

Stunnel.org

[Home](#)[<Examples>](#)[About](#)[News](#)[FAQ](#)[Examples](#)[Download](#)[Patches](#)[Support](#)[Related](#)

Encrypting traffic to a remote syslog-ng server including SSL peer authentication

1. Install stunnel and syslog-ng on both machines.
2. Create certificates for both machines. On RedHat 9 and similar machines, you can do the following as root:

```
# cd /usr/share/ssl/certs
# make syslog-ng-server.pem
# make syslog-ng-client.pem
```
3. Place copies of both certificates on both machines in /etc/stunnel with two important alterations. The server only needs the certificate section of syslog-ng-client.pem and the client only needs the certificate section of syslog-ng-server.pem. In other words, remove the private key sections from the respective certificate copies.
4. Give only root ownership, read and write permissions for certificates.
5. On server, create /etc/stunnel/stunnel.conf containing the following replacing *client IP address* accordingly:

```
cert = /etc/stunnel/syslog-ng-server.pem
CAfile = /etc/stunnel/syslog-ng-client.pem
verify = 3
[5140]
    accept = client IP address:5140
    connect = 127.0.0.1:514
```

- On client, create /etc/stunnel/stunnel.conf containing the following replacing *server IP address* accordingly:

```
client = yes
cert = /etc/stunnel/syslog-ng-client.pem
CAfile = /etc/stunnel/syslog-ng-server.pem
verify = 3
[5140]
    accept = 127.0.0.1:514
    connect = server IP address:5140
```

6. On server, create the following in /etc/syslog-ng.conf:

```

options { long_hostnames(off);
          sync(0);
          keep_hostname(yes);
          chain_hostnames(no); };
source src {unix-stream("/dev/log");
           pipe("/proc/kmsg");
           internal();};
source stunnel {tcp(ip("127.0.0.1")
                   port(514)
                   max-connections(1));};
destination remoteclient {file("/var/log/remoteclient");};
destination dest {file("/var/log/messages");};
log {source(src); destination(dest);};
log {source(stunnel); destination(remoteclient);};

```

On client, create the following in `/etc/syslog-ng.conf`:

```

options {long_hostnames(off);
        sync(0);};
source src {unix-stream("/dev/log"); pipe("/proc/kmsg");
           internal();};
destination dest {file("/var/log/messages");};
destination stunnel {tcp("127.0.0.1" port(514));};
log {source(src);destination(dest);};
log {source(src);destination(stunnel);};

```

(See `syslog-ng` documentation for more sophisticated `syslog-ng.conf` alternatives.)

7. Open necessary ports with regards to packet filtering and TCP wrappers.

8. On both machines, add the following lines to boot procedure and execute them now:

```

# stunnel
# syslog-ng -f /etc/syslog-ng.conf

```

Please send questions and comments to Christian Seberino (chris <at> pythonsoft <dot> com).