Виртуализация сетей: новый подход к безопасности

В начале июня 2016 г. VMware объявила о завершении интеграции корпоративной платформы управления мобильными устройствами VMware AirWatch с решением VMware NSX, предназначенного для развертывания программно-конфигурируемых сетей, что позволило вывести управление безопасностью внутри виртуализованного ЦОД на качественно новый уровень.

Владимир Ткачев – технический директор VMware в России и СНГ.

Введение

Об интеграции VMware AirWatch с VMware NSX компания объявила около года назад. Ее завершение позволило создать уникальный динамический сетевой продукт, который дает возможность защищать пользовательские данные или/и прикладную нагрузку при работе с любого устройства внутри ЦОДа.

Благодаря интеграции VMware AirWatch с NSX достигаются следующие преимущества:

- *обеспечивается безопасность корпоративных ресурсов независимо от типа точек доступа и самого устройства – будь то мобильный телефон, ноутбук, планшет и др., даже, если они подключены по незащищенному Wi-Fi или по каким-либо другим сетям общего доступа;*
- *значительно расширяются возможности продвижения концепции BYOD (bring your own device) в организации, т.к. интеграция AirWatch с NSX позволяет обезопасить любые мобильные приложения для конкретного ресурса в пределах центра обработки данных рамками микросегментированной сети;*
- *управление политиками безопасности мобильных устройств/приложений может осуществляться в течение секунд, независимо от того, из каких источников они развернуты – частных или публичных облаков, корпоративных приложений или из других источников. Если какое-либо устройство является потенциально опасным, микросегментация с NSX гарантирует, что воздействие ограничивается только этим одним пользователем/устройством.*

В соответствии с последним отчетом Gartner ("Magic Quadrant for Enterprise Mobility Management Suites", июнь, 2016 г.), AirWatch среди корпоративных решений управления мобильными устройствами заняло первое место как по присутствию на рынке, так и по концепции развития (прим. ред.).

Необходимо также отметить, что интеграция VMware AirWatch с NSX поддерживается, начиная только с расширенной версии NSX (табл. 1, http://www.vmware.com/files/pdf/products/nsx/VMware-NSX-Datasheet.pdf).

Табл. 1. Поддерживаемый функционал в различных реализациях NSX.

	STANDARD	ADVANCED	ENTERPRISE
Distributed switching and routing	•	•	•
NSX Edge firewall	•	•	•
NAT	•	•	•
Software L2 bridging to physical environment	•	•	•
Dynamic routing with ECMP (active-active)	•	•	•
API-driven automation	•	•	•
Integration with vRealize and OpenStack	•	•	•
Log management with vRealize Log Insight for NSX	•	•	•
Automation of security policies with vRealize		•	•
NSX Edge load balancing		•	•
Distributed firewalling		•	•
Integration with Active Directory		•	•
Server activity monitoring		•	•
Service insertion (third-party integration)		•	•
Integration with VMware AirWatch®		•	•
Cross vCenter NSX			•
Multisite NSX optimizations			•
VPN (IPSEC and SSL)			•
Remote gateway			•
Integration with hardware VTEPs			•

Традиционная и новая концепция ИБ

Расходы на безопасность за последние несколько лет заметно выросли – в 2015 г. они достигли $75,5 млрд (http://www.gartner.com/newsroom/id/3135617), но растут и убытки от взломов. Особое беспокойство вызывает тот факт, что четверть (25%) ИТ-директоров в России скрывают от топ-менеджмента информацию об утечках. Это данные исследования VMware и Vanson Bourne, проведенного весной 2016 г. среди ИТ-директоров и офисных сотрудников. Утаивание такой информации говорит о том, что руководители, отвечающие за работу бизнеса, не имеют полной картины рисков. Необходимо пересматривать подход к кибербезопасности.

В настоящее время около 80% инвестиций компаний, выделяемых на ИБ, тратится на защиту периметра и только 20% – на борьбу с внутренними угрозами и утечками (рис. 1). Такой подход на ИБ имеет существенную уязвимость по двум причинам. *Во-первых*, вследствие того, что размер периметра из-за перехода на распределенные инфраструктуры существенно возрос, соответственно, выросла и вероятность проникновения. *Во-вторых*, из-за низкого контроля внутри ЦОДа (не соответствующего техническому уровню обеспечения возможных утечек) вероятность внутренних угроз также значительно выросла. Это может усугубляться еще и такими причинами, как:

- наличие низкоприоритетных «забытых» серверов;
- возможность свободного перемещения злоумышленника по сети после проникновения;
- возможность свободного обмена данными внутри ЦОДа;
- возможность нахождения злоумышленника в сети длительное время (месяцы и более).

