7.4 NetScreen/SSG側の設定

前のセクションで，PC側の設定が終わりました．このセクションでは，NetScreen/SSG側の設定について説明します．

7.4.1 ２つのIPアドレス払い出し方法

設定に入る前に，IPアドレスの2通りの払い出し（割り振り）方法について説明します．IPアドレスの払い出し方法には，IP PoolとDIPの2つがあります．

①IP Pool

内部ネットワークと払い出すIPのネットワークを分ける方式です．払い出すIPアドレスを分離することで，セキュリティ強化が図れます．IPアドレスを分けているため，IPフィルタによるセキュリティ設定ができるからです．

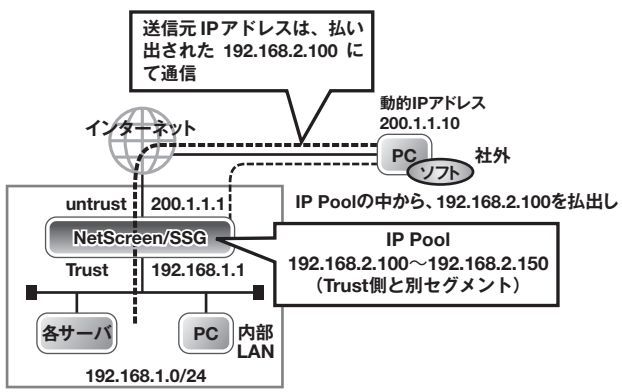


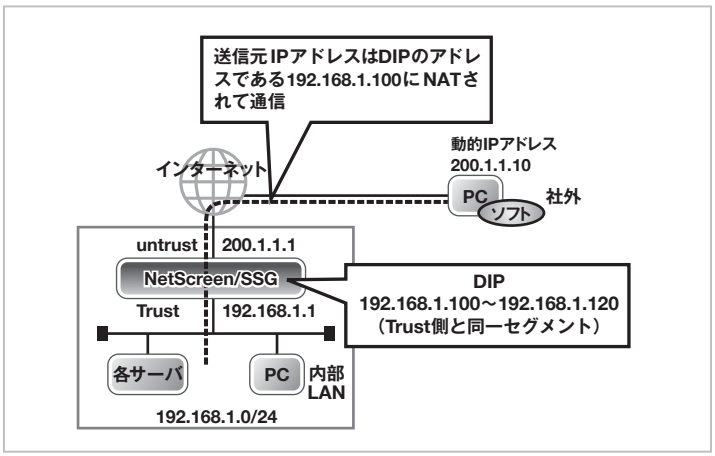
図 7-15
IP Poolのイメージ図

②DIP

内部ネットワークと払い出すIPのネットワークを同一にする方式です．払い出すIPアドレスが同一ネットワークであるため，リモートから接続であっても，あたかも社内LANにいるかのように通信が行えます．社内のネットワークや各種サーバの設定変更も必要ありません．

ただし，同一ネットワークということは，ファイアウォールによるフィルタリングが行いにくくなります．その点を注意して利用しましょう．

図 7-16
DIPのイメージ図



7.4.2　実際の設定

NetScreenは各種設定が終わり，インターネットに接続されているものとします．今回は，DIPによる設定を説明します（IP Poolに関しては「7.7　IP Poolの設定」にて説明します）．

設定の流れは次のようになります．

✚ 設定の流れ

①DIPの設定
②ユーザの作成
③Phase1の設定
④Phase2の設定
⑤Policiesの設定

✚ 設定環境

今回の設定パラメータは以下です.

- DIP：192.168.1.100～192.168.1.120
- User Name：user1
- IKE Identity：user1@viva-netscreen.net
- VPN Name：VPN-Remote
- security level：custom（g2-esp-3des-md5）
- Gateway Name：GW-Remote
- Preshared Key：netscreen
- Policy：Dial-Up VPN→192.168.1.0/24

