Tufin Orchestration Suite™

Оптимизация и контроль правил безопасности в физических сетях и средах виртуализации

tufin

Организация защиты сетей

В современном мире предприятия сталкиваются с проблемами защиты сетей значительно чаще, чем ранее. Ведущие новостные каналы регулярно сообщают об инцидентах спланированных компьютерных атак. Между тем сети продолжают усложняться и требуют постоянной модернизации. Отвечающие за безопасность сотрудники должны учитывать эту модернизацию, как и потребности деловой активности: структурировать группы пользователей приложений, переносить данные в ЦОД, решать вопросы организации подключений, подготавливать объекты к проверкам и так далее. Кроме того, необходимо разрабатывать и реализовывать такие задачи в сфере IT, как виртуализация, «облачные» технологии и SDN. Без сомнения, перечисленные задачи покажутся «крепким орешком» даже самым профессиональным группам ИТ и ИБ специалистов. Какие из современных технологий в значительной степени смогут посодействовать отмеченным задачам?

Tufin Orchestration Suite™

Tufin Orchestration Suite™ - это комплексное решение для администрирования задач сетевой безопасности. Оно позволяет осуществлять мониторинг, оперативно фиксировать изменения, выполнять качественный анализ правил защиты в межсетевых экранах и устройствах маршрутизации и коммутации. Помимо этого, оно обеспечивает автоматическое управление корректировкой правил брандмауэров, а также централизованное администрирование подключений сервисов. Решение гарантирует высокую степень анализа защищенности доступов, как и соответствие внутренним и внешним нормативам по безопасности.

Преимущества

- ✓ Предоставление специалистам ИТ и ИБ единой консоли управления политиками безопасности для всех сетевых брандмауэров, маршрутизаторов, коммутаторов и т.п., включая подсистемы защиты облачных сред.
- ✓ Улучшение качества защиты, обеспечение соответствия требованиям, оперативная адаптации к изменениям структуры.
- ✓ Оптимизация политик безопасности согласно рекомендациям производителей средств защиты.
- ✓ Сокращение площади поверхности атак на сетевую инфраструктуру.
- ✓ Поддержка требований к непрерывности функционирования сервисов за счет контроля доступов.
- ✓ Возможность поддержания постоянного соответствия системы нормативам предприятия и отрасли.
- ✓ Assure business continuity by minimizing network and application downtime
- ✓ Enable continuous compliance with enterprise and industry regulations

Что может требоваться вашей компании?

- администрирование подключений компонент приложений;
- защита «облачных» систем;
- перенос и объединение центров обработки данных (ЦОД);
- централизованное управление правилами безопасности сетевых устройств;
- автоматизация коррекции мер сетевой безопасности;
- разбиение сетей на сегменты;
- наглядное представление о действующих доступах по всей сети;
- соответствие нормативным требованиям;
- управление рисками.

Недавно полученные награды

SC MAGAZINE BEST BUY

SC MAGAZINE RECOMMENDED

Best of INTEROP 2015 Finalist

Info Security Products Guide 2014 GLOBAL EXCELLENCE AWARDS

NETWORK computing AWARDS 2015 WINNER DEVICE MANAGEMENT PRODUCT OF THE YEAR

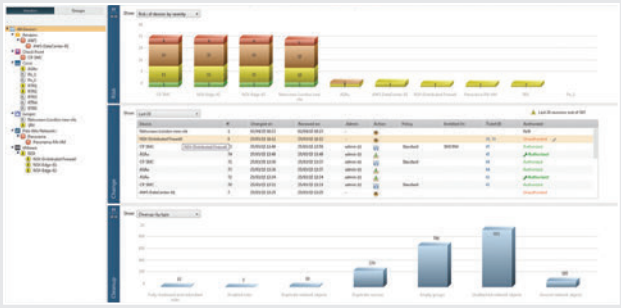
Deloitte. Technology Fast500

Tufin Orchestration Suite™

Безопасность и соответствие

Централизованное администрирование правил безопасности физических сетей, SDDC и смешанных облачных платформ

В современной сложной и разнородной IT-среде необходимо обладать целостным представлением о соблюдении правил безопасности доступа на всех платформах - в физических, виртуальных и «облачных» средах. Решение Tufin Orchestration Suite поддерживает все ключевые брандмауэры ведущих производителей (NGFW), а также такие сетевые устройства, как коммутаторы, маршрутизаторы и NLB-устройства. Также поддерживаются программно-определяемые ЦОД (SDDC) и ведущие облачные платформы. Решение позволяет контролировать и администрировать правила безопасности всех указанных платформ с единой консоли. Tufin охватывает всю структуру, отслеживая все изменения в политиках доступов, обеспечивая точное и оперативное представление о сетевой безопасности. Кроме того, Tufin предоставляет рекомендации по оптимизации правил, а также расширенный функционал для работы с рисками.



