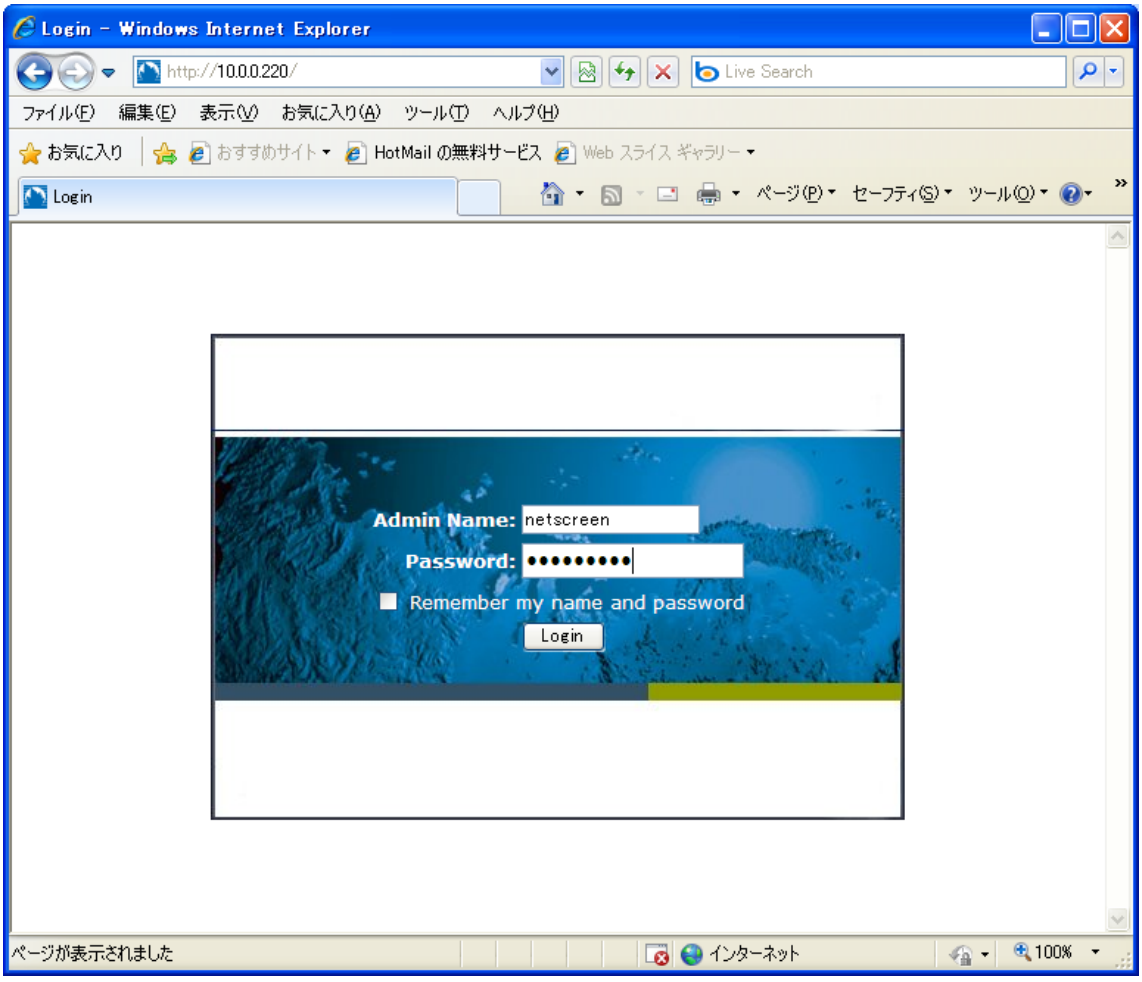
2.基礎編

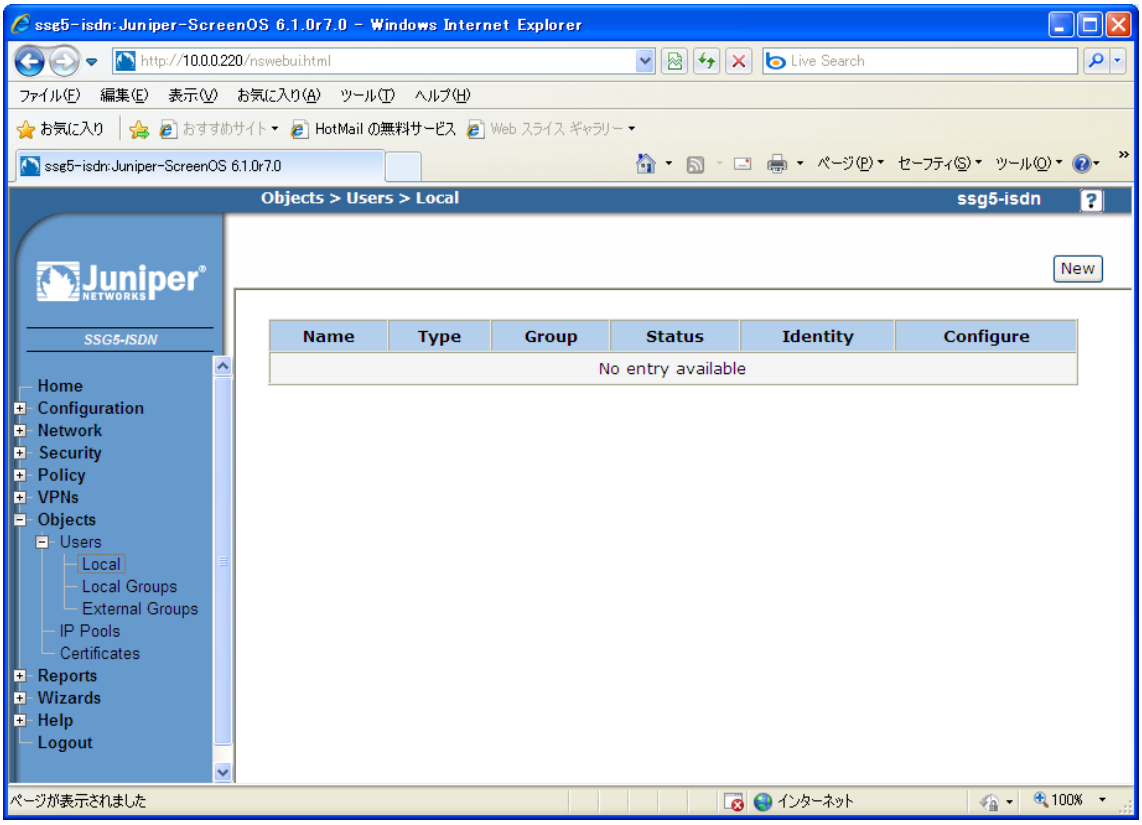
2-1.NetScreen/SSG 側の設定

まず初めに NetScreen/SSG の設定を行います。デフォルト設定の状態から IP アドレス等のネットワークに関する設定は既に済んでいるものとし、ここでは VPN 設定に関連する内容のみを対象としています。

