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.

<u>Network Diagram</u>



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

0

- 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
 - o /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
- o mv newreq.pem clientvpn.pem
- o openssl pkcs12 –export –in clientvpn.pem –out clientvpn.p12
- o This will create a pkcs file which can be imported into the VPN Client
- o cp clientvpn.pem clientvpn-pub.pem
- o 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
 - o /usr/share/ssl/misc/CA.sh -newcert
 - o 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
 - o mv newreq.pem freeswan.pem
 - o 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
 - o 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
compress=yes
 auto=add
 type=tunnel
 authby=rsasig
 keyexchange=ike
 keyingtries=3
 pfs=yes
 left=xxx.xxx.xxx
 leftsubnet=192.168.2.100/32
 leftnexthop=192.168.2.1

leftcert=freeswan-pub.pem right=yyy.yyy.yyy rightsubnet=192.168.1.0/24 rightnexthop=zzz.zzz.zzz rightcert=clientypn-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
 - o /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/sl	n-e	
#/etc/rc	.d/ipsecF	S : start or stop IPSec Services
case "\$1	" in	
cuse ϕ_1	ni start)	
	start)	acho n "Starting IDSac sorvices"
		loto/init d/ingoo start
		reic/init.d/ipsec start
		echo -e "."
		·· ??
	stop)	
		echo -n "Stopping IPSec services"
		/etc/init.d/ipsec stop
		iptableszero
		echo -e "."
	restart re	eload force-reload)
	1	\$0 stop
		\$0 start
	*)	"
	/	echo 'Usage: /etc/rc.d/ipsecFS {start stop restart}'
		exit 1
6590		
esue		
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 <u>all</u> 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

My Certificates Root CA Certificates Trust Policy CA Certificates RA Certificates CRLr	Request	s About
Personal certificates identify you to people and security gateways you communicate with Personal certificates are signed by the certificate authority (CA1 that issued them	IETG	EAR
Show certificates for: C users C this computer C all		S
Administrator's EPS File Enclyption Certificate IU		View
		Verily
		Delete
		- Inportan
Request Certificate		
		11

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

	The contractor of	Trust Policy	CA Certific	ates RA Certifi	cates CRLs	Request	s About
A CA is an orga with the same I	anization that issues cer ssuer and Subject.	tilicates. Roo	ot CA certific	ates are self-sig	ned, N	ETG	EAR
Show only Trust policy	trusted roots. / - trust these roots for II	PSec: 🕫 co	nfigured roo	ts 🔿 issuers of i	my certs 🔿 .	all roots	S
FreeSWAN - 2	×××						
CITERCOFM	***						View
							Verify
							Configure .
							Export
							Delete
		da da da da da					

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

Enable automatic CRL retrieval every Hour(s). Default LDAP Server for CRLs: Default CRL Distribution Point. Use HTTP proxy server for online certificate requests and CRL updates. Proxy DNS name or IP address: Online certificate request polling intervat. 15 minute(s).
Default LDAP Server for CRLs: Default CRL Distribution Point Use HTTP proxy server for online certificate requests and CRL updates. Proxy DNS name or IP address: Online certificate request polling intervat: 15 minute(s).
Default CRL Distribution Point: Use HTTP proxy server for online certificate requests and CRL updates. Proxy DNS name or IP address: Online certificate request polling interval: 15 minute(s).
Use HTTP proxy server for online certificate requests and CRL updates. Proxy DNS name or IP address: Online certificate request polling interval: 15 minute(s).
Proxy DNS name or IP address: Online certificate request polling intervat 15 minute(s).
Online certificate request poling interval: 15 minute(s);
Advanced

Click Advanced and ensure the following settings

DOD.	IDE Contractilité Consiste Donistes	
san:	I'me cryptographic service Provider	<u> </u>
		
ey Size	1024 💌	
 Place 	e certificate and keys in local machine store.	

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
 - o ID Type: IP Subnet
 - o Subnet: 192.168.1.0
 - o Mask: 255.255.255.0
 - o Protocol: All
 - Check Connect Using
 - Secure Gateway Tunnel
 - ID Type: Any, Any ID
 - Gateway IP Address, yyy.yyy.yyy

Network Security Policy	NETGEAR S
My Connections My Connections My Connections My Identity Security Policy G Authentication (Phase 1)	Connection Security C Secure C Non-secure C Block
Key Exchange (Phase 2) Proposal 1 SAM Test VPN (PSK) Other Connections	Remote Party Identity and Addressing ID Type IP Subnet Subnet 192.168.1.0 Mask: 255.255.250 Protocol All Pot All Y Connect using Secure Gateway Tunnel ID Type Any Gateway IP Address Any ID

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)

Network Security Policy	NETGEAR 5
My Connections 	My Identity Select Certificate
E Security Policy	FreeSWAN's XXX FreeSWAN-Cert ID
Connections	ID Type Port Distinguished Name Virtual Adapter Urtual Adapter Internal Network IP Address 0000
	Internet Interface Name [1] Intel 8255x-based PCI Ethernet Adapter (10/

