цепочка рассуждений вида "Нам нужен VPN на 200 Мбит/с → производитель указал, что устройство может построить как раз такой VPN → берем!" очень опасна. Интернет-сообществом были предприняты попытки разработать более приближенную к реальности модель распределения трафика для подобных тестов (семейство моделей IMIX), и часто производителями отдельно указывается пропускная способность именно для такого трафика, но кто даст гарантию, что она адекватно отражает конкретную сеть? Поэтому необходимо только обследование, других вариантов не существует.

В-третьих, имеющиеся каналы связи часто эксплуатируются с уровнем загрузки, близким к максимальному. Криптообработка всегда добавляет определенные накладные расходы из служебных заголовков и издержек алгоритмов шифрования к каждому пакету, следовательно, шифрованный трафик требует большей полосы пропускания, и чем средний размер пакета меньше, тем доля этих расходов будет выше, вплоть до превышения полезного трафика в несколько раз. Если планируется передача данных, чувствительных к задержкам/потерям (IP-телефония, видеоконференцсвязь), то необходимо выбрать устройство, поддерживающее функционал Quality of Service (QoS), позволяющее определить чувствительный трафик и обеспечить его приоритетную обработку. В противном случае велика вероятность значительного снижения качества звонков. В случае экстремально узких каналов может не справиться и с помощью QoS, и единственным решением тогда будет расширение канала. Согласитесь, об этом лучше узнать заранее, а не постфактум, уже потратив значительное количество времени и денег на закупку и внедрение решения.

В-четвертых, необходимо заранее продумать архитектуру сети. Какова будет топология виртуальных туннелей? Будет ли это "звезда", полносвязная или какой-то гибридный вариант? У каждого из них есть свои преимущества и недостатки, универсального варианта нет, и выбрать оптимальную топологию для конкретной сети возможно только с учетом маршрутов трафика и пропускной способности каналов. Какие сетевые сегменты планируется связать и каким именно образом? Где-то, возможно, потребуется двойной эшелон защиты, когда в сети необходимо организовать отдельный сегмент с наиболее чувствительной информацией (финансы, R&D-отделы). Чтобы грамотно спроектировать защищенную сеть, жизненно важно иметь максимально полную информацию о данных и маршрутах их передачи, что в очередной раз приводит нас к необходимости проведения тщательного обследования, документирования и анализа существующей сети, выполненных профессионалами.

Наконец, рекомендуется выбирать производителя аппаратного обеспечения и реализующего проект внедрения интегратора, гарантирующих поддержку и после внедрения. Оборудование для построения виртуальных защищенных сетей требует специализированных знаний оператора как для начальной настройки, так и (особенно!) для устранения неисправностей. Согласитесь, крайне неприятно остаться один на один с вышедшим из строя неведомым, но жизненно важным для бизнеса оборудованием. Тем более что редкая сеть остается статичной значительное время. Как правило, внедренную систему виртуальных защищенных сетей требуется периодически донастраивать – добавлять и удалять узлы, вносить изменения в политики приоритезации трафика, шифрования и межсетевого экранирования. Рекомендуется убедиться, что для оказания подобных услуг есть надежный партнер.

Заключение

Задача построения виртуальной защищенной сети требует комплексного подхода, учета тонкостей российского законодательства, особенностей работы оборудования и глубоких системных знаний по построению сетей в целом. Выполнение этого своими силами, как правило, невозможно. Лучше обратиться к профессионалам, имеющим опыт реализации подобных проектов и хорошо зарекомендовавшим себя на рынке. ●

Ваше мнение и вопросы присылайте по адресу
infosec@groteck.ru

Комментарий эксперта

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

Выбор решения для построения виртуальных защищенных решений (VPN) – непростая задача. И для ее решения важно обратить внимание на несколько ключевых параметров.

Высокая производительность решения

Решение не просто должно быть высокопроизводительным на некоем 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 без избыточной задержки и потери пакетов. В противном случае высокого качества сервиса ждать не стоит.

Высокий уровень масштабируемости

Решение должно легко подстраиваться под текущие требования бизнеса. В случае роста ЦОД, появления новых филиалов, увеличения количества потребителей сервиса должно осуществляться плавное наращивание мощностей системы, а не ее полная замена.

Отказоустойчивость

Система должна выполнять свои функции, даже если часть ее вышла из строя. Для этого требуется предусмотреть резервирование основных компонентов (шлюзов безопасности, каналов связи и др.) с автоматическим обнаружением отказа и переходом на резервное оборудование.

Высокие эксплуатационные характеристики

Предсказуемость поведения сети, хорошая документированность решения, простота поиска ошибок – это важно учитывать 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. Поэтому система информационной безопасности должна обеспечить высокий уровень защиты, не внося при этом ухудшений в качество предоставляемого сервиса.

