Free s/wan 1.8 ←→ IRE SafeNet / Soft-PK 5.1.0
Road-Warrior VPN Configuration Guide

By Keith T. Morgan
Network Security Specialist
Terradon Communications Group
keith.morgan@terradon.com

Introduction: The purpose of this document is to provide other firewall and network Administrators knowledge that I have gathered to deploy a Free S/Wan to IRE SafeNet road warrior VPN solution. I, or Terradon Communications, LLC make no warranty expressed or implied regarding the accuracy, or usability of this document. Nor are we affiliated with IRE in any way. We would simply like to help the information security community in their efforts to provide secure, strongly encrypted road-warrior connectivity to their users.

Assumptions: The author of this document is assuming that the reader is familiar with the basic installation and configuration of Free S/Wan. If this is not the case, please visit **http://www.freeswan.org** and read the fine manuals provided on that website and other locations. Installation of Free S/Wan and basic configuration is beyond the scope of this document, as are the lower-level aspects of data and traffic encryption.

Free S/Wan side: Below is a sample ipsec.conf file containing only one entry. This is a good example of a road-warrior type connection. In our configuration, we are running this concurrent with network to network and endpoint to network VPN configurations. Also, we are running automatic key exchange via Pluto. In this example the other connections and actual IP addresses in our configurations have been omitted or changed to protect the innocent.

Example network:

```
Road-warrior ----- 10.19.17.13(router)-----10.19.17.254(firewall)==192.168.27.0(protected network)
```

/etc/ipsec.secrets.

To my knowledge, the easiest way to configure SafeNet to Free S/Wan authentication is via a pre-shared secret. Note that all road-warriors must share the same secret. Your /etc/ipsec.secrets file must contain the following line (substitute your pre-shared secret) along with the private key information that should already be present.

```
0.0.0.0   10.19.17.254 : PSK "verylongveryhardtoguessstringpreferablyrandomcharacters"
```

/etc/ipsec.conf

```
config setup
        interfaces=”ipsec0=eth0”
        klipsdebug=none
        plutodebug=none
        plutoload=%search
        plutostart=%search
        uniqueids=no

conn %default
        keyingtries=0

conn road-warrior
        type=tunnel
        keyingtries=1
        left=%any
        leftnexthop=
        right=10.19.17.254
        rightsubnet=192.168.27.0
        rightfirewall=yes
        authby=secret
        auto=add
```

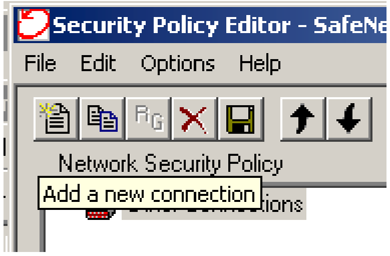
** Note: Substitute eth0 for the external interface of your free-swan VPN server.

SafeNet / Soft PK configuration

Now we’ll run through the SafeNet / Soft PK configuration step by step (assuming you already have it installed on your road-warrior workstation.)

- Launch the SafeNet Security Policy Editor (right-mouse click the S/N icon in the system tray)

Add a new connection and name it

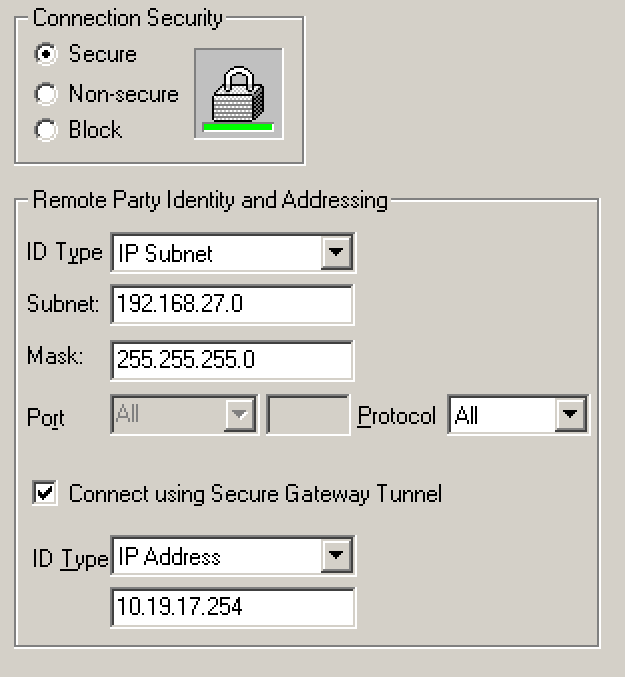


- Click your new connection in the left pane so it is highlighted.

In the right pane,

- The connection security should be set to “secure.”
- The remote party addressing should be set to ip subnet.

- Fill in the appropriate network and mask. This is your protected network sitting behind the firewall.
- Select the checkbox labeled "Connect using Secure Gateway Tunnel."
- Set the IP address to the external IP address of your firewall or VPN server.



