# IPsec in Tunnel Mode between Windows XP Professional and OpenBSD with X.509v3 Certificate Authentication

Thomas Walpuski
**<thomas@koeln.h07.org>**
February 7th, 2002
*Translated into English by Mike van Opstal mvanopst@cs.umd.edu*

For the fundamental understanding of this paper, knowledge of IPsec is not mandatory, but nevertheless helpful. As an introduction it's recommended to read: `http://www.informatik.uni-bremen.de/grp/ag-sec/Seminar/WS00/ipsec.ps`.

The following paper describes in detail the configuration of an IPsec Host-to-Host connection between OpenBSD and Windows XP Professional with Authentication via X.509v3 Certificates. A VPN can be implemented with simple modifications. Windows XP Professional's IPsec implementation corresponds approximately to that of Windows 2000 Professional with the High Encryption Service Pack (3DES). Most sections of this paper's descriptions can also be used with Windows 2000 Professional.

# 1 Preparation

Before we can really begin with the configuration, we must first produce the necessary RSA keys and certificates.

## 1.1 RSA-Key and Certificate for the CA

If no Certificate Authority is available to be used, the first step is to create the RSA keys for the CA.

```
# openssl genrsa -out /etc/ssl/private/ca.key 1024
Generating RSA private key, 1024 bit long modulus
..............................++++++
....++++++
e is 65537 (0x10001
```

Then you need to create a CSR (Certificate Signing Request) for this.

```
# openssl req -new -key /etc/ssl/private/ca.key -out \
> /etc/ssl/private/ca.csr
Using configuration from /etc/ssl/openssl.cnf
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) []:DE
State or Province Name (full name) []:Thuringia
Locality Name (eg, city) []:Jena
Organization Name (eg, company) []:IPsec Labs
Organizational Unit Name (eg, section) []:Certification Authority
Common Name (eg, fully qualified host name) []:ca.ipseclabs.org
Email Address []:ca@ipseclabs.org
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

This CSR will be signed with the key that the CSR created.

```
# openssl x509 -req -days 365 -in /etc/ssl/private/ca.csr \
> -signkey /etc/ssl/private/ca.key -out /etc/ssl/ca.crt
Signature ok
subject=/C=DE/ST=Thuringia/L=Jena/O=IPsec Labs/OU=Certification
Authority/CN=ca.ipseclabs.org/Email=ca@ipseclabs.org
Getting Private
```

## 1.2 RSA Keys, Certificates, etc, for the Hosts

First an RSA key must be created. In our case the key must be 1024 bits long, since as far as I know Windows XP can only deal with that length.

```
# openssl genrsa -out local.key 1024
Generating RSA private key, 1024 bit long modulus
.....................................................................
.++++++
.++++++
e is 65537 (0x10001)
```

For this key we create a CSR. The fields should be filled out based on an agreed upon convention. This will save you problems later.

```
# openssl req -new -key local.key -out tyr.csr
Using configuration from /etc/ssl/openssl.cnf
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) []:DE
State or Province Name (full name) []:Thuringia
Locality Name (eg, city) []:Jena
Organization Name (eg, company) []:IPsec Labs
Organizational Unit Name (eg, section) []:Networking
Common Name (eg, fully qualified host name)
[]:tyr.networking.ipseclabs.org
Email Address []:root@tyr.networking.ipseclabs.org
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Den CSR lassen wir nun von der CA signieren.

```
# openssl x509 -req -days 365 -in tyr.csr -CA \
> /etc/ssl/ca.crt -CAkey /etc/ssl/private/ca.key \
> -CAcreateserial -out tyr.crt
Signature ok
subject=/C=DE/ST=Thuringia/L=Jena/O=IPsec
Labs/OU=Networking/CN=tyr.networking.ipse
clabs.org/Email=root@tyr.networking.ipseclabs.org
Getting CA Private Key
```

