPsec トンネルポリシー1 の説明として Cloudn、ネゴシエーションモードとして auto を設定します。

```
NXR(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR(config-ipsec-tunnel)#set pfs group5
NXR(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効とし、かつ DH グループとして group5、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR(config-ipsec-tunnel)#match address ipsec_acl
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

9. <トンネルインタフェース設定>

```
NXR(config)#interface tunnel 1
NXR(config-tunnel)#tunnel mode ipsec ipv4
NXR(config-tunnel)#tunnel protection ipsec policy 1
NXR(config-tunnel)#ip tcp adjust-mss auto
```

トンネル 1 インタフェースでトンネルモードを ipsec ipv4、使用するトンネルポリシーとして 1 を設定します。また TCP MSS の調整機能をオートに設定します。

10. <WAN 側(ppp0)インタフェース設定>

```
NXR(config)#interface ppp 0
NXR(config-ppp)#ip address 10.10.10.1/32
```

WAN 側(ppp0)インタフェースを設定します。

IP アドレスとして固定 IP アドレス 10.10.10.1/32 を設定します。

```
NXR(config-ppp)#ip masquerade
NXR(config-ppp)#ip access-group in ppp0_in
NXR(config-ppp)#ip spi-filter
NXR(config-ppp)#ip tcp adjust-mss auto
NXR(config-ppp)#no ip redirects
```

IP マスカレードを有効、IP アクセスリスト ppp0_in を in フィルタに適用、ステートフルパケットインスペクションを有効に設定します。

また TCP MSS の調整機能をオート、ICMP リダイレクト機能を無効に設定します。

```
NXR(config-ppp)#ppp username test1@example.jp password test1pass
NXR(config-ppp)#ipsec policy 1
```

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

また IPsec トンネルのエンドポイントとなるため IPsec ローカルポリシー1 を設定します。

11. <ethernet1 インタフェース設定>

```
NXR(config)#interface ethernet 1
NXR(config-if)#no ip address
NXR(config-if)#pppoe-client ppp 0
```

ethernet1 インタフェースで、ppp0 インタフェースを PPPoE クライアントとして使用できるよう設定します。

12. <DNS 設定>

```
NXR(config)#dns
NXR(config-dns)#service enable
```

DNS 設定で DNS サービスを有効にします。

13. <ファストフォワーディングの有効化>

```
NXR(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(☞) ファストフォワーディングの詳細および利用時の制約については、NXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

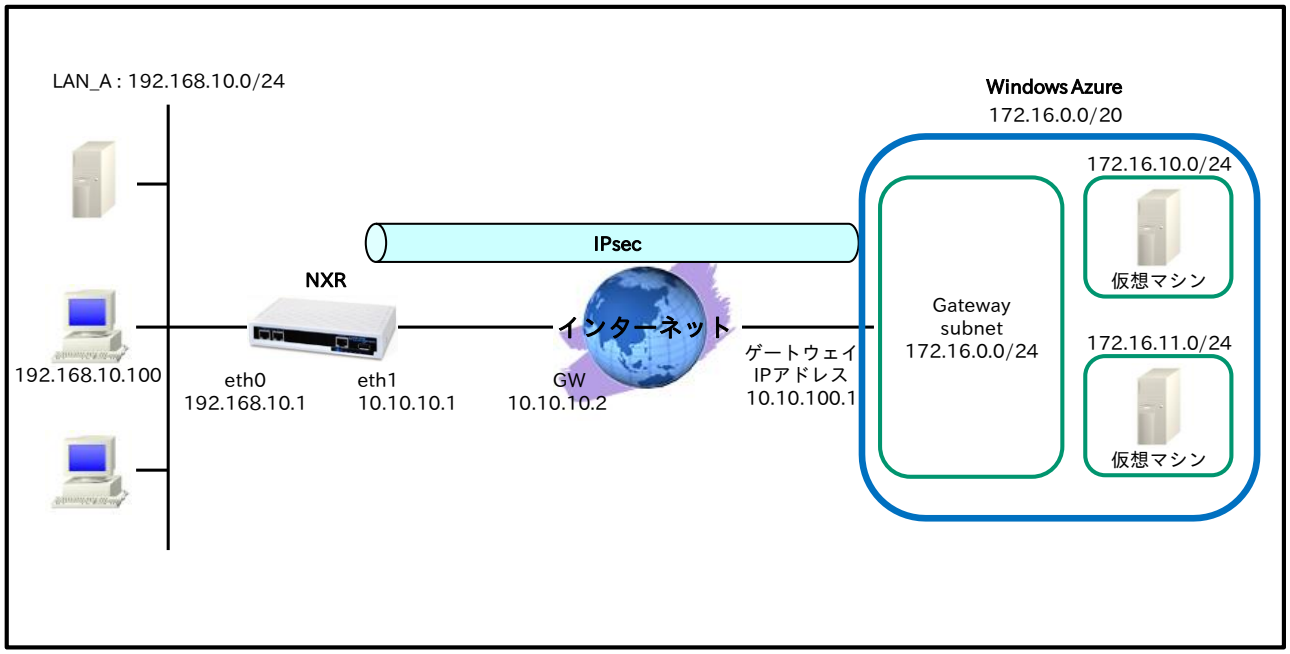
【 パソコンの設定例 】

	LAN A のパソコン
IP アドレス	192.168.10.100
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	192.168.10.1
DNS サーバアドレス	192.168.10.1

4-2. Windows Azure 接続設定例

Windows Azure は、Microsoft 社が提供するクラウド上に論理的なプライベートネットワーク(Virtual Private Cloud)を構築するサービスです。
なお、この設定例は弊社独自の検証結果を元に作成しております。よって、Windows Azure の仮想ネットワークとの接続を保証するものではありません。
※Windows Azure に関する情報は下記 URL をご参照ください。
http://www.windowsazure.com/ja-jp/

【 構成図 】



- 本設定例では NXR で Route Based IPsec 設定を行います。
- Windows Azure との接続に ISAKMP ポリシー(フェーズ 1)で以下のプロポーザルを設定します。

認証アルゴリズム	SHA-1
暗号化アルゴリズム	AES-256
Diffie-Hellman(DH)グループ	Group2
対向の認証方式	事前共有鍵(Pre-Shared Key)
ネゴシエーションモード	Main
ライフタイム	28800(s)

トンネルポリシー(フェーズ 2)で以下のプロポーザルを設定します。

認証アルゴリズム	SHA1-HMAC
暗号化アルゴリズム	AES256
ライフタイム	3600(s)

- Windows Azure 側の設定については設定マニュアル等をご参照ください。

【 設定例 】

〔NXR の設定〕

```
nxr125#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr125(config)#hostname NXR
NXR(config)#interface ethernet 0
NXR(config-if)#ip address 192.168.10.1/24
NXR(config-if)#exit
NXR(config)#ip route 172.16.0.0/20 tunnel 1 1
NXR(config)#ip route 172.16.0.0/20 null 254
NXR(config)#ip route 0.0.0.0/0 10.10.10.2
NXR(config)#ip access-list eth1_in permit any 10.10.10.1 udp any 500
NXR(config)#ip access-list eth1_in permit any 10.10.10.1 udp any 4500
NXR(config)#ip access-list eth1_in permit any 10.10.10.1 50
NXR(config)#ipsec access-list ipsec_acl ip 192.168.10.0/24 172.16.0.0/20
NXR(config)#ipsec nat-traversal enable
% restart ipsec service to take affect.
NXR(config)#ipsec local policy 1
NXR(config-ipsec-local)#address ip
NXR(config-ipsec-local)#exit
NXR(config)#ipsec isakmp policy 1
NXR(config-ipsec-isakmp)#description WindowsAzure
NXR(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR(config-ipsec-isakmp)#hash sha1
NXR(config-ipsec-isakmp)#encryption aes256
NXR(config-ipsec-isakmp)#group 2
NXR(config-ipsec-isakmp)#lifetime 28800
NXR(config-ipsec-isakmp)#isakmp-mode main
NXR(config-ipsec-isakmp)#remote address ip 10.10.100.1
NXR(config-ipsec-isakmp)#no keepalive
NXR(config-ipsec-isakmp)#local policy 1
NXR(config-ipsec-isakmp)#exit
NXR(config)#ipsec tunnel policy 1
NXR(config-ipsec-tunnel)#description WindowsAzure
NXR(config-ipsec-tunnel)#negotiation-mode auto
NXR(config-ipsec-tunnel)#set transform esp-aes256 esp-sha1-hmac
NXR(config-ipsec-tunnel)#no set pfs
NXR(config-ipsec-tunnel)#set sa lifetime 3600
NXR(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR(config-ipsec-tunnel)#match address ipsec_acl
NXR(config-ipsec-tunnel)#exit
NXR(config)#interface tunnel 1
NXR(config-tunnel)#tunnel mode ipsec ipv4
NXR(config-tunnel)#tunnel protection ipsec policy 1
NXR(config-tunnel)#ip tcp adjust-mss 1350
NXR(config-tunnel)#exit
NXR(config)#interface ethernet 1
NXR(config-if)#ip address 10.10.10.1/30
NXR(config-if)#ip masquerade
NXR(config-if)#ip access-group in eth1_in
NXR(config-if)#ip spi-filter
NXR(config-if)#ip tcp adjust-mss auto
NXR(config-if)#no ip redirects
NXR(config-if)#ipsec policy 1
NXR(config-if)#exit
NXR(config)#dns
NXR(config-dns)#service enable
NXR(config-dns)#address 10.255.1.1
NXR(config-dns)#exit
NXR(config)#fast-forwarding enable
NXR(config)#exit
NXR#save config
```

