BROADBAND GATE

インターネットVPN対応ブロードバンドルータ

FutureNet XR シリーズ

FutureNet XR VPN Client 接続設定ガイド

センチュリー・システムズ 株式会社

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 XR VPN Client はセンチュリー・システムズ株式会社の商標です。

■ ssh(R) 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 Sentinel および SSH Accession 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。

■ SSH Sentinel 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、オンラインヘルプ「SSH Sentinel1.4 ユーザーマニュアル」をご覧ください。

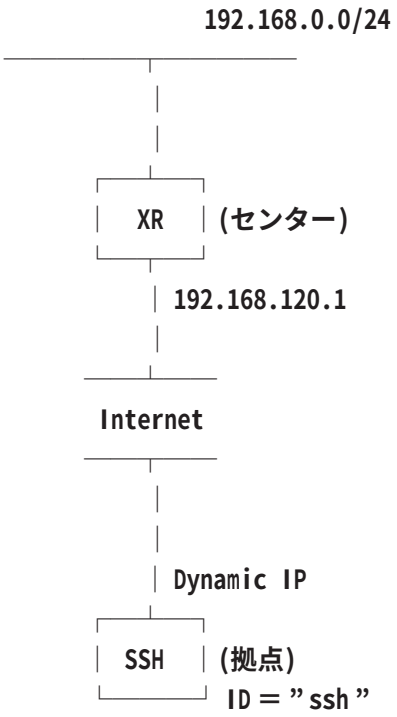
■本ガイドは、以下の FutureNet XR 製品に対応しております。

- XR-380、XR-380/DES
- XR-410
- XR-1000 Ver2.0 以降
- XR-1000/TX4

接続環境例

ネットワーク構成

XR をセンター、SSH Sentinel 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。



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。

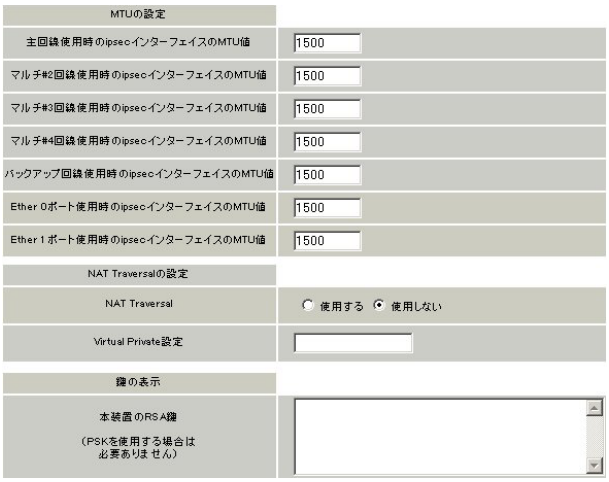
暗号方式 ： 3DES
整合性 ： SHA-1
IKE で使用するグループ ： group2
拠点の ID ： ssh

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。

XR の設定

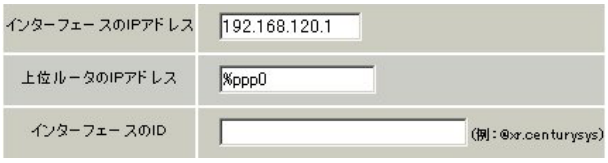
IPsec設定画面において以下のように設定します。

[本装置の設定]



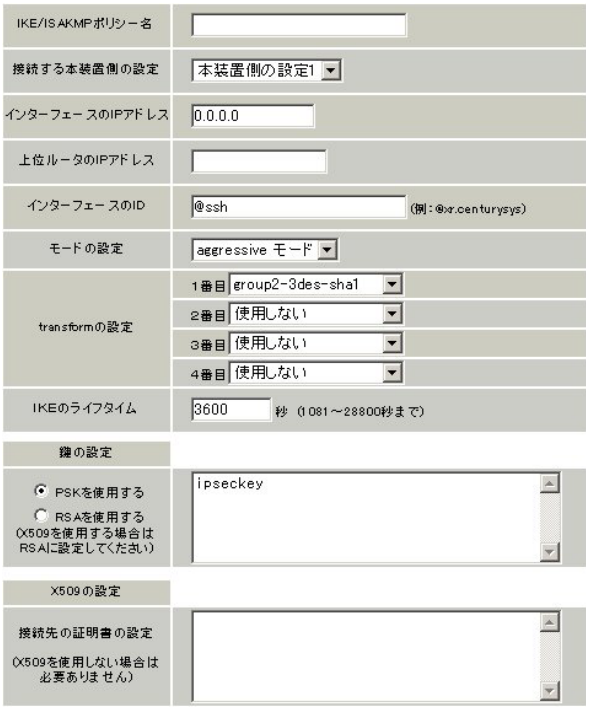
・MTU の設定 必要に応じて設定します。
・NAT Traversal の設定 「使用しない」
・VirtualPrivate 設定 「空欄」
・鍵の表示 「空欄」

