Развертывание и настройка дуального TLS GOST | RSA

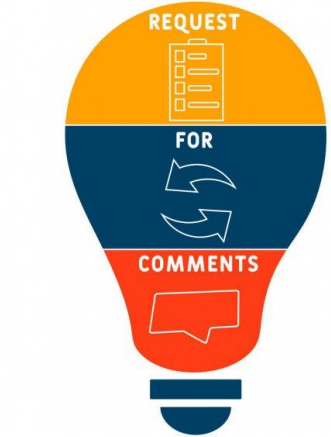
Еранов Сергей

Долгополов Игорь

ТехноФест 2021 infotecs

Зачем нам ГОСТ TLS?

Стандартизация

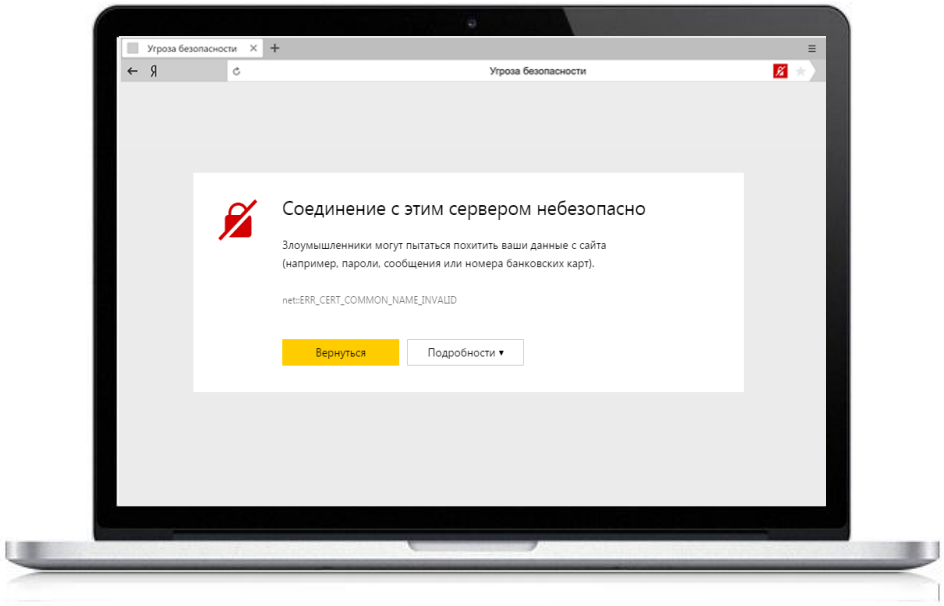


- ГОСТ
- RFC
- Рекомендации ТК26
- Контрольные примеры

IETF

Результат: мультивендорность для конечных потребителей

Независимость и безопасность



Какие возникают проблемы

SSL-сертификат, выданный иностранным УЦ, могут отозвать из-за санкций:

GeoTrust отозвала сертификат для сайта Общественной палаты из-за «аффилированности» с ДНР

Как решаются эти проблемы

Ведется запуск **Национального удостоверяющего центра**

Распространенность

- ✓ Популярность систем с веб-интерфейсом, REST API и т.д.
- ✓ Наличие СКЗИ на рабочих местах для задач ЭП

Активное продвижение со стороны государства

- Пр-1380. Поручение об обеспечении разработки и реализации комплекса мероприятий, необходимых для перехода органов власти на использование российских криптографических алгоритмов и средств шифрования

- Постановление Правительства № 963 «О реализации пилотного проекта по использованию российских криптографических алгоритмов и средств шифрования в государственных информационных системах»

