Организация защищенного подключения к корпоративным ресурсам при помощи ViPNet TLS Gateway

Докладчики

Сергей Еранов

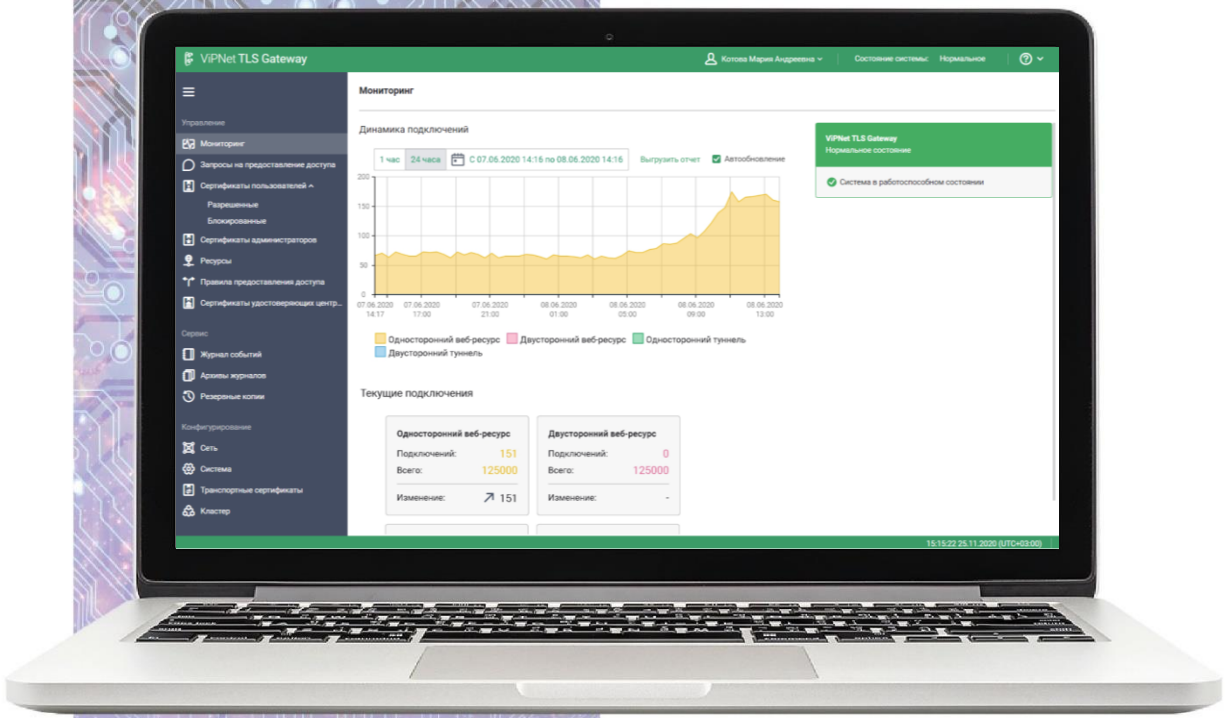
Начальник отдела разработки компонентов PKI

Игорь Долгополов

Менеджер проекта TLS Gateway

Что будет на мастер-классе?

- Расскажем о назначении продуктов ViPNet TLS Gateway и ViPNet PKI Client.
- Покажем, как легко и быстро подготовить TLS Gateway к работе.
- Подготовим всю инфраструктуру PKI в TLS Gateway.
- Как пользователь, подключимся к веб-ресурсу через TLS Gateway с аутентификацией клиента.
- Настроим работу через TLS Gateway к ресурсу с импортными криптоалгоритмами и подключимся к нему.



ViPNet TLS Gateway – это

высокопроизводительный TLS-криптошлюз, использующий российские и иностранные криптоалгоритмы.

Соответствует требованиям к СКЗИ, имеет сертификат ФСБ России по классам КС1 (VA) и КС3.

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+

Назначение ViPNet PKI Client

- Универсальный клиент для работы в инфраструктуре открытых ключей
- Простой и удобный

PKI Client: кроссплатформенный, кроссбраузерный и сертифицированный


ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-3411 от "20" июня 2018 г.

Действителен до "20" июня 2021 г.

Выдан Открытому акционерному обществу «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»).

Настоящий сертификат удостоверяет, что изделие ViPNet ... в комплектации согласно формуляру ФРКЕ.00175-01 30 01 ФО,

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнения 1), КС2 (для исполнения 2), КС3 (для исполнения 3), утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1 (для исполнения 1), КС2 (для исполнения 2), КС3 (для исполнения 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, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных ... сертификационных испытаний образца продукции ...

