Content Filtering, Event Detail Records, and X-Header Enrichment Support

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The SMF supports the following functionality:

- Content Filtering
- Event Detail Record (EDR)
- X-header Enrichment

Content Filtering Support

The Content Filtering (CF) service prevents subscribers from inadvertently getting exposed to universally unacceptable content, or content that is inappropriate as per subscriber preferences. Based on the URLs in the subscriber requests, the CF service filters HTTP and WAP requests from mobile subscribers. Operators can filter and control the content for an individual subscriber to access.

The CF service provides the following solutions:

- URL Blacklisting—In this solution, all HTTP or WAP URLs in subscriber requests must match against a database of "blacklisted" URLs. If there is a match, it discards the flow, redirects, or terminates as per the configuration. In case of no match, subscribers view the content as usual.

  URL Blacklisting may not be a subscriber opt-in service. Operators can enable URL Blacklisting either for all subscribers or for a subset of subscribers. Typical cases include applying a blacklisted database of child porn URLs to all subscribers so that they are inadvertently not exposed to the universally unacceptable content.

- Category-based Static Content Filtering—In this solution, all HTTP or WAP URLs in subscriber requests must match against a static URL categorization database. Action initiates based on the URL's category and as per the configuration in the subscriber CF policy. Possible actions include:
  - Permitting
  - Blocking
  - Redirecting
  - Inserting content

EDR Support

EDRs are usage records with support to configure content information, format, and generation of triggers by the system administrative user. The EDRs are generated according to explicit action statements in rule commands. Several EDR schema types, where each schema type includes a series of analyzer parameter names, exist in the EDR. The EDRs are generated in CSV format at the time of each event.

The EDRs are stored in timestamped files that you can download through SFTP from the configured context. The EDRs are generated on per flow basis, and they catch whatever bytes get transmitted over that flow including those retransmitted.

Metadata Provided by SMF for EDR

The SMF provides the following metadata to the User Plane Function (UPF), which includes the data in the generated EDRs:

- Called-Station-ID: Specifies the DNN for the session
- Calling-Station-ID: Specifies the MSISDN of the UE
- RAT Type: RAT type for the current session (NR or EUTRAN)
- ULI: User location for the current session

The UPF receives the above data in the "Subscriber Parameters" IE in the PFCP Session Establishment Request message. The RAT type and ULI can change during the lifetime of session (for events, such as 5G to 4G handover). The UPF receives the changed values of these parameters in the PFCP Session Modification Request message.

Note

- All the parameters are always sent from the SMF to the UPF irrespective of EDR configuration being available. These parameters ensure that any change in configuration after the session creation is immediately applied on the UPF.
- The SMF supports EDR-related configurations. However, the SMF does not require these configurations for its functionality. These configurations are sent to the UPF through RCM.

X-Header Insertion Support

With the X-Header Insertion and X-Header Encryption features, collectively known as Header Enrichment, you can append headers to HTTP or WSP GET and POST request packets, and HTTP response packets for use by end applications. For example, mobile advertisement insertion (MSISDN, IMSI, IP address, user-customizable, and so on.

Supported X-Header Information

Out of all the configurable X-header information, some information requires control plane (SMF) to send the corresponding values to the user plane (UPF). The following table lists the information that is sent from the SMF to the UPF for X-header Insertion support.

Xheader Field	Description	Present in Session Establishment	Modified in Session Modification
String Constant	Inserts the configured string in xheader	N/A	N/A
Charging ID	Per Flow/Bearer Charging Id	Yes	N/A
IMEI	IMEI for the call	Yes	N/A
IMSI	IMSI for the call	Yes	N/A
Rat-Type	RAT type for the UE session	Yes	Yes
s-mcc-mnc	MCC/MNC of the SGW/AMF	Yes	N/A
Sgsn-address	AMF/SGW address	Yes	Yes
ULI	User Location Info	Yes	Yes
GGSN-Address	N4/S5 endpoint of SMF	Yes	Yes
Radius-station-ID	MSISDN of the UE	N/A	N/A
Sn-rulebase	Rulebase for a call	Yes	Yes
Subscriber-ip-address	IP address allocated to UE	N/A	N/A
Msisdn-no-cc	Obtained from MSISDN	Yes	No

The subscriber-specific fields—IMSI, MSIDN, and IMEI—are encoded in the "User ID" standard IE. See, 3GPP 29.244, Section 8.2.101 for more information.

