# モバイル ネットワークのインスペクション

次の項では、LTE などのモバイル ネットワークで使用されるプロトコルに対するアプリケーション インスペクションについて説明します。これらのインスペクションには、キャリア ライセンスが必要です。特定のプロトコルに関してインスペクションを使用する必要がある理由、およびインスペクションを適用する全体的な方法については、アプリケーション レイヤ プロトコル インスペクションの準備を参照してください。



# モバイル ネットワーク インスペクションの概要

次の項では、LTE などのモバイル ネットワークで使用されるプロトコルに対応するインスペクションについて説明します。インスペクションに加えて SCTP トラフィックで利用できるサービスは他にもあります。

## GTP インスペクションの概要

GPRS トンネリング プロトコルは、General Packet Radio Service（GPRS）トラフィック用に GSM、UMTS および LTE ネットワークで使用されます。GTP は、トンネル制御および管理プロトコルを提供します。このプロトコルによるトンネルの作成、変更、および削除により、モバイル ステーションに GPRS ネットワーク アクセスが提供されます。GTP は、ユーザ データ パケットの伝送にもトンネリング メカニズムを使用します。

サービス プロバイダー ネットワークは、GTP を使用して、エンドポイント間の GPRS バックボーンを介してマルチプロトコル パケットをトンネリングします。GTPv0-1 では、GTP は gateway GPRS support node（GGSN）と serving GPRS support node（SGSN）間のシグナリングの

ために使用されます。GTPv2 では、シグナリングは Packet Data Network Gateway（PGW）と Serving Gateway（SGW）および他のエンドポイント間で行われます。GGSN/PGW は、GPRS 無線データ ネットワークと他のネットワークとの間のインターフェイスです。SGSN/SGW は、モビリティ、データ セッション管理、およびデータ圧縮を実行します。

ASA を使用して、不正なローミング パートナーに対する保護を行えます。デバイスをホームの GGSN/PGW エンドポイントと訪問した SGSN/SGW エンドポイント間に配置し、トラフィック上で GTP インスペクションを使用します。GTP インスペクションは、これらのエンドポイント間のトラフィックでのみ動作します。GTPv2 では、これは S5/S8 インターフェイスとして知られています。

GTP および関連する規格は、3GPP（第 3 世代パートナーシップ プロジェクト）によって定義されます。詳細については、http://www.3gpp.org を参照してください。

次に、GTP インスペクションに関する制限事項の一部を示します。

- GTPv2 ピギーバック メッセージはサポートされていません。これらは常にドロップされます。
- GTPv2 emergency UE attach は、IMSI（International Mobile Subscriber Identity）が含まれている場合にのみサポートされます。
- GTP インスペクションは初期のデータは検査しません。つまり、セッション要求の作成直後かつセッション応答の作成前に PGW または SGW から送信されたデータのことです。
- GTPv2 の場合、インスペクションは 3GPP 29.274 リリース 10 バージョン 13 までサポートしています。GTPv0/v1 の場合、3GPP 29.060 のリリース 9 までサポートされます。
- GTP インスペクションは、セカンダリ PDP コンテキストへの SGSN 間ハンドオフをサポートしていません。インスペクションは、プライマリおよびセカンダリ両方の PDP コンテキストに対しハンドオフを実行する必要があります。

# Stream Control Transmission Protocol（SCTP）インスペクションとアクセス制御

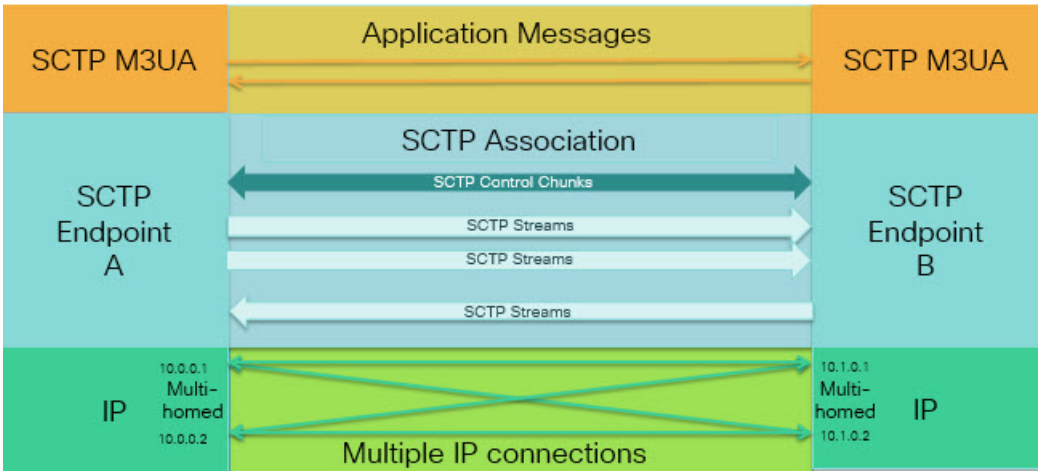
SCTP（Stream Control Transmission Protocol）は RFC 4960 で説明されています。プロトコルは IP 経由のテレフォニー シグナリング プロトコル SS7 をサポートしており、4G LTE モバイル ネットワーク アーキテクチャにおける複数のインターフェイス用の転送プロトコルでもあります。

SCTP は、TCP や UDP と同様、プロトコル スタックの IP の最上部で動作するトランスポート層プロトコルです。ただし、SCTP は、1 つ以上の送信元 IP アドレスまたは宛先 IP アドレス上の 2 つのエンド ノード間でアソシエーションと呼ばれる論理的な通信チャネルを作成します。これはマルチホーミングと呼ばれます。アソシエーションでは、各ノード（送信元と宛先）での IP アドレスのセットと、各ノードでのポートが定義されます。セット内の任意の IP アドレスは、複数の接続を形成するためにこのアソシエーションに関連付けられたデータ パケットの送信元または宛先 IP アドレスとして使用できます。各接続内では、メッセージを送信するた

めに複数のストリームが存在する可能性があります。SCTP 内のストリームは、論理的なアプリケーション データ チャネルを表します。

次の図は、アソシエーションとそのストリームとの関係を示しています。

**図 *1 : SCTP* アソシエーションとストリームの関係**




ASA を通過する SCTP トラフィックがある場合、SCTP ポートに基づいてアクセスを制御し、アプリケーション層のインスペクションを実行して、接続を有効にし、オプションでペイロード プロトコル ID でフィルタリングを行い、アプリケーションを選択的にドロップ、ログに記録、またはレート制限できます。

（注） 各ノードは、最大 3 つの IP アドレスを持つことができます。上限である 3 を超えたアドレスは無視され、アソシエーションに含まれません。セカンダリ IP アドレスのピンホールは、自動的に開きます。これらを許可するアクセス制御ルールを記述する必要はありません。

次の項では、SCTP トラフィックで利用できるサービスについて詳しく説明します。

## SCTP ステートフル インスペクション

TCP と同様、SCTP トラフィックは、正しく構造化されたトラフィックと RFC 4960 の限定的な適用についてレイヤ 4 で自動的に検査されます。次のプロトコル要素が検査され、適用されます。

- チャンクのタイプ、フラグ、および長さ。
- 検証タグ。
- 送信元ポートと宛先ポート。アソシエーション リダイレクト攻撃を防ぐため。
- IP アドレス。

SCTP ステートフル インスペクションは、アソシエーションの状態に基づいてパケットの受け入れまたは拒否を行います。

- 最初のアソシエーション確立のための 4 方向開閉シーケンスの検証。
- アソシエーションおよびストリーム内の TSN の転送進捗状況の確認。
- ハートビートの障害による中断チャンクを確認した場合のアソシエーションの終了。SCTP エンドポイントは、爆弾攻撃に応答して中断チャンクを送信する場合があります。

これらの強制チェックを行わない場合は、特定のトラフィック クラスの接続の設定（すべてのサービス） で説明されているように、特定のトラフィック クラスに対し SCTP ステート バイパスを設定できます。

## SCTP アクセス制御

SCTP トラフィックのアクセス ルールを作成できます。これらのルールは TCP/UDP ポート ベースのルールと似ており、プロトコルとして単に **sctp** を使用し、ポート番号は SCTP ポートです。SCTP 用のサービス オブジェクトまたはグループを作成するか、またはポートを直接指定できます。次の項を参照してください。

- サービス オブジェクトとサービス グループの設定
- 拡張 ACL の設定
- アクセス ルールの設定

## SCTP NAT

SCTP アソシエーション確立メッセージのアドレスにスタティック ネットワーク オブジェクト NAT を適用できます。スタティック Twice NAT を設定できますが、SCTP アソシエーションの宛先部分のトポロジが不明であるため、これは推奨されません。ダイナミック NAT/PAT を使用することはできません。

SCTP 用の NAT は、SCTP アプリケーション レイヤのインスペクションではなく、SCTP ステートフルインスペクションによって決まります。したがって、SCTP ステート バイパスを設定している場合は、NAT トラフィックはできません。

## SCTP アプリケーション レイヤのインスペクション

SCTP アプリケーション SCTP インスペクションとフィルタリングを有効にすることにより、アクセス ルールをさらに絞り込むことができます。ペイロード プロトコル ID（PPID）に基づいて、SCTP トラフィック クラスを選択的にドロップ、ログに記録、またはレート制限することができます。

PPID でフィルタリングする場合は、次の点に注意してください。

- PPID はデータのかたまりの中にあり、特定のパケットは複数のデータ チャンクまたは 1 つの制御チャンクを持つことができます。パケットに 1 つの制御チャンクまたは複数のデータ チャンクが含まれている場合、割り当てられたアクションがドロップされてもパケットはドロップされません。

- PPID フィルタリングを使用してパケットをドロップまたはレート制限する場合は、トランスミッタによりドロップされたパケットが再送されることに注意してください。レート制限が適用された PPID のパケットは再試行で通過する可能性がありますが、ドロップされた PPID のパケットは再びドロップされます。ネットワーク上のこのような反復的ドロップの最終成果を評価することができます。

## SCTP に関する制限事項

SCTP サポートには次の制限事項が含まれます。

- 各ノードは、最大 3 つの IP アドレスを持つことができます。上限である 3 を超えたアドレスは無視され、アソシエーションに含まれません。セカンダリ IP アドレスのピンホールは、自動的に開きます。これらを許可するアクセス制御ルールを記述する必要はありません。
- 使用されないピンホールは、5 分後にタイムアウトします。
- マルチホーム エンドポイントのデュアル スタック IPv4 および IPv6 アドレスはサポートされません。
- ネットワーク オブジェクト スタティック NAT は、唯一サポートされているタイプの NAT です。また、NAT46 および NAT64 はサポートされません。
- SCTP パケットのフラグメンテーションとリアセンブリは、Diameter、M3UA、および SCTP の PPID ベースのインスペクションで処理されたトラフィックにのみ実行されます。
- SCTP で IP アドレスを動的に追加または削除するために使用される ASCONF チャンクは、サポートされません。
- IP アドレスに解決できるホスト名を指定するために使用される、INIT および INIT-ACK SCTP メッセージ内のホスト名パラメータは、サポートされません。
- ASA、またはネットワーク内の他の場所で設定されているかどうかにかかわらず、SCTP/M3UA は等コスト マルチパス ルーティング（ECMP）をサポートしません。ECMP を使用すると、複数のベストパスを介してパケットを宛先にルーティングできます。ただし、単一の宛先への SCTP/M3UA パケット応答は、送出されたときと同じインターフェイスに戻る必要があります。応答が M3UA サーバから送信される可能性があるとしても、常に送出されたときと同じインターフェイスに戻る必要があります。この問題の症状として、SCTP INIT-ACK パケットがドロップされます。これは、**show asp drop flow sctp-chunk-init-timeout** カウンタで確認できます。

```
Flow drop:
SCTP INIT timed out (not receiving INIT ACK)(sctp-chunk-init-timeout)
```

この問題が発生した場合は、M3UA サーバへのスタティック ルートを設定するか、またはポリシーベース ルーティングを設定して、INIT-ACK パケットが INIT パケットと同じインターフェイスを確実に通過するネットワーク設計を実装することで解決できます。

