Работа утилиты stunnel в режиме клиента на

MAC OS X

В данном документе будет пошагово описан процесс подготовки к работе и функционирования утилиты stunnel в режиме клиента в среде OS X El Capitan.

Утилита stunnel предназначена для шифрования трафика между приложениями, в которых данный функционал не был реализован. Возможна работа в режиме клиента и сервера. Stunnel, работающий в режиме клиента, принимает незашифрованный трафик от некоего клиентского ПО по указанному ip-адресу и порту, затем зашифровывает (трафик) и передаёт его на сервер. Если сервер поддерживает TLS (IIS, TrustedTLS и тд) – серверная часть stunnel'а не требуется. В режиме сервера, stunnel принимает на заранее определённый в конфигурационном файле ip-адрес и порт, зашифрованный трафик, затем расшифровывает его и передает соответствующему ПО на сервере.

В используемом в Mac OS по умолчанию браузере Safari, отсутствует возможность шифрования трафика по ГОСТ алгоритмам и для того, чтобы обойти данное ограничение будет использоваться утилита stunnel, запущенная в режиме клиента. В качестве же сервера, для примера, будет использоваться сервис проверки работы двухстороннего TLS на сайте Крипто-ПРО https://www.cryptopro.ru:4444/test/tls-cli.asp.

Следует также отметить, что данную задачу можно решить и не прибегая к функционалу stunnel. Можно использовать браузер, в котором реализована поддержка ГОСТ изначально – CryptoProFox http://cryptopro.ru/products/cpfox



Утилита stunnel входит в дистрибутив Крипто-ПРО для MAC OS X, и должна быть выбрана для установки вместе с остальными пакетами.

Следует удостовериться в наличии "галки" напротив пакета CPROstnl

		высорочная установка на «rosemite»		Language II I	
A CONTRACT OF THE OWNER OF		Имя пакета	деиствие	Размер	
的复数 网络 网络教育	• введение	CPROcspd	Установить	7,6 M5	
	 Лицензия 	CPROdrvd	Пропустить	684 K5	
	• Размещение	CPROcuri	Установить	897 KB	
			Установить	524 Kb	
	• тип установки		Установить	369 K5	
A A A A A A A A A A A A A A A A A A A	Установка	CPROCades	Установить	512 K5	
	🖌 💿 Обзор	CPROOCSPut	Установить	512 K5	
	Apr	CPROTSPut!	Установить	512 K6	100
		CPROnpcades	Установить	512 K5	1000
	1	CPROrsa	Пропустить	512 K6	10.20
	•	Требуется места на диске: 29,1 МБ	Останется:	19,08 F6	
CAN AN A SHA	top	Универсальный SSL-туннель			12.0
10.cryp					1 3
	CSP				
	40		Haaa	DOGODYUT	ALL.
			Спазад	родолжить	100
					de.
					184
Carl Contraction of the second					100

Завершив установку, можно проверить содержимое папки /opt/cprocsp/sbin



Использоваться будет stunnel_thread.

Следующим действием будет создание конфигурационного файла stunnel.conf в произвольном месте и внесения параметров запуска\работы утилиты.



Краткое описание наиболее часто используемых параметров конфигурации.

Опция	Описание		
pid	Путь к файлу, в котором будет храниться идентификатор процесса		
output	Путь к лог-файлу		
socket	Опции для конфигурирования принимающих, локальных, удалённых		
	сокетов.		
debug	Уровень протоколирования		
client	Работа в режиме клиента		
accept	Адрес и порт для приёма незашифрованного трафика		
connect	Адрес и порт сервера, на который передаётся зашифрованный трафик		
cert	Путь к файлу сертификата клиента		
verify	Возможные варианты проверки сертификата удалённого сервера		
	0. Не проверять сертификат сервера		
	1. Проверять сертификат при его наличии		
	2. Проверять сертификат всегда		
	3. Проверять наличие данного сертификата в хранилище		
	TrustedUsers		

Детальную документацию можно найти в /opt/cprocsp/share/man/man8

Ввиду того, что в примере рассматривается двусторонний TSL, для работы понадобится клиентский сертификат, который к примеру можно выпустить средствами тестового удостоверяющего Крипто-ПРО <u>https://www.cryptopro.ru/certsrv/</u> Нужно также добавить, что этот тестовый удостоверяющий центр, выпустивший личный сертификат является доверенным для сервера, к которому производится подключение.

