VMWARE NSX

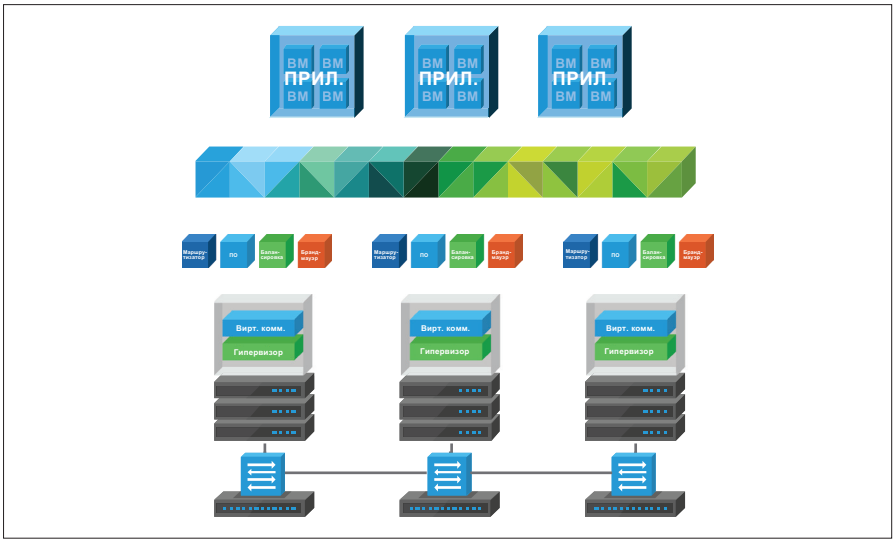
Платформа виртуализации и обеспечения безопасности сети

КРАТКОЕ ОПИСАНИЕ

VMware NSX® — это платформа виртуализации сети и обеспечения сетевой безопасности для программного ЦОД, которая дает возможность применить модель эксплуатации виртуальных машин к сети. При использовании NSX такие сетевые возможности, как коммутация, маршрутизация и защита трафика с помощью брандмауэров, встроены в гипервизор и распределяются по всей среде. Фактически это «сетевой гипервизор», который выполняет роль платформы для виртуальных сетевых служб и служб безопасности. 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 топологии сети: от базовых до сложных многоуровневых. Используя сочетания служб NSX, пользователи могут создавать в безопасных средах множество виртуальных сетей, отвечающих различным требованиям.

ОСНОВНЫЕ ПРЕИМУЩЕСТВА

- Микросегментация и гибкие политики безопасности, применяемые к отдельным рабочим нагрузкам.
- Сокращение времени инициализации сети с нескольких дней до нескольких секунд и повышение эксплуатационной эффективности за счет 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.



Виртуализация сети, система безопасности и программный ЦОД

VMware NSX реализует инновационную эксплуатационную модель сети, которая формирует основу для программного ЦОД. Благодаря программному подходу к созданию сетей платформа NSX помогает администраторам ЦОД достигать новых уровней адаптивности, безопасности и экономии, которые были немыслимы 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 на базе любой платформы управления облаком с помощью API-интерфейсов NSX. Развертывание виртуальных сетей выполняется без прерывания работы пользователей на любом существующем сетевом оборудовании.

Основные компоненты NSX

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	Распределенные службы брандмауэра с сохранением состояния, встроенные в ядро гипервизора, с пропускной способностью до 20 Гбит/с на узел гипервизора. Поддержка Active Directory и мониторинга действий. Кроме того, NSX обеспечивает 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. Этот компонент встроен в платформу NSX, а также поддерживается надстоечными коммутаторами, поставляемыми партнерами по экосистеме.
NSX API	Поддерживаются API-интерфейсы на базе RESTful для интеграции с любыми платформами управления облаком или пользовательскими системами автоматизации.
Эксплуатация	Встроенные возможности управления процессами, 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™, расширяет 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.
Микросегментация с учетом контекста	Платформа NSX 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 BM, 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.
Сеть и безопасность за пределами vCenter	Расширение служб сети и безопасности на несколько серверов vCenter и центров обработки данных, независимо от базовой физической топологии, чтобы обеспечить аварийное восстановление и развернуть центры обработки данных в режиме «активный-активный».
Управление журналами	Ускоренное устранение проблем благодаря дополнительным средствам визуализации vRealize Log Insight для NSX. Визуализация тенденций развития событий, создание оповещений и другие возможности в режиме реального времени.

Сценарии использования

Безопасность

С помощью NSX можно разделить 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 угрозы, проникшие сквозь защиту периметра, не смогут горизонтально перемещаться внутри ЦОД.

Автоматизация

Благодаря автоматизации трудоемких и подверженных ошибкам задач платформа NSX помогает решить такие проблемы, как длительная инициализация сетей, ошибки в конфигурациях и высокие расходы. В NSX сети создаются программным образом, что исключает «узкие места», типичные для физических сетей.

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

Обеспечение непрерывной работы приложений

Поскольку NSX абстрагирует сеть от физического оборудования, политики сети и безопасности связаны с соответствующими рабочими нагрузками. ИТ-отделы могут без труда полностью реплицировать среды приложений в удаленные ЦОД для аварийного восстановления, перемещать их между корпоративными ЦОД или развертывать в гибридных облачных средах — всё это за считаные минуты, без прерывания работы приложений и без взаимодействия с физической сетью.

Редакции VMware NSX

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, а также службы сети и система безопасности для нескольких доменов.

ROBO

Для организаций, которым требуется виртуализировать и защитить приложения в удаленном офисе или филиале

ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ

Дополнительную информацию см. на сайте 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	ROBO
Распределенная коммутация	•	•	•	•*
Распределенная маршрутизация	•	•	•	
Брандмауэр NSX Edge	•	•	•	•
Преобразование сетевых адресов	•	•	•	•
Программный мост между уровнем 2 и физической средой	•	•	•	
Динамическая маршрутизация с ECMP (в режиме «активный-активный»)	•	•	•	•
Автоматизация на основе API-интерфейсов	•	•	•	•
Интеграция с vRealize и OpenStack	•	•	•	•
Управление журналами с помощью vRealize Log Insight для NSX	•	•	•	•
Автоматизация политик безопасности с помощью vRealize		•	•	•
Балансировка нагрузки с помощью NSX Edge		•	•	•
Распределенный брандмауэр (с интеграцией 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			•	
Распределенный брандмауэр с поддержкой уровня 7			•	

* С поддержкой виртуальной локальной сети

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

1/18