Возможность централизованного управления и мониторинга системы

Система централизованного управления позволяет существенно снизить эксплуатационные расходы, а также обнаруживать проблемы на ранней стадии и легко получать полную информацию о состоянии системы.

Соответствие требованиям регулятора

Применение сертифицированных средств защиты позволяет выполнять требования российского законодательства, в том числе, например, аттестовать информационную систему.

Выбор решения для защиты данных – это не вопрос веры или удачи. Если необходимо получить решение, которое будет удовлетворять именно ваши (а не какие-то абстрактные) потребности, то лучше провести предварительное тестирование. Конечно, реализация демо-стенда или пилотной зоны требует больше трудозатрат, чем изучение решения по бумагам производителя. Но эти затраты окупаются с лихвой. Тем более что серьезные производители всегда готовы оказать поддержку и помочь пользователю в организации подобного тестирования.

Особенности построения виртуальных защищенных сетей

Павел Глушков, *системный инженер компании Softline*

В современном высокотехнологичном мире перед руководством любой компании рано или поздно встает вопрос об объединении своей компьютерной сети с удаленными площадками. Филиалы в других городах, заказчики, партнеры, удаленные сотрудники – многим группам пользователей может потребоваться предоставление безопасного доступа к внутренним ресурсам. И тогда возникает вопрос – посредством каких технологий решить эту бизнес-задачу?

Пути решения

Традиционное решение данной задачи, используемое уже много лет, – организация выделенного канала либо с помощью прокладки физического кабеля, либо через сеть провайдера услуг, что в условиях динамического рынка недостаточно гибко и чрезмерно затратно. В самом деле, не тянуть ведь оптическую линию к каждому партнеру. И кто даст гарантию, что передаваемые по сети провайдера услуг данные не будут перехвачены, подслушаны или, хуже того, изменены в интересах третьей стороны? Это особенно актуально, если каналом для передачи данных выбран Интернет.

Решением озвученной проблемы все чаще становятся виртуальные частные сети (VPN, virtual private network) – шифрованные туннели, позволяющие передавать данные по недоверенному каналу и при этом гарантировать их конфиденциальность и целостность. Конечные точки туннеля аутентифицируют друг друга посредством цифровых сертификатов или заранее переданных по защищенному каналу ключей, после чего весь передаваемый трафик подвергается криптообработке, исключающей возможность дешифровки или подмены данных за любое разумное время.

Особенности защищенных сетей

Задача построения защищенных сетей во многом схожа с построением обычных сетей передачи данных, но имеет ряд особенностей, которые крайне желательно учитывать при проектировании, выборе архитектуры и производителя оборудования.

Во-первых, стоит отметить, что существуют категории информации (например, персональные данные), передача которых по сетям общего пользования жестко регламентирована нормативными актами ФСБ и ФСТЭК. Стандартные алгоритмы шифрования (DES, 3DES, AES) и обеспечения целостности данных (MD5, SHA), повсеместно применяемые в оборудовании западных производителей, для защиты такой информации использовать противозаконно, это может повлечь за собой суровые санкции вплоть до ликвидации предприятия-нарушителя. В таких случаях организации обязаны использовать отечественные криптоалгоритмы семейства ГОСТ, причем устройства шифрования обязательно должны иметь сертификаты вышеупомянутых регуляторов. Аналогичные требования предъявляются и к государственным предприятиям – вне зависимости от степени конфиденциальности передаваемых данных.

На рынке сейчас представлен широкий ряд решений как отечественных производителей ("Код безопасности", "ИнфоТеКС" и др.), изначально предназначенных для построения ГОСТ VPN-сетей, так и зарубежных вендоров, реализующих ГОСТ-алгоритмы в дополнение к имеющимся стандартным (Stonesoft, Check Point и др.). Некоторые идут по пути выноса шифрующих функций в отдельные аппаратные модули для сетевого оборудования (например, модули NME-RVPN компании "С-Терра СиЭсПи" для маршрутизаторов Cisco). Но следует учитывать, что на законность использования того или иного решения, помимо типа криптоалгоритма, влияет еще ряд факторов (модель угроз, класс системы и т.д.). И точную юридическую оценку применительно к конкретной системе сможет дать только профессиональный консультант после проведения соответствующего тщательного обследования.

Во-вторых, следует очень внимательно подойти к выбору модели оборудования. Нельзя забывать, что основная задача построения виртуальной защищенной сети – передача данных без потерь и задержек. Криптографическая обработка требует значительных вычислительных ресурсов, следовательно, выбираемое устройство должно быть достаточно мощным, чтобы на лету обработать нужный объем трафика. Будем откровенны, производители оборудования, публикуя технические характеристики своих устройств, зачастую лукавят. Заявленные данные получаются путем замеров в "оптимальных условиях для тестирования", то есть максимально выгодных, когда все остальные функции устройства отключены (все ресурсы отданы системе шифрования), а размер проходящих через него пакетов максимален (количество криптоопераций в секунду минимально). В таких условиях