FutureNet VPN Client/NET-G

接続設定ガイド　v1.1.1

CENTURY SYSTEMS

目次

1. 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、NETG 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、製品に添付の 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。

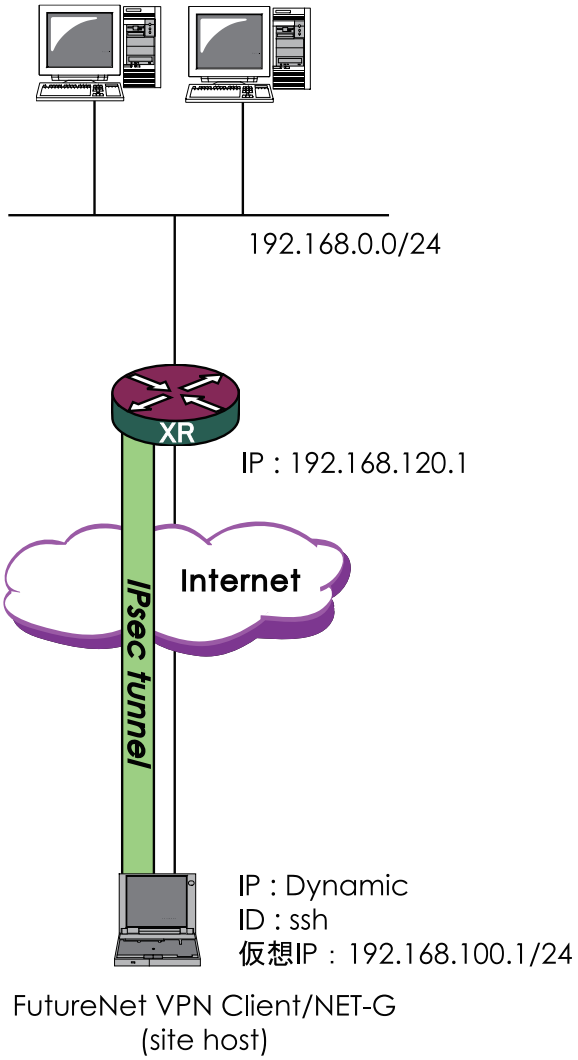
■本ガイドは、以下の FutureNet XR 製品に対応しております。

- XR-380、XR-380/DES
- XR-410 シリーズ
- XR-410/CD-L2
- XR-440/C
- XR-640/CD
- XR-640/CD-L2
- XR-510/C
- XR-540/C
- XR-1000 Ver2.0 以降
- XR-1000/TX4
- XR-1100 シリーズ

2.　接続設定例　～基本的な設定～

2-1. ネットワーク構成

XR をセンター、VPN Client を拠点とし、この間で Ipsec トンネルを生成して 192.168.0.0/24 と拠点側ホストをセキュアに通信可能とします。



2-2. 接続条件

・PSK（共通鍵）方式で認証します。

・agressive モードで接続します。

・仮共通鍵は「ipseckey」とします。

・XR 側は固定 IP、SSH 側は動的 IP とします。

・XR 側は PPPoE 接続するものとします。

・IP アドレス等は図中の表記を使うものとします。

・IPsec 設定で使用するパラメータ値は以下の通りとします。

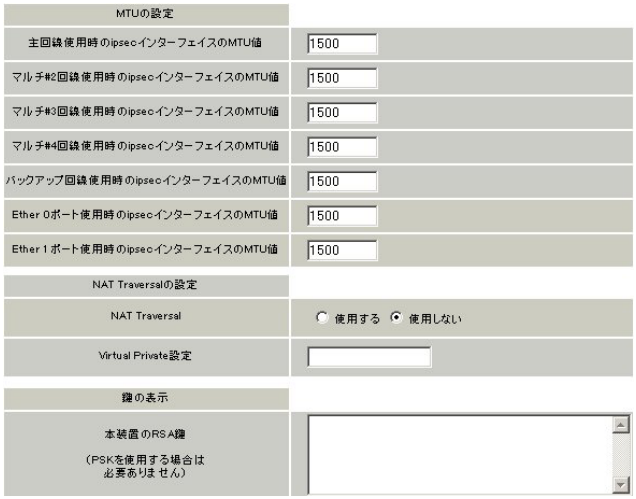
暗号方式　：　3DES
整合性　：　SHA-1
IKE で使用するグループ　：　group2
拠点の ID　：　ssh

本ガイドではプライベート IP アドレスを用いた設定例としておりますが、実環境ではグローバルアドレスに置き換えて設定してください。

2-3. XR の設定

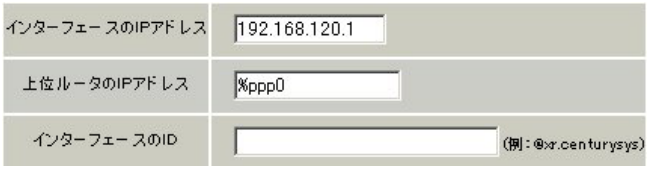
IPsec 設定画面において以下のように設定します。

[本装置の設定]



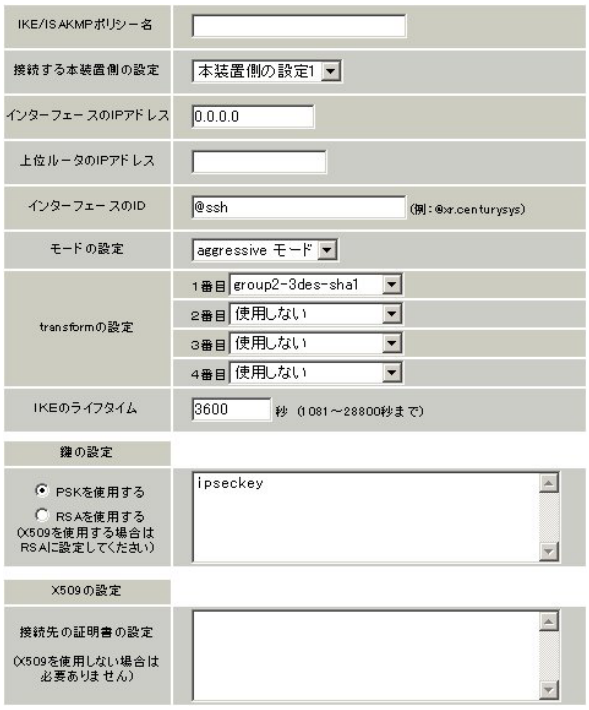
・MTU の設定 必要に応じて設定します。
・NAT Traversal の設定　「使用しない」
・VirtualPrivate 設定　「空欄」
・鍵の表示　「空欄」

[本装置の設定 1]



・インタフェースの IP アドレス「192.168.120.1」
・上位ルータの IP アドレス　「%ppp0」
・インタフェースの ID　「空欄」

[IKE/ISAKMP ポリシーの設定]



・IKE/ISAKMP ポリシー名　「任意で入力」
・接続する本装置側の設定
　「本装置側の設定」で設定した番号と同じもの
　を選択してください。
・インタフェースの IP アドレス　「0.0.0.0」
・上位ルーターの IP アドレス　「空欄」
・インタフェースの ID　「@ssh」　・・・(※1)
・モードの設定　「agressive モード」
・Transform の設定　1 番目　「group2-3des-sha1」
　2 ～ 3 番目は「使用しない」
・IKE のライフタイム　「任意で設定」
・鍵の表示　「PSK を使用する」を選択し、「ipseckey」
　を入力します。

(※1)XR における ID の設定では”@”を付けますが、Sentinel 側では、”@”を付けない形式で設定してください。VPN Client でも”@”を付けて設定すると接続できません。

