CHAPTER 8

ポリシー テンプレートとポリシーの設定

この章では、Cisco Anomaly Guard Module（Guard モジュール）のゾーン ポリシー、ポリシー構造、およびポリシー テンプレートについて説明します。また、ゾーン ポリシーとポリシー テンプレートのパラメータの設定方法についても説明します。

この章は、次の項で構成されています。

ゾーン ポリシーについて

Guard モジュールは、ゾーン ポリシーにより、ゾーンのトラフィック フローの統計分析を行うことができます。ポリシーは、ポリシー タイプに応じて、次のいずれかのトラフィック特性を監視します。

- トラフィック レート：パケット / 秒単位またはパケット / 時単位で測定した、トラフィックのレート。パケット / 時単位でトラフィックを監視するポリシー（PPH ポリシー）は、ゾーン トラフィックで、何時間または何日も続くことのある低レート ゾンビ攻撃を監視するために使用されます。PPH ポリシーの詳細については、P.8-14 の「ポリシー パラメータの設定」を参照してください。
- 接続：同時接続の数。
- パケットの比率：あるパケット タイプと別のパケット タイプの比率。

ゾーン ポリシーは、特定のトラフィック フローが悪意のあるものまたは異常なものと判断された場合（トラフィック フローがポリシーのしきい値を超えた場合）、そのフローに対してアクションを実行し、フィルタ（動的フィルタ）を動的に設定し、攻撃の重大度に応じてそのフローを保護するように設定されます。ポリシーのトリガー、およびポリシーがアクティブになったときに実行するアクションを設定できます。

各ゾーン設定には、ポリシーのセットが含まれています。ポリシー テンプレートを使用して新しいゾーンを作成する場合、Guard モジュールは、そのテンプレートに関連付けられているポリシーを新しいゾーンに設定します。既存のゾーンをコピーして新しいゾーンを作成する場合、Guard モジュールは、既存のゾーンのポリシーを新しいゾーンに設定します。

ゾーン固有のポリシーを作成し、通常のゾーン トラフィックを認識するようしきい値を調整するために、Guard モジュールは 2 つのフェーズのラーニング プロセスでゾーン トラフィックをラーニングします（P.1-5 の「ラーニング プロセスについて」を参照）。Guard モジュールは事前定義されたポリシー テンプレートを使用してポリシーを構築し、それからゾーン トラフィックによって決定されたポリシーのしきい値をラーニングします。Guard モジュールは、各ポリシー テンプレートを使用して、特定の DDoS 攻撃（分散型サービス拒絶攻撃）の脅威からゾーンを保護するために必要なポリシーを作成します。Guard モジュールがゾーン ポリシーを作成および調整したら、ゾーン ポリシーの追加および削除、またはゾーン ポリシー パラメータの変更が行えます。

ポリシーには、相互依存性および優先度があります。2 つの異なるポリシーが同じトラフィック フローを定義する場合、Guard モジュールは、より限定的なポリシーを使用してフローを分析します。たとえば、TCP サービスに関連するポリシーでは、HTTP 関連のポリシーによって処理される HTTP サービスが除外されます。

ポリシー テンプレートとその設定について

ポリシー テンプレートとは、Guard モジュールがポリシー構築フェーズでゾーン ポリシーを作成するときに使用する、ポリシー構築の規則の集まりです。ポリシー構築フェーズの終わりに、Guard モジュールは、ポリシー テンプレートを使用して作成されたゾーン固有のポリシー セットを持つようになります。ポリシー テンプレートには、テンプレートから作成されるすべてのポリシーに共通の特性に由来した名前が付けられます。共通の特性の例には、プロトコル（dns など）、アプリケーション（http など）、または目的（ip_scan など）があります。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生成します。新しいゾーンを作成するときに、Guard モジュールによって一連のポリシー テンプレートがゾーン設定に組み込まれます。

表 8-1 で、Guard モジュールのポリシー テンプレートについて説明します。GUARD_DEFAULT ゾーン テンプレートを使用して新しいゾーンを作成すると、Guard モジュールはこれらのポリシー テンプレートを含めます。

表 8-1　ポリシー テンプレート

ポリシー テンプレート	構築されるポリシーのグループが関連する対象
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）または他のユーザ設定ポートを経由する HTTP トラフィック。
ip_scan	IP スキャニング（1 つの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する状況）。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向け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 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多くのシステム リソースを消費するため、Guard モジュールの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 以外のプロトコルと UDP 以外のプロトコル。
port_scan	ポート スキャンニング（1 つの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する状況）。 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 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多くのシステム リソースを消費するため、Guard モジュールの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 モジュールのスプーフィング防止機能によって認証されていない TCP 接続。
tcp_outgoing	ゾーンによって開始された TCP 接続。

表 8-1　ポリシー テンプレート（続き）

ポリシー テンプレート	構築されるポリシーのグループが関連する対象
tcp_ratio	異なるタイプの TCP パケット間の比率（たとえば、SYN パケットの数と FIN/RST パケットの数の比率）。
tcp_services	HTTP 関連のポート（ポート 80 やポート 8080 など）以外のポート上の TCP サービス。
tcp_services_ns	TCP サービス。デフォルトでは、このポリシー テンプレートから作成されたポリシーは、IRC ポート（666X）、SSH、および Telnet を監視します。このポリシー テンプレートは、Guard モジュールに対し、トラフィック フローに強化保護レベルを適用するよう要求するアクションを持つポリシーは作成しません。強化保護レベルの詳細については、P.1-8 の「保護サイクルについて」を参照してください。
udp_services	UDP サービス。

Guard モジュールには、特定のタイプの攻撃または特定のサービス向けに設定されているゾーン テンプレートから作成されたゾーン用に追加のポリシー テンプレートがあります。表 8-2 に、特定のゾーン テンプレートに基づいて Guard モジュールがゾーン設定に追加する、ポリシー テンプレートを示します。

表 8-2　追加のポリシー 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
GUARD_VOIP	sip_udp：VoIP[1] アプリケーションを監視するポリシー グループを構築します。監視対象の VoIP アプリケーションは、IP[2] over UDP を使用して VoIP セッションを確立し、セッション確立後に RTP/RTCP[3] を使用して音声データを SIP エンド ポイント間で伝送します。

1. VoIP = Voice over IP
2. SIP = Session Initiation Protocol
3. RTP/RTCP = Real-Time Transport Protocol/Real-Time Control Protocol

