

Content Filtering Server Group Configuration Mode Commands

Content Filtering Server Group Configuration Mode sets the parameters for interoperating with a group of external servers. It is accessed by entering the **content-filtering server-group** command in the Context Configuration Mode.

Command Modes

Exec > Global Configuration > Context Configuration > CFSG Configuration

configure > context *context_name* **> content-filtering server-group** *server_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-content-filtering)#
```

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

- connection retry-timeout, on page 1
- deny-response code, on page 2
- dictionary, on page 3
- end, on page 4
- exit, on page 5
- failure-action, on page 5
- header extension options, on page 7
- icap server, on page 8
- origin address, on page 10
- response-timeout, on page 10
- timeout action, on page 11
- url-extraction, on page 11

connection retry-timeout

Configures the TCP connection retry timer for Internet Content Adaptation Protocol (ICAP) server and client.

Product CF

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > CFSG Configuration

configure > context *context_name* **> content-filtering server-group** *server_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-content-filtering)#`

Syntax Description

`connection retry-timeout` *duration*
`{ default | no } connection retry-timeout`

default

Configures the default setting of 30 seconds.

no

Removes the connection retry timeout configuration.

duration

Specifies the duration (in seconds) as an integer from 1 to 3600. Default: 30

Usage Guidelines Use this command to configure the connection retry timer between ICAP server and client TCP connection, i.e. how long to wait before re-attempting to establish a TCP connection.

Example

The following command sets the ICAP client and server connection retry timer to 120 seconds:

```
connection retry-timeout 120
```

deny-response code

Configures the deny response message that is to be sent from the ICAP server to the subscribers.

Product ICAP

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > CFSG Configuration

configure > context *context_name* **> content-filtering server-group** *server_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-content-filtering)#`

Syntax Description

`deny-response code { 200 message` *string* **`| 403 }`**
`{ default | no } deny-response code`

default

Configures the default setting of **deny-response code 200**.

no

Removes previously configured deny response message setting.

deny-response code 200 message *string*

Specifies a text message that is to be returned to the subscriber in a code 200 deny response. as an alphanumeric string of 1 through 511 characters.

If **deny-response code 200** is configured, the response sent to the subscriber will be of the form 200 OK with deny messages denied. If a message is configured for response code 200, that message will be used instead of "Access denied".

deny-response code 403

This keyword is used to set response code 403 for the deny response message.

When this keyword is configured, the deny response from the ICAP server will be sent "as is" to the subscriber.

Usage Guidelines

Use this command to define a text message that is returned to the subscriber in a deny response.

Example

The following command sets the text message to *Not allowed* in a deny response message:

```
deny-response code 200 message Not allowed
```

dictionary

Specifies the dictionary to use for requests to the server(s) in this Content Filtering Server Group (CFSG).

Product

CF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CFSG Configuration

configure > context *context_name* **> content-filtering server-group** *server_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-content-filtering)#
```

Syntax Description

```
dictionary { custom1 | custom2 | custom3 | custom4 | standard }
{ default | no } dictionary
```

default

Sets the default dictionary.

Default: **default**

no

Removes the previously configured dictionary setting.

custom1

Specifies a custom-defined dictionary that conforms to TS 32.015 v 3.6.0 for R99. It provides proprietary header fields for MSISDN and APN/subscriber. Please contact your local Cisco representative for more information.

custom2

Custom-defined dictionary. Please contact your local Cisco representative for additional information.

custom3

Custom-defined dictionary. Please contact your local Cisco representative for additional information.

custom4

Specifies a custom-defined dictionary that conforms to RFC 3507. Please contact your local Cisco representative for additional information.

standard

Default: Enabled

This dictionary uses an HTTP Get Request to specify the URL. It conforms to TS 32.215 v 4.6.0 for R4 (and also R5 - extended QoS format).

Usage Guidelines

Use this command to specify the standard and customized encoding mechanism used for elements included messages.

