Развертывание и настройка дуального TLS ГОСТ | RSA

Бадмаева Римма
Ипаев Алексей

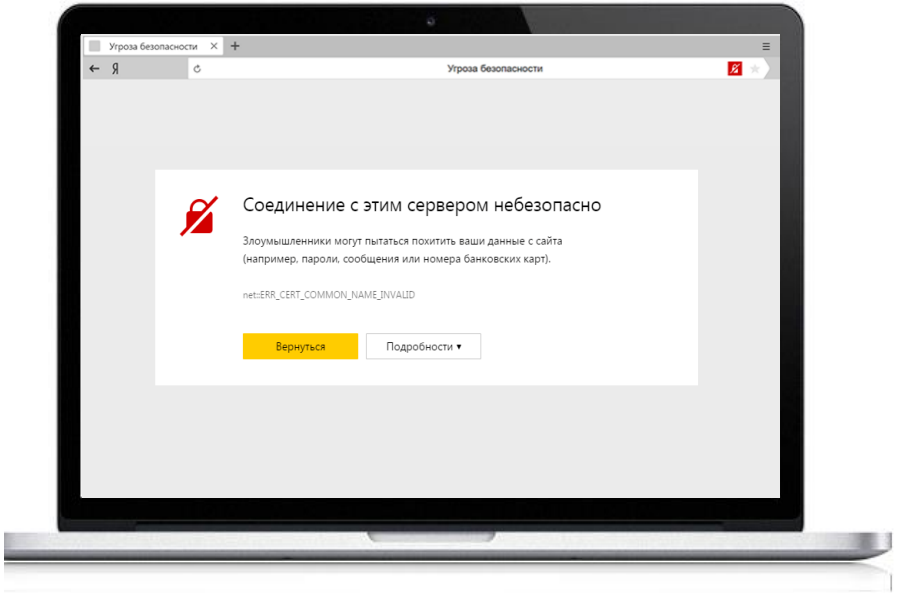
Зачем нам ГОСТ TLS?

Давайте разберемся…

Распространенность

- Популярность систем с веб-интерфейсом
- Государственная политика по обеспечению ИБ
- Наличие СКЗИ на рабочих местах для задач ЭП

Независимость и безопасность



Какие возникают проблемы

Отзыв сертификатов со стороны зарубежных УЦ, отказ в выпуске

Как решаются эти проблемы

Ведется запуск **Национального удостоверяющего центра.**

На базе НУЦ оперативно создан удостоверяющий центр для выпуска TLS/SSL сертификатов с использованием зарубежных криптографических алгоритмов (RSA) через Госуслуги

Проблемы и вопросы

Где получить сертификаты TLS ГОСТ?

- УЦ, в т.ч. Аккредитованные, затем НУЦ
- Свой корпоративный УЦ

Критерии выбора СКЗИ для организации TLS ГОСТ

Для пользователей:

- Просто и удобно
- Недорого
- Поддержка разных платформ и браузеров

Для серверов:

- Высокопроизводительный
- Сертифицированный
- Надежный
- Поддержка дуальной криптографии – режим одновременной работы с российскими и иностранными алгоритмами

Наше решение – ViPNet TLS Gateway

ViPNet TLS Gateway

Высокопроизводительный TLS-криптошлюз

- Обратный прокси-сервер, обеспечивающий защищенный удаленный HTTPS-доступ к ресурсам
- Туннелирование TCP-трафика по протоколу TLS
- Аутентификация клиента и сервера
- Управление доступом на основе сертификатов
- Дуальный режим работы
- Удаленное управление
- Кластеризация
- TLS 1.0 – 1.3

Модификации

Исполнение	TLS 550	TLS 1100	TLS 5500
Форм-фактор	ПАК 19” Rack 1U	ПАК 19” Rack 1U	ПАК 19” Rack 1U
Предельная пропускная способность (Мбит/с)	до 600	до 1800	до 7600
Число одновременных соединений	до 7000	до 14000	до 65000
Интерфейсы	6x Ethernet 10/100/1000	8x Ethernet 10/100/1000 4x 1G Ethernet Fiber SFP	4x Ethernet 10/100/1000 8x 10G Ethernet Fiber SFP+

Платформы виртуализации

ViPNet TLS Gateway сертифицирован

- СКЗИ КС3 (исполнения ПАК)
- СКЗИ КС1 (исполнение VA)
- Зарегистрирован в Реестре российского ПО

