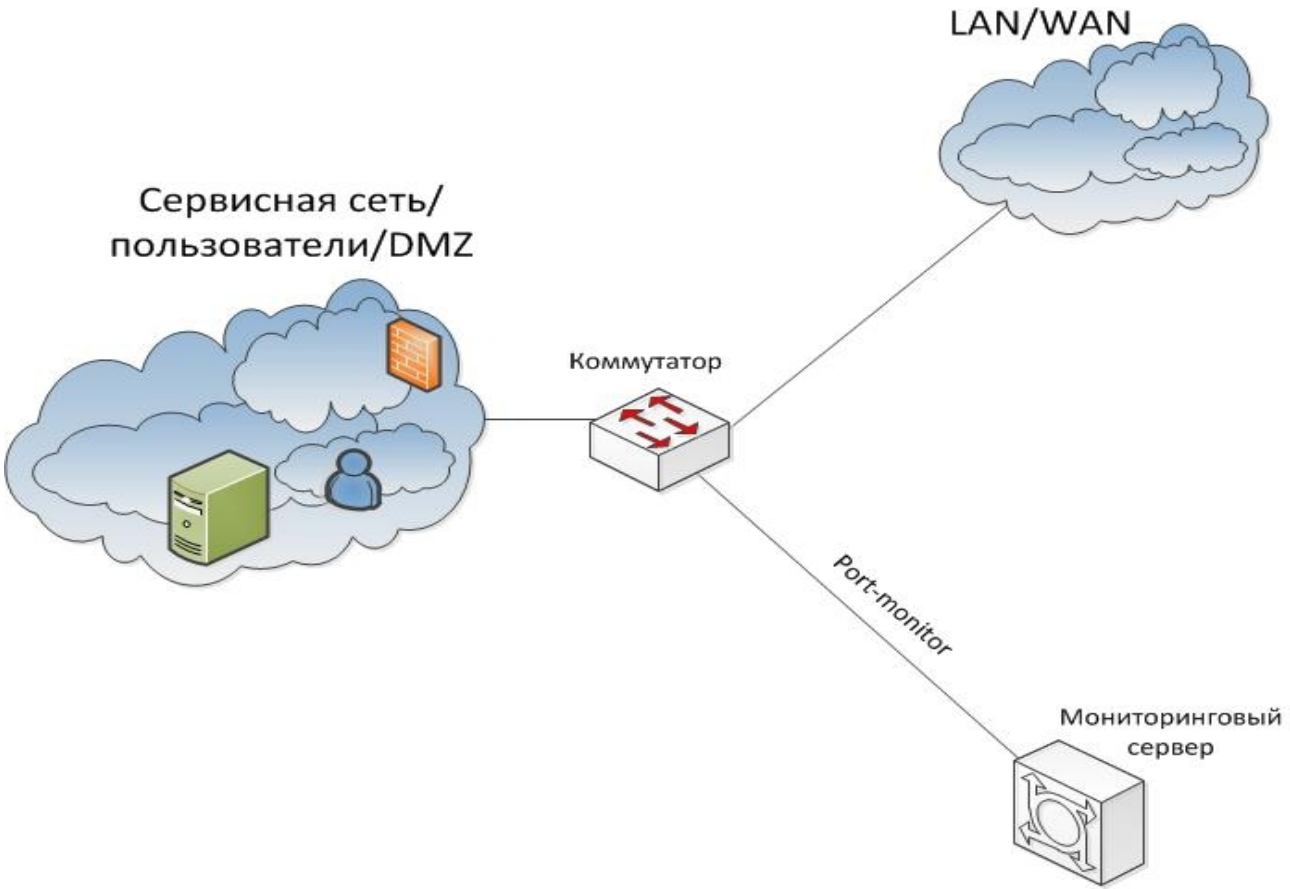
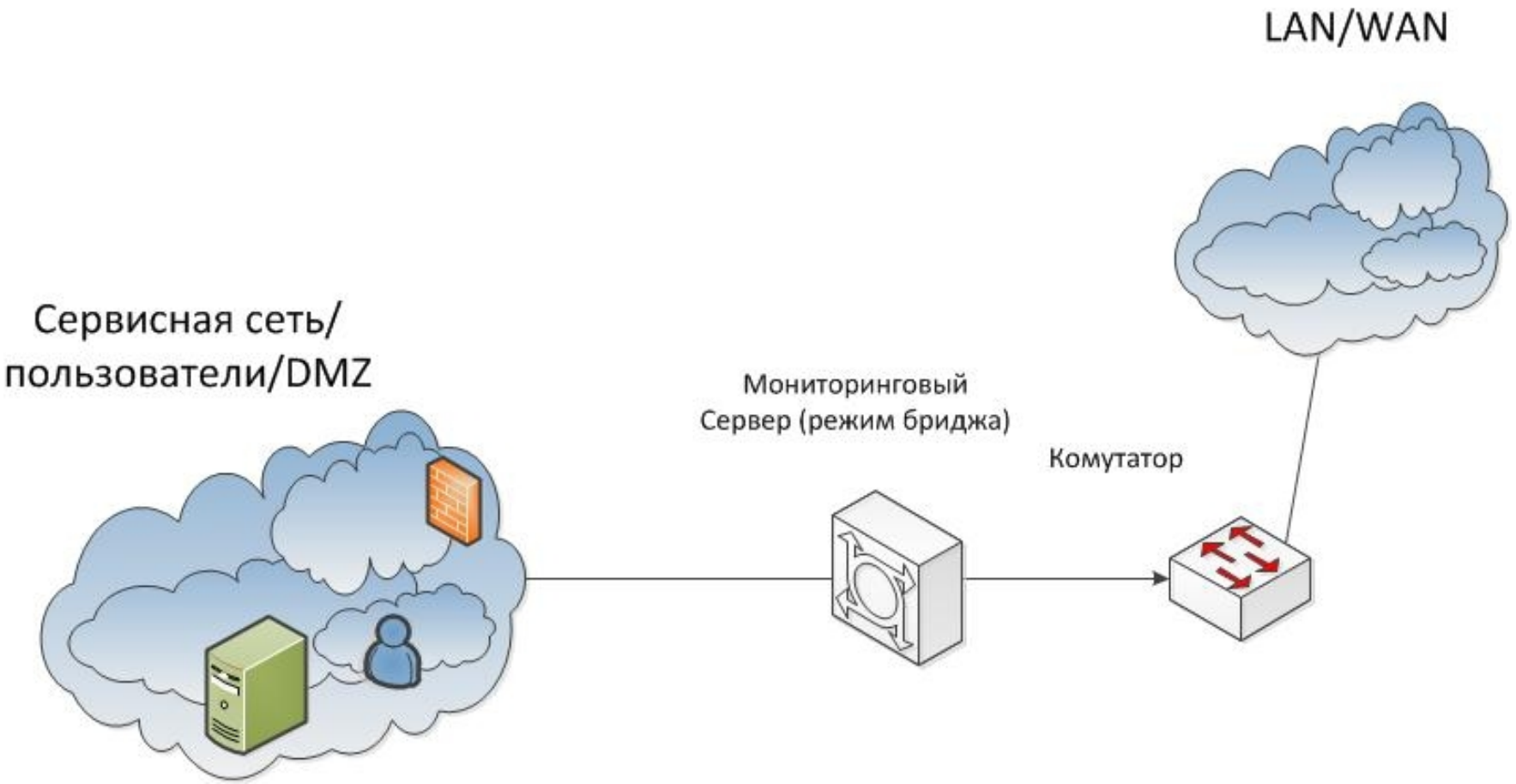
Область применения

