インターネット VPN 対応ルータ

FutureNet XR シリーズ

インターネット VPN 設定例集

IPsec 編

Ver 1.3.0

センチュリー・システムズ株式会社

目次

はじめに

本書は XR シリーズを利用した設定例集になります。
本書を利用する際は、各製品のユーザーズガイドも合わせてご利用下さい。

注意事項

- 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 XR-510/C, XR-540/C Ver3.2.0 をベースに作成しております。IPsec および IPsec KeepAlive 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。
- 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。

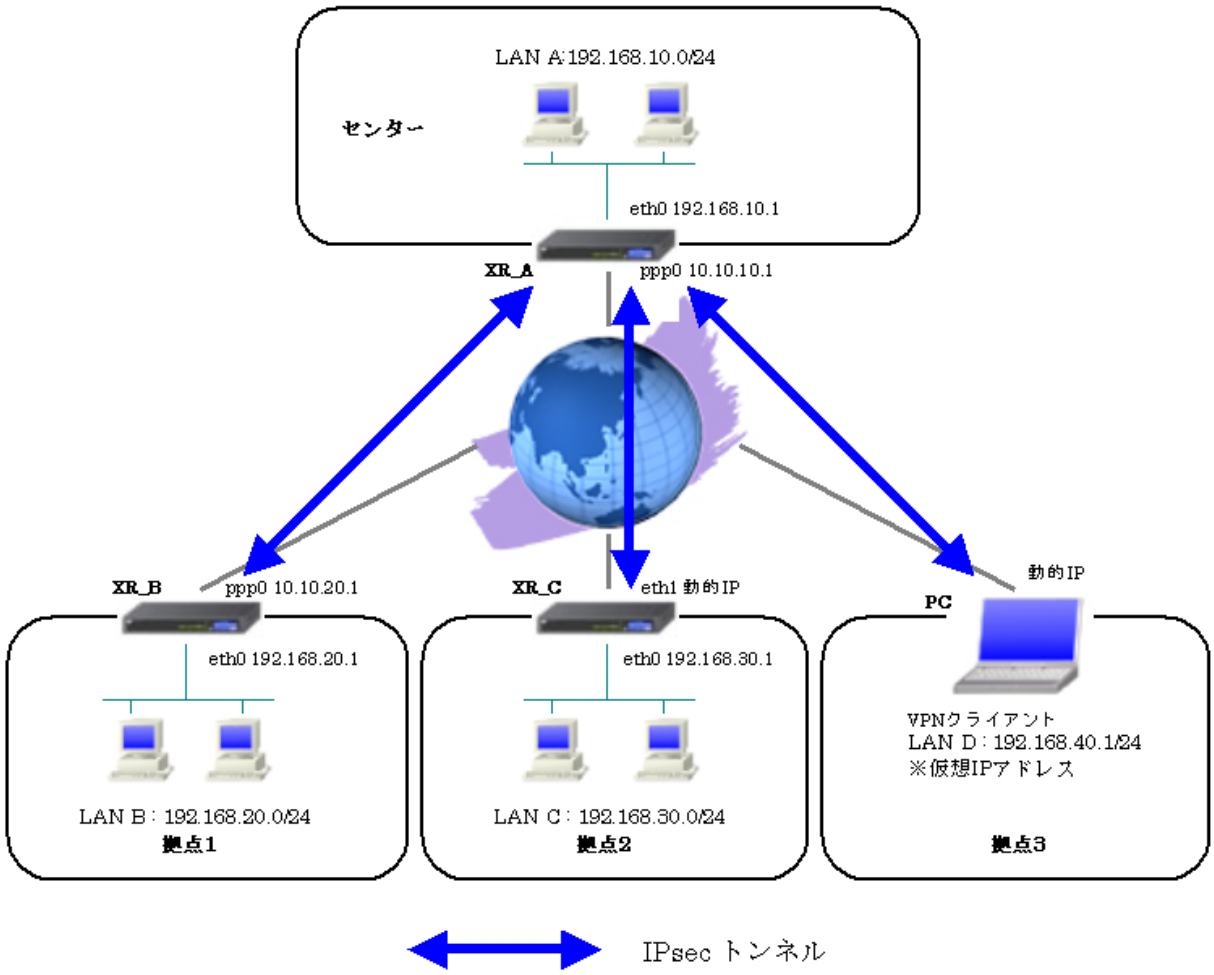
改版履歴

Version	更新内容
1.1.0	初版
1.2.0	NAT-Traversal 設定例２追加 設定例構成図変更
1.3.0	複数セグメントでの IPsec 設定例追加 IPsec での NAT 利用例追加

1. 様々な接続形態での IPsec 接続例

この例は、PPPoE や DHCP クライアントでの接続で IPsec によるインターネット VPN を実現する設定例です。また PC にインストールして使用する VPN クライアント「FutureNet VPN Client/Net-G」を利用することにより、外出先などのリモートからも IPsec によるインターネット VPN が利用可能です。この例では、PPP 回線を利用した VPN クライアントによるリモートアクセスを実現しています。

1-1. 構成例



1-2. 要件

- インタフェースおよび PPPoE

  - XR_A(センター), XR_B(拠点 1)はインターネットに PPPoE で接続します。
  - XR_C(拠点 2)はインターネットに Ether(DHCP クライアント)で接続します。
  - PC(拠点 3)はインターネットに PPP で接続します。
  - PPPoE 接続は、自動再接続するように設定しています。
  - WAN 側インタフェースの 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は「有効」にしています。

主なインタフェースおよび PPPoE のパラメータ

	XR_A(センター)	XR_B(拠点 1)	XR_C(拠点 2)	PC(拠点 3)
LAN 側インタフェース	Ether0	Ether0	Ether0	-
LAN 側 IP アドレス	192.168.10.1	192.168.20.1	192.168.30.1	
WAN 側インタフェース	Ether1[ppp0]	Ether1[ppp0]	Ether1	-
WAN 側 IP アドレス	10.10.10.1	10.10.20.1	動的 IP	動的 IP
PPPoE ユーザ名	test1@centurysys	test2@centurysys	-	test3
PPPoE パスワード	test1pass	test2pass	-	test3
接続回線	PPPoE 接続	PPPoE 接続	Ether 接続	PPP 接続

➢ IPsec

- 鍵交換モードは XR_A <-> XR_B はメインモード, XR_A <-> XR_C, XR_A <-> PC はアグレッシブモードを使用しています。
- XR_A(センター)は 192.168.10.0/24 <-> 192.168.20.0/24, 192.168.30.0/24, 192.168.40.1/32 の時に IPsec を適用します。
- XR_B(拠点 1)は 192.168.20.0/24 <-> 192.168.10.0/24 の時に IPsec を適用します。
- XR_C(拠点 2)は 192.168.30.0/24 <-> 192.168.10.0/24 の時に IPsec を適用します。
- PC(拠点 3)は 192.168.40.1/32 <-> 192.168.10.0/24 の時に IPsec を適用します。
- IPsec KeepAlive は拠点のみ(PC 拠点 3 は除く)に使用しています。

本装置側のパラメータ

	XR_A(センター)	XR_B(拠点 1)	XR_C(拠点 2)
インタフェースの IP アドレス	10.10.10.1	10.10.20.1	%eth1
上位ルータの IP アドレス	%ppp0	%ppp0	
インタフェースの ID			@ipsec2

IKE/ISAKMP ポリシーのパラメータ(1) 「XR_A(センター)」

	XR_A(センター)		
対向拠点	XR_B(拠点 1)	XR_C(拠点 2)	PC(拠点 3)
IKE/ISAKMP ポリシー名	XR_B	XR_C	PC
リモート IP アドレス	10.10.20.1	0.0.0.0	0.0.0.0
インタフェースの ID		@ipsec2	@vpnclient
モード	Main	Aggressive	Aggressive
暗号化アルゴリズム	AES-128	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1	SHA1
DH グループ	Group2	Group2	Group2
ライフタイム	3600(秒)	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey2	ipseckey3

IPsec ポリシーのパラメータ(1) 「XR_A(センター)」

	XR_A(センター)		
対向拠点	XR_B(拠点 1)	XR_C(拠点 2)	PC(拠点 3)
使用する IKE ポリシー名	XR_B(IKE1)	XR_C(IKE2)	PC(IKE3)
本装置の LAN 側のネットワークアドレス	192.168.10.0/24	192.168.10.0/24	192.168.10.0/24
相手側の LAN 側のネットワークアドレス	192.168.20.0/24	192.168.30.0/24	192.168.40.1/32
暗号化アルゴリズム	AES-128	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1	SHA1
PFS(DH グループ)	使用する(Group2)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)	28800(秒)
DISTANCE	1	1	1

IKE/ISAKMP ポリシーのパラメータ(2) 「XR_B(拠点 1), XR_C(拠点 2)」

	XR_B(拠点 1)	XR_C(拠点 2)
対向拠点	XR_A(センター)	XR_A(センター)
IKE/ISAKMP ポリシー名	XR_A	XR_A
リモート IP アドレス	10.10.10.1	10.10.10.1
モード	Main	Aggressive
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
DH グループ	Group2	Group2
ライフタイム	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey2

IPsec ポリシーのパラメータ(2) 「XR_B(拠点 1), XR_C(拠点 2)」

	XR_B(拠点 1)	XR_C(拠点 2)
対向拠点	XR_A(センター)	XR_A(センター)
使用する IKE ポリシー名	XR_A(IKE1)	XR_A(IKE1)
本装置の LAN 側のネットワークアドレス	192.168.20.0/24	192.168.30.0/24
相手側の LAN 側のネットワークアドレス	192.168.10.0/24	192.168.10.0/24
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
PFS(DH グループ)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)
DISTANCE	1	1

IPsec Keepalive のパラメータ

	XR_A(センター)	XR_B(拠点 1)	XR_C(拠点 2)
対向拠点	XR_B(拠点 1)	XR_A(センター)	XR_A(センター)
Policy No.	1	1	1
source address	192.168.10.1	192.168.20.1	192.168.30.1
destination address	192.168.20.1	192.168.10.1	192.168.10.1
interval(sec)	30	45	45
watch count	3	3	3
timeout/delay(sec)	60	60	60
動作 option	1	1	2
interface	ipsec0	ipsec0	ipsec6

1-3. 設定例

センタールータ（XR_A）

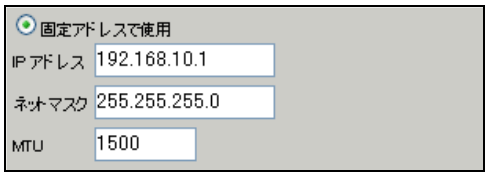
ポイント

拠点 1～3 と IPsec 接続するための設定を行います。

拠点 2, 3 は動的 IP のため、アグレッシブモードを使用しています。

<<インタフェース設定>>

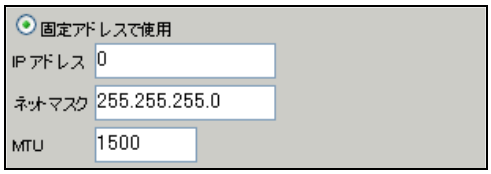
[Ethernet0 の設定]



Ethernet0 に関する設定をします。

※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

[Ethernet1 の設定]

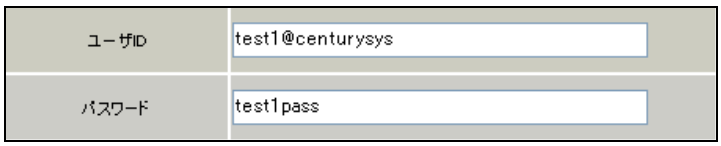


Ethernet1 に関する設定をします。

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

<<PPP/PPPoE 設定>>

[接続先設定 1]



PPPoE 接続で使用するユーザ ID，パスワードを登録します。

［接続設定］

接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ◉Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ○RS232C
接続形態	○手動接続 ◉常時接続 ○スケジューラ接続
RS232C/BRI接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	○無効 ◉有効
ステートフルパケット インスペクション	○無効 ◉有効 ☐DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ◉有効

PPPoE 接続するインタフェース、および接続形態を選択します。
※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション (全回線共通)	☑回線接続時に前回のPPPoEセッションのPADTを強制送出 ☑非接続SessionのIPv4Packet受信時にPADTを強制送出 ☑非接続SessionのLCP-EchoRequest受信時にPADTを強制送出

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

<<フィルタ設定>>

［入力フィルタ］

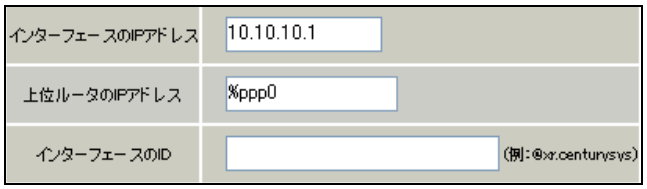
インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	udp		500		500	☐
ppp0	パケット受信時	許可	esp					☐

IKE パケット，ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

<IPsec サーバ>

[本装置側の設定 1]

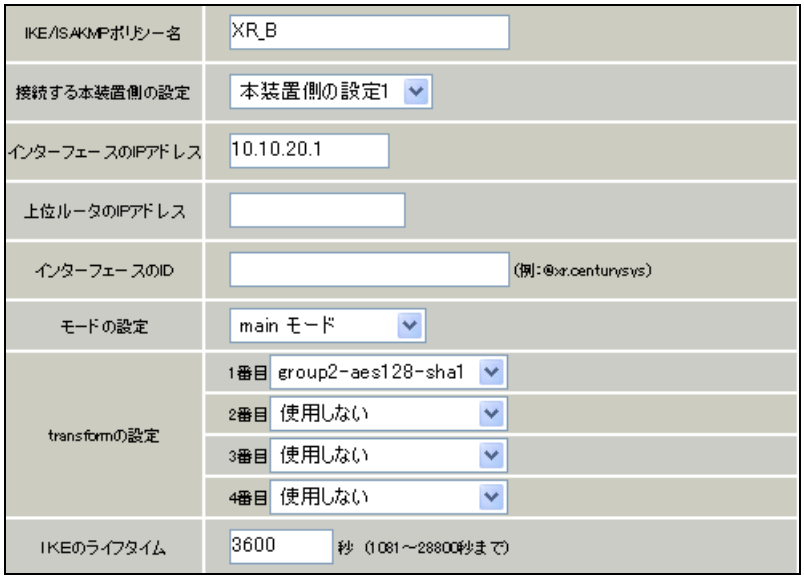


XR_A(センター)の WAN 側インタフェースの IP アドレス,および上位ルータの IP アドレスを設定します。
PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

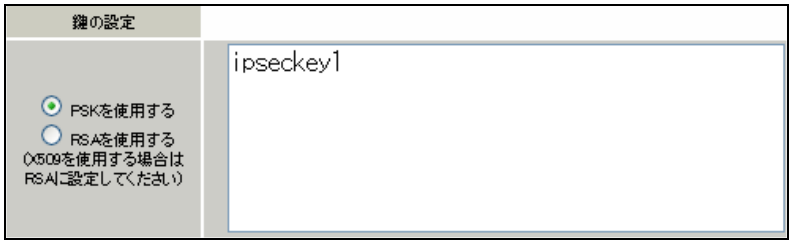
[IKE/ISAKMP の設定 1]

IKE/ISAKMP ポリシーのパラメータは以下のとおりです。

設定項目	パラメータ
IKE/ISAKMP ポリシー名	XR_B
リモート IP アドレス	10.10.20.1
モード	Main
暗号化アルゴリズム	AES-128
認証アルゴリズム	SHA1
DH グループ	Group2
ライフタイム	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1



XR_B(拠点 1)に対する IKE/ISAKMP ポリシーを設定します。



事前共有鍵(PSK)として「ipseckey1」を設定しています。

[IPsec ポリシーの設定 1]

XR_B(拠点 1)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

IPsec ポリシーのパラメータは以下のとおりです。

設定項目	パラメータ
使用する IKE ポリシー名	XR_B(IKE1)
本装置の LAN 側のネットワークアドレス	192.168.10.0/24
相手側の LAN 側のネットワークアドレス	192.168.20.0/24
暗号化アルゴリズム	AES-128
認証アルゴリズム	SHA1
PFS(DH グループ)	使用する(Group2)
ライフタイム	28800(秒)
DISTANCE	1

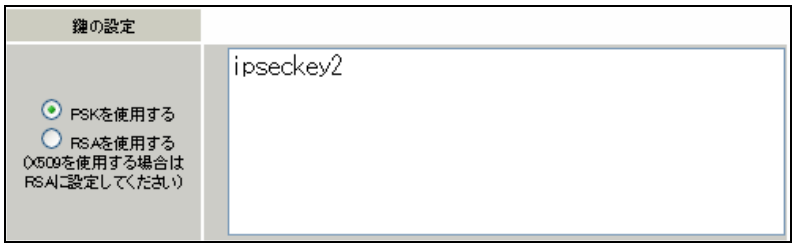
XR_B(拠点 1)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

[IKE/ISAKMP の設定 2]

IKE/ISAKMP ポリシーのパラメータは以下のとおりです。

設定項目	パラメータ
IKE/ISAKMP ポリシー名	XR_C
リモート IP アドレス	0.0.0.0
インタフェースの ID	@ipsec2
モード	Aggressive
暗号化アルゴリズム	AES-128
認証アルゴリズム	SHA1
DH グループ	Group2
ライフタイム	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey2

XR_C(拠点 2)に対する IKE/ISAKMP ポリシーの設定を行います。



事前共有鍵(PSK)として「ipseckey2」を設定します。

[IPsec ポリシーの設定 2]

XR_C(拠点 2)の IP アドレスが不定のため、「Responder として使用する」を選択します。

IPsec ポリシーのパラメータは以下のとおりです。

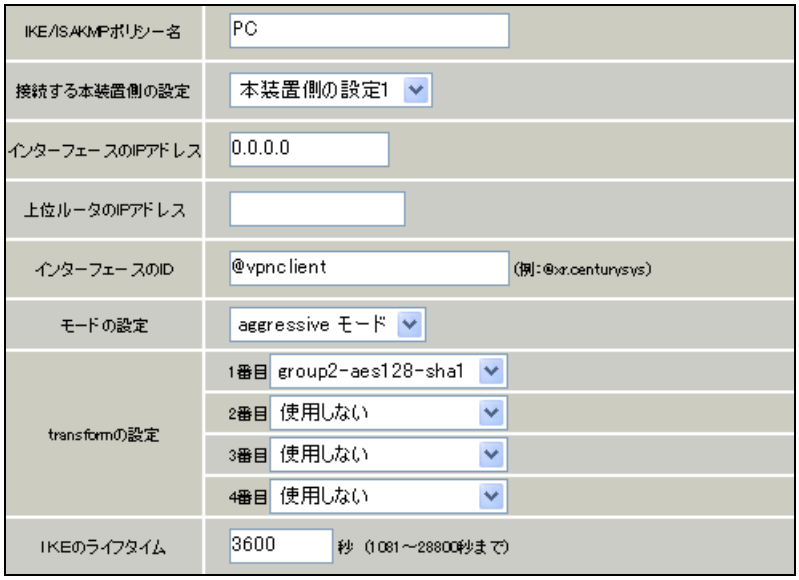
設定項目	パラメータ
使用する IKE ポリシー名	XR_C(IKE2)
本装置の LAN 側のネットワークアドレス	192.168.10.0/24
相手側の LAN 側のネットワークアドレス	192.168.30.0/24
暗号化アルゴリズム	AES-128
認証アルゴリズム	SHA1
PFS(DH グループ)	使用する(Group2)
ライフタイム	28800(秒)
DISTANCE	1

XR_C(拠点 2)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

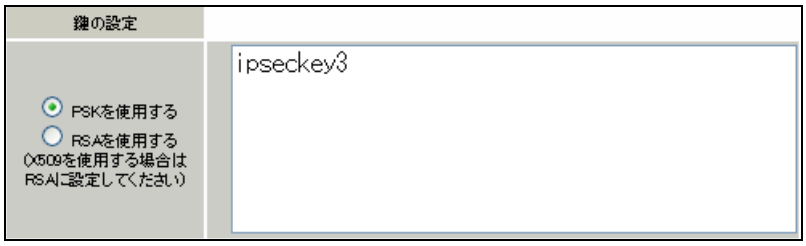
[IKE/ISAKMP の設定 3]

IKE/ISAKMP ポリシーのパラメータは以下のとおりです。

設定項目	パラメータ
IKE/ISAKMP ポリシー名	PC
リモート IP アドレス	0.0.0.0
インタフェースの ID	@vpnclient
モード	Aggressive
暗号化アルゴリズム	AES-128
認証アルゴリズム	SHA1
DH グループ	Group2
ライフタイム	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey3



PC(拠点 3)に対する IKE/ISAKMP ポリシーの設定を行います。

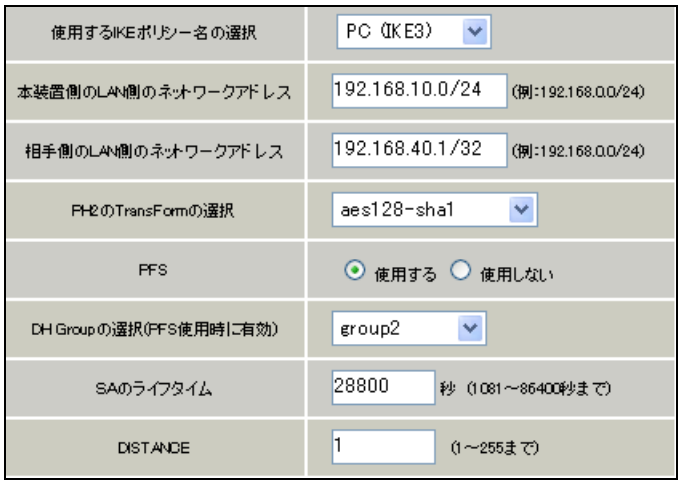


事前共有鍵(PSK)として「ipseckey3」を設定します。

[IPsec ポリシーの設定 3]

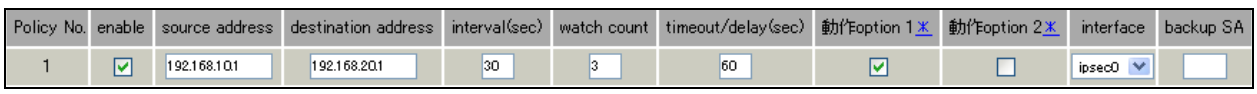
PC(拠点 3)の IP アドレスが不定のため、「Responder として使用する」を選択します。

設定項目	パラメータ
使用する IKE ポリシー名	PC(IKE3)
本装置の LAN 側のネットワークアドレス	192.168.10.0/24
相手側の LAN 側のネットワークアドレス	192.168.40.1/32
暗号化アルゴリズム	AES-128
認証アルゴリズム	SHA1
PFS(DH グループ)	使用する(Group2)
ライフタイム	28800(秒)
DISTANCE	1



PC(拠点 3)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

[IPsec Keep-Alive 設定]



XR_B(拠点 1)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

IPsec サーバ機能を起動します。

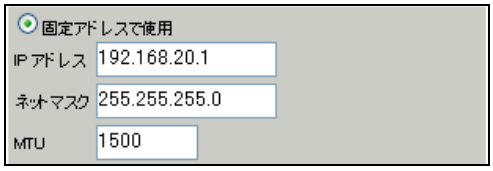
拠点 1 ルータ（XR_B）

ポイント

XR_A(センター)に対して IPsec 接続を行います。XR_A，XR_B ともに WAN 側 IP アドレスが固定 IP アドレスであるため、鍵交換モードとして「Main モード」を使用しています。

<<インタフェース設定>>

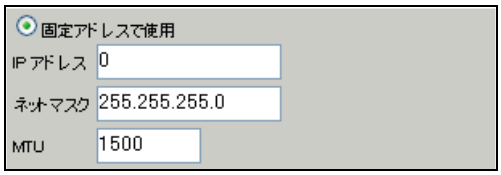
[Ethernet0 の設定]



Ethernet0 の設定をします。

※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

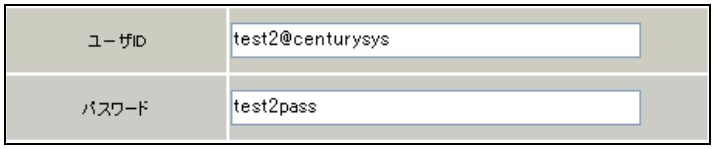
[Ethernet1 の設定]



PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

<<PPP/PPPoE 設定>>

[接続先設定１]



PPPoE 接続で使用するユーザ ID，パスワードを登録します。

［接続設定］

接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ◉Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ○RS232C
接続形態	○手動接続 ◉常時接続 ○スケジューラ接続
RS232C/BRI接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	○無効 ◉有効
ステートフルパケット インスペクション	○無効 ◉有効 ☐DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ◉有効

PPPoE 接続するインタフェース、および接続形態を選択します。
※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション (全回線共通)	☑回線接続時に前回のPPPoEセッションのPADTを強制送出 ☑非接続SessionのIPv4Packet受信時にPADTを強制送出 ☑非接続SessionのLCP-EchoRequest受信時にPADTを強制送出

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

<<フィルタ設定>>

［入力フィルタ］

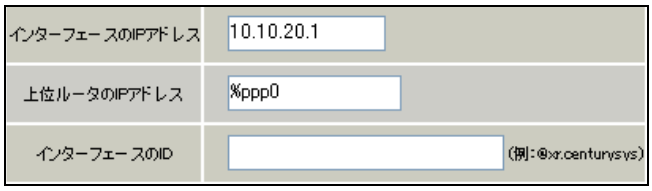
インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	udp		500		500	☐
ppp0	パケット受信時	許可	esp					☐

IKE パケット，ESP パケットの「許可」を設定します。

<<各種サービスの設定>>

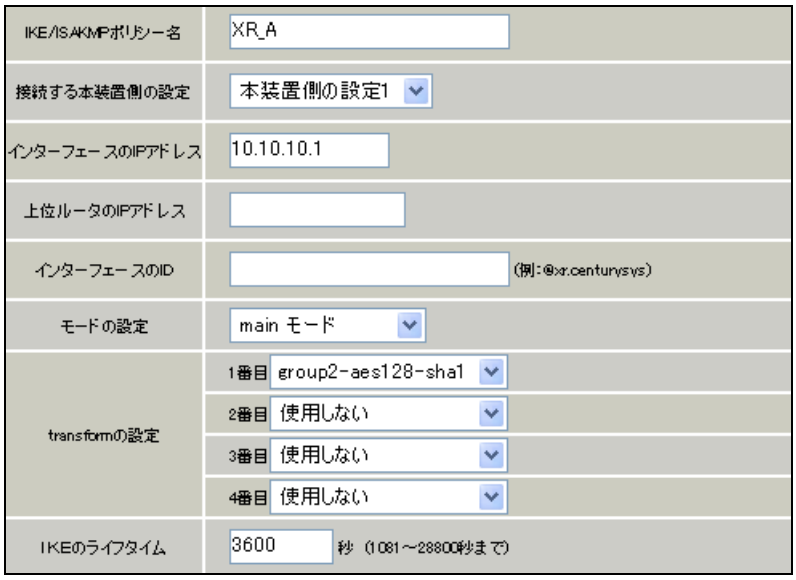
<IPsec サーバ>

[本装置側の設定 1]

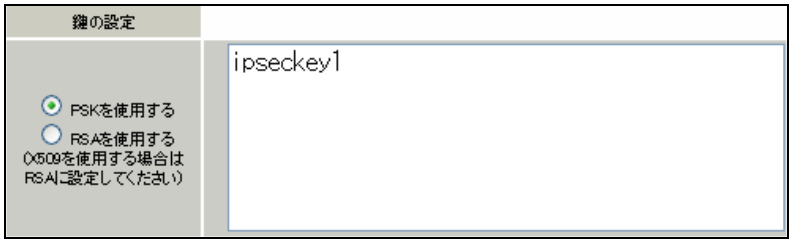


WAN 側インタフェースの IP アドレス，および上位ルータの IP アドレスを設定します。

[IKE/ISAKMP の設定 1]



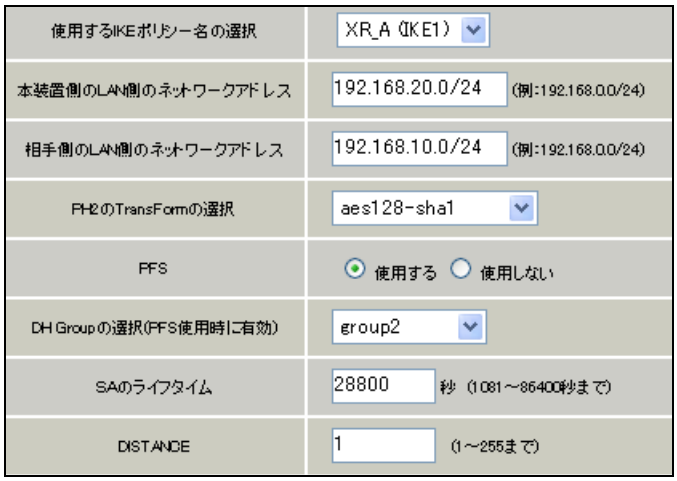
XR_A(センター)に対する ISAKMP ポリシーの設定を行います。



事前共有鍵(PSK)として「ipseckey1」を設定します。

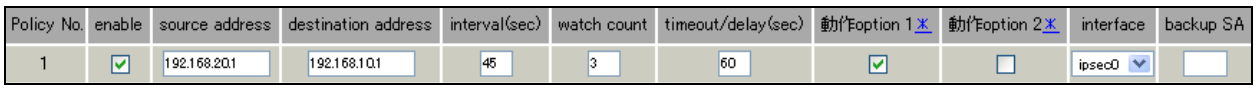
[IPsec ポリシーの設定 1]

XR_A(センター)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。



XR_A(センター)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

[IPsec Keep-Alive 設定]



XR_A(センター)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

IPsec サーバ機能を起動します。

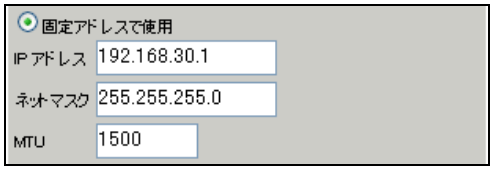
拠点 2 ルータ（XR_C）

ポイント

XR_A(センター)に対して IPsec 接続を行います。WAN 側 IP アドレスが動的 IP アドレスであるため、鍵交換モードとして「Aggressive モード」を使用しています。

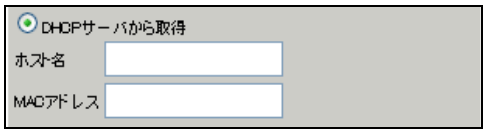
<<インタフェース設定>>

[Ethernet0 の設定]

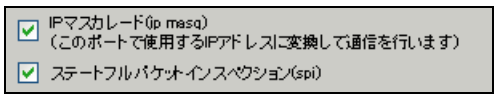


Ethernet0 の設定をします。
※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

[Ethernet1 の設定]



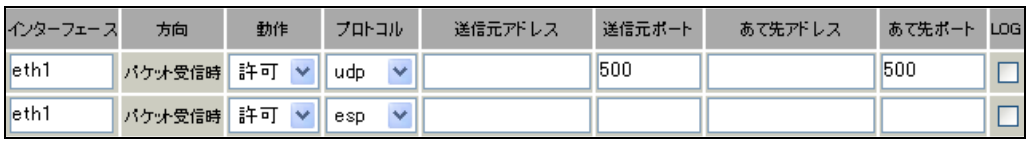
DHCP サーバから IP アドレスを取得するため、「DHCP サーバから取得」を選択します。



ルータ経由でインターネットアクセスを行う場合、IP マスカレード設定を「有効」にしています。ステートフルパケットインスペクション(SPI)を「有効」に設定します。

<<フィルタ設定>>

[入力フィルタ]

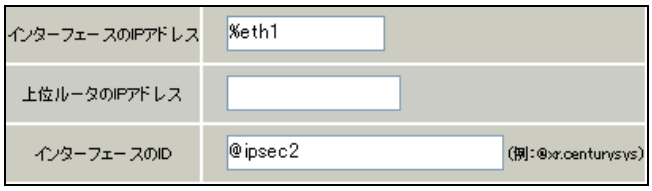


IKE パケット，ESP パケットの「許可」を設定します。

<<各種サービスの設定>>

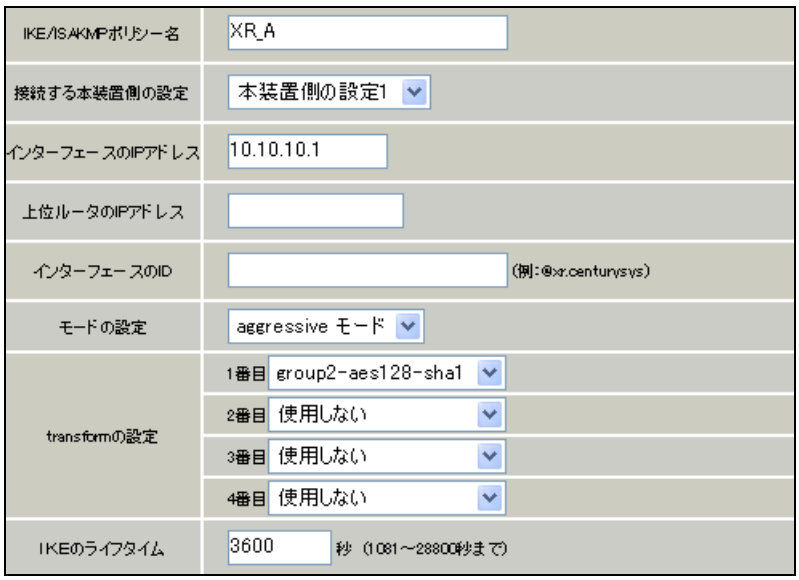
<IPsec サーバ>

[本装置側の設定 1]

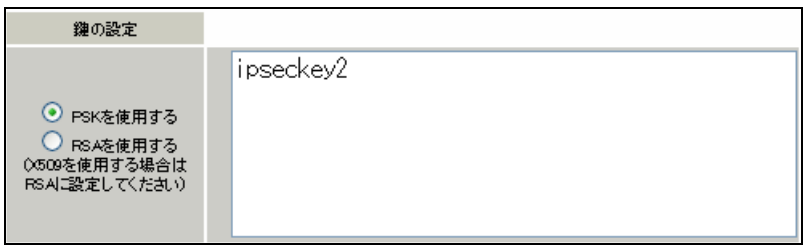


Ethernet 接続(DHCP クライアント)で WAN 側(Ether1)インタフェースの IP アドレスが不定のためインタフェースの IP アドレスに「%eth1」, インタフェースの ID として「@ipsec2」を設定します。

[IKE/ISAKMP の設定 1]



XR_A(センター)に対する IKE/ISAKMP ポリシーの設定を行います。



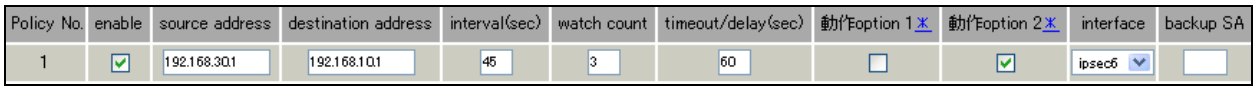
事前共有鍵(PSK)として「ipseckey2」を設定します。

[IPsec ポリシーの設定 1]

XR_A(センター)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

XR_A(センター)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

[IPsec Keep-Alive 設定]



XR_A(センター)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

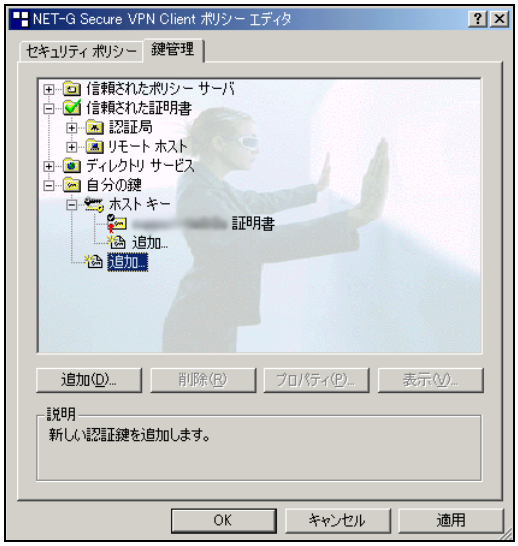
IPsec サーバ機能を起動します。

拠点 3 PC（PC）

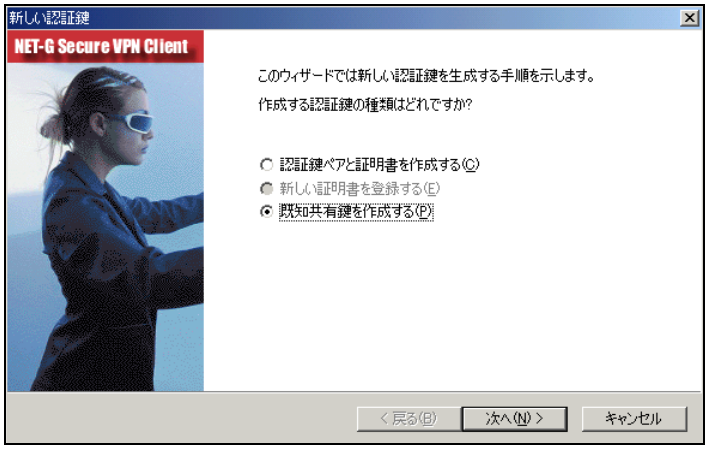
ポイント

拠点 3 は「FutureNet VPN Client/NET-G」をインストールした PC からの IPsec 接続になります。この例では、PPP 接続による Internet へのアクセスが可能になっている状態とします。

