Решение обеспечения безопасности J-Protect

Превратим уязвимость в защиту

Poplar SYSTEMS

“Обеспечение безопасности для конечных пользователей – одна из основных задач компании Telecom New Zealand. Решить эту задачу нам помогла Juniper Networks, предоставив интегрированное масштабируемое решение J-Protect для всех ключевых точек”.

Мюррей Милнер
Главный технолог
Telecom New Zealand

Введение

Защита пользователей, приложений и сетевых решений от атак злоумышленников стала одной из основных задач сетевых операторов, особенно в условиях растущей частоты и постоянного усложнения кибернетических угроз. До недавнего времени выполнение этого требования было достаточно сложным и дорогостоящим. Существующие стратегии защиты подразумевали применение разнообразных архитектур, устройств и систем управления. В результате не только увеличивались эксплуатационные затраты, но и становилось невозможным развитие рынка услуг обеспечения безопасности.

Сетевая индустрия находится на пороге глобальных преобразований. При правильном подходе она готова перейти от экономических ценностей Интернет-модели к единой интегрированной сетевой инфраструктуре, в которой всеохватность открытой сети Интернет объединится с защищенностью и управляемостью частных сетей. Образцом для таких преобразований послужат "инфрасети", характеризующиеся одновременно масштабами и охватом открытых сетей и безопасностью и управляемостью частных сетей. Особую роль в грядущих преобразованиях играет безопасность, в частности, защита инфрасети и защита пользователей этой сети.

Решение обеспечения безопасности Juniper Networks J-Protect предлагает единый, масштабируемый, унифицированный комплекс защитных средств, предназначенный для удовлетворения вышеизложенных требований. Созданный на базе трансформационной модели Juniper Networks MINT (Model for InfraNet Transformation) комплекс J-Protect объединяет в себе все ее четыре уровня: пакетная передача от каждого к каждому, сегментация ресурсов, обработка пакетов, контроль и политики. Такое сочетание основных "китов" безопасности не только позволяет оператору экономично защитить свою собственную сеть, используя согласованный комплекс программных и аппаратных платформ, но и выходить на новые рынки, привлекать новых пользователей, предлагая инновационные пакеты услуг обеспечения безопасности.

Комплекс J-Protect, являясь интегральной частью всех платформ Juniper Networks, обеспечивает интеграцию, масштабируемость и охват, необходимые для создания инфрасетей и преобразования сетевой индустрии.

Рисунок 1. J-Protect и модель трансформации MINT

Инструментарий J-Protect Toolkit

Фундамент решения обеспечения безопасности Juniper Networks J-Protect составляет инструментарий J-Protect Toolkit, предоставляющий интегрированные функции защиты для всех продуктов Juniper Networks. Инструментарий J-Protect Toolkit предоставляет полнофункциональный набор возможностей для защиты как самой сети, так и ее пользователей.

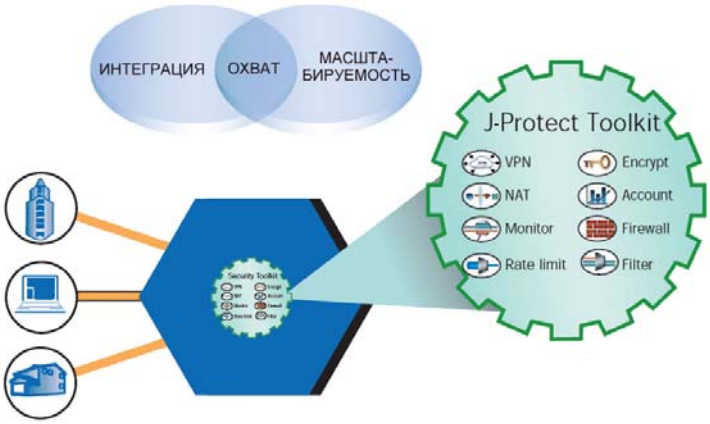

Рисунок 2. Инструментарий J-Protect Toolkit

Основные функции:

- Фильтрация и ограничение скорости
- Шифрование
- Виртуальные частные сети (VPN) IPSec/MPLS
- Мониторинг потока
- Трансляция сетевых адресов (NAT)
- Межсетевой экран в режиме Stateful
- Учет

Важно отметить, что интеграция и унификация функций J-Protect Toolkit гарантируют сетевым операторам как гибкость, так и возможность постепенного масштабирования. Специализированные средства J-Protect, такие как, например, мониторинг потоков или межсетевой экран в режиме stateful, быстро, легко и экономично масштабируются в случае необходимости расширения сети.

