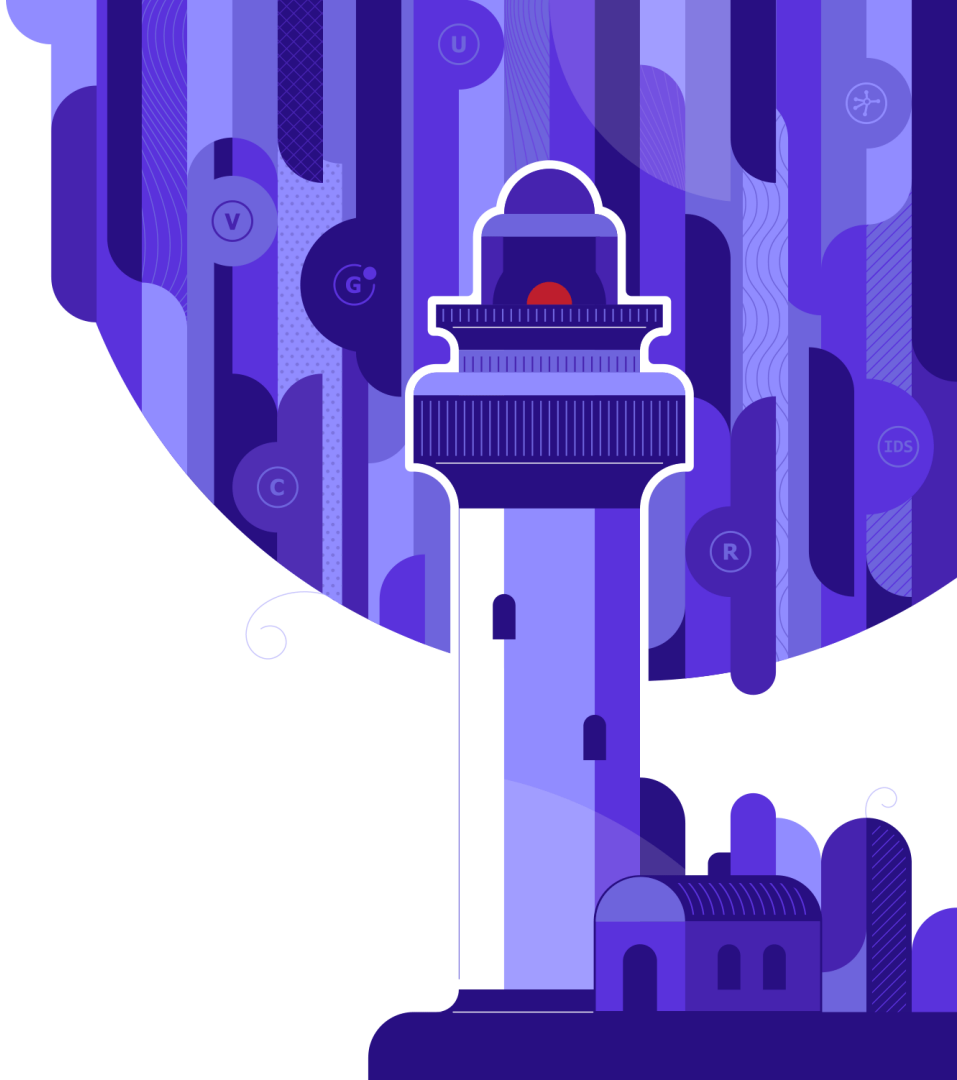
s•terra®

Ваш ориентир в мире безопасности

Версия 4.3
С-Терра КП, С-Терра Клиент



Дмитрий Махоткин,
пресейл инженер,
dmahotkin@s-terra.ru
+7 (499) 940 9001 доб. 181

Москва, 2021

План вебинара

s•terra®

С-Терра КП – централизованное управление

- Как С-Терра КП управляется VPN устройствами;
- Как разграничить доступ администраторов к VPN устройствам;
- Как обновить ключи сразу на всех С-Терра Клиент;
- Что будет, если С-Терра КП выйдет из строя, как сделать backup?