・「Responder として使用する」

［IPsec ポリシーの設定 ］

・使用する IKE ポリシー名の選択　「IKE1」
・本装置側の LAN 側のネットワークアドレス
「192.168.0.0/24」
・相手側の LAN 側のネットワークアドレス
「192.168.100.1/32」　・・・（※2 ）
・PH2 の Transform の設定　「3des-sha1」
○ PFS　「使用する」（ 推奨 ）
○ DH Group の選択　「group2」
○ SA のライフタイム　「任意で設定」

（※2）ここで設定したアドレスと同じ値を、VPN Client 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。

パケットフィルタ設定

入力フィルタで以下の 2 つの設定を追加してください。

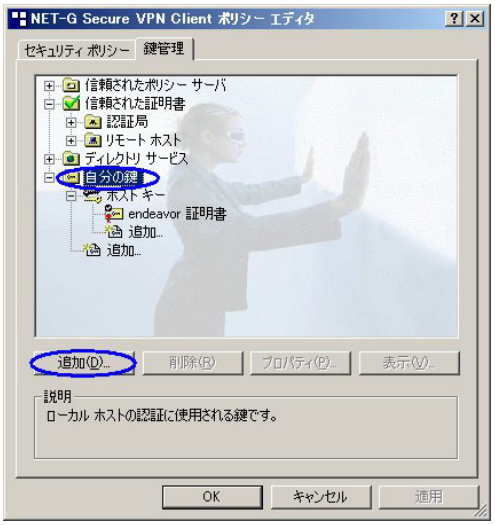
(1)
「インタフェース」外部接続しているポートを選択
「gre No.」 空欄
「方向」 パケット受信時
「動作」 許可
「プロトコル」 udp
「送信元アドレス」 空欄
「送信元ポート」 空欄
「あて先アドレス」 空欄
「あて先ポート」 500

(2)
「インタフェース」外部接続しているポートを選択
「gre No.」 空欄
「方向」 パケット受信時
「動作」 許可
「プロトコル」 esp
「送信元アドレス」 空欄
「送信元ポート」 空欄
「あて先アドレス」 空欄
「あて先ポート」 空欄

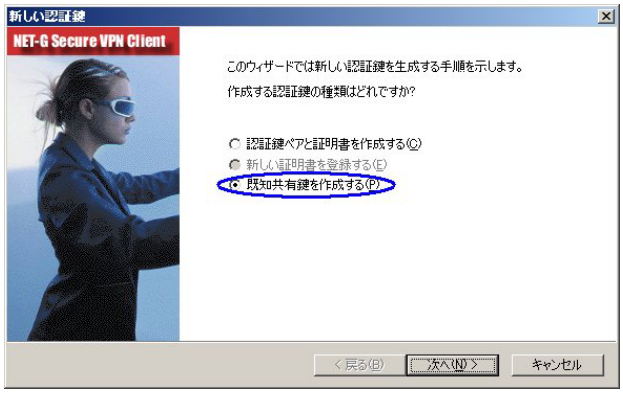
2-4. VPN Client の設定

Windows のタスクトレイから、VPN Client の”ポリシーエディタ”を開いて設定します。

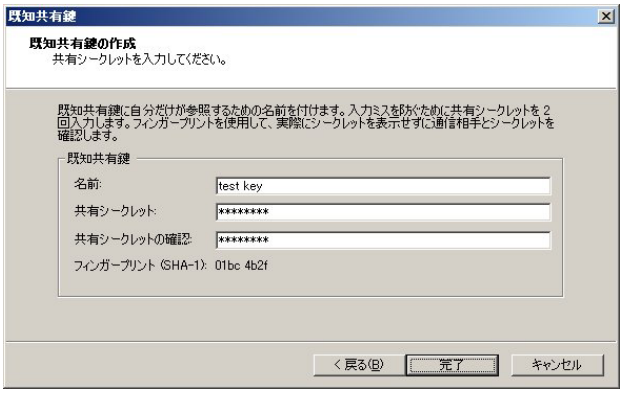
2-4-1. 仮共有鍵の設定



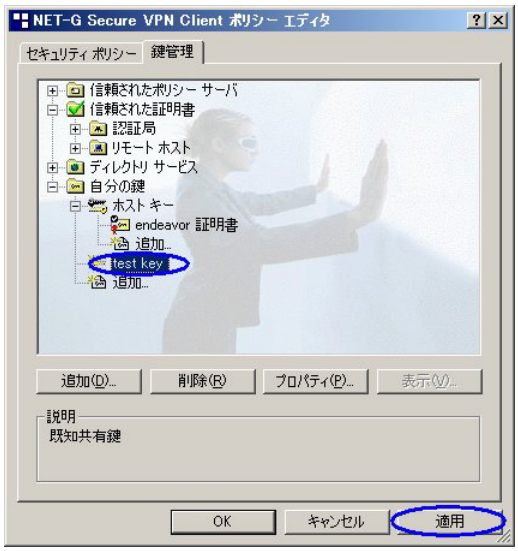
「鍵管理」タブをクリックします。
「自分の鍵」を選択し、「追加」ボタンをクリックします。



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

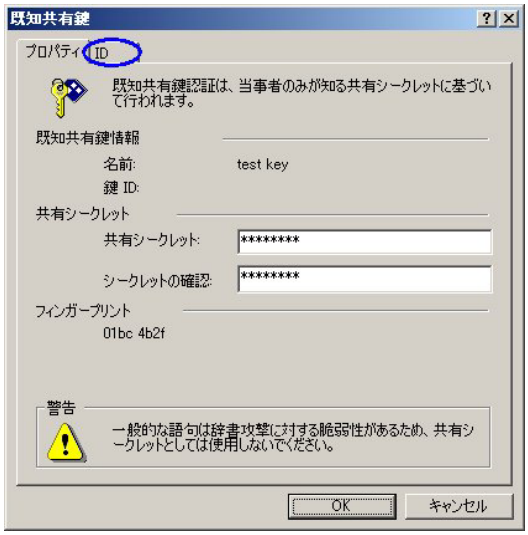


「事前共有鍵情報」画面が開きます。ここで事前共有鍵を設定します。
「名前」項目には任意の設定名を入力します。
「共有シークレット」「共有シークレットの確認」項目には、事前共有鍵（PSK）を入力して「完了」をクリックします。
このとき、入力した鍵は”＊”や”●”等で表示されます。



「鍵管理」画面に戻ります。事前共有鍵情報が登録されていることを確認したら、「適用」ボタンをクリックしてください。「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。

2-4-2. ID の設定



引き続き「鍵管理」画面で、登録した事前共有鍵情報を選択して「プロパティ」ボタンをクリックします。

「事前共有鍵」画面が開きますので、「ID」タブをクリックします（この画面では仮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 設定「IKE/ISAKMP ポリシー設定」における”インタフェース ID”と同じ ID を入力します。

ただしこのとき、ホストドメイン名には”@”を付けないで入力してください。

「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ください。
「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。

続いて XR への IPsec 接続設定を行ないます。

2-4-3. セキュリティポリシーの設定

ポリシーエディタの「セキュリティーポリシー」タブをクリックします。

「VPN 接続」を選択し「追加」ボタンをクリックします。

「VPN 接続を追加」画面が開きます。

「ゲートウェイ名」は、右端の”IP”をクリックして「ゲートウェイ IP アドレス」とし、XR の WAN 側 IP アドレスを入力します。
「認証鍵」は 1. 事前共有鍵の設定で登録した仮共有鍵の設定名を選択します。
「レガシ候補を使用する」にはチェックを入れます。

さらに、「リモートネットワーク」については、右端にある”...”をクリックしてください。続いて「ネットワークエディタ」画面が開きます。
「ネットワークエディタ」画面では、「ネットワーク名」は