[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」

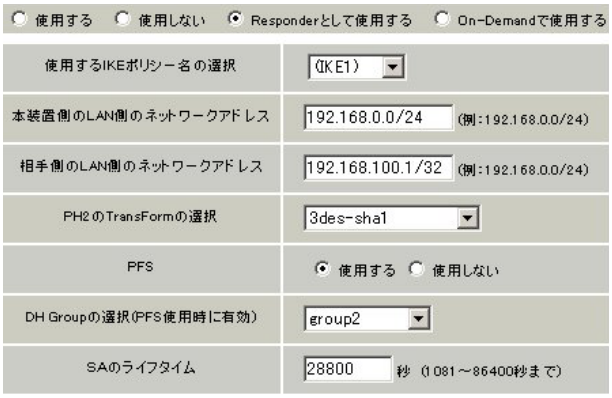
[IKE/ISAKMP ポリシーの設定]



・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。SSH Sentinel でも”@”を付けて設定すると接続できません。

[IPsecポリシーの設定]



・「Responderとして使用する」
・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」
・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」

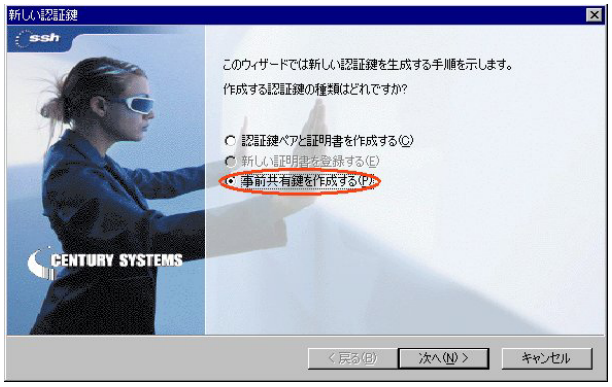
(※2)ここで設定したアドレスと同じ値を、SSH Sentinelの「仮想IPアドレスを取得する」項目で設定します。ただしXRの設定では必ず”**<IP address>/32**”の形式で設定します。”<IP address>/24”の設定では接続できませんのでご注意ください。

SSL Sentinel の設定

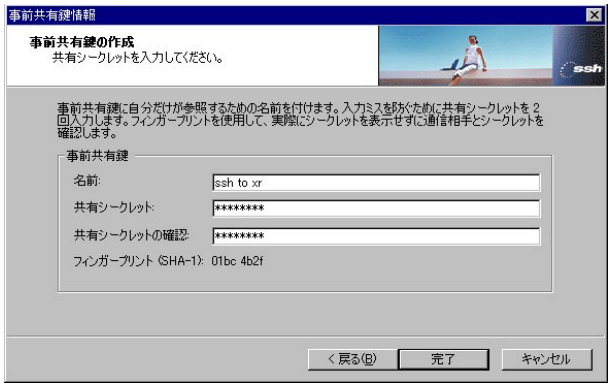
ポリシーエディタを開いて設定します。

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。
「事前共有鍵を作成する」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、事前共有鍵を入力して「完了」をクリックします。

「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、**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。

2. ID の設定

「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」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. 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」をクリックします。

