МИКРОСЕГМЕНТАЦИЯ С УЧЕТОМ КОНТЕКСТА С ПОМОЩЬЮ VMWARE NSX DATA CENTER

Защита сети от горизонтального распространения угроз

Современные приложения — это сложные, распределенные и динамические системы

Каждая организация пытается решить, как ей работать в эпоху повсеместного подключения к сети, когда приложения и данные играют первостепенную роль. Современные приложения распределены по нескольким ЦОД и облакам и достигают границы среды.

Виртуализация, а также распространение микрослужб и интегрированных процессов разработки и эксплуатации ускорили создание и изменение приложений. Распределенный характер современных приложений и скорость их изменения значительно усложняют обеспечение безопасности.

Традиционные стратегии обеспечения безопасности больше не эффективны

Число приложений продолжает расти, поэтому традиционные подходы к обеспечению безопасности, ориентированные на периметр, не могут гарантировать защиту приложений и данных. Злоумышленники доказали, что могут обойти любые средства обеспечения безопасности периметра. Преодолев защиту, они начинают беспрепятственно двигаться горизонтально, с сервера не сервер, в поисках информации для кражи или требования выкупа.

В мире современных распределенных приложений отделы по ИТ-безопасности и обслуживанию сети часто сталкиваются с необходимостью поддерживать разрозненные политики безопасности в различных компонентах среды, что приводит к ослаблению общего уровня защиты.

Согласованная система безопасности в ЦОД, облаке и на границе сети

VMware NSX® Data Center помогает настраивать согласованные политики безопасности для всей среды, независимо от типа приложения или точки его развертывания. Политики принудительно применяются на уровне отдельных рабочих нагрузок, что обеспечивает сегментацию рабочих нагрузок, размещенных на одном физическом узле, без перенаправления пакетов через внешний физический или виртуальный брандмауэр. Такой гибкий уровень безопасности называют микросегментацией.

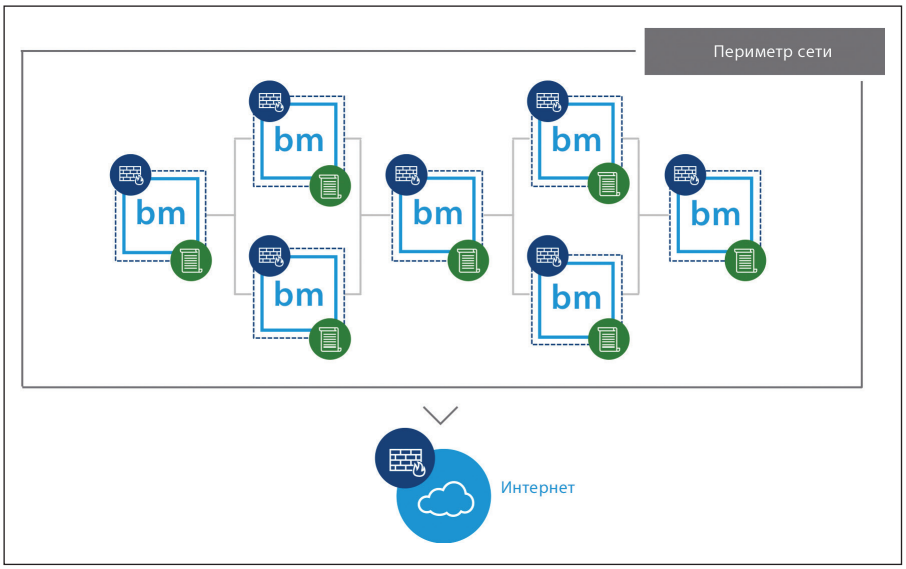

Рис. 1. Микросегментация подразумевает применение политик безопасности сети на уровне отдельных рабочих нагрузок.

«Учитывая рост числа устройств Интернета вещей, необходимо повышать уровень сегментации сети... Это ограничивает возможность горизонтального распространения угроз в ЦОД».

— КРИСТОФЕР ФРЕНЦ (CHRISTOPHER FRENZ)
ДИРЕКТОР ПО ИНФРАСТРУКТУРЕ
INTERFAITH MEDICAL CENTER

ОСНОВНЫЕ ФАКТЫ

- Из-за распределенного и динамичного характера современных приложений традиционные системы безопасности, ориентированные на периметр, не могут гарантировать надежную защиту.
- VMware NSX Data Center реализует микросегментацию для защиты приложений от горизонтального распространения угроз.
- Политики безопасности определяются на основе контекста приложения и применяются к отдельным рабочим нагрузкам.
- Безопасность обеспечивается согласованно в ЦОД, облаке и на границе сети.

