VMware NSX Data Center

Развитие ИТ-инфраструктуры в соответствии с темпами роста бизнеса

«Технологии стремительно развиваются, открывая широчайшие возможности перед инициативными компаниями».

БАРТ ВАН АРК (BART VAN ARK), ДОКТОР НАУК
ИСПОЛНИТЕЛЬНЫЙ ВИЦЕ-ПРЕЗИДЕНТ,
СТАРШИЙ ЭКОНОМИСТ И ДИРЕКТОР ПО СТРАТЕГИЧЕСКОМУ РАЗВИТИЮ
THE CONFERENCE BOARD

VMware NSX® Data Center — это комплексная платформа виртуализации и обеспечения безопасности сети уровней 2–7, которая помогает реализовать виртуальную облачную сеть — программно-определяемую сеть, охватывающую центры обработки данных, облака и платформы приложений. NSX Data Center помогает разместить сетевые службы и систему безопасности ближе к среде приложений — от виртуальных машин (ВМ) до контейнеров и аппаратной инфраструктуры. Инициализация и администрирование виртуальных сетей, как и ВМ, могут осуществляться независимо от базового оборудования. NSX Data Center воспроизводит полную модель сети программным образом, что дает возможность создавать и инициализировать любые топологии сети — от базовых до сложных многоуровневых — за считаные секунды. Пользователи могут создать несколько виртуальных сетей с различными требованиями, используя сочетание служб, предоставляемых платформой NSX, или многочисленные интегрированные сторонние решения — от брандмауэров нового поколения до решений по управлению производительностью — для формирования более адаптивных и безопасных сред. Затем эти службы можно распространить на множество конечных устройств в различных облаках.

Противоречивые требования ведут к компромиссным решениям

Скорость, адаптивность, надежная защита и высокая доступность приложений являются важнейшими приоритетами для ИТ-отделов. Надежная инфраструктура приложений настолько необходима компаниям, что ИТ становятся важнейшим фактором для инновационного развития компании и цифровой трансформации. Однако в связи с быстрым развитием информационных технологий и меняющимися ожиданиями компаниям приходится постоянно менять приоритеты, часто в ущерб эффективности внедрения ИТ.

ИТ-специалисты не понаслышке знают, как сложно удовлетворить требования сразу нескольких заинтересованных сторон, и нередко вынуждены отдавать предпочтение одним в ущерб другим. Например, при быстром развертывании приложения проблематично обеспечить его безопасность, поскольку это технически сложная и трудоемкая задача. На аналогичные компромиссы приходится идти и при обеспечении доступности приложений в разных средах — эти требования, по сути, противоречат интересам компании в целом.

Постоянное напряжение и необходимость поиска компромиссов существенно осложняют работу ИТ-отделов. В результате возникают серьезные проблемы в различных сферах ответственности: невозможность быстро удовлетворять потребности бизнеса, уязвимость ЦОД и облачных сред, а также недостаточная адаптивность.

Полная реализация возможностей инфраструктуры

Большинство компаний уже виртуализировали вычислительные компоненты своих ЦОД. Кроме того, многие компании также приняли решение виртуализировать хранилища, а более 70% из них уже внедрили или планируют внедрить программно-определяемое хранилище.

ОСНОВНЫЕ ПРЕИМУЩЕСТВА

Гибкое управление безопасностью: предотвращение горизонтального распространения угроз в среде благодаря микросегментации политик безопасности на уровне рабочих нагрузок.

Быстродействие и адаптивность: сокращение времени инициализации сети с нескольких дней до считаных секунд и повышение операционной эффективности благодаря использованию автоматизации.

Согласованные политики и процессы: согласованное управление политиками сети и безопасности независимо от топологии физической сети в ЦОД, публичных и частных облаках, а также на платформах приложений.

Благодаря абстрагированию возможностей от оборудования и их переносу на программную платформу компании могут быстро инициализировать компоненты приложений, перемещать виртуальные системы в пределах одного ЦОД или между различными ЦОД и автоматизировать важные процессы. Без виртуализации брандмауэров, а также средств коммутации, маршрутизации и балансировки нагрузки сложно реализовать полный спектр возможностей программно-определяемого ЦОД.

Компании, использующие аппаратные сетевые компоненты, уступают в быстродействии, адаптивности и защищенности компаниям с виртуализированной сетью. Успех бизнеса определяется эффективностью работы корпоративной сети.

Необходима абсолютно новая сетевая инфраструктура ЦОД, где нет места компромиссу между быстродействием, безопасностью и адаптивностью. Подход к использованию ЦОД нужно менять: ИТ-отделы должны беспрепятственно и в полном объеме реализовать все возможности для бизнеса. Тысячи компаний пришли к выводу, что виртуализация сети — это именно то, что им требуется.

