# FutureNet NXR, WXR 設定例集

## IPsec 編

Ver 1.1.0

センチュリー・システムズ株式会社

# 目次

# はじめに

- FutureNet はセンチュリー・システムズ株式会社の登録商標です。
- 本書に記載されている会社名，製品名は、各社の商標および登録商標です。
- 本ガイドは、以下の FutureNet NXR, WXR 製品に対応しております。
  NXR-120/C, NXR-125/CX, NXR-130/C, NXR-155/C-WM, NXR-155/C-XW,
  NXR-155/C-L, NXR-230/C, NXR-350/C, NXR-1200, WXR-250
- 本書の内容の一部または全部を無断で転載することを禁止しています。
- 本書の内容については、将来予告なしに変更することがあります。
- 本書の内容については万全を期しておりますが、ご不審な点や誤り、記載漏れ等お気づきの点がありましたらお手数ですが、ご一報下さいますようお願い致します。
- 本書は FutureNet NXR-120/C 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 Ver5.22.2
  各種機能において、ご使用されている製品およびファームウェアのバージョンによっては、一部機能，コマンドおよび設定画面が異なっている場合もありますので、その場合は各製品のユーザーズガイドを参考に、適宜読みかえてご参照および設定を行って下さい。
- Route Based IPsec 機能は各製品で本機能が実装されているバージョンでのみ利用可能です。
- 本バージョンでは IPv4 のみを対象とし、IPv6 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 |
| 1.1.0 | 設定例を NXR-120/C Ver5.22.2 ベースに変更<br>第 3 章 L2TP/IPsec 追加<br>IPsec 接続確認方法更新<br>L2TP/IPsec 接続確認方法追加<br>設定例 show config 形式サンプル追加<br>FutureNet サポートデスクへのお問い合わせページ更新 |

# 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 NXR シリーズ，WXR シリーズ全製品で利用することができます。
※2013 年 4 月現在

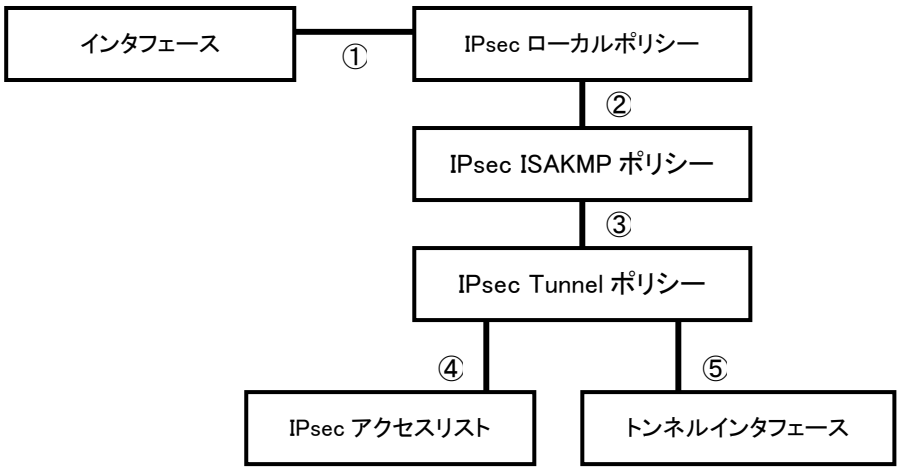
**・Policy Based IPsec と Route Based IPsec の機能比較**

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 | ○ | ×<br>（無効に設定してください） |
| NAT | △<br>（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<br>（OSPF/RIPv1/v2） | × | ○ |
| DF bit が 1 のパケットの<br>強制フラグメント | ○ | ○ |
| プレ/ポストフラグメントの選択 | ×<br>（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)<br>※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。

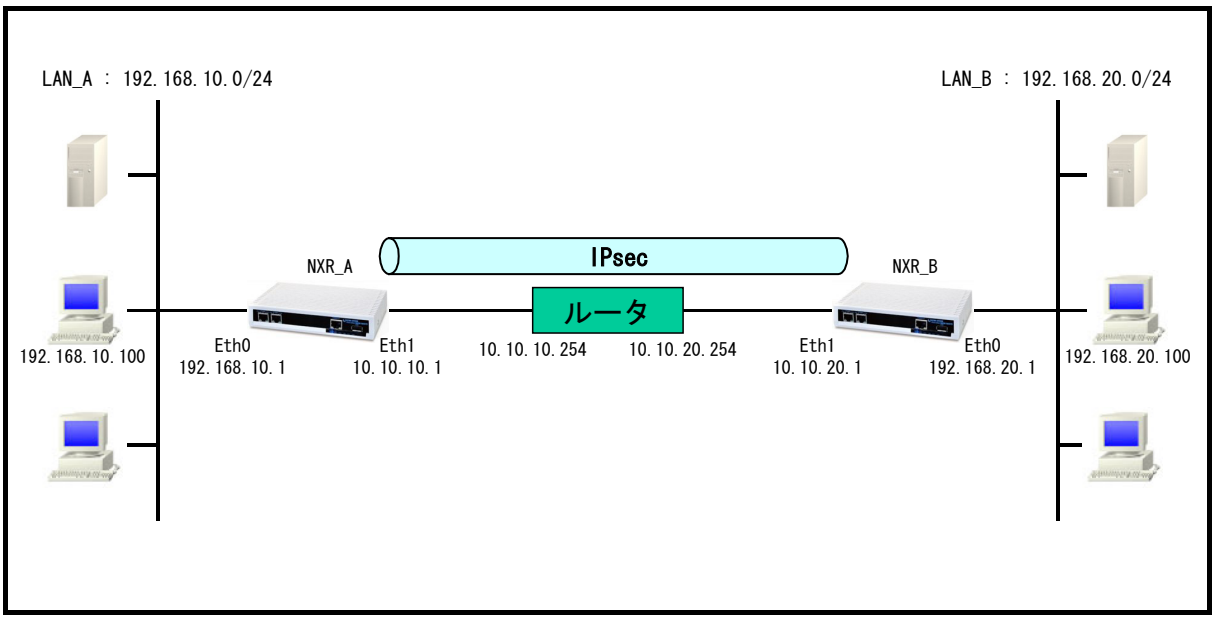
# tunnel mode ipsec ipv4

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

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 0.0.0.0/0 10.10.20.254
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address 10.10.20.1/24
NXR_B(config-if)#ipsec policy 1
NXR_B(config-if)#exit
NXR_B(config)#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 30 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 30 秒間隔で 3 回リトライを行い、keepalive 失敗時に SA を削除し、IKE のネゴシエーションを開始するように設定します。

```
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。

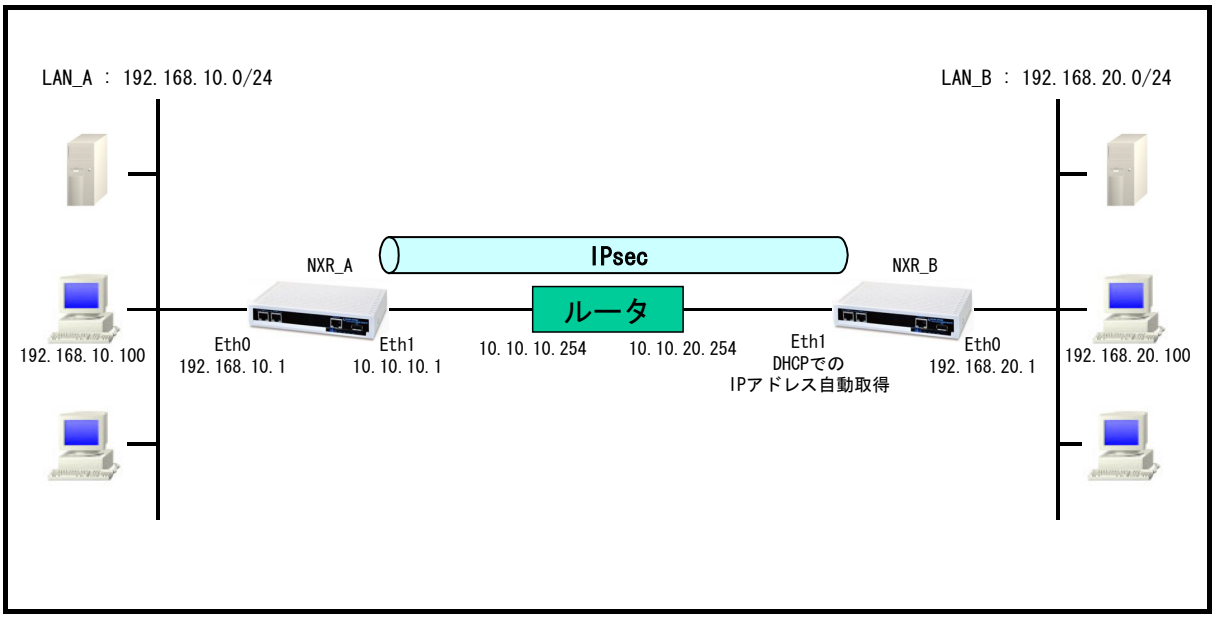
## 【 パソコンの設定例 】

| | 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 アドレスが必要となります。

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

〔NXR_B の設定〕

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

**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。

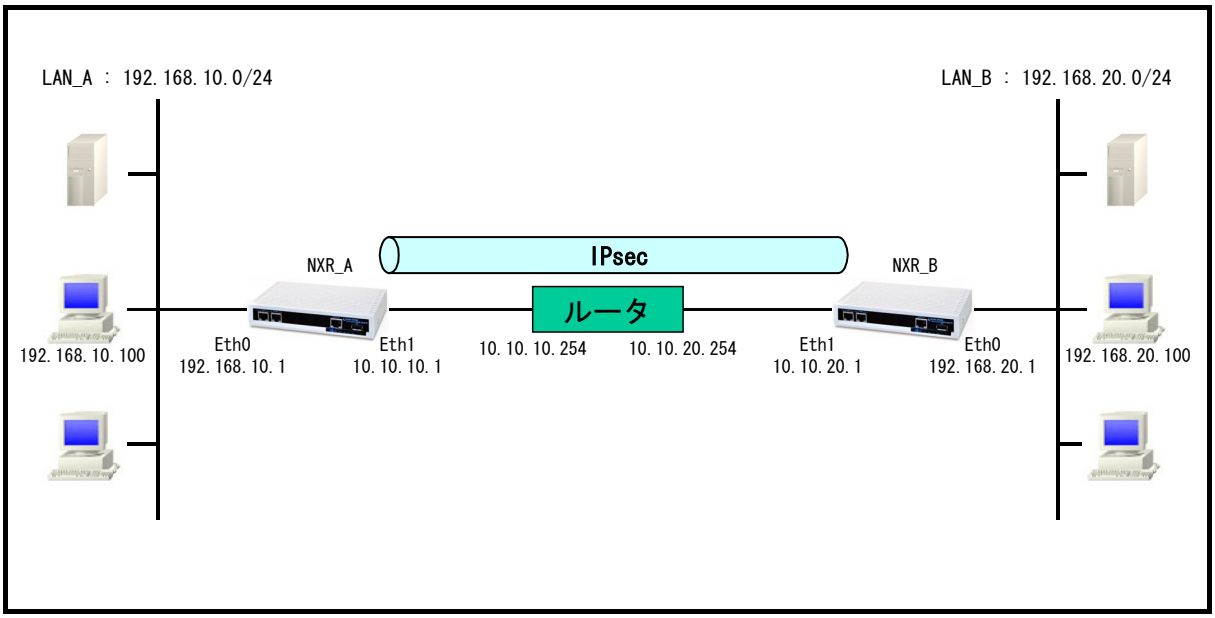
## 【 パソコンの設定例 】

| | 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
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 0.0.0.0/0 10.10.10.254
NXR_A(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
NXR_A(config)#ipsec generate rsa-sig-key 1024
RSA-SIG KEY generating...
NXR_A(config)#exit
NXR_A#show ipsec rsa-pub-key
RSA public key :
0sAQNe9Ghb4CNEaJuIIy67aSxECLJDHhvndH1opuMs6P8yGiTNlcGeSOQ8XEy8iYTst2bv022XUxSt37
RhOR5lRiY1i83TXkQZbhnJDCNJv+rtX/aro745MbJ9auXT1L5tda4C54S7SELboAtU28sD3si0OwlzLW
tE7yRUqLP4ZiiNMw==
NXR_A#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#self-identity fqdn nxra
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication rsa-sig 0sAQOx8kE6uhZTvWMikunsy3uK5/7j
IkTXsCjQpgo4B+X64UAVeuxFQZ3KG3bzyjmyCbpkt0xEiU+v1kF4AOAOXoDfgND+KAdEky/YWqQYzMuu
uu2uy/K6E9JA24NACufuqMqgGSXc51fJ/6V5Qi9YtVd7TWBkZQSZJJADBHs/YyYD9Q==
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode main
NXR_A(config-ipsec-isakmp)#remote address ip 10.10.20.1
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrb
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address LAN_B
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#ip address 10.10.10.1/24
NXR_A(config-if)#ipsec policy 1
NXR_A(config-if)#exit
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 0.0.0.0/0 10.10.20.254
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
NXR_B(config)#ipsec generate rsa-sig-key 1024
RSA-SIG KEY generating...
NXR_B(config)#exit
NXR_B#show ipsec rsa-pub-key
RSA public key :
0sAQOx8kE6uhZTvWMikunsy3uK5/7jIkTXsCjQpgo4B+X64UAVeuxFQZ3KG3bzyjmyCbpkt0xEiU+v1k
F4AOAOXoDfgND+KAdEky/YWqQYzMuuuu2uy/K6E9JA24NACufuqMqgGSXc51fJ/6V5Qi9YtVd7TWBkZQ
SZJJADBHs/YyYD9Q==
NXR_B#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication rsa-sig 0sAQNe9Ghb4CNEaJuIIy67aSxECLJD
HhvndH1opuMs6P8yGiTNlcGeSOQ8XEy8iYTst2bv022XUxSt37RhOR5lRiY1i83TXkQZbhnJDCNJv+rt
X/aro745MbJ9auXT1L5tda4C54S7SELboAtU28sD3si0OwlzLWtE7yRUqLP4ZiiNMw==
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#remote identity fqdn nxra
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address 10.10.20.1/24
NXR_B(config-if)#ipsec policy 1
NXR_B(config-if)#exit
NXR_B(config)#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 :
0sAQNe9Ghb4CNEaJuIIy67aSxECLJDHhvndH1opuMs6P8yGiTNlcGeSOQ8XEy8iYTst2bv022XUxSt37
RhOR5lRiY1i83TXkQZbhnJDCNJv+rtX/aro745MbJ9auXT1L5tda4C54S7SELboAtU28sD3si0OwlzLW
tE7yRUqLP4ZiiNMw==
```

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 0sAQOx8kE6uhZTvWMikunsy3uK5/7j
IkTXsCjQpgo4B+X64UAVeuxFQZ3KG3bzyjmyCbpkt0xEiU+v1kF4AOAOXoDfgND+KAdEky/YWqQYzMuu
uu2uy/K6E9JA24NACufuqMqgGSXc51fJ/6V5Qi9YtVd7TWBkZQSZJJADBHs/YyYD9Q==
```

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

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

認証アルゴリズムを設定します。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 30 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 30 秒間隔で 3 回リトライを行い、keepalive 失敗時に SA を削除し、IKE のネゴシエーションを開始するように設定します。

```
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 :
0sAQOx8kE6uhZTvWMikunsy3uK5/7jIkTXsCjQpgo4B+X64UAVeuxFQZ3KG3bzyjmyCbpkt0xEiU+v1k
F4AOAOXoDfgND+KAdEky/YWqQYzMuuuu2uy/K6E9JA24NACufuqMqgGSXc51fJ/6V5Qi9YtVd7TWBkZQ
SZJJADBHs/YyYD9Q==
```

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

### 7. ＜IPsec ローカルポリシー設定＞

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

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 0sAQNe9Ghb4CNEaJuIIy67aSxECLJD
HhvndH1opuMs6P8yGiTNlcGeSOQ8XEy8iYTst2bv022XUxSt37RhOR5lRiY1i83TXkQZbhnJDCNJv+rt
X/aro745MbJ9auXT1L5tda4C54S7SELboAtU28sD3si0OwlzLWtE7yRUqLP4ZiiNMw==
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#remote identity fqdn nxra
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
```

NXR_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。

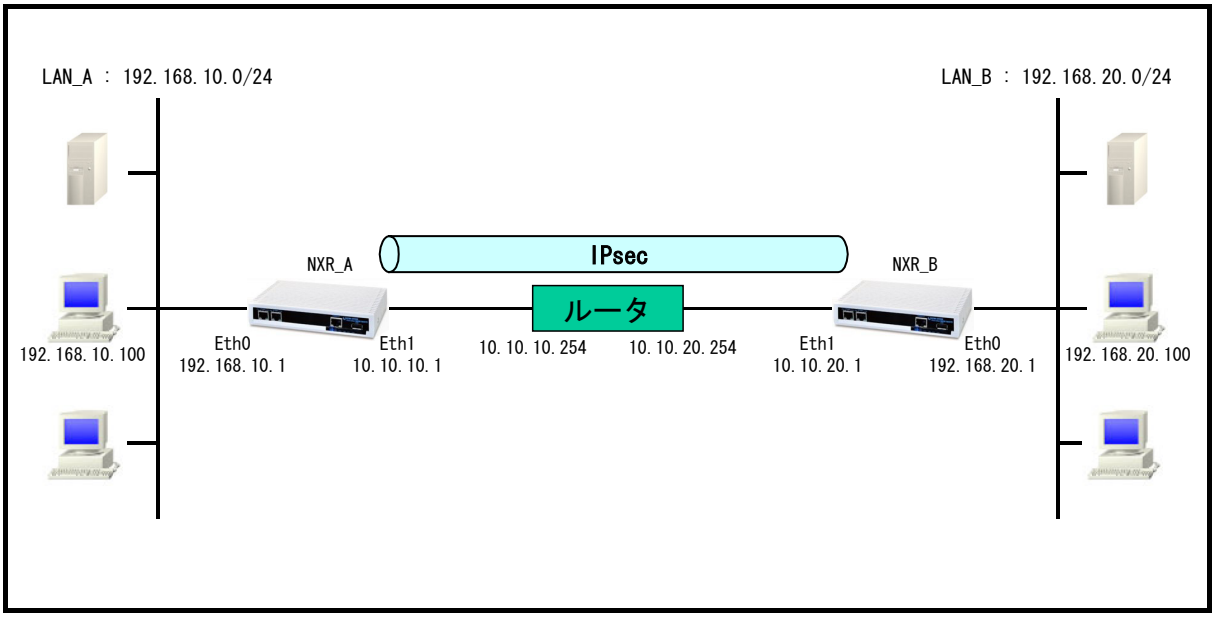
## 【 パソコンの設定例 】

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

〔NXR_B の設定〕

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

NXR_A 用秘密鍵のパスフレーズである nxrapass を設定します。

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

### 11. ＜IPsec ローカルポリシー設定＞

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

IPsec ローカルポリシー1を設定します。

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

IPsec トンネルの送信元 IP アドレスを指定します。

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 30 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 30 秒間隔で 3 回リトライを行い、keepalive 失敗時に SA を削除し、IKE の ネゴシエーションを開始するように設定します。

```
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 nxrbpass
```

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

### 6. ＜IPsec ローカルポリシー設定＞

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

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 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 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。

