

APN ACL Support

This chapter covers the following topics:

- Feature Summary and Revision History, on page 1
- Feature Description, on page 2
- IP Source Violation, on page 5
- Gating Control, on page 5

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

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

Revision History

Table 2: Revision History

Revision Details	Release
Gating control feature is enhanced to display the gating status as enabled/disabled through an additional QER per PDR for dynamic rules.	2024.01.1

Revision Details	Release
A configurable mechanism has been introduced to apply traffic classification and policy enforcement on selective subscriber sessions.	2021.01.0
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. Once configured, an ACL can be applied to an individual subscriber. Separate ACLs can be created for IPv4 and IPv6 access routes.

The following are the two main aspects of ACLs:

- Rule(s)
- Rule Order

Rule(s)

A single ACL consists of one or more ACL rules. Each rule is a filter configured to take a specific action when packets match a specific criteria.

Each rule specifies the action to take when a packet matches the specifies criteria. This section discusses the rule actions and criteria supported by the system.

Actions

ACLs specify that one of the following actions can be taken on a packet that matches the specified criteria:

- **Permit**: The packet is accepted and processed for classification and policy enforcement.
- **Deny**: The packet is rejected.
- **Redirect CSS**: The behaviour is the same as Permit action.

NOTES:

- In UPF, it's recommended to use Permit option instead of Redirect CSS. Functionally, both the options are equivalent in UPF. Support for Redirect CSS option is only for backward compatibility and should be used only in such scenarios.
- Configured ACLs consisting of no rules imply a "deny any" rule. This is the default behavior for an empty ACL.
- In UPF, if ACLs aren't associated with an APN, then call is up. By default, traffic is processed for classification and policy enforcement. For non-UPF architecture, call fails as Redirect CSS is mandatory.
- If only Deny option is given in the ACL for certain traffic, then to pass the rest of the traffic, Permit option must be given explicitly.

- If only permit option is given in the ACL for certain traffic, then to pass the rest of the traffic, permit must be given explicitly for that traffic.
- Router Advertisement/Router Solicitation (RA/RS) packets are candidate for ACL. So, take caution in putting the IPv6 ACL.
- Configuration change in ACL is applied for a new call and not on the existing call.

Criteria

Each ACL consists of one or more rules specifying the criteria that packets will be compared against.

The following criteria are supported:

- **Any**: Filters all packets
- **Host**: Filters packets based on the source host IP address
- **ICMP**: Filters Internet Control Message Protocol (ICMP) packets
- **IP**: Filters Internet Protocol (IP) packets
- **Source IP Address**: Filter packets based on one or more source IP addresses
- **TCP**: Filters Transport Control Protocol (TCP) packets
- **UDP**: Filters User Datagram Protocol (UDP) packets

Each of the above-mentioned criteria is described in detail in the sections that follow.

- **Any**: The rule applies to all packets.
- **Host**: The rule applies to a specific host as determined by its IP address.
- **ICMP**: The rule applies to specific Internet Control Message Protocol (ICMP) packets, Types, or Codes. ICMP type and code definitions can be found at *www.iana.org* (RFC 3232).
- **IP**: The rule applies to specific IP packets or fragments.
- **IP Packet Size Identification Algorithm**: The rule applies to specific IP packets identification for fragmentation during forwarding.

  This configuration is related to the "IP Identification field" assignment algorithm used by the system, when subscriber packets are being encapsulated (such as Mobile IP and other tunneling encapsulation). Within the system, subscriber packet encapsulation is done in a distributed way and a 16-bit IP identification space is divided and distributed to each entity which does the encapsulation, so that unique IP identification value can be assigned for IP headers during encapsulation.

  Since this distributed IP Identification space is small, a nonzero unique identification will be assigned only for those packets which may potentially be fragmented during forwarding (since the IP identification field is only used for reassembly of the fragmented packet). The total size of the IP packet is used to determine the possibility of that packet getting fragmented.
- **Source IP Address**: The rule applies to specific packets originating from a specific source address or a group of source addresses.
- **TCP**: The rule applies to any TCP traffic and could be filtered on any combination of source/destination IP addresses, a specific port number, or a group of port numbers. TCP port numbers definitions can be found at *www.iana.org*.

- **UDP**: The rule applies to any UDP traffic and could be filtered on any combination of source/destination IP addresses, a specific port number, or a group of port numbers. UDP port numbers definitions can be found at *www.iana.org*.

Rule Order

A single ACL can consist of multiple rules. Each packet is compared against each of the ACL rules, in the order in which they were entered, until a match is found. Once a match is identified, all subsequent rules are ignored.

Limitations

Following are the known limitations of APN ACL feature in UPF:

- Readdress option in ACL is not supported.
- Redirect ACL for context and next-hop is not supported.
- Log option is not supported in ACLs.
- APN-level bulkstats for ACL drops (only IPv4) are supported.

Configuring ACL

To apply the ACL to individual subscriber through APN, use the following configuration:

```
configure
   context dest_context_name [ -noconfirm ]
      { ip | ipv6 } access-list acl_list_name
         { permit | deny | redirect }acl
         end
configure
   apn apn_name
      { ip | ipv6 } access-group acl_list_name [ in | out ]
      end
```

Notes:

- The ACL to be applied must be in the destination context of the APN (which can be different from the context where the APN is configured).
- If neither the **in** nor the **out** keyword is specified, the ACL will be applied to all inbound and outbound packets.
- This command supports only one ACL. However, the ACL can have up to 128 rules.
- Four access-groups can be applied for each APN, for example:

  ip access-group acl_list_name_1 in

  ip access-group acl_list_name_2 out

  ipv6 access-group acl_list_name_3 in

  ipv6 access-group acl_list_name_4 out

Verifying ACL Configuration

Use the following CLI commands in Exec mode to check if your ACL lists were applied properly, and also for packet drops due to ACL:

- **show subscriber user-plane-only full all**
- **show subscribers user-plane-only full callid** *call_id*
- **show user-plane-service pdn-instance statistics** *name*

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 that is 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

Table 3: Feature History

Feature Name	Release Information	Description
Gating Control Using Additional QER	2024.01.1	The number of QERs per PDR supported in UPF is increased from two to three in this release. All rules and filters are sent to UPF through PDRs. SMF sends an additional QER for dynamic rules installed on default QFI/bearer. The Gate Status IE indicates whether the gate is open or closed. **Default Setting:** Not Applicable

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 status in the UPF by creating QERs associated with the PDRs for service data flow(s) or application's traffic to be detected. The QER associated with 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 default PDRs two QERs get associated to the dynamic rule's PDRs on default QFI/bearer. Therefore, SMF creates an additional QER to display the GATE status for the dynamic rule on default QFI/bearer. The additional QER gets associated with the PDR in the dynamic rule. Hence, the UPF supports up to three QERs per PDR association.

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.