

# SAPC Network Description

Ericsson Service-Aware Policy Controller

USER GUIDE

## **Copyright**

© Ericsson España, S.A. 2017, 2018. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

## **Disclaimer**

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

## **Trademark List**

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Target Audience	1
<b>2</b>	<b>SAPC Overview</b>	<b>3</b>
<b>3</b>	<b>Network Overview</b>	<b>5</b>
3.1	SAPC Connected to the Gateway Routers of the External Network (Recommended)	5
3.2	SAPC Deployment Including VIP Gateway Routers to Interconnect the SAPC with the Gateway Routers of the External Network (To Be Deprecated)	6
<b>4</b>	<b>Network Description</b>	<b>9</b>
4.1	Internal Networks	9
4.2	VIP Networks	9
4.2.1	VIP Gateway Routers	10
4.3	External Networks	11
4.3.1	Routing Protocols for External Networks	12
4.4	SysMGMT Network	13
<b>5</b>	<b>Traffic Network Separation</b>	<b>15</b>
<b>6</b>	<b>VIP Address Allocation</b>	<b>19</b>
6.1	OAM VIP	19
6.2	Provisioning VIP	19
6.3	Traffic VIPs	19
6.4	Replication VIP	20
6.5	External Database VIP	20
6.6	Event-Based Monitoring VIP	20
<b>7</b>	<b>Traffic Flows</b>	<b>21</b>
7.1	Incoming Traffic	21
7.2	Outgoing Traffic	23
<b>8</b>	<b>Security</b>	<b>27</b>





# 1 Introduction

The purpose of this document is to describe the general network infrastructure of a SAPC node, from the internal components of a SAPC to the integration with the customer network environment. This document covers network details that are independent of the SAPC deployment.

The following subjects are within the scope of this document:

- Network infrastructure overview
- Internal and external networks overview
- Connectivity overview

The following subjects are out of the scope of this document:

- Deployment-specific network configuration details
- Details of the customer network outside the SAPC node

## 1.1 Target Audience

The main users of this document are the following:

- System architects, system administrators, and any other Ericsson personnel with an interest in the SAPC network architecture

It is assumed that the target audience has knowledge about networking, basic SAPC product architecture, both at system and node level. For more information regarding SAPC, refer to *Service-Aware Policy Controller*.





## 2 SAPC Overview

The SAPC application can be deployed, as a VNF, on top of a Network Functions Virtualization Infrastructure (NFVI) and, as a PNF deployment, on any HW fulfilling the minimum requirements. Both are described in [Service-Aware Policy Controller](#).

The concepts behind the networks and their characteristics for both type of deployments are the same, although the particular configuration needed is slightly different. Details on the configuration can be found in the [SAPC VNF Network Configuration Guide for VNF](#) and in the [BSP 8100 Network Configuration Guide](#) and [NSP 6.1 Network Configuration Guide for PNF](#).







## 3 Network Overview

This section gives an overview of the different networks configured for a SAPC, both for internal communications and for integrating the SAPC with customer external traffic and OAM networks. This overview considers two possible scenarios for configuration.

### 3.1 SAPC Connected to the Gateway Routers of the External Network (Recommended)

In this configuration, System Controllers (SC) are directly connected to the OAM Gateway Routers and Payloads (PL) are connected to the Traffic Gateway Routers, as it is shown in Figure 1.

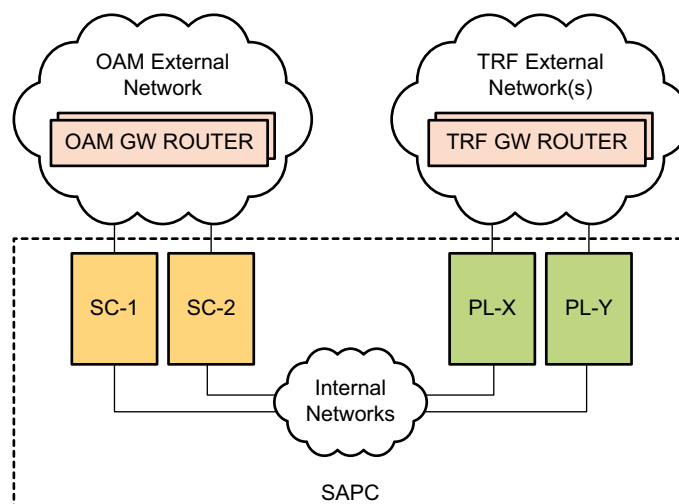


Figure 1 SAPC Connected to the Gateway Routers of the External Network

The SAPC networks needed for this configuration are classified into the following categories, depending on their use and the region they belong to:

- **Internal:** Internal networks inside the node are used to internally address the blades or Virtual Machines in each SAPC node. Therefore, addresses within these networks are not routable outside the SAPC.
- **External:** External networks are used to transport incoming and outgoing traffic between the SAPC SCs and PLs and the Gateway Routers, the latter serving as VIP Gateway Routers, so, these networks can also be referred to as VIP networks. Through these networks, the Virtual IP (VIP) addresses that neighbors can use to communicate with the SAPC node are accessible. These neighbors include, among others, PCEFs, External Databases, or Provisioning

Systems. The addresses of the External networks must not overlap with other networks within the site.

- **SysMGMT:** The SysMGMT network is defined for host administration purposes. Only in use for PNF deployments.

For VNF, this is the most efficient configuration, in relation with resources consumption, as only the Virtual Machines (VM) of the SAPC cluster are needed. This is also a robust solution since up to six PLs have connectivity to the External Traffic networks and if any of them falling, their IP address is still available from another PL. As drawback, routes must be added in the configuration in the Traffic Gateway Routers for the IP addresses of the six PLs with external connectivity.

## 3.2 SAPC Deployment Including VIP Gateway Routers to Interconnect the SAPC with the Gateway Routers of the External Network (To Be Deprecated)

VIP Gateway Routers are intermediate elements to interconnect the SAPC cluster with the Customer Gateway Routers. For VNF deployments, these routers are additional Virtual Machines deployed together with the SAPC. For PNF deployments, BSP CMXB serves as VIP Gateway Routers.

The SAPC networks needed for this configuration are the same as described in the previous section, although in this deployment, External and VIP networks are considered as two different networks:

- **VIP:** The VIP networks for OAM and Traffic are used to provide access to the VIP addresses of the SAPC node from the External networks. When the SAPC deployment does not include VIP Gateway Routers, the VIP networks and the External networks are the same.
- **External:** External networks are used to transport incoming and outgoing traffic between the VIP Gateway Routers and Customer Gateway Routers. Through these networks, the neighbors can communicate with the SAPC node through the Virtual IP (VIP) addresses. These neighbors include, among others, PCEFs, External Databases, or Provisioning Systems. The addresses of the External networks must not overlap with other networks within the site.

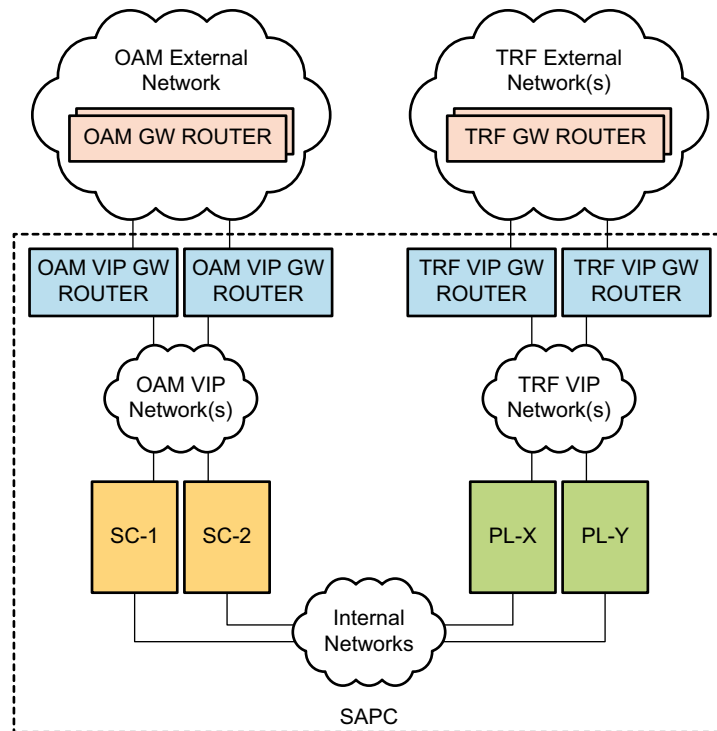


Figure 2 SAPC Deployment Including VIP Gateway Routers to Interconnect the SAPC with the Gateway Routers of the External Network

