L7 PCC ルール

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。

改訂の詳細	リリース
初版	21.24 より前

機能説明

この機能により、L7 アナライザ機能が CUPS アーキテクチャでサポートされます。

次の L7 アナライザがサポートされています。

- HTTP
- HTTPS
- RTP/RTSP
- FTP
- DNS
- コンテンツ フィルタリング
- DNS スヌーピング

次の課金アクションがサポートされています。

- 廃棄
- 終了フロー
- リダイレクト（該当する場合）

機能の仕組み

この項では、この機能の一部としてサポートされている L7 アナライザ機能の概要について説明します。

コンテンツ フィルタリング

コンテンツフィルタリングは、3GPP および 3GPP2 ネットワークで使用可能なインラインサービスです。HTTP リクエスト内の URL に基づいてモバイルサブスクライバからの HTTP リクエストをフィルタ処理します。これにより、オペレータは個々のサブスクライバがアクセスできるコンテンツをフィルタ処理して制御できるため、サブスクライバが常識的に容認されないコンテンツや望まないコンテンツに思いがけずさらされることはありません。

コンテンツフィルタリング機能は、非 CUPS アーキテクチャで実装されているものと同じです。詳細については、『 *CF Administration Guide*』 の「 *Content Filtering Support Overview*」の章 [英語] を参照してください。

コンテンツフィルタリングの設定

コンテンツフィルタリングを有効にするには、次の追加設定を使用します。

```
configure
  require user-plane content-filtering
    content-filtering category database directory path path_address
    content-filtering category database max-version version_number
    end
```

（注） コンテンツフィルタリングを有効にするには、ブート時に上記の設定をユーザープレーンで設定する必要があります。ユーザープレーン設定後に上記の設定を定義すると、エラーや不整合が発生します。

（注） この機能を有効にするには、ユーザープレーンのライセンスと既存のコンテンツ フィルタリング ライセンスがユーザープレーンで必要です。

（注） ICSR ユーザープレーン 1:1 の場合、データベースは両方の UP に個別にロードされます。コントロールプレーンの残りのコンテンツフィルタリング設定はそのままです。コンテンツフィルタリングの設定は、コントロールプレーンからアクティブユーザープレーンにプッシュされ、次にスタンバイユーザープレーンにプッシュされます。

コントロールプレーンでの設定

次の設定例は、コンテンツフィルタリング機能に対応するためにコントロールプレーンで必要な変更を示しています。

```
config
            active-charging-service ACS
               content-filtering category policy-id 1
               analyze priority 1 category ABOR
               analyze priority 2 category ADVERT action allow
               analyze priority 2 category ADVERT action allow action content-insert
"Content Restricted : The Web Guard feature has been enabled on your line. Web Guard has
 restricted your access to this content. The person on your Wireless account who is
designated as the Primary Account Holder can disable this restriction through the account
 management website"
                exit
           rulebase cisco
              content-filtering mode category static-only
              content-filtering flow-any-error permit
              content-filtering category policy-id 5
```

コントロールプレーンの設定は、PFD メカニズムを使用してユーザープレーンにプッシュされます。

ユーザープレーンのコンテンツフィルタリング設定を検証するには、次の show コマンドを使用します。

- show user-plane-service rulebase name cisco
- show user-plane-service content-filtering category policy-id

ユーザープレーンでの CFDB の生成を確認するには、次の show コマンドを使用します。

- show content-filtering category database facility srdbmgr
- show content-filtering category database verbose debug-only
- show content-filtering category database verbose
- show content-filtering category database url
- show content-filtering category url

特定のサブスクライバの PCRF から受信したコンテンツ フィルタリング ポリシー ID は、コールの確立時にユーザープレーンに送信されます。PFCP メッセージの Sx 確立要求や Sx 変更要求には、CF ポリシー ID が含まれています。

ユーザープレーンの CF ポリシー ID を確認するには、次のコマンドを使用します。

show subscribers user-plane-only callid full all

CUPS のコンテンツフィルタリングをサポートするために、次のフィールドが表示されます。

- Content Filtering Policy ID

SRDB 要求/応答/CF ポリシーアクションをモニターするには、次の show コマンドを使用します。

- show user-plane-service inline-services content-filtering category statistics
- show user-plane-service inline-services content-filtering category statistics rulebase name
- show content-filtering category statistics
- show content-filtering category statistics facility srdbmgr instance 1
- show content-filtering category statistics volume all