Rest of the fields are sent in the "Subscriber Parameters" proprietary AVP. Some fields, such as the "Rulebase" and "UE IP address", are sent as a part of the created PDRs.

Note

- All the parameters are always sent from the SMF to the UPF irrespective of whether X-header configuration is available. These parameters ensure that any change in configuration after session creation is immediately applied on the UPF.
- The SMF supports X-header Insertion-related configurations. The SMF does not require these configurations for its functionality. These configurations are sent to the UPF through the RCM.

Configuring Content Filtering, EDR, and X-Header Insertion Support

This section describes how to configure the following:

- Content Filtering
- Event Detail Records (EDRs)
- X-Header Enrichment

Configuring Content Filtering Support

This section describes how to configure CF support.

Note Apart from the following configurations, all other configurations are used only in the UPF, and are only sent from the SMF to the UPF via RCM. The SMF does not use these configurations.

Configuring Content Filtering under Active Charging Service

To configure CF support under the active charging service, use the following configuration:

```
configure
   active-charging service service_name
      content-filtering category policy-id cf_policy_id
         analyze priority priority { all | category category
          | x-category xcategory } action { allow |
          content-insert content_string | discard | redirect-url url |
          terminate-flow | www-reply-code-and-terminate-flow reply_code
          } [ edr edr_format] failure-action { allow |
          content-insert content_string | discard | redirect-url url
          | terminate-flow | www-reply-code-and-terminate-flow reply_code}
          [ edr edr_format]
          end
```

Configuring Content Filtering under Rulebase

To configure CF under the rulebase, use the following configuration:

```
configure
   active-charging service service_name
      content-filtering category policy-id cf_policy_id
      content-filtering mode category static-only
      end
```

Configuring Content Filtering under APN

To configure CF under the APN, use the following configuration:

```
configure
   context context_name
      apn apn_name
         content-filtering category policy-id cf_policy_id
         end
```

Content Filtering Policy ID on N7 Interface

The CF categories are configured under the active charging service under specific policy IDs. The rulebase and APN also have an associated policy ID. For any session, one policy ID can be associated with the session at anytime. The categories configured under that CF policy ID are applicable for the session on the UPF.

The PCF can override the CF policy ID by sending this value on the N7 interface. For this purpose, a proprietary IE is available in the YAML definition for the N7 interface. The hierarchy for the CF policy ID is as follows:

```
smPolicyDecision
   ciscoAvpSet:
      cfPolicyId: uint32 value
```

When the PCF does not send a CF policy ID, the existing CF policy ID in the rulebase configuration or the policy ID configured in the APN configuration is selected, in the order of precedence. This CF policy ID value is sent to the UPF in PFCP Session Establishment Request message in the "Subscriber Parameters" attribute. During PDU Session Modification, if the PCF changes the CF policy ID, the ID is sent to the UPF in PFCP Session Modification Request message.

Configuring EDR Support

The SMF supports EDR-related configurations. The SMF does not require configurations for EDR functionality. The required configurations are sent to the UPF through RCM.

To configure the EDR formats, use the following configuration:

```
configure
   active-charging service acs_service_name
      edr-format edr_format_name
         attribute attribute_name { [ format { MM/DD/YY-HH:MM: SS
         | MM/DD/YYYY-HH:MM:SS | YYYY/MM/DD-HH:MM:SS | YYYYMMDDHHMMSS
         | seconds } ] [ localtime ] | [ { ip | tcp } { bytes | pkts }
         { downlink | uplink } ] priority priority_value }
         rule-variable protocol rule priority priority
         event-label event_label priority  priority
         delimiter { comma | tab }
         end
```

Configuring X-Header Insertion Support

The SMF supports X-Header Insertion-related configurations. The SMF does not require configurations for X-Header Insertion functionality. The required configurations are sent to the UPF through RCM.

