

Stunnel Database and Sensor Configuration

This document outlines how to setup Stunnel between a sensor and the Sguil database server. This setup is in two parts. The first part must be done on the database server by creating a Stunnel (SSL) certificate and then configuring the Stunnel configuration as well as the hosts.allow file to allow the sensors to connect to the database server.

Configuring the Database Server	1
Database TCP Wrapper Configuration	1
Stunnel SSL keys	1
stunnel.conf Database Example	2
Start the stunnel service on the database.....	2
Add Sguil user on MySQL database.....	3
Snort Sensor Configuration.....	4
Sensor TCP Wrapper Configuration.....	4
Stunnel SSL keys	4
Stunnel.conf example.....	4
Start the stunnel service on the sensor	5
Configuring Barnyard.....	6
Test the Snort Sensor Connectivity.....	6

Configuring the Database Server

Database TCP Wrapper Configuration

This setup in the hosts.allow file must be repeated for each Snort sensor reporting to the database.

```
vi /etc/hosts.allow
```

```
3307: 192.168.25.50 \      # This will allow Barnyard to connect to the database from
      192.168.30.6        the remote sensor
7737: 192.168.25.50 \      # This will allow Barnyard to connect to sguil from the
      192.168.30.6        remote sensor
```

Stunnel SSL keys

```
cd /etc/stunnel
```

```
./generate-stunnel-key.sh    Note: Common Name can be set to localhost
```

Note: This certs.pem is used to copy the CERTIFICATE information from the sensors for authentication.

```
touch /etc/stunnel/certs.pem
```

Guy Bruneau - seeker@whitehats.ca

```
chown root:root certs.pem  
chmod 600 certs.pem
```

Create a default stunnel configuration file

```
cp stunnel.conf_server stunnel.conf  
vi stunnel.conf
```

stunnel.conf Database Example

```
# Sample stunnel configuration file  
# Copyright by Michal Trojnara 2002
```

```
#chroot = /usr/var/run/stunnel/  
# PID is created inside chroot jail  
pid = /tmp/stunnel.pid  
setuid = nobody  
setgid = nogroup
```

```
# Authentication stuff  
verify = 2  
CAfile = /etc/stunnel/certs.pem  
cert = /etc/stunnel/stunnel.pem
```

```
# Some debugging stuff  
#debug = 7  
#output = stunnel.log
```

```
# Use it for client mode  
client = no
```

```
# Service-level configuration
```

```
[3307]  
accept = IP_mysql_database:3307  
connect = 127.0.0.1:3306
```

```
[7737]  
accept = IP_mysql_database:7737  
connect = 127.0.0.1:7736
```

Start the stunnel service on the database

```
# stunnel [Enter]
```

Edit the /etc/rc.d/rc.local and uncomment the echo and stunnel lines

Add Sguil user on MySQL database

The correct Sguil (default password is **password**) user account is already preconfigured if you are using the database included on this CD. Suggest you use Webmin to change the password.

```
mysql -p (root password set earlier)
\u mysql (User mysql)
```

```
GRANT ALL ON sguildb.* TO sguil@127.0.0.1 IDENTIFIED BY \
'make_a_password_for_user_snort' WITH GRANT OPTION;
\q (Quit mysql)
```

Snort Sensor Configuration

Sensor TCP Wrapper Configuration

```
vi /etc/hosts.allow
```

```
3306: 127.0.0.1      # This will allow Barnyard to connect to the database server
7736: 127.0.0.1      # This will allow Barnyard to connect to the database server
```

Stunnel SSL keys

Note: If you want to simplify things, you can use the same certificate (stunnel.pem) created on the database server and copy it here. Just make sure that you copy the stunnel.pem CERTIFICATE information into the certs.pem as see below.

```
cd /etc/stunnel
./generate-stunnel-key.sh    Note: Common Name can be set to localhost
```

Create a default stunnel configuration file

```
cp stunnel.conf_sensor stunnel.conf
vi stunnel.conf
```

Stunnel.conf example

```
# Sample stunnel configuration file
# Copyright by Michal Trojnara 2002
```

```
pid = /tmp/stunnel.pid
setuid = nobody
setgid = nogroup
cert = /etc/stunnel/stunnel.pem
CAfile = /etc/stunnel/stunnel.pem
```

```
# Some debugging stuff
#debug = 7
#output = stunnel.log
```

```
# Use it for client mode
client = yes
```

```
# Service-level configuration
```

```
[3306]
accept = 127.0.0.1:3306
connect = IP_mysql_database:3307
```

```
[7736]
accept = 127.0.0.1:7736
connect = IP_mysql_database:7737
```

On the Snort sensor, copy from the file /etc/stunnel/stunnel.pem the section:

```
-----BEGIN CERTIFICATE-----
f05yAI/ICUxXYdOMIICOTCCAaKg
MBEGA1UECBMKf05yAI/ICUxXYdO
f05yAI/ICUxXYdOIEx0ZDESMBAG
MTA5MzA1NFowf05yAI/ICUxXYdO
f05yAI/ICUxXYdOBgNVBAoTFIN0
dDCBnzANBgkqf05yAI/ICUxXYdO
f05yAI/ICUxXYdOexW1uigvYk7f
bBDRCEC39YIQf05yAI/ICUxXYdO
f05yAI/ICUxXYdOUjOPdHWz5CB2
SIb3DQEBBAUAf05yAI/ICUxXYdO
f05yAI/ICUxXYdOITG9m64pAyD6
U44OtGGV+cwcf05yAI/ICUxXYdO
-----END CERTIFICATE-----
```

and paste it in the MySQL Server Database file /etc/stunnel/certs.pem

Start the stunnel service on the sensor

```
# stunnel [Enter]
```

Edit the /etc/rc.d/rc.local and uncomment the echo and stunnel lines.

Configuring Barnyard

You can uncomment the default settings for Barnyard to start logging. However, if you change the user and password to for logging into the database, you will need to edit the barnyard.eth1.conf file to change the settings:

```
cd /usr/local/barnyard/etc
```

```
edit barnyard.eth1.conf
```

Find: config hostname: **shadow** (Change shadow to the correct sensor name)

(Go to the bottom with Shift-G)

Uncomment the following two lines (#)

```
output sguil: mysql, sensor_id 0, database sguildb, server 127.0.0.1, user sguil, \
password password, sguil_host 127.0.0.1, sguil_port 7736
```

Note: If your server is something other than **127.0.0.1**, change it accordingly.

Test the Snort Sensor Connectivity

telnet 127.0.0.1 3306 You should see a MySQL database prompt at this point confirming the traffic is getting routed correctly.