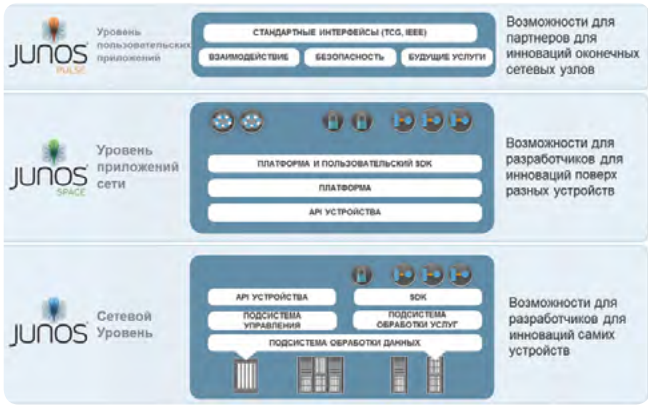
СЕТЕВАЯ БЕЗОПАСНОСТЬ ЦОД — СИСТЕМНЫЙ ПОДХОД

ИГОРЬ СУЩЕВСКИЙ

Тема информационной безопасности многогранна и охватывает множество компонентов и уровней обеспечения. В то же время, сетевая инфраструктура любого предприятия является базисом, который позволяет обеспечить непосредственный обмен данными в системе. В связи с этим важно уделить внимание компонентам сетевой безопасности и особый интерес в этом аспекте представляют технологии компании Juniper Networks.

Решения Juniper в области сетевой безопасности можно условно разделить на две группы: по типу использования и по функциональному назначению систем. Первая группа включает продукты для защиты корпоративной сети, ресурсов центров обработки данных, ресурсов серверов приложений и, наконец, защиты инфраструктуры клиентов как сервис-провайдера.



Многоуровневая структура операционной системы Junos

Ко второй группе можно отнести решения для защиты периметра сети, виртуальной среды, веб-приложений и клиентских сетевых устройств. Также сюда входят унифицированный контроль доступа, управление компонентами и устройствами безопасности, мониторинг событий безопасности.

Защита периметра сети

Только чётко обозначив границы ответственности, очертив периметр, в пределах которого находятся защищаемые ресурсы, можно переходить к правилам, которые будут определять условия пересечения линий разграничения. В информационном пространстве такие границы часто размыты, а правила, по которым происходит обмен данными, выполнить не просто из-за их частой противоречивости и наличия большого числа анализируемых параметров. Перечисленные факты предъявляют высокие требования к функционалу граничных устройств и их производительности.

Для работы на границе сети компания Juniper предлагает универсальное решение на основе платформы SRX, полностью удовлетворяющее предъявляемым высоким требованиям. Платформа обеспечивает необходимую скорость, безотказность и масштабируемость при выполнении операций в центре обработки данных или обслуживания сети в филиале предприятия. Безопасность серии SRX, сервисы защиты и широкие возможности маршрутизации основаны на архитектуре динамического предоставления услуг операционной системы Junos.

В рамках платформы SRX компания Juniper предлагает два подкласса устройств, отличающихся своей специализацией и, как следствие, набором уникальных для каждого подкласса характеристик.

Шлюзы Services Gateway серии SRX для филиалов предприятия объединяют в одной платформе службы коммутации и маршрутизации трафика, трансляции сетевых адресов (NAT), обеспечивают требуемое качество обслуживания (QoS) и мониторинг производительности. Устройства позволяют выполнять безопасное объединение филиалов по шифрованным каналам (VPN) через глобальные сети, поддерживают унифицированное управление защитой от угроз (UTM).

Продукты Services Gateway SRX для центров обработки данных, в первую очередь, предназначены для защиты сетей крупных предприятий, поставщиков телекоммуникационных и сервисных услуг. В дополнение к общим функциональным характеристикам SRX-платформы данный класс устройств обладает уникальной масштабируемостью и производительностью, позволяет проводить потоковую обработку трафика. За счёт модульной архитектуры имеется возможность гибкого наращивания вычислительных и коммуникационных ресурсов платформы, не прерывая работы. Такие характеристики обеспечивают рост сетевой инфраструктуры без ухудшения безопасности, способствуют быстрому развёртыванию управляемых услуг и объединённым решениям по безопасности.

