ERICSSON

Content Filtering

DESCRIPTION

511/22102-AXB 250 12-V3 Uen V

Contents

1 Introduction

This document describes support for content filtering in the GGSN or PGW.

1.1 Scope

This document provides an overview of content filtering in the PGW, including content filtering elements, interfaces, deployment scenarios, and example traffic cases.

For information about configuring content filtering in the PGW, see Content Filtering Configuration. For information about the Internet Content Adaptation Protocol (ICAP) interface used for content filtering, see ICAP Interface Description.

Note: For the purpose of this document, the term PGW is used to identify both the GGSN and the PGW functions of the EPG, unless otherwise stated.

1.2 Target Groups

This document is intended as an introduction to PGW content filtering for network operators, network and service planners, as well as system engineers and administrators. It can be used as a basis for training and assumes a basic knowledge of data communication and telecommunication.

For information about counters related to content filtering, see Counters and Gauges for the GGSN and PGW.

For information about alarms related to content filtering, see Alarm and Alert List.

2 Content Filtering in the PGW

Content filtering provides a mechanism for the operator to control subscriber access to web resources. The PGW supports fine-grained content filtering for services using HTTP/1.1 and HTTP/2, or HTTP over Secure Sockets Layer (SSL)/Transport Layer Security (TLS) including HTTPS. From a functional perspective, content filtering is based on a set of configured web resources that subscribers are - or are not - allowed to access. Content filtering is also performed based on content classification, performed by an external server, into categories configured in the PGW, such as adult, violence, news, and so on.

A user session subject to content filtering is assigned to a content filtering profile, which is locally configured in the PGW. All user sessions assigned to the same

content filtering profile receive the same treatment, from a content filtering perspective. A content filtering profile defines, among others, the content filtering policy actions to be performed on requests for web resources. According to the content filtering policy action configured for a content category, the PGW can perform one of the following actions:

— Allow the request to pass through, and enable access to the web resource for the user session.

— Redirect the request to a different web resource. Redirect destinations are configured in the PGW.

  Note: The `Redirect` action applies to HTTP requests, but not to SSL/TLS requests.

— Block the request, and deny access to the web resource for the user session.

The PGW uses the Uniform Resource Identifier (URI) extracted from the `HTTP GET` request or Server Name Indication (SNI) extracted from the SSL/TLS `Client Hello` message to apply content filtering policies based on the category of the URI, or on URI black and white lists. SNI in the `Client Hello` message indicates to which hostname the client attempts to connect at the start of the handshaking process. The domain present in the SNI field is converted to URI format to check its category.

The PGW supports local configuration of content filtering policy actions to be performed on lists of Uniform Resource Identifiers (URIs). For instance, a content filtering profile can include one list of URIs to be allowed to pass, one list of URIs to be blocked, and one list of URIs to be redirected to a specified destination. The configured URIs will match any request for a URI that starts with the configured URI. For instance, if the URI `http://www.example.co` is configured, this will match requests for both `http://www.example.com` and `http://www.example.co.uk`.

A white-list of IP addresses can be optionally configured in the PGW. Subscriber requests for URIs located on a white-listed IP address are allowed to pass through without being subjected to content filtering.

In order to reduce the latency of subsequent URI requests, the PGW caches the URI, the content filtering profile, and the resulting content filtering policy action for the URI. The PGW uses this information to resolve a content filtering policy action for subsequent requests to the URI, instead of looking up the content filtering profile for each request.

When a UE requests a web resource that is not white-listed in the PGW - where the port is either `80` (HTTP), `8080` (HTTP), `443` (HTTPS), or in the configured list - the PGW uses the following sources in the listed order of precedence, to resolve a content filtering policy action for the URI:

1. Cache (if enabled). See Section 6 on page 14 for more details.

2. Locally configured pass, block, and redirect lists for URIs.

Note: The `Block` action is performed for the user session if the `Redirect` action is selected for SSL/TLS traffic.

3. An ICAP server, if ICAP is configured and enabled, to retrieve the content category for which a content filtering policy action is locally configured.

To ensure that the URIs of the requested web resources are always in a normalized format when comparing against the configured URIs, the PGW performs the following Packet Inspection and Service Classification (PISC) related operations on received HTTP requests:

— Escape character normalization

— IPv6 address normalization

— Port normalization

For more information about PISC and content filtering, see Packet Inspection and Service Classification (PISC).

2.1 Port Setup

The PGW supports configuration of a list of HTTP ports on which content filtering is applied. In addition to the configured list of HTTP ports, the PGW always applies content filtering for HTTP services on ports `80` and `8080`.

When content filtering is enabled for HTTP, the PGW can also be optionally configured to apply SNI-based content filtering to SSL/TLS traffic.

The PGW supports configuration of a list of SSL/TLS ports on which content filtering is applied. In addition to the configured list of SSL/TLS ports, the PGW always applies content filtering for HTTPS services on port `443`.

The same TCP port cannot be configured for both HTTP and SSL/TLS due to content filtering.

2.2 ICAP

The PGW can optionally connect to an ICAP server, which acts as an external content classification engine, over the ICAP interface. The PGW uses the ICAP server to retrieve content category information for a requested URI or SNI.

