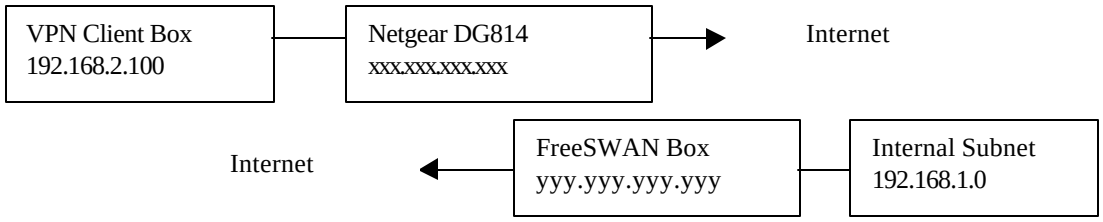
FreeSWAN with Netgear ProSafe VPN Client

Mini Howto - setup & Configure Netgear ProSafe VPN Client V10.1 (on Win2K Pro) & FreeSWAN V1.98b with Certificates.

By Ratware (April 2004)

Netgear ProSafe VPN Client is a cheap IPSec client for Windows. At the time of writing, a single user license can be purchased in the UK for about £25-£30, 5 user packs are also available.

Network Diagram



Netgear DG814 Router Setup

I am using a Netgear DG814 router with VPN (IPSec) passthru. This router just needs to be setup as per the manual, nothing special is needed to enable VPN passthru only port forward UDP 500 to the VPN client on later firmware releases. Note the VPN Client PC must have a static IP (not DHCP). This should be able to be applied to any router with IPSec passthru.

You may wish to enable the Ping on the WAN address whilst you are setting up the link.

FreeSWAN Setup (V1.98b – should be similar for other versions)

Basic FreeSWAN Setup

Install FreeSWAN + x509 patches – see normal FreeSWAN docs, on Linux with a 2.4 kernel and iptables

Creating the Certificates

- Ensure the openssl command can be found in your current path – i.e. type openssl from anywhere and it should run the command –duh!
- Enter the directory /etc/ipsec.d
- Create the ClientVPN Certificate
    - /usr/share/ssl/misc/CA.sh –newcert
    - This will create the certificate by asking for several parameters, fill in the important ones:-
        - Password: be inventive… but note it down!
        - (C) Country: UK
        - (S or ST) State: Your State
        - (O) Organisation Name : Company
        - (OU) Organisation Unit: ClientVPN-Cert
        - (L) Locality: Home
        - (CN) Common Name: ClientVPN
        - (E) Email: you@isp.co.uk

    - The above are just examples.
    - This will produce a public & private key in the file newreq.pem
    - mv newreq.pem clientvpn.pem
    - openssl pkcs12 –export –in clientvpn.pem –out clientvpn.p12
    - This will create a pkcs file which can be imported into the VPN Client
    - cp clientvpn.pem clientvpn-pub.pem
    - Edit clientvpn-pub.pem and remove the private key
    - Move clientvpn.p12 to a floppy
    - Copy clientvpn-pub.pem to the floppy
    - Delete clientvpn.pem (only keep the public key on the server).
- Create the Server Certificate
    - /usr/share/ssl/misc/CA.sh –newcert
    - This will create the certificate by asking for several parameters, fill in the important ones:-
        - Password: be inventive… but note it down!
        - (C) Country: UK
        - (S or ST) State: Your State
        - (O) Organisation Name : Company
        - (OU) Organisation Unit: FreeSWAN-Cert
        - (L) Locality: Office
        - (CN) Common Name: FreeSWAN
        - (E) Email: you@isp.co.uk
    - The above are just examples
    - This will produce a public & private key in the file newreq.pem
    - mv newreq.pem freeswan.pem
    - cp freeswan.pem freeswan-pub.pem
    - Edit freeswan-pub.pem and remove the private key
    - Copy freeswan-pub.pem to the same floppy
    - Copy freeswan.pem to /etc/ipsec.d/private
- Create the RSA key in the ipsec.secrets file
    - Enter the line:-
        - : RSA : freeswan.pem "The Password you entered for the certificate"