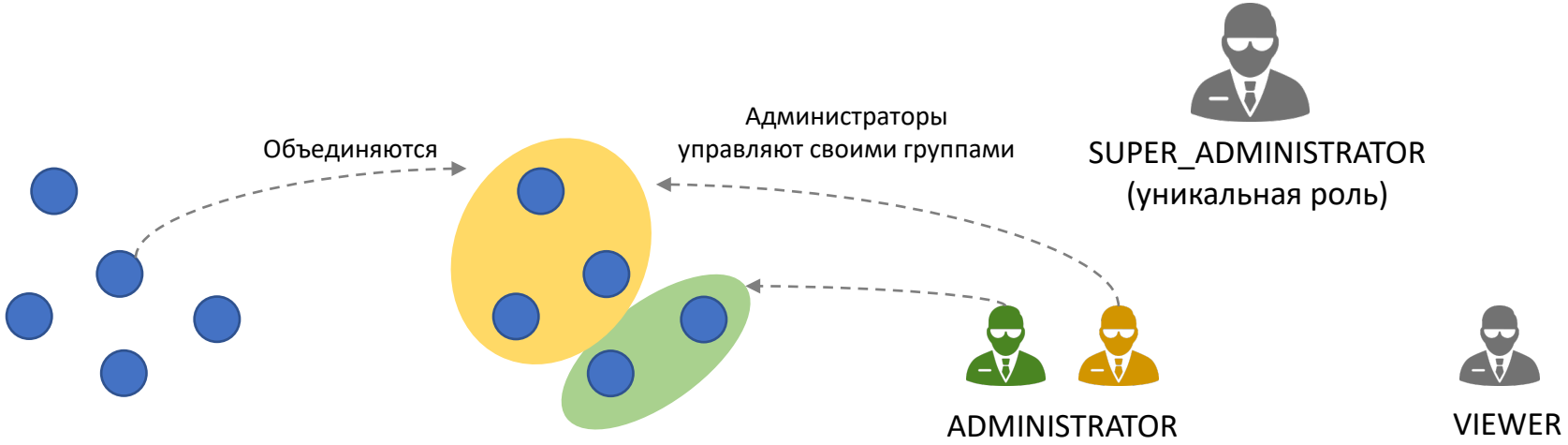
С-Терра Клиент – клиентское ПО для Windows, Astra Linux

- Как автоматизировать выпуск множества С-Терра Клиент;
- Как обеспечить двухфакторную аутентификацию пользователя;
- Как настроить прозрачный режим работы;
- Почему «отваливается» RDP в процессе установки?

