FutureNet VPN Client/NET-G

接続設定ガイド

Ver 2.0.0

センチュリー・システムズ株式会社

目次

はじめに

- FutureNet はセンチュリー・システムズ株式会社の登録商標です。
- FutureNet VPN Client/NET-G はセンチュリー・システムズ株式会社の商標です。
-
- ssh® は SSH Communications Security Corp の米国および一部の地域での登録商標です。
- SSH のロゴ、SSH Certifier、NET-G Secure VPN Client は、SSH Communications Security Corp の商標であり、一部の地域では登録されている場合もあります。その他の名前およびマークは各社の所有物です。
- 本書の内容の正確性または有用性については、準拠法に従って要求された場合または書面で明示的に合意された場合を除き、一切の保証を致しません。
- FutureNet VPN Client/NET-G のインストール方法および詳細な操作方法につきましては、CD-ROM に収録されております「ユーザーマニュアル」をご覧ください。
- 本ガイドは、以下の FutureNet XR 製品に対応しております。
  - XR-380, XR-380/DES
  - XR-410 シリーズ
  - XR-410/TX2-L2
  - XR-440/C
  - XR-640/CD
  - XR-640/CD-L2
  - XR-510/C
  - XR-540/C
  - XR-730/C
  - XR-1000 Ver2.0 以降
  - XR-1000/TX4
  - XR-1100 シリーズ

- 本書の内容の一部または全部を無断で転載することを禁止しています。
- 本書の内容については、将来予告なしに変更することがあります。
- 本書の内容については万全を期しておりますが、ご不審な点や誤り、記載漏れ等お気づきの点がありましたらお手数ですが、ご一報下さいますようお願い致します。
- 本書は FutureNet VPN Client/NET-G は Ver2.3.0.4, XR は XR-510/C, XR-540/C Ver3.5.0 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。

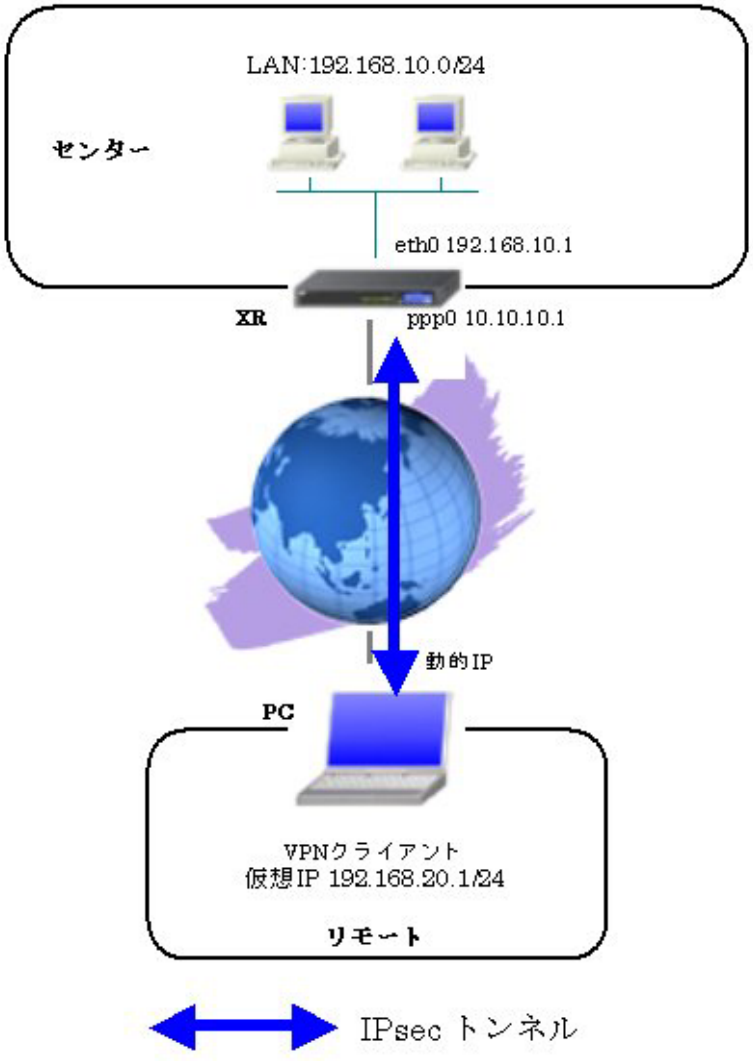
改版履歴

Version	更新内容
1.1.0	初版
1.1.1	フィルタ設定の内容を一部変更
2.0.0	WindowsVista 対応版 Ver2.3.0.4 リリースに伴う改版

1. 基本設定例１ ～仮想 IP アドレスを使用した設定～

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 VPN が利用可能です。この設定例では、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.　設定例

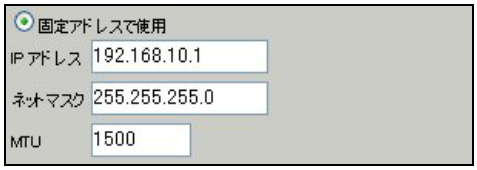
1-2-1.　センタールータ（XR）

ポイント

VPN クライアントをインストールした PC と IPsec 接続するための設定を行います。
VPN クライアントをインストールした PC は動的 IP アドレスを取得しているため、IKE モードとして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]



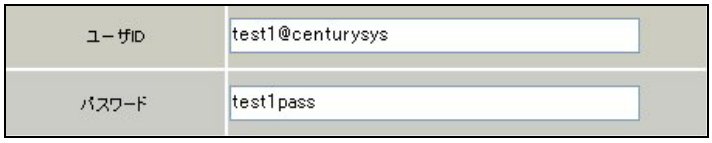
Ethernet0 に関する設定をします。
※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

[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) ○Leased Line(64K) ○Leased Line(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、XR 配下の端末からの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］

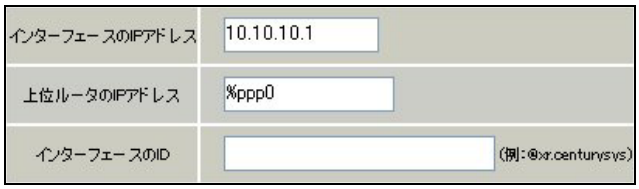
インターフェース	方向	動作	プロトコル		送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	ICMP type/code	送信元MACアドレス	LOG
ppp0	パケット受信時	許可	udp			500		500			☐
ppp0	パケット受信時	許可	esp								☐

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]

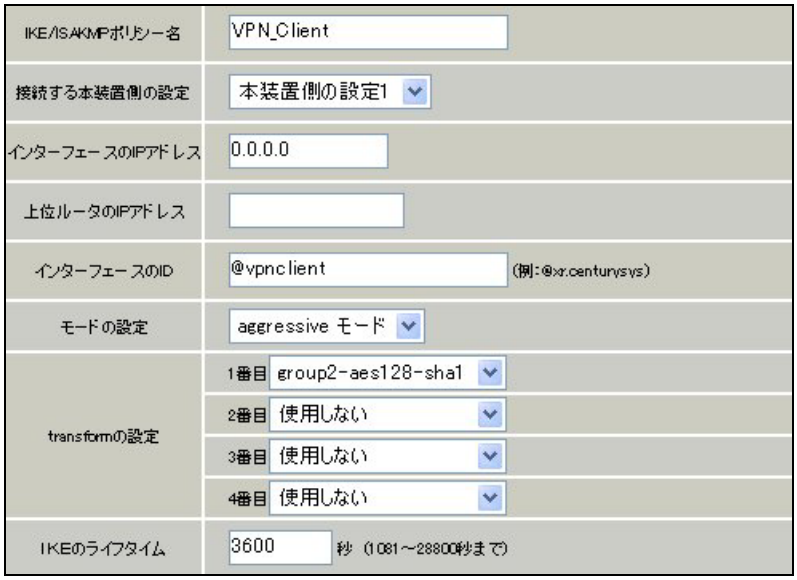


XR の WAN 側インタフェースの IP アドレス，および上位ルータの IP アドレスを設定します。PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

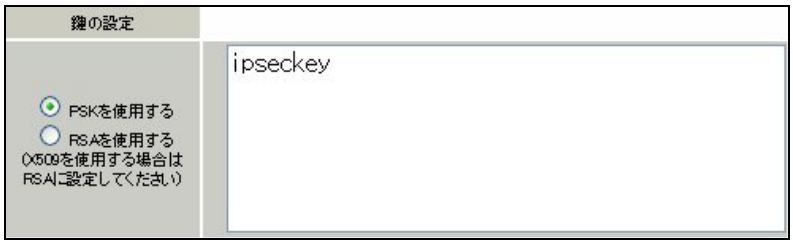
[IKE/ISAKMP の設定 1]

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	VPN_Client
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)	ipseckey



VPN クライアントに対する IKE/ISAKMP ポリシーを設定します。
XR における ID の設定では”@”を付けますが、VPN Client/NET-G では、”@”を付けない形式で設定してください。VPN Client/NET-G でも”@”を付けて設定すると接続できません。



事前共有鍵(PSK)として「ipseckey」を設定しています。

[IPsec ポリシーの設定 1]

VPN クライアントの 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	VPN_Client (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	192.168.20.1/32
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

VPN クライアントに対して IPsec 通信を行う IP アドレスの範囲を設定します。
ここで設定したアドレスと同じ値を、VPN Client/NET-G の「仮想 IP アドレスを取得する」項目で設定します。ただし XR の設定では必ず”<IP address>/32”の形式で設定します。”<IP address>/24”の設定では接続できませんのでご注意ください。

【IPsec サーバ】

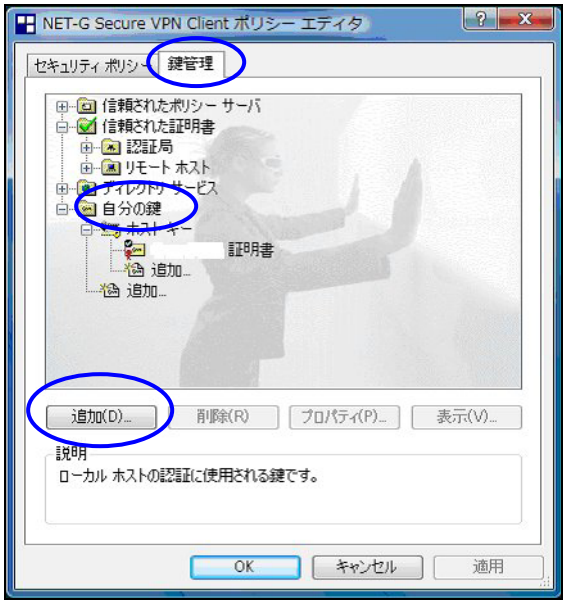
IPsec サーバ機能を起動します。

1-2-2. VPN クライアント（PC）

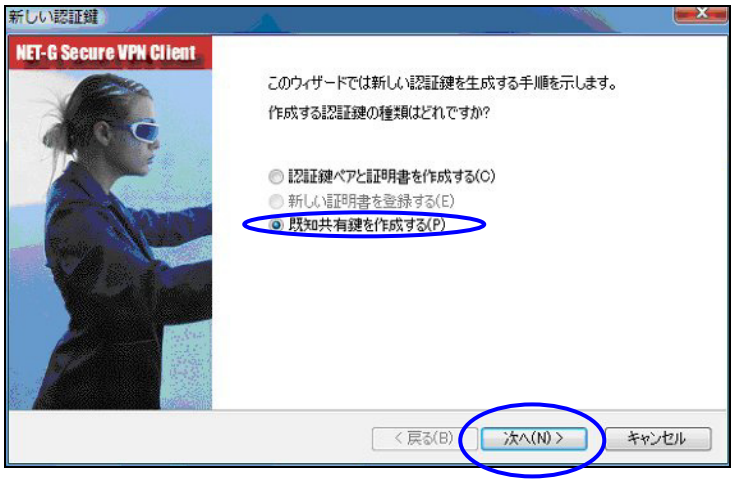
ポイント

FutureNet VPN Client/NET-G をインストールした PC と XR との IPsec 接続になります。
本設定例では、IKE モードとしてアグレッシブモードおよび仮想 IP アドレスを使用しています。

