CHAPTER 6

ポリシー テンプレートの設定

この章では、Cisco Traffic Anomaly Detector Module（Detector モジュール）がゾーンのポリシーの作成に使用するゾーンのポリシー テンプレートの設定方法について説明します。

ここでは、Detector モジュールの付属製品である Cisco Guard（Guard）について説明します。Guard は Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃を検出および軽減するデバイスです。攻撃トラフィックをドロップし、正当なトラフィックをネットワークに再注入することで、トラフィックがゾーンを通過するときにゾーン トラフィックをクリーニングします。Detector モジュールは、ゾーンが攻撃を受けていると判断したときに、Guard の攻撃軽減サービスをアクティブにすることができます。また、Detector モジュールはゾーンの設定を Guard と同期させることもできます。Guard の詳細については、『*Cisco Anomaly Guard Module Configuration Guide*』または『*Cisco Guard Configuration Guide*』を参照してください。

この章は、次の項で構成されています。

ポリシー テンプレートについて

ポリシー テンプレートは、ゾーンのポリシーを作成するために Detector モジュールがラーニング プロセスのポリシー構築フェーズ中に使用するポリシー構築規則を集めたものです。新しいゾーンを作成すると、Detector モジュールはゾーンの設定に一連のポリシー テンプレートを含めます。各ポリシー テンプレートの使用により、Detector モジュールは、ポリシー構築フェーズ中にゾーンのトラフィックの特性に基づいてポリシーのグループを生成できます。Detector モジュールは、ポリシーを使用して、ゾーンのトラフィックにゾーンへの攻撃の兆候を示す異常がないかどうかを監視します。ゾーンのポリシーは、特定のトラフィック フローがポリシーのしきい値を超過すると、そのフローに対してアクションを実行するように設定されます。

ゾーンのポリシー テンプレートの設定を変更すると、ポリシー構築フェーズが影響を受けます。WBM を使用してゾーンのポリシー テンプレートをイネーブルまたはディセーブルにするか、変更すると、Detector モジュールがポリシー構築フェーズ中に作成するポリシーを制御できます。

Detector モジュールがポリシー構築フェーズ中に使用するポリシー テンプレートには、トラフィック フローのサービスと適合させるために、いくつかのタイプがあります。ポリシー テンプレートの名前は、作成するすべてのポリシーに共通の特性に由来し、Domain Name System（DNS; ドメイン ネーム システム）などのプロトコル、HTTP などのアプリケーション、または ip_scan などの目的を表すものになります。たとえば、ポリシー テンプレート *tcp_connections* は、同時接続数など、接続に関連するポリシーを作成します。

表 6-1 に、Detector モジュールのポリシー テンプレート タイプの説明を示します。

表 6-1　ポリシー テンプレート

ポリシー テンプレート	作成される一連のポリシーの関連先
dns_tcp	DNS-TCP プロトコル トラフィック。
dns_udp	DNS-UDP プロトコル トラフィック。
fragments	断片化されたトラフィック。
http	ポート 80（デフォルト）またはその他のユーザ設定ポートを通過する HTTP トラフィック。
ip_scan	IP スキャニング。クライアントが特定の送信元 IP アドレスからゾーン内の多数の宛先 IP アドレスにアクセスしようとしている状況です。このポリシー テンプレートは、主に、IP アドレス定義がサブネットであるゾーンのために設計されています。 デフォルトでは、このポリシー テンプレートはディセーブルになっています。このポリシー テンプレートのデフォルトのアクションは、notify です。 **（注）** このポリシー テンプレートから生成されたポリシーはリソース消費量が多いため、ネットワーク パフォーマンスに影響を及ぼす可能性があります。
other_protocols	TCP と UDP 以外のプロトコル。

表 6-1　ポリシー テンプレート（続き）

ポリシー テンプレート	作成される一連のポリシーの関連先
port_scan	ポート スキャニング。クライアントが特定の送信元 IP アドレスからゾーン内の多数のポートにアクセスしようとしている状況です。 デフォルトでは、このポリシー テンプレートはディセーブルになっています。このポリシー テンプレートのデフォルトのアクションは、notify です。 **（注）** このポリシー テンプレートから生成されたポリシーはリソース消費量が多いため、ネットワーク パフォーマンスに影響を及ぼす可能性があります。
tcp_connections	TCP 接続の特性。
tcp_not_auth	Detector モジュールのスプーフィング防止機能が認証していない TCP 接続。
tcp_outgoing	ゾーンによって開始された TCP 接続。
tcp_ratio	SYN パケットと FIN/RST パケットの比率など、各種の TCP パケットの比率。
tcp_services	HTTP 関連ポート（ポート 80 や 8080 など）以外のポートの TCP サービス。
udp_services	UDP サービス。

