Брандмауэр SDF для виртуальных рабочих мест

Микросегментация сред VDI помогает изолировать виртуальные рабочие места и блокировать горизонтальное распространение угроз

КРАТКОЕ ОПИСАНИЕ

Виртуальные рабочие места помогают консолидировать приложения и данные конечных пользователей в центрах обработки данных с эффективным управлением. Это позволяет сократить расходы и улучшить защиту данных. Однако при этом в инфраструктуре ЦОД возникает риск нарушения безопасности конечных пользователей. VMware обеспечивает удобную микросегментацию для виртуальных рабочих мест, что помогает изолировать конечных пользователей от инфраструктуры ЦОД.

ОСНОВНЫЕ ФАКТЫ

- **Унифицированная инфраструктура системы безопасности.** Использование единой инфраструктуры брандмауэра для всего ЦОД, включая зоны безопасности, приложения и инфраструктуру виртуальных рабочих мест (VDI).
- **Компактные политики.** Определение компактных политик безопасности с помощью таких удобных компонентов, как идентификатор пользователя, идентификатор приложения и метки безопасности.
- **Ограничение горизонтального распространения угроз.** Изоляция виртуальных рабочих мест от серверной части VDI и остальных компонентов инфраструктуры ЦОД позволяет ограничить горизонтальное распространение угроз.

Виртуальные рабочие места упрощают работу и обеспечивают экономию, но при этом могут быть причиной появления угроз

VMware Horizon обеспечивает централизованное размещение сеансов виртуальных рабочих мест пользователей с помощью узла RDSH или пулов виртуальных рабочих мест. Консолидация приложений и данных конечных пользователей снижает расходы на инфраструктуру, а также оптимизирует управляемость и защиту данных. Однако, поскольку иногда безопасность виртуальных рабочих мест нарушается, их близость к инфраструктуре ЦОД с конфиденциальными данными способствует возникновению новых угроз. Злоумышленник может получить контроль над виртуальным рабочим местом и воспользоваться им для проникновения на ближайшие серверы. Группы обеспечения безопасности должны изолировать виртуальные рабочие места и заблокировать атаки с горизонтальным распространением угроз.

Решение: брандмауэр SDF для виртуальных рабочих мест

Решение VMware NSX Service-defined Firewall (SDF) защищает горизонтальный сетевой трафик в многооблачных средах с помощью распределенного брандмауэра уровней 2–7 с сохранением состояния. Брандмауэр SDF поддерживает детализированную сегментацию сети ЦОД вплоть до уровня отдельной рабочей нагрузки. При этом он обеспечивает идентификацию пользователей и приложений. С помощью брандмауэра SDF администраторы могут изолировать зоны виртуальных рабочих мест от остальной части инфраструктуры ЦОД, проверять трафик между зонами и блокировать возможное горизонтальное распространение угроз.

Обычно у пользователей есть различные права на доступ к приложениям и ресурсам на основе ролей (например, доступ к финансовым системам есть только у представителей финансового отдела). Однако для сеансов виртуальных рабочих мест используются одинаковые IP-адреса пользователей, что затрудняет применение соответствующих прав доступа только на основе использования IP-адресов. Брандмауэр SDF обеспечивает межсетевую защиту на основе учетных данных посредством полной интеграции с Active Directory. Таким образом, администраторы могут использовать брандмауэр SDF, чтобы контролировать доступ пользователей к ресурсам на основе их групп и учетных данных Active Directory.

