CISCO SERVICE CONTROL SOLUTION GUIDE

Cisco Service Control URL Blacklisting Solution Guide, Release 3.5.5

Revised: January 20, 2011, OL-17972-06

1 Managing URL Blacklists Using the SCE Platform

The SCE platform-managed URL database is a URL database that resides in the SCE platform and is managed via CLI commands rather than being managed by the SCA BB Console. In addition to the advantage of having a separate URL database that is configurable directly by CLI commands, this database can be used to hide a list of URLs so that they are not accessible by the Console or the CLI.

The database must be declared as a separate flavor in the SCA BB application, but all other configuration and management is performed using the CLI.

The database can be protected. When the sce-url-database is protected, one user is designated as the owner of the database and only that user can execute any CLI commands on the database. This requires defining the AAA authorization method (either based on local users or based on a TACACS+ server, etc.) and defining at least one user to be the owner of the database. For further details see the "Configuring the Management Interface and Security" chapter in the *Cisco SCE8000 10GBE Software Configuration Guide* or the "Configuring the Management Interface and Security" chapter in the *Cisco SCE8000 GBE Software Configuration Guide*.

If the database is defined to be protected, none of the database information (including the owner, the database entries, and the authorization information itself) is accessible to any users, including the relevant saved configuration in the log files and in the relevant SCA BB reports. The database owner user may change the authorizations using the CLI; however, when any of the protections are relaxed (or all of the protections are relaxed by removing the protections entirely) the database is reset.

In order to ensure the secrecy of the database information, the database entries may be imported to the SCE (using the CLI) in an encrypted form using 128-bit key length AES. The key may be set or updated using the appropriate CLI command; typically, this command should be run over a secure Telnet session.

There are two general categories of CLI commands related to the SCE managed URL database:

- User authorization commands
- Database management commands

2 Configuring User Authorization

The sce-url-database is managed by a single authorized user, who is the designated owner of the sce-url-database.

- When there is no designated owner, the sce-url-database is unprotected and the contents can be read and modified by any user.
- When there is a designated owner, the sce-url-database is protected. The default protection settings are as follows:
  - Read permission—no-user. This setting is not configurable
  - Write permission—owner-only. The owner can configure this setting to all-users.
  - Lookup permission—no-user. The owner can configure this setting to owner-only.
  - Encryption key—no key. The owner can configure an encryption key.

User Authorization Guidelines:

- The default user cannot be the owner.
- Only the owner can configure the protection settings. If there is no owner, the database is unprotected and any user has read and write permission. A user may be configured to be the owner of the database only while no owner user is designated for the database.

- When any protection setting is relaxed, the database is reset. Protection is relaxed in the following cases:
  - Protection is removed completely using the **no sce-url-database protection** command.
  - Write permission is changed from owner-only to all-users.
  - Lookup permission is changed from no-user to owner-only.
- The sce-url-database configuration information is not accessible as part of the running config and startup config files.
  - Protected information is not displayed when a **show** or **more** command is executed on the config files.
  - Protected information is included when a **copy** command is executed on the config files.

How to specify a new owner of the sce-url-database

sce-url-database protection owner (**myself** | (**name** *user-name*))

Command Mode—Interface LineCard Configuration

Authorization Level—Admin

Prerequisite

If there is currently an owner assigned to the sce-url-database, that owner must first remove the owner designation using the **no sce-url-database protection** command, which removes all DB protection (see How to remove all sce-url-database protection, page 5).

Options:

- **myself**—The owner of the DB is the user who is currently logged in. Cannot be logged in under the default username.
- *user-name*—The user name to be assigned as the owner of the DB. Cannot be the default username. Note that in this case, if no such user exists (either in the local database or in the Tacacs+ server) or the AAA authorization is not configured accordingly (that is, the logic user), there is no effective way of utilizing this owner user's permissions. Once the relevant user or AAA settings are configured, the owner user's permissions are effective accordingly.

Default:

no owner

Results

- The specified user is the owner of the sce-url-database.
- Read of the sce-url-database is not permitted for any user (including the owner).
- No RDRs or traps will contain data of these URLs.
- By default, only the owner has Write permission to the sce-url-database.
- By default, Lookup is not permitted for any user (including the owner).

