127018, Москва, Сущёвский Вал, 18
Телефон: (495) 995 4820
Факс: (495) 995 4820
https://CryptoPro.ru
E-mail: info@CryptoPro.ru

КРИПТОПРО

Средство Криптографической Защиты Информации

КриптоПро CSP Версия 5.0 КС1 1-Base Приложение для создания TLS-туннеля

ЖТЯИ.00101-01 93 03
Листов 8

2019 г

Содержание

Аннотация

Данный документ содержит общую информацию по использованию программного продукта «ЖТЯИ.00101-01 93 03. КриптоПро CSP. Приложение для создания TLS-туннеля», предназначенного для создания TLS защищенного соединения между клиентом и локальным (inetd-запускаемым) или удаленным сервером.

1 Системные требования

Приложение функционирует в программно-аппаратных средах, перечисленных в ЖТЯИ.00101-01 30 01. КриптоПро CSP. Формуляр, п. 3.2.

2 Использование программы на операционной системе Windows

2.1 Установка службы stunnel

Установка службы производится путём запуска следующей команды:

```
stunnel.exe -install
```

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

2.2 Настройка службы stunnel

Перед установкой службы `stunnel` необходимо выбрать режим работы службы, установить сертификаты и сформировать файл конфигурации.

2.2.1 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.

2.2.2 Установка сертификатов

Для работы службы `stunnel` 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:

1. сертификат корневого Центра Сертификации (ЦС) должен быть установлен в хранилище «Доверенные корневые Центры Сертификации» локального компьютера;

2. если сертификат сервера или клиента выдан на подчинённом ЦС, сертификаты всех подчинённых ЦС в цепочке должны быть установлены в хранилище «Промежуточные Центры Сертификации» локального компьютера;

3. на сервере должен быть установлен сертификат сервера в хранилище «Личные» локального компьютера с привязкой к контейнеру закрытого ключа сервера;

4. 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.

2.2.3 Запись сертификатов в файл

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

2.2.4 Формирование файла конфигурации

В файл конфигурации заносятся следующие опции:

Параметр	**Описание**
debug	Уровень протоколирования
output	Писать лог в file
service	Имя сервиса
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.
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

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.

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\srvcer.cer
verify=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
verify=2
```

2.3 Запуск службы

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

2.4 Удаление службы

Удаление службы `stunnel` производится путём запуска следующей команды:

```
stunnel.exe -remove
```

3 Использование программы в среде UNIX

3.1 Реализации stunnel

Существует две реализации службы `stunnel` — с использованием библиотеки pthread и с использованием fork, бинарные файлы называются stunnel_thread и stunnel_fork соответственно. Реализацию `stunnel` с использованием fork возможно использовать только с КриптоПро CSP версия 5.0 КС2.

3.2 Настройка stunnel

3.2.1 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.

3.2.2 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:

1. сертификат корневого Центра Сертификации (ЦС) должен быть установлен в хранилище ROOT;
`/opt/cprocsp/bin/<архитектура>/certmgr -inst -file root.cer -store ROOT`

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

3. 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'`

4. 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'
```

3.2.3 Запись сертификатов в файл

После установки сертификата сервера или клиента в хранилище необходимо 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'
```

3.2.4 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

Примечание. Описание всех доступных в конфигурационном файле опций можно найти, вызвав в консоли `man stunnel`.

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.

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
```

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
```

3.3 Запуск службы

Запуск службы производится следующей командой:

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

3.4 Остановка службы

Для остановки необходимо завершить процесс stunnel.