Securepoint Security Systems

Version 2007nx Release 3

SECUREPOINT

Contents

VPN with IPSec and roadwarrior (GreenBow VPN client))

A VPN connects one or several computers or networks by using a different network, e. g. the internet, as a means of transport. For instance, this could be the computer of a member of staff at their home or in a subsidiary which is linked to the network at the headquarter through the internet.

For the user, the VPN looks like a normal network connection to the destination computer. The actual way of transmission is not perceived. The VPN provides the user with a virtual IP-connection which is tunneled by an actual one. The data packages transmitted via this connection are encoded at the client and decoded by the Securepoint servers - and the other way around.

Target: Setting up a VPN with IPSec between the Securepoint appliance and a roadwarrior (VPN-Client).

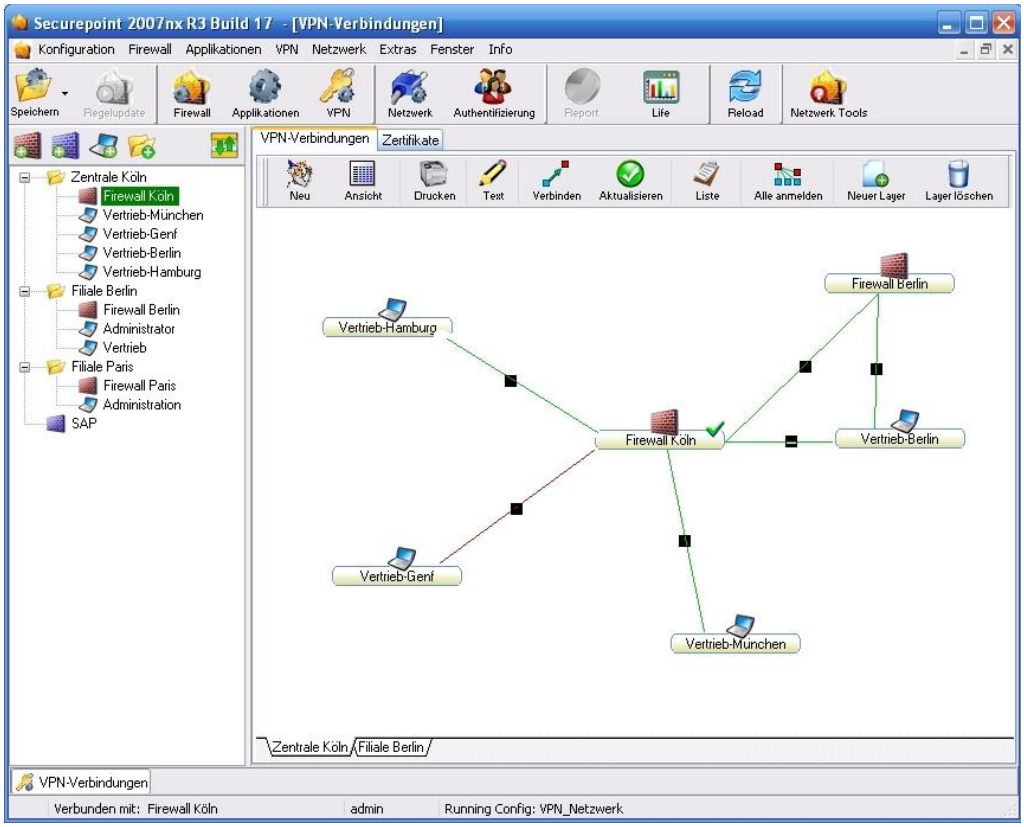

fig. 1 VPN layer

1 Configuration of the appliance

1.1 Setting up network objects

The first step is to create a number of network objects. In this example the roadwarriors were set up as individual objects and moved into the group “Grp-roadwarrior“. They may also be bundled in a subnet (192.168.31.0/24). This is useful when all roadwarriors always have the same privileges. In that case an exact identification as described in section (A) would not be necessary. A configuration as in section (B) would be sufficient.

4 computers and 3 computer groups are created:

Computer group	**Computer**	**Meaning**
Grp-external-interface	external-interface	The external firewall interface.
Grp-internal-net	internal-net	The internal net
Grp-roadwarrior	Roadwarrior01 Roadwarrior02	The roadwarriors (VPN clients).

Proceed as follows:

- Over *Firewall* select the tab *Network-objects.* Click on the button *Computer*.

Two possibilities are presented to you here. If you have a permanent IP-address, continue with A (permanent IP-address). In the case of dynamic IP-addresses continue with B (dynamic IP-addresses).

Section A permanent IP-address

- The IP is inserted, therefore the bitcount 32 has to be (= Host). The zone is firewall-external. A symbol has to be selected in the group Grp-external-interface.

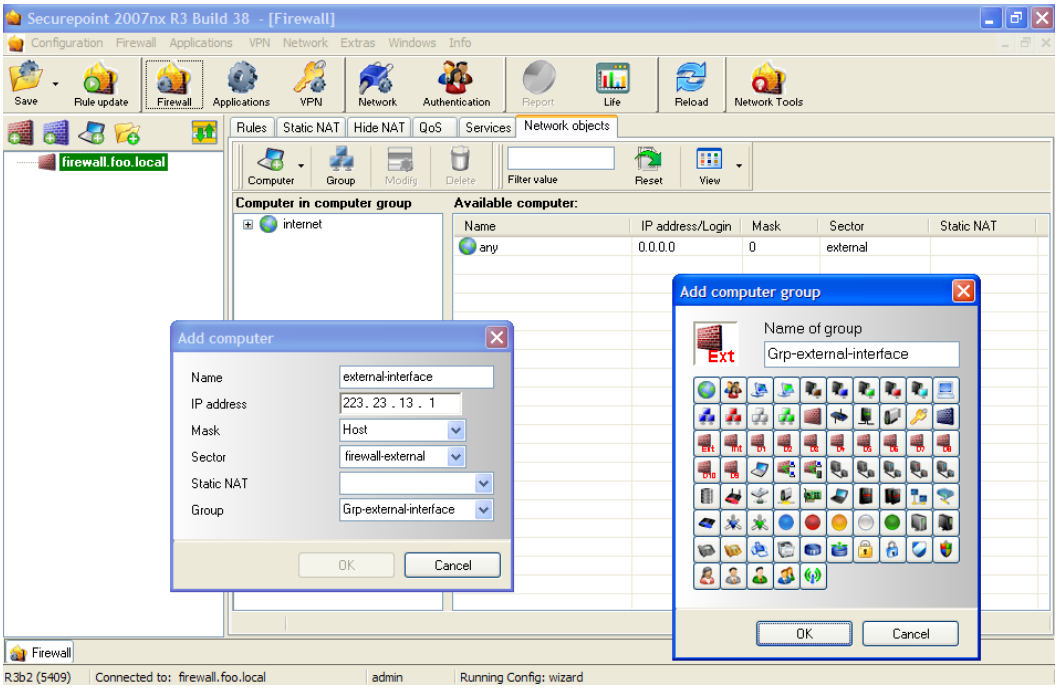

fig. 2 external interface with permanent IP-address

Section B dynamic IP-address

- If a permanent IP does not exist, but a dynamic DNS service (dyn-DNS) is used, the interface has to be set up with the IP 0.0.0.0 and the mask 0.

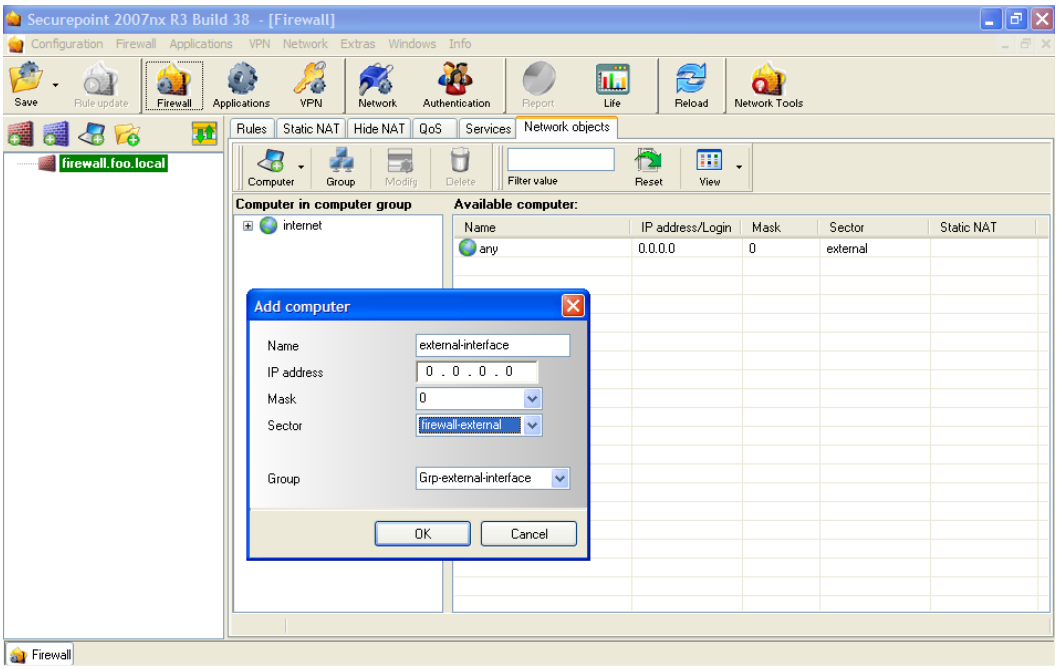

fig. 3 external interface with dynamio IP-address

- Now set up the internal net and the roadwarriors in the way shown.
  The first roadwarrior here receives the IP 192.168.31.1. The second roadwarrior receives the IP 192.168.31.2 .

