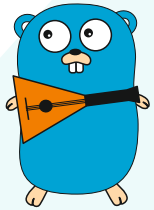
POWER live

Network support

PowerC



Сделано в России
Не зависит от
сторонних библиотек

# PowerSLAL

Статистика AnyConnect пользователей

Для оборудования cisco

# Краткое описание

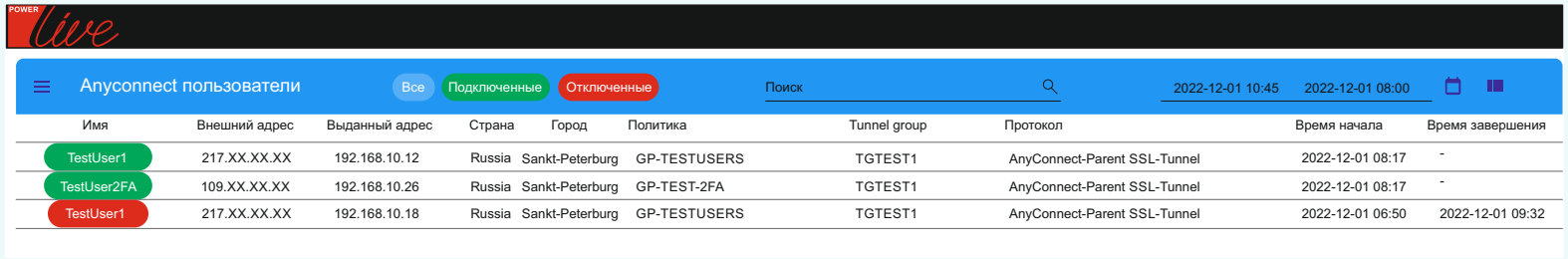
Программное обеспечение предназначено для сбора и хранения информации о подключениях к устройствам безопасности **Cisco ASA/FTD**
Сбор данных производится через функцию посылки сообщения через HTTP с устройства безопасности что обеспечивает гарантированную доставку которую не гарантирует Syslog.

Информация о геолокации может быть получена с различных внешних источников, таких как https://ipstack.com/

В следующей версии будет доступна информация о трафике в каждой сессии пользователя.

Коммерческая версия включает поддержку и обновления.

**Пример:**




| Имя | Внешний адрес | Выданный адрес | Страна | Город | Политика | Tunnel group | Протокол | Время начала | Время завершения |
|---|---|---|---|---|---|---|---|---|---|
| TestUser1 | 217.XX.XX.XX | 192.168.10.12 | Russia | Sankt-Peterburg | GP-TESTUSERS | TGTEST1 | AnyConnect-Parent SSL-Tunnel | 2022-12-01 08:17 | - |
| TestUser2FA | 109.XX.XX.XX | 192.168.10.26 | Russia | Sankt-Peterburg | GP-TEST-2FA | TGTEST1 | AnyConnect-Parent SSL-Tunnel | 2022-12-01 08:17 | - |
| TestUser1 | 217.XX.XX.XX | 192.168.10.18 | Russia | Sankt-Peterburg | GP-TESTUSERS | TGTEST1 | AnyConnect-Parent SSL-Tunnel | 2022-12-01 06:50 | 2022-12-01 09:32 |

# Cisco ASA

**Настройки на  Cisco ASA, пример (192.168.0.5 IP адрес сервера, где запущен контейнер)**

```
logging list SSLUSERS2 level informational
logging list SSLUSERS2 message 605005
logging list SSLUSERS2 message 611103
logging list SSLUSERS2 message 113039
logging list SSLUSERS2 message 722051
logging trap SSLUSERS2
logging host inside

event manager applet StartSession
 event syslog id 722051 occurs 1
 action 0 cli command "call-home send alert-group snapshot profile VPNSH"
 output none
event manager applet EndSession
 event syslog id 113019 occurs 1
 action 0 cli command "call-home send alert-group snapshot profile VPNSH"
 output none

service call-home

call-home
 alert-group-config snapshot
  add-command "show vpn-sessiondb anyconnect"
 profile VPNSH
   destination address http http://192.168.0.5:7002/vpnsession msg-format xml
```

# Запуск сервисов

Установка (на докер сервер): **git clone https://github.com/OlegPowerC/anyconnectusers3.git**
Зайти в папку и запустить файл initdb.sh
**cd anyconnectusersandsyslog**
**chmod 777 initdb.sh**
**./initdb.sh**
Дождаться готовности PSQL сервера Не должно быть сообщений об ошибках и вывод должен быть примерно следующий:

```
server started
/usr/local/bin/docker-entrypoint.sh: sourcing /docker-entrypoint-initdb.d/1_createdb.sh
CREATE ROLE
CREATE DATABASE GRANT
/usr/local/bin/docker-entrypoint.sh: sourcing /docker-entrypoint-initdb.d/2_createtabledb.sh
CREATE TABLE
CREATE TABLE

PostgreSQL init process complete;
ready for start up

LOG: database system is ready to accept connections
```

После этого остановить запущеный контейнер - ctrl+c

Затем можно запускать все контейнеры командой: **docker-compose up -d**
По умолчанию интерфейс доступен по пдресу: HTTP://<ваш docker сервер>:8182

Порты:
SQL порт TCP снаружи 5442 (можно выключить)
Порт TCP 7002 слушает Call-Home сообщения от Cisco ASA

Для геолокации по IP адресу используется сервис
https://ipstack.com/ Необходимо получить API ключ и указать его в файле **docker-compose.yml** (параметр **GEOLOCATIONAPIKEY:)**

# Больше информации

Россия, Санкт-Петербург
Таллинская 6-В
Телефон: +7 (812) 7034338
http://www.powerc.ru
http://www.ciscolive.ru

info@powerc.ru