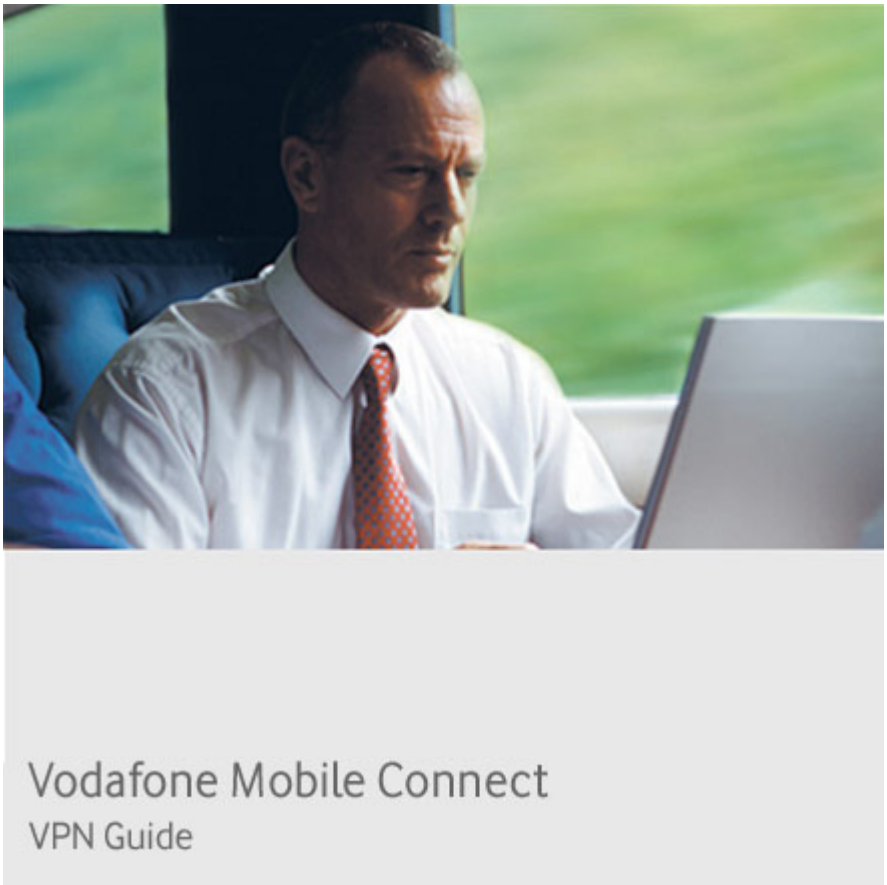
VPN End to End – Juniper NetScreen

Appendix A: Concentrator Configuration Example

Technical Notes for use with Vodafone Mobile Connect services

Date: **3 May 2007**

Revision No: **3.0**



© VODAFONE GROUP 2007

Scope

This document presents results of installation, configuration, and operations testing of VPN components with the Vodafone Mobile Connect service. The document is not intended to be a tutorial on VPN concepts nor does it supersede or replace the vendor's documentation. The reader is referred to the VPN vendor for definitive guidance on the proper and recommended use of their product. While Vodafone Group has taken care to ensure that the information contained herein is accurate, no responsibility can be accepted for errors, omissions, or inaccuracies.

Document History

Version	Date	Reason
1.0	October 2003	Initial release using GPRS network. Client documentation included in main document.
2.0	May 2007	Creation of separate document for client configuration. Update to new versions of VPN software and focus on 3G network performance.
3.0	May 2007	Final edits for web publication.

File Reference

VPN - Junier Netscreen 5GT_Appendix_A_Concentrator.doc

Document Authors

Joerg Pfeffer, TECON Terenci
Peter Jaeger, TECON Terenci
Miroslaw Grzesica, TECON Terenci

Document Distribution

Public via websites of Vodafone, its Affiliates, and its Partner Networks

© Vodafone Group 2007.

Other than as permitted by law, no part of this document may be reproduced, adapted, or distributed, in any form or by any means, without the prior written consent of Vodafone Group Plc.

Contents

1 Executive summary 4

2 NetScreen appliance Installation and Configuration (Version 5.3.0r2a.0).....5

2.1 Initial setup.....5

2.2 Rapid Deployment Wizard 5

2.3 Configuration of Routing and Users 8

2.4 Configuration of VPN 15

2.5 Configuration of the VPN Firewall Policy 19

2.6 Advanced Configuration.....21

3 Logging.....23

4 Xauth Parameter.....24

Tables & Figures

Nil

1 Executive summary

This Appendix is a supplement to the overall system description for the Juniper Netscreen VPN solution and describes the setup and update process for the VPN concentrator in a detailed way with example screen shots taken from the initial processes.

Furthermore logging and additional functionality is available in the appropriate chapters.

© VODAFONE GROUP 2007

2 NetScreen appliance Installation and Configuration (Version 5.3.0r2a.0)

The following description is intended for network administrators who are familiar with networking and IP concepts. The appliance has to be integrated into the internal company network. The appliance setup therefore has to comply with the configuration of the internal networking. This description is intended to allow a network administrator not yet familiar with the Juniper NetScreen appliance to configure a VPN with UMTS/GPRS usage.

2.1 Initial setup

After unpacking the device, connect one of the trusted network connection to a PC and the untrusted network connection to the internet gateway. The PC must be configured to use DHCP to receive the IP address and network data from the network. Connect the power.

2.2 Rapid Deployment Wizard

The initial configuration is aided by a startup wizard when using a web browser for the initial setup.

Advanced administrators can attain finer control by using the Command Line Interface (CLI). To configure a security device with the CLI, you can use any software that emulates a VT100 terminal. With a terminal emulator, you can configure the security device using a console from any Windows, UNIX, or Macintosh operating system. For remote administration through the CLI, you can use Telnet or Secure Shell (SSH). With a direct connection through the console port, you can use HyperTerminal.

NOTE: For a complete listing of the ScreenOS CLI commands, refer to „ScreenOS CLI Reference Guide IPv4 Command Descriptions“.

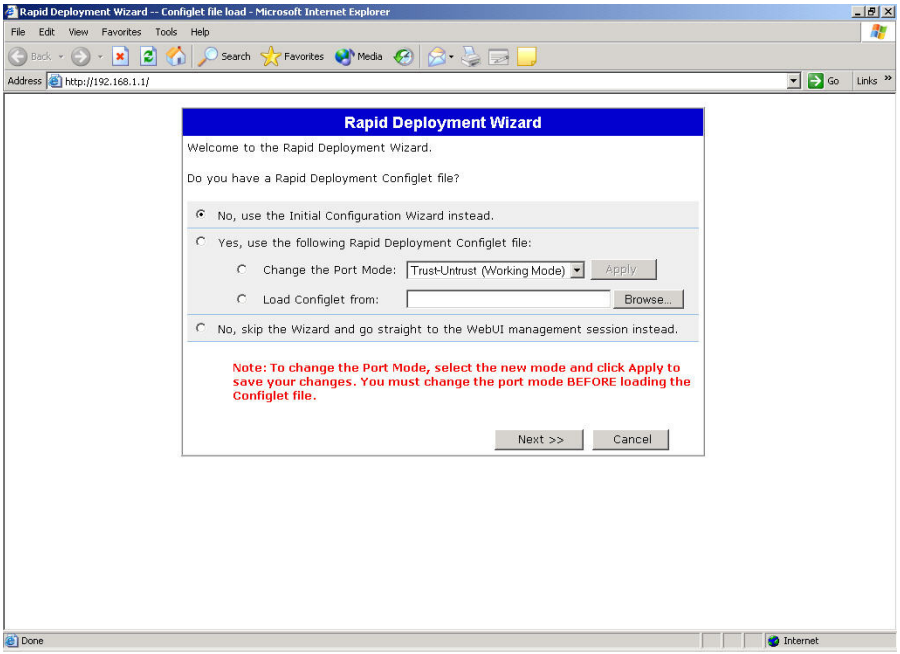
We recommend using a web browser to contact the Juniper NetScreen appliance. The NetScreen Security Manager requires a Java-enabled web browser, e.g.

