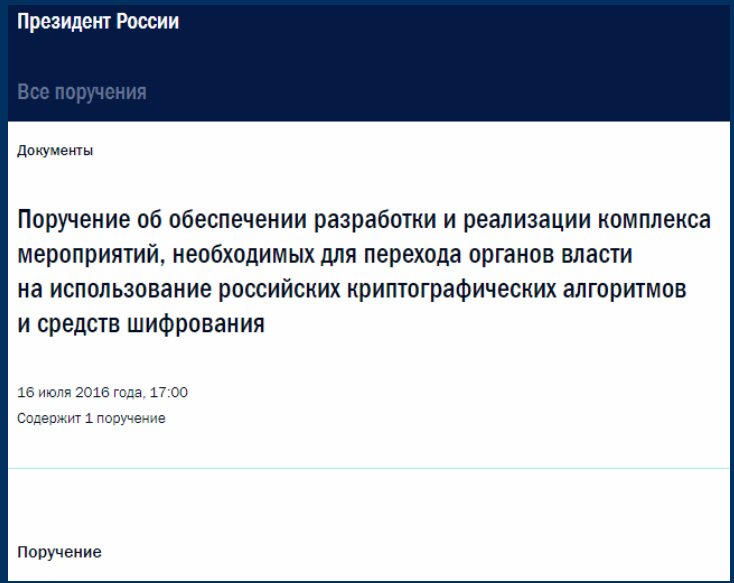
Как организовать защиту портальных решений с использованием ViPNet TLS Gateway

TLS ГОСТ: зачем «оно» нам надо?

Причина №1: активное распространение.

- ✓ Исполнение поручения президента от 16.07.2016 №ПР-1380 (ФОИВ, органы гос.власти субъектов РФ и т.д. должны перейти на использование российских криптоалгоритмов и средств шифрования при электронном взаимодействии между собой, с гражданами и организациями).
- ✓ Директива А.Г. Силуанова от 06.12.2018 о преимущественном использовании отечественного ПО в АО с гос.участием до 2021 года.
- ✓ Использование в проектах, например, в ЕБС.



Президент России

Все поручения

Документы

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

16 июля 2016 года, 17:00

Содержит 1 поручение

Поручение

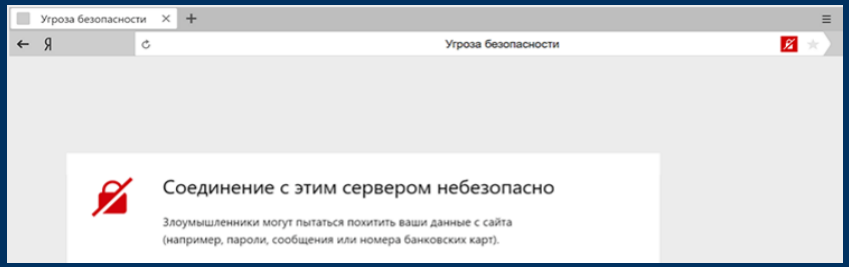
TLS ГОСТ: зачем «оно» нам надо?

Причина №2: надежность и независимость.

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

4 июня 2018 года GeoTrust отозвала сертификат, выданный для сайта Общественной палаты.

Ведется разработка Национального удостоверяющего центра



У нас есть техническое решение!

ТЕХНО 2020 infotecs ФЕСТ

Шлюз безопасности, обеспечивающий защиту каналов по протоколу TLS с использованием алгоритмов ГОСТ и не ГОСТ

01 02

ГОСТ Р 34.10-2001/2012,
ГОСТ Р 34.11-94/2012,
ГОСТ 28147-89
ГОСТ Р 34.12-2015 («Магма», «Кузнечик»)

Поддержка сертификатов, изданных разными УЦ, в т.ч. аккредитованными

03 04

Разные схемы аутентификации для защищаемых ресурсов

Поддержка политик разграничения доступа

05 06

Исполнения ПАК и VA

Решение сертифицировано!

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

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 «Лизэ»).