Клиентское СКЗИ

ViPNet CSP

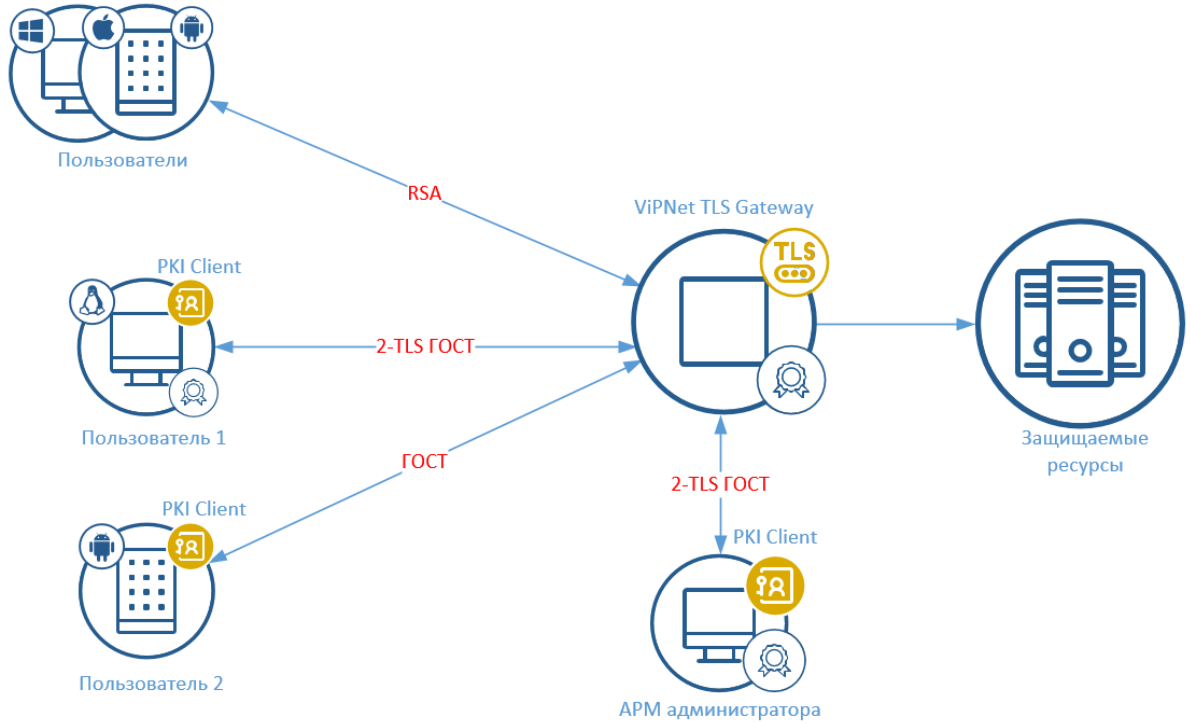
ViPNet PKI Client

Любое сертифицированное СКЗИ

Демонстрация

Переходим к практике!

Дуальный режим
(https://tlsgateway.tk)



