



VPN Connection to FreeS/WAN IPSec Gateway

28 November 2002

This document explains how to configure a network environment where an SSH Sentinel client connects to a FreeS/WAN IPSec gateway. An OpenSSL certification authority issues certificates necessary for authentication.

© 2000-2002 SSH Communications Security Corp

No part of this publication may be reproduced, published, stored in an electronic database, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, for any purpose, without the prior written permission of SSH Communications Security Corp.

This software is protected by international copyright laws. All rights reserved. ssh® is a registered trademark of SSH Communications Security Corp in the United States and in certain other jurisdictions. SSH2, the SSH logo, IPSEC Express, SSH Certifier, SSH Sentinel, SSH NAT Traversal, IPSEC on silicon, Hypermode, SSH Accession, SSH Token Master, SSH Secure Shell and Making the Internet Secure are trademarks of SSH Communications Security Corp and may be registered in certain jurisdictions. All other names and marks are property of their respective owners.

THERE IS NO WARRANTY OF ANY KIND FOR THE ACCURACY OR USEFULNESS OF THIS INFORMATION EXCEPT AS REQUIRED BY APPLICABLE LAW OR EXPRESSLY AGREED IN WRITING.

SSH Communications Security Corp.

Fredrikinkatu 42
FIN-00100 Helsinki
FINLAND

SSH Communications Security Inc.
1076 East Meadow Circle
Palo Alto, CA 94303
USA

SSH Communications Security K.K.
House Hamamatsu-cho Bldg. 5F
2-7-1 Hamamatsu-cho, Minato-ku
Tokyo 105-0013, JAPAN

<http://www.ssh.com/>
e-mail: ipsec-sales@ssh.com (sales), sentinel-support@ssh.com (technical support)
Tel: +358 20 500 7030 (Finland), +1 650 251 2700 (USA), +81 3 3459 6830 (Japan)
Fax: +358 20 500 7031 (Finland), +1 650 251 2701 (USA), +81 3 3459 6825 (Japan)

Contents

1	VPN Connection to FreeS/WAN IPsec Gateway	5
1.1	Introduction	5
1.1.1	Further Information	7
1.1.2	Requirements	7
1.2	Compiling the FreeS/WAN Gateway with the Patches	8
1.3	Setting Up the OpenSSL-Based CA	10
1.4	Creating the Certificate Revocation List (CRL)	11
1.5	Creating the Certificate for the FreeS/WAN Gateway	12
1.6	Creating the Certificate for the SSH Sentinel Client	14
1.7	Configuring FreeS/WAN for VPN Remote Clients	17
1.8	Restarting the FreeS/WAN Gateway	17
1.9	FreeS/WAN Sample Configurations	18
1.9.1	VPN Tunnel without Virtual IP Support	19
1.9.2	VPN Tunnel with Virtual IP Support: DHCP over IPsec	23
1.9.3	VPN Tunnel with Virtual IP Support: Manual Assignment	30
1.10	Configuring SSH Sentinel	39
1.10.1	Creating the Authentication Key	39
1.10.2	Creating the VPN Rule	39
1.11	Troubleshooting	42

1.11.1 FreeS/WAN IPsec Gateway	42
1.11.2 SSH Sentinel	44

Chapter 1

VPN Connection to FreeS/WAN IPsec Gateway

The goal of this interoperability document is to give a good start for an experienced FreeS/WAN IPsec administrator to deploy a roadwarrior gateway for SSH Sentinel VPN remote clients.

This document does not instruct installing the Linux distribution, patching and compiling Linux sources, updating active kernel, planning IP routing, and so on. We recommend that you use the documentation of your software vendor for reference. This interoperability guide is an *additional* information source, not a comprehensive manual for VPN deployment.

1.1 Introduction

This document explains how to create a network environment shown in Figure 1.1 (The network environment). The FreeS/WAN host acts as a security gateway, which is contacted by the SSH Sentinel host to establish a virtual private connection to the private network protected by the gateway.

The document also explains how to create the certificates necessary for authentication. The OpenSSL certification authority runs on the FreeS/WAN host.

Although you can use pre-shared keys for authentication, certificates are recommended for security reasons. The support for X.509 certificates is imported by a user-contributed software patch.

All the combinations of the following variables are tested:

- Authentication: pre-shared key, X.509 certificate
- Encryption: 3DES, AES
- Virtual IP technique: none, manual, DHCP over IPsec.

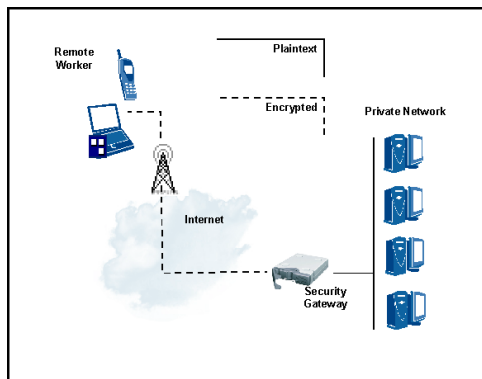


Figure 1.1: The network environment

In addition to these proposal variables, all the sample configurations in this document use the following IKE/IPSec proposals:

- IP compress: disabled
- IKE lifetime: 240 minutes (4 hours)
- IPSec lifetime: 60 minutes (1 hour)
- IKE integrity: MD5
- IKE mode: main mode
- IKE group: MODP 1024 (group 2)
- IPSec integrity: MD5
- IPSec mode: tunnel (for all VPN connections)
- PFS: enabled (MODP 1024, group 2).

This document does **not** cover the following scenarios:

- NAT-Traversal (NAT-T) patch
- Transport mode host-to-host connections.

SSH Sentinel supports NAT-Traversal and we have received feedback about successful NAT-T deployments from FreeS/WAN users by using a NAT-T patch from <http://open-source-arkoon.net/> but since it requires an additional add-on patch onto FreeS/WAN sources and we are already using several add-on patches here, the patches may interfere with each other.

If you are interested in deploying NAT-Traversal for you FreeS/WAN gateway, please take a look on a pre-patched FreeS/WAN source package called SuperFreeS/WAN available at <http://www.freeswan.ca/code/super-freeswan/>.

If you are interested in securing a *transport mode* host-to-host connection between the FreeS/WAN and SSH Sentinel hosts, please refer to the FreeS/WAN and SSH Sentinel documentation. SSH Sentinel supports transport mode connections (**Security Policy** -> **Secured Connections** -> **Add**). Depending on your FreeS/WAN configuration, you may want to use X.509 certificates or a pre-shared key for authentication, and 3DES or AES for encryption. **Note:** FreeS/WAN must have a transport mode connection profile (`type=transport` for the FreeS/WAN connection profile) for this kind of host-to-host usage.

1.1.1 Further Information

- SSH Sentinel User Manual (also available as online help)
- SSH Sentinel technical support: <http://www.ssh.com/support/products/sentinel/>
- FreeS/WAN IPSec project: <http://www.freeswan.org>
- X.509 patch for FreeS/WAN: <http://www.strongsec.com/freeswan>
- OpenSSL: <http://www.openssl.org>
- Linux Documentation Project: <http://www.linuxdoc.org>
- Red Hat Inc.: <http://www.redhat.com>
- ALGO (AES) patch: <http://www.irrigacion.gov.ar/juanjo/ipsec/>
- Delete SA Notification patch: <http://open-source-arkoon.net/>.

1.1.2 Requirements

The interoperability between SSH Sentinel and FreeS/WAN IPSec was tested using the following software:

- Red Hat Linux v7.3
- Linux kernel 2.4.18-10 from RH 7.3 Errata
- FreeS/WAN v1.99
- x509patch-0.9.15-freeswan-1.99 (required for X.509 certificate support)
- algo patch v0.8.0 (required for AES/Rijndael encryption support)
- dhcrelay v0.3.1 (required for DHCP over IPSec support)
- notify_delete-freeswan-1.98b-020904 patch (for Delete SA Notification support)
- OpenSSL v0.9.6b
- SSH Sentinel v1.4.

Even though this document is based on a configuration with Red Hat Linux, you should be able to run any Linux distribution to get similar results. Moreover, you can also try using a newer version of Red Hat Linux. However, the functionality is only verified with the above components.

Using kernel sources from Red Hat Linux `kernel-source-*.src.rpm` might be problematic because of the numerous patches from Red Hat Linux Inc. that might not merge properly with the FreeS/WAN sources.