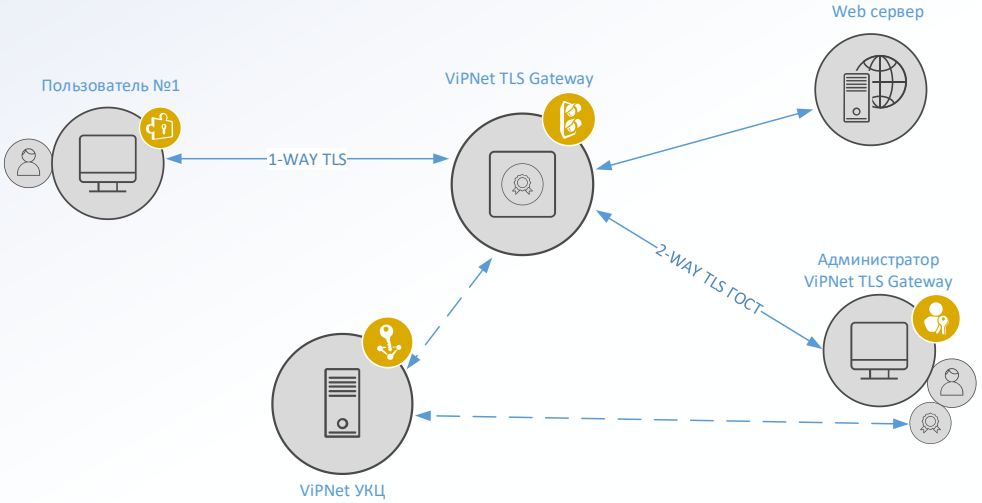
- Проект Приказа Минкомсвязи «Об утверждении требований к технологиям взаимодействия средств информатизации, реализующих российские криптографические алгоритмы, с иными средствами информатизации»

ТЕХНО infotecs 2021 ФЕСТ

Сценарии применения

Сценарий 1

Публичный портал



Задачи:

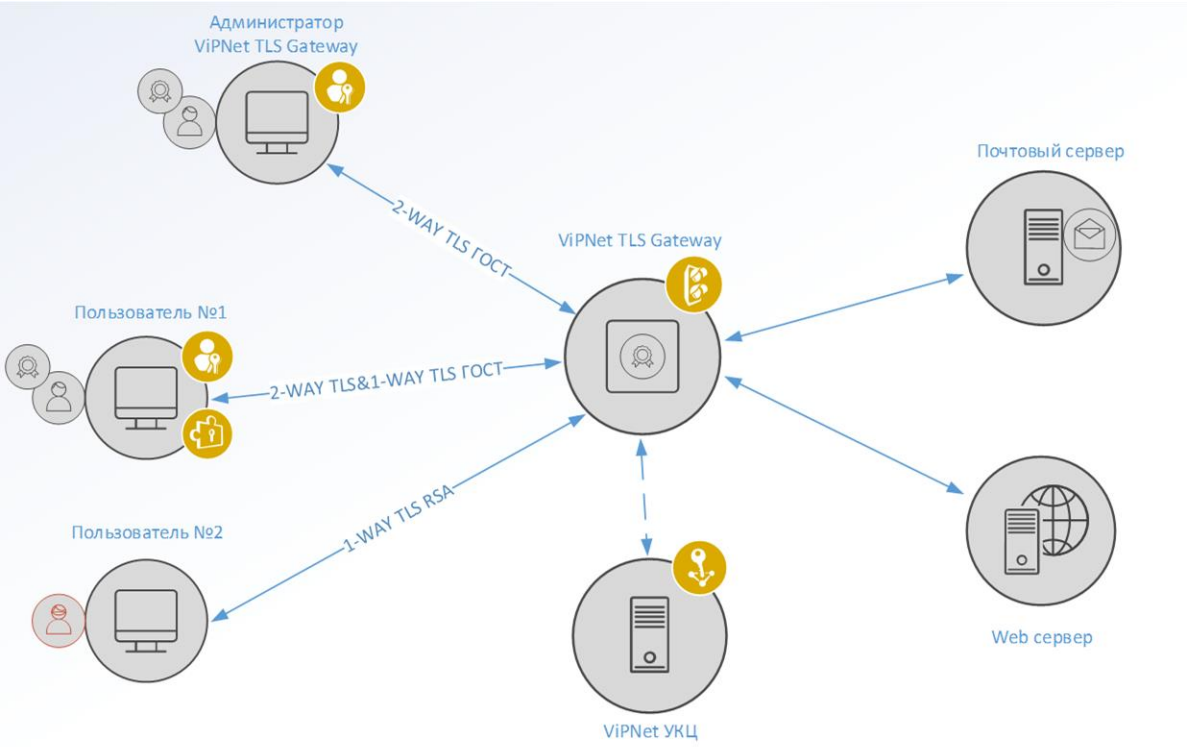
1. Подтверждение подлинности сервера
2. Защита передаваемых данных

Для этого требуется:

- Единое пространство доверия – НУЦ
- Аутентификация сервера
- Общедоступность клиентского СКЗИ
- Дуальный режим

Сценарий 2

Доступ к корпоративным ресурсам



Задачи:

1. Подтверждение подлинности сервера
2. Разграничение доступа
3. Защита передаваемых данных
4. TCP-трафик