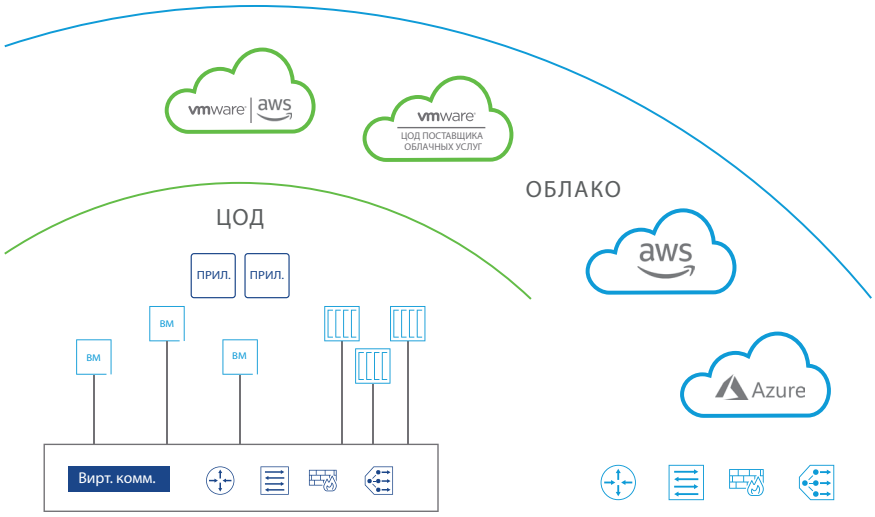

РИС. 1. Реализация согласованных служб сети и системы безопасности с помощью NSX Data Center

Виртуализация сети — это перенос сетевых служб и служб безопасности на уровень виртуализации ЦОД, благодаря чему можно создавать среды приложений, делать их снимки, хранить, перемещать, удалять и восстанавливать их так же быстро и удобно, как развертывать ВМ. NSX Data Center применяет общие политики сети и безопасности в разнородных средах и на различных платформах приложений, обеспечивая реализацию этих преимуществ в разных центрах обработки данных, частных и публичных облаках, а также для традиционных и современных приложений. Это, в свою очередь, обеспечивает высокий уровень безопасности и эффективности, который до этого был недостижим с эксплуатационной и финансовой точек зрения.

С помощью NSX ИТ-специалисты получают возможность внедрять инновации и удовлетворять требования множества заинтересованных лиц, а не рассматривать их как противоречивые и взаимоисключающие. Теперь они могут не только обеспечивать беспрецедентно высокий уровень безопасности, но и делать это с необходимой для бизнеса скоростью.

ОСНОВНЫЕ ВОЗМОЖНОСТИ

Распределенный брандмауэр с сохранением состояния: брандмауэр с сохранением состояния вплоть до уровня 7, встроенный в ядро гипервизора и распределенный по всей среде с интеграцией непосредственно в облачные приложения, среды публичных облаков и аппаратные узлы.

Микросегментация с учетом контекста: динамическое создание политик и групп безопасности с автоматическим обновлением в соответствии со множеством атрибутов и данных о приложениях уровня 7, помогающее реализовать политику адаптивной микросегментации.

Управление облаком: интеграция с vRealize Suite, OpenStack и другими решениями, а также полная поддержка интеграции с Terraform Provider, модулями Ansible и PowerShell.

Интеграция со сторонними решениями: усиление безопасности и расширение возможностей сетевых служб благодаря сотрудничеству с ведущими сторонними поставщиками.

Поддержка облачных технологий: поддержка расширенных служб сети и безопасности корпоративного класса на различных платформах контейнеров, в BM и аппаратных узлах с визуализацией сети контейнеров.

NSX Intelligence™: ускорение процессов обнаружения, анализа и применения политик сегментации приложений без развертывания новых средств и агентов; упрощение процессов обеспечения защиты благодаря встроенной в инфраструктуру системе безопасности.

NSX Distributed IDS/IPS™: передовая система обнаружения угроз, предназначенная для выявления их распространения в горизонтальном трафике, которая использует встроенное средство распределенного анализа и адаптированного распределения сигнатур.

Встроенная система безопасности

NSX Data Center обеспечивает уникальную возможность визуализации компонентов приложений — от сетевых коммуникаций до поведения отдельных рабочих нагрузок на уровне процессов — благодаря тому, что это решение встраивается в гипервизор и другие стандартные контрольные точки, поверх которых развертываются приложения. Визуализация способствует автоматическому созданию политик сетевой безопасности в соответствии с требуемым уровнем безопасности приложения. Благодаря этому ИТ-персонал, специалисты по информационной безопасности и разработчики приложений тратят меньше времени на циклы проверки безопасности.

