

# VIPNet TLS Gateway: дуальный, надежный, ТВОЙ

Бадмаева Римма



техно infotecs  
2023 Фест  
ТЕХНИЧЕСКАЯ  
КОНФЕРЕНЦИЯ

# Зачем нам ГОСТ TLS?

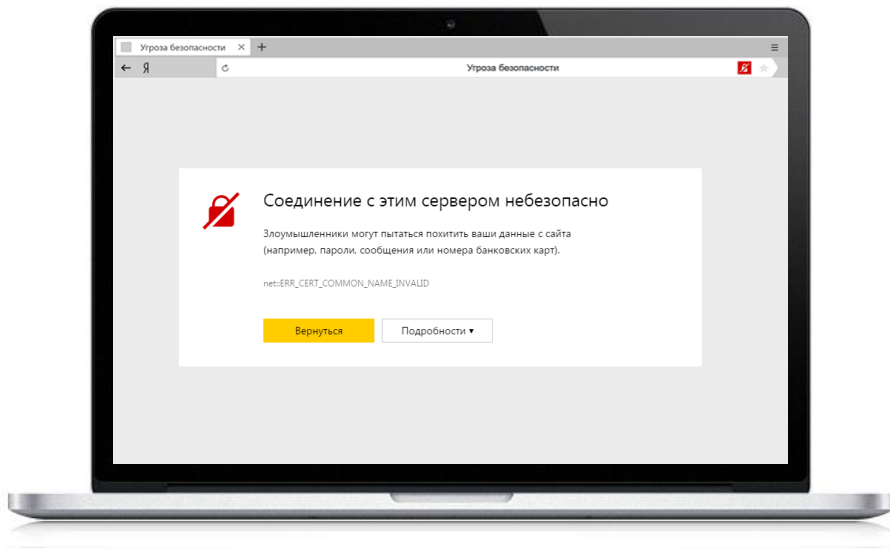
Давайте разберемся...

# 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)

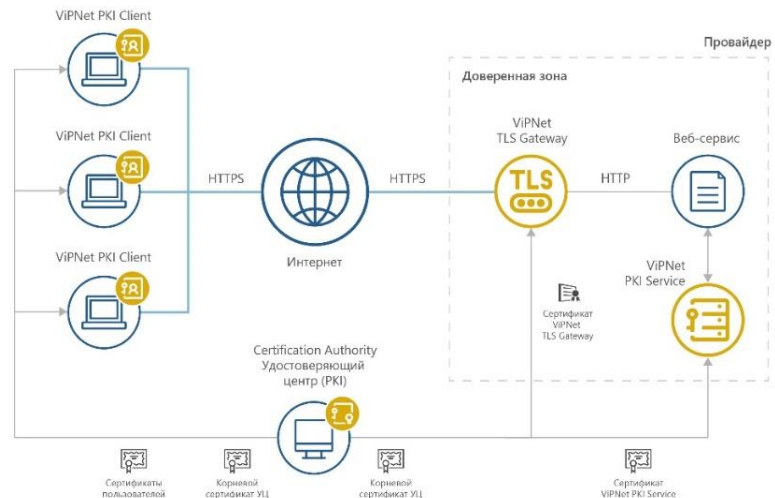
# VIPNet TLS Gateway

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)
- Обюдная 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

Создание правила предоставления доступа

Шаг 2 из 3. Задайте условие выполнения правила

The screenshot shows a configuration window for creating an access rule. On the left, there is a vertical list of conditions, each with a plus and minus icon and a checkbox. The conditions are: 'Издатель.Наименование' (yellow), 'Владелец.Организация' (green), 'Издатель.Наименование' (red), 'Владелец.Организация' (blue), and 'Владелец.СНИЛС владельца' (orange). To the right of this list are five rows of configuration fields. Each row corresponds to a condition and contains a dropdown menu with the condition name, a comparison operator (all set to '=='), and a text input field. The first four rows are grouped together by a vertical bar on the left, and their dropdown menus are set to 'Или' (OR). The fifth row is separate and has a dropdown menu set to 'И' (AND). At the bottom left, there is a '+ Добавить условие' button.

Издатель.Наименование	==	Компания 1
Владелец.Организация	==	Организация 1
Издатель.Наименование	==	Компания 2
Владелец.Организация	==	Организация 2
Владелец.СНИЛС владельца	Regex	.*