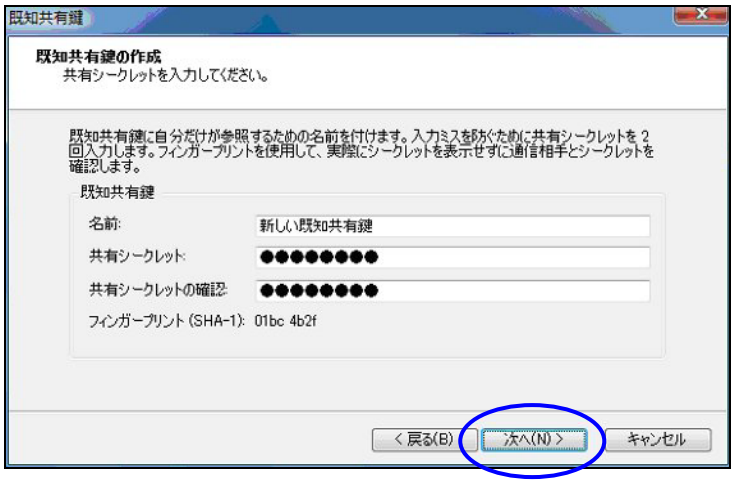
<<既知共有鍵(Pre shared Key)の設定>>



「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。

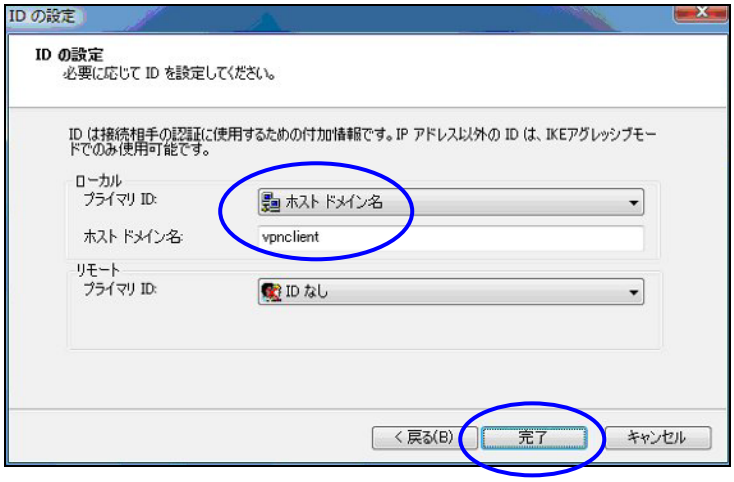


「新しい認証鍵」ウィンドウが開きますので、「既知共有鍵を作成する」を選択し、「次へ」ボタンをクリックして下さい。

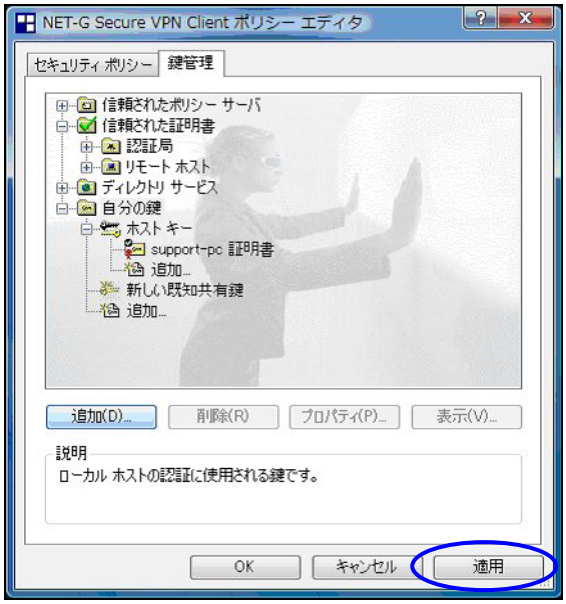


「既知共有鍵の作成」画面が開きます。ここで既知共有鍵（PSK）を作成します。「名前」には任意の設定名を入力します。「共有シークレット」「共有シークレットの確認」項目には既知共有鍵を入力し、「次へ」ボタンをクリックします。
このとき入力した鍵は“＊”,“●”等で表示されます。
この例では共有シークレットとして「ipseckey」を設定しています。

<<ID の設定>>

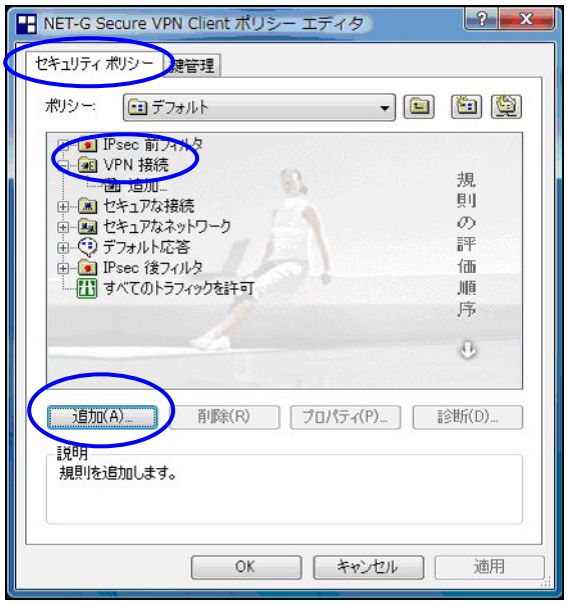


既知共有鍵の作成後、「ID の設定」画面で、「ローカル」側項目について、プライマリ ID は「ホストドメイン名」を選択し、ホストドメイン名に ID を入力します。ここには XR シリーズの IPsec サーバ「IKE/ISAKMP の設定」における「インタフェース ID」と同じ ID を設定します。
※ただしこの時、ホストドメイン名には”@”をつけないで設定して下さい。
「完了」ボタンをクリックすると「鍵管理」画面に戻ります。

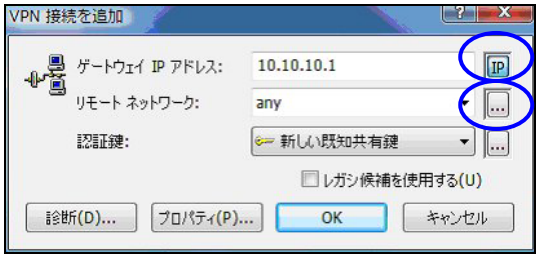


ここまでの設定が終わったら、必ず「適用」ボタンをクリックして下さい。「適用」ボタンをクリックしないと適切に設定されない場合があります。

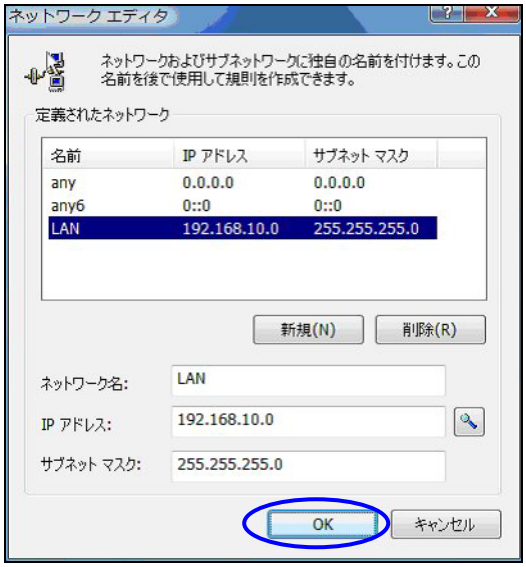
<<セキュリティポリシーの設定>>



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。

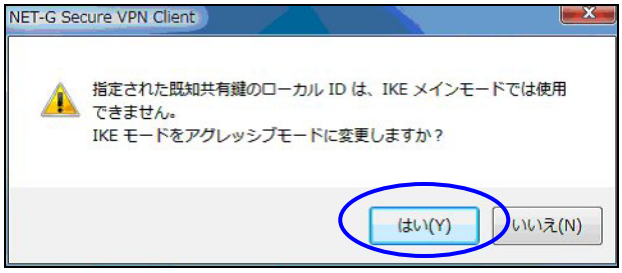


「VPN 接続を追加」画面が開きます。「ゲートウェイ IP アドレス」で右端の”IP”をクリックし、XR の WAN 側 IP アドレスを設定します。
「認証鍵」は、既知共有鍵の設定で登録した既知共有鍵の設定名を選択します。
「リモートネットワーク」については右端にある”・・・”をクリックして下さい。

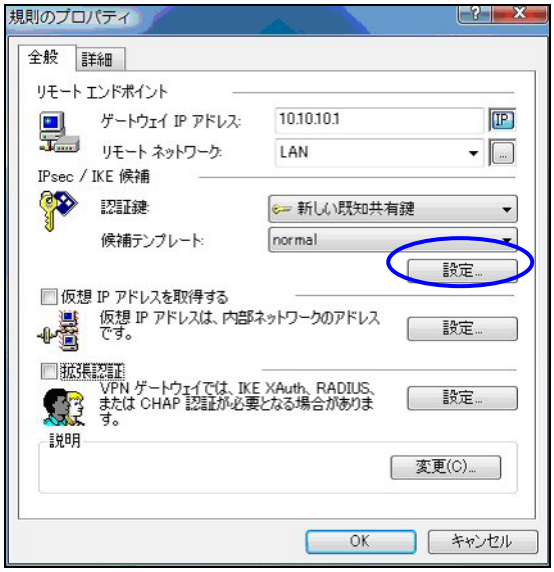


「ネットワークエディタ」画面が開きます。
「ネットワーク名」は任意の名前を設定することができます。
「IP アドレス」「サブネットマスク」は XR に接続している LAN について設定し（ここでは LAN[センター側のネットワーク]の値を設定しています)、「OK」をクリックします。

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。

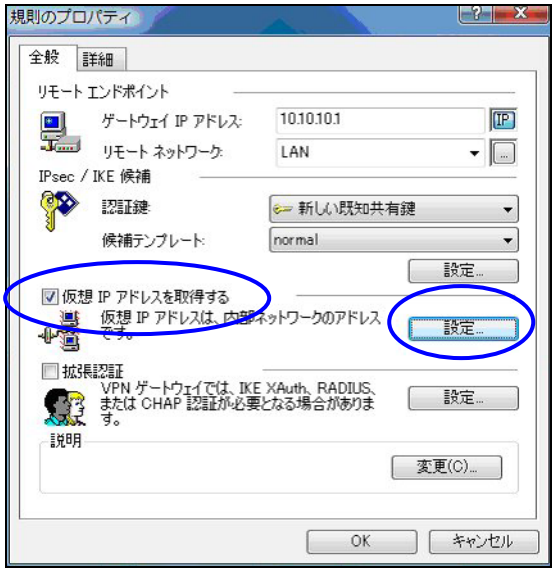


既知共有鍵のローカル ID は IKE アグレッシブモードでのみ利用可能なため、「IKE モードをアグレッシブモードに変更しますか？」と表示されますので、「はい」をクリックします。



「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 モードが「main　mode」になっている場合は、「aggressive mode」に変更します。また「選択した値のみを候補に加える」にチェックして下さい。
「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。



