КРАТКОЕ ТЕХНИЧЕСКОЕ ОПИСАНИЕ

Arbor Peakflow SP

ГЛУБОКАЯ ВИЗУАЛИЗАЦИЯ И ЗАЩИТА СЕТИ, УПРАВЛЯЕМЫЕ УСЛУГИ

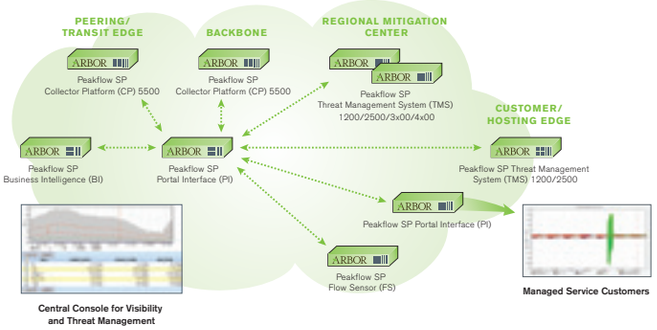
Интернет и хостинг-провайдеры, крупные корпорации – все сталкиваются с проблемами предоставления надёжного и качественного сервиса за приемлемую цену. С учётом постоянно растущих объемов трафика и трендов по переходу на протокол IPv6, решение таких проблем является нетривиальной задачей, и компания Arbor Networks это знает лучше многих. Arbor Peakflow SP ("Peakflow SP") - это решение не только для глобального анализа трафика, но и обеспечения безопасности и доступности всей сети. Будучи де-факто стандартом для большинства мировых сервис-провайдеров, Peakflow SP является ключевым элементом системы защиты от DDoS-атак. Сегодня решения Peakflow SP анализируют и защищают более 70% глобального интернет-трафика

Знание - сила

Arbor Peakflow SP - это уникальное решение для обнаружения аномалий и интеллектуальной защиты в масштабах всей сети. Peakflow SP изучает поведение трафика, используя данные сетевых потоков, SNMP и обновления BGP с сотен маршрутизаторов и тысяч интерфейсов, а затем коррелирует эти шаблоны с данными о топологии для построения логической модели. Эта информация позволяет технической поддержке и специалистам по информационной безопасности обнаруживать и предотвращать угрозы доступности, повышать производительность сети и сервисов, а также принимать правильные решения при планировании развития сети и предлагаемых сервисов.

Peakflow SP основан на следующих принципах:

- **Анализ сети:** глубокая визуализация сети, приложений и трафика помогает принимать правильные решения по поводу транзитных партнёров, сетевой архитектуры, заказчиков и новых IP-сервисов.
- **Защита сети:** обнаружение и защита от угроз в реальном времени и исчерпывающие отчёты об инцидентах позволяют минимизировать их отрицательное влияние на сеть, услуги, а главное - заказчиков.
- **Развитие сети:** возможность организации и предоставления прибыльных управляемых услуг по защите от DDoS-атак на базе единой платформы Arbor Peakflow SP.



Архитектура Peakflow SP

Архитектура решения включает 5 типов устройств: 1) Платформа сбора данных Peakflow SP Collector Platform (CP) на границе сети или на магистрали; 2) Датчики Peakflow SP Flow Sensor (FS) на границе агрегации клиентского трафика; 3) Устройства Peakflow SP Business Intelligence (BI), обеспечивающие масштабируемость и резервирование для управления критичными бизнес-объектами; 4) Интерфейсные устройства Peakflow SP Portal Interface (PI) для повышения масштабируемости, резервирования и рентабельности управляемых услуг Arbor; 5) Системы Peakflow SP Threat Management System (TMS), устанавливаемые в любой части сети и предназначенные для точного отражения сетевых угроз.

Основные функции и преимущества

Защита сервисов

Обеспечение доступности критичных сервисов, таких как веб, передача голоса, видео, электронная коммерция и электронная почта.

Защита инфраструктуры

Обнаружение и отражение атак, направленных на маршрутизаторы, коммутаторы, межсетевые экраны, серверы DNS и переполнение полосы пропускания. Очистка вредоносного трафика из сети передачи данных.

Улучшение качества сервиса

Отображение ключевых метрик производительности трафика, таких как джиттер, задержки и потери пакетов с разбивкой по типам сервиса. Обнаружение проблем и принятие мер до того, как пользователи начнут проявлять беспокойство.