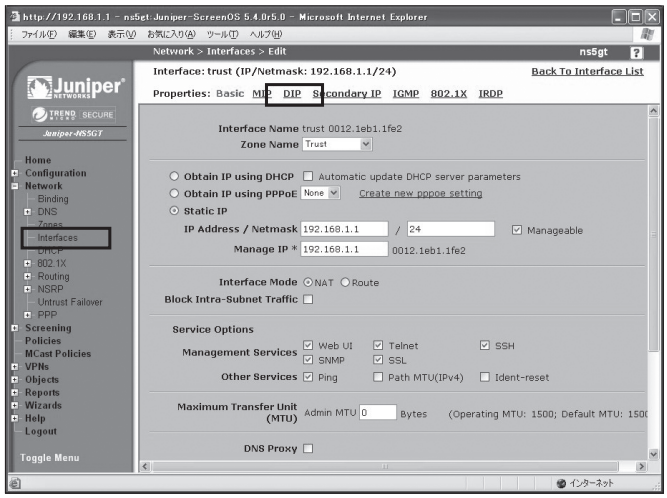
ここからは，NetScreen/SSGの設定を画面を含めて説明します.

①DIPの設定

（1）メニューからNetwork ＞ Interfacesを開き，「trust」のインターフェースの「edit」をクリックします.

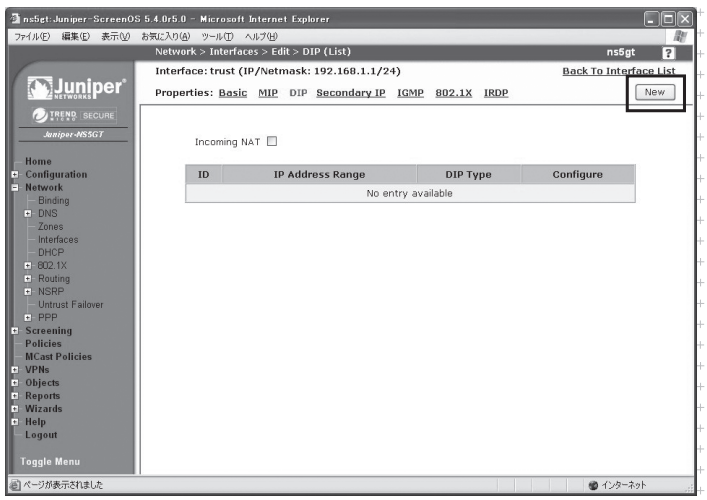
(2) 上部にある「DIP」をクリックします.

図 7-17
Network > Interfaces > Edit



(3) DIP (List) の画面が開きますので,「New」をクリックします.

図 7-18
Network > Interface > Edit > DIP (List)



(4) DIPの設定を行います.

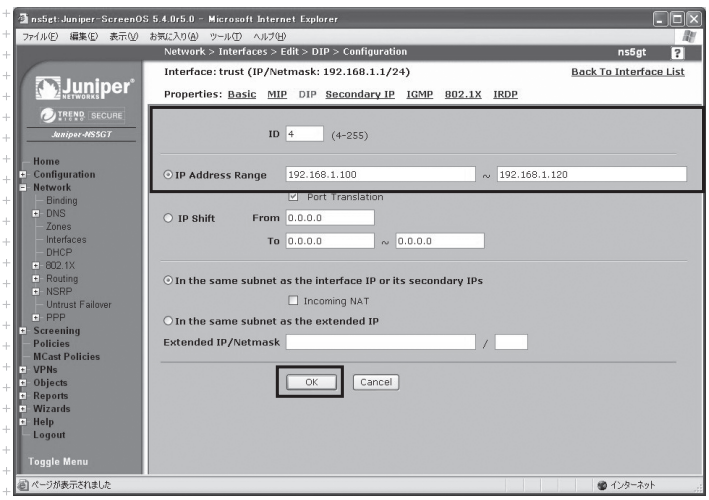


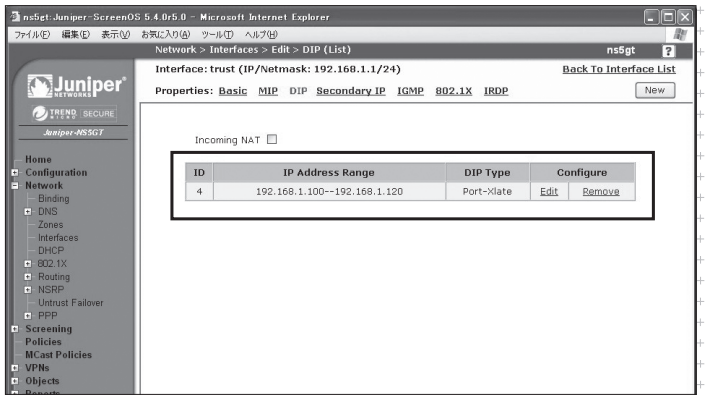
図 7-19
Network > Interfaces > Edit > DIP > Configuration