# Diameter インスペクション

Diameter は、LTE（Long Term Evolution）および IMS（IP Multimedia Subsystem）用の EPS（Evolved Packet System）などの次世代モバイルと固定電気通信ネットワークで使用される認証、認可、およびアカウンティング（AAA）プロトコルです。RADIUS や TACACS がこれらのネットワークで Diameter に置き換えられます。

Diameter はトランスポート層として TCP および SCTP を使用し、TCP/TLS および SCTP/DTLS によって通信を保護します。また、オプションで、データ オブジェクトの暗号化も提供できます。Diameter の詳細については、RFC 6733 を参照してください。

Diameter アプリケーションは、課金のユーザ アクセス、サービス認証、QoS、およびレートの決定といったサービス管理タスクを実行します。Diameter アプリケーションは LTE アーキテクチャのさまざまなコントロール プレーン インターフェイスで使用されますが、ASA は、次のインターフェイスについてのみ、Diameter コマンド コードおよび属性値ペア（AVP）を検査します。

- S6a：モビリティ マネージメント エンティティ（MME）- ホーム サブスクリプション サービス（HSS）
- S9：PDN ゲートウェイ（PDG）- 3GPP AAA プロキシ/サーバ
- Rx：ポリシー/課金ルール機能（PCRF） - コール セッション制御機能（CSCF）

Diameter インスペクションでは、Diameter エンドポイント用にピンホールを開いて通信を可能にします。このインスペクションは、3GPP バージョン 12 をサポートし、RFC 6733 に準拠しています。TCP/TLS（インスペクションをイネーブルにするときに TLS を指定する場合）および SCTP には使用できますが、SCTP/DTLS には使用できません。SCTP Diameter セッションにセキュリティを提供するには IPsec を使用します。

パケットや接続のドロップまたはロギングなどの特別なアクションを適用するために、オプションで、Diameter インスペクション ポリシー マップを使用し、アプリケーション ID、コマンド コード、および AVP に基づいてトラフィックをフィルタリングできます。新規に登録された Diameter アプリケーション用のカスタム AVP を作成できます。フィルタリングにより、ネットワークで許可するトラフィックを微調整できます。

（注） 他のインターフェイス上で動作するアプリケーションに対する Diameter メッセージはデフォルトで許可され、渡されます。ただし、アプリケーション ID によってこれらのアプリケーションを破棄するための Diameter インスペクション ポリシー マップを設定できますが、これらのサポートされていないアプリケーションに対してコマンド コードまたは AVP に基づいてアクションを指定することはできません。

# M3UA インスペクション

MTP3 User Adaptation（M3UA）は、SS7 Message Transfer Part 3（MTP3）レイヤと連動する IP ベース アプリケーション用の SS7 ネットワークへのゲートウェイを提供するクライアント/サー

バ プロトコルです。M3UA により、IP ネットワーク上で SS7 ユーザ パート（ISUP など）を実行することが可能になります。M3UA は RFC 4666 で定義されています。

M3UA は SCTP をトランスポート層として使用します。SCTP ポート 2905 がデフォルト ポートです。

MTP3 レイヤは、ルーティングおよびノードアドレッシングなどのネットワーク機能を提供しますが、ノードの識別にポイント コードを使用します。M3UA 層は、発信ポイント コード（OPC）および宛先ポイント コード（DPC）を交換します。これは、IP が IP アドレスを使用してノードを識別する仕組みと似ています。

M3UA インスペクションは、限定されたプロトコル準拠を提供します。オプションで、厳密なアプリケーション サーバ プロセス（ASP）のステート チェックおよび選択されたメッセージの追加のメッセージの検証を実装できます。厳密な ASP のステート チェックが必要なのは、ステートフル フェールオーバーが必要な場合、またはクラスタ内での動作が必要な場合です。ただし、厳密な ASP のステート チェックは、上書きモードでのみ動作し、ロードシェアリングまたはブロードキャスト モードで実行している場合は動作しません（RFC 4666 より）。インスペクションは、エンドポイントごとに ASP が 1 つだけあると仮定します。

オプションで、ポイント コードまたはサービス インジケータ（SI）に基づいてアクセス ポリシーを適用できます。また、メッセージのクラスおよびタイプに基づいてレート制限を適用できます。

## M3UA プロトコル準拠

M3UA インスペクションでは、次の限定されたプロトコルを強制できます。インスペクションは、要件を満たさないパケットをドロップしてログに記録します。

- 共通のメッセージヘッダー。インスペクションでは、共通ヘッダー内のすべてのフィールドを確認します。
  - バージョン 1 のみ。
  - メッセージの長さが正しく設定されている必要があります。
  - 予約済みの値を使用したメッセージ タイプのクラスは許可されません。
  - メッセージ クラス内での無効なメッセージ ID は許可されません。
- ペイロード データ メッセージ。
  - 特定のタイプの 1 つのパラメータのみが許可されます。
  - SCTP ストリーム 0 でのデータ メッセージは許可されません。
- [Affected Point Code] フィールドは次のメッセージに含まれている必要があり、含まれていない場合、メッセージはドロップされます。利用可能な宛先（DAVA）、利用できない宛先（DUNA）、宛先の状態監査（DAUD）、シグナリング輻輳（SCON）、利用できない宛先ユーザ部（DUPU）、制限された宛先（DRST）。
- 次のメッセージについてメッセージ タグの検証を有効にすると、特定のフィールドの内容が確認および検証されます。検証で合格しなかったメッセージはドロップされます。

- 利用できない宛先ユーザ部（DUPU）：ユーザ/理由フィールドが存在し、有効な理由およびユーザ コードのみが含まれている必要があります。
- エラー：すべての必須フィールドが存在し、許可された値のみが含まれている必要があります。各エラー メッセージには、そのエラー コードの必須フィールドが含まれている必要があります。
- 通知：ステータス タイプおよびステータス情報フィールドには、許可された値のみが含まれている必要があります。

- アプリケーション サーバ プロセス（ASP）の厳密な状態検証を有効にすると、システムは M3UA セッションの ASP の状態を維持し、検証結果に基づいて ASP メッセージを許可またはドロップします。ASP の厳密な状態検証を無効にすると、すべての ASP メッセージが検査されずに転送されます。

## M3UA インスペクションの制限事項

次に、M3UA インスペクションに関する制限事項の一部を示します。

- NAT は、M3UA データに埋め込まれている IP アドレスではサポートされません。
- M3UA の厳密なアプリケーション サーバ プロセス（ASP）状態の確認は、SCTP ステートフル インスペクションと依存性があります。SCTP ステート バイパスと M3UA の厳密な ASP 確認は、同じトラフィック上で実行しないでください。
- 厳密な ASP のステート チェックが必要なのは、ステートフル フェールオーバーが必要な場合、またはクラスタ内での動作が必要な場合です。ただし、厳密な ASP のステート チェックは、上書きモードでのみ動作し、ロードシェアリングまたはブロードキャスト モードで実行している場合は動作しません（RFC 4666 より）。インスペクションは、エンドポイントごとに ASP が 1 つだけあると仮定します。

# RADIUS アカウンティング インスペクションの概要

RADIUS アカウンティング インスペクションの目的は、RADIUS サーバを使用した GPRS ネットワークの過剰請求攻撃を防ぐことです。RADIUS アカウンティング インスペクションを実行するためにキャリア ライセンスは必要ありませんが、GTP インスペクションを実行し、GPRS を設定しなければ意味がありません。

GPRS ネットワークの過剰請求攻撃は、コンシューマに対して、利用していないサービスの請求を行います。この場合、悪意のある攻撃者は、サーバへの接続をセットアップし、SGSN から IP アドレスを取得します。攻撃者がコールを終了しても、攻撃者のサーバはパケットの送信を続けます。このパケットは GGSN によってドロップされますが、サーバからの接続はアクティブなままです。攻撃者に割り当てられていた IP アドレスが解放され、正規ユーザに再割り当てされるので、正規ユーザは、攻撃者が利用するサービスの分まで請求されることになります。

RADIUS アカウンティング インスペクションは、GGSN へのトラフィックが正規のものかどうかを確認することにより、このような攻撃を防ぎます。RADIUS アカウンティングの機能を正

しく設定しておくと、ASA は、RADIUS アカウンティング要求の開始メッセージと終了メッセージに含まれる Framed IP 属性との照合結果に基づいて接続を切断します。終了メッセージの Framed IP 属性の IP アドレスが一致している場合、ASA は、一致する IP アドレスを持つ送信元との接続をすべて検索します。

ASA でメッセージを検証できるように、RADIUS サーバとの事前共有秘密キーを設定することもできます。共有秘密が設定されていない場合、ASA は、ソース IP アドレスが RADIUS メッセージを送信できるよう設定された IP アドレスであるということだけをチェックします。

（注） GPRS をイネーブルにして RADIUS アカウンティング インスペクションを使用すると、ASA はアカウンティング要求の STOP メッセージで 3GPP-Session-Stop-Indicator をチェックして、セカンダリ PDP コンテキストを正しく処理します。具体的には、ASA では、アカウンティング要求の終了メッセージがユーザ セッションおよび関連するすべての接続を終了する前に、メッセージに 3GPP-SGSN-Address 属性が含まれる必要があります。一部のサードパーティの GGSN は、この属性をデフォルトでは送信しない場合があります。

# モバイル ネットワーク プロトコル インスペクションのライセンス

次のプロトコルのインスペクションには、次の表に記載されているライセンスが必要です。

- GTP
- SCTP。
- Diameter
- M3UA

| モデル | ライセンス要件 |
|---|---|
| • ASA 5525-X<br>• ASA 5545-X<br>• ASA 5555-X<br>• ASA 5585-X<br>• ASASM | キャリア license |
| ASAv（全モデル） | キャリア ライセンス（デフォルトではイネーブル） |
| Firepower 4100 の ASA | キャリア ライセンス |
| Firepower 9300 の ASA | キャリア ライセンス |

| モデル | ライセンス要件 |
|---|---|
| 他のすべてのモデル | キャリア ライセンスは他のモデルでは使用できません。これらのプロトコルは検査できません。 |

# GTP インスペクションのデフォルト

GTPインスペクションはデフォルトではイネーブルになっていません。ただし、ユーザ自身のインスペクション マップを指定せずにイネーブルにすると、次の処理を行うデフォルト マップが使用されます。マップを設定する必要があるのは、異なる値が必要な場合のみです。

- エラーは許可されません。
- 要求の最大数は 200 です。
- トンネルの最大数は500です。これは、PDPコンテキスト（エンドポイント）の数に相当します。
- GTPエンドポイントのタイムアウトは30分です。エンドポイントには、GSN（GTPv0,1）およびSGW/PGW（GTPv2）が含まれています。
- PDP コンテキストのタイムアウトは 30 分です。GTPv2 では、これはベアラ- コンテキスト タイムアウトです。
- 要求のタイムアウトは 1 分です。
- シグナリング タイムアウトは 30 分です。
- トンネリングのタイムアウトは 1 時間です。
- T3 応答タイムアウトは 20 秒です。
- 不明なメッセージ ID はドロップされ、ログに記録されます。この動作は、3GPP が S5S8 インターフェースについて定義するメッセージに制限されます。他のGPRSインターフェイスについて定義されたメッセージは、最小限の検査によって許可される場合があります。

  未定義のメッセージやシステムでサポートされていない GTP リリースで定義されたメッセージは不明と見なされます。サポート対象のリリースは、GTPv1 リリース 6.1 および GTPv2 リリース 10.13 です。

# モバイル ネットワーク インスペクションの設定

モバイルネットワークで使用されるプロトコルのインスペクションはデフォルトで有効になっていません。モバイルネットワークをサポートするには、それらを設定する必要があります。

### 手順

**ステップ 1** （任意）GTP インスペクション ポリシー マップの設定 （11 ページ）。

**ステップ 2** （任意）SCTP インスペクション ポリシー マップの設定 （15 ページ）。

**ステップ 3** （任意）Diameter インスペクション ポリシー マップの設定 （17 ページ）。

ソフトウェアではまだサポートされていない属性値ペア（AVP）でフィルタリングする場合は、Diameter インスペクション ポリシー マップで使用するカスタム AVP を作成できます。カスタム Diameter 属性値ペア（AVP）の作成 （20 ページ）を参照してください。