Detector モジュールには、表 6-2 に示すように、特定のゾーン テンプレートから作成されたゾーンのための追加のポリシー テンプレートがあります。

表 6-2　特定のポリシー テンプレート

ゾーン テンプレート	ポリシー テンプレート
DETECTOR_WORM	worm_tcp：TCP ワームに関する一連のポリシーを構築します。ワーム TCP ポリシーはワーム攻撃を管理します。ワーム攻撃では、1 つまたは複数の送信元 IP アドレスが、同一ポート上に数多くの宛先 IP アドレスとの不完全な接続を多数作成します。このポリシー テンプレートは、主に、IP アドレス定義がサブネットであるゾーンのために設計されています。 Detector モジュールは、ポリシー構築フェーズ中ではなく、ラーニング プロセスのしきい値調整フェーズ中に、このポリシー テンプレートから作成されたポリシーにサービスを追加します。ポリシー テンプレートのパラメータ max_services と min_threshold は、このポリシー テンプレートには適用されません。

GUARD_ ゾーン テンプレートからゾーンを作成する場合、Guard に同期させることができる、追加のポリシー テンプレートのパラメータを設定できます。Guard は、次の追加のポリシー テンプレートをサポートします。

- tcp_services_ns：TCP サービス。デフォルトでは、tcp_services_ns テンプレートによって作成されたポリシーは IRC ポート（666X）、Secure Shell（SSH; セキュア シェル）、および Telnet に関連します。このポリシー テンプレートは、トラフィック フローに強化保護レベルを適用するアクションを持つポリシーを作成しません。

- tcp_connections_ns、tcp_outgoing_ns、および http_ns：Guard には、TCP プロキシのスプーフィング防止機能を使用しないゾーンを保護できる、追加のポリシー テンプレートが用意されています。Internet Relay Chat（IRC; インターネット リレー チャット）サーバ タイプ ゾーンなど、ゾーンが IP アドレスに基づいて制御されている場合や、ゾーン上で実行されているサービスのタイプが不明な場合、これらのポリシー テンプレートを使用できます。
- GUARD_TCP_NO_PROXY ゾーン テンプレートを使用してゾーンを定義する場合、Guard は、ポリシー テンプレート http、tcp_connections、および tcp_outgoing を、ポリシー テンプレート http_ns、tcp_connections_ns、および tcp_outgoing_ns に置き換えます。http_ns、tcp_connections_ns、および tcp_outgoing_ns の各ポリシー テンプレートは、Guard に対して強化保護レベルの使用を要求するアクションを実行するポリシーを作成しません。

ポリシー テンプレートの設定の変更

ラーニング プロセス時、Detector モジュールはゾーン トラフィックのコピーを分析します。アクティブなポリシー テンプレートはそれぞれ、ポリシー定義とゾーンのトラフィック特性に基づいて、ポリシーのグループを生成します。Detector モジュールは、ポリシー テンプレートが監視するサービス（プロトコルとポート番号）をトラフィック量のレベルによってランク付けします。次に Detector モジュールは、トラフィック量が最大のサービス、および定義済みの最小しきい値を超えたサービスを選択し、各サービスのポリシーを作成します。ポリシー テンプレートの中には、特定のポリシーが追加されなかったすべてのトラフィック フローを *any* というサービスで処理するために、追加のポリシーを作成するものもあります。

次のようにポリシー テンプレートのパラメータを変更し、ポリシー構築フェーズを管理することができます。

- ポリシー テンプレートをイネーブルまたはディセーブルにします。ポリシー構築フェーズ中にポリシーを生成できるのは、イネーブルになっているポリシー テンプレートだけです。
- ポリシー テンプレートがラーニング プロセスのどの時点でサービスのトラフィック量に基づいてポリシーを作成するかを制御します。
- ポリシー構築フェーズ中に Detector モジュールがポリシー テンプレートを使用して作成できるポリシーの最大数を定義します。

ポリシー テンプレートの設定を変更するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Configuration > Policy Templates > View** を選択します。Policy Templates 画面が表示されます。