（注）　Guard モジュールは、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次のように探します。

- これらのポート上でトラフィックがトレースされる場合、tcp_services_ns ポリシー テンプレートがポリシー グループを構築し、tcp_services ポリシー テンプレートが他のポート上の TCP サービスを監視します。
- これらのポート上でトレースされるトラフィックがない場合、tcp_services_ns ポリシー テンプレートは使用されません。

tcp_services_ns ポリシー テンプレートから作成されたポリシーにはサービスを追加できます。

Guard モジュールには、TCP プロキシのスプーフィング防止機能（Guard モジュールがプロキシの役割を果たす）を使用しないゾーンを保護する追加のポリシー テンプレートがあります。これらのポリシー テンプレートは、ゾーンが IP アドレスに基づいて制御されている場合（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）、またはゾーンで実行されているサービスのタイプが不明の場合に使用できます。

GUARD_TCP_NO_PROXY ゾーン テンプレートでゾーンを定義する場合、Guard モジュールによって、表 8-3 に示されるポリシー テンプレートが使用されます。Guard モジュールは、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。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 モジュールに対し、トラフィック フローに強化保護レベルを適用するよう要求するアクションを持つポリシーは作成しません。

表 8-3 に、Guard モジュールの GUARD_TCP_NO_PROXY ポリシー テンプレートの詳細を示します。

表 8-3　GUARD_TCP_NO_PROXY のポリシー テンプレート

ポリシー テンプレート	置き換えるポリシー テンプレート	構築されるポリシーのグループが関連する対象
tcp_connections_ns	tcp_connections	TCP 接続の特性。
tcp_outgoing_ns	tcp_outgoing	ゾーンによって開始された TCP 接続。
http_ns	http	ポート 80（デフォルト）または他のユーザ設定ポートを経由する HTTP トラフィック。

すべてのポリシー テンプレートのリストを表示するには、ゾーン設定モードで **policy-template** コマンドを使用し、**Tab** キーを 2 回押してください。

ラーニング プロセス中、ゾーン トラフィックは Guard モジュールを透過的に通過します。アクティブな各ポリシー テンプレートは、ポリシー定義とゾーン トラフィック特性に基づいてポリシー グループを作成します。Guard モジュールは、トラフィック量のレベルに応じて、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）をランク付けします。次に Guard モジュールは、トラフィック量が最大のサービスと、定義済みの最小しきい値を超えたサービスを選択し、各サービスに対するポリシーを作成します。一部のポリシー テンプレートは、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、**any** というサービスを備えた追加のポリシーを作成します。

次のポリシー テンプレート パラメータを設定できます。

- サービスの最大数：Guard モジュールがポリシー テンプレートを選択して特定のポリシーを作成する対象になるサービスの最大数を定義します。
- 最小しきい値：Guard モジュールでサービスをランク付けするために超える必要のある最小しきい値を定義します。
- ポリシー テンプレートの状態：Guard モジュールがポリシー テンプレートからポリシーを作成するかどうかを定義します。

ポリシー テンプレートのパラメータを設定するには、ゾーン設定モードで次のコマンドを入力して、ポリシー テンプレート設定モードに入ります。

policy-template *policy-template-name*

policy-template-name 引数には、ポリシー テンプレートの名前を指定します。詳細については、表 8-1 を参照してください。

次の例は、http ポリシー テンプレート設定モードに入る方法を示しています。

```
user@GUARD-conf-zone-scannet# policy-template http
user@GUARD-conf-zone-scannet-policy_template-http#
```

特定のポリシー テンプレートのパラメータを表示するには、ポリシー テンプレート設定モードで **show** コマンドを使用します。

この項では、次のトピックについて取り上げます。

サービスの最大数の設定

サービスの最大数のパラメータで、ポリシー テンプレートが選択してポリシーを作成する対象となるサービスの最大数（プロトコル番号またはポート番号）を定義します。Guard モジュールは、ポリシー テンプレートに関連するサービスを、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 Guard モジュールは、トラフィック量が最大のサービスと、定義済みの最小しきい値（*min-threshold* パラメータで定義される）を超えたサービスを選択し、各サービスに対するポリシーを作成します。Guard モジュールは **any** というサービスを備えた追加のポリシーを追加し、ポリシー テンプレートの特性を持つその他のすべてのトラフィック フローを処理することができます。

（注）　サービスの最大数が大きいほど、ゾーンが必要とする Guard モジュール のメモリも多くなります。

サービスの最大数のパラメータは、サービスを検出するポリシー テンプレート（tcp_services、tcp_services_ns、udp_services、および other protocols など）にのみ定義できます。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、このパラメータは設定できません。

Guard 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 アドレスになります。**any** サービスを監視するポリシーは、特定のポリシーで処理されないすべてのサービスで送信元 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と、目的のトラフィック フロー要件に合せて Guard モジュールのポリシーを設定できます。

サービスの最大数を設定するには、ポリシー テンプレート設定モードで次のコマンドを使用します。

max-services *max-services*

max-services 引数は、Guard モジュールが選択するサービスの最大数を定義する、1 より大きい整数です。サービスの最大数が 10 を超えないようにすることをお勧めします。

次の例は、Guard モジュールが監視するサービスの最大数を 5 に設定する方法を示しています。

```
user@GUARD-conf-zone-scannet-policy_template-tcp_services# max-services 5
```

最小しきい値の設定

最小しきい値のパラメータは、サービスの最小トラフィック量を定義します。このしきい値を超えると、Guard モジュールは、しきい値を超えた特定のトラフィック フローに応じて、サービスの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と、ゾーン サービスのトラフィック量に保護を的確に合せることができます。

ポリシー テンプレート dns_tcp、dns_udp、fragments、ip_scan、port_scan、tcp_connections、tcp_not_auth、tcp_outgoing、および tcp_ratio に最小しきい値のパラメータを設定することはできません。これらのテンプレートは、正しいゾーン保護に不可欠で、必ずポリシーを構築します。

最小しきい値を設定するには、ポリシー テンプレート設定モードで次のコマンドを使用します。

min-threshold *min-threshold*

min-threshold 引数は、0 以上の実数（小数点以下が 2 桁の浮動小数点型の数字）で、最小しきい値レートをパケット / 秒（pps）単位で定義します。同時接続および SYN/FIN の比率を測定する場合、しきい値は接続の合計数を定義する整数になります。

次の例は、ポリシー テンプレート http の最小しきい値を設定する方法を示しています。

```
user@GUARD-conf-zone-scannet-policy_template-http# min-threshold 12.3
```