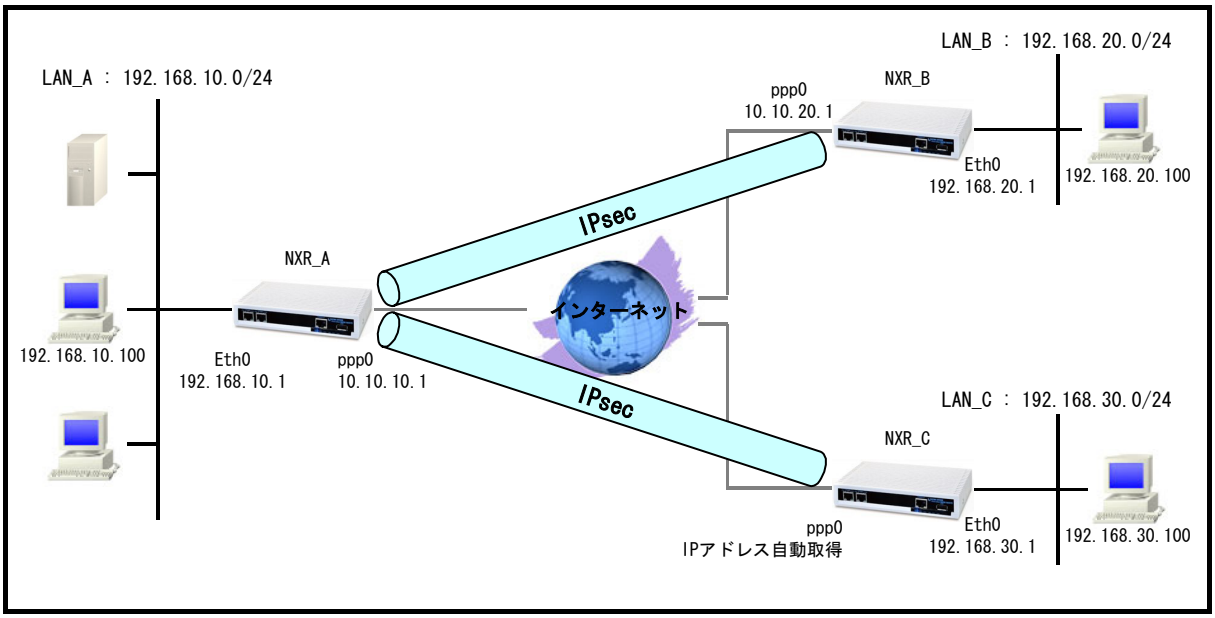
## 【 パソコンの設定例 】

| | 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 NAT 設定（IP マスカレード）やフィルタ設定（SPI）および DNS 設定を行います。

## 【 設定例 】

〔NXR_A の設定〕

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

```
NXR_A(config-ppp)#ip access-group in ppp0_in
NXR_A(config-ppp)#ip spi-filter
NXR_A(config-ppp)#ip tcp adjust-mss auto
NXR_A(config-ppp)#no ip redirects
NXR_A(config-ppp)#ppp 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(config-dns)#service enable
NXR_A(config-dns)#exit
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

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

```
NXR_B(config-ppp)#ppp 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(config-dns)#service enable
NXR_B(config-dns)#exit
NXR_B(config)#exit
NXR_B#save config
```

〔NXR_C の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_C
NXR_C(config)#interface ethernet 0
NXR_C(config-if)#ip address 192.168.30.1/24
NXR_C(config-if)#exit
NXR_C(config)#ip route 0.0.0.0/0 ppp 0
NXR_C(config)#ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
NXR_C(config)#ip access-list ppp0_in permit 10.10.10.1 any 50
NXR_C(config)#ipsec access-list LAN_A ip 192.168.30.0/24 192.168.10.0/24
NXR_C(config)#ipsec local policy 1
NXR_C(config-ipsec-local)#address ip
NXR_C(config-ipsec-local)#self-identity fqdn nxrc
NXR_C(config-ipsec-local)#exit
NXR_C(config)#ipsec isakmp policy 1
NXR_C(config-ipsec-isakmp)#description NXR_A
NXR_C(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR_C(config-ipsec-isakmp)#hash sha1
NXR_C(config-ipsec-isakmp)#encryption aes128
NXR_C(config-ipsec-isakmp)#group 5
NXR_C(config-ipsec-isakmp)#lifetime 10800
NXR_C(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_C(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_C(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_C(config-ipsec-isakmp)#local policy 1
NXR_C(config-ipsec-isakmp)#exit
NXR_C(config)#ipsec tunnel policy 1
NXR_C(config-ipsec-tunnel)#description NXR_A
NXR_C(config-ipsec-tunnel)#negotiation-mode auto
NXR_C(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_C(config-ipsec-tunnel)#set pfs group5
NXR_C(config-ipsec-tunnel)#set sa lifetime 3600
NXR_C(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_C(config-ipsec-tunnel)#match address LAN_A
NXR_C(config-ipsec-tunnel)#exit
NXR_C(config)#interface ppp 0
NXR_C(config-ppp)#ip address negotiated
NXR_C(config-ppp)#ip masquerade
NXR_C(config-ppp)#ip access-group in ppp0_in
NXR_C(config-ppp)#ip spi-filter
NXR_C(config-ppp)#ip tcp adjust-mss auto
NXR_C(config-ppp)#no ip redirects
NXR_C(config-ppp)#ppp 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(config-dns)#service enable
NXR_C(config-dns)#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 30 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 30 秒間隔で 3 回リトライを行い、keepalive 失敗時に SA を削除し、IKE のネゴシエーションを開始するように設定します。

```
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 30 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 30 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 30 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 30 秒間隔で 3 回リトライを行い、keepalive 失敗時に SA を削除し IKE の ネゴシエーションを開始するように設定します。

```
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 30 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 30 秒間隔で 3 回リトライを行い、keepalive 失敗時に SA を削除し、IKE のネゴシエーションを開始するように設定します。

```
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。

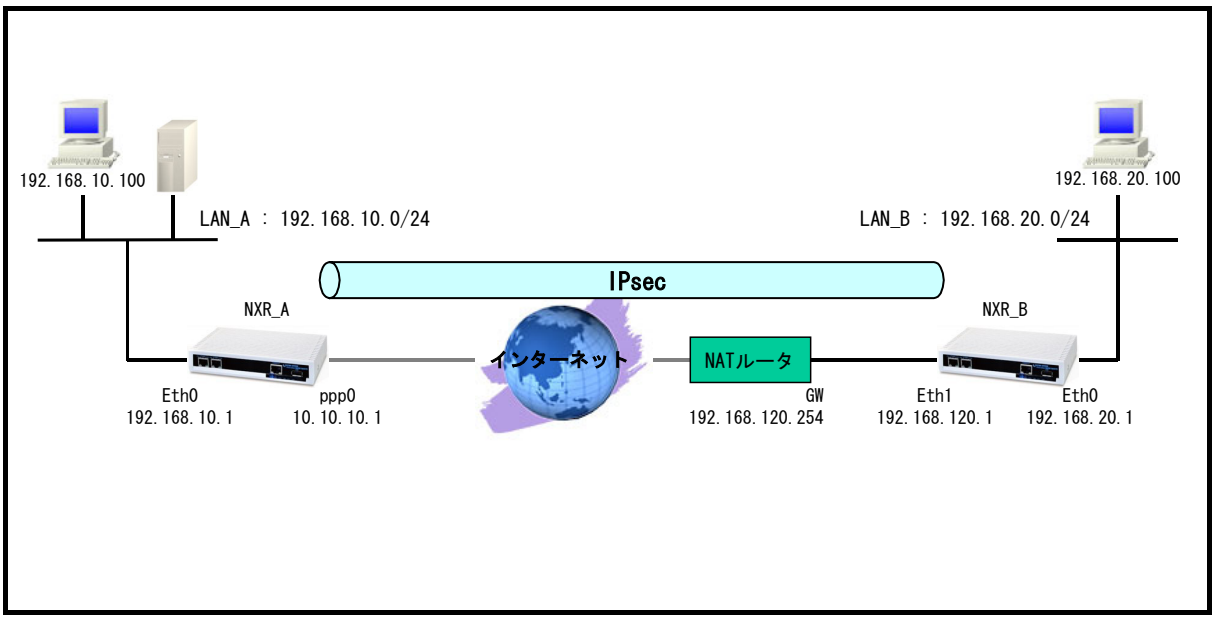
## 【 パソコンの設定例 】

| | 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設定および NXR_B へのルート設定が完了しているとします。

## 【 設定例 】

〔NXR_A の設定〕

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

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 0.0.0.0/0 192.168.120.254
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
NXR_B(config)#ipsec nat-traversal enable
% restart ipsec service to take affect.
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address 192.168.120.1/24
NXR_B(config-if)#ipsec policy 1
NXR_B(config-if)#exit
NXR_B(config)#dns
NXR_B(config-dns)#service enable
NXR_B(config-dns)#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 30 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 30 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 30 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 30 秒間隔で 3 回リトライを行い、keepalive 失敗時に SA を削除し IKE の ネゴシエーションを開始するように設定します。

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 】

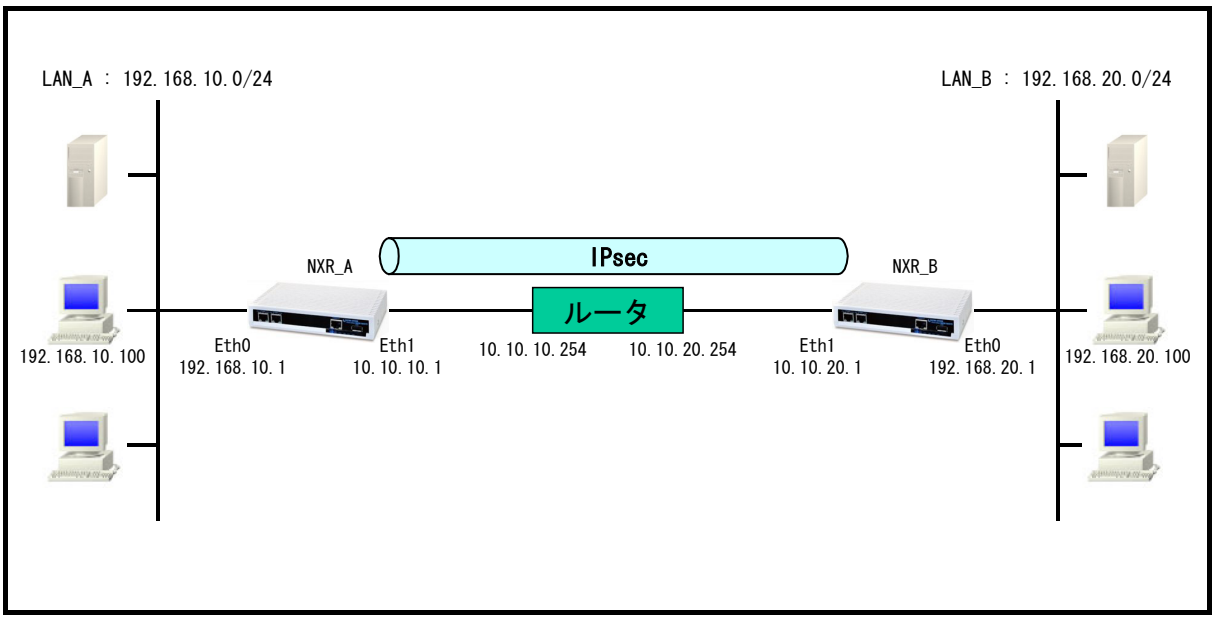
| | LAN A のパソコン | LAN B のパソコン |
|---|---|---|
| IP アドレス | 192.168.10.100 | 192.168.20.100 |
| サブネットマスク | 255.255.255.0 | 255.255.255.0 |
| デフォルトゲートウェイ | 192.168.10.1 | 192.168.20.1 |

# 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
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1
NXR_A(config)#ip route 0.0.0.0/0 10.10.10.254
NXR_A(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode main
NXR_A(config-ipsec-isakmp)#remote address ip 10.10.20.1
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address LAN_B
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
NXR_A(config-tunnel)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#ip address 10.10.10.1/24
NXR_A(config-if)#ipsec policy 1
NXR_A(config-if)#exit
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1
NXR_B(config)#ip route 0.0.0.0/0 10.10.20.254
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
NXR_B(config-tunnel)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address 10.10.20.1/24
NXR_B(config-if)#ipsec policy 1
NXR_B(config-if)#exit
NXR_B(config)#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_A(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

〔NXR_B の設定〕

(☞) ここに記載のない設定項目は、1-1. 固定 IP アドレスでの接続設定例(MainMode の利用)の〔NXR_B の設定〕が参考になりますので、そちらをご参照下さい。

**1. ＜スタティックルート設定＞**

```
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1
```

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_B(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。
TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

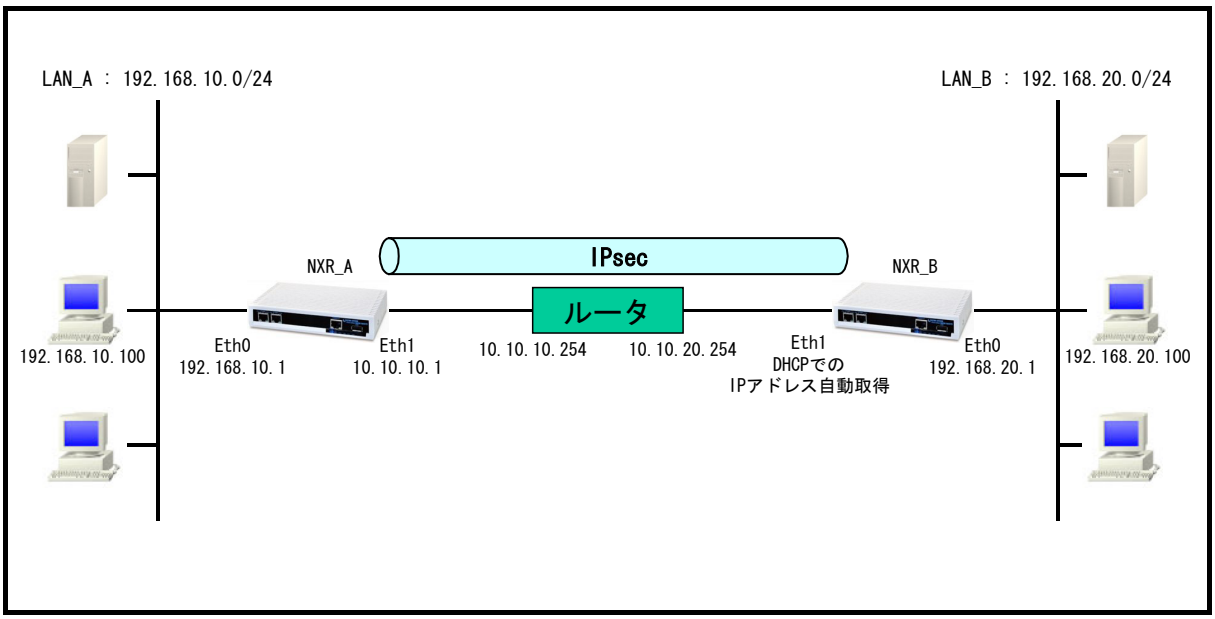
## 【 パソコンの設定例 】

| | 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)の内容も一部参考になりますので、ご参照下さい。

## 【 設定例 】

〔NXR_A の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1
NXR_A(config)#ip route 0.0.0.0/0 10.10.10.254
NXR_A(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A(config-ipsec-isakmp)#remote address ip any
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrb
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address LAN_B
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
NXR_A(config-tunnel)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#ip address 10.10.10.1/24
NXR_A(config-if)#ipsec policy 1
NXR_A(config-if)#exit
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
NXR_B(config-tunnel)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address dhcp
NXR_B(config-if)#ipsec policy 1
NXR_B(config-if)#exit
NXR_B(config)#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_A(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

〔NXR_B の設定〕

(☞) ここに記載のない設定項目は、1-2. 動的 IP アドレスでの接続設定例（AggressiveMode の利用）の〔NXR_B の設定〕が参考になりますので、そちらをご参照下さい。

**1. ＜スタティックルート設定＞**

```
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1
```

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_B(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

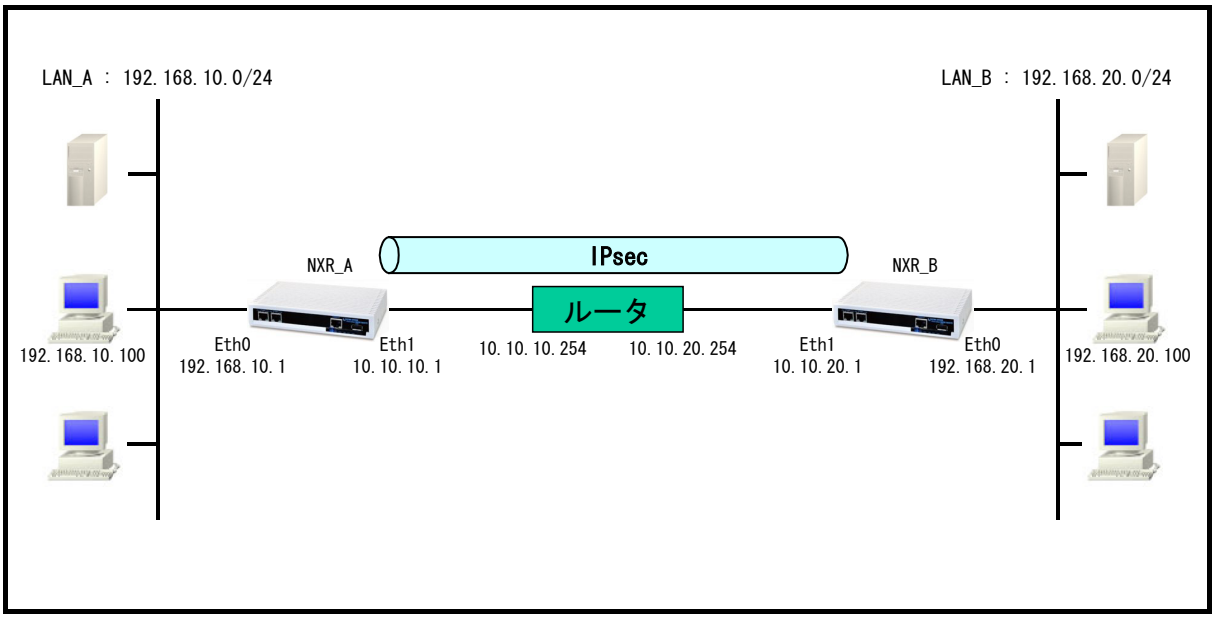
## 【 パソコンの設定例 】

| | 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
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1
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 :
0sAQNe9Ghb4CNEaJuIIy67aSxECLJDHhvndH1opuMs6P8yGiTNlcGeSOQ8XEy8iYTst2bv022XUxSt37
RhOR5lRiY1i83TXkQZbhnJDCNJv+rtX/aro745MbJ9auXT1L5tda4C54S7SELboAtU28sD3si0OwlzLW
tE7yRUqLP4ZiiNMw==
NXR_A#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#self-identity fqdn nxra
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication rsa-sig 0sAQOx8kE6uhZTvWMikunsy3uK5/7j
IkTXsCjQpgo4B+X64UAVeuxFQZ3KG3bzyjmyCbpkt0xEiU+v1kF4AOAOXoDfgND+KAdEky/YWqQYzMuu
uu2uy/K6E9JA24NACufuqMqgGSXc51fJ/6V5Qi9YtVd7TWBkZQSZJJADBHs/YyYD9Q==
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode main
NXR_A(config-ipsec-isakmp)#remote address ip 10.10.20.1
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrb
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address LAN_B
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
NXR_A(config-tunnel)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#ip address 10.10.10.1/24
NXR_A(config-if)#ipsec policy 1
NXR_A(config-if)#exit
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1
NXR_B(config)#ip route 0.0.0.0/0 10.10.20.254
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
NXR_B(config)#ipsec generate rsa-sig-key 1024
RSA-SIG KEY generating...
NXR_B(config)#exit
NXR_B#show ipsec rsa-pub-key
RSA public key :
0sAQOx8kE6uhZTvWMikunsy3uK5/7jIkTXsCjQpgo4B+X64UAVeuxFQZ3KG3bzyjmyCbpkt0xEiU+v1k
F4AOAOXoDfgND+KAdEky/YWqQYzMuuuu2uy/K6E9JA24NACufuqMqgGSXc51fJ/6V5Qi9YtVd7TWBkZQ
SZJJADBHs/YyYD9Q==
NXR_B#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication rsa-sig 0sAQNe9Ghb4CNEaJuIIy67aSxECLJD
HhvndH1opuMs6P8yGiTNlcGeSOQ8XEy8iYTst2bv022XUxSt37RhOR5lRiY1i83TXkQZbhnJDCNJv+rt
X/aro745MbJ9auXT1L5tda4C54S7SELboAtU28sD3si0OwlzLWtE7yRUqLP4ZiiNMw==
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#remote identity fqdn nxra
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
NXR_B(config-tunnel)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address 10.10.20.1/24
NXR_B(config-if)#ipsec policy 1
NXR_B(config-if)#exit
NXR_B(config)#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_A(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

