Cisco Service Control Value Added Services Solution Guide

Release 4.0.x
May 27, 2013

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number: OL-29104-01

Cisco Service Control Value Added Services Solution Guide

About this Guide

Revised: March 17, 2015

Introduction

This preface describes who should read the *Cisco Service Control Value Added Services Solution Guide,* how it is organized, and its document conventions.

This guide is for experienced network administrators who are responsible for configuring and maintaining the Cisco Service Control solution.

Document Revision History

Table 1 records changes to this document.

Table 1 Document Revision History

Revision	Cisco Service Control Release and Date	Change Summary
OL-30605-01	Supports all 4.1.x releases December 23, 2013	First version of the document for Release 4.1.x train. No changes from the previous release.

Organization

This guide contains the following sections:

Table 2 Document Organization

Section	Title	Description
1	Overview of the Cisco Service Control Value Added Services Feature	Provides an overview of the Cisco Service Control Value Added Services feature.
2	Configuring the SCE Platform to Support VAS Traffic Forwarding	Describes how to configure the SCE platform to support Cisco Service Control Value Added Services (VAS). From the SCE platform, you can do the following: • Enable VAS support • Configure global VAS parameters • Configure VAS servers • Configure VAS server groups
3	Configuring the SCA BB Application to Support VAS Traffic Forwarding	Describes how to configure packages for VAS support. From the SCA BB console, you can do the following: • Enable VAS support • Assign meaningful names to VAS server groups • Assign specific traffic flows to specific VAS server groups
4	Monitoring VAS Traffic Forwarding	Describes how to monitor VAS support.
5	VAS Configuration Example	Provides a complete VAS configuration example.

Related Publications

Your SCE platform and the software running on it contain extensive features and functionality, which are documented in the following resources:

- For further information about the Service Control CLI and a complete listing of all CLI commands, see these guides:
  - *Cisco SCE 8000 CLI Command Reference*
  - *Cisco SCE 2000 and SCE 1000 CLI Command Reference*
- For further information about configuring the SCE platform, see these guides:
  - *Cisco SCE 8000 10GBE Software Configuration Guide*
  - *Cisco SCE 8000 GBE Software Configuration Guide*
  - *Cisco SCE 2000 and SCE 1000 Software Configuration Guide*
- For further information about configuring the SCA BB application, see the *Cisco Service Control Application for Broadband User Guide.*

- For viewing Cisco documentation or obtaining general information about the documentation, see the following sources:
  - *Obtaining Documentation and Submitting a Service Request, page 4*
  - The Cisco Information Packet that shipped with your SCE platform.

Conventions

This document uses the following conventions:

Table 3 Conventions

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem*.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning **Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.**

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Overview of the Cisco Service Control Value Added Services Feature

Revised: March 17, 2015

Introduction

The VAS feature enables the Cisco SCE platform to access an external "expert system" for classification and control of services not supported by Cisco SCA BB. Using the VAS feature, you can forward selected flows to an external, third-party system for per-subscriber processing in addition to the existing services and functions of the SCA BB solution. For example, this feature can be used to forward selected subscriber traffic to third-party servers for intrusion detection or content-filtering.

The VAS feature enables you to divert a specified part of the traffic stream to an individual VAS server or a cluster of servers. The diversion of the traffic stream is based on the subscriber package, flow type, and the availability of the VAS servers. The feature provides load balancing for even distribution of the load on the various VAS servers.

The VAS feature supports multiple VAS service types using different VAS server groups. Several servers of the same type can be deployed in a group to increase the processing capacity and provide redundancy for each VAS service type.

The SCE platform performs subscriber load sharing between the active servers of the same server group. It is able to identify the active servers among the defined servers through a dedicated health check mechanism.

VAS Service Goals

The VAS traffic forwarding functionality enables the Service Control solution to meet several important service goals:

- Service providers can provide a range of value-added services to their subscribers, thus increasing customer satisfaction.
- The SCE platform can forward part of the traffic to third-party devices that can provide additional, complementary services.

  The SCE platform, due to its strong classification capabilities, forwards only the part of the traffic that requires additional service based on:

  - Subscriber awareness

  - Policy that was configured
- The Service Control solution can include value-added servers that cannot be deployed inline for various reasons. For example, they cannot support throughput or are not carrier grade for inline insertion.
- Easy interoperability and flexibility for setting different services.

  Because the VAS feature emulates a regular IP network for the third-party devices, no special support is required on the part of the third-party entity.

How VAS Traffic Forwarding Works

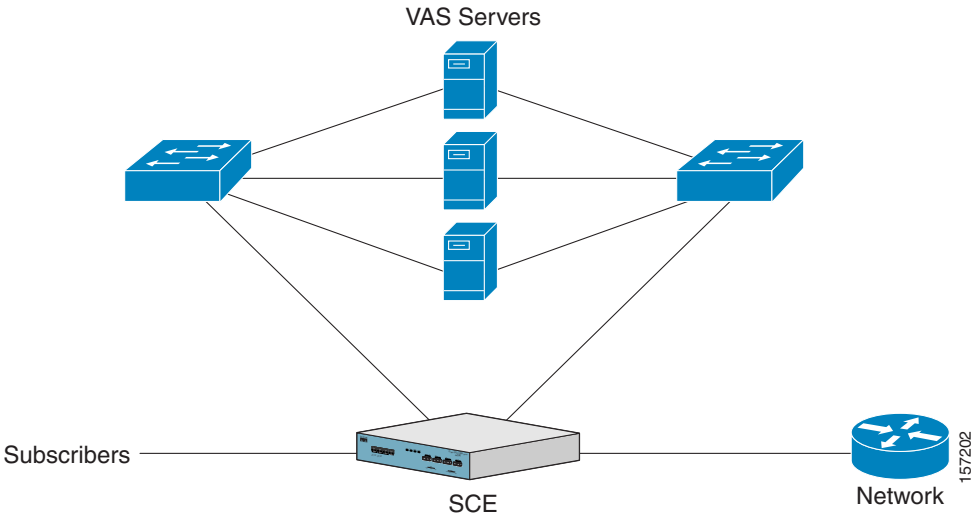
Subscribers are provisioned to the VAS services as part of the normal provisioning process of new subscribers to SCA BB.

When VAS traffic forwarding is enabled (see Figure 1-1), in addition to all its basic functions, the SCA BB classifies each flow as either a VAS flow or as a standard flow (nonVAS flow).

Flows that are classified to a VAS service get the usual SCA BB service, additionally these flows are forwarded the VAS servers for additional service. Traffic is processed first by the SCA BB application and then forwarded to the VAS servers.

Traffic is routed to the VAS servers using VLAN tags to identify the traffic flows.

Figure 1-1 Typical VAS Traffic Forwarding Installation



VAS traffic forwarding guidelines:

- Maximum number of VAS servers per single SCE platform:
  - SCE 2000—8
  - SCE8000—64
- Maximum number of SCE platforms that can be connected:
  - SCE 2000—512
  - SCE8000—64

- Maximum number of VAS server groups—Eight (applies to both SCE8000 and SCE 2000 platforms).
- More than one SCE platform may use the same VAS server.
- The VAS traffic forwarding feature is not supported on the SCE 1000 2xGBE platform.

Note In VAS mode, the SCE performance envelope might be up to 50 percent lower than in the normal operation mode. The exact performance envelope is specific to the traffic mix in the customer network and should be sized in advance.

The following sections provide a detailed description of how VAS traffic forwarding works:

Requirements for VAS Servers

Because VAS devices are installed behind the SCE platform, they should follow the network behavior of the SCE platform. Therefore, VAS devices must meet the following two requirements:

- VAS devices must be equipped with two separate interfaces, one for the subscriber side and one for the network side.

  Traffic toward the subscribers should be sent from the subscriber interface and for the Internet from the network interface.
- VAS devices must be transparent in Layer 2. The VAS servers must act like Layer 2 switches in that they are not allowed to change traffic headers or to generate new traffic.

Layer 2 Transparency

To handle nonmanagement traffic of VAS services, follow these guidelines:

- The VAS services should work in promiscuous-mode in Layer 2 and accept packets with any destination MAC address.
- When forwarding traffic back to the network after processing, the VAS devices must preserve the original Layer 2 headers containing the MAC addresses and the VLAN tag. The VAS devices must not change the MAC addresses (destination or source) or the VLAN tags. The following restrictions apply to the injected traffic:
  - The VAS device is not permitted to initiate new flows.
  - New traffic can be injected only in the context of an existing flow.
  - When injecting traffic, the Layer 2 information (MAC addresses, VLAN tags, and the TCP/IP parameters) must be taken from the flow into which the traffic is being injected.
- A VAS device must not generate its own network transactions or relay such transactions. Network transactions such as ARP requests or pings are not permitted.

VAS Management Traffic

VAS devices that are managed inband (through the traffic interface) must meet the following requirements:

- Management traffic should either be carried over a dedicated VLAN or without any VLAN header.
- The switches that are connected to the VAS devices should be directly connected to the POP router.
- The switches that are connected to the VAS devices should be configured so that management traffic is sent directly to the router and not through the SCE platform.

VAS Traffic Forwarding and SCA BB

When VAS traffic forwarding is enabled, in addition to all its basic functions, the SCA BB application classifies each flow as either a VAS flow or as a standard flow (nonVAS flow). This classification is made on the first packet of the flow (for example, TCP SYN packet). This classification is used to select the routing of the packet to a VAS server, to the subscriber, or to a network. Hence, it is important that the classification is performed on the first packet.

The VAS traffic forwarding rules table is configured using the SCA BB console. These rules map certain traffic to the VAS server groups. When a flow is classified as a VAS flow, the VAS server group for this flow is selected. If the group includes more than one VAS server, traffic is forwarded so that the subscriber load is shared between the servers on the same group.

The mapping of traffic portions per package to VAS server groups is also done using the SCA BB console.

VLAN Tags for VAS Traffic Forwarding

The VLANs router traffic between the SCE platform and the VAS servers. There is a unique VLAN tag for each SCE platform and VAS server combination.

Before the traffic is forwarded to the VAS servers, the SCE platform adds the VLAN tags to the original traffic. When the traffic returns to the SCE platform, the SCE platform removes the VLAN tag it previously added, and then forwards the traffic on its original link.

The VLAN tag for each VAS server is user-configured. To preserve consistency of the traffic flow, the VAS feature requires a unique VLAN tag be configured for each SCE platform and VAS server combination.

The VLAN tag has 12 bits, divided as follows:

- SCE8000 (maximum of 64 VAS servers):
  - The lower 6 bits identify the VAS server.
  - The higher 6 bits identify the SCE platform.