КРИПТО-ПРО Тестовый УЦ		КРИПТО-ПРО КриптоПро ТІ
Для удобства разработчиков в ООО "КРИПТО-ПРО" развернуты дв центра: <u>тестовый УЦ на основе веб-интерфейса КриптоПро УЦ</u>. Ре использующих Windows и Internet Explorer. 	за тестовых удостоверяющих екомендуется для клиентов,	
тестовый УЦ на основе веб-интерфейса службы сертифик	кации Microsoft (из состава	Вход
Windows Server 2012 R2). Рекомендуется для клиентов, ис	спользующих другие ОС или	Имя пользователя: *
другие браузеры. Для работы с этим УЦ требуется Крипто	Про ЭЦП Browser plug-in.	
Обратившись на выбранный тестовый УЦ, вы можете получить сес	ртификаты ключей электронной	Пароль: *
подписи.		
Используйте эти сертификаты только в целях тестирования.		Вход Регистрация Вход для дилеров
		Забыли пароль?
Не следует доверять сертификатам, которые выпуще	ны тестовым центром, т.к.	
он выдает сертификаты любым пользователям, не вы	ыполняя никаких проверок!	Подписка на обновлен
🖶 Страница для печати		Повости
		· 🔟 Блог
		🔰 Читать

Сперва следует скачать корневой сертификат данного УЦ.

Службы сертификации Active Directory (<i>Microsoft</i>) — CRYPTO-PRO Test Center 2					
Службы сертификации Active Directory (Microsoft) КРИП					
	🗎 cryptopro.ru	C			

Чтобы доверять сертификатам, выданным этим центром сертификации, установите эту цепочку сертификатов ЦС.

Чтобы загрузить сертификат ЦС, цепочку сертификатов или список отзыва сертификатов (CRL), выберите этот сертификат и мето сертификат ЦС:

Текуш	ий (СКУРТО-РЕ	RO Test Center 2

Метод шифрования:

ODER Base 64

Загрузка сертификата ЦС Загрузка цепочки сертификатов ЦС Загрузка последнего базового CRL



Установка корневого сертификата производится командой ./certmgr —inst —store —root —file /Users/admin/Downloads/certnew.cer

Cлужбы сертификации Active Directory (Microsoft)	Mac-Admin:bin ad	bin — -bash — 98×24
Службы сертификации Active Directory (Microsoft)	Mac-Admin:bin ad	ning (neutron inst stand and file (Uneus/admin/P 1 1 1 1
Службы сертификации Active Directory (Microsoft)	Certmor 1.0 (C)	Imina ./certmgr -inst -store root -tile /Users/admin/Downloads/certnew. "CryntoPro", 2007-2010.
	program for mana	iging certificates, CRLs and stores
ужбы сертификации Active Directory (<i>Microsoft</i>) CRYPTO-PRO Test Center 2	WARNING: Legacy	parameter: "-store root"
	Install:	
рузка сертификата ЦС, цепочки сертификатов или CRL	1	
оставлять сертификатам выданным этим центром сертификации устан	Issuer OBL Contor 2	: E=support@cryptopro.ru, C=RU, L=Moscow, O=CRYPTO-PRO LLC, CN=CRYP
ны доверять сертификатам, выданным отим центром сертификации, устан	Subject	: E=support@cryptopro.ru, C=RU, L=Moscow, O=CRYPTO-PRO LLC, CN=CRYF
обы загрузить сертификат ЦС, цепочку сертификатов или список отзыва сер	TH Center 2	- 0
	SHA1 Hash	: 0x046255290b0eb1cdd1797d9ab8c81f699e3687f3
тификат ЦС:	SubjKeyID	: 15317cb08d1ade66d7159c4952971724b9017a83
Текущий [CRYPTO-PRO Test Center 2]	PublicKey Algori	thm : FOCT P 34.10-2001 (512 bits)
	Not valid before	: 05/08/2014 13:44:24 UTC
	Not valid after PrivateKey Link	: 05/08/2019 13:54:03 UTC : No
од шифрования:	[ErrorCode: 0x00	0000001
• DER	Mac-Admin:bin ad	lmin\$
Base 64		
рузка сертификата ЦС		
рузка цепочки сертификатов ЦС		
рузка последнего базового CRL		

Далее производится генерация контейнера.

