Высокопроизводительное сертифицированное решение для защиты ЦОД

Обзор требований, предъявляемых к системам сетевой защиты ЦОД, и представление 10Gb решения для сетевой защиты компании ЗАО "С-Терра СиЭсПи", анонсированного осенью 2012 г.



Владимир Воротников – руководитель отдела перспективных исследований и проектов, ЗАО "С-Терра СиЭсПи".

Введение

Существенный рост количества информации, передаваемой по сети, желание получать доступ к информации и пользоваться привычными IT-сервисами из любой точки мира неизбежно ведут к консолидации хранимых данных в СХД, а всех IT-ресурсов – в ЦОДах. Этот тренд действительно выводит качество предоставляемых пользователям сервисов на новый уровень. Однако не стоит забывать и о чрезвычайной важности обеспечения безопасности таких решений. Конфиденциальные данные не должны передаваться по сетям общего доступа в открытом виде. Также следует понимать, что, если в прошлом десятилетии мы говорили о гигабитных каналах, то сейчас речь идет уже, по меньшей мере, о десяти гигабитах и более.

Требования к защите доступа к ЦОДам

К решениям, защищающим взаимодействие между ЦОДами и доступ к ЦОДам, предъявляются особые качественные и эксплуатационные требования:

- ***высокий уровень безопасности***. Если данное требование не выполняется – то зачем вообще нужна такая система защиты?
- ***высокая производительность решения.*** Решение должно быть не просто "высокопроизводительным" на неком синтетическом оптимальном трафике, но и обеспечивать требуемое качество сервиса с реальным трафиком, который может включать в себя пакеты разной длины, разного приоритета, IP-телефонию, видеоконференцсвязь и т.д. Задача шлюза безопасности (помимо непосредственно защиты) – быть прозрачным для конечных IT-сервисов, не внося избыточную задержку и потери пакетов. Только в этом случае будет обеспечено высокое качество сервиса;
- ***высокий уровень масштабируемости.*** Решение должно легко подстраиваться под текущие требования бизнеса. Рост ЦОДа, появление новых филиалов, увеличение количества потребителей сервиса – в любом подобном случае желательно избежать полной замены системы (в том числе, и по соображениям экономичности), то есть необходимо плавное наращивание мощностей системы;
- ***отказоустойчивость.*** Система должна выполнять свои функции при любых условиях, даже если часть ее вышла из строя;
- ***высокие эксплуатационные характеристики.*** Предсказуемость поведения сети, хорошая документированность решения, простота поиска ошибок – все это важно для непрерывного качественного функционирования системы и снижения издержек на эксплуатацию;
- ***обеспечение высокого уровня сервиса и прозрачность для конечных приложений.*** Безопасность – это сервис для IT, а не наоборот. Цель решения – обеспечить высокий уровень защиты, при этом не внося ухудшений в качество предоставляемого сервиса;
- ***возможность централизованного управления и мониторинга системы.*** Это позволяет снизить эксплуатационные расходы, обнаруживать проблемы на ранней стадии и легко получать полную информацию о состоянии системы;
- ***соответствие требованиям регулятора.*** Выполнение этого требования гарантирует соответствие шифровальных средств требованиям российских стандартов, а также функционирование системы в рамках законодательства Российской Федерации.

Несмотря на достаточно внушительный список требований, построить такое решение вполне возможно. На основе проведенных исследований и опыта эксплуатации, компанией "С-Терра" были разработаны сценарии защиты каналов между ЦОДами.

На рис. 1 изображена концептуальная схема защиты 10Gb-канала между ЦОДами. Топология изображена так, чтобы максимально просто иллюстрировать архитектуру решения по защите канала. В зависимости от потребностей конечного заказчика, схема может быть существенно изменена: маршрутизаторы в каждом из ЦОДов могут физически представлять собой одно устройство (в т.ч. коммутатор L3), а для обеспечения отказоустойчивости все устройства и каналы могут быть продублированы.

Работа схемы основана на следующем принципе: маршрутизатор распределяет



Рис. 1. Защита канала 10Gb на уровне L3.



Рис. 2. Защита канала 10Gb на уровне L2.

трафик на несколько шлюзов безопасности CSP VPN Gate, которые шифруют его.

Существует отдельный класс задач, для которых связь между ЦОДами удобнее обеспечивать на канальном уровне (L2). В качестве классического примера можно привести физическую миграцию ЦОДов. При таком сценарии L2-решение просто незаменимо. Можно объединить старый и новый ЦОДы L2-каналом и постепенно, в часы наименьшей нагрузки, мигрировать отдельные серверы и виртуальные машины, не меняя при этом логическую структуру своей сети.

На рис. 2 изображена концептуальная схема защиты 10Gb-канала между ЦОДами на уровне L2. Логика работы аналогична первой схеме, с той лишь разницей, что, если в L3-решении для балансировки и отказоустойчивости применяется технология GRE и протокол динамической маршрутизации, то на L2 уровне работает технология EtherChannel.

