ICAP Interface Support

This chapter provides information on configuring the external Active Content Filtering servers for a core network service subscriber. This chapter also describes the configuration and commands that are used to implement this feature.

It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in respective product Administration Guide, before using the procedures in this chapter.

The following products currently support ICAP interface functionality:

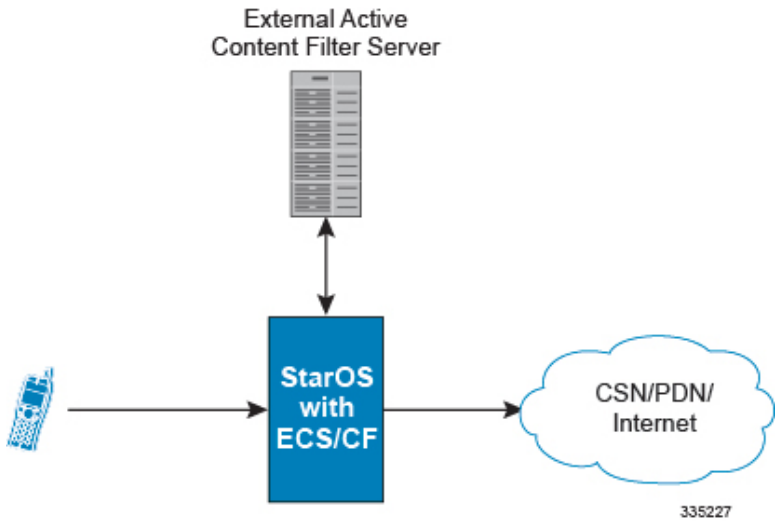
- GGSN
- P-GW

ICAP Interface Support Overview

This feature supports streamlined ICAP interface to leverage Deep Packet Inspection (DPI) to enable external application servers to provide their services without performing DPI, and without being inserted in the data flow. For example with an external Active Content Filtering (ACF) Platform.

A high-level view of the streamlined ICAP interface support for external ACF is shown in the following figure:

Figure 1: High-Level View of Streamlined ICAP Interface with external ACF



The system with ECS is configured to support DPI and the system uses this capability for content charging as well. WAP and HTTP traffic is content filtered over the ICAP interface. RTSP traffic that contains adult content can also be content filtered on the ICAP interface. Only the RTSP Request packets will be considered for content filtering over the ICAP interface.

If a subscriber initiates a WAP (WAP1.x or WAP2.0) or Web session, the subsequent GET/POST request is detected by the DPI function. The URL of the GET/POST request is extracted and passed, along with subscriber identification information and the subscriber request, in an ICAP message to the application server. The application server checks the URL on the basis of its category and other classifications like, type, access level, content category and decides if the request should be authorized, blocked, or redirected by answering to the GET/POST with:

- A 200 OK message if the request is accepted.
- A 302 Redirect message in case of redirection. This redirect message includes the URL to which the subscriber must be redirected.
- Deny-response code 200 for RTSP requests is not supported. Only 403 "Forbidden" deny-response code will be supported.

Depending on the response received, the system with ECS will either pass the request unmodified, or discard the message and respond to the subscriber with the appropriate redirection or block message.

Content charging is performed by the Active Charging Service (ACS) only after the request has been controlled by the application server. This guarantees the appropriate interworking between the external application and content-based billing. In particular, this guarantees that charging will be applied to the appropriate request in case of redirection, and that potential charging-based redirections (i.e. Advice of Charge, Top Up page, etc.) will not interfere with the decisions taken by the application server.

Functions of the ACF include:

- Retrieval of subscriber policies based on the subscriber identity passed in the ICAP message
- Determining the appropriate action (permit, deny, redirect) to take for the type of content based on subscriber profile
- Communication of the action (permit, deny, or redirect) decision for the URL back to the ACS module

Supported Networks and Platforms

This feature supports the Cisco ASR 5500 platform for the core network services configured on the system.

For additional platform information, refer to the appropriate *System Administration Guide* and/or contact your Cisco account representative.

License Requirements

External Content Filtering Server support through Internet Content Adaptation Protocol (ICAP) interface is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements.

For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Failure Action on Retransmitted Packets

ICAP rating is enabled for retransmitted packet when default ICAP failure action was taken on an ICAP request for that flow. ICAP default failure action is taken on the pending ICAP request for a connection when the connection needs to be reset and there is no other redundant connection available. For example, in the ICAP request timeout and ICAP connection timeout scenarios. In these cases the retransmitted packet in the uplink direction is sent for ICAP rating again.