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

Модификации

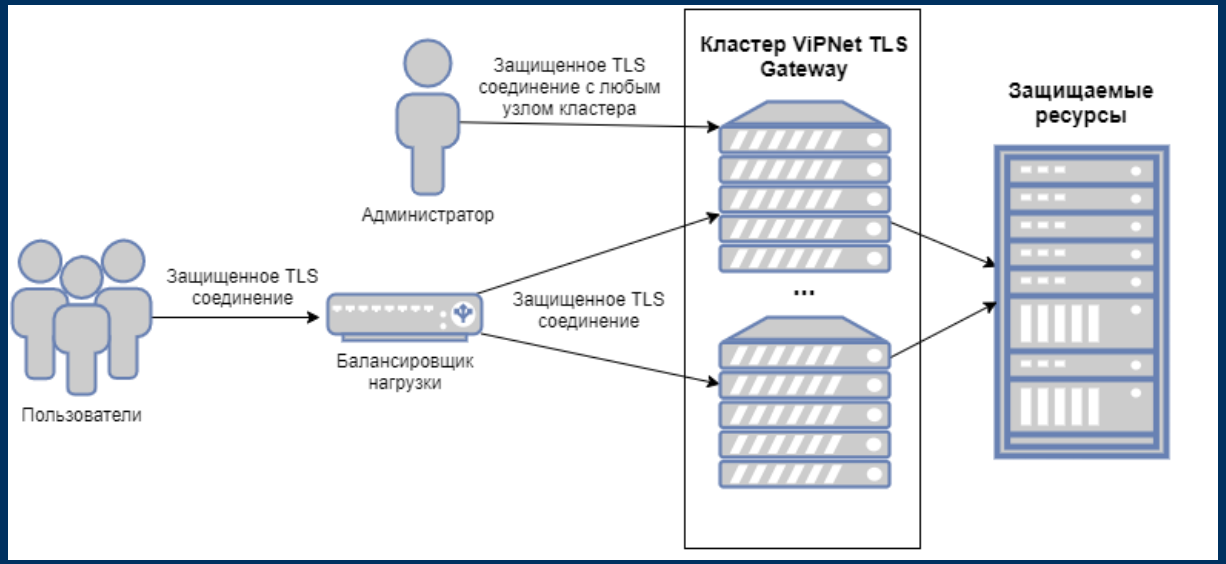
Платформы виртуализации:

- Oracle VM VirtualBox 5.1, 5.2, 6.0;
- VMware vSphere ESXi 6.0, 6.5, 6.7;
- VMware Workstation 14, 15.
- Kernel Virtual Machine

