CISCO SERVICE CONTROL SOLUTION GUIDE

Cisco Service Control Online Advertising Solution Guide: Behavioral Profile Creation Using Traffic Mirroring, Release 5.0.x

Note This document supports all 5.0.x releases.

1 Overview

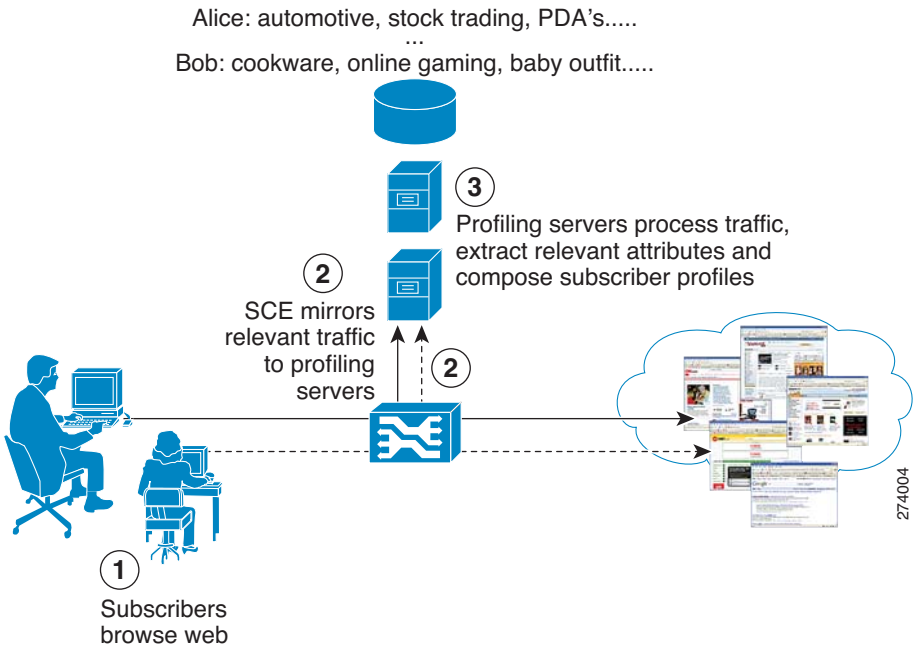
Online Behavioral Targeting is an online advertising approach that involves presenting users with advertisements based on their interests, as deduced by monitoring their web browsing preferences. The Cisco Service Control Engine (Cisco SCE) platform can enable online behavioral targeting based on an analysis of subscriber online usage patterns.

Such behavioral targeting does not require the analysis of each and every HTTP request on the line, because this would result in a lot of excess information. The Cisco SCE platform performs the first level of analysis in the behavioral targeting chain by inspecting the user browsing sessions, detecting the particular requests that are triggered by the actual user browsing (these events are termed ClickStream), and mirroring the traffic pertaining to these events. (Mirroring criteria may be different, depending on actual need.) The mirrored traffic is typically received by an entity that analyzes the nature of usage and creates a profile of the subscriber to be used later for targeting. The way the greater solution works is outside the scope of this document.

The mirroring capability on its own is useful for a number of other solutions that use the Cisco SCE platform. Although the mirroring solution focuses on the behavioral targeting, the description of the mirroring capability and related configuration is also applicable for such solutions.

Figure 1 illustrates the high-level overview of a mirroring-based behavioral targeting solution.

Figure 1 High-Level Overview of a Mirroring-Based Behavioral Targeting Solution



The mirroring decision can be taken based on a number of criteria. In fact, the mirroring decision can be triggered based on each of the criteria that are used by the Cisco Service Control Application for Broadband (Cisco SCA BB) for classification of traffic.

One such example is traffic mirroring of HTTP traffic that is based on ClickStream. ClickStream detection is a fundamental capability of the solution, because it can detect which specific requests, out of the enormous number of HTTP requests generated throughout the subscriber web activity, were triggered by the subscriber. When a subscriber clicks a link, or enters a URL in the browser address bar, an HTTP request is generated for this URL. Typically, an HTML page is returned, which constitutes the outline of the contents requested. For the browser to be able to render this page, it must download multiple objects (tens or sometimes around a hundred for a single page viewed), which in turn results in multiple HTTP requests for obtaining these objects.

To conduct behavioral targeting, it is sufficient to understand what the user was trying to do (represented by the initial request, such as biz.publisher.com/ap/081120/world_markets.html > global markets), rather than looking at each object downloaded as a secondary result of such a request (such as: http://ads.adnetwork.com/a/a/in/interbroke/300x250_yah.jpg > broker ad).

ClickStream detection makes exactly this distinction and reduces the number of requests being analyzed, which is necessary to enable a scalable analysis solution. At same time, no data is provided about what the subscriber is actually doing.

Traffic that has been designated to be mirrored is replicated by the Cisco SCE platform and sent over a designated VLAN and a designated pair of ports towards the listening servers.

The Cisco SCE platform supports multiple logical destinations for mirroring, each of which can be represented by one or more VLANs, which are load-shared by the Cisco SCE platform. Load sharing ensures that all the traffic of a given subscriber belonging to a particular server group is handled by the same VLAN.

Mirroring of a flow can continue indefinitely (until the flow is terminated) or can be limited to a predefined volume passed over the flow, after which the mirroring is stopped.

The impact of traffic mirroring on overall system performance depends on the actual percentage of traffic that is mirrored. We recommend monitoring Cisco SCE performance when enabling traffic mirroring.

2 Configuring Traffic Mirroring Support: Highlights

This section provides the highlights of configuring the main components of traffic mirroring on the Cisco SCE platform. For complete configuration details, see the "Configuring an SCE Platform for Traffic Mirroring" section on page 9.

Defining the Mirroring Server Groups

The mirrored traffic can be sent to one of eight possible server groups. These are server groups rather than individual servers, because the underlying infrastructure allows load-sharing the traffic destined to a server group across multiple VLANs.

