# Виртуальная среда: защита доступа

**Александр Веселов,** *руководитель отдела технического консалтинга ООО "С-Терра СиЭсПи"*

В наше время уже трудно представить себе современную информационную систему, состоящую только из физических компонентов. Виртуализируются серверы, рабочие места сотрудников (VDI), сетевое оборудование и даже средства защиты информации. Эти тенденции реализуют новые преимущества: пользователи получили простоту установки и перераспределение ресурсов между виртуальными машинами, удобное резервное копирование и восстановление, экономию электроэнергии и мест в стойке, а интеграторы и производители — новый сегмент рынка. В то же время регуляторы, признавая неизбежность прихода новых решений, вынуждены корректировать нормативные документы.

После выхода продуктов "С-Терра Виртуальный Шлюз" и "С-Терра Клиент-М" для ОС Android в 2014 г. компания "С-Терра СиЭсПи" присоединилась к программе Citrix Ready, которая помогает пользователям дополнять продуктами других разработчиков базовые решения компании Citrix Systems для виртуализации, сетевого взаимодействия и облачных вычислений.

Компаниями проведено совместное тестирование, результаты которого показали полную сочетать продуктов С-Терра с Citrix Xen Server и Xen Mobile. Это позволяет сочетать преимущества виртуализации, централизованного управления и распределения политик для мобильных устройств с функциональными возможностями сертифицированного отечественного VPN-продукта.

В решении на базе инфраструктуры Citrix VPN-продукты С-Терра не только обеспечивают интегрированную защиту конфиденциальности и целостности данных при их передаче по недоверенным каналам связи, включая доступ к виртуальной инфраструктуре, но и позволяют соответствовать требованиям российского законодательства.

Сегодня виртуализация для разработчиков и пользователей систем защиты – не маркетинговый слоган, а эффективный рабочий инструмент. Значительно упрощается решение ряда проблем безопасности, например сложность и трудоемкость проведения полнофункционального тестирования обновлений ПО на работающей инфраструктуре. Виртуализация позволяет применить обновление не на "боевой" сервер, а на его клон с последующим тестированием работоспособности и только потом применением на основном.

## Актуальные угрозы

Но часть угроз все равно остается актуальной. Их можно условно разделить на два типа: угрозы, связанные непосредственно с виртуализацией, и угрозы, перекочевавшие в виртуальную среду из физической.

Первый тип характеризуется тем, что несколько виртуальных машин работают на одном физическом сервере и теоретически могут влиять друг на друга, порождая новые разновидности угроз несанкционированного доступа. Защититься от них можно средствами гипервизора или отдельными специализированными продуктами. Некоторые эксперты считают первый тип угроз неактуальным. С ними можно соглашаться, можно спорить, но это – тема для отдельной статьи.

Второй тип угроз уже хорошо знаком специалистам по ИБ. Средства защиты от них, как и сами угрозы, пришли в виртуальную среду из физической. Это – антивирусы, межсетевые экраны и, конечно же, криптография и VPN-устройства.

Повсеместное распространение виртуализации и централизация ресурсов привели к всплеску спроса на рынке VPN. Заказчики ожидают от производителей логичного шага – портирования своих продуктов в виртуальную среду. Производители обязаны оперативно реагировать, несмотря на особенности новой технологии и медленное обновление нормативной базы. При этом перед ними стоят следующие задачи:

1. Сохранение текущей функциональности аппаратного средства защиты.

Сохранение привычных пользователю функций подразумевается подсознательно, тем не менее, выделим это в отдельный пункт. Конечно, могут быть некоторые ограничения, связанные с особенностями виртуальной среды, но их количество должно быть сведено к минимуму.

2. Интеграция VPN-устройства в виртуальную инфраструктуру.

Если раньше для защиты виртуальной инфраструктуры использовали "стоящие рядом" программно-аппаратные средства, то сейчас требуется интеграция VPN-устройств непосредственно в виртуальную среду. Это позволяет применить основные преимущества виртуализации к средствам защиты информации: независимость от аппаратной платформы, экономия электропитания/охлаждения, удобное резервное копирование/восстановление. Причем у разных заказчиков могут быть разные гипервизоры: одни используют VMware, другие – Citrix Xen Server, третьи – KVM и т.д. VPN-продукт, в свою очередь,з должен быть максимально универсальным – поддерживать работу на любых гипервизорах с учетом их особенностей.

3. Сохранение качества сервисов.

