

SAPC Network Description

Ericsson Service-Aware Policy Controller

USER GUIDE

Copyright

© Ericsson España, S.A. 2017. 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.

Abstract

The purpose of this document is to provide a description of network details of the SAPC node.



Contents

1	Introduction	1
1.1	Document Purpose and Scope	1
1.2	Target Audience	1
2	SAPC Overview	3
3	Network Overview	5
3.1	Internal Network	6
3.2	VIP Networks	6
3.3	External Networks	12
3.4	SysMGMT Network	14
4	Traffic Flows	15
4.1	Incoming Traffic	15
4.2	Outgoing Traffic	17
5	Security	19





1 Introduction

1.1 Document Purpose and Scope

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.
- Private and public 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.

1.2 Target Audience

The main users of this document are the following:

- System architects, system administrators, and any other Ericsson personnel with an interest in 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 [Technical Product Description](#).





2 SAPC Overview

SAPC application can be deployed on top of Cloud Data Centers (VNF deployments) and on any HW fulfilling the minimum requirements (PNF deployments), both described in [Technical Product Description](#).

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.

The SAPC networks are classified into the following categories, depending on its use and the region it belongs to:

- **External:** External networks are used to transport incoming and outgoing traffic to the customer routers. Those addresses must not overlap with other networks within the site.
- **VIP:** VIP Networks for OAM and Traffic are used to announce to the External networks, the Virtual IP (VIP) addresses that neighbors can use to communicate with the SAPC node. These neighbors include, among others, PCEFs, External Databases, or Provisioning Systems.
- **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.
- **SysMGMT:** The SysMGMT network is defined for host administration purposes. Only in use for PNF deployments.

