ТЕМАТИЧЕСКАЯ СТАТЬЯ, **МАРТ 2020 Г.**

Четыре препятствия на пути к микросегментации

vmware®

Содержание

Введение

Растущее число сложных атак на корпоративные информационные ресурсы вызывает обеспокоенность. Размер ущерба от утечки данных достигает в среднем около 4 млн долларов[1], поэтому директорам по информационной безопасности необходимо искать способы повышения уровня *корпоративной безопасности*. Число атак, относящихся к категории продолжительных атак повышенной сложности (APT), постоянно увеличивается. Злоумышленники находят нестандартные способы проникновения в ЦОД, пребывают в нем на протяжении нескольких месяцев и используют внутренние каналы передачи данных для достижения своих целей и нарушения безопасности.

Традиционный подход к безопасности в основном опирается на защиту периметра — обеспечение безопасности вертикального трафика. При этом предполагается, что горизонтальный трафик в ЦОД защищен[2]. Таким образом, традиционный подход не способствует предотвращению продолжительных атак повышенной сложности.

Модель нулевого доверия — это подход, ориентированный на улучшение средств защиты ЦОД. Он предусматривает проверку каждого потока трафика в ЦОД. При использовании модели нулевого доверия инфраструктура ЦОД разделяется на небольшие зоны безопасности. Трафик между зонами проверяется, чтобы обеспечить его соответствие политикам безопасности, определенным организацией.

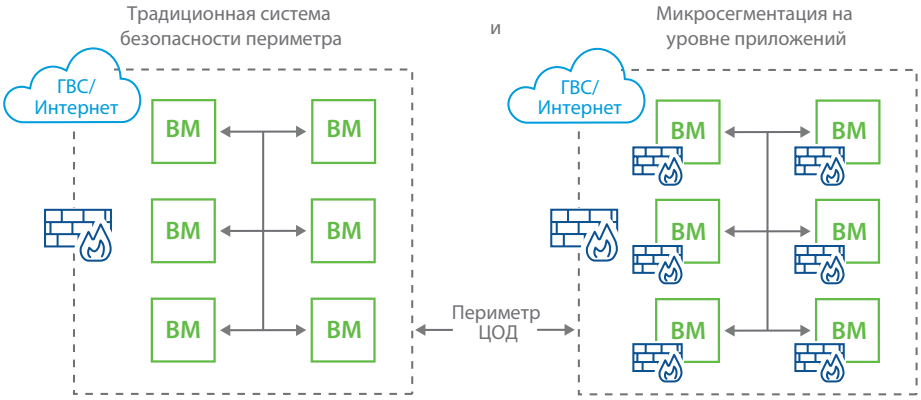

РИС. 1. Сравнение защиты периметра и микросегментации

Микросегментация — это подход, предполагающий разделение инфраструктуры ЦОД на небольшие зоны безопасности (см. рис. 1). Фактически микросегментация обеспечивает гибкий контроль потоков трафика между всеми рабочими нагрузками, позволяя администратору защищать горизонтальную передачу данных. Другими словами, микросегментация помогает реализовать модель нулевого доверия.

Однако микросегментация не решает проблему полностью. Несмотря на то что концепция микросегментации существует уже некоторое время, организации все еще сталкиваются с препятствиями при ее реализации. Рассмотрим некоторые из главных препятствий для использования микросегментации.

- **Проблемы обнаружения политик**. Определение правильных микросегментов и настройка надлежащих политик безопасности оказываются чрезвычайно сложными задачами, особенно в динамичной среде ЦОД.
- **Средства контроля с ограниченным доступом**. Недостаточно использовать атрибуты уровня 4 (например, IP-адреса и порты) в качестве основы для микросегментации. Из-за динамичности приложений и потоков требуется нечто большее.

1. Verizon. 2018 Data Breach Investigations Report («Отчет по результатам исследования утечек данных в 2018 г.»), апрель 2018 г.
2. SANS Institute. «Насколько эффективна ваша система безопасности?», 11 марта 2020 г.

- **Зависимость от агентов**. В некоторых случаях для внедрения микросегментации требуется установка дополнительных программных агентов на каждую виртуальную машину (ВМ), из-за чего возникают сложности и уязвимости.
- **Отсутствие средств обнаружения и предотвращения угроз**. Угрозы часто маскируются под обычный трафик. Настройки основных правил блокировки трафика недостаточно.

В следующих разделах мы рассмотрим эти препятствия и предложим способы их преодоления.

