Инструкция

по установке и настройке доступа к мСМДО

«G-SecTLS» сервер

Минск 2023

Оглавление

[1. Введение 3](#_Toc127544644)

[2. Нормативные ссылки 4](#_Toc127544645)

[3. Обозначения и сокращения 5](#_Toc127544646)

[4. Возможные схемы использования GsecTLS сервера для доступа к мСМДО 6](#_Toc127544647)

[5. Порядок установки «GsecTLS» сервер 8](#_Toc127544648)

[6. Настройка G-Seс TLS сервера 9](#_Toc127544649)

[6.1. Создание каталога логирования 9](#_Toc127544650)

[6.2. Редактирование файла host 9](#_Toc127544651)

[6.3. Первичное обновление сертификатов 11](#_Toc127544652)

[6.4. Настройка файла конфигурации 12](#_Toc127544653)

[6.5. Настройка автоматического обновления СОС 14](#_Toc127544654)

[6.6. Проверка запуска сервер GSecTLS сервера 15](#_Toc127544655)

[7. Проверка работоспособности 16](#_Toc127544656)

[7.1. Проверка доступности по порту 16](#_Toc127544657)

[7.2. Проверка доступа на API мСМДО 16](#_Toc127544658)

# Введение

Данная инструкция предназначена для настройки и использования программного обеспечения «GsecTLS» сервер.

«GsecTLS» сервер предназначен для криптографической защиты информации и аутентификации сторон при взаимодействии в информационной системе организации с применением алгоритмов электронной цифровой подписи и транспорта ключа согласно требованиям СТБ 34.101.45-2013.

Программное обеспечение представляет собой локальный обратный прокси-сервер. «GsecTLS» сервер принимает запросы на локальном интерфейсе по заданным портам и перенаправляет их на конечный сервис через «GsecTLS» сервер с использованием протокола защиты транспортного уровня TLS. Таким образом, «GsecTLS» сервер может использоваться не только для браузеров, но и для других приложений, работающих по порту.

# Нормативные ссылки

Настоящая Инструкция разработана в соответствии с требованиями следующих нормативных правовых и технических нормативных правовых актов, а также локальных распорядительных документов НЦЭУ:

* Указ Президента Республики Беларусь от 16.04.2013 № 196 «О некоторых мерах по совершенствованию защиты информации»;
* Закон Республики Беларусь от 10.11.2008 г. № 455‑З «Об информации, информатизации и защите информации»;

- СТБ.34.101.31-2011 «Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности»;

- СТБ.34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей»;

- СТБ.34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых»;

- СТБ.34.101.65-2014 «Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS)»;

- СТБ.34.101.47-2017 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел»;

# Обозначения и сокращения

В настоящей Инструкции используются следующие обозначения и сокращения:

|  |  |  |
| --- | --- | --- |
| ИБ | – | информационная безопасность; |
| ОЗУ | – | оперативное запоминающее устройство; |
| ОС | – | операционная система; |
| ПЭВМ  | ‒ | персональная электронно-вычислительная машина; |
| СКЗИ | – | средства криптографической защиты информации; |
| СОС | – | список отозванных сертификатов |
| РМ | – | рабочее место |
|  |  |  |

Программное обеспечение «GsecTLS» сервер предназначен для работы на ПЭВМ (ЭВМ), под управлением следующих операционных систем:

Операционная система Linux

– Ubuntu 18.04 версии ядра 4.18

«GsecTLS» сервер предназначен для обеспечения функций криптографической защиты информации.

**ВНИМАНИЕ!** **Шифрованию подлежит канал связи между сервером ВСЭД организации и НЦЭУ.**

Серверное приложение «GsecTLS» рекомендовано к установке при следующих условиях:

- сервер ВСЭД располагается в инфраструктуре организации;

- количество пользователей ВСЭД более 15;

- в организации объем трафика превышает 100 писем в месяц;

- при использовании корпоративной сети территориально распределенными организациями и размещении сервера приложений ВСЭД у вышестоящей организации.

# Возможные схемы использования GsecTLS сервера для доступа к мСМДО

Программа реализации защищенного взаимодействия должна эксплуатироваться на ЭВМ и устройствах со следующими техническими характеристиками:

- Тактовая частота процессора не менее 2 ГГц;

- Объем ОЗУ не менее 2 ГБ;

- Объем памяти на жестком диске не менее 80 ГБ.

