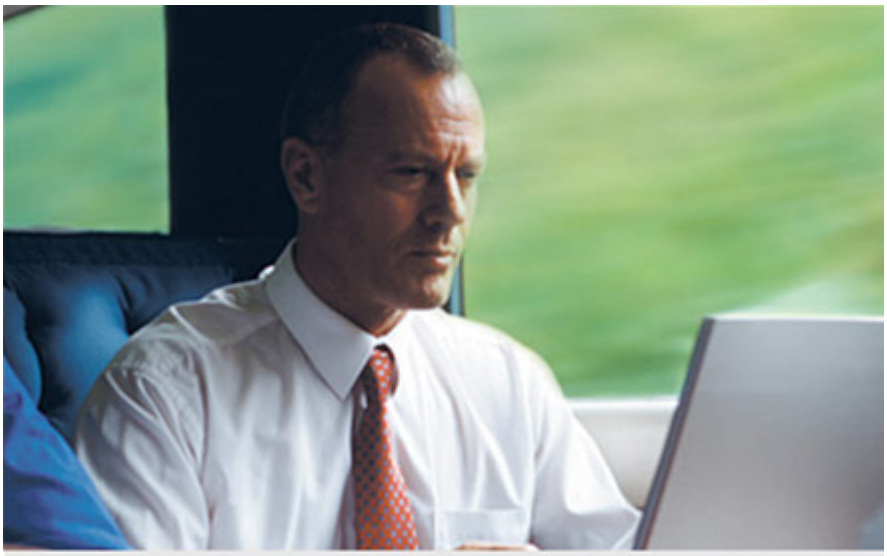
VPN End to End – Netgear VPN Router FVS318 – Appendix A

Appendix A: Netgear VPN Router FVS318

Technical Notes for use with Vodafone Mobile Connect services

Date: **26 June 2006**

Revision No: **2.1**



Vodafone Mobile Connect

VPN Guide

© 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	June 2006	Creation of separate document for client configuration. Update to new versions of VPN software and focus on 3G network performance.
3.0	May 2007	Minor changes & R9 review

File Reference

VPN_Netgear_FVS318_App A.doc

Document Authors

Peter Jaeger, TECON Terenci
Miroslaw Grzesica, TECON Terenci
Joerg Pfeffer, 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 Netgear VPN Router Installation and Configuration (Version 3.0_22) 5

2.1 Initial setup 5

2.2 Netgear Smart Wizard configuration assistant 5

2.3 Configuration of Routing 8

2.4 Configuration of VPN 10

2.5 Configuration of the Firewall Policy 15

2.6 Advanced Configuration 16

3 Logging 18

Tables & Figures

Figure 1: Netgear VPN Router FVS318 5

© VODAFONE GROUP 2007

1 Executive summary

This Appendix is in addition to the detailed document for Netgear firewall/VPN appliance and describes the setup and update process in a detailed way with example screen shots taken from the initial processes.

- Only Version 3 of the Netgear hardware is supported with mobile networks.
- Care must be taken to ensure client and concentrator parameters match exactly as this is not handled automatically by the VPN system.
- If different VPN clients are used, individual IKE and IPSec policies must be established for each client.

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

© VODAFONE GROUP 2007

2 Netgear VPN Router Installation and Configuration (Version 3.0_22)

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 Netgear VPN Router FVS318 to configure a VPN with UMTS/GPRS usage.

The current hardware revision of the Netgear FVS318 is Version 3. This description is based on this Version.

Due to missing support for IPSec encapsulation, Version 1 is not able to be used with most 3G or GPRS networks. Version 2 is only partially usable.

For these older versions, please refer to the documentation available with the VPN router or online at http://www.netgear.com.

2.1 Initial setup

After unpacking the device, connect the WAN interface to the internet and one of the LAN switch ports to the management PC. The PC must be configured to use DHCP to receive the IP address and network data from the network. Connect the power.

Figure 1: Netgear VPN Router FVS318

The IP address for the management PC will be assigned via DHCP. Open a web browser. You will be redirected to the Netgear Smart Wizard configuration assistant for the initial configuration.

If not, enter the URL http://192.168.0.1/BSW_welcome.htm.

2.2 Netgear Smart Wizard configuration assistant

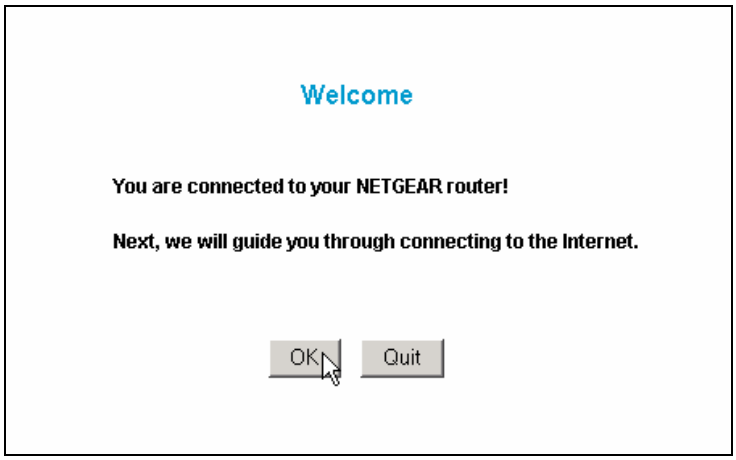
The initial configuration is aided by a start up wizard when using a web browser for the initial setup.

We recommend using one of the following web browsers to contact the Netgear VPN Router FVS318.

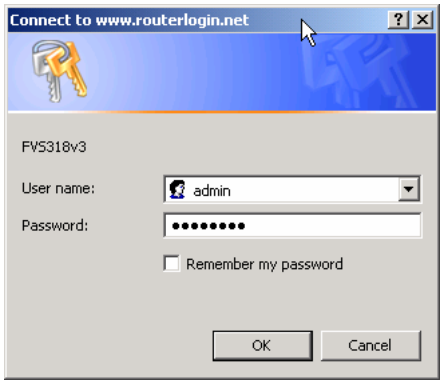
- Microsoft Internet Explorer version 6.0 SP1 or higher (Windows) (SP2 required for Windows XP)
- Netscape Navigator version 7.2 or higher (Windows, Linux, or Solaris)
- Mozilla 1.73 or higher (Windows, Linux, or Solaris)
- Firefox 1.0 or 1.5 (Windows, Macintosh, or Linux)

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.