【 設定例解説 】

〔NXR の設定〕

1. <ホスト名の設定>

```
nxr125(config)#hostname NXR
```

ホスト名に NXR を設定します。

2. <LAN 側(ethernet0)インタフェース設定>

```
NXR(config)#interface ethernet 0
NXR(config-if)#ip address 192.168.10.1/24
```

LAN 側(ethernet0)インタフェースの IP アドレスとして 192.168.10.1/24 を設定します。

3. <スタティックルート設定>

```
NXR(config)#ip route 172.16.0.0/20 tunnel 1 1
```

Windows Azure 向け 172.16.0.0/20 のルートを設定します。なおゲートウェイインタフェースは tunnel 1 を設定します。またこのルートのディスタンス値として 1 を設定します。

(☞) これは IPsec で使用するスタティックルートであり、ここで設定した宛先 IP アドレスにマッチしたパケットが IPsec のカプセル化対象となります。なおゲートウェイアドレスは IPsec で使用するトンネルインタフェースを設定します。

```
NXR(config)#ip route 172.16.0.0/20 null 254
```

Windows Azure 向け 172.16.0.0/20 のルートを設定します。ただしゲートウェイインタフェースは null を設定します。またこのルートのディスタンス値として 254 を設定します。

(☞) null インタフェースを出力インタフェースとして設定した場合、パケットが出力されることはありません(ドロップされます)。よってパケット出力を行う場合は null インタフェースよりもディスタンス値が小さいルートを設定する必要があります。

```
NXR(config)#ip route 0.0.0.0/0 10.10.10.2
```

デフォルトルートを設定します。なおゲートウェイアドレスは、プロバイダより指定された上位ルータの IP アドレスを設定します。この設定例では、10.10.10.2 とします。

4. <IP アクセスリスト設定>

```
NXR(config)#ip access-list eth1_in permit any 10.10.10.1 udp any 500
NXR(config)#ip access-list eth1_in permit any 10.10.10.1 udp any 4500
NXR(config)#ip access-list eth1_in permit any 10.10.10.1 50
```

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を eth1_in とします。

一行目は宛先 IP アドレス 10.10.10.1,宛先 UDP ポート番号 500 のパケットを許可する設定です。

二行目は宛先 IP アドレス 10.10.10.1,宛先 UDP ポート番号 4500 のパケットを許可する設定です。

三行目は宛先 IP アドレス 10.10.10.1,プロトコル番号 50(ESP)のパケットを許可する設定です。

この IP アクセスリスト設定は eth1 インタフェース設定で登録します。

5. <IPsec アクセスリスト設定>

```
NXR(config)#ipsec access-list ipsec_acl ip 192.168.10.0/24 172.16.0.0/20
```

IPsec アクセスリスト名を ipsec_acl とし、送信元 IP アドレス 192.168.10.0/24,宛先 IP アドレス 172.16.0.0/20 を設定します。

6. <IPsec NAT トラバーサル設定>

```
NXR(config)#ipsec nat-traversal enable
```

NAT トラバーサルを有効にします。

7. <IPsec ローカルポリシー設定>

```
NXR(config)#ipsec local policy 1
NXR(config-ipsec-local)#address ip
```

IPsec ローカルポリシー1 で IPsec トンネルの送信元 IP アドレスを設定します。

8. <IPsec ISAKMP ポリシー設定>

```
NXR(config)#ipsec isakmp policy 1
NXR(config-ipsec-isakmp)#description WindowsAzure
NXR(config-ipsec-isakmp)#authentication pre-share ipseckey
```

Windows Azure との IPsec 接続で使用する ISAKMP ポリシー1 を設定します。
ISAKMP ポリシー1 の説明として WindowsAzure、認証方式として pre-share(事前共有鍵)を選択し事前共有鍵 ipseckey を設定します。
(☞) 事前共有鍵は Windows Azure で自動生成された値を設定します。

```
NXR(config-ipsec-isakmp)#hash sha1
NXR(config-ipsec-isakmp)#encryption aes256
NXR(config-ipsec-isakmp)#group 2
NXR(config-ipsec-isakmp)#lifetime 28800
NXR(config-ipsec-isakmp)#isakmp-mode main
```

認証アルゴリズムとして sha1、暗号化アルゴリズムとして aes256、Diffie-Hellman(DH)グループとして group 2、ISAKMP SA のライフタイムとして 28800 秒、フェーズ 1 のネゴシエーションモードとしてメインモードを設定します。

```
NXR(config-ipsec-isakmp)#remote address ip 10.10.100.1
NXR(config-ipsec-isakmp)#no keepalive
NXR(config-ipsec-isakmp)#local policy 1
```

Windows Azure の WAN 側 IP アドレス 10.10.100.1、IKE KeepAlive(DPD)を無効に設定します。
そして IPsec ローカルポリシー1 と関連づけを行います。

9. <IPsec トンネルポリシー設定>

```
NXR(config)#ipsec tunnel policy 1
NXR(config-ipsec-tunnel)#description WindowsAzure
NXR(config-ipsec-tunnel)#negotiation-mode auto
```

Windows Azure との IPsec 接続で使用するトンネルポリシー1 を設定します。IPsec トンネルポリシー1 の説明として WindowsAzure、ネゴシエーションモードとして auto を設定します。

```
NXR(config-ipsec-tunnel)#set transform esp-aes256 esp-sha1-hmac
NXR(config-ipsec-tunnel)#no set pfs
NXR(config-ipsec-tunnel)#set sa lifetime 3600
```

暗号化アルゴリズムとして aes256、認証アルゴリズムとして sha1、PFS を無効、IPsec SA のライフタイムとして 3600 秒を設定します。

```
NXR(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR(config-ipsec-tunnel)#match address ipsec_acl
```

ISAKMP ポリシー1 と関連づけを行い、IPsec アクセスリストとして ipsec_acl を設定します。

10. <トンネルインタフェース設定>

```
NXR(config)#interface tunnel 1
NXR(config-tunnel)#tunnel mode ipsec ipv4
NXR(config-tunnel)#tunnel protection ipsec policy 1
NXR(config-tunnel)#ip tcp adjust-mss 1350
```

トンネル 1 インタフェースでトンネルモードを ipsec ipv4、使用するトンネルポリシーとして 1 を設定します。また TCP MSS 値を 1350 に設定します。

11. <WAN 側(eth1)インタフェース設定>

```
NXR(config)#interface ethernet 1
NXR(config-if)#ip address 10.10.10.1/30
```

WAN 側(eth1)インタフェースを設定します。

IP アドレスとして固定 IP アドレス 10.10.10.1/30 を設定します。

```
NXR(config-if)#ip masquerade
NXR(config-if)#ip access-group in eth1_in
NXR(config-if)#ip spi-filter
NXR(config-if)#ip tcp adjust-mss auto
NXR(config-if)#no ip redirects
```

IP マスカレードを有効、IP アクセスリスト eth1_in を in フィルタに適用、ステートフルパケットインスペクションを有効に設定します。

また TCP MSS の調整機能をオート、ICMP リダイレクト機能を無効に設定します。

```
NXR(config-if)#ipsec policy 1
```

IPsec トンネルのエンドポイントとなるため IPsec ローカルポリシー1 を設定します。

12. <DNS 設定>

```
NXR(config)#dns
NXR(config-dns)#service enable
```

DNS 設定で DNS サービスを有効にします。

```
NXR(config-dns)#address 10.255.1.1
```

プロバイダから通知されている DNS サーバアドレスを設定します。この設定例では、DNS サーバアドレスとして 10.255.1.1 を設定します。

13. <ファストフォワーディングの有効化>

```
NXR(config)#fast-forwarding enable
```

ファストフォワーディングを有効にします。ファストフォワーディングを設定することによりパケット転送の高速化を行うことができます。

(☞) ファストフォワーディングの詳細および利用時の制約については、NXR シリーズのユーザーズガイド(CLI 版)に記載されているファストフォワーディングの解説をご参照ください。

【 パソコンの設定例 】

	LAN A のパソコン
IP アドレス	192.168.10.100
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	192.168.10.1
DNS サーバアドレス	192.168.10.1

付録

IPsec 接続確認方法

● ステータスの確認

IPsec の各トンネル状況を一覧で確認する場合は、show ipsec status brief コマンドを使用します。

<実行例>

```
nxr120#show ipsec status brief
TunnelName          Status
tunnel1             up
tunnel2             down
```

IPsec SA が確立している(IPsec established)ものを up,それ以外を down として表示します。

IPsec の SA 確立状況等を確認する場合は、show ipsec status コマンドを使用します。また show ipsec status コマンドの後に tunnel <ポリシー番号>を指定することにより tunnel ポリシー毎にステータスを表示させることができます。これは多拠点収容構成で個々のポリシーを確認するのに有効です。

<実行例>

```
nxr120#show ipsec status
000 "tunnel1":192.168.30.0/24===10.10.30.1[nxrc]...10.10.10.1[10.10.10.1]===192.168.10.0/24; erouted;
eroute owner: #2
000 "tunnel1":     ike_life: 10800s; ipsec_life: 3600s; margin: 270s; inc_ratio: 100%
000 "tunnel1":     newest ISAKMP SA: #1; newest IPsec SA: #2;
000 "tunnel1":     IKE proposal: AES_CBC_128/HMAC_SHA1/MODP_1536
000 "tunnel1":     ESP proposal: AES_CBC_128/HMAC_SHA1/MODP_1536
000
000 #2: "tunnel1" STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in 3212s; newest
IPSEC; eroute owner
000 #2: "tunnel1" esp.7a5cb4c1@10.10.10.1 (0 bytes) esp.9867e772@10.10.30.1 (0 bytes); tunnel
000 #1: "tunnel1" STATE_AGGR_I2 (sent AI2, ISAKMP SA established); EVENT_SA_REPLACE in 10291s;
newest ISAKMP
000
Connections:
Security Associations:
   none
```