When we use this on the OpenBSD side, we must add a subjectAltName extention to the certificate with certpatch. This should configure an IP address, FQDN, or a UFQDN. In our situation, we're adding an FQDN.

```
# certpatch -t fqdn -i tyr.networking.ipseclabs.org \
> -k /etc/ssl/private/ca.key tyr.crt tyr.crt
Reading ssleay created certificate tyr.crt and modify it
```

```
Creating Signature: PKEY_TYPE = RSA: X509_sign: 128 OKAY
Writing new certificate to tyr.crt
```

For the Windows XP Host we must also add a PKCS-12 Bundle.

```
# openssl pkcs12 -export -in tyr.crt -inkey local.key \
> -certfile ca.crt -out tyr.p12
Enter Export Password:
Verifying password - Enter Export Password:
```

The procedure must now be executed again for the receiving station. On the OpenBSD side it's not necessary to create the PKCS-12 Bundle.

# 2 Configuration of the OpenBSD Hosts

```
# ls -l /etc/isakmpd/*
-rw------- 1 root wheel 1744 Jan 30 18:34 /etc/isakmpd/isakmpd.conf
-rw------- 1 root wheel 128 Jan 28 17:14 /etc/isakmpd/isakmpd.policy
/etc/isakmpd/ca:
3
total 2
-rw------- 1 root wheel 1001 Jan 28 18:00 ca.crt
/etc/isakmpd/certs:
total 8
-rw------- 1 root wheel 1119 Jan 28 18:06
heimdal.programming.ipseclabs.org.crt
-rw------- 1 root wheel 1094 Jan 28 18:05
tyr.networking.ipseclabs.org.crt
/etc/isakmpd/keynote:
/etc/isakmpd/private:
total 2
-rw------- 1 root wheel 887 Jan 28 18:00 local.key
```

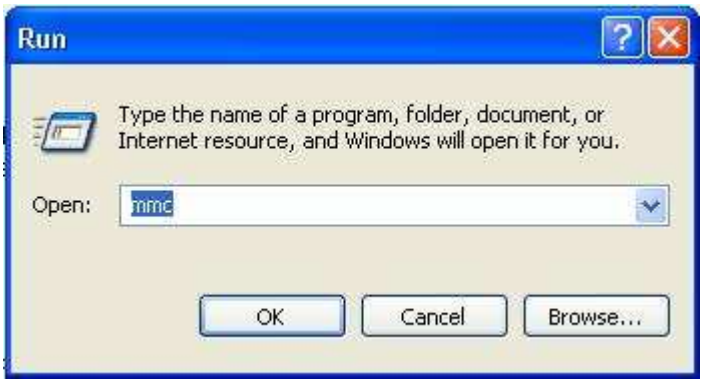
The certificate of the Windows XP Hosts does not have to be available, because for some reason isakmpd can not detect it, so it must be transferred using the main mode by Windows XP.

```
# cat /etc/isakmpd/isakmpd.conf
[Phase 1]
10.0.0.3= ISAKMP-peer-tyr
[Phase 2]
Connections= IPsec-heimdall-tyr
[ISAKMP-peer-tyr]
Phase= 1
Transport= udp
Local-address= 10.0.0.1
Address= 10.0.0.3
ID= FQDN-heimdall
# Windows XP doesn't send it, like PGPnet
# subjectAltName, instead of the 'normal' Subject
# Certificates. Meaning you can't use Remote-ID here
#Remote-ID= FQDN-tyr
Configuration= Default-main-mode
[FQDN-heimdall]
ID-type= FQDN
# Its necessary to make sure that the certificates can
# be found exactly the same as the names (+ .crt) in the
# certs/ directory.
Name= heimdal.programming.ipseclabs.org
# s.o.
#[FQDN-tyr]
#ID-type= FQDN
```

```
#Name= tyr.networking.ipseclabs.org
[IPsec-heimdall-tyr]
Phase= 2
ISAKMP-peer= ISAKMP-peer-tyr
Configuration= Default-quick-mode
Local-ID= Host-heimdall
4
Remote-ID= Host-tyr
[Host-heimdall]
ID-type= IPV4_ADDR
Address= 10.0.0.1
[Host-tyr]
ID-type= IPV4_ADDR
Address= 10.0.0.3
[Default-main-mode]
DOI= IPSEC
EXCHANGE_TYPE= ID_PROT
Transforms= 3DES-MD5
[Default-quick-mode]
DOI= IPSEC
EXCHANGE_TYPE= QUICK_MODE
Suites= QM-ESP-3DES-MD5-SUITE
[3DES-MD5]
ENCRYPTION_ALGORITHM= 3DES_CBC
HASH_ALGORITHM= MD5
AUTHENTICATION_METHOD= RSA_SIG
GROUP_DESCRIPTION= MODP_1024
# cat /etc/isakmpd/isakmpd.policy
KeyNote-Version: 2
Authorizer: "POLICY"
Licensees: "DN:/C=DE/ST=Thuringia/L=Jena/O=IPsec Labs/\
OU=Certification Authority/CN=ca.ipseclabs.org/\
Email=ca@ipseclabs.org"
Conditions: app_domain == "IPsec policy" &&
esp_present == "yes" &&
mnesp_enc_alg != "null" &&
remote_id_type == "ASN1 DN" &&
remote_id == "/C=DE/ST=Thuringia/L=Jena/\
O=IPsec Labs/OU=Networking/\
CN=tyr.networking.ipseclabs.org/\
Email=root@tyr.networking.ipseclabs.org" -> "true";
```