（注） 非CUPSアーキテクチャでコンテンツフィルタリング用に定義された既存のすべてのバルク統計情報は、CUPS にも適用できます。

制限事項

- ダイナミック コンテンツ フィルタリング モードはサポートされていません。
- ルールベースコマンド **content-filtering flow-any-error [permit | deny]** はサポートされていません。

DNS

SM-P へのオフロード

DNS パケットは SM-P にオフロードされません。

課金

DNS パケットは SM-P で課金されます。

ルールの照合

この機能は、非 CUPS アーキテクチャと同じです。

統計

DNSに関連する統計情報を取得するには、CLI コマンド**show user-plane-service statistics analyzer name dns** を使用します。

DNS スヌーピング

充電中

DNS スヌーピングの課金は SM-P で実行されます。

ルール定義

ルール定義のホスト名（domain-names）とホスト名の一部を指定するには、次の CLI コマンドを使用します。

```
ruledef <ruledef_name>
        ip [server-domain-name {contains|=|ends-with|starts-with}
<url_string>]
        ip [server-domain-name {contains|=|ends-with|starts-with}
<url_string>]
        multi-line-OR enabled
```

ip server-domain-name のルールラインを削除するには、この CLI の no バージョンを使用します。

```
ruledef <ruledef_name>
   no ip [server-domain-name {contains|=|ends-with|starts-with}
<url_string>]
   exit
```

ECS レベルで DNS エントリについて設定可能なタイマーには、次の CLI を使用します。

```
configure
         active-charging service service_name
            ip dns-resolved-entries timeout <value_secs>
            end
```

ip server-domain-name キーワードを含む ruledef が定義され、ルールベースで使用されるたびに、インスタンス単位でルールベースごとに ip-table が作成されます。

ルールの照合

この機能は、非 CUPS アーキテクチャの機能と同じです。

show CLI

次の CLI を使用して、DNS IP エントリ：**show user-plane-service [statistics dns-learnt-ip-addresses {summary | sessmgr instance <id> |all [verbose] }]** のテーブルを確認します。

バルク統計情報

DNS スヌーピング機能をサポートするために、次のバルク統計情報を使用できます。

- ecs-dns-learnt-ipv4-entries
- ecs-dns-flushed-ipv4-entries
- ecs-dns-replaced-ipv4-entries

- ecs-dns-overflown-ipv4-entries
- ecs-dns-learnt-ipv6-entries
- ecs-dns-flushed-ipv6-entries
- ecs-dns-replaced-ipv6-entries
- ecs-dns-overflown-ipv6-entries

前述のバルク統計情報は、非 CUPS アーキテクチャと同様に ECS スキーマに追加されます。

（注） SNMP トラップ生成コマンドは、CUPS DNS スヌーピング機能ではサポートされていません。

FTP

SM-P へのオフロード

FTP データの場合のみ、TRM エンゲージメントが実行されます。FTP データフローは、SM-P へのオフロードに適しています。

制御 FTP フローに対する TRM エンゲージメントはありません。

課金

FTP パケットは SM-P で課金されます。

ルールの照合

この機能は、非 CUPS アーキテクチャと同じです。

統計

FTP に関連する統計情報を取得するには、CLI コマンド **show user-plane-service statistics analyzer name ftp** を使用します。

HTTP

SM-P への HTTP オフロード

HTTP リクエスト/応答ヘッダーが完了すると、次の場合にアップリンク/ダウンリンクのデータパケットが VPP にオフロードされます。

- Content-Length：ボリュームベースのオフロードは、GET や POST などのメソッドでサポートされます。チャンクエンコーディングによるデータ転送メカニズムを使用した HTTP フローは、HTTP で定義されているメソッドに関係なくオフロードされません。ストリームがコンテンツ長に基づいてオフロードされた場合、もう一方のストリームも、前者がオンロードされなくなるまでオフロードされます。