〔NXR_B の設定〕

(☞) ここに記載のない設定項目は、1-3. RSA 公開鍵暗号方式での接続設定例の〔NXR_B の設定〕が参考になりますので、そちらをご参照下さい。

**1. ＜スタティックルート設定＞**

```
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1
```

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_B(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

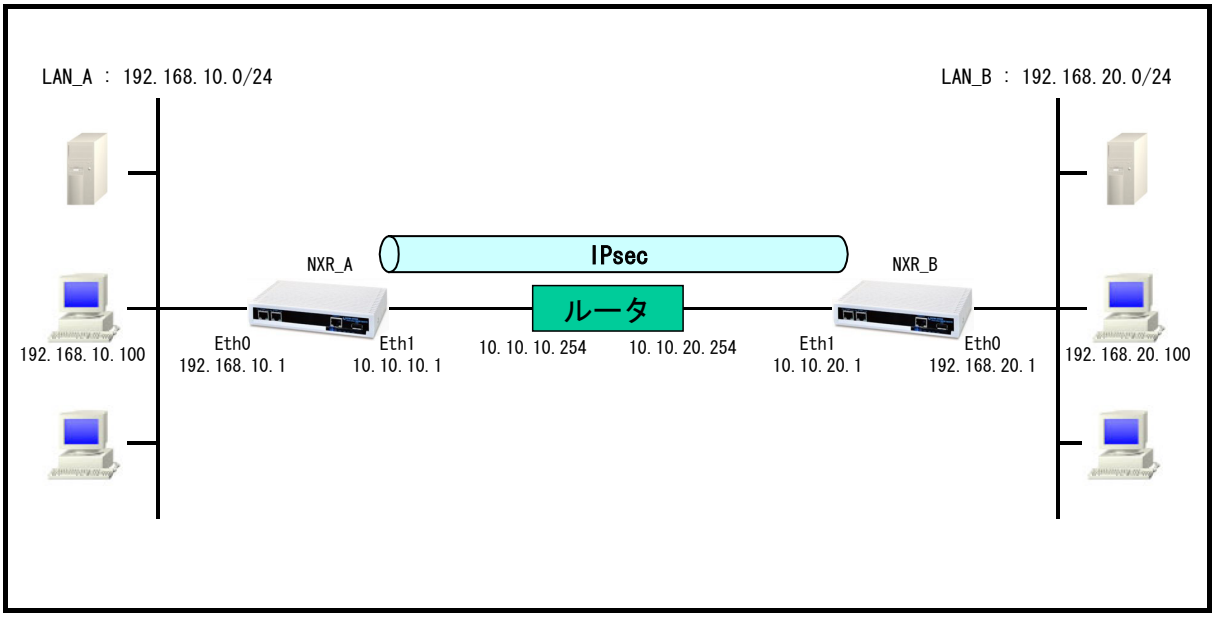
## 【 パソコンの設定例 】

| | 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
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1
NXR_A(config)#ip route 0.0.0.0/0 10.10.10.254
NXR_A(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
NXR_A(config)#ipsec x509 enable
NXR_A(config)#ipsec x509 ca-certificate nxr ftp://192.168.10.10/nxrCA.pem
NXR_A(config)#ipsec x509 crl nxr ftp://192.168.10.10/nxrCRL.pem
NXR_A(config)#ipsec x509 certificate nxra ftp://192.168.10.10/nxraCert.pem
NXR_A(config)#ipsec x509 private-key nxra key ftp://192.168.10.10/nxraKey.pem
NXR_A(config)#ipsec x509 private-key nxra password nxrapass
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#x509 certificate nxra
NXR_A(config-ipsec-local)#self-identity dn /C=JP/CN=nxra/E=nxra@example.com
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication rsa-sig
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode main
NXR_A(config-ipsec-isakmp)#remote address ip 10.10.20.1
NXR_A(config-ipsec-isakmp)#remote identity dn /C=JP/CN=nxrb/E=nxrb@example.com
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address LAN_B
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
NXR_A(config-tunnel)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#ip address 10.10.10.1/24
NXR_A(config-if)#ipsec policy 1
NXR_A(config-if)#exit
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1
NXR_B(config)#ip route 0.0.0.0/0 10.10.20.254
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
NXR_B(config)#ipsec x509 enable
NXR_B(config)#ipsec x509 ca-certificate nxr ftp://192.168.20.10/nxrCA.pem
NXR_B(config)#ipsec x509 crl nxr ftp://192.168.20.10/nxrCRL.pem
NXR_B(config)#ipsec x509 certificate nxrb ftp://192.168.20.10/nxrbCert.pem
NXR_B(config)#ipsec x509 private-key nxrb key ftp://192.168.20.10/nxrbKey.pem
NXR_B(config)#ipsec x509 private-key nxrb password nxrbpass
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#x509 certificate nxrb
NXR_B(config-ipsec-local)#self-identity dn /C=JP/CN=nxrb/E=nxrb@example.com
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication rsa-sig
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#remote identity dn /C=JP/CN=nxra/E=nxra@example.com
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
NXR_B(config-tunnel)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address 10.10.20.1/24
NXR_B(config-if)#ipsec policy 1
NXR_B(config-if)#exit
NXR_B(config)#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_A(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

〔NXR_B の設定〕

(☞) ここに記載のない設定項目は、1-4. X.509(デジタル署名認証)方式での接続設定例の〔NXR_B の設定〕が参考になりますので、そちらをご参照下さい。

**1. ＜スタティックルート設定＞**

```
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1
```

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_B(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

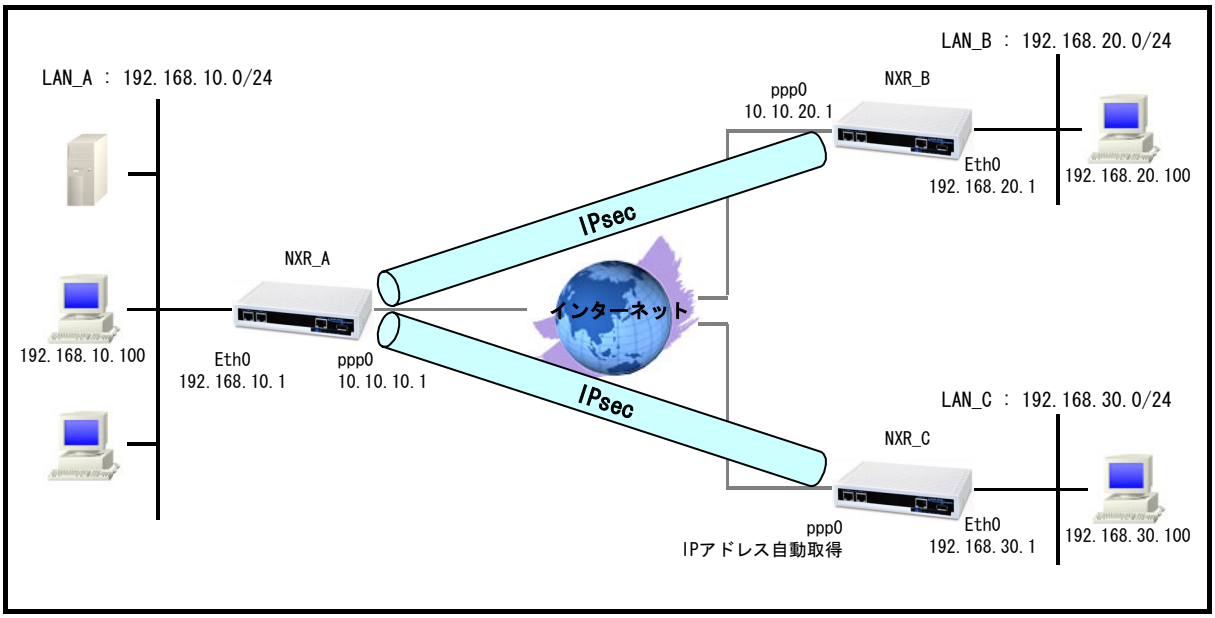
## 【 パソコンの設定例 】

| | 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） ー NXR_B（拠点）間はメインモードを NXR_A（センタ） ー 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
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1
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 30 3 periodic restart
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address LAN_B
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
NXR_A(config-tunnel)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#ipsec isakmp policy 2
NXR_A(config-ipsec-isakmp)#description NXR_C
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A(config-ipsec-isakmp)#remote address ip any
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrc
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 2
NXR_A(config-ipsec-tunnel)#description NXR_C
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
```

```
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 2
NXR_A(config-ipsec-tunnel)#match address 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)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#interface ppp 0
NXR_A(config-ppp)#ip address 10.10.10.1/32
NXR_A(config-ppp)#ip masquerade
NXR_A(config-ppp)#ip access-group in ppp0_in
NXR_A(config-ppp)#ip spi-filter
NXR_A(config-ppp)#ip tcp adjust-mss auto
NXR_A(config-ppp)#no ip redirects
NXR_A(config-ppp)#ppp 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(config-dns)#service enable
NXR_A(config-dns)#exit
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1
NXR_B(config)#ip route 0.0.0.0/0 ppp 0
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 udp 500 500
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 50
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
```

```
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
NXR_B(config-tunnel)#exit
NXR_B(config)#interface ppp 0
NXR_B(config-ppp)#ip address 10.10.20.1/32
NXR_B(config-ppp)#ip masquerade
NXR_B(config-ppp)#ip access-group in ppp0_in
NXR_B(config-ppp)#ip spi-filter
NXR_B(config-ppp)#ip tcp adjust-mss auto
NXR_B(config-ppp)#no ip redirects
NXR_B(config-ppp)#ppp 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(config-dns)#service enable
NXR_B(config-dns)#exit
NXR_B(config)#exit
NXR_B#save config
```

〔NXR_C の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_C
NXR_C(config)#interface ethernet 0
NXR_C(config-if)#ip address 192.168.30.1/24
NXR_C(config-if)#exit
NXR_C(config)#ip route 192.168.10.0/24 tunnel 1
NXR_C(config)#ip route 0.0.0.0/0 ppp 0
NXR_C(config)#ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
NXR_C(config)#ip access-list ppp0_in permit 10.10.10.1 any 50
NXR_C(config)#ipsec access-list LAN_A ip 192.168.30.0/24 192.168.10.0/24
NXR_C(config)#ipsec local policy 1
NXR_C(config-ipsec-local)#address ip
NXR_C(config-ipsec-local)#self-identity fqdn nxrc
NXR_C(config-ipsec-local)#exit
NXR_C(config)#ipsec isakmp policy 1
NXR_C(config-ipsec-isakmp)#description NXR_A
NXR_C(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR_C(config-ipsec-isakmp)#hash sha1
NXR_C(config-ipsec-isakmp)#encryption aes128
NXR_C(config-ipsec-isakmp)#group 5
NXR_C(config-ipsec-isakmp)#lifetime 10800
NXR_C(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_C(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_C(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_C(config-ipsec-isakmp)#local policy 1
NXR_C(config-ipsec-isakmp)#exit
```

```
NXR_C(config)#ipsec tunnel policy 1
NXR_C(config-ipsec-tunnel)#description NXR_A
NXR_C(config-ipsec-tunnel)#negotiation-mode auto
NXR_C(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_C(config-ipsec-tunnel)#set pfs group5
NXR_C(config-ipsec-tunnel)#set sa lifetime 3600
NXR_C(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_C(config-ipsec-tunnel)#match address LAN_A
NXR_C(config-ipsec-tunnel)#exit
NXR_C(config)#interface tunnel 1
NXR_C(config-tunnel)#tunnel mode ipsec ipv4
NXR_C(config-tunnel)#tunnel protection ipsec policy 1
NXR_C(config-tunnel)#ip tcp adjust-mss auto
NXR_C(config-tunnel)#exit
NXR_C(config)#interface ppp 0
NXR_C(config-ppp)#ip address negotiated
NXR_C(config-ppp)#ip masquerade
NXR_C(config-ppp)#ip access-group in ppp0_in
NXR_C(config-ppp)#ip spi-filter
NXR_C(config-ppp)#ip tcp adjust-mss auto
NXR_C(config-ppp)#no ip redirects
NXR_C(config-ppp)#ppp 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(config-dns)#service enable
NXR_C(config-dns)#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。

```
NXR_A(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

**4. ＜トンネル 2 インタフェース設定＞**

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

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_A(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

〔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_B(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

## 〔NXR_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。

```
NXR_C(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

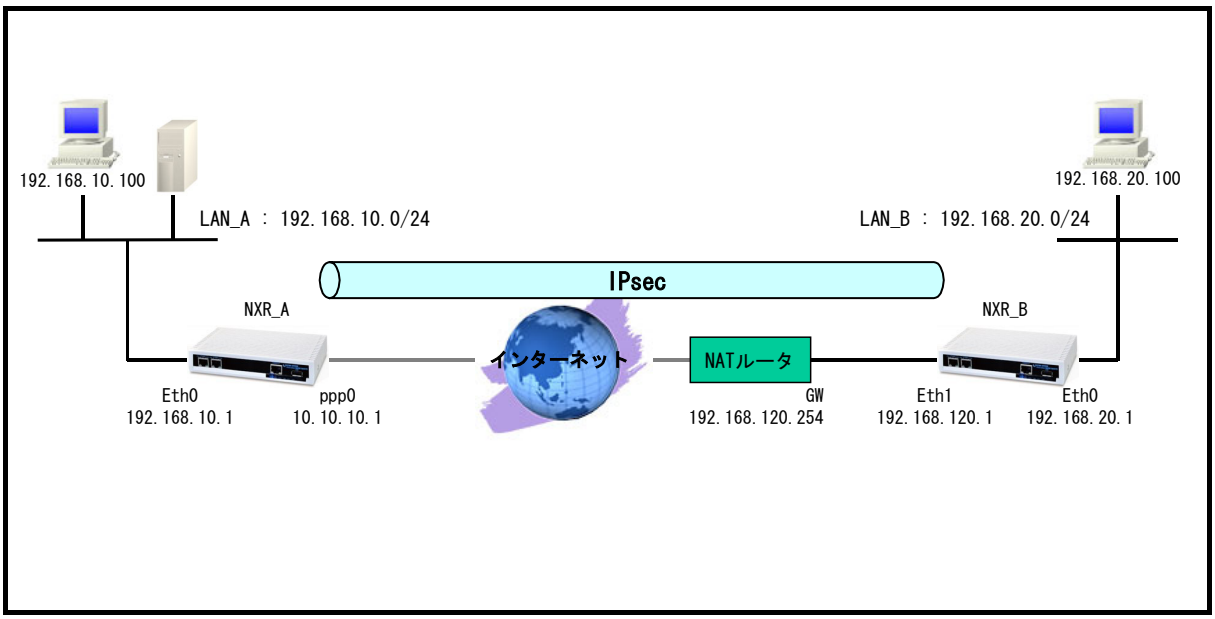
## 【 パソコンの設定例 】

| | 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
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1
NXR_A(config)#ip route 0.0.0.0/0 ppp 0
NXR_A(config)#ip access-list ppp0_in permit any 10.10.10.1 udp any 500
NXR_A(config)#ip access-list ppp0_in permit any 10.10.10.1 udp any 4500
NXR_A(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
NXR_A(config)#ipsec nat-traversal enable
% restart ipsec service to take affect.
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A(config-ipsec-isakmp)#remote address ip any
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrb
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address LAN_B
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 1
NXR_A(config-tunnel)#no ip address
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
NXR_A(config-tunnel)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#interface ppp 0
NXR_A(config-ppp)#ip address 10.10.10.1/32
NXR_A(config-ppp)#ip masquerade
NXR_A(config-ppp)#ip access-group in ppp0_in
NXR_A(config-ppp)#ip spi-filter
NXR_A(config-ppp)#ip tcp adjust-mss auto
NXR_A(config-ppp)#no ip redirects
NXR_A(config-ppp)#ppp 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(config-dns)#service enable
NXR_A(config-dns)#exit
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1
NXR_B(config)#ip route 0.0.0.0/0 192.168.120.254
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
NXR_B(config)#ipsec nat-traversal enable
% restart ipsec service to take affect.
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#no ip address
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
NXR_B(config-tunnel)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address 192.168.120.1/24
NXR_B(config-if)#ipsec policy 1
NXR_B(config-if)#exit
NXR_B(config)#dns
NXR_B(config-dns)#service enable
NXR_B(config-dns)#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_A(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

〔NXR_B の設定〕

(☞) ここに記載のない設定項目は、1-6. 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。