任意の設定名を付けます。
「IP アドレス」「サブネットマスク」は、XR に接続している LAN について入力します。
設定後に「OK」をクリックすると「セキュリティーポリシー」画面に戻ります。

「セキュリティーポリシー」画面で、これまでのセキュリティーポリシー設定が登録されていることを確認したら、「適用」ボタンをクリックしてください。
「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。

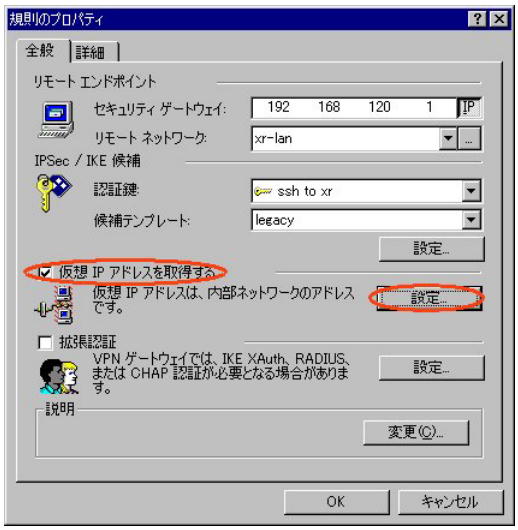
引き続いて、登録した設定を選択し、「プロパティ」ボタンをクリックしてください。「規則のプロパティ」画面が開きます。

3 つある「設定」ボタンのうち、一番上の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について設定します。

「IKE モード」は”agressive mode”に設定してください。

設定後に「OK」ボタンをクリックしてください。「規則のプロパティ」画面に戻ります。



「規則のプロパティ」画面に戻りましたら、続いて「仮想 IP アドレスを取得する」にチェックを入れ、2 つ目の「設定」ボタンをクリックしてください。「仮想 IP アドレス」画面が開きます。

「仮想 IP アドレス」画面では、ホストが XR に IPsec 接続する際に使用する仮想的な IP アドレスを設定します。XR からみたときには、仮想 IP アドレスが IPsec 対向のホストということになります。

「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 設定における「IPsec ポリシー」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。ただしサブネットマスクは 24 ビットマスクとしてください。設定後に「OK」ボタンをクリックしてください。

ここまで設定しましたら、すべての画面で「OK」をクリックして設定完了です。IPsec 接続を開始してください（操作方法につきましては、製品マニュアルをご参照くださ

3.　接続設定例　～仮想 IP アドレスを使わない設定～

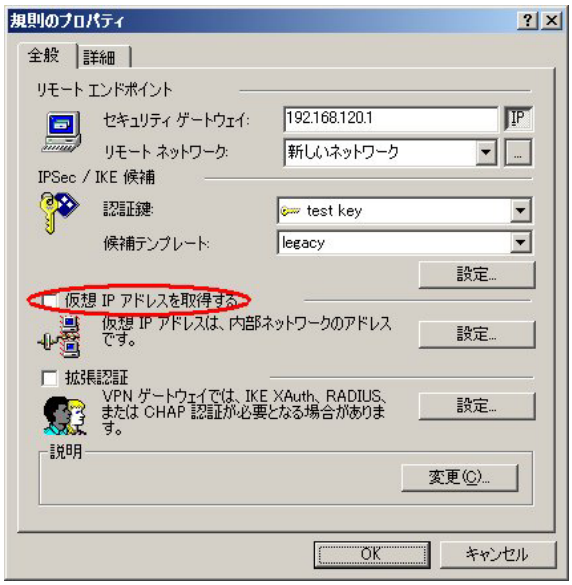
前セクションの基本設定例では、VPN Clinet 側では IPsec 接続時に使われる「仮想 IP アドレス」を設定しました。このとき XR 側の LAN からは、VPN Client に設定した「仮想 IP アドレス」に対して IPsec 経由での通信をおこないます。

この設定以外に､「仮想 IP アドレス」を使わずに、VPN Clinet と XR シリーズを 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 Clinet 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。

3-1. VPN Clinet の設定

「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。



3-2. XR の設定

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。

（画面は設定例です）

この 2 点以外については、基本設定と同様に設定してください。

〈この設定での注意点〉

VPN Client 側が動的 IP 側の場合、IPsec 接続中に VPN Client 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。

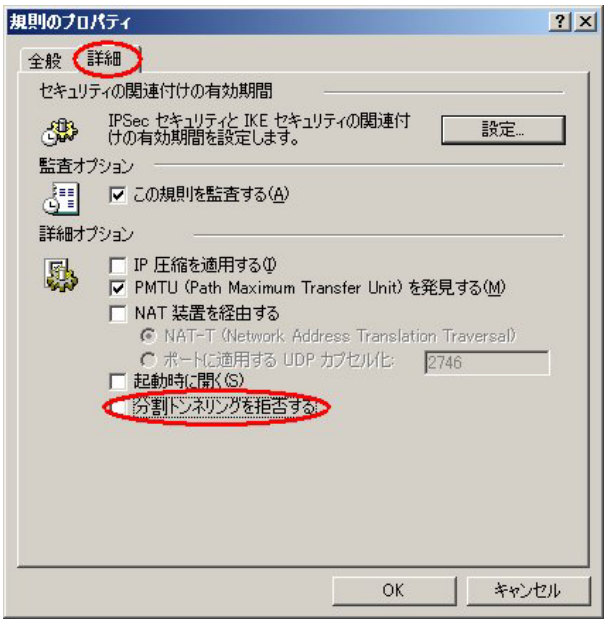
- XR の IPsecKeep-Alive 機能により、IPsecSA を削除したとき
- IPsec SA のライフタイムが経過したとき
- 削除ペイロードを受信したとき
- XR 側を再起動したとき

