VPN Tracker for Mac OS X

How-to:

Interoperability with

NetScreen

Internet Security Appliances

Rev. 4.0

1. Introduction

This document describes how VPN Tracker can be used to establish a connection between a Macintosh running Mac OS X and a NetScreen Internet Security Appliance.

The NetScreen is configured as a router connecting a company LAN to the Internet.

This paper is only a supplement to, not a replacement for, the instructions that have been included with your NetScreen. Please be sure to read those instructions and understand them before starting.

2. Prerequisites

First you have to make sure that your NetScreen has VPN support built in. Please refer to your NetScreen manual for details.

Furthermore you should use a recent NetScreen fimware version. The latest firmware release for your NetScreen appliance can be obtained from

http://www.NetScreen.com/

For this document, ScreenOS 4.01 and 5.0.0r3.0 has been used.

When using Pre-shared key authentication you need one VPN Tracker Personal Edition license for each Mac connecting to the NetScreen.

VPN Tracker is compatible with Mac OS X 10.2.5+ / 10.3.

3. Connecting to a NetScreen VPN Appliance (single user)

In this example the Mac running VPN Tracker is directly connected to the Internet via a dialup or PPP connection.[1]

The NetScreen is configured in NAT mode and has the static WAN IP address 169.1.2.3 and the private LAN IP address 192.168.1.1. The Stations in the LAN behind the NetScreen use 192.168.1.1 as their default gateway and should have a working Internet connection.

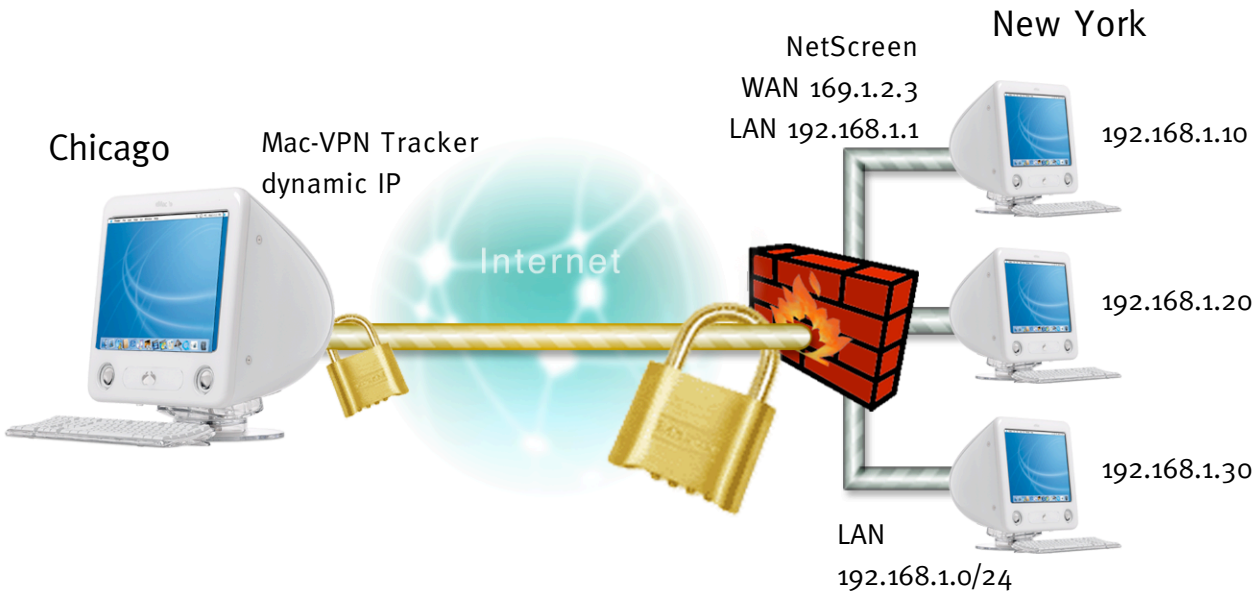

Figure 1: VPN Tracker – NetScreen connection diagram

[1] Please note that the connection via a router, which uses Network Address Translation (NAT), only works if the NAT router supports „IPSEC passthrough“. Please contact your router's manufacturer for details.

3.1 NetScreen Configuration

The pre-defined VPN Tracker connection type has been created using the default settings for your NetScreen appliance. If you change any of the settings on the NetScreen, you will eventually have to adjust the connection type in VPN Tracker.

Step 1 Create a new User Group:

Go to [Objects -› Users -› Local Groups]. Click “New” to add a goup. Type in an arbritary group name eg. vpntracker-dialup.

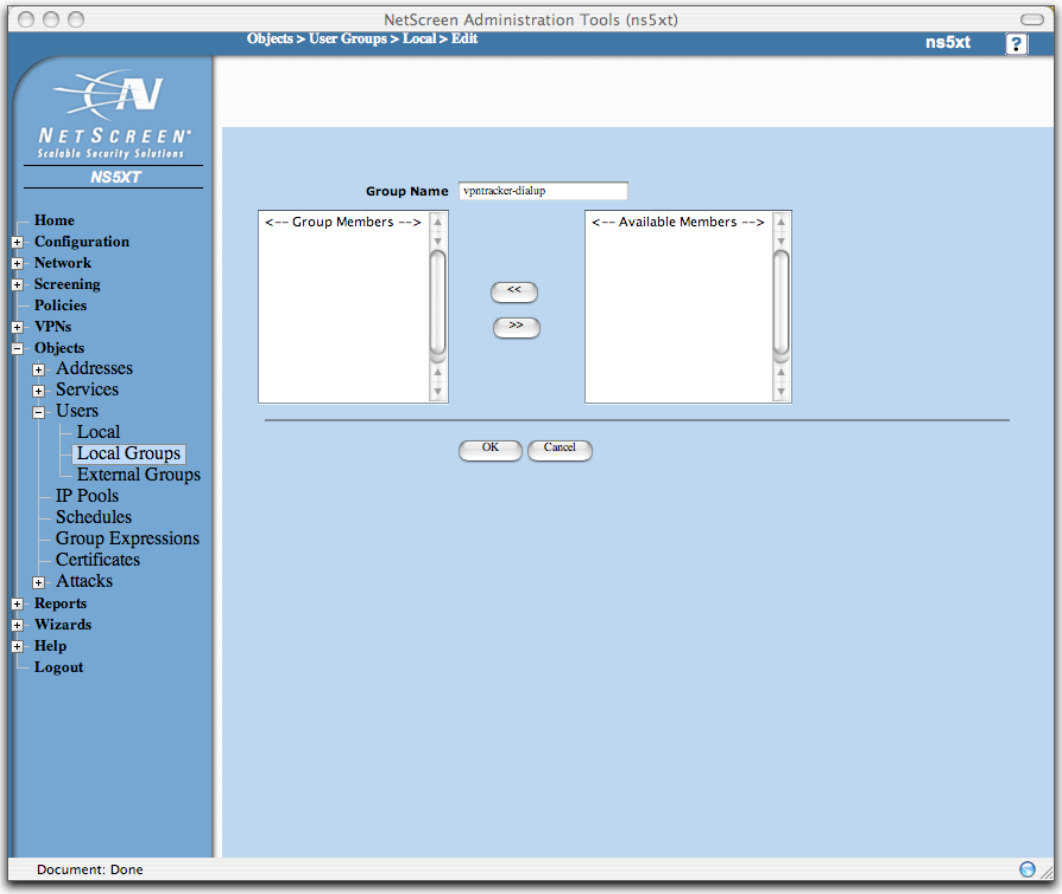

Figure 2: NetScreen – Create User Group

Step 2

Create a new user:

Go to [Objects -› Users -› Local]. Then add a user (eg. vpntracker@example.net) to the previously created group. Select **“IKE User”** and **“Simple Identity”** and type in an IKE Identity eg. your email adress.

