



Konfiguration Greenbow VPN Client mit X.509 Zertifikaten

Securepoint Firewall & VPN Server 4.0

Stand: 05. April 2004

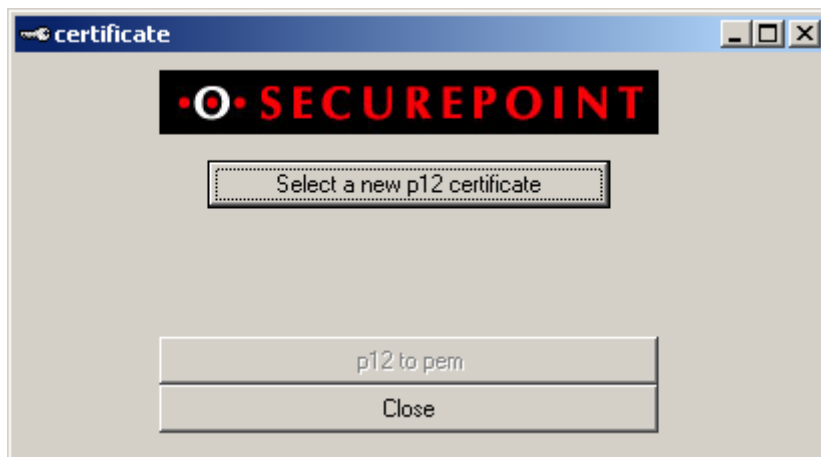


The Greenbow VPN Client doesn't understand the PKCS format. So, you have to convert the X.509 client certificate of the Securepoint Firewall to PEM format.

You can do this by using the tool "certificate". This program splits the root CA, the certificate of the client, the private key and the subject line of the certificate in four different files.

For example the certificate pkcs12_HansMustermann.p12.

- Start the program "certificate.exe".



Pic. Start the program

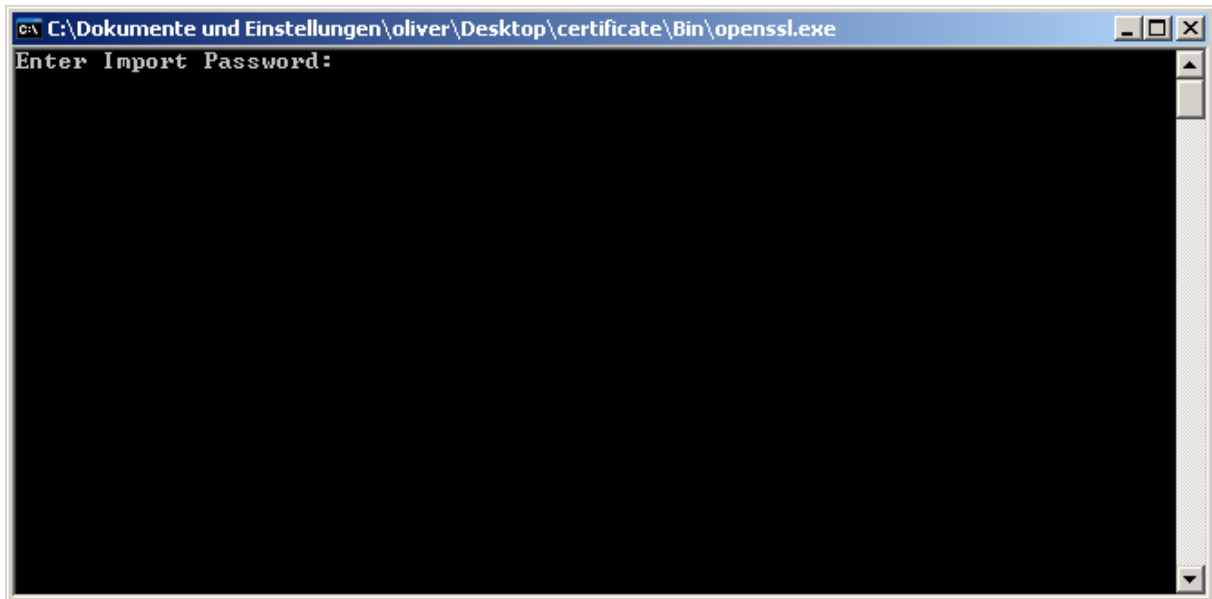
- Select the certificate pkcs12_HansMustermann.p12.