Оптимизация ресурсов

Визуализация и детальная отчетность для инжиниринга трафика и быстрого, более эффективного решения проблем. Оптимизация транзитных отношений, повышение утилизации и помощь при развитии сети.

Предоставление дополнительных услуг

Используйте платформу Arbor Peakflow SP как для мониторинга и защиты собственной сети, так и для организации и предоставления корпоративным клиентам прибыльных, гибко управляемых услуг по защите от DDoS-атак в облаке провайдера.

ARBOR NETWORKS

Глобальный анализ угроз в реальном времени

Компания Arbor создала сообщество ASERT (Arbor's Network Security, Engineering and Response Team), взаимодействующее с интернет-провайдерами всего мира с целью сбора данных о сетевых атаках и угрозах. Результаты работы группы доступны участникам сообщества и заказчикам Arbor в рамках масштабной инициативы, известной как программа ATLAS (Active Threat Level Analysis System), предоставляющая своим участникам ряд преимуществ:

Портал безопасности ATLAS

Портал безопасности ATLAS (http://atlas.arbor.net) отображает в реальном времени статистику по атакам во всём мире. Эта информация доступна с консоли Peakflow SP, и пользователи системы могут оценить возможное влияние актуальных атак на их сети.

Цифровые отпечатки

При анализе глобальной активности ASERT создаёт так называемые «цифровые отпечатки», регистрирующие характерное поведение трафика в процессе атак. Эти шаблоны автоматически рассылаются пользователям Peakflow SP через специальный сервис ATF (Active Threat Feed) для того, чтобы система Peakflow SP TMS сразу могла обнаруживать и отражать атаки, соответствующие полученным отпечаткам.

Альянс обмена отпечатками FSA

Распределённый характер DDoS-атак зачастую требует от интернет-провайдеров совместных действий в процессе защиты. Чтобы упростить эту задачу, компания Arbor создала сообщество обмена отпечатками FSA (Fingerprint Sharing Alliance), в которое входят пользователи систем Peakflow SP.

Облачная сигнализация

Решение Arbor Pravail для защиты от DDoS-атак совместно с решением Arbor Peakflow SP обеспечивает комплексную защиту от атак, которые направлены как на исчерпание сетевой полосы пропускания, так и на сервисы ЦОДов.

Мощность, масштабируемость и доступность, которая Вам нужна

С ростом сети и постоянным увеличением объёмов трафика неотъемлемым атрибутом решения для мониторинга и обеспечения безопасности является возможность масштабирования. Визуализация всей сети и управление системой защиты от DDoS-атак с максимальной производительностью до 2-х терабит осуществляется с единой консоли Peakflow SP. Peakflow SP не требует установки дополнительных датчиков, сетевых сенсоров и устройств, устанавливаемых в разрыв. Решение поддерживает многочисленные форматы потоков (flow) и форматы данных, что даёт возможность использовать Peakflow SP в самой разнообразной сетевой инфраструктуре.

Всесторонняя и надёжная защита от DDoS-атак

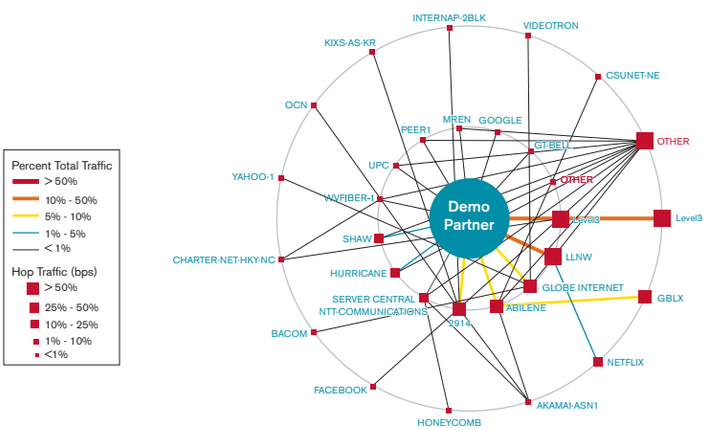
DDoS-атаки являются основной угрозой доступности сети. Peakflow SP защищает как от масштабных атак, направленных на переполнение полосы пропускания каналов связи, так и от атак уровня приложений, направленных на критичные IP-сервисы, такие как DNS, HTTP и VoIP. Опыт Peakflow SP по детектированию сложных атак в связке с полным набором противомер, даёт операторам возможность успешно отражать атаки, при этом оставляя нетронутым легитимный трафик. Peakflow SP является наиболее распространенным и проверенным решением для защиты от DDoS-атак.