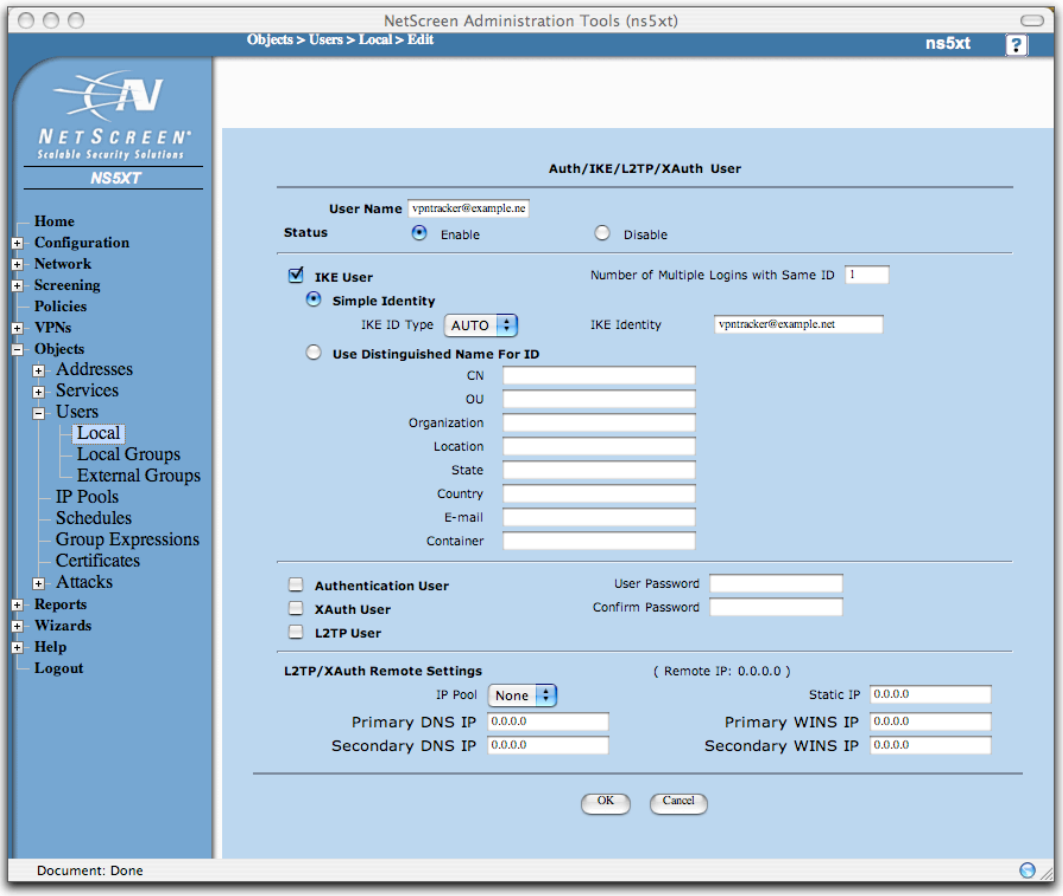

Figure 3: NetScreen – Create User

Step 3

Add user to your vpnuser group:

Go to [Objects -› Users -› Local Groups]. Then click on “Edit”. Select the user from the list and click on “«”.

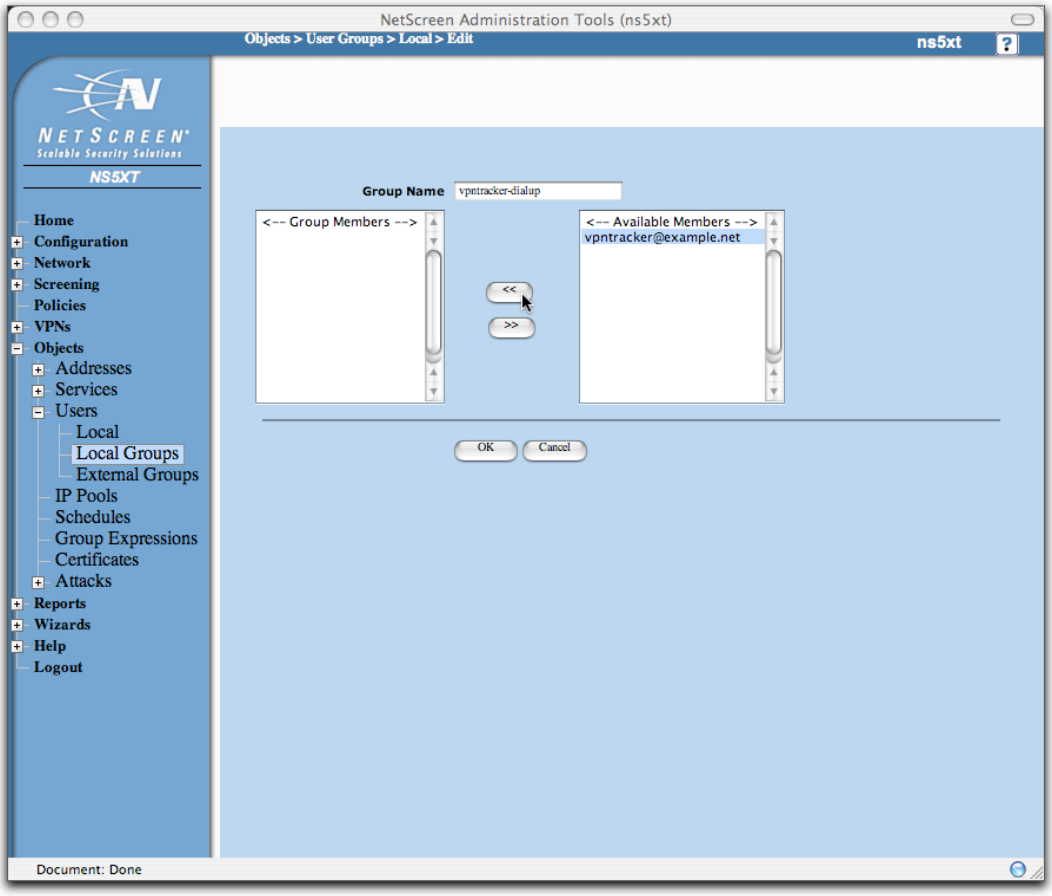

Figure 4: NetScreen - User Group settings

Step 4

Create a new Gateway:

- Gateway Name: arbritary Name (e.g. **mac-vpntracker**)
- Security Level: **Compatible**
- Remote Gateway Type: **Dialup User**: the previously created User Group
- Preshared Key: your Pre-shared key

Please Note: Every user in the Dialup User Group "vpntracker-dialup" uses the same Pre-shared key. If you don't want to allow this, you must create a separate gateway for every user.

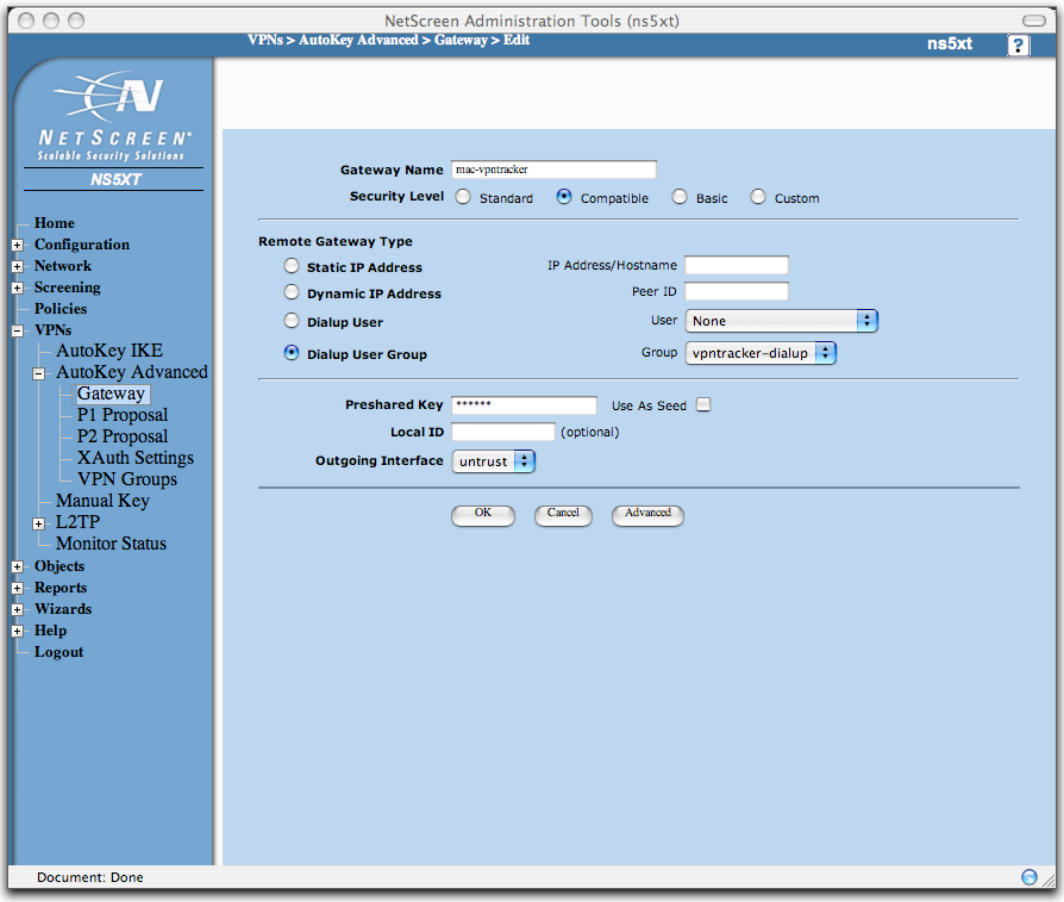

Figure 5: NetScreen – Gateway Settings

Click on the "Advanced" Button and enable "**Aggressive Mode**". You can leave the other settings at their default value (i.e. NAT-Traversal and all other options should be unchecked).