基本設定例にしたがって設定したときは、IPsec 通信とインターネットの同時アクセスができません。

IPsec とインターネットを同時に利用するときは、つぎのいずれかの設定をおこなってください。

4-1. VPN Client の設定 1

「規則のプロパティ」画面の「詳細」タブをクリックし、「分割トンネリングを拒否する」のチェックを外します。



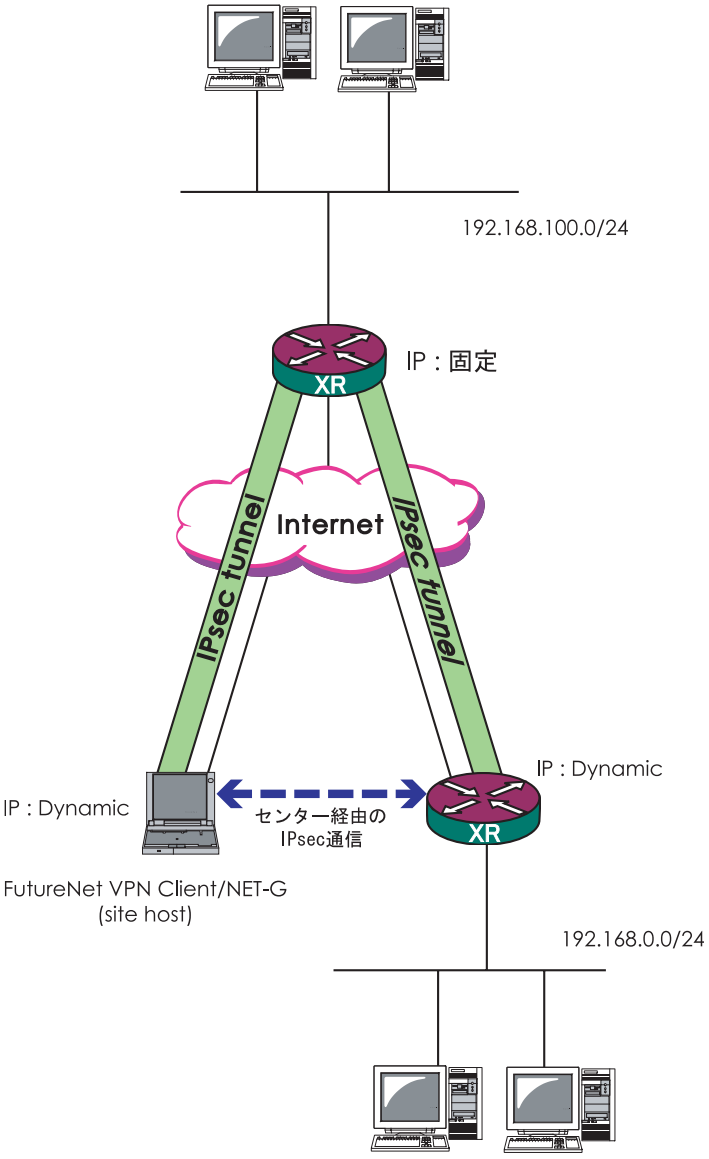
4-2. VPN Client の設定 2

「3.　接続設定例　～仮想 IP アドレスを使わない設定」にしたがって設定します。

5.　接続設定例　～センター経由で IPsec 接続をおこなう設定～

5-1. ネットワーク構成

VPN Client は、センター側 LAN と拠点側 LAN に IPsec で接続します。
拠点側にはセンター側 LAN を経由して IPsec 接続します。
IPsec トンネルは、VPN Client と XR #1 間、XR #2 と XR #1 間で生成します。



5-2. VPN Client の設定

P.3 からの設定通りに設定します。
ただし「規則のプロパティ」画面では、つぎのように設定してください。

・「リモートネットワーク」を指定する項目では、
「any」を選択します。(P.7 を参照)

5-3. XR の設定

5-3-1. XR #1(センター側)の設定

本装置の設定、および IKE/ISAKMP ポリシー設定については、固定 IP - 動的 IP(aggressive モード)での接続設定をおこないます。

IPsec ポリシーについては、以下のような設定をしてください。

a.(VPN Client とセンター側 LAN を結ぶ設定)
本装置側の LAN 側のネットワークアドレス
「0.0.0.0/0」
相手側の LAN 側のネットワークアドレス
「VPN Client の仮想 IP アドレス /32」

b.(センター側 LAN と拠点側 LAN を結ぶ設定)
本装置側の LAN 側のネットワークアドレス
「0.0.0.0/0」
相手側の LAN 側のネットワークアドレス
「192.168.0.0/24」

5-3-2.XR #2（拠点側）の設定

本装置の設定、および IKE/ISAKMP ポリシー設定については、固定 IP - 動的 IP(aggressive モード）での接続設定をおこないます (P.4、もしくは IPsec 設定ガイドをご参照下さい)。

IPsec ポリシーについては、以下のような設定をしてください。

a.（センター側 LAN と拠点側 LAN を結ぶ設定）
本装置側の LAN 側のネットワークアドレス
「192.168.0.0/24」
相手側の LAN 側のネットワークアドレス
「0.0.0.0/0」

これらの設定によって、VPN Client は全てのパケットをセンター側に送信し、センター側 LAN および拠点側 LAN に IPsec 接続可能となります。

この設定を用いると、動的 IP アドレスを持つ拠点 / クライアント同士を IPsec 接続できるようになります。

またこの運用においては、通常のインターネットアクセスもすべてセンター経由となります。

5-3-3. パケットフィルタ設定

各 XR の入力フィルタで以下の 2 つの設定を加えます。

a.
「インタフェース」外部接続しているポートを選択
「gre No.」 空欄
「方向」 パケット受信時
「動作」 許可
「プロトコル」 udp
「送信元アドレス」 空欄
「送信元ポート」 空欄
「あて先アドレス」 空欄
「あて先ポート」 500

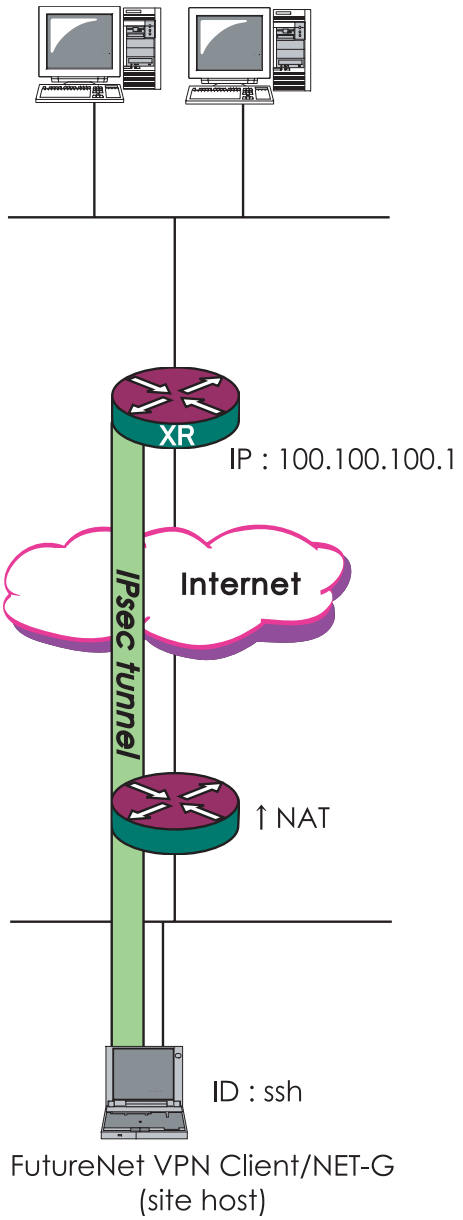
b.
「インタフェース」外部接続しているポートを選択
「gre No.」 空欄
「方向」 パケット受信時
「動作」 許可
「プロトコル」 esp
「送信元アドレス」 空欄
「送信元ポート」 空欄
「あて先アドレス」 空欄
「あて先ポート」 空欄

6.　接続設定例　～ NAT トラバーサルを用いた接続 1 ～

NAT トラバーサル機能を使って、NAT ルータの下にあるホストから IPsec 通信をおこなうための設定例です。

6-1. ネットワーク構成

XR #2 をセンター、VPN Client を拠点とします。VPN Client と LAN A をセキュアに通信可能とします。ただし､｢ルータ｣は NAT ルータとして機能するものとします。



6-2. 接続条件

・PSK（共通鍵）方式で認証します。

・agressive モードで接続します。

・XR 側は PPPoE 接続 / 固定 IP とします。

・NET-G の上位ルータは、IP マスカレード処理だけをしているものとします。

・それぞれの LAN は以下の設定とします。

LAN A ： 192.168.10.0/24
LAN B ： 192.168.1.0/24

・NET-G の仮想 IP アドレスは「192.168.20.1/24」とします。

・XR 側は PPPoE 接続するものとします。

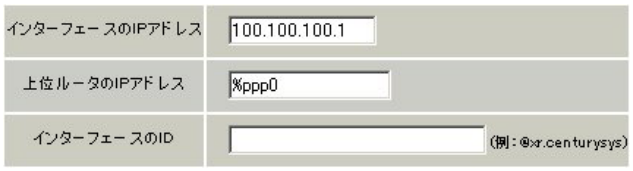
・IP アドレス等は図中の表記を使うものとします。

・IPsec 設定で使用するパラメータ値は以下の通りとします。

暗号方式 ： 3DES
整合性 ： SHA-1
IKE で使用するグループ ： group2
PSK：「ipseckey」
拠点の ID ： ssh

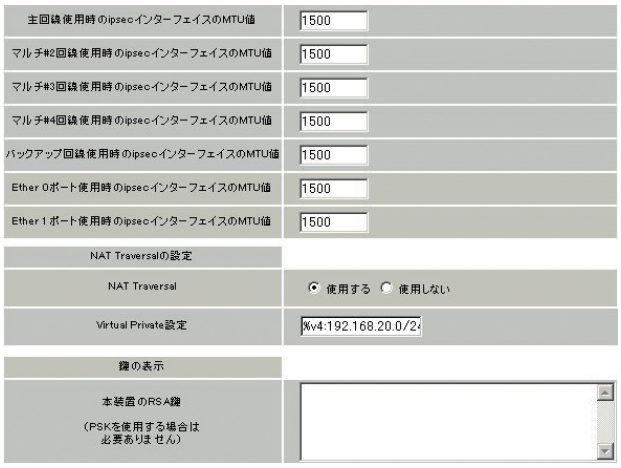
6-3. XR の設定

[本装置側の設定]