Кластеризация шлюза

Высоко-производительный отказоустойчивый кластер TLS

Бадмаева Римма
Ипаев Алексей

ViPNet TLS Gateway 2

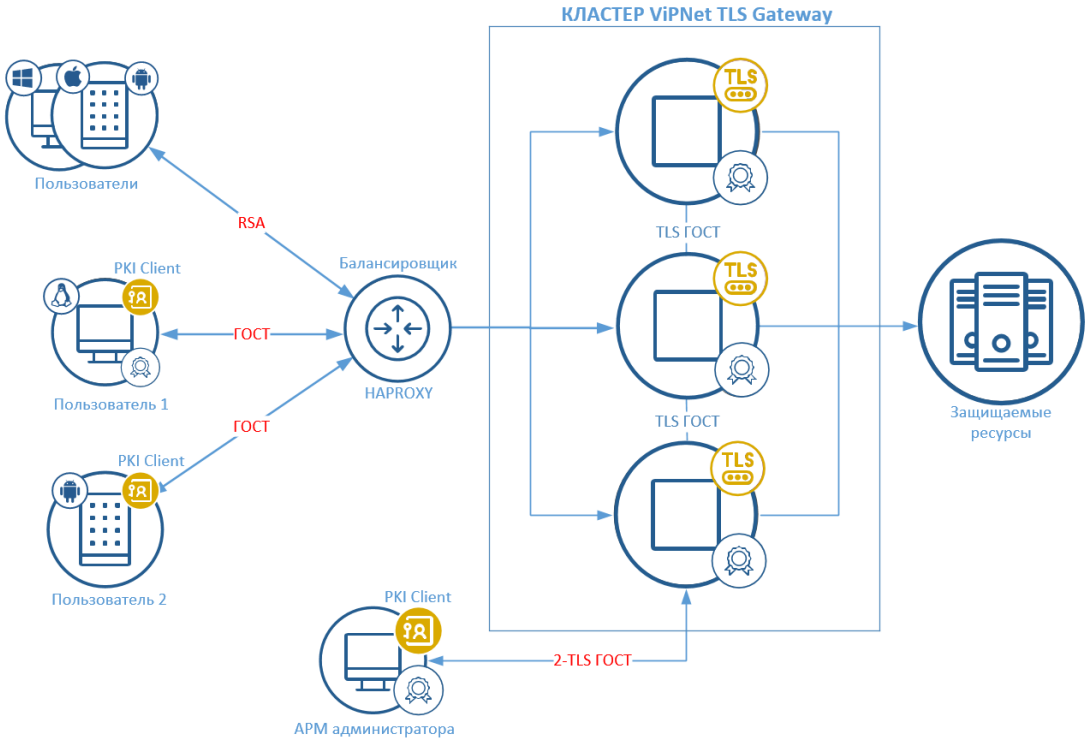
Кластер

- От 2 до 64 узлов
- Работа Active-Active
- Внешний балансировщик для распределения нагрузки
- Поддержка Proxy Protocol
- Защищенное соединение между узлами (TLS ГОСТ)
- Не нужен дополнительный центр управления
- Устойчивость к разделению сети – продолжает обслуживание пользователей на всех работоспособных узлах

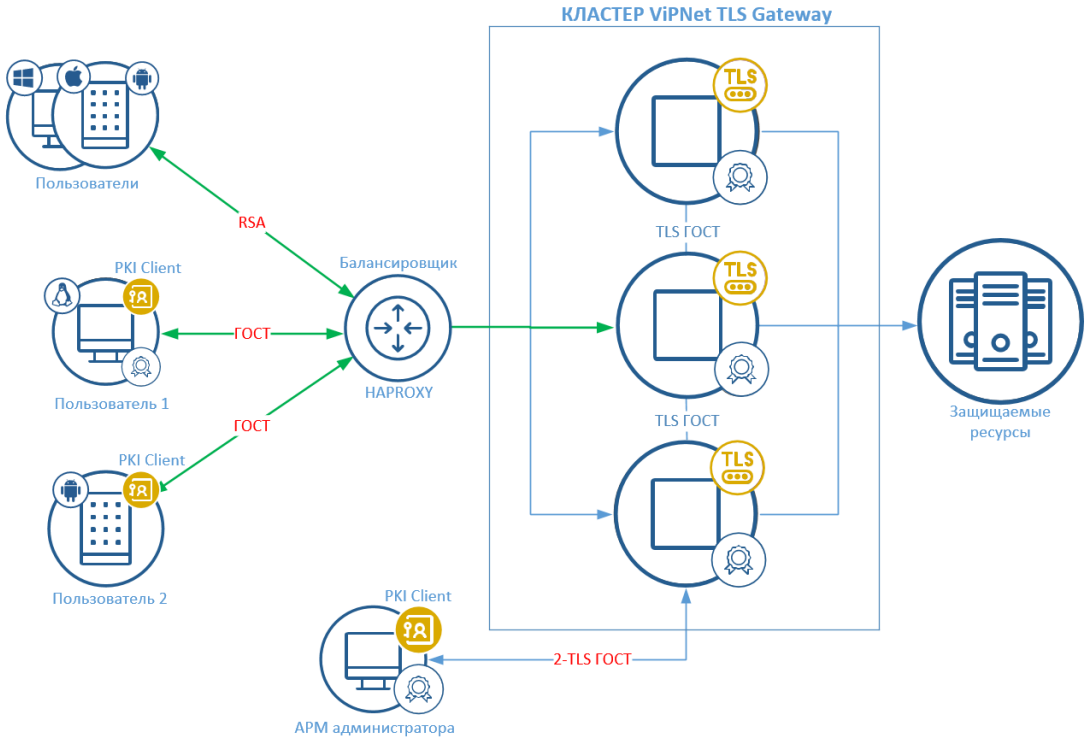
Демонстрация

Еще практика!

