s•terra

ЗАЩИЩЕННЫЙ ДОСТУП К УДАЛЕННЫМ РАБОЧИМ СТОЛАМ

Задача

Организация доступа сотрудников к удаленным рабочим столам весьма актуальна как для государственных, так и для коммерческих организаций, причем потребность в защите такого доступа растет год от года. Поэтому комплексная система безопасности является обязательным компонентом решения. Она должна охватывать как серверный, так и клиентский сегмент, включая и периферийное оборудование (принтеры, сканеры и т.п.). При удаленной работе сотрудника вне офиса его оборудование оказывается вне контролируемой зоны, а значит, требуется обеспечить защиту каналов связи. Перед тем, как предоставить доступ работников к удаленным, в т. ч. виртуальным, рабочим столам, важно убедиться, что устройство не содержит вредоносных программ, а файлы клиентского ПО не модифицированы злоумышленником. Так как сотрудники могут находиться в любой точке мира, службе безопасности компании нужно быть уверенной, что подключающийся пользователь – действительно тот, за кого себя выдает.

Важно учесть, что если в информационной системе компании обрабатывается информация, подлежащая обязательной защите в соответствии с российским законодательством (например, персональные данные), то необходимо использовать сертифицированные средства защиты, прошедшие процедуру оценки регуляторами – ФСБ России и ФСТЭК России.

Всё более распространенной становится технология предоставления доступа к удаленным рабочим столам - Virtual Desktop Infrastructure (VDI), которая позволяет организовать готовое к работе стандартизированное виртуальное рабочее место, настраиваемое под конкретные задачи. С помощью технологии VDI пользователи получают доступ к информационным ресурсам своей компании и необходимому программному обеспечению. Данная технология предоставляет следующие преимущества:

- Универсальность использования
- Централизованное управление и контроль
- Снижение эксплуатационных расходов
- Единый интерфейс рабочего стола для комфортной работы
- Непрерывность бизнес-процессов

Безусловно, доступ к удаленным рабочим столам необходимо защищать. Системы VDI уже содержат в своем составе некоторые компоненты защиты, но они неспособны нейтрализовать многие современные угрозы, такие как, например, несанкционированный доступ нарушителя к внутренним ресурсам компании. Кроме того, они не могут выполнить требования законодательства.

Эти задачи можно решить одним из следующих способов:

- **Использовать SSL VPN с дополнительной аутентификацией**. При этом каждому сотруднику компании необходимо предоставить индивидуальный защищенный носитель (USB-токен) с размещенным на нем цифровым сертификатом. Для доступа к информационным ресурсам компании пользователь должен подтвердить свою подлинность с помощью этого токена и пароля. Защита данных при их передаче обеспечивается с помощью протокола SSL VPN, который может быть встроен в приложение VDI. Соблюдение пользователем политик безопасности компании, а также отсутствие в

операционной системе сотрудника вредоносных программ и прочее обеспечивается дополнительными средствами. Кроме того, на рынке отсутствуют не только системы VDI с встроенным криптографическим модулем SSL, сертифицированным регуляторами, но и отдельные сертифицированные SSL-клиенты. Таким образом, первая задача решается частично, а вторая вовсе остается нерешенной.

- **Использовать IPsec VPN с дополнительной аутентификацией.** С точки зрения логики работы данный способ практически аналогичен предыдущему. Отличие заключается в VPN протоколах – используется IPsec вместо SSL. IPsec клиент устанавливается отдельным приложением и работает на уровне операционной системы. Это позволяет защищать любой трафик между рабочим местом пользователя и корпоративной сетью, в том числе присутствует возможность использования доменных политик безопасности. Защита операционной системы от вредоносного ПО и модификации может осуществляться дополнительными средствами. Предложений IPsec клиентов на рынке VPN более чем достаточно. Недостатками данного решения является отсутствие контроля операционной системы пользователя, так как за пределами контролируемой зоны сотрудники компании могут вносить изменения в среду функционирования: добавлять и удалять файлы, использовать не регламентируемые средства обмена информации и т.д.