- Microsoft Internet Explorer version 6.0 SP1 or higher (Windows) (SP2 required for Windows XP)
- Netscape Navigator version 7.2 or higher (Windows, Linux, or Solaris)
- Mozilla 1.73 or higher (Windows, Linux, or Solaris)
- Firefox 1.0 or 1.5 (Windows, Macintosh, or Linux)

© VODAFONE GROUP 2007

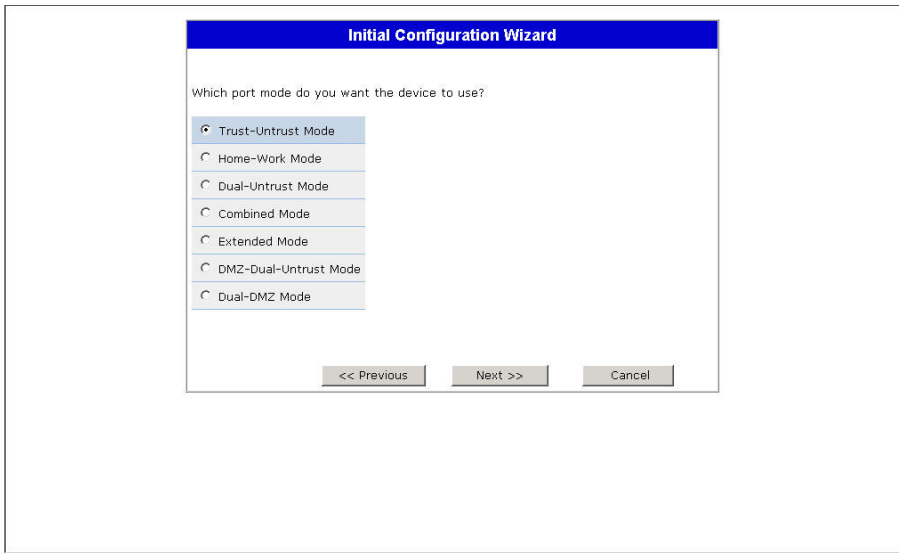
For best results, we recommend Internet Explorer. Whatever browser and version you use, install the latest patches and service packs for it. Make sure you have Java script/Active scripting enabled in your browser.

When starting the NetScreen Security Manager for the first time, the quick start wizard is activated.

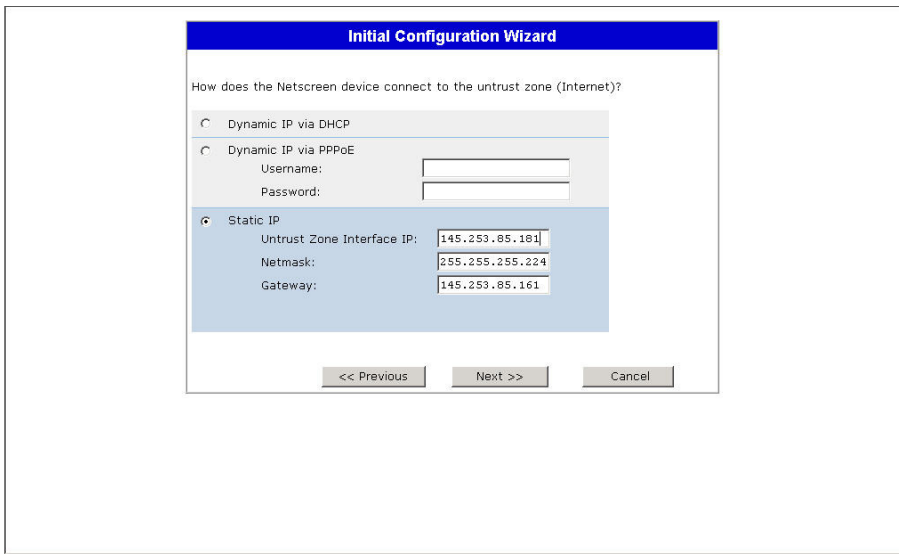


Follow the web pages of the dialog and enter the administrator credentials.

Depending on the usage of the device, several port definition modes are possible. This VPN example configuration is based on the Trust-Untrust Mode.



For a VPN connection, the external interface must be well defined and should be a static official IP address.



© VODAFONE GROUP 2007

Next, configure the internal (trusted) interface. Click “Next” and keep the defaults on the next pages.

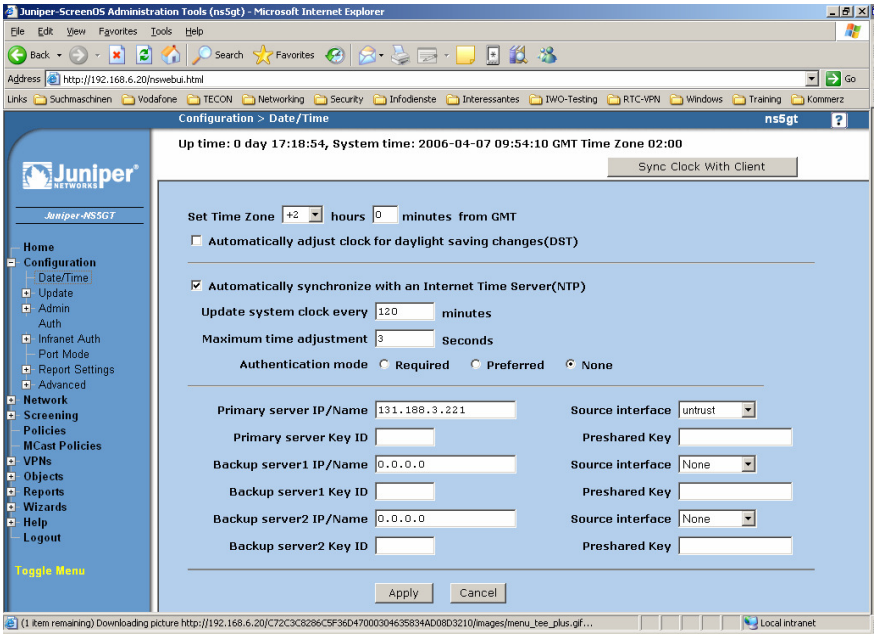
After the initial configuration wizard is completed, the appliance will reboot and the settings will be activated. Now, the machine can be configured from the internal network via the web management. Make sure the configuration PC’s network interface is configured correctly. Since the initial configuration wizard does not allow configuring routes, the configuration PC must be connected to the same network as the trusted interface of the NetScreen device. When the new internal network address is entered in the web browser, the administrator authentication screen will appear.

2.3 Configuration of Routing and Users

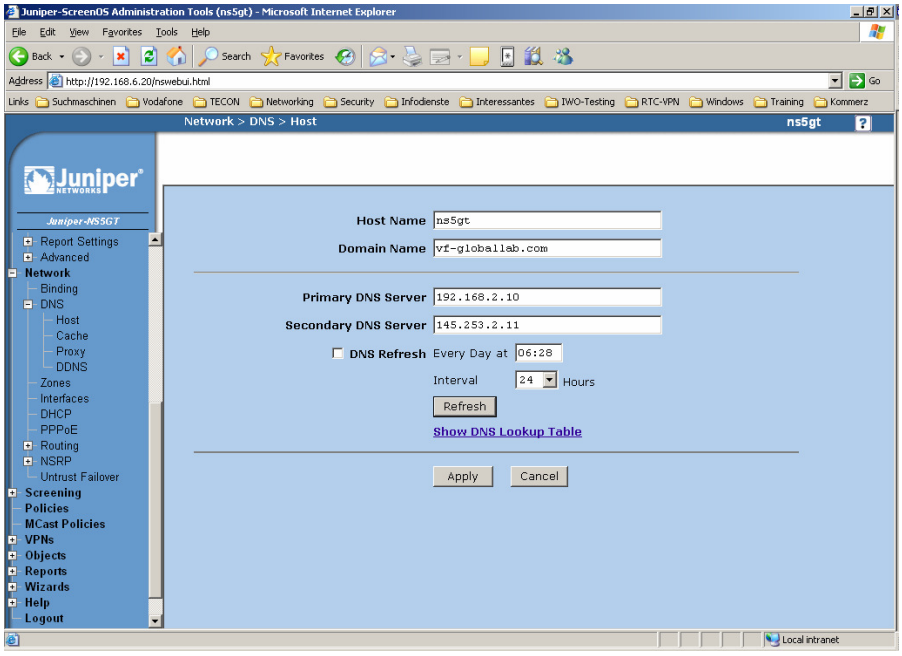
After the initial configuration of port type and interfaces, routing, VPN and firewall policies have to be configured. This is done via the web interface.

The web configuration consists of two areas: On the left, all available screens are listed in an explorer-type tree view. On the right, the currently selected screen is shown.

First, set time and date correctly on the screen "**Configuration > Date/Time**". When certificates are used, the time between server and client must match. The NetScreen appliance also allows updating the time automatically from NTP servers. Do not use the daylight saving time feature, since the algorithm used is fixed and may not be compatible to your time zone.

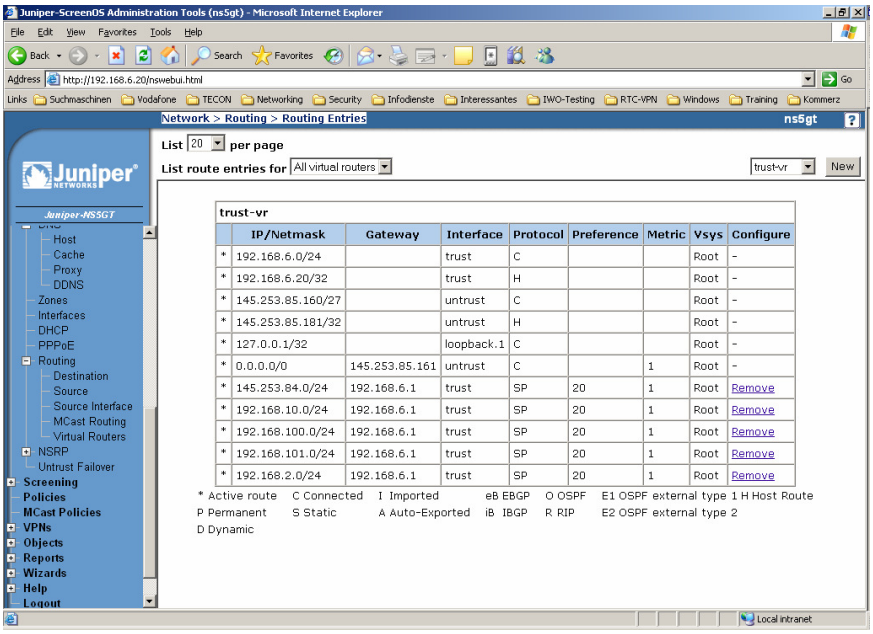


The appliance name, domain name and DNS servers are set up on the screen "**Network > DNS > Host**".

