ИССЛЕДОВАНИЕ

Руководство по оптимизации сетевых операций в ходе внедрения сегментации на основе намерений

Основные методы обеспечения соответствия требованиям и снижения рисков по всем векторам атак

Аннотация

Технологии сегментации сетей, устройств, пользователей и приложений уже довольно давно применяются в целях защиты периметра и деления плоских внутренних сетей на уровни. Однако эти технологии не отвечают требованиям руководителей отделов проектирования сетей и управления операциями, отдающих приоритет таким задачам, как снижение рисков, обеспечение соответствия требованиям и эффективное управление системами безопасности.

Традиционные методики управления доступом недостаточно детализированы и не соответствуют современным бизнес-требованиям. Они используют быстро устаревающие данные оценки надежности и сигнализируют о защите сети от угроз даже в том случае, если организация не защищена от атак по всем векторам. Работая с такой инфраструктурой, руководители отделов проектирования сетей и управления операциями не имеют возможности принимать упреждающие меры защиты, а корпоративная сеть подвергается значительным рискам.

В связи с широким распространением мультиоблачных сред, мобильных приложений, Интернета вещей (IoT) и других технологий цифровой трансформации растет количество векторов атак. Выходом может стать сегментация на основе намерений. Это решение лишено недостатков существующих технологий сегментации и легко встраивается в самые разные сценарии управления доступом.

Среднестатистическая организация использует 75 разных инструментов защиты. Как с учетом этого факта можно говорить о прозрачности и комплексном отслеживании?[1]

Эффективную защиту можно обеспечить только при условии сегментации с учетом целей бизнеса, которая позволяет своевременно определять необходимые меры и целевые ресурсы.

Принципы сегментации на основе намерений

Сегментация на основе намерений преобразует бизнес-задачи руководителей в сфере сетевых технологий в ответы на вопросы «где», «как» и «что», необходимые для сегментации системы безопасности:

- **«Где»** определяет расположение границ между сегментами и логику сегментации ИТ-активов.
- **«Как»** обеспечивает реализацию бизнес-задач при помощи детального управления доступом на основе динамического разделения ресурсов на доверенные группы.
- **«Что»** обеспечивает управление доступом при помощи современных высокопроизводительных систем безопасности (уровень 7) по всей сети.

Эти три элемента функционируют в рамках интегрированной системы компонентов безопасности, которые связываются и взаимодействуют с другими устройствами инфраструктуры и сети. Таким образом, руководители в сфере сетевых технологий могут повысить эффективность системы безопасности и рабочих процессов, устранить риски и обеспечить соблюдение требований без изменения сетевой архитектуры.

Сегментация в соответствии с бизнес целями

Сегментация на основе намерений поддерживает распространенные **архитектуры макро- и микросегментации,** а также **сегментации на уровне приложений, процессов и конечных точек**. За счет разделения плоской сети при помощи одной из перечисленных технологий сегментации сетевой оператор может создать более компактные и управляемые инфраструктуры, а затем обеспечить их защиту от атак по разным векторам с помощью современных высокопроизводительных систем безопасности (уровень 7).

Благодаря технологии сегментации на основе намерений сетевые операторы могут создавать домены безопасности и разделять сеть на сегменты в зависимости от целей бизнеса. Однако достижение этих целей возможно при условии, что средство сегментации поддерживает детальное управление доступом на основе **личности пользователей или бизнес-логики** и настройку управления доступом в зависимости от актуальных сведений, полученных из внешней базы данных доверенных элементов, предназначенной для непрерывной оценки надежности.

Разделение ресурсов на доверенные группы в целях информированного управления рисками

В прошлом технологии управления доступом не предусматривали изменения уровней доверия для пользователей, устройств и приложений. Однако в реальных условиях надежность перечисленных элементов часто изменяется, что связано либо с естественными изменениями в ходе ведения коммерческой деятельности, либо с проникновением угроз. Изменение уровня доверия серьезно сказывается на эффективности корпоративных систем безопасности и приводит к появлению новых рисков. Статичность уровней доверия чревата недостаточной информированностью руководителей в сфере сетевых технологий.

В связи с этим средство сегментации на основе намерений осуществляет управление доступом на базе постоянно обновляющихся уровней доверия. Комплексные системы сегментации на основе намерений получают эту информацию как из внешних, так и из внутренних источников.