  For example, 0x171 = 1011 10001 = SCE 11, VAS 17
- SCE 2000 (maximum of eight VAS servers):
  - The lower 3 bits identify the VAS server.
  - The higher 9 bits identify the SCE platform.

  For example, 0x20 = 100 000 = SCE 4, VAS 0

Observe the following for the higher bits that identify the SCE platform:

- The higher bits must be the same for all VAS servers attached to a specific SCE platform.
- These bits must be different for VAS servers attached to different SCE platforms.

The SCE platform enforces that the user-configured VLAN tags retain this format, that is, the lower bits match the VAS server number for which the VLAN tag is configured and the higher bits match the higher bits previously configured for other VAS servers on this SCE platform. However, the SCE platform cannot determine the configuration of other SCE platforms, and therefore, it is important that the configured SCE ID (higher bits) is unique for each SCE platform.

The use of VLAN tags is an integral part of the VAS feature, and therefore, requires that the VAS device is able to work in 802.1q trunk while preserving the VLAN information.

Service Flow

The SCE platform classifies a flow to a VAS server group based on the subscriber package and the TCP/UDP ports of the flow. It then selects one server within this group to handle the flow.

The SCE platform performs load sharing between multiple VAS servers belonging to the same server group; the balance is based on the subscriber load. In other words, the SCE platform ensures that the subscribers are evenly distributed between the VAS servers in the same group. The mapping of subscriber to a VAS server (per group) is maintained even when servers are added or removed from the group either due to configuration changes or changes in the operational status of the servers in the group. The mapping changes only if the same server changes its status.

The following sections explain in more detail when and how the mapping is changed.

- NonVAS Data Flow, page 1-6
- VAS Data Flow, page 1-6

Data Flow

In a deployment using VAS traffic forwarding, there are two types of data flows:

- NonVAS flow
- VAS flow

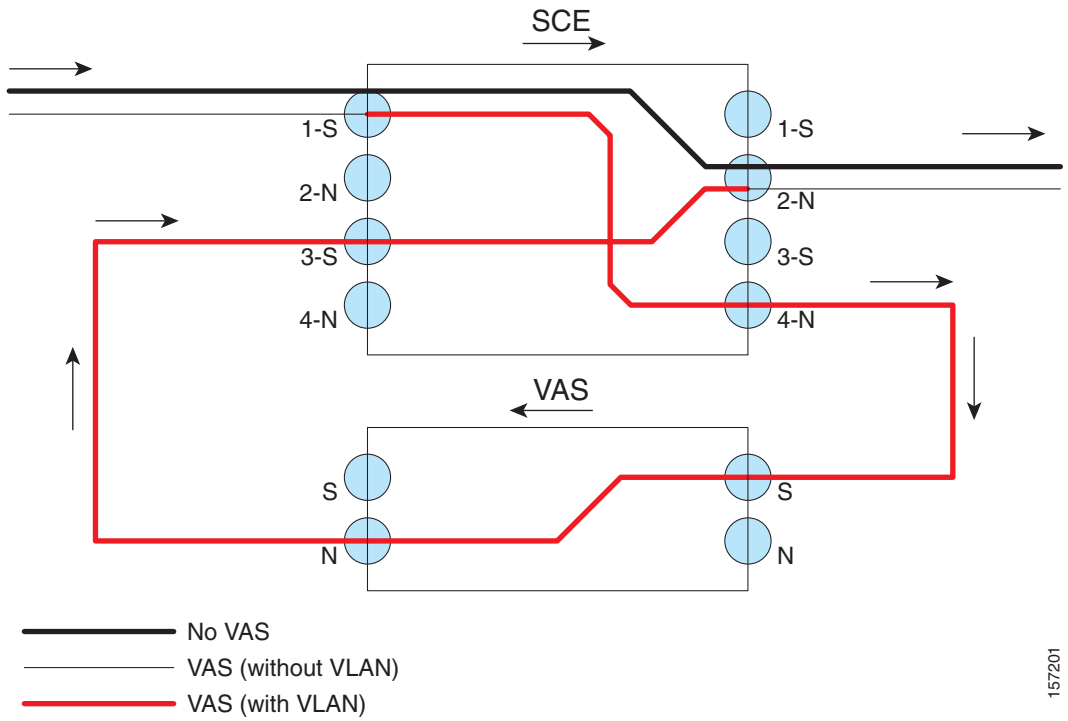
Figure 1-2 depicts the two types of data flows running through a single SCE platform and a single VAS server.

- Ports are illustrated as two unidirectional half ports, RX (on the left side) and TX (on the right side):
  - The SCE platform has four ports.
  - The VAS server has two ports.
- For the sake of illustration, the SCE platform traffic flow direction is from left to right while the VAS traffic flow is from right to left. The arrow below the name of the element indicates the traffic flow direction.
- The Ethernet switches are omitted.
- Each line represents a flow:
  - Thick line is a nonVAS flow.
  - Thin line is a VAS flow.

- Black line indicates part of a flow that does not have a VLAN tag.
- Red line indicates part of a flow that has a VLAN tag.

Figure 1-2 illustrates the data flow from the subscriber to the network. Data flow from the network to the subscriber works in the same way, but is received on the network port (N) and transmitted on the subscriber port (S).

Figure 1-2 Data Flow in a VAS System



NonVAS Data Flow

The data flow steps for a nonVAS flow are:

1. A subscriber packet is received at the SCE platform Port 1 (S).
2. The SCE platform classifies the flow as nonVAS flow.
3. The packet is sent to the network on Port 2 (N).

VAS Data Flow

A VAS data flow is slightly more complex than the basic data flow. A VAS data flow is received and transmitted in the same manner as a basic nonVAS SCE platform flow. The difference is, before a VAS data flow is transmitted to its original destination, it flows through the VAS server.

The data flow steps for a VAS flow are:

1. A subscriber packet is received at the SCE platform Port 1 (S).
2. The SCE platform classifies the flow as a VAS flow.
3. The SCE platform adds a VLAN tag to the packet.

4. The Ethernet switch uses the VLAN tag to route the packet to the proper VAS server.

   The packet now has a VLAN tag. The red line in Figure 1-2 indicates the VLAN tag.

5. The packet is sent to the VAS subscriber port from the SCE platform Port 4 (N).

6. The VAS server processes the packets and either drops the packet or sends it back to the SCE platform from the VAS network port to the SCE platform subscribers Port 3 (S).

   The VAS server passes the VLAN tag transparently. This is important to enable the Ethernet switch (not shown in the Figure) to route the packet back to the proper SCE platform.

7. The SCE platform receives the packet on Port 3 (S), drops the VLAN tag, and passes the packet towards the network through Port 2 (N).

Load Balancing

VAS servers can be grouped logically according to their service type. Consider, for example, a system that requires both FTP caching and virus filtering. A single VAS server for each service might not have enough capacity. For example, assume that the system requires five VAS servers, three to provide FTP caching, and two to provide virus filtering. Defining two VAS server groups, for example, FTP caching and virus filtering, permits load sharing across the servers for each server group.

The subscriber package determines the VAS server group to which the flow should be attached. The selection of a specific VAS server from the VAS servers within the group is based on the current load on each VAS server. The system tries to create an equal subscriber load for all the VAS servers belonging to the same group.

In some cases, more than one SCE platform uses a single VAS server. SCE platform performs load balancing only on the traffic that it sends to the VAS server; it receives no information on the load the VAS server may be bearing from a different SCE platform. It is vital to allocate available VAS servers properly to the SCE platforms to ensure a balanced load on each VAS server.

Load Balancing and Subscribers

The system balances the usage of the VAS servers within a VAS server group. The system tries to create an equal subscriber load for all the VAS servers in one VAS server group. The load balancing is subscriber-based, that is, the subscribers are evenly distributed between the servers.

VAS load sharing is subscriber based rather than bandwidth based. This ensures that all the traffic of the subscriber gets to the same server so that the server can make subscriber-based decisions.

The SCE platform uses the same VAS server for all the traffic of a subscriber (per server group) regardless of the change in the number of active servers in the group. Traffic from a subscriber is assigned to a new server only if the current server becomes inactive. This applies only on new flows. Flows that were already mapped to a server before it became active remain attached to it.

The mapping of subscriber to VAS servers is not saved across subscriber logouts or SCE platform reload.

Load Balancing and Subscriber Mode

Load balancing is subscriber-based. This feature does not work properly in the subscriberless mode, because only one VAS server in each group carries the entire traffic load.

Tip Use anonymous mode rather than subscriberless mode with VAS traffic forwarding.

In pull mode, the first flow of the subscriber behaves as configured in the anonymous template. If no anonymous template is configured, such first flows are processed as defined by the default template. Therefore, the default template should provide a proper package, so these flows get VAS service.

VAS Redundancy

Configure high availability on VAS servers so that the total system performance and availability are not affected due to the failure of the single VAS server. This requirement must be considered when determining the number of VAS servers necessary for each VAS service.

There are two mechanisms that guarantee the performance and availability of the VAS services:

- Load sharing—The SCE platform distributes the subscribers between all the active VAS servers within a server group.
- Monitoring—The SCE platform monitors connectivity with the VAS servers and handles server failure according to the applied configuration.

In addition to failure of an individual VAS server, a complete VAS server group is considered to be failed if a defined minimum number of servers are not active.

The following sections provide more information about the possible points of failure in a VAS traffic forwarding deployment:

- VAS Server Failure, page 1-8
- VAS Server Group Failure, page 1-8
- Ethernet Switch Failure, page 1-9
- Disabling a VAS Server, page 1-9

VAS Server Failure

The system monitors the health of a VAS server by periodically checking the connectivity between the SCE platform and the VAS server. When the SCE platform fails to establish or maintain a connection to the server within a configurable window of time, the server is considered to be in **Down** state.

When the server is in **Down** state:

- New logged-in subscribers are distributed between the other active servers in the group.
- If subscribers mapped to this server initiate new flows, they are mapped to a new server.
- If the failure causes the number of active servers in the group to go below the minimum number of active servers configured, the server group moves to a **Failure** state.

If the connectivity to the server resumes, the state of the server is changed to **Up.** The server returns to the list of active servers and continues to serve subscribers that were mapped to it before the failure and have not yet been mapped to a new server during the failure time, as well as new subscribers.

VAS Server Group Failure

For each VAS server group, you can configure:

- The minimum number of active servers necessary.
- The action to take in case the actual number of active servers goes below the configured minimum.