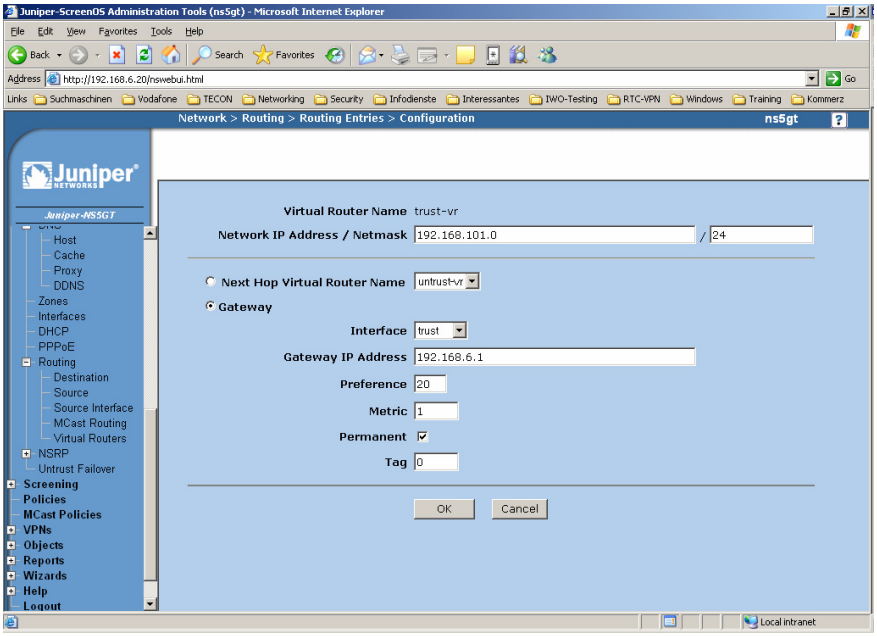


If additional trusted networks need to be reached through the internal (trusted) interface, the routes must be defined on the screen "**Network > Routing > Routing Entries**". Due to the

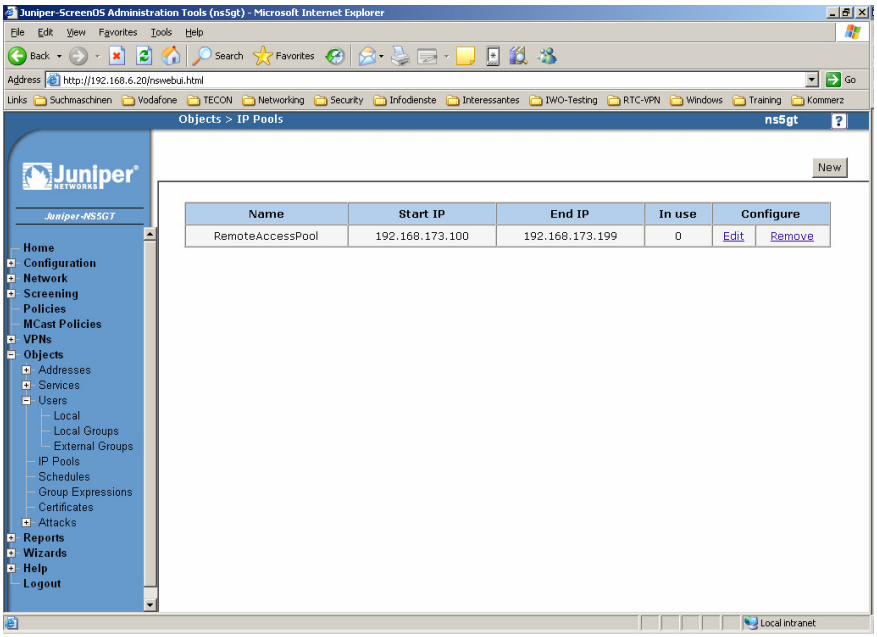
concept of Juniper NetScreen to manage several separate virtual routers, you must be careful to select the “trust-vr” when you enter the new internal networks.



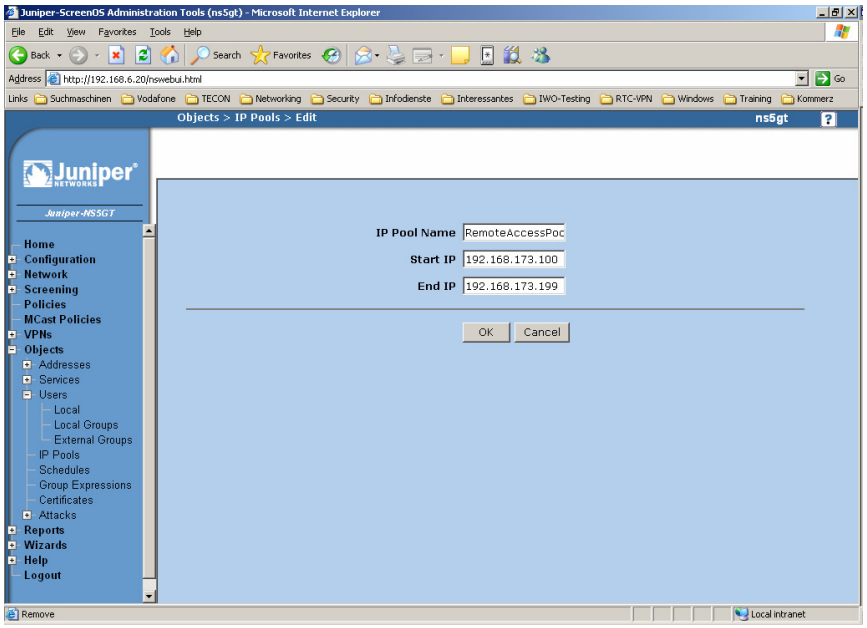
Select “trust-vr” in the top right corner of the screen and click “New” to enter the route. Enter the network address and the netmask (number of bits). Select the radio-button “Gateway” to define a route to a gateway and define Interface “trust” and the gateway IP address. Select “Permanent” to keep the route even if the interface is down and click “OK”.



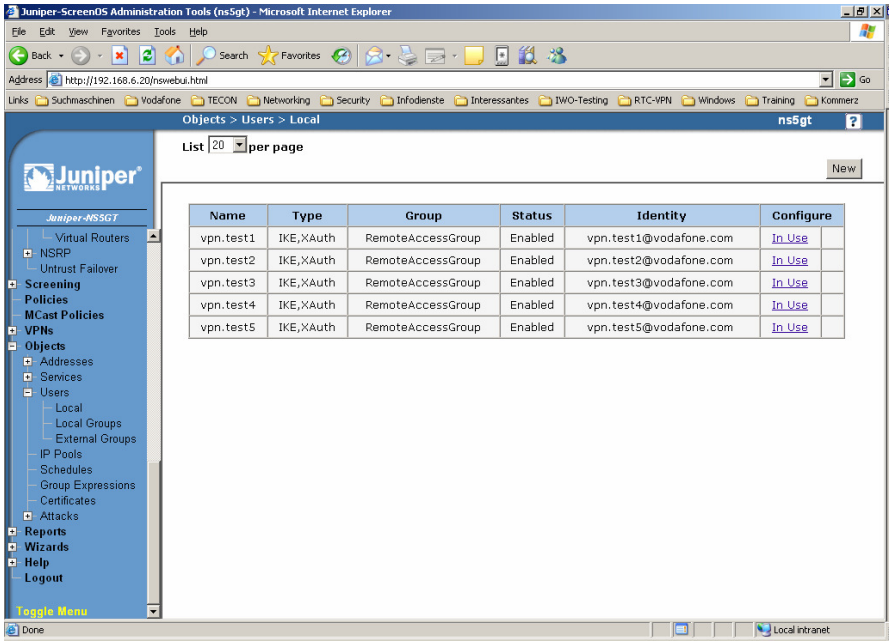
To define a pool of IP addresses, from which the VPN client internal IP addresses will be taken, open the screen "**Objects > IP Pools**".



