

Содержание

- IP source guard 3
 - Назначение 3
 - Включение режима 3
 - Логика обработки пакетов 3
 - Режим терминции по AS 3
 - Фильтрация по флагам source AS 3

IP source guard

Назначение

FastDPI BRAS контролирует соответствие VLAN-тегов и IP-адреса абонента.

При выдаче IP-адреса через DHCP FastDPI BRAS запоминает VLAN/QinQ-теги абонента во встроенной БД [UDR](#). В дальнейшем эти данные используются для проверки соответствия source IP пакета и его VLAN-тегов.

IP source guard применяется только для исходящего трафика (LAN → WAN).

Включение режима

Для активации необходимо задать параметр `bras_ip_source_guard` в файле `fastdpi.conf`:

- 0 — режим отключен (по умолчанию)
- 1 — режим включен и применяется только для активных сессий

Если после перезапуска fastDPI состояние сессии неизвестно, IP source guard не применяется и пакет пропускается.

Логика обработки пакетов

При `bras_ip_source_guard=1` пакет пропускается, если:

- сессия активна и VLAN-теги пакета совпадают с тегами, зарегистрированными при DHCP
- статус сессии неизвестен

Во всех остальных случаях пакет дропается.

Режим терминации по AS

Доступен режим [терминации по AS](#).

В этом режиме IP source guard применяется только к source IP, у которых AS помечена флагом `term`.

Фильтрация по флагам source AS

Поддерживается дополнительная фильтрация subs-трафика по флагам AS на направлении

subs → inet до этапа обработки пакета. Механизм предназначен для блокирования исходящего от оператора DDoS-трафика с подменой IP-адреса.

В fastdpi.conf используется параметр `ip_filter_source_as_flags` (hot).

В обработку допускаются только пакеты, у которых AS source IP содержит хотя бы один из указанных флагов. В противном случае пакет дропается.

Значения флагов (битовая маска):

- 0 — фильтрация отключена (по умолчанию), `ip_filter_source_as_flags=0x0`
- 0x0100 — pass
- 0x0200 — local
- 0x0400 — peer
- 0x0800 — term
- 0x1000 — mark1
- 0x2000 — mark2
- 0x4000 — mark3