RSA

The Security Division of EMC

Обзор решений RSA

Подробные сведения об аутентификации пользователей при помощи RSA SecurID®

Предоставить доступ только авторизованным пользователям - это критически важная задача.

Информационная безопасность - необходимая основа развития электронного бизнеса. Такие технологии, как шифрование сессий, беспроводные сети, межсетевые экраны, виртуальные корпоративные сети и цифровые сертификаты являются частичным решением данной задачи. Несмотря на то, что каждая из указанных систем разработана для решения какой-либо конкретной проблемы обеспечения информационной безопасности, например, ограничения доступа или предотвращения перехвата конфиденциальных сведений, ни одна из них не предназначена для ответа на самый главный вопрос информационной безопасности, который лежит в основе наиболее громких преступлений - «Лицо, пытающееся получить доступ к защищенным файлам и/или ресурсам, является законным пользователем или злоумышленником?»

В настоящем официальном документе рассматривается то, каким образом программное обеспечение RSA® Authentication Manager, являющееся компонентом системы RSA SecurID® для двухфакторной аутентификации пользователей, способно помочь эффективно управлять процессом аутентификации пользователей в сети, приложениях и на Web-сайтах. Кроме того, рассматриваются ключевые вопросы, непосредственно относящиеся к затронутой выше проблеме, касающиеся безопасности, эксплуатации и рынка решений.

Аутентификация пользователя: «зеленый свет» для электронного бизнеса

Если Вы можете положиться на результаты идентификации сотрудника, пытающегося соединиться с Вашей корпоративной сетью из своего дома, во время командировки или с использованием корпоративной беспроводной сети, Вы можете повысить производительность такого сотрудника и способствовать своему бизнесу благодаря предоставлению ему доступа к требуемым данным.

Если Вы можете положиться на результаты идентификации дилеров, которые пытаются получить доступ к Вашему партнерскому Web-порталу, на данном портале Вы можете сделать доступной важную информацию, которая поможет им осуществлять продажи. При этом у Вас не будет причин беспокоиться о том, что Вы раскрываете эту информацию конкуренту или потребителю.

Если Вы можете положиться на результаты идентификации потребителей, которые пытаются получить доступ к Вашей сетевой базе данных, Вы можете повысить качество их обслуживания, предоставляя наиболее свежую информацию и одновременно снижая затраты на техническую поддержку.

Сервер аутентификации больше не является частным тактическим решением, предназначенным для одной группы или одного приложения. Правильнее будет сказать, что серверы аутентификации, например, RSA Authentication Manager, стали критически важным, стратегическим элементом инфраструктуры сети. Все больше сотрудников предприятия и стратегических партнеров входят в сеть из дома или из удаленных офисов, поэтому потребность в системе безопасности, надежной и простой в управлении, становится чрезвычайно высокой.

Клиентам понадобится доступ к Вашим ресурсам, а администраторам системы безопасности потребуется быстро обрабатывать их права доступа, не допуская потери клиентов. Поэтому жизненно важно обладать высокоскоростной, масштабируемой и эффективной системой аутентификации.

Необходимость в аутентификации пользователя становится препятствием для злоумышленников.

Многие наиболее опасные преступления, совершаемые в сети, имеют общие признаки: обход системы защиты с помощью паролей для получения доступа к информации или денежным средствам. Несмотря на то, что для защиты второстепенных систем может оказаться достаточно стандартных паролей, приложения, файлы и системы, важные для обеспечения деятельности организации, требуют более высокой степени защищенности. К счастью, для борьбы со всеми видами незаконного проникновения в корпоративную сеть, связанными со взломом паролей, может быть применено единое решение, обеспечивающее безопасность: замена стандартной системы использования паролей на систему двухфакторной аутентификации. Данное решение не только снижает риск взлома системы безопасности, но и позволяет компаниям взаимодействовать с потребителями и стратегическими партнерами, нуждающимися в защищённых электронных коммерческих ресурсах, что дает возможность избежать многолетних расходов, связанных с нарушениями защиты, и помогает повысить доходы.

Система двухфакторной аутентификации пользователей RSA SecurID®

Система аутентификации пользователей RSA SecurID® построена по принципу, имеющему название «двухфакторная аутентификация». Исходным условием для данного принципа является тот факт, что единственный запоминаемый признак, например, пароль, по существу обеспечивает низкую степень защиты аутентичности, поскольку любой, кто подслушает или похитит пароль, превратится в полностью реального пользователя. Дополнительной гарантией защиты является второе, физическое свидетельство, которое делает достоверность аутентификации значительно выше. Широко известным примером двухфакторной аутентификации являются банковские карты: условие наличия комбинации PIN-кода и действующей банковской карты обеспечивает достаточный уровень безопасности для доступа к услугам и денежным средствам банка.

В случае использования системы RSA для двухфакторной аутентификации пользователей уполномоченные пользователи получают индивидуальные токены RSA SecurID, которые генерируют токен-коды разового использования, изменяемые по определённому временному алгоритму.

Новый токен-код генерируется каждые 60 секунд. Сервер аутентификации (RSA Authentication Manager), который защищает сеть и приложения, используемые для ведения электронного бизнеса, подтверждает правильность этого динамического кода. Каждый токен RSA SecurID является уникальным, заранее вычислить значение будущего токен-кода путем регистрации и обработки предыдущих токен-кодов невозможно. Поэтому если корректный токен-код предоставляется вместе с PIN-кодом, то обеспечивается высокая степень уверенности в том, что данное лицо является законным пользователем, обладающим аутентификатором RSA SecurID.

Совместная работа: сервер, агент и пользователь

Аутентификация пользователя при доступе к проводным или беспроводным локальным сетям, удаленном доступе через модем, соединения Internet/VPN или Web-приложения производится через сервер аутентификации RSA Authentication Manager. Если пользователь пытается получить доступ к защищенной системе, специальный программный модуль, называемый RSA Authentication Agent, запускает процесс аутентификации с использованием RSA Authentication Manager вместо стандартного процесса проверки пароля.

Какова ценность / окупаемость?

Более высокие доходы

- Новые источники получения доходов
- Новые клиенты
- Новые рынки
- Конкурентные преимущества

Пониженные издержки

- Снижение стоимости
- Экономия на затратах
- Экономическая эффективность
- Экономичность

Повышение степени соответствия

- Нормативные требования
- Клиенты
- Партнеры
- Конкуренты
- Внутренние ресурсы организации

Снижение риска

- Информация высокой ценности
- Операции высокой ценности

Какая система?

