VMWARE NSX DATA CENTER

Платформа виртуализации и обеспечения безопасности сети

КРАТКОЕ ОПИСАНИЕ

VMware NSX® Data Center — это платформа виртуализации и обеспечения безопасности сети, которая реализует виртуальную облачную сеть, программный подход к созданию и эксплуатации сети, охватывающий центры обработки данных, облака, различные устройства и элементы. NSX Data Center помогает разместить сетевые службы и систему безопасности ближе к среде выполнения приложений — от виртуальных машин до контейнеров и аппаратной инфраструктуры. Инициализация и администрирование виртуальных сетей, как и виртуальных машин, могут осуществляться программно, независимо от базового оборудования. NSX Data Center воспроизводит полную модель сети программным образом, что дает возможность в течение нескольких секунд создавать и инициализировать любые топологии сети: от базовых до сложных многоуровневых. Пользователи могут создать несколько виртуальных сетей с различными требованиями, используя сочетание служб, предоставляемых платформой NSX, или многочисленные интегрированные решения партнеров — от брандмауэров нового поколения до решений по управлению производительностью — для формирования более адаптивных и безопасных сред. Затем эти службы можно распространить на ряд конечных устройств в различных облаках.

ОСНОВНЫЕ ПРЕИМУЩЕСТВА

- Микросегментация и гибкие политики безопасности, применяемые к отдельным рабочим нагрузкам.
- Сокращение времени инициализации сети с нескольких дней до нескольких секунд, повышенная эксплуатационная эффективность в результате использования автоматизации.
- Возможности переноса рабочих нагрузок между центрами обработки данных и внутри них, независимо от топологии физической сети.
- Повышение уровня безопасности и расширение возможностей сетевых служб благодаря сотрудничеству с ведущими сторонними поставщиками.

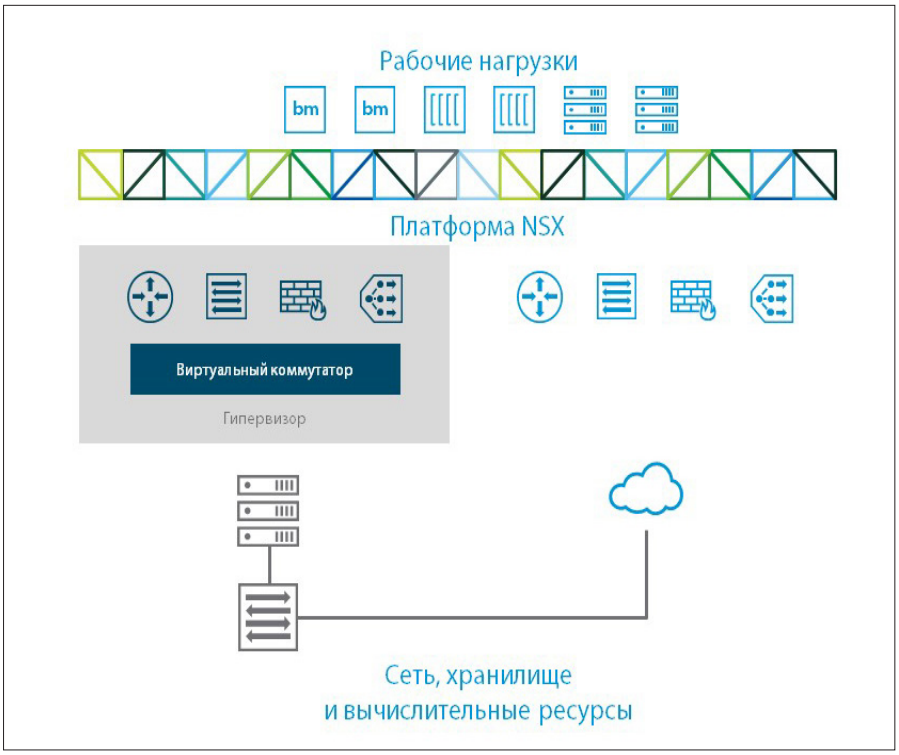

Рис. 1. NSX Data Center: платформа виртуализации и обеспечения безопасности сети

Виртуализация сети, безопасность и программный ЦОД

VMware NSX Data Center предоставляет инновационную эксплуатационную модель сети, которая реализуется в программном обеспечении и составляет основу для программного ЦОД. Администраторы ЦОД теперь могут достигать новых уровней адаптивности, безопасности и экономии, которые были немыслимы, когда сеть ЦОД была привязана к физическому оборудованию. NSX Data Center включает в себя полный комплект элементов логической сетевой инфраструктуры и служб, таких как логические коммутаторы, маршрутизаторы, брандмауэры, средства балансировки нагрузки, сети VPN, а также компоненты для мониторинга и обеспечения качества обслуживания. Эти службы предоставляются в виртуальных сетях с помощью любой платформы управления облаком и API-интерфейсов NSX Data Center. Развертывание виртуальных сетей выполняется без прерывания работы пользователей на любом существующем сетевом оборудовании.

