# ViPNet TLS Gateway: дуальный, надежный, твой


Николай Смирнов
директор по продуктам

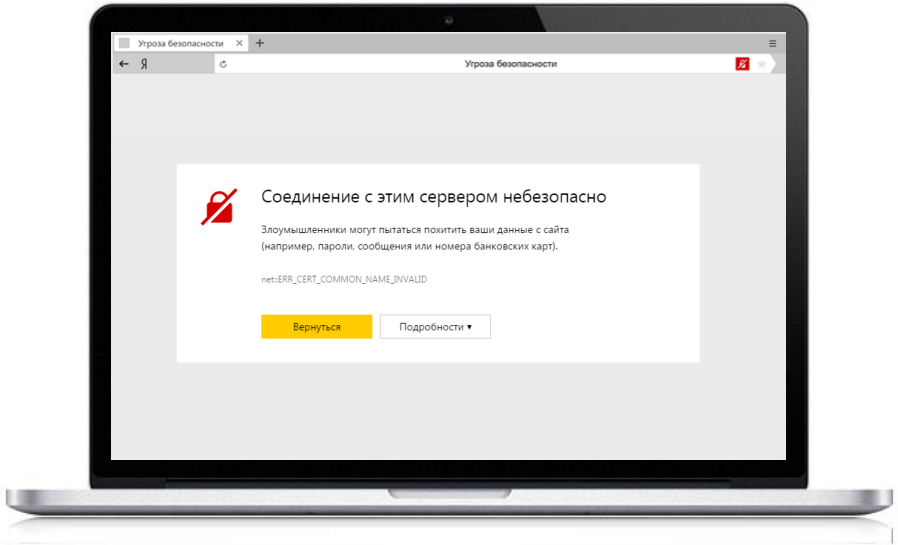
# Зачем нам ГОСТ TLS?

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

1. Шлюз безопасности для организации TLS-соединений
2. Поддержка актуальных криптоалгоритмов, в т.ч. иностранных
3. Поддержка сертификатов, изданных разными УЦ, в т.ч. аккредитованными
4. Поддержка разных схем аутентификации
5. Кластер
6. Исполнения ПАК и ПК (VA)

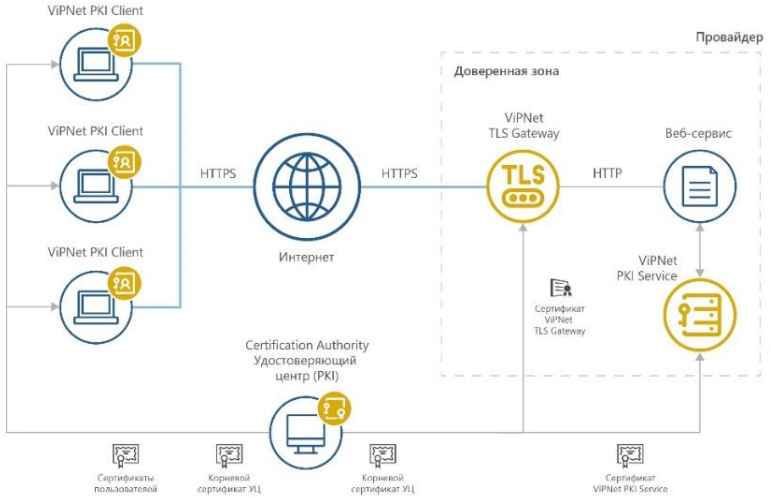
# ViPNet TLS Gateway

Обратный прокси-сервер, обеспечивающий защищенный удаленный HTTPS-доступ к ресурсам

- С использованием любого сертифицированного СКЗИ, например, ViPNet PKI Client

Туннелирование TCP-трафика по протоколу TLS

- Только с использованием ViPNet PKI Client (Desktop) версии 1.3 и выше



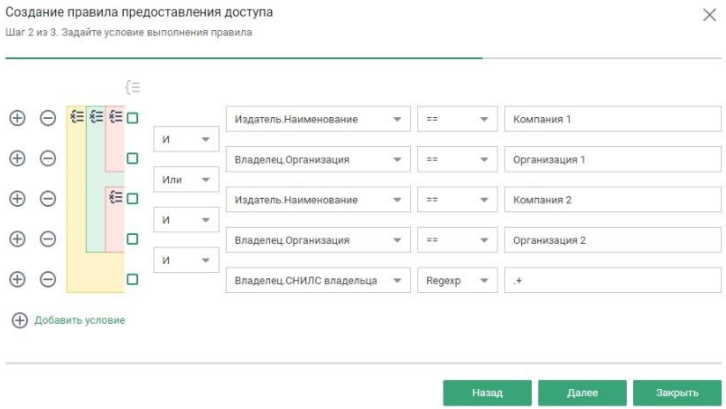
# ViPNet TLS Gateway

## Поддержка разных схем аутентификации

- Аутентификация сервера (односторонний TLS)
- Обоюдная аутентификация сервера и клиента (двусторонний TLS)

