



ViPNet TLS Gateway

Руководство пользователя



© ОАО «ИнфоТеКС», 2019

ФРКЕ.00169-01 34 01

Версия продукта 1.4.0

Этот документ входит в комплект поставки продукта VipNet, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения ОАО «ИнфоТеКС».

VipNet® является зарегистрированным товарным знаком ОАО «ИнфоТеКС».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1, 2 этаж

Телефон: +7 (495) 737-6192, 8-800-250-0260 — бесплатный звонок из России (кроме Москвы)

Веб-сайт: <https://infotecs.ru>

Служба технической поддержки: hotline@infotecs.ru

Содержание

Введение	4
О документе.....	5
Для кого предназначен документ	5
Соглашения документа.....	5
О ViPNet TLS Gateway	6
Обратная связь.....	7
Глава 1. Общие сведения	8
Способы подключения пользователей к ViPNet TLS Gateway для доступа к ресурсам	9
Подключение по каналу TLS с двусторонней аутентификацией.....	9
Подключение по каналу TLS с односторонней аутентификацией.....	11
Требования к компьютеру пользователя для подключения к веб-интерфейсу ViPNet TLS Gateway	12
Глава 2. Подключение пользователей к ресурсам по протоколу TLS с двусторонней аутентификацией	13
Порядок организации защищенного подключения нового пользователя к ресурсам по протоколу TLS с двусторонней аутентификацией	14
Требования к сертификатам пользователей	15
Настройка параметров веб-браузера для подключения по протоколу TLS	17
Подключение к доступным ресурсам.....	18
Отправка запроса на доступ к ресурсам.....	20
Глава 3. Подключение пользователей к ресурсам по протоколу TLS с односторонней аутентификацией	23
Порядок организации защищенного подключения нового пользователя к ресурсам по протоколу TLS с односторонней аутентификацией	24
Подключение к доступным ресурсам.....	26
Приложение А. Глоссарий	28



Введение

О документе	5
О ViPNet TLS Gateway	6
Обратная связь	7

О документе

Для кого предназначен документ

Документ предназначен для пользователей, которым необходимо настроить защищенный удаленный доступ к веб-ресурсам корпоративной сети через ViPNet TLS Gateway.

Соглашения документа

Ниже перечислены соглашения, принятые в этом документе для выделения информации.

Таблица 1. Обозначения, используемые в примечаниях




Обозначение	Описание
	Внимание! Указывает на обязательное для исполнения или следования действие или информацию.
	Примечание. Указывает на необязательное, но желательное для исполнения или следования действие или информацию.
	Совет. Содержит дополнительную информацию общего характера.

Таблица 2. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
Название	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.
Клавиша+Клавиша	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
Меню > Подменю > Команда	Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации.
Код	Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки.

О ViPNet TLS Gateway

Изделие ViPNet TLS Gateway (далее — ViPNet TLS Gateway) позволяет организовывать безопасный удаленный доступ пользователей к корпоративным информационным веб-ресурсам и туннелируемым ресурсам из любых точек мира путем создания защищенных каналов передачи данных на базе протокола TLS, обеспечивая тем самым криптографически защищенное соединение. При этом ViPNet TLS Gateway позволяет контролировать удаленный доступ пользователей к этим ресурсам.

Удаленный доступ пользователей осуществляется без их прямого обращения к адресам ресурсов за счет прохождения всего трафика через ViPNet TLS Gateway, предоставляющего функции прокси-сервера.

Пользователям для безопасного доступа к ресурсам не нужно устанавливать специальное программное обеспечение на своих компьютерах кроме сертифицированного средства криптографической защиты информации (ViPNet CSP, ViPNet PKI Client или криптопровайдера сторонних производителей).



Примечание. Подключение к туннелируемым ресурсам возможно только в программе ViPNet PKI Client версии не ниже 1.3.

ViPNet TLS Gateway выпускается в следующих исполнениях: TLS 500, TLS 1000, TLS 5000 и TLS VA.

ViPNet TLS Gateway в исполнениях TLS 500/1000/5000 представляет собой программно-аппаратный комплекс (далее — ПАК) на базе специализированной аппаратной платформы и программного обеспечения (далее — ПО) ViPNet TLS Gateway, которое функционирует под управлением адаптированной операционной системы (далее — ОС) Debian.

ViPNet TLS Gateway в исполнении TLS 1000 поставляется совместно с модулем Web Application Firewall (далее — WAF) производства компании Positive Technologies. Для использования модуля WAF необходима соответствующая лицензия.

Модуль WAF — самообучающийся динамический межсетевой экран, способный снижать риски атак на приложения при их появлении. Подробнее о WAF см. документ .

ViPNet TLS Gateway в исполнении TLS VA представляет собой программную реализацию ПАК, предназначенную для развертывания в среде виртуализации.

Обратная связь

Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте ОАО «ИнфоТекС»:

- Информация о продуктах ViPNet <https://infotecs.ru/product/>.
- Информация о решениях ViPNet <https://infotecs.ru/resheniya/>.
- Часто задаваемые вопросы <https://infotecs.ru/support/faq/>.
- Форум пользователей продуктов ViPNet <https://infotecs.ru/forum/>.

