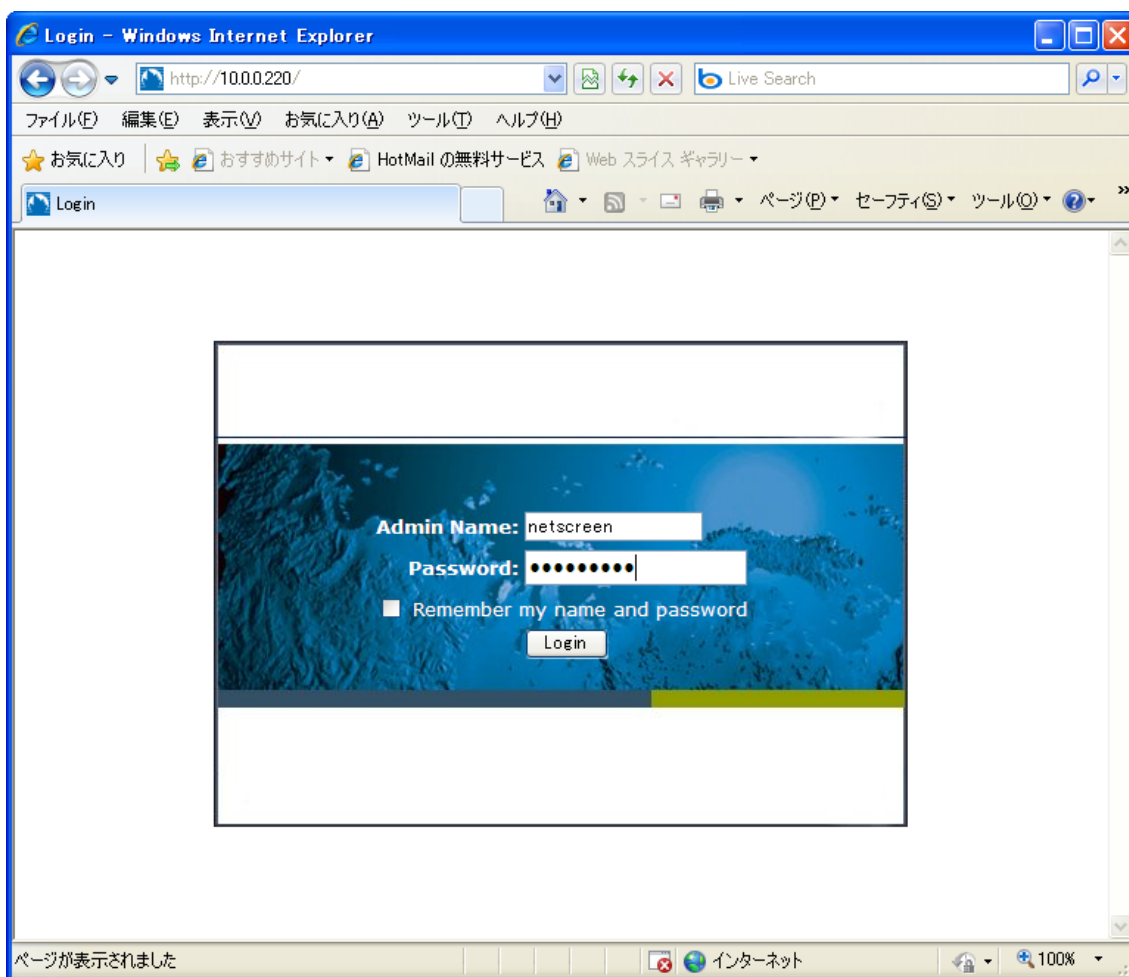


2.基礎編

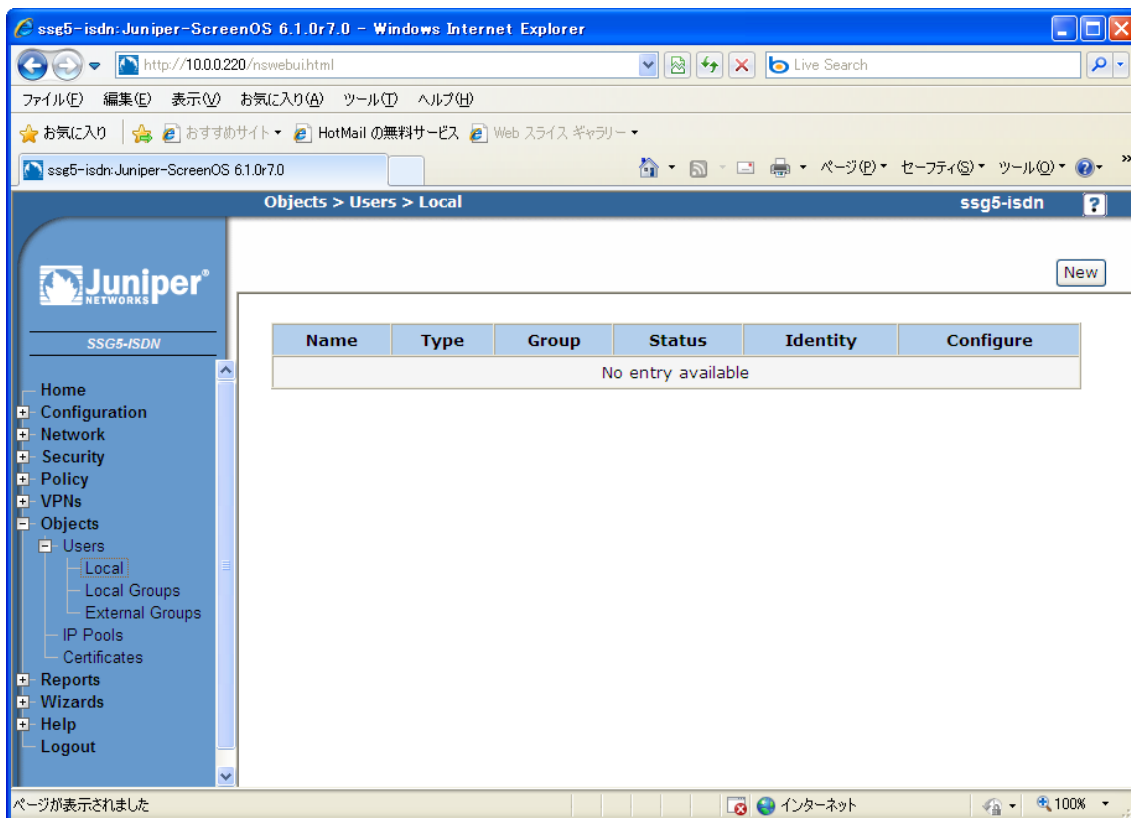
2-1.NetScreen/SSG 側の設定

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。

The screenshot shows a configuration form titled 'Auth/IKE/XAuth/L2TP User'. The form has two main sections. The first section is 'User Name', which has a text input field containing 'testuser'. The second section is 'Status', which has two radio buttons: 'Enable' (which is selected) and 'Disable'.

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。

IKE User Number of Multiple Logins with Same ID

Simple Identity

IKE ID Type IKE Identity

Use Distinguished Name For ID

入力を終わったら、OK を選択します。

Auth/IKE/XAuth/L2TP User