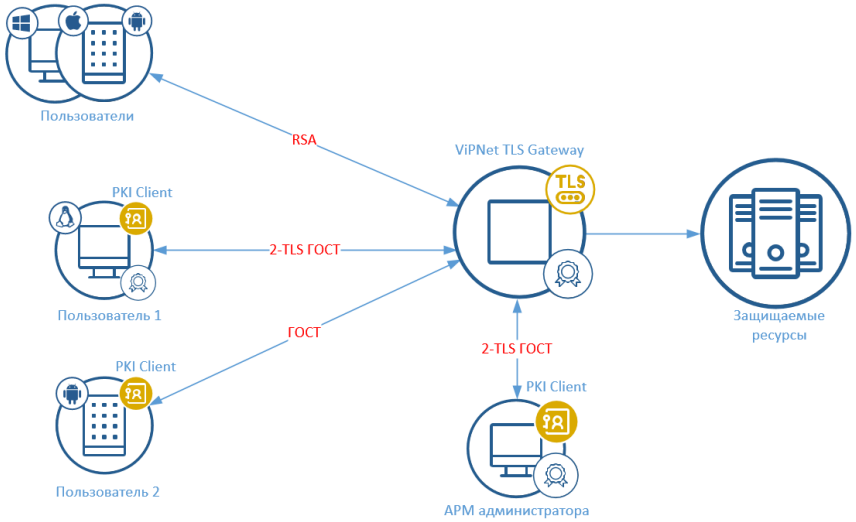
## Управление доступом на основе сертификатов

- Конструктор правил (с возможностью подключения к LDAP-каталогам)
- Загрузка сертификатов (например, из ViPNet PKI Service)
- Запрос пользователя



# ViPNet TLS Gateway: дуальный режим

- Поддерживаемые криптоалгоритмы ГОСТ: ГОСТ 28147-89, ГОСТ 34.12-2018, ГОСТ 34.13-2018, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012.
- Поддержка иностранных криптоалгоритмов* (RSA, ECDSA, AES) для работы в дуальном режиме.
- Импорт ключей в формате PFX.