Контактная информация

Если у вас есть вопросы, свяжитесь со специалистами ОАО «ИнфоТекС»:

- Единый многоканальный телефон:
+7 (495) 737-6192,
8-800-250-0-260 — бесплатный звонок из России (кроме Москвы).
- Служба технической поддержки: hotline@infotecs.ru.
Форма для обращения в службу технической поддержки через сайт <https://infotecs.ru/support/request/>.
Консультации по телефону для клиентов с расширенной схемой технической поддержки:
+7 (495) 737-6196.
- Отдел продаж: soft@infotecs.ru.

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов ОАО «ИнфоТекС» регулируется политикой ответственного разглашения <https://infotecs.ru/disclosure.php>.

1

Общие сведения

Способы подключения пользователей к ViPNet TLS Gateway для доступа к ресурсам	9
Требования к компьютеру пользователя для подключения к веб-интерфейсу ViPNet TLS Gateway	12

Способы подключения пользователей к ViPNet TLS Gateway для доступа к ресурсам

Удаленный доступ пользователей к корпоративным веб-ресурсам (далее — ресурсам) сети осуществляется через ViPNet TLS Gateway по защищенному каналу TLS. При этом аутентификация пользователя и ViPNet TLS Gateway может производиться одним из следующих способов:

- Двусторонняя аутентификация (см. [Подключение по каналу TLS с двусторонней аутентификацией](#) на стр. 9).
- Односторонняя аутентификация (см. [Подключение по каналу TLS с односторонней аутентификацией](#) на стр. 11).

Для возможности получения доступа к ресурсам пользователи должны настроить на своем рабочем месте защищенное подключение к ViPNet TLS Gateway по протоколу TLS одним из следующих способов:

- Порядок организации защищенного подключения нового пользователя к ресурсам по протоколу TLS с двусторонней аутентификацией (на стр. 14).
- Порядок организации защищенного подключения нового пользователя к ресурсам по протоколу TLS с односторонней аутентификацией (на стр. 24).

Подключение по каналу TLS с двусторонней аутентификацией

Для установки защищенного соединения по протоколу TLS и двусторонней аутентификации пользователя на его рабочем месте, с которого будет происходить подключение к ViPNet TLS Gateway, должны использоваться ключи электронной подписи и соответствующий им сертификат. Их использование обеспечивает криптографически защищенное соединение. При этом низкоуровневые криптографические функции может выполнять криптопровайдер ViPNet CSP или криптопровайдер сторонних производителей, который необходимо установить на компьютере пользователя.

Сертификаты пользователей могут быть изданы в любом сертифицированном УЦ. На ViPNet TLS Gateway должно быть установлено доверие к УЦ, где изданы сертификаты пользователей. Администратор должен добавить сертификат пользователя на ViPNet TLS Gateway и явно разрешить или запретить пользователю доступ к каждому ресурсу (вручную или по запросу пользователя), для которых на ViPNet TLS Gateway настроена возможность получения доступа при двусторонней аутентификации. Пользователям также будут доступны те ресурсы, для которых на

ViPNet TLS Gateway настроена возможность получения доступа по каналу TLS с односторонней аутентификацией.

Доступ пользователя к ресурсам по каналу TLS с двусторонней аутентификацией возможен при наличии у него следующих сертификатов:

- Сертификата пользователя.
- Сертификата УЦ, в котором издан сертификат пользователя.
- Сертификата УЦ, в котором изданы транспортные сертификаты ViPNet TLS Gateway.
- Если какой-либо из вышеуказанных сертификатов УЦ не является корневым, то потребуются сертификаты всех УЦ, образующие [цепочку доверия к сертификатам УЦ, выпустившим сертификаты \(пользователя и ViPNet TLS Gateway\)](#) (см. глоссарий, стр. 31).

Все сертификаты должны быть действительными и установлены на компьютере пользователя в системное хранилище ОС. Корневые сертификаты устанавливаются в хранилище **Доверенные корневые центры сертификации**. Остальные сертификаты УЦ из цепочки доверия устанавливаются в хранилище **Промежуточные центры сертификации**.

При подключении пользователей к ViPNet TLS Gateway с использованием двусторонней аутентификации по протоколу TLS производятся следующие проверки:

- Со стороны пользователя проверяется [транспортный сертификат ViPNet TLS Gateway](#) (см. глоссарий, стр. 30) и IP-адрес (или DNS-имя) интерфейса подключения по TLS-каналу с двусторонней аутентификацией, прописанные в данном сертификате. Действительность транспортного сертификата проверяется с помощью корневого сертификата УЦ, в котором издан транспортный сертификат ViPNet TLS Gateway, установленного на компьютере пользователя или с помощью [цепочки доверия к сертификату](#) (см. глоссарий, стр. 31).
- Со стороны ViPNet TLS Gateway проверяется:
 - Действительность сертификата пользователя,



Внимание! Чтобы успешно проводилась проверка действительности сертификатов по времени, время на ViPNet TLS Gateway и в УЦ должно быть синхронизировано.

- Наличие сертификата пользователя в списке разрешенных сертификатов пользователей.
- Что установлено доверие к УЦ, где изданы сертификаты пользователей.

