Безопасный удаленный доступ. Мобильность и дорога в облака

Андрей Шпаков, *ведущий инженер ЗАО "С-Терра СиЭсПи"*

Сотрудники современных быстро развивающихся компаний уже не могут представить себе работу без возможности удаленного доступа к внутренним ресурсам. Корпоративный чат, почта, файловые хранилища, системы учета проектов, базы знаний, видеоконференцсвязь с офисом — без этого уже сложно обойтись в командировке, при визите к клиенту или партнеру, зачастую даже дома или во время отпуска. Оперативный доступ к корпоративной информации является одним из важнейших факторов успешной бизнес-модели.

Перспективным направлением является не просто удаленный доступ к центральному офису, а размещение ресурсов сотрудников в облаках. Важным аспектом такого решения является совместное использование конкретных приложений и средств защиты, таких как концепция защищенных рабочих столов. Для полноценного взаимодействия со своим рабочим местом пользователи могут использовать любые устройства с ОС Windows, средства построения доверенного сеанса или мобильные платформы.

Существует множество технологий для организации сеанса удаленного доступа. Они различаются по модели подключения (клиент – сервер, клиент – промежуточный сервер – клиент), используемому протоколу (открытые/закрытые реализации), модели распространения (платные/бесплатные) и другим параметрам. При этом все продукты, реализующие данную функциональность, обычно содержат лишь примитивные средства защиты сеанса (или не содержат их вовсе). В лучшем случае поддерживается шифрование трафика с помощью западных криптоалгоритмов, что в некоторой степени обеспечивает конфиденциальность, но не соответствует современному законодательству. Ситуация усугубляется повсеместным использованием мобильных устройств, средств защиты для которых немного (а сертифицированных – буквально единицы). Как следствие – невозможность аттестации системы.

Кроме того, нельзя забывать о таких важных аспектах безопасности, как изоляция пользовательского окружения от вредоносного ПО, фишинга и т.д.

Существуют особые случаи, когда сотрудник вынужден осуществлять доступ с устройства, рабочей среде которого нельзя доверять. В этом случае одним из решений проблемы является использование специальных загрузочных носителей для реализации защищенного доверенного сеанса.

Бизнес выбирает VPN

Традиционно средний и крупный бизнес для защиты канала связи между центральным офисом и рабочим местом сотрудника использует VPN-клиент на стороне пользователя и VPN-концентратор в офисе компании. При этом к VPN-клиенту предъявляется ряд требований: совместимость с различными ОС (Windows 7/8/8.1 и т.д.) и другими компонентами инфраструктуры, централизованное управление, встроенный межсетевой экран, сертификация регуляторами. В связи с регулярно появляющейся информацией об уязвимостях в проприетарных и даже в стандартных протоколах (например, Heartbleed в SSL) следует отметить важность выбора продуктов с действительно надежным протоколом. В качестве примера можно предложить набор протоколов IPSec. Одним из его преимуществ является защита всего трафика пользователя, включая служебный (ICMP, Keepalive, SIP), что бывает критично для сложных сценариев применения. Хорошим примером реализации перечисленных выше требований является "С-Терра Клиент" от компании "С-Терра СиЭсПи".

При использовании VPN-клиента крайне важно обеспечить его взаимосвязь с другими компонентами системы защиты. Использование дополнительных инструментов аутентификации значительно повышает уровень защищенности системы. Например, таким является сценарий хранения на USB-токене не только ключевой информации, но и локальной политики безопасности (так называемый клиент на токене). Другой вариант – использование для аутентификации Radius-сервера, интегрированного с Active Directory и другими средствами управления. Оба эти функциональных преимущества реализованы в продукте "С-Терра Клиент".

Для полноценного включения мобильного устройства в защищаемый периметр и контроля деятельности целесообразно весь трафик с устройства направить VPN-клиентом в защищаемый периметр, безопасность которого обеспечивают корпоративный proxy-сервер, межсетевой экран, антивирусный сервер, система обнаружения/предотвращения вторжений, VPN-шлюз и другие инструменты безопасности.

Для обеспечения защищенного доступа с портативных мобильных устройств (планшетов, смартфонов и пр.) применяются комплексные решения, такие как MDM (Mobile Device Management) в сочетании с мобильным VPN-клиентом. Частая смена технологий и операционных систем вынуждает выбирать продукты и решения, защищающие наиболее широкий круг различ-

ных устройств. Таковым является "С-Терра Клиент-М", функционирующий под ОС Android 4.x и не привязанный к конкретной платформе. Продукт позволяет защитить канал передачи данных от мобильного телефона или планшета, имеет удобный и понятный графический интерфейс, а также не требует взлома устройства (получение прав root) для своей работы.