Example

The following command configures the system to use standard dictionary to encode messages:

```
default dictionary
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

```
end
```

Usage Guidelines Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **exit**

Usage Guidelines Use this command to return to the parent configuration mode.

failure-action

Specifies the actions to be taken when communication between ICAP endpoints within this Content Filtering Server Group (CFSG) fail.

Product CF

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > CFSG Configuration

configure > **context** *context_name* > **content-filtering server-group** *server_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-content-filtering)#`

Syntax Description **failure-action { allow | content-insertion** *content_string* **| discard | redirect-url** *url* **| terminate-flow }**
{ default | no } failure-action

default

Configures the default setting of **terminate-flow**.

no

Removes previously configured failure action.

allow

For static content filtering, this option allows the request for content. In dynamic content filtering, it allows the content itself.

content-insertion *content_string*

Specifies the content string to be used for failure action.

For static content filtering, the specified text is used to create a response to the subscriber's attempt to get content. In dynamic content filtering, the specified text replaces the content returned by a server.

content_string must be an alphanumeric string of 1 through 128 characters.

discard

For static content filtering, this option discards the packet(s) requested. In dynamic content filtering, it discards the packet(s) that contain(s) the content.

redirect-url *url*

Redirects the subscriber to the specified URL.

url must be an alphanumeric string of 1 through 128 characters in the following format: *http://search.com/subtarg=#HTTP.URL#*

terminate-flow

For TCP, gracefully terminates the connection between the subscriber and external server, and sends a TCP FIN to the subscriber and a TCP RST to the server.

For WAP-Connection Oriented, the WSP session is gracefully terminated by sending WTP Aborts for each of the outstanding requests, and WSP Disconnect to the client and the server. For WSP-Connectionless, only the current WSP request is rejected.

Usage Guidelines

Use this command to set the actions on failure for server connection.

ICAP rating is enabled for retransmitted packets when the 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, the retransmitted packet in the uplink direction is sent for ICAP rating again.

For WAP CO, uplink retransmitted packets for the WAP transactions for which ICAP failure action was taken will be sent for ICAP rating. The 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), the uplink retransmitted packet for each of the transactions is sent for rating again.

For HTTP, uplink retransmitted packets for the HTTP flow on which ICAP failure action is taken are 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 requests for the same flow (pipelined request), the retransmitted packet for the URL sent for rating will be that of the last GET request.

Retransmission in various cases of failure-action taken on retransmitted 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 will be dropped and not charged.

Example

The following command sets the failure action to terminate:

```
failure-action terminate-flow
```

header extension options

Configures the extension options for the ICAP header in the ICAP request message.

Product

CF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CFSG Configuration

configure > context *context_name* **> content-filtering server-group** *server_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-content-filtering)#
```

Syntax Description

header extension options { cipa-category *cipa_category_name* **| subscriber-number** *subscriber_num_string* **}**
no header extension options

no

When configured, CIPA category and subscriber number will not be inserted in the ICAP request message to ICAP server. The values are string names present in the ICAP request message.

cipa-category *cipa_category_name*

Specifies the CIPA category in the ICAP Request message.

cipa_category_name must be an alphanumeric string of 1 through 31 characters.

subscriber-number *subscriber_num_string*

Specifies the subscriber number in the ICAP Request message.

subscriber_num_string must be an alphanumeric string of 1 through 31 characters.

Usage Guidelines

Use this command to configure header extension options in the ICAP request header - CIPA category and Subscriber number.

Example

The following command configures the ICAP header with CIPA category **x-icap-cipa-category**:

```
header extension options cipa-category x-icap-cipa-category
```

icap server

Adds an Internet Content Adaptation Protocol (ICAP) server configuration to the current Content Filtering Server Group (CFSG).



Important A maximum of five ICAP servers and only one ICAP Server can be configured per Content Filtering Server Group.

Product

CF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CFSG Configuration

configure > **context** *context_name* > **content-filtering server-group** *server_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-content-filtering)#
```

Syntax Description

