CHAPTER 13

管理アプリケーション プロトコルのインスペクションの設定

この章では、アプリケーション レイヤ プロトコル インスペクションを設定する方法について説明します。インスペクション エンジンは、ユーザのデータ パケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリ チャネルを開くサービスに必要です。これらのプロトコルでは、高速パスでパケットを渡すのではなく、ASA で詳細なパケット インスペクションを行う必要があります。そのため、インスペクション エンジンがスループット全体に影響を与えることがあります。

ASA では、デフォルトでいくつかの一般的なインスペクション エンジンがイネーブルになっていますが、ネットワークによっては他のインスペクション エンジンをイネーブルにしなければならない場合があります。

この章は、次の項で構成されています。

DCERPC インスペクション

この項では、DCERPC インスペクション エンジンについて説明します。この項では、次のトピックについて取り上げます。

DCERPC の概要

DCERPC は、Microsoft 社の分散クライアント / サーバ アプリケーションで広く使われているプロトコルです。このプロトコルによって、ソフトウェア クライアントがサーバにあるプログラムをリモートで実行できるようになります。

通常、このプロトコルの接続では、クライアントが予約済みポート番号で接続を受け入れるエンドポイント マッパーというサーバに、必要なサービスについてダイナミックに割り当てられるネットワーク情報を問い合わせます。次に、クライアントは、サービスを提供しているサーバのインスタンスへのセカンダリ接続をセットアップします。セキュリティ アプライアンスは、適切なポート番号とネットワーク アドレスへのセカンダリ接続を許可し、必要に応じて NAT を適用します。

DCERPC インスペクション マップは、TCP の予約済みポート 135 を経由した、EPM とクライアント間のネイティブ TCP の通信を検査します。クライアント用に EPM のマッピングとルックアップがサポートされています。クライアントとサーバは、どのセキュリティ ゾーンにあってもかまいません。埋め込まれたサーバの IP アドレスとポート番号は、EPM からの応答メッセージで受け取ります。クライアントが EPM から返されたサーバのポートに対して複数の接続を試みる可能性があるので、ピンホールが複数使用でき、ユーザがそのタイムアウトを設定できるようになっています。

（注）　DCERPC インスペクションでは、ASA にピンホールを開くための EPM とクライアント間の通信だけがサポートされます。EPM を使用しない RPC 通信を使用するクライアントは、DCERPC インスペクションではサポートされません。

Select DCERPC Map

[Add/Edit Service Policy Rule Wizard] > [Rule Actions] > [Protocol Inspection] タブ > [Select DCERPC Map]

[Select DCERPC Map] ダイアログボックスでは、DCERPC マップを選択または新しく作成できます。DCERPC マップにより、DCERPC アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select DCERPC Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default DCERPC inspection map] : デフォルトの DCERPC マップの使用を指定します。
- [Select a DCERPC map for fine control over inspection] : 定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add] : そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

DCERPC Inspect Map

[Configuration] > [Global Objects] > [Inspect Maps] > [DCERPC]

[DCERPC] ペインでは、DCERPC アプリケーションの事前に設定されたインスペクション マップを表示できます。DCERPC マップでは、DCERPC アプリケーション インスペクションのデフォルト設定値を変更できます。

DCERPC は、Microsoft 社の分散クライアント / サーバ アプリケーションで広く使われているプロトコルです。このプロトコルによって、ソフトウェア クライアントがサーバにあるプログラムをリモートで実行できるようになります。

通常、このプロトコルの接続では、クライアントがウェルノウン ポート番号で接続を受け入れるエンドポイント マッパー（EPM）というサーバに、必要なサービスについて動的に割り当てられるネットワーク情報を問い合わせます。次に、クライアントは、サービスを提供しているサーバのインスタンスへのセカンダリ接続をセットアップします。セキュリティ アプライアンスは、適切なポート番号とネットワーク アドレスへのセカンダリ接続を許可し、必要に応じて NAT を適用します。

