Настройка двухфакторной аутентификации в Stunnel

Параметры стенда

ip сервера=10.0.2.15

OS сервера = Ubuntu

Порт сервиса=22

Порт Туннеля=443

Туннелированный сервис = SSH

OS клиента = Ubuntu

За основу настройки сервера и клиента была взята эта статья. Для настройки клиента с аутентфикацией по ГОСТу можно можно воспользоваться данной статьей

Настройка сервера

Выполним первичную настройку сервера:

Первичная настройка сервера

```
#  firewall     443
sudo ufw allow 443/tcp
sudo ufw allow 22/tcp
sudo ufw enable

#
sudo apt-get update
sudo apt-get upgrade
sudo apt-get install stunnel4 openssl opensc libengine-pkcs11-openssl1.1

#         ssh
sudo apt-get install ssh

#    (      )
sudo systemctl start ssh

#   pkcs11
wget https://download.rutoken.ru/Rutoken/PKCS11Lib/Current/Linux/x64/librtpkcs11ecp_2.0.5.1-1_amd64.deb
sudo dpkg -i librtpkcs11ecp_2.0.5.1-1_amd64.deb

#
sudo mkdir /var/lib/stunnel4/certs
```

Создадим файл **/etc/stunnel/stunnel.conf** с конфигурацией stunnel

/etc/stunnel/stunnel.conf

```
; **************************************************************************
; * Global options                                                         *
; **************************************************************************

;
debug = 7
; -
output = /var/lib/stunnel4/stunnel.log
;   syslog
syslog = no


; **************************************************************************
; * Service defaults may also be specified in individual service sections  *
; **************************************************************************

; /
cert = /etc/stunnel/servercert.pem
key = /etc/stunnel/serverkey.pem

;  . 0 -  , 1 -   , 2 -  , ...
verify = 2

;    .
;   .      -
CApath = /var/lib/stunnel4/certs

;   SSLv2
options = NO_SSLv2

; **************************************************************************
; * Service definitions (remove all services for inetd mode)               *
; **************************************************************************


[ssh]
;    :   .  accept = 192.168.0.1:443
accept = 443
;    :   .  connect = 127.0.0.1:22
connect = 22
```

Создадим необходимый набор ключевых пар и сертификатов для УЦ, сервера и клиента.

Упрощенное создание ключа и сертификата на токене

Для упрощения процесса создания ключей и заявок на сертификат на токене, а также их импорт на него можно воспользоваться утилитой по работе с токеном.

Создание ключей и сертификатов

```
#
sudo openssl req -nodes -new -days 365 -newkey rsa:2048 -x509 -keyout cakey.pem -out cacert.pem

#
sudo openssl genrsa -out serverkey.pem 2048
#
sudo openssl req -new -out server.req -key serverkey.pem
#
sudo openssl x509 -req -in server.req -CAkey cakey.pem -CA cacert.pem -out servercert.pem -CAcreateserial


#
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so --keypairgen --key-type rsa:2048 -l --id 454647
#
openssl
OpenSSL> engine dynamic -pre SO_PATH:/usr/lib/x86_64-linux-gnu/engines-1.1/pkcs11.so -pre ID:pkcs11 -pre
LIST_ADD:1 -pre LOAD -pre MODULE_PATH:librtpkcs11ecp.so
...
OpenSSL> req -engine pkcs11 -new -key "pkcs11:id=%45%46%47" -keyform engine -out client.req -subj "/C=RU
/ST=Moscow/L=Moscow/O=Aktiv/OU=dev/CN=testuser/emailAddress=testuser@mail.com"

#
sudo openssl x509 -req -in client.req -CAkey cakey.pem -CA cacert.pem -out clientcert.pem -CAcreateserial
#
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -l -y cert -w ./clientcert.pem --id 454647

sudo mv serverkey.pem /etc/stunnel/
sudo mv servercert.pem /etc/stunnel/

sudo mv clientcert.pem /var/lib/stunnel4/certs
sudo mv cacert.pem /var/lib/stunnel4/certs

cd /var/lib/stunnel4/certs

#
function get_hash()
{
        local file=$1
        openssl x509 -noout -hash -in "$file"
}

#
sudo ln -s cacert.pem "`get_hash cacert.pem`.0"
sudo ln -s clientcert.pem "`get_hash clientcert.pem`.0"

#   stunnel
sudo systemctl restart stunnel4
```

Настройка Stunnel на клиенте

Произведем первичную настройку на стороне клиента.

Первичная настройка клиента

```
#
sudo apt-get update
sudo apt-get upgrade
sudo apt-get install stunnel4 openssl opensc libengine-pkcs11-openssl1.1

#   pkcs11
wget https://download.rutoken.ru/Rutoken/PKCS11Lib/Current/Linux/x64/librtpkcs11ecp_2.0.5.1-1_amd64.deb
sudo dpkg -i librtpkcs11ecp_2.0.5.1-1_amd64.deb

cp cacert.pem /etc/stunnel/cacert.pem
```

Узнаем где находится директория с файлом конфигурации openssl.

Получения директории с файлом конфигурации openssl

```
openssl version -d
```

В данный конфигурационный файл **/path/to/openssl.cnf** добавим следующие строчки:

Настройка openssl

```
#   :
openssl_conf = openssl_def

...

#   :
# OpenSSL default section
[openssl_def]
engines = engine_section

[engine_section]
pkcs11 = pkcs11_section

[pkcs11_section]
engine_id = pkcs11
dynamic_path = /usr/lib/x86_64-linux-gnu/engines-1.1/pkcs11.so #
MODULE_PATH = /usr/lib/librtpkcs11ecp.so #
default_algorithms = CIPHERS, DIGEST, PKEY, RAND
```

Сконфигурируем клиент stunnel через файл **/etc/stunnel/stunnel.conf**:

/etc/stunnel/stunnel.conf

```
;      -
debug = 7
output = /var/lib/stunnel4/stunnel.log

;    TLSv1.2
sslVersion=TLSv1.2

;
engine=pkcs11

;
[ssh]
;  engine,
engineId=pkcs11

;   2 (  )
verify = 2
;
CAFile = /etc/stunnel/cacert.pem
;
cert=pkcs11:id=%45%46%47

;     .
key=pkcs11:id=%45%46%47
options = NO_SSLv2


client = yes
accept = 127.0.0.1:22
connect = 10.0.2.15:443
```

Попробуем создать соединение и подключиться по ssh:

Подключение по ssh через туннель

```
sudo stunnel
ssh user@127.0.0.1
```

Если соединение установлено успешно, то мы получим следующий вывод:

```
lo1ol@lo1ol-VirtualBox:~$ sudo stunnel
Enter PKCS#11 token PIN for Rutoken ECP <no label>:
lo1ol@lo1ol-VirtualBox:~$ ssh lo1ol@127.0.0.1
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:nyrOa7FL5fHgZueXTTVfD/YHwuRZKQanSXiQEcUnq3g.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
lo1ol@127.0.0.1's password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-40-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


207 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
*** System restart required ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

lo1ol@lo1ol-VirtualBox:~$
```

Если соединение не будет установлено, то можно посмотреть логи **/var/lib/stunnel4/stunnel.log**.