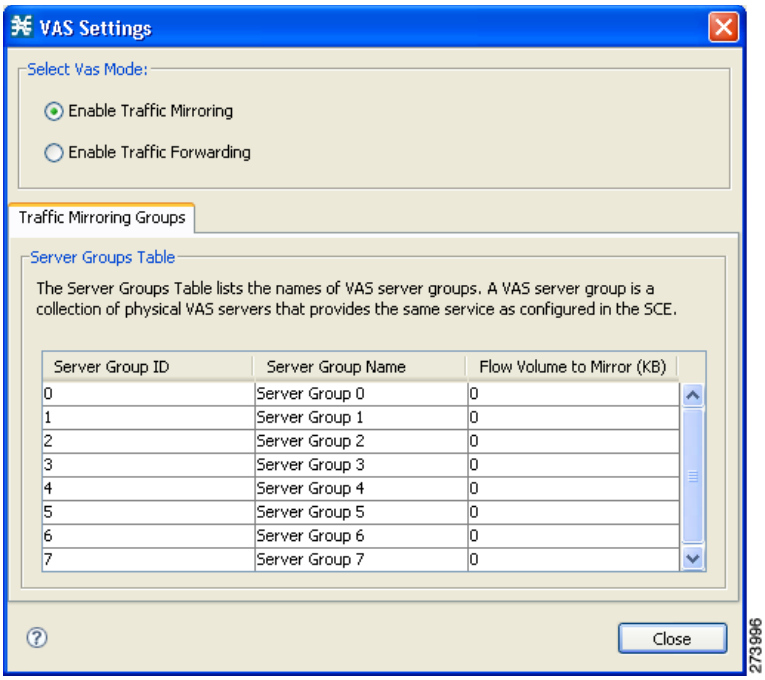
These server groups are defined on the Policies tab of the Service Configuration Editor. Click **Configuration** and select **VAS Settings**.

Click the top radio button for traffic mirroring, and then define the names of the server groups you use. Enable the server group IDs to define the transport setting for the solution later on.

For each server group, you can specify the flow volume (in Layer 3 kilobytes) to mirror to the server. If left at 0 (the default), the entire flow is mirrored. Otherwise, mirroring is stopped after the specified volume has been mirrored.

Define the mirroring server groups in the VAS Settings window (see Figure 2).

Figure 2 VAS Settings



Creating a ClickStream Service

Note Classifying traffic as ClickStream is one way of identifying traffic to be mirrored. Other approaches may involve classification based on other attributes, such as the URL matching a certain prefix or a user agent. This section is relevant when ClickStream is the criterion for traffic mirroring.

ClickStream signatures are mapped by default to the HTTP Browsing protocol and consequently to the browsing service. To be able to act on them separately, first move them to a protocol of their own, then assign this protocol to a service of its own.

Figure 3 and Figure 4 represents two Cisco SCA BB GUIs to configure the ClickStream Protocol.

Figure 3 Configuring the ClickStream Protocol

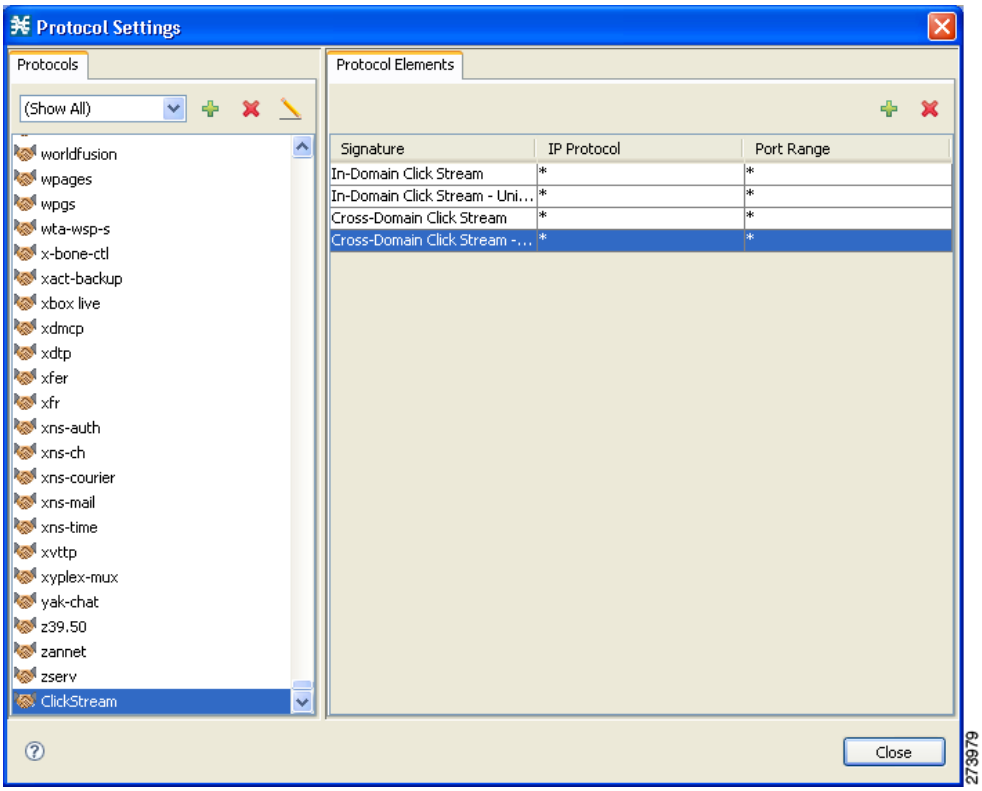
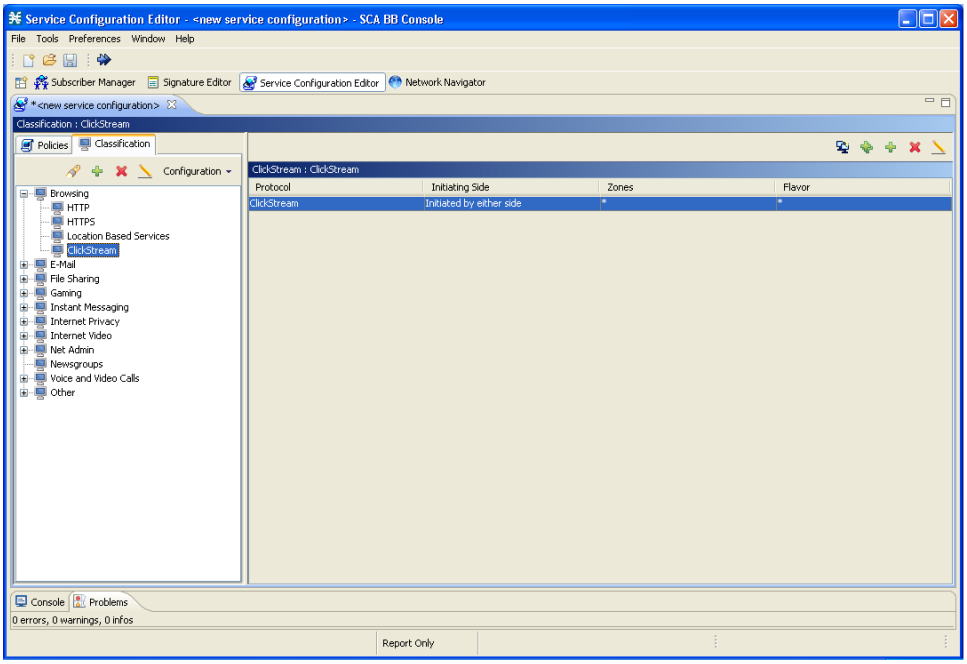


