FutureNet NXR,WXR シリーズ

設定例集

IPv6編

Ver 1.1.0

センチュリー・システムズ株式会社



目次

目次	2
はじめに	3
改版履歴	4
1. IPv6 ブリッジ設定	5
1-1. IPv4 PPPoE+IPv6 ブリッジ設定	6
2. IPv6 PPPoE 設定	10
2-1. IPv6 PPPoE 接続設定	11
2-2. IPv4+IPv6 PPPoE 接続設定	
3. IPv6 IPoE 設定	22
3-1. IPv6 IPoE(RA)接続設定	23
3-2. IPv6 IPoE(DHCPv6-PD)接続設定	27
3-3. IPv4 PPPoE+IPv6 IPoE(RA)接続設定	31
3-4. IPv4 PPPoE+IPv6 IPoE(DHCPv6-PD)接続設定	36
4. IPv6 IPsec 設定	41
4-1. IPv6 PPPoE IPsec 接続設定	42
4-2. IPv6 IPoE(RA)IPsec 接続設定(ネームの利用)	54
4-3. IPv6 IPoE(DHCPv6-PD)IPsec 接続設定	
付録	77
設定例 show config 形式サンプル	
サポートデスクへのお問い合わせ	96
サポートデスクへのお問い合わせに関して	97
サポートデフクのご利田に関して	00

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-155/C シリーズ, NXR-230/C.NXR-350/C.NXR-1200.NXR-G100 シリーズ.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-G100 シリーズの以下のバージョンをベースに作成しております。 FutureNet NXR-G100 Ver6.6.5

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。

なお NXR-155/C シリーズは IPv6 アドレスが動的に割り当てられる環境で IPsec を利用することができません。(2015/9 現在)

- 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。
- モバイルデータ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	IPv6 IPsec 設定例追加

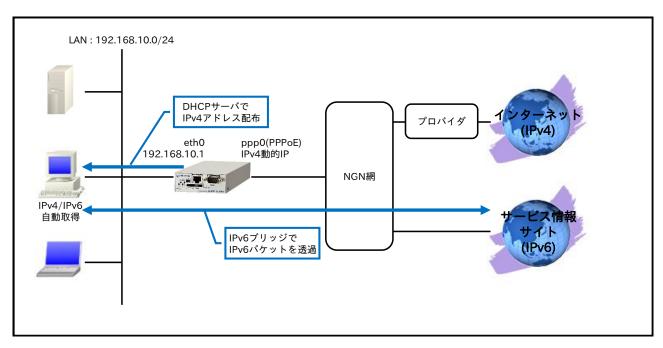
1. IPv6 ブリッジ設定

1-1. IPv4 PPPoE+IPv6 ブリッジ設定

1-1. IPv4 PPPoE+IPv6 ブリッジ設定

NTT 東日本/西日本が提供するフレッツ光ネクスト回線で PPPoE によるインターネット接続(IPv4)を行います。また、IPv6 ブリッジを同時に行うことでサービス情報サイト(IPv6)にも接続できるようにします。

【構成図】



・ IPv6 でサービス情報サイトにアクセスできるようにするため、IPv6 ブリッジを有効にします。これによりルータ配下の端末は NGN 網から広告されるプレフィックス情報を元に IPv6 アドレスを自動生成することができます。

【設定データ】

	設定項目	設定内容
LAN 側インタフェース	ethernet0のIPアドレス	192.168.10.1/24
	PPPoE クライアント(ethernet1)	ppp0
	ppp0のIPv4アドレス	動的 IP アドレス
	IPマスカレード	有効
WAN 側インタフェース	SPI フィルタ	有効
	IPv4 TCP MSS 自動調整	オート
	IPv4 ISP 接続用ユーザ ID	test1@example.jp
	IPv4 ISP 接続用パスワード	test1pass
フクニュックリ し	宛先 IP アドレス	0.0.0.0/0
スタティックルート	ゲートウェイ(インタフェース)	ppp0
	IPv4 アドレス払い出し範囲(始点)	192.168.10.200
DIICD # 18	IPv4 アドレス払い出し範囲(終点)	192.168.10.210
DHCP サーバ	ゲートウェイ	192.168.10.1
	プライマリ DNS サーバ	192.168.10.1
ID O THE ST	対角ノンカフェーフ	ethernet0
IPv6 ブリッジ	対象インタフェース	ethernet1
DNS	サービス	有効
FastFowarding	•	有効

【設定例】

```
nxrg100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg100(config)#interface ethernet 0
nxrg100(config-if)#ip address 192.168.10.1/24
nxrg100(config-if)#exit
nxrg100(config)#dhcp-server 1
nxrg100(config-dhcps)#network 192.168.10.0/24 range 192.168.10.200 192.168.10.210
nxrg100(config-dhcps)#gateway 192.168.10.1
nxrg100(config-dhcps)#dns-server 192.168.10.1
nxrg100(config-dhcps)#exit
nxrg100(config)#ipv6 bridge ethernet 0 ethernet 1
nxrg100(config)#ip route 0.0.0.0/0 ppp 0
nxrg100(config)#ppp account username test1@example.jp password test1pass
nxrg100(config)#interface ppp 0
nxrg100(config-ppp)#ip address negotiated
nxrg100(config-ppp)#ip masquerade
nxrg100(config-ppp)#ip spi-filter
nxrg100(config-ppp)#ip tcp adjust-mss auto
nxrg100(config-ppp)#ppp username test1@example.jp
nxrg100(config-ppp)#exit
nxrg100(config)#interface ethernet 1
nxrg100(config-if)#no ip address
nxrg100(config-if)#pppoe-client ppp 0
nxrg100(config-if)#exit
nxrg100(config)#dns
nxrg100(config-dns)#service enable
nxrg100(config-dns)#exit
nxrg100(config)#fast-forwarding enable
nxrg100(config)#exit
nxrg100#save config
```

【設定例解説】

1. <LAN 側(ethernet0)インタフェース設定>

```
nxrg100(config)#interface ethernet 0
nxrg100(config-if)#ip address 192.168.10.1/24
```

ethernet() インタフェースの IP アドレスを設定します。

2. <DHCP サーバ設定>

```
nxrg100(config)#dhcp-server 1
nxrg100(config-dhcps)#network 192.168.10.0/24 range 192.168.10.200 192.168.10.210
nxrg100(config-dhcps)#gateway 192.168.10.1
nxrg100(config-dhcps)#dns-server 192.168.10.1
```

DHCP サーバのサーバナンバを1とし、配布する IPv4 アドレス情報を設定します。

3. <IPv6 ブリッジ設定>

```
nxrg100(config)#ipv6 bridge ethernet 0 ethernet 1
```

IPv6 ブリッジするインタフェースを設定します。

4. <スタティックルート設定>

nxrg100(config)#ip route 0.0.0.0/0 ppp 0

デフォルトルートを設定します。

5. <PPP アカウント設定>

nxrg100(config)#ppp account username test1@example.jp password test1pass

ppp0 インタフェースで使用する IPv4 ISP 接続用ユーザ 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 ppp0 インタフェースの設定で利用します。

6. <WAN 側(ppp0)インタフェース設定>

nxrg100(config)#interface ppp 0

nxrg100(config-ppp)#ip address negotiated

ppp0 インタフェースの IPv4 アドレスが動的 IP アドレスの場合は、negotiated を設定します。

(1957) IP アドレスに negotiated を設定した場合は、プロバイダ等から払い出された IP アドレス(IPCP で取得した IP アドレス)を利用します。

nxrg100(config-ppp)#ip masquerade

nxrg100(config-ppp)#ip spi-filter

nxrg100(config-ppp)#ip tcp adjust-mss auto

IP マスカレード、ステートフルパケットインスペクションを有効に設定します。また、IPv4 TCP MSS の 調整機能をオートに設定します。

nxrg100(config-ppp)#ppp username test1@example.jp

IPv4 ISP 接続用ユーザ ID を設定します。

7. <ethernet1 インタフェース設定>

nxrg100(config)#interface ethernet 1

nxrg100(config-if)#no ip address

nxrg100(config-if)#pppoe-client ppp 0

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

8. <DNS 設定>

nxrg100(config)#dns

nxrg100(config-dns)#service enable

DNS サービスを有効にします。

9. <ファストフォワーディングの有効化>

nxrg100(config)#fast-forwarding enable

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

(☞) ファストフォワーディングの詳細および利用時の制約については、NXR, WXR シリーズのユーザーズ

ガイド(CLI版)に記載されているファストフォワーディングの解説をご参照ください。

【端末の設定例】

	アドレス	
TD 4	サブネットマスク	DHCP サーバから取得
IPv4	デフォルトゲートウェイ	DHCFリーハから取付
	DNS サーバ	
	プレフィックス	NGN 網から取得
IPv6	アドレス	プレフィックス情報を元に自動生成
IPVO	デフォルトゲートウェイ	NGN 網から取得
	DNS サーバ	INGN 桐かり SAX1分

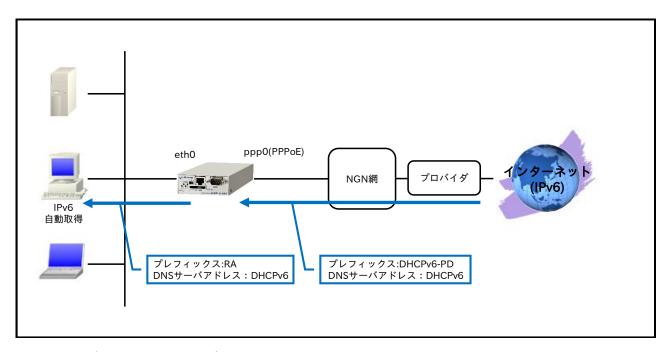
2. IPv6 PPPoE 設定

- 2-1. IPv6 PPPoE 接続設定
- 2-2. IPv4+IPv6 PPPoE 接続設定

2-1. IPv6 PPPoE 接続設定

NTT 東日本/西日本が提供するフレッツ光ネクスト回線を利用して IPv6 PPPoE によるインターネット接続を行います。

【構成図】



- ・ IPv6 プレフィックスおよび DNS サーバアドレスは DHCPv6 で取得します。
- ・ ルータ配下の端末に IPv6 プレフィックスは RA で DNS サーバアドレスは DHCPv6 で広告します。
- ・ IPv6 インターネット接続と NGN 網内の IPv6 サービスを同時に利用することはできません。

【設定データ】

設定項目			設定内容	
	ethernet0 の IPv4 アドレ	無効		
	ethernet0のIPv6アドレス	dhcpv6pd ::1/64		
LAN 側インタフェース	RA 送信	RA 送信		
	O フラグ(other-config-flag	g)	有効	
	DHCPv6 サーバ	サーバ名	ipv6dhcps	
	PPPoE クライアント(ethe	rnet1)	ppp0	
	ppp0 の IPv4 アドレス		無効	
	IPCP	無効		
	IPv6CP	有効		
┃ ┃ WAN 側インタフェース	DHCPv6 クライアント	クライアント名	ipv6dhcpc	
WAN 側インタフェース	IPv6 アクセスグループ	in	ppp0_in	
	IPv6 SPI フィルタ		有効	
	IPv6 MSS 自動調整	IPv6 MSS 自動調整		
	ISP 接続用ユーザ ID	ISP 接続用ユーザ ID		
	ISP 接続用パスワード	ISP 接続用パスワード		
スタティックルート	宛先 IPv6 アドレス	宛先 IPv6 アドレス		
\(\frac{1}{2}\) \(\frac{1}2\) \(\frac{1}{2}\) \(\frac{1}2\) \(\frac{1}2\) \(\frac{1}2\) \(\frac{1}2\) \(\frac\	ゲートウェイ(インタフェー	-ス)	ppp0	
IPv6 フィルタ	ルール名		ppp0_in	
11 10 7 1 1/2	ppp0_in	動作	許可	

		送信元 IPv6 アドレス	any
		宛先 IPv6 アドレス	any
		プロトコル	UDP
		送信元ポート	any
		宛先ポート	546
	名前		ipv6dhcps
DHCPv6 サーバ	option-send		DNS サーバ
	DNS サーバ	IPv6 アドレス	DHCPv6 取得プレフィックス::1
	名前		ipv6dhcpc
DHCPv6 クライアント	ia-pd	名前	dhcpv6pd
	option-request		DNS サーバ
DMC	サービス		有効
DNS	EDNS		有効

【設定例】

```
nxrg100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg100(config)#ipv6 dhcp-client ipv6dhcpc
nxrg100(config-dhcp6c)#ia-pd dhcpv6pd
nxrg100(config-dhcp6c)#option-request dns-servers
nxrg100(config-dhcp6c)#exit
nxrg100(config)#ipv6 dhcp-server ipv6dhcps
nxrg100(config-dhcp6s)#option-send dns-server address [DHCPv6 で取得したプレフィックス::1]
nxrg100(config-dhcp6s)#exit
nxrg100(config)#interface ethernet 0
nxrg100(config-if)#no ip address
nxrg100(config-if)#ipv6 address dhcpv6pd ::1/64
nxrg100(config-if)#ipv6 nd send-ra
nxrg100(config-if)#ipv6 nd other-config-flag
nxrg100(config-if)#ipv6 dhcp server ipv6dhcps
nxrg100(config-if)#exit
nxrg100(config)#ipv6 route ::/0 ppp 0
nxrg100(config)#ipv6 access-list ppp0_in permit any any udp any 546
nxrg100(config)#ppp account username test1@v6.example.jp password test1pass
nxrg100(config)#interface ppp 0
nxrg100(config-ppp)#no ip address
nxrg100(config-ppp)#no ppp ipcp enable
nxrg100(config-ppp)#ppp ipv6cp enable
nxrg100(config-ppp)#ipv6 dhcp client ipv6dhcpc
nxrg100(config-ppp)#ipv6 access-group in ppp0_in
nxrg100(config-ppp)#ipv6 spi-filter
nxrg100(config-ppp)#ipv6 tcp adjust-mss auto
nxrg100(config-ppp)#ppp username test1@v6.example.jp
nxrg100(config-ppp)#exit
nxrg100(config)#interface ethernet 1
nxrg100(config-if)#no ip address
nxrg100(config-if)#pppoe-client ppp 0
nxrg100(config-if)#exit
nxrg100(config)#dns
nxrg100(config-dns)#service enable
nxrg100(config-dns)#edns-query enable
nxrg100(config-dns)#exit
nxrg100(config)#exit
nxrg100#save config
```

【 設定例解説 】

1. <DHCPv6 クライアント設定>

nxrg100(config)#ipv6 dhcp-client ipv6dhcpc

DHCPv6 クライアント設定の名前を定義します。

nxrg100(config-dhcp6c)#ia-pd dhcpv6pd

Identity Association for Prefix Delegation(IAPD)を有効にし IPv6 プレフィックスの名前を定義します。

nxrg100(config-dhcp6c)#**option-request dns-servers**

DHCPv6 サーバに対して DNS サーバアドレスの通知を要求するように設定します。

2. <DHCPv6 サーバ設定>

nxrg100(config)#ipv6 dhcp-server ipv6dhcps

DHCPv6 サーバ設定の名前を定義します。

nxrg100(config-dhcp6s)#option-send dns-server address [DHCPv6 で取得したプレフィックス::1]

DHCPv6 Reply 送信時に、DNS サーバアドレスを通知するように設定します。

(☞) この設定例では DNS サーバアドレスにルータの LAN 側 IPv6 アドレスを固定で設定しています。

3. <LAN 側(ethernet0)インタフェース設定>

nxrg100(config) # interface ethernet 0

nxrg100(config-if)#no ip address

ethernet0 インタフェースの IPv4 アドレスを無効にします。

(m) この設定例では IPv6 のみの利用を想定しています。

nxrg100(config-if)#ipv6 address dhcpv6pd ::1/64

ethernet0 インタフェースの IPv6 アドレスを設定します。

(**PP)** DHCPv6 クライアントで取得した IPv6 プレフィックスを使用し、プレフィックス以降は::1/64 とします。

nxrg100(config-if)#ipv6 nd send-ra

IPv6 RA(Router Advertisement)を送信するように設定します。

nxrg100(config-if)#ipv6 nd other-config-flag

RA パケットの O フラグ(other-config-flag)を設定します。

nxrg100(config-if)#ipv6 dhcp server ipv6dhcps

DHCPv6 サーバ名を指定し、DHCPv6 サーバを有効に設定します。

4. <スタティックルート設定>

nxrg100(config)#ipv6 route ::/0 ppp 0

IPv6 デフォルトルートを設定します。

5. <IPv6 アクセスリスト設定>

nxrg100(config)#ipv6 access-list ppp0_in permit any any udp any 546

IPv6 アクセスリスト名を ppp0_in とし、宛先 UDP ポート 546 番(DHCPv6 クライアント)を許可します。 なお、この IPv6 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。

(F) IPv6 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。

6. <PPP アカウント設定>

nxrg100(config)#ppp account username test1@v6.example.jp password test1pass

ppp0 インタフェースで使用する IPv6 ISP 接続用ユーザ ID,パスワードを設定します。

(F) 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。

7. <WAN 側(ppp0)インタフェース設定>

nxrg100(config)#interface ppp 0 nxrg100(config-ppp)#no ip address

ppp0 インタフェースの IPv4 アドレスを無効に設定します。

nxrg100(config-ppp)#no ppp ipcp enable

IPCP を無効に設定します。

nxrg100(config-ppp)#ppp ipv6cp enable

IPv6CP を有効に設定します。

nxrg100(config-ppp)#ipv6 dhcp client ipv6dhcpc

DHCPv6 クライアント名を指定し、DHCPv6 クライアントを有効にします。

nxrg100(config-ppp)#ipv6 access-group in ppp0_in

IPv6 アクセスリスト ppp0_in を in フィルタに適用します。

nxrg100(config-ppp)#ipv6 spi-filter

IPv6 ステートフルパケットインスペクションを有効に設定します。

nxrg100(config-ppp)#ipv6 tcp adjust-mss auto

IPv6 TCP MSS の調整機能をオートに設定します。

nxrg100(config-ppp)#ppp username test1@v6.example.jp

IPv6 ISP 接続用ユーザ ID を設定します。

8. <ethernet1 インタフェース設定>

nxrg100(config)#interface ethernet 1

nxrg100(config-if)#no ip address

nxrg100(config-if)#pppoe-client ppp 0

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

9. <DNS 設定>

nxrg100(config)#**dns** nxrg100(config-dns)#**service enable**

DNS サービスを有効にします。

nxrg100(config-dns)#edns-query enable

EDNS を有効にします。

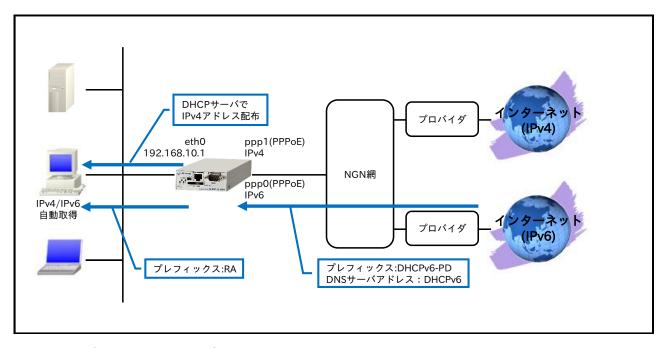
【端末の設定例】

	プレフィックス	ルータから RA で取得
IDG	アドレス	プレフィックス情報を元に自動生成
IPv6	デフォルトゲートウェイ	ルータから RA で取得
	DNS サーバ	ルータから DHCPv6 で取得

2-2. IPv4+IPv6 PPPoE 接続設定

NTT 東日本/西日本が提供するフレッツ光ネクスト回線で IPv4 および IPv6 の PPPoE を同時に接続します。これにより IPv4 および IPv6 のインターネットを同時に利用することができます。