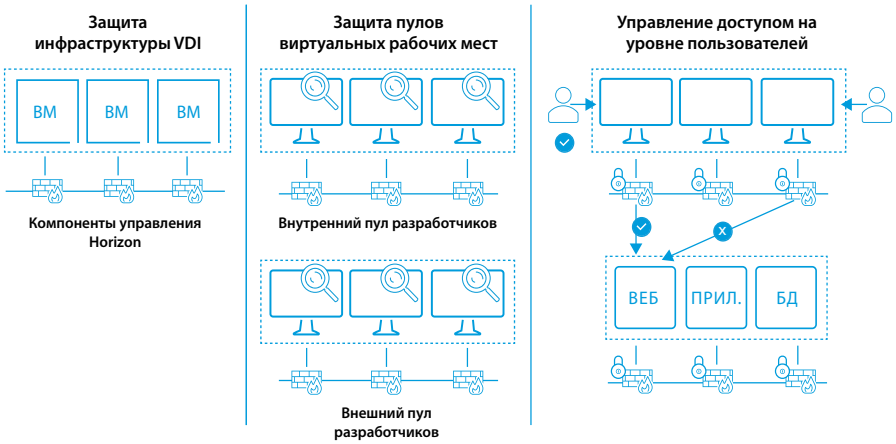

РИС. 1. Брандмауэр SDF обеспечивает защиту VDI, виртуальных рабочих мест и приложений

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ (см. рис. 1)

Защита инфраструктуры VDI. Используйте распределенную архитектуру брандмауэра SDF, чтобы защитить саму инфраструктуру VDI, в том числе компоненты управления Horizon.

Изоляция пулов виртуальных рабочих мест. Изолируйте уязвимые виртуальные рабочие места пользователей от остальной части инфраструктуры ЦОД посредством сегментации сети с помощью брандмауэра SDF.

Управление доступом на уровне пользователей. Определяйте политики безопасности, ориентируясь на учетные данные пользователей и их членство в группе Active Directory. Используйте брандмауэр SDF, чтобы проверять и применять права управления доступом пользователей к назначенным приложениям и ресурсам ЦОД.

ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ

Чтобы узнать дополнительные сведения о защите ваших виртуальных рабочих мест, ознакомьтесь со следующими ресурсами. За подробной информацией обращайтесь к торговому представителю VMware.

VMware Horizon

NSX Data Center

Брандмауэр NSX SDF

Независимое тестирование решения

Основные возможности

Распределенная микросегментация
Брандмауэр SDF использует виртуальную сеть VMware NSX, чтобы изолировать и сегментировать ресурсы независимо от базовой физической сети. Его распределенная архитектура поддерживает проверку сетевого трафика с сохранением состояния и применение политик на уровне рабочей нагрузки.

Политики на уровне пользователей
Благодаря интеграции с Active Directory (AD) брандмауэр SDF позволяет применять политики безопасности на уровне конкретных пользователя. Доступ пользователей к важным ресурсам ЦОД определяется членством в группе AD и правами доступа.

Компактная модель на основе объектов
Политики безопасности основаны на общей модели объектов с использованием таких атрибутов, как тип ОС, имена ВМ и записи Active Directory. Эта модель исключает зависимость от временных IP-адресов и специфичных атрибутов трафика. При этом с помощью всего нескольких политик обеспечивается изоляция виртуальных рабочих мест.

Централизованное управление
Политики безопасности определяются централизованно и распределяются по всей сети. Центральная плоскость контроля обеспечивает согласованность виртуальных рабочих мест и гибридной сети, состоящей из ВМ, контейнеров, аппаратных машин и облачных сервисов.

Использование VMware Horizon в сочетании с брандмауэром SDF обеспечивает безопасность виртуальных рабочих мест

VMware Horizon — это комплексное решение для виртуализации рабочих мест. Брандмауэр SDF добавляет уровень безопасности к виртуализации рабочих мест. Это обеспечивает защиту важных ресурсов ЦОД от атак с горизонтальным распространением угроз, инициируемых посредством виртуальных рабочих мест пользователей. При использовании VMware Horizon в сочетании с брандмауэром SDF реализуются эксплуатационные преимущества виртуальных рабочих мест и сводятся к минимуму проблемы, связанные с безопасностью.

Независимое тестирование

Coalfire, одна из ведущих фирм, предоставляющих консультации в области кибербезопасности, провела независимое тестирование возможностей защиты виртуальных рабочих мест с помощью брандмауэра SDF. Тестирование, проведенное экспертами Coalfire Labs, показало, что брандмауэр SDF может предотвращать кибератаки, осуществляемые посредством виртуальных рабочих мест.

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