APN ACL Support

This chapter covers the following topics:

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product (s) or Functional Area	5G-UPF
Applicable Platforms	VPC-SI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
First Introduced	2020.02.0

Feature Description

IP Access Lists commonly known as Access Control Lists (ACLs) control the flow of packets into and out of the system. The configuration is per-context basis and consists of rules (ACL rules) or filters that control the action applicable for packets that match the filter criteria. Configuration must be done on the user plane's APN configuration.

ACL in the UPF supports the following configuration:

```
{ deny | permit } [ log ] source_ip_address source_ip_wildcard
no { deny | permit } [ log ] source_ip_address source_ip_wildcard
```

ACL in UPF do not support the following configuration:

- In **ip access-list** *access_list_name*
  - **after** - Apply filter after packet is received or transmitted.
  - **before** - Apply filter before packet is received or transmitted.
  - **readdress** - Packet filtering rule to change destination address/port of a packet to a specific server.
  - **redirect** - Packet filtering rule to redirect a packet to a specific next hop.
- Context-level ACL is not supported.
- Interface-level ACL is not supported.

NOTE: For information on ACL-related CLI commands, refer to the *StarOS CLI Reference*.

IP Source Violation

Source validation requires the source address of incoming packets to match the IP address of the subscriber during the session. This allows operators to configure the network to prevent problems when a user gets handed back and forth between two gateways several times during a handoff scenario.

When the UPF receives a subscriber packet with a source IP address violation, the system increments the IP source violation drop-limit counter and starts the timer for the IP source violation period. Every subsequent packet received with a bad source address during the IP source violation period causes the drop-limit counter to increment. For example, if you set the drop limit to 10, after 10 source violations, the call is dropped. The detection period timer continues to count throughout this process.

The following must be configured in the User Planes APN configuration:

```
ip source-violation { ignore | check [ drop-limit limit ] } [
exclude-from-accounting ]
```

NOTE: For information on IP source violation CLI commands, refer to the StarOS *Command Line Interface Reference*.

Gating Control

Gating Control in the UPF enables or disables the forwarding of IP packets belonging to a service data flow or detected application's traffic to pass through to the desired endpoint. See 3GPP TS 23.203, subclause 4.3.2.

The SMF controls the gating in the UPF by creating PDRs for the service data flow(s) or application's traffic to be detected, and by associating a QER, including the Gate Status IE, to the PDRs.

The Gate Status IE indicates whether the service data flow or detected application traffic is allowed to be forwarded (the gate is open) or to be discarded (the gate is closed) in the uplink and/or in downlink directions.

The UPF identifies the UL and DL flows by the Source Interface IE in the PDI of the PDRs or the destination Interface IE in the FARs. The UPF applies UL and DL gating accordingly.

The SMF requests the UPF to discard the packets that are received for the PDR by setting the gate fields in the Gate Status IE of QERs to CLOSED.