DCERPC インスペクション マップは、TCP の予約済みポート 135 を経由した、EPM とクライアント間のネイティブ TCP の通信を検査します。クライアント用に EPM のマッピングとルックアップがサポートされています。クライアントとサーバは、どのセキュリティ ゾーンにあってもかまいません。埋め込まれたサーバの IP アドレスとポート番号は、EPM からの応答メッセージで受け取ります。クライアントは EPM によって返されたサーバ ポートに複数の接続を試行できるため、ユーザが設定可能なタイムアウトのあるピンホールを複数使用できます。

フィールド

- [DCERPC Inspect Maps] : 定義されている DCERPC インスペクション マップを一覧表示するテーブルです。
- [Add] : 新しい DCERPC インスペクションを設定します。DCERPC インスペクション マップを編集するには、[DCERPC Inspect Maps] テーブルで DCERPC のエントリを選択し、[Customize] をクリックします。
- [Delete] : [DCERPC Inspect Maps] テーブルで選択したインスペクション マップを削除します。
- [Security Level] : セキュリティ レベル（High、Medium、Low）を選択します。
  - Low

    ピンホールのタイムアウト : 00:02:00

    エンドポイント マッパー サービス : 適用強制しない

    エンドポイント マッパー サービス ルックアップ : イネーブル

    エンドポイント マッパー サービス ルックアップのタイムアウト : 00:05:00
  - Medium : デフォルト

    ピンホールのタイムアウト : 00:01:00

    エンドポイント マッパー サービス : 適用強制しない

    エンドポイント マッパー サービス ルックアップ : ディセーブル
  - High

    ピンホールのタイムアウト : 00:01:00

    エンドポイント マッパー サービス : 適用強制する

    エンドポイント マッパー サービス ルックアップ : ディセーブル
  - [Customize] : [Add/Edit DCERPC Policy Map] ダイアログボックスを開き、追加の設定を行います。
  - [Default Level] : セキュリティ レベルをデフォルトの Medium レベルに戻します。

Add/Edit DCERPC Policy Map

[Configuration] > [Global Objects] > [Inspect Maps] > [DCERPC] > [DCERPC Inspect Map] > [Basic/Advanced View]

[Add/Edit DCERPC Policy Map] ペインでは、DCERPC アプリケーション インスペクション マップのセキュリティ レベルとパラメータを設定できます。

フィールド

- [Name]：DCERPC マップの追加時に DCERPC マップの名前を入力します。DCERPC マップの編集時には、事前に設定した DCERPC マップの名前が表示されます。
- [Description]：DCERPC マップの説明を 200 文字以内で入力します。
- [Security Level]：セキュリティ レベル（High、Medium、Low）を選択します。
  - Low

    ピンホールのタイムアウト：00:02:00

    エンドポイント マッパー サービス：適用強制しない

    エンドポイント マッパー サービス ルックアップ：イネーブル

    エンドポイント マッパー サービス ルックアップのタイムアウト：00:05:00
  - Medium：デフォルト

    ピンホールのタイムアウト：00:01:00

    エンドポイント マッパー サービス：適用強制しない

    エンドポイント マッパー サービス ルックアップ：ディセーブル
  - High

    ピンホールのタイムアウト：00:01:00

    エンドポイント マッパー サービス：適用強制する

    エンドポイント マッパー サービス ルックアップ：ディセーブル
  - [Default Level]：セキュリティ レベルをデフォルトの Medium レベルに戻します。
- [Details]：詳細な設定を行うためのパラメータを表示します。
  - [Pinhole Timeout]：ピンホール タイムアウトを設定します。クライアントが使用するサーバ情報は、複数の接続のエンドポイント マッパーから返される場合があるため、タイムアウト値はクライアントのアプリケーション環境を考慮して設定します。範囲は、0:0:1 ～ 1193:0:0 です。デフォルトは 2 分です。
  - [Enforce endpoint-mapper service]：バインディング中にエンドポイント マッパー サービスを適用します。
  - [Enable endpoint-mapper service lookup]：エンドポイント マッパー サービスのルックアップをイネーブルにします。ディセーブルの場合、ピンホール タイムアウトが適用されます。

