Rsyslog+ssl

Настройка серверной части

Создаем новый самоподписанный сертификат

```
openssl genrsa 2048 > ca-key.pem

openssl req -new -x509 -nodes -days 3600 -key ca-key.pem -out ca-cert.pem
```

Создаем набор ключей

```
openssl req -newkey rsa:2048 -days 3600 -nodes -keyout server-key.pem -out server-req.pem

openssl rsa -in server-key.pem -out server-key.pem

openssl x509 -req -in server-req.pem -days 3600 -CA ca-cert.pem -CAkey ca-key.pem -set_serial 01 -out server-
cert.pem
```

Все *.pem* файлы копируем в */etc/ssl/certs*

Редактируем */etc/rsyslog.conf* (порядок строк важен!)

```
$DefaultNetstreamDriver gtls

$DefaultNetstreamDriverCAFile /etc/ssl/certs/ca-cert.pem

$DefaultNetstreamDriverCertFile /etc/ssl/certs/server-cert.pem

$DefaultNetstreamDriverKeyFile /etc/ssl/certs/server-key.pem

$ModLoad imtcp

$InputTCPServerStreamDriverMode 1

$InputTCPServerStreamDriverAuthMode anon

$InputTCPServerRun 514
```

Перезапускаем rsyslog

```
/etc/init.d/rsyslog restart
```

Настройка клиентской части

Загружаем *ca-cert.pem* с сервера на клиентскую машину в */etc/ssl/certs*

Ставим rsyslog-gnutls

```
apt-get install rsyslog-gnutls
```

Редактируем */etc/rsyslog.conf* (порядок строк важен!)

```
$DefaultNetstreamDriverCAFile /etc/ssl/certs/ca-cert.pem

$DefaultNetstreamDriver gtls

$ActionSendStreamDriverMode 1

$ActionSendStreamDriverAuthMode anon

*.* @@192.168.1.1
```

(где 192.168.1.1 — адрес сервера)

Перезапускаем rsyslog

```
/etc/init.d/rsyslog restart
```

Проверка

На сервере устанавливаем tcpdump

```
apt-get install tcpdump
```

запускаем дамп пакетов

```
tcpdump -A > tcp.txt
```

На клиенте

```
sudo login test

exit
```

На сервере

```
grep test tcp.txt
```