The main advantage for this alternative is that the configuration in the Gateway Routers is simple, just a single route to interconnect them with the correspondent VIP Gateway Routers. As drawbacks, additional resources are needed in VNF deployments for the VMs acting as VIP Gateway Routers. Also, comparing with the previous configuration, this is a less robust solution, as the connectivity depends on the availability of the two VIP Gateway Routers of the same type (OAM or Traffic), in case they are lost, the connectivity is also lost.





## 4 Network Description

This section provides a further description of the different network configurations for a SAPC.

### 4.1 Internal Networks

The Internal network provides internal blade or virtual machine cluster connectivity, and therefore exists in each SAPC node. This network is used for the communication between the members of the cluster, including traffic distribution, installation, booting and internal services, such as NTP and NFS.

Also, a Layer 2 Internal Network also exists for TIPC communication among the members of the cluster.

### 4.2 VIP Networks

The VIP addresses of the SAPC hide the internal architecture of the cluster by presenting only a limited set of IP addresses to the External network. Also, they provide scalability and redundancy for IP-based services by transparently distributing the IP traffic among the members of the SAPC node.

The VIP networks are used to provide access to the VIP addresses of the SAPC from the External network.

The following table collects the most relevant information regarding SAPC VIP networks.



Table 1 VIP Networks Summary

Network Common Name	Purpose	Allocated VIPs
OAM VIP Networks	<p>Provides access to the public IP addresses of the SAPC application for OAM and Provisioning purposes.</p> <p>There is always one mandatory OAM VIP Network to connect both OAM VIP Gateway Routers with the SAPC System Controllers. Also, there can be a second network dedicated to provisioning traffic.</p>	OAM and Provisioning VIPs
Traffic VIP Networks	<p>Provide access to the public Virtual IP addresses of the SAPC application for traffic handling.</p> <p>The Traffic VIP Networks connect both Traffic VIP Gateway Routers with the SAPC PLs providing the VIP addresses. The number of Traffic VIP Networks depends on the Traffic Network Separation Solution implemented. See chapter for Traffic Network Separation in Section 5 on page 15.</p>	Traffic VIPs

#### 4.2.1 VIP Gateway Routers

Depending on the Networking configuration scenario, the VIP Gateway Routers can be the Gateway Routers of the External network (scenario described in Section 3.1 on page 5) or specific ones part of the SAPC deployment (scenario described in Section 3.2 on page 6). In both cases, the VIP Gateway Routers are the integrating point of the SAPC cluster into the External network, and together with the VIP addresses of the SAPC, distribute and balance traffic.

For the VIP addresses to be properly available, the VIP Gateway Routers must have specific functionality and configuration on them, aligned with the one



defined in the SAPC cluster. Details on the particular configuration can be found in the [SAPC VNF Network Configuration Guide for VNF deployments](#) and in the [BSP 8100 Network Configuration Guide](#) and [NSP 6.1 Network Configuration Guide for PNF](#).

## 4.3 External Networks

The External networks are used to interoperate with the neighbors nodes in the customer networking. Addresses are always allocated from the IP range of the customer networking.

Through the External networks, the SAPC VIP addresses are reachable. When the SAPC is directly connected to the Gateway Routers of the External network, the External networks and the VIP networks are the same.

The following table collects the most relevant information regarding SAPC external networks.



