データベース、ディレクトリ、および管理プロトコルのインスペクション

ここでは、データベース、ディレクトリ、および管理の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。

DCERPC インスペクション

デフォルトのインスペクション ポリシーでは、DCERPC インスペクションがイネーブルにされていないため、この検査が必要な場合はイネーブルにします。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。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。

次の項では、DCERPC インスペクション エンジンについて説明します。

DCERPC の概要

DCERPC に基づく Microsoft リモート プロシージャ コール（MSRPC）は、Microsoft 分散クライアントおよびサーバアプリケーションで広く使用されているプロトコルであり、ソフトウェア クライアントがサーバ上のプログラムをリモートで実行できるようにします。

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 エンジンは、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、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。

DCE インスペクションは、次の汎用一意識別子（UUID）とメッセージをサポートします。

- エンドポイントマッパー（EPM）UUID。すべての EPM メッセージがサポートされます。
- ISystemMapper UUID（非 EPM）。サポートされるメッセージ タイプは次のとおりです。
  - RemoteCreateInstance opnum4
  - RemoteGetClassObject opnum3
- IP アドレスまたはポート情報を含まない任意のメッセージ（これらのメッセージでは検査の必要がないため）。

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。

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。

手順

ステップ 1　**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[DCERPC]** 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。セキュリティ レベルを直接変更することも、[Customize] をクリックしてマップを編集することもできます。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 [DCERPC Inspect Map] ダイアログボックスの [Security Level] のビューで、希望する設定に一致するレベルを選択します。

プリセット レベルのいずれかが要件と一致する場合、以上で終了です。[OK] をクリックし、残りの手順をとばし、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、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。

これで、DCERPC 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。「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」を参照してください。

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が、すべてのデバイスモデルでサポートされているわけではありません。詳細については、一般的なコンフィギュレーションガイドのライセンスの章を参照してください。

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。GGSNは、GPRSワイヤレスデータネットワークと他のネットワーク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。

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エンドポイントと訪問したSGSN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。

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。

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。
- 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。

  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。

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してください。

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 （5 ページ）。

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 （8 ページ）。

ステップ 3 （任意）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 （9 ページ）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 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、ロード バランシングをサポートするために、GSN 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 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。応答している GSN が GTP 要求の送信先の GSN と同じオブジェクト グループに属している場合、および応答している GSN 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 がある場合、ASA はその応答を許可します。

  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。
  - [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 コンテキストを削除するまでの非アクティブ時間の最大値です。
  - [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。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。

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 [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。

GTP 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、GTP インスペクションがイネーブルにされていないため、この検査が必要な場合はイネーブルにします。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。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。
- GTP インスペクション ルールがある場合、または GTP インスペクションを追加するルールがある場合、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、GTP 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) [GTP] チェックボックスをオンにします。
b) [OK] をクリックします。
c) [適用（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] をクリックして以下のようにします。

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 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 （5 ページ）を参照してください。

b) [GTP 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。

ILS インスペクション

Internet Locator Service（ILS）インスペクション エンジンは、LDAP を使用してディレクトリ情報を ILS サーバと交換する Microsoft NetMeeting、SiteServer、および Active Directory の各製品に対して NAT をサポートします。LDAP データベースには IP アドレスだけが保存されるため、ILS インスペクションで PAT は使用できません。

LDAP サーバが外部にある場合、内部ピアが外部 LDAP サーバに登録された状態でローカルに通信できるように、検索応答に対して NAT を使用することを検討してください。NAT を使用する必要がなければ、パフォーマンスを向上させるためにインスペクションエンジンをオフにすることを推奨します。

ILS サーバが ASA 境界の内部にある場合は、さらに設定が必要なことがあります。この場合、外部クライアントが指定されたポート（通常は TCP 389）の LDAP サーバにアクセスするためのホールが必要となります。

（注） ILS トラフィック（H225 コール シグナリング）はセカンダリ UDP チャネルだけで発生するため、TCP 接続は TCP 非アクティブ間隔の後に切断されます。デフォルトでは、この間隔は 60 分です。この値は、TCP timeout コマンドを使用して調整できます。ASDM では、これは [Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ペインにあります。

ILS インスペクションには、次の制限事項があります。

- 照会要求や応答はサポートされません。
- 複数のディレクトリのユーザは統合されません。
- 複数のディレクトリに複数の ID を持っている単一のユーザは NAT には認識されません。

ILSインスペクションをイネーブルにする方法については、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設定を参照してください。

RADIUS アカウンティング インスペクション

次の項では、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

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、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。

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 （11 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 （12 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) [適用（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 （11 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。

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。

デフォルトのインスペクション ポリシーでは、SNMP インスペクションがイネーブルにされていないため、この検査が必要な場合はイネーブルにします。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。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]** > **[Objects]** > **[Inspect Maps]** > **[SNMP]** を選択します。

ステップ 2 [Add] をクリックするか、マップを選択し、[Edit] をクリックします。マップの追加時にマップ名を入力します。

ステップ 3 拒否する SNMP のバージョンを選択します。

ステップ 4 [OK] をクリックします。

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。「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」を参照してください。

SQL*Net インスペクション

SQL*Net 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。インスペクション エンジンは、SQL*Net バージョン 1 および 2 をサポートしていますが、形式は Transparent Network Substrate（TNS）のみです。インスペクションでは、表形式データ ストリーム（TDS）形式をサポートしていません。SQL*Net メッセージは、埋め込まれたアドレスとポートについてスキャンされ、必要に応じて NAT の書き換えが適用されます。