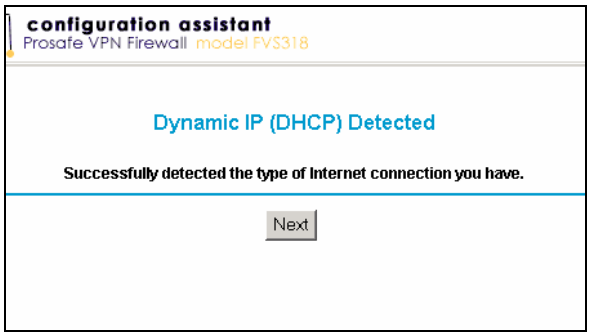


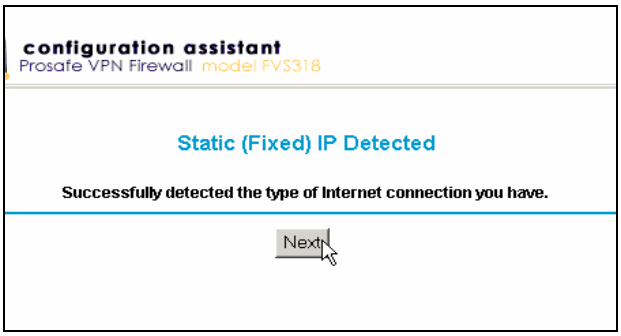
The user must authenticate to continue. The default username is “admin”, the password is “password”.



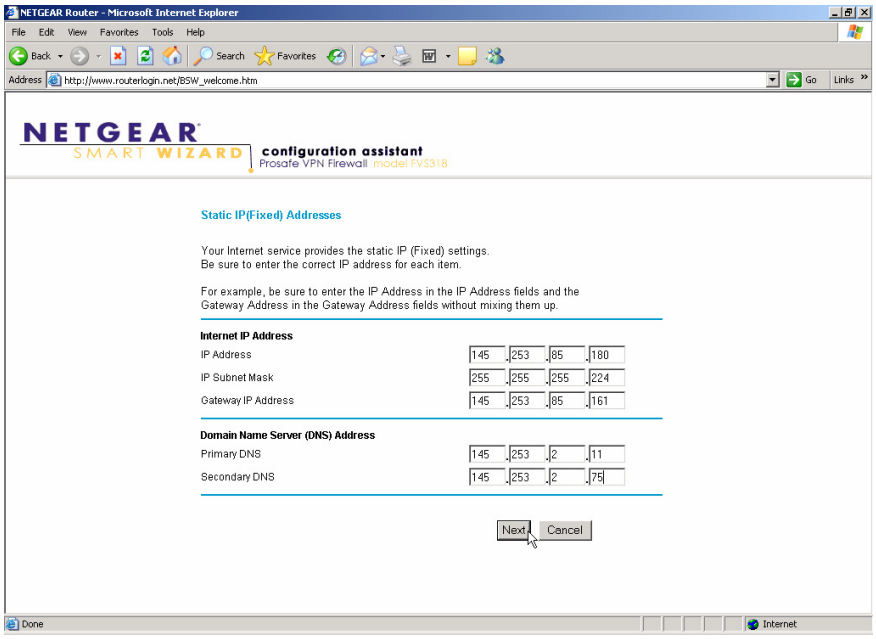
Next, the wizard will try to detect the internet connection. Make sure the WAN connection is connected to the device and the link is showing active. After a while, the router may have detected how to connect to the internet, e.g. via PPPoE, DHCP or static IP address.

© VODAFONE GROUP 2007





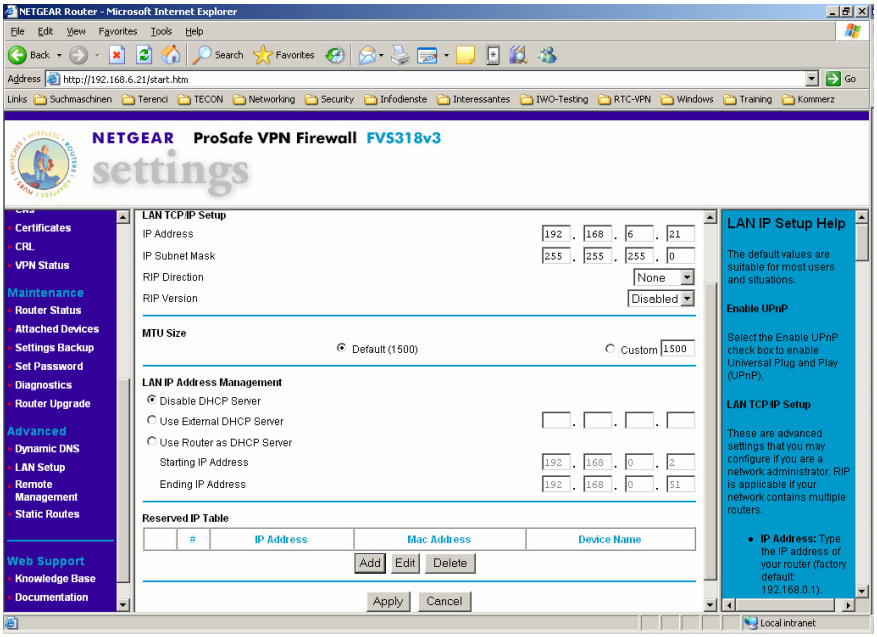
According to the type of internet connection, further parameters will be requested.



Then, the router tries to access the internet using the entered parameters. If successful, the wizard will apply the WAN setup and restart the router.

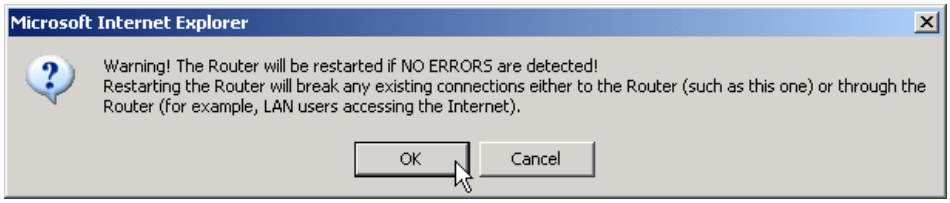
Further configuration can be done via the URL http://192.168.0.1/start.htm.

To setup the LAN interface, use the URL above to enter the settings. Go to the screen "**Advanced > LAN Setup**". Set the IP address and subnet mask according to the network's necessities.



If needed, enable the built-in DHCP server and enter the IP range used for the clients.

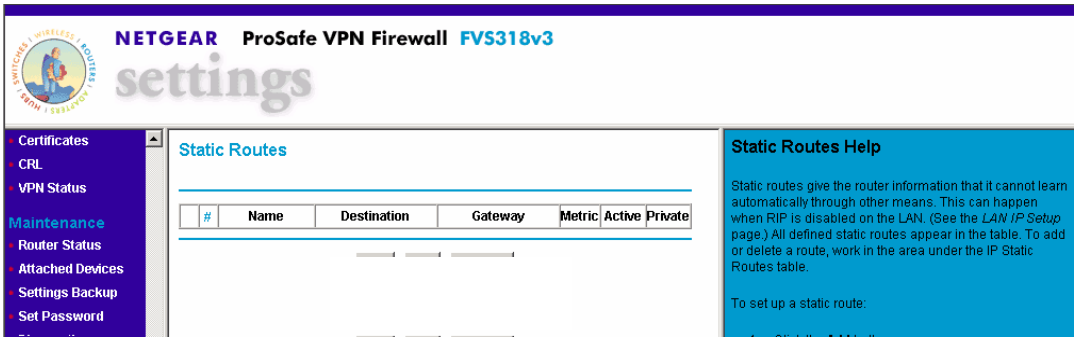
Click “Apply” to accept the settings. Keep in mind that the network settings will change immediately and the management PC must be adapted to the changed network settings to continue with the setup of the Netgear VPN router. The Netgear VPN router will restart to adapt to the changed settings and the current browser connection to the device will be lost.



