DPI в Enterprise

Контроль сетевого трафика на предприятиях

Алексей Бизня

Особенности Enterprise

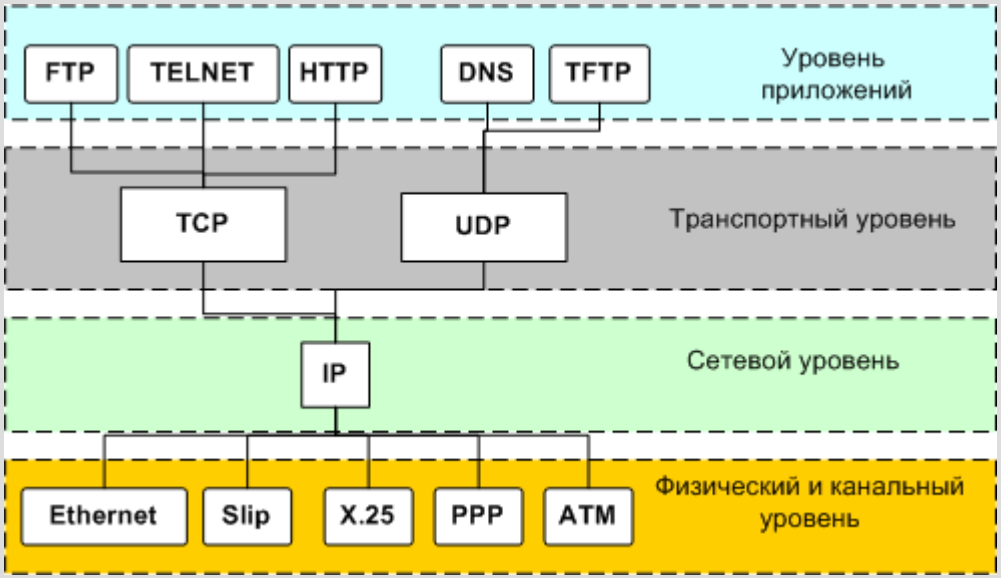
- Возможность административного воздействия на пользователей
- Применение любых конфигураций и технологий в служебных целях как на конечных узлах пользователей, так и на сетевом оборудовании.

Применение DPI

- Защита периметра (фильтрация, журналирование, обнаружение и расследование инцидентов)
- Оптимизация трафика (приоритезация, кеширование, статистика, балансировка)
- Диагностика проблем (сетевые анализаторы, системы мониторинга и корреляции событий)
- Соответствие требованиям внутренней политики безопасности и требованиям регуляторов (фильтрация)

Эволюция средств защиты
Пакет -> Приложение -> Контент

- Packet Filtering
- Statefull Packet Inspection
- Deep Packet Inspection



- Deep Content Inspection (реконструкция, декомпрессия, исполнение в песочнице)

Средства с DPI

- Firewall (Router)
- Sniffer
- IDS/IPS
- Proxy
- Antivirus
- Antispam
- DLP
- UTM firewall (Unified Threat Management)
- Next Generation Firewall (NGFW, L2-L8, application)

Технологии перехвата и обработки трафика

- Зеркалирование трафика (пассивный анализ) с промежуточного сетевого устройства на устройство для обработки
  - (R)SPAN, Promiscuous mode
- Обработка трафика на промежуточном сетевом устройстве в режиме маршрутизации или в разрыв между маршрутизаторами
  - Inline or Routed mode, IDS, UTM firewall
- Маршрутизация необходимого трафика через устройство обработки (BGP\OSPF, central services VPN/MPLS)

Технологии перехвата и обработки трафика

- Прозрачный для клиентов перехват соединений с промежуточного сетевого устройства и направление через встроенного/удаленного посредника (вмешательство на транспортном,сеансовом и прикладном уровнях)
  - WCCP, SSL Bump, HTTP/FTP proxy
- Дополнительная фильтрация и модификация контента посредниками
  - ICAP/eCAP, DLP, HTTP/FTP proxy

Технологии перехвата и обработки трафика

- Настройка клиентского ПО на явное использование посредников
- Перехват и обработка данных на конечных узлах (клиентах) при работе с сетью (агенты, WAF)
-

Технологии перехвата и обработки трафика

- Сигнатурный анализ
- Статистический анализ
- Словари, черные списки, репутационные базы
- Поведенческий анализ и корреляция
- Анализ в облаке
-
- Буферизация контента на время обработки (задержки)
- Баланс между производительностью и защитой

Источники

- http://www.tnarg.org/pdf/DPI_article_final.pdf
- http://en.wikipedia.org/wiki/Deep_packet_inspection
- http://en.wikipedia.org/wiki/Deep_content_inspection

Спасибо!