Полная стоимость владения

- Приобретение
- Развертывание
- Эксплуатация

Стратегическое соответствие (пользователи)

- Удобство / легкость в использовании
- Совместимость
- Универсальность

Стратегическое соответствие (корпорация/система)

- Взаимная защищенность
- Функциональная совместимость / интеграция интерфейсов
- Надежность / масштабируемость
- Возможность переналадки в будущем

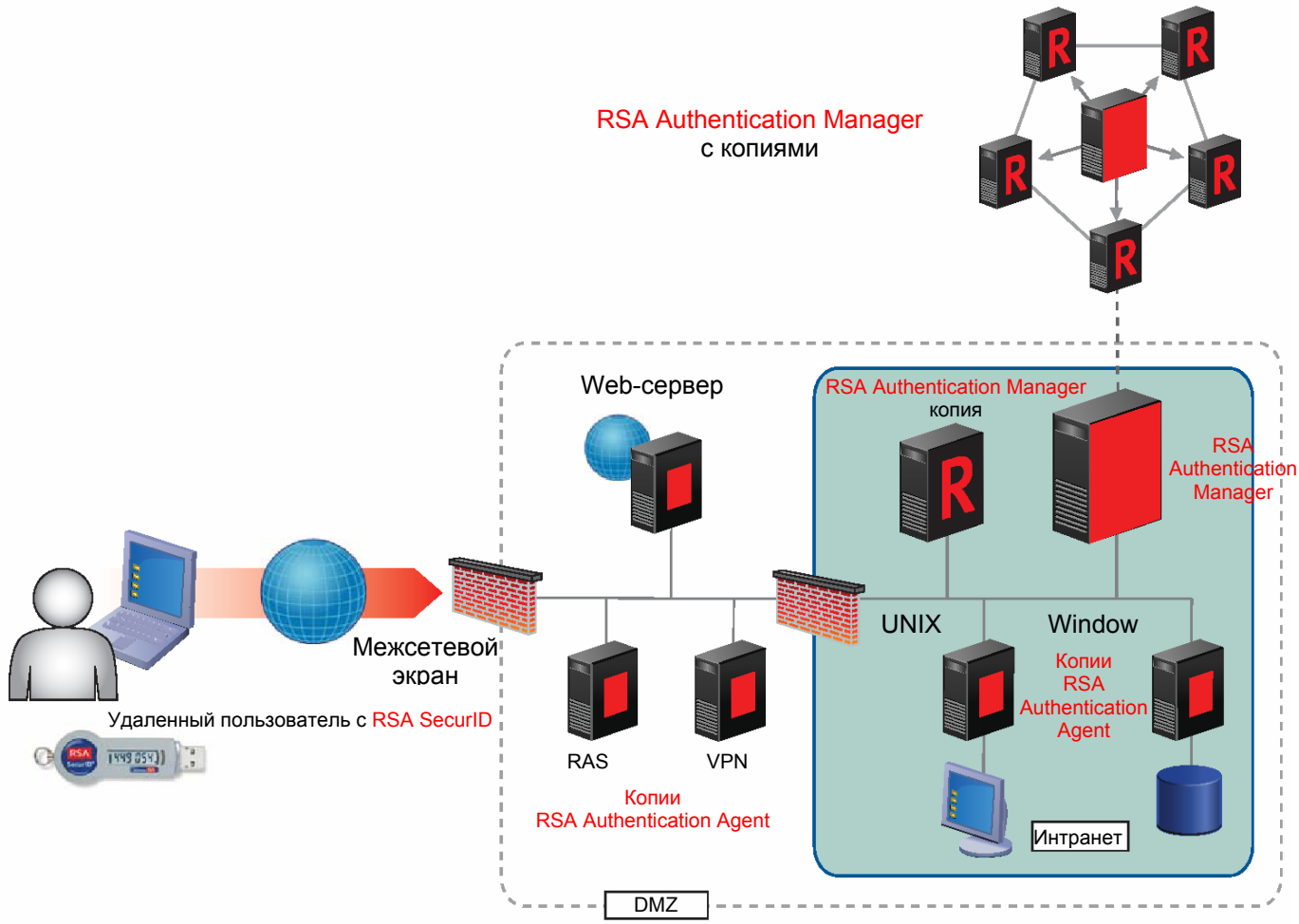
Какой поставщик?

Критерии выбора поставщика

- Полные затраты владения
- Техническая архитектура
- Концепция
- Экономическая целесообразность
- Добросовестность
- Сервис и поддержка

При оценке системы аутентификации необходимо рассмотреть следующие вопросы:

- В чем заключаются достоинства данной системы? Какие дивиденды принесет ее внедрение?
- Какая система аутентификации больше всего подходит для Вашей организации? При поиске ответа на данный вопрос оценивается не просто относительная стоимость приобретения и гарантируемая степень защищенности, но также анализируются такие факторы, как удобство для конечных пользователей, функциональная совместимость и возможность переналадки в будущем.
- Какая компания является лучшим партнером для поставки подобной системы?



Современные серверы удалённого доступа, межсетевой экран, виртуальная корпоративная сеть, средства беспроводного доступа и маршрутизаторы снабжены встроенными опциями Agent для обеспечения совместимости с системой двухфакторной аутентификации RSA SecurID. Кроме того, RSA Authentication Manager поддерживает сеансы аутентификации TACACS+ и RADIUS. Authentication Manager включает в себя совместимый с версиями 802.1x сервер RADIUS от компании Funk Software Steel-Belted Radius®. Таким образом, компании могут осуществлять управление счетами пользователей в единой базе данных, используемой для работы как системы RADIUS, так и SecurID. В рамках сеанса двухфакторной аутентификации пользователю требуется ввести имя пользователя и, вместо пароля, PIN-код плюс текущий токен-код с личного устройства RSA SecurID. Agent передает данную информацию на сервер RSA Authentication Manager, который разрешает доступ лишь в том случае, если представленная информация является правильной. Пользователю предоставляется доступ в соответствии с личным уровнем прав, который зарегистрирован в файле журнала RSA Authentication Manager.

Аутентификаторы RSA SecurID Authenticator

Доступ к защищенной сети и приложениям, предназначенным для ведения электронного бизнеса, начинается с обеспечения процесса надежной аутентификации пользователя с помощью аутентификатора RSA SecurID Authenticator. Аутентификаторы SecurID предлагаются в различных видах: аппаратные токены, программные токены, смарт-карты и устройства USB. Наиболее распространенной аппаратной формой является ключ-брелок - устройство со встроенной микросхемой, ЖК-дисплеем, способным отображать до восьми цифровых символов (или токен-код), в то же время обладающее достаточно малыми размерами для того, чтобы его можно было повесить на кольцо для ключей. При осуществлении поставки компанией RSA выполняется инициализация ключа-брелка с использованием уникального случайного значения; каждую минуту встроенная микросхема, согласно заданному алгоритму, выполняет операцию сложения и кодирования исходного значения и текущего времени для вычисления псевдослучайного числа.

Помимо ключей-брелков могут использоваться другие типы токенов, в том числе аутентификаторы размером с банковскую карту и модели устройства RSA SecurID PINpad, которое требует ввода пользовательского PIN-кода для отображения токен-кода; а также программный токен RSA SecurID для настольных ПК, работающих на платформе Windows®, для компьютерной платформы Palm™, для устройств Microsoft® PocketPC, для портативных устройств BlackBerry™ и мобильных телефонов, которые копируют функции токена RSA SecurID PINpad благодаря специальной сервисной программе. Исходное значение программного токена RSA SecurID Software Token может также храниться на смарт-карте SecurID или на USB-токене. Технология SecurID Software Token защищена от копирования для предотвращения переноса программных средств с одного устройства на другое. Так же существует USB-устройство SecurID, которое отображает токен-код и может использоваться для хранения цифровых сертификатов и паролей.

Все аутентификаторы RSA SecurID работают с использованием патентованной технологии генерации псевдослучайного токен-кода, будучи разработанными с учетом использования преимуществ алгоритма AES, принятого в качестве отраслевого стандарта. Клиенты RSA пользуются преимуществами надежности и гарантии качества, которые обеспечиваются благодаря применению стандартного алгоритма AES.