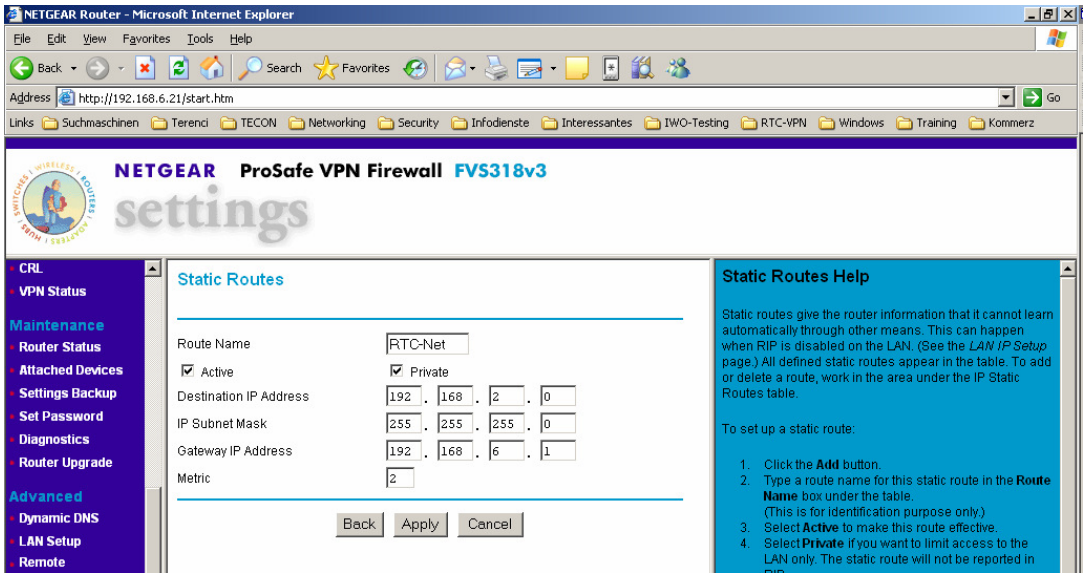
2.3 Configuration of Routing

After the Netgear Router has rebooted and the adaptation of the management PC’s network settings, open the browser with the URL http://<your Netgear router’s LAN IP address>/start.htm. (Insert the IP address entered in the LAN Setup in the URL).

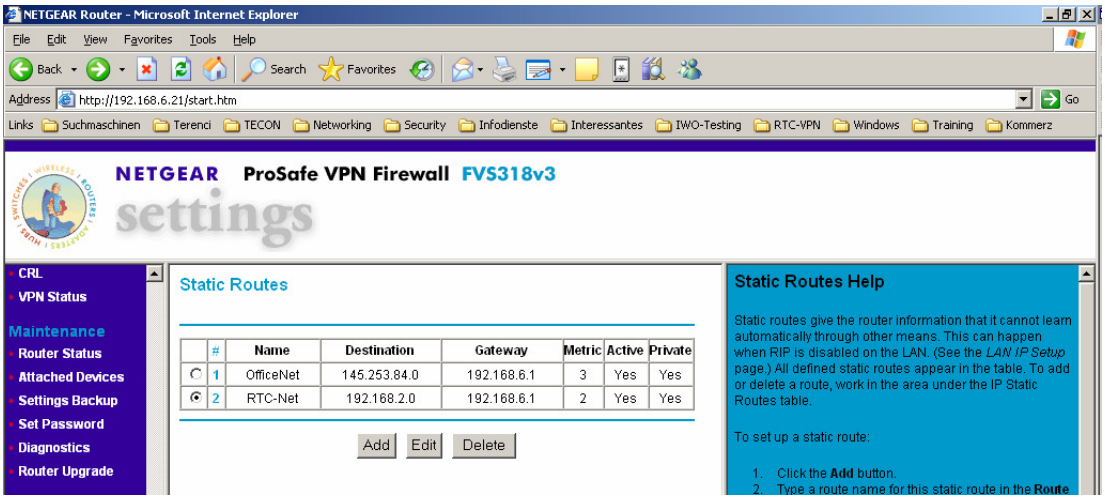
Go to the screen at “**Advanced > Static Routes**”.



Click “Add” to open a window to add a new route.



Enter a name for the route, network address, network mask, gateway address and Metric. The Metric represents the number of routers to the target network and must be between 2 and 15. Click “Apply” to save the route. Add routes until finished.



© VODAFONE GROUP 2007

2.4 Configuration of VPN

Unfortunately, the Netgear VPN Router needs one “IKE Policy” and one “IPSec Policy” per VPN client. There is no user data base or generic VPN client configuration as with other VPN gateways.

Further, the clients are not automatically configured from the Netgear router, so that the setup on both client and router must match.

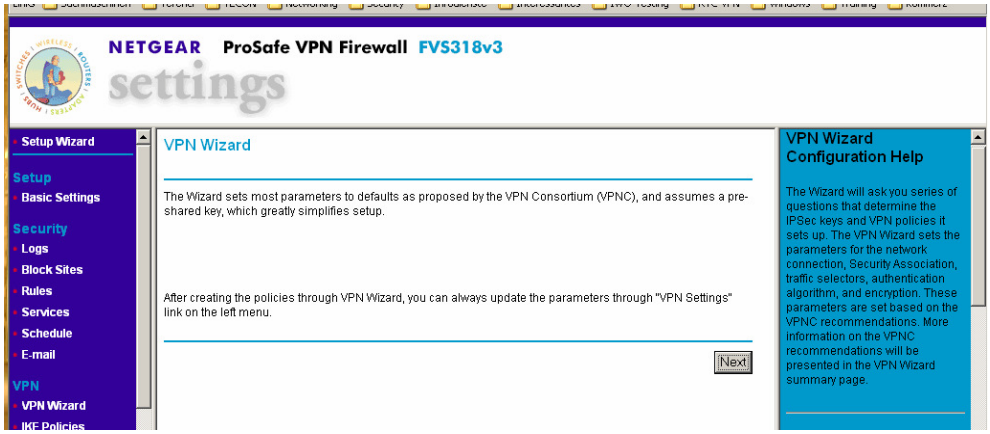
To ensure optimal setup, before starting the configuration, we recommend making a list containing the following items for each client to be configured.