••• <>		🗎 cryptopro.ru	Ċ)
	Службы сертификации Active Direct	ory (Microsoft)	КРИПТО-ПРС
Организация:	stunnel.cint		
Подразделение:	stunceLcint		
Город:	stunnel_cint		
Область, штат:	stunnel_cint		
Страна, регион:	RU		
Тип требуемого сер	отификата:		
	Сертификат проверки подлинности клиен	ата 📀	
Параметры ключа:			
	⊙Создать новый набор ключей 🛛 🔿 И	спользовать существующий набор ключей	
c	SP: Crypto-Pro GOST R 34.10-2001 KC1 CSP		
Использование клю	ней: ◯Exchange ◯Подпись 🧿Оба		
Размер кли	оча: 512 Минимальный:512 (стандартные размер	ы ключей: <u>512</u>)	
	• Автоматическое имя контейнера клк	ча Заданное пользователем имя контейнера ключа	
	🔽 Пометить ключ как экспортируемый		
	Использовать локальное хранилище Сохраняет сертификат в локалы вместо пользовательского хрании Не устанавливает корневой серт Необходимо быть администратор локальное хранилище.	компьютера для сертификата ном хранилище пища сертификатов. ификат ЦС. ром, чтобы создать	
Дополнительные п	араметры:		
Формат запр	oca: CMC PKCS10		
Алгоритм хеширова	ния: ГОСТ Р 34.11-94 😒		
	Используется только для подписания	sanpoca.	
	Сохранить запрос		
		🐖 📁 🙉 🍙 🕣 🦳	

Интерфейс БиоДСЧ. При необходимости для контейнера задаётся PIN.

		iii cryptopro.ru	C
Службы сертифи	кации Active Directory (Microsoft)		КРИПТО-ПРО КриптоПро
ОАвтоматическое им	ия контейнера ключа ОЗаданное г	пользователем имя контейнера ключа	
🛃 Пометить ключ как	экспортируемый		
Использовать лока	льное хранилище к		
Сохраняет серт вместо попьзова Не устанаеливае Необходимо быт покальное хрании покальное хрании	идикат в покально, тельского хранили т корневой сертид ь администраторо лище.	CryptoPro CSP random number general Move mouse pointer	itor
CMC PKCS	10		
Формат запроса: CIVIC PRC3			
ритм хеширования: ГОСТ Р 34.11-94 📀			Cancel
Используется только Сохранить запрос	о для подписания за		
Атрибуты:		Создание запроса	





При желании, после установки, можно удостовериться в наличии сертификата в хранилище командой

./certmgr -list -store my

	iii cryptopro.ru C
Службы сертификации Active Directory (М	
Спужбы сертификации Active Directory (<i>Microsoft</i>) — CRYPTO-PRO Сертификат установлен	Test Center Mac-Admin:bin admin\$./certmgr -list -store my Certmgr 1.0 (c) "CryptoPro", 2007-2010. program for managing certificates, CRLs and stores WARNING: Legacy parameter: "-store my"
Новый сертификат успешно установлен.	Issuer : E=support@cryptopro.ru, C=RU, L=Moscow, 0=CRYPT0-PR0 LLC, CN=CRYPT0-PR0 Test Center 2 : E=stunnel_clnt, CN=stunnel_clnt, 0U=stunnel_clnt, 0=stunnel_clnt, L=stunnel_ clnt, S=stunnel_clnt, C=RU Serial : 0x12000A5B0AFAF66A47A5C085D000000A5B0A SHA1 Hash : 0x553d561e768a5346fc85585a37cfce126d83d91 SubjKeyID : C2as52443af1e7fbc22bace12081ee706a4a1149 Signature Algorithm : fOCT P 34.11/34.10=2001 PublicKey Algorithm : fOCT P 34.11/34.10=2001 (S12 bits) Not valid before : 12/11/2015 07:15:127 UTC Not valid before : 1021/02/2016 07:15:127 UTC PrivateKey Link : Yes Container : HOIMAGE\\b6491d25.000\72E3 Provider Name : Crypto-Pro COST R 34.10=2001 KC1 CSP Provider Name : Crypto-Pro COST R 34.10=2001 KC1 CSP Provider Name : 13.6.1.5.5.7.3.2
	[ErrorCode: 9x00000000] Mac-Admin:Din admins