- Анализ качества работы сетевых сервисов
- IPS/IDS(snort, suricata)
- Business Intelligence (ntop)
- Network troubleshooting(wireshark, tcpdump)
- Lawful Interception

Типовая схема



Типовая схема(2)



PF_RING

- PF_RING — модуль в ядро
- Поставляется с libpcap wrapper-ом (совместимость со всеми существующими приложениями)
- Поддержка аппаратной фильтрации трафика
- Модульная архитектура(плагины)
- Работает на различных платформах(x86, MIPS и т.д.)

PF_RING как работает

- Создается сокет PF_RING
- Ядро выделяет память под циклический буфер, и освобождает память, когда приложение закрывает сокет
- При получении ethernet кадра через DMA, кадр копируется в циклический буфер. Если буфер заполнен кадр сбрасывается.
- Циклический буфер экспортируется в userland через mmap()
- При вызове mmap() приложение получает указатель чтения на позицию в циклическом буфере

PF_RING как работает(2)

- При записи в буфер ядро сдвигает указатель записи
- Указатель чтения сдвигается по мере получения пакетов приложением
- Для управления потоком кадрв используется leacky bucket

PF_RING архитектура

Wire speed Захват 10G - DNA

- DNA(Direct NIC Access)-способ трансляции памяти и регистров сетевого адаптера в userland. Копирование кадра в DMA производится NPU сетевого адаптера а не NAPI, что позволяет значительно снизить загрузку процессора при захвате пакетов.

DNA архитектура

PF_RING

PF_RING+DNA

Другие решения

- Libpcap-mmap-значительно повышает производительность захвата, но не достаточно для wire speed
- Gulp-может писать трафик со скоростью до 1Gbit без потерь. Использует много поточность и mmap. Более не поддерживается.
- Netsniff-ng-использует механизм RX_RING. На современном железе захватывает до 1.2Mpps.
- DiCAP-Алгоритм распределенного захвата трафика. Может захватывать любые обьемы трафика. Существует только на бумаге.

Контакты

Email: andrey.loginov@smartnet.in.ua

Телефон: +380504186701

Спасибо!