# Table of Contents

# IP source guard

## Purpose

FastDPI BNG verifies the consistency between subscriber VLAN tags and the subscriber IP address.

When assigning an IP address via DHCP, FastDPI BNG stores the subscriber VLAN/QinQ tags in the built-in UDR database. These data are later used to validate the correspondence between the packet source IP and its VLAN tags.

IP source guard is applied only to outbound traffic (LAN → WAN).

## Enabling the mode

To activate, set the parameter `bras_ip_source_guard` in the fastdpi.conf file:

- 0 — mode disabled (default)
- 1 — mode enabled and applied only to active sessions

If after restarting fastDPI the session state is unknown, IP source guard is not applied and the packet is allowed.

## Packet processing logic

With `bras_ip_source_guard=1`, a packet is allowed if:

- the session is active and the packet VLAN tags match the tags registered during DHCP
- the session status is unknown

In all other cases, the packet is dropped.

## AS-based termination mode

The AS-based termination mode is available.

In this mode, IP source guard is applied only to source IP addresses whose AS is marked with the `term` flag.

## Filtering by source AS flags

Additional filtering of subscriber traffic by AS flags is supported in the subs → inet direction before

packet processing. The mechanism is intended to block outbound DDoS traffic with spoofed IP addresses originating from the operator network.

The parameter `ip_filter_source_as_flags` (hot) is used in fastdpi.conf.

Only packets whose source IP AS contains at least one of the specified flags are allowed for processing. Otherwise, the packet is dropped.

Flag values (bitmask):

- `0` — filtering disabled (default), `ip_filter_source_as_flags=0x0`
- `0x0100` — pass
- `0x0200` — local
- `0x0400` — peer
- `0x0800` — term
- `0x1000` — mark1
- `0x2000` — mark2
- `0x4000` — mark3