- user name (any unique character string)
- Password (Pre-shared secret key, at least 8 characters, alternatively certificates)
- IP address from internally defined range
- IP range or network to be accessed by the user via the remote access

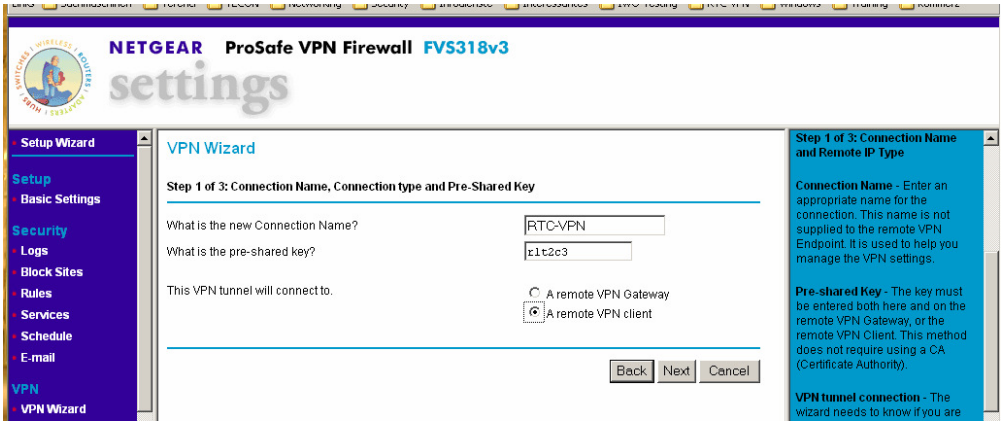
Further, the following parameters should be clarified in advance (Recommendation in brackets):

- IKE/Phase 1 Encryption algorithm (3DES)
- IKE/Phase 1 Hash or authentication (SHA-1)
- IKE/Phase 1 SA life time (28800 seconds / 8 hours)
- IPSec/Phase 2 Encryption algorithm (3DES)
- IPSec/Phase 2 Hash or authentication (SHA-1)
- IPSec/Phase 2 SA life time (3600 seconds / 1 hour)
- Perfect Forwarding Security / PFS (No)

To set up an initial IKE- and VPN policy, use the VPN wizard available via “**VPN > VPN Wizard**”. Click “Next” to continue.

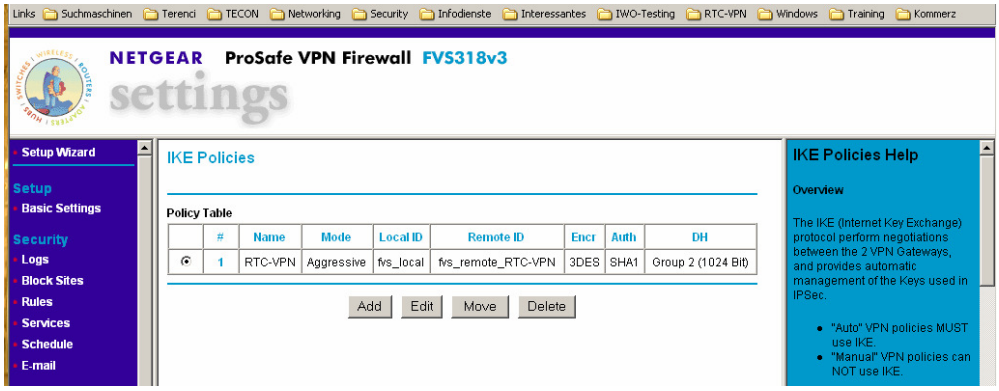


Enter a Connection name and a pre-shared key. **Make sure that the key has a minimum length of 8 characters.** Select “A remote VPN client” as the peer for this connection. Then click next.



The wizard will display the generated “VPN-Auto Policy”. Click “Done” to confirm it.

Go to the screen “VPN > IKE Policies” to adapt the Phase 1 parameters. Click “Edit” to adapt the policy generated by the wizard.

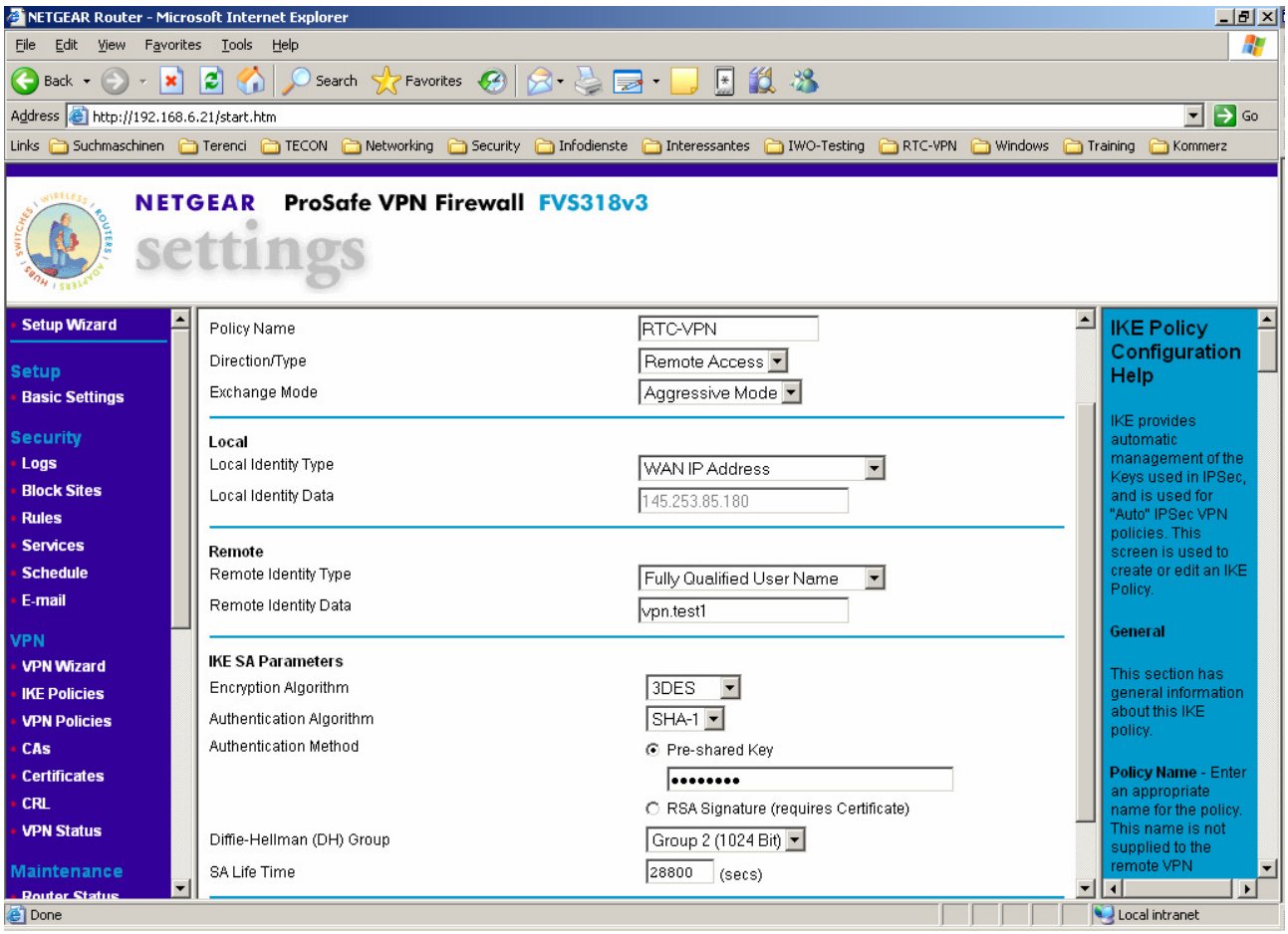


You will need one IKE Policy per used VPN client. Within the Policy configuration, **for each IKE Policy, the Policy Name and the Remote Identity Data must be unique.**