Figure 4 Configuring the ClickStream Service



Enabling Deep HTTP Inspection

To enable comprehensive detection of the ClickStream events in the traffic stream, it is important to enable deep inspection of HTTP, which configures the Cisco SCE platform to analyze and classify all HTTP requests within a single flow.

Some browsers, in conjunction with some web server implementations, use the same TCP flow to carry multiple requests triggered by clicks that target the same host. Such events are not detected if the classification is done only at the beginning of the flow (which is the default for Cisco SCA BB).

To enable deep HTTP inspection, in the SCA BB Console Service Configuration Editor, choose **Configuration > System Settings > Advanced Options** tab **> Advanced Service Configuration Options.**

Note Enabling deep HTTP inspection impacts the Cisco SCE performance because of the excessive processing associated with it, the actual figure depending on the amount, and the nature of HTTP traffic. We recommend that you monitor SCE platform performance when enabling this capability.

Creating Traffic Mirroring Rules

The traffic to be mirrored is defined by creating traffic rules that specify the mirroring action for the relevant traffic.

As a prerequisite, you must create a service that includes the type of traffic to be mirrored. This can be either the ClickStream service, or any other service defined through the Cisco SCA BB service configuration.

For each package with traffic to be mirrored, select the relevant service and activate mirroring to the proper server (that you have already configured using the VAS Settings window, see the"Defining the Mirroring Server Groups" section on page 3). The mirroring action is not exclusive, and you can configure it in parallel with other actions that need to be applied to the same service.

Note Leveraging subscriber awareness with traffic mirroring: Subscriber awareness is key to behavioral targeting using traffic mirroring, because it enables a network level opt-in or opt-out, a feature that is considered important to subscriber privacy. This is implemented using the SCE platform native subscriber awareness. The Cisco SCE creates packages that allow or deny traffic mirroring, and assigns subscribers to these packages based on their opted-in or opted-out nature.

Cisco SCE Connectivity

Any change required in this section?

Traffic mirroring is implemented by sending the mirrored packets over a designated VLAN through a predefined link of the Cisco SCE platform. The link that has been defined for traffic mirroring can be either used exclusively for this purpose, or it can be one of the traffic ports, in which case the Tx capacity of the link is shared between the original egress traffic and the mirrored traffic.

Traffic that is received on the subscriber interface on either link is sent over a VLAN on the network interface over this predefined link. Traffic that is received on the network interface on either link is sent over a VLAN on the subscriber interface over this predefined link.

Figure 5 shows an Cisco SCE 10000 platform using a dedicated link for mirroring.

Figure 5 Traffic Mirroring on a Dedicated Link

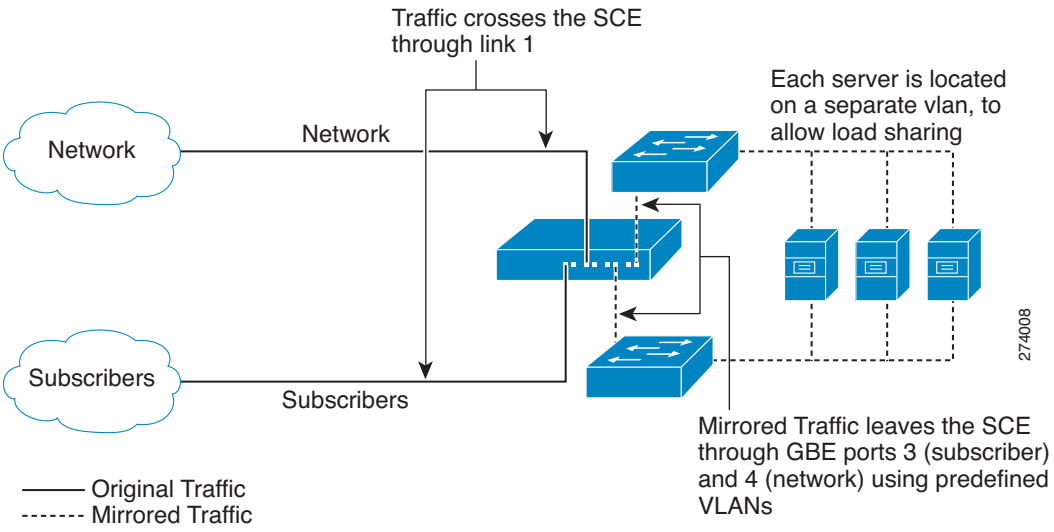
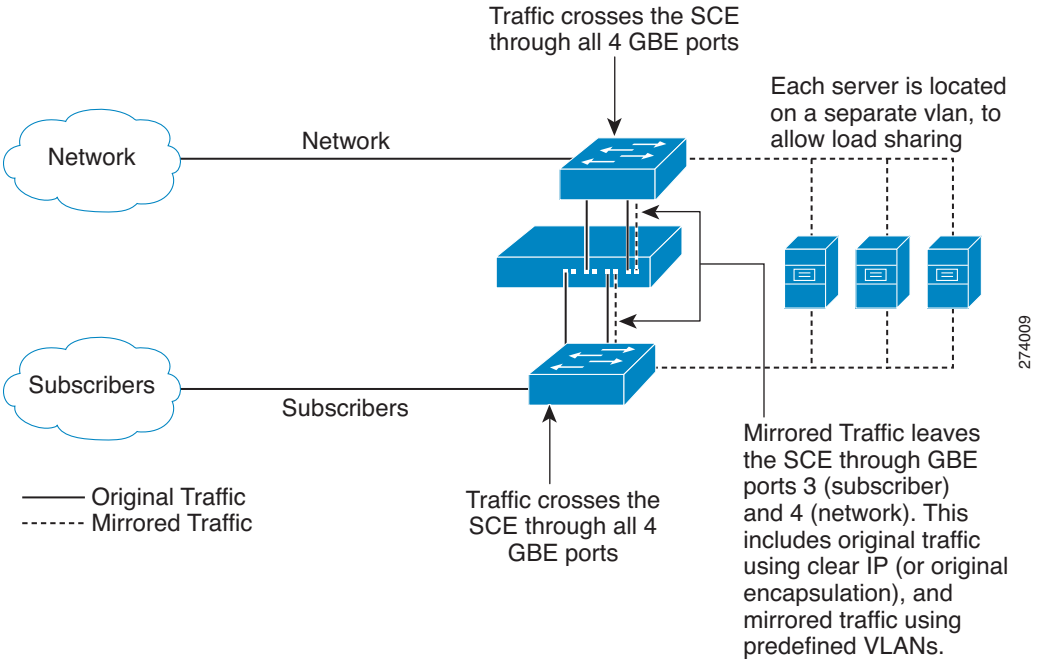