Проблемы обнаружения политик

Микросегментация подразумевает разделение сети ЦОД на небольшие зоны безопасности и контроль потоков трафика между ними. Внедрение не вызывает никаких сложностей, если знать, где установить границы сегментов.

Во многих случаях администраторы стремятся применить микросегментацию к уже имеющейся архитектуре ЦОД. Имеющиеся топологии сложны для анализа, поскольку они представляют собой продукт многолетнего фрагментированного развития. Документация по архитектуре может быть неполной или просроченной либо вовсе отсутствовать. Создание карты актуальной топологии ЦОД — это медленный процесс, подверженный ошибкам. Политики безопасности, которые применяются на основе неполной информации и неточного определения, обычно оставляют серьезные пробелы в защите.

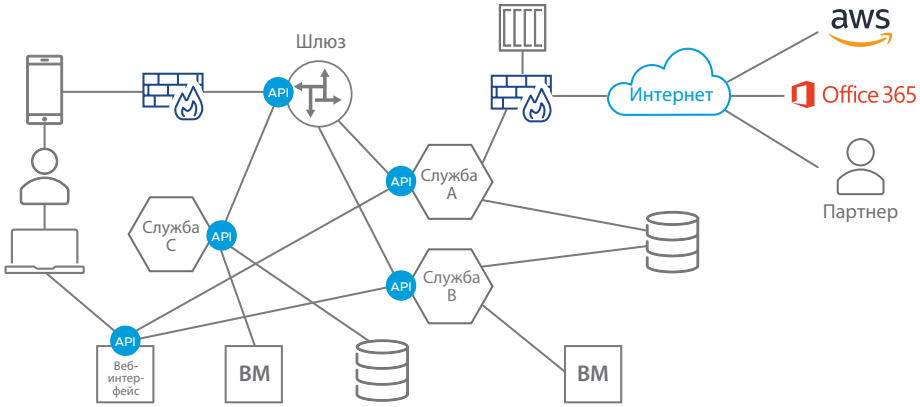

РИС. 2. Современная архитектура приложений

Использование новейших архитектур ЦОД также сопряжено с проблемами. Современные приложения, которые запускаются в новых ЦОД, чаще всего не являются монолитными и не работают на выделенных серверах. Подкомпоненты приложений охватывают несколько динамичных ресурсов. Одни приложения разделены на уровни, другие построены на базе микрослужб, а некоторые работают на основе облачных сервисов (см. рис. 2).

Понимание актуальной топологии приложений и потоков передачи данных между их подкомпонентами дается непросто. Кроме того, поскольку многие приложения динамичны по своей природе, их топология и поток передачи со временем изменяется.

Администраторы должны создать карту приложений и потоков, которая отображает актуальную топологию приложений и потоков передачи данных между подкомпонентами, чтобы определить подходящие политики микросегментации.

Разработка такой карты подразумевает сбор и анализ сведений из нескольких источников, таких как базы данных управления конфигурациями (CMDB), платформы управления ЦОД (например, VMware vCenter®) и журналы трафика. Собранные данные часто оказываются неполными, а иногда бывают несогласованными. Кроме того, они изменяются со временем.

Создание точных карт приложений и потоков вручную отнимает много времени и сопряжено с риском ошибок. Из-за этого администраторы применяют бессистемный подход, основывая политики безопасности микросегментации на догадках и устаревших сведениях. Этот подход приводит к появлению пробелов в системе безопасности, что делает ЦОД уязвимым для атак.

Специалисты VMware определили проблему с обнаружением политик и разработали *VMware NSX® Intelligence™* для ее решения. NSX Intelligence — это *модуль распределенной аналитики*, который автоматизирует процесс обнаружения политик, как описано ниже.

1. Модуль NSX Intelligence, поддерживаемый другими источниками данных (например, VMware vRealize® Network Insight™), собирает сведения о запущенных приложениях и их потоках передачи данных. Выполняется централизованный анализ собранных сведений.
2. В результате организации получают комплексную топографическую карту приложений и потоков (см. рис. 3). Администраторы могут легко увидеть фактические компоненты приложений и потоки передачи данных между ними. Карта имеет иерархическую структуру, что позволяет легко охватывать крупные сети и устранить фактор неопределенности при анализе топологии.
3. На основе карты на рис. 3 NSX Intelligence автоматически составляет рекомендации в отношении политик безопасности для микросегментации. Эти рекомендации основываются на полученных данных о потоках и определяют, какие из них должны быть разрешены. Остальные потоки блокируются. То есть фактически применяется модель нулевого доверия.
4. Администратор может применить эти рекомендации одним нажатием кнопки. Выбранные политики распространяются на распределенный брандмауэр NSX и применяются к каждому узлу сети.
5. NSX Intelligence сопоставляет топологии с политиками безопасности и представляет карту соответствия с цветовыми обозначениями. Администраторы могут сразу определить, какие потоки соответствуют требованиям, а какие нет.
6. Администратор может добавлять или изменять политики и проводить итерации процессов.