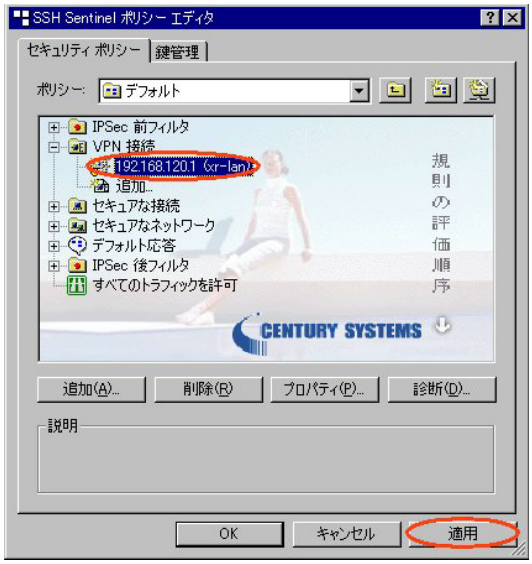
「VPN 接続を追加」画面が開きます。

「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。

「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。

「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、「OK」をクリックします。



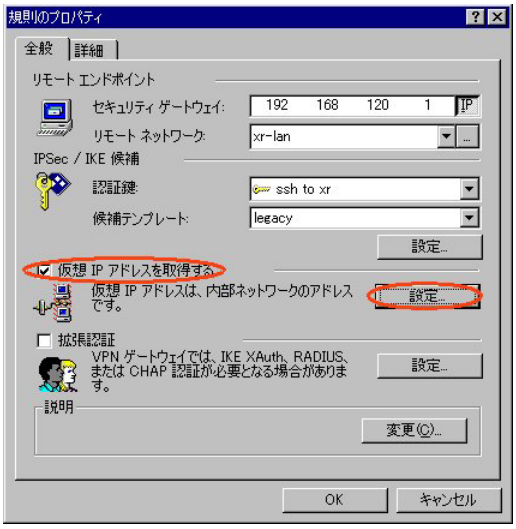
「セキュリティーポリシー」画面に戻ります。
これまでのセキュリティーポリシー設定が登録されていることを確認したら、**必ず「適用」ボタンをクリックしてください。**
「適用」ボタンをクリックしないと適切に設定されない場合があります。

引き続いて、登録した設定の「プロパティ」を開いてください。

「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。

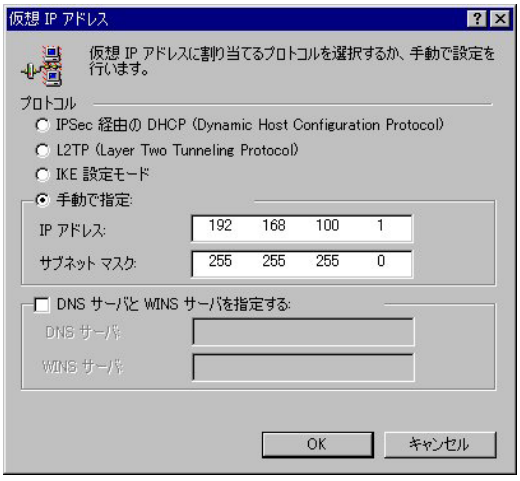
「パラメータ候補」画面が開きます。ここで暗号化方式などについて設定します。

「IKE モード」は ” agressive mode ” に設定してください。



「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、2 つ目の「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 IPsec 接続する際に、この PC が使用する仮想的な 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 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 ビットマスクとします。

ここまで設定できましたら、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(操作方法はオンラインヘルプをご参照ください)。

IPsec 接続とインターネット接続を同時に行う設定

前セクションまでの設定では、SSH Sentinel 側は IPsec とインターネットに同時に接続できません。SSH Sentinel で Ipsec を確立しているときは IPsec のみ通信可能となります。

IPsec とインターネットに同時に接続するには、以下のように設定してください。

仮想 IP アドレスを使わない方法

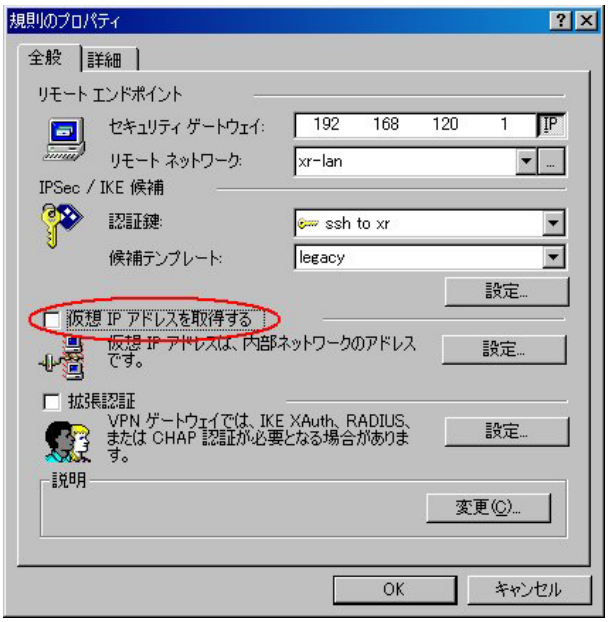
◯ XR 側の設定

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)

◯ SSH Sentinel 側の設定

「規則のプロパティ」画面の「仮想 IP アドレスを取得する」にはチェックを入れません。



(画面は設定例です)

この 2 点以外については、前セクションまでと同様に設定してください。

この設定では、VPN クライアント(が動作している PC)自身が保持するグローバル IP アドレスを使って VPN 接続します。

<この設定での注意点>
SSH Sentinel 側が動的 IP 側の場合、IPsec 接続中に SSH Sentinel 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。