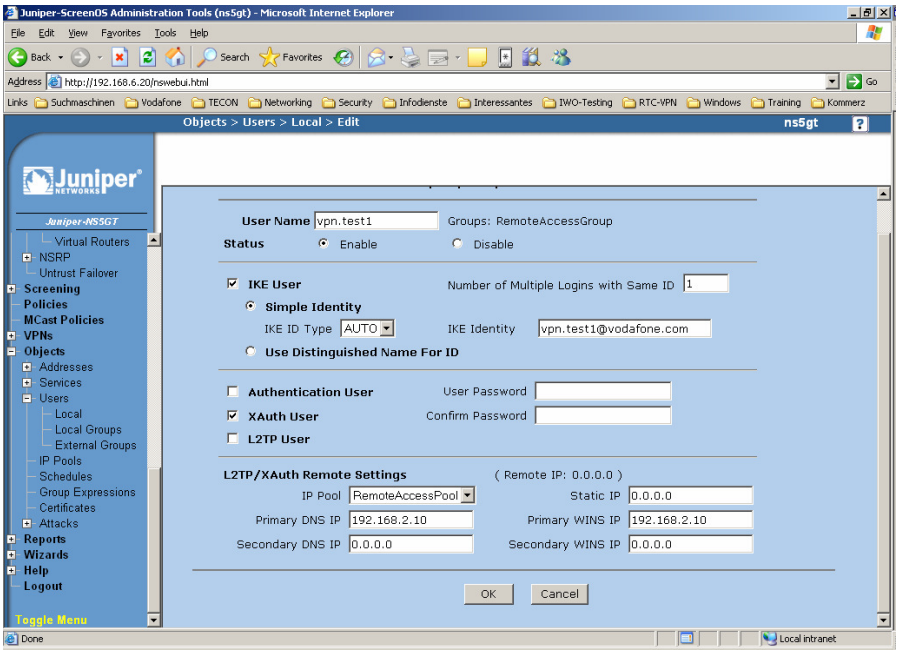
Click "New" on the top right corner of the screen and enter an "IP Pool Name" and a "Start IP" and an "End IP". Click OK to accept the input.



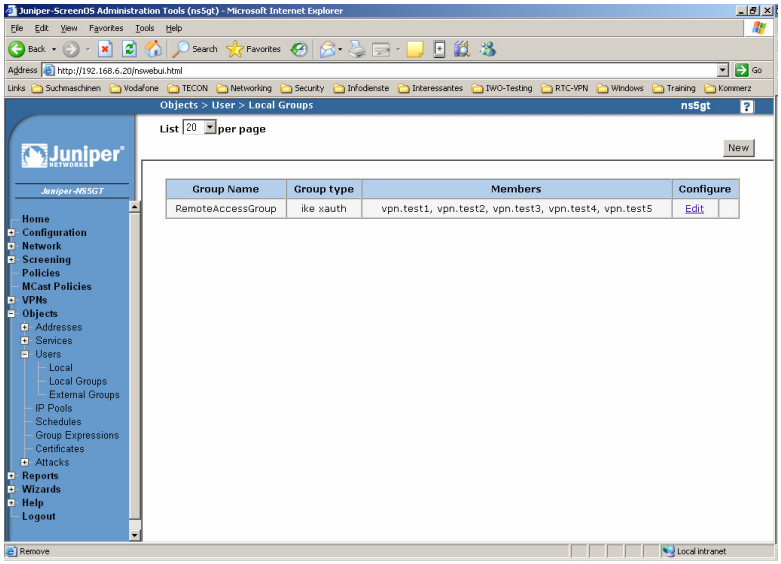
Next, define users in the screen "**Objects > Users > Local**". Click "New" to define a new user.



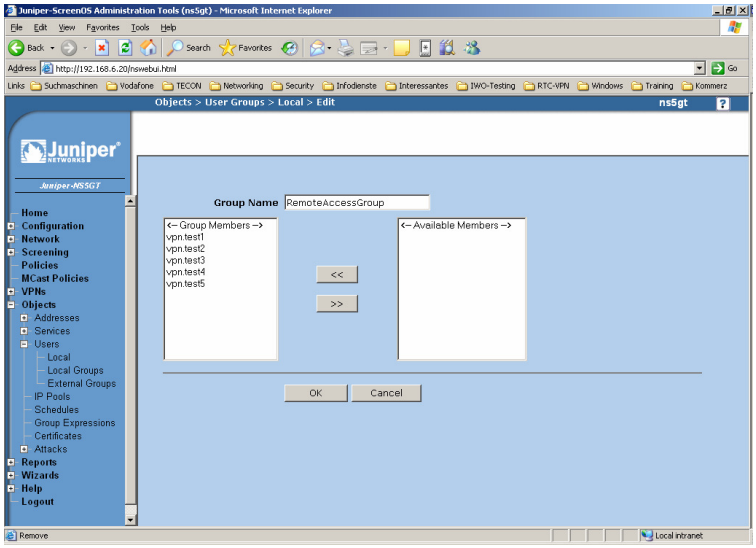
Enter a user name and select "IKE user", "Simple Identity" and enter the "IKE Identity". Select "XAuth User" and enter a "User Password" with a minimum length of 8 characters. Repeat it in the "Confirm Password" field. When "XAuth User" was selected, the "L2TP/XAuth Remote Settings" appeared. Select a valid IP Pool from the drop down list. When logging in, the user's internal IP address will be taken out of this pool. Enter values for the DNS and /or WINS IP addresses. Keep the Static IP on "0.0.0.0" to take a free address out of the pool.



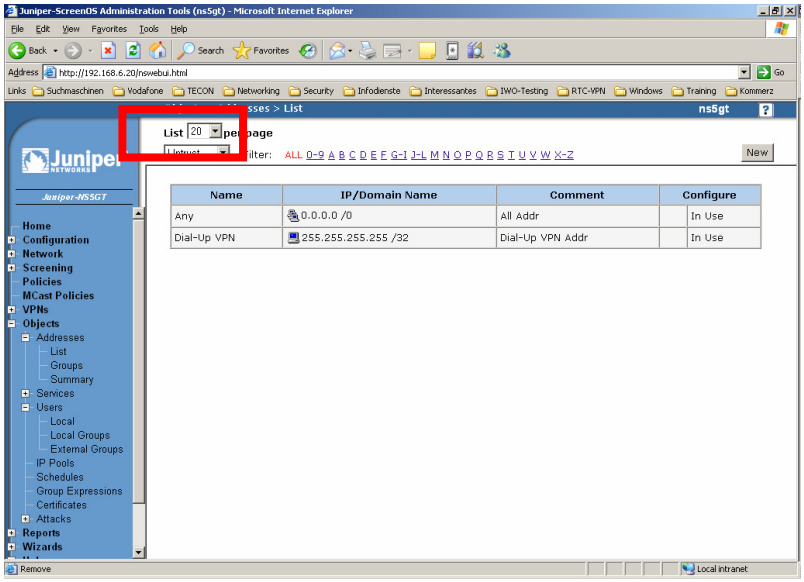
If more than one user shall use the VPN, a local user group is needed. Open the screen "**Objects > User > Local Groups**" and click "New" in the top right corner of the screen.



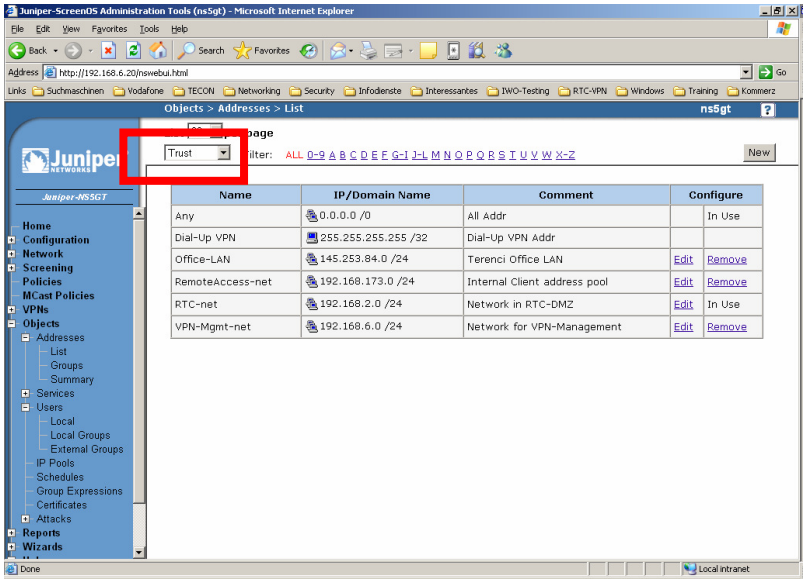
Enter a "Group name" and select the users from the list of available members and insert them into the group by clicking " << ". Make sure the authentication method (IKE user, XAuth, not Auth) is identical for all members. Click OK to accept the changes.