User Name

Status Enable Disable

IKE User Number of Multiple Logins with Same ID

Simple Identity

IKE ID Type IKE Identity

Use Distinguished Name For ID

Authentication User User Password

XAuth User Confirm Password

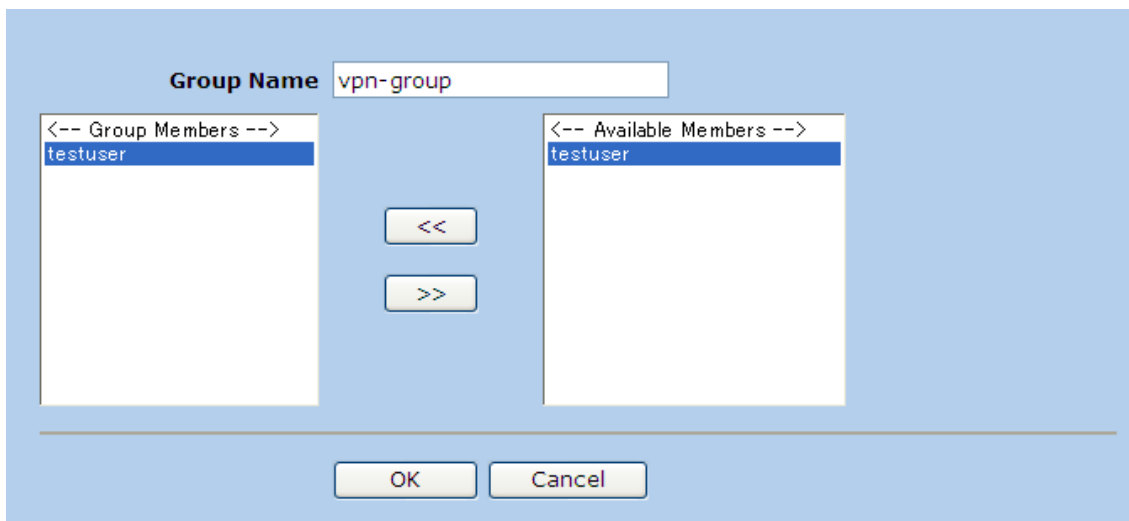
L2TP User

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

The screenshot shows the Juniper Networks configuration interface. On the left is a navigation tree with the following items: Home, Configuration, Network, Security, Policy, VPNs, Objects, Users, Local, and Local Groups. The 'Local Groups' item is highlighted. In the main area, there is a 'New' button in the top right corner and a table with the following structure:

Group Name	Group type	Members	Configure
No entry available			

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。



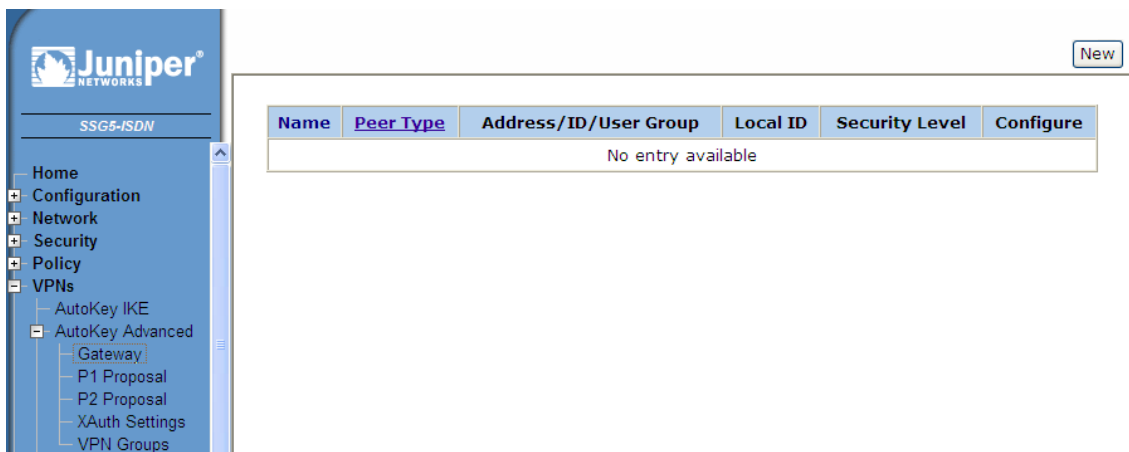
The screenshot shows a configuration window with a light blue background. At the top, there is a text input field labeled 'Group Name' containing the text 'vpn-group'. Below this, there are two list boxes. The left one is titled '<-- Group Members -->' and contains the text 'testuser'. The right one is titled '<-- Available Members -->' and also contains 'testuser'. Between these two list boxes are two buttons: '<<' and '>>'. At the bottom of the window, there are two buttons: 'OK' and 'Cancel'.

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。

Gateway Name

Version IKEv1 IKEv2

- 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。

Remote Gateway

Static IP Address IP Address/Hostname

Dynamic IP Address Peer ID

Dialup User User

Dialup User Group Group

ACVPN-Dynamic

Local ID

ACVPN-Profile

※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。

Dialup User User

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。

Preshared Key Use As Seed

※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。

Outgoing Interface

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。

Security Level

Predefined Standard Compatible Basic

User Defined Custom

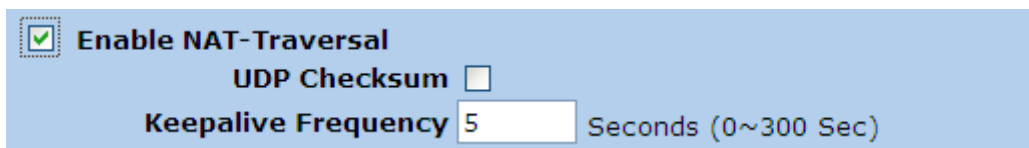
Phase 1 Proposal

<input type="text" value="pre-g2-aes128-sha"/>	<input type="text" value="None"/>
<input type="text" value="None"/>	<input type="text" value="None"/>

Mode(Initiator)は、Aggressive を選びます。

Mode (Initiator) Main (ID Protection) Aggressive

“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。

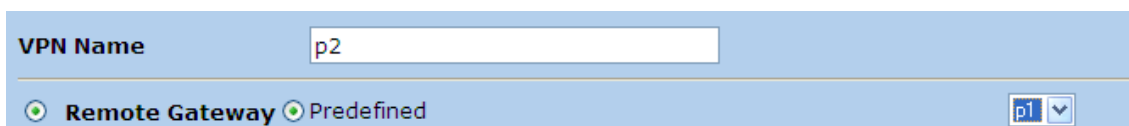
Name	Peer Type	Address/ID/User Group	Local ID	Security Level	Configure
p1	Dialup	vpn-group	-	Custom	Edit Xauth Remove

・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。

Security Level

Predefined Standard Compatible Basic

User Defined Custom

Phase 2 Proposal

g2-esp-aes128-sha	None
None	None

・他の内容をデフォルトのままページ下欄の 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。

Juniper NETWORKS
SSG5-ISDN

Home
+ Configuration
+ Network
+ Security
+ Policy
- Policies
- MCast Policies
+ Policy Elements

List 20 per page

From All zones To All zones Go

Search New

From Trust To Untrust, total policy: 1

ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
1	Any	Any	ANY			Edit Clone Remove	<input checked="" type="checkbox"/>	

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

From Untrust To Trust Go New

・ 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。

The screenshot shows a configuration form with the following fields and values:

- Name (optional)**: [Empty text box]
- Source Address**: New Address [Empty] / [Empty]; Address Book Entry: Dial-Up VPN [Multiple]
- Destination Address**: New Address [Empty] / [Empty]; Address Book Entry: 172.16.32.0/24 [Multiple]
- Service**: ANY [Multiple]
- Application**: None

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

The screenshot shows the following configuration options:

- WEB Filtering
- Action**: Tunnel [Deep Inspection]
- Antivirus Profile**: None
- Antispam enable**:
- Tunnel**: VPN p2

・ 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	<input checked="" type="checkbox"/>		
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	<input checked="" type="checkbox"/>		

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