```
NXR_B(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

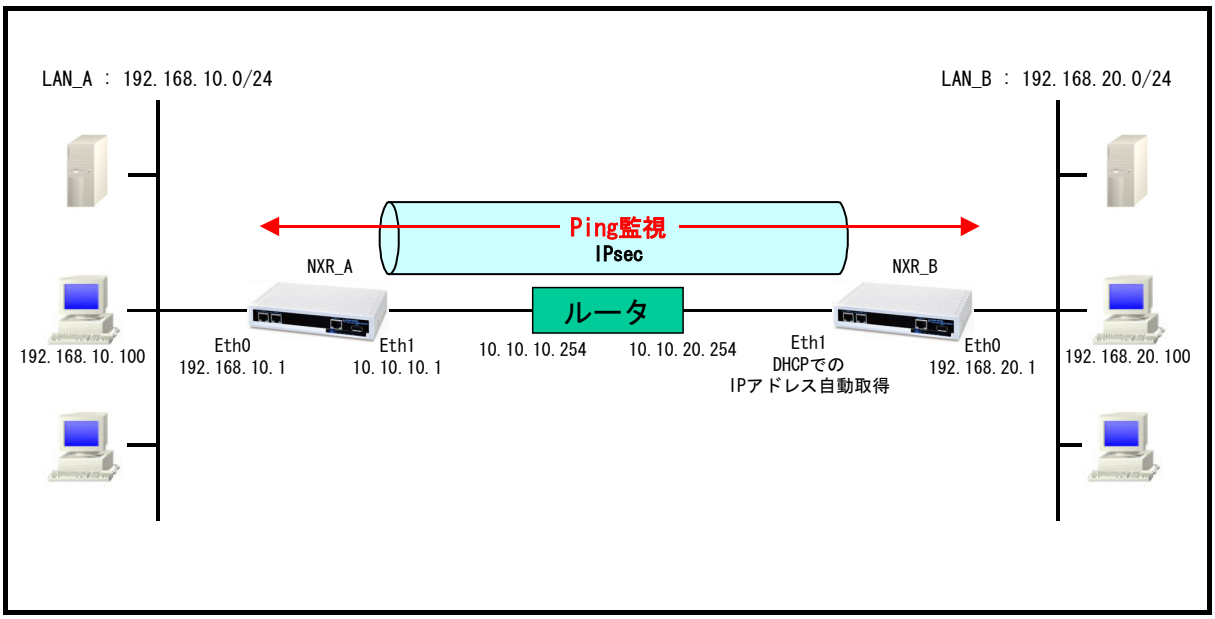
## 【 パソコンの設定例 】

| | 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
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1
NXR_A(config)#ip route 0.0.0.0/0 10.10.10.254
NXR_A(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description NXR_B
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A(config-ipsec-isakmp)#remote address ip any
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrb
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address LAN_B
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
NXR_A(config-tunnel)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#ip address 10.10.10.1/24
NXR_A(config-if)#ipsec policy 1
NXR_A(config-if)#exit
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1
NXR_B(config)# track 1 ip reachability 192.168.10.1 interface tunnel 1 10 3
NXR_B(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#self-identity fqdn nxrb
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description NXR_A
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#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)#ip tcp adjust-mss auto
NXR_B(config-tunnel)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#ip address dhcp
NXR_B(config-if)#ipsec policy 1
NXR_B(config-if)#exit
NXR_B(config)#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
```

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。

**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。

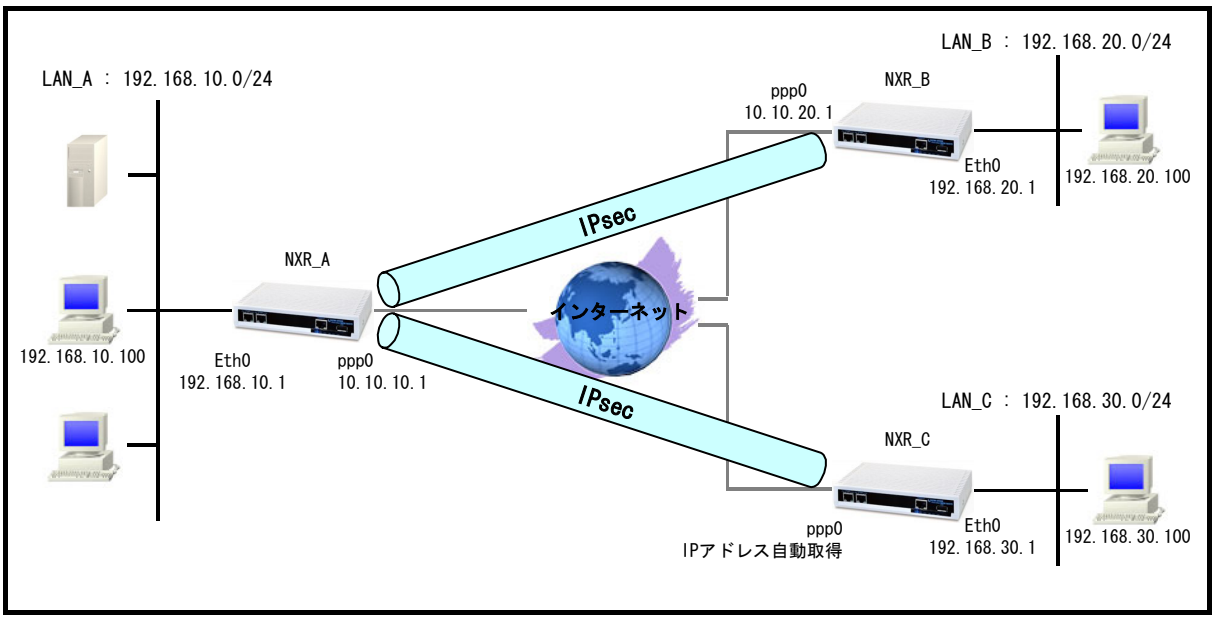
## 【 パソコンの設定例 】

| | 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 】




- 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
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#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 30 3 periodic restart
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description NXR_B
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address LAN_B
NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 1
NXR_A(config-tunnel)#ip address 192.168.10.1/32
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
NXR_A(config-tunnel)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#ipsec isakmp policy 2
NXR_A(config-ipsec-isakmp)#description NXR_C
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 5
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_A(config-ipsec-isakmp)#remote address ip any
NXR_A(config-ipsec-isakmp)#remote identity fqdn nxrc
NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 2
```

```
NXR_A(config-ipsec-tunnel)#description NXR_C
NXR_A(config-ipsec-tunnel)#negotiation-mode responder
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group5
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 2
NXR_A(config-ipsec-tunnel)#match address 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)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#interface ppp 0
NXR_A(config-ppp)#ip address 10.10.10.1/32
NXR_A(config-ppp)#ip masquerade
NXR_A(config-ppp)#ip access-group in ppp0_in
NXR_A(config-ppp)#ip spi-filter
NXR_A(config-ppp)#ip tcp adjust-mss auto
NXR_A(config-ppp)#no ip redirects
NXR_A(config-ppp)#ppp 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(config-dns)#service enable
NXR_A(config-dns)#exit
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#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
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 5
```

```
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode main
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#ip address 192.168.20.1/32
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#ip tcp adjust-mss auto
NXR_B(config-tunnel)#exit
NXR_B(config)#interface ppp 0
NXR_B(config-ppp)#ip address 10.10.20.1/32
NXR_B(config-ppp)#ip masquerade
NXR_B(config-ppp)#ip access-group in ppp0_in
NXR_B(config-ppp)#ip spi-filter
NXR_B(config-ppp)#ip tcp adjust-mss auto
NXR_B(config-ppp)#no ip redirects
NXR_B(config-ppp)#ppp 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(config-dns)#service enable
NXR_B(config-dns)#exit
NXR_B(config)#exit
NXR_B#save config
```

〔NXR_C の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR_C
NXR_C(config)#interface ethernet 0
NXR_C(config-if)#ip address 192.168.30.1/24
NXR_C(config-if)#exit
NXR_C(config)#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-router)#ip route 0.0.0.0/0 ppp 0
NXR_C(config)#ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
NXR_C(config)#ip access-list ppp0_in permit 10.10.10.1 any 50
NXR_C(config)#ipsec access-list LAN_A ip 192.168.30.0/24 192.168.10.0/24
NXR_C(config)#ipsec local policy 1
NXR_C(config-ipsec-local)#address ip
NXR_C(config-ipsec-local)#self-identity fqdn nxrc
```

```
NXR_C(config-ipsec-local)#exit
NXR_C(config)#ipsec isakmp policy 1
NXR_C(config-ipsec-isakmp)#description NXR_A
NXR_C(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR_C(config-ipsec-isakmp)#hash sha1
NXR_C(config-ipsec-isakmp)#encryption aes128
NXR_C(config-ipsec-isakmp)#group 5
NXR_C(config-ipsec-isakmp)#lifetime 10800
NXR_C(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_C(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_C(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR_C(config-ipsec-isakmp)#local policy 1
NXR_C(config-ipsec-isakmp)#exit
NXR_C(config)#ipsec tunnel policy 1
NXR_C(config-ipsec-tunnel)#description NXR_A
NXR_C(config-ipsec-tunnel)#negotiation-mode auto
NXR_C(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_C(config-ipsec-tunnel)#set pfs group5
NXR_C(config-ipsec-tunnel)#set sa lifetime 3600
NXR_C(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_C(config-ipsec-tunnel)#match address LAN_A
NXR_C(config-ipsec-tunnel)#exit
NXR_C(config)#interface tunnel 1
NXR_C(config-tunnel)#ip address 192.168.30.1/32
NXR_C(config-tunnel)#tunnel mode ipsec ipv4
NXR_C(config-tunnel)#tunnel protection ipsec policy 1
NXR_C(config-tunnel)#ip tcp adjust-mss auto
NXR_C(config-tunnel)#exit
NXR_C(config)#interface ppp 0
NXR_C(config-ppp)#ip address negotiated
NXR_C(config-ppp)#ip masquerade
NXR_C(config-ppp)#ip access-group in ppp0_in
NXR_C(config-ppp)#ip spi-filter
NXR_C(config-ppp)#ip tcp adjust-mss auto
NXR_C(config-ppp)#no ip redirects
NXR_C(config-ppp)#ppp 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(config-dns)#service enable
NXR_C(config-dns)#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。

```
NXR_A(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

**4. ＜トンネル2インタフェース設定＞**

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

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_A(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

〔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_B(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

## 〔NXR_C の設定〕

(☞) ここに記載のない設定項目は、2-5. PPPoE を利用した IPsec 接続設定例の〔NXR_C の設定〕が参考になりますので、そちらをご参照下さい。

### 1. ＜OSPF 設定＞

```
NXR_C(config)#router ospf
```

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。

```
NXR_C(config-tunnel)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

## 【 パソコンの設定例 】

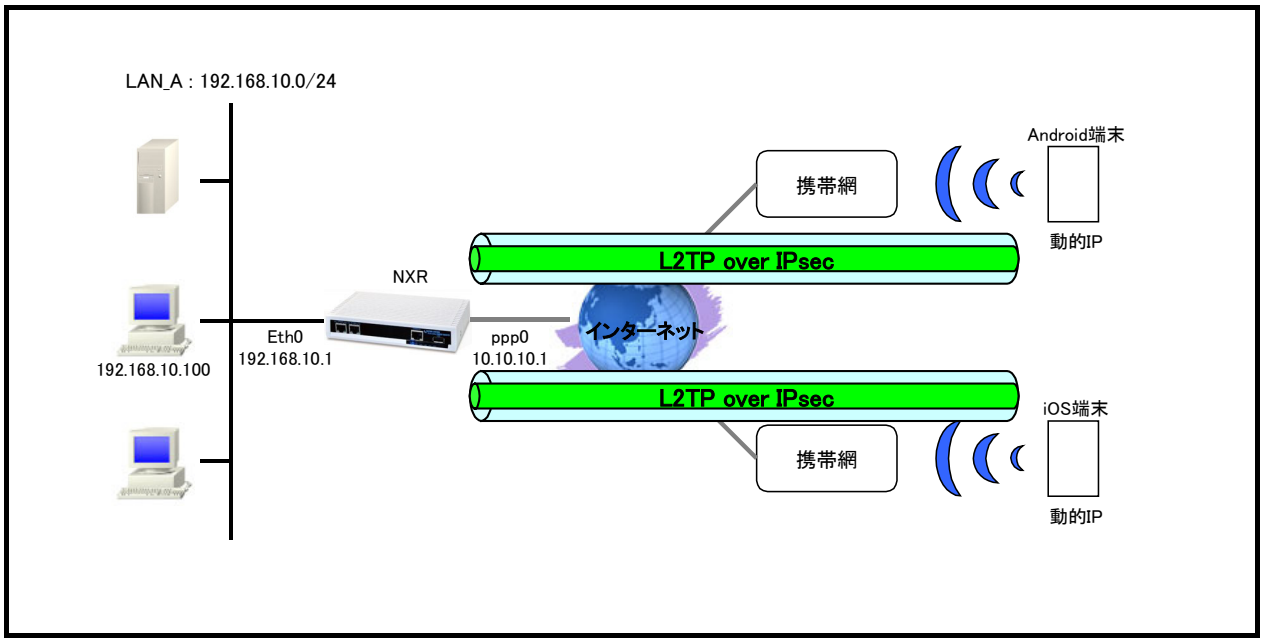
| | LAN A のパソコン | LAN B のパソコン | LAN C のパソコン |
|---|---|---|---|
| IP アドレス | 192.168.10.100 | 192.168.20.100 | 192.168.30.100 |
| サブネットマスク | 255.255.255.0 | 255.255.255.0 | 255.255.255.0 |
| デフォルトゲートウェイ | 192.168.10.1 | 192.168.20.1 | 192.168.30.1 |

# 3. L2TP/IPsec 設定

# 3-1. スマートフォンとの L2TP/IPsec 接続設定例

Android や iOS のスマートフォンに搭載されている L2TP/IPsec の VPN 機能を利用することで、NXR と VPN 接続することが可能です。なおこの設定例では IPsec で事前共有鍵を利用して接続を行います。

## 【 構成図 】




- L2TP/IPsec を設定する場合は大きく分けて以下の設定が必要となります。
  - IPsec 設定
  - L2TP 設定
  - virtual-template インタフェース設定
  - アクセスサーバ(RAS)設定
- IPsec はトランスポートモードを使用し、L2TP パケットを暗号化します。
- L2TPv2 の LNS 機能による着信では virtual-template インタフェースを使用します。
- 接続してきたスマートフォンには IP アドレスプールより IP アドレスを割り当てます。この設定例では2台に IP アドレスを割り当てるため IP アドレスを2つ設定し、かつユーザ ID 毎に指定した IP アドレスを割り当てます。

## 【 設定例 】

〔NXR の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR
NXR(config)#interface ethernet 0
NXR(config-if)#ip address 192.168.10.1/24
NXR(config-if)#exit
NXR(config)#ip route 0.0.0.0/0 ppp 0
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 50
NXR(config)#ipsec local policy 1
NXR(config-ipsec-local)#address ip
NXR(config-ipsec-local)#exit
NXR(config)#ipsec isakmp policy 1
NXR(config-ipsec-isakmp)#description smartphone
NXR(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR(config-ipsec-isakmp)#hash sha1
NXR(config-ipsec-isakmp)#encryption aes128
NXR(config-ipsec-isakmp)#group 5
NXR(config-ipsec-isakmp)#lifetime 86400
NXR(config-ipsec-isakmp)#isakmp-mode main
NXR(config-ipsec-isakmp)#remote address ip any
NXR(config-ipsec-isakmp)#local policy 1
NXR(config-ipsec-isakmp)#exit
NXR(config)#ipsec tunnel policy 1
NXR(config-ipsec-tunnel)#description smartphone
NXR(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR(config-ipsec-tunnel)#no set pfs
NXR(config-ipsec-tunnel)#set sa lifetime 28800
NXR(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR(config-ipsec-tunnel)#match protocol l2tp-smartphone
NXR(config-ipsec-tunnel)#exit
NXR(config)#ppp account username android01 password android01pass
NXR(config)#ppp account username ios01 password ios01pass
NXR(config)#ppp account username test1@centurysys password test1pass
NXR(config)#access-server profile 0
NXR(config-ras)#ppp username android01 ip 172.16.0.10
NXR(config-ras)#exit
NXR(config)#access-server profile 1
NXR(config-ras)#ppp username ios01 ip 172.16.0.11
NXR(config-ras)#exit
NXR(config)#ip local pool smartphoneip address 172.16.0.10 172.16.0.11
NXR(config)#interface virtual-template 0
NXR(config-if-vt)#ip address 172.16.0.1/32
NXR(config-if-vt)#ip tcp adjust-mss auto
NXR(config-if-vt)#no ip redirects
NXR(config-if-vt)#no ip rebound
NXR(config-if-vt)#peer ip pool smartphoneip
NXR(config-if-vt)#exit
NXR(config)#l2tp udp source-port 1701
NXR(config)#l2tp 1
NXR(config-l2tp)#tunnel address any ipsec
NXR(config-l2tp)#tunnel mode lns
NXR(config-l2tp)#tunnel virtual-template 0
NXR(config-l2tp)#exit
% Restarting l2tp service. Please wait.....
NXR(config)#interface ppp 0
NXR(config-ppp)#ip address 10.10.10.1/32
NXR(config-ppp)#ip masquerade
NXR(config-ppp)#ip access-group in ppp0_in
NXR(config-ppp)#ip spi-filter
```

```
NXR(config-ppp)#ip tcp adjust-mss auto
NXR(config-ppp)#no ip redirects
NXR(config-ppp)#ppp username test1@centurysys
NXR(config-ppp)#ipsec policy 1
NXR(config-ppp)#exit
NXR(config)#interface ethernet 1
NXR(config-if)#no ip address
NXR(config-if)#pppoe-client ppp 0
NXR(config-if)#exit
NXR(config)#dns
NXR(config-dns)#service enable
NXR(config-dns)#exit
NXR(config)#exit
NXR#save config
```

## 【 設定例解説 】

〔NXR の設定〕

### 1. ＜ホスト名の設定＞

```
nxr120(config)#hostname NXR
```

ホスト名に NXR を設定します。

### 2. ＜LAN 側（ethernet0）インタフェース設定＞

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

Ethernet0 インタフェースの IP アドレスに 192.168.10.1/24 を設定します。

### 3. ＜スタティックルート設定＞

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

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を ppp0_in とします。

一行目は宛先 IP アドレス 10.10.10.1 送信元 UDP ポート番号 500 宛先 UDP ポート番号 500 のパケットを許可するように設定します。

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 ローカルポリシー設定＞

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

IPsec ローカルポリシー1を設定します。

```
NXR(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1＞

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

スマートフォンとの接続で使用する ISAKMP ポリシー1を設定します。

```
NXR(config-ipsec-isakmp)#description smartphone
```

ISAKMP ポリシー1の説明として、ここでは smartphone と設定します。

```
NXR(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、スマートフォンと同じ値を設定する必要があります。

```
NXR(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(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(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(config-ipsec-isakmp)#lifetime 86400
```

ISAKMP SA のライフタイムを設定します。ここでは 86400 秒を設定します。

```
NXR(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。ここではメインモードを設定します。

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

対向のスマートフォンの IP アドレスを設定します。ここでは any を設定します。

```
NXR(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1＞

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

スマートフォンとの接続で使用するトンネルポリシー1を設定します。

```
NXR(config-ipsec-tunnel)#description smartphone
```

トンネルポリシー1の説明として、ここでは smartphone と設定します。

```
NXR(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(config-ipsec-tunnel)#no set pfs
```

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 を無効に設定します。

```
NXR(config-ipsec-tunnel)#set sa lifetime 28800
```

IPsec SA のライフタイムを設定します。ここでは 28800 秒を設定します。

```
NXR(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(config-ipsec-tunnel)#match protocol l2tp-smartphone
```

スマートフォンとの間で L2TPv2 over IPsec 接続する際に設定します。

本設定を有効にすると下記の設定が有効となり、IPsec 接続を行う際に下記のパラメータが自動設定されます。

・protocol-mode → transport

・negotiation-mode → responder

・IPsec セレクタ → 以下のように自動設定されます。

| ID ペイロード | NXR 側 | スマートフォン側 |
|---|---|---|
| IPv4 アドレス | host | host |
| プロトコル | UDP | UDP |
| ポート番号 | 1701 | any(どのポートでも受け付ける) |

### 8. ＜PPP アカウント設定＞

```
NXR(config)#ppp account username android01 password android01pass
NXR(config)#ppp account username ios01 password ios01pass
```

PPP のアカウントを設定します。

ここでは L2TPv2 の LNS 機能による着信時のユーザ ID，パスワードを設定します。

(☞) ここで設定したアカウントはアクセスサーバ設定で利用します。

```
NXR(config)#ppp account username test1@centurysys password test1pass
```

ここでは ppp0 インタフェースで使用するユーザ名，パスワードを設定します。

(☞) ここで設定したアカウントは ppp0 インタフェースの設定で利用します。

### 9. ＜アクセスサーバ(RAS)プロファイル設定0＞

```
NXR(config)#access-server profile 0
```

アクセスサーバプロファイル 0 を設定します。

```
NXR(config-ras)#ppp username android01 ip 172.16.0.10
```

ユーザ名 android01 に 172.16.0.10 の IP アドレスを割り当てるよう設定します。

### 10. ＜アクセスサーバ(RAS)プロファイル設定1＞

```
NXR(config)#access-server profile 1
```

アクセスサーバプロファイル 1 を設定します。

```
NXR(config-ras)#ppp username ios01 ip 172.16.0.11
```

ユーザ名 ios01 に 172.16.0.11 の IP アドレスを割り当てるよう設定します。

### 11. ＜IP アドレスプール設定＞

```
NXR(config)#ip local pool smartphoneip address 172.16.0.10 172.16.0.11
```

IP アドレスプールを設定します。

ここでは IP アドレスプール名を smartphoneip としスマートフォンに割り当てる 172.16.0.10～172.16.0.11 の IP アドレスを設定します。

### 12. ＜virtual-template 0 インタフェース設定＞

```
NXR(config)#interface virtual-template 0
```

virtual-template 0 インタフェースを設定します。

virtual-template インタフェースは仮想的なインタフェースであり、実際に作成されるわけではありません。

virtual-template インタフェースを使用するとコールを受けた際に PPP のクローンを作成し、本ノードの設定内容を当該 PPP に適用します。なお PPP クローンのインタフェース番号は、本装置が自動的に割り当てます。

```
NXR(config-if-vt)#ip address 172.16.0.1/32
```

virtual-template インタフェースの IP アドレスに 172.16.0.1/32 を設定します。

```
NXR(config-if-vt)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

```
NXR(config-if-vt)#no ip redirects
```