How to configure the sce-url-database write-protection

This command can be executed only by the assigned owner of the sce-url-database.

sce-url-database protection allow-write (all-users | owner-only)

Command Mode—Interface LineCard Configuration

Authorization Level—Admin

Prerequisite

Assign an owner to the sce-url-database.

Options:

- all-users
- owner-only

Result

If protections are relaxed (changed from owner-only to all-users), the sce-url-database is reset.

Default:

- If no owner has been assigned, the default is **all-users.**
- If an owner has been assigned, the default is **owner-only.**

How to configure the sce-url-database lookup-protection

This command can be executed only by the assigned owner of the sce-url-database.

sce-url-database protection allow-lookup (owner-only | no-user)

Command Mode—Interface LineCard Configuration

Authorization Level—Admin

Prerequisite

Assign an owner to the sce-url-database.

Options:

- owner-only
- no-user

Results

If protections are relaxed (changed from no-user to owner-only), the sce-url-database is reset.

Default:

- If no owner has been assigned, the default is **all-users**.
- If an owner has been assigned, the default is **no-user**.

How to configure the sce-url-database encryption key

This command can be executed only by the assigned owner of the sce-url-database.

sce-url-database protection encryption-key *encryption-key*

Command Mode—Interface LineCard Configuration

Authorization Level—Admin

Prerequisite

Assign an owner to the sce-url-database.

Options:

- *encryption-key*—The AES encryption key (128 bits long). The key is supplied in hexadecimal format and is 32, 48, or 64 hexadecimal digits respectively.

Default:

no encryption key

Removing the Encryption Key

no sce-url-database protection encryption-key

No other sce-url-database protection settings are changed by this command.

Note:

When you change the encryption key of the sce-url-database, the following message may appear on the CLI:

Due to changes in security settings existing protection database is being removed.

For example:

```
SCE8000(config if)#>do show int 1 0 sce-url-database num-entries
14 entries found
SCE8000(config if)#>sce-url-database protection encryption-key 3c24d0924706e5498c7c415954e9ba70
Due to changes in security settings existing protection database is being removed
SCE8000(config if)#>do show int 1 0 sce-url-database num-entries
14 entries found
```

You can ignore this message.

How to remove all sce-url-database protection

This command can be executed only by the assigned owner of the sce-url-database.

no sce-url-database protection

Command Mode—Interface LineCard Configuration

Authorization Level—Admin

Prerequisite

Assign an owner to the sce-url-database.

Results

- Removes all the sce-url-database protections and resets the sce-url-database
- Reverts to default protection settings:
  - no designated owner user
  - no protections
  - no encryption key.

How to view the current sce-url-database protection settings

show interface linecard 0 sce-url-database protection

Command Mode—User Exec

Authorization Level—Viewer

Results

Displays the following information:

- owner username
- current protection settings
- whether a key is configured

Sample Output

```
SCE>show interface linecard 0 sce-url-database protection
Protection Domain BLACK_LIST_DOMAIN Status:
Domain owner:black
Read is allowed to no user
Write is allowed to user black only
Lookup is allowed to no user
Encryption key is not set
```

3 Managing the sce-url-database

The designated owner of the sce-url-database can do the following:

- import the list of URLs from a sce-url-database file
- add a single entry to the sce-url-database
- clear the sce-url-database
- lookup a specific URL (unless lookup protection is set to no-user)

If write protection is set to all-users, any user can do the following:

- import the list of URLs from a sce-url-database file
- add a single entry to the sce-url-database
- clear the sce-url-database

If there is no designated owner (and therefore no protection), any user can do the following:

- display a listing of the entire sce-url-database

  If there is a designated owner, the contents of the sce-url-database are protected and cannot be displayed.

Guidelines for Managing the sce-url-database

- When a new file is imported, the existing database is cleared before the import. Incremental update is not supported. Therefore the import file must contain all the relevant URLs, not only new ones to be added to the database.
- Note also that the import operation ensures zero downtime regarding the protected URL blacklisting. The previous list of URLs remains in effect throughout the import operation and then, once the new list of URLs (from the imported file) has been fully imported, it takes immediate effect instead of the previous list.
- Add a large number of new URLs by importing an updated sce-url-database file. Typically, if the database is protected this option is used with an encrypted file.
- Add a few new URLs by adding the new URLs using the **sce-url-database add-entry** command.

sce-url-database Import File

The database import file may be either contain cleartext or be encrypted. If the file is encrypted, the matching encryption key must be configured by the database owner.