ポリシー テンプレートの状態の設定

ポリシー テンプレートの状態のパラメータは、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どうかを定義します。ポリシー テンプレートをディセーブルにすると、Guard モジュールがポリシー構築フェーズになっても、ポリシーは作成されません。

注意　ポリシー テンプレートをディセーブルにすると、ゾーン保護に重大な支障をきたすおそれがあります。ポリシー テンプレートをディセーブルにすると、Guard モジュールはそのポリシー テンプレートに関連するトラフィックからゾーンを保護できません。たとえば、dns_udp ポリシー テンプレートをディセーブルにすると、Guard モジュールは、DNS（UDP）攻撃を管理するゾーン ポリシーを作成しなくなります。

ポリシー テンプレートをディセーブルにするには、ポリシー テンプレート設定モードで **disable** コマンドを使用します。

ポリシー テンプレートをイネーブルにするには、ポリシー テンプレート設定モードで **enable** コマンドを使用します。

次の例は、ポリシー テンプレート http をディセーブルにする方法を示しています。

```
user@GUARD-conf-zone-scannet-policy_template-http# disable
```

すべてのポリシー テンプレート パラメータの同時設定

ゾーン設定モードで次のコマンドを入力して、1 つのコマンドで、ポリシー テンプレートのすべての動作パラメータを設定できます。

policy-template *policy-template-name max-services min-threshold* {**disabled** | **enabled**}

表 8-4 に、**policy-template** コマンドの引数とキーワードを示します。

表 8-4　policy-template コマンドの引数とキーワード

パラメータ	説明
policy-template-name	ポリシー テンプレート名。詳細については、表 8-5 を参照してください。
max-services	Guard モジュールが選択して特定のポリシー テンプレートからポリシーを構築する対象となるサービスの最大数。Guard モジュールで現在の値が変更されないようにするには、-1 という値を入力します。詳細については、P.8-6 の「サービスの最大数の設定」を参照してください。
min-threshold	Guard モジュールでサービスをランク付けするために超える必要のある最小しきい値。Guard モジュールで現在の値が変更されないようにするには、-1 という値を入力します。詳細については、P.8-7 の「最小しきい値の設定」を参照してください。
disabled	ポリシー テンプレートをディセーブルにして、ポリシーが作成されないようにします。詳細については、P.8-7 の「ポリシー テンプレートの状態の設定」を参照してください。
enabled	ポリシー テンプレートをイネーブルにします。詳細については、P.8-7 の「ポリシー テンプレートの状態の設定」を参照してください。

次の例は、ポリシー テンプレート tcp_services のパラメータを設定する方法を示しています。この例では、サービスの最大数は 3 に、ポリシーの状態は **enabled** に設定され、最小しきい値は変更されていません（–1）。

```
user@GUARD-conf-zone-scannet# policy-template tcp_services 3 -1 enabled
```

ポリシー パスについて

ポリシー パス（ポリシー名）は、複数のセクションから成り立っており、各セクションは測定対象であるトラフィック特性を示しています。たとえば、ポリシー http/80/analysis/syns/src_ip は、Guard モジュールの分析保護機能によって認証され、送信元 IP アドレスに応じて集約された、ポート 80 宛ての HTTP SYN パケットのトラフィック フローを測定します。

図 8-1 に、ゾーン ポリシー名の例を示します。

図 8-1　ポリシー名のセクション

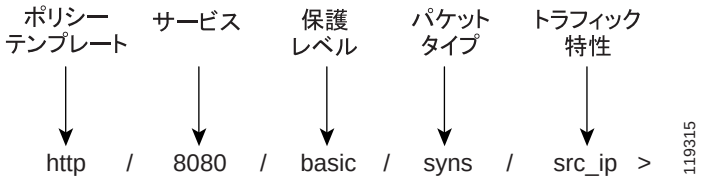

表 8-5 に、ポリシー名のセクションを示します。

表 8-5　ポリシー名のセクション

セクション	説明
ポリシー テンプレート	ポリシーの構築に使用されたポリシー テンプレート。各ポリシー テンプレートは、特定の DDoS 攻撃の脅威に対する保護のために Guard モジュールが必要とする特性を扱います。詳細については、P.8-3 の「ポリシー テンプレートとその設定について」を参照してください。
サービス	ゾーン ポリシーが監視するトラフィック フローのポート番号またはプロトコル番号。
保護レベル	Guard モジュールがトラフィック フローに適用する保護レベル。
パケット タイプ	Guard モジュールが監視するパケット タイプ。
トラフィック特性	Guard モジュールがポリシーの集約に使用するトラフィック特性。

ポリシー名の最初の 4 つのセクション（ポリシー テンプレート、サービス、保護レベル、およびパケット タイプ）は、分析されるトラフィックのタイプを定義します。ポリシー パスの最後のセクション（トラフィック特性）は、フローの分析方法を定義します。

この項では、次のトピックについて取り上げます。

- ポリシー サービスの概要と管理
- Guard モジュールの保護レベルについて
- Guard モジュールが監視するパケット タイプについて
- Guard モジュールが監視するトラフィック特性について

ポリシー サービスの概要と管理

サービス セクションは、各ポリシーに関連するゾーン アプリケーションのポートまたはプロトコルを定義します。ポリシーには、相互依存性および優先度があります。2 つの異なるポリシーが同じトラフィック フローを定義する場合、Guard モジュールは、より限定的なポリシーを使用してフローを分析します。サービス **any** は、同じポリシー テンプレートから作成された他のサービスと特に一致しないすべてのトラフィックに関連します。

個々のニーズに最適な保護にするために、ゾーンのメイン サービスに具体的なポリシーを定義することをお勧めします。

注意　Guard モジュールのパフォーマンスを低下させるおそれがあるため、複数のポリシーに同じサービス（ポート番号）を追加しないでください。

ゾーンのポリシーにサービスを追加または削除すると、Guard モジュールはゾーンのポリシーを未調整としてマークします。ゾーン保護とラーニング プロセスをイネーブルにした場合、次のいずれかの操作を実行するまで、Guard モジュールはゾーン トラフィックの異常を検出できません。

- ラーニング プロセスのしきい値調整フェーズを実行して、その結果を受け入れる（P.9-8 の「しきい値調整フェーズのアクティブ化」を参照）。
- ゾーンのポリシーを調整済みとしてマークする（P.9-12 の「ポリシーに対する調整済みのマーク付け」を参照）。