ICMP リダイレクト機能を無効に設定します。

```
NXR(config-if-vt)#no ip rebound
```

IP リバウンド機能を無効に設定します。

```
NXR(config-if-vt)#peer ip pool smartphoneip
```

使用する IP アドレスプールを設定します。

ここではアクセスサーバ設定で設定した IP アドレスプール名 smartphoneip を設定します。

### 13. ＜L2TPv2 設定＞

```
NXR(config)#l2tp udp source-port 1701
```

L2TPv2 で使用する送信元ポートを 1701 に設定します。

```
NXR(config)#l2tp 1
```

スマートフォンとの接続で使用する L2TP1を設定します。

```
NXR(config-l2tp)#tunnel mode lns
```

L2TPv2 のトンネルモードを設定します。ここでは LNS を指定します。

```
NXR(config-l2tp)#tunnel address any ipsec
```

接続先に IP アドレスとして any を設定します。

また any 指定時にバインドするプロトコルとして IPsec を指定します。これにより IPsec SA の確立したクライアントからの接続のみを許可します。

```
NXR(config-l2tp)#tunnel virtual-template 0
```

LNS 利用時に使用する virtual-template 0 インタフェースを設定します。

**14. ＜WAN 側(ppp0)インタフェース設定＞**

```
NXR(config)#interface ppp 0
```

WAN 側(ppp0)インタフェースを設定します。

```
NXR(config-ppp)#ip address 10.10.10.1/32
```

IP アドレスを 10.10.10.1/32 に設定します。

```
NXR(config-ppp)#ip masquerade
```

IP マスカレードを設定します。

```
NXR(config-ppp)#ip access-group in ppp0_in
```

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パケット(NXR 自身宛)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。

```
NXR(config-ppp)#ip spi-filter
```

ステートフルパケットインスペクションを設定します。

ステートフルパケットインスペクションはパケットを監視してパケットフィルタリング項目を随時変更する機能で、動的パケットフィルタリング機能として利用できます。

該当インタフェースでこの設定を有効にした場合、通常そのインタフェースで受信したパケットは全て破棄されますが、そのインタフェースから送信されたパケットに対応する戻りパケットに対してはアクセスを許可します。

これにより自動的に WAN からの不要なアクセスを制御することが可能です。

```
NXR(config-ppp)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

```
NXR(config-ppp)#no ip redirects
```

ICMP リダイレクト機能を無効に設定します。

```
NXR(config-ppp)#ppp username test1@centurysys
```

PPPoE 接続で使用するユーザ ID を設定します。

ここでは PPP アカウント設定で作成した test1@centurysys を設定します。

```
NXR(config-ppp)#ipsec policy 1
```

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。

**15. ＜ethernet1 インタフェース設定＞**

```
NXR(config)#interface ethernet 1
```

ethernet1 インタフェースを設定します。

```
NXR(config-if)#no ip address
```

ethernet1 インタフェースに IP アドレスを割り当てない設定をします。
PPPoE 接続でプロバイダ等から割り当てられる IP アドレスはイーサネットインタフェースではなく PPP インタフェースに割り当てられますので、PPPoE のみで使用する場合は IP アドレスの設定は不要です。

```
NXR(config-if)#pppoe-client ppp 0
```

ethernet1 インタフェース上で ppp0 インタフェースを使用するための設定をします。
PPPoE で PPP インタフェースを使用する場合は、pppoe-client コマンドによるインタフェース設定での登録が必要になります。

**16. ＜DNS 設定＞**

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

DNS サービスを有効にします。

## 【 スマートフォン設定例 】

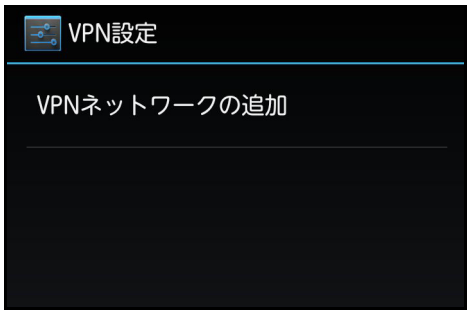
〔Android の設定〕

(☞) ここで記載した設定はあくまで一例ですので、ご利用頂いている Android 端末によって設定が異なる場合があります。
設定の詳細はご利用中の Android 端末の取扱説明書等をご確認下さい。

(☞) 本設定例は Android 端末との接続性を保証するものではありません。
ご利用頂く際には十分な検証を行った上でのご利用をお願い致します。

1. メニュー画面から「設定」をタップします。
2. 設定画面で「無線とネットワーク」をタップします。
3. 無線とネットワーク画面で「VPN 設定」をタップします。


4. VPN 設定画面で「VPN ネットワークの追加」をタップします。



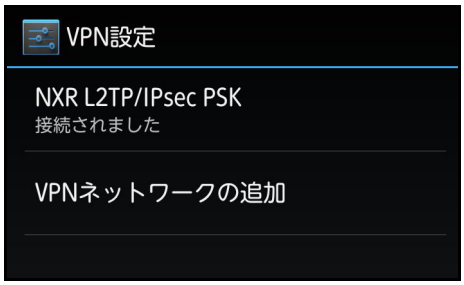
5. VPN ネットワークの編集で以下の各項目を設定し保存します。


| 設定項目 | 設定値 | 備考 |
|---|---|---|
| 名前 | NXR L2TP/IPsec PSK | 任意の名称を設定します |
| タイプ | L2TP/IPSec PSK | |
| サーバーアドレス | 10.10.10.1 | NXR の WAN 側 IP アドレスを設定します |
| L2TP セキュリティ保護 | （未使用） | 本設定例では使用していません |
| IPSec ID | （未使用） | 本設定例では使用していません |
| IPSec 事前共有鍵 | ipseckey | NXR で設定した事前共有鍵を設定します |
| 詳細オプションを表示する | 無効 | |

6. VPN 名「NXR L2TP/IPsec PSK」が作成されますので、作成した「NXR L2TP/IPsec PSK」をタップします。

7. ユーザ名とパスワードの入力画面が表示されますので、L2TP/IPsec 用に設定した PPP のユーザ名とパスワードを入力します。


8. 入力後接続をタップすると VPN 接続を開始し、接続が完了（成功）すると VPN 名の下に「接続されました」と表示されます。

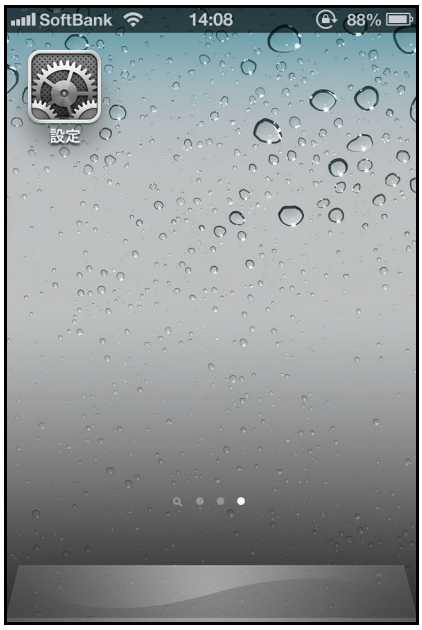


〔iOS の設定〕

(☞) ここで記載した設定はあくまで一例ですので、ご利用頂いている iOS 搭載端末によって設定が異なる場合があります。
設定の詳細はご利用中の iOS 端末の取扱説明書等をご確認下さい。

(☞) 本設定例は iOS 端末との接続性を保証するものではありません。
ご利用頂く際には十分な検証を行った上でのご利用をお願い致します。

1. ホーム画面から「設定」をタップします。




2. 設定画面で「一般」をタップします。

3. 一般画面で「VPN」をタップします。


4. VPN 画面で「VPN 構成を追加…」をタップします。

※この例では「test」という設定が定義されているところに VPN 設定を追加します。

5.　構成を追加画面で「L2TP」を選択し以下の各項目を設定し保存します。


| 設定項目 | 設定値 | 備考 |
|---|---|---|
| 説明 | NXR L2TP/IPsec PSK | 任意の名称を設定します |
| サーバ | 10.10.10.1 | NXR の WAN 側 IP アドレスを設定します |
| アカウント | ios01 | PPP 認証で使用するアカウントを設定します |
| RSA SecurID | オフ | ― |
| パスワード | ios01pass | PPP 認証で使用するパスワードを設定します |
| シークレット | ipseckey | NXR で設定した事前共有鍵を設定します |
| すべての信号を送信 | オン | ― |
| プロキシ | オフ | ― |

6. VPN 構成「NXR L2TP/IPsec PSK」が作成されますので、チェックがついていることを確認します。チェックがついていない場合は作成した VPN 構成をタップします。
そして VPN をオンにし VPN 接続を開始します。


7. VPN 接続完了後は以下のような画面が表示されます。

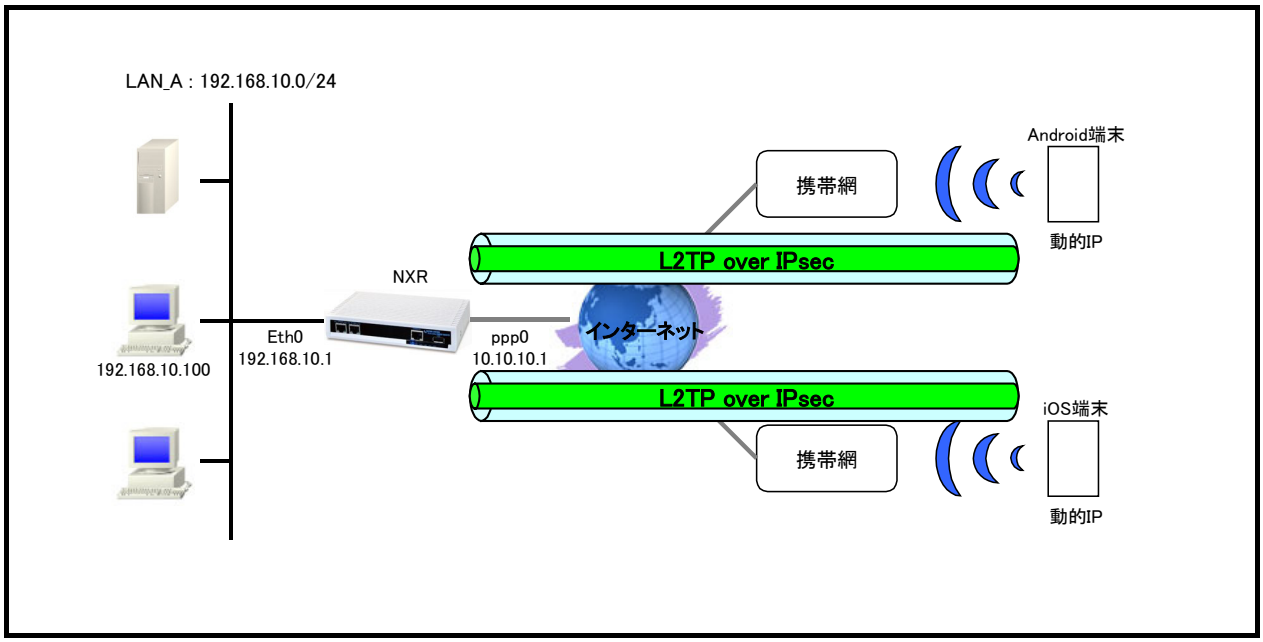

なお「状況」をタップすることで IP アドレスなどの VPN 接続情報が表示されます。


SoftBank
VPN
14:10
87%
VPN
状況
サーバ
10.10.10.1
接続時間
0:21
接続先
172.16.0.1
IPアドレス
172.16.0.11

## 3-2. スマートフォンとの L2TP/IPsec 接続設定例(CRT)

Android や iOS のスマートフォンに搭載されている L2TP/IPsec の VPN 機能を利用することで NXR と VPN 接続することが可能です。この設定例では IPsec で認証に証明書を利用して接続を行います。

### 【 構成図 】




- 接続してきたスマートフォンには IP アドレスプールより IP アドレスを割り当てます。この設定例では2台に IP アドレスを割り当てるため IP アドレスを2つ設定し、かつユーザ ID 毎に指定した IP アドレスを割り当てます。
- X.509 で必要となる証明書や鍵は NXR シリーズでは発行をすることができませんので、FutureNet RA シリーズで発行するか、別途 CA 等で用意しておく必要があります。
- 各種証明書は、NXR では FTP などでインポートが可能です。この設定例では FTP サーバからのインポートを行います。
- 証明書を保管しているサーバを 192.168.10.10 とし、サーバには以下の証明書が保管されています。

| 192.168.10.10 のサーバ | |
|---|---|
| 証明書名 | ファイル名 |
| CA 証明書 | nxrCA.pem |
| CRL | nxrCRL.pem |
| NXR 用証明書 | nxrCert.pem |
| NXR 用秘密鍵 | nxrKey.pem |

ここでは各証明書の拡張子として pem を使用します。

(☞) 各証明書は DER または PEM フォーマットでなくてはなりません。なおどのフォーマットの証明書かどうかはファイルの拡張子で自動的に判断されます。よって PEM の場合は pem,DER の場合は der ま

た cer の拡張子でなければなりません。

なおシングル DES で暗号化された鍵ファイルは使用することができません。

Android であれば SD カードのルートディレクトリへのコピー、iPhone であれば iPhone 構成ユーティリティを使用することで証明書をインポートすることができます。

証明書のインポートについてはご利用機器のマニュアル等をご参照下さい。

## 【 設定例 】

〔NXR の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR
NXR(config)#interface ethernet 0
NXR(config-if)#ip address 192.168.10.1/24
NXR(config-if)#exit
NXR(config)#ip route 0.0.0.0/0 ppp 0
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 50
NXR(config)#ipsec x509 enable
NXR(config)#ipsec x509 ca-certificate nxrCA ftp://192.168.10.10/nxrCA.pem
NXR(config)#ipsec x509 crl nxrCA ftp://192.168.10.10/nxrCRL.pem
NXR(config)#ipsec x509 certificate nxr ftp://192.168.10.10/nxrCert.pem
NXR(config)#ipsec x509 private-key nxr key ftp://192.168.10.10/nxrKey.pem
NXR(config)#ipsec x509 private-key nxr password nxrpass
NXR(config)#ipsec local policy 1
NXR(config-ipsec-local)#address ip
NXR(config-ipsec-local)#x509 certificate nxr
NXR(config-ipsec-local)#exit
NXR(config)#ipsec isakmp policy 1
NXR(config-ipsec-isakmp)#description smartphone
NXR(config-ipsec-isakmp)#authentication rsa-sig
NXR(config-ipsec-isakmp)#hash sha1
NXR(config-ipsec-isakmp)#encryption aes128
NXR(config-ipsec-isakmp)#group 5
NXR(config-ipsec-isakmp)#lifetime 86400
NXR(config-ipsec-isakmp)#isakmp-mode main
NXR(config-ipsec-isakmp)#remote address ip any
NXR(config-ipsec-isakmp)#remote identity dn C=JP,CN=smartphone,E=smartphone@example.com
NXR(config-ipsec-isakmp)#local policy 1
NXR(config-ipsec-isakmp)#exit
NXR(config)#ipsec tunnel policy 1
NXR(config-ipsec-tunnel)#description smartphone
NXR(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR(config-ipsec-tunnel)#no set pfs
NXR(config-ipsec-tunnel)#set sa lifetime 28800
NXR(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR(config-ipsec-tunnel)#match protocol l2tp-smartphone
NXR(config-ipsec-tunnel)#exit
NXR(config)#ppp account username android01 password android01pass
NXR(config)#ppp account username ios01 password ios01pass
NXR(config)#ppp account username test1@centurysys password test1pass
NXR(config)#access-server profile 0
NXR(config-ras)#ppp username android01 ip 172.16.0.10
NXR(config-ras)#exit
NXR(config)#access-server profile 1
NXR(config-ras)#ppp username ios01 ip 172.16.0.11
NXR(config-ras)#exit
NXR(config)#ip local pool smartphoneip address 172.16.0.10 172.16.0.11
NXR(config)#interface virtual-template 0
NXR(config-if-vt)#ip address 172.16.0.1/32
NXR(config-if-vt)#ip tcp adjust-mss auto
NXR(config-if-vt)#no ip redirects
NXR(config-if-vt)#no ip rebound
NXR(config-if-vt)#peer ip pool smartphoneip
NXR(config-if-vt)#exit
NXR(config)#l2tp udp source-port 1701
NXR(config)#l2tp 1
NXR(config-l2tp)#tunnel address any ipsec
NXR(config-l2tp)#tunnel mode lns
```

```
NXR(config-l2tp)#tunnel virtual-template 0
NXR(config-l2tp)#exit
% Restarting l2tp service. Please wait.....
NXR(config)#interface ppp 0
NXR(config-ppp)#ip address 10.10.10.1/32
NXR(config-ppp)#ip masquerade
NXR(config-ppp)#ip access-group in ppp0_in
NXR(config-ppp)#ip spi-filter
NXR(config-ppp)#ip tcp adjust-mss auto
NXR(config-ppp)#no ip redirects
NXR(config-ppp)#ppp username test1@centurysys
NXR(config-ppp)#ipsec policy 1
NXR(config-ppp)#exit
NXR(config)#interface ethernet 1
NXR(config-if)#no ip address
NXR(config-if)#pppoe-client ppp 0
NXR(config-if)#exit
NXR(config)#dns
NXR(config-dns)#service enable
NXR(config-dns)#exit
NXR(config)#exit
NXR#save config
```

## 【 設定例解説 】

〔NXR の設定〕

(☞) ここに記載のない設定項目は、3-1. スマートフォンとの L2TP/IPsec 接続設定例が参考になります ので、そちらをご参照下さい。

### 1. ＜X.509 の有効化＞

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

X.509 機能を有効にします。

### 2. ＜CA 証明書の設定＞

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

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

### 3. ＜CRL の設定＞

```
NXR(config)#ipsec x509 crl nxrCA ftp://192.168.10.10/nxrCRL.pem
```

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

### 4. ＜NXR 用公開鍵証明書の設定＞

```
NXR(config)#ipsec x509 certificate nxr ftp://192.168.10.10/nxrCert.pem
```

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

### 5. ＜NXR 用秘密鍵の設定＞

```
NXR(config)#ipsec x509 private-key nxr key ftp://192.168.10.10/nxrKey.pem
```

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

### 6. ＜NXR 用秘密鍵パスフレーズの設定＞

```
NXR(config)#ipsec x509 private-key nxr password nxrpass
```

NXR 用秘密鍵のパスフレーズである nxrpass を設定します。

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

### 7. ＜IPsec ローカルポリシー設定＞

```
NXR(config-ipsec-local)#x509 certificate nxr
```

X.509 で利用する証明書を指定します。ここでは 4. NXR 用公開鍵証明書の設定で設定した certificate name nxr を設定します。

### 8. ＜IPsec ISAKMP ポリシー設定＞

```
NXR(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(config-ipsec-isakmp)#remote identity dn C=JP,CN=smartphone,E=smartphone@example.com
```

対向のスマートフォンの identity を設定します。

対向のスマートフォンの identity に関しては DN(Distinguished Name)方式で設定しますので、設定前に対向スマートフォンの証明書の DN または subject 等をご確認下さい。
なお X.509 を利用する場合は、identity 設定は必須になります。

## 【 スマートフォン設定例 】

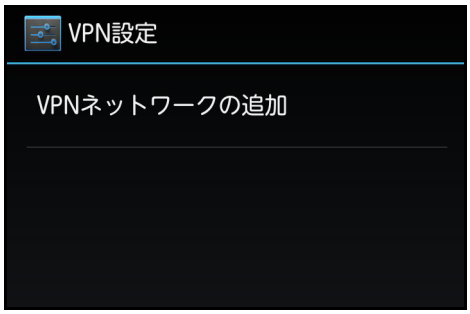
〔Android の設定〕

(☞) ここで記載した設定はあくまで一例ですので、ご利用頂いている Android 端末によって設定が異なる場合があります。
設定の詳細はご利用中の Android 端末の取扱説明書等をご確認下さい。
また証明書は SD カードのルートディレクトリにコピーします。
なお本設定例では証明書はすでにインポート済みとします。