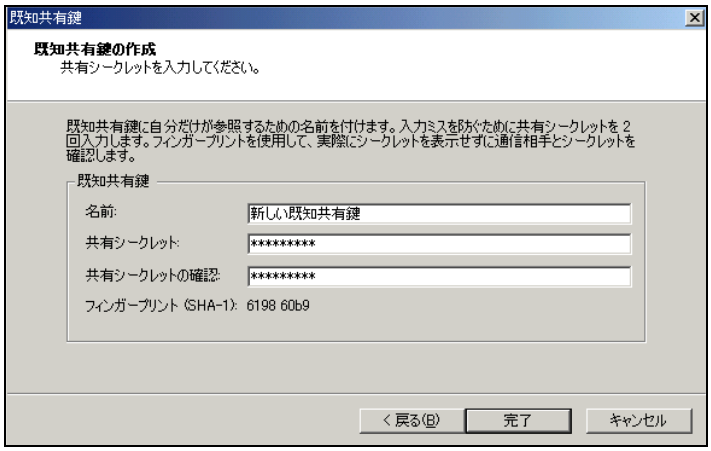
<<既知共有鍵(Pre shared Key)の設定>>



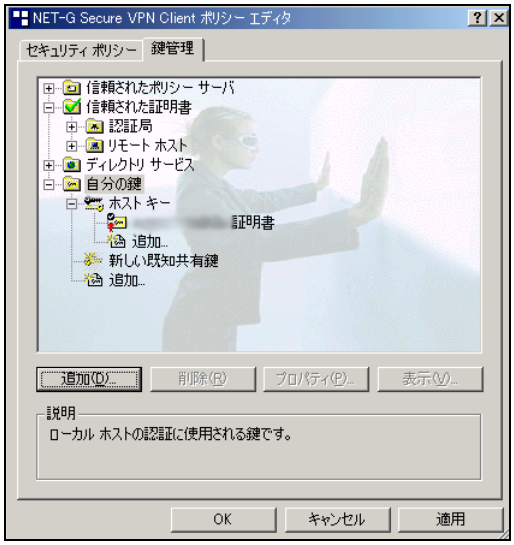
「鍵管理」タブをクリックし、「自分の鍵」を選択し、「追加」ボタンをクリックします。



「新しい認証鍵」ウィンドウが開きますので、「既知共有鍵を作成する」を選択し、「次へ」ボタンをクリックして下さい。

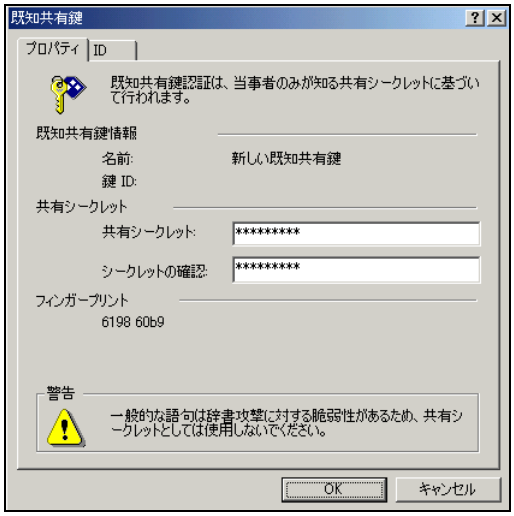


「既知共有鍵の作成」画面が開きます。ここで既知共有鍵を作成します。「名前」には任意の設定名を入力します。「共有シークレット」「共有シークレットの確認」項目には既知共有鍵を入力し、「完了」ボタンをクリックします。
この例では共有シークレットとして「ipseckey3」を設定しています。

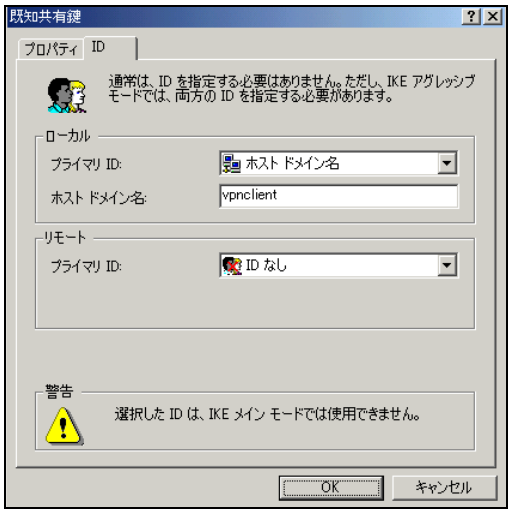


「鍵管理」画面に戻ります。既知共有鍵が登録されていることを確認したら、必ず「適用」ボタンをクリックして下さい。「適用」ボタンをクリックしないと適切に設定されない場合があります。

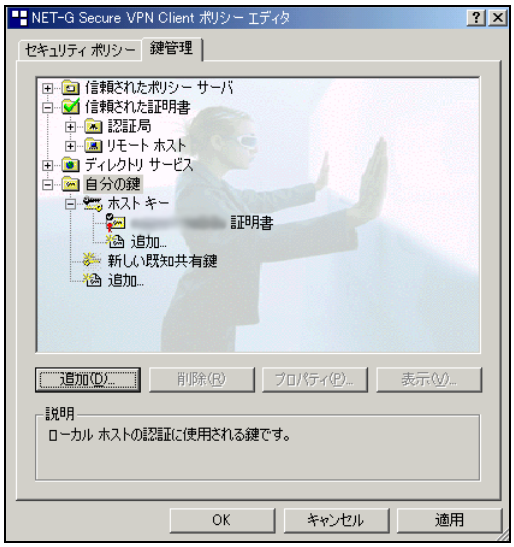
<<ID の設定>>



「鍵管理」画面で、登録した既知共有鍵を選択して「プロパティ」をクリックします。「既知共有鍵」画面が開きますので、「ID」タブをクリックします(この画面では既知共有鍵を変更できます)。



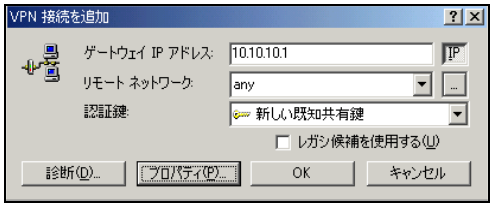
「ローカル」側項目について、プライマリ ID は「ホストドメイン名」を選択し、ホストドメイン名に ID を入力します。ここには XR シリーズの IPsec サーバ「IKE/ISAKMP の設定」における「インタフェース ID」と同じ ID を設定します。
※ただしこの時、ホストドメイン名には”@”をつけないで設定して下さい。



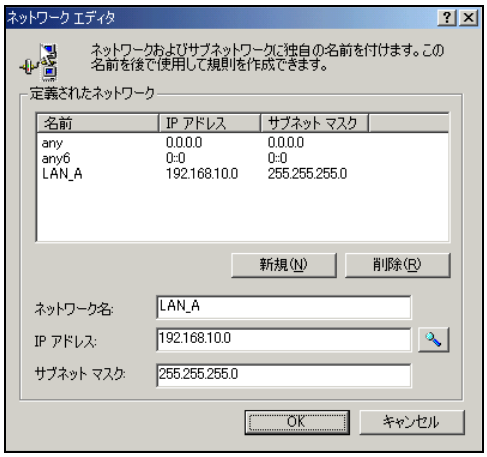
「OK」ボタンをクリックすると、「鍵管理」画面に戻ります。ここまでの設定が終わったら、必ず「適用」ボタンをクリックして下さい。「適用」ボタンをクリックしないと適切に設定されない場合があります。

<<セキュリティポリシーの設定>>

ポリシーエディタの「セキュリティポリシー」タブをクリックします。「VPN 接続」を選択し「追加」をクリックします。

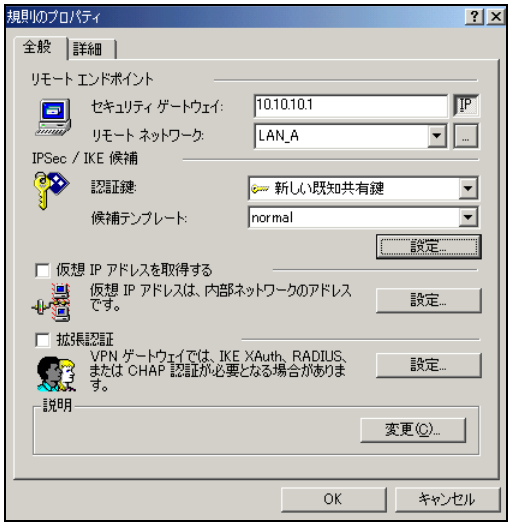


「VPN 接続を追加」画面が開きます。「ゲートウェイ IP アドレス」で右端の”IP”をクリックし、XR_A(センター)の WAN 側 IP アドレスを設定します。
「認証鍵」は、既知共有鍵の設定で登録した既知共有鍵の設定名を選択します。
「リモートネットワーク」については右端にある”・・・”をクリックして下さい。



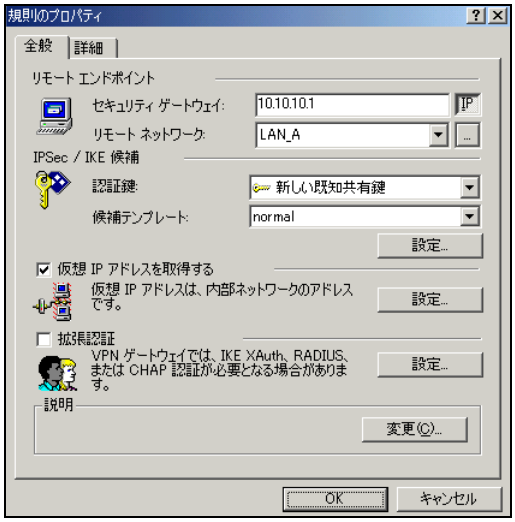
「ネットワークエディタ」画面が開きます。
「ネットワーク名」は任意の名前を設定することができます。
「IP アドレス」「サブネットマスク」は XR に接続している LAN について設定し（ここでは LAN_A[センター側のネットワーク]の値を設定しています)、「OK」をクリックします。

リモートネットワーク設定後、「VPN 接続を追加」画面が開きますので、続いてプロパティをクリックします。



「規則のプロパティ」画面が開きます。ここで IPsec/IKE 候補の
設定ボタンをクリックします。

「パラメータ候補画面」が開きます。ここで暗号化方式などを設定します。IKE モードは「aggressive mode」を設定します。また「選択した値のみを候補に加える」にチェックをいれます。

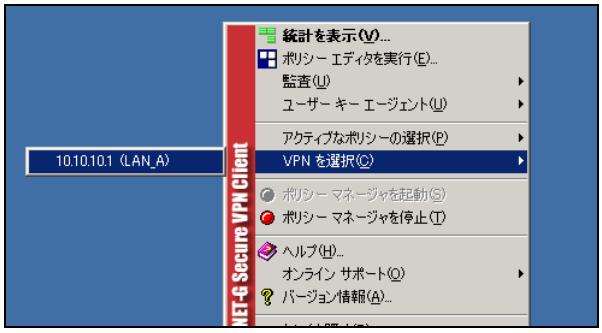


「OK」ボタンをクリックして「規則のプロパティ」画面に戻ります。
続いて「仮想 IP アドレスを取得する」にチェックを入れ、「設定」ボタンをクリックします。

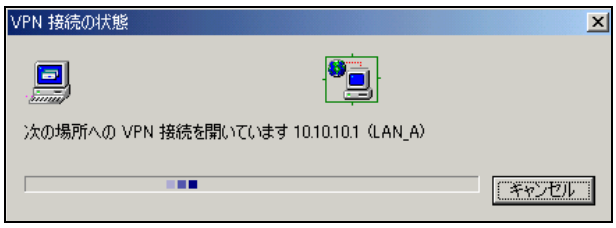
「仮想 IP アドレス」画面が開きます。
ここでは XR に接続する際に使用するこの PC の仮想的な IP アドレスを設定します。
「プロトコル」は”手動で指定”を選択し、任意のプライベート IP アドレスとサブネットマスクを入力します。
ここで設定する IP アドレスは XR の IPsec サーバにおける「IPsec ポリシーの設定」の”相手側の LAN 側のネットワークアドレス”と一致させます。この例では、サブネットマスクは 24 ビットマスクとしています。
※XR_A(センター)の IPsec ポリシーで設定したサブネットと異なるので注意して下さい。
（32 ビットマスクは設定することができません。）

これで設定は完了です。

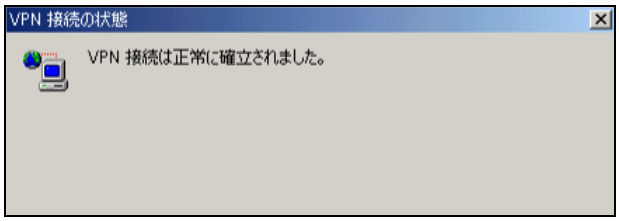
続いて IPsec 接続を行います。



タスクバーの中にある FutureNet Net-G VPNclient のアイコンを右クリックします。そして「VPN を選択」の指定し、作成した IPsec ポリシーを選択します。



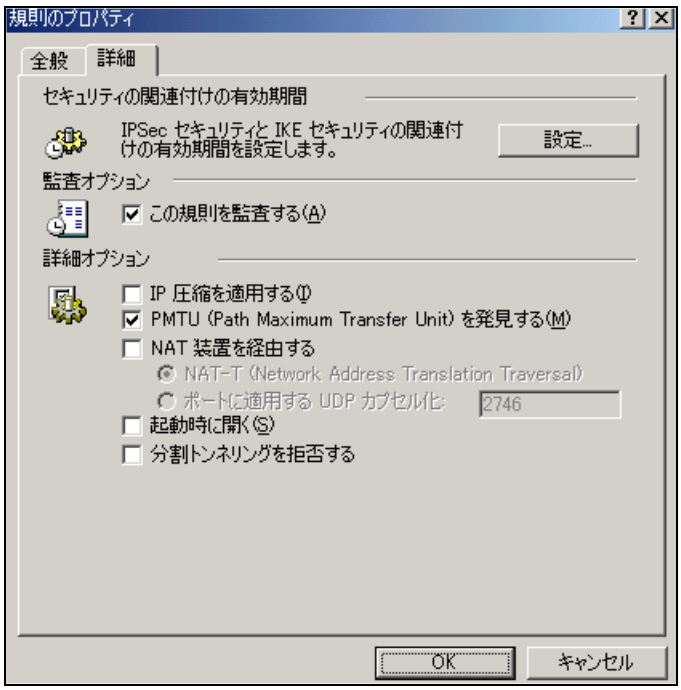
選択後、IKE のネゴシエーションを行う画面が表示されます。



IPsec が正常に確立した場合、「VPN 接続は正常に確立しました」という画面が表示されます。

これで IPsec 接続は完了です。

なおこの設定例では、IPsec 接続時の Internet へのアクセスは拒否になっています。
IPsec 接続と Internet へのアクセスを両方同時に利用したい場合には、以下の設定を行って下さい。

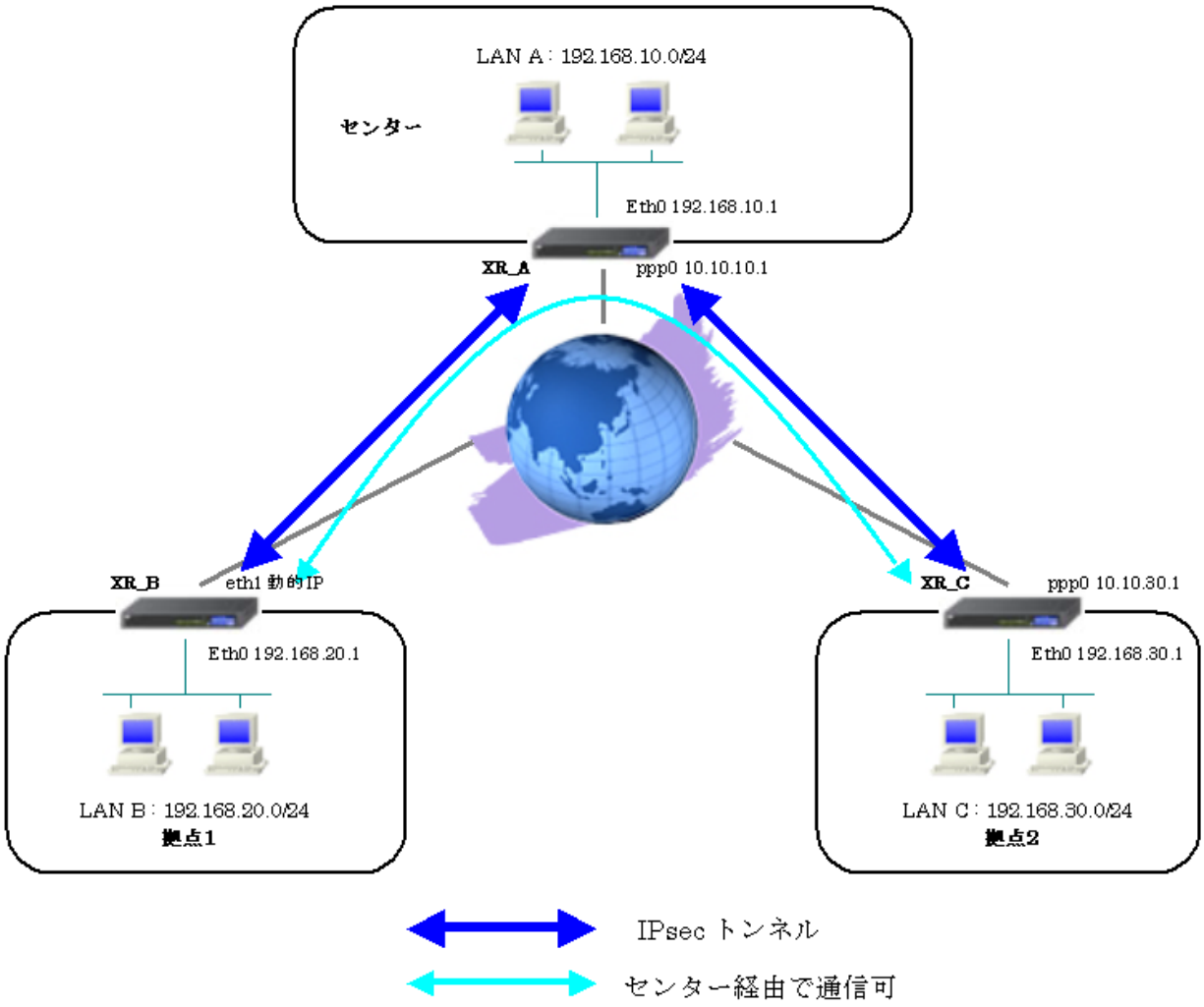


「規則のプロパティ」画面を開き、「詳細タブ」をクリックします。ここで詳細オプションにある「分割トンネリングを拒否する」のチェックボックスのチェックを外します。

2. IPsec を利用したセンター経由インターネット接続例

この例は、PPPoE や Ether での接続で IPsec によるインターネット VPN を行い、拠点の端末はインターネットアクセスする場合、センターの XR 経由でアクセスするというものです。
またこの例では、センター<->拠点間の通信だけではなく、拠点間通信も可能になっています。

2-1. 構成例



2-2. 要件

➢ インタフェースおよび PPPoE

- XR_A(センター), XR_B(拠点 1)はインターネットに PPPoE で接続します。
- XR_C(拠点 2)はインターネットに Ether で接続します。
- PPPoE 接続は、自動再接続するように設定しています。
- WAN 側インタフェースの IP マスカレードは「無効」, ステートフルパケットインスペクションは「有効」にしています。

主なインタフェースおよび PPPoE のパラメータ

	XR_A(センター)	XR_B(拠点 1)	XR_C(拠点 2)
LAN 側インタフェース	Ether0	Ether0	Ether0
LAN 側 IP アドレス	192.168.10.1	192.168.20.1	192.168.30.1
WAN 側インタフェース	Ether1[ppp0]	Ether1[ppp0]	Ether1
WAN 側 IP アドレス	10.10.10.1	動的 IP	10.10.30.1
PPPoE ユーザ名	test1@centurysys	test2@centurysys	-
PPPoE パスワード	test1pass	test2pass	-
接続回線	PPPoE 接続	PPPoE 接続	Ether 接続

➢ IPsec

- 鍵交換モードは XR_A <-> XR_B はアグレッシブモード, XR_A <-> XR_C はメインモードを使用しています。
- XR_A(センター)は 0.0.0.0/0 <-> 192.168.20.0/24, 192.168.30.0/24 の時に IPsec を適用します。
- XR_B(拠点 1)は 192.168.20.0/24 <-> 0.0.0.0/0 の時に IPsec を適用します。
- XR_C(拠点 2)は 192.168.30.0/24 <-> 0.0.0.0/0 の時に IPsec を適用します。
- XR_A(センター)は、XR_C(拠点 2)に対してのみ IPsec KeepAlive を使用しています。
- XR_B(拠点 1)は、XR_A(センター)に対して IPsec KeepAlive を使用しています。
- XR_C(拠点 2)は、XR_A(センター)に対して IPsec KeepAlive を使用しています。

本装置側のパラメータ

	XR_A(センター)	XR_B(拠点 1)	XR_C(拠点 2)
インタフェースの IP アドレス	10.10.10.1	%ppp0	10.10.30.1
上位ルータの IP アドレス	%ppp0		10.10.30.254
インタフェースの ID		@ipsec1	

IKE/ISAKMP ポリシーのパラメータ(1) 「XR_A(センター)」

	XR_A(センター)	
対向拠点	XR_B(拠点 1)	XR_C(拠点 2)
IKE/ISAKMP ポリシー名	XR_B	XR_C
リモート IP アドレス	0.0.0.0	10.10.10.1
インタフェースの ID	@ipsec1	
モード	Aggressive	Main
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
DH グループ	Group2	Group2
ライフタイム	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey2

IPsec ポリシーのパラメータ(1) 「XR_A(センター)」

	XR_A(センター)	
対向拠点	XR_B(拠点 1)	XR_C(拠点 2)
使用する IKE ポリシー名	XR_B(IKE1)	XR_C(IKE2)
本装置の LAN 側のネットワークアドレス	0.0.0.0/0	0.0.0.0/0
相手側の LAN 側のネットワークアドレス	192.168.20.0/24	192.168.30.0/24
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
PFS(DH グループ)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)
DISTANCE	1	1

IKE/ISAKMP ポリシーのパラメータ(2) 「XR_B(拠点 1), XR_C(拠点 2)」

	XR_B(拠点 1)	XR_C(拠点 2)
対向拠点	XR_A(センター)	XR_A(センター)
IKE/ISAKMP ポリシー名	XR_A	XR_A
リモート IP アドレス	10.10.10.1	10.10.10.1
モード	Aggressive	Main
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
DH グループ	Group2	Group2
ライフタイム	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey2

IPsec ポリシーのパラメータ(2) 「XR_B(拠点 1), XR_C(拠点 2)」

	XR_B(拠点 1)	XR_C(拠点 2)
対向拠点	XR_A(センター)	XR_A(センター)
使用する IKE ポリシー名	XR_A(IKE1)	XR_A(IKE1)
本装置の LAN 側のネットワークアドレス	192.168.20.0/24	192.168.30.0/24
相手側の LAN 側のネットワークアドレス	0.0.0.0/0	0.0.0.0/0
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
PFS(DH グループ)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)
DISTANCE	1	1

IPsec Keepalive のパラメータ

	XR_A(センター)	XR_B(拠点 1)	XR_C(拠点 2)
対向拠点	XR_C(拠点 2)	XR_A(センター)	XR_A(センター)
Policy No.	2	1	1
source address	192.168.10.1	192.168.20.1	192.168.30.1
destination address	192.168.30.1	192.168.10.1	192.168.10.1
interval(sec)	30	45	45
watch count	3	3	3
timeout/delay(sec)	60	60	60
動作 option	1	2	1
interface	ipsec0	ipsec0	ipsec6

2-3. 設定例

センタールータ（XR_A）

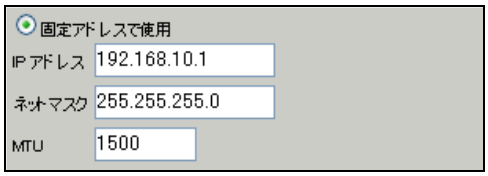
ポイント

拠点 1,2 と IPsec 接続するための設定を行います。

XR_B(拠点 1)は動的 IP のため、アグレッシブモードを使用しています。

<<インタフェース設定>>

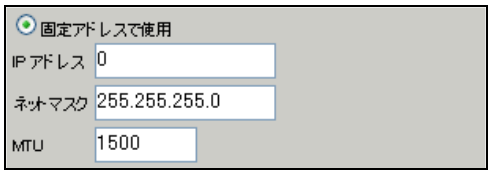
[Ethernet0 の設定]



Ethernet0 に関する設定をします。

※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

[Ethernet1 の設定]

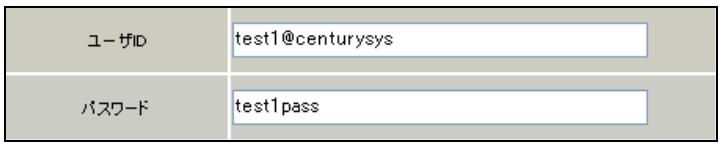


Ethernet1 に関する設定をします。

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

<<PPP/PPPoE 設定>>

[接続先設定 1]



PPPoE 接続で使用するユーザ ID，パスワードを登録します。

［接続設定］

接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ◉Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ○RS232C
接続形態	○手動接続 ◉常時接続 ○スケジューラ接続
RS232C/BRI接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	○無効 ◉有効
ステートフルパケット インスペクション	○無効 ◉有効 ☐DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ◉有効

PPPoE 接続するインタフェース、および接続形態を選択します。
※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション（全回線共通）	☑回線接続時に前回のPPPoEセッションのPADTを強制送出 ☑非接続SessionのIPv4Packet受信時にPADTを強制送出 ☑非接続SessionのLCP-EchoRequest受信時にPADTを強制送出

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

<<フィルタ設定>>

［入力フィルタ］

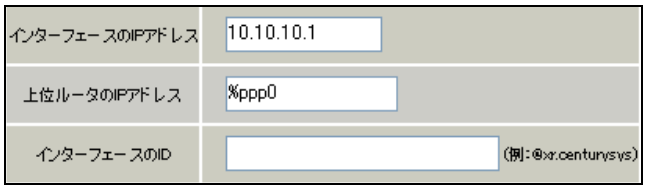
インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	udp		500		500	☐
ppp0	パケット受信時	許可	esp					☐

IKE パケット，ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

<IPsec サーバ>

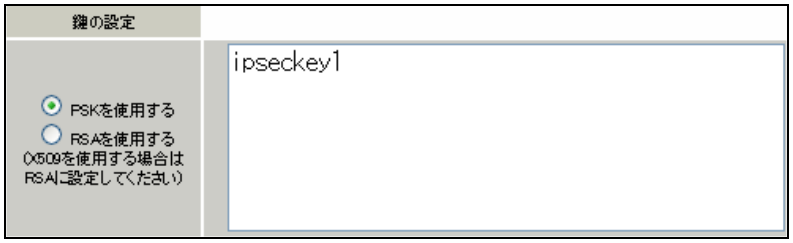
[本装置側の設定 1]



XR_A(センター)の WAN 側インタフェースの IP アドレス,および上位ルータの IP アドレスを設定します。
PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

[IKE/ISAKMP の設定 1]

XR_B(拠点 1)に対する IKE/ISAKMP ポリシーを設定します。



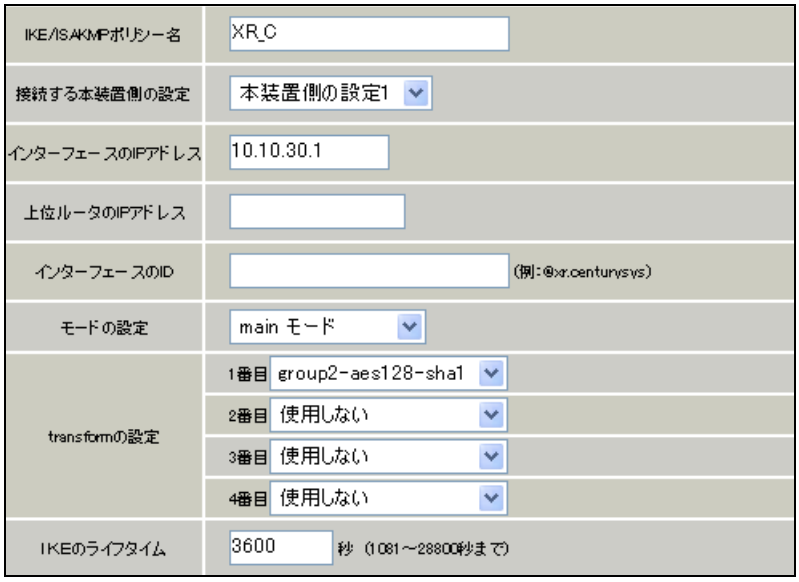
事前共有鍵(PSK)として「ipseckey1」を設定しています。

[IPsec ポリシーの設定 1]

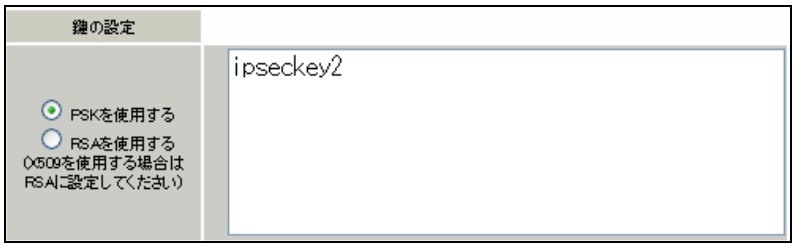
XR_B(拠点 1)の IP アドレスが不定のため、「Responder として使用する」を選択します。

XR_B(拠点 1)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。

[IKE/ISAKMP の設定 2]



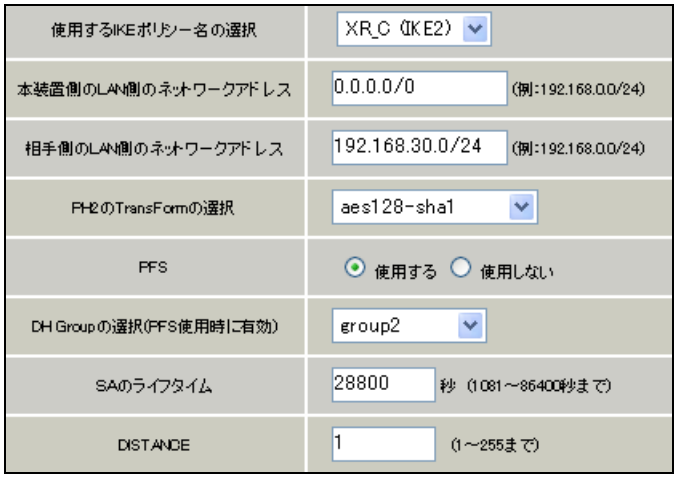
XR_C(拠点 2)に対する ISAKMP ポリシーの設定を行います。



事前共有鍵(PSK)として「ipseckey2」を設定します。

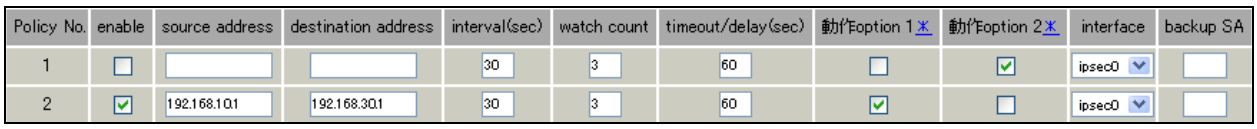
[IPsec ポリシーの設定 2]

XR_C(拠点 2)に対して IKE のネゴシエーションを行うため、「使用する」を選択しています。



XR_C(拠点 2)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

[IPsec Keep-Alive 設定]



Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1※	動作option 2※	interface	backup SA
1	☐			30	3	60	☐	☑	ipsec0	
2	☑	192.168.10.1	192.168.30.1	30	3	60	☑	☐	ipsec0	

XR_C(拠点 2)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

IPsec サーバ機能を起動します。

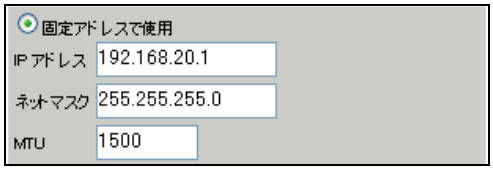
拠点 1 ルータ（XR_B）

ポイント

XR_A(センター)に対して IPsec 接続を行います。WAN 側 IP アドレスが動的 IP アドレスであるため、鍵交換モードとして「Aggressive モード」を使用しています。

<<インタフェース設定>>

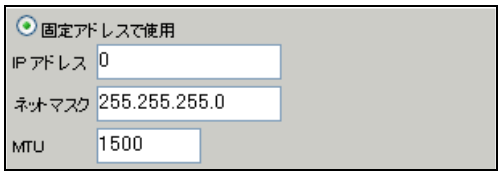
[Ethernet0 の設定]



Ethernet0 の設定をします。

※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

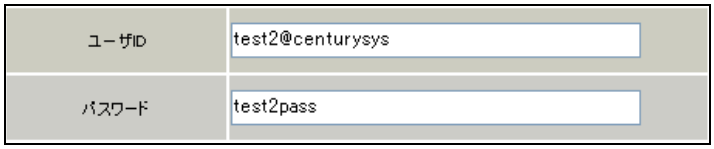
[Ethernet1 の設定]



PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

<<PPP/PPPoE 設定>>

[接続先設定１]



PPPoE 接続で使用するユーザ ID，パスワードを登録します。

［接続設定］

接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ◉Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ○RS232C
接続形態	○手動接続 ◉常時接続 ○スケジューラ接続
RS232C/BRI接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	◉無効 ○有効
ステートフルパケット インスペクション	○無効 ◉有効 ☐DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ◉有効

PPPoE 接続するインタフェース、および接続形態を選択します。
インターネットアクセスはセンター経由で行うため、IP マスカレード設定を「無効」にしています。

PPPoE特殊オプション (全回線共通)	☑回線接続時に前回のPPPoEセッションのPADTを強制送出 ☑非接続SessionのIPv4Packet受信時にPADTを強制送出 ☑非接続SessionのLCP-EchoRequest受信時にPADTを強制送出

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

<<フィルタ設定>>

［入力フィルタ］

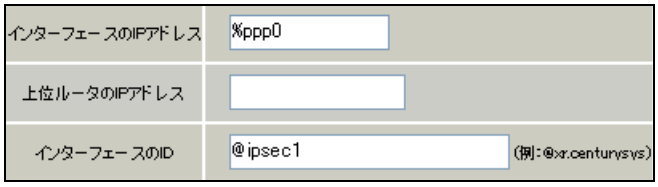
インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	udp		500		500	☐
ppp0	パケット受信時	許可	esp					☐

IKE パケット，ESP パケットの「許可」を設定します。

<<各種サービスの設定>>

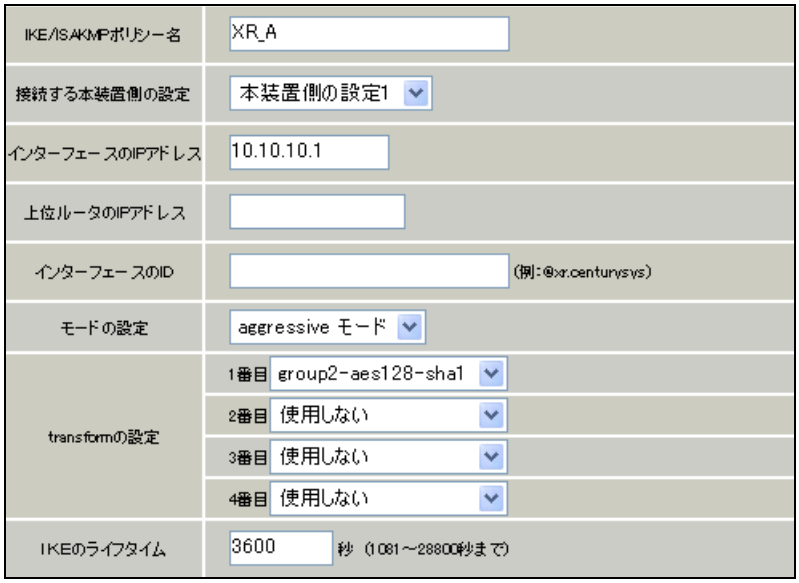
<IPsec サーバ>

[本装置側の設定 1]

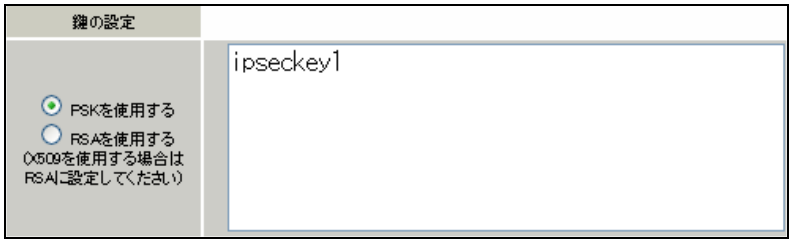


PPPoE 接続で WAN 側(ppp0)インタフェースの IP アドレスが不定のため「%ppp0」, インタフェースの ID として「@ipsec1」を設定します。

[IKE/ISAKMP の設定 1]



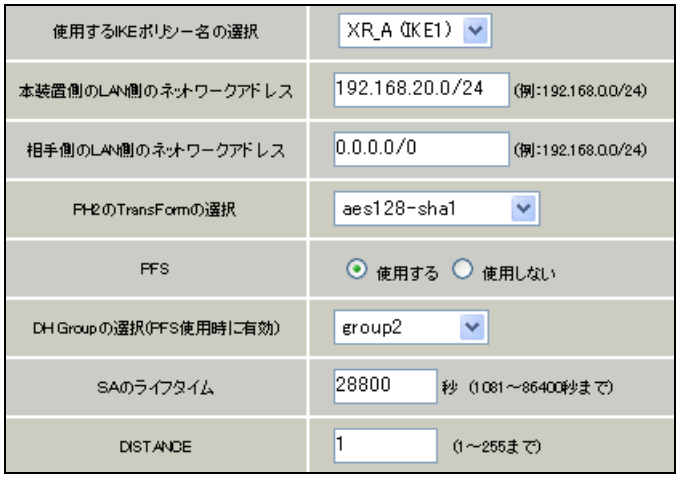
XR_A(センター)に対する ISAKMP ポリシーの設定を行います。



事前共有鍵(PSK)として「ipseckey1」を設定します。

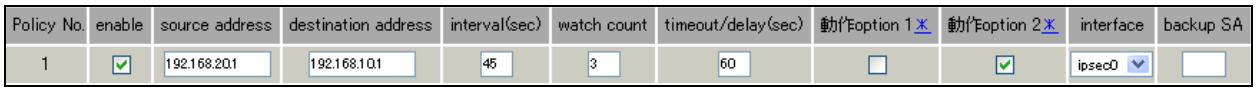
[IPsec ポリシーの設定 1]

XR_A(センター)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。



XR_A(センター)に対して IPsec 通信を行う IP アドレスの範囲を設定します。
この例では、IPsec 通信を行う宛先 IP アドレスを「0.0.0.0/0」に設定しています。

[IPsec Keep-Alive 設定]



