VMware NSX Data Center

ОСНОВНЫЕ ПРЕИМУЩЕСТВА

- Защита приложений с помощью гибких политик безопасности и микросегментации на уровне рабочих нагрузок.
- Сокращение времени инициализации сети с нескольких дней до считаных секунд и повышение операционной эффективности благодаря автоматизации.
- Согласованное управление политиками сети и безопасности в центрах обработки данных и публичных облаках, а также между ними, независимо от топологии физической сети.
- Обеспечение подробной визуализации топологии приложений, автоматизированные рекомендации по политикам безопасности и непрерывный мониторинг потоков.
- Расширенная защита от распространения угроз в горизонтальном трафике с помощью полностью распределенной встроенной системы предотвращения угроз.

VMware NSX® Data Center — это платформа виртуализации и обеспечения безопасности сети, 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 решения партнеров — 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.

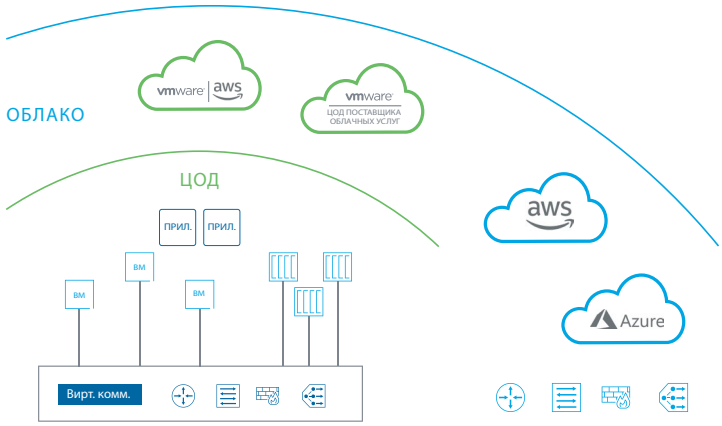

РИС. 1. Платформа виртуализации и обеспечения безопасности сети NSX Data Center

Программная реализация сети

VMware NSX Data Center предоставляет инновационную эксплуатационную модель сети, которая реализуется в программном обеспечении, составляет основу для программно-определяемого ЦОД и распространяется на виртуальную облачную сеть. Администраторы ЦОД теперь могут обеспечивать новые уровни адаптивности, безопасности и экономии, которые были недостижимы, когда сеть ЦОД была привязана исключительно к физическому оборудованию. NSX Data Center предоставляет полный комплект элементов логической сетевой инфраструктуры, средств безопасности и служб, таких как логические коммутаторы, маршрутизаторы, брандмауэры, средства балансировки нагрузки, виртуальные частные сети (VPN), а также средства 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 имеющемся сетевом оборудовании. Такие сети могут охватывать ЦОД, публичные и частные облака, платформы контейнеров и аппаратные серверы.