Агенты RSA Authentication Agent

Промежуточным средством, обеспечивающим возможность применения двухфакторной аутентификации, является внедрение агентского ПО - RSA® Authentication Agent, функционирующего в качестве средства защиты и увеличивающего степень эффективности политики обеспечения безопасности, реализуемой в рамках системы. Встроенными средствами Authentication Agent обладает наиболее передовое сетевое оборудование, а также программные системы (полный список компаний, которые поддерживают технологию двухфакторной аутентификации с помощью встроенных агентов, представлен на сайте www.rsasecured.com). Кроме того, компания RSA предлагает собственные программные агенты для обеспечения надежной аутентификации, например, на популярных Web-серверах: Microsoft® IIS, Apache и SunONE*, для защиты *NIX сред, и т.д.

Агенты RSA Authentication Agent

Доступ через Web
– Microsoft IIS
– Apache
– Stronghold
– SunONE

Локальный и удаленный доступ
– Windows 2000, 2003
– Windows XP
– Windows Vista
– Solaris
– IBM AIX
– HP-UX
– Red Hat Linux
– NMAS (модульная система аутентификации Novell)

Для получения более подробных сведений относительно поддержки RSA Authentication Agent посетите страницу http://www.rsasecurity.com/products/securid/authenticationagents.html

Уникальная система для операционной среды Microsoft® Windows®

При использовании в сочетании с агентским ПО для операционной системы Microsoft® Windows® программное обеспечение RSA Authentication Manager является эффективным решением для организаций, стремящихся найти надежные средства аутентификации пользователей в среде Microsoft. Благодаря использованию инновационной технологии RSA SecurID для среды Microsoft Windows обеспечивает возможность выполнения аутентификации RSA SecurID в среде Microsoft независимо от того, подключен пользователь к сети или нет. Данная система повышает степень защищенности в среде Windows и предоставляет простые и унифицированные средства аутентификации пользователей. Программное обеспечение RSA Authentication Manager поддерживает аутентификацию по протоколу RADIUS, и поэтому может осуществляться централизованное управление всеми учетными записями пользователей RADIUS. Также поддерживается аутентификация по протоколу TACACS+. Для шифрования информации, передаваемой между агентом и сервером, используется 128-bit RC5®. Одна система RSA Authentication Manager способна осуществлять поддержку тысяч агентов, гарантируя широкие возможности защиты ресурсов предприятия. Администрирование агентов и задание политик выполняется централизованно, с помощью административного приложения, что позволяет администраторам службы безопасности модифицировать настройки путем указания нужных опций с помощью кнопок, вместо написания собственного кода.

Функция автоматической регистрации клиента позволяет автоматизировать процесс безопасного создания и обновления параметров каждой копии ПО RSA Authentication Agent.

RSA Authentication Manager

ПО RSA Authentication Manager, управляемое администратором системы безопасности или администратором сети, используется для выполнения следующих функций:

- Присвоение аутентификаторов RSA SecurID доверенным лицам;
- Задание и усиление политик обеспечения безопасности, настройка защиты доступа к системам, файлам и приложениям корпоративной сети (сюда же относится функция присвоения прав доступа в зависимости от времени суток или дня недели, прав группы пользователей или параметров доступа, заданных самим пользователем),
- Поддержка журналов проверки доступа пользователей и деятельности администратора;
- А также централизованное управление параметрами учетной записи пользователя, группы, агента, копии или токена.

Программное обеспечение RSA Authentication Manager работает на платформах Windows, UNIX и LINUX. Одна копия ПО обеспечивает возможность аутентификации свыше миллиона пользователей.

Репликация базы данных необходима для компаний, которые нуждаются в высокоэффективной поддержке больших баз учетных данных пользователей, а также в удобных функциях администрирования методов аутентификации пользователей в любой точке сети. Такой способ резервирования не только обеспечивает круглосуточную работоспособность системы, но также позволяет клиентам разрабатывать эффективные и рентабельные топологии глобальной сети.

Программное обеспечение RSA Authentication Manager обладает большим количеством прогрессивных функций администрирования и контроля безопасности (которые будут рассмотрены далее в настоящем документе), в том числе возможностью многоуровневого делегирования управления, централизованного управления параметрами учетной записи пользователя и токена, а также дистанционного системного администрирования с настольного ПК, работающего на платформе Windows, или через Web-браузер.

Базовая лицензия для RSA Authentication Manager допускает одновременную работу двух серверов аутентификации: одного основного и одного сервера-копии. Корпоративная лицензия допускает взаимодействие одного основного сервера и до десяти серверов-копий в рамках одной логической области пользователей и агентов, а также совместную работу шести таких областей.

RSA Authentication Deployment Manager

Программное обеспечение RSA Authentication Deployment Manager представляет собой сетевую систему автоматизации документооборота и помогает снизить административные расходы, обеспечивая конечных пользователей самообслуживаемой платформой для запроса, активации и инициализации процесса предоставления токенов RSA SecurID. Данная система полностью автоматизирует процесс предоставления токенов, в том числе начальную загрузку в базу данных RSA Authentication Manager сведений о пользователе, назначение и активацию токенов, а также упрощение обработки запросов на получение токена RSA SecurID. Являясь настраиваемым и масштабируемым, ПО RSA Authentication Deployment Manager представляет собой идеальное решение для развертывания корпоративных систем и систем электронного бизнеса благодаря ускоренному, упрощенному и высокоэффективному процессу предоставления токенов. ПО RSA Authentication Deployment Manager включено в корпоративную лицензию и поставляется за дополнительную плату с базовой лицензией.

Основные преимущества ПО RSA Authentication Manager и RSA SecurID

Программное обеспечение RSA Authentication Manager обеспечивает высокую рентабельность инвестиций, помогая применять процессы, приносящие прибыль, снижать издержки, обеспечивать соблюдение законодательных требований и снижать риски.

Увеличение прибыли

Обеспечивая возможность надежной и доверенной аутентификации пользователей, система RSA SecurID позволяет предприятиям автоматизировать важные бизнес-процессы и внедрять их сетевое использование, гарантируя сохранение конфиденциальности обрабатываемых данных, что дает возможность привлекать новых клиентов и открывать новые источники получения доходов. Система RSA SecurID помогает предприятиям сделать важную информацию доступной в глобальной или корпоративной сети, что, в свою очередь, позволяет сотрудникам предприятия или стратегическим партнерам получать доступ к такой информации и использовать ее для предоставления услуг и заключения сделок.

Значительные возможности функциональной совместимости системы RSA SecurID обеспечивают клиентам расширенные средства эффективной защиты отдельных приложений, гарантирующие высокую степень достоверности при аутентификации конечного пользователя.

Снижение издержек

Система RSA SecurID способна помочь предприятию сэкономить деньги за счет замены систем обработки паролей. Системы обработки паролей дороги в обслуживании вследствие скрытых расходов, связанных со звонками в службу поддержки и потерей производительности пользователями. Применение системы RSA SecurID значительно снижает данные издержки за счет сокращения количества паролей, необходимых каждому пользователю, и упрощения процесса аутентификации пользователя при входе в систему.

Система RSA SecurID удобна в работе для конечных пользователей. Благодаря простому и понятному интерфейсу конечные пользователи быстро осваивают методы взаимодействия с данной системой и легко начинают применять их. Диапазон выбора форм-факторов для аутентификации гарантирует, что данная система подойдет для условий работы большинства клиентов. Установка и развертывание системы RSA SecurID осуществляется очень легко. Предоставление токенов еще более упрощено благодаря приложению RSA Authentication Deployment Manager - средству, которое способно существенно ускорить внедрение системы и снизить расходы на получение аутентификаторов RSA SecurID конечными пользователями.