```
icap server ip_address [ port port_number ] [ max messages ] [ priority priority
 ] [ standby ]
no icap server ip_address [ port port_number ] [ priority priority ] [ standby
 ]
```

no

Removes the specified ICAP server configuration from the current Content Filtering Server Group.

ip_address

Specifies the ICAP server's IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

port *port_number*

Specifies the ICAP server's port number to use for communications as an integer from 1 to 65535. Default: 1344

max *messages*

Specifies the maximum number of unanswered outstanding messages that may be allowed to the ICAP server as an integer from 1 to 4096. Default: 256



Important The maximum outstanding requests per ICAP connection is limited to one. Therefore the value configured using the **max** keyword will be ignored.

priority *priority*

Specifies priority of the ICAP server in the current Content Filtering Server Group. The priority is used in server selection to determine which standby server becomes active. *priority* must be an integer from 1 (highest priority) to 65535 (lowest priority). Default: 1



Important The **priority** keyword is only available in 8.1 and later releases.

standby

Configures the ICAP server as standby. A maximum of ten active and standby servers per group can be configured.

Usage Guidelines

This command is used to add an ICAP server configuration to a Content Filtering Server Group with which the system is to communicate for content filtering communication.

The ICAP solution supports only one connection between ACS Manager and ICAP server.

Multiple ICAP server connections are supported per manager. At any time only one connection is active with the other connections acting as standby. In case of a connection failure, based on its priority, a standby connection becomes active. Any pending ICAP requests are moved to the new active connection. If a standby connection is unavailable, failure action is taken on all pending ICAP requests. See the command.

A maximum of five ICAP servers can be configured per Content Filtering Server Group with a priority associated with each server. Once configured, an ICAP server's priority cannot be changed. To change a server's priority, the server configuration must be removed, and added with the new priority.

A maximum of ten active and standby servers per group can be configured.

Example

The following command sets the ICAP server IP address to *209.165.200.225* and port to *1024*:

```
icap server 209.165.200.225 port 1024
```

The following command specifies an ICAP server with IP address *209.165.200.226*, port number *1024*, and priority *3*:

```
icap server 209.165.200.226 port 1024 priority 3
```

origin address

Specifies a bind address for the Content Filtering Server Group (CFSG) endpoint.

Product

CF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CFSG Configuration

configure > **context** *context_name* > **content-filtering server-group** *server_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-content-filtering)#
```

Syntax Description

origin address *ip_address*
no origin address

no

Disables/releases the binding address for the CFSG endpoint.

ip_address

Specifies the IP address to bind the CFSG endpoint in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage Guidelines

Use this command to set the bind address for the CFSG endpoint.

Example

The following command sets the origin address of *209.165.200.225*:

```
origin address 209.165.200.225
```

response-timeout

Sets the response timeout for the ICAP connection between the ICAP server and client.

Product CF

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > CFSG Configuration

configure > context *context_name* **> content-filtering server-group** *server_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-content-filtering)#
```

Syntax Description

response-timeout *duration*
{ default | no } response-timeout

default

Configures the default setting of 30 seconds.

no

Removes the response timeout configuration.

duration

Specifies the timeout duration (in seconds) as an integer from 1 to 300. Default: 30

Usage Guidelines Use this command to set the ICAP connection response timeout, after which connection will be marked as unsuccessful between ICAP endpoint.

Example

The following command sets the ICAP connection response timeout to *100* seconds:

```
response-timeout 100
```

timeout action

This command has been deprecated, and is replaced by the failure-action, on page 5 command.

url-extraction

Enables configuration of ICAP URL extraction behavior.

Product CF

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > CFSG Configuration

configure > context *context_name* **> content-filtering server-group** *server_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-content-filtering)#
```

Syntax Description

```
url-extraction { after-parsing | raw }
default url-extraction
```

default

Configures the default setting of **after-parsing**.

after-parsing

Specifies sending the parsed URI and host name. Percent-encoded hex characters in URLs sent from the ACF client to the ICAP server will be converted to corresponding ASCII characters before being sent.

For example, the URL: *http://www.google.co.uk/?this%20is%20a%20test* will be sent to the ICAP server as:

http://www.google.co.uk/?this is a test

raw

Specifies sending raw URI and host name. The URLs will contain percent-encoded hex characters "as is".

For example, the URL *http://www.google.co.uk/?this%20is%20a%20test* will be sent to the ICAP server as:

http://www.google.co.uk/?this%20is%20a%20test

Important The raw URL configuration asserts that there are no changes in the URL before sending the request to ICAP. However, if there are spaces in the original URI then the same is forwarded to ICAP.

Usage Guidelines

Use this command to configure the ICAP URL extraction behavior. Percent-encoded hex characters—for example, space (%20) and the percent character (%25)—in URLs sent from the ACF client to the ICAP server can be sent either as percent-encoded hex characters or as their corresponding ASCII characters.

Example

The following command configures URLs sent from the ACF client to the ICAP server to contain the escape encoding as is:

```
url-extraction raw
```