If the file is encrypted, it must be prefixed with a cleartext header. The encrypted file header must be exactly as follows:

Encrypted file version: 0x01

Block cipher index: 0x01

Mode of operation index: 0x02

Padder index: 0x02

IV length: 0x10

IV: *<16 unformatted bytes which form the128 bits IV of the encrypted data >*

Following the header, the following data should appear in AES 128, CFB mode, encrypted format:

A random number (in the range [16…31]) of random bytes, followed by the word "Signed", and then again 32 random bytes.

Each following line represents a single URL.

sce-url-database Import File Format

[Flavor <tab>] URL

Where:

- Flavor: Flavor-id. The flavor ID must either be included for every line in the file or none of the lines. The flavor must be separated from the URL by a <tab>.

- URL: (* | [*] [Host-Suffix] | [*] [Host-Suffix] / [URL-Prefix [*]] [URL suffix] [? Params-prefix])
  Refer to Table 1 for URL examples.

Table 1 Examples for Defining URLs

URL Input	Lut Key Output	Result
*	*:*:*:*	blocks all URLs
*.com	*.com:*:*:*	blocks all URLs in which the host ends with .com
*/media	*:/media:*:*	blocks all URLs in which the path contains only media
*/media*mp3	*:/media*:*mp3:*	blocks all URLs in which the path starts with media and ends with mp3
/?key	*:/*:*:key*	blocks all URLs in which the parameters start with key
*.com/media*mp4?download	*.com:/media*:*mp4:download*	blocks all URLs in which: • the host ends with .com • the path starts with media and ends with mp4 • the parameters start with download

How to import the sce-url-database file

See sce-url-database Import File, page 6 for the required format of the sce-url-database import file.

If the import file does not contain the flavor, you must specify the flavor in the CLI command. The specified flavor must be the one that was designated for the black list in the pqb file that was applied, other wise the operation will fail.

sce-url-database import cleartext-file | encrypted-file *file-name* **flavor-id** *flavor-id*

If the import file does contain the flavor, you may not specify the flavor in the CLI command.

sce-url-database import cleartext-file | encrypted-file *file-name*

Command Mode—Interface LineCard Configuration

Authorization Level—Admin

Prerequisite

The user executing the command must have write permission for the sce-url-database.

Options:

- cleartext-file
- **encrypted-file**—An encrypted file may be imported only if a matching encryption key has been configured.
- *file-name*—Path and filename of the sce-url-database import file.
- *flavor-id*—The flavor is applied to all entries in the file.

Default:

sce-url-database is empty

Results

- The sce-url-database is first cleared.
- The entries from the file are written to the database.
- Duplicate keys in the file are overwritten with no warning.
- In case of a failure, writing continues to the next entry.
  The total number of failures and a listing of the failed file line numbers are reported when the import is finished.

- If the sce-url-database import file has a problem (for example, the file does not contain a flavor ID), the import procedure stops and does not proceed further. This may also result in an empty LUT.

  For example:

```
SCE8000(config if)#>do show int 1 0 sce-url num-entries
14 entries found
SCE8000(config if)#><k:vk@64.103.125.217/c:/NirTemp/enc/URLONLY2E.CSV
Error - Line 1 can not be parsed. Flavor-id is not found, it wasn't supplied through CLI
Error - Operation aborted.
SCE8000(config if)#>do show int 1 0 sce-url num-entries
No entries found
```

How to add an entry to the sce-url-database

sce-url-database add-entry url-wildcard *URL-wildcard-format* **flavor-id** *flavor-id*

Command Mode—Interface LineCard Configuration

Authorization Level—Admin

Prerequisite

The user executing the command must have write permission for the sce-url-database.