Защитите вашу сеть

Надежная и экономичная защита сети – одна из основных задач любого бизнеса. Однако с усложнением и ростом количества атак (по данным Координационного центра CERT, количество атак выросло с 21756 в 2000 до 82094 в 2002 г.) сетевые операторы зачастую прибегают к точечным или наложенным решениям, предназначенным для устранения определенной угрозы или защиты конкретных сетевых компонентов, что приводит к неоправданному усложнению эксплуатации и росту издержек. Кроме того, такой сценарий усложняет создание и развертывание управляемых услуг обеспечения безопасности и снижает и рентабельность.

Решение Juniper Networks J-Protect предлагает операторам альтернативу точечным решениям, которая заключается в том, что безопасность начинается с изначально защищенной инфраструктуры. Всеохватный, интегрированный подход, реализованный в решении J-Protect, предусматривает:

- защиту устройств;
- защиту подсистем управления;
- разделение частных и открытых потоков информации.

Такой подход позволяет оператору создать поле защищенных ресурсов, используемых для обеспечения конкретных требований пользователей по безопасности и производительности.

Защита устройств

Защита сети начинается с оборудования. Если не защитить от возможных атак все устройства, сетевые ресурсы и, соответственно, данные пользователей находятся под угрозой. Оборудование Juniper Networks разработано с учетом возможности унифицированного развертывания сетевой защиты.

- Разделение функций подсистем управления и данных обеспечивает защиту управляющего трафика в режиме stateless.
- Защита управляющего трафика в режиме stateful.
- Ограничение скорости по отдельным протоколам.
- Унификация функций по всем платформам Juniper.
- Защищенное администрирование с использованием командной строки:
  - многоуровневый пользовательский доступ;
  - шифрование;
  - централизованная аутентификация (RADIUS и TACACS+).
- Регистрация и аудит

- Контроль конфигурационных изменений
- Подтверждение и откат конфигурации для минимизации ошибок.

Защита подсистемы управления

Подсистема контроля включает важнейшие протоколы управления и маршрутизации, обеспечивающие межсетевое взаимодействие. Для защиты подсистемы контроля Juniper Networks использует следующие методы.

- Защита адресов обратной связи (loopback addresses). Интерфейсу между подсистемами контроля и форвардинга могут присваиваться виртуальные адреса, что позволяет реализовать механизмы фильтрации и ограничения скорости в целях безопасности. Таким образом между подсистемами контроля и форвардинга создается "виртуальная демилитаризованная зона", гарантирующая защиту важнейших функций управления маршрутизатором.
- Шифрование. Juniper Networks реализует шифрование для протоколов маршрутизации, таких как BGP, а также широкополосные сервисы защиты на базе IPSec. Поддержка цифровых сертификатов облегчает управление ключами и защищенными связями (security associations).
- Защита в режиме stateful. Для анализа трафика управления (напр., TCP) в режиме stateful используется модуль Juniper Networks Adaptive Services PIC (ASP), распространяющий защиту на важнейшие функции управления.

Разделение частных и открытых потоков информации

Логическое разделение открытого и частного трафика посредством виртуальных частных сетей (VPN) разделяет пользовательский трафик по виртуальным общностям и гарантирует отделение данных контроля и управления от сервисного трафика. Сети VPN на основе туннельных технологий (L2TP, IPSec) могут также использоваться для создания экстрасетей, безопасной межсетевой передачи или абонентских сообществ. Juniper Networks предлагает широкий портфель сервисов VPN и сегментации.