Благодаря программе работы со стратегическими партнерами RSA SecurID Ready система RSA SecurID совместима с ведущими отраслевыми программными продуктами для защиты информации и работы в сети. Суммарно рядом компаний разработано свыше 300 продуктов, которые предназначены для беспроблемного взаимодействия с системой RSA SecurID. Такая встроенная функциональная совместимость может существенно снизить затраты на интеграцию и обезопасить текущие инвестиции. Полный список стратегических партнеров RSA SecurID Ready и руководств по практическому внедрению системы представлен по адресу www.rsa.com/partners/secured/securidpartners.html.

Программное обеспечение RSA Authentication Manager снижает административные расходы, предоставляя средства централизованного управления параметрами учетных записей пользователей, создания иерархической административной структуры по спискам задач и областей деятельности администраторов, а также средств сетевого администрирования для оказания помощи администраторам справочной службы.

Средства синхронизации с каталогом LDAP предоставляют возможность централизованного администрирования в нем параметров учетной записи пользователя. Синхронизация параметров учетной записи пользователя из каталога LDAP с системой RSA Authentication Manager может быть выполнена автоматически в соответствии с установленным графиком выполнения процедур синхронизации. Благодаря функции реплицирования базы данных компании могут отслеживать процесс аутентификации пользователей в любой точке мира в реальном времени, одновременно обновлять политику обеспечения безопасности в своих глобальных сетях и разрабатывать топологии глобальных сетей, которые позволяют повысить эксплуатационные характеристики. Программное обеспечение RSA Authentication Manager позволяет компаниям выполнять все указанные мероприятия, обеспечивая создание гибкой архитектуры сети, распределение нагрузки и, в конечном счете, упрощение процесса работы и снижение административных расходов.

Соответствие стандартам

Система RSA SecurID способна помочь предприятиям обеспечить соответствие отраслевым требованиям и постановлениям правительств, гарантируя надежную аутентификацию пользователей, пытающихся получить доступ к конфиденциальной информации. Надежная двухфакторная аутентификация, реализуемая, например, в рамках технологии SecurID, способна помочь предприятиям выполнить требования нормативов США, таких как Закон об отчетности и безопасности медицинского страхования 1996 года (HIPAA) в области здравоохранения, Закон Грэмма-Лича-Блайли (GLBA) в сфере финансовых услуг, и требования Европейских норм, таких как законодательство, регламентирующее использование электронных подписей.

Снижение риска

Программное обеспечение RSA Authentication Manager помогает снизить риск вынужденного простоя во время аутентификации. Эта надежная система характеризуется высокой степенью готовности и способна обрабатывать запросы миллионов пользователей и выполнять сотни аутентификаций в секунду. Поддержка основного сервера и до десяти серверов-копий в одной логической области обеспечивает автоматическое распределение нагрузки и переключение при отказе. Это позволяет повысить производительность и масштабируемость при аутентификации в разнообразных средах, в том числе в виртуальных корпоративных сетях, на серверах удаленного доступа, в беспроводных сетях, операционных системах и WEB-приложениях. При отказе основного сервера функция восстановления работоспособности производит быстрое включение сервера-копии в качестве нового основного сервера, т.е. незамедлительно восстанавливает административную архитектуру данной области.

Система RSA SecurID помогает снизить риск нарушения работоспособности сети, сэкономить деньги и время, а также уменьшить вероятность неприятных последствий, например, в виде негативной рекламы. Данная система обеспечивает высшую степень безопасности.

Предотвращение несанкционированного доступа с помощью системы аутентификации RSA SecurID

Аутентификация на предприятии

Программное обеспечение RSA Authentication Manager предоставляет доступ только тем пользователям, которые предъявляют действующую комбинацию PIN+токен-код; это дает предприятиям высокую гарантию того, что указанные лица, запросившие доступ, действительно являются уполномоченными пользователями. Это значительно уменьшает риск несанкционированного доступа. Даже корпоративные сети, объединяющие миллионы пользователей и многочисленные офисы по всему миру, могут быть защищены с помощью функций реплицирования базы данных и взаимодействия с различными областями данных для надежной аутентификации пользователей, находящихся за пределами своей области.

Контроль доступа

Система RSA Authentication Manager позволяет организациям осуществлять внедрение приложения RSA Authentication Agent для защиты различных способов доступа, а также файлов данных, приложений и других ресурсов. Путем группирования учетных записей пользователей в базе RSA Authentication Manager организации могут с легкостью централизованно назначать параметры доступа к определенным ресурсам. Кроме того, организации могут внедрять RSA Authentication Manager вместе с RSA Access Manager для создания более структурированной системы управления доступом к сетевым ресурсам.

Предотвращение попыток обхода защиты

Программное обеспечение RSA Authentication Manager будет автоматически отключать токен после серии неудачных попыток, например, попыток ввода некорректных PIN или токен-кодов. Хакеры будут пытаться использовать неожиданные средства для получения доступа к сети предприятия или к отдельному приложению электронного бизнеса, работающему в такой сети. Путем мониторинга журналов RSA Authentication Manager или событий, которые RSA Authentication Manager регистрирует, в зависимости от настройки, в системном журнале UNIX или журнале событий Windows, администратор системы безопасности способен обнаружить попытку проникновения и отреагировать на нее до того, как такая попытка нанесет ущерб.

Ответственность пользователей

Важные информационные ресурсы предприятия могут оказаться под угрозой в том случае, если пароль пользователя позаимствован (без согласия владельца) или похищен.

Однако поскольку вход в систему через процедуру двухфакторной аутентификации RSA SecurID требует ввода пользователем личного PIN-кода и токен-кода, это гарантирует отказ пользователя от любых запрещённых действий, совершённых от его имени. Осознание данного факта, а также того, что в отчетах содержатся исчерпывающие сведения обо всех попытках доступа к защищенным ресурсам, помогает пользователям оценить степень собственной ответственности за защиту информации и вести себя соответствующим образом. И несмотря на то, что хакеры часто пытаются удалить следы своей деятельности, журналы доступа RSA Authentication Manager могут оказаться важным инструментом для возбуждения и расследования судебного дела против злоумышленников.

Применение двухфакторной аутентификации

Организации могут внедрять систему RSA SecurID и настраивать её для защиты сетевых корпоративных ресурсов различными способами. При этом может быть организована глобальная защита с аутентификацией попыток доступа ко всем ресурсам сети предприятия или защита лишь стратегически важной конфиденциальной информации. Одна система может решать любую или все из перечисленных ниже задач:

- аутентификация пользователя при соединении через сервер удаленного доступа;
- аутентификация при попытке доступа через виртуальную корпоративную сеть или межсетевой экран, из сети Интернет к внутренней сети;
- аутентификация всех попыток доступа к беспроводным сетям или проводным корпоративным сетям; может быть применена ко всем пользователям, к конкретной рабочей группе, к подразделению или только к пользователям с определенным уровнем доступа;
- защита конфиденциальных данных в интрасетях и экстрасетях путем ограничения доступа к Web-страницам, URL и каталогам;
- ограничение доступа к ответственным приложениям, файлам конфиденциальных данных или другим ресурсам,
- предотвращение манипулирования административными настройками.