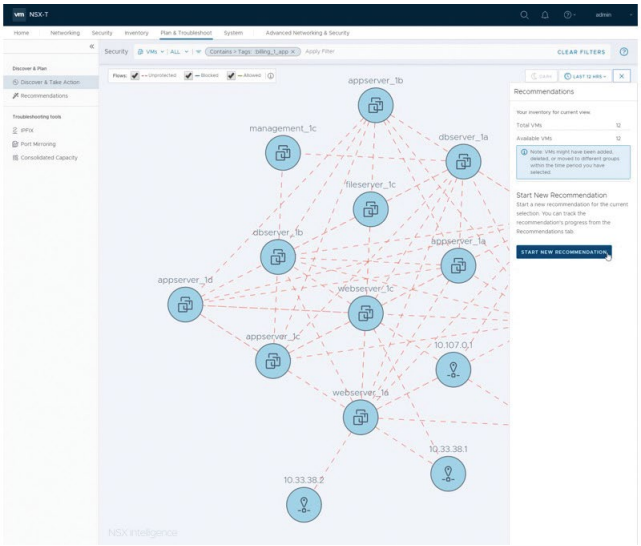

РИС. 3. Карта приложений и потоков NSX Intelligence

Средства управления с ограниченным доступом

Понимание актуальной топологии ЦОД помогает определять, где необходимо применить политики микросегментации. Однако эффективность этих политик зависит от их уровня сложности. Можно провести аналогию с защитой дома, когда возможность удерживать взломщиков снаружи зависит от сложности дверных замков.

В основе большинства политик безопасности микросегментации лежат сетевые параметры уровня 4, то есть исходный и целевой IP-адреса и номера портов. Например, чтобы заблокировать (или разрешить) трафик HTTP между двумя узлами, может потребоваться заблокировать (или разрешить) трафик TCP между этими узлами для порта 80.

Параметры уровня 4 определяют многие стандартные схемы потоков трафика, но не стоит ожидать, что злоумышленники станут использовать стандартные схемы. Например, многие атаки были отслежены до трафика порта 80, который выглядит вполне безопасным.

Более того, поскольку современные приложения и потоки динамичны, они часто используют непостоянные IP-адреса и номера. Политики безопасности микросегментации должны иметь возможность распознавать такие потоки, основываясь не только на обычных параметрах уровня 4. Необходимы более эффективные «дверные замки».

Однако проблема распознавания безопасных и небезопасных потоков трафика не ограничивается номерами портов. Например, для HTTPS обычно используется порт 443. Можно ли при этом утверждать, что любой трафик, проходящий через порт 443, защищен? Не совсем. Для трафика HTTPS могут использоваться разные версии протокола безопасности транспортного уровня (TLS), например TLS 1.0, 1.2 и 1.3. Предположим, что нам необходимо разрешить использование только TLS 1.2 и более поздних версий для трафика HTTPS. Как это можно сделать? Использования порта 443 в качестве индикатора недостаточно для распознавания соответствующего и несоответствующего трафика HTTPS.

Если нам необходимо выявлять трафик HTTPS, то нужно расширить возможности средств анализа для более глубокого изучения трафика и выявления трафика HTTPS, независимо от используемого порта. Это значит, что средства анализа трафика должны поддерживать использование характеристик уровня приложений (уровень 7).