При успешной аутентификации будет установлено защищенное взаимодействие и отобразится главная страница ViPNet TLS Gateway со списком доступных веб-ресурсов (если есть) (см. [Подключение к доступным ресурсам](#) на стр. 18) и кнопкой запроса необходимых ресурсов (см. [Отправка запроса на доступ к ресурсам](#) на стр. 20).

Подключение по каналу TLS с односторонней аутентификацией

Для доступа пользователя к ресурсам по каналу TLS с односторонней аутентификацией достаточно иметь только действительный корневой сертификат УЦ, в котором изданы транспортные сертификаты ViPNet TLS Gateway. Если сертификат УЦ не является корневыми, то потребуются сертификаты всех УЦ, образующие [цепочку доверия к сертификатам](#) (см. глоссарий, стр. 31). Пользователям будут доступны только те ресурсы, для которых на ViPNet TLS Gateway настроена возможность получения доступа при односторонней аутентификации. Доступ к этим ресурсам не разграничивается.

Все сертификаты должны быть установлены на компьютере пользователя в системное хранилище ОС. Корневые сертификаты устанавливаются в хранилище **Доверенные корневые центры сертификации**. Остальные сертификаты УЦ из цепочки доверия устанавливаются в хранилище **Промежуточные центры сертификации**.

При подключении пользователей к ViPNet TLS Gateway с использованием односторонней аутентификации по протоколу TLS со стороны пользователя проверяется [транспортный сертификат ViPNet TLS Gateway](#) (см. глоссарий, стр. 30) и IP-адрес (или DNS-имя) интерфейса подключения по TLS-каналу с односторонней аутентификацией, прописанные в данном сертификате.

Действительность транспортного сертификата проверяется с помощью корневого сертификата УЦ, в котором издан транспортный сертификат ViPNet TLS Gateway, установленного на компьютере пользователя или с помощью [цепочки доверия к сертификату](#) (см. глоссарий, стр. 31).

При успешной аутентификации будет установлено защищенное взаимодействие и отобразится главная страница ViPNet TLS Gateway со списком доступных веб-ресурсов (если они есть) (см. [Подключение к доступным ресурсам](#) на стр. 26).

Требования к компьютеру пользователя для подключения к веб-интерфейсу ViPNet TLS Gateway

Для подключения к веб-интерфейсу ViPNet TLS Gateway по защищенному каналу на компьютере пользователя должно быть установлено следующее программное обеспечение:

- Операционная система — Windows 7 SP1 (32/64-разрядная), Windows Server 2008 R2 SP1 (64-разрядная), Windows 8 (32/64-разрядная), Windows Server 2012 (64-разрядная), Windows 8.1 (32/64-разрядная), Windows Server 2012 R2 (64-разрядная), Windows 10 (32/64-разрядная).

Для операционной системы рекомендуется установить последний пакет обновлений.

- Криптопровайдер:
 - ViPNet CSP:
 - Для ОС Windows 10 — версии 4.2 (8.51670) и выше.
 - Для остальных ОС Windows — версии 4.2.2 и выше.
 - ViPNet PKI Client версии 1.1 и выше.
 - Криптопровайдер сторонних производителей.
- Веб-браузер:
 - При использовании совместно с ViPNet CSP — Internet Explorer 11.
 - При использовании совместно с ViPNet PKI Client — Internet Explorer 11, а также Edge, Google Chrome, Mozilla Firefox, «Спутник» последних версий.



Примечание. Для корректного отображения страниц веб-интерфейса установите разрешение экрана не менее 1280x800.

2

Подключение пользователей к ресурсам по протоколу TLS с двусторонней аутентификацией

Порядок организации защищенного подключения нового пользователя к ресурсам по протоколу TLS с двусторонней аутентификацией	14
Подключение к доступным ресурсам	18
Отправка запроса на доступ к ресурсам	20

Порядок организации защищенного подключения нового пользователя к ресурсам по протоколу TLS с двусторонней аутентификацией

Для организации защищенного подключения к ViPNet TLS Gateway вам потребуются:

- Контейнер ключей и сертификат пользователя.
- Сертификат УЦ, в котором издан ваш сертификат, а если сертификат УЦ не является корневым, то все сертификаты УЦ из [цепочки доверия к сертификатам этого УЦ](#) (см. глоссарий, стр. 31).
- Сертификат УЦ, в котором изданы транспортные сертификаты ViPNet TLS Gateway, а если сертификат УЦ не является корневым, то все сертификаты УЦ из [цепочки доверия к сертификатам этого УЦ](#) (см. глоссарий, стр. 31).
- Адрес ViPNet TLS Gateway для подключения пользователей по TLS-каналу с двусторонней аутентификацией. Адрес подключения к ViPNet TLS Gateway вы можете получить у администратора ViPNet TLS Gateway.

Чтобы организовать защищенное подключение по протоколу TLS с двусторонней аутентификацией и получить доступ к необходимым ресурсам, выполните все действия из приведенного ниже списка:



Внимание! Если у вас уже имеются установленные в системное хранилище сертификат пользователя и необходимые сертификаты вашего удостоверяющего центра, первый и второй шаги выполнять не нужно.

