Консолидированная безопасность

Обзор особенностей интегрированного решения для непосредственной защиты данных, анонсированного Gemalto в начале 2015 г.

Игорь Афанасьев – пресейл-менеджер, SafeNet Europe B.V. *(подразделение Identity and Data Protection компании Gemalto)* в России и СНГ.

Введение

В начале 2015 г. компания Gemalto интегрировала SafeNet KeySecure и SafeNet Virtual KeySecure for security policy and key management в единое решение – SafeNet Crypto Pack – на базе специализированного аплайнса (рис. 1). Это позволило полностью консолидировать функции как управления ключами, так и процедуру шифрования чувствительных структурированных и неструктурированных корпоративных данных, развертываемых на локальных физических/виртуальных или облачных серверах, в составе частных или распределенных датацентров. При этом данные могут шифроваться на уровне приложений, отдельных полей таблиц баз данных, файловых систем, виртуальных машин.

Консолидация управления безопасностью данных позволила:

- *снизить влияние шифрования на приложения за счет переноса ресурсоемких задач симметричного шифрования на выделенное устройство;*
- *снизить стоимость администрирования шифрования и управления ключами за счет централизации и автоматизации операций;*
- *упростить соблюдение комплаенса за счет централизованного, эффективного аудита процессов шифрования и управления ключами, что дало возможность сократить время сотрудников, затрачиваемое на соблюдение регламентов;*
- *снизить TCO (Total Cost of Ownership) за счет "выровненных" требований к процедурам шифрования в каждом случае;*
- *упростить поддержку требований безопасности и комплаенса для виртуализованных сред;*
- *снизить риски, обеспечивая максимальную безопасность ключей за счет использования специальных аппаратных решений.*

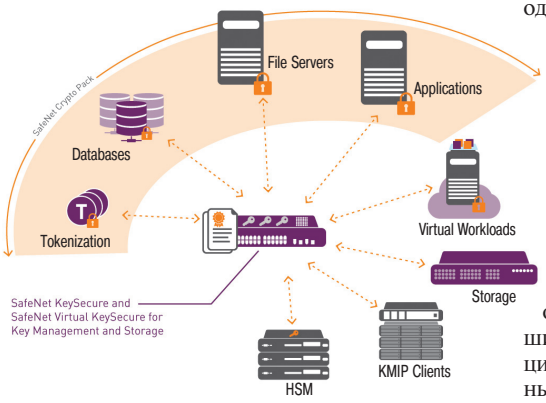

Рис. 1. Решение SafeNet Crypto Pack обеспечивает безопасность корпоративных данных на всех уровнях, а также управление ключами шифрования в течение всего жизненного цикла данных.

Решения SafeNet Crypto Pack

Шифрование на уровне приложений (KeySecure/Virtual KeySecure с Crypto Pack + ProtectApp)

Решение Gemalto SafeNet ProtectApp поддерживает шифрование конфиденциальных данных на уровне приложений как неструктурированных типов, например, файлы Excel и PDF, так и структурированных, таких как номера кредитных карт и социального страхования, паспорта, пароли. В результате, эффективно достигается выполнение как всех внутренних политик и требований, так и региональных и международных стандартов (включая Payment Card Industry Data Security Standard – PCI DSS).

Здесь шифрование происходит на этапе появления данных на сервере приложения, оставаясь после этого в зашифрованном виде в течение всего жизненного цикла, включая процедуры резервного копирования, миграции и др. Решение может быть развернуто на физических, виртуальных и облачных инфраструктурах, поддерживая миграцию данных из одной среды в другую.

Решение позволяет отделить задачи управления политиками доступа от доступа к данным и ключам шифрования. Например, может быть применена политика, которая будет запрещать администратору вносить какие-либо изменения в конфигурацию без дополнительного согласования.

SafeNet ProtectApp может выполнять широкий спектр криптографических операций, включая шифрование, дешифрование, подписание и проверку цифровой подписи, поддержку безопасных алгоритмов хэширования (SHA) и аутентификацию сообщения на основе хэш-кода (HMAC). Также оно позволяет автоматизировать процедуры ротации ключей. Решение обеспечивает единый интерфейс для регистрации, аудита и отчетности доступа к защищенным данным и ключам шифрования.