● ログの確認

ログは show syslog message コマンドで確認することができます。

(☞) ここで設定しているシスログのプライオリティは info(初期値)となります。このプライオリティを debug に変更することによりより多くのログが出力されます。

IPsec 接続完了時には以下のようなログが出力されます。

➢イニシエータでメインモード利用時

<出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Main Mode
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [strongSwan]
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [XAUTH]
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "tunnel1" #1: ISAKMP SA established
pluto[XXXX]: "tunnel1" #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP {using isakmp#1}
charon: 03[KNL] interface tunnel1 activated
pluto[XXXX]: "tunnel1" #2: sent QI2, IPsec SA established {ESP=>0x14bd33f0 <0xf49c1f56 DPD}
```

➢レスポンダでメインモード利用時

<出力例>

```
pluto[XXXX]: packet from 10.10.10.1:500: received Vendor ID payload [strongSwan]
pluto[XXXX]: packet from 10.10.10.1:500: received Vendor ID payload [XAUTH]
pluto[XXXX]: packet from 10.10.10.1:500: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "tunnel1" #3: responding to Main Mode
pluto[XXXX]: "tunnel1" #3: sent MR3, ISAKMP SA established
pluto[XXXX]: "tunnel1" #3: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1" #4: responding to Quick Mode
charon: 03[KNL] interface tunnel1 activated
pluto[XXXX]: "tunnel1" #4: IPsec SA established {ESP=>0x9c4fb981 <0xc30f38e1 DPD}
```

➢イニシエータでアグレッシブモード利用時

<出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [strongSwan]
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [XAUTH]
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "tunnel1" #1: sent AI2, ISAKMP SA established
pluto[XXXX]: "tunnel1" #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP+0x4000000
  {using isakmp#1}
charon: 03[KNL] interface tunnel1 activated
pluto[XXXX]: "tunnel1" #2: sent QI2, IPsec SA established {ESP=>0xc5e28ab0 <0x899ed286 DPD}
```

➢レスポンダでアグレッシブモード利用時

<出力例>

```
pluto[XXXX]: packet from 10.10.30.1:500: received Vendor ID payload [strongSwan]
pluto[XXXX]: packet from 10.10.30.1:500: received Vendor ID payload [XAUTH]
pluto[XXXX]: packet from 10.10.30.1:500: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "tunnel1"[1] 10.10.30.1 #1: responding to Aggressive Mode from unknown peer 10.10.30.1
pluto[XXXX]: "tunnel1"[1] 10.10.30.1 #1: ISAKMP SA established
pluto[XXXX]: "tunnel1"[1] 10.10.30.1 #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1"[1] 10.10.30.1 #2: responding to Quick Mode
charon: 03[KNL] interface tunnel1 activated
pluto[XXXX]: "tunnel1"[1] 10.10.30.1 #2: IPsec SA established {ESP=>0x899ed286 <0xc5e28ab0 DPD}
```

「ISAKMP SA established」が ISAKMP SA が確立したことを、「IPsec SA established」が IPsec SA が確立したことを示しています。

IPsec 接続が失敗する時に出力されるログとして以下のようなものが挙げられます。

➢対向機器からの応答がない(メインモード)

<イニシエータ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Main Mode
・・・
pluto[XXXX]: "tunnel1" #1: max number of retransmissions (20) reached STATE_MAIN_I1.  No response(or
no acceptable response) to our first IKE message
pluto[XXXX]: "tunnel1" #1: starting keying attempt 2 of an unlimited number
pluto[XXXX]: "tunnel1" #2: initiating Main Mode to replace #1
```

(☞) 対向ルータの WAN 回線が接続されているか、パケットが届いているか、IPsec のフィルタ(UDP500)は許可されているか、IPsec サービスが起動しているか、対向ルータで該当する IPsec 設定が正しく設定されているかなどを確認してください。

➢対向機器からの応答がない(アグレッシブモード)

<イニシエータ側のログ出力例>

```
pluto[XXXX]: “tunnel1” #1: initiating Aggressive Mode #1, connection "tunnel1"
・・・
pluto[XXXX]: "tunnel1" #1: max number of retransmissions (20) reached STATE_AGGR_I1
pluto[XXXX]: "tunnel1" #1: starting keying attempt 2 of an unlimited number
pluto[XXXX]: "tunnel1" #2: initiating Aggressive Mode #2 to replace #1, connection "tunnel1"
```

(☞) 対向ルータの WAN 回線が接続されているか、パケットが届いているか、IPsec のフィルタ(UDP500)は許可されているか、IPsec サービスが起動しているか、対向ルータで該当する IPsec 設定が正しく設定されているかなどを確認してください。

➢該当するポリシがない(イニシエータがメインモード)

<レスポンダ側のログ出力例>

```
pluto[XXXX]: packet from 10.10.20.1:500: initial Main Mode message received on 10.10.10.1:500 but no connection has been authorized with policy=PSK
```

(☞) フェーズ 1 のモードは正しいか、対向のルータの IP アドレスの設定は正しいか、IPsec の設定の関連づけは正しいかなどを確認してください。

➢該当するポリシがない(イニシエータがアグレッシブモード)

<レスポンダ側のログ出力例>

```
pluto[XXXX]: packet from 10.10.20.1:500: initial Aggressive Mode message received on 10.10.10.1:500 but no connection has been authorized with policy=PSK
```

(☞) フェーズ 1 のモードは正しいか、IPsec の設定の関連づけは正しいかなどを確認してください。

➢事前共有鍵の不一致(メインモード)

<レスポンダ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: responding to Main Mode
pluto[XXXX]: "tunnel1" #1:"tunnel1" #1: next payload type of ISAKMP Identification Payload has an unknown value
pluto[XXXX]: "tunnel1" #1: probable authentication failure (mismatch of preshared secrets?):
malformed payload in packet
```

(☞) お互いのルータで設定した事前共有鍵(PSK)の値が正しいか確認してください。

<イニシエータ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Main Mode
pluto[XXXX]: "tunnel1" #1: next payload type of ISAKMP Hash Payload has an unknown value:
```

(☞) お互いのルータで設定した事前共有鍵(PSK)の値が正しいか確認してください。

➢事前共有鍵の不一致(アグレッシブモード)

<レスポンダ側のログ出力例>

```
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: responding to Aggressive Mode from unknown peer 10.10.30.1
```

(☞) お互いのルータで設定した事前共有鍵(PSK)の値が正しいか確認してください。

<イニシエータ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
```

```
pluto[XXXX]: "tunnel1" #1: received Hash Payload does not match computed value
pluto[XXXX]: "tunnel1" #1: sending notification INVALID_HASH_INFORMATION to 10.10.10.1:500
```

(☞) お互いのルータで設定した事前共有鍵(PSK)の値が正しいか確認してください。

➢フェーズ 1 の ID 不一致(イニシエータの self-identity 不一致)

<レスポンダ側のログ出力例>

```
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: no suitable connection for peer 'nxr'
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: initial Aggressive Mode packet claiming to be from 10.10.30.1 but
no connection has been authorized
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: sending notification INVALID_ID_INFORMATION to 10.10.30.1:500
```

(☞) ipsec isakmp policy 設定モードの remote identity コマンドで設定した値(ID タイプを含む)が対向機器の self-identity と一致しているか確認してください。

<イニシエータ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
pluto[XXXX]: packet from 10.10.10.1:500: ignoring informational payload, type INVALID_ID_INFORMATION
```

(☞) ipsec local policy 設定モードの self-identity コマンドで設定した値(ID タイプを含む)が対向機器の remote identity と一致しているか確認してください。

➢フェーズ 1 の ID 不一致(レスポンダの self-identity 不一致)

<レスポンダ側のログ出力例>

```
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: responding to Aggressive Mode from unknown peer 10.10.30.1
pluto[XXXX]: packet from 10.10.30.1:500: ignoring informational payload, type INVALID_ID_INFORMATION
```

(☞) ipsec isakmp policy 設定モードの remote identity コマンドで設定した値(ID タイプを含む)が対向機器の self-identity と一致しているか確認してください。

<イニシエータ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
pluto[XXXX]: "tunnel1" #1: no suitable connection for peer '10.10.10.1'
pluto[XXXX]: "tunnel1" #1: initial Aggressive Mode packet claiming to be from 10.10.10.1but no connection
has been authorized
pluto[XXXX]: "tunnel1" #1: sending notification INVALID_ID_INFORMATION to 10.10.10.1:500
```

(☞) ipsec local policy 設定モードの self-identity コマンドで設定した値(ID タイプを含む)が対向機器の remoteidentity と一致しているか確認してください。

➢フェーズ 2 の ID 不一致

<レスポンダ側のログ出力例>

```
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: responding to Aggressive Mode from unknown peer 10.10.30.1
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: ISAKMP SA established
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: cannot respond to IPsec SA request because no connectionis known
for 192.168.10.0/24===10.10.10.1[10.10.10.1]...10.10.30.1[nxrc]===192.168.30.0/24
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: sending encrypted notification INVALID_ID_INFORMATION
to10.10.30.1:500
```

