Content Filtering and X-Header Enrichment

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
- X-header Enrichment

Content Filtering

Feature Description

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.

Configuring Content Filtering

This section describes how to configure CF support.

Note Apart from the following configurations, all other configurations are used only in the UPF, and SMF sends it to the UPF. The SMF doesn't use these configurations. For more information on how to enable the feature on UPF, see the *UCC 5G UPF Configuration and Administration Guide*.

Configuring Content Filtering under Active Charging Service

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

```
config
   active-charging service service_name
      content-filtering category policy-id cf_policy_id
      end
```

NOTES:

- **content-filtering category policy-id** *cf_policy_id*: Specify the CF policy number. *cf_policy_id* must be an integer in the range of 1-4294967295.

Configuring Content Filtering under Rulebase

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

```
config
   active-charging service service_name
      rulebase rulebase_name
         content-filtering category policy-id cf_policy_id
         end
```

NOTES:

- **content-filtering category policy-id** *cf_policy_id*: Specify the CF policy number. *cf_policy_id* must be an integer in the range of 1-4294967295.

Configuring Content Filtering under APN

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

```
config
   apn apn_name
      content-filtering category policy-id cf_policy_id
      end
```

NOTES:

- **content-filtering category policy-id** *cf_policy_id*: Specify the CF policy number. *cf_policy_id* must be an integer in the range of 1-4294967295.

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.

X-Header Insertion

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 SMF to send the corresponding values to the UPF. The following table lists the information that is sent from the SMF to the UPF for X-header insertion.

Table 3: X-header Information

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

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

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.