Content Filtering Database Support for URL Classification

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• GGSN • HA • PDSN • P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - License Required
Related Changes in This Release	Not Applicable
Related Documentation	• *CF Administration Guide* • *Command Line Interface Reference* • *Content Classification Manager Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.4

Feature Description

The Content Filtering feature that is supported on Cisco ASR 5500 and Cisco Virtual Platforms previously used Static Rating Categorization Database (SRDB), a third-party database, for URL classification and reputation scores. With Release 21.4, database support is extended to include the new Content Classification Manager (CCM) product for content filtering. This section covers the Content Filtering enhancements implemented in support of CCM.

Content Classification Manager uses the functionality provided by Cisco Talos Security Intelligence. For more information about Cisco Talos Security Intelligence, refer to https://talosintelligence.com/.

Note

- For more information regarding Content Filtering, refer to the "Content Filtering Support Overview" chapter in this guide (*CF Administration Guide*).
- For more information about CCM, refer to the *Content Classification Manager Administration Guide*.

How It Works

Content Filtering is implemented using the Session Manager. One Content Classification Manager category database and its Talos Security Intelligence (TSI) daemon is present per card (complex). The Session Manager queries the database for URL categorization. A category is returned asynchronously and the Session Manager applies the corresponding action (Redirect, Discard, and so on) as per the Content Filtering policy.

Note The TSI daemon and database reside only on data plane cards, that is, DPC and DPC2 on ASR 5500, SF on DI, and SI.

Session Managers already had a query and response interface with SRDB Manager. Now, the TSI database has replaced the Rulespace/Symantec database along with the control elements (like MCRDBS, WEM). For a Session Manager, except for the query interface that has changed, the response to a category request to TSI database remains unchanged (it is similar to the SRDB response).

The following sections briefly describe the Content Filtering Manager, Categories, and Session Manager integration.

Content Filtering Manager

The Content Filtering (TSI) Manager tasks (cfmgr) run in the data-plane cards. The Content Filtering (TSI) Controller (cfctrl) starts the process when it (Controller) is configured and the update directory is ready. The

manager process is responsible for starting and recovering the TSI daemon and SAS (TSI module) and managing database updates with the TSI daemon and SAS.

Categories

The Content Filtering library maintains a static enumeration of verdict types.

ECS also maintains a static enumeration of category IDs. The URL query result from SAS is the assigned category ID. The Content Filtering library maps this ID to the ECS ID (if known). If there is no mapping (if the category is new), the SAS category ID is passed through as unmapped to the Session Manager's query.

For more information, refer to the "Category-based Content Filtering Subsystem" section in the *"Content Filtering Support Overview"* chapter in the *CF Administration Guide*.

Session Manager Integration

1. **URL Query:** Based on the query, URL-based categorization is processed for HTTP and WTP and WSP requests. If the Content Filtering is enabled and operational, the Session Manager initiates a URL categorization query. Else, queries are not made and the default behavior of content filtering is applied.
2. **Query Response:** As a response to the query, the category received in the verdict is converted to ASR 5500 understandable category. The rest of the processing occurs as it did with the SRDB.

Configuring Content Filtering Database Support for URL Classification

Content Filtering Database Support for URL Classification functionality requires a valid license be applied to the StarOS system. Contact your Cisco Account Representative for more information. The commands listed in the following sections are not visible unless a valid license is present. See the *System Administration Guide* for more details about managing and applying licenses.

Example Configuration

The following example shows the steps to configure a connection with the Content Classification Manager and enable URL categorization.

```
configure
  security
    server talos-intelligence my-server
      ip 1.1.1.1 port 5341
      sftp port 2222 username my-username password my-password
    exit
    category server my-server
    end
```

Important The Content Classification Manager IP address port number must be 5341, and the SFTP server port number must be 2222.

To verify your Content Classification Manager is operational, execute the following command: **show security server talos-intelligence my-server**.

The "State" information listed in the output should show something other than "NOT RUNNING".

