Контроль и анализ правил безопасности брандмауэров Check Point

Краткий обзор в рамках технологического партнерства

Функционал решений Check Point® и Tufin® позволяет создать безопасные и управляемые сетевые инфраструктуры

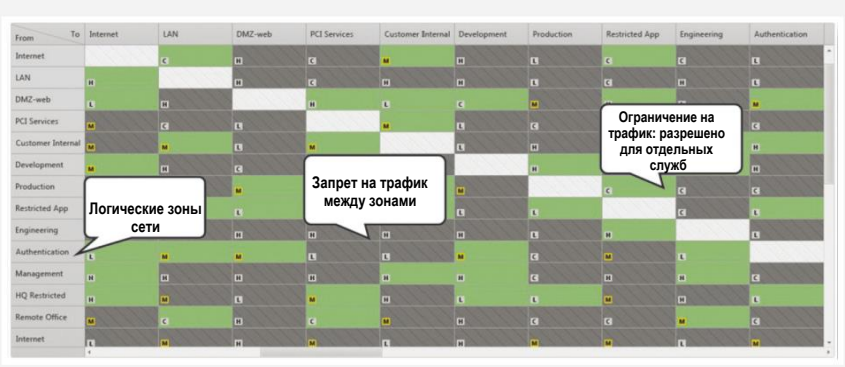
Сотрудники IT-служб предприятий и специалисты по безопасности прилагают значительные усилия для реализации комплексных мер по безопасности сетей, учитывая растущие запросы бизнеса. Недостаток наглядного представления о сложной структуре логического доступа в распределенной сети затрудняет организацию выполнения работ с должным уровнем оперативности, безопасности и точности. Вместе с решением Tufin Orchestration Suite™, управление брандмауэрами и шлюзами Check Point® дополняется, в том числе, функционалом превентивного анализа рисков, позволяя эффективно оценивать вносимые изменения. При использовании современных технологий анализа и автоматизации, с помощью функционала Tufin Orchestration Suite™, внесение изменений в правила доступа можно организовать в разнородных сетевых средах, включая «облачные» платформы и среды виртуализации. Tufin Orchestration Suite™ представляет собой комплексное решение для автоматизированного анализа, формирования и внесения изменений на уровень сетевой безопасности, включая доступ по протоколам приложений. Решение от Tufin позволяет администрировать и автоматизировать изменения в правила безопасности на отдельных устройствах Check Point, и в структуре Provider-1.

Автоматическое проектирование коррекции мер сетевой безопасности

Совместное использование решений от Check Point и Tufin значительно сокращает время, затрачиваемое на внесение корректив в меры сетевой безопасности. Это возможно за счет автоматизации процессов проектирования сетевых доступов, и их последующего внедрения. Автоматизация базируется на новейшей технологии эмуляции топологии сети, которая определяет релевантные устройства и анализирует политики каждого соответствующего брандмауэра, принимая во внимание особенности архитектуры разработчика. После этого решение предлагает подробный план внесения корректив, и после его одобрения применяет изменения к брандмауэрам. Такой подход обеспечивает быстрое и точное исполнение, включая уровень доступа к приложениям.

Понимание и контроль сложных сетей

Специалистам сферы IT бывает нелегко удержать в голове схему разбиения сети на различные сегменты. Security Zone Matrix функционал упрощает им задачу, формируя визуальное представление сетевого зонирования, мгновенно отображая карту разрешенного и запрещенного трафика между ними. В числе прочего - решение позволяет сформировать стандарт доступа между логическими зонами, и применить его в качестве шаблона для физических и виртуальных устройств защиты сети.



Security Zone Matrix функционал обеспечивает простой и централизованный контроль над сегментами сети с точки зрения администрирования правил сетевого доступа

Преимущества для бизнеса:

- централизованная поддержка «из коробки» брандмауэров Check Point и средств управления безопасностью от множества производителей;
- превентивный анализ рисков, связанных с коррекцией правил сетевой безопасности;
- реализация коррекции мер сетевой защиты за минуты;
- гарантия постоянного соответствия требованиям PCI DSS и готовности к проверкам;
- ускорение подготовки к аудиту сетевой инфраструктуры вплоть до 70 %.