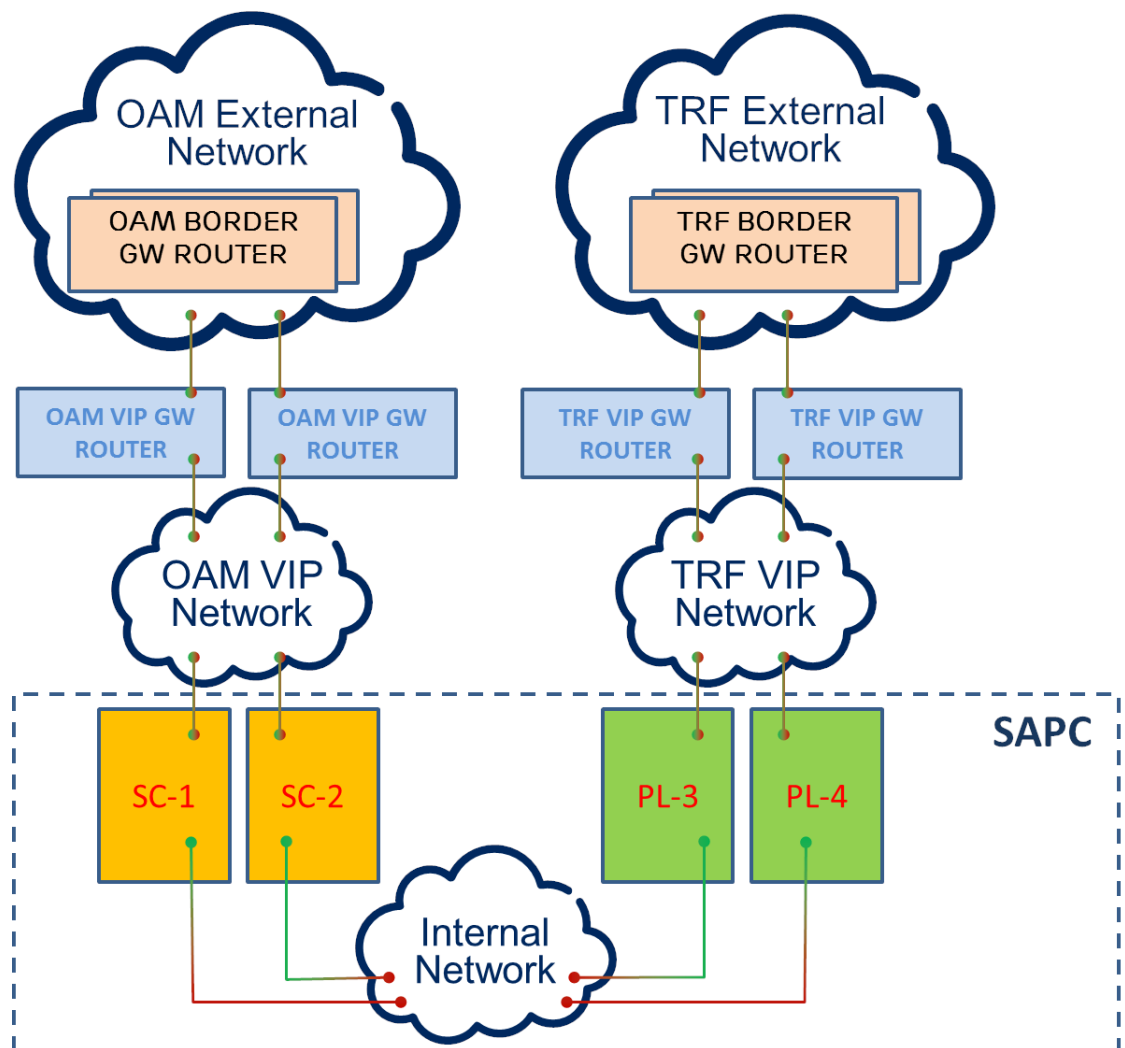


Figure 1 SAPC Networks Overview

3.1 Internal Network

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, TIPC traffic, installation, booting and internal services such as NTP and NFS.

3.2 VIP Networks

The VIP function provides scalability and redundancy for IP-based services by transparently distribute the IP traffic among the members of the SAPC node. It also hides the internal architecture of the cluster by presenting only a limited set of IP address, the Virtual IP (VIP) addresses, to the customer network.



The VIP networks are used to announce to the neighbors in the External network the Virtual IP Addresses of the SAPC.

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

Table 1 VIP Networks Summary

Network Common Name	Purpose	Allocated VIPs
OAM VIP Networks	<p>Announce public IP addresses to access SAPC application for OAM and Provisioning purposes.</p> <p>There is an OAM VIP Network to connect each OAM VIP Gateway Router with the SAPC System Controllers.</p>	OAM and Provisioning VIPs.
Traffic VIP Networks	<p>Announce public Virtual IP addresses to access SAPC application for traffic handling.</p> <p>The Traffic VIP Networks connect each Traffic VIP Gateway Router with the SAPC Traffic Processors providing the VIP function (including VIP front ends). The number of Traffic VIP Networks depends on the Traffic Network Separation Solution implemented. See next chapter.</p>	Traffic VIPs.

3.2.1 Traffic Network Separation In SAPC

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 is separated into different communication channels. Also it can define which traffic protocols share communication channel for different applications:
 - One network for Gx protocol.
 - One network for Rx protocol (by default, together with Sy).
 - One network for Geographical Redundancy replication.
 - One network for External Database communication.

Note: Both Gx and Rx communication channels support TCP, but only one of them, can be configured to support SCTP.

When all control plane Traffic is carried through the same communication channel, each Traffic VIP Gateway Router is connected by a Traffic VIP network with the SAPC Traffic Processors (TP) providing the VIP function.