「本装置側の設定 1」を選択します。
・インタフェースの IP アドレス「100.100.100.1」
・上位ルータの IP アドレス 「%ppp0」
・インタフェースの ID 「空欄」

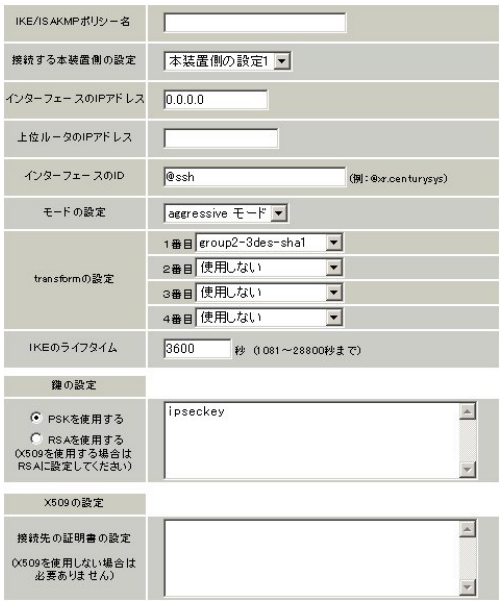
[本装置の設定]



・NAT Traversal 「使用する」にチェック
・Virtual Private 設定 「%v4 : 192.168.20.0/24」(※ 3)
・本装置の RSA 鍵 「空欄」

(※ 3)VPN Client の仮想 IP アドレス**設定と同じネットワークア**ドレスを指定します。

[IKE/ISAKMP ポリシーの設定]



・IKE/ISAKMP ポリシー名 「任意設定」
・接続する本装置側の設定
「本装置側の設定」で設定した番号と同じもの
を選択してください。
・インタフェースの IP アドレス 「0.0.0.0」
・上位ルータの IP アドレス 「空欄」
・インタフェースの ID 「@ssh」
・モードの設定 「aggressive モード」
・transform の設定 1 番目 「group2-3des-sha1」
2 ～ 3 番目は「使用しない」
・IKE のライフタイム 「任意で設定」
・鍵の表示 「PSK を使用する」を選択し、
「ipseckey」を入力します。
・X.509 の設定 「空欄」

[IPsec ポリシーの設定]

・「Responder として使用する」にチェック。
・使用する IKE ポリシー名の選択
「IKE/ISAKMP ポリシー」で設定したものを選択
・本装置側の 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
「vhost:%priv」
・PH2 の Transform の設定 「3des-sha1」
・PFS 「使用する」(推奨)
・DH Group の選択 「group2」
・SA のライフタイム 「任意で設定」

［パケットフィルタ設定］

入力フィルタで以下の設定を加えます。

a.
「インタフェース」外部接続しているポートを選択
「gre No.」 空欄
「方向」 パケット受信時
「動作」 許可
「プロトコル」 udp
「送信元アドレス」 空欄
「送信元ポート」 空欄
「あて先アドレス」 500
「あて先ポート」 空欄

b.
「インタフェース」外部接続しているポートを選択
「gre No.」 空欄
「方向」 パケット受信時
「動作」 許可
「プロトコル」 udp
「送信元アドレス」 空欄
「送信元ポート」 空欄
「あて先アドレス」 4500
「あて先ポート」 空欄

［パケットフィルタ設定時の注意点］

NAT ルータ配下の複数の VPN Client から同時に IPsec 接続する場合は、XR の入力フィルタ設定を以下のようにしてください。

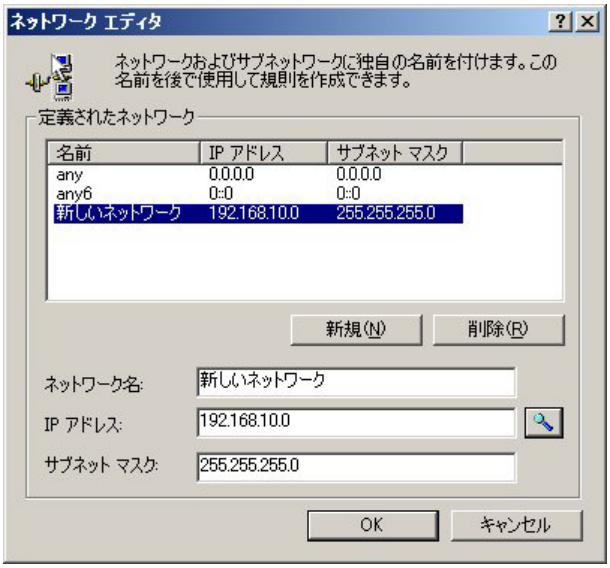
a.
「インタフェース」外部接続しているポートを選択
「gre No.」 空欄
「方向」 パケット受信時
「動作」 許可
「プロトコル」 udp
「送信元アドレス」 空欄
「送信元ポート」 空欄
「あて先アドレス」 空欄
「あて先ポート」 空欄

6-4.VPN Clinent の設定

［規則のプロパティ＜全般＞設定］

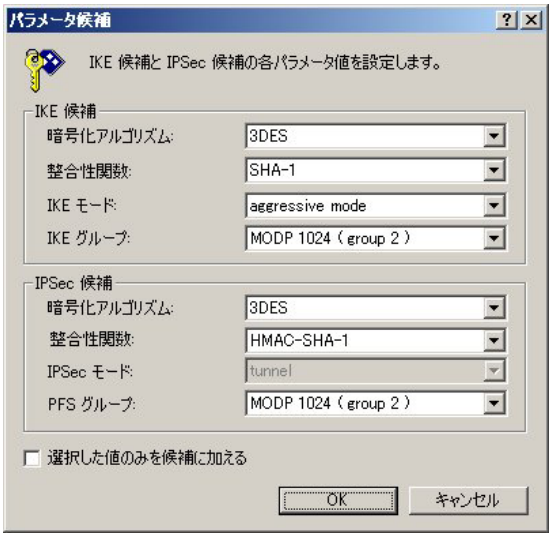
・セキュリティゲートウェイ　「100.100.100.1」
・リモートネットワーク
　作成したリモートネットワーク設定を選択します（次項を参照ください）。
・認証鍵：事前に作成した鍵を選択します。
・候補テンプレート　「normal」
・仮想 IP アドレスを使用する　「チェックなし」
・拡張認証　「チェックなし」

