

Уже не раз говорилось о повсеместном распространении виртуализации и облачных технологий. Но давайте спустимся с облачных высот на землю – виртуализация приносит не только преимущества, но и новые угрозы



Александр Веселов,
начальник отдела технического
консалтинга ООО «С-Терра СиЭсПи»

Виртуализация. VPN. ГОСТ

Угрозы можно условно разделить на два типа: связанные непосредственно с виртуализацией и перекочевавшие в виртуальную среду из физической.

Первый тип обусловлен тем, что в виртуальной среде несколько виртуальных машин работает на одном физическом сервере и теоретически могут влиять друг на друга. Следовательно, возникают новые разновидности угроз несанкционированного доступа. Защититься от них можно как средствами, встроенными в гипервизор, так и специализированными средствами обеспечения безопасности. А может, и вовсе считать их не актуальными.

Угрозы второго типа знакомы каждому специалисту по безопасности. Для защиты от них из физической среды в виртуальную пришли антивирусы, сетевые средства и, конечно же, криптография. Если раньше для обеспечения безопасности виртуальной инфраструктуры использовали стоящие рядом программно-аппаратные средства, то теперь есть возможность построить виртуальную частную сеть – VPN (в том числе с применением ГОСТ-шифрования) непосредственно в виртуальной среде. Таким образом, обеспечивается защищенное взаимодействие как с ЦОД, так и с другими объектами.

Одним из немногих отечественных продуктов, разработанным специально для виртуальной среды, является С-Терра Виртуальный шлюз. Это виртуальная машина для гипервизоров VMware, Xen, KVM и Hyper-V с функционалом полноценного аппаратного

криптошлюза, в котором для построения защищенных соединений используется IPsec VPN с ГОСТ-алгоритмами. Продукт содержит встроенный межсетевой экран, управление осуществляется как с помощью централизованной системы управления С-Терра КП, так и с использованием привычного cisco-like интерфейса. Одно из важных преимуществ С-Терра Виртуального шлюза в том, что он сертифицирован ФСБ России (по классу КС1) и ФСТЭК России.

Зная преимущества виртуализации, нетрудно спроецировать их на виртуальный криптошлюз. В большинстве компаний используются аппаратные платформы различных брендов. При покупке аппаратного криптошлюза добавляется еще одна платформа, которая часто не совпадает с преобладающим брендом «железа». В результате в компании используется множество платформ, у которых разный срок службы и разные условия сервисной поддержки. У Виртуального шлюза такой проблемы нет – он работает на принятом у заказчика «железе» и условно независим от аппаратной платформы.

Важное преимущество С-Терра Виртуального шлюза – гибко масштабируемая производительность, которая зависит от мощности аппаратной платформы и регулируется лицензионно. Лицензией определяется количество ядер процессора, используемых для шифрования. При недостаточной производительности можно перенести VPN-шлюз на платформу с более мощным процессором или приобрести дополнительную лицензию для увеличения количества используемых ядер.

При использовании Виртуального шлюза появляются дополнительные возможности резервирования, например, snapshot и клонирование виртуальной машины, которое можно делать по расписанию либо перед изменением настроек.

Одна из приятных особенностей Виртуального шлюза – минимальный срок поставки. Виртуальный шлюз применяется для решения задач:

- защита корпоративной сети путем встраивания непосредственно в виртуальную инфраструктуру;
- защита трафика между сегментами ЦОДов;
- защита сетей управления;
- VPN-as-a-Service.

Вариант «VPN как услуга» наиболее интересен. У операторов связи появилась новая возможность – расширить услугу «безопасность как сервис», а именно добавить компонент «сертифицированный VPN как сервис». С помощью продуктов С-Терра оператор может предоставлять каждому своему заказчику отдельный виртуальный шлюз в облаке и при необходимости виртуальные шлюзы в другие точки, которым необходим доступ к облаку. Оператору не требуется хранить у себя несколько десятков аппаратных криптошлюзов – он просто разворачивает виртуальную машину из шаблона по требованию клиента. Таким образом, клиент получает легитимную и надежную защиту в кратчайшие сроки.

//Рассматривая виртуальный шлюз, не стоит забывать о его предшественниках – аппаратных криптошлюзах. У каждого из них есть преимущества. С одной стороны, традиционное проверенное временем решение, с другой, перспективная новинка. Независимо от выбранного варианта с продуктами С-Терра вы получите надежную и легитимную защиту. Какой из вариантов использовать – выбор за вами. **ADV**