IP Services Gateway Engineering Rules

This appendix lists IPSG-specific engineering rules that must be considered prior to configuring the system for your network deployment. General and network-specific rules are available in the appendix of the *System Administration Guide* for the specific network type.

The following rules are covered in this appendix:

IPSG Context and Service Rules

- Only one IPSG service can be configured within a context.
- Single context configurations must have the ingress port identified using the **ingress-mode** command in the Ethernet Port Configuration Mode.
- In single context configurations, if data packets are received before a session is initiated, the packets could be routed to their destination without being processed. Use separate ingress and egress contexts to prevent this issue.
- Regardless of number of contexts in the configuration, **ingress-mode** CLI command must be configured for ASR5500 and VPC-SI or VPC-DI platforms. This is done to give precedence to the two matching flows. For example, cases when IPv4SA or IPv4DA both are matched for the ingress packet, then if the incoming interface is designated as ingress, the lookup will be performed in the order of IPv4SA first and then IPv4DA. But if the ingress mode is not set, priority is given to the IPv4DA flow. This is true only for ASR5500 and later platforms such as VPC-SI and VPC-DI.

IPSG RADIUS Messaging Rules

- The sending of RADIUS accounting start messages to the RADIUS server is delayed by the IPSG until a session is successfully started.