VMWARE NSX

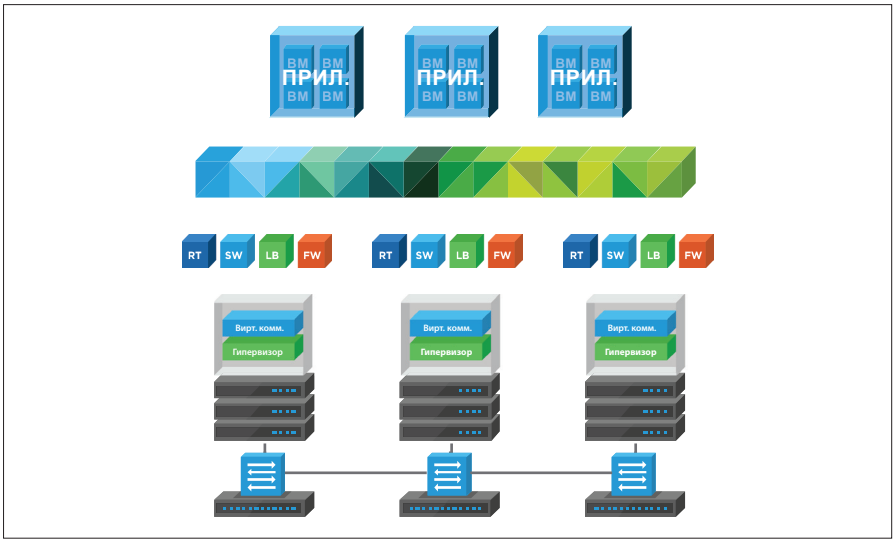
Платформа виртуализации сети

КРАТКОЕ ОПИСАНИЕ

VMware NSX® — это платформа виртуализации сети для программного центра обработки данных, реализующая эксплуатационную модель виртуальных машин для сети. При использовании NSX такие сетевые задачи, как коммутация, маршрутизация и защита трафика с помощью брандмауэров, распределенно выполняются во всей среде гипервизором. Фактически это «сетевой гипервизор», который выполняет роль платформы для виртуальных сетей и служб. Аналогично виртуальным машинам, инициализация виртуальных сетей и управление ими осуществляются программным способом, независимо от базового оборудования. NSX воспроизводит полную модель сети программным образом, что помогает за секунды создавать и инициализировать любые сетевые топологии: от базовых до сложных многоуровневых. Используя сочетания служб NSX для создания безопасных сред, пользователи могут развертывать множество виртуальных сетей с различными требованиями.

ОСНОВНЫЕ ПРЕИМУЩЕСТВА

- Микросегментация и гибкие политики безопасности, применяемые к отдельным рабочим нагрузкам.
- Сокращение времени инициализации сети с нескольких дней до нескольких секунд, более высокая эксплуатационная эффективность в результате автоматизации.
- Возможности переноса рабочих нагрузок между центрами обработки данных и внутри них, независимо от топологии физической сети.
- Улучшенная система безопасности и расширенные сетевые службы на основе экосистемы решений, созданных ведущими сторонними поставщиками.



Виртуализация сети и программный ЦОД

VMware NSX воплощает инновационную эксплуатационную модель сети, которая составляет основу для программного ЦОД. Благодаря программному подходу к созданию сетей платформа NSX помогает администраторам ЦОД реализовать новые уровни адаптивности, безопасности и рентабельности, которые были недостижимы при использовании физических сетей. NSX 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. Развертывание виртуальных сетей выполняется без нарушения работы пользователей на любом существующем сетевом оборудовании.

Основные компоненты NSX

Коммутация (SW)	Логическое наложение уровня 2 обеспечивается по всей коммутируемой матрице уровня 3 внутри и вне ЦОД. Поддержка наложения сетей на основе VXLAN.
Маршрутизация (RT)	Динамическая маршрутизация между виртуальными сетями выполняется распределенно ядром гипервизора; поддерживается горизонтальное масштабирование с аварийным переключением типа «активный-активный» на физические маршрутизаторы. Поддерживаются протоколы статической и динамической маршрутизации (OSPF, BGP).
Распределенный брандмауэр (FW)	Распределенные службы брандмауэра с сохранением состояния, встроенные в ядро гипервизора, с пропускной способностью до 20 Гбит/с на сервер гипервизора. Поддержка Active Directory и мониторинга действий. Кроме того, NSX обеспечивает вертикальный брандмауэр с помощью NSX Edge™.