Таблица 3. Порядок организации защищенного подключения нового пользователя к ViPNet TLS Gateway для доступа к ресурсам

Действие	Ссылка
<input type="checkbox"/> На своем рабочем месте создайте запрос на сертификат пользователя с помощью программы ViPNet CSP версии не ниже 4.2 (2.36190) или стандартных средств криптопровайдеров сторонних производителей. Передайте его администратору вашего УЦ для издания сертификата	См. документ «ViPNet CSP. Руководство пользователя» или см. документацию к соответствующим средствам Требования к сертификатам пользователей (на стр. 15)

Действие	Ссылка
<input type="checkbox"/> Получите изданный сертификат пользователя, а также сертификаты УЦ из цепочки доверия к сертификатам вашего УЦ у администратора вашего УЦ и установите их в системное хранилище с помощью программы ViPNet CSP или стандартных средств операционной системы	См. документ «ViPNet CSP. Руководство пользователя» или см. документацию к соответствующим средствам
<input type="checkbox"/> Получите сертификаты УЦ из цепочки доверия к сертификатам УЦ, в котором изданы транспортные сертификаты ViPNet TLS Gateway, у администратора ViPNet TLS Gateway, и установите их в системное хранилище с помощью стандартных средств операционной системы	См. документацию к соответствующим средствам
<input type="checkbox"/> Настройте параметры веб-браузера для защищенного подключения по протоколу TLS	Настройка параметров веб-браузера для подключения по протоколу TLS (на стр. 17)
<input type="checkbox"/> Подключитесь к веб-интерфейсу ViPNet TLS Gateway с помощью установленного сертификата пользователя и откройте доступные ресурсы или запросите доступ к необходимым ресурсам	Подключение к доступным ресурсам (на стр. 18) Отправка запроса на доступ к ресурсам (на стр. 20)



Совет. Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

Требования к сертификатам пользователей

Для аутентификации пользователя при подключении к веб-интерфейсу ViPNet TLS Gateway по протоколу TLS с двусторонней аутентификацией необходим сертификат, удовлетворяющий следующим требованиям:

- Сертификаты изданы в сертифицированном удостоверяющем центре (по требованиям к средствам УЦ по классу КСЗ, например, в ПО ViPNet Удостоверяющий центр).
- Формат сертификата: X.509.
- Назначение сертификата: подпись и шифрование.
- Алгоритм подписи: ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, RSA или ECDSA.
- Иметь расширение «Расширенное использование ключа» с назначением ключа «Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)».
- Сертификат должен быть действительным:
 - Срок действия сертификата наступил и не истек.

- Сертификат не находится в списке [аннулированных сертификатов удостоверяющего центра](#) (см. глоссарий, стр. 30).
- [Цепочка доверия к сертификату](#) (см. глоссарий, стр. 31) полна, и все входящие в нее сертификаты удостоверяющих центров действительны.
- Файл с сертификатом может иметь одно из следующих расширений: *.cer, *.crt или *.pem.
- Ограничения на максимальную длину строковых полей сертификатов представлены в таблице ниже.

Таблица 4. Ограничения на строковые поля сертификатов

Имя поля	Обозначение и описание	Ограничение
Обязательные поля		
Subject.CN	Наименование (общее имя субъекта)	до 64 символов
Subject.O	Организация	до 1024 символов
Subject.SNILS	СНИЛС	11 цифр
Issuer.CN	Выпущен (общее имя издателя)	до 64 символов
Valid from	Действителен с	дата
Valid to	Действителен до	дата
Необязательные поля		
Subject.SN	Фамилия (фамилия уполномоченного лица, получающего сертификат). Может совпадать с Subject.CN	до 40 символов
Subject.GN	Имя и отчество (уполномоченного лица)	до 64 символов
Subject.T	Должность (уполномоченного лица)	до 64 символов
Subject.OU	Подразделение	до 64 символов
Subject.STREET	Улица (название улицы, номер дома)	до 30 символов
Subject.L	Город (населенный пункт)	до 128 символов
Subject.S	Код субъекта РФ (код и название субъекта федерации согласно классификатору КЛАДР)	до 128 символов
Subject.C	Страна (двухсимвольный код страны)	2 символа
Subject.E	Адрес электронной почты	до 255 символов
Subject.INN	ИНН	10-12 цифр
Subject.OGRN	ОГРН	13 цифр

Настройка параметров веб-браузера для подключения по протоколу TLS

Чтобы произвести настройки веб-браузера для защищенного подключения по протоколу TLS к веб-интерфейсу ViPNet TLS Gateway, выполните следующие действия:

- 1 Откройте веб-браузер Microsoft Internet Explorer и в меню **Сервис** выберите пункт **Свойства браузера**.
- 2 В открывшемся окне перейдите на вкладку **Дополнительно** и проверьте, что установлен флажок **Использовать TLS 1.2**, разрешающий соединения по TLS-протоколу версии 1.2.
- 3 Перейдите на вкладку **Безопасность** и убедитесь, что снят флажок **Включить защищенный режим**.
- 4 Нажмите кнопку **ОК**.

Также для корректной работы с веб-интерфейсом ViPNet TLS Gateway в свойствах браузера необходимо разрешить использование Cookie.