【構成図】



- ・ IPv6 プレフィックスおよび DNS サーバアドレスは DHCPv6 で取得します。
- ・ ルータ配下の端末に対して IPv4 アドレスは DHCP で配布します。また IPv6 プレフィックスは RA で広告します。
 - (F) この設定例では IPv6 の DNS サーバアドレスを広告しません。
- ・ IPv6 インターネット接続と NGN 網内の IPv6 サービスを同時に利用することはできません。

【設定データ】

	設定内容			
	ethernet0のIPv4アド	192.168.10.1/24		
LAN 側インタフェース	ethernet0 の IPv6 アドレス			dhcpv6pd ::1/64
	RA 送信			有効
	PPPoE クライアント(ethernet1)			ppp0,ppp1
	ppp0 インタフェース	ppp0の IPv4 アド	レス	無効
	(IPv6 側)	IPCP		無効
		IPv6CP		有効
		DHCPv6 クライ	クライアント名	ipv6dhcpc
		アント		
WAN 側インタフェース		IPv6 アクセスグ	in	ppp0_in
		ループ		
		IPv6 SPI フィルタ IPv6 MSS 自動調整 IPv6 ISP 接続用ユーザ ID		有効
				オート
				test1@v6.example.jp
		IPv6 ISP 接続用パスワード		test1pass
	ppp1 インタフェース	ppp1のIPv4アド	レス	動的 IP アドレス

	(IPv4 側)	IP マスカレード	有効
		IPv4 SPI フィルタ	有効
		IPv4 MSS 自動調整	オート
		IPv4 ISP 接続用ユーザ ID	test1@example.jp
		IPv4 ISP 接続用パスワード	test1pass
	No.1	宛先 IPv6 アドレス	::/0
 スタティックルート	100.1	ゲートウェイ(インタフェース)	ppp0
	No 9	宛先 IPv4 アドレス	0.0.0.0/0
	No.2	ゲートウェイ(インタフェース)	ppp1
	ルール名	•	ppp0_in
		動作	許可
	ppp0_in	送信元 IPv6 アドレス	any
IPv6 フィルタ		宛先 IPv6 アドレス	any
		プロトコル	UDP
		送信元ポート	any
		宛先ポート	546
	名前	•	ipv6dhcpc
DHCPv6 クライアント	ia-pd	名前	dhcpv6pd
	option-request		DNS サーバ
	IPv4 アドレス払い出し範囲(始点)		192.168.10.200
DHCP サーバ	IPv4 アドレス払い出し範囲(終点)		192.168.10.210
	ゲートウェイ		192.168.10.1
	プライマリ DNS サーバ		192.168.10.1
DMC	サービス		有効
DNS	EDNS		有効
FastFowarding	•		有効

【設定例】

```
nxrg100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg100(config)#ipv6 dhcp-client ipv6dhcpc
nxrg100(config-dhcp6c)#ia-pd dhcpv6pd
nxrg100(config-dhcp6c)#option-request dns-servers
nxrg100(config-dhcp6c)#exit
nxrg100(config)#interface ethernet 0
nxrg100(config-if)#ip address 192.168.10.1/24
nxrg100(config-if)#ipv6 address dhcpv6pd ::1/64
nxrg100(config-if)#ipv6 nd send-ra
nxrg100(config-if)#exit
nxrg100(config)#dhcp-server 1
nxrg100(config-dhcps)#network 192.168.10.0/24 range 192.168.10.200 192.168.10.210
nxrg100(config-dhcps)#gateway 192.168.10.1
nxrg100(config-dhcps)#dns-server 192.168.10.1
nxrg100(config-dhcps)#exit
nxrg100(config)#ipv6 route ::/0 ppp 0
nxrg100(config)#ip route 0.0.0.0/0 ppp 1
nxrg100(config)#ipv6 access-list ppp0_in permit any any udp any 546
nxrg100(config)#ppp account username test1@v6.example.jp password test1pass
nxrg100(config)#ppp account username test1@example.jp password test1pass
nxrg100(config)#interface ppp 0
nxrg100(config-ppp)#no ip address
nxrg100(config-ppp)#no ppp ipcp enable
nxrg100(config-ppp)#ppp ipv6cp enable
nxrg100(config-ppp)#ipv6 dhcp client ipv6dhcpc
nxrg100(config-ppp)#ipv6 access-group in ppp0_in
nxrg100(config-ppp)#ipv6 spi-filter
nxrg100(config-ppp)#ipv6 tcp adjust-mss auto
nxrg100(config-ppp)#ppp username test1@v6.example.jp
nxrg100(config-ppp)#exit
nxrg100(config)#interface ppp 1
```

nxrg100(config-ppp)#ip address negotiated nxrg100(config-ppp)#ip masquerade nxrg100(config-ppp)#ip spi-filter nxrg100(config-ppp)#ip tcp adjust-mss auto nxrg100(config-ppp)#ppp username test1@example.jp nxrg100(config-ppp)#exit nxrg100(config)#interface ethernet 1 nxrg100(config-if)#no ip address nxrg100(config-if)#pppoe-client ppp 0 nxrg100(config-if)#pppoe-client ppp 1 nxrg100(config-if)#exit nxrg100(config)#dns nxrg100(config-dns)#service enable nxrg100(config-dns)#edns-query enable nxrg100(config-dns)#exit nxrg100(config)#fast-forwarding enable nxrg100(config)#exit

【設定例解説】

nxrg100#save config

1. <DHCPv6 クライアント設定>

nxrg100(config)#ipv6 dhcp-client ipv6dhcpc

DHCPv6 クライアント設定の名前を定義します。

nxrg100(config-dhcp6c)#ia-pd dhcpv6pd

Identity Association for Prefix Delegation(IAPD)を有効にし IPv6 プレフィックスの名前を定義します。

nxrg100(config-dhcp6c)#option-request dns-servers

DHCPv6 サーバに対して DNS サーバアドレスの通知を要求するように設定します。

2. <LAN 側(ethernet0)インタフェース設定>

nxrg100(config)#interface ethernet 0

nxrg100(config-if)#ip address 192.168.10.1/24

ethernet0 インタフェースの IPv4 アドレスを設定します。。

nxrg100(config-if)#ipv6 address dhcpv6pd ::1/64

ethernet0 インタフェースの IPv6 アドレスを設定します。

(**IPF**) DHCPv6 クライアントで取得した IPv6 プレフィックスを使用し、プレフィックス以降は::1/64 とします。

nxrg100(config-if)#ipv6 nd send-ra

IPv6 RA(Router Advertisement)を送信するように設定します。

3. <DHCP サーバ設定>

nxrg100(config)#dhcp-server 1

nxrg100(config-dhcps)#network 192.168.10.0/24 range 192.168.10.200 192.168.10.210

nxrg100 (config-dhcps) # gateway 192.168.10.1

nxrg100(config-dhcps)#dns-server 192.168.10.1

DHCP サーバのサーバナンバを1とし、配布する IPv4 アドレス情報を設定します。

4. <スタティックルート設定>

nxrg100(config)#ipv6 route ::/0 ppp 0

IPv6 デフォルトルートを設定します。

nxrg100(config)#ip route 0.0.0.0/0 ppp 1

IPv4 デフォルトルートを設定します。

5. <IPv6 アクセスリスト設定>

nxrg100(config)#ipv6 access-list ppp0_in permit any any udp any 546

IPv6 アクセスリスト名を ppp0_in とし、宛先 UDP ポート 546 番(DHCPv6 クライアント)を許可します。 なお、この IPv6 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。

(**☞**) IPv6 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。

6. <PPP アカウント設定>

nxrg100(config)#ppp account username test1@v6.example.jp password test1pass

ppp0 インタフェースで使用する IPv6 ISP 接続用ユーザ ID,パスワードを設定します。

(F) 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。

nxrg100(config)#ppp account username test1@example.jp password test1pass

ppp1 インタフェースで使用する IPv4 ISP 接続用ユーザ 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 ppp1 インタフェースの設定で利用します。

7. <WAN 側(ppp0)インタフェース設定>

nxrg100(config)#interface ppp 0 nxrg100(config-ppp)#no ip address

ppp0 インタフェースの IPv4 アドレスを無効に設定します。

nxrg100(config-ppp)#no ppp ipcp enable

IPCP を無効に設定します。

nxrg100(config-ppp)#ppp ipv6cp enable

IPv6CP を有効に設定します。

nxrg100(config-ppp)#ipv6 dhcp client ipv6dhcpc

DHCPv6 クライアント名を指定し、DHCPv6 クライアントを有効にします。

nxrg100(config-ppp)#ipv6 access-group in ppp0_in

IPv6 アクセスリスト ppp0_in を in フィルタに適用します。

nxrg100(config-ppp)#ipv6 spi-filter

IPv6 ステートフルパケットインスペクションを有効に設定します。

nxrg100(config-ppp)#ipv6 tcp adjust-mss auto

IPv6 TCP MSS の調整機能をオートに設定します。

nxrg100(config-ppp)#ppp username test1@v6.example.jp

IPv6 ISP 接続用ユーザ ID を設定します。

8. <WAN 側(ppp1)インタフェース設定>

nxrg100(config)#interface ppp 1

nxrg100(config-ppp)#ip address negotiated

ppp1 インタフェースの IPv4 アドレスが動的 IP アドレスの場合は、negotiated を設定します。

nxrg100(config-ppp)#ip masquerade

nxrg100(config-ppp)#ip spi-filter

nxrg100(config-ppp)#ip tcp adjust-mss auto

IP マスカレード、ステートフルパケットインスペクションを有効に設定します。また、IPv4 TCP MSS の調整機能をオートに設定します。

nxrg100(config-ppp)#ppp username test1@example.jp

IPv4 ISP 接続用ユーザ ID を設定します。

9. <ethernet1 インタフェース設定>

nxrg100(config)#interface ethernet 1

nxrg100(config-if)#no ip address

nxrg100(config-if)#pppoe-client ppp 0

nxrg100(config-if)#pppoe-client ppp 1

PPPoE クライアントとして ppp0,ppp1 インタフェースを使用できるように設定します。

10. <DNS 設定>

nxrg100(config)#dns

nxrg100(config-dns)#service enable

DNS サービスを有効にします。

nxrg100(config-dns)#edns-query enable

EDNS を有効にします。

11. <ファストフォワーディングの有効化>

nxrg100(config)#fast-forwarding enable

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

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

【端末の設定例】

	アドレス		
IPv4 サブネットマスク デフォルトゲートウェイ DNS サーバ	サブネットマスク	DHCP サーバから取得	
	リカロアリーハから取付		
	DNS サーバ		
	プレフィックス	ルータから RA で取得	
IPv6	アドレス	プレフィックス情報を元に自動生成	
	デフォルトゲートウェイ	ルータから RA で取得	

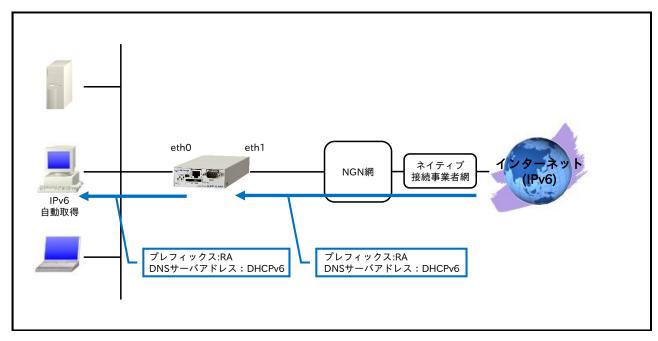
3. IPv6 IPoE 設定

- 3-1. IPv6 IPoE(RA)接続設定
- 3-2. IPv6 IPoE(DHCPv6-PD)接続設定
- 3-3. IPv4 PPPoE+IPv6 IPoE(RA)接続設定
- 3-4. IPv4 PPPoE+IPv6 IPoE(DHCPv6-PD)接続設定

3-1. IPv6 IPoE(RA)接続設定

NTT 東日本/西日本が提供するフレッツ光ネクスト回線で IPv6 IPoE によるインターネット接続を行います。なお、この設定例ではひかり電話契約なしの場合を想定しています。

【構成図】



- ・ ひかり電話契約なしの場合、IPv6 プレフィックスは RA で DNS サーバアドレスは DHCPv6 で取得します。
- ・ ルータ配下の端末に IPv6 プレフィックスは RA で DNS サーバアドレスは DHCPv6 で広告します。

【設定データ】

設定項目			設定内容	
	ethernet0 0	ethernet0 の IPv4 アドレス		無効
	ethernet0	D IPv6 アドレン	自動設定	
LAN 側インタフェース	RA 送信			有効
	O フラグ(ot	her-config-flag	g)	有効
	DHCPv6 サ	ーバ	サーバ名	ipv6dhcps
	ethernet1	D IPv4 アドレン	ス	無効
	RA プロキシ	/		有効(ethernet0)
WAN 側インタフェース	DHCPv6 クライアント		クライアント名	ipv6dhcpc
	IPv6 アクセスグループ in		in	eth1_in
	IPv6 SPI フィルタ			有効
	ルール名			eth1_in
			動作	許可
		No.1	送信元 IPv6 アドレス	any
		110.1	宛先 IPv6 アドレス	any
IPv6 フィルタ	oth 1 in		プロトコル	ICMPv6
	eth1_in		動作	許可
	No.2	No 2	送信元 IPv6 アドレス	any
		100.2	宛先 IPv6 アドレス	any
			プロトコル	UDP

		送信元ポート	any
		宛先ポート	546
	名前		ipv6dhcps
DHCPv6 サーバ	option-send		DNS サーバ
	DNS サーバ	取得インタフェース	ethernet1
	名前		ipv6dhcpc
DHCPv6 クライアント	information-only		有効
	option-request		DNS サーバ
DNS	サービス		有効
DING	EDNS		有効

【設定例】

nxrg100#configure terminal Enter configuration commands, one per line. End with CNTL/Z. nxrg100(config)#ipv6 dhcp-client ipv6dhcpc nxrg100(config-dhcp6c)#information-only enable nxrg100(config-dhcp6c)#option-request dns-servers nxrg100(config-dhcp6c)#exit nxrg100(config)#ipv6 dhcp-server ipv6dhcps nxrg100(config-dhcp6s)#option-send dns-server add dhcp-client ethernet 1 nxrg100(config-dhcp6s)#exit nxrg100(config)#interface ethernet 0 nxrg100(config-if)#no ip address nxrg100(config-if)#ipv6 address autoconfig nxrg100(config-if)#ipv6 nd send-ra nxrg100(config-if)#ipv6 nd other-config-flag nxrg100(config-if)#ipv6 dhcp server ipv6dhcps nxrg100(config-if)#exit nxrg100(config)#ipv6 access-list eth1_in permit any any icmpv6 nxrg100(config)#ipv6 access-list eth1_in permit any any udp any 546 nxrg100(config)#interface ethernet 1 nxrg100(config-if)#no ip address nxrg100(config-if)#ipv6 nd accept-ra proxy ethernet 0 nxrg100(config-if)#ipv6 dhcp client ipv6dhcpc nxrg100(config-if)#ipv6 access-group in eth1_in nxrg100(config-if)#ipv6 spi-filter nxrg100(config-if)#exit nxrg100(config)#dns nxrg100(config-dns)#service enable nxrg100(config-dns)#edns-query enable nxrg100(config-dns)#exit nxrg100(config)#exit nxrg100#save config

【 設定例解説 】

1. <DHCPv6 クライアント設定>

nxrg100(config)#ipv6 dhcp-client ipv6dhcpc

DHCPv6 クライアント設定の名前を定義します。

nxrg100 (config-dhcp6c) # information-only enable

information-only 機能を有効に設定します。

nxrg100(config-dhcp6c)#option-request dns-servers

DHCPv6 サーバに対して DNS サーバアドレスの通知を要求するように設定します。

2. <DHCPv6 サーバ設定>

nxrg100(config)#ipv6 dhcp-server ipv6dhcps

DHCPv6 サーバ設定の名前を定義します。

nxrg100(config-dhcp6s)#option-send dns-server add dhcp-client ethernet 1

DHCPv6 Reply 送信時に、DNS サーバアドレスを通知するように設定します。

(☞) この設定例では DHCPv6 クライアントで取得した DNS サーバアドレスを広告します。

3. <LAN 側(ethernet0)インタフェース設定>

nxrg100(config)#interface ethernet 0 nxrg100(config-if)#no ip address

ethernet0 インタフェースの IPv4 アドレスを無効にします。

(F) この設定例では IPv6 のみの利用を想定しています。

nxrg100(config-if)#ipv6 address autoconfig

ethernet0 インタフェースの IPv6 アドレスを設定します。

nxrg100(config-if)#ipv6 nd send-ra

IPv6 RA(Router Advertisement)を送信するように設定します。

nxrg100(config-if)#ipv6 nd other-config-flag

RA パケットの O フラグ(other-config-flag)を設定します。

nxrg100(config-if)#ipv6 dhcp server ipv6dhcps

DHCPv6 サーバ名を指定し、DHCPv6 サーバを有効に設定します。

4. <IPv6 アクセスリスト設定>

nxrg100(config)#ipv6 access-list eth1_in permit any any icmpv6

nxrg100(config)#ipv6 access-list eth1_in permit any any udp any 546

IPv6 アクセスリスト名を eth1_in とし、ICMPv6 および宛先 UDP ポート 546 番(DHCPv6 クライアント) を許可します。

なお、この IPv6 アクセスリスト設定は ethernet1 インタフェース設定で登録します。

(**☞**) IPv6 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。

5. <WAN 側(ethernet1)インタフェース設定>

nxrg100(config)#interface ethernet 1

nxrg100(config-if)#no ip address

ethernet1 インタフェースの IPv4 アドレスを無効に設定します。

nxrg100(config-if)#ipv6 nd accept-ra proxy ethernet 0

RA プロキシを有効に設定します。

(IFF) RA プロキシは受信した RA パケット内のプレフィックス情報を指定したインタフェースに対して代理で送信する機能です。

nxrg100(config-if)#ipv6 dhcp client ipv6dhcpc

DHCPv6 クライアント名を指定し、DHCPv6 クライアントを有効にします。

nxrg100(config-if)#ipv6 access-group in eth1_in

IPv6 アクセスリスト eth1 in を in フィルタに適用します。

nxrg100(config-if)#ipv6 spi-filter

IPv6 ステートフルパケットインスペクションを有効に設定します。

6. <DNS 設定>

nxrg100 (config) # dns

nxrg100(config-dns)#service enable

DNS サービスを有効にします。

nxrg100(config-dns)#edns-query enable

EDNS を有効にします。

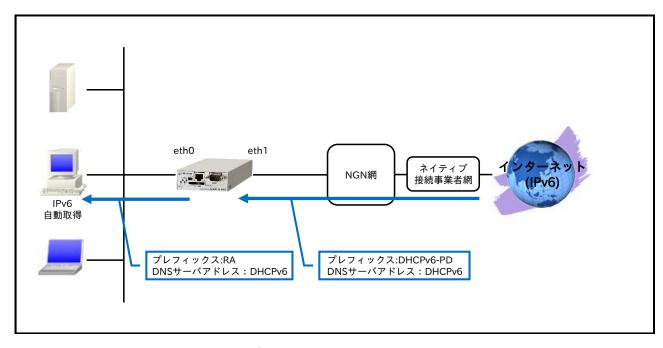
【端末の設定例】

	プレフィックス	ルータから RA で取得
IPv6	アドレス	プレフィックス情報を元に自動生成
11700	デフォルトゲートウェイ	ルータから RA で取得
	DNS サーバ	ルータから DHCPv6 で取得