Представленные решения в полной мере соответствуют требованиям, которые были приведены выше:

- ***высокий уровень безопасности.*** Решение является безопасным не только с позиции криптографии (что обеспечивается использованием алгоритмов шифрования и контроля целостности ГОСТ 28147-89, ГОСТ Р 34.11-94), но и с позиции сетевой архитектуры: технология IPSec определена в RFC и прошла многолетнюю проверку мировым IT-сообществом;
- ***высокая производительность решения.*** Производительность решения зависит от производительности отдельного шифрующего шлюза и их общего количества. Может ли по такой технологии быть закрыт, например, 10Gb-канал? Ответ очевиден: да, конечно;
- ***масштабируемость решения.*** Зачастую, 10Gb-каналы не бывают загружены полностью. В таком случае данная технология позволяет внедрять необходимое количество шлюзов безопасности для существующего объема реально используемого трафика, а в дальнейшем увеличивать количество этих шлюзов по мере необходимости;
- ***отказоустойчивость.*** Отказоустойчивость схемы достигается при помощи использования технологии GRE и протокола динамической маршрутизации на балансирующем устройстве. Скорость отработки отказа зависит от конфигурации. На схеме резервируются только шлюзы безопасности, но при необходимости возможно резервирование любого компонента решения, как балансирующего устройства, так и канала связи (провайдера);
- ***высокие эксплуатационные характеристики.*** Все технологии, лежащие в основе этого решения, стандартизованы в RFC и/или ГОСТ. Это позволяет получить предсказуемое поведение сети, существенно уменьшить затраты на обучение персонала, ускорить нахождение и разрешение проблем, застраховать от ошибок в дизайне, т.к. аналогичные архитектуры решения предлагаются к использованию всеми крупнейшими сетевыми вендорами.

  Кроме того, все рассмотренные схемы позволяют обслуживать (например, обновлять версию ПО) шлюзы безопасности компании "С-Терра" без ухудшения качества сервиса: отдельный шлюз можно плавно вывести из процесса обработки трафика, распределив нагрузку между другими, и точно так же, плавно, ввести в строй после обновления;
- ***обеспечение высокого уровня сервиса.*** В продуктах компании "С-Терра" есть возможность корректной обработки приоритетного трафика. Это позволяет для критичных к качеству канала сервисов (например, для IP-телефонии и ВКС) обеспечить минимальный уровень задержек и джиттера, даже в том случае, если шлюз перегружен;
- ***возможность централизованного управления и мониторинга системы.*** Централизованное управление всей системой реализуется при помощи Cisco Security Manager. В случае необходимости управления только шлюзами безопасности S-terra может использоваться система управления "С-Терра КП". Для мониторинга подойдет любая привычная эксплуатирующему инженеру система: все компоненты решения поддерживают работу по стандартам syslog и SNMP;
- ***соответствие требованиям регулятора.*** Продукты компании "С-Терра", на которых основано решение, сертифицированы ФСБ России и ФСТЭК России, в соответствии с требованиями законодательства РФ к шифровальным (криптографическим) средствам.

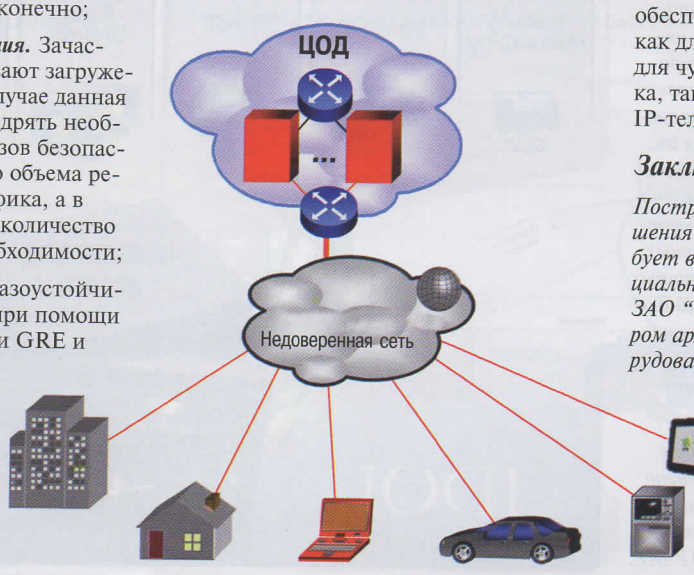


Рис. 3. Защита массового доступа в ЦОД.

Таким образом, все требования, выполнение которых необходимо для надежной защиты каналов взаимодействия между ЦОДами, выполняются.

На рис. 3 изображена концептуальная схема защиты решения для массового доступа к ресурсам ЦОД. Данная схема, как и две другие, описанные выше, обеспечивает отказоустойчивость и хорошую масштабируемость: при увеличении нагрузки на шлюзы, соответственно, увеличивается их количество. В случае выхода из строя одного из шлюзов, нагрузка равномерно распределится между оставшимися. Для обеспечения такой балансировки нагрузки используется технология RRI.

Для доступа к ресурсам ЦОД используются как шлюзы безопасности CSP VPN Gate, так и мобильный клиент CSP VPN Client, а также устройство доверенной загрузки СПДС "ПОСТ". Благодаря использованию среды построения доверенного сеанса (СПДС), защищенный доступ пользователя к ресурсам ЦОД возможен практически с любого ноутбука или ПК. При этом используется строгая двухфакторная аутентификация пользователя, криптографическая защита трафика и данных, обеспечивается доверенная загрузка целостной информационной среды и изолированное сетевое соединение с сервером приложений, запуск какого-либо непредусмотренного ПО совершенно исключен.

Защита ЦОДа – критически важная задача, и к выбору решения следует подойти ответственно. Следует принимать во внимание не синтетическую, а реальную производительность. Кроме того, возможности шлюза безопасности должны обеспечить требуемый уровень сервиса, как для передачи обычных данных, так и для чувствительного к задержкам трафика, такого, как видеоконференцсвязь и IP-телефония.

Заключение

Построение высокопроизводительного решения – непростая задача, которая требует высокой квалификации, опыта и специальных навыков. Специалисты компании ЗАО "С-Терра СиЭсПи" помогут с выбором архитектуры решения и моделей оборудования, а также окажут необходимую поддержку для успешной, своевременной и беспроблемной реализации проекта создания защищенных высокопроизводительных каналов для взаимодействия между ЦОДами и доступа к ЦОДам.

Владимир Воротников,
компания ЗАО "С-Терра СиЭсПи"