If the minimum number of active servers equals the total number of configured servers, it means that there is no redundancy and failure of one server causes the failure of the whole server group.

When the SCE platform detects that the number of active servers within a group is below the configured minimum, it changes the state of the group to **Failure**. The configured action-on-failure is then applied to all new flows mapped for that VAS server group (existing flows are not affected.)

There are two possible actions when the VAS server group has failed:

- **Block**—The SCE platform blocks all new flows assigned to the failed VAS server group.
- **Pass**—All new flows assigned to the failed VAS server group are considered as regular non-VAS flows, and are processed without VAS service. This means that these flows receive SCA BB service but no VAS service.

When the number of active servers is above the minimum and the state of the group is changed to Active again, the configured action-on-failure is no longer applied to the new flows. However, to maintain the coherency of the network, the change in the state of the server group does not affect the flows that were blocked or passed.

Ethernet Switch Failure

The Ethernet switches are a single point of failure in a VAS topology. If an Ethernet switch fails completely, all VAS services connected to that switch are declared as failed. Action configured for on-failure instances is taken for all new VAS flows.

Disabling a VAS Server

A VAS server can be disabled for maintenance via the CLI.

No errors are reported on a disabled VAS server. However, if disabling the server reduces the number of active servers to below the minimum number configured for the group, it brings down the VAS server group because a disabled VAS server is equal to a VAS server in **Down** state.

Health check is not performed on disabled VAS servers.

VAS Status and VAS Health Check

To manage the VAS redundancy, the SCE platform has to be aware of the state of each VAS server. The SCE platform performs periodic health checks for all the configured VAS servers. These checks are the basis for VAS redundancy control. These checks enable the SCE platform to:

- Identify and react to VAS server failure.
- Check the connectivity between the SCE platform and the VAS server before enabling the server to handle traffic.

The health check is performed over the VAS link, that is, the link that connects the SCE platform with the VAS servers. It validates the traffic flow between the SCE platform and the VAS server in both directions through special health check packets generated by the SCE platform.

The health check mechanism does not require special interaction with the VAS device. Special interaction is not required because the VAS server does not have to answer health check packets; it only passes them as they are, back to the SCE platform. As long as the SCE platform receives the packets, the

VAS server is considered to be alive. If the SCE platform fails to receive the packets back from the VAS server within a predefined window, the VAS server is considered as failed and the server status is changed to **Down**.

Health check packets are:

- Carried over UDP flows.
- Contain source and destination IP addresses that can be user-configured.

  IP addresses should be:

  - Unique to the SCE platform.
  - Addresses that are not used by the network traffic (such as private IP addresses).

The SCE platform uses default UDP ports beginning with 63140 and 63141 for VAS Server 0, unless you configure different ports for the health check.

The SCE platform adds its own Layer 7 data on top of the UDP transport layer, and uses this data to validate the correctness of the packet upon retrieval.

The health check is performed under the following conditions:

- VAS mode is enabled.
- VAS server is enabled.
- Health check for the VAS server is enabled.
- Server has a VLAN tag.
- Pseudo IP addresses are configured for the traffic interfaces.

If the check is enabled, but any one of the conditions is not met, the server state will be **Down** (the same as if the server did not pass the health check).

Check the connectivity between the SCE platform and the VAS server before you assign the server to a server group.

The health check procedure does not require a special interface with the VAS server; the health check traffic goes through the same network channels as any other VAS traffic. However, there are two assumptions the VAS servers should fulfill:

- The VAS server should not drop traffic unless it is specifically configured to do so. Therefore, if the connectivity between the VAS server and the SCE platform is operative, the health check packets should reach the SCE platform safely.

  Alternatively, it should be possible to configure the VAS server to pass traffic on specific ports (the health check ports).
- In a failure, the VAS server should drop and not bypass, the traffic (cut the link), so that the SCE platform is able to identify the failure.

VAS Server States

When determining whether a VAS server is active, the system considers the following two parameters:

- User-configured Admin mode—Enabled or disabled
- VAS server state as reported by the health check

VAS Traffic Forwarding Topologies

These sections describe the following VAS traffic forwarding topologies:

- Single SCE Platform, Multiple VAS Servers, page 1-11
- Multiple SCE Platforms, Multiple VAS Servers, page 1-12

Note A topology in which a VAS server is directly connected to the SCE platform is not supported. To create a topology with a single SCE platform connected to a single VAS server, use a switch between the SCE platform and the VAS server.

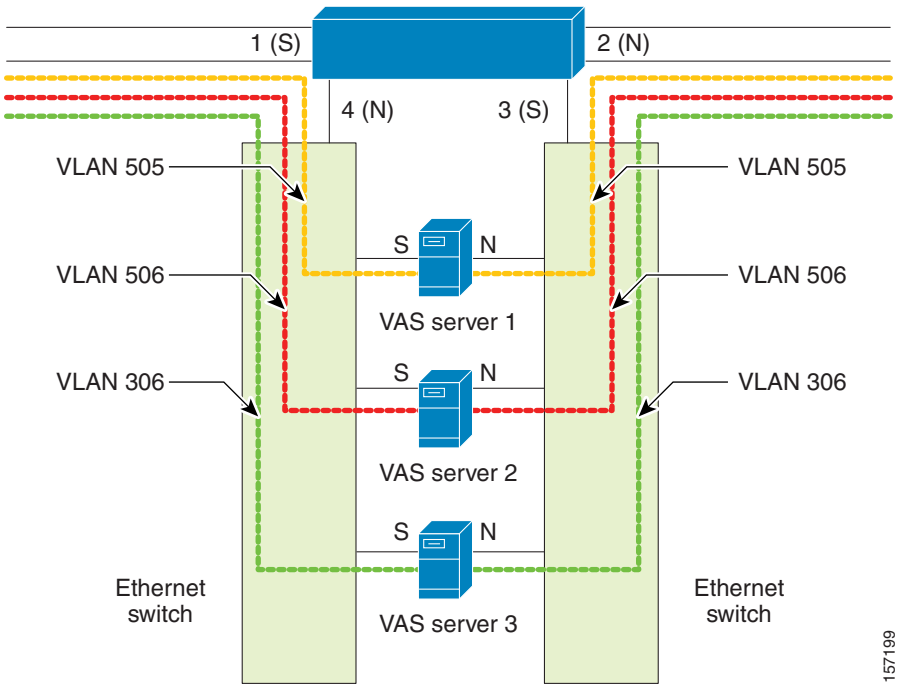
Single SCE Platform, Multiple VAS Servers

In this topology, a single SCE platform forwards VAS traffic to one or more VAS servers through two Ethernet switches (Figure 1-3).

The presence of two Ethernet switches avoids a situation in which a single MAC address has two ports or a single VLAN tag has two destinations.

Configure trunk mode on each Ethernet switch and disable MAC learning.

Figure 1-3 Single SCE Platform, Multiple VAS Servers



Data Flow

In a data flow:

1. A subscriber packet is received at Port 1 (Subscriber).

2. The SCE platform opens a flow and classifies the flow as either a nonVAS (blue) flow or as a VAS flow (red).
3. If the flow is nonVAS (blue), the SCE platform passes the packet to the network. The VAS server is not involved in this case.
4. If the flow is a VAS flow (red), the SCE platform selects the destination VAS server, adds the server VLAN tag to the packet, and transmits the packet on Port 4 (Network).
5. The Ethernet switch routes the packet to the VAS server based on its VLAN tag. The port towards the VAS server should be the only port with this VLAN tag allowed.
6. The VAS server processes the packet and either drops or forwards it without changing the VLAN tag.
7. The Ethernet switch forwards the packet to the SCE platform based on its VLAN tag. The port towards the SCE platform should be the only port with this VLAN tag allowed.
8. The SCE platform receives the packet on Port 3 (Subscriber), removes the VLAN tag, and forwards the packet to the network via Port 2 (Network).

Multiple SCE Platforms, Multiple VAS Servers

In this topology, multiple SCE platforms are connected to multiple VAS servers. At least one VAS server receives traffic from more than one SCE platform; if the VAS servers are each in an exclusive relationship to a particular SCE platform, it would simply be several single SCE platforms to multiple VAS server topologies grouped together.

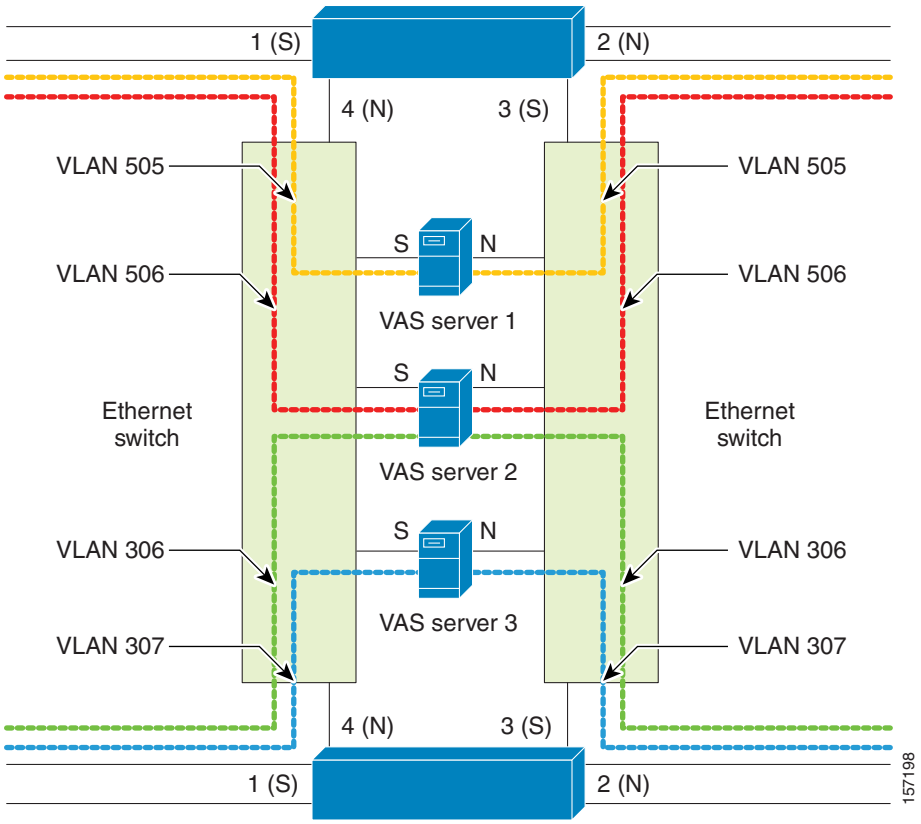
In Figure 1-4, the top SCE platform forwards traffic to VAS Server 1 and Server 2, while the bottom SCE platform forwards to VAS Server 2 and Server 3. A unique VLAN tag must designate each SCE-platform-to-VAS-server path. This topology is illustrated with two SCE platforms, but a maximum of 64 SCE8000 platforms or 512 SCE 2000 platforms is supported (limited by the VLAN tag size).