Балансировка нагрузки (LB)	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 по VPN и VPN-подключение типа «среда-среда», VPN без управления для служб облачных шлюзов.
Шлюз NSX	Поддержка мостов между сетями VXLAN и VLAN обеспечивает оптимальное подключение к физическим рабочим нагрузкам. Эта возможность встроена в платформу NSX, а также поддерживается надстоечными коммутаторами, поставляемыми партнерами по экосистеме.
API-интерфейс NSX	Поддерживаются API-интерфейсы на базе REST для интеграции с любыми платформами управления облаком или специализированными средствами автоматизации.
Эксплуатация	Встроенные возможности управления процессами, такие как центральная командная строка, 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 NSX, как управление правилами для приложений 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.
Динамическая политика безопасности	С помощью NSX Service Composer можно создавать динамические группы безопасности. Чтобы повысить эффективность применения динамических групп безопасности, добавление в них можно осуществлять как на основе IP- или MAC-адреса, так и на основе объектов и меток VMware vCenter™, типа операционной системы и ролей Active Directory.
Управление облаком	Встроенная интеграция с vRealize Automation™ и OpenStack.
Интеграция со сторонними партнерскими решениями	Поддерживается интеграция служб управления, плоскости управления и плоскости данных сторонних поставщиков в широком спектре категорий, таких как брандмауэры следующего поколения, IDS/IPS, антивирусы без агентов, контроллеры предоставления приложений, коммутаторы, процессы, средства визуализации, усовершенствованные системы безопасности и т. д.
Сеть и безопасность для нескольких серверов vCenter	Расширение возможностей работы сети и обеспечения безопасности на несколько серверов vCenter и центров обработки данных, независимо от базовой физической топологии (например, за счет аварийного восстановления и поддержки ЦОД типа «активный-активный»).
Управление журналами	Ускоренное устранение проблем благодаря дополнительным средствам визуализации vRealize Log Insight для NSX. Визуализация тенденций развития событий и запуск оповещений в режиме реального времени, а также другие возможности.

Сценарии использования

Безопасность

С помощью NSX можно разбить центр обработки данных компании на логические сегменты безопасности, вплоть до уровня отдельной рабочей нагрузки, независимо от ее подсети или виртуальной локальной сети. Затем ИТ-отделы могут настроить для каждой рабочей нагрузки политики и средства безопасности на основе динамических групп безопасности. В результате гарантируется незамедлительная реакция на угрозы, возникающие внутри ЦОД, и применение политик безопасности на всех уровнях, вплоть до отдельной виртуальной машины. В отличие от традиционных сетей, в данном случае вредоносное ПО, нарушившее защиту периметра, не сможет горизонтально перемещаться внутри ЦОД.

Автоматизация

Ранее инициализация сетей занимала много времени, требовала значительных расходов и выполнялась вручную, что вело к возникновению ошибок. С появлением NSX от всех этих недостатков удалось избавиться. В NSX сети создаются программным образом, что исключает «узкие места», связанные с аппаратными сетями.

Встроенная в NSX интеграция с платформами управления облаком, такими как vRealize Automation и OpenStack, обеспечивает расширенные возможности автоматизации.

Обеспечение непрерывной работы приложений

Поскольку в модели NSX сеть абстрагирована от физического оборудования, политики сети и безопасности связаны с соответствующими рабочими нагрузками. ИТ-отделы компаний могут без труда реплицировать среды приложений целиком в удаленные ЦОД при аварийном восстановлении, перемещать их между корпоративными ЦОД или проводить развертывание в гибридных облачных средах — все это за считаные минуты, без прерывания работы приложений и без взаимодействий с физической сетью.

Редакции VMware NSX

Новые предложения NSX соответствуют широкому спектру требований к виртуализации сети: практически любая компания найдет для себя подходящее решение для перехода к программному ЦОД.

Standard

Для организаций, которым требуется адаптивность и автоматизация сети.

Advanced

Для организаций, которым требуются возможности редакции Standard и более высокий уровень безопасности ЦОД, реализуемый с помощью микросегментации.

Enterprise

Для организаций, которым требуются возможности редакции Advanced и платформа для расширенных сетевых служб и служб безопасности для нескольких доменов.

ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ

Дополнительную информацию см. по адресу 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 http://www.vmware.com/ru/products или найдите уполномоченного торгового посредника на сайте VMware.

	STANDARD	ADVANCED	ENTERPRISE
Распределенная коммутация и маршрутизация	•	•	•
Брандмауэр NSX Edge	•	•	•
NAT	•	•	•
Программный мост уровня 2 с физической средой	•	•	•
Динамическая маршрутизация с ECMP (типа «активный-активный»)	•	•	•
Автоматизация на основе API-интерфейса	•	•	•
Интеграция с vRealize и OpenStack	•	•	•
Управление журналами с помощью vRealize Log Insight для NSX	•	•	•
Автоматизация политик безопасности с помощью vRealize		•	•
Балансировка нагрузки NSX Edge		•	•
Распределенный брандмауэр		•	•
Интеграция с Active Directory		•	•
Мониторинг активности серверов		•	•
Внедрение служб (интеграция со сторонними решениями)		•	•
Интеграция с VMware AirWatch®		•	•
Управление правилами для приложений		•	•
NSX для нескольких серверов vCenter			•
Оптимизация NSX в нескольких средах			•
VPN (IPSEC и SSL)			•
Удаленный шлюз			•
Интеграция с оборудованием конечного устройства туннеля VXLAN			•
Мониторинг конечных устройств			•

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.ru

1/17