Create connection structure in ipsec.conf

```
# Connect ClientVPN via Netgear ProSafe VPN
conn ClientVPN
        compress=yes
        auto=add
        type=tunnel
        authby=rsasig
        keyexchange=ike
        keyingtries=3
        pfs=yes
        left=xxx.xxx.xxx.xxx
        leftsubnet=192.168.2.100/32
        leftnexthop=192.168.2.1
        leftcert=freeswan-pub.pem
        right=yyy.yyy.yyy.yyy
        rightsubnet=192.168.1.0/24
        rightnexthop=zzz.zzz.zzz.zzz
        rightcert=clientvpn-pub.pem
```

leftnexthop is the internal IP address of the Netgear router at the client end.
rightnexthop is the firewall at the FreeSWAN end

- Now restart FreeSWAN
    - /etc/rc.d/ipsec restart

FreeSWAN Firewall & IPSec Startup script

You may want/need to create a startup script for FreeSWAN… I use my own script that starts NAT (iptables).

Create the following script in /etc/rc.d then add it to various run levels (see your Linux manuals on how to do this).

```
#!/bin/sh -e
# /etc/rc.d/ipsecFS : start or stop IPSec Services

case "$1" in
        start)
                echo -n "Starting IPSec services"
                /etc/init.d/ipsec start
                modprobe iptable_nat
                iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
                echo -e "."
                ;;
        stop)
                echo -n "Stopping IPSec services"
                /etc/init.d/ipsec stop
                iptables --zero
                echo -e "."
                ;;
        restart|reload|force-reload)
                $0 stop
                $0 start
                ;;
        *)
                echo 'Usage: /etc/rc.d/ipsecFS {start|stop|restart}'
                exit 1
esac

exit 0
```

The iptables line enables the IPSec traffic to route into the network via NAT, thus looks like it comes from single IP address and does not conflict with normal routed traffic. This is because my FreeSWAN box is on a DMZ but has a NIC with a direct internal connection and not running via the firewall/normal network routed traffic.

My FreeSWAN server is in a DMZ behind a proper Firewall, and although **all** other services have been disabled via the firewall, if you want to be extra secure then you can add additional firewall rules to disable all other traffic apart from what is needed for IPSec.

Use this script in all the needed run levels to start FreeSWAN (see you Linux manual on how to do this!).

Windows Client Install with Netgear ProSafe VPN V10.1

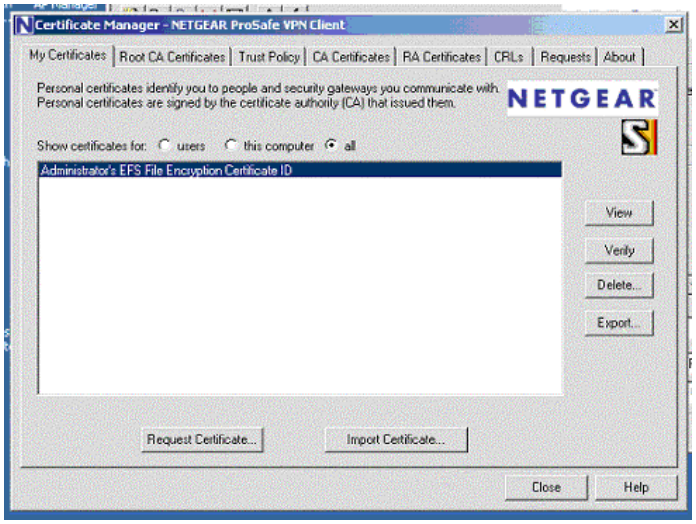
Note the screen shots have been doctored to show that sample configs

Install the VPN Client as per the manual (the config sample and screen shots are from a Win2K installation).

