VMware NSX для Horizon

КРАТКОЕ ОПИСАНИЕ

VMware NSX™ для Horizon® обеспечивает быстрое и удобное управление сетью в среде VDI. Благодаря этому решению ИТ-администраторы могут мгновенно создавать динамические политики, которые следуют за виртуальными компьютерами, без трудоемкой инициализации сетевых ресурсов. VMware NSX для Horizon распространяет возможности политик безопасности с ЦОД на виртуальные компьютеры и приложения и предоставляет расширяемую платформу, которая интегрируется с ведущими в отрасли решениями для обеспечения безопасности.

ПРЕИМУЩЕСТВА

- Повышенная безопасность виртуальных компьютеров, размещенных в ЦОД вместе с другими рабочими нагрузками.
- Быстрое и удобное управление политиками сетей и безопасности для пользователей на основе логических групп, ролей или меток.
- Автоматическая привязка политики к виртуальному компьютеру при его создании; политика следует за виртуальной машиной независимо от ее размещения в базовой инфраструктуре.
- Интеграция с ведущими в отрасли службами обеспечения безопасности нового поколения и решениями для защиты от вирусов и вредоносных программ, а также предотвращения вторжений.

Сеть и система безопасности для виртуальных компьютеров и приложений: производительность, удобство, возможности расширения

Многие организации виртуализируют настольные компьютеры и приложения для повышения безопасности клиентской вычислительной среды и обеспечения мобильности бизнеса. Централизация виртуальных компьютеров и приложений обеспечивает защиту данных на хранении, предотвращает несанкционированный доступ к приложениям и предоставляет эффективные способы установки исправлений, обновлений и обслуживания образов.

Однако виртуализация настольных компьютеров и приложений приводит к новым проблемам безопасности даже за брандмауэром ЦОД, где размещены сотни или даже тысячи виртуальных компьютеров. Эти виртуальные компьютеры непосредственно связаны с рабочими нагрузками пользователей и другими важными нагрузками, и любая проблема делает их уязвимыми для вредоносных программ и прочих атак. Эти атаки могут распространиться с виртуального компьютера на сервер, что увеличивает площадь для атак в рамках ЦОД. Подобное «горизонтальное» распространение угроз — типичный сценарий, затрагивающий многих заказчиков, особенно тех, которые обязаны соблюдать высочайшие требования к безопасности и обеспечению соответствия нормативным требованиям.

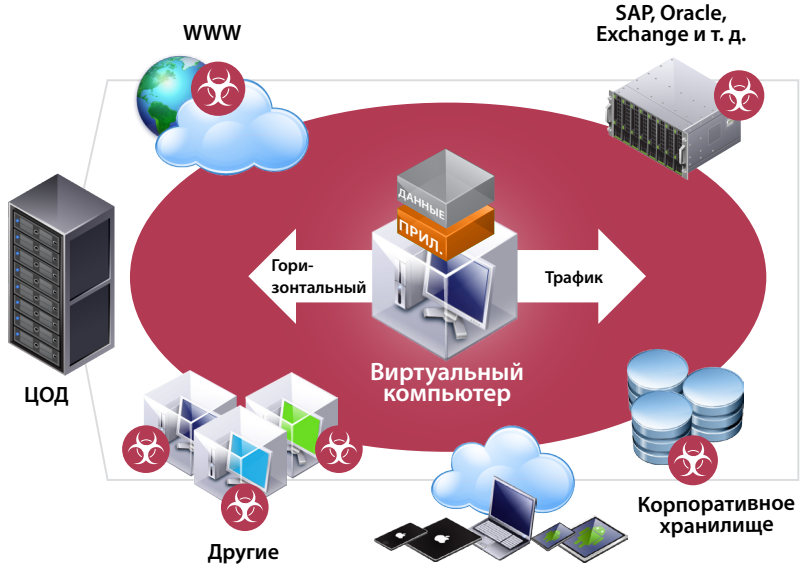

Рис. 1. Проблемы защиты горизонтального трафика в ЦОД

Организации, заинтересованные в управлении сетевыми политиками и политиками безопасности, которые следуют за пользователями и рабочими нагрузками, как правило, вкладывают значительные средства в аппаратную архитектуру. Это ведет к повышению капитальных расходов, сложностям управления и медленной адаптации к динамическому развитию бизнес-среды.

VMware NSX для Horizon

VMware NSX для Horizon обеспечивает эффективную защиту горизонтального трафика в ЦОД, предоставляя ИТ-отделу средства для быстрого и удобного управления сетевыми политиками и политиками безопасности, которые следуют за виртуальными компьютерами и приложениями конечных пользователей независимо от расположения в инфраструктуре, используемого устройства и местоположения.