・ ID：自動で割り当てられます. Policiesを作成するときに, このIDを割り当てます
・ IP Address Range：割り当てるIPアドレスを指定してください. 今回のケースは192.168.1.100～192.168.1.120です※3

※3：Trust側と同一セグメントで設定してください.

(5)「OK」をクリックすると設定完了です.

図 7-20
Network > Interface > Edit > DIP (List)



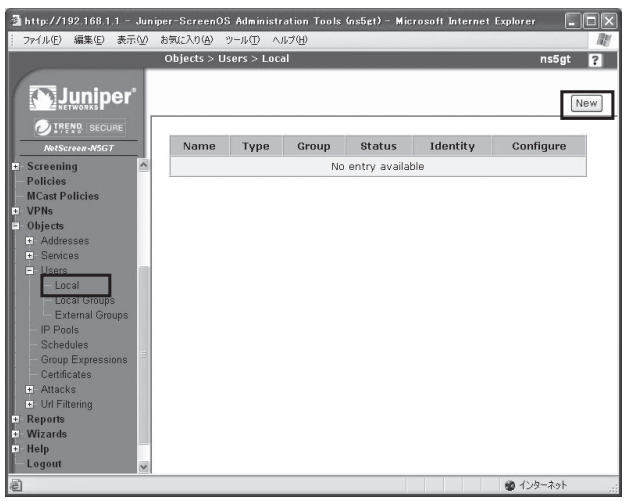
DIPが正しく設定されているかを確認してください.

②ユーザの作成

リモートアクセスを許可するユーザを作成します.

（1）メニューからObjects > Users > Localを開きます.

図 7-21
Objects > Users > Local



(2) 画面右上の「New」をクリックします.

(3) Userの設定を行います.

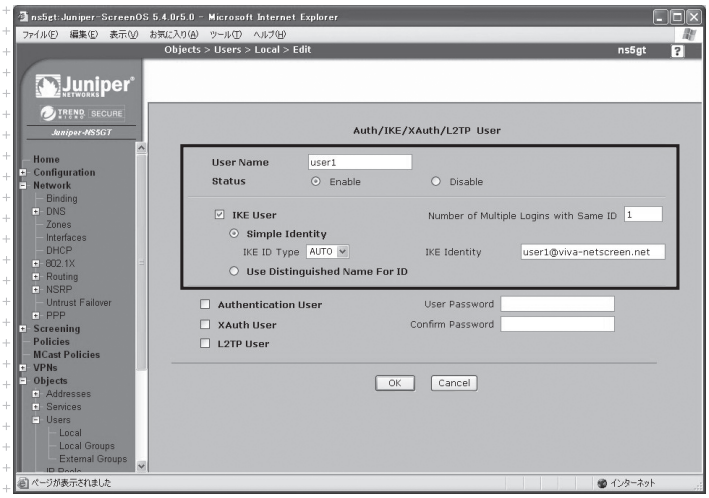


図 7-22
Objects > Users > Local > Edit

- User Name：ユーザ名を入力してください. 今回はuser1
- Status：Enable
- IKE User：チェックします.
- IKE Identity：ユーザのメールアドレス※4. 今回はuser1@viva-netscreen.net

※4：IKE IDはメールアドレス以外でも良いのですが，クライアントソフト側のE-mail Addressという設定と合わせています.

(4) OKを押して，ユーザ登録の完了です.

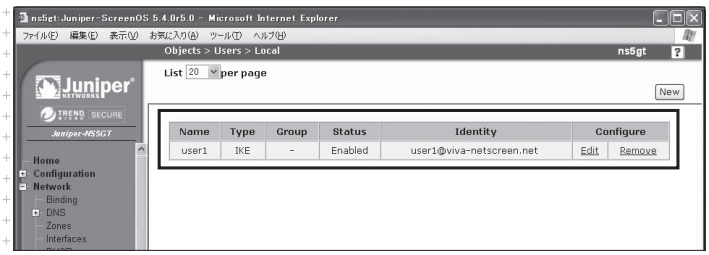


図 7-23
Objects > Users > Local > Edit

ユーザが正しく設定されているかを確認してください.