Возможные схемы использования GsecTLS сервера для доступа к мСМДО:

1. Рабочее место пользователя и сервер ВСЭД расположены на одном ПК с ОС Ubuntu 18.04 версии ядра 4.18



1. Сервер ВСЭД находится отдельно от рабочих мест пользователей и расположен на ПК с ОС Ubuntu 18.04 версии ядра 4.18
2. Сервер ВСЭД находится отдельно от рабочих мест пользователей и расположен **не** на ПК с ОС Ubuntu 18.04 версии ядра 4.18



# Порядок установки «GsecTLS» сервер

Для установки «GsecTLS» сервер необходимо:

1. загрузить дистрибутив GsecTLS сервер на ПВЭМ.

2) запустить файл “**GSecTLS\_1.1.0-1\_amd64.deb**” на сервере, введя в терминале команду: sudo apt install /home/user/GSecTLS\_1.1.0-1\_amd64.deb

Ввести “Y” для продолжения и завершения процесса установки сервера, рисунок 11.



Рисунок 11 – Установка «GsecTLS» сервер

|  |  |
| --- | --- |
|  | Программное обеспечение устанавливается по следующим путям:/usr/local/etc/GSecTLS//usr/local/sbin/  |

# Настройка G-Seс TLS сервера

**ВАЖНО !**

В соответствии от провайдера используются следующие IP адреса:

БОТ – 10.252.0.35

БФТ – 10.53.8.35

Другие – 10.101.1.35

Internet – 185.227.96.96

## Создание каталога логирования

После успешной установки сервера нужно настроить логирование работы сервера. Для этого надо создать каталог:

 mkdir /var/log/GsecTLS/

Установить в созданном каталоге при помощи *chmod* права, достаточные для его редактирования пользователем, под учетной записью которого будет запускаться сервер.

## Редактирование файла host

После успешной установки сервера нужно настроить файл host/ Для этого открываем файл host:

sudo nano /etc/hosts

В файл hosts следует добавить следующие записи.

Если используются схемы подключения 1,2:

**Интернет**

127.0.0.1 gw.gov.by

127.0.0.1 esiful-idp.gov.by

127.0.0.1 ei.gov.by

127.0.0.1 is.gov.by

127.0.0.1 am.gov.by

127.0.0.1 gw.nces.by

127.0.0.1 esiful-idp.nces.by

127.0.0.1 ei.nces.by

127.0.0.1 is.nces.by

127.0.0.1 am.nces.by

**БTK и другие:**

127.0.0.1 gw.gov.by

127.0.0.1 esiful-idp.gov.by

127.0.0.1 ei.gov.by

127.0.0.1 is.gov.by

127.0.0.1 am.gov.by

127.0.0.1 gw.nces.by

127.0.0.1 esiful-idp.nces.by

127.0.0.1 ei.nces.by

127.0.0.1 is.nces.by

127.0.0.1 am.nces.by

**БОТ:**

127.0.0.1 gw.gov.by

127.0.0.1 esiful-idp.gov.by

127.0.0.1 ei.gov.by

127.0.0.1 is.gov.by

127.0.0.1 am.gov.by

127.0.0.1 gw.nces.by

127.0.0.1 esiful-idp.nces.by

127.0.0.1 ei.nces.by

127.0.0.1 is.nces.by

127.0.0.1 am.nces.by

**БФТ:**

127.0.0.1 gw.gov.by

127.0.0.1 esiful-idp.gov.by

127.0.0.1 ei.gov.by

127.0.0.1 is.gov.by

127.0.0.1 am.gov.by

127.0.0.1 gw.nces.by

127.0.0.1 esiful-idp.nces.by

127.0.0.1 ei.nces.by

127.0.0.1 is.nces.by

127.0.0.1 am.nces.by

Если схема подключения будет 3



В случае, если в вашей организации отсутствует DNS-сервер, то на сервере ВСЭД в hosts необходимо добавить следующие записи:

<IP адрес сервера GsecTLS> gw.gov.by

<IP адрес сервера GsecTLS> esiful-idp.gov.by

<IP адрес сервера GsecTLS> ei.gov.by

<IP адрес сервера GsecTLS> is.gov.by

<IP адрес сервера GsecTLS> am.gov.by

<IP адрес сервера GsecTLS> gw.nces.by

<IP адрес сервера GsecTLS> esiful-idp.nces.by

<IP адрес сервера GsecTLS> ei.nces.by

<IP адрес сервера GsecTLS> is.nces.by

<IP адрес сервера GsecTLS> am.nces.by

В случае, если в вашей организации используется DNS-сервер, то на DNS-сервере необходимо добавить следующие A-записи:

<IP адрес сервера GsecTLS> gw.gov.by

<IP адрес сервера GsecTLS> esiful-idp.gov.by

<IP адрес сервера GsecTLS> ei.gov.by

<IP адрес сервера GsecTLS> is.gov.by

<IP адрес сервера GsecTLS> am.gov.by

<IP адрес сервера GsecTLS> gw.nces.by

<IP адрес сервера GsecTLS> esiful-idp.nces.by

<IP адрес сервера GsecTLS> ei.nces.by

<IP адрес сервера GsecTLS> is.nces.by

<IP адрес сервера GsecTLS> am.nces.by

## Первичное обновление сертификатов

В связи с выпуском СОС КУЦ, требуется вручную заменить в программном обеспечении GsecTLS файл (**trusted.cer.pem**).

Там же необходимо скачать СОС РУЦ переименовав его в ruc.crl.pem.

Файлы можно скачать, перейдя по ссылке:

|  |  |
| --- | --- |
| Ваш провайдер | Адрес |
| БФТ | http://10.53.8.35:10480/  |
| БОТ | http://10.252.0.35:10480/  |
| Все остальные | http://10.101.1.35:10480/  |
| Internet | http://185.227.96.96:10480/ |



Заменить сертификаты в PEM формате

- сертификат УЦ (trusted.cer.pem)

- СОС УЦ (ruc.crl.pem).

поместив скачанные в директорию

/usr/local/etc/GSecTLS/certs/

## Настройка файла конфигурации

Заменить файл конфигурации **GSecTLS.conf** в директории **usr/local/etc/GSecTLS** на преднастроенный файл, размещенный вместе с инсталляционным пакетом.

Для этого скачиваете файл в зависимости от провайдера

|  |  |
| --- | --- |
|  Провайдер | Конфигурационный файл |
| БФТ | GSecTLS\_bft.conf |
| БОТ | GSecTLS\_bot.conf |
| Другие | GSecTLS\_vpn.conf |
| Internet | GSecTLS\_internet.conf |

Для этого переименовываете его в **GSecTLS.conf** и заменяетев директории **usr/local/etc/GSecTLS.**

Пример для ОС Linux “/usr/local/etc/GSecTLS/GSecTLS.conf”

user root;

daemon on;

master\_process on;

worker\_processes auto;

worker\_priority -20;

worker\_rlimit\_nofile 262144;

error\_log /var/log/GsecTLS/GsecTLS.log info;

events {

 multi\_accept on;

 worker\_connections 4096;

}

stream {

 proxy\_ssl on;

 proxy\_ssl\_protocols TLSv1.2;

 proxy\_ssl\_ciphers DHT-BIGN-BELT-CTR-MAC-HBELT;

 proxy\_ssl\_server\_name on;

 proxy\_ssl\_session\_reuse on;

 proxy\_ssl\_verify on;

 proxy\_ssl\_verify\_depth 3;

 proxy\_ssl\_trusted\_certificate certs/trusted.cer.pem;

 proxy\_ssl\_crl certs/ruc.crl.pem;

#====================================================

# AISMV prod

#====================================================

 server {

 listen \*:40001;

 proxy\_pass *<ipaddr>*:11001;

 proxy\_ssl\_name AISMVprod.GsecTLS.nces;

 }

#====================================================

# AISMV dev

#====================================================

 server {

 listen \*:40002;

 proxy\_pass *<ipaddr>*:11002;

 proxy\_ssl\_name AISMVdev.GsecTLS.nces;

 }

#====================================================

# Test page

#====================================================

 server {

 listen \*:9080;

 proxy\_pass *<ipaddr>*:11000;

 proxy\_ssl\_name TestPage.GsecTLS.nces;