Pic. Select the certificate

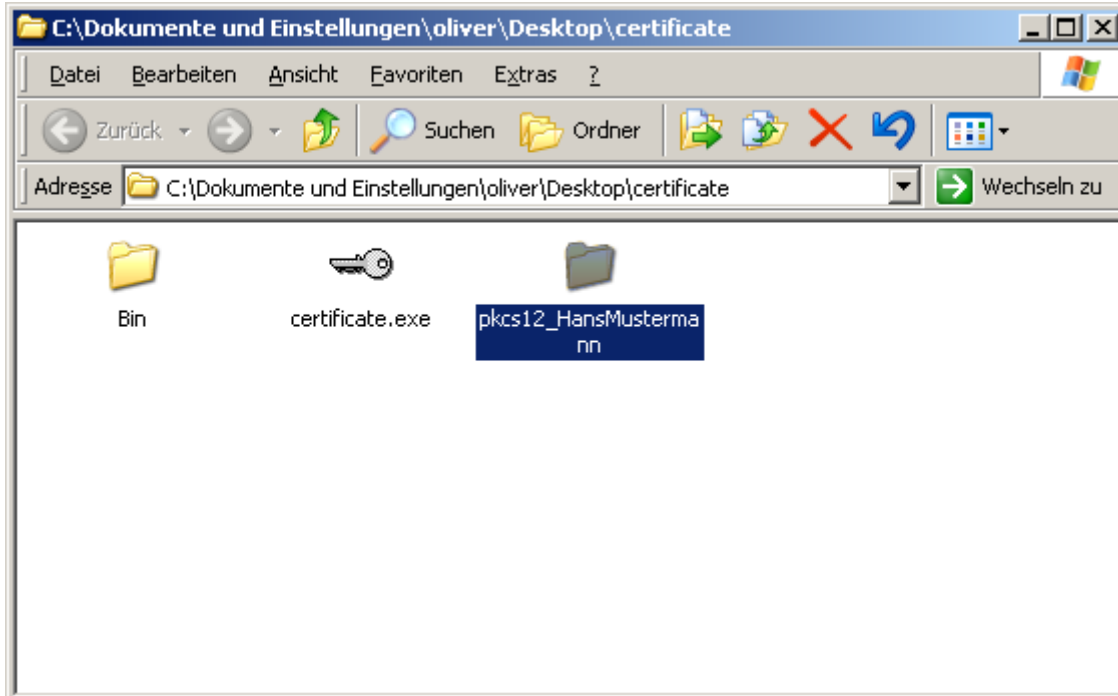
- Choose the button p12 to pem.

- And enter the password of the certificate.



Pic. Enter the password

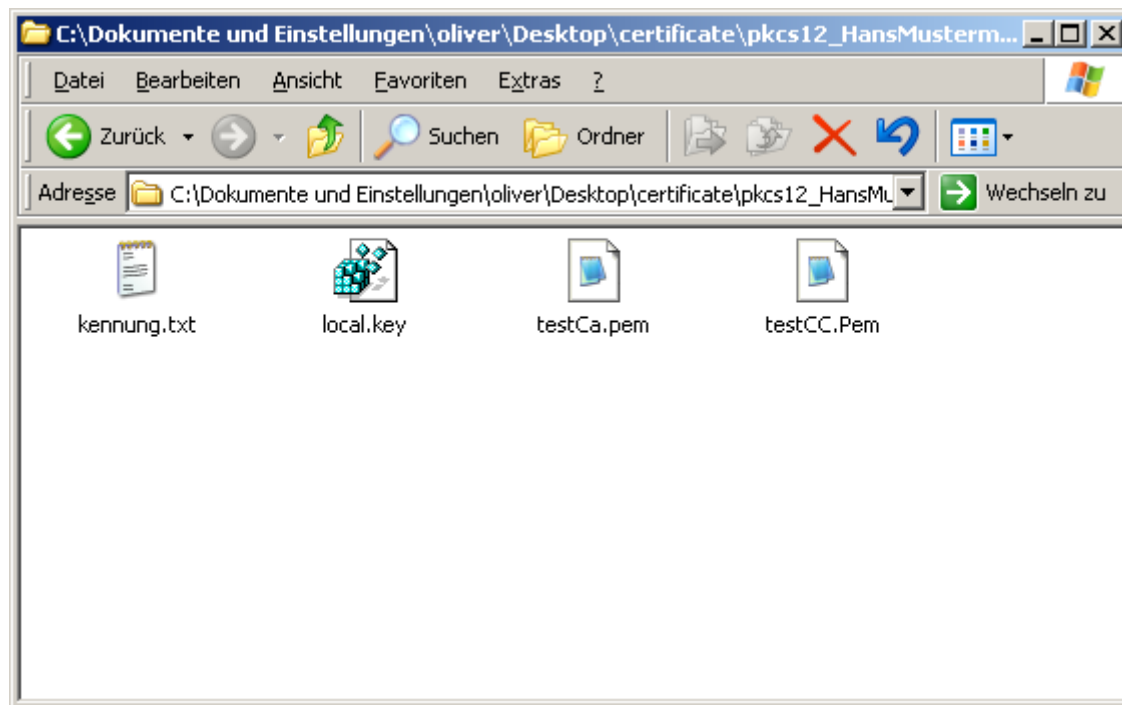
After converting, you have a new folder called pkcs12_HansMustermann.