В результате будут настроены параметры для установления защищенного соединения с веб-интерфейсом ViPNet TLS Gateway. Далее можете подключиться к веб-интерфейсу ViPNet TLS Gateway.

Подключение к доступным ресурсам

Если у вас уже организовано защищенное подключение по протоколу TLS с двусторонней аутентификацией к ViPNet TLS Gateway (см. [Порядок организации защищенного подключения нового пользователя к ресурсам по протоколу TLS с двусторонней аутентификацией](#) на стр. 14) и администратор предоставил вам доступ к ресурсам, вы можете подключиться к ним одним из следующих способов:

- Сначала подключиться к веб-интерфейсу ViPNet TLS Gateway, а затем выбрать необходимые ресурсы.
- Сразу подключиться к нужному вам ресурсу (если вам известен адрес подключения к ресурсу). Адрес подключения к ресурсу вы можете получить у администратора ViPNet TLS Gateway.
- Подключиться к нужному ресурсу непосредственно по его адресу, если настроена такая возможность (подробнее см. документ «ViPNet TLS Gateway. Руководство администратора», раздел «Настройка подключения к защищаемым ресурсам непосредственно по их адресам»). Адрес ресурса вы можете получить у администратора ViPNet TLS Gateway.

Для подключения первым способом выполните следующие действия:

- 1 Откройте веб-браузер Internet Explorer и в адресной строке введите адрес в формате:

`https://<Адрес ViPNet TLS Gateway для подключения пользователей по TLS-каналу с двусторонней аутентификацией:порт>`.



Внимание! Если для защищенных подключений пользователей по TLS-каналу с двусторонней аутентификацией используется порт 443, заданный по умолчанию, в адресной строке порт можно не указывать:

`https://<Адрес ViPNet TLS Gateway для подключения пользователей по TLS-каналу с двусторонней аутентификацией>`

- 2 В появившемся окне со списком сертификатов выберите свой сертификат, который вы установили в системное хранилище (см. [Порядок организации защищенного подключения нового пользователя к ресурсам по протоколу TLS с двусторонней аутентификацией](#) на стр. 14).

После успешной аутентификации будет установлено защищенное соединение по протоколу TLS и откроется главная страница ViPNet TLS Gateway со списком доступных ресурсов.

- 3 Щелкните плитку нужного вам ресурса.

В результате откроется страница выбранного вами ресурса.

Для подключения сразу к нужному вам ресурсу выполните следующие действия:

- 1 Откройте веб-браузер Internet Explorer и в адресной строке введите имеющийся у вас адрес подключения к ресурсу, например, адрес подключения к ресурсу может выглядеть следующим образом: `https://192.168.81.83:4431/wiki`.
- 2 В появившемся окне со списком сертификатов выберите свой сертификат, который вы установили в системное хранилище.

После успешной аутентификации будет установлено защищенное соединение по протоколу TLS и откроется страница выбранного вами ресурса.

Примечание. Если доступ к подключаемому ресурсу был заблокирован администратором, откроется главная страница ViPNet TLS Gateway со списком доступных ресурсов и кнопкой создания запроса на предоставление доступа к нужным вам ресурсам (см. [Отправка запроса на доступ к ресурсам](#) на стр. 20).



Если администратор заблокировал вам доступ к ViPNet TLS Gateway и ко всем ресурсам, откроется страница с информацией о запрете доступа к ресурсам. Для выяснения причины блокировки свяжитесь с администратором по адресу электронной почты, указанному на странице блокировки.

Отправка запроса на доступ к ресурсам

Если у вас уже организовано защищенное подключение по протоколу TLS с двусторонней аутентификацией к ViPNet TLS Gateway (см. [Порядок организации защищенного подключения нового пользователя к ресурсам по протоколу TLS с двусторонней аутентификацией](#) на стр. 14), но администратор еще не предоставил вам доступ к ресурсам или доступ есть, но вам необходим доступ еще к каким-либо ресурсам, вы можете подключиться к ViPNet TLS Gateway и отправить администратору запрос на предоставление вам доступа к нужным ресурсам.

Для создания и отправки запроса на предоставление доступа к ресурсам выполните следующие действия:

- 1 Откройте веб-браузер Internet Explorer и в адресной строке введите

`https://<Адрес ViPNet TLS Gateway для подключения пользователей по TLS-каналу с двусторонней аутентификацией:порт>`.



Внимание! Если для защищенных подключений пользователей по TLS-каналу с двусторонней аутентификацией используется порт 443, заданный по умолчанию, в адресной строке порт можно не указывать:

`https://<Адрес ViPNet TLS Gateway для подключения пользователей по TLS-каналу с двусторонней аутентификацией>`

- 2 В появившемся окне со списком сертификатов выберите свой сертификат, который вы установили в системное хранилище (см. [Порядок организации защищенного подключения нового пользователя к ресурсам по протоколу TLS с двусторонней аутентификацией](#) на стр. 14).

После успешной аутентификации будет установлено защищенное соединение по протоколу TLS и откроется главная страница веб-интерфейса ViPNet TLS Gateway.



Примечание. Внешний вид страницы веб-интерфейса ViPNet TLS Gateway зависит от настроек, заданных администратором на ViPNet TLS Gateway, и может отличаться от вида, представленного на рисунках ниже.

