FutureNet NXR シリーズ

IPsec 設定例集

Ver 1.0.0

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 製品に対応しております。
  - NXR-120/C, NXR-125/CX, NXR-130/C, NXR-1200
- 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 の以下のバージョンをベースに作成しております。
  FutureNet NXR シリーズ NXR-120/C Ver5.9.0
  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場合にのみ利用可能です。
- 本バージョンでは IPv4 のみを対象とし、IPv6 の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

NXR 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２種類の方式の IPsec 機能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, 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 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。
この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 機能は以下のファームウェアから対応しています。

- NXR-120/C Ver5.8.0～
- NXR-125/CX Ver5.8.1～
- NXR-1200 Ver5.8.2～

※2010 年 10 月現在

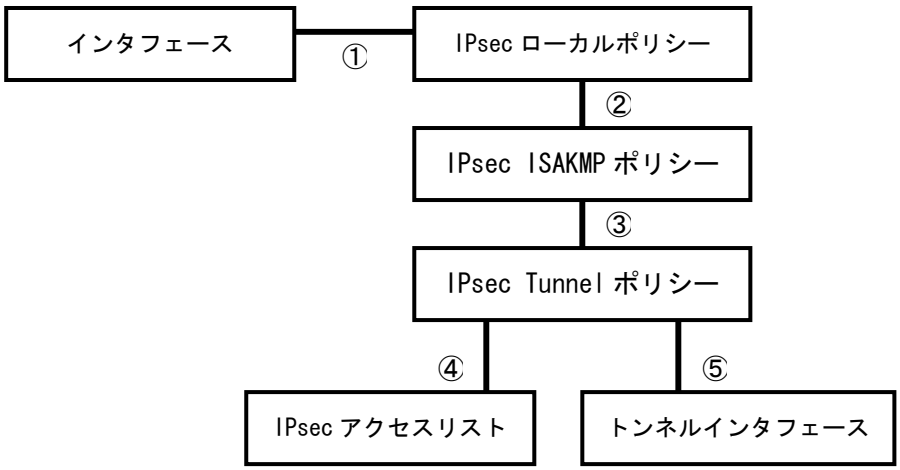
・Policy Based IPsec と Route Based IPsec の機能比較

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 シリーズの IPsec 設定の関連付け

NXR 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 アクセスリスト設定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)

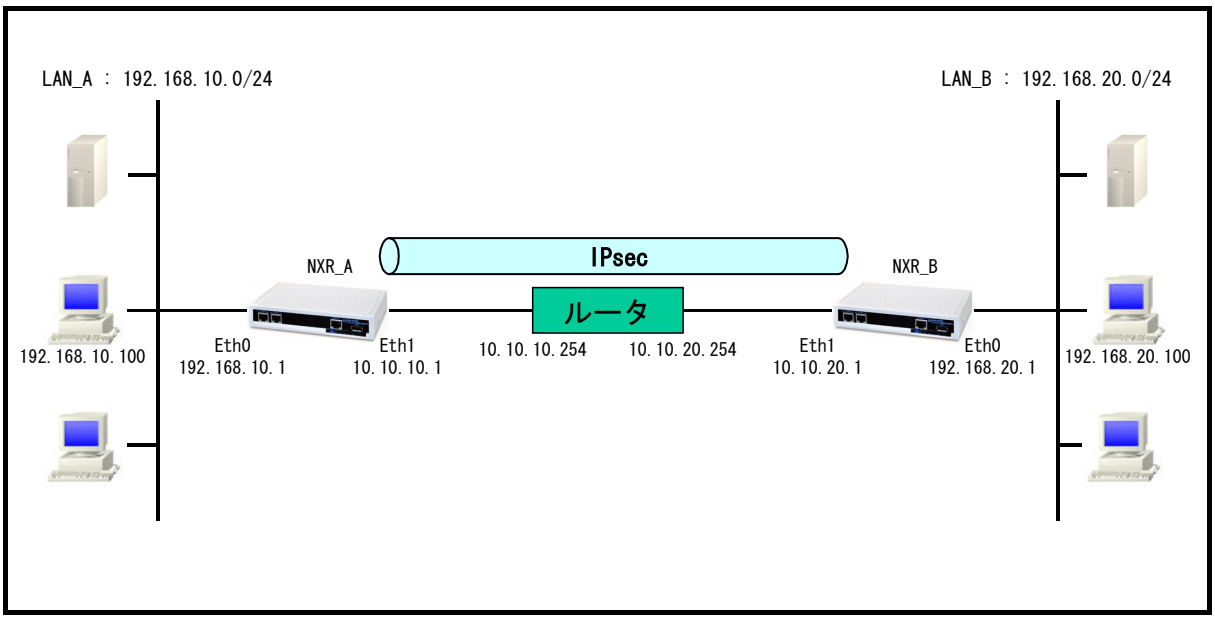
⑤トンネルインタフェース設定で、IPsec トンネルポリシー設定を指定する場合は以下のコマンドを設定します。(Route Based IPsec のみ)
  # tunnel protection ipsec policy N (N は IPsec トンネルポリシー番号)
  ※その他にトンネルインタフェースを IPsec で使用する場合は以下のコマンドが必要です。
    # tunnel mode ipsec ipv4 # tunnel mode ipsec ipv4

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。

※デフォルトで設定されているプロポーザルに関しては、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	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)

・ 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
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 10 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)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
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 10 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)#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. ＜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
```

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_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
```

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。
ここでは 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。

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、ここでは NXR_B と設定します。

```
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、事前共有鍵として ipseckey を設定します。
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
```

認証アルゴリズムを設定します。ここでは sha1 を設定します。

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

暗号化アルゴリズムを設定します。ここでは aes128 を設定します。

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

Diffie-Hellman(DH)グループを設定します。ここでは group 5 を設定します。

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

ISAKMP SA のライフタイムを設定します。ここでは 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。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 10 3 periodic restart
```

IKE KeepAlive(DPD)を設定します。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。
ここでは監視を 10 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に設定します。

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

関連づけを行う IPsec ローカルポリシーを指定します。
ここでは 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_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、ここでは NXR_B と設定します。

```
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を設定します。この設定によって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 esp-aes128, 認証アルゴリズム esp-sha1-hmac 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 を使用し、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 のライフタイムを設定します。ここでは 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 ポリシーを指定します。

ここでは ISAKMP ポリシー１と関連づけを行います。

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

使用する IPsec アクセスリストを指定します。

ここでは IPsec アクセスリスト LAN_B を設定します。

8. ＜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
```

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
```

このインタフェースが IPsec トンネルのエンドポイントとなるよう設定します。

ここで指定するのは、IPsec ローカルポリシーとなります。

ここでは IPsec ローカルポリシー１を設定します。

〔NXR_B の設定〕

1. ＜ホスト名の設定＞

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

ホスト名を NXR_B と設定します。

2. ＜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
```

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 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
```

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。

ここでは 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を設定します。

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_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_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、ここでは NXR_A と設定します。

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

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。

対向の NXR の WAN 側 IP アドレスとして 10.10.10.1 を設定します。

その他の設定内容は NXR_A と同等ですので、詳細は、6. ＜IPsec ISAKMP ポリシー設定＞をご参照下さい。

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_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 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。

トンネルポリシー１の説明として、ここでは NXR_B と設定します。

ここでは使用する IPsec アクセスリスト LAN_A を設定します。

その他の設定内容は NXR_A と同等ですので、詳細は 7. ＜IPsec トンネルポリシー設定＞をご参照下さい。

8. ＜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
```

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。

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

このインタフェースが IPsec トンネルのエンドポイントとなるよう設定します。

ここで指定するのは、IPsec ローカルポリシーとなります。

ここでは IPsec ローカルポリシー１を設定します。

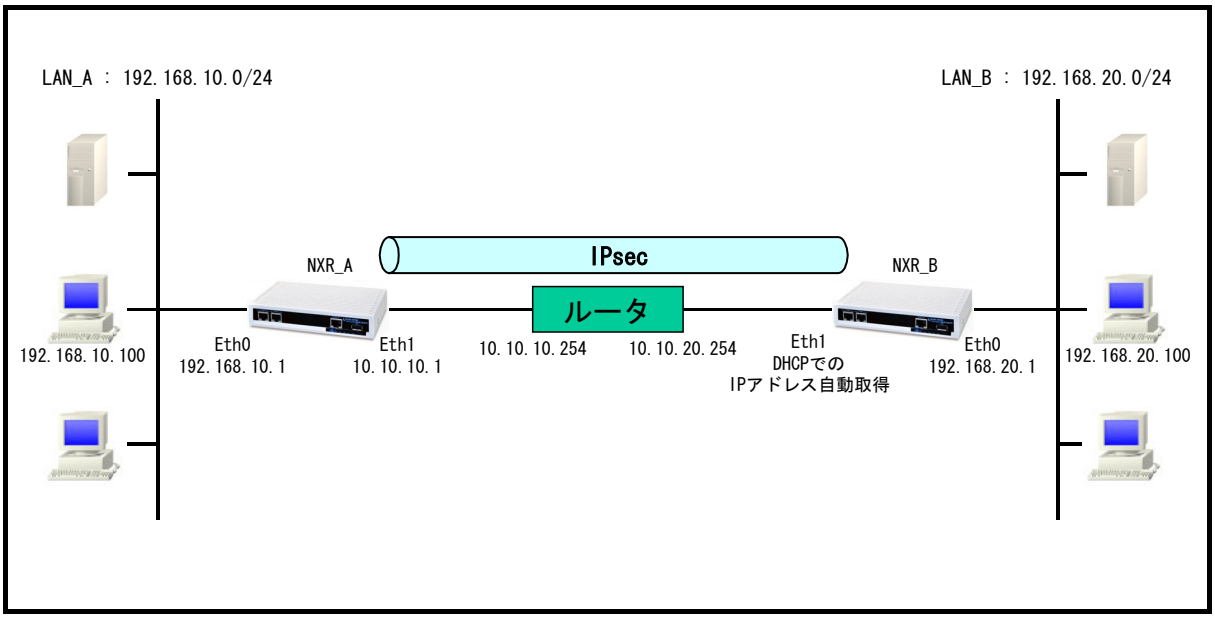
【 パソコンの設定例 】

	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	192.168.10.1	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。ただしもう一方の NXR の WAN 側 IP アドレスは固定 IP アドレスが必須となります。

【 構成図 】



- IPsec トンネルを構築する際は、必ず動的 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。
  ※デフォルトで設定されているプロポーザルに関しては、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	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)

- 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
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 10 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)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
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 10 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)#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. ＜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
```

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_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
```

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。
ここでは 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。

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、ここでは NXR_B と設定します。

```
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、事前共有鍵として ipseckey を設定します。
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
```

認証アルゴリズムを設定します。ここでは sha1 を設定します。

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

暗号化アルゴリズムを設定します。ここでは aes128 を設定します。

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

Diffie-Hellman(DH)グループを設定します。ここでは group 5 を設定します。

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

ISAKMP SA のライフタイムを設定します。ここでは 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を設定します。ここでは 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。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。ここでは ID として nxrb を fqdn 方式で設定します。