(☞) ipsec access-list コマンドで設定した値が対向機器と対になっているか確認してください。

<イニシエータ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
pluto[XXXX]: "tunnel1" #1: sent AI2, ISAKMP SA established
pluto[XXXX]: "tunnel1" #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP+0x4000000 {using
isakmp#1}
```

pluto[XXXX]: "tunnel1" #1: ignoring informational payload, type **INVALID_ID_INFORMATION**

(☞) ipsec access-list コマンドで設定した値が対向機器と対になっているか確認してください。

➢PFS 設定の不一致(レスポンダ側でのみ PFS を設定)

<レスポンダ側のログ出力例>

pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: responding to Aggressive Mode from unknown peer 10.10.30.1
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: ISAKMP SA established
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #2**: we require PFS but Quick I1 SA specifies no GROUP_DESCRIPTION**
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #2: sending encrypted notification **NO_PROPOSAL_CHOSEN** to 10.10.30.1:500

(☞) ipsec tunnel policy 設定モードの set pfs コマンドで設定した値が対向機器と一致しているか確認してください。

<イニシエータ側のログ出力例>

pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
pluto[XXXX]: "tunnel1" #1: sent AI2, ISAKMP SA established
pluto[XXXX]: "tunnel1" #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+UP+0x4000000 {using isakmp#1}
pluto[XXXX]: "tunnel1" #1: ignoring informational payload, type **NO_PROPOSAL_CHOSEN**

(☞) ipsec tunnel policy 設定モードの set pfs コマンドを設定しているか確認してください。

L2TP/IPsec 接続確認方法

● ステータスの確認

L2TP/IPsec では IPsec,L2TP,PPP の全てが確立および接続している必要があります。

IPsec のトンネル状況を一覧で確認する場合は、show ipsec status brief コマンドを使用します。

<実行例>

```
NXR#show ipsec status brief
TunnelName          Status
tunnel1             up
```

IPsec SA が確立している(IPsec established)ものを up,それ以外を down として表示します。なおスマートフォン接続用のトンネルポリシは異なる IP アドレスからの複数接続を許可しているため、複数のスマートフォンが接続してる場合でも上記のような表示となります。

IPsec の SA 確立状況等を確認する場合は、show ipsec status コマンドを使用します。また show ipsec status コマンドの後に tunnel <ポリシー番号>を指定することにより tunnel ポリシー毎にステータスを表示させることができます。これは多拠点収容構成で個々のポリシーを確認するのに有効です。

<実行例>

```
NXR#show ipsec status
000 "tunnel1": 10.10.10.1[10.10.10.1]:17/1701...%any[%any]:17/%any; unrouted; eroute owner: #0
000 "tunnel1":     ike_life: 86400s; ipsec_life: 28800s; margin: 270s; inc_ratio: 100%
000 "tunnel1":     newest ISAKMP SA: #0; newest IPsec SA: #0;
000 "tunnel1"[1]: 10.10.10.1[10.10.10.1]:17/1701...10.10.20.10[10.10.20.10]:17/50891; erouted; eroute
owner: #2
000 "tunnel1"[1]:     ike_life: 86400s; ipsec_life: 28800s; margin: 270s; inc_ratio: 100%
000 "tunnel1"[1]:     newest ISAKMP SA: #1; newest IPsec SA: #2;
000 "tunnel1"[1]:     IKE proposal: AES_CBC_256/HMAC_SHA1/MODP_1024
000 "tunnel1"[1]:     ESP proposal: AES_CBC_256/HMAC_SHA1/<N/A>
000
000 #2: "tunnel1"[1] 10.10.20.10 STATE_QUICK_R2 (IPsec SA established); EVENT_SA_REPLACE in 3451s;
newest IPSEC; eroute owner
000 #2: "tunnel1"[1] 10.10.20.10 esp.26594af@10.10.20.10 (528 bytes, 14s ago) esp.44242e17@10.10.10.1
(562 bytes, 14s ago); transport
000 #1: "tunnel1"[1] 10.10.20.10 STATE_MAIN_R3 (sent MR3, ISAKMP SA established);
EVENT_SA_REPLACE in 3449s; newest ISAKMP
000
Connections:
Security Associations:
   none
```

L2TP の確立状況を確認する場合は、show l2tp コマンドを使用します。

<実行例>

```
NXR#show l2tp
NumL2TPTunnels 1
Tunnel MyID 62277 AssignedID 8 NumSessions 1 PeerIP 10.10.20.10 State established
Session LNS MyID 48685 AssignedID 1055 State established
```

PPP の接続状況をを確認する場合は、show ppp コマンドを使用します。

<実行例>

```
NXR#show ppp
PPP100 session state is connected, line type is L2TP(LNS), time since change 00:00:21
   See also 'show l2tp' command.
```

● ログの確認

L2TP/IPsec 接続完了時には以下のようなログが出力されます。

<ログ出力例>

```
pluto[XXXX]: packet from 10.10.20.10:500: ignoring Vendor ID payload [RFC 3947]
pluto[XXXX]: packet from 10.10.20.10:500: ignoring Vendor ID payload
[4df37928e9fc4fd1b3262170d515c662]
pluto[XXXX]: packet from 10.10.20.10:500: ignoring Vendor ID payload
[8f8d83826d246b6fc7a8a6a428c11de8]
pluto[XXXX]: packet from 10.10.20.10:500: ignoring Vendor ID payload
[439b59f8ba676c4c7737ae22eab8f582]
pluto[XXXX]: packet from 10.10.20.10:500: ignoring Vendor ID payload
[4d1e0e136deafa34c4f3ea9f02ec7285]
pluto[XXXX]: packet from 10.10.20.10:500: ignoring Vendor ID payload
[80d0bb3def54565ee84645d4c85ce3ee]
pluto[XXXX]: packet from 10.10.20.10:500: ignoring Vendor ID payload
[9909b64eed937c6573de52ace952fa6b]
pluto[XXXX]: packet from 10.10.20.10:500: ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03]
pluto[XXXX]: packet from 10.10.20.10:500: ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02]
pluto[XXXX]: packet from 10.10.20.10:500: ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02_n]
pluto[XXXX]: packet from 10.10.20.10:500: ignoring Vendor ID payload [FRAGMENTATION 80000000]
pluto[XXXX]: packet from 10.10.20.10:500: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "tunnel1"[1] 10.10.20.10 #1: responding to Main Mode from unknown peer 10.10.20.10
pluto[XXXX]: "tunnel1"[1] 10.10.20.10 #1: received IPSEC_INITIAL_CONTACT, delete old states
pluto[XXXX]: "tunnel1"[1] 10.10.20.10 #1: sent MR3, ISAKMP SA established
pluto[XXXX]: "tunnel1"[1] 10.10.20.10 #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1"[1] 10.10.20.10 #2: responding to Quick Mode
pluto[XXXX]: "tunnel1"[1] 10.10.20.10 #2: IPsec SA established {ESP=>0x026594af <0x44242e17 DPD}
l2tp[XXXX]: L2TP Session Established
l2tp[XXXX]:     Peer IP = 10.10.20.10, port = 50891
l2tp[XXXX]:     Local   Tunnel/Session ID = 62277/48685
l2tp[XXXX]:     Remote Tunnel/Session ID = 8/1055
pppd[XXXX]: L2TPv2 plugin loaded.
pppd[XXXX]: pppd 2.4.4 started
pppd[XXXX]: Using interface ppp100
pppd[XXXX]: Connect: ppp100 <-->
charon: 02[KNL] interface ppp100 activated
pppd[XXXX]: local   IP address 172.16.0.1
pppd[XXXX]: remote IP address 172.16.0.11
```

L2TP/IPsec 接続が失敗する時に出力されるログとして以下のようなものが挙げられます。

※IPsec の接続失敗時のログは IPsec 接続確認方法をご参照下さい。

➢L2TP での PPP 接続時のユーザ名が不正

<ログ出力例(L2TP 部分抜粋)>

```
l2tp[XXXX]: L2TP Session Established
l2tp[XXXX]:     Peer IP = 10.10.20.10, port = 59139
l2tp[XXXX]:     Local   Tunnel/Session ID = 51172/15957
l2tp[XXXX]:     Remote Tunnel/Session ID = 18/1354
pppd[XXXX]: L2TPv2 plugin loaded.
pppd[XXXX]: pppd 2.4.4 started
pppd[XXXX]: Using interface ppp102
pppd[XXXX]: Connect: ppp102 <-->
pppd[XXXX]: No CHAP secret found for authenticating ios011
pppd[XXXX]: Peer ios011 failed CHAP authentication
l2tp[XXXX]: L2TP Session Closed
```

(☞) NXR およびスマートフォンでユーザ名が正しく設定されているかを確認してください。

L2TP での PPP 接続時のパスワードが不正

<ログ出力例(L2TP 部分抜粋)>

```
l2tp[XXXX]: L2TP Session Established
l2tp[XXXX]:     Peer IP = 10.10.20.10, port = 53244
l2tp[XXXX]:     Local   Tunnel/Session ID = 48235/16523
l2tp[XXXX]:     Remote Tunnel/Session ID = 19/1360
pppd[XXXX]: L2TPv2 plugin loaded.
pppd[XXXX]: pppd 2.4.4 started
pppd[XXXX]: Using interface ppp102
pppd[XXXX]: Connect: ppp102 <-->
pppd[XXXX]: Peer ios01 failed CHAP authentication
l2tp[XXXX]: L2TP Session Closed
```

(☞) NXR およびスマートフォンでパスワードが正しく設定されているかを確認してください。

設定例 show config 形式サンプル

1-1. 固定 IP アドレスでの接続設定例(MainMode の利用)

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.20.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_B
!
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 ip address 10.10.10.1/24
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
```

```
!
!
!
ip route 0.0.0.0/0 10.10.10.254
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 ip address 10.10.20.1/24
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
```

```
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 10.10.20.254
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
!
!
!
end
```

1-2. 動的 IP アドレスでの接続設定例(AggressiveMode の利用)

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
  address ip
!
!
ipsec isakmp policy 1
  description NXR_B
  authentication pre-share ipseckey
  keepalive 30 3 periodic clear
  hash sha1
  encryption aes128
  group 5
  isakmp-mode aggressive
  remote address ip any
  remote identity fqdn nxrb
  local policy 1
!
!
ipsec tunnel policy 1
  description NXR_B
  negotiation-mode responder
  set transform esp-aes128 esp-sha1-hmac
  set pfs group5
  set key-exchange isakmp 1
  match address LAN_B
!
!
```