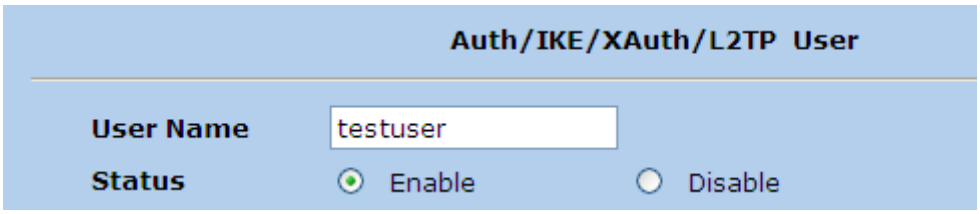
・Web ブラウザで SSG の WebUI にアクセスし、ログインを行います。



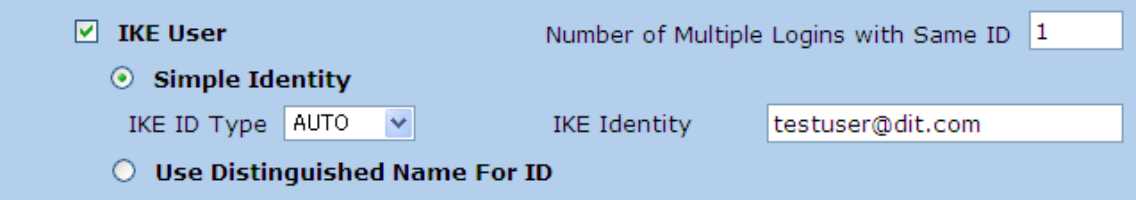
・初めにユーザを作成します。左欄のメニューから Objects -> Users -> Local を選択します。



