

[win32] stunnel / OpenSSL / Synergy howto

Author: Patrick Jansen, Germany
Contact: cruchot83@nospammail.net
Last update: 07/05/2007

This is a short but hopefully useful doc how to install, configure and use stunnel.

What is stunnel?

To improve privacy stunnel encrypts TCP connections and offers the secure communication between a SSL server and non-SSL aware applications and protocols.

It makes use of OpenSSL and in opposition to SSH (catchword „PuTTY“) you don't have to setup a SSH server and can install it as Windows service. stunnel is free and available for different platforms.

What is Synergy?

An open-source solution to control two or more systems with only one keyboard and one mouse.

This howto should be a guide for other applications (than Synergy) too.

Downloads

Always use the latest versions of

stunnel

URL: <ftp://stunnel.mirt.net/stunnel/>

File: stunnel-4.20-installer.exe + stunnel-4.20.tar.gz

OpenSSL

URL: <ftp://stunnel.mirt.net/stunnel/openssl/> => binary-0.9.8e-zdll

File: openssl.zip

Synergy

URL: <http://synergy2.sourceforge.net/>

Install and configure Synergy

Install Synergy on both systems and configure it as server on the first, as client on the other.

Install stunnel and OpenSSL

The following steps have to be done on the Synergy server and client:

Install stunnel with *stunnel-4.20-installer.exe*.

Unpack *openssl.zip* in the stunnel installation folder and overwrite already existing files (libssl32.dll, libeay32.dll, zlib1.dll).

Unpack *stunnel-4.20.tar.gz* (e.g. with WinRAR) to a temporary folder and copy the included file *stunnel.cnf*, it is in the subfolder *tools*, in the stunnel installation folder – do not confound it with the *stunnel.conf*.

Note: The Windows Explorer does not show the file extension *.cnf*.

Configure stunnel on the Synergy server

Overwrite the content of *stunnel.conf* in the stunnel installation folder with this one:

```
output = stunnel.log
socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1
cert = stunnel.pem
[synergy]
accept = 25800
connect = 24800
```

The Synergy default port is 24800. Instead of 25800 you can choose some arbitrary high port.

Configure stunnel on the Synergy client

Overwrite the content of *stunnel.conf* in the stunnel installation folder with this one:

```
client = yes
output = stunnel.log
socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1
cert = stunnel.pem
[synergy]
accept = 24800
connect = mainpc:25800
```

Replace *mainpc* with the hostname of your own Synergy server.

Start stunnel on the Synergy server

Run *stunnel.exe* in the stunnel installation folder

Start the Synergy server

Start stunnel on the Synergy client

Run *stunnel.exe* in the stunnel installation folder

Configure and start the Synergy client

Set the Synergy client option „Other Computer's Host Name“ to „localhost“.

Start the Synergy client.

The stunnel log window (double click the stunnel icon in the taskbar) on the Synergy server should show something like this:

```
synergy accepted connection from 192.168.2.33:1043  
synergy connected remote server from 127.0.0.1:1330
```

and on the Synergy client:

```
synergy accepted connection from 127.0.0.1:1042  
synergy connected remote server from 192.168.2.33:1043
```

If both Synergy taskbar icons show a established connection, the encryption between server and client is up and running.

Note: If you change the stunnel.conf files while stunnel is running, you have to restart stunnel.

Create a private key and certificate – **highly recommended**

To allow only connections from authenticated clients you should create your own certificates!

The following steps have to be done on the Synergy server and client:

Shutdown Synergy and stunnel.

Delete the file *stunnel.pem* in the stunnel installation folder.

Open a command line box, go to the stunnel installation folder and type

```
openssl.exe req -new -x509 -days 365 -nodes -config stunnel.cnf -out stunnel.pem -keyout stunnel.pem
```

```
C:\WINDOWS\system32\cmd.exe
D:\stunnel>openssl.exe req -new -x509 -days 365 -nodes -config stunnel.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'stunnel.pem'
-----
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) [PL]:xx
State or Province Name (full name) [Some-State]:mystate
Locality Name (eg, city) []:mycity
Organization Name (eg, company) [Stunnel Developers Ltd]:mycompany
Organizational Unit Name (eg, section) []:mysection
Common Name (FQDN of your server) [localhost]:mainpc
D:\stunnel>
```

Set „Common Name (FQDN of your server)“ to the hostname you are running the command onto

In the stunnel installation folder create an empty file *certs.pem*.

Copy the

```
-----BEGIN CERTIFICATE-----
[...]
-----END CERTIFICATE-----
```

part in the new created *stunnel.pem* into the *certs.pem*.

Attach the

```
-----BEGIN CERTIFICATE-----
[...]
-----END CERTIFICATE-----
```

part in *stunnel.pem* of the remote station into the local *certs.pem*.

The *certs.pem* files should now look like this:

```
-----BEGIN CERTIFICATE-----
[own certificate]
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
[remote certificate]
-----END CERTIFICATE-----
```

Extend the *stunnel.conf*:

Synergy server:

```
output = stunnel.log
socket = l:TCP_NODELAY=1
```

```
socket = r:TCP_NODELAY=1
cert = stunnel.pem
verify = 2
CAfile = certs.pem
[synergy]
accept = 25800
connect = 24800
```

Synergy client:

```
client = yes
output = stunnel.log
socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1
cert = stunnel.pem
verify = 2
CAfile = certs.pem
[synergy]
accept = 24800
connect = mainpc:25800
```

After the restart of stunnel and Synergy on both systems there should be additional entries in the stunnel log windows:

```
Server (hostname in this howto „mainpc“):
VERIFY OK: depth=0, /C=xx/ST=mystate/L=mycity/O=mycompany/OU=mysection/CN=notebook
```

```
Client (hostname in this howto „notebook“):
VERIFY OK: depth=0, /C=xx/ST=mystate/L=mycity/O=mycompany/OU=mysection/CN=mainpc
```

Install stunnel and Synergy as services

Synergy (server und client): look at the configuration GUI, „AutoStart“ => „When Computer Starts“.

Set the Synergy server and client option „Logging Level“ (look at the configuration GUI) to „Error“.

stunnel (server und client): Windows start menu => „stunnel“ => „Service install“

It could take some seconds after a system restart to establish the connection(s).

Abbreviated connection setup

Synergy client => stunnel client (port 24800) ==> stunnel server (port 25800) => Synergy server (port 24800)

Client system / Server system / => unencrypted / ==> encrypted (stunnel)