Далее производится экспорт личного сертификата в файл, путь к которому указан в файле конфигурации, используя команду

./certmgr -export -store my -dn stunnel_clnt -dest /Users/admin/Documents/stun_cert.crt

	🗎 cryptopro.ru 🖒
Службы сертификации Active Directory (N цифровои подписи в соответстви	icrosoft) исторати Р. • • • • • • • • • • • • • • • • • •
использования сертификатов отк электронной цифровой подписи в	JUITENX KINO- Mac-Admin:bin admin\$./certmgr -export -store my -dn stunnel_clnt -dest /Users/admin/Documents/stul n_cert.crt COOTBBTCTB Certmgr 1.0 (c) "CryptoPro", 2007-2010. program for managing certificates, CRLs and stores
Использование:	WARNING: Legacy parameter: "-store my" Exporting:
Для <u>КриптоПро CSP</u> версии 2.0 К	
виде отдельного дистрибутива. Д состав <u>КриптоПро CSP</u> на всех О	IM <u>КриптоП</u> 1 IS <u>КриптоП</u> 1 IS ине треб Center 2 S ине треб Subject : E=stunnel_clnt, CN=stunnel_clnt, 0U=stunnel_clnt, 0=stunnel_clnt, L=stunnel_
Для использования протокола SS	L (TLS) npe, cint, S=stunnel_cint, C=RU
"Сертификат пользователя УЦ". З <u>Про</u> .	TO MCMHO & SHA1 Hash : 0x1200000000000000000000000000000000000
Тестовая страница для установле аутентификацией. Для работы те соединений.	PublicKey Algorithm : FOCT P 34.10-2001 (512 bits) Hws 3augual Not valid before : 12/02/2016 07:15:27 UTC TOBOÑ CTPA PrivateKey Link : Yes Container : HDIMAGE\\b6491d25.000\72E3 Provider Name : Crypto-Pro GOST R 34.10-2001 KC1 CSP Provider Tho : ProvVipe: 75, KeySpec: 1, Flags: 0x0
Документация:	Extended Key Usage : 1.3.6.1.5.5.7.3.2
Онлайн-версия руководства прог	раммистад Export complete
Смотрите также:	[ErrorCode: 0x00000000] Mac-Admin:bin admin\$
Подробнее о протоколе TLS	з Подписка на обновления
Спецификация протокола TLS - R	FC 2246
Описание протокола TLS (SSL) M	icrosoft technet (eng)
Описание протокола TLS (SSL) (р	ус) УЧитать
🖶 Страница для печати	
	🐖 🥣 🗊 🙈 🍙 🕋 🎧 🥵 🎦 🦱 🔚 👘

Запуск утилиты с указанием пути к конфигурационному файлу и просмотр идентификатора запущенного процесса производятся командами /stunnel_thread /Users/admin/Documents/stunnel.conf и cat/Users/admin/Documents/stunnel.pid соответственно.

		🗎 cryptopro.ru	Ċ
c	лужбы сертификации Active Directory (N		КРИПТО-ПРО КриптоПро TLS
	использования сертификатов отк	рытых ключей, также используются алгоритмы проверки	
	электронной цифровой подписи в	а соответствии с ГОСТ Р 34.10-2001 или ГОСТ Р 34.10-94.	5
	Использование:	[Mac-Admin:sbin admin\$./stunnel_thread /Users/admin/Document [Mac-Admin:sbin admin\$ top	s/stunnel.conf
	Для <u>КриптоПро CSP</u> версии 2.0 К	[Mac-Admin:sbin admin\$ cat /Users/admin/Documents/stunnel.pid 31788	
	виде отдельного дистрибутива. Д	Mac-Admin:sbin admin\$	
	состав КриптоПро CSP на всех О	С и не требует отдельной установки.	
	Для использования протокола SS	SL (TLS) предварительно получите сертификат по шаблону	
	"Сертификат пользователя УЦ". З	Это можно сделать на тестовом Удостоверяющем центре Крипто-	Вхол
	Про.		Блод
	Toppop of the second second		Имя пользователя: "
		сторой страници и необходинения с сервером с двусторонней	
	соединений.	стовой страницы неооходимо разрешить порт 4444 для исходящих	Пароль: *
	Документация:		Вход Регистрация
		2.0	БХОД ДЛЯ ДИЛЕРОВ

Следует сделать пояснение: рассматриваемый случай не подразумевает проверку сертификата сервера, на который организуется доступ (verify=0). Если указанная проверка всё же требуется, можно указать значение опции verify = 1 или 2 Тогда следует скачать и установить в хранилище root корневой сертификат удостоверяющего центра, выпустившего сертификат веб-сервера <u>https://www.cryptopro.ru/ui/</u> и

Далее производится попытка подключения. Вводится PIN на контейнер, если при генерации оный был установлен.



