CHAPTER 15

アプリケーション インスペクションの特別なアクションの設定（インスペクション ポリシー マップ）

モジュラ ポリシー フレームワークでは、多くのアプリケーション インスペクションで実行される特別なアクションを設定できます。レイヤ 3/4 ポリシー マップでインスペクション エンジンをイネーブルにする場合は、*インスペクション ポリシー マップ*で定義されるアクションを必要に応じてイネーブルにすることもできます。インスペクション ポリシー マップが、インスペクション アクションを定義したレイヤ 3/4 クラス マップ内のトラフィックと一致すると、トラフィックのそのサブセットが指定したとおりに動作します（たとえば、ドロップやレート制限など）。

この章は、次の項で構成されています。

インスペクション ポリシー マップに関する情報

インスペクション ポリシー マップをサポートするアプリケーションのリストについては、「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.19-6）を参照してください。

インスペクション ポリシー マップは、次に示す要素の 1 つ以上で構成されています。インスペクション ポリシー マップで使用可能な実際のオプションは、アプリケーションに応じて決まります。

- トラフィック照合コマンド：インスペクション ポリシー マップで直接トラフィック照合コマンドを定義して、アプリケーションのトラフィックを、URL 文字列などのアプリケーションに固有の基準と照合できます。一致した場合にはアクションをイネーブルにします。
  - 一部のトラフィック照合コマンドでは、正規表現を指定してパケット内部のテキストを照合できます。ポリシー マップを設定する前に、正規表現クラス マップ内で、正規表現を単独またはグループで作成およびテストしておいてください。
- インスペクション クラス マップ：（すべてのアプリケーションで使用できるわけではありません。サポートされるアプリケーションのリストについては、CLI ヘルプを参照してください）。インスペクション クラス マップには、アプリケーション トラフィックを URL 文字列などのアプリケーション固有の基準と照合するトラフィック照合コマンドが含まれています。その後、ポリシー

マップ内のクラス マップを特定し、アクションをイネーブルにします。クラス マップを作成することと、インスペクション ポリシー マップ内で直接トラフィック照合を定義することの違いは、より複雑な一致基準を作成できる点と、クラス マップを再使用できる点です。

  - 一部のトラフィック照合コマンドでは、正規表現を指定してパケット内部のテキストを照合できます。ポリシー マップを設定する前に、正規表現クラス マップ内で、正規表現を単独またはグループで作成およびテストしておいてください。

- パラメータ：パラメータは、インスペクション エンジンの動作に影響します。

ガイドラインと制限事項

すべてのインスペクション ポリシー マップ：使用中のインスペクション ポリシー マップを別のマップ名と交換する場合は、**inspect** *protocol map* コマンドを削除して新しいマップを使用して再度追加します。例：

```
hostname(config)# policy-map test
hostname(config-pmap)# class sip
hostname(config-pmap-c)# no inspect sip sip-map1
hostname(config-pmap-c)# inspect sip sip-map2
```

デフォルトのインスペクション ポリシー マップ

デフォルトのインスペクション ポリシー マップ コンフィギュレーションには、次のコマンドが組み込まれています。このコンフィギュレーションでは、DNS パケットの最大メッセージ長を 512 バイトに設定しています。

```
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
```

（注）　**policy-map type inspect esmtp _default_esmtp_map** など、他のデフォルトのインスペクション ポリシー マップもあります。これらのデフォルト ポリシー マップは、**inspect** *protocol* コマンドで暗黙的に作成されます。たとえば、**inspect esmtp** はポリシー マップ「_default_esmtp_map」を暗黙的に使用します。すべてのデフォルト ポリシー マップは、**show running-config all policy-map** コマンドを使用して表示できます。

インスペクション ポリシー マップのアクションの定義

レイヤ 3/4 ポリシー マップでインスペクション エンジンをイネーブルにする場合は、インスペクション ポリシー マップで定義されるアクションを必要に応じてイネーブルにすることもできます。

制限事項

ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。

1 つのパケットが複数の異なる **match** コマンドまたは **class** コマンドと一致する場合、ASA 1000V がアクションを適用する順序は、ポリシー マップにアクションが追加された順序ではなく、ASA 1000V の内部ルールによって決まります。内部ルールは、アプリケーションのタイプとパケット解析の論理的進捗によって決まり、ユーザが設定することはできません。