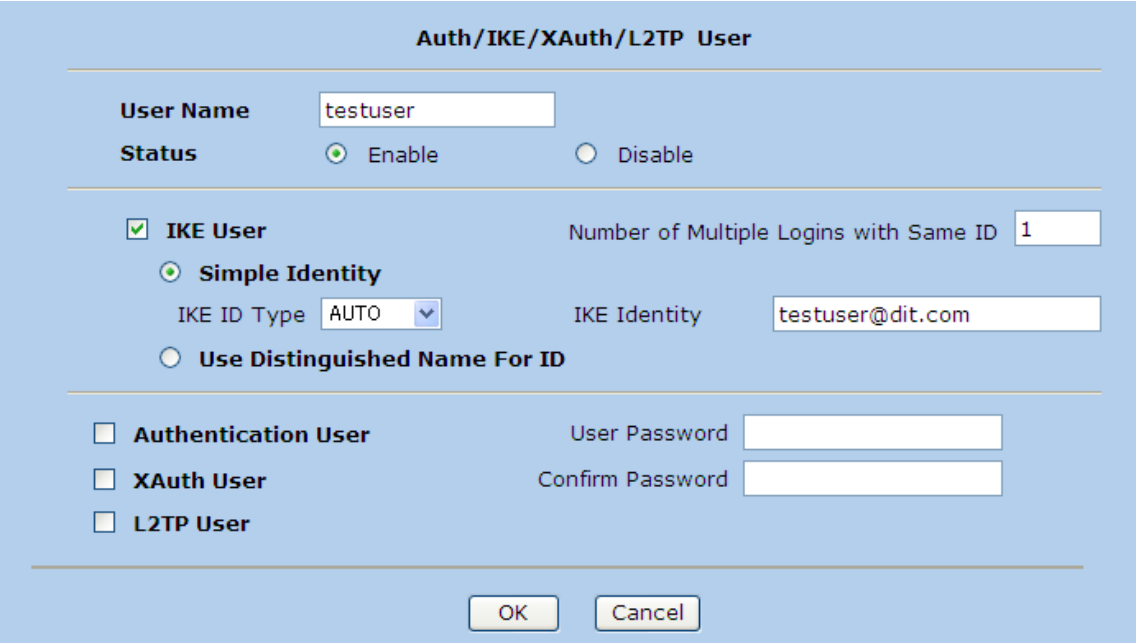
・ページ右上の New を選択し、User Name の欄に任意の名前でユーザ名を設定します。



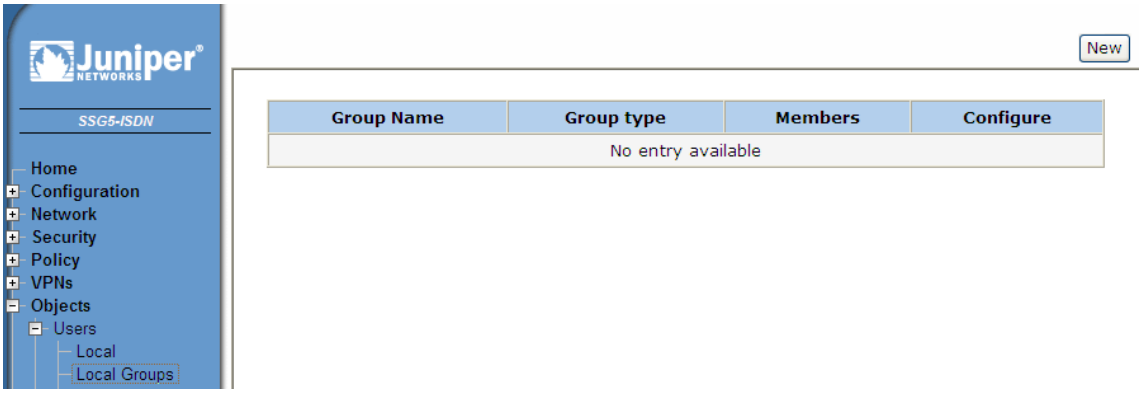
ついで、IKE User にチェックを入れ、Simple Identity を選び内容としてメールアドレスを設定します。