Для этого требуется:

- Аутентификация сервера
- Аутентификация клиента
- TLS-туннель

Что для этого нужно

Для порталов

- ✓ Высокопроизводительные криптошлюзы
- ✓ Средства установления TLS-соединений для веб-серверов

Для разработчиков

- ✓ Библиотеки и SDK для установки TLS-соединений из приложений

Для пользователей

- ✓ Готовое СКЗИ для TLS

ViPNet TLS Gateway

ViPNet TLS Gateway

Высокопроизводительный TLS-криптошлюз

- Аутентификация клиента и сервера
- Управление доступом на основе сертификатов
- «Дуальный» режим работы
- Удаленное управление

Модификации

Исполнение	TLS 500	TLS 1000	TLS 5000	TLS VA
Форм-фактор	ПАК 19” Rack 1U	ПАК 19” Rack 1U	ПАК 19” Rack 1U	виртуальная машина
Предельная пропускная способность (Мбит/с)	до 300	до 750	до 3000	зависит от характеристик аппаратного обеспечения
Число одновременных соединений	до 4700	до 8900	до 44000	зависит от характеристик аппаратного обеспечения
Интерфейсы	4x Ethernet 10/100/1000	4x Ethernet 10/100/1000	4x Ethernet 10/100/1000 4x 10G Ethernet Fiber SFP+	зависят от характеристик аппаратного обеспечения

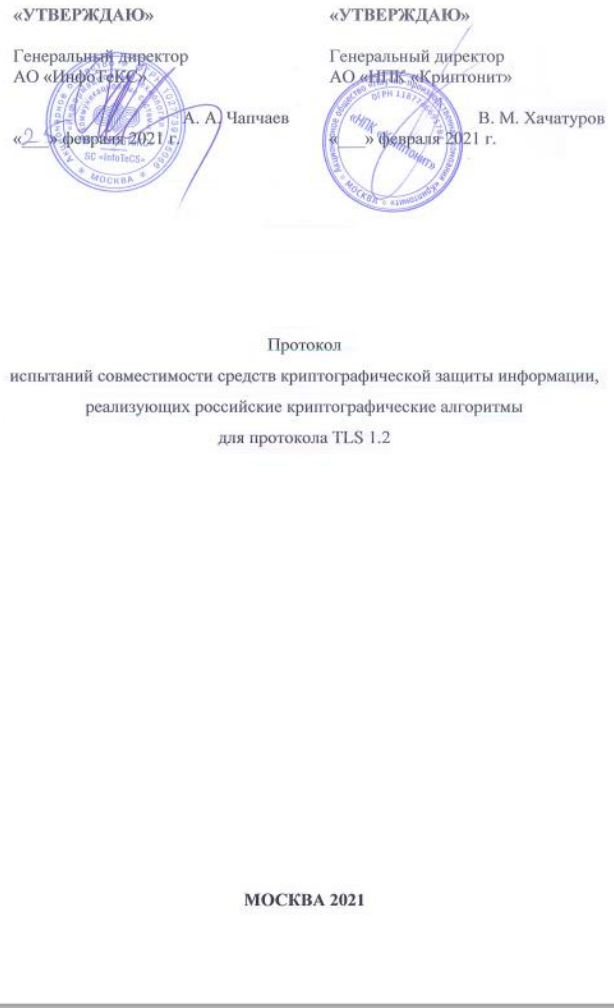
Платформы виртуализации

Oracle VM VirtualBox
5.1, 5.2, 6.0

VMware vSphere ESXi
6.0, 6.5, 6.7

VMware Workstation
14, 15

KVM
Kernel
Virtual Machine



«УТВЕРЖДАЮ»

Генеральный директор
АО «ИнфоТеКС»

А. А. Чапчаев
«__» февраля 2021 г.

«УТВЕРЖДАЮ»

Генеральный директор
АО «НПК «Криптонит»

В. М. Хачатуров
«__» февраля 2021 г.

Протокол
испытаний совместимости средств криптографической защиты информации,
реализующих российские криптографические алгоритмы
для протокола TLS 1.2

МОСКВА 2021

Клиентское СКЗИ

ТехноInfotecs Фест 2021

- ViPNet CSP
- ViPNet PKI Client
- ? Любое сертифицированное СКЗИ

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-3676 от "12" апреля 2019 г.

Действителен до "12" апреля 2022 г.

Выдан Открытому акционерному обществу «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»).
Обществу с ограниченной ответственностью «Линия защиты» (ООО «Линза»).