(☞) 本設定例は Android 端末との接続性を保証するものではありません。
ご利用頂く際には十分な検証を行った上でのご利用をお願い致します。

1. メニュー画面から「設定」をタップします。
2. 設定画面で「無線とネットワーク」をタップします。
3. 無線とネットワーク画面で「VPN 設定」をタップします。


4. VPN 設定画面で「VPN ネットワークの追加」をタップします。



5. VPN ネットワークの編集で以下の各項目を設定し保存します。


| 設定項目 | 設定値 | 備考 |
|---|---|---|
| 名前 | NXR L2TP/IPsec CRT | 任意の名称を設定します |
| タイプ | L2TP/IPSec RSA | |
| サーバーアドレス | 10.10.10.1 | NXR の WAN 側 IP アドレスを設定します |
| L2TP セキュリティ保護 | (未使用) | 本設定例では使用していません |
| IPSec ユーザー証明書 | nxr L2TP/IPsec | インポートした証明書を選択します |
| IPSecCA 証明書 | nxr L2TP/IPsec | インポートした証明書を選択します |
| IPSec サーバー証明書 | (サーバーから受信) | |
| 詳細オプションを表示する | 無効 | |

6. VPN 名「NXR L2TP/IPsec CRT」が作成されますので、作成した「NXR L2TP/IPsec CRT」をタップします。

7. ユーザ名とパスワードの入力画面が表示されますので、L2TP/IPsec 用に設定した PPP のユーザ名とパスワードを入力します。


8. 入力後接続をタップすると VPN 接続を開始し、接続が完了(成功)すると VPN 名の下に「接続されました」と表示されます。

〔iOS の設定〕

iOS では iPhone 構成ユーティリティを使用することで証明書をインポートすることができます。

また VPN の設定も iPhone 構成ユーティリティを使用することで行うことができます。証明書をインポートすることができます。

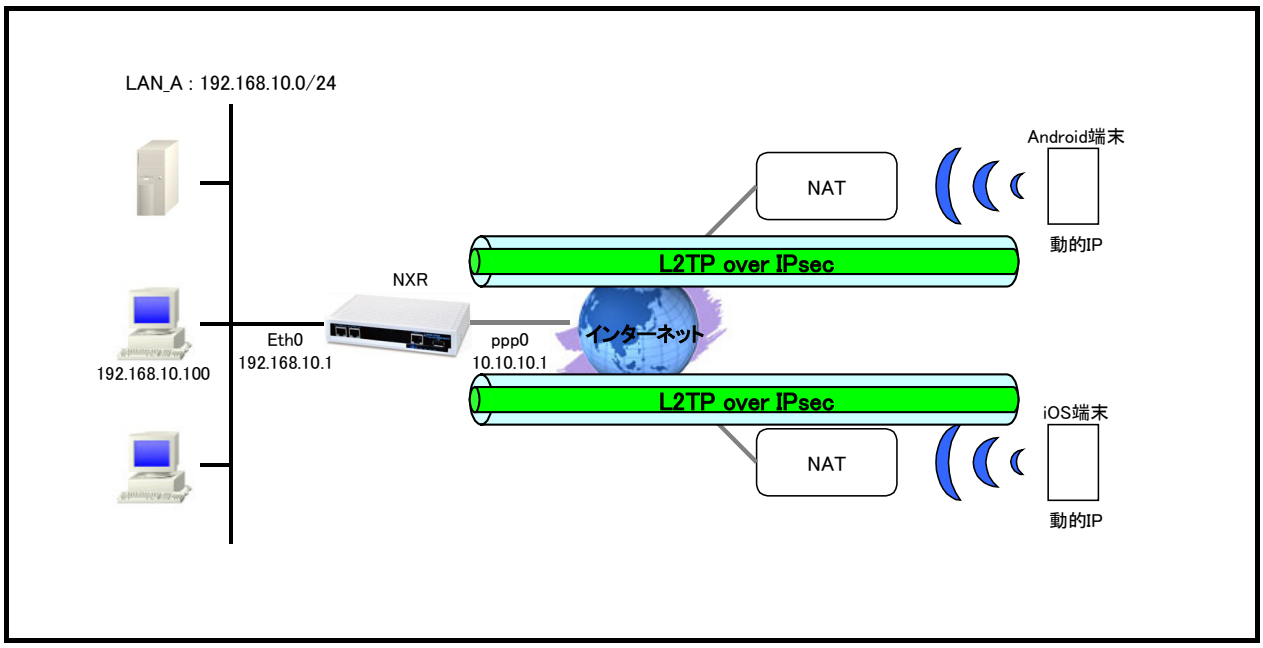
iPhone 構成ユーティリティの使用方法等についてはマニュアル等をご参照下さい。

(☞) 本設定例は iOS 端末との接続性を保証するものではありません。
ご利用頂く際には十分な検証を行った上でのご利用をお願い致します。

# 3-3. スマートフォンとの L2TP/IPsec NAT トラバーサル接続設定例

Android や iOS のスマートフォンが NAT 環境下にある場合に NXR と L2TP/IPsec 接続する設定例です。この設定例では IPsec で事前共有鍵を利用して接続を行います。

## 【 構成図 】




- 接続してきたスマートフォンには IP アドレスプールより IP アドレスを割り当てます。この設定例では2台分の IP アドレスを設定します。また接続してきた端末のユーザ ID に対して IP アドレスプールの範囲内から動的に IP アドレスを割り当てます。
- IP アドレスプールの範囲は NXR の LAN 側ネットワーク内のアドレスとするため virtual-template 0 インタフェースでプロキシ ARP を有効にします。

## 【 設定例 】

〔NXR の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR
NXR(config)#interface ethernet 0
NXR(config-if)#ip address 192.168.10.1/24
NXR(config-if)#exit
NXR(config)#ip route 0.0.0.0/0 ppp 0
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 udp any 500
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 udp any 4500
NXR(config)#ipsec nat-traversal enable
% restart ipsec service to take affect.
NXR(config)#ipsec local policy 1
NXR(config-ipsec-local)#address ip
NXR(config-ipsec-local)#exit
NXR(config)#ipsec isakmp policy 1
NXR(config-ipsec-isakmp)#description smartphone
NXR(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR(config-ipsec-isakmp)#hash sha1
NXR(config-ipsec-isakmp)#encryption aes128
NXR(config-ipsec-isakmp)#group 5
NXR(config-ipsec-isakmp)#lifetime 86400
NXR(config-ipsec-isakmp)#isakmp-mode main
NXR(config-ipsec-isakmp)#remote address ip any
NXR(config-ipsec-isakmp)#local policy 1
NXR(config-ipsec-isakmp)#exit
NXR(config)#ipsec tunnel policy 1
NXR(config-ipsec-tunnel)#description smartphone
NXR(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR(config-ipsec-tunnel)#no set pfs
NXR(config-ipsec-tunnel)#set sa lifetime 28800
NXR(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR(config-ipsec-tunnel)#match protocol l2tp-smartphone nat-traversal
NXR(config-ipsec-tunnel)#exit
NXR(config)#ppp account username android01 password android01pass
NXR(config)#ppp account username ios01 password ios01pass
NXR(config)#ppp account username test1@centurysys password test1pass
NXR(config)#ip local pool smartphoneip address 192.168.10.10 192.168.10.11
NXR(config)#interface virtual-template 0
NXR(config-if-vt)#ip address 192.168.10.1/32
NXR(config-if-vt)#ip tcp adjust-mss auto
NXR(config-if-vt)#no ip redirects
NXR(config-if-vt)#no ip rebound
NXR(config-if-vt)#peer ip pool smartphoneip
NXR(config-if-vt)#peer ip proxy-arp
NXR(config-if-vt)#exit
NXR(config)#l2tp udp source-port 1701
NXR(config)#l2tp 1
NXR(config-l2tp)#tunnel address any ipsec
NXR(config-l2tp)#tunnel mode lns
NXR(config-l2tp)#tunnel virtual-template 0
NXR(config-l2tp)#exit
% Restarting l2tp service. Please wait.....
NXR(config)#interface ppp 0
NXR(config-ppp)#ip address 10.10.10.1/32
NXR(config-ppp)#ip masquerade
NXR(config-ppp)#ip access-group in ppp0_in
NXR(config-ppp)#ip spi-filter
NXR(config-ppp)#ip tcp adjust-mss auto
NXR(config-ppp)#no ip redirects
NXR(config-ppp)#ppp username test1@centurysys
```

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

## 【 設定例解説 】

〔NXR の設定〕

### 1. ＜ホスト名の設定＞

```
nxr120(config)#hostname NXR
```

ホスト名に NXR を設定します。

### 2. ＜LAN 側（ethernet0）インタフェース設定＞

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

Ethernet0 インタフェースの IP アドレスに 192.168.10.1/24 を設定します。

### 3. ＜スタティックルート設定＞

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

フィルタの動作を規定するルールリストを作成します。

ここでは IP アクセスリスト名を ppp0_in とします。

一行目は宛先 IP アドレス 10.10.10.1 宛先 UDP ポート番号 500 のパケットを許可するように設定します。

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。

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

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

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

### 5. ＜IPsec NAT トラバーサルの有効化＞

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

NAT トラバーサルを有効にします。

### 6. ＜IPsec ローカルポリシー設定＞

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

IPsec ローカルポリシー1を設定します。

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

スマートフォンとの接続で使用する ISAKMP ポリシー1を設定します。

```
NXR(config-ipsec-isakmp)#description smartphone
```

ISAKMP ポリシー1の説明として、ここでは smartphone と設定します。

```
NXR(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、スマートフォンと同じ値を設定する必要があります。

```
NXR(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(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(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(config-ipsec-isakmp)#lifetime 86400
```

ISAKMP SA のライフタイムを設定します。ここでは 86400 秒を設定します。

```
NXR(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。ここではメインモードを設定します。

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

対向のスマートフォンの IP アドレスを設定します。ここでは any を設定します。

```
NXR(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(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(config-ipsec-tunnel)#description smartphone
```

トンネルポリシー1の説明として、ここでは smartphone と設定します。

```
NXR(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(config-ipsec-tunnel)#no set pfs
```

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 を無効に設定します。

```
NXR(config-ipsec-tunnel)#set sa lifetime 28800
```

IPsec SA のライフタイムを設定します。ここでは 28800 秒を設定します。

```
NXR(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(config-ipsec-tunnel)#match protocol l2tp-smartphone nat-traversal
```

スマートフォンとの間で L2TPv2 over IPsec NAT トラバーサル接続する際に設定します。

本設定を有効にすると下記の設定が有効となり、IPsec 接続を行う際に下記のパラメータを自動設定します。

・protocol-mode → transport

・negotiation-mode → responder

・IPsec セレクタ → 以下のように自動設定します。また NAT トラバーサル有効時は、NAT 配下のどのアドレスからの接続も受け付けます。

| ID ペイロード | NXR 側 | スマートフォン側 |
|---|---|---|
| IPv4 アドレス | host | host |
| プロトコル | UDP | UDP |
| ポート番号 | 1701 | any(どのポートでも受け付ける) |

### 9. ＜PPP アカウント設定＞

```
NXR(config)#ppp account username android01 password android01pass
NXR(config)#ppp account username ios01 password ios01pass
```

PPP のアカウントを設定します。

ここでは L2TPv2 の LNS 機能による着信時のユーザ ID，パスワードを設定します。

(☞) ここで設定したアカウントはアクセスサーバ設定で利用します。

```
NXR(config)#ppp account username test1@centurysys password test1pass
```

ここでは ppp0 インタフェースで使用するユーザ名，パスワードを設定します。

(☞) ここで設定したアカウントは ppp0 インタフェースの設定で利用します。

### 10. ＜IP アドレスプール設定＞

```
NXR(config)#ip local pool smartphoneip address 172.16.0.10 172.16.0.11
```

IP アドレスプールを設定します。

ここでは IP アドレスプール名を smartphoneip としスマートフォンに割り当てる 172.16.0.10～172.16.0.11 の IP アドレスを設定します。

### 11. ＜virtual-template 0 インタフェース設定＞

```
NXR(config)#interface virtual-template 0
```

virtual-template 0 インタフェースを設定します。

virtual-template インタフェースは仮想的なインタフェースであり、実際に作成されるわけではありません。

virtual-template インタフェースを使用するとコールを受けた際に PPP のクローンを作成し、本ノードの設定内容を当該 PPP に適用します。なお PPP クローンのインタフェース番号は、本装置が自動的に割り当てます。

```
NXR(config-if-vt)#ip address 172.16.0.1/32
```

virtual-template インタフェースの IP アドレスに 172.16.0.1/32 を設定します。

```
NXR(config-if-vt)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

TCP MSS 調整機能は TCP のネゴシエーション時に MSS 値を調整することで、サイズの大きい TCP パケットを転送する際にフラグメントによるスループットの低下を抑制する場合に利用します。

```
NXR(config-if-vt)#no ip redirects
```

ICMP リダイレクト機能を無効に設定します。

```
NXR(config-if-vt)#no ip rebound
```

IP リバウンド機能を無効に設定します。

```
NXR(config-if-vt)#peer ip pool smartphoneip
```

使用する IP アドレスプールを設定します。

ここではアクセスサーバ設定で設定した IP アドレスプール名 smartphoneip を設定します。

```
NXR(config-if-vt)#peer ip proxy-arp
```

プロキシ ARP を設定します。

### 12. ＜L2TPv2 設定＞

```
NXR(config)#l2tp udp source-port 1701
```

L2TPv2 で使用する送信元ポートを 1701 に設定します。

```
NXR(config)#l2tp 1
```

スマートフォンとの接続で使用する L2TP1を設定します。

```
NXR(config-l2tp)#tunnel mode lns
```

L2TPv2 のトンネルモードを設定します。ここでは LNS を指定します。

```
NXR(config-l2tp)#tunnel address any ipsec
```

接続先に IP アドレスとして any を設定します。

また any 指定時にバインドするプロトコルとして IPsec を指定します。これにより IPsec SA の確立したクライアン

トからの接続のみを許可します。

```
NXR(config-l2tp)#tunnel virtual-template 0
```

LNS 利用時に使用する virtual-template 0 インタフェースを設定します。

### 13. ＜WAN 側(ppp0)インタフェース設定＞

```
NXR(config)#interface ppp 0
```

WAN 側(ppp0)インタフェースを設定します。

```
NXR(config-ppp)#ip address 10.10.10.1/32
```

IP アドレスを 10.10.10.1/32 に設定します。

```
NXR(config-ppp)#ip masquerade
```

IP マスカレードを設定します。

```
NXR(config-ppp)#ip access-group in ppp0_in
```

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パケット(NXR 自身宛)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。

```
NXR(config-ppp)#ip spi-filter
```

ステートフルパケットインスペクションを設定します。
ステートフルパケットインスペクションはパケットを監視してパケットフィルタリング項目を随時変更する機能で、動的パケットフィルタリング機能として利用できます。
該当インタフェースでこの設定を有効にした場合、通常そのインタフェースで受信したパケットは全て破棄されますが、そのインタフェースから送信されたパケットに対応する戻りパケットに対してはアクセスを許可します。
これにより自動的に WAN からの不要なアクセスを制御することが可能です。

```
NXR(config-ppp)#ip tcp adjust-mss auto
```

TCP MSS の調整機能をオートに設定します。

```
NXR(config-ppp)#no ip redirects
```

ICMP リダイレクト機能を無効に設定します。

```
NXR(config-ppp)#ppp username test1@centurysys
```

PPPoE 接続で使用するユーザ ID を設定します。
ここでは PPP アカウント設定で作成した test1@centurysys を設定します。

```
NXR(config-ppp)#ipsec policy 1
```

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。

### 14. ＜ethernet1 インタフェース設定＞

```
NXR(config)#interface ethernet 1
```

ethernet1 インタフェースを設定します。

```
NXR(config-if)#no ip address
```

ethernet1 インタフェースに IP アドレスを割り当てない設定をします。

PPPoE 接続でプロバイダ等から割り当てられる IP アドレスはイーサネットインタフェースではなく PPP インタフェースに割り当てられますので、PPPoE のみで使用する場合は IP アドレスの設定は不要です。

```
NXR(config-if)#pppoe-client ppp 0
```

ethernet1 インタフェース上で ppp0 インタフェースを使用するための設定をします。

PPPoE で PPP インタフェースを使用する場合は、pppoe-client コマンドによるインタフェース設定での登録が必要になります。

### 15. ＜DNS 設定＞

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

DNS サービスを有効にします。

## 【 スマートフォン設定例 】

〔Android の設定〕

3-1. スマートフォンとの L2TP/IPsec 接続設定例の〔Android の設定〕と同一ですのでそちらをご参照下さい。

〔iOS の設定〕

3-1. スマートフォンとの L2TP/IPsec 接続設定例の〔iOS の設定〕と同一ですのでそちらをご参照下さい。

# 付録

# IPsec 接続確認方法

## ● ステータスの確認

IPsec の各トンネル状況を一覧で確認する場合は、show ipsec status brief コマンドを使用します。

<実行例>

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

IPsec SA が確立している(IPsec established)ものを up,それ以外を down として表示します。

IPsec の SA 確立状況等を確認する場合は、show ipsec status コマンドを使用します。

また show ipsec status コマンドの後に tunnel <ポリシー番号>を指定することにより tunnel ポリシー毎にステータスを表示させることができます。これは多拠点収容構成で個々のポリシーを確認するのに有効です。

<実行例>

```
nxr120#show ipsec status
000 "tunnel1":192.168.30.0/24===10.10.30.1[nxrc]...10.10.10.1[10.10.10.1]===192.168.10.0/24; erouted; eroute owner: #2
000 "tunnel1":     ike_life: 10800s; ipsec_life: 3600s; margin: 270s; inc_ratio: 100%
000 "tunnel1":     newest ISAKMP SA: #1; newest IPsec SA: #2;
000 "tunnel1":     IKE proposal: AES_CBC_128/HMAC_SHA1/MODP_1536
000 "tunnel1":     ESP proposal: AES_CBC_128/HMAC_SHA1/MODP_1536
000
000 #2: "tunnel1" STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in 3212s; newest IPSEC; eroute owner
000 #2: "tunnel1" esp.7a5cb4c1@10.10.10.1 (0 bytes) esp.9867e772@10.10.30.1 (0 bytes); tunnel
000 #1: "tunnel1" STATE_AGGR_I2 (sent AI2, ISAKMP SA established); EVENT_SA_REPLACE in 10291s; newest ISAKMP
000
Connections:
Security Associations:
   none
```

## ● ログの確認

ログは show syslog message コマンドで確認することができます。

(☞) ここで設定しているシスログのプライオリティは info(初期値)となります。このプライオリティを debug に変更することによりより多くのログが出力されます。

IPsec 接続完了時には以下のようなログが出力されます。

- イニシエータでメインモード利用時

<出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Main Mode
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [strongSwan]
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [XAUTH]
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "tunnel1" #1: ISAKMP SA established
pluto[XXXX]: "tunnel1" #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP {using isakmp#1}
charon: 03[KNL] interface tunnel1 activated
pluto[XXXX]: "tunnel1" #2: sent QI2, IPsec SA established {ESP=>0x14bd33f0 <0xf49c1f56 DPD}
```

- レスポンダでメインモード利用時

<出力例>

```
pluto[XXXX]: packet from 10.10.10.1:500: received Vendor ID payload [strongSwan]
pluto[XXXX]: packet from 10.10.10.1:500: received Vendor ID payload [XAUTH]
pluto[XXXX]: packet from 10.10.10.1:500: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "tunnel1" #3: responding to Main Mode
pluto[XXXX]: "tunnel1" #3: sent MR3, ISAKMP SA established
pluto[XXXX]: "tunnel1" #3: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1" #4: responding to Quick Mode
charon: 03[KNL] interface tunnel1 activated
pluto[XXXX]: "tunnel1" #4: IPsec SA established {ESP=>0x9c4fb981 <0xc30f38e1 DPD}
```

- イニシエータでアグレッシブモード利用時

<出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [strongSwan]
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [XAUTH]
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "tunnel1" #1: sent AI2, ISAKMP SA established
pluto[XXXX]: "tunnel1" #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP+0x4000000
 {using isakmp#1}
charon: 03[KNL] interface tunnel1 activated
pluto[XXXX]: "tunnel1" #2: sent QI2, IPsec SA established {ESP=>0xc5e28ab0 <0x899ed286 DPD}
```