The two Ethernet switches route the traffic to the VAS servers. The routing is VLAN-based. Configure the trunk mode on the Ethernet switch and disable the learning.

The data flow is the same as the flow for the single SCE platform to multiple VAS servers topology (see "Data Flow" section on page 1-11).

Note The multiple SCE platforms to multiple VAS servers topology do not support SCE platform redundancy on the cascade ports.

Figure 1-4 Multiple SCE Platforms, Multiple VAS Servers



SNMP Support for VAS

The following items in the "PCUBE-SE-MIB" proprietary MIB support VAS traffic forwarding:

- SCE-MIB object—vasTrafficForwardingGrp SCE-MIB
- Object type—vasServersTable provides information on each VAS server operational status.
- SNMP Trap—vasServerOperationalStatusChangeTrap signifies that the agent entity has detected a change in the operational status of a VAS server.

Interactions Between VAS Traffic Forwarding and Other SCE Platform Features

This section consists of these topics:

Incompatible SCE Platform Features

There are certain SCE platform features that are incompatible with VAS traffic forwarding. Before you enable VAS traffic forwarding, make sure that no incompatible features or modes are configured.

The following features and modes cannot coexist with VAS mode:

- Line-card connection modes—receive-only, receive-only-cascade, inline-cascade
- Link mode other than forwarding
- All link encapsulation protocols, including VLAN, MPLS, and L2TP
- Traffic mirroring

Note If VAS forwarding is enabled, Cisco SCE devices do not forward VLAN-tagged subscriber traffic received from subscriber side and network side traffic ports to the VAS interface for processing.

VAS Traffic Forwarding and DDoS Processing

VAS traffic forwarding has minor effects on the distributed denial of service (DDoS) mechanisms.

This section consists of these topics:

Specific IP DDoS Attack Detection

The specific IP DDoS mechanism uses software counters. The second pass VAS packets do not reach the Service Control Operating System (SCOS), so they are not counted twice.

The attack-detector handles the network-side packets in the first pass, when these packets open a flow, so these packets are also not counted twice.

Specific IP Attack Filter

The behavior depends on the action configured.

- Report only—VAS is not affected.
- Block—Flow is blocked, no VAS service is provided.
- Bypass—Traffic is bypassed and NO SCA BB or VAS services are provided.

VAS Traffic Forwarding and Bandwidth Management

The complexity of the VAS traffic forwarding results in the modification of some SCE platform bandwidth management capabilities:

- VAS flows are not subject to global bandwidth control.
- The number of global controllers available to regular flows is decreased from 64 to 48.

Global Controllers and VAS Flows

When VAS traffic forwarding is enabled, the global controllers function slightly differently.

- Only 48 global controllers are available.
- Global controllers 49 - 63 are used to count VAS traffic.
- Reserved global controllers cannot be configured.
- VAS flows do not get the global controller from the traffic controller to which they belong. Rather, the global controller is set according to VAS rules.

Managing VAS Traffic Forwarding

Configuration of the VAS traffic forwarding feature is distributed between the SCA BB console and the SCE platform CLI:

- SCE platform CLI configuration:
  - Physical VAS server parameters—VLAN tag, Admin status, and health check parameters.
  - VAS server groups parameters—The VAS servers that belong to the group and the action to take if the group enters a **Failure** state.
- SCA BB console configuration—The traffic forwarding rules, defining which portion of the subscriber traffic should be forwarded to the VAS servers.

  The SCA BB configuration is defined per package, so that different subscribers can receive different VAS service, based on the package they bought.

The following section provides a high-level description of the steps for configuring and monitoring VAS traffic forwarding. Each step is explained in detail in the referenced sections in the following chapters.

Configuring the SCE Platform for VAS Traffic Forwarding

To configure the SCE platform for VAS traffic forwarding, complete the following steps:

Step 1 Define the VAS servers.

Step 2 Configure the VAS server groups.

Step 3 Enable VAS traffic forwarding on the SCE platform

Step 4 Verify that the individual VAS servers and the VAS server groups are all in **Up** state (see Chapter 1, “Monitoring VAS Traffic Forwarding”).

Configuring the SCA BB Application for VAS Traffic Forwarding

To configure the SCA BB for VAS traffic forwarding, complete the following steps:

Step 1 Enable VAS traffic forwarding in the SCA BB application.

Step 2 (Optional) Assign meaningful names to the server groups.

Step 3 Configure the VAS forwarding tables to configure which traffic goes to which VAS server group.

Step 4 Assign the VAS forwarding tables to the relevant packages.

Configuring the SCE Platform to Support VAS Traffic Forwarding

Revised: March 17, 2015

Introduction

This chapter consists of the following sections:

VAS Configuration on the SCE Platform: Servers and Groups

There are three broad aspects to configuring VAS traffic forwarding on the SCE platform:

- Configuring global VAS traffic forwarding options, such as enabling or disabling VAS traffic forwarding, or specifying the VAS traffic link.
- Configuring a VAS server, such as enabling or disabling a specific VAS server, or enabling or disabling the VAS health check for a specified VAS server.
- Configuring a VAS server group, such as adding or removing a specific VAS server, configuring the minimum number of active servers per group, or configuring VAS server group failure behavior.

Configuring the Global Options

There are two global VAS traffic forwarding options:

- Enable or disable VAS traffic forwarding.
- Configure the link number on which to transmit VAS traffic. This configuration is necessary only if the VAS servers are connected on link 0, rather than link 1, which is the default VAS traffic link.

Enabling VAS Traffic Forwarding

By default, VAS traffic forwarding is disabled. If you require VAS traffic forwarding, you can enable it any time.

For instructions on how to disable VAS traffic forwarding, see Disabling VAS Traffic Forwarding, page 1-2.

There are certain other SCE platform features that are incompatible with VAS traffic forwarding. Before enabling VAS traffic forwarding, you must make sure that no incompatible features or modes are configured.

These features and modes cannot coexist with VAS mode:

- Line-card connection modes—receive-only, receive-only-cascade, inline-cascade
- Link mode other than forwarding
- All link encapsulation protocols, including VLAN, MPLS, L2TP
- Enhanced open flow mode

Options for Enabling VAS Traffic Forwarding

The following options are available:

- **Enable**—Enable VAS traffic forwarding.
- **Disable**—Disable VAS traffic forwarding.
  - Default—Disable

To enable VAS traffic forwarding, use the **VAS-traffic-forwarding** command in the SCE interface configuration mode.

Example:

```
SCE(config if)# VAS-traffic-forwarding
```

Disabling VAS Traffic Forwarding

There are two conditions to consider while disabling the VAS Traffic Forwarding feature in run time:

- You cannot disable VAS mode on the SCE platform while the applied SCA BB policy instructs the SCE platform to forward traffic to the VAS servers.

  Therefore, dismiss all VAS traffic forwarding rules in the applied SCA BB policy before you disable the VAS traffic forwarding in the SCE platform.
- After the SCA BB has been reconfigured, there may still be some open flows that have already been forwarded to the VAS servers. If the VAS feature is stopped while there are still such flows open, the packets coming back from the VAS servers may be routed to their original destination with the VLAN tag of the VAS server on it.

  Therefore, to avoid inconsistency with the flows that are already forwarded to the VAS servers, shutdown the line card before you disable the VAS traffic forwarding in the SCE platform.

To disable VAS traffic forwarding, complete the following steps:

Step 1 From the SCA BB console, remove all the VAS table associations to packages and apply the changed policy.

Step 2 Shut down the line card.

At the SCE(config if)# prompt, enter the **shutdown** command, and press **Enter**.

Step 3 Disable VAS traffic forwarding.

At the SCE(config if)# prompt, enter the **no VAS-traffic-forwarding** command and press **Enter**.

Step 4 Restart the line card.

At the SCE(config if)# prompt, enter the **no shutdown** command and press **Enter**.

Configuring the VAS Traffic Link

By default, the VAS traffic is transmitted on Link 1. If the VAS servers are connected on Link 0, configure the VAS traffic link to Link 0.

Note Although it supports up to eight GBE links, the SCE 8000 GBE platform supports VAS traffic forwarding only on Link 0 and Link 1. VAS traffic cannot be configured on any other link.

Note The VAS traffic link should be in Forwarding mode.

Options for Configuring the VAS Traffic Link

The following option is available:

- **VAS traffic-link {link-0|link-1}**—The link number on which to transmit VAS traffic
  - Default—Link 1

Selecting the Link for VAS Traffic

To select the link for VAS traffic, enter the **VAS-traffic-forwarding traffic-link {link-0|link-1}** command at the SCE interface configuration mode.

Example:

```
SCE(config if)# VAS-traffic-forwarding traffic-link link-0
```

Reverting to the Default Link for VAS Traffic

To revert to the default link for VAS traffic, enter the **no VAS-traffic-forwarding traffic-link** command at the SCE interface configuration mode.

Example:

```
SCE(config if)# no VAS-traffic-forwarding traffic-link
```

Configuring a VAS Server

To configure a VAS server, first define the VAS servers. Each VAS server has the following parameters:

- Admin-mode — Enabled or disabled.
- Health Check mode — Enabled or Disabled
- Health Check ports
- VLAN tag

These sections explain how to perform the following operations for individual VAS servers:

- Enable a specified VAS server.
- Disable a specified VAS server.
- Define the VLAN tag for a specified VAS server.
- Enable or disable the Health Check for a VAS server.
- Define the source and destination ports to use for the Health Check.
- Delete all properties for a specified VAS server. The server returns to the default state, which is enabled. However, it is not operational since it does not have VLAN.

Note The VAS server is not operational until the VLAN tag is defined, even if the server itself is enabled.

VAS Server Options

The following VAS server option is available:

- **number**—The number of the VAS server:
  - SCE8000—0-63
  - SCE 2000—0-7

Enabling a VAS Server

Note The server is not operational until a VLAN tag has also been defined.

To enable a VAS server, enter **VAS-traffic-forwarding VAS server-id** *number* **enable** command at the SCE interface configuration mode.