Table 2 External Networks Summary

Network Common Name	Purpose	Allocated VIPs
OAM Networks	<p>OAM network. Provides a public IP address to access SAPC application for OAM and optionally, another public IP address for Provisioning purposes. The VIP for OAM and the VIP for provisioning, if exist, are external addresses reachable through this network.</p> <p>Provisioning network. Optional. It can be configured to separate provisioning traffic. In such cases, provisioning VIP is reachable through this network.</p>	<p>One OAM VIP per SAPC node in the site.</p> <p>One optional Provisioning VIP per SAPC node in the site.</p> <p>For Geographical Redundancy Active-Standby scenarios, one Provisioning VIP per GeoRed pair.</p>
Traffic Networks	<p>Traffic network. Provides public Virtual IP addresses to access the SAPC application for traffic handling.</p> <p>For deployments with no traffic separation, all the VIP Addresses for traffic handling, Replication, and External Database are reachable through this network.</p> <p>For deployments with traffic separation, all the VIP Addresses for traffic handling, Replication, and External Database are reachable through different networks.</p>	<p>One or several Traffic VIPs per SAPC node in the site.</p>

### 4.3.1 Routing Protocols for External Networks

For standalone and Active-Active Geographical Redundancy deployments, static routes are recommended to interoperate with the External networks. High





Availability in the Gateway Routers may be required, being provided by any mechanism, for example VRRP. For further details, see [SAPC VNF Deployment Instruction for OpenStack](#) and [SAPC VNF Deployment Instruction for VMware](#) for VNF deployments and [SAPC PNF Deployment Instruction](#) for PNF deployments.

For Active-Standby Geographical Redundancy scenarios, OSPF in the External network is mandatory, as there is only one connection point to the redundant SAPC pair from the external network independently of the node that is handling traffic and provisioning. The redundant SAPC solution exposes single VIP addresses for the SAPC pair to handle traffic and provisioning. These VIPs are announced by the active SAPC node through the OSPF protocol.

The usage of other routing protocols in the External network should be deployed as part of an integration project for the operator.

## 4.4 SysMGMT Network

SysMGMT is a mandatory network that provides external access to the host OSs of the SAPC cluster for system administration purposes in PNF deployments. The access is performed using statically configured IPs. No VIP is allocated for this network. IP addresses assigned must belong to the customer network plan.





## 5 Traffic Network Separation

The SAPC placement on the customer networks is intended to follow traffic separation principles. Traffic separation is used to isolate various traffic types from each other, for example O&M traffic and control plane Traffic are always kept strictly separated. There are numerous motivating reasons for traffic separation, the most important of these being **security** and **overlapping private IP address ranges**.

Two different scenarios for control plane Traffic Network separation are available in SAPC:

- **No Traffic separation:** All the supported protocols for Traffic handling (Gx, Rx, and so on) are carried through the same communication channel. Both TCP and SCTP are supported.
- **Traffic separation:** Traffic can be separated into different communication channels. Each traffic protocol may be handled separately in its own communication channel or configured to share communication channel than other of the protocols.

**Note:** All communication channels support TCP, but only one of them can be configured to support SCTP.

The following figures show the networking schema when all control plane traffic is carried through the same communication channel.

The figure on the left shows the schema in which the SAPC is connected to the Gateway Routers of the External network. The Gateway Routers are connected by a single External Traffic network with the SAPC PLs with external connectivity.

The figure on the right shows the schema in which the SAPC deployment contains VIP Gateway Routers. The Traffic VIP Gateway Routers are connected by a single Traffic VIP network with the SAPC PLs with external connectivity. The Gateway Routers are connected by a single External Traffic network with the VIP Gateway Routers.

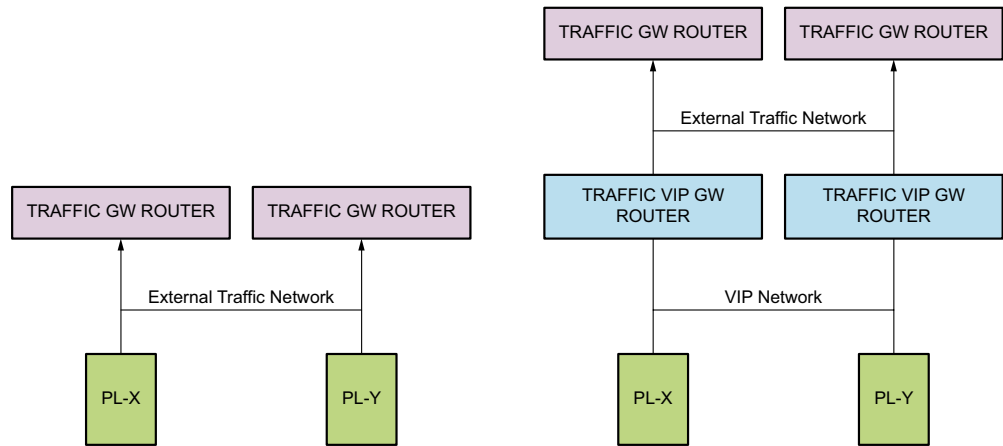


Figure 3 SAPC Traffic Networks without Traffic Separation: With and Without VIP Gateway Routers