1.2 Compiling the FreeS/WAN Gateway with the Patches

1. Download the source code.
2. The source code for Linux kernel must be in `/usr/src/linux`. For example Red Hat 7.3 requires you to add a symbolic link as follows:

```
# cd /usr/src
# ln -s linux-2.4 linux
```

3. Extract both FreeS/WAN and x509patch sources to `/usr/src` (this example assumes that you have first downloaded them to `/root/src` directory):

```
cd /usr/src
tar xvfz /root/src/freeswan-1.99.tar.gz
tar xvfz /root/src/x509patch-0.9.15-freeswan-1.99.tar.gz
```

4. To get X.509 certificate support for FreeS/WAN, install the x509patch:

```
# cd /usr/src/freeswan-1.99
# patch -p1 < ../x509patch-0.9.15-freeswan-1.99/freeswan.diff
```

For more detailed information, please refer to the x509patch README file or <http://www.strongsec.com/freeswan>.

5. To get AES/Rijndael encryption support, install the following patches:

```
# zcat /root/src/freeswan-alg-0.8.0-BASE-common.diff.gz | patch -p1 -s
# zcat /root/src/freeswan-alg-0.8.0-BASE-klips.diff.gz | patch -p1 -s
# zcat /root/src/freeswan-alg-0.8.0-BASE-pluto_with_x509.diff.gz | patch -p1 -s
# zcat /root/src/freeswan-alg-0.8.0-enc-aes.diff.gz | patch -p1 -s
```

For more detailed information, please refer to the patch HOWTO-ipsec_alg.txt document or <http://www.irrigacion.gov.ar/juanjo/ipsec/>.

6. Install the Delete SA Notification patch:

```
# zcat /root/src/notify_delete-freeswan-1.98b-020904.diff.gz|patch -p1 -s
```

For more detailed information, please refer to <http://open-source.arkoon.net/>.

7. Patch the Linux kernel sources with FreeS/WAN and compile FreeS/WAN.

If you use the kernel-sources rpm package instead of the official kernel tar package and you would like to compile an identical kernel with those standard Red Hat Linux kernels but patched for FreeS/WAN IPsec support, you may want to use the .config files included in the kernel-source rpm package. For example, if you have a single processor machine with a i686 CPU you could use the /usr/src/linux/configs/kernel-2.4.18-i686.config file:

```
# cd /usr/src/linux
# cp configs/kernel-2.4.18-i686.config .config
# make config
# make dep
```

Enter the following commands to compile both FreeS/WAN and the kernel:

```
# cd /usr/src/freeswan-1.99
# make ogo
```

If you used the algo patch for AES support, you must select the following kernel options:

```
IPSEC Modular Extensions (CONFIG_IPSEC_ALG) [Y/n/?] y AES
encryption algorithm (CONFIG_IPSEC_ALG_AES) [M/n/y/?] m
```

For more information on the kernel options required and recommended by FreeS/WAN, please refer to the FreeS/WAN documentation, especially [doc/kernel.html](#).

8. Compile the kernel and kernel modules, install them, and configure the boot loader (LILO, Grub, ...) to boot up the system with the new kernel as a default.

When using Red Hat Linux you may want to use the following procedure:

```
# cd /usr/src/linux
# make bzImage
# make install
# make modules
# make modules_install
```

Finally, prepare your default boot loader to boot up the system with this newly compiled and installed kernel.

Please refer to the FreeS/WAN documentation for more details. The Kernel-HOWTO document by Linux Documentation Project gives a lot of useful information about compiling and setting up a new kernel to the system (<http://www.tdlp.org>).

9. Configure the boot-up scripts to load the AES kernel module automatically after a reboot. You can load the AES module automatically with the rc.local script, for example:

```
# echo "modprobe ipsec_aes" >> /etc/rc.d/rc.local
```

1.3 Setting Up the OpenSSL-Based CA

1. Create your own OpenSSL-based Certificate Authority (CA).

You must have OpenSSL installed on your CA host. The Red Hat Linux 7.3 based test CA server used in this example has the following rpm packages installed:

```
# rpm -qa | grep openssl | sort
openssl-0.9.6b-28
openssl-devel-0.9.6b-28
```

You can find the configuration file for OpenSSL from `/usr/share/ssl/openssl.cnf`. Check the `openssl.cnf` default settings. Also, check the script file `/usr/share/ssl/misc/CA` installed by `openssl-0.9.6b-28` rpm package. These two files and their default settings are used for creating the CA and client certificates later.

To create a new CA, enter the following command:

```
# cd /usr/share/ssl/misc
# ./CA -newca
CA certificate filename (or enter to create)

Making CA certificate ...
Using configuration from /usr/share/ssl/openssl.cnf
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to './demoCA/private/./cakey.pem'
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:FI
State or Province Name (full name) [Berkshire]:Eastern Finland
Locality Name (eg, city) [Newbury]:Kuopio
Organization Name (eg, company) [My Company Ltd]:SSH Communications Security Corp
Organizational Unit Name (eg, section) []:SSH Sentinel OpenSSL test CA team
Common Name (eg, your name or your server's hostname) []:ca.kuo.ipsec.com
Email Address []:sentinel-support@ssh.com
```

Since you will need the password protecting the private key later (when issuing certificates, for example) make sure to memorize it.

In this example, we used `ca.kuo.ipsec.com` as the Common Name (identity) for our CA certificate. The Fully Qualified Domain Name (FQDN) of the host in the test environment was `freeswan.kuo.ipsec.com`.

Note: Do not use the same Common Names (identities) for both the CA root certificate and the FreeS/WAN host certificate.

By default, the `/usr/share/ssl/misc/CA` script creates CA and client certificates which are valid for 365 days. If you want to create a root CA certificate which is valid for 10 years, you must create the CA manually as follows (all the client certificates issued by the CA are still valid for 365 days but the root CA certificate is valid for 3650 days (about 10 years)):

```
# cd /usr/share/ssl/misc
# mkdir demoCA
# cd demoCA
# mkdir certs crl newcerts private
# openssl req \
    -new \
    -x509 \
    -keyout private/cakey.pem \
    -out cacert.pem \
    -days 3650
# cd ..
```

2. The FreeS/WAN gateway needs the certificate of the root CA when authenticating the remote host. The root CA certificate must be available in FreeS/WAN directory `/etc/ipsec.d/cacerts/` :
-

```
# cd /usr/share/ssl/misc/demoCA
# ls
cacert.pem  certs  crl  index.txt  newcerts  private  serial
# cp -p cacert.pem /etc/ipsec.d/cacerts/myCAcert.pem
```

1.4 Creating the Certificate Revocation List (CRL)

The `x509patched` FreeS/WAN checks Certificate Revocation Lists (CRLs) from directory `/etc/ipsec.d/crls/`.

To create and install a CRL valid for 15 days, use the following procedure. The required password is the one used for protecting private keys of the root CA certificate in the previous section.

```
# cd /usr/share/ssl/misc
```

```
# openssl ca -gencrl -crl days 15 -out crl.pem
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
```

```
# cp -p crl.pem /etc/ipsec.d/crls/myCrl.pem
```

The documentation of the x509patch gives more information about revocating a certificate and updating the CRL file. Check the README document included in the x509patch source package, or the homepage of the patch at <http://www.strongsec.com/freeswan/>.

1.5 Creating the Certificate for the FreeS/WAN Gateway

1. Run the following command to create a certificate request:

```
# cd /usr/share/ssl/misc

# ./CA -newcert
Using configuration from /usr/share/ssl/openssl.cnf
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'newreq.pem'
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
-----

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----

Country Name (2 letter code) [GB]:FI
State or Province Name (full name) [Berkshire]:Eastern Finland
Locality Name (eg, city) [Newbury]:Kuopio
Organization Name (eg, company) [My Company Ltd]:SSH Communications Security Corp
Organizational Unit Name (eg, section) []:SSH Sentinel FreeSWAN test team
Common Name (eg, your name or your server's hostname) []:ca.kuo.ipsec.com
Email Address []:sentinel-support@ssh.com
Certificate (and private key) is in newreq.pem
```

Since you will need the password protecting the private key when later accessing it, make sure to memorize it.

Note: The Common Name (identity) for the FreeS/WAN host certificate and the root CA certificate created earlier must be different, even when both services (OpenSSL CA and FreeS/WAN IPSec) are running on the same host.

2. Sign the certificate request with your OpenSSL root CA certificate. The first required password is for the certificate request, and the second for the CA:

```
# cd /usr/share/ssl/misc

# ./CA -signcert
Cert passphrase will be requested twice - bug?
Getting request Private Key
Enter PEM pass phrase:
Generating certificate request
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
Check that the request matches the signature
Signature ok
The Subjects Distinguished Name is as follows
countryName          :PRINTABLE:'FI'
stateOrProvinceName  :PRINTABLE:'Eastern Finland'
localityName         :PRINTABLE:'Kuopio'
organizationName     :PRINTABLE:'SSH Communications Security Corp'
organizationalUnitName:PRINTABLE:'SSH Sentinel FreeSWAN test team'
commonName           :PRINTABLE:'ca.kuo.ipsec.com'
emailAddress         :IA5STRING:'sentinel-support@ssh.com'
Certificate is to be certified until Oct 11 12:52:31 2003 GMT (365 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

[ properties of your freeswan host certificate listed here ]
```

3. Install the signed FreeS/WAN host certificate and private keys:

```
# cp -p newcert.pem /etc/ipsec.d/certs/myCert.pem

# cp -p newreq.pem /etc/ipsec.d/private/myKey.pem
```

The private keys are included in the certificate request file.