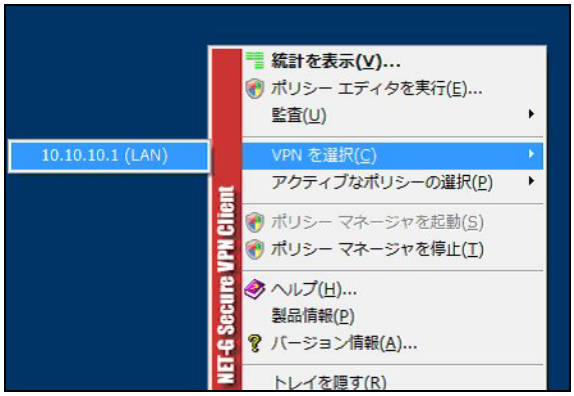
続いて「仮想 IP アドレスを取得する」にチェックを入れ、「設定」ボタンをクリックします。

「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 VPN クライアントの仮想的な 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 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。）
「OK」ボタンをクリックして「規則のプロパティ」画面に戻り、「規則のプロパティ」画面で「OK」ボタンをクリックして「VPN 接続を追加」画面に戻り、「OK」ボタンをクリックしてポリシーエディタに戻ります。

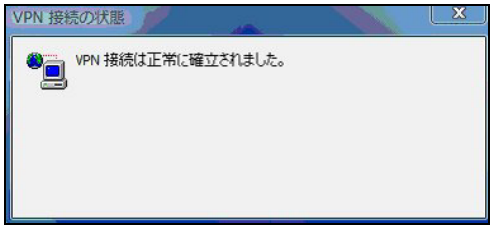
「適用」をクリックし、これで設定は完了です。

続いて IPsec 接続を行います。



タスクバーの中にある VPN Client/NET-G 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。

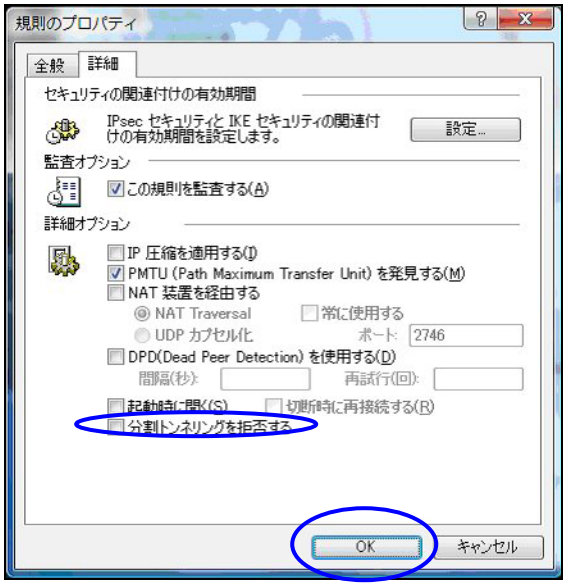


IPsec が正常に確立した場合、「VPN 接続は正常に確立しました」という画面が表示されます。

これで IPsec 接続は完了です。

1-2-3. VPN クライアントでの IPsec 通信と Internet 通信の同時に利用について

この設定例では、IPsec 接続時の Internet への通信は拒否になっています。
IPsec 接続時に IPsec 通信と Internet 通信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.　基本設定例２　～仮想 IP アドレスを使用しない設定～

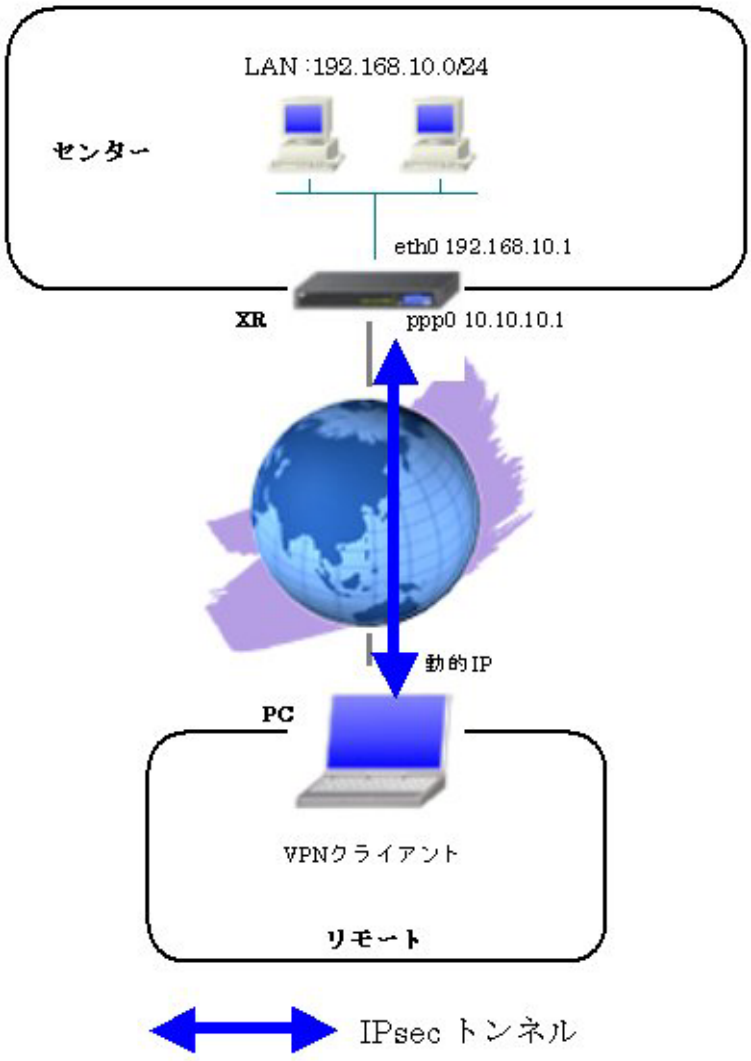
基本設定例１では、VPN クライアント側では IPsec 接続時に使われる「仮想 IP アドレス」を設定しました。このとき XR 側の LAN からは、VPN クライアントに設定した「仮想 IP アドレス」に対して IPsec 経由での通信をおこないます。

この設定以外に、「仮想 IP アドレス」を使わずに、VPN クライアントと XR を IPsec 接続することもできます。

「仮想 IP アドレス」を使わないときは、XR 側の LAN からは、VPN クライアントが動作しているホスト自身が持つ IP アドレスに対して IPsec 通信をおこないます。

なお下記設定例は、基本設定例１からの差分のみ記載しておりますので、その他の設定に関しましては、基本設定例１をご参照下さい。

2-1.　構成例



2-2.　設定例

2-2-1.　センタールータ（XR）

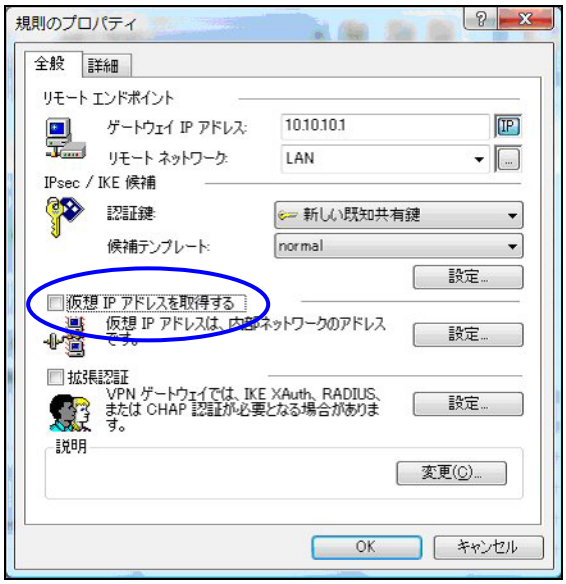
ポイント

IPsec 設定の「IPsec ポリシー」にある「相手側の LAN 側のネットワークアドレス」について、この項目を"空欄"に設定します。

2-2-2.　VPN クライアント（PC）

ポイント

「規則のプロパティ」画面の「仮想 IP アドレスを取得する」にチェックを入れずに設定します。

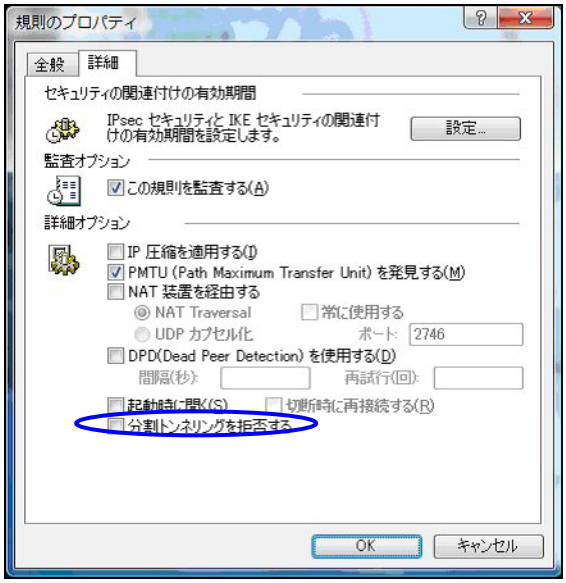


〈この設定での注意点〉
VPN クライアント側が動的 IP 側の場合、IPsec 接続中に VPN クライアント側の IP アドレスが何らかの理由で変わってしまうと、一時的に通信できない状態となります。もしこのような状況になったときは、XR 側が保持している IPsec SA が無効となるまで再接続できません。
XR が保持する IPsec SA が無効になるのは以下の場合です。

- XR の IPsecKeep-Alive 機能により、IPsecSA を削除したとき
- IPsec SA のライフタイムが経過したとき
- 削除ペイロードを受信したとき
- XR 側を再起動したとき

2-2-3. VPN クライアントでの IPsec 通信と Internet 通信の同時に利用について

なおこの設定例では、IPsec 接続時の Internet への通信は拒否になっています。
IPsec 接続に IPsec 通信と Internet 通信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。
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。



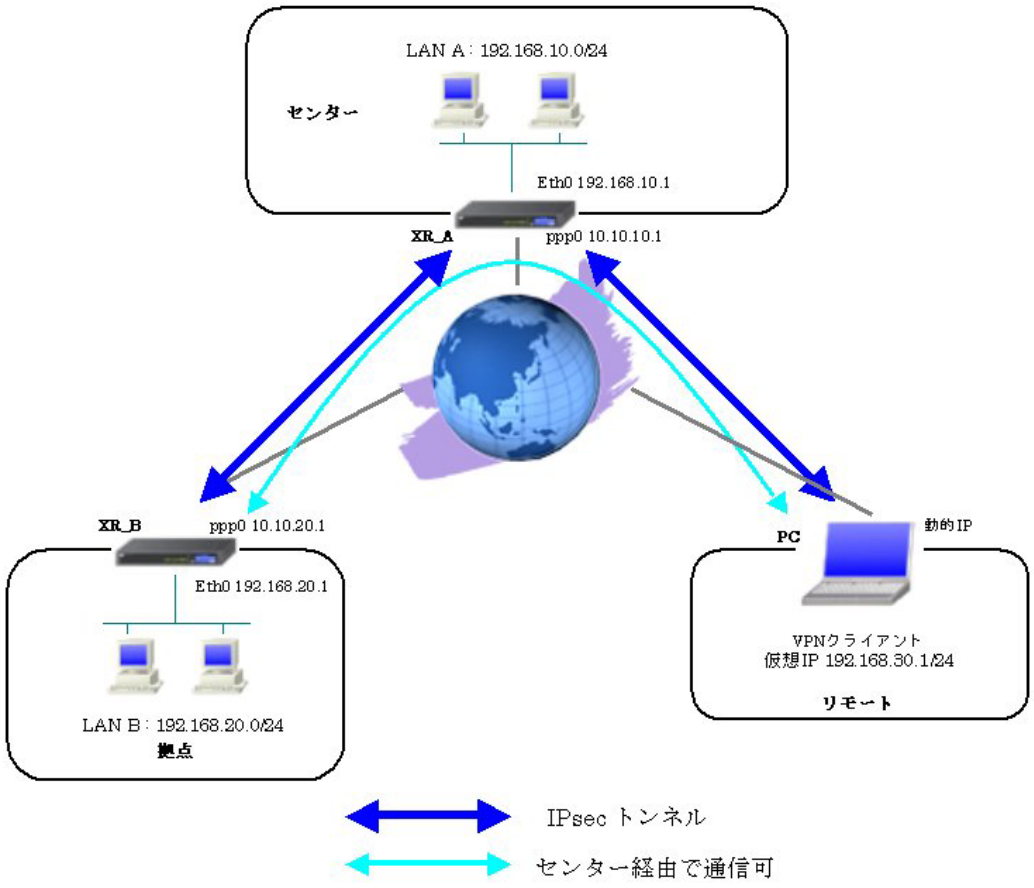
「規則のプロパティ」画面を開き、「詳細タブ」をクリックします。ここで詳細オプションにある「分割トンネリングを拒否する」のチェックボックスのチェックを外します。