```
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 ip address 10.10.10.1/24
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 10.10.10.254
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrb
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip 10.10.10.1
 local policy 1
!
!
```

```
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 ip address dhcp
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
!
!
!
end
```

1-3. RSA 公開鍵暗号方式での接続設定例

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
ipsec generate rsa-sig-key 1024
!
ipsec local policy 1
 address ip
 self-identity fqdn nxra
!
!
ipsec isakmp policy 1
 description NXR_B
```

```
 authentication rsa-sig 0sAQOx8kE6uhZTvWMikunsy3uK5/7jIkTXsCjQpgo4B+X64UAVeuxFQZ3KG3bz
yjmyCbpkt0xEiU+v1kF4AOAOXoDfgND+KAdEky/YWqQYzMuuuu2uy/K6E9JA24NACufuqMqgGSXc51fJ/6V
5Qi9YtVd7TWBkZQSZJJADBHs/YyYD9Q==
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.20.1
 remote identity fqdn nxrb
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_B
!
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 ip address 10.10.10.1/24
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 10.10.10.254
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
```

```
fast-forwarding enable
!
!
ipsec generate rsa-sig-key 1024
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrb
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication rsa-sig 0sAQNe9Ghb4CNEaJuIIy67aSxECLJDHhvndH1opuMs6P8yGiTNlcGeSO Q8XEy8
iYTst2bv022XUxSt37RhOR5lRiY1i83TXkQZbhnJDCNJv+rtX/aro745MbJ9auXT1L5tda4C54S7SELboAtU28s
D3si0OwlzLWtE7yRUqLP4ZiiNMw==
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.10.1
 remote identity fqdn nxra
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 ip address 10.10.20.1/24
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 10.10.20.254
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
!
!
!
end
```

1-4. X.509(デジタル署名認証)方式での接続設定例

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
ipsec x509 enable
ipsec x509 ca-certificate nxr
ipsec x509 certificate nxra
ipsec x509 private-key nxra key
ipsec x509 private-key nxra password nxrapass
ipsec x509 crl nxr
!
ipsec local policy 1
 address ip
 self-identity dn /C=JP/CN=nxra/E=nxra@example.com
 x509 certificate nxra
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication rsa-sig
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.20.1
 remote identity dn /C=JP/CN=nxrb/E=nxrb@example.com
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_B
!
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 ip address 10.10.10.1/24
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
```

```
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 10.10.10.254
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
ipsec x509 enable
ipsec x509 ca-certificate nxr
ipsec x509 certificate nxrb
ipsec x509 private-key nxrb key
ipsec x509 private-key nxrb password nxrbpass
ipsec x509 crl nxr
!
ipsec local policy 1
 address ip
 self-identity dn /C=JP/CN=nxrb/E=nxrb@example.com
 x509 certificate nxrb
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication rsa-sig
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.10.1
 remote identity dn /C=JP/CN=nxra/E=nxra@example.com
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
```

```
 match address LAN_A
!
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 ip address 10.10.20.1/24
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 10.10.20.254
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
!
!
!
end
```

1-5. PPPoE を利用した IPsec 接続設定例

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey1
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
```

```
 remote address ip 10.10.20.1
 local policy 1
!
ipsec isakmp policy 2
 description NXR_C
 authentication pre-share ipseckey2
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrc
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_B
!
ipsec tunnel policy 2
 description NXR_C
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 2
 match address LAN_C
!
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@example.jp password test1pass
 ipsec policy 1
!
interface bridge 0
 no ip address
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
```

```
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
ip access-list ppp0_in permit any 10.10.10.1 50
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
ipsec access-list LAN_C ip 192.168.10.0/24 192.168.30.0/24
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey1
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface ppp 0
 ip address 10.10.20.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
```

```
 ppp username test2@example.jp password test2pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 udp 500 500
ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 50
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
!
!
!
end
```

〔NXR_C の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_C
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrc
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey2
 hash sha1
 encryption aes128
```

```
 group 5
 isakmp-mode aggressive
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test3@example.jp password test3pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.30.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
ip access-list ppp0_in permit 10.10.10.1 any 50
!
ipsec access-list LAN_A ip 192.168.30.0/24 192.168.10.0/24
!
!
!
end
```

1-6. センタ経由拠点間通信設定例

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey1
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.20.1
 local policy 1
!
ipsec isakmp policy 2
 description NXR_C
 authentication pre-share ipseckey2
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrc
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_B
!
ipsec tunnel policy 2
 description NXR_C
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 2
 match address LAN_C
!
!
interface ppp 0
 ip address 10.10.10.1/32
```

```
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@example.jp password test1pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
ip access-list ppp0_in permit any 10.10.10.1 50
!
ipsec access-list LAN_B ip 192.168.0.0/16 192.168.20.0/24
ipsec access-list LAN_C ip 192.168.0.0/16 192.168.30.0/24
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
```

```
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey1
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface ppp 0
 ip address 10.10.20.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test2@example.jp password test2pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.20.1/24
 ipsec policy-ignore
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 udp 500 500
ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 50
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.0.0/16
!
!
!
end
```

〔NXR_C の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_C
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrc
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey2
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test3@example.jp password test3pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.30.1/24
 ipsec policy-ignore
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
```

```
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
ip access-list ppp0_in permit 10.10.10.1 any 50
!
ipsec access-list LAN_A ip 192.168.30.0/24 192.168.0.0/16
!
!
!
end
```

1-7. IPsec NAT トラバーサル接続設定例

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
ipsec nat-traversal enable
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrb
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 negotiation-mode responder
```

```
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_B
!
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@example.jp password test1pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.10.1 udp any 500
ip access-list ppp0_in permit any 10.10.10.1 udp any 4500
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
```

```
!
!
ipsec nat-traversal enable
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrb
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 ip address 192.168.120.1/24
 ipsec policy 1
!
dns
 service enable
 address 192.168.120.254
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 192.168.120.254
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
!
!
!
end
```

1-8. FQDN での IPsec 接続設定例

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.5 (build 4/18:30 28 03 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey1
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrb
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_B
!
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@example.jp password test1pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
```

```
!
syslog
 local enable
!
warplink
 service enable
 account username warplinksample password warplinksamplepass
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any any udp 500 500
ip access-list ppp0_in permit any any 50
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.5 (build 4/18:30 28 03 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrb
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey1
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip test.subdomain.warplink.ne.jp
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
```

```
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test2@example.jp password test2pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any any udp 500 500
ip access-list ppp0_in permit any any 50
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
!
!
!
end
```

1-9. 冗長化設定(backup policy の利用)

〔NXR_A1 の設定〕

```
!
! Century Systems NXR-125 Series ver 5.25.1 (build 17/19:22 05 12 2013)
!
hostname NXR_A1
telnet-server enable
http-server enable
!
!
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey1
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrb
 local policy 1
 netevent 2 disconnect
!
!
ipsec tunnel policy 1
 description NXR_B
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 set route
 match address LAN_B
!
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@example.jp password test1pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
 no ip redirects
 vrrp ip 1 address 192.168.10.254
 vrrp ip 1 priority 254
```

```
 vrrp ip 1 timers advertise 5
 vrrp ip 1 netevent 1 priority 50
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
track 1 interface ppp 0 initial-timeout 30
track 2 interface ethernet 0
!
!
ip route 192.168.20.0/24 192.168.10.2 10
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
ip access-list ppp0_in permit any 10.10.10.1 50
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
!
!
!
end
```

〔NXR_A2 の設定〕

```
!
! Century Systems NXR-125 Series ver 5.25.1 (build 17/19:22 05 12 2013)
!
hostname NXR_A2
telnet-server enable
http-server enable
!
!
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey2
 keepalive 30 3 periodic clear
```

```
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrb
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 set route
 match address LAN_B
!
!
interface ppp 0
 ip address 10.10.20.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test2@example.jp password test2pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.2/24
 no ip redirects
 vrrp ip 1 address 192.168.10.254
 vrrp ip 1 timers advertise 5
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.20.0/24 null 254
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.20.1 udp 500 500
ip access-list ppp0_in permit any 10.10.20.1 50
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
!
!
```

```
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrb
!
!
ipsec isakmp policy 1
 description NXR_A1
 authentication pre-share ipseckey1
 backup policy 2
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip 10.10.10.1
 local policy 1
!
ipsec isakmp policy 2
 description NXR_A2
 authentication pre-share ipseckey2
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip 10.10.20.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A1
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 set route
 match address LAN_A
!
ipsec tunnel policy 2
 description NXR_A2
 negotiation-mode manual
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 2
 set priority 10
```

```
  set route
  match address LAN_A
!
!
interface ppp 0
  ip address negotiated
  no ip redirects
  ip tcp adjust-mss auto
  ip access-group in ppp0_in
  ip masquerade
  ip spi-filter
  ppp username test3@example.jp password test3pass
  ipsec policy 1
!
interface ethernet 0
  ip address 192.168.20.1/24
!
interface ethernet 1
  no ip address
  pppoe-client ppp 0
!
dns
  service enable
!
syslog
  local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.10.0/24 null 254
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
ip access-list ppp0_in permit 10.10.10.1 any 50
ip access-list ppp0_in permit 10.10.20.1 any udp 500 500
ip access-list ppp0_in permit 10.10.20.1 any 50
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
!
!
!
end
```

2-1. 固定 IP アドレスでの接続設定例(MainMode の利用)

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.20.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 ip address 10.10.10.1/24
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
```

```
!
!
!
!
!
!
ip route 192.168.20.0/24 tunnel 1
ip route 192.168.20.0/24 null 254
ip route 0.0.0.0/0 10.10.10.254
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ethernet 0
```

```
 ip address 192.168.20.1/24
!
interface ethernet 1
 ip address 10.10.20.1/24
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.10.0/24 tunnel 1
ip route 192.168.10.0/24 null 254
ip route 0.0.0.0/0 10.10.20.254
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

2-2. 動的 IP アドレスでの接続設定例(AggressiveMode の利用)

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
```

```
 remote identity fqdn nxrb
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 ip address 10.10.10.1/24
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.20.0/24 tunnel 1
ip route 192.168.20.0/24 null 254
ip route 0.0.0.0/0 10.10.10.254
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
```

```
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrb
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 ip address dhcp
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.10.0/24 tunnel 1
ip route 192.168.10.0/24 null 254
!
ipsec access-list ipsec_acl ip any any
!
!
```

```
!
end
```