Pic. New folder

In the folder you will find:

- testCA.pem -> the root CA
- testCC.pem -> the client certificate
- local.key -> the private key
 - kennung.txt -> the subject of the client certificate

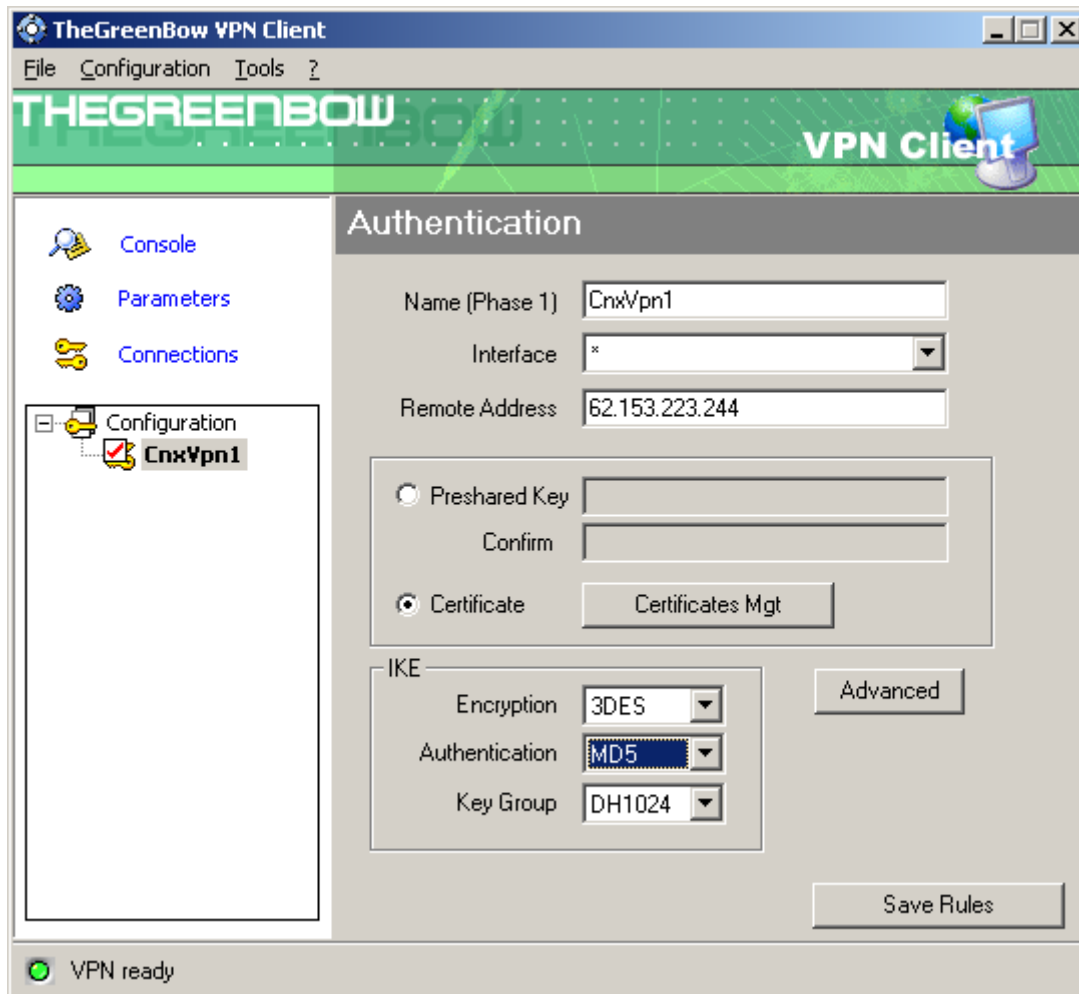


Pic. Content in folder

Authentication