［リモートネットワークの設定］



・「新規」をクリックして以下のように設定してください。
・IP アドレス　「192.168.10.0」
・サブネットマスク　「255.255.255.0」

［パラメータの設定］

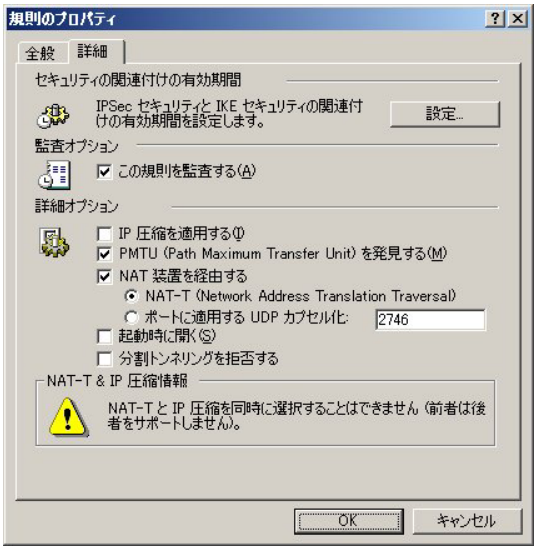


「IKE/IPsec 候補」項目の「設定...」をクリックします。

IKE 候補
- 暗号化アルゴリズム 「3DES」
- 整合性関数 「SHA-1」
- IKE モード 「aggressive mode」
- IKE グループ 「MODP 1024 (group2)」

IPsec 候補
- 暗号化アルゴリズム 「3DES」
- 整合性関数 「SHA-1」
- PFS グループ 「MODP 1024 (group2)」

［規則のプロパティ＜詳細＞設定］



詳細オプション項目にある

- NAT 装置を経由する
- NAT-T

の 2 カ所にチェックをしてください。

以上で VPN Client の設定は完了です。

［規則のプロパティ＜仮想 IP アドレス＞設定］

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

仮想 IP アドレス画面では、次のように設定します。

- 手動で設定にチェック
- IP アドレス 「192.168.20.1」
- サブネットマスク 「255.255.255.0」

6-6. 複数の VPN Clinent を接続する場合

NAT ルータ配下の複数の VPN Client から同時に IPsec 接続する場合は、それぞれの VPN Client に重複しないインタフェース ID、**仮想 IP アドレスを設定してください。**

XR 側では、インタフェース ID ごとに IKE/ISAKMP ポリシー設定・IPsec ポリシー設定を追加してください。

また XR のフィルタ設定も異なります。
フィルタ設定についてはP18[パケットフィルタ設定時の注意点] を参照してください。

7-7. 異なる複数の LAN から接続する場合

複数の異なる LAN 内にある VPN Client 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。

(例)%v4 : 192.168.10.0/24 ,%v4 : 192.168.20.0/24 ,%v4 : 192.168.30.0/24

LAN ごとの Virtual Private 設定を”カンマ”で区切り設定していきます (例ではレイアウトの都合上改行していますが、実際の設定では続けて設定してください)。

また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 Virutal Private 設定ができるようになっています。

7-7-1. バックアップテキストでの設定

以下の項目で設定します。

・[IPsec 本装置、本装置側の設定 1]
VIRTUALPRIVATE= ;Virtual Private

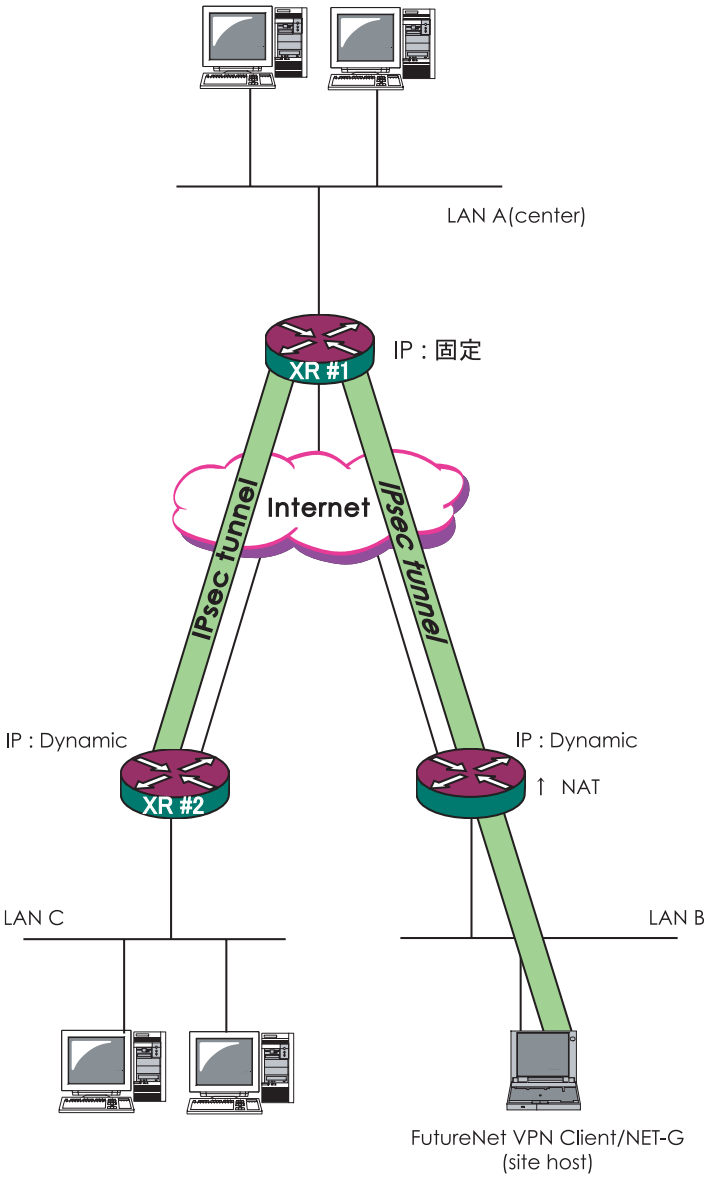
項目で、”VIRTUALPRIVATE=”に続いて上記 (**例**) **のよう**に入力します。

バックアップテキストで設定したときには、設定の復帰時に XR 本体が自動的に再起動されます。

7.　接続設定例　～ NAT トラバーサルを用いた接続 2 ～

NAT トラバーサルによる IPsec 接続と、通常の IPsec 接続を同時におこなうための設定です。

7-1. ネットワーク構成



7-2. 運用条件

・R1、R2、R3 ともに PPPoE 接続をします。

・R1 は固定 IP アドレス、R2 と R3 は動的 IP アドレスとします。

・R2 は通常の NAT ルータでの動作とします。

・R1 と PC は、NAT トラバーサルによって IPsec 接続をおこないます。

・R1 と R3 は aggressive モードで IPsec 接続をおこないます。

・それぞれの LAN は以下の設定とします。
LAN A ： 192.168.10.0/24
LAN B ： 192.168.100.0/24
LAN C ： 192.168.0.0/24

・その他の IP アドレス等は図中の表記を使うものとします。

・IPsec 設定で使用するパラメータ値は以下の通りとします。

暗号方式 ： 3DES
整合性 ： SHA-1
IKE で使用するグループ ： group2

・VPN Client の仮想 IP アドレス設定は 192.168.50.1/255.255.255.0 とします。

7-3. XR の設定

7-3-1. #1 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	%ppp0
インターフェースのID	(例：@xr.centurysys)

[本装置の設定]

NAT Traversal	◉ 使用する ○ 使用しない
Virtual Private設定	%v4:192.168.50.0/24

NAT-T の設定をおこないます。

[IKE/ISAKMP ポリシーの設定 1]

IKE/ISAKMPポリシー名	
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	@branch (例：@xr.centurysys)
モードの設定	aggressive モード
transformの設定	1番目 group2-3des-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)
鍵の設定	
◉ PSKを使用する ○ RSAを使用する (X509を使用する場合はRSAに設定してください)	test

[IKE/ISAKMP ポリシーの設定 2]