Консоль администрирования сетевой безопасности

Постоянное соответствие и готовность к проверкам Решение

Tufin Orchestration Suite позволяет организациям добиться постоянного соответствия корпоративным нормам и регулирующим стандартам, таким как PCI DSS, HIPAA и др. Tufin позволяет определять зоны PCI и соответствующих ресурсов, мгновенно генерировать отчеты о соответствии правил доступа брандмауэров заданным требованиям. Помимо этого, при необходимости, Tufin обеспечивает возможность создания исключений из проверки, а также рассчитывает информацию о соответствии по факту изменения правил доступов.

Настраиваемый отчет о соответствии PCI DSS для подготовки к проверкам

Контроль и оценка правил безопасности в физических сетях и средах виртуализации

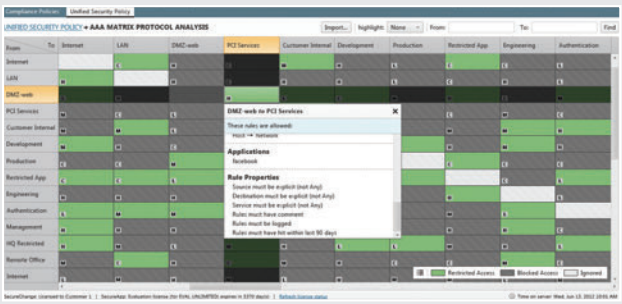
Автоматический журнал регистрации событий и настраиваемые бизнес-процессы в системе от Tufin позволяют поддерживать соответствие основополагающим стандартам, таким как ITIL, COBIT и ISO 27001.
Tufin проверяет все запросы доступа и корректировки правил безопасности на соответствие задаваемым политикам — как до выдачи разрешения на внесение изменений, так и после внесения. В окне Compliance отображается текущее состояние контролируемых систем по соответствию. Здесь же можно создать настраиваемые отчеты, что значительно сокращает время подготовки к проверкам.

Программно-определяемые ЦОД и безопасность виртуализованных систем

Сейчас значительное число компаний широко используют частные, общедоступные и смешанные виртуализованные и «облачные» структуры.
Специалистам в области безопасности требуется сформировать правильные процедуры и методы работы, гарантирующие защиту информационных ресурсов в таких средах от современных угроз.
Решение Tufin Orchestration Suite позволяет администрировать локальные брандмауэры «стандартного» типа решения защиты следующего поколения (NGFW), а также встроенные средства обеспечения безопасности систем виртуализации сетевых сред, в том числе VMware NSX, AWS и OpenStack. Использование решения от Tufin позволяет автоматизировать и обеспечить достаточно высокий уровень безопасности структуры доступа благодаря механизмам централизованного управления, подсистемам анализа рисков и средствам оценки соответствия.

Структурирование сети и сокращение площади поверхности атак

Целый ряд из числа крупных инцидентов по взлому произошли в результате начальных ошибок конфигурации сетевых средств, которые позволяли выполнить дальнейшее распознавание инфраструктуры и провести атаку на ресурсы. Тщательно сегментированная сеть позволяет избежать использования ряда «лазеек» путем изоляции и выделенной защиты сервисов. Для дополнительного и тщательного контроля рекомендуется создание микросегментов сети, выделенных зон ресурсов. Для учета и контроля внутренней логики разделения сети и обеспечения безопасности доступов в микросегментах – решение Tufin предоставляет функционал Unified Security Policy™. С его помощью можно контролировать логический сетевой доступ, например, между системами разработчиков, бухгалтерии, техподдержки и внешними сетями. Решение по обновляемой топологии сети само определит, какие правила на каких устройствах не соответствуют задаваемой схеме микросегментов. Таким образом – решение контролирует доступы между отдельными наборами ресурсов в подразделах внутренней сети, сокращая площадь поверхности потенциальных атак.