Now open the configuration program of the Greenbow VPN Client.

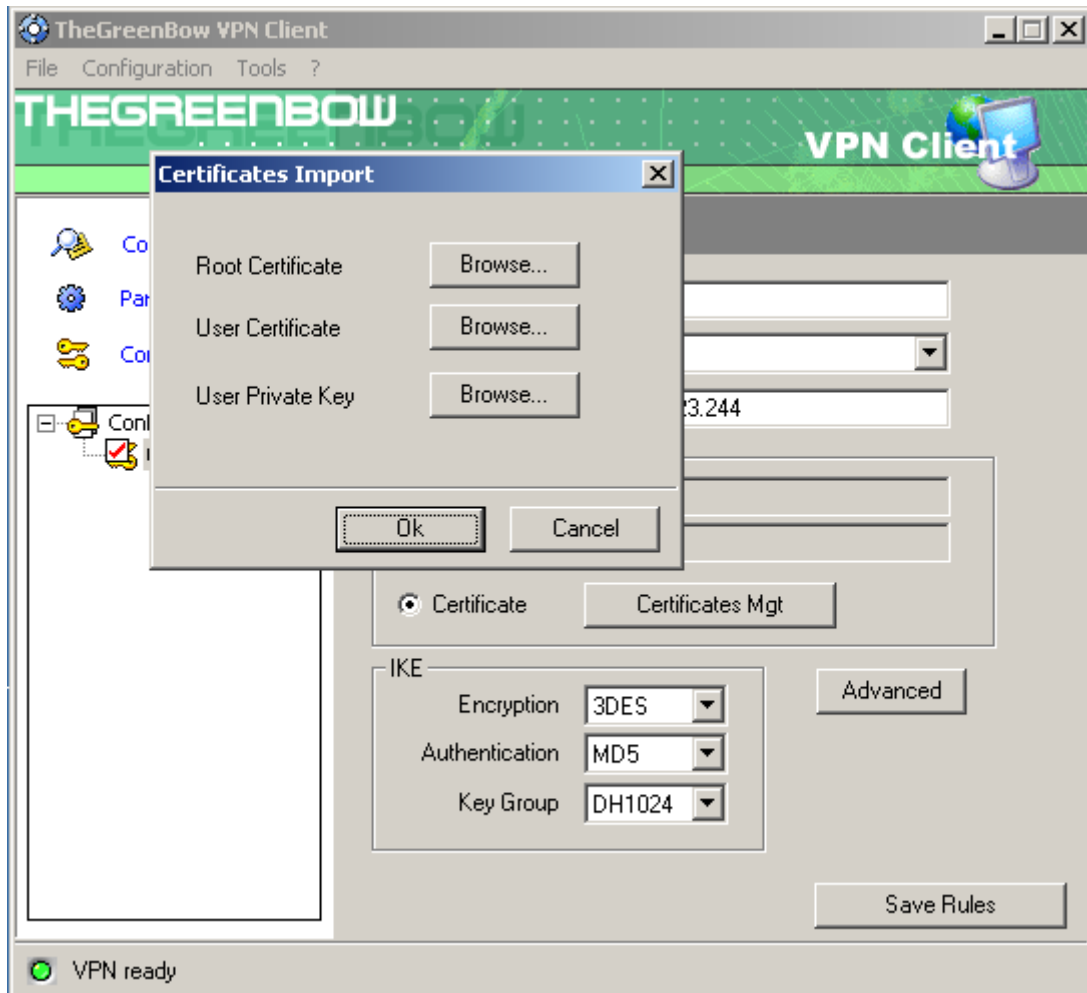
- With right mouse-click choose a new phase 1.
- For remote address select the external ip address of your Securepoint Firewall.
- For authentication choose certificate and click on the "Certificates Mgt".