Connection Security

● Secure

○ Non-secure

○ Block

Remote Party Identity and Addressing

ID Type: IP Subnet

Subnet: 192.168.27.0

Mask: 255.255.255.0

Port: All

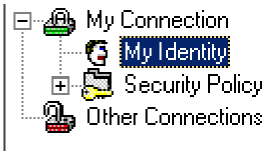
Protocol: All

☑ Connect using Secure Gateway Tunnel

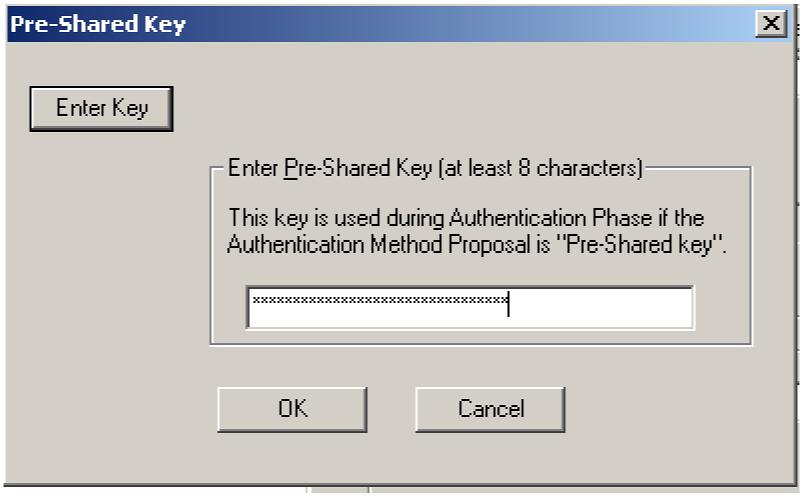
ID Type: IP Address

10.19.17.254

- Expand the connection properties in the left pane, and select "My Identity."



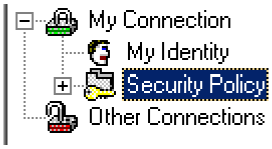
- In the right pane click the button labeled “Pre Shared Key.”
- Click the “Enter Key” button.



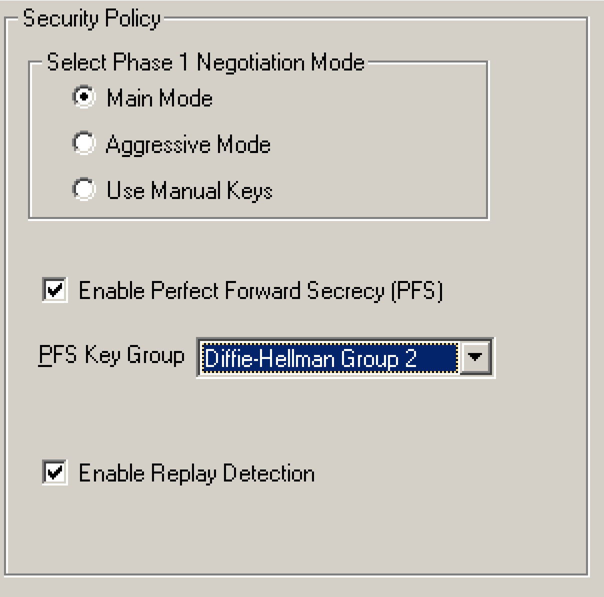
Enter Pre-Shared Key (at least 8 characters)

This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".

- Enter the string used in /etc/ipsec.secrets after the “PSK:” (omit the quotes.)
- Leave the “select certificate,” “id type” and “internet interfaces” at their defaults.
- In the left pane, click the “Security Policy” branch.



- In the right pane, leave the “Select Phase 1 Negotiation Mode” at its default setting of “Main Mode.”
- Check the “Enable Perfect Forward Secrecy (PFS)” checkbox.
- In the “PFS Key Group” dropdown list, select Diffie-Hellman Group 2.
- Check the “Enable Replay Detection” checkbox.



Security Policy

Select Phase 1 Negotiation Mode

● Main Mode

○ Aggressive Mode

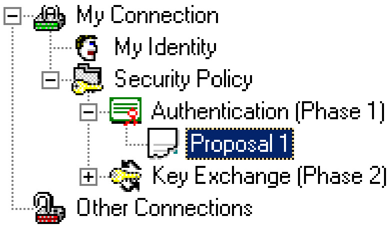
○ Use Manual Keys

☑ Enable Perfect Forward Secrecy (PFS)