- 3 В разделе **Доступные ресурсы** щелкните ссылку **Создать или изменить запрос**.
- 4 В окне **Запрос доступа к ресурсам** выполните следующие действия:
 - 4.1 В списке **Ресурсы, к которым требуется доступ** установите флажки напротив тех ресурсов, к которым вам нужен доступ.
 - 4.2 При необходимости введите текст, поясняющий ваш запрос.
 - 4.3 Укажите электронный адрес для связи с вами.
 - 4.4 Нажмите кнопку **Отправить запрос**.

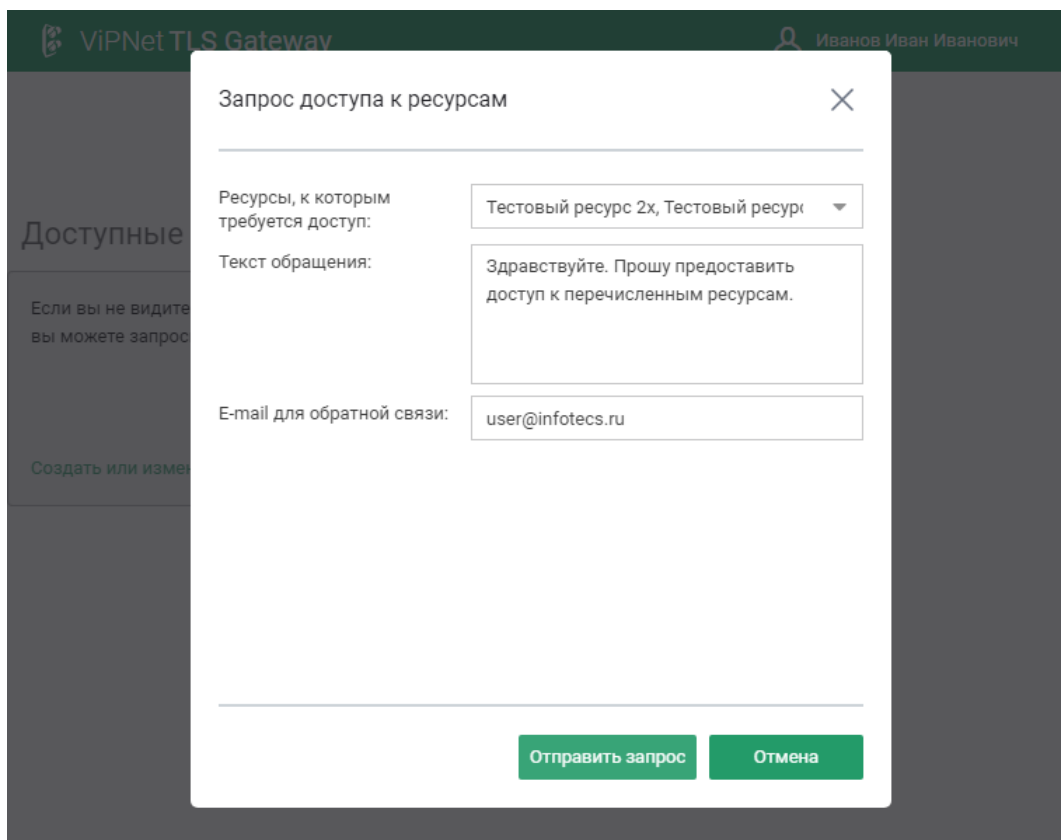


Рисунок 1. Создание запроса на доступ к ресурсам

В результате запрос будет отправлен на ViPNet TLS Gateway. Информация о запрашиваемых ресурсах появится на главной странице веб-интерфейса ViPNet TLS Gateway в разделе **Запросы на предоставление доступ**. Для каждого запрашиваемого ресурса вы увидите статус его обработки администратором. Пока запрос на предоставление доступа к ресурсу не будет обработан администратором, для ресурса будет отображаться статус **Ваш запрос рассматривается**. При необходимости вы можете изменить параметры запроса (например, добавить еще какие-нибудь ресурсы), щелкнув ссылку статуса и изменив данные в окне **Запрос доступа к ресурсам** (как указано выше).

После обработки администратором на ViPNet TLS Gateway запроса на каждый запрашиваемый ресурс возможны следующие результаты:

- Если доступ к ресурсу был разрешен администратором, плитка со ссылкой на ресурс появится в разделе **Доступные ресурсы**. Щелкнув эту ссылку, вы сможете открыть страницу ресурса (см. [Подключение к доступным ресурсам](#) на стр. 18).
- Если доступ к ресурсу был запрещен администратором, плитка со ссылкой на ресурс не появится в разделе **Доступные ресурсы**. Этот ресурс будет вам недоступен. Повторная отправка запроса на получение к нему доступа будет также недоступна.
- Если вместо страницы со списком доступных ресурсов появится страница с информацией о запрете доступа к ViPNet TLS Gateway, значит администратор полностью запретил вам доступ к ViPNet TLS Gateway и всем ресурсам. Для выяснения причины полной блокировки доступа вы можете связаться с администратором по адресу электронной почты, указанному на странице блокировки.