**ステップ 4** （任意）暗号化された Diameter TCP/TLS トラフィックを検査する場合は、次の説明に従って、必要な TLS プロキシを作成します。 暗号化された Diameter セッションの検査 （21 ページ）

**ステップ 5** （任意） M3UA インスペクション ポリシー マップの設定 （29 ページ）

**ステップ 6** モバイル ネットワーク インスペクションのサービス ポリシーの設定 （33 ページ）。

**ステップ 7** （任意）RADIUS アカウンティング インスペクションの設定 （34 ページ）。

RADIUS アカウンティング インスペクションは、過剰請求攻撃から保護します。

# GTP インスペクション ポリシー マップの設定

GTP トラフィックで追加のパラメーターを実行する際にデフォルト マップがニーズを満たさない場合は、GTP マップを作成し、設定します。

### 始める前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

### 手順

**ステップ 1** **[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[GTP]** を選択します。

**ステップ 2** 次のいずれかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- 内容を表示するマップを選択します。マップを編集するには、[Customize] をクリックします。この後の手順では、マップをカスタマイズまたは追加するものとします。

**ステップ 3** 新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップを編集するときは、変更できるのは説明のみです。

**ステップ 4** [GTP Inspect Map] ダイアログボックスの [Security Level] ビューで、マップの現在の設定を確認します。

ビューはマップがデフォルト値を使用しているのか、またはカスタマイズしているのかを示します。設定をさらにカスタマイズする必要がある場合は、[Details] をクリックし、手順を続けます。

ヒント　[IMSI Prefix Filtering] ボタンは、この手順の後半で説明される IMSI プレフィックス フィルタリングを設定するショートカットです。

**ステップ 5**　[Permit Parameters] タブをクリックして必要なオプションを設定します。

- [Permit Response] ：ASA が GTP インスペクションを実行する場合、デフォルトで ASA は、GTP 要求で指定されていない GSN または PGW からの GTP 応答をドロップします。これは、GSN/PGW エンドポイントのプール間でロードバランシングを使用して、GPRS の効率とスケーラビリティを高めているときに発生します。

  GSN/PGW プーリングを設定し、ロード バランシングをサポートするために、GSN/PGW エンドポイントを指定するネットワーク オブジェクト グループを作成し、これを「**From Object Group**」として選択します。同様に、SGSN/SGW のためにネットワーク オブジェクト グループを作成し、「**To Object Group**」として選択します。応答を行う GSN/PGW が GTP 要求の送信先 GSN/PGW と同じオブジェクト グループに属しており、応答している GSN/PGW による GTP 応答の送信が許可されている先のオブジェクト グループに SGSN/SGW がある場合に、ASA で応答が許可されます。

  ネットワーク オブジェクト グループは、エンドポイントをホスト アドレスまたはエンドポイントを含むサブネットから識別できます。

- [Permit Errors] ：無効なパケットやインスペクション時にエラーが見つかったパケットを、ドロップしないで ASA から送信することを許可するかどうか設定します。

**ステップ 6**　[General Parameters] タブをクリックし、必要なオプションを設定します。

- [Maximum Number of Requests] ：応答待ちでキューに格納される GTP 要求の最大数を設定します。
- [Maximum Number of Tunnels] ：許可されるアクティブな GTP トンネルの最大数を設定します。これは、PDP コンテキストまたはエンドポイントの数に相当します。デフォルトは 500 です。新しい要求はトンネルの最大数に達するとドロップされます。
- [Enforce Timeout] ：次の動作のアイドル タイムアウトを実行するかどうか設定します。タイムアウトは hh: mm: ss 形式です。
  - [Endpoint]：GTP エンドポイントが削除されるまでの非アクティブ時間の最大値です。
  - [PDP-Context]：GTP セッションの PDP コンテキストを削除するまでの非アクティブ時間の最大値です。GTPv2 では、これはベアラー コンテキストです。
  - [Request]：リクエストがリクエスト キューから削除されるまでの非アクティブ時間の最大値です。ドロップされた要求への後続の応答もドロップされます。
  - [Signaling]：GTP シグナリングが削除されるまでの非アクティブ時間の最大値です。
  - [T3-Response timeout]：接続を削除するまでの、応答待ち時間の最大値です。

- [Tunnel]：GTP トンネルが切断されるまでの非アクティブ時間の最大値です。

**ステップ 7** 必要に応じて[IMSI Prefix Filtering] タブをクリックして、IMSI プレフィックス フィルタリングを設定します。

デフォルトでは、セキュリティアプライアンスは、有効なモバイル カントリ コード（MCC）とモバイル ネットワーク コード（MNC）の組み合わせをチェックしません。IMSI プレフィックス フィルタリングを設定すると、受信パケットの IMSI の MCC と MNC が、設定された MCC と MNC の組み合わせと比較され、一致しないものはドロップされます。

モバイル カントリ コードは 0 以外の 3 桁の数字で、1 桁または 2 桁の値のプレフィックスとして 0 が追加されます。モバイル ネットワーク コードは 2 桁または 3 桁の数字です。

割り当てられたすべての MCC と MNC の組み合わせを追加します。デフォルトでは、ASA は MNC と MCC の組み合わせが有効であるかどうかをチェックしないため、設定した組み合わせが有効であるかどうかを確認する必要があります。MCC および MNC コードの詳細については、ITU E.212 勧告『*Identification Plan for Land Mobile Stations*』を参照してください。

**ステップ 8** [Inspections] タブをクリックし、トラフィックの特性に基づいて実装する特定のインスペクションを定義します。

a) 次のいずれかを実行します。

- [Add] をクリックして、新しい基準を追加します。
- 既存の基準を選択し、[Edit] をクリックします。

b) 基準の一致タイプとして、[Match] （トラフィックは基準と一致する必要がある）または [No Match] （トラフィックは基準と異なる必要がある）を選択します。次に、基準を設定します。

- [Access Point Name] ：指定した正規表現または正規表現クラスとアクセス ポイント名に一致します。デフォルトでは、有効なアクセス ポイント名を持つすべてのメッセージが検査され、どの名前でも許可されます。
- [Message ID] ：1 ～ 255 のメッセージ ID に一致します。1 つの値または値の範囲を指定できます。メッセージが GTPv1 向けか（GTPv0 を含む）、GTPv2 向けかを指定する必要があります。デフォルトでは、すべての有効なメッセージ ID が許可されます。
- [Message Length] ：UDP ペイロードの長さが、指定した最小値と最大値の間にあるメッセージに一致します。
- [Version]：0 ～ 255 の GTP バージョンに一致します。1 つの値または値の範囲を指定できます。 デフォルトでは、すべての GTP バージョンが許可されます。
- [MSISDN]：PDP コンテキスト作成要求、セッション作成要求、およびベアラー変更応答のメッセージ内のモバイル ステーション国際サブスクライバ電話番号（MSISDN）の情報要素を指定した正規表現または正規表現クラスと照合します。正規表現では、特定の MSISDN または MSISDN の範囲を最初の x 桁に基づいて識別できます。MSISDN フィルタリングは GTPv1 および GTPv2 のみでサポートされています。

- [選択モード（Selection Mode）]：PDP コンテキスト作成要求内の選択モードの情報要素を照合します。選択モードでは、メッセージにアクセス ポイント名（APN）の発信元を指定しますが、次のいずれかになります。選択モードフィルタリングは、GTPv1 および GTPv2 のみでサポートされています。
  - 0：確認済み。APN はモバイル ステーションまたはネットワークによって指定されており、サブスクリプションが確認されています。
  - 1：モバイル ステーション。APN はモバイル ステーションによって指定されており、サブスクリプションは確認されていません。
  - 2：ネットワーク。APN はネットワークによって指定されており、サブスクリプションは確認されていません。
  - 3：予約済み（未使用）

c) メッセージ ID の一致には、パケットをドロップするかパケット/秒のレート制限を適用するかのいずれかを選択します。他のすべての一致のアクションは、パケットをドロップします。すべての一致に対してロギングをイネーブルにするかどうか選択できます。

d) [OK] をクリックして、インスペクションを追加します。必要に応じてプロセスを繰り返します。

**ステップ 9** [アンチリプレイの保護（Anti-Replay Protection）] タブをクリックし、アンチリプレイ オプションを設定します。

- [データ パケット リプレイ ウィンドウの有効化（Enable Data Packet Replay Window）]：GTP-U メッセージのスライディング ウィンドウを指定して、アンチリプレイを有効にするかどうかを指定します。スライディング ウィンドウのサイズはメッセージの数であり、128、256、512、または 1024 になります。有効なメッセージが表示されると、ウィンドウは新しいシーケンス番号に移行します。シーケンス番号は 0 ～ 65535 の範囲であり、最大値に達するとラッピングされます。また、これらは PDP コンテキストごとに一意です。メッセージは、シーケンス番号がウィンドウ内であれば有効と見なされます。アンチリプレイは、ハッカーが GTP データ パケットをキャプチャし、それらをリプレイするときに発生する可能性があるセッション ハイジャックや DoS 攻撃を防ぐのに役立ちます。

**ステップ 10** [ユーザスプーフィング（User-Spoofing）] タブをクリックし、アンチスプーフィング オプションを設定します。

- [GTP ヘッダーの確認（GTP Header Check）]：GTP データ パケットの内部ペイロードを確認し、非 IP ヘッダーがある場合はそのパケットをドロップするかどうか。アンチスプーフィングを実装するには、このオプションを選択する必要があります。
- [アンチスプーフィング（Anti-Spoofing）]：内部ペイロードの IP ヘッダー内のモバイル ユーザ IP アドレスが、セッション作成応答などの GTP 制御メッセージに割り当てられている IP アドレスと一致するかどうかを確認し、IP アドレスが一致しない場合はそのメッセージをドロップするかどうか。GTP-C を通じて割り当てたものではない別の IP アドレスを使用してハッカーが別の顧客であるように装う（スプーフィング）可能性がありま

す。アンチスプーフィングは、使用されている GTP-U アドレスが実際に GTP-C を使用して割り当てたものであるかどうかを確認します。

モバイル ステーションが DHCP を使用してそのアドレスを取得する場合、GTPv2 でのエンドユーザの IP アドレスは 0.0.0.0 になります。その場合、システムは内部パケットで検出した最初の IP アドレスを使用してエンドユーザ IP アドレスを更新します。次のキーワードを使用して、DHCP で取得したアドレスのデフォルトの動作を変更できます。

- [GTPV2-DHCP-ByPass]：アドレス 0.0.0.0 を更新しません。その代わりに、エンドユーザの IP アドレスが 0.0.0.0 の場合はパケットを許可します。IP アドレスの取得に DHCP を使用すると、このオプションはアンチスプーフィング チェックをバイパスします。
- [GTPV2-DHCP-DROP]：アドレス 0.0.0.0 を更新しません。その代わりに、エンドユーザの IP アドレスが 0.0.0.0 の場合はすべてのパケットをドロップします。このオプションは、IP アドレスの取得に DHCP を使用するユーザへのアクセスを防ぎます。

**ステップ 11** [GTP Inspect Map] ダイアログボックスの [OK] をクリックします。

これで、GTP インスペクションのサービス ポリシーで、インスペクション マップを使用できます。

### 次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。モバイル ネットワーク インスペクションのサービス ポリシーの設定 （33 ページ）を参照してください。

# SCTP インスペクション ポリシー マップの設定

レート制限などのアプリケーション固有のペイロードプロトコル ID（PPID）に基づいて SCTP トラフィックに代替アクションを適用するには、サービス ポリシーで使用される SCTP インスペクション ポリシー マップを作成します。

（注） PPID はデータのかたまりの中にあり、特定のパケットは複数のデータ チャンクまたは 1 つの制御チャンクを持つことができます。パケットに 1 つの制御チャンクまたは複数のデータ チャンクが含まれている場合、割り当てられたアクションがドロップされてもパケットはドロップされません。たとえば、PPID 26 をドロップする SCTP インスペクション ポリシー マップを設定すると、PPID 26 データ チャンクは、Diameter PPID データ チャンクを持つパケットに結合され、そのパケットはドロップされません。