- VPN уровня 2
- VPN уровня 3 (2547)
- Операторские VPN
- VPN между провайдерами
- VPLS

Виртуальная маршрутизация Juniper Networks также обеспечивает логическое разделение путем сегментации множества пользователей или заказчиков в пределах одного маршрутизатора. Такая сегментация ресурсов на уровне устройства имеет существенные преимущества при развертывании управляемых сервисов, снижая капвложения и гарантируя безопасность и разделения информации форвардинга и маршрутизации заказчика.

Рисунок 3. Защитите вашу сеть

Применение J-Protect

Сервис-провайдеры
Высокая производительность фильтрации и ограничения скорости J-Protect помогает сервис-провайдерам обезопасить свою собственную сетевую инфраструктуру и позволяет использовать те же платформы для оказания прибыльных услуг VPN и управления безопасностью.

Правительственные организации
J-Protect предоставляет полнофункциональный инструментарий для защиты сетевой инфраструктуры, обеспечения конфиденциальности информации и тщательного анализа трафика.

Наука и образование
J-Protect предоставляет широкий спектр средств сетевой сегментации, фильтрации и ограничения скорости, позволяя усилить контроль за конкретными сообществами пользователей, облегчить защиту от подмены адресов и атак типа "отказ в обслуживании".

Предприятия
J-Protect предлагает интегрированную трансляцию адресов NAT, межсетевой экрана в режиме stateful, средства VPN для реализации полнофункционального, высокопроизводительного клиентского решения; предприятия, интенсивно обменивающиеся информацией, по достоинству оценят средства фильтрации, ограничения скорости и учета J-Flow.

Защитите своих пользователей

В своем недавнем исследовании компания IDC отметила, что приблизительно 60 - 70% всех межсетевых экранов неправильно сконфигурированы, а Национальный альянс кибернетической безопасности обнаружил, что у 40% пользователей широкополосных сетей межсетевой экран вообще отсутствует. Эти данные в сочетании с возрастающей частотой атак, о которой говорят документы агентств CERT и CAIDA, говорят о необходимости ускоренного внедрения пользовательских решений обеспечения безопасности. Неудивительно, что в прогнозе Infonetics Research прогнозируется более чем 100% рост затрат конечных пользователей на услуги защиты и VPN к 2006 г.

Сетевые операторы, внедрившие решение Juniper Networks J-Protect, могут использовать возможности интеграции, масштабирования, унифицированные средства управления решения не только для защиты своих активов, но и для оказания прибыльных услуг по обеспечению безопасности.

Базовые услуги обеспечения безопасности

Основной заботой большинства предприятий, пользующихся услугами сетей, является защита своего канала доступа, связывающего их с сетью сервис-провайдера. Полоса пропускания этого канала является как существенной статьей расходов, так и важнейшей частью повседневного бизнес-процесса. Как следствие, многие предприятия и правительственные организации обращаются к операторам за гарантиями по основным параметрам полосы пропускания. Многие заказчики Juniper Networks используют для выполнения этих требований базовый пакет обеспечения безопасности, включенный в ПО JUNOS (фильтрация, ограничение скорости, учет, маршрутизация в соответствии с правилами). Универсальная интеграция данных средств по всем продуктам Juniper Networks в сочетании с их высокой производительностью позволяет операторам значительно повысить привлекательность своих предложений для предприятий и конечных пользователей.

Межсетевой экран в режиме stateful и трансляция сетевых адресов

Функции МЭ в режиме stateful и трансляции сетевых адресов (NAT) реализуются с помощью модулей адаптивных сервисов Adaptive Services PIC и туннельных сервисов Tunnel Service Module. Эти высокопроизводительные, масштабируемые платы позволяют операторам настраивать сервисы МЭ и NAT в соответствии с расширяющимися сервисными требованиями. Постепенное инкрементное масштабирование обеспечивает экономичное развертывание сервисов путем простого добавления плат без необходимости долгосрочного планирования и приобретения излишней аппаратуры.
С помощью системы развертывания сервисов Juniper Networks SDX корпоративные заказчики могут создавать и контролировать различные профили безопасности для множества площадок, а сетевой оператор в составе управляемых услуг обеспечения безопасности может контролировать и модифицировать профили отдельных пользователей. Вследствие тесной интеграции и унификации инструментария J-Protect Toolkit сервисы NAT и МЭ легко объединяются с другими сервисами J-Protect, такими как MPLS VPN, при необходимости создания всеобъемлющих бизнес-предложений или полных решений по предоставлению управляемых услуг.