Load the Certificate Manager

- Select My Certificates Tab
- Click Import Certificate
- Browse to the floppy and open the clientvpn.p12 certificate
- Check Import certificate to local machine store
- Enter the password for the certificate

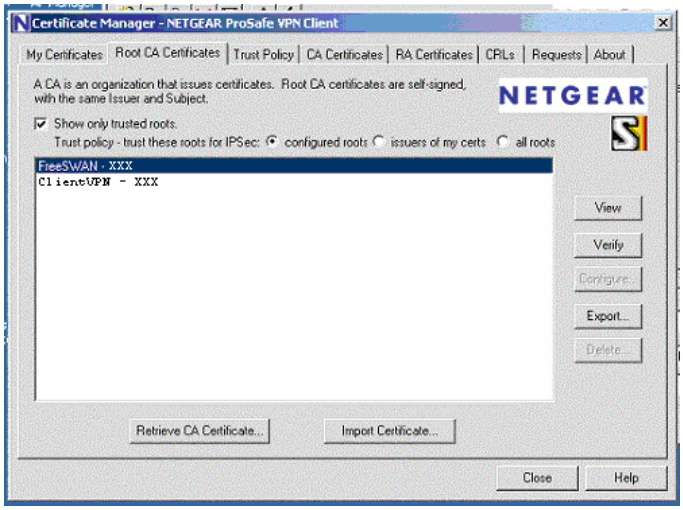
Below is a sample screen shot



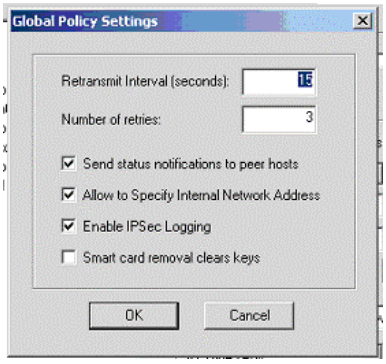
With the Certificate Manager

- Select Root CA Certificates Tab
- Click Import Certificate
- Select Files of Type and change to All Files (*.*)
- Open freeswan-pub-pem, select Yes
- Do the Same for the clientvpn-pub.pem file
- Click Close

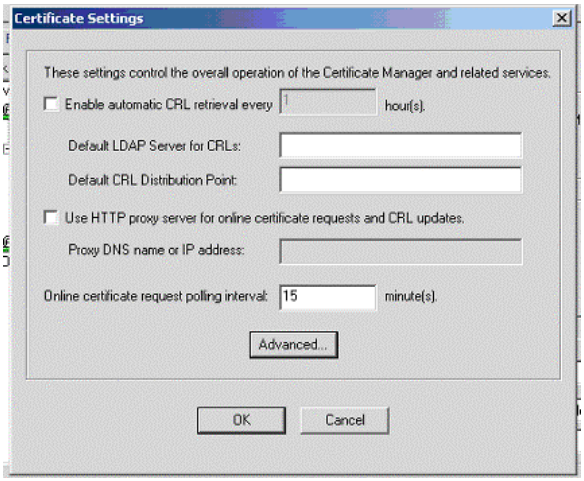
Below is a sample screen shot



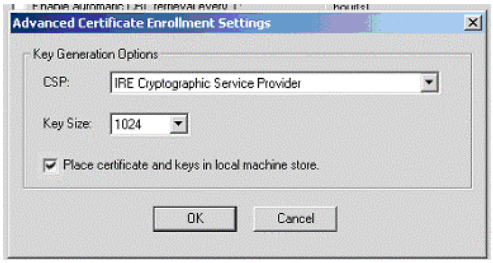
Load the Security Policy Manager, select Global Policy Settings from the Options menu and ensure the following settings



With the Security Policy Manager, select Certificate Settings from the Options menu and ensure the following settings



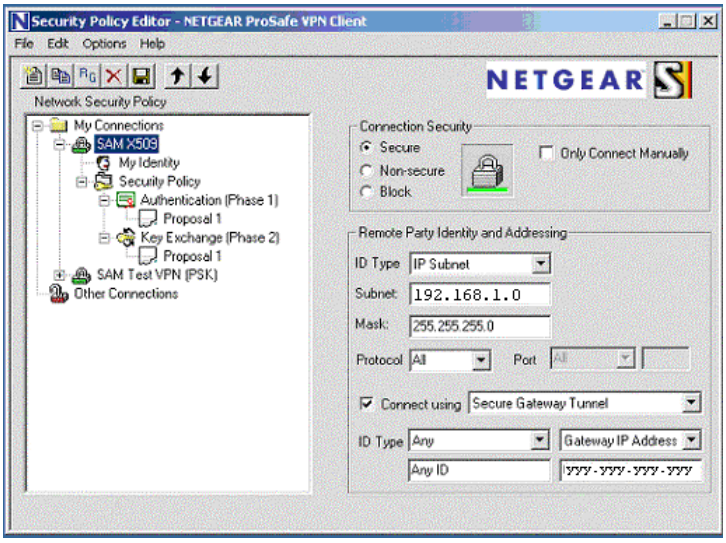
Click Advanced and ensure the following settings