Важно не допустить деградации сервисов при интеграции системы защиты в виртуальную среду. Не стоит умалять значимость производительности и поддержки качества обслуживания (QoS). Подбор производительности вызывал множество спорных ситуаций и на зафиксированных аппаратных платформах – при декларировании речь шла о маркетинговых показателях, представляющих собой пиковые значения, которые достигаются при шифровании пакетов большого размера. В виртуальной среде вопросов стало еще больше, ведь появился новый промежуточный компонент между "железом" и продуктом – гипервизор. Теперь может использоваться практически любая аппаратная платформа с разделением ресурсов между виртуальными машинами. Кроме того,

в гипервизорах есть различные варианты поддержки сетевых интерфейсов – виртуальные с различными драйверами или "проброс" сетевой карты непосредственно в виртуальную машину. Все эти факторы нужно учитывать при декларировании производительности, т.е. важно убедиться, что и производитель, и заказчик "говорят на одном языке" и одинаково понимают сущность термина "производительность" в рамках решаемой задачи.

4. Легитимность использования.

Не секрет, что если в информационной системе компании обрабатывается информация, подлежащая обязательной защите в соответствии с законодательством (например, персональные данные), то необходимо использовать сертифицированные регуляторами – ФСБ и ФСТЭК России – средства защиты. Развитие технологий опережает разработку руководящих документов, поэтому зачастую специальные нормативные документы для виртуальной среды отсутствуют. В таком случае руководствуются более общими актами, положениями, методиками и т.п.

## Традиции, опыт, качество

Опираясь на многолетний опыт разработки VPN-продуктов и учитывая перечисленные выше требования, компания "С-Терра СиЭсПи" выпустила на рынок новый продукт – С-Терра Виртуальный Шлюз (ВШ). Это яркий пример традиционного средства защиты – VPN-концентратора, – пришедшего из физической среды в виртуальную. ВШ предоставляет функциональные возможности сертифицированного средства криптографической защиты информации (СКЗИ) на основе стандартов IPsec VPN с поддержкой алгоритмов ГОСТ, а также является сертифицированным межсетевым экраном. Основная его задача – построение защищенных соединений – при переходе в виртуальную среду не изменилась, но теперь он позволяет реализовать дополнительные сценарии – защита трафика как между виртуальными машинами, находящимися на одном и нескольких физических серверах, так и с внешними объектами (site-to-site и/или remote access).

Продукт реализует все вышеуказанные задачи следующим образом:

- обладает той же функциональностью, что и программно-аппаратный комплекс;
- интегрируется непосредственно в виртуальную среду, поддерживаются все основные гипервизоры, представленные на рынке: VMware, Citrix Xen Server, KVM, Hyper-V, Parallels;
- производительность достигает 300 Мбит/с на ядро в зависимости от частоты процессора и типа трафика. Увеличение производительности возможно лицензионно (за счет увеличения количества ядер, используемых для шифрования). Поддерживается прямой доступ виртуального шлюза к сетевым картам (технология SR-IOV), что особенно важно для высокопроизводительных решений;
- сертифицирован ФСБ России как СКЗИ по классу КС1, ФСТЭК России как межсетевой экран 3-го класса, на отсутствие недекларированных возможностей по 3-му уровню контроля, оценочный уровень доверия 4-й усиленный. Продукт может использоваться в автоматизированных системах класса защищенности до 1В включительно, а также в государственных информационных системах до 1 класса защищенности включительно, в том числе обеспечивающих 1, 2, 3 и 4 уровни защищенности персональных данных.

На данный момент это единственное подобное решение на рынке.

Кроме того, ВШ в полной мере использует все преимущества виртуализации, такие как работа на аппаратной платформе принятого у заказчика бренда, перераспределение ресурсов, более гибкий подход к производительности. Значительно упрощается процесс установки, расширяются возможности по резервному копированию и восстановлению. Не стоит забывать об экономии мест в стойке и снижении энергозатрат. Отсутствие в составе продукта аппаратной платформы позволяет сократить сроки поставки и не зависеть от курса валют. ВШ поставляется буквально в считанные дни и поможет оперативно решить задачи заказчика. Цена продукта зафиксирована в рублях, что дает возможность заранее прогнозировать стоимость долговременной закупки.


Решения с использованием продукта С-Терра Виртуальный Шлюз уже нашли широкое применение в различных областях. Например, успешно реализован проект MNP, более известный как "отмена мобильного рабства"; в перечне услуг облачных операторов уже появилась новая строка "Сертифицированный VPN-as-a-Service".

"С-Терра СиЭсПи" является одним из лидеров рынка отечественных VPN-продуктов. Компания предлагает решения, соответствующие всем современным техническим требованиям в области информационной безопасности и легитимные по мнению регуляторов. Именно такой подход обеспечивает надежную защиту любой информационной системы. ●

s•terra

NM ●
АДРЕСА И ТЕЛЕФОНЫ ООО "С-Терра СиЭсПи" см. стр. 48