③Phase1の設定

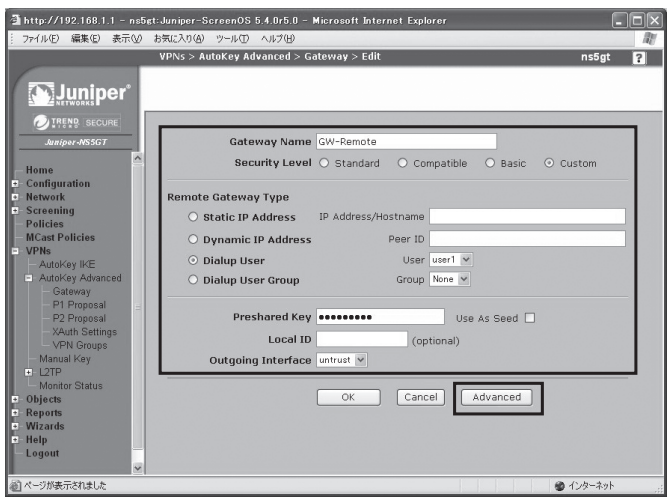
（1）メニューからVPNs > AutoKey Advanced > Gatewayを開きます.

図 7-24
VPNs > AutoKey Advanced > Gateway

（2）画面右上の「New」をクリックします.

（3）Gatewayの設定をします.

図 7-25
VPNs > AutoKey Advanced > Gateway > Edit



・Gateway Name：わかりやすい名前を入力します．今回はGW-Remote
・Security Level：Custom※5
・Remote Gateway Type：Dialup Userとし，先ほど作成したユーザを選択します．ここではuser1
・Preshared Key：Preshared Keyを入力します．ここではnetscreen
・Outgoing Interface：「untrust」に設定します．

※5：Customの詳細な設定は，「Advanced」にて設定します．

(4)「Advanced」をクリックします．
(5)「Advanced」の設定を行います．

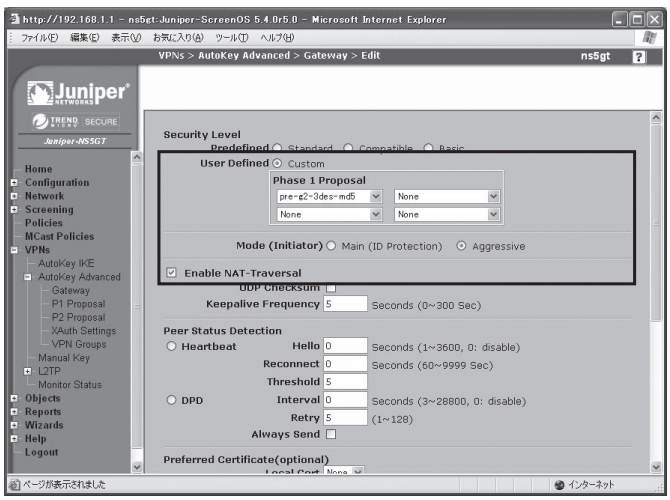


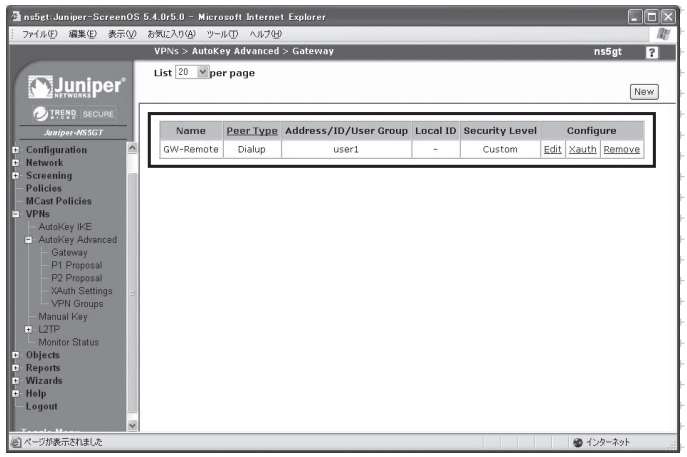
図 7-26
VPNs > AutoKey Advanced > Gateway > Edit (Advanced)

・Security Level：Customになっているかを確認し，プルダウンから「pre-g2-3des-md5」を選択
・Mode (Initiator)：Aggressive
・Enable NAT-Traversal：必要に応じてチェックを入れます※6

※6：詳しくは，後述する補足説明「NAT Traversalについて」にて説明します．

(6)「Return」をクリックして前の画面に戻り,「OK」をクリックすると設定完了です.