この項では、次のトピックについて取り上げます。

サービスの追加

特定のポリシー テンプレートから作成されたすべてのポリシーに、サービスを追加できます。新しいサービスは、ポリシー構築フェーズ中に検出されたサービスに追加され、デフォルト値で定義されます。しきい値を手動で定義することもできますが、ラーニング プロセスのしきい値調整フェーズを実行して、ポリシーをゾーン トラフィックに合せて調整することをお勧めします。詳細については、P.9-8 の「しきい値調整フェーズのアクティブ化」を参照してください。

新しいサービスを追加できるのは、次のポリシー テンプレートから作成されたポリシーです。

- tcp_services、udp_services、または tcp_services_ns
  このサービスは、ポート番号を表します。
- other_protocols
  このサービスは、プロトコル番号を表します。

（注）　サービスを追加した後でポリシー構築フェーズをアクティブにすると、新しいサービスによって、手動で追加したサービスが無効にされる場合があります。

次の状況では、ポリシー構築フェーズをイネーブルにしない場合は、サービスを手動で追加する必要があります。

- 新しいアプリケーションまたはサービスがゾーン ネットワークに追加された。
- ポリシー構築フェーズの実行期間が短かったため、一部のネットワーク サービスが反映されていない（たとえば、週に 1 回のみあるいは夜間のみアクティブになる既知のアプリケーションまたはサービスがある）。

サービスを追加するには、次のコマンドのいずれかを使用します。

- **add-service** *service-num*（ポリシー テンプレート設定モードで使用）
- **policy-template** *policy-template-name* **add-service** *service-num*（ゾーン設定モードで使用）

表 8-6 に、**add-service** コマンドの引数を示します。

表 8-6　add-service コマンドの引数

パラメータ	説明
service-num	プロトコル番号またはポート番号。
policy-template-name	ポリシー テンプレート名。詳細については、表 8-1 を参照してください。

次の例は、ポリシー テンプレート tcp_services から作成されたすべてのポリシーに、サービスを追加する方法を示しています。

```
user@GUARD-conf-zone-scannet-policy_template-tcp_services# add-service 25
```

サービスの削除

すべてのポリシー テンプレートから作成された特定のサービスを削除できます。Guard モジュールは、特定のポリシー テンプレートから作成されたすべてのポリシーからサービスを削除します。

サービスを削除するには、次のコマンドのいずれかを使用します。

- **remove-service** *service-num*（ポリシー テンプレート設定モードで使用）
- **policy-template** *policy-template-name* **remove-service** *service-num*（ゾーン設定モードで使用）

表 8-7 に、**remove-service** コマンドの引数を示します。

表 8-7　remove-service コマンドの引数

パラメータ	説明
service-num	削除するプロトコル番号またはポート番号。
policy-template-name	ポリシー テンプレート名。詳細については、表 8-1 を参照してください。

注意　サービスを削除すると、Guard　モジュールはそのサービスのトラフィックを監視できなくなり、ゾーン保護に支障をきたすおそれがあります。

次のポリシー テンプレートからサービスを削除できます。

- tcp_services、udp_services、または tcp_services_ns

  このサービスは、ポート番号です。
- other_protocols

  このサービスは、プロトコル番号です。

次の状況では、ラーニング プロセスのポリシー構築を実行しない場合は、サービスを手動で削除する必要があります。

- アプリケーションまたはサービスがネットワークから削除された。
- （ネットワーク環境内で一般的でないという理由から）保護をイネーブルにしたくないアプリケーションまたはサービスが、ポリシー構築フェーズ中に識別された。

（注）　サービスを削除した後でポリシー構築フェーズを実行すると、Guard モジュールが同じサービスをゾーン設定に追加する場合があります。

次の例は、ポリシー テンプレート tcp_services から作成されたすべてのポリシーから、サービスを削除する方法を示しています。

```
user@GUARD-conf-zone-scannet-policy_template-tcp_services# remove-service 25
```

Guard モジュールの保護レベルについて

Guard モジュールには 3 つの保護レベルがあり、各レベルではさまざまなプロセスをトラフィック フローに適用しています。Guard には、次の 3 つの保護レベルがあります。

- 分析保護レベル：Guard モジュールはトラフィックの通過を許可します。ゾーン保護中、通過するトラフィックは、監視された状態ですが、異常がトレースされない限り遮断されません。Guard モジュールが異常をトレースすると、そのトラフィックを適切な保護レベルに誘導します。
- 基本保護レベル：Guard モジュールはスプーフィング防止機能やゾンビ防止機能をアクティブにし、疑わしいトラフィック フローを調べてトラフィックを認証し、その送信元を確認します。Guard モジュールは、各ホストに対して認証を行います。認証は、事前定義された期間に限り有効です。この期間が経過すると、Guard モジュールはもう一度ホストを認証します。
- 強化保護レベル：Guard モジュールは、強力なスプーフィング防止機能をアクティブにします。この機能により、トラフィック フローのパケットが調べられ、その正当性が確認されます。

Guard モジュールは、各接続に対して認証を行います。

保護機能をアクティブにした後、Guard モジュールは引き続きトラフィックを分析します。Guard モジュールは、ゾーン宛てのトラフィックでトラフィック異常を検出すると、より強力な保護メカニズムをアクティブにします。

（注）　保護レベルの設定は静的であり、手動で設定することはできません。

Guard モジュールが監視するパケット タイプについて

Guard モジュールはパケット特性を監視します。パケット特性は、次のいずれかです。

- パケット タイプ（TCP-SYN パケットなど）
- パケット分析（認証済みパケットなど。認証済みパケットとは、パケット接続で TCP ハンドシェイクを実行していることを Guard モジュールが確認済みであるパケットのこと）
- パケット方向（着信接続など）

表 8-8 で、Guard モジュールが監視するパケット タイプについて説明します。

表 8-8　パケット タイプ

パケット タイプ	説明
auth_pkts	TCP ハンドシェイクまたは UDP 認証が実行されたパケット。
auth_tcp_pkts	TCP ハンドシェイクが実行されたパケット。
auth_udp_pkts	UDP 認証が実行されたパケット。
in_nodata_conns	接続上でデータ転送のない着信ゾーン接続（データ ペイロードのないパケット）。
in_conns	着信ゾーン接続。
in_pkts	着信ゾーンの DNS クエリー パケット。
in_unauth_pkts	着信ゾーンの認証されていない DNS クエリー。

