Contents

[**Stunnel** 1](#_Toc503634853)

[**Configuration at Server side** 1](#_Toc503634854)

[**Configuration at Client side** 3](#_Toc503634855)

[**References** 3](#_Toc503634856)

# **Stunnel**

* Stunnel is an SSL security wrapper that allows to encrypt data being transmitted from source to destination.
* Mainly, stunnel is used to encrypt particular services like http, pop3, imap4, etc.

## **Configuration at Server side**

* Install stunnel and openssl

Command: yum install stunnel -y

Command: yum install openssl -y

* Create your own certificate,

Navigate to /etc/pki/tls/certs

Command: make stunnel.pem

D:\RHEL 6.4\snaps\stunnel\server\make stunnel certificate.PNG

Default certificate: /etc/pki/tls/cert.pem

* Verify created certificate,

Command: openssl verify /etc/pki/tls/certs/stunnel.pem

* Configuration files: /etc/stunnel/stunnel.conf

If it doesn’t exist, create by own.

cert = path of certificate

chroot = changed root directory in which stunnel will run

setuid = nobody

setgid = nobody

pid = file in which stunnel PID will be saved

sslVersion = version of SSL

options = additional options

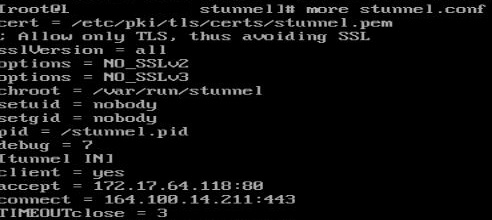
output = path of log file for stunnel (Default: /var/log/secure)

[service name]

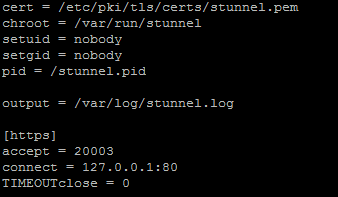
accept = port to listen on (stunnel will listen this port)

connect = port to connect to (must be the port that service being used)

TIMEOUTclose = no of seconds to wait for close-notify alert from the client



Example: At Server Side



* Create chroot directory if doesn’t exist and give it ownership to nobody user.

Command: mkdir -p /var/run/stunnel

D:\RHEL 6.4\snaps\stunnel\server\create chroot directory.PNG

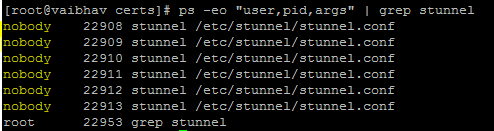
Command: chown nobody:nobody /var/run/stunnel

D:\RHEL 6.4\snaps\stunnel\server\nobody to chroot directory.PNG

* If firewall/iptables are enabled then allow ports to enable stunnel.
* Start stunnel

Command: stunnel /etc/stunnel/stunnel.conf

D:\RHEL 6.4\snaps\stunnel\server\start.PNG



## **Configuration at Client side**

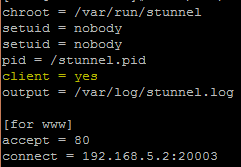
* Install stunnel

Command: yum install stunnel -y

* Configuration files: /etc/stunnel/stunnel.conf

If it doesn’t exist, create by own.

client = yes



* Create chroot directory if doesn’t exist and give it ownership to nobody user.

Command: mkdir -p /var/run/stunnel

Command: chown nobody:nobody /var/run/stunnel

* Start stunnel

Command: stunnel /etc/stunnel/stunnel.conf

* Verify from client,

Command: telnet localhost 80

**References**:

* <https://www.stunnel.org/index.html>
* Sample configuration file: <https://www.stunnel.org/config_unix.html>
* Redhat example: <https://access.redhat.com/solutions/333043>