- **Использовать IPsec VPN на специализированном терминале.** В данном сценарии сотрудники работают на терминальных станциях с оптимизированной операционной системой, находящейся на защищенном съемном носителе. Аутентификация пользователя на рабочей станции происходит до загрузки операционной системы, а после загрузки - в самом VDI приложении. Защита данных при их передаче обеспечивается встроенным в ОС IPsec VPN клиентом. Защита от вредоносного ПО реализуется с помощью замкнутой программной среды и проверки целостности при запуске.

На протяжении ряда лет продукты С-Терра успешно используются во втором сценарии. Более того, в связи с возросшими потребностями пользователей в эффективном и комплексном решении, компания "С-Терра СиЭсПи" сформировала предложение на основе третьего варианта.

Решение Защищенный доступ к VDI

Предлагаемое решение совместимо с любыми системами VDI и соответствует требованиям российского законодательства в области информационной безопасности. Оно позволяет сотрудникам получить защищенный доступ к инфраструктуре виртуальных рабочих столов и приложений из любой точки мира.

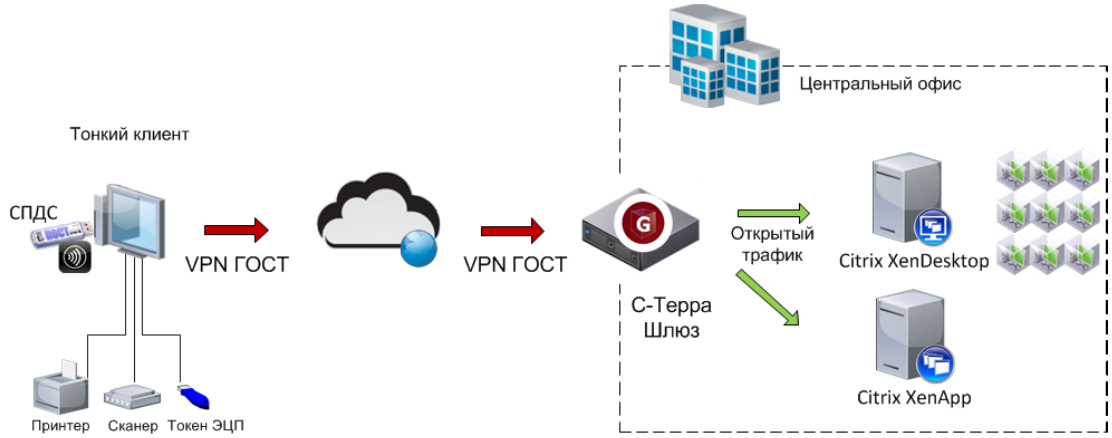

Рисунок 1. Пример защиты удаленного доступа к инфраструктуре Citrix VDI на базе продуктов С-Терра

Защита серверной части VDI построена с использованием VPN-продукта С-Терра Шлюз, сертифицированного ФСБ России и ФСТЭК России. Благодаря использованию международных стандартов IKE/IPsec и применению отечественных криптоалгоритмов обеспечивается криптографическая защита передаваемого трафика по ГОСТ 28147-89, а также взаимная аутентификация по ГОСТ Р 34.10. Для защиты серверной части можно использовать как шлюз безопасности в виде виртуальной машины для популярных гипервизоров (VMware ESX, Citrix XenServer, Parallels, KVM) – С-Терра Виртуальный Шлюз, так и традиционный С-Терра Шлюз на аппаратной платформе.

На клиентской стороне для доступа к инфраструктуре виртуальных рабочих столов используется защищенный терминал, состоящий из тонкого клиента и специального загрузочного носителя (СЗН) «Пост». При этом обеспечивается:

- Доверенная загрузка эталонной среды. При каждом запуске защищенного терминала с СЗН загружается эталонная программная среда.