- CONNECTメソッド：フローがCONNECTにアップグレードされると、アップリンクとダウンリンクの両方のストリームがオフロードされるメソッド。
- WebSocket メソッド：フローが WebSocket プロトコルとして分類されると、アップリンクとダウンリンクの両方のストリームがオフロードされます。
- ストリームは、次のいずれかの場合に SM-U アプリケーションにオンロードされます。
  - FIN パケットを受信した場合
  - コンテンツ長に違反している場合
  - PDN の更新

ヘッダー解析

非 CUPS 実装と同様に、rulebase に含まれる ruledef で定義されているヘッダーフィールドのみが解析されます。または、X-Headerなどの機能の場合は、一部のHTTPヘッダーフィールドに応じたリダイレクトが設定されます。

ルール照合

CUPS で行われるルール照合の方法に機能的な変更はありません。唯一の変更は、アップリンクとダウンリンクの両方に独自の TRM がある場合の TRM に特有なものです。

HTTP 課金

- 完全なパケットは SM-P で課金されます。
- 部分的パケットは、完成時にSM-Uで課金されます。部分的パケットを完成させるパケットも SM-U で課金されます。
- 連結パケットは SM-U で課金されます。
- 遅延課金が有効になっている場合：未課金のバイトがあると、パケットと合わせて未課金のバイトも SM-U で課金されます。
- 応答ベースの課金が有効になっている場合：応答を受信すると、アップリンクとダウンリンクの両方のパケットがSM-Uで課金されます。後続のアップリンクおよびダウンリンクパケットは、部分的パケットまたは連結パケットでない限り、SM-P で課金されます。

X-Header の解析とルール照合

x-header ルール行が含まれる ruledef が解析され、照合されます。

WebSocket

機能は、非 CUPS アーキテクチャと同じです。

TRM および応答ベースの課金

トランザクションルール照合では、フローが完全に分類されてはじめて、パケットごとのルール照合が回避されます。

方向ベースの TRM が CUPS で導入されました。1 つのフローに対して、アップリンク方向とダウンリンク方向の 2 つの TRM があます。1 つのパケットが TRM を有効にすると、後続の（TRM 対応）パケットも続けて同じルールに一致するため、効率的なルール照合が行われます。つまり、アップリンクパケットはアップリンク TRM キャッシュルールに一致し、ダウンリンクパケットはダウンリンク TRM キャッシュルールに一致します。

URL ベースのリダイレクト

機能は、非 CUPS アーキテクチャと同じです。

フローアクションの redirect-url で [encrypt] はサポートされません。現在、次のダイナミックフィールドがサポートされています。

- #HTTP.URI#
- #HTTP.HOST#
- #HTTP.URL#
- #ACSMGR_BEARER_CALLED_STATION_ID#
- #RULEBASE#
- #RTSP.URI#

X-Header の挿入

HTTP リクエストへの X-Header の挿入がサポートされます。動作は、非 CUPS アーキテクチャでの動作と同じです。SM-P へのオフロードに関しては、次のとおりです。

- パケットに X-Header が挿入されているフローはオフロードされません。
- X-Header 設定では、送信順序 CLI に関係なく、すべての TCP OOO パケットがバッファされ、順序変更後に送信されます。

X-Header 挿入統計 CLI

show user-plane-service statistics charging-action name *charging_action_name*

X-Header の挿入をサポートする次のフィールドが追加されました。

- 要求の場合：
  - 挿入された XHeader のバイト数
  - 挿入された XHeader のパケット数
  - 削除された XHeader のバイト数
  - 削除された XHeader のパケット数

• XHeader によって消費される IP フラグメント数

制限事項

- X-Header スプーフィングはサポートされません。
- 応答パケットへの X-Header への挿入はサポートされません。
- X-Header の暗号化では、RSA および RC4MD5 はサポートされますが、AES はサポートされません。
- X-Header のモニタープロトコルはサポートされません。
- パケットへの次の X-Header フィールドの挿入はサポートされません：QoS、UIDH、Customer ID、Hash Value、Time of the Day、Radius String、Session-Id、Congestion Level、User-Profile

HTTP アナライザ統計

HTTP アナライザに関連する統計を取得するには、**show user-plane-service statistics analyzer name http** CLI コマンドを使用します。