2-3. RSA 公開鍵暗号方式での接続設定例

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
ipsec generate rsa-sig-key 1024
!
ipsec local policy 1
 address ip
 self-identity fqdn nxra
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication rsa-sig 0sAQOx8kE6uhZTvWMikunsy3uK5/7jIkTXsCjQpgo4B+X64UAVeuxFQZ3KG3bzyjmy
Cbpkt0xEiU+v1kF4AOAOXoDfgND+KAdEky/YWqQYzMuuuu2uy/K6E9JA24NACufuqMqgGSXc51fJ/6V5Qi9
YtVd7TWBkZQSZJJADBHs/YyYD9Q==
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.20.1
 remote identity fqdn nxrb
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 ip address 10.10.10.1/24
 ipsec policy 1
!
```

```
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 10.10.10.254
ip route 192.168.20.0/24 tunnel 1
ip route 192.168.20.0/24 null 254
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
ipsec generate rsa-sig-key 1024
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrb
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication rsa-sig 0sAQNe9Ghb4CNEaJuIIy67aSxECLJDHhvndH1opuMs6P8yGiTNlcGeSO Q8XEy8iYT
st2bv022XUxSt37RhOR5lRiY1i83TXkQZbhnJDCNJv+rtX/aro745MbJ9auXT1L5tda4C54S7SELboAtU28sD3si
0OwlzLWtE7yRUqLP4ZiiNMw==
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.10.1
 remote identity fqdn nxra
 local policy 1
!
!
ipsec tunnel policy 1
```

```
  description NXR_A
  set transform esp-aes128 esp-sha1-hmac
  set pfs group5
  set key-exchange isakmp 1
  match address ipsec_acl
!
!
interface tunnel 1
  no ip address
  ip tcp adjust-mss auto
  tunnel mode ipsec ipv4
  tunnel protection ipsec policy 1
!
interface ethernet 0
  ip address 192.168.20.1/24
!
interface ethernet 1
  ip address 10.10.20.1/24
  ipsec policy 1
!
dns
  service enable
!
syslog
  local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 10.10.20.254
ip route 192.168.10.0/24 tunnel 1
ip route 192.168.10.0/24 null 254
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

2-4. X.509(デジタル署名認証)方式での接続設定例

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
ipsec x509 enable
ipsec x509 ca-certificate nxr
ipsec x509 certificate nxra
ipsec x509 private-key nxra key
ipsec x509 private-key nxra password nxrapass
ipsec x509 crl nxr
!
ipsec local policy 1
 address ip
 self-identity dn /C=JP/CN=nxra/E=nxra@example.com
 x509 certificate nxra
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication rsa-sig
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.20.1
 remote identity dn /C=JP/CN=nxrb/E=nxrb@example.com
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 ip address 10.10.10.1/24
 ipsec policy 1
!
```

```
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.20.0/24 tunnel 1
ip route 192.168.20.0/24 null 254
ip route 0.0.0.0/0 10.10.10.254
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
ipsec x509 enable
ipsec x509 ca-certificate nxr
ipsec x509 certificate nxrb
ipsec x509 private-key nxrb key
ipsec x509 private-key nxrb password nxrbpass
ipsec x509 crl nxr
!
ipsec local policy 1
 address ip
 self-identity dn /C=JP/CN=nxrb/E=nxrb@example.com
 x509 certificate nxrb
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication rsa-sig
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.10.1
 remote identity dn /C=JP/CN=nxra/E=nxra@example.com
```

```
  local policy 1
!
!
ipsec tunnel policy 1
  description NXR_A
  set transform esp-aes128 esp-sha1-hmac
  set pfs group5
  set key-exchange isakmp 1
  match address ipsec_acl
!
!
interface tunnel 1
  no ip address
  ip tcp adjust-mss auto
  tunnel mode ipsec ipv4
  tunnel protection ipsec policy 1
!
interface ethernet 0
  ip address 192.168.20.1/24
!
interface ethernet 1
  ip address 10.10.20.1/24
  ipsec policy 1
!
dns
  service enable
!
syslog
  local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.10.0/24 tunnel 1
ip route 192.168.10.0/24 null 254
ip route 0.0.0.0/0 10.10.20.254
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

2-5. PPPoE を利用した IPsec 接続設定例

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
ipsec priority-ignore enable
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey1
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.20.1
 local policy 1
!
ipsec isakmp policy 2
 description NXR_C
 authentication pre-share ipseckey2
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrc
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
ipsec tunnel policy 2
 description NXR_C
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 2
 match address ipsec_acl
!
!
interface tunnel 1
```

```
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface tunnel 2
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 2
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@example.jp password test1pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.20.0/24 tunnel 1
ip route 192.168.30.0/24 tunnel 2
ip route 192.168.20.0/24 null 254
ip route 192.168.30.0/24 null 254
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
ip access-list ppp0_in permit any 10.10.10.1 50
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey1
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ppp 0
 ip address 10.10.20.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test2@example.jp password test2pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
```

```
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.10.0/24 tunnel 1
ip route 192.168.10.0/24 null 254
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 udp 500 500
ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 50
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

〔NXR_C の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_C
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrc
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey2
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
```

```
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test3@example.jp password test3pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.30.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.10.0/24 tunnel 1
ip route 192.168.10.0/24 null 254
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
ip access-list ppp0_in permit 10.10.10.1 any 50
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

2-6. センタ経由拠点間通信設定例

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
ipsec priority-ignore enable
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey1
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.20.1
 local policy 1
!
ipsec isakmp policy 2
 description NXR_C
 authentication pre-share ipseckey2
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrc
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
ipsec tunnel policy 2
 description NXR_C
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 2
 match address ipsec_acl
!
!
interface tunnel 1
```

```
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface tunnel 2
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 2
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@example.jp password test1pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.20.0/24 tunnel 1
ip route 192.168.30.0/24 tunnel 2
ip route 192.168.20.0/24 null 254
ip route 192.168.30.0/24 null 254
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
ip access-list ppp0_in permit any 10.10.10.1 50
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey1
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ppp 0
 ip address 10.10.20.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test2@example.jp password test2pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
```

```
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.0.0/16 tunnel 1
ip route 192.168.0.0/16 null 254
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 udp 500 500
ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 50
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

〔NXR_C の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_C
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrc
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey2
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
```

```
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test3@example.jp password test3pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.30.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.0.0/16 tunnel 1
ip route 192.168.0.0/16 null 254
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
ip access-list ppp0_in permit 10.10.10.1 any 50
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

2-7. IPsec NAT トラバーサル接続設定例

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
ipsec nat-traversal enable
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrb
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@example.jp password test1pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
```

```
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.20.0/24 tunnel 1
ip route 192.168.20.0/24 null 254
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.10.1 udp any 500
ip access-list ppp0_in permit any 10.10.10.1 udp any 4500
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
ipsec nat-traversal enable
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrb
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
```

```
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 ip address 192.168.120.1/24
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.10.0/24 tunnel 1
ip route 192.168.10.0/24 null 254
ip route 0.0.0.0/0 192.168.120.254
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

2-8. FQDN での IPsec 接続設定例

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
```

```
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey1
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrb
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@example.jp password test1pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
warplink
 service enable
```

```
 account username warplinksample password warplinksamplepass
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.20.0/24 tunnel 1
ip route 192.168.20.0/24 null 254
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any any udp 500 500
ip access-list ppp0_in permit any any 50
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrb
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey1
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip test.subdomain.warplink.ne.jp
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
```

```
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test2@example.jp password test2pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.10.0/24 tunnel 1
ip route 192.168.10.0/24 null 254
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any any udp 500 500
ip access-list ppp0_in permit any any 50
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

2-9. 冗長化設定 1(backup policy の利用)

〔NXR_A1 の設定〕

```
!
! Century Systems NXR-125 Series ver 5.25.1 (build 17/19:22 05 12 2013)
!
hostname NXR_A1
telnet-server enable
http-server enable
!
!
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey1
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrb
 local policy 1
 netevent 2 disconnect
!
!
ipsec tunnel policy 1
 description NXR_B
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@example.jp password test1pass
 ipsec policy 1
!
```

```
interface ethernet 0
 ip address 192.168.10.1/24
 no ip redirects
 vrrp ip 1 address 192.168.10.254
 vrrp ip 1 priority 254
 vrrp ip 1 timers advertise 5
 vrrp ip 1 netevent 1 priority 50
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
track 1 interface ppp 0 initial-timeout 30
track 2 interface ethernet 0
!
!
ip route 192.168.20.0/24 tunnel 1
ip route 192.168.20.0/24 192.168.10.2 10
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
ip access-list ppp0_in permit any 10.10.10.1 50
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

〔NXR_A2 の設定〕

```
!
! Century Systems NXR-125 Series ver 5.25.1 (build 17/19:22 05 12 2013)
!
hostname NXR_A2
telnet-server enable
http-server enable
!
!
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
```

```
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey2
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrb
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ppp 0
 ip address 10.10.20.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test2@example.jp password test2pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.2/24
 no ip redirects
 vrrp ip 1 address 192.168.10.254
 vrrp ip 1 timers advertise 5
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
```

