Содержание

Защита от UDP flood 3

Защита от UDP flood

Данный тип атаки осуществляется фрагментированными udp пакетами, на сборку и анализ которых атакуемая платформа вынуждена тратить много ресурсов.

Защита осуществляется путем отбрасывания неактуального для защищаемого сайта набора протоколов. Конфигурирование фильтра протоколов приведено в описании опции Назначение приоритетов

Для типового защищаемого WEB-сайта актуальные протоколы это HTTP и HTTPS, поэтому конфигурация для этого случая выглядит так:

```
http        cs0
https       cs0
default     drop
```

Подготовленный файл конфигурации конвертируем во внутренний формат и загружаем в DPI

```
cat my_dscp.txt|lst2dscp protocols.dscp
mv protocols.dscp  /etc/dpi/protocols.dscp
service fastdpi reload
```

Аналогичным образом возможна защита от DDoS атаки по типу DNS/NTP amplification, при которых входящий канал забивается трафиком, превышающим возможности канала. Действие данной защиты ограничено возможностями оператора по предоставлению дополнительной канальной емкости. При ее превышении потребуется аренда дополнительных каналов или перенаправление трафика на специализированные сервисы, которые защищают от атак подобного типа, арендуя большие канальные емкости, превышающие мощность DDoS атак.