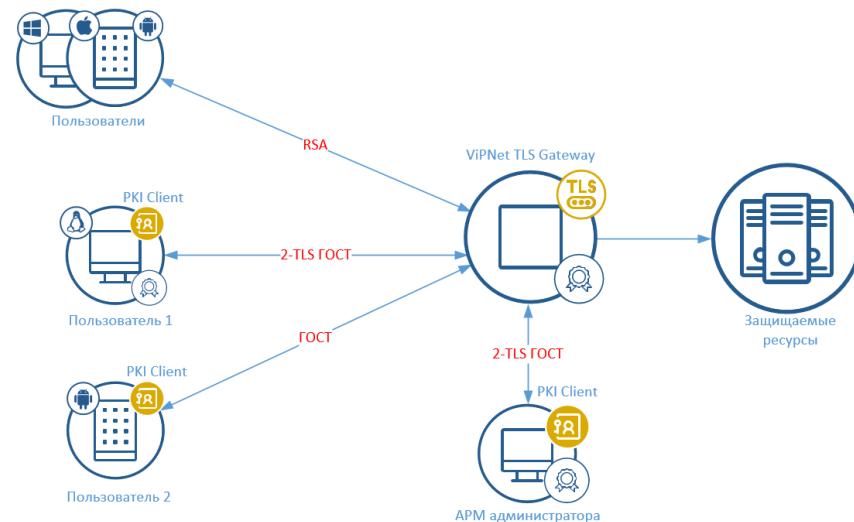
Назад

Далее

Закрыть

# 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  $\neq$  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.

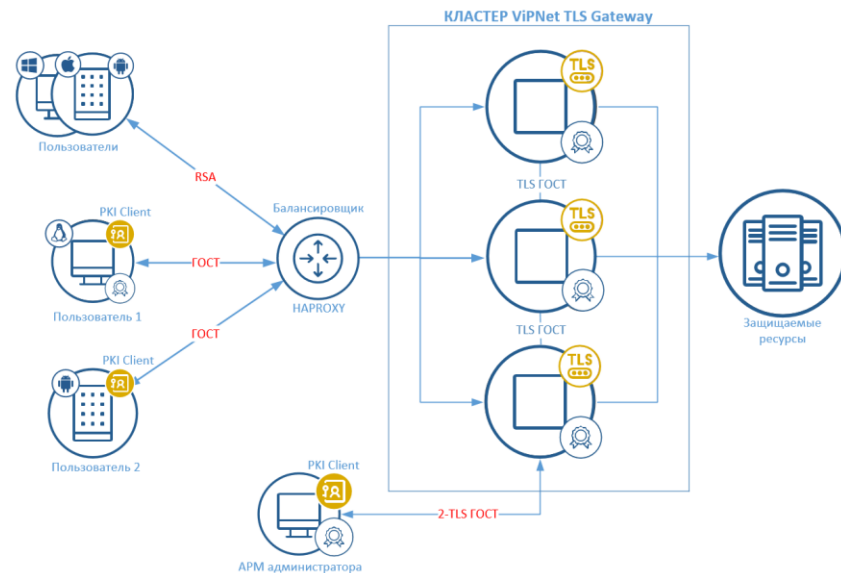
Добавление сертификатов УЦ

Владелец сертификата	Срок действия	Кем выдан	Точки распространения CRL
<input checked="" type="checkbox"/> ЗАО «Национальный удост... Новый	24.10.2033	Минкомсвязь Р...	<a href="http://cdp.ncarf.ru/download/zaonucp...">http://cdp.ncarf.ru/download/zaonucp...</a> <a href="http://www.ncarf.ru/download/zaonuc...">http://www.ncarf.ru/download/zaonuc...</a>
<input checked="" type="checkbox"/> ЗАО "Национальный удост... Новый	21.03.2034	Минкомсвязь Р...	<a href="http://cdp.ncarf.ru/download/zaonucp...">http://cdp.ncarf.ru/download/zaonucp...</a> <a href="http://www.ncarf.ru/download/zaonuc...">http://www.ncarf.ru/download/zaonuc...</a>
<input checked="" type="checkbox"/> ЗАО "Национальный удост... Новый	26.10.2026	Головной удост...	<a href="http://cdp.ncarf.ru/download/zaonucp...">http://cdp.ncarf.ru/download/zaonucp...</a> <a href="http://www.ncarf.ru/download/zaonuc...">http://www.ncarf.ru/download/zaonuc...</a>
<input checked="" type="checkbox"/> АО "ОСД" Новый	22.11.2026	Головной удост...	<a href="http://www.usdep.ru/upload/uc/qcaus...">http://www.usdep.ru/upload/uc/qcaus...</a>
<input checked="" type="checkbox"/> ФГУП "Почта России" Новый	15.02.2027	Головной удост...	<a href="http://fc.russianpost.ru/Download/For...">http://fc.russianpost.ru/Download/For...</a>
<input checked="" type="checkbox"/> ФГУП "Почта России" Новый	17.01.2034	Минкомсвязь Р...	<a href="http://fc.russianpost.ru/Download/For...">http://fc.russianpost.ru/Download/For...</a>
<input checked="" type="checkbox"/> ГБУ РС(Я) "РЦИТ" Новый	02.10.2034	Минкомсвязь Р...	<a href="http://cdp.yakutia-pki.ru/cdp/sakha201...">http://cdp.yakutia-pki.ru/cdp/sakha201...</a> <a href="http://cdp2.yakutia-pki.ru/cdp/sakha20...">http://cdp2.yakutia-pki.ru/cdp/sakha20...</a>
<input checked="" type="checkbox"/> КГ НИЦ Новый	30.10.2033	Минкомсвязь Р...	<a href="http://svyaz.gov39.ru/ca/kgnic-2018.crl">http://svyaz.gov39.ru/ca/kgnic-2018.crl</a> <a href="http://kgnic.ru/ca39ksrc/kgnic-2018.crl">http://kgnic.ru/ca39ksrc/kgnic-2018.crl</a>
<input checked="" type="checkbox"/> КГ НИЦ Новый	27.12.2026	Головной удост...	<a href="http://kgnic.ru/ca39ksrc/kgnic-2017.crl">http://kgnic.ru/ca39ksrc/kgnic-2017.crl</a>

Добавить Отмена

# 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 4x 1G Ethernet Fiber SFP	4x Ethernet 10/100/1000 8x 10G Ethernet Fiber SFP+

## Платформы виртуализации



# ViPNet TLS Gateway

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





техно infotecs  
2023 Фест

Спасибо  
за внимание!

---

Подписывайтесь на наши соцсети



[vk.com/infotecs\\_news](https://vk.com/infotecs_news)



[https://t.me/infotecs\\_official](https://t.me/infotecs_official)



[rutube.ru/channel/24686363](https://rutube.ru/channel/24686363)