Example:

```
SCE(config if)# VAS-traffic-forwarding VAS server-id 5 enable
```

Disabling a VAS Server

To disable a VAS server, enter **VAS-traffic-forwarding VAS server-id** *number* **disable** command at the SCE interface configuration mode.

Example:

```
SCE(config if)# VAS-traffic-forwarding VAS server-id 5 disable
```

Restoring All VAS Server Properties to Default

To restore all VAS server properties to default value, **no VAS-traffic-forwarding VAS server-id** *number* command at the SCE interface configuration mode.

Example:

SCE(config if)# **VAS-traffic-forwarding VAS server-id** *5*

Assigning a VLAN ID to a VAS Server

Use **VAS-traffic-forwarding VAS server-id** *number* **VLAN** *vlan-id* command to the assign the VLAN ID to a specified VAS server.

Options for Assigning a VLAN ID to a VAS Server

The following options are available:

- **number**—The number of the VAS server.
- **vlan-id**—The VLAN tag to use for the specified VAS server

  The VLAN tag can be redefined as necessary.
  - Default—No VLAN.

Note the following important points:

- The VAS server is not operational until the VLAN tag is defined.
- Disabling the server does not remove the VLAN tag number configured to the server.
- The **no** form of the command (same as the **default** form of the command), removes the previously configured VLAN tag (no VLAN is the default configuration).

Configuring the VLAN Tag Number for a Specified VAS Server

To configure the VLAN tag number for a VAS server, enter the **VAS-traffic-forwarding VAS server-id** *number* **VLAN** *vlan-id* command at the SCE interface configuration mode.

Example:

```
SCE(config if)# VAS-traffic-forwarding VAS server-id 5 VLAN 5
```

Removing the VLAN Tag Number from a Specified VAS Server

To remove the VLAN tag number from a VAS server, enter the **no VAS-traffic-forwarding VAS server-id** *number* **VLAN** command at the SCE interface configuration mode.

Example:

```
SCE(config if)# no VAS-traffic-forwarding VAS server-id number VLAN
```

You can also use the default form of the command to remove the VLAN tag configuration.

Example:

```
SCE(config if)# default VAS-traffic-forwarding VAS server-id  number VLAN
```

Configuring the Health Check

By default, the VAS server health check is enabled, however you may disable it.

The health check is activated only if all the following conditions are true. If the health check is enabled and if any one or more of the following conditions are not met, then the server will be in a **Down** state:

- VAS Traffic Forwarding mode is enabled.
- Pseudo IP addresses are configured for the SCE platform GBE ports on the VAS traffic link.
- VAS server is enabled.
- Server has a VLAN tag.
- Health check for the server is enabled.

If the health check of the server is disabled, its operational status depends on the following (requirements for **Up** state are in parentheses):

- admin status (enable).
- VLAN tag configuration (VLAN tag defined).
- group mapping (assigned to group).

Health Check Options

The following options are available:

- **number**—The ID number of the VAS server for which to enable or disable the health check
- **Enable/disable**—Enable or disable VAS server health check
  - Default—Enable
- **UDP ports**—Configure the UDP ports for the health check traffic:
  - **source portnumber**—Source port number for health check.
  - **destination portnumber**—Destination port number for health check.
  - Default—<63140,63141>used for Server 0 through <63154,63155> used for Server 7.

Enabling VAS Server Health Check

To enable VAS server health check, enter the **VAS-traffic-forwarding VAS server-id** *number* **health-check** command at the SCE interface configuration mode.

Example:

```
SCE(config if)# VAS-traffic-forwarding VAS server-id 2 health-check
```

Disabling VAS Server Health Check

To disable VAS server health check, enter the **no VAS-traffic-forwarding VAS server-id** *number* **health-check** command at the SCE interface configuration mode.

Example:

```
SCE(config if)# no VAS-traffic-forwarding VAS server-id 2 health-check
```

Defining the UDP Ports for Health Check Traffic

To define the UDP ports for health check traffic, enter the **VAS-traffic-forwarding VAS server-id** *number* **health-check UDP ports source** *portnumber* **destination** *portnumber* command at the SCE interface configuration mode.

Example:

```
SCE(config if)# VAS-traffic-forwarding VAS server-id 2 health-check UDP ports source
portnumber destination portnumber
```

Removing the UDP Ports Configuration

To remove the UDP ports configuration, enter the **no VAS-traffic-forwarding VAS server-id** *number* **health-check UDP ports** command at the SCE interface configuration mode.

Example:

```
SCE(config if)# no VAS-traffic-forwarding VAS server-id number health-check UDP ports
```

You can also use the default form of the command to remove the UDP port configuration.

Example:

```
SCE(config if)# VAS-traffic-forwarding VAS server-id  number health-check UDP ports
```

Configuring Pseudo IP Addresses for the Health Check Packets

Use the **pseudo-ip** *ip-address [mask]* command to configure source and destination pseudo IP addresses for the health check packets. This command allows you to specify a unique IP address for use by the health check packets.

This command is a ROOT level command and is available under the GBE configuration interface mode. Configure those interfaces that connect the SCE platform to the VAS servers. The following are the default interfaces:

- SCE 2000—GBE 0/3 and GBE 0/4
- SCE8000 GBE—3/0/2 and 3/0/3
- SCE8000 10G—3/2/0 and3/3/0

The SCE platform uses the pseudo IP address as follows:

- Pseudo IP address configured for the subscriber-side interface:
  - Source IP address for health check packets going upstream direction.
  - Destination IP address for health check packets going downstream direction.
- Pseudo IP address configured for the network-side interface:
  - Source IP address for health check packets going downstream direction.
  - Destination IP address for health check packets going upstream direction.

Options for Configuring Pseudo IP Addresses for Health Check Packets

The following options are available:

- **ip-address**—Configures the IP address for the health check packets. You can configure any IP address as long as it is not possible to be found in the network traffic, such as a private IP address.

  - Default—no IP address
- **mask** (Optional)—Defines the range of IP addresses the SCE platform can use. Note that the SCE platform is not required to be in this subnet.
  - Default—255.255.255.255 (The subnet mask can be set to 255.255.255.255, because the health check mechanism requires only one IP address per interface.)

Defining the Pseudo IP Address

To define the pseudo IP address, enter the **pseudo-ip** *ip-address [mask]* command at the SCE interface configuration mode.

Example:

```
SCE(config if)# pseudo-ip ip-address [mask]
```

Deleting the Pseudo IP Address

To delete the pseudo IP address, enter the **no pseudo-ip** *ip-address [mask]* command at the SCE interface configuration mode.

Example:

```
SCE(config if)# no pseudo-ip ip-address [mask]
```

Configuring a VAS Server Group

You can define up to eight VAS server groups. Each VAS server group has the following parameters:

- Server Group ID
- A list of VAS servers attached to this group.
- Failure detection—Minimum number of active servers required for this group in order for the group to be considered as Active. If the number of active servers goes below this minimum, the group is said to be in a Failure state.
- Failure action—Action performed on all new data flows that has to be mapped to this server group while it is in Failure state.

  Options:
  - block
  - pass

You can perform these operations for a VAS server group:

- Add or remove a VAS server to or from a specified group.
- Configure the minimum number of active servers for a specified group.
- Configure failure behavior for a specified group.

Adding and Removing Servers

This section explains how to add servers to and remove servers from a specified VAS server group. This section consists of these topics:

Options for Configuring a VAS Server Group

The following options are available:

- **group-number**—The ID number of the VAS server group (0-7).
- **id-number**—The ID number of the VAS server:
  - SCE8000—0-63
  - SCE 2000—0-7

Adding a VAS Server to a Specified VAS Server Group

To add a VAS server to a VAS server group, enter the **VAS-traffic-forwarding VAS server-group** *group-number* **server-id** *id-number* command at the SCE interface configuration mode.

Removing a VAS Server from a Specified VAS Server Group

To remove a VAS server from a VAS server group, enter the **no VAS-traffic-forwarding VAS server-group** *group-number* **server-id** *id-number* command at the SCE interface configuration mode.

Removing All VAS Servers from a Specified VAS Server Group

To remove all VAS servers from a specified VAS server group and set all group parameters to their default values, enter the **no VAS-traffic-forwarding VAS server-group** *group-number* command at the SCE interface configuration mode.

Configuring VAS Server Group Failure Parameters

This section explains how to configure the following failure parameters for the specified VAS server group:

- Minimum number of active servers—If the number of active servers in the server group goes below this number, the group is said to be in a Failure state.
- Failure action—The action taken on all new flows mapped to this server group while it is in Failure state:
  - Block—The SCE platform blocks all new flows assigned to the failed VAS server group.
  - Pass—The SCE platform considers all new flows assigned to the failed VAS server group as regular nonVAS flows and processes these flows without VAS service.

Options for Configuring VAS Server Group Failure Parameters

The following options are available:

- **group-number**—The ID number of the VAS server group.
- minimum-active-servers **min-number**—The minimum number of active servers required for the specified server group.
  - Default—1
- **failure action**—The action taken all new flows for the specified server group while it is in Failure state. Values are:
  - **block**
  - **pass** (default)

Configuring the Minimum Number of Active Servers for a Specified VAS Server Group

To configure the minimum number of active servers, enter the **VAS-traffic-forwarding VAS server-group** *group-number* **failure minimum-active-servers** *min-number* command at the SCE interface configuration mode.

Resetting the Minimum Number of Active Servers for a Specified VAS Server Group to the Default

To reset the minimum number of active servers, enter the **default VAS-traffic-forwarding VAS server-group** *group-number* **failure minimum-active-servers** *min-number* command at the SCE interface configuration mode.

Configuring the Failure Action for a Specified VAS Server Group

To configure the failure action for a specified VAS server group, enter the **VAS-traffic-forwarding VAS server-group** *group-number* **failure action {block | pass}** command at the SCE interface configuration mode.

Configuring the Failure Action for a Specified VAS Server Group to the Default

To revert the failure action configuration for the specified VAS server group to the default value (pass), enter the **default VAS-traffic-forwarding VAS server-group** *group-number* **failure action** command at the SCE interface configuration mode.

Configuring the SCA BB Application to Support VAS Traffic Forwarding

Revised: March 17, 2015

VAS Configuration in the SCA BB Application: Traffic-Forwarding Tables

In the SCA BB application, you define a set of parameters that enable the application to relate a particular traffic flow to a VAS service. Based on the combination of IP protocol and port number, traffic flows are assigned to a VAS server group. You can create one or more VAS forwarding tables defining the traffic forwarding schemes. Each forwarding table is then assigned to a package. Subscriber traffic in a package is forwarded to the respective VAS server groups according to the assigned VAS forwarding table.