```
NXR_A(config-ipsec-isakmp)#keepalive 10 3 periodic clear
```

IKE KeepAlive(DPD)を設定します。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。
ここでは監視を 10 秒間隔で 3 回リトライを行い、keepalive 失敗時に SA を削除します。IKE のネゴシエーションは開始しません。

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

関連づけを行う IPsec ローカルポリシーを指定します。
ここでは 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_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、ここでは NXR_B 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を設定します。この設定によって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 esp-aes128, 認証アルゴリズム esp-sha1-hmac 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 を使用し、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 のライフタイムを設定します。ここでは 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 ポリシーを指定します。

ここでは ISAKMP ポリシー１と関連づけを行います。

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

使用する IPsec アクセスリストを指定します。

ここでは IPsec アクセスリスト LAN_B を設定します。

8. ＜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
```

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
```

このインタフェースが IPsec トンネルのエンドポイントとなるよう設定します。

ここで指定するのは、IPsec ローカルポリシーとなります。

ここでは IPsec ローカルポリシー１を設定します。

〔NXR_B の設定〕

1. ＜ホスト名の設定＞

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

ホスト名を NXR_B と設定します。

2. ＜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
```

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. ＜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
```

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。

ここでは 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
```

IPsec ローカルポリシー１を設定します。

```
NXR_B(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。

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

本装置の identity を設定します。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。ここでは ID として nxrb を fqdn 方式で設定します。

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_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 10 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
```

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、ここでは NXR_A と設定します。

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

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。

対向の NXR の WAN 側 IP アドレスとして 10.10.10.1 を設定します。

IKE KeepAlive(DPD)は、ここでは監視を 10 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に設定します。

その他の設定内容は NXR_A と同等ですので、詳細は、6. ＜IPsec ISAKMP ポリシー設定＞をご参照下さい。

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_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_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。

トンネルポリシー１の説明として、ここでは NXR_A と設定します。

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。

ここでは使用する IPsec アクセスリスト LAN_A を設定します。

その他の設定内容は NXR_A と同等ですので、詳細は、7. ＜IPsec トンネルポリシー設定＞をご参照下さい。

7. ＜Ethernet1 インタフェース設定＞

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

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。

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

このインタフェースが IPsec トンネルのエンドポイントとなるよう設定します。

ここで指定するのは、IPsec ローカルポリシーとなります。

ここでは IPsec ローカルポリシー１を設定します。

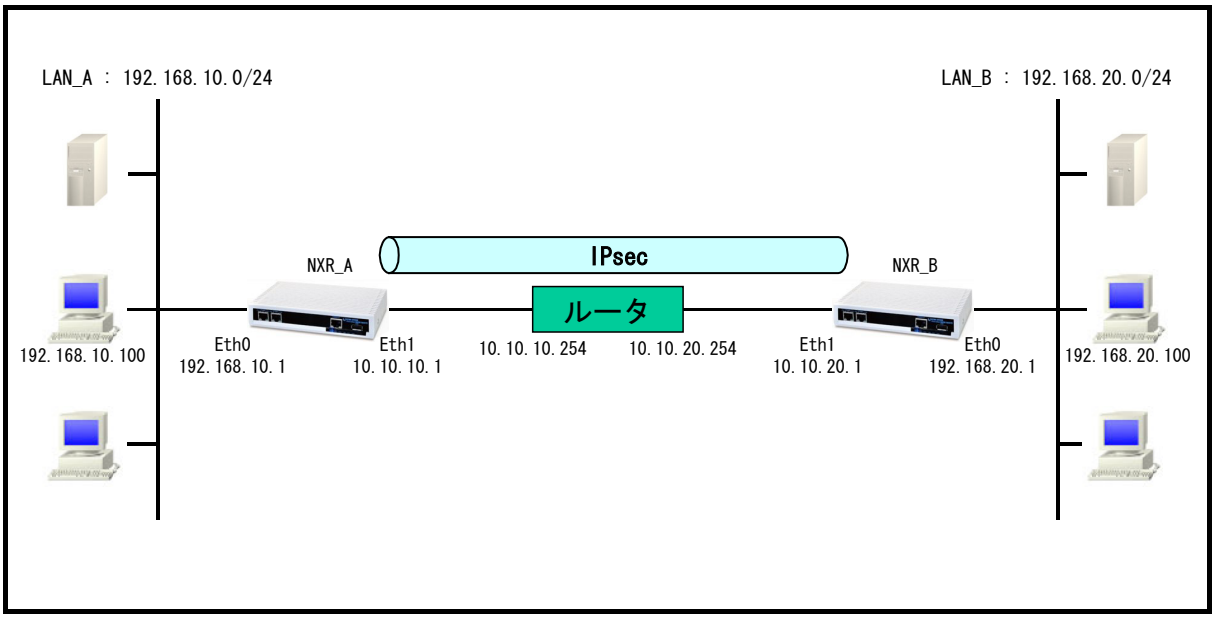
【 パソコンの設定例 】

	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	192.168.10.1	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 】



- 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。
- 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。

【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
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 :
0sAQNyjiS2aqmmPHvKp6GvDIVG6eC6yclJxWRk+syfUozTqPW7OR3TcFP74gjNZp3p16GN3SET2/M9+qVQIySERsh3
rBrzEuwzJQ/ShSv7XwJw7Awb2hlsZ8NvFKkIQ9AEGPOF223KT3T8O7QjxuX5wNToUWqJKZgURAoWIpY9ufM2qw==
NXR_A#configure terminal
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 0sAQOZe2V6nfz4pY9P/I5XONiGgTDjY6yUZ+cPSI
np9dAZqe9QLQwtDitiHZMUo2Liz2/8NIvq78+Vz7/rdNhoKAPDO7cqndlbPR1EnmaLfyNRC2Je19CJyHjCCz0vOL5q
Ob+eFKbAK3icFzi1ryr3tRCA2VIox57Wn2W7KkD96j5urQ==
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 10 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)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
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 :
0sAQOZe2V6nfz4pY9P/I5XONiGgTDjY6yUZ+cPSInp9dAZqe9QLQwtDitiHZMUo2Liz2/8NIvq78+Vz7/rdNhoKAPD
O7cqndlbPR1EnmaLfyNRC2Je19CJyHjCCz0v0L5qOb+eFKbAK3icFzi1ryr3tRCA2VIox57Wn2W7KkD96j5urQ==
NXR_B#configure terminal
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 0sAQNyjiS2aqmmPHvKp6GvDIVG6eC6yclJxWRk+s
yfUozTqPW7OR3TcFP74gjNZp3p16GN3SET2/M9+qVQIySERsh3rBrzEuwzJQ/ShSv7XwJw7Awb2hlsZ8NvFKkIQ9AE
GPOF223KT3T8O7QjxuX5wNToUWqJKZgURAoWlpY9ufM2qw==
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 10 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)#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. ＜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
```

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_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
```

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。

ここでは 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。

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 :
0sAQNyjiS2aqmmPHvKp6GvDIVG6eC6yclJxWRk+syfUozTqPW7OR3TcFP74gjNZp3p16GN3SET2/M9+qVQIySERsh3
rBrzEuwzJQ/ShSv7XwJw7Awb2hlsZ8NvFKkIQ9AEGPOF223KT3T8O7QjxuX5wNToUWqJKZgURAoWIpY9ufM2qw==
```

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。

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

本装置の identity を設定します。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。ここでは ID として nxra を fqdn 方式で設定します。

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、ここでは NXR_B と設定します。

```
NXR_A(config-ipsec-isakmp)#authentication rsa-sig 0sAQ0Ze2V6nfz4pY9P/l5X0NiGgTDjY6yUZ+cPSInp9dAZqe9QLQwtDitiHZMUo2Liz2/8Nlvq78+Vz7/rdNhoKAPD07cqndlbPR1EnmaLfyNRC2Je19CJyHjCCz0v0L5qOb+eFKbAK3icFzi1ryr3tRCA2Vlox57Wn2W7KkD96j5urQ==
```

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
```

認証アルゴリズムを設定します。ここでは sha1 を設定します。

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

暗号化アルゴリズムを設定します。ここでは aes128 を設定します。

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

Diffie-Hellman(DH)グループを設定します。ここでは group 5 を設定します。

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

ISAKMP SA のライフタイムを設定します。ここでは 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
```

対向機器の identity を設定します。ここでは ID として nxrb を fqdn 方式で設定します。

```
NXR_A(config-ipsec-isakmp)#keepalive 10 3 periodic restart
```

IKE KeepAlive(DPD)を設定します。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。
ここでは監視を 10 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に設定します。

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

関連づけを行う IPsec ローカルポリシーを指定します。
ここでは 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_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、ここでは NXR_B と設定します。

```
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を設定します。この設定によって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 esp-aes128, 認証アルゴリズム esp-sha1-hmac 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 を使用し、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 のライフタイムを設定します。ここでは 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 ポリシーを指定します。

ここでは ISAKMP ポリシー１と関連づけを行います。

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

使用する IPsec アクセスリストを指定します。

ここでは IPsec アクセスリスト LAN_B 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)#ip address 10.10.10.1/24
```

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
```

このインタフェースが IPsec トンネルのエンドポイントとなるよう設定します。

ここで指定するのは、IPsec ローカルポリシーとなります。

ここでは IPsec ローカルポリシー１を設定します。

〔NXR_B の設定〕

1. ＜ホスト名の設定＞

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

ホスト名を NXR_B と設定します。

2. ＜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
```

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 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
```

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。

ここでは 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 :
0sAQOZe2V6nfz4pY9P/I5XONiGgTDjY6yUZ+cPSInp9dAZqe9QLQwtDitiHZMUo2Liz2/8NIvq78+Vz7/rdNhoKAPD
O7cqndlbPR1EnmaLfyNRC2Je19CJyHjCCz0v0L5qOb+eFKbAK3icFzi1ryr3tRCA2VIox57Wn2W7KkD96j5urQ==
```

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
```

IPsec ローカルポリシー１を設定します。

```
NXR_B(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。

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

本装置の identity を設定します。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。ここでは ID として nxrb を fqdn 方式で設定します。

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 0sAQNyjiS2aqmmPHvKp6GvDIVG6eC6ycIJxWRk+s
yfUozTqPW70R3TcFP74gjNZp3p16GN3SET2/M9+qVQIySERsh3rBrzEuwzJQ/ShSv7XwJw7Awb2hlsZ8NvFKkIQ9AE
GP0F223KT3T807QjxuX5wNToUWqJKZgURAoWIpY9ufM2qw==
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 10 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
```

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、ここでは NXR_A と設定します。

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。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。

対向の NXR の WAN 側 IP アドレスとして 10.10.10.1 を設定します。

対向の NXR の identity を設定します。ここでは ID として nxra を fqdn 方式で設定します。

その他の設定内容は NXR_A と同等ですので、詳細は、8. ＜IPsec ISAKMP ポリシー設定＞をご参照下さい。

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_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_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。