XR_A(センター)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

IPsec サーバ機能を起動します。

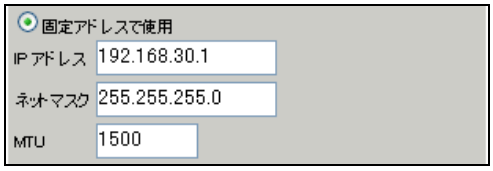
拠点 2 ルータ（XR_C）

ポイント

XR_A(センター)に対して IPsec 接続を行います。XR_A,XR_C の WAN 側 IP アドレスが固定 IP アドレスであるため、鍵交換モードとして「Main モード」を使用しています。

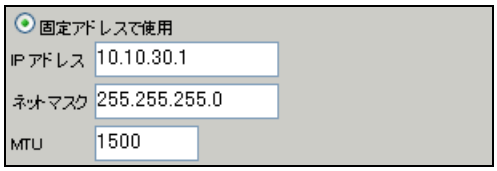
<<インタフェース設定>>

[Ethernet0 の設定]

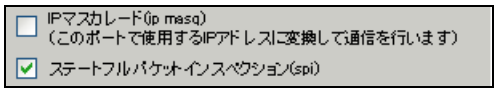


Ethernet0 の設定をします。
※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

[Ethernet1 の設定]



WAN 側 IP アドレスの設定をします。



インターネットアクセスはセンター経由で行うため、IP マスカレード設定を「無効」にしています。ステートフルパケットインスペクション(SPI)を「有効」に設定します。

<<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
eth1	パケット受信時	許可	udp		500		500	□
eth1	パケット受信時	許可	esp					□

IKE パケット，ESP パケットの「許可」を設定します。

<<各種サービスの設定>>

<IPsec サーバ>

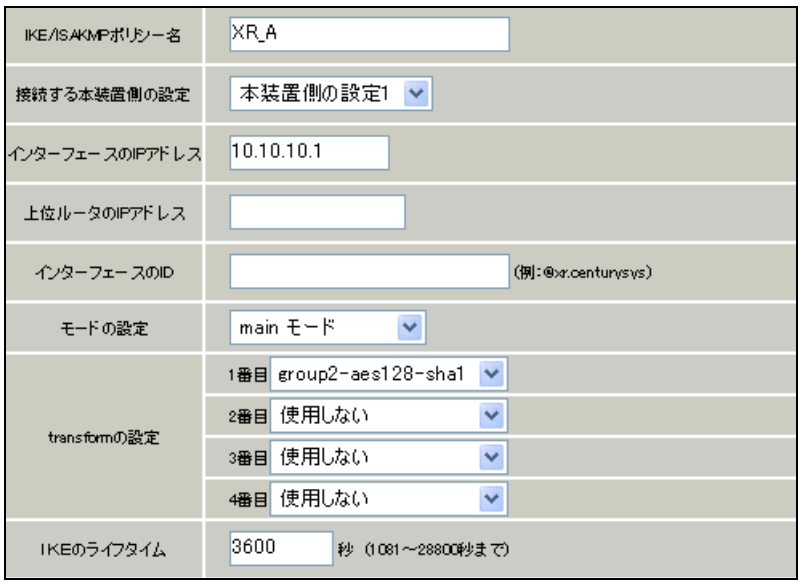
[本装置側の設定 1]

インターフェースのIPアドレス	10.10.30.1
上位ルータのIPアドレス	10.10.30.254
インターフェースのID	(例:@xr.centurysys)

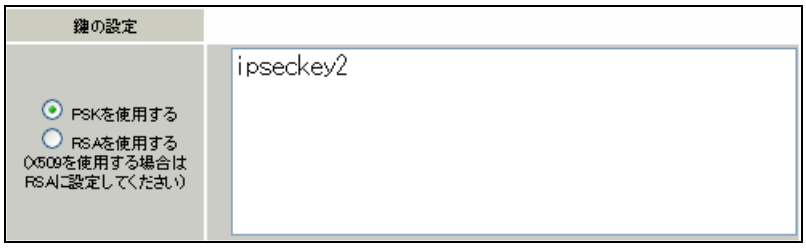
XR_A(センター)の WAN 側インタフェースの IP アドレス,および上位ルータの IP アドレスを設定します。

※Ether 接続で WAN 側 IP アドレスが固定 IP の場合、「上位ルータの IP アドレス」は「%eth1」と設定することはできません。

[IKE/ISAKMP の設定 1]



XR_A(センター)に対する ISAKMP ポリシーの設定を行います。



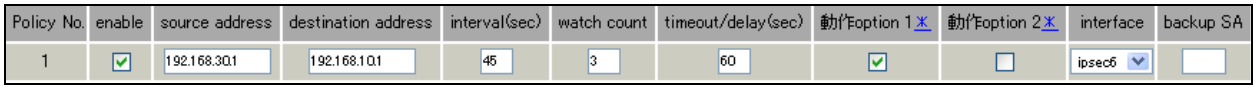
事前共有鍵(PSK)として「ipseckey2」を設定します。

[IPsec ポリシーの設定 1]

XR_A(センター)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

XR_A(センター)に対して IPsec 通信を行う IP アドレスの範囲を設定します。
この例では、IPsec 通信を行う宛先 IP アドレスを「0.0.0.0/0」に設定しています。

[IPsec Keep-Alive 設定]



XR_A(センター)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

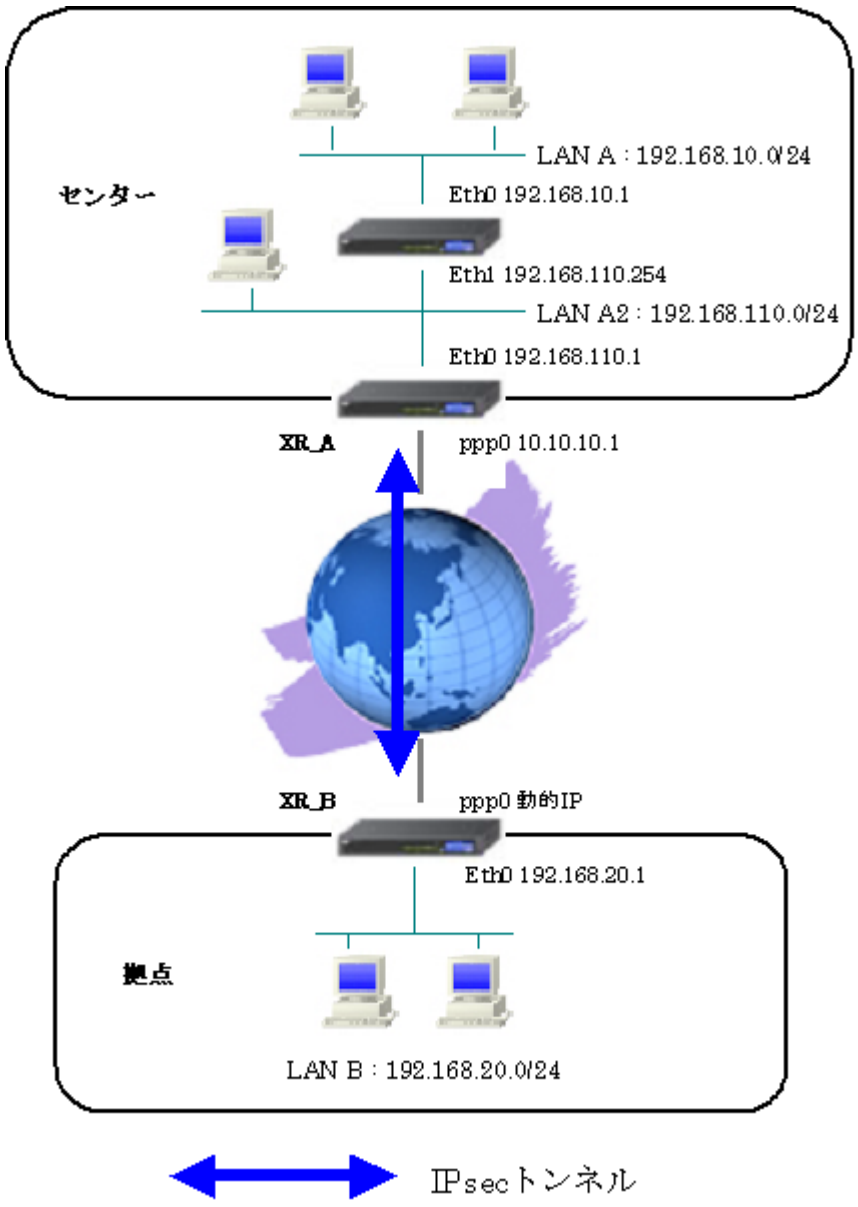
【IPsec サーバ】

IPsec サーバ機能を起動します。

3. 複数セグメントでの IPsec 設定例

IPsec を行っている XR 配下に複数のセグメントがあった場合の IPsec 設定例になります。
この例では、センター側にある２つのセグメントに対して IPsec ポリシーを２つ作成しています。

3-1. 構成例



3-2. 要件

➢ インタフェースおよび PPPoE

- XR_A(センター1), XR_B(拠点)はインターネットに PPPoE で接続します。
- XR_A2(センター2)はローカルルータになります。
- PPPoE 接続は、自動再接続するように設定しています。
- XR_A(センター1),XR_B(拠点)の WAN 側インタフェースの IP マスカレードは「有効」, ステートフルパケットインスペクションは「有効」にしています。

主なインタフェースおよび PPPoE のパラメータ(1)

	XR_A(センター)	XR_B(拠点)
LAN 側インタフェース	Ether0	Ether0
LAN 側 IP アドレス	192.168.110.1	192.168.20.1
WAN 側インタフェース	Ether1[ppp0]	Ether1[ppp0]
WAN 側 IP アドレス	10.10.10.1	動的 IP
PPPoE ユーザ名	test1@centurysys	test2@centurysys
PPPoE パスワード	test1pass	test2pass
接続回線	PPPoE 接続	PPPoE 接続

主なインタフェースおよび PPP/PPPoE のパラメータ(2)

	XR_A2(センター2)
LAN 側インタフェース	Ether0
LAN 側 IP アドレス	192.168.10.1
WAN 側インタフェース	Ether1
WAN 側 IP アドレス	192.168.110.254
デフォルトゲートウェイ	192.168.110.1

➢ IPsec

- 鍵交換モードは XR_A <-> XR_B はアグレッシブモードを使用しています。
- XR_A(センター1)は 192.168.10.0/24, 192.168.110.0/24 <-> 192.168.20.0/24 の時に IPsec を適用します。
- XR_B(拠点)は 192.168.20.0/24 <-> 192.168.10.0/24, 192.168.110.0/24 の時に IPsec を適用します。
- XR_B(拠点)は、XR_A(センター)に対して IPsec KeepAlive を使用しています。

本装置側のパラメータ

	XR_A(センター1)	XR_B(拠点)
インタフェースの IP アドレス	10.10.10.1	%ppp0
上位ルータの IP アドレス	%ppp0	
インタフェースの ID		@ipsec1

IKE/ISAKMP ポリシーのパラメータ 「XR_A(センター1), XR_B(拠点)」

	XR_A(センター1)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター1)
IKE/ISAKMP ポリシー名	XR_B	XR_A
リモート IP アドレス	0.0.0.0	10.10.10.1
インタフェースの ID	@ipsec1	
モード	Aggressive	Aggressive
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
DH グループ	Group2	Group2
ライフタイム	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey1

IPsec ポリシーのパラメータ(1) 「XR_A(センター1)」

	XR_A(センター1)	
対向拠点	XR_B(拠点)	
使用する IKE ポリシー名	XR_B(IKE1)	XR_B(IKE1)
本装置の LAN 側のネットワークアドレス	192.168.10.0/24	192.168.110.0/24
相手側の LAN 側のネットワークアドレス	192.168.20.0/24	192.168.20.0/24
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
PFS(DH グループ)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)
DISTANCE	1	1

IPsec ポリシーのパラメータ(2) 「XR_B(拠点)」

	XR_B(拠点)	
対向拠点	XR_A(センター)	
使用する IKE ポリシー名	XR_A(IKE1)	XR_A(IKE1)
本装置の LAN 側のネットワークアドレス	192.168.20.0/24	192.168.20.0/24
相手側の LAN 側のネットワークアドレス	192.168.10.0/24	192.168.110.0/24
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
PFS(DH グループ)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)
DISTANCE	1	1

IPsec Keepalive のパラメータ

	XR_B(拠点)	
対向拠点	XR_A(センター)	
Policy No.	1	2
source address	192.168.20.1	192.168.20.1
destination address	192.168.10.254	192.168.110.1
Interval(sec)	45	60
watch count	3	3
timeout/delay(sec)	60	60
動作 option	2	2
interface	ipsec0	ipsec0

➢ その他

- XR_A(センター1)では、XR_B(拠点)の IPsec 192.168.20.0/24 <-> 192.168.10.0/24 の IPsec KeepAlive 応答用に仮想インタフェース設定で「192.168.10.254」を設定しています。

3-3. 設定例

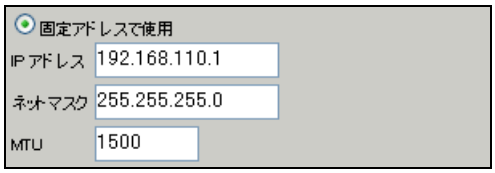
センタールータ（XR_A）

ポイント

拠点と IPsec 接続するための設定を行います。
XR_B(拠点)は動的 IP のため、アグレッシブモードを使用しています。
「192.168.10.0/24」,「192.168.110.0/24」の二つのセグメントで IPsec を使用しますので、IPsec ポリシーを二つ設定しています。
XR_B(拠点)の IPsec 192.168.20.0/24 <-> 192.168.10.0/24 の IPsec KeepAlive 応答用に仮想インタフェース設定で「192.168.10.254」を設定しています。

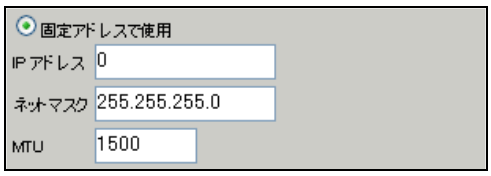
<<インタフェース設定>>

[Ethernet0 の設定]



Ethernet0 に関する設定をします。
※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

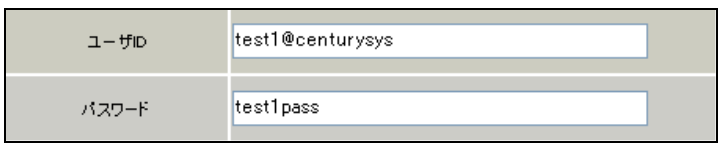
[Ethernet1 の設定]



Ethernet1 に関する設定をします。
PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

<<PPP/PPPoE 設定>>

[接続先設定 1]



PPPoE 接続で使用するユーザ ID，パスワードを登録します。

［接続設定］

接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ◉Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ○RS232C
接続形態	○手動接続 ◉常時接続 ○スケジューラ接続
RS232C/BRI接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	○無効 ◉有効
ステートフルパケット インスペクション	○無効 ◉有効 ☐DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ◉有効

PPPoE 接続するインタフェース、および接続形態を選択します。
※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション (全回線共通)	☑回線接続時に前回のPPPoEセッションのPADTを強制送出 ☑非接続SessionのIPv4Packet受信時にPADTを強制送出 ☑非接続SessionのLCP-EchoRequest受信時にPADTを強制送出

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

<<フィルタ設定>>

［入力フィルタ］

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	udp		500		500	☐
ppp0	パケット受信時	許可	esp					☐

IKE パケット，ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<スタティックルート設定>>

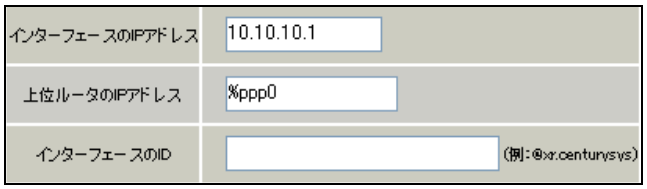
アドレス	ネットマスク	インターフェース/ゲートウェイ		ディスタンス <1-255>
192.168.10.0	255.255.255.0		192.168.110.254	1

LAN A(192.168.10.0/24)宛のパケットを XR_A2 へ転送するための設定をしています。

<<各種サービスの設定>>

<IPsec サーバ>

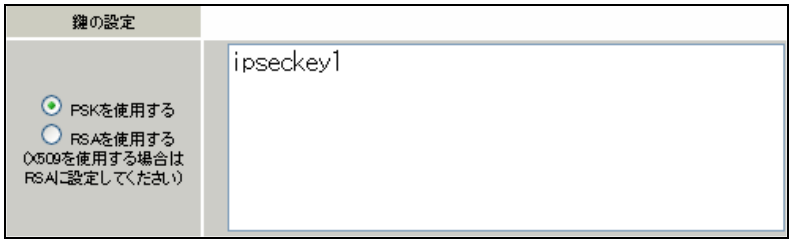
[本装置側の設定 1]



XR_A(センター)の WAN 側インタフェースの IP アドレス,および上位ルータの IP アドレスを設定します。
PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

[IKE/ISAKMP の設定 1]

XR_B(拠点 1)に対する IKE/ISAKMP ポリシーを設定します。



事前共有鍵(PSK)として「ipseckey1」を設定しています。

[IPsec ポリシーの設定 1]

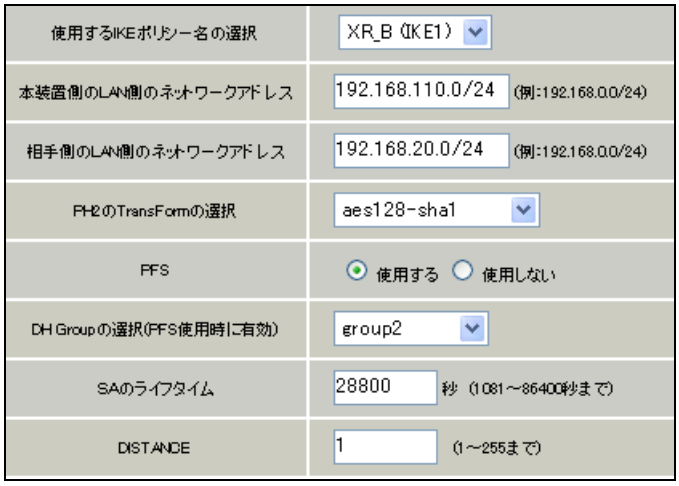
XR_B(拠点)の IP アドレスが不定のため、「Responder として使用する」を選択します。

使用するIKEポリシー名の選択	XR_B (IKE1)
本装置側のLAN側のネットワークアドレス	192.168.10.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.20.0/24 (例:192.168.0.0/24)
PH2のTransFormの選択	aes128-sha1
PFS	使用する 使用しない
DH Groupの選択(PFS使用時に有効)	group2
SAのライフタイム	28800 秒 (1081～86400秒まで)
DISTANCE	1 (1～255まで)

XR_B(拠点)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。
この IPsec ポリシーは、192.168.10.0/24 <-> 192.168.20.0/24 の通信に適用されます。

[IPsec ポリシーの設定 2]

XR_B(拠点)の IP アドレスが不定のため、「Responder として使用する」を選択します。

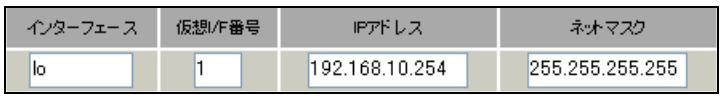


XR_B(拠点)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。
この IPsec ポリシーは、192.168.110.0/24 <-> 192.168.20.0/24 の通信に適用されます。

【IPsec サーバ】

IPsec サーバ機能を起動します。

<<仮想インタフェース設定>>



仮想インタフェース設定で「lo」インタフェースを設定します。
このインタフェースは XR_B(拠点)の IPsec 192.168.20.0/24 <-> 192.168.10.0/24 の IPsec KeepAlive 応答用に設定しています。
この設定を行うことにより、「192.168.10.254」宛のパケットを XR_A(センター1)で受信した場合は、XR_A(センター1)が応答を返すようになります。

センタールータ 2（XR_A2）

ポイント

この設定例では、センタールータ 2（XR_A2）の設定例は記載していません。

センタールータ 2（XR_A2）の主な必要な要件は以下のとおりです。

・宛先 192.168.20.0/24　ゲートウェイ 192.168.110.1 のスタティックルートが設定されていること

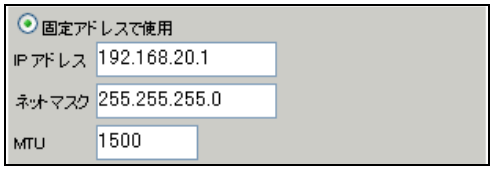
拠点ルータ（XR_B）

ポイント

XR_A(センター1)に対して IPsec 接続を行います。WAN 側 IP アドレスが動的 IP アドレスであるため、鍵交換モードとして「Aggressive モード」を使用しています。
IPsec 通信の宛先として 192.168.10.0/24, 192.168.110.0/24 がありますので、IPsec ポリシーを２つ設定しています。

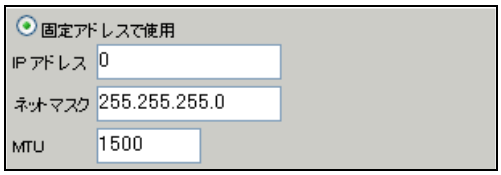
<<インタフェース設定>>

[Ethernet0 の設定]



Ethernet0 の設定をします。
※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

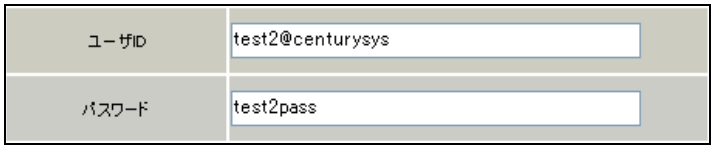
[Ethernet1 の設定]



PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

<<PPP/PPPoE 設定>>

[接続先設定１]



PPPoE 接続で使用するユーザ ID, パスワードを登録します。

［接続設定］

接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ◉Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ○RS232C
接続形態	○手動接続 ◉常時接続 ○スケジューラ接続
RS232C/BRI接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	○無効 ◉有効
ステートフルパケット インスペクション	○無効 ◉有効 ☐DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ◉有効

PPPoE 接続するインタフェース、および接続形態を選択します。
※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション（全回線共通）	☑回線接続時に前回のPPPoEセッションのPADTを強制送出 ☑非接続SessionのIPv4Packet受信時にPADTを強制送出 ☑非接続SessionのLCP-EchoRequest受信時にPADTを強制送出

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

<<フィルタ設定>>

［入力フィルタ］

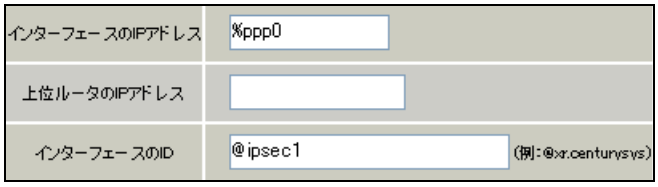
インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	udp		500		500	☐
ppp0	パケット受信時	許可	esp					☐

IKE パケット，ESP パケットの「許可」を設定します。

<<各種サービスの設定>>

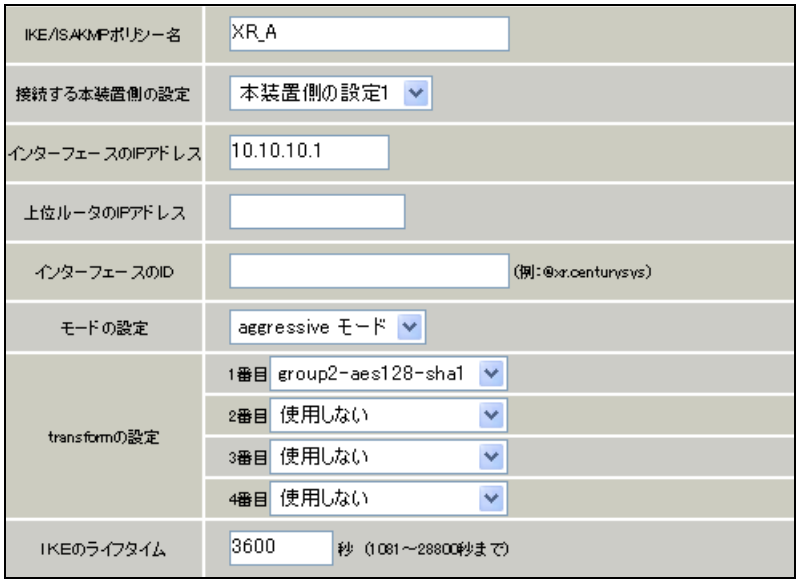
<IPsec サーバ>

[本装置側の設定 1]

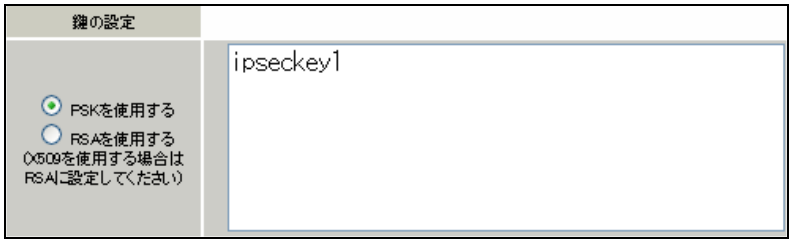


PPPoE 接続で WAN 側(ppp0)インタフェースの IP アドレスが不定のため「%ppp0」, インタフェースの ID として「@ipsec1」を設定します。

[IKE/ISAKMP の設定 1]



XR_A(センター1)に対する ISAKMP ポリシーの設定を行います。



事前共有鍵(PSK)として「ipseckey1」を設定します。

[IPsec ポリシーの設定 1]

XR_A(センター1)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

XR_A(センター1)に対して IPsec 通信を行う IP アドレスの範囲を設定します。
この IPsec ポリシーは、192.168.20.0/24 <-> 192.168.10.0/24 の通信に適用されます。

[IPsec ポリシーの設定 2]

XR_A(センター1)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

XR_A(センター1)に対して IPsec 通信を行う IP アドレスの範囲を設定します。
この IPsec ポリシーは、192.168.20.0/24 <-> 192.168.110.0/24 の通信に適用されます。

[IPsec Keep-Alive 設定]

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1 *	動作option 2 *	interface	backup SA
1	☑	192.168.20.1	192.168.10.254	45	3	60	☐	☑	ipsec0	
2	☑	192.168.20.1	192.168.110.1	60	3	60	☐	☑	ipsec0	

XR_A(センター1)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。
IPsec ポリシー1 の宛先として XR_A(センター1)で設定している仮想インタフェースの IP アドレスを指定しています。

【IPsec サーバ】

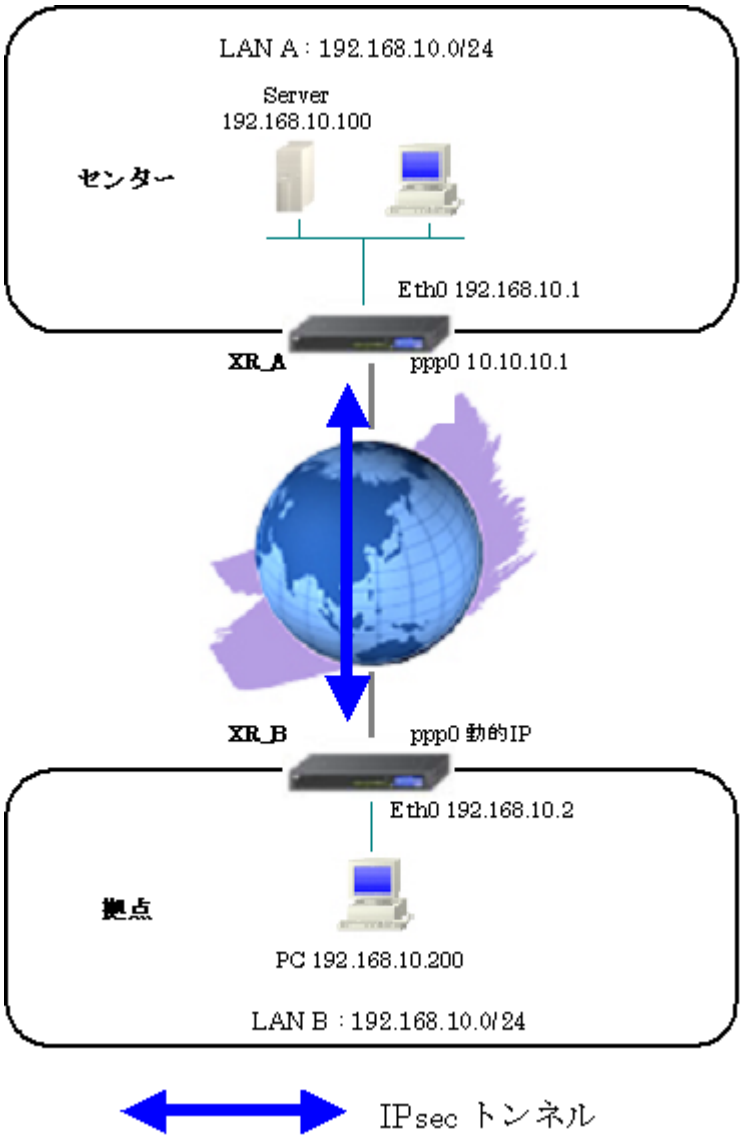
IPsecサーバ	○停止 ◉起動

IPsec サーバ機能を起動します。

4. IPsec での NAT 利用例

通常同一のネットワークアドレスを利用している拠点間では、IPsec による通信はできませんが、IPsec での NAT を利用することにより、同一ネットワークアドレスを利用している拠点間の特定の機器同士で IPsec による通信を利用できます。

4-1. 構成例



4-2. 要件

➢ インタフェースおよび PPP/PPPoE

- インターネットに PPPoE で接続します。
- PPPoE 接続は、自動再接続するように設定しています。
- WAN 側インタフェースの 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は「有効」にしています。

主なインタフェースおよび PPP/PPPoE のパラメータ

	XR_A(センター)	XR_B(拠点)
LAN 側インタフェース	Ether0	Ether0
LAN 側 IP アドレス	192.168.10.1	192.168.10.2
WAN 側インタフェース	Ether1[ppp0]	Ether1[ppp0]
WAN 側 IP アドレス	10.10.10.1	動的 IP
PPPoE ユーザ名	test1@centurysys	test2@centurysys
PPPoE パスワード	test1pass	test2pass
WAN 側接続回線	PPPoE 接続	PPPoE 接続

➢ IPsec

- 鍵交換モードはアグレッシブモードを使用しています。
- XR_A(センター)は 172.16.10.0/24 <-> 172.16.20.0/24 の時に IPsec を適用します。
- XR_B(拠点)は 172.16.20.0/24 <-> 172.16.10.0/24 の時に IPsec を適用します。

本装置側のパラメータ

	XR_A(センター)	XR_B(拠点)
インタフェースの IP アドレス	10.10.10.1	%ppp0
上位ルータの IP アドレス	%ppp0	
インタフェースの ID		@ipsec1

IKE/ISAKMP ポリシーのパラメータ「XR_A(センター),XR_B(拠点)」

	XR_A(センター)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター)
IKE/ISAKMP ポリシー名	XR_B	XR_A
リモート IP アドレス	0.0.0.0	10.10.10.1
インタフェースの ID	@ipsec1	
モード	Aggressive	Aggressive
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
DH グループ	Group2	Group2
ライフタイム	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey1

IPsec ポリシーのパラメータ「XR_A(センター),XR_B(拠点)」

	XR_A(センター)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター)
使用する IKE ポリシー名	XR_B(IKE1)	XR_A(IKE1)
本装置の LAN 側のネットワークアドレス	172.16.10.0/24	172.16.20.0/24
相手側の LAN 側のネットワークアドレス	172.16.20.0/24	172.16.10.0/24
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
PFS(DH グループ)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)
DISTANCE	1	1

IPsec Keepalive のパラメータ

	XR_B(拠点)
対向拠点	XR_A(センター)
Policy No.	1
source address	172.16.20.1
destination address	172.16.10.1
interval(sec)	45
watch count	3
timeout/delay(sec)	60
動作 option	2
interface	ipsec0

- NAT

  - XR_A(センター)では IPsec を経由して「172.16.10.1」宛のパケットを受信した場合には宛先を「192.168.10.1」に変換し、「172.16.10.2」宛のパケットを受信した場合には宛先を「192.168.10.100」に変換します。
    また IPsec を経由して送信元「192.168.10.1」のパケットを送信する場合には、送信元を「172.16.10.1」に変換し、送信元「192.168.10.100」のパケットを送信する場合には、送信元を「172.16.10.2」に変換します。
  - XR_B(拠点)では IPsec を経由して「172.16.20.1」宛のパケットを受信した場合には宛先を「192.168.10.2」に変換し、「172.16.20.2」宛のパケットを受信した場合には宛先を「192.168.10.200」に変換します。
    また IPsec を経由して送信元「192.168.10.2」のパケットを送信する場合には、送信元を「172.16.20.1」に変換し、送信元「192.168.10.200」のパケットを送信する場合には、送信元を「172.16.20.2」に変換します。

バーチャルサーバのパラメータ「XR_A(センター),XR_B(拠点)」

	XR_A(センター)		XR_B(拠点)	
サーバのアドレス	192.168.10.1	192.168.10.100	192.168.10.2	192.168.10.200
公開するグローバルアドレス	172.16.10.1	172.16.10.2	172.16.20.1	172.16.20.2
プロトコル	全て	全て	全て	全て
ポート				
インタフェース	ipsec0	ipsec0	ipsec0	ipsec0

送信元 NAT のパラメータ「XR_A(センター),XR_B(拠点)」

	XR_A(センター)		XR_B(拠点)	
送信元のプライベートアドレス	192.168.10.1	192.168.10.100	192.168.10.2	192.168.10.200
変換後のグローバルアドレス	172.16.10.1	172.16.10.2	172.16.20.1	172.16.20.2
インタフェース	ipsec0	ipsec0	ipsec0	ipsec0

4-3. 設定例

センタールータ（XR_A）

ポイント

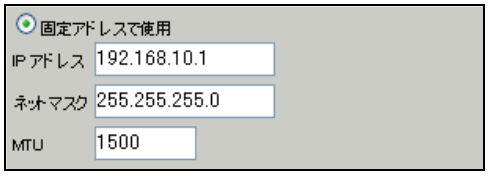
XR_B(拠点)と IPsec で接続するための設定を行います。

IPsec の鍵交換モードはアグレッシブモードを使用します。

IPsec での NAT を利用するため、バーチャルサーバ，送信元 NAT を設定しています。

<<インタフェース設定>>

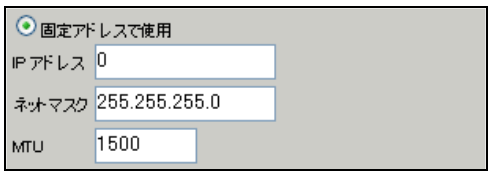
[Ethernet0 の設定]



Ethernet0 に関する設定をします。

※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

[Ethernet1 の設定]

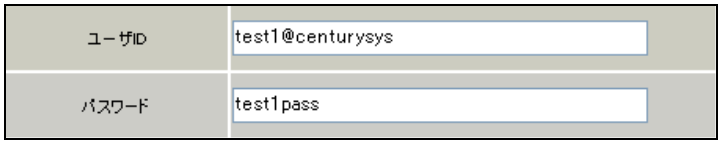


Ethernet1 に関する設定をします。

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

<<PPP/PPPoE 設定>>

[接続先設定 1]



PPPoE 接続で使用するユーザ ID，パスワードを登録します。

［接続設定］

接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ◉Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ○RS232C
接続形態	○手動接続 ◉常時接続 ○スケジューラ接続
RS232C/BRI接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	○無効 ◉有効
ステートフルパケット インスペクション	○無効 ◉有効 ☐DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ◉有効

PPPoE 接続するインタフェース、および接続形態を選択します。
※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション (全回線共通)	☑回線接続時に前回のPPPoEセッションのPADTを強制送出 ☑非接続SessionのIPv4Packet受信時にPADTを強制送出 ☑非接続SessionのLCP-EchoRequest受信時にPADTを強制送出

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

<<フィルタ設定>>

［入力フィルタ］

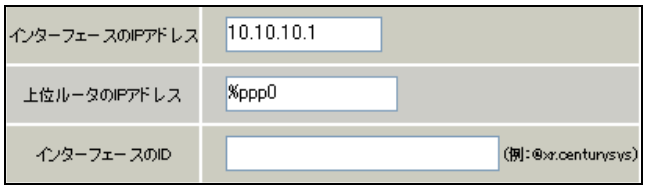
インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	udp		500		500	☐
ppp0	パケット受信時	許可	esp					☐

IKE パケット，ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

<IPsec サーバ>

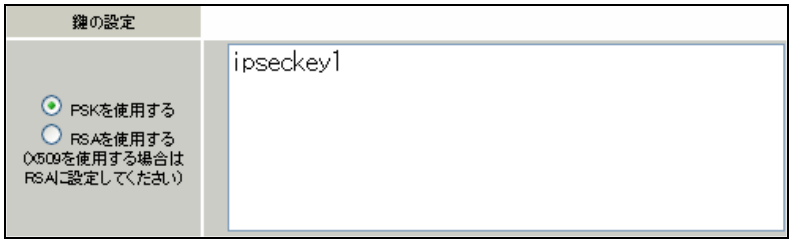
[本装置側の設定 1]



XR_A(センター)の WAN 側インタフェースの IP アドレス,および上位ルータの IP アドレスを設定します。
PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

[IKE/ISAKMP の設定 1]

XR_B(拠点)に対する IKE/ISAKMP ポリシーを設定します。



事前共有鍵(PSK)として「ipseckey1」を設定しています。

[IPsec ポリシーの設定 1]

XR_B(拠点)の IP アドレスが不定のため、「Responder として使用する」を選択します。

XR_B(拠点)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。
この例では、本装置側の仮想ネットワーク「172.16.10.0/24」と対向の仮想ネットワーク「172.16.20.0/24」の通信に対して IPsec を適用します。

【IPsec サーバ】

IPsec サーバ機能を起動します。

<<NAT 設定>>

[バーチャルサーバ]

IPsec を経由して「172.16.10.1」宛のパケットを受信した場合には宛先を「192.168.10.1」に変換し、「172.16.10.2」宛のパケットを受信した場合には宛先を「192.168.10.100」に変換します。

[送信元 NAT]

送信元のプライベートアドレス	変換後のグローバルアドレス	インターフェース
192.168.10.1	172.16.10.1	ipsec0
192.168.10.100	172.16.10.2	ipsec0

IPsec を経由して送信元「192.168.10.1」のパケットを送信する場合には、送信元を「172.16.10.1」に変換し、送信元「192.168.10.100」のパケットを送信する場合には、送信元を「172.16.10.2」に変換します。