Настоящий сертификат удостоверяет, что изделие ViPNet TLS Gateway (исполнения 1, 2, 3, 5) в комплектации согласно формуляру ФРКЕ.00169-01 30 01 ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнения 5), класса КС3 (для исполнений 1, 2, 3), 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 ОАО «ИнфоТеКС» сертификационных испытаний образцов продукции №№ 906-000501, 906-000502, 906-000503, 906-000504.

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00169-01 30 01 ФО.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России А.М. Ивашко

Настоящий сертификат внесён в Государственный реестр сертифицированных средств защиты информации 12 апреля 2019 г.

Первый заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России В.Н. Мартынов

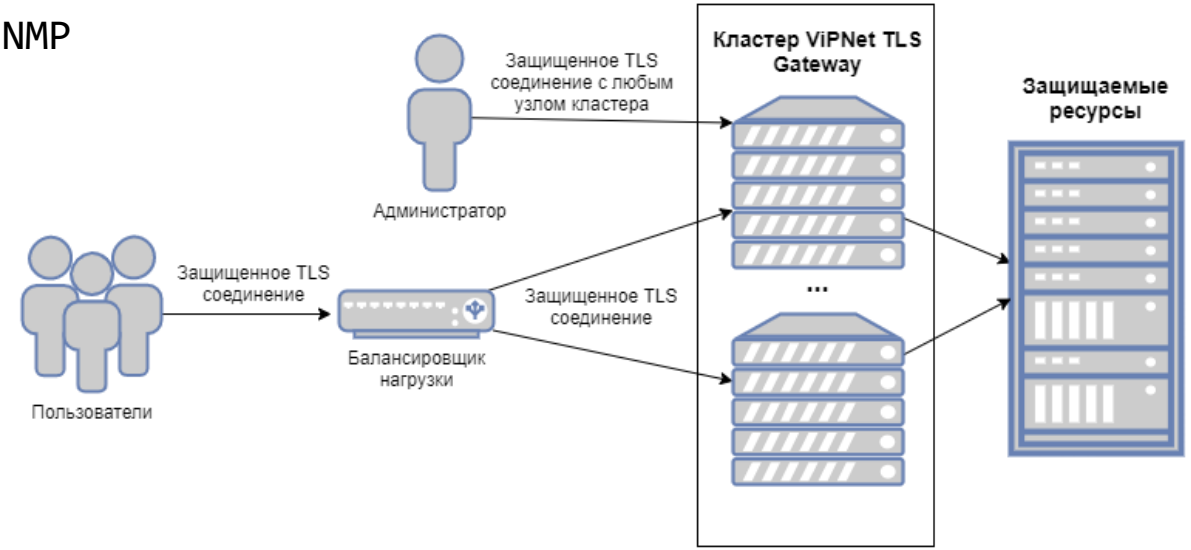
ViPNet TLS Gateway сертифицирован

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

ViPNet TLS Gateway 2

Новые возможности

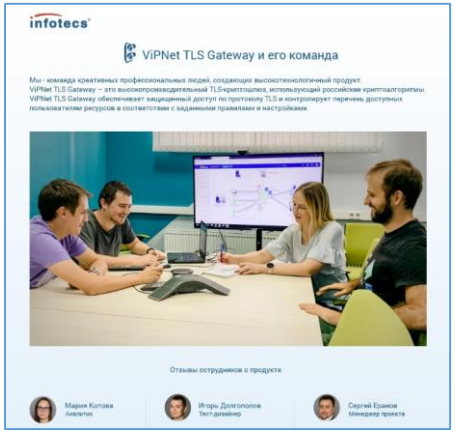
- Кластер (2 – 64 узла)
- Настройка сети с IPv6
- Мониторинг шлюза по SNMP
- Проверка статусов сертификатов по OCSP

