VMware NSX с комплексным управлением безопасностью от Tufin

Краткий обзор в рамках технологического партнерства

Повышение безопасности программно-ориентированных сетей

Программно-определяемые ЦОД (SDDC) и частные сети на основе VMware NSX позволяют значительно повысить число и плотность полезных информационных ресурсов и сетевых коммуникаций, а также снизить операционные расходы. А значит - применять более экономичную модель капиталовложений.

VMware NSX обеспечивает виртуализацию сетевых инфраструктур, предоставляя собой полнофункциональную платформу создания оверлейных сетей. С помощью NSX создается виртуальная сетевая инфраструктура «поверх» физической сети, полностью готовая к работе. Кроме успешной виртуализации хостов, сервисов, сетевого оборудования и каналов передачи данных – NSX является основой для создания полностью виртуализованного центра обработки данных.

Кроме того, VMware NSX предлагает встроенные методы защиты оверлейных сетей. При работе с SDDC механизмы NSX предоставляют возможность создания «изолированных» наборов политик безопасности, используемых соответственно для различных виртуальных подсетей, сегментов, объектов виртуальных машин. При этом решение содержит возможность использования логических коммутаторов, маршрутизаторов, межсетевых экранов, балансировщиков трафика и т.п.

NSX по умолчанию обеспечивает должный уровень сегментирования и изоляции определяемых сегментов. Виртуальные сети используют собственное адресное пространство, и могут не располагать (если так надо) каналами для связи между собой или физическими сетями. Собственные брандмауэры и функция реализации политик в виртуальном слое обеспечивают разбиение среды на микросегменты для контроля безопасности на уровне сервисов, приложений, экземпляров виртуальных машин.

Благодаря технологии оверлейных сетей (SDDC) - предоставляется возможность создать более гибкую и гранулированную архитектуру сетевой безопасности, обеспечивая при этом высокую масштабируемость и должный уровень доступности сервисов.

Tufin Orchestration Suite™ для VMware NSX

VMware NSX — это гибкая платформа виртуализации, позволяющая осуществлять развертывание самых современных решений мониторинга и контроля, таких как Tufin Orchestration Suite. Tufin Orchestration Suite представляет собой комплексное решение анализа, оценки и внесения корректив на уровень логического доступа, контролируемый оборудованием сетевой защиты. От 3-его уровня модели OSI до уровня приложений.

С помощью Tufin Orchestration Suite специалисты ИТ и служб информационной безопасности могут централизованно администрировать и контролировать логический доступ между микросегментами в физических и оверлейных сетях, постоянно вести наблюдение за соответствием доступов правилам корпоративной безопасности, а также автоматизировать задачи защиты ключевых бизнес-приложений. Tufin Orchestration Suite обеспечивает высочайший уровень визуализации оверлейных сетей на основе VMware NSX, при этом обладая мощными механизмами анализа и контроля безопасности. Решение гарантирует реализацию комплексного управления правилами безопасности в физических, виртуальных и смешанных сетях.

Разбиение на микросегменты в программно-ориентированных ЦОД
Совместное использование решений VMware NSX и Tufin Orchestration Suite обеспечивает визуализацию и контроль внутреннего разделения корпоративной LAN-сети, что упрощает создание и применение релевантных политик защиты. С помощью функционала Security Zone Matrix можно контролировать нарушения по трафику между самостоятельно определяемыми микросегментами, при этом переходя барьер «классического» разделения зон на «внешние, внутренние и DMZ»(см. рис. 1).

Особенности

Совместное использование VMware NSX™ и Tufin Orchestration Suite™ обеспечивает консолидированное управление правилами безопасности доступов физических и виртуальных сетей. Ключевые преимущества:

- контроль доступов в физических, виртуальных и смешанных сетях, микросегментах;
- централизованное управление правилами безопасности брандмауэров, маршрутизаторов и коммутаторов всего программного ЦОД с помощью единого интерфейса;
- выполнение оценки рисков до внесения корректив в правила ACL оборудования;
- реализация оперативного мониторинга соответствия, анализ и оповещения при возникновении нарушений;
- постоянное отслеживание изменений в конфигурациях правил безопасности для оборудования физических и виртуальных сетей;
- ускорение подготовки к аудитам вплоть до 70%.