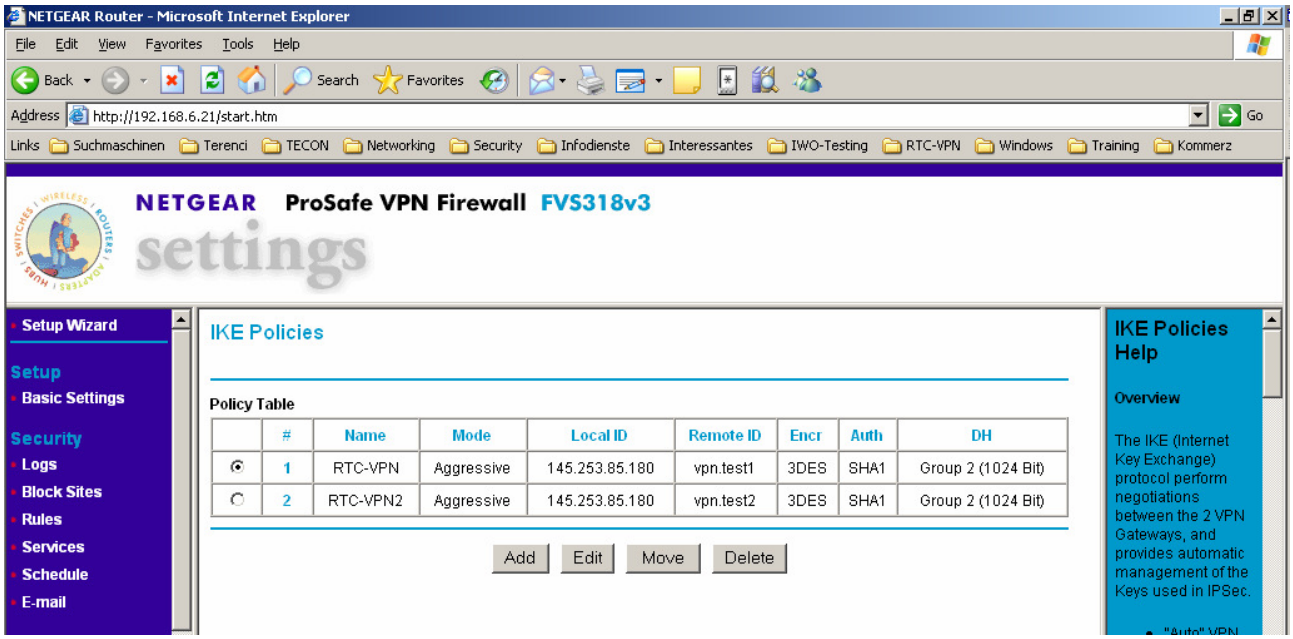
The Direction/Type must be “Remote Access”; the Exchange Mode must be “Aggressive Mode” to work with the ProSafe VPN Client. The local Identity Type can be set to WAN IP Address if the IP address of the gateway is a static address. In this case, the Local Identity data will be supplied automatically.

The Remote Identity Type should be set to Fully Qualified User Name. In this case, the Remote Identity Data can be any unique character string. **Make sure to note down this user name, since it is needed for the client configuration.** See appendix B.

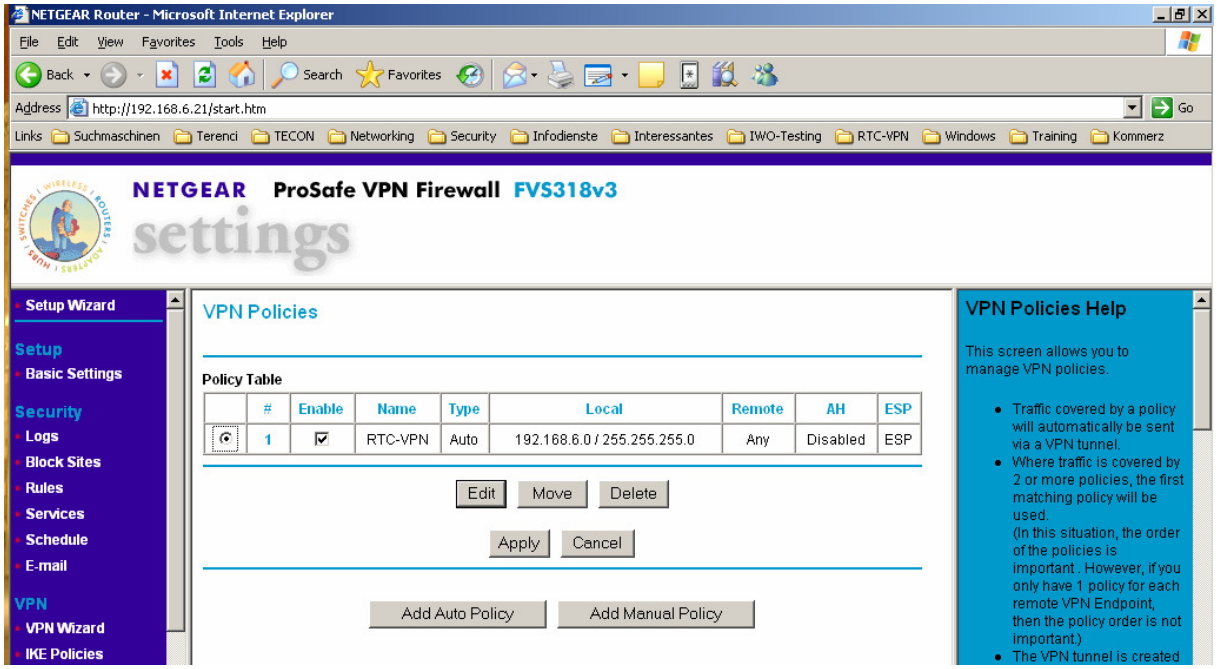
We recommend using 3DES encryption or higher and SHA-1 authentication. As authentication method, Pre-shared key is used. **Make sure the key length is at least 8 characters!** The Diffie-Hellman-Group should be 2 or higher. For secure operation, we recommend a SA life time of 8 hours or 28800 seconds.