3-2. IPv6 IPoE(DHCPv6-PD)接続設定

NTT 東日本/西日本が提供するフレッツ光ネクスト回線で IPv6 IPoE によるインターネット接続を行います。なお、この設定例ではひかり電話契約ありの場合を想定しています。

【構成図】



- ・ ひかり電話契約ありの場合 IPv6 プレフィックス、DNS サーバアドレスは DHCPv6 で取得します。
- ・ ルータ配下の端末に IPv6 プレフィックスは RA で DNS サーバアドレスは DHCPv6 で広告します。

【 設定データ 】

	設定内容			
	ethernet0 の IPv4 アドレス		無効	
	ethernet0のIPv6アドレス			dhcpv6pd ::/64 eui-64
LAN 側インタフェース	RA 送信			有効
	O フラグ(other-config-flag)		有効	
	DHCPv6 サ	ーバ	サーバ名	ipv6dhcps
	ethernet1	D IPv4 アドレ	ス	無効
	RA 受信			有効
WAN 側インタフェース	DHCPv6 クライアント		クライアント名	ipv6dhcpc
	IPv6 アクセスグループ		in	eth1_in
	IPv6 SPI フィルタ		有効	
	ルール名			eth1_in
		No.1	動作	許可
			送信元 IPv6 アドレス	any
			宛先 IPv6 アドレス	any
			プロトコル	ICMPv6
IPv6 フィルタ	oth 1 in		動作	許可
	eth1_in		送信元 IPv6 アドレス	any
		No.2	宛先 IPv6 アドレス	any
			プロトコル	UDP
			送信元ポート	any
			宛先ポート	546

	名前		ipv6dhcps
DHCPv6 サーバ	option-send		DNS サーバ
	DNS サーバ	取得インタフェース	ethernet1
	名前		ipv6dhcpc
DHCPv6 クライアント	ia-pd	名前	dhcpv6pd
	option-request		DNS サーバ
DNS	サービス		有効
	EDNS		有効

【設定例】

nxrg100#configure terminal Enter configuration commands, one per line. End with CNTL/Z. nxrg100(config)#ipv6 dhcp-client ipv6dhcpc nxrg100(config-dhcp6c)#ia-pd dhcpv6pd nxrg100(config-dhcp6c)#option-request dns-servers nxrg100(config-dhcp6c)#exit nxrg100(config)#ipv6 dhcp-server ipv6dhcps nxrg100(config-dhcp6s)#option-send dns-server add dhcp-client ethernet 1 nxrg100(config-dhcp6s)#exit nxrg100(config)#interface ethernet 0 nxrg100(config-if)#no ip address nxrg100(config-if)#ipv6 address dhcpv6pd ::/64 eui-64 nxrg100(config-if)#ipv6 nd send-ra nxrg100(config-if)#ipv6 nd other-config-flag nxrg100(config-if)#ipv6 dhcp server ipv6dhcps nxrg100(config-if)#exit nxrg100(config)#ipv6 access-list eth1_in permit any any icmpv6 nxrg100(config)#ipv6 access-list eth1_in permit any any udp any 546 nxrg100(config)#interface ethernet 1 nxrg100(config-if)#no ip address nxrg100(config-if)#ipv6 nd accept-ra nxrg100(config-if)#ipv6 dhcp client ipv6dhcpc nxrg100(config-if)#ipv6 access-group in eth1_in nxrg100(config-if)#ipv6 spi-filter nxrg100(config-if)#exit nxrg100(config)#dns nxrg100(config-dns)#service enable nxrg100(config-dns)#edns-query enable nxrg100(config-dns)#exit nxrg100(config)#exit nxrg100#save config

【 設定例解説 】

1. <DHCPv6 クライアント設定>

nxrg100(config)#ipv6 dhcp-client ipv6dhcpc

DHCPv6 クライアント設定の名前を定義します。

nxrg100(config-dhcp6c)#ia-pd dhcpv6pd

Identity Association for Prefix Delegation(IAPD)を有効にし IPv6 プレフィックスの名前を定義します。

nxrg100(config-dhcp6c)#option-request dns-servers

DHCPv6 サーバに対して DNS サーバアドレスの通知を要求するように設定します。

2. <DHCPv6 サーバ設定>

nxrg100(config)#ipv6 dhcp-server ipv6dhcps

DHCPv6 サーバ設定の名前を定義します。

nxrg100(config-dhcp6s)#option-send dns-server add dhcp-client ethernet 1

DHCPv6 Reply 送信時に、DNS サーバアドレスを通知するように設定します。

(☞) この設定例では DHCPv6 クライアントで取得した DNS サーバアドレスを広告します。

3. <LAN 側(ethernet0)インタフェース設定>

nxrg100(config)#interface ethernet 0

nxrg100(config-if)#no ip address

ethernet0 インタフェースの IPv4 アドレスを無効にします。

(☞) この設定例では IPv6 のみの利用を想定しています。

nxrg100(config-if)#ipv6 address dhcpv6pd ::/64 eui-64

ethernet0 インタフェースの IPv6 アドレスを設定します。

(IFF) DHCPv6 クライアントで取得した IPv6 プレフィックスを使用し、プレフィックス以降はインタフェース ID によって自動生成します。

nxrg100(config-if)#ipv6 nd send-ra

IPv6 RA(Router Advertisement)を送信するように設定します。

nxrg100(config-if)#ipv6 nd other-config-flag

RA パケットの O フラグ(other-config-flag)を設定します。

nxrg100(config-if)#ipv6 dhcp server ipv6dhcps

DHCPv6 サーバ名を指定し、DHCPv6 サーバを有効に設定します。

4. <IPv6 アクセスリスト設定>

nxrg100(config)#ipv6 access-list eth1_in permit any any icmpv6

nxrg100(config)#ipv6 access-list eth1_in permit any any udp any 546

IPv6 アクセスリスト名を eth1_in とし、ICMPv6 および宛先 UDP ポート 546 番(DHCPv6 クライアント) を許可します。

なお、この IPv6 アクセスリスト設定は ethernet1 インタフェース設定で登録します。

(F) IPv6 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。

5. <WAN 側(ethernet1)インタフェース設定>

nxrg100(config)#interface ethernet 1

nxrg100(config-if)#no ip address

ethernet1 インタフェースの IPv4 アドレスを無効に設定します。

nxrg100(config-if)#ipv6 nd accept-ra

RA を受信するように設定します。

nxrg100(config-if)#ipv6 dhcp client ipv6dhcpc

DHCPv6 クライアント名を指定し、DHCPv6 クライアントを有効にします。

nxrg100(config-if)#ipv6 access-group in eth1_in

IPv6 アクセスリスト eth1_in を in フィルタに適用します。

nxrg100(config-if)#ipv6 spi-filter

IPv6 ステートフルパケットインスペクションを有効に設定します。

6. <DNS 設定>

nxrg100(config)#dns

nxrg100(config-dns)#service enable

DNS サービスを有効にします。

nxrg100(config-dns)#edns-query enable

EDNS を有効にします。

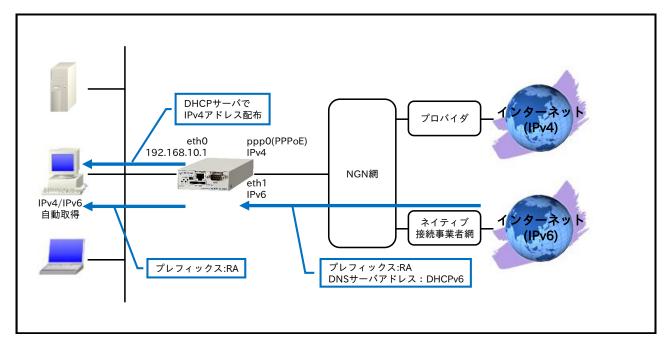
【端末の設定例】

	プレフィックス	ルータから RA で取得
IDeeG	アドレス	プレフィックス情報を元に自動生成
IPv6	デフォルトゲートウェイ	ルータから RA で取得
	DNS サーバ	ルータから DHCPv6 で取得

3-3. IPv4 PPPoE+IPv6 IPoE(RA)接続設定

NTT 東日本/西日本が提供するフレッツ光ネクスト回線で IPv4 は PPPoE、IPv6 は IPoE を同時に接続します。これにより IPv4 および IPv6 のインターネットを同時に利用することができます。なお、この設定例ではひかり電話契約なしの場合を想定しています。

【構成図】



- ・ ひかり電話契約なしの場合、IPv6 プレフィックスは RA で、DNS サーバアドレスは DHCPv6 で取得します。
- ・ ルータ配下の端末に対して IPv4 アドレスは DHCP で配布します。IPv6 プレフィックスは RA で広告します。
 - (F) この設定例では IPv6 の DNS サーバアドレスを広告しません。

【 設定データ 】

設定項目				設定内容
	ethernet() の IPv4 アドレス			192.168.10.1/24
LAN 側インタフェース	ethernet0のIPv6アドレス			自動設定
	RA 送信			有効
		ethernet1のIPv4アドレス		無効
	ethernet1 インタフェース (IPv6 側)	RA プロキシ		有効(ethernet0)
		DHCPv6 クライアント	クライアント名	ipv6dhcpc
WAN 側インタフェース		IPv6 アクセスグループ	in	eth1_in
		IPv6 SPI フィルタ		有効
	PPPoE クライアント(ethernet1)			ppp0
	ppp0 インタフェース	ppp0 の IPv4 アドレス		動的 IP アドレス
	(IPv4 側)	IPマスカレード	IP マスカレード	
		IPv4 SPI フィルタ		有効

	IPv4 MSS 自動調整		オート	
		IPv4 ISP 接続用ユ	test1@example.jp	
		IPv4 ISP 接続用パスワード		test1pass
フクニュックルート	宛先 IPv4 アドレス			0.0.0.0/0
スタティックルート	ゲートウェイ(インタフ	ェース)		ppp0
	ルール名	•		eth1_in
			動作	許可
		N _a 1	送信元 IPv6 アドレス	any
		No.1	宛先 IPv6 アドレス	any
	eth1_in		プロトコル	ICMPv6
IPv6 フィルタ		No.2	動作	許可
			送信元 IPv6 アドレス	any
			宛先 IPv6 アドレス	any
			プロトコル	UDP
			送信元ポート	any
			宛先ポート	546
	名前			ipv6dhcpc
DHCPv6 クライアント	information-only			有効
	option-request			DNS サーバ
	IPv4 アドレス払い出し範囲(始点)			192.168.10.200
DHOD II	IPv4 アドレス払い出し範囲(終点)			192.168.10.210
DHCP サーバ	ゲートウェイ			192.168.10.1
	プライマリ DNS サーバ			192.168.10.1
DMC	サービス			有効
DNS	EDNS			有効
FastFowarding			有効	

【設定例】

```
nxrg100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg100(config)#ipv6 dhcp-client ipv6dhcpc
nxrg100(config-dhcp6c)#information-only enable
nxrg100(config-dhcp6c)#option-request dns-servers
nxrg100(config-dhcp6c)#exit
nxrg100(config)#interface ethernet 0
nxrg100(config-if)#ip address 192.168.10.1/24
nxrg100(config-if)#ipv6 address autoconfig
nxrg100(config-if)#ipv6 nd send-ra
nxrg100(config-if)#exit
nxrg100(config)#dhcp-server 1
nxrg100(config-dhcps)#network 192.168.10.0/24 range 192.168.10.200 192.168.10.210
nxrg100(config-dhcps)#gateway 192.168.10.1
nxrg100(config-dhcps)#dns-server 192.168.10.1
nxrg100(config-dhcps)#exit
nxrg100(config)#ip route 0.0.0.0/0 ppp 0
nxrg100(config)#ipv6 access-list eth1_in permit any any icmpv6
nxrg100(config)#ipv6 access-list eth1_in permit any any udp any 546
nxrg100(config)#ppp account username test1@example.jp password test1pass
nxrg100(config)#interface ppp 0
nxrg100(config-ppp)#ip address negotiated
nxrg100(config-ppp)#ip masquerade
nxrg100(config-ppp)#ip spi-filter
nxrg100(config-ppp)#ip tcp adjust-mss auto
nxrg100(config-ppp)#ppp username test1@example.jp
nxrg100(config-ppp)#exit
nxrg100(config)#interface ethernet 1
nxrg100(config-if)#no ip address
nxrg100(config-if)#ipv6 nd accept-ra proxy ethernet 0
nxrg100(config-if)#ipv6 dhcp client ipv6dhcpc
nxrg100(config-if)#ipv6 access-group in eth1_in
```

nxrg100(config-if)#ipv6 spi-filter

nxrg100(config-if)#pppoe-client ppp 0

nxrg100(config-if)#exit

nxrg100(config)#dns

nxrg100(config-dns)#service enable

nxrg100(config-dns)#edns-query enable

nxrg100(config-dns)#exit

nxrg100(config)#fast-forwarding enable

nxrg100(config)#exit

nxrg100#save config

【設定例解説】

1. <DHCPv6 クライアント設定>

nxrg100(config)#ipv6 dhcp-client ipv6dhcpc

DHCPv6 クライアント設定の名前を定義します。

nxrg100(config-dhcp6c)#information-only enable

information-only 機能を有効に設定します。

nxrg100(config-dhcp6c)#option-request dns-servers

DHCPv6 サーバに対して DNS サーバアドレスの通知を要求するように設定します。

2. <LAN 側(ethernet0)インタフェース設定>

nxrg100(config)#interface ethernet 0

nxrg100(config-if)#ip address 192.168.10.1/24

ethernet0 インタフェースの IPv4 アドレスを設定します。

nxrg100(config-if)#ipv6 address autoconfig

ethernet0 インタフェースの IPv6 アドレスを設定します。

nxrg100(config-if)#ipv6 nd send-ra

IPv6 RA(Router Advertisement)を送信するように設定します。

3. <DHCP サーバ設定>

nxrg100(config)#dhcp-server 1

 $nxrg100 (config-dhcps) \# network\ 192.168.10.0/24\ range\ 192.168.10.200\ 192.168.10.210$

nxrg100(config-dhcps)#gateway 192.168.10.1

nxrg100(config-dhcps)#dns-server 192.168.10.1

DHCP サーバのサーバナンバを1とし、配布する IPv4 アドレス情報を設定します。

4. <スタティックルート設定>

nxrg100(config)#ip route 0.0.0.0/0 ppp 0

IPv4 デフォルトルートを設定します。

5. <IPv6 アクセスリスト設定>

nxrg100(config)#ipv6 access-list eth1_in permit any any icmpv6 nxrg100(config)#ipv6 access-list eth1_in permit any any udp any 546

IPv6 アクセスリスト名を eth1_in とし、ICMPv6 および宛先 UDP ポート 546 番(DHCPv6 クライアント) を許可します。

なお、この IPv6 アクセスリスト設定は ethernet1 インタフェース設定で登録します。

(IP) IPv6 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。

6. <PPP アカウント設定>

nxrg100(config)#ppp account username test1@example.jp password test1pass

ppp0 インタフェースで使用する IPv4 ISP 接続用ユーザ 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 ppp0 インタフェースの設定で利用します。

7. <WAN 側(ppp0)インタフェース設定>

nxrg100(config)#interface ppp 0

nxrg100(config-ppp)#ip address negotiated

ppp0 インタフェースの IPv4 アドレスが動的 IP アドレスの場合は、negotiated を設定します。

nxrg100(config-ppp)#ip masquerade

nxrg100(config-ppp)#ip spi-filter

nxrg100(config-ppp)#ip tcp adjust-mss auto

IP マスカレード、ステートフルパケットインスペクションを有効に設定します。また、IPv4 TCP MSS の調整機能をオートに設定します。

nxrg100(config-ppp)#ppp username test1@example.jp

IPv4 ISP 接続用ユーザ ID を設定します。

8. < WAN 側(ethernet1)インタフェース設定>

nxrg100 (config) # interface ethernet 1

nxrg100(config-if)#no ip address

ethernet1 インタフェースの IPv4 アドレスを無効に設定します。

 $nxrg100(config\text{-}\mathrm{if})\text{\#}\text{ipv6}$ nd accept-ra proxy ethernet 0

RA プロキシを有効に設定します。

(☞) RA プロキシは受信した RA パケット内のプレフィックス情報を、指定したインタフェースに対して代理で送信する機能です。

nxrg100(config-if)#ipv6 dhcp client ipv6dhcpc

DHCPv6 クライアント名を指定し、DHCPv6 クライアントを有効にします。

nxrg100(config-if)#ipv6 access-group in eth1_in

IPv6 アクセスリスト eth1 in を in フィルタに適用します。

nxrg100(config-if)#ipv6 spi-filter

IPv6 ステートフルパケットインスペクションを有効に設定します。

nxrg100(config-if)#**pppoe-client ppp 0**

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

9. <DNS 設定>

nxrg100 (config) # dns

nxrg100(config-dns)#service enable

DNS サービスを有効にします。

nxrg100(config-dns)#edns-query enable

EDNS を有効にします。

10. <ファストフォワーディングの有効化>

nxrg100(config)#fast-forwarding enable

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

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

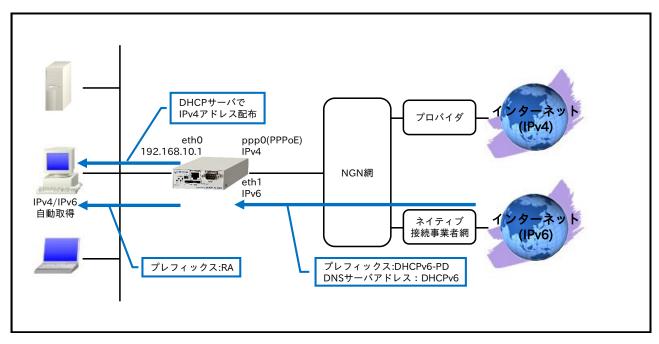
【端末の設定例】

ID4	アドレス		
	サブネットマスク	DHCP サーバから取得	
IPv4	デフォルトゲートウェイ	」」」」の以行	
	DNS サーバ		
	プレフィックス	ルータから RA で取得	
IPv6	アドレス	プレフィックス情報を元に自動生成	
	デフォルトゲートウェイ	ルータから RA で取得	

3-4. IPv4 PPPoE+IPv6 IPoE(DHCPv6-PD)接続設定

NTT 東日本/西日本が提供するフレッツ光ネクスト回線で IPv4 は PPPoE、IPv6 は IPoE を同時に接続します。これにより IPv4 および IPv6 のインターネットを同時に利用することができます。なお、この設定例ではひかり電話契約ありの場合を想定しています。

【構成図】



- ・ ひかり電話契約ありの場合 IPv6 プレフィックス、DNS サーバアドレスは DHCPv6 で取得します。
- ・ ルータ配下の端末に対して IPv4 アドレスは DHCP で配布します。IPv6 プレフィックスは RA で広告します。
 - (F) この設定例では IPv6 の DNS サーバアドレスを広告しません。。

【 設定データ 】

	設定内容			
	ethernet0 の IPv4 アドレス			192.168.10.1/24
LAN 側インタフェース	ethernet0のIPv6アドレス			dhcpv6pd ::/64 eui-64
	RA 送信			有効
		ethernet1のIPv4	アドレス	無効
	ethernet1 インタフェース (IPv6 側)	RA 受信		有効
		DHCPv6 クライアント	クライアント名	ipv6dhcpc
WANT HILLS A TO THE TOTAL TO		IPv6 アクセスグループ	in	eth1_in
WAN 側インタフェース		IPv6 SPI フィルタ		有効
	PPPoE クライアント(ethernet1)			ppp0
	ppp0 インタフェース	ppp0のIPv4アドレス		動的 IP アドレス
	(IPv4 側)	IPマスカレード		有効
		IPv4 SPI フィルタ		有効
	IPv4 MSS 自動調整		オート	