Особенности решения:

- *поддерживаемые веб-серверы приложений:* Apache Tomcat, IBM WebSphere, JBoss, Microsoft IIS, Oracle WebLogic, SAP NetWeaver, Sun ONE и др.;
- *поддерживаемые облачные и виртуальные инфраструктуры*: работает со всеми основными облачными платформами, в том числе с AWS и VMware;
- *поддерживаемые алгоритмы шифрования:* 3DES, AES-256, SHA-256, SHA-384, SHA-512, RSA-1024, RSA-2048, RSA-3072, RSA-4096;
- *поддерживаемые платформы для ICAPI-провайдеров:* Red Hat Enterprise Linux 5.4 и выше; Microsoft Windows 2003, 2008 R2 и 7 (32-bi/64-bit);

Прозрачное шифрование БД (KeySecure/Virtual KeySecure с Crypto Pack + ProtectDB)

SafeNet ProtectDB обеспечивает прозрачное шифрование “чувствительных” данных в мультивендорных СУБД на уровне полей таблиц БД и дает возможность централизованного управления ключами, а также политиками управления шифрованием и доступа к данным. Поддерживаемые СУБД: Oracle, Microsoft SQL Server, IBM DB2.

Токенизация: (KeySecure/Virtual KeySecure с Crypto Pack + Tokenization Manager)

Токенизация, в отличие от шифрования, не влияет ни на структуру БД, ни на формат отдельных полей БД и требует минимального изменения приложений.

При токенизации часть данных (“чувствительных” к утечке) какого-то поля фиксированной длины заменяется на токен. При этом сами данные в зашифрованном виде хранятся в отдельном хранилище, что позволяет, например, сузить область хранения и обработки “чувствительных” данных и, соответственно, область внешнего аудита (PCIDSS).

Особенности решения:

- *поддерживаемые СУБД:* IBM DB2, Microsoft SQL Server и Oracle;
- *поддерживаемые платформы:* Microsoft Windows, Linux, Solaris, HP-UX, AIX;
- *поддерживаемые API:* Java, .NET, Web Service (SOAP, REST/JSON).

Шифрование на уровне виртуальных машин (KeySecure/Virtual KeySecure с Crypto Pack + ProtectV)

Решение обеспечивает полное шифрование диска образа виртуальной машины и подключаемых томов (включая систем-

Рис. 2. ProtectV обеспечивает безопасность как самих данных виртуальной машины, так и ее образа на всех этапах использования.

ные разделы), делая возможной безопасную миграцию "чувствительных" данных или/и данных с жесткими регламентными требованиями в облако или виртуальный датацентр. Поддерживаемые платформы: AWS EC2, Amazon VPC, VMware vSphere. Поддерживаемые ОС виртуальных машин: Microsoft Windows Server, CentOS, SUSE Linux Enterprise Server (SLES), Red Hat Enterprise Linux (RHEL), Ubuntu.

Шифрование на уровне файловой системы (KeySecure/Virtual KeySecure с Crypto Pack + ProtectFile)

Решение обеспечивает прозрачное и автоматизированное шифрование данных приложений при хранении на уровне файловой системы в условиях распределенной ИТ-инфраструктуры без заметного влияния на бизнес-операции, производительность приложений и конечных пользователей. Поддерживаемые платформы: Linux (Red Hat Enterprise, Suse, Oracle Unbreakable Enterprise Kernel), Microsoft Windows, Apache Hadoop.

Шифрование данных hadoop-кластера (KeySecure/Virtual KeySecure с Crypto Pack + ProtectFile for Linux)

Вопросы защиты больших данных, вследствие резко возросшей их актуальности, в настоящее время приобретают особое значение. В апреле 2014 г. были опубликованы результаты 7-го ежегодного исследования «Цифровая вселенная», проведенного IDC. В соответствии с исследованием, объем цифровой вселенной каждые два года расширяется в 2 раза и к 2020 г. достигнет 44 трлн гигабайт (10% этого объема будет создаваться датчиками). В нем также отмечается изменение удельной доли «полезных данных», т.е. данных, пригодных для анализа. В 2013 г. в эту категорию попадало только 22% информации цифровой вселенной. При этом фактически анализировалось всего 5% данных. К 2020 г., благодаря развитию «Интернета вещей», более 35% данных будут считаться полезными.