Pic. Authentication

Certificates Import

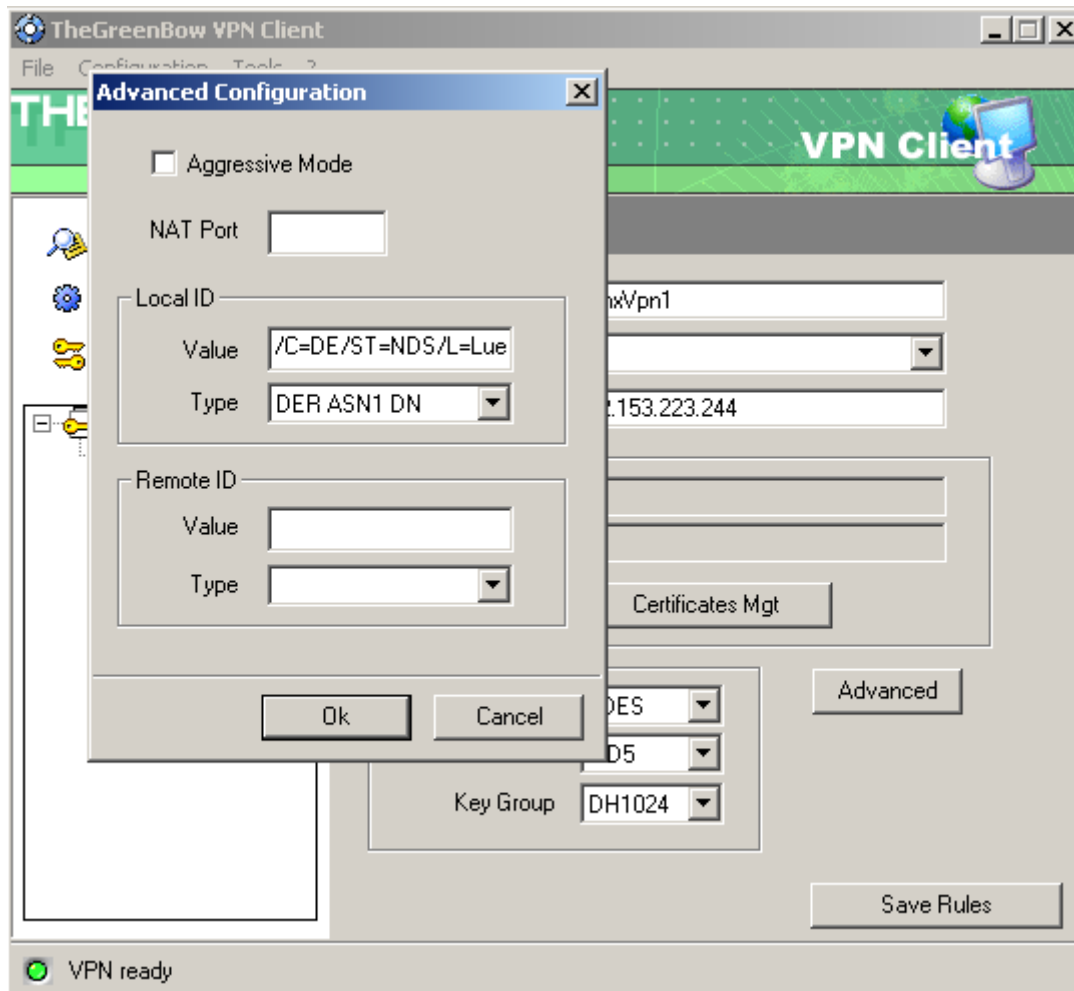
- For root certificate select the file testCA.pem.
- For the user certificate select testCC.pem file and for the private key select local.key file.