Options:

- *URL-wildcard-format*:

  URL: (* | [*] [Host-Suffix] | [*] [Host-Suffix] / [URL-Prefix [*]] [URL suffix] [? Params-prefix])

  See Table 1 for examples of how to define the URL.
- *flavor-id*—Decimal number representing the Flavor. flavor-id is required when adding a single entry.

How to view the sce-url-database

show interface linecard 0 sce-url-database all-entries

Command Mode—Privileged Exec

Authorization Level—Admin

Prerequisite

The sce-url-database must have all protection removed and no assigned owner. If there is an assigned owner, the database is protected and cannot be displayed.

How to look for a specific URL in the sce-url-database

show interface linecard 0 sce-url-database url *url*

Command Mode—Privileged Exec

Authorization Level—Admin

Prerequisite

The user executing the command must have lookup permission for the sce-url-database.

Options:

- *url*—Specific URL to lookup in the sce-url-database.

Results

- If the specified URL exists, the flavor index is returned.
- If you are trying to lookup a URL on a database for which you are not the owner, you might get a message that the URL does not exist; even if the URL exists.

How to clear the sce-url-database

sce-url-database remove-all

Command Mode—Interface LineCard Configuration

Authorization Level—Admin

Prerequisite

The user executing the command must have write permission for the sce-url-database.

4 Enabling Deep HTTP Inspection

Since the HTTP flows may be composed of multiple transactions, typically you would require that each such inner URL be verified against the protected URL database (and not only the initial one). However, since this has a performance impact such deep HTTP inspection is disabled by default.

You can enable deep HTTP inspection option from the SCA BB console. The actual configuration relates to the number of HTTP transactions that are examined per HTTP flow (Number of HTTP GET detections). By default, only the first transaction is examined; you may define it to be any number of transactions between 1 and 65,535 .

Note It is recommended that you monitor SCE platform performance when deep HTTP inspection is enabled, as enabling this functionality may result in performance degradation.

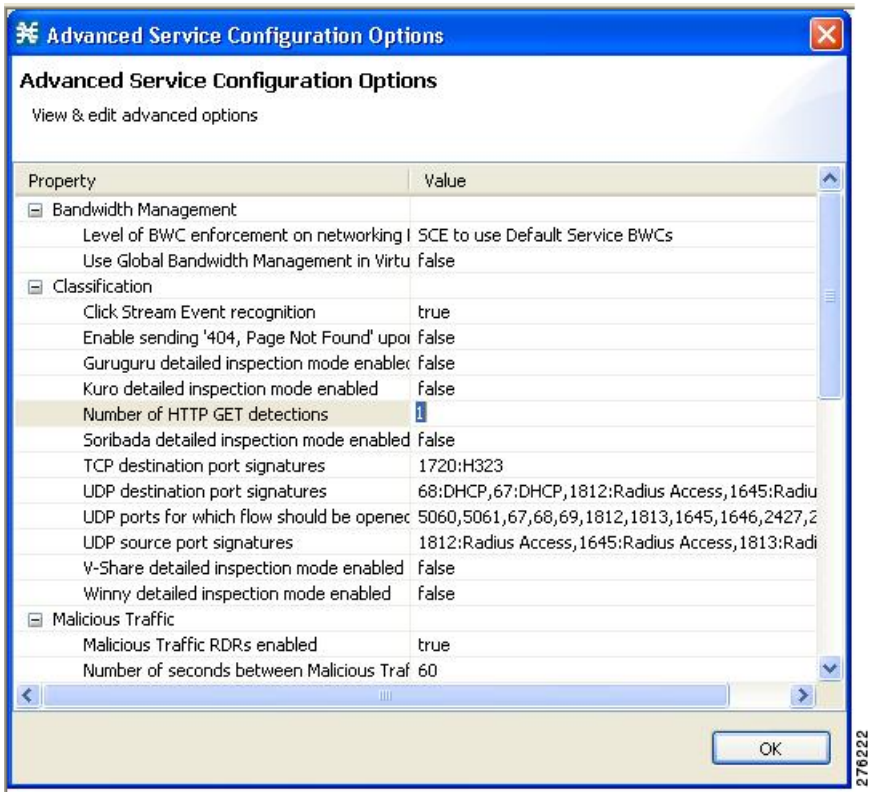
How to Enable Deep HTTP Inspection

Step 1 In the SCA BB Console Service Configuration Editor, go to:

Configuration > System Settings > Advanced Options > Advanced Service Configuration Options

The Advanced Service Configuration Options window opens as shown in Figure 1.