Превентивный анализ рисков и оценка последствий

Каждая спешная корректировка конфигурации брандмауэра может стать потенциальной угрозой безопасности для важных данных, или для доступности критически важных приложений. Оценка последствий внесения корректив в распределенной инфраструктуре практически невозможна без правильных инструментов. В ходе автоматического внесения изменений - решение Tufin Orchestration Suite™ заранее проверяет все правила доступа на устройствах с учетом частных, внесенных в систему корпоративных мер безопасности, а также базы рекомендаций производителя устройств защиты. Это позволяет определять и оперативно отмечать потенциальные риски.

Оптимизация структуры листов доступа брандмауэров

Tufin Orchestration Suite™ помогает специалистам оптимизировать листы доступа брандмауэров в разнородных сетевых средах. Отмечаемые особенности:

- оптимизация политик за счет определения частично и полностью перекрывающихся, избыточных и неиспользуемых правил и объектов внутри правил;
- предоставление рекомендаций по приведению правил NGFW в соответствие с лучшими методами отрасли и рекомендациями производителей;
- наличие инструментария для пост-анализа конфигурации брандмауэров, составление наглядных отчетов для IT-специалистов и сотрудников служб информационной безопасности;
- встроенные и корректируемые механизмы для внесения изменений в параметры правил доступов брандмауэров, коммутаторов и маршрутизаторов.

Постоянное соответствие нормам и стандартам отрасли

Tufin Orchestration Suite™ предоставляет также инструментарий для контроля, проверки и документирования соответствия логических доступов стандартам отрасли, таким как PCI DSS, SOX и NERC CIP. Перед внедрением - каждая корректировка политики брандмауэра проходит автоматизированную оценку, что гарантирует внедрение изменений без нарушения рекомендаций стандартов. Кроме того, автоматически регистрируются вручную внесенные изменения, противоречащие нормам стандартов. При этом предлагается план решения проблемы.

Что такое Tufin Orchestration Suite™?

Tufin Orchestration Suite™ представляет собой комплексное решение автоматического анализа, создания и проверки корректности изменений на уровне безопасности сетевых доступов, включая уровень соединений критически важных приложений. Использование Tufin Orchestration Suite™ сокращает количество ошибок при конфигурации и последующей работы по перенастройке, позволяя быстро подключать новые сервисы, следить за соответствием регулятивных требований и безопасностью доступов.
Tufin предоставляет решение мирового класса в области Unified Firewall Management. Это решение позволяет организациям по всему миру точно и эффективно управлять изменениями сетевых конфигураций.
Формализуя сложные бизнес-процессы процессы (с участием разных подразделений) для защиты доступов к приложениям, серверам и сетевым устройствам - Tufin помогает избежать трудностей, знакомым многим подразделениям компаний, позволяя им более эффективно взаимодействовать между собой в процессе работы с доступом по сети.

Несколько слов о Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com) — крупнейший мировой поставщик решений безопасности, предоставляющий ведущие решения в данной отрасли, и обеспечивающий защиту клиентов от значительного числа атак с непревзойденным уровнем качества защиты. Check Point предлагает комплексные системы безопасности для защиты разнообразных устройств, включая мобильные средства коммуникации. Компания предоставляет самые полные и легко администрируемые средства управления безопасностью. Check Point защищает более 100 000 крупных и небольших организаций.

Коротко о Tufin

Офисы: Израиль (головной офис, R&D), Европа и Азиатско-Тихоокеанский регион, Северная Америка

Клиенты: более 1500 в 50 с лишним странах

Основные отрасли: финансы, телекоммуникации, ТЭК и коммунальные службы, здравоохранение, розничная торговля, образование, правительственные учреждения, производство, транспортировка, аудиторская деятельность

Партнеры по продажам: более 240 по всему миру

Технологические партнеры и поддерживаемые платформы: VMware NSX, BMC, Blue Coat, Check Point, Cisco, F5 Networks, Fortinet, Intel Security, Juniper Networks, Openstack, Palo Alto Networks и другие

tufin

www.tufin.com

SB-4-15

Check Point SOFTWARE TECHNOLOGIES LTD.