トンネルポリシー１の説明として、ここでは NXR_A と設定します。

ここでは使用する IPsec アクセスリスト LAN_A を設定します。

その他の設定内容は NXR_A と同等ですので、詳細は、9. ＜IPsec トンネルポリシー設定＞をご参照下さい。

10. ＜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
```

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。

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

このインタフェースが IPsec トンネルのエンドポイントとなるよう設定します。

ここで指定するのは、IPsec ローカルポリシーとなります。

ここでは IPsec ローカルポリシー１を設定します。

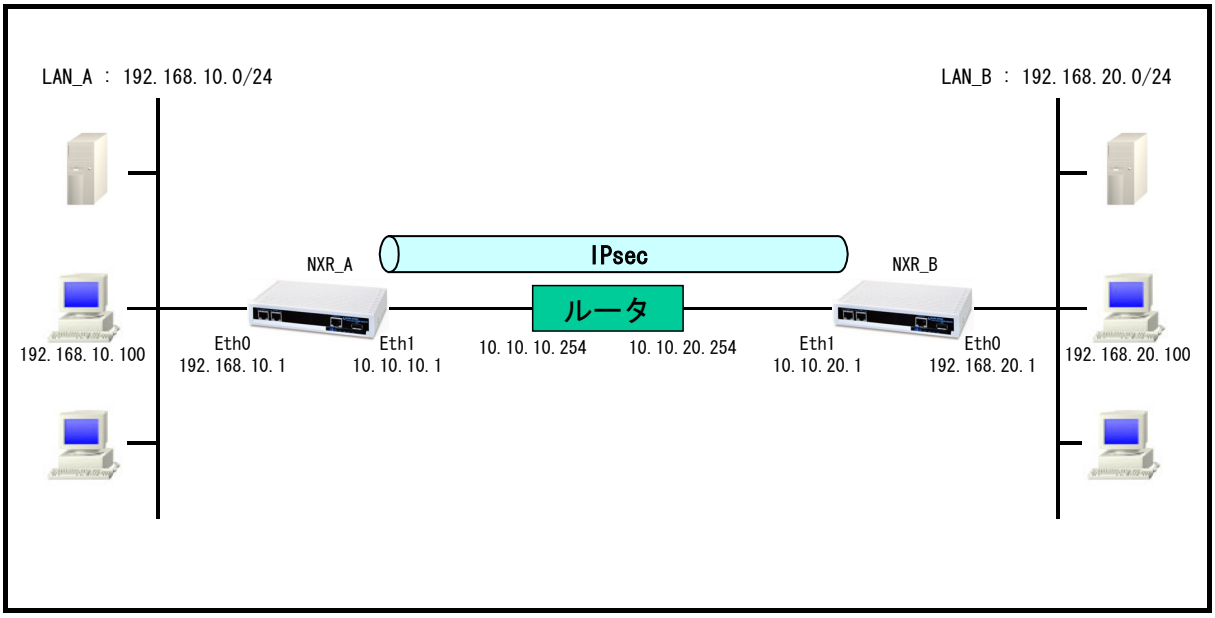
【 パソコンの設定例 】

	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	192.168.10.1	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 のフェーズ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）。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 】



- 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 または 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。

【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
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 hidden 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 10 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)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
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 hidden 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 10 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)#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. ＜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
```

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_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
```

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。

ここでは 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。

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 hidden nxrapass
```

NXR_A 用秘密鍵のパスフレーズである nxrapass を設定し、かつそのパスフレーズを暗号化するため 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。

```
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。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。ですので、設定前に証明書の DN または subject 等をご確認下さい。
ここでは/C=JP/CN=nxra/E=nxra@example.com を設定します。
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、ここでは NXR_B と設定します。

```
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
```

認証アルゴリズムを設定します。ここでは sha1 を設定します。

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

暗号化アルゴリズムを設定します。ここでは aes128 を設定します。

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

Diffie-Hellman(DH)グループを設定します。ここでは group 5 を設定します。

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

ISAKMP SA のライフタイムを設定します。ここでは 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。
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。
ここでは/C=JP/CN=nxrb/E=nxrb@example.com を設定します。
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 10 3 periodic restart
```

IKE KeepAlive(DPD)を設定します。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。
ここでは監視を 10 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に設定します。

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

関連づけを行う IPsec ローカルポリシーを指定します。
ここでは IPsec ローカルポリシー１と関連づけを行います。

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、ここでは NXR_B と設定します。

```
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を設定します。この設定によって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 esp-aes128, 認証アルゴリズム esp-sha1-hmac 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 を使用し、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 のライフタイムを設定します。ここでは 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 ポリシーを指定します。
ここでは ISAKMP ポリシー１と関連づけを行います。

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

使用する IPsec アクセスリストを指定します。
ここでは IPsec アクセスリスト LAN_B を設定します。

14. ＜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
```

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
```

このインタフェースが IPsec トンネルのエンドポイントとなるよう設定します。
ここで指定するのは、IPsec ローカルポリシーとなります。
ここでは IPsec ローカルポリシー１を設定します。

〔NXR_B の設定〕

1. ＜ホスト名の設定＞

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

ホスト名を NXR_B と設定します。

2. ＜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
```

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 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
```

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。

ここでは 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 hidden 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＞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
```

IPsec ローカルポリシー１を設定します。

```
NXR_B(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。

```
NXR_B(config-ipsec-local)#x509 certificate nxrb
```

X.509 で利用する証明書を指定します。ここでは 5. NXR_B 用公開鍵証明書の設定で設定した 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。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。ですので、設定前に証明書の DN または subject 等をご確認下さい。
ここでは/C=JP/CN=nxrb/E=nxrb@example.com を設定します。
なお X.509 を利用する場合は、identity 設定は必須になります。

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_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 10 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
```

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、ここでは NXR_A と設定します。
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。
対向の NXR の WAN 側 IP アドレスとして 10.10.10.1 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。
その他の設定内容は NXR_A と同等ですので、詳細は 12. ＜IPsec ISAKMP ポリシー設定＞をご参照下さい。

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_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_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。
トンネルポリシー１の説明として、ここでは NXR_A と設定します。
ここでは使用する IPsec アクセスリスト LAN_A を設定します。
その他の設定内容は NXR_A と同等ですので、詳細は 13. ＜IPsec トンネルポリシー設定＞をご参照下さい。

9. ＜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
```

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。

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

このインタフェースが IPsec トンネルのエンドポイントとなるよう設定します。

ここで指定するのは、IPsec ローカルポリシーとなります。

ここでは IPsec ローカルポリシー１を設定します。

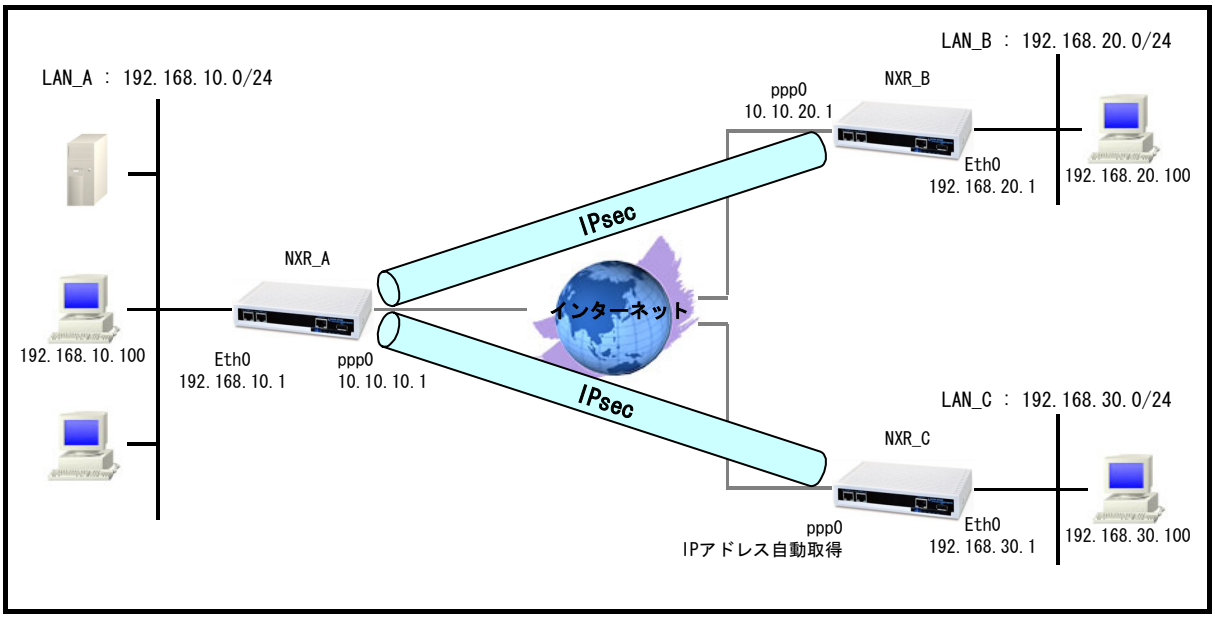
【 パソコンの設定例 】

	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	192.168.10.1	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。なおここでは拠点間の IPsec 経由での通信は行いません。
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。

【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
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 10 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 10 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

----- 次のページに続きがあります -----
```

```
----- 前のページからの続きです -----

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 authentication auto
NXR_A(config-ppp)#ppp username test1@centurysys 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(dns-config)#service enable
NXR_A(dns-config)#exit
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
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 10 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 authentication auto
NXR_B(config-ppp)#ppp username test2@centurysys 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(dns-config)#service enable
NXR_B(dns-config)#exit
NXR_B(config)#exit
NXR_B#save config
```

〔NXR_C の設定〕

```
nxr120#configure terminal
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 10 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 authentication auto
NXR_C(config-ppp)#ppp username test3@centurysys 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(dns-config)#service enable
NXR_C(dns-config)#exit
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. ＜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
```

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_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。PPPoE を利用する場合は、通常ゲートウェイとして ppp 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ように設定します。

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ように設定します。

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
```

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。

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。

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１＞

```
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、ここでは NXR_B と設定します。

```
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、事前共有鍵として ipseckey1 を設定します。

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
```

認証アルゴリズムを設定します。ここでは sha1 を設定します。

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

暗号化アルゴリズムを設定します。ここでは aes128 を設定します。

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

Diffie-Hellman(DH)グループを設定します。ここでは group 5 を設定します。

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

ISAKMP SA のライフタイムを設定します。ここでは 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。ここでは NXR_A, NXR_B ともに WAN 側 IP アドレスが固定 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_B 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 10 3 periodic restart
```

IKE KeepAlive(DPD)を設定します。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。
ここでは監視を 10 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に設定します。

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

関連づけを行う IPsec ローカルポリシーを指定します。
ここでは 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１＞

```
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、ここでは NXR_B と設定します。

```
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を設定します。この設定によって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 esp-aes128, 認証アルゴリズム esp-sha1-hmac 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 を使用し、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 のライフタイムを設定します。ここでは 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 ポリシーを指定します。

ここでは ISAKMP ポリシー１と関連づけを行います。

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

使用する IPsec アクセスリストを指定します。

ここでは IPsec アクセスリスト LAN_B を設定します。

9. ＜IPsec ISAKMP ポリシー設定２＞