In case of WAP CO, uplink retransmitted packet for the WAP transactions for which ICAP failure action was taken will be sent for ICAP rating. WSP header of the retransmitted packet is not parsed by the WSP analyzer. The URL received in the previous packet for that transaction is used for ICAP rating. If failure action was taken on multiple WTP transactions for the same flow (case: WTP concatenated GET request) then uplink retransmitted packet for each of the transaction is sent for rating again.

In case of HTTP, uplink retransmitted packets for the HTTP flow on which ICAP failure action is taken is sent for ICAP rating. The URL present in the current secondary session (last uplink request) is used for ICAP rating. However, if there were multiple outstanding ICAP request for the same flow (pipelined request) then for the retransmitted packet the URL that will be sent for rating will be that of the last GET request.

Retransmission in various cases of failure-action taken on re-transmitted packets when the ICAP response is not received for the original request and the retransmitted request comes in:

- WSP CO:
  - Permit: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed/blocked. It is possible that the WAP gateway sends the response for the permitted GET request. Hence, there is a race condition and the subscriber may be able to view the web page even thought the rating was redirect or content insert.
  - Content Insert: The retransmitted packet is not sent for ICAP rating.
  - Redirect: The retransmitted packet is not sent for ICAP rating.
  - Discard: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed/blocked.
  - Terminate flow: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed or blocked. The WAP gateway may send an Abort transaction for this

GET request if the WSP disconnect packet sent while terminating the flow is received by the WAP gateway.

- HTTP:
  - Permit: The uplink packet is sent for ICAP rating and depending on the ICAP response the last HTTP GET request. It is possible that the HTTP server sends the response for the permitted GET request. Hence there is a race condition and the subscriber may be able to view the web page even thought the rating was redirect or content insert.
  - Content Insert: Retransmitted packets are dropped and not charged.
  - Redirect: Retransmitted packets are dropped and not charged.
  - Discard: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction allowed/blocked.
  - Terminate flow: Retransmitted packets are dropped and not charged.
- RTSP:

  The following scenarios describe the failure actions where an RTSP request is received from the client. If ICAP is enabled, then the request goes to the ICAP server for content filtering.
  - Allow: If the failure action configured is "allow", the RTSP request packet is sent out after applying the appropriate disposition action. Here, the flow remains the same as in the case if the ICAP response received is 200 OK.
  - Content Insert: If the failure action configured is "content-insertion <string of size 1 to 128>", then this failure action for RTSP request will not be supported. Instead the failure action "Discard" for such an RTSP request will be supported.
  - Redirect-URL: If the failure action configured is "redirect-url <string of size 1 to 128>", then a TCP FIN_ACK packet with an RTSP "302 Moved Temporarily" response header is inserted towards the client containing the said URL for redirection. A TCP RST packet is inserted towards the server. The underlying TCP connection is thus closed. If the RTSP client wants to retry to the redirected URL, the opening of a new TCP connection must be initiated.
  - Discard: If the failure action configured is "discard", then the RTSP request packet received from the client is quietly discarded and no notification is sent to the client.
  - Terminate flow: If the failure action configured is "terminate-flow", then the TCP connection is torn down by injecting a TCP FIN-ACK towards the client and a RST packet towards the server. However, no notification will be sent to the RTSP client and the server regarding this flow termination.

ICAP Client Communication with RFC 3507 compliance

The ICAP Content Filtering solution is extended to support ICAP client communication with ICAP server on Cisco ASR 5500 P-GW and HA in compliance with RFC 3507 - Internet Content Adaptation Protocol (ICAP). Only HTTP Request modification and partial enhancement of error codes per RFC 3507 is addressed in this release. The ICAP client running on P-GW/HA communicates with external ICAP server over ICAP protocol. If content filtering is enabled for a subscriber, all HTTP GET requests from that subscriber are validated by

the content filtering server (ICAP server), and is allowed, denied or redirected depending on the content categorization request.

Content-Filtering can be enabled for subscribers either through Override Control (OC) feature for predefined and static rules, or L7 Dynamic Rule Activation feature. A configurable option is added in the Content Filtering Server Group Configuration Mode to configure ICAP header that includes two parameters - Subscriber number information and CIPA (Children's Internet Protection Act) category.

Important Override Control and L7 Dynamic Rule Activation are license-controlled features. A valid feature license must be installed prior to configuring these features. Contact your Cisco account representative for more information.

- Subscriber Number: The "Subscription ID" AVP is sent from gateway to PCRF in CCR message. The AVP values are received to the gateway from HSS. The gateway does not receive this AVP in CCI-A message.
- CIPA category: The category string will be provided by PCRF and is included as an extension header in ICAP request modification message. The AVP will be received from PCRF in CCA-I or RAR.

