Защита межсетевого взаимодействия уровня "ЦОД – ЦОД"

Александр Веселов, *ведущий инженер ЗАО "С-Терра СиЭсПи"*

По прогнозам Cisco, к 2017 г. общий объем мирового трафика в ЦОД увеличится втрое и составит 7,7 зеттабайт. Причем около 7% трафика будет генерироваться при обеспечении связи между ЦОД (главным образом при репликации данных).

Задача по защите высокопроизводительных каналов связи с каждым годом становится все более востребованной и актуальной. На данный момент большинство российских ЦОД сосредоточено в пределах столицы, в то время как для создания катастрофоустойчивых информационных систем ЦОД должны быть географически разнесены, следовательно, трафик между ними потребует дополнительной защиты.

Производительность

Обеспечение конфиденциальности и целостности трафика при передаче между ЦОД осложняется не только их географической удаленностью, но и ресурсоемкостью процесса шифрования, увеличением задержек и внесением дополнительной информации в пакет (overhead). Для данных, подлежащих обязательной защите согласно российскому законодательству, необходимо применять шифрование по ГОСТ-алгоритмам. В то же время производительность современных отечественных VPN-шлюзов на топовых аппаратных платформах составляет порядка 500–900 Мбит/с при передаче IMIX-трафика. Более того, зачастую речь идет о маркетинговых показателях, представляющих собой пиковые значения, которые достигаются при шифровании пакетов большого размера.

Кроме того, все ЦОД имеют свои особенности, у них различная пропускная способность и MTU каналов связи, различный трафик. Поэтому наилучшим способом при выборе подходящего решения является организация тестовых испытаний на площадке заказчика.

Отказоустойчивость и масштабируемость

Кроме производительности, важными и неотъемлемыми свойствами решения по обеспечению защиты трафика ЦОД являются отказоустойчивость и масштабируемость. Оптимальный вариант в этом случае – модульная архитектура, применение которой позволяет одновременно решать эти задачи.

При этом необходимо обратить внимание на распределение нагрузки между модулями. Входной сетевой поток нужно разобрать на несколько более мелких, а на другой стороне агрегировать их. К балансировке есть два основных подхода:

1. Выделение отдельного устройства. Традиционное решение – распределение трафика между шлюзами на L3-устройстве с помощью маршрутизации (рис. 1). В этом случае маршрутизаторы в каждом ЦОД могут представлять собой одно физическое устройство. Поддерживается резервирование всех компонентов системы: каналов связи, шлюзов безопасности, маршрутизаторов.

Альтернативный вариант – распределение трафика между шлюзами, работающими в режиме L2, на коммутаторе с помощью агрегирования EtherChannel (рис. 2). Решение на канальном уровне (L2) позволяет охватить достаточно широкий класс задач, которые на L3 решить значительно сложнее, например миграция сетевой инфраструктуры без изменения адресации. Также существенным плюсом решения является низкая стоимость балансировщика.

2. Использование встроенного механизма. Примером такой архитектуры может служить платформа CrossBeam с интегрированным балансировщиком нагрузки. Шлюз безопасности CSP VPN Gate устанавливается на модули приложений (вычислительные "лезвия"), а модуль управления распределяет трафик между ними в зависимости от их текущей загрузки. Платформа предоставляет широкие возможности резервирования управляющих модулей, модулей приложений, сетевых модулей и интерфейсов, каналов связи и т.д.

Используя решения компании "С-Терра СиЭсПи", можно реализовать оба варианта.

Централизованные управление и мониторинг

Важным аспектом любого решения по безопасности, в том числе для ЦОД, является возможность централизованного управления и мониторинга. Шлюзами безопасности CSP VPN Gate можно управлять через Cisco Security Manager и "С-Терра КП". "С-Терра КП" – собственная разработка, которая позволяет осуществлять более тонкую настройку шлюзов.

Таким образом, проектируя распределенную информационную систему, необходимо предусмотреть систему комплексной безопасности ЦОД, учитывая при этом перечисленные в статье аспекты. Только тогда работа ЦОД будет эффективной, а защита данных – надежной и легитимной.

Применение шлюза безопасности CSP VPN Gate 7000 версии 4,1 (шифрование ГОСТ 28147-89 с имитозащитой) позволило при шифровании iSCSI-трафика между ЦОД на TCP (MTU9K) достичь производительности 7 Гбит/с, на UDP512 – 1,4 Гбит/с. А суммарная производительность ГОСТ-шифрования на платформе CrossBeam X80S составила более 10 Гбит/с смешанного трафика.

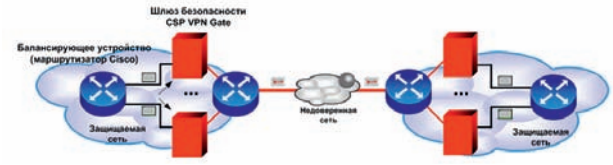

Рис. 1. Защита 10G-канала на L3

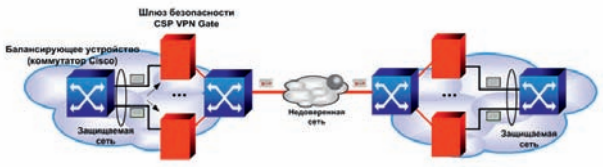

Рис. 2. Защита 10G-канала на L2