Брандмауэр *VMware SDF* предоставляет широкий спектр возможностей уровня 7 для микросегментации (см. рис. 4), в том числе следующие:

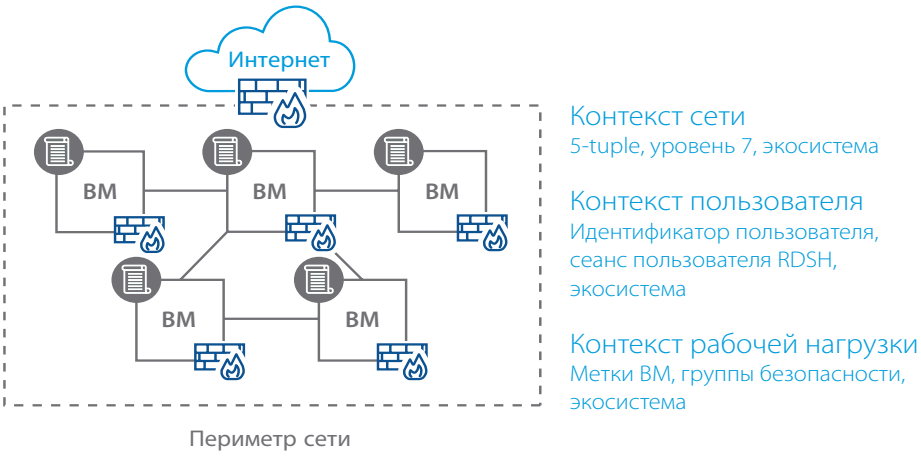

РИС. 4. Атрибуты микросегментации уровня 7

- **Идентификатор приложений**. Политики безопасности могут задействовать идентификатор приложений (AppID), который использует атрибуты уровня 7 для идентификации определенного потока. Например, администратор может определить службу с именем APP_HTTPS_TLS_V12 для обозначения трафика HTTPS, использующего протокол TLS 1.2. Брандмауэр SDF использует встроенный модуль глубокого анализа пакетов для применения политики в режиме реального времени. Использование AppID позволяет перейти от обычного определения портов к расширенным возможностям анализа трафика, упрощая определение намерения администратора.

- **Идентификатор пользователя**. Распространение инфраструктуры виртуальных рабочих мест позволяет нескольким пользователям подключаться к одному серверу и инициировать с него запросы. Поскольку пользователи имеют разные права доступа, важно разрешать (или блокировать) трафик на основе реального идентификатора пользователя. Например, запросы к приложению отдела кадров должны быть разрешены только для пользователей с правом доступа к этой конфиденциальной информации. Брандмауэр SDF поддерживает использование атрибутов идентификатора пользователя для определения политик микросегментации. Идентификатор пользователя синхронизируется с информацией, которая хранится в Active Directory, что позволяет администраторам определять политики безопасности, разрешающие или блокирующие трафик на основе идентификаторов пользователей, а не IP-адресов.
- **Фильтрация URL-адресов**. Для быстрого внедрения модели «программное обеспечение как услуга» и других облачных сервисов требуется гибкая фильтрация адресов назначения интернет-трафика. Чтобы применять такую фильтрацию, брандмауэр SDF поддерживает правила политики, которые точно устанавливают полностью определенные доменные имена, позволяя администраторам разрешить трафик, направленный на допустимые адреса назначения (например, office365.com), и блокировать подозрительные адреса.

Возможности VMware уровня 7 выходят далеко за пределы правил уровня 4, что позволяет администраторам выполнить развертывание более эффективных средств защиты в сети ЦОД.

Зависимость от агентов

Понимать топологию и создать карту потоков и приложений очень важно. Не менее важна и возможность определять политики уровня 7, которые могут блокировать сложные атаки. Однако микросегментация не сможет работать без возможности проверки трафика в режиме реального времени и применения политик на каждом узле.

Как правило, проверка сетевого трафика и применение политик безопасности — задача брандмауэров. Однако использовать традиционные брандмауэры для микросегментации сложно и слишком дорого. Чтобы брандмауэр мог выполнять проверку, трафик должен проходить через него. Это возможно, если приблизить брандмауэры к трафику или трафик к брандмауэрам. Первый вариант предусматривает развертывание множества устройств брандмауэров в сети, а это сложно и дорого. Второй вариант требует перенаправления трафика узла на брандмауэр и обратно, что создает дополнительные объемы трафика и ненужные задержки.

Поскольку традиционные брандмауэры не подходят для решения этих задач, в некоторых средах с *микросегментацией* на каждый сервер устанавливается программный агент и с его помощью активируется брандмауэр в ОС сервера. Рассмотрим ограничения этого подхода.