		IPv4 ISP 接続用ユ	ーザ ID	test1@example.jp
		IPv4 ISP 接続用パ		test1pass
	宛先 IPv4 アドレス	11 (1 101 32/70/13		0.0.0.0/0
スタティックルート	ゲートウェイ(インタフ	ェース)		ppp0
	ルール名	,		eth1_in
			動作	許可
		No.1	送信元 IPv6 アドレス	any
		NO.1	宛先 IPv6 アドレス	any
			プロトコル	ICMPv6
IPv6 フィルタ	eth1_in	No.2	動作	許可
			送信元 IPv6 アドレス	any
			宛先 IPv6 アドレス	any
			プロトコル	UDP
			送信元ポート	any
			宛先ポート	546
	名前	ipv6dhcpc		
DHCPv6 クライアント	ia-pd	名前		dhcpv6pd
	option-request			DNS サーバ
	IPv4 アドレス払い出し			192.168.10.200
DHCP サーバ	IPv4 アドレス払い出し	192.168.10.210		
DHCP 9-7	ゲートウェイ	192.168.10.1		
	プライマリ DNS サーノ	192.168.10.1		
DNS	サービス			有効
מאמ	EDNS			有効
FastFowarding				有効

【設定例】

nxrg100(config-if)#ipv6 spi-filter

```
nxrg100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg100(config)#ipv6 dhcp-client ipv6dhcpc
nxrg100(config-dhcp6c)#ia-pd dhcpv6pd
nxrg100(config-dhcp6c)#option-request dns-servers
nxrg100(config-dhcp6c)#exit
nxrg100(config)#interface ethernet 0
nxrg100(config-if)#ip address 192.168.10.1/24
nxrg100(config-if)#ipv6 address dhcpv6pd ::/64 eui-64
nxrg100(config-if)#ipv6 nd send-ra
nxrg100(config-if)#exit
nxrg100(config)#dhcp-server 1
nxrg100(config-dhcps)#network 192.168.10.0/24 range 192.168.10.200 192.168.10.210
nxrg100(config-dhcps)#gateway 192.168.10.1
nxrg100(config-dhcps)#dns-server 192.168.10.1
nxrg100(config-dhcps)#exit
nxrg100(config)#ip route 0.0.0.0/0 ppp 0
nxrg100(config)#ipv6 access-list eth1_in permit any any icmpv6
nxrg100(config)#ipv6 access-list eth1_in permit any any udp any 546
nxrg100(config)#ppp account username test1@example.jp password test1pass
nxrg100(config)#interface ppp 0
nxrg100(config-ppp)#ip address negotiated
nxrg100(config-ppp)#ip masquerade
nxrg100(config-ppp)#ip spi-filter
nxrg100(config-ppp)#ip tcp adjust-mss auto
nxrg100(config-ppp)#ppp username test1@example.jp
nxrg100(config-ppp)#exit
nxrg100(config)#interface ethernet 1
nxrg100(config-if)#no ip address
nxrg100(config-if)#ipv6 nd accept-ra
nxrg100(config-if)#ipv6 dhcp client ipv6dhcpc
nxrg100(config-if)#ipv6 access-group in eth1_in
```

nxrg100(config-if)#pppoe-client ppp 0

nxrg100(config-if)#exit

nxrg100(config)#dns

nxrg100(config-dns)#service enable

nxrg100(config-dns)#edns-query enable

nxrg100(config-dns)#exit

nxrg100(config)#fast-forwarding enable

nxrg100(config)#exit

nxrg100#save config

【設定例解説】

1. <DHCPv6 クライアント設定>

nxrg100(config)#ipv6 dhcp-client ipv6dhcpc

DHCPv6 クライアント設定の名前を定義します。

nxrg100(config-dhcp6c)#ia-pd dhcpv6pd

Identity Association for Prefix Delegation(IAPD)を有効にし IPv6 プレフィックスの名前を定義します。

nxrg100(config-dhcp6c)#option-request dns-servers

DHCPv6 サーバに対して DNS サーバアドレスの通知を要求するように設定します。

2. <LAN 側(ethernet0)インタフェース設定>

nxrg100(config)#interface ethernet 0

nxrg100(config-if)#ip address 192.168.10.1/24

ethernet0 インタフェースの IPv4 アドレスを設定します。

nxrg100(config-if)#ipv6 address dhcpv6pd ::/64 eui-64

ethernet0 インタフェースの IPv6 アドレスを設定します。

(**☞**) DHCPv6 クライアントで取得した IPv6 プレフィックスを使用し、プレフィックス以降はインタフェース ID によって自動生成します。

nxrg100(config-if)#ipv6 nd send-ra

IPv6 RA(Router Advertisement)を送信するように設定します。

3. <DHCP サーバ設定>

nxrg100(config)#dhcp-server 1

nxrg100(config-dhcps)#network 192.168.10.0/24 range 192.168.10.200 192.168.10.210

nxrg100(config-dhcps)#gateway 192.168.10.1

nxrg100(config-dhcps)#dns-server 192.168.10.1

DHCP サーバのサーバナンバを1とし、配布する IPv4 アドレス情報を設定します。

4. <スタティックルート設定>

nxrg100(config)#ip route 0.0.0.0/0 ppp 0

IPv4 デフォルトルートを設定します。

5. <IPv6 アクセスリスト設定>

nxrg100(config)#ipv6 access-list eth1_in permit any any icmpv6 nxrg100(config)#ipv6 access-list eth1_in permit any any udp any 546

IPv6 アクセスリスト名を eth1_in とし、ICMPv6 および宛先 UDP ポート 546 番(DHCPv6 クライアント) を許可します。

なお、この IPv6 アクセスリスト設定は ethernet1 インタフェース設定で登録します。

(IF) IPv6 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。

6. <PPP アカウント設定>

nxrg100(config)#ppp account username test1@example.jp password test1pass

ppp0 インタフェースで使用する IPv4 ISP 接続用ユーザ 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 ppp0 インタフェースの設定で利用します。

7. <WAN 側(ppp0)インタフェース設定>

nxrg100(config)#interface ppp 0

nxrg100(config-ppp)#ip address negotiated

ppp0 インタフェースの IPv4 アドレスが動的 IP アドレスの場合は、negotiated を設定します。

nxrg100(config-ppp)#ip masquerade

nxrg100(config-ppp)#ip spi-filter

nxrg100(config-ppp)#ip tcp adjust-mss auto

IP マスカレード、ステートフルパケットインスペクションを有効に設定します。また、IPv4 TCP MSS の調整機能をオートに設定します。

nxrg100(config-ppp)#ppp username test1@example.jp

IPv4 ISP 接続用ユーザ ID を設定します。

8. < WAN 側(ethernet1)インタフェース設定>

nxrg100(config)#interface ethernet 1

nxrg100(config-if)#no ip address

ethernet1 インタフェースの IPv4 アドレスを無効に設定します。

 $nxrg100 (config-if) \# \textbf{ipv6} \ \textbf{nd} \ \textbf{accept-ra}$

RA を受信するように設定します。

nxrg100(config-if)#ipv6 dhcp client ipv6dhcpc

DHCPv6 クライアント名を指定し、DHCPv6 クライアントを有効にします。

nxrg100(config-if)#ipv6 access-group in eth1_in

IPv6 アクセスリスト eth1_in を in フィルタに適用します。

nxrg100(config-if)#ipv6 spi-filter

IPv6 ステートフルパケットインスペクションを有効に設定します。

nxrg100(config-if)#pppoe-client ppp 0

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

9. <DNS 設定>

nxrg100(config)#dns

nxrg100(config-dns)#service enable

DNS サービスを有効にします。

nxrg100(config-dns)#edns-query enable

EDNS を有効にします。

10. <ファストフォワーディングの有効化>

nxrg100(config)#fast-forwarding enable

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

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

【端末の設定例】

	アドレス		
IPv4	サブネットマスク	DHCD サーバかと取得	
	デフォルトゲートウェイ	DHCP サーバから取得	
	DNS サーバ		
	プレフィックス	ルータから RA で取得	
IPv6	アドレス	プレフィックス情報を元に自動生成	
	デフォルトゲートウェイ	ルータから RA で取得	

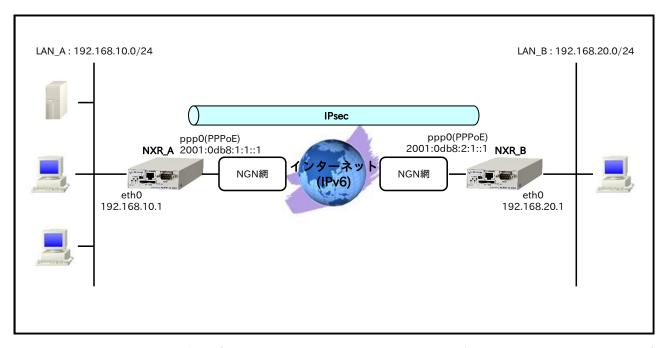
4. IPv6 IPsec 設定

- 4-1. IPv6 PPPoE IPsec 接続設定
- 4-2. IPv6 IPoE(RA)IPsec 接続設定(ネームの利用)
- 4-3. IPv6 IPoE(DHCPv6-PD)IPsec 接続設定

4-1. IPv6 PPPoE IPsec 接続設定

NTT 東日本/西日本が提供するフレッツ光ネクスト回線で IPv6 PPPoE 接続を行います。そして、それを利用して拠点間で IPv4 over IPv6 の IPsec 接続を行います。

【構成図】



- ・ ルータ NXR_A には固定でプレフィックス「2001:0db8:1:1::/56」が、ルータ NXR_B には固定でプレフィックス「2001:0db8:2:1::/56」が割り当てられるものとします。
- ・ この設定例では Route Based IPsec を利用します。
- ・ この設定例ではルータ配下の端末からインターネットへアクセスすることはできません。

【 設定データ 】

[NXR_A の設定]

	設定内容		
ホスト名	NXR_A		
LAN 側インタフェース	ethernet0のIPv4アドレス	ζ	192.168.10.1/24
	PPPoE クライアント(ether	rnet1)	ppp0
	ppp0 の IPv4 アドレス		無効
	ppp0 の IPv6 アドレス		dhcpv6pd ::1/64
	IPCP	無効	
	IPv6CP	有効	
WAN 側インタフェース	DHCPv6 クライアント (PD)	クライアント名	dhcpv6pd
	IPv6 アクセスグループ	in	ppp0_in
	IPv6 SPI フィルタ	有効	
	IPv6 TCP MSS 自動調整	オート	
	ISP 接続用ユーザ ID	test1@v6.example.jp	
	ISP 接続用パスワード	test1pass	
	IPsec ローカルポリシー		1

			宛先 IPv4 アドレス	192.168.20.0/24
	No.1		ゲートウェイ(インタフェース)	tunnel1
			ディスタンス	1
			宛先 IPv4 アドレス	192.168.20.0/24
スタティックルート	No.2	-	ゲートウェイ(インタフェース)	null
	110.2	-	ディスタンス	254
			宛先 IPv6 アドレス	::/0
	No.3	-	ゲートウェイ(インタフェース)	ppp0
	ルール名)	ppp0_in
	70 70-11		動作	許可
			送信元 IPv6 アドレス	any
			宛先 IPv6 アドレス	any
		No.1	プロトコル	UDP
			送信元ポート	any
			宛先ポート	546
			動作	許可
IPv6 フィルタ			送信元 IPv6 アドレス	2001:0db8:2:1::1
IFVO 7170X	ppp0_in		宛先 IPv6 アドレス	2001:0db8:1:1::1
		No.2	プロトコル	UDP
			送信元ポート	500
			宛先ポート	500
			動作	<u></u> 許可
			送信元 IPv6 アドレス	2001:0db8:2:1::1
		No.3		
			宛先 IPv6 アドレス プロトコル	2001:0db8:1:1::1
				50(ESP)
ID > 41.		1471171	リスト名	ipsec_acl
	IPsec アクセスリスト		送信元 IPv4 アドレス	any
	ID	ا دا با الاد	宛先 IPv4 アドレス	any
	IPsec Li —	カルポリシー1		ipv6
			名前	NXR_B
			認証方式	pre-share
			認証鍵	ipseckey
			認証アルゴリズム	sha1
			暗号化アルゴリズム	aes128
			DHグループ	5
	IPsec ISAI	KMP ポリシー1		10800秒
ID.			ISAKMP モード	メインモード
IPsec			リモートアドレス	2001:0db8:2:1::1
			再送間隔	30 秒
			DPD リトライ回数	3 回
			動作	restart
			ローカルポリシー	1
			名前	NXR_B オート
			ネゴシエーションモード	
			認証アルゴリズム	shal
	IPsec トン	ネルポリシー1	暗号化アルゴリズム	aes128
			PFS	有効(グループ 5)
			ライフタイム	3600 秒
			ISAKMP ポリシー	1
	1 1 1 2 2 2 7	1,0	IPsec アクセスリスト	ipsec_acl
1 1 2 1 1 2 1 2 2 2 2 2	トンネルモ			IPsec(IPv6)
トンネル1インタフェース		ロテクション MCC 中制調軟		ipsec policy 1
	IPV4 TCP	MSS 自動調整	オート	

〔NXR_B の設定〕

	設定内容	
ホスト名		NXR_B
LAN 側インタフェース	ethernet0のIPv4アドレス	192.168.20.1/24
WAN 側インタフェース	PPPoE クライアント(ethernet1)	ppp0
WAN 側インタフェース	ppp0のIPv4アドレス	無効

		0 : = 10 1 : =		
		v6 アドレス		dhcpv6pd ::1/64
	IPCP		無効	
	IPv6CP			有効
	DHCPv6 2 (PD)	ラライアント	dhcpv6pd	
	IPv6 アクセ	z スグループ	ppp0_in	
	IPv6 SPI 7	フィルタ	有効	
	IPv6 TCP I	MSS 自動調整	オート	
	ISP 接続用	ユーザ ID	test2@v6.example.jp	
	ISP 接続用	パスワード	test2pass	
	IPsec □ —	カルポリシー		1
			宛先 IPv4 アドレス	192.168.10.0/24
	No.1		ゲートウェイ(インタフェース)	tunnel1
			ディスタンス	1
 スタティックルート			宛先 IPv4 アドレス	192.168.10.0/24
	No.2		ゲートウェイ(インタフェース)	null
			ディスタンス	254
	No.3		宛先 IPv6 アドレス	::/0
			ゲートウェイ(インタフェース)	ppp0
	ルール名			ppp0_in
			動作	許可
			送信元 IPv6 アドレス	any
		No.1	宛先 IPv6 アドレス	any
		110.1	プロトコル	UDP
			送信元ポート	any
			宛先ポート	546
			動作	許可
IPv6 フィルタ	ppp0_in		送信元 IPv6 アドレス	2001:0db8:1:1::1
		No.2	宛先 IPv6 アドレス	2001:0db8:2:1::1
			プロトコル	UDP
			送信元ポート	500
			宛先ポート	500
			動作	許可
		No.3	送信元 IPv6 アドレス	2001:0db8:1:1::1
			宛先 IPv6 アドレス プロトコル	2001:0db8:2:1::1
			リスト名	50(ESP)
	IPsec アク	レフ ロフ ト	送信元 IPv4 アドレス	ipsec_acl
	IFSEC 7.9	セスリスト	宛先 IPv4 アドレス	any
	IPcoc II -	カルポリシー1		ipv6
	11 200 11	747447 Z - 1	名前	NXR_A
			認証方式	pre-share
			認証鍵	ipseckey
			認証アルゴリズム	shal
			暗号化アルゴリズム	aes128
			DH グループ	5
	IPsec ISAF	KMP ポリシー		10800 秒
			ISAKMP モード	メインモード
IPsec			リモートアドレス	2001:0db8:1:1::1
			再送間隔	30 秒
			DPD リトライ回数	3回
			動作	restart
			ローカルポリシー	1
			名前	NXR_A
			ネゴシエーションモード	オート
			認証アルゴリズム	sha1
	IPsec by	ネルポリシー1	暗号化アルゴリズム	aes128
		1,7-4-7 2	PFS	有効(グループ 5)
			ライフタイム	3600 秒
			ISAKMP ポリシー	1
	1	10	IPsec アクセスリスト	ipsec_acl
トンネル1インタフェース	トンネルモ	ード		IPsec(IPv6)

トンネルプロテクション	ipsec policy 1
IPv4 TCP MSS 自動調整	オート

【設定例】

〔NXR_A の設定〕

NXR_A(config-ppp)#ipsec policy 1

NXR_A(config-ppp)#exit

nxrg100#configure terminal Enter configuration commands, one per line. End with CNTL/Z. nxrg100(config)#hostname NXR_A NXR_A(config)#interface ethernet 0 NXR_A(config-if)#ip address 192.168.10.1/24 NXR_A(config-if)#exit NXR_A(config)#ip route 192.168.20.0/24 tunnel 1 1 NXR_A(config)#ip route 192.168.20.0/24 null 254 NXR_A(config)#ipv6 route ::/0 ppp 0 NXR_A(config)#ipv6 access-list ppp0_in permit any any udp any 546 NXR_A(config)#ipv6 access-list ppp0_in permit 2001:0db8:2:1::1 2001:0db8:1:1::1 udp 500 500 NXR_A(config)#ipv6 access-list ppp0_in permit 2001:0db8:2:1::1 2001:0db8:1:1::1 50 NXR_A(config)#ipsec access-list ipsec_acl ip any any NXR_A(config)#ipsec local policy 1 NXR_A(config-ipsec-local)#address ipv6 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 ipv6 2001:0db8:2:1::1 NXR_A(config-ipsec-isakmp)#keepalive 30 3 periodic restart NXR_A(config-ipsec-isakmp)#local policy 1 NXR_A(config-ipsec-isakmp)#exit NXR_A(config)#ipsec tunnel policy 1 NXR A(config-ipsec-tunnel)#description NXR B NXR_A(config-ipsec-tunnel)#negotiation-mode auto NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac NXR_A(config-ipsec-tunnel)#set pfs group5 NXR_A(config-ipsec-tunnel)#set sa lifetime 3600 NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1 NXR_A(config-ipsec-tunnel)#match address ipsec_acl NXR_A(config-ipsec-tunnel)#exit NXR_A(config)#interface tunnel 1 NXR_A(config-tunnel)#tunnel mode ipsec ipv6 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)#ppp account username test1@v6.example.jp password test1pass NXR_A(config)#interface ppp 0 NXR A(config-ppp)#no ip address NXR_A(config-ppp)#no ppp ipcp enable NXR A(config-ppp)#ppp ipv6cp enable NXR A(config-ppp)#ipv6 dhcp client pd dhcpv6pd NXR_A(config-ppp)#ipv6 address dhcpv6pd ::1/64 NXR_A(config-ppp)#ipv6 access-group in ppp0_in NXR_A(config-ppp)#ipv6 spi-filter NXR_A(config-ppp)#ipv6 tcp adjust-mss auto NXR_A(config-ppp)#ppp username test1@v6.example.jp