Возможность анализировать очень большие объемы неструктурированных данных позволяют решения аналитики больших данных, развертываемые на базе распределенных hadoop-кластеров, которые постепенно становятся неотъемлемой компонентой многих ИТ-систем. Эти специализированные хранилища позволяют интегрировать и обрабатывать данные от всех корпоративных OLTP- и OLAP-хранилищ, обогащая их информацией из других общедоступных источников (рис. 1). В результате развиваются принципиально новые способы взаимодействия с заказчиками, но одновременно возникают и новые сложности, например, необходимость администрировать, хранить и защищать огромные объемы разнообразных данных.

Согласно этому отчету, 40% данных в цифровой вселенной нуждаются в различных мерах защиты – от обеспечения повышенной конфиденциальности до полного шифрования. При этом фактически защищается только половина этих данных (20% от общего объема). При развертывании решений аналитики больших данных, если не предпринимать дополнительных мер по обеспечению безопасности данных, эта проблема может во многом усугубиться.

В hadoop-кластере информация записывается и обрабатывается на неком подмножестве узлов (DataNodes). Их число вместе с управляющими узлами может достигать сотен и тысяч. В настоящее время нативной функциональности Apache Hadoop недостаточно для обеспечения защиты данных, и каждый DataNode узел представляет собой потенциальную точку утечки данных. Это обстоятельство часто служит сдерживающим фактором внедрения hadoop-решений, если организация соблюдает жесткие требования по комплаенсу или регулятивные (законодательные/отраслевые/внутренние) требования.

SafeNet ProtectFile for Linux обеспечивает прозрачное шифрование конфиденциальных данных (на уровне файлов, локальных и сетевых папок), хранящихся в hadoop-кластере на узлах DataNode с минимальным влиянием на производительность и конечных пользователей. Решение основано на совместной работе агента, устанавливаемого на защищаемый DataNode-узел, и аппаратного сервера SafeNet KeySecure для защиты ключей шифрования и управления политиками доступа.

ProtectFile хранит файловые ключи в зашифрованном виде, а ключи шифрования ключей (Key Encryption Key) хранятся отдельно от защищаемых данных для их гарантированной защиты от несанкционированного доступа. Гранулированное управление доступом позволяет создавать и исполнять политики с правом доступа к зашифрованным данным только для целевых групп пользователей и служб Hadoop.

ProtectFile for Linux может работать со следующими ОС: Red Hat Enterprise Linux (RHEL), Oracle Enterprise Linux (OEL), SUSE Linux, Ubuntu. Операционная система узла DataNode должна быть в списке поддерживаемых систем.

Остановимся чуть подробней на внутренних технических особенностях решения. На защищаемом сервере (узле DataNode) работает «драйвер виртуальной файловой системы» (safenetfs), который перехватывает все запросы от приложений (ПО Hadoop для DataNode) к файловой системе Linux и передает на агент ProtectFile (FEAgent). Агент ProtectFile сверяется с политикой безопасности и в зависимости от результатов дает "разрешение" на файловые операции. Это "разрешение" означает передачу ключа шифрования (KEK) для расшифровки ключа шифрования файла/папки, что позволяет произвести стандартные операции с файлами (чтение, модификация и др.).

Файловая система Hadoop является своего рода клиентом для файловой системы safenetfs. С точки зрения «ПО Hadoop для DataNode», доступ к файловой системе Linux прозрачный в случае наличия разрешения на доступ. ПО Hadoop «не знает» о существовании ProtectFile. Фильтр драйвер находится «выше» файловой системы Linux (ext2,3,4 NFSv3,4)

С точки зрения развертывания, Hadoop отличается от обычных систем большим количеством узлов, на которые необходимо установить ProtectFile. Для автоматизации задачи используется Automation Helpers (AH) – набор скриптов, входящих в стандартный инсталляционный пакет. При этом не требуется внесения каких-либо изменений в существующую имплементацию hadoop-кластера. После развертывания ProtectFile сервисы Hadoop продолжают работать, как и прежде: шифрование и дешифрование данных происходит для них прозрачно (также, как и для конечных пользователей). Любая попытка доступа к зашифрованным данным, осуществляемая неавторизованным сервисом или процессом, будет заблокирована.