アクションがパケットをドロップすると、インスペクション ポリシー マップではそれ以降のアクションは実行されません。たとえば、最初のアクションが接続のリセットである場合、それ以降の **match** コマンドまたは **class** コマンドとの照合は行われません。最初のアクションがパケットのログへの記録である場合、接続のリセットなどの 2 番目のアクションは実行されます（同じ **match** または **class** コマンドで、**reset**（または **drop-connection** など）と **log** の両方のアクションを設定できます。この場合パケットは、指定された照合でリセットされる前にログに記録されます）。

パケットが、同じ複数の **match** コマンドまたは **class** コマンドと照合される場合は、ポリシー マップ内のそれらのコマンドの順序に従って照合されます。たとえば、ヘッダーの長さが 1001 のパケットの場合は、次に示す最初のコマンドと照合されてログに記録され、それから 2 番目のコマンドと照合されてリセットされます。2 つの **match** コマンドの順序を逆にすると、2 番目の **match** コマンドとの照合前にパケットのドロップと接続のリセットが行われ、ログには記録されません。

```
match request header length gt 100
  log
match request header length gt 1000
  reset
```

クラス マップは、そのクラス マップ内で重要度が最低の **match** コマンド（重要度は、内部ルールに基づきます）に基づいて、別のクラス マップまたは **match** コマンドと同じタイプであると判断されます。クラス マップに、別のクラス マップと同じタイプの重要度が最低の **match** コマンドがある場合、それらのクラス マップはポリシー マップに追加された順序で照合されます。クラス マップごとに最低重要度のコマンドが異なる場合は、最高重要度の **match** コマンドを持つクラス マップが最初に照合されます。たとえば、次の 3 つのクラス マップには、**match request-cmd**（高プライオリティ）と **match filename**（低プライオリティ）という 2 つのタイプの **match** コマンドがあります。ftp3 クラス マップには両方のコマンドが含まれていますが、最低重要度のコマンドである **match filename** に従ってランク付けされています。ftp1 クラス マップには最高重要度のコマンドがあるため、ポリシー マップ内での順序に関係なく最初に照合されます。ftp3 クラス マップは ftp2 クラス マップと同じ重要度としてランク付けされており、**match filename** コマンドも含まれています。これらのクラス マップの場合、ポリシー マップ内での順序に従い、ftp3 が照合されてから ftp2 が照合されます。

```
class-map type inspect ftp match-all ftp1
  match request-cmd get
class-map type inspect ftp match-all ftp2
  match filename regex abc
class-map type inspect ftp match-all ftp3
  match request-cmd get
  match filename regex abc

policy-map type inspect ftp ftp
  class ftp3
    log
  class ftp2
    log
  class ftp1
    log
```

手順の詳細

	コマンド	目的
ステップ 1	（任意） インスペクション クラス マップを作成します。	「インスペクション クラス マップ内のトラフィックの特定」（P.15-5）を参照してください。または、ポリシー マップ内でトラフィックを直接特定できます。
ステップ 2	**policy-map type inspect** *application policy_map_name* **例：** `hostname(config)# policy-map type inspect ftp ftp_policy`	インスペクション ポリシー マップを作成します。インスペクション ポリシー マップをサポートするアプリケーションのリストについては、「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.19-6）を参照してください。 *policy_map_name* 引数は、最大 40 文字のポリシー マップ名です。すべてのタイプのポリシー マップで同じ名前スペースが使用されるため、別のタイプのポリシー マップですでに使用されている名前は再度使用できません。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 3	次のいずれかの方法を使用して、アクションを実行するトラフィックを指定します。	

	class *class_map_name*
	
	例：
	`hostname(config-pmap)# class _traffic`
	`hostname(config-pmap-c)#`
		「インスペクション クラス マップ内のトラフィックの特定」（P.15-5）で作成したインスペクション クラス マップを指定します。
		
		すべてのアプリケーションがインスペクション クラス マップをサポートするわけではありません。

	インスペクションの章でアプリケーションごとに説明されている **match** コマンドの 1 つを使用して、ポリシー マップで直接トラフィックを指定します。
	
	例：
	`hostname(config-pmap)# match req-resp content-type mismatch`
	`hostname(config-pmap-c)#`
		match not コマンドを使用すると、**match not** コマンドの基準に一致するすべてのトラフィックにアクションは適用されません。

	コマンド	目的
ステップ 4	{[**drop** [**send-protocol-error**] | **drop-connection** [**send-protocol-error**]| **mask** | **reset**] [**log**] | **rate-limit** *message_rate*} **例：** `hostname(config-pmap-c)# drop-connection log`	一致した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。それぞれのアプリケーションですべてのオプションを設定できるわけではありません。アプリケーションに固有の他のアクションも適用可能な場合があります。使用可能な実際のオプションについては、該当するインスペクションの章を参照してください。 • **drop**：一致するすべてのパケットをドロップします。 • **send-protocol-error**：プロトコル エラー メッセージを送信します。 • **drop-connection**：パケットをドロップし、接続を閉じます。 • **mask**：パケットの一致する部分をマスクします。 • **reset**：パケットをドロップし、接続を閉じ、サーバとクライアントの両方またはいずれかに TCP リセットを送信します。 • **log**：システム ログ メッセージを送信します。**log** は単独で、または他のキーワードの 1 つと一緒に使用できます。 • **rate-limit** *message_rate*：メッセージのレートを制限します。

ステップ 5	**parameters**
	
	例：
	`hostname(config-pmap)# parameters`
	`hostname(config-pmap-p)#`
		インスペクション エンジンに影響するパラメータを設定します。CLI はパラメータ コンフィギュレーション モードに移行します。各アプリケーションで設定可能なパラメータについては、該当するインスペクションの章を参照してください。

インスペクション クラス マップ内のトラフィックの特定

このタイプのクラス マップを使用して、アプリケーション固有の基準と照合できます。たとえば DNS トラフィックの場合は、DNS クエリー内のドメイン名と照合可能です。

クラス マップは、複数のトラフィック照合をグループ化します（match-all クラス マップ）。あるいはクラス マップで、照合リストのいずれかを照合できます（match-any クラス マップ）。クラス マップを作成することと、インスペクション ポリシー マップ内で直接トラフィック照合を定義することの違いは、クラス マップを使用して複数の match コマンドをグループ化できる点と、クラス マップを再使用できる点です。このクラス マップで指定するトラフィックに対しては、インスペクション ポリシー マップで、接続のドロップ、リセット、またはロギングなどのアクションを指定できます。タイプの異なるトラフィックで異なるアクションを実行する場合は、ポリシー マップで直接トラフィックを指定してください。

制限事項

すべてのアプリケーションがインスペクション クラス マップをサポートするわけではありません。サポートされるアプリケーションのリストについては、**class-map type inspect** の CLI ヘルプを参照してください。

手順の詳細

	コマンド	目的
ステップ 1	（任意） 正規表現を作成します。	「正規表現の作成」（P.8-11）および「正規表現クラス マップの作成」（P.8-13）を参照してください。

ステップ 2	**class-map type inspect** *application* [**match-all** | **match-any**] *class_map_name*
	
	例：
	`hostname(config)# class-map type inspect ftp ftp_traffic`
	`hostname(config-cmap)#`
		インスペクション クラス マップを作成します。*application* は検査するアプリケーションです。サポートされるアプリケーションのリストについては、CLI ヘルプまたは第 19 章「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。
		
		class_map_name 引数は、最大 40 文字のクラス マップ名です。
		
		match-all キーワードはデフォルトです。トラフィックがクラス マップと一致するには、すべての基準と一致する必要があることを指定します。
		
		match-any キーワードは、トラフィックが少なくとも基準の 1 つに一致したらクラス マップと一致することを指定します。
		
		CLI がクラスマップ コンフィギュレーション モードに入り、1 つ以上の **match** コマンドを入力できます。

ステップ 3	（任意） **description** *string* **例：** `hostname(config-cmap)# description All UDP traffic`	クラス マップに説明を追加します。
ステップ 4	アプリケーションで使用可能な 1 つ以上の **match** コマンドを入力して、クラスに含めるトラフィックを定義します。	クラス マップと照合しないトラフィックを指定するには、**match not** コマンドを使用します。たとえば、**match not** コマンドで文字列「example.com」を指定すると、「example.com」が含まれるすべてのトラフィックはクラス マップと照合されません。 各アプリケーションで使用可能な **match** コマンドについては、該当するインスペクションの章を参照してください。

例

ユーザ名とパスワードを送信する前に、すべての FTP ユーザに接続時バナーが表示されます。デフォルトでは、このバナーには、ハッカーがシステムの弱点を特定するのに役立つバージョン情報が含まれます。このバナーをマスクする方法を次に示します。

```
hostname(config)# policy-map type inspect ftp mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mask-banner
hostname(config)# class-map match-all ftp-traffic
hostname(config-cmap)# match port tcp eq ftp
hostname(config)# policy-map ftp-policy
hostname(config-pmap)# class ftp-traffic
hostname(config-pmap-c)# inspect ftp strict mymap
hostname(config)# service-policy ftp-policy interface VM1
```

関連情報

インスペクション ポリシーを使用するには、第 14 章「モジュラ ポリシー フレームワークを使用したサービス ポリシーの設定」を参照してください。

関連情報