Start the Security Policy Editor

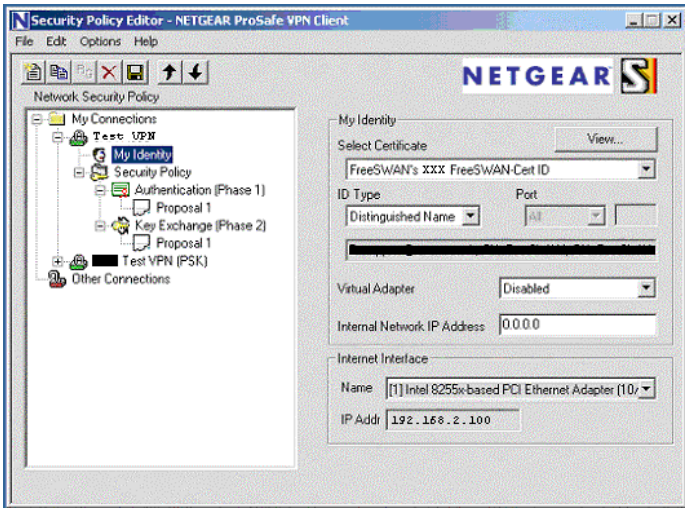
- From the Edit menu, select Add, Connection
- Right Click on the New Connection and rename it to something descriptive (Example below shows SAM X509

- Select Secure under Connection Security
- Under Remote Party Indentity and Addressing
    - ID Type: IP Subnet
    - Subnet: 192.168.1.0
    - Mask: 255.255.255.0
    - Protocol: All
    - Check Connect Using
        - Secure Gateway Tunnel
    - ID Type: Any, Any ID
        - Gateway IP Address, yyy.yyy.yyy.yyy



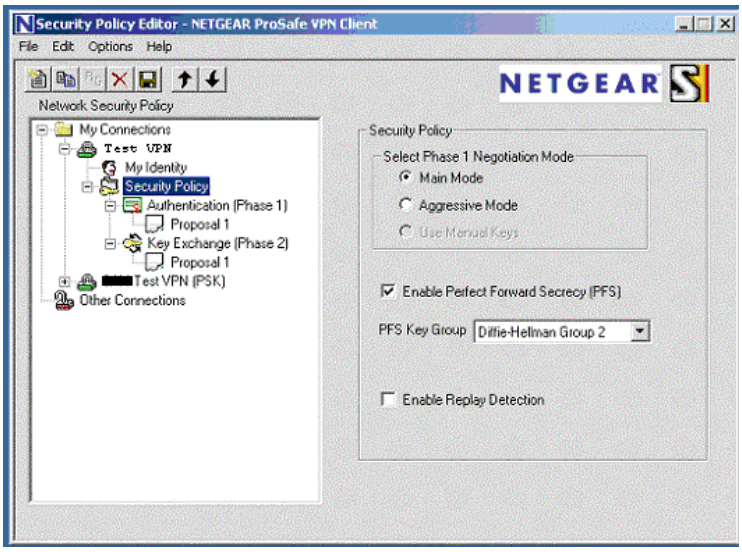
With the Security Policy Editor

- Select My Identity (for you new connection)
- Select the Certificate imported earlier, it should be – ClientVPN's SAM ClientVPN-Cert (in the example below it is called FreeSWAN's SAM FreeSWAN-Cert)
- ID Type: Distinguished Name
- Virtual Adapter: Disabled
- Internet Network IP Address: 0.0.0.0
- Select the Network Interface that you will be using (usually there is only one)