Pic. Certificates Import

Advanced Configuration

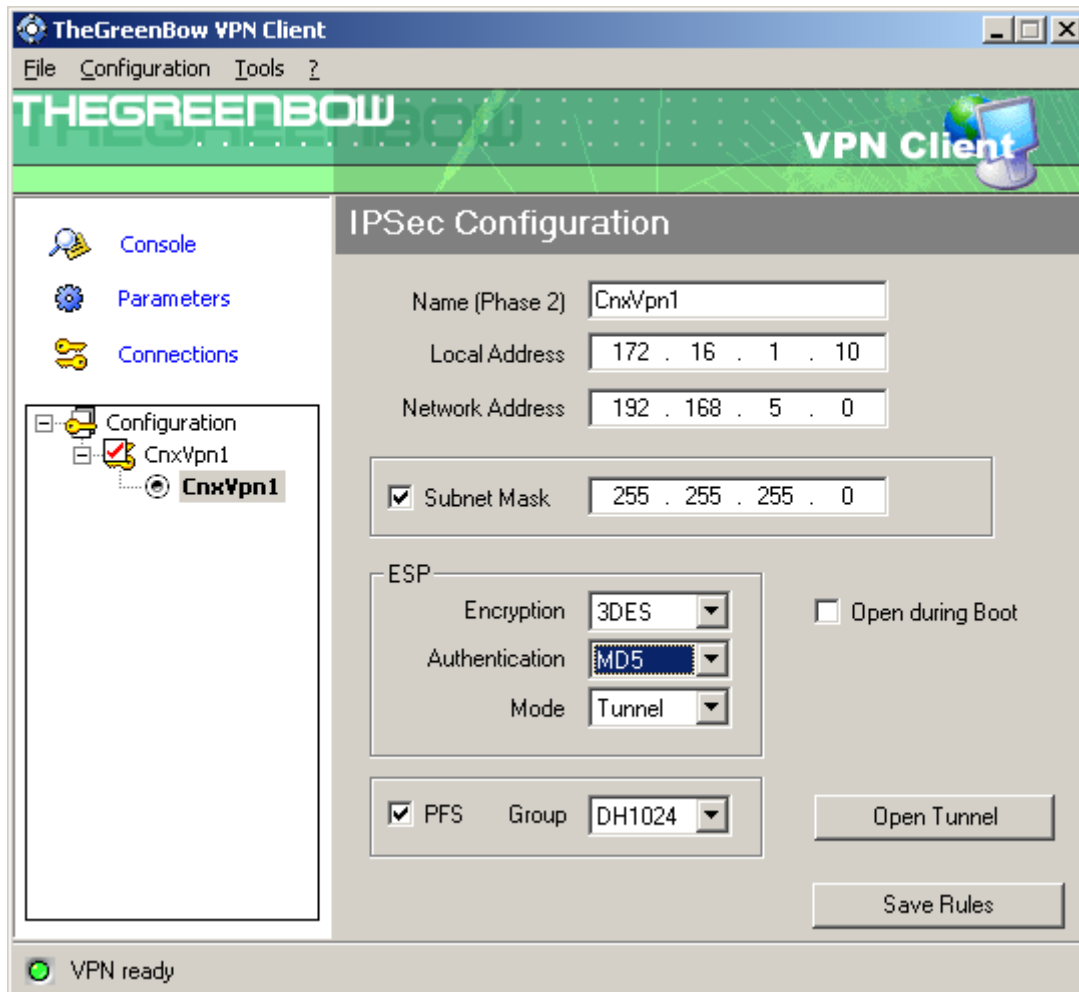
- Now, select the button „advanced“ and for the local id choose the type “DER ASN1 DN”.
- In the field above paste the subject line that is saved in the file kennung.txt.



Pic. Advanced Configuration

IPSec Configuration

- With a right mouse click on the name of your configuration, select "add phase 2".
- The local address is the ip address you use in the tunnel. With this ip address you will reach the internal lan behind the firewall. The network address is the lan behind the firewall. Choose the right settings for esp and open the tunnel for testing.
- Don't forget to save your settings (save rules).



Pic. IPsec Configuration