FORTINET

Для защиты распределенных гибридных центров обработки данных требуются дополнительные функции межсетевых экранов NGFW

Содержание

FORTINET

Аннотация

В процессе развития технологий центров обработки данных неуклонно растет степень распределенности приложений и данных в гибридных инфраструктурах. Это повышает гибкость важных рабочих процессов, однако приводит к появлению новых векторов атак, затруднению отслеживания и снижению управляемости. Руководителям отделов проектирования сетей и управления операциями необходимы интегрированные системы безопасности, включающие современные функции защиты гибридных ИТ-сред центров обработки данных. В частности, речь идет о межсетевых экранах следующего поколения (NGFW) с такими ключевыми характеристиками, как наличие функций управления рисками, масштабируемость и охват системой безопасности всех частей организации, обеспечение непрерывности бизнес-процессов за счет отказоустойчивости, а также функции автоматизации и оркестрации, которые ускоряют реагирование и снижают нагрузку на персонал.

Появление новых векторов атак в связи с развертыванием распределенных центров обработки данных

Теперь бизнес-пользователи получают доступ к важным приложениям из распределенных центров обработки данных, которые работают на базе гибридной ИТ-инфраструктуры. Для выполнения рабочих процессов и хранения данных используются локальные расположения, колокация, общедоступные и частные облака. В связи с распределенным размещением уязвимого содержимого постоянно возникают новые направления атак на корпоративные сети.

В целях противодействия этим рискам, устранения уязвимостей и обеспечения соответствия новым требованиям многие руководители отделов проектирования сетей и управления операциями начали внедрять специализированные решения. К сожалению, такой фрагментарный подход не позволяет полностью решить текущие и будущие проблемы. Риск дестабилизации бизнеса в результате деятельности злоумышленников или стихийного бедствия растет. Также повышается совокупная стоимость владения (TCO) и усложняется управление корпоративными системами безопасности.

Средний размер убытков организации в связи с простоем, включая ущерб репутации и лояльности, за двухгодовой период составляет 67,2 млн долл. США[1].

Защита гибридных ИТ-сред

Для защиты от атак на центры обработки данных руководителям отделов проектирования сетей и управления операциями необходимо интегрировать компоненты безопасности во все части гибридных ИТ-сред. Также необходимы межсетевые экраны NGFW, которые обеспечивают комплексное отслеживание, управление политиками и предотвращение вторжений (IPS), а также обладают рядом новаторских характеристик:

- **Производительность.** Для эффективного управления рисками система безопасности должна работать на той же скорости, что и высокопроизводительные сети. Также устранению уязвимостей способствуют надежные функции.
- **Устойчивость и масштабируемость.** По мере расширения и диверсификации гибридных ИТ-сред растут требования к масштабируемости, устойчивости и доступности систем безопасности, приоритетной задачей которых является обеспечение непрерывности бизнес-процессов. Кроме того, архитектура сетей и безопасности должна успешно противостоять сбоям, вызванным отказами сети и стихийными бедствиями.
- **Автоматизация и оркестрация.** Интегрированная архитектура безопасности поддерживает интеллектуальную автоматизацию гибридной ИТ-инфраструктуры. За счет автоматизации реагирования системы безопасности и ускорения работы функций управления сокращаются временные промежутки реагирования, снижается роль человеческого фактора, уменьшаются нагрузки на персонал и эксплуатационные расходы (OpEx).

К основным проблемам, связанным с гибридными рабочими нагрузками, относятся необходимость обеспечения соответствия требованиям (71 %), падение производительности (62 %) и сложность управления (53 %)[2].

Повышение эффективности управления рисками

Как правило, межсетевые экраны центров обработки данных развертываются в самой быстрой части сети. Таким образом, эффективное решение NGFW должно обеспечивать безопасность на уровне L7, при этом оказывая минимальное воздействие на производительность сети. Для этого необходим межсетевой экран NGFW на базе **специализированных процессоров безопасности**, которые способствуют стабильной реализации функций безопасности, не препятствуя работе сети.