ステップ 3　ポリシー テンプレートを選択します。Config Policy Template 画面が表示されます。

ステップ 4　ポリシー テンプレートの目的のパラメータを変更します。表 6-3 に、Policy Template フォームに表示されるポリシー テンプレートのパラメータの説明を示します。選択したポリシー テンプレートのタイプに応じて、この表に表示されている一部または全部のパラメータが編集対象として表示されます。

表 6-3　ポリシー テンプレートのパラメータ

パラメータ	説明
State	ポリシー テンプレートの動作状態。次のいずれかのオプションを選択します。 • enable：Detector　モジュールは、ラーニング　プロセスのポリシー構築フェーズ実行中にポリシー テンプレートをトラフィック フローに適用します。Detector モジュールは、サービスを検出すると、そのサービス用に設計されているポリシー テンプレートの規則に基づいて、新しいポリシーを作成します。 • disable：Detector　モジュールは、ラーニング　プロセスのポリシー構築フェーズ実行中にポリシー テンプレートをトラフィック フローに適用しません。ディセーブルになっているポリシー テンプレートに関連付けられたサービスを検出した場合、Detector モジュールは新しいポリシーを作成しません。 **注意**　ポリシー テンプレートをディセーブルにすると、Detector モジュールによるゾーン トラフィックの異常の検出に大きな支障をきたす恐れがあります。ポリシー テンプレートをディセーブルにした場合、Detector モジュールは、そのポリシー テンプレートが管理対象にしている悪意のあるトラフィック タイプを管理するポリシーを作成しません。
Min Threshold	サービスの最小トラフィック量。サービスのトラフィック レートがしきい値を超過すると、Detector モジュールは、しきい値を超過した特定のトラフィック フローに応じて、そのサービス トラフィックに関連するポリシーを構築します。このしきい値を設定することにより、異常の検出動作をより適切にゾーン サービスの既知のトラフィック量に合せることができます。 トラフィック異常の検出の適切な実行に不可欠なポリシー テンプレートの最小しきい値パラメータを設定することはできません。tcp_services、udp_services、other_protocols、http、fragments などのポリシーでは、ゾーンのトラフィックの必要に応じて常にポリシーが作成されます。 最小しきい値レートを入力します（パケット / 秒単位）。同時接続および SYN/FIN 比率を測定する場合、しきい値は接続の合計数です。

表 6-3　ポリシー テンプレートのパラメータ（続き）

パラメータ	説明
Max Services	ポリシー テンプレートがポリシーを選択して作成する対象となるサービス（プロトコル番号またはポート番号）の最大数。Detector モジュールは、ポリシー テンプレートが関連しているサービスを、各サービスのトラフィック量のレベルによってランク付けします。次に Detector モジュールは、トラフィック量が最大のサービス、および定義済みの最小しきい値（*min-threshold* パラメータで定義したもの）を超えたサービスを選択し、各サービスのポリシーを作成します。Detector モジュールは、*any* というサービスが含まれたポリシーを追加して、このポリシー テンプレートの特性を備えた他のすべてのトラフィック フローを処理する場合もあります。 **（注）** サービスの最大数が大きいほど、ゾーンは多くのメモリを使用します。 最大サービス数パラメータは、tcp_services、tcp_services_ns、udp_services、および他のプロトコルなどのサービスを検出するポリシー テンプレートだけに定義できます。最大サービス数は、特定のサービスを監視するポリシー テンプレート（サービス 53 を監視する *dns_tcp* など）や、特定のトラフィック特性に関連するポリシー テンプレート（*fragments* など）には定義できません。 Detector モジュールは、ポリシーのトラフィック特性に基づいて、サービスのトラフィック レートを測定します。トラフィック特性は、送信元 IP アドレスまたは宛先 IP アドレスです。サービス *any* を監視するポリシーは、特定のポリシーによって処理されないために精密ではないすべてのサービス上の送信元 IP アドレスのレートを測定します。 サービス数を制限することにより、独自のトラフィック フロー要件に合せて Detector モジュール ポリシーを設定できます。

ステップ 5　次のいずれかのオプションを選択します。

- **OK**：新しいポリシー テンプレートの設定を保存します。Policy Template 画面が表示されます。
- **Clear**：フォームの情報をデフォルト値に戻し、追加した情報をすべて消去します。
- **Cancel**：情報を保存せずに Config policy template 画面を終了します。Policy Template 画面が表示されます。

特定のポリシー テンプレートで作成されたすべてのポリシーに関してサービスを追加または削除する方法については、第 8 章「ゾーンのポリシーの管理」の「サービスの追加」または「サービスの削除」の項を参照してください。