Основные возможности NSX Data Center

Коммутация	Логическое наложение уровня 2 обеспечивается по всей коммутируемой матрице уровня 3 внутри и за пределами ЦОД. Поддержка наложения сетей на основе VXLAN.
Маршрутизация	Динамическая маршрутизация между виртуальными сетями выполняется в ядре гипервизора распределенными службами, поддерживается горизонтальное масштабирование с аварийным переключением типа «активный-активный» на физические маршрутизаторы. Поддерживаются протоколы статической и динамической маршрутизации (OSPF, BGP).
Распределенный брандмауэр	Возможности распределенных брандмауэров с проверкой состояния встроены в ядро гипервизора и обеспечивают пропускную способность до 20 Гбит/с на каждый узел гипервизора. Поддержка Active Directory и мониторинга действий. Кроме того, NSX Data Center предоставляет брандмауэр для вертикального трафика с помощью NSX Edge™.
Балансировка нагрузки	Балансировка нагрузки для уровней 4–7 с переносом нагрузок SSL и сквозной передачей, средства проверки работоспособности сервера и правила для приложений обеспечивают возможности программирования и манипулирования трафиком.
VPN	Удаленный доступ через VPN и VPN-подключение типа «среда-среда», неуправляемая сеть VPN для служб облачных шлюзов.
Шлюз NSX	Поддержка мостов между сетями VXLAN и VLAN обеспечивает оптимальное подключение к физическим рабочим нагрузкам. Эта возможность встроена в NSX Data Center, а также поддерживается надстоечными коммутаторами, поставляемыми партнерами по экосистеме.
API-интерфейсы NSX Data Center	Поддерживаются API-интерфейсы на базе RESTful для интеграции с любыми платформами управления облаком или пользовательскими системами автоматизации.
Эксплуатация	Встроенные возможности управления эксплуатацией, такие как центральный интерфейс командной строки, трассировка, SPAN и IPFIX, облегчают устранение неполадок и помогают проводить упреждающий мониторинг инфраструктуры. Интеграция с такими средствами, как VMware vRealize® Operations™ и vRealize Log Insight™, обеспечивает дополнительные возможности анализа и устранения неполадок. Благодаря таким возможностям, как Application Rule Manager и мониторинг конечных устройств, обеспечивается комплексная визуализация сетевого трафика до уровня 7. Разработчики приложений получают возможность определять как внешние, так и внутренние конечные устройства и создавать соответствующие правила безопасности.
Микросегментация с учетом контекста	NSX Data Center дает возможность создавать динамические группы безопасности и связанные политики не только на основе IP- и MAC-адресов, но и с учетом объектов и меток VMware vCenter®, типа операционной системы и сведений о приложениях уровня 7, что помогает реализовать контекстную микросегментацию приложений. Благодаря политикам на основе учетных данных, в которых используются данные для входа в систему, получаемые от ВМ, из каталога Active Directory и из интегрированных систем управления мобильными устройствами, можно реализовать систему безопасности на уровне пользователя, в том числе на уровне сеанса в удаленных средах и средах виртуальных компьютеров.
Управление облаком	Встроенная интеграция с vRealize Automation™ и OpenStack.
Интеграция со сторонними партнерскими решениями	Поддерживается интеграция служб управления, плоскости управления и плоскости данных с решениями сторонних поставщиков в широком спектре категорий, таких как брандмауэры следующего поколения, IDS/IPS, антивирусы без агентов, контроллеры предоставления приложений, коммутаторы, управление процессами, средства визуализации, усовершенствованные системы безопасности и т. д.
Сети и средства безопасности в нескольких средах	Расширение служб сети и безопасности на несколько центров обработки данных, независимо от базовой физической топологии, чтобы обеспечить аварийное восстановление и развернуть центры обработки данных в режиме «активный-активный».

ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ

Посетите страницу www.vmware.com/go/nsx.

Дополнительные сведения о вариантах лицензирования редакций NSX см. по адресу https://kb.vmware.com/kb/2145269.

Для получения информации или приобретения продуктов VMware обращайтесь по телефону +7 (495) 212–2900, посетите страницу www.vmware.com/ru/products или найдите уполномоченного торгового посредника на сайте VMware.

Сценарии использования

Безопасность

С помощью NSX Data Center можно разделить центр обработки данных компании на выделенные сегменты безопасности вплоть до уровня отдельной рабочей нагрузки, независимо от того, где она выполняется. ИТ-отделы могут настроить для каждой рабочей нагрузки политики безопасности на основе контекста приложений и пользователей. Это обеспечивает незамедлительное реагирование на угрозы, возникающие внутри ЦОД, и применение политик безопасности на всех уровнях, вплоть до отдельного приложения. Угрозы, проникшие сквозь защиту периметра, не смогут горизонтально перемещаться внутри ЦОД, в отличие от традиционных сетей.