Помимо более точных сведений о сетевых рисках технология сегментации на основе намерений также использует данные непрерывной оценки эффективности системы безопасности. **Сервисы оценки систем безопасности** служат для анализа конфигурации безопасности сети и предоставления актуальных данных о рисках и уязвимостях, а также рекомендаций по устранению недостатков конфигурации. Кроме того, эти сервисы отслеживают эффективность системы безопасности в динамике и сравнивают полученные показатели с аналогичными показателями других организаций той же отрасли и принятыми стандартами безопасности. Предпочтение следует отдавать средствам сбора данных об угрозах, поддерживающим оценку систем безопасности в режиме реального времени. Такие средства можно использовать для централизованного отображения данных «в одном окне», что позволяет получить полное представление об уязвимостях по всем векторам атак. Помимо оценки систем безопасности, сотрудники отделов проектирования сетей и управления операциями могут отнести к числу приоритетных такие задачи, как исправление уязвимостей и выявление новых угроз, появляющихся по мере изменения обстановки внутри и снаружи сети.

В настоящее время объем зашифрованного интернет-трафика достиг 72%. Киберпреступники используют этот трафик для проникновения в сети и хищения данных.

В связи с распространением продвинутых угроз в число обязанностей руководителей отделов проектирования сетей и управления операциями вошла непрерывная оценка эффективности систем безопасности.

Защита от продвинутых постоянных угроз

Во многих случаях организации, приступающие к развертыванию систем управления доступом, не располагают всеми компонентами архитектуры безопасности, необходимыми для поддержки таких средств. При этом имеющиеся компоненты безопасности не всегда интегрированы друг с другом. Это снижает эффективность деятельности руководителей отделов проектирования сетей и управления операциями по выявлению развивающихся угроз, противодействию атакам и предотвращению заражения сетей.

Всегда активная функция проверки SSL в сети. Сегментация на основе намерений обеспечивает реализацию политик доступа и защиту сети от атак по всем векторам за счет развертывания экономичных высокопроизводительных межсетевых экранов следующего поколения (NGFW) уровня 7, одной из основных функций которых является проверка SSL трафика.

В настоящее время объем зашифрованного интернет-трафика достиг 72%. Функции проверки трафика с шифрованием SSL или TLS (безопасность уровня транспорта) перешли в число обязательных.[2] Появление таких видов вредоносного ПО, как Heartbleed, Poodle и Zeus, выявили насколько уязвимы стандарты шифрования.[3] Тем не менее многие организации не торопятся развертывать функции проверки SSL в полном объеме, так как это может негативно сказаться на пропускной способности сети и удобстве пользователей. В связи с этим межсетевые экраны NGFW, используемые технологией сегментации на основе намерений, должны базироваться на **специально разработанных высокопроизводительных процессорах**, задачей которых является предотвращение снижения пропускной способности. Такие процессоры поддерживают непрерывную работу функций проверки SSL на всех межсетевых экранах NGFW.

Важной характеристикой сегментации на основе намерений является возможность развертывания средств защиты от угроз в тех расположениях, где они необходимы, включая как локальные, так и облачные корпоративные расположения. Некоторые руководители отделов проектирования сетей и управления операциями могут посчитать стоимость таких мероприятий чрезмерно высокой. Однако совокупную стоимость владения (TCO) можно снизить, если отдать предпочтение продуктам поставщика, предлагающего линейку межсетевых экранов NGFW с разной плотностью портов и в разных физических и виртуальных форм-факторах. В этом случае задача обеспечения безопасности нескольких развертываний становится вполне решаемой.

Сквозное управление. Развертывание в сети разнообразных компонентов защиты от угроз должно сопровождаться внедрением эффективных средств комплексного отслеживания и управления. Не следует забывать о средствах сегментации на основе намерений, интегрированных с адаптивной системой сетевой безопасности, так как они в упреждающем режиме обеспечивают защиту всей сети от угроз независимо от того, какой точкой входа воспользовались злоумышленники. Средство сегментации также должно поддерживать функции комплексного отслеживания и согласованного применения политик во всех точках обеспечения безопасности.

Примеры использования

Технология сегментации на основе намерений легко встраивается в самые разные сценарии управления доступом. Ниже приведено два примера, из которых видно, как при помощи надлежащей классификации доступа и современных высокопроизводительных компонентов защиты от угроз руководители отделов проектирования сетей и управления операциями могут повысить управляемость архитектуры безопасности и результативность устранения рисков.