### 手順

**ステップ 1** **[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[SCTP]** を選択します。

**ステップ 2** 次のいずれかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- マップを選択して [Edit] をクリックします。

**ステップ 3** 新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップを編集するときは、変更できるのは説明のみです。

**ステップ 4** SCTP データ チャンクの PPID に基づいて、トラフィックをドロップ、レート制限、またはログに記録します。

a) 次のいずれかを実行します。

- [Add] をクリックして、新しい基準を追加します。
- 既存の基準を選択し、[Edit] をクリックします。

b) 基準の一致タイプとして、[Match]（トラフィックは PPID と一致する必要がある）または [No Match]（トラフィックは PPID と異なる必要がある）を選択します。

たとえば、Diameter PPID で [No Match] を選択した場合は、Diameter を除くすべての PPID がクラス マップから除外されます。

c) [Minimum Payload PID] を選択し、任意で、照合する [Maximum Payload PID] を選択します。

名前または番号（0 ～ 4294967295）で PPID を入力できます。PPID のリストから選択するには、各フィールドで [...] ボタンをクリックします。最大数の PPID を選択した場合、照合は PPID の範囲に適用されます。

SCTP PPID の現在のリストは http://www.iana.org/assignments/sctp-parameters/sctp-parameters.xhtml#sctp-parameters-25 で確認できます。

d) 一致するパケットをドロップ（してログに記録）するか、ログに記録するか、またはレート制限（キロビット/秒（kbps）単位）するかを選択します。

e) [OK] をクリックして、インスペクションを追加します。必要に応じてプロセスを繰り返します。

**ステップ 5** [SCTP Inspect Map] ダイアログボックスの [OK] をクリックします。

これで、SCTP インスペクション サービス ポリシーでインスペクション マップを使用できるようになります。

### 次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。モバイル ネットワーク インスペクションのサービス ポリシーの設定 （33 ページ）を参照してください。

# Diameter インスペクション ポリシー マップの設定

さまざまな Diameter プロトコル要素でフィルタリングするための Diameter インスペクション ポリシー マップを作成できます。その後、接続を選択的にドロップまたはログに記録できます。

Diameter メッセージ フィルタリングを設定するには、これらのプロトコル要素は RFC および技術仕様で定義されているので、これらの要素について詳しい知識を持っている必要があります。たとえば、IETF には、http://www.iana.org/assignments/aaa-parameters/aaa-parameters.xhtml に示す登録済みアプリケーション、コマンドコード、および属性値ペアのリストがありますが、Diameterインスペクションではリストされているすべての項目をサポートしていません。技術仕様については、3GPP Web サイトを参照してください。

オプションとして、Diameter インスペクション クラス マップを作成し、Diameter インスペクションのメッセージフィルタリング基準を定義できます。他のオプションとしては、Diameter インスペクション ポリシー マップでフィルタリング基準を直接定義することもできます。クラス マップを作成することとインスペクション マップでフィルタリング基準を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるという点です。この手順ではインスペクション マップについて説明しますが、クラス マップで使用される一致基準は、[Inspection] タブに関する手順で説明されているものと同じです。**[Configuration]** > **[Firewall]** > **[Objects]** > **[Class Maps]** > **[Diameter]** を選択するか、またはインスペクション マップの設定時に作成することによって、Diameter クラス マップを設定できます。

**ヒント** 以下で説明する手順に加えて、サービス ポリシーの作成中にインスペクション マップを設定できます。マップの内容は、作成方法に関係なく同じです。

### 始める前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

### 手順

**ステップ 1** **[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[Diameter]** を選択します。

**ステップ 2** 次のいずれかを実行します。

- [Add] をクリックして、新しいマップを追加します。

- マップを選択して [Edit] をクリックすると、その内容を表示できます。

**ステップ 3** 新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップを編集するときは、変更できるのは説明のみです。

**ステップ 4** [Parameters] タブをクリックし、サポート対象外の Diameter 要素を含むメッセージをログに記録するかどうかについて希望するオプションを選択します。

- [Unsupported Parameters]：サポート対象外の Diameter 要素を含むメッセージをログに記録するかどうか。サポート対象外の [Application ID]、[Command Code]、または [Attribute Value Pair] の要素をログに記録できます。
- [Strict Diameter Validation Parameters]：RFC 6733 への厳密な Diameter プロトコルの準拠を有効にします。デフォルトでは、インスペクションによって、Diameter のフレームが RFC に準拠していることが確認されます。セッション関連メッセージの検証およびステートマシンの検証を追加できます。

**ステップ 5** [Inspections] タブをクリックし、トラフィックの特性に基づいて実装する特定のインスペクションを定義します。

Diameter クラス マップに基づいて、またはインスペクション マップで一致を直接設定することによって、またはその両方で、トラフィックの一致基準を定義できます。

a) 次のいずれかを実行します。

- [Add] をクリックして、新しい基準を追加します。
- 既存の基準を選択し、[Edit] をクリックします。

b) [Single Match] を選択して基準を直接定義するか、または [Multiple Match] を選択して基準を定義する Diameter クラス マップを選択します。

c) 基準をここで定義した場合は、基準の一致タイプとして [Match]（トラフィックは基準と一致する必要がある）または [No Match]（トラフィックは基準と異なる必要がある）を選択します。次に、基準を以下のように設定します。

- [Application ID]：Diameter アプリケーションの名前または番号（0 ～ 4294967295）を入力します。照合する連続番号が付されたアプリケーションの範囲がある場合は、2 番目の ID を含めることができます。アプリケーションの名前または番号別に範囲を定義でき、第 1 ID および第 2 ID の間のすべての番号に適用されます。

  これらのアプリケーションは IANA に登録されます。次のコア アプリケーションがサポートされますが、他のアプリケーションもフィルタ処理できます。

  - **3gpp-rx-ts29214**（16777236）
  - **3gpp-s6a**（16777251）
  - **3gpp-s9**（16777267）
  - **common-message**（0）。（基本 Diameter プロトコル）

- [Command Code]：Diameter コマンド コードの名前または番号（0 ～ 4294967295）を入力します。照合する連続番号が付されたコマンド コードの範囲がある場合は、2 番目

のコードを含めることができます。コマンドコードの名前または番号別に範囲を定義でき、第 1 コードおよび第 2 コードの間のすべての番号に適用されます。

たとえば、Capability Exchange Request/Answer コマンド コード CER/CEA を照合するには、**cer-cea** と入力します。

- [Attribute Value Pair]：属性のみによる AVP、AVP の範囲、または属性の値に基づく AVP を照合できます。[AVP Begin Value] の場合は、カスタム AVP の名前、または RFC または 3GPP 技術仕様に登録されていて、ソフトウェアで直接サポートされているものの名前を指定できます。リストから選択するには、フィールドで [...] ボタンをクリックします。

  AVP の範囲を照合する場合は、番号のみによる [AVP End Value] を指定します。値によって AVP を照合する場合は、2 番目のコードを指定できません。

  オプションの [Vendor ID] を 0 ～ 4294967295 の範囲で指定することで、照合をさらに絞り込むことができます。たとえば、3GPP ベンダー ID は 10415、IETF は 0。

  AVP のデータ タイプがサポートされている場合にのみ、値の照合を設定できます。たとえば、アドレス データ タイプがある AVP の IP アドレスを指定できます。AVP のリストには、それぞれのデータ タイプが表示されます。どのように値を指定するかは、AVP のデータ タイプによって異なります。

  - [Diameter Identity]、[Diameter URI]、[Octet String]：これらのデータ タイプを照合するには正規表現または正規表現のクラス オブジェクトを選択します。
  - [Address]：照合する IPv4 または IPv6 アドレスを指定します。たとえば、10.100.10.10 または 2001:DB8::0DB8:800:200C:417A。
  - [Time]：開始日時と終了日時を指定します。両方を指定する必要があります。時間は 24 時間形式で指定します。
  - [Numeric]：番号の範囲を指定します。有効な番号の範囲は、データ タイプによって異なります。
    - Integer32：-2147483647 ～ 2147483647
    - Integer64：-9223372036854775807 ～ 9223372036854775807
    - Unsigned32：0 ～ 4294967295
    - Unsigned64：0 ～ 18446744073709551615
    - Float32：8 桁の小数点表現
    - Float64：16 桁精度の小数点表記

d) 一致するトラフィックに対して実行するアクション（パケットのドロップ、接続のドロップ、またはロギング）を選択します。

e) [OK] をクリックして、インスペクションを追加します。必要に応じてプロセスを繰り返します。

**ステップ 6** [Diameter Inspect Map] ダイアログボックスの [OK] をクリックします。

これで、Diameter インスペクションのサービス ポリシーで、インスペクション マップを使用できます。

### 次のタスク

マップを使用するためのインスペクションポリシーを設定できるようになりました。モバイル ネットワーク インスペクションのサービス ポリシーの設定 （33 ページ）を参照してください。

# カスタム Diameter 属性値ペア（AVP）の作成

新しい属性値ペア（AVP）が定義され、登録されると、カスタム Diameter AVP を作成して、Diameterインスペクションポリシーマップにそれらを定義し、使用することができます。RFC または AVP を定義するその他のソースから AVP の作成に必要な情報を取得します。

カスタム AVP は、AVP 照合用の Diameterインスペクション ポリシー マップまたはクラス マップで使用する場合にのみ、作成します。

### 手順

**ステップ 1** **[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[Diameter AVP]** を選択します。

**ステップ 2** [Add] をクリックして、新しい AVP を作成します。

AVP を編集するときは、説明のみを変更できます。

**ステップ 3** 次のオプションを設定します。

- [Name]：作成しているカスタム AVP の名前（最大 32 文字）。属性値ペアの照合を定義する場合は、Diameter インスペクション ポリシー マップまたはクラス マップでこの名前を参照してください。
- [Custom Code]：カスタム AVP コード値（256 ～ 4294967295）。システムで定義済みのコードとベンダー ID の組み合わせを入力することはできません。
- [Data Type]：AVP のデータ タイプ。次のいずれかの型で AVP を定義できます。新しい AVP が別の型の場合は、その型のカスタム AVP は作成できません。
  - アドレス（IP アドレスの場合）
  - Diameter ID
  - Diameter Uniform Resource Identifier（URI）
  - 32 ビット浮動小数点
  - 64 ビット浮動小数点

- 32 ビット整数
- 64 ビット整数
- オクテット文字列
- 時刻
- 32 ビットの符号なし整数
- 64 ビットの符号なし整数

- [Vendor ID]：（任意）AVP を定義したベンダーの 0 ～ 4294967295 の ID 番号。たとえば、3GPP ベンダー ID は 10415、IETF は 0。
- [Description]：（任意） AVP の説明（最大 80 文字）。

**ステップ 4** [OK] をクリックします。

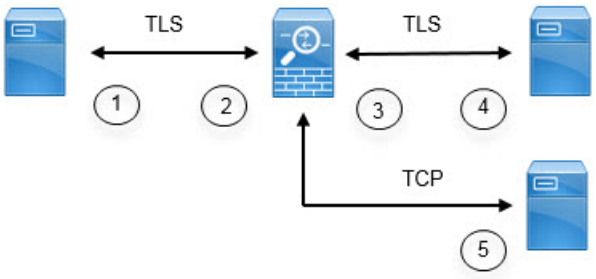
# 暗号化された Diameter セッションの検査

Diameter アプリケーションが TCP 上で暗号化されたデータを使用する場合、インスペクションはメッセージのフィルタリングルールを実装するためにパケット内を確認することはできません。したがって、フィルタリング ルールを作成し、それらを暗号化された TCP トラフィックにも適用する場合は、TLS プロキシを設定する必要があります。暗号化されたトラフィックで厳密なプロトコルを適用するには、プロキシも必要です。この設定は SCTP/DTLS トラフィックには適用されません。

TLS プロキシは中間者として機能します。このプロキシは、トラフィックを復号化し、検査してから再度暗号化し、目的の宛先に送信します。したがって、接続の両側（Diameter サーバと Diameter クライアント）は ASA を信頼する必要があり、すべての当事者が必要な証明書を保有している必要があります。TLS プロキシを実装するには、デジタル証明書を十分に理解しておく必要があります。ASA 全般設定ガイドのデジタル証明書に関する章を参照してください。