```
!
!
ip route 192.168.20.0/24 tunnel 1
ip route 192.168.20.0/24 null 254
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.20.1 udp 500 500
ip access-list ppp0_in permit any 10.10.20.1 50
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrb
!
!
ipsec isakmp policy 1
 description NXR_A1
 authentication pre-share ipseckey1
 backup policy 2
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip 10.10.10.1
 local policy 1
!
ipsec isakmp policy 2
 description NXR_A2
 authentication pre-share ipseckey2
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip 10.10.20.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A1
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
```

```
 set key-exchange isakmp 1
 match address ipsec_acl
!
ipsec tunnel policy 2
 description NXR_A2
 negotiation-mode manual
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 2
 set priority 10
 match address ipsec_acl
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface tunnel 2
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 2
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test3@example.jp password test3pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.10.0/24 tunnel 1
ip route 192.168.10.0/24 tunnel 2 10
ip route 192.168.10.0/24 null 254
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
```

```
ip access-list ppp0_in permit 10.10.10.1 any 50
ip access-list ppp0_in permit 10.10.20.1 any udp 500 500
ip access-list ppp0_in permit 10.10.20.1 any 50
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

2-10. 冗長化設定 2(IPsec 同時接続)

〔NXR_A1 の設定〕

```
!
! Century Systems NXR-125 Series ver 5.25.1 (build 17/19:22 05 12 2013)
!
hostname NXR_A1
telnet-server enable
http-server enable
!
!
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey1
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrb
 local policy 1
 netevent 2 disconnect
!
!
ipsec tunnel policy 1
 description NXR_B
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
```

```
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@example.jp password test1pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
 no ip redirects
 vrrp ip 1 address 192.168.10.254
 vrrp ip 1 priority 254
 vrrp ip 1 timers advertise 5
 vrrp ip 1 netevent 1 priority 50
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
track 1 interface ppp 0 initial-timeout 30
track 2 interface ethernet 0
!
!
ip route 192.168.20.0/24 tunnel 1
ip route 192.168.20.0/24 192.168.10.2 10
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
ip access-list ppp0_in permit any 10.10.10.1 50
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

〔NXR_A2 の設定〕

```
!
! Century Systems NXR-125 Series ver 5.25.1 (build 17/19:22 05 12 2013)
!
hostname NXR_A2
telnet-server enable
http-server enable
!
!
```

```
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey2
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrb
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ppp 0
 ip address 10.10.20.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test2@example.jp password test2pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.2/24
 no ip redirects
 vrrp ip 1 address 192.168.10.254
 vrrp ip 1 timers advertise 5
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
```

```
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.20.0/24 tunnel 1
ip route 192.168.20.0/24 null 254
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.20.1 udp 500 500
ip access-list ppp0_in permit any 10.10.20.1 50
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
ipsec priority-ignore enable
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrb
!
!
ipsec isakmp policy 1
 description NXR_A1
 authentication pre-share ipseckey1
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip 10.10.10.1
 local policy 1
!
ipsec isakmp policy 2
 description NXR_A2
 authentication pre-share ipseckey2
 hash sha1
```

```
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip 10.10.20.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A1
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
ipsec tunnel policy 2
 description NXR_A2
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 2
 match address ipsec_acl
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface tunnel 2
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 2
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test3@example.jp password test3pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
```

```
!
!
!
ip route 192.168.10.0/24 tunnel 1
ip route 192.168.10.0/24 tunnel 2 10
ip route 192.168.10.0/24 null 254
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
ip access-list ppp0_in permit 10.10.10.1 any 50
ip access-list ppp0_in permit 10.10.20.1 any udp 500 500
ip access-list ppp0_in permit 10.10.20.1 any 50
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

2-11. ネットワークイベント機能で IPsec トンネルを監視

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrb
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
```

```
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 ip address 10.10.10.1/24
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.20.0/24 tunnel 1
ip route 192.168.20.0/24 null 254
ip route 0.0.0.0/0 10.10.10.254
!
ipsec access-list ipsec_acl ip any any
!
!
!
End
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrb
!
!
ipsec isakmp policy 1
 description NXR_A
```

```
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip 10.10.10.1
 local policy 1
 netevent 1 reconnect
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 ip address dhcp
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
track 1 ip reachability 192.168.10.1 interface tunnel 1 10 3
!
!
ip route 192.168.10.0/24 tunnel 1
ip route 192.168.10.0/24 null 254
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

2-12. IPsec トンネルでダイナミックルーティング(OSPF)を利用する

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
ipsec priority-ignore enable
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey1
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.20.1
 local policy 1
!
ipsec isakmp policy 2
 description NXR_C
 authentication pre-share ipseckey2
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrc
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
ipsec tunnel policy 2
 description NXR_C
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 2
 match address ipsec_acl
!
!
interface tunnel 1
```

```
 ip address 192.168.10.1/32
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface tunnel 2
 ip address 192.168.10.1/32
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 2
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@example.jp password test1pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
router ospf
 router-id 172.31.0.1
 network 192.168.10.0/24 area 0
 passive-interface ethernet 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.0.0/16 null 254
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
ip access-list ppp0_in permit any 10.10.10.1 50
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey1
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
!
interface tunnel 1
 ip address 192.168.20.1/32
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ppp 0
 ip address 10.10.20.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test2@example.jp password test2pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
```

```
router ospf
 router-id 172.31.0.2
 network 192.168.20.0/24 area 0
 passive-interface ethernet 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.0.0/16 null 254
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 udp 500 500
ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 50
!
ipsec access-list ipsec_acl ip any any
!
!
!
end
```

〔NXR_C の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR_C
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrc
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey2
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip 10.10.10.1
 local policy 1
```

```
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
!
interface tunnel 1
 ip address 192.168.30.1/32
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test3@example.jp password test3pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.30.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
router ospf
 router-id 172.31.0.3
 network 192.168.30.0/24 area 0
 passive-interface ethernet 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.0.0/16 null 254
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
ip access-list ppp0_in permit 10.10.10.1 any 50
!
ipsec access-list ipsec_acl ip any any
!
!
!
```

```
end
```

3-1. スマートフォンとの L2TP/IPsec 接続設定例

〔NXR の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
ppp account username android01 password android01pass
ppp account username ios01 password ios01pass
ppp account username test1@example.jp password test1pass
!
!
l2tp udp source-port 1701
!
l2tpv3 udp source-port 40001
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description smartphone
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 lifetime 86400
 isakmp-mode main
 remote address ip any
 local policy 1
!
!
ipsec tunnel policy 1
 description smartphone
 set transform esp-aes128 esp-sha1-hmac
 no set pfs
 set key-exchange isakmp 1
 set sa lifetime 28800
 match protocol l2tp-smartphone
!
!
l2tp 1
 tunnel address any ipsec
 tunnel mode lns
 tunnel virtual-template 0
!
interface virtual-template 0
 ip address 172.16.0.1/32
 no ip redirects
 no ip rebound
 ip tcp adjust-mss auto
```

```
  peer ip pool smartphoneip
!
interface ppp 0
  ip address 10.10.10.1/32
  no ip redirects
  ip tcp adjust-mss auto
  ip access-group in ppp0_in
  ip masquerade
  ip spi-filter
  ppp username test1@example.jp
  ipsec policy 1
!
interface ethernet 0
  ip address 192.168.10.1/24
!
interface ethernet 1
  no ip address
  pppoe-client ppp 0
!
dns
  service enable
!
syslog
  local enable
!
!
access-server profile 0
  ppp username android01 ip 172.16.0.10
!
access-server profile 1
  ppp username ios01 ip 172.16.0.11
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip local pool smartphoneip address 172.16.0.10 172.16.0.11
!
ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
ip access-list ppp0_in permit any 10.10.10.1 50
!
!
!
end
```

3-2. スマートフォンとの L2TP/IPsec 接続設定例(CRT)

〔NXR の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
ppp account username android01 password android01pass
ppp account username android02 password android02pass
ppp account username test1@example.jp password test1pass
!
ipsec x509 enable
ipsec x509 ca-certificate nxrCA
ipsec x509 certificate nxr
ipsec x509 private-key nxr key
ipsec x509 private-key nxr password nxrpass
ipsec x509 crl nxrCA
!
l2tp udp source-port 1701
!
l2tpv3 udp source-port 40001
!
ipsec local policy 1
 address ip
 x509 certificate nxr
!
!
ipsec isakmp policy 1
 description smartphone1
 authentication rsa-sig
 hash sha1
 encryption aes128
 group 5
 lifetime 86400
 isakmp-mode main
 remote address ip any
 remote identity dn C=JP,CN=smartphone1,E=smartphone@example.com
 local policy 1
!
ipsec isakmp policy 2
 description smartphone2
 authentication rsa-sig
 hash sha1
 encryption aes128
 group 5
 lifetime 86400
 isakmp-mode main
 remote address ip any
 remote identity dn C=JP,CN=smartphone2,E=smartphone@example.com
 local policy 1
!
!
ipsec tunnel policy 1
 description smartphone
```

```
 set transform esp-aes128 esp-sha1-hmac
 no set pfs
 set key-exchange isakmp 1
 set sa lifetime 28800
 match protocol l2tp-smartphone
!
ipsec tunnel policy 2
 description smartphone
 set transform esp-aes128 esp-sha1-hmac
 no set pfs
 set key-exchange isakmp 2
 set sa lifetime 28800
 match protocol l2tp-smartphone
!
!
l2tp 1
 tunnel address any ipsec
 tunnel mode lns
 tunnel virtual-template 0
!
interface virtual-template 0
 ip address 172.16.0.1/32
 no ip redirects
 no ip rebound
 ip tcp adjust-mss auto
 peer ip pool smartphoneip
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@example.jp
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
access-server profile 0
 ppp username android01 ip 172.16.0.10
!
access-server profile 1
 ppp username android02 ip 172.16.0.11
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
```

```
!
!
ip route 0.0.0.0/0 ppp 0
!
ip local pool smartphoneip address 172.16.0.10 172.16.0.11
!
ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
ip access-list ppp0_in permit any 10.10.10.1 50
!
!
!
end
```