Monitoring and Troubleshooting

This section provides information regarding show commands and/or their outputs in support of this feature.

Show Commands and/or Outputs

The output of the following CLI commands is enhanced in support of this feature:

show active-charging content-filtering category statistics

The output of the above command now includes the following values for the “Time taken for rating” field:

- 50-100ms
- 100-200ms
- 200-300ms
- 300ms

This show command excludes the statistics for the following fields:

- Total number of successful Cache lookups
- Time taken for rating: > 50ms

These fields are removed because in TSI, the Session Manager does not maintain any cache internally. A cache is present in the TSI Daemon.

```
show active-charging content-filtering category statistics
Service Name: ACS

  Cumulative Content Filtering Statistics:
      Flows discarded:                0 Flows redirected:             0
      Flows allowed:                  0 Flows terminated:             1
      Flows discarded with content insertion:                         0
      Total Flows blocked:                                            1
      Total number of static DB lookups:                              1
      Total number of successful Cache lookups:                       0
      Total number of unknown URLs:                                   0
      Failure Action (Rating Attempts Not Completed):
        Flows discarded:              0 Flows redirected:             0
        Flows allowed:                0 Flows terminated:             0
        Flows discarded with content insertion:                       0
        Total Flows blocked:                                          0

      Time taken for rating      Number of URLs
      0-5ms                             0
      5-10ms                            0
      10-15ms                           0
      15-20ms                           1
      20-25ms                           0
      25-30ms                           0
```

```
    30-35ms                          0
    35-40ms                          0
    40-45ms                          0
    45-50ms                          0
    50-100ms                         0
    100-200ms                        0
    200-300ms                        0
    > 300ms                          0
    Attempts not completed           0
```

A similar change can be seen in the output of the following CLIs:

- show active-charging content-filtering category statistics verbose
- show active-charging content-filtering category statistics rulebase all
- show active-charging content-filtering category statistics rulebase all verbose
- show active-charging content-filtering category statistics rulebase name
- show active-charging content-filtering category statistics rulebase name verbose

show active-charging content-filtering category statistics debug-only

The output of the above command now includes the following values for the “Time taken for rating” field:

- 50-100ms
- 100-200ms
- 200-300ms
- 300ms

This show command excludes the statistics for the following fields:

- Total number of successful Cache lookups
- Number of URLs(CACHE)
- Time taken for rating: > 50ms

```
show active-charging content-filtering category statistics debug-only
Service Name: ACS

  Cumulative Content Filtering Statistics:
      Flows discarded:                0 Flows redirected:             0
      Flows allowed:                  0 Flows terminated:             1
      Flows discarded with content insertion:                         0
      Total Flows blocked:                                            1
      Total number of static DB lookups:                              1
      Total number of unknown URLs:                                   0
      Failure Action (Rating Attempts Not Completed):
        Flows discarded:              0 Flows redirected:             0
        Flows allowed:                0 Flows terminated:             0
        Flows discarded with content insertion:                       0
        Total Flows blocked:                                          0

      Time taken for rating      Number of URLs
      0-5ms                               0
      5-10ms                              0
      10-15ms                             1
```

```
      15-20ms                              0
      20-25ms                              0
      25-30ms                              0
      30-35ms                              0
      35-40ms                              0
      40-45ms                              0
      45-50ms                              0
      50-100ms                             0
      100-200ms                            0
      200-300ms                            0
      > 300ms                              0
      Attempts not completed               0
      Memblock Failure                   0
1
```

A similar change can be seen in the output of the following CLIs:

- show active-charging content-filtering category statistics debug-only
- show active-charging content-filtering category statistics rulebase all debug-only
- show active-charging content-filtering category statistics rulebase name debug-only

System Logs

Two event logging facilities are provided to control the level of events logged for this feature:

- **cfctrl**: Content filtering controller logging facility
- **cfmgr**: Content filtering manager logging facility

See the *System Logs* chapter of the *System Administration Guide* for information about event logging.