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

** Характеристики указаны для сценариев с использованием ГОСТ*

Уже скоро. TLS Gateway 2.0

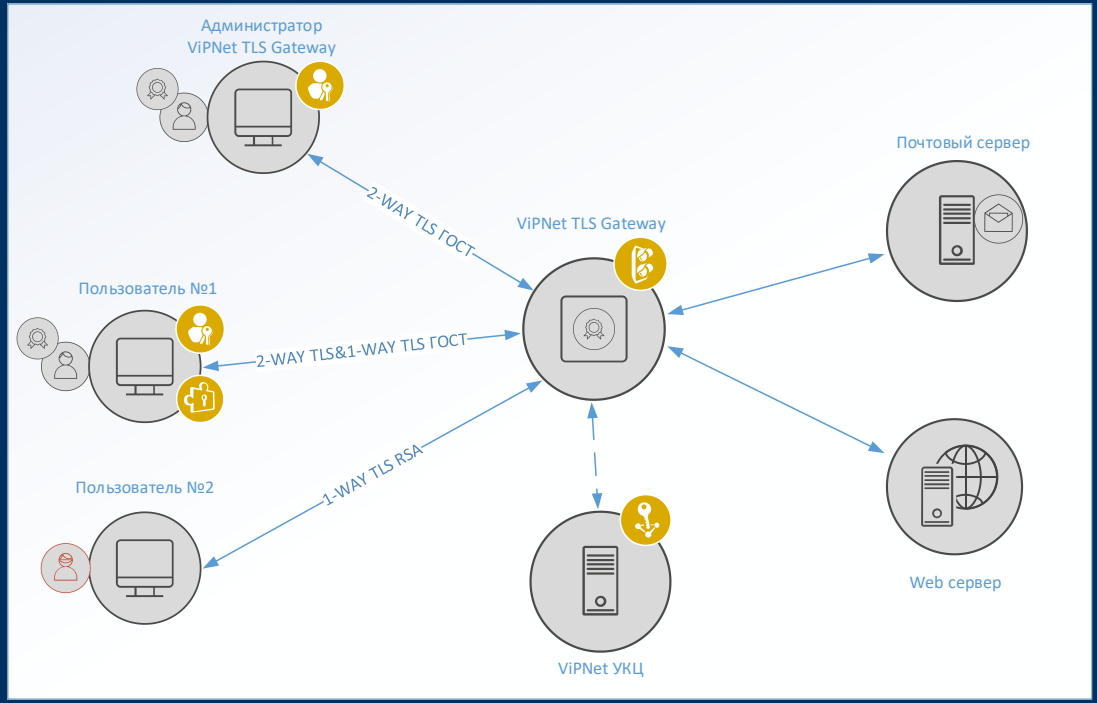


- Кластер
- IPv6
- OCSP
- SNMP

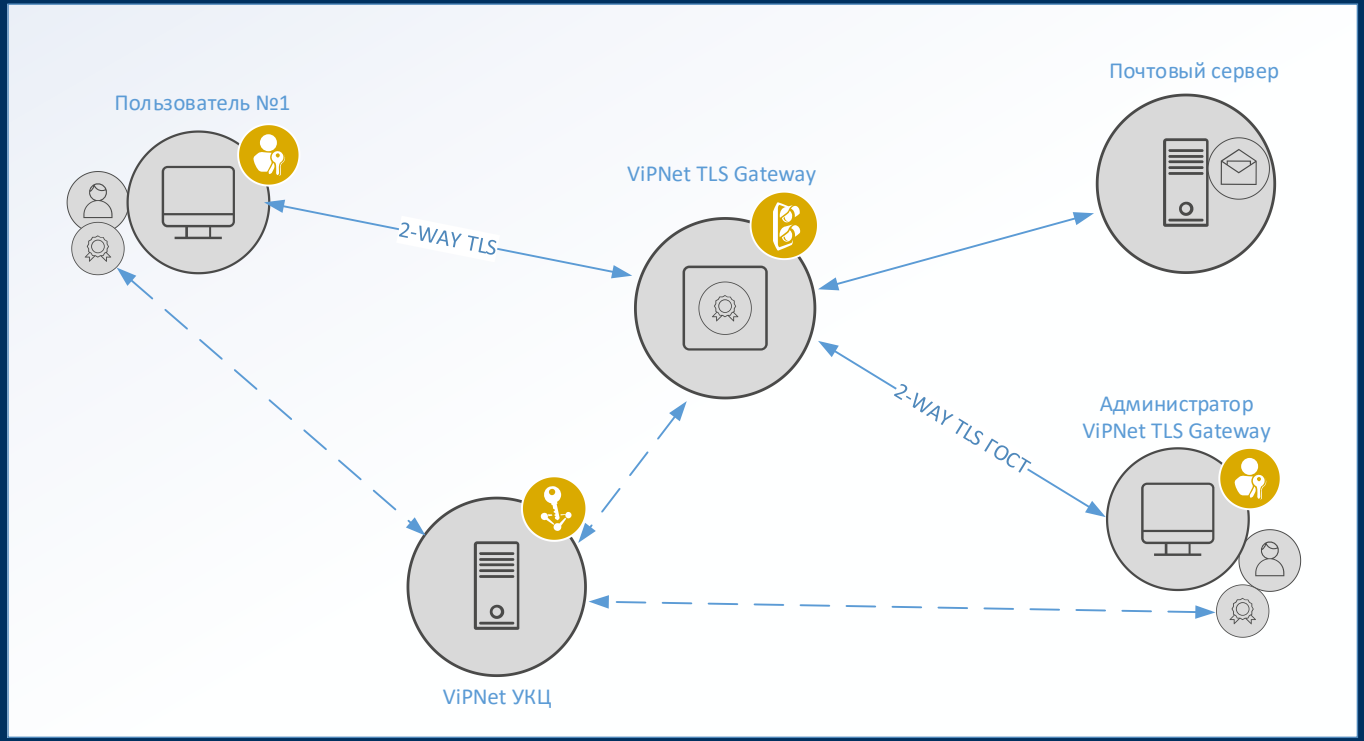
Хотите TLS ГОСТ? Смотрите как!