- Замкнутая программная среда. Ни пользователь, ни злоумышленник не имеет возможности добавить какие-либо компоненты в программную среду терминала.

- Строгая двухфакторная аутентификация для построения защищенного соединения и доступа к виртуальным рабочим столам. В решении возможно использование различных токенов, например, компании «Aladdin» (eToken, eToken PRO, NG-FLASH) и «Актив» (Рутокен S, Рутокен ЭЦП).

- Изолированное сетевое соединение с инфраструктурой VDI. Целевой трафик передается по защищенному VPN-туннелю, при этом обеспечивается конфиденциальность и целостность передаваемой информации. Остальной трафик либо запрещен, либо передается через корпоративный proxy-сервер, в зависимости от политики безопасности компании заказчика.

- Подпись документов локальной электронной подписью (ЭП). Использование ЭП в инфраструктуре виртуальных рабочих столов достигается за счет прозрачного пробрасывания токена в терминальную сессию.
- Поддержка периферийных устройств, таких как принтеры и сканеры.
- Адаптация решения под требования заказчика.
- Большой выбор функционального программного обеспечения для работы удаленного пользователя с различными сервисами компании.

Использование замкнутой программной среды и СЗН минимизирует воздействие агрессивной информационной среды на работу с важной информацией, а также снижает риски, связанные с возможными деструктивными действиями пользователей. Кроме того, заказчик может отказаться от применения антивирусного программного обеспечения на рабочих местах пользователей. Это позволяет не только сэкономить средства, но и существенно облегчить процесс эксплуатации терминалов, поскольку нет необходимости контролировать их конфигурацию и обновлять антивирусные базы данных.

Таблица 1. Особенности решения С-Терра по защите VDI

Возможности решения	**Подробное описание**
Поддержка любых VDI-систем	Поддерживаются Citrix, VMware, Parallels, KVM и другие
Интеграция с инфраструктурой	Возможно встраивание Виртуального Шлюза в существующую инфраструктуру или использование аппаратного шлюза (производителя АП выбирает заказчик)
Поддержка периферии	Поддержка мультимедиа. Поддержка USB и периферийных устройств. Поддержка токенов и смарт-карт современных производителей.
Масштабирование	Удобное наращивание мощностей (в том числе лицензионное, без обновления аппаратной части)
Надежность и отказоустойчивость	Использование надежной аппаратной части. Возможность кластеризации любых компонентов.
Адаптация под требования заказчика	Брендирование различных компонентов ОС (логотипы заказчика на заставке при загрузке и т.д.) Использование оборудования заказчика в качестве терминалов (добавление драйверов и т.д.)

Возможности решения	Подробное описание
Механизмы защиты	Проверка целостности при запуске. Усиленная аутентификация. Замкнутая программная среда. Интегрированный МЭ. Шифрование трафика. Минимальные возможности пользователя.
Криптографические алгоритмы	Шифрование: ГОСТ28147-89 (в том числе комбинированное преобразование ESP_GOST-4M-IMIT). Электронная подпись: ГОСТ Р 34.10-2001/2012 Контроль целостности: ГОСТ Р 34.11-94/2012.
Сертификация ФСБ	СКЗИ КС2 и МЭ 4
Сертификация ФСТЭК	НДВ 3, МЭ 3, ОУД 4+, АС 1В, ГИС до 1 кл. включительно, ПДн до 1-4 ур.

Выбор продуктов

Выбор продуктов для использования в решении зависит от необходимого класса защиты. Рекомендации приведены в таблице 2.

Таблица 2. Рекомендации по выбору продуктов С-Терра для защиты VDI

Класс сертификации	КС1	КС2
Серверная часть	С-Терра Виртуальный Шлюз *или* С-Терра Шлюз	С-Терра Шлюз
Клиентская часть	С-Терра «Пост»	С-Терра «Пост»

Для более точного выбора конкретных продуктов необходимо учитывать не только необходимый класс защиты, но объем и тип передаваемого трафика, требования к резервированию, отказоустойчивости и т.д. Рекомендации по выбору представлены в таблицах 3 и 4.

