CHAPTER 6

ポリシー テンプレートの設定

ポリシー テンプレートは、ラーニング プロセスのポリシー構築フェーズ中に Guard が使用する規則とガイドラインの集合です。このテンプレートを使用して、ゾーンのトラフィック フローで検出されたサービスのための新しいゾーン ポリシーが構築されます。各ポリシー テンプレートの出力は、DDoS 攻撃からゾーンを保護するために Guard が使用する一連のゾーン ポリシーです。新しいゾーンを作成すると、Guard は新しい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。

この章では、高度なポリシー テンプレート設定作業を実施する方法について説明します。ゾーンのポリシー テンプレートの設定を変更すると、ラーニング プロセスのポリシー生成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、Guard がポリシー生成フェーズ中に作成するポリシーを制御できます。

この章は、次の項で構成されています。

ポリシー テンプレートのタイプ

Guard がポリシー構築フェーズ中に使用できるポリシー 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、Guard がテンプレートから作成するすべてのポリシーに共通の特性に由来しています。この特性は、プロトコル（DNS など）やアプリケーション（http など）、目的（ip_scan など）です。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 で、Guard の各ポリシー テンプレート タイプについて説明します。

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 トラフィック（送信元 IP アドレスが、ゾーン内部の複数の宛先 IP アドレスにアクセスしようとしている状況）。このポリシー テンプレートは、主に定義済みゾーンがサブネットであるアプリケーショ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 テンプレートに設定されているデフォルト アクションは、**notify** です。 **注意**　ip_scan ポリシー テンプレートに基づいて作成されたポリシーはリソース消費量が多いため、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。port_scan ポリシー テンプレートは、リモート クライアントが特定の送信元 IP アドレスからゾーン内部の複数のポートにアクセスしようとする攻撃を管理するためのポリシーを作成します。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。 **注意**　port_scan ポリシー テンプレートに基づいて作成されたポリシーはリソース消費量が多いため、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	Guard 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。
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）、SSH、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。
udp_services	UDP サービス。

Guard は、まず、専用ポート 6660 ～ 6670 および 21 ～ 23 上の TCP トラフィックのインジケータを検索します。Guard がこれらのポート上でトラフィックを検出した場合は、次の処理が実行されます。

- tcp_services_ns ポリシー テンプレートは、ポート 6660 ～ 6670 および 21 ～ 23 上の TCP トラフィックに関連する一連のポリシーを作成します。
- tcp_services ポリシー テンプレートは、他のすべてのポート上の TCP サービスを処理します。

Guard がこれらのポート上でトラフィックを検出しない場合、tcp_services_ns ポリシー テンプレートは使用されません。

表 6-2 に、Guard をプロキシとして使用しないゾーン用に設計されたその他のポリシー テンプレートを示します。これらのポリシー テンプレートは、インターネット リレー チャット（IRC）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運用されている場合に使用できます。これらのテンプレートで作成されたポリシーには、強化保護レベルをトラフィック フローに適用するアクションがありません。

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と、Guard は表 6-2 で説明するポリシー テンプレートを使用します。Guard は、http、tcp_connections、および tcp_outgoing のポリシー テンプレートをそれぞれ http_ns、tcp_connections_ns、および tcp_outgoing_ns のポリシー テンプレートに置き換えます。

表 6-2　TCP_NO_PROXY 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
tcp_connections_ns	TCP 接続の特性。
tcp_outgoing_ns	ゾーンによって開始された TCP 接続。
http_ns	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。

ポリシー テンプレート設定の変更

ポリシー構築フェーズを管理するには、ポリシー テンプレートの特定のパラメータを次の方法で変更して、ポリシー生成フェーズを管理します。

- 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。ポリシー生成フェーズ中に Guard が検出するサービスに基づいてポリシーを作成するのは、イネーブルになっているポリシー テンプレートのみです。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 フローを処理する追加のポリシーを作成するものもあります。このようなポリシーは、*any* というサービスで追加されます。
- 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 テンプレートがポリシーを作成するかを制御します。
- ラーニング プロセス中に Guard 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** 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 Form 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、このテーブル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**：ポリシー テンプレートは、ラーニング プロセスのポリシー構築フェーズ実行中にトラフィック フローに適用されます。Guard は、サービスを検出すると、検出された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**：Guard 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。Guard は、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するサービスを検出しても、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、ゾーン保護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、Guard 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を定義します。当該のサービスを使用している特定のトラフィック フローがこのしきい値を超過すると、Guard はそのトラフィックに関連するポリシーを構築します。正しいゾーン保護に不可欠であるためにポリシーを常に構築するポリシー テンプレートに、このパラメータを設定することはできません。ポリシー テンプレート（http、tcp_services、tcp_services_ns、udp_services、other_protocols、および port_scan）に、最小しきい値を設定することはできません。 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 テンプレートが検出して、ポリシーの作成対象にするサービス（プロトコル番号またはポート番号）の最大数。サービスの最大数を定義する整数を入力します。 Guard は、ポリシー テンプレートの適用対象となるサービスをトラフィック量のレベルによってランク付けします。Guard は、定義済みの最小しきい値（Min Threshold パラメータで定義）を超えたサービスの中で最大のトラフィック量を持ついくつかのサービスを選択して、各サービスのポリシーを作成します。Guard は、そのポリシー 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 フローを処理する追加のポリシーを、**any** というサービス パラメータ設定で追加することがあります。設定するサービスの最大数が大きいほど、ゾーンが必要とする Guard メモリが多くなります。 サービス（tcp_services、tcp_services_ns、udp_services、および other_protocols）だけを検出するポリシー テンプレートに、このパラメータを定義することができます。次のポリシー テンプレートに対しては、このパラメータを設定できません。 • サービス 53 に関連する dns_tcp ポリシー テンプレートなど、特定のサービスに関連するポリシー テンプレート。 • fragments ポリシー テンプレートなど、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。 Guard は、ポリシーのトラフィック特性に応じて、サービスに対するトラフィック レートを測定します。トラフィック特性には、送信元 IP アドレス、宛先 IP アドレス、または送信元ネットを指定できます。サービス **any** に関連するポリシーは、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。

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から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。