



EDNS0 レコードのデバイス ID

- [マニュアルの変更履歴](#) (1 ページ)
- [機能説明](#) (1 ページ)
- [機能の仕組み](#) (2 ページ)
- [EDNS フォーマットとトリガーアクションの設定](#) (5 ページ)
- [モニタリングおよびトラブルシューティング](#) (8 ページ)

マニュアルの変更履歴



(注) リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

表 1: マニュアルの変更履歴

改訂の詳細	リリース
この機能は、21.25以降のリリースでサポートされています。	21.25
最初の導入。	21.24 より前

機能説明

EDNS0 のデバイス ID を使用すると、カスタマイズされたドメインを Cisco Umbrella を介してブロッキングできます。

EDNS0 機能でデバイス ID を有効にするには、次の手順を実行します。

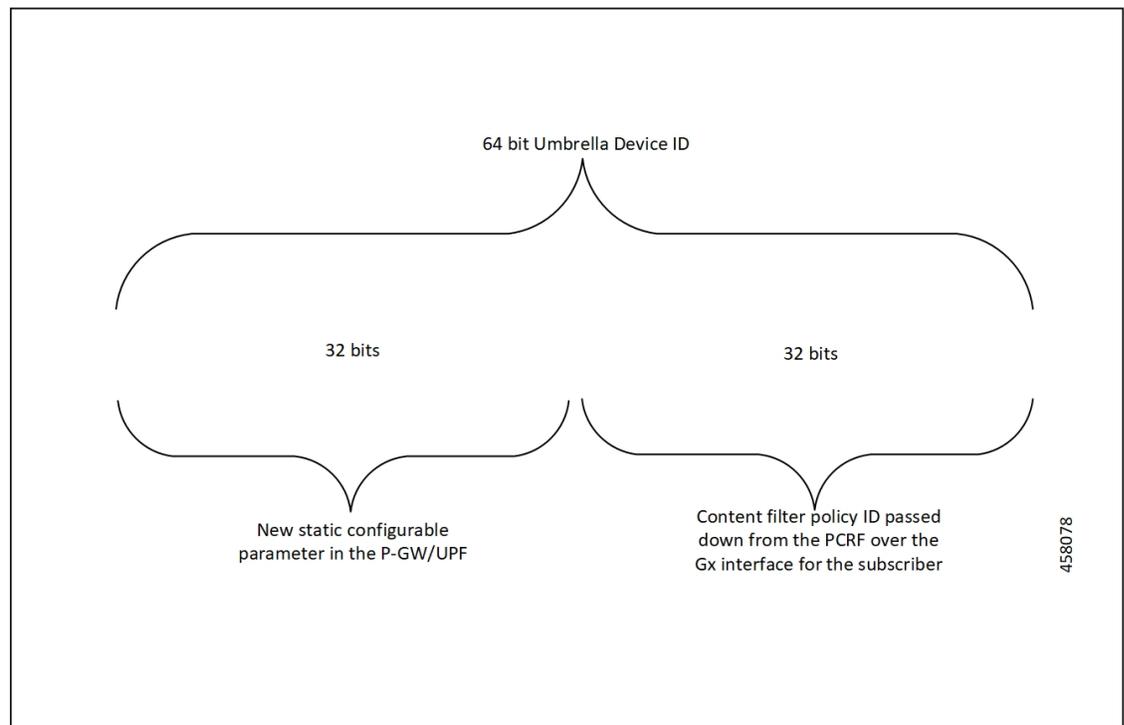
- UP はサブスクリバ DNS 要求を EDNS0 要求に再フォーマットする必要があります。
- UP では EDNS0 パケットに Cisco Umbrella の「デバイス ID」を含める必要があります。Cisco Umbrella DNS リゾルバはデバイス ID を使用して、EDNS0 パケット内のデバイス ID に関連付けられた、または設定されたドメインフィルタを適用できます。

コントロールプレーン（CP）は、PCRFまたはPCFからドメインフィルタリングポリシーIDを受信します。CPはドメインフィルタリングポリシーIDをサブスライバパラメータでユーザープレーン（UP）に渡します。UPはドメインフィルタリングポリシーIDを使用して、ドメインフィルタリング機能をサブスライバに適用します。

機能の仕組み

EDNS0 パケットが OPT RR データとして 64 ビットのデバイス ID を受信します。すべてのデバイス ID の最初の 32 ビットは、UP で設定された固定値です。サブスライバデバイス ID の最後の 32 ビットは、PCRF または PCF から受信したコンテンツフィルタ ID 値です。UP はこの 2 つの 32 ビット値を連結して、サブスライバ EDNS0 クエリに入力するための 64 ビットからなる完全なサブスライバデバイス ID を作成します。CLI コマンドによって、静的デバイス ID 値の最初の 32 ビットを設定します。32-bit static prefix CLI コマンドを設定しない場合、発信パケットには device-ID = 32 ビット CF PolicyID が表示されます。

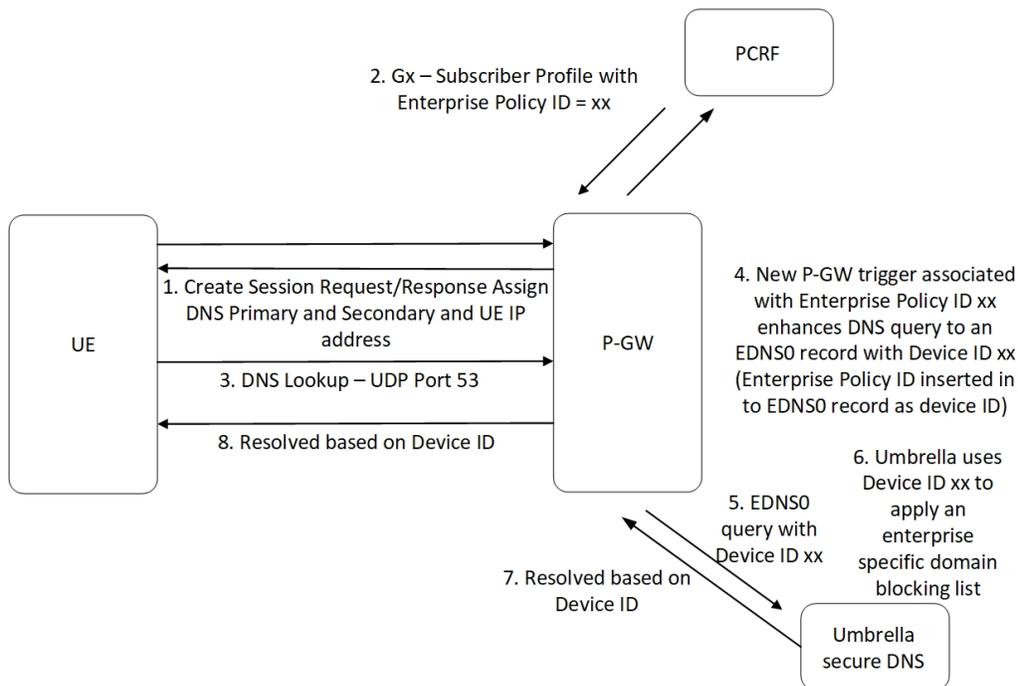
EDNS0 レコードのデバイス ID 番号により、Cisco Umbrella DNS システムは EDNS0 クエリにドメインフィルタのカスタムセットを適用できます。



プロセスフロー

次のプロセスフローは、EDNS0 レコードにデバイス ID を挿入するためのコンテンツフィルタリングの拡張機能を示しています。

図 1: EDNS0 レコードへのデバイス ID の挿入



4E9879

EDNS0 パケット形式

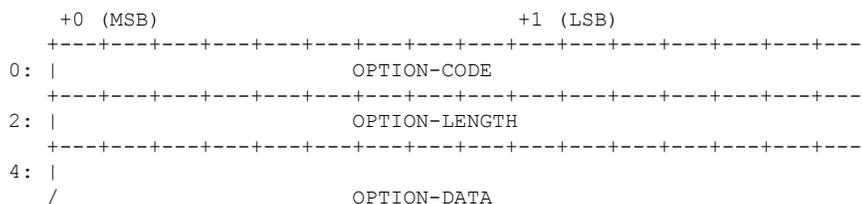
PCRF からのエンタープライズポリシー ID (CF_POLICY_ID) は、デバイス ID の作成に役立ちます。CP はデバイス ID を UP に送信します。DNS パケットにデバイス ID を追加すると、EDNS0 パケットの作成に役立ちます。EDNS0 パケットの形式は RFC2671 で指定されています。

次に、パケット形式の仕様を示します。

- 次に、OPT RR の固定部分の構造を示します。

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

- 次に、RDATA でエンコードされた OPT RR の可変部分を示します。



```

/
+-----+

```

- OPTION-CODE : IANA によって割り当て済み
- OPTION-LENGTH : OPTION-DATA のサイズ (オクテット単位)
- OPTION-DATA : OPTION-CODE によって異なる

例 :

PCF または PCRF から受信したポリシー ID が「1234」で、UP で設定された静的プレフィックスが「5678」の場合、64 ビットのデバイス ID は「0000162e000004d2」になります。

- 0000162e : 5678 (10 進数)
- 000004d2 : 1234 (10 進数)

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 (文字列)
- 0000162e : 5678 (MSB)
- 000004d2 : 1234 (LSB)

IP 再アドレス指定を使用した EDNS0

トリガーアクション内で設定された CLI コマンドにより、DNS トラフィックは Umbrella DNS に再びアドレス指定されます。この CLI は、ACS サービスの既存の再アドレスサーバーリスト設定を使用します。パケットの宛先 IP アドレスに基づいてパケットを再アドレス指定することで、再アドレス指定されたサーバーリスト内の設定済みサーバーやポートにゲートウェイトラフィックをリダイレクトできます。

動作と制限事項

この機能の動作と制約事項は以下のとおりです。

- フロー作成時にトリガー条件を評価します。フロー間のトリガー条件の変更は、既存のフローには影響しませんが、新しいフローに影響します。
- トリガーアクションの変更は、同じフローに適用されます。
- CF ポリシーの ID 範囲は定義されているが、サービススキーマが定義されていない場合、または EDNS に関連するトリガー条件が設定されていない場合、CF も EDNS も適用されません。

- Gx から CF ポリシー ID を受信しない場合、範囲チェックは実行されず、コンテンツフィルタリングはルールベースで定義されているとおりに機能します。
- 「security-profile」 CLI コマンドがトリガーアクションで EDNS 形式の CLI に関連付けられていない場合、EDNS 送信パケットのデバイス ID は 32 ビットの CF ポリシー ID でのみ送信されます。
- A、AAAA、CNAME、NS、PTR、SRV、TXT、NULL 以外のタイプの DNS クエリは、EDNS に変換することはできません。
- インフロー間の Gx に対する CF ポリシー ID の変更は、現在のフローには適用されません。現在のフローでは、フローの作成時に存在する CF ポリシー ID が引き続き挿入されます。

制限事項

この機能には、次の制限事項があります。

- EDNS 応答パケットの再フォーマットはサポートしていません。
- UP では、EDNS0 クエリに IMSI MSISDN タグ値を含めることができるようにする必要があります。この機能は、EDNS0 パケットの暗号化された IMSI と、次の設定の EDNS フィールドもサポートしていません。

```

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

```

EDNS フォーマットとトリガーアクションの設定

DNS フィルタの設定

DNS フィルタリングを有効または無効にするには、次の設定を使用します。

```

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

```

注：

- range パラメータが 10 ~ 1000 に設定されている場合、コンテンツ フィルタリング ポリシー ID が 10 ~ 1000 のサブスクリバプロファイルは、標準コンテンツフィルタリング

機能を使用します。コンテンツ フィルタリング ポリシー ID が 1000 より大きい、または 10 より小さいサブスクリバプロファイルは、EDNS0 機能をトリガーします。

- DNS フィルタリングが無効になっている場合、標準コンテンツ フィルタリング ポリシーは、設定または PCF からの受信内容に応じて再開されます。

EDNS0 パケットの設定

アクティブ課金サービスで EDNS0 パケットアクションおよびフォーマットを設定するには、次の設定を使用します。

configure

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

注：

- **external-content-filtering**：このフラグが「true」に設定され、範囲条件が指定されている場合に、EDNS0 機能を有効にします。デフォルトでは、このフラグは無効です。
- **app-proto = dns**：DNS 以外のトラフィックの IP アドレスの再指定を回避します。このコマンドが multiline-or CLI で有効になっている場合、すべての DNS トラフィックが EDNS0 でエンコードされます。

次の設定により、EDNS0 パケットに挿入される EDNS0 フォーマットを定義します。

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
```

注：

- **trigger-action trigger_action_name**：トリガーアクションで flow-action CLI を有効にします。
- **edns-format format_name**：EDNS0 が適用されている場合に EDNS0 フォーマットを使用します。
- **security-profile profile_name**：EDNS0 のセキュリティプロファイル設定を定義して、デバイス ID マッピングを追加します。



(注) この機能は、複数のセキュリティプロファイルをサポートしません。

- **flow action readdress server-list** *server_list_name* [**hierarchy**] [**round-robin**] [**discard-on-failure**] : EDNS を IP アドレス再指定に関連付けます。IP アドレス再指定は、設定済みのサーバー IP 宛てにパケットのアドレスを再指定するために使用されます。トリガーアクションのこの CLI は、サーバーリスト設定のみをサポートします。単一サーバーの IP やポート設定 (**charging-action** など) はサポートされません。

CF ポリシー ID の挿入

次の設定を使用して、EDNS に CF ポリシー ID を挿入します。

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

注 :

- 32 ビットを設定するため、セキュリティプロファイルを含む静的な値が EDNS レベルで提供されます。

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

- 新しいタグを挿入するには、ペイロード長の値を 576 ~ 4096 までの整数で指定します。

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

設定例

以下に、EDNS パケットを設定するための設定例を示します。

```
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

```

モニタリングおよびトラブルシューティング

以下に、EDNS0 レコードにデバイス ID を挿入するための拡張コンテンツフィルタリングをサポートする show コマンドとその出力を示します。

show コマンドと出力

この機能をサポートする、次の show コマンドと出力が変更されました。

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
```

トリガーアクション統計

トリガーアクションの統計を表示するには、次の show コマンドを使用します。

- **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

```

バルク統計情報

この機能では、ECS スキーマで次のバルク統計がサポートされます。

表 2: ECS スキーマ

統計	説明
ecs-dns-udp-edns-encode-succeed	UDP を介して DNS から EDNS に変換されたパケットの数。
ecs-dns-udp-edns-encode-failed	UDP を介した DNS から EDNS への変換に失敗した回数。
ecs-dns-udp-edns-encode-response	UDP を介した EDNS クエリに対して受信された応答の数。
ecs-dns-tcp-edns-encode-succeed	TCP を介して DNS から EDNS に変換されたパケットの数。
ecs-dns-tcp-edns-encode-failed	TCP を介した DNS から EDNS への変換に失敗した回数。
ecs-dns-tcp-edns-encode-response	TCP を介した EDNS クエリに対して受信された応答の数。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。