次の図は、Diameter のクライアントおよびサーバと ASA の間の関係と、信頼を確立するための認定要件を示します。このモデルでは、Diameter クライアントは MME（モビリティ マネージメント エンティティ）であり、エンドユーザではありません。リンクの各側の CA 証明書は、リンクの反対側の証明書の署名に使用されるものです。たとえば、ASA プロキシ TLS サーバ CA 証明書は、Diameter/TLS クライアント証明書の署名に使用されるものです。

図 *2 : Diameter TLS* インスペクション




| | | | |
|---|---|---|---|
| 1 | Diameter TLS クライアント（MME）<br>• クライアント ID 証明書<br>• ASA TLS プロキシ サーバの ID 証明書の署名に使用される CA 証明書 | 2 | ASA プロキシ TLS サーバ<br>• サーバ ID 証明書<br>• Diameter TLS クライアントの ID 証明書の署名に使用される CA 証明書 |
| 3 | ASA プロキシ TLS クライアント<br>• クライアント ID（スタティックまたは LDC）証明書<br>• Diameter TLS サーバの ID 証明書の署名に使用される CA 証明書 | 4 | Diameter TLS サーバ（フル プロキシ）<br>• サーバ ID 証明書<br>• ASA プロキシ TLS クライアントの ID 証明書の署名に使用される CA 証明書 |
| 5 | Diameter TCP サーバ（TLS オフロード） | — | — |

Diameter インスペクション用の TLS プロキシを設定するには、次のオプションがあります。

- フル TLS プロキシ：ASA および Diameter クライアントと ASA および Diameter サーバ間のトラフィックを暗号化します。TLS サーバとの信頼関係を確立するには、次のオプションがあります。
  - スタティック プロキシ クライアント トラストポイントを使用します。ASA は、Diameter サーバとの通信時に、すべての Diameter クライアントに同じ証明書を示します。Diameter サーバにとって全クライアントが同じように見えるので、クライアントごとに差別化サービスを提供することはできません。一方、このオプションは LDC 方式よりも高速です。
  - ローカル ダイナミック証明書（LDC）を使用します。このオプションを使用すると、ASA は Diameter サーバとの通信時に、Diameter クライアントごとに一意の証明書を示します。LDC は、公開キーと ASA からの新しい署名を除き、受信したクライアント ID 証明書からのすべてのフィールドを保持します。この方法では、Diameter サーバでクライアント トラフィックの可視性が向上し、クライアント証明書の特性に基づいて差別化サービスを提供できるようになります。

- TLS オフロード：ASA と Diameter クライアント間のトラフィックを暗号化しますが、ASA と Diameter サーバ間でクリアテキスト接続を使用します。このオプションは、デバイス間のトラフィックが保護された場所から離れることがないと確信している場合に、Diameter サーバが ASA と同じデータセンターにあれば実行可能です。TLS オフロードを使用すると、必要な暗号化処理量が減るので、パフォーマンスを向上させることができます。これは、オプションの中で最速です。Diameter サーバは、クライアントの IP アドレスのみに基づいて差別化サービスを適用できます。

3 つすべてのオプションは、ASA と Diameter クライアント間の信頼関係に対して同じ設定を使用します。

（注） TLS プロキシは TLSv1.0 ～ 1.2 を使用します。TLS のバージョンと暗号スイートを設定できます。

次の項では、Diameter インスペクション用の TLS プロキシを設定する方法について説明します。

## Diameter クライアントとのサーバ信頼関係の設定

ASA は、Diameter クライアントに対して TLS プロキシ サーバとして機能します。相互信頼関係を確立するには：

- ASA のサーバ証明書への署名に使用された認証局（CA）証明書を Diameter クライアントにインポートする必要があります。これは、クライアントの CA 証明書ストアまたはクライアントが使用する他の場所に保存されている場合があります。証明書の使用の詳細については、クライアントのドキュメントを参照してください。
- ASA がクライアントを信頼できるように、Diameter TLS クライアントの証明書への署名に使用された CA 証明書をインポートする必要があります。

次の手順では、Diameter クライアントの証明書への署名に使用された CA 証明書をインポートし、ASA TLS プロキシ サーバで使用する ID 証明書をインポートする方法について説明します。ID 証明書をインポートする代わりに、ASA で自己署名証明書を作成できます。また、TLS プロキシを作成するときにこれらの証明書をインポートすることもできます。

### 手順

**ステップ 1** Diameter クライアントの証明書への署名に使用されている CA 証明書を ASA トラストポイントにインポートします。

この手順によって、ASA が Diameter クライアントを信頼できます。

a) **[Configuration]** > **[Firewall]** > **[Advanced]** > **[Certificate Management]** > **[CA Certificates]** を選択します。

b) [Add] をクリックし、トラストポイントの名前を入力します。たとえば、**diameter-clients** などと入力します。
c) 証明書を追加します。

証明書をファイルからインポートするか、PEM 形式で貼り付けるか、または SCEP を使用してインポートできます。

d) [Install Certificate] をクリックします。

**ステップ 2** 証明書をインポートし、ASA プロキシ サーバの ID 証明書およびキーペア用のトラストポイントを作成します。

この手順によって、Diameter クライアントが ASA を信頼できます。

a) **[Configuration] > [Firewall] > [Advanced] > [Certificate Management] > [Identity Certificates]** を選択します。
b) [Add] をクリックし、トラストポイントの名前を入力します。たとえば、**tls-proxy-server-tp** などと入力します。
c) [Import the identity certificate from a file] を選択し、復号パスフレーズを入力し、ファイル（pkcs12 形式）を選択します。

または、新しい証明書を作成できます。

d) [Add Certificate] をクリックします。

## Diameter インスペクション用のスタティック クライアント証明書によるフル TLS プロキシの設定

Diameter サーバがすべてのクライアントに対して同じ証明書を受け入れることができる場合は、Diameter サーバと通信するときに使用する ASA 用のスタティック クライアント証明書を設定できます。

この設定では、ASA とクライアント間（Diameter クライアントとのサーバ信頼関係の設定 （23 ページ） で説明されているように）、および ASA と Diameter サーバ間に相互の信頼関係を確立する必要があります。ASA と Diameter サーバの信頼要件は次のとおりです。

- Diameter サーバの ID 証明書への署名に使用された CA 証明書をインポートする必要があるので、ASA は、TLS ハンドシェイク中にサーバの ID 証明書を検証できます。
- Diameter サーバも信頼しているクライアント証明書をインポートする必要があります。Diameter サーバがまだ証明書を信頼していない場合は、その署名に使用される CA 証明書をサーバにインポートします。詳細については、Diameter サーバのドキュメントを参照してください。

### 手順

**ステップ 1** **[Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy]** を選択します。

**ステップ 2** [Add] をクリックします。

**ステップ 3** TLS プロキシ名を指定します（たとえば **diameter-tls-static-proxy**）。[Next] をクリックします。

**ステップ 4** Diameter クライアントとのサーバ信頼関係の設定 （23 ページ） で追加した TLS サーバ プロキシ ID 証明書を選択します。[Next] をクリックします。

まだ ID 証明書を作成していなければ、[Manage] をクリックして追加できます。[Install TLS Server's Certificate] をクリックして、Diameter クライアントの CA 証明書をインストールすることもできます。

必要に応じ、サーバが使用できるセキュリティ アルゴリズム（暗号方式）を、使用可能なアルゴリズムのリストからアクティブ アルゴリズムのリストに移行することによって定義できます。暗号方式を指定しない場合、デフォルトのシステムの暗号方式が使用されます。

（注） テスト目的の場合、または Diameter クライアントを信頼できると確信している場合は、この手順をスキップして、TLS プロキシ コンフィギュレーションで [Enable client authentication during TLS Proxy handshake] を選択解除できます。

**ステップ 5** [Specify the proxy certificate for TLS client] を選択し、次を実行します。

a) ASA TLS プロキシ クライアント用の証明書を選択します。

まだ証明書を追加していない場合は、[Manage] をクリックして今すぐ追加します。

b) Diameter サーバの証明書への署名に使用された CA 証明書をまだ追加していない場合は、[Install TLS Client's Certificate] をクリックして追加します。

c) （任意）クライアントが使用できるセキュリティ アルゴリズム（暗号方式）を、使用可能なアルゴリズムのリストからアクティブ アルゴリズムのリストに移行することによって定義します。

TLS プロキシが使用可能な暗号方式を定義していない場合、プロキシは **[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSL Settings]** の暗号化設定によって定義されたグローバル暗号スイートを使用します。デフォルトでは、グローバル暗号方式レベルは medium です。つまり、NULL-SHA、DES-CBC-SHA、および RC4-MD5 を除くすべての暗号方式が使用できます。ASA で一般に使用可能なものとは異なるスイートを使用する場合にのみ、TLS プロキシに個別の暗号方式を指定します。

d) [Next] をクリックします。

**ステップ 6** [Finish] をクリックしてから、[Apply] をクリックします。

### 次のタスク

Diameter インスペクションで TLS プロキシを使用できるようになりました。モバイル ネットワーク インスペクションのサービス ポリシーの設定 （33 ページ）を参照してください。

# Diameter インスペクション用のローカル ダイナミック証明書によるフル TLS プロキシの設定

Diameter サーバでクライアントごとに一意の証明書が必要な場合は、ローカル ダイナミック証明書（LDC）を生成するように ASA を設定することができます。これらの証明書は、クライアントが接続している間存在し、その後は破棄されます。

この設定では、ASA とクライアント間（Diameter クライアントとのサーバ信頼関係の設定 （23 ページ） で説明されているように）、および ASA と Diameter サーバ間に相互の信頼関係を確立する必要があります。設定は Diameter インスペクション用のスタティック クライアント証明書によるフル TLS プロキシの設定 （24 ページ） で説明するものと同様ですが、Diameter クライアント証明書をインポートする代わりに ASA 上で LDC をセットアップする点が異なります。ASA と Diameter サーバの信頼要件は次のとおりです。

- Diameter サーバの ID 証明書への署名に使用された CA 証明書をインポートする必要があるので、ASA は、TLS ハンドシェイク中にサーバの ID 証明書を検証できます。
- LDC トラストポイントを作成する必要があります。LDC サーバの CA 証明書をエクスポートし、Diameter サーバにインポートする必要があります。エクスポート設定は次のとおりです。証明書のインポートの詳細については、Diameter サーバのドキュメントを参照してください。

## 手順

**ステップ 1** **[Configuration]** > **[Firewall]** > **[Unified Communications]** > **[TLS Proxy]** を選択します。

**ステップ 2** [Add] をクリックします。

**ステップ 3** TLS プロキシ名を指定します（たとえば **diameter-tls-ldc-proxy**）。

**ステップ 4** Diameter クライアントとのサーバ信頼関係の設定 （23 ページ） で追加した TLS サーバ プロキシ ID 証明書を選択します。[Next] をクリックします。

まだ ID 証明書を作成していなければ、[Manage] をクリックして追加できます。[Install TLS Server's Certificate] をクリックして、Diameter クライアントの CA 証明書をインストールすることもできます。

必要に応じ、サーバが使用できるセキュリティ アルゴリズム（暗号方式）を、使用可能なアルゴリズムのリストからアクティブ アルゴリズムのリストに移行することによって定義できます。暗号方式を指定しない場合、デフォルトのシステムの暗号方式が使用されます。

（注） テスト目的の場合、または Diameter クライアントを信頼できると確信している場合は、この手順をスキップして、TLS プロキシ コンフィギュレーションで [Enable client authentication during TLS Proxy handshake] を選択解除できます。

**ステップ 5** [Specify the internal Certificate Authority to sign for local dynamic certificates] を選択し、次の手順を実行します（IP フォン関連のテキストは無視してください）。

この手順は、証明書とキーが未作成であることを前提としています。必要な証明書とキーを作成済みの場合は、それを選択し、セキュリティ アルゴリズムの手順に進んでください。

a) ローカル ダイナミック証明書のキー ペアの場合は、[New] をクリックします。（ボタンを表示するにはダイアログボックスのサイズを変更する必要があります。）

b) 新しいキー ペアの名前（**ldc-signer-key** など）で汎用 RSA 証明書を作成します。[Generate Now] をクリックして、キーを作成します。