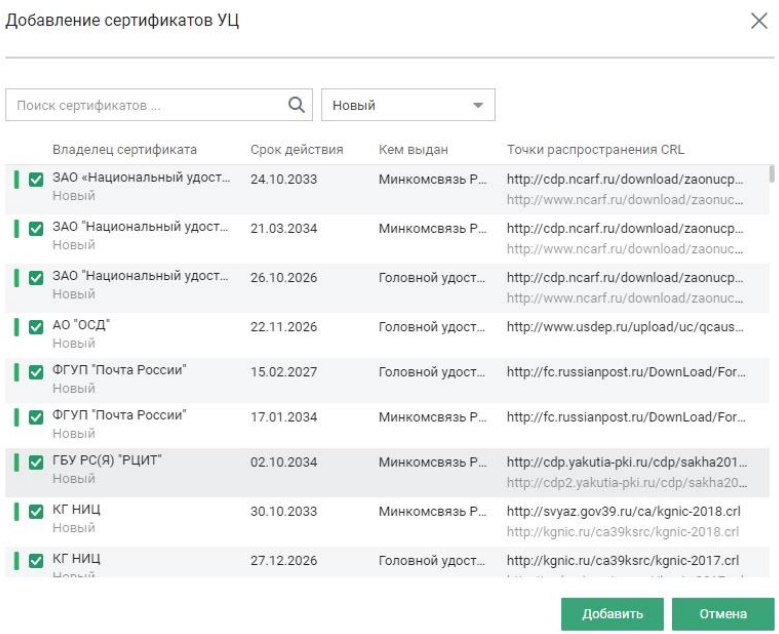

**Не могут использоваться для защиты конфиденциальной информации*

# ViPNet TLS Gateway: поддержка УЦ

**Транспортный сертификат ≠ Сертификат для ЭП**

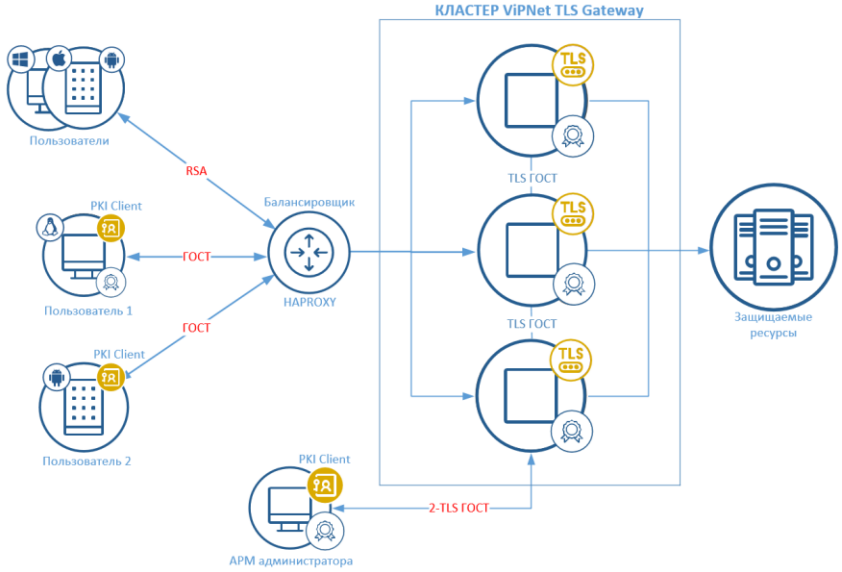
**Требования 63-ФЗ и приказов 795 и 796 на ViPNet TLS Gateway не распространяются.**

- Запрос на сертификат в формате PKCS#10.
- Использование сертификатов, изданных различными УЦ.
- Поддержка TSL-списка аккредитованных УЦ от Минцифры для установки корневых и CRL.
- Поддержка OCSP.



# ViPNet TLS Gateway: кластер

- Доступен, начиная с версии 2.0.
- 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.



# 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<br>4x 1G Ethernet Fiber SFP | 4x Ethernet 10/100/1000<br>8x 10G Ethernet Fiber SFP+ |

Платформы виртуализации

# ViPNet TLS Gateway

- СКЗИ КС3 (исполнения ПАК)
- СКЗИ КС1 (исполнение VA)
- Зарегистрирован в Реестре российского ПО, в реестре ПАК, в реестре МПТ
- Клиентское ПО: ViPNet PKI Client, ViPNet CSP или любое сертифицированное СКЗИ

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-4382 от "14" ноября 2022 г.

Действителен до "14" ноября 2025

Выдан Акционерному обществу «Информацио
Обществу с ограниченной ответственно

Настоящий сертификат удостоверяет, что из
6, 7, 8) в комплектации согласно формуляру Ф

соответствует Требованиям к средства
предназначенным для защиты информаци
государственную тайну, класса КС3 и может
(создание и управление ключевой информации
в областях оперативной памяти, вычисление ко
в областях оперативной памяти, вычисление
содержащихся в областях оперативной пам
содержащей сведений, составляющих государст

Сертификат выдан на основании результа
ответственностью «СФБ Лаборатория»

сертификационных испытаний образцов
906-000502 (исполнение 2), 906-000503 (испол
(исполнение 7), 906-000507 (исполнение 8)

Безопасность информации обеспечивается
требованиями эксплуатационной документации

Заместитель руководителя Научно-техническ
службы – начальник Центра защиты информ
и специальной связи ФСБ России

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/114-4473 от "08" марта 2023 г.

Действителен до "08" марта 2026 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы»,
Обществу с ограниченной ответственностью «Линия защиты».

Настоящий сертификат удостоверяет, что изделие ViPNet TLS Gateway (исполнение 5)
в комплектации согласно формуляру ФРКЕ.00169-02 30 01 ФО с учётом извещения об
изменении № 1 ФРКЕ.00169.FB.1-2023

соответствует Требованиям к средствам криптографической защиты информации,
предназначенным для защиты информации, не содержащей сведений, составляющих
государственную тайну, класса КС1 и может использоваться для криптографической защиты
(создание и управление ключевой информацией, шифрование файлов и данных, содержащихся
в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся
в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных,
содержащихся в областях оперативной памяти, защита TLS-соединений) информации, не
содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной
ответственностью «СФБ Лаборатория».

сертификационных испытаний образца продукции № 906-000504

Безопасность информации обеспечивается при использовании изделия в соответствии с
требованиями эксплуатационной документации согласно формуляру ФРКЕ.00169-02 30 01 ФО
с учётом извещения об изменении № 1 ФРКЕ.00169.FB.1-2023.

Заместитель руководителя Научно-технической
службы – начальник Центра защиты информации
и специальной связи ФСБ России О.В. Скрябин

ТЕХНО 2024 infotecs ФЕСТ

# Задавайте вопросы в приложении!

Подписывайтесь на наши соцсети