ТЕМАТИЧЕСКАЯ СТАТЬЯ, **ДЕКАБРЬ 2019 Г.**

VMware NSX Distributed IDS/IPS

Новая парадигма безопасности горизонтального трафика

vmware®

Содержание

Системы обнаружения вторжений (IDS) появились в конце 1990-х для выявления схем потоков трафика, свидетельствующих о проводимых атаках. В 2000-х решения IDS трансформировались в системы предотвращения вторжений (IPS), поскольку приобрели дополнительные возможности обеспечения безопасности. С годами система IDS/IPS стала стандартным компонентом стека сети и безопасности. Несмотря на это, из-за стоимости и эксплуатационной сложности область применения IDS/IPS ограничивалась отдельными сегментами сети, например находящимися на периметре организаций с общедоступными сетями.

По мере развития распределенных приложений и микрослужб сетевой трафик в ЦОД также вырос в разы. В то же время границы ЦОД стали размытыми из-за растущих возможностей подключения приложений в ЦОД к публичному облаку и устройствам конечных пользователей. В результате организации стали намного чаще использовать IDS/IPS в качестве уровня безопасности ЦОД. В этой тематической статье рассказывается о новом подходе к архитектуре IDS/IPS, который обеспечивает необходимый охват системы безопасности без повышения стоимости и эксплуатационной сложности.

Встроенная система безопасности в VMware NSX

Встроенная система безопасности — основа стратегии безопасности VMware. Это встроенная в инфраструктуру система, распределенная по ИТ-среде и учитывающая требования приложений. Брандмауэр VMware SDF, встроенный в платформу VMware NSX® уровней 2–7, — результат реализации этой стратегии в ЦОД. Он позволяет операторам одновременно обеспечивать безопасность горизонтального трафика во всех многооблачных средах.

Платформа NSX[1] предназначена для двух основных сценариев использования в ЦОД: виртуализации сети и обеспечения безопасности горизонтального трафика. Виртуализация сети отделяет управление потоками трафика от базовой физической сети. Защита горизонтального трафика позволяет задавать и применять политики безопасности в ЦОД с детализацией на уровне потоков трафика с помощью средств безопасности, расположенных в гипервизоре. Комплексная виртуализация сети и системы безопасности обеспечивает высокую гибкость архитектуры сети ЦОД и в то же время предоставляет встроенную систему безопасности.

За счет своей архитектуры NSX встраивает систему безопасности в инфраструктуру виртуализации сети. Средства безопасности всегда присутствуют в инфраструктуре, поэтому их не нужно развертывать отдельно. Более того, возможность несанкционированного доступа к средствам управления безопасностью исключена, поскольку они расположены в гипервизоре, что отделяет их от целевой области атаки (то есть рабочей нагрузки).

NSX имеет распределенную архитектуру. Средства управления безопасностью расположены в виртуальном сетевом интерфейсе каждой рабочей нагрузки и предоставляют гибкий механизм для контроля потоков трафика. При этом отсутствует централизованное устройство, ограничивающее ресурсы системы безопасности, поэтому нет необходимости в искусственной привязке сетевого трафика к стеку средств сетевой безопасности.

Наконец, поскольку платформа NSX интегрирована в инфраструктуру виртуализации, она обеспечивает визуализацию всех приложений и рабочих нагрузок. NSX использует эту визуализацию для определения широкого контекста приложений, подробного отслеживания жизненного цикла рабочих нагрузок и автоматизации управления политиками безопасности.

Распределенная система IDS/IPS

Функции VMware NSX Distributed IDS/IPS™ обеспечивают дополнительные возможности проверки трафика для брандмауэра SDF[2]. Для IDS/IPS применяются те же принципы встроенной системы безопасности, что и для брандмауэра SDF. Поэтому преимущества брандмауэра SDF распространяются и на NSX Distributed IDS/IPS.

1. Для удобства изложения в данной статье подразумевается, что VMware NSX-T™ развертывается в среде VMware ESXi™.
2. VMware. Обзор решения: брандмауэр VMware SDF.