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)#exit

NXR_A#save config

[NXR_B の設定]

nxrg100#configure terminal Enter configuration commands, one per line. End with CNTL/Z. nxrg100(config)#hostname NXR B NXR_B(config)#interface ethernet 0 NXR B(config-if)#ip address 192.168.20.1/24 NXR B(config-if)#exit NXR B(config)#ip route 192.168.10.0/24 tunnel 1 1 NXR B(config)#ip route 192.168.10.0/24 null 254 NXR B(config)#ipv6 route ::/0 ppp 0 NXR B(config)#ipv6 access-list ppp0 in permit any any udp any 546 NXR B(config)#ipv6 access-list ppp0 in permit 2001:0db8:1:1::1 2001:0db8:2:1::1 udp 500 500 NXR B(config)#ipv6 access-list ppp0 in permit 2001:0db8:1:1::1 2001:0db8:2:1::1 50 NXR_B(config)#ipsec access-list ipsec_acl ip any any NXR B(config)#ipsec local policy 1 NXR_B(config-ipsec-local)#address ipv6 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 ipv6 2001:0db8:1:1::1 NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart NXR_B(config-ipsec-isakmp)#local policy 1 NXR B(config-ipsec-isakmp)#exit NXR_B(config)#ipsec tunnel policy 1 NXR_B(config-ipsec-tunnel)#description NXR_A NXR_B(config-ipsec-tunnel)#negotiation-mode auto NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac NXR B(config-ipsec-tunnel)#set pfs group5 NXR B(config-ipsec-tunnel)#set sa lifetime 3600 NXR B(config-ipsec-tunnel)#set key-exchange isakmp 1 NXR B(config-ipsec-tunnel)#match address ipsec acl NXR_B(config-ipsec-tunnel)#exit NXR_B(config)#interface tunnel 1 NXR_B(config-tunnel)#tunnel mode ipsec ipv6 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)#ppp account username test2@v6.example.jp password test2pass NXR_B(config)#interface ppp 0 NXR B(config-ppp)#no ip address NXR_B(config-ppp)#no ppp ipcp enable NXR B(config-ppp)#ppp ipv6cp enable NXR B(config-ppp)#ipv6 dhcp client pd dhcpv6pd NXR_B(config-ppp)#ipv6 address dhcpv6pd ::1/64 NXR_B(config-ppp)#ipv6 access-group in ppp0_in NXR_B(config-ppp)#ipv6 spi-filter NXR_B(config-ppp)#ipv6 tcp adjust-mss auto

NXR_B(config-ppp)#ppp username test2@v6.example.jp

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)#exit

NXR_B#save config

【設定例解説】

[NXR_A の設定]

1. <ホスト名の設定>

nxrg100(config)#hostname NXR_A

ホスト名を設定します。

2. <LAN 側(ethernet0)インタフェース設定>

NXR_A(config)#interface ethernet 0

NXR_A(config-if)#ip address 192.168.10.1/24

ethernet0 インタフェースの IPv4 アドレスを設定します。

3. <スタティックルート設定>

NXR_A(config)#ip route 192.168.20.0/24 tunnel 1 1 NXR_A(config)#ip route 192.168.20.0/24 null 254

LAN_B 向けのルートを設定します。なお、IPsec SA 確立時はトンネル 1 インタフェースを、未確立時は null インタフェースのルートを利用するように設定します。

(IPF) null インタフェースを出力インタフェースとして設定した場合、パケットが出力されることはありません(ドロップされます)。

NXR_A(config)#ipv6 route ::/0 ppp 0

IPv6 デフォルトルートを設定します。

4. <IPv6 アクセスリスト設定>

NXR_A(config)#ipv6 access-list ppp0_in permit any any udp any 546

IPv6 アクセスリスト名を ppp0_in とし、宛先 UDP ポート 546 番(DHCPv6 クライアント)を許可します。

NXR_A(config)#ipv6 access-list ppp0_in permit 2001:0db8:2:1::1 2001:0db8:1:1::1 udp 500 500 NXR_A(config)#ipv6 access-list ppp0_in permit 2001:0db8:2:1::1 2001:0db8:1:1::1 50

IPv6 アクセスリスト名を ppp0_in とし、送信元が NXR_B の WAN 側 IPv6 アドレス 2001:0db8:2:1::1、 宛先が NXR_A の WAN 側 IPv6 アドレス 2001:0db8:1:1::1 の IKE パケット(UDP ポート 500 番)、ESP パケット(プロトコル番号 50)を許可します。

なお、これら IPv6 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。

(FF) IPv6 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。

5. <IPsec アクセスリスト設定>

NXR_A(config)#ipsec access-list ipsec_acl ip any any

ipsec_acl という名前の IPsec アクセスリストを設定します。なお、送信元 IPv4 アドレス,宛先 IPv4 アドレスともに any とします。

6. <IPsec ローカルポリシー設定>

NXR_A(config)#ipsec local policy 1

NXR_A(config-ipsec-local)#address ipv6

IPsec トンネルの送信元 IP アドレスを ipv6 と設定します。

7. <IPsec ISAKMP ポリシー設定>

NXR_A(config)#ipsec isakmp policy 1

NXR_A(config-ipsec-isakmp)#description NXR_B

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

ISAKMP ポリシーの説明として NXR_B、認証方式として pre-share(事前共有鍵)を選択し事前共有鍵 ipseckey を設定します。なお、事前共有鍵は NXR B と共通の値を設定します。

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

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

NXR_A(config-ipsec-isakmp)#remote address ipv6 2001:0db8:2:1::1

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

 ${\tt NXR_A(config-ipsec-isakmp)\#local\ policy\ 1}$

リモートアドレスに NXR_B の WAN 側 IPv6 アドレスを設定します。また、IKE KeepAlive(DPD)を監視間隔 30 秒,リトライ回数 3 回とし keepalive 失敗時に SA を削除し IKE のネゴシエーションを開始するよう設定します。そして、IPsec ローカルポリシー1 と関連づけを行います。

8. <IPsec トンネルポリシー設定>

NXR_A(config)#ipsec tunnel policy 1

NXR_A(config-ipsec-tunnel)#description NXR_B

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

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

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

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

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

暗号化アルゴリズムとして aes128、認証アルゴリズムとして sha1、PFS を有効にし、かつ DH グループ

として group5、IPsec SA のライフタイムとして 3600 秒を設定します。

NXR A(config-ipsec-tunnel)#set key-exchange isakmp 1

NXR_A(config-ipsec-tunnel)#match address ipsec_acl

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

9. <トンネル1インタフェース設定>

NXR_A(config)#interface tunnel 1

NXR_A(config-tunnel)#tunnel mode ipsec ipv6

NXR_A(config-tunnel)#tunnel protection ipsec policy 1

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

トンネル 1 インタフェースでトンネルモードを ipsec ipv6、使用するトンネルポリシーとして 1 を設定します。また、IPv4 TCP MSS の調整機能をオートに設定します。

10. <PPP アカウント設定>

NXR_A(config)#ppp account username test1@v6.example.jp password test1pass

ppp0 インタフェースで使用する IPv6 ISP 接続用ユーザ ID,パスワードを設定します。

(F) 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。

11. <WAN 側(ppp0)インタフェース設定>

NXR_A(config)#interface ppp 0

NXR_A(config-ppp)#no ip address

ppp0 インタフェースの IPv4 アドレスを無効に設定します。

NXR_A(config-ppp)#no ppp ipcp enable

 $NXR_A (config-ppp) \# \textbf{ppp ipv6cp enable}$

IPCP を無効、IPv6CP を有効に設定します。

NXR_A(config-ppp)#ipv6 dhcp client pd dhcpv6pd

DHCPv6-PD 名を指定し、DHCPv6-PD を有効にします。

NXR_A(config-ppp)#ipv6 address dhcpv6pd ::1/64

ppp0 インタフェースの IPv6 アドレスを設定します。

(m) DHCPv6-PD で取得した IPv6 プレフィックスを使用し、プレフィックス以降は::1/64 とします。

NXR_A(config-ppp)#ipv6 access-group in ppp0_in

IPv6 アクセスリスト ppp0_in を in フィルタに適用します。

NXR_A(config-ppp)#ipv6 spi-filter

IPv6 ステートフルパケットインスペクションを有効に設定します。

NXR_A(config-ppp)#ipv6 tcp adjust-mss auto

IPv6 TCP MSS の調整機能をオートに設定します。

 $NXR_A (config-ppp) \# \textbf{ppp username test1@v6.example.jp}$

IPv6 ISP 接続用ユーザ ID を設定します。

NXR_A(config-ppp)#ipsec policy 1

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

12. <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

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

[NXR B の設定]

1. <ホスト名の設定>

nxrg100(config)#hostname NXR_B

ホスト名を設定します。

2. <LAN 側(ethernet0)インタフェース設定>

NXR_B(config)#interface ethernet 0

NXR_B(config-if)#ip address 192.168.20.1/24

ethernet0 インタフェースの IPv4 アドレスを設定します。

3. <スタティックルート設定>

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

 ${\rm NXR_B(config)} \# ip \ route \ 192.168.10.0/24 \ null \ 254$

LAN_A向けのルートを設定します。なお、IPsec SA確立時はトンネル1インタフェースを、未確立時はnullインタフェースのルートを利用するように設定します。

(IFF) null インタフェースを出力インタフェースとして設定した場合、パケットが出力されることはありません(ドロップされます)。

NXR_B(config)#ipv6 route ::/0 ppp 0

IPv6 デフォルトルートを設定します。

4. <IPv6 アクセスリスト設定>

NXR_B(config)#ipv6 access-list ppp0_in permit any any udp any 546

IPv6 アクセスリスト名を ppp0_in とし、宛先 UDP ポート 546 番(DHCPv6 クライアント)を許可します。

NXR_B(config)#ipv6 access-list ppp0_in permit 2001:0db8:1:1::1 2001:0db8:2:1::1 udp 500 500 NXR_B(config)#ipv6 access-list ppp0_in permit 2001:0db8:1:1::1 2001:0db8:2:1::1 50

IPv6 アクセスリスト名を ppp0_in とし、送信元が NXR_A の WAN 側 IPv6 アドレス 2001:0db8:1:1::1、 宛先が NXR_B の WAN 側 IPv6 アドレス 2001:0db8:2:1::1 の IKE パケット(UDP ポート 500 番)、ESP パケット(プロトコル番号 50)を許可します。

なお、これら IPv6 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) IPv6 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。

5. <IPsec アクセスリスト設定>

NXR_B(config)#ipsec access-list ipsec_acl ip any any

ipsec_acl という名前の IPsec アクセスリストを設定します。なお、送信元 IPv4 アドレス,宛先 IPv4 アドレスともに any とします。

6. <IPsec ローカルポリシー設定>

NXR_B(config)#ipsec local policy 1

NXR_B(config-ipsec-local)#address ipv6

IPsec トンネルの送信元 IP アドレスを ipv6 と設定します。

7. <IPsec ISAKMP ポリシー設定>

NXR_B(config)#ipsec isakmp policy 1

NXR_B(config-ipsec-isakmp)#description NXR_A

NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey

ISAKMP ポリシーの説明として NXR_A、認証方式として pre-share(事前共有鍵)を選択し事前共有鍵 ipseckey を設定します。なお、事前共有鍵は NXR_A と共通の値を設定します。

NXR_B(config-ipsec-isakmp)#hash sha1

NXR_B(config-ipsec-isakmp)#encryption aes128

NXR_B(config-ipsec-isakmp)#group 5

NXR_B(config-ipsec-isakmp)#lifetime 10800

NXR_B(config-ipsec-isakmp)#isakmp-mode main

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

NXR_B(config-ipsec-isakmp)#remote address ipv6 2001:0db8:1:1::1

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

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

リモートアドレスに NXR_A の WAN 側 IPv6 アドレスを設定します。また、IKE KeepAlive(DPD)を監視間隔 30 秒,リトライ回数 3 回とし keepalive 失敗時に SA を削除し IKE のネゴシエーションを開始するよう設定します。そして、IPsec ローカルポリシー1 と関連づけを行います。

8. <IPsec トンネルポリシー設定>

NXR_B(config)#ipsec tunnel policy 1

NXR_B(config-ipsec-tunnel)#description NXR_A

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

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

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

NXR_B(config-ipsec-tunnel)#set pfs group5

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

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

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

NXR_B(config-ipsec-tunnel)#match address ipsec_acl

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

9. <トンネル1インタフェース設定>

NXR_B(config)#interface tunnel 1

NXR_B(config-tunnel)#tunnel mode ipsec ipv6

NXR_B(config-tunnel)#tunnel protection ipsec policy 1

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

トンネル 1 インタフェースでトンネルモードを ipsec ipv6、使用するトンネルポリシーとして 1 を設定します。また、IPv4 TCP MSS の調整機能をオートに設定します。

10. <PPP アカウント設定>

NXR_B(config)#ppp account username test2@v6.example.jp password test2pass

ppp0 インタフェースで使用する IPv6 ISP 接続用ユーザ ID,パスワードを設定します。

(pr) 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。

11. <WAN 側(ppp0)インタフェース設定>

NXR_B(config)#interface ppp 0

NXR_B(config-ppp)#no ip address

ppp0 インタフェースの IPv4 アドレスを無効に設定します。

NXR_B(config-ppp)#no ppp ipcp enable

 $NXR_B(config\text{-}ppp) \# \textbf{ppp ipv6cp enable}$

IPCP を無効、IPv6CP を有効に設定します。

NXR_B(config-ppp)#ipv6 dhcp client pd dhcpv6pd

DHCPv6-PD 名を指定し、DHCPv6-PD を有効にします。

NXR_B(config-ppp)#ipv6 address dhcpv6pd ::1/64

ppp0 インタフェースの IPv6 アドレスを設定します。

(☞) DHCPv6-PD で取得した IPv6 プレフィックスを使用し、プレフィックス以降は::1/64 とします。

NXR_B(config-ppp)#ipv6 access-group in ppp0_in

NXR_B(config-ppp)#ipv6 spi-filter

NXR_B(config-ppp)#ipv6 tcp adjust-mss auto

IPv6 アクセスリスト ppp0_in を in フィルタに適用し、IPv6 ステートフルパケットインスペクションを有効に設定します。また IPv6 TCP MSS の調整機能をオートに設定します。

NXR_B(config-ppp)#ppp username test2@v6.example.jp

IPv6 ISP 接続用ユーザ ID を設定します。

NXR_B(config-ppp)#ipsec policy 1

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

12. <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

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

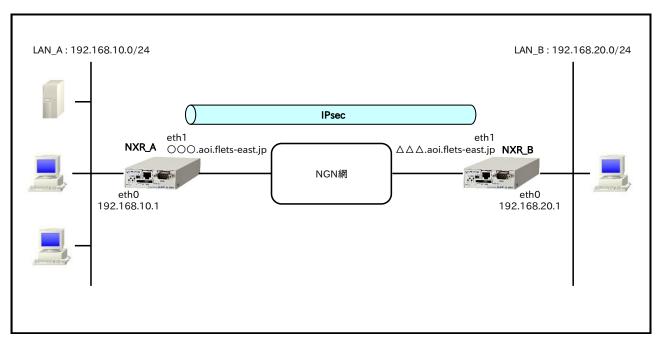
【端末の設定例】

	LAN_A の端末	LAN_B の端末
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
デフォルトゲートウェイ	192.168.10.1	192.168.20.1

4-2. IPv6 IPoE(RA)IPsec 接続設定(ネームの利用)

NTT 東日本/西日本が提供するフレッツ光ネクスト回線で IPv6 IPoE 接続を行います。そして、それを利用して拠点間で IPv4 over IPv6 の IPsec 接続を行います。なお、この設定例ではひかり電話契約なしの場合を想定しており、かつ NGN 網内で VPN を行います。

【構成図】



- ・ この設定例はフレッツ v6 オプションの「ネーム」の利用を想定しています。よって、事前に「ネーム」の登録が必要です。
 - (PF) 「ネーム」を利用して NTT 東日本,西日本間で通信することはできません。
- ・ ルータ NXR_A,B ともに対向ルータの FQDN の名前解決後、IPsec 接続を開始します。よって名前解 決ができない場合、IPsec 接続を開始することができませんのでご注意ください。
- ・ この設定例では Route Based IPsec を利用します。

【 設定データ 】

[NXR A の設定]

	設定内容			
ホスト名	NXR_A			
LAN 側インタフェース	ethernet0のIPv4ア	ドレス		192.168.10.1/24
	ethernet1のIPv4ア	無効		
	ethernet1のIPv6ア	自動設定		
WAN 側インタフェース	DHCPv6 クライアント		クライアント名	ipv6dhcpc
WAN MIT DATE A	IPv6 アクセスグループ		in	eth1_in
	IPv6 SPI フィルタ	有効		
	IPsec ローカルポリシ	1		
			v4 アドレス	192.168.20.0/24
スタティックルート	No.1	ゲートウェイ(インタフェース)		tunnel1
		ディスク	タンス	1

			<u></u> 先 IPv4 アドレス	192.168.20.0/24
			ートウェイ(インタフェース)	null
	110.2		ィスタンス	254
	ルール名	<u>'</u>	1112 111	eth1_in
	,, ,, <u>,,</u>		動作	—————————————————————————————————————
			送信元 IPv6 アドレス	any
		No.1	宛先 IPv6 アドレス	any
			プロトコル	ICMPv6
				許可
			送信元 IPv6 アドレス	any
			宛先 IPv6 アドレス	any
		No.2	プロトコル	UDP
			送信元ポート	
IPv6 フィルタ			宛先ポート	any 546
IFVO 7170X	eth1_in		動作	
			送信元 IPv6 アドレス 宛先 IPv6 アドレス	any
		No.3	別先 IPVO アドレス プロトコル	any UDP
			送信元ポート	500
			宛先ポート	500
			動作	許可
		No.4	送信元 IPv6 アドレス	any
			宛先 IPv6 アドレス	any
			プロトコル	50(ESP)
	IPsec アクセスリスト IPsec ローカルポリシー1		リスト名	ipsec_acl
			送信元 IPv4 アドレス	any
			宛先 IPv4 アドレス	any
				ipv6
			名前	NXR_B
			認証方式	pre-share
			認証鍵	ipseckey
			認証アルゴリズム	sha1
			暗号化アルゴリズム	aes128
			DH グループ	5
	IPsec ISAKM	P ポリシー	1 ライフタイム	10800 秒
			ISAKMP モード	メインモード
IPsec			リモートアドレス	$\triangle\triangle\triangle$.aoi.flets-east.jp
			再送間隔	30 秒
			DPD リトライ回数	3回
			動作	restart
			ローカルポリシー	1
			名前	NXR B
			ネゴシエーションモード	オート
			認証アルゴリズム	sha1
			暗号化アルゴリズム	aes128
	IPsec トンネル	レポリシー1	PFS	有効(グループ 5)
			ライフタイム	3600 秒
			ISAKMP ポリシー	1
			IPsec アクセスリスト	ipsec_acl
	トンネルモー	ド	II SEC / / ピハリハト	IPsec(IPv6)
│ │ トンネル 1 インタフェース	トンネルプロラ			ipsec policy 1
r v n n 1 1 v x / ± - X				1psec policy 1 オート
	IPv4 TCP MS	3 日期調発		
DUCDES AS AS AS A	名前 information o	nltr		ipv6dhcpc
DHCPv6 クライアント	information-o			有効
	option-request			DNS サーバ
DNS	サービス			有效
	EDNS			有効