[Manage Identity Certificates] ダイアログボックスに戻ります。

c) [Certificate] を選択して [Manage] をクリックし、ASA TLS プロキシ クライアント用の証明書およびキーを作成します。

d) [Manage Identity Certificates] ダイアログボックスで [Add] をクリックします。

e) トラストポイントに名前を付けます（**ldc-server** など）。

f) [Add a new identity certificate] を選択します。

g) [Key Pair] では、ローカル ダイナミック証明書キー用に作成したものと同じキーを選択します。

h) [Certificate Subnet DN] では、必要な識別名属性を選択します。

デバイスの共通名はデフォルトです。Diameter アプリケーションにサブジェクト名に関する固有の要件があるかどうかを確認します。

i) [Generate self-signed certificate] を選択します。このパラメータは必須です。

j) [Act as a local certificate authority and issue dynamic certificates to TLS Proxy] を選択します。このオプションによって、この証明書が LDC 発行元になります。

k) [Add Certificate] をクリックします。

[Manage Identity Certificates] ダイアログボックスに戻ります。

l) 作成したばかりの証明書を選択し、[Export] をクリックします。

Diameter サーバにインポートできるように証明書をエクスポートする必要があります。ファイル名と PEM 形式を指定し、[Export Certificate] をクリックします。

[Manage Identity Certificates] ダイアログボックスに戻ります。

m) 証明書を選択したままで、[OK] をクリックします。

[TLS Proxy] ウィザードに戻ります。証明書が [Certificate] フィールドで選択されていない場合は、今すぐ選択します。

n) （任意）クライアントが使用できるセキュリティ アルゴリズム（暗号方式）を、使用可能なアルゴリズムのリストからアクティブ アルゴリズムのリストに移行することによって定義します。

TLS プロキシが使用可能な暗号方式を定義していない場合、プロキシは **[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSL Settings]** の暗号化設定によって定義されたグローバル暗号スイートを使用します。デフォルトでは、グローバル暗号方式レベルは medium です。つまり、NULL-SHA、DES-CBC-SHA、および RC4-MD5 を除くすべての暗号方式が使用できます。ASA で一般に使用可能なものとは異なるスイートを使用する場合にのみ、TLS プロキシに個別の暗号方式を指定します。

o) [Next] をクリックします。

**ステップ 6** [Finish] をクリックしてから、[Apply] をクリックします。

**ステップ 7** LDC CA 証明書を Diameter サーバにインポートできるようになりました。手順については、Diameter サーバのドキュメントを参照してください。データは Base64 形式であることに注意してください。サーバにバイナリ形式または DER 形式が必要な場合は、OpenSSL ツールを使用して形式を変換する必要があります。

### 次のタスク

Diameter インスペクションで TLS プロキシを使用できるようになりました。モバイル ネットワーク インスペクションのサービス ポリシーの設定 （33 ページ）を参照してください。

## Diameter インスペクション用の TLS オフロードによる TLS プロキシの設定

ASA と Diameter サーバ間のネットワーク パスが安全であると確信している場合は、ASA とサーバ間のデータを暗号化するパフォーマンス コストを回避できます。TLS オフロードを使用すると、TLS プロキシは Diameter クライアントと ASA の間のセッションを暗号化/復号化しますが、Diameter サーバではクリア テキストを使用します。

この設定では、ASA とクライアント間のみに相互の信頼関係を確立する必要があり、これにより設定が簡略化されます。次の手順を実行する前に、Diameter クライアントとのサーバ信頼関係の設定 （23 ページ） の手順を完了します。

### 手順

**ステップ 1** **[Configuration]** > **[Firewall]** > **[Unified Communications]** > **[TLS Proxy]** を選択します。

**ステップ 2** [Add] をクリックします。

**ステップ 3** TLS プロキシ名を指定します（たとえば **diameter-tls-offload-proxy**）。

**ステップ 4** Diameter クライアントとのサーバ信頼関係の設定 （23 ページ） で追加した TLS サーバ プロキシ ID 証明書を選択します。[Next] をクリックします。

まだ ID 証明書を作成していなければ、[Manage] をクリックして追加できます。[Install TLS Server's Certificate] をクリックして、Diameter クライアントの CA 証明書をインストールすることもできます。

必要に応じ、サーバが使用できるセキュリティ アルゴリズム（暗号方式）を、使用可能なアルゴリズムのリストからアクティブ アルゴリズムのリストに移行することによって定義できます。暗号方式を指定しない場合、デフォルトのシステムの暗号方式が使用されます。

（注） テスト目的の場合、または Diameter クライアントを信頼できると確信している場合は、この手順をスキップして、TLS プロキシ コンフィギュレーションで [Enable client authentication during TLS Proxy handshake] を選択解除できます。

**ステップ 5** [Configure the proxy client to use clear text to communicate with the remote TCP client] を選択し、[Next] をクリックします。

**ステップ 6** [Finish] をクリックしてから、[Apply] をクリックします。

**ステップ 7** Diameter ポートは TCP と TLS では異なるため、Diameter サーバからクライアントへのトラフィックに対しては、TCP ポートを TLS ポートに変換する NAT ルールを設定します。

各 Diameter サーバ用のオブジェクト NAT ルールを作成します。

a) **[Configuration]** > **[Firewall]** > **[NAT]** を選択します。
b) **[Add]** > **[Object NAT Rule]** をクリックします。
c) 基本的なプロパティを設定します。
   - [Name]：オブジェクト名（たとえば、DiameterServerA）。
   - [Type]（オブジェクトの場合）：[Host] を選択します。
   - [IP Version]：適宜 IPv4 または IPv6。
   - [IP Address]：Diameter サーバの IPアドレス（たとえば、10.100.10.10）。
   - [Add Automatic Address Translation]：このオプションは必ず選択してください。
   - [Type]（NAT ルールの場合）：[Static] を選択します。
   - [Translated Addr]：Diameter サーバの IP アドレス。これは、オブジェクトの IP アドレスと同じになります（たとえば 10.100.10.10）。
d) [Advanced] をクリックし、次の [Interface] および [Service] オプションを設定します。
   - [Source Interface]：Diameter サーバに接続するインターフェイスを選択します。
   - [Destination Interface]：Diameter クライアントに接続するインターフェイスを選択します。
   - [Protocol]：[TCP] を選択します。
   - [Real Port]：3868 と入力します。これは、デフォルトの Diameter TCP ポート番号です。
   - [Mapped Port]：5868 と入力します。これは、デフォルトの Diameter TLS ポート番号です。
e) [OK] をクリックし、[Add Network Object] ダイアログボックスで [OK] をもう一度クリックします。

### 次のタスク

Diameter インスペクションで TLS プロキシを使用できるようになりました。モバイル ネットワーク インスペクションのサービス ポリシーの設定 （33 ページ）を参照してください。

# M3UA インスペクション ポリシー マップの設定

M3UA インスペクション ポリシー マップを使用して、ポイント コードに基づくアクセス制御を設定します。また、クラスやタイプ別にメッセージをドロップおよびレート制限できます。

デフォルトのポイント コード形式はITUです。別の形式を使用している場合は、ポリシーマップで要求される形式を指定します。

ポイント コードまたはメッセージ クラスに基づいてポリシーを適用しない場合は、M3UA ポリシー マップを設定する必要はありません。マップなしでインスペクションを有効にできます。

### 手順

**ステップ 1** **[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[M3UA]** を選択します。

**ステップ 2** 次のいずれかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- マップを編集するには、マップを選択して [Edit] をクリックします。

**ステップ 3** 新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップを編集するときは、変更できるのは説明のみです。

**ステップ 4** [Parameters] タブをクリックし、必要なオプションを設定します。

- [SS7]：ネットワークで使用される SS7 のバリアント：ITU、ANSI、Japan、China。このオプションによって、ポイント コードの有効な形式が決定します。オプションを設定して M3UA ポリシーを導入した後は、ポリシーを削除しない限り変更はできません。デフォルトのバリアントは ITU です。
- [Enable M3UA Application Server Process (ASP) state validation]：厳密なアプリケーション サーバ プロセス（ASP）状態の確認を実行するかどうか。システムは M3UA セッションの ASP の状態を維持し、検証結果に基づいて ASP メッセージをドロップします。ASP の厳密な状態検証を無効にすると、すべての ASP メッセージが検査されずに転送されます。厳密な ASP のステート チェックが必要なのは、ステートフル フェールオーバーが必要な場合、またはクラスタ内での動作が必要な場合です。ただし、厳密な ASP のステート チェックは、上書きモードでのみ動作し、ロードシェアリングまたはブロードキャスト モードで実行している場合は動作しません（RFC 4666 より）。インスペクションは、エンドポイントごとに ASP が 1 つだけあると仮定します。
- **[Enforce Timeout]** > **[Endpoint]**：M3UA エンドポイントの統計情報を削除するアイドル タイムアウト（hh:mm:ss 形式）。タイムアウトを付けない場合は、0 を指定してください。デフォルトは 30 分（0:30:00）です。
- **[Enforce Timeout]** > **[Session]**：厳密な ASP 状態の確認を有効にしている場合の、M3UA セッションを削除するためのアイドル タイムアウトを hh:mm:ss 形式で設定します。タイムアウトを付けない場合は、0 を指定してください。デフォルトは 30 分（0:30:00）です。このタイムアウトを無効にすると、失効したセッションの削除を防止できます。
- [Message Tag Validation]：指定したメッセージ タイプの特定のフィールドの内容を確認および検証するかどうか。検証で合格しなかったメッセージはドロップされます。検証はメッセージ タイプによって異なります。検証するメッセージを選択します。

- 利用できない宛先ユーザ部（DUPU）：ユーザ/理由フィールドが存在し、有効な理由およびユーザ コードのみが含まれている必要があります。
- エラー：すべての必須フィールドが存在し、許可された値のみが含まれている必要があります。各エラー メッセージには、そのエラー コードの必須フィールドが含まれている必要があります。
- 通知：ステータス タイプおよびステータス情報フィールドには、許可された値のみが含まれている必要があります。

**ステップ 5** [Inspections] タブをクリックし、トラフィックの特性に基づいて実装する特定のインスペクションを定義します。

a) 次のいずれかを実行します。

- [Add] をクリックして、新しい基準を追加します。
- 既存の基準を選択し、[Edit] をクリックします。

b) 基準の一致タイプとして、[Match]（トラフィックは基準と一致する必要がある）または [No Match]（トラフィックは基準と異なる必要がある）を選択します。次に、基準を設定します。

- [Class ID]：M3UA メッセージのクラスとタイプを照合します。次の表に、使用可能な値を示します。これらのメッセージの詳細については、M3UA の RFC およびドキュメンテーションを参照してください。

| M3UA メッセージ クラス | メッセージ ID タイプ |
|---|---|
| 0（管理メッセージ） | 0 ～ 1 |
| 1（転送メッセージ） | 1 |
| 2（SS7 シグナリング ネットワーク管理メッセージ） | 1 ～ 6 |
| 3（ASP 状態メンテナンス メッセージ） | 1 ～ 6 |
| 4（ASP トラフィック メンテナンス メッセージ） | 1 ～ 4 |
| 9（ルーティング キー管理メッセージ） | 1-4 |

- [OPC]：発信ポイント コード、つまりトラフィックの送信元を照合します。ポイント コードは *zone-region-sp* 形式で、各要素に使用可能な値は SS7 バリアントによって異なります。
  - **ITU**：ポイント コードは 3-8-3 形式の 14 ビット値です。値の範囲は、[0-7]-[0-255]-[0-7] です。

- **ANSI**：ポイント コードは 8-8-8 形式の 24 ビット値です。値の範囲は、[0-255]-[0-255]-[0-255] です。
- **Japan**：ポイント コードは 5-4-7 形式の 16 ビット値です。値の範囲は、[0-31]-[0-15]-[0-127] です。
- **China**：ポイント コードは 8-8-8 形式の 24 ビット値です。値の範囲は、[0-255]-[0-255]-[0-255] です。

