# Контроль и анализ правил безопасности брандмауэров Palo Alto Networks

## Краткий обзор в рамках технологического партнерства

### Функционал решений Palo Alto Networks® и Tufin® позволяет создать безопасные и управляемые сетевые инфраструктуры

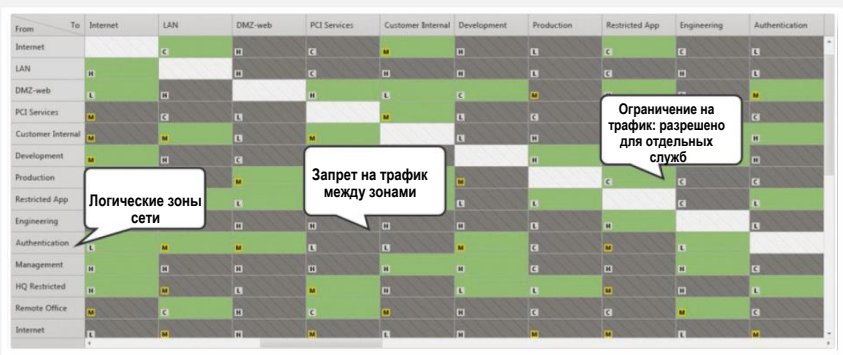
Сотрудники IT-служб предприятий и специалисты по безопасности прилагают значительные усилия для реализации комплексных мер по безопасности сетей, учитывая растущие запросы бизнеса. Недостаток наглядного представления о сложной структуре логического доступа в распределенной сети затрудняет организацию выполнения работ с должным уровнем оперативности, безопасности и точности. Вместе с решением Tufin Orchestration Suite™, управление брандмауэрами следующего поколения (NGFW) Palo Alto Networks® 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 работать с правилами безопасности на отдельных устройствах Palo Alto Networks, а также в структурах под управлением Palo Alto Networks Panorama®.

### Автоматическое проектирование коррекции мер сетевой безопасности, включая распознавание App-ID для приложений

Совместное использование решений от Palo Alto Networks 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, включая релевантное распознавание App-ID приложений. После этого решение предлагает подробный план внесения корректив и после его одобрения применяет изменения к брандмауэрам.

### 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:

- Решение от Tufin интегрировано с подсистемой Palo Alto Networks App-ID™;
- 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;
- возможность получения наглядной статистики по фактической используемости правил доступа и отдельных объектов внутри правил.

## 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™?

Компания Tufin является лидером в области централизованного контроля безопасности логического доступа на сетевом оборудовании. Tufin Orchestration Suite™ представляет собой решение автоматического анализа, создания и проверки корректности изменений на уровне безопасности сетевых доступов, включая уровень соединений критически важных приложений. Благодаря подсистеме обработки заявок, совмещенной с техническим модулем анализа правил и функционалом рекомендаций по оптимизации политик – клиенты смогут эффективно сократить временные затраты на согласование и внедрение соответствующих изменений в доступах. Экономия может достигать 70% полезного рабочего времени. Что касается задач IT-подразделений, то Tufin Orchestration Suite поможет избежать ошибок при работе с комплексными листами доступа (ACL), следить за соответствием создаваемых правил частным требованиям политик безопасности, повысить эффективность выполнения повседневных задач работы с сетевым оборудованием. Компания Tufin была основана в 2005 году. Сегодня она обслуживает более 1500 клиентов из разных отраслей: от телекоммуникаций и финансового сектора до сфер энергетики, транспорта и фармацевтики. Партнерами Tufin выступают ведущие поставщики товаров и услуг, такие как Amazon Web Services, BMC, Blue Coat, Check Point, Cisco, F5 Networks, Fortinet, Intel Security, Juniper Networks, Palo Alto Networks, VMware и другие. Компания известна своими технологическими новшествами и высоким уровнем обслуживания потребителей.

## Несколько слов о Palo Alto Networks

Palo Alto Networks — компания, успешно реализующая в своих решениях совмещение высочайшей производительности и высококачественной фильтрации трафика для защиты сетевых инфраструктур. Оборудование Palo Alto Networks защищает тысячи сетей компаний разных видов деятельности: правительственных учреждений, производственных фирм, компаний-поставщиков услуг, торговых организаций. Целостная и интегрированная платформа безопасности Palo Alto Networks надежно защищает информационные активы Заказчиков, оперируя неотъемлемыми понятиями межсетевых экранов следующего поколения: объекты приложений, пользователей, идентификаторы контента. Более подробную информацию о решениях можно получить на сайте www.paloaltonetworks.com.

## Коротко о Tufin

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

**Клиенты:** более 1500 в более чем 50 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 и другие

tufin

www.tufin.com



SB-4-15

paloalto NETWORKS