Dictionary and AVP Support

A new Content Filtering (CF) dictionary "custom4" is introduced and the following new AVPs are added to r8-gx-standard and custom4 dictionaries.

- Override-Content-Filtering-State: This attribute carries information about Content Filtering status (CF state) of rules or charging-action. This AVP is used for overriding the content-filtering status of static and predefined rules. This attribute is included in the Override-Control grouped AVP.
- CIPA: This attribute contains the Children's Internet Protection Act (CIPA) category string value that is treated as an ICAP plan identifier. This identifier helps ICAP server in locating the correct Content Filtering plan i.e. CIPA category based on which the packet is processed.

  This attribute value is received from PCRF over Gx interface and is included in ICAP header while sending ICAP request.
- L7-Content-Filtering-State: This attribute carries information about Content Filtering status (CF state) of L7 rules. This attribute indicates whether or not the ICAP functionality is enabled or disabled for L7 charging rule definition received for installation from PCRF. Based on this attribute value, the traffic matching to the dynamic rule is sent to ICAP server.

  This attribute is included in the L7-Application-Description grouped AVP for L7 rule processing. This is applicable only for HTTP protocol.

Important CIPA and flags for controlling content filtering via OC and L7 Dynamic Rules features is applicable only for r8-gx-standard dictionary.

In addition to the new AVP support, L7-Field AVP in the L7-Application-Description grouped AVP is encoded to additionally accept ANY-MATCH as the input. The current framework does not support the existing field "vlan-id" in Override-Control, which is present in charging action. Hence, the Override-Content-Filtering-State AVP replaces Override-VLAN-ID to support OC.

When subscriber initiates create session request, P-GW/HA sends CCR-I message to PCRF to obtain subscriber profile. PCRF responds with CCA-I message that contains CIPA and OC information if ICAP functionality is enabled for this subscriber.

In the case of L7 dynamic rules, the Content-Filtering capability is enabled by sending L7-Content-Filtering-State AVP in L7-Application-Description grouped AVP. At least one L7 filter should be present when L7-Content-Filtering-State is received for the dynamic rule. If L7-Content-Filtering-state AVP is sent along with L7 filter information AVP, then the Content-Filtering state will not be considered. Hence, the filter received with L7-Content-Filtering-State will not be processed and the L7 rule will be discarded.

In the case of Override Control, when content filtering is enabled for subscriber, PCRF sends ICAP flag through Override-Control AVP. This AVP overwrites charging action to enable ICAP feature for that subscriber.

Refer to the *AAA Interface Administration and Reference* for more information on the supported AVPs.

Limitations

The limitations for this feature are listed below:

- Only IPv4 addressing scheme is supported.
- ICAP content filtering is applicable only for HTTP traffic. HTTPS traffic is not supported by ICAP client.
- Accelerated path will not be supported for this feature.

Configuring ICAP Interface Support

This section describes how to configure the Content Filtering Server Group (CFSG) through Internet Content Adaptation Protocol (ICAP) interface between ICAP client and ACF server (ICAP server).

Important This section provides the minimum instruction set for configuring external content filtering servers on ICAP interface on the system. For more information on commands that configure additional parameters and options, refer to *CFSG Configuration Mode Commands* chapter in *Command Line Interface Reference*.

To configure the system to provide ICAP interface support for external content filtering servers:

Step 1 Create the Content Filtering Server Group and create ICAP interface with origin (local) IP address of chassis by applying the example configuration in Creating ICAP Server Group and Address Binding, on page 7.

Step 2 Specify the active content filtering server (ICAP server) IP addresses and configure other parameters for ICAP server group by applying the example configuration in Configuring ICAP Server and Other Parameters, on page 7.

Step 3 Configure the content filtering mode to external content filtering server group mode in ECS rule base by applying the example configuration in Configuring ECS Rulebase for ICAP Server Group, on page 8.

Step 4 Configure the charging action to forward HTTP/RTSP/WAP GET request to external content filtering servers on ICAP interface in Active Charging Configuration mode by applying the example configuration in Configuring Charging Action for ICAP Server Group, on page 8.

Step 5 Verify your ICAP interface and external content filtering server group configuration by following the steps in Verifying the ICAP Server Group Configuration, on page 9.

Step 6 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Creating ICAP Server Group and Address Binding

Use the following example to create the ICAP server group and bind the IP addresses:

```
configure
   context <icap_ctxt_name> [ -noconfirm ]
      content-filtering server-group <icap_svr_grp_name> [ -noconfirm ]
         origin address <ip_address>
         end
```

Notes:

- <*ip_address*> is local IP address of the CFSG endpoint.