Информация об обработанных администратором ресурсах исчезнет из раздела **Запросы на предоставление доступа**.

3

Подключение пользователей к ресурсам по протоколу TLS с односторонней аутентификацией

Порядок организации защищенного подключения нового пользователя к ресурсам по протоколу TLS с односторонней аутентификацией	24
Подключение к доступным ресурсам	26

Порядок организации защищенного подключения нового пользователя к ресурсам по протоколу TLS с односторонней аутентификацией

Для организации защищенного подключения к ViPNet TLS Gateway вам потребуются:

- Сертификат УЦ, в котором изданы транспортные сертификаты ViPNet TLS Gateway, а если сертификат УЦ не является корневым, то все сертификаты УЦ из [цепочки доверия к сертификатам этого УЦ](#) (см. глоссарий, стр. 31).
- Адрес ViPNet TLS Gateway для подключения пользователей по TLS-каналу с односторонней аутентификацией. Адрес подключения к ViPNet TLS Gateway вы можете получить у администратора ViPNet TLS Gateway.

Чтобы организовать защищенное подключение по протоколу TLS с односторонней аутентификацией и получить доступ к необходимым ресурсам, выполните все действия из приведенного ниже списка:

Таблица 5. Порядок организации защищенного подключения нового пользователя к ViPNet TLS Gateway для доступа к ресурсам

Действие	Ссылка
<input type="checkbox"/> Получите сертификаты УЦ из цепочки доверия к сертификатам УЦ, в котором изданы транспортные сертификаты ViPNet TLS Gateway, у администратора ViPNet TLS Gateway, и установите их в системное хранилище с помощью стандартных средств операционной системы	См. документацию к соответствующим средствам
<input type="checkbox"/> Настройте параметры веб-браузера для защищенного подключения по протоколу TLS	Настройка параметров веб-браузера для подключения по протоколу TLS (на стр. 17)
<input type="checkbox"/> Подключитесь к веб-интерфейсу ViPNet TLS Gateway и откройте доступные ресурсы (если они есть)	Подключение к доступным ресурсам (на стр. 26)



Совет. Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

Подключение к доступным ресурсам

Если у вас уже организовано защищенное подключение по протоколу TLS с односторонней аутентификацией (см. [Порядок организации защищенного подключения нового пользователя к ресурсам по протоколу TLS с односторонней аутентификацией](#) на стр. 24) к ViPNet TLS Gateway и администратор на ViPNet TLS Gateway настроил ресурсы, доступ к которым можно получить при односторонней аутентификации, вы можете подключаться к этим ресурсам одним из следующих способов:

- Подключиться к веб-интерфейсу ViPNet TLS Gateway, а затем выбрать необходимые ресурсы.
- Сразу подключиться к нужному вам ресурсу (если вам известен адрес подключения к ресурсу). Адрес подключения к ресурсу вы можете получить у администратора ViPNet TLS Gateway.
- Подключиться к нужному ресурсу непосредственно по его адресу, если настроена такая возможность (подробнее см. документ «ViPNet TLS Gateway. Руководство администратора», раздел «Настройка подключения к защищаемым ресурсам непосредственно по их адресам»). Адрес ресурса вы можете получить у администратора ViPNet TLS Gateway.

Для подключения первым способом выполните следующие действия:

- 1 Откройте веб-браузер Internet Explorer и в адресной строке введите адрес в формате:

```
https://<Адрес ViPNet TLS Gateway для подключения пользователей по TLS-каналу с односторонней аутентификацией:порт>.
```



Внимание! Если для защищенных подключений пользователей по TLS-каналу с односторонней аутентификацией используется порт 443, заданный по умолчанию, в адресной строке порт можно не указывать:

```
https://<Адрес ViPNet TLS Gateway для подключения пользователей по TLS-каналу с односторонней аутентификацией>
```

После успешной аутентификации будет установлено защищенное соединение по протоколу TLS и откроется главная страница ViPNet TLS Gateway со списком доступных веб-ресурсов.



Примечание. Если доступные ресурсы не настроены, вы увидите пустую страницу **Доступные ресурсы**. Для запроса доступных ресурсов вам нужно организовать защищенное соединение по протоколу TLS с двухсторонней аутентификацией (см. [Порядок организации защищенного подключения нового пользователя к ресурсам по протоколу TLS с двухсторонней аутентификацией](#) на стр. 14).

- 2 Щелкните плитку нужного вам ресурса.

В результате откроется главная страница выбранного вами ресурса.

Для подключения сразу к нужному ресурсу откройте веб-браузер Internet Explorer и в адресной строке введите имеющийся у вас адрес подключения к ресурсу, например, адрес подключения к ресурсу может выглядеть следующим образом: <https://192.168.81.83:4431/wiki>.

После успешной аутентификации будет установлено защищенное соединение по протоколу TLS и откроется главная страница выбранного вами ресурса.

А

Глоссарий

IP-адрес

Адрес узла в сети, построенной на основе протокола IP.

TLS

Криптографический протокол, обеспечивающий защищенную передачу данных между узлами в Интернете. Использует асимметричную криптографию для обмена ключами, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.

ViPNet CSP

Программа ViPNet CSP представляет собой криптопровайдер, обеспечивающий вызов криптографических функций из различных приложений. Может использоваться как средство электронной подписи — для формирования ключей электронной подписи.