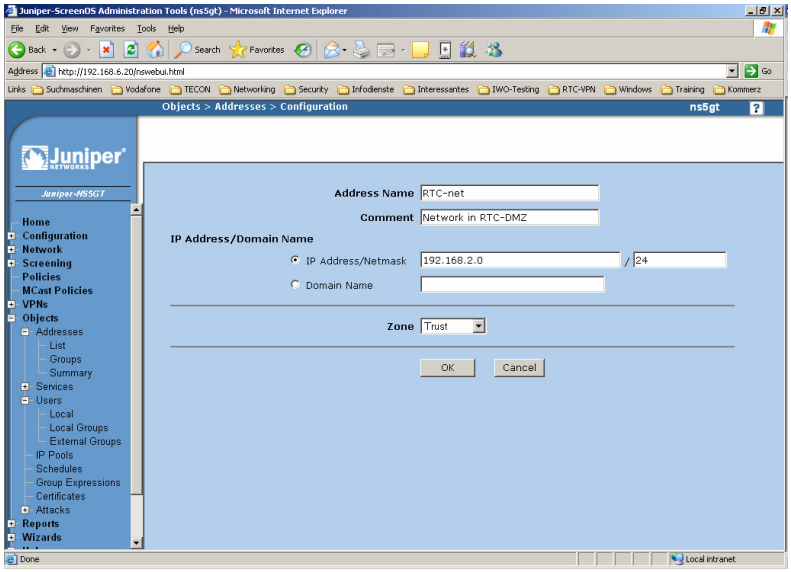
Check in the screen “**Objects > Addresses > Configuration**” if the address object “Dial-Up VPN” is defined. Make sure that the Filter selection at the top left corner of the list shows “Untrust” as the selected zone. If not, define it by clicking “New”. Enter the “Address Name” and the “IP Address/Netmask”. The zone of this network should be “Untrust”. Confirm the changes by clicking “OK”.



Display the address objects of the protected zone by selecting “Trust” at the top left of the list. Define the networks you want to allow access via VPN for later use. Here, we define the “RTC-net”.

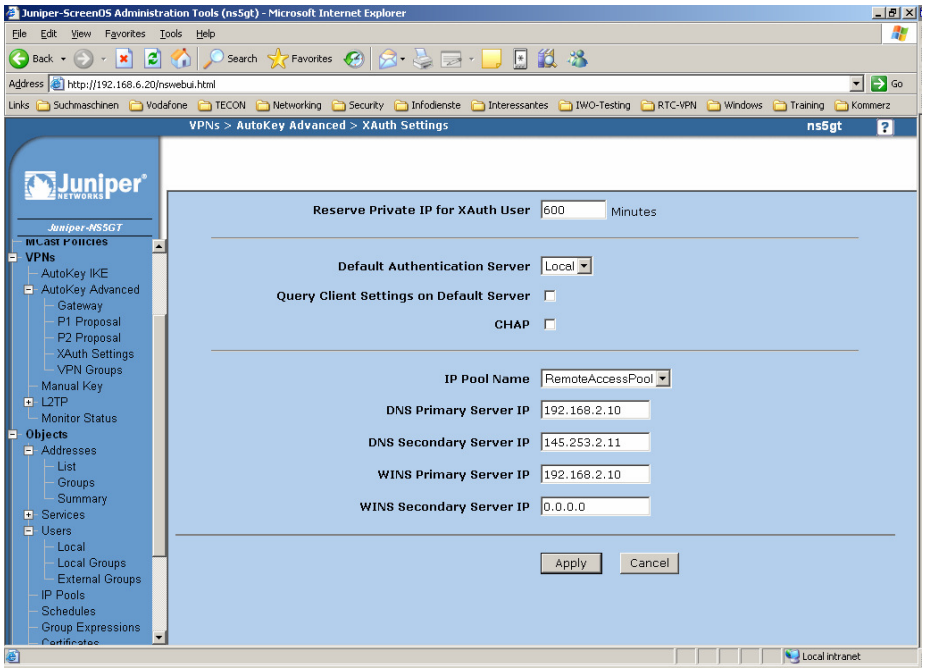


© VODAFONE GROUP 2007



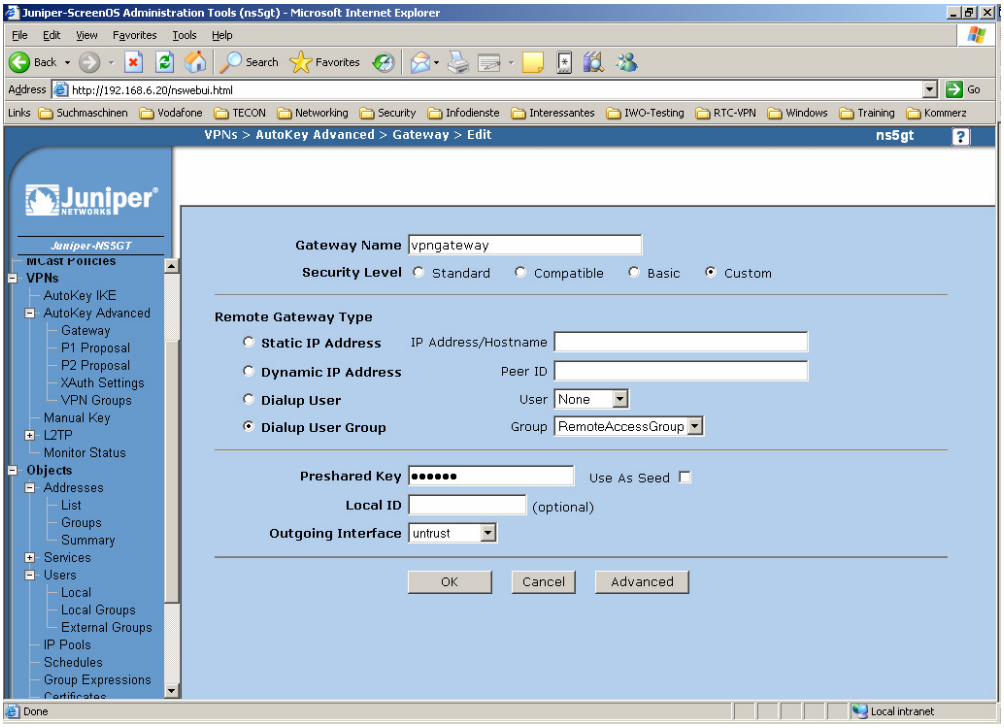
2.4 Configuration of VPN

First, define the default XAuth Settings on the screen "**VPNs > AutoKey Advanced > XAuth Settings**". Set the lease time for the private IP addresses to 600 minutes and select "Local" as the "Default Authentication Server". Again select the previously defined IP pool in the "IP Pool Name" drop down list and define the DNS and/or WINS servers. Confirm the changes by clicking "Apply".



Define a new "VPN gateway" on the screen "**VPNs > AutoKey Advanced > Gateway**" by clicking "New" at the top right corner. Enter a "Gateway Name". Set the "Security Level" to "Custom". Select the "Dialup User Group"-radio-button. Select the previously defined user group from the drop down list. Alternatively, if only one user is needed, the gateway type

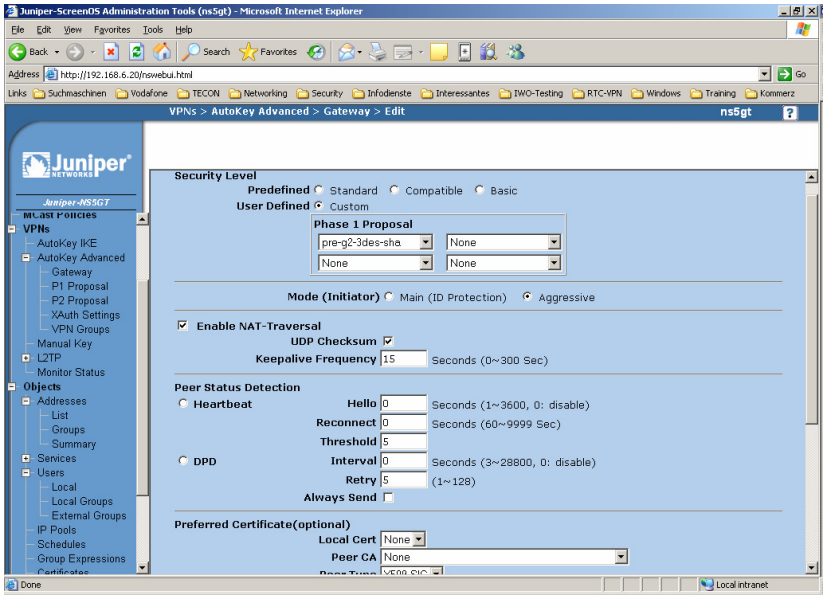
“Dialup User” can be used respectively. Enter a “Preshared Key” that must correspond to the setup in the NetScreen-Remote client. Select “Untrust” as the outgoing interface.



Continue the setup in the advanced setup by clicking the “Advanced”-button at the bottom. Here, the Phase 1 (IKE) proposal is selected. Also, this setup must correlate with the client setup. In this example, 3DES encryption, SHA1 hashing and Diffie Hellman group 2 is used. The drop down option for this “Phase 1 Proposal” setup is named “pre-g2-3des-sha”.