3. センター経由での IPsec 通信設定例

VPN クライアントは、センター側 XR と IPsec 接続を行い、センター経由で拠点側 LAN へもアクセスします。

本設定例では、XR に関しましては IPsec 設定に関してのみ記載しております。IPsec 設定以外の設定に関しましては、インターネット VPN 設定例集 IPsec 編の「IPsec を利用したセンター経由インターネット接続例」をご参照下さい。

3-1. 構成例



3-2. 設定例

3-2-1. センタールータ（XR_A）

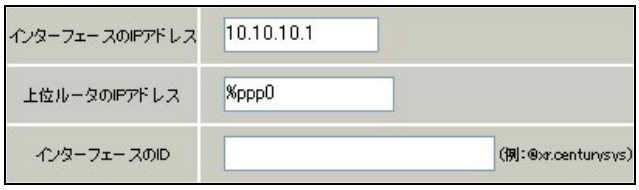
ポイント

XR_B(拠点)およびリモートの PC と IPsec 接続するための設定を行います。
XR_B(拠点)およびリモートの PC は動的 IP のため、IKE モードとしてアグレッシブモードを使用しています。

<<各種サービスの設定>>

<IPsec サーバ>

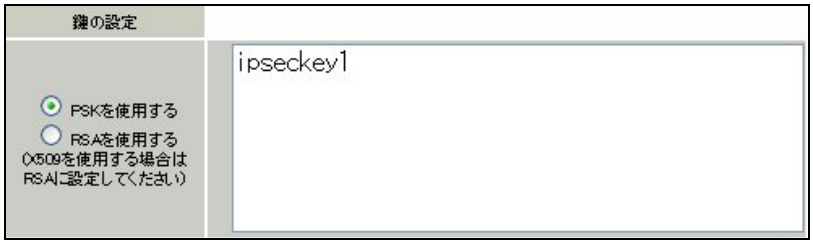
[本装置側の設定 1]



XR 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。



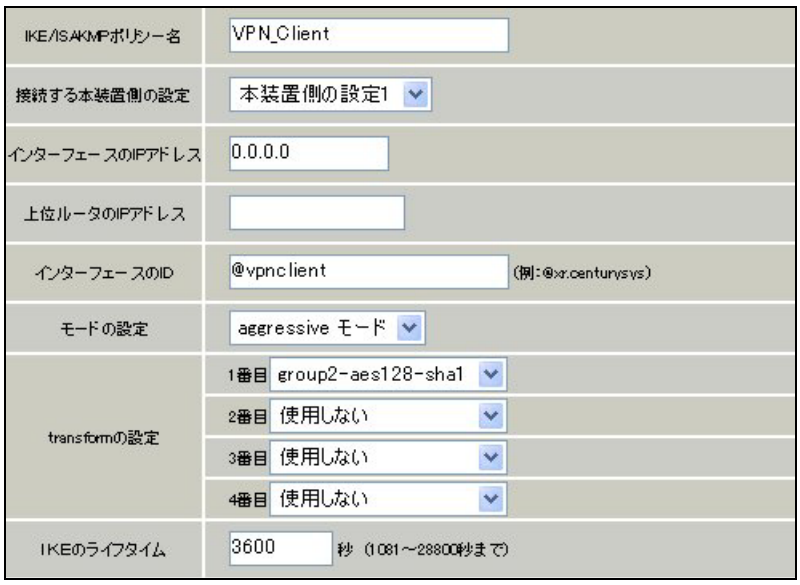
事前共有鍵(PSK)として「ipseckey1」を設定しています。

[IPsec ポリシーの設定 1]

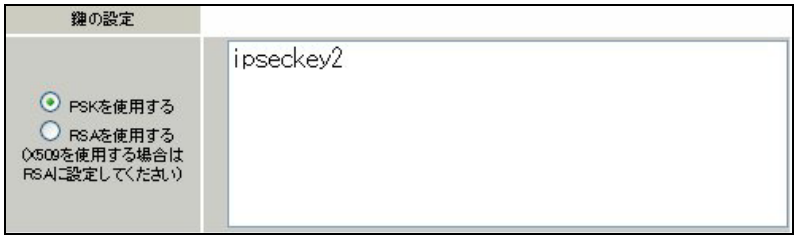
XR_B(拠点)の IP アドレスが不定のため、「Responder として使用する」を選択します。

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ます。

[IKE/ISAKMP の設定 2]



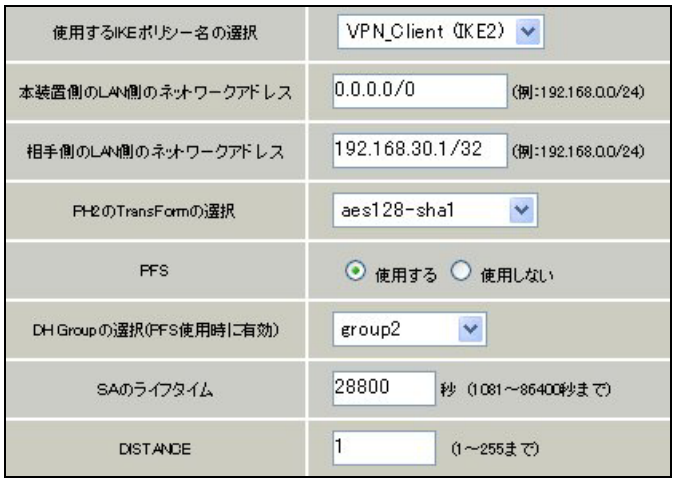
VPN クライアントに対する IKE/ISAKMP ポリシーを設定します。
XR における ID の設定では”@”を付けますが、VPN Client/NET-G 側では、”@”を付けない形式で設定してください。VPN Client/NET-G でも”@”を付けて設定すると接続できません。



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]

VPN クライアントの 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。



VPN クライアントに対して IPsec 通信を行う IP アドレスの範囲を設定します。
ここで設定したアドレスと同じ値を、VPN Client/NET-G の「仮想 IP アドレスを取得する」項目で設定します。ただし XR の設定では必ず”<IP address>/32”の形式で設定します。”<IP address>/24”の設定では接続できませんのでご注意ください。

【IPsec サーバ】

IPsec サーバ機能を起動します。

3-2-2. 拠点ルータ（XR_B）

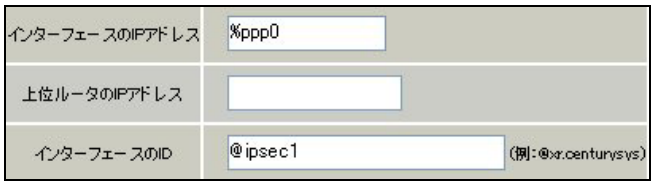
ポイント

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、IKE モードとしてアグレッシブモードを使用しています。

<<各種サービスの設定>>

<IPsec サーバ>

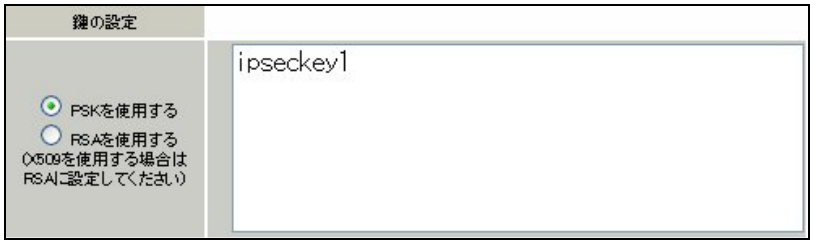
[本装置側の設定 1]



