2020

Инструкция пользователя

ПО ОРГАНИЗАЦИИ ПОДКЛЮЧЕНИЯ К ПОРТАЛУ УЧЕБНОГО КАБИНЕТА ИС ЕПТ РОСТЕХНАДЗОРА С ИСПОЛЬЗОВАНИЕМ ПРОДУКТОВ КОМПАНИИ «С-ТЕРРА СИЭСПИ»

Перечень принятых сокращений

РТН	РосТехНадзор
Производитель	Компания «С-Терра СиЭсПи»
Продукт	Продукт производства компании «С-Терра СиЭсПи»
Портал	Портал учебно-методического кабинета РТН https://eptb.umkrtn.ru/
Пользователь	Организация, обратившаяся по вопросу подключению к Порталу
Партнер	Организация, являющаяся партнером компании «С-Терра СиЭсПи», оказывающая интеграционные услуги Пользователю
ССДЗ	Сертифицированное средство доверенной загрузки

Введение

Инструкция описывает необходимые действия со стороны Пользователя и РТН для организации защищенного подключения к Порталу

Этапы

1. Приобретение Пользователем Продукта
2. Выпуск сертификата и создание дистрибутивов с настройками Продукта специалистами РТН
3. Подключение и первичная настройка Пользователем Продукта
4. Применение к Продукту дистрибутивов, полученных от РТН
5. Самостоятельная настройка Продукта
6. Проверка работы защищенного соединения

1. Приобретение пользователей Продукта

Пользователь своими силами или с помощью Партнера подбирает и приобретает в соответствии с потребностями по количеству рабочих мест и по производительности шифрования решение, руководствуясь рекомендациями Производителя. При выборе С-Терра Клиент КС2 потребуется также дополнительно закупить и установить на рабочие места ССДЗ из списка совместимых:

электронный замок «Соболь», «Аккорд-АМДЗ», АПМДЗ «КРИПТОН-ЗАМОК», «Тринити АПМДЗ», «МАКСИМ-М1».

2. Выпуск сертификата и создание дистрибутивов

Выпуск сертификата и создание дистрибутивов с настройками Продукта выполняется специалистами РТН после получения заявки. К заявке должны быть приложены файлы с лицензиями на Продукт, а также следующая информация для С-Терра Шлюз:

- адреса и маски для внешнего и внутреннего интерфейса шлюза
- маршрут, через который будут доступны ресурсы РТН (например, шлюз по умолчанию)
- маршрут до защищаемой подсети (в случае если она не подключена непосредственно к шлюзу)
- общий кластерный адрес для внутреннего и для внешнего интерфейсов, если используется отказоустойчивая конфигурация

Выполнение следующих этапов зависит от используемого продукта и будет описано отдельно для каждого случая.

Если Пользователь планирует использовать имеющееся оборудование и/или самостоятельно выполнять настройки, то следует перейти к этапу 6.

3. Подключение и первичная настройка

Для С-Терра Клиент предварительных настроек не требуется, за исключением установки и настройки ССДЗ на АРМ пользователя.

4. Применение к Продукту дистрибутивов, полученных от РТН

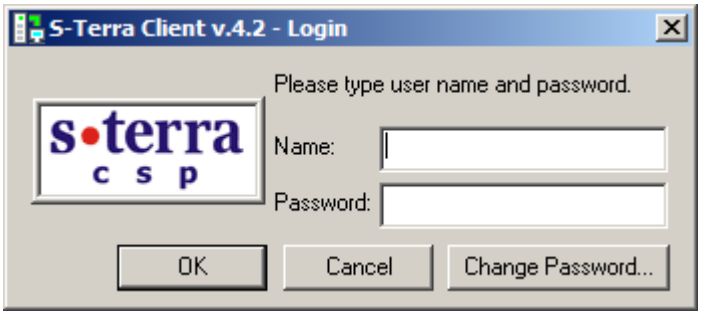
Для каждой отправленной лицензии на С-Терра Клиент РТН пришлет установочные дистрибутивы:

- *setup_product.exe* – дистрибутив VPN-клиента (инструкция по инсталляции)
- *setup_upagent.exe* – дистрибутив агента системы управления (запустить исполняемый файл и следовать указанием мастера установки)

Дистрибутивы необходимо установить на рабочие места.