When traffic is separated in several communication channels, per each channel, an extra Traffic network is configured.

The figure on the left shows the schema in which the SAPC is connected to the Gateway Routers of the External network. An External Traffic network per communication channel connects the Gateway Routers with the SAPC PLs with external connectivity. The Gateway Routers could be different for every channel.

The figure on the right shows the schema in which the SAPC deployment contains VIP Gateway Routers. A VIP Traffic network per communication channel connects the Traffic VIP Gateway Routers with the SAPC PLs with external connectivity. An External Traffic network per communication channel connects the Gateway Routers with the VIP Gateway Routers. The Gateway Routers could be different for every channel.

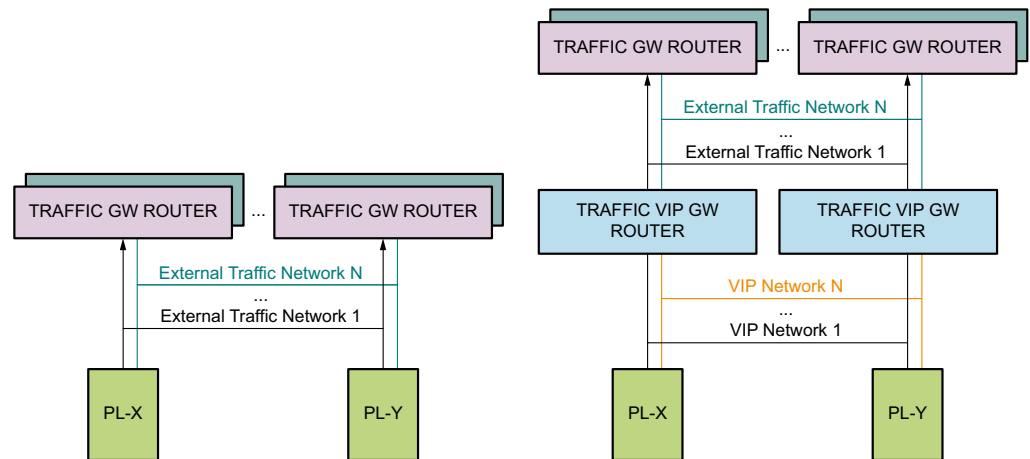


Figure 4 SAPC Traffic Networks with Two Communications Channels for Traffic Separation

For further details, see SAPC VNF Deployment Instruction for OpenStack and SAPC VNF Deployment Instruction for VMware for VNF deployments and SAPC PNF Deployment Instruction for PNF deployments.





## 6 VIP Address Allocation

The following sections describe the virtual IP addresses announced by the SAPC cluster towards the external network. All of them are IP addresses that combined with a protocol and a port provide the access point to the services offered by a SAPC node to interoperate with other network nodes. Additional VIP address can be configured in the same or different communication channels.

### 6.1 OAM VIP

Mandatory address that corresponds to the VIP accessible from the External OAM network and used to communicate with the SAPC node for administration purposes.

The address must be allocated from the customer network plan and is accessible through the External OAM operator network in the site.

Any outgoing traffic, produced as response to incoming requests to the OAM VIP, carry SAPC node OAM VIP as source address.

### 6.2 Provisioning VIP

Optional address for SAPC standalone and Active-Active Geographical Redundancy deployments and mandatory for Active-Standby Geographical Redundancy. It corresponds to the VIP used by the Provisioning Systems to communicate with the SAPC node. If not defined in standalone, OAM VIP is used for provisioning instead.

The address must be allocated from the customer network plan and is accessible through the External OAM operator network in the site, either sharing communication channels with OAM VIP (default) or having separated channels.

