VPN-CLIENT V1.1
РУКОВОДСТВО АДМИНИСТРАТОРА

Версия документа v1.0

СОДЕРЖАНИЕ

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

- OCSP - Протокол состояния сетевого сертификата - это интернет-протокол, используемый для получения статуса отзыва цифрового сертификата X.509.

2. ОПИСАНИЕ

VPN-CLIENT предназначен для установления шифрованного канала с сервером НИЦ НТ и проксирования HTTP-запросов для домена e-imzo.uz через данный канал. VPN-CLIENT используется совместно с ПО DSV-SERVER. DSV-SERVER при проверки статуса сертификата по протоколу OCSP соединяется к серверу НИЦ НТ посредством VPN-CLIENT.

2.1. Технические требования

Для запуска VPN-CLIENT потребуется:

- ОС Windows 7/10 (x64) или Linux x64 (предпочтительно)
- JRE 1.8
- CPU - 0.2 лог. CPU за 1 сек.
- RAM - не менее 4Гб, так же зависит от объема передаваемого трафика.
- Интернет соединение - для соединения к серверам НИЦ НТ.

2.2. Состав файлов и их описание

Файл	**Описание**
`vpn-client.jar`	Основной запускаемый модуль
`lib/*.jar`	Необходимые библиотеки
`truststore.jks`	Файл хранит доверенные корневые сертификаты. Должен быть недоступен для изменения неавторизованными лицами.
`run.sh`	Shell-скрипт для запуска DSV-SERVER в ОС Linux
`run.bat`	Shell-скрипт для запуска DSV-SERVER в ОС Windows
`client-eimzo.conf`	Файл конфигурации

3. НАСТРОЙКА

3.1. Перенаправление OCSP-запросов

Для отправки OCSP-запросов для домена e-imzo.uz через VPN-CLIENT, добавьте следующую запись:

```
127.0.0.5 e-imzo.uz
```

в файл:

- ОС Windows - `c:\Windows\System32\drivers\etc\hosts`
- ОС Linux - `/etc/hosts`

После добавления выполните команду `ping`:

```
ping e-imzo.uz
```

`Ping` должен отображать IP-адрес `127.0.0.5`

3.2. Настройка nginx

Если на сервере работает nginx, то по умолчанию он настроен слушать все IP-адреса 80-го порта (*:80) и при запуске VPN-CLIENT, он выдаст ошибку "`java.net.BindException: Address already in use`".
Измените настройку nginx так, чтобы он слушал 80 порт конкретного IP-адреса.

Например: если IP-адрес сетевой карты `192.168.0.1` , замените

```
listen *:80
```

на

```
listen 192.168.0.1:80
```

и перезапустите nginx.

В случае web-сервера Apache HTTPd, измените настройку аналогично но в соответствии с документации Apache HTTPd.

3.3. Настройка файла конфигурации

Откройте файл `client-eimzo.conf` и заполните поля:

- `client.keystore.path` - Путь к файлу ключа полученный от НИЦ НТ. Файл обычно начинается с префикса `client-`, заканчивается названием основного

домена и имеет расширение .yks. Путь к файлу и название директорий не должно содержать спец. символов и пробелов.

- `client.keystore.password` - Пароль к файлу ключа полученный от НИЦ НТ.
- `client.keystore.alias` - Алиас ключа полученный от НИЦ НТ.

Пример заполнения файла конфигурации:

```
#Please, Fill in the fields respectively
#Thu Feb 25 17:41:12 UZT 2016

listen.address=127.0.0.5
listen.port=80

connect.address=89.236.209.82
connect.port=9443
connect.failover.address.1=89.236.209.82
connect.failover.port.1=9443

virtual.address=e-imzo.uz
virtual.port=80

client.keystore.path=/vpn-client/client-aaaaa.bb.yks
client.keystore.password=aaaaapass
client.keystore.alias=bb

truststore.path=truststore.jks
truststore.password=12345678
```

Другие поля не рекомендуется изменять, особенно поле `listen.port=80`, т.к. Адрес OCSP сервера указан на каждом изданном НИЦ НТ сертификате (`http://e-imzo.uz/cams/ocsp`) и подключение идет по TCP-порту 80.
Поле `listen.address` можно заменить на IP-адрес сетевой карты которая подключена к локальной сети (не к Интернету), если DSV-SERVER работает на другом сервере. В данном случае следует прописать IP-адрес сервера VPN-CLIENT в `hosts` файле на сервере где запущен DSV-SERVER.
Поле `connect.address и connect.port` указывают IP-адрес и порт сервера НИЦ НТ, следовательно, сервер на котором запущен VPN-CLIENT должен иметь доступ по сети к этому IP-адресу и порту.
Поле `truststore.path` содержит путь к файлу, который хранит доверенные корневые сертификаты для VPN и не предназначен для сервиса DSV-SERVER.

4. УСТАНОВКА И ЗАПУСК

Для установки, извлеките файлы из архива в директорию на сервере. Путь и название директорий не должно содержать спец. символов и пробелов.

Откройте консоль, перейдите в директорию где находится файл `vpn-client.jar` и выполните команды:

- На ОС Windows

```
java -jar vpn-client.jar client-eimzo.conf
```

- На ОС Linux

```
java -jar vpn-client.jar client-eimzo.conf
```

приложение будет слушать сокет 127.0.0.5:80, на экране напечатает лог.

```
...
Feb 19, 2021 2:12:30 AM uz.yt.vpn.client.Application main
INFO: VPN-CLIENT v1.1.
Feb 19, 2021 2:12:30 AM uz.yt.vpn.client.Application main
INFO: Trying run configuration in /vpn-client/client-eimzo.conf.
Feb 19, 2022 2:12:30 AM uz.yt.vpn.client.Application main
INFO: Running VPN client on 127.0.0.5:80.
...
```

5. ПРОВЕРКА РАБОТЫ СЕРВИСА

Для проверки работы сервиса выполните команду:

```
curl -v http://e-imzo.uz/cams/ocsp
```

Ответ об успешности соединения

```
*   Trying 127.0.0.5...
* Connected to e-imzo.uz (127.0.0.5) port 80 (#0)
> GET /cams/ocsp HTTP/1.1
> Host: e-imzo.uz
> User-Agent: curl/7.47.0
> Accept: */*
>
< HTTP/1.1 405 Method Not Allowed
< Server: Microsoft-IIS
< Date: Tue, 16 Mar 2021 06:48:31 GMT
< Content-Type: text/html;charset=utf-8
< Content-Length: 1066
< Connection: keep-alive
< Content-Language: en
...
```

Если HTTP код ответа равен “`HTTP/1.1 403 Forbidden`” (или другой), то возможно `hosts` файл настроен не правильно.