3-3. スマートフォンとの L2TP/IPsec NAT トラバーサル接続設定例

〔NXR の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
ppp account username android01 password android01pass
ppp account username ios01 password ios01pass
ppp account username test1@example.jp password test1pass
!
ipsec nat-traversal enable
!
l2tp udp source-port 1701
!
l2tpv3 udp source-port 40001
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description smartphone
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 lifetime 86400
 isakmp-mode main
 remote address ip any
 local policy 1
!
!
ipsec tunnel policy 1
 description smartphone
 set transform esp-aes128 esp-sha1-hmac
 no set pfs
 set key-exchange isakmp 1
 set sa lifetime 28800
 match protocol l2tp-smartphone nat-traversal
```

```
!
!
l2tp 1
 tunnel address any ipsec
 tunnel mode lns
 tunnel virtual-template 0
!
interface virtual-template 0
 ip address 192.168.10.1/32
 no ip redirects
 no ip rebound
 ip tcp adjust-mss auto
 peer ip proxy-arp
 peer ip pool smartphoneip
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@example.jp
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip local pool smartphoneip address 192.168.10.10 192.168.10.11
!
ip access-list ppp0_in permit any 10.10.10.1 udp any 500
ip access-list ppp0_in permit any 10.10.10.1 udp any 4500
!
!
!
end
```

3-4. スマートフォンとの L2TP/IPsec FQDN 接続設定例

〔NXR の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.5 (build 4/18:30 28 03 2013)
!
hostname NXR
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
ppp account username android01 password android01pass
ppp account username ios01 password ios01pass
ppp account username test1@example.jp password test1pass
!
ipsec nat-traversal enable
!
l2tp udp source-port 1701
!
l2tpv3 udp source-port 40001
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description smartphone
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 lifetime 86400
 isakmp-mode main
 remote address ip any
 local policy 1
!
!
ipsec tunnel policy 1
 description smartphone
 set transform esp-aes128 esp-sha1-hmac
 no set pfs
 set key-exchange isakmp 1
 set sa lifetime 28800
 match protocol l2tp-smartphone nat-traversal
!
!
l2tp 1
 tunnel address any ipsec
 tunnel mode lns
 tunnel virtual-template 0
!
interface virtual-template 0
 ip address 192.168.10.1/32
 no ip redirects
 no ip rebound
 ip tcp adjust-mss auto
 peer ip proxy-arp
 peer ip pool smartphoneip
```

```
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@example.jp
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
warplink
 service enable
 account username warplinksample password warplinksamplepass
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip local pool smartphoneip address 192.168.10.10 192.168.10.11
!
ip access-list ppp0_in permit any any udp any 500
ip access-list ppp0_in permit any any udp any 4500
!
!
!
end
```

4-1. Cloud^n Compute(VPC タイプ OpenNW)接続設定例

〔NXR の設定〕

```
!
! Century Systems NXR-120 Series ver 5.24.1C (build 1/13:44 26 09 2013)
!
hostname NXR
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
```

```
fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description Cloudn
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.100.1
 local policy 1
!
!
ipsec tunnel policy 1
 description Cloudn
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@example.jp password test1pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
```

```
!
!
ip route 10.0.0.0/16 tunnel 1
ip route 10.0.0.0/16 null 254
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
ip access-list ppp0_in permit any 10.10.10.1 50
!
ipsec access-list ipsec_acl ip 192.168.10.0/24 10.0.0.0/16
!
!
!
end
```

4-2. Windows Azure 接続設定例

〔NXR の設定〕

```
!
! Century Systems NXR-125 Series ver 5.25.2 (build 1/21:01 17 01 2014)
!
hostname NXR
telnet-server enable
http-server enable
!
!
!
!
!
!
ipv6 forwarding
fast-forwarding enable
!
!
ipsec nat-traversal enable
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description WindowsAzure
 authentication pre-share ipseckey
 no keepalive
 hash sha1
 encryption aes256
 group 2
 lifetime 28800
 isakmp-mode main
 remote address ip 10.10.100.1
 local policy 1
!
!
ipsec tunnel policy 1
 description WindowsAzure
 set transform esp-aes256 esp-sha1-hmac
 no set pfs
 set key-exchange isakmp 1
 match address ipsec_acl
!
```

```
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss 1350
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 ip address 10.10.10.1/30
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in eth1_in
 ip masquerade
 ip spi-filter
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 172.16.0.0/20 tunnel 1
ip route 172.16.0.0/20 null 254
ip route 0.0.0.0/0 10.10.10.2
!
ip access-list eth1_in permit any 10.10.10.1 udp any 500
ip access-list eth1_in permit any 10.10.10.1 udp any 4500
ip access-list eth1_in permit any 10.10.10.1 50
!
ipsec access-list ipsec_acl ip 192.168.10.0/24 172.16.0.0/20
!
!
!
end
```

サポートデスクへのお問い合わせ

サポートデスクへのお問い合わせに関して

サポートデスクにお問い合わせ頂く際は、以下の情報をお知らせ頂けると効率よく対応させて頂くことが可能ですので、ご協力をお願い致します。

※FutureNet サポートデスク宛にご提供頂きました情報は、製品のお問合せなどサポート業務以外の目的には利用致しません。
なおご提供頂く情報の取り扱いについて制限等がある場合には、お問い合わせ時または事前にその旨ご連絡下さい。(設定ファイルのプロバイダ情報や IPsec の事前共有鍵情報を削除してお送り頂く場合など)
弊社のプライバシーポリシーについては下記 URL の内容をご確認下さい。
http://www.centurysys.co.jp/company/philosophy.html#tab3
http://www.centurysys.co.jp/company/philosophy.html#tab4

■ ご利用頂いている NXR 製品を含むネットワーク構成図
(ご利用頂いている回線やルータを含むネットワーク機器の IP アドレスを記載したもの)

■ 障害・不具合の内容およびその再現手順
(いつどこで何を行った場合にどんな問題が発生したのかをできるだけ具体的にお知らせ下さい)

□ 問い合わせ内容例 1

〇月〇日〇〇時〇〇分頃より拠点 A と拠点 B の間で IPsec による通信ができなくなった。障害発生前までは問題なく利用可能だった。現在当該拠点のルータの LAN 側 IP アドレスに対して Ping による疎通は確認できたが、対向ルータの LAN 側 IP アドレス,配下の端末に対しては Ping による疎通は確認できない。障害発生前後で拠点 B のバックアップ回線としてモバイルカードを接続し、ppp1 インタフェースの設定を行った。設定を元に戻すと通信障害は解消する。
機器の内蔵時計は NTP で同期を行っている。

□ 問い合わせ内容例 2

- 発生日時
  〇月〇日〇〇時〇〇分頃
- 発生拠点
  拠点 AB 間
- 障害内容
  IPsec による通信ができなくなった。
- 切り分け内容
  ルータ配下の端末から当該拠点のルータの LAN 側 IP アドレスに対して Ping による疎通確認可能。
  対向ルータの LAN 側 IP アドレス,配下の端末に対しては Ping による疎通確認不可。
- 障害発生前後での作業
  ルータの設定変更やネットワークに影響する作業は行っていない。
- 備考

障害発生前までは問題なく利用可能だった。
機器の内蔵時計は拠点 A の機器で 10 分、拠点 B の機器で 5 分遅れている。

□ 問い合わせ内容例 3
現在 IPsec の設定中だが、一度も IPsec SA の確立および IPsec の通信ができていない。IPsec を設定している拠点からのインターネットアクセスおよび該当拠点への Ping による疎通確認も可能。
設定例集,設定例集内のログ一覧および NXR シスログ一覧は未確認。

□ 良くない問い合わせ内容例 1
VPN ができない。
→VPN として利用しているプロトコルは何か。VPN のトンネルが確立できないのか、通信ができないのかなど不明。

□ 良くない問い合わせ内容例 2
通信ができない。
→どのような通信がいつどこでできない(またはできなくなった)のかが不明。

NXR での情報取得方法は以下のとおりです。
※情報を取得される前に
シリアル接続で情報を取得される場合は取得前に下記コマンドを実行してください。
#terminal width 180(初期値に戻す場合は terminal no width)

■ ご利用頂いている NXR 製品での不具合発生時のログ
ログは以下のコマンドで出力されます。
#show syslog message

■ ご利用頂いている NXR 製品のテクニカルサポート情報の結果
テクニカルサポート情報は以下のコマンドで出力されます。
show tech-support

■ 障害発生時のモバイル関連コマンドの実行結果(モバイルカード利用時のみ)
#show mobile <N> ap
#show mobile <N> phone-number
#show mobile <N> signal-level
※<N>はモバイルデバイスナンバ

サポートデスクのご利用に関して

電話サポート

電話番号：0422-37-8926

電話での対応は以下の時間帯で行います。

月曜日 ～ 金曜日 10:00 - 17:00

ただし、国の定める祝祭日、弊社の定める年末年始は除きます。

電子メールサポート

E-mail： support@centurysys.co.jp

ＦＡＸサポート

FAX 番号：0422-55-3373

電子メール、FAX は 毎日 24 時間受け付けております。

ただし、システムのメンテナンスやビルの電源点検のため停止する場合があります。 その際は弊社ホームページ等にて事前にご連絡いたします。

FutureNet NXR,WXR 設定例集

IPsec 編

Ver 1.5.0

2014 年 3 月

発行　センチュリー・システムズ株式会社