```
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、ここでは NXR_C と設定します。

```
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、事前共有鍵として ipseckey2 を設定します。

この設定は、対向の NXR_C と同じ値を設定する必要があります。

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

認証アルゴリズムを設定します。ここでは sha1 を設定します。

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

暗号化アルゴリズムを設定します。ここでは aes128 を設定します。

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

Diffie-Hellman(DH)グループを設定します。ここでは group 5 を設定します。

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

ISAKMP SA のライフタイムを設定します。ここでは 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、アグレッシブモードを設定します。

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

NXR_C の WAN 側 IP アドレスを設定します。ここでは 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
```

対向機器の identity を設定します。本設定が必要な理由は、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。ここでは ID として nxrc を fqdn 方式で設定します。

```
NXR_A(config-ipsec-isakmp)#keepalive 10 3 periodic clear
```

IKE KeepAlive(DPD)を設定します。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。
ここでは監視を 10 秒間隔で 3 回リトライを行い、keepalive 失敗時に SA を削除します。IKE のネゴシエーションは開始しません。

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

関連づけを行う IPsec ローカルポリシーを指定します。
ここでは IPsec ローカルポリシー１と関連づけを行います。

10. ＜IPsec トンネルポリシー設定２＞

```
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、ここでは 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を設定します。この設定によって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 esp-aes128, 認証アルゴリズム esp-sha1-hmac 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 を使用し、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 のライフタイムを設定します。ここでは 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 ポリシーを指定します。

ここでは ISAKMP ポリシー２と関連づけを行います。

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

使用する IPsec アクセスリストを指定します。

ここでは IPsec アクセスリスト LAN_C を設定します。

11. ＜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
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 authentication auto
NXR_A(config-ppp)#ppp username test1@centurysys password test1pass
NXR_A(config-ppp)#ipsec policy 1
```

ppp0 インタフェースを設定します。

固定の IP アドレスが割り当てられているため、IP アドレス 10.10.10.1/32 を設定します。

IP マスカレードによる NAT 設定およびステートフルパケットインスペクションによるフィルタを設定します。

IP アクセスリスト設定で設定した ppp0-in を in フィルタに適用します。これにより ppp0 インタフェースで受信した NXR 自身宛のパケットに対して IP アクセスリストによるチェックが行われます。

IPsec ローカルポリシー１を適用します。これによりこのインタフェースが IPsec トンネルのエンドポイントとなります。

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

13. ＜DNS 設定＞

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

DNS サービスを有効にします。

〔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. ＜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
```

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 ppp 0
```

デフォルトルートを設定します。通常ゲートウェイとして ppp 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ように設定します。

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ように設定します。

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。

(☞) 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
```

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。

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
```

IPsec ローカルポリシー１を設定します。

```
NXR_B(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１＞

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

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

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

ISAKMP ポリシー１の説明として、ここでは NXR_A と設定します。

```
NXR_B(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、事前共有鍵として ipseckey1 を設定します。
この設定は、対向の NXR_A と同じ値を設定する必要があります。

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

認証アルゴリズムを設定します。ここでは sha1 を設定します。

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

暗号化アルゴリズムを設定します。ここでは aes128 を設定します。

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

Diffie-Hellman(DH)グループを設定します。ここでは group 5 を設定します。

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

ISAKMP SA のライフタイムを設定します。ここでは 10800 秒を設定します。

```
NXR_B(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。ここでは NXR_A, NXR_B ともに WAN 側 IP アドレスが固定 IP アドレスのため、メインモードを設定します。

```
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
```

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

```
NXR_B(config-ipsec-isakmp)#keepalive 10 3 periodic restart
```

IKE KeepAlive(DPD)を設定します。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。
ここでは監視を 10 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に設定します。

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

関連づけを行う IPsec ローカルポリシーを指定します。
ここでは 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１＞

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

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。

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

トンネルポリシー１の説明として、ここでは NXR_A と設定します。

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

IPsec ポリシーのネゴシエーションモードを設定します。この設定によって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_B(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 esp-aes128, 認証アルゴリズム esp-sha1-hmac を設定します。

```
NXR_B(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 を使用し、DH グループとして group5 を設定します。

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

IPsec SA のライフタイムを設定します。ここでは 3600 秒を設定します。

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

関連づけを行う ISAKMP ポリシーを指定します。
ここでは ISAKMP ポリシー１と関連づけを行います。

```
NXR_B(config-ipsec-tunnel)#match address LAN_A
```

使用する IPsec アクセスリストを指定します。
ここでは IPsec アクセスリスト LAN_A を設定します。

9. ＜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
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 authentication auto
NXR_B(config-ppp)#ppp username test2@centurysys password test2pass
NXR_B(config-ppp)#ipsec policy 1
```

ppp0 インタフェースを設定します。

固定の IP アドレスが割り当てられているため、IP アドレス 10.10.20.1/32 を設定します。

IP マスカレードによる NAT 設定およびステートフルパケットインスペクションによるフィルタを設定します。

IP アクセスリスト設定で設定した ppp0-in を in フィルタに適用します。これにより ppp0 インタフェースで受信した NXR 自身宛のパケットに対して IP アクセスリストによるチェックが行われます。

IPsec ローカルポリシー１を適用します。これによりこのインタフェースが IPsec トンネルのエンドポイントとなります。

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

11. ＜DNS 設定＞

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

DNS サービスを有効にします。

〔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. ＜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
```

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。

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。通常ゲートウェイとして ppp 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ように設定します。

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ように設定します。

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。

(☞) 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
```

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。

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
```

IPsec ローカルポリシー１を設定します。

```
NXR_C(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。

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

本装置の identity を設定します。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 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。ここでは ID として nxrc を fqdn 方式で設定します。

7. ＜IPsec ISAKMP ポリシー設定１＞

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

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

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

ISAKMP ポリシー１の説明として、ここでは NXR_A と設定します。

```
NXR_C(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、事前共有鍵として ipseckey2 を設定します。
この設定は、対向の NXR_A と同じ値を設定する必要があります。

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

認証アルゴリズムを設定します。ここでは sha1 を設定します。

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

暗号化アルゴリズムを設定します。ここでは aes128 を設定します。

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

Diffie-Hellman(DH)グループを設定します。ここでは group 5 を設定します。

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

ISAKMP SA のライフタイムを設定します。ここでは 10800 秒を設定します。

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

フェーズ１のネゴシエーションモードを設定します。ここでは本装置の 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_C(config-ipsec-isakmp)#remote address ip 10.10.10.1
```

対向の NXR_A の WAN 側 IP アドレスを設定します。ここでは対向の NXR_A の WAN 側 IP アドレス 10.10.10.1 を設定します。

```
NXR_C(config-ipsec-isakmp)#keepalive 10 3 periodic restart
```

IKE KeepAlive(DPD)を設定します。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。
ここでは監視を 10 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に設定します。

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

関連づけを行う IPsec ローカルポリシーを指定します。

ここでは 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１＞

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

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。

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

トンネルポリシー１の説明として、ここでは NXR_A と設定します。

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

IPsec ポリシーのネゴシエーションモードを設定します。この設定によって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_C(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 esp-aes128, 認証アルゴリズム esp-sha1-hmac を設定します。

```
NXR_C(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 を使用し、DH グループとして group5 を設定します。

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

IPsec SA のライフタイムを設定します。ここでは 3600 秒を設定します。

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

関連づけを行う ISAKMP ポリシーを指定します。

ここでは ISAKMP ポリシー１と関連づけを行います。

```
NXR_C(config-ipsec-tunnel)#match address LAN_A
```

使用する IPsec アクセスリストを指定します。

ここでは IPsec アクセスリスト LAN_A を設定します。

9. ＜ppp0 インタフェース設定＞

```
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 authentication auto
NXR_C(config-ppp)#ppp username test3@centurysys password test3pass
NXR_C(config-ppp)#ipsec policy 1
```

ppp0 インタフェースを設定します。

動的 IP アドレスが割り当てられているため、IP アドレスとして negotiated を設定します。

IP マスカレードによる NAT 設定およびステートフルパケットインスペクションによるフィルタを設定します。

IP アクセスリスト設定で設定した ppp0-in を in フィルタに適用します。これにより ppp0 インタフェースで受信した NXR 自身宛のパケットに対して IP アクセスリストによるチェックが行われます。

IPsec ローカルポリシー１を適用します。これによりこのインタフェースが IPsec トンネルのエンドポイントとなります。

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

11. ＜DNS 設定＞

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

DNS サービスを有効にします。

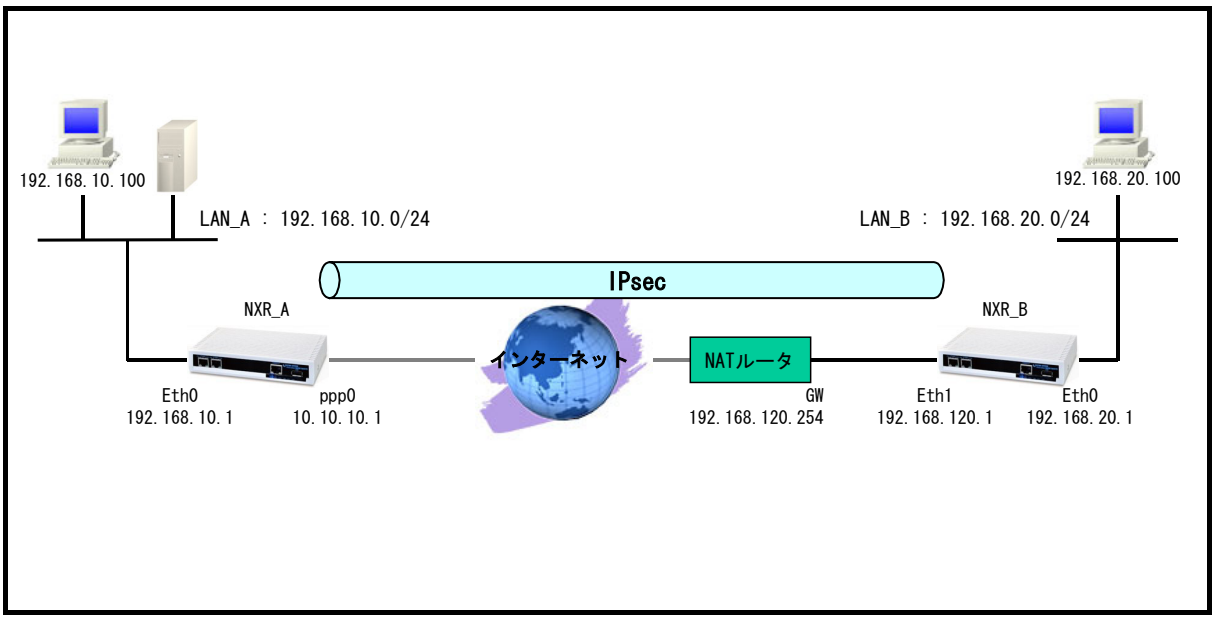
【 パソコンの設定例 】

	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

1-6. 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 NATPT 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)。
- 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の設定および NXR_B へのルート設定が完了しているものとします。