Кроме того, это решение обеспечивает согласованное применение политик безопасности в средах с несколькими ЦОД и в гибридных облаках, а также полный контроль над приложениями на основе BM, контейнеров и аппаратных серверов. NSX Intelligence обеспечивает непрерывную визуализацию в масштабе ЦОД, что значительно упрощает и автоматизирует внедрение микросегментации.

Решение VMware NSX Distributed IDS/IPS помогает без труда обеспечивать соответствие нормативным требованиям, создавать виртуальные зоны безопасности и обнаруживать распространение угроз в горизонтальном трафике. NSX Data Center также предоставляет возможности визуализации и управления для сторонних служб безопасности, например брандмауэров нового поколения, систем предотвращения и обнаружения вторжений (IPS и IDS) и антивирусных средств, что повышает их эффективность.

NSX Data Center помогает превратить обеспечение безопасности (которое до этого заключалось в реагировании на возникшие угрозы) в упреждающий, интегрированный и автоматизированный этап жизненного цикла разработки приложений. Новые инициализированные рабочие нагрузки автоматически наследуют политики безопасности, которые продолжают действовать в течение всего их жизненного цикла. При удалении рабочих нагрузок политики безопасности удаляются вместе с ними, что уменьшает общее число политик и упрощает управление.

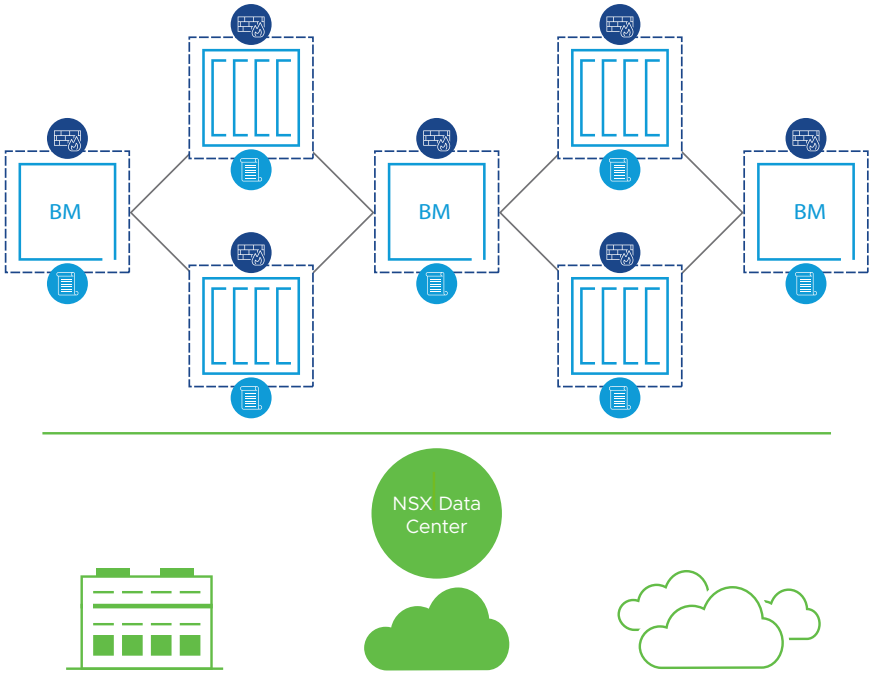

РИС. 2. Принудительное применение политик безопасности на самом детализированном уровне ЦОД

Автоматизация

В условиях расширения сфер деятельности и ускорения развития компаний автоматизация виртуализированных сетей и систем безопасности обеспечивает создание и развертывание служб и приложений в соответствии с темпами роста бизнеса. Автоматизация помогает избавиться от выполняемых вручную и подверженных ошибкам задач и может существенно ускорить развертывание приложений.

NSX Data Center в сочетании с ПО для управления облаком (например, VMware vRealize® Automation Cloud™) реализует централизованное управление инициализацией, развертыванием, процессами и выводом из эксплуатации инфраструктуры сети и безопасности, а также приложений. С помощью таких средств, как Terraform и Ansible, решения VMware интегрируют жизненный цикл служб сетей и безопасности и благодаря этому автоматизируют все процессы в инфраструктуре и устраняют «узкие места» жизненного цикла приложений, связанные с сетями и безопасностью.