    [Enforce Service Lookup Timeout]：指定されたサービス ルックアップ タイムアウトを適用します。

    [Service Lookup Timeout]：ルックアップでピンホールした場合のタイムアウトを設定します。

GTP インスペクション

この項では、GTP インスペクション エンジンについて説明します。この項では、次のトピックについて取り上げます。

- 「GTP インスペクションの概要」（P.13-5）
- 「Select GTP Map」（P.13-6）
- 「GTP Inspect Map」（P.13-6）
- 「IMSI Prefix Filtering」（P.13-7）

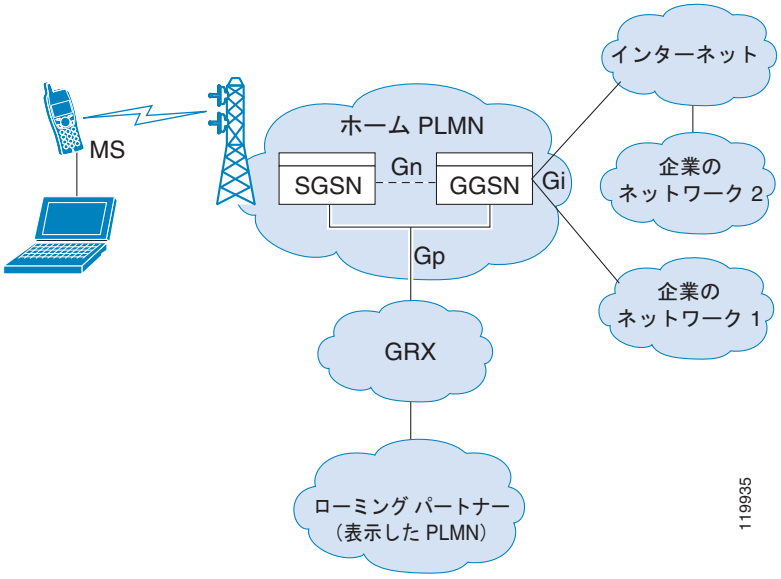
- 「[Add/Edit GTP Policy Map]（セキュリティ レベル）」（P.13-7）
- 「[Add/Edit GTP Policy Map]（詳細）」（P.13-8）
- 「Add/Edit GTP Map」（P.13-10）

（注）　GTP インスペクションには、特別なライセンスが必要です。

GTP インスペクションの概要

GPRS は、モバイル ユーザに対して、GSM ネットワークと企業ネットワークまたはインターネットとの間で中断しない接続を提供します。GGSN 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 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（図 13-1 を参照）。

図 13-1　　GPRS トンネリング プロトコル



UMTS は、固定回線テレフォニー、モバイル、インターネット、コンピュータ テクノロジーの商用コンバージェンスです。UTRAN は、このシステムで無線ネットワークを実装するためのネットワーキング プロトコルです。GTP を使用すると、GGSN、SGSN、および UTRAN 間の UMTS/GPRS バックボーンで、マルチプロトコル パケットをトンネリングできます。

GTP には固有のセキュリティやユーザ データの暗号化は含まれていませんが、ASA で GTP を使用することによって、これらの危険性からネットワークを保護できます。

SGSN は、GTP を使用する GGSN に論理的に接続されます。GTP を使用すると、GSN 間の GPRS バックボーンで、マルチプロトコル パケットをトンネリングできます。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って、SGSN は、トンネルの作成、変更、および削除を行い、モバイル ステーションに GPRS ネットワーク アクセスを提供できます。GTP は、トンネリング メカニズムを使用して、ユーザ データ パケットを伝送するためのサービスを提供します。

（注）　GTP をフェールオーバーと同時に使用しているとき、GTP 接続が確立され、データがトンネルを超えて伝送される前にアクティブ装置に障害が発生した場合、GTP データ接続（「j」フラグが設定されています）は、スタンバイ装置に複製されません。これは、アクティブ装置が初期接続をスタンバイ装置に複製しないためです。

Select GTP Map

[Add/Edit Service Policy Rule Wizard] > [Rule Actions] > [Protocol Inspection] タブ > [Select GTP Map]

[Select GTP Map] ダイアログボックスでは、GTP マップを選択または新しく作成できます。GTP マップにより、GTP アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select GTP Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