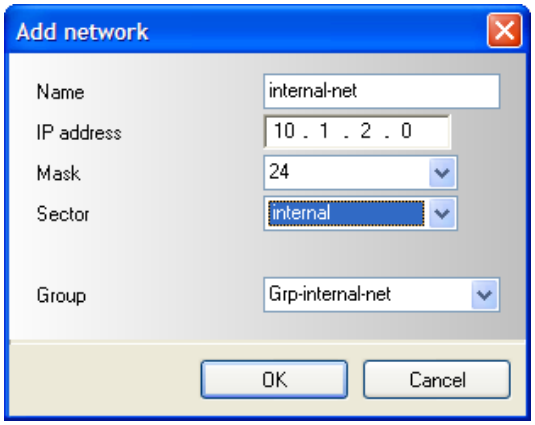

fig. 4 internal net

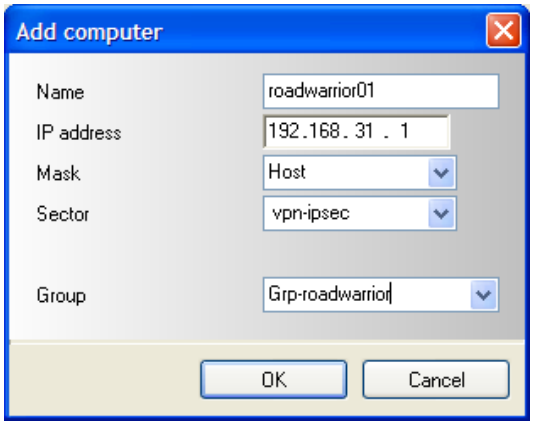

fig. 5 roadwarrior01

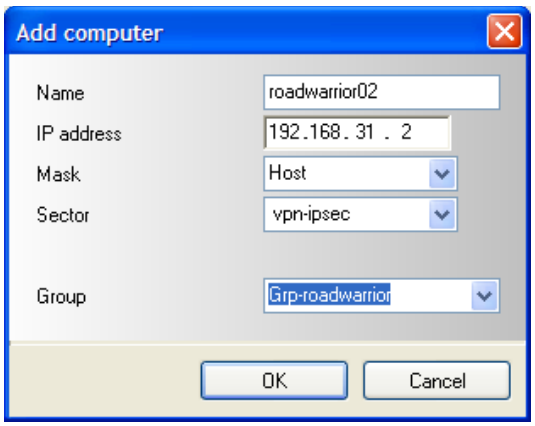

fig. 6 roadwarrior02

The result is shown in fig. 7.

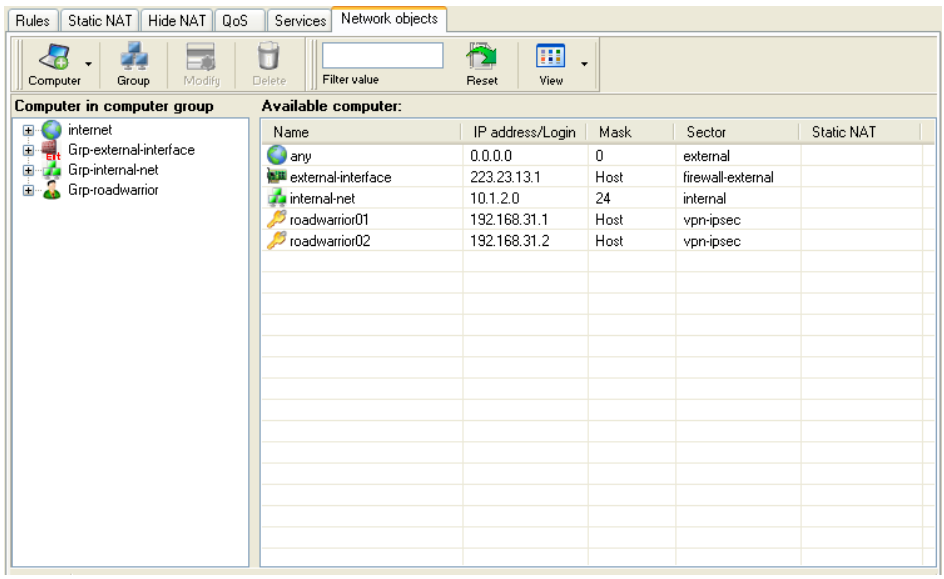

fig. 7 result of setting up network objects

1.2 Creating firewall rules

Proceed as follows:

- Over *Firewall* select the tab *Rules* and create the firewall-rules as shown in the images.

Only two rules are needed. The first rule enables the external computers to create an IPSec-connection to the external interface of the appliance.

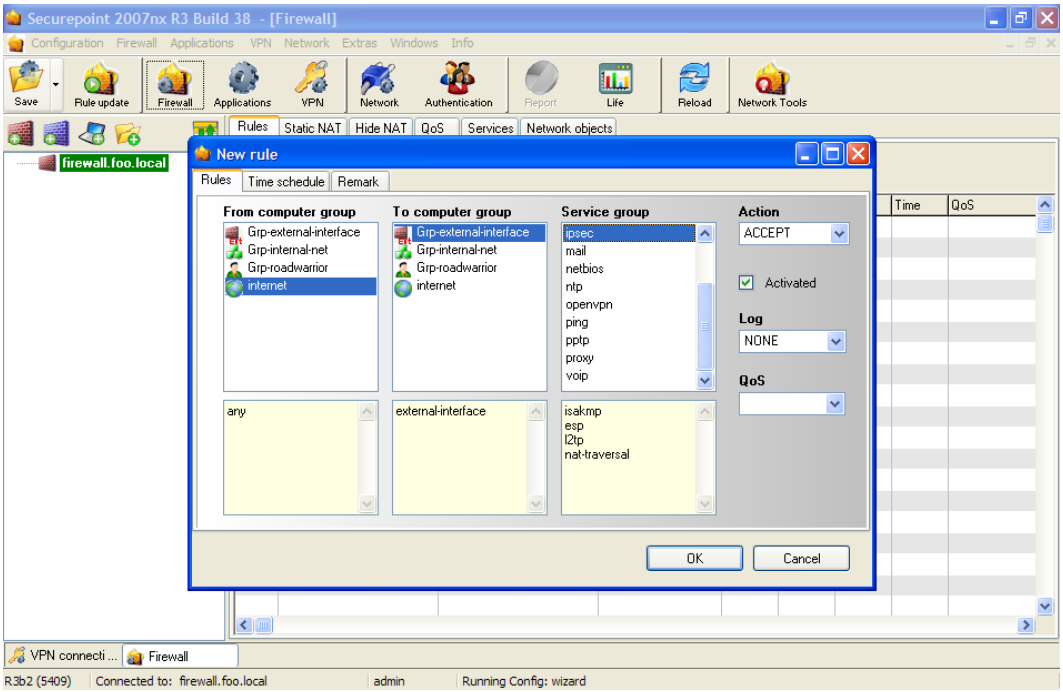

fig. 8 firewall rule internet

The second rule enables the roadwarrior to fully access the internal network.

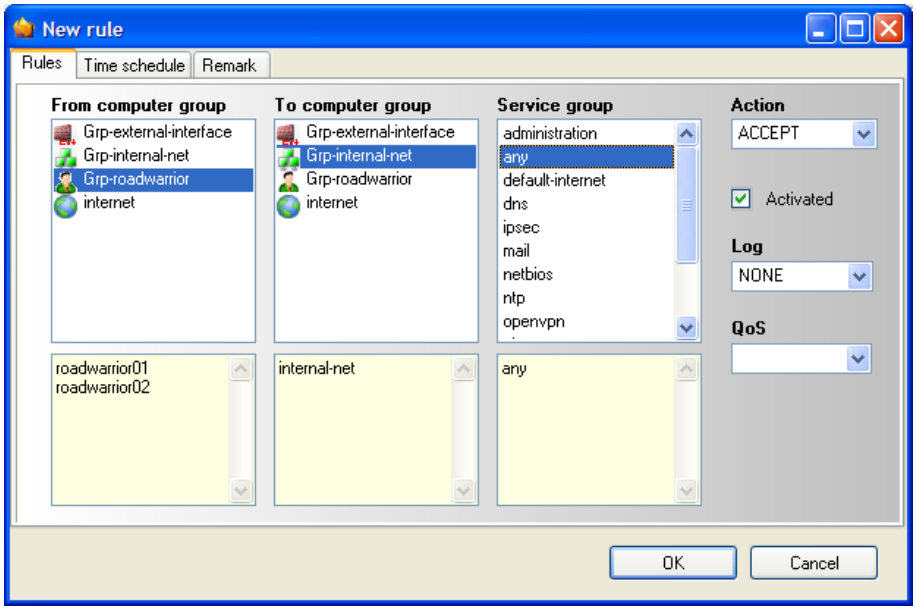

fig. 9 firewall rule roadwarrior

- In order to complete this step perform a rule update to activate the rules.