В этих условиях концепция ИБ в виртуальном ЦОДе должна предусматривать тотальную динамичную адаптивную защиту всех ресурсов (включая информацию на всех этапах ее жизненного цикла) не только от внешних, но и внутренних угроз с возможностью простого и быстрого управления ею (рис. 2).

Такой подход несет следующие преимущества для бизнеса:

Рис. 1. В настоящее время около 80% инвестиций компаний, выделяемых на ИБ, тратится на защиту периметра и только 20% – на борьбу с внутренними угрозами и утечками.

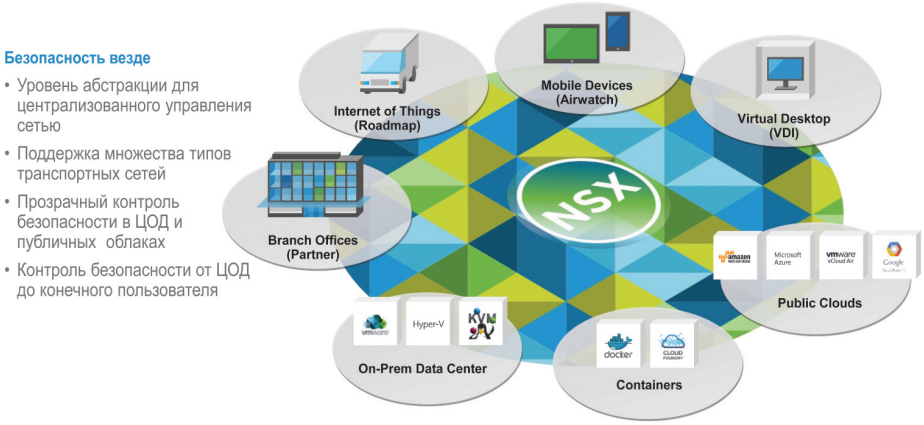

Рис. 2. Управление связностью и безопасностью на всех этапах существования информации.

– *с точки зрения автоматизации:* достаточно однажды согласовать шаблон сети и профиль безопасности для типовых задач, после чего полное время развертывания уменьшается до минут;

– *с точки зрения безопасности:* в ЦОДе больше нет доверенных зон – каждая ВМ, каждый сервис, каждый кластер в своем контуре безопасности, и вы всегда контролируете трафик между ними;

– *с точки зрения аварийного восстановления*: вы получаете единую сеть и сетевые функции на любом оборудовании, в любых кластерах, в любом вашем ЦОДе. А сетевое оборудование берите любое, какое вам удобнее и/или дешевле;

– *с точки зрения экономии*: свобода выбора оборудования рождает конкуренцию и возможности оптимизации. К тому же вы сможете дольше использовать вашу текущую архитектуру и оборудование, т.к. оно должно только перенаправлять пакеты.

Безопасность – еще одна функция сетевой виртуализации

Виртуализация серверов позволила компаниям по всему миру консолидировать и перераспределять инфраструктурные ресурсы, упрощать работу, проводить своевременную отладку и масштабирование инфраструктурных приложений в соответствии с меняющимися приоритетами бизнеса. Виртуальные серверы и решения для хранения данных кардинальным образом преобразили центры обработки данных, существенно снизив операционные издержки за счет автоматизации, а капитальные вложения – за счет консолидации и разделения аппаратных средств. Но, несмотря на полученный эффект, большая часть возможностей программно-определяемого ЦОДа остается неиспользованной. Говоря точнее, развитие бизнеса в этой области сдерживается устаревшими принципами работы сети.

Сети центров обработки данных, будучи консервативными в своем развитии, долгое время остаются достаточно сложными, узкоспециализированными и закрытыми для инноваций. Это оказывает непосредственное влияние на время развертывания приложений, поскольку приложениям, помимо вычислительных, требуются также и сетевые ресурсы. Решением в данном случае является переход на программно-конфигурируемые сети (SDN), которые подразумевают разделение процессов передачи и управления данными, а также построение инфраструктурных облачных сервисов (рис. 3). В качестве инструмента виртуализации сетей и сетевых функций VMware предлагает платформу NSX, которая позволяет создать и развернуть поверх физической сети виртуальную инфраструктуру, реализующую сетевые функции. Развивать данное направление VMware начала в 2012 г. после приобретения компании-стартапа Nicira, которая разрабатывала решения в области SDN. Одними из основных преимуществ SDN являются простота масштабирования и эластичность сети, а также возможность создания унифицированной технологической платформы для различных сетевых приложений, пользователей и арендаторов.

