CHAPTER 12

管理アプリケーション プロトコルのインスペクション

ここでは、管理アプリケーション プロトコルのアプリケーション インスペクションについて説明します。特定のプロトコルに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適用の方法全体については、「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」（P.8-1）を参照してください。

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。

DCERPC インスペクション

ここでは、DCERPC インスペクション エンジンについて説明します。

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、EPM とウェルノウン TCP ポート 135 上のクライアントとの間のネイティブ TCP 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、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 の検査は、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。

DCERPC インスペクションの設定

DCERPC 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。DCERPC インスペクションが必要な場合は設定する必要があります。

手順

ステップ 1　「DCERPC インスペクション ポリシー マップの設定」（P.12-2）

ステップ 2　「DCERPC インスペクションのサービス ポリシーの設定」（P.12-3）

DCERPC インスペクション ポリシー マップの設定

DCERPC インスペクションの追加のパラメータを指定するには、DCERPC インスペクション ポリシー マップを作成します。作成したインスペクション ポリシー マップは、DCERPC インスペクションをイネーブルにすると適用できます。

はじめる前に

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いずれかを使用する場合は、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] > [DCERPC] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [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。マップのセキュリティ レベルは直接変更するか、[Customize] をクリックすることで編集できます。残りの手順は、マップをカスタマイズするか追加することが前提になります。

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。マップの編集時には、説明のみを変更できます。

ステップ 4　[DCERPC Inspect Map] ダイアログ ボックスの [Security Level] ビューで、目的の設定に最も一致するレベルを選択します。

プリセット レベルの 1 つが要件と一致する場合は、これで完了です。[OK] をクリックし、残りの手順をスキップして、DCERPC インスペクションのサービス ポリシー ルールでマップを使用します。

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。

ステップ 5　必要なオプションを設定します。

- [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。
- [Enforce endpoint-mapper service]：サービスのトラフィックだけが処理されるように、バインディング時にエンドポイント マッパー サービスを実行するかどうかを設定します。
- [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操作をイネーブルにするかどうかを設定します。サービス ルックアップのタイムアウトも適用できます。タイムアウトを設定しない場合は、ピンホール タイムアウトが適用されます。

ステップ 6　[OK] をクリックします。

DCERPC 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。

DCERPC インスペクションのサービス ポリシーの設定

DCERPC インスペクションは、デフォルトのインスペクション ポリシーでイネーブルになっていないため、このインスペクションが必要な場合はイネーブル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、DCERPC インスペクションを追加できます。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] の順に選択し、ルールを開きます。

- デフォルトのグローバル 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、[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。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- DCERPC インスペクション ルール、つまり DCERPC インスペクションを追加しているルールがある場合は、そのルールを選択し、[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）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 マップを使用する場合は、DCERPC インスペクションをディセーブルにしてから、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する必要があります。

a. [DCERPC] チェックボックスをオフにします。

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 4　[DCERPC] を選択します。

ステップ 5　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a. デフォルト マップを使用するか、設定した DCERPC 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。詳細については、「DCERPC インスペクション ポリシー マップの設定」（P.12-2）を参照してください。

b. [Select DCERPC Inspect Map] ダイアログ ボックスで [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。