Микросегменты, созданные с помощью NSX Data Center, определяются и администрируются в ПО, что делает их адаптивными и дает возможность их автоматизировать. К новым рабочим нагрузкам автоматически применяются политики безопасности, которые сохраняются в течение всего жизненного цикла рабочей нагрузки, независимо от точки ее инициализации или перемещения.

Микросегментация с учетом контекста: система безопасности, ориентированная на приложения и данные

Возможность настраивать политики безопасности на основе наиболее существенных аспектов столь же важна, как и согласованное применение политик. NSX Data Center отделяет политики безопасности от статичных сетевых атрибутов, таких как IP-адрес, порт и протокол, и дает возможность настраивать политики в зависимости от контекста приложения и инфраструктуры. Такой контекст включает в себя атрибуты пользователя и учетных данных, атрибуты рабочих нагрузок (например, операционную систему) и даже степени соответствия нормативным требованиям.

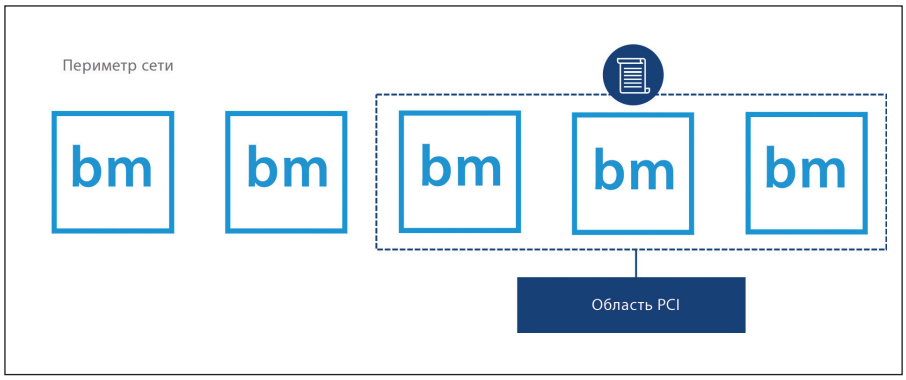

Рис. 2. Микросегменты в NSX Data Center можно определять на основе различных видов контекста, в том числе с учетом степени соответствия нормативным требованиям.

Благодаря микросегментации с учетом контекста, реализуемой с помощью NSX Data Center, группы по обеспечению безопасности сети получают необходимую гибкость для защиты приложений и данных на основе самых важных факторов. Например, NSX Data Center можно использовать для защиты инфраструктуры виртуальных компьютеров за счет принудительного применения сетевой политики на основе контекста пользователя вплоть до уровня отдельного сеанса RDSH. Кроме того, политики безопасности можно применять ко всем рабочим нагрузкам, которые относятся к стандартам безопасности данных для платежных карт, независимо от точки их размещения в среде.

Расширенные службы безопасности только там, где это необходимо

NSX Data Center поддерживает добавление расширенных сторонних служб безопасности в заданном микросегменте. Вместо маршрутизации всего сетевого трафика через физическое или виртуальное устройство, такое как брандмауэр нового поколения, система обнаружения или предотвращения вторжений, NSX Data Center может динамически направлять определенный трафик этим службам на уровне виртуальной сети. Это помогает добавлять расширенные службы безопасности в нужное время и в нужных расположениях, повышает эффективность передачи сетевого трафика и самих служб безопасности.

Визуализация сетевого трафика во всей среде

Первый шаг к микросегментации — понимание потоков сетевого трафика в существующей среде. VMware Network Insight™ обеспечивает комплексное представление всего сетевого трафика в ЦОД, в том числе трафика физических и виртуальных сетей. После анализа трафика VMware Network Insight автоматически рекомендует политики микросегментации, которые можно реализовать в NSX Data Center.

Начните внедрение микросегментации с помощью бесплатной оценки виртуальной сети, которая поможет проанализировать существующий сетевой трафик и начать планирование проекта микросегментации. Дополнительные сведения см. на странице www.vmware.com/ru/products/nsx/security.

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