Автоматизация

В VMware NSX Data Center реализована виртуализация всех служб сети и безопасности, что помогает ускорить развертывание и согласованно автоматизировать весь жизненный цикл традиционных и новых приложений в различных средах и облаках. Автоматизация трудоемких задач, развертывания новых облачных приложений и текущей эксплуатации дает ИТ-отделам и разработчикам возможность реагировать на быстро меняющиеся потребности бизнеса.

Сети для сред на базе нескольких облаков

NSX Data Center абстрагирует сеть от физического оборудования, поэтому политики сети и безопасности связаны с соответствующими рабочими нагрузками. ИТ-отделы без труда могут полностью реплицировать среды приложений в удаленные ЦОД для аварийного восстановления, быстро перемещать рабочие нагрузки между центрами обработки данных и развертывать их в гибридных облачных средах — все это за считаные минуты, без прерывания работы приложений и взаимодействия с физической сетью.

Службы сети и безопасности для облачных приложений

VMware NSX Data Center предоставляет полноценный стек служб сети и безопасности для приложений в контейнерах и микрослужб, обеспечивая гибкое применение политик на уровне контейнеров при разработке новых приложений. Благодаря этому организации могут создать встроенные сети уровня 3 между контейнерами, реализовать микросегментацию для микрослужб и обеспечить комплексную визуализацию политик сети и безопасности для традиционных и новых приложений.

Редакции VMware NSX Data Center

Standard

Для организаций, которым требуются адаптивность и автоматизация сети.

Professional

Для организаций, которым требуются возможности редакции Standard и микросегментация и которые могут использовать конечные устройства общедоступного облака.

Advanced

Для организаций, которым требуются возможности редакции Professional, а также дополнительные службы сети и безопасности, интеграция с обширной экосистемой партнеров и возможность использования нескольких сред.

Enterprise Plus

Для организаций, которым требуются все самые эффективные возможности NSX Data Center, а также визуализация сети, средства безопасности (vRealize Network Insight™) и мобильность гибридного облака (NSX Hybrid Connect).

ROBO

Для организаций, которым требуется виртуализировать службы сети и безопасности для приложений в удаленном офисе или филиале.

	STANDARD	PROFESSIONAL	ADVANCED	ENTERPRISE PLUS	ROBO
NSX DATA CENTER[1]					
Распределенная коммутация и маршрутизация	•	•	•	•	•[5]
Брандмауэр NSX Edge	•	•	•	•	•
Служба преобразования сетевых адресов NSX Edge	•	•	•	•	•
Программный мост уровня 2 с физическими средами	•	•	•	•	
Динамическая маршрутизация на основе технологии ECMP (в режиме «активный-активный»)	•	•	•	•	•
Интеграция с платформами управления облаком[3]	•	•	•	•	•
Распределенный брандмауэр		•	•	•	•
VPN уровней 2 и 3		•	•	•	•
Интеграция с NSX Cloud[4]		•	•	•	•
Балансировка нагрузки с помощью NSX Edge			•	•	•
Интеграция с распределенным брандмауэром (Active Directory, AirWatch® и инициализация сторонних служб)			•	•	•
Application Rule Manager			•	•	•
Службы сети и безопасности контейнеров			•	•	
Сети и средства безопасности в нескольких средах			•	•	
Интеграция с аппаратными шлюзами			•	•	
Мониторинг конечных устройств				•	
Микросегментация с учетом контекста (идентификация приложений, RDSH)				•	
+vREALIZE NETWORK INSIGHT ADVANCED[2]					
Визуализация трафика (IPFIX) и мониторинг сети				•	
Планирование и администрирование брандмауэра				•	
Эксплуатация и устранение неполадок NSX				•	
+NSX HYBRID CONNECT ADVANCED[2]					
Крупномасштабный перенос рабочих нагрузок				•	
Оптимизация ГВС для переноса рабочих нагрузок				•	
Управление трафиком и нагрузкой по нескольким подключениям				•	

[1] Подробное описание возможностей см. в статьях базы знаний, посвященных возможностям NSX Data Center для vSphere и NSX-T™ Data Center.

[2] В состав NSX Data Center Enterprise Plus входят полные версии vRealize Network Insight Advanced и NSX Hybrid Connect Advanced.

[3] Только интеграция уровней 2, 3 и NSX Edge. Без групп безопасности.

[4] Для поддержки рабочих нагрузок общедоступного облака требуется подписка NSX Cloud.

[5] Только коммутация с поддержкой виртуальной локальной сети.

vmware®

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