表 8-8　パケット タイプ（続き）

パケット タイプ	説明
num_sources	TCP の発信元 IP アドレスがゾーン宛てで、Guard モジュールのスプーフィング防止機能に認証されているパケット。
out_pkts	着信ゾーン DNS 応答パケット。
reqs	データ ペイロードを持つ要求パケット。ポリシー パスでこのパケット タイプ ID に _pph が追加されている場合（たとえば、reqs_pph）、ポリシーは要求パケットのトラフィック レートをパケット / 秒単位ではなくパケット / 時単位で測定します。
syns	同期パケット（TCP SYN フラグの付いたパケット）。ポリシー パスでこのパケット タイプ ID に _pph が追加されている場合（たとえば、syns_pph）、ポリシーは同期パケットのトラフィック レートをパケット / 秒単位ではなくパケット / 時単位で測定します。
syn_by_fin	SYN および FIN フラグの付いたパケット。Guard モジュールは SYN フラグの付いたパケット数と FIN フラグの付いたパケット数の比率を確認します。
unauth_pkts	TCP ハンドシェイクが実行されなかったパケット。
pkts	同じ保護レベルの他のどのカテゴリにも入らないすべてのパケット タイプ。

Guard モジュールが監視するトラフィック特性について

トラフィック特性とは、トラフィック フローをどのように分析するか、またポリシーの集約にどのような特性が使用されたか定義するものです。分析するトラフィックが同じでも、異なる特性に基づいてレートを測定する異なるポリシーがあります。次にその例を示します。

dns_tcp/53/analysis/pkts/dst_ip と dns_tcp/53/analysis/pkts/src_ip。

表 8-9 に、Guard モジュールが監視するトラフィック特性を示します。

表 8-9　トラフィック特性

トラフィック特性	説明
dst_ip	ゾーンの IP アドレス宛のトラフィック。
dst_ip_ratio	特定の IP アドレス宛の、SYN フラグの付いたパケットと FIN フラグの付いたパケットの比率。
dst_port	特定のゾーン ポート宛のトラフィック。
dst_port_ratio	特定のポート宛の、SYN フラグの付いたパケットと FIN フラグの付いたパケットの比率。
global	他のポリシー セクションによって定義されたすべてのトラフィック フローの合計。
protocol	プロトコルに基づいて集約された、ゾーン宛のトラフィック。
src_ip	送信元 IP アドレスに応じて集約された、ゾーン宛のトラフィック。
src_ip_many_dst_ips	同一ポート上の多数のゾーン IP アドレスにアクセスしようとしている 1 つの IP アドレスからのトラフィック。このキーは IP スキャニングに使用されます。
src_ip_many_ports	1 つのゾーン宛先 IP アドレス上の多数のポートにアクセスしようとしている 1 つの IP アドレスからのトラフィック。このキーはポート スキャニングに使用されます。

ポリシー パラメータの設定

ラーニング プロセスの完了後は、特定のポリシー パラメータ（ポリシー状態、ポリシーしきい値、ポリシー タイムアウト、ポリシー アクション、およびポリシーのインタラクティブ状態）を表示して、ポリシー パラメータがゾーン トラフィックに適合するかどうかを判断できます。単一のポリシーまたはポリシー グループのポリシー パラメータがゾーン トラフィック要件を満たすように設定できます。

ゾーンに関連付けられているポリシーのリストを表示するには、ゾーン設定モードで次のコマンドを使用します。

show policies

特定のポリシーの現在のパラメータ設定を表示するには、ポリシー設定モードで **show** コマンドを使用します。ポリシー設定モードに入るには、ゾーン設定モードで次のコマンドを使用します。

policy *policy-path*

policy-path 引数には、ポリシー パス セクションを指定します。パスは、ポリシー セクションの一部のみを含む部分パスでもかまいません。ポリシー パスの詳細については、「ポリシー パスについて」の項を参照してください。

（注）　ポリシー パス階層で 1 レベル上に移動するには、ポリシー パス プロンプトで **policy. . .** を入力します。

次の例は、dns_tcp/53/analysis/syns/global ポリシー設定モードに入る方法を示しています。

```
user@GUARD-conf-zone-scannet# policy dns_tcp/53/analysis/syns/global
user@GUARD-conf-zone-scannet-policy-/dns_tcp/53/analysis/syns/global#
```

ポリシーのアクション、タイムアウト、しきい値、およびラーニングのパラメータは、ポリシー パスの各セクションで変更できます。ただし、上位レベルのポリシー セクション（ポリシー テンプレート セクションまたはサービス セクションなど）でこれらのパラメータを変更すると、より多くのポリシーが影響を受けます。上位レベルのポリシー パス階層でこれらのパラメータを設定すると、すべてのサブポリシー パスでこれらのパラメータが変更されます。各ポリシー パス セクションでは、ワイルドカード文字としてアスタリスク（*）を使用できます。ポリシー パス セクションを指定しないと、指定していないセクションが Guard モジュールによってワイルドカード（*）と見なされます。たとえば、tcp_services//analysis//global ポリシーでは、サービスとパケット タイプにワイルドカードが使用されています。

ゾーン トラフィックの低トラフィック レート ゾンビ攻撃を監視するポリシーの検出時間パラメータを設定することもできます。このようなポリシーは PPH ポリシーと呼ばれ、（パケット / 秒単位ではなく）パケット / 時単位でトラフィック レートを監視します。このようなポリシーのパス名のパケット タイプには、次の例のように _pph が追加されています。

```
user@GUARD-conf-zone-scannet-policy-/tcp_services/any/strong/reqs_pph/src_ip#
```

（注）　PPH ポリシーは、6.1 または 6.1-XG ソフトウェア リリースで作成するゾーン設定だけに含まれます。以前のソフトウェア バージョンで作成したゾーンには、PPH ポリシーが含まれません。

（注）　新しいゾーンの作成時には、PPH ポリシーはデフォルトでディセーブル状態に設定されています。これは、PPH ポリシーにより、ゾーンが使用するメモリ量が増加したり、Guard モジュールのパフォーマンスに影響が及んだりする可能性があるからです。ゾーンの PPH ポリシーをイネーブルにするには、ポリシーの状態をアクティブに変更する必要があります（「ポリシーの状態の変更」の項を参照）。

この項では、次のトピックについて取り上げます。

- ポリシーの状態の変更
- ポリシーのしきい値の設定
- ポリシーのタイムアウトの設定
- ポリシー アクションの設定
- PPH ポリシーの検出時間パラメータの設定
- ポリシーのインタラクティブ ステータスの設定