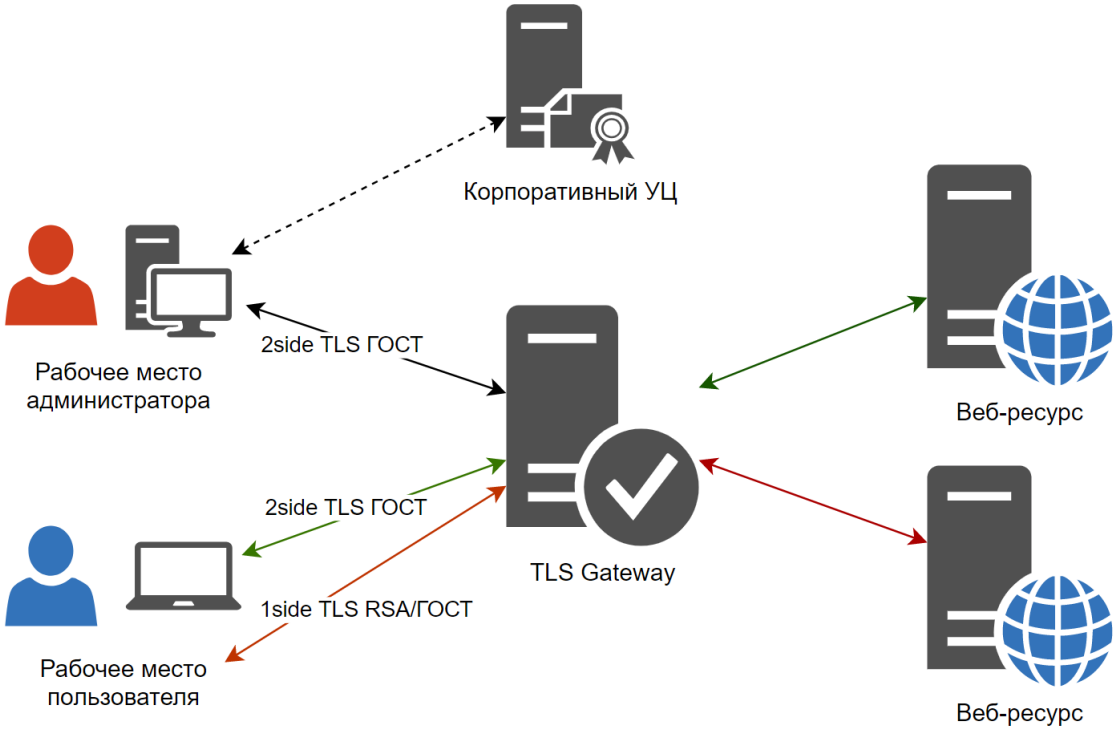
Безопасность информации обеспечивается при использовании ... в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00175-01 30 01 ФО.

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 25 декабря 2018 г.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России А.В. Парфенов

Схема демонстрационного стенда



Приступим!
Шаг 1. Рабочее место администратора

Настроим рабочее место администратора:

- Добавим сертификаты УЦ и CRL
- Создадим запрос на сертификат с алгоритмом ГОСТ
- Выпустим сертификат для администратора в корпоративном УЦ

Шаг 2. Инициализация TLS Gateway

Посмотрим как быстро и легко можно пройти инициализацию TLS Gateway:

- Установим новый пароль
- Настроим время
- Зададим сетевые настройки
- Выберем версии TLS-протокола
- Создадим запрос на транспортный сертификат с алгоритмом ГОСТ
- Добавим сертификаты УЦ и CRL
- Выпустим транспортный сертификат в корпоративном УЦ
- Загрузим транспортный сертификат
- Загрузим сертификат администратора