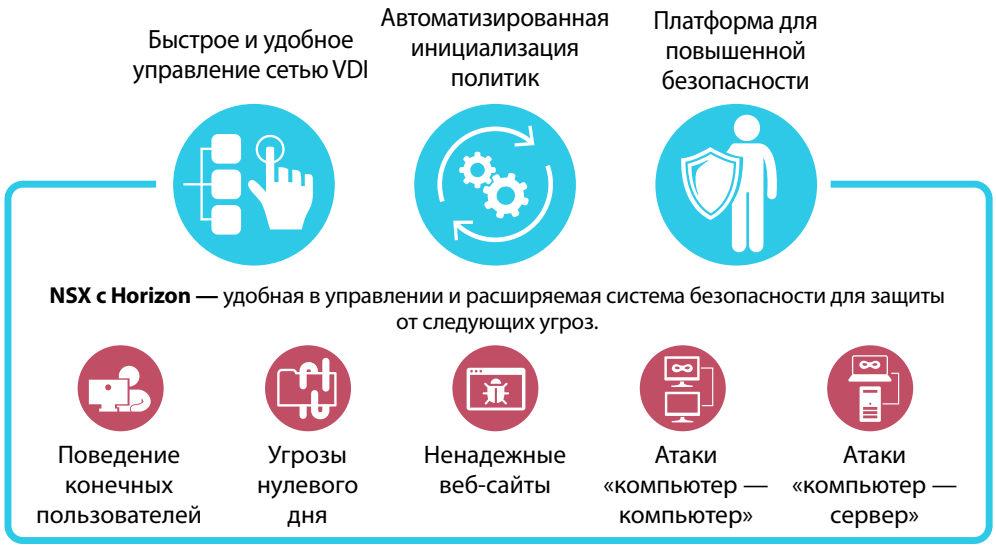

Рис. 2. NSX для Horizon обеспечивает удобство управления и расширяемость сети и системы безопасности для сред VDI

Используя это решение, организации могут воспользоваться преимуществами упрощенного и удобного управления сетями и системой безопасности в среде VDI. Благодаря этому решению ИТ-администраторы могут мгновенно создавать динамические политики, которые следуют за виртуальными компьютерами, без трудоемкой инициализации сетевых ресурсов.

Распространяя действие политик безопасности с ЦОД на виртуальные компьютеры и приложения, данное решение также предоставляет расширяемую платформу, которая интегрируется с экосистемой решений ведущих в отрасли партнеров VMware по обеспечению безопасности. В результате заказчики получают мощные средства комплексной защиты виртуальных компьютеров.

Принципы работы

VMware NSX для Horizon обеспечивает повышенную безопасность виртуальных компьютеров и защиту горизонтального трафика за счет централизованного определения политик. Политики распределяются на уровне гипервизора на каждом узле vSphere и автоматически привязываются к каждому виртуальному компьютеру при его создании. Чтобы защитить виртуальные компьютеры и связанные с ними рабочие нагрузки внутри периметра ЦОД, VMware NSX использует технологию микросегментации, которая обеспечивает защиту периметра каждого виртуального компьютера. Эта технология использует возможности распределенного виртуального брандмауэра VMware NSX для применения политик к входящему и исходящему трафику каждой виртуальной машины, что помогает избежать случаев несанкционированного доступа между виртуальными компьютерами и смежными рабочими нагрузками. При переносе виртуального компьютера с одного узла на другой или изменении его расположения в ЦОД присвоенная политика автоматически следует за ним.

Возможности и преимущества

VMware NSX для Horizon упрощает управление сетями VDI за счет динамических политик безопасности, которые следуют за конечными пользователями независимо от расположения в инфраструктуре, используемого устройства и местоположения.

Быстрое и удобное управление сетью VDI

Благодаря VMware NSX для Horizon администраторы могут создавать и изменять политики безопасности для всех виртуальных компьютеров, а также управлять ими всего несколькими щелчками мышью. Для ускорения развертывания виртуальных компьютеров можно быстро назначать политики безопасности группам пользователей. Путем развертывания виртуализированных сетевых служб (коммутаторов, маршрутизаторов, брандмауэров, средств балансировки нагрузки) администраторы могут создавать виртуальные сети в средах VDI, не обладая специальными знаниями в области виртуальных локальных сетей, списков управления доступом и синтаксиса настройки оборудования.

Автоматизированные динамические политики, следующие за конечными пользователями и виртуальными компьютерами

Администраторы могут настраивать динамические политики, которые адаптируются к условиям вычислительной среды конечных пользователей, и службы сетевой безопасности, которые присваиваются пользователям на основе ролей, логических групп, операционной системы компьютера и т. п. и не зависят от базовой сетевой инфраструктуры. Централизованное управление политиками обеспечивает их автоматическую привязку к каждому виртуальному компьютеру при его создании, что обеспечивает надежное масштабирование и неизменно высокий уровень безопасности каждого виртуального компьютера независимо от его расположения в ЦОД.

Платформа для повышенной безопасности

VMware NSX предоставляет расширяемую платформу с возможностью интеграции с лучшими в своем классе решениями для обеспечения безопасности, созданными нашими надежными партнерами. За счет динамического добавления служб безопасность виртуальных компьютеров в ЦОД распространяется на конечные устройства и приложения. Наша экосистема партнеров включает в себя такие компании, как Trend Micro, Intel Security и Palo Alto Networks, которые предлагают средства предотвращения вторжений, службы обеспечения безопасности нового поколения и решения для защиты операционных систем, веб-браузеров и электронной почты от вирусов и вредоносных программ.

Дополнительные сведения

Для получения дополнительных сведений о Horizon и VMware NSX посетите веб-сайт VMware и следите за нашими новостями в Twitter.

Ресурсы по VMware Horizon

Веб-сайт: http://www.vmware.com/ru/products/horizon-view

Блог: http://blogs.vmware.com/euc/

Twitter: @VMwareHorizon

Ресурсы по VMware NSX

Веб-сайт: http://www.vmware.com/ru/products/nsx/

Блог: http://blogs.vmware.com/networkvirtualization/

Twitter: @VMwareNSX

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