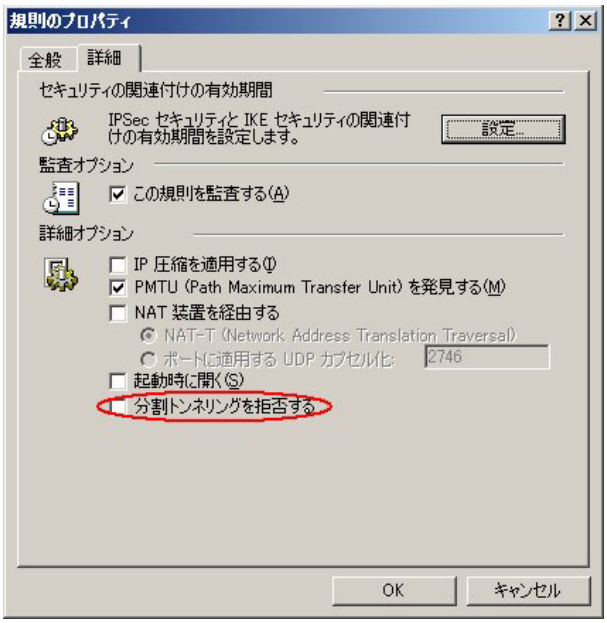
※ XR が保持する IPsec SA が無効になるのは以下の場合です。
・XR の IPsecKeep-Alive 機能により、IPsecSA を削除したとき
・IPsec SA のライフタイムが経過したとき
・削除ペイロードを受信したとき
・XR 側を再起動したとき

仮想 IP アドレスを使う方法

前セクションの設定はそのままで、さらに以下の設定をしてください。

○ SSH Sentinel 側の設定

「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。

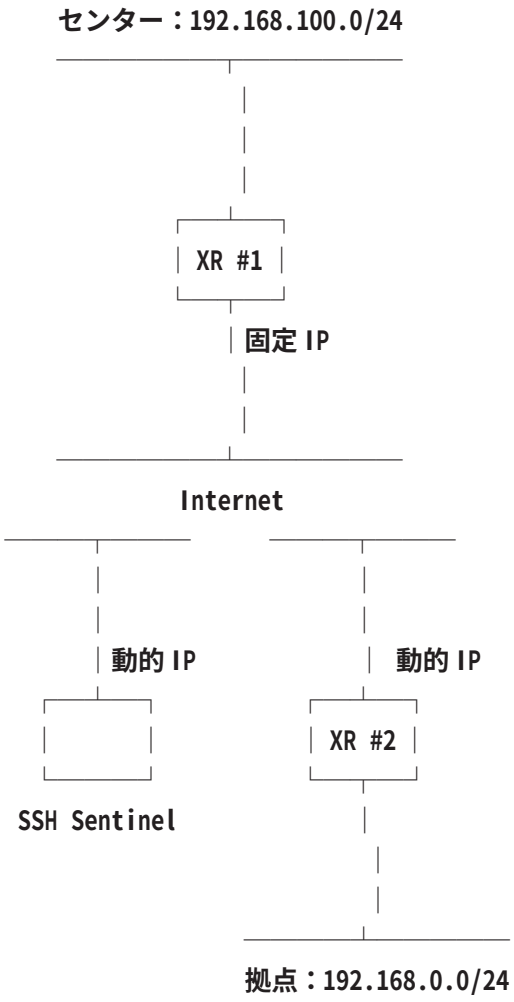


この設定では、VPN クライアント側で設定した仮想 IP アドレスを使って VPN 接続します。

すべてセンター経由で IPsec 接続を行う設定

ネットワーク構成

SSH Sentinel クライアントは、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、SSH Sentinel と XR #1 間、XR #2 と XR #1 間で生成します。



SSH Sentinel 側の設定

P.3 からの設定通りに設定します。
ただし以下の項目については

- 「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)

のように設定をしてください。

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.(SSH Sentinel 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
「SSH Sentinel 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」

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、SSH Sentinel 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。

