СТРОГАЯ АУТЕНТИФИКАЦИЯ ПРИ УДАЛЕННОЙ РАБОТЕ С КОРПОРАТИВНЫМИ РЕСУРСАМИ

Буквально через 10 лет по прогнозам Gartner, число сотрудников, работающих в удаленном режиме, существенно увеличится. Их прирост уже сейчас составляет 10—15% в год. Gartner приводит в пример опыт корпораций Sun и IBM: за три года после внедрения дистанционной работы для своих штатных сотрудников Sun Microsystems сэкономила на аренде помещений 300 млн. долл., а по подсчетам IBM, корпорация ежегодно экономит на «удалёнке» до 500 млн. долл. Возможно, российским компаниям стоит перенять опыт крупнейших игроков ИТ-рынка? Тем более, что вопрос экономии в нестабильных финансовых условиях более чем актуален, причем не только для корпораций, но и компаний сегмента SMB. Оценка применения концепции дистанционной работы сотрудников с технологической точки зрения, дает понять, что помимо оснащения рабочего места сотрудника соответствующим набором приложений, неизменно возникает вопрос обеспечения защиты удаленного доступа к корпоративным информационным ресурсам.

Решением этого вопроса на стыке технологий не первый год занимаются многие прогрессивные компании. О нескольких сценариях обеспечения безопасной удаленной работы пользователей данная статья.

Одним из самых распространенных способов обеспечения защищенного удаленного взаимодействия между территориально разнесёнными филиалами является организация виртуальных частных сетей (VPN , Virtual Private Network) на базе коммутируемых сетей общего пользования (чаще всего - Интернет). VPN-технологии не требуют построения выделенного канала связи и при грамотном использовании средств защиты, могут обеспечивать приемлемый для любой организации уровень информационной безопасности.

При соединении удалённых площадок между собой с помощью VPN-туннеля оконечные устройства (например, компьютеры или шлюзы) могут идентифицироваться, как «обезличенные» узлы сети (например, по IP-адресу) и как рабочие места конкретных пользователей (такая идентификация производится, как правило, по сертификату пользователя). Одни туннели могут обеспечивать только взаимную аутентификацию отправителя и получателя информации, а также целостность потока данных. Другие – шифровать данные, причем для различных туннелей могут применяться различные криптографические алгоритмы.

Для удаленной работы пользователей с корпоративными ресурсами повсеместно используются открытые Интернет-каналы передачи данных, что, по понятным причинам, не исключает атаки на ресурсы локальной сети в рамках этого информационного обмена. В качестве временного рабочего места пользователя может выступать его домашний компьютер, ноутбук, подключенный к публичной WiFi-сети, терминал в Интернет-кафе или даже мобильное устройство. В таких обстоятельствах на первый план выходят проблемы проверки подлинности пользователя/устройства, обращающегося к корпоративным ресурсам, а также обеспечения конфиденциальности и целостности передаваемой информации. Как правило, защита данных в этом случае осуществляется с использованием шифрования, реализованного в протоколах IPSec и SSL. Для проведения аутентификации пользователя, работающего в дистанционном режиме, могут использоваться следующие варианты: пароли, цифровые сертификаты, токены, генераторы одноразовых паролей (OTP, One-Time Password) или же их комбинация.

Для организации безопасной удаленной работы сотрудника на первом этапе устанавливается соединение с интернет-сервис провайдером, при этом используемый протокол (Ethernet, PPP и т.п.) зависит от среды передачи и конкретного способа соединения с сетью Интернет. Адрес соединения конфигурируется сервис-провайдером. Далее, подсоединившийся к Интернет удалённый клиент, устанавливает туннель с защищённым периметром корпоративной сети, при этом адресом со стороны корпоративной сети будет являться туннельный адрес VPN-шлюза. Если для защиты туннеля используется протокол IPSec, то после этого внутри туннеля клиент работает с внутренними ресурсами сети по протоколу IP и в этом соединении

адрес клиента конфигурируется шлюзом. Ему присваивается внутренний адрес и клиент становится фактически внутренним хостом корпоративной сети. Понятно, что для столь глубоко проникающего в систему пользователя крайне важно пройти процедуру аутентификации.