【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
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
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 authentication auto
NXR_A(config-ppp)#ppp username test1@centurysys 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(dns-config)#service enable
NXR_A(dns-config)#exit
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
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
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)#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_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(dns-config)#service enable
NXR_B(dns-config)#exit
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. ＜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
```

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。PPPoE を利用する場合は、通常ゲートウェイとして ppp 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ように設定します。

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ように設定します。

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
```

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 IPv4 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。

IPsec アクセスリスト名を LAN_B とし、送信元 IPv4 アドレス 192.168.10.0/24, 宛先 IPv4 アドレス 192.168.20.0/24 を設定します。

6. ＜IPsec NAT トラバーサルの有効化＞

```
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 と指定したそのインタフェースの 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、ここでは NXR_B と設定します。

```
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、事前共有鍵として ipseckey を設定します。
この設定は、対向 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
```

認証アルゴリズムを設定します。ここでは sha1 を設定します。

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

暗号化アルゴリズムを設定します。ここでは aes128 を設定します。

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

Diffie-Hellman(DH)グループを設定します。ここでは group 5 を設定します。

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

ISAKMP SA のライフタイムを設定します。ここでは 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、アグレッシブモードを設定します。

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

NXR_B の WAN 側 IP アドレスを設定します。ここでは 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、any を設定します。

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

対向機器の identity を設定します。本設定が必要な理由は、NXR_B の WAN 側 IP アドレスがプライベート IP アドレスのためです。ここでは ID として nxrb を fqdn 方式で設定します。

```
NXR_A(config-ipsec-isakmp)#keepalive 10 3 periodic clear
```

IKE KeepAlive(DPD)を設定します。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 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。

ここでは監視を 10 秒間隔で 3 回リトライを行い、keepalive 失敗時に SA を削除します。IKE のネゴシエーションは開始しません。

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

関連づけを行う IPsec ローカルポリシーを指定します。
ここでは 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_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、ここでは NXR_B 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を設定します。この設定によって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 esp-aes128, 認証アルゴリズム esp-sha1-hmac 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 を使用し、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 のライフタイムを設定します。ここでは 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 ポリシーを指定します。
ここでは ISAKMP ポリシー１と関連づけを行います。

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

使用する IPsec アクセスリストを指定します。
ここでは IPsec アクセスリスト LAN_B を設定します。

10. ＜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
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 authentication auto
NXR_A(config-ppp)#ppp username test1@centurysys password test1pass
NXR_A(config-ppp)#ipsec policy 1
```

ppp0 インタフェースを設定します。

固定の IP アドレスが割り当てられているため、IP アドレス 10.10.10.1/32 を設定します。

IP マスカレードによる NAT 設定およびステートフルパケットインスペクションによるフィルタを設定します。

IP アクセスリスト設定で設定した ppp0-in を in フィルタに適用します。これにより ppp0 インタフェースで受信した NXR 自身宛のパケットに対して IP アクセスリストによるチェックが行われます。

IPsec ローカルポリシー１を適用します。これによりこのインタフェースが IPsec トンネルのエンドポイントとなります。

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 インタフェースを PPPoE クライアントとし、ppp0 インタフェースを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 サービスを有効にします。

〔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. ＜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
```

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
```

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。
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
```

IPsec ローカルポリシー１を設定します。

```
NXR_B(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 と指定したそのインタフェースの IP アドレスが自動的に設定されます。

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

本装置の identity を設定します。本設定が必要な理由は、WAN 側 IP アドレスがプライベート IP アドレスのためです。ここでは ID として nxrb を fqdn 方式で設定します。

7. ＜IPsec ISAKMP ポリシー設定＞

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

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

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

ISAKMP ポリシー１の説明として、ここでは NXR_A と設定します。

```
NXR_B(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、事前共有鍵として ipseckey を設定します。
この設定は、対向の NXR_A と同じ値を設定する必要があります。

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

認証アルゴリズムを設定します。ここでは sha1 を設定します。

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

暗号化アルゴリズムを設定します。ここでは aes128 を設定します。

```
NXR_B(config-ipsec-isakmp)#group 5
```
Diffie-Hellman(DH)グループを設定します。ここでは group 5 を設定します。

```
NXR_B(config-ipsec-isakmp)#lifetime 10800
```
ISAKMP SA のライフタイムを設定します。ここでは 10800 秒を設定します。

```
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
```
フェーズ１のネゴシエーションモードを設定します。ここでは本装置の WAN 側 IPv4 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_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
```
対向の NXR_A の WAN 側 IP アドレスを設定します。ここでは対向の NXR_A の WAN 側 IP アドレス 10.10.10.1 を設定します。

```
NXR_B(config-ipsec-isakmp)#keepalive 10 3 periodic restart
```
IKE KeepAlive(DPD)を設定します。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。
ここでは監視を 10 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に設定します。

```
NXR_B(config-ipsec-isakmp)#local policy 1
```
関連づけを行う IPsec ローカルポリシーを指定します。
ここでは 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_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。

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

```
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
```
IPsec ポリシーのネゴシエーションモードを設定します。この設定によって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_B(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 esp-aes128, 認証アルゴリズム esp-sha1-hmac を設定します。

```
NXR_B(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 を使用し、DH グループとして group5 を設定します。

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

IPsec SA のライフタイムを設定します。ここでは 3600 秒を設定します。

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

関連づけを行う ISAKMP ポリシーを指定します。

ここでは ISAKMP ポリシー１と関連づけを行います。

```
NXR_B(config-ipsec-tunnel)#match address LAN_A
```

使用する IPsec アクセスリストを指定します。

ここでは IPsec アクセスリスト LAN_A を設定します。

9. ＜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
```

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。

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

このインタフェースが IPsec トンネルのエンドポイントとなるよう設定します。

ここで指定するのは、IPsec ローカルポリシーとなります。

ここでは 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(dns-config)#service enable
```

DNS サービスを有効にします。

【 パソコンの設定例 】

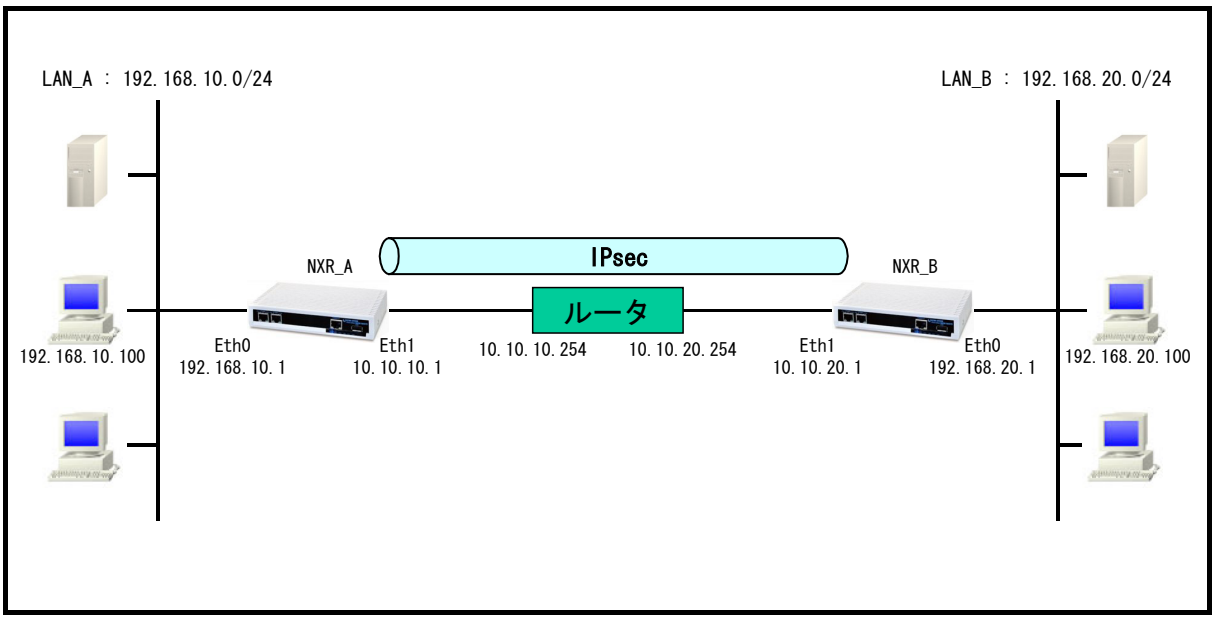
	LAN A のパソコン	LAN B のパソコン
IP アドレス	192.168.10.100	192.168.20.100
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1

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 では Policy Based IPsec での設定に対して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
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
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 10 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 tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
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)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
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
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 10 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 tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
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)#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
```

IPsec で使用するスタティックルートを設定します。

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。

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。

ここでは LAN_B 向けのルートで NXR_B との間の IPsec トンネルにトンネル１インタフェースを使用しますので、ゲートウェイインタフェースは tunnel 1 を設定します。

2. ＜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
```

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。

ここでは 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。

3. ＜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ので、ipsec policy 1 と設定します。

(☞) 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_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
```

IPsec で使用するスタティックルートを設定します。
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。
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。
ここでは LAN_A 向けのルートで NXR_A との間の IPsec トンネルにトンネル 1 インタフェースを使用していますので、ゲートウェイインタフェースは tunnel 1 を設定します。

2. ＜IPsec アクセスリスト設定＞

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

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。

ここでは 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。

3. ＜トンネルインタフェース設定＞

```
NXR_B(config)#interface tunnel 1
```

トンネル 1 インタフェースを設定します。

```
NXR_B(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_B(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ので、ipsec policy 1 と設定します。

(☞) IPsec ローカルポリシーではありませんので、ご注意下さい。

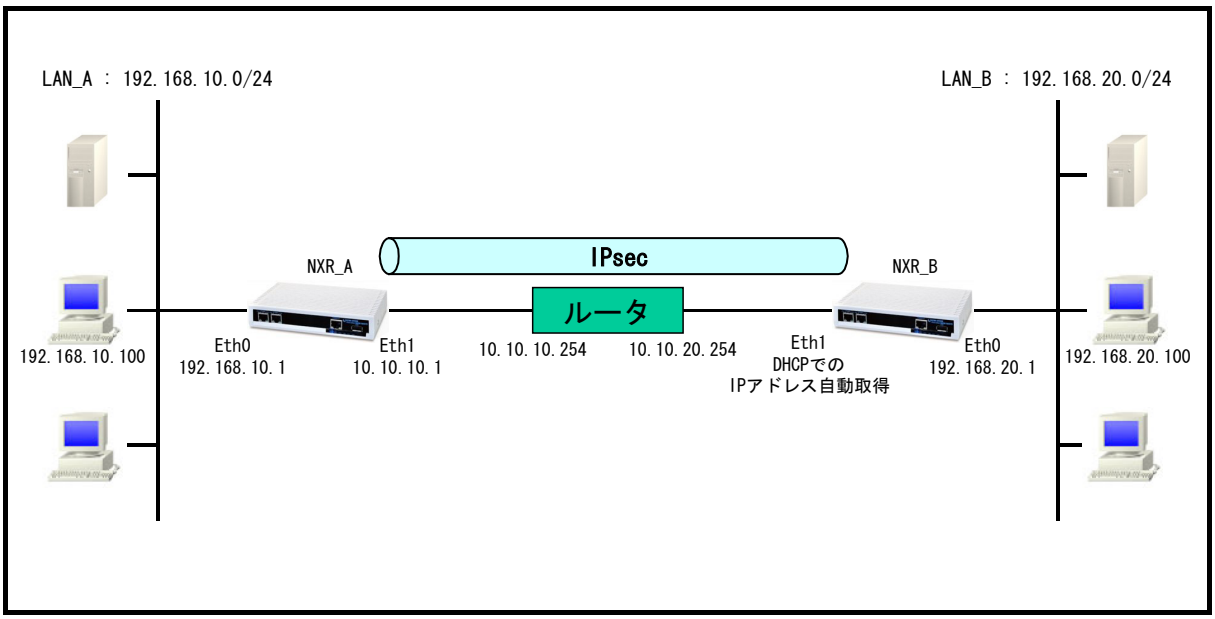
【 パソコンの設定例 】

	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 アドレスが接続の度に変わる動的 IP アドレス環境でも IPsec を利用することが可能です。ただしもう一方の NXR の WAN 側 IP アドレスは固定 IP アドレスが必須となります。
また ISAKMP のネゴシエーションでは、アグレッシブモードを使用します。

【 構成図 】



- Route Based IPsec では Policy Based IPsec での設定に対して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
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
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 10 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 tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
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)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
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
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 10 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 tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
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)#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
```