- レスポンダでアグレッシブモード利用時

<出力例>

```
pluto[XXXX]: packet from 10.10.30.1:500: received Vendor ID payload [strongSwan]
pluto[XXXX]: packet from 10.10.30.1:500: received Vendor ID payload [XAUTH]
pluto[XXXX]: packet from 10.10.30.1:500: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "tunnel1"[1] 10.10.30.1 #1: responding to Aggressive Mode from unknown peer 10.10.30.1
pluto[XXXX]: "tunnel1"[1] 10.10.30.1 #1: ISAKMP SA established
pluto[XXXX]: "tunnel1"[1] 10.10.30.1 #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1"[1] 10.10.30.1 #2: responding to Quick Mode
charon: 03[KNL] interface tunnel1 activated
pluto[XXXX]: "tunnel1"[1] 10.10.30.1 #2: IPsec SA established {ESP=>0x899ed286 <0xc5e28ab0 DPD}
```

「ISAKMP SA established」が ISAKMP SA が確立したことを、「IPsec SA established」が IPsec SA が確立したことを示しています。

IPsec 接続が失敗する時に出力されるログとして以下のようなものが挙げられます。

- 対向機器からの応答がない（メインモード）

<イニシエータ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Main Mode
・・・
pluto[XXXX]: "tunnel1" #1: max number of retransmissions (20) reached STATE_MAIN_I1.  No response(or no acceptable response) to our first IKE message
pluto[XXXX]: "tunnel1" #1: starting keying attempt 2 of an unlimited number
pluto[XXXX]: "tunnel1" #2: initiating Main Mode to replace #1
```

(☞) 対向ルータの WAN 回線が接続されているか、パケットが届いているか、IPsec のフィルタ（UDP500）は許可されているか、IPsec サービスが起動しているか、対向ルータで該当する IPsec 設定が正しく設定されているかなどを確認してください。

- 対向機器からの応答がない(アグレッシブモード)

<イニシエータ側のログ出力例>

```
・luto[XXXX]: “tunnel1” #1: initiating Aggressive Mode #1, connection ″tunnel1″
・・・
pluto[XXXX]: ″tunnel1″ #1: max number of retransmissions (20) reached STATE_AGGR_I1
pluto[XXXX]: ″tunnel1″ #1: starting keying attempt 2 of an unlimited number
pluto[XXXX]: ″tunnel1″ #2: initiating Aggressive Mode #2 to replace #1, connection ″tunnel1″
```

(☞) 対向ルータの WAN 回線が接続されているか、パケットが届いているか、IPsec のフィルタ(UDP500)は許可されているか、IPsec サービスが起動しているか、対向ルータで該当する IPsec 設定が正しく設定されているかなどを確認してください。

- 該当するポリシがない(イニシエータがメインモード)

<レスポンダ側のログ出力例>

```
pluto[XXXX]: packet from 10.10.20.1:500: initial Main Mode message received on 10.10.10.1:500 but no connection has been authorized with policy=PSK
```

(☞) フェーズ1のモードは正しいか、対向のルータの IP アドレスの設定は正しいか、IPsec の設定の関連づけは正しいかなどを確認してください。

- 該当するポリシがない(イニシエータがアグレッシブモード)

<レスポンダ側のログ出力例>

```
pluto[XXXX]: packet from 10.10.20.1:500: initial Aggressive Mode message received on 10.10.10.1:500 but no connection has been authorized with policy=PSK
```

(☞) フェーズ1のモードは正しいか、IPsec の設定の関連づけは正しいかなどを確認してください。

- 事前共有鍵の不一致(メインモード)

<レスポンダ側のログ出力例>

```
pluto[XXXX]: ″tunnel1″ #1: responding to Main Mode
pluto[XXXX]: ″tunnel1″ #1:″tunnel1″ #1: next payload type of ISAKMP Identification Payload has an unknown value
pluto[XXXX]: ″tunnel1″ #1: probable authentication failure (mismatch of preshared secrets?):
malformed payload in packet
```

(☞) お互いのルータで設定した事前共有鍵(PSK)の値が正しいか確認してください。

<イニシエータ側のログ出力例>

```
pluto[XXXX]: ″tunnel1″ #1: initiating Main Mode
pluto[XXXX]: ″tunnel1″ #1: next payload type of ISAKMP Hash Payload has an unknown value:
```

(☞) お互いのルータで設定した事前共有鍵(PSK)の値が正しいか確認してください。

- 事前共有鍵の不一致(アグレッシブモード)

<レスポンダ側のログ出力例>

```
pluto[XXXX]: ″tunnel2″[1] 10.10.30.1 #1: responding to Aggressive Mode from unknown peer 10.10.30.1
```

(☞) お互いのルータで設定した事前共有鍵(PSK)の値が正しいか確認してください。

<イニシエータ側のログ出力例>

```
pluto[XXXX]: ″tunnel1″ #1: initiating Aggressive Mode #1, connection ″tunnel1″
pluto[XXXX]: ″tunnel1″ #1: received Hash Payload does not match computed value
pluto[XXXX]: ″tunnel1″ #1: sending notification INVALID_HASH_INFORMATION to 10.10.10.1:500
```

(☞) お互いのルータで設定した事前共有鍵(PSK)の値が正しいか確認してください。

- フェーズ1の ID 不一致(イニシエータの self-identity 不一致)

<レスポンダ側のログ出力例>

```
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: no suitable connection for peer 'nxr'
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: initial Aggressive Mode packet claiming to be from 10.10.30.1 but no connection has been authorized
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: sending notification INVALID_ID_INFORMATION to 10.10.30.1:500
```

(☞) ipsec isakmp policy 設定モードの remote identity コマンドで設定した値(ID タイプを含む)が対向機器の self-identity と一致しているか確認してください。

<イニシエータ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
pluto[XXXX]: packet from 10.10.10.1:500: ignoring informational payload, type INVALID_ID_INFORMATION
```

(☞) ipsec local policy 設定モードの self-identity コマンドで設定した値(ID タイプを含む)が対向機器の remote identity と一致しているか確認してください。

- フェーズ1の ID 不一致(レスポンダの self-identity 不一致)

<レスポンダ側のログ出力例>

```
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: responding to Aggressive Mode from unknown peer 10.10.30.1
pluto[XXXX]: packet from 10.10.30.1:500: ignoring informational payload, type INVALID_ID_INFORMATION
```

(☞) ipsec isakmp policy 設定モードの remote identity コマンドで設定した値(ID タイプを含む)が対向機器の self-identity と一致しているか確認してください。

<イニシエータ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
pluto[XXXX]: "tunnel1" #1: no suitable connection for peer '10.10.10.1'
pluto[XXXX]: "tunnel1" #1: initial Aggressive Mode packet claiming to be from 10.10.10.1but no connection has been authorized
pluto[XXXX]: "tunnel1" #1: sending notification INVALID_ID_INFORMATION to 10.10.10.1:500
```

(☞) ipsec local policy 設定モードの self-identity コマンドで設定した値(ID タイプを含む)が対向機器の remoteidentity と一致しているか確認してください。

- フェーズ 2 の ID 不一致

<レスポンダ側のログ出力例>

```
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: responding to Aggressive Mode from unknown peer 10.10.30.1
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: ISAKMP SA established
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: cannot respond to IPsec SA request because no connectionis known for 192.168.10.0/24===10.10.10.1[10.10.10.1]...10.10.30.1[nxrc]===192.168.30.0/24
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: sending encrypted notification INVALID_ID_INFORMATION to10.10.30.1:500
```

(☞) ipsec access-list コマンドで設定した値が対向機器と対になっているか確認してください。

<イニシエータ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
pluto[XXXX]: "tunnel1" #1: sent AI2, ISAKMP SA established
pluto[XXXX]: "tunnel1" #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP+0x4000000 {using isakmp#1}
pluto[XXXX]: "tunnel1" #1: ignoring informational payload, type INVALID_ID_INFORMATION
```

(☞) ipsec access-list コマンドで設定した値が対向機器と対になっているか確認してください。

- PFS 設定の不一致(レスポンダ側でのみ PFS を設定)

<レスポンダ側のログ出力例>

```
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: responding to Aggressive Mode from unknown peer 10.10.30.1
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: ISAKMP SA established
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #2: we require PFS but Quick I1 SA specifies no GROUP_DESCRIPTION
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #2: sending encrypted notification NO_PROPOSAL_CHOSEN to 10.10.30.1:500
```

(☞) ipsec tunnel policy 設定モードの set pfs コマンドで設定した値が対向機器と一致しているか確認してください。

<イニシエータ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
pluto[XXXX]: "tunnel1" #1: sent AI2, ISAKMP SA established
pluto[XXXX]: "tunnel1" #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+UP+0x4000000 {using isakmp#1}
pluto[XXXX]: "tunnel1" #1: ignoring informational payload, type NO_PROPOSAL_CHOSEN
```

(☞) ipsec tunnel policy 設定モードの set pfs コマンドを設定しているか確認してください。

# L2TP/IPsec 接続確認方法

## ● ステータスの確認

L2TP/IPsec では IPsec, L2TP, PPP の全てが確立および接続している必要があります。

IPsec のトンネル状況を一覧で確認する場合は、show ipsec status brief コマンドを使用します。

<実行例>

```
NXR#show ipsec status brief
TunnelName              Status
tunnel1                  up
```

IPsec SA が確立している(IPsec established)ものを up,それ以外を down として表示します。なおスマートフォン接続用のトンネルポリシは異なる IP アドレスからの複数接続を許可しているため、複数のスマートフォンが接続してる場合でも上記のような表示となります。

IPsec の SA 確立状況等を確認する場合は、show ipsec status コマンドを使用します。

また show ipsec status コマンドの後に tunnel <ポリシー番号>を指定することにより tunnel ポリシー毎にステータスを表示させることができます。これは多拠点収容構成で個々のポリシーを確認するのに有効です。

<実行例>

```
NXR#show ipsec status
000 "tunnel1": 10.10.10.1[10.10.10.1]:17/1701...%any[%any]:17/%any; unrouted; eroute owner: #0
000 "tunnel1":     ike_life: 86400s; ipsec_life: 28800s; margin: 270s; inc_ratio: 100%
000 "tunnel1":     newest ISAKMP SA: #0; newest IPsec SA: #0;
000 "tunnel1"[1]: 10.10.10.1[10.10.10.1]:17/1701...10.10.20.10[10.10.20.10]:17/50891; erouted; eroute owner: #2
000 "tunnel1"[1]:     ike_life: 86400s; ipsec_life: 28800s; margin: 270s; inc_ratio: 100%
000 "tunnel1"[1]:     newest ISAKMP SA: #1; newest IPsec SA: #2;
000 "tunnel1"[1]:     IKE proposal: AES_CBC_256/HMAC_SHA1/MODP_1024
000 "tunnel1"[1]:     ESP proposal: AES_CBC_256/HMAC_SHA1/<N/A>
000
000 #2: "tunnel1"[1] 10.10.20.10 STATE_QUICK_R2 (IPsec SA established); EVENT_SA_REPLACE in 3451s; newest IPSEC; eroute owner
000 #2: "tunnel1"[1] 10.10.20.10 esp.26594af@10.10.20.10 (528 bytes, 14s ago) esp.44242e17@10.10.10.1 (562 bytes, 14s ago); transport
000 #1: "tunnel1"[1] 10.10.20.10 STATE_MAIN_R3 (sent MR3, ISAKMP SA established); EVENT_SA_REPLACE in 3449s; newest ISAKMP
000
Connections:
Security Associations:
   none
```

L2TP の確立状況を確認する場合は、show l2tp コマンドを使用します。

<実行例>

```
NXR#show l2tp
NumL2TPTunnels 1
Tunnel MyID 62277 AssignedID 8 NumSessions 1 PeerIP 10.10.20.10 State established
Session LNS MyID 48685 AssignedID 1055 State established
```

PPP の接続状況をを確認する場合は、show ppp コマンドを使用します。

<実行例>

```
NXR#show ppp
PPP100 session state is connected, line type is L2TP(LNS), time since change 00:00:21
   See also 'show l2tp' command.
```

## ● ログの確認

L2TP/IPsec 接続完了時には以下のようなログが出力されます。

<ログ出力例>

```
pluto[XXXX]: packet from 10.10.20.10:500: ignoring Vendor ID payload [RFC 3947]
pluto[XXXX]: packet from 10.10.20.10:500: ignoring Vendor ID payload [4df37928e9fc4fd1b3262170d515c662]
pluto[XXXX]: packet from 10.10.20.10:500: ignoring Vendor ID payload [8f8d83826d246b6fc7a8a6a428c11de8]
pluto[XXXX]: packet from 10.10.20.10:500: ignoring Vendor ID payload [439b59f8ba676c4c7737ae22eab8f582]
pluto[XXXX]: packet from 10.10.20.10:500: ignoring Vendor ID payload [4d1e0e136deafa34c4f3ea9f02ec7285]
pluto[XXXX]: packet from 10.10.20.10:500: ignoring Vendor ID payload [80d0bb3def54565ee84645d4c85ce3ee]
pluto[XXXX]: packet from 10.10.20.10:500: ignoring Vendor ID payload [9909b64eed937c6573de52ace952fa6b]
pluto[XXXX]: packet from 10.10.20.10:500: ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03]
pluto[XXXX]: packet from 10.10.20.10:500: ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02]
pluto[XXXX]: packet from 10.10.20.10:500: ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02_n]
pluto[XXXX]: packet from 10.10.20.10:500: ignoring Vendor ID payload [FRAGMENTATION 80000000]
pluto[XXXX]: packet from 10.10.20.10:500: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "tunnel1"[1] 10.10.20.10 #1: responding to Main Mode from unknown peer 10.10.20.10
pluto[XXXX]: "tunnel1"[1] 10.10.20.10 #1: received IPSEC_INITIAL_CONTACT, delete old states
pluto[XXXX]: "tunnel1"[1] 10.10.20.10 #1: sent MR3, ISAKMP SA established
pluto[XXXX]: "tunnel1"[1] 10.10.20.10 #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1"[1] 10.10.20.10 #2: responding to Quick Mode
pluto[XXXX]: "tunnel1"[1] 10.10.20.10 #2: IPsec SA established {ESP=>0x026594af <0x44242e17 DPD}
l2tp[XXXX]: L2TP Session Established
l2tp[XXXX]:     Peer IP = 10.10.20.10, port = 50891
l2tp[XXXX]:     Local    Tunnel/Session ID = 62277/48685
l2tp[XXXX]:     Remote Tunnel/Session ID = 8/1055
pppd[XXXX]: L2TPv2 plugin loaded.
pppd[XXXX]: pppd 2.4.4 started
pppd[XXXX]: Using interface ppp100
pppd[XXXX]: Connect: ppp100 <-->
charon: 02[KNL] interface ppp100 activated
pppd[XXXX]: local    IP address 172.16.0.1
pppd[XXXX]: remote IP address 172.16.0.11
```

L2TP/IPsec 接続が失敗する時に出力されるログとして以下のようなものが挙げられます。

※IPsec の接続失敗時のログは IPsec 接続確認方法をご参照下さい。

- L2TP での PPP 接続時のユーザ名が不正

<ログ出力例(L2TP 部分抜粋)>

```
l2tp[XXXX]: L2TP Session Established
l2tp[XXXX]:     Peer IP = 10.10.20.10, port = 59139
l2tp[XXXX]:     Local    Tunnel/Session ID = 51172/15957
l2tp[XXXX]:     Remote Tunnel/Session ID = 18/1354
pppd[XXXX]: L2TPv2 plugin loaded.
pppd[XXXX]: pppd 2.4.4 started
pppd[XXXX]: Using interface ppp102
pppd[XXXX]: Connect: ppp102 <-->
pppd[XXXX]: No CHAP secret found for authenticating ios011
pppd[XXXX]: Peer ios011 failed CHAP authentication
l2tp[XXXX]: L2TP Session Closed
```

(☞) NXR およびスマートフォンでユーザ名が正しく設定されているかを確認してください。

- L2TP での PPP 接続時のパスワードが不正

<ログ出力例(L2TP 部分抜粋)>

```
l2tp[XXXX]: L2TP Session Established
l2tp[XXXX]:     Peer IP = 10.10.20.10, port = 53244
l2tp[XXXX]:     Local   Tunnel/Session ID = 48235/16523
l2tp[XXXX]:     Remote Tunnel/Session ID = 19/1360
pppd[XXXX]: L2TPv2 plugin loaded.
pppd[XXXX]: pppd 2.4.4 started
pppd[XXXX]: Using interface ppp102
pppd[XXXX]: Connect: ppp102 <-->
pppd[XXXX]: Peer ios01 failed CHAP authentication
l2tp[XXXX]: L2TP Session Closed
```

(☞) NXR およびスマートフォンでパスワードが正しく設定されているかを確認してください。

# 設定例 show config 形式サンプル

## 1-1. 固定 IP アドレスでの接続設定例(MainMode の利用)

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.20.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_B
!
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 ip address 10.10.10.1/24
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
```

```
!
!
!
ip route 0.0.0.0/0 10.10.10.254
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 ip address 10.10.20.1/24
 ipsec policy 1
!
dns
 service enable
!
```

```
syslog
  local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 10.10.20.254
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
!
!
!
end
```

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

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrb
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_B
!
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 ip address 10.10.10.1/24
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
```

```
!
!
!
ip route 0.0.0.0/0 10.10.10.254
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrb
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 ip address dhcp
 ipsec policy 1
!
dns
 service enable
```

```
!
syslog
  local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
!
!
!
end
```

## 1-3. RSA 公開鍵暗号方式での接続設定例

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
ipsec generate rsa-sig-key 1024
!
ipsec local policy 1
 address ip
 self-identity fqdn nxra
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication rsa-sig 0sAQOx8kE6uhZTvWMikunsy3uK5/7jIkTXsCjQpgo4B+X64UAVeuxFQZ
3KG3bzyjmyCbpkt0xEiU+v1kF4AOAOXoDfgND+KAdEky/YWqQYzMuuuu2uy/K6E9JA24NACufuqMqgGS
Xc51fJ/6V5Qi9YtVd7TWBkZQSZJJADBHs/YyYD9Q==
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.20.1
 remote identity fqdn nxrb
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_B
!
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 ip address 10.10.10.1/24
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
```

```
!
!
!
!
!
ip route 0.0.0.0/0 10.10.10.254
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
ipsec generate rsa-sig-key 1024
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrb
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication rsa-sig 0sAQNe9Ghb4CNEaJuIIy67aSxECLJDHhvndH1opuMs6P8yGiTNlcGeSO
Q8XEy8iYTst2bv022XUxSt37RhOR5lRiY1i83TXkQZbhnJDCNJv+rtX/aro745MbJ9auXT1L5tda4C54
S7SELboAtU28sD3si0OwlzLWtE7yRUqLP4ZiiNMw==
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.10.1
 remote identity fqdn nxra
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface ethernet 0
 ip address 192.168.20.1/24
!
```

```
interface ethernet 1
  ip address 10.10.20.1/24
  ipsec policy 1
!
dns
  service enable
!
syslog
  local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 10.10.20.254
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
!
!
!
end
```

## 1-4. X.509(デジタル署名認証)方式での接続設定例

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
ipsec x509 enable
ipsec x509 ca-certificate nxr
ipsec x509 certificate nxra
ipsec x509 private-key nxra key
ipsec x509 private-key nxra password nxrapass
ipsec x509 crl nxr
!
ipsec local policy 1
 address ip
 self-identity dn /C=JP/CN=nxra/E=nxra@example.com
 x509 certificate nxra
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication rsa-sig
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.20.1
 remote identity dn /C=JP/CN=nxrb/E=nxrb@example.com
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_B
!
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 ip address 10.10.10.1/24
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
```

