Device ID in EDNS0 Records

Revision History

Note Revision history details are not provided for features introduced before release 21.24.

Table 1: Revision History

Revision Details	Release
The feature is supported in 21.25 and later releases.	21.25
First introduced.	Pre 21.24

Feature Description

The Device ID in EDNS0 offers each enterprise with a customized domain blocking through Umbrella.

To enable the Device ID in EDNS0 functionality:

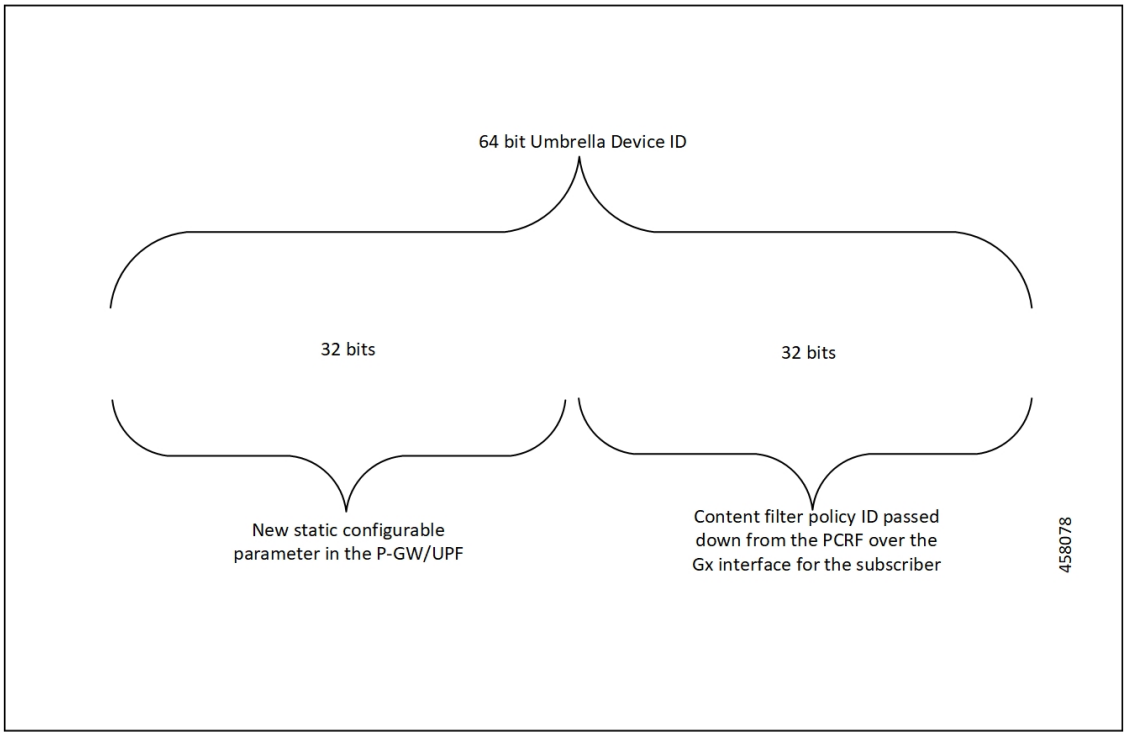
- The UP must reformat a subscriber DNS request into an EDNS0 request.
- The UP must include an Umbrella "Device ID" in the EDNS0 packet so that the Umbrella DNS resolver can use the Device ID to apply the domain filter associated or configured with the Device ID in the EDNS0 packet.

The Control Plane (CP) receives the domain filtering policy ID from PCRF or PCF. The CP passes the domain filtering policy ID to the User Plane (UP) in Subscriber Parameters. The UP uses the domain filtering policy ID to apply domain filtering functionality to the subscriber.

How it Works

The EDNS0 packet receives the 64-bit device ID as OPT RR data. The first 32 bits of all device IDs is a fixed value configured in the UP. The last 32 bits of a subscriber device ID is the content filter ID value received from PCRF or PCF. The UP concatenates the two 32-bit values to build a subscriber-full 64-bit Device ID for populating the subscriber EDNS0 queries. The CLI command configures the first 32 bits of static Device ID value. If you do not configure the 32-bit static prefix CLI command, the outgoing packet displays the device-ID = 32-bit CF PolicyID.