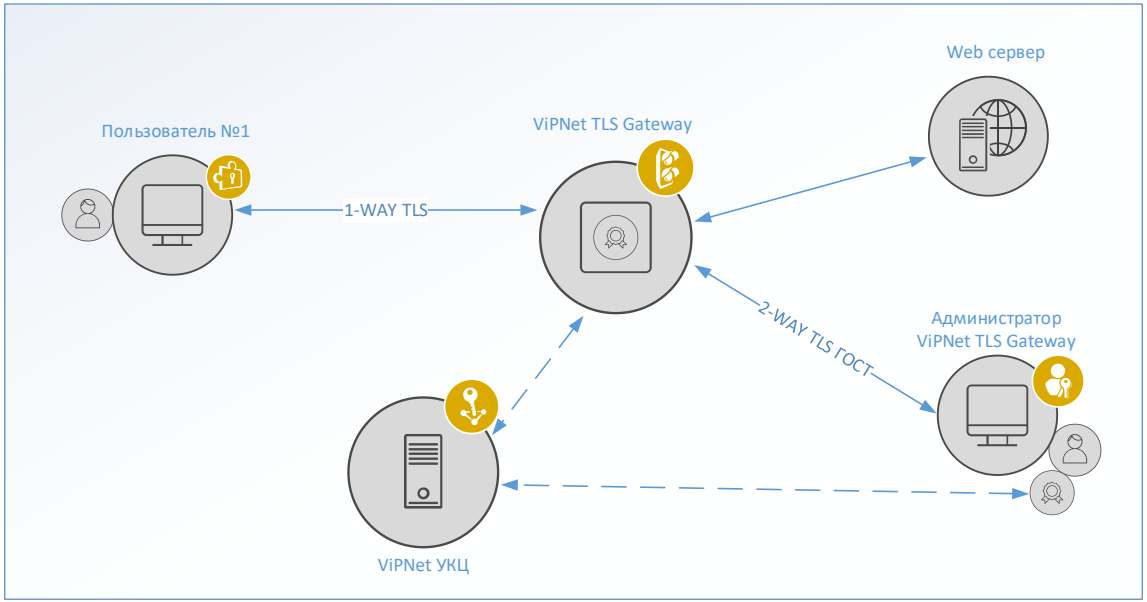


Демонстрация

Сценарий: Прозрачный режим

Доступ по DNS-имени ресурса – web1:

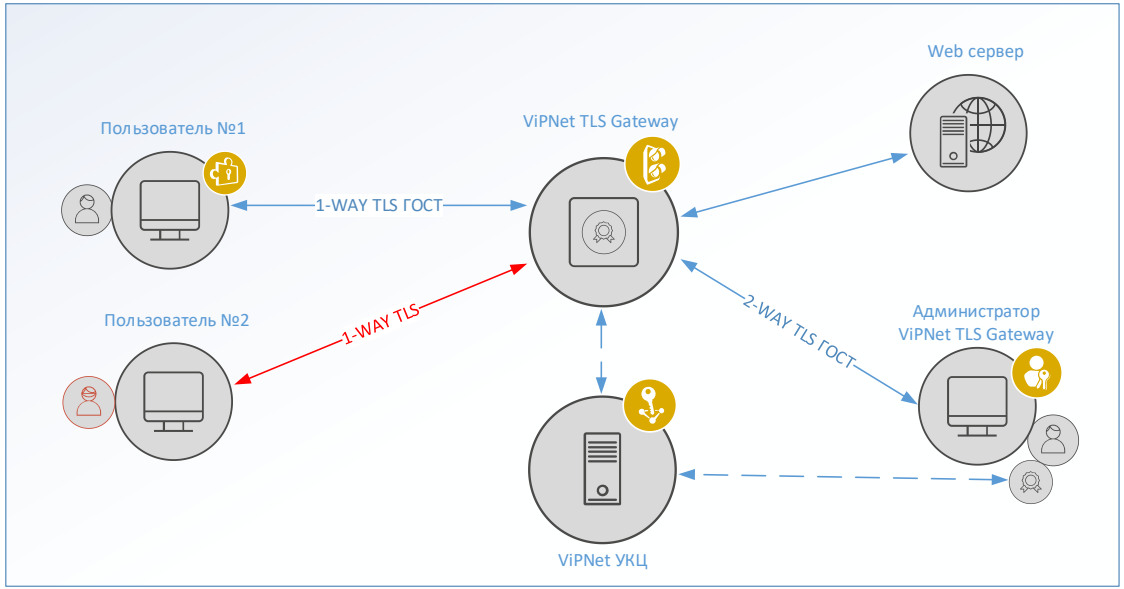




Сценарий: Дуальный режим

Доступ по DNS-имени ресурса – web1.

Приоритет у ГОСТ-сертификата.



ТЕХНО 2021 infotecs Фест

Спасибо за внимание!

Еранов Сергей

sergey.eranov@infotecs.ru

Подписывайтесь на наши соцсети

@infotecs.ru

@vpninfotecs

@InfoTeCS_Moscow