IPsec で使用するスタティックルートを設定します。
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。
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。
ここでは LAN_B 向けのルートで NXR_B との間の IPsec トンネルにトンネル 1 インタフェースを使用していますので、ゲートウェイインタフェースは tunnel 1 を設定します。

2. ＜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
```

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。

ここでは 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。

3. ＜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ので、ipsec policy 1 と設定します。

(☞) 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_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
```

IPsec で使用するスタティックルートを設定します。
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。
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。
ここでは LAN_A 向けのルートで NXR_A との間の IPsec トンネルにトンネル 1 インタフェースを使用していますので、ゲートウェイインタフェースは tunnel 1 を設定します。

2. ＜IPsec アクセスリスト設定＞

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

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。

ここでは 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。

3. ＜トンネルインタフェース設定＞

```
NXR_B(config)#interface tunnel 1
```

トンネル 1 インタフェースを設定します。

```
NXR_B(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_B(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ので、ipsec policy 1 と設定します。

(☞) IPsec ローカルポリシーではありませんので、ご注意下さい。

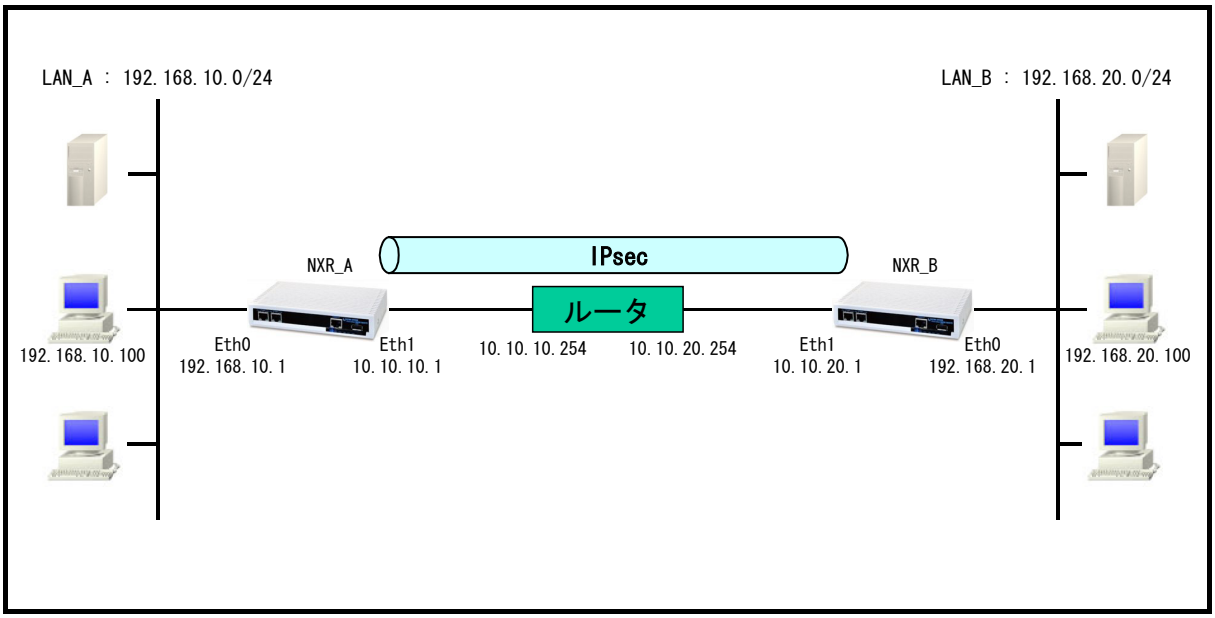
【 パソコンの設定例 】

	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 では Policy Based IPsec での設定に対して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
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
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 :
0sAQNyjiS2aqmmPHvKp6GvDIVG6eC6yclJxWRk+syfUozTqPW7OR3TcFP74gjNZp3p16GN3SET2/M9+qVQlySERsh3
rBrzEuwzJQ/ShSv7XwJw7Awb2hlsZ8NvFKkIQ9AEGPOF223KT3T8O7QjxuX5wNToUWqJKZgURAoWlpY9ufM2qw==
NXR_A#configure terminal
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 0sAQOZe2V6nfz4pY9P/I5XONiGgTDjY6yUZ+cPSI
np9dAZqe9QLQwtDitiHZMUo2Liz2/8NIvq78+Vz7/rdNhoKAPDO7cqndlbPR1EnmaLfyNRC2Je19CJyHjCCz0v0L5q
Ob+eFKbAK3icFzi1ryr3tRCA2VIox57Wn2W7KkD96j5urQ==
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 10 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 tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
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)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
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
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 :
0sAQOZe2V6nfz4pY9P/I5XONiGgTDjY6yUZ+cPSInp9dAZqe9QLQwtDitiHZMUo2Liz2/8NIvq78+Vz7/rdNhoKAPD
O7cqndlbPR1EnmaLfyNRC2Je19CJyHjCCzOvOL5qOb+eFKbAK3icFzi1ryr3tRCA2VIox57Wn2W7KkD96j5urQ==
NXR_B#configure terminal
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 0sAQNyjiS2aqmmPHvKp6GvDIVG6eC6yclJxWRk+s
yfUozTqPW7OR3TcFP74gjNZp3p16GN3SET2/M9+qVQIySERsh3rBrzEuwzJQ/ShSv7XwJw7Awb2hlsZ8NvFKkIQ9AE
GPOF223KT3T8O7QjxuX5wNToUWqJKZgURAoWlpY9ufM2qw==
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 10 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 tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
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)#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
```

IPsec で使用するスタティックルートを設定します。

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。

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。

ここでは LAN_B 向けのルートで NXR_B との間の IPsec トンネルにトンネル 1 インタフェースを使用していますので、ゲートウェイインタフェースは tunnel 1 を設定します。

2. ＜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
```

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。

ここでは 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。

3. ＜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ので、ipsec policy 1 と設定します。

(☞) 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_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
```

IPsec で使用するスタティックルートを設定します。
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。
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。
ここでは LAN_A 向けのルートで NXR_A との間の IPsec トンネルにトンネル 1 インタフェースを使用していますので、ゲートウェイインタフェースは tunnel 1 を設定します。

2. ＜IPsec アクセスリスト設定＞

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

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。

ここでは 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。

3. ＜トンネルインタフェース設定＞

```
NXR_B(config)#interface tunnel 1
```

トンネル 1 インタフェースを設定します。

```
NXR_B(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_B(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ので、ipsec policy 1 と設定します。

(☞) IPsec ローカルポリシーではありませんので、ご注意下さい。

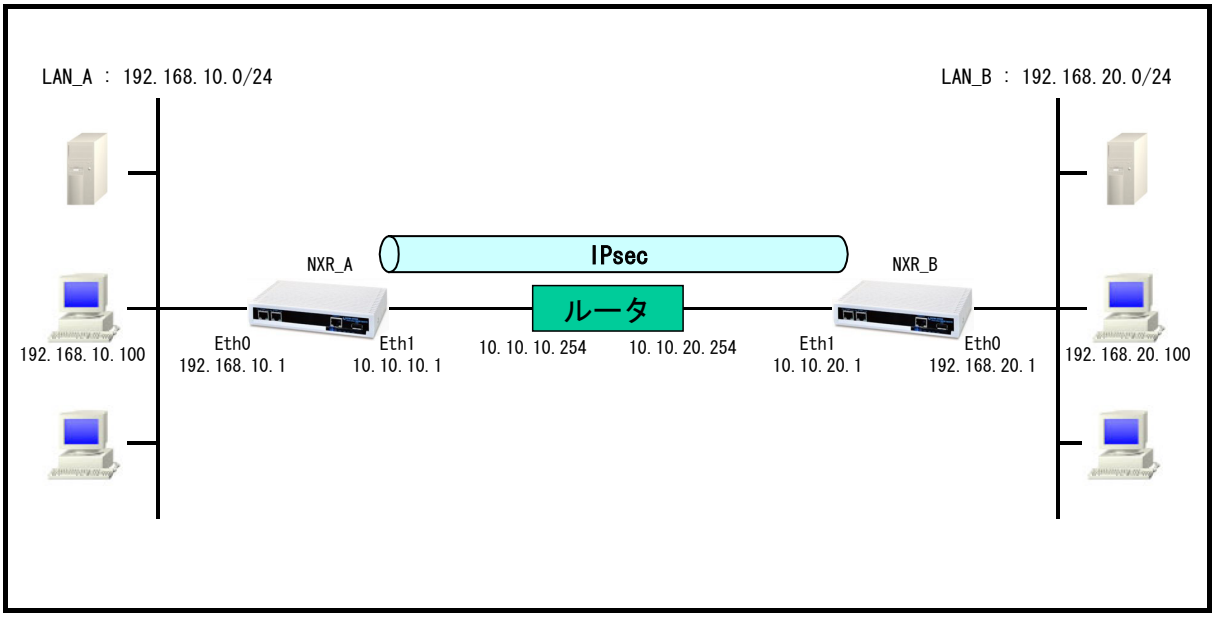
【 パソコンの設定例 】

	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 では Policy Based IPsec での設定に対して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
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
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 hidden 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 10 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 tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
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)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
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
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 hidden 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 10 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 tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
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)#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
```

IPsec で使用するスタティックルートを設定します。

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。

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。

ここでは LAN_B 向けのルートで NXR_B との間の IPsec トンネルにトンネル 1 インタフェースを使用していますので、ゲートウェイインタフェースは tunnel 1 を設定します。

2. ＜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
```

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。

ここでは 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。

3. ＜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ので、ipsec policy 1 と設定します。

(☞) 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_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
```