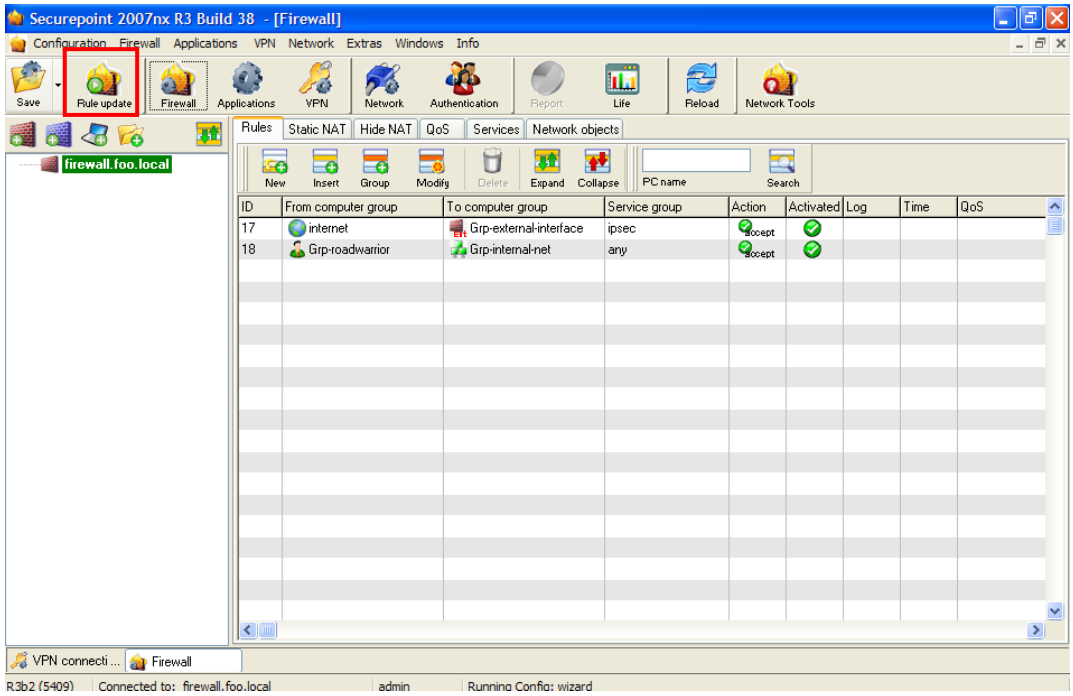

fig. 10 firewall rule update

1.3 Setting up certificates

Proceed as follows:

- Over *VPN* select the tab *Certificates*.

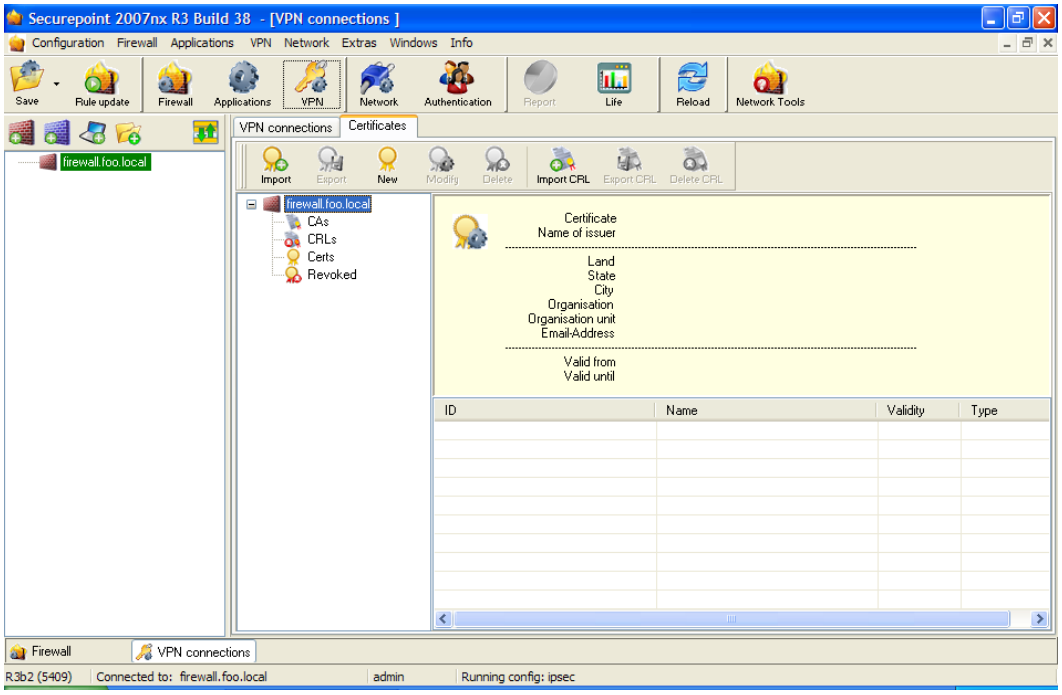

fig. 11 VPN tab certificates

First the certification authority (CA) has to be established with which the server certificate and the client certificates for the roadwarriors are signed. Therefore, the first step is to create a root certificate.

- Click on the icon *New* and select *Root certificate.*
- Insert the data in the way shown in the following image.

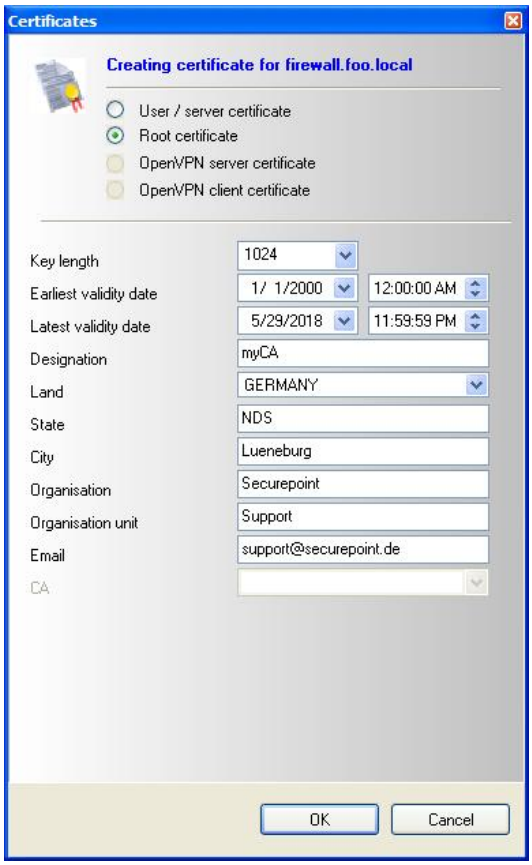

fig. 12 creating a root certificate

When you click on *OK* the dialog is shown again to setting up a client or server certificate.

After a CA has been created, server- and client-certificates may be generated. One server is needed as well as one client-certificate for each roadwarrior. These certificates only have to differ in their names.

- Select User / server certificate.
- Insert the data as shown in the following image. The most fields are already set with the data from the root certificate.

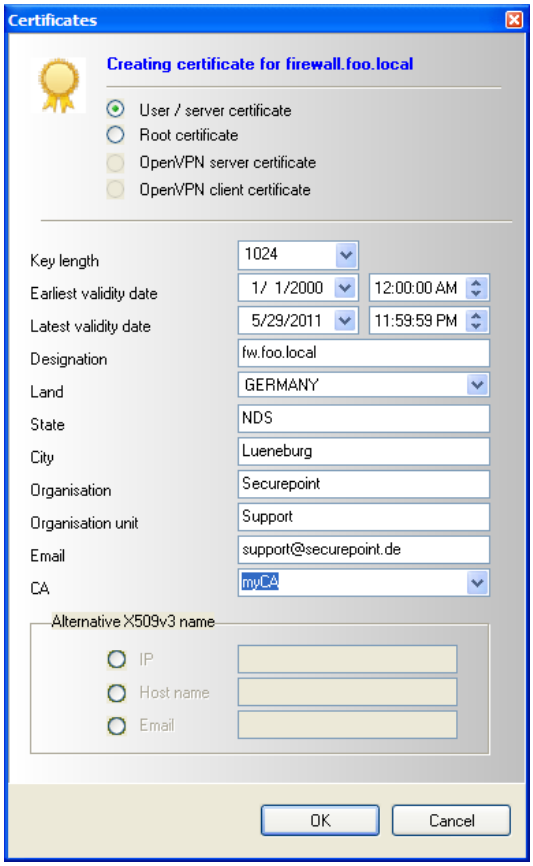

fig. 13 creating server certificate

Afterwards, client-certificates are needed.

- Select *User / server-certificate*.
- Insert the data as shown in the following image.

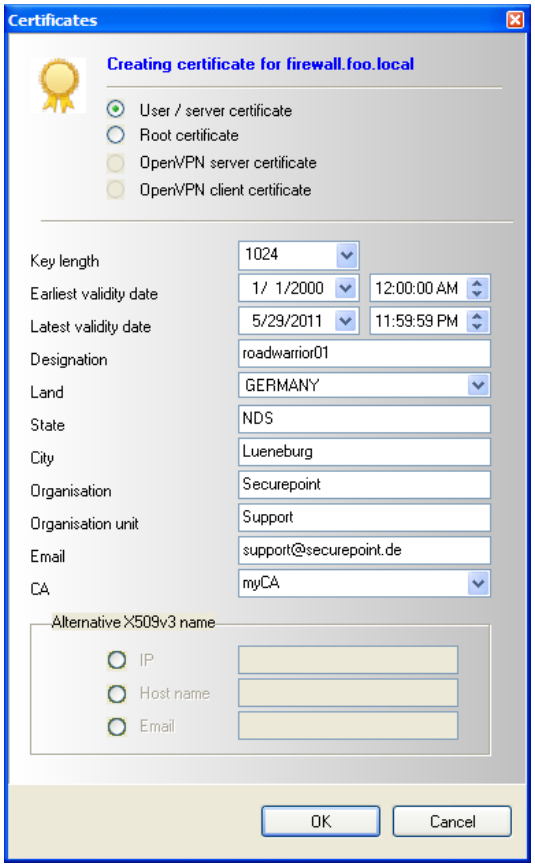

fig. 14 roadwarrior01 certificate

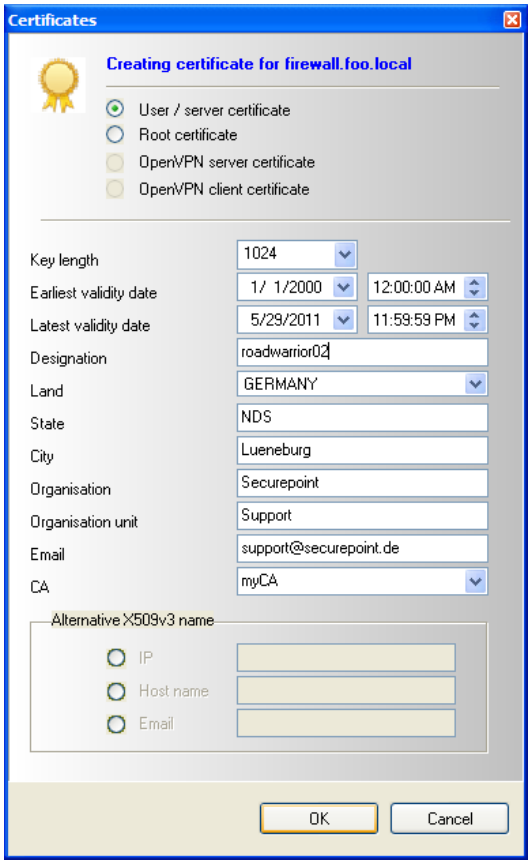

fig. 15 roadwarrior02 certificate

- Click Cancel on the new dialog to finish the certificate creation.