Figure 1 shows a simplified model of the signaling involved when content filtering is applied to an HTTP or SSL/TLS request. In this scenario, ICAP communication is enabled for the content filtering profile.

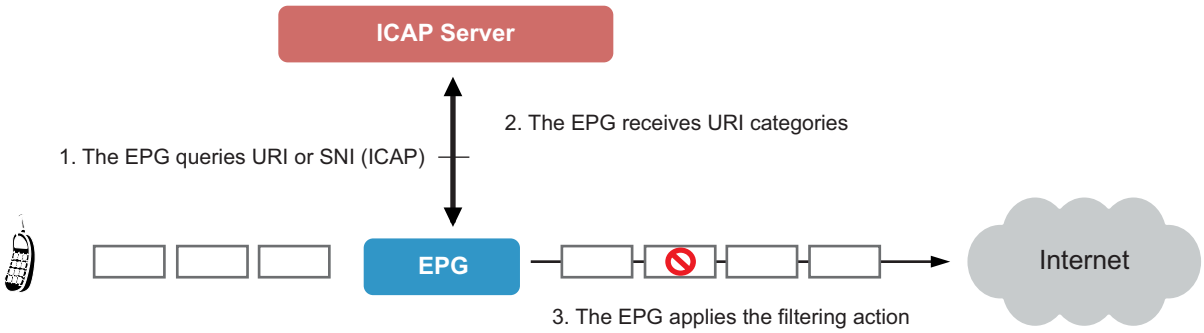


Figure 1 Content Filtering Interactions in the PGW

3 Content Filtering Policy Actions, Policies, and Profiles

This section describes the following elements of content filtering support in the PGW:

- Content filtering policy actions
- Content filtering policies
- Content filtering profiles

3.1 Content Filtering Policy Actions

A content filtering policy action defines the action performed by the PGW on a URI request. The PGW supports the following content filtering policy actions, listed in order from least restrictive to the most restrictive:

Pass If the `Pass` action is selected for a URI, access to the requested web resource is allowed for the user session.

Block If the `Block` action is selected for a URI, access to the requested web resource is not allowed for the user session, and the received HTTP request is silently discarded.

Redirect

If the `Redirect` action is selected for a URI, direct access to the requested web resource is not allowed for the user session. Instead, the request is redirected to a specific web resource configured in the PGW.

The `Redirect` action generates a new request to the configured destination. This new request is also subject to content filtering. It is recommended to configure the target destination in a pass list, see Section 3.3 on page 6.

If the `Redirect` action is selected for SSL/TLS traffic, the `Block` action is performed for the user session.

For information about the signaling involved during HTTP redirect, see Traffic Redirection.

In the PGW, content filtering policy actions can be defined in the following ways:

— As actions to be performed on a set of URIs. These actions are configured as part of a content filtering profile.

— As actions to be performed on a set of categories. These actions are configured as part of a content filtering policy.

For the purpose of this document, the term policy action is used to refer to a content filtering policy action.

3.1.1 Redirect URI Formatting

The query part of a redirect destination URI can be formatted with special codes. During redirection, the EPG can replace the formatting codes with corresponding variable information.

The following formatting codes can be replaced by the EPG with the corresponding information at the specified point within the URI:

— `%M`

The Mobile Subscriber ISDN Number (MSISDN) of the UE

— `%S`

The International Mobile Subscriber Identity (IMSI) of the UE

— `%U`

The URI of the redirected request

Note: The EPG truncates the redirect destination URI at a maximum of 899 characters.

3.1.1.1 Redirect URI Formatting Example

The query part of a redirect destination URI `http://www.redirect-address.com/?imsi=%S&msisdn=%M&requri=%U` includes the following formatting codes: `%M`, `%S`, and `%U`.

For a request to `http://www.request-address.com/index.html` from a user session with IMSI `100200000000007` and MSISDN `111220000001`, the resulting redirect destination URI is `http://www.redirect-address.com/?imsi=100200000000007&msisdn=111220000001&requri=http%3A%2F%2Fwww.request-address.com%2Findex.html`.

Note: The special characters `/` and `:` are replaced with `%2F` and `%3A` respectively. For more information on the special characters, see RFC 2396.

3.2 Content Filtering Policies

A content filtering policy defines policy actions to be applied to different content categories in the PGW.

A content filtering policy can optionally contain one or more of the following:

— One list of allowed content categories

— One list of blocked content categories

— One or more lists of content categories and a URI for each list. The URI for each list specifies the destination to which each category in the list is redirected.

A content filtering policy is referenced by a locally configured content filtering profile in the PGW, and can be referenced by several content filtering profiles.

Note: If a content filtering policy is updated by configuration, the new policy actions are applied to all URI requests that occur subsequent to the configuration update, and to URI requests for which a policy action has not yet been resolved.

If a requested URI belongs to several categories corresponding to different content filtering policies, the PGW applies the most restrictive policy.

3.3 Content Filtering Profiles

Content filtering profiles are locally configured in the PGW. A content filtering profile defines content filtering options available for a user session, and performs the following functions:

— Defines a profile ID, which is used to identify the content filtering profile over the Gx+ interface when profile selection is performed using Gx+.