Figure 6 shows a Cisco SCE 10000 platform using traffic ports for mirroring.

Figure 6 Traffic Mirroring over Traffic Ports



Configuring Traffic Mirroring Transport

Traffic mirroring transport is configured by using the Cisco SCE platform CLI, and connects between the logical mapping to server groups, as defined through the Cisco SCA BB console, and the actual transmission of mirrored traffic, which is done over a VLAN.

You do this by defining physical servers that are mapped to VLANs, and associating these servers to server groups (which have been defined through the Cisco SCA BB console).

To configure the link over which traffic is mirrored, use this CLI command:

SCE10000(config if)# **VAS-traffic-forwarding traffic-link {link-0|link-1}**

To view the link over which traffic is mirrored, use this CLI command:

SCE10000# **show interface linecard 0 VAS-traffic-forwarding**

The server assigned to this traffic by the policy selects the VLAN to send the traffic over. One or more VLANs can be associated with each server, and the Cisco SCE platform load-shares the traffic destined to each server between these VLANs. Load sharing is done at the subscriber level (all traffic belonging to a specific subscriber is transmitted on the same VLAN). Up to 64 distinct VLANs can be supported by an SCE10000 platform.

To configure a VLAN to be used for a particular server, use this CLI command in linecard interface configuration mode:

SCE10000(config if)# **VAS-traffic-forwarding VAS server-id** *number* **VLAN** *vlan-id*

To view VLANs that are used for a particular server, use this CLI command:

SCE10000# **show interface linecard 0 VAS-traffic-forwarding VAS server-id** *id-number*

To remove VLAN from a particular server, use this CLI command in linecard interface configuration mode:

SCE10000(config if)# **no VAS-traffic-forwarding VAS server-id** *number* **VLAN** *vlan-id*

To associate a server with a server group, use this CLI command in linecard interface configuration mode):

SCE10000(config if)# **VAS-traffic-forwarding VAS server-group** *group-number* **server-id** *id-number*

Mirrored Traffic: The Server Side

The listening server should be aware of few assumptions about mirrored traffic.

Start Mirroring

Mirroring starts after the flow has been classified and matched to a service by the Cisco SCE platform. For TCP flows, this typically (but not always) happens on the first payload packet. As a result, the entire TCP handshake is not mirrored.

Mirroring of ACK Only Packets

ACK only packets (or more generically, packets with no payload at all) are not mirrored. Although this should not affect the ability of a server to process the traffic, packets that were on the original data flow may be missing. RST and FIN packets are exceptions to this rule. For more information, see the "Mirroring of Connection Termination" section on page 8.

Mirroring of Connection Termination

- For connections that have been terminated in an orderly fashion—Only the last FIN and ACK packets are mirrored.
- For connections that have been terminated by using RST—Only the RST packet is mirrored.
- For connections that for some reason have not been terminated—No connection termination indication is sent.

Stop Mirroring Indication

When the Cisco SCE platform stops mirroring a flow because the specified volume has already been mirrored, it generates an RST packet over the mirrored VLAN, to indicate that mirroring has stopped for this flow.

Traffic Encapsulation

Mirrored traffic is encapsulated in a VLAN based on the VLAN number that has been assigned to that particular subscriber by the SCE platform.

If the traffic is originally encapsulated in a VLAN, an Cisco SCE 10000 removes the original VLAN and inserts the mirroring VLAN instead.

For all other types of encapsulation, the original packet is encapsulated in a VLAN as it is.

3 Configuring an SCE Platform for Traffic Mirroring

This section explains in detail how to configure a system for traffic mirroring.

- To configure a solution that mirrors ClickStream traffic, complete all the steps.
- To configure a solution that does not mirror ClickStream traffic, skip to Step 22. (Steps 1 through 21 define the ClickStream traffic that is required only if mirroring is used.)