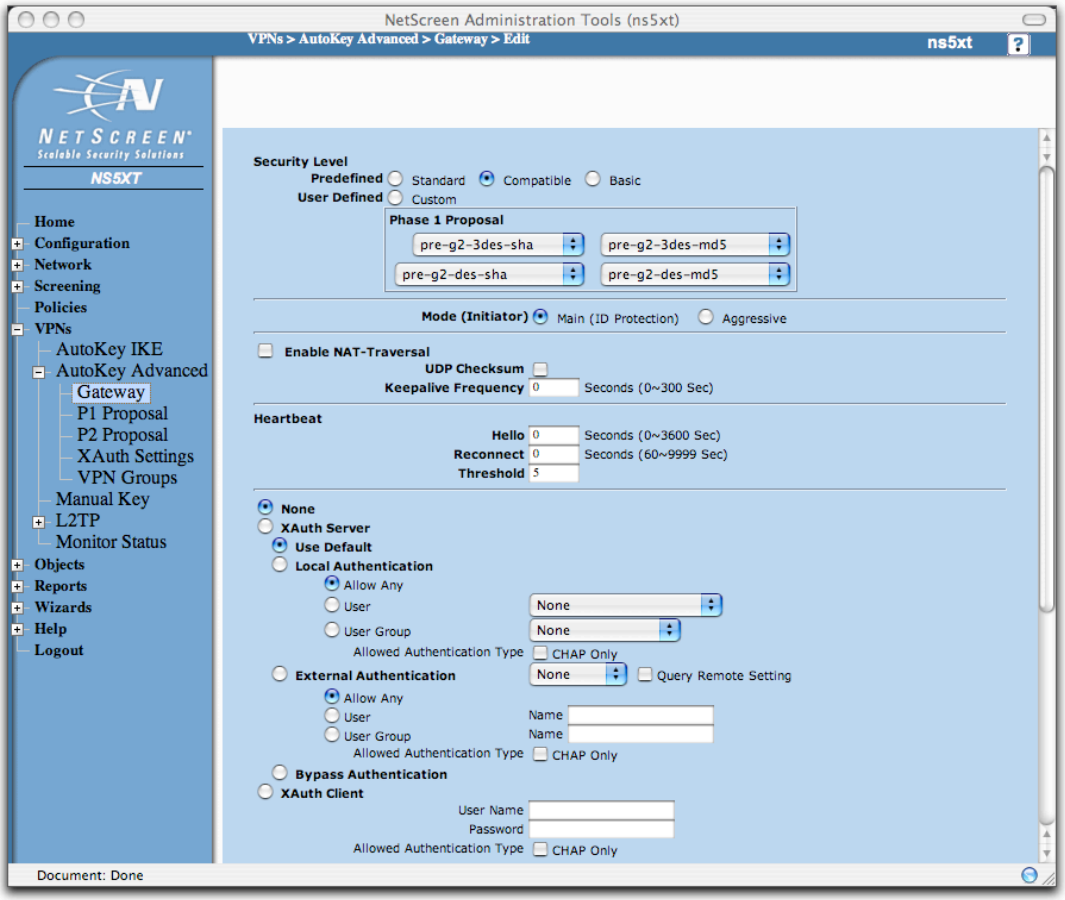

Figure 6: NetScreen – Advanced Gateway settings

Step 5 Create a new AutoKey IKE

Go to [VPNs -› Autokey IKE] and click “New”. Enter a name and select “**Compatible**” as Security Level. Choose as “Remote Gateway” the predefined gateway from step 4 (e.g. “**mac-vpntracker**”).

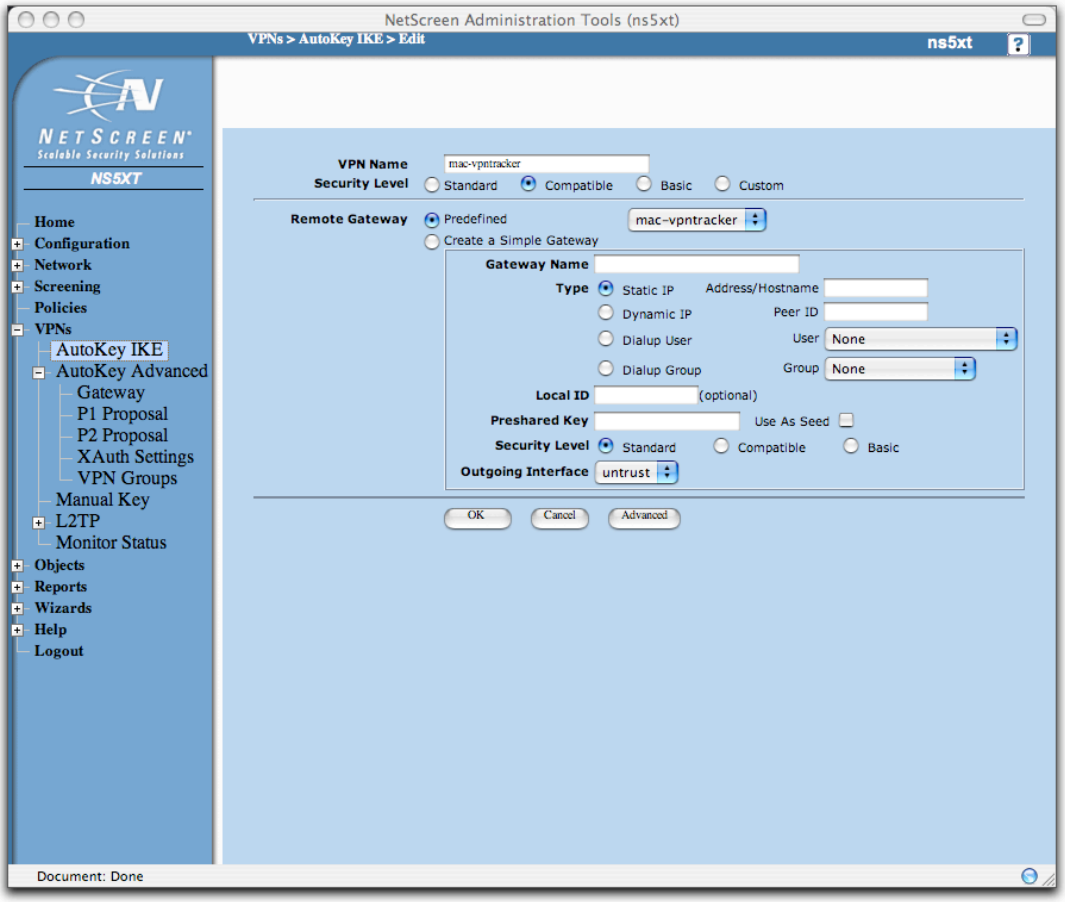

Figure 7: NetScreen - AutoKey IKE settings

Click on “Advanced” to check the default settings. Normally it isn’t necessary to change anything here.