```
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 10.10.10.254
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
ipsec x509 enable
ipsec x509 ca-certificate nxr
ipsec x509 certificate nxrb
ipsec x509 private-key nxrb key
ipsec x509 private-key nxrb password nxrbpass
ipsec x509 crl nxr
!
ipsec local policy 1
 address ip
 self-identity dn /C=JP/CN=nxrb/E=nxrb@example.com
 x509 certificate nxrb
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication rsa-sig
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.10.1
 remote identity dn /C=JP/CN=nxra/E=nxra@example.com
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
```

```
  set pfs group5
  set key-exchange isakmp 1
  match address LAN_A
!
!
interface ethernet 0
  ip address 192.168.20.1/24
!
interface ethernet 1
  ip address 10.10.20.1/24
  ipsec policy 1
!
dns
  service enable
!
syslog
  local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 10.10.20.254
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
!
!
!
end
```

## 1-5. PPPoE を利用した IPsec 接続設定例

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey1
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.20.1
 local policy 1
!
ipsec isakmp policy 2
 description NXR_C
 authentication pre-share ipseckey2
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrc
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_B
!
ipsec tunnel policy 2
 description NXR_C
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 2
 match address LAN_C
!
!
interface ppp 0
 ip address 10.10.10.1/32
```

```
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@centurysys password test1pass
 ipsec policy 1
!
interface bridge 0
 no ip address
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
ip access-list ppp0_in permit any 10.10.10.1 50
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
ipsec access-list LAN_C ip 192.168.10.0/24 192.168.30.0/24
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
```

```
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey1
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface ppp 0
 ip address 10.10.20.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test2@centurysys password test2pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 udp 500 500
ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 50
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
!
```

```
!
!
end
```

〔NXR_C の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_C
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrc
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey2
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test3@centurysys password test3pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.30.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
```

```
!
dns
  service enable
!
syslog
  local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
ip access-list ppp0_in permit 10.10.10.1 any 50
!
ipsec access-list LAN_A ip 192.168.30.0/24 192.168.10.0/24
!
!
!
end
```

## 1-6. IPsec NAT トラバーサル接続設定例

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
ipsec nat-traversal enable
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrb
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_B
!
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@centurysys password test1pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
```

```
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.10.1 udp any 500
ip access-list ppp0_in permit any 10.10.10.1 udp any 4500
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
ipsec nat-traversal enable
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrb
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
```

```
  set transform esp-aes128 esp-sha1-hmac
  set pfs group5
  set key-exchange isakmp 1
  match address LAN_A
!
!
interface ethernet 0
  ip address 192.168.20.1/24
!
interface ethernet 1
  ip address 192.168.120.1/24
  ipsec policy 1
!
dns
  service enable
!
syslog
  local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 192.168.120.254
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
!
!
!
end
```

## 2-1. 固定 IP アドレスでの接続設定例(MainMode の利用)

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.20.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_B
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 ip address 10.10.10.1/24
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
```

```
!
!
!
!
!
!
ip route 192.168.20.0/24 tunnel 1
ip route 0.0.0.0/0 10.10.10.254
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
```

```
interface ethernet 0
  ip address 192.168.20.1/24
!
interface ethernet 1
  ip address 10.10.20.1/24
  ipsec policy 1
!
dns
  service enable
!
syslog
  local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.10.0/24 tunnel 1
ip route 0.0.0.0/0 10.10.20.254
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
!
!
!
end
```

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

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrb
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_B
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 ip address 10.10.10.1/24
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
```

```
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.20.0/24 tunnel 1
ip route 0.0.0.0/0 10.10.10.254
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrb
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface tunnel 1
 no ip address
```

```
  ip tcp adjust-mss auto
  tunnel mode ipsec ipv4
  tunnel protection ipsec policy 1
!
interface ethernet 0
  ip address 192.168.20.1/24
!
interface ethernet 1
  ip address dhcp
  ipsec policy 1
!
dns
  service enable
!
syslog
  local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.10.0/24 tunnel 1
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
!
!
!
end
```

## 2-3. RSA 公開鍵暗号方式での接続設定例

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
ipsec generate rsa-sig-key 1024
!
ipsec local policy 1
 address ip
 self-identity fqdn nxra
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication rsa-sig 0sAQOx8kE6uhZTvWMikunsy3uK5/7jIkTXsCjQpgo4B+X64UAVeuxFQZ
3KG3bzyjmyCbpkt0xEiU+v1kF4AOAOXoDfgND+KAdEky/YWqQYzMuuuu2uy/K6E9JA24NACufuqMqgGS
Xc51fJ/6V5Qi9YtVd7TWBkZQSZJJADBHs/YyYD9Q==
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.20.1
 remote identity fqdn nxrb
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_B
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 ip address 10.10.10.1/24
 ipsec policy 1
!
dns
 service enable
!
syslog
```

```
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 10.10.10.254
ip route 192.168.20.0/24 tunnel 1
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
ipsec generate rsa-sig-key 1024
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrb
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication rsa-sig 0sAQNe9Ghb4CNEaJuIIy67aSxECLJDHhvndH1opuMs6P8yGiTNlcGeSO
Q8XEy8iYTst2bv022XUxSt37RhOR5lRiY1i83TXkQZbhnJDCNJv+rtX/aro745MbJ9auXT1L5tda4C54
S7SELboAtU28sD3si0OwlzLWtE7yRUqLP4ZiiNMw==
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.10.1
 remote identity fqdn nxra
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
```

```
  set key-exchange isakmp 1
  match address LAN_A
!
!
interface tunnel 1
  no ip address
  ip tcp adjust-mss auto
  tunnel mode ipsec ipv4
  tunnel protection ipsec policy 1
!
interface ethernet 0
  ip address 192.168.20.1/24
!
interface ethernet 1
  ip address 10.10.20.1/24
  ipsec policy 1
!
dns
  service enable
!
syslog
  local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 10.10.20.254
ip route 192.168.10.0/24 tunnel 1
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
!
!
!
end
```

## 2-4. X.509(デジタル署名認証)方式での接続設定例

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
ipsec x509 enable
ipsec x509 ca-certificate nxr
ipsec x509 certificate nxra
ipsec x509 private-key nxra key
ipsec x509 private-key nxra password nxrapass
ipsec x509 crl nxr
!
ipsec local policy 1
 address ip
 self-identity dn /C=JP/CN=nxra/E=nxra@example.com
 x509 certificate nxra
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication rsa-sig
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.20.1
 remote identity dn /C=JP/CN=nxrb/E=nxrb@example.com
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_B
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 ip address 10.10.10.1/24
 ipsec policy 1
!
```

```
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.20.0/24 tunnel 1
ip route 0.0.0.0/0 10.10.10.254
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
ipsec x509 enable
ipsec x509 ca-certificate nxr
ipsec x509 certificate nxrb
ipsec x509 private-key nxrb key
ipsec x509 private-key nxrb password nxrbpass
ipsec x509 crl nxr
!
ipsec local policy 1
 address ip
 self-identity dn /C=JP/CN=nxrb/E=nxrb@example.com
 x509 certificate nxrb
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication rsa-sig
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.10.1
```

```
 remote identity dn /C=JP/CN=nxra/E=nxra@example.com
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 ip address 10.10.20.1/24
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.10.0/24 tunnel 1
ip route 0.0.0.0/0 10.10.20.254
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
!
!
!
end
```

## 2-5. PPPoE を利用した IPsec 接続設定例

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey1
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.20.1
 local policy 1
!
ipsec isakmp policy 2
 description NXR_C
 authentication pre-share ipseckey2
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrc
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_B
!
ipsec tunnel policy 2
 description NXR_C
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 2
 match address LAN_C
!
!
interface tunnel 1
 no ip address
```

```
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface tunnel 2
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 2
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@centurysys password test1pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.20.0/24 tunnel 1
ip route 192.168.30.0/24 tunnel 2
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
ip access-list ppp0_in permit any 10.10.10.1 50
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
ipsec access-list LAN_C ip 192.168.10.0/24 192.168.30.0/24
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey1
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ppp 0
 ip address 10.10.20.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test2@centurysys password test2pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
```

```
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.10.0/24 tunnel 1
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 udp 500 500
ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 50
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
!
!
!
end
```

〔NXR_C の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_C
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrc
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey2
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
```

```
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test3@centurysys password test3pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.30.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.10.0/24 tunnel 1
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
ip access-list ppp0_in permit 10.10.10.1 any 50
!
ipsec access-list LAN_A ip 192.168.30.0/24 192.168.10.0/24
!
!
!
end
```

## 2-6. IPsec NAT トラバーサル接続設定例

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
ipsec nat-traversal enable
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrb
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_B
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@centurysys password test1pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
```

```
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.20.0/24 tunnel 1
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.10.1 udp any 500
ip access-list ppp0_in permit any 10.10.10.1 udp any 4500
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
ipsec nat-traversal enable
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrb
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
```

```
 isakmp-mode aggressive
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 ip address 192.168.120.1/24
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.10.0/24 tunnel 1
ip route 0.0.0.0/0 192.168.120.254
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
!
!
!
end
```

## 2-7. ネットワークイベント機能で IPsec トンネルを監視

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrb
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_B
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 ip address 10.10.10.1/24
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
```

```
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 192.168.20.0/24 tunnel 1
ip route 0.0.0.0/0 10.10.10.254
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrb
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip 10.10.10.1
 local policy 1
 netevent 1 reconnect
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface tunnel 1
```

```
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 ip address dhcp
 ipsec policy 1
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
track 1 ip reachability 192.168.10.1 interface tunnel 1 10 3
!
!
ip route 192.168.10.0/24 tunnel 1
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
!
!
!
end
```

## 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

〔NXR_A の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_A
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey1
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.20.1
 local policy 1
!
ipsec isakmp policy 2
 description NXR_C
 authentication pre-share ipseckey2
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn nxrc
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_B
!
ipsec tunnel policy 2
 description NXR_C
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 2
 match address LAN_C
!
!
interface tunnel 1
 ip address 192.168.10.1/32
```

```
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface tunnel 2
 ip address 192.168.10.1/32
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 2
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@centurysys password test1pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
router ospf
 router-id 172.31.0.1
 network 192.168.10.0/24 area 0
 passive-interface ethernet 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
ip access-list ppp0_in permit any 10.10.10.1 50
!
ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
ipsec access-list LAN_C ip 192.168.10.0/24 192.168.30.0/24
!
!
!
end
```

〔NXR_B の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_B
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey1
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ip 10.10.10.1
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface tunnel 1
 ip address 192.168.20.1/32
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ppp 0
 ip address 10.10.20.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test2@centurysys password test2pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.20.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
```

```
router ospf
 router-id 172.31.0.2
 network 192.168.20.0/24 area 0
 passive-interface ethernet 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 udp 500 500
ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 50
!
ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
!
!
!
end
```

〔NXR_C の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR_C
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
 self-identity fqdn nxrc
!
!
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey2
 hash sha1
 encryption aes128
 group 5
 isakmp-mode aggressive
 remote address ip 10.10.10.1
```

```
 local policy 1
!
!
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address LAN_A
!
!
interface tunnel 1
 ip address 192.168.30.1/32
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ppp 0
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test3@centurysys password test3pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.30.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
router ospf
 router-id 172.31.0.3
 network 192.168.30.0/24 area 0
 passive-interface ethernet 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
ip access-list ppp0_in permit 10.10.10.1 any 50
!
ipsec access-list LAN_A ip 192.168.30.0/24 192.168.10.0/24
!
!
!
```

```
end
```

## 3-1. スマートフォンとの L2TP/IPsec 接続設定例

〔NXR の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
ppp account username android01 password android01pass
ppp account username ios01 password ios01pass
ppp account username test1@centurysys password test1pass
!
!
l2tp udp source-port 1701
!
l2tpv3 udp source-port 40001
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description smartphone
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 lifetime 86400
 isakmp-mode main
 remote address ip any
 local policy 1
!
!
ipsec tunnel policy 1
 description smartphone
 set transform esp-aes128 esp-sha1-hmac
 no set pfs
 set key-exchange isakmp 1
 set sa lifetime 28800
 match protocol l2tp-smartphone
!
!
l2tp 1
 tunnel address any ipsec
 tunnel mode lns
 tunnel virtual-template 0
!
interface virtual-template 0
 ip address 172.16.0.1/32
 no ip redirects
 no ip rebound
 ip tcp adjust-mss auto
 peer ip pool smartphoneip
!
interface ppp 0
```

```
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@centurysys
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
access-server profile 0
 ppp username android01 ip 172.16.0.10
!
access-server profile 1
 ppp username ios01 ip 172.16.0.11
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip local pool smartphoneip address 172.16.0.10 172.16.0.11
!
ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
ip access-list ppp0_in permit any 10.10.10.1 50
!
!
!
end
```

## 3-2. スマートフォンとの L2TP/IPsec 接続設定例(CRT)

〔NXR の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
ppp account username android01 password android01pass
ppp account username ios01 password ios01pass
ppp account username test1@centurysys password test1pass
!
ipsec x509 enable
ipsec x509 ca-certificate nxrCA
ipsec x509 certificate nxr
ipsec x509 private-key nxr key
ipsec x509 private-key nxr password nxrpass
ipsec x509 crl nxrCA
!
l2tp udp source-port 1701
!
l2tpv3 udp source-port 40001
!
ipsec local policy 1
 address ip
 x509 certificate nxr
!
!
ipsec isakmp policy 1
 description smartphone
 authentication rsa-sig
 hash sha1
 encryption aes128
 group 5
 lifetime 86400
 isakmp-mode main
 remote address ip any
 remote identity dn C=JP,CN=smartphone,E=smartphone@example.com
 local policy 1
!
!
ipsec tunnel policy 1
 description smartphone
 set transform esp-aes128 esp-sha1-hmac
 no set pfs
 set key-exchange isakmp 1
 set sa lifetime 28800
 match protocol l2tp-smartphone
!
!
l2tp 1
 tunnel address any ipsec
 tunnel mode lns
 tunnel virtual-template 0
!
```

```
interface virtual-template 0
 ip address 172.16.0.1/32
 no ip redirects
 no ip rebound
 ip tcp adjust-mss auto
 peer ip pool smartphoneip
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@centurysys
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
access-server profile 0
 ppp username android01 ip 172.16.0.10
!
access-server profile 1
 ppp username ios01 ip 172.16.0.11
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip local pool smartphoneip address 172.16.0.10 172.16.0.11
!
ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
ip access-list ppp0_in permit any 10.10.10.1 50
!
!
!
end
```

## 3-3. スマートフォンとの L2TP/IPsec NAT トラバーサル接続設定例

〔NXR の設定〕

```
!
! Century Systems NXR-120 Series ver 5.22.2 (build 29/16:42 01 02 2013)
!
hostname NXR
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
ppp account username android01 password android01pass
ppp account username ios01 password ios01pass
ppp account username test1@centurysys password test1pass
!
ipsec nat-traversal enable
!
l2tp udp source-port 1701
!
l2tpv3 udp source-port 40001
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description smartphone
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 lifetime 86400
 isakmp-mode main
 remote address ip any
 local policy 1
!
!
ipsec tunnel policy 1
 description smartphone
 set transform esp-aes128 esp-sha1-hmac
 no set pfs
 set key-exchange isakmp 1
 set sa lifetime 28800
 match protocol l2tp-smartphone nat-traversal
!
!
l2tp 1
 tunnel address any ipsec
 tunnel mode lns
 tunnel virtual-template 0
!
interface virtual-template 0
 ip address 192.168.10.1/32
 no ip redirects
 no ip rebound
 ip tcp adjust-mss auto
 peer ip proxy-arp
 peer ip pool smartphoneip
```

```
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@centurysys
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
system led ext 0 signal-level mobile 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip local pool smartphoneip address 192.168.10.10 192.168.10.11
!
ip access-list ppp0_in permit any 10.10.10.1 udp any 500
ip access-list ppp0_in permit any 10.10.10.1 udp any 4500
!
!
!
end
```

# サポートデスクへのお問い合わせ

# サポートデスクへのお問い合わせに関して

サポートデスクにお問い合わせ頂く際は、以下の情報をお知らせ頂けると効率よく対応させて頂くことが可能ですので、ご協力をお願い致します。

※FutureNet サポートデスク宛にご提供頂きました情報は、製品のお問合せなどサポート業務以外の目的には利用致しません。
なおご提供頂く情報の取り扱いについて制限等がある場合には、お問い合わせ時または事前にその旨ご連絡下さい。(設定ファイルのプロバイダ情報や IPsec の事前共有鍵情報を削除してお送り頂く場合など)
弊社のプライバシーポリシーについては下記 URL の内容をご確認下さい。
http://www.centurysys.co.jp/company/privacy.html

■ ご利用頂いている NXR 製品を含むネットワーク構成図
(ご利用頂いている回線やルータを含むネットワーク機器の IP アドレスを記載したもの)

■ 障害・不具合の内容およびその再現手順
(いつどこで何を行った場合にど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)

□ 問い合わせ内容例1

〇月〇日〇〇時〇〇分頃より拠点 A と拠点 B の間で IPsec による通信ができなくなった。障害発生前までは問題なく利用可能だった。現在当該拠点のルータの LAN 側 IP アドレスに対して Ping による疎通は確認できたが、対向ルータの LAN 側 IP アドレス, 配下の端末に対しては Ping による疎通は確認できない。
障害発生前後で拠点 B のバックアップ回線としてモバイルカードを接続し、ppp1 インタフェースの設定を行った。設定を元に戻すと通信障害は解消する。
機器の内蔵時計は NTP で同期を行っている。

□ 問い合わせ内容例2

- 発生日時
  〇月〇日〇〇時〇〇分頃
- 発生拠点
  拠点 AB 間
- 障害内容
  IPsec による通信ができなくなった。
- 切り分け内容
  ルータ配下の端末から当該拠点のルータの LAN 側 IP アドレスに対して Ping による疎通確認可能。
  対向ルータの LAN 側 IP アドレス, 配下の端末に対しては Ping による疎通確認不可。
- 障害発生前後での作業
  ルータの設定変更やネットワークに影響する作業は行っていない。
- 備考
  障害発生前までは問題なく利用可能だった。
  機器の内蔵時計は拠点 A の機器で 10 分、拠点 B の機器で 5 分遅れている。

□ 問い合わせ内容例3

現在 IPsec の設定中だが、一度も IPsec SA の確立および IPsec の通信ができていない。IPsec を設定している拠点からのインターネットアクセスおよび該当拠点への Ping による疎通確認も可能。設定例集，設定例集内のログ一覧および NXR シスログ一覧は未確認。

□ 良くない問い合わせ内容例1

VPN ができない。

→VPN として利用しているプロトコルは何か。VPN のトンネルが確立できないのか、通信ができないのかなど不明。

□ 良くない問い合わせ内容例2

通信ができない。

→どのような通信がいつどこでできない（またはできなくなった）のかが不明。

NXR での情報取得方法は以下のとおりです。

※情報を取得される前に

シリアル接続で情報を取得される場合は取得前に下記コマンドを実行してください。

#terminal width 180（初期値に戻す場合は terminal no width）

■ ご利用頂いている NXR 製品での不具合発生時のログ

ログは以下のコマンドで出力されます。

#show syslog message

■ ご利用頂いている NXR 製品のテクニカルサポート情報の結果

テクニカルサポート情報は以下のコマンドで出力されます。

# show tech-support

■ 障害発生時のモバイル関連コマンドの実行結果（モバイルカード利用時のみ）

#show mobile <N> ap

#show mobile <N> phone-number

#show mobile <N> signal-level

※<N>はモバイルデバイスナンバ

# サポートデスクのご利用に関して

電話サポート

電話番号:**0422－37－8926**

電話での対応は以下の時間帯で行います。

月曜日 ～ 金曜日 10:00 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, WXR 設定例集

IPsec 編

Ver 1.1.0

2013 年 4 月

発行　センチュリー・システムズ株式会社