IKE/ISAKMPポリシー名	
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	@client (例：@xr.centurysys)
モードの設定	aggressive モード
transformの設定	1番目 group2-3des-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)
鍵の設定	
◉ PSKを使用する ○ RSAを使用する (X509を使用する場合はRSAに設定してください)	test2

[IPsec ポリシーの設定 1]

○ 使用する ○ 使用しない ◉ Responderとして使用する ○ On-Demandで使用する

使用するIKEポリシー名の選択	(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	192.168.0.0/24 (例：192.168.0.0/24)
PH2のTransFormの選択	すべてを送信する
PFS	◉ 使用する ○ 使用しない
DH Groupの選択(PFS使用時に有効)	指定しない
SAのライフタイム	28800 秒 (1081～86400秒まで)
DISTANCE	1 (1～255まで)

[IPsec ポリシーの設定 2]

○ 使用する ○ 使用しない ◉ Responderとして使用する ○ On-Demandで使用する

使用するIKEポリシー名の選択	(IKE2)
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	vhost:%priv (例：192.168.0.0/24)
PH2のTransFormの選択	すべてを送信する
PFS	◉ 使用する ○ 使用しない
DH Groupの選択(PFS使用時に有効)	指定しない
SAのライフタイム	28800 秒 (1081～86400秒まで)
DISTANCE	1 (1～255まで)

［パケットフィルタ設定］
入力フィルタで以下の設定を加えます。

a.
「インタフェース」外部接続しているポートを選択
「gre No.」 空欄
「方向」 パケット受信時
「動作」 許可
「プロトコル」 udp
「送信元アドレス」 空欄
「送信元ポート」 空欄
「あて先アドレス」 500
「あて先ポート」 空欄

b.
「インタフェース」外部接続しているポートを選択
「gre No.」 空欄
「方向」 パケット受信時
「動作」 許可
「プロトコル」 udp
「送信元アドレス」 空欄
「送信元ポート」 空欄
「あて先アドレス」 4500
「あて先ポート」 空欄

c.
「インタフェース」外部接続しているポートを選択
「gre No.」 空欄
「方向」 パケット受信時
「動作」 許可
「プロトコル」 esp
「送信元アドレス」 空欄
「送信元ポート」 空欄
「あて先アドレス」 空欄
「あて先ポート」 空欄

［パケットフィルタ設定時の注意点］
NAT ルータ配下の複数の VPN Client から同時に IPsec 接続する場合は、XR の入力フィルタ設定を以下のようにしてください。

a.
「インタフェース」外部接続しているポートを選択
「gre No.」 空欄
「方向」 パケット受信時
「動作」 許可
「プロトコル」 udp
「送信元アドレス」 空欄
「送信元ポート」 空欄
「あて先アドレス」 空欄
「あて先ポート」 空欄

b.
「インタフェース」外部接続しているポートを選択
「gre No.」 空欄
「方向」 パケット受信時
「動作」 許可
「プロトコル」 esp
「送信元アドレス」 空欄
「送信元ポート」 空欄
「あて先アドレス」 空欄
「あて先ポート」 空欄

7-3-2. #2 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	%ppp0
上位ルータのIPアドレス	
インターフェースのID	@branch (例：@xr.centurysys)

[本装置の設定]

設定の必要はありませんが、MTU 値については適宜変更できます。

[IKE/ISAKMP ポリシーの設定 1]

IKE/ISAKMPポリシー名	
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 group2-3des-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)
鍵の設定	
PSKを使用する RSAを使用する (X509を使用する場合はRSAに設定してください)	test

[IPsec ポリシーの設定 1]

使用する / 使用しない / Responderとして使用する / On-Demandで使用する

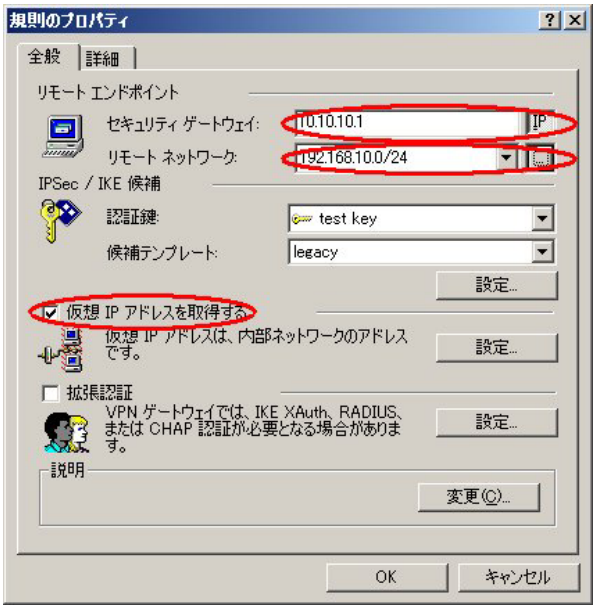
使用するIKEポリシー名の選択	(IKE1)
本装置側のLAN側のネットワークアドレス	192.168.0.0/24 (例：192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.10.0/24 (例：192.168.0.0/24)
PH2のTransFormの選択	すべてを送信する
PFS	使用する / 使用しない
DH Groupの選択(PFS使用時に有効)	指定しない
SAのライフタイム	28800 秒 (1081～86400秒まで)
DISTANCE	1 (1～255まで)

[パケットフィルタ設定]

入力フィルタ設定で、「udp/500 番ポート」と「esp プロトコル」を解放してください。

7-4. VPN Clinent の設定

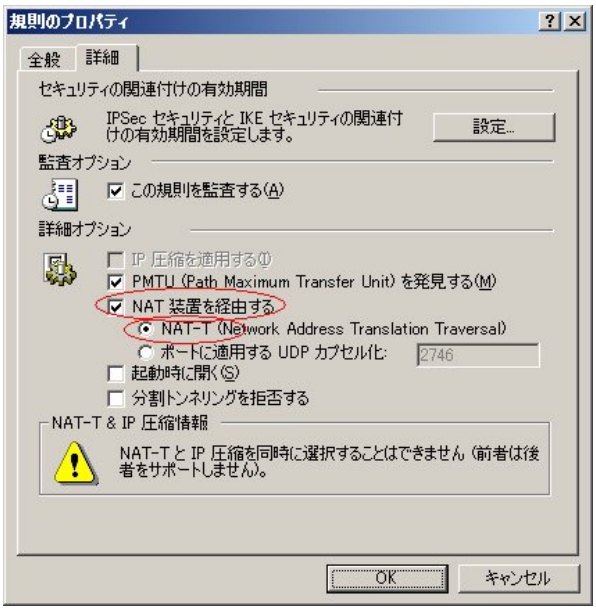
[規則のプロパティ＜全般＞設定]



「仮想 IP アドレスを取得する」にチェックします。

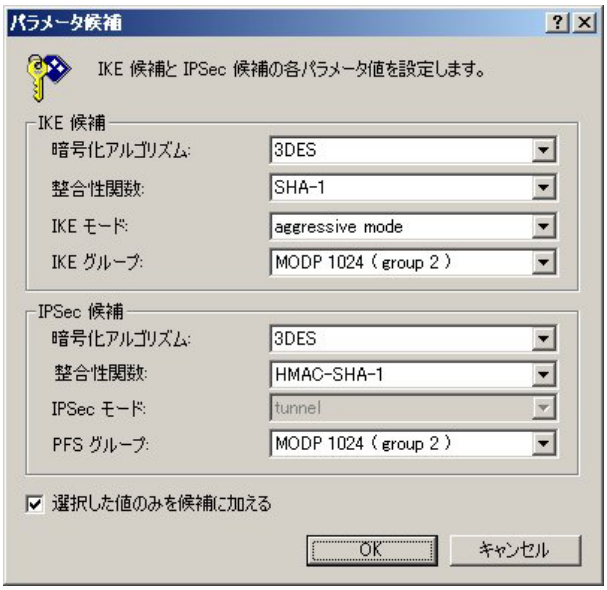
[仮想 IP アドレス画面]