Комплексная зональная политика безопасности

Автоматизация изменений в доступах

Топология сети

Сетевая инфраструктура во многих компаниях, зачастую, образуется в результате целого ряда этапов расширения и модернизации, слияния ресурсов и их распределения. Для четкого и всеобъемлющего контроля специалисты по безопасности должны иметь четкое представление о текущей топологии и структуре логического доступа. Tufin Orchestration Suite автоматически составляет и обновляет топологическую схему всей, формируя модель для точного планирования и внедрения изменений доступов, а также для оценки рисков. Функция карты сети

Топологическая карта сети

поддерживает анализ всех стандартных технологий маршрутизации (статическая и динамическая), а также технологий VRF, MPLS, NAT, IPsec и др. Автоматически обновляемая интерактивная карта позволяет просматривать и анализировать доступы в сети любого уровня сложности, экспортируя данные в форматах PDF, PNG и Visio

Автоматическая корректировка правил безопасности на сетевых устройствах

Специалисты по работе с сетевым оборудованием тратят значительную часть рабочего времени на внесение изменений в действующие политики (ACL) устройств защиты сети.

Обычно за неделю вносятся несколько десятков (а то и более) изменений в структуру доступа. Решение Tufin Orchestration Suite сокращает время внесения изменений за счет полной автоматизации данного процесса. Сетевые инженеры и архитекторы приложений могут подавать запросы на коррективы в доступе через простой Web-интерфейс решения, предоставляя системе задачи по оценке риска и точному составлению правил на всех сетевых устройствах по пути запроса. При автоматическом внесении изменений Tufin использует карту топологии сети и определяет релевантные устройства. Затем решение анализирует актуальные правила брандмауэров и определяет степень необходимых изменений. Если необходимость в создании нового правила есть - оно находит оптимальное место размещения правила в ACL, принимая во внимание уже существующие правила и логику обработки политик на устройствах того или иного производителя. После внесения всех изменений Tufin Orchestration Suite мгновенно сверяет результат с первоначальным запросом и автоматически его документирует.

Защита подключений к приложениям

Администрирование подключений к приложениям

Приложения — «сердце» современной сетевой структуры.

По мере развития и наполнения их реальными данными - их важность только возрастает. Как современной компании гарантировать доступность к критичным бизнес-приложениям в любое время? Tufin Orchestration Suite позволяет обеспечивать автоматическую защиту доступов как между компонентами распределенных приложений, так и доступов изнутри/снаружи к ним. Это функционал можно назвать «охраной доступов приложений». Решение Tufin Orchestration Suite анализирует изменения в доступах, не позволяя нарушать взаимосвязи между ключевыми приложениями и их пользователями. Или мгновенно оповещая о нарушении доступов приложений по факту некорректного изменения. При этом отображается информация о том, какая учетная запись, на каком устройстве создала несоответствующее изменение. Оперативные оповещения могут получать как ИТ-специалисты, так и сотрудники службы информационной безопасности.

REST API

Взаимодействие с IT Service Management, Ticketing и другими сторонними системами

Tufin Orchestration Suite работает в комплексе с ведущими системами ITSM: BMC Remedy, ServiceNow, CA Service Desk и HP Service Manager. Интеграция выполняется на уровне Web-API, причем у вендора есть отдельное подразделение (не относящееся к Professional Service), специализирующееся на данных задачах. Это позволяет вносить необходимую техническую, аналитическую и контекстную составляющую в структуру заявок, созданную имеющимися системами IT Service Management и Ticketing. Применение структуры RESTful API Tufin позволяет вносить более расширенные и глубокие интегративные изменения и дополнения.

Технологические партнеры и поддерживаемые платформы

amazon web services™ · bmcsoftware · BlueCoat · Check Point SOFTWARE TECHNOLOGIES LTD. · Microsoft Azure · cisco · f5

FORTINET · intel Security · JUNIPER NETWORKS · openstack · paloalto NETWORKS · servicenow · vmware

Коротко о Tufin

Офисы: Израиль (головная компания, R&D), Европа, Азиатско-Тихоокеанский регион, Северная Америка

Клиенты: более 1600 в более чем 50 странах

Основные отрасли: финансы, телекоммуникации, ТЭК и коммунальные службы, здравоохранение, розничная торговля, образование, правительственные учреждения, производство, транспорт, аудит

Партнеры по продажам: более 240 по всему миру

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

tufin

www.tufin.com

SB-10-15