

## SonicWALL VPN with FreeS/WAN using IKE

Prepared by SonicWALL, Inc.

09/09/2002

### Introduction:

VPN standards are still evolving and interoperability between products is a continued effort. SonicWALL has made progress in this area and is interoperable with the open source Linux VPN client FreeS/WAN using IKE as shown below.

This technote assumes the reader has a working knowledge of Linux and SonicWALL appliance configuration. This tech-note describes the required steps to set-up a compatible Security Association on both FreeS/WAN and SonicWALL products.

### Technical Notes:

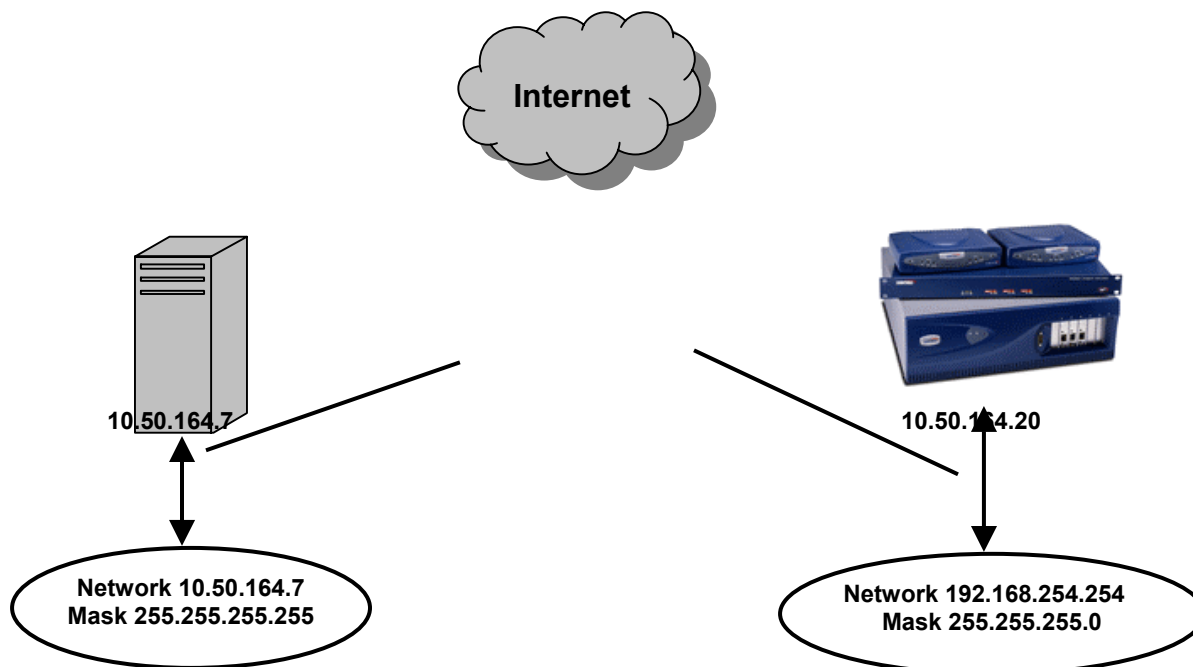
SonicWALL has tested VPN interoperability with an x86-based system running FreeS/WAN version 1.94 and a SonicWALL Pro 300 version 6.3.1.4, using the following VPN Security Association information:

- Keying Mode: IKE
- IKE Mode: Main Mode with PFS (perfect forward secrecy)
- SA Authentication Method: Pre-Shared key
- Keying Group: DH (Diffie-Hellman) Group 2
- Encryption and Data Integrity: ESP 3DES with MD5

Free S/WAN currently does NOT support Aggressive Mode, as its developers are not convinced of the security of Aggressive Mode IKE. Therefore Aggressive Mode has not been tested.

### Example:

The network configuration shown below is used in the example VPN configuration. The example will configure a VPN using 3DES encryption with MD5 and with PFS.