Click “Apply” to commit any changes. Add as many IKE Policies as Remote VPN Clients.



Go to the “VPN > VPN Policies” screen. Here, one VPN Policy for each IKE policy is needed. Edit the existing VPN Policy and add as many policies as needed by clicking “Add Auto Policy”.



As with the IKE Policy, the Policy name must be unique for the VPN Policies. Select one of the corresponding IKE Policies from the drop down list. There is no IKE Keep Alive needed, because the VPN client is generating it automatically. We recommend setting the SA Life Time to 1 hour or 3600 seconds. IPSec PFS is not needed but increases security

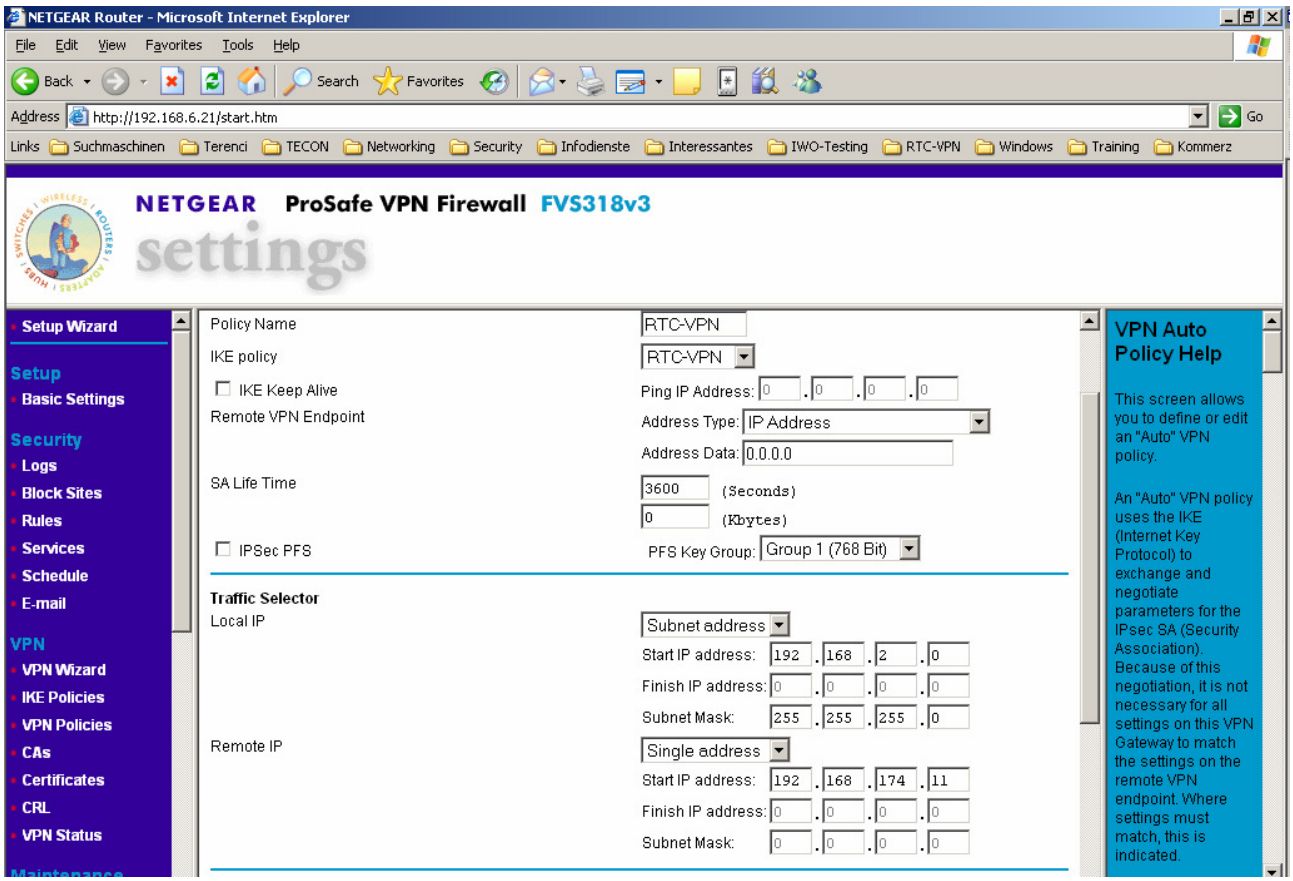
© VODAFONE GROUP 2007

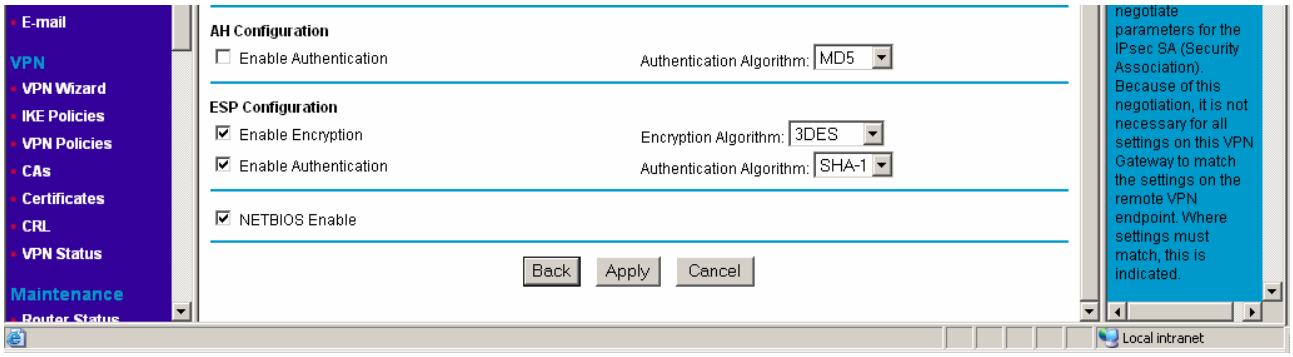
from “man in the middle”-type attacks. Make sure to configure the parameters identically on the client.

The “Traffic Selector” defines the network involved in the VPN connection: The local IP part represents the hosts or network the VPN client needs to access via the VPN connection. Select the address type according to the need (e.g. subnet address, range, any) and enter the network data accordingly. The remote IP is the internal IP address of the VPN client. That means, the Netgear router has to know the IP address which will be configured on the virtual network interface of the VPN client to route the data correctly.

AH is not needed, so remove the checkmark in front of “Enable Authentication” in the AH configuration. Authenticity of the data is also ensured by the encryption via ESP. Check “Enable Encryption” and “Enable Authentication” in the ESP configuration. We recommend 3DES encryption and SHA-1 authentication.