Configuring an X-Header Format

To create and/or configure an x-header format, use the following configuration:

```
configure
   active-charging service acs_service_name
      xheader-format xheader_format_name
         insert xheader_field_name { string-constant xheader_field_value
         | variable { bearer { 3gpp { apn | charging-characteristics
         | charging-id | imei | imsi | qos | rat-type | s-mcc-mnc
```

```
          | sgsn-address } | acr | customer-id | ggsn-address| mdn |
msisdn-no-cc
          | radius-string | radius-calling-station-id | session-id |
sn-rulebase |
          subscriber-ip-address | username } [ encrypt ] | http { host |
url } }
          end
```

Configuring Charging Action for Insertion of X-Header Fields

To configure a charging action for insertion of x-header fields, use the following configuration:

```
configure
   active-charging service acs_service_name
      charging-action charging_action_name
         xheader-insert xheader-format xheader_format_name [ encryption
         { rc4md5 | aes-256-gcm-sha384 [ salt ] } [ encrypted ] key key
         ] [ first-request-only ] [ msg-type { response-only
         | request-and-response } ] [ -noconfirm ]
         end
```

Bearer QCI Support

Feature Description

The User Plane function (UPF) requires the Bearer level information (BLI) for each QoS flow like QFI for 5G and Bearer Id for 4G, 5G QoS Identifier (5QI) allocation and retention priority (ARP), and Charging ID, to support inline services. The Bearer QCI Support feature facilitates this requirement with the SMF.

Note The Bearer QCI Support feature also includes support for Bli_ID and QFI values in the "Create PDR" message.

The SMF sends the Bearer QoS Class Identifier (QCI) Information Element (IE), which is cisco proprietary IE, in the PFCP session establishment request and PFCP session modification request. The UPF implicitly derives the deletion indication. If a BLI ID is no longer associated with any PDR, the UPF removes it from the PFCP session context. The UPF adds the 5QI or QCI value in the EDR. Currently, the Bearer QCI field is used for 5G to add the 5QI.

The BLI is reported to the UPF as shown in the following table. The formats and encoding and decoding of these IEs are the same as other 3GPP IEs as described in *TS 29.244*.

Information Elements	Mandatory /Optional	Data Type	Description
valid		guint8	Validity of the Bearer level information IE

bli_id	Mandatory	PfcpBliId	QoS flow identifier (QFI) of 5G or Bearer ID (4G)
qci	Optional	PfcpQci	Used by PGW-C, not relevant for SMF
_5qi	Optional	Pfcp5qi	5QI associated with the QoS flow
arp	Mandatory	PfcpArp	ARP comprises of pre-emption capability, Pre-emption vulnerability, and priority level.
charging_id	Optional	PfcpChargingId	Charging ID associated with the QoS flow or Bearer (or both).

Bearer Level Information ID

The unique ID for each Bearer level information sent from SMF. The recommended value of this IE is QFI (in 5G) or Bearer-id (in 4G). The format of IE is as below:

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 232 (decimal)							
3 to 4	Length = 1							
5	BLI_ID value							
6 to n+4	These octets are present only if explicitly specified							

QCI : This is not applicable for 5G. It is used in CUPS, if required.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 233 (decimal)							
3 to 4	Length = 1							
5	QCI value							
6 to n+4	These octets are present only if explicitly specified							

5QI: The SMF uses this this IE to send the 5QI value.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**

1 to 2	Type = 234 (decimal)
3 to 4	Length = 1
5	5QI value
6 to n+4	These octets are present only if explicitly specified

ARP: The ARP value is sent with this IE.

Note From SMF, the ARP value is encoded as arp->pci)<<4) | arp->pl)<<2)| arp->pvi)

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 235 (decimal)							
3 to 4	Length = 1							
5	ARP value							
6 to n+4	These octets are present only if explicitly specified							

Charging ID: The Charging IE is sent with this IE.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 236 (decimal)							
3 to 4	Length = 1							
5	Charging Id value							
6 to n+4	These octets are present only if explicitly specified							

Triggers for Bearer Level Information IE

The following are the triggers for sending the BLI IE in PFCP messages:

PFCP Session Establishment Message

The Bearer level information IE is sent for each new QoS flow with the unique QFI ID. This IE is added in the policy decision in the N7 Policy Control Create Response message from the PCF. Therefore, SMF sends multiple instances of this IE, in a single PFCP message.

PFCP Session Modification Message:

Any new QoS flow addition or new PCC rule referring to an existing QoS flow that results in a new QER or PDR IE that has a new Bearer level information IE for each unique QFI ID.

The BLI IE is not included in the PFCP Session Modification Message if the modification is for IDFT tunnels.