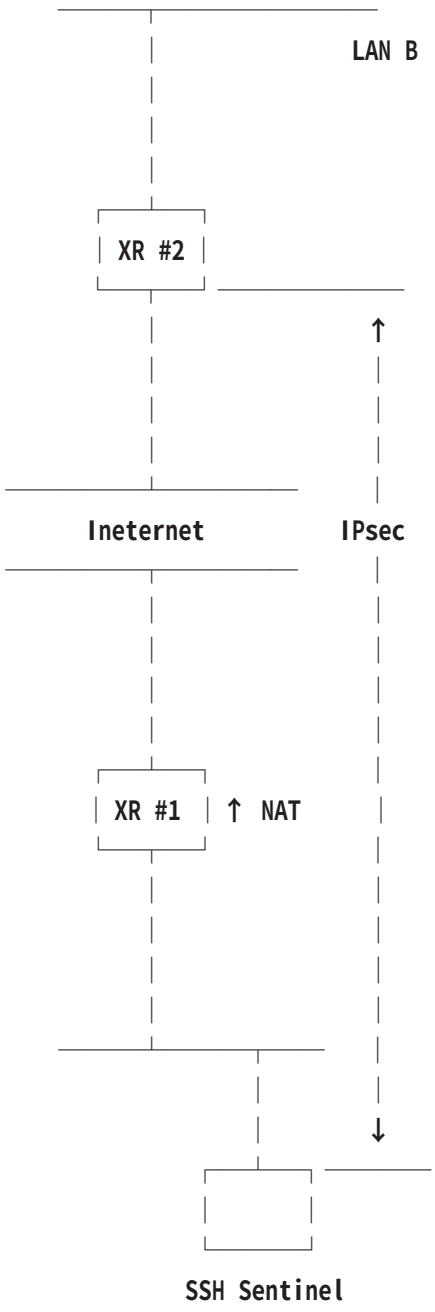
この設定を用いると、**動的 IP アドレスを持つ拠点 / クライアント同士を IPsec 接続できるようになります**。

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**。

NAT ルータを経由して IPsec 接続をする場合の設定

ネットワーク構成

XR #2 をセンター、SSH Sentinel を拠点とします。SSH Sentinel と LAN B をセキュアに通信可能とします。ただし、XR #1 は NAT ルータとして機能するものとします。



この構成では、IPsec 設定につきましては当ガイド P.3 からの設定通りに設定します。

さらに XR #1(NAT ルータ)において、以下のようにバーチャルサーバ設定とパケットフィルタ設定をしてください。

バーチャルサーバ設定

以下の 2 つの設定を加えます。

a.
「サーバのアドレス」SSH Sentinel の IP アドレス
「公開するグローバルアドレス」空欄
「プロトコル」udp
「ポート」500
「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

b.
「サーバのアドレス」SSH Sentinel の IP アドレス
「公開するグローバルアドレス」空欄
「プロトコル」esp
「ポート」空欄
「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

パケットフィルタ設定
転送フィルタで以下の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

これらの設定を加えることで、SSH Sentinelは
NATルータであるXR #1を経由してIPsec接続が可
能となります。

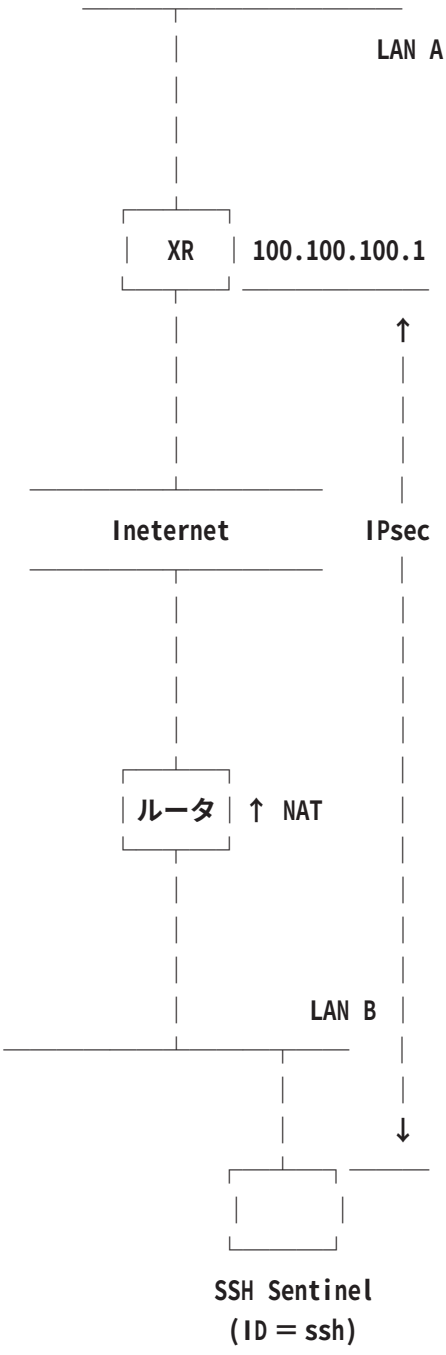
FutureNet XRシリーズ以外のNATルータを経由す
る場合は、これに準じた設定をしてください。