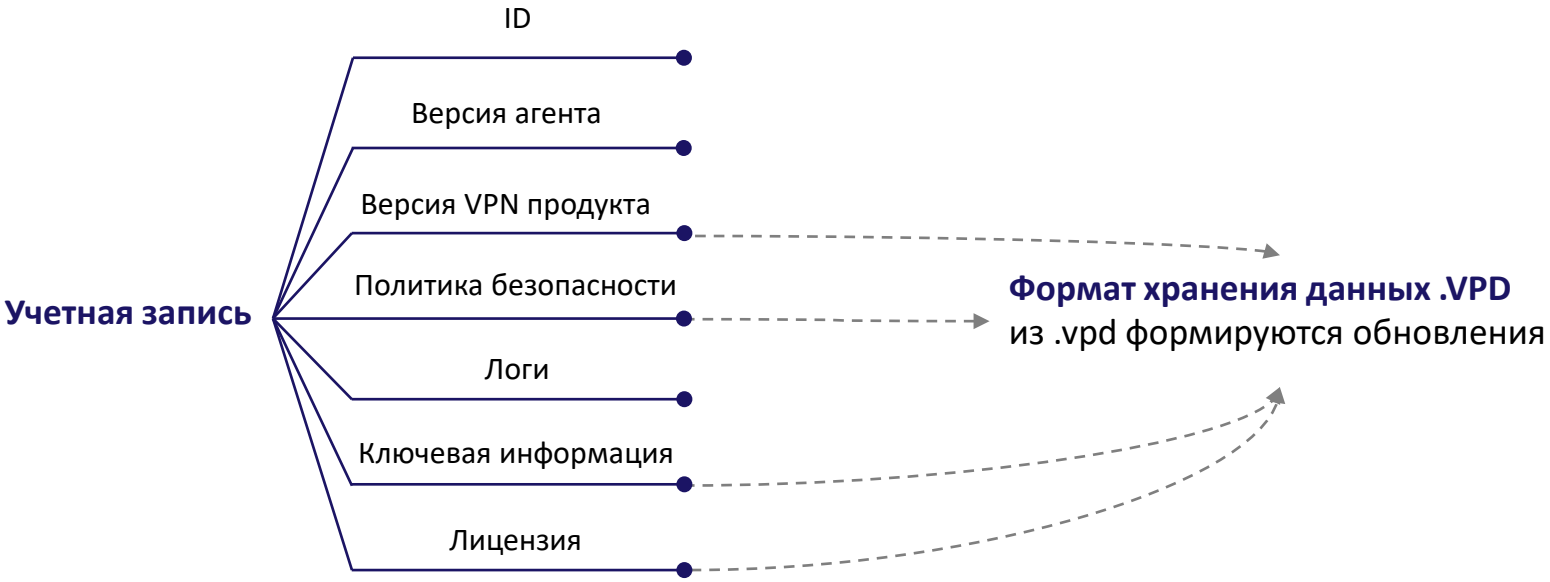
Архитектура С-Терра КП

Учетные записи и пользователи

Агент С-Терра КП:
Для каждого агента создается учетная запись на Сервере



Внутри учетной записи



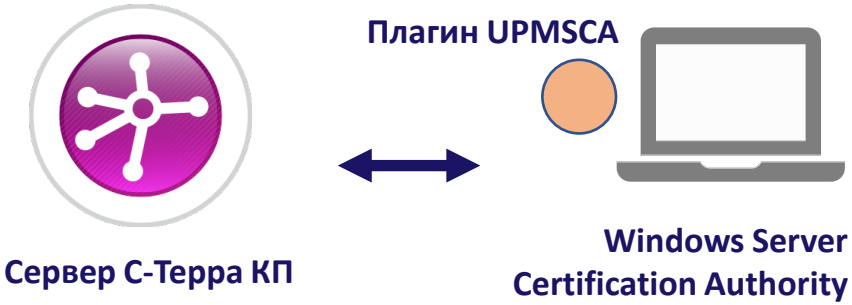
Центр выдачи сертификатов

Сервер С-Терра КП:
Интегрируется со службой **Certification Authority** MS Windows Server с помощью плагина UPMSCA

Сервер С-Терра КП и служба Certification Authority могут быть развернуты на одном Windows Server, либо на разных

Если на разных – UPMSCA ставится на машину с Certification Authority

ВАЖНО. Сперва настраивается Удостоверяющий центр, только потом устанавливается плагин