Основы IDS/IPS

Работу IDS/IPS обеспечивают модули регулярных выражений, определяющие схемы потоков трафика. Эти модули запрограммированы на поиск известных угроз на основе схем потоков трафика с помощью языка конфигурации. Операторы сети и систем безопасности используют схемы, выраженные с помощью языка конфигурации IDS/IPS, в качестве сигнатур. В настоящее время в большинстве систем IDS/IPS помимо обнаружения угроз на основе сигнатур используются такие методы обеспечения безопасности, как проверки соответствия протоколов и портов, а также обнаружение аномального трафика.

Системы IDS/IPS регулярно подключаются к частным облакам для обновления информации об обнаружении, в том числе о сигнатурах. Эту информацию, передаваемую в режиме реального времени, создают, тестируют и распространяют организации по исследованию угроз, которые отслеживают новые типы уязвимостей.

Системы IDS/IPS можно внедрять в виде автономных специализированных устройств или в составе брандмауэра. В первом случае системы IDS/IPS работают в скрытом режиме на втором уровне стека протокола. Во втором случае система анализирует трафик, предварительно разрешенный в брандмауэре, и функционирует на третьем уровне стека протокола.

Большинство традиционных систем IDS/IPS на современном рынке (как автономных, так и интегрированных с брандмауэром) — это отдельные централизованные устройства. Операторы устанавливают эти устройства на небольшом количестве предварительно выбранных участков сети, на которых необходима проверка трафика с помощью систем IDS/IPS.

IDS/IPS в NSX: принцип работы

Системы NSX Distributed IDS/IPS были созданы в рамках Suricata, известного и широко признанного проекта с открытым исходным кодом. Платформа NSX расширяет возможности Suricata, предоставляя модулям IDS/IPS среду выполнения, включая функции контроля сетевых операций ввода-вывода и управления.

NSX совмещает функции IDS/IPS и брандмауэра, что обеспечивает однопроходную структуру анализа трафика. Сначала весь трафик проходит через брандмауэр, а затем выполняется анализ IDS/IPS в зависимости от конфигурации. Кроме того, совмещение функций IDS/IPS и брандмауэра упрощает определение и применение политик сетевой безопасности.

Как показано на рис. 1, системы NSX Distributed IDS/IPS размещены в области пользователя и подключены к модулю брандмауэра, который находится в ядре гипервизора. Одно приложение взаимодействует с другим, отправляя трафик в гипервизор, в котором брандмауэр анализирует его. Далее брандмауэр направляет трафик в модуль IDS/IPS в области пользователя.

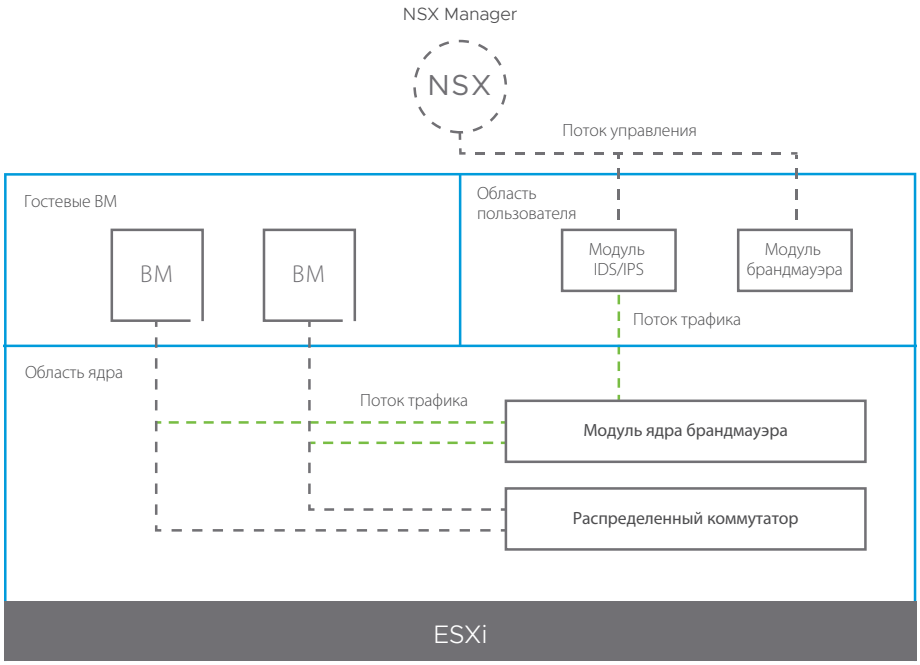

РИС. 1. Брандмауэр и IDS/IPS в NSX

Модуль IDS/IPS использует сигнатуры, декодеры протоколов и обнаружение аномалий для поиска атак в потоке трафика. Если атак не обнаружено, трафик направляется обратно в брандмауэр для дальнейшей отправки в место назначения. Если же атака обнаружена, создается и записывается оповещение.