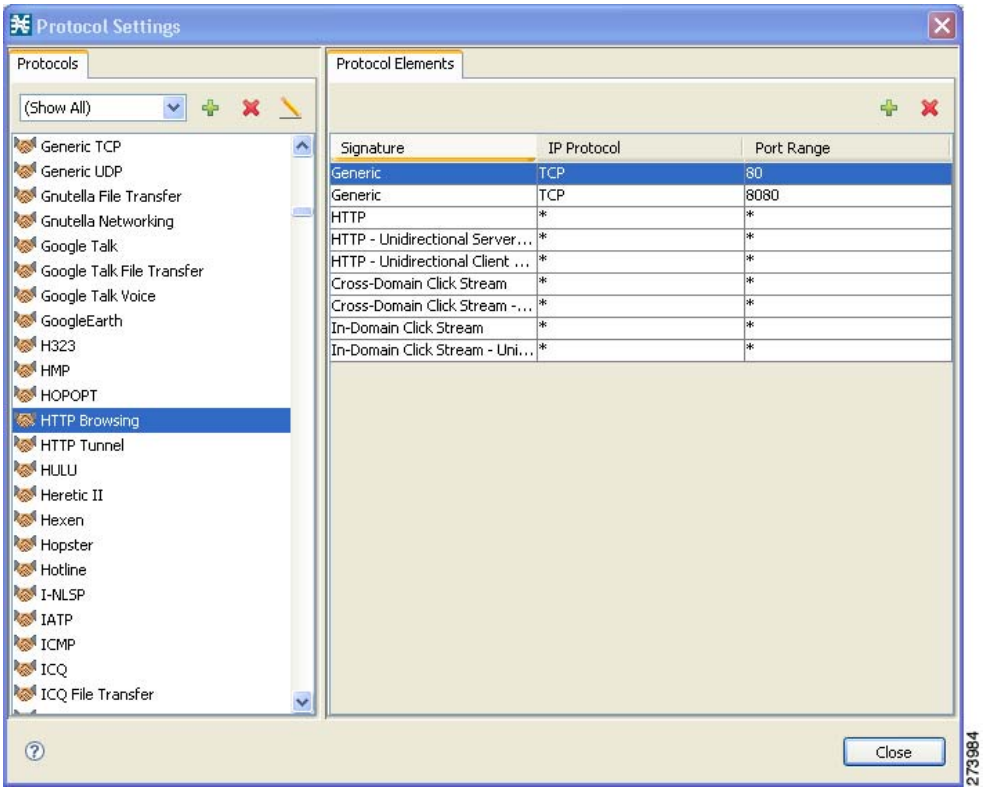
Step 1 In the Cisco SCA BB Policy Editor, click the **Classification** tab (left pane), click **Configuration,** and select **Protocols**.

Step 2 In the Protocol Settings window (see Figure 7), select the **HTTP Browsing** service.

Step 3 On the **Protocol Elements** tab, remove the ClickStream-related protocol elements:

- In-Domain Click Stream
- In-Domain Click Stream - Unidirectional Client Request
- Cross-Domain Click Stream
- Cross-Domain Click Stream - Unidirectional Client Request

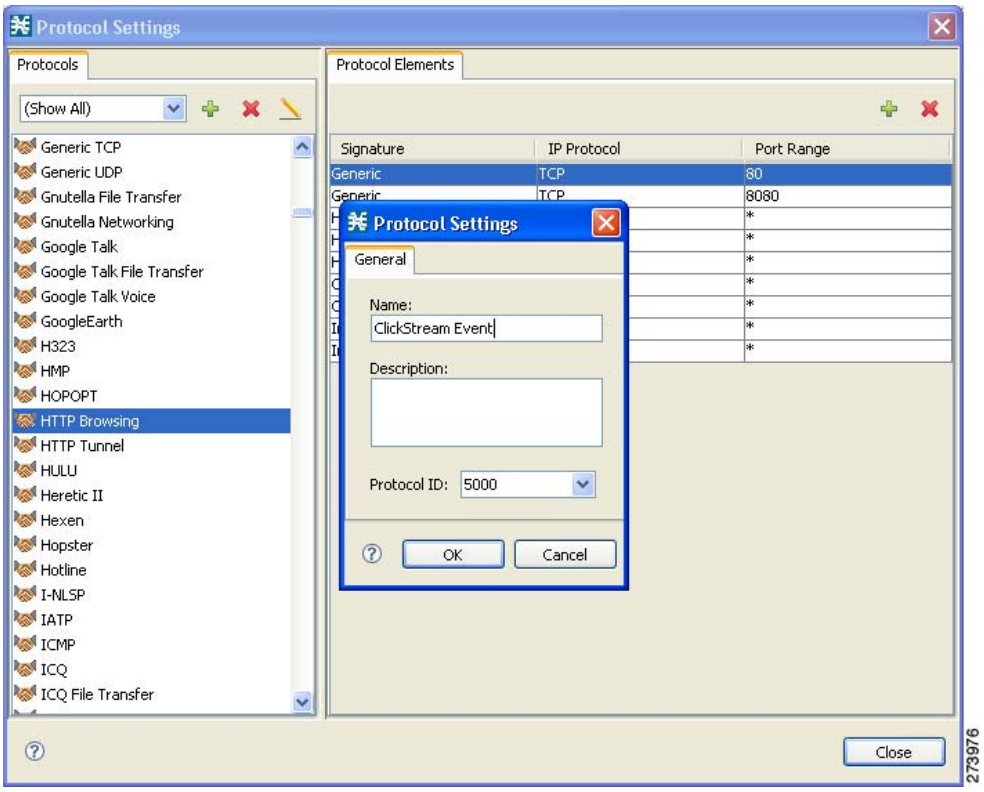
Figure 7 Protocol Settings Window



Step 4 In the Protocol Settings window, on the Protocols tab, click the Add (**+**) icon to add a new protocol.

Step 5 Enter the name for the new protocol **ClickStream Event**, and click **OK** (see Figure 8).

Figure 8 Protocol Settings Window—Protocol Name

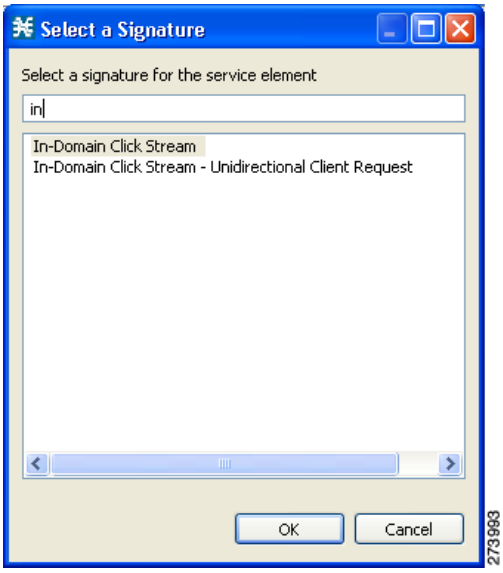


Step 6 In the Protocol Elements tab, click the Add (**+**) icon to add protocol elements to the ClickStream Protocol.