Кроме того, шлюзы Services Gateway серии SRX имеют в своём составе расширения системы безопасности AppSecure. Данная подсистема позволяет выполнять классификацию и идентификацию сетевых приложений для проведения глубокого анализа поведения и поиска уязвимости приложений, обеспечивает выполнения политик безопасности и управления этими политиками в рамках общей стратегии защиты сети.

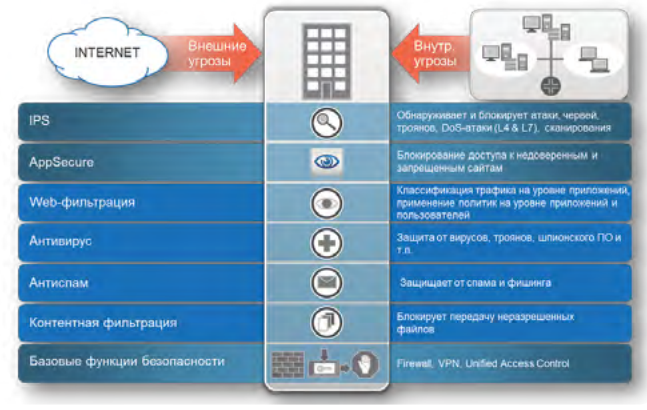
Подсистема AppSecure содержит в своём составе пять логических модулей, которые совместно реализуют комплексный подход к защите сети и управлению политиками безопасности шлюзов серии SRX. Посредством модуля AppTrack осуществляется комплексный анализ данных для получения подробной информации о типах сетевых приложений и их классификации по уровням риска, идентификаторам пользователей, зонам, адресам отправителей и получателей, объёмам переданной информации. Данный модуль используется для оценки соответствия проходящего трафика разрешённым политикам, формирования правил управления полосой пропускания и сбора статистики об активности пользователей и приложений.

Для формирования подробных правил управления трафиком на основе названия приложения или названия группы динамически загружаемых приложений используется модуль AppFW. Для упрощения правил и определения дальнейших действий в отношении анализируемого трафика применяются разрешительные и ограничительные списки приложений.

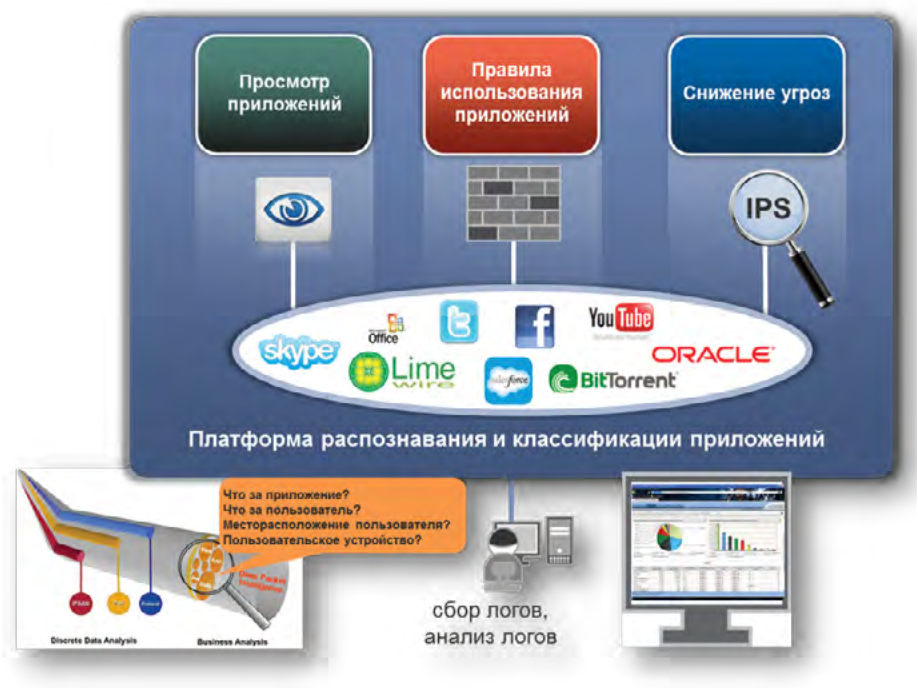
Модуль AppQoS в системе безопасности отвечает за процедуру маркировки трафика приложений и его обработку. В результате работа критически важных приложений не прерывается во время пиковых нагрузок, менее важные приложения получают доступ к сетевым ресурсам по мере высвобождения полосы пропускания. Этот модуль поддерживается в шлюзах серии SRX, предназначенных для центров обработки данных.