ポリシーの状態の変更

ゾーン ポリシーには、次の 3 つの状態があります。

- アクティブ：ポリシーはトラフィックを監視し、しきい値を超えた場合にアクションを実行します。
- 非アクティブ：ポリシーはトラフィックを監視し、しきい値を取得しますが、しきい値を超えてもアクションは実行しません。ポリシーを非アクティブにし、ラーニング プロセスのしきい値調整フェーズが再度実行されないようにすることができます。
- ディセーブル：ポリシーはトラフィック フローを監視しないので、しきい値を取得しません。

（注）　Guard モジュールが他のポリシーの正確なしきい値を監視するようにするには、ラーニング プロセスのしきい値調整フェーズをアクティブにすることをお勧めします。

注意　ポリシーをディセーブルにすると、アクティブなゾーン ポリシーは、ディセーブル済みポリシーが通常監視するトラフィックに対して責任を負うようになります。アクティブなポリシーのしきい値を調整するには、ゾーン保護をアクティブにする前に、しきい値調整フェーズをアクティブにすることをお勧めします。

ポリシーの状態を変更するには、ポリシー設定モードで次のコマンドを使用します。

state {**active** | **disabled** | **inactive**}

表 8-10 に、**state** コマンドのキーワードを示します。

表 8-10　state コマンドの引数とキーワード

パラメータ	説明
active	ポリシーをアクティブにして、トラフィックがポリシーのしきい値を超えた場合に、割り当てられたアクションを実行できるようにします。
disabled	ポリシーをディセーブルにします（ポリシーが存在しないかのように、ポリシーの機能が無効になります）。
inactive	トラフィックがポリシーのしきい値を超えた場合に、割り当てられたアクションをポリシーが実行するのを禁止します。

次の例は、ポリシー状態を設定する方法を示しています。

```
user@GUARD-conf-zone-scannet-policy-/dns_tcp/53/analysis/syns# state disabled
```

次の例は、すべてのグローバル ポリシーの状態を設定する方法を示しています。

```
user@GUARD-conf-zone-scannet-policy-/*/*/*/global# state notify
```

注意　ゾーン ポリシーを非アクティブまたはディセーブルにすると、非アクティブなポリシーが提供していた保護機能をアクティブなゾーン ポリシーが引き継がないことがあり、ゾーン保護に支障をきたすおそれがあります。

ゾーン ポリシーをディセーブルにした後でポリシー構築フェーズを実行すると、現在のトラフィック フローに応じてすべてのゾーン ポリシーが再設定され、ポリシーが再度アクティブになることがあります。

ポリシーのしきい値の設定

ポリシーのしきい値は、特定のポリシーのしきい値トラフィック レートを定義するもので、しきい値調整フェーズで調整されます。しきい値は、デフォルトで、オンデマンド保護に適した値に設定されています。このしきい値を超過すると、ポリシーはゾーンを保護するアクションを実行します。

しきい値は、次のポリシー テンプレートで構築されたポリシーを除き、パケット / 秒またはパケット / 時で測定されます。

- num_sources：しきい値は IP アドレスまたはポートの数で測定されます。
- tcp_connections：しきい値は接続の数で測定されます。
- tcp_ratio：しきい値は比率値で測定されます。

ポリシーのしきい値は、次の方法で設定できます。

- しきい値を設定する：ポリシーのしきい値の値を設定できます。P.8-17 の「ポリシーのしきい値の設定」を参照してください。
- しきい値を乗算する：Guard モジュールは、現在のポリシーのしきい値に係数を掛けます。新しい値を固定値として設定しない場合、後続のしきい値調整フェーズでこの値が変更されることがあります。P.8-19 の「係数によるしきい値の乗算」を参照してください。
- 特定の IP しきい値を設定する：Guard モジュールは、ゾーン アドレス範囲内で、特定の IP 送信元アドレスのしきい値を設定します。P.8-19 の「特定の IP しきい値の設定」を参照してください。

- プロキシのしきい値を設定する：Guard モジュールは、プロキシを介して HTTP でゾーンに接続するクライアントのトラフィックのしきい値を設定します。P.8-20 の「プロキシしきい値の設定」を参照してください。

ポリシーのしきい値は、しきい値調整フェーズをさらに実行すると変更される場合があります。後続のしきい値調整フェーズでしきい値が変更されるかどうかは、次の方法で指定できます。

- しきい値を固定値として設定する：Guard モジュールは、以後のしきい値調整フェーズで、ポリシーのしきい値（proxy-threshold および threshold-list）の値を変更しません。P.8-17 の「固定値としてのしきい値の設定」を参照してください。
- ポリシーのしきい値に固定乗数を設定する：Guard モジュールは、以降のしきい値調整フェーズで、現在のポリシーのしきい値、ラーニングしたしきい値、および固定乗数に基づいてポリシーのしきい値を計算します。P.8-18 の「しきい値の乗数の設定」を参照してください。

この項では、次のトピックについて取り上げます。

ポリシーのしきい値の設定

ポリシーのしきい値を設定するには、ポリシー設定モードで次のコマンドを使用します。

threshold *threshold*

threshold 引数は、ポリシーのしきい値を指定する正数です。

次の例は、ポリシー policy dns_tcp/53/analysis/syns/global のしきい値を 300 に設定する方法を示しています。

```
user@GUARD-conf-zone-scannet-policy-/dns_tcp/53/analysis/syns/global# threshold 300
```

固定値としてのしきい値の設定

ポリシーのしきい値（proxy-threshold および threshold-list）を固定値として設定できます。Guard モジュールは、ラーニング プロセスのしきい値調整フェーズで新しいしきい値を無視し、現在のしきい値を保持します。しきい値を固定値として設定することにより、特定のポリシーのしきい値は手動で設定するが他のポリシーのしきい値は引き続きラーニングするということが可能になります。

ポリシーのしきい値を固定値として設定するには、ポリシー設定モードで次のコマンドを使用します。

learning-params fixed-threshold

次の例は、ポリシー policy dns_tcp/53/analysis/syns/global のしきい値を固定値として設定する方法を示しています。

```
user@GUARD-conf-zone-scannet-policy-/dns_tcp/53/analysis/syns/global# learning-params
fixed-threshold
```