〔NXR_B の設定〕

	設定	官項目			設定内容
ホスト名		NXR_B			
LAN 側インタフェース	ethernet0の	IPv4 ア	192.168.20.1/24		
	ethernet1の		無効		
	ethernet1の	自動設定			
	DHCPv6 クラ		ipv6dhcpc		
WAN 側インタフェース	IPv6 アクセス			クライアント名 in	eth1_in
	IPv6 SPI フィ			***	有効
	IPsec ローカノ		/_		1
	11000 : 777	. , , ,		v4 アドレス	192.168.10.0/24
	No.1			ウェイ(インタフェース)	tunnel1
	110.1		ディス		1
スタティックルート				v4 アドレス	192.168.10.0/24
	No.2			ウェイ(インタフェース)	null
	110.2		ディス		254
	ルール名		7 1 2 1 2 1 2	,, , , , , , , , , , , , , , , , , , ,	eth1_in
	70 7041			動作	<u></u> 許可
				送信元 IPv6 アドレス	any
		No.1		宛先 IPv6 アドレス	
		1		プロトコル	any ICMPv6
		-		動作	許可
		1		- 動作 - 送信元 IPv6 アドレス	
					any
		No.2		宛先 IPv6 アドレス プロトコル	any UDP
				送信元ポート	
ID C > 1 h					any
IPv6 フィルタ	eth1_in			宛先ポート	546
	No.3			動作	許可
				送信元 IPv6 アドレス	any
		No.3		宛先 IPv6 アドレス	any
				プロトコル	UDP
				送信元ポート	500
				宛先ポート	500
				動作	許可
		-	送信元 IPv6 アドレス	any	
				宛先 IPv6 アドレス	any
				プロトコル	50(ESP)
				リスト名	ipsec_acl
	IPsec アクセスリ		`	送信元 IPv4 アドレス	any
				宛先 IPv4 アドレス	any
	IPsec ローカルポリシー1			address	ipv6
				名前	NXR_A
				認証方式	pre-share
				認証鍵	ipseckey
				認証アルゴリズム	sha1
				暗号化アルゴリズム	aes128
				DH グループ	5
	IPsec ISAKM	Ρポリ	シー1	ライフタイム	10800 秒
IPsec				ISAKMP モード	メインモード
				リモートアドレス	○○○.aoi.flets-east.jp
				再送間隔	30 秒
				DPD リトライ回数	3 回
				動作	restart
				ローカルポリシー	1
				名前	NXR_A
				ネゴシエーションモード	オート
	IDage by	1,4911.5	/ _ 1	認証アルゴリズム	sha1
	IPsec トンネルポリシー1		暗号化アルゴリズム	aes128	
			PFS	有効(グループ 5)	
				ライフタイム	3600 秒
<u> </u>	•			•	

		ISAKMP ポリシー	1
		IPsec アクセスリスト	ipsec_acl
	トンネルモード		IPsec(IPv6)
トンネル1インタフェース	トンネルプロテクション		ipsec policy 1
	IPv4 TCP MSS 自動調整	オート	
	名前		ipv6dhcpc
DHCPv6 クライアント	information-only		有効
	option-request		DNS サーバ
DNS	サービス		有効
DNS	EDNS	有効	

【設定例】

[NXR A の設定]

NXR_A(config-tunnel)#exit

NXR_A(config)#interface ethernet 1

nxrg100#configure terminal Enter configuration commands, one per line. End with CNTL/Z. nxrg100(config)#hostname NXR_A NXR A(config)#ipv6 dhcp-client ipv6dhcpc NXR_A(config-dhcp6c)#information-only enable NXR A(config-dhcp6c)#option-request dns-servers NXR A(config-dhcp6c)#exit NXR_A(config)#interface ethernet 0 NXR_A(config-if)#ip address 192.168.10.1/24 NXR A(config-if)#exit NXR_A(config)#ip route 192.168.20.0/24 tunnel 1 1 NXR_A(config)#ip route 192.168.20.0/24 null 254 NXR_A(config)#ipv6 access-list eth1_in permit any any icmpv6 NXR_A(config)#ipv6 access-list eth1_in permit any any udp any 546 NXR_A(config)#ipv6 access-list eth1_in permit any any udp 500 500 NXR A(config)#ipv6 access-list eth1 in permit any any 50 NXR A(config)#ipsec access-list ipsec acl ip any any NXR A(config)#ipsec local policy 1 NXR A(config-ipsec-local)#address ipv6 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 ipv6 $\triangle \triangle \triangle$.aoi.flets-east.jp NXR A(config-ipsec-isakmp)#keepalive 30 3 periodic restart NXR A(config-ipsec-isakmp)#local policy 1 NXR A(config-ipsec-isakmp)#exit NXR_A(config)#ipsec tunnel policy 1 NXR_A(config-ipsec-tunnel)#description NXR_B NXR_A(config-ipsec-tunnel)#negotiation-mode auto NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac NXR_A(config-ipsec-tunnel)#set pfs group5 NXR_A(config-ipsec-tunnel)#set sa lifetime 3600 NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1 NXR_A(config-ipsec-tunnel)#match address ipsec_acl NXR A(config-ipsec-tunnel)#exit NXR_A(config)#interface tunnel 1 NXR A(config-tunnel)#tunnel mode ipsec ipv6 NXR A(config-tunnel)#tunnel protection ipsec policy 1 NXR_A(config-tunnel)#ip tcp adjust-mss auto

NXR_A(config-if)#no ip address

NXR_A(config-if)#ipv6 address autoconfig

NXR_A(config-if)#ipv6 access-group in eth1_in

NXR_A(config-if)#ipv6 spi-filter

NXR_A(config-if)#ipv6 dhcp client ipv6dhcpc

NXR_A(config-if)#ipsec policy 1

NXR_A(config-if)#exit

NXR_A(config)#dns

NXR_A(config-dns)#service enable

NXR_A(config-dns)#edns-query enable

NXR_A(config-dns)#exit

NXR_A(config)#exit

NXR_A#save config

[NXR B の設定]

nxrg100#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

nxrg100(config)#hostname NXR_B

NXR_B(config)#ipv6 dhcp-client ipv6dhcpc

NXR_B(config-dhcp6c)#information-only enable

NXR_B(config-dhcp6c)#option-request dns-servers

NXR_B(config-dhcp6c)#exit

NXR_B(config)#interface ethernet 0

NXR_B(config-if)#ip address 192.168.20.1/24

NXR_B(config-if)#exit

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

 $NXR_B(config) \#ip\ route\ 192.168.10.0/24\ null\ 254$

NXR_B(config)#ipv6 access-list eth1_in permit any any icmpv6

NXR_B(config)#ipv6 access-list eth1_in permit any any udp any 546

NXR_B(config)#ipv6 access-list eth1_in permit any any udp 500 500 $\,$

NXR_B(config)#ipv6 access-list eth1_in permit any any 50

NXR_B(config)#ipsec access-list ipsec_acl ip any any

NXR_B(config)#ipsec local policy 1

NXR_B(config-ipsec-local)#address ipv6

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 ipv6 OOO.aoi.flets-east.jp

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

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

NXR_B(config-ipsec-isakmp)#exit

NXR_B(config)#ipsec tunnel policy 1

NXR_B(config-ipsec-tunnel)#description NXR_A

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

NXR B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac

NXR_B(config-ipsec-tunnel)#set pfs group5

NXR B(config-ipsec-tunnel)#set sa lifetime 3600

NXR B(config-ipsec-tunnel)#set kev-exchange isakmp 1

NXR_B(config-ipsec-tunnel)#match address ipsec_acl

NXR B(config-ipsec-tunnel)#exit

NXR_B(config)#interface tunnel 1

NXR_B(config-tunnel)#tunnel mode ipsec ipv6

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)#no ip address

NXR_B(config-if)#ipv6 address autoconfig

NXR_B(config-if)#ipv6 access-group in eth1_in

NXR_B(config-if)#ipv6 spi-filter

NXR_B(config-if)#ipv6 dhcp client ipv6dhcpc

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)#edns-query 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>

nxrg100(config)#hostname NXR_A

ホスト名を設定します。

2. <DHCPv6 クライアント設定>

NXR_A(config)#ipv6 dhcp-client ipv6dhcpc

DHCPv6 クライアント設定の名前を定義します。

NXR_A(config-dhcp6c)#information-only enable

NXR_A(config-dhcp6c)#option-request dns-servers

information-only 機能を有効、DHCPv6 サーバに対して DNS サーバアドレスの通知を要求するように設定します。

3. <LAN 側(ethernet0)インタフェース設定>

NXR_A(config)#interface ethernet 0

NXR A(config-if)#ip address 192.168.10.1/24

ethernet0 インタフェースの IPv4 アドレスを設定します。

4. <スタティックルート設定>

 ${\rm NXR_A(config)\#ip\ route\ 192.168.20.0/24\ tunnel\ 1\ 1}$

NXR_A(config)#ip route 192.168.20.0/24 null 254

LAN_B 向けのルートを設定します。なお、IPsec SA 確立時はトンネル 1 インタフェースを、未確立時は null インタフェースのルートを利用するように設定します。

(IFF) null インタフェースを出力インタフェースとして設定した場合、パケットが出力されることはありません(ドロップされます)。

5. <IPv6 アクセスリスト設定>

NXR_A(config)#ipv6 access-list eth1_in permit any any icmpv6

NXR_A(config)#ipv6 access-list eth1_in permit any any udp any 546

IPv6 アクセスリスト名を eth1_in とし、ICMPv6 および宛先 UDP ポート 546 番(DHCPv6 クライアント) を許可します。

NXR_A(config)#ipv6 access-list eth1_in permit any any udp 500 500

NXR_A(config)#ipv6 access-list eth1_in permit any any 50

IPv6 アクセスリスト名を eth1_in とし、IKE パケット(UDP ポート 500 番)、ESP パケット(プロトコル番号 50)を許可します。

なお、これら IPv6 アクセスリスト設定は ethernet1 インタフェース設定で登録します。

(**☞**) IPv6 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。

6. <IPsec アクセスリスト設定>

NXR_A(config)#ipsec access-list ipsec_acl ip any any

ipsec_acl という名前の IPsec アクセスリストを設定します。なお、送信元 IPv4 アドレス,宛先 IPv4 アドレスともに any とします。

7. <IPsec ローカルポリシー設定>

NXR_A(config)#ipsec local policy 1

NXR_A(config-ipsec-local)#address ipv6

IPsec トンネルの送信元 IP アドレスを ipv6 と設定します。

8. <IPsec ISAKMP ポリシー設定>

NXR_A(config)#ipsec isakmp policy 1

 $NXR_A (config-ipsec-isakmp) \# \textbf{description NXR_B}$

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

ISAKMP ポリシーの説明として NXR_B、認証方式として pre-share(事前共有鍵)を選択し事前共有鍵 ipseckey を設定します。なお、事前共有鍵は NXR_B と共通の値を設定します。

NXR_A(config-ipsec-isakmp)#hash sha1

 $NXR_A (config-ipsec-isakmp) \# \textbf{encryption aes} 128$

NXR_A(config-ipsec-isakmp)#group 5

NXR_A(config-ipsec-isakmp)#lifetime 10800

 $NXR_A (config-ipsec-isakmp) \verb|#isakmp-mode main|$

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

NXR_A(config-ipsec-isakmp)#remote address ipv6 \(\Delta \Delta \Delta \alpha \

NXR A(config-ipsec-isakmp)#keepalive 30 3 periodic restart

 $NXR_A(config-ipsec-isakmp)\#local\ policy\ 1$

リモートアドレスに NXR_B の FQDN を設定します。また、IKE KeepAlive(DPD)を監視間隔 30 秒,リト

ライ回数 3 回とし keepalive 失敗時に SA を削除し IKE のネゴシエーションを開始するよう設定します。 そして、IPsec ローカルポリシー1 と関連づけを行います。

9. <IPsec トンネルポリシー設定>

NXR_A(config)#ipsec tunnel policy 1

NXR_A(config-ipsec-tunnel)#description NXR_B

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

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

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

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

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

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

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

NXR_A(config-ipsec-tunnel)#match address ipsec_acl

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

10. <トンネル 1 インタフェース設定>

NXR_A(config)#interface tunnel 1

NXR_A(config-tunnel)#tunnel mode ipsec ipv6

NXR_A(config-tunnel)#tunnel protection ipsec policy 1

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

トンネル 1 インタフェースでトンネルモードを ipsec ipv6、使用するトンネルポリシーとして 1 を設定します。また、IPv4 TCP MSS の調整機能をオートに設定します。

11. <WAN 側(ethernet1)インタフェース設定>

 ${\rm NXR_A(config)} \# interface\ ethernet\ 1$

NXR_A(config-if)#no ip address

NXR_A(config-if)#ipv6 address autoconfig

ethernet1 インタフェースの IPv4 アドレスを無効、IPv6 アドレスを自動設定に設定します。

NXR_A(config-if)#ipv6 access-group in eth1_in

IPv6 アクセスリスト eth1_in を in フィルタに適用します。

NXR_A(config-if)#ipv6 spi-filter

IPv6 ステートフルパケットインスペクションを有効に設定します。

NXR_A(config-if)#ipv6 dhcp client ipv6dhcpc

DHCPv6 クライアント名を指定し、DHCPv6 クライアントを有効にします。

NXR_A(config-if)#ipsec policy 1

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

12. <DNS 設定>

NXR_A(config)#dns

NXR_A(config-dns)#service enable

DNS サービスを有効にします。

NXR_A(config-dns)#edns-query enable

EDNS を有効にします。

[NXR B の設定]

1. <ホスト名の設定>

nxrg100(config)#hostname NXR_B

ホスト名を設定します。

2. <DHCPv6 クライアント設定>

NXR_B(config)#ipv6 dhcp-client ipv6dhcpc

DHCPv6 クライアント設定の名前を定義します。

NXR_B(config-dhcp6c)#information-only enable

NXR_B(config-dhcp6c)#option-request dns-servers

information-only 機能を有効、DHCPv6 サーバに対して DNS サーバアドレスの通知を要求するように設定します。

3. <LAN 側(ethernet0)インタフェース設定>

NXR_B(config)#interface ethernet 0

 $NXR_B(config-if)$ #ip address 192.168.20.1/24

ethernet0 インタフェースの IPv4 アドレスを設定します。

4. <スタティックルート設定>

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

NXR_B(config)#ip route 192.168.10.0/24 null 254

LAN_A向けのルートを設定します。なお、IPsec SA確立時はトンネル 1 インタフェースを、未確立時は null インタフェースのルートを利用するように設定します。

(**☞**) null インタフェースを出力インタフェースとして設定した場合、パケットが出力されることはありません(ドロップされます)。

5. <IPv6 アクセスリスト設定>

NXR_B(config)#ipv6 access-list eth1_in permit any any icmpv6 NXR_B(config)#ipv6 access-list eth1_in permit any any udp any 546

IPv6 アクセスリスト名を eth1_in とし、ICMPv6 および宛先 UDP ポート 546 番(DHCPv6 クライアント) を許可します。

NXR_B(config)#ipv6 access-list eth1_in permit any any udp 500 500

NXR_B(config)#ipv6 access-list eth1_in permit any any 50

IPv6 アクセスリスト名を eth1_in とし、IKE パケット(UDP ポート 500 番)、ESP パケット(プロトコル番号 50)を許可します。

なお、これら IPv6 アクセスリスト設定は ethernet1 インタフェース設定で登録します。

(P) IPv6 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。

6. <IPsec アクセスリスト設定>

NXR_B(config)#ipsec access-list ipsec_acl ip any any

ipsec_acl という名前の IPsec アクセスリストを設定します。なお、送信元 IPv4 アドレス,宛先 IPv4 アドレスともに any とします。

7. <IPsec ローカルポリシー設定>

NXR_B(config)#ipsec local policy 1

NXR_B(config-ipsec-local)#address ipv6

IPsec トンネルの送信元 IP アドレスを ipv6 と設定します。

8. <IPsec ISAKMP ポリシー設定>

NXR_B(config)#ipsec isakmp policy 1

NXR_B(config-ipsec-isakmp)#description NXR_A

NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey

ISAKMP ポリシーの説明として NXR_A、認証方式として pre-share(事前共有鍵)を選択し、事前共有鍵 ipseckey を設定します。なお、事前共有鍵は NXR_A と共通の値を設定します。

NXR_B(config-ipsec-isakmp)#hash sha1

NXR_B(config-ipsec-isakmp)#encryption aes128

NXR_B(config-ipsec-isakmp)#group 5

NXR B(config-ipsec-isakmp)#lifetime 10800

NXR_B(config-ipsec-isakmp)#isakmp-mode main

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

NXR_B(config-ipsec-isakmp)#remote address ipv6 OOO.aoi.flets-east.jp

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

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

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

9. <IPsec トンネルポリシー設定>

NXR_B(config)#ipsec tunnel policy 1

NXR_B(config-ipsec-tunnel)#description NXR_A

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

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

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

NXR_B(config-ipsec-tunnel)#set pfs group5

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

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

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

NXR_B(config-ipsec-tunnel)#match address ipsec_acl

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

10. <トンネル 1 インタフェース設定>

NXR_B(config)#interface tunnel 1

NXR_B(config-tunnel)#tunnel mode ipsec ipv6

NXR_B(config-tunnel)#tunnel protection ipsec policy 1

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

トンネル 1 インタフェースでトンネルモードを ipsec ipv6、使用するトンネルポリシーとして 1 を設定します。また、IPv4 TCP MSS の調整機能をオートに設定します。

11. <WAN 側(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)#ipv6 address autoconfig

ethernet1 インタフェースの IPv4 アドレスを無効、IPv6 アドレスを自動設定に設定します。

 $NXR_B(config-if)$ #ipv6 access-group in eth1_in

NXR_B(config-if)#ipv6 spi-filter

IPv6 アクセスリスト eth1_in を in フィルタに適用し、IPv6 ステートフルパケットインスペクションを有効に設定します。

NXR_B(config-if)#ipv6 dhcp client ipv6dhcpc

DHCPv6 クライアント名を指定し、DHCPv6 クライアントを有効にします。

NXR_B(config-if)#ipsec policy 1

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

12. <DNS 設定>

NXR_B(config)#dns

 $NXR_B(config\text{-}dns) \# \textbf{service enable}$

DNS サービスを有効にします。

NXR_B(config-dns)#**edns-query enable**

EDNS を有効にします。

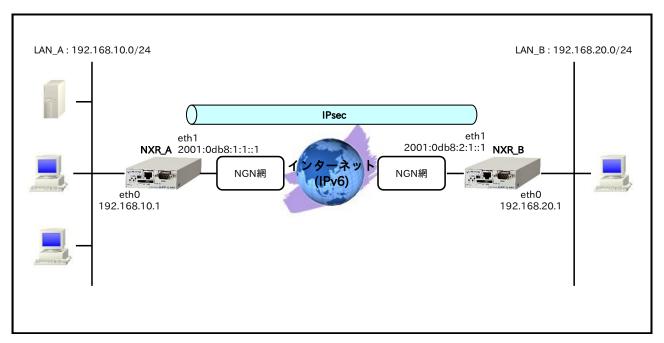
【端末の設定例】

	LAN_A の端末	LAN_B の端末	
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		
デフォルトゲートウェイ	192.168.10.1	192.168.20.1	

4-3. IPv6 IPoE(DHCPv6-PD)IPsec 接続設定

NTT 東日本/西日本が提供するフレッツ光ネクスト回線で IPv6 IPoE 接続を行います。そして、それを利用して拠点間で IPv4 over IPv6 の IPsec 接続を行います。なお、この設定例ではひかり電話契約ありの場合を想定しています。

【構成図】



- ・ ルータ NXR_A には固定でプレフィックス「2001:0db8:1:1::/60」が、ルータ NXR_B には固定でプレフィックス「2001:0db8:2:1::/60」が割り当てられるものとします。
- ・ この設定例では Route Based IPsec を利用します。
- ・ この設定例ではルータ配下の端末からインターネットへアクセスすることはできません。

【 設定データ 】

[NXR_A の設定]

設定項目				設定内容
ホスト名				NXR_A
LAN 側インタフェース	ethernet() の IPv4 アドレス			192.168.10.1/24
WAN 側インタフェース	ethernet1のIPv4アドレス			無効
	ethernet1のIPv6アドレス			dhcpv6pd ::1/64
	RA 受信			有効
	DHCPv6 クライアン	ト(PD)	クライアント名	dhcpv6pd
	IPv6 アクセスグループ in			eth1_in
	IPv6 SPI フィルタ			有効
	IPsec ローカルポリシー			1
スタティックルート		宛先 IPv4 アドレス		192.168.20.0/24
	No.1	ゲートウェイ(インタフェース)		tunnel1
		ディスタンス		1
	No.2	宛先 IPv4 アドレス		192.168.20.0/24
		ゲートウェイ(インタフェース)		null