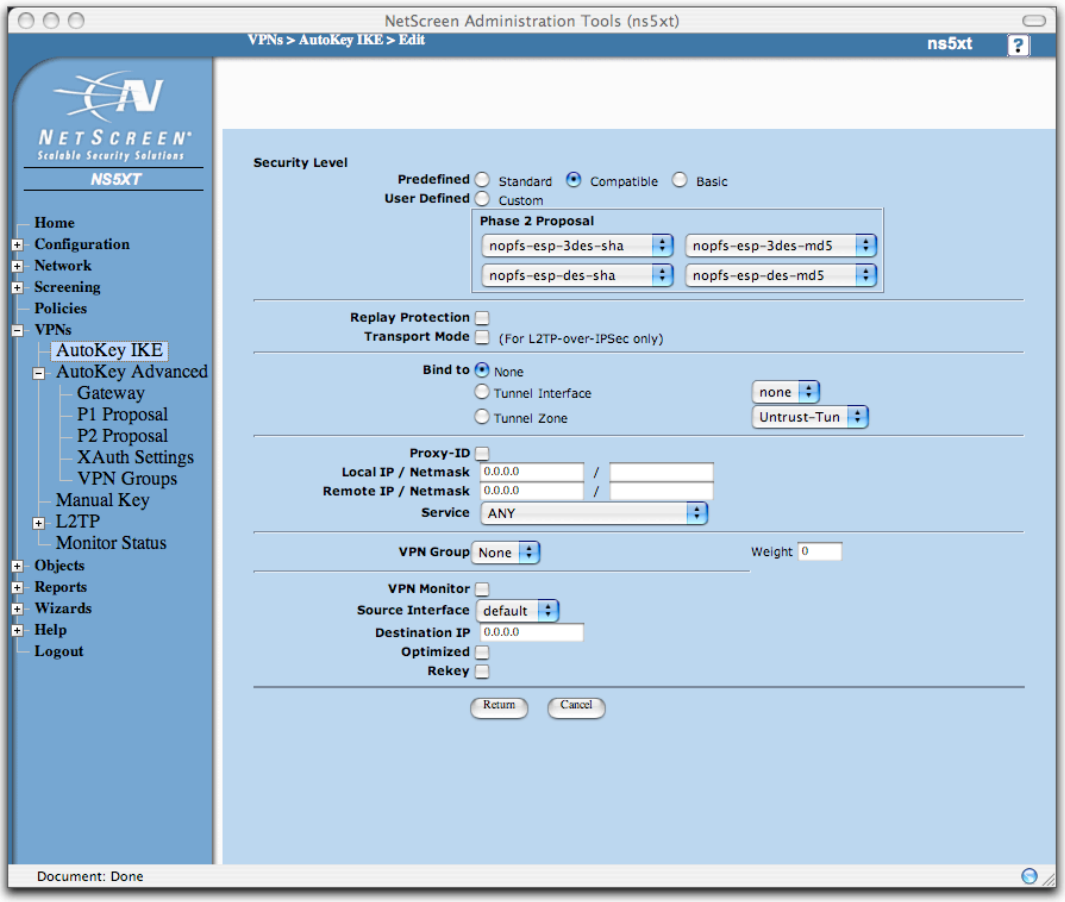

Figure 8: NetScreen - Advanced AutoKey IKE settings

After steps 1-5 the IPSec Configuration should look like this:

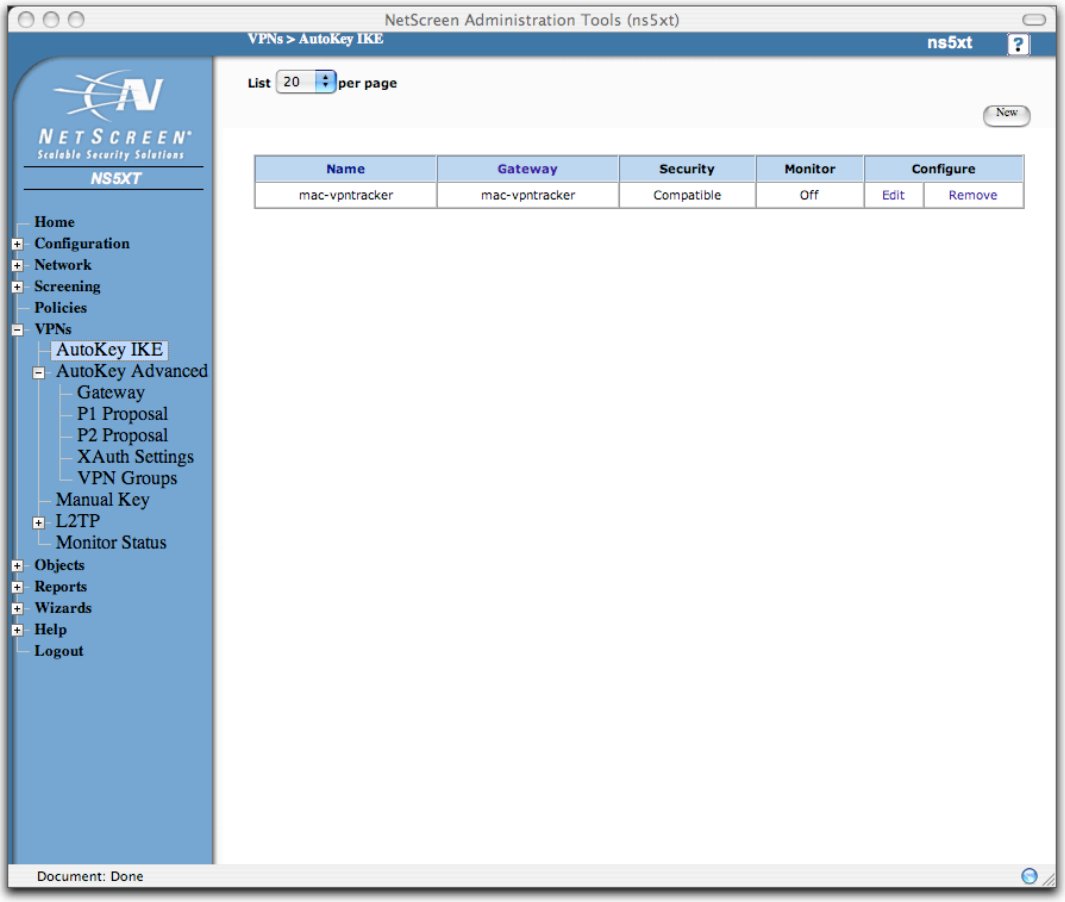

Figure 9: NetScreen - Auto IKE Summary

Step 6 Create a new Policy

You must now edit the Firewall policies to allow the VPN Tracker Mac to access the local network on the NetScreen side.

To create a new policy, choose “From: Untrust” -› “To: Trust” and press the “New” button:

- Source Address: **Address Book -› Dial-Up VPN**
- Destination Address: the network behind your Netscreen appliance (e.g. **192.168.1.0/24**)
- Action: **Tunnel**
- Tunnel: the previously created VPN (e.g. **mac-vpntracker**)
- Position at Top: **checked**

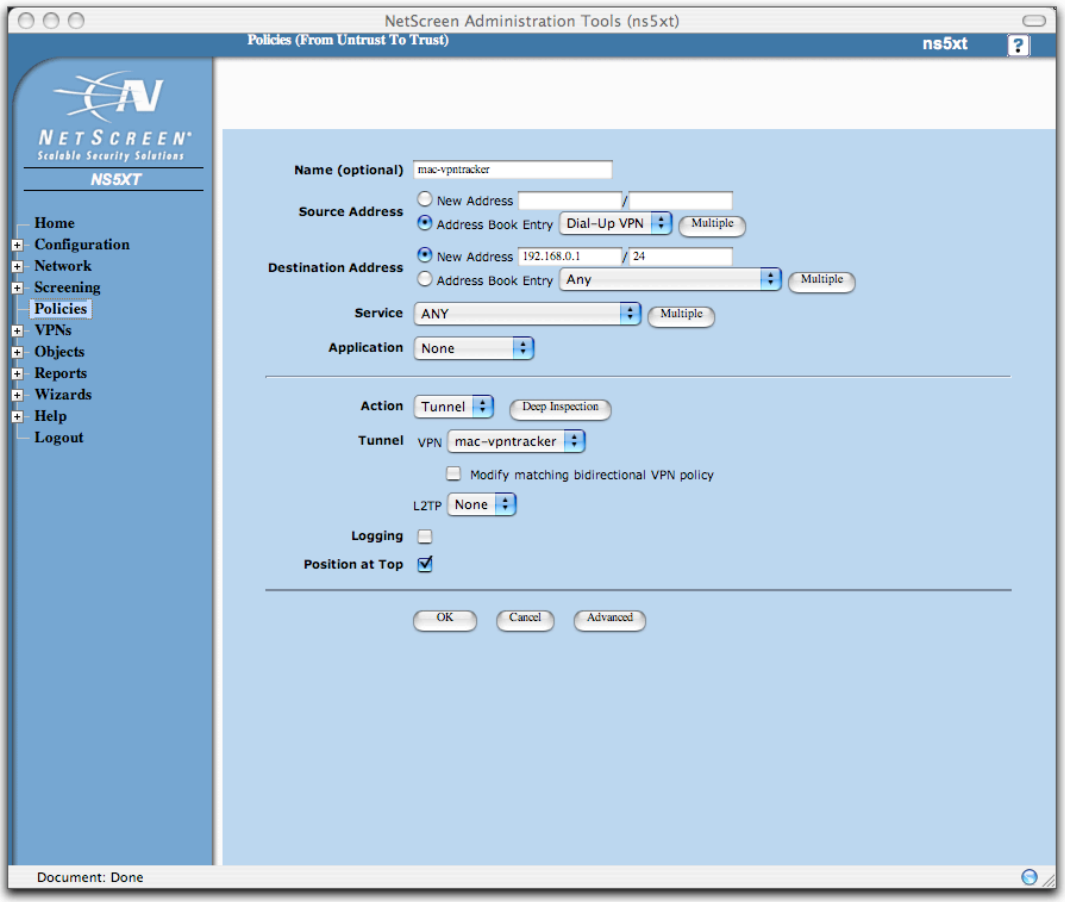

Figure 10: NetScreen - Policies

3.2 VPN Tracker configuration

Step 1

Add a new connection with the following options:

- Vendor: „NetScreen“
- Model: your VPN device

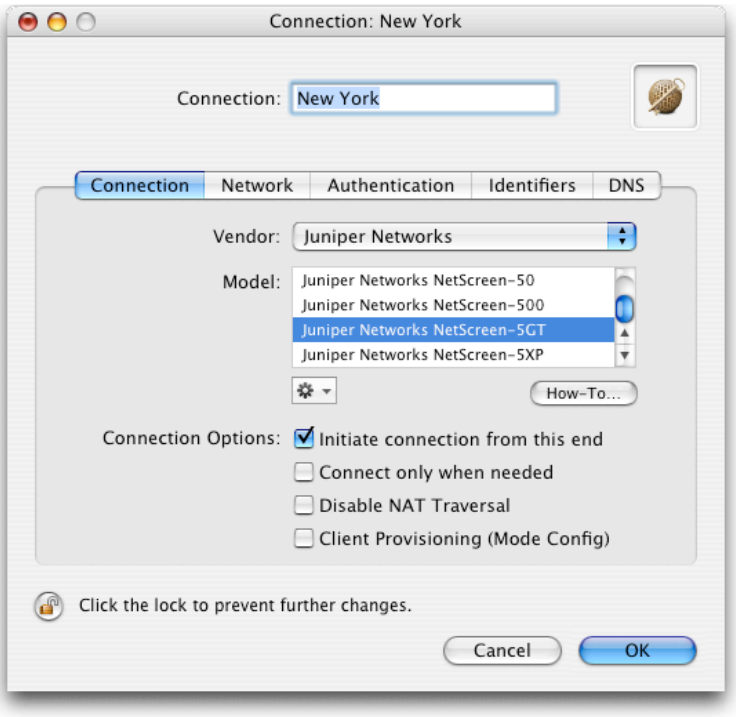

Figure 11: VPN Tracker - Connection settings

Step 2

Change your Network Settings:

- VPN Server Address: public IP address of your VPN Gateway (e.g. **169.1.2.3**)
- Remote Network/Mask: network address and netmask of the remote network (eg. 192.168.1.0/255.255.255.0).

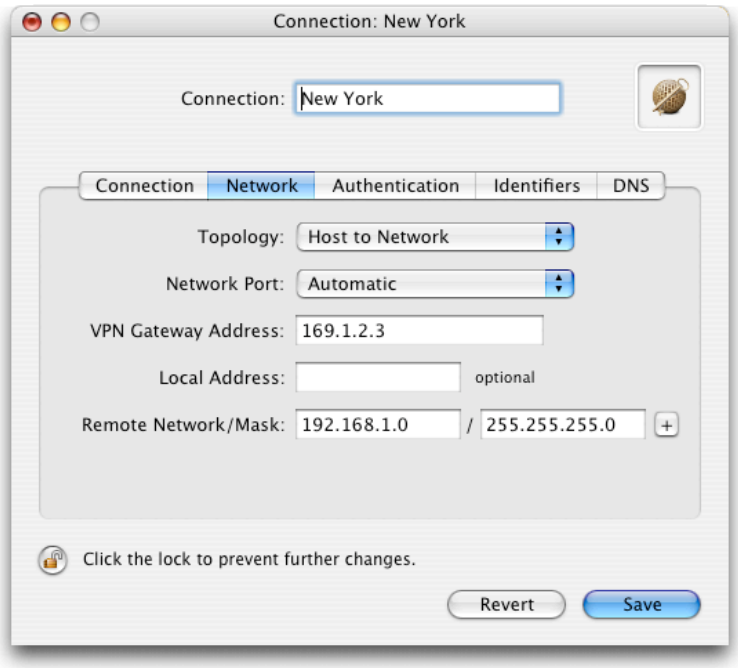

Figure 12: VPN Tracker – Network settings

Please note: In order to access multiple remote networks simultaneously, just add them by pressing the Plus-button.[2]

[2] For this step VPN Tracker Professional Edition is needed.

Step 3 Change your Authentication Settings:

- Pre-shared key: the same Pre-shared key as in the NetScreen configuration.
- Enable XAUTH if the corresponding option is enabled on the NetScreen.

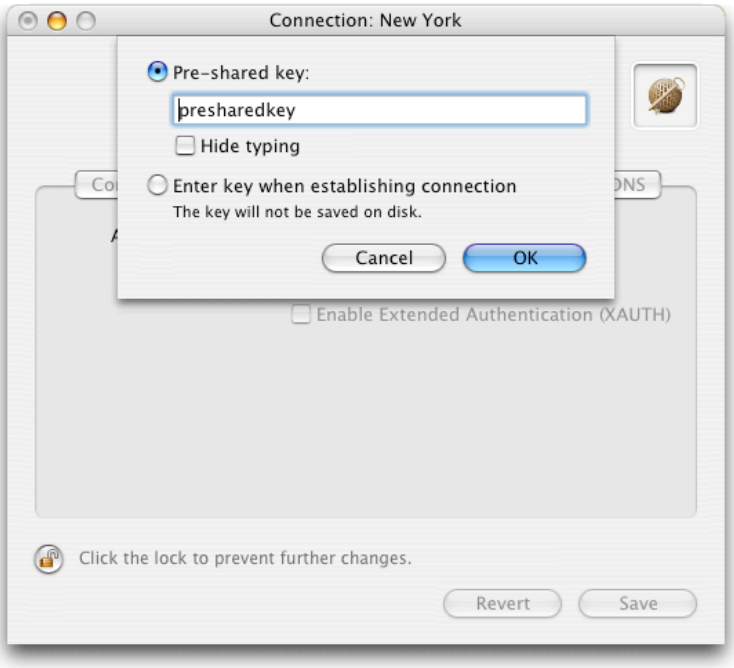

Figure 13: VPN Tracker - Authentication settings

Step 4 Identifier Settings:

- Local Identifier: your identity you've supplied in figure 2 in section 3.1 (e.g. **vpntracker@equinux.com**)
- Remote Identifier: **Remote endpoint IP address**.

Figure 14: VPN Tracker - Identifier settings

Step 5 Save the connection and Click „Start IPsec" in the VPN Tracker main window.

You're done. After 10-20 seconds the red status indicator for the connection should change to green, which means you're securely connected to the NetScreen. After IPsec has been started, you may quit VPN Tracker. The IPsec service will keep running.

Now to test your connection simply ping a host in the NetScreen network from the dialed-in Mac in the "Terminal" utility:

ping 192.168.1.10

4. Connecting to a NetScreen VPN Appliance (multiple users)

In order to authenticate multiple clients with different credentials, we recommend using XAuth for user authentication. To assign virtual IP addresses by the NetScreen appliance, Mode-Config will be used.

Step 1 Please refer to step 1 in section 3.2.

Step 2

Create new users:

Go to [Objects -› Users -› Local]. Then add a user (eg. vpntracker@example.net) to the previously created group. Select **“IKE User”** and **“Simple Identity”** and type in an IKE Identity eg. your email adress. Additionally, check the **“XAuth User”** box and enter a password for the user. Repeat this step for all your users.