Шифрование

Juniper Networks реализует шифрование на базе IPSec на скорости до 800 Мбит/с при 5000 туннелей на одну сервисную карту, обеспечивая простое и экономичное масштабирование шифрования. Такой подход позволяет сетевым операторам комбинировать базовые сервисы доступа и транспорта с шифрованием IPSec для предоставления различных защищенных услуг.

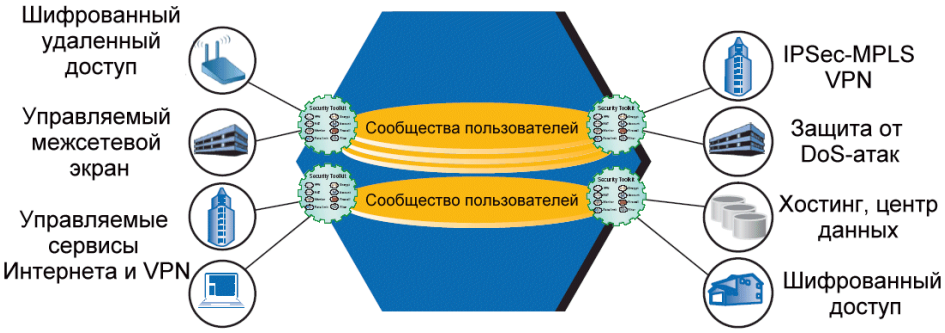

Рисунок 4. Защитите своих пользователей

- Защищенный удаленный доступ
- Защищенные точки беспроводного доступа (hot spots)
- Услуги VPN на базе IPSec
- Защищенный транспорт трафика других провайдеров

Как и сервисы МЭ и NAT, сервисы шифрования реализованы на всех платформах Juniper Networks и могут легко соединяться с другими средствами J-Protect в пакеты услуг.

Дополнительные сервисы

Постоянный рост количества кибер-атак требует постоянного развития решений защиты. Решение Juniper Networks J-Protect предоставляет сетевым операторам дополнительные возможности для предоставления услуг обеспечения безопасности с учетом последних угроз.

- Атаки типа "отказ в обслуживании" (DoS) – один из ярких примеров постоянного развития и усложнения кибер-атак. Для борьбы с ними Juniper Networks предлагает интегрированные средства J-Protect Toolkit:
    - Мониторинг потока (составная часть решения Juniper Networks J-Flow). Выборка и анализ данных для выявления подозрительных действий без ухудшения характеристик форвардинга.
    - Классы назначения (DCU). Инструментарий DCU позволяет подсчитывать трафик с определенным префиксом назначения для трассировки входных точек атак DoS и принятия соответствующих мер (отбрасывание или ограничение скорости).
    - Предотвращение подмены адреса. Эта функция использует метод uRPF (Unicast Reverse Path Forwarding) для проверки и верификации исходных адресов, позволяя оператору предотвращать их подмену адресов.
- Anti-worm. деятельность сетевых червей часто характеризуется значительным повышением загрузки полосы пропускания абонента на конкретном порту TCP. Функции политик и слежения J-Protect в сочетании с системой развертывания сервисов SDX Service Deployment System дают оператору возможность устанавливать пороги полосы пропускания. если порог превышен вследствие подозрительной активности, абонент или конечный пользователь перенаправляется на специальный портал и уведомляется о наличии вируса и возможных способах его устранения.
- Перенаправление спама. Мощные средства фильтрации пакетов и ограничения скорости Juniper Networks, такие как форвардинг на основе фильтров, могут использоваться в сочетании с системами обнаружения спама для фильтрации тысяч известных источников спама. Отфильтрованный трафик либо автоматически отбрасывается, либо перенаправляется до того, как он повлияет на производительность сети или приложения.