Configuring ICAP Server and Other Parameters

Use the following example to configure the active content filtering (ICAP server) and other related parameters:

```
configure
   context <icap_context_name>
      content-filtering server-group <icap_server_grp_name>
         icap server <ip_address> [ port <port_number> ] [ max <max_msgs>] [
priority <priority> ] [ standby ]
         connection retry-timeout <retry_timeout>
         deny-message <msg_string>
         dictionary { custom1 | custom2 | custom3 | custom4 | standard }
        failure-action { allow | content-insertion <content_string> | discard
 | redirect-url <url> | terminate-flow }
         header extension options { cipa-category cipa_category_name |
subscriber-number subscriber_num_name } +
         response-timeout <timeout>
         end
```

Notes:

- In 8.1 and later releases, a maximum of five ICAP servers can be configured per Content Filtering Server Group. In release 8.0, only one ICAP Server can be configured per Content Filtering Server Group.
- The **standby** keyword can be used to configure the ICAP server as standby. A maximum of ten active and standby ICAP servers per Content Filtering Server Group can be configured. The active and standby servers under the same server group can be configured to work in active-standby mode.
- The maximum outstanding request per ICAP connection configured using the optional **max** <*max_msgs*> keyword is limited to one. Therefore, any other value configured using the **max** keyword will be ignored.
- *Optional*. To configure the ICAP URL extraction behavior, in the Content Filtering Server Group configuration mode, enter the following command:

  url-extraction { after-parsing | raw }

By default, percent-encoded hex characters in URLs sent from the ACF client to the ICAP server will be converted to corresponding ASCII characters and sent.

- The **custom4** dictionary is a custom-defined dictionary that specifies user-defined information in the ICAP request message. The ICAP request message includes subscriber number and CIPA category values.

  When **custom4** dictionary is configured, ICAP requests are formed as part of ICAP RFC 3507 request mode request. If any other dictionary is configured, the earlier implementation of ICAP client will not be partial RFC compliant.

- The **header extension options** command configures ICAP header parameters - subscriber number and CIPA category.

Configuring ECS Rulebase for ICAP Server Group

Use the following example to configure the content filtering mode to ICAP server mode in the ECS rulebase for content filtering:

```
configure
   require active-charging [ optimized-mode ]
   active-charging service <acs_svc_name> [ -noconfirm ]
      rulebase <rulebase_name> [ -noconfirm ]
         content-filtering mode server-group <cf_server_group>
         end
```

Notes:

- In release 8.1, the **optimized-mode** keyword enables ACS in the Optimized mode, wherein ACS functionality is managed by SessMgrs. In release 8.1, ACS must be enabled in the Optimized mode.
- In release 8.3, the **optimized-mode** keyword is obsolete. With or without this keyword ACS is always enabled in Optimized mode.
- In release 8.0 and release 9.0 and later, the **optimized-mode** keyword is not available.

Important After you configure **configure**, **require active-charging [optimized-mode]**, **active-charging service** *<acs_svc_name>* **[-noconfirm]**, and **rulebase** CLI commands, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Configuring Charging Action for ICAP Server Group

Use the following example to configure the charging action to forward HTTP/WAP GET request to ICAP server for content processing.

```
configure
   active-charging service <acs_svc_name>
      charging-action <charging_action_name> [ -noconfirm ]
         [ no ] content-filtering processing server-group
         end
```

Notes:

- If the content-filtering flag supplied by charging action is required to configure the Override Control feature, then the **no content-filtering processing** command must be configured. This will ensure overriding content-filtering processing to be enabled or disabled through the Override Control feature.

Verifying the ICAP Server Group Configuration

This section explains how to display and review the configurations after saving them in a .cfg file and also to retrieve errors and warnings within an active configuration for a service.

Important All commands listed here are under Exec mode. Not all commands are available on all platforms.

These instructions are used to verify the configuration for this feature.

Step 1 Verify your ICAP Content Filtering Server Group configuration by entering the following command in Exec Mode:

show content-filtering server-group

The following is a sample output. In this example, an ICAP Content Filtering server group named *icap_cfsg1* was configured.

```
Content Filtering Group:         icap_cfsg1
    Context:                             icap1
    Origin Address:                      1.2.3.4
    ICAP Address(Port):                  1.2.3.4(1344)
    Max Outstanding:                     256
    Priority:                            1
    Response Timeout: 30(secs)  Connection Retry Timeout: 30(secs)
    Dictionary:                          standard
    Timeout Action:                      terminate-flow
    Deny Message:                        "Service Not Subscribed"
    URL-extraction:                      after-parsing
    Header Extension Options:            subscriber-number i-sub
    Content Filtering Group Connections: NONE
Total content filtering groups matching specified criteria:  1
```

Step 2 Verify any configuration error in your configuration by entering the following command in Exec Mode:

show configuration errors