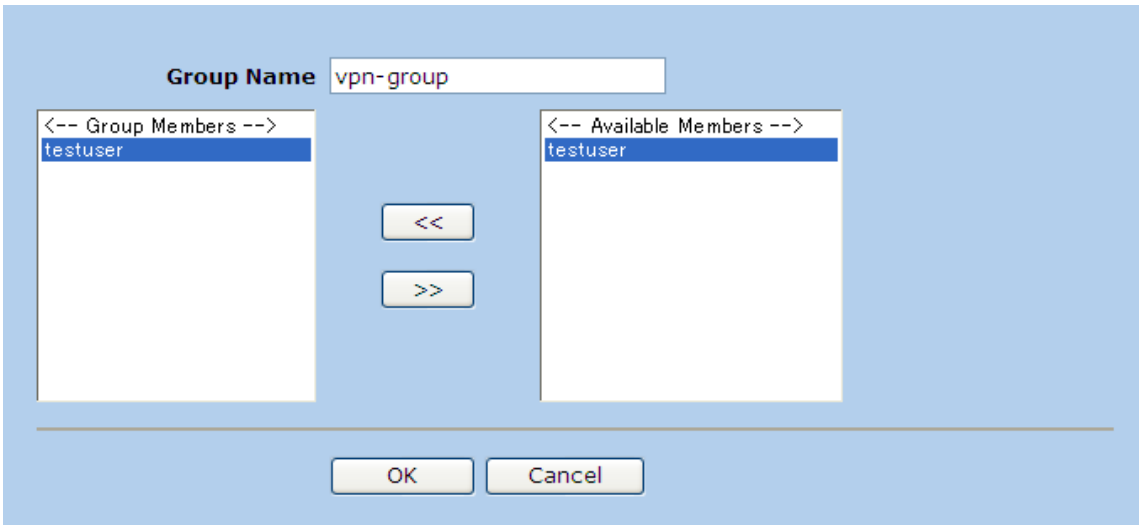
入力を終えたら、OK を選択します。



・ついで、Objects -> Users -> Local Groups を選択します。



ページ右上の New を選択し、Group Name にグループ名を入力し、同時に先に作成したユーザをグループに追加します。

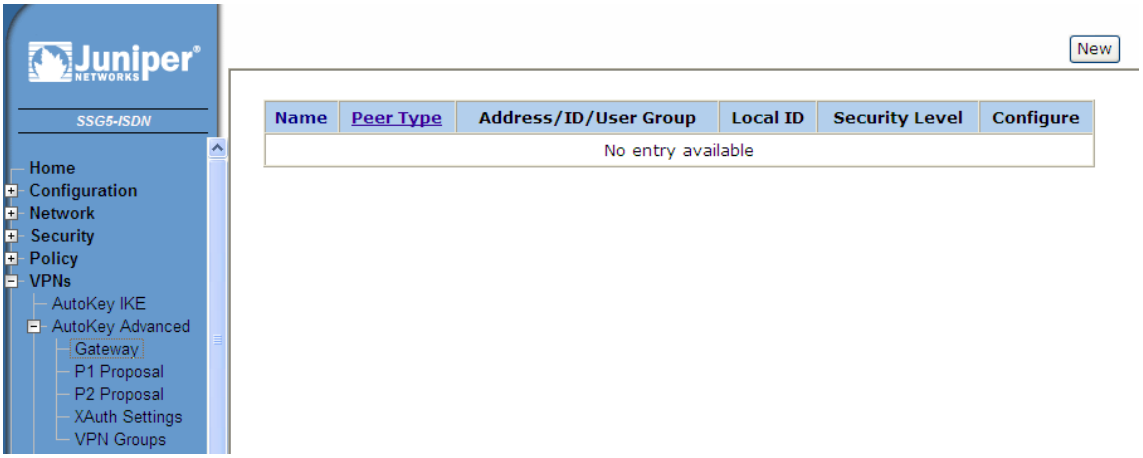


OK を押して前画面に戻ると下記のようにグループが作成されます。Members にユーザが追加されていることを確認してください。

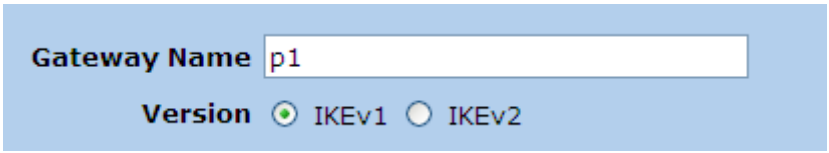
Group Name	Group type	Members	Configure	
vpn-group	ike	testuser	Edit	Remove