The x509patch version used supposes that the certificates are stored under the /etc/ipsec.d/ directory. Later patch releases targeted to FreeS/WAN v2.0 require the certificates to be in directory /etc/ipsec.d/certs/.

Since this document is targeted to FreeS/WAN v1.9x, we install the certificates under the `/etc/ipsec.d/certs/` directory, and our FreeS/WAN sample configurations read the certificates (namely FreeS/WAN host certificate `myCert.pem`) from the `/etc/ipsec.d/certs/` directory.

4. Configure the FreeS/WAN secrets file for the RSA private key.

The secrets file of FreeS/WAN IPsec is `/etc/ipsec.secrets`. Here you must either declare the pre-shared key (PSK, shared secret) or the location of the RSA private keys if deploying X.509 certificates instead.

If using pre-shared key authentication, the secrets file `/etc/ipsec.secrets` of a FreeS/WAN gateway with public `eth0` interface IP address `172.16.13.9` serving roadwarrior VPN clients must include the pre-shared key as

```
172.16.13.9 %any : PSK "My123Super456Secret789PSK"
```

Note: Using pre-shared keys for roadwarrior clients is not recommended since all the remote clients will be using the same pre-shared key.

If using X.509 certificates, you must define the RSA private key in the `/etc/ipsec.secrets` file as follows:

```
: RSA /etc/ipsec.d/private/myKey.pem "MyTopSecretPasswd"
```

In this example, the private keys were protected with the password 'MyTopSecretPasswd' earlier when creating a certificate request for the FreeS/WAN host as `CN=freeswan.kuo.ipsec.com`.

Note: If you want to use both a pre-shared key and X.509 certificates, your `/etc/ipsec.secrets` file must contain both of the above-mentioned definitions. Please refer to the FreeS/WAN documentation for more information on creating and setting up your private key in the `/etc/ipsec.secrets` file.

Now both the OpenSSL root CA certificate and FreeS/WAN host certificate and/or the private key have been installed properly.

1.6 Creating the Certificate for the SSH Sentinel Client

1. Create the key pair and the certification request with the following command. Use the remote user's e-mail address as the identity (in this example, `user1@kuo.ipsec.com`):

```
# cd /usr/share/ssl/misc/

# ./CA -newcert
Using configuration from /usr/share/ssl/openssl.cnf
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'newreq.pem'
```

```

Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:FI
State or Province Name (full name) [Berkshire]:Eastern Finland
Locality Name (eg, city) [Newbury]:Kuopio
Organization Name (eg, company) [My Company Ltd]:SSH Communications Security Corp
Organizational Unit Name (eg, section) []:SSH Sentinel staff
Common Name (eg, your name or your server's hostname) []:user1@kuo.ipsec.com
Email Address []:user1@kuo.ipsec.com
Certificate (and private key) is in newreq.pem

```

Since you will need the password later, make sure to memorize it.

2. Sign the certificate request with your OpenSSL root CA certificate:

```

# cd /usr/share/ssl/misc/

# ./CA -signcert
Cert passphrase will be requested twice - bug?
Getting request Private Key
Enter PEM pass phrase:
Generating certificate request
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
Check that the request matches the signature
Signature ok
The Subjects Distinguished Name is as follows
countryName           :PRINTABLE:'FI'
stateOrProvinceName   :PRINTABLE:'Eastern Finland'
localityName          :PRINTABLE:'Kuopio'
organizationName      :PRINTABLE:'SSH Communications Security Corp'
organizationalUnitName:PRINTABLE:'SSH Sentinel staff'
commonName            :T61STRING:'user1@kuo.ipsec.com'
emailAddress          :IA5STRING:'user1@kuo.ipsec.com'
Certificate is to be certified until Oct 10 07:40:49 2003 GMT (365 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y

```

Write out database with 1 new entries
Data Base Updated

[properties of your sentinel client certificate listed here]

Now we have a signed certificate for the remote user in a PEM-formatted file `newcert.pem`, and the private keys in a PEM-formatted and password-protected file `newreq.pem`.

3. Create a PKCS #12 formatted certificate package for the remote user.

Importing the client certificate into SSH Sentinel is very easy when the root CA certificate, the remote client certificate, and the private keys are packaged into a single, password-protected PKCS #12 file.

```
# cd /usr/share/ssl/misc/

# openssl pkcs12 \
    -export \
    -inkey newreq.pem \
    -in newcert.pem \
    -name "OpenSSL client certificate" \
    -certfile demoCA/cacert.pem \
    -caname "OpenSSL Root CA certificate" \
    -out pkcs12_certpack_for_user1.p12
Enter PEM pass phrase:
Enter Export Password:
Verifying password - Enter Export Password:

Export password used was 'MySecretExportPasswd'.
```

The PKCS #12 certificate package for the remote user can now be found in file `pkcs12_certpack_for_user1.p12`.

4. Deliver the PKCS #12 certificate package to the remote user.

Even though the PKCS #12 file is password-protected, the safest way to deliver the certificate file to the remote user is to use a secured scp file transfer (using, for example, SSH Secure Shell). Alternatively, consider using SSL-encrypted transfer via a https Web server, or perhaps a floppy disk.

Mount a (vfat) formatted floppy disk into the system and copy the PKCS #12 file into the floppy:

```
# cd /usr/share/ssl/misc/

# mount -t vfat /dev/fd0 /mnt/floppy

# cp pkcs12_certpack_for_user1.p12 /mnt/floppy/.

# umount /mnt/floppy
```

5. Configure FreeS/WAN for a strict CRL policy.

With the x509patch release v0.9.14 you can set FreeS/WAN to use a strict CRL policy. FreeS/WAN trusts remote client certificates only if the root CA certificate can be found from directory `/etc/ipsec.d/cacerts/`, and if the client certificate is valid and not revoked.

For older x509patch releases, you had to keep copies of the remote client certificates in the `/etc/ipsecd.d/` directory, but with the new strict CRL policy support that is no longer required. This makes administration of the FreeS/WAN gateway much easier and safe.

If your own OpenSSL-based CA was used to sign the certificates for both the FreeS/WAN host and SSH Sentinel remote clients, you just have to keep the OpenSSL root CA certificate in the `/etc/ipsec.d/cacerts/` directory, and the CRL file in the `/etc/ipsec.d/crls/` directory. (These files were already installed in previous steps in this example).

To configure the x509patched FreeS/WAN for a strict CRL policy, you must add the following parameter under the config setup section of the `/etc/ipsec.conf` config file:

```
config setup
    strictcrlpolicy=yes
```

Note: A valid Certificate Revocation List (CRL) file is very important now. Using the following command you can verify all the installed and valid certificates:

```
# /usr/local/sbin/ipsec auto --listall
```

1.7 Configuring FreeS/WAN for VPN Remote Clients

The FreeS/WAN VPN gateway must be configured to allow authenticated remote users to establish a virtual private connection to the private network protected by the gateway. Typically, the FreeS/WAN VPN gateway is configured for *roadwarrior* remote clients, that is, clients without a fixed IP address. Access is based on authentication and not the source IP address.

Please check Section 1.9 (FreeS/WAN Sample Configurations) for sample `/etc/ipsec.conf` configuration files, and Section 1.10 (Configuring SSH Sentinel) for SSH Sentinel VPN client settings.

1.8 Restarting the FreeS/WAN Gateway

FreeS/WAN IPsec must be restarted after reconfiguration. If AES support and `ipsec_aes` kernel module were used, the module must be removed before restarting FreeS/WAN.

```
# rmmod ipsec_aes
# service ipsec restart
# insmod ipsec_aes
```

1.9 FreeS/WAN Sample Configurations

All the following FreeS/WAN sample configurations are for a *roadwarrior* gateway usage (SSH Sentinel VPN remote client may connect to the gateway from any source IP address). In the sample configurations, the setting `remote network = any (0.0.0.0/0)` means that connection to other networks (such as the Internet) is not allowed simultaneously with the VPN tunnel.

It is also possible to open the VPN tunnel to the target network (for example, 192.168.1.0/24) and allow SSH Sentinel to connect to other networks, such as the Internet. In this case, set the SSH Sentinel remote network to 192.168.1.0/24, and in the FreeSWAN `/etc/ipsec.conf` file `leftsubnet=192.168.1.0/24`.