# 3 Configuration of the Windows XP Hosts

The configuration of IPsec and certificate based connections are done in Windows XP with snap-ins to the Management Console (mmc). Start mmc at Start/Run …



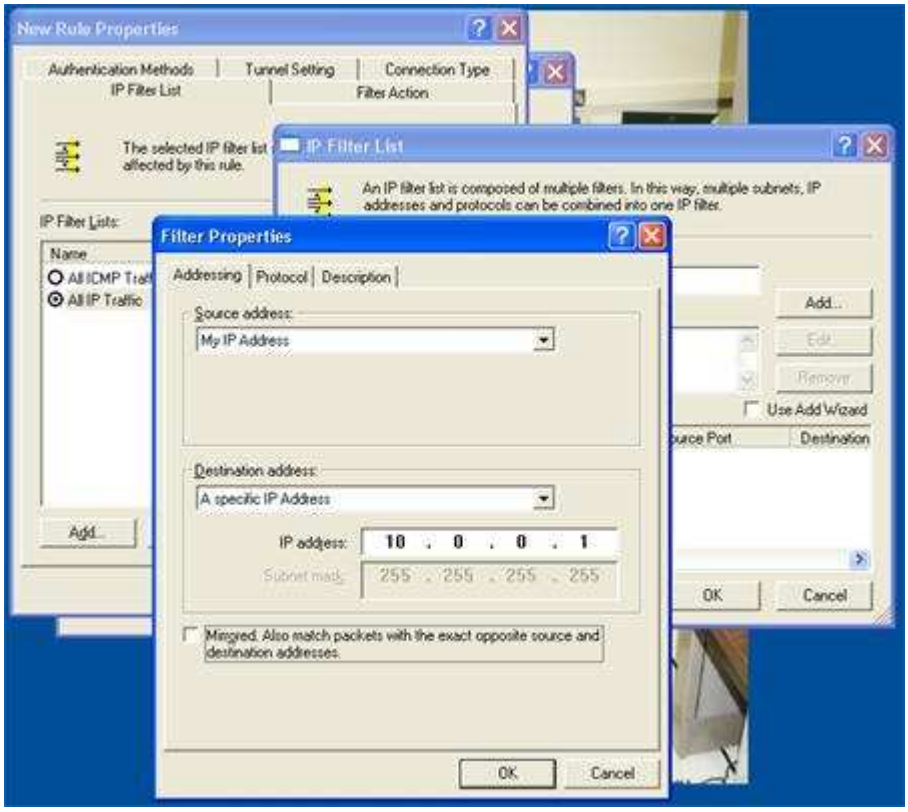
Press Control+M to bring up the Add/Remove Snap-Ins manager. Select Add, and select the IP Security Monitor, IP Security Policies for the local computer, and Certificates for the local computer.