5. Проверка работы защищенного соединения

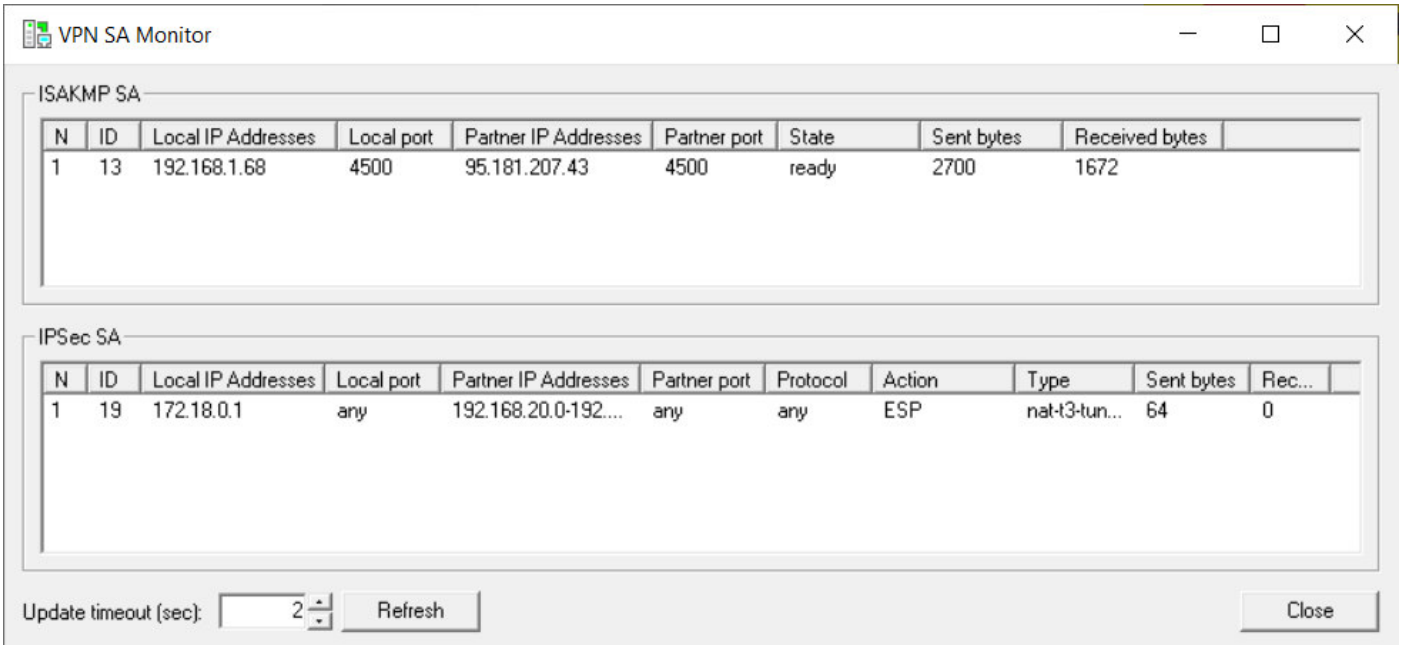
После установки дистрибутива клиента (*setup_product.exe*) VPN-клиент автоматически запустится и выдаст приглашение авторизоваться:



Если окно не появилось, можно выполнить *Login* с помощью иконки Клиента на панели задач (подробнее)

По умолчанию логин *user*, пароль пустой. При необходимости можно изменить пароль (см. инструкцию)

Через некоторое время после выполнения логина должно установиться защищенное соединения. Статус можно проверить в *SA Monitor*, в нем должны присутствовать записи об активных туннелях, например:



После установления защищенного соединения должен стать доступен Портал – откройте в браузере страницу по адресу https://eptb.umkrtn.ru/

В случае если Портал недоступен, убедитесь, что:

1) Выполнен логин в VPN-клиенте. Если в трее статус клиента  то необходимо выполнить логин, нажав *ПКМ* на иконке и выбрать *Login*…
2) Установлен защищенный туннель с ИС ЕПТ. В *VPN SA Monitor* в разделе *ISAKMP SA* должна быть запись о защищенном соединении со статусом (*State*) *ready*. Если статус *incompleted*, значит соединение устанавливается. Если статус не переходит в *ready* в течение нескольких минут, то нужно:
    a. Попробовать отключить антивирус и брандмауэр. Если соединение после этого установилось, то следует разрешить прохождение защищенного трафика – это UDP по 500 и 4500 портам между Local IP address и Partner IP address, которые указаны в *SA Monitor* в разделе *ISAKMP SA*. Это необходимо сделать как на компьютере пользователя, так и корпоративном межсетевом экране.
    b. Обратиться к Партнеру, РТН или службу поддержки Производителя.