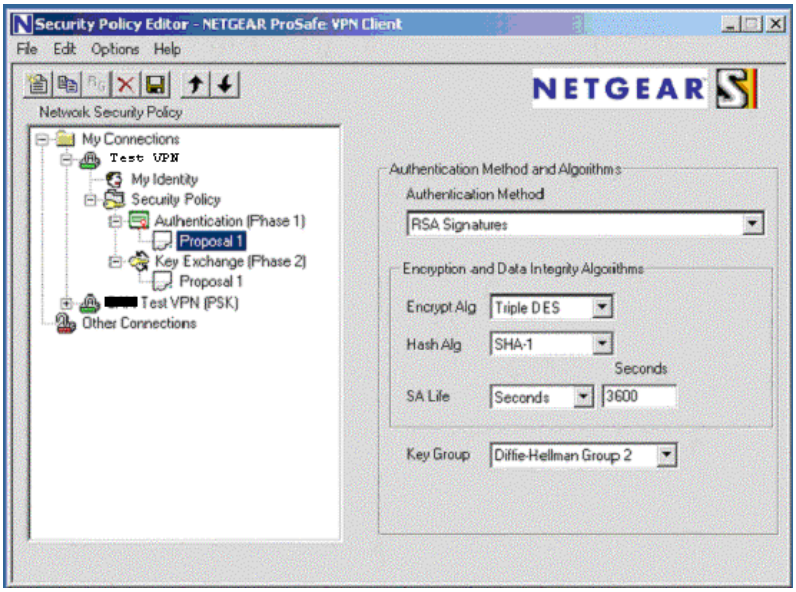
With the Security Policy Editor

- Select Security Policy (for you new connection)
- Select Main Mode
- Check Enable Perfect Forward Secrecy (PFS)
- PFS Key Group: Diffie-Hellman Group 2
- Uncheck Enable Replay Detection



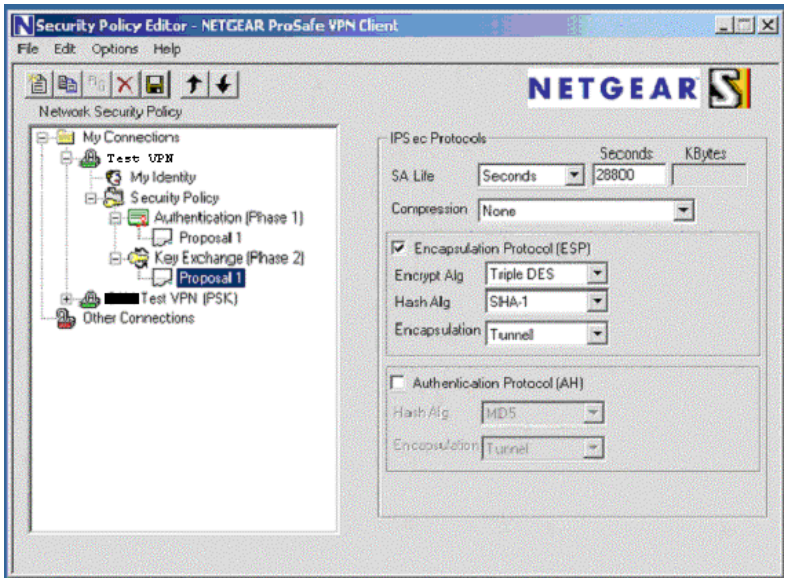
With the Security Policy Editor

- Select Proposal 1 under Authentication (Phase 1) (for you new connection)
- Authentication Method: RSA Signatures
- Encrypt Alg: Triple DES
- Hash Alg: SHA-1
- SA Life: Seconds, 3600
- Key Group: Diffie-Hellman Group 2



With the Security Policy Editor

- Select Proposal 1 under Key Exchange (Phase 2) (for you new connection)
- SA Life: Seconds, 28800
- Compression: Deflate
- Check Encapsulation Protocol (ESP)
- Encrypt Alg: Triple DES
- Hash Alg: SHA-1
- Encapsulation: Tunnel



Click the Floppy Disk icon to save the Connection Policy. You should now be ready to connect the VPNs, this can be done via the SysTray icon for Netgear ProSafe.

The log for a successful connection is shown below