HTTPS

SM-P への HTTPS オフロード

HTTPS フローは、アプリケーションパケットの受信後に SM-P にオフロードされます。P2P アナライザの場合、P2P アナライザが L7 プロトコルを検出するとオフロードが機能します。

HTTPS 課金

HTTPS パケットの課金は SM-P で行われます。

統計

HTTPS に関連する統計情報を取得するには、次の CLI コマンドを使用します。**show user-plane-service statistics analyzer name secure-http**

HTTP URL フィルタリング機能

HTTP URL フィルタリング機能は、URL 検出に使用されるルール定義を簡素化します。

HTTP リクエストパケットには、プロキシ（プレフィックス付き）URL と実際の URL を含めることができます。プロキシ URL が HTTP リクエストパケットで見つかった場合、HTTP URL フィルタリング機能は解析された情報からこの URL を切り捨て、実際の URL のみがルール照合とイベントデータレコード（EDR）の生成に使用されます。

HTTP URL フィルタリング機能の設定

ここでは、HTTP URL フィルタリング機能の設定方法について説明します。

プレフィックス付き URL のグループの設定

プレフィックス付き URL のグループを設定するには、次の CLI コマンドを使用します。

```
configure
  active-charging service ecs_service_name
    group-of-prefixed-urls prefixed_urls_group_name
    end
```

プレフィックス付き URL のグループ内 URL の設定

プレフィックス付き URL のグループでフィルタリング対象の URL を設定するには、次の CLI コマンドを使用します。

```
configure
  active-charging service ecs_service_name
    group-of-prefixed-urls prefixed_urls_group_name
      prefixed-url url_1
      ...
      prefixed-url url_10
      end
```

ルールベースでのプレフィックス付き URL のグループの有効化

プレフィックス付き URL を処理するためにルールベースでプレフィックス付き URL のグループを有効にするには、次の CLI コマンドを使用します。

```
configure
  active-charging service ecs_service_name
    rulebase rulebase_name
      url-preprocessing bypass group-of-prefixed-urls
prefixed_urls_group_name_1
      ...
      url-preprocessing bypass group-of-prefixed-urls
prefixed_urls_group_name_64
      end
```

コントロール プレーン シャーシのこの設定は、「group-of-prefixed-urls」と「rulebase-url-preprocessing」の PFD メッセージを使用してユーザープレーンにプッシュされます。

プレフィックス付き URL のグループにはプロキシ URL のリストがあり、このリストは削除する必要があります。rulebase には、プレフィックス付き URL の複数のグループが含まれており、フィルタリングする必要があります。課金 ruledef には、プレフィックス付き URL グループ内の URL を削除してから検索する必要がある実際の URL のルールが含まれています。

（注）
- プレフィックス付き URL の 1 グループあたり、最大 10 個のプレフィックス付き URL を追加できます。
- 最大 64 のプレフィックス付き URL グループを作成および設定できます。

コマンドの表示

show user-plane-service group-of-prefixed-urls all | name *group_name*

この show コマンドをユーザープレーンで使用すると、プレフィックス付き URL のグループがプッシュされているかどうかを確認できます。このコマンドの出力は次のとおりです。

- Name of the group of prefixed URLs
- Prefixed URLs
- Total number of prefixed URLs found

show user-plane-service rulebase name *rbase_name*

この show コマンドをユーザープレーンで使用すると、プレフィックス付き URL のグループが rulebase で設定されているかどうかを確認できます。このコマンドの出力は次のとおりです。

- Name of rulebase
- Name of the groups of prefixed Urls for URL pre-processing

show user-plane-service statistics analyzer name http

このコマンドの出力は次のとおりです。

- Total HTTP Sessions
- Current HTTP Sessions
- Total Uplink Bytes
- Total Downlink Bytes
- Total Uplink Pkts
- Total Downlink Pkts
- Uplink Bytes Retrans
- Downlink Bytes Retrans
- Uplink Pkts Retrans
- Downlink Pkts Retrans
- Total Request Succeed
- Total Request Failed
- GET Requests