Пример использования: защита от угроз по всем векторам атаки

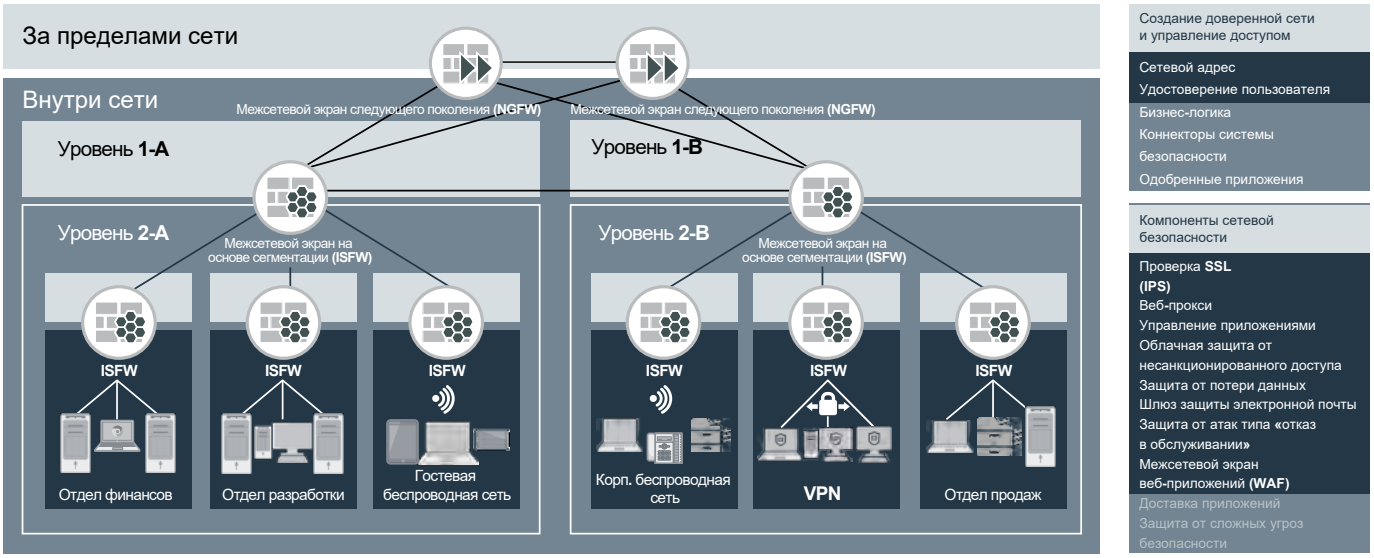

Рис. 1. Пример использования: снижение рисков за счет уменьшения количества векторов атак

В большинстве случаев для обеспечения безопасности сетевых ресурсов недостаточно одних только средств защиты периметра. Киберпреступники могут воспользоваться ошибками конфигурации, подключиться к внутренней сети при помощи зараженных устройств или воспользоваться угрозами «нулевого дня», способными обойти систему безопасности. В связи с этим в сети необходимо развернуть **дополнительные уровни безопасности** (на рис. 1 они находятся на границах между уровнями 1 и 2, а также внутри уровня 2).

Дополнительные межсетевые экраны внутренней сегментации применяют различные средства безопасности, предназначенные для блокировки вредоносной активности в зонах, находящихся под защитой. В данном случае для проверки подлинности используются идентификатор ресурса (сетевой адрес) или удостоверение пользователя. Обратите внимание, что для развертывания сегментации системы безопасности не требуется изменять саму сетевую архитектуру.

Все межсетевые экраны взаимодействуют друг с другом и с централизованной системой управления, что обеспечивает комплексное отслеживание сетевого трафика. В целях создания полных журналов аудита система управления на основе инфраструктуры безопасности собирает сведения обо всех мерах защиты от угроз, реализуемых всеми компонентами инфраструктуры.