（注）　GTP インスペクションには、特別なライセンスが必要です。必要なライセンスがないときに ASA で GTP アプリケーション インスペクションのイネーブル化を試みると、ASA はエラー メッセージを表示します。

フィールド

- [Use the default GTP inspection map]：デフォルトの GTP マップの使用を指定します。
- [Select an GTP map for fine control over inspection]：定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

GTP Inspect Map

[Configuration] > [Global Objects] > [Inspect Maps] > [GTP]

[GTP] ペインでは、GTP アプリケーションの事前に設定されたインスペクション マップを表示できます。GTP マップでは、GTP アプリケーション インスペクションのデフォルト設定値を変更できます。

GTP は比較的新しいプロトコルで、インターネットなど TCP/IP ネットワークと無線接続する場合のセキュリティを提供します。GTP マップを使用して、タイムアウト値、メッセージ サイズ、トンネル数、およびセキュリティ アプライアンスを通過する GTP バージョンを制御できます。

（注）　GTP インスペクションには、特別なライセンスが必要です。

フィールド

- [GTP Inspect Maps]：定義されている GTP インスペクション マップを一覧表示するテーブルです。
- [Add]：新しい GTP インスペクション マップを設定します。GTP インスペクション マップを編集するには、[GTP Inspect Maps] テーブルで GTP のエントリを選択し、[Customize] をクリックします。
- [Delete]：[GTP Inspect Maps] テーブルで選択したインスペクション マップを削除します。
- [Security Level]：セキュリティ レベルは常に Low です。

  - エラーを許可しない
  - トンネルの最大数：500
  - GSN タイムアウト：00:30:00
  - PDP コンテキスト タイムアウト：00:30:00
  - 要求タイムアウト：00:01:00
  - シグナリング タイムアウト：00:30:00
  - トンネル タイムアウト：01:00:00
  - T3 応答タイムアウト：00:00:20
  - 未知のメッセージ ID をドロップしてログを出力
- [IMSI Prefix Filtering]：[IMSI Prefix Filtering] ダイアログボックスを開き、IMSI プレフィックス フィルタを設定します。
- [Customize]：[Add/Edit GTP Policy Map] ダイアログボックスを開き、追加の設定を行います。
- [Default Level]：セキュリティ レベルをデフォルトに戻します。

IMSI Prefix Filtering

[Configuration] > [Global Objects] > [Inspect Maps] > [GTP] > [IMSI Prefix Filtering]

[IMSI Prefix] タブでは、GTP 要求の中で使用できるように IMSI プレフィックスを定義できます。

フィールド

- [Mobile Country Code]：0 以外の 3 桁の値でモバイル カントリ コードを定義します。エントリが 1 桁または 2 桁の場合には、その先頭に 0 が付加されて 3 桁の値が作成されます。
- [Mobile Network Code]：2 桁または 3 桁の数字でネットワーク コードを定義します。
- [Add]：指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルに追加します。
- [Delete]：指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルから削除します。

[Add/Edit GTP Policy Map]（セキュリティ レベル）

[Configuration] > [Global Objects] > [Inspect Maps] > [GTP] > [GTP Inspect Map] > [Basic View]

[Add/Edit GTP Policy Map] ペインでは、GTP アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：GTP マップの追加時に GTP マップの名前を入力します。GTP マップの編集時には、事前に設定した GTP マップの名前が表示されます。
- [Description]：GTP マップの説明を 200 文字以内で入力します。
- [Security Level]：セキュリティ レベルは常に Low です。

  エラーを許可しない

  トンネルの最大数：500

  GSN タイムアウト：00:30:00

PDP コンテキスト タイムアウト：00:30:00

要求タイムアウト：00:01:00

シグナリング タイムアウト：00:30:00

トンネル タイムアウト：01:00:00

T3 応答タイムアウト：00:00:20

未知のメッセージ ID をドロップしてログを出力

- [IMSI Prefix Filtering]：[IMSI Prefix Filtering] ダイアログボックスを開き、IMSI プレフィックス フィルタを設定します。
- [Default Level]：セキュリティ レベルをデフォルトに戻します。