Всеобъемлющий подход, реализованный в системе обеспечения безопасности J-Protect, позволяет сетевым операторам предоставлять прибыльные услуги по обеспечению безопасности. От базовых сервисов МЭ, NAT и шифрования до расширенных сервисов отражения атак типа "отказ в обслуживании", обнаружения червей и фильтрации спама, решение J-Protect предлагает сетевым операторам масштабируемый, интегрированный и универсальный подход для быстрого и экономичного предоставления востребованных услуг.

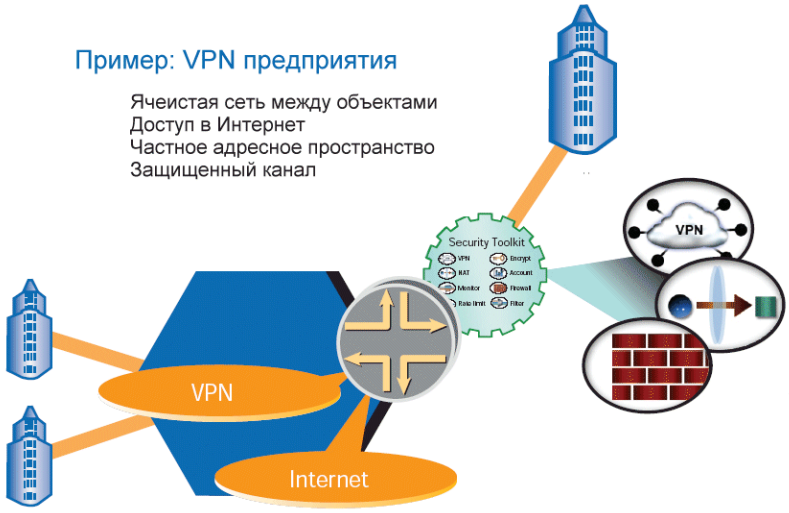

Рисунок 5. J-Protect VPN и сервисы безопасности

Преобразование сетевого бизнеса

Конечно же, главным преимуществом решения J-Protect является его важность для достижения основной цели сетевой индустрии - преобразования. По мнению Juniper Networks, уникальная концепция глобальной сетевой инфраструктуры на базе инфрасетей обеспечит как операторам, так и пользователям преимущества с точки зрения экономики, производительности и безопасности. Инфрасети, основанные на общей платформе IP и MPLS, обеспечат предоставление пользователям высококачественных и защищенных услуг и приложений на базе различных сетевых технологий в сетях разных сервис-провайдеров.

Решение обеспечения безопасности Juniper Network J-Protect предоставляет необходимые средства для развертывания инфрасетей уже сегодня. Сервисы J-Protect основаны на стандартах и универсально реализованы на всех аппаратных и программных платформах Juniper Networks; с их помощью операторы могут оказывать услуги уже сейчас, будучи готовы к дальнейшему масштабированию. Самое важное, что решение J-Protect позволяет операторам гарантировать качество обслуживания пользователей независимо от требований приложений.

Безопасность будет играть главную роль в реализации долгосрочных целей инфрасетей: обеспечение расширения сервисов за пределами собственной инфраструктуры оператора. Сетевые операторы прекрасно понимают значение возможности расширения своих сервисных предложений за пределы сегодняшней сетевой географии. Однако для выхода на новые рынки необходимо обеспечить защиту на границе сетей. Реализация обеспечения безопасности на практике требует, однако, нового открытого стандарта взаимосвязи операторов инфрасетей.

Juniper Networks, ее партнеры и заказчики уже работают над новым стандартом.

Заключение

Решение Juniper Networks J-Protect предоставляет сетевым операторам интегрированный, масштабируемый и универсальный инструментарий для экономичной и эффективной защиты сетевых ресурсов от атак злоумышленников. Кроме того, J-Protect предлагает сетевым операторам фундамент для предоставления новых прибыльных услуг с использованием межсетевых экранов, NAT, защиты от атак DOS, сетевых червей и спама. Все эти возможности обеспечения безопасности встроены в платформы Juniper Networks. Решение J-Protect – это краеугольный камень создания инфрасетей и непрерывной трансформации сетевой индустрии.

http://www.poplar.ru