拠点ルータ（XR_B）

ポイント

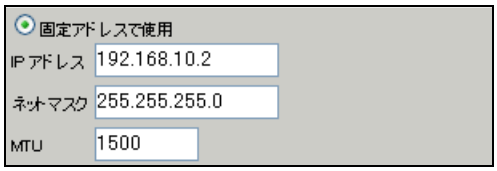
XR_A(センター)と IPsec で接続するための設定を行います。

IPsec の鍵交換モードはアグレッシブモードを使用します。

IPsec での NAT を利用するため、バーチャルサーバ，送信元 NAT を設定しています。

<<インタフェース設定>>

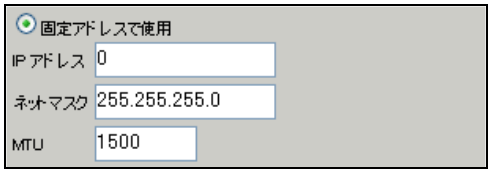
[Ethernet0 の設定]



Ethernet0 に関する設定をします。

※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

[Ethernet1 の設定]

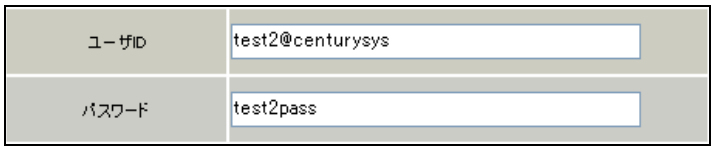


Ethernet1 に関する設定をします。

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

<<PPP/PPPoE 設定>>

[接続先設定 1]



PPPoE 接続で使用するユーザ ID，パスワードを登録します。

［接続設定］

接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ◉Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ○RS232C
接続形態	○手動接続 ◉常時接続 ○スケジューラ接続
RS232C/BRI接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	○無効 ◉有効
ステートフルパケット インスペクション	○無効 ◉有効 ☐DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ◉有効

PPPoE 接続するインタフェース、および接続形態を選択します。
※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション (全回線共通)	☑回線接続時に前回のPPPoEセッションのPADTを強制送出 ☑非接続SessionのIPv4Packet受信時にPADTを強制送出 ☑非接続SessionのLCP-EchoRequest受信時にPADTを強制送出

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

<<フィルタ設定>>

［入力フィルタ］

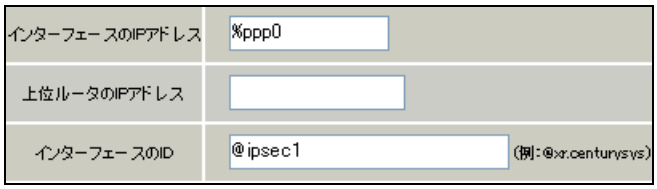
インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	udp		500		500	☐
ppp0	パケット受信時	許可	esp					☐

IKE パケット，ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

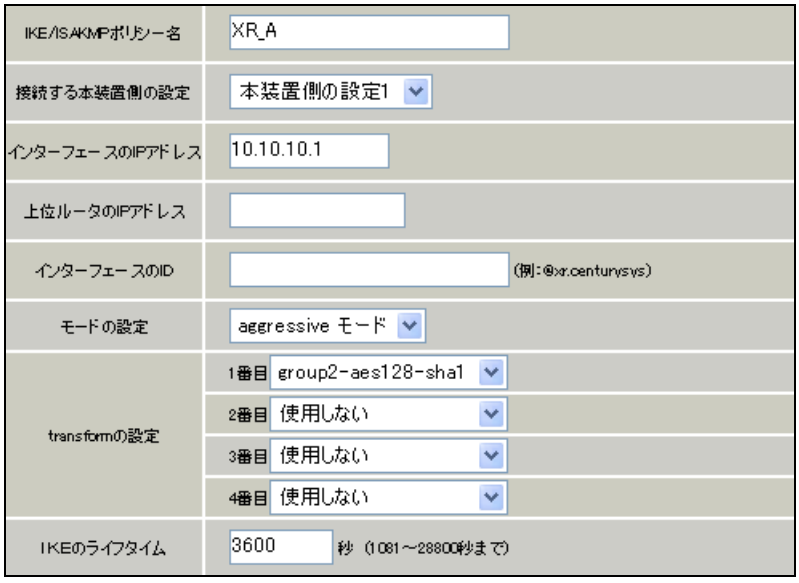
<IPsec サーバ>

[本装置側の設定 1]

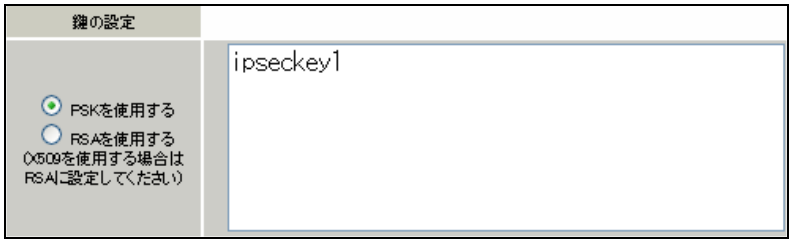


WAN 側インタフェースの IP アドレス，および上位ルータの IP アドレスを設定します。

[IKE/ISAKMP の設定 1]



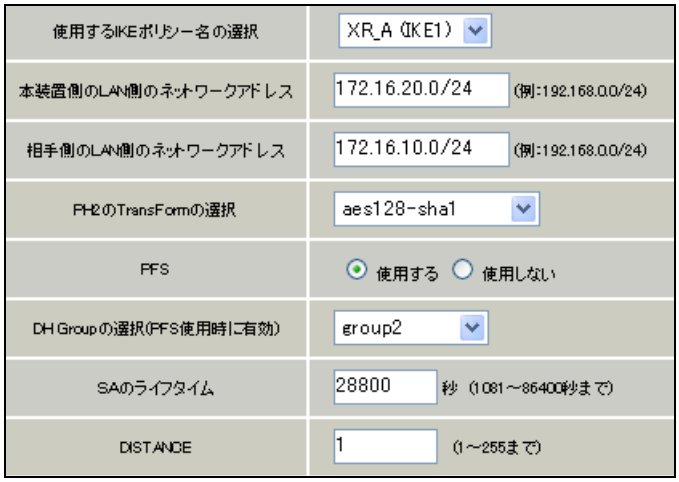
XR_A(センター)に対する ISAKMP ポリシーの設定を行います。



事前共有鍵(PSK)として「ipseckey1」を設定します。

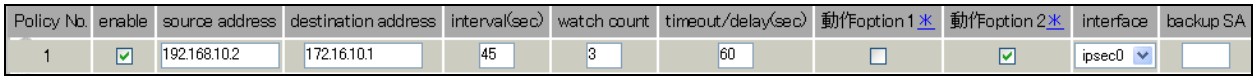
[IPsec ポリシーの設定 1]

XR_A(センター)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。



XR_A(センター)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。
この例では、本装置側の仮想ネットワーク「172.16.20.0/24」と対向の仮想ネットワーク「172.16.10.0/24」の通信に対して IPsec を適用します。

[IPsec Keep-Alive 設定]



XR_A(センター)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。
この設定例では、IPsec KeepAlive パケットが送信時に送信元 NAT で変換されるのを利用しているため、source address が「192.168.10.2」と設定されています。

【IPsec サーバ】

IPsec サーバ機能を起動します。

<<NAT 設定>>

[バーチャルサーバ]

サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース
192.168.10.2	172.16.20.1	全て		ipsec0
192.168.10.200	172.16.20.2	全て		ipsec0

IPsec を経由して「172.16.20.1」宛のパケットを受信した場合には宛先を「192.168.10.2」に変換し、「172.16.20.2」宛のパケットを受信した場合には宛先を「192.168.10.200」に変換します。

[送信元 NAT]

送信元のプライベートアドレス	変換後のグローバルアドレス	インターフェース
192.168.10.2	172.16.20.1	ipsec0
192.168.10.200	172.16.20.2	ipsec0

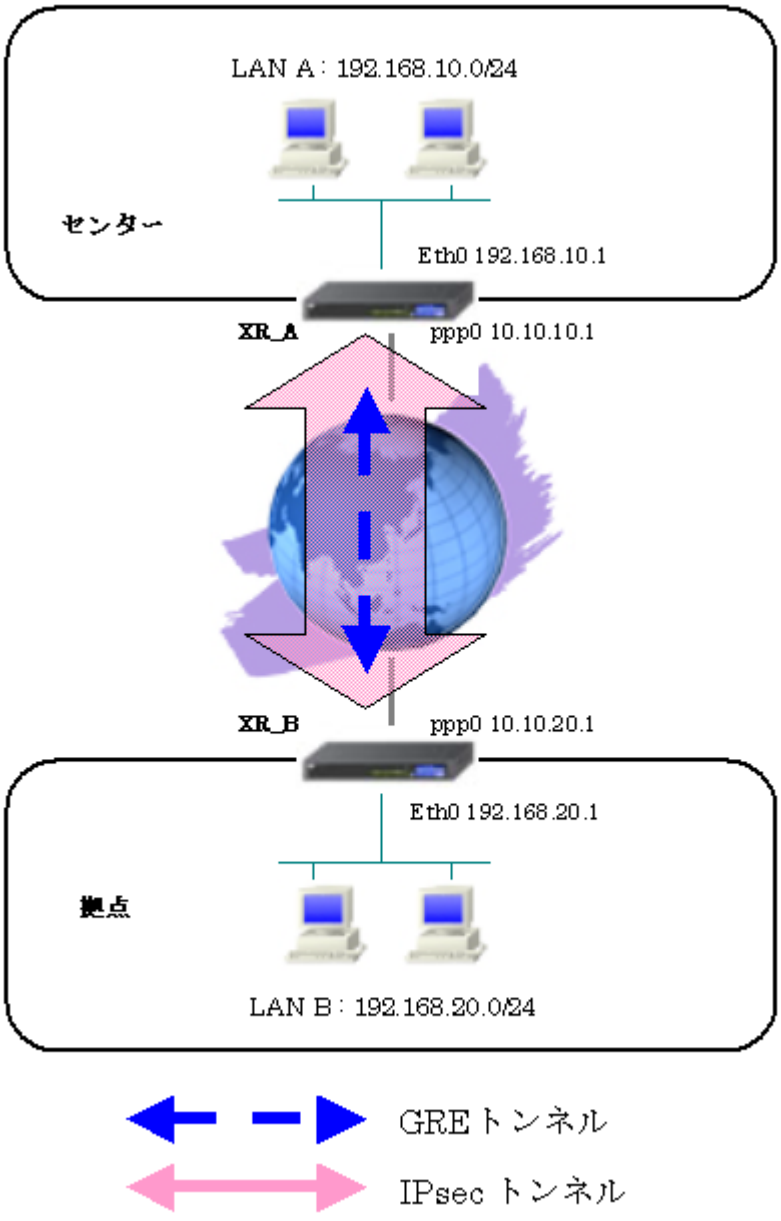
IPsec を経由して送信元「192.168.10.2」のパケットを送信する場合には、送信元を「172.16.20.1」に変換し、送信元「192.168.10.200」のパケットを送信する場合には、送信元を「172.16.20.2」に変換します。

5. GRE over IPsec 設定例

この例は、GRE over IPsec の設定例です。GRE だけでは通信内容を暗号化できませんでしたが、IPsec を併用することにより暗号化することができます。

なお GRE over IPsec は WAN 側 IP アドレスが固定 IP アドレスの場合のみ利用可能です。

5-1. 構成例



5-2. 要件

➢ インタフェースおよび PPP/PPPoE

- インターネットに PPPoE で接続します。
- PPPoE 接続は、自動再接続するように設定しています。
- WAN 側インタフェースの 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は「有効」にしています。

主なインタフェースおよび PPP/PPPoE のパラメータ

	XR_A(センター)	XR_B(拠点)
LAN 側インタフェース	Ether0	Ether0
LAN 側 IP アドレス	192.168.10.1	192.168.20.1
WAN 側インタフェース	Ether1[ppp0]	Ether1[ppp0]
WAN 側 IP アドレス	10.10.10.1	10.10.20.1
PPPoE ユーザ名	test1@centurysys	test2@centurysys
PPPoE パスワード	test1pass	test2pass
WAN 側接続回線	PPPoE 接続	PPPoE 接続

➢ IPsec

- 鍵交換モードはメインモードを使用しています。
- XR_A(センター)は 10.10.10.1/32 <-> 10.10.20.1/32 の時に IPsec を適用します。
- XR_B(拠点)は 10.10.20.1/32 <-> 10.10.10.1/32 の時に IPsec を適用します。
- IPsec KeepAlive は XR_A(センター)，XR_B(拠点)で動作オプション 1 で使用しています。

本装置側のパラメータ

	XR_A(センター)	XR_B(拠点)
インタフェースの IP アドレス	10.10.10.1	10.10.20.1
上位ルータの IP アドレス	%ppp0	%ppp0
インタフェースの ID		

IKE/ISAKMP ポリシーのパラメータ「XR_A(センター),XR_B(拠点)」

	XR_A(センター)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター)
IKE/ISAKMP ポリシー名	XR_B	XR_A
リモート IP アドレス	10.10.20.1	10.10.10.1
インタフェースの ID		
モード	Main	Main
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
DH グループ	Group2	Group2
ライフタイム	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey1

IPsec ポリシーのパラメータ「XR_A(センター),XR_B(拠点)」

	XR_A(センター)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター)
使用する IKE ポリシー名	XR_B(IKE1)	XR_A(IKE1)
本装置の LAN 側のネットワークアドレス	10.10.10.1/32	10.10.20.1/32
相手側の LAN 側のネットワークアドレス	10.10.20.1/32	10.10.10.1/32
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
PFS(DH グループ)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)
DISTANCE	1	1

IPsec Keepalive のパラメータ

	XR_A(センター)	XR_B(拠点 1)
対向拠点	XR_B(拠点 1)	XR_A(センター)
Policy No.	1	1
source address	10.10.10.1	10.10.20.1
destination address	10.10.20.1	10.10.10.1
interval(sec)	30	45
watch count	3	3
timeout/delay(sec)	60	60
動作 option	1	1
interface	ipsec0	ipsec0

- GRE

  - XR_A(センター)のインタフェースアドレスを「172.16.0.1」と設定しています。
  - XR_B(拠点)のインタフェースアドレスを「172.16.0.2」と設定しています。
  - GRE over IPsec を使用するを選択し、IPsec インタフェースを指定します。

主な GRE のパラメータ

	XR_A(センター)	XR_B(拠点)
インタフェースアドレス	172.16.0.1/30	172.16.0.2/30
リモート(宛先)アドレス	10.10.20.1	10.10.10.1
ローカル(送信元)アドレス	10.10.10.1	10.10.20.1
PEER アドレス	172.16.0.2/30	172.16.0.1/30
GREoverIPsec	使用する[ipsec0]	使用する[ipsec0]

- その他

  - XR_A(センター)では拠点側へのルートをスタティックルートでインタフェース「gre1」で設定しています。
  - XR_B(拠点)ではセンター側へのルートをスタティックルートでインタフェース「gre1」で設定しています。

5-3. 設定例

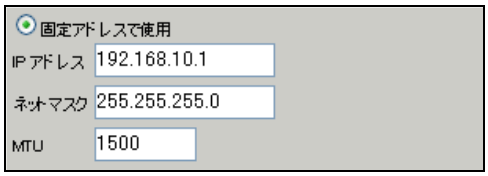
センタールータ（XR_A）

ポイント

XR_B(拠点)と GRE over IPsec で接続するための設定を行います。
IPsec の鍵交換モードはメインモードを使用します。
拠点側への通信が GRE トンネルを通るようにスタティックルートで GRE インタフェースを指定しています。

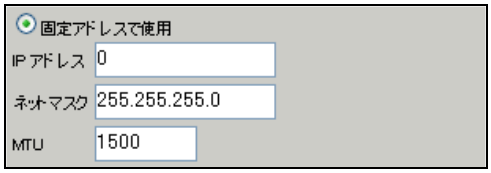
<<インタフェース設定>>

[Ethernet0 の設定]



Ethernet0 に関する設定をします。
※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

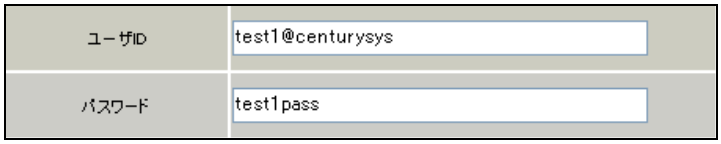
[Ethernet1 の設定]



Ethernet1 に関する設定をします。
PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

<<PPP/PPPoE 設定>>

[接続先設定 1]



PPPoE 接続で使用するユーザ ID，パスワードを登録します。

［接続設定］

接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ◉Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ○RS232C
接続形態	○手動接続 ◉常時接続 ○スケジューラ接続
RS232C/BRI接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	○無効 ◉有効
ステートフルパケット インスペクション	○無効 ◉有効 ☐DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ◉有効

PPPoE 接続するインタフェース、および接続形態を選択します。
※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション（全回線共通）	☑回線接続時に前回のPPPoEセッションのPADTを強制送出 ☑非接続SessionのIPv4Packet受信時にPADTを強制送出 ☑非接続SessionのLCP-EchoRequest受信時にPADTを強制送出

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

<<フィルタ設定>>

［入力フィルタ］

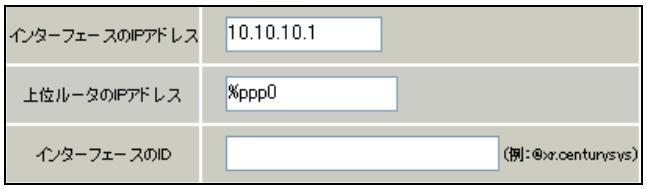
インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	udp		500		500	☐
ppp0	パケット受信時	許可	esp					☐

IKE パケット，ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

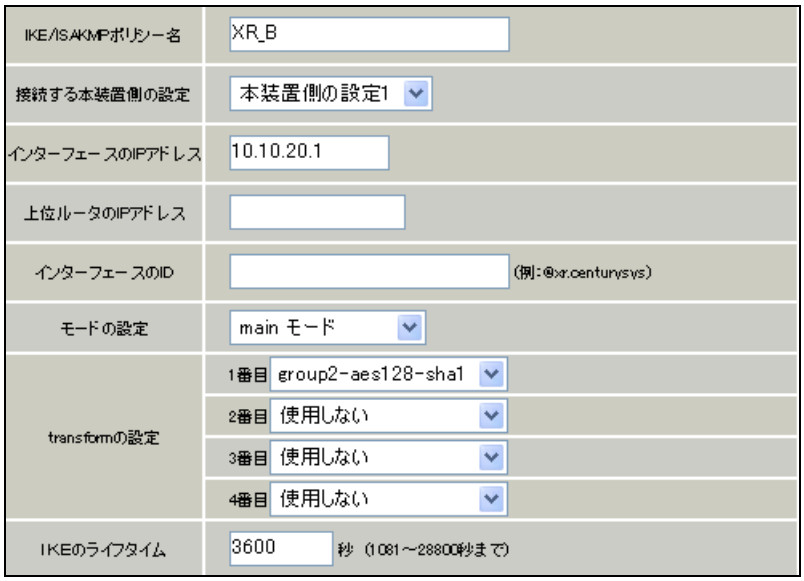
<IPsec サーバ>

[本装置側の設定 1]

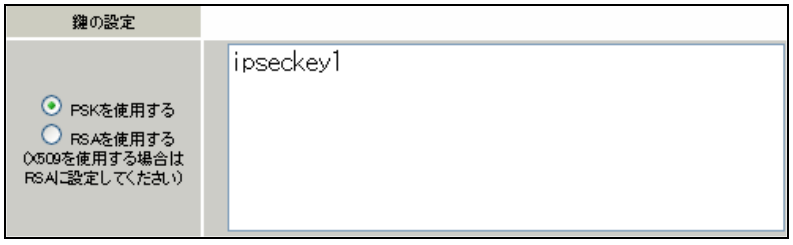


XR_A(センター)の WAN 側インタフェースの IP アドレス,および上位ルータの IP アドレスを設定します。
PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

[IKE/ISAKMP の設定 1]



XR_B(拠点)に対する IKE/ISAKMP ポリシーを設定します。



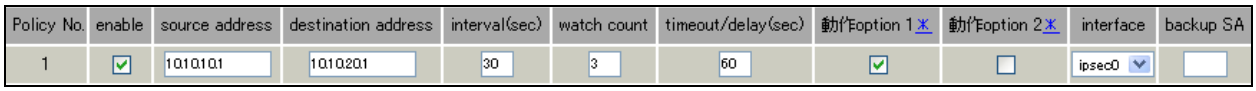
事前共有鍵(PSK)として「ipseckey1」を設定しています。

[IPsec ポリシーの設定 1]

XR_B(拠点)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

XR_B(拠点)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。
この例では GRE over IPsec を使用しているため、XR_A(センター)と XR_B(拠点)の WAN 側 IP アドレスをそれぞれ指定しています。
※ 本装置の LAN 側ネットワークアドレス,および相手の LAN 側ネットワークアドレスの項目に関しては、この項目に「空欄」を設定した場合、WAN 側 IP アドレスを設定したのと同じ意味になります。

[IPsec Keep-Alive 設定]



XR_B(拠点)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

IPsec サーバ機能を起動します。

<<GRE 設定>>

インタフェースアドレス	172.16.0.1/30 (例:192.168.0.1/30)
リモート(宛先)アドレス	10.10.20.1 (例:192.168.1.1)
ローカル(送信元)アドレス	10.10.10.1 (例:192.168.2.1)
PEERアドレス	172.16.0.2/30 (例:192.168.0.2/30)

XR_B(拠点)との GRE トンネルを設定します。

GREoverIPSec	◉ 使用する ipsec0 ○ Routing Tableに依存

この例では GRE over IPsec を使用しますので、「使用する」を選択し、インタフェースとして「ipsec0」を設定しています。

<<スタティックルート設定>>

アドレス	ネットマスク	インターフェース/ゲートウェイ		ディスタンス <1-255>
192.168.20.0	255.255.255.0	gre1		1

拠点側への通信が GRE トンネルを通るように GRE インタフェースを指定しています。

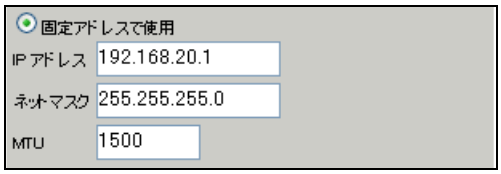
拠点ルータ（XR_B）

ポイント

XR_A(センター)と GRE over IPsec で接続するための設定を行います。
IPsec の鍵交換モードはメインモードを使用します。
拠点側への通信が GRE トンネルを通るようにスタティックルートで GRE インタフェースを指定しています。

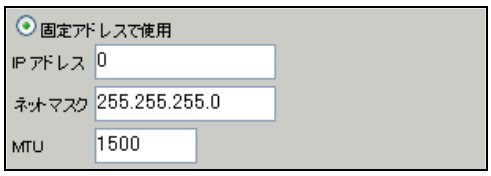
<<インタフェース設定>>

[Ethernet0 の設定]



Ethernet0 に関する設定をします。
※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

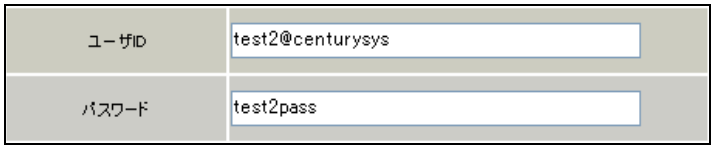
[Ethernet1 の設定]



Ethernet1 に関する設定をします。
PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

<<PPP/PPPoE 設定>>

[接続先設定 1]



PPPoE 接続で使用するユーザ ID，パスワードを登録します。

［接続設定］

接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ◉Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ○RS232C
接続形態	○手動接続 ◉常時接続 ○スケジューラ接続
RS232C/BRI接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	○無効 ◉有効
ステートフルパケット インスペクション	○無効 ◉有効 ☐DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ◉有効

PPPoE 接続するインタフェース、および接続形態を選択します。
※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション (全回線共通)	☑回線接続時に前回のPPPoEセッションのPADTを強制送出 ☑非接続SessionのIPv4Packet受信時にPADTを強制送出 ☑非接続SessionのLCP-EchoRequest受信時にPADTを強制送出

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

<<フィルタ設定>>

［入力フィルタ］

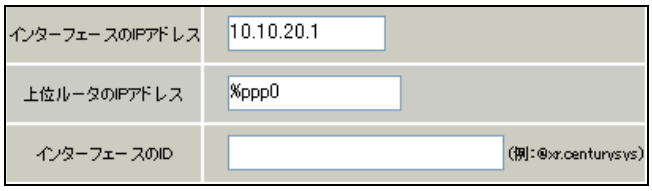
インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	udp		500		500	☐
ppp0	パケット受信時	許可	esp					☐

IKE パケット，ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

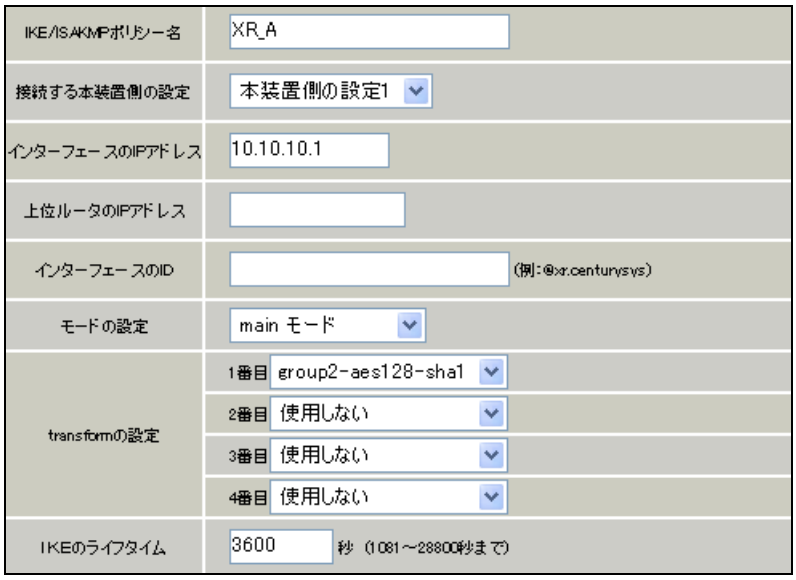
<IPsec サーバ>

[本装置側の設定 1]

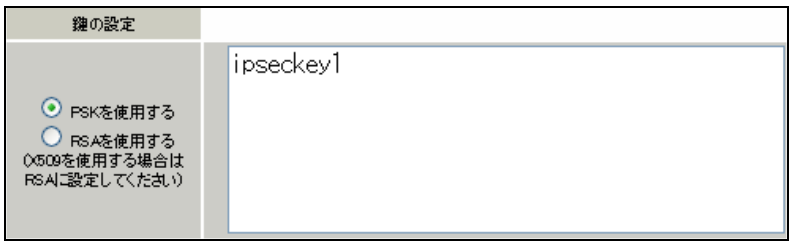


WAN 側インタフェースの IP アドレス，および上位ルータの IP アドレスを設定します。

[IKE/ISAKMP の設定 1]



XR_A(センター)に対する ISAKMP ポリシーの設定を行います。



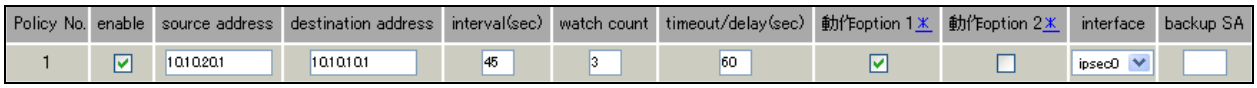
事前共有鍵(PSK)として「ipseckey1」を設定します。

[IPsec ポリシーの設定 1]

XR_A(センター)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

XR_A(センター)に対して IPsec 通信を行う IP アドレスの範囲を設定します。
この例では GRE over IPsec を使用しているため、XR_B(拠点)と XR_A(センター)との WAN 側 IP アドレスをそれぞれ指定しています。
※ 本装置の LAN 側ネットワークアドレス,および相手の LAN 側ネットワークアドレスの項目に関しては、この項目に「空欄」を設定した場合、WAN 側 IP アドレスを設定したのと同じ意味になります。

[IPsec Keep-Alive 設定]



XR_A(センター)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

IPsec サーバ機能を起動します。

<<GRE 設定>>

インタフェースアドレス	172.16.0.2/30 (例:192.168.0.1/30)
リモート(宛先)アドレス	10.10.10.1 (例:192.168.1.1)
ローカル(送信元)アドレス	10.10.20.1 (例:192.168.2.1)
PEERアドレス	172.16.0.1/30 (例:192.168.0.2/30)

XR_A(センター)との GRE トンネルを設定します。

GREoverIPSec	◉ 使用する ipsec0 ○ Routing Tableに依存

この例では GRE over IPsec を使用しますので、「使用する」を選択し、インタフェースとして「ipsec0」を設定しています。

<<スタティックルート設定>>

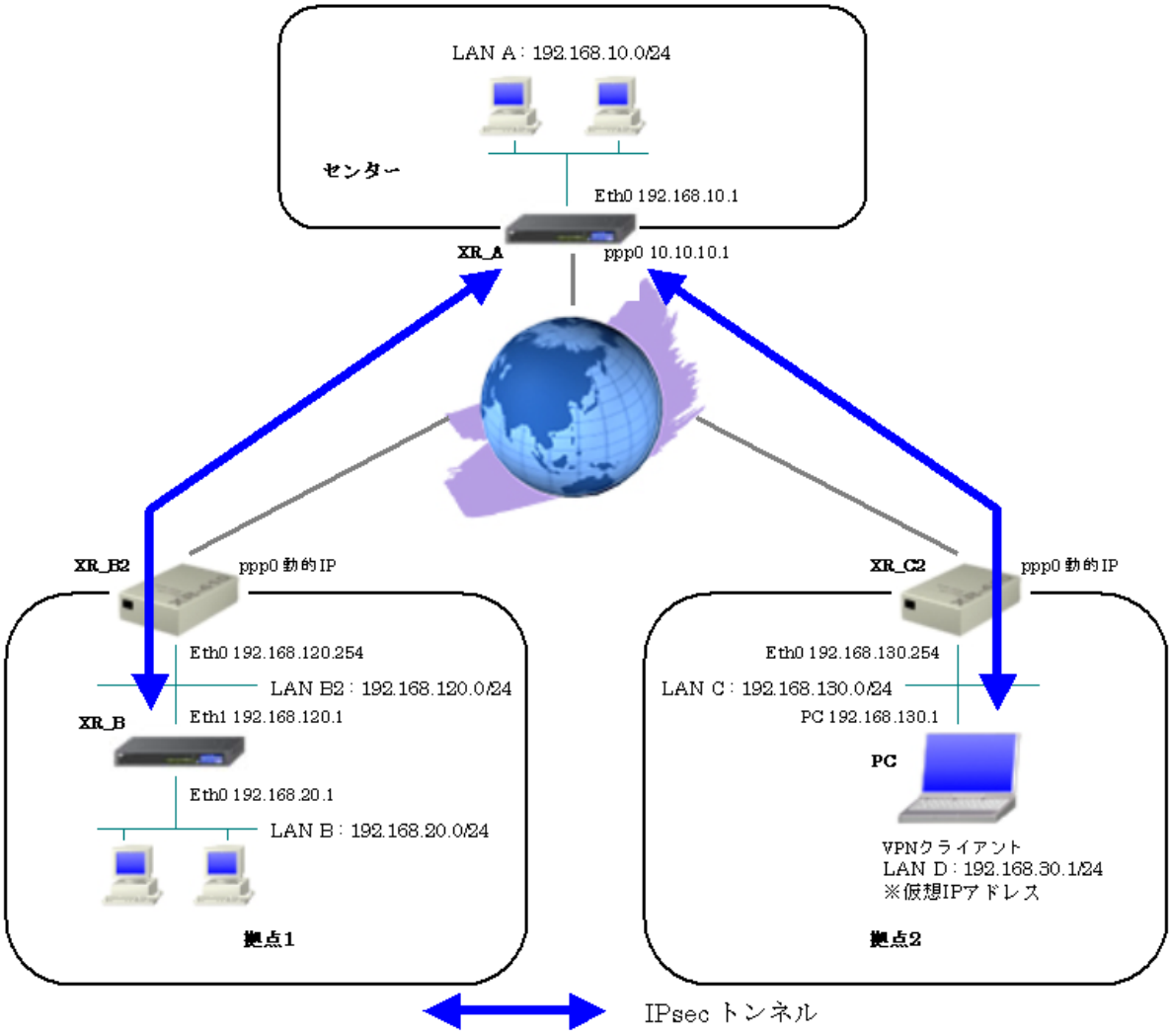
アドレス	ネットマスク	インターフェース/ゲートウェイ		ディスタンス <1-255>
192.168.10.0	255.255.255.0	gre1		1

センター側への通信が GRE トンネルを通るように GRE インタフェースを指定しています。

6. IPsec NAT-Traversal 設定例 1

この例は、IPsec NAT-Traversal を利用した IPsec 接続の設定例です。拠点側にインターネットアクセス用の NAT ルータがあり、その配下に IPsec 接続をするルータや VPN クライアントが存在する構成です。

6-1. 構成例



6-2. 要件

➢ インタフェースおよび PPP/PPPoE

- インターネットに PPPoE で接続します。
- PPPoE 接続は、自動再接続するように設定しています。
- WAN 側インタフェースの 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は「有効」にしています。
- XR_B(拠点 1)はローカルルータの設定をします。

主なインタフェースおよび PPP/PPPoE のパラメータ(1)

	XR_A(センター)	XR_B2(拠点 1)	XR_C2(拠点 2)
LAN 側インタフェース	Ether0	Ether0	Ether0
LAN 側 IP アドレス	192.168.10.1	192.168.120.254	192.168.130.254
WAN 側インタフェース	Ether1[ppp0]	Ether1[ppp0]	Ether1[ppp0]
WAN 側 IP アドレス	10.10.10.1	動的 IP	動的 IP
PPPoE ユーザ名	test1@centurysys	test2@centurysys	test3@centurysys
PPPoE パスワード	test1pass	test2pass	test3pass
WAN 側接続回線	PPPoE 接続	PPPoE 接続	PPPoE 接続

主なインタフェースおよび PPP/PPPoE のパラメータ(2)

	XR_B(拠点 1)	PC(拠点 2)
LAN 側インタフェース	Ether0	-
LAN 側 IP アドレス	192.168.20.1	-
WAN 側インタフェース	Ether1	-
WAN 側 IP アドレス	192.168.120.1	192.168.130.1
デフォルトゲートウェイ	192.168.120.254	192.168.130.254

- IPsec

  - 鍵交換モードはアグレッシブモードを使用しています。
  - XR_A(センター)は 192.168.10.0/24 <-> 192.168.20.0/24, 192.168.10.0/24 <-> 192.168.30.1/32 の時に IPsec を適用します。
  - XR_B(拠点 1)は 192.168.20.0/24 <-> 192.168.10.0/24 の時に IPsec を適用します。
  - PC(拠点 2)は 192.168.30.1/32 <-> 192.168.10.0/24 の時に IPsec を適用します。
  - XR_A(センター)は、IPsec NAT-Traversal の Responder 側になるため、NAT-Traversal の Virtual Private 設定を行っています。
  - XR_B(拠点 1)は、IPsec NAT-Traversal の Initiator 側になるため、NAT-Traversal を「使用する」を選択し、Virtual Private 設定を行っていません。
  - IPsec KeepAlive は XR_B(拠点)が動作オプション 2 で使用しています。

本装置側のパラメータ

	XR_A(センター)	XR_B(拠点 1)
NAT Traversal	使用する	使用する
Virtual Private 設定	192.168.20.0/24	
Virtual Private 設定 2	192.168.30.1/32	
インタフェースの IP アドレス	10.10.10.1	192.168.120.1
上位ルータの IP アドレス	%ppp0	192.168.120.254
インタフェースの ID		@ipsec1

IKE/ISAKMP ポリシーのパラメータ「XR_A(センター),XR_B(拠点 1)」

	XR_A(センター)		XR_B(拠点 1)
対向拠点	XR_B(拠点 1)	PC(拠点 2)	XR_A(センター)
IKE/ISAKMP ポリシー名	XR_B	PC	XR_A
リモート IP アドレス	0.0.0.0	0.0.0.0	10.10.10.1
インタフェースの ID	@ipsec1	@vpnclient	
モード	Aggressive	Aggressive	Aggressive
暗号化アルゴリズム	AES-128	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1	SHA1
DH グループ	Group2	Group2	Group2
ライフタイム	3600(秒)	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey2	ipseckey1

IPsec ポリシーのパラメータ「XR_A(センター),XR_B(拠点 1)」

	XR_A(センター)		XR_B(拠点)
対向拠点	XR_B(拠点 1)	PC(拠点 2)	XR_A(センター)
使用する IKE ポリシー名	XR_B(IKE1)	PC(IKE2)	XR_A(IKE1)
本装置の LAN 側のネットワークアドレス	192.168.10.0/24	192.168.10.0/24	192.168.20.0/24
相手側の LAN 側のネットワークアドレス	vnet:%priv	vhost:%priv	192.168.10.0/24
暗号化アルゴリズム	AES-128	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1	SHA1
PFS(DH グループ)	使用する(Group2)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)	28800(秒)
DISTANCE	1	1	1

IPsec Keepalive のパラメータ

	XR_B(拠点 1)
対向拠点	XR_A(センター)
Policy No.	1
source address	192.168.20.1
destination address	192.168.10.1
interval(sec)	45
watch count	3
timeout/delay(sec)	60
動作 option	2
interface	ipsec6

- その他

  - 本設定例では、NAT ルータとして XR を使用しています。

6-3. 設定例

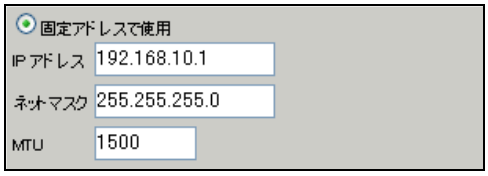
センタールータ（XR_A）

ポイント

XR_B(拠点 1)と PC(拠点 2)と IPsec NAT-Traversal で接続するための設定を行います。
IPsec の鍵交換モードはアグレッシブモードを使用します。
XR_A(センター)は、IPsec NAT-Traversal の Responder 側になるため、NAT-Traversal の Virtual Private 設定を行っています。
IPsec NAT-Traversal で使用する UDP のポート番号をフィルタで許可しています。