В целях защиты современного распределенного центра обработки данных необходимо обеспечить отслеживание всех компонентов безопасности в разных средах (локальных расположениях, колокациях, облаках и т. д.), а также пользователей, приложений и устройств. В настоящее время более трети (34 %) нарушений исходят из доверенных внутренних источников[3], поэтому приоритетом становится внедрение средств управления доступом к внутренней сети. Руководители отделов проектирования сетей и управления операциями могут решить эту задачу при помощи гибкой и масштабируемой технологии **сегментации сети**, которая поддерживает разные сценарии применения (в том числе динамическая оценка надежности пользователей, устройств и приложений). Однако сама по себе сегментация не может обеспечить реализацию важных функций противодействия современным продвинутым угрозам, в частности, проверки содержимого. Таким образом, межсетевые экраны NGFW для центров обработки данных должны адаптироваться к разным технологиям сегментации, обмениваться данными об угрозах со сторонними средствами безопасности, а также поддерживать функции проверки содержимого и автоматизированной защиты от угроз.

Эффективное противодействие огромному количеству стремительно распространяющихся угроз может обеспечить только интегрированная система безопасности, поддерживающая обмен данными в режиме реального времени. Для выявления неизвестных угроз эта система должна включать технологию искусственного интеллекта (ИИ). Необходимо обеспечить охват **компонентами выявления и предотвращения угроз на базе ИИ** всех цифровых ресурсов независимо от расположения.

77 %

современных организаций в той или иной степени используют неинтегрированные специализированные средства защиты[4].

Устойчивость и масштабируемость

Стремительное распространение инновационных цифровых технологий напрямую влияет на безопасность. В условиях нарастающей децентрализации и распределения нагрузок центров обработки данных на базе гибридных ИТ-инфраструктур важнейшим свойством системы безопасности становится **достаточная эластичность и масштабируемость** для адаптации к растущим рабочим нагрузкам и новым приложениям. Организации отказываются от традиционных средств безопасности, развернутых в локальных расположениях, в пользу облаков и виртуальных машин (VM).

Также системы безопасности центров обработки данных должны оперативно адаптироваться к непрерывному росту объема как зашифрованного, так и незашифрованного трафика. В настоящее время более 72 % сетевого трафика составляют зашифрованные данные, и этот показатель с каждым годом увеличивается почти на 20 %[5]. Большой объем зашифрованного трафика требует отслеживания при помощи современных инструментов проверки трафика HTTP и HTTPS.

Распределенные центры обработки данных особенно уязвимы для угроз, скрытно перемещающихся в потоках зашифрованных данных. Для противодействия этой угрозе необходима система безопасности с поддержкой **проверки зашифрованного трафика на уровне защищенных сокетов (SSL) и протокола (TLS)** (а также технологий «песочницы», маскировки и интеграции «медоносов»). Эти технологии обеспечивают проверку больших объемов трафика пользователей и систем, в том числе внутреннего, без снижения производительности приложений. Кроме того, система должна включать новейшие функции проверки **TLS 1.3**[6].

С точки зрения устойчивости и доступности, в случае сбоя компонента решение должно обеспечивать переход системы на другой ресурс в режиме реального времени. Встроенная технология **кластеризации N+1** предоставляет полностью избыточную архитектуру, дублирующую все возможные точки отказа. Также надежность решения повышают **независимые испытания** в реальных условиях с участием отраслевых специалистов.

60 %

зашифрованного трафика содержит вредоносное ПО[7]; 28 % атак совершается посредством установки вредоносного ПО[8].

Автоматизация и оркестрация

В условиях недостатка специалистов по информационной безопасности многие организации вынуждены бороться с проблемами кадрового голода и повышенной нагрузки на персонал. За счет упрощения управления можно снизить эксплуатационные расходы и высвободить ресурсы безопасности. Это позволит отказаться от выполнения задач вручную и сосредоточиться на бизнес-результатах и оптимизации. С этой точки зрения эффективный межсетевой экран центра обработки данных должен поддерживать **оптимизированные рабочие процессы** развертывания и управления.