PFS Key Group: Diffie-Hellman Group 2

☑ Enable Replay Detection

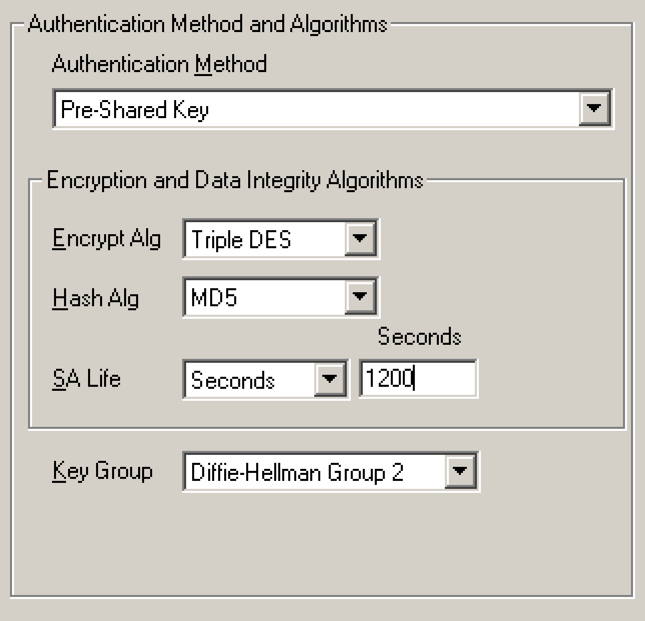
- Expand the Security Policy branch.
- Expand the Authentication Phase 1 branch.



```
⊟ My Connection
    My Identity
  ⊟ Security Policy
    ⊟ Authentication (Phase 1)
        Proposal 1
    ⊞ Key Exchange (Phase 2)
  Other Connections
```

- Select the Proposal 1 branch.

- In the right pane, set the “Authentication Method” to “Pre-Shared key.”
- Set the “Encryption Alg” to “Triple DES.”
- Set the “Hash Alg” to “MD5.”
- Set the “SA Life” to “seconds” in the dropdown menu, and “1200” in the input box.
- Set the “Key Group” to “Diffie-Hellman Group 2.”



Authentication Method and Algorithms

Authentication Method: Pre-Shared Key

Encryption and Data Integrity Algorithms

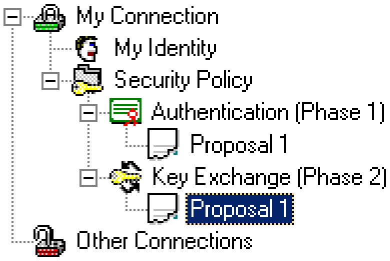
Encrypt Alg: Triple DES

Hash Alg: MD5

SA Life: Seconds — Seconds: 1200

Key Group: Diffie-Hellman Group 2

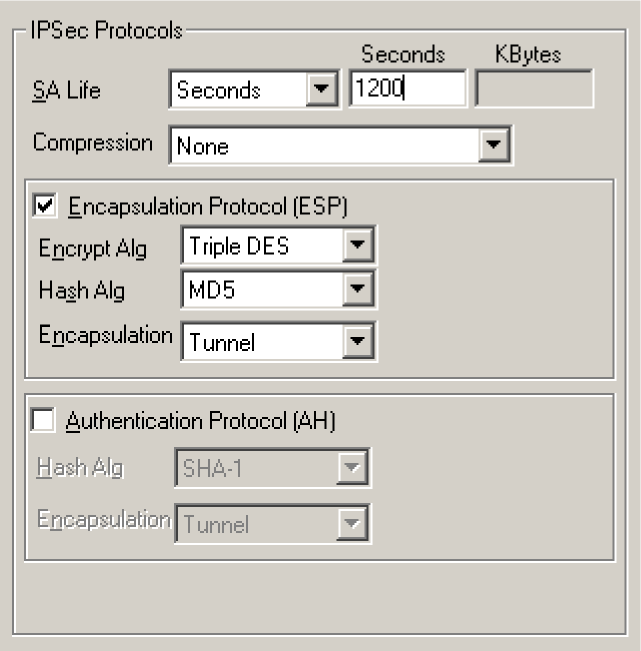
- Expand the “Key Exchange Phase 2” branch.



My Connection
My Identity
Security Policy
Authentication (Phase 1)
Proposal 1
Key Exchange (Phase 2)
Proposal 1
Other Connections

- Select the “Proposal 1” branch.

- Set the “SA Life” to 1200 seconds.
- Set the Compression to “None.”
- Check the “Encapsulation Protocol (ESP)” checkbox.
- Set the “Encryption Alg” to “Triple DES.”
- Set the “Hash Alg” to “MD5.”
- Set the Encapsulation to “Tunnel.”



IPSec Protocols

		Seconds	KBytes
SA Life	Seconds	1200	
Compression	None		

☑ Encapsulation Protocol (ESP)

Encrypt Alg: Triple DES

Hash Alg: MD5

Encapsulation: Tunnel

☐ Authentication Protocol (AH)

Hash Alg: SHA-1

Encapsulation: Tunnel

Save your connection and you should be ready to connect. Key exchanges should take place in the background, requiring no user input to establish the VPN connection. When SafeNet / Soft PK detects traffic destined for the defined network, it automatically connects to Free S/Wan on UDP port 500 for the key exchanges, and will then encrypt your traffic over TCP Proto 50.