Основные возможности

Коммутация	Логическое наложение уровня 2 обеспечивается по всей коммутируемой матрице уровня 3 внутри и за пределами ЦОД. Поддержка наложения сетей на основе VXLAN и GENEVE.
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, в том числе IPv6.
Брандмауэр шлюза	Брандмауэр с сохранением состояния вплоть до уровня 7 (включая идентификацию приложений и распределенные разрешенные списки полностью определенных доменных имен), встроенный в шлюз NSX и распределенный по всей инфраструктуре с централизованной политикой и управлением.
Распределенный брандмауэр	Брандмауэр с сохранением состояния вплоть до уровня 7 (включая идентификацию приложений и распределенные разрешенные списки полностью определенных доменных имен), встроенный в ядро гипервизора и распределенный по всей инфраструктуре с централизованной политикой и управлением. Кроме того, распределенный брандмауэр NSX интегрируется непосредственно с облачными платформами, такими как Kubernetes и Pivotal Cloud Foundry, публичными облаками (например, AWS и Azure) и аппаратными серверами.
Балансировка нагрузки	Балансировка нагрузки для уровней 4–7 с переносом нагрузок SSL и сквозной передачей, средства проверки работоспособности сервера (в том числе средства пассивной проверки работоспособности) и правила для приложений обеспечивают возможности программирования и манипулирования трафиком с помощью графического пользовательского интерфейса или API-интерфейса.
VPN	Удаленный доступ через VPN и VPN-подключение типа «среда-среда», неуправляемая сеть VPN для служб облачных шлюзов.
Шлюз NSX	Возможность создания моста между виртуальными локальными сетями, настроенными на базе физических сетей, и наложенными сетями NSX обеспечивает стабильное подключение между виртуальными и физическими рабочими нагрузками.
NSX Intelligence™	NSX Intelligence предоставляет автоматизированные рекомендации по политикам безопасности, а также обеспечивает непрерывный мониторинг и визуализацию всех потоков сетевого трафика для улучшения отслеживания. Это гарантирует широкие возможности и удобство аудита системы безопасности. Решение NSX Intelligence входит в состав того же пользовательского интерфейса, что и NSX-T™ Data Center, и предоставляет единую консоль управления для рабочих групп по управлению сетью и безопасностью.
Распределенная система предотвращения угроз NSX (NSX Distributed IDS/IPS[1])	NSX Distributed IDS/IPS™ — это передовая система обнаружения угроз, предназначенная для выявления их горизонтального распространения в трафике. Уникальная распределенная архитектура в сочетании с точным контекстом приложений позволяет рабочим группам по безопасности заменять отдельные устройства, обеспечивать соответствие законодательству и создавать виртуальные зоны безопасности без физического разделения инфраструктуры.
Объединение	Централизованная настройка политик и их применение в разных точках из единой консоли управления обеспечивает согласованность политик во всей сети, удобство эксплуатации и упрощение архитектуры аварийного восстановления.
Виртуальная маршрутизация и переадресация (VRF)	Полная изоляция арендаторов в плоскости данных благодаря отдельным таблицам маршрутизации, поддержке NAT и брандмауэров периметра в каждом экземпляре VRF в шлюзе NSX нулевого уровня.
API-интерфейсы NSX Data Center	Поддерживаются API-интерфейсы REST на базе JSON для интеграции с платформами управления облаком, средствами автоматизации DevOps и пользовательскими системами автоматизации.
Эксплуатация	Встроенные возможности управления эксплуатацией, такие как центральный интерфейс командной строки, трассировка, наложенный логический анализатор SPAN и IPFIX, облегчают устранение неполадок и помогают проводить упреждающий мониторинг инфраструктуры виртуальной сети. Интеграция с такими средствами, как VMware vRealize® Network Insight™, обеспечивает расширенный анализ и устранение неполадок.

Микросегментация с учетом контекста	Группы и политики безопасности можно создавать динамически и обновлять автоматически на основе атрибутов, которые не ограничиваются IP-адресами, портами и протоколами, а включают в себя и такие элементы, как имя компьютера и теги, тип операционной системы и сведения о приложениях уровня 7. Такой подход обеспечивает применение политики адаптивной микросегментации. Политики на основе сведений об учетных данных из Active Directory и других источников обеспечивают безопасность на уровне пользователя (вплоть до отдельных сеансов пользователей) в службах удаленных рабочих столов и в инфраструктуре виртуальных рабочих мест.
Автоматизация и управление облаком	Полная интеграция с vRealize Automation™ / vRealize Automation Cloud™, OpenStack и т. д. Полная поддержка интеграции с Ansible Module, Terraform Provider и PowerShell.
Интеграция со сторонними партнерскими решениями	Поддерживается интеграция служб управления, плоскости контроля и плоскости данных с решениями сторонних поставщиков в широком спектре категорий, таких как брандмауэры нового поколения, системы обнаружения и предотвращения вторжений, безагентные антивирусы, коммутаторы, управление процессами, средства визуализации, усовершенствованные системы безопасности и т. д.
Сеть и система безопасности в многооблачной среде	Обеспечивается согласованность сети и системы безопасности между средами нескольких ЦОД, а также в различных частных и публичных облаках, независимо от базовой физической топологии или облачной платформы.
Сеть и система безопасности для контейнеров	Поддерживаются балансировка нагрузки, микросегментация (распределенный брандмауэр), маршрутизация и коммутация для контейнеров на платформах на базе Kubernetes и Cloud Foundry, которые работают на BM или аппаратных узлах. Обеспечивается визуализация сетевого трафика для контейнеров (логические порты, SPAN/Mi, IPFIX и трассировка).

Сценарии использования

Безопасность

NSX Data Center повышает доступность и эффективность использования модели безопасности нулевого доверия для приложений в средах частных и публичных облаков. NSX Data Center дает возможность использовать микросегментацию, чтобы определять и применять политику безопасности сети на уровне отдельных рабочих нагрузок для различных целей: обеспечения защиты важных приложений, создания логической демилитаризованной зоны в ПО или уменьшения площади атаки в среде виртуальных рабочих мест.