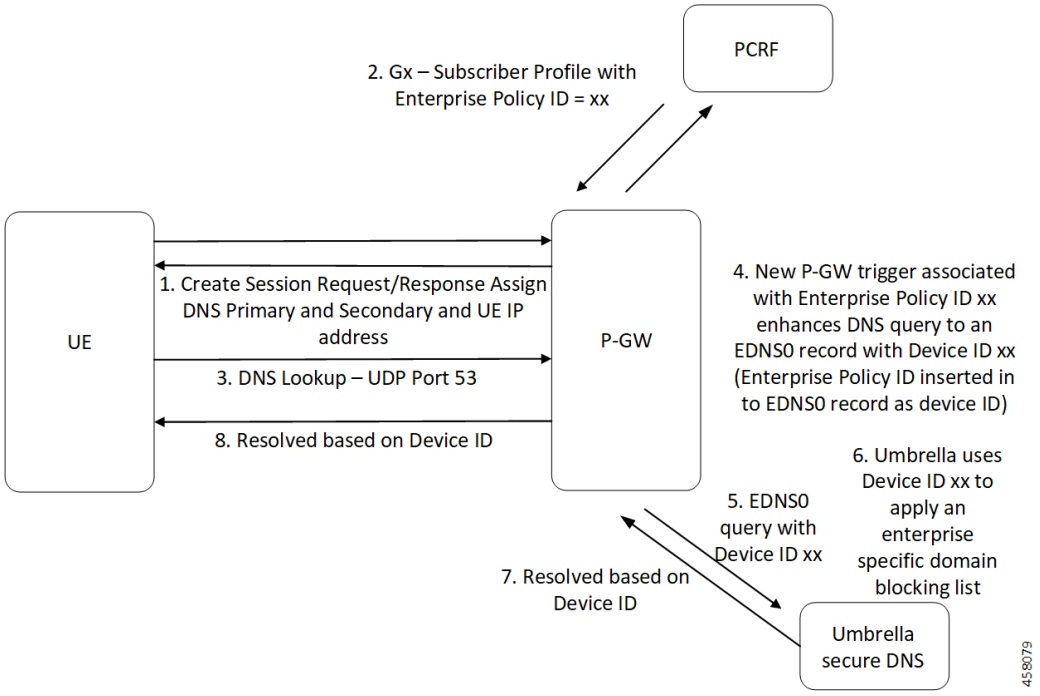
The Device ID number in the EDNS0 record allows the Umbrella DNS system to apply a custom set of domain filters for the EDNS0 queries.



Process Flow

The following process flow describes the Content Filtering enhancement to insert Device ID in EDNS0 records:

Figure 1: Inserting Device ID in EDNS Records



EDNS0 Packet Format

The enterprise policy ID (CF_POLICY_ID) from PCRF helps to create the Device ID. The CP sends the Device ID to the UP. Adding the Device ID to the DNS packet helps in creating the EDNS0 packet. The format of EDNS0 packets is specified by RFC2671.

The following are specifics of the packet format:

- The following is the structure for the fixed part of an OPT RR:

```
Field Name   Field Type     Description
-------------------------------------------------------
NAME         domain name    empty (root domain)
TYPE           u_int16_t          OPT
CLASS          u_int16_t          sender's UDP payload size
TTL            u_int32_t          extended RCODE and flags
RDLEN          u_int16_t          describes RDATA
RDATA          octet stream       {attribute, value} pairs
```