Шаг 3. Настройка TLS Gateway

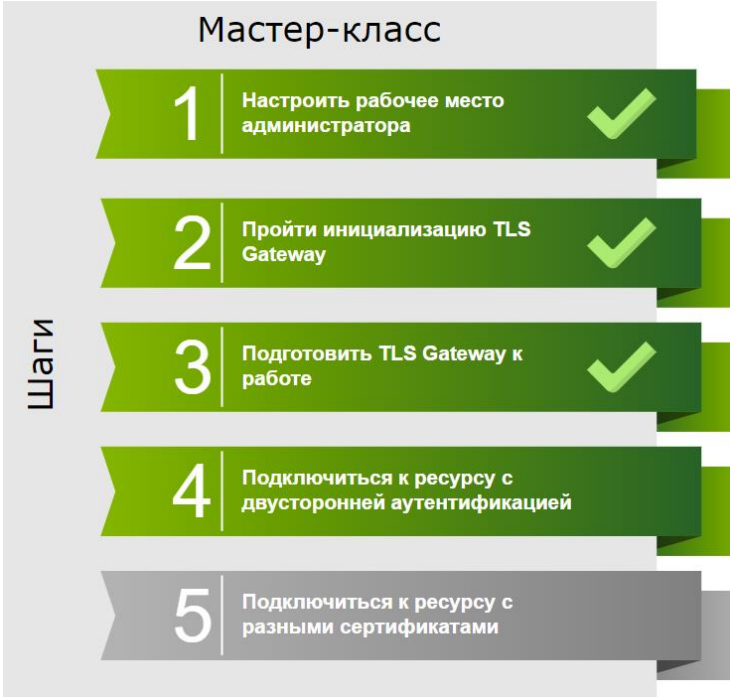
Подготовим TLS Gateway к работе:

- Настроим отдельный интерфейс для доступа пользователей
- Создадим запрос и выпустим транспортный сертификат для доступа к TLS Gateway по доменному имени, добавив в запрос доменное имя ресурса (для прямого доступа)
- Создадим веб-ресурс с двусторонней аутентификацией
- Настроим правило доступа, чтобы сертификат пользователя проверился и автоматически добавился в список разрешенных

Шаг 4. Подключение к веб-ресурсу с аутентификацией клиента

Посмотрим, как пользователю подключиться к веб-ресурсу с двусторонней аутентификацией через TLS Gateway:

- Подключимся к веб-ресурсу с рабочего места пользователя, используя PKI Client.



Шаг 5. Подключение к веб-ресурсу с разными сертификатами

Настроим для пользователя подключение к веб-ресурсу через TLS Gateway:

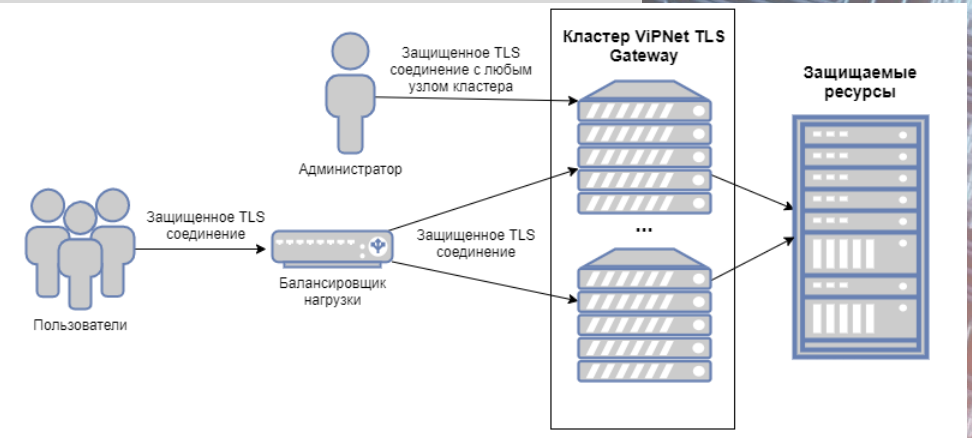
- Создадим веб-ресурс в TLS Gateway
- Добавим сертификат УЦ и CRL для сертификата с иностранным алгоритмом
- Загрузим файл PFX с сертификатом с иностранным алгоритмом (RSA)
- Покажем, что пользователь может подключиться к ресурсу по ГОСТ
- А если отключить поддержку ГОСТ (TLS Unit), то на тот же ресурс пользователь сможет попасть по RSA

Готово!

Мы выполнили все шаги и теперь TLS Gateway настроен для работы, а пользователи могут подключаться к защищаемым ресурсам.

Наши дополнительные возможности

- Кластер - повышение производительности, обеспечение отказоустойчивости (2 - 64 узла)



- Проверка статусов сертификатов по OCSP
- Мониторинг шлюза по SNMP
- Настройка сети с IPv6
- E-mail оповещения администраторов

Ответы на вопросы!

Еранов Сергей
Начальник отдела разработки компонентов PKI

Sergey.Eranov@infotecs.ru

Игорь Долгополов
Менеджер проекта TLS Gateway

Igor.Dolgopolov@infotecs.ru

infotecs

Спасибо
за внимание!