



about me | linux
album | my

This document describes how to get [Openswan](#) working with various other IPsec stacks, including Openswan and Windows 2000/XP. If you have any difficulties with this process, please e-mail the [Openswan mailing list](#), or if you can't get help from there, e-mail me at: ipsec@natecarlson.com. Also you'd like an alternate way of doing this (IPsec with L2TP), see [Jacco de Leeuw's page](#).

IMPORTANT NOTE: On March 1, 2004, the FreeS/WAN maintainers announced that the FreeS/WAN project is ending, for many reasons. The [Openswan project](#) is going to be taking over development. Openswan is based on Super FreeS/WAN, and already includes most of the patches that people wanted updated these directions to use examples for Openswan 2.1.2; they should still run as-is on FreeS/WAN with the X.509 patches, and will work with FreeS/WAN 1.99+X.509 and Openswan 1 with some minor modifications. They should also work as-is with Strongswan. I no longer cover patching FreeS/WAN X.509; if you are going to start with a base FreeS/WAN installation, you will need to follow the directions <http://www.strongsec.com/freeswan> on how to patch it.

IMPORTANT NOTE #2: As of June 17 2004, this document has been updated to reflect Openswan configuration instead of FreeS/WAN. I've also reorganized a few things; hopefully it will flow better. Please let me know if you run into any problems with the new configuration. If you need it, the old page is available at: <http://www.natecarlson.com/linux/ipsec-x509-fs1.php>.

Contents:

[Changes made to this document](#)
[Setting up a Certificate Authority](#)
[Generating a Certificate](#)
[Installing Openswan](#)
[Installing the Certificate on your Gateway](#)
[Configuring Openswan on the Gateway Machine](#)
[Client Setup: Openswan](#)
[Client Setup: Windows 2000/XP with ipsec.exe](#)
[Some common errors, and resolutions for them](#)
[References used to write this document](#)

Changes made to this document

\$Id: ipsec-x509.php,v 1.22 2004/06/21 14:41:22 natecars Exp \$\br/>
 [06/17/04] Major updates to cover Openswan 2.1.2+ configuration.
 [04/06/04] In 'Common errors', add section on how to get rightca correct.
 [04/06/04] Some bugfixes to ipsec.conf examples from Paul of the Openswan team.
 [04/06/04] Added note under the cert copy section to make sure you set the pw, for non-newbies.
 [03/21/04] Added note about FreeS/WAN going away, and Openswan.
 [02/13/04] Added update note, saying it's based on 1.9x, and will be updated to 2.x.
 [11/13/03] Fix link to Strongsec site; thanks Jima!
 [05/06/03] Remove alternate way to get NAT working; add rightsubnetwithin note.
 [01/02/03] Link to Jacco de Leeuw's IPsec/L2TP page
 [11/21/02] Add a note for FreeS/WAN configuration files saying indentation is important. Thanks Stephen!
 [10/14/02] Updated RootCA.der entry in Client section to match with the Server.
 [10/10/02] Updated to new template for my main site. Cleaned things up a bit.
 [10/10/02] Put everything in CVS, finally.
 [10/09/02] Added paths for RH7.x/RH8.x (thanks for the reminder, Johan!)
 [08/08/02] Added note in the CA section to make sure that CA cert is longer than the client cert
 [06/19/02] Added color highlights to openssl commands; split into more sections
 [06/07/02] Switched from pre to classes to fix scrolling annoyances
 [05/30/02] Misc cleanup
 [04/30/02] Removed 'roadwarrior' conn from wireless section since it's not necessary; added example ipsec.exe output.
 [04/18/02] Added 'common errors' section; fixed some type-o's.
 [04/16/02] Added changelog.
 [04/15/02] Fixed type-o in Windows config section -- I had 'rightnet='; should be 'rightsubnet='.
 [04/01/02] Added section with example wireless setup.

Setting up your Certificate Authority

For the sake of this document, I'm assuming you want to use X.509 certificates for authentication. It is