今後発生する設定変更のために適当な内容で構わないのでもう一つユーザを作成しグループに追加しておくことをお勧めします。

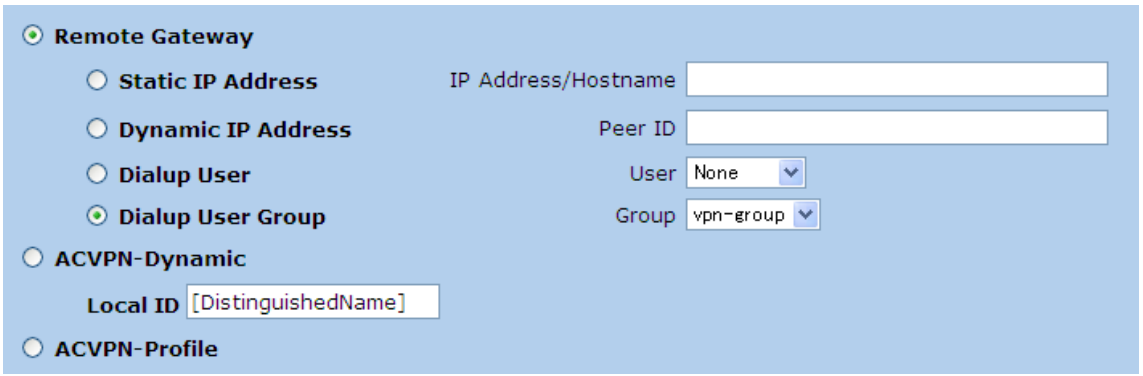
・左欄のメニューから VPNs -> AutoKey Advanced -> Gateway を選択し、IKE のフェーズ 1 にあたる設定を行います。



・ページ右上の New を選択し、Gateway Name として適当な名前を入力します。IKE のバージョンは IKEv1 となります、Secure VPN Client は IKEv2 には対応していません。



Remote Gateway として Dialup User Group をチェックし、先に作成したグループを選択するようにします。



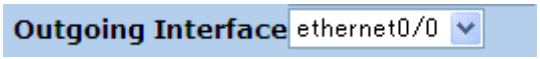
※特定のユーザのみを指定する場合は、下記のように Dialup User でユーザ名を選びます。

そのまま、Advanced を選択します。

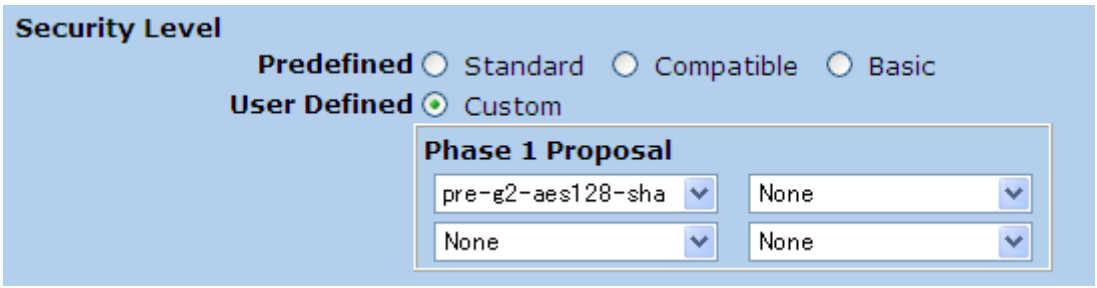
Preshared Key に任意の値の文字列を設定します。

※後ほど Secure VPN Client 側にも同じ内容を設定するので控えておいてください。

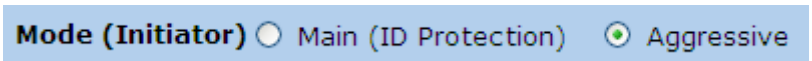
Outgoing Interface として、Untrust のゾーンに割り当てているインターフェイスを選択します。