SQL*Net のデフォルトのポート割り当ては 1521 です。これは、Oracle が SQL*Net 用に使用している値ですが、構造化照会言語（SQL）の IANA ポート割り当てとは一致しません。アプリケーションが別のポートを使用する場合は、そのポートを含むトラフィック クラスに SQL*Net インスペクションを適用します。

（注） SQL 制御 TCP ポート 1521 と同じポートで SQL データ転送が行われる場合は、SQL*Net のインスペクションをディセーブルにします。SQL*Net インスペクションがイネーブルになっていると、セキュリティ アプライアンスはプロキシとして機能し、クライアントのウィンドウ サイズを 65000 から約 16000 に減らすため、データ転送の問題が発生します。

SQL*Net インスペクションをイネーブルにする方法については、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設定を参照してください。

Sun RPC インスペクション

この項では、Sun RPC 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。

Sun RPC インスペクションの概要

Sun RPC プロトコル インスペクションはデフォルトではイネーブルです。Sun RPC サーバ テーブルを管理するだけで、ファイアウォールの通過を許可されているサービスを識別できます。ただし、NFS のピンホール化は、サーバ テーブルの設定がなくても各サーバで実行されます。

Sun RPC は、NFS および NIS で使用されます。Sun RPC サービスはどのポート上でも実行できます。サーバ上の Sun RPC サービスにアクセスしようとするクライアントは、そのサービスが実行されているポートを知る必要があります。そのためには、予約済みポート 111 でポート マッパー プロセス（通常は rpcbind）に照会します。

クライアントがサービスの Sun RPC プログラム番号を送信すると、ポート マッパー プロセスはサービスのポート番号を応答します。クライアントは、ポート マッパー プロセスによって特定されたポートを指定して、Sun RPC クエリーをサーバに送信します。サーバが応答すると、ASA はこのパケットを代行受信し、そのポートで TCP と UDP の両方の初期接続を開きます。

Sun RPC ペイロード情報の NAT または PAT はサポートされていません。

Sun RPC サービスの管理

Sun RPC サービス テーブルを使用して、確立された Sun RPC セッションに基づいて Sun RPC トラフィックを制御します。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Advanced]** > **[SUNRPC Server]** 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サーバを追加します。
- サーバを選択して [Edit] をクリックします。

ステップ 3 サービス プロパティを設定します。

- [Interface Name] ：サーバへのトラフィックが伝送されるインターフェイス。
- [IP Address/Mask] ：Sun RPC サーバのアドレス。
- [Service ID] ：サーバのサービス タイプ。サービス タイプ（100003 など）を判定するには、Sun RPC サーバ マシンの UNIX または Linux コマンドラインで、sunrpcinfo コマンドを使用します。
- [Protocol]：サービスがプロトコルとして使用する TCP または UDP。
- [Port/Port Range] ：サービスによって使用されているポートまたはポートの範囲。
- [Timeout]：Sun RPC インスペクションによって接続のために開かれたピンホールのアイドル タイムアウト。

ステップ 4 [OK] をクリックします。

ステップ 5 （任意）これらのサービス用に作成されたピンホールをモニタします。

Sun RPC サービスで開かれているピンホールを表示するには、**show sunrpc-server active** 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。次に例を示します。

```
hostname# show sunrpc-server active
LOCAL FOREIGN SERVICE TIMEOUT
----------------------------------------------
1 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
2 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
3 209.165.200.5/0 192.168.100.2/647 100005 0:30:00
4 209.165.200.5/0 192.168.100.2/650 100005 0:30:00
```

LOCAL カラムのエントリは、内部インターフェイスのクライアントまたはサーバの IP アドレスを示します。FOREIGN カラムの値は、外部インターフェイスのクライアントまたはサーバの IP アドレスを示します。

必要に応じ、次のコマンドを使用してこれらのサービスをクリアすることができます。 **clear sunrpc-server active**

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。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、TCP ポートを許可するアクセス ルールを使用できます。または、ASA で **established** コマンドを使用できます。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 を参照してください。

VXLAN インスペクション

Virtual Extensible Local Area Network （VXLAN）インスペクションは、ASA を通過する VXLAN のカプセル化されたトラフィックで機能します。VXLAN ヘッダーフォーマットが標準に準拠し、不正な形式のパケットをドロップすることを確認します。VXLAN インスペクションは、ASA が VXLAN トンネル エンドポイント（VTEP）または VXLAN ゲートウェイとして機能するトラフィックでは行われません。これは、それらのチェックが VXLAN パケットの通常の非カプセル化の一部として行われるためです。

VXLAN パケットは通常、ポート 4789 の UDP です。このポートは、default-inspection-traffic クラスの一部であるため、inspection_default サービス ポリシー ルールに VXLAN インスペクションを追加するだけです。または、それに対してポートまたは ACL マッチングを使用してクラスを作成することもできます。

データベース、ディレクトリ、および管理プロトコルのインスペクションの履歴

機能名	リリース	機能情報
DCERPC インスペクションで ISystemMapper UUID メッセージ RemoteGetClassObject opnum3 をサポート。	9.4(1)	ASA は、リリース 8.3 で EPM 以外の DCERPC メッセージのサポートを開始し、ISystemMapper UUID メッセージ RemoteCreateInstance opnum4 をサポートしています。この変更により、RemoteGetClassObject opnum3 メッセージまでサポートが拡張されます。 変更された ASDM 画面はありません。
VXLAN パケット インスペクション	9.4(1)	ASA は、標準形式に準拠するために VXLAN ヘッダーを検査できます。 次の画面が変更されました。[Configuration] > [Firewall] > [Service Policy Rules] > [Add Service Policy Rule] > [Rule Actions] > [Protocol Inspection]。