— Enables or disables ICAP communication for the content filtering profile.

— References a locally configured content filtering policy, which defines policy actions to be performed on different content categories.

— References pass, block, and redirect lists for URIs.

— Defines a default policy, that is, a content filtering policy action to be enforced when no policy action is configured for a content category.

— Defines an error policy, that is, a content filtering policy action to be enforced when the PGW encounters an error while resolving a policy action for the requested URI. This can happen, for instance, when the PGW is unable to communicate with the ICAP server.

— Defines an unknown policy, that is, a content filtering policy action to be enforced when either of the following conditions is satisfied:

  - The requested URI is not configured in a URI list and ICAP is not enabled for the profile.
  - The ICAP server fails to categorize the requested URI.

To activate content filtering for a user session, an existing content filtering profile must be associated with the user session. The PGW enforces policy actions to URI requests according to the rules included in the content filtering profile selected for the user session. For information about content filtering profile selection methods supported by the PGW, see Section 4 on page 7.

An existing content filtering profile can optionally be configured as the default profile, which is selected when no other content filtering profile is assigned to the user session.

Note: If a content filtering profile is removed by configuration, the content filtering action `Pass` is applied to all URI-based traffic for the affected user sessions. This action is applied until the next content filtering profile selection occurs.

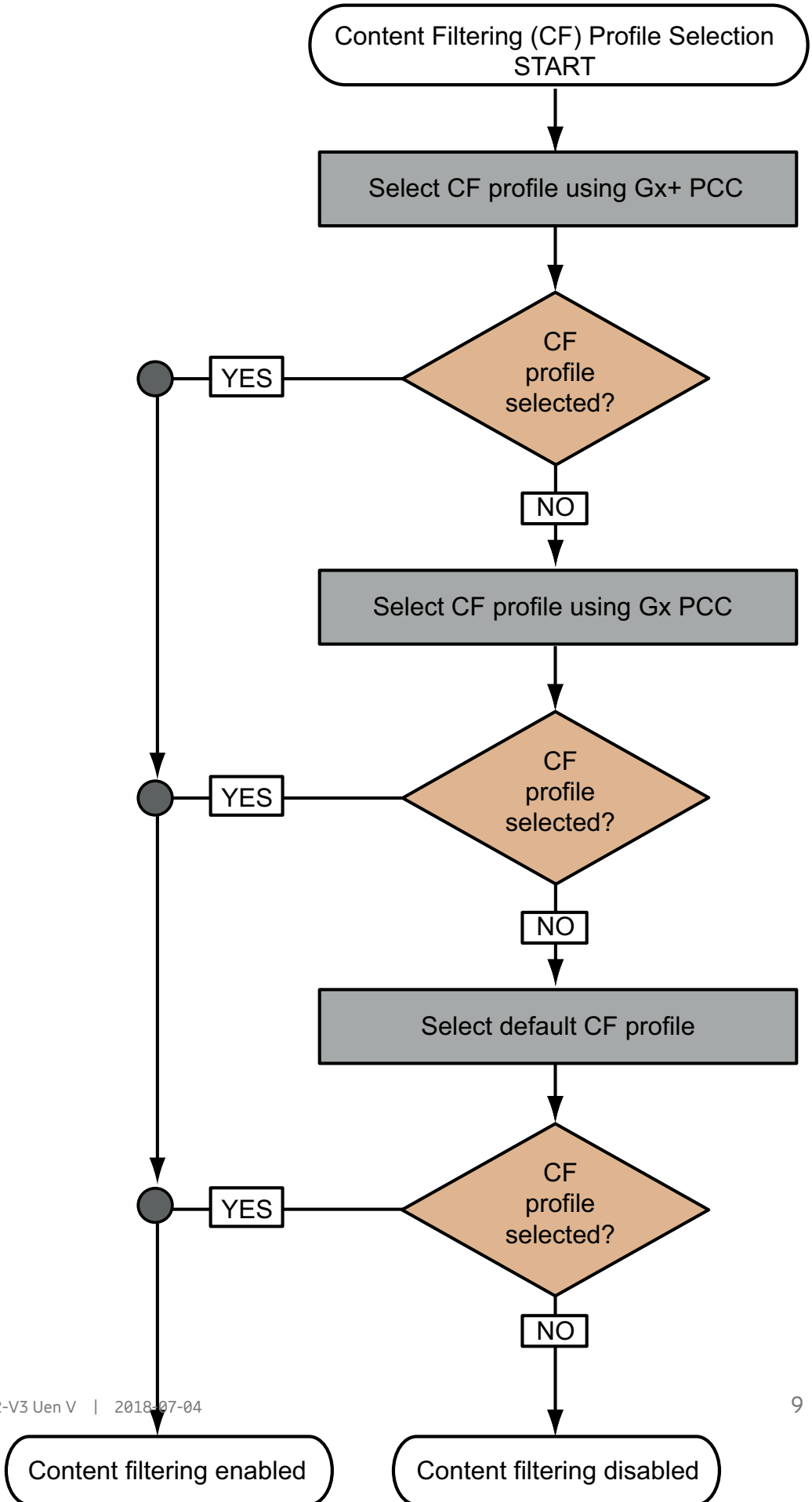
4 Content Filtering Profile Selection

The PGW applies content filtering to a user session based on the rules included in a content filtering profile. A content filtering profile is selected for a user session from the set of locally configured content filtering profiles, using the following methods in the listed order of precedence:

1. PCRF-based content filtering profile selection using Gx+ PCC.
2. PCRF-based content filtering profile selection using Gx PCC

3. Default content filtering profile selection

Figure 2 describes the content filtering profile selection process for a user session in the PGW.