[規則のプロパティ＜詳細＞設定]

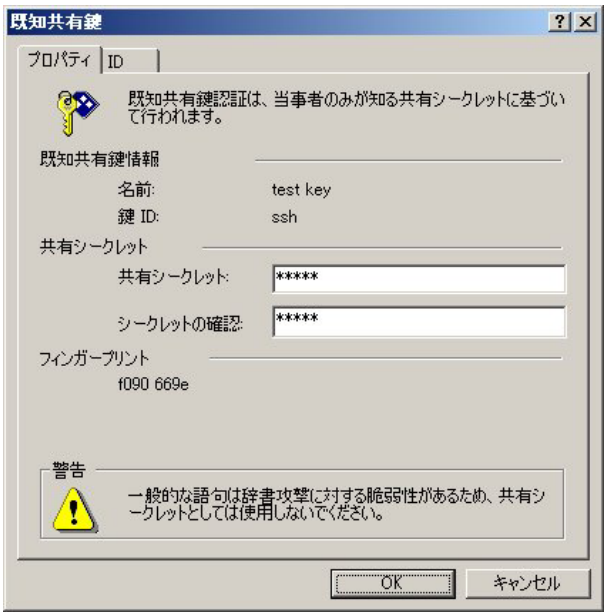


VPN　Client は NAT-T によって IPsec 接続をおこないますので、「NAT 装置を経由する」と「NAT-T」にチェックを入れてください。

[パラメータ候補画面]



[事前共有鍵＜プロパティ＞画面]



[事前共有鍵＜ID＞画面]

8. VPN Client のログについて

VPN Client では「IKE のログウィンドウ」を表示させることで、Ipsec の状態を把握することができます。

万が一 IPsec が確立できない場合もログを確認することで、ある程度の原因追及が可能です。

ここでは、IPsec が確立できないときの主なログの読み方を説明します。

[正常に接続できたときのログ表示例]

```
0.0.0.0:500 (Initiator) <-> xxx.xxx.xxx.xxx:500
{ bee8ab89 5a000003 - 647c30a6 94998148 [-1] /
0x00000000 } Aggr; MESSAGE: Phase 1 version = 1.0,
auth_method = Pre shared keys, cipher = 3des-cbc,
hash = sha1, prf = hmac-sha1, life = 0 kB / 14400
sec, key len = 0, group = 2

Phase-1 [initiator] between fqdn(udp:500,[0..2]=ssh)
and ipv4(any:0,[0..3]=xxx.xxx.xxx.xxx) done.

0.0.0.0:500 (Initiator) <-> xxx.xxx.xxx.xxx:500
{ bee8ab89 5a000003 - 647c30a6 94998148 [0] /
0xbaf3de8e } QM; MESSAGE: Phase 2 connection suc-
ceeded, Using PFS, group = 2

0.0.0.0:500 (Initiator) <-> xxx.xxx.xxx.xxx:500
{ bee8ab89 5a000003 - 647c30a6 94998148 [0] /
0xbaf3de8e } QM; MESSAGE: SA[0][0] = ESP 3des, life
= 409600 kB/3600 sec, group = 2, tunnel, hmac-
sha1-96, key len = 0, key rounds = 0

Phase-2 [initiator] done bun-
dle 2 with 2 SA's by rule 21:`ipsec
```

[IKE フェーズ 1 が確立できないときのログ表示例　その 1]

0.0.0.0:500 (Initiator) <-> xxx.xxx.xxx.xxx:500
{ a2196204 1e000003 - 00000000 00000000 [-1] /
0x00000000 } Aggr; Connection timed out or error,
calling callback

Phase-1 [initiator] between fqdn(udp:500,[0..2]=ssh)
and ipv4(udp:500,[0..3]=xxx.xxx.xxx.xxx) failed;
Timeout.

このログは IKE フェーズ 1 ネゴシエーションがうまく開始できていないことを示しています。以下の点をご確認ください。

・IPsec ゲートウェイの IP アドレス設定
XR 側：本装置の設定「インタフェースの IP アドレス」
SSH 側：セキュリティーポリシー「セキュリティーゲートウェイ」(P.8)

・インタフェース ID
XR 側：IKE/ISAKMP ポリシー設定「インタフェースの ID」
SSH 側：事前共有鍵設定「ID」のホストドメイン名 (P.6)
※ XR 側は <@ID> の入力、SSH 側は <ID> の入力

・モード間違い
XR 側：IKE/ISAKMP ポリシー設定「モードの設定」
SSH 側：規則のプロパティ「パラメータ候補」(P.9)
※どちらも”aggressive モード”で設定します。

・XR 側でステートフルパケットインスペクションが有効になっていませんか？有効になっているのであれば、無効にするか、IPsec 用のフィルタ設定をしてください。

[IKE フェーズ 1 が確立できないときのログ表示例　その 2]

0.0.0.0:500 (Initiator) <-> xxx.xxx.xxx.xxx:500
{ 878a3c20 b4000000 - 0e6a4ab9 116f8cc3 [-1] /
0x00000000 } Aggr; Hash value mismatch

Phase-1 [initiator] between fqdn(udp:500,[0..2]=ssh)
and ipv4(udp:500,[0..3]=xxx.xxx.xxx.xxx) failed;
Authentication failed.

0.0.0.0:500 (Initiator) <-> xxx.xxx.xxx.xxx:500
{ 878a3c20 b4000000 - 0e6a4ab9 116f8cc3 [-1] /
0x00000000 } Aggr; Error = Authentication failed (24)

このログは IKE フェーズ 1 ネゴシエーションを始めていますが、ホスト認証で失敗していることを示しています。共有鍵設定が間違っている可能性が高いので、以下の点をご確認ください。

XR 側：IKE/ISAKMP ポリシー設定の「鍵の設定」aggressive モードの場合は PSK 方式のみ使用可能です。

SSH 側：鍵管理「プロパティ」(P.6)

※同じ文字列の鍵を入力します。

[IKE フェーズ 2 が確立できないときのログ表示例]

```
0.0.0.0:500 (Initiator) <-> xxx.xxx.xxx.xxx:500
{ 0202f991 16000008 - 0e6a4ab9 116f8cc3 [-1] /
0x00000000 } Aggr; MESSAGE: Phase 1 version = 1.0,
auth_method = Pre shared keys, cipher = 3des-cbc,
hash = sha1, prf = hmac-sha1, life = 0 kB / 14400
sec, key len = 0, group = 2

Phase-1 [initiator] between fqdn(udp:500,[0..2]=ssh)
and ipv4(any:0,[0..3]=xxx.xxx.xxx.xxx) done.

0.0.0.0:500 (Initiator) <-> xxx.xxx.xxx.xxx:500 {
0202f991 16000008 - 0e6a4ab9 116f8cc3 [0] / 0xb-
00c7f69 } QM; Connection timed out or error, calling
callback

Phase-2 [initiator] for ipv4(icmp:0,[0..3]=192.168.
100.1) and ipv4(icmp:0,[0..3]=192.168.1.1) failed;
Timeout.
```

このログは IKE フェーズ 2 ネゴシエーションがうまくできていないことを示しています。以下の点をご確認ください。

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」と「相手側の LAN 側のネットワークアドレス」

SSH 側 : セキュリティーポリシー「ネットワークエディタ」と規則のプロパティ「仮想 IP アドレス」(P.9)

FutureNet VPN Client/NET-G 接続設定ガイド　v1.1.1

2006年8月版

発行 センチュリー・システムズ株式会社