Готовность к глобальным изменениям

С введением IPv6, DNSSEC и четырехбайтных ASN сети и центры обработки данных входят в период глобальных изменений, который затрагивает большинство аспектов их операционной деятельности. Теперь, как никогда ранее, специалистам важна всеобъемлющая визуализация состояния сети и защита от DDoS-атак для обеспечения доступности и контроля за издержками. Peakflow SP защищает сети от всё новых разновидностей DDoS-атак и даёт возможность операторам принимать экономически обоснованные решения.

Интеллектуальный инжиниринг трафика, планирование ёмкости и диагностика сети

Peakflow SP обеспечивает детальную визуализацию трафика IPv4 и IPv6, маршрутов протокола BGP, MPLS VPNs, QoS и приложений, включая DNS, VoIP и пиринговые сети P2P. Это даёт возможность оператору определять и устранять проблемы доступности сервисов в режиме реального времени, а также улучшать инжиниринг трафика и планирование ёмкости сети.



Отчёт по анализу пиров - Снижение стоимости транзита

Визуализация сервисов, производительности и защиты

С точки зрения пользователя, всю ценность в сети представляют приложения и сервисы в ней, без которых сеть сама по себе ничего не значит. Разнообразие приложений, от конвергентных сервисов triple-play (дата, голос и видео) до приложений типа IM, Skype™ и YouTube™, делает их оптимизацию как никогда сложной задачей. Используя анализ потоков и содержимого сетевых пакетов, Peakflow SP и Arbor Peakflow Threat Management System ('TMS') автоматически определяют более 90 приложений, а также дают возможность добавлять свои шаблоны приложений для мониторинга. Для обеспечения соответствия потребностям пользователей по качеству сервиса и оптимизации производительности приложений, таких как HTTP, VoIP и DNS, Peakflow SP анализирует показатели таких ключевых метрик, как джиттер, задержки и потери пакетов.

Расширенные возможности для отчетности и управления

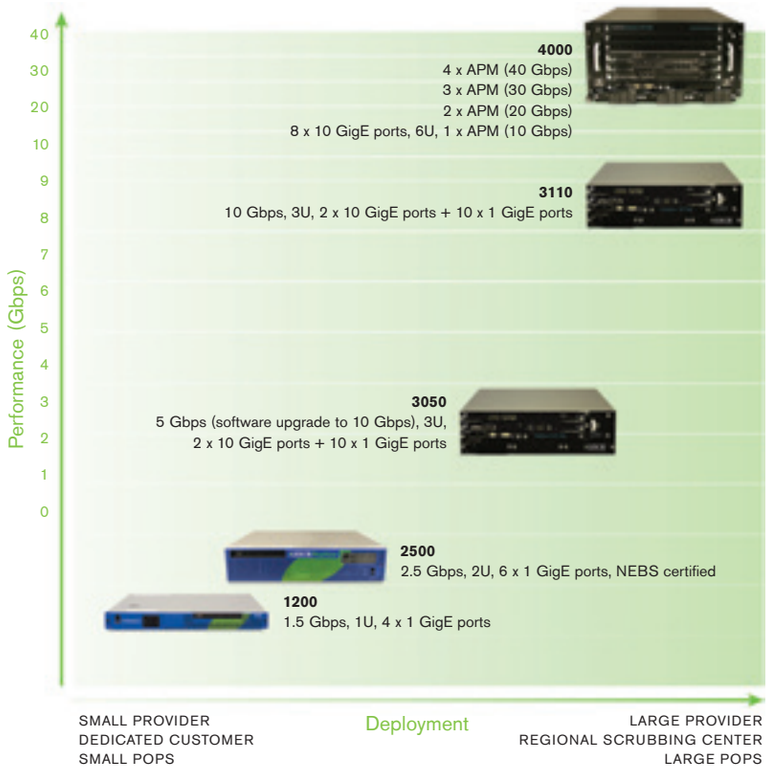
Peakflow SP предоставляет наиболее полные и гибкие возможности для визуализации и обеспечения безопасности. Решение специально создавалось для использования в различных сетях, от крупных компаний до международных сервис-провайдеров. Функционал включает в себя мониторинг, управление и защиту до 10 000 объектов (таких как клиенты, списки IP-адресов, интерфейсы, маршрутизаторы и различные сервисы), расширенные возможности формирования отчётов и детализации, доступа к отчётам по API и ролевое управление.