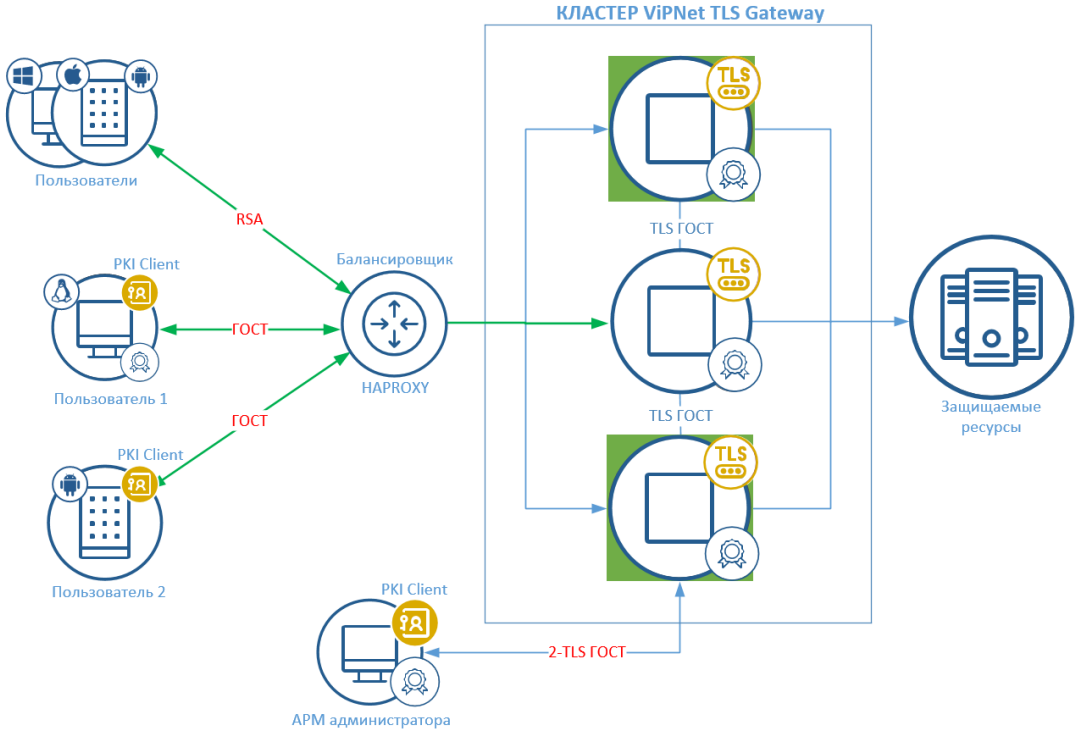
Настраиваем кластер
(https://tlsgateway.tk)



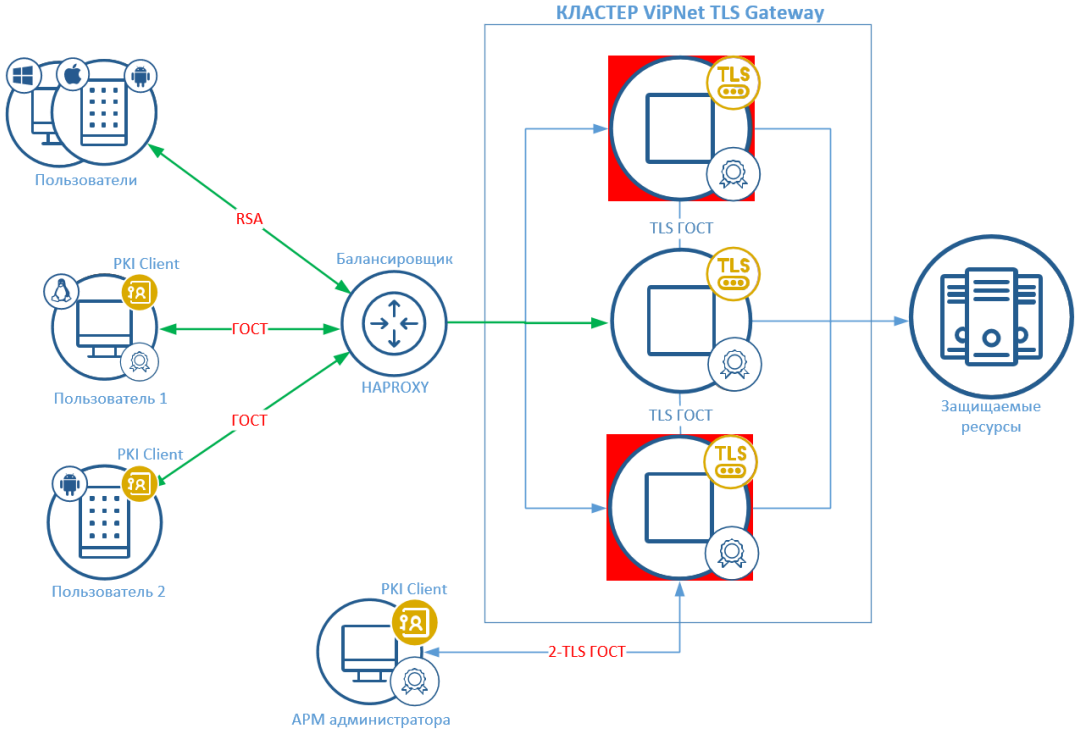
Запускаем скачивание файла
(https://tlsgateway.tk)