Интегрированная архитектура безопасности выступает в качестве основы для обмена данными, автоматизированного реагирования и координации мер безопасности в гибридных инфраструктурах. Решение NGFW с поддержкой **открытых интерфейсов программирования приложений (API)** обладает такими важными преимуществами, как автоматизация рабочих процессов, оркестрация и синхронизированное реагирование на угрозы безопасности уязвимых приложений и динамично изменяющихся сред DevOps. Также это решение должно **поддерживать бизнес-логику, которая обеспечивает непрерывную оценку надежности пользователей, устройств и приложений** в целях автоматизации процедур безопасности (к примеру, выделения ресурсов и управления доступом). Такой подход сокращает нагрузку на персонал и снижает эксплуатационные издержки, а также повышает эффективность рабочих процессов и операций безопасности.

Кроме того, при помощи функций межсетевого экрана NGFW, которые способствуют **автоматизации аудита и ведения отчетности о соответствии требованиям**, руководители отделов проектирования сетей и управления операциями могут добиться снижения рабочей нагрузки и обеспечить соответствие новым правительственным и отраслевым нормативным требованиям и стандартам безопасности, к примеру, установленным Национальным институтом стандартов и технологий (NIST) и Центром интернет-безопасности (CIS).

Более половины ИТ-специалистов (54 %) полагают, что трудности в процессе внедрения гибридной модели возникают в связи с нехваткой квалифицированных кадров[9].

Интеграция и внедрение лучших в своем классе межсетевых экранов NGFW

Центры обработки данных становятся более распределенными, широко распространяются гибридные ИТ-инфраструктуры. Это способствует появлению новых направлений атак на корпоративные сети. Растут и требования к производительности центров обработки данных, однако руководители отделов проектирования сетей и управления операциями не должны удовлетворять запросы пользователей в ущерб безопасности. В связи с ростом количества рисков и повышением вероятности отказа сетей организациям следует пересмотреть стратегии безопасности современных центров обработки данных.

Руководители отделов проектирования сетей и управления операциями должны понимать, что обеспечить защиту и при этом сохранить производительность на прежнем уровне можно только при помощи интегрированной архитектуры безопасности, в основе которой лежит надежное решение NGFW, обладающее такими характеристиками, как производительность, устойчивость, масштабирование и автоматизация.

[1] Филип Трута (Filip Truta), Downtime Can Cost a Company up to $67 Million Over Two Years, Threatening Brand Reputation, Security Boulevard, 21 февраля 2019 г.

[2] Элисон ДеНиско Рейом (Alison DeNisco Rayome), 91% of tech leaders say hybrid cloud is 'ideal' IT model, TechRepublic, 15 ноября 2018 г.

[3] 2019 Data Breach Investigations Report, Verizon, апрель 2019 г.

[4] The CIO and Cybersecurity: A Report on Current Priorities and Challenges, Fortinet, 23 мая 2019 г.

[5] Джон Мэддисон (John Maddison), Encrypted Traffic Reaches A New Threshold, Network Computing, 28 ноября 2018 г.

[6] Алекс Сэмонт (Alex Samonte), TLS 1.3: What This Means For You, Fortinet, 15 марта 2019 г.

[7] Омар Яакуби (Omar Yaacoubi), The hidden threat in GDPR's encryption push, PrivSec Report, 8 января 2019 г.

[8] 2019 Data Breach Investigations Report, Verizon, апрель 2019 г.

[9] Элисон ДеНиско Рейом (Alison DeNisco Rayome), 91% of tech leaders say hybrid cloud is 'ideal' IT model, TechRepublic, 15 ноября 2018 г.

FORTINET

www.fortinet.com/ru

472724-0-0-RU

24 апреля, 2020 9:15 AM

eb-advanced-ngfw-security_RU