Note: Even if you set your remote network to something else than any (0.0.0.0/0), for example 192.168.1.0/24, you can efficiently deny all plain text traffic when the VPN tunnel is activated. After closing the VPN tunnel, the plain text traffic is routed normally. This feature improves security: even if the remote network is a subnet (like 192.168.1.0/24) and you are creating a VPN tunnel for the subnet only, you can deny all plain text traffic while using the tunnel. There is no chance of IP packets being routed from the Internet to the target private network over the VPN tunnel since the routing to the Internet is disabled when using the VPN tunnel. To do this, just select the option **Deny split tunneling** under the **Advanced** properties of the SSH Sentinel VPN rule.

Using X.509 certificates for authentication is strongly recommended, since using pre-shared key (PSK) based authentication with roadwarriors requires that all the remote users are using the same PSK. If your PSK leaks out to some intruder, your private LAN can be easily compromised. If you change the PSK, all the remote users must reconfigure their SSH Sentinel for an updated PSK.

When using certificates, a network administrator can just revoke a compromised certificate to prevent its use for a VPN connection. FreeS/WAN denies any remote client trying to authenticate with a revoked certificate. All the other users may use the connection without any interruption.

The following sample configurations are sorted by the virtual IP technique used: no virtual IP, DHCP over IPSec, and manual assignment. Every section has separate sample configurations for all the authentication (pre-shared keys vs. X.509 certificates) and encryption (3DES vs. AES) variants.

Virtual IP Technique	Authentication	Encryption
Not used	Pre-Shared Keys (1)	3DES
Not used	Pre-Shared Keys (1)	AES
Not used	Certificates	3DES
Not used	Certificates	AES
DHCP over IPSec (2)	Pre-Shared Keys (1)	3DES
DHCP over IPSec (2)	Pre-Shared Keys (1)	AES
DHCP over IPSec (2)	Certificates	3DES
DHCP over IPSec (2)	Certificates	AES
Manual (3)	Pre-Shared Keys (1)	3DES
Manual (3)	Pre-Shared Keys (1)	AES
Manual (3)	Certificates	3DES
Manual (3)	Certificates	AES

(1 Using pre-shared key based authentication in roadwarrior environments is not recommended, since all the remote users are using the same pre-shared key for authentication.

(2 Using DHCP over IPsec as a virtual IP solution makes the configuration of SSH Sentinel VPN remote clients very easy, but there is no method for assigning a certain virtual IP address for a certain remote user. All the virtual IP addresses are assigned from a dynamic pool of a private DHCP server. Thus, you cannot allow/reject traffic in your internal firewall coming from DHCP over IPsec remote clients based on the source IP address of the remote client.

(3 Assigning the virtual IP addresses manually allows a remote user to spoof his/hers manual virtual IP address. Nothing prevents the remote user from using an IP address that conflicts with an IP address reserved for some other remote user. However, when using X.509 certificates for authentication, it is possible to setup FreeS/WAN VPN connection profiles per remote user configured as roadwarrior usage and forcing the remote user to use the manual virtual IP address assigned to him/her by the network administrator. See the following configuration examples for more information.

Note: All the configurations using certificates are using the `strictcrlpolicy=yes` parameter. Remote client certificates are not stored in the FreeS/WAN host. Instead, the FreeS/WAN relies on the OpenSSL root CA certificate and all the remote client certificates issued by the root CA. Using this new feature requires that the Certificate Revocation List (CRL) is valid. You must update the CRL before it expires.

1.9.1 VPN Tunnel without Virtual IP Support

SSH Sentinel VPN remote client communicates with the private target remote network over a VPN tunnel using the IP address of the network adapter as the source address. The IP address of the FreeS/WAN private interface (typically eth1) must be used as a default gateway for the private network to route reply packets back to FreeS/WAN and the VPN tunnel.

Using Pre-Shared Keys and 3DES

Configuration:

- roadwarrior gateway
- authentication with pre-shared keys
- encryption with 3DES
- no Virtual IP support.

```
# /etc/ipsec.conf - FreeS/WAN IPsec configuration file

config setup
    interfaces=%defaultroute
```

```
klipsdebug=none
plutodebug=none
plutoload=%search
uniqueids=yes

conn %default
    keyingtries=1
    disablearrivalcheck=no
    authby=secret
    keyexchange=ike
    ikelifetime=240m
    keylife=60m
    pfs=yes
    compress=no
    left=%defaultroute
    auto=add

conn rw-psk-3des-novip
    type=tunnel
    right=%any
    # remote network for sentinel vpn rule:
    leftsubnet=0.0.0.0/0

# end of /etc/ipsec.conf
```

Using Pre-Shared Keys and AES

Configuration:

- roadwarrior gateway
 - authentication with pre-shared keys
 - encryption with AES
 - no Virtual IP support.
-

```
# /etc/ipsec.conf - FreeS/WAN IPsec configuration file

config setup
    interfaces=%defaultroute
    klipsdebug=none
    plutodebug=none
    plutoload=%search
    uniqueids=yes
```

```
conn %default
    keyingtries=1
    disablearrivalcheck=no
    authby=secret
    keyexchange=ike
    ikelifetime=240m
    keylife=60m
    pfs=yes
    compress=no
    left=%defaultroute
    auto=add

conn rw-psk-aes-novi
    type=tunnel
    right=%any
    auth=esp
    esp=aes128-md5
    ike=aes128-md5
    # remote network for sentinel vpn rule:
    leftsubnet=0.0.0.0/0

# end of /etc/ipsec.conf
```

Using Certificates and 3DES

Configuration:

- roadwarrior gateway
 - authentication with X.509 certificates
 - encryption with 3DES
 - no Virtual IP support.
-

```
# /etc/ipsec.conf - FreeS/WAN IPsec configuration file
```

```
config setup
    interfaces=%defaultroute
    klipsdebug=none
    plutodebug=none
    plutoload=%search
    uniqueids=yes
```

```
strictcrlpolicy=yes

conn %default
    keyingtries=1
    disablearrivalcheck=no
    authby=rsasig
    keyexchange=ike
    ikelifetime=240m
    keylife=60m
    pfs=yes
    compress=no
    right=%any
    rightrsasigkey=%cert
    left=%defaultroute
    leftcert=certs/myCert.pem
    auto=add

conn rw-cert-3des-novip
    type=tunnel
    right=%any
    # remote network for sentinel vpn rule:
    leftsubnet=0.0.0.0/0

# end of /etc/ipsec.conf
```

Using Certificates and AES

Configuration:

- roadwarrior gateway
 - authentication with X.509 certificates
 - encryption with AES
 - no Virtual IP support.
-

```
# /etc/ipsec.conf - FreeS/WAN IPsec configuration file
```

```
config setup
    interfaces=%defaultroute
    klipsdebug=none
    plutodebug=none
    plutoload=%search
    uniqueids=yes
```

```

    strictcrlpolicy=yes

conn %default
    disablearrivalcheck=no
    authby=rsasig
    keyexchange=ike
    ikelifetime=240m
    keylife=60m
    pfs=yes
    compress=no
    right=%any
    rightrsasigkey=%cert
    left=%defaultroute
    leftcert=certs/myCert.pem
    auto=add

conn rw-cert-aes-novip
    type=tunnel
    right=%any
    auth=esp
    esp=aes128-md5
    ike=aes128-md5
    # remote network for sentinel vpn rule:
    leftsubnet=0.0.0.0/0

# end of /etc/ipsec.conf

```

1.9.2 VPN Tunnel with Virtual IP Support: DHCP over IPsec

SSH Sentinel VPN remote client communicates with the private target remote network over a VPN tunnel using the dynamic IP address of the SSH Sentinel virtual adapter as the source address. The IP address comes from a private DHCP server. In the private network, the DHCP over IPsec virtual IP address scope must be routed to the IP address of the FreeS/WAN private interface (typically eth1). The default gateway of the private network may be some other router if required. After deploying the Virtual IP technique, you are no longer required to use your FreeS/WAN gateway as the default gateway.

DHCP requests are relayed from the SSH Sentinel VPN client to a private DHCP server by `dhcrelay` daemon. The target DHCP server used in these tests was DHCPd v2 by ISC, <http://www.isc.org/products/DHCP/>.

