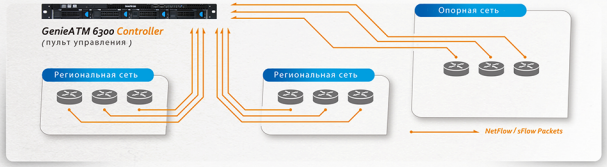
Развертывание системы GenieATM

Распределенная архитектура с централизованным управлением

- Решение «все в одном»: сбор данных для анализа, определение сетевых аномалий, простота настройки
- гибкая архитектуры позволяет постепенного наращивать систему по мере роста сети, и соответствует принципу Pay-As-You-Grow(«Плати по мере роста»)



О Genie Networks

Основана в июне 2000, Genie Networks Ltd. (Genie Networks) развилась в лидирующую технологическую компанию, предоставляющую анализ/визуализацию сетевого трафика и решения сетевой безопасности для оптимизации производительности и снижения операционных затрат крупномасштабных сетей.

GenieATM включает в себя комплексный набор инструментов поведенческого анализа (NBA), такие как детекция аномалий для определения вредноносного трафика и защиты от таких угроз как DDoS атаки, программных червей в масштабах сети.

Среди наших клиентов международные Tier-1 операторы связи, такие как NTT, KDDI, Softbank, China Telecom, China Mobile, SingTel, а также государственные учреждения, университеты и крупные корпорации. На сегодняшний день более 1200 устройств GenieATM развернуты и служат около 600 клиентам по всему миру.

Вэбсайт:	www.genie-networks.com
Тел:	+886-2-26571088
Эл. Почта:	sales@genie-networks.com
YouTube:	www.youtube.com / user / GenieATM
Тайбэй:	5F, No.15, Lane 360, Section 1, Neihu Road, Taipei, Taiwan (Headquarter)
Токио:	K.S Bldg. 6F, 6-2-9 Minami-Aoyama, Minato-ku, Tokyo, Japan
Пекин:	Rm 416, Block B, 8A, Guanghua Road, Chaoyang District, Beijing, China
Шанхай:	5F Crystal Century Tower, No.567 Weihai Road, Shanghai, China

GenieNetworks
Visualize Your Network

GenieATM

Визуализация сетевого трафика, обнаружение и предотвращение DDoS атак

GenieATM (Advanced Traffic Mining) - это комплексное решение операторского класса для анализа сети и выявления сетевых аномалий. Genie ATM использует инновационные технологии сбора данных и обнаружения сетевых угроз, что позволяет решать задачи: анализа ip-трафика, мониторинга сети, сбора статистики, построения отчетов, проактивного обнаружения и предотвращения проблем сетевой безопасности. Genie ATM предоставляет поддержку устройств подавления сетевых угроз от сторонних производителей.

GenieATM это комплексное решение операторского класса для обнаружения и устранения последствий атаки.

- Обеспечение непрерывной работы сервисов сети и мониторинг в режиме реального времени.
- Оповещение оператора сети об обнаружении сетевой аномалии в режиме реального времени и инициация механизма подавления DDoS атак и вредоносного интернет трафика.
- Встроенные отчеты предоставляют быстрый доступ к наиболее важной информации.
- Подробный аналитический отчет помогает определить источник аномального трафика.
- Экономически эффективное решение доказавшее свою эффективность на реальных проектах за счет эффективного управления и эксплуатации.

Visualize Your Network

Достоинства

Высокие показатели производительности: одно устройство GenieATM поддерживает до 100 маршрутизаторов, обработка до 110 тыс. Flow/сек.

Гибкая настройка формирования отчетов: отчеты создаются на основе множества разнообразных фильтров и критериев.

Инструменты расследования инцидентов: мощные инструменты диагностики для анализа изменений параметров трафика как в историческом плане, так и в реальном времени.

Экономическая эффективность: планирования развития сети, анализ параметров пиринговых взаимоотношений и другие возможности, весь функционал доступен в одном продукте

MSSP: Возможность предоставления всего функционала комплекса, как услуги для Ваших клиентов

Решения GenieATM

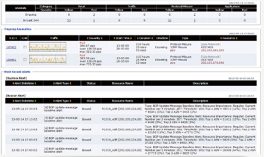
Genie ATM предлагает полное решение для анализа сетевого трафика, обнаружения и подавления угроз, с высокой производительностью и встроенной аналитикой

Анализ сетевых данных

GenieATM снабжен мощным механизмом для исследования трафика, выполняющим классификацию, статистический анализ и сортировку полученных данных для формирования детальных отчетов. Встроенные алгоритмы сетевого моделирования позволяют создавать автоматические отчеты по различным сетевым Flow которые могут быть выбраны(внутренняя сеть/Интернет, пир, магистраль, маршрутизатор, интерфейс, подсеть и сервер), соответствующие отчеты будут сгенерированы автоматически.