Независимо от области защиты используется один и тот же основной процесс двухфакторной аутентификации. Когда пользователь пытается получить доступ к защищенному ресурсу, ПО RSA Authentication Agent, защищающее данный ресурс (сервер RAS, беспроводное устройство контроля доступа, Web-сервер, ОС Windows или приложение), генерирует запрос на аутентификацию. Для получения доступа пользователь обязан ввести свое имя, PIN-код и токен-код. Запрос на аутентификацию шифруется и затем пересылается в RSA Authentication Manager.

Как выбрать систему аутентификации?

Категория	Программное обеспечение RSA Authentication Manager с аппаратными токенами RSA SecurID
Полная стоимость владения	
Приобретение	– Меньшая стоимость по сравнению со смарт-картами или устройствами проверки биометрических характеристик, если учитывать комбинации смарт-карта + устройство чтения карт + промежуточное программное обеспечение или приборы биометрической аутентификации, например, устройства сканирования радужной оболочки глаза, устройства считывания дактилоскопических узоров + соответствующее программное обеспечение. – Большая стоимость по сравнению с системами проверки паролей.
Развертывание	– Развертывание требует распространения только аппаратных токенов, необходимость в развертывании программного обеспечения, драйверов, устройств считывания или кабелей отсутствует. – Пониженные затраты на развертывание по сравнению со смарт-картами, приборами биометрической аутентификации или любыми другими системами с клиентскими программами, которые предусматривают установку на каждый настольный ПК конечного пользователя. – RSA Authentication Deployment Manager (поставляемый без дополнительной платы в корпоративной лицензии) позволяет значительно снизить затраты на развертывание.
Управление	– Эксплуатационные затраты существенно ниже по сравнению с системами проверки паролей благодаря сниженным затратам на содержание справочной службы (см. документ под названием «Оценка систем аутентификации: системы проверки паролей в сравнении с RSA SecurID»). – Централизованное администрирование исключает необходимость управления многочисленными массивами данных.
Удобство (пользователи)	
Удобство / легкость использования	– Пользователям нет необходимости запоминать многочисленные пароли. – Легкость использования: следует просто набрать на клавиатуре то, что видите. – По принципу действия система аналогична банковским картам, поэтому комбинация PIN-кода и устройства (токена) легко принимается пользователями.
Совместимость	– Работает в любом месте. Не требует установки ПО на компьютер пользователя.
Универсальность	– Простая функция: токен генерирует новый код каждые 60 секунд. В то же самое время единый аппаратный токен может служить средством доступа к многочисленным ресурсам: программа RSA SecurID Ready обеспечивает защиту более чем 300 приложений более чем от 200 поставщиков - от систем удаленного доступа к корпоративной сети до систем доступа по беспроводной сети к ресурсам на базе Web.
Удобство (корпорации)	
Соответствующая защита	– Двухфакторная аутентификация = очень мощный способ защиты. – Токен-код невозможно угадать или спрогнозировать. – Исключает угрозы «подглядывания через плечо» и троянских программ, поскольку токен-код меняется через каждые 60 секунд. – В процессе передачи по сети токен-коды не могут быть легко определены. – Если токен похищен или утерян, то пользователь знает об этом. – Поскольку токен-код генерируется динамически, он неуязвим для инструментов взлома. – Уровень безопасности повышается, поскольку необходимость записывать пароль исключена. – ПО RSA Authentication Manager предоставляет средства регистрации событий и подготовки отчетов для повышения степени ответственности конечных пользователей. – Централизованное администрирование устраняет слабые места в системе безопасности по мере добавления новых устройств, приложений и процедур связи, а также по мере добавления и удаления учетных записей пользователей или изменения их ролей. – Разграничение административных полномочий.
Функциональная совместимость / интеграция	– Функциональная совместимость более чем с 300 сертифицированными приложениями и программными продуктами более чем от 200 партнеров. – Поддержка аутентификации RSA SecurID для платформы Microsoft® Windows® независимо от того, подключен пользователь к сети или нет. – В отличие от конкурирующих программ, продукты стратегических партнеров RSA SecurID Ready проходят всестороннее тестирование и документирование перед получением сертификата.
Надежность / масштабируемость	– Программное обеспечение RSA Authentication Manager может обеспечивать одновременную обработку данных миллионов пользователей. – Функции репликации, переключения при отказе и восстановления после отказа обеспечивают высокую степень готовности системы.
Гибкость использования в будущем	– Система может быть использована для обеспечения безопасного доступа к цифровым сертификатам. – Система RSA SecurID адаптирована к методам доступа через модем, Web, корпоративную сеть и беспроводную сеть и в дальнейшем будет обеспечивать средства доступа для новых продуктов через программу SecurID Ready.

После получения запроса на аутентификацию система RSA Authentication Manager проводит поиск в своей базе данных и, после нахождения имени пользователя, сравнивает PIN-код и токен-код с данными, записанными в этой базе. Если комбинация PIN-кода и токен-кода является верной, пользователю предоставляется доступ.

Подробное функциональное описание

Архитектура

Программное обеспечение RSA Authentication Manager используется для организации защитного периметра вокруг заданных сетевых ресурсов. Системному администратору предоставляется возможность выбора защищаемых сетевых ресурсов; решение принимается в процессе установки программы, однако может быть изменено в любой момент. ПО Authentication Manager может быть установлено на одной из широкого ряда серверных платформ Windows и UNIX. Одна инсталляция может поддерживать взаимодействие более чем с одним миллионом пользователей. Каждый защищаемый сетевой объект считается агентом и работает с ПО RSA Authentication Agent. Одна инсталляция RSA Authentication Manager способна работать с тысячами агентов. ПО RSA Authentication Agent встроено в большую часть сетевого оборудования (маршрутизаторы, межсетевые экраны, корпоративные сети, корпоративные сети SSL, точки беспроводного доступа, коммутаторы и пр.), а также доступно для операционных систем и Web-серверов. Более того, существует API для интеграции двухфакторной аутентификации в нестандартные приложения.

Всякий раз при попытке получения доступа к сетевому объекту RSA Authentication Agent определяет, разрешен ли данному пользователю доступ к этому объекту, и, если ответ положительный, начинает сеанс двухфакторной аутентификации. Если пользователем введены правильные PIN-код и токен-код, доступ предоставляется; в противном случае доступ пользователю запрещается.

Многие сетевые ресурсы рассчитаны на использование протокола аутентификации RADIUS. Для обеспечения максимальной гибкости при обслуживании пользователей RSA Authentication Manager также включает в себя сервер RADIUS, совместимый с 802.1x, который поддерживает работу с методом PAP и несколькими методами EAP, включая POTP, TTLS, PEAP и EAP15.

Элементы системы

Система RSA Authentication Manager состоит из следующих основных элементов:

- База учетных записей пользователей, аутентификаторов и параметров агентов RSA Authentication Agent, а также база регистрации попыток аутентификации пользователей и действий администраторов. База данных RSA Authentication Manager построена на основе реляционной базы данных Progress Software®, лидирующей OEM-системы. Преимуществом базы данных Progress является быстрый доступ, позволяющий обрабатывать запросы на аутентификацию и сохранять информацию за минимально возможное время.
- Система RSA Authentication Manager выполняет аутентификацию пользователей на основании токенов. Данная система является основой процесса аутентификации. Работая совместно с агентом, ПО RSA Authentication Manager использует базу данных для проверки параметров учетной записи пользователя, после чего предоставляет или запрещает доступ.
- Программа администрирования, основанная на графическом пользовательском интерфейсе, предоставляет системному администратору возможность управлять системой, т.е. задавать и изменять параметры, назначать аутентификаторы, готовить отчеты. Подробное описание данной программы содержится в следующей главе.
- Функции тиражирования базы данных и администрирования защиты данных для предотвращения взлома защиты путем замещения оригинала.