- POST Requests
- CONNECT Requests
- PUT requests
- HEAD requests
- Websocket Flows
- Invalid packets
- Wrong FSM packets
- Unknown request method
- Pipeline overflow requests
- Corrupt request packets
- Corrupt response packets
- Unhandled request packets
- Unhandled response packets
- Partial HTTP Header Anomaly prevented
- New requests on closed connection
- Memory allocation failures
- Packets after permanent failure
- Prefixed Urls Bypassed
- FastPath Statistics
- Total FP Flows
- Uplink (Total FP Pkts)
- Downlink (Total FP Pkts)
- Uplink (Total FP Bytes)
- Downlink (Total FP Bytes)

（注） パフォーマンス測定指標として、[Prefixed URLs Bypassed] カウンタが http アナライザ統計に追加されました。削除済みのプレフィックス付き URL 数を表示します。

RTP/RTSP

SM-P へのオフロード

UDP プロトコル上にある RTP はすぐにオフロードされます。

RTSP フローはオフロードされません。RTSP フローの TRM エンゲージメントはありません。

課金

RTP パケットは SM-P で課金されます。 RTSP パケットは、パケットが部分的でない場合、または遅延課金が有効になっている場合に SM-P で課金されます。

ルールの照合

この機能は、非 CUPS アーキテクチャと同じです。

統計

RTP に関連する統計情報を取得するには、CLI コマンド **show user-plane-service statistics analyzer name rtp** を使用します。

RTSP に関連する統計情報を取得するには、次の CLI コマンドを使用します。

- **show user-plane-service statistics analyzer name rtsp**
- **show user-plane-service statistics analyzer name rtsp verbose**

RTP ダイナミックフローの検出

rtp dynamic-flow-detection CLI コマンドは、[ACS Rulebase Configuration] モードで、Real Time Streaming Protocol（RTSP）および Session Description Protocol（SDP）アナライザが子 RTP および RTCP フローを検出できるようにします。RTSP/SIP および SDP アナライザを設定し、**rtp dynamic-flow-detection** CLI が存在していれば、RTP/RTCP の明示的な設定は必要ありません。**rtp dynamic-flow-detection** CLI コマンドを使用すると、子 RTP または RTCP フローが親 RTSP/SIP-SDP フローと相互に関連付けられます。

親フロー（RTSP/SIP-SDP）がクリアされると、子 RTP/RTCP フローもクリアされます。この CLI がない場合、RTP および RTCP の L7 レイヤ分析には、別途アナライザの設定が必要です。RTP/RTCP フローと RTSP/SIP-SDP フローとの相関関係はありません。

ベアラー固有フィルタのルール照合

ルール照合

機能は、非 CUPS アーキテクチャと同じです。

IMSI ベースのルールは、サブスクライバの IMSI に従って照合されます。

APN ベースのルールを使用すると、ベアラーフローのアクセスポイント名（APN）と一致するルール式を定義できます。

RAT タイプを使用すると、ベアラーフロー内の無線アクセス技術（RAT）に一致するルール式を定義できます。

ルール定義

IMSI プールを設定するには、次の CLI コマンドを使用します。

```
configure
  active-charging service service_name
    imsi-pool pool_name
      imsi { imsi_number | range start_imsi to end_imsi }
```

imsi-pool には、IMSI 値または IMSI の範囲を含めることができます。

次の CLI コマンドを使用して、ruledef でルール行を設定します。

```
configure
  active-charging service service_name
    ruledef ruledef_name
      bearer 3gpp imsi { = imsi_value } | { range imsi-pool pool_name }
      bearer 3gpp apn operator apn_name
      bearer 3gpp rat-type operator rat_type
```

IMSI 範囲は、IMSI プールを使用してルール内で設定できます。

上記の CLI コマンドの詳細については、StarOS の『*Command Line Interface Reference*』[英語] の「*ACS Ruledef Configuration Mode Commands*」を参照してください。

show CLI

サービスで設定されている IMSI プールに関する情報を表示するには、ユーザープレーンで次の CLI を使用します：**show user-plane-service imsipool name** *pool_name*

SIP

SM-P へのオフロード

SIP フローはオフロードされません。

充電中

SIP パケットは SM-P で課金されます。

ルールの照合

この機能は、非 CUPS アーキテクチャの機能と同じです。

統計

SIP に関連する統計情報を取得するには、次の CLI コマンドを使用します。**show user-plane-service statistics analyzer name sip**

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。