ВАРИАНТЫ АУТЕНТИФИКАЦИИ

При аутентификации пользователей сети удалённого доступа обычно используются следующие варианты:

- индивидуальный предустановленный ключ или пароль (pre-shared key);
- цифровой сертификат с закрытым ключом, хранящимся на компьютере;
- цифровой сертификат с закрытым ключом, хранящимся в памяти токена;
- комбинация цифрового сертификата одноразового пароля.

Выбор конкретного метода определяется в зависимости от масштаба сети, количества пользователей, сложности инфраструктуры, вариантов подключения пользователей и, конечно, требований по обеспечению информационной безопасности.

Сведём основные плюсы и минусы указанных методов в таблицу:

ТАБЛИЦА 1. ПРЕИМУЩЕСТВА И НЕДОСТАТКИ РАЗЛИЧНЫХ МЕТОДОВ АУТЕНТИФИКАЦИИ

Метод аутентификации	Преимущества	Недостатки
Pre-shared key	Простота технического решения	Сложность в использовании технически неподготовленным сотрудником, низкая масштабируемость системы, требуется доверенный канал для распространения ключей, неприемлемо низкий уровень безопасности
Цифровой сертификат с закрытым ключом, хранящимся на компьютере	Простота управления (создание, распространение, отзыв сертификатов), масштабируемость системы	Требуется наличие инфраструктуры открытых ключей (PKI, Public Key Infrastructure), дополнительные эксплуатационные расходы, низкая мобильность пользователя в силу «привязки» сертификата к конкретному компьютеру
Цифровой сертификат с закрытым ключом, хранящимся в памяти токена	Простота управления (создание, распространение, отзыв сертификатов), масштабируемость системы, простота использования, высокий уровень обеспечиваемой безопасности, возможность использования однократной аутентификации (Single Sign-On)	Требуется наличие инфраструктуры открытых ключей (PKI), дополнительные эксплуатационные расходы и затраты на токены
Цифровой сертификат и одноразовый пароль	Простота управления (создание, распространение, отзыв сертификатов), масштабируемость системы, увеличение стойкости	Требуется наличие инфраструктуры открытых ключей (PKI) , инфраструктуры аутентификации (TACAS+ или RADIUS), высокие эксплуатационные расходы, дополнительные затраты на устройства и наличие

В зависимости от структуры сети, аутентификация пользователя при доступе к ресурсам и приложениям может выполняться на шлюзе внешнего или внутреннего периметра, а также внутри него. Многократное прохождение процедуры аутентификации не слишком удобно, в связи с чем, широкое распространение получили методы сквозной аутентификации Single Sign-On (SSO). Существует два варианта реализации SSO: использование единых атрибутов аутентификации или на основе построения так называемых отношений доверия между системами.

В первом случае для аутентификации применяется один и тот же пароль или один и тот же цифровой сертификат при обращении к различным ресурсам. Недостаток такого способа заключается в том, что компрометация одного атрибута аутентификации приводит к компрометации всей системы.

При втором подходе пользователь аутентифицируется лишь единожды, например, при входе в домен. Далее, ко всем необходимым ресурсам и сервисам сети он получает доступ автоматически. Реализация SSO предполагает наличие так называемого сервера авторизации, который отвечает за предоставление пользователю прав доступа. Главным недостатком такого подхода является невозможность его применения в гетерогенной инфраструктуре, где функционируют программные продукты разных вендоров, несовместимые между собой, или же унаследованные приложения, не поддерживающие работу с имеющимся в сети сервером авторизации.