There are four broad aspects to VAS traffic forwarding configuration in the SCA BB application:

- Enabling VAS traffic forwarding in the SCA BB application.
- (Optional) Assigning meaningful names to the server groups that were defined in the SCE platform.
- Configuring the VAS forwarding tables to configure which traffic goes to which VAS server group. If there are different traffic forwarding schemes for different groups of subscribers, create a traffic forwarding table for each scheme.
- Assigning the VAS forwarding tables to the relevant packages.

Enabling VAS Traffic Forwarding

By default, VAS traffic forwarding is disabled. You can enable it at any time.

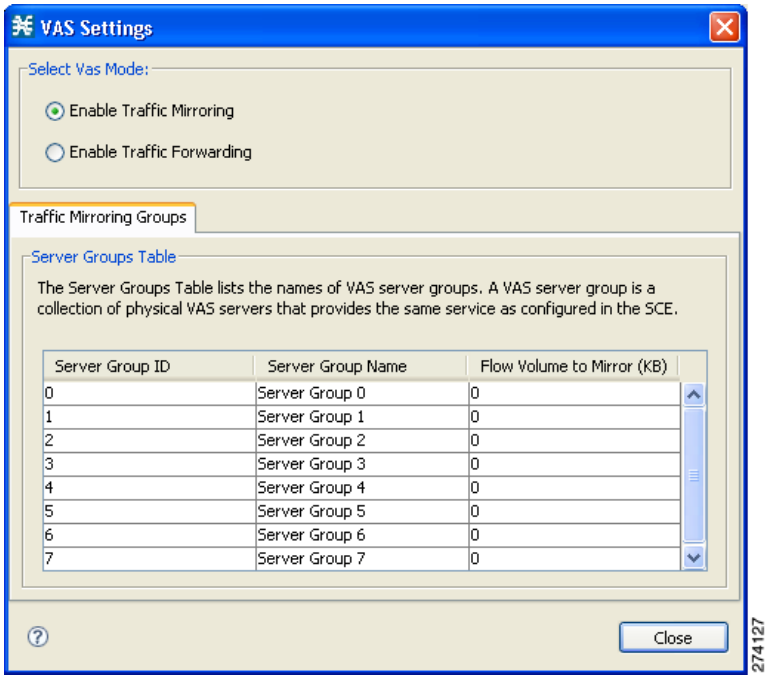
Note VAS traffic forwarding is not supported in asymmetric routing classification mode. If you try to enable traffic forwarding when asymmetric routing classification mode is enabled, a VAS error message appears.

To enable VAS traffic forwarding, complete the following steps:

Step 1 From the Service Configuration Editor, choose **Configuration > Policies > VAS Settings**.

The VAS Settings dialog box appears (Figure 1-1).

Figure 1-1 VAS Settings



Step 2 Click the **Enable Traffic Forwarding** radio button.

A VAS warning message appears.

Step 3 Click **Yes**.

Renaming the VAS Server Groups

An SCE platform can forward flows to up to eight different VAS server groups. By default, the eight server groups are named "Server Group *n*", where n takes a value from 0 to 7. These values correspond to the number you assigned to the server group when you created it using the SCE platform CLI.

For your own convenience, you can give the server groups meaningful names. The names you give appear in the drop-down list in the Server Group field when creating traffic-forwarding tables (see Managing VAS Table Parameters, page 1-5).

To rename the VAS server group, complete the following steps:

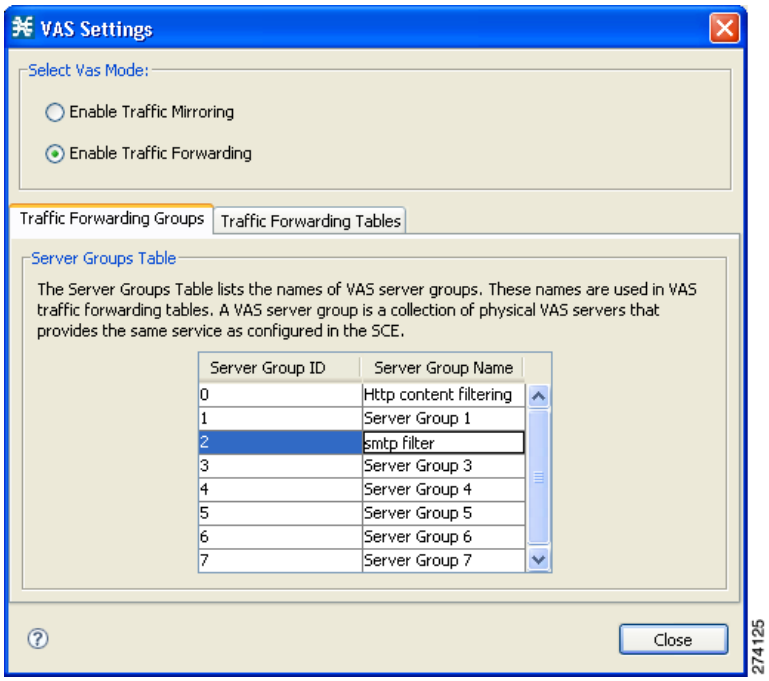
Step 1 From the Service Configuration Editor, choose **Configuration > Policies > VAS Settings**.

Step 2 In the table in the Server Groups Table area in the Traffic Forwarding Groups tab(see Figure 1-2), double-click in a cell containing a server group name.

Step 3 Enter a meaningful name in the cell.

Step 4 Repeat Step 2 and Step 3 for other server groups you wish to rename.

Figure 1-2 Traffic Forwarding Groups Tab



Managing the VAS Traffic-Forwarding Tables

SCA BB decides whether a flow passing through an SCE platform should be forwarded to a VAS server group based on a traffic-forwarding table. Each entry in a traffic-forwarding table defines which VAS server group the specified flows should be forwarded to. Flows are defined by IP protocols and port numbers.

Adding a VAS Traffic-Forwarding Table

A default traffic-forwarding table is included in the service configuration. You can add up to 63 more traffic-forwarding tables, and then assign different traffic-forwarding tables to different packages.

To add a VAS traffic-forwarding table, complete the following steps:

Step 1 From the Service Configuration Editor, choose **Configuration > Policies > VAS Settings**.

The VAS Settings dialog box appears.

Step 2 Click the **Traffic Forwarding Tables** tab.

The Traffic Forwarding Tables tab opens.

Step 3 In the Traffic Forwarding Tables area, click the Add icon.

A new table named Table (n), where *n* is a value from 1 through 63, is added to the list of traffic-forwarding tables.

The table name is also displayed in the Item Name box in the Table Parameters tab.

Step 4 In the Item Name field, enter a unique and relevant name for the traffic-forwarding table.

You can now add table parameters to the new traffic-forwarding table ("Adding VAS Table Parameters" section on page 1-5).

Step 5 Click **Close** to save the changes and close the dialog box.

Viewing VAS Traffic-Forwarding Tables

To view VAS traffic-forwarding table, complete the following steps:

Step 1 From the Service Configuration Editor, choose **Configuration > Policies > VAS Settings**.

The VAS Settings dialog box appears.

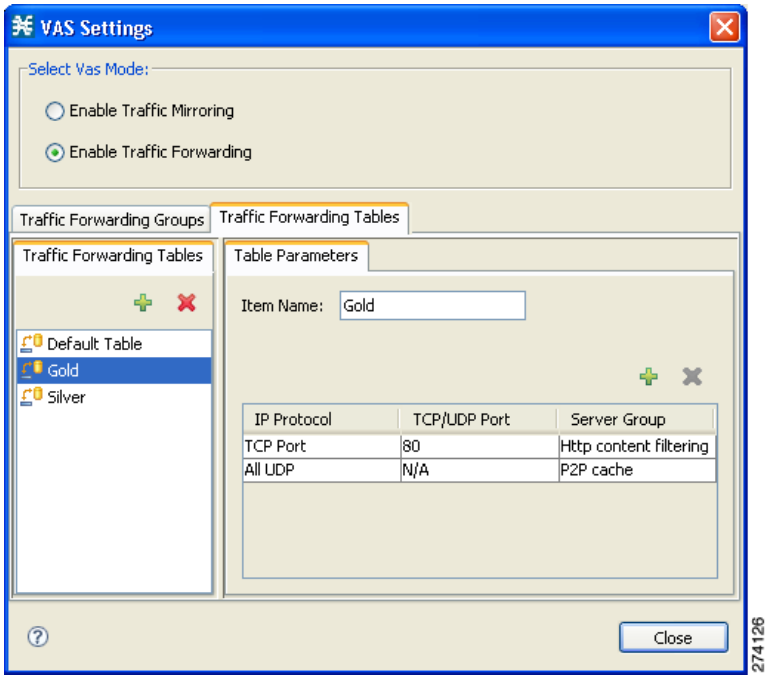
Step 2 Click the **Traffic Forwarding Tables** tab.

The Traffic Forwarding Tables tab opens, displaying a list of all traffic-forwarding tables in the left pane.

Step 3 Click a table in the list to display the table parameters.

A list of all table parameters defined for this traffic-forwarding table opens in the Table Parameters tab (Figure 1-3).

Figure 1-3 Traffic Forwarding Tables Tab



Deleting VAS Traffic-Forwarding Tables

You can delete all user-created traffic-forwarding tables. The default traffic-forwarding table cannot be deleted.

Note A traffic-forwarding table cannot be deleted while it is associated with a package.

To delete VAS traffic-forwarding tables, complete the following steps:

Step 1 From the Service Configuration Editor, choose **Configuration > Policies > VAS Settings**.

The VAS Settings dialog box appears.

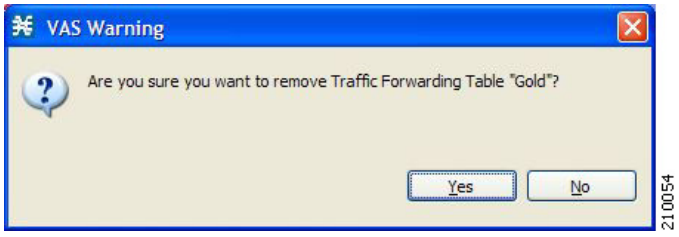
Step 2 Click the **Traffic Forwarding Tables** tab.

Step 3 From the list of traffic-forwarding tables in the Traffic Forwarding Tables area, select a table.

Step 4 Click the delete icon.

A VAS Warning message appears (Figure 1-4).

Figure 1-4 VAS Warning



Step 5 Click **Yes**.