- [Details]：詳細な設定を行うための [Parameters] タブ、[IMSI Prefix Filtering] タブ、および [Inspections] タブを表示します。

[Add/Edit GTP Policy Map]（詳細）

[Configuration] > [Global Objects] > [Inspect Maps] > [GTP] > [GTP Inspect Map] > [Advanced View]

[Add/Edit GTP Policy Map] ペインでは、GTP アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：GTP マップの追加時に GTP マップの名前を入力します。GTP マップの編集時には、事前に設定した GTP マップの名前が表示されます。
- [Description]：GTP マップの説明を 200 文字以内で入力します。
- [Security Level]：設定するセキュリティ レベルと IMSI プレフィックス フィルタリング設定を表示します。
- [Permit Parameters]：このタブで GTP インスペクション マップの許可パラメータを設定します。
  - Object Groups to Add

    [From object group]：オブジェクト グループを指定して、または [Browse] ボタンをクリックして、[Add Network Object Group] ダイアログボックスを開きます。

    [To object group]：オブジェクト グループを指定して、または [Browse] ボタンをクリックして、[Add Network Object Group] ダイアログボックスを開きます。
  - [Add]：指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルに追加します。
  - [Delete]：指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルから削除します。
  - [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 から送信します。デフォルトでは、解析時に失敗したすべての無効パケットがドロップされます。
- [General Parameters]：このタブで GTP インスペクション マップの一般パラメータを設定します。
  - [Maximum Number of Requests]：許容される要求キュー サイズのデフォルト最大値を変更できます。要求キュー サイズのデフォルト最大値は 200 です。キューで応答待ちができる GTP 要求数の最大値を指定します。1 ～ 9999999 の範囲で指定できます。

- [Maximum Number of Tunnels]：許容されるトンネル数のデフォルト最大値を変更できます。デフォルトのトンネル制限値は 500 です。許可されるトンネルの最大数を指定します。グローバルなトンネル全体の制限値を 1 ～ 9999999 の範囲で指定できます。
- Timeouts

  [GSN timeout]：GSN を削除するまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 30 分です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。

  [PDP-Context timeout]：GTP セッションで PDP コンテキストを受け取るまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 30 分です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。

  [Request Queue]：GTP セッション中に GTP メッセージを受け取るまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 1 分です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。

  [Signaling]：GTP シグナリングを削除するまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 30 分です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。

  [Tunnel]：GTP トンネルの非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 1 時間です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は切断しないことを意味します。Request timeout：GTP 要求のアイドル タイムアウト値を指定します。

  [T3-Response timeout]：接続を削除するまでの、応答待ち時間の最大値を指定します。

- [IMSI Prefix Filtering]：このタブで GTP インスペクション マップの IMSI プレフィックス フィルタリングを設定します。
  - [Mobile Country Code]：0 以外の 3 桁の値でモバイル カントリ コードを定義します。エントリが 1 桁または 2 桁の場合には、その先頭に 0 が付加されて 3 桁の値が作成されます。
  - [Mobile Network Code]：2 桁または 3 桁の数字でネットワーク コードを定義します。
  - [Add]：指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルに追加します。
  - [Delete]：指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルから削除します。
- [Inspections]：このタブで GTP インスペクション マップを設定します。
  - [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion]：GTP インスペクションの基準を示します。
  - [Value]：GTP インスペクションで照合する値を示します。
  - [Action]：照合条件が一致したときのアクションを示します。
  - [Log]：ログの状態を示します。
  - [Add]：[Add GTP Inspect] ダイアログボックスが開き、GTP インスペクションを追加できます。
  - [Edit]：[Edit GTP Inspect] ダイアログボックスが開き、GTP インスペクションを編集できます。
  - [Delete]：GTP インスペクションを削除します。
  - [Move Up]：インスペクションをリストの上に移動します。

- [Move Down]：インスペクションをリストの下に移動します。

Add/Edit GTP Map

[Configuration] > [Global Objects] > [Inspect Maps] > [GTP] > [GTP Inspect Map] > [Add/Edit GTP Map]