Figure 1 Advanced Service Configuration Options Window



Step 2 On the Advance Services Configuration Options window, in the **Number of HTTP GET detections** field, type in the number of HTTP transactions to examine per HTTP flow (1 — 65,535).

5 URL Normalization

URL normalization is a procedure that brings URL flavors with exactly the same meaning into canonical presentation, which minimizes the number of false-negative lookup results and may significantly improve the efficiency of the protected blacklisting operation.

URL normalization refers to two issues:

- percent encoding
- case sensitiveness

By default these normalization operations are disabled, but when enabling URL normalization, both of them are in effect for the protected blacklist.

You must first enable URL normalization and then import the Blacklist entries so that they are affected accordingly.

Configuring URL Normalization

Use the URL normalization commands to do the following:

- Globally enable URL normalization
- Globally disable URL normalization (default)
- Set URL normalization to the default state (disabled)
- Display the currently configured state of URL normalization

URL normalization should be configured before the Service Configuration (PQB file) is applied to the SCE platform and before loading the sce-url-database.

How to Enable URL Normalization

lookup canonical

Command Mode—Interface LineCard Configuration

Authorization Level—Root

How to Disable URL Normalization

no lookup canonical

Command Mode—Interface LineCard Configuration

Authorization Level—Root

How to Reset URL Normalization to the Default State

By default, URL normalization is disabled.

no lookup canonical

Command Mode—Interface LineCard Configuration

Authorization Level—Root

How to Display the Currently URL Normalization Configuration

show applications slot 0 lookup canonical

Command Mode—User Exec

Authorization Level—Viewer

Sample Output

```
SCE>show applications slot 0 lookup canonical
Normalization of lookup entries is enabled
```

6 Protected URL Database Configuration Example

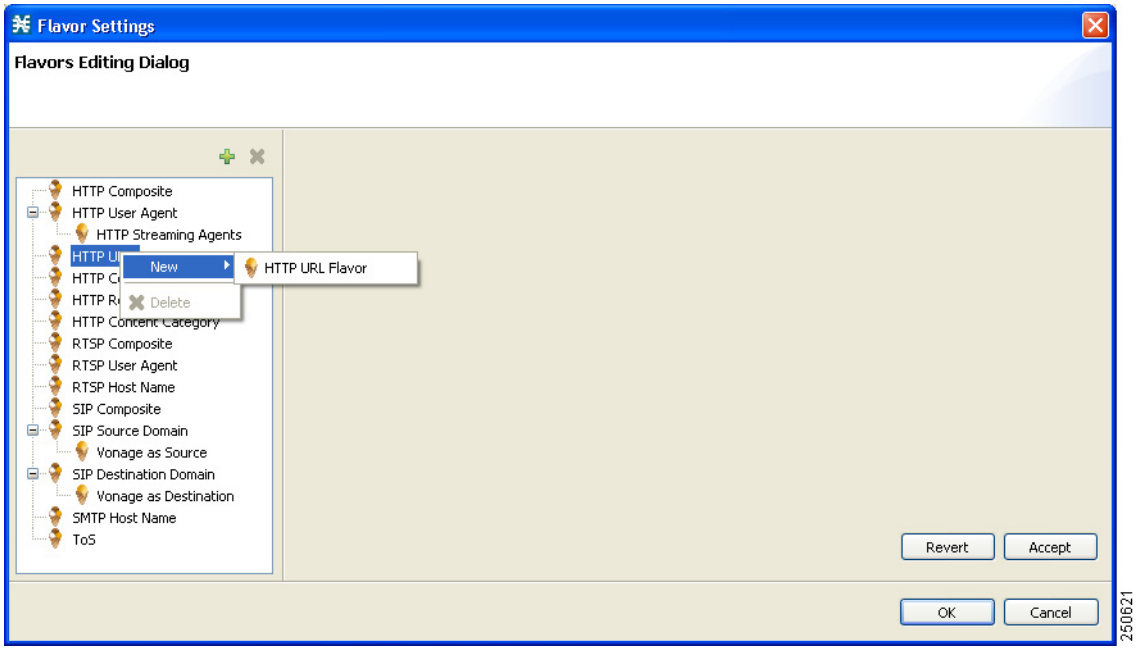
The following example shows how to configure the protected URL database, including defining the flavor in the SCA BB console, configuring the protections in the SCE platform and importing a URL file.