IPsec で使用するスタティックルートを設定します。
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。
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。
ここでは LAN_A 向けのルートで NXR_A との間の IPsec トンネルにトンネル 1 インタフェースを使用していますので、ゲートウェイインタフェースは tunnel 1 を設定します。

2. ＜IPsec アクセスリスト設定＞

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

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。

ここでは 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。

3. ＜トンネルインタフェース設定＞

```
NXR_B(config)#interface tunnel 1
```

トンネル 1 インタフェースを設定します。

```
NXR_B(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_B(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ので、ipsec policy 1 と設定します。

(☞) IPsec ローカルポリシーではありませんので、ご注意下さい。

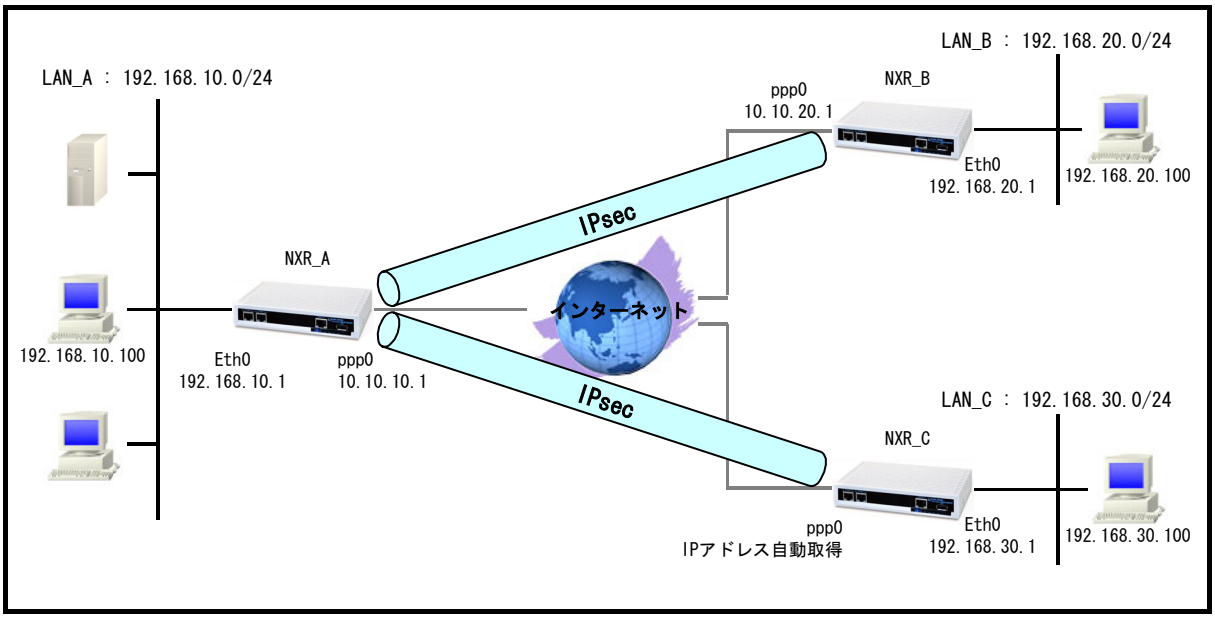
【 パソコンの設定例 】

	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。なおここでは拠点間の IPsec 経由での通信は行いません。
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 では Policy Based IPsec での設定に対して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。
- 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
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
NXR_A(config)#ip route 192.168.30.0/24 tunnel 2
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 10 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 tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
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 10 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

----- 次のページに続きがあります -----
```

```
----- 前のページからの続きです -----

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
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 tunnel 2
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 2
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 authentication auto
NXR_A(config-ppp)#ppp username test1@centurysys 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(dns-config)#service enable
NXR_A(dns-config)#exit
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
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
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 10 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 tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
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 authentication auto
NXR_B(config-ppp)#ppp username test2@centurysys 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(dns-config)#service enable
NXR_B(dns-config)#exit
NXR_B(config)#exit
NXR_B#save config
```

〔NXR_C の設定〕

```
nxr120#configure terminal
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
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 10 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 tunnel 1
NXR_C(config-tunnel)#tunnel mode ipsec ipv4
NXR_C(config-tunnel)#tunnel protection ipsec policy 1
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 authentication auto
NXR_C(config-ppp)#ppp username test3@centurysys 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(dns-config)#service enable
NXR_C(dns-config)#exit
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
NXR_A(config)#ip route 192.168.30.0/24 tunnel 2
```

IPsec で使用するスタティックルートを設定します。

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。

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。

一行目は LAN_B 向けのルートで NXR_B との間の IPsec トンネルにトンネル１インタフェースを使用していますので、ゲートウェイインタフェースは tunnel 1 を設定します。

二行目は LAN_C 向けのルートで NXR_C との間の IPsec トンネルにトンネル２インタフェースを使用していますので、ゲートウェイインタフェースは tunnel 2 を設定します。

2. ＜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
```

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。

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。

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)#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ので、ipsec policy 1 と設定します。

(☞) IPsec ローカルポリシーではありませんので、ご注意下さい。

4. ＜トンネル２インタフェース設定＞

```
NXR_A(config)#interface tunnel 2
```

トンネル２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 2
```

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２と関連づけを行いますので、ipsec policy 2 と設定します。

(☞) 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_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
```

IPsec で使用するスタティックルートを設定します。

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。

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。

ここでは LAN_A 向けのルートで NXR_A との間の IPsec トンネルにトンネル１インタフェースを使用していますので、ゲートウェイインタフェースは tunnel 1 を設定します。

2. ＜IPsec アクセスリスト設定＞

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

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。

ここでは 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。

3. ＜トンネルインタフェース設定＞

```
NXR_B(config)#interface tunnel 1
```

トンネル１インタフェースを設定します。

```
NXR_B(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_B(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ので、ipsec policy 1 と設定します。
(☞) 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_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
```

IPsec で使用するスタティックルートを設定します。
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。
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。
ここでは LAN_A 向けのルートで NXR_A との間の IPsec トンネルにトンネル１インタフェースを使用していますので、ゲートウェイインタフェースは tunnel 1 を設定します。

2. ＜IPsec アクセスリスト設定＞

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

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。
ここでは 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。

3. ＜トンネルインタフェース設定＞

```
NXR_C(config)#interface tunnel 1
```

トンネル１インタフェースを設定します。

```
NXR_C(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_C(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ので、ipsec policy 1 と設定します。

(☞) IPsec ローカルポリシーではありませんので、ご注意下さい。

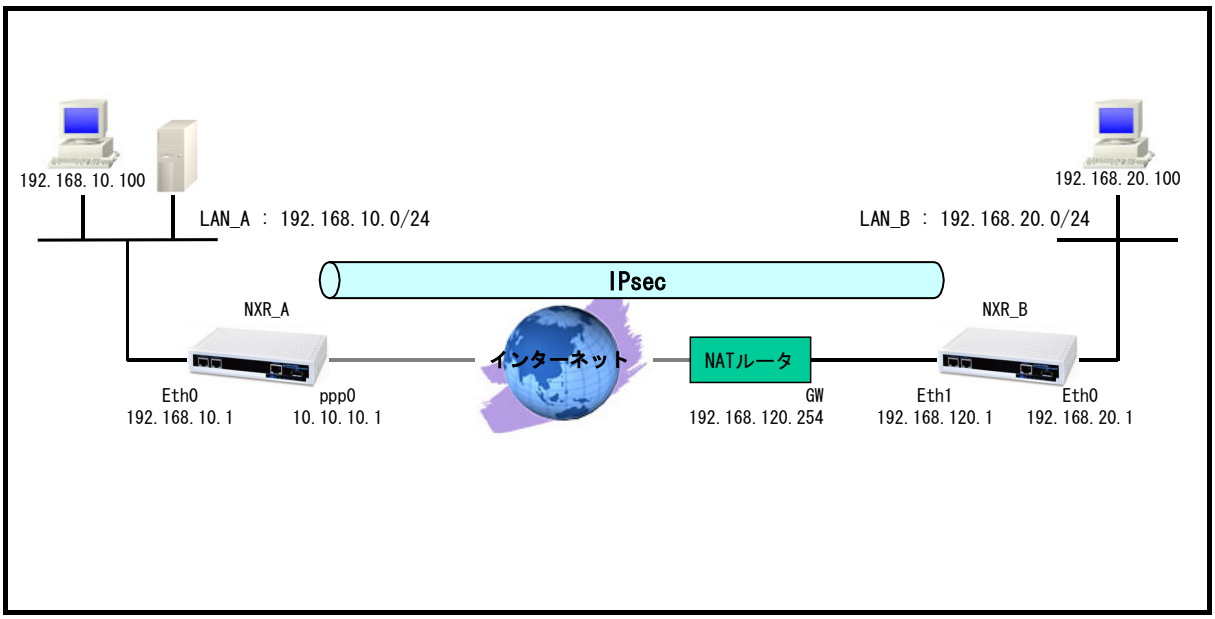
【 パソコンの設定例 】

	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

2-6. 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 では Policy Based IPsec での設定に対して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)
- 1-6. 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
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
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
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 10 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 tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
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 authentication auto
NXR_A(config-ppp)#ppp username test1@centurysys 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

----- 次のページに続きがあります -----
```

```
----- 前のページからの続きです -----

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

〔NXR_B の設定〕

```
nxr120#configure terminal
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
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
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 10 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 tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
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(dns-config)#service enable
NXR_B(dns-config)#exit
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、1-6. 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
```

IPsec で使用するスタティックルートを設定します。

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。

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。

ここでは LAN_B 向けのルートで NXR_B との間の IPsec トンネルにトンネル１インタフェースを使用していますので、ゲートウェイインタフェースは tunnel 1 を設定します。

2. ＜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
```

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。

ここでは 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。

3. ＜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ので、ipsec policy 1 と設定します。

(☞) 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_B の設定〕

(☞) ここに記載のない設定項目は、1-6. 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
```

IPsec で使用するスタティックルートを設定します。
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。
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。
ここでは LAN_A 向けのルートで NXR_A との間の IPsec トンネルにトンネル１インタフェースを使用していますので、ゲートウェイインタフェースは tunnel 1 を設定します。

