3.応用編

2 の基礎編では文字どうり基本的な接続情報を利用して、SSG に対して VPN 接続することを目的として見てきました。次に応用編としてその他の機能を利用するケースをご紹介いたします。

3-1. 仮想 IP アドレスの利用

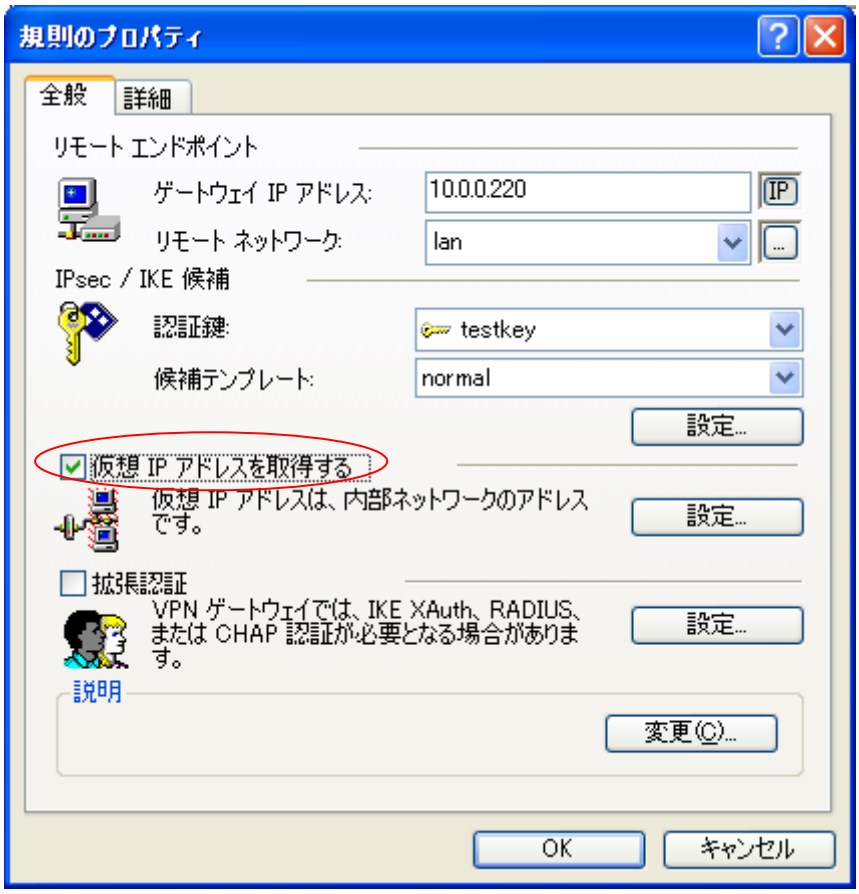
基礎編で設定した内容で VPN 接続を行った場合、VPN Client がインストールされている端末のローカルに割り振られている IP アドレスがそのまま送信元アドレスとなり通信が行われますが、代わりに仮想 IP アドレスを送信元として利用することができます。

また、例えば社内にある DNS サーバや WINS サーバを利用したいといった場合もこの仮想 IP アドレスを設定して利用する形となります。

※利用しない場合の SSG 側のログ（192.168.1.34 が端末ローカルの IP）

| Date/Time | Source Address/Port | Destination Address/Port | Translated Source Address/Port | Translated Destination Address/Port | Service |
|---|---|---|---|---|---|
| 2010-05-21 16:54:38 | 192.168.1.34:17408 | 172.16.32.152:512 | 192.168.1.34:17408 | 172.16.32.152:512 | ICMP |
| 2010-05-21 16:54:37 | 192.168.1.34:17664 | 172.16.32.152:512 | 192.168.1.34:17664 | 172.16.32.152:512 | ICMP |
| 2010-05-21 16:54:37 | 192.168.1.34:17152 | 172.16.32.152:512 | 192.168.1.34:17152 | 172.16.32.152:512 | ICMP |
| 2010-05-21 16:54:36 | 192.168.1.34:16896 | 172.16.32.152:512 | 192.168.1.34:16896 | 172.16.32.152:512 | ICMP |