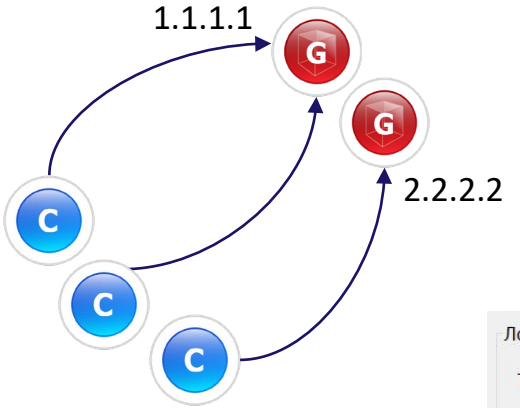


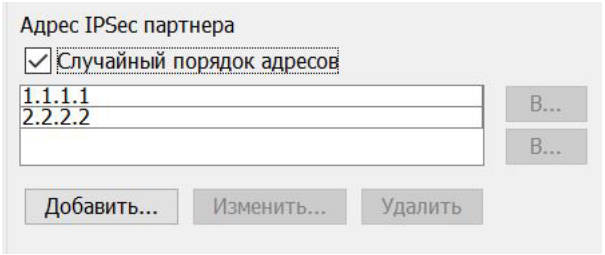
C-Терра Клиент

s•terra®

1. Балансировка нагрузки

Создаем список пиров
и используем случайный
порядок подключения

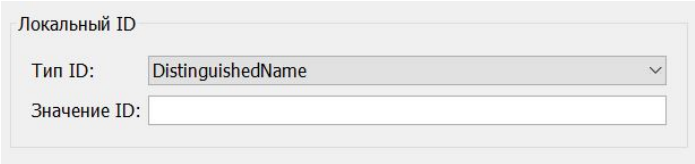




Wizard. Создание правила
обработки трафика

2. Массовые обновления сертификатов

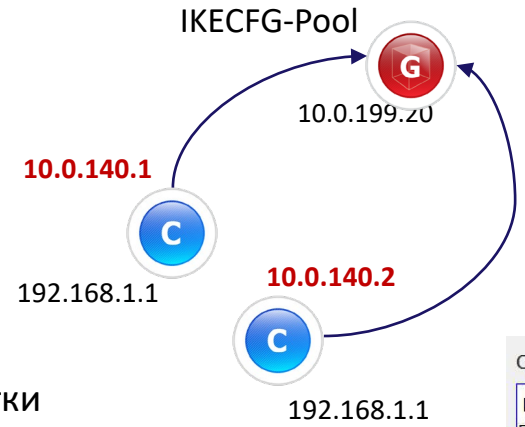
Отвязываем политику
безопасности С-Терра Клиент
от локального сертификата

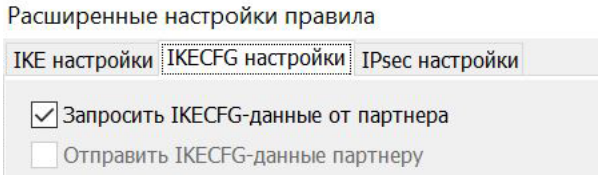



```
IdentityEntry local_auth_identity_01(
    DistinguishedName *= USER_SPECIFIC_DATA
)
```

3. IKECFG адресация

Каждому клиентскому подключению выделяется один адрес из IKECFG-Pool. Решается проблема пересечения адресных пространств



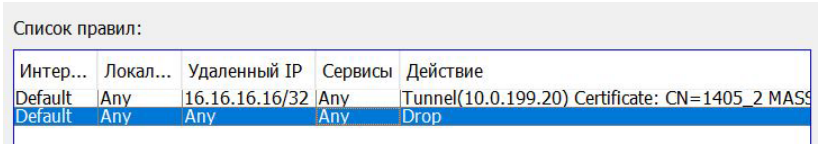


Wizard. Создание правила обработки трафика

4. Управления трафиком

С помощью правил обработки трафика можно строить сценарии:

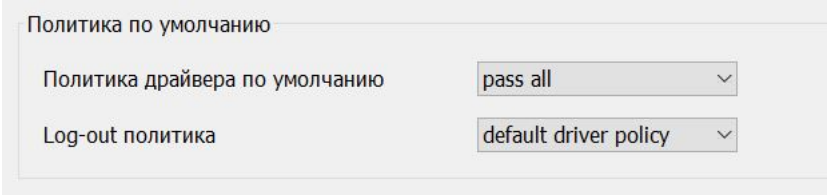
- Все в туннель;
- Туннель + Интернет;
- Только туннель