	ディスタンス			254
	ルール名			eth1_in
			動作	許可
			送信元 IPv6 アドレス	any
		No.1	宛先 IPv6 アドレス	any
			プロトコル	ICMPv6
			動作	許可
			送信元 IPv6 アドレス	any
		No.2	宛先 IPv6 アドレス	·
			プロトコル	any UDP
			送信元ポート	
ID C T . I h				any
IPv6 フィルタ	eth1 in		宛先ポート	546
			動作	許可
			送信元 IPv6 アドレス	2001:0db8:2:1::1
		No.3	宛先 IPv6 アドレス	2001:0db8:1:1::1
		110.0	プロトコル	UDP
			送信元ポート	500
			宛先ポート	500
			動作	許可
		No.4	送信元 IPv6 アドレス	2001:0db8:2:1::1
		No.4	宛先 IPv6 アドレス	2001:0db8:1:1::1
			プロトコル	50(ESP)
	•		リスト名	ipsec_acl
	IPsec アクセン	スリスト	送信元 IPv4 アドレス	any
			宛先 IPv4 アドレス	any
	IPsec ローカルポリシー1		address	ipv6
			名前	NXR_B
			認証方式	pre-share
			認証鍵	ipseckey
			認証アルゴリズム	sha1
			暗号化アルゴリズム	aes128
			DH グループ	5
	IPsec ISAKM	Pポリシー1	ライフタイム	10800 秒
	II SEC ISMINI	1 4.70 1	ISAKMP モード	メインモード
IPsec			リモートアドレス	2001:0db8:2:1::1
IPsec			再送間隔	30秒
			円送间隔 DPD リトライ回数	30 秒 3 回
			動作 ローカルポリシー	restart
				1
			名前	NXR_B
			ネゴシエーションモード	オート
	IPsec トンネルポリシー1 暗号化 PFS ライフ ISAKM IPsec		認証アルゴリズム	sha1
			暗号化アルゴリズム	aes128
				有効(グループ 5)
			ライフタイム	3600 秒
			ISAKMP ポリシー	1
			IPsec アクセスリスト	ipsec_acl
	トンネルモード			IPsec(IPv6)
トンネル1インタフェース	トンネルプロ			ipsec policy 1
	IPv4 TCP MSS 自動調整			オート

〔NXR_B の設定〕

設定項目			設定内容
ホスト名	NXR_B		
LAN 側インタフェース	ethernet0 の IPv4 アドレス	192.168.20.1/24	
WAN 側インタフェース	ethernet1 の IPv4 アドレス	無効	
	ethernet1 の IPv6 アドレス	dhcpv6pd ::1/64	
	RA 受信	有効	
	DHCPv6 クライアント(PD)	クライアント名	dhcpv6pd
	IPv6 アクセスグループ	in	eth1_in

	ID-G CDI フィルカ				
	IPv6 SPI フィルタ IPsec ローカルポリシー				有効 1
	IPsec ローカルホリシー 宛先 IPv4 アドレス			192.168.10.0/24	
スタティックルート	No 1				
	No.1			ウェイ(インタフェース)	tunnel1
			ディス		-
	N. 0			v4アドレス	192.168.10.0/24
	No.2			ウェイ(インタフェース)	null
	3 3 5		ディス	タンス	254
	ルール名	ルール名			eth1_in
				動作	許可
		No.1		送信元 IPv6 アドレス	any
				宛先 IPv6 アドレス	any
				プロトコル	ICMPv6
				動作	許可
				送信元 IPv6 アドレス	any
		No.2		宛先 IPv6 アドレス	any
		110.2		プロトコル	UDP
				送信元ポート	any
IPv6 フィルタ	eth1_in			宛先ポート	546
	Curr_m			動作	許可
				送信元 IPv6 アドレス	2001:0db8:1:1::1
		No.3		宛先 IPv6 アドレス	2001:0db8:2:1::1
		10.5		プロトコル	UDP
				送信元ポート	500
				宛先ポート	500
				動作	許可
		NT - 4		送信元 IPv6 アドレス	2001:0db8:1:1::1
		No.4		宛先 IPv6 アドレス	2001:0db8:2:1::1
				プロトコル	50(ESP)
		リスト名		ipsec_acl	
	IPsec アクセス	スリスト		送信元 IPv4 アドレス	any
				宛先 IPv4 アドレス	any
	IPsec ローカノ	レポリシ	√ - 1	address	ipv6
				名前	NXR_A
				認証方式	pre-share
				認証鍵	ipseckey
				認証アルゴリズム	sha1
				暗号化アルゴリズム	aes128
				DH グループ	5
	IPsec ISAKM	P ポリ [、]	シー1	ライフタイム	10800 秒
	II Sec ISAMII 4077		ISAKMP モード	メインモード	
IPsec			リモートアドレス	2001:0db8:1:1::1	
			再送間隔	30 秒	
			DPD リトライ回数	3 回	
			動作	restart	
			ローカルポリシー	1	
				名前	NXR_A
			オゴシエーションモード	オート	
				認証アルゴリズム	sha1
			暗号化アルゴリズム	aes128	
	IPsec トンネノ	IPsec トンネルポリシー1		PFS	aes126 有効(グループ 5)
				1	
			ライフタイム ISAKMP ポリシー	3600 秒 1	
	1 1 2 0 -	1.0		IPsec アクセスリスト	ipsec_acl
15.39 4 25.5-		トンネルモード		IPsec(IPv6)	
トンネル1インタフェース	トンネルプロテクション		ipsec policy 1		
	IPv4 TCP MSS 自動調整		オート		

【設定例】

[NXR A の設定]

```
nxrg100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg100(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.1/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 192.168.20.0/24 tunnel 1 1
NXR_A(config)#ip route 192.168.20.0/24 null 254
NXR_A(config)#ipv6 access-list eth1_in permit any any icmpv6
NXR A(config)#ipv6 access-list eth1 in permit any any udp any 546
NXR A(config)#ipv6 access-list eth1 in permit 2001:0db8:2:1::1 2001:0db8:1:1::1 udp 500 500
NXR_A(config)#ipv6 access-list eth1_in permit 2001:0db8:2:1::1 2001:0db8:1:1::1 50
NXR A(config)#ipsec access-list ipsec acl ip any any
NXR_A(config)#ipsec local policy 1
NXR A(config-ipsec-local)#address ipv6
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 ipv6 2001:0db8:2:1::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 kev-exchange isakmp 1
NXR A(config-ipsec-tunnel)#match address ipsec acl
NXR A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv6
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)#no ip address
NXR_A(config-if)#ipv6 dhcp client pd dhcpv6pd
NXR A(config-if)#ipv6 address dhcpv6pd ::1/64
NXR A(config-if)#ipv6 nd accept-ra
NXR A(config-if)#ipv6 access-group in eth1 in
NXR A(config-if)#ipv6 spi-filter
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〕

```
nxrg100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg100(config)#hostname NXR B
NXR B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.20.1/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1 1
NXR_B(config)#ip route 192.168.10.0/24 null 254
NXR_B(config)#ipv6 access-list eth1_in permit any any icmpv6
NXR_B(config)#ipv6 access-list eth1_in permit any any udp any 546
NXR_B(config)#ipv6 access-list eth1_in permit 2001:0db8:1:1::1 2001:0db8:2:1::1 udp 500 500
NXR_B(config)#ipv6 access-list eth1_in permit 2001:0db8:1:1::1 2001:0db8:2:1::1 50
NXR_B(config)#ipsec access-list ipsec_acl ip any any
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ipv6
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 ipv6 2001:0db8:1:1::1
NXR_B(config-ipsec-isakmp)#keepalive 30 3 periodic restart
NXR B(config-ipsec-isakmp)#local policy 1
NXR B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description NXR_A
NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group5
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address ipsec_acl
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv6
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)#no ip address
NXR_B(config-if)#ipv6 dhcp client pd dhcpv6pd
NXR_B(config-if)#ipv6 address dhcpv6pd ::1/64
NXR_B(config-if)#ipv6 nd accept-ra
NXR_B(config-if)#ipv6 access-group in eth1_in
NXR_B(config-if)#ipv6 spi-filter
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>

nxrg100(config)#hostname NXR_A

ホスト名を設定します。

2. <LAN 側(ethernet0)インタフェース設定>

NXR_A(config)#interface ethernet 0

NXR_A(config-if)#ip address 192.168.10.1/24

ethernet0 インタフェースの IPv4 アドレスを設定します。

3. <スタティックルート設定>

NXR_A(config)#ip route 192.168.20.0/24 tunnel 1 1

NXR_A(config)#ip route 192.168.20.0/24 null 254

LAN_B向けのルートを設定します。なお、IPsec SA確立時はトンネル 1 インタフェースを、未確立時は null インタフェースのルートを利用するように設定します。

(IFF) null インタフェースを出力インタフェースとして設定した場合、パケットが出力されることはありません(ドロップされます)。

4. <IPv6 アクセスリスト設定>

NXR_A(config)#ipv6 access-list eth1_in permit any any icmpv6

NXR_A(config)#ipv6 access-list eth1_in permit any any udp any 546

IPv6 アクセスリスト名を eth1_in とし、ICMPv6 および宛先 UDP ポート 546 番(DHCPv6 クライアント) を許可します。

NXR_A(config)#ipv6 access-list eth1_in permit 2001:0db8:2:1::1 2001:0db8:1:1::1 udp 500 500 NXR_A(config)#ipv6 access-list eth1_in permit 2001:0db8:2:1::1 2001:0db8:1:1::1 50

IPv6 アクセスリスト名を eth1_in とし、送信元が NXR_B の WAN 側 IPv6 アドレス 2001:0db8:2:1::1、 宛先が NXR_A の WAN 側 IPv6 アドレス 2001:0db8:1:1::1 の IKE パケット(UDP ポート 500 番)、ESP パケット(プロトコル番号 50)を許可します。

なお、これら IPv6 アクセスリスト設定は ethernet1 インタフェース設定で登録します。

(IPV6 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。

5. <IPsec アクセスリスト設定>

NXR_A(config)#ipsec access-list ipsec_acl ip any any

ipsec_acl という名前の IPsec アクセスリストを設定します。なお、送信元 IPv4 アドレス,宛先 IPv4 アドレスともに any とします。

6. <IPsec ローカルポリシー設定>

NXR_A(config)#ipsec local policy 1

NXR_A(config-ipsec-local)#address ipv6

IPsec トンネルの送信元 IP アドレスを ipv6 と設定します。

7. <IPsec ISAKMP ポリシー設定>

NXR_A(config)#ipsec isakmp policy 1

NXR_A(config-ipsec-isakmp)#description NXR_B

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

ISAKMP ポリシーの説明として NXR_B、認証方式として pre-share(事前共有鍵)を選択し事前共有鍵 ipseckey を設定します。なお、事前共有鍵は NXR_B と共通の値を設定します。

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

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

NXR_A(config-ipsec-isakmp)#remote address ipv6 2001:0db8:2:1::1

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

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

リモートアドレスに NXR_B の IPv6 アドレスを設定します。また、IKE KeepAlive(DPD)を監視間隔 30 秒,リトライ回数 3 回とし keepalive 失敗時に SA を削除し IKE のネゴシエーションを開始するよう設定します。そして、IPsec ローカルポリシー1 と関連づけを行います。

8. <IPsec トンネルポリシー設定>

NXR_A(config)#ipsec tunnel policy 1

NXR_A(config-ipsec-tunnel)#description NXR_B

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

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

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

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

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

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

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

NXR_A(config-ipsec-tunnel)#match address ipsec_acl

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

9. <トンネル1インタフェース設定>

NXR_A(config)#interface tunnel 1

NXR_A(config-tunnel)#tunnel mode ipsec ipv6

NXR_A(config-tunnel)#tunnel protection ipsec policy 1

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

トンネル1 インタフェースでトンネルモードを ipsec ipv6、使用するトンネルポリシーとして1 を設定します。また、IPv4 TCP MSS の調整機能をオートに設定します。

10. <WAN 側(ethernet1)インタフェース設定>

NXR_A(config)#interface ethernet 1

NXR_A(config-if)#no ip address

ethernet1 インタフェースの IPv4 アドレスを無効に設定します。

NXR_A(config-if)#ipv6 dhcp client pd dhcpv6pd

DHCPv6 クライアントで IPv6 プレフィックスの名前を定義します。

NXR_A(config-if)#ipv6 address dhcpv6pd ::1/64

ethernet1 インタフェースの IPv6 アドレスを設定します。

(**☞**) DHCPv6 クライアントで取得した IPv6 プレフィックスを使用し、プレフィックス以降は::1/64 とします。

NXR_A(config-if)#ipv6 nd accept-ra

RA を受信するように設定します。

NXR_A(config-if)#ipv6 access-group in eth1_in

IPv6 アクセスリスト eth1 in を in フィルタに適用します。

NXR_A(config-if)#ipv6 spi-filter

IPv6 ステートフルパケットインスペクションを有効に設定します。

NXR_A(config-if)#ipsec policy 1

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

〔NXR_B の設定〕

1. <ホスト名の設定>

nxrg100(config)#hostname NXR_B

ホスト名を設定します。

2. <LAN 側(ethernet0)インタフェース設定>

NXR_B(config)#interface ethernet 0

 $NXR_B(config-if)$ #ip address 192.168.20.1/24

ethernet0 インタフェースの IPv4 アドレスを設定します。

3. <スタティックルート設定>

NXR_B(config)#ip route 192.168.10.0/24 tunnel 1 1 NXR B(config)#ip route 192.168.10.0/24 null 254

LAN_A 向けのルートを設定します。なお、IPsec SA 確立時はトンネル 1 インタフェースを、未確立時は null インタフェースのルートを利用するように設定します。

(IPP) null インタフェースを出力インタフェースとして設定した場合、パケットが出力されることはありません(ドロップされます)。

4. <IPv6 アクセスリスト設定>

NXR_B(config)#ipv6 access-list eth1_in permit any any icmpv6 NXR_B(config)#ipv6 access-list eth1_in permit any any udp any 546

IVAA_b(coming)#ipvo access-iist eiiii_iii perimit any any uup any 040

IPv6 アクセスリスト名を eth1_in とし、ICMPv6 および宛先 UDP ポート 546 番(DHCPv6 クライアント) を許可します。

NXR_B(config)#ipv6 access-list eth1_in permit 2001:0db8:1:1::1 2001:0db8:2:1::1 udp 500 500 NXR B(config)#ipv6 access-list eth1_in permit 2001:0db8:1:1::1 2001:0db8:2:1::1 50

IPv6 アクセスリスト名を eth1_in とし、送信元が NXR_A の WAN 側 IPv6 アドレス 2001:0db8:1:1::1、 宛先が NXR_B の WAN 側 IPv6 アドレス 2001:0db8:2:1::1 の IKE パケット(UDP ポート 500 番)、ESP パケット(プロトコル番号 50)を許可します。

なお、これら IPv6 アクセスリスト設定は ethernet1 インタフェース設定で登録します。

(**☞**) IPv6 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。

5. <IPsec アクセスリスト設定>

NXR_B(config)#ipsec access-list ipsec_acl ip any any

ipsec_acl という名前の IPsec アクセスリストを設定します。なお、送信元 IPv4 アドレス,宛先 IPv4 アドレスともに any とします。

6. <IPsec ローカルポリシー設定>

NXR_B(config)#ipsec local policy 1

NXR_B(config-ipsec-local)#address ipv6

IPsec トンネルの送信元 IP アドレスを ipv6 と設定します。

7. <IPsec ISAKMP ポリシー設定>

NXR_B(config)#ipsec isakmp policy 1

NXR_B(config-ipsec-isakmp)#description NXR_A

NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey

ISAKMP ポリシーの説明として NXR_A、認証方式として pre-share(事前共有鍵)を選択し、事前共有鍵 ipseckey を設定します。なお、事前共有鍵は NXR_A と共通の値を設定します。

NXR_B(config-ipsec-isakmp)#hash sha1

NXR_B(config-ipsec-isakmp)#encryption aes128

NXR_B(config-ipsec-isakmp)#group 5

NXR_B(config-ipsec-isakmp)#lifetime 10800

NXR_B(config-ipsec-isakmp)#isakmp-mode main

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

NXR_B(config-ipsec-isakmp)#remote address ipv6 2001:0db8:1:1::1

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

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

リモートアドレスに NXR_A の IPv6 アドレスを設定します。また、IKE KeepAlive(DPD)を監視間隔 30 秒,リトライ回数 3 回とし keepalive 失敗時に SA を削除し IKE のネゴシエーションを開始するよう設定します。そして、IPsec ローカルポリシー1 と関連づけを行います。

8. <IPsec トンネルポリシー設定>

NXR_B(config)#ipsec tunnel policy 1

NXR B(config-ipsec-tunnel)#description NXR A

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

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

NXR B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac

NXR_B(config-ipsec-tunnel)#set pfs group5

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

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

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

NXR_B(config-ipsec-tunnel)#match address ipsec_acl

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

9. <トンネル1インタフェース設定>

NXR_B(config)#interface tunnel 1

NXR_B(config-tunnel)#tunnel mode ipsec ipv6

NXR_B(config-tunnel)#tunnel protection ipsec policy 1

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

トンネル 1 インタフェースでトンネルモードを ipsec ipv6、使用するトンネルポリシーとして 1 を設定します。また、IPv4 TCP MSS の調整機能をオートに設定します。

10. <WAN 側(ethernet1)インタフェース設定>

 ${\rm NXR_B}({\rm config}) \# interface \ ethernet \ 1$

NXR_B(config-if)#**no ip address**

ethernet1 インタフェースの IPv4 アドレスを無効に設定します。

NXR_B(config-if)#ipv6 dhcp client pd dhcpv6pd

DHCPv6 クライアントで IPv6 プレフィックスの名前を定義します。

NXR_B(config-if)#ipv6 address dhcpv6pd ::1/64

ethernet1 インタフェースの IPv6 アドレスを設定します。

(ほ) DHCPv6 クライアントで取得した IPv6 プレフィックスを使用し、プレフィックス以降は::1/64 とします。

NXR_B(config-if)#ipv6 nd accept-ra

RA を受信するように設定します。

NXR_B(config-if)#ipv6 access-group in eth1_in

NXR_B(config-if)#ipv6 spi-filter

IPv6 アクセスリスト eth1_in を in フィルタに適用し、IPv6 ステートフルパケットインスペクションを有効に設定します。

NXR_B(config-if)#ipsec policy 1

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

【端末の設定例】

	LAN_A の端末	LAN_B の端末
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	
デフォルトゲートウェイ	192.168.10.1	192.168.20.1

付録

設定例 show config 形式サンプル

設定例 show config 形式サンプル

1-1. IPv4 PPPoE+IPv6 ブリッジ設定

```
! Century Systems NXR-G100 Series ver 6.6.5 (build 9/21:09 19 05 2015)
    DIP-SW: 1:off 2:off 3:off 4:off
hostname nxrg100
telnet-server enable
http-server enable
system power-management mode balance
ipv6 forwarding
fast-forwarding enable
ppp account username test1@example.jp password test1pass
interface ppp 0
 ip address negotiated
 ip tcp adjust-mss auto
 ip masquerade
 ip spi-filter
ppp username test1@example.jp
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
dhcp-server 1
 network 192.168.10.0/24 range 192.168.10.200 192.168.10.210
 gateway 192.168.10.1
 dns-server 192.168.10.1
ipv6 bridge ethernet 0 ethernet 1
ip route 0.0.0.0/0 ppp 0
```

```
!
end
```