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 ISAKMP ポリシーの設定を行います。



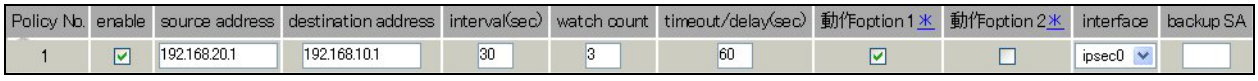
事前共有鍵(PSK)として「ipseckey1」を設定します。

[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】

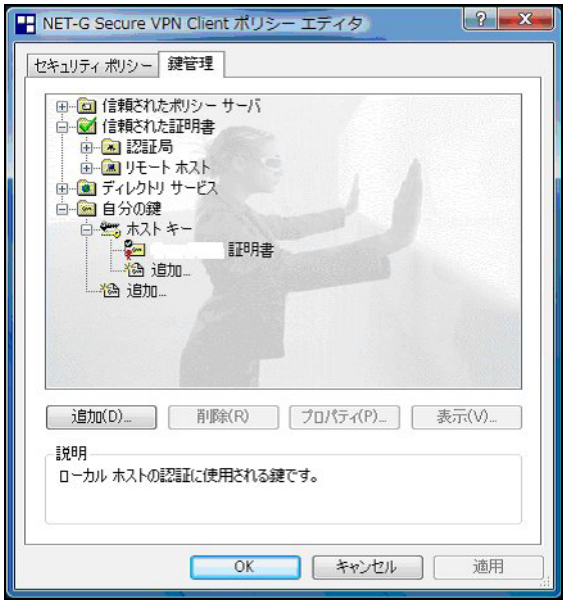
IPsec サーバ機能を起動します。

3-2-3. VPN クライアント（PC）

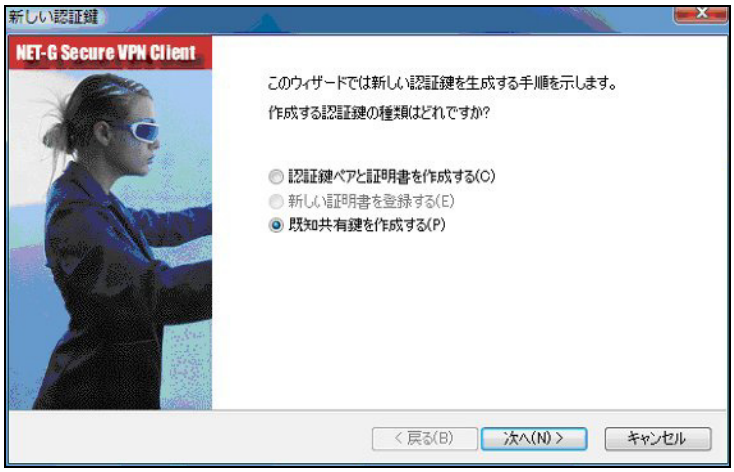
ポイント

XR_A(センター)に対して IPsec 接続を行います。
XR_A(センター)経由で拠点とも通信するため、リモートネットワークで「any」を設定しています。

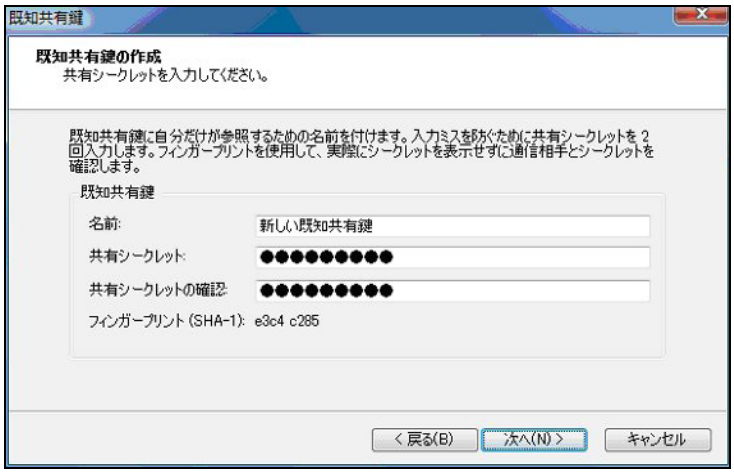
<<既知共有鍵(Pre shared Key)の設定>>



「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。

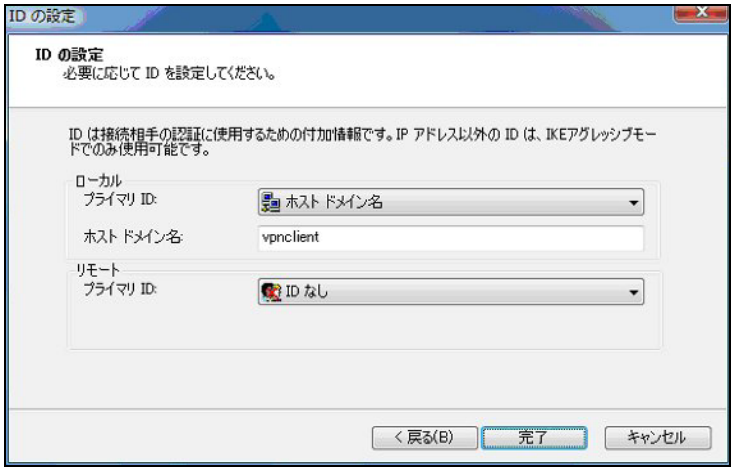


「新しい認証鍵」ウィンドウが開きますので、「既知共有鍵を作成する」を選択し、「次へ」ボタンをクリックして下さい。

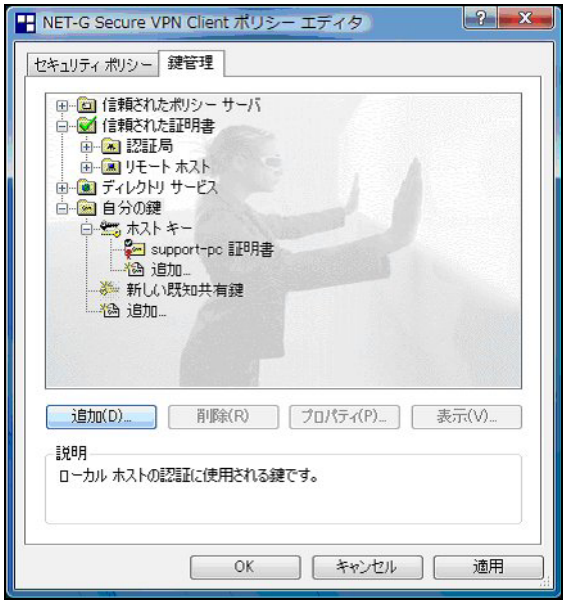


「既知共有鍵の作成」画面が開きます。ここで既知共有鍵（PSK）を作成します。「名前」には任意の設定名を入力します。「共有シークレット」「共有シークレットの確認」項目には既知共有鍵を入力し、「次へ」ボタンをクリックします。
このとき入力した鍵は“＊”,“●”等で表示されます。
この例では共有シークレットとして「ipseckey2」を設定しています。

<<ID の設定>>



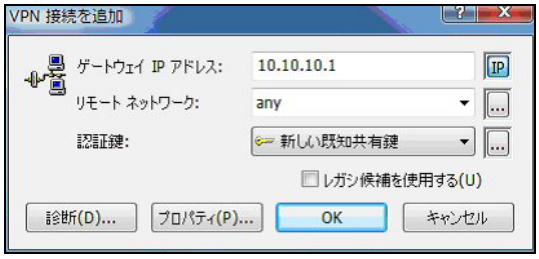
既知共有鍵の作成後、「ID の設定」画面で、「ローカル」側項目について、プライマリ ID は「ホストドメイン名」を選択し、ホストドメイン名に ID を入力します。ここには XR シリーズの IPsec サーバ「IKE/ISAKMP の設定」における「インタフェース ID」と同じ ID を設定します。
※ただしこの時、ホストドメイン名には”@”をつけないで設定して下さい。
「完了」ボタンをクリックすると「鍵管理」画面に戻ります。



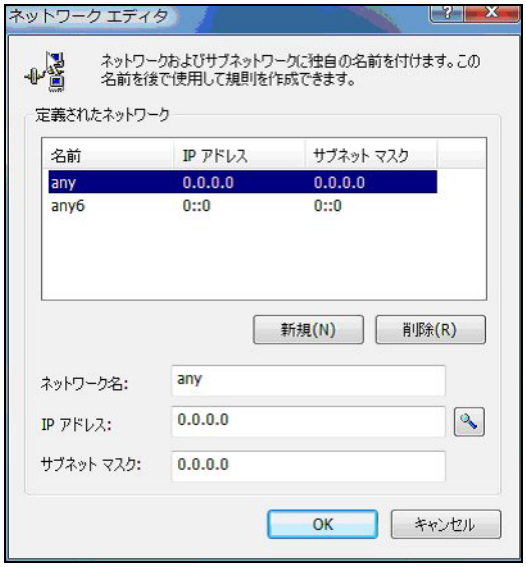
ここまでの設定が終わったら、必ず「適用」ボタンをクリックして下さい。「適用」ボタンをクリックしないと適切に設定されない場合があります。

<<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。

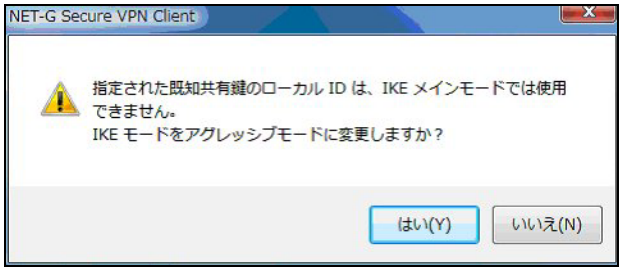


「VPN 接続を追加」画面が開きます。「ゲートウェイ IP アドレス」で右端の”IP”をクリックし、XR の WAN 側 IP アドレスを設定します。
「認証鍵」は、既知共有鍵の設定で登録した既知共有鍵の設定名を選択します。
「リモートネットワーク」については右端にある”・・・”をクリックして下さい。



「ネットワークエディタ」画面が開きます。
デフォルトで登録されている「any」を選択し、「OK」をクリックします。

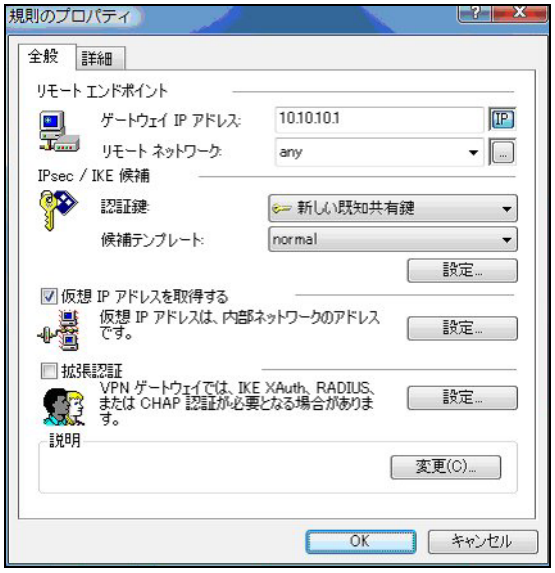
リモートネットワーク設定後、「VPN 接続を追加」画面が開きますので、続いてプロパティをクリックします。



既知共有鍵のローカル ID は IKE アグレッシブモードでのみ利用可能なため、「IKE モードをアグレッシブモードに変更しますか？」と表示されますので、「はい」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 モードが「main mode」になっている場合は、「aggressive mode」に変更します。また「選択した値のみを候補に加える」にチェックして下さい。
「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。

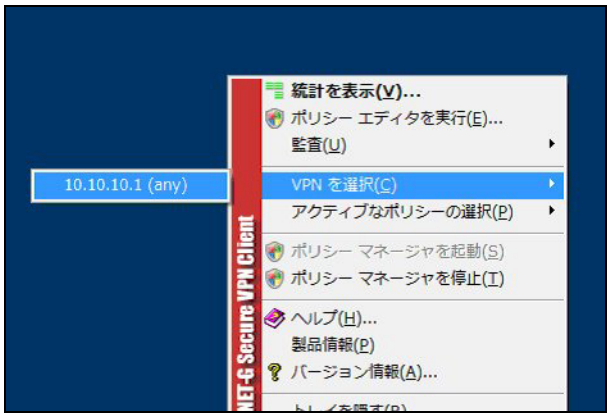


続いて「仮想 IP アドレスを取得する」にチェックを入れ、「設定」ボタンをクリックします。

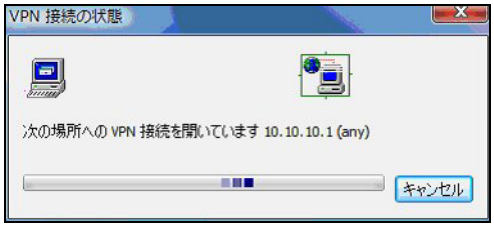
「仮想 IP アドレス」画面が開きます。
ここでは XR に接続する際に使用するこの PC の仮想的な IP アドレスを設定します。
「プロトコル」は”手動で指定”を選択し、任意のプライベート IP アドレスとサブネットマスクを入力します。ここで設定する IP アドレスは XR の IPsec サーバにおける「IPsec ポリシーの設定」の”相手側の LAN 側のネットワークアドレス”と一致させます。この例では、サブネットマスクは 24 ビットマスクとしています。
※XR_A の IPsec ポリシーで設定したサブネットと異なるので注意して下さい。
（32 ビットマスクは設定することができませ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

「適用」をクリックし、これで設定は完了です。

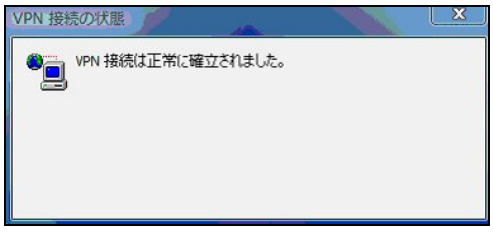
続いて IPsec 接続を行います。



タスクバーの中にある FutureNet VPN Client/NET-G 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。