2. ＜IPsec アクセスリスト設定＞

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

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。

ここでは 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。

3. ＜トンネルインタフェース設定＞

```
NXR_B(config)#interface tunnel 1
```

トンネル１インタフェースを設定します。

```
NXR_B(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_B(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ので、ipsec policy 1 と設定します。

(☞) IPsec ローカルポリシーではありませんので、ご注意下さい。

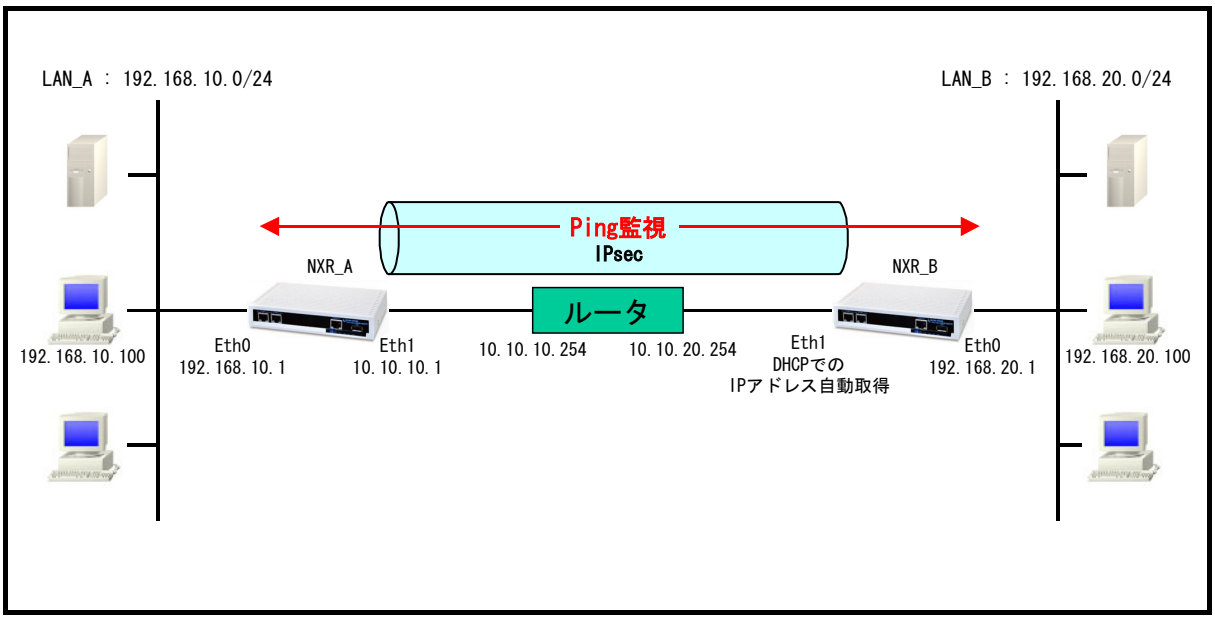
【 パソコンの設定例 】

	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

2-7. 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、２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 ポリシー設定で IPsec の再接続を指定します。
- 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
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
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 20 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 tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
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)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
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
NXR_B(config)# track 1 ip reachability 192.168.10.1 interface tunnel 1 10 3 delay 65
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 20 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 LAN_A
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)#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)#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 delay 65
```

Ping 監視を track No.1 として登録します。

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 down に状態遷移します。

ここでは delay も合わせて設定します。delay は復旧時(ステータスが up と認識した場合)から実際に up 時の動作を実行するまでの遅延時間を設定できます。

delay タイマが動作している場合は down 状態が維持され、この間も Ping 監視は行われます。なお delay タイマ中にダウンイベントを検知した場合は、delay タイマはキャンセルされます。

そして delay タイマがタイムアウトするとイベントアップとなります。このとき delay タイマ中にカウントした Ping 監視の失敗回数は 0 クリアされ、再度 Ping 監視が開始されます。

(☞) delay タイマがタイムアウトした場合は、netevent コマンドで指定した動作が実行されます。

2. ＜IPsec ISAKMP ポリシー設定＞

```
NXR_B(config-ipsec-isakmp)#netevent 1 reconnect
```

ISAKMP ポリシー１で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で障害を検知した場合に、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 Ping 監視で障害を検知した場合、IPsec トンネルの再接続を行う動作を指定します。

(☞) 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。

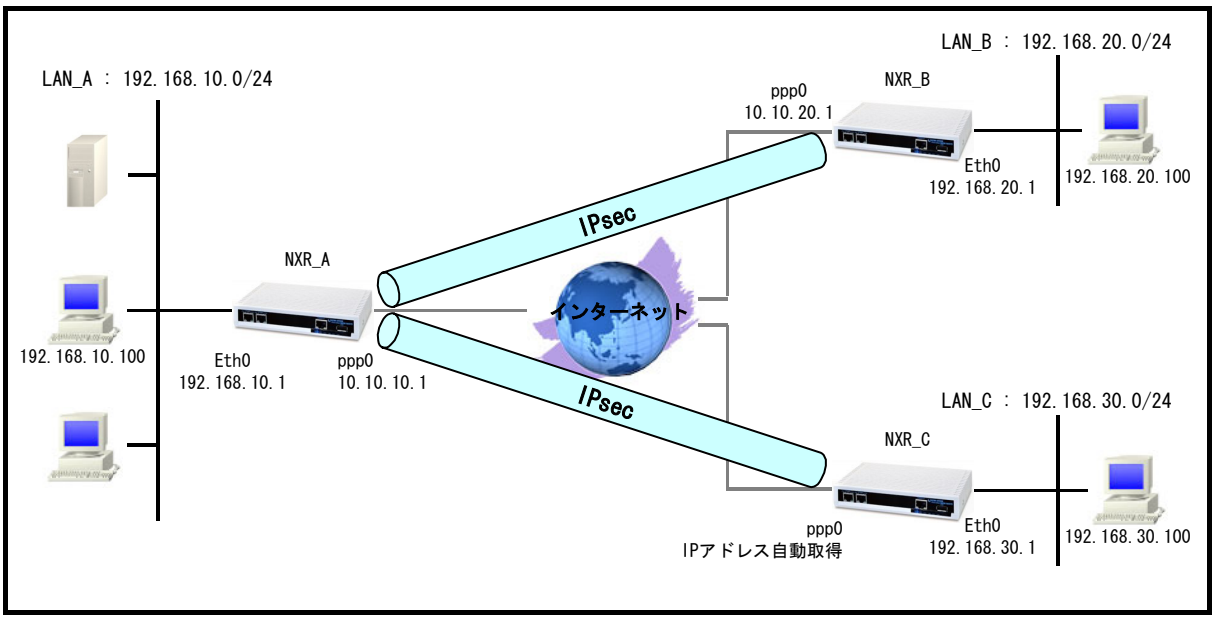
【 パソコンの設定例 】

	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

2-8. 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 の時と違い、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、各拠点からそれぞれ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 では Policy Based IPsec での設定に対して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)
- 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で OSPF を動作させる場合、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
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)#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 ethernet 0
NXR_A(config-router)#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 10 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 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)#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 10 3 periodic clear
NXR_A(config-ipsec-isakmp)#local policy 1
```

----- 次のページに続きがあります -----

```
----- 前のページからの続きです -----

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 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)#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 authentication auto
NXR_A(config-ppp)#ppp username test1@centurysys 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(dns-config)#service enable
NXR_A(dns-config)#exit
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
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)#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 ethernet 0
NXR_B(config-router)#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

----- 次のページに続きがあります -----
```

```
----- 前のページからの続きです -----

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 10 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 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)#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 authentication auto
NXR_B(config-ppp)#ppp username test2@centurysys 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(dns-config)#service enable
NXR_B(dns-config)#exit
NXR_B(config)#exit
NXR_B#save config
```

〔NXR_C の設定〕

```
nxr120#configure terminal
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)#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 ethernet 0
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

----- 次のページに続きがあります -----
```

----- 前のページからの続きです -----

```
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 10 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 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)#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 authentication auto
NXR_C(config-ppp)#ppp username test3@centurysys 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(dns-config)#service enable
NXR_C(dns-config)#exit
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 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 ethernet 0
```

パッシブインタフェースとして Ethernet0 を設定します。これは Ethernet0 インタフェース側の LAN に他に OSPF を動作させているルータがなく、Ethernet0 インタフェースから OSPF パケットのやりとりの必要がないためです。

2. ＜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
```

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。

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。

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 の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ので、ipsec policy 1 と設定します。

(☞) IPsec ローカルポリシーではありませんので、ご注意下さい。

4. ＜トンネル２インタフェース設定＞

```
NXR_A(config)#interface tunnel 2
```

トンネル２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２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。

(☞) トンネル２インタフェースと同一の IP アドレスを設定することができます。

```
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 2
```

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２と関連づけを行いますので、ipsec policy 2 と設定します。

(☞) 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_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
```

OSPF を設定します。

```
NXR_B(config-router)#router-id 172.31.0.2
```

OSPF のルータ ID を設定します。

```
NXR_B(config-router)#network 192.168.20.0/24 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。
これにより 192.168.20.0/24 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_B(config-router)#passive-interface ethernet 0
```

パッシブインタフェースとして Ethernet0 を設定します。これは Ethernet0 インタフェース側の LAN に他に OSPF を動作させているルータがなく、Ethernet0 インタフェースから OSPF パケットのやりとりの必要がないためです。

2. ＜IPsec アクセスリスト設定＞

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

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。

ここでは 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。

3. ＜トンネルインタフェース設定＞

```
NXR_B(config)#interface tunnel 1
```

トンネル１インタフェースを設定します。

```
NXR_B(config-tunnel)#ip address 192.168.20.1/32
```

トンネル１インタフェースの IP アドレスに 192.168.20.1/32 を設定します。
これによりトンネルインタフェースで OSPF の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_B(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_B(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ので、ipsec policy 1 と設定します。
(☞) 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_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
```

OSPF を設定します。

```
NXR_C(config-router)#router-id 172.31.0.3
```

OSPF のルータ ID を設定します。

```
NXR_C(config-router)#network 192.168.30.0/24 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。
これにより 192.168.30.0/24 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_C(config-router)#passive-interface ethernet 0
```

パッシブインタフェースとして Ethernet0 を設定します。これは Ethernet0 インタフェース側の LAN に他に OSPF を動作させているルータがなく、Ethernet0 インタフェースから OSPF パケットのやりとりの必要がないためです。

2. ＜IPsec アクセスリスト設定＞

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

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の有無で決まります。
ここでは 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。

3. ＜トンネルインタフェース設定＞

```
NXR_C(config)#interface tunnel 1
```

トンネル１インタフェースを設定します。

```
NXR_C(config-tunnel)#ip address 192.168.30.1/32
```

トンネル１インタフェースの IP アドレスに 192.168.30.1/32 を設定します。

これによりトンネルインタフェースで OSPF の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_C(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_C(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ので、ipsec policy 1 と設定します。

(☞) IPsec ローカルポリシーではありませんので、ご注意下さい。

【 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

付録

IPsec 接続確認方法

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。このコマンドでは 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。

実行例

```
nxr120#show ipsec status brief
TunnelName          Status
tunnel1             up
tunnel2             down
```

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(※)では IPsec 接続完了時には以下のように表示されます。ログは show syslog message コマンドで確認できます。

ログ出力例

```
pluto[XXXX]: added connection description "tunnel1"
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}
pluto[XXXX]: "tunnel1" #2: sent QI2, IPsec SA established {ESP=>0x7a5cb4c1 <0x9867e772 DPD}
```

※IPsec Aggressive mode Initiator log(IPv4)

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。

- ご利用頂いている NXR 製品の機種名,バージョン番号
- ご利用頂いている NXR 製品を含んだネットワーク構成
- 不具合の内容および不具合の再現手順（何を行った場合にどのよう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）
- ご利用頂いている NXR 製品での不具合発生時のログ（show syslog message）
- ご利用頂いている NXR 製品の設定ファイル, show tech-support コマンドの実行結果

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 AM - 5:00 PM

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 シリーズ

IPsec 設定例集

Ver 1.0.0

2010 年 10 月

発行　センチュリー・システムズ株式会社