- [DPC]：宛先ポイントコードを照合します。ポイントコードは、**OPC** について説明しているとおり、*zone-region-sp* 形式です。
- [Service Indicator]：サービス インジケータ番号を照合します（0 ～ 15）。使用可能なサービス インジケータは次のとおりです。これらのサービス インジケータの詳細については、M3UA RFC およびドキュメントを参照してください。
  - 0：シグナリング ネットワーク管理メッセージ
  - 1：シグナリング ネットワーク テストおよびメンテナンス メッセージ
  - 2：シグナリング ネットワーク テストおよびメンテナンス特別メッセージ
  - 3：SCCP
  - 4：電話ユーザ部
  - 5：ISDN ユーザ部
  - 6：データ ユーザ部（コールおよび回線関連のメッセージ）
  - 7：データ ユーザ部（設備の登録およびキャンセル メッセージ）
  - 8：MTP テスト ユーザ部に予約済み
  - 9：ブロードバンド ISDN ユーザ部
  - 10：サテライト ISDN ユーザ部
  - 11：予約済み
  - 12：AAL タイプ 2 シグナリング
  - 13：ベアラー非依存コール制御
  - 14：ゲートウェイ制御プロトコル
  - 15：予約済み

c) クラス ID の一致には、パケットをドロップするかパケット/秒のレート制限を適用するかのいずれかを選択します。他のすべての一致のアクションは、パケットをドロップします。すべての一致に対してロギングをイネーブルにするかどうか選択できます。
d) [OK] をクリックして、インスペクションを追加します。必要に応じてプロセスを繰り返します。

**ステップ 6** [M3UA Inspect Map] ダイアログボックスの [OK] をクリックします。

M3UA インスペクション サービス ポリシーでインスペクション マップを使用できるようになります。

### 次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。モバイル ネットワーク インスペクションのサービス ポリシーの設定 （33 ページ）を参照してください。

# モバイル ネットワーク インスペクションのサービス ポリシーの設定

モバイル ネットワークで使用されるプロトコルのインスペクションは、デフォルトのインスペクション ポリシーでは有効になっていないので、これらのインスペクションが必要な場合は有効にする必要があります。デフォルトのグローバル インスペクション ポリシーを編集するだけで、これらのインスペクションを追加できます。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

### 手順

**ステップ 1** **[Configuration]** > **[Firewall]** > **[Service Policy]** を選択して、ルールを開きます。

- デフォルト グローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択して、[Edit] をクリックします。
- 新しいルールを作成するには、**[Add]** > **[Add Service Policy Rule]** をクリックします。ウィザードの [Rules] ページまで進みます。
- モバイル ネットワーク インスペクション ルールがある場合、またはこれらのインスペクションを追加するルールがある場合は、それを選択し、[Edit] をクリックします。

**ステップ 2** [Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

**ステップ 3** （使用中のポリシーを変更する場合。）異なるインスペクション ポリシー マップを使用するために使用中のポリシーを編集する場合は、インスペクションをディセーブルにし、新しいインスペクション ポリシー マップ名で再度イネーブルにします。

a) 関連するすでに選択されているチェックボックスをオフにします：[GTP]、[SCTP]、[Diameter]
b) [OK] をクリックします。
c) [Apply] をクリックします。
d) この手順を繰り返して [Protocol Inspections] タブに戻ります。

**ステップ 4** 目的のモバイル ネットワーク プロトコルを選択します：[GTP]、[SCTP]、[Diameter]

**ステップ 5** これらのプロトコルの 1 つ以上に対しデフォルト以外のインスペクションが必要な場合は、オプションの横にある [Configure] をクリックして、以下を実行します。

a) デフォルト マップを使用するか、またはユーザが設定したインスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。

b) （Diameter のみ。）暗号化されたメッセージの Diameter インスペクションを有効にするには、[Enable Encrypted Traffic Inspection] を選択し、復号化に使用する TLS プロキシを選択します。

（注） Diameter インスペクション用の TLS プロキシを指定し、Diameter サーバ トラフィックに NAT ポート リダイレクションを適用した場合（たとえば、ポート 5868 から 3868 にサーバ トラフィックをリダイレクトするなど）は、グローバルに、または入力インターフェイスのみでインスペクションを設定します。出力インターフェイスにインスペクションを適用すると、NATed Diameter トラフィックはインスペクションをバイパスします。

c) [Select Inspect Map] ダイアログ ボックスの [OK] をクリックします。

**ステップ 6** [OK] または [Finish] をクリックして、サービス ポリシー ルールを保存します。

# RADIUS アカウンティング インスペクションの設定

RADIUS アカウンティング インスペクションはデフォルトではイネーブルになっていません。RADIUS アカウンティング インスペクションが必要な場合は設定してください。

**手順**

**ステップ 1** RADIUS アカウンティング インスペクション ポリシー マップの設定 （34 ページ）。

**ステップ 2** RADIUS アカウンティング インスペクションのサービス ポリシーの設定 （35 ページ）.

## RADIUS アカウンティング インスペクション ポリシー マップの設定

検査に必要な属性を設定する RADIUS アカウンティング インスペクション ポリシー マップを作成します。

**手順**

**ステップ 1** **[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[RADIUS Accounting]** を選択します。

**ステップ 2** 次のいずれかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- マップを選択して [Edit] をクリックします。

**ステップ 3** 新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップを編集するときは、変更できるのは説明のみです。

**ステップ 4** [Host Parameters] タブをクリックし、各 RADIUS サーバまたは GGSN の IP アドレスを追加します。

ASA がメッセージを許可できるよう、任意で秘密キーを含めることができます。キーがない場合、IP アドレスだけがチェックされます。ASA は、これらのホストから RADIUS アカウンティング メッセージのコピーを受信します。

**ステップ 5** [Other Parameters] タブをクリックし、必要なオプションを設定します。

- [Send responses to the originator of the RADIUS accounting message] ：バナーを ESMTP サーバからマスクするかどうか設定します。
- [Enforce user timeout] ：ユーザのアイドル タイムアウトを実行するかどうか、また、タイムアウト値を設定します。デフォルトは 1 時間です。
- [Enable detection of GPRS accounting]：GPRS 過剰請求の保護を実行するかどうか設定します。セカンダリ PDP コンテキストを適切に処理するため、ASA は、Accounting-Request の Stop および Disconnect メッセージの 3GPP VSA 26-10415 属性をチェックします。この属性が存在する場合、ASA は、設定インターフェイスのユーザ IP アドレスに一致するソース IP を持つすべての接続を切断します。
- [Validate Attribute] ：Accounting-Request Start メッセージを受信する際、ユーザ アカウントのテーブルを作成する場合に使用する追加基準。これらの属性は、ASA が接続を切断するかどうかを決定する場合に役立ちます。

  検証する追加属性を指定しない場合は、Framed IP アドレス属性の IP アドレスのみに基づいて決定されます。追加属性を設定し、ASA が現在追跡されているアドレスを含むが、その他の検証する属性が異なるアカウンティング開始メッセージを受信すると、古い属性を使用して開始するすべての接続は、IP アドレスが新しいユーザに再割り当てされたという前提で、切断されます。

  値の範囲は 1 ～ 191 で、このコマンドは複数回入力できます。属性番号および説明のリストについては、http://www.iana.org/assignments/radius-types を参照してください。

**ステップ 6** [OK] をクリックします。

これで、RADIUS アカウンティング インスペクションのサービス ポリシーで、インスペクション マップを使用できます。

## RADIUS アカウンティング インスペクションのサービス ポリシーの設定

デフォルトのインスペクション ポリシーでは、RADIUS アカウンティング インスペクションはイネーブルにされてないため、この検査が必要な場合はイネーブルにします。RADIUS アカウンティング インスペクションは ASA のトラフィック用に指示されますので、標準ルールではなく、管理インスペクション ルールとして設定してください。

手順

**ステップ 1** **[Configuration]** > **[Firewall]** > **[Service Policy]** を選択して、ルールを開きます。

- 新しいルールを作成するには、[Add] > [Add Management Service Policy Rule] をクリックします。ウィザードの [Rules] ページまで進みます。
- RADIUS アカウンティング インスペクション ルールまたは、RADIUS アカウンティング インスペクションを追加する管理ルールがある場合は、それを選択して、[Edit] をクリックし、[Rule Actions] タブをクリックします。

**ステップ 2** （使用中のポリシーを変更するには）使用中のポリシーを編集して別のインスペクション ポリシー マップを使用するには、RADIUS アカウンティング インスペクションを無効にしてから、新しいインスペクション ポリシー マップの名前で再度イネーブルにしてください。

a) RADIUS アカウンティング マップに [None] を選択します。
b) [OK] をクリックします。
c) [Apply] をクリックします。
d) この手順を繰り返して [Protocol Inspections] タブに戻ります。

**ステップ 3** 目的の [RADIUS Accounting Map] を選択します。この時点でマップを作成できます。詳細については、RADIUS アカウンティング インスペクション ポリシー マップの設定 （34 ページ）を参照してください。

**ステップ 4** [OK] または [Finish] をクリックしてマネジメント サービス ポリシー ルールを保存します。

# モバイルネットワークインスペクションのモニタリング

ここでは、モバイル ネットワーク インスペクションをモニタリングする方法について説明します。

## GTP インスペクションのモニタリング

GTP コンフィギュレーションを表示するには、特権 EXEC モードで show service-policy inspect gtp コマンドを入力します。コマンドを入力するには、**[Tools]** > **[Command Line Interface]** を選択します。

**show service-policy inspect gtp statistics** コマンドを使用して、GTP インスペクションの統計情報を表示します。次にサンプル出力を示します。

```
firewall(config)# show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support                0     msg_too_short              0
  unknown_msg                        0     unexpected_sig_msg         0
  unexpected_data_msg                0     ie_duplicated              0
  mandatory_ie_missing               0     mandatory_ie_incorrect     0
  optional_ie_incorrect              0     ie_unknown                 0
  ie_out_of_order                    0     ie_unexpected              0
```

```
  total_forwarded                  67     total_dropped             1
  signalling_msg_dropped            1     data_msg_dropped          0
  signalling_msg_forwarded         67     data_msg_forwarded        0
  total created_pdp                33     total deleted_pdp         32
  total created_pdpmcb             31     total deleted_pdpmcb      30
  total dup_sig_mcbinfo             0     total dup_data_mcbinfo    0
  no_new_sgw_sig_mcbinfo            0     no_new_sgw_data_mcbinfo   0
  pdp_non_existent                  1
```

**show service-policy inspect gtp statistics** *ip_address* コマンドに IP アドレスを入力すると、特定の GTP エンドポイントの統計情報を取得できます。

```
firewall(config)# show service-policy inspect gtp statistics 10.9.9.9
1 in use, 1 most used, timeout 0:30:00
 GTP GSN Statistics for 10.9.9.9, Idle 0:00:34, restart counter 0
  Tunnels Active                      0
  Tunnels Created                     1
  Tunnels Destroyed                   0
  Total Messages Received             1
                         Signalling Messages        Data Messages
  total received                     1                           0
  dropped                            0                           0
  forwarded                          1                           0
```

**show service-policy inspect gtp pdp-context** コマンドを使用して、PDP コンテキストに関する情報を表示します。GTPv2 の場合、これはベアラー コンテキストです。次に例を示します。

```
ciscoasa(config)# show service-policy inspect gtp pdp-context
4 in use, 5 most used

Version v1,   TID 050542012151705f,  MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22,      Idle 0:52:01,   Timeout 3:00:00,   APN ssenoauth146

Version v2,   TID 0505420121517056,  MS Addr 100.100.100.102,
SGW Addr 10.0.203.24,      Idle 0:00:05,   Timeout 3:00:00,   APN ssenoauth146

Version v2,   TID 0505420121517057,  MS Addr 100.100.100.103,
SGW Addr 10.0.203.25,      Idle 0:00:04,   Timeout 3:00:00,   APN ssenoauth146

Version v2,   TID 0505420121517055,  MS Addr 100.100.100.101,
SGW Addr 10.0.203.23,      Idle 0:00:06,   Timeout 3:00:00,   APN ssenoauth146

ciscoasa(config)# show service-policy inspect gtp pdp-context detail
1 in use, 1 most used

Version v1,   TID 050542012151705f,  MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22,      Idle 0:06:14,   Timeout 3:00:00,   APN ssenoauth146

    user_name (IMSI):  50502410121507    MS address: 2005:a00::250:56ff:fe96:eec
    nsapi: 5                 linked nsapi: 5
    primary pdp: Y         sgsn is Remote
    sgsn_addr_signal: 10.0.203.22    sgsn_addr_data: 10.0.203.22
    ggsn_addr_signal: 10.0.202.22    ggsn_addr_data: 10.0.202.22
    sgsn control teid:     0x00000001    sgsn data teid:        0x000003e8
    ggsn control teid:     0x000f4240    ggsn data teid:        0x001e8480
    signal_sequence:               18     state:    Ready
...
```