Пример реализации «Только туннель».
Первое правило – шифрование
Второе правило – сбросить все

5. Политика драйвера по умолчанию (DDP)

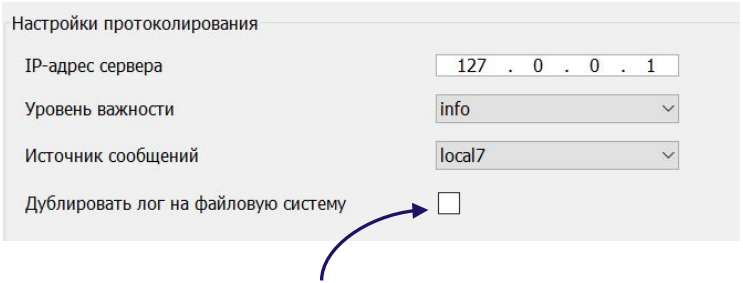
Когда С-Терра Клиент не запущен работает DDP. По умолчанию политика – сбрасывать все пакеты, поэтому после установки отваливается RDP



Редактирование .vpd. Вкладка «Настройки»

6. Логи

Поддерживается локальный лог и внешний syslog сервер

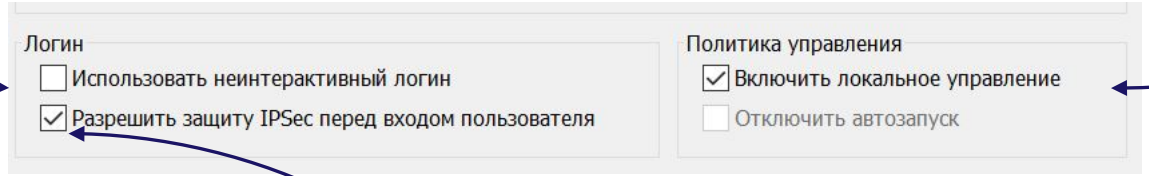


Забыли? Не критично. Можно включить локально после установки

С-Терра Клиент

Прозрачный режим работы.
С-Терра Клиент не выведет окно
с приглашением ввести логин и пароль

По умолчанию пользователь не может
менять политику безопасности
С-Терра Клиент. С включенным локальным
управлением может



С-Терра Клиент запустится до входа
пользователя в систему

Все опции нельзя
изменить локально

Автоматизируем выпуск дистрибутивов

s•terra®

Шаг 1. Список учетных записей

Создаем clients.txt со списком учетных записей

Шаг 2. Список лицензий

Создаем license.txt со списком лицензий. Можно использовать скрипт, который создаст список из Excel-таблицы. Excel-таблицу с лицензиями запросите у аккаунт-менеджера

Шаг 3. Шаблон С-Терра Клиент

Политика безопасности отвязана от локального сертификата. Удалена структура local_cert_description

Запускаем скрипт

В результате:

- Автоматически создаются ключевые контейнеры;
- Автоматически создаются сертификаты;
- Автоматически создаются учетные записи на сервере С-Терра КП;
- Автоматически выпускаются дистрибутивы

Доставляем дистрибутивы на компьютеры пользователей и устанавливаем

Обновления для группы учетных записей

s•terra®

Правила Пользования:

Менять закрытый ключ раз в 15 месяцев. Обновим сразу для всех С-Терра Клиент

Правильные С-Терра Клиент:

Политика безопасности не привязана к локальному сертификату

local_auth_identity

DistinguishedName *= USER_SPECIFIC_DATA

Шаг 1. Ключевой контейнер

Ключевой контейнер создается локально на устройствах. Передается только запрос на сертификат открытого ключа