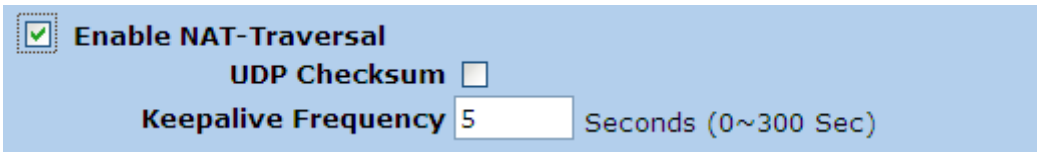
Security Level の内容として User Defined を Custom とし、Phase 1 Proposal を
下記のように選びます。利用する環境に応じて別の暗号方式を選んでも構いませんが、
共有鍵認証の場合は pre で始まるものを選択します。



Mode(Initiator)は、Aggressive を選びます。



“Enable NAT-Traversal”にチェックをつけます。



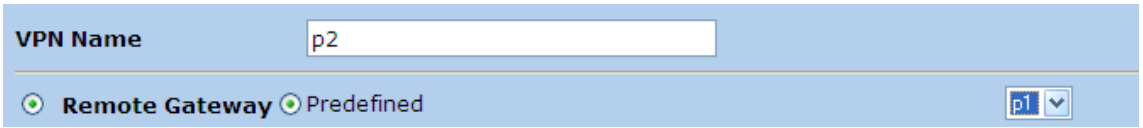
・他の内容はデフォルトのままで Return を選択し、前の画面に戻り、OK を押します。下記のようになっていることを確認します。

Name	Peer Type	Address/ID/User Group	Local ID	Security Level	Configure		
p1	Dialup	vpn-group	-	Custom	Edit	Xauth	Remove

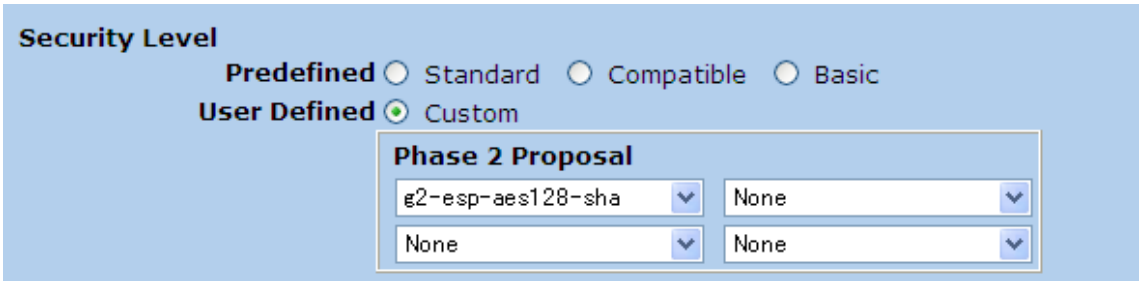
・続いて VPNs -> AutoKey IKE より、IKE フェーズ 2 にあたる設定を行います。