Content Filtering (CF) Profile Selection START
Select CF profile using Gx+ PCC
CF profile selected?
YES
NO
Select CF profile using Gx PCC
CF profile selected?
YES
NO
Select default CF profile
CF profile selected?
YES
NO
Content filtering enabled
Content filtering disabled

If a content filtering profile is not selected using any of the previously described options, the PGW disables content filtering for the user session.

A content filtering profile selection in the PGW can be triggered by any of the following scenarios:

— PDN connection creation

— PDN connection modification

— GGSN- or PGW-initiated PCC session update

— PCC session reestablishment over Gx

For information about the signaling involved in the scenarios mentioned above, see Session Management and Policy Control.

4.1 PCRF-based Content Filtering Profile Selection

The PGW provides support for activating and updating the content filtering profile applied to a user session, using the PCRF. A content filtering profile can be selected using Gx+ PCC if supported by the PCRF, or using Gx PCC.

4.1.1 Content Filtering Profile Selection using Gx+ PCC

Note: In this section, it is assumed that a content filtering profile is configured, and that the content filtering profile is mapped to a unique content filtering profile ID.

The following procedure describes the content filtering profile selection process, using Gx+ PCC:

1. The PGW indicates support for the `Content-Filtering-Profile-Id` Attribute-Value Pair (AVP), using a flag in the `Gx-Capability-List` AVP. The `Gx-Capability-List` AVP is included in the `Credit-Control-Request Initial (CCR-Initial)` message to the PCRF.

2. The PCRF indicates support for the `Content-Filtering-Profile-Id` AVP, using a flag in the `Gx-Capability-List` AVP. The `Gx-Capability-List` AVP is included in the `Credit-Control-Answer Initial (CCA-Initial)` message to the PGW.

3. The PGW receives the `Content-Filtering-Profile-Id` AVP as part of the following messages:

   — `CCA-Initial`

   — `CCA-Update`

   — `Re-Auth Request (RAR)` (only Gx+ Release 8 or later)

4. If the `Content-Filtering-Profile-Id` AVP contains a valid content filtering profile ID, the PGW selects the corresponding content filtering profile for the user session.

   If Gx+ Release 7 is used, and an invalid content filtering profile ID is received or the AVP is not received in a `CCA-U` or `RAR` message, content filtering is disabled or not started for the user session.

   If Gx+ Release 8 or later is used, and an invalid content filtering profile ID is received or the **`0xFFFFFFFF`** value is included in the `Content-Filtering-Profile-Id` AVP, content filtering is disabled or not started for the user session. If the `Content-Filtering-Profile-Id` AVP is not received in the `CCA-U` or `RAR` message, the status of the content filtering profile remains the same.

4.1.2 Content Filtering Profile Selection using Gx PCC

The PGW supports content filtering profile selection by the PCRF over the Gx PCC interface using the installation of charging rules mapped to content filtering profiles. In order for the PGW to select a content filtering profile based on charging rules using Gx PCC, at least one content filtering profile selection configuration must be performed. This configuration defines mappings from Access Control Rules (ACRs) to content filtering profiles. Several mappings can be configured with different priority levels. For information about configuring content filtering profile selection based on charging rules, see Content Filtering Configuration.

The following procedure describes the content filtering profile selection process, using Gx PCC. It is assumed that at least one mapping from an ACR to an existing content filtering profile is configured.

1. The PGW receives a `Charging-Rule-Install` AVP, included with any of the following messages from the PCRF:

   — `CCA-Initial`

   — `CCA-Update`

   — `Re-Auth Request (RAR)`

   The received `Charging-Rule-Install` AVP contains `Charging-Rule-Name` AVPs that indicate ACRs mapped to content filtering profiles in the PGW.

2. The PGW goes through the installed ACRs mapped to content filtering profiles, and selects the content filtering profile that is configured with the highest priority level to be applied for the user session.

4.2 Default Content Filtering Profile

The PGW applies a default content filtering profile to a user session if all of the following conditions are fulfilled:

— No content filtering profile is selected using Gx+ PCC or using Gx PCC

— An existing content filtering profile is configured as the default profile for the APN to which the user session is connected.

4.3 Content Filtering Profile Selection: Example Signal Flows

In the following sections, it is assumed that the content filtering profile is retrieved from the PCRF over Gx+ PCC.

4.3.1 PDN Connection Activation

It is possible to enable content filtering at PDN connection activation. In this case, the PGW receives a PDN connection activation request from the UE, and sends a `CCR-Initial` message to the PCRF. The PGW receives a `CCA-Initial` message from the PCRF that includes a `Content-Filtering-Profile-Id` Attribute-Value Pair (AVP) to be applied to the PDN connection. The PGW maps the `Content-Filtering-Profile-Id` to a content filtering profile, and content filtering is considered active for the PDN connection.