Стоит отметить, что AppDoS умеет распознавать и отделять вредоносный трафик злоумышленников от нормального трафика, тем самым эффективно предотвращая атаки типа «отказ в обслуживании» (DoS). Многоуровневый алгоритм модуля распознает аномалии в поведении сетевого трафика, сигнализирующие о DoS-атаках, выдаёт предупреждения, блокирует IP-адреса, полностью разъединяет не отвечающие правилам сессии и отбрасывает нестандартные пакеты.

Система предупреждения вторжений (IPS) транслирует функции безопасности приложений на сетевую инфраструктуру. Тем самым минимизируются риски возникновения угроз, и обеспечивается защита от них. Данный модуль применяется при анализе данных и идентификации контекстуализированных приложений для определения методов декодирования протоколов и распознавания алгоритмов атак при прохождении трафика, обрабатываемого IPS.



Структура системы защиты, обеспечивающей безопасность центров обработки данных и корпоративных сетей



Подсистема AppSecure позволяет выполнять классификацию и идентификацию сетевых приложений для проведения глубокого анализа поведения и поиска уязвимости приложений

Защита виртуальной среды

Для обеспечения безопасности виртуальных центров обработки данных и облачных служб используется решение Virtual Gateway (vGW), которое защищает виртуальную сетевую инфраструктуру, обеспечивая максимальную масштабируемость и производительность. В этом решении межсетевой экран на основе гипервизора содержит интегрированную систему обнаружения вторжений (IDS), средства антивирусной защиты для виртуальных сред (AV) и средства отслеживания соответствия стандартам сетевого взаимодействия.

Шлюз vGW осуществляет мониторинг всего сетевого трафика и контролирует применение корпоративных и нормативно-правовых политик безопасности в виртуальном пространстве центров обработки данных. Кроме того, шлюз обеспечивает разделение выполняемых функций, в соответствии с бизнес-логикой функционирования приложений, и проверяет выполнение политик относительно всех транзакций в виртуальном пространстве. В соответствии с правилами доступ к виртуальной машине может быть ограничен приложением, протоколом, а также типом и ролью самой виртуальной машины.

Групповые политики создаются по результатам анализа данных, полученных при взаимодействии подсистем VM Introspection и vCenter, и обеспечивают защиту определённых типов виртуальных машин. Так же подсистема VM Introspection обеспечивает полную визуализацию сетевого трафика, передаваемого между виртуальными машинами, что позволяет выполнять полную инвентаризацию параметров виртуальных машин или групп виртуальных машин, включая настройки виртуальных сетей. Кроме того, подсистема позволяет получить подробные сведения о состоянии каждой виртуальной машины, включая тип операционной системы и перечень установленных приложений.

Межсетевой экран с контролем состояния соединений предоставляет дополнительные уровни защиты и автоматическую систему обеспечения безопасности. Применяется контроль доступа для всех типов трафика с помощью набора правил, определяющих, какие протоколы, порты, адреса сетевых узлов и виртуальных машин должны быть заблокированы. Встроенный механизм обнаружения вторжений проверяет трафик на предмет аномальной активности при выполнении соединений, а так же анализирует сетевые данные на наличие вредоносных программ. При необходимости выдаётся предупреждение о подозрительной активности, а средства антивирусной защиты выполняют сканирование дисков и файлов виртуальной машины с возможностью перемещения подозрительных файлов в карантин.

В статье были затронуты лишь самые важные решения для обеспечения безопасности ЦОД. Более подробный обзор — предмет будущих публикаций.

Автор статьи — главный консультант отдела системных решений «ЭС ЭНД ТИ УКРАИНА»