Step 1 Enable URL normalization.

```
>enable 15
#>configure
(config)#>interface LineCard 0
(config if)#>lookup canonical
```

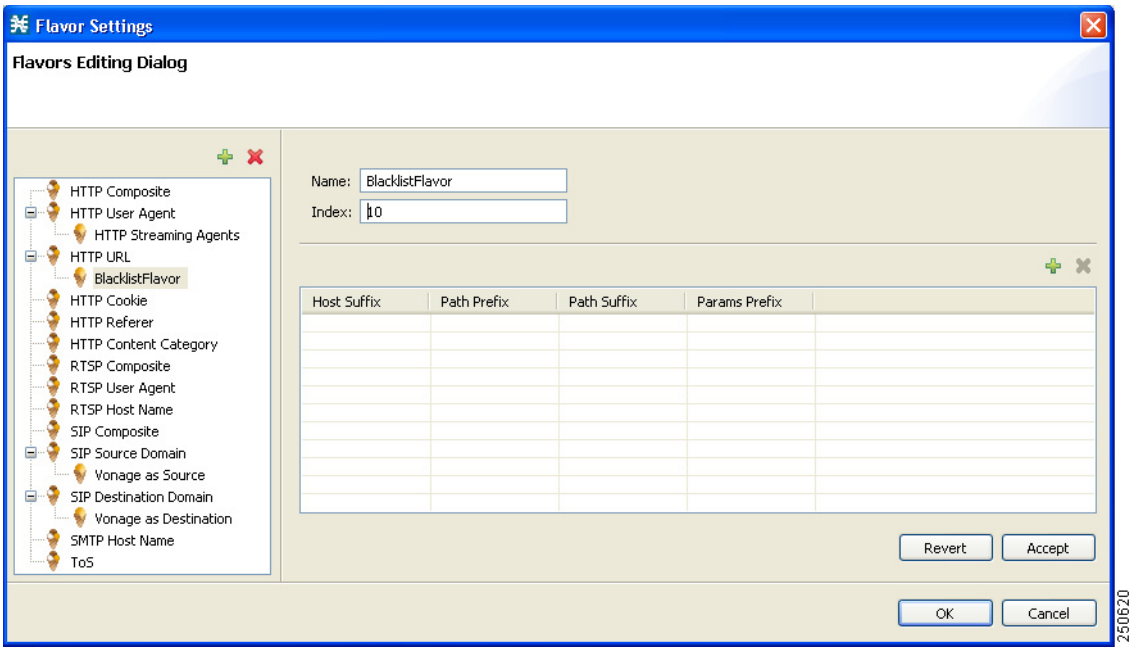
Step 2 From the Flavor Settings window, right-click HTTP URL and choose **New > HTTP URL Flavor** (Figure 2).

Figure 2 Flavor Settings Window—Flavors Editing Dialog



Step 3 Enter a Name and Index as required (Figure 3).

Figure 3 Flavor Settings Window—Flavors Editing Dialog with Name and Index Information



Note The Index number is the flavor-id that is required by a number of CLI commands.

Step 4 Click **OK**.

Step 5 Define a Service that uses the new Flavor.