Сценарии мастер-класса:

1. *Портальный режим.*
2. *Прозрачный режим.*
3. *Дуальный режим.*

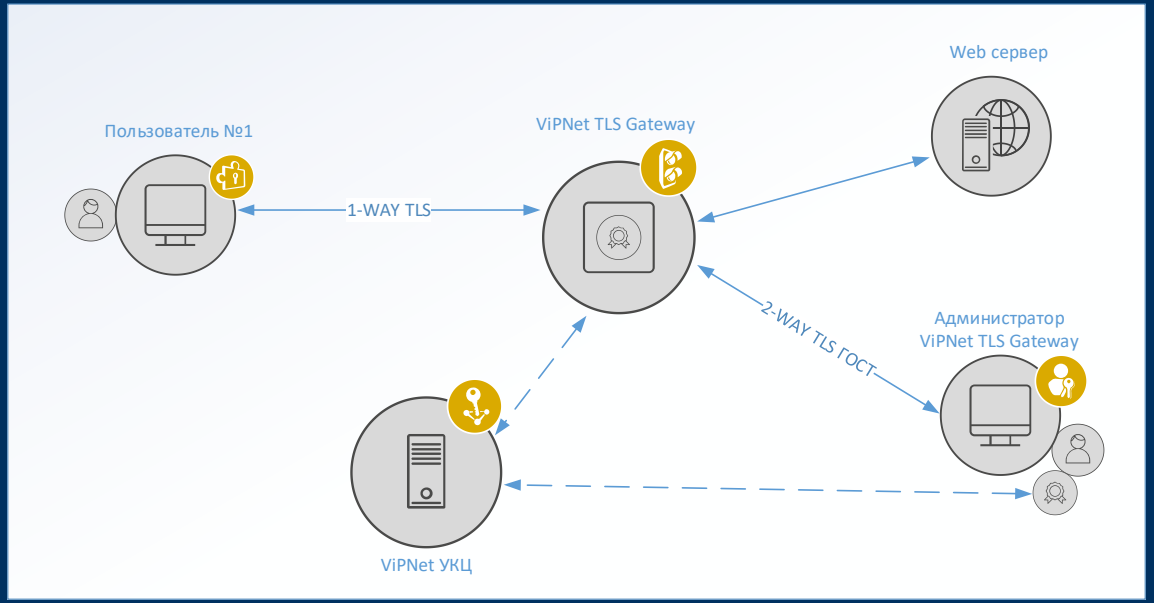


Сценарий: Портальный режим



Сценарий: Прозрачный режим

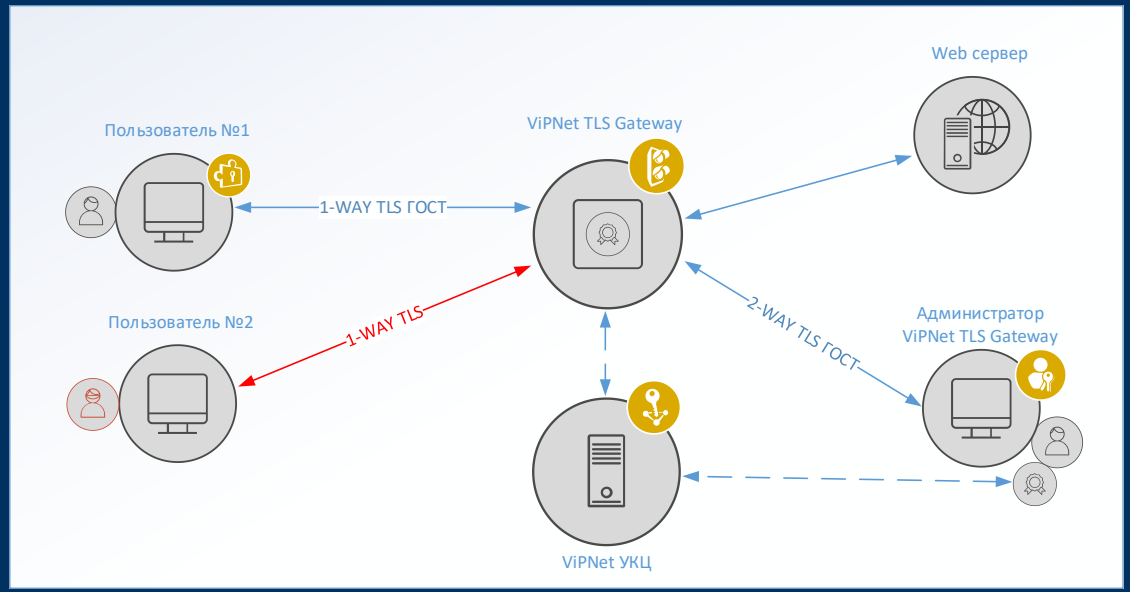
Доступ по dns-имени ресурса – web1:



Сценарий: Дуальный режим

Доступ по dns-имени ресурса – web1.

Приоритет у ГОСТ-сертификата.



ТЕХНО 2020 infotecs Фест

Спасибо за внимание!