При успешном соединении отображается следующее окно.

12.02.2016 7:25:27

ValidUntil (Действителен до)

	192.168.154.128	0	0 1 0	
Защищенное соединение устано	овлено			
Сертификат пользователя предостав	лен			
Для отображения данных сертификата Request.ClientCertificate(Key[SubField	пользователя используется функция 1])			
Поле сертификата 1	Значен	ние		
Issuer (Издатель)	EMAIL=support@cryptopro.ru, C=RU, L=Moscow, O=CRYPTO-PRO LLC, CM	N=CRYPTO-PRO Test Center 2		
Subject (Владелец)	EMAIL=stunnel_clnt, CN=stunnel_clnt, OU=stunnel_clnt, O=stunnel_clnt, L=stunnel_clnt, S=stunnel_clnt, C=RU			
SerialNumber (Серийный номер)	12-00-0a-5b-8a-fa-fb-6a-47-a5-cb-85-dd-00-00-00-0a-5b-8a			
ValidFrom (Действителен с)	12.11.2015 7:15:27/td>			



Ошибки в работе

В случае возникновения проблем с подключением следует изучить содержимое файла журнала событий, который создаётся автоматически при первом запуске службы по указанному в конфигурационном файле пути. При некорректно сформированном конфигурационном файле утилита не запустится, при этом файлы журнала и идентификатора процесса могут не создаваться.

При отсутствии в хранилище корневого сертификата веб-сервера к которому производится подключение (если в конфигурационном файле имеется требование проверки), в журнале событий отобразится сообщение следующего плана:

16:12:39 L0G3[927:123145307148288]: Error 0x20 ((unknown)) returned by CertVerifyCertificateChainPolicy! 16:12:39 L0G3[927:123145307148288]: Error 0x20 when validate certificate

```
16:12:39 L0G3[927:123145307148288]: Error 0x80092004 returned by VeryfySertChain
16:12:39 L0G3[927:123145307148288]: **** Error 0x80092004 authenticating server credentials!
16:12:39 L0G5[927:123145307148288]: Connection reset: 0 byte(s) sent to SSL, 0 byte(s) sent to socket
16:12:39 L0G7[927:123145307148288]: delete c->hContext]
16:12:39 L0G7[927:123145307148288]: delete c->hClientCreds
16:12:39 L0G7[927:123145307148288]: delete c->hClientCreds
16:12:39 L0G7[927:123145307148288]: delete c->hClientCreds
16:12:39 L0G7[927:123145307148288]: nemote socket (FD=17) closed
16:12:39 L0G7[927:123145307148288]: Local socket (FD=10) closed
16:12:39 L0G7[927:123145307148288]: Service [https] finished (1 left)
16:12:39 L0G7[927:123145307148288]: str_stats: 6 block(s), 768 data byte(s), 444 control byte(s)
16:12:39 L0G7[927:123145307148288]: str_stats: 128 byte(s) at /dailybuildsbranches/CSP_4_0/CSPbuild/CSP/sa
```

В случае ввода неправильного PIN от контейнера некоторого количества раз – соединение не удастся, а в журнале отобразится следующая ошибка.

16:24:40 L0G5[958:123145307148288]: 1405 bytes of handshake(in handshake loop) data received. 16:24:44 L0G5[958:123145307148288]: 935 bytes of handshake data sent 16:24:44 L0G3[958:123145307148288]: **** Error 0x80090304 returned by InitializeSecurityContext (2) 16:24:44 L0G3[958:123145307148288]: Couldn't complete RENEGOTIATE 16:24:44 L0G3[958:123145307148288]: error on SSPI_read 16:24:44 L0G5[958:123145307148288]: Connection reset: 340 byte(s) sent to SSL, 0 byte(s) sent to socket 16:24:44 L0G7[058:123145307148288]: free Buffers 16:24:44 L0G7[058:123145307148288]: delete c=bContext