The used configuration file `/etc/dhcpd.conf` was:

```

# begin of /etc/dhcpd.conf -----
server-identifier my-private-dhcp-server;

```

```

#       IP address of eth0 interface in this DHCP server
#       is 192.168.1.41
#
#       IP address of private eth1 interface of FreeS/WAN
#       gateway is 192.168.1.67
#
#       DHCP-over-IPSec remote clients will get IP address
#       from scope 10.2.67.0/24 (range 10.2.67.2 - 10.2.67.253).
#
#       NOTE: DHCP service ports of this DHCP server are
#       closed by default. This DHCP server serves
#       DHCP-over-IPSec remote clients only.
#       Reconfigure ipchains/iptables firewall rules to
#       open or close DHCP ports 67-68/udp for a host.
#       Currently ports 6768/udp are opened only for
#       FreeS/WAN gateway 192.168.1.67 (for initial
#       DHCP request) as well as for DHCP-over-IPSec
#       Virtual IP address scope 10.2.67.0/24 (for
#       DHCP renew).

# Dummy empty scope to get dhcpd running:
subnet 192.168.1.41 netmask 255.255.255.255 {
}

shared-network SUBNET-10-2-67 {
    subnet 192.168.1.67 netmask 255.255.255.255 {
    }
    subnet 10.2.67.0 netmask 255.255.255.0 {
        range 10.2.67.2 10.2.67.253;
        default-lease-time 21600;           # 6 hours
        max-lease-time 43200;              # 12 hours
        option routers                      10.2.67.254;
        option broadcast-address            10.2.67.255;
        option subnet-mask                  255.255.255.0;
        option nis-domain                   "kuo.fi.ssh.com";
        option domain-name                  "kuo.fi.ssh.com";
        option domain-name-servers          10.2.3.11, 10.2.3.13;
        option netbios-name-servers         10.2.3.12, 10.2.3.14;
    }
}
# end of /etc/dhcpd.conf -----

```

The `dhcrelay` daemon must be launched during a system boot, for example by the `/etc/rc.d/rc.local` script. If the target DHCP server is located at IP address 192.168.1.41,

the FreeS/WAN virtual adapter used is ipsec0, and the private interface of FreeS/WAN is eth1, then the dhcprelay daemon could be launched as follows:

```
/usr/local/sbin/dhcprelay ipsec0 eth1 192.168.1.41
```

To auto-launch the daemon after a reboot, you can add it into the rc.local script as follows:

```
echo "/usr/local/sbin/dhcprelay ipsec0 eth1 192.168.1.41 \  
>> /var/log/dhcprelay.log &" >> /etc/rc.d/rc.local
```

The command line parameters of the dhcprelay daemon can also be set in the /usr/local/etc/dhcprelay.conf configuration file. For more details, please refer to the dhcprelay documentation at <http://www.strongsec.com/freeswan/dhcprelay>.

Using Pre-Shared Keys and 3DES

Configuration:

- roadwarrior gateway
 - authentication with pre-shared keys
 - encryption with 3DES
 - virtual IP support with DHCP over IPsec.
-

```
# /etc/ipsec.conf - FreeS/WAN IPsec configuration file
```

```
config setup  
    interfaces=%defaultroute  
    klipsdebug=none  
    plutodebug=none  
    plutoload=%search  
    uniqueids=yes
```

```
conn %default  
    keyingtries=1  
    disablearrivalcheck=no  
    authby=secret  
    keyexchange=ike  
    ikelifetime=240m  
    keylife=60m  
    pfs=yes
```

```
        compress=no
        left=%defaultroute
        auto=add

conn dhcp
    type=tunnel
    rekey=no
    ikelifetime=60s
    keylife=20s
    rekeymargin=10s
    right=%any
    leftsubnet=0.0.0.0/0
    leftprotoport=udp/bootps
    rightprotoport=udp/bootpc

conn rw-psk-3des-doi
    type=tunnel
    right=%any
    auth=esp
    # virtual ip address scope for sentinel remote clients:
    leftsubnet=0.0.0.0/0
    # remote network for sentinel vpn rule:
    rightsubnetwithin=10.2.67.0/24

# end of /etc/ipsec.conf
```

Using Pre-Shared Keys and AES

Configuration:

- roadwarrior gateway
 - authentication with pre-shared keys
 - encryption with AES
 - virtual IP support with DHCP over IPsec.
-

```
# /etc/ipsec.conf - FreeS/WAN IPsec configuration file
```

```
config setup
    interfaces=%defaultroute
    klipsdebug=none
    plutodebug=none
    plutoload=%search
```

```
uniqueids=yes

conn %default
    keyingtries=1
    disablearrivalcheck=no
    authby=secret
    keyexchange=ike
    ikelifetime=240m
    keylife=60m
    pfs=yes
    compress=no
    left=%defaultroute
    auto=add

conn dhcp
    type=tunnel
    rekey=no
    ikelifetime=60s
    keylife=20s
    rekeymargin=10s
    right=%any
    leftsubnet=0.0.0.0/0
    leftprotoport=udp/bootps
    rightprotoport=udp/bootpc
    auth=esp
    esp=aes128-md5
    ike=aes128-md5

conn rw-psk-3des-doi
    type=tunnel
    authby=secret
    right=%any
    auth=esp
    esp=aes128-md5
    ike=aes128-md5
    # remote network for sentinel vpn rule:
    leftsubnet=0.0.0.0/0
    # virtual ip address scope for sentinel remote clients:
    rightsubnetwithin=10.2.67.0/24

# end of /etc/ipsec.conf
```

Using Certificates and 3DES

Configuration:

- roadwarrior gateway
 - authentication with X.509 certificates
 - encryption with 3DES
 - virtual IP support with DHCP over IPsec.
-

```
# /etc/ipsec.conf - FreeS/WAN IPsec configuration file
```

```
config setup
    interfaces=%defaultroute
    klipsdebug=none
    plutodebug=none
    pluto_load=%search
    uniqueids=yes
    strictcrlpolicy=yes

conn %default
    keyingtries=1
    disablearrivalcheck=no
    authby=rsasig
    keyexchange=ike
    ikelifetime=240m
    keylife=60m
    pfs=yes
    compress=no
    right=%any
    rightrsasigkey=%cert
    left=%defaultroute
    leftcert=certs/myCert.pem
    auto=add

conn dhcp
    type=tunnel
    rekey=no
    ikelifetime=60s
    keylife=20s
    rekeymargin=10s
    right=%any
    leftsubnet=0.0.0.0/0
    leftprotoport=udp/bootps
```

```
rightprotoport=udp/bootpc

conn rw-cert-3des-doi
    type=tunnel
    right=%any
    right=%any
    # virtual ip address scope for sentinel remote clients:
    rightsubnetwithin=10.2.67.0/24
    # remote network for sentinel vpn rule:
    leftsubnet=0.0.0.0/0

# end of /etc/ipsec.conf
```

Using Certificates and AES

Configuration:

- roadwarrior gateway
 - authentication with X.509 certificates
 - encryption with AES
 - virtual IP support with DHCP over IPsec.
-

```
# /etc/ipsec.conf - FreeS/WAN IPsec configuration file
```

```
config setup
    interfaces=%defaulttroute
    klipsdebug=none
    plutodebug=none
    plutoload=%search
    uniqueids=yes
    strictcrlpolicy=yes
```

```
conn %default
    keyingtries=1
    disablearrivalcheck=no
    authby=rsasig
    keyexchange=ike
    ikelifetime=240m
    keylife=60m
    pfs=yes
    compress=no
    right=%any
```

```
    rightrsasigkey=%cert
    left=%defaultroute
    leftcert=certs/myCert.pem
    auto=add

conn dhcp
    type=tunnel
    rekey=no
    ikelifetime=60s
    keylife=20s
    rekeymargin=10s
    right=%any
    leftsubnet=0.0.0.0/0
    leftprotoport=udp/bootps
    rightprotoport=udp/bootpc
    auth=esp
    esp=aes128-md5
    ike=aes128-md5

conn rw-cert-3des-doi
    type=tunnel
    right=%any
    auth=esp
    esp=aes128-md5
    ike=aes128-md5
    # virtual ip address scope for sentinel remote clients:
    rightsubnetwithin=10.2.67.0/24
    # remote network for sentinel vpn rule:
    leftsubnet=0.0.0.0/0

# end of /etc/ipsec.conf
```

1.9.3 VPN Tunnel with Virtual IP Support: Manual Assignment

SSH Sentinel VPN remote client communicates with the private target remote network over a VPN tunnel using the static IP address of the SSH Sentinel virtual adapter as the source address. The IP address is manually set for the VPN rule. In the private network, the manual IP address scope must be routed to the IP address of the FreeS/WAN private interface (typically eth1). The default gateway of the private network may be some other router if required. After deploying the virtual IP technique, you are not required to use your FreeS/WAN gateway as a default gateway.