ゾーン設定モードで次のコマンドを入力すると、1 つのコマンドで複数のポリシーのしきい値を固定値として設定できます。ゾーン設定モードでポリシーのしきい値を固定値として設定するには、次のコマンドを使用します。

policy *policy-path* **learning-params fixed-threshold**

policy-path 引数には、ポリシー パスを指定します。パスは、ポリシー セクションの一部のみを含む部分パスでもかまいません。詳細については、P.8-2 の「ゾーン ポリシーについて」を参照してください。

次の例は、ポリシー テンプレート dns_tcp から作成されたすべてのポリシーのしきい値を固定値にする方法を示しています。

```
user@GUARD-conf-zone-scannet# policy dns_tcp learning-params fixed-threshold
```

ポリシーのラーニング パラメータを表示するには、ポリシー設定モードで **show learning-params** コマンドを使用するか、ゾーン設定モードで **show policies** *policy-path* **learning-params** コマンドを使用します。

しきい値の乗数の設定

ポリシーのしきい値の乗数を設定できます。Guard モジュールは、以後のしきい値調整フェーズの結果を受け入れる前に、指定された乗数をラーニングしたしきい値に掛けて新しいポリシーのしきい値を計算します。Guard モジュールは、設定されているしきい値選択方式を使用して、しきい値調整フェーズの結果を受け入れます。P.9-12 の「しきい値選択方式の設定」を参照してください。

ポリシーのしきい値の乗数を設定するには、ゾーン設定モードで次のコマンドを使用します。

policy *policy-path* **learning-params threshold-multiplier** *threshold-multiplier*

表 8-11 に、**policy learning-params threshold-multiplier** コマンドの引数とキーワードを示します。

表 8-11　policy learning-params threshold-multiplier コマンドの引数とキーワード

パラメータ	説明
policy-path	しきい値を掛ける対象のポリシー パス。パスは、ポリシー セクションの一部のみを含む部分パスでもかまいません。詳細については、P.8-2 の「ゾーン ポリシーについて」を参照してください。
learning-params	ラーニング パラメータを設定します。
threshold-multiplier *threshold-multiplier*	ポリシーのしきい値を乗算します。*threshold-multiplier* は、ポリシーのしきい値に掛ける正の実数（小数点以下が 2 桁の浮動小数点型の数字）。ポリシーのしきい値を小さくするには、1 より小さい数値を入力します。

ポリシー設定モードでポリシーのしきい値の乗数を設定するには、**learning-params threshold-multiplier** *threshold-multiplier* コマンドを使用します。

次の例は、以後のしきい値調整フェーズで Guard モジュールがポリシー テンプレート dns_tcp から作成されたポリシーのしきい値を半減するように、しきい値乗数を設定する方法を示しています。

```
user@GUARD-conf-zone-scannet# policy dns_tcp learning-params threshold-multiplier 0.5
```

ポリシーのラーニング パラメータを表示するには、ポリシー設定モードで **show learning-params** コマンドを使用するか、ゾーン設定モードで **show policies** *policy-path* **learning-params** コマンドを使用します。

係数によるしきい値の乗算

ポリシーまたはポリシー グループのしきい値に係数を掛けて、トラフィック量がゾーン トラフィックを表していない場合に、ポリシーまたはポリシー グループのしきい値を増減することができます。Guard モジュールでは、ポリシーのしきい値、プロキシのしきい値、および **policy threshold-list** コマンドで定義されたしきい値の乗算をイネーブルにできます。

ポリシーのしきい値と係数を乗算するには、ゾーン設定モードで次のコマンドを使用します。

policy *policy-path* **thresh-mult** *threshold-multiply-factor*

表 8-12 に、**policy thresh-mult** コマンドの引数とキーワードを示します。

表 8-12　policy thresh-mult コマンドの引数とキーワード

パラメータ	説明
policy-path	ポリシー テンプレート名。詳細については、表 8-1 を参照してください。
thresh-mult *threshold-multiply-factor*	しきい値に掛ける正の実数（小数点以下が 4 桁の浮動小数点型の数字）を指定します。ポリシーのしきい値を小さくするには、1 より小さい数値を入力します。

次の例は、ポリシー テンプレート dns_tcp から作成されたポリシーのしきい値を半減する方法を示しています。

```
user@GUARD-conf-zone-scannet# policy */*/*/*/src_ip thresh-mult 0.5
```

（注）　しきい値は、Guard モジュールによって後続のしきい値調整フェーズで変更される場合があります。Guard モジュールがしきい値を変更しないようにするには、しきい値を固定値として設定します。P.8-17 の「固定値としてのしきい値の設定」を参照してください。

ポリシーのラーニング パラメータを表示するには、ポリシー設定モードで **show learning-params** コマンドを使用するか、ゾーン設定モードで **show policies** *policy-path* **learning-params** コマンドを使用します。

特定の IP しきい値の設定

トラフィックが大量であることがわかっている送信元または宛先 IP アドレスでトラフィックが増加するときに、Guard モジュールが誤って攻撃として検出しないようにするために、その IP アドレスに関連付けられたトラフィック用のしきい値を指定してポリシーを設定できます。

次の状況のいずれかが発生した場合は、特定の IP しきい値を設定することを考慮する必要があります。

- ある送信元 IP アドレスから大量のトラフィックがあることがわかっている場合は、特定の送信元 IP アドレスからのトラフィックに適用するしきい値を設定できる。
- 非同種ゾーン（複数の IP アドレスが定義されているゾーン）があり、そのゾーンの一部に大量のトラフィックが流れることがわかっている場合は、そのゾーン内の特定の宛先 IP アドレスに適用するしきい値を設定できる。

次のポリシーだけに、特定の IP しきい値を設定できます。

- トラフィック特性が宛先 IP（dst_ip）であるポリシー。

- デフォルトのポリシー アクションが drop である、トラフィック特性が送信元 IP アドレス（src_ip）のポリシー。デフォルトのポリシー アクションとは、新しいゾーンを作成するときに Guard モジュールがポリシーに適用するアクションのことです。これらのポリシーには、ポリシー アクションを変更する場合でも、しきい値のリストを設定できます。

特定の IP しきい値を設定するには、次のコマンドのいずれかを使用します。

- **policy** *policy-path* **threshold-list** *ip threshold* [*ip threshold* . . .]（ゾーン設定モードで使用）
- **threshold-list** *ip threshold* [*ip threshold* . . .]（ポリシー設定モードで使用）