[Add/Edit GTP Inspect] ダイアログボックスでは、GTP インスペクション マップの照合基準と値を定義できます。

フィールド

- [Match Type]：トラフィックと値を一致させるかどうかを指定します。

  たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。

- [Criterion]：GTP トラフィックに適用する照合基準を指定します。
  - [Access Point Name]：アクセス ポイント名を照合します。
  - [Message ID]：メッセージ ID を照合します。
  - [Message Length]：メッセージの長さを照合します。
  - [Version]：バージョンを照合します。
- [Access Point Name Criterion Values]：照合するアクセス ポイント名を指定します。デフォルトでは、有効な APN のメッセージをすべて検査します。すべての APN が指定できます。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
  - [Action]：Drop。
  - [Log]：イネーブルまたはディセーブルにします。
- [Message ID Criterion Values]：照合するメッセージの数値識別子を指定します。有効な指定範囲は 1 ～ 255 です。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。
  - [Value]：値を完全一致で照合するか、範囲で照合するかを指定します。

    [Equals]：値を入力します。

    [Range]：値の範囲を入力します。
  - [Action]：Drop packet または limit rate (pps)。
  - [Log]：イネーブルまたはディセーブルにします。
- [Message Length Criterion Values]：許可される UDP ペイロードの、メッセージの長さのデフォルト最大値を変更できます。
  - [Minimum value]：UDP ペイロードの最小バイト数を指定します。範囲は、1 ～ 65,536 です。
  - [Maximum value]：UDP ペイロードの最大バイト数を指定します。範囲は、1 ～ 65,536 です。
  - [Action]：Drop packet。
  - [Log]：イネーブルまたはディセーブルにします。

- [Version Criterion Values]：照合するメッセージの GTP バージョンを指定します。有効な指定範囲は 0 ～ 255 です。バージョン 0 を指定するには 0 を使用し、バージョン 1 を指定するには 1 を使用します。GTP のバージョン 0 はポート 3386 を使用し、バージョン 1 はポート 2123 を使用します。デフォルトでは、すべての GTP バージョンが許可されます。
  - [Value]：値を完全一致で照合するか、範囲で照合するかを指定します。

    [Equals]：値を入力します。

    [Range]：値の範囲を入力します。
  - [Action]：Drop packet。
  - [Log]：イネーブルまたはディセーブルにします。

RADIUS アカウンティング インスペクション

この項では、IM インスペクション エンジンについて説明します。この項では、次のトピックについて取り上げます。

RADIUS アカウンティング インスペクションの概要

よく知られている問題の 1 つに GPRS ネットワークでの過剰請求攻撃があります。過剰請求攻撃では、利用していないサービスについて料金を請求されるため、ユーザが怒りや不満を感じるおそれがあります。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、セキュリティ アプライアンスは、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、セキュリティ アプライアンスは、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。

セキュリティ アプライアンス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。事前共有秘密キーを設定しないと、セキュリティ アプライアンスは、メッセージの送信元を検証する必要がなく、その IP アドレスが、RADIUS メッセージの送信を許可されているアドレスの 1 つかどうか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終了メッセージで 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。

Select RADIUS Accounting Map

[Select RADIUS Accounting Map] ダイアログボックスでは、定義済み RADIUS アカウンティング マップを選択するか、新しい RADIUS アカウンティング マップを定義できます。

フィールド

- [Add]：新しい RADIUS アカウンティング マップを追加できます。

Add RADIUS Accounting Policy Map

[Add RADIUS Accounting Policy Map] ダイアログボックスでは、RADIUS アカウンティング マップの基本設定を追加できます。

フィールド

- [Name]：事前に設定されている RADIUS アカウンティング マップの名前を入力します。
- [Description]：RADIUS アカウンティング マップの説明を 100 文字以内で入力します。
- [Host Parameters] タブ：
  - [Host IP Address]：RADIUS メッセージの送信元となるホストの IP アドレスを指定します。
  - [Key: (optional)]：キーを指定します。
  - [Add]：[Host] テーブルにホスト エントリを追加します。
  - [Delete]：[Host] テーブルからホスト エントリを削除します。
- [Other Parameters] タブ：
  - [Attribute Number]：「Accounting Start」を受信したときに確認する属性番号を指定します。
  - [Add]：[Attribute] テーブルにエントリを追加します。
  - [Delete]：[Attribute] テーブルからエントリを削除します。
  - [Send response to the originator of the RADIUS message]：RADIUS メッセージの送信元ホストにメッセージを返信します。
  - [Enforce timeout]：ユーザのタイムアウトをイネーブルにします。
  - [Users Timeout]：データベース内のユーザのタイムアウト（hh:mm:ss）。