Figure 3 illustrates the signaling involved.

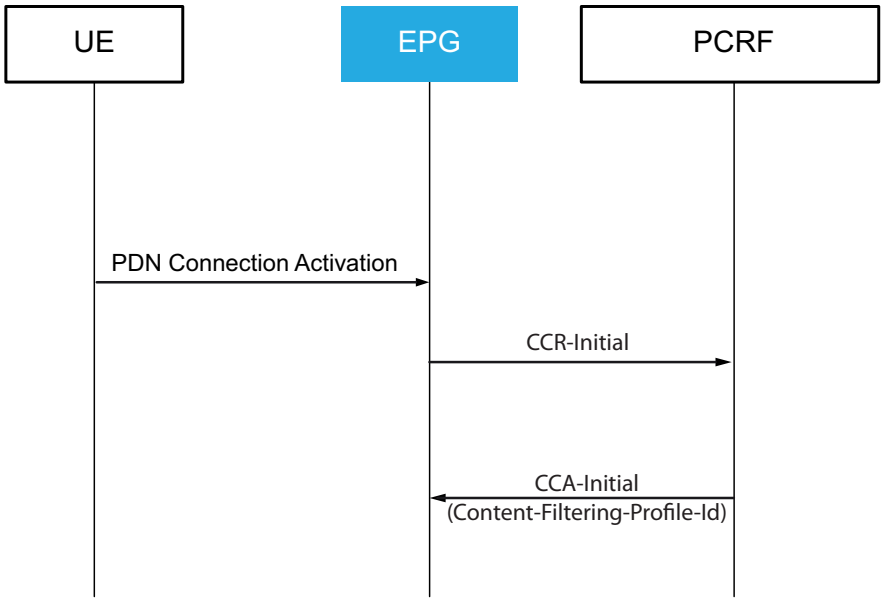


Figure 3 PDN Connection Activation subject to Content Filtering

In order for the PGW to activate a PDN connection subject to content filtering, support for content filtering has to be communicated in the `Gx-Capability-List` AVP in both the `CCR-Initial` and `CCA-Initial` messages.

4.3.2 UE or Network-Initiated Content Filtering Profile Update

The PGW detects that the user session undergoes an evet to which PCRF subscribes - for instance, an Inter-Radio Access technology (IRAT) handover - and sends a `CCR-Update` message to the PCRF. The PCRF sends a `CCA-Update` message to the PGW, including the updated `Content-Filtering-Profile-Id` to be applied to the PDN connection.

The updated content filtering profile applies to new URI requests through the PGW, and does not affect the content filtering action previously determined for existing flows and for URI requests received before the content filtering profile update.

Figure 4 illustrates the signaling involved.

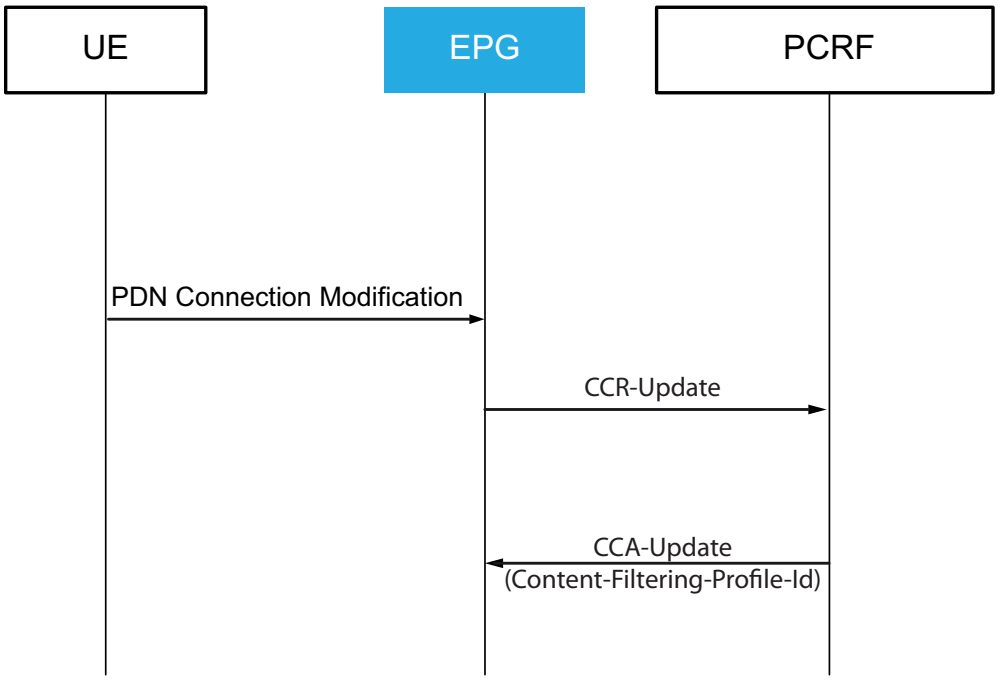


Figure 4 PGW-Initiated Content Filtering Profile Update

4.3.3 Content Filtering Profile Deactivation at PGW-Initiated Update

The PGW initiates a Gx+ PCC session update with a `CCR-Update` message to the PCRF. The PCRF returns a `CCA-Update` message to the PGW, without including a `Content-Filtering Profile-Id` AVP. The PGW checks if a configured default content filtering profile is applicable to the PDN connection. If no applicable content filtering profile is found, the PGW deactivates content filtering for the PDN connection.