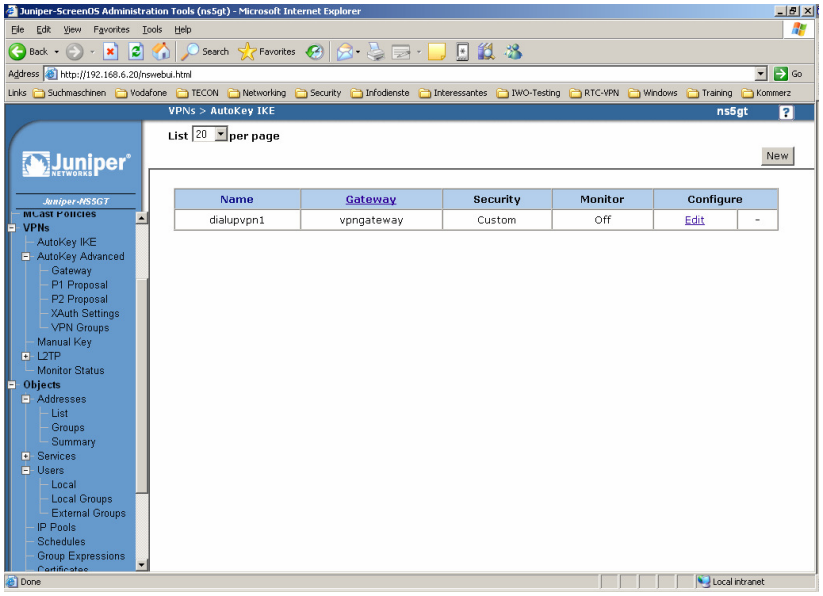
To be able to work on most mobile networks, which use NAT, the checkbox “Enable NAT-Traversal” must be checked. Also enable “UDP Checksum” and set the Keepalive Frequency to a higher value. We recommend a value between 15 and 60 seconds. Due to the Keepalive in the NAT traversal, Heartbeat and DPD is not needed. Click “Return” and “OK” in the previous screen to accept the changes.

© VODAFONE GROUP 2007

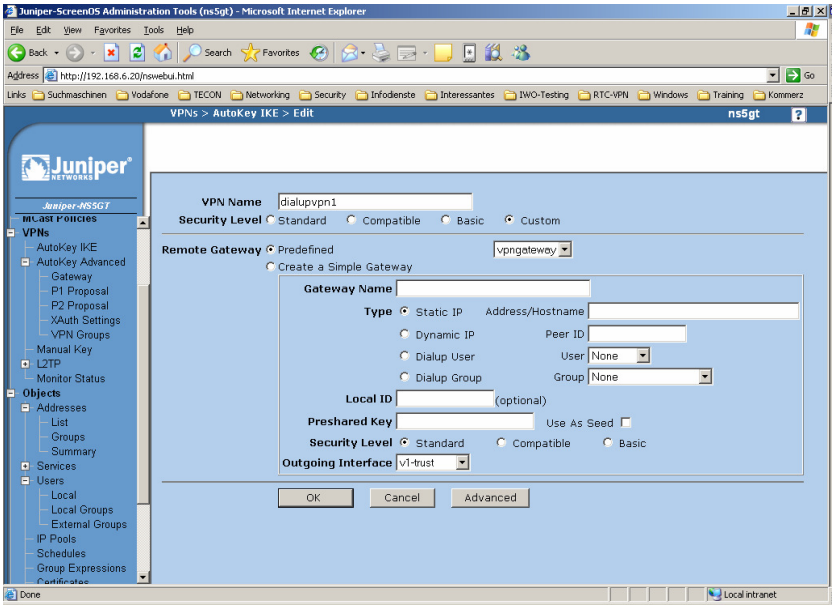


Selecting the predefined “Phase 1 Proposal” “pre-g2-3DES-sha” implies that a re-key interval (“Life Time”) of 28800 seconds (8 hours) is chosen. Alternate proposals can be generated on the “**VPNs > AutoKey Advanced > P1 Proposal”** screen, but the security of the default proposal meets current industry levels.

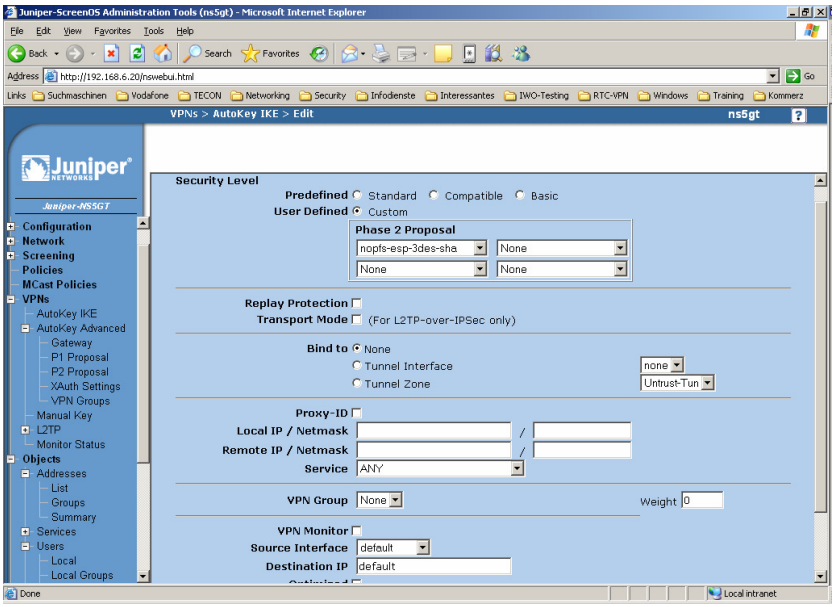
Now define an “AutoKey IKE” object in the “**VPNs > AutoKey IKE**” screen. Click “New” in the top right corner.



Enter a “VPN Name” and select “Custom” as “Security Level”. Select “Predefined” as “Remote Gateway” and select the previously defined VPN gateway. This defines the Phase 1 (IKE) negotiation.



Click the “Advanced” button to define the Phase 2 (ESP) encryption parameters. Make sure the “Security Level” “User Defined” (“Custom”) is selected. Select up to four “Phase 2 Proposals” from the drop down list. In this example, “nopfs-esp-3des-sha” is selected as the only proposal. Click the “Return” button and the “OK” button in the previous screen to confirm the changes.



Selecting the predefined “Phase 2 Proposal” “nopfs-esp-3des-sha” implies that a re-key interval (“Life Time”) of 3600 seconds (1 hour) and no volume limit is chosen and that no “Perfect forwarding Secrecy” was selected in the proposal. Individual proposals can be

generated on the "**VPNs > AutoKey Advanced > P2 Proposal**" screen. But at the time being, the security of the given encryption algorithm and hashing is still industry level. The security could be improved by selecting a proposal supporting PFS, but make sure that this is taken into account on the configuration of the client.

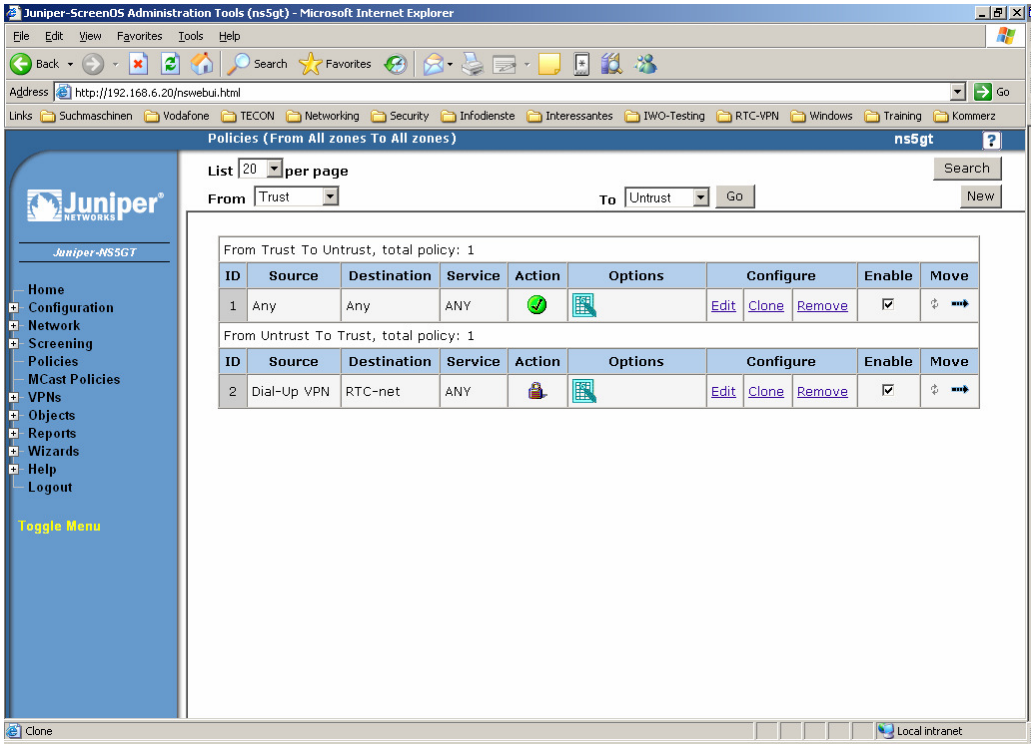
2.5 Configuration of the VPN Firewall Policy

To view the Firewall policies set up on the Juniper NetScreen device, Select "**Policies (From All zones To All zones)"** from the menu tree. All implemented security policies will be displayed. Since we are not explaining the firewalling concept of Juniper NetScreen, only a few remarks to the setup are made:

- The policies handle sessions specified by a matching set of source object / source zone, destination object / destination zone and service. All policies are tested from top to bottom, until a matching policy is found.