Процесс анализа IDS/IPS на узле назначения, получающем трафик, аналогичен вышеописанному. Однако операторы могут отказаться от анализа IDS/IPS в среде назначения (или в источнике), если считают, что анализа IDS/IPS на одном конце потока трафика достаточно.

Преимущества NSX Distributed IDS/IPS

Архитектура NSX Distributed IDS/IPS кардинально отличается от архитектуры традиционных систем IDS/IPS. Разница связана с тем, что в традиционных системах IDS/IPS анализ выполняется централизованно на отдельном виртуальном или физическом устройстве. Система NSX, напротив, распределена и полностью интегрирована с инфраструктурой виртуализации.

- Оптимизированный поток трафика. Операторы развертывают IDS/IPS вместе с брандмауэром или за ним в точке входа/выхода трафика ЦОД. Потоки трафика в ЦОД, требующие анализа IDS/IPS, направляются к централизованному устройству и возвращаются от него, создавая схему перенаправления и затрачивая при этом сетевые ресурсы. NSX устраняет перенаправление и упрощает структуру сети благодаря размещению модуля IDS/IPS вместе с источником или местом назначения потока трафика, как показано на рис. 2.
- Никаких ограничений при анализе. В традиционных системах IDS/IPS на устройстве IDS/IPS или в брандмауэре ресурсы для анализа ограничены. Чтобы добавлять дополнительные ресурсы, операторам приходится постоянно обновлять аппаратные устройства до новейшего поколения, а это дорого и связано с прерываниями работы. NSX Distributed IDS/IPS использует свободные ресурсы на серверах, где работают защищенные приложения, и линейно масштабируется по мере добавления новых рабочих нагрузок. Таким образом, ресурсы для анализа не ограничены, что позволяет использовать большой объем ресурсов для анализа трафика ЦОД.
- Полное покрытие для всего трафика. Учитывая описанные выше ограничения, операторы сети и системы безопасности вынуждены выбирать трафик для анализа IDS/IPS. Часто системы IDS/IPS обеспечивают анализ только незначительной части трафика, поступающего в брандмауэр. В других случаях автономные системы IDS/IPS размещаются глубоко внутри сети и обеспечивают защиту незначительного количества серверов, что усложняет сетевую структуру. Система NSX является распределенной, благодаря чему модули IDS/IPS можно использовать для анализа всех потоков трафика для всех рабочих нагрузок, что устраняет «слепые зоны». У операторов есть возможности точной настройки функций IDS/IPS для каждой рабочей нагрузки без ограничений, связанных с базовыми структурами сети.
- Контроль и настройка сигнатур на основе контекста. Поскольку традиционные системы IDS/IPS централизованы и через них проходит множество потоков трафика, им необходимо включать тысячи сигнатур, чтобы обеспечить покрытие всех потоков трафика. При большом количестве включенных сигнатур и разнообразии их типов возникают задержки в работе систем IDS/IPS и снижается их пропускная способность. В результате операторы тратят много времени на настройку сигнатур IDS/IPS. Решение NSX Distributed IDS/IPS учитывает потребности приложений и дает возможность адаптировать сигнатуры для каждой рабочей нагрузки. Чтобы уменьшить вероятность ложных срабатываний, для рабочей нагрузки можно включить только небольшое количество сигнатур. Кроме того, модуль IDS/IPS может изменять уровень серьезности оповещений, создаваемых при обнаружении соответствующих сигнатур, в зависимости контекста приложения и важности защищаемой рабочей нагрузки. Например, оповещение в базе данных кредитных карт может требовать большего внимания по сравнению с другими рабочими нагрузками.
- Поддержка мобильности рабочих нагрузок. Виртуализированный ЦОД позволяет переносить рабочие нагрузки в другой узел или ЦОД (с помощью vMotion®). При использовании традиционных систем IDS/IPS невозможно удобно и быстро перенастроить политики безопасности с учетом нового места расположения рабочей нагрузки. В NSX политики безопасности перемещаются вместе с виртуальной машиной (ВМ) рабочей нагрузки. В результате трафик остается полностью защищенным, независимо от того, куда была перемещена ВМ. Кроме того, во время перемещения не происходят потери трафика или разрывы подключения, поскольку NSX сразу же перенаправляет трафик в новое место расположения.