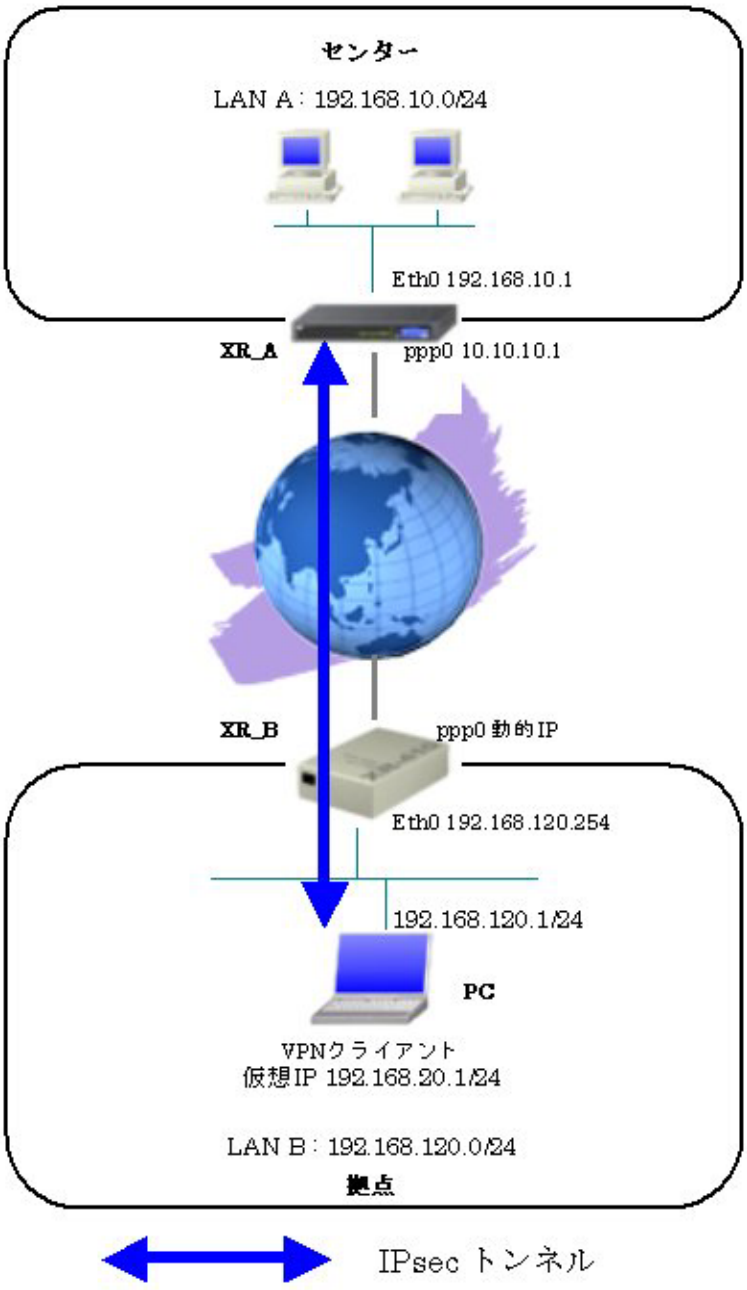
IPsec が正常に確立した場合、「VPN 接続は正常に確立しました」という画面が表示されます。

これで IPsec 接続は完了です。

4. IPsec NAT-Traversal 設定例

この設定例は、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 接続を行う VPN クライアントが存在する構成です。

4-1. 構成例



4-2. 設定例

4-2-1. センタールータ（XR_A）

ポイント

VPN クライアントをインストールしている PC(拠点)と IPsec NAT-Traversal で接続するための設定を行います。

IPsec の IKE モードはアグレッシブモードを使用します。

センタールータ（XR_A）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。

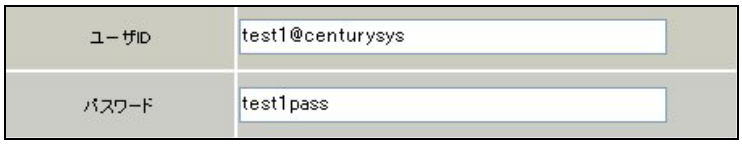
[Ethernet1 の設定]

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) ○Leased Line(64K) ○Leased Line(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、XR 配下の端末からの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	ICMP type/code	送信元MACアドレス	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。

<<各種サービスの設定>>

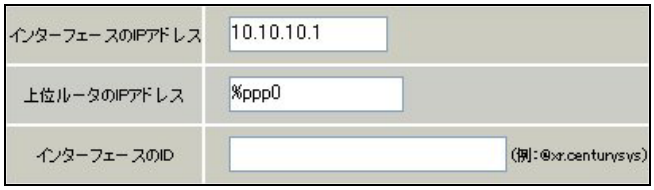
<IPsec サーバ>

[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 を使用する VPN クライアントの IP アドレスを設定します。

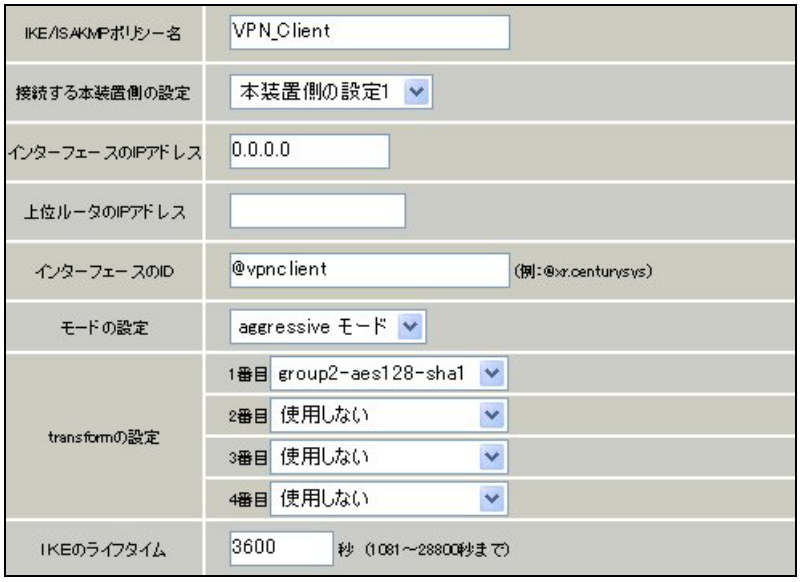
[本装置側の設定 1]



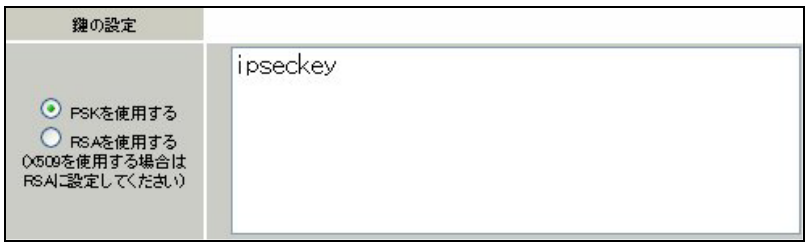
XR_A(センター)の WAN 側インタフェースの IP アドレス,および上位ルータの IP アドレスを設定します。

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]



VPN クライアントに対する IKE/ISAKMP ポリシーを設定します。



事前共有鍵(PSK)として「ipseckey」を設定しています。

[IPsec ポリシーの設定 1]

VPN クライアントの 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。

VPN クライアントに対して 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】

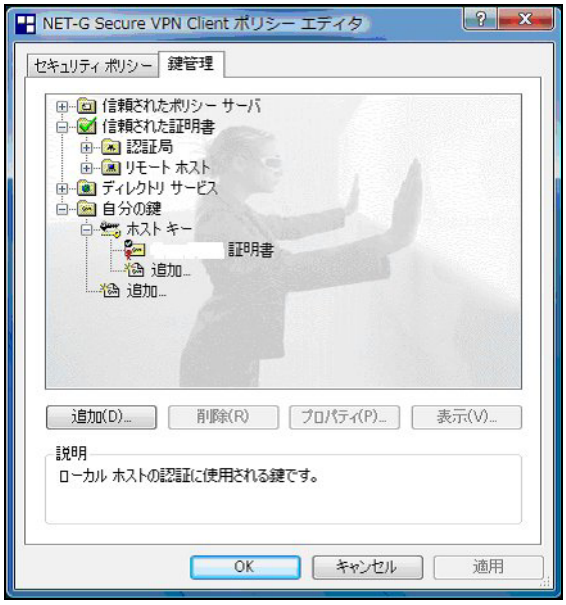
IPsec サーバ機能を起動します。

4-2-2. VPN クライアント（拠点 PC）

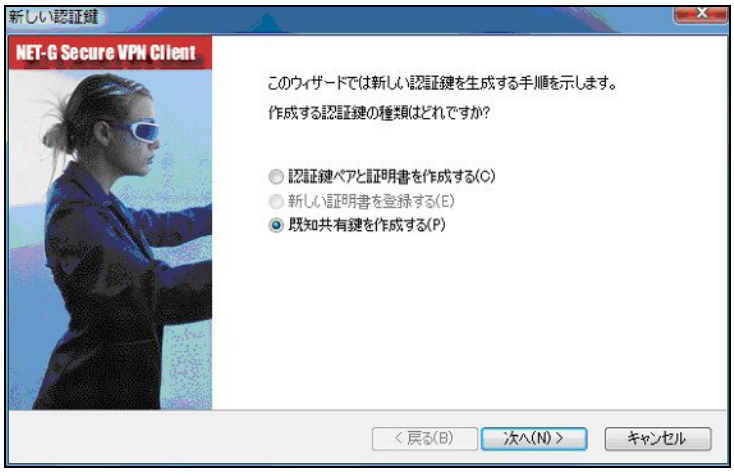
ポイント

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。

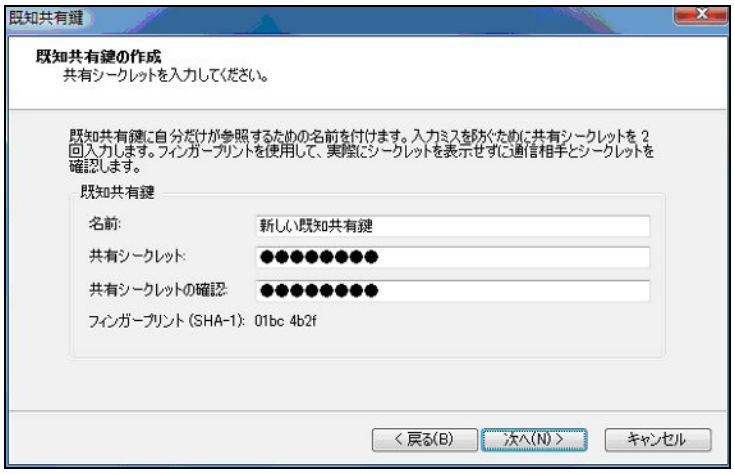
<<既知共有鍵(Pre shared Key)の設定>>



「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。

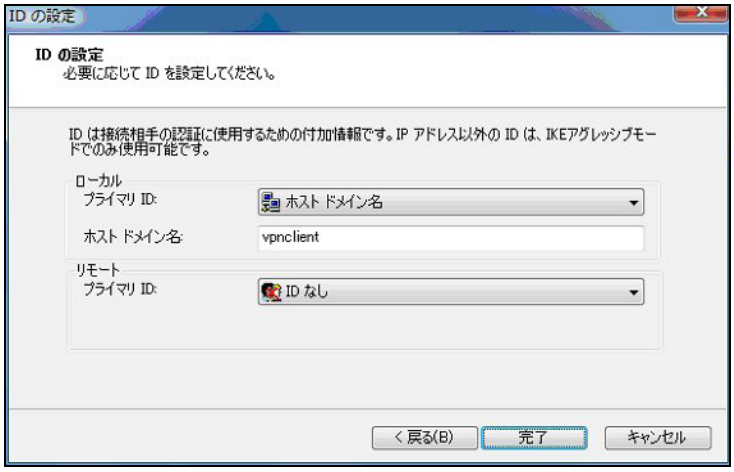


「新しい認証鍵」ウィンドウが開きますので、「既知共有鍵を作成する」を選択し、「次へ」ボタンをクリックして下さい。

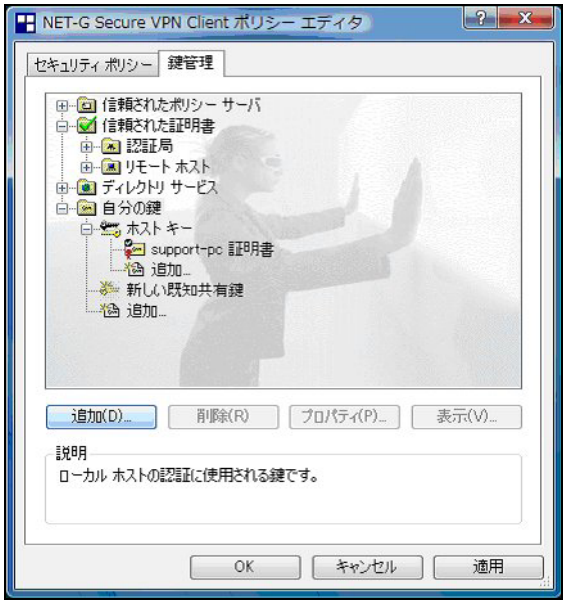


「既知共有鍵の作成」画面が開きます。ここで既知共有鍵（PSK）を作成します。「名前」には任意の設定名を入力します。「共有シークレット」「共有シークレットの確認」項目には既知共有鍵を入力し、「次へ」ボタンをクリックします。
このとき入力した鍵は“＊”,“●”等で表示されます。
この例では共有シークレットとして「ipseckey」を設定しています。

