Телекомунікаційні системи

УДК 621.394

С.А. Анейчик, В.М. Нозик

Государственное научное учреждение "Объединенный институт проблем информатики НАН Беларуси", Минск

СИСТЕМА СЕТЕВОГО ХРАНЕНИЯ ДАННЫХ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ СЕТИ

Системы сетевого хранения данных в последнее время становятся неотъемлемыми компонентами современных центров обработки данных. В докладе отражаются результаты построения сервиса сетевого хранения данных на основе архитектуры SAN с повышенным уровнем информационной безопасности в сети Национальной академии наук Беларуси.

Ключевые слова: *сеть BASNET, система сетевого хранения данных, архитектура SAN, протокол iSCSI, центр обработки данных, информационная безопасность, протокол IPSec.*

Введение

Совершенствование государственной системы научно-технической информации (ГСНТИ) предполагает модернизацию ее инфраструктуры, включая телекоммуникационную составляющую, расширение информационных сервисов, повышение их безопасности. Одним из инфраструктурных компонентов ГСНТИ является научно-исследовательская сеть Национальной академии наук Беларуси BASNET как наиболее развитая научная компьютерная сеть республики.

Пользователи корпоративных сетей все чаще сталкиваются с проблемой недостатка ресурсов для хранения данных на локальных станциях или серверах рабочих групп. Результатом этого является заметная потеря производительности сетевых аппаратно-программных средств [1]. Экстенсивный путь решения данной проблемы за счет простого наращивания дискового пространства на локальных серверах и серверах приложений без заметных затрат на модернизацию аппаратных платформ часто невозможен по ряду технических причин: всегда имеются ограничения на количество одновременно подключаемых устройств и типов интерфейсов, ограничены пропускные способности внутренних контроллеров обмена данными, имеются ограничения на уровне операционных систем (ОС) серверов и т. д. Повышение эффективности хранения данных возможно путем создания системы сетевого хранения данных (СХД) в виде архитектуры SAN (Storage Area Network), использующей IP-сети в качестве инфраструктуры доступа к данным. СХД в комплексе с системой резервного копирования (использующих, как правило, единые решения) становятся де-факто обязательными компонентами современного центра обработки данных (ЦОД) [2, 3].

Создаваемая СХД построена на основе открытого программного обеспечения (ПО) OpenFiler, для доступа к ресурсам хранения используется протокол iSCSI, при этом подключенные удаленные устройства распознаются ОС как локальные [4, 5].

Результаты исследований

В Республике Беларусь (РБ) к поставщикам интернет-услуг приказом Оперативно-аналитического центра при Президенте Республики Беларусь (ОАЦ) от 02.08.2010 № 60 определен перечень требований по обеспечению защиты информации. Поскольку услуга хранения данных предоставляется в виде IaaS (инфраструктура как сервис), в создаваемой СХД предусмотрен комплекс мер информационной безопасности – как надежная авторизация и развитая IP-фильтрация, так и защищенный транспорт данных между клиентскими рабочими станциями и удаленным сервером-хранилищем, поскольку информация может передаваться через не доверенные сети. При этом используемые провайдером средства криптографической защиты транспорта данных в канале связи (КС) должны быть сертифицированы в РБ. Популярные iSCSI-инициаторы, в частности, Microsoft iSCSI Software Initiator for WinXP, имеют встроенные средства организации IPSec/vpn-туннеля, но они формально не могут быть использованы для защиты КС по указанной причине.

Требованиям приказа ОАЦ отвечает, например, программный комплекс «Средство криптографической защиты сетевого протокола IP BelIPSec», разработанный ЗАО «БелХард Групп», который может быть применен для защиты данных в КС между кли-

ентами и сервером СХД. Комплекс обеспечивает защиту данных на сетевом уровне методом шифрования IP-пакетов и автоматически обеспечивает защиту всех протоколов, лежащих на более высоких уровнях, однако работает только под управлением ОС Windows 98, 2000, 2003, XP. Средство криптографической защиты информации (СКЗИ) BelIPSec реализует функции криптографической защиты информации в КС в соответствии со стандартами РБ: шифрование по ГОСТ 28147-89; ЭЦП в соответствии с СТБ 1176.2-99; функцию хэширования в соответствии с СТБ 1176.1-99; процедуру выработки псевдослучайных данных в соответствии с РД РБ 07040.1202-2003 «Банковские технологии» и др. Шифрование данных в КС осуществляется на сеансовых ключах, вырабатываемых при установлении защищенного соединения.