- **Сложность из-за разнообразия версий**. В большинстве ЦОД в любой конкретный момент времени может быть множество вариантов и версий ОС. В решениях по микросегментации, в которых используются брандмауэры ОС, должны учитываться разнообразие ОС, изменение их версий и различные возможности брандмауэра в каждой из них. Управление разными версиями брандмауэров ОС может стать слишком сложной задачей.
- **Привилегированный доступ**. Чтобы администратор мог установить и настроить программный агент в ОС, ему потребуется привилегированный доступ к серверу. Получить такой доступ бывает непросто. Более того, предоставление привилегированного доступа создает еще одну брешь в системе безопасности, чего организации хотят избежать.
- **Ограниченные возможности**. Брандмауэры серверных ОС имеют собственные ограничения, которые различаются в зависимости от ОС. Большинство поставщиков ОС для серверов предоставляют только средства контроля уровня 4 и не предлагают план по внедрению возможностей уровня 7.
- **Уязвимость агентов**. Программные агенты обычно работают в области пользователя, а не ядра. В связи с этим злоумышленник, который получает привилегированный доступ к серверу узла, может легко обойти агент. В дальнейшем злоумышленник может нейтрализовать агент и отменить все политики безопасности.
- **Перегруженность администраторов агентов**. Большинство администраторов безопасности управляют десятками агентов[3]. Обычно их не прельщает перспектива взять под контроль еще один агент для осуществления микросегментации. Решения по микросегментации, требующие добавления дополнительных агентов к уже имеющимся у администратора, отнимают время, необходимое для выполнения других задач по обеспечению безопасности.

3. Forrester Consulting. To Enable Zero Trust, Rethink Your Firewall Strategy («Пересмотр стратегии использования брандмауэра для внедрения модели нулевого доверия»), февраль 2020 г.

Для сравнения: брандмауэр SDF встроен в гипервизор (см. рис. 5), что устраняет необходимость установки и настройки отдельного ПО на каждой ВМ. Поскольку функции плоскости данных NSX относятся к области ядра, брандмауэр защищен от попыток злоумышленников его нейтрализовать.

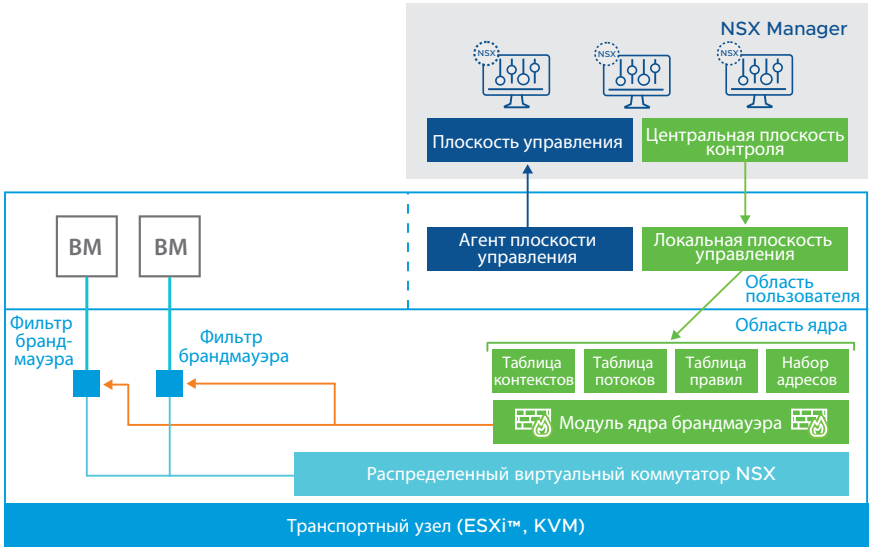

РИС. 5. Встроенные функции брандмауэра

Брандмауэр SDF интегрирован с основными сетевыми функциями NSX, что обеспечивает его доступ к каждому пакету и каждой рабочей нагрузке без дополнительной настройки или перенаправления трафика.

Политики безопасности определяются централизованно с помощью единой консоли управления NSX. После этого они автоматически распространяются для применения на каждом узле.

Устранив необходимость в установке, настройке и администрировании дополнительных программных агентов, компания VMware ликвидировала еще одно значительное препятствие на пути к микросегментации. Администраторы могут сосредоточиться на определении политик безопасности для микросегментации и позволить системе выполнить все остальное автоматически.

Отсутствие средств обнаружения и предотвращения угроз

Мы уже рассмотрели снижение сложности, связанной с определением политик безопасности, добавление необходимых возможностей уровня 7 и встроенные в платформу функции брандмауэра. Эти улучшения повышают эффективность микросегментации и ее доступность. Однако это еще не все.

Злоумышленники используют методы маскирования для внедрения угроз в потоки трафика, которые выглядят безопасными. Средства микросегментации идентифицируют типы потоков трафика, которые должны быть разрешены (или заблокированы) между сегментами. Однако без расширенных возможностей проверки средства микросегментации не смогут самостоятельно устранять скрытые угрозы.

