# Documentation Bulletin

| | | | |
|---|---|---|---|
| **Severity Level** | Enhancement | **Bulletin Number** | F11446-01 |
| **Issue Date** | 10/16/2018 | **Expires** | N/A |
| **Title** | Reverse Routing Check Behavior | | |
| **Product** | Oracle Communication Policy Management | **Release** | 12.3 |
| **Priority** | FYI | **Related Bugs** | 28788453 |
| **Impacts Compatibility** | NO | **Impacted Product Line(s):** | Oracle Communication Policy Management |
| **Markets** | ALL | **Part No. Affected** | E85334-01; E85333-01 |

## Author and Formal Approvers

| | | | |
|---|---|---|---|
| **Author** | S. Simala 10/16/2018 | **Customer Documentation** | B. Chappell 10/16/2018 |

## Problem Description

Security enhancement to reverse routing check behavior

## Impact

Release 12.3.0 of Oracle Communications Policy Management increased the security of the reverse routing check behavior.

## Cause

N/A

## Needed Actions

**N/A**

## Configuration

Release 12.3.0 of Oracle Communications Policy Management increased the security of the reverse routing check behavior. This increase added security control in the kernel level to avoid an external IP attack. Now, the kernel checks the source IP from any arriving packets received with a predefined routing table to find the specific route for the related IP. If a specific route is not found for the source IP, the default route is used, and only one default route exists in routing table for each server. If the outgoing interface of the route does not match the incoming interface of the packet, the kernel rejects the packet. The kernel check is performed on every interface, including OAM, SIGA, SIGB, and SIGC. For example, if the kernel identifies a packet arriving at the OAM with an outgoing interface of SIGA/SIGB and routing does not exist between the OAM and

SIGA/SIGB; the packet is rejected. The same case applies to a packet incoming from SIGB and outgoing by SIGA.

Applications such as SMS and SNMP can be blocked by this security change after the upgrade. Packets for these applications do not usually come through SIG interfaces and specific routings were not configured for related applications servers' IP addresses in previous routing tables. To unblock usage for applications, customers must perform specific configuration in the routing settings. You must collect corresponding IPs and configure the related routings for remote application servers or gateway servers.

For example, if the SMS packets are sent via the OAM interface, then you must add:

- A route with OAM as the interface
- SMS server IP as the destination
- SMS gateway IP as gateway address.

For routing of subnet type it is the same configuration model. However, you do not need to add special routes for applications that adopt the SIGA interface as a default transmission.

SCTP multiple homing can also be blocked. Ensure that the remote SCTP endpoint never sends packets back to a different interface of PCRF against the one that it previously receives SCTP packets from. The cross link communication is not supported since PCRF version 12.3.0.

Therefore, if any packets do not have consistent IPs between the incoming and outgoing paths, rejection occurs. If you want to have paths that are not consistent, you must specify the routings in your configuration unless the related traffic is going through the default path.