# VMWARE NSX CLOUD

## Согласованные параметры сети и системы безопасности для приложений, выполняемых в общедоступных облаках

### КРАТКОЕ ОПИСАНИЕ

VMware NSX® Cloud предоставляет согласованные сетевые средства и обеспечивает безопасность приложений в общедоступном облаке. В NSX Cloud используются те же плоскости контроля и управления, что и в NSX Data Center, благодаря чему заказчики получают единое решение для создания сети и обеспечения безопасности — от частного ЦОД до общедоступного облака.

### ОСНОВНЫЕ ПРЕИМУЩЕСТВА

Единые службы сети и безопасности в общедоступных облаках, таких как AWS и Azure, значительно улучшают масштабируемость, управление и визуализацию, а также снижают эксплуатационные расходы.

- Удобное масштабирование в различных виртуальных сетях, зонах доступности, регионах и общедоступных облаках.
- Точный контроль над службами сети и безопасности обеспечивает защиту и стандартизацию приложений.
- Комплексная визуализация сети и системы безопасности обеспечивают работоспособность приложений и их соответствие нормативным требованиям в общедоступных облаках.

### ЦЕНЫ

- Модель ценообразования на основе подписок (доступны лицензии на один год и три года)
- Расчет цен на основе числа виртуальных процессоров, которые используют активные рабочие нагрузки в общедоступном облаке, независимо от количества виртуальных сетей (например, AWS VPC и Azure VNets)
- Для использования только в облаке лицензия NSX Data Center не требуется

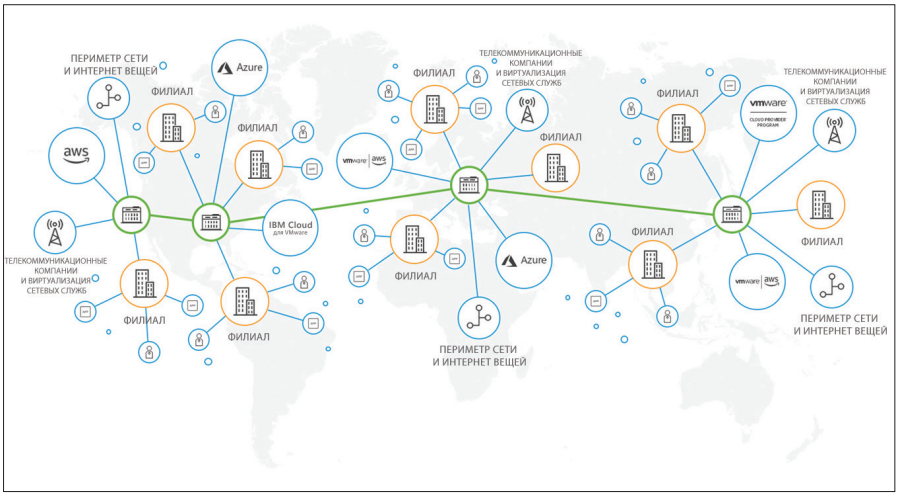


**Рис. 1. Виртуальная облачная сеть**

## Сеть, созданная для облака

VMware NSX Cloud предоставляет согласованные службы сети и безопасности для приложений, выполняемых в общедоступных облаках. При использовании с продуктами VMware NSX решение VMware NSX Cloud помогает реализовать виртуальную облачную сеть — программную платформу для создания и эксплуатации сети, охватывающую центры обработки данных, облака, конечные устройства и элементы Интернета вещей.

## Сценарии использования

### Согласованная система безопасности в различных облаках

NSX Cloud обеспечивает применение политик к рабочим нагрузкам в различных общедоступных облаках. В NSX Cloud используются те же плоскости управления и данных, что и в NSX Data Center, благодаря чему заказчики получают возможность комплексного управления политиками в центрах обработки данных и облаках. Политика настраивается один раз и применяется к любым рабочим нагрузкам — в виртуальных облачных сетях, разных регионах, зонах доступности и средах различных поставщиков облачных услуг. Политики безопасности применяются динамически к каждой рабочей нагрузке на основе ее атрибутов и определенных пользователем меток. Скомпрометированные рабочие нагрузки можно автоматически переводить в режим карантина, если к ним не применяется политика безопасности на основе микросегментации.