仮想の IP アドレスを利用するには、まず Secure VPN Client の設定を変更します。

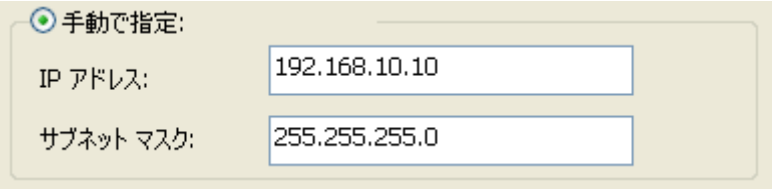



仮想 IP を利用する手段としては数種類選択ができますが、SSG に対しては以下の 2 つが有効です。

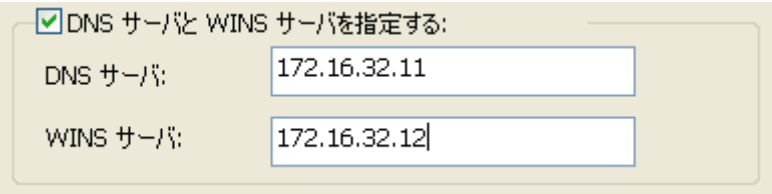
**・手動で設定**
**・IKE 設定モード**

はじめに手動で設定した場合について解説を行います。

○手動で設定
以下のように適当なアドレスを指定し、OK を選択します。ここで設定する IP アドレスは原則として接続先に存在しないサブネット上のアドレスを入力する必要があります。