Разумным выходом в таком случае является использование токена – аппаратного USB-устройства (или смарт-карты), которое позволяет хранить несколько различных сертификатов с индивидуальными политиками безопасности (например, в части длины ключа или срока действия закрытого ключа) и совместимо с большинством современных систем и приложений мировых вендоров. Кроме того, в защищенную область памяти токена можно записать логины и пароли пользователей от унаследованных приложений, не поддерживающих работу с инфраструктурой открытых ключей (PKI).

РЕШЕНИЕ НА СТЫКЕ ТЕХНОЛОГИЙ

РИС.1. АППАРАТНЫЙ МОДУЛЬ NME-RVPN И USB-КЛЮЧ ETOKEN PRO С СЕРТИФИКАТОМ ПОЛЬЗОВАТЕЛЯ И ПОЛИТИКАМИ БЕЗОПАСНОСТИ

Один из вариантов решения проблемы защищенного корпоративного взаимодействия при удалённой работе пользователей был представлен в рамках технологического проекта компаний Aladdin, Cisco и S-Terra. Совместное решение компаний объединило различные методы аутентификации, интегрированные инновационные решения для IP-телефонии, передачи данных, голоса, видео и решения для построения VPN-соединений.

В широкой продуктовой линейке средств построения безопасных сетевых соединений компании S-Terra особого внимания заслуживает модуль NME-RVPN. Данный аппаратный модуль может использоваться в составе маршрутизаторов серии Cisco® 2800 и 3800 Integrated Services Routers. Устройство позволяет обеспечить эффективную маршрутизацию и защиту трафика данных, голоса, видео. При этом для управления им не требуется дополнительных интерфейсов - модуль NME-RVPN использует интерфейс Cisco для формирования правил маршрутизации и защиты сетевых взаимодействий. Глубокая интеграция позволяет упростить построение сети, не предъявлять дополнительных требований к квалификации персонала и, как результат, снизить затраты на поддержку, а также сократить сроки развертывания подсистемы информационной безопасности. Модуль NME-RVPN поддерживает работу с аппаратными средствами аутентификации eToken, чему указанные разработчики уделяют особое внимание.

В сценариях удалённого доступа ключи eToken могут использоваться не только для аутентификации пользователей. Так, например, в защищённой памяти ключа могут сохраняться политики безопасности самого VPN-клиента (см. Рис.1). Данные политики определяют права доступа пользователя и уровень его привилегий при подключении к корпоративной сети организации. Политики безопасности могут обновляться с помощью централизованной системы управления токенами – TMS, Token Management System.

АУТЕНТИФИКАЦИЯ ПО ПАРОЛЯМ И ЦИФРОВЫМ СЕРТИФИКАТАМ

Для подключения удалённого рабочего места пользователя к корпоративной сети организации необходимо установить на компьютер сотрудника CSP VPN Client. Данное ПО предназначено для обеспечения защищенного сетевого взаимодействия с использованием российской криптографии в рамках международного стандарта IPsec. При этом в качестве VPN-сервера выступают маршрутизаторы серии Cisco® 2800 и 3800 Integrated Services Routers с установленным модулем NME-RVPN.

Несмотря на реализованную возможность использования паролей для аутентификации пользователей, такой режим работы крайне не рекомендуется. Обеспечиваемый парольной защитой уровень безопасности во многих случаях оказывается неприемлемым даже при работе сотрудников в локальной сети организации. Использование открытых каналов связи ещё более ужесточает требования к степени защищённости как самого канала связи, так и первоначальной процедуры установления соединения, в ходе которой происходит аутентификация подключаемого пользователя.