- The following is the variable part of an OPT RR encoded in its RDATA:

```
     +0 (MSB)                            +1 (LSB)
   +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
 0: |                         OPTION-CODE                           |
   +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
 2: |                         OPTION-LENGTH                         |
   +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
 4: |                                                               |
   /                         OPTION-DATA                           /
   /                                                               /
   +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

  - OPTION-CODE: Assigned by IANA

- OPTION-LENGTH: Size (in octets) of OPTION-DATA
- OPTION-DATA: Varies as per OPTION-CODE

Example:

If the policy-id received from PCF or PCRF is "1234" and static prefix configured on UP is "5678, the 64-bits Device-ID will be "0000162e000004d2".

- 0000162e -- 5678 (decimal)
- 000004d2 -- 1234 (decimal)

RDATA 69 42 00 0f 4f 70 65 6e 44 4e 53 00 00 16 2e 00 00 04 d2

- 6942 -- option-code
- 000f -- option-length
- 4f70656e444e53 -- OpenDNS (string)
- 0000162e -- 5678 (MSB)
- 000004d2 -- 1234 (LSB)

EDNS0 with IP Readdressing

The CLI command configured within trigger action readdresses the DNS traffic to the Umbrella DNS. This CLI uses the existing readdress-server list configuration from the ACS service. Readdressing of packets based on the destination IP address of the packets enables redirecting gateway traffic to configured server or port in the readdressed-server list.

Behavior and Restrictions

This feature has the following behaviors and restrictions:

- Evaluates the trigger condition at flow creation time. Any change in the trigger condition in between the flow does not affect the existing flow but affects the new flows.
- Any change to trigger action is applicable on the same flow.
- Neither CF nor EDNS is enforced when the CF Policy ID range is defined but service-schema is not defined, or the trigger condition pertaining to EDNS is not configured.
- If no CF Policy ID is received from Gx, range check is not performed, and content filtering works as defined in rule base.
- Cases where the "security-profile" CLI command is not associated with the EDNS format CLI under trigger action, the Device ID in the outgoing EDNS packet is sent only with the 32-bit CF Policy ID.
- DNS queries with type other than A, AAAA, CNAME, NS, PTR, SRV, TXT, NULL must not be EDNS converted.
- CF Policy ID change over Gx in between inflows is not applicable for the current flows. The current flows continue to insert the CF Policy ID present at the time of flow creation.

Limitations

This feature has the following limitations:

- Does not support the EDNS response packet reformat.
- The UP must be able to include the IMSI MSISDN tag value in the EDNS0 queries. This feature does not support the encrypted IMSI in EDNS0 packet and also the EDNS fields in the following configuration.

```
configure
   active-charging-service service_name
      edns
         fields fields_name
            tag default device-id
            tag 101 imsi encrypt
            tag 102 pgw-address
            end
```

Configuring EDNS Format and Trigger Action

Configuring DNS Filter

Use the following configuration to enable or disable DNS filtering:

```
configure
   active-charging-service service_name
      content-filtering range start_min_val to end_max_val
      no content-filtering range
      end
```

NOTES:

- If the range parameter is set from 10 to 1000, any subscriber profile with a content filtering policy ID from 10 to 1000 uses the standard content filtering functionality. Any subscriber profile with a content filtering policy ID higher than 1000 or lower than 10 triggers the EDNS0 functionality.
- When DNS filtering is disabled, the standard content filtering policies resume as configured or as received from PCF.

Configuring EDNS Packets

Use the following configuration to configure the EDNS packet action and format under the active-charging service:

```
configure
   active-charging-service service_name
      trigger-condition trigger_condition_name
         external-content-filtering
            app-proto = dns
            end
```

NOTES:

- **external-content-filtering**: Enable the EDNS0 feature when this flag is set to true along with the range criteria. By default, this flag is disabled.
- **app-proto = dns**: Avoid IP readdressing of non-DNS traffic. If this command is enabled with multiline-or CLI, then all DNS traffic is EDNS encoded.

The following configuration defines the EDNS format to be inserted in the EDNS packet:

```
configure
  active-charging-service service_name
    trigger-action trigger_action_name
      edns-format format_name
        security-profile profile_name
          flow action readdress server-list server_list_name [ hierarchy ]
 [ round-robin ] [ discard-on-failure ]
           end
```

NOTES:

- **trigger-action** *trigger_action_name*: Enable the flow-action CLIs under trigger action.
- **edns-format** *format_name*: Use the EDNS format when EDNS is applied.
- **security-profile** *profile_name*: Define the security profile configuration in EDNS to add the Device-ID mapping.

Note This feature feature supports multiple security profiles.

- **flow action readdress server-list** *server_list_name* **[hierarchy] [round-robin] [discard-on-failure]**: Associate EDNS with IP readdressing. IP readdressing is used to readdress the packets to the configured server IPs. This CLI under trigger action supports only the server list configuration. It does not support single-server IP or port configuration such as charging-action.

Inserting CF Policy ID

Use the following configuration to insert the CF policy ID in EDNS:

```
configure
  active-charging-service service_name
    edns
      fields fields_name
        tag { val { imsi | msisdn | cf-policy-id } }
        end
```

NOTES:

- To configure the 32-bit, static value is provided at the EDNS level with the security profile.