3. Подключение и первичная настройка

1) Коммутацию шлюза следует выполнить следующим образом, руководствуясь соответствием интерфейсов:
   Подключение к WAN – порт *eth0* (*GigabitEthernet 0/0*)
   Подключение к LAN – порт *eth1* (GigabitEthernet 0/1)
2) Выполните подключение к Шлюзу по инструкции. Процедуру инициализации выполнять не требуется, она будет выполнена в результате работы скриптов, предоставленных позднее специалистами РТН.
3) Перейдите в консоль операционной системы:
   administrator@sterragate] system
4) Запустите инициализацию датчика случайных чисел:
   root@sterragate:~# /opt/VPNagent/bin/rnd_mgr
   В зависимости от установленного ССДЗ инициализация может происходить интерактивно. В этом случае система запрашивает нажатие определенных символов. Следует следовать указаниям системы до окончания инициализации.
5) Смените пароль для пользователя root командой:
   root@sterragate:~# passwd
   Пароль потребуется при дальнейшем подключении по *SSH* и при переносе файлов

4. Применение к Продукту дистрибутивов, полученных от РТН

Для каждой отправленной лицензии на С-Терра Шлюз РТН пришлет скрипты настройки:

- *setup.sh* – скрипт инициализации
- *setup_product.sh* – скрипт настройки VPN-агента
- *setup_upagent.sh* – скрипт настройки агента системы управления

Их требуется переместить на шлюз в каталог /root. Это можно сделать несколькими способами, подробнее в инструкции.

Далее:

1) перейдите в консоль ОС шлюза (подключившись ко шлюзу по SSH под пользователем *root*; выполнив команду *system* в *Initial CLI*; выполнив команду *run bash* в *Cisco-like* консоли)
2) перейдите в каталог */root* :
   root@sterragate:~# cd /root
3) назначьте файл скрипта инициализации исполняемым:
   root@sterragate:~# chmod +x setup.sh

4) запустите выполнение скрипта:
   root@sterragate:~# ./setup.sh
   Запускать скрипты *setup_product.sh* и *setup_upagent.sh* не требуется, они запускаются автоматически при запуске *setup.sh*

Смените стандартные пароли по инструкции. Следует учесть, что после применения настроек от РТН, возможность входа под пользователем *cscons* пропадает. Попасть в *Cisco-like* консоль возможно из консоли *bash*:

```
root@sterragate:~# cs_console
sterragate>enable
Password: csp (по умолчанию)
sterragate#
```

5. Проверка работы защищенного соединения

1) Если выполнение скрипта завершилось без ошибок, со шлюза должен сдать доступен Портал. Это можно проверить, выполнив ping на адрес 192.168.20.100:
   root@sterragate:~# ping 192.168.20.100
2) Если адрес Портала недоступен следует проверить, построился ли защищенный туннель до площадки РТН:

```
root@gate1:~# sa_mgr show
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 31 (10.0.101.60,4500)-(95.181.207.43,4500) active 1636 1688

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 88 (172.19.0.1,*)-(192.168.20.0-192.168.20.255,*) * ESP nat-t-tunn 464 992
2 89 (172.19.0.1,*)-(192.168.20.0-192.168.20.255,*) * ESP nat-t-tunn 105848 140864
```

3) Если статус туннеля в разделе *ISAKMP connections* отличается от *active* (выделено желтым), то следует проверить доступность шлюза РТН(выделено зеленым):
   root@sterragate:~# ping 95.181.207.43
   Если шлюз РТН доступен, следует обратиться к Партнеру с описанием проблемы
   В ином случае нужно проверить искать причину недоступности шлюза РТН - проверять доступность локального маршрутизатора, через который осуществляется доступ к ресурсам РТН, или обращаться к провайдеру канала.

6. Самостоятельный выпуск дистрибутивов и настройка Продукта Пользователем.

Если у Пользователя уже есть оборудование С-Терра версии 4.2 и, например, оно используется для подключения к другим организациям или к собственным площадкам, потребуется настроить Продукт таким образом, чтобы он работал с 2 удостоверяющими центрами.

Проще всего это сделать при помощи С-Терра КП. В этом случае необходимо в настройках IPSec-правил указать соответствующий сертификат в поле Auth Object (например, Инструкция по созданию клиента, рисунок 159).

Параметры для подключения пришлет РТН вместе с локальным и корневым сертификатами и контейнером с закрытым ключом.

Для С-Терра Шлюз также потребуется перенести в его файловую систему (аналогично этапу 4) скрипт setup_NAT.sh, предварительно отредактировав в нем переменную *WAN_IFACE* – в ней нужно указать название интерфейса в ОС, через который будет уходить трафик в сегмент РТН.

В случае если нет возможности использовать С-Терра КП, то потребуется настраивать Продукт путем изменения LSP-конфигурации.

В качестве примера можно использовать сценарий Добавление на центральном шлюзе аутентификации с использованием сертификатов второго УЦ (Миграция УЦ)