Вариант использования цифрового сертификата, хранящегося вместе с закрытым ключом пользователя в реестре операционной системы (или просто на жёстком диске компьютера), в определённом смысле ещё более уязвим, чем обычный пароль. Домашний компьютер, используемый не только в рабочих целях, и ноутбук сотрудника, регулярно находящийся вне контролируемой зоны, подвержены высокому риску заражения вредоносным программным обеспечением. Современный типы вредоносного кода – трояны и шпионские приложения – с лёгкостью могут скопировать закрытый ключ пользователя и переслать его злоумышленнику. Конечно, на практике такой метод чаще используется для атак на программное обеспечение клиент-банков, но при высокой степени мотивации злоумышленника не исключена вероятность подобной атаки и с целью получения доступа в корпоративную сеть, например, компании-конкурента.

Не следует также забывать о высокой вероятности кражи мобильного компьютера сотрудника, характер работы которого предполагает частые командировки и разъездной режим работы. При хранении закрытого ключа на жёстком диске вместе с ноутбуком злоумышленник может получить практически свободный доступ в корпоративную сеть.

Наиболее распространённым и безопасным вариантом подключения к корпоративной сети при использовании упомянутого CSP VPN Client является предварительное размещение в защищённой памяти ключа eToken закрытого ключа пользователя и политик безопасности (опционально). При таком подходе риск компрометации минимален, т.к. для доступа к памяти eToken требуется не только обладать самим токеном, но и знать PIN-кода от него. Метод подбора PIN-кода в этом случае неэффективен в силу аппаратного ограничения количества попыток его ввода. Вторым преимуществом этого варианта аутентификации является мобильность сотрудника. Благодаря хранению ключевого материала и политик доступа на USB-ключе, пользователь получает возможность подключаться не только со своего преднастроенного администратором ПК, но и с любого компьютера организации, например, с ноутбука коллеги в совместной командировке.

АУТЕНТИФИКАЦИЯ С ИСПОЛЬЗОВАНИЕМ ОДНОРАЗОВОГО ПАРОЛЯ

Наличие в продуктовой линейке компании Aladdin специальных моделей eToken PASS и eToken NG-OTP, а также поддержка в решениях компаний Cisco и S-Terra современных протоколов защищённого соединения позволяет выполнять аутентификацию пользователя с помощью одноразовых паролей. Как и любые другие пароли, одноразовые (т.е. действительные только один раз) пароли подвергаются риску перехвата их злоумышленником, в связи с чем, до прохождения процедуры аутентификации пользователя необходимо установить защищённое соединение, например, с использованием протокола SSL (Secure Socket Layer). Важной особенностью такого способа удалённого доступа является возможность полностью мобильной работы с любого рабочего места, где бы ни оказался сотрудник. Достигается это за счёт односторонней аутентификации сервера по цифровому сертификату и установления защищённого соединения, уже в рамках которого пользователь вводит для аутентификации одноразовый пароль, сгенерированный устройством. Вариант с двусторонней аутентификацией по протоколу SSL сервера и пользователя и последующим вводом одноразового пароля на практике используется редко, т.к. в этом случае требуется установка на рабочее место пользователя сертификата и закрытого ключа, что для временных рабочих мест нецелесообразно. Одним из вариантов применения комбинации сертификата пользователя и одноразового пароля является работа сотрудника с мобильного устройства (коммуникатор, смартфон), не оснащённого USB-разъёмом. Стоит также отметить, что протокол SSL и аутентификация с применением одноразовых паролей чаще всего используется для удалённого доступа к Web-ресурсам, однако, на практике возможны и иные варианты применения.

Важно упомянуть, что имеющиеся в арсенале технологических партнёров Aladdin и S -Terra решения по централизованному управлению (например, уже упоминавшаяся система eToken TMS со специально разработанным коннектором) позволяют эффективно решать задачи массового развёртывания программного обеспечения CSP VPN Client на рабочих компьютерах мобильных пользователей с автоматическим формированием политики доступа к ресурсам сети, а так же централизованной генерации ключевой информации, выдачи и обновления сертификатов пользователей, размещённых в памяти ключей eToken.

Рассмотренные подходы по совместному использованию решений компании Aladdin, Cisco и S-Terra способны существенно усилить защищенность и управляемость системы в целом за счёт возможностей двухфакторной аутентификации, прозрачного администрирования средств безопасности в рамках системы на стороне организации и пользователя, работающего в удаленном режиме.