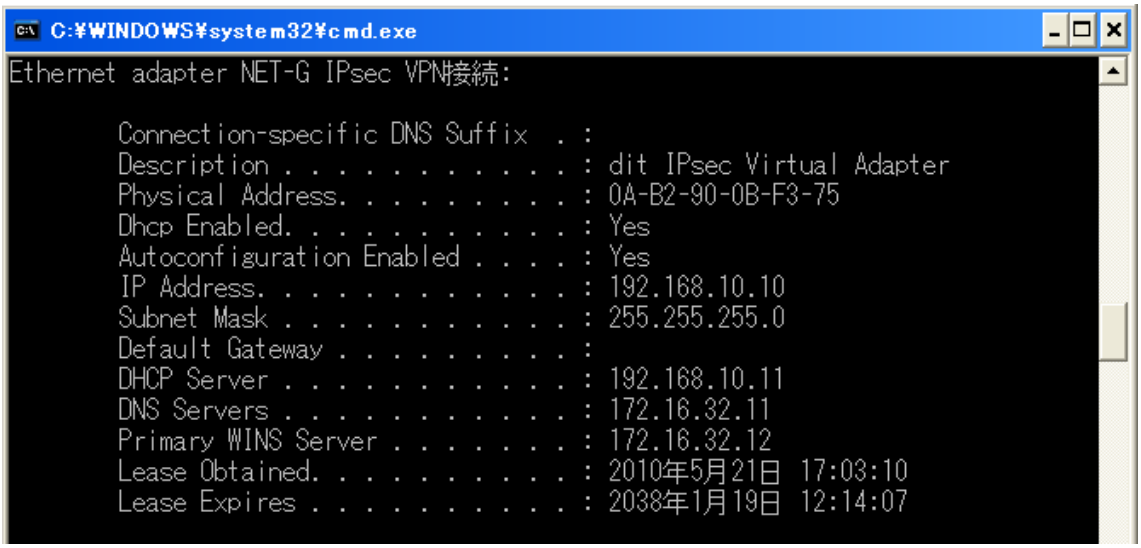



さらに、必要に応じて社内のローカルネットワークにある DNS/WINS サーバの情報も指定することができます。




以上の設定で VPN 接続を行うと仮想インターフェイスが有効となります。

例、VPN 接続後の ipconfig /all を実行した結果




・SSG 側のログ

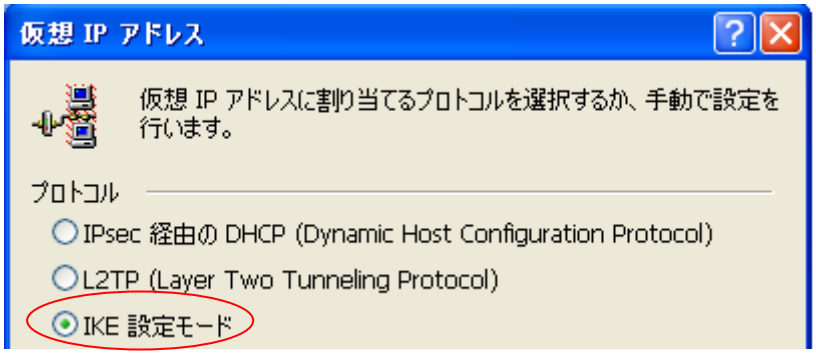
以下のように、設定した仮想 IP アドレスからの通信となりました。

| Date/Time | Source Address/Port | Destination Address/Port | Translated Source Address/Port | Translated Destination Address/Port | Service |
|---|---|---|---|---|---|
| 2010-05-21 17:03:27 | 192.168.10.10:512 | 172.16.32.152:1024 | 192.168.10.10:512 | 172.16.32.152:1024 | ICMP |
| 2010-05-21 17:03:26 | 192.168.10.10:256 | 172.16.32.152:1024 | 192.168.10.10:256 | 172.16.32.152:1024 | ICMP |
| 2010-05-21 16:54:38 | 192.168.1.34:17408 | 172.16.32.152:512 | 192.168.1.34:17408 | 172.16.32.152:512 | ICMP |