Дополнительный сервис по защите от DDoS-атак

Peakflow SP снижает стоимость развёртывания и сложность эксплуатации управляемого сервиса по защите от DDoS-атак. Основные особенности включают в себя шаблоны/APIs для настройки портала, резервирование, отказоустойчивость, синхронизацию данных, “oneclick” или автозащиту, настраиваемые шаблоны противомер, консоль с отображением информации в режиме реального времени и широкий список отчётов. Эти функции упрощают предоставление сервиса, повышая доходы и удовлетворённость клиентов. Arbor Peakflow SP TMS играет ключевую роль в управляемом сервисе для защиты от DDoS-атак на базе решения Peakflow SP. TMS - это устройство уровня приложений для конвергентных мультисервисных сетей, которое ускоряет скорость очистки трафика за счёт применения высокоуровневой идентификации угроз с анализом на пакетном уровне. TMS позволяет провайдерам обнаруживать атаки на сетевом уровне и уровне приложений и хирургически очищать вредоносный трафик, при этом не мешая прохождению легитимного трафика.

Оптимизированная защита от DDoS-атак

Важное место при построении системы защиты от атак DDoS занимает правильный выбор модели Peakflow SP TMS. На следующей диаграмме представлены различные модели, параметры производительности и варианты установки систем.



Развертывание Peakflow SP TMS

Комплексные методы обнаружения и отражения угроз

С помощью Peakflow SP и Peakflow SP TMS сервис-провайдер защищает критичные IP-сервисы, используя набор методов обнаружения и отражения атак и аномалий.

Блокировка известных атакующих хостов с использованием чёрных и белых списков. В белый список вносятся авторизованные узлы, в чёрный - зомби и скомпрометированные узлы, чей трафик должен быть заблокирован.

Блокировка вредоносного кода прикладного уровня (эксплойтов) при помощи комплексных фильтров. Peakflow SP TMS обеспечивает надёжную фильтрацию сетевого трафика, отражая замаскированные атаки на критичные сервисы.

Защита от веб-угроз и аномалий с использованием механизмов обнаружения и отражения специфичных HTTP-атак. Эти же механизмы помогают справиться с внезапным ростом посещаемости (атаки типа “flash-crowd”)

Защита сервиса DNS от бот-сетей, маскирующих и передающих эксплойты в инфраструктуру и сервисы DNS. В решениях Arbor Peakflow предусмотрены специализированные средства обнаружения и отражения атак на сервис DNS.

Защита критичных сервисов VoIP от автоматизированных скриптов и бот-сетей, использующих атаки типа “flood” и пакеты с неправильными запросами. В решениях Arbor Peakflow предусмотрены специализированные средства обнаружения и отражения атак на сервисы VoIP/SIP.

Контроль бот-сетей с использованием специализированных, постоянно совершенствующихся средств обнаружения зомби и предотвращения атак на инфраструктуру с зараженных хостов.

Обеспечение базовой защиты путём построения самообучающихся моделей сетевого поведения. Получаемая информация может использоваться для идентификации аномального трафика и его блокирования в момент атаки.

“Мы используем продукты Arbor Peakflow с самого начала, когда мы были лишь небольшим интернет-провайдером, вплоть до сегодняшнего дня, несмотря на то что переросли в сервис-провайдера международного уровня. После пяти лет сотрудничества, могу сказать, что работать с Arbor - одно удовольствие. Я без колебаний рекомендую оборудование Arbor любому, кто эксплуатирует IP-сеть, независимо от масштаба.”