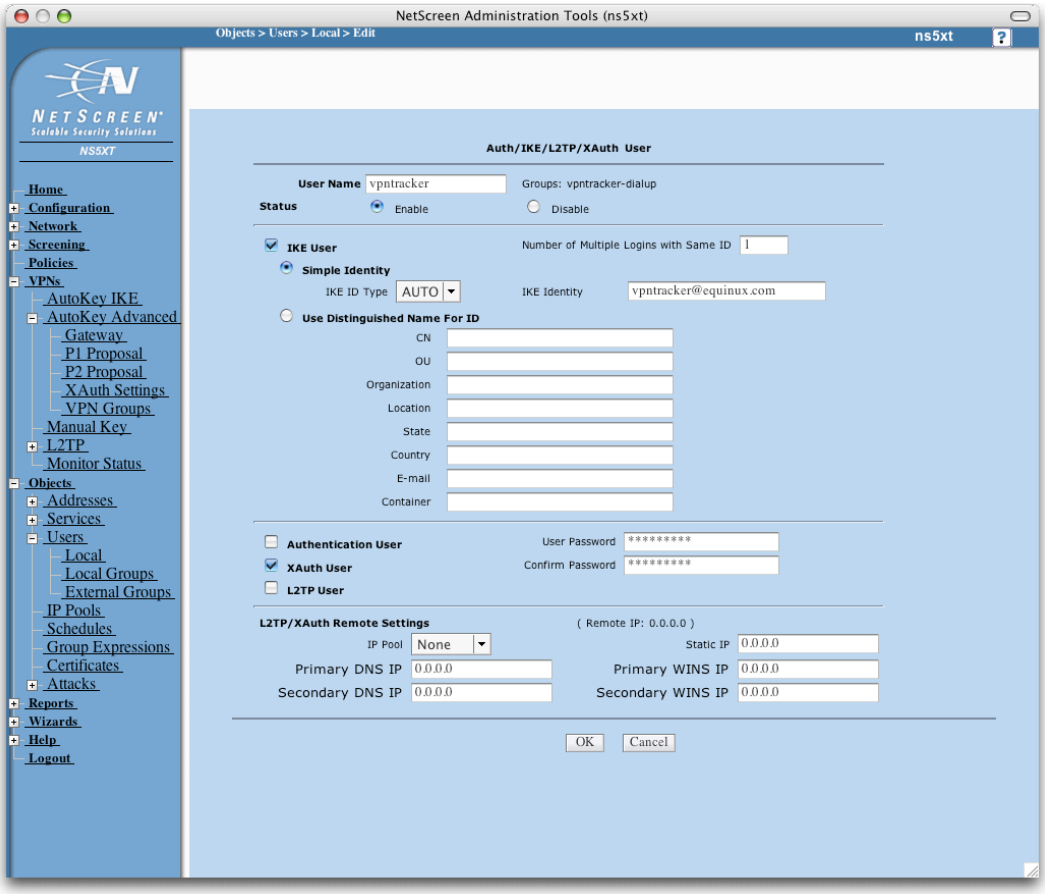

Figure 15: NetScreen - XAuth User settings

Step 3

Add users to your vpnuser group:

Go to [Objects -› Users -› Local Groups]. Then click on “Edit”. Select the users from the list and click on “«”, in order to add them to your group.

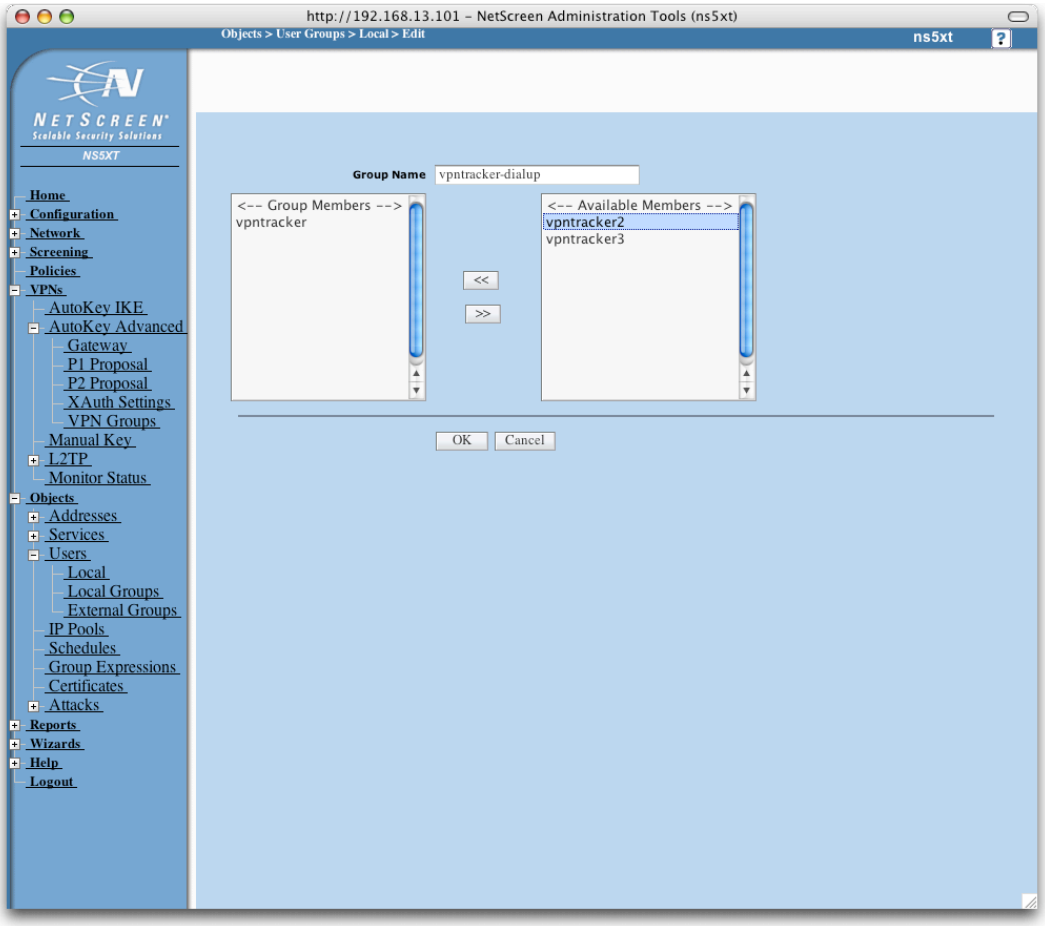

Figure 16: NetScreen - User Group settings

Step 4 Create a new Gateway:

- Gateway Name: arbritary Name (e.g. **mac-vpntracker**)
- Security Level: **Compatible**
- Remote Gateway Type: **Dialup User**: the previously created User Group
- Preshared Key: your Pre-shared key

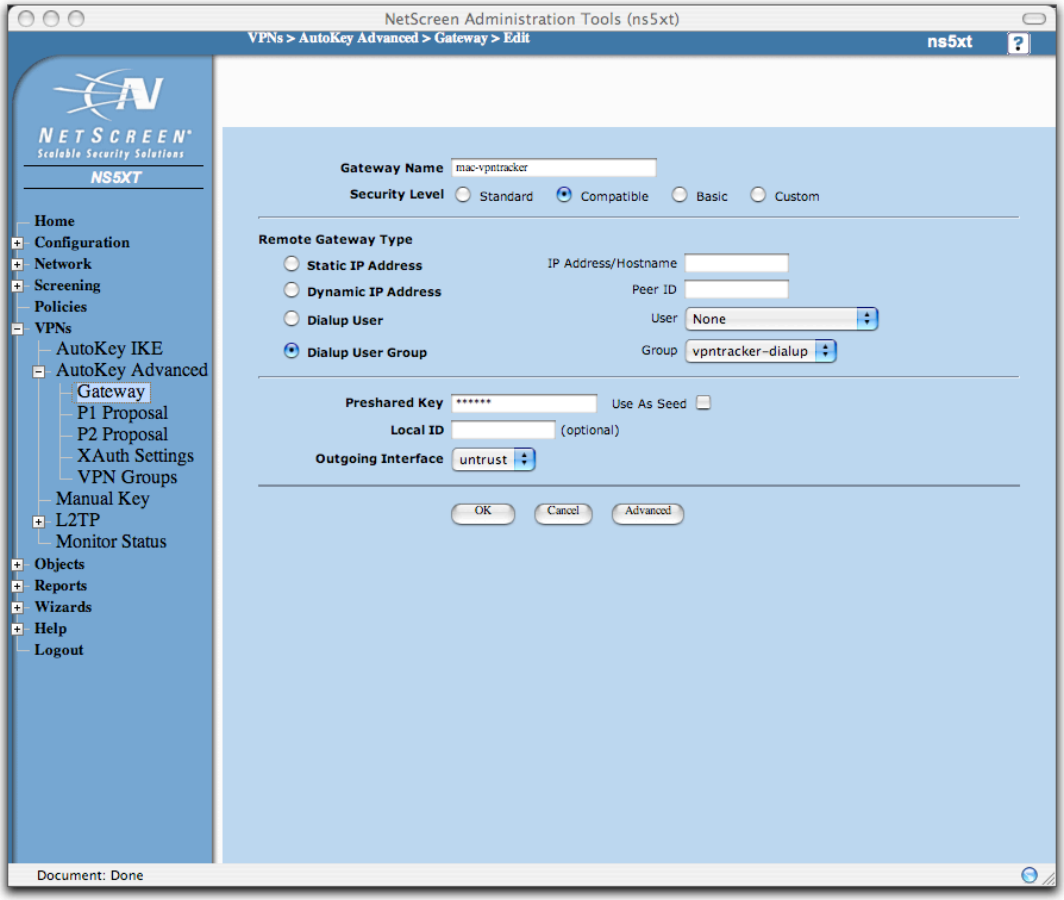

Figure 17: NetScreen – Gateway Settings

Advanced Gateway Settings:

- Security Level (Predefined): **Compatible**
- Mode (Initiator): **Aggressive**
- NAT-Traversal: **Enabled**
- XAuth Server: **Enabled**
  - Local Authentication: **User Group** (select your VPN user group here)

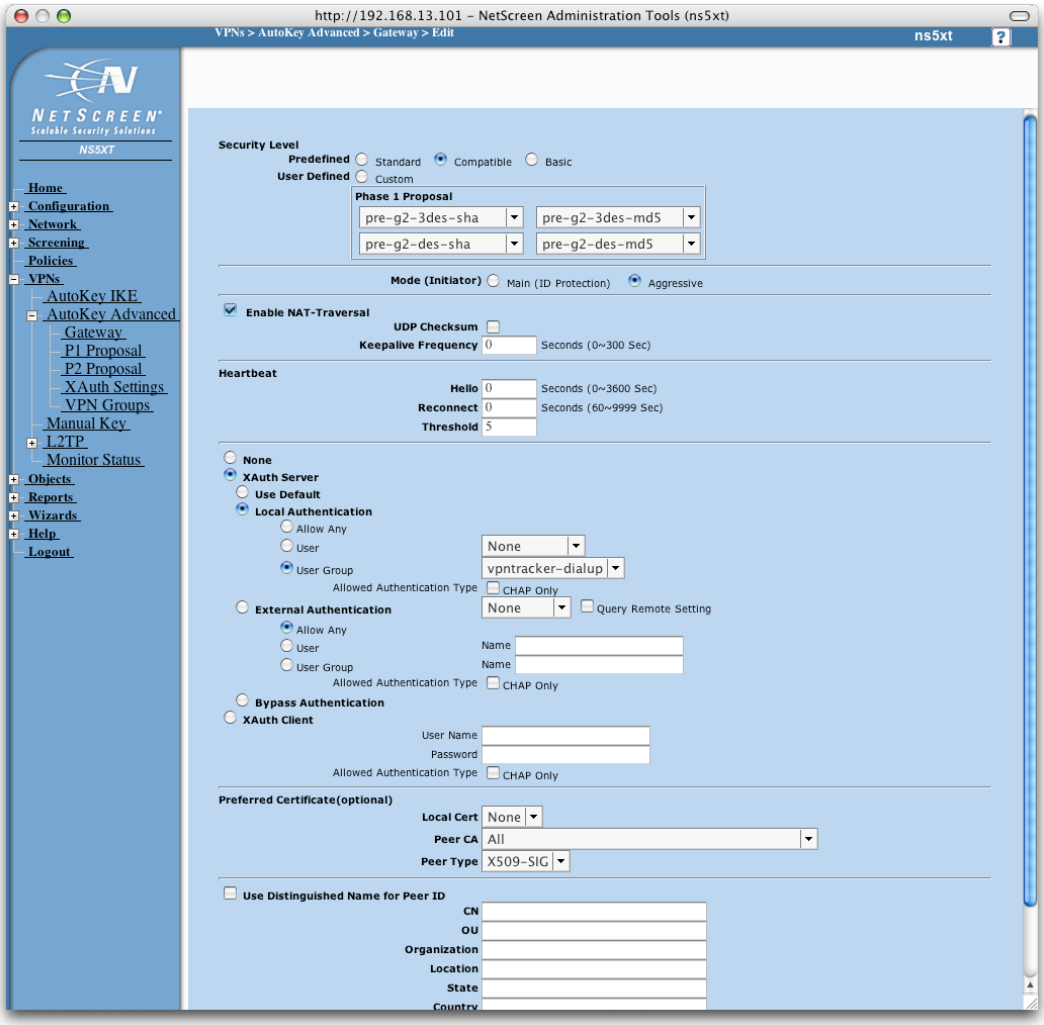

Figure 18: NetScreen - Advanced Gateway settings

Step 5 IP Pool settings:

Please create an IP pool with IP addresses that should get assigned to the VPN clients. This could be addresses from the local network or any other (private) network.

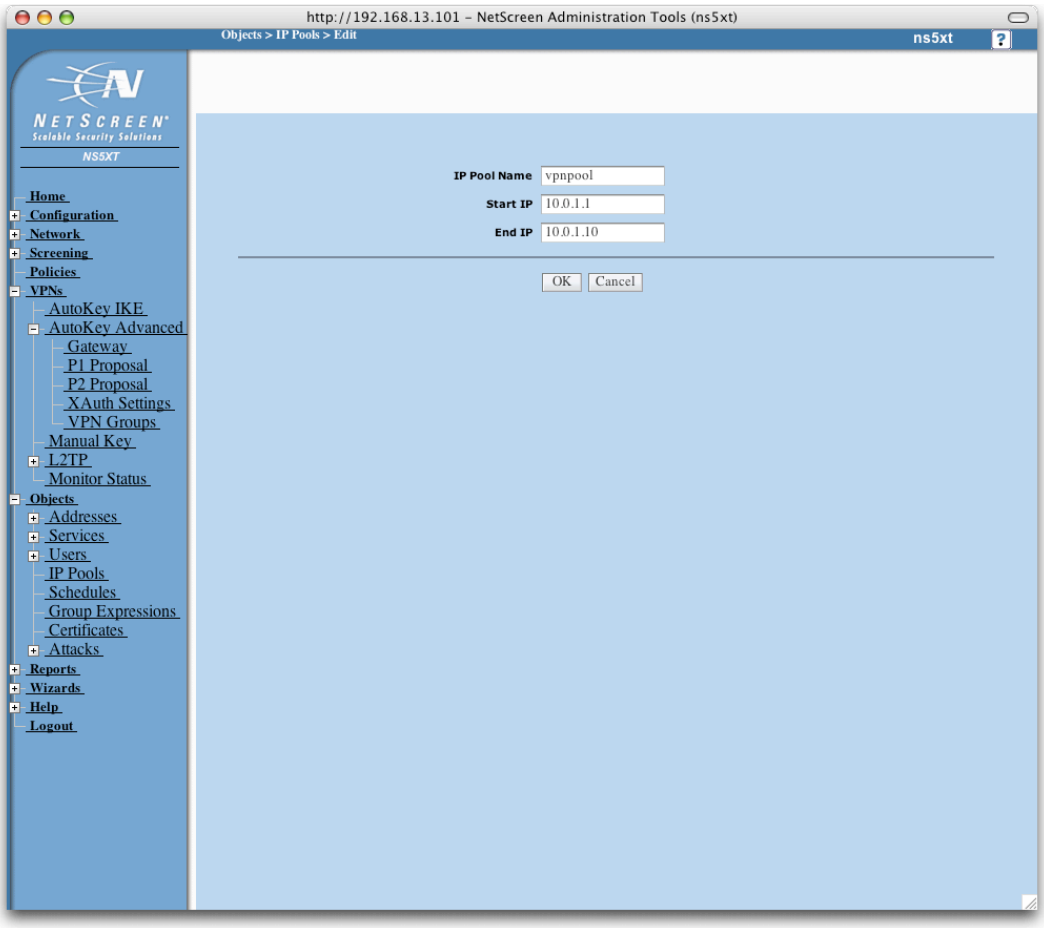

Figure 19: NetScreen - IP Pool settings

Step 6 XAuth Settings:

- IP Pool Name: a previously defined IP Pool (e.g. **vpnpool**)
- DNS Primary Server IP: your local primary DNS Server (e.g **192.168.1.1**)
- DNS Secondary Server IP: optional