Deactivation of a content filtering profile applies to new URI requests through the PGW, and does not affect the content filtering action previously determined for

existing flows and for URI requests received before the content filtering profile is deactivated.

5 ICAP Interface

The ICAP interface connects the PGW to the ICAP server. The PGW uses the ICAP interface to query URI content categories.

The ICAP interface only supports IPv4 signaling, but can exchange attributes related to IPv6 traffic.

5.1 Supported Messages

The ICAP interface supports the following messages:

— `OPTIONS` request and response messages

— `REQMOD` request and response messages

For information on messages and headers supported by the ICAP interface, see ICAP Interface Description.

6 Cache

The PGW supports using a cache in order to resolve content filtering requests locally. If the content filtering cache is enabled, signaling and latency is reduced.

If the cache is enabled, the PGW always tries to look up requested URIs in the cache before trying to resolve the URI locally or using the ICAP interface. The cache is enabled by default. For information about how to disable the cache, see Content Filtering Configuration.

For each content filtering profile, the PGW caches the action associated with the most used URIs. Each Packet Processing Board (PPB) instance has a separate cache instance.

Note: If the ICAP server performs classification on a per subscriber basis the cache must be disabled since the URIs are cached on a per content filtering profile basis.

The PGW can cache either an exact URI or a URI prefix based on how the URI was resolved:

— URIs in the locally configured URI lists are prefixes and are cached as prefix URIs.

— URIs resolved through the ICAP server may either be prefix or exact URIs in accordance with directives received from the ICAP server. For detailed information, see ICAP Interface Description. If no directives are received from the ICAP server, the URI is cached as an exact entry.

Exact cache entries have a higher precedence than prefix entries. When looking up a URI in the cache, the PGW attempts to find an exact URI entry that is identical to the requested URI. If the exact URI entry is not found in the cache, then the PGW attempts to find a prefix entry that is a prefix of the requested URI.

Note: Actions determined by the Error policy are never cached.

The PGW can be configured to accept cache control directives from the ICAP server. This configuration allows the ICAP server to indicate if the URI and associated action should be cached or not. For more information, see ICAP Interface Description.

By default, the PGW ignores cache control directives. For information on how to configure ICAP cache control, see Content Filtering Configuration.

6.1 Cache Flushing

The cache is flushed in the following cases:

— When the PGW receives a modified `IsTag` value in a `REQMOD Response` or `OPTIONS Response` message from the ICAP server

— When the content filtering configuration is modified

7 Deployment Scenario

In the deployment scenario, the PGW queries the ICAP server for URI categories based on the requested URI. Figure 5 shows the deployment scenario.

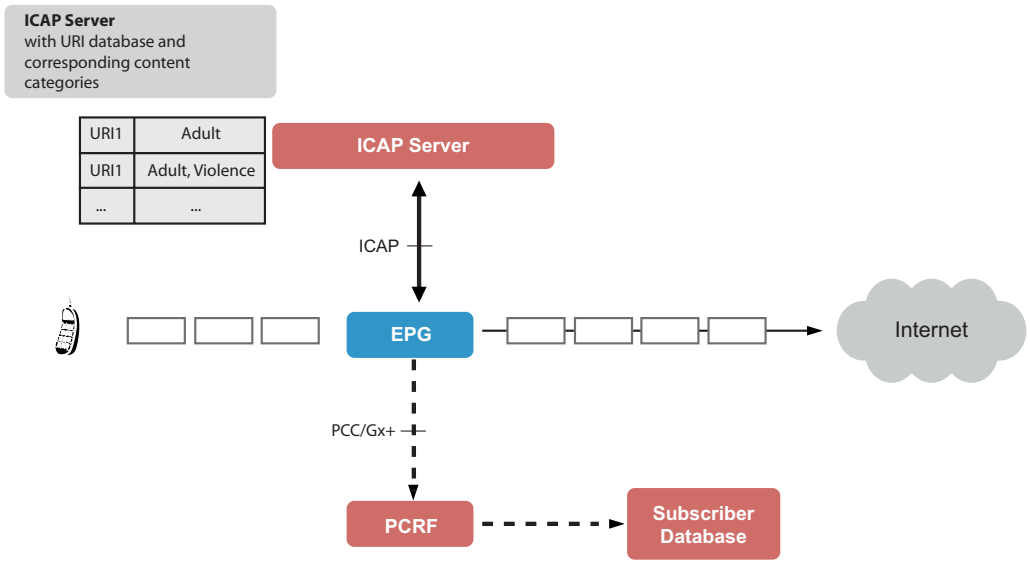


Figure 5 Content filtering Deployment Scenario

Content filtering in this deployment involves the following procedure:

1. The UE initiates a PDN connection.
2. If PCC is deployed, the PGW initiates a PCC session with the PCRF. A content filtering profile for the PDN connection is selected according to Section 4 on page 7.
3. The UE requests web content.
4. If a content filtering profile has been selected for the PDN connection, the PGW applies a policy action according to the following procedure:
    1 The PGW checks for the URI in the pass, block, and redirect lists configured in the content filtering profile selected for the PDN connection.
    2 If a policy action for the requested URI is not found in the URI lists, the PGW queries the ICAP server for the category of the requested content.
    3 The ICAP server resolves one or more content categories for the requested URI, and returns a successful ICAP response with the list of resulting categories.
    4 The PGW determines the policy actions corresponding to the resulting content categories, and applies the most restrictive policy.

7.1 Content Filtering Signal Flow Example

This section presents an example traffic case of using content filtering in the PGW.

An overview of the signaling involved in this traffic case is shown in Figure 6. For the purpose of this example, the following assumptions are made:

— A content filtering profile has been selected for the PDN connection.

— The selected content filtering profile includes a list of categories to be redirected to a specified destination.

— ICAP communication is enabled for the selected content filtering profile.

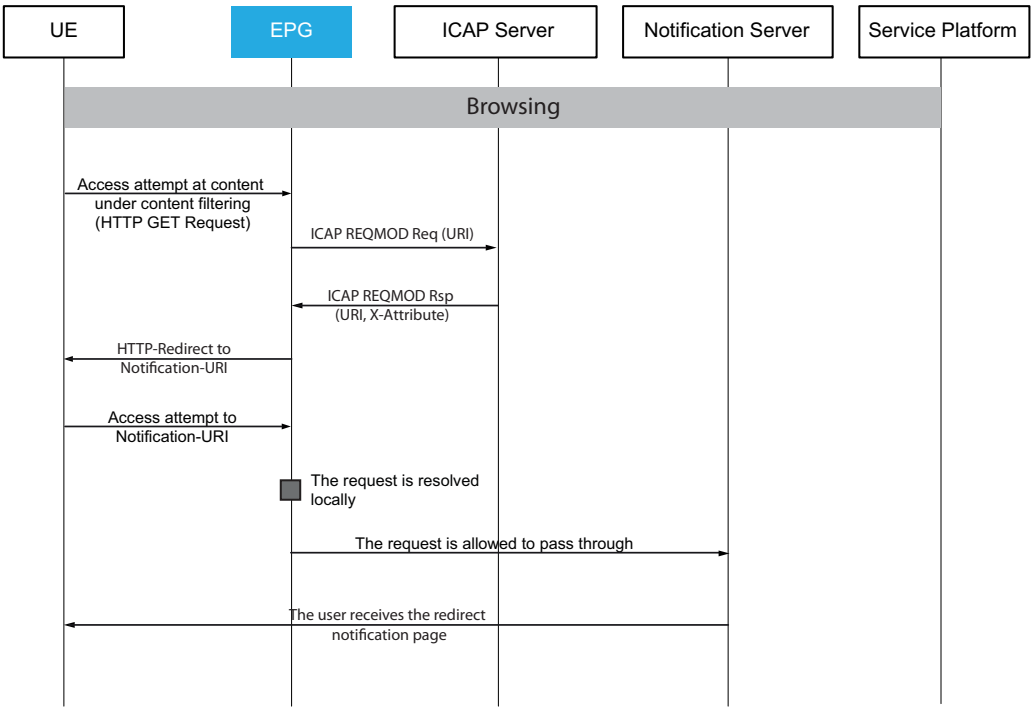


Figure 6 Call Flow for Content Filtering Policy Redirect

The following signaling is involved in this example:

1. The UE requests a web resource using a HTTP URI.
2. The PGW checks the URI lists configured for the content filtering profile, and does not find a match for the requested URI.
3. The PGW sends a request to the ICAP server, including the requested URI.
4. The ICAP server responds with a content category for the requested URI.
5. The PGW detects that the selected content category is configured to be redirected, according to the selected content filtering profile, and sends a `HTTP Redirect` message to the UE.
6. The UE sends a `HTTP GET` request for the redirect URI to the PGW.
7. The request is resolved locally in the PGW.
8. The PGW sends a request to the notification server.

9. The UE is redirected to the configured redirect destination, and is provided information about the reason for the redirect.

For information about the signaling involved during HTTP redirect, see Traffic Redirection.

7.2 Cache Enabled Signal Flow Example

This section presents an example traffic case of using the cache in the PGW. An overview of the signaling involved in this traffic case is shown in Figure 7. For the purpose of this example, the following assumptions are made:

— The same content filtering profile is selected for two different UEs.

— ICAP communication is enabled for the selected content filtering profile.

— The cache is enabled.