2-1. IPv6 PPPoE 接続設定

```
! Century Systems NXR-G100 Series ver 6.6.5 (build 9/21:09 19 05 2015)
    DIP-SW: 1:off 2:off 3:off 4:off
hostname nxrg100
telnet-server enable
http-server enable
system power-management mode balance
ipv6 forwarding
no fast-forwarding enable
ppp account username test1@v6.example.jp password test1pass
interface ppp 0
no ip address
 ipv6 access-group in ppp0_in
 ipv6 spi-filter
 ipv6 dhcp client ipv6dhcpc
 ipv6 tcp adjust-mss auto
 ppp username test1@v6.example.jp
 no ppp ipcp enable
ppp ipv6cp enable
interface ethernet 0
 no ip address
ipv6 address dhcpv6pd ::1/64
 ipv6 nd other-config-flag
 ipv6 nd send-ra
 ipv6 dhcp server ipv6dhcps
interface ethernet 1
 no ip address
 pppoe-client ppp 0
dns
 service enable
 edns-query enable
syslog
local enable
ipv6 dhcp-client ipv6dhcpc
 ia-pd dhcpv6pd
 option-request dns-servers
ipv6 dhcp-server ipv6dhcps
 option-send dns-server address [DHCPv6 で取得したプレフィックス::1]
```

```
!
!
!
!
!
!
!
ipv6 route ::/0 ppp 0
!
ipv6 access-list ppp0_in permit any any udp any 546
!
end
```

2-2. IPv4+IPv6 PPPoE 接続設定

```
! Century Systems NXR-G100 Series ver 6.6.5 (build 9/21:09 19 05 2015)
    DIP-SW: 1:off 2:off 3:off 4:off
hostname nxrg100
telnet-server enable
http-server enable
system power-management mode balance
ipv6 forwarding
fast-forwarding enable
ppp account username test1@v6.example.jp password test1pass
ppp account username test1@example.jp password test1pass
interface ppp 0
 no ip address
 ipv6 access-group in ppp0_in
 ipv6 spi-filter
 ipv6 dhcp client ipv6dhcpc
 ipv6 tcp adjust-mss auto
 ppp username test1@v6.example.jp
 no ppp ipcp enable
ppp ipv6cp enable
interface ppp 1
ip address negotiated
 ip tcp adjust-mss auto
 ip masquerade
 ip spi-filter
 ppp username test1@example.jp
interface ethernet 0
 ip address 192.168.10.1/24
 ipv6 address dhcpv6pd ::1/64
 ipv6 nd send-ra
interface ethernet 1
 no ip address
 pppoe-client ppp 0
```

```
pppoe-client ppp 1
dns
 service enable
 edns-query enable
syslog
local enable
dhcp-server 1
network 192.168.10.0/24 range 192.168.10.200 192.168.10.210
 gateway 192.168.10.1
 dns-server 192.168.10.1
ipv6 dhcp-client ipv6dhcpc
 ia-pd dhcpv6pd
 option-request dns-servers
ip\ route\ 0.0.0.0/0\ ppp\ 1
ipv6 route ::/0 ppp 0
ipv6 access-list ppp0_in permit any any udp any 546
end
```

3-1. IPv6 IPoE(RA)接続設定

```
! Century Systems NXR-G100 Series ver 6.6.5 (build 9/21:09 19 05 2015)
! DIP-SW: 1:off 2:off 3:off 4:off
! hostname nxrg100
telnet-server enable
http-server enable
!
! system power-management mode balance
!
! ipv6 forwarding
no fast-forwarding enable
!
!!
! interface ethernet 0
no ip address
ipv6 address autoconfig
ipv6 nd other-config-flag
ipv6 nd send-ra
```

```
ipv6 dhcp server ipv6dhcps
interface ethernet 1
 no ip address
 ipv6 access-group in eth1_in
 ipv6 spi-filter
 ipv6 nd accept-ra proxy ethernet 0
 ipv6 dhcp client ipv6dhcpc
dns
service enable
 edns-query enable
syslog
local enable
ipv6 dhcp-client ipv6dhcpc
 information-only enable
 option-request dns-servers
ipv6 dhcp-server ipv6dhcps
 option-send dns-server add dhcp-client ethernet 1
ipv6 access-list eth1_in permit any any icmpv6
ipv6 access-list eth1_in permit any any udp any 546
end
```

3-2. IPv6 IPoE(DHCPv6-PD)接続設定

```
! Century Systems NXR-G100 Series ver 6.6.5 (build 9/21:09 19 05 2015)
! DIP-SW: 1:off 2:off 3:off 4:off
! hostname nxrg100
telnet-server enable
http-server enable
!
! system power-management mode balance
!
! ipv6 forwarding
no fast-forwarding enable
!
!
! ipterface ethernet 0
no ip address
ipv6 address dhcpv6pd::/64 eui-64
```

```
ipv6 nd other-config-flag
 ipv6 nd send-ra
 ipv6 dhcp server ipv6dhcps
interface ethernet 1
 no ip address
 ipv6 access-group in eth1_in
 ipv6 spi-filter
 ipv6 nd accept-ra
 ipv6 dhcp client ipv6dhcpc
dns
 service enable
 edns-query enable
syslog
local enable
ipv6 dhcp-client ipv6dhcpc
 ia-pd dhcpv6pd
 option-request dns-servers
ipv6 dhcp-server ipv6dhcps
 option-send dns-server add dhcp-client ethernet 1
ipv6 access-list eth1_in permit any any icmpv6
ipv6 access-list eth1_in permit any any udp any 546
end
```

3-3. IPv4 PPPoE+IPv6 IPoE(RA)接続設定

```
! Century Systems NXR-G100 Series ver 6.6.5 (build 9/21:09 19 05 2015)
! DIP-SW: 1:off 2:off 3:off 4:off
! hostname nxrg100
telnet-server enable
http-server enable
!
! system power-management mode balance
!
! ipv6 forwarding
fast-forwarding enable
!
! ppp account username test1@example.jp password test1pass
!
```

```
interface ppp 0
 ip address negotiated
 ip tcp adjust-mss auto
 ip masquerade
 ip spi-filter
ppp username test1@example.jp
interface ethernet 0
ip address 192.168.10.1/24
 ipv6 address autoconfig
ipv6 nd send-ra
interface ethernet 1
 no ip address
 ipv6 access-group in eth1_in
 ipv6 spi-filter
 ipv6 nd accept-ra proxy ethernet 0
 ipv6 dhcp client ipv6dhcpc
pppoe-client ppp 0
dns
 service enable
 edns-query enable
syslog
local enable
dhcp-server 1
 network 192.168.10.0/24 range 192.168.10.200 192.168.10.210
 gateway 192.168.10.1
 dns-server 192.168.10.1
ipv6 dhcp-client ipv6dhcpc
information-only enable
 option-request dns-servers
ip route 0.0.0.0/0 ppp 0
ipv6 access-list eth1_in permit any any icmpv6
ipv6 access-list eth1_in permit any any udp any 546
end
```

3-4. IPv4 PPPoE+IPv6 IPoE(DHCPv6-PD)接続設定

```
!
! Century Systems NXR-G100 Series ver 6.6.5 (build 9/21:09 19 05 2015)
! DIP-SW: 1:off 2:off 3:off 4:off
!
hostname nxrg100
telnet-server enable
http-server enable
!
```

```
system power-management mode balance
ipv6 forwarding
fast-forwarding enable
ppp account username test1@example.jp password test1pass
interface ppp 0
 ip address negotiated
 ip tcp adjust-mss auto
 ip masquerade
 ip spi-filter
ppp username test1@example.jp
interface ethernet 0
 ip address 192.168.10.1/24
 ipv6 address dhcpv6pd ::/64 eui-64
 ipv6 nd send-ra
interface ethernet 1
 no ip address
 ipv6 access-group in eth1_in
 ipv6 spi-filter
 ipv6 nd accept-ra
 ipv6 dhcp client ipv6dhcpc
pppoe-client ppp 0
dns
 service enable
 edns-query enable
syslog
local enable
dhcp-server 1
 network 192.168.10.0/24 range 192.168.10.200 192.168.10.210
 gateway 192.168.10.1
 dns-server 192.168.10.1
ipv6 dhcp-client ipv6dhcpc
 ia-pd dhcpv6pd
 option-request dns-servers
ip route 0.0.0.0/0 ppp 0
ipv6 access-list eth1_in permit any any icmpv6
ipv6 access-list eth1_in permit any any udp any 546
```

end

4-1. IPv6 PPPoE IPsec 接続設定

[NXR_A の設定]

```
! Century Systems NXR-G100 Series ver 6.6.5 (build 9/21:09 19 05 2015)
    DIP-SW: 1:off 2:off 3:off 4:off
hostname NXR_A
telnet-server enable
http-server enable
system power-management mode balance
ipv6 forwarding
no fast-forwarding enable
ppp account username test1@v6.example.jp password test1pass
ipsec local policy 1
address ipv6
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ipv6 2001:db8:2:1::1
 local policy 1
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv6
 tunnel protection ipsec policy 1
interface ppp 0
 no ip address
 ipv6 access-group in ppp0_in
 ipv6 spi-filter
 ipv6 address dhcpv6pd ::1/64
 ipv6 dhcp client pd dhcpv6pd
```

```
ipv6 tcp adjust-mss auto
 ppp username test1@v6.example.jp
 no ppp ipcp enable
 ppp ipv6cp enable
 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
ip route 192.168.20.0/24 tunnel 1
ip route 192.168.20.0/24 null 254
ipv6 route ::/0 ppp 0
ipv6 access-list ppp0_in permit any any udp any 546
ipv6 access-list ppp0_in permit 2001:db8:2:1::1 2001:db8:1:1::1 udp 500 500
ipv6 access-list ppp0_in permit 2001:db8:2:1::1 2001:db8:1:1::1 50
ipsec access-list ipsec_acl ip any any
end
```

〔NXR_B の設定〕

```
! Century Systems NXR-G100 Series ver 6.6.5 (build 9/21:09 19 05 2015)
! DIP-SW: 1:off 2:off 3:off 4:off
! hostname NXR_B
telnet-server enable
http-server enable
!
! system power-management mode balance
!
!!
ipv6 forwarding
no fast-forwarding enable
!
!!
ppp account username test2@v6.example.jp password test2pass
```

```
ipsec local policy 1
 address ipv6
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey
 hash shal
 encryption aes128
 group 5
 isakmp-mode main
 remote address ipv6 2001:db8:1:1::1
 local policy 1
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
interface tunnel 1
no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv6
 tunnel protection ipsec policy 1
interface ppp 0
 no ip address
 ipv6 access-group in ppp0_in
 ipv6 spi-filter
 ipv6 address dhcpv6pd ::1/64
 ipv6 dhcp client pd dhcpv6pd
 ipv6 tcp adjust-mss auto
 ppp username test2@v6.example.jp
 no ppp ipcp enable
 ppp ipv6cp enable
 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
```

```
!
ip route 192.168.10.0/24 tunnel 1
ip route 192.168.10.0/24 null 254
!
ipv6 route ::/0 ppp 0
!
ipv6 access-list ppp0_in permit any any udp any 546
ipv6 access-list ppp0_in permit 2001:db8:1:1::1 2001:db8:2:1::1 udp 500 500
ipv6 access-list ppp0_in permit 2001:db8:1:1::1 2001:db8:2:1::1 50
!
ipsec access-list ipsec_acl ip any any
!
end
```

4-2. IPv6 IPoE(RA)IPsec 接続設定(ネームの利用)

〔NXR_A の設定〕

```
! Century Systems NXR-G100 Series ver 6.6.5 (build 9/21:09 19 05 2015)
    DIP-SW: 1:off 2:off 3:off 4:off
hostname NXR_A
telnet-server enable
http-server enable
system power-management mode balance
ipv6 forwarding
no fast-forwarding enable
ipsec local policy 1
 address ipv6
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ipv6 \Delta\Delta\Delta.aoi.flets-east.jp
 local policy 1
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp1\,
 match address ipsec_acl
interface tunnel 1
```

```
no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv6
 tunnel protection ipsec policy 1
interface ethernet 0
 ip address 192.168.10.1/24
interface ethernet 1
no ip address
 ipv6 access-group in eth1_in
 ipv6 spi-filter
 ipv6 address autoconfig
 ipv6 dhcp client ipv6dhcpc
 ipsec policy 1
dns
 service enable
 edns-query enable
syslog
 local enable
ipv6 dhcp-client ipv6dhcpc
 information-only enable
 option-request dns-servers
ip route 192.168.20.0/24 tunnel 1
ip route 192.168.20.0/24 null 254
ipv6 access-list eth1_in permit any any icmpv6
ipv6 access-list eth1_in permit any any udp any 546
ipv6 access-list eth1_in permit any any udp 500 500
ipv6 access-list eth1_in permit any any 50
ipsec access-list ipsec_acl ip any any
end
```

〔NXR_B の設定〕

```
! Century Systems NXR-G100 Series ver 6.6.5 (build 9/21:09 19 05 2015)
! DIP-SW: 1:off 2:off 3:off 4:off
! hostname NXR_B telnet-server enable http-server enable ! ! system power-management mode balance !
```

```
ipv6 forwarding
no fast-forwarding enable
ipsec local policy 1
 address ipv6
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ipv6 OOO.aoi.flets-east.jp
 local policy 1
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv6
 tunnel protection ipsec policy 1
interface ethernet 0
ip address 192.168.20.1/24
interface ethernet 1
 no ip address
 ipv6 access-group in eth1_in
 ipv6 spi-filter
 ipv6 address autoconfig
 ipv6 dhcp client ipv6dhcpc
 ipsec policy 1
dns
service enable
 edns-query enable
syslog
local enable
ipv6 dhcp-client ipv6dhcpc
information-only enable
 option-request dns-servers
```

```
!
!
!
!
ip route 192.168.10.0/24 tunnel 1
ip route 192.168.10.0/24 null 254
!
ipv6 access-list eth1_in permit any any icmpv6
ipv6 access-list eth1_in permit any any udp any 546
ipv6 access-list eth1_in permit any any udp 500 500
ipv6 access-list eth1_in permit any any 50
!
ipsec access-list ipsec_acl ip any any
!
end
```

4-3. IPv6 IPoE(DHCPv6-PD)IPsec 接続設定

[NXR_A の設定]

```
! Century Systems NXR-G100 Series ver 6.6.5 (build 9/21:09 19 05 2015)
    DIP-SW: 1:off 2:off 3:off 4:off
hostname NXR_A
telnet-server enable
http-server enable
system power-management mode balance
ipv6 forwarding
no fast-forwarding enable
ipsec local policy 1
 address ipv6
ipsec isakmp policy 1
 description NXR_B
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ipv6 2001:db8:2:1::1
 local policy 1
ipsec tunnel policy 1
 description NXR_B
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
```

```
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv6
 tunnel protection ipsec policy 1
interface ethernet 0
ip address 192.168.10.1/24
interface ethernet 1
no ip address
 ipv6 access-group in eth1_in
 ipv6 spi-filter
 ipv6 address dhcpv6pd ::1/64
 ipv6 nd accept-ra
 ipv6 dhcp client pd dhcpv6pd
 ipsec policy 1
dns
 service enable
syslog
 local enable
ip route 192.168.20.0/24 tunnel 1
ip route 192.168.20.0/24 null 254
ipv6 access-list eth1_in permit any any icmpv6
ipv6 access-list eth1_in permit any any udp any 546
ipv6 access-list eth1_in permit 2001:0db8:2:1::1 2001:0db8:1:1::1 udp 500 500
ipv6 access-list eth1_in permit 2001:0db8:2:1::1 2001:0db8:1:1::1 50
ipsec access-list ipsec_acl ip any any
end
```

〔NXR_B の設定〕

```
! Century Systems NXR-G100 Series ver 6.6.5 (build 9/21:09 19 05 2015)
! DIP-SW: 1:off 2:off 3:off 4:off
! hostname NXR_B telnet-server enable http-server enable ! ! system power-management mode balance ! ! ! ipv6 forwarding
```

```
no fast-forwarding enable
ipsec local policy 1
 address ipv6
ipsec isakmp policy 1
 description NXR_A
 authentication pre-share ipseckey
 hash sha1
 encryption aes128
 group 5
 isakmp-mode main
 remote address ipv6 2001:db8:1:1::1
 local policy 1
ipsec tunnel policy 1
 description NXR_A
 set transform esp-aes128 esp-sha1-hmac
 set pfs group5
 set key-exchange isakmp 1
 match address ipsec_acl
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv6
 tunnel protection ipsec policy 1
interface ethernet 0
ip address 192.168.20.1/24
interface ethernet 1
 no ip address
 ipv6 access-group in eth1_in
 ipv6 spi-filter
 ipv6 address dhcpv6pd ::1/64
 ipv6 nd accept-ra
 ipv6 dhcp client pd dhcpv6pd
 ipsec policy 1
dns
 service enable
syslog
local enable
ip route 192.168.10.0/24 tunnel 1
ip route 192.168.10.0/24 null 254
```

```
!
ipv6 access-list eth1_in permit any any icmpv6
ipv6 access-list eth1_in permit any any udp any 546
ipv6 access-list eth1_in permit 2001:0db8:1:1::1 2001:0db8:2:1::1 udp 500 500
ipv6 access-list eth1_in permit 2001:0db8:1:1::1 2001:0db8:2:1::1 50
!
ipsec access-list ipsec_acl ip any any
!
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

サポートデスクのご利用に関して

サポートデスクへのお問い合わせに関して

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

※FutureNet サポートデスク宛にご提供頂きました情報は、製品のお問合せなどサポート業務以外の目的には利用致しません。

なおご提供頂く情報の取り扱いについて制限等がある場合には、お問い合わせ時または事前にその旨ご連絡下さい。(設定ファイルのプロバイダ情報や IPsec の事前共有鍵情報を削除してお送り頂く場合など) 弊社のプライバシーポリシーについては下記 URL の内容をご確認下さい。

http://www.centurysys.co.jp/company/philosophy.html#tab3

http://www.centurysys.co.jp/company/philosophy.html#tab4

- ご利用頂いている NXR,WXR 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
 - ○月○日○○時○○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。設定例集および設定例集内のログ一覧は未確認。

□ 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,WXR 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,WXR 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,WXR 製品のテクニカルサポート情報の結果 テクニカルサポート情報は以下のコマンドで出力されます。

show tech-support

■ 障害発生時のモバイル関連コマンドの実行結果(モバイルカード利用時のみ)

#show mobile <N> ap

#show mobile <N> phone-number

#show mobile <N> signal-level

※<N>はモバイルデバイスナンバ

サポートデスクのご利用に関して

電話サポート

電話番号:0422-37-8926

電話での対応は以下の時間帯で行います。

月曜日 ~ 金曜日 10:00 - 17:00

ただし、国の定める祝祭日、弊社の定める年末年始は除きます。

電子メールサポート

E-mail: support@centurysys.co.jp

FAXサポート

FAX 番号: **0422-55-3373**

電子メール、FAX は 毎日 24 時間受け付けております。

ただし、システムのメンテナンスやビルの電源点検のため停止する場合があります。 その際は弊社ホーム ページ等にて事前にご連絡いたします。

FutureNet NXR,WXR シリーズ

設定例集

IPv6 編

Ver 1.1.0

2015年9月

発行 センチュリー・システムズ株式会社

 $Copyright(c)\ 2009\text{-}2015\ Century\ Systems\ Co.,\ Ltd.\ All\ Rights\ Reserved.$