ProtectFile for Linux делает возможным развертывание решений на базе Hadoop для организаций, соблюдающих жесткие организационные и регулятивные требования, такие, как HIPAA и PCI DSS. Это обеспечивается за счет 256-битного шифрования, расширенных возможностей управления ключами, а также комплексных возможностей по аудиту и подготовки отчетности.

Производительность и масштабируемость

В решении SafeNet Crypto Pack используются два подхода для шифрования: агентный и с использованием специализированного аппаратного аплайнса. Агенты шифрования используются для наиболее ресурсоемких с точки зрения сетевого взаимодействия криптопроцедур (например, для шифрования больших файлов). Этот подход используется в ProtectFile и ProtectV, где для выполнения криптографии используются процессорные мощности самого сервера, на котором установлен агент.

При втором подходе – для ProtectDB, ProtectApp и токенизации – также используется агент, который перехватывает все криптозапросы и пересылает их на выполнение в KeySecure-аплайнс.

Таким образом, например, для шифрования баз данных могут использоваться два подхода. Если база данных небольшая, например, "внутренняя" mySQL небольшого web-приложения, то она может быть зашифрована целиком с помощью ProtectFile. Если объемы БД – сотни гигабайт, то разумнее шифровать только от-

дельные чувствительные поля, например, с помощью ProtectDB.

Для обработки большого числа потоков KeySecure-аплайнс может быть организован в виде кластера со множеством узлов, в которых балансировка нагрузки осуществляется автоматически. Одновременно решается и вопрос надежности.

Для минимизации обращений к KeySecure-аплайнс агенты ProtectFile и ProtectV в момент загрузки забирают к себе ключи шифрования и политики из KeySecure.

Заключение

В настоящее время не только увеличивается количество утечек данных, но и характер этих утечек становится все более серьезным. Вопрос "произойдет ли утечка данных" уже не стоит. Он трансформировался в другой: "когда именно это случится?" Системы предотвращения утечек и мониторинг угроз позволяют лишь выявить факт инцидента, но не всегда позволяют его предотвратить. Средства защиты периметра имеют свои множественные уязвимости, эксплуатируемые внешними нарушителями, а также не позволяют защитить данные от «внутренних» угроз. В этом контексте только непосредственная защита данных сможет стать единственной преградой как от внутренних, так и от внешних угроз.

Игорь Афанасьев,
SafeNet Europe B.V. (подразделение Identity and Data Protection компании Gemalto)

Gemalto: представления не совпадают с реальностью

Апрель 2015 г. – Компания Gemalto опубликовала результаты Индекса Уверенности в Безопасности Данных за 2015 год (2015 Data Security Confidence Index, DSCI). Отчет выявил существенное расхождение между представлениями об эффективности периметра безопасности, которые сложились у лиц, принимающих решения в ИТ-сфере, и реальным положением дел. Результаты исследования свидетельствуют об увеличении уровня инвестиций в этот тип защиты данных, несмотря на экспоненциальный рост числа утечек данных.

Общее количество утечек данных в мире продолжает увеличиваться: согласно индексу критичности утечек Breach Level Index (BLI), составленному компанией Gemalto, только в 2014 г. произошло более 1500 утечек, что на 49% больше по сравнению с 2013 г. Количество похищенных записей данных возросло на 78%. Так, в 2014 г. было скомпрометировано более 1 млрд записей данных.

Несмотря на это, индекс уверенности DSCI указывает на то, что примерно 9 из 10 (87%) лиц, принимающих решения в сфере ИТ, считают периметр безопасности в своей корпоративной инфраструктуре эффективным с точки зрения защиты сети от неавторизованного доступа. Результаты исследования свидетельствуют о том, что ИТ-руководители продолжают увеличивать инвестиции в обеспечение периметра безопасности: 64% опрошенных намерены заняться этим в ближайшие 12 месяцев. Анализ самых последних утечек данных выявил любопытный факт: среднее количество записей данных, защищенных с помощью технологий шифрования, оказалось менее 8% от общего числа записей данных, скомпрометированных в результате этих утечек.