Step 7 For the new protocol element created, click the "**...**" button in the Signature column.

Step 8 On the Select a Signature window (see Figure 9), add the **In-Domain Click Stream** signature, and click **OK**.

Figure 9 Select a Signature Window



Step 9 Repeat Step 6 through Step 8 for the rest of the ClickStream signatures:

- In-Domain Click Stream - Unidirectional Client Request
- Cross-Domain Click Stream

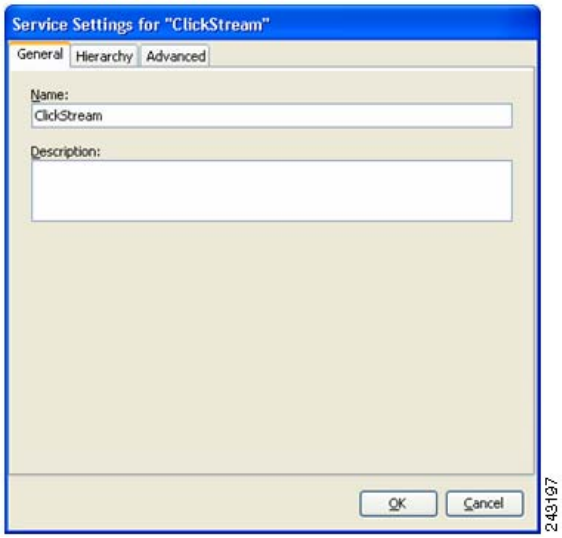
- Cross-Domain Click Stream - Unidirectional Client Request

Step 10 On the Cisco SCA BB Policy Editor, click the **Classification** tab (left pane), and highlight the **Browsing** service

Step 11 Click the Add (**+**) icon to add a new service under the **Browsing** service.

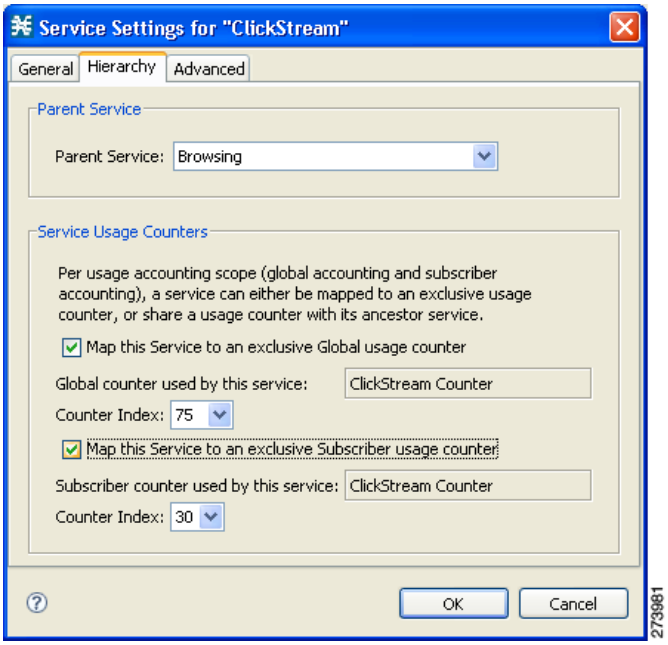
Step 12 Name the service **ClickStream** (or any other name you choose) (see Figure 10).

Figure 10 Service Settings Window



Step 13 Click the **Hierarchy** tab (see Figure 11) and check the two check boxes to add a dedicated service counter to the ClickStream Service.

Figure 11 Hierarchy Tab

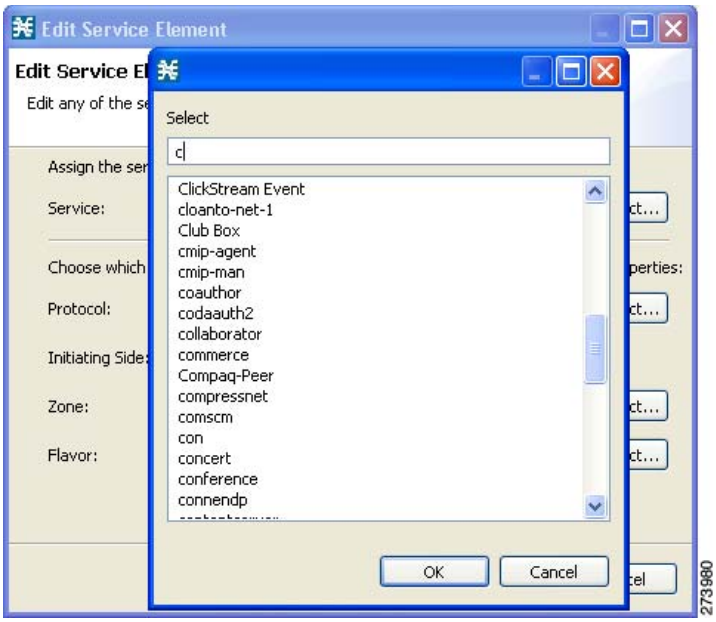


Step 14 Click **OK**.

Step 15 In the right pane, click the Add (**+**) icon to add a service element.

Step 16 In the dialog box that opens, click **Select** next to the Protocol field and select the **ClickStream Event** protocol (or whatever you named your ClickStream protocol) from the list (see Figure 12).

Figure 12 Edit Service Element Window—Select Protocol



Step 17 Click **OK**.