Managing VAS Table Parameters

A table parameter is an entry in the VAS table. It consists of three parts:

- IP protocol type
- Associated TCP/UDP port or range of ports (where applicable)
- VAS server group or a range of IP addresses

A traffic-forwarding table can contain up to 64 table parameters.

- Adding VAS Table Parameters, page 1-5
- Editing VAS Table Parameters, page 1-6
- Deleting VAS Table Parameters, page 1-7

Adding VAS Table Parameters

You can add up to 64 table parameters to a traffic-forwarding table.

To add VAS table parameters, complete the following steps:

Step 1 From the Service Configuration Editor, choose **Configuration > Policies > VAS Settings**.

The VAS Settings dialog box appears.

Step 2 Click the **Traffic Forwarding Tables** tab.

Step 3 From the list of traffic-forwarding tables in the Traffic Forwarding Tables area, select a table.

Step 4 In the Traffic Parameters tab, click the add icon.

A new table parameter is added to the list of table parameters in the Table Parameters tab.

Note Each new table parameter has the default values as listed in Table 1-1.

Table 1-1 Table Parameter Default Values

Parameter	Default value
IP Protocol	TCP Port
Server Group	Server Group 0
TCP/UDP Port	80

You can now edit the new table parameter, as described in the following section.

Editing VAS Table Parameters

To edit VAS table parameters, complete the following steps:

Step 1 From the Service Configuration Editor, choose **Configuration > Policies > VAS Settings**.

The VAS Settings dialog box appears.

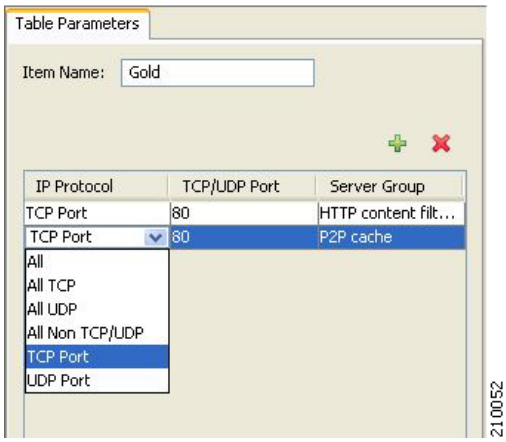
Step 2 Click the **Traffic Forwarding Tables** tab.

Step 3 From the list of traffic-forwarding tables in the Traffic Forwarding Tables area, select a table.

Step 4 In the table in the Table Parameters tab, select a protocol, port, and server group.

a. Click in a cell in the IP Protocol column, and, from the drop-down list that opens, select an IP protocol type (Figure 1-5).

Figure 1-5 Table Parameters Tab

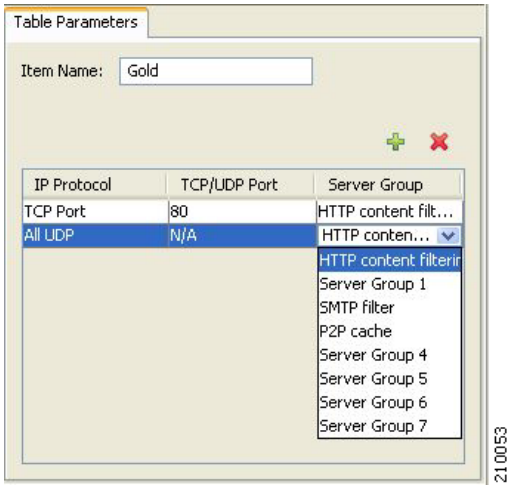


If you select All, All TCP, All UDP, or All Non TCP/UDP, "N/A" appears in the TCP/UDP Port cell when you move to another cell in the table.

b. If you select TCP Port or UDP Port, double-click in the cell in the TCP/UDP Port column, and enter the port number or a range of ports in the format *port1-port2*.

c. Click in the cell in the Server Group column, and, from the drop-down list that opens, select a server group (Figure 1-6).

Figure 1-6 Tables Parameters Tab



Step 5 Click **Close** to save the changes and close the dialog box.

Deleting VAS Table Parameters

To delete VAS table parameters, complete the following steps:

Step 1 From the Service Configuration Editor, choose **Configuration > Policies > VAS Settings**.

The VAS Settings dialog box appears.

Step 2 Click the **Traffic Forwarding Tables** tab.

Step 3 From the list of traffic-forwarding tables in the Traffic Forwarding Tables area, select a table.

Step 4 From the list of table parameters in the Table Parameters tab, select a table parameter.

Step 5 Click the delete  icon.

The selected table parameter is deleted and is no longer displayed in the list of table parameters.

Step 6 Click **Close** to save the changes and close the dialog box.

Assigning a VAS Forwarding Table to a Package

Traffic is forwarded to the appropriate VAS server group based on the package assigned to the subscriber. A traffic-forwarding table defining the desired traffic forwarding scheme is assigned to the package. The SCE platform then forwards all traffic for that package to the server groups according to protocol and port as defined in the assigned traffic forwarding table.

To assign a VAS forwarding table to a package, complete the following steps:

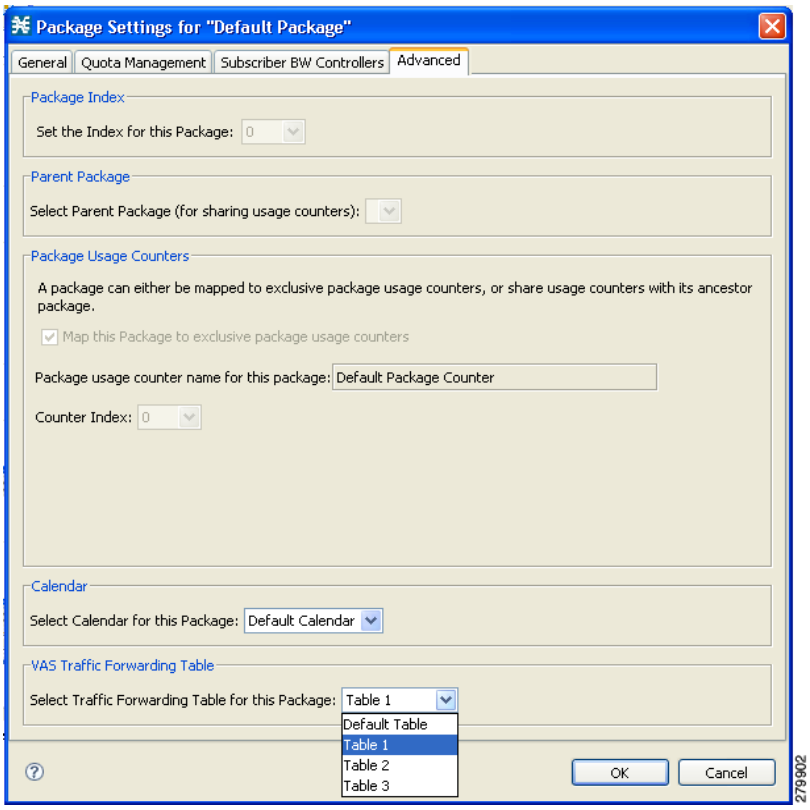
Step 1 In the **Policies** tab of the Service Configuration Editor, right-click the desired package name and select **Edit Package**.

The Package Settings dialog box for the selected package appears.

Step 2 Click the **Advanced** tab.

Step 3 At the bottom of the tab, in the VAS Traffic Forwarding Table area, select the desired traffic forwarding table from the drop-down list.

Figure 1-7 Edit Package Advanced Tab



Monitoring VAS Traffic Forwarding

Published: March 17, 2015

Introduction

Use the commands described in this chapter to display the following information for VAS configuration and operational status summary:

- Global VAS status summary—VAS mode, the traffic link used
- VAS Server Groups information summary—Operational status, number of configured servers, number of current active servers

The following information may be displayed for a specific server group or all server groups:

- VAS servers information summary—Operational status, health check operational status, number of subscribers attached to this server

The following information may be displayed for a specific server or all servers:

- Bandwidth per VAS server and VAS direction (to VAS or from VAS)
- VAS health check counters

Sample outputs are included.

How to Display Global VAS Status and Configuration

At the SCE> prompt, enter the **show interface linecard 0 VAS-traffic-forwarding** command and press **Enter**.

Example

```
SCE> show interface linecard 0 VAS-traffic-forwarding

VAS traffic forwarding is enabled
VAS traffic link configured: Link-1  actual: Link-1
```

How to Display Operational and Configuration Information for a Specific VAS Server Group

At the SCE> prompt, enter the **show interface linecard 0 VAS-traffic-forwarding VAS server-group** *id-number* command and press **Enter**.

Example

```
SCE> show interface linecard 0 VAS-traffic-forwarding VAS server-group 0

VAS server group 0:
State: Failure  configured servers: 0   active servers: 0
minimum active servers required for Active state: 1   failure action: Pass
```

How to Display Operational and Configuration Information for All VAS Server Groups

At the SCE> prompt, enter the **show interface linecard 0 VAS-traffic-forwarding VAS server-group all** command and press **Enter**.

How to Display Operational and Configuration Information for a Specific VAS Server

At the SCE> prompt, enter the **show interface linecard 0 VAS-traffic-forwarding VAS server-id** *id-number* command and press **Enter**.

Example

```
SCE> show interface linecard 0 VAS-traffic-forwarding VAS server-id 0

VAS server 0:
Configured mode: enable   actual mode: enable   VLAN:  520  server group:    3
State: UP
Health Check configured mode: enable  status: running
Health Check source port: 63140  destination port: 63141
Number of subscribers:       0
```

How to Display Operational and Configuration Information for All VAS Servers

At the SCE> prompt, enter the **show interface linecard 0 VAS-traffic-forwarding VAS server-id all** command and press **Enter**.

How to Display the VAS Servers Used by a Specified Subscriber

At the SCE> prompt, enter the **show interface linecard 0 subscriber name** *subscriber-name* **VAS-servers** command and press **Enter**.

How to Display Health Check Counters for a Specified VAS Server

At the SCE> prompt, enter the **show interface linecard 0 VAS-traffic-forwarding VAS server-id** *id-number* **counters health-check** command and press **Enter**.