Система RSA Authentication Manager включает в себя большое количество дополнительных элементов, среди которых следующие:

- Сервер RADIUS, который поддерживает процессы аутентификации с помощью протокола RADIUS и допускает централизованное управление учетными записями пользователей и профилями RADIUS. (Сервер RADIUS может работать на том же ПК, где установлена система RSA Authentication Manager или дистанционно.)
- Сервер TACACS+, который поддерживает процессы аутентификации с помощью протокола TACACS+.

Тиражирование базы данных и распределение нагрузки

Одним из наиболее привлекательных свойств системы RSA Authentication Manager является функция тиражирования базы данных. Благодаря тиражированию базы данных администраторы системы защиты имеют возможность повысить производительность путем настройки нескольких серверов-копий для одновременной обработки запросов на аутентификацию.

Приложение RSA Authentication Agent обеспечивает автоматическое распределение нагрузки путем определения времени отклика серверов-копий и направления запросов на аутентификацию соответствующим образом. Администраторы также могут вручную определить порядок обращения к серверам путём редактирования файла конфигурации.

Обладая лицензией RSA Authentication Manager Base, клиенты могут развертывать комплекс, включающий в себя один основной сервер для выполнения административных функций и аутентификации и один сервер-копию, также предназначенный для выполнения аутентификации. Обладая лицензией Enterprise Edition, клиенты могут развертывать до шести комплексов (областей данных), каждый из которых будет включать в себя основной сервер и до десяти сервер-копий. Такая архитектура не только гарантирует готовность системы, но также позволяет клиентам разрабатывать эффективные и рентабельные топологии глобальной сети.

Каждый сервер-копия снабжен полной копией базы учетных записей пользователей. При отказе основного сервера сервер-копия легко может быть назначен новым основным сервером, при этом быстро восстанавливаются как административные функции, так и база данных.

Блокировка учётной записи

Для обнаружения и предотвращения взлома защиты путем повторного использования введённой пользователем информации система снабжена процедурой блокировки учётной записи пользователя. При успешной аутентификации пользователя его учётная запись блокируется на одну минуту – ровно столько времени требуется на смену токен-кода.

Обмен данными в системе

Для обеспечения надежного обмена данными между основным сервером и серверами-копиями RSA Authentication Manager использует протокол TCP. Поток данных шифруется, и ключ шифрования изменяется каждые десять минут.

Для обмена данными между RSA Authentication Manager и агентом используется комбинация UDP и Unicast, что позволяет обеспечить максимальную скорость работы. Пакеты данных шифруются каждый своим отдельным ключом для защиты от перехвата информации и имитации пользователем другого лица.

Шифрование

Каждая копия агента RSA Authentication Agent в системе обладает уникальным ключом или секретным кодом. Данный «секретный код» представляет собой строку псевдослучайных данных, которая известна только клиенту и серверу. Этот код используется для шифрования и дешифрования передаваемых данных. После получения агентом PIN-кода и токен-кода пользователя данная информация шифруется с помощью секретного кода и других данных, уникальных для аутентификации, и пересылается в RSA Authentication Manager.

Синхронизация времени с UCT

Для синхронизации всех продуктов компании RSA используется универсальное скоординированное время (UCT). Токен RSA SecurID настраивается по UCT (идентично среднему времени по Гринвичу) перед передачей клиенту; в процессе установки системные часы RSA Authentication Manager также устанавливаются по UCT. В сущности, все продукты компании RSA по всему миру точно устанавливаются по одним и тем же часам, что исключает необходимость учитывать разницу между часовыми поясами и переход на «летнее время» и обратно.

Регулирование действительного временного интервала токена и отклонений часов

При использовании аппаратных токенов программное обеспечение RSA Authentication Manager рассчитано на выполнение аутентификации в рамках временного интервала продолжительностью три минуты для компенсации небольших несоответствий в настройках времени и отклонений часов. Интервал рассчитывается следующим образом: текущее универсальное скоординированное время на системных часах плюс минута до и минута после данного времени. Если имя пользователя и PIN-код введены верно, но введенный токен-код не соответствует текущей минуте, RSA Authentication Manager выполняет автоматическую проверку на предмет его соответствия правильному коду, рассчитанному для предыдущей и последующей минуты. Данная процедура позволяет компенсировать ситуацию, когда часы аутентификатора имеют небольшое отклонение от системных часов ПО RSA Authentication Manager. Если обнаружено совпадение с предыдущим или следующим токен-кодом, аутентификация пользователя считается выполненной успешно, а в базе учетных записей пользователей делается соответствующая запись для внесения необходимых изменений с целью учета отклонения в настройке часов.

Попытки повторного использования недавно использованных токен-кодов обнаруживаются и регистрируются. Попытки использования очень старого токен-кода предотвращаются, поскольку в любом одном сеансе аутентификации сервер допускает наличие малого количества действительных токен-кодов.

Путем регулярного обновления журналов параметров учетной записи пользователя система RSA Authentication Manager обеспечивает такое регулирование времени токена, что токен-код всегда попадает в диапазон временного интервала, составляющего три минуты. Однако если пользователь не входит в систему в течение длительного времени (как правило, составляющего несколько месяцев), время токена может отклониться за пределы трехминутного интервала, что приводит к ситуации, когда токен-код не признается действительным. В этом случае RSA Authentication Manager проверяет токен-коды, соответствующие интервалу времени, который начинается за 20 минут до текущего момента и заканчивается через 20 минут после текущего момента. Если токен-код соответствует одному из этих токен-кодов, RSA Authentication Manager запрашивает у пользователя следующий токен-код, чтобы проверить обладание токеном; если второй токен-код характеризуется аналогичным отклонением времени, то токен признается действительным. Аутентификация пользователя считается выполненной успешно и RSA Authentication Manager отмечает в журнале параметров учетной записи пользователя отклонение часов конкретного аутентификатора для его корректировки при попытках доступа в будущем.

Тем не менее, если введенный PIN-код не соответствует требуемому или введен неправильный токен-код, неправильность которого не может быть объяснена отклонением часов, система RSA Authentication Manager требует повторения пользователем попытки аутентификации. Количество повторов попыток аутентификации, возможных до блокирования учетной записи пользователя и создания предупреждающей записи в журнале, может быть задано администратором.

Несмотря на то, что RSA Authentication Manager применяет аналогичный процесс аутентификации для всех токен-кодов RSA SecurID, допуски отклонения времени для токена RSA SecurID немного шире, по этой причине отклонение часов может быть больше, чем то, которое допускается для персональных компьютеров и устройств PDA.

Поддержка пользователей мобильных устройств

Система RSA Authentication Manager может быть настроена таким образом, что если в процессе аутентификации приложение не может распознать введенное имя пользователя, то приложение автоматически уведомляет об этом системы RSA Authentication Manager, обеспечивающие защиту других областей данных корпоративной сети.

В каждой области данных работает один основной сервер RSA Authentication Manager и один или несколько серверов-копий, которые обладают одной и той же базой сведений о пользователях и попытках входа в систему. База данных тиражируется между серверами конкретной области данных. Если учетная запись пользователя относится к одной области данных, а пользователь пытается получить доступ к ресурсу, защищаемому программой RSA Authentication Agent, которая передает запрос на аутентификацию в систему RSA Authentication Manager другой области, то выполняется операция перекрестной аутентификации пользователя в рамках сети предприятия. Если учетная запись пользователя идентифицируется системой RSA Authentication Manager другой области в качестве действительного Удаленного пользователя, то запрос на аутентификацию будет направлен в систему RSA Authentication Manager данной области для проверки правильности.