SSH Sentinelを使用したいクライアントの台数
分だけのグローバルアドレスが必要となります。

NAT トラバーサルを用いた IPsec 接続 1

ネットワーク構成

XR #2 をセンター、SSH Sentinel を拠点とします。SSH Sentinel 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。



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。

・SSH 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

・XR 側は PPPoE 接続するものとします。

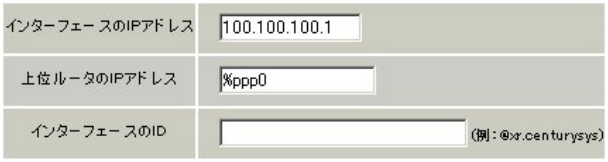
・IP アドレス等は図中の表記を使うものとします。

・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

XR の設定

[本装置側の設定]



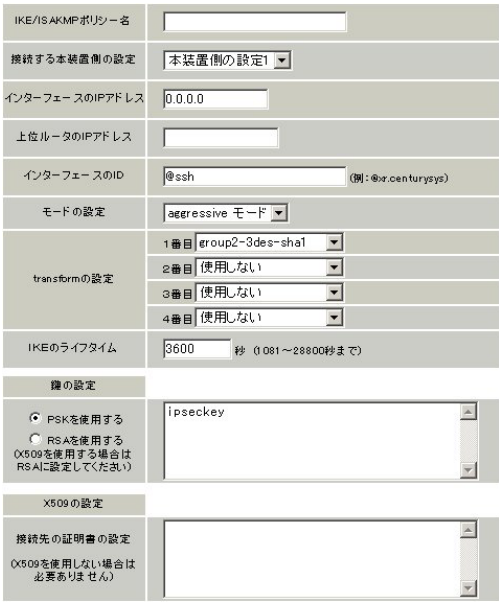
「本装置側の設定 1」を選択します。
・インタフェースの IP アドレス「100.100.100.1」
・上位ルータの IP アドレス 「%ppp0」
・インタフェースの ID 「空欄」

[本装置の設定]

・NAT Traversal 「使用する」にチェック
・Virtual Private 設定 「***%v4：192.168.1.0/24***」(※3)
・本装置の RSA 鍵 「空欄」

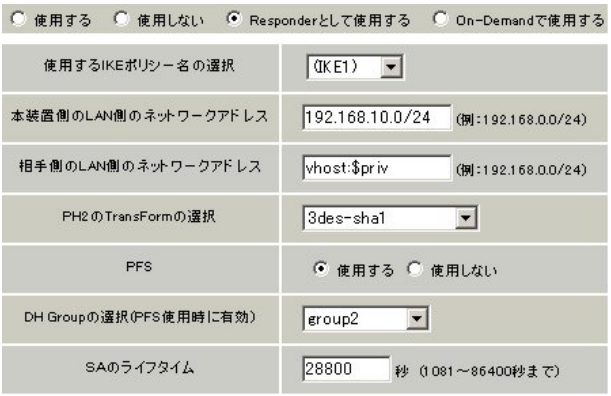
(※3)VPN Client が属しているものと同じネットワークアドレスを指定します。
また VPN Client が仮想 IP アドレスを使っている場合は、その仮想 IP アドレスと同じネットワークアドレスを指定します。

[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]



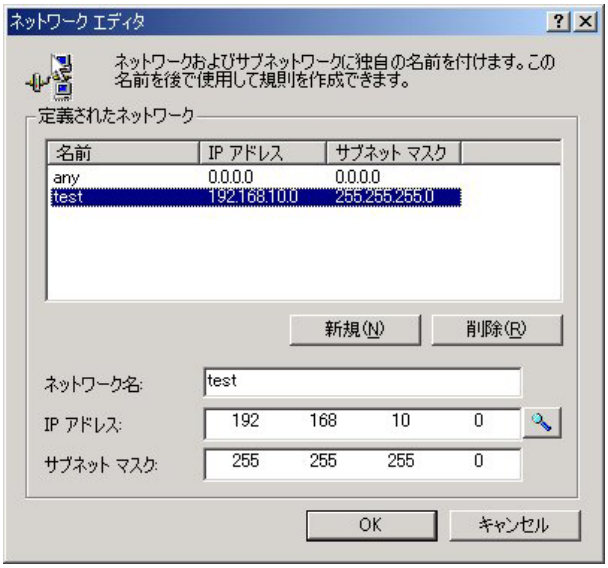
・「Responder として使用する」にチェック。
・使用する IKE ポリシー名の選択
「IKE/ISAKMP ポリシー」で設定したものを選択
・本装置側の LAN 側のネットワークアドレス
「192.168.10.0/24」
・**相手側の LAN 側のネットワークアドレス**
「***vhost:%priv***」
・PH2 の Transform の設定 「3des-sha1」
・PFS 「使用する」(推奨)
・DH Group の選択 「group2」
・SA のライフタイム 「任意で設定」