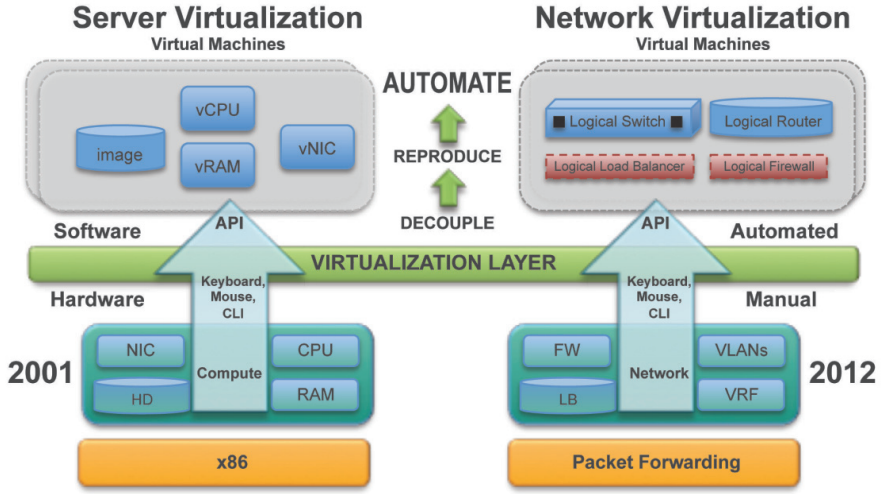

Рис. 3. Сравнение серверной и сетевой виртуализации.

Одним из базовых принципов NSX является принцип микросегментации сети – это неотъемлемая способность платформы NSX сегментировать сеть ЦОДа до уровня виртуальной машины, что позволяет поместить каждую виртуальную машину ЦОД в выделенный домен безопасности с полным контролем ее сетевых коммуникаций. Микросегментация играет большую роль в обеспечении безопасности центра обработки данных.

Многие компании проделывают большую работу по внедрению межсетевых экранов, которые защищают их от внешних угроз. В то же время почти каждый третий (31%) ИТ-руководитель в России считает одной из самых значительных уязвимостей своей организации устаревшее программное обеспечение систем безопасности. Проблема заключается в том, что когда злоумышленник проникает внутрь периметра, у компаний, инвестировавших в упомянутые выше межсетевые экраны, не остается никаких средств защиты от атаки. Проникнув внутрь сети, злоумышленники могут свободно «перемещаться» от одного сетевого ресурса к другому, месяцами собирая информацию, ведь обнаружить следы их присутствия можно будет разве что случайно. Поэтому локализация угроз становится критической необходимостью. Благодаря микросегментации внутренняя структура распределенного межсетевого экрана ЦОДа принимает форму сот (сегментов), обеспечивая снижение потенциального ущерба от внешней атаки.

Заключение

Микросегментация позволяет оперативно применять новые правила сетевого взаимодействия к различным сегментам внутри центра обработки данных. Внося изменения в конфигурацию распределенного межсетевого экрана с микросотовой архитектурой, встроенного в NSX, компании получают возможность эффективно обнаруживать и изолировать угрозы до того, как они атакуют другие компьютеры.

Таким образом, межсетевой экран можно подключить к каждому компьютеру, ноутбуку, виртуальной машине или даже смартфону. При этом нет необходимости обновлять аппаратную часть, VMware NSX можно развернуть поверх сети, построенной на любом оборудовании, обеспечивающем L2 и/или L3 коммутацию. Весь трафик внутри ЦОД оказывается под контролем. В ЦОД больше нет доверенных зон – каждая виртуальная машина, каждый сервис, каждый кластер размещается в своем сегменте безопасности с возможностью контроля трафика между сегментами.

VMware работает с ведущими вендорами в области информационной безопасности и предлагает интегрированные решения с Intel Security, Check Point Software Technologies, Palo Alto Networks, Trend Micro, Symantec и другими производителями. Направление VMware NSX является для компании одним из ключевых, особенно в свете постоянных инцидентов в области кибербезопасности, которые мы наблюдаем каждый день.

Владимир Ткачев,
VMware в России и СНГ.