After creating the client-certificate, now export the certificates for usage on a roadwarrior.

➢ Click on the icon *Export* and select the data type that you want.

Depending on the destination system, you have to choose whether the certificates are to be saved in the standard format (.pem) or in the Personal Information Exchange Syntax (.p12). PKCS#12-files are given a password.

➢ In the following step the certificate can be stored locally.

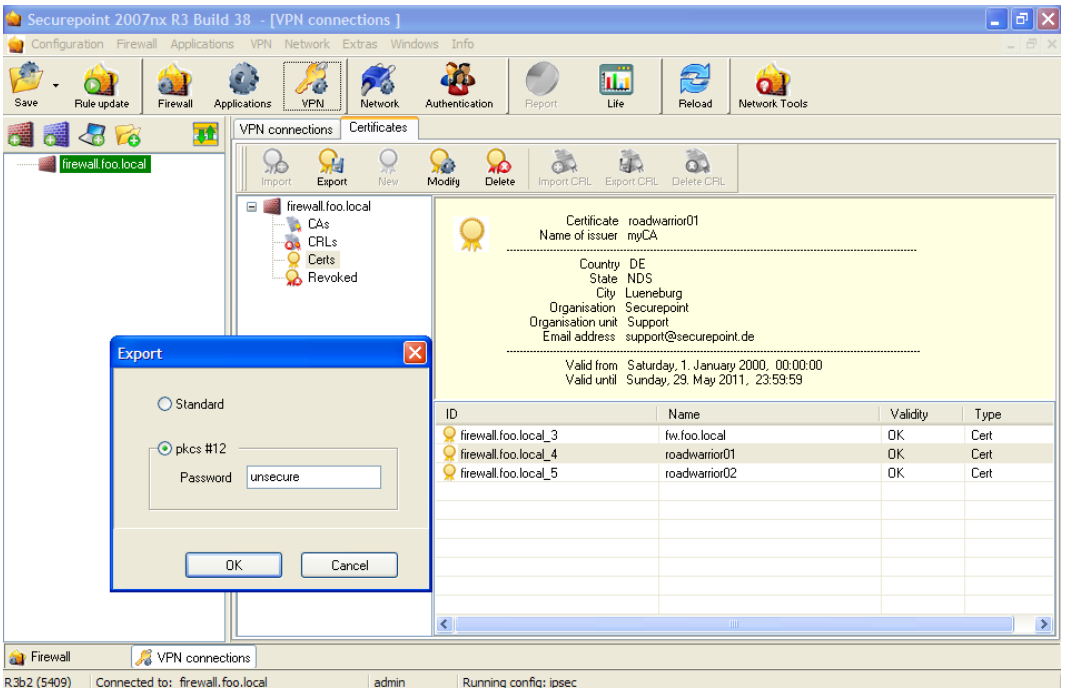

fig. 16 export certificate

1.4 IPSec configuration

This configuration can be conducted in two different methods. Either through a assistant guided configuration or a manual configuration based on a drawing layer.

1.4.1 Configuration with the assistant

Proceed as follows:

- Click the icon *VPN* and select the tab *VPN connections*.
- Click the icon *New*. The *IPSec Wizard* appears.
- Select *Roadwarrior* and click *Next*.

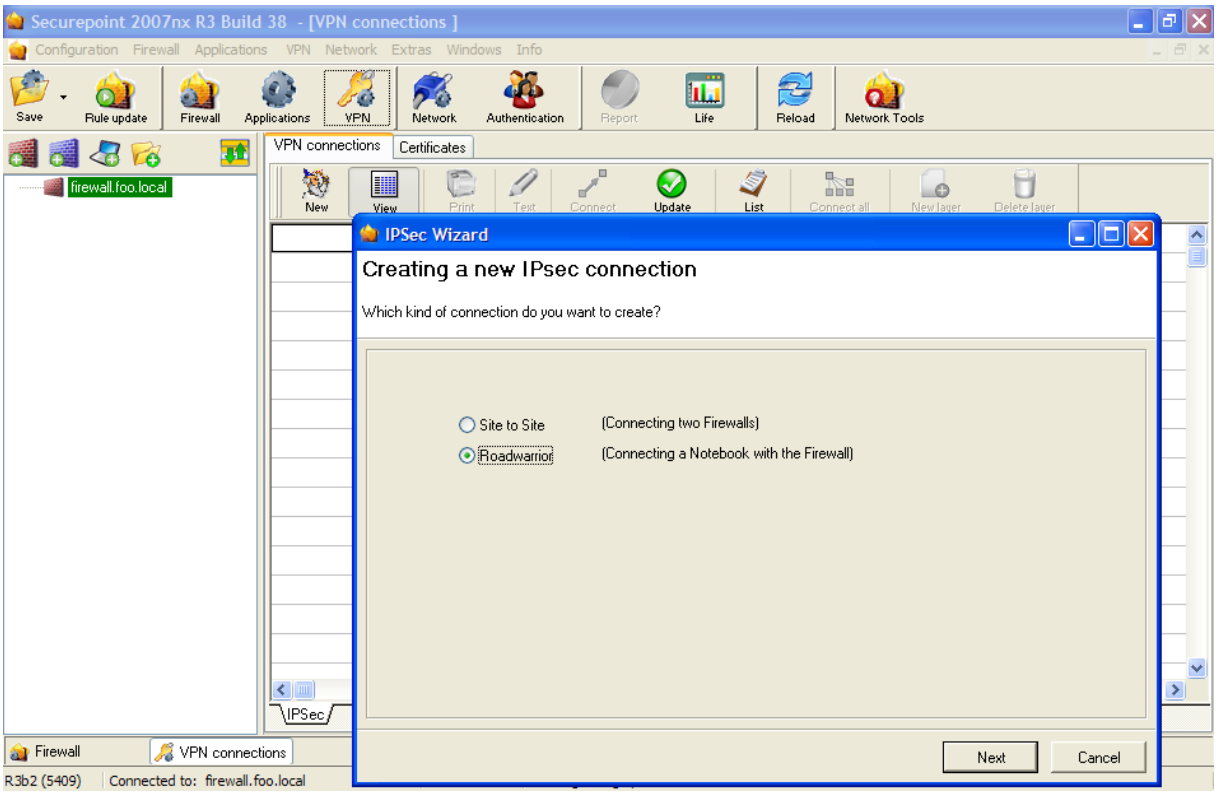

fig. 17 IPSec Wizard - step 1

- Select *Native IPSec* and click *Next*.

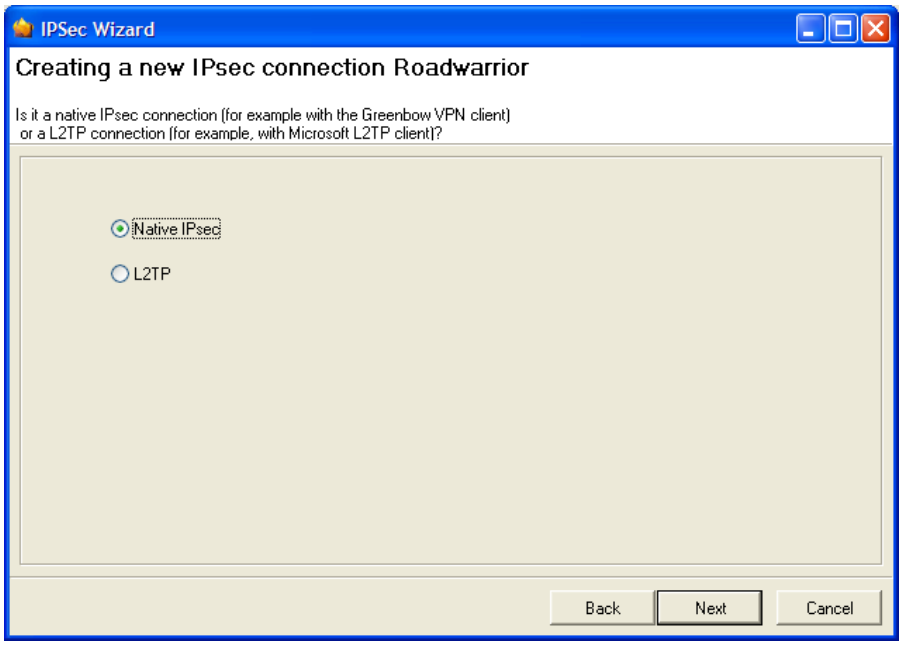

fig. 18 IPSec Wizad - step2

- Enter a name for the connection.
- Select *Certificate* as authentication method and select the *roadwarrior01* certificate out of the dropdown list.