Christiaan Keet, Network Services Director, Easynet Global Services

Peakflow SP Appliances

Arbor Peakflow SP Collector Platform (CP), Flow Sensor (FS), Business Intelligence (BI), Portal Interface (PI). Все устройства имеют одинаковый корпус

NETWELL

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР НЕТВЕЛЛ

г. Москва, 1-й Дербеневский пер., дом 5
Контакты: +7 (495) 66 239 66
info@netwell.ru
www.netwell.ru

ARBOR NETWORKS

Корпоративная штаб-квартира

6 Omni Way
Chelmsford, Massachusetts 01824
Бесплатный телефон в США: +1 866 212 7267
Тел.: +1 978 703 6600
Факс: +1 978 250 1905

Европа

Тел.: +44 208 622 3108

Азиатско-Тихоокеанский регион

Тел.: +65 6299 0695

www.arbornetworks.com

DS/SP/RU/0611

Технические характеристики оборудования Arbor Peakflow SP Collector Platform (CP), Flow Sensor (FS), Business Intelligence (BI), Portal Interface (PI)

Электропитание
Резервные блоки питания (2)
Переменный ток: 100 ... 240 В (50-60 Гц),
Постоянный ток: -38 ... -75 В

Габаритные размеры
шасси: высота 2U
масса: 17,7 кг
высота: 8,76 см
ширина: 43,53 см
глубина: 51 см
Установка в стандартные стойки 19” и 23”

Жёсткие диски
4 жёстких диска по схеме RAID 5

Сетевые адаптеры
2 x 10/100/1000BaseT (возможен оптический вариант)

Параметры окружающей среды
Условия эксплуатации: 0° ... 40°C
Относительная влажность (при хранении): 95% (без образования конденсата при температуре +23° ... +40°C)

Операционная система
ArbOS*/ArbUX, фирменные встроенные операционные системы на базе открытого кода, таких как Linux и Open BSD.

Производительность
Конфигурация для NetFlow (OC-48) и пакетов (GigE)

Совместимость
Типы потоков: поддержка Cisco NetFlow v5, v7, v9; Juniper cflowd
Мониторинг: интегрирован с консолью управления
Поддержка SNMPv3
Веб-интерфейс: IE 5-7.0 и Mozilla 1.2+ с использованием SSL

Соответствие стандартам
ETSI, NEBS and RoHS

Спецификация Arbor Peakflow SP TMS

Электропитание
Резервные блоки питания (2)

3050/3100/3110/4000
Переменный ток: 100/240 В, 50-60 Гц, 460 Вт номинал
Постоянный ток: -48 ... -68 В; 460 Вт номинал

2500
Переменный ток: 100/240 В, 8,5 А (50-60 Гц)
Постоянный ток: -48 ... -60 В, 20,5 А макс.

1200
Переменный ток: 100/240 В, 8,5 А (50-60 Гц)
Постоянный ток: -48 ... -60 В, 12 А макс

Габаритные размеры
Установка в стандартные стойки 19” и 23”

4000
шасси: 6U
масса: 38,7 кг
высота: 26,7 см
ширина: 44,8 см
глубина: 41,4 см

3050/3100/3110
шасси: высота 3U
масса: 15,2 кг
высота: 13,34 см
ширина: 44,8 см
глубина: 41,33 см

2500
шасси: высота 2U
масса: 17,7 кг
высота: 8,76 см
ширина: 43,46 см
глубина: 51 см

1200
шасси: высота 1U
масса: 11,52 кг
высота: 4,32 см
ширина: 43 см
глубина: 51 см

Жёсткие диски
2 жёстких диска по схеме RAID 1

Сетевые адаптеры

4000
8 x 10 GigE (SFP+)

3100
2 x 10 GigE (SFP+)

3050/3110
2 x 10 GigE (SFP+)
10 x 1 GigE (SFP)

2500
6 x 10/100/1000 (варианты: оптика GigE SX и LX)

1200
4 x 10/100/1000 (варианты: оптика GigE SX и LX)

Параметры окружающей среды
3050/3100/3110/4000
Условия эксплуатации: 0° ... 55°C
Относительная влажность (рабочая): 5 ... 80% (без образования конденсата)

2500
Условия эксплуатации: 0° ... 40°C
Относительная влажность (рабочая): 10 ... 90% (без образования конденсата)

1200
Условия эксплуатации: 10° ... 35°C
Относительная влажность (рабочая): 12 ... 90% (без образования конденсата)

Операционная система
1200/2500/3050/3100/3110/4000
ArbOS*/ArbUX, фирменные встроенные операционные системы на базе открытого кода такие как Linux и Open BSD