RADIUS インスペクション マップ

[RADIUS] ペインでは、事前に設定された RADIUS アプリケーション インスペクション マップを表示できます。RADIUS マップでは、RADIUS アプリケーション インスペクションで使用されるコンフィギュレーションのデフォルト値を変更できます。RADIUS マップを使用すると、過剰請求攻撃を防御できます。

フィールド

- [Name]：インスペクション マップの名前を 40 文字以内で入力します。
- [Description]：インスペクション マップの説明を 200 文字以内で入力します。
- [RADIUS Inspect Maps]：定義されている RADIUS インスペクション マップを一覧表示するテーブルです。定義されているインスペクション マップは、[Inspect Maps] ツリーの [RADIUS] エリアにも表示されます。
- [Add]：新規の RADIUS インスペクション マップを、[RADIUS Inspect Maps] テーブルの定義リストと [Inspect Maps] ツリーの [RADIUS] エリアに追加します。RADIUS マップを新たに設定するには、[Inspect Maps] ツリーで [RADIUS] エントリを選択します。
- [Delete]：[RADIUS Inspect Maps] テーブルで選択したアプリケーション インスペクション マップを削除します。[Inspect Maps] ツリーの [RADIUS] エリアからも削除されます。

RADIUS インスペクション マップ（ホスト）

[RADIUS Inspect Map Host Parameters] ペインでは、インスペクション マップのホスト パラメータを設定できます。

フィールド

- [Name]：事前に設定されている RADIUS アカウンティング マップの名前を示します。
- [Description]：RADIUS アカウンティング マップの説明を 200 文字以内で入力します。
- [Host Parameters]：ホストのパラメータを設定できます。
  - [Host IP Address]：RADIUS メッセージの送信元となるホストの IP アドレスを指定します。
  - [Key: (optional)]：キーを指定します。
- [Add]：[Host] テーブルにホスト エントリを追加します。
- [Delete]：[Host] テーブルからホスト エントリを削除します。

RADIUS インスペクション マップ（その他）

[RADIUS Inspect Map Other Parameters] ペインでは、インスペクション マップに追加するパラメータを設定できます。

フィールド

- [Name]：事前に設定されている RADIUS アカウンティング マップの名前を示します。
- [Description]：RADIUS アカウンティング マップの説明を 200 文字以内で入力します。
- [Other Parameters]：追加するパラメータを設定できます。
  - [Send response to the originator of the RADIUS message]：RADIUS メッセージの送信元ホストにメッセージを返信します。
  - [Enforce timeout]：ユーザのタイムアウトをイネーブルにします。

    [Users Timeout]：データベース内のユーザのタイムアウト（hh:mm:ss）。
  - [Enable detection of GPRS accounting]：GPRS アカウンティングの検出をイネーブルにします。このオプションは、GTP/GPRS ライセンスがイネーブルの場合にだけ使用できます。
  - [Validate Attribute]：属性情報です。

[Attribute Number]：「Accounting Start」を受信したときに確認する属性番号を指定します。

[Add]：[Attribute] テーブルにエントリを追加します。

[Delete]：[Attribute] テーブルからエントリを削除します。

RSH インスペクション

RSH インスペクションはデフォルトでイネーブルになっています。RSH プロトコルは、TCP ポート 514 で RSH クライアントから RSH サーバへの TCP 接続を使用します。クライアントとサーバは、クライアントが STDERR 出力ストリームを受信する TCP ポート番号をネゴシエートします。RSH インスペクションは、必要に応じて、ネゴシエートされたポート番号の NAT をサポートします。