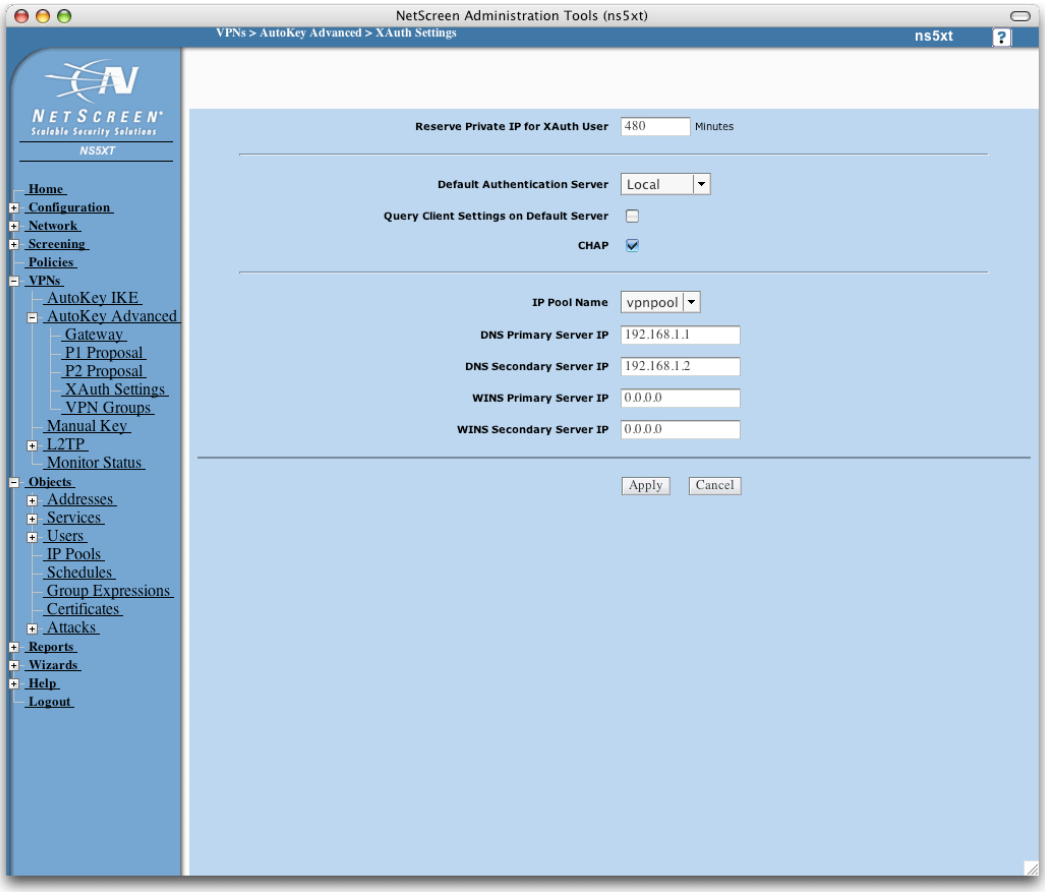

Figure 20: NetScreen - Advanced Gateway settings

Step 7-8 Please refer to steps 5-6 in chapter 3.2.

4.1 VPN Tracker Configuration

Step 1 Add a new connection with the following options:

- Vendor: **„NetScreen“**
- Model: your VPN device
- Client Provisioning (Mode Config): **Enabled**

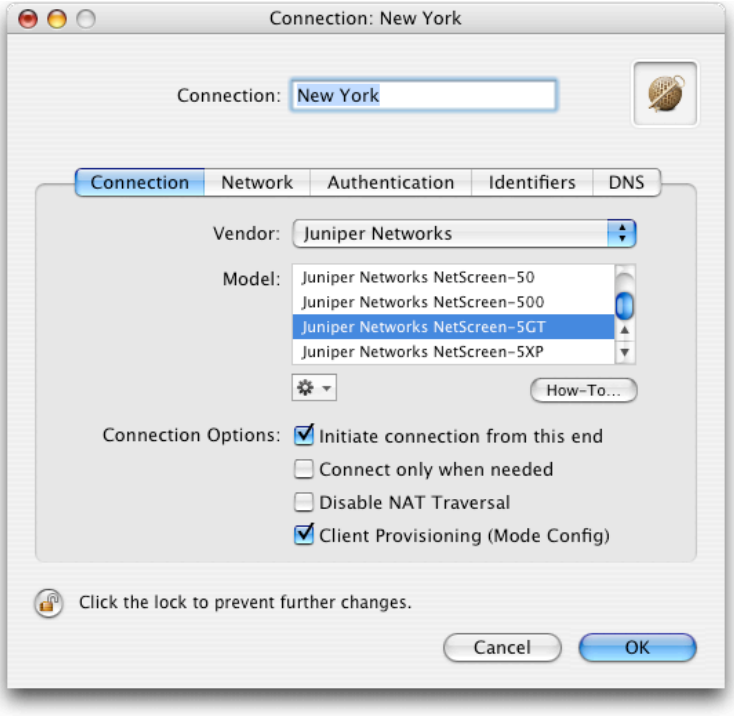

Figure 21: VPN Tracker - Connection setting

Step 2

Change your Network Settings:

- VPN Server Address: public IP address of your VPN Gateway (e.g. **169.1.2.3**)
- Remote Network/Mask: network address and netmask of the remote network (eg. **192.168.1.0/255.255.255.0**).

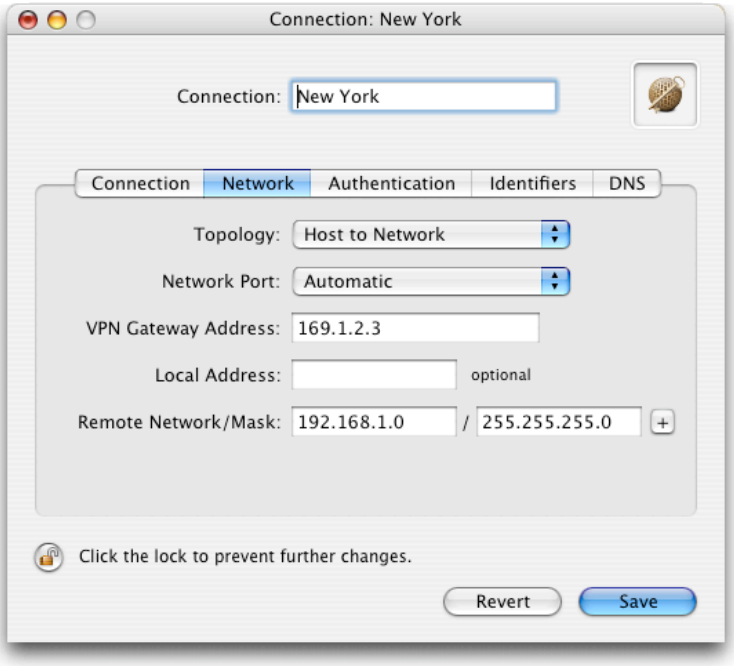

Figure 22: VPN Tracker – Network settings

Please note: In order to access multiple remote networks simultaneously, just add them by pressing the Plus-button.[3]

[3] For this step VPN Tracker Professional Edition is needed.

Step 3 Change your Authentication Settings:

- Pre-shared key: the same Pre-shared key as in the NetScreen configuration.
- Enable Extendended Authentication (XAUTH): **Enabled**

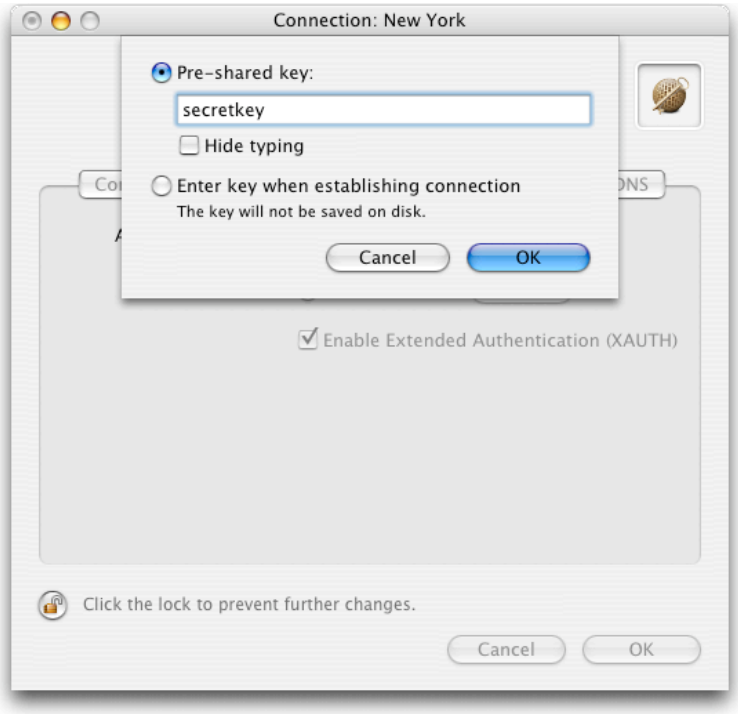

Figure 23: VPN Tracker - Authentication settings

Step 4 – 5 Please refer to steps 4-5 in chapter 3.2.