## SonicWALL Configuration

1. On the SonicWALL, create an SA
2. Change the IPsec Keying Mode to IKE using pre-shared secret
3. Name your SA. (In this example TestFreeS-WAN)
4. Fill in the IPsec gateway (in this example 10.50.164.7)
5. Select Group 2 for Phase 1 DH Group
6. Select 3DES & MD5 for Phase 1 Encryption/Authentication
7. Select ESP 3DES HMAC MD5 for Phase 2 Encryption/Authentication
8. Enter your Shared Secret (In this example MySharedSecret)
9. Fill in the appropriate Destination Network (in this example 10.50.164.7) and Subnet Mask (in this example 255.255.255.255)
10. A Sample Screen shot from SonicWALL firmware version 6.3.1.4 is displayed below

The screenshot shows the SonicWALL VPN configuration interface for IPsec Security Associations. The interface is divided into several sections: Summary, Configure, Authentication Service, Local Certificates, and CA Certificates. The main configuration area is titled "Add/Modify IPsec Security Associations".

**Add/Modify IPsec Security Associations**

Security Association: TestFreeS-WAN  
IPsec Keying Mode: IKE using Preshared Secret  
Name: TestFreeS-WAN  
Disable This SA:   
IPsec Gateway Address: 10.50.164.7

**Security policy**

Phase 1 DH Group: Group 2  
SA Life time (secs): 28800  
Phase 1 Encryption/Authentication: 3DES & MD5  
Phase 2 Encryption/Authentication: Strong Encrypt and Authenticate (ESP 3DES HMAC MD5)  
Shared Secret: MySharedSecret

**Destination Networks**

Use this SA as default route for all Internet traffic  
 Destination network obtains IP addresses using DHCP through this SA  
 Specify destination networks below

Network	Subnet Mask		
10.50.164.7	255.255.255.255		

Add New Network...  
Advanced Settings...  
Delete This SA

Update Reset

## SonicWALL VPN with Free-S/WAN using IKE

1. Click on Advanced Settings
2. Select Group 2 for Phase 2 DH Group
3. Click OK
4. Click Update
5. A sample screen shot from SonicWALL firmware version 6.3.1.4 is displayed below

**Edit Advanced Settings**

Use Aggressive Mode

Enable Keep Alive

Require authentication of local users

Require authentication of remote users

Remote users behind VPN gateway  
 Remote VPN clients with XAUTH

Enable Windows Networking (NetBIOS) broadcast

Apply NAT and firewall rules

Forward packets to remote VPNs

Enable Perfect Forward Secrecy

Phase 2 DH Group

Default LAN Gateway

VPN Terminated at  LAN  DMZ  LAN/DMZ

OK Cancel

*Note that after clicking OK, you must click Update on the main page to save changes made here.*

## Free-S/WAN Configuration

First configure the Linux machine as normal. Then make sure the FreeS/WAN client has been installed correctly.

Below you will find the configuration files as used in this test. There is not much else to configure except perhaps the internal firewall (ipchains, netfilter, etc).

The test was performed with a Red Hat 7.1 distribution Linux and the FreeS/WAN RPM distribution for Red Hat version 1.94.

The /etc/ipsec.conf should look like this:

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

# setup for SonicWALL interop

# basic configuration
config setup
    interfaces=%defaultroute
    # %defaultroute will suffice in the vast majority of setups
    klipsdebug=none
    plutodebug=none
    plutoload=%search
    plutostart=%search
    # This will close existing SA's if a new one with the same ID comes in.
    uniqueids=yes

conn TestFreeS-WAN
    # Left security gateway, subnet behind it, next hop toward right.
    left=%defaultroute
    # %defaultroute will suffice in the vast majority of setups
    # Right security gateway, subnet behind it, next hop toward right.
    right=10.50.164.20
    rightsubnet=192.168.254.0/24
    keyingtries=0
    auto=route
    auth=esp
    esp=3des-hmac-md5
    authby=secret
```

The /etc/ipsec.secrets should look like this:

```
# This file holds shared secrets or RSA private keys for inter-Pluto
# authentication. See ipsec_pluto(8) manpage, and HTML documentation.

10.50.164.7 10.50.164.20 @0040100E633A : PSK "MySharedSecret"
```

The IP addresses used are the IPsec gateway IP's. The serial number as it appears behind the @ sign is actually the Unique Firewall Identifier as set in the VPN General screen. PSK stands for Pre-Shared Key.

Please note that both Pre-Shared Key and UFI are case-sensitive, and that the UFI cannot contain spaces. Also note that in the 'ipsec.conf' file indentation is very important. Only items with the same indent are considered part of the same section.