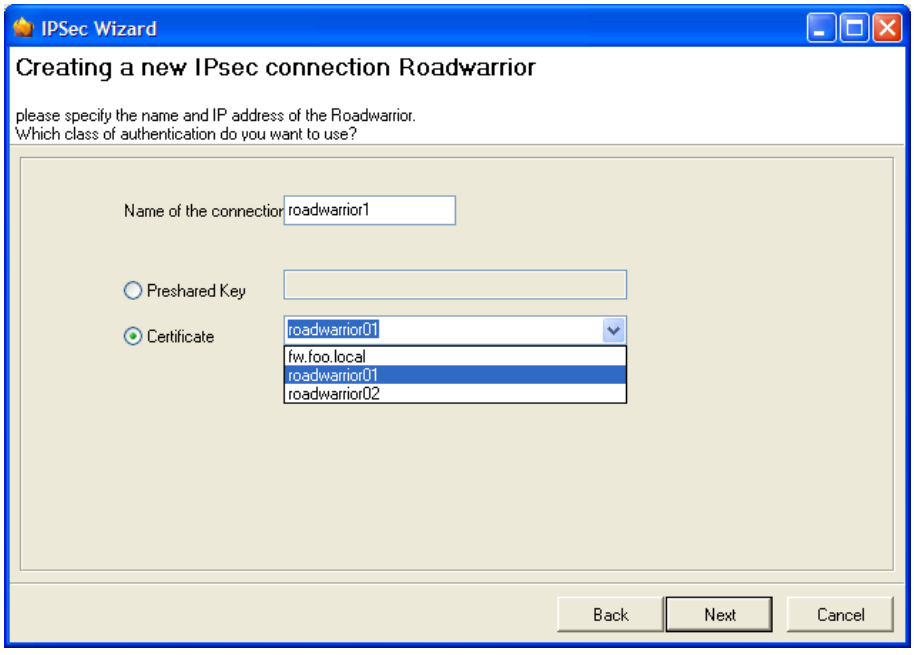

fig. 19 IPSec Wizard - step 3

- Enter the local net that the roadwarrior is entitled to access.
- Allocate a permanent tunnel IP-address.
- Complete the configuration by clicking the *Finish* button.

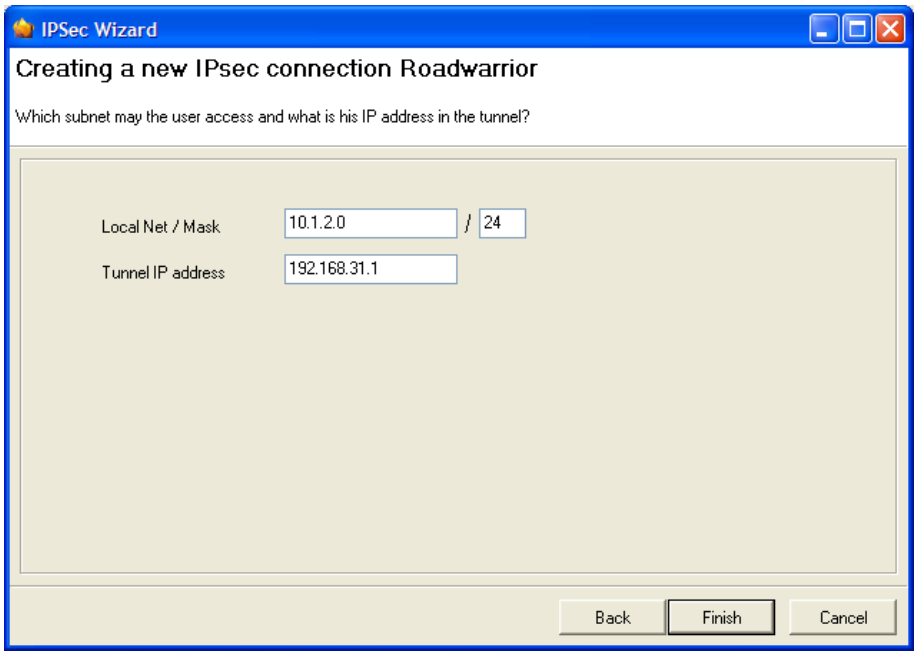

fig. 20 IPSec Wizard - step 4

- The result of the configuration is shown in fig. 21.
- Repeat the procedure for the second roadwarrior.
- At last you have to update the connections. Click onto the icon *Update*.

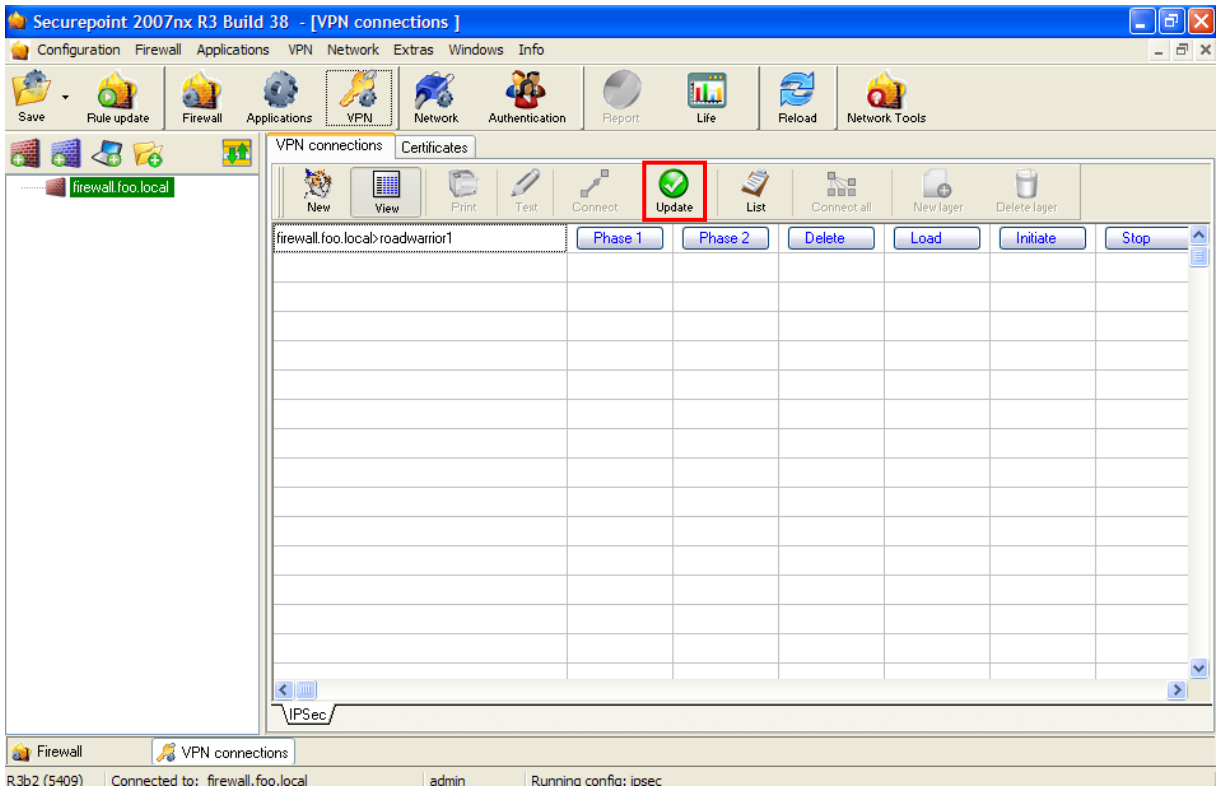

fig. 21 result of the configuration - updating the connection

1.4.2 Configuration using the layer view

Proceed as follows:

- Over*VPN* select the tab *VPN connections.*
- Change to the VPN layer view by clicking onto the icon *View*.
- By using the mouse move the existing firewall-object from the left window onto the VPN viewport.

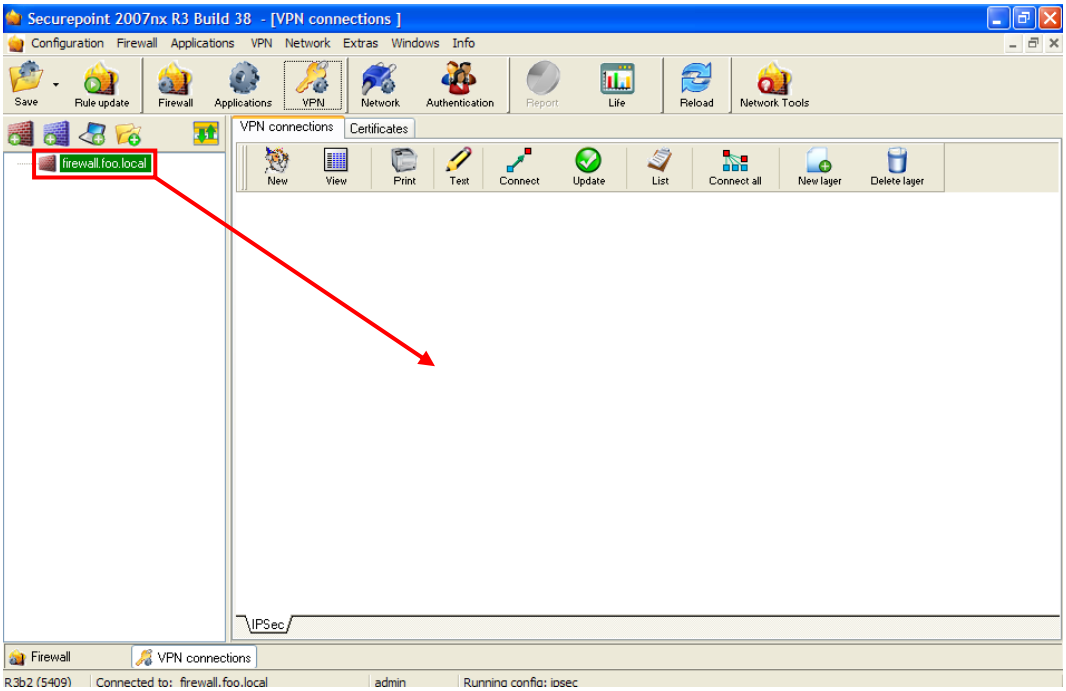

fig. 22 Draging the firewall symbol onto the VPN layer

- Now create a new roadwarrior object in the left window.
- Click on the notebook icon in the toolbar of the left window.
- In the dialog *Roadwarrior – add* the roadwarrior is set up with IP (0.0.0.0), because it may vary all the time!