Any outgoing traffic, produced as response to incoming requests to the Provisioning VIP, carry SAPC node Provisioning VIP as source address.

### 6.3 Traffic VIPs

Mandatory addresses that correspond to the VIPs that external traffic applications use to send and receive traffic to and from the SAPC node.

These addresses must be allocated from the customer network plan and are accessible through the External Traffic network in the site.

Any outgoing traffic, produced as response to incoming requests to any of the Traffic VIPs, carry this particular VIP as source address.



Any outgoing traffic for End User Notifications to SMS Server or WEB Server, carry the Gx Traffic VIP as source address.

## 6.4 Replication VIP

Only for Geographical Redundancy scenarios in which its presence is mandatory. It corresponds to the VIP SAPC uses to send and receive database replication data to and from current SAPC node to its geo-replicated pair.

The address must be allocated from the customer network plan and is accessible through the External Traffic network in the site.

Any outgoing traffic, produced as response to incoming requests to the Replication VIP of each of the SAPC nodes in GeoRed, carry this SAPC node Replication VIP as source address.

## 6.5 External Database VIP

Only for deployments with an External Database in which its presence is optional. It corresponds to the VIP used to provide access to an external database system and receive SOAP notifications. If not defined, Traffic VIP dedicated to Gx is used instead.

The address must be allocated from the customer network plan and is accessible through the External Traffic network in the site.

Any outgoing traffic, produced as response to incoming requests to the External Database VIP, carry the SAPC node External Database VIP as source address.

## 6.6 Event-Based Monitoring VIP

Only for EBM scenarios in which its presence is mandatory. It corresponds to the VIP that the SAPC uses to send EBM traffic to the EBM server.

The address must be allocated from the customer network plan and is accessible through the External Traffic network in the site.

Any outgoing traffic for EBM events to the EBM server carries the SAPC node EBM VIP as source address.





## 7 Traffic Flows

This section describes the traffic flows that a SAPC node manages. Overall details are included, however, several low-level details that vary depending on the capabilities provided by routing and switching solutions provided by the hardware platform are intentionally omitted. The omitted details included in the hardware-specific network configuration document are the following:

- Quality of Service and traffic handling profiles
- Low level routing details

### 7.1 Incoming Traffic

This section details traffic flows coming from external entities across a SAPC node.

For each traffic flow, the following is shown:

- Purpose of each traffic flow.
- Access point the SAPC node exposes as entry point for the traffic flow. This corresponds to a transport address.
- Networks where the traffic flow is enabled. That is, networks through which the traffic flow is received and accepted.
- Any other detail relevant for the traffic flow.

Table 3 OAM\_SSH

Purpose	Access Point	Enabled on Networks
SSH access to System Controller (SC) processors from OAM customer network for OAM purposes (Northbound Interface, NBI).	VIP belonging to OAM network allocated from customer network plan, considered as OAM VIP of the node.  TCP port 22	OAM



Table 4 OAM\_NETCONF

Purpose	Access Point	Enabled on Networks
Access to NETCONF service from for OAM purposes.	VIP belonging to OAM network allocated from customer network plan, considered as OAM VIP of the node.  TCP port 830	OAM

Table 5 SAPC\_DIAMETER

Purpose	Access Point	Enabled on Networks
Point of access to DIAMETER traffic front ends to applications from customer network.	VIPs belonging to Traffic networks allocated from customer network plan, considered as Traffic VIPs of the node.  TCP/SCTP Port 3868 (default)	Traffic

Table 6 GEORED\_REPLICATION\_IN

Purpose	Access Point	Enabled on Networks
Point of access to database replication channel front ends from customer networks.	VIP belonging to Replication network allocated from customer network plan, considered as Replication VIP of the node.  TCP port 5666	Replication



Table 7 GEORED\_HEARTBEAT\_IN

Purpose	Access Point	Enabled on Networks
Point of access for GeoRed process heartbeat.	<p>VIP belonging to Replication network allocated from customer network plan, considered as Replication VIP of the node.</p> <p>For Active-Active Geographical Redundancy deployments, default VIP belonging to Traffic network allocated from customer network plan, considered as default Traffic VIP of the node.</p> <p>TCP port 9981</p>	<p>Replication.</p> <p>Traffic, for Active-Active Geographical Redundancy deployments.</p>

Table 8 SOAP\_NOTIFICATIONS\_IN

Purpose	Access Point	Enabled on Networks
Point of access for incoming SOAP Notifications.	<p>If defined, VIP belonging to ExtDB network allocated from customer network plan, considered as ExtDB VIP of the node.</p> <p>TCP port 8080</p>	ExtDB if defined

## 7.2 Outgoing Traffic

This section describes the details for the traffic originated in a SAPC node towards external entities.