図 7-27
VPNs > AutoKey Advanced > Gateway

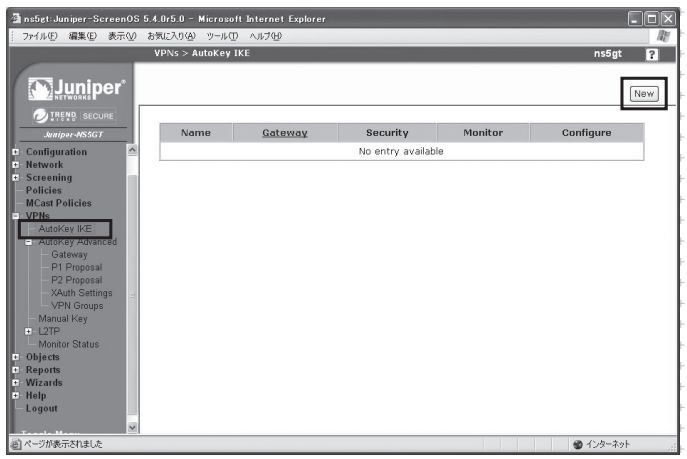


Gatewayが正しく設定されているかを確認してください.

④Phase2の設定

(1) メニューからVPNs > AutoKey IKEを開きます.

図 7-28
VPNs > AutoKey IKE



(2) 画面右上の「New」をクリックします.

(3) VPNの設定をします.

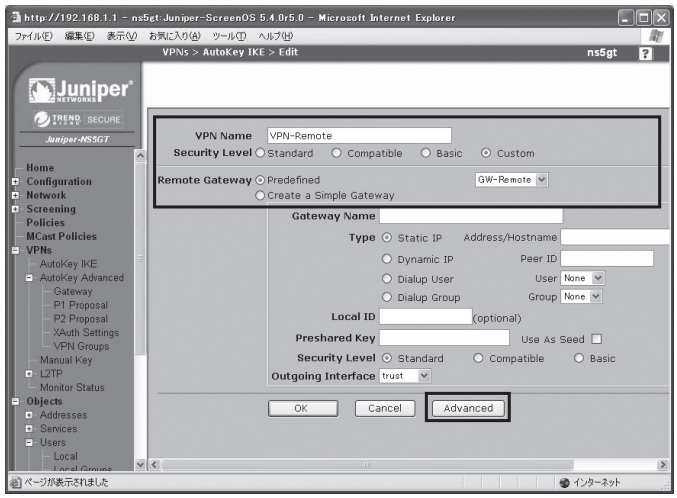


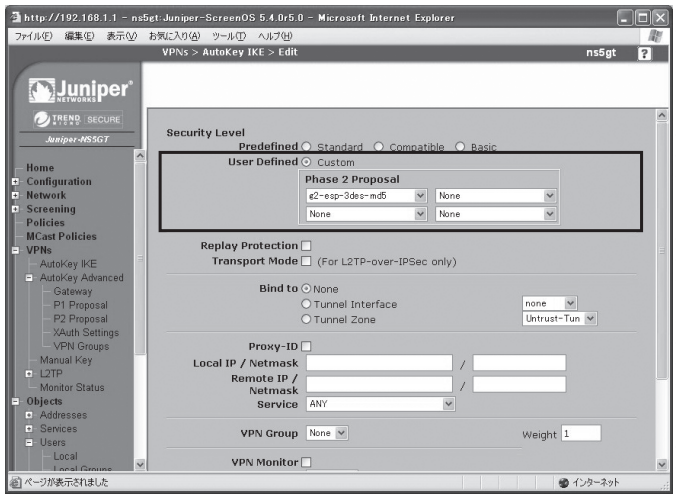
図 7-29
VPNs > AutoKey IKE > Edit

- VPN Name： わかりやすい名前を入力します. ここではVPN-Remote
- Security Level：「Custom」を選択します.
- Remote Gateway：「Predefined」がチェックされていることを確認し, 先ほどのPhase1で作成した「GW-Remote」を選択します.