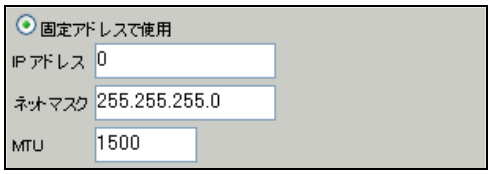
<<インタフェース設定>>

[Ethernet0 の設定]



Ethernet0 に関する設定をします。
※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

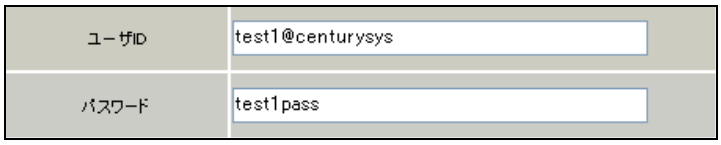
[Ethernet1 の設定]



Ethernet1 に関する設定をします。
PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

<<PPP/PPPoE 設定>>

[接続先設定 1]



PPPoE 接続で使用するユーザ ID，パスワードを登録します。

［接続設定］

接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ◉Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ○RS232C
接続形態	○手動接続 ◉常時接続 ○スケジューラ接続
RS232C/BRI接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	○無効 ◉有効
ステートフルパケット インスペクション	○無効 ◉有効 ☐DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ◉有効

PPPoE 接続するインタフェース、および接続形態を選択します。
※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション (全回線共通)	☑回線接続時に前回のPPPoEセッションのPADTを強制送出 ☑非接続SessionのIPv4Packet受信時にPADTを強制送出 ☑非接続SessionのLCP-EchoRequest受信時にPADTを強制送出

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

<<フィルタ設定>>

［入力フィルタ］

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	udp		500		500	☐
ppp0	パケット受信時	許可	udp		4500		4500	☐

IKE パケット，NAT-Traversal 使用時にカプセル化する UDP ポート「4500」のパケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

<IPsec サーバ>

[本装置の設定]

NAT Traversal	◉ 使用する ○ 使用しない
Virtual Private設定	%v4:192.168.20.0/24
Virtual Private設定2	%v4:192.168.30.1/32

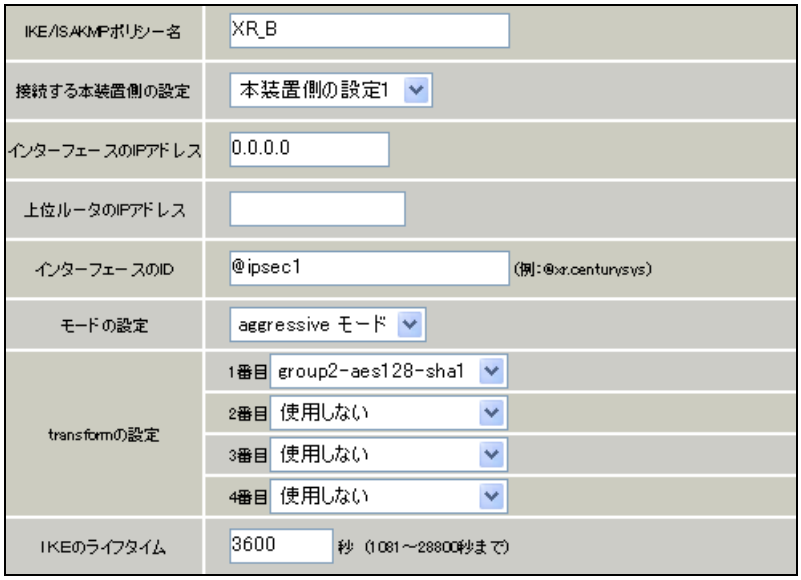
NAT Traversal を利用するため、「使用する」を選択します。
Virtual Private 設定では、NAT-Traversal を使用しているルータ配下の LAN または NAT-Traversal を使用している機器のアドレスを設定します。
この例では、XR_B(拠点 1)の配下の LAN「192.168.20.0/24」と NAT-Traversal を使用している機器「PC(拠点 2)」のアドレスを設定しています。

[本装置側の設定 1]

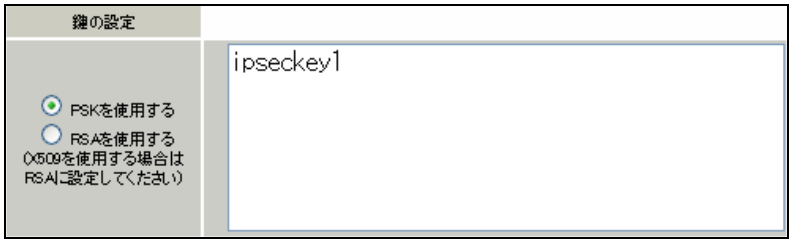
インターフェースのIPアドレス	10.10.10.1
上位ルータのIPアドレス	%ppp0
インターフェースのID	(例:@xr.centurysys)

XR_A(センター)の WAN 側インタフェースの IP アドレス,および上位ルータの IP アドレスを設定します。
PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

[IKE/ISAKMP の設定 1]



XR_B(拠点 1)に対する IKE/ISAKMP ポリシーを設定します。



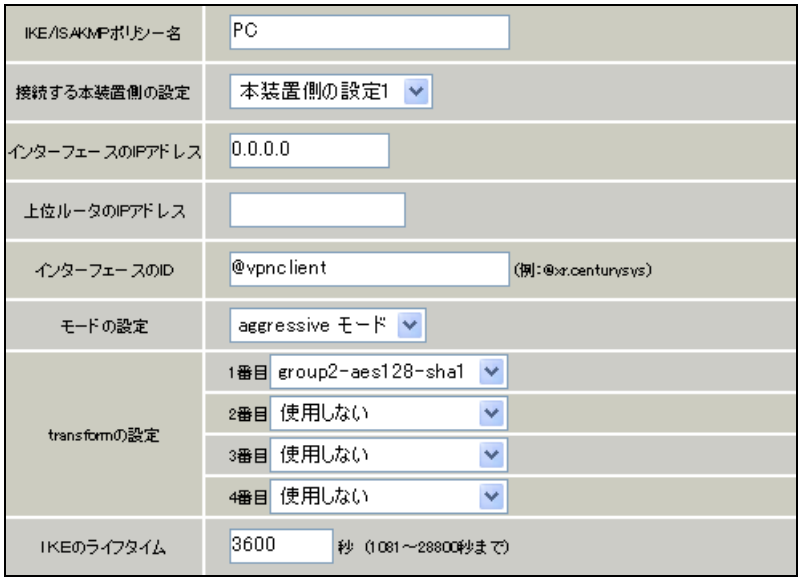
事前共有鍵(PSK)として「ipseckey1」を設定しています。

[IPsec ポリシーの設定 1]

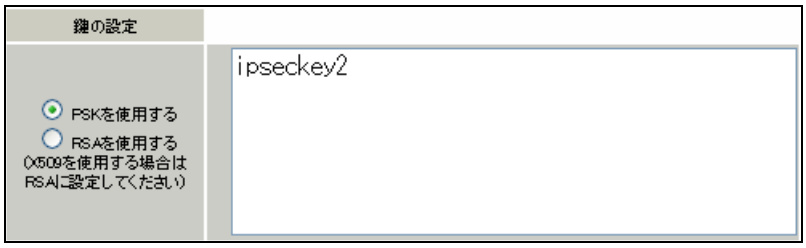
XR_B(拠点 1)の IP アドレスが不定のため、「Responder として使用する」を選択します。

XR_B(拠点 1)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。
NAT-Traversal を使用しているルータ配下の LAN を指定する場合は「vnet:%priv」を指定します。

[IKE/ISAKMP の設定 2]



PC(拠点 2)に対する IKE/ISAKMP ポリシーを設定します。



事前共有鍵(PSK)として「ipseckey2」を設定しています。

[IPsec ポリシーの設定 2]

PC(拠点 2)の IP アドレスが不定のため、「Responder として使用する」を選択します。

PC(拠点 2)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。
NAT-Traversal を使用している機器を指定する場合は「vhost:%priv」を指定します。

【IPsec サーバ】

IPsec サーバ機能を起動します。

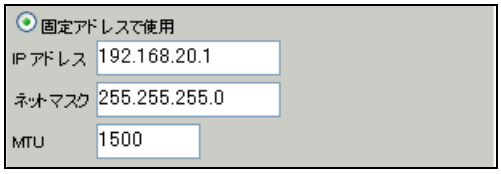
拠点 1 ルータ（XR_B）

ポイント

XR_A(センター)と IPsec NAT-Traversal で接続するための設定を行います。
IPsec の鍵交換モードはアグレッシブモードを使用します。
XR_B(拠点 1)は、IPsec NAT-Traversal の Initiator 側になるため、NAT-Traversal を「使用する」を選択し、Virtual Private 設定を行っていません。
IPsec NAT-Traversal で使用する UDP のポート番号をフィルタで許可しています。

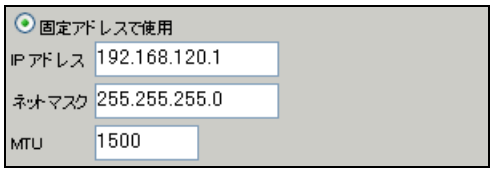
<<インタフェース設定>>

[Ethernet0 の設定]

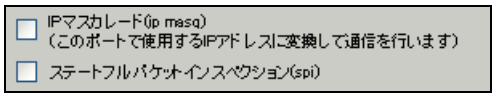


Ethernet0 に関する設定をします。
※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

[Ethernet1 の設定]

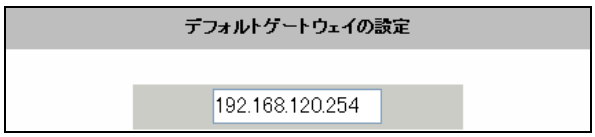


Ethernet1 の IP アドレスの設定をします。



この例では、NAT Traversal を使用するルータの WAN 側では IP マスカレードおよびステートフルパケットインスペクション(spi)は使用していません。

[その他の設定]



XR_B の上位ルータである XR_B2 をデフォルトゲートウェイとして指定しています。

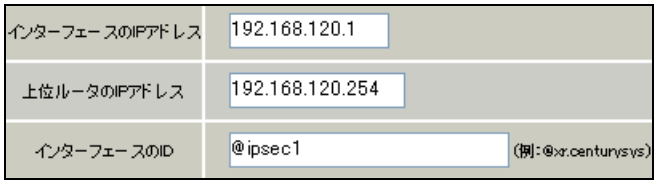
<<各種サービスの設定>>

<IPsec サーバ>

[本装置の設定]

NAT Traversal を利用するため、「使用する」を選択します。

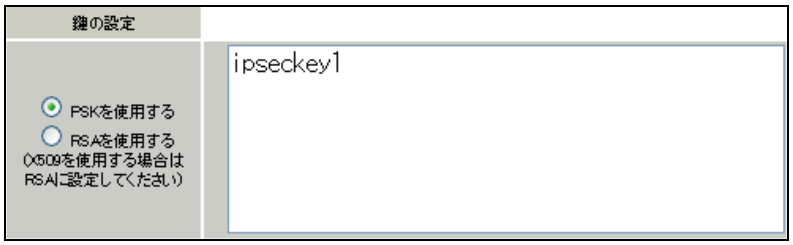
[本装置側の設定 1]



WAN 側インタフェースの IP アドレス，および上位ルータの IP アドレスを設定します。
XR_B は NAT ルータ配下にあるため、「インタフェースの ID」を設定しています。

[IKE/ISAKMP の設定 1]

XR_A(センター)に対する ISAKMP ポリシーの設定を行います。



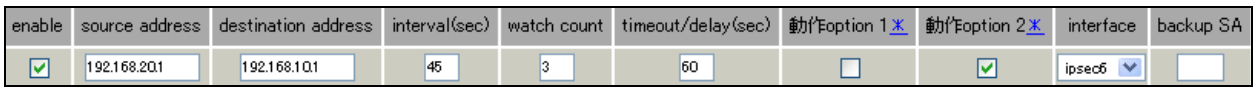
事前共有鍵(PSK)として「ipseckey1」を設定します。

[IPsec ポリシーの設定 1]

XR_A(センター)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

XR_A(センター)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

[IPsec Keep-Alive 設定]



XR_A(センター)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

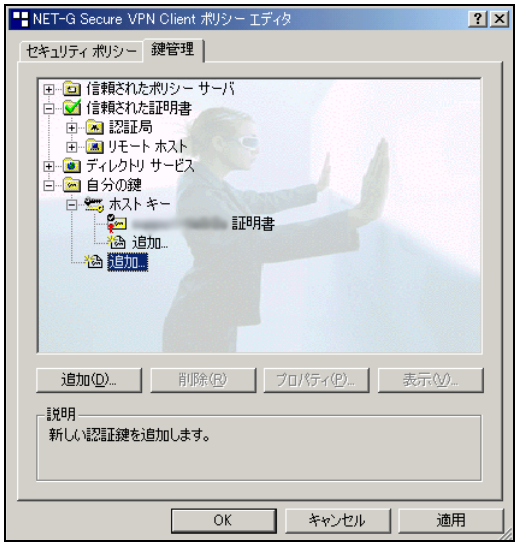
IPsec サーバ機能を起動します。

拠点 2 PC（PC）

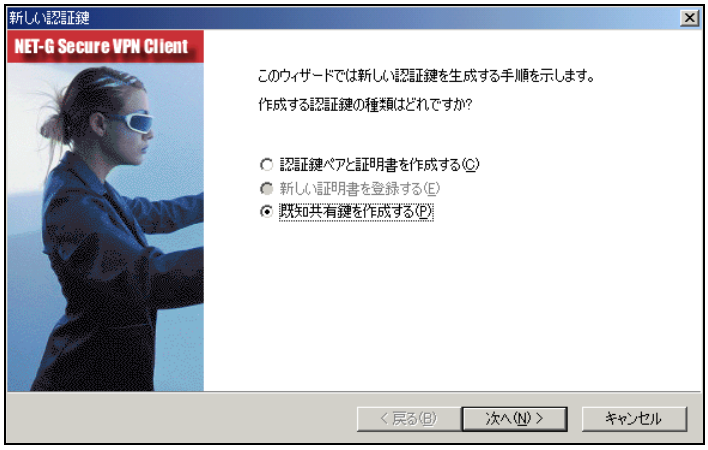
ポイント

拠点 2 は「FutureNet VPN Client/NET-G」をインストールした PC からの IPsec NAT Traversal 接続になります。

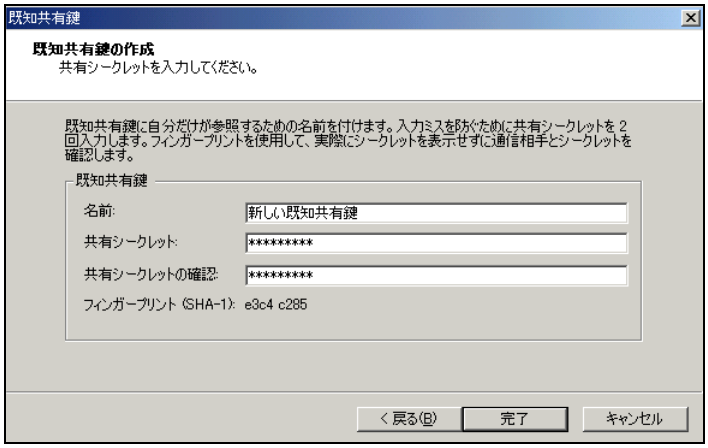
<<既知共有鍵(Pre shared Key)の設定>>



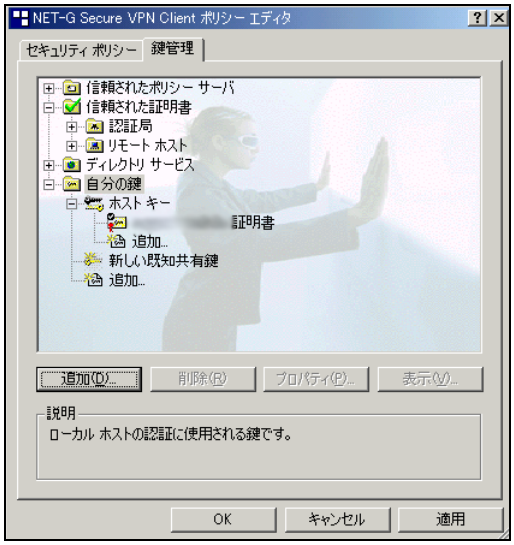
「鍵管理」タブをクリックし、「自分の鍵」を選択し、「追加」ボタンをクリックします。



「新しい認証鍵」ウィンドウが開きますので、「既知共有鍵を作成する」を選択し、「次へ」ボタンをクリックして下さい。

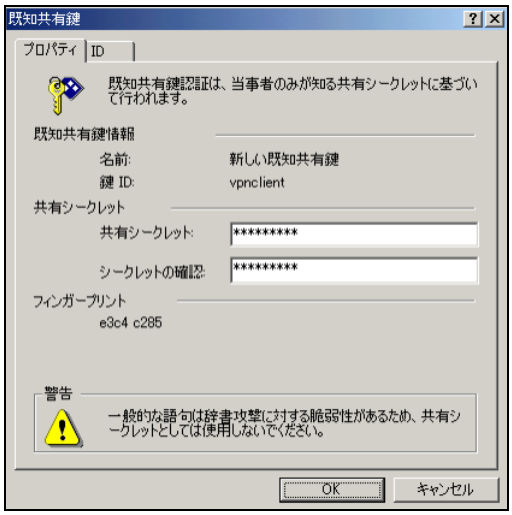


「既知共有鍵の作成」画面が開きます。ここで既知共有鍵を作成します。「名前」には任意の設定名を入力します。「共有シークレット」「共有シークレットの確認」項目には既知共有鍵を入力し、「完了」ボタンをクリックします。
この例では共有シークレットとして「ipseckey2」を設定しています。

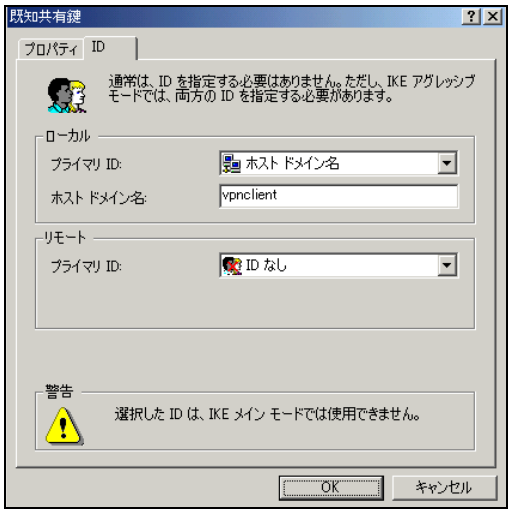


「鍵管理」画面に戻ります。既知共有鍵が登録されていることを確認したら、必ず「適用」ボタンをクリックして下さい。「適用」ボタンをクリックしないと適切に設定されない場合があります。

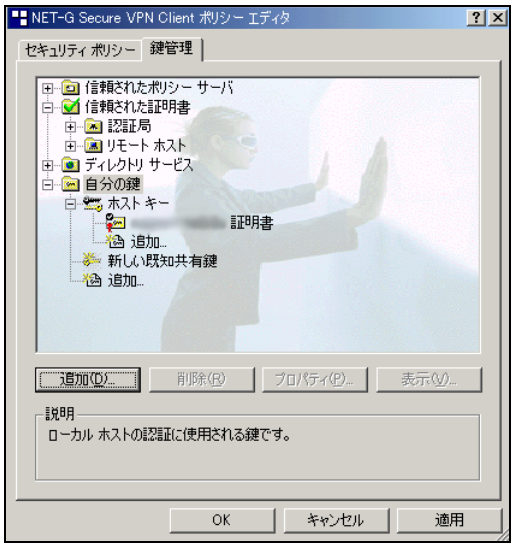
<<ID の設定>>



「鍵管理」画面で、登録した既知共有鍵を選択して「プロパティ」をクリックします。「既知共有鍵」画面が開きますので、「ID」タブをクリックします(この画面では既知共有鍵を変更できます)。



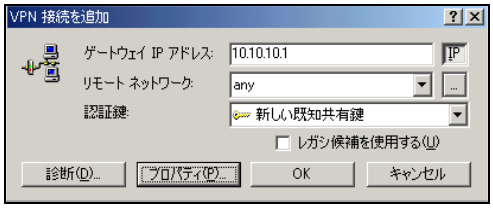
「ローカル」側項目について、プライマリ ID は「ホストドメイン名」を選択し、ホストドメイン名に ID を入力します。ここには XR シリーズの IPsec サーバ「IKE/ISAKMP の設定」における「インタフェース ID」と同じ ID を設定します。
※ただしこの時、ホストドメイン名には”@”をつけないで設定して下さい。



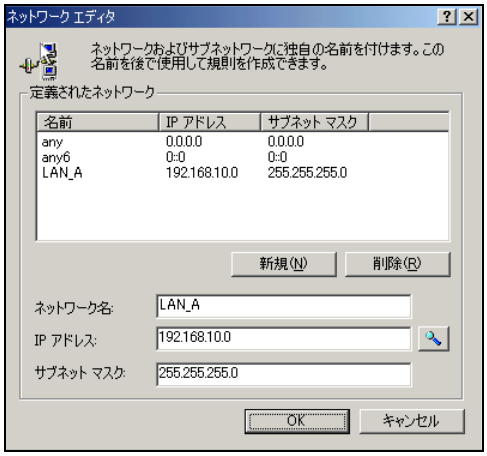
「OK」ボタンをクリックすると、「鍵管理」画面に戻ります。ここまでの設定が終わったら、必ず「適用」ボタンをクリックして下さい。「適用」ボタンをクリックしないと適切に設定されない場合があります。

<<セキュリティポリシーの設定>>

ポリシーエディタの「セキュリティポリシー」タブをクリックします。「VPN 接続」を選択し「追加」をクリックします。

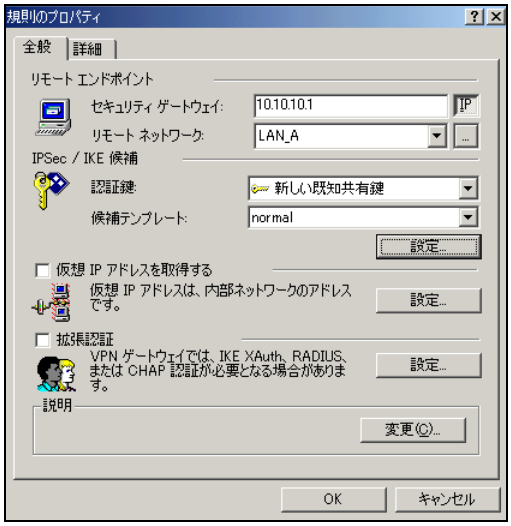


「VPN 接続を追加」画面が開きます。「ゲートウェイ IP アドレス」で右端の”IP”をクリックし、XR_A(センター)の WAN 側 IP アドレスを設定します。
「認証鍵」は、既知共有鍵の設定で登録した既知共有鍵の設定名を選択します。
「リモートネットワーク」については右端にある”・・・”をクリックして下さい。



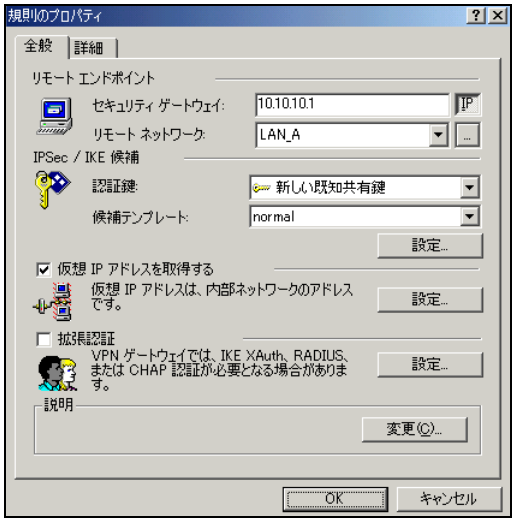
「ネットワークエディタ」画面が開きます。
「ネットワーク名」は任意の名前を設定することができます。
「IP アドレス」「サブネットマスク」は XR に接続している LAN について設定し（ここでは LAN_A[センター側のネットワーク]の値を設定しています)、「OK」をクリックします。

リモートネットワーク設定後、「VPN 接続を追加」画面が開きますので、続いてプロパティをクリックします。

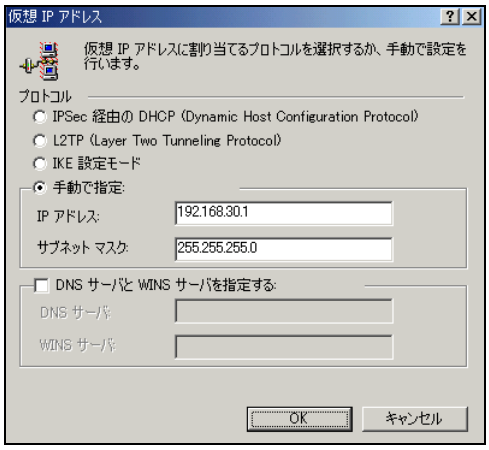


「規則のプロパティ」画面が開きます。ここで IPsec/IKE 候補の
設定ボタンをクリックします。

「パラメータ候補画面」が開きます。ここで暗号化方式などを設定します。IKE モードは「aggressive mode」を設定します。また「選択した値のみを候補に加える」にチェックをいれます。

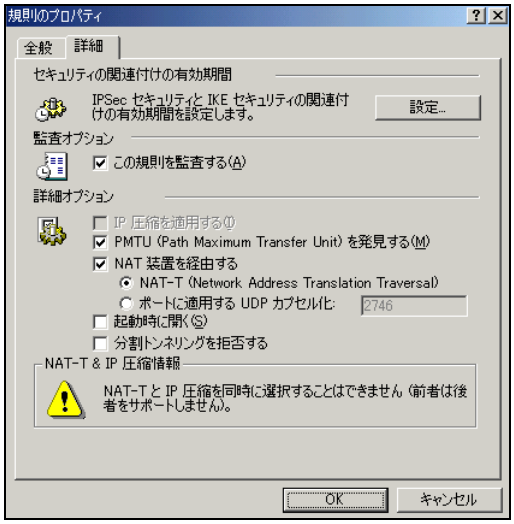


「OK」ボタンをクリックして「規則のプロパティ」画面に戻ります。
続いて「仮想 IP アドレスを取得する」にチェックを入れ、「設定」ボタンをクリックします。

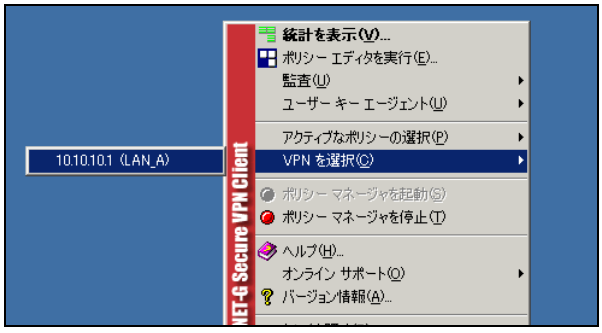


「仮想 IP アドレス」画面が開きます。
ここでは XR に接続する際に使用するこの PC の仮想的な IP アドレスを設定します。
この例では「192.168.30.1」としています。
「プロトコル」は”手動で指定”を選択し、任意のプライベート IP アドレスとサブネットマスクを入力します。
ここで設定する IP アドレスは XR_A(センター)の IPsec サーバにおける「IPsec ポリシーの設定 2」の”相手側の LAN 側のネットワークアドレス”と一致させます。この例では、サブネットマスクは 24 ビットマスクとしています。(32 ビットマスクは設定することができません。)

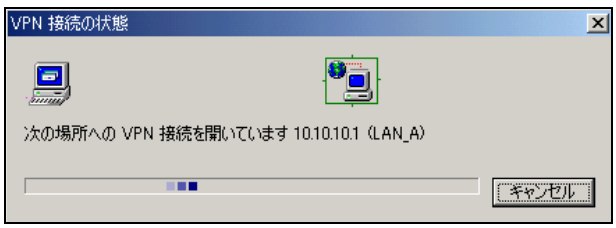
仮想 IP アドレス設定後、「規則のプロパティ」画面を開き、「詳細タブ」をクリックします。ここで詳細オプションにある「NAT 装置を経由する」のチェックボックスを有効にし、「NAT-T(Network Address Translation Traversal)」を選択します。



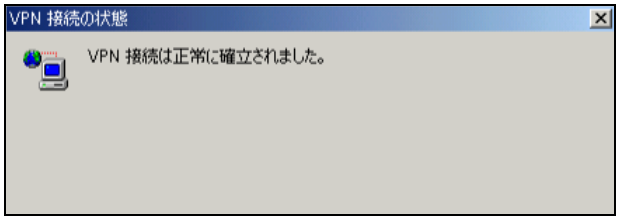
これで設定は完了です。
続いて IPsec 接続を行います。



タスクトレーの中にある FutureNet Net-G VPNclient のアイコンを右クリックします。そして「VPN を選択」の指定し、作成した IPsec ポリシーを選択します。



選択後、IKE のネゴシエーションを行う画面が表示されます。



IPsec が正常に確立した場合、「VPN 接続は正常に確立しました」という画面が表示されます。

これで IPsec 接続は完了です。

NAT ルータ

ポイント

この設定例では、NAT ルータの設定例は記載していません。

NAT ルータの主な必要な要件は以下のとおりです。

・インターネット接続ができていること

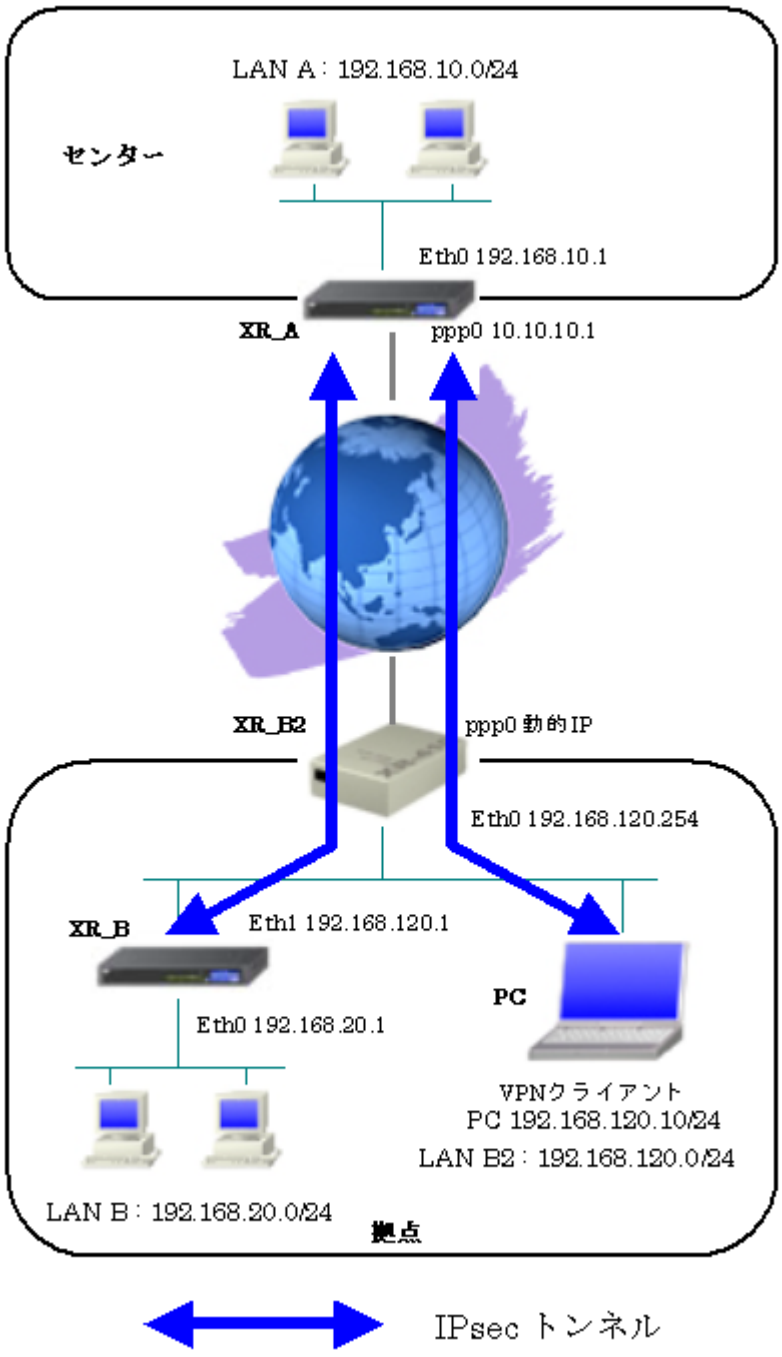
・IP マスカレードが有効になっていること

・フィルタ設定で IPsec NAT-Traversal で使用する UDP ポートが許可されていること

7. IPsec NAT-Traversal 設定例２

この例は、IPsec NAT-Traversal を利用した IPsec 接続の設定例です。拠点側にインターネットアクセス用のNATルータがあり、その配下にIPsec接続をするXRやVPNクライアントが複数存在する構成です。

7-1. 構成例



7-2. 要件

➢ インタフェースおよび PPP/PPPoE

- インターネットに PPPoE で接続します。
- PPPoE 接続は、自動再接続するように設定しています。
- WAN 側インタフェースの 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は「有効」にしています。
- XR_B(拠点)はローカルルータの設定をします。

主なインタフェースおよび PPP/PPPoE のパラメータ(1)

	XR_A(センター)	XR_B2(拠点)
LAN 側インタフェース	Ether0	Ether0
LAN 側 IP アドレス	192.168.10.1	192.168.120.254
WAN 側インタフェース	Ether1[ppp0]	Ether1[ppp0]
WAN 側 IP アドレス	10.10.10.1	動的 IP
PPPoE ユーザ名	test1@centurysys	test2@centurysys
PPPoE パスワード	test1pass	test2pass
WAN 側接続回線	PPPoE 接続	PPPoE 接続

主なインタフェースおよび PPP/PPPoE のパラメータ(2)

	XR_B(拠点)	PC(拠点)
LAN 側インタフェース	Ether0	-
LAN 側 IP アドレス	192.168.20.1	-
WAN 側インタフェース	Ether1	-
WAN 側 IP アドレス	192.168.120.1	192.168.120.10
デフォルトゲートウェイ	192.168.120.254	192.168.120.254

➢ IPsec

- 鍵交換モードはアグレッシブモードを使用しています。
- XR_A(センター)は 192.168.10.0/24 <-> 192.168.20.0/24, 192.168.10.0/24 <-> 192.168.120.10/32 の時に IPsec を適用します。
- XR_B(拠点)は 192.168.20.0/24 <-> 192.168.10.0/24 の時に IPsec を適用します。
- PC(拠点)は 192.168.120.10/32 <-> 192.168.10.0/24 の時に IPsec を適用します。
- XR_A(センター)は、IPsec NAT-Traversal の Responder 側になるため、NAT-Traversal の Virtual Private 設定を行っています。
- XR_B(拠点)は、IPsec NAT-Traversal の Initiator 側になるため、NAT-Traversal を「使用する」を選択し、Virtual Private 設定を行っていません。
- IPsec KeepAlive は XR_B(拠点)が動作オプション 2 で使用しています。

本装置側のパラメータ

	XR_A(センター)	XR_B(拠点)
NAT Traversal	使用する	使用する
Virtual Private 設定	192.168.20.0/24	
Virtual Private 設定 2	192.168.120.10/32	
インタフェースの IP アドレス	10.10.10.1	192.168.120.1
上位ルータの IP アドレス	%ppp0	192.168.120.254
インタフェースの ID		@ipsec1

IKE/ISAKMP ポリシーのパラメータ「XR_A(センター),XR_B(拠点)」

	XR_A(センター)		XR_B(拠点)
対向拠点	XR_B(拠点)	PC(拠点)	XR_A(センター)
IKE/ISAKMP ポリシー名	XR_B	PC	XR_A
リモート IP アドレス	0.0.0.0	0.0.0.0	10.10.10.1
インタフェースの ID	@ipsec1	@vpnclient	
モード	Aggressive	Aggressive	Aggressive
暗号化アルゴリズム	AES-128	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1	SHA1
DH グループ	Group2	Group2	Group2
ライフタイム	3600(秒)	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey2	ipseckey1

IPsec ポリシーのパラメータ「XR_A(センター),XR_B(拠点)」

	XR_A(センター)		XR_B(拠点)
対向拠点	XR_B(拠点)	PC(拠点)	XR_A(センター)
使用する IKE ポリシー名	XR_B(IKE1)	PC(IKE2)	XR_A(IKE1)
本装置の LAN 側のネットワークアドレス	192.168.10.0/24	192.168.10.0/24	192.168.20.0/24
相手側の LAN 側のネットワークアドレス	vnet:%priv	vhost:%priv	192.168.10.0/24
暗号化アルゴリズム	AES-128	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1	SHA1
PFS(DH グループ)	使用する(Group2)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)	28800(秒)
DISTANCE	1	1	1

IPsec Keepalive のパラメータ

	XR_B(拠点)
対向拠点	XR_A(センター)
Policy No.	1
source address	192.168.20.1
destination address	192.168.10.1
interval(sec)	30
watch count	3
timeout/delay(sec)	60
動作 option	2
interface	ipsec6

- その他

  - 本設定例では、NAT ルータとして XR を使用しています。

7-3. 設定例

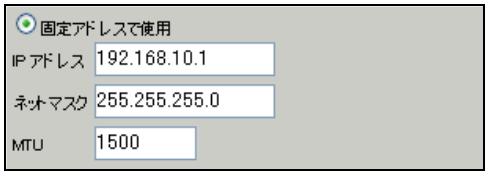
センタールータ（XR_A）

ポイント

XR_B(拠点),PC(拠点)と IPsec NAT-Traversal で接続するための設定を行います。
IPsec の鍵交換モードはアグレッシブモードを使用します。
XR_A(センター)は、IPsec NAT-Traversal の Responder 側になるため、NAT-Traversal の Virtual Private 設定を行っています。
IPsec NAT-Traversal で使用する UDP のポート番号宛先 500 番，4500 番をフィルタで許可しています。

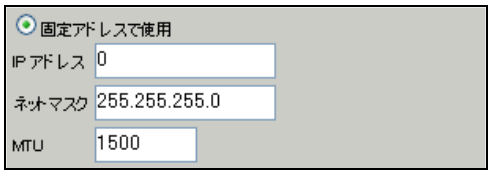
<<インタフェース設定>>

[Ethernet0 の設定]



