Правила использования программы Stunnel на ОС Linux

Программа stunnel предназначена для шифрования трафика между произвольным приложением на клиентском компьютере, которое работает с приложением или службой на удаленном компьютере (сервере). Шифрование делается между двумя экземплярами программы stunnel (на сервере и на клиенте) без необходимости вносить изменения в работу клиентского или серверного ПО. Кроме шифрования, возможно настроить требование аутентификации клиента по сертификату клиента.

1. Установка пакета stunnel

Установка stunnel должна производиться после установки и настройки КриптоПро CSP.
Дистрибутив поставляется в виде пакета cprocsp-stunnel типа rpm.
Для его установки используются стандартные средства для установки rpm из состава дистрибутива.
Для дистрибутивов Linux, основанных на rpm это утилита rpm:

rpm -i cprocsp-stunnel-3.6.1-4.i486.rpm

Для дистрибутивов, основанных на deb, это утилита alien:

alien -kci cprocsp-stunnel-3.6.1-4.i486.rpm

После установки пакета бинарные файлы, предназначенные для запуска stunnel, будут помещёны в */opt/cprocsp/sbin/<архитектура>/* .

Существует две реализации службы stunnel: с импользованием библиотеки pthread и с использованием fork, бинарные файлы называются stunnel_thread и stunnel_fork соответственно. Stunnel с использованием fork возможно использовать только с КриптоПро CSP исполнение КС2.

2. Настройка stunnel

2.1. Выбор варианта использования

Службу stunnel можно использовать либо в режиме клиента, либо в режиме сервера. В режиме клиента stunnel принимает трафик от клиентского приложения, зашифровывает его и отправляет на сервер. На сервере трафик расшифровывается и передаётся конечному приложению или другой службе на этом сервере.

2.2. Установка сертификатов

Установка сертификатов производится при помощи утилит certmgr и cryptcp из состава КриптоПро CSP.

Для работы службы в режиме сервера обязательно нужен сертификат аутентификации сервера. Сервер может требовать, а может не требовать сертификат клиента при соединении клиента с сервером.
Как на клиенте, так и на сервере нужно установить необходимые сертификаты:

а) сертификат корневого Центра Сертификации (ЦС) – в хранилище *ROOT*;
/opt/cprocsp/bin/<архитектура>/certmgr -inst -file root.cer -store ROOT

б) если сертификат сервера или клиента выдан на подчинённом ЦС - сертификаты всех подчиненных ЦС в цепочке должны быть установлены в хранилище *CA*;
/opt/cprocsp/bin/<архитектура>/certmgr -inst -file ca.cer -store CA

в) на сервере должен быть установлен сертификат сервера в хранилище My (текущего пользователя или локального компьютера) с привязкой к контейнеру закрытого ключа сервера;
/opt/cprocsp/bin/<архитектура>/certmgr -inst -file server.cer -cont '\\.\HDIMAGE\server'

г) если сервер требует сертификат клиента – то на клиентском компьютере должен

быть установлен сертификат клиента в хранилище My (текущего пользователя или локального компьютера) с привязкой к контейнеру закрытого ключа клиента.
/opt/cprocsp/bin/<архитектура>/certmgr -inst -file client.cer -cont '\\.\HDIMAGE\client'

2.3. Запись сертификатов в файл

После установки сертификата сервера или клиента в хранилище нужно дополнительно сохранить этот сертификат в файл на диске в формате DER.
Если сертификат в виде файла отсутствует, его можно сохранить из хранилища или из контейнера при помощи утилиты certmgr из состава КриптоПро CSP.

/opt/cprocsp/sbin/<архитектура>/certmgr -expr -dest server.cer -cont '\\.\HDIMAGE\server'

2.4. Формирование файла конфигурации

В файл конфигурации заносятся следующие опции:

Параметр	Описание
chroot	Каталог вызова функции chroot(), которая вызывается после разбора конфигурационного файла stunnel.
debug	Уровень протоколирования.
foreground	foreground режим.
output	Писать лог в file, а не в syslog.
Pid	Файл для сохранения pid.
service	Имя сервиса.
Setgid	Выполняется setgid() в эту группу.
Setuid	Выполняется setuid() под этого пользователя
socket	Опции setsockopt() для сокета приема соединений, а так же для локального и удаленного сокетов.
Service-mode options.	
accept	Принимать соединения на host:port.
cert	Сертификат в der кодировке. Соответствующий сертификат в хранилище должен иметь ссылку на закрытый ключ.
client	Режим клиента (удаленный сервис использует TLS/SSL).

connect	Соединять с удаленным сервером host:port
delay	Задержка для DNS запроса для 'connect' опции.
local	Интерфейс, который должен быть использован для соединения с удаленным хостом.
Verify	Уровень проверки сертификата удаленного компьютера 0 — Игнорировать сертификат 1 — Проверять сертификат если есть 2 — Всегда проверять сертификат 3 — Проверять наличие сертификата в хранилище TrustedUsers

Более подробное описание опций и примеры их использования можно найти на странице man в директории: /opt/cprocsp/share/man/man8.

Далее приведены примеры файлов конфигурации клиента и сервера для следующей задачи. Клиент с компьютера comp1 должен установить соединение с веб-сервером (srv1.test.ru), причём трафик должен быть зашифрован и клиент должен быть аутентифицирован по сертификату.

2.4.1. Пример файла конфигурации для сервера

pid=/var/opt/cprocsp/tmp/stunnel_serv.pid
output=/var/opt/cprocsp/tmp/stunnel_serv.log
socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1
debug = 7

[https]
accept=srv1.test.ru:1502
connect = srv1.test.ru:80
cert=/etc/stunnel/server.cer
verify=2

2.4.2. Пример файла конфигурации для клиента

pid=/var/opt/cprocsp/tmp/stunnel_cli.pid
output=/var/opt/cprocsp/tmp/stunnel_cli.log
socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1
debug = 7

[https]
client = yes
accept=comp1:1500
connect = srv1.test.ru:1502
cert=/etc/stunnel/client.cer
verify=2

Описание всех доступных в конфигурационном файле опций можно найти в странице *man* находящейся в */opt/cprocsp/share/man/man8/*

3. Запуск службы

Запуск службы производится командой

/opt/cprocsp/sbin/<архитектура>/stunnel_thread "путь к файлу конфигурации"

Для остановки необходимо завершить процесс stunnel.

4. Удаление пакета

Удаление пакета производится стандартными средствами операционной системы, предназначенными для удаления rpm. Для дистрибутивов, основанных на rpm:
rpm -e cprocsp-stunnel
Для дистрибутивов, основанных на deb:
dpkg -P cprocsp-stunnel