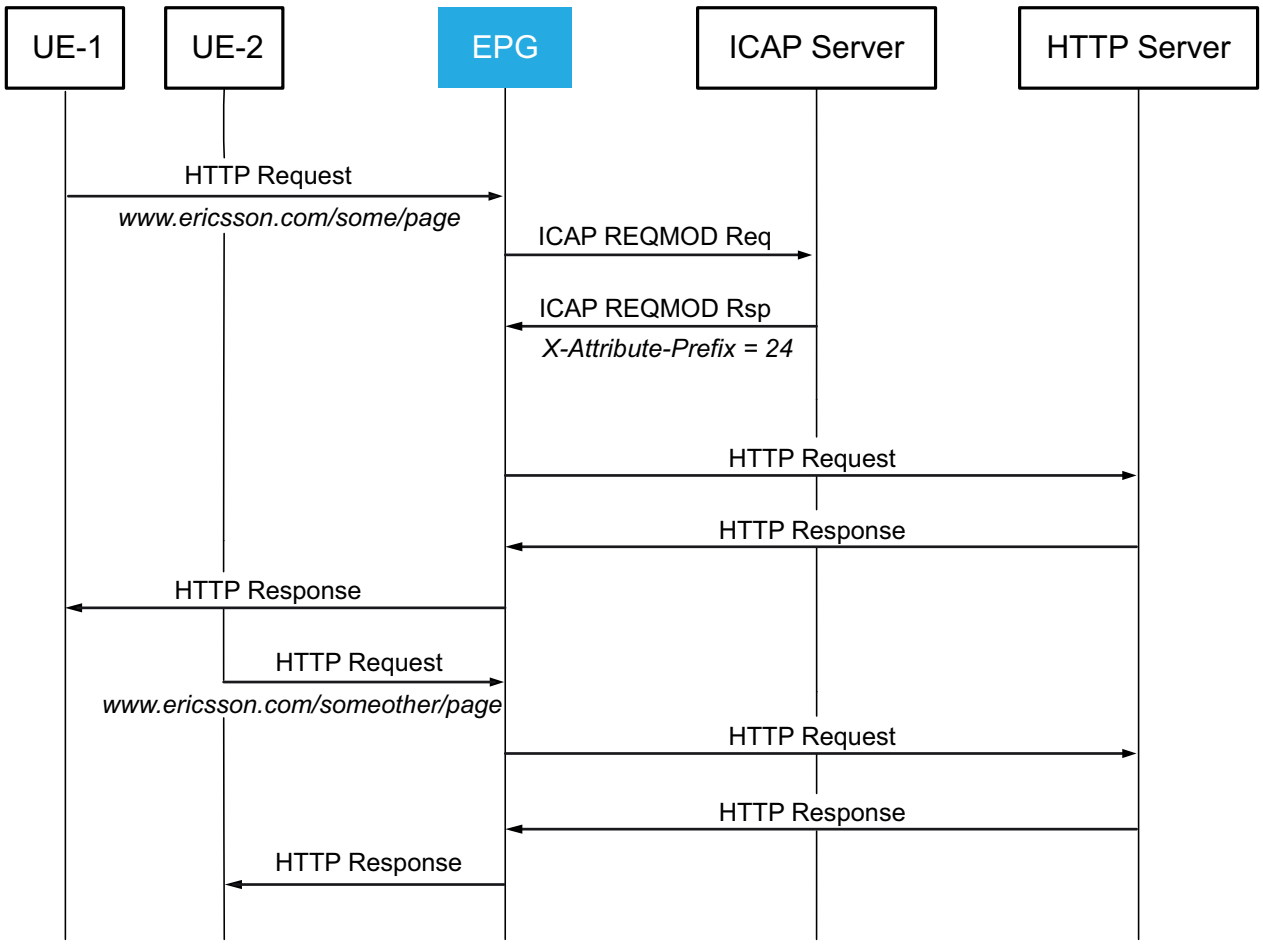


Figure 7 Call Flow for Content Filtering When Cache is Enabled

1. The first UE requests a web resource.

2. The PGW checks the cache and URI lists configured for the content filtering profile, but does not find a match for the requested URI.
3. The PGW sends a request to the ICAP server, including the requested URI.
4. The ICAP server responds with a content category for the requested URI and also sets the value of the `X-Attribute-Prefix` to 24.
5. The PGW detects that the selected content category matches a pass policy, and that the `X-Attribute-Prefix` is equal to the length of the domain name and the protocol specifier. The PGW caches the domain `http://www.ericsson.com/`.
6. The PGW forwards the `HTTP Request` to the HTTP server and caches the action for the domain.
7. The HTTP server sends an `HTTP Response` to the PGW.
8. The PGW forwards the `HTTP Response` to the UE.
9. The second UE sends an `HTTP Request` for the same domain, but for another URI, to the PGW.
10. The PGW detects that the domain is cached and the action is pass, and forwards the `HTTP Request` to the HTTP server.
11. The HTTP server sends an `HTTP Response` to the PGW.
12. The PGW forwards the `HTTP Response` to the UE.

Reference List

Standards

[1] Hypertext Transfer Protocol -- HTTP/1.1, IETF RFC 2616

[2] Hypertext Transfer Protocol version 2, draft-ietf-httpbis-http2-17, https://tools.ietf.org/html/draft-ietf-httpbis-http2-17

[3] Uniform Resource Identifiers (URI): Generic Syntax, RFC 2396

[4] Transport Layer Security (TLS) Extensions: Extension Definitions, RFC 6066