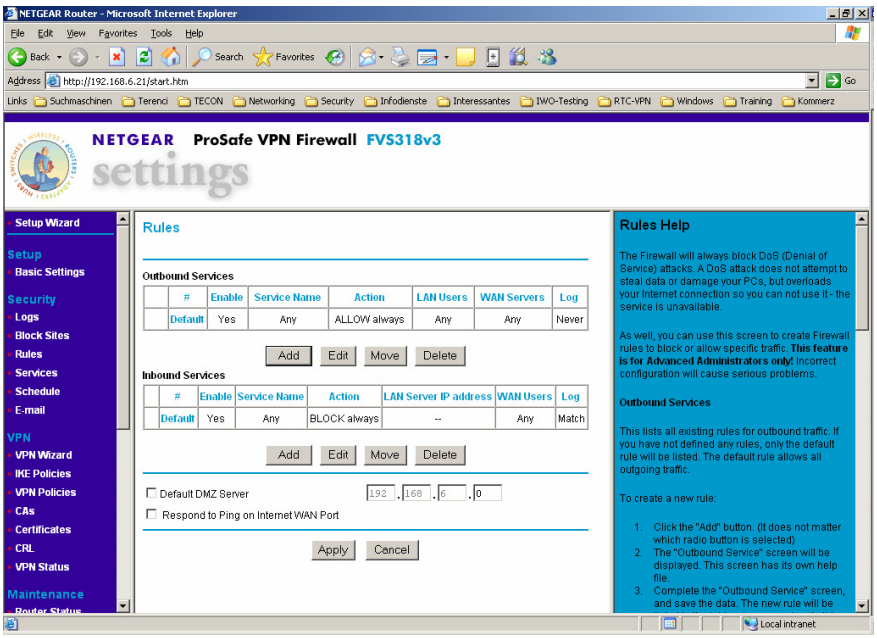
Check “NETBIOS Enable” to transfer NetBIOS data. Commit changes by clicking “Apply”.





2.5 Configuration of the Firewall Policy

The firewall policy is initially set up to block any traffic from the outside and allow any traffic from the inside. For setting up a VPN, this policy is sufficient. Change the Security rules according to your needs at "**Security > Rules**".



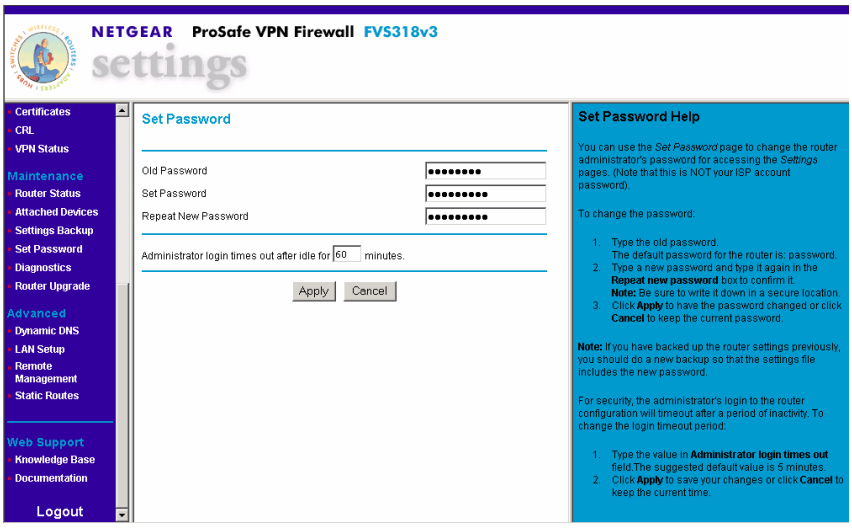
- The firewall differentiates between Inbound and Outbound Services. The firewall is stateful, that means it will pass answers returning automatically.
- The policies handle sessions specified by a matching set of Service Name, source (LAN user), and destination (WAN Servers). All policies are tested 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 "BLOCK", "BLOCK by schedule", "ALLOW", and "ALLOW by schedule". Schedule can be a combination of weekday and time of day.
- If no matching policy is found, the default rule is executed.

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

2.6 Advanced Configuration

2.6.1 Set Administrator Password

Go to the screen "**Maintenance > Set Password**". Enter the current password and the new password. Repeat the new password in the "Repeat" field.

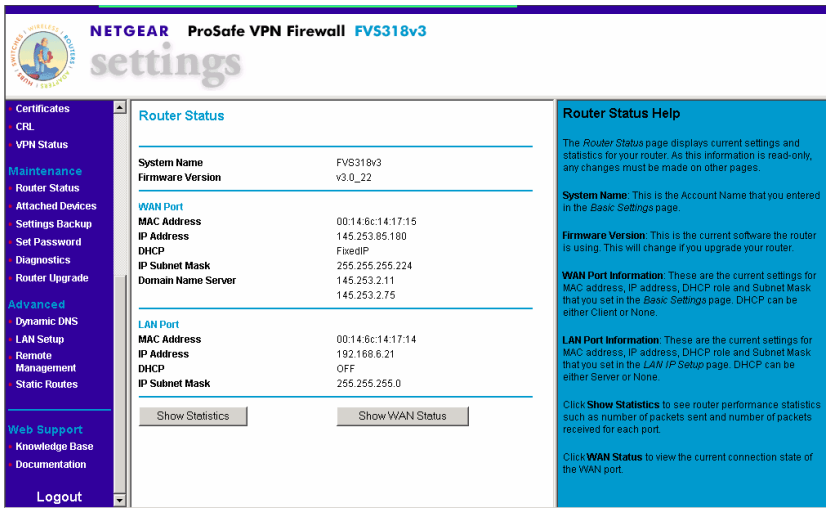


2.6.2 Upgrade the Router Firmware

The router can be upgraded by downloading a firmware file to the router. The file can be obtained on the Netgear homepage http://www.netgear.com. Download this file to the management PC to make it available.

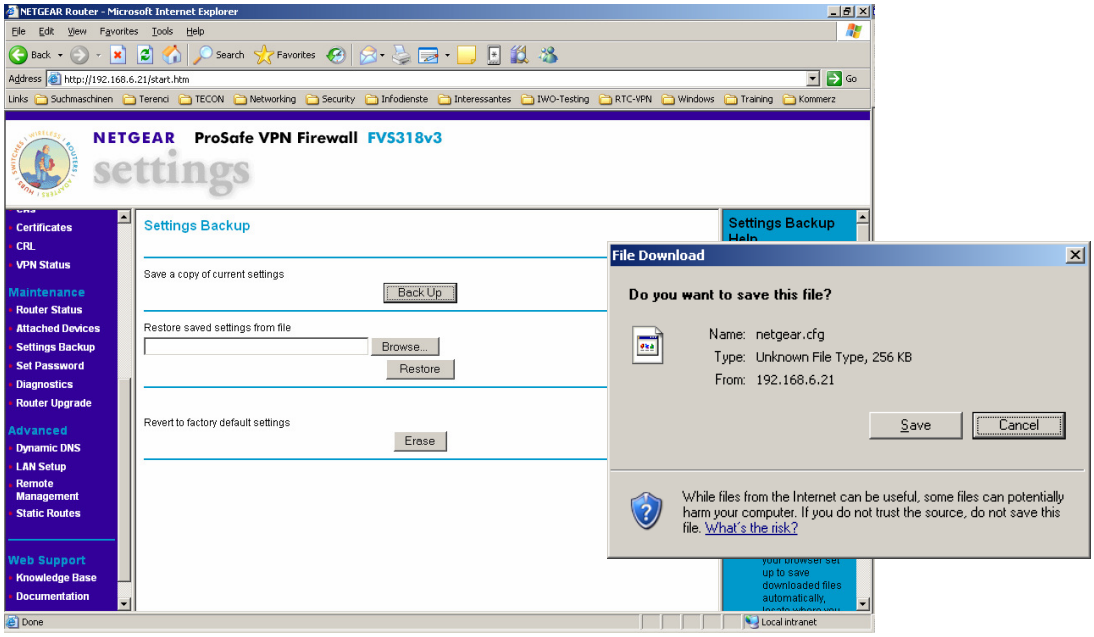
Go to the screen "**Maintenance > Router Upgrade**". Click "Browse…" to locate the firmware file on the management computer. Click upload to transfer it to the device. The router will ask you to confirm the upload.