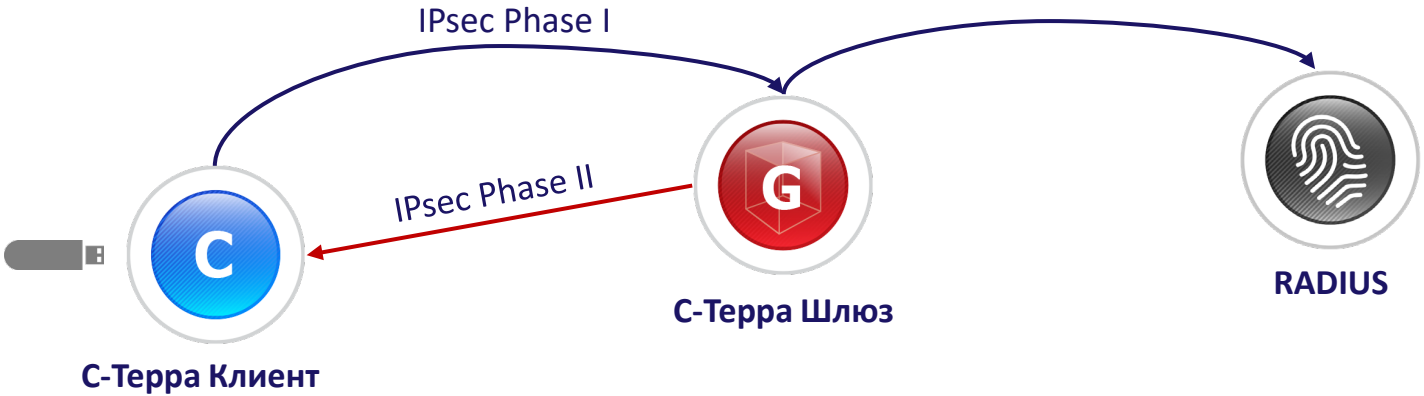
Шаг 2. Сертификат

С помощью инструментов УЦ подписываем все клиентские запросы

Шаг 3. Обновление

Создаем одно обновление для всех учетных записей С-Терра Клиент

Факторы аутентификации С-Терра Клиент



1. Логин – Пароль

Пользователь вводит логин и пароль, чтобы запустить С-Терра Клиент

2. Токен

Пользователь подключает токен с закрытым ключом. Строится IPsec Phase I

С-Терра Шлюз и С-Терра Клиент аутентифицируют друг друга

3. Внешний Radius Server

Внутри IPsec Phase I RADIUS сервер аутентифицирует пользователя с помощью XAuth

Резервное копирование сервера С-Терра КП

s•terra®

1. Задать путь до сетевой папки

Протокол SMB.

Файл – Настройка – Дополнительно –
Настройки автоматических резервных копий

Пример:

\\10.0.0.37\exchange\dmahotkin

2. Создать задачу

Инструменты – Резервное копирование – Задачи…

Простая – выполнить Backup

Расширенная – отложенное время старта/периодичность

3. Управление копиями

Инструменты – Резервное копирование – Управление…

Дерево снапшотов. Простой переход между резервными копиями

Резервное копирование не затрагивает

Закрытый ключ сервера С-Терра КП.
Отдельная инструкция по резервному копированию

Спасибо за внимание

С-Терра КП – централизованное управление

- Как С-Терра КП управляется VPN устройствами;
- Как разграничить доступ администраторов к VPN устройствам;
- Как обновить ключи сразу на всех С-Терра Клиент;
- Что будет, если С-Терра КП выйдет из строя, как сделать backup?

С-Терра Клиент – клиентское ПО для Windows, Astra Linux

- Как автоматизировать выпуск множества С-Терра Клиент;
- Как обеспечить двухфакторную аутентификацию пользователя;
- Как настроить прозрачный режим работы;
- Почему «отваливается» RDP в процессе установки?

dmahotkin@s-terra.ru
+7 (499) 940 9001 доб. 181