- Автоматизированное управление жизненным циклом политик. Традиционные системы IDS/IPS не учитывают жизненный цикл приложений, безопасность которых обеспечивают. Из-за этого операторам сети и систем безопасности приходится вручную задавать новые политики безопасности при создании новых рабочих нагрузок и изменять их при выводе рабочих нагрузок из эксплуатации. Часто операторы опасаются допустить ошибки при частом создании новых политик или удалении устаревших, что усложняет поддержку актуальности систем безопасности. Благодаря динамическим группам в NSX операторы могут поддерживать актуальность политик без риска внесения ошибок. NSX автоматически настраивает политики безопасности при создании или выведении из эксплуатации рабочей нагрузки, предотвращая появление незащищенных рабочих нагрузок и накопление устаревших политик безопасности.

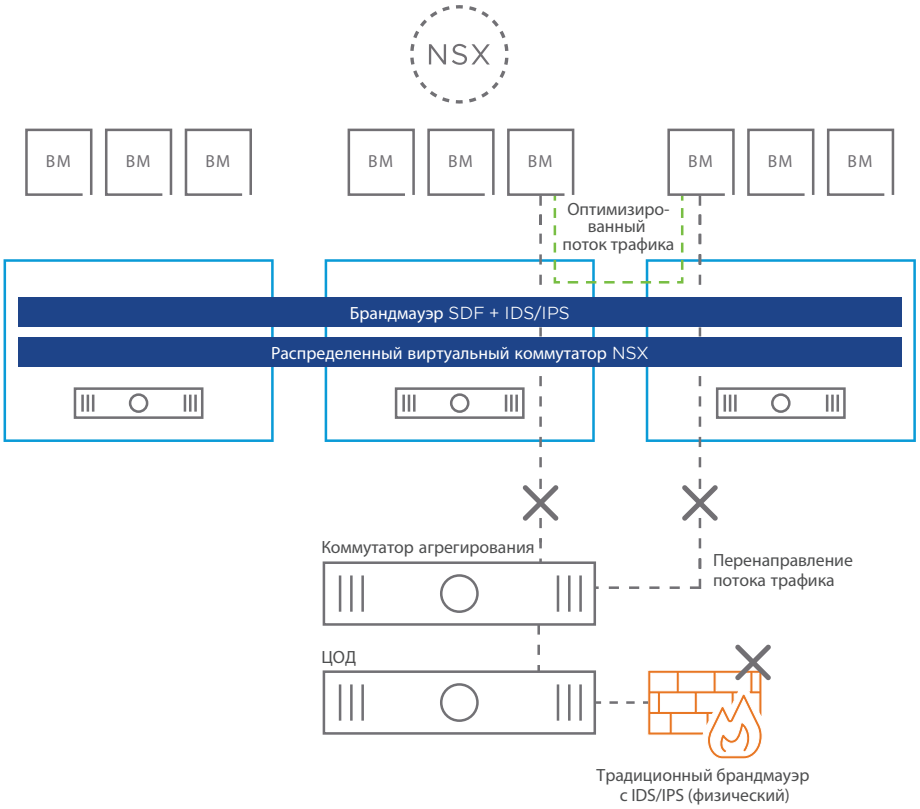

РИС. 2. NSX Distributed IDS/IPS устраняет перенаправление трафика

Сценарии использования NSX Distributed IDS/IPS

Благодаря совмещению функций IDS/IPS с брандмауэром SDF платформа NSX позволяет операторам решать дополнительные проблемы с безопасностью. Ниже описаны несколько распространенных сценариев использования.

Обеспечение соответствия законодательству

Во множестве ЦОД размещаются приложения, содержащие конфиденциальную информацию, например медицинские или финансовые данные. Часто такие приложения должны соответствовать нормативным требованиям стандартов HIPAA в сфере здравоохранения и PCI DSS или SOX в сфере финансов. Нормативные требования регулируют использование IDS/IPS для предотвращения утечки или кражи данных.