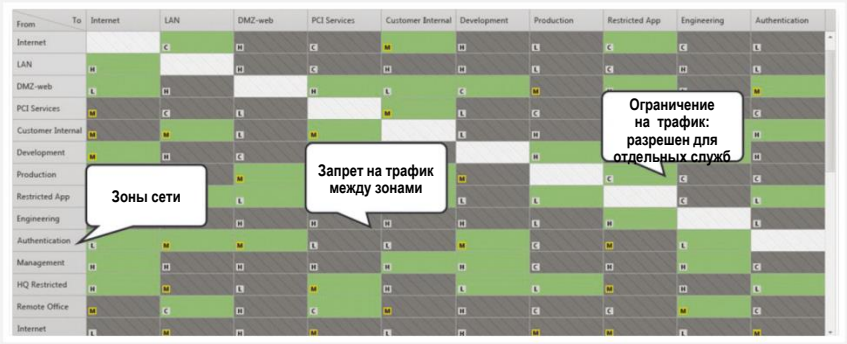

Рис. 1. Функционал Security Zone Matrix в решении от компании Tufin

При этом функционал Tufin Orchestration Suite предоставляет возможность проверять потенциальные нарушения в изменениях доступа до их фактического внесения, как и создавать гибкие бизнес-процессы по распределению полномочий между специалистами.

Управление соответствием в структурах программно-ориентируемых сетей
Tufin Orchestration Suite позволяет специалистам централизованно оценивать и корректировать соответствие между правилами доступа на сетевых логических устройствах в NSX и внутренними требованиями безопасности с помощью централизованного интерфейса. Благодаря оперативным отчетам и оповещениям о нарушении такого соответствия - компания может значительно сократить время подготовки к проверкам, обеспечивая постоянный контроль соответствия.

Комплексное управление правилами безопасности
Tufin Orchestration Suite консолидирует управление правилами безопасности всего центра обработки данных, работая с решениями ведущих поставщиков средств защиты сети как для физических, так и для виртуализованных сред. Tufin Orchestration Suite позволяет осуществлять постоянный мониторинг и оперативное оповещение при изменении конфигураций правил безопасности физических и виртуальных брандмауэров, маршрутизаторов и коммутаторов. Благодаря функциям отслеживания и визуального представления изменений – специалисты ИТ и служб информационной безопасности получают полную картину внесенных в конфигурации корректив. Наглядность позволяет понять кто, когда и почему вносил эти коррективы, и оценить влияние на безопасность при каждой инициации внесения изменений.

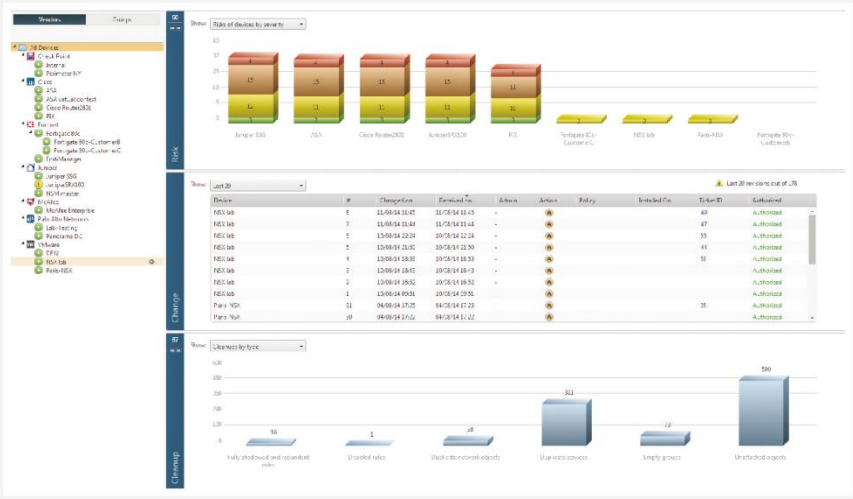

Рис. 2. Панель верхнего уровня Tufin

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

Резюме

Совместное использование VMware NSX и Tufin Orchestration Suite представляет возможности централизованной визуализации, анализа и автоматизации сетевых доступов для существующего или проектируемого программно-ориентированного центра обработки данных. Это решение позволяет организациям пользоваться всеми преимуществами SDDC, одновременно обеспечивая соблюдение должных мер сетевой безопасности, учитывая внутреннюю структуру микросегментов, а также требований доступности ключевых бизнес-приложений.