<<ID の設定>>



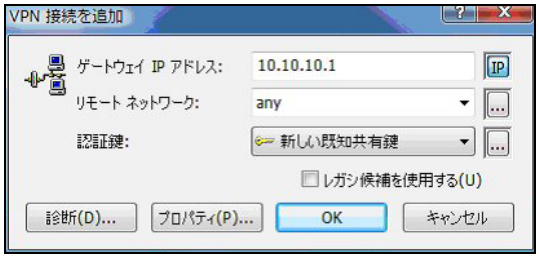
既知共有鍵の作成後、「ID の設定」画面で、「ローカル」側項目について、プライマリ ID は「ホストドメイン名」を選択し、ホストドメイン名に ID を入力します。ここには XR シリーズの IPsec サーバ「IKE/ISAKMP の設定」における「インタフェース ID」と同じ ID を設定します。
※ただしこの時、ホストドメイン名には”@”をつけないで設定して下さい。
「完了」ボタンをクリックすると「鍵管理」画面に戻ります。



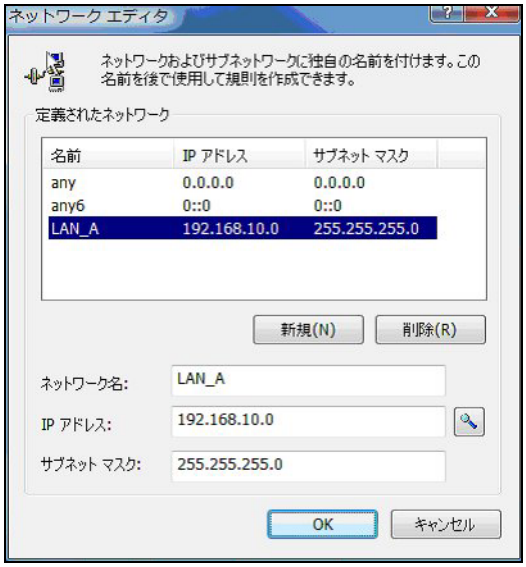
ここまでの設定が終わったら、必ず「適用」ボタンをクリックして下さい。「適用」ボタンをクリックしないと適切に設定されない場合があります。

<<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。

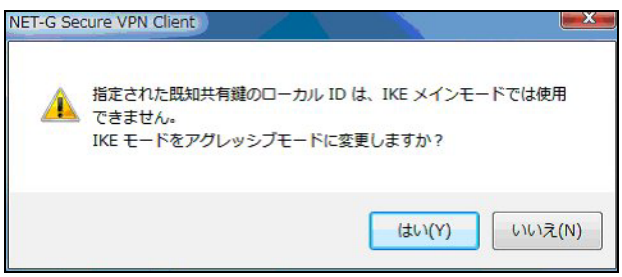


「VPN 接続を追加」画面が開きます。「ゲートウェイ IP アドレス」で右端の”IP”をクリックし、XR の WAN 側 IP アドレスを設定します。
「認証鍵」は、既知共有鍵の設定で登録した既知共有鍵の設定名を選択します。
「リモートネットワーク」については右端にある”・・・”をクリックして下さい。

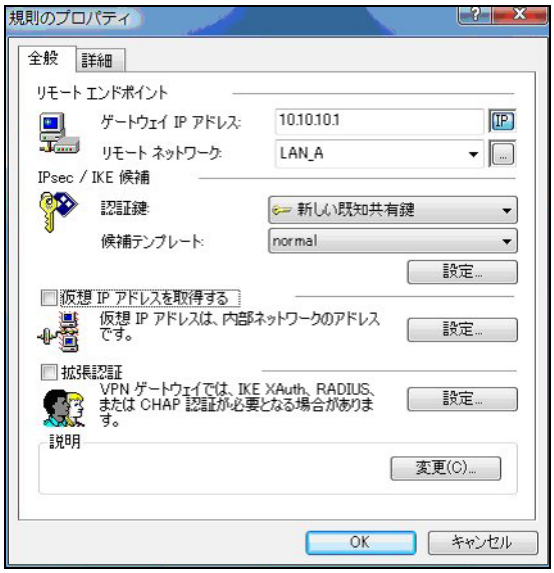


「ネットワークエディタ」画面が開きます。
「ネットワーク名」は任意の名前を設定することができます。
「IP アドレス」「サブネットマスク」は XR に接続している LAN について設定し（ここでは LAN[センター側のネットワーク]の値を設定しています)、「OK」をクリックします。

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。

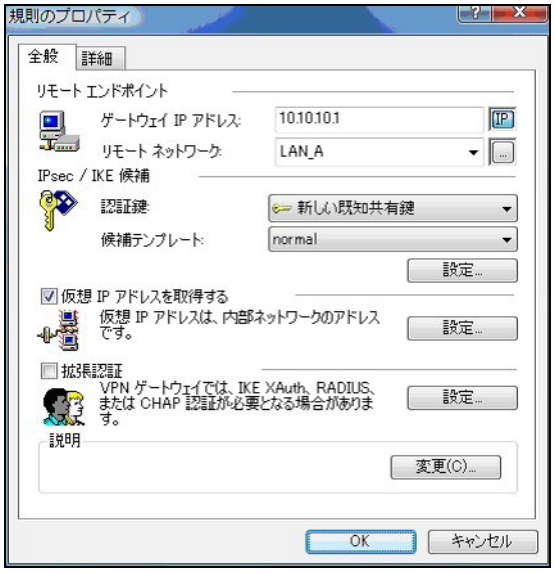


既知共有鍵のローカル ID は IKE アグレッシブモードでのみ利用可能なため、「IKE モードをアグレッシブモードに変更しますか？」と表示されますので、「はい」をクリックします。

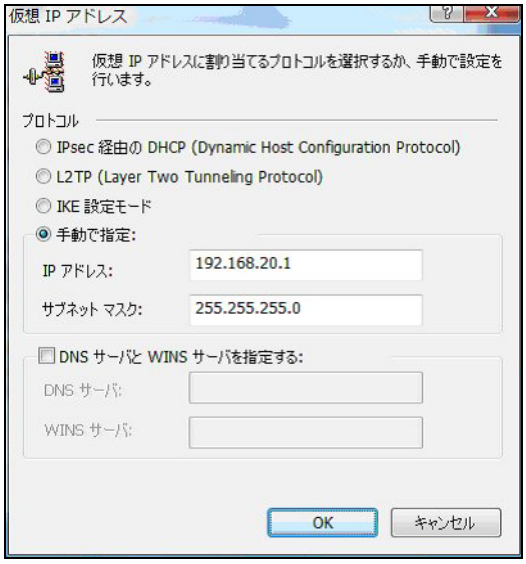


「規則のプロパティ」画面が開きます。ここで IPsec/IKE 候補の
設定ボタンをクリックします。

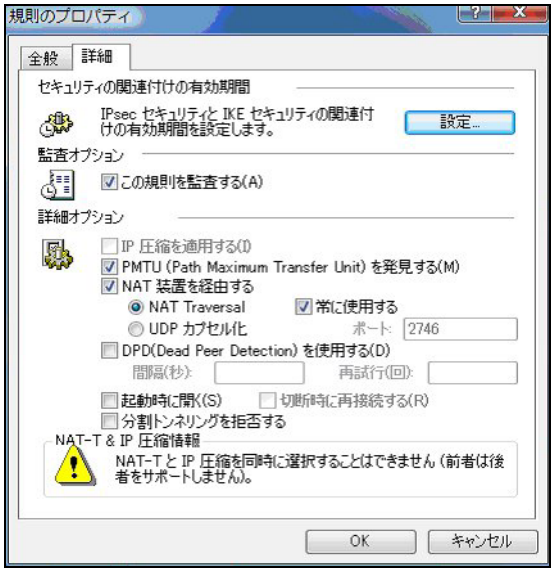
「パラメータ候補画面」が開きます。ここで暗号化方式などを設定します。IKE モードが「main mode」になっている場合は、「aggressive mode」に変更します。また「選択した値のみを候補に加える」にチェックして下さい。
「OK」ボタンをクリックして「規則のプロパティ」画面に戻ります。



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。



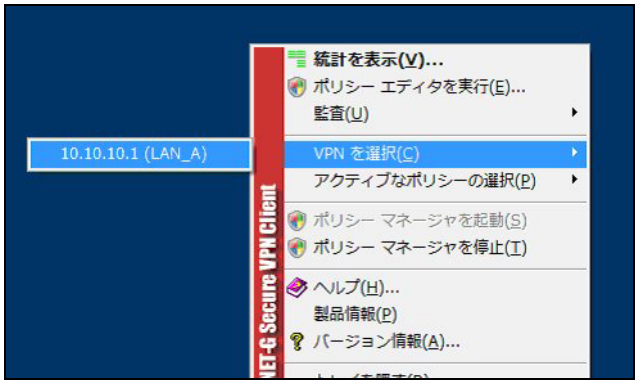
「仮想 IP アドレス」画面が開きます。
ここでは XR に接続する際に使用するこの PC の仮想的な IP アドレスを設定します。
「プロトコル」は”手動で指定”を選択し、任意のプライベート IP アドレスとサブネットマスクを入力します。ここで設定する IP アドレスは XR の IPsec サーバにおける Virtual Private 設定と一致させます。
この例では、サブネットマスクは 24 ビットマスクとしています。
※XR_A の Virtual Private 設定で設定したサブネットと異なるので注意して下さい。
（32 ビットマスクは設定することができません。）
「OK」ボタンをクリックして「規則のプロパティ」画面に戻り、「詳細タブ」をクリックします。



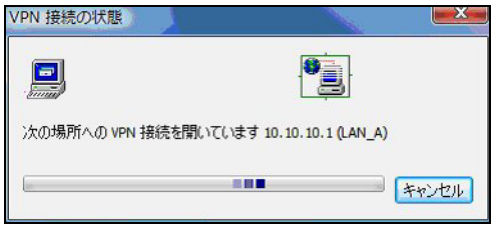
ここで詳細オプションにある「NAT 装置を経由する」のチェックボックスを有効にし、「NAT-T(Network Address Translation Traversal)」を選択し、「常に使用する」にチェックを入れます。
「OK」ボタンをクリックしてポリシーエディタに戻ります。

「適用」をクリックし、これで設定は完了です。

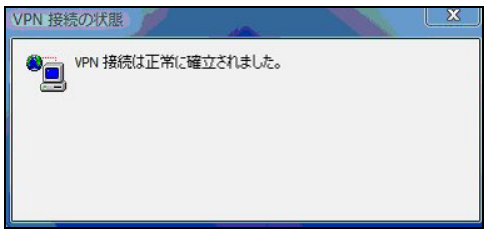
続いて IPsec 接続を行います。



タスクバーの中にある FutureNet VPN Client/NET-G 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。