Пример использования: обеспечение соответствия требованиям

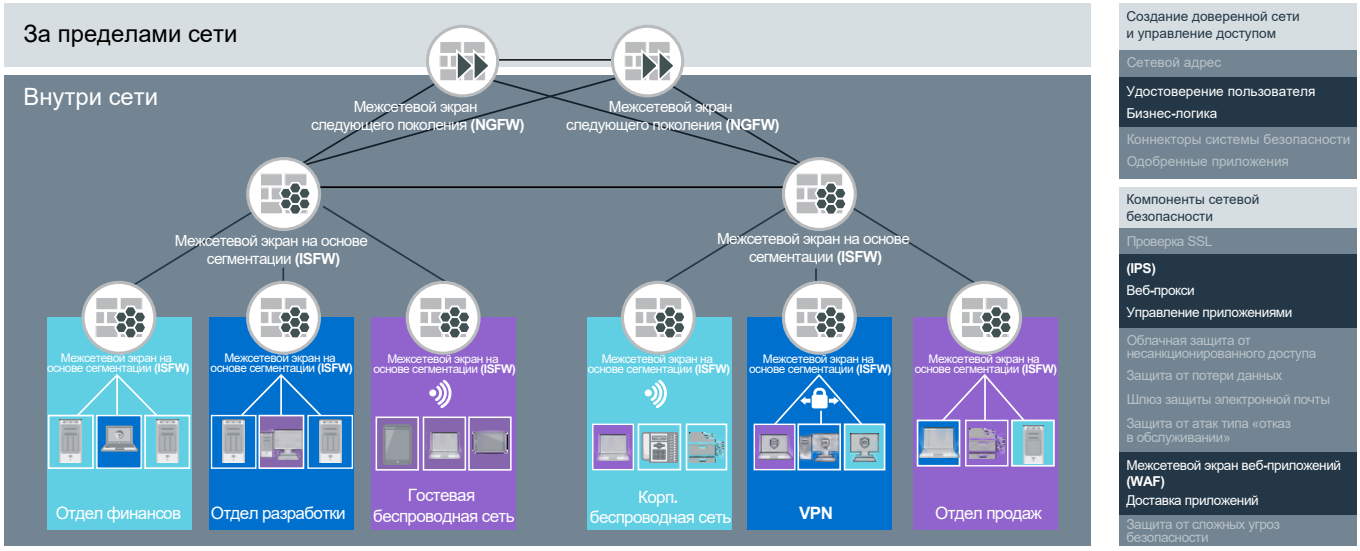

Рис. 2. Пример использования: обеспечение соответствия сложной системе требований

Как правило, обеспечение соответствия правительственным и отраслевым нормативным требованиям — это обязательное условие. Однако перенастраивать сеть при каждом изменении процедур обеспечения соответствия и вступлении в силу новых нормативных требований было бы нерационально.

К примеру, крайне сложно реализовать сегментацию ресурсов в соответствии со стандартом безопасности данных индустрии платежных карт (PCI DSS) лишь за счет изоляции подсети финансового отдела, как показано на рис. 2. В реальных условиях далеко не все устройства в подсети финансового отдела подпадают под действие стандарта PCI. В то же время другие подсети или удаленные расположения могут включать устройства, на которые распространяются требования PCI.

Технология сегментации на основе намерений поддерживает настройку и реализацию политик доступа при помощи подключенных к системе безопасности компонентов защиты. Для целей обеспечения соответствия требованиям PCI ресурсам и пользователям можно присваивать пометки независимо от их расположения в сети и применяющихся к ним иных требований и политик доступа.

Заключение

Сегментация на основе намерений — это новая технология, однако она уже готова к внедрению. Продукты и сервисы, необходимые для развертывания сегментации на основе намерений, широко доступны, а список компонентов защиты от угроз, поддерживающих подключение к системе безопасности, неуклонно расширяется.

Мы приглашаем руководителей отделов проектирования сетей и управления операциями к испытаниям пилотной версии технологии сегментации на основе целей. Можно последовать описанным в данном руководстве примерам использования, либо применить технологию для иных целей бизнеса. По запросу компания Fortinet предоставит сведения о пошаговой процедуре развертывания сегментации на основе намерений путем внедрения ключевых компонентов, которые подключаются к существующим корпоративным сетевым ресурсам.

[1] Кейси Цуркус (Kacy Zurkus), «Defense in depth: Stop spending, start consolidating», CSO Online, 14 марта 2016 г.

[2] «Q3 2018 Threat Landscape Report», Fortinet, 6 ноября 2018 г.

[3] Ананда Раджагопал (Ananda Rajagopal), «How SSL encryption gives a false sense of security», CSO Online, по состоянию на 4 февраля 2019 г.

FORTINET

www.fortinet.com/ru

348072-0-1-RU июля 2, 2019 8:19 ДП
WP-Solution-research-network-director-RU-A4