Существуют решения, разработанные специально для этого: *системы обнаружения и предотвращения вторжений (IDS/IPS)* обеспечивают эффективное сканирование трафика, используя заранее определенные сигнатуры для обнаружения угроз. После обнаружения несущий угрозу трафик немедленно блокируется, чтобы предотвратить возможную атаку.

Решение VMware *NSX Distributed IDS/IPS™* (см. рис. 6) позволяет расширить возможности микросегментации с помощью средств обнаружения угроз.

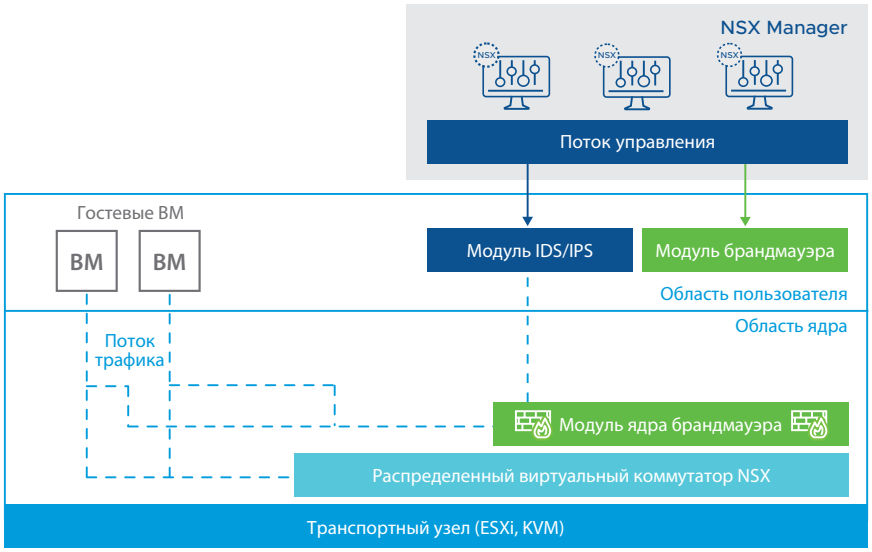

РИС. 6. Встроенные средства обнаружения и предотвращения угроз

Распределенная архитектура решения VMware IDS/IPS предоставляет ряд основных преимуществ:

- Проверка трафика выполняется на каждом узле, что позволяет избежать необходимости развертывания дополнительных отдельных устройств.
- Проверка сигнатур является распределенной, что обеспечивает широкие возможности проверки каждого потока.
- Поскольку NSX учитывает особенности рабочих нагрузок, проверка на основе сигнатур происходит выборочно, в соответствии со знаниями о запущенных приложениях.
- Управление политиками IDS/IPS выполняется централизовано вместе со всеми прочими политиками безопасности посредством удобного и масштабируемого решения NSX Manager™.

Встроенные возможности IDS/IPS позволяют администраторам контролировать потоки трафика между сегментами, а также выявлять и останавливать скрытые атаки.

Заключение

Защита корпоративных информационных ресурсов очень важна, особенно учитывая риски и расходы, связанные с кибератаками. Микросегментация — это надежная стратегия повышения уровня безопасности ЦОД. Однако традиционные подходы к микросегментации связаны со значительными ограничениями, которые влияют на эффективность и внедрение этого решения.

Компания VMware создала решение VMware NSX Intelligence, которое кардинально упростило и оптимизировало создание необходимых политик безопасности. Расширенные средства контроля уровня 7 повышают эффективность и удобство управления политиками безопасности. Возможности встроенного брандмауэра (без агентов) упрощают развертывание и устраняют накладные расходы и риски, связанные с решениями на базе агентов. Наконец, благодаря встроенным возможностям IDS/IPS политики могут обеспечивать защиту от скрытых атак.

Компания VMware стала новатором в области микросегментации, встроив соответствующие возможности в виртуальную сетевую платформу NSX. Микросегментация — это результат применения концепции встроенной системы безопасности VMware, согласно которой средства безопасности встраиваются в инфраструктуру, а не добавляются к ней в виде надстроек. VMware продолжает внедрять передовые инновации в области микросегментации. Возможности, описанные в этой статье, не только расширяют использование микросегментации, но и устраняют серьезные препятствия на пути к ее внедрению.

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

Номер по каталогу: 485849aq-wp-four-barrs-micro-segmntatn-a4-Final **3/20.**