В СКЗИ BelIPSec определены два протокола защиты передаваемых данных – Authentication Header (AH) и Encapsulated Security Payload (ESP). Протокол AH гарантирует целостность и аутентичность данных путем добавления в IP-пакет дайджеста пакета, вычисляемого на основе его содержимого и общего секретного ключа. Протокол AH защищает весь исходный пакет, включая заголовок IP. Для шифрования передаваемых данных используется протокол ESP, криптующий содержимое пакета (все данные, начиная с заголовков транспортного уровня). ESP также добавляет в пакет дайджест, обеспечивающий целостность данных.

Поскольку вероятность прямой сетевой атаки на серверы хранения несравненно более высока, нежели перехват данных в КС, применительно к СХД, на наш взгляд, достаточно использовать режим AH, поскольку при передаче по КС важно защитить данные, в основном, от несанкционированной модификации. Вопрос обеспечения конфиденциальности информации при транспорте по КС хотя и важен, но будет достигаться за счет значительной потери производительности клиента и сервера. Как показали эксперименты, режим ESP достаточно ресурсоемкий и приводит к заметному снижению эффективности работы СХД.

В СКЗИ BelIPSec реализована поддержка двух режимов функционирования IPSec: транспортный и туннельный (с ограничениями). В транспортном режиме пакет, соответствующий фильтру IPSec, защищается при помощи протокола AH или ESP и пересылается на адрес, указанный в заголовке IP. В туннельном режиме к пакету добавляется новый заголовок IP, где в качестве IP-адреса отправителя указывается адрес данного компьютера, а в качестве адреса получателя – адрес, указанный в правиле; это вторая конечная точка туннеля. Затем пакет защищается при помощи AH или ESP. Использование транспортного режима позволяет защищать коммуникации между двумя компьютерами (схема «точка-точка»).

В реальных условиях режим IPSec-транспорта («точка-точка») не обеспечивает доступ к произвольному внутреннему хосту внутри периметра защищаемой сети. Это ограничение проявляется в том, что сервер СХД должен быть развернут на том же сервере, на котором запущен IPSec-сервер. Но такая сетевая конфигурация в реальной ситуации невозможна, так как BelIPSec работает под ОС Windows, а СХД – под rPath Linux. Проблема, однако, разрешима – программный комплекс СКЗИ BelIPSec реализует частичный вариант туннельного режима – «точка-шлюз». Использование такого режима является реальной возможностью обеспечения безопасного доступа к СХД через не доверенную или условно доверенную сеть, поскольку позволяет повысить гибкость и эффективность схемы обмена данными в неоднородных сетевых конфигурациях: IPSec-шлюз развертывается на Windows-платформе, к отдельному интерфейсу подключается сервер СХД под ОС Linux.

В данном режиме IPSec-туннель устанавливается от компьютера клиента до IPSec-шлюза, ассоциация безопасности задается от компьютера клиента до сервера СХД. На IPSec-шлюзе пакеты расшифровываются и перенаправляются на шлюзовый интерфейс, к которому подключена внутренняя сеть, далее с него в нешифрованном виде по внутренней доверенной сети они передаются к серверу СХД.

Необходимо иметь в виду, что версия BelIPSec, работающая, к сожалению, только на 32-битных платформах Windows, по данным разработчиков, обеспечивает приемлемую производительность при потоке 100 Мбит/с и следующих минимальных аппаратных конфигурациях: сервер – CPU Intel Pentium 4/3000 МГц/RAM 1024 Мбайт, рабочая станция – CPU Intel Pentium 4/1000 МГц/RAM 512 Мбайт. Для эффективного использования iSCSI необходима минимальная скорость КС 1 Гбит/с. Понятно, что СКЗИ будет заметно ограничивать скорость работы с удаленным iSCSI-диском. Для оценки работоспособности системы были проведены испытания и выполнены замеры максимальной скорости доступа к СХД без использования и с использованием BelIPSec.

Испытания проводились в следующих условиях: коммутируемая сеть 1 Гбит/с, коммутатор D-Link DGS-1024D/GE; в качестве инструмента измерений использовался файл-менеджер TC 7.56a (32-bit), антивирус KAV 6.0 на IPSec-шлюзе (Intel Pentium E5200/2500 МГц, RAM 2037 Мбайт/Win XP SP3) и клиентском компьютере-ноутбуке (Intel Pentium/1860 МГц, RAM 512 Мбайт/Win XP Tablet PC Edition SP2). Используемый режим аутентификации BelIPSec: протокол формирования общего ключа шифрования данных с аутентификацией. Используемый iSCSI-клиент на стороне рабочей станции – Microsoft iSCSI Software Initiator for WinXP version 2.08 (build3825-x86fre).