- If a session matches in all criteria above, the action defined in the policy is executed. Actions can be "Permit", "Deny", "Reject", and "Tunnel". Permit will allow the session, which includes answers coming back that are related to the original request. "Deny" and "Reject" inhibit the packets to reach their destination. "Tunnel" will encrypt the data.

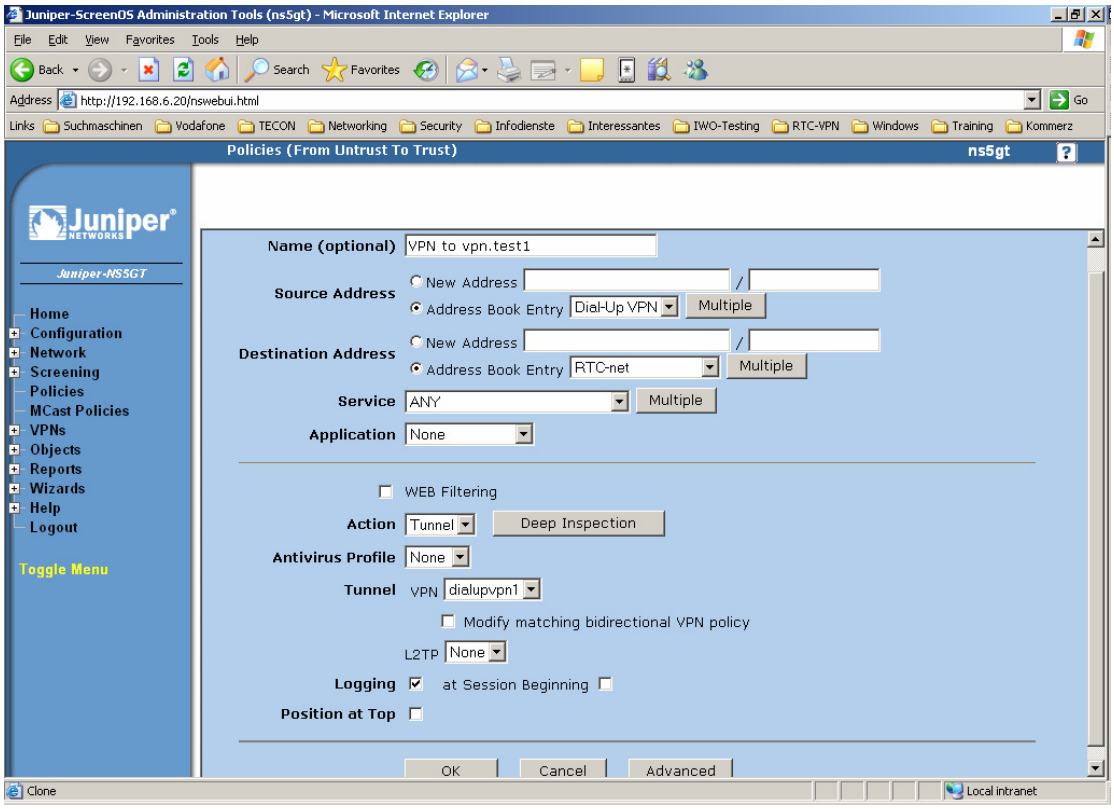
- If no matching policy is found, the session is denied.



For the VPN tunnel, a new policy is needed. Select "From Untrust" "To Trust" and click "New" to open a new Policy. Optionally enter a name in the field "Name (optional)". For the "Source Address" select "Address Book Entry" and select the network object that corresponds to the IP address pool from which the client's internal IP address is chosen

(“Dial-Up VPN). For the “Destination Address”, again choose the “Address Book Entry” out of the drop down list, which corresponds to the internal network that shall be reached via VPN (“RTC-net”). For the example, “ANY” service is allowed.

The Action chosen for this policy is “Tunnel”. Select the previously prepared AutoKey IKE VPN from the drop down list for the field “Tunnel”. “Logging” should be checked. By default new policies are added at the bottom of the policy list. To avoid that this policy is “shadowed” by another policy, the checkmark at “Position at Top” can be checked, which would position the new policy as the first one. Alternatively, the policy can be moved later. Confirm the changes by clicking “OK”.



After confirming, the policy can optionally be moved by clicking on the Ø-icon in the “Move” column in the policy overview. The new position number can be entered in the popup window.

This concludes the VPN configuration. With the appropriately configured client, a remote connection can now be established.

2.6 Advanced Configuration

2.6.1 Disable the client's request for username / password on re-keying

As configured in the IKE proposal (Phase 1, "**VPNs > AutoKey Advanced > Gateway**"), after the configured interval, a re-keying is attempted. In the case that XAuth with user authentication is configured, the re-key process would involve entering user name and password again. In the example here, this would be necessary after 8 hours. To avoid the repeated entry of user name and password, a change of the configuration on the command line interface (CLI) is necessary: The idle timeout must be configured differently from 0. The following command generated by the web interface:

```
set vpn "<name of auto-key vpn>" gateway "<name of vpn
gateway>" no-replay tunnel idletime 0 proposal "nopfs-esp-
3des-sha"
```

Has to be changed to:

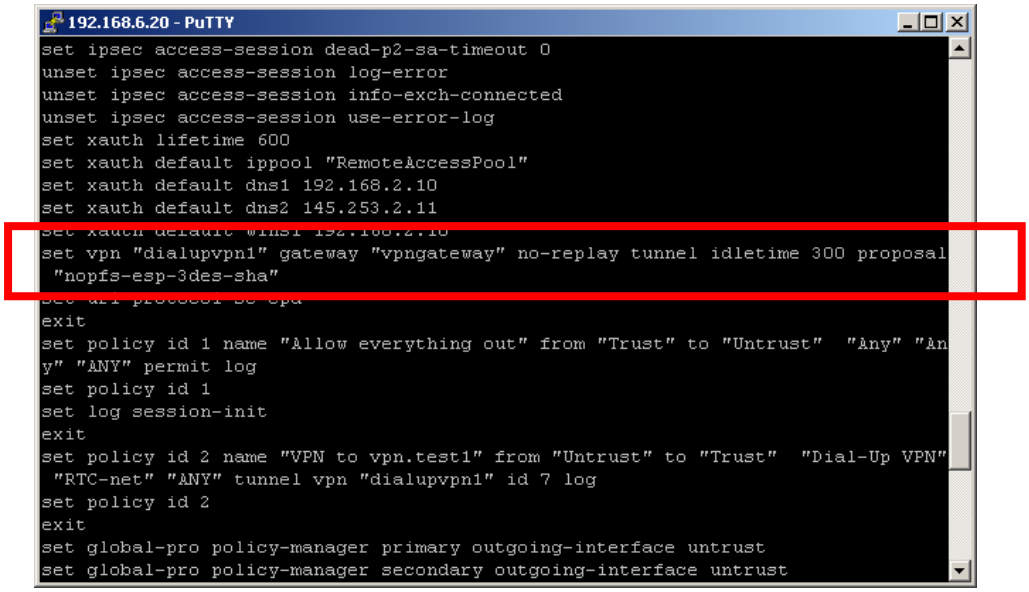
```
set vpn "<name of auto-key vpn>" gateway "<name of vpn
gateway>" no-replay tunnel idletime 300 proposal "nopfs-esp-
3des-sha"
```

This can either be done by saving the configuration file as described below and changing the respective line with an ASCII editor program and then replace the current configuration file with the edited one.

Alternatively, the CLI can be used by logging into the machine via the console interface or Secure Shell. After authentication, list the configuration with the command

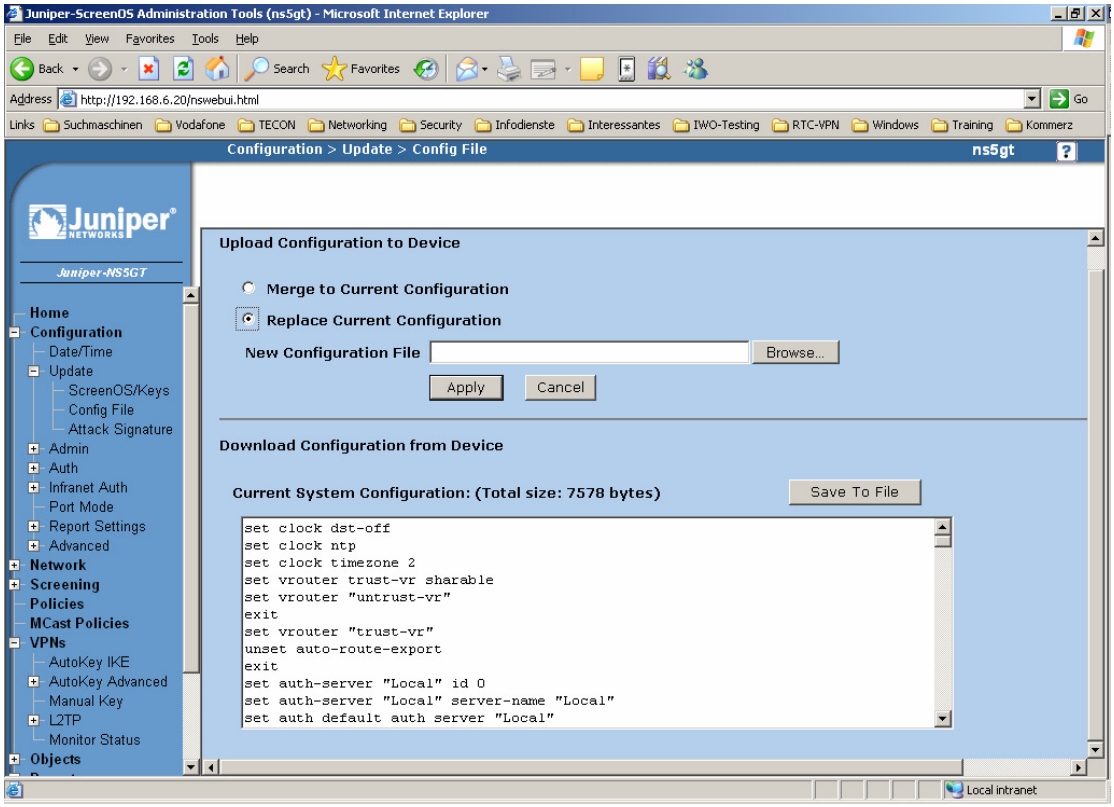
```
get config
```

Identify the above command in the configuration and re-enter it with the parameter corrected.