Using Pre-Shared Keys and 3DES

Configuration:

- roadwarrior gateway
- authentication with pre-shared keys
- encryption with 3DES
- virtual IP support with a manually set virtual IP address.

```
# /etc/ipsec.conf - FreeS/WAN IPsec configuration file

config setup
    interfaces=%defaultroute
    klipsdebug=none
    plutodebug=none
    plutoload=%search
    uniqueids=yes

conn %default
    keyingtries=1
    disablearrivalcheck=no
    authby=secret
    keyexchange=ike
    ikelifetime=240m
    keylife=60m
    pfs=yes
    compress=no
    left=%defaultroute
    auto=add

conn rw-psk-3des-manual
    type=tunnel
    right=%any
    # remote network for sentinel vpn rule:
    leftsubnet=0.0.0.0/0
    # virtual ip address scope for sentinel remote clients:
    rightsubnetwithin=10.2.67.0/24

# end of /etc/ipsec.conf
```

To prevent IP conflicts between remote clients, you must maintain good documentation about the manually assigned virtual IP addresses. It is important to remember that nothing prevents the remote users from setting

conflicting IP addresses in their SSH Sentinel VPN rules. You cannot trust that a virtual IP source address is used only by one particular remote user. Then you cannot allow or reject traffic in an internal firewall based on the virtual IP address used, because the source IP address and the certificate used for authentication are not linked.

In the FreeS/WAN end, you can use VPN connection profiles per remote user instead of the generic roadwarrior profile introduced above. Unfortunately when using PSK authentication, all the remote users are using the same PSK. To effectively force a remote client to use a specified manual virtual IP address, the remote client should have a static IP address and you should declare a VPN connection profile for FreeS/WAN per remote IP address instead of the roadwarrior configuration. Please refer to the FreeS/WAN and x509patch documentation for more details.

Using Pre-Shared Keys and AES

Configuration:

- roadwarrior gateway
 - authentication with pre-shared keys
 - encryption with AES
 - virtual IP support with a manually set virtual IP address.
-

```
# /etc/ipsec.conf - FreeS/WAN IPsec configuration file
```

```
config setup
    interfaces=%defaultroute
    klipsdebug=none
    plutodebug=none
    plutoload=%search
    uniqueids=yes
```

```
conn %default
    keyingtries=1
    disablearrivalcheck=no
    authby=secret
    keyexchange=ike
    ikelifetime=240m
    keylife=60m
    pfs=yes
    compress=no
    left=%defaultroute
    auto=add
```

```
conn rw-psk-aes-manual
    type=tunnel
    right=%any
    auth=esp
    esp=aes128-md5
    ike=aes128-md5
    # remote network for sentinel vpn rule:
    leftsubnet=0.0.0.0/0
    # virtual ip address scope for sentinel remote clients:
    rightsubnetwithin=10.2.67.0/24

# end of /etc/ipsec.conf
```

Using Certificates and 3DES

Configuration:

- roadwarrior gateway
 - authentication with X.509 certificates
 - encryption with 3DES
 - virtual IP support with a manually set virtual IP address.
-

```
# /etc/ipsec.conf - FreeS/WAN IPsec configuration file
```

```
config setup
    interfaces=%defaulttroute
    klipsdebug=none
    plutodebug=none
    plutoload=%search
    uniqueids=yes
```

```
conn %default
    keyingtries=1
    disablearrivalcheck=no
    authby=rsasig
    keyexchange=ike
    ikelifetime=240m
    keylife=60m
    pfs=yes
    compress=no
    right=%any
    rightrsasigkey=%cert
```

```

    left=%defaultroute
    leftcert=certs/myCert.pem
    auto=add

conn rw-cert-3des-manual
    type=tunnel
    right=%any
    # virtual ip address scope for sentinel remote clients:
    rightsubnetwithin=10.2.67.0/24
    # remote network for sentinel vpn rule:
    leftsubnet=0.0.0.0/0

# end of /etc/ipsec.conf

```

To prevent IP conflicts between remote clients, you must maintain good documentation about the manually assigned virtual IP addresses. It is important to remember that nothing prevents the remote users from setting conflicting IP addresses in their SSH Sentinel VPN rules. You cannot trust that a virtual IP source address is used only by one particular remote user. Then you cannot allow or reject traffic in an internal firewall based on the virtual IP address used, because the source IP address and the certificate used for authentication are not linked.

In the FreeS/WAN end, you can use VPN connection profiles per remote user instead of the generic roadwarrior profile introduced above. When using X.509 certificates for authentication, you can create a roadwarrior-style FreeS/WAN VPN connection profile per a remote user, and force a remote user to use a particular manually assigned virtual IP address with his/hers certificate. If the remote user tries spoofing the virtual IP address assigned for him, the IPsec SA negotiation fails and the remote user is not able to communicate, even with a valid certificate. In this case your `/etc/ipsec.conf` configuration could look like follows:

```

# /etc/ipsec.conf - FreeS/WAN IPsec configuration file

config setup
    interfaces=%defaultroute
    klipsdebug=none
    plutodebug=none
    plutoload=%search
    uniqueids=yes
    strictcrlpolicy=yes

conn %default
    keyingtries=1
    disablearrivalcheck=no
    authby=rsasig
    keyexchange=ike
    ikelifetime=240m
    keylife=60m

```

```
pfs=yes
compress=no
right=%any
rightrsasigkey=%cert
left=%defaulttroute
leftcert=certs/myCert.pem
auto=add

conn rw-psk-3des-manual-for-user1
    type=tunnel
    # connections allowed from any source IP address:
    right=%any
    # remote network for sentinel vpn rule:
    leftsubnet=0.0.0.0/0
    # this virtual ip address for sentinel remote user1:
    rightsubnet=10.2.67.201/32
    # ... and it can be used only with this certificate:
    rightid="C=FI, ST=Eastern Finland, L=Kuopio, O=SSH
    Communications Security Corp, OU=SSH Sentinel Team,
    CN=user1@kuo.ipsec.com, E=user1@kuo.ipsec.com

conn rw-psk-3des-manual-for-user2
    type=tunnel
    # connections allowed from any source IP address:
    right=%any
    # remote network for sentinel vpn rule:
    leftsubnet=0.0.0.0/0
    # this virtual ip address for sentinel remote user2:
    rightsubnet=10.2.67.202/32
    # ... and it can be used only with this certificate:
    rightid="C=FI, ST=Eastern Finland, L=Kuopio, O=SSH
    Communications Security Corp, OU=SSH Sentinel Team,
    CN=user2@kuo.ipsec.com, E=user2@kuo.ipsec.com"

conn rw-psk-3des-manual-for-user3
    type=tunnel
    # connections allowed from any source IP address:
    # remote network for sentinel vpn rule:
    leftsubnet=0.0.0.0/0
    # this virtual ip address for sentinel remote user3:
    rightsubnet=10.2.67.203/32
    # ... and it can be used only with this certificate:
    rightid="C=FI, ST=Eastern Finland, L=Kuopio, O=SSH
    Communications Security Corp, OU=SSH Sentinel Team,
    CN=user3@kuo.ipsec.com, E=user3@kuo.ipsec.com"
```

```
# end of /etc/ipsec.conf
```

Using Certificates and AES

Configuration:

- roadwarrior gateway
 - authentication with X.509 certificates
 - encryption with AES
 - virtual IP support with a manually set virtual IP address.
-

```
# /etc/ipsec.conf - FreeS/WAN IPsec configuration file
```

```
config setup
    interfaces=%defaultroute
    klipsdebug=none
    plutodebug=none
    plutoload=%search
    uniqueids=yes
    strictcrlpolicy=yes

conn %default
    keyingtries=1
    disablearrivalcheck=no
    authby=rsasig
    keyexchange=ike
    ikelifetime=240m
    keylife=60m
    pfs=yes
    compress=no
    right=%any
    rightrsasigkey=%cert
    left=%defaultroute
    leftcert=certs/myCert.pem
    auto=add

conn rw-cert-aes-manual
    type=tunnel
    right=%any
    auth=esp
    esp=aes128-md5
```

```
ike=aes128-md5
# remote network for sentinel vpn rule:
leftsubnet=0.0.0.0/0
# virtual ip address scope for sentinel remote clients:
rightsubnetwithin=10.2.67.0/24
```

```
# end of /etc/ipsec.conf
```

