Защита ЦОДов:
простые и эффективные решения сложных проблем

Владимир ВОРОТНИКОВ,
руководитель отдела перспективных исследований и проектов, компания «С-Терра СиЭсПи»

В современном мире ЦОДы становятся неотъемлемой частью бизнеса, повышая его эффективность и выводя качество сервиса на новый уровень. Однако с их развитием обостряется проблема защиты информации: неавторизованный доступ или порча информации могут стать серьезной проблемой для любой компании. Для защиты ЦОДов требуется отказоустойчивое и хорошо масштабируемое решение, которое не станет узким местом в ИТ-инфраструктуре.

Сегодня никого уже не удивить 10Gb-каналами, которыми связаны между собой ЦОДы и по которым осуществляется массовый доступ к ним. Создание доверенного канала и шифрование больших объемов трафика требуют применения высокопроизводительного решения. Причем такое решение должно не только показывать высокую производительность при работе с неким «синтетическим» оптимальным трафиком, но и обеспечивать требуемое качество сервиса, имея дело с реальным трафиком, который может включать в себя пакеты разной длины, разного приоритета, сервисы IP-телефонии, видеоконференцсвязи и многое другое. Помимо обеспечения непосредственно защиты шлюз безопасности должен быть прозрачным для потребительских ИТ-сервисов, не вносить избыточную задержку и потери пакетов. В противном случае высокого качества сервиса ожидать не приходится.

Обеспечение необходимого качества сервиса включает в себя и быструю автоматическую обработку сообщений об отказах, в какой бы части сети ни произошла поломка. Очевидно, что шлюзы безопасности также должны обеспечивать возможность построения отказоустойчивого решения как для защиты связи между ЦОДами, так и для массового доступа к ресурсам ЦОДа.

Кроме того, существуют задачи и сегменты сети, для которых работа только на уровне L3 не подходит или крайне неудобна: при использовании протоколов, не входящих в стек TCP/IP; при необходимости передачи меток VLAN и MPLS; при задаче постепенной физической миграции ИТ-инфраструктуры. Для них гораздо удобнее использовать шифрование трафика второго уровня. Это можно сделать при помощи решения компании «С-Терра СиЭсПи» – L2VPN. Принцип его работы прост: шлюз безопасности CSP VPN Gate перехватывает фреймы на уровне L2 и инкапсулирует их в пакеты UDP, которые, в свою очередь, отправляются по защищенному туннелю.

На основе проведенных исследований и опыта эксплуатации компанией «С-Терра СиЭсПи» были разработаны сценарии защиты каналов между ЦОДами.

На рис. 1 изображена концептуальная схема защиты 10Gb-канала между ЦОДами, которая иллюстрирует архитектуру решения. В зависимости от потребностей конечного заказчика схема может быть изменена: маршрутизаторы в каждом из ЦОДов могут физически представлять собой одно устройство (в том числе коммутатор L3), а