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」

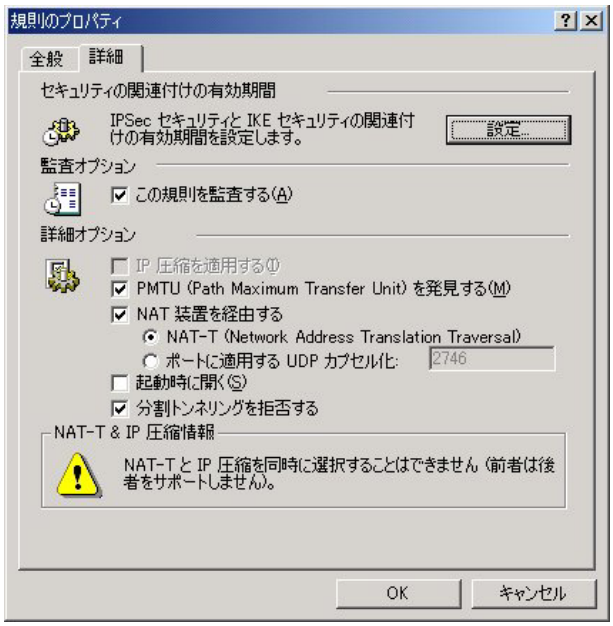
[パラメータの設定]

「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。
それ以外については、任意で設定してください。

VPN Clinentの設定で仮想IPアドレスを使う場合

VPN Clientの設定で、以下のように仮想IPアドレスを設定したとします。

・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」

この場合は、XRの本装置の設定にある「Virtual Private設定」を以下のように設定してください。

%v4：192.168.20.0/24（仮想IPアドレスと同じネットワークアドレスを指定します）

複数のVPN Clinentを接続する場合

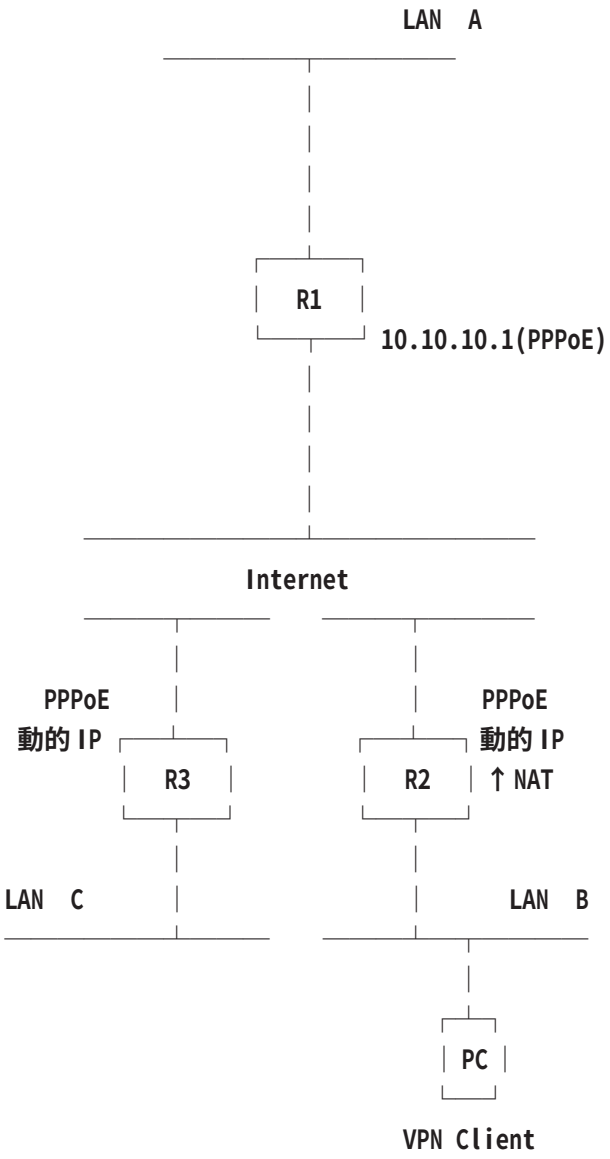
複数のVPN ClientからIPsec接続する場合は、それぞれのVPN Clientに重複しないインタフェースIDを設定してください。