Note: Nothing prevents a remote user from spoofing his/her manual virtual IP address for the SSH Sentinel VPN rule, and using a conflicting IP address. Check the previous `rw-cert-3des-manual` example for more information. In this case, the FreeS/WAN `/etc/ipsec.conf` could be:

```
# /etc/ipsec.conf - FreeS/WAN IPsec configuration file
```

```
config setup
```

```
interfaces=%defaultroute
klipsdebug=none
plutodebug=none
plutoload=%search
uniqueids=yes
strictcrlpolicy=yes
```

```
conn %default
```

```
keyingtries=1
disablearrivalcheck=no
authby=rsasig
keyexchange=ike
ikelifetime=240m
keylife=60m
pfs=yes
compress=no
right=%any
rightrsasigkey=%cert
left=%defaultroute
leftcert=certs/myCert.pem
auto=add
```

```
conn rw-psk-aes-manual-for-user1
```

```
type=tunnel
# connections allowed from any source IP address:
right=%any
auth=esp
esp=aes128-md5
ike=aes128-md5
# remote network for sentinel vpn rule:
```

```
leftsubnet=0.0.0.0/0
# this virtual ip address for sentinel remote user1:
rightsubnet=10.2.67.201/32
# ... and it can be used only with this certificate:
rightid="C=FI, ST=Eastern Finland, L=Kuopio, O=SSH
Communications Security Corp, OU=SSH Sentinel Team,
CN=user1@kuo.ipsec.com, E=user1@kuo.ipsec.com"

conn rw-psk-aes-manual-for-user2
    type=tunnel
    # connections allowed from any source IP address:
    right=%any
    auth=esp
    esp=aes128-md5
    ike=aes128-md5
    # remote network for sentinel vpn rule:
    leftsubnet=0.0.0.0/0
    # this virtual ip address for sentinel remote user1:
    rightsubnet=10.2.67.202/32
    # ... and it can be used only with this certificate:
    rightid="C=FI, ST=Eastern Finland, L=Kuopio, O=SSH
Communications Security Corp, OU=SSH Sentinel Team,
CN=user2@kuo.ipsec.com, E=user2@kuo.ipsec.com"

conn rw-psk-aes-manual-for-user3
    type=tunnel
    # connections allowed from any source IP address:
    right=%any
    auth=esp
    esp=aes128-md5
    ike=aes128-md5
    # remote network for sentinel vpn rule:
    leftsubnet=0.0.0.0/0
    # this virtual ip address for sentinel remote user1:
    rightsubnet=10.2.67.203/32
    # ... and it can be used only with this certificate:
    rightid="C=FI, ST=Eastern Finland, L=Kuopio, O=SSH
Communications Security Corp, OU=SSH Sentinel Team,
CN=user3@kuo.ipsec.com, E=user3@kuo.ipsec.com"

# end of /etc/ipsec.conf
```

1.10 Configuring SSH Sentinel

The following summarizes the steps required to add the essential SSH Sentinel connection rules. For complete instructions on how to handle the rules, refer to the SSH Sentinel User Manual.

1.10.1 Creating the Authentication Key

First you must either declare the pre-shared key, or import a PKCS #12 formatted X.509 certificate package to be used for authenticating the VPN tunnel.

To add a new pre-shared key, launch SSH Sentinel Policy Editor. On the **Key Management** page, select **My Keys** and click the **Add** button. Select the **Create a pre-shared key** option.

To import a PKCS #12 formatted certificate package, on the **Key Management** page, select **My Keys**, right-click and select **Import**. Select PKCS #12 certificate files (`*.pfx`, `*.p12`) as **Files of type**. You must enter a password to open the PKCS #12 file for importing. The password is the one created earlier while creating the PKCS #12 file.

Finally, click **Apply** to save the changes into the SSH Sentinel Policy Manager database.

1.10.2 Creating the VPN Rule

In the following, setting remote network to any (`0.0.0.0/0`) means that connection to other networks (such as the Internet) is not allowed simultaneously with the VPN tunnel.

It is also possible to open the VPN tunnel to the target network (for example, `192.168.1.0/24`) and allow SSH Sentinel to connect to other networks, such as the Internet. In this case, set the SSH Sentinel remote network to `192.168.1.0/24`, and in the `FreeS/WAN/etc/ipsec.conf` file `leftsubnet=192.168.1.0/24`.

Note: Even if you set your remote network to something else than any (`0.0.0.0/0`), for example `192.168.1.0/24`, you can efficiently deny all plain text traffic when the VPN tunnel is activated. After closing the VPN tunnel, the plain text traffic is routed normally. This feature improves security: even if the remote network is a subnet (like `192.168.1.0/24`) and you are creating a VPN tunnel for the subnet only, you can deny all plain text traffic while using the tunnel. There is no chance of IP packets being routed from the Internet to the target private network over the VPN tunnel since the routing to the Internet is disabled when using the VPN tunnel. To do this, just select the option **Deny split tunneling** under the **Advanced** properties of the SSH Sentinel VPN rule.

To create a virtual private network connection to the private network protected by the FreeS/WAN gateway, do the following:

1. On the **Security Policy** page of the Policy Editor, select **VPN Connections**, and click **Add**.
2. On the **Add VPN Connection** dialog box, specify the following settings:

- Security gateway: the domain name or the IP address of the FreeS/WAN gateway. Shift between the two with the **IP** button.
- Remote network: any (0.0.0.0/0).
- Authentication key: the FreeS/WAN authentication key (a pre-shared key or a X.509 certificate).
- Select **legacy** as the proposal template when using 3DES for encryption, and **normal** when using AES (Rijndael).
- Click **Properties** to specify more properties.
- Select the **Acquire virtual IP address** check box when virtual IP addressing is used. Click **Settings...** and select **Dynamic Host Configuration Protocol (DHCP) over IPSec** or **Specify manually**. Select **Specify DNS and WINS servers** to specify the IP addresses of (private) DNS and WINS name servers being used when the VPN tunnel is active.

If using manual virtual IP addressing, we recommend using a 24-bit netmask for the virtual IP address; for example 10.2.67.201/24 (equals to 10.2.67.201/255.255.255.0).

Note: When deploying virtual IP addressing with DHCP over IPSec, there is no need to specify the IP addresses of the name servers manually. The private DHCP server can set up the DNS and WINS servers for SSH Sentinel. The sample `dhcpd.conf` configuration file in Section 1.9.2 (VPN Tunnel with Virtual IP Support: DHCP over IPSec) shows how to set up the IP addresses of the servers.

- Do not select **Extended authentication** since FreeS/WAN does not currently support it.

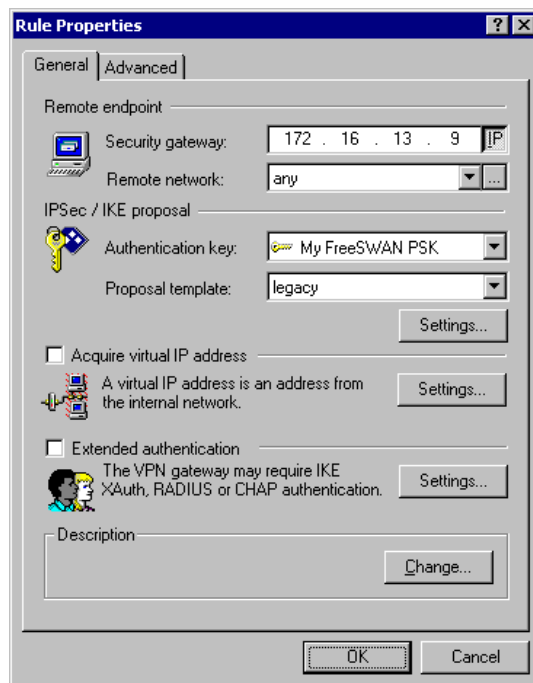


Figure 1.2: The general properties of the VPN connection

3. On the **Rule properties** dialog box, under **IPSec/IKE proposal**, click **Settings...** to specify the following:

- IKE proposal
 - Encryption algorithm: 3DES
 - Integrity function: MD5
 - IKE mode: main mode
 - IKE group: MODP 1024 (group 2).
 - IPSec proposal
 - Encryption algorithm: 3DES
 - Integrity function: HMAC-MD5
 - IPSec mode: tunnel
 - PFS group: MODP 1024 (group 2).
4. On the **Advanced** page, the default values for **Security association lifetimes** should be OK.
- In addition, select the options as shown in Figure 1.3 (The advanced properties of the VPN connection).

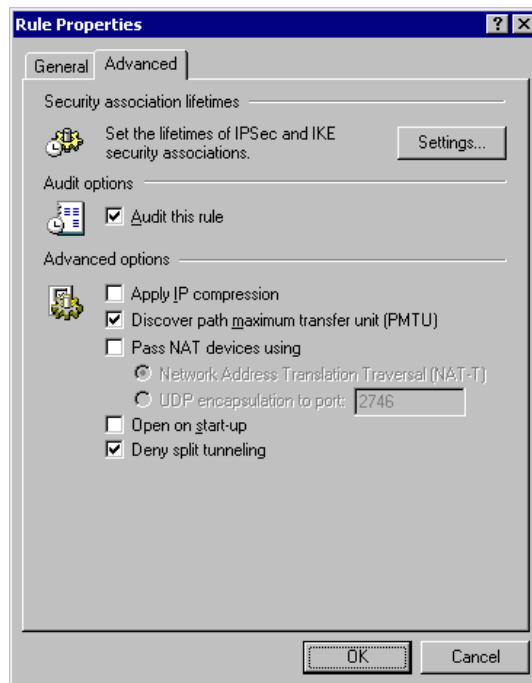


Figure 1.3: The advanced properties of the VPN connection

Select **Open on start-up** if you want the VPN tunnel to be activated automatically after a reboot. The **Apply IP compression** option requires option `compress=yes` for FreeS/WAN as well. The benefit of IP compression depends on the bandwidth available, as well as on the CPU power at both ends of the VPN tunnel. Generally, IP compression is useful only if you have fast machines for the SSH Sentinel VPN client and for FreeS/WAN VPN gateway, but low bandwidth between them (like 28.8 kbit/s modem or a GPRS connection).