・ページ右上の New を選択し、VPN Name に適当な名前を入力します。

Remote Gateway は Predefined として、先に設定したフェーズ 1 の内容を選択します。



下欄より Advanced を選択し、Security Level を Custom として、任意の暗号方式等を選択します。

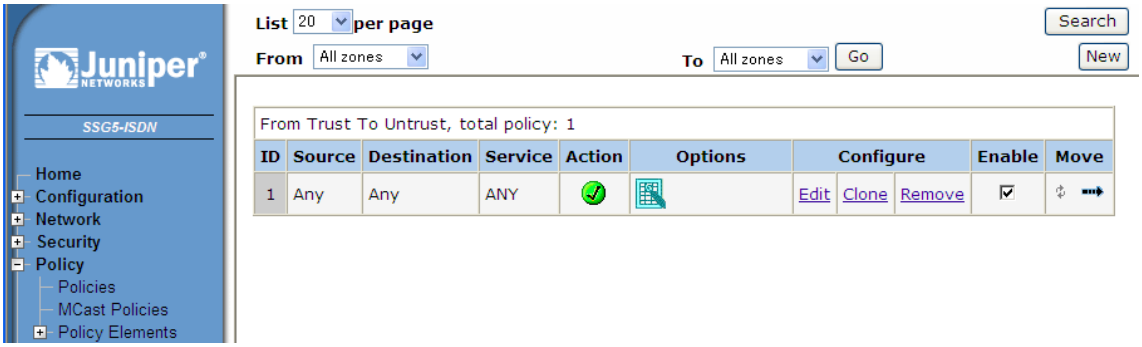


・他の内容をデフォルトのままでページ下欄の Return を選択します。

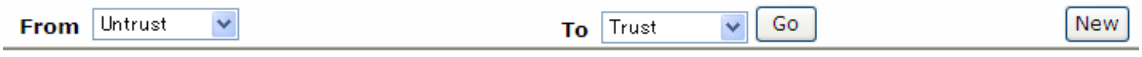
OK を押して、前の画面に戻って設定が追加されていることを確認します。

Name	Gateway	Security	Monitor	Configure	
p2	p1	Custom	Off	Edit	Remove

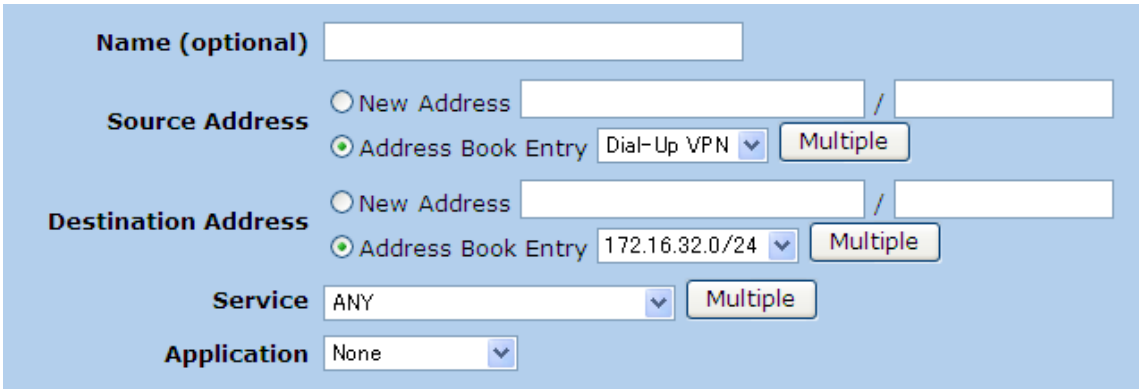
・左欄のメニューから Policy -> Policies を選択します。



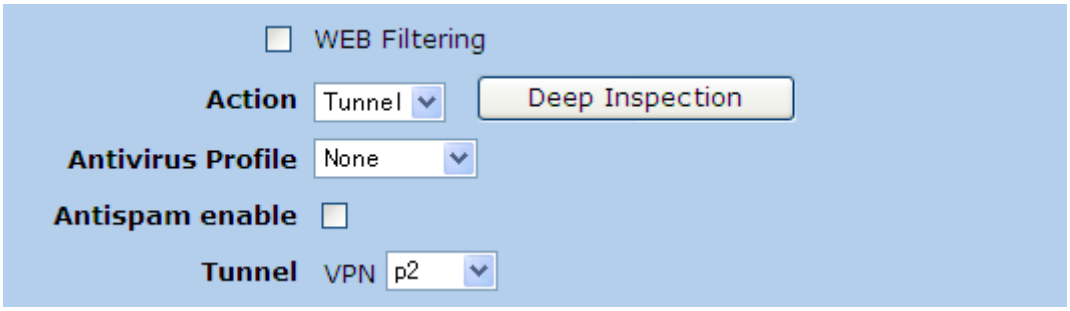
・下記のように From で Untrust、To で Trust を選択し、New を選びます。



・Source Address には Dialup を、Destination Address には trust 側に当たるネットワークをそれぞれ指定します。



Action では Tunnel を、Tunnel では VPN として設定した”p2”を選択します。



・OK を選択し、”From Untrust to Trust”のポリシー項目に Action が鍵マークのトンネルのポリシーが追加されていることを確認します。

From Trust To Untrust, total policy: 1

ID	Source	Destination	Service	Action	Options	Configure			Enable	Move
1	Any	Any	ANY			Edit	Clone	Remove	☑	

From Untrust To Trust, total policy: 1

ID	Source	Destination	Service	Action	Options	Configure			Enable	Move
2	Dial-Up VPN	172.16.32.0/24	ANY			Edit	Clone	Remove	☑	

ついで、2-2.NET-G Secure VPN Client の設定を行います。