

Правила использования программы Stunnel на ОС Windows

Программа stunnel предназначена для шифрования трафика между произвольным приложением на клиентском компьютере, которое работает с некоторым 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, можно настроить требование аутентификации клиента по сертификату клиента.

1. Установка службы Stunnel

Установка делается путём запуска
stunnel.exe –install

В дальнейшем служба для старта будет использовать файл stunnel.exe из той папки, откуда была проведена установка.

Перед установкой нужно выбрать режим работы службы, установить сертификаты и сформировать файл конфигурации (см. далее по тексту данного документа).

2. Настройка службы 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

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 «Доверенные корневые Центры Сертификации» локального компьютера;
- б) если сертификат сервера или клиента выдан на подчинённом ЦС - сертификаты всех подчиненных ЦС в цепочке должны быть установлены в хранилище «Промежуточные Центры Сертификации» локального компьютера;
- в) на сервере должен быть установлен сертификат сервера в хранилище «Личные» локального компьютера с привязкой к контейнеру закрытого ключа сервера;
- г) если сервер требует сертификат клиента – то на клиентском компьютере должен быть установлен сертификат клиента в хранилище «Личные» локального компьютера с привязкой к контейнеру закрытого ключа клиента.

2.3. Запись сертификатов в файл

После установки сертификата сервера или клиента в хранилище нужно дополнительно сохранить этот сертификат в файл на диске (без закрытого ключа, без цепочки сертификатов (файл *.cer) в формате BASE64 или DER)

2.4. Формирование файла конфигурации

В файл конфигурации заносятся следующие данные:

Параметр	Описание
accept	ip-адрес (или символическое имя хоста) и порт, на которых stunnel принимает трафик
connect	ip-адрес (или символическое имя хоста) и порт, с которых stunnel передает трафик
cert	имя файла сертификата сервера или клиента
client	режим работы службы: клиент (значение «yes») или сервер (значение «no» или отсутствие параметра)
mutual_auth	для сервера: признак того, требуется ли сертификат клиента (значение «yes») или не требуется (значение «no»)
socket	дополнительные параметры TCP
output	имя файла журнала
debug	степень подробности журналирования: 0 – ничего не записывать, 1 – только ошибки, 3 – ошибки и предупреждения, 7 – все сообщения

Далее приведены примеры файлов конфигурации для 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

```
output=c:\stun-srv\stun.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=C:\stun-srv\svrcer.cer
```

2.4.2. Пример файла конфигурации для клиента

```
output=c:\stun-cli\stun.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=C:\stun-cli\clicer.cer
```

Если сертификат клиента не требуется, то в файл конфигурации сервера нужно добавить строку (в секцию [https])

```
mutual_auth = no
```

2.5. Запись файла конфигурации

Файл конфигурации должен иметь имя `stunnel.conf` и должен быть записан в папку `windows\system32` на системном диске

3. Запуск службы

Запуск, останов и изменение параметров службы запускаются через стандартную оснастку управления службами (`services.msc`)

4. Удаление службы

Удаление службы делается путём запуска `stunnel.exe -remove`