О СООТВЕТСТВИИ ТРЕБОВАНИЯМ РЕГУЛЯТОРОВ

В силу принятия ряда законодательных инициатив, одно из первых мест среди которых справедливо отводится Федеральному Закону «О персональных данных», хорошим тоном считается упоминание о наличии соответствующих сертификатов регулирующих органов на средства обеспечения информационной безопасности. Не нарушая традиций, упомянем об этой стороне вопроса в контексте обеспечения дистанционной работы сотрудников организаций.

При построении информационных систем, обрабатывающих персональные данные, в соответствии с законодательством необходимо использование российских криптографических алгоритмов: ГОСТ 28147-89 (шифрование), ГОСТ Р 34.11-94 (хеширование), ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 (электронная цифровая подпись). В этом контексте важной особенностью решения Aladdin, Cisco и S-Terra CSP является возможность использования российской криптографии для аутентификации пользователей и защиты передаваемых данных. Недавно полученный компанией Aladdin Сертификат соответствия №1883 ФСТЭК России от 11 августа 2009 года распространяется на всю линейку электронных ключей eToken, включая новые модели на платформе eToken Java и программное обеспечение eToken PKI Client 5.1. С получением данного сертификата eToken стал фактически единственным на российском рынке средством аутентификации и хранения ключевой информации, имеющим уровень доверия ОУД 2 и рекомендуемым для использования в информационных системах операторов персональных данных.

Компания S-Terra так же уделяет пристальное внимание вопросу соответствия своих продуктов требованиям регуляторов. В настоящее время получены сертификаты ФСТЭК как на модуль NME-RVPN, так и на программное обеспечение CSP VPN Client.

65% РОССИЙСКИХ КОМПАНИЙ ЗА УДАЛЕННУЮ РАБОТУ

В заключении хотелось привести данные онлайн-исследования, проведенного компанией Avaya. Согласно его результатам, 63% SMB-компаний в России считают, что коммуникационные технологии являются решающим фактором в развитии бизнеса и планируют продолжать инвестиции в эту сферу. При этом 78% опрошенных в России (для сравнения, 65% в Италии, 59% в Великобритании) заявили, что они бы приобрели технологии, обеспечивающие работу сотрудников из дома, если бы у них была возможность сначала их испытать и оценить преимущества. Основными аргументами «за» отечественные компании считают снижение расходов. Но при этом, более половины респондентов в России (57%) утверждают, что в их компаниях менее четверти сотрудников обладает необходимым оборудованием для работы вне офиса (т.е. в дороге, дома, во время путешествий и т.д.), а в некоторых компаниях такой возможности нет ни у одного сотрудника.

Зададимся логичным вопросом: является ли технологическая неподготовленность основным препятствием на пути внедрения концепции дистанционной работы? Далеко не всегда. Наш вывод подтверждает следующий показатель: руководство большинства компаний (66% в России, 65% в Великобритании и в 61% в Италии) настаивает на том, что сотрудники должны находиться на рабочем месте в офисе каждый день. То есть привычка хождения на работу («чтоб сотрудник был под рукой») пока не позволяет топ-менеджменту в полной мере оценить все преимущества «мобильного штата» сотрудников. Между тем, инновационные решения, позволяющие в полной мере осуществлять функциональные обязанности сотрудника, начиная от участия в видео-конференциях и заканчивая групповым редактированием документов пользователями, разделенными тысячами километров, уже сегодня доступны компаниям любого масштаба. Более того, организация удаленных рабочих мест в защищенном исполнении, построенных на базе продуктов и решений, соответствующих требованиям регуляторов рынка, - это эффективный и технологичный способ сокращения издержек. В этой связи, внедрение концепции дистанционный работы – это скорее вопрос решимости руководства, а не технологической готовности.