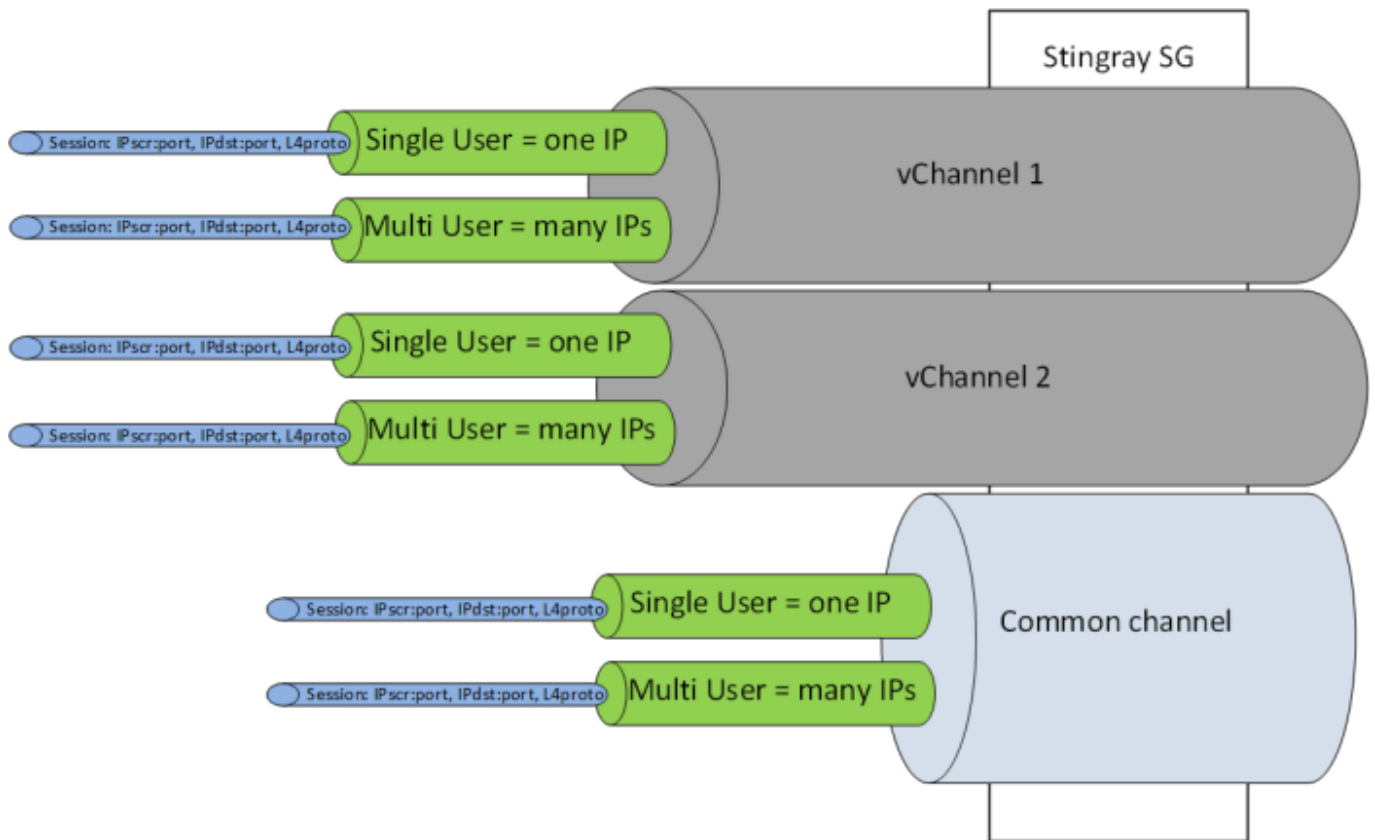


Содержание

- Общее описание полисинга 3
 - Обработка TCP трафика 4
 - Обработка ICMP, UDP трафика 4

Общее описание полисинга



СКАТ применяет полисинг на следующие логические объекты:

1. Общий канал (Common Channel) - Весь Трафик проходящий через DPI устройство, который не выделен в Виртуальный канал (vChannel). [Полисинг Общего канала](#).
2. Виртуальный канал (vChannel) - Трафик, который описывается парой физических портов или VLAN или CIDR. Данный трафик не входит в Общий канал (Common Channel) и имеет собственную настройку [Полисинг Виртуального канала \(vChannel\)](#).
3. Абонент (Subscriber) - Трафик конкретного абонента, который определяется списком IP адресов или CIDR. На трафик Абонента (Subscriber) может быть назначен [Полисинг абонентского канала](#), но так же действует полисинг Общего или Виртуального канала, в котором находится Абонент.
4. Сессия (Session) - Трафик, который определяется набором параметров IPsrc:port, IPdst:port и признаком протокола TCP, UDP, ICMP etc. [Полисинг по сессии и переопределение классов трафика](#)

Полисинг применяется для 8 классов трафика, выставляемых опцией [Разметка приоритета трафика в зависимости от протокола или направления](#)



Попадание протокола в свой класс также регулируется опцией ([класс <-> приоритет](#)). Такой подход позволяет комбинировать совместимым образом использование внешних и внутреннего полисеров.

Доступны два механизма полисинга на выбор:

1. TBF без иерархии ([Token Bucket Function](#)), используется для ограничения/блокировки конкретного класса полисинга. Ограничение полосы с поддержкой burst.
2. НТВ с иерархией для 8 классов ([Hierarchical Token Bucket](#)), используется для приоритизации по классам трафика. Ограничение полосы с заимствованием.

Сценарии применения полисинга Общего и Виртуального каналов:

1. контролировать приближение к верхней границе полосы канала ("полке") и приоритезировать трафик по протоколам и направлениям, так чтобы низкоприоритетный трафик вытеснялся из полосы в пользу высокоприоритетного. Данный механизм позволяет держать полку под контролем и экономить на том, что не требуется покупка избыточной полосы, можно даже понизить верхнюю границу на 10-15% без заметного для абонентов эффекта.
2. ограничить размер занимаемой полосы для группы протоколов. Популярное применение данный механизм находит для ограничения торрентов. Один из возможных use case описан в документе ["Оптимизируем использование uplink канала"](#)

Обработка TCP трафика

Для полисинга и правила drop по умолчанию СКАТ пропускает без обработки 2 первых пакета TCP Handshake (SYN и SYN-ACK) для оптимизации работы и устойчивости перед SYN Flood. В случае подключения любой услуги из списка ниже СКАТ обрабатывает TCP соединения с первого пакета.

- 10 - DDOS защита
- 11 - CGNAT и NAT 1:1
- 15 - спецабонент (весь трафик помещается в cs0, не применяется фильтрация (4 услуга) для vChannel и общего канал)

Это связано с тем, что данные услуги требуют обработки всего трафика с первого пакета.

Обработка ICMP, UDP трафика

Полисинг и drop для ICMP регулируется отдельным протоколом. Полисинг и drop для UDP применяется в зависимости от протокола L7 в котором UDP используется как транспорт (пример QUIC).