  ```
  security-profile security_profile cf-policy-id-static-prefix value
  ```

- To insert a new tag, specify the payload length value as an integer in the range 576 to 4096:

  ```
  tag default payload-length [ tcp | udp ] value
  ```

Sample Configuration

The following is a sample configuration for configuring the EDNS packets:

```
configure
   active-charging service ACS
      content-filtering range 10 to 100

      ruledef dns-port
         udp either-port = 53
         tcp either-port = 53
         multi-line-or all-lines
         rule-application routing
      #exit

      readdress-server-list re_adr_list_ta
         server 100.100.100.14
         server 2001::14
         server 100.100.100.15
         server 2001::15
       #exit

      rulebase test
         route priority 20 ruledef dns-port analyzer dns
         #exit

      edns
         security-profile sec_profile cf-policy-id-static-prefix 123456
         fields test_fields
            tag 26946 cf-policy-id
         #exit

         format test_format
            fields test_fields encode
         #exit

         trigger-action TA1
            edns format test_format security-profile sec_profile
            flow action readdress server-list re_adr_list_ta hierarchy
          #exit

         trigger-condition TC1
            external-content-filtering
            app-proto = dns
            #exit

         service-scheme SS1
            trigger flow-create
               priority 1 trigger-condition TC1 trigger-action TA1
         #exit

         subs-class SC1
            rulebase = test
            multi-line-or all-lines
         #exit

         subscriber-base SB1
            priority 1 subs-class SC1 bind service-scheme SS1
         #exit
end
```

Monitoring and Troubleshooting

Following are the show commands and outputs in support of enhance content filtering support to Insert device ID in EDNS0 records.

Show Commands and Outputs

The following show commands and outputs are modified in support of this feature:

show user-plane-service inline-services info

```
CF Range: Enabled
  Start Value:  1
  End Value:    1000
```

show user-plane-service statistics analyzer name dns

```
EDNS Over UDP:
EDNS Encode Success:            0         EDNS Encode Failed:      0
EDNS Encode Success Bytes:      0
EDNS Response Received:         0

EDNS Over TCP:
EDNS Encode Success:            0         EDNS Encode Failed:      0
EDNS Encode Success Bytes:      0
EDNS Response Received:         0
```

show subscribers user-plane-only full callid <call_id>

```
DNS-to-EDNS Uplink Pkts:     0       DNS-to-EDNS Uplink Bytes:     0
EDNS Response Received:      0
```

show user-plane-service edns all

```
Fields:
    Fields Name: fields_1
    tag 26946 cf-policy-id

    Fields Name: fields_2
    tag 2001 imsi
    tag 2002 msisdn
    tag 26946 cf-policy-id

    Format:
    Format Name: format_1
    fields fields_1 encode

    Format Name: format_2
    fields fields_2 encode

    Security-profile Name: high
    CF Prefix Policy ID: 1234
```

Trigger Action Statistics

Use the following show commands to view the trigger action statistics:

- **show user-plane-service statistics trigger-action all**

```
Trigger-Action: TA1
  Total EDNS PKTS           :  1
  Total readdressed Flows   :  1
  Total Trigger action(s)   :  1
```

- **show user-plane-service statistics trigger-action name** *trigger_action_name*

```
Trigger-Action: TA1
  Total EDNS PKTS           :  1
  Total readdressed Flows   :  1
  Total Trigger action(s)   :  1
```

- **show user-plane-service trigger-condition all**

```
Trigger-Condition: TC1
       External-content-filtering : Enabled
       App-proto : dns
       Multi-line-OR All lines : Disabled
```

- **show user-plane-service trigger-action all**

```
Trigger-Action: TA1
       HTTP Response Based TRM      : none
       HTTP Response Based Charging : none
       Throttle Suppress            : Disabled
       Flow Recovery                : Disabled
       Traffic Optimization         : Disabled
       Step Up GBR                  : Disabled
       Step Down GBR                : Disabled
       TCP Acceleration             : Disabled
       TCP Acceleration Threshold   : Disabled
       Service-Chain                : none
       UP-Service-Chain             : none
       EDNS-Encode                  : Enabled
       Flow-IP-Readdressing         : Enabled
```

Bulk Statistics

This feature supports the following bulk statistics in the ECS schema:

Table 2: ECS Schema

Statistics	Description
ecs-dns-udp-edns-encode-succeed	The number of DNS to EDNS converted packets over UDP.
ecs-dns-udp-edns-encode-failed	The number of failed DNS to EDNS conversions over UDP.
ecs-dns-udp-edns-encode-response	The number of responses received for EDNS query over UDP.
ecs-dns-tcp-edns-encode-succeed	The number of DNS to EDNS converted packets over TCP.
ecs-dns-tcp-edns-encode-failed	The number of failed DNS to EDNS conversions over TCP.
ecs-dns-tcp-edns-encode-response	The number of responses received for EDNS query over TCP.