Результаты сравнительных замеров максимальной скорости доступа к СХД без использования и с использованием BelIPSec показали, что производительность используемой версии СКЗИ на данных аппаратных конфигурациях действительно не слишком высока (100-150 Мбит/с), использование режима АН примерно в 4-5 раз ухудшает скорость обмена данными, производительность же комплекса в наиболее «тяжелом» режиме полного криптования пакетов (ESP) неприемлема, хотя протокол iSCSI при этом работает стабильно. Пропускная способность локальной сети в данном случае не является сколько-нибудь важным фактором ограничения скорости файловых операций. Узким местом является малый объем оперативной памяти, низкая производительность дисковой системы и процессора рабочей станции, на которой развернуто ПО криптоклиента. Лучшие показатели могут быть достигнуты при использовании более современных конфигураций аппаратных платформ криптосервера и криптоклиента.

Тем не менее, результаты экспериментов показали общую работоспособность такой схемы защищенного взаимодействия с СХД, но при условии использования режима АН IPSec.

Следует добавить, что дополнительно к IPSec-протоколу, работающему на сетевом уровне, на прикладном уровне клиент может самостоятельно применять допустимые встроенные возможности используемых платформ и внешние программные средства для шифрования своих данных (MS EFS, TrueCrypt и т.п.).

Создание комплекса сетевого хранения данных с повышенной информационной безопасностью обеспечит:

- снижение влияния факторов, вызывающих потерю производительности как результата неорганизованного хранения информации либо недостатка ресурсов для ее хранения на локальных станциях или серверах рабочих групп;
- минимизацию нагрузки на серверы приложений и файловые серверы рабочих групп и организаций;
- уменьшение времени задержки доступа к данным;
- повышение общей надежности и безопасности хранения данных;
- повышение целостности и аутентичности пользовательских данных при обмене по КС между клиентскими рабочими станциями и сервером СХД.

Вывод

Внедрение СХД – одно из наиболее перспективных направлений развития корпоративных информационных систем. В настоящее время, когда вопросы информационной безопасности становятся предельно актуальными, предоставление подобного защищенного сервиса в академсети будет способствовать ускоренному накоплению и развитию национального научно-технического контента, содействовать созданию в республике условий для развития новых направлений исследований и разработок, а также расширению международного сотрудничества с полной доступностью научного потенциала ученых Беларуси для всего мирового информационного пространства.

Список литературы

1. Гринфилд, Д. Управление производительностью распределенных приложений / Д. Гринфилд // Сети и системы связи, 2008. – № 9(171). – С. 42-45.

2. Бирс, К.Т. Проектирование ЦОДа / К.Т. Бирс, Б. Фишер // Сети и системы связи. – 2007. – № 10(158). – С. 36-42.

3. Мартынюк, А.В. Проектирование и создание ЦОД / А.В. Мартынюк // Сети и системы связи, 2007. – № 11(159). – С. 42-49.

4. Фарли, М. Сети хранения данных / М. Фарли. – М.: Лори, 2004. – 576 с.

5. Анейчик, С.А., Нозик, В.М. Опыт построения телекоммуникационного узла с повышенной отказоустойчивостью // Ракетно-космическая техника. Информационные системы и технологии. Научные труды в 2 т. – Т. 2. – Юбилейный : НИИ КС, 2012. - С. 180-191.

Поступила в редколлегию 11.07.2013

Рецензент: д-р техн. наук, проф. С.М. Порошин, Национальный технический университет «ХПИ», Харьков.

СИСТЕМА МЕРЕЖЕВОГО ЗБЕРІГАННЯ ДАНИХ НАУКОВО-ДОСЛІДНОЇ МЕРЕЖІ

С.А. Анейчик, В.М. Нозік

Системи мережевого зберігання даних останнім часом стають невід'ємними компонентами сучасних центрів обробки даних. У доповіді відбиваються результати побудови сервісу мережевого зберігання даних на основі архітектури SAN з підвищеним рівнем інформаційної безпеки в мережі Національної академії наук Білорусі.

Ключові слова: *мережа BASNET, система мережевого зберігання даних, архітектура SAN, протокол iSCSI, центр обробки даних, інформаційна безпека, протокол IPSec.*

SYSTEM OF NETWORK STORAGE OF DATA OF RESEARCH NETWORK

S.A. Aneychik, V.M. Nozik

The systems of network data storage become the inalienable components of modern data processing centers. In a lecture the results of the service design for network data storage are reflected. The service is developed on the basis of SAN architecture with enhanced information security level in the network of the National academy of sciences of Byelorussia.

Keywords: *network of BASNET, system of network data storage, SAN architecture, iSCSI-protocol, data processing center, information security, IPSec-protocol.*