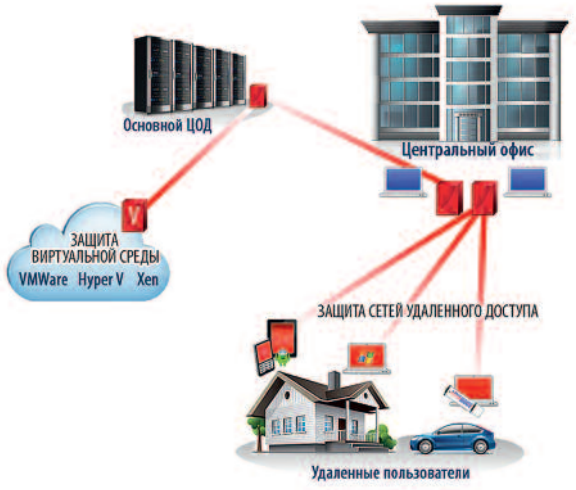
Среда построения доверенного сеанса

Существуют особые случаи, когда сотрудник вынужден осуществлять доступ с устройства, рабочей среде которого нельзя доверять. В этом случае одним из решений проблемы является использование специальных загрузочных носителей для реализации защищенного доверенного сеанса. Такой подход позволяет добиться более высокого уровня защищенности за счет значительного сокращения возможностей пользователя. Важными преимуществами являются невозможность экспортировать (импортировать) файлы в доверенную среду и из нее, а также строгая двухфакторная аутентификация с проверкой PIN-кода, реализуемая на одном загрузочном носителе. Примером продукта из этого сегмента является СПДС "ПОСТ" компании "С-Терра СиЭсПи". Это специальный загрузочный носитель, выполненный в форм-факторе USB. По результатам аутентификации определяется роль пользователя и предоставляются соответствующие права, выполняются проверка целостности операционной системы и ее загрузка. Пользователь может подключиться по одному из трех принципиально разных видов удаленного доступа – протокол RDP, браузер с поддержкой плагина VNC, либо удаленный рабочий стол Citrix XenDesktop. При этом не происходит обращения к жесткому диску компьютера, а список используемой периферии строго регламентирован.

Разнообразие аппаратной базы современной портативной техники и вариации окружения пользователей создают проблемы для решений, базирующихся на изолированной среде и доверенном сеансе. И здесь на помощь может прийти создание эталонного рабочего места. Например, комплекты доверенного сеанса, которые состоят из "тонкого" клиента, обеспечивающего загрузку только с определенного носителя с помощью электронного замка в BIOS и самого носителя (СПДС "ПОСТ"). В таком случае заведомо обеспечена совместимость специального загрузочного носителя с аппаратными составляющими терминала. Решение получается типовым и полностью законченным.

Альтернативным подходом является применение технологии виртуализации. В этом случае специальный загрузочный носитель используется как средство хранения эталонной виртуальной машины. Пользователь загружает ее из защищенной области, целостность гарантируется аппаратными средствами специального загрузочного носителя. Виртуальная машина содержит только необходимый набор программного обеспечения, в том числе VPN-клиент для установления защищенного соединения. Проблема отсутствия совместимости с аппаратным обеспечением полностью отсутствует благодаря фиксированному набору виртуального "железа". На носителе может быть размещено несколько форматов виртуальной машины для различных гипервизоров, в результате становится возможным использование под большинством популярных операционных системы (Windows, Linux и MacOS).

Перспективным направлением является не просто удаленный доступ к центральному офису, а размещение ресурсов сотрудников в облаках. Важным аспектом такого решения является совместное использование конкретных приложений и средств защиты, таких как концепция защищенных рабочих столов. Для полноценного взаимодействия со своим рабочим местом пользователи могут использовать любые устройства с ОС Windows, средства построения доверенного сеанса или мобильные платформы. VPN-клиент устанавливает защищенное соединение с виртуальным шлюзом в облаке (или физическим шлюзом в том же ЦОД), у которого обеспечена



совместимость с популярными гипервизорами. Далее пользователь попадает на свое рабочее место, физическое или виртуальное, либо к отдельным приложениям, установленным у него на офисном компьютере или корпоративном сервере. Такой подход позволяет при необходимости отказаться от стационарных рабочих мест и получать доступ к своим ресурсам где угодно и когда угодно. В частности, такой сценарий реализован с помощью продуктов "С-Терра Виртуальный шлюз" и Citrix XenDesktop.

Реализация предложенных процедур и решений с применением продуктов компании "С-Терра СиЭсПи" позволяет заказчику приобрести целостное решение, поддерживающее все типы современных конечных устройств и совместимое с другими компонентами инфраструктуры, в том числе средствами обеспечения безопасности. Сочетание общепринятых международных стандартов и сертифицированной отечественной криптографии обеспечивает полноценную защиту без потери уровня сервиса.