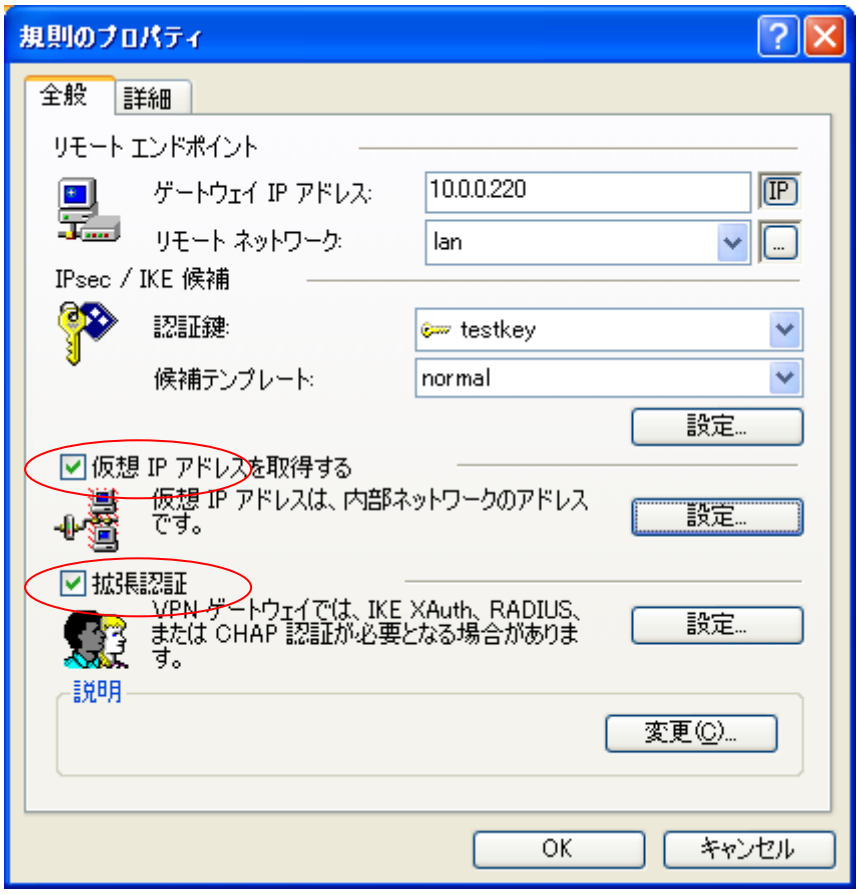
○IKE 設定モード

IKE 設定モードを利用して、VPN 接続時に SSG からアドレスを受け取るという設定をすることも可能となっています。

Secure VPN Client では以下のように”IKE 設定モード”の設定にチェックを入れるだけです。



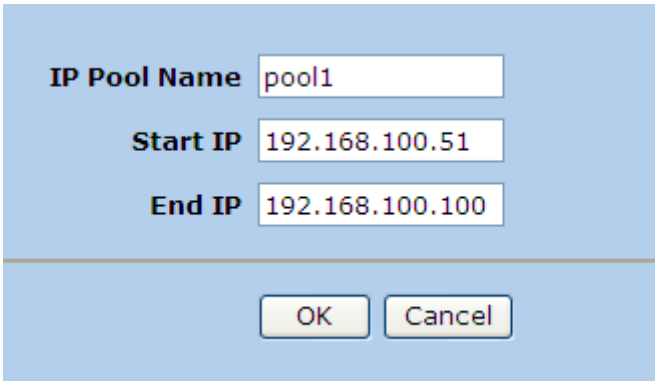

なお、IKE 設定モードは XAuth 機能と併用する必要があるので事前に XAuth を利用する設定を行う必要があります。最終的に VPN Client では以下のような設定となります。




・SSG では下記の設定を追加します。
事前に XAuth の設定が必要となります。まだ設定していない場合は次の項目である”3-2. XAuth を利用したユーザ認証”の設定を実施後、再度本項をご覧ください。

・左欄のメニューより Objects -> IP Pools を選択します。

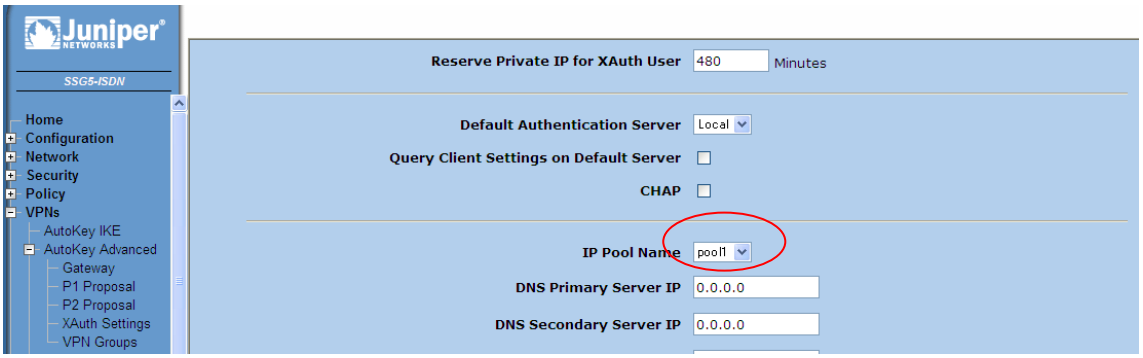
・New を選択し、IP Pool Name に適当な名前を、そして Start IP、End IP として配布する IP アドレスの範囲を指定します。




下記のように追加がされました。

| Name | Start IP | End IP | In use | Configure | |
|---|---|---|---|---|---|
| pool1 | 192.168.100.51 | 192.168.100.100 | 0 | Edit | Remove |

・VPNs -> AutoKey Advanced -> XAuth Settings より、設定した IP Pool の名前を選択します。




DNS サーバや WINS サーバの設定は必要に応じて行ってください。

・設定を変更した後の VPN 接続の手順はこれまでと同じです。IP プールで設定した範囲の IP アドレスが”ipconfig /all”コマンドを実行した結果で割り振られることを確認します。