Ethernet0 に関する設定をします。
※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

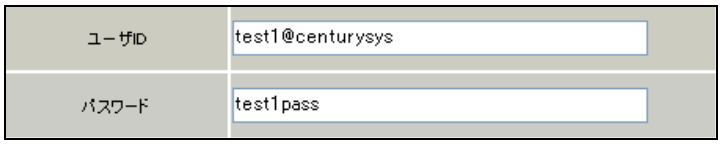
[Ethernet1 の設定]



Ethernet1 に関する設定をします。
PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

<<PPP/PPPoE 設定>>

[接続先設定１]



PPPoE 接続で使用するユーザ ID，パスワードを登録します。

［接続設定］

接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ◉Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ○RS232C
接続形態	○手動接続 ◉常時接続 ○スケジューラ接続
RS232C/BRI接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	○無効 ◉有効
ステートフルパケット インスペクション	○無効 ◉有効 ☐DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ◉有効

PPPoE 接続するインタフェース、および接続形態を選択します。
※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション (全回線共通)	☑回線接続時に前回のPPPoEセッションのPADTを強制送出 ☑非接続SessionのIPv4Packet受信時にPADTを強制送出 ☑非接続SessionのLCP-EchoRequest受信時にPADTを強制送出

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

<<フィルタ設定>>

［入力フィルタ］

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	udp				500	☐
ppp0	パケット受信時	許可	udp				4500	☐

IKE パケット，NAT-Traversal 使用時にカプセル化する UDP ポート「4500」のパケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。
この時拠点からの IKE パケットや NAT-Traversal でカプセル化されたパケットは、NAT ルータでポート変換されることを考慮し、送信元ポートを「空欄」に設定しています。

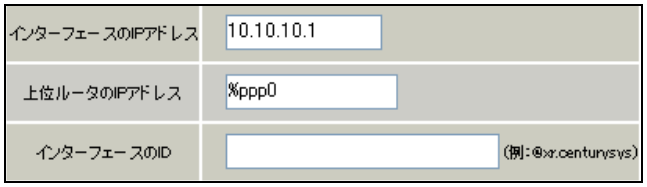
<<各種サービスの設定>>

<IPsec サーバ>

[本装置の設定]

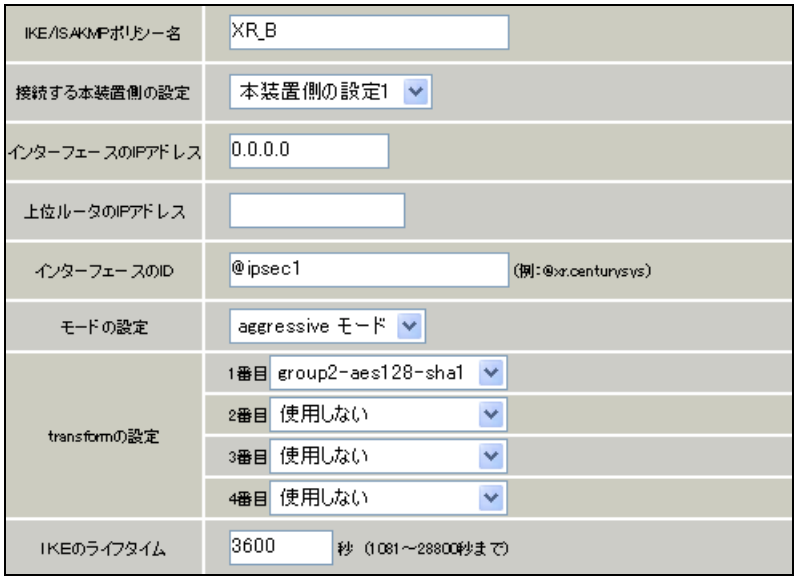
NAT Traversal を利用するため、「使用する」を選択します。
Virtual Private 設定では、NAT-Traversal を使用しているルータ配下の LAN または NAT-Traversal を使用している機器のアドレスを設定します。
この例では、XR_B2(拠点)の配下のルータ XR_B の LAN 側「192.168.20.0/24」および VPN Client の IP アドレスを設定しています。

[本装置側の設定 1]

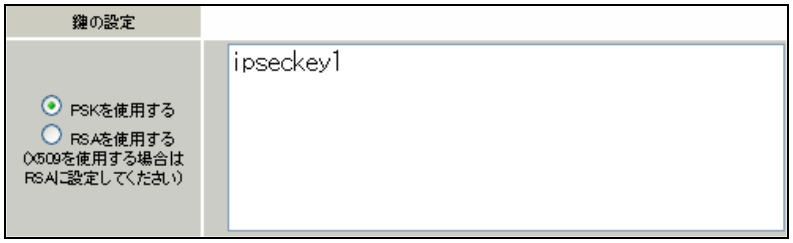


XR_A(センター)の WAN 側インタフェースの IP アドレス,および上位ルータの IP アドレスを設定します。
PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

[IKE/ISAKMP の設定 1]



XR_B(拠点)に対する IKE/ISAKMP ポリシーを設定します。



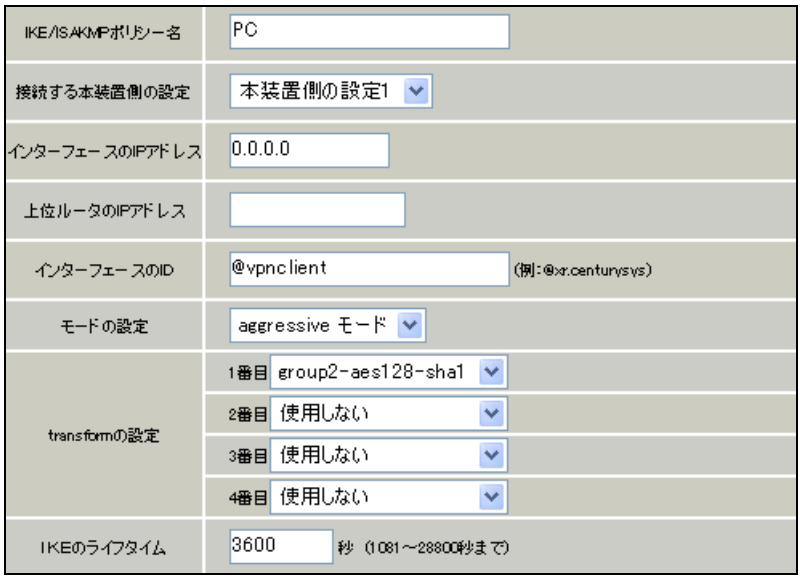
事前共有鍵(PSK)として「ipseckey1」を設定しています。

[IPsec ポリシーの設定 1]

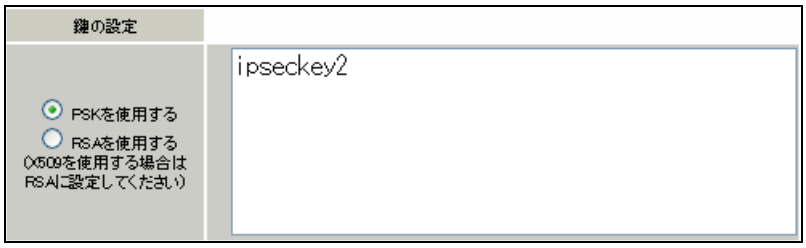
XR_B(拠点)の IP アドレスが不定のため、「Responder として使用する」を選択します。

XR_B(拠点)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。
NAT-Traversal を使用しているルータ配下のネットワークを指定する場合は「vnet:%priv」を指定します。

[IKE/ISAKMP の設定 2]



PC(拠点)に対する IKE/ISAKMP ポリシーを設定します。



事前共有鍵(PSK)として「ipseckey2」を設定しています。

[IPsec ポリシーの設定 2]

PC(拠点)の IP アドレスが不定のため、「Responder として使用する」を選択します。

PC(拠点)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。
NAT-Traversal を使用している機器を指定する場合は「vhost:%priv」を指定します。

【IPsec サーバ】

IPsec サーバ機能を起動します。

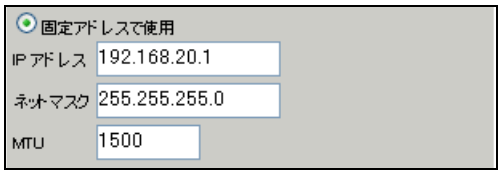
拠点ルータ（XR_B）

ポイント

XR_A(センター)と IPsec NAT-Traversal で接続するための設定を行います。
IPsec の鍵交換モードはアグレッシブモードを使用します。
XR_B(拠点)は、IPsec NAT-Traversal の Initiator 側になるため、NAT-Traversal を「使用する」を選択し、Virtual Private 設定を行っていません。

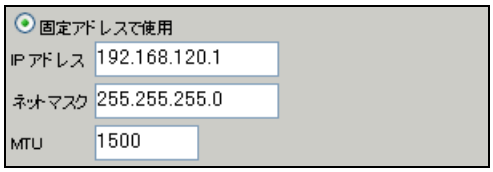
<<インタフェース設定>>

[Ethernet0 の設定]

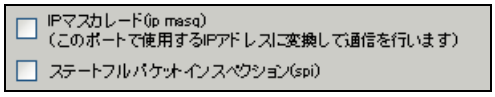


Ethernet0 に関する設定をします。
※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

[Ethernet1 の設定]

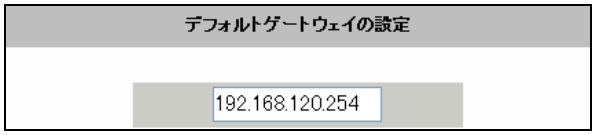


Ethernet1 の IP アドレスの設定をします。



この例では、NAT Traversal を使用するルータの WAN 側では IP マスカレードおよびステートフルパケットインスペクション(spi)は使用していません。

[その他の設定]



XR_B の上位ルータである XR_B2 をデフォルトゲートウェイとして指定しています。

<<各種サービスの設定>>

<IPsec サーバ>

[本装置の設定]

NAT Traversal	◉ 使用する ○ 使用しない

NAT Traversal を利用するため、「使用する」を選択します。

[本装置側の設定 1]

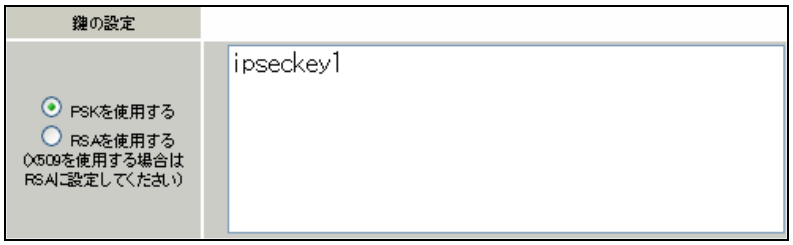
インターフェースのIPアドレス	192.168.120.1
上位ルータのIPアドレス	192.168.120.254
インターフェースのID	@ipsec1 (例:@xr.centurysys)

WAN 側インタフェースの IP アドレス，および上位ルータの IP アドレスを設定します。
XR_B は NAT ルータ配下にあるため、「インタフェースの ID」を設定しています。

[IKE/ISAKMP の設定 1]

IKE/ISAKMPポリシー名	XR_A
接続する本装置側の設定	本装置側の設定1
インターフェースのIPアドレス	10.10.10.1
上位ルータのIPアドレス	
インターフェースのID	(例:@xr.centurysys)
モードの設定	aggressive モード
transformの設定	1番目 group2-aes128-sha1
	2番目 使用しない
	3番目 使用しない
	4番目 使用しない
IKEのライフタイム	3600 秒 (1081～28800秒まで)

XR_A(センター)に対する ISAKMP ポリシーの設定を行います。



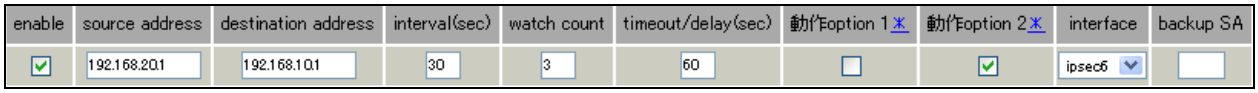
事前共有鍵(PSK)として「ipseckey1」を設定します。

[IPsec ポリシーの設定 1]

XR_A(センター)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

XR_A(センター)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

[IPsec Keep-Alive 設定]



XR_A(センター)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

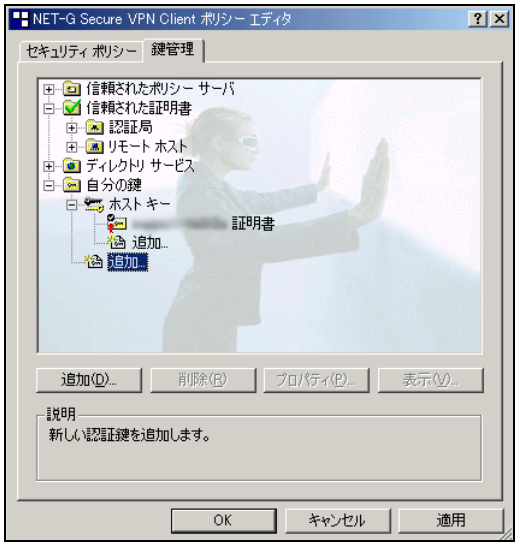
IPsec サーバ機能を起動します。

PC（拠点）

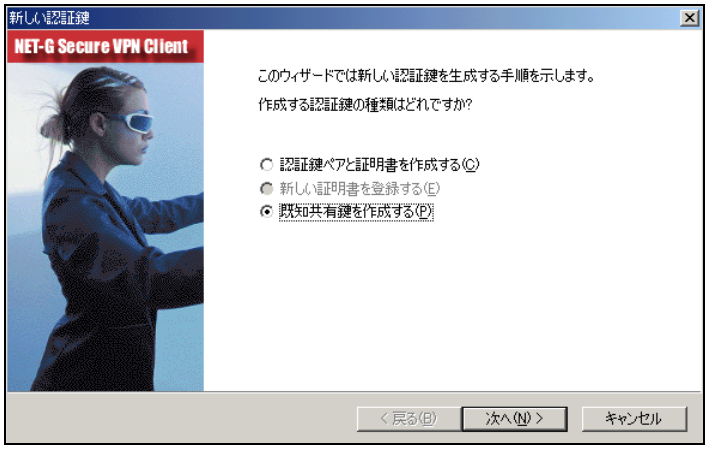
ポイント

PC(拠点)は「FutureNet VPN Client/NET-G」をインストールした PC からの IPsec NAT-Traversal 接続になります。

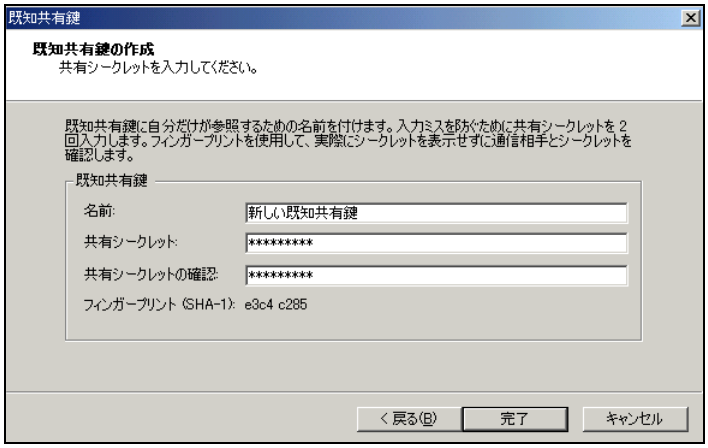
<<既知共有鍵(Pre shared Key)の設定>>



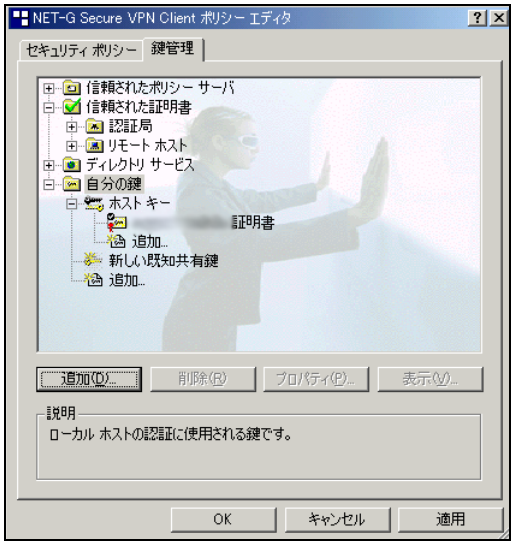
「鍵管理」タブをクリックし、「自分の鍵」を選択し、「追加」ボタンをクリックします。



「新しい認証鍵」ウィンドウが開きますので、「既知共有鍵を作成する」を選択し、「次へ」ボタンをクリックして下さい。

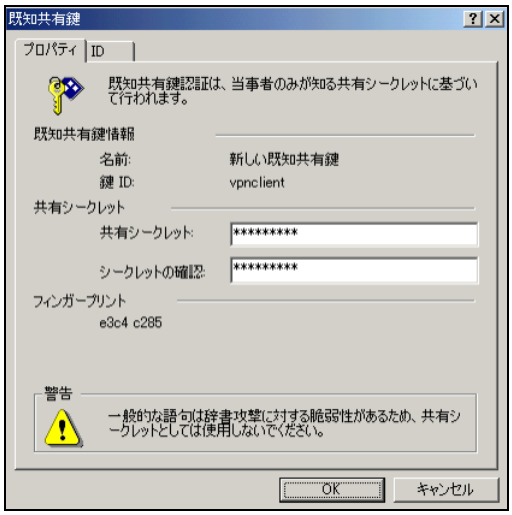


「既知共有鍵の作成」画面が開きます。ここで既知共有鍵を作成します。「名前」には任意の設定名を入力します。「共有シークレット」「共有シークレットの確認」項目には既知共有鍵を入力し、「完了」ボタンをクリックします。
この例では共有シークレットとして「ipseckey2」を設定しています。

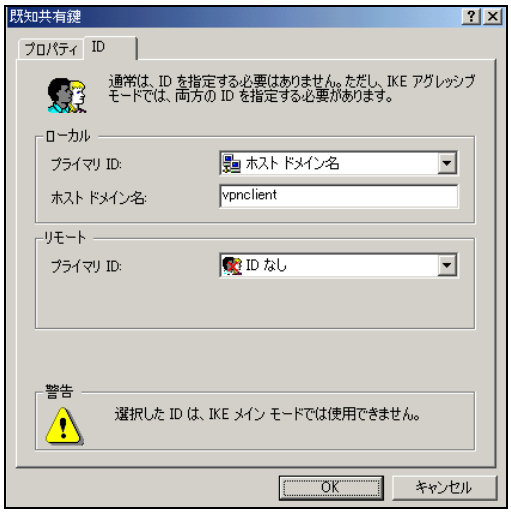


「鍵管理」画面に戻ります。既知共有鍵が登録されていることを確認したら、必ず「適用」ボタンをクリックして下さい。「適用」ボタンをクリックしないと適切に設定されない場合があります。

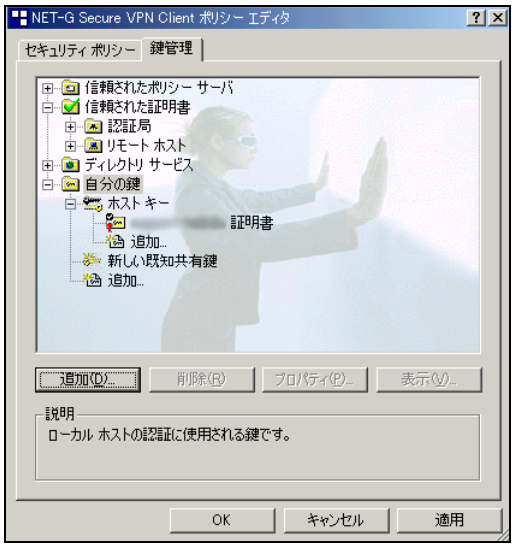
<<ID の設定>>



「鍵管理」画面で、登録した既知共有鍵を選択して「プロパティ」をクリックします。「既知共有鍵」画面が開きますので、「ID」タブをクリックします(この画面では既知共有鍵を変更できます)。



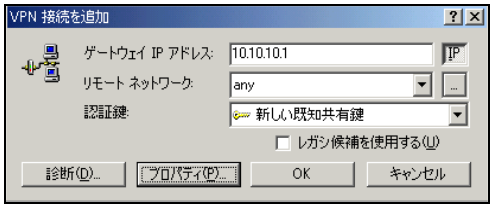
「ローカル」側項目について、プライマリ ID は「ホストドメイン名」を選択し、ホストドメイン名に ID を入力します。ここには XR シリーズの IPsec サーバ「IKE/ISAKMP の設定」における「インタフェース ID」と同じ ID を設定します。
※ただしこの時、ホストドメイン名には”@”をつけないで設定して下さい。



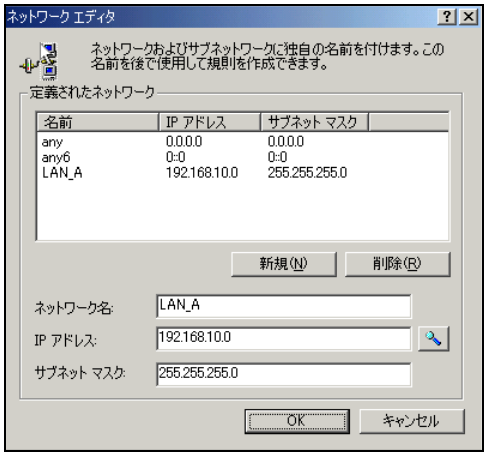
「OK」ボタンをクリックすると、「鍵管理」画面に戻ります。ここまでの設定が終わったら、必ず「適用」ボタンをクリックして下さい。「適用」ボタンをクリックしないと適切に設定されない場合があります。

<<セキュリティポリシーの設定>>

ポリシーエディタの「セキュリティポリシー」タブをクリックします。「VPN 接続」を選択し「追加」をクリックします。

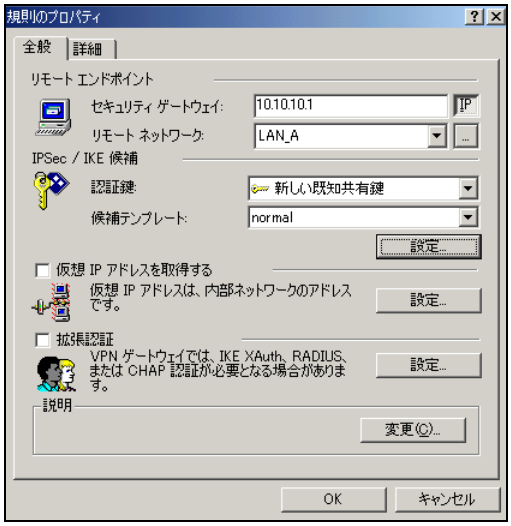


「VPN 接続を追加」画面が開きます。「ゲートウェイ IP アドレス」で右端の”IP”をクリックし、XR_A(センター)の WAN 側 IP アドレスを設定します。
「認証鍵」は、既知共有鍵の設定で登録した既知共有鍵の設定名を選択します。
「リモートネットワーク」については右端にある”・・・”をクリックして下さい。



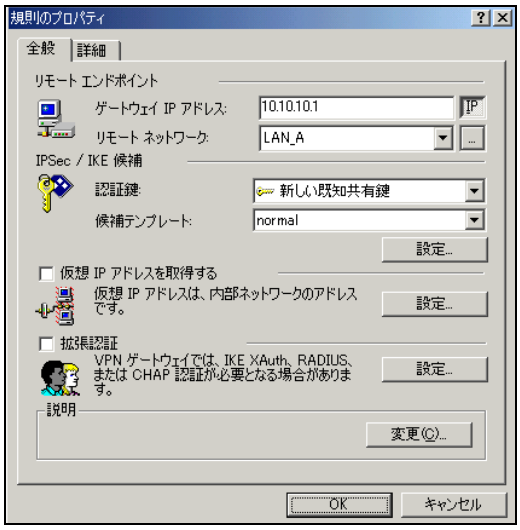
「ネットワークエディタ」画面が開きます。
「ネットワーク名」は任意の名前を設定することができます。
「IP アドレス」「サブネットマスク」は XR に接続している LAN について設定し（ここでは LAN_A[センター側のネットワーク]の値を設定しています)、「OK」をクリックします。

リモートネットワーク設定後、「VPN 接続を追加」画面が開きますので、続いてプロパティをクリックします。



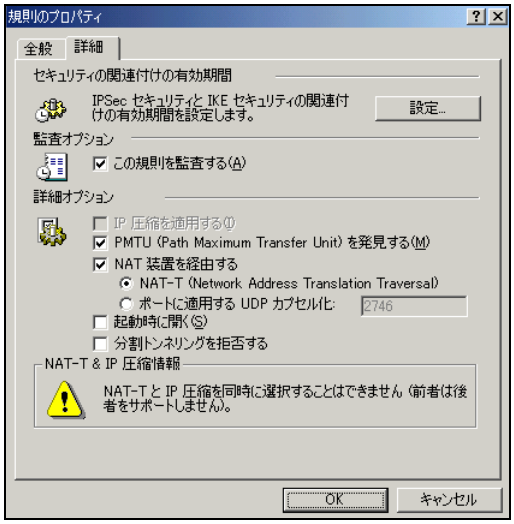
「規則のプロパティ」画面が開きます。ここで IPsec/IKE 候補の
設定ボタンをクリックします。

「パラメータ候補画面」が開きます。ここで暗号化方式などを設定します。IKE モードは「aggressive mode」を設定します。また「選択した値のみを候補に加える」にチェックをいれます。

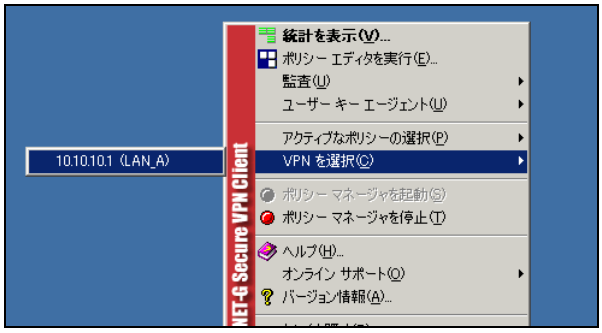


「OK」ボタンをクリックして「規則のプロパティ」画面に戻ります。

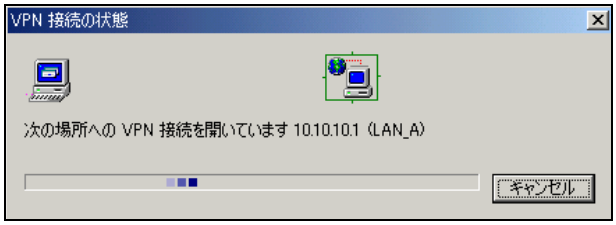
「詳細タブ」をクリックします。ここで詳細オプションにある「NAT 装置を経由する」のチェックボックスを有効にし、「NAT-T(Network Address Translation Traversal)」を選択します。



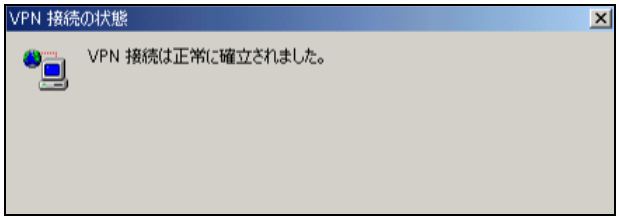
これで設定は完了です。
続いて IPsec 接続を行います。



タスクトレーの中にある FutureNet Net-G VPNclient のアイコンを右クリックします。そして「VPN を選択」の指定し、作成した IPsec ポリシーを選択します。



選択後、IKE のネゴシエーションを行う画面が表示されます。



IPsec が正常に確立した場合、「VPN 接続は正常に確立しました」という画面が表示されます。

これで IPsec 接続は完了です。

NAT ルータ

ポイント

この設定例では、NAT ルータの設定例は記載していません。

NAT ルータの主な必要な要件は以下のとおりです。

・インターネット接続ができていること

・IP マスカレードが有効になっていること

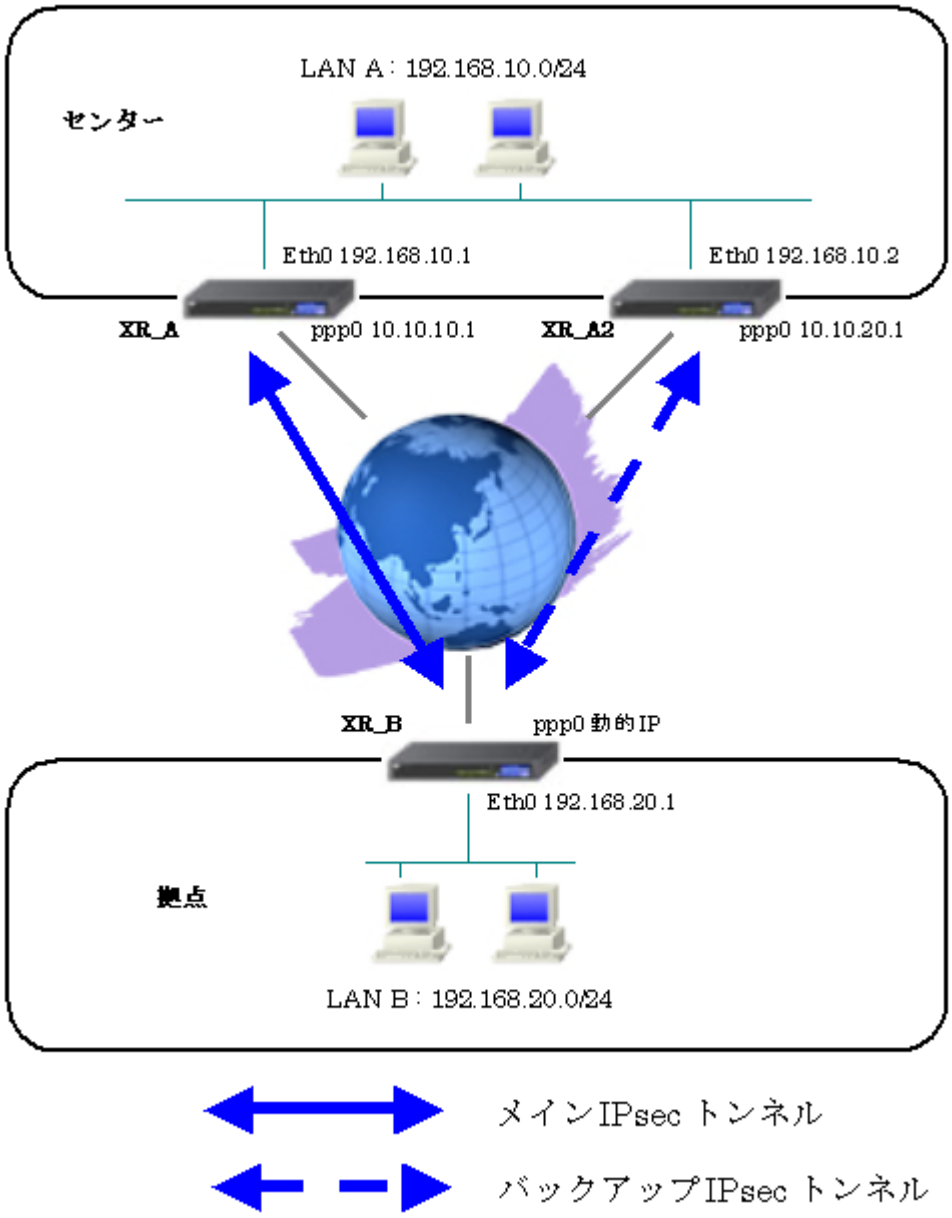
・フィルタ設定で IPsec NAT-Traversal で使用する UDP ポートが許可されていること

8. IPsec backupSA 機能（IPsec 冗長化）利用例

センター側回線やセンター側の障害に備えて、IPsec backupSA 機能を搭載しています。IPsec のメインの VPN 回線に障害が発生した場合、バックアップ側のセキュリティゲートウェイに対して即時に VPN を張ることができます。

この例では、センターメインルータの WAN 回線に障害が発生した場合に、拠点ルータの IPsec backupSA 機能によりバックアップ経路を確立するための設定例です。

8-1. 構成例



8-2. 要件

- インタフェースおよび PPPoE

  - インターネットには PPPoE で接続します。
  - PPPoE 接続は、自動再接続するように設定しています。
  - WAN 側インタフェースの 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は「有効」にしています。

主なインタフェースおよび PPPoE のパラメータ

	XR_A(センター1)	XR_A2(センター2)	XR_B(拠点)
LAN 側インタフェース	Ether0	Ether0	Ether0
LAN 側 IP アドレス	192.168.10.1	192.168.10.2	192.168.20.1
WAN 側インタフェース	Ether1[ppp0]	Ether1[ppp0]	Ether1[ppp0]
WAN 側 IP アドレス	10.10.10.1	10.10.20.1	動的 IP
PPPoE ユーザ名	test1@centurysys	test2@centurysys	test3@centurysys
PPPoE パスワード	test1pass	test2pass	test3pass
接続回線	PPPoE 接続	PPPoE 接続	PPPoE 接続

- IPsec

  - 鍵交換モードはアグレッシブモードを使用します。
  - XR_A(センター1)は 192.168.10.0/24 <-> 192.168.20.0/24 の時に IPsec を適用します。
  - XR_A2(センター2)は 192.168.10.0/24 <-> 192.168.20.0/24 の時に IPsec を適用します。
  - XR_B(拠点)は 192.168.20.0/24 <-> 192.168.10.0/24 の時に IPsec を適用します。
  - IPsec KeepAlive は XR_A(センター1), XR_A2(センター2)が動作オプション 1 で、XR_B(拠点)が動作オプション 2 で使用します。
  - XR_B(拠点)は IPsec KeepAlive backup SA 機能を使用します。
    この時 XR_A(センター1)に対する IPsec トンネルのディスタンス値を「1」, XR_A2(センター2)に対する IPsec トンネルのディスタンス値を「2」に設定しています。

本装置側のパラメータ

	XR_A(センター1)	XR_A2(センター2)	XR_B(拠点)
インタフェースの IP アドレス	10.10.10.1	10.10.20.1	%ppp0
上位ルータの IP アドレス	%ppp0	%ppp0	
インタフェースの ID			@ipsec1

IKE/ISAKMP ポリシーのパラメータ(1) 「XR_A(センター), XR_A2(センター2)」

	XR_A(センター1)	XR_A2(センター2)
対向拠点	XR_B(拠点)	XR_B(拠点)
IKE/ISAKMP ポリシー名	XR_B	XR_B
リモート IP アドレス	0.0.0.0	0.0.0.0
モード	Aggressive	Aggressive
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
DH グループ	Group2	Group2
ライフタイム	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey2

IPsec ポリシーのパラメータ(1) 「XR_A(センター), XR_A2(センター2)」

	XR_A(センター1)	XR_A2(センター2)
対向拠点	XR_B(拠点)	XR_B(拠点)
使用する IKE ポリシー名	XR_B(IKE1)	XR_B(IKE1)
本装置の LAN 側のネットワークアドレス	192.168.10.0/24	192.168.10.0/24
相手側の LAN 側のネットワークアドレス	192.168.20.0/24	192.168.20.0/24
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
PFS(DH グループ)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)
DISTANCE	1	1

IKE/ISAKMP ポリシーのパラメータ(2) 「XR_B(拠点)」

	XR_B(拠点)	
対向拠点	XR_A(センター1)	XR_A2(センター2)
IKE/ISAKMP ポリシー名	XR_A	XR_A2
リモート IP アドレス	10.10.10.1	10.10.20.1
モード	Aggressive	Aggressive
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
DH グループ	Group2	Group2
ライフタイム	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey2

IPsec ポリシーのパラメータ(2) 「XR_B(拠点)」

	XR_B(拠点)	
対向拠点	XR_A(センター1)	XR_A2(センター2)
使用する IKE ポリシー名	XR_A(IKE1)	XR_A2(IKE2)
本装置の LAN 側のネットワークアドレス	192.168.20.0/24	192.168.20.0/24
相手側の LAN 側のネットワークアドレス	192.168.10.0/24	192.168.10.0/24
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
PFS(DH グループ)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)
DISTANCE	1	2

IPsec Keepalive のパラメータ (1) 「XR_A(センター1), XR_A2(センター2)」

	XR_A(センター1)	XR_A2(センター2)
対向拠点	XR_B(拠点)	XR_B(拠点)
Policy No.	1	1
source address	192.168.10.1	192.168.10.2
destination address	192.168.20.1	192.168.20.1
interval(sec)	30	30
watch count	3	3
timeout/delay(sec)	60	60
動作 option	1	1
interface	ipsec0	ipsec0

IPsec Keepalive のパラメータ (2) 「XR_B(拠点)」

	XR_B(拠点)	
対向拠点	XR_A(センター1)	XR_A2(センター2)
Policy No.	1	2
source address	192.168.20.1	192.168.20.1
destination address	192.168.10.1	192.168.10.2
interval(sec)	45	60
watch count	3	3
timeout/delay(sec)	60	60
動作 option	2	2
interface	ipsec0	ipsec0
backup SA	2	

- その他

  - XR_A(センター1), XR_A2(センター2)では IPsec 接続していないときに、拠点方向へのルートを IPsec 接続中の XR へ切り替えるためのスタティックルートを設定しています。

8-3. 設定例

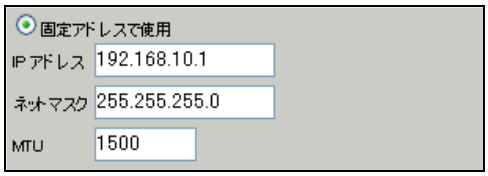
センタールータ 1（XR_A）

ポイント

拠点とメインで IPsec 接続するルータになります。
拠点が動的 IP のため、アグレッシブモードを使用します。
WAN 側の回線断等で IPsec KeepAlive による障害が検出された場合、XR_A2(センター2)へのルーティングを有効にします。

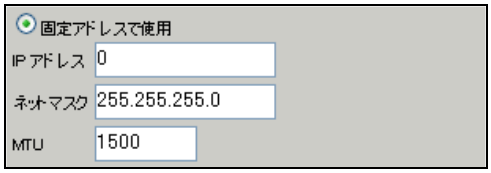
<<インタフェース設定>>

[Ethernet0 の設定]



Ethernet0 に関する設定をします。
※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

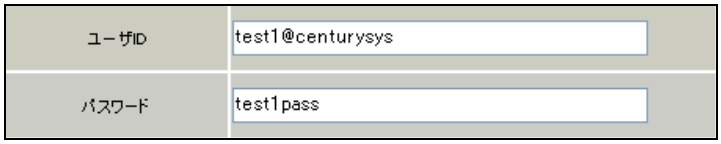
[Ethernet1 の設定]