### Точное управление облачными сетевыми ресурсами

Платформа VMware NSX Cloud создана для сред общедоступного облака, таких как Amazon (AWS) и Microsoft Azure. NSX Cloud дополняет услуги, предоставляемые этими поставщиками общедоступного облака. Благодаря NSX Cloud организации могут продолжать без ограничений использовать инфраструктуру и службы приложений поставщика общедоступного облака (например, AWS ELB и Azure Load Balancer, AWS Route53 и Azure DNS, AWS Direct Connect и Azure ExpressRoute, Amazon RDS и Azure Database) для рабочих нагрузок. Инициализацию и управление конфигурациями можно автоматизировать с помощью запросов к API-интерфейсам REST, используя имеющиеся средства автоматизации.

**ДЛЯ ПОЛУЧЕНИЯ ИНФОРМАЦИИ ИЛИ ПРИОБРЕТЕНИЯ ПРОДУКТОВ VMWARE**

**ОБРАЩАЙТЕСЬ ПО ТЕЛЕФОНУ**
+7 (495) 212–2900,

**ПОСЕТИТЕ СТРАНИЦУ**
www.vmware.com/ru/products/nsx-cloud.html или http://www.vmware.com/ru/products для поиска уполномоченного торгового посредника.

**Комплексные управление эксплуатацией и визуализация**

VMware NSX Cloud предоставляет стандартные интерфейсы и протоколы для доступа к данным служб сети и безопасности из облачных сетей. Сведения о потоках, пакетах и событиях можно получить с помощью IPFIX, Traceflow, Port Mirroring и Syslog. Эти данные можно передать существующим локальным средствам эксплуатации и использовать для обеспечения комплексной визуализации для мониторинга, устранения неполадок и аудита. Подробные данные об эксплуатации значительно ускоряют выявление и устранение проблем сетевого подключения, производительности и безопасности во всей среде гибридного облака, в том числе в локальной среде и общедоступном облаке.

## Основные возможности

**Среды на базе нескольких облаков, службы сети и безопасности для нескольких сред.** NSX Cloud реализует службы сети и безопасности для конечных устройств в различных облаках и за счет интеграции с NSX Data Center помогает организациям управлять сетями и системой безопасности вместе с облаками и средами ЦОД.

**Микросегментация.** Управление горизонтальным трафиком между приложениями, которые выполняются в общедоступных облаках.

**Группы безопасности.** Группы и правила безопасности можно настраивать на основе расширенных параметров политик, таких как имя экземпляра, тип ОС, идентификатор AMI и определяемые пользователем метки.

**Динамическая политика.** Политика безопасности применяется автоматически на основе атрибутов рабочей нагрузки и определенных пользователем меток. Политики автоматически переносятся вместе с рабочими нагрузками при их перемещении в пределах облака или между облаками.

**Рабочие нагрузки в карантине.** Скомпрометированные рабочие нагрузки, выполняемые в общедоступном облаке, можно переводить в режим карантина без использования микросегментации. Экземплярам в режиме карантина запрещается взаимодействие по облачной сети.

**Распределенная архитектура.** Распределенная архитектура брандмауэра NSX Cloud снижает число дополнительных сетевых узлов и объема трафика, так как политики принудительно применяются в виртуальном сетевом адаптере каждого экземпляра, а не перенаправляются через внешний брандмауэр.

**Брандмауэр на границе сети.** NSX Cloud предоставляет брандмауэр с сохранением состояния, который фильтрует вертикальный трафик между рабочими нагрузками в виртуальных сетях и общедоступном Интернете.

**API-интерфейс на базе RESTful.** API-интерфейс на базе RESTful и средства автоматизации помогают программными средствами инициализировать и настраивать инфраструктуру сети и безопасности по требованию.

**Шаблоны.** Использование существующих средств автоматизации и управления для создания стандартизированных шаблонов приложений и упрощения инициализации и администрирования служб сети и безопасности в различных общедоступных облаках.

**Визуализация горизонтального трафика.** Использование существующих средств эксплуатации для визуализации горизонтального трафика как в пределах виртуального частного облака, так и между облаками.

**Журналы системы безопасности.** Визуализация и аудит событий безопасности, таких как предоставление доступа, отказ в доступе и перевод экземпляров в режим карантина, в режиме реального времени. Передача данных событий безопасности на сервер Syslog или SIEM.

**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