2.6.2 Backup of the Juniper NetScreen Configuration File

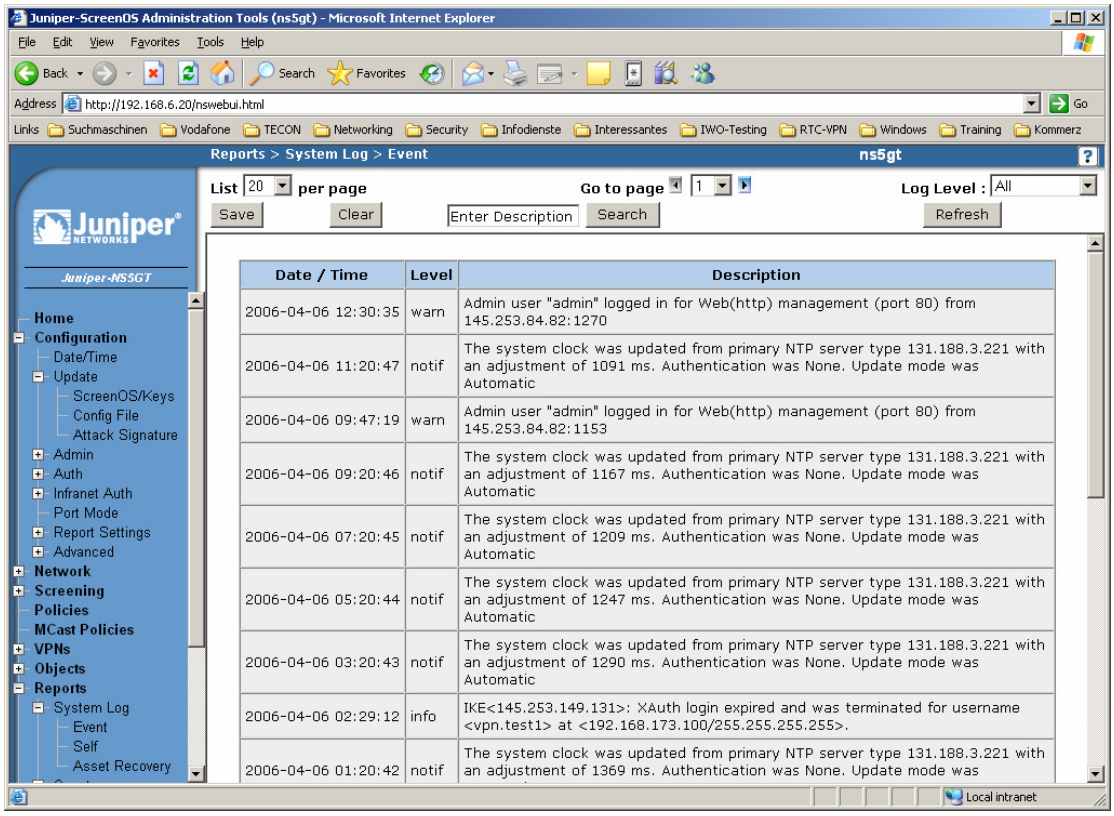
Backup and restore of saved configurations can be done via the Config File Screen "**Configuration > Update > Config File**". In the "Current System Configuration" field, the active configuration can be reviewed. By clicking the "Save To File" button, the ASCII configuration file can be saved to the local PC. This configuration file contains all information necessary to restore the machine.



A previously saved configuration can also be restored by uploading it to the device. Make sure you select "Replace Current Configuration" clicking "Apply", otherwise the new configuration is only merged into the existing one and residual commands may remain from the old configuration.

3 Logging

Event logging is available via clicking "**Reports > System Log > Event**". This screen shows the current events.



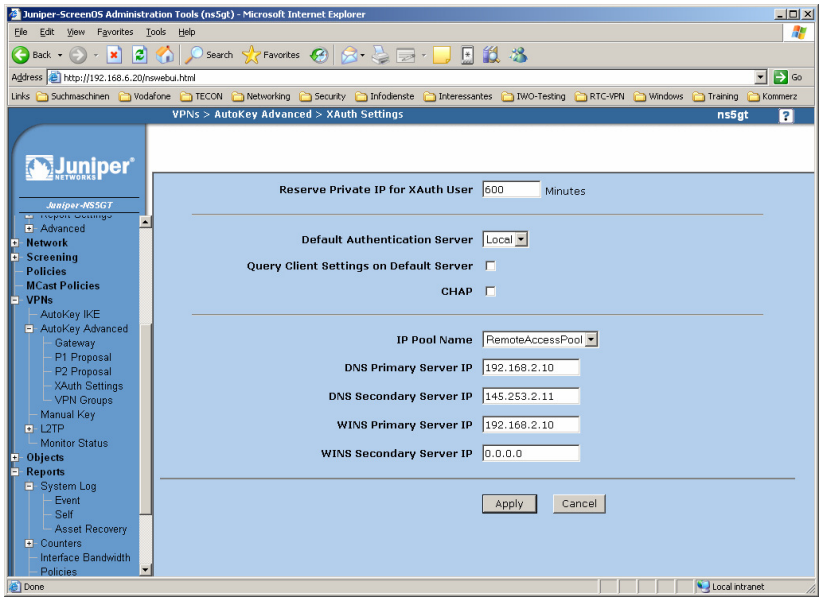
To save a copy of the current event log as a file, click the "Save" button. Further, it is possible to Clear the log or search in it. The current display can be refreshed and the log level can be selected. The user can navigate by selecting the number of entries per page and select the page to be displayed.

To review the statistics, the administrator can display several web pages below the path "**Reports > Counters**" showing statistical counters of key parameters of the device.

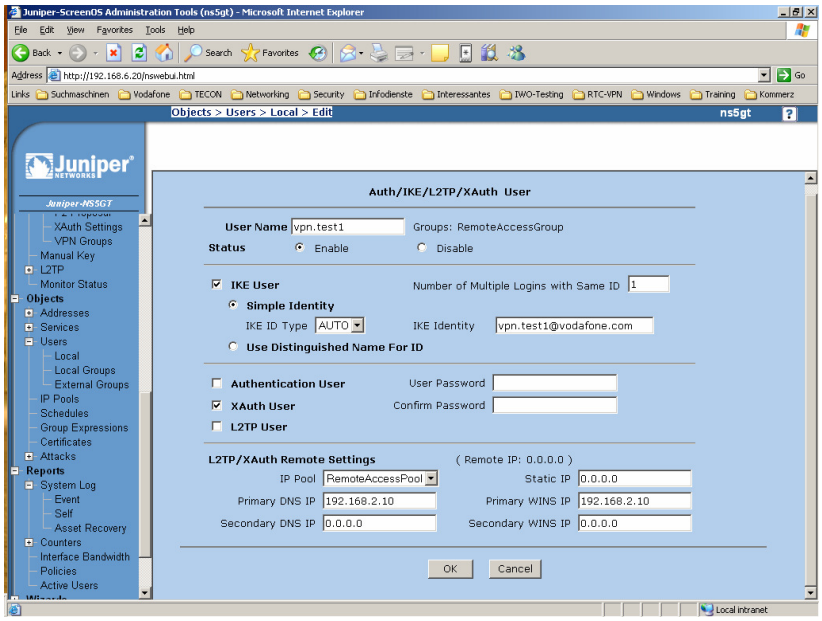
4 Xauth Parameter

Remote DNS and WINS configuration is integrated in the XAUTH setup. After connection establishment DNS and WINS server IP addresses is assigned by the appliance to the Client as primary/secondary DNS resp. WINS server for resolving host names.

The default XAUTH parameters can be reached via the path "**VPNs > AutoKey Advanced > XAuth Settings**".



Additionally, XAUTH parameters can be set on a per user basis in the user setup ("**Objects > Users > Local > Edit**") when "XAUTH user" is checked.



**** End of Document ****