Ethernet1 に関する設定をします。
PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

<<PPP/PPPoE 設定>>

[接続先設定 1]



PPPoE 接続で使用するユーザ ID，パスワードを登録します。

[接続設定]

接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ◉Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ○RS232C
接続形態	○手動接続 ◉常時接続 ○スケジューラ接続
RS232C/BRI接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	○無効 ◉有効
ステートフルパケット インスペクション	○無効 ◉有効 ☐DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ◉有効

PPPoE 接続するインタフェース、および接続形態を選択します。
※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション (全回線共通)	☑回線接続時に前回のPPPoEセッションのPADTを強制送出 ☑非接続SessionのIPv4Packet受信時にPADTを強制送出 ☑非接続SessionのLCP-EchoRequest受信時にPADTを強制送出

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

<<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	udp		500		500	☐
ppp0	パケット受信時	許可	esp					☐

IKE パケット，ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

[転送フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ipsec0	パケット受信時	破棄	icmp	192.168.20.1		192.168.10.2		

メインの IPsec SA で接続中に、バックアップの IPsec SA に対する IPsec KeepAlive 要求がセンターメインルータ(XR_A)からセンター側 LAN を経由してセンターバックアップルータ(XR_A2)へ届いてしまいます。
このフィルタによりそれを防止します。

<<各種サービスの設定>>

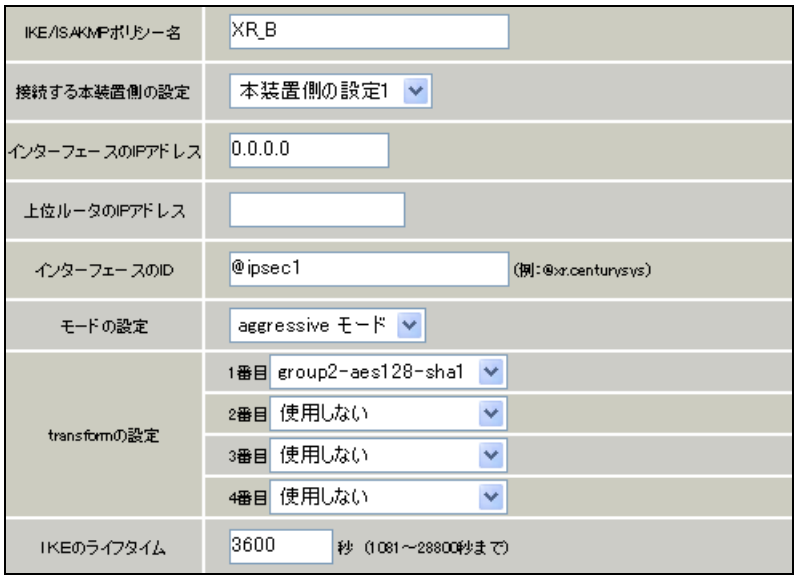
<IPsec サーバ>

[本装置側の設定 1]

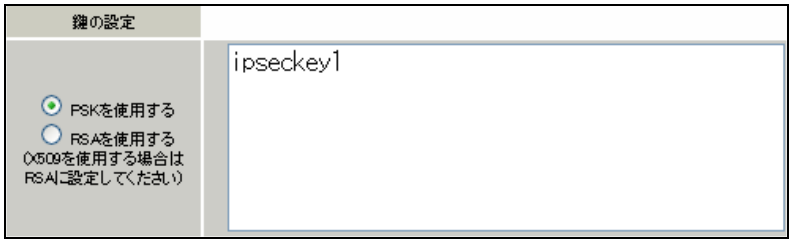
インターフェースのIPアドレス	10.10.10.1
上位ルータのIPアドレス	%ppp0
インターフェースのID	(例:@xr.centurysys)

XR_A(センター1)の WAN 側インタフェースの IP アドレス,および上位ルータの IP アドレスを設定します。
PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

[IKE/ISAKMP の設定 1]



XR_B(拠点)に対する IKE/ISAKMP ポリシーを設定します。



事前共有鍵(PSK)として「ipseckey1」を設定しています。

[IPsec ポリシーの設定 1]

XR_B(拠点)の IP アドレスが不定のため、「Responder として使用する」を選択します。

使用するIKEポリシー名の選択	XR_B (IKE1)
本装置側のLAN側のネットワークアドレス	192.168.10.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.20.0/24 (例:192.168.0.0/24)
PH2のTransFormの選択	aes128-sha1
PFS	使用する 使用しない
DH Groupの選択(PFS使用時に有効)	group2
SAのライフタイム	28800 秒 (1081～86400秒まで)
DISTANCE	1 (1～255まで)

XR_B(拠点)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。

[IPsec Keep-Alive 設定]

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1 *	動作option 2 *	interface	backup SA
1	☑	192.168.10.1	192.168.20.1	30	3	60	☑	☐	ipsec0	

XR_B(拠点)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

IPsecサーバ	○停止 ◉起動

IPsec サーバ機能を起動します。

<<スタティックルート設定>>

No.	アドレス	ネットマスク	インターフェース/ゲートウェイ		ディスタンス <1-255>
1	192.168.20.0	255.255.255.0		192.168.10.2	10

IPsec 接続していないときに、拠点方向へのルートを IPsec 接続中の XR へフローティングさせるために、スタティックルートの設定を行います。
この例では、IPsec 接続しているときは、IPsec ルートのディスタンス値(=1)の方がスタティックルートのディスタンス値(=10)より小さいため、IPsec ルートが有効になっているときは、このスタティックルートは無効の状態になっています。

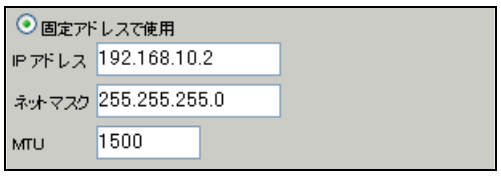
センタールータ 2（XR_A2）

ポイント

拠点とバックアップで IPsec 接続するルータになります。
拠点が動的 IP のため、アグレッシブモードを使用します。

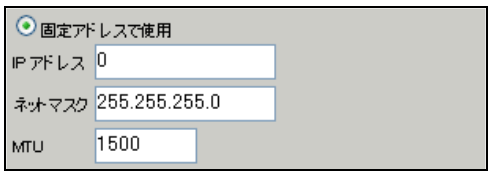
<<インタフェース設定>>

[Ethernet0 の設定]



Ethernet0 に関する設定をします。
※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

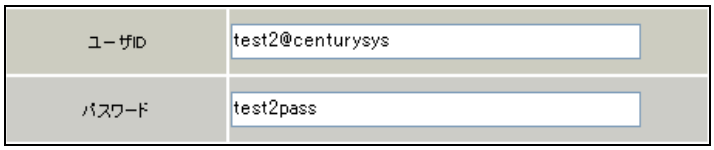
[Ethernet1 の設定]



Ethernet1 に関する設定をします。
PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

<<PPP/PPPoE 設定>>

[接続先設定 1]



PPPoE 接続で使用するユーザ ID，パスワードを登録します。

[接続設定]

接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ◉Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ○RS232C
接続形態	○手動接続 ◉常時接続 ○スケジューラ接続
RS232C/BRI接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	○無効 ◉有効
ステートフルパケット インスペクション	○無効 ◉有効 ☐DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ◉有効

PPPoE 接続するインタフェース、および接続形態を選択します。
※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション (全回線共通)	☑回線接続時に前回のPPPoEセッションのPADTを強制送出 ☑非接続SessionのIPv4Packet受信時にPADTを強制送出 ☑非接続SessionのLCP-EchoRequest受信時にPADTを強制送出

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

<<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	udp		500		500	☐
ppp0	パケット受信時	許可	esp					☐

IKE パケット，ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

[転送フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ipsec0	パケット受信時	破棄	icmp	192.168.20.1		192.168.10.1		

バックアップの IPsec SA で接続中に、メインの IPsec SA に対する IPsec KeepAlive 要求がセンターバックアップルータ(XR_A2)からセンター側 LAN を経由してセンターメインルータ(XR_A)へ届いてしまいます。
これによりメインの IPsec SA が復旧したと誤認してしまうため、IPsec 接続が不安定な状態になります。
このフィルタにより IPsec 接続が不安定になるのを防止します。

<<各種サービスの設定>>

<IPsec サーバ>

[本装置側の設定 1]

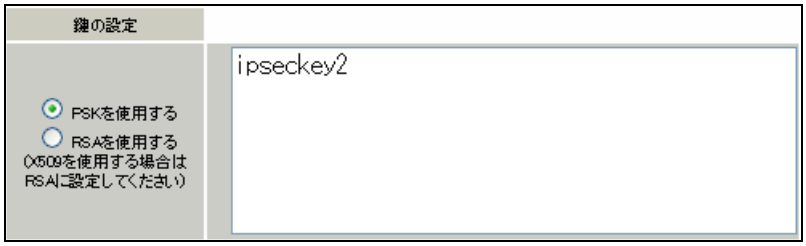
インターフェースのIPアドレス	10.10.20.1
上位ルータのIPアドレス	%ppp0
インターフェースのID	(例:@xr.centurysys)

XR_A2(センター2)の WAN 側インタフェースの IP アドレス，および上位ルータの IP アドレスを設定します。
PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

[IKE/ISAKMP の設定 1]

IKE/ISAKMP ポリシーのパラメータは以下のとおりです。

XR_B(拠点)に対する IKE/ISAKMP ポリシーを設定します。



事前共有鍵(PSK)として「ipseckey2」を設定しています。

[IPsec ポリシーの設定 1]

XR_B(拠点)の IP アドレスが不定のため、「Responder として使用する」を選択します。

使用するIKEポリシー名の選択	XR_B (IKE1)
本装置側のLAN側のネットワークアドレス	192.168.10.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.20.0/24 (例:192.168.0.0/24)
PH2のTransFormの選択	aes128-sha1
PFS	使用する 使用しない
DH Groupの選択(PFS使用時に有効)	group2
SAのライフタイム	28800 秒 (1081～86400秒まで)
DISTANCE	1 (1～255まで)

XR_B(拠点)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。

[IPsec Keep-Alive 設定]

enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1	動作option 2	interface	backup SA
☑	192.168.10.2	192.168.20.1	30	3	60	☑	☐	ipsec0	

XR_B(拠点)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

IPsecサーバ	○停止 ◉起動

IPsec サーバ機能を起動します。

<<スタティックルート設定>>

アドレス	ネットマスク	インターフェース/ゲートウェイ		ディスタンス <1-255>
192.168.20.0	255.255.255.0		192.168.10.1	10

IPsec 接続していないときに、拠点方向へのルートを IPsec 接続中の XR へフローティングさせるために、スタティックルートの設定を行います。
この例では、IPsec 接続しているときは、IPsec ルートのディスタンス値(=1)の方がスタティックルートのディスタンス値(=10)より小さいため、IPsec ルートが有効になっているときは、このスタティックルートは無効の状態になっています。

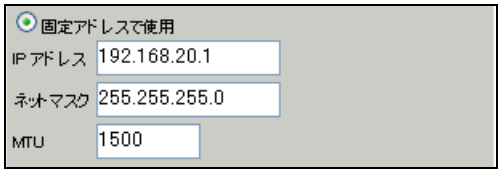
拠点ルータ（XR_B）

ポイント

正常時は XR_A(センター1)と IPsec 接続を行い、XR_A(センター1)の WAN 側の回線断等で IPsec KeepAlive による障害が検出された場合、XR_A2(センター2)と IPsec 接続を行います。
WAN 側 IP アドレスが動的 IP のため、アグレッシブモードを使用します。

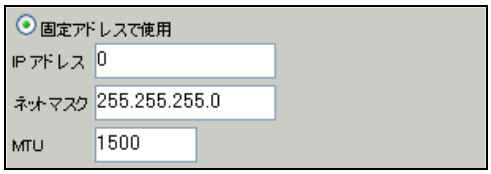
<<インタフェース設定>>

[Ethernet0 の設定]



Ethernet0 に関する設定をします。
※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

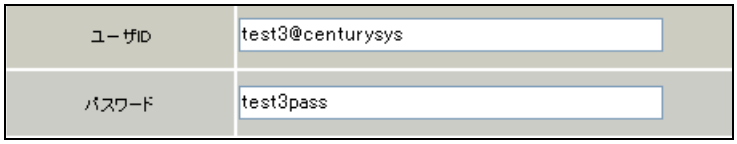
[Ethernet1 の設定]



Ethernet1 に関する設定をします。
PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

<<PPP/PPPoE 設定>>

[接続先設定 1]



PPPoE 接続で使用するユーザ ID，パスワードを登録します。

[接続設定]

接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ◉Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ○RS232C
接続形態	○手動接続 ◉常時接続 ○スケジューラ接続
RS232C/BRI接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	○無効 ◉有効
ステートフルパケット インスペクション	○無効 ◉有効 ☐DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ◉有効

PPPoE 接続するインタフェース、および接続形態を選択します。
※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション (全回線共通)	☑回線接続時に前回のPPPoEセッションのPADTを強制送出 ☑非接続SessionのIPv4Packet受信時にPADTを強制送出 ☑非接続SessionのLCP-EchoRequest受信時にPADTを強制送出

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

<<フィルタ設定>>

[入力フィルタ]

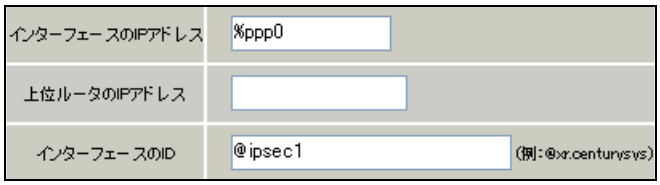
インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	udp		500		500	☐
ppp0	パケット受信時	許可	esp					☐

IKE パケット，ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

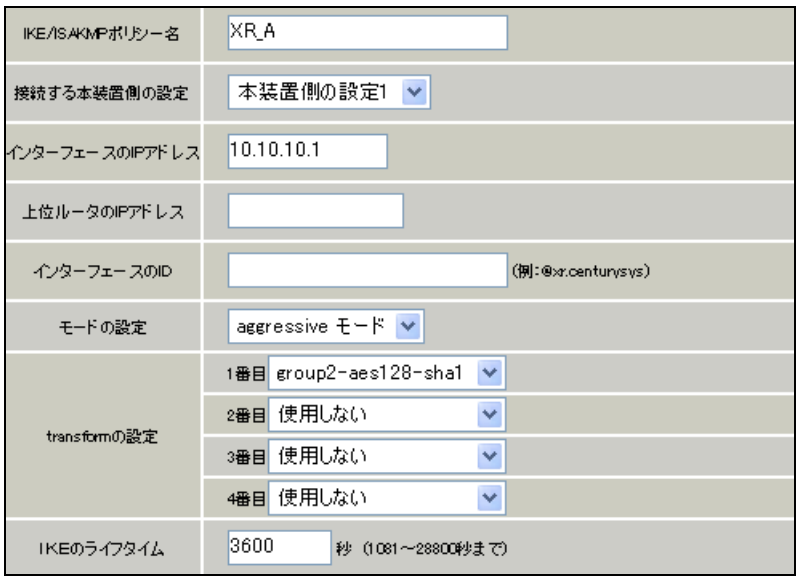
<IPsec サーバ>

[本装置側の設定 1]

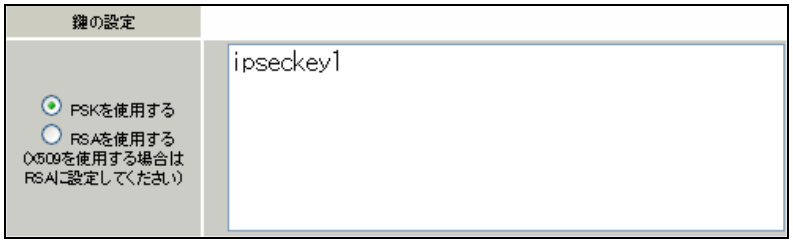


PPPoE 接続で WAN 側(ppp0)インタフェースの IP アドレスが不定のため「%ppp0」, インタフェースの ID として「@ipsec1」を設定します。

[IKE/ISAKMP の設定 1]



XR_A(センター1)に対する IKE/ISAKMP ポリシーを設定します。



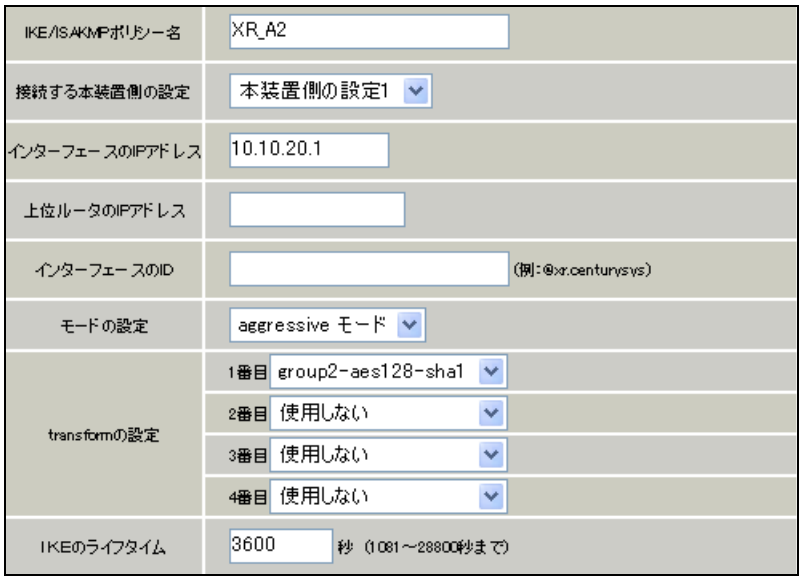
事前共有鍵(PSK)として「ipseckey1」を設定しています。

[IPsec ポリシーの設定 1]

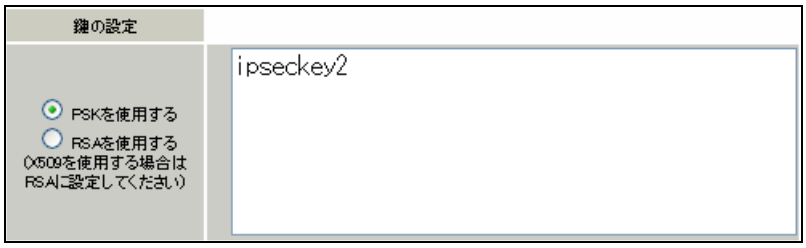
XR_A(センター1)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

XR_A(センター1)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

[IKE/ISAKMP の設定 2]



XR_A2(センター2)に対する IKE/ISAKMP ポリシーを設定します。



事前共有鍵(PSK)として「ipseckey2」を設定しています。

[IPsec ポリシーの設定 2]

XR_B(拠点)は Initiator として動作しますが、backup SA 用の IPsec ポリシーの場合「Responder として使用する」を選択します。

XR_A2(センター2)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。

[IPsec Keep-Alive 設定]

enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1 *	動作option 2 *	interface	backup SA
☑	192.168.201	192.168.101	45	3	60	☐	☑	ipsec0	2
☑	192.168.201	192.168.102	60	3	60	☐	☑	ipsec0	

XR_A(センター), XR_A2(センター2)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。
XR_A(センター), XR_A2(センター2)に IPsec KeepAlive を設定している理由は、拠点が WAN 側動的 IP アドレスを用いた構成で、センター側からの通信があるようなケースでは SA の不一致が起こりうるため、メイン側, バックアップ側でそれぞれ IPsec KeepAlive を設定しています。(推奨)
※メイン SA とバックアップ SA、または拠点側とセンター側の interval が同じ値の場合、KeepAlive の周期が同期してしまい、障害時の IPsec 切り替え直後に、切り替えた先でもすぐに障害を検出して、IPsec 通信が不安定になることがあります。これを防ぐために、拠点側の XR 同士の interval は、それぞれ異なる値を設定することを推奨します。さらにそれぞれの値はセンター側とも異なる値を設定して下さい。

【IPsec サーバ】

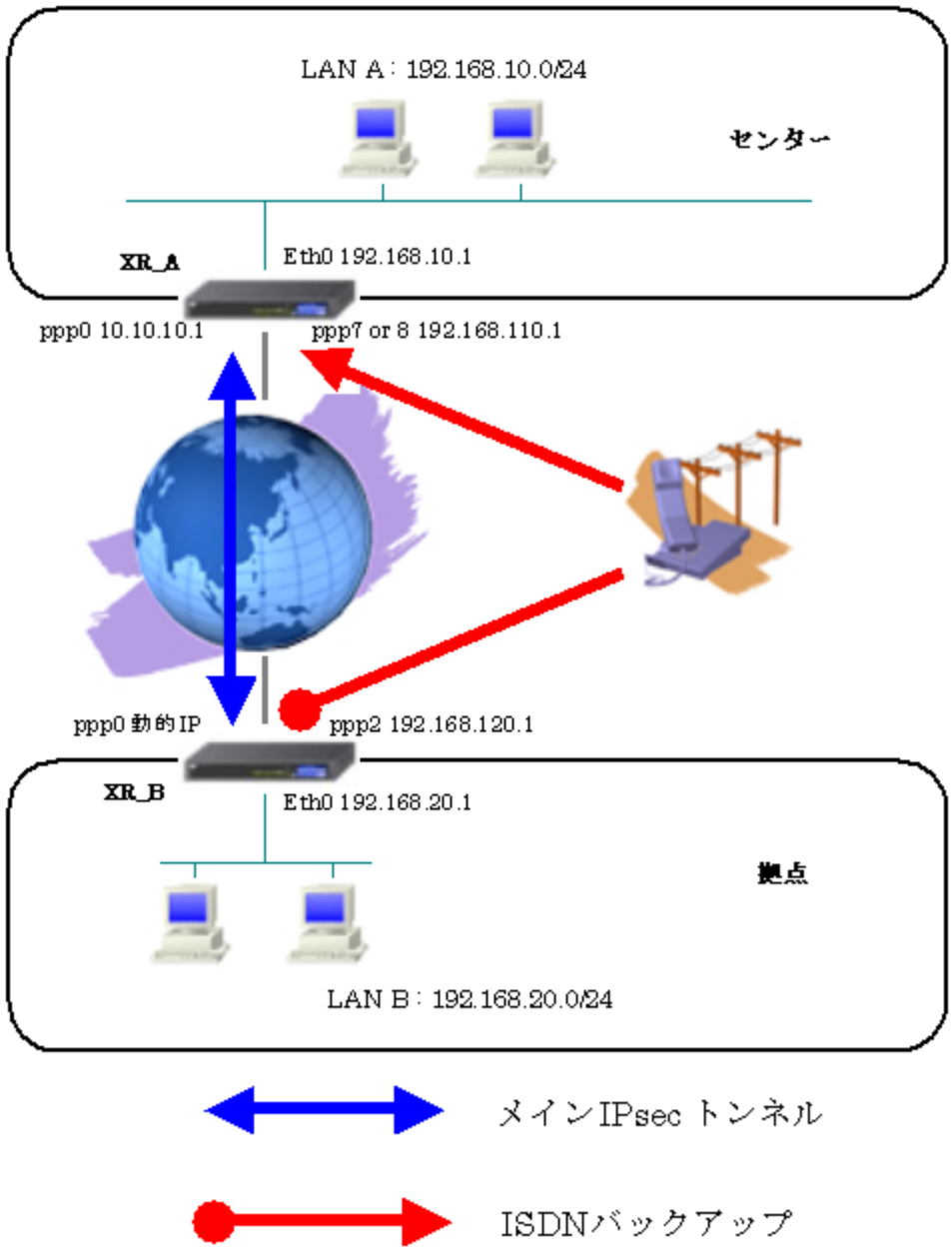
IPsecサーバ	○停止 ◉起動

IPsec サーバ機能を起動します。

9. ISDN を利用した回線バックアップ例その１（メイン回線 IPsec）

この例は、PPPoE で IPsec 接続しているメイン回線で障害が発生したときに、拠点側からの ISDN によるバックアップを実現する設定例です。

9-1. 構成例



9-2. 要件

➢ インタフェースおよび PPP/PPPoE

- インターネットに PPPoE で接続します。
- PPPoE 接続は、自動再接続するように設定しています。
- WAN 側インタフェースの 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は「有効」にしています。
- XR_B(拠点)はマルチ回線で ISDN オンデマンド接続をします。
- XR_A(センター)ではアクセスサーバ機能を使用し、XR_B(拠点)からのダイアルアップ接続を受け付けます。

主なインタフェースおよび PPP/PPPoE のパラメータ

	XR_A(センター)	XR_B(拠点)
LAN 側インタフェース	Ether0	Ether0
LAN 側 IP アドレス	192.168.10.1	192.168.20.1
WAN 側インタフェース	Ether1[ppp0]	Ether1[ppp0]
WAN 側 IP アドレス	10.10.10.1	動的 IP
PPPoE ユーザ名	test1@centurysys	test2@centurysys
PPPoE パスワード	test1pass	test2pass
WAN 側接続回線	PPPoE 接続	PPPoE 接続
ISDN 番号	XR_A-123	XR_B-123
ISDN ユーザ名	-	isdntest
ISDN パスワード	-	isdnpass
ISDN 側 IP アドレス	192.168.110.1	192.168.120.1

- IPsec

  - 鍵交換モードはアグレッシブモードを使用しています。
  - XR_A(センター)は 192.168.10.0/24 <-> 192.168.20.0/24 の時に IPsec を適用します。
  - XR_B(拠点)は 192.168.20.0/24 <-> 192.168.10.0/24 の時に IPsec を適用します。
  - IPsec KeepAlive は XR_A(センター)が動作オプション 1 で、XR_B(拠点)が動作オプション 2 で使用しています。

本装置側のパラメータ

	XR_A(センター)	XR_B(拠点)
インタフェースの IP アドレス	10.10.10.1	%ppp0
上位ルータの IP アドレス	%ppp0	
インタフェースの ID		@ipsec1

IKE/ISAKMP ポリシーのパラメータ「XR_A(センター),XR_B(拠点)」

	XR_A(センター)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター)
IKE/ISAKMP ポリシー名	XR_B	XR_A
リモート IP アドレス	0.0.0.0	10.10.10.1
インタフェースの ID	@ipsec1	
モード	Aggressive	Aggressive
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
DH グループ	Group2	Group2
ライフタイム	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey1

IPsec ポリシーのパラメータ 「XR_A(センター),XR_B(拠点)」

	XR_A(センター)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター)
使用する IKE ポリシー名	XR_B(IKE1)	XR_A(IKE1)
本装置の LAN 側のネットワークアドレス	192.168.10.0/24	192.168.20.0/24
相手側の LAN 側のネットワークアドレス	192.168.20.0/24	192.168.10.0/24
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
PFS(DH グループ)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)
DISTANCE	1	1

IPsec Keepalive のパラメータ 「XR_A(センター), XR_B(拠点)」

	XR_A(センター)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター)
Policy No.	1	1
source address	192.168.10.1	192.168.20.1
destination address	192.168.20.1	192.168.10.1
interval(sec)	30	45
watch count	3	3
timeout/delay(sec)	60	60
動作 option	1	2
interface	ipsec0	ipsec0

- その他

  - XR_A(センター)では IPsec トンネルで障害が発生したときに、拠点方向へのルートを ISDN に切り替えるためのスタティックルートを設定しています。
  - XR_B(拠点)では IPsec トンネルで障害が発生したときにセンター側へのルートを ISDN に切り替えるためのルートを設定しています。

9-3. 設定例

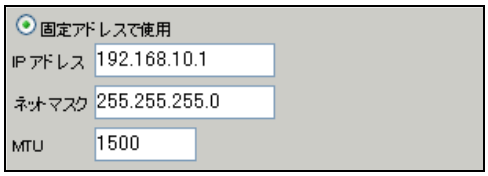
センタールータ（XR_A）

ポイント

拠点と IPsec 接続するための設定を行います。
拠点が動的 IP のため、アグレッシブモードを使用します。
アクセスサーバの設定を行い、WAN 側の回線断等で IPsec KeepAlive による障害が検出された場合、ISDN による着信後、XR_B(拠点)へのルーティングを有効にします。

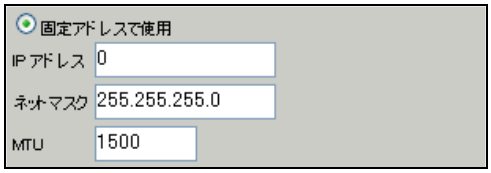
<<インタフェース設定>>

[Ethernet0 の設定]



Ethernet0 に関する設定をします。
※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

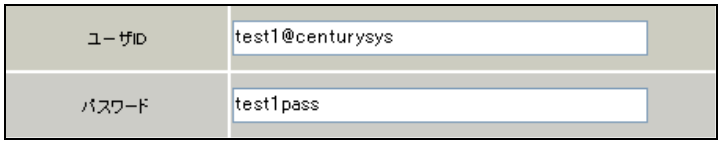
[Ethernet1 の設定]



Ethernet1 に関する設定をします。
PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

<<PPP/PPPoE 設定>>

[接続先設定１]



PPPoE 接続で使用するユーザ ID，パスワードを登録します。

［接続設定］

接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ◉Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ○RS232C
接続形態	○手動接続 ◉常時接続 ○スケジューラ接続
RS232C/BRI接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	○無効 ◉有効
ステートフルパケットインスペクション	○無効 ◉有効 ☐DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ◉有効

PPPoE 接続するインタフェース、および接続形態を選択します。
※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション（全回線共通）	☑回線接続時に前回のPPPoEセッションのPADTを強制送出 ☑非接続SessionのIPv4Packet受信時にPADTを強制送出 ☑非接続SessionのLCP-EchoRequest受信時にPADTを強制送出

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

<<フィルタ設定>>

［入力フィルタ］

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	udp		500		500	☐
ppp0	パケット受信時	許可	esp					☐

IKE パケット，ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

<IPsec サーバ>

[本装置側の設定 1]

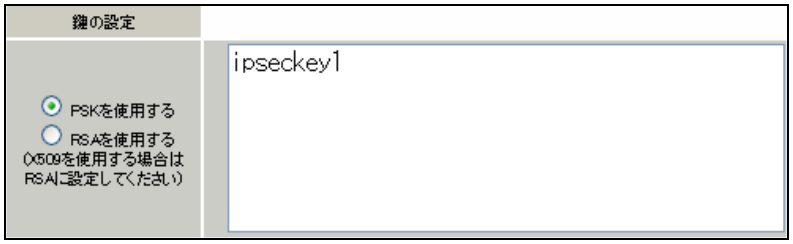
インターフェースのIPアドレス	10.10.10.1
上位ルータのIPアドレス	%ppp0
インターフェースのID	(例:@xr.centurysys)

XR_A(センター)の WAN 側インタフェースの IP アドレス,および上位ルータの IP アドレスを設定します。
PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

[IKE/ISAKMP の設定 1]

IKE/ISAKMPポリシー名	XR_B
接続する本装置側の設定	本装置側の設定1
インターフェースのIPアドレス	0.0.0.0
上位ルータのIPアドレス	
インターフェースのID	@ipsec1 (例:@xr.centurysys)
モードの設定	aggressive モード
transformの設定	1番目 group2-aes128-sha1
	2番目 使用しない
	3番目 使用しない
	4番目 使用しない
IKEのライフタイム	3600 秒 (1081～28800秒まで)

XR_B(拠点)に対する IKE/ISAKMP ポリシーを設定します。



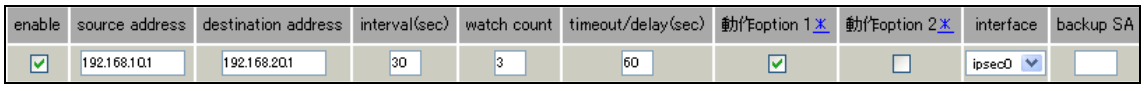
事前共有鍵(PSK)として「ipseckey1」を設定しています。

[IPsec ポリシーの設定 1]

XR_B(拠点)の IP アドレスが不定のため、「Responder として使用する」を選択します。

XR_B(拠点)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。

[IPsec Keep-Alive 設定]



XR_B(拠点)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

IPsecサーバ	○停止 ◉起動

IPsec サーバ機能を起動します。

【アクセスサーバ】

BRI 回線	
回線1 着信	○許可しない ◉許可する

BRI 回線での着信を許可する設定をします。

No.	アカウント	パスワード	アカウント毎に別IPを割り当てる場合	
			本装置のIP	クライアントのIP
1	isdntest	isdnpass	192.168.110.1	192.168.120.1

BRI 回線で着信したときのアカウント，パスワードを設定します。この時に「アカウント毎に別 IP を割り当てる場合」に IP アドレスを設定することにより、着信時に指定した IP アドレスを割り当てることが可能です。

<<スタティックルート設定>>

アドレス	ネットマスク	インターフェース/ゲートウェイ		ディスタンス <1-255>
192.168.20.0	255.255.255.0	ppp6	192.168.120.1	10

IPsec 接続していないときに、拠点方向へのルートを ISDN 側へフローティングさせるために、スタティックルートの設定を行います。
この例では、IPsec 接続しているときは、IPsec ルートのディスタンス値(=1)の方がスタティックルートのディスタンス値(=10)より小さいため、IPsec のルートが有効になっているときは、このスタティックルートは無効の状態になっています。
またゲートウェイの IP アドレスはアクセスサーバ設定で対向ルータに対して割り当てた IP アドレスになっています。

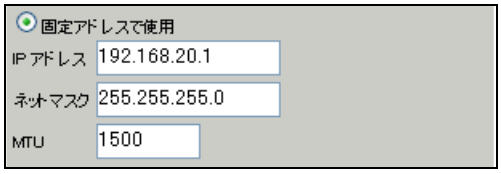
拠点ルータ（XR_B）

ポイント

センターと IPsec 接続するための設定を行います。
WAN 側 IP アドレスが動的 IP のため、アグレッシブモードを使用します。
PPP のマルチセッションの設定を行い、ISDN のオンデマンド接続を行える状態に設定します。
WAN 側の回線断等で IPsec KeepAlive による障害が検出された場合、ISDN 側のルートが有効になり、XR_A(センター)に対して ISDN による発信を行います。

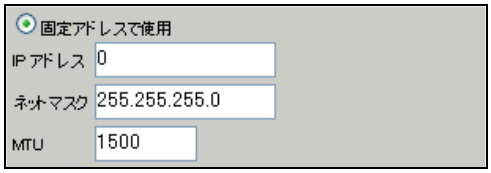
<<インタフェース設定>>

[Ethernet0 の設定]



Ethernet0 に関する設定をします。
※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

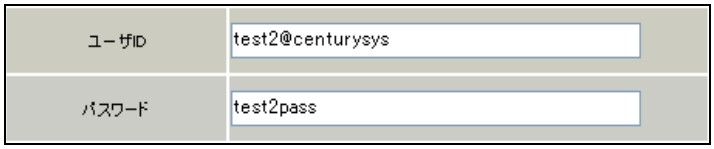
[Ethernet1 の設定]



Ethernet1 に関する設定をします。
PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

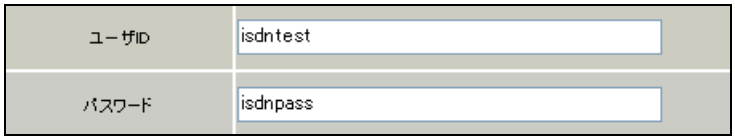
<<PPP/PPPoE 設定>>

[接続先設定 1]

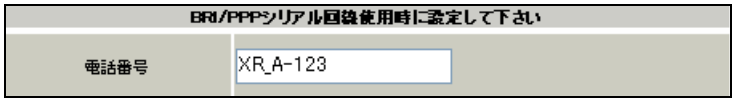


PPPoE 接続で使用するユーザ ID，パスワードを登録します。

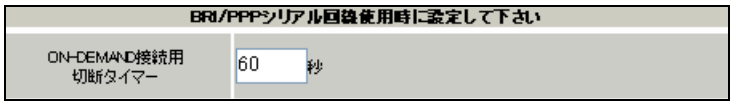
［接続先設定 2］



PPP(ISDN)接続で使用するユーザ ID，パスワードを登録します。

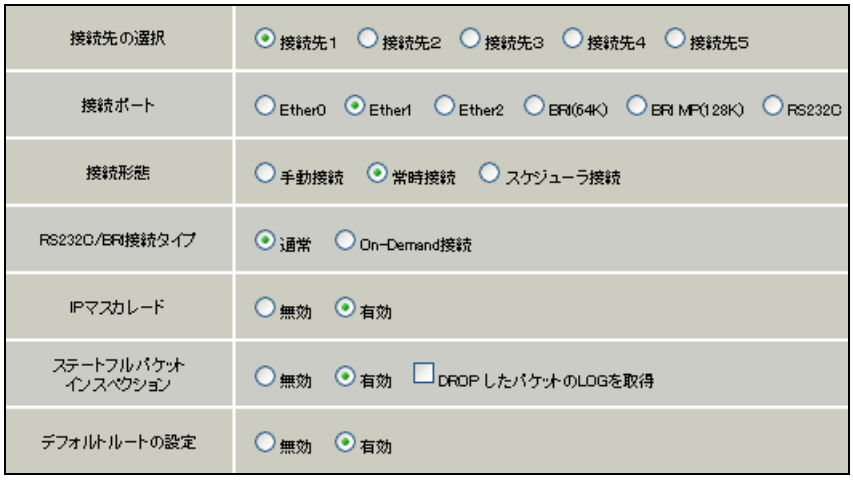


XR_A(センター)の電話番号を登録します。



※この例では ISDN の ON-DEMAND 接続を利用するため、ON-DEMAND 接続用切断タイマーを設定します。
デフォルト値は「180 秒」になります。ご利用環境によって適宜設定を変更して下さい。

［接続設定］



PPPoE 接続するインタフェース、および接続形態を選択します。
※この例では、ルータ経由でのインターネットアクセスも可能になっています。

マルチPPP/PPPoEセッション機能を利用する際は以下を設定して下さい	
マルチ接続 #2	○無効 ◉有効
接続先の選択	○接続先1 ◉接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ○Ether1 ○Ether2 ◉BRI(64K) ○BRI MP(128K) ○RS232C
RS232C/BRI接続タイプ	○通常 ◉On-Demand接続
IPマスカレード	◉無効 ○有効
ステートフルパケットインスペクション	◉無効 ○有効 ☐DROP したパケットのLOGを取得

マルチ接続側(ISDN 側)の接続先，接続ポートおよび接続タイプを設定します。

PPPoE特殊オプション（全回線共通）	☑回線接続時に前回のPPPoEセッションのPADTを強制送出 ☑非接続SessionのIPv4Packet受信時にPADTを強制送出 ☑非接続SessionのLCP-EchoRequest受信時にPADTを強制送出

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

<<フィルタ設定>>

[入力フィルタ]