SNMP インスペクション

この項では、IM インスペクション エンジンについて説明します。この項では、次のトピックについて取り上げます。

- 「SNMP インスペクションの概要」（P.13-14）
- 「Select SNMP Map」（P.13-14）
- 「SNMP Inspect Map」（P.13-15）

SNMP インスペクションの概要

SNMP アプリケーション インスペクションでは、SNMP トラフィックを特定のバージョンの SNMP に制限できます。以前のバージョンの SNMP は安全性が低いため、セキュリティ ポリシーを使用して特定の SNMP バージョンを拒否する必要が生じる場合もあります。ASA は、SNMP バージョン 1、2、2c、または 3 を拒否できます。許可するバージョンは、SNMP マップを作成して制御します。

作成した SNMP マップは、「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設定」（P.9-7）に従って SNMP インスペクションをイネーブルにすると適用できます。

Select SNMP Map

[Add/Edit Service Policy Rule Wizard] > [Rule Actions] > [Protocol Inspection] タブ > [Select SNMP Map]

[Select SNMP Map] ダイアログボックスでは、SNMP マップを選択または新しく作成できます。SNMP マップにより、SNMP アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select SNMP Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default SNMP inspection map]：デフォルトの SNMP マップの使用を指定します。
- [Select an SNMP map for fine control over inspection]：定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

SNMP Inspect Map

[Configuration] > [Global Objects] > [Inspect Maps] > [SNMP]

[SNMP] ペインでは、SNMP アプリケーションの事前に設定されたインスペクション マップを表示できます。SNMP マップでは、SNMP アプリケーション インスペクションのデフォルト設定値を変更できます。

フィールド

- [Map Name]：すでに設定されているアプリケーション インスペクション マップを一覧表示します。マップを選択し、[Edit] をクリックして、既存のマップの表示または変更ができます。
- [Add]：新しい SNMP インスペクション マップを設定します。
- [Edit]：[SNMP Inspect Maps] テーブルで選択した SNMP のエントリを編集します。
- [Delete]：[SNMP Inspect Maps] テーブルで選択したインスペクション マップを削除します。

Add/Edit SNMP Map

[Configuration] > [Global Objects] > [Inspect Maps] > [SNMP] > [Add/Edit SNMP Map]（このダイアログボックスにはさまざまなパスからアクセスできます）。

[Add/Edit SNMP Map] ダイアログボックスでは、SNMP のアプリケーション インスペクションを制御する SNMP マップを新規作成できます。

フィールド

- [SNMP Map Name]：アプリケーション インスペクション マップの名前を定義します。
- [SNMP version 1]：SNMP バージョン 1 のアプリケーション インスペクションをイネーブルにします。
- [SNMP version 2 (party based)]：SNMP バージョン 2 のアプリケーション インスペクションをイネーブルにします。
- [SNMP version 2c (community based)]：SNMP バージョン 2c のアプリケーション インスペクションをイネーブルにします。
- [SNMP version 3]：SNMP バージョン 3 のアプリケーション インスペクションをイネーブルにします。

XDMCP インスペクション

XDMCP インスペクションはデフォルトでイネーブルになっていますが、XDMCP インスペクション エンジンは、**established** コマンドが適切に構成されていないと使用できません。

XDMCP は、UDP ポート 177 を使用して X セッションをネゴシエートするプロトコルです。X セッションは確立時に TCP を使用します。

XWindows セッションを正常にネゴシエートして開始するために、ASA は、Xhosted コンピュータからの TCP 戻り接続を許可する必要があります。戻り接続を許可するには、ASA で **established** コマンドを使用します。XDMCP がディスプレイを送信するポートをネゴシエートすると、**established** コマンドが参照され、この戻り接続を許可すべきかどうかが確認されます。

XWindows セッション中、マネージャは予約済みポート 6000 | n 上でディスプレイ Xserver と通信します。次の端末設定を行うと、各ディスプレイは別々に Xserver と接続します。

```
setenv DISPLAY Xserver:n
```

n はディスプレイ番号です。

XDMCP が使用されている場合、ディスプレイは IP アドレスを使用してネゴシエートされます。IP アドレスは、ASA が必要に応じて NAT を行うことができます。XDCMP インスペクションでは、PAT はサポートされません。