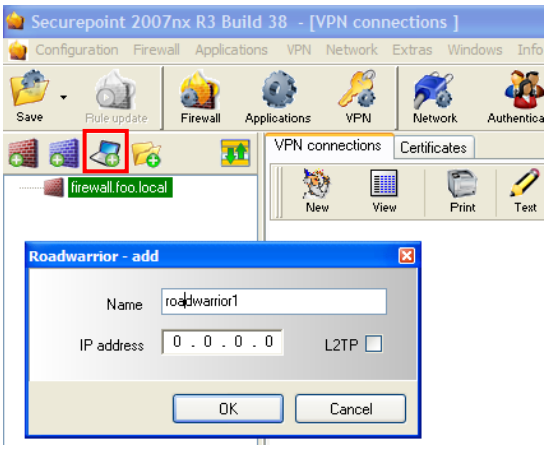

fig. 23 creating object roadwarrior1

➢ Now move the freshly created roadwarrior object from the left window onto the VPN viewport.

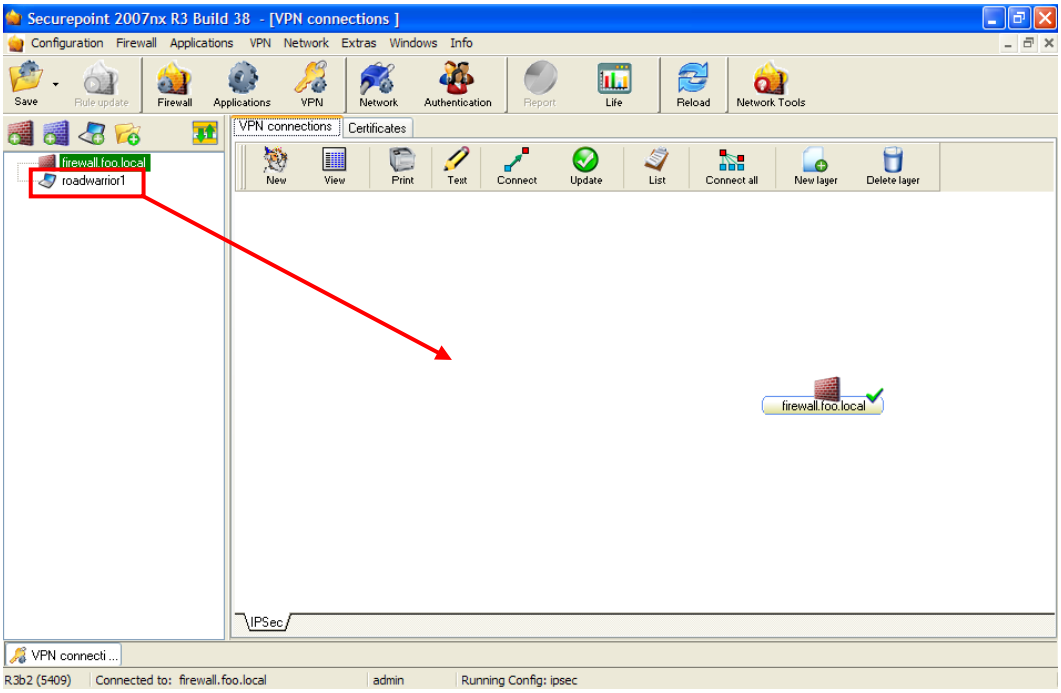

fig. 24 Draging roadwarrior object onto the VPN layer

➢ Now click on the icon *Connect* and on the roadwarrior object.

A flag appears on the roadwarrior object with the information *Please click on destination object*.

➢ Click on the firewall object.

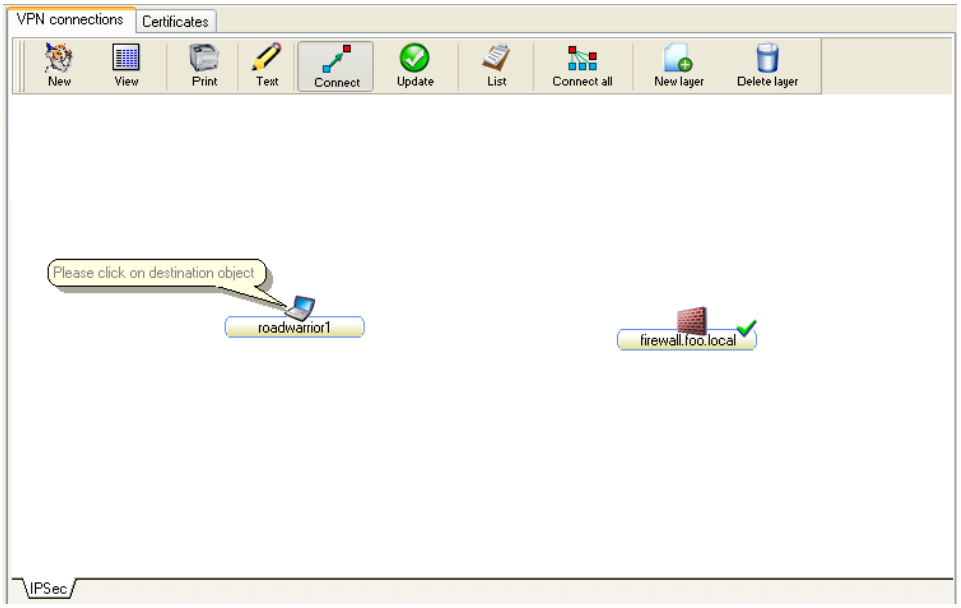

fig. 25 connecting objects

Now a new dialog opens automatically: *IPSec connection - accept*

You may now choose between two ways to proceed:

Procedure A
If a roadwarrior is to be identified exactly, it is recommended to enter the certificate reference. The configured connection will then be assigned to exactly one roadwarrior.

Procedure B
This describes how to set up a configuration for several roadwarriors with a valid certificate.

Procedure A

- In the dialog *IPSec connection - accept, General* select the authentication method CERT and the ID-type SUBJECT. In a default case further settings can simply be adopted.
- In the tab *firewall.foo.local* select the server certificate and confirm your entries with *OK*.

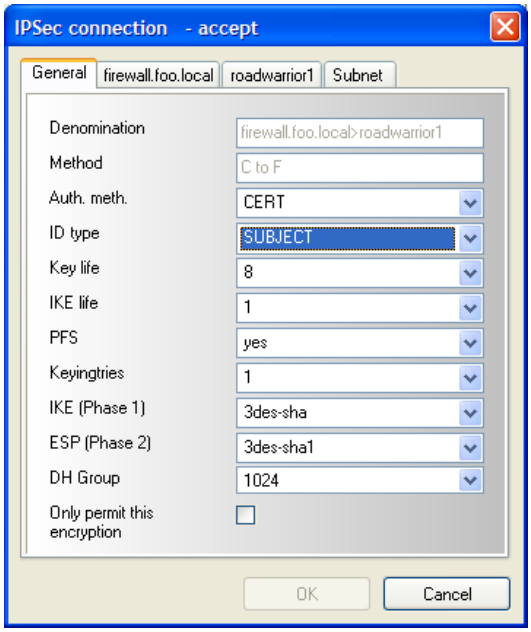

fig. 26 IPSec connection - tab General

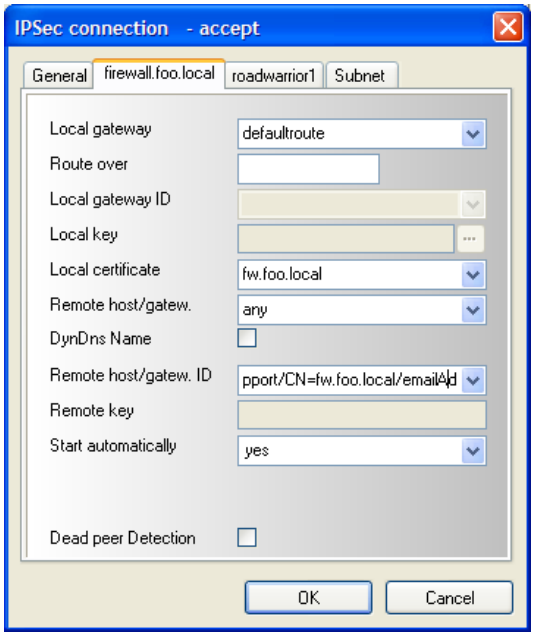

fig. 27 IPSec connection - tab firewall.foo.local

After clicking *OK* the tab *Subnet* is displayed. You have to configure the subnet which regulates the routing between the roadwarrior and the internal net. The subnet for a roadwarrior consists of one single IP (bitcount 32).

- Click on the icon *New*. The dialog *IPSec subnet* appears.
- Enter the subnets and click *OK*.