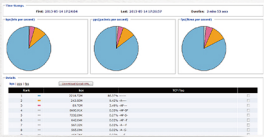
Обнаружение сетевых аномалий

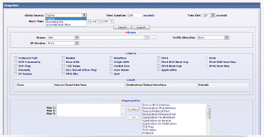
С помощью анализа IP заголовков сетевых потоков, GenieATM следит за появлением аномального трафика. Поддерживается обнаружение таких аномалий, как: Traffic Anomaly, Worm, DDoS Attack, Interface Anomaly, BGP Route Instability.



Инструменты расследования инцидентов

Моментальный снимок происходящего в режиме реального времени возможен с помощью инструмента Traffic SnapShot, который использует различные критерии для формирования Top-N отчетов.





Решение для крупных операторов связи

Надежность: для увеличения доступности и обеспечения отказоустойчивости системы применяются технологии: VRRP и FLB(Flow Load Balancer). Производительность: GenieATM спроектирована с учетом возможности линейного расширения системы без ограничения размера сети. Совместимость: прием и обработка Flow данных (NetFlow(v1,v5,v7,v9), sFlow (v2, v4, v5), NetStreamTM(v5,v9), IPFIX, cFlowd), одновременно с множества сетевых устройств и с поддержкой протокола IPv6.

Защита от DDoS

Как только обнаружена аномальная активность GenieATM отправит сообщение, чтобы оповестить оператора о возникновении угрозы. Перечень доступных средств по подавлению возникших атак включают: EACL, blackholing, BGP FlowSpec и т.д.. GenieATM также поддерживает интеграцию с устройствами очистки трафика сторонних производителей, перенаправляя вредоносный трафик и защищая производительность ядра сети.

Аналитика MPLS сетей

GenieATM MPLS формирует отчеты и визуализирует соответствующий профиль трафика между P/PE маршрутизаторами, VPN сетями и VPN сайтами. Решение повышает безопасность всей сетевой инфраструктуры, позволяя осуществлять определение разнообразных сетевых аномалии, DDoS атак и аномалий BGP для каждой VPN сети. С помощью инструмента Traffic SnapShot, оператор может получить снимок MPLS трафика всей сети, отдельной VPN или маршрутизатора. GenieATM MPLS, это лучшее решение оператора связи для визуализации MPLS VPN сетей.

Применение GenieATM

Анализ трафика

- Мониторинг ключевых узлов сети: исследование состояния и тенденции распределения трафика в сети оператора, региональных сетей, глобальных сетей, сервисов, границы сети провайдера и клиента.
- Возможность выбора модели анализа трафика в соответствии с сетевыми областями которые необходимо проанализировать позволяет точно классифицировать и проанализировать(без дублирования данных) различные профили трафика.
- Расширяемая архитектура системы позволят устанавливать дополнительные коллекторы по мере необходимости.

Анализ peering/routing

- Управление меж-операторским трафиком: имея детализированные отчеты прохождения трафика оператор может решать задачи оптимизации пиринговых отношений с точки зрения стоимости и надежности.
- Аналитическая оценка пиринга: GenieATM содержит инструментарий для проведения различных аналитических оценок существующих и потенциальных пиринг-партнеров.
- Мониторинг сети позволяет оценить надежность транзита трафика.

Безопасность инфраструктуры

- Уменьшение расходов на транзитный трафик и защита инфраструктуры оператора.
- Защита пропускной способности сети для клиентов и подсетей.
- Защита от DDoS атак.
- Не создается дополнительная точка сбоя сети, данные сетевого трафика собираются через xFlow.

Инструменты расследования инцидентов информационной безопасности

- Снижение финансовых потерь за счет сокращения перерывов в обслуживании клиентов.
- Исследование периода активности атаки в выбранном интервале времени.

Диагностика

- Поддержка функции быстрого просмотра параметров трафика в определенный момент времени с возможностью глубокого анализа позволяет быстро найти источник проблемы.
- Уменьшение обращений в тех-поддержку и сокращение времени на решение проблем.

Планирование развития сети

- Определение уязвимых участков и наиболее нагруженных узлов сети.
- Определение требований к пропускной способности каналов связи на границе сети.
- Оптимизация трафика: мониторинг маршрутов, настройка политик и т.д.

Выявление потребностей бизнеса

- Мониторинг сетевого трафика: анализ атрибутов трафика, направление трафика в/из ЦОД, анализ клиентского трафика, анализ использования сервисов и т.д.
- Определение профилей трафика клиента для анализа возможностей предоставления дополнительных услуг.
- Оптимизация производительности сети.

Система анализа трафика, как услуга

- Управление услугами через пользовательский портал для клиента.
- Аналитика трафика и защита от сетевых атак может быть использована для предоставления дополнительных
- услуг клиентам и генерирования дополнительной прибыли оператора