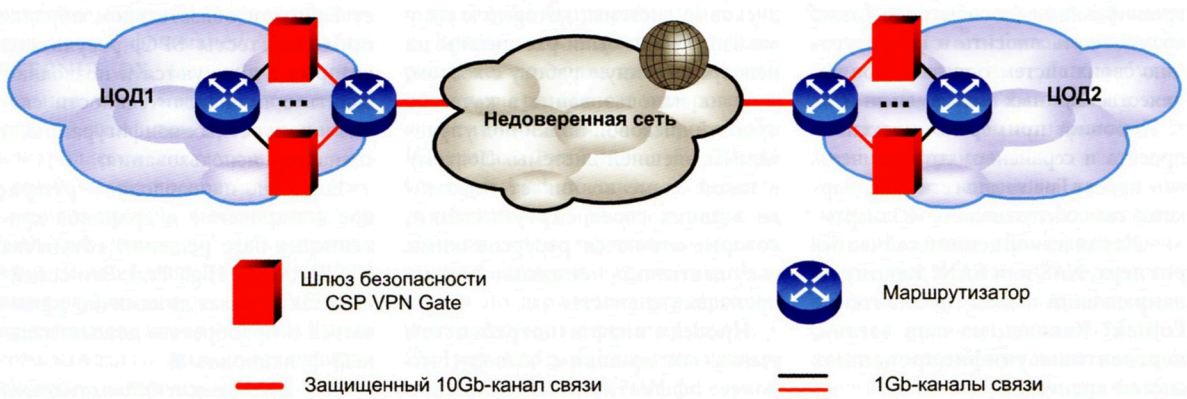

Рис. 1. Защита канала 10Gb на уровне L3

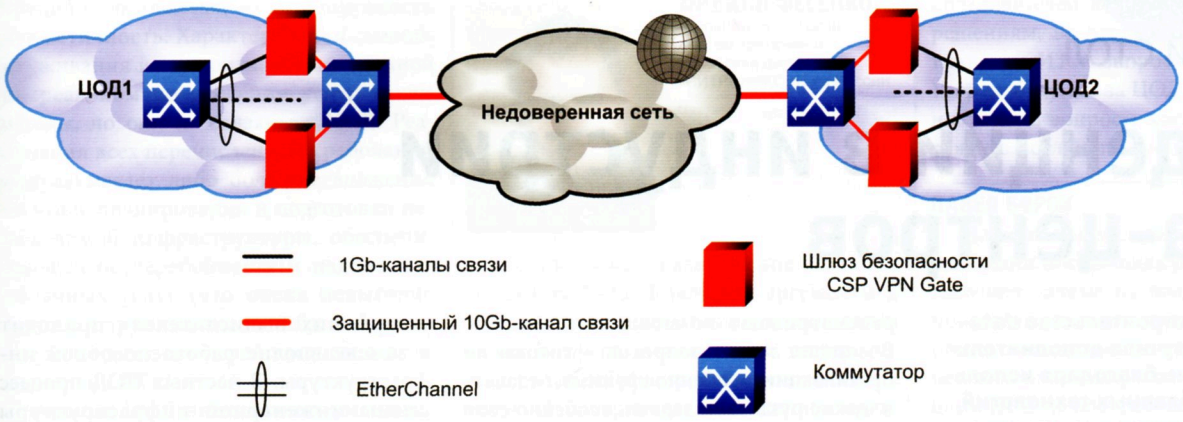

Рис. 2. Защита канала 10Gb на уровне L2

для обеспечения отказоустойчивости все устройства и каналы можно продублировать.

Принцип работы следующий: маршрутизатор распределяет трафик на несколько шлюзов безопасности CSP VPN Gate, которые шифруют его. Количество шлюзов безопасности зависит от их производительности и объема трафика. Отказоустойчивость при этом обеспечивается балансирующим устройством, которое в случае отказа шлюза безопасности перестает передавать на него трафик, распределяя нагрузку между оставшимися шлюзами. Кроме того, схема обладает высоким уронем масштабируемости. Не секрет, что некоторые 10Gb-каналы никогда полностью не загружены. В таком случае можно внедрить то количество шлюзов безопасности, которое соответствует реальному объему трафика, а в дальнейшем, по мере необходимости, увеличивать количество шлюзов.

Как уже было сказано, иногда удобнее обеспечивать связь не на уровне L3, а на уровне L2. Концептуальная схема защиты 10Gb-канала между ЦОДами на уровне L2 приведена на рис. 2. Логика работы аналогична предыдущей схеме, разница лишь в том, что если в L3-решении для балансировки применяются технология GRE (Generic Routing Encapsulation) и протокол *динамической маршрутизации, то* на L2-уровне работает технология EtherChannel.

На рис. 3 изображена концептуальная схема защиты при массовом доступе к ресурсам ЦОД. Данная схема, как и две другие, обеспечивает отказоустойчивость и хорошую масштабируемость: при возрастании нагрузки на шлюзы можно увеличить их количество. В случае выхода из строя одного из шлюзов нагрузка равномерно распределится между оставшимися. Для этого в данной схеме используется технология RRI (Reverse Route Injection).

Для доступа к ресурсам ЦОДа используются шлюзы безопасности CSP VPN Gate, мобильный клиент CSP VPN Client, а также продукт «ПОСТ», обеспечивающий построение среды доверенного сеанса связи. Используя продукт «ПОСТ», защищенный доступ пользователя к ресурсам ЦОДа возможен практически с любого ноутбука или ПК. При этом применяется 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.

Все рассмотренные схемы позволяют обслуживать шлюзы безопасности компании «С-Терра СиЭсПи» (например, обновлять версию ПО) 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.

Защита ЦОДа – критически важная задача, и к выбору решения надо подходить ответственно. Следует смотреть не на «синтетическую», а на реальную его производительность. Кроме того, возможности шлюза безопасности должны обеспечить требуемый уровень сервиса и для передачи обычных данных, и для чувствительных к задержкам трафика, таких как видеоконференцсвязь и IP-телефония. ■

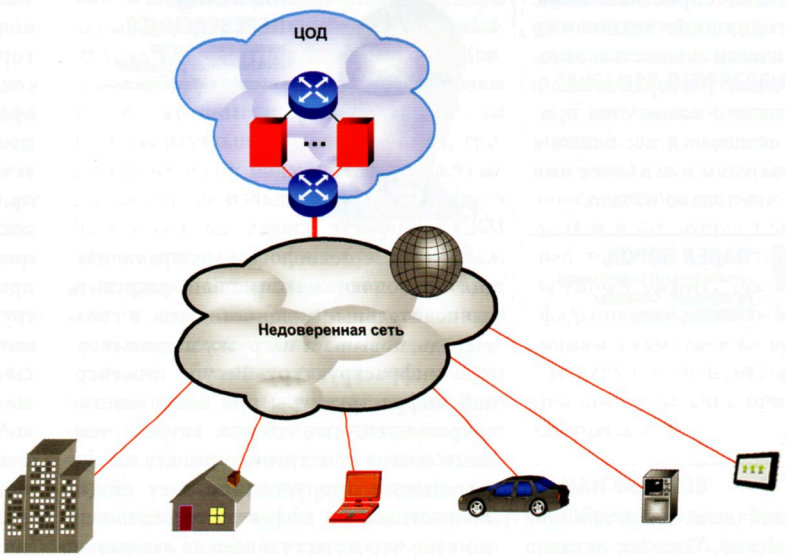

Рис. 3. Обеспечение защищенного массового доступа к ЦОДу