Автоматизация служб сети и безопасности для традиционных (на основе ВМ) и новых (на основе контейнеров) приложений становится возможна благодаря применению общих политик сети и безопасности на обеих платформах. Кроме того, это обеспечивает автоматическое развертывание, перенос и вывод из эксплуатации приложений в локальных ЦОД, в частных и публичных облаках.

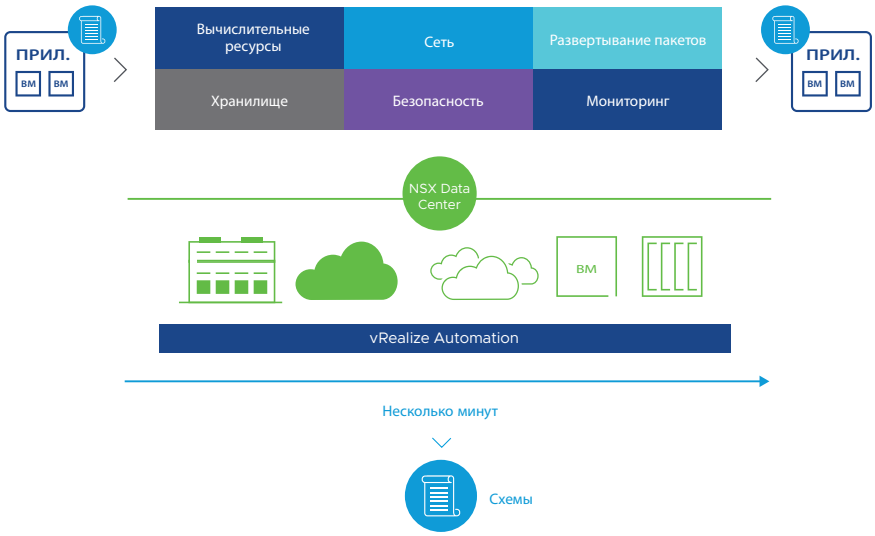

РИС. 3. Быстрое и воспроизводимое развертывание за счет автоматизации служб сети и безопасности

Сети для многооблачных сред

NSX Data Center и NSX Cloud™ образуют единую модель сети и системы безопасности для разных сред, избавляя вас от необходимости настраивать сеть вручную и обеспечивая высокую операционную эффективность благодаря автоматизации сети. Политики сети и безопасности применяются к каждой рабочей нагрузке в течение всего ее жизненного цикла, упрощая управление гибридными и многооблачными средами. Решение NSX Federation обеспечивает централизованное управление политиками в разных средах (локальных и облачных), удобство эксплуатации и согласованное применение политик в различных облаках.

Это дает возможность переносить виртуальные машины и даже ЦОД из одной среды в другую с минимальным или даже нулевым простоем приложений. Благодаря этому компании могут ускорить восстановление во время запланированных процессов миграции или незапланированных простоев. Если сеть и система безопасности охватывают разнородные среды, компании также могут использовать ресурсы различных физических ЦОД как единое частное облако. Эта форма объединения ресурсов в пулы с центрами обработки данных в режиме «активный-активный» называется объединением нескольких ЦОД в пул или географически распределенными пулами.

Совместно они обеспечивают безопасное и удобное перемещение приложений, упрощая миграцию рабочих нагрузок в облако и из него, а также между физическими средами. Благодаря NSX Data Center и NSX Cloud виртуализированная платформа сети и безопасности, которую ИТ-отделы используют в инфраструктуре, станет доступной в облаке и в других средах, что упростит и ускорит миграцию.

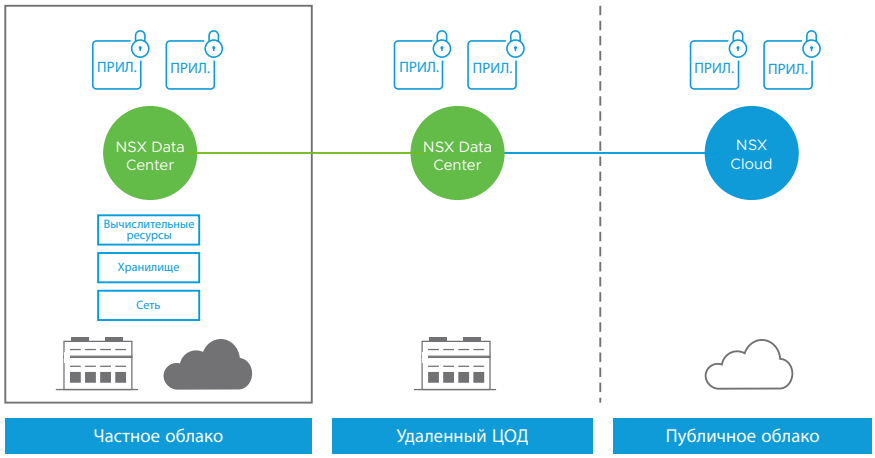

РИС. 4. Согласованная между средами и облаками инфраструктура сети и системы безопасности, снижающая ущерб от простоев

Сеть и система безопасности для современных приложений

Интеграция VMware NSX Data Center с новыми платформами приложений помогает развернуть средства управления службами сети и безопасности (например, подсистемы балансировки нагрузки, брандмауэры, коммутаторы и маршрутизаторы) исключительно программным способом и использовать их по модели «инфраструктура как код» на основе API.