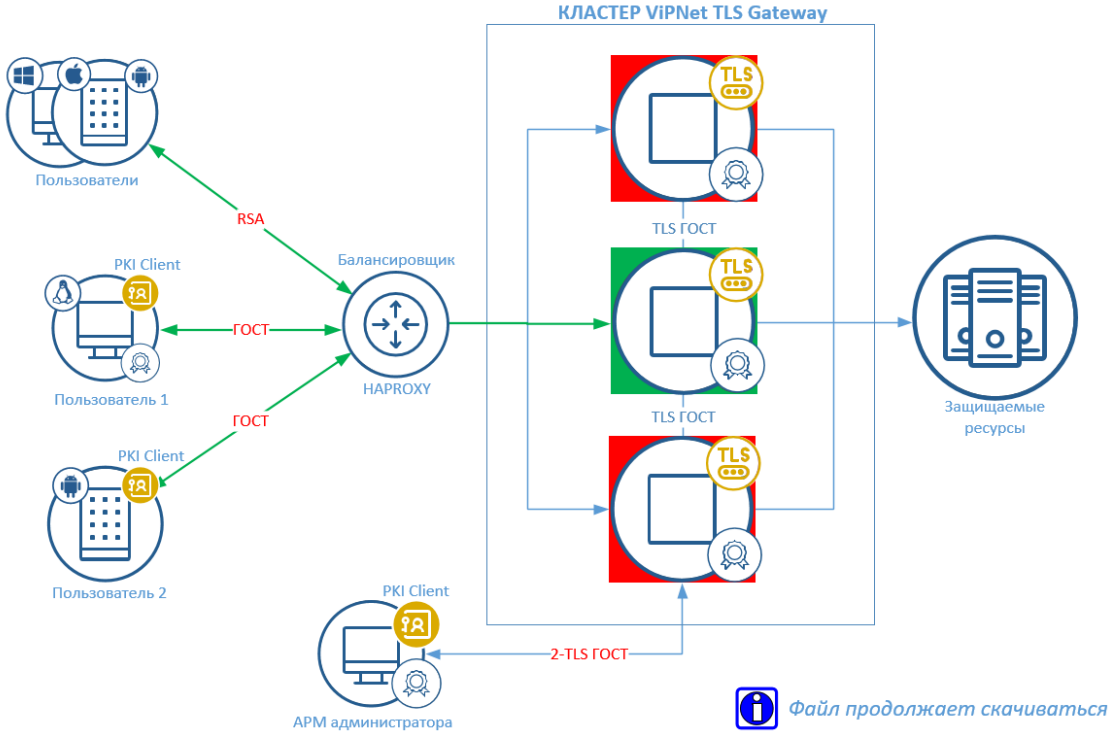
Определяем активные узлы



Отключаем активные узлы



Проверяем скачивание
(https://tlsgateway.tk)



ТЕХНО infotecs 2023 ФЕСТ

Спасибо за внимание!

Бадмаева Римма

e-mail: Rimma.Badmaeva@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363