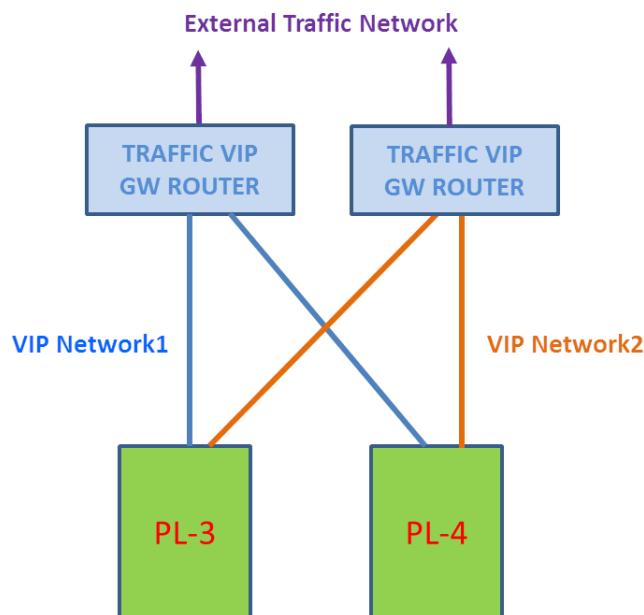


Figure 2 SAPC Traffic VIP Networks without Traffic Separation

When traffic is separated in several communication channels, per each channel, additional Traffic VIP networks connect each Traffic VIP Gateway Router with the SAPC TPs providing the VIP function to guarantee a proper network separation.

Next figure shows traffic separation using two communication channels with only two TPs providing the VIP function:

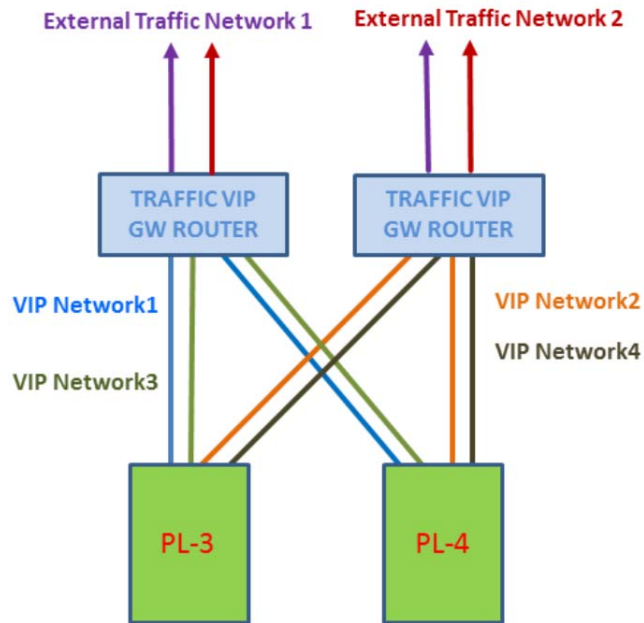


Figure 3 SAPC Traffic VIP Networks with Two Communications Channels for Traffic Separation

Next figure shows traffic separation using four communication channels with several TPs providing the VIP function:

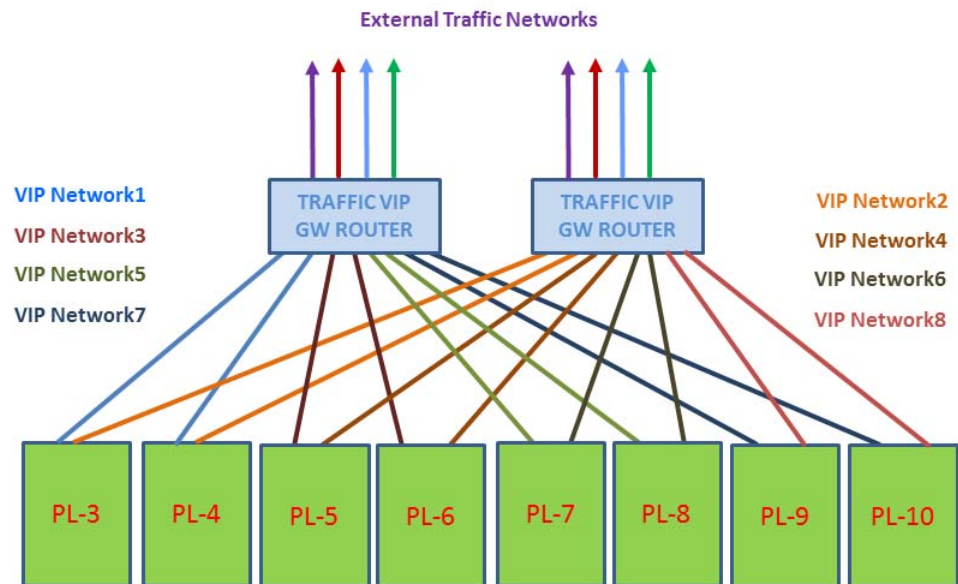


Figure 4 SAPC Traffic VIP Networks with Four Communications Channels for Traffic Separation

3.2.2

VIP Addresses

The following sections describe the virtual IP addresses announced by the SAPC cluster towards the external network. All them are network 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.

OAM VIP

Mandatory address that corresponds to the VIP within the External OAM network use to communicate with the SAPC node for administration purposes.

The address must be allocated from the customer network plan and is announced 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.



Provisioning VIP

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

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

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

Traffic VIPs

Mandatory addresses that corresponds to the VIPs within the External Traffic network that external traffic applications use to send/receive traffic to/from the SAPC node.

These addresses must be allocated from the customer network plan and are announced 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.

Replication VIP

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

The address must be allocated from the customer network plan and is announced 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.

External Database VIP

Only for deployments with an External Database in which its presence is optional. It corresponds to the VIP within the External Traffic network 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 announced 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.



3.2.3 VIP Gateway Routers

The VIP networks connect the VIP front ends defined in the SAPC cluster with the VIP Gateway Routers. The VIP Gateway Routers are the integrating point of the SAPC cluster into the External network and together with the SAPC 's VIP function distributes and balances traffic.

The VIP Gateway Routers are not a part of the VIP function, however, VIP does require specific functionality and configuration on them, that is, Open Shortest Path First (OSPF) protocol support and configuration aligned with the one defined in the SAPC cluster. Details on the particular OSPF 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](#).

In Cloud Data Centers, the VIP Gateway Routers, not being part the SAPC cluster, are created as additional Virtual Machines during the SAPC VNF deployment.

3.3 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.

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



Table 2 External Networks Summary

Network Common Name	Purpose	Allocated VIPs
OAM	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 exists, are external addresses announced through this network.	One OAM VIP per SAPC node in the site. One Provisioning VIP per SAPC node in the site. For Geographical Redundancy scenarios, one Provisioning VIP per GeoRed pair.
Traffic Networks	Traffic network. Provides public Virtual IP addresses to access SAPC application for traffic handling. For deployments with no traffic separation, all the VIP Addresses for traffic handling, Replication, and External Database are announced through this network. For deployments with traffic separation, all the VIP Addresses for traffic handling, Replication, and External Database are announced through different networks.	One or several Traffic VIPs per SAPC node in the site.

3.3.1 Routing Protocols for External Networks

OSPF is the protocol used between the VIP gateway routers and the Border gateway routers in the External network. Details on the particular OSPF configuration to interoperate with the External network 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](#).

For Geographical Redundancy scenarios, OSPF 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 OSPF protocol.

For standalone deployments, static routes can be also used instead of OSPF. For further details, see [SAPC VNF Deployment Instruction for CEE](#) and [SAPC VNF Deployment Instruction for VMware](#) for VNF deployments and [SAPC PNF Deployment Instruction](#) for PNF deployments.

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

3.4 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 customer network plan.

4 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. Omitted details, included in the hardware-specific network configuration document, are:

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

4.1 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.	VIP belonging to Replication network allocated from customer network plan, considered as Replication VIP of the node. TCP port 9981	Replication.



Table 8 SOAP_NOTIFICATIONS_IN

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

4.2 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 class Snmp.	Port stated in SNMPvxTargetVx MO. For more details, refer to class Snmp.	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 /cluster/etc/cluster.conf, parameters ntp	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 gateway



5 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.