4-2-3. 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

4-2-4. 複数の VPN クライアント接続時の注意事項

NAT ルータ配下の複数の VPN クライアントから同時に IPsec 接続する場合は、それぞれの VPN クライアントに重複しない ID, 仮想 IP アドレスを設定して下さい。
XR 側では、インタフェース ID 毎に IKE/ISAKMP ポリシー設定・IPsec ポリシー設定を追加して下さい。

4-2-5. 異なる複数の LAN からの VPN クライアント接続時の注意事項

複数の異なる LAN 内にある VPN クライアントから IPsec 接続する場合は、XR の「Virtual Private 設定」を次のように設定します。

Ex.）%v4:192.168.10.0/24,%v4:192.168.20.0/24,%v4:192.168.30.0/24

LAN 毎の Virtual Private 設定を“カンマ”で区切り設定します。

また機種・ファームウェアのバージョンによっては、GUI 上で最大４つまで Virtual Private 設定ができるようになっています。

5. VPN クライアントのログについて

VPN クライアントでは、IPsec 接続時のログを取得することが可能です。
これにより IPsec が確立できない場合もログを確認することによりある程度の原因追及が可能です。
ログを取得するためには、VPN Client/NET-G のメインメニューから「監査」->「IKE ログウィンドウを表示」を選択します。
※詳細は、VPN クライアントのユーザーマニュアルをご参照下さい。
表示される情報量は、選択したレベルにより異なります。
ここでは、IPsec に関する主なログについて説明します。なお表示されているログのレベルは「Low」になっております。

5-1. 正常に IPsec 接続できた場合のログ表示例

DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <-> 10.10.10.1:500 { fed2b9f8 c413f515 - 2b657cb2 40b8c650 [-1] / 0x00000000 } Aggr; MESSAGE: Phase 1 version = 1.0, auth_method = Pre shared keys, cipher = aes-cbc, hash = sha1, prf = hmac-sha1, life = 0 kB / 14400 sec, key len = 128, group = 2

Auth: Info: Phase-1 [initiator] between fqdn(udp:500,[0..8]=vpnclient) and ipv4(any:0,[0..3]=10.10.10.1) done.

DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <-> 10.10.10.1:500 { fed2b9f8 c413f515 - 2b657cb2 40b8c650 [0] / 0x964d311a } QM; MESSAGE: Phase 2 connection succeeded, Using PFS, group = 2

DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <-> 10.10.10.1:500 { fed2b9f8 c413f515 - 2b657cb2 40b8c650 [0] / 0x964d311a } QM; MESSAGE: SA[0][0] = ESP aes, life = 409600 kB/3600 sec, group = 2, tunnel, hmac-sha1-96, key len = 128, key rounds = 0

Auth: Info: Phase-2 [initiator] done bundle 4 with 2 SA's by rule 119:`ipsec ipv4(any:0,[0..3]=192.168.20.1)<->ipv4_subnet(any:0,[0..7]=192.168.10.0/24)(gw:ipv4(any:0,[0..3]=10.10.10.1))'

Auth: Info: SA ESP[6bc0e300] alg [aes-cbc/16]+hmac[hmac-sha1-96] bundle [4,0] pri 0 opts src=ipv4(any:0,[0..3]=192.168.20.1) dst=ipv4_subnet(any:0,[0..7]=192.168.10.0/24)

Auth: Info: SA ESP[29d3ba2f] alg [aes-cbc/16]+hmac[hmac-sha1-96] bundle [4,0] pri 0 opts src=ipv4_subnet(any:0,[0..7]=192.168.10.0/24) dst=ipv4(any:0,[0..3]=192.168.20.1)

5-2. 正常に IPsec NAT-Traversal 接続できた場合のログ表示例

Security: Info: The remote server at 10.10.10.1:500 is 'draft-ietf-ipsec-nat-t-ike-03'

DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <-> 10.10.10.1:4500 { 296edd29 ba64a7f8 - 849ef7c3 95f8f38e [-1] / 0x00000000 } Aggr; MESSAGE: Phase 1 version = 1.0, auth_method = Pre shared keys, cipher = aes-cbc, hash = sha1, prf = hmac-sha1, life = 0 kB / 14400 sec, key len = 128, group = 2

Auth: Info: Phase-1 [initiator] between fqdn(udp:500,[0..8]=vpnclient) and ipv4(any:0,[0..3]=10.10.10.1) done.

DEBUG: unknown (unknown) <-> unknown { unknown [unknown] / unknown } unknown; Packet to unknown Isakmp SA, ip = 10.10.10.1:500

DEBUG: *** SSH_IPADDR_ANY ***:4500 (Initiator) <-> 10.10.10.1:4500 { 296edd29 ba64a7f8 - 849ef7c3 95f8f38e [0] / 0x1085ae8e } QM; MESSAGE: Phase 2 connection succeeded, Using PFS, group = 2

DEBUG: *** SSH_IPADDR_ANY ***:4500 (Initiator) <-> 10.10.10.1:4500 { 296edd29 ba64a7f8 - 849ef7c3 95f8f38e [0] / 0x1085ae8e } QM; MESSAGE: SA[0][0] = ESP aes, life = 409600 kB/3600 sec, group = 2, udp-tunnel, hmac-sha1-96, key len = 128, key rounds = 0

Auth: Info: Phase-2 [initiator] done bundle 1 with 2 SA's by rule 20:`ipsec ipv4(any:0,[0..3]=192.168.20.1)<->ipv4_subnet(any:0,[0..7]=192.168.10.0/24)(gw:ipv4(any:0,[0..3]=10.10.10.1))'

Auth: Info: SA ESP[c1337433] alg [aes-cbc/16]+hmac[hmac-sha1-96] bundle [1,0] pri 0 opts udpencap src=ipv4(any:0,[0..3]=192.168.20.1) dst=ipv4_subnet(any:0,[0..7]=192.168.10.0/24)

Auth: Info: SA ESP[fb8a9608] alg [aes-cbc/16]+hmac[hmac-sha1-96] bundle [1,0] pri 0 opts udpencap src=ipv4_subnet(any:0,[0..7]=192.168.10.0/24) dst=ipv4(any:0,[0..3]=192.168.20.1)

5-3. IKE フェーズ１の確立に失敗した場合のログ表示例１

DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <-> 10.10.10.1:500 { b8906bb2 8239f108 - 00000000 00000000 [-1] / 0x00000000 } Aggr; Connection timed out or error, calling callback
Auth: Info: Phase-1 [initiator] between fqdn(udp:500,[0..7]=vpnclien) and ipv4(udp:500,[0..3]=10.10.10.1) failed; Timeout.

このログは IKE フェーズ１のネゴシエーションで IPsec ゲートウェイの IP アドレス，インタフェース ID，モード等が異なる場合に表示されるログの例になります。

解決策
ご利用頂いている環境で以下の設定項目をご確認下さい。

IPsec ゲートウェイの IP アドレス
VPN クライアント側：「セキュリティポリシー」->「規則のプロパティ」->「ゲートウェイ IP アドレス」
XR 側：「本装置の設定」->「インタフェースの IP アドレス」

インタフェース ID
VPN クライアント側：「既知共有鍵」->「ID」のホストドメイン名
XR 側：「IKE/ISAKMP ポリシー設定」->「インタフェース ID」

モード間違い
VPN クライアント側：「セキュリティポリシー」->「規則のプロパティ」->「IKE/IPsec 候補の設定（パラメータ候補)」->「IKE モード」
XR 側：「IKE/ISAKMP ポリシー設定」->「モードの設定」

5-4. IKE フェーズ１の確立に失敗した場合のログ表示例２

DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <-> 10.10.10.1:500 { 876a10d8 dec0d6be - 95e70656 be42b39d [-1] / 0x00000000 } Aggr; Hash value mismatch
Auth: Info: Phase-1 [initiator] between fqdn(udp:500,[0..8]=vpnclient) and ipv4(udp:500,[0..3]=10.10.10.1) failed; Authentication failed.
DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <-> 10.10.10.1:500 { 876a10d8 dec0d6be - 95e70656 be42b39d [-1] / 0x00000000 } Aggr; Error = Authentication failed (24)

このログは IKE フェーズ１のネゴシエーションで事前共有鍵（Pre Shared Key）が異なる場合に表示されるログの例になります。

解決策
ご利用頂いている環境で以下の設定項目をご確認下さい。

VPN クライアント側：「既知共有鍵」->「共有シークレット」
XR 側：「IKE/ISAKMP ポリシー設定」->「鍵の設定（PSK を使用する）」※aggressive モードの場合は、事前共有鍵（Pre Shared Key）方式のみ使用可能です。

5-5. IKE フェーズ２の確立に失敗した場合のログ表示例

DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <-> 10.10.10.1:500 { eaa2115e d020b582 - 1098cb16 2318cefe [-1] / 0x00000000 } Aggr; MESSAGE: Phase 1 version = 1.0, auth_method = Pre shared keys, cipher = aes-cbc, hash = sha1, prf = hmac-sha1, life = 0 kB / 14400 sec, key len = 128, group = 2

Auth: Info: Phase-1 [initiator] between fqdn(udp:500,[0..8]=vpnclient) and ipv4(any:0,[0..3]=10.10.10.1) done.

DEBUG: *** SSH_IPADDR_ANY ***:500 (Responder) <-> 10.10.10.1:500 { eaa2115e d020b582 - 1098cb16 2318cefe [1] / 0x23e64fd1 } Info; Received notify err = Invalid ID information (18) to isakmp sa, delete it

Auth: Info: Phase-2 [initiator] for ipv4(icmp:0,[0..3]=192.168.20.2) and ipv4(icmp:0,[0..3]=192.168.10.1) failed; Aborted notification.

このログは IKE フェーズ２のネゴシエーションで失敗している場合に表示されるログの例になります。

解決策
ご利用頂いている環境で以下の設定項目をご確認下さい。

VPN クライアント側：「セキュリティポリシー」->「規則のプロパティ」->「仮想 IP アドレスを取得する」-> 「仮想 IP アドレス」
XR 側：「IPsec ポリシー設定」->「本装置側の LAN 側のネットワークアドレス」,「相手側の LAN 側のネットワークアドレス」

6. サポートデスクへのお問い合わせ

6-1. サポートデスクへのお問い合わせに関して

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

- ご利用頂いている FutureNet VPN Client/NET-G のバージョン番号
- ご利用頂いている FutureNet VPN Client/NET-G を含んだネットワーク構成
- 不具合の内容および不具合の再現手順（何を行った場合にどのような問題が発生したのかをできるだけ具体的にお知らせ下さい）
- ご利用頂いている VPN クライアントでの不具合発生時のログ（レベルに関しましては、「Detailed」で取得をお願い致します）
- VPN クライアントと接続する、または接続している XR の設定ファイル，ログ，IPsec のステータス情報（取得方法に関しましては、ご利用頂いている製品のユーザーズガイドをご参照下さい）

6-2. サポートデスクのご利用に関して

電話サポート

電話番号：０４２２－３７－８９２６

電話での対応は以下の時間帯で行います。

月曜日 ～ 金曜日 10:00 AM - 5:00 PM

ただし、国の定める祝祭日、弊社の定める年末年始は除きます。

電子メールサポート

E-mail： support@centurysys.co.jp

ＦＡＸサポート

FAX 番号：０４２２－５５－３３７３

電子メール、FAX は 毎日 24 時間受け付けております。

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

FutureNet VPN Client/NET-G 接続設定ガイド
Ver2.0.0
2008 年 1 月
発行　センチュリー・システムズ株式会社