表 8-13 に、**threshold-list** コマンドの引数を示します。

表 8-13　policy threshold-list コマンドの引数

パラメータ	説明
policy-path	ポリシー テンプレート名。詳細については、表 8-1 を参照してください。
ip	特定の IP アドレス。
threshold	しきい値トラフィック レート（パケット / 秒）。ただし、同時接続および SYN 対 FIN の比率を測定するポリシーの場合、しきい値は接続数になります。

ポリシーごとに特定の IP しきい値を 10 個まで追加できます。特定の IP しきい値をすべて 1 つのコマンドで入力できます。

Guard モジュールは、しきい値選択方式が new-thresholds に設定されている場合、以後のしきい値調整フェーズでポリシーのしきい値を変更する可能性があります。詳細については、P.9-12 の「しきい値選択方式の設定」を参照してください。

次の例は、ポリシー http/80/analysis/syns/src_ip に、IP アドレス 10.10.10.2 および 10.10.15.2 の特定の IP しきい値を設定する方法を示しています。

```
user@GUARD-conf-zone-scannet-policy-/http/80/analysis/syns/src_ip# threshold-list
10.10.10.2 500 10.10.15.2 500
```

プロキシしきい値の設定

プロキシしきい値パラメータは、プロキシを介して HTTP によりゾーンに接続するクライアントのトラフィック レートを定義し、Guard モジュールが、さまざまな送信元から送られてくるトラフィック量にポリシーを合せることができるようにします。Guard モジュールはトラフィックをブロックするためだけにプロキシしきい値を使用します。したがって、強化保護レベルの DEFAULT ゾーン テンプレートで作成されたポリシー、および基本保護レベルの TCP_NO_PROXY ゾーン テンプレートで作成されたポリシーだけにプロキシしきい値を設定できます。

プロキシしきい値は、http、http_ns、tcp_connections、および tcp_connections_ns ポリシーでのみ使用でき、ゾーンにアクティブな http または http_ns ポリシーがある場合に、tcp_connections または tcp_connections_ns ポリシー テンプレートでのみ有効です。

プロキシしきい値を設定するには、ポリシー設定モードで次のコマンドを使用します。

proxy-threshold *proxy-threshold*

proxy-threshold 引数には、http ポリシーおよび http_ns ポリシーのプロキシしきい値のトラフィック レートをパケット / 秒単位で指定します。この引数は、tcp_connections ポリシーおよび tcp_connections_ns ポリシーの接続数でプロキシしきい値を指定します。

プロキシ サーバが処理するトラフィック量はゾーンの一部であるネットワーク クライアントの処理量よりはるかに多いため、プロキシしきい値を設定する場合は、*threshold* 引数より大きな値を *proxy-threshold* 引数に設定することをお勧めします。

次の例は、ポリシー *tcp_ratio/any/basic/syn_by_fin/dst_ip_ratio* のプロキシしきい値を 20 に設定する方法を示しています。

```
user@GUARD-conf-zone-scannet-policy-/tcp_ratio/any/basic/syn_by_fin/dst_ip_ratio#
proxy-threshold 20
```

ポリシーのタイムアウトの設定

タイムアウト パラメータは、ポリシーによって作成される動的フィルタがアクションを適用する最小期間を定義します。タイムアウト期限が切れると、Guard モジュールは、ポリシーによって生成された動的フィルタを非アクティブにするかどうかを決定します。Guard モジュールが動的フィルタを非アクティブにしないと決定した場合、フィルタのアクティベーション タイムアウトが新たにゼロから再びカウントされます。動的フィルタの非アクティベーションの基準を変更するには、**filter-termination** コマンドを使用します。詳細については、P.7-25 の「動的フィルタの非アクティブ化」を参照してください。

ポリシーのタイムアウトを設定するには、ポリシー設定モードで次のコマンドを使用します。

timeout {**forever** | *timeout*}

表 8-14 に、**timeout** コマンドの引数とキーワードを示します。

表 8-14　timeout コマンドの引数とキーワード

パラメータ	説明
forever	無限の期間を示します。
timeout	ポリシーによって生成される動的フィルタがアクティブである最小期間を秒単位指定する 1 ～ 3,000,000 の整数。パケット / 秒単位でトラフィック レートを測定するポリシーの場合、デフォルトは 600 秒です。パケット / 時単位でトラフィック レートを測定するポリシーの場合、デフォルトは 3600 秒（1 時間）です。

次の例は、ポリシー http/80/analysis/syns/src_ip のタイムアウトを 100 秒に設定する方法を示しています。

```
user@GUARD-conf-zone-scannet-policy-/http/80/analysis/syns/src_ip# timeout 100
```

ポリシー グループのタイムアウトを同時に変更するには、ゾーン設定モードで **policy set-timeout** コマンドを使用します。

次の例は、HTTP ポリシー テンプレートから作成されたすべてのポリシーのタイムアウトを 100 秒に設定し、送信元 IP アドレスを測定する方法を示しています。

```
user@GUARD-conf-zone-scannet# policy http/*/*/*/src_ip set-timeout 100
```

ポリシー アクションの設定

アクション パラメータは、しきい値を超過したときにポリシーが実行するアクションのタイプを定義します。

ポリシー アクションは、ポリシーに定義されている保護を強化するように設定してください。たとえば、分析保護レベルのポリシーにはポリシー アクションを to-user-filters に設定したり、強化保護レベルのポリシーにはポリシー アクションを filter/drop に設定します。ポリシーに定義されている

保護を低下させるようなポリシー アクションを設定しないでください。たとえば、基本保護レベルまたは強化保護レベルのポリシーに、ポリシー アクションを to-user-filters に設定してはいけません。

ポリシー アクションを設定するには、ポリシー設定モードで次のコマンドを使用します。

action *policy-action*

表 8-15 に、ポリシー アクションを示します。

表 8-15　ポリシーのアクション

ポリシーのアクション	説明
block-unauthenticated	事前ハンドシェイクなしの ACK など、スプーフィング防止機能に認証されなかったトラフィックをブロックするフィルタを追加します。 このポリシー アクションは、パケット タイプが in_unauth_pkts および unauth_pkts のポリシーにのみ設定します。
filter/strong	トラフィック フローに強化保護レベルを適用するフィルタを追加します。 このポリシー アクションは、分析保護レベルおよび基本保護レベルのポリシーに設定します。このポリシー アクションは、トラフィック特性が src_ip の TCP（着信）ポリシーにのみ使用し、トラフィック特性がグローバルのポリシーには使用しないことをお勧めします。これは、ロード バランサまたは ACL[1] