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。

手順

ステップ 1 DCERPC インスペクション ポリシー マップを作成します。**policy-map type inspect dcerpc** *policy_map_name*

policy_map_name には、ポリシーマップの名前を指定します。CLI はポリシーマップ コンフィギュレーション モードに入ります。

ステップ 2 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 3 インスペクションエンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a) パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **timeout pinhole** *hh:mm:ss*：DCERPC ピンホールのタイムアウトを設定し、2 分のグローバル システム ピンホール タイムアウトを上書きします。タイムアウトは 00:00 01 ～ 119:00:00 まで指定できます。
- **endpoint-mapper** [**epm-service-only**] [**lookup-operation** [**timeout** *hh:mm:ss*]]：エンドポイント マッパー トラフィックのオプションを設定します。**epm-service-only** キーワードを指定すると、バインド中にエンドポイント マッパー サービスを実行し、このサービスのトラフィックだけが処理されるようにします。**lookup-operation** キーワードを指定すると、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します。ルックアップ操作で生成されたピンホールのタイムアウトを設定できます。ルックアップ操作にタイムアウトが設定されていない場合は、timeout pinhole コマンドで指定した値かデフォルトの値が使用されます。

例

次の例は、DCERPC インスペクション ポリシー マップを定義し、DCERPC のピンホールのタイムアウトを設定する方法を示しています。

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# timeout pinhole 0:10:00

hostname(config)# class-map dcerpc
hostname(config-cmap)# match port tcp eq 135

hostname(config)# policy-map global-policy
hostname(config-pmap)# class dcerpc
hostname(config-pmap-c)# inspect dcerpc dcerpc-map

hostname(config)# service-policy global-policy global
```

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 （9 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 （12 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 GTP インスペクション ポリシー マップを作成します。**policy-map type inspect gtp** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 3 一致したトラフィックにアクションを適用するには、次の手順を実行します。

a) 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **apn regex** {*regex_name* | **class** *class_name*}：指定した正規表現または正規表現クラスに対する Access Point Name (APN) に一致します。
- **match** [**not**] **message id** {*message_id* | **range** *message_id_1 message_id_2*}：1 ～ 255 のいずれかのメッセージ ID に一致します。1 つの ID または ID の範囲を指定できます。
- **match** [**not**] **message length min** *bytes* **max** *bytes*：UDP ペイロード（GTP ヘッダーと残りのメッセージ）の長さが最小値と最大値の間（1 ～ 65536）であるメッセージを照合します。
- **match** [**not**] **version** {*version_id* | **range** *version_id_1 version_id_2*}：0 ～ 255 のいずれかの GTP バージョンに一致します。1 つのバージョンまたはバージョンの範囲を指定できます。

b) 次のコマンドのいずれかを入力して、一致するトラフィックに対して実行するアクションを指定します。

- **drop** [**log**]：一致するすべてのパケットをドロップします。システム ログ メッセージも送信するには、**log** キーワードを追加します。
- **rate-limit** *message_rate*：メッセージのレートを制限します。このオプションでは、**message id** のみ使用できます。

ポリシー マップでは、複数の **match** コマンドを指定できます。**match** コマンドの順序については、複数のトラフィック クラスの処理方法を参照してください。

ステップ 4 インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a) パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **permit errors**：無効な GTP パケットや別の方法で解析されるとドロップされるパケットを許可します。
- **request-queue** *max_requests*：キューで応答待ちができる GTP 要求数の最大値を設定します。デフォルトは 200 です。この上限に達した後に新しい要求が到着すると、最も

長い時間キューに入っていた要求が削除されます。「Error Indication」、「Version Not Supported」および「SGSN Context Acknowledge」というメッセージは、要求と見なされないため、応答待ち要求のキューに入れられません。

- **tunnel-limit** *max_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。このコマンドで指定したトンネル数に達すると、新しい要求はドロップされます。
- **timeout** {**gsn** | **pdp-context** | **request** | **signaling** | **t3-response** | **tunnel**} *time*：指定したサービスのアイドル タイムアウトを設定します（hh: mm: ss 形式）。タイムアウトを設定しない場合は、番号に 0 を指定します。このコマンドは、タイムアウトごとに別々に入力します。
  - **gsn**：GSN が削除されるまでの非アクティブ時間の最大値。
  - **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。
  - **request**：要求キューから要求が削除されるまでの非アクティブ時間の最大値。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。
  - **t3-response**：接続を除去する前に応答を待機する最大時間。
  - **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。

ステップ 5 必要に応じて、パラメータ コンフィギュレーション モードに入っている間に、IMSI プレフィックス フィルタリングを設定します。

mcc *country_code* **mnc** *network_code*

デフォルトでは、GTP インスペクションは、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 6 必要に応じて、パラメータ コンフィギュレーション モードに入っている間に、GSN プーリングを設定します。

permit-response to-object-group *SGSN_name* **from-object-group** *GSN_pool*

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** パラメータで指定します。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** パラメータとして選択します。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。

例：

次の例では、GSN プールと SGSN のネットワーク オブジェクトを定義して GSN プーリングをサポートする方法を示します。クラス C ネットワーク全体が GSN プールとして定義されていますが、ネットワーク全体を指定する代わりに、複数の個別の IP アドレスを **network-object** コマンドで 1 つずつ指定できます。この例では、次に、GSN プールから SGSN への応答を許可するように、GTP インスペクション マップを変更します。

```
hostname(config)# object-group network gsnpool32
hostname(config-network)# network-object 192.168.100.0 255.255.255.0
hostname(config)# object-group network sgsn32
hostname(config-network)# network-object host 192.168.50.100

hostname(config)# policy-map type inspect gtp gtp-policy
hostname(config-pmap)# parameters
hostname(config-pmap-p)# permit-response to-object-group sgsn32
from-object-group gsnpool32
```

例

次の例は、ネットワークのトンネル数を制限する方法を示しています。

```
hostname(config)# policy-map type inspect gtp gmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# tunnel-limit 3000

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect gtp gmap

hostname(config)# service-policy global_policy global
```

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 必要な場合は、L3/L4 クラス マップを作成して、インスペクションを適用するトラフィックを識別します。

```
class-map name
match parameter
```

例：

```
hostname(config)# class-map gtp_class_map
hostname(config-cmap)# match access-list gtp
```

デフォルト グローバル ポリシーの inspection_default クラス マップは、すべてのインスペクション タイプのデフォルト ポートを含む特別なクラス マップです（**match default-inspection-traffic**）。このマップをデフォルト ポリシーまたは新しいサービス ポリシーで使用する場合は、このステップを省略できます。

照合ステートメントについては、通過トラフィック用のレイヤ 3/4 クラス マップの作成 を参照してください。

ステップ 2 クラス マップ トラフィックで実行するアクションを設定するポリシー マップを追加または編集します。**policy-map** *name*

例：

```
hostname(config)# policy-map global_policy
```

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3 GTP インスペクションに使用する L3/L4 クラス マップを特定します。**class** *name*

例：

```
hostname(config-pmap)# class inspection_default
```

デフォルト ポリシーを編集する場合、または新しいポリシーで特別な inspection_default クラス マップを使用する場合は、*name* として **inspection_default** を指定します。それ以外の場合は、この手順ですでに作成したクラスを指定します。

ステップ 4 GTP インスペクションを設定します。**inspect gtp** [*gtp_policy_map*]

gtp_policy_map は任意の GTP インスペクション ポリシー マップです。デフォルト以外のインスペクション処理が必要な場合にのみマップが必要です。インスペクション ポリシー マップの作成の詳細については、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。

例：

```
hostname(config-class)# no inspect gtp
hostname(config-class)# inspect gtp gtp-map
```

（注） 別のインスペクション ポリシー マップを使用するためにデフォルト グローバル ポリシー（または使用中のポリシー）を編集する場合は、 **no inspect gtp** コマンドで GTP インスペクションを削除してから、新しいインスペクション ポリシー マップの名前で再追加します。

ステップ 5 既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

```
hostname(config)# service-policy global_policy global
```

global キーワードはポリシー マップをすべてのインターフェイスに適用し、**interface** はポリシーを 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシーマップを 1 つだけ適用できます。

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。

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。

```
hostname# 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                   0     total_dropped             0
  signalling_msg_dropped            0     data_msg_dropped          0
  signalling_msg_forwarded          0     data_msg_forwarded        0
  total created_pdp                 0     total deleted_pdp         0
  total created_pdpmcb              0     total deleted_pdpmcb      0
  pdp_non_existent                  0
```

次に、**show service-policy inspect gtp statistics gsn** コマンドの GSN 出力例を示します。

```
hostname# show service-policy inspect gtp statistics gsn 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。次に例を示します。

```
hostname# show service-policy inspect gtp pdp-context detail
1 in use, 1 most used, timeout 0:00:00

Version TID                 MS Addr        SGSN Addr    Idle      APN
v1      1234567890123425         10.0.1.1        10.0.0.2 0:00:13  gprs.cisco.com

    user_name (IMSI): 214365870921435    MS address:         10.0.1.1
    primary pdp: Y                       nsapi: 2
    sgsn_addr_signal:        10.0.0.2    sgsn_addr_data:          10.0.0.2
    ggsn_addr_signal:        10.1.1.1    ggsn_addr_data:          10.1.1.1
    sgsn control teid:     0x000001d1    sgsn data teid:        0x000001d3
    ggsn control teid:     0x6306ffa0    ggsn data teid:        0x6305f9fc
    seq_tpdu_up:                  0    seq_tpdu_down:                 0
    signal_sequence:              0
    upstream_signal_flow:         0     upstream_data_flow:          0
    downstream_signal_flow:       0     downstream_data_flow:        0
    RAupdate_flow:                0
```

PDP コンテキストは、IMSI と NSAPI の値の組み合わせであるトンネル ID によって識別されます。GTP トンネルは、それぞれ別個の GSN ノードにある、2 つの関連する PDP 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、パケットを外部パケット データ ネットワークと MS ユーザの間で転送するために必要です。

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 （13 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 （15 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 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。**policy-map type inspect radius-accounting** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 3 パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

ステップ 4 1つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **send response**：Accounting-Request の Start および Stop メッセージを、それらのメッセージの送信元（**host** コマンド内で識別されています）へ送信するよう ASA に指示します。
- **enable gprs**：GPRS 過剰請求の保護を実装します。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** *number*：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。
- **host** *ip_address* [**key** *secret*]：RADIUS サーバまたは GGSN の IP アドレスです。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。複数の RADIUS と GGSN のホストを識別するため、このコマンドは繰り返し実行できます。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。
- **timeout users** *time*：ユーザのアイドル タイムアウトを設定します（hh: mm: ss 形式）。タイムアウトを付けない場合は、00:00:00 を指定してください。デフォルトは 1 時間です。

例

```
policy-map type inspect radius-accounting radius-acct-pmap
  parameters
    send response
    enable gprs
    validate-attribute 31
    host 10.2.2.2 key 123456789
    host 10.1.1.1 key 12345
class-map type management radius-class
  match port udp eq radius-acct
policy-map global_policy
  class radius-class
    inspect radius-accounting radius-acct-pmap
```

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 検査を適用するトラフィックを識別するため L3/L4 マネジメント クラス マップを作成し、一致するトラフィックを識別します。

class-map type management *name*
match {port | access-list} *parameter*

例：

```
hostname(config)# class-map type management radius-class-map
hostname(config-cmap)# match port udp eq radius-acct
```

この例では、一致は radius acct UDP ポート（1646）です。ポートの範囲（**match port udp range** *number1 number2*）または **match access-list** *acl_name* と ACL を使って異なるポートを指定できます。

ステップ 2 クラス マップ トラフィックで実行するアクションを設定するポリシー マップを追加または編集します。**policy-map** *name*

例：

```
hostname(config)# policy-map global_policy
```

デフォルト設定では、global_policy ポリシーマップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3 RADIUS アカウンティング インスペクションに使用する L3/L4 管理クラス マップを特定します。**class** *name*

例：

```
hostname(config-pmap)# class radius-class-map
```

ステップ 4 RADIUS アカウンティング インスペクションを設定します。**inspect radius-accounting**[*radius-accounting_policy_map*]

radius_accounting_policy_map 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 （13 ページ）で作成した RADIUS アカウンティング インスペクション ポリシー マップです。

例：

```
hostname(config-class)# no inspect radius-accounting
hostname(config-class)# inspect radius-accounting radius-class-map
```

（注） 別のインスペクション 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、**no inspect radius-accounting** コマンドで RADIUS アカウンティング インスペクションを削除してから、新しいインスペクション ポリシー マップの名前で再追加します。

ステップ 5 既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

```
hostname(config)# service-policy global_policy global
```

global キーワードはポリシー マップをすべてのインターフェイスに適用し、**interface** はポリシーを 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシーマップを 1 つだけ適用できます。

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

SNMP マップを作成します。

snmp-map *map_name* コマンドを使ってマップを作成して SNMP マップ 設定モードに入り、次に **deny version** *version* コマンドで拒否するバージョンを識別します。バージョンは 1、 2、 2c、 3 があります。

例：

次の例では、SNMP バージョン 1 および 2 を拒否しています。

```
hostname(config)# snmp-map sample_map
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# deny version 2
```

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 Sun RPC サービス プロパティを設定します。

sunrpc-server *interface_name ip_address mask* **service** *service_type* **protocol** {**tcp** | **udp**} *port*[*-port*] **timeout** *hh:mm:ss*

それぞれの説明は次のとおりです。

- *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** *service_type*：特定のサービス タイプとそのサービスに使用するポート番号の間のマッピングである、サーバ上のサービス 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** {**tcp** | **udp**}：サービスが TCP と UDP のどちらを使用するかを示します。
- *port*[*-port*]：サービスによって使用されるポートまたはポートの範囲。ポート範囲を指定するには、範囲の開始ポート番号と終了ポート番号をハイフンで区切ります（111-113 など）。
- **timeout** *hh:mm:ss*：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。

例：

たとえば、IP アドレスが 192.168.100.2 の Sun RPC サーバに対して 30 分のタイムアウトを作成するには、次のコマンドを入力します。この例では、Sun RPC サーバは TCP ポート 111 を使用する内部インターフェイスにあります。

```
hostname(config)# sunrpc-server inside 192.168.100.2 255.255.255.255
service 100003 protocol tcp 111 timeout 00:30:00
```

ステップ 2 （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。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。 変更されたコマンドはありません。
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。 **inspect vxlan** コマンドが導入されました。

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