For each traffic flow, the following is shown:

- Network or equipment that receives the traffic and, when applicable, UDP or TCP port
- Description of each traffic flow
- Required source address to set in outgoing packets
- Gateway to use in case the traffic must traverse its immediate receiving network



— Any other detail relevant for the traffic flow

Table 9 OAM\_Out\_SNMP

Description	Destination IP Address	Destination Port	Source Address	Gate way
SNMPVx traffic generated from the node towards the system acting as trap collector (Vx means SNMP versions v1, v2c, and v3).	IP address stated in SNMPvxTargetVx Managed Object (MO). For more details, refer to <code>class Snmp</code> .	Port stated in SNMPvxTargetVx MO. For more details, refer to <code>class Snmp</code> .	OAM VIP	OAM network gateway

Table 10 OAM\_Out\_NTP

Description	Destination IP Address	Destination Port	Source Address	Gate way
NTP requests	NTP servers configured in file <code>/cluster/etc/cluster.conf</code> , parameters <code>ntp</code>	UDP port 123.	OAM VIP	OAM network gateway

Table 11 Traffic\_Out\_Diameter

Description	Destination IP Address	Destination Port	Source Address	Gate way
Outgoing connections towards DIAMETER clients.	Any	Any	Traffic VIP	Traffic network gateway

Table 12 REPLICATION\_OUT

Description	Destination IP Address	Destination Port	Source Address	Gate way
Outgoing database replication channel traffic.	Any	Any	Replication VIP	REPLICATION network gateway



Table 13 LDAP\_OUT

Description	Destination IP Address	Destination Port	Source Address	Gate way
Outgoing external database queries.	Any	Any	ExtDB VIP	ExtDB network gate way

Table 14 END\_USER\_NOTIFICATIONS\_OUT

Description	Destination IP Address	Destination Port	Source Address	Gate way
Outgoing End User Notifications to SMS Server and WEB Server	Any	Any	GX Traffic VIP	Traffic network gate way

Table 15 EBM\_OUT

Description	Destination IP Address	Destination Port	Source Address	Gate way
Outgoing EBM events to EBM server	Any	Any	EBM VIP	EBM network gate way





## 8 Security

This section includes general guidelines for protecting the network infrastructure of the SAPC.

The main and most important recommendation is protecting the VIP Gateway Router requiring administrator authentication, by using passwords and Access Control Lists. Also, any potentially vulnerable "default setting" must be changed on the VIP Gateway Router.

The following security policies are recommended to be implemented in the VIP Gateway Router:

- Create a firewall policy that specifies how the firewall handles inbound and outbound network traffic.
- Configure ingress filtering for the services provided by the SAPC.
- Incoming packets that have an internal source address must be dropped.
- A stateful firewall must be used to block unwanted incoming traffic, but allowing bidirectional connections initiated by the SAPC.
- Make sure that incoming packets in an established connection and packets that are related to them are allowed.
- Configure logging of blocked packets as they match the firewall policies.
- When both IPv4 and IPv6 are used, configure security settings individually for each protocol.
- Configure the VIP Gateway Router to deny all incoming and outgoing Internet Control Message Protocol (ICMP) traffic except for those types and codes permitted by the organization: Allow only those ICMP messages which are essential for the supervision of the customer network and the customer security policy.
- Even though the SAPC is placed in a safe network, to prevent Distributed Denial of Service (DDoS) attacks, limit the connection rate at the VIP Gateway Router, or to set / configure the DDoS protection at this gateway router.

If the VIP Gateway Router cannot or partially provide sufficient security features, deploy an extra external firewall or security Gateway Router providing the functions previously described.