The router will reboot to activate the new firmware after download was completed. After re-login, check the active version by opening the screen "**Maintenance > Router Status**".



2.6.3 Backup of the Netgear Configuration File

Backup and restore of saved configurations can be done via the Config File Screen "**Maintenance > Settings Backup**". By clicking the "Back Up" button the configuration file can be saved to the local PC. This configuration file contains all information necessary to restore the machine.

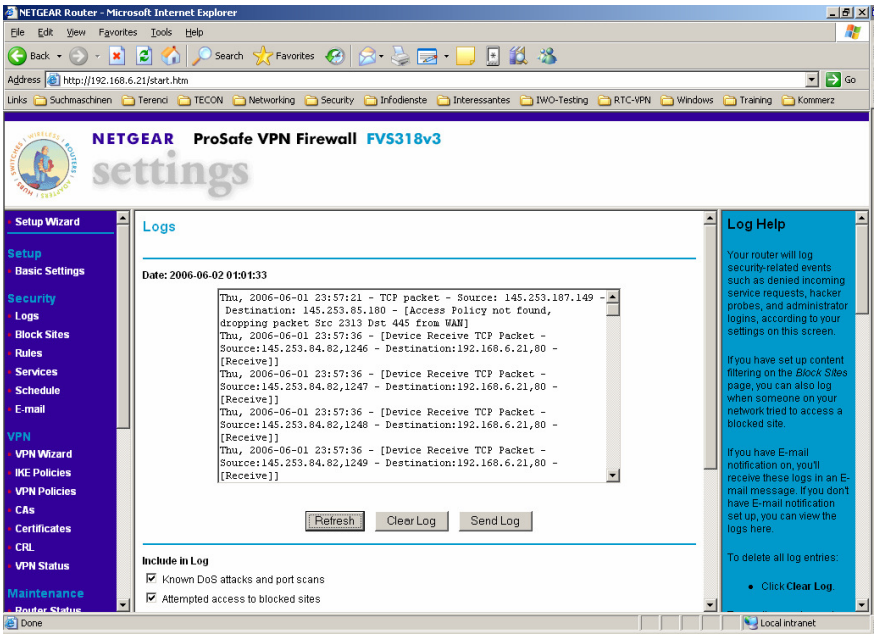


A previously saved configuration can also be restored by uploading it to the device. Click "Browse" to select the file and then click "Restore"

If necessary, the factory defaults can be restored by clicking "Erase"

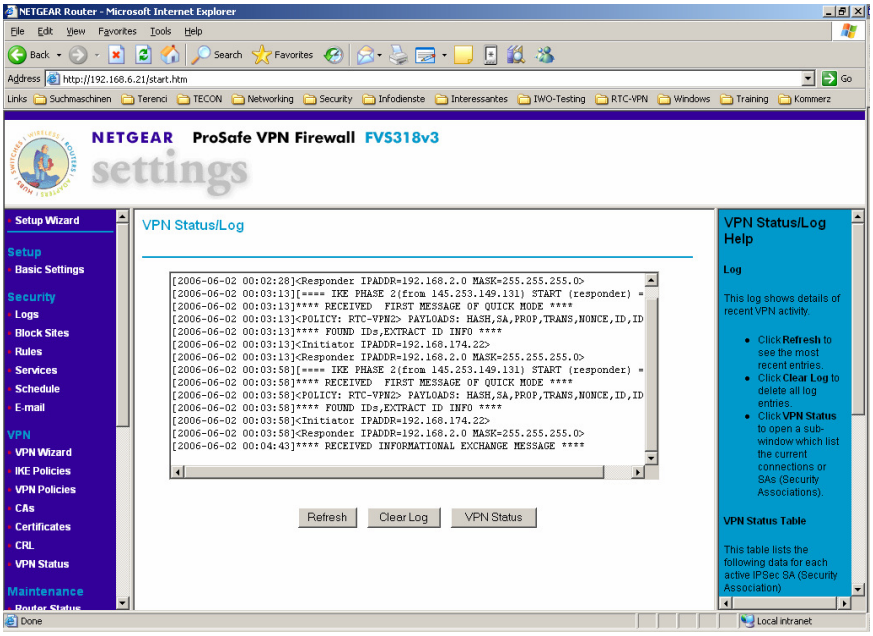
3 Logging

Event logging is available via clicking "**Security> Logs**". This screen shows the current firewall events.

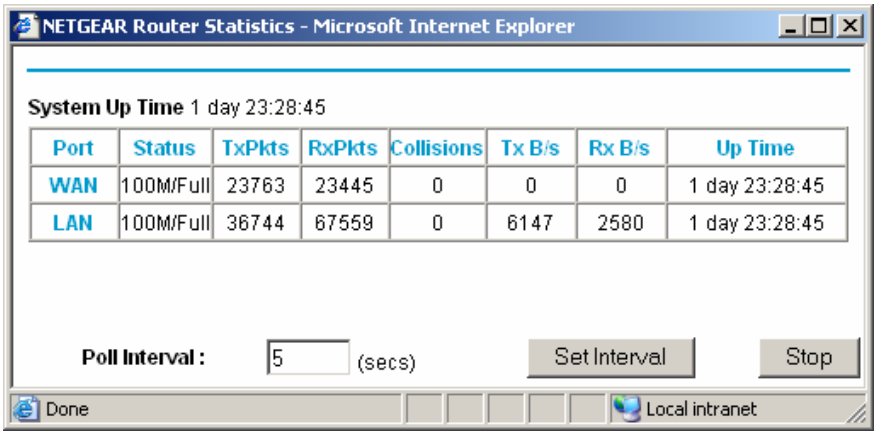


Via the options below "Include in Log", the information displayed can be extended.

VPN logs and user information can be found below the path "**VPN > VPN Status**".



Statistical information can be obtained by opening the screen "**Maintenance > Router Status**". Clicking "Show Statistics" will open a new window.



**** End of Document ****