Сети для многооблачных сред

NSX Data Center — это решение для виртуализации сети, которое обеспечивает согласованность параметров сети и системы безопасности в разнородных средах, чтобы оптимизировать эксплуатацию многооблачной среды. Благодаря этому NSX Data Center подходит для сценариев использования в многооблачных средах: от удобного расширения ЦОД до объединения нескольких ЦОД в пулы и быстрого переноса рабочих нагрузок.

Автоматизация

Благодаря виртуализации служб сети и безопасности NSX Data Center обеспечивает быструю инициализацию и развертывание полностековых приложений, устраняя сложности, связанные с управлением службами и политиками сети и безопасности вручную. NSX Data Center полностью интегрируется с платформами управления облаком и другими средствами автоматизации, такими как vRealize Automation / vRealize Automation Cloud, OpenStack, Terraform, Ansible и т. д., чтобы предоставить разработчикам и ИТ-отделам возможности для инициализации, развертывания и администрирования приложений в соответствии с темпом развития бизнеса.

Сеть и система безопасности для облачных приложений

NSX Data Center предоставляет полный интегрированный 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 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 требуется адаптивная и автоматизированная сеть.

Professional

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

Advanced

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

Enterprise Plus

Для организаций, которым требуются все самые эффективные возможности NSX Data Center, а также сетевые процессы vRealize Network Insight, VMware HCX® для мобильности гибридного облака, визуализация потока сетевого трафика и процессы обеспечения безопасности NSX Intelligence.

Remote Office Branch Office (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[2]					
Распределенная коммутация и маршрутизация	•	•	•	•	•[6]
Брандмауэр шлюза NSX (с сохранением состояния)	•	•	•	•	•
Служба NAT шлюза NSX	•	•	•	•	•
Программный мост уровня 2 с физическими средами	•	•	•	•	
Динамическая маршрутизация на основе технологии ECMP (в режиме «активный-активный»)	•	•	•	•	•
Интеграция с платформами управления облаком[3]	•	•	•	•	•
IPv6 со статической маршрутизацией и статическое распределение адресов IPv6	•	•	•	•	
Распределенный брандмауэр для ВМ и рабочих нагрузок, которые обрабатываются в аппаратной инфраструктуре		•	•	•	•
VPN уровней 2 и 3		•	•	•	•
Интеграция с NSX Cloud™[4] для поддержки AWS и Azure		•	•	•	•
Балансировка нагрузки			•	•	•
Интеграция с распределенным брандмауэром (Active Directory, VMware AirWatch®, защита конечных устройств и внедрение сторонних служб)			•	•	•
Сеть и система безопасности для контейнеров			•	•	
Несколько экземпляров vCenter® для управления сетью и системой безопасности			•	•	
IPv6-адрес с динамической маршрутизацией, динамическое распределение адресов IPv6 и службы			•	•	
Микросегментация с учетом контекста (идентификация приложений уровня 7, RDSH, анализатор протоколов)			•	•	
Распределенные разрешенные списки полностью определенных доменных имен			•	•	
NSX Distributed IDS/IPS[1]			•	•	
Виртуальная маршрутизация и переадресация (VRF шлюза нулевого уровня)			•	•	
Объединение				•	

	STANDARD	PROFESSIONAL	ADVANCED	ENTERPRISE PLUS	ROBO
NSX INTELLIGENCE					
Анализ потоков трафика между ВМ				•	
Визуализация брандмауэра				•	
Автоматизированная политика безопасности				•	
Анализ правил и групповых рекомендаций				•	
vRealize Network Insight Advanced[5]				•	
VMware HCX Advanced[5]				•	

1. Для использования NSX Distributed IDS/IPS необходима дополнительная подписка. Обратите внимание: NSX-T 3.0 предоставляет только функции IDS.
2. Подробное описание возможностей см. в статьях базы знаний, посвященных функциям NSX Data Center for vSphere® и NSX-T Data Center, в том числе в статье *Product Offerings for NSX-T Data Center 3.0* («Продукты для NSX-T Data Center 3.0») с актуальными сведениями.
3. Только интеграция уровней 2, 3 и шлюз NSX. Без групп безопасности.
4. Для поддержки рабочих нагрузок публичного облака требуется подписка NSX Cloud.
5. В состав NSX Data Center Enterprise Plus входят полные версии vRealize Network Insight Advanced и VMware HCX Advanced. Дополнительные сведения см. в *техническом проспекте vRealize Network Insight* и *техническом проспекте HCX*.
6. Только коммутация 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