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

Security Policy Editor - NETGEAR ProSafe VF File Edit Options Help	N Client
Network Security Policy Network Security Policy My Connections Test UPN Security Policy Contentication (Phase 1) Proposal 1 Key Exchange (Phase 2) Proposal 1 Test VPN (PSK) Other Connections	Security Policy Select Phase 1 Negotiation Mode Main Mode Aggressive Mode Cuse Merival Keys Frable Perfect Forward Secrecy (PFS) PFS Key Group Diffie-Helman Group 2

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

1 Ba Ba X III ↑ ↓ Network Security Policy	NETGEAR S
My Connections Test VPX - S My Identity - S Security Policy	Authentication Method and Algorithms Authentication Method
Authentication (Phase 1) Proposal 1 Second Second	RSA Signatures
	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

Network Security Policy	
Connections	SA Life Seconds 28800 KBytes SA Life Seconds 28800 Seconds Sec
	Authentication Protocol (AH) Hash Alg MDS Y EncossUlation Turnel

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

			1.000	sonaad association service			: 2999			angeroona na a					
NL	og Viewer - NETGEAF	R ProSafe VPN C	lient	:- :-											
	Clear Freeze	Savelog	Print 1	Close	P										
	Ciodi Hocco	J Jave Log	THIC	CIOSO											Alex Second
-				-						1.1.1.1.1.1					-
4	23: 14:07:24.010 HIS 29: 14:07:24.010 Mu Ca	COUKIE SCIDE 3	0 Z D Z/ a/	INCSSS IC		INCO SUAS		10							
	29: 14:07:49 146 Filter I	table loaded	, SEINE	11402222215	MANIP UMA	INFO (RMS	SH, DEL)							10.00
4	29: 14:07:49.146 My Co	annections	- Filter r	ecord 1 upd	ated.										2017
4	29: 14:07:49.146 My Co	onnections\	Fest VPN (PS	K) · Filter re	cord 2 upda	ted.									1.1
4	29: 14:07:55.395														200
4	29: 14:07:55.395 My Co	onnections	 Initiati 	ng IKE Phas	e 1 (IP ADD	R=62.49.10	0.101)								20122
4	29: 14:07:56.016 My Lo 29: 14:07:56 026 My Lo	onnections v	- SENU	ING>>>> IS	AKMP UAK	MM (SA, VI MM (SA)	iU ZXJ								673.65
	29: 14:07:56.958 My Co	onnections'	SEND	ING>>>> IS	AKMP DAK	MM (KE N	ION. VID	D 3v)							12.5
4	29. 14:07:57.198 My Co	onnections\	- RECE	IVED<<< IS	AKMP OAK	MM (KE, NO	ION, CEF	RT_REQ)							22122
4	29: 14:07:58.570 My Co	onnections\{	 Using 	configured r	nachine cerl	ificate "Free	eSWAN	N's 🖬 Fre	eeSWAN-C	ert ID".					
4	29: 14:07:58.690 My Co	onnections	- SEND	ING>>>> IS	AKMP OAK	MM "(ID, CE	ERT, CE	CERT_REQ	2x, SIG, N	OTIFY:ST	ATUS_INI	TIAL_COM	ITACT)		100
4	29: 14:07:58.800 My Co 29: 14:07:58.800 My Co	onnections	- HELE	IVED<<< ISI	AKMP UAK	MM "(ID, CE	ERI, SI	(16)							2018
	29: 14:07:58:901 My LC	COOKIE 2167 a8	b6 12 69 9a	ISNED INE SI	4										
4	29:14:07:58.901 HIS	COOKIE 9 te 2e	e3 6a 62 23	e9											(S. 198
4	29: 14:08:00.042 My Co	onnections	<509 - Initiati	ng IKE Phas	e 2 with Clie	nt IDs (mess	isage id:	: AB040FA	1)						1.000
4	29: 14:08:00.042 Initia	tor = IP ADDR=62	2.49.10.108,	prot = 0 port	= 0		-								1.1
4	29:14:08:00.042 Resp	ponder = IP SUBN	IET/MASK=	199.97.191.0	1/255.255.2	55.0, prot =	= 0 port =	= 0							
4	23: 14:08:00.042 My Co 29: 14:09:00 202 My Co	onnections	- SENL	ING>>>> 15 D/ED//// IC	AKMP DAK	UM THASH	H, SA, N LI CA NI	NUN, KE, IL	D 2xj						
4	29: 14:08:00.233 My Co	onnections'	- SEND	ING>>>> IS	AKMP DAK	OM "HASH	H)	NUN, NE, IL	2 2 AJ						
4	29: 14:08:00.453 My Co	onnections	Loadi	na IPSec SA	(Message I	D = A8040F	FÁ1 OUT	JTBOUND :	SPI = 8181:	8665 INB(DUND SPI	= 67D 775	001		
4	29: 14:08:00.453			-									-		-
18 mg	a construction of the second second														
						1001							and the second	 	