Step 18 On the Policies tab of the Service Configuration Editor, choose:

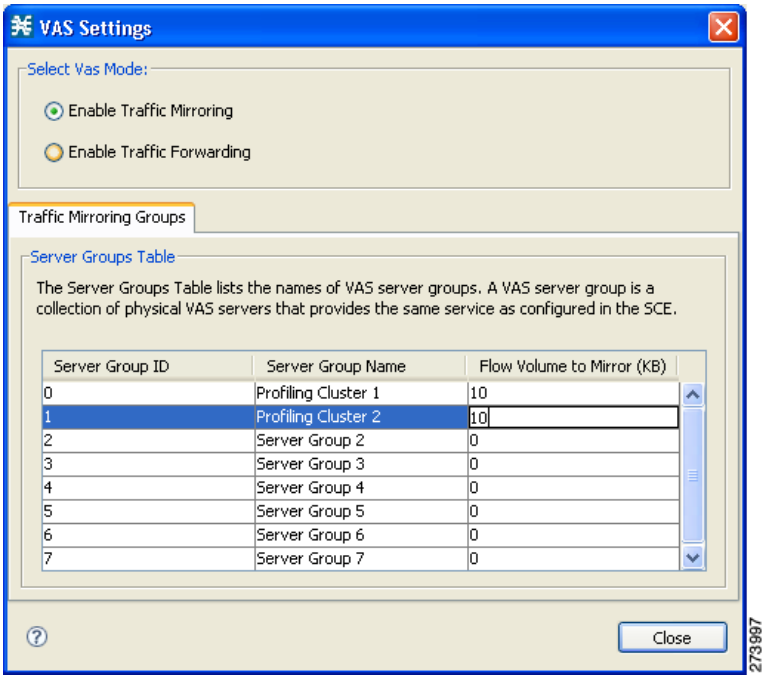
Configuration >VAS settings

Step 19 Click the **Enable Traffic Mirroring** radio button.

Step 20 In the lower part of the window, define a name for each of the server groups you use.

Step 21 For each server group, define the per-flow volume (in KB) to be mirrored to this group (for flows matching the criteria). Leaving the value 0 allows the entire flow to be mirrored (see Figure 13).

Figure 13 VAS Settings Window

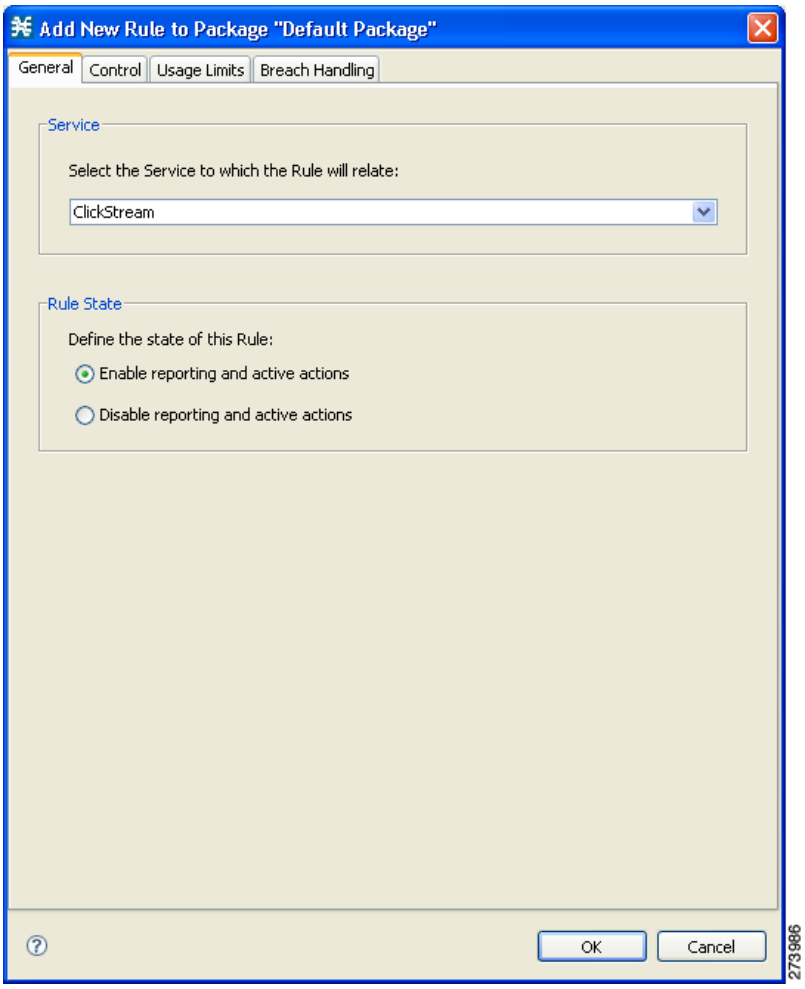


Step 22 In the Cisco SCA BB Policy Editor, click the **Policies** tab (left pane), and then select the package for which to mirror the traffic.

Step 23 In the right pane, click the Add (**+**) icon to add the ClickStream service (or any other service whose traffic is to be mirrored).

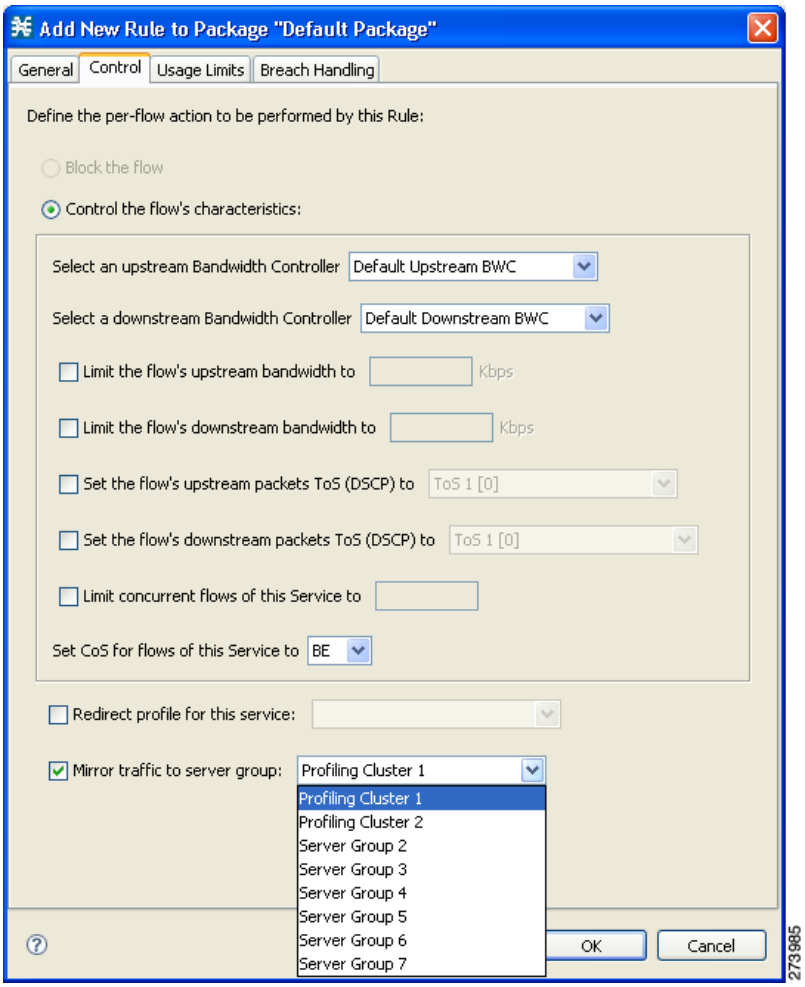
Step 24 In the window that opens, select **ClickStream** (or any other service) from the drop-down list (see Figure 14).