Example

```
SCE> show interface linecard 0 VAS-traffic-forwarding VAS server-id 0

Health Checks statistics for VAS server '0'    Upstream      Downstream
-------------------------------------------------------------------------
Flow Index '0'
-----------------
Total packets sent                          :       31028  :       31027 :
Total packets received                      :       31028  :       31027 :
Good packets received                       :       31028  :       31027 :
Error packets received                      :           0  :           0 :
Not handled packets                         :           0  :           0 :
Average roundtrip (in millisecond)          :           0  :           0 :
Error packets details                       :              :             :
--------------------                        :              :             :
Reordered packets                           :           0  :           0 :
Bad Length packets                          :           0  :           0 :
IP Checksum error packets                   :           0  :           0 :
L4 Checksum error packets                   :           0  :           0 :
L7 Checksum error packets                   :           0  :           0 :
Bad VLAN tag packets                        :           0  :           0 :
Bad Device ID packets                       :           0  :           0 :
Bad Server ID packets                       :           0  :           0 :
```

How to Display Health Check Counters for All VAS Servers

At the SCE> prompt, enter the **show interface linecard 0 VAS-traffic-forwarding VAS server-id all counters health-check** command and press **Enter**.

How to Clear the Health Check Counters for a Specified VAS Server

At the SCE> prompt, enter the **clear interface linecard 0 VAS-traffic-forwarding VAS server-id** *id-number* **counters health-check** command and press **Enter**.

How to Clear the Health Check Counters for All VAS Servers

At the SCE> prompt, enter the **clear interface linecard 0 VAS-traffic-forwarding VAS server-id all counters health-check** command and press **Enter**.

How to Display Bandwidth Per VAS Server and VAS Direction

The bandwidth presented in the **VAS-traffic-bandwidth** command is measured at the Transmit queues. The first table in the example presents the bandwidth of traffic transmitted towards the VAS servers. The second table presents the bandwidth of traffic transmitted out of the SCE platform after the VAS servers processed the traffic.

The counting is based on Layer 2 bytes.

At the SCE> prompt, enter the **show interface linecard 0 counters VAS-traffic-bandwidth** command and press **Enter**.

Example

```
SCE> show interface linecard 0 counters VAS-traffic-bandwidth

Traffic sent to VAS processing TxBW [Kbps] (bytes are counted from Layer 2):

Port 1    Port 2    Port 3    Port 4
--------  --------  --------  --------
VAS server id 0:         0         0         0         0
VAS server id 1:         0         0         0         0
VAS server id 2:         0         0         0         0
VAS server id 3:         0         0         0         0
VAS server id 4:         0         0         0         0
VAS server id 5:         0         0         0         0
VAS server id 6:         0         0         0         0
VAS server id 7:         0         0         0         0
Traffic after VAS processing TxBW [Kbps] (bytes are counted from Layer 2):

Port 1    Port 2    Port 3    Port 4
--------  --------  --------  --------
VAS server id 0:         0         0         0         0
VAS server id 1:         0         0         0         0
VAS server id 2:         0         0         0         0
VAS server id 3:         0         0         0         0
VAS server id 4:         0         0         0         0
VAS server id 5:         0         0         0         0
VAS server id 6:         0         0         0         0
VAS server id 7:         0         0         0         0
```

VAS Configuration Example

Revised: March 17, 2015

Configuration Examples for VAS

Following is an example illustrating the steps in configuring VAS traffic forwarding, first on the SCE platform and then from the SCA BB Console. This example shows how to configure one VAS group. This group will forward traffic to VAS servers for content filtering.

Configuring the SCE Platform

In configuring the SCE platform for VAS traffic forwarding, the purpose of the traffic forwarding is irrelevant. It is only necessary to know how many servers there are, how many server groups, and which servers should be assigned to which groups.

	Command	Purpose
Step 1	enable 15	Access the root level to configure the pseudo IP address.
Step 2	**configure** **interface range GigabitEthernet 3/0/0-1**	Enter Gigabit Ethernet Interface configuration mode for the relevant range of GBE interfaces.
Step 3	**pseudo-ip** *1.1.1.1 255.255.255.252*	Configure the pseudo IP address for the health check.
Step 4	exit **interface linecard 0**	Enter Interface Linecard configuration mode.
Step 5	**shutdown**	Shutdown the line card when configuring VAS servers and groups.
Step 6	**VAS-traffic-forwarding**	Set the SCE platform to forward VAS traffic (enable VAS traffic forwarding).
Step 7	**VAS-traffic-forwarding traffic-link** *link-0*	Set the VAS traffic forwarding link to link-0.
Step 8	**VAS-traffic-forwarding VAS server-id** *0* **VLAN** *600* **VAS-traffic-forwarding VAS server-id** *1* **VLAN** *601* **VAS-traffic-forwarding VAS server-id** *2* **VLAN** *602*	Assign VAS servers 0 to 2 to VLAN 600 to 602 respectively.

	Command	Purpose
Step 9	**VAS-traffic-forwarding VAS server-group** *0* **server-id** *0* **VAS-traffic-forwarding VAS server-group** *0* **server-id** *1* **VAS-traffic-forwarding VAS server-group** *0* **server-id** *2*	Map VAS servers to server group 0, allowing server redundancy within the group.
Step 10	**VAS-traffic-forwarding VAS server-id** *0* **health-check UDP ports source** *63154* **destination** *63155* **VAS-traffic-forwarding VAS server-id** *1* **health-check UDP ports source** *63156* **destination** *63157* **VAS-traffic-forwarding VAS server-id** *2* **health-check UDP ports source** *63158* **destination** *63159*	Define UDP ports for health check on VAS servers.
Step 11	**VAS-traffic-forwarding VAS server-group** *0* **failure minimum-active-servers** *2*	Configure the minimum number of servers required.
Step 12	**VAS-traffic-forwarding VAS server-group** *0* **failure action block**	Configure the failure action to “block”.
Step 13	**no shutdown**	Restart the line card.

Configuring the SCA BB Application for VAS Traffic Forwarding

After the SCE platform has been configured, open the SCA BB console to configure VAS traffic forwarding in the SCA BB application. While configuring the SCA BB application for VAS traffic forwarding, the purpose of the traffic forwarding is relevant. So, assign meaningful names to the VAS server groups and traffic forwarding tables.

This example illustrates how to configure the SCA BB application to forward traffic for content filtering. The VAS server group and the traffic forwarding table are both named ‘Content Filtering’. A package is created, named ‘VAS Package’, and the Content Filtering table is assigned to that package.

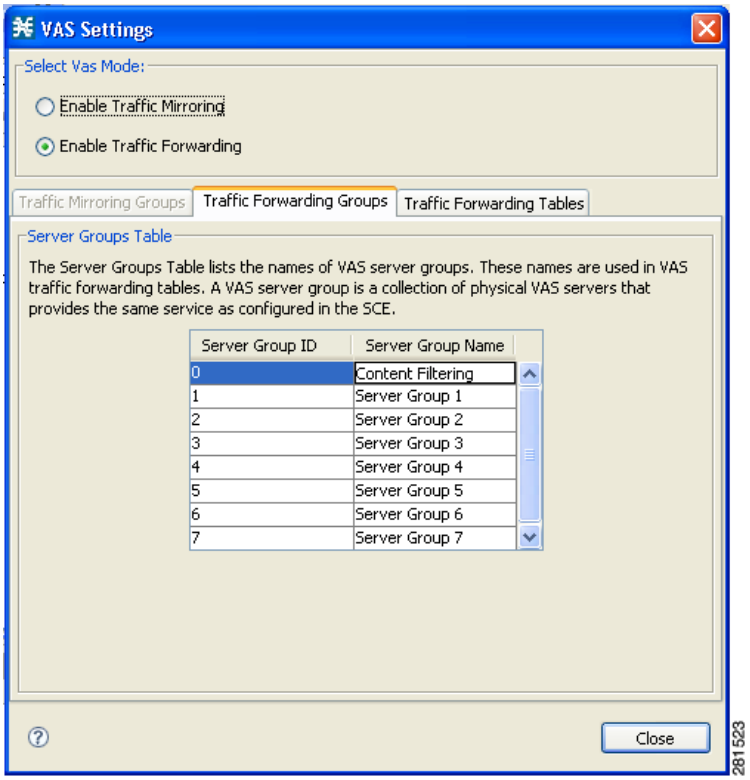
See Chapter 1, “Configuring the SCA BB Application to Support VAS Traffic Forwarding” for a full description of the steps provided in this section.

To configure VAS traffic forwarding in the SCA BB application, complete the following steps:

Step 1 Enable VAS in SCA BB.

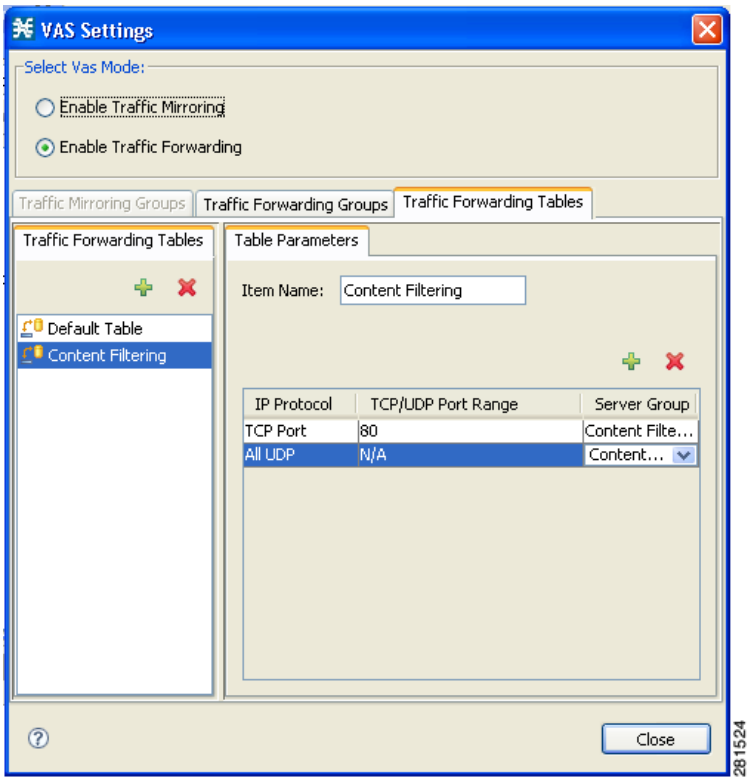
Step 2 Rename the VAS server group to “Content Filtering”.

Figure 1-1 Renaming the Traffic Forwarding Group



Step 3 Create and configure the “Content Filtering” VAS forwarding table.

Figure 1-2 Configuring the VAS Forwarding Table



Step 4 Create the “VAS Package” package and assign the “Content Filtering” VAS forwarding table to it.

Figure 1-3 Assigning the VAS Forwarding Table to a Package