С помощью решения Distributed IDS/IPS, которое входит в состав NSX, операторы сети и систем безопасности могут обеспечить соответствие требованиям, выборочно задействуя системы IDS/IPS только для рабочих нагрузок приложений, содержащих конфиденциальные данные. Благодаря программному подходу NSX выполняет сложную часть работы, применяя политики безопасности для всех соответствующих рабочих нагрузок. Это устраняет необходимость покупать и развертывать отдельные устройства или брандмауэры. Для более подробного анализа и мониторинга соответствия нормативным требованиям операторы могут отслеживать входящие и исходящие потоки трафика в важных приложениях с помощью таких средств, как VMware NSX Intelligence™.

СВЯЗАННЫЕ ПРОДУКТЫ И РЕШЕНИЯ

- NSX Data Center:
  vmware.com/ru/products/nsx
  Брандмауэр VMware SDF:
  vmware.com/ru/security/internal-firewall
- Микросегментация с помощью NSX:
  vmware.com/ru/solutions/micro-segmentation

Внедрение виртуальных зон

Некоторым организациям требуется установить прямые сетевые подключения к организациям-партнерам. Другие организации рассматривают бизнес-подразделения и дочерние компании как арендаторов центрального ИТ-отдела. Операторы сети и систем безопасности могут обеспечить соответствие вышеуказанным требованиям с помощью NSX, используя брандмауэр и IDS/IPS для внедрения виртуальной зоны. Операторы могут добавлять новых партнеров и арендаторов без необходимости заказывать, устанавливать и настраивать новые аппаратные брандмауэры или системы IDS/IPS. Аналогичным образом операторы могут отключать партнеров и арендаторов, не оставляя незадействованным оборудование, приобретенное ранее.

Замена отдельных устройств IDS/IPS

Операторы сети и систем безопасности время от времени меняют архитектуру частей ЦОД для консолидации функций безопасности. Операторы, которые уже приняли решение виртуализировать сети ЦОД, теперь могут заменить отдельные централизованные устройства IDS/IPS распределенной платформой NSX. Это дает операторам сети и систем безопасности возможность управлять функциями брандмауэра и системы IDS/IPS из единой консоли управления (VMware NSX Manager™).

Обнаружение горизонтального распространения угроз

Злоумышленники, которым удается проникнуть в ЦОД, обычно пытаются осуществить горизонтальный переход от ВМ, в которые они проникли, к другим ВМ, на которых размещены конфиденциальные данные. Чтобы выполнить такое горизонтальное перемещение, злоумышленники проводят разведку с помощью таких средств, как Netcat. Системы IDS/IPS с соответствующими сигнатурами могут обнаружить попытки разведки и оповестить о них операторов сети и систем безопасности. Далее операторы могут блокировать действия злоумышленников (в том числе с помощью IDS/IPS) либо отслеживать их, используя NSX Intelligence или другие средства.

NSX Intelligence и NSX Distributed IDS/IPS

NSX Intelligence — это распределенная система сбора данных и анализа безопасности, доступ к которой можно получить с помощью NSX Manager (консоли управления NSX). NSX Intelligence эффективно собирает метаданные с гипервизоров в среде NSX и сохраняет информацию для дальнейшего использования.

NSX Intelligence создает детализированные схемы зависимостей приложений, которые обеспечивают визуализацию рабочих нагрузок и потоков в сети, помогая операторам получить общий обзор среды. Кроме того, NSX Intelligence автоматически рекомендует политики безопасности брандмауэра на основе выявленных схем потоков трафика между приложениями, что значительно упрощает внедрение микросегментации и внутреннего брандмауэра. Наконец, NSX Intelligence непрерывно отслеживает каждый поток трафика и позволяет операторам применять политики безопасности к потокам, чтобы продемонстрировать и поддерживать соответствие нормативным требованиям к безопасности.

NSX Intelligence органично дополняет брандмауэр SDF и систему IDS/IPS в качестве уровня визуализации и управления политиками. NSX Intelligence, брандмауэр SDF и система IDS/IPS вместе образуют комплексный и удобный в развертывании стек внутреннего брандмауэра, обеспечивающий реализацию стратегии встроенной системы безопасности в ЦОД.

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: 422052aq-fy20q4-nsbu-launch-wp-nsx-dist-idsips-a4-Final **12/19**.