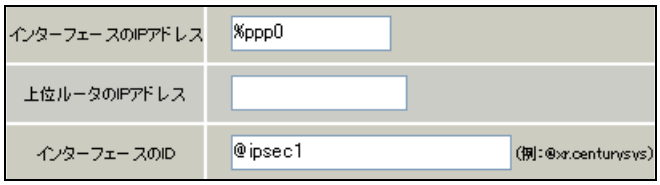
インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	udp		500		500	☐
ppp0	パケット受信時	許可	esp					☐

IKE パケット，ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

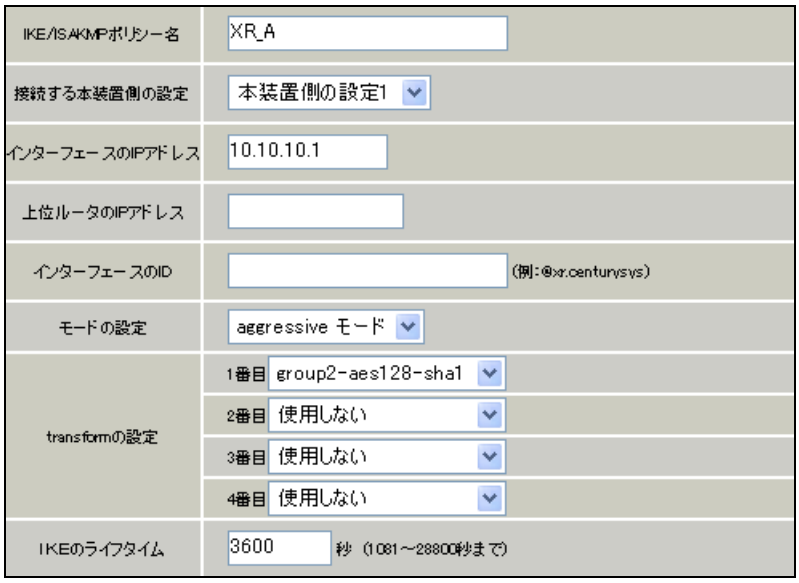
<IPsec サーバ>

[本装置側の設定 1]

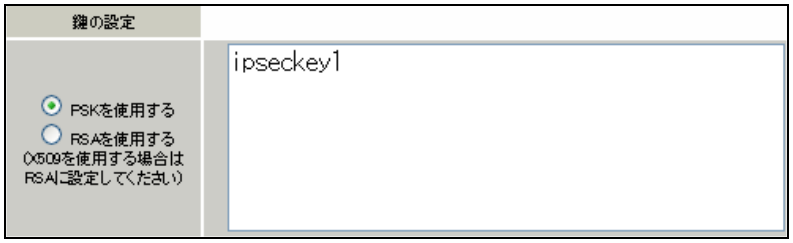


PPPoE 接続で WAN 側(ppp0)インタフェースの IP アドレスが不定のため「%ppp0」，インタフェースの ID として「@ipsec1」を設定します。

[IKE/ISAKMP の設定 1]



XR_A(センター)に対する IKE/ISAKMP ポリシーを設定します。



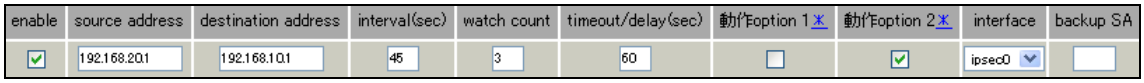
事前共有鍵(PSK)として「ipseckey1」を設定しています。

[IPsec ポリシーの設定 1]

XR_A(センター)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

XR_A(センター)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

[IPsec Keep-Alive 設定]



XR_A(センター)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

IPsec サーバ機能を起動します。

<<スタティックルート設定>>

アドレス	ネットマスク	インターフェース/ゲートウェイ		ディスタンス <1-255>
192.168.10.0	255.255.255.0	ppp2		10

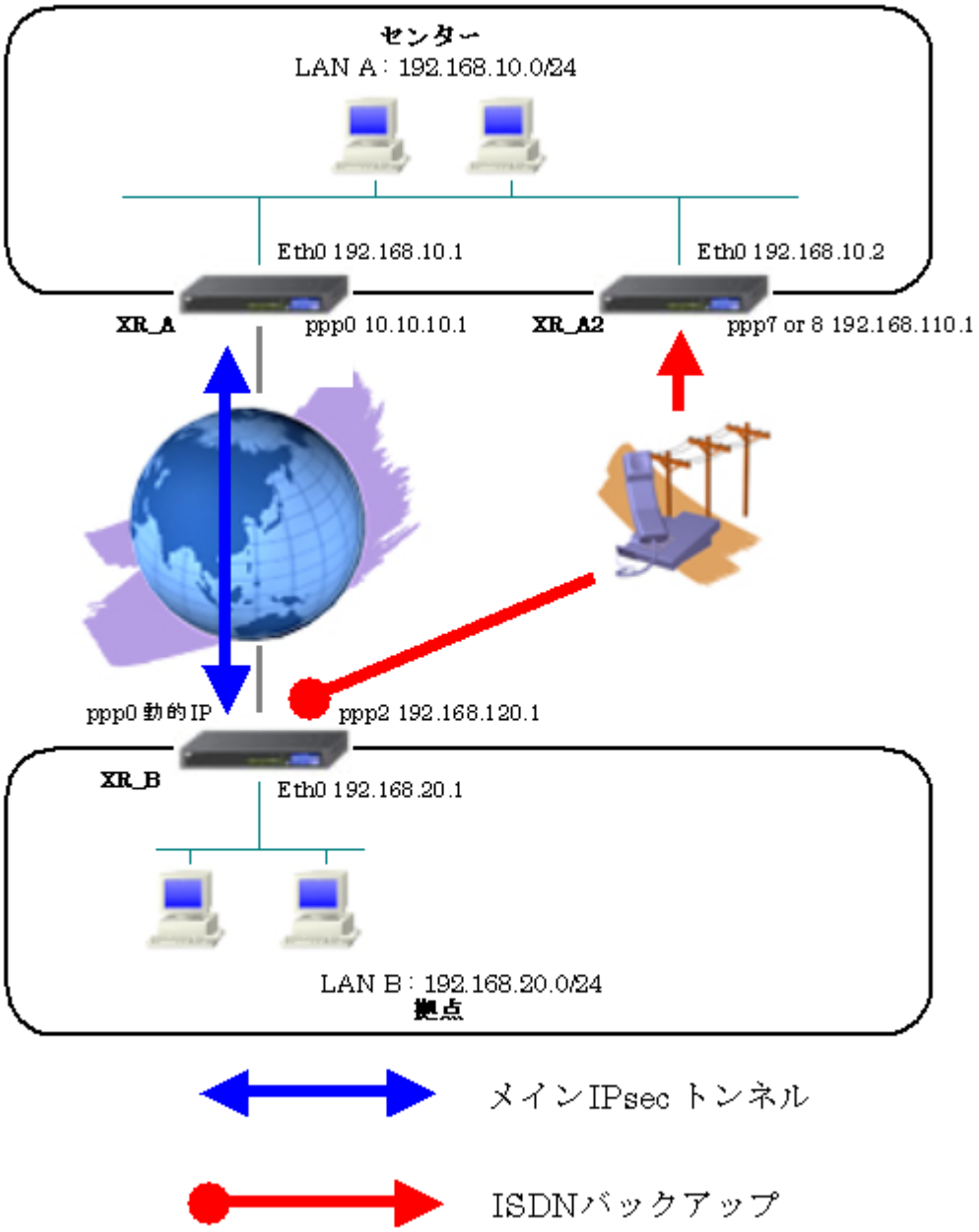
IPsec 接続していないときに、センター方向へのルートを ISDN 側へフローティングさせるために、スタティックルートの設定を行います。
この例では、IPsec 接続しているときは、IPsec ルートのディスタンス値(=1)の方がスタティックルートのディスタンス値(=10)より小さいため、IPsec ルートが有効になっているときは、このスタティックルートは無効の状態になっています。
またこの例では ISDN 側は「ppp2」インタフェースとなるため、インタフェースの項目に「ppp2」を設定しています。

10. ISDN を利用した回線バックアップ例その２（メイン回線 IPsec）

この例は、PPPoE で IPsec 接続しているメイン回線で障害が発生したときに、拠点からの ISDN によるバックアップを実現する設定例です。

またセンターメインルータの機器障害が発生した場合でも、VRRP との組み合わせによりバックアップ経路を利用できます。

10-1. 構成例



10-2. 要件

➢ インタフェースおよび PPP/PPPoE

- インターネットに PPPoE で接続します。
- PPPoE 接続は、自動再接続するように設定しています。
- WAN 側インタフェースの 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は「有効」にしています。
- XR_B(拠点)はマルチ回線で ISDN オンデマンド接続をします。
- XR_A2(センター2)ではアクセスサーバ機能を使用し、XR_B(拠点)からのダイアルアップ接続を受け付けます。

主なインタフェースおよび PPP/PPPoE のパラメータ

	XR_A(センター1)	XR_A2(センター2)	XR_B(拠点)
LAN 側インタフェース	Ether0	Ether0	Ether0
LAN 側 IP アドレス	192.168.10.1	192.168.10.2	192.168.20.1
WAN 側インタフェース	Ether1[ppp0]	-	Ether1[ppp0]
WAN 側 IP アドレス	10.10.10.1	-	動的 IP
PPPoE ユーザ名	test1@centurysys	-	test2@centurysys
PPPoE パスワード	test1pass	-	test2pass
WAN 側接続回線	PPPoE 接続	-	PPPoE 接続
ISDN 番号	-	XR_A-123	XR_B-123
ISDN ユーザ名	-	-	isdntest
ISDN パスワード	-	-	isdnpass
ISDN 側 IP アドレス	-	192.168.110.1	192.168.120.1

➢ VRRP

- Ether0 側で VRRP を使用しています。
- 優先度は XR_A(センター1)「100」,XR_A2(センター2)「50」に設定しています。

主な VRRP のパラメータ

	XR_A(センター1)	XR_A2(センター2)
使用するインターフェース	Ether0	Ether0
ルータ ID	51	51
優先度	100	50
IP アドレス	192.168.10.100	

➢ IPsec

- 鍵交換モードはアグレッシブモードを使用しています。
- XR_A(センター1)は 192.168.10.0/24 <-> 192.168.20.0/24 の時に IPsec を適用します。
- XR_B(拠点)は 192.168.20.0/24 <-> 192.168.10.0/24 の時に IPsec を適用します。
- IPsec KeepAlive は XR_A(センター1)が動作オプション 1 で、XR_B(拠点)が動作オプション 2 で使用しています。

本装置側のパラメータ

	XR_A(センター1)	XR_B(拠点)
インタフェースの IP アドレス	10.10.10.1	%ppp0
上位ルータの IP アドレス	%ppp0	
インタフェースの ID		@ipsec1

IKE/ISAKMP ポリシーのパラメータ「XR_A(センター),XR_B(拠点)」

	XR_A(センター1)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター1)
IKE/ISAKMP ポリシー名	XR_B	XR_A
リモート IP アドレス	0.0.0.0	10.10.10.1
インタフェースの ID	@ipsec1	
モード	Aggressive	Aggressive
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
DH グループ	Group2	Group2
ライフタイム	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey1

IPsec ポリシーのパラメータ 「XR_A(センター),XR_B(拠点)」

	XR_A(センター1)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター1)
使用する IKE ポリシー名	XR_B(IKE1)	XR_A(IKE1)
本装置の LAN 側のネットワークアドレス	192.168.10.0/24	192.168.20.0/24
相手側の LAN 側のネットワークアドレス	192.168.20.0/24	192.168.10.0/24
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
PFS(DH グループ)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)
DISTANCE	1	1

IPsec Keepalive のパラメータ 「XR_A(センター1), XR_B(拠点)」

	XR_A(センター1)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター1)
Policy No.	1	1
source address	192.168.10.1	192.168.20.1
destination address	192.168.20.1	192.168.10.1
interval(sec)	30	45
watch count	3	3
timeout/delay(sec)	60	60
動作 option	1	2
interface	ipsec0	ipsec0

- その他

  - XR_A(センター1)では IPsec トンネルで障害が発生したときに、拠点方向へのルートを XR_A2(センター2)に切り替えるためのスタティックルートを設定しています。
  - XR_A2(センター2)では ISDN 接続していないときに拠点方向へのルートを XR_A(センター1)へ切り替えるためのスタティックルートを設定しています。
  - XR_B(拠点)では IPsec トンネルで障害が発生したときにセンター側へのルートを ISDN に切り替えるためのルートを設定しています。

10-3. 設定例

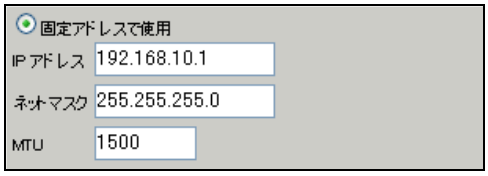
センタールータ１（XR_A）

ポイント

拠点と IPsec 接続するための設定を行います。
拠点が動的 IP のため、アグレッシブモードを使用します。
WAN 側の回線断等で IPsec KeepAlive による障害が検出された場合、XR_A2(センター2)へのルーティングを有効にします。
XR_A の機器障害が発生した場合に備えて、XR_A2(センター2)との VRRP で冗長化を行っています。

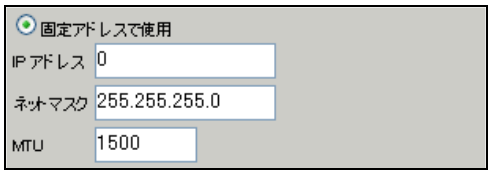
<<インタフェース設定>>

[Ethernet0 の設定]



Ethernet0 に関する設定をします。
※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

[Ethernet1 の設定]



Ethernet1 に関する設定をします。
PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

<<PPP/PPPoE 設定>>

［接続先設定１］

ユーザID	test1@centurysys
パスワード	test1pass

PPPoE 接続で使用するユーザ ID，パスワードを登録します。

［接続設定］

接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ◉Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ○RS232C
接続形態	○手動接続 ◉常時接続 ○スケジューラ接続
RS232C/BRI接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	○無効 ◉有効
ステートフルパケットインスペクション	○無効 ◉有効 □DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ◉有効

PPPoE 接続するインタフェース、および接続形態を選択します。

※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション（全回線共通）	☑回線接続時に前回のPPPoEセッションのPADTを強制送出 ☑非接続SessionのIPv4Packet受信時にPADTを強制送出 ☑非接続SessionのLCP-EchoRequest受信時にPADTを強制送出

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

<<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	udp		500		500	□
ppp0	パケット受信時	許可	esp					□

IKE パケット，ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

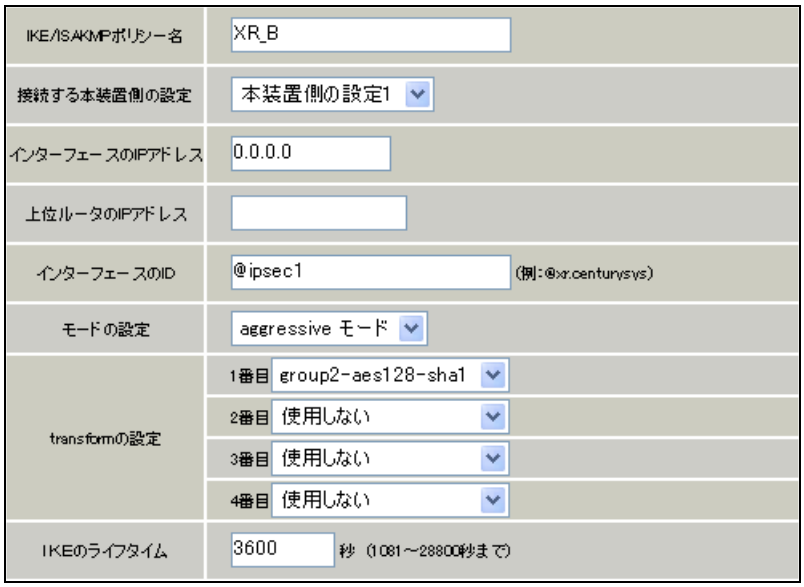
<IPsec サーバ>

[本装置側の設定 1]

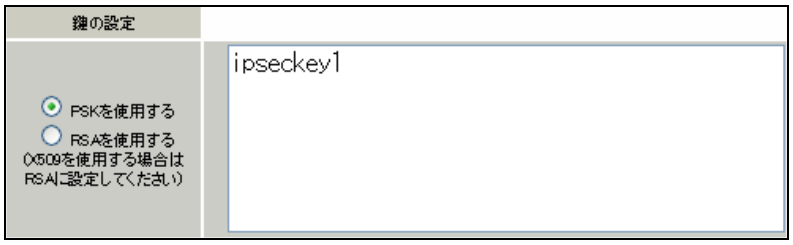
インターフェースのIPアドレス	10.10.10.1
上位ルータのIPアドレス	%ppp0
インターフェースのID	(例:@xr.centurysys)

XR_A(センター)の WAN 側インタフェースの IP アドレス,および上位ルータの IP アドレスを設定します。
PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

[IKE/ISAKMP の設定 1]



XR_B(拠点)に対する IKE/ISAKMP ポリシーを設定します。



事前共有鍵(PSK)として「ipseckey1」を設定しています。

[IPsec ポリシーの設定 1]

XR_B(拠点)の IP アドレスが不定のため、「Responder として使用する」を選択します。

使用するIKEポリシー名の選択	XR_B (IKE1)
本装置側のLAN側のネットワークアドレス	192.168.10.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.20.0/24 (例:192.168.0.0/24)
PH2のTransFormの選択	aes128-sha1
PFS	使用する 使用しない
DH Groupの選択(PFS使用時に有効)	group2
SAのライフタイム	28800 秒 (1081～86400秒まで)
DISTANCE	1 (1～255まで)

XR_B(拠点)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。

［IPsec Keep-Alive 設定］

enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1 *	動作option 2 *	interface	backup SA
☑	192.168.10.1	192.168.20.1	30	3	60	☑	☐	ipsec0	

「LAN_B」に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

IPsecサーバ	○停止 ◉起動

IPsec サーバを起動します。

【VRRP サービス】

使用するインターフェース	仮想MACアドレス	ルータID	優先度	IPアドレス	インターバル	Auth_Type	password
Ether 0	使用しない	51	100	192.168.10.100	1	指定しない	

LAN 側インタフェース「Ether0」で XR_A2(センター2)と VRRP による冗長化を行います。

VRRPサービス	○停止 ◉起動

VRRP サービスを起動します。

<<スタティックルート設定>>

アドレス	ネットマスク	インターフェース/ゲートウェイ		ディスタンス <1-255>
192.168.20.0	255.255.255.0		192.168.10.2	10

IPsec 接続していないときに、拠点方向へのルートを XR_A2 側へフローティングさせるために、スタティックルートの設定を行います。
この例では、IPsec 接続しているときは、IPsec ルートのディスタンス値(=1)の方がスタティックルートのディスタンス値(=10)より小さいため、IPsec ルートが有効になっているときは、このスタティックルートは無効の状態になっています。

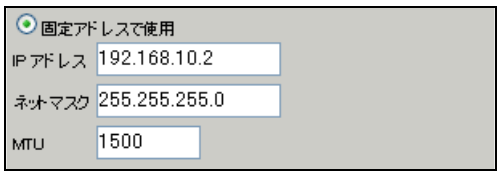
センタールータ 2（XR_A2）

ポイント

アクセスサーバの設定を行い、ISDN による着信後、XR_B(拠点)へのルーティングを有効にします。
XR_A の LAN 側で障害が発生した場合に備えて、VRRP で冗長化を行っています。

<<インタフェース設定>>

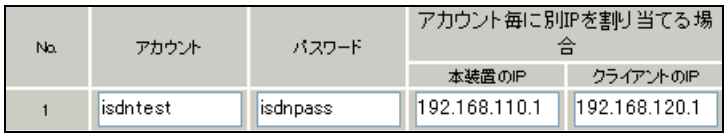
[Ethernet0 の設定]



Ethernet0 に関する設定をします。
※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

【アクセスサーバ】

BRI 回線での着信を許可する設定をします。



BRI 回線で着信したときのアカウント，パスワードを設定します。この時に「アカウント毎に別 IP を割り当てる場合」に IP アドレスを設定することにより、着信時に指定した IP アドレスを割り当てることが可能です。

<<スタティックルート設定>>

アドレス	ネットマスク	インターフェース/ゲートウェイ		ディスタンス <1-255>
192.168.20.0	255.255.255.0	ppp6	192.168.120.1	1
192.168.20.0	255.255.255.0		192.168.10.1	10

一行目は XR_B(拠点)からの ISDN 発信を着信した場合に有効になるルートです。ゲートウェイの IP アドレスはアクセスサーバ設定で対向ルータに対して割り当てた IP アドレスになっています。着信していない場合は、二行目のルートが有効になっています。

【VRRP サービス】

使用するインターフェース	仮想MACアドレス	ルータID	優先度	IPアドレス	インターバル	Auth_Type	password
Ether 0	使用しない	51	50	192.168.10.100	1	指定しない	

LAN 側インタフェース「Ether0」で XR_A(センター1)と VRRP による冗長化を行います。
この例では、正常時 XR_A2(センター2)はバックアップとなるため、XR_A(センター1)より低い優先度「50」を設定しています。

VRRPサービス	○停止　◉起動

VRRP サービスを起動します。

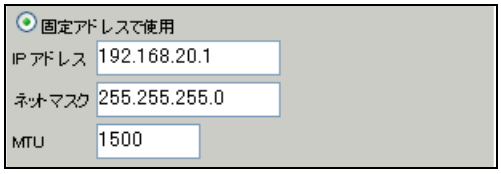
拠点ルータ（XR_B）

ポイント

XR_A(センター1)と IPsec 接続するための設定を行います。
WAN 側 IP アドレスが動的 IP のため、アグレッシブモードを使用します。
PPP のマルチセッションの設定を行い、ISDN のオンデマンド接続を行える状態に設定します。
WAN 側の回線断等で IPsec KeepAlive による障害が検出された場合、ISDN 側のルートが有効になり、
XR_A2(センター2)に対して ISDN による発信を行います。

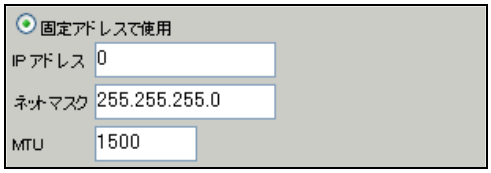
<<インタフェース設定>>

[Ethernet0 の設定]



Ethernet0 に関する設定をします。
※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

[Ethernet1 の設定]



Ethernet1 に関する設定をします。
PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

<<PPP/PPPoE 設定>>

[接続先設定 1]

ユーザID	test2@centurysys
パスワード	test2pass

PPPoE 接続で使用するユーザ ID，パスワードを登録します。

[接続先設定 2]

ユーザID	isdntest
パスワード	isdnpass

PPP(ISDN)接続で使用するユーザ ID，パスワードを登録します。

BRI/PPPシリアル回線使用時に設定して下さい	
電話番号	XR_A-123

センタールータ(XR_A2)の電話番号を登録します。

BRI/PPPシリアル回線使用時に設定して下さい	
ON-DEMAND接続用 切断タイマー	60 秒

※この例では ISDN の ON-DEMAND 接続を利用するため、ON-DEMAND 接続用切断タイマーを設定します。
デフォルト値は「180 秒」になります。ご利用環境によって適宜設定を変更して下さい。

［接続設定］

接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ◉Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ○RS232C
接続形態	○手動接続 ◉常時接続 ○スケジューラ接続
RS232C/BRI接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	○無効 ◉有効
ステートフルパケット インスペクション	○無効 ◉有効 □DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ◉有効

PPPoE 接続するインタフェース、および接続形態を選択します。
※この例では、ルータ経由でのインターネットアクセスも可能になっています。

マルチPPP/PPPoEセッション機能を利用する際は以下を設定して下さい	
マルチ接続 #2	○無効 ◉有効
接続先の選択	○接続先1 ◉接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ○Ether1 ○Ether2 ◉BRI(64K) ○BRI MP(128K) ○RS232C
RS232C/BRI接続タイプ	○通常 ◉On-Demand接続
IPマスカレード	◉無効 ○有効
ステートフルパケット インスペクション	◉無効 ○有効 □DROP したパケットのLOGを取得

マルチ接続側(ISDN 側)の接続先，接続ポートおよび接続タイプを設定します。

PPPoE特殊オプション (全回線共通)	☑回線接続時に前回のPPPoEセッションのPADTを強制送出 ☑非接続SessionのIPv4Packet受信時にPADTを強制送出 ☑非接続SessionのLCP-EchoRequest受信時にPADTを強制送出

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

<<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	udp		500		500	□
ppp0	パケット受信時	許可	esp					□

IKE パケット，ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

<IPsec サーバ>

[本装置側の設定 1]

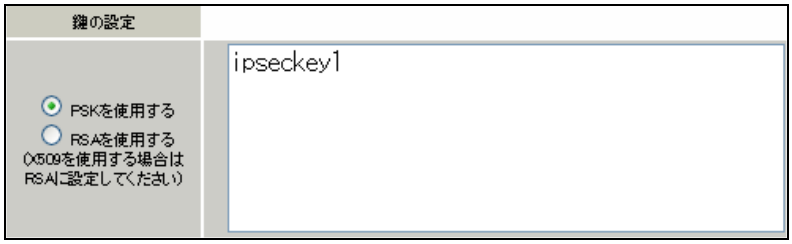
インターフェースのIPアドレス	%ppp0
上位ルータのIPアドレス	
インターフェースのID	@ipsec1 (例:@xr.centurysys)

PPPoE 接続で WAN 側(ppp0)インタフェースの IP アドレスが不定のため「%ppp0」，インタフェースの ID として「@ipsec1」を設定します。

[IKE/ISAKMP の設定 1]

IKE/ISAKMPポリシー名	XR_A
接続する本装置側の設定	本装置側の設定1
インターフェースのIPアドレス	10.10.10.1
上位ルータのIPアドレス	
インターフェースのID	(例:@xr.centurysys)
モードの設定	aggressive モード
transformの設定	1番目 group2-aes128-sha1
	2番目 使用しない
	3番目 使用しない
	4番目 使用しない
IKEのライフタイム	3600 秒 (1081～28800秒まで)

XR_A(センター1)に対する IKE/ISAKMP ポリシーを設定します。



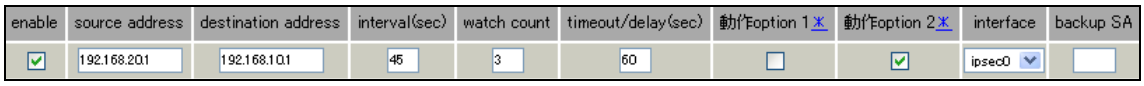
事前共有鍵(PSK)として「ipseckey1」を設定しています。

[IPsec ポリシーの設定 1]

XR_A(センター1)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

XR_A(センター1)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

[IPsec Keep-Alive 設定]



XR_A(センター1)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

IPsec サーバ機能を起動します。

<<スタティックルート設定>>

アドレス	ネットマスク	インターフェース/ゲートウェイ		ディスタンス <1-255>
192.168.10.0	255.255.255.0	ppp2		10

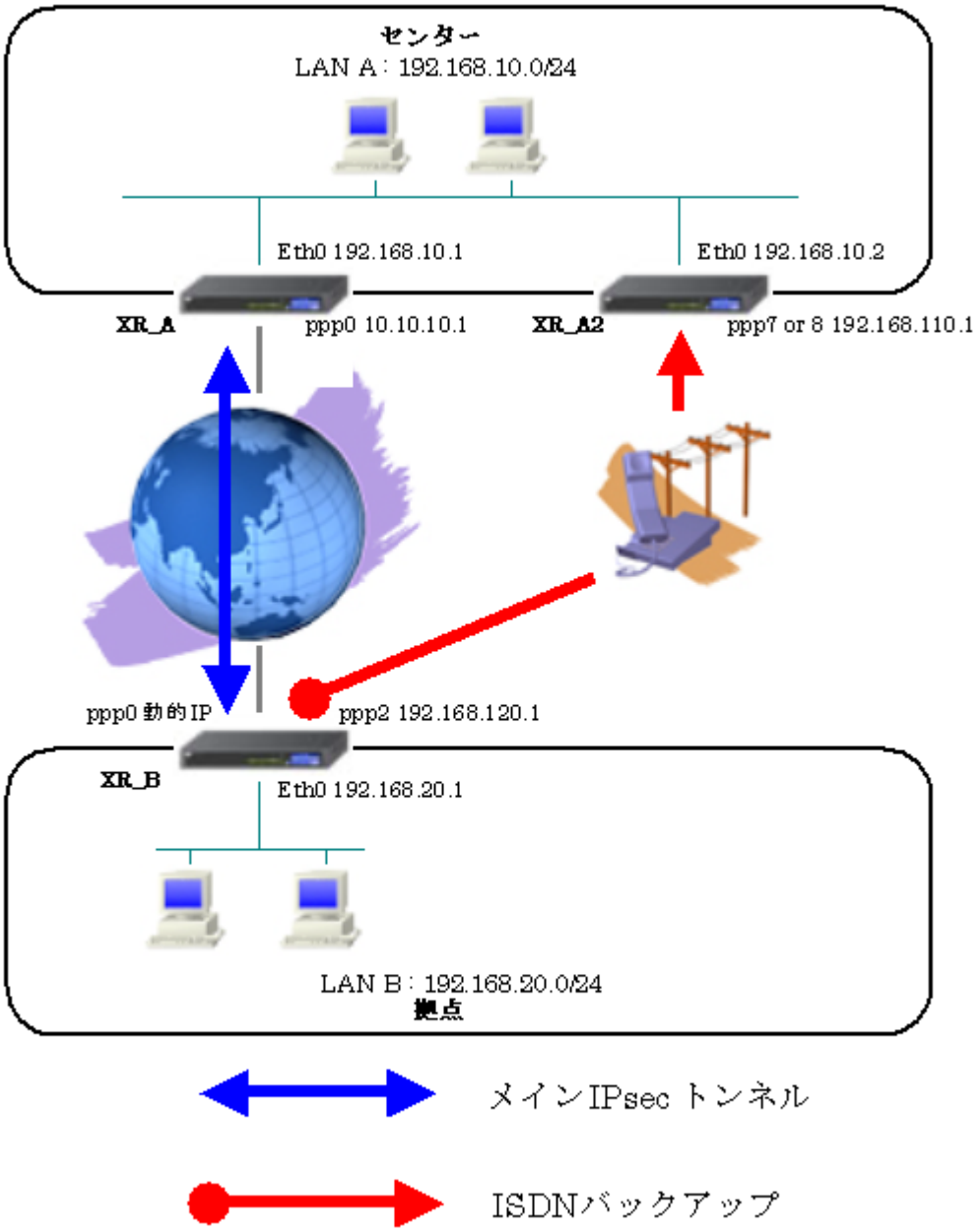
IPsec 接続していないときに、センター方向へのルートを ISDN 側へフローティングさせるために、スタティックルートの設定を行います。
この例では、IPsec 接続しているときは、IPsec ルートのディスタンス値(=1)の方がスタティックルートのディスタンス値(=10)より小さいため、IPsec ルートが有効になっているときは、このスタティックルートは無効の状態になっています。
また ISDN 側は「ppp2」インタフェースとなるため、インタフェースの項目に「ppp2」を設定しています。

11. ISDN を利用した回線バックアップ例その３（メイン回線 IPsec）

この例は、PPPoE で IPsec 接続しているメイン回線で障害が発生したときに、拠点側からの ISDN によるバックアップを実現する設定例です。

またセンターメインルータの機器障害や VRRP の状態変化を検出した場合でも、VRRP, Netevent 機能との組み合わせによりバックアップ経路を利用できる設定になっています。

11-1. 構成例



11-2. 要件

➢ インタフェースおよび PPP/PPPoE

- インターネットに PPPoE で接続します。
- PPPoE 接続は、自動再接続するように設定しています。
- WAN 側インタフェースの 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は「有効」にしています。
- XR_B(拠点)はマルチ回線で ISDN オンデマンド接続をします。
- XR_A2(センター2)ではアクセスサーバ機能を使用し、XR_B(拠点)からのダイアルアップ接続を受け付けます。

主なインタフェースおよび PPP/PPPoE のパラメータ

	XR_A(センター1)	XR_A2(センター2)	XR_B(拠点)
LAN 側インタフェース	Ether0	Ether0	Ether0
LAN 側 IP アドレス	192.168.10.1	192.168.10.2	192.168.20.1
WAN 側インタフェース	Ether1[ppp0]	-	Ether1[ppp0]
WAN 側 IP アドレス	10.10.10.1	-	動的 IP
PPPoE ユーザ名	test1@centurysys	-	test2@centurysys
PPPoE パスワード	test1pass	-	test2pass
WAN 側接続回線	PPPoE 接続	-	PPPoE 接続
ISDN 番号	-	XR_A-123	XR_B-123
ISDN ユーザ名	-	-	isdntest
ISDN パスワード	-	-	isdnpass
ISDN 側 IP アドレス	-	192.168.110.1	192.168.120.1

➢ VRRP

- Ether0 側で VRRP を使用しています。
- 優先度は XR_A(センター1)「100」,XR_A2(センター2)「50」に設定しています。

主な VRRP のパラメータ

	XR_A(センター1)	XR_A2(センター2)
使用するインターフェース	Ether0	Ether0
ルータ ID	51	51
優先度	100	50
IP アドレス	192.168.10.100	

➢ IPsec

- 鍵交換モードはアグレッシブモードを使用しています。
- XR_A(センター1)は 192.168.10.0/24 <-> 192.168.20.0/24 の時に IPsec を適用します。
- XR_B(拠点)は 192.168.20.0/24 <-> 192.168.10.0/24 の時に IPsec を適用します。
- IPsec KeepAlive は XR_A(センター1)が動作オプション 1 で、XR_B(拠点)が動作オプション 2 で使用しています。

本装置側のパラメータ

	XR_A(センター1)	XR_B(拠点)
インタフェースの IP アドレス	10.10.10.1	%ppp0
上位ルータの IP アドレス	%ppp0	
インタフェースの ID		@ipsec1

IKE/ISAKMP ポリシーのパラメータ「XR_A(センター1),XR_B(拠点)」

	XR_A(センター1)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター1)
IKE/ISAKMP ポリシー名	XR_B	XR_A
リモート IP アドレス	0.0.0.0	10.10.10.1
インタフェースの ID	@ipsec1	
モード	Aggressive	Aggressive
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
DH グループ	Group2	Group2
ライフタイム	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey1

IPsec ポリシーのパラメータ(1) 「XR_A(センター1),XR_B(拠点)」

	XR_A(センター1)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター1)
使用する IKE ポリシー名	XR_B(IKE1)	XR_A(IKE1)
本装置の LAN 側のネットワークアドレス	192.168.10.0/24	192.168.20.0/24
相手側の LAN 側のネットワークアドレス	192.168.20.0/24	192.168.10.0/24
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
PFS(DH グループ)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)
DISTANCE	1	1

IPsec Keepalive のパラメータ 「XR_A(センター1), XR_B(拠点)」

	XR_A(センター1)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター1)
Policy No.	1	1
source address	192.168.10.1	192.168.20.1
destination address	192.168.20.1	192.168.10.1
interval(sec)	30	45
watch count	3	3
timeout/delay(sec)	60	60
動作 option	1	2
interface	ipsec0	ipsec0

- その他

  - XR_A(センター1)では IPsec トンネルで障害が発生したときに、拠点方向へのルートを XR_A2(センター2)に切り替えるためのスタティックルートを設定しています。
    また VRRP の状態がマスタから変化したとき、Netevent 機能により IPsec を切断します。
  - XR_A2(センター2)では ISDN 接続していないときに拠点方向へのルートを XR_A(センター1)へ切り替えるためのスタティックルートを設定しています。
  - XR_B(拠点)では IPsec トンネルで障害が発生したときにセンター側へのルートを ISDN に切り替えるためのルートを設定しています。

11-3. 設定例

センタールータ１（XR_A）

ポイント

拠点と IPsec 接続するための設定を行います。
拠点が動的 IP のため、アグレッシブモードを使用します。
WAN 側の回線断等で IPsec KeepAlive による障害が検出された場合、XR_A2(センター2)へのルーティングを有効にします。
XR_A の機器障害が発生した場合に備えて、XR_A2(センター2)との VRRP で冗長化を行っています。
XR_A の VRRP をトリガに IPsec を接続切断する Netevent 機能の設定を行っています。
「ISDN を利用した回線バックアップ例その２」の「センタールータ 1(XR_A)」の設定に下記の設定を追加することにより、この例のセンタールータ 1(XR_A)の設定条件を満たします。

<<ネットワークイベント機能>>

［VRRP 監視の設定］

NO	enable	トリガー番号	インターバル	リトライ	VRRP ルータID
1	☑	1	10	3	51

監視する VRRP のルータ ID を指定します。
これがトリガとなります。

［IPsec 接続切断設定］

NO	IPSECポリシー番号,又はインターフェース名	使用IKE連動機能	使用interface連動機能
1	ipsec0	使用しない	使用する

VRRP の状態変化が発生したときのイベント(この例では IPsec)を設定します。
IPsec のインタフェースを指定することにより、このインタフェースで接続している全ての IPsec は切断されます。トリガ復旧時には再度 IPsec 接続されます。

［イベント実行テーブル設定］

NO	実行イベント設定	オプション設定
1	IPSECポリシー	1

実行されるイベントとして IPsec を選択します。
その時の動作は「IPsec 接続切断設定」で設定した動作になります。

［ネットワークイベント設定］

トリガー番号	実行イベントテーブル番号
1	1

「トリガ番号」は、この例では「VRRP 監視の設定」で指定した番号を、「実行イベントテーブル番号」は「イベント実行テーブル設定」を設定します。

［ネットワークイベントサービス設定］

ネットワークイベント	○ 停止 ◉ 起動
ping監視	◉ 停止 ○ 起動
link監視	◉ 停止 ○ 起動
vrrp監視	○ 停止 ◉ 起動

この設定例では、「ネットワークイベント」と「VRRP 監視」を使用しますので、この二つを起動します。

センタールータ 2（XR_A2）

ポイント

「ISDN を利用した回線バックアップ例その２」のセンタールータ 2(XR_A2)と同じ設定です。

(設定省略)

拠点ルータ（XR_B）

ポイント

「ISDN を利用した回線バックアップ例その２」の拠点ルータ(XR_B)と同じ設定です。

(設定省略)

FutureNet XR シリーズ　インターネット VPN 設定例集

IPsec 編

2007 年 3 月

発行　センチュリー・システムズ株式会社