GTP インスペクション

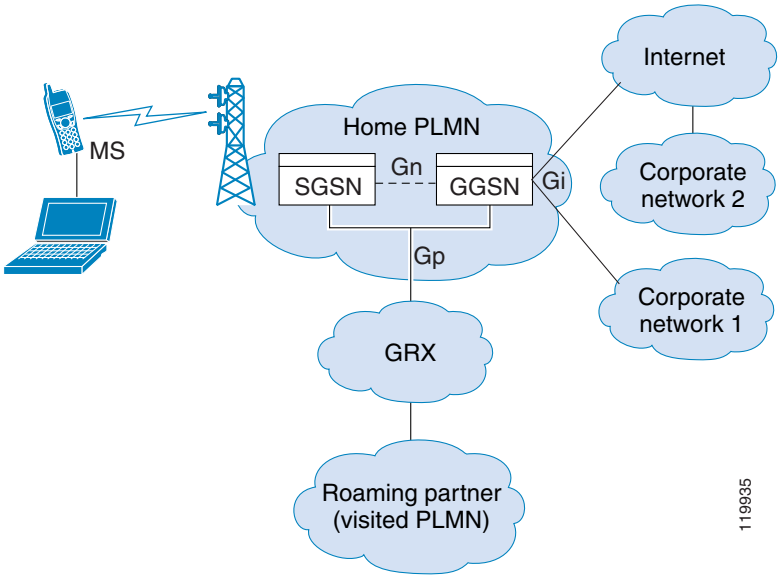
ここでは、GTP インスペクション エンジンについて説明します。

（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。

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 12-1　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。

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。
- GSN タイムアウトは 30 分です。

- PDP コンテキストのタイムアウトは 30 分です。
- 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 応答のタイムアウトは 20 秒です。
- 未知のメッセージ ID はドロップされ、ログに記録されます。

GTP インスペクションの設定

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。GTP インスペクションが必要な場合は設定する必要があります。

手順

ステップ 1　「GTP インスペクション ポリシー マップの設定」（P.12-6）

ステップ 2　「GTP インスペクションのサービス ポリシーの設定」（P.12-8）

ステップ 3　（オプション）過剰請求攻撃から保護するために RADIUS アカウンティング インスペクションを設定します。「RADIUS アカウンティング インスペクション」（P.12-9）を参照してください。

GTP インスペクション ポリシー マップの設定

GTP トラフィックに追加のパラメーターを適用する必要があり、デフォルト マップがニーズを満たさない場合は、GTP マップを作成して設定します。

はじめる前に

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いずれかを使用する場合は、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] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [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。残りの手順は、マップをカスタマイズするか追加することが前提になります。

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。マップの編集時には、説明のみを変更できます。

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。

この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され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、IMSI プレフィックス フィルタリングを設定するためのショートカットです。これについては後で説明します。

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 からの GTP 応答をドロップします。これは、GSN 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 プーリングを設定してロード バランシングをサポートするには、GSN を指定するオブジェクト 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 のネットワーク オブジェクト グループを作成し、これを「**To Object Group**」として選択します。GSN 応答が、GTP 要求を送信した GSN と同じオブジェクト グループに属し、SGSN が、応答する GSN が GTP 応答の送信を許可されているオブジェクト グループに属している場合、ASA は応答を許可します。

  ネットワーク オブジェクト グループは、GSN または SGSN をホスト アドレスまたは GSN や SGSN 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を設定します。

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]：許可されるトンネルの最大数を設定します。
- [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を設定します。タイムアウトは hh: mm: ss 形式です。
  - [GSN]：GSN 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 コンテキストを受け取るまでの非アクティブ時間の最大値です。
  - [Request]：GTP セッション時に GTP メッセージを受け取るまでの非アクティブ時間の最大値です。
  - [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 桁の数字です。1 桁または 2 桁の値にはプレフィックスとして 0 を追加します。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。

許可されるすべての 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] タブをクリックして、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に一致する必要がある）または [No Match]（トラフィックは基準とは異なっている必要がある）を選択します。次に、基準を設定します。

- [Access Point Name]：アクセス ポイント名を、指定された正規表現または正規表現クラスに対して照合します。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]：メッセージ ID（1 ～ 255）を照合します。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を照合します。
- [Version]：GTP バージョン（0 ～ 255）を照合します。1 つの値または値の範囲を指定できます。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。

c. メッセージ ID の照合には、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。他のすべての照合のアクションは、パケットをドロップします。すべての照合に対してロギングをイネーブルにするかどうかを選択できます。

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

ステップ 9　[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、このインスペクション マップを GTP インスペクション サービス ポリシーで使用できるようになります。

GTP インスペクションのサービス ポリシーの設定

GTP インスペクションは、デフォルトのインスペクション ポリシーでイネーブルになっていないため、このインスペクションが必要な場合はイネーブル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、GTP インスペクションを追加できます。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] の順に選択し、ルールを開きます。