Figure 14 Add New Rule to Package Window—General Tab



Step 25 Click the **Control** tab and check the **Mirror Traffic to Server Group** check box. From the associated drop-down list, select the server group to which to mirror the traffic to (see Figure 15).

Figure 15 Add New Rule to Package Window—Control Tab



Step 26 Click **OK**.

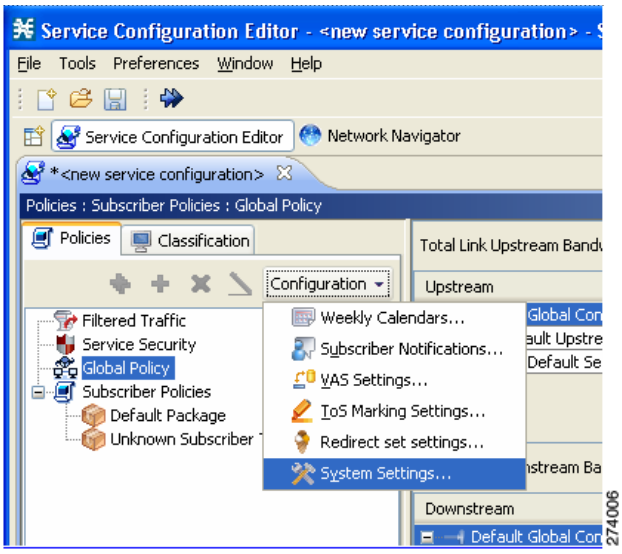
Step 27 Repeat Step 23 through Step 26 for all the services in the selected package that require traffic mirroring.

Step 28 Repeat Step 22 through Step 27 for all the packages that require traffic mirroring.

Step 29 (Optional) Enable deep HTTP inspection. This allows the mirroring decision to be taken for each HTTP request within a flow separately.

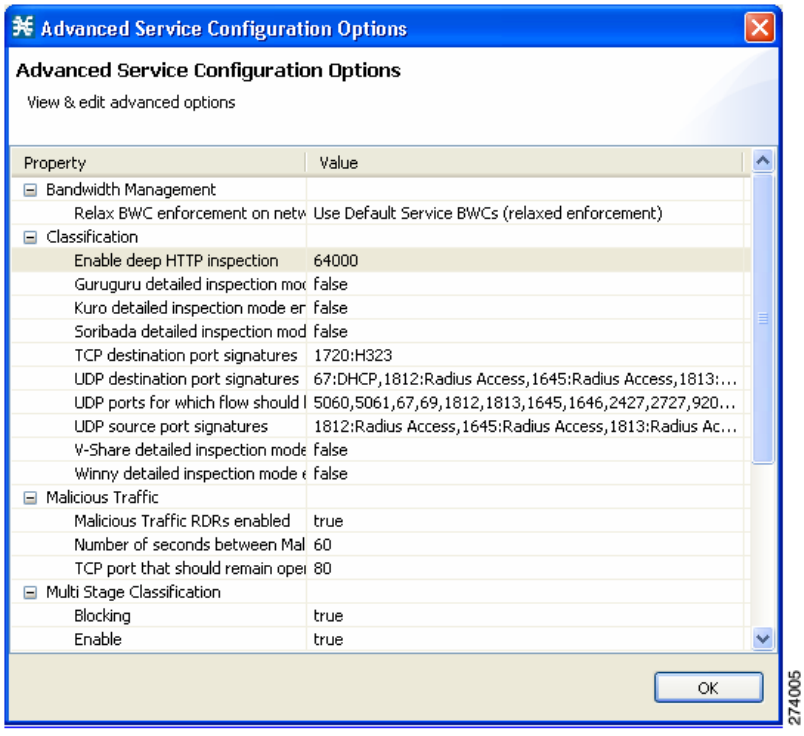
a. Choose **Policies > Configuration > System Settings** (see Figure 16).

Figure 16 Service Configuration Editor—Policies > Configuration > System Settings



b. On the Advanced Options tab, click **Advanced Service Configuration Options** to enable deep inspection of HTTP flows by setting the highlighted value to **64000.** This selection enables the analysis of multiple transactions within a single HTTP flow, which is important for comprehensive detection of ClickStream events (see Figure 17).

Figure 17 Advanced Service Configuration Options Window



This concludes the policy editing part of the configuration.

Step 30 Apply the Service Configuration to the SCE platform.

Step 31 Configure the link to be used for traffic mirroring on the SCE platform using this command:

```
SCE10000(config if)# VAS-traffic-forwarding traffic-link {link-0 |link-1}
```

Step 32 Configure a VLAN tag for each physical VAS server using this command:

```
SCE10000(config)# VAS-traffic-forwarding VAS server-id number VLAN number
```

Step 33 Assign each server to a server group using this command:

```
SCE10000(config)# VAS-traffic-forwarding VAS server-group number server-id number
```

Step 34 Save the configuration using this command:

```
SCE10000# copy running-config-all startup-config-all
```

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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**.