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。

NAT トラバーサルを用いた IPsec 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。

ネットワーク構成



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。

R1 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	%v4:192.168.50.0/2

NAT-T の設定をおこないます。
MTU 値については適宜設定してください。

[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)

R3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]

とくに設定するところはありません。
MTU値については適宜設定してください。

[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

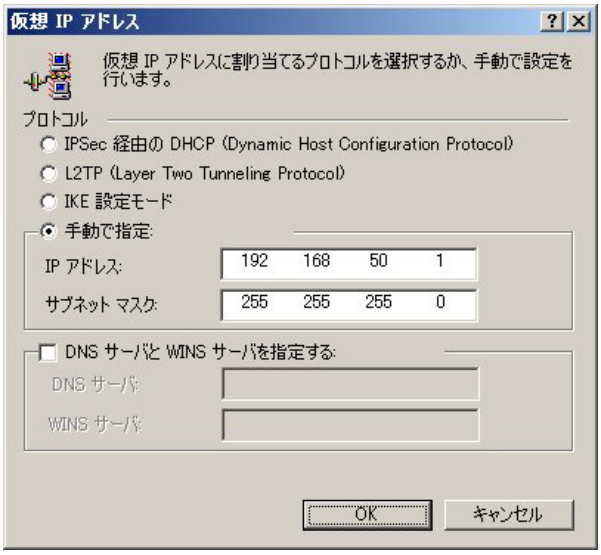
使用するIKEポリシー名の選択	(IKE1)
本装置側のLAN側のネットワークアドレス	192.168.0.0/24 (例：192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.10.0/24 (例：192.168.0.0/24)
PH2のTransFormの選択	すべてを送信する
PFS	○ 使用する ○ 使用しない
DH Groupの選択(PFS使用時に有効)	指定しない
SAのライフタイム	28800 秒 (1081～86400秒まで)
DISTANCE	1 (1～255まで)

VPN Clinentの設定

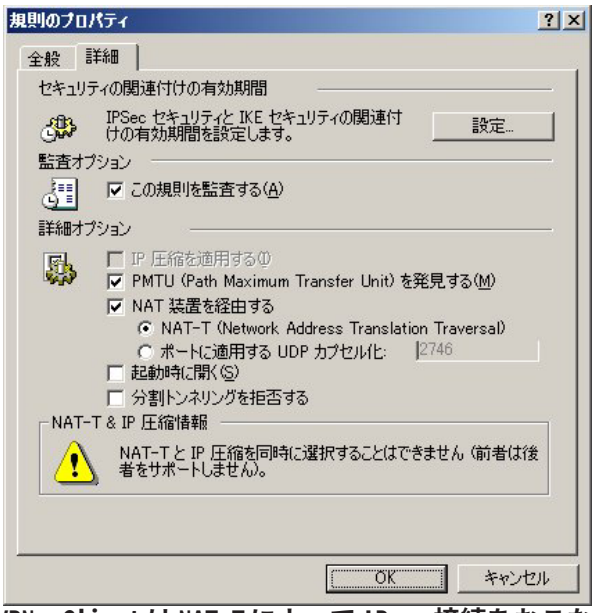
[規則のプロパティ<全般>設定]

「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]

SSH Sentinel のログについて

SSH Sentinel 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 succeeded, 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 bundle 2 with 2 SA's
by rule 21:`ipsec ipv4(any:0,[0..3]
=192.168.100.1)<->ipv4_subnet(any:0,[0..7]
=192.168.1.0/24)(gw:ipv4(any:0,[0..3]
=xxx.xxx.xxx.xxx))'

SA ESP[be022262] alg [3des-cbc/24]+hmac[hmac-
sha1-96] bundle [2,0] pri 0 opts src=ipv4
(any:0,[0..3]=192.168.100.1) dst=ipv4_subnet
(any:0,[0..7]=192.168.1.0/24)

SA ESP[491547c3] alg [3des-cbc/24]+hmac[hmac-
sha1-96] bundle [2,0] pri 0 opts
src=ipv4_subnet(any:0,[0..7]=192.168.1.0/24)
dst=ipv4(any:0,[0..3]=192.168.100.1)
```

SSH Sentinel のログについて

[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 = Authentica-
tion 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。

SSH Sentinel のログについて

[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] / 0xb00c7f69 } 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 XR VPN Client 接続設定ガイド　v1985

2004年5月版

発行 センチュリー・システムズ株式会社