ViPNet Удостоверяющий и ключевой центр (УКЦ)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Администратор УКЦ формирует и обновляет ключи для сетевых узлов ViPNet, а также управляет сертификатами и списками аннулированных сертификатов.

Администратор УКЦ

Лицо, обладающее правом доступа к программе ViPNet Удостоверяющий и ключевой центр (УКЦ), отвечающее за создание ключей для сетевых узлов ViPNet, создание и обслуживание сертификатов ViPNet, обеспечение взаимодействия с доверенными сетями ViPNet.

Асимметричное шифрование

Система шифрования, при которой алгоритмы используют два математически связанных ключа. Открытый ключ используется для зашифрования и передается по незащищенному каналу. Закрытый ключ служит для расшифрования.

Аутентификация

Процесс идентификации пользователя, как правило, на основании его учетной записи. Аутентификация служит для подтверждения того, что входящий в систему пользователь является тем, за кого себя выдает, но процесс аутентификации не затрагивает права доступа пользователя (в отличие от авторизации).

Внешняя сеть

Сеть, отделенная от внутренней сети межсетевым экраном.

Доверенная зона

Доверенная зона содержит сетевые узлы, которые считаются безопасными друг для друга. Понятие доверенной зоны определяется политикой безопасности организации, эксплуатирующей ViPNet TLS Gateway. Например, доверенной зоной может считаться периметр помещения, в котором установлен ViPNet TLS Gateway.

Запрос на сертификат

Защищенное электронной подписью сообщение, содержащее имя пользователя, ключ проверки электронной подписи и его параметры, желаемый срок действия сертификата, предполагаемые назначения сертификата и другие параметры (полный набор параметров зависит от формата запроса и программного обеспечения, в котором он был сформирован).

Ключ проверки электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом проверки электронной подписи называется открытый ключ, который является не секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, однозначно связанную с закрытым ключом и предназначенную для проверки подлинности электронной подписи.

Ключ электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом электронной подписи называется закрытый ключ, который является секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, предназначенную для создания электронной подписи.

Контейнер ключей

Файл или устройство, в котором хранятся ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи.

Корневой сертификат

Сертификат администратора удостоверяющего центра, являющийся последним сертификатом в цепочке доверия. Другими словами, для корневого сертификата нет сертификата, с помощью которого можно было бы проверить его достоверность. С помощью корневого сертификата проверяется достоверность сертификатов (пользователей и издателей), заверенных этим сертификатом.

Расширения сертификата ключа проверки электронной подписи

Дополнительные атрибуты сертификата, такие как использование ключа, политики сертификата, базовые ограничения, ограничения имени и другие. Расширение может быть критичным или некритичным. Система, использующая сертификаты, должна отвергать сертификат, если она встретила критичное расширение, которое не в состоянии распознать; однако некритичные расширения могут игнорироваться, если они не распознаются. Каждое расширение сертификата должно иметь соответствующий идентификатор объекта (OID).

Сертификат ключа проверки электронной подписи

Электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сетевой интерфейс

Физическое или виртуальное устройство для подключения компьютера к сети. С помощью сетевого интерфейса компьютер осуществляет прием и передачу IP-пакетов. В качестве физического интерфейса может служить сетевая плата, модем и другие подобные устройства, в качестве виртуального — агрегированный интерфейс, интерфейс для VLAN.

Список аннулированных сертификатов (CRL)

Список сертификатов, которые до истечения срока их действия были аннулированы или приостановлены администратором Удостоверяющего центра и потому недействительны на момент, указанный в данном списке аннулированных сертификатов.

Транспортный сертификат ViPNet TLS Gateway

Сертификат серверной аутентификации при взаимодействии по протоколу TLS между ViPNet TLS Gateway и пользователями (или администраторами). Представляет собой сертификат ключа проверки электронной подписи, в котором указан IP-адрес (или DNS-имя) сетевого интерфейса ViPNet TLS Gateway для подключения пользователей (или администраторов) и который имеет расширение «Расширенное использование ключа» с назначением ключа «Проверка подлинности

сервера (1.3.6.1.5.5.7.3.1)». Для ViPNet TLS Gateway издаются следующие транспортные сертификаты: сертификат для подключения администраторов, сертификат для подключения пользователей по TLS-каналу с односторонней аутентификацией, сертификат для подключения пользователей по TLS-каналу с двусторонней аутентификацией.

Удостоверяющий центр

Организация, осуществляющая выпуск сертификатов ключей проверки электронной подписи, а также сертификатов другого назначения.

Цепочка доверия к сертификатам

Упорядоченная последовательность сертификатов, соответствующая иерархии издателей этих сертификатов. При криптографических операциях каждый сертификат из цепочки проверяется на следующем сертификате. Сертификат считается действительным, если цепочка доверия полна (то есть завершается корневым сертификатом) и все входящие в нее сертификаты также действительны.

Электронная подпись

Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Электронная рулетка

Встроенный компонент программного обеспечения ViPNet, который позволяет инициализировать датчик случайных чисел на основе действий пользователя. Полученная последовательность используется при формировании ключей узла.