 }

}

После замены нужно сохранить внесенные изменения и запустить GsecTLS:

sudo GSecTLS

## Настройка автоматического обновления СОС

Для корректной работы сервера GsecTLS, необходимо настроить синхронизацию времени (отредактировать файл timesyncd.conf).

|  |  |
| --- | --- |
|  | Редактирование timesyncd.conf: Файл располагается по следующему пути:/etc/systemd/timesyncd.conf NTP=ipaddresssystemctl restart systemd-timesyncdtimedatectl set-timezone Europe/Minsk |

Затем следует настроить автообновление СОС. Для этого можно использовать планировщик задач *cron*.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Использование планировщика задач cron для обновления СОС: Открыть на редактирование конфигурацию cron:crontab -eДобавить задание (одной строкой):0 0 \* \* \* wget -O /usr/local/etc/GSecTLS/certs/ruc.crl.pem http://<ipaddr>:10480/files/ruc\_pem.crlГде в *<ipaddr>*указываем адрес в зависимости от провайдера:

|  |  |
| --- | --- |
|  Провайдер | <ipaddr> |
| БФТ | 10.53.8.35 |
| БОТ | 10.252.0.35 |
| Другие | 10.101.1.35 |
| Internet | 185.227.96.96 |

 |

## Проверка запуска сервер GSecTLS сервера

После первичной настройки нужно проверить запускается ли сервер GSecTLS. Сервер запускается командой:

sudo GSecTLS

(sudo GSecTLS -s stop – остановка сервера)

|  |  |
| --- | --- |
|  | Если сервер запустился без ошибок, то не будет никаких сообщений |

В противном случае выведется сообщение об ошибке с указанием

что помешало началу работы сервера.

# Проверка работоспособности

В зависимости от выбранной схемы использования GsecTLS сервера для доступа к мСМДО выполняется следующая проверка настройки и работоспособности

## Проверка доступности по порту

Выполните команду telnet <IP адрес провайдера> 11000



корректное подключение telnet

Так же можно проверит порты 11001 и 11002

## Проверка доступа на API мСМДО

Проверка выполняется в два этапа, сначала получаем токен доступа, потом используя токен доступа проверяем доступ к API мСМДО

**Этап 1.**

Для получения токена делаем запрос в командной строке:

*curl -k -d "scope=application&grant\_type=client\_credentials" -H "Authorization: Basic STJuVGlVUGFPR3NwbmVmTDNua0FyMkM2RGswYTpCSDV2RXNIRVlYSzNmeFJuUUlhQ3h0WkRJMXdh" -H "Content-Type: application/x-www-form-urlencoded" https://gw.gov.by:40001/api/token*



В ответ, на запрос будет получен json объект вида:

*{"access\_token":"b109d1da-0bd6-324d-a96c-75ca662c0dcf","scope":"application","token\_type":"Bearer","expires\_in":3453}*

Срок действия токена 1 час.

**Этап 2.**

Выполняем запрос

*curl -k -d "{ \"filter\": {\"organization\": {\"id\":[{\"value\": \"055ef52c-d037-4202-bc15-fd1f35f293a8\",\"operation\": \"equals\"}]}},\"paging\": {\"page\": 0,\"limit\": 10}}" -H "Authorization: Bearer <****access\_token>****" -H "Content-Type: application/json" -X POST https://gw.gov.by:40001/api/smdo\_nsi\_subscriber/1.0.0/smdo\_nsi/subscriber/v1/search*

подставив значение *access\_token* из предыдущего ответа



***Пример:***

*curl -k -d "{ \"filter\": {\"organization\": {\"id\":[{\"value\": \"055ef52c-d037-4202-bc15-fd1f35f293a8\",\"operation\": \"equals\"}]}},\"paging\": {\"page\": 0,\"limit\": 10}}" -H "Authorization: Bearer b109d1da-0bd6-324d-a96c-75ca662c0dcf" -H "Content-Type: application/json" -X POST https://gw.gov.by:40001/api/smdo\_nsi\_subscriber/1.0.0/smdo\_nsi/subscriber/v1/search*

При корректном доступе в ответ получим список вида