5. Once ready, click the **OK** button to add the rule. On Policy Editor, click **Apply** to save your changes.

Testing the Connection

To test that the connection can be established and to verify that the data packets are encrypted, select your VPN rule under **VPN Connections** and click **Diagnostics**.

If Diagnostics succeeds, you will see **Diagnostics complete** display.

If Diagnostics fails, you will see an error message (and more details if the **Details** option was selected).

Opening the VPN Tunnel

You can open the VPN tunnel either via the SSH Sentinel tray icon (**Select VPN** -> your VPN rule), or you can enable **Open on start-up** under the **Advanced** properties of the VPN rule to open the VPN tunnel automatically when the system reboots.

For more information on using VPN tunnels with SSH Sentinel, please refer to the SSH Sentinel User Manual.

1.11 Troubleshooting

1.11.1 FreeS/WAN IPSec Gateway

1. Check the system log files. Typically, you find them at `/var/log/secure` and `/var/log/messages`.
2. Check the FreeS/WAN barf output:

```
# /usr/local/sbin/ipsec barf | more
```

3. Kernel parameter `rp_filter` must be set to '0' for the interface used by FreeS/WAN. If your default gateway is found via `eth0` and FreeS/WAN is configured to bind itself to that interface, you must set `rp_filter=0` for the `eth0` interface.

To check the status of the parameter, enter the following command:

```
# cat /proc/sys/net/ipv4/conf/eth0/rp_filter
0
```

If `rp_filter=1`, then you can reset it with the following command:

```
# echo 0 > /proc/sys/net/ipv4/conf/eth0/rp_filter
```

If your Linux distribution uses the `sysctl` utility to initialize kernel parameters, you may want to edit the `/etc/sysctl.conf` configuration file to do it automatically. For more information, please check the FreeS/WAN documentation.

-
4. Kernel parameter `ip_forward` must be set to '1':
-

```
# cat /proc/sys/net/ipv4/ip_forward
1
```

If `ip_forward=0`, then you must enable IP forwarding with the following command:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Typically that parameter is set via the `sysctl` command. For Red Hat Linux you must edit the `/etc/sysctl.conf` configuration file. For more information, please check the FreeS/WAN documentation.

5. If a SA comes up, you can ping the IP address of the private LAN interface of the FreeS/WAN host (typically `eth1`). If you cannot ping any other host in the private network, you have a routing problem in your private network. The FreeS/WAN host must route packets targeted to your private network IP subnet via its private LAN interface (`eth1`), and in addition, sometimes also via static routes directed to some other router(s) located in your private network.

Note: Reply packets from the hosts of your private network to the SSH Sentinel clients must be routed back to the private interface (`eth1`) of your FreeS/WAN gateway. Virtual IP technique helps you solve routing problems in a private network environment when your FreeS/WAN VPN gateway is not used as a default gateway for the hosts in the private network. Without virtual IP technique, the reply packets are typically routed out via your default gateway and not via the FreeS/WAN VPN gateway.

If `eth0` is your public interface, FreeS/WAN is binded to the interface with its virtual adapter `ipsec0`, and `eth1` is the interface to your private network, then you can use

- `tcpdump -i eth0` to diagnose the ISAKMP and ESP traffic between the SSH Sentinel VPN client and FreeS/WAN VPN gateway.
- `tcpdump -i ipsec0` to diagnose tunneled plain text traffic inside the VPN tunnel between the SSH Sentinel VPN client and FreeS/WAN VPN gateway.
- `tcpdump -i eth1` to diagnose clear text traffic between SSH Sentinel VPN remote client and a target host in private network.

6. If the routing works but the FreeS/WAN host just does not forward packets, check your `ipchains/iptables` firewalling rules:

- `eth0` interface: You must allow ISAKMP traffic (UDP, protocol 17, port 500) as well as ESP traffic (protocol 50) for both INPUT and OUTPUT rule chains. Depending on your needs and other usage of the FreeS/WAN gateway, you may want to close all other TCP/UDP ports.
- IP forwarding: Allow IP forwarding between the SSH Sentinel remote client and your target private network. If virtual IP technique is used, the source IP address of SSH Sentinel VPN remote clients is allocated from a subnet that you select to be used. In our FreeS/WAN sample configuration, `10.2.67.0/24` was used for virtual IP addressing. In this case, you need to allow IP forwarding between the `10.2.67.0/24` remote client subnet and your private network (for example, `192.168.1.0/24`) in the FORWARD rule chain.

If virtual IP technique was not used, the source IP address of SSH Sentinel VPN client may be anything. You must now allow IP forwarding from `0.0.0.0/0` (any) subnet to your private network subnet (for example, `192.168.1.0/24`).

7. When deploying X.509 certificates you can check your certificates, keys, and Certificate Revocation List (CRL) using the following command:

```
# /usr/local/sbin/ipsec auto --listall | more
```

8. The original FreeS/WAN does **not** support X.509 certificates. For X.509 certificate patch related problems check <http://www.strongsec.com/freeswan/> and FreeS/WAN mailing lists.
9. The original FreeS/WAN does **not** support AES/Rijndael encryption. For also patch related problems check <http://www.irrigacion.gov.ar/juanjo/ipsec/> and FreeS/WAN mailing lists.
10. The original FreeS/WAN does **not** support DHCP overIPSec. When deploying it and encountering problems with the `dhcprelay` daemon, check <http://www.strongsec.com/freeswan/dhcprelay/> and FreeS/WAN mailing lists.
11. The original FreeS/WAN does **not** support Delete SA Notifications. For patch related problems check <http://open-source-arkoon.net/> and FreeS/WAN mailing lists.
12. If there is a Network Address Translation (NAT) router between the SSH Sentinel VPN client and the FreeS/WAN gateway, the NAT router must support IPSec pass-through or you must deploy a NAT-T patch for your FreeS/WAN installation and enable NAT-T support for your SSH Sentinel VPN rule (select the VPN connection, click **Properties**, on the **Advanced** page select **Pass NAT devices using** and **Network Address Translation Traversal (NAT-T)**. The NAT-T patch is available at <http://open-source.arkoon.net/>.

In any other FreeS/WAN related problems, read the documentation and mailing list archive at <http://www.freeswan.org> .

1.11.2 SSH Sentinel

1. Check the proposal parameters of the VPN rule. They must match the proposal parameters used in your FreeS/WAN configuration.
2. On the **Key Management** page of the Policy Manager under **My Keys**, check your pre-shared key or the validity of your X.509 certificate.
3. On the **Key Management** page under **Trust Policy -> Trusted Certificates -> Certification Authorities**, check that the trusted root CA certificate issuing your client certificate has been installed and is valid. Under **Certificate Properties** you must have options **Trust in certification path verification** and **Accept connections authenticated with a certificate issued by this CA** selected for the CA certificate.
4. Enable IKE logging via the SSH Sentinel tray icon. Select **Auditing -> View IKE Log Window** and set **IPSec/IKE logging** to **Detailed**, and check the log after trying to open the VPN connection.
5. Open **Auditing -> View Audit Log** via the SSH Sentinel tray icon to check possible Pre-IPSec and/or Post-IPSec Filter traps if auditing the filtering rules.

6. Read the SSH Sentinel v1.4 User Manual and all the related documentation. You can find them from <http://www.ssh.com/support/documentation/all/sentinel/1.4/>.
7. Check the latest information from the SSH Sentinel support pages at <http://www.ssh.com/support/products/sentinel/>.
8. Contact SSH Sentinel support by filling the feedback forms at <http://www.ssh.com/support/products/sentinel/>, or e-mail directly to sentinel-support@ssh.com.

Please note that the more exact request you write, the better chance our technical support staff has to resolve your problem. A good request includes all the necessary information about your networking scenario (a ASCII drawing preferred, but .gif/.jpg formatted graphics are suitable too), the configurations used for both the VPN client and the gateway, error messages and/or log files, and a description of what you are trying to do.