Тем не менее, треть опрошенных (33%) считает, что неавторизованные пользователи по-прежнему имеют возможность доступа к их корпоративной сети, и еще 34% не уверены в безопасности своих корпоративных данных в случае утечки. Фактически результаты индекса DSCI свидетельствуют о том, что в результате роста количества крупных утечек данных, 71% организаций скорректировали свои стратегии безопасности, но эти стратегии по-прежнему сосредоточены на обеспечении периметра безопасности. Ситуацию усугубляет тот факт, что 3/4 лиц, принимающих решения в ИТ-сфере (72%), указали, что инвестиции за последние пять лет только увеличились, хотя 30% признали, что за последние 12 месяцев в их компаниях по-прежнему происходили утечки данных.

Все это говорит о необходимости иного подхода к обеспечению безопасности. Хотя в результате нашумевших утечек данных примерно 7 из 10 (71%) организаций внесли изменения в свои стратегии обеспечения безопасности, примерно у 3 из 5 опрошенных (62%) не прибавилось уверенности по сравнению с прошлым годом в способности отраслевых игроков предоставить действующие решения для обнаружения и защиты от новых угроз безопасности.

В результате подобных атак 9 из 10 организаций (90%) испытывали негативные последствия для своей коммерческой деятельности, в том числе задержки с развитием продуктов или сервисов (31%), снижение продуктивности своих сотрудников (30%), снижение потребительской уверенности (28%) и определенное давление (24%). Все это указывает на весьма значительные негативные последствия утечек данных, которые негативным образом сказываются как на корпоративной репутации, так и на общих результатах деятельности компаний, а также на уверенности их заказчиков в данной отрасли.

"Следует сосредоточиться на защите пользовательских данных, и, в частности, рассмотреть возможность внедрения *стратегии "безопасной утечки"*, которая позволяет обеспечить защиту данных даже в том случае, если злоумышленник проник внутрь периметра безопасности. А это означает, что необходимо применить технологии безопасности непосредственно в отношении данных, в том числе за счет использования средств многофакторной аутентификации и шифрования данных, а также за счет внедрения инструментов безопасного управления ключами шифрования. При таком подходе даже в случае кражи данных, эти данные будут бесполезны", – говорит Сергей Кузнецов, Региональный директор Identity and Data Protection Gemalto.

NetApp: флеш-массивы AFF8000

Июнь 2015 г. – NetApp расширила линейку своих флеш-массивов СХД новыми моделями – All Flash FAS (AFF) 8000, разработанными для корпоративных клиентов. Сегодня на рынке доступны четыре модели AFF8000, которые можно заказать как автономные системы, а также как компонент конвергентной инфраструктуры FlexPod®.

«Линейка AFF8000 разработана для того, чтобы вывести высокопроизводительные СХД на базе флеш-памяти в категорию массовых», – сказал Ли Кэсуэлл *(Lee Caswell)*, вице-президент по маркетингу продуктов и решений NetApp».

Основные особенности новых систем

Серия AFF8000 обеспечивает полный набор функций флеш-технологий для предприятий: возможности встроенной защиты данных; поддержка нескольких протоколов, масштабируемая производительность и бесперебойное перемещение данных с флеш на диск и в облако. Решения AFF8000 также предлагают такие преимущества, как качество обслуживания, многопользовательская среда и интеграция приложений от NetApp, которые упрощают настройку баз данных SQL и Oracle, виртуальных серверов и рабочих нагрузок VDI, а также управление ими. Основные компоненты нового ПО:

- *FlashEssentials*. В системе All Flash FAS реализованы усовершенствования ПО, над которым работала опытная лаборатория передовых технологий NetApp. Среди новых разработок – оптимизированный под флеш-память путь передачи считываемых данных, сжатие данных при поступлении в СХД и дедупликация данных до их записи на диск. FlashEssentials является компонентом системы clustered Data ONTAP, на базе которой компания NetApp реализует свою стратегию управления данными будущего поколения — Data Fabric. Подход NetApp позволяет заказчикам определять способы управления данными, их защиты и перемещения с флеш-памяти на диск и в облако, а также полностью контролировать эти процессы;
- *NetApp OnCommand® Performance Manager 2.0*. Это новое ПО обеспечивает пользователям доступ к комплексной панели инструментов для автоматической оценки производительности и устранения неполадок, а в конечном итоге — для достижения оптимальных показателей системы;
- *Workload Wizard*. Мастер позволяет автоматически настраивать процесс установки Oracle и Microsoft SQL Server, упрощая настройку СХД и процедуру подключения хост-сервера.