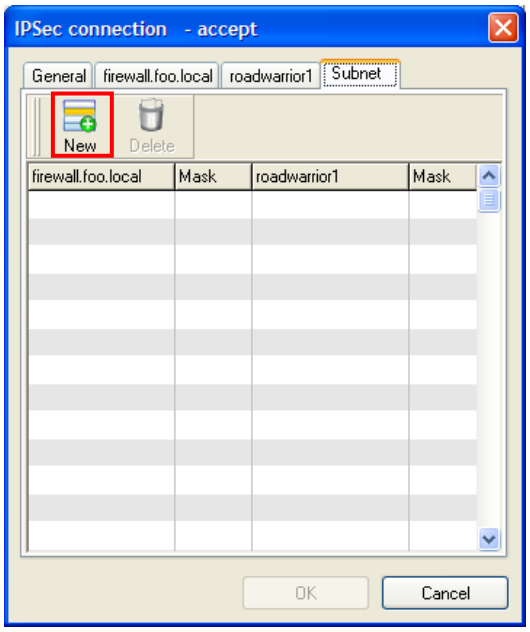

fig. 28 IPSec connection - tab Subnet

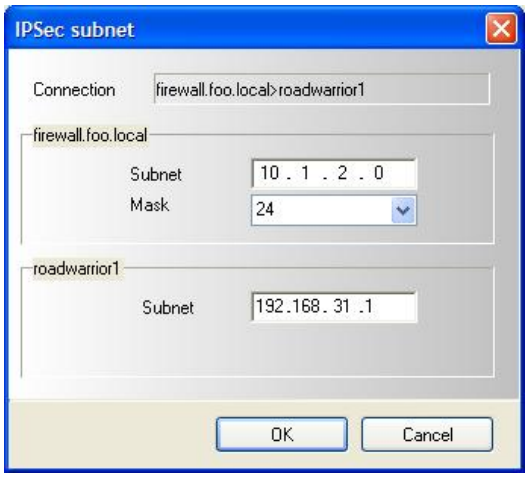

fig. 29 enter subnets

- After the configuration you have to update the connections by click on the icon *Update* (fig. 34).
- In the following step check the status of the services under *Applications* in the tab *Status of services*. For the VPN connection the SERVICE_IPSEC is required (see fig. 35).
- Now copy the certificates that have been created in the section certificates (see 1.3) onto the destination systems.

Procedure B

If “CERT” is chosen as the ID-type, all roadwarriors with a valid certificate can use this connection (if the subnet-configuration is compatible).

- Select the ID type *CERT* on the tab *General*.
- On the tab *firewall.foo.local* select the server certificate.

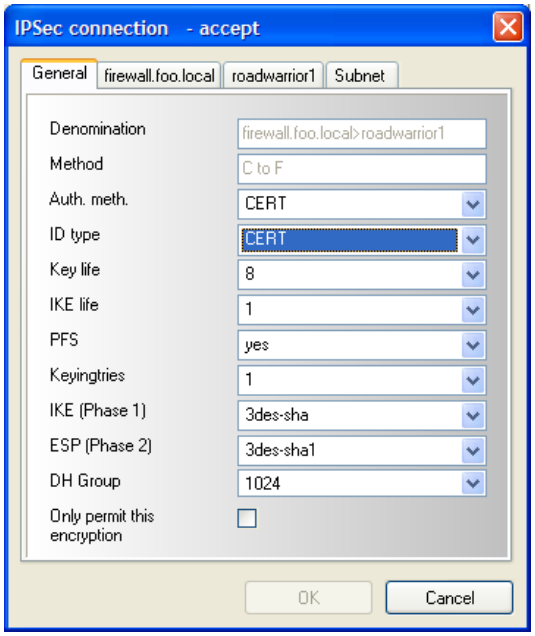

fig. 30 IPSec connection - ID type CERT

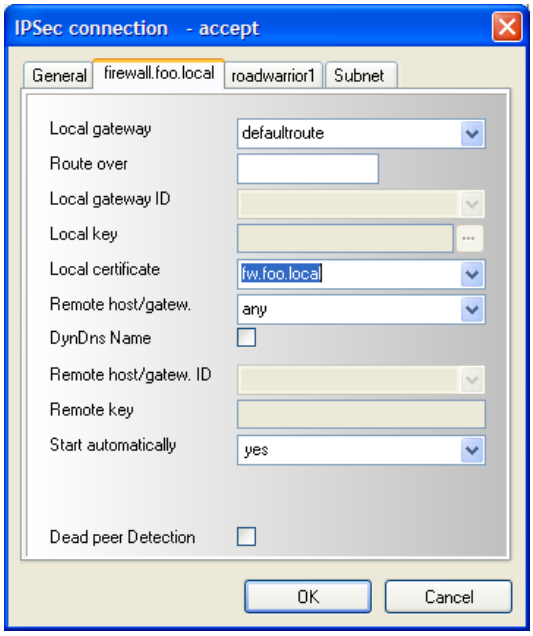

fig. 31 IPSec connection – enter local certificate

The advantage of this configuration is that all roadwarrior-IPs can be configured in one single window.

After clicking *OK* the tab *Subnet* is displayed. You have to configure the subnet which regulates the routing between the roadwarrior and the internal net. The subnet for a roadwarrior consists of one single IP (bitcount 32).

- Click on the icon *New*. The dialog *IPSec subnet* appears.
- Enter the subnets and click *OK*.

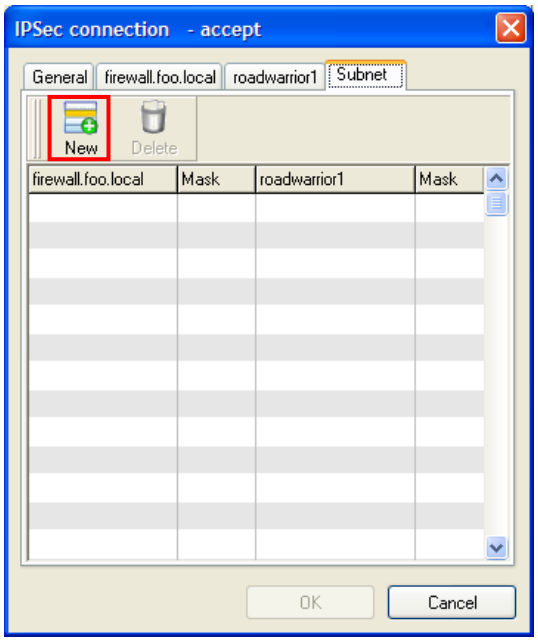

fig. 32 tab Subnet - click icon New

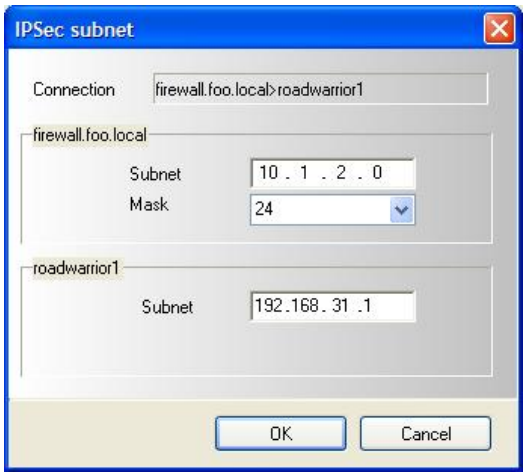

fig. 33 enter subnets

- After the configuration you have to update the connections by click on the icon *Update*.

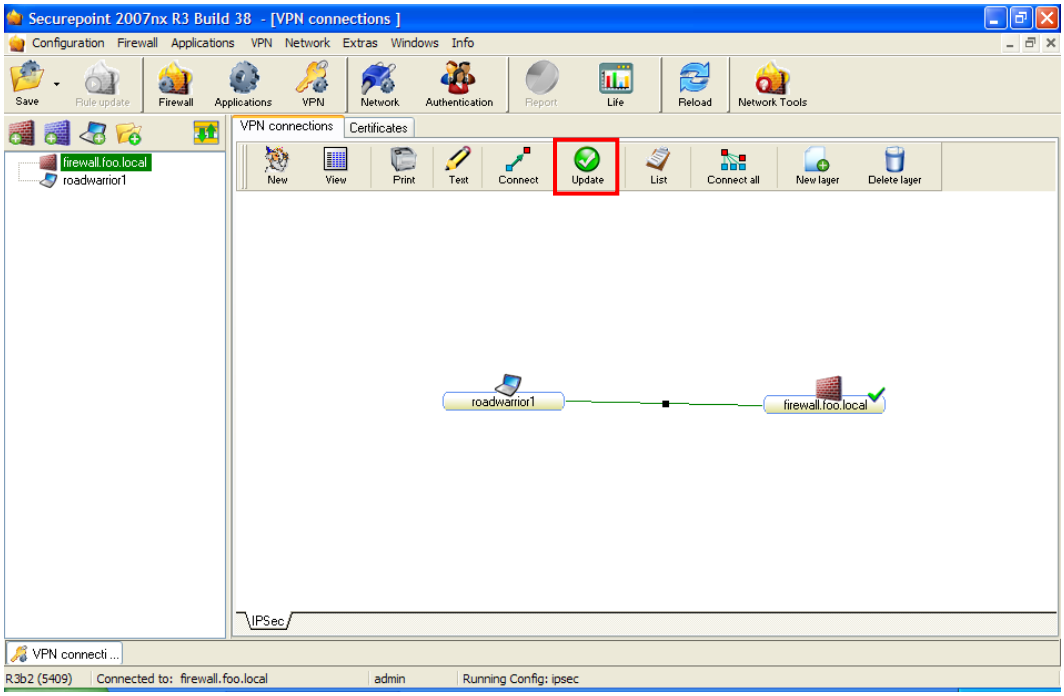

fig. 34 update the connections

- In the following step check the status of the services under *Applications* in the tab *Status of services*. For the VPN connection the SERVICE_IPSEC is required.