Таблица 3. Расчет примерного состава решения по защите доступа к VDI. СКЗИ класса КС1.

КС1	До 10 устройств	До 100 устройств	До 500 устройств
Управление	1xC-Терра КП (лицензия на 10 устройств)	1xC-Терра КП (лицензия на 100 устройств)	1x C-Терра КП (лицензия на 500 устройств)
Серверная часть	1xC-Терра Виртуальный Шлюз (лицензия на 1 ядро) *или* 1xC-Терра Шлюз 100	1xC-Терра Виртуальный Шлюз (лицензия на 4 ядра) *или* 1xC-Терра Шлюз 3000LE	2xC-Терра Виртуальный Шлюз (лицензия на 4 ядра) *или* 2xC-Терра Шлюз 3000 *или* 1xC-Терра Шлюз 7000
Клиентская часть	10xКДС	100xКДС	500xКДС

Таблица 4. Расчет примерного состава решения по защите доступа к VDI. СКЗИ класса КС2

КС2	До 10 устройств	До 100 устройств	До 500 устройств
Управление	1xC-Терра КП (лицензия на 10 устройств)	1xC-Терра КП (лицензия на 100 устройств)	1x C-Терра КП (лицензия на 500 устройств)
Серверная часть	1xC-Терра Шлюз 100	1xC-Терра Шлюз 3000LE	2xC-Терра Шлюз 3000 *или* 1xC-Терра Шлюз 7000
Клиентская часть	10xКДС	100xКДС	500xКДС

Приведенные в таблицах данные носят ориентировочный характер, поскольку трафик целевых приложений может отличаться в различных прикладных задачах. Кроме того, при оценке производительности шлюза безопасности следует учитывать статистику сеансов доступа. Данные в таблицах приведены для одновременной работы пользователей. Если сеансы пользователей статистически распределены во времени, мощность шлюза серверной части может быть снижена.

Подробную информацию о компонентах данного решения вы можете получить на www.s-terra.com и сайтах производителей компонентов VDI.

Получить помощь в выборе продуктов и оборудования, а также расчет стоимости решения для вашей организации Вы можете, обратившись к нашим менеджерам:

- по телефону +7 (499) 940-90-61
- или по электронной почте: sales@s-terra.com.

Вам обязательно помогут!

О компании «С-Терра СиЭсПи»

ООО «С-Терра СиЭсПи» основано в 2003 году и является ведущим российским разработчиком и производителем средств сетевой информационной безопасности на основе технологии IPsec VPN.

Компания «С-Терра СиЭсПи» предлагает органично входящие в сетевую инфраструктуру решения, которые используют российские сертифицированные криптографические алгоритмы ГОСТ. Решения характеризуются отличной масштабируемостью, надежностью и рекордной производительностью, что обеспечивает высокую экономическую эффективность.

Продукты и решения С-Терра обеспечивают защиту каналов связи любой производительности (как на сетевом, так и на канальном уровне), безопасный удаленный доступ, в том числе с мобильных платформ, а также предоставляет эффективное управление VPN-инфраструктурой С-Терра.

Продукты С-Терра сертифицированы ФСТЭК России и ФСБ России, в том числе как средства криптографической защиты информации (СКЗИ) по классу КС1, КС2, КС3, а также как межсетевой экран по классу МЭ4 (ФСБ России) и МЭ3 (ФСТЭК России).

Компания является первым российским технологическим партнером Cisco (Cisco Solution Technology Integrator), Серебряным партнером Samsung и Авторизованным партнером Huawei.

Партнерская сеть компании "С-Терра СиЭсПи" состоит из более чем 300 компаний, включая всех крупнейших российских системных интеграторов. Имеется представительство компании в Республике Беларусь.