- デフォルトのグローバル 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、[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。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- GTP インスペクション ルール、つまり GTP インスペクションを追加しているルールがある場合は、そのルールを選択し、[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）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 マップを使用する場合は、GTP インスペクションをディセーブルにしてから、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する必要があります。

a. [GTP] チェックボックスをオフにします。

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 4　[GTP] を選択します。

ステップ 5　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a. デフォルト マップを使用するか、設定した GTP 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。詳細については、「GTP インスペクション ポリシー マップの設定」（P.12-6）を参照してください。

b. [Select GTP 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

ここでは、RADIUS アカウンティング インスペクション エンジンについて説明します。

- 「RADIUS アカウンティング インスペクションの概要」（P.12-9）
- 「RADIUS アカウンティング インスペクションの設定」（P.12-10）

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 ネットワークで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のに GTP/GPRS 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て GPRS セットアップを設定しない限り、意味がありません。

GPRS ネットワークにおける過剰請求攻撃によって、コンシューマに対して利用していないサービスの請求が行われます。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、送信元 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いずれかの 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。

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する必要があります。

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」（P.12-10）

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」（P.12-11）

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

RADIUS アカウンティング インスペクション ポリシー マップを作成して、インスペクションに必要な属性を設定する必要があります。

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もインスペクション 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。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [RADIUS Accounting] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [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。マップの編集時には、説明のみを変更できます。

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 がメッセージを検証できるように、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を設定します。
- [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 過剰請求保護を実行するかどうかを設定します。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、設定したインターフェイスのユーザ IP アドレスに一致する送信元 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です。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、このインスペクション マップを使用できるようになります。

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

RADIUS アカウンティング インスペクションは、デフォルトのインスペクション ポリシーでイネーブルになっていないため、このインスペクションが必要な場合はイネーブルにする必要があります。RADIUS アカウンティング インスペクションは ASA に送られるトラフィックのためのものですので、標準ルールではなく、管理インスペクション ルールとして設定する必要があります。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、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。「管理トラフィックのサービス ポリシー ルールの追加」（P.1-14）に従って、ウィザードを使って [Rules Actions] ページに進みます。

- RADIUS アカウンティング インスペクション ルール、つまり RADIUS アカウンティング インスペクションを追加した管理ルールがある場合は、そのルールを選択して [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場合）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 マップを使用する場合は、RADIUS アカウンティング インスペクションをディセーブルにしてから、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する必要があります。

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」（P.12-10）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、管理サービス ポリシー ルールを保存します。

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。

RSH インスペクションのイネーブル化の詳細については、「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設定」（P.8-10）を参照してください。

SNMP インスペクション

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。

SNMP インスペクションは、デフォルトのインスペクション ポリシーでイネーブルになっていないため、このインスペクションが必要な場合はイネーブル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、SNMP インスペクションを追加できます。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] > [Objects] > [Inspect Maps] > [SNMP] の順に選択し、次を実行します。

a. [Add] をクリックするか、マップを選択して [Edit] をクリックします。マップを追加する場合はマップ名を入力します。

b. 拒否する SNMP のバージョンを選択します。

c. [OK] をクリックします。

ステップ 2　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル 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、[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。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- SNMP インスペクション ルール、つまり SNMP インスペクションを追加しているルールがある場合は、そのルールを選択し、[Edit] をクリックします。

ステップ 3　[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 4　（使用中のポリシーを変更する場合）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 マップを使用する場合は、SNMP インスペクションをディセーブルにしてから、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する必要があります。

a. [SNMP] チェックボックスをオフにします。

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 5　[SNMP] を選択します。

ステップ 6　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a. デフォルト マップ（すべてのバージョンを許可します）を使用するか、または設定した SNMP 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. [SNMP Inspect Map] ダイアログ ボックスで [OK] をクリックします。

ステップ 7　[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。

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。

XDMCP インスペクションのイネーブル化の詳細については、「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設定」（P.8-10）を参照してください。