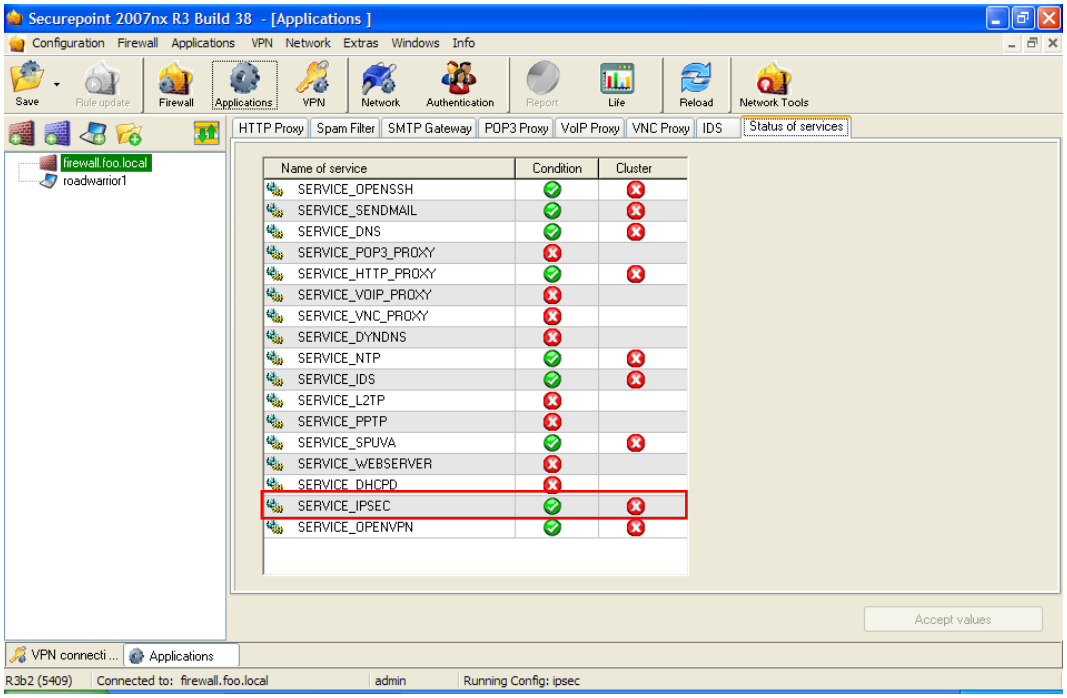

fig. 35 checking status of SERVICE_IPSEC

- Now copy the certificates that have been created in the section certificates (see 1.3) onto the destination systems.

2 Configuration of the VPN client 'The GreenBow' under Windows

Proceed as follows:

- Install the GreenBow VPN client on an assigned computer and start the client.

- With GreenBow a new phase 1 is set up by clicking on *Configuration* with the right mouse-button.
- In *Phase 1* the IP of the Securepoint Security Appliance as well as the wanted encoding have to be entered first.

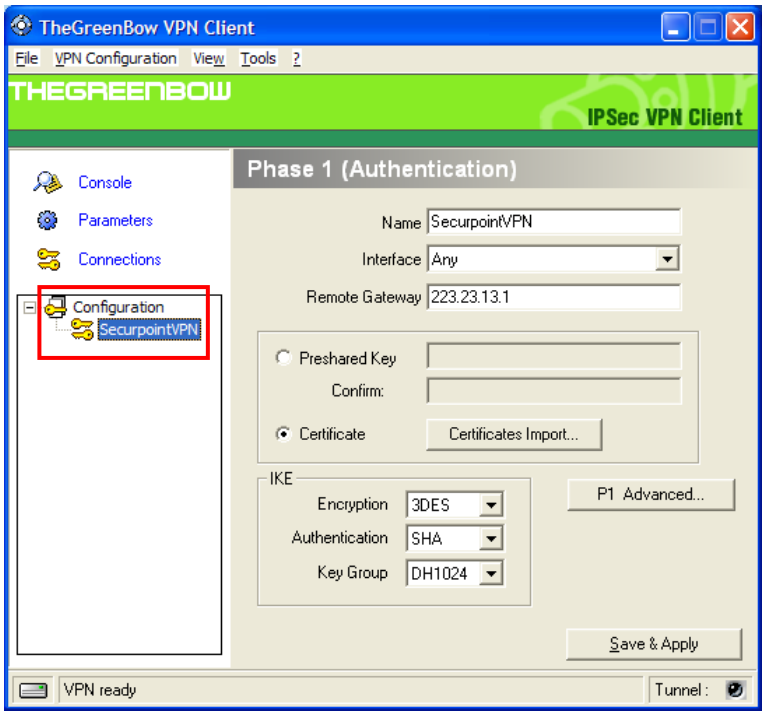

fig. 36 create new phase 1

Then the certificate is imported.

- Click on the button *Certificates import*.

The dialog *Certificate import* opens.

- The p12 file can be imported via *Import*.

After the import you see a string.

- The string under *User Certificate* has to be marked and copied. This string is needed under *P1 Advanced*.
- Save your entries with *OK*.

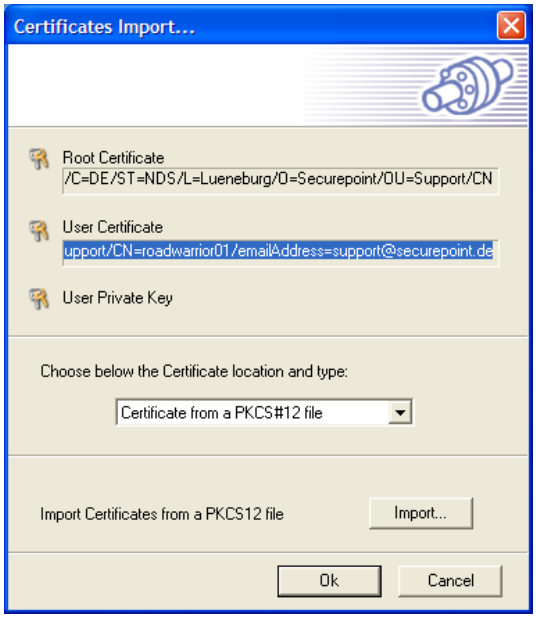

fig. 37 Import dialog - copy the string under User Certificate

- Click on the button *P1 Advanced*.

The dialog *Phase 1 Advanced* opens.

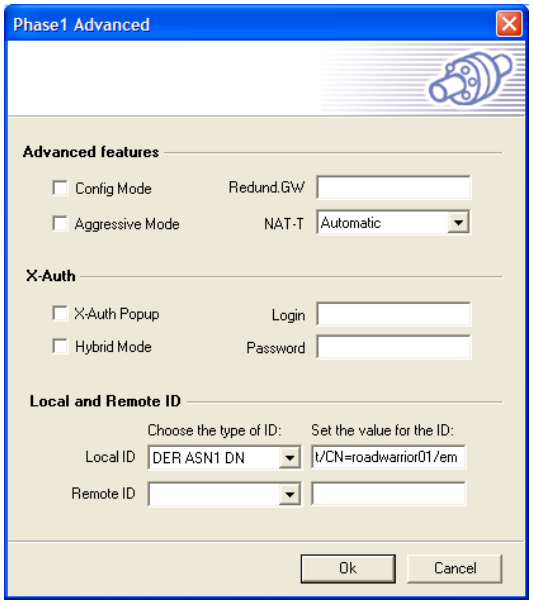

fig. 38 Phase 1 - entering copied string

- Here, the type: “DER ANS1 DN” is to be selected as the local ID. The copied string is inserted as the *ID*. Afterwards, a new Phase 2 can be set up.
- Save your entries with *OK*.

In Phase 2 the network configuration is conducted. The local address is the IP which the roadwarrior receives in the VPN tunnel. The address with which the roadwarrior want to connect is the subnet as has already been entered during firewall configuration.

- With the right mouse-button click on the created Phase 1 in the left window.
- Create a Phase 2.
- Insert the information according to the following image.

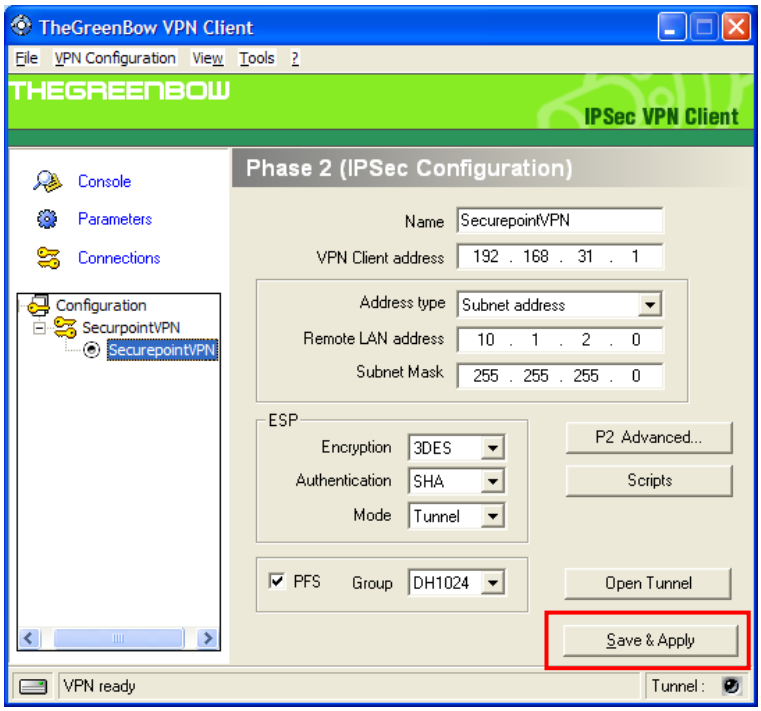

fig. 39 setting up phase 2

- The tunnel can be opened after a concluding click on *Save & Apply*.