It's recommended that you save your console settings by pressing Control+S.

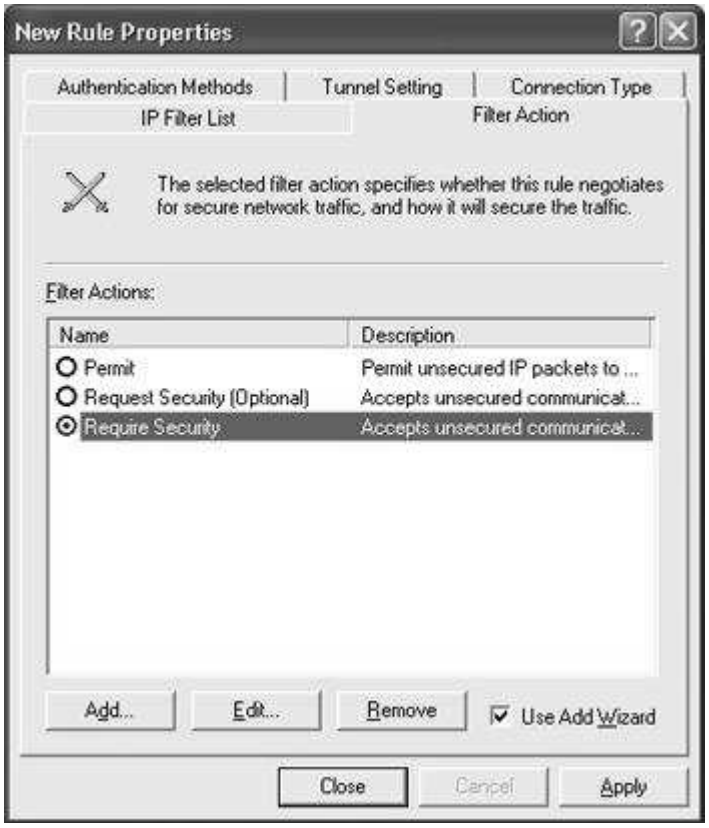
Right clicking on IP Security Policies on Local Computer brings up a menu, from which select Create IP Security Policy.


The IP Security Policy Wizard should start. In this wizard we choose a meaningful name for the new IP Security Policy (such as IPsec Connection between tyr and heimdal). Deselect the Activate the Default Response Rule option. At the completion of the wizard select Edit Properties, and then Finish.

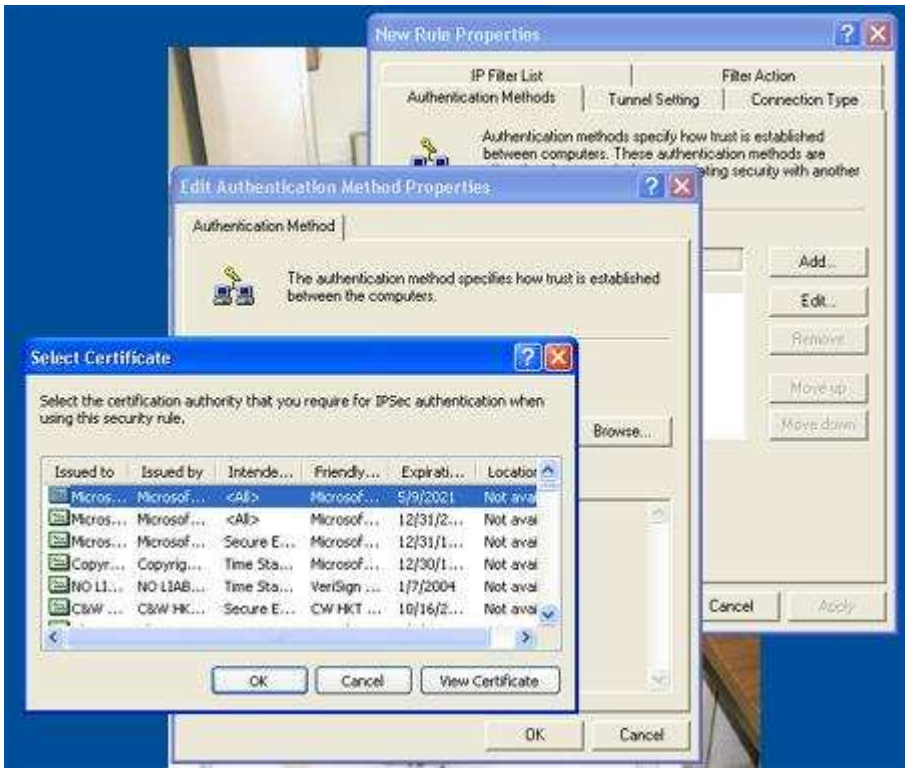
Next we add a new IP Security Rule. This creates a filter for all traffic from our IP address (10.0.0.3) to the receiving station (10.0.0.1). Select Add (make sure that options for wizard are turned off), and select Add again to create a new IP Filter list, and Add a new filter. The filter will not work unless “Mirrored. Also match packets with the exact opposite source and destination addresses” is deselected.