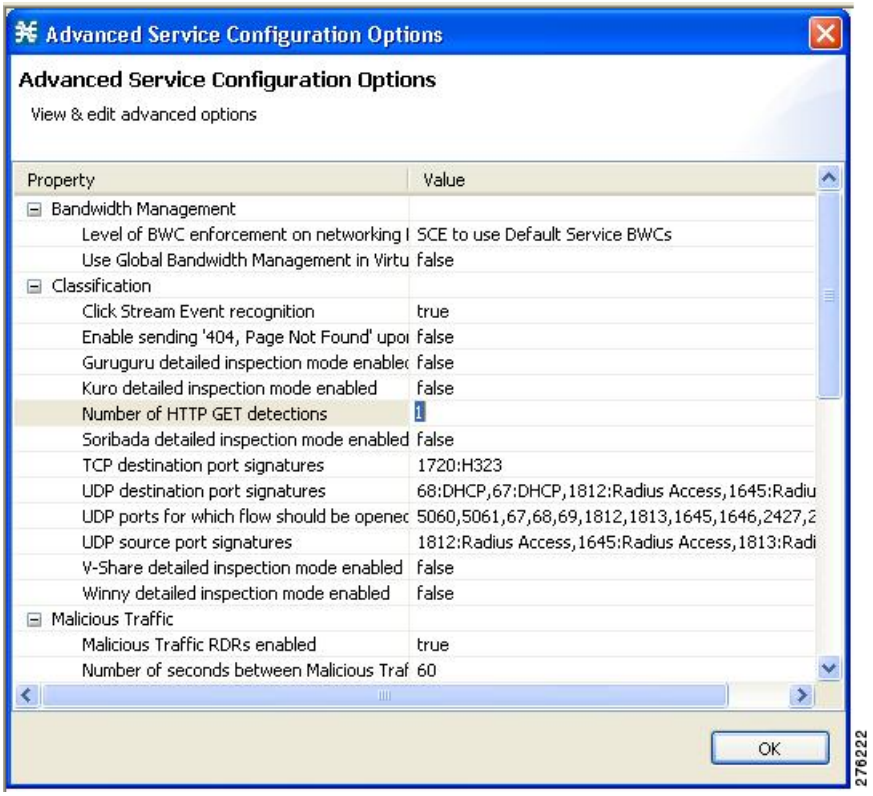
Step 6 Specify the number of HTTP GET detections.

In the Service Configuration Editor, go to:

Configuration>System Settings>Advanced Options tab**>Advanced Service Configuration Options.**

The Advanced Service Configuration Options window opens as shown in Figure 4.

Figure 4 Advanced Service Configuration Options Window



In the Advance Services Configuration Options screen, in the **Number of HTTP GET detections** field, type in the number of HTTP transactions to examine per HTTP flow (1 — 65,535).

Step 7 Apply the service configuration to the SCE.

Step 8 Define the SCE to require user login and define the special owner user:

```
#configure
(config)#aaa authentication login default local enable none
(config)#username BlacklistOwner privilege 10 password pass
```

Step 9 Login as the owner user:

```
User Access Verification
Username: BlacklistOwner
Password:
```

Step 10 Set the owner of the sce-url-database:

```
#configure
(config)#interface LineCard 0
(config if)#sce-url-database protection owner myself
```

Step 11 (Optional) Allow all users to update the database:

```
(config if)#sce-url-database protection allow-write all-users
```

Step 12 (Optional) Allow the owner to perform lookup on the database:

```
(config if)#sce-url-database protection allow-lookup owner-only
```

Step 13 Define an encryption key to be used when importing an encrypted URLs file:

This is typically done periodically over a secure Telnet session.

```
(config if)#sce-url-database protection encryption-key AABBCCDDEEFF11223344556677889900
```

Step 14 Import an encrypted (according to the key defined in Step 11) file containing the required URLs for the relevant flavor ID:

This is typically done periodically; either first copy the file to the SCE or import directly over FTP.

```
(config if)#sce-url-database import encrypted-file urls.csv flavor-id 10
```

Step 15 Save the configuration:

```
(config if)#>ex
(config)#>ex
#>copy running-config-all startup-config-all
Writing general configuration file to temporary location...
Backing-up general configuration file...
Copy temporary file to final location...
Writing general (protected) configuration file to temporary location...
Backing-up general (protected) configuration file...
Copy temporary (protected) file to final location...
Writing general configuration file to temporary location...
Removing old application configuration file...
Renaming temporary application configuration file with the final file's name...
Writing general (protected) configuration file to temporary location...
Removing old application (protected) configuration file...
Renaming temporary application (protected) configuration file with the final file's name...
```

Step 16 Logout to prevent unauthorized users from manipulating the protected database:

```
#logout
```

7 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.

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**.

OL-17972-06