Как только аутентификация будет успешно завершена, локальная система Authentication Manager поместит персональные сведения о пользователе в свою кэш-память для того, чтобы ускорить последующие входы пользователя в сеть. Это позволит избежать дублирования учетных записей пользователей в каждой области, контролируемой системой RSA Authentication Manager, и предотвратить ситуацию, когда пользователь более не работает в компании, а фантомные учетные записи пользователя по-прежнему хранятся в различных базах основных серверов системы RSA Authentication Manager.

Для поддержки нескольких областей данных и установления перекрестного взаимодействия необходимо обладать лицензией Authentication Manager Enterprise.

Управляемые услуги аутентификации

Многие организации интересуются возможностями защиты своих сетей с помощью системы двухфакторной аутентификации пользователей, однако просто не обладают инфраструктурой или средствами для развертывания и обслуживания такой системы. В качестве альтернативы многие ведущие поставщики услуг сейчас предлагают систему RSA SecurID в качестве составной части их комплексов для обеспечения удаленного доступа, настройки корпоративных сетей, межсетевых экранов или предоставления услуг управления системой безопасности. В зависимости от необходимой клиенту степени управляемости система RSA Authentication Manager может быть установлена либо в сети поставщика услуг, либо в сети клиента и управляться поставщиком услуг дистанционно. Некоторые поставщики услуг помимо этого предлагают программный токен RSA SecurID в качестве встроенного компонента утилиты подключения клиента корпоративной сети на настольном ПК пользователя.

Если компания использует RSA Authentication Manager, установленный в сети поставщика услуг, то сервер выполняет аутентификацию удаленного пользователя до того, как будет создан защищенный канал связи с корпоративной сетью.

Функциональная совместимость

Благодаря программе RSA SecurID Ready система RSA Authentication Manager совместима с ведущими отраслевыми программными продуктами для защиты информации и работы в сети. RSA Authentication Manager может взаимодействовать более чем с 300 продуктами более чем от 200 стратегических партнеров RSA SecurID Ready. Полный список стратегических партнеров RSA SecurID Ready представлен по адресу www.rsasecurity.com/partners/secured/securidpartners.html.

Одним из преимуществ данной прогрессивной стратегии обеспечения функциональной совместимости является то, что компании могут использовать уже имеющуюся инфраструктуру и экономить на текущих инвестициях.

Защита инвестиций

Если Вам необходимо усилить способы аутентификации, действующие в Вашей сети (например, с использованием RSA SecurID для защиты конфиденциальной информации инфраструктуры открытых ключей), Вы можете просто задействовать уже установленную систему RSA SecurID. RSA Authentication Manager без проблем работает с системой RSA Digital Certificate. Кроме того, система RSA SecurID может быть применена для аутентификации пользователей системы RSA Access Manager. Идентификационная информация RSA SecurID также может быть интегрирована с информацией на других площадках с помощью опции RSA Federated Identity Manager.

Администрирование системы RSA Authentication Manager

Программное обеспечение RSA Authentication Manager включает в себя определенное количество функций, позволяющих усовершенствовать как оперативное управление системой, так и управление системой безопасности.

Управление системой безопасности

Доступ к комплексным административным функциям предоставляется через интуитивно понятный и удобный для использования графический пользовательский интерфейс, снижающий требования к уровню подготовки оператора.

В качестве альтернативного варианта Web-утилита, называемая Quick Admin, позволяет администратору системы защиты редактировать параметры учетной записи пользователя и токена без установки администрирующего клиента на каждом настольном ПК.

Предназначенная для использования в справочной службе первого уровня, утилита Quick Admin снабжена интуитивно понятным Web-интерфейсом для решения самых распространенных задач управления параметрами учетных записей пользователей и токенов (например, восстановление PIN-кодов, деактивация утерянных токенов и присвоение новых токенов).

Система RSA Authentication Manager поддерживает возможность использования каталога LDAP в качестве централизованного заслуживающего доверия источника информации о пользователях. В каталоге LDAP можно централизованно управлять параметрами учетной записи пользователя и группы пользователей, а также автоматически импортировать эти сведения в базу данных системы RSA Authentication Manager на основании заданного графика синхронизации. Информация относительно аутентификаторов хранится в защищенном виде и управляется только через консоль администратора.

Учетные записи пользователей могут быть объединены в группы для назначения общих политик обеспечения безопасности, что в результате упрощает работу администратора. Например, вход в систему для каждого пользователя или группы может быть ограничен временем суток или днем недели. То же самое относится к отдельным агентам. Выполнив простые действия, администратор имеет возможность централизованно ограничить доступ выбранной группе пользователей или отдельным лицам.

Права администратора могут быть назначены путем создания административных ролей в масштабе предприятия. При использовании данной возможности назначение новых токенов может выполняться локально, а управление политиками доступа - централизованно. Администрирование областей данных также может выполняться централизованно или локально.

Кроме того, управление профилями RADIUS может осуществляться централизованно через систему RSA Authentication Manager, которая объединяет в себе функции аутентификации и администрирования.

Назначение и замена токенов

При использовании программного обеспечения RSA Authentication Manager процесс управления токенами осуществляется централизованно и весьма эффективно. Интерфейс с удобным управлением для настройки учетных записей пользователей и групп, назначения и удаления аутентификаторов, а также задания параметров доступа существенно упрощает процедуры администрирования аутентификаторов. Группы токенов с истекшим сроком действия могут быть заменены одновременно, при этом периодически повторяющаяся и часто занимающая много времени задача полностью автоматизирована.

Новые учетные записи пользователей могут быть добавлены в базу данных в любое время, а RSA Authentication Manager автоматически воспрепятствует дублированию пользовательских ID. Данные функции в сочетании с комплексной пожизненной гарантией на токены значительно упрощают работу и снижают общие затраты на управление системой и ее обслуживание.

Типы лицензий RSA Authentication Manager

	Base	Enterprise Edition
Количество серверов аутентификации	1 основной и 1 сервер-копия	1 основной и до 10 серверов-копий в каждой области данных
Количество областей данных (групп основных серверов и серверов-копий)	1 область	До 6 областей
RSA Authentication Deployment Manager	Дополнительная стоимость	Включено

Автоматическая процедура распределения токенов с помощью браузера

Программное приложение RSA Authentication Deployment Manager помогает снизить административные расходы, обеспечивая конечных пользователей самообслуживаемой платформой для запроса, активации и инициализации процесса предоставления токенов с помощью RSA SecurID. Данная система полностью автоматизирует процесс предоставления токенов, в том числе начальную загрузку в базу данных RSA Authentication Manager сведений о пользователе, назначение и активацию токенов, а также упрощение обработки запросов на получение токена в RSA SecurID. В ручном присвоении токена пользователю более нет необходимости. Любой токен может быть послан любому пользователю, поскольку Deployment Manager программным способом управляет процессом присвоения токена пользователю. Единственным административным действием остается утверждение токена и фактическая передача токена конечному пользователю. Будучи настраиваемым и масштабируемым, приложение RSA Authentication Deployment Manager является идеальным решением для развертывания корпоративных систем и систем электронного бизнеса благодаря ускорению, упрощению и повышению эффективности процесса предоставления токенов.