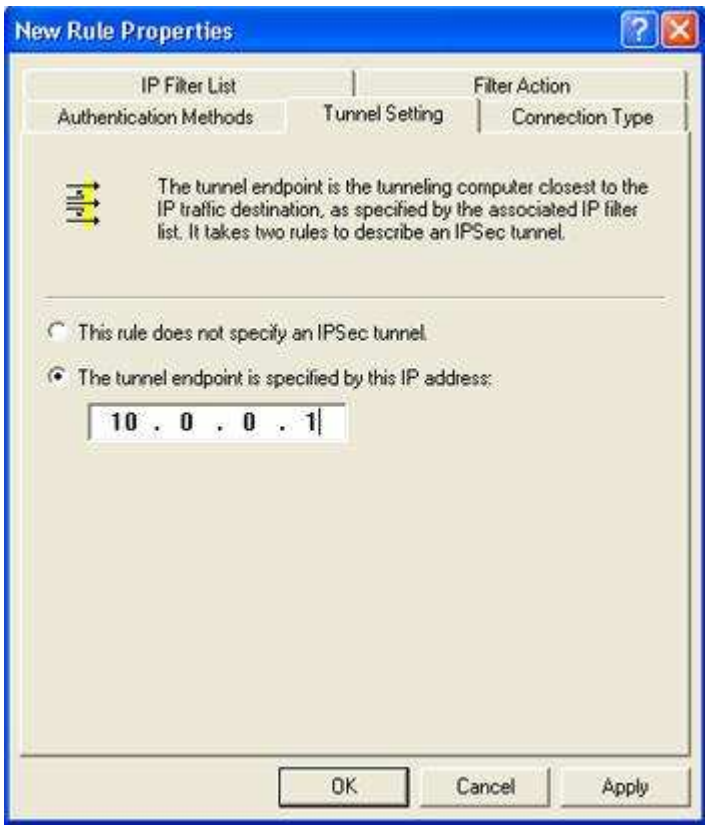

Then select Require Security as Filter Action.



Edit the default Authentication method to “Use a certificate from this certification authority”, and select the certificate from our CA.




As tunnel terminating point we configure the IP Address of the receiving station (10.0.0.1)




After we have finished the creation of the first rule, we create a second. In this rule we configure the filter from the end point to our address, and give our IP address as the tunnel termination point.

# 4 Test of the Configuration

On the OpenBSD host start isakmpd in debug mode with the option –L, which writes the IKE process in /var/run/isakmpd.pcap  With help from tcpdump you can get it in a human readable format.

```
# isakmpd -d -L
```

To test the connection goto Start/Run, and run the command prompt (cmd) and ping the destination.

If there are no problems you can set the isakmpd_flags in /etc/rc.conf to “”.