Все больше приложений создается на основе контейнеров и микрослужб, поэтому возможность подключать и защищать эти новые приложения в виде единой рабочей нагрузки очень важна. NSX Data Center предоставляет контейнерам и микрослужбам те же возможности, что и всем остальным рабочим нагрузкам и конечным устройствам, включая поддержку сетей уровня 3. Это решение поддерживает создание сетей между контейнерами, а также микросегментацию до уровня отдельных контейнеров (в том числе для микрослужб) с помощью политик, переносимых с рабочими нагрузками по мере их инициализации, изменения, перемещения и вывода из эксплуатации.

NSX Data Center интегрируется с несколькими платформами для оркестрации приложений и контейнеров, гипервизорами и публичными облачными средами. Это решение также интегрируется с платформами приложений, что помогает реализовать встроенные адаптивные возможности управления службами сети и безопасности по мере разработки новых приложений.

ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ

Дополнительные сведения см. на странице vmware.com/go/nsx.

NSX Data Center: технический проспект

NSX Intelligence: обзор решения

Страница продукта NSX Distributed IDS/IPS

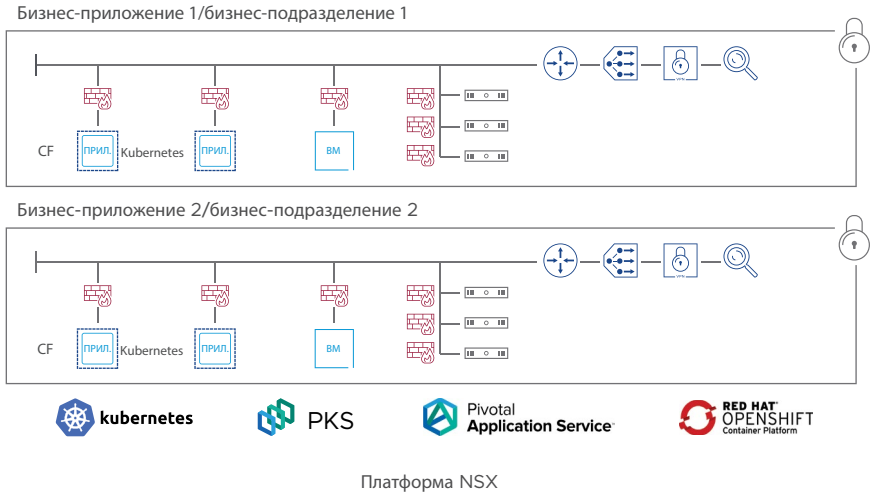

РИС. 5. Реализация расширенных служб сети и безопасности для рабочих нагрузок в контейнерах на разных платформах приложений, в различных средах и облаках

Ускоренная реализация преимуществ для бизнеса и создание платформы для дальнейшего развития

В компаниях, использующих NSX Data Center, это решение быстро становится основой стратегии реализации инфраструктуры ЦОД и многооблачной среды, а также играет определяющую роль в успешной работе ИТ-отдела. В настоящее время тысячи заказчиков NSX Data Center реализуют преимущества для своих компаний, используя важные приложения в быстрых, адаптивных и безопасных виртуальных сетях, эффективность которых недостижима для традиционных аппаратных сетей.

Благодаря современным сетевым технологиям и механизмам безопасности заказчики NSX Data Center не только моментально получают существенные преимущества, но и избавляются от необходимости решения длительных и трудоемких задач, ранее отнимавших значительную часть рабочего времени. Это, в свою очередь, дает компаниям возможность оптимизировать организационную структуру с учетом будущих потребностей бизнеса и ролей ИТ-специалистов, необходимых для удовлетворения этих потребностей.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel (877) 486–9273 Fax (650) 427–5001 www.vmware.com
125284, Россия, Москва, ул. Беговая, д. 3/1. Тел.: +7 (495) 212–2900 Факс: +7 (495) 212–2901 www.vmware.com/ru

Номер по каталогу: 497393aq-so-nsx-data-cntr-a4-Final 3/20.