Приложение RSA Authentication Deployment Manager включено в пакет лицензии RSA Authentication Manager Enterprise Edition и поставляется за дополнительную плату с пакетом лицензии RSA Authentication Manager Base Edition.

Регистрация данных в журнале и подготовка отчетов

Помимо прочего, программное обеспечение RSA Authentication Manager поддерживает функцию уведомления о происходящих событиях. Выбранные сообщения из журнала проверки Manager могут быть переданы в системный журнал UNIX или журнал событий Windows, привлекая внимание к наиболее важным событиям из обширного списка журнальных записей системы.

Благодаря этому проверка каждой попытки входа в систему и каждой выполненной операции осуществляется автоматически. Область проверки распространяется на параметры учетной записи пользователя, что помогает предупредить убытки от злонамеренных действий или халатности штатного персонала в отношении политик обеспечения безопасности. Функция автоматического обслуживания журналов позволяет администраторам задавать настройки для архивации файлов журналов. Данная функция, работающая по принципу «сделал и забыл», обеспечивает безопасное сохранение эксплуатационных журналов без вмешательства администратора. Программное обеспечение RSA Authentication Manager позволяет администраторам легко настраивать вид предоставления отчетов в соответствии с собственными требованиями к безопасности. Отчеты могут быть настроены таким образом, чтобы обеспечивать возможность просматривать информацию о действиях, особых состояниях или инцидентах, а также итоговые отчеты о работе.

Прочие функции

Программное обеспечение RSA Authentication Manager обладает множеством других функций, предназначенных для общего расширения возможностей системы, а также снабжено онлайн-документацией, справочными средствами и набором административных инструментов, позволяющих администраторам выполнять свои функции.

Лицензия RSA Authentication Manager Enterprise edition

Различия между лицензиями RSA Authentication Manager

Возможность поддержки до одиннадцати серверов аутентификации обеспечивает владельцам лицензии RSA Authentication Manager Enterprise Edition преимущество сниженного риска вынужденного простоя при аутентификации. Благодаря работе нескольких резервных серверов аутентификации можно избежать различных негативных последствий при таких происшествиях, как отказ сети, отказ сервера и отказ узла в процессе эксплуатации.

Несколько областей позволяют владельцам лицензии Enterprise Edition конфигурировать до шести копий RSA Authentication Manager (один основной сервер и до десяти серверов-копий в каждой); каждая область будет обладать своей отдельной базой учетных записей пользователей и журналов. При этом может быть организовано перекрестное взаимодействие, что позволит копии Authentication Manager одной области, в которой введенное имя пользователя не будет распознано, автоматически связаться с остальными областями для проверки.

Несколько областей и серверов-копий позволяют приложению версии Enterprise Edition обеспечивать клиентов гибкими средствами работы для эффективного и безопасного внедрения технологии RSA SecurID в глобальной сети компании. Клиенты могут снабдить серверами-копиями пользователей различных регионов, что уменьшит трафик и расходы на трансконтинентальную передачу информации по сети, а также повысит производительность. Помимо этого, клиенты могут разделить американских, европейских и азиатских сотрудников на две области с локальным администрированием, поддерживая возможность международного доступа для командированных сотрудников.

Гибкость, характерная для приложения версии Enterprise Edition, дает возможность предприятиям обеспечить режим работы, отвечающий соответствующим требованиям политик администрирования и обеспечения безопасности. Компании любого размера могут нуждаться в соответствии различным административным требованиям (т.е. иметь отдельные подразделения или филиалы), что делает необходимым создание групп пользователей в отдельных базах данных (т.е. областях данных). Некоторые правительственные нормативы требуют хранить сведения о компаниях или сотрудниках в базах данных согласно соответствующему законодательству, регламентирующему защиту конфиденциальности.

Приложение версии RSA Authentication Manager Enterprise Edition позволяет компаниям организовывать конфигурацию размещения данных в сети таким образом, чтобы расширить число пользователей и проектов, которые могут воспользоваться технологиями аутентификации RSA SecurID. По мере добавления учетных записей пользователей и проектов распределение нагрузки по дополнительным серверам аутентификации приводит к существенному росту производительности и положительной оценке результатов работы конечными пользователями.

Программное приложение RSA Authentication Deployment Manager дает пользователям, независимо от их местонахождения, возможность самостоятельной работы с параметрами токенов.

Чтобы обеспечить максимальное время готовности к работе, ПО версии Enterprise Edition сертифицировано для работы с платформой высокой степени готовности Veritas Cluster Server для Solaris. Благодаря запуску основной копии RSA Authentication Manager в системе с высокой степенью готовности администраторы могут быть уверены в том, что RSA Authentication Manager всегда будет доступным для администрирования и синхронизации баз данных.

Заключение

Программное обеспечение RSA Authentication Manager является ключевым элементом системы RSA SecurID. При использовании системы RSA SecurID компании могут проверять идентификационные данные пользователей, стратегических партнеров и клиентов в процессе совместной работы с ними. Высокая уверенность в точной идентификации пользователей позволяет компаниям открывать удаленный доступ к большему числу приложений и данных, повышая прибыль и снижая расходы, одновременно уменьшая риски и обеспечивая соблюдение требований государственных, отраслевых и внутрикорпоративных нормативов.

Предоставление доступа ограниченному числу уполномоченных пользователей является важным фактором защиты информации, систем и ресурсов предприятия. Убытки, связанные с нарушением системы безопасности, считаются одними из наиболее дорогостоящих и деструктивных преступлений в сфере защиты информации. Следовательно, компании очень важно инвестировать в высокоэффективную систему аутентификации, которая может масштабироваться с целью защиты ответственных приложений в рамках предприятия. Система двухфакторной аутентификации RSA SecurID, включающая обеспечение RSA Authentication Manager, предоставляет высокоэффективные средства, позволяющие избежать указанных убытков. Данная система является гибкой, масштабируемой и может быть развернута различными способами: для защиты особых объектов, для защиты файлов и приложений или для защиты всех каналов доступа к сети предприятия.

Программное обеспечение RSA Authentication Manager поддерживается широким рядом производителей аппаратного и программного обеспечения систем связи, что делает его наиболее функционально совместимым по сравнению с любой системой аутентификации из числа представленных на рынке. Данная система не только защищает текущие инвестиции в инфраструктуру, но также обеспечивает компаниям гибкость, необходимую для дальнейшего развития.

RSA – это Ваш проверенный партнер

RSA - отделение компании EMC, занимающееся проблемами обеспечения безопасности, является экспертом в области защиты централизованных информационных систем, и помогает обеспечить защиту информации в течение всего времени ее существования. RSA снабжает клиентов рентабельными средствами защиты важных информационных ресурсов и интерактивной идентификационной информации, независимо от сферы деятельности и уровня развития предприятия клиента, а также средствами управления информацией по вопросам обеспечения безопасности и информацией о событиях, позволяющими упростить процесс обеспечения соответствия требованиям стандартов.
RSA предлагает ведущие в отрасли решения по обеспечению идентификационной информации и контролю доступа, управлению шифрами и ключами защиты, управлению соответствием стандартам и управлению информацией по вопросам обеспечения безопасности, а также решения по защите от фальсификаций. Эти решения применяются для защиты личных данных миллионов пользователей, сведений о выполняемых ими операциях и данных, создаваемых в результате выполнения этих операций. Дополнительные сведения приведены на сайтах www.RSA.com и www.EMC.com.

AS51 SB 0607

RSA®
The Security Division of EMC
RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com