(4)「Advanced」をクリックします.

(5)「Advanced」の設定を行います.

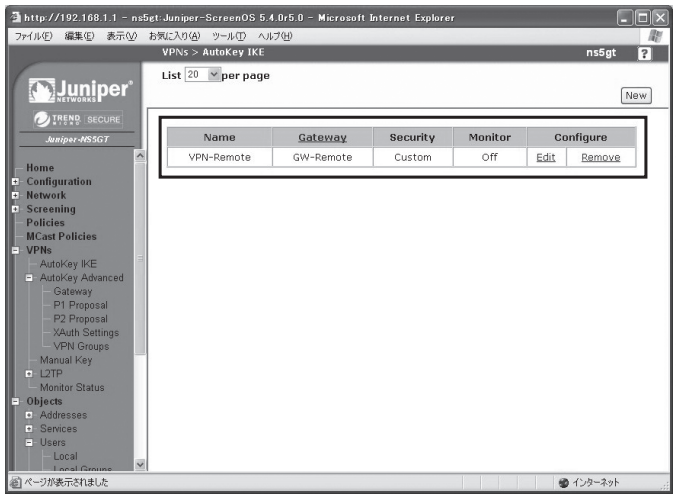
図 7-30
VPNs > AutoKey IKE > Edit(Advanced)



・ Security Level：「Custom」になっていることを確認します
・ Phase 2 Proposal：「g2-esp-3des-md5」を選択します

(6)「Return」をクリックして前の画面に戻り，「OK」をクリックすると設定完了です.

図 7-31
VPNs > AutoKey IKE



VPNが正しく設定されているかを確認してください.

⑤Policiesの設定

(1) メニューからPoliciesを開きます.

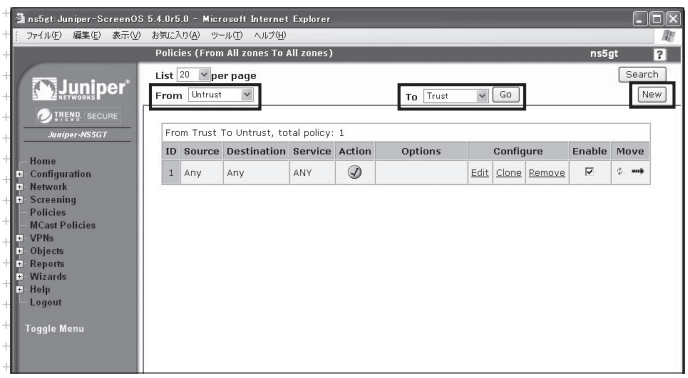


図 7-32
Policies
(From Untrust To Trust)

(2) Fromを「Untrust」, Toを「Trust」として「New」をクリックします※7.

(3) Policiesの設定をします.

※7：Untrust（インターネット）からTrust（内部LAN）への通信なので，このポリシーを作成します.

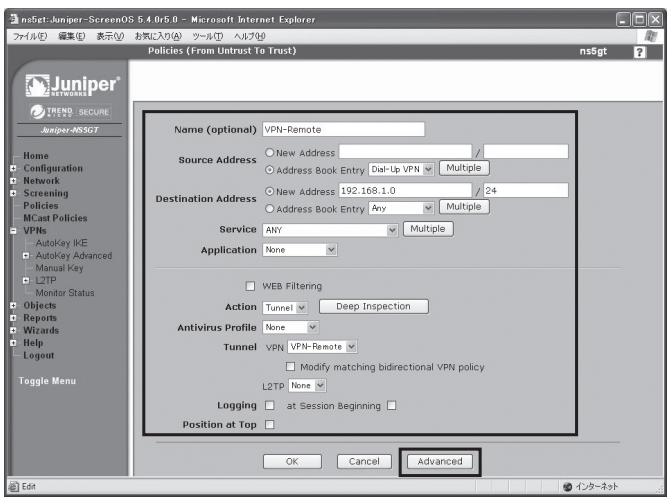
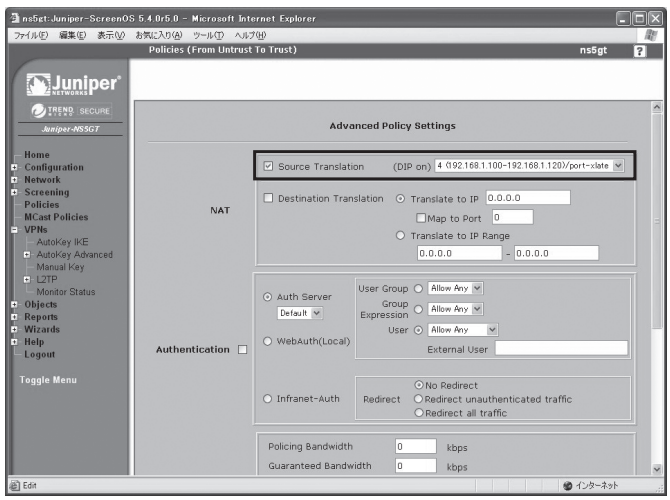


図 7-33
Policies
(From Untrust To Trust)

・Name：わかりやすい名前を入力します（省略可能）．今回はVPN-Remote
・Source Address：「Dial-Up VPN」を選択します
・Destination Address：LANのセグメントを入力します．今回は192.168.1.0/24
・Action：「Tunnel」を選択します
・Tunnel：作成した「VPN-Remote」を選択します

（4）「Advanced」をクリックします．
（5）NATの設定をします．

図 7-34
Policies (From Untrust To Trust)
Edit(Advanced)



・Source Translation：チェックを入れます
・（DIP On）：先ほど作成したDIPを選択します．今回はIDが4のDIPです

(6)「OK」をクリックすると設定完了です.

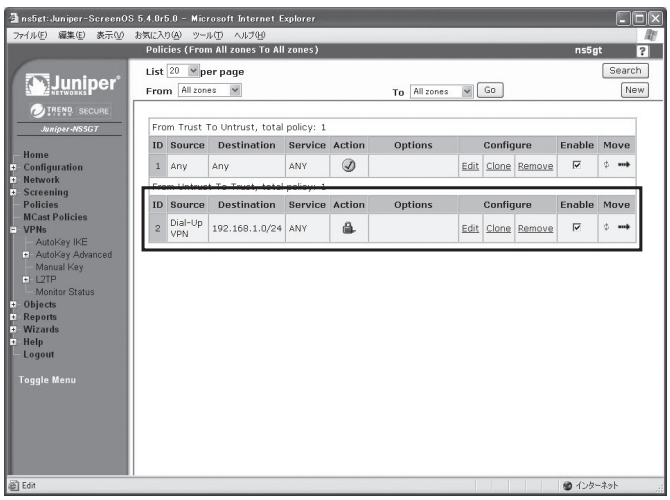


図 7-35
Policies (From Untrust To Trust)

VPNが正しく設定されているかを確認してください. 今回の設定のConfigは次のようになります(該当部分のみ).

❶ DIPの設定

```
set interface trust dip 4 192.168.1.100 192.168.1.120
```

❷ ユーザの作成

```
set user "user1" uid 1
set user "user1" ike-id u-fqdn "user1@viva-netscreen.net" share-limit 1
set user "user1" type  ike
set user "user1" "enable “
```

❸ Phase1の設定

```
set ike gateway "GW-Remote" dialup "user1" Aggr outgoing-interface "untrust" preshare “netscreen"
proposal "pre-g2-3des-md5"
 set ike gateway "GW-Remote" nat-traversal keepalive-frequency 5
```

実際には暗号化されます

❹ Phase2の設定

```
set vpn "VPN-Remote" gateway "GW-Remote" no-replay tunnel idletime 0 proposal "g2-esp-3des-md5"
```

❺ Policiesの設定

```
set policy id 2 name "VPN-Remote" from "Untrust" to "Trust"  "Dial-Up VPN" "192.168.1.0/24" "ANY" nat src dip-id 4 tunnel vpn "VPN-Remote" id 6
```