PDP またはベアラー コンテキストは、IMSI と NSAPI（GTPv0-1）または IMSI と EBI（GTPv2）の値の組み合わせであるトンネル ID（TID）によって識別されます。GTP トンネルは、それぞれ別個の GSN または SGW/PGW ノードにある、2 つの関連するコンテキストによって定義され、トンネル ID によって識別されます。GTP トンネルは、外部パケット データ ネットワークとモバイル サブスクライバ（MS）ユーザとの間でパケットを転送する場合に必要です。

# SCTP のモニタリング

次のコマンドを使用して、SCTP をモニタできます。コマンドを入力するには、**[Tools]** > **[Command Line Interface]** を選択します。

- **show service-policy inspect sctp**

  SCTP インスペクションの統計情報を表示します。sctp-drop-override カウンタは、PPID がドロップ アクションに一致するたびに増加しますが、パケットには PPID が異なるデータのかたまりが含まれていたのでパケットはドロップされません。次に例を示します。

```
ciscoasa# show service-policy inspect sctp
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: sctp sctp, packet 153302, lock fail 0, drop 20665, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0, sctp-drop-override 4910
        Match ppid 30 35
           rate-limit 1000 kbps, chunk 2354, dropped 10, bytes 21408, dropped-bytes
 958
        Match: ppid 40
           drop, chunk 5849
        Match: ppid 55
           log, chunk 9546
```

- **show sctp** [**detail**]

  現在の SCTP Cookie およびアソシエーションを表示します。SCTP アソシエーションに関する詳細情報を表示するには、**detail** キーワードを追加します。詳細ビューには、マルチホーミング、複数のストリーム、およびフラグメント リアセンブリに関する情報も表示されます。

```
ciscoasa# show sctp

AssocID: 71adeb15
Local:  192.168.107.12/50001 (ESTABLISHED)
Remote: 192.168.108.122/2905 (ESTABLISHED)
Secondary Conn List:
    192.168.108.12(192.168.108.12):2905 to 192.168.107.122(192.168.107.122):50001
    192.168.107.122(192.168.107.122):50001 to 192.168.108.12(192.168.108.12):2905
    192.168.108.122(192.168.108.122):2905 to 192.168.107.122(192.168.107.122):50001

    192.168.107.122(192.168.107.122):50001 to 192.168.108.122(192.168.108.122):2905

    192.168.108.12(192.168.108.12):2905 to 192.168.107.12(192.168.107.12):50001
    192.168.107.12(192.168.107.12):50001 to 192.168.108.12(192.168.108.12):2905
```

- **show conn protocol sctp**

現在の SCTP 接続に関する情報を表示します。

- **show local-host** [**connection sctp** *start*[*-end*]]

  インターフェイスごとに、ASA を経由して SCTP 接続を行うホストに関する情報を表示します。特定の数または範囲の SCTP 接続を持つホストのみを表示するには、**connection sctp** キーワードを追加します。

- **show traffic**

  **sysopt traffic detailed-statistics** コマンドをイネーブルにしている場合は、インターフェイスごとの SCTP 接続とインスペクションの統計情報が表示されます。

# Diameter のモニタリング

次のコマンドを使用して、Diameter をモニタできます。コマンドを入力するには、**[Tools]** > **[Command Line Interface]** を選択します。

- **show service-policy inspect diameter**

  Diameter インスペクションの統計情報を表示します。次に例を示します。

```
ciscoasa# show service-policy inspect diameter
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: Diameter Diameter_map, packet 0, lock fail 0, drop 0, -drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0
        Class-map: log_app
            Log: 5849
         Class-map: block_ip
             drop-connection: 2
```

- **show diameter**

  各 Diameter 接続のステータス情報を表示します。次に例を示します。

```
ciscoasa# show diameter
Total active diameter sessions: 5
Session 3638
       ==========
       ref_count: 1 val = .; 1096298391; 2461;
           Protocol : diameter Context id : 0
           From inside:211.1.1.10/45169 to outside:212.1.1.10/3868
...
```

- **show conn detail**

  接続情報を表示します。Diameter 接続は、Q フラグを使用してマークされます。

- **show tls-proxy**

  TLS プロキシを Diameter インスペクションで使用する場合は、そのプロキシに関する情報が表示されます。

# M3UA のモニタリング

次のコマンドを使用して、M3UA をモニタできます。コマンドを入力するには、**[Tools]** > **[Command Line Interface]** を選択します。

- **show service-policy inspect m3ua drops**

  M3UA インスペクションに対するドロップの統計情報を表示します。

- **show service-policy inspect m3ua endpoint** [*IP_address*]

  M3UA エンドポイントの統計情報を表示します。エンドポイントの IP アドレスを指定して、特定のエンドポイントに関する情報を表示できます。ハイアベイラビリティまたはクラスタ化されたシステムでは、統計情報はユニットごとに提供され、ユニット間で同期されません。次に例を示します。

```
ciscoasa# sh service-policy inspect m3ua endpoint
 M3UA Endpoint Statistics for 10.0.0.100, Idle : 0:00:06 :
                  Forwarded        Dropped          Total Received
 All Messages     21                5                26
 DATA Messages    9                 5                14
 M3UA Endpoint Statistics for 10.0.0.110, Idle : 0:00:06 :
                  Forwarded        Dropped          Total Received
 All Messages     21                8                29
 DATA Messages    9                 8                17
```

- **show service-policy inspect m3ua session**

  厳密なアプリケーション サーバ プロセス（ASP）状態の確認を有効にすると、M3UA セッションに関する情報が表示されます。情報には、送信元アソシエーション ID、セッションがシングルまたはダブルいずれの交換であるか、また、クラスタの場合はクラスタ オーナー セッションとバックアップ セッションのいずれであるかが含まれます。3 つ以上のユニットを持つクラスタでは、ユニットがクラスタから抜けた後に戻って来る場合、古いバックアップ セッションが表示されることがあります。これらの古いセッションは、セッション タイムアウトを無効にしていなければ、タイムアウト時に削除されます。

```
Ciscoasa# show service-policy inspect m3ua session
0 in use, 0 most used
Flags: o - cluster owner session, b - cluster backup session
       d - double exchange      , s - single exchange
AssocID: cfc59fbe in Down state, idle:0:00:05, timeout:0:01:00, bd
AssocID: dac2e123 in Active state, idle:0:00:18, timeout:0:01:00, os
```

- **show service-policy inspect m3ua table**

  分類ルールを含むランタイム M3UA インスペクション テーブルを表示します。

- **show conn detail**

  接続情報を表示します。M3UA 接続は、v フラグを使用してマークされます。

# モバイル ネットワーク インスペクションの履歴

| 機能名 | リリース | 機能情報 |
|---|---|---|
| GTPv2 インスペクションと GTPv0/1 インスペクションの改善 | 9.5(1) | GTP インスペクションは GTPv2 を処理できるようになりました。また、すべてのバージョンの GTP インスペクションで IPv6 アドレスがサポートされるようになりました。<br><br>GTPv1 および GTPv2 に一致する個別のメッセージ ID を設定できるように、**[GTP Inspect Map]** > **[Inspections]** ダイアログボックスが変更されました。[General] パラメータ タブで、[GSN] タイムアウトが [Endpoint] タイムアウトになりました。 |
| SCTP インスペクション | 9.5(2) | ペイロード プロトコル ID（PPID）に基づいてアクションを適用するために、アプリケーション層インスペクションを Stream Control Transmission Protocol（SCTP）トラフィックに適用できるようになりました。<br><br>次の画面が追加または変更されました。**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[SCTP]**、**[Configuration]** > **[Firewall]** > **[Service Policy]** 追加/編集ウィザードの **[Rule Actions]** > **[Protocol Inspection]** タブ。 |
| Diameter インスペクション | 9.5(2) | アプリケーション層インスペクションを Diameter トラフィックに適用できるようになり、アプリケーション ID、コマンドコード、および属性値ペア（AVP）のフィルタリングに基づいてアクションを適用できるようになりました。<br><br>次の画面が追加または変更されました。**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[Diameter]** および [Diameter AVP]、**[Configuration]** > **[Firewall]** > **[Service Policy]** 追加/編集ウィザードの **[Rule Actions]** > **[Protocol Inspection]** タブ。 |
| Diameter インスペクションの改善 | 9.6(1) | TCP/TLS トラフィック上の Diameter を検査し、厳密なプロトコル準拠チェックを適用し、クラスタ モードで SCTP 上の Diameter を検査できるようになりました。<br><br>次の画面が追加または変更されました。**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[Diameter]**、**[Configuration]** > **[Firewall]** > **[Service Policy]** の [add/edit] ウィザードの **[Rule Actions]** > **[Protocol Inspection]** タブ。 |

| 機能名 | リリース | 機能情報 |
|---|---|---|
| クラスタ モードでの SCTP ステートフル インスペクション | 9.6(1) | SCTP ステートフル インスペクションがクラスタ モードで動作するようになりました。また、クラスタ モードで SCTP ステートフル インスペクション バイパスを設定することもできます。<br>追加または変更された画面はありません。 |
| MTP3 User Adaptation（M3UA）インスペクション。 | 9.6(2) | M3UA トラフィックを検査できるようになりました。また、ポイント コード、サービス インジケータ、およびメッセージのクラスとタイプに基づいてアクションを適用できるようになりました。<br>次のページが追加または変更されました：**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspection Maps]** > **[M3UA]**、サービス ポリシー ルールの場合は **[Rule Action]** > **[Protocol Inspection]** タブ。 |
| SCTP マルチストリーミングの並べ替えとリアセンブル、およびフラグメンテーションのサポート。SCTP エンドポイントに複数の IP アドレスが設定された SCTP マルチホーミングのサポート。 | 9.7(1) | このシステムは、SCTP マルチストリーミングの並べ替え、リアセンブル、およびフラグメンテーションを完全にサポートしており、これにより SCTP トラフィックに対する Diameter および M3UA インスペクションの有効性が改善されています。このシステムは、各エンドポイントに複数の IP アドレスが設定された SCTP マルチホーミングもサポートしています。マルチホーミングでは、セカンデリ アドレスに必要なピンホールをシステムが開くので、セカンデリ アドレスを許可するためのアクセス ルールをユーザが設定する必要はありません。SCTP エンドポイントは、それぞれ 3 つの IP アドレスに制限する必要があります。<br>変更された ASDM 画面はありません。 |
| M3UA インスペクションの改善。 | 9.7(1) | M3UA インスペクションは、ステートフル フェールオーバー、半分散クラスタリング、およびマルチホーミングをサポートするようになりました。また、アプリケーション サーバ プロセス（ASP）の状態の厳密な検証や、さまざまなメッセージの検証も設定できます。ASP 状態の厳密な検証は、ステートフル フェールオーバーとクラスタリングに必要です。<br>次の画面が変更されました。**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspection Maps]** > **[M3UA]** [Add/Edit] ダイアログボックス。 |

| 機能名 | リリース | 機能情報 |
|---|---|---|
| TLS プロキシ サーバの SSL 暗号スイートの設定サポート | 9.8(1) | ASA が TLS プロキシサーバとして動作している場合は、SSL 暗号スイートを設定できるようになりました。以前は、**[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSL Settings]** > **[Encryption]** ページでASA のグローバル設定のみが可能でした。<br>次の画面が変更されました。**[Configuration]** > **[Firewall]** > **[Unified Communications]** > **[TLS Proxy]**、[Add/Edit] ダイアログボックス、[Server Configuration] ページ。 |
| MSISDN および選択モードのフィルタリング、アンチリプレイ、およびユーザ スプーフィング保護に対する GTP インスペクションの機能拡張。 | 9.10(1) | モバイル ステーション国際サブスクライバ電話番号（MSISDN）または選択モードに基づいて PDP コンテキストの作成メッセージをドロップするように GTP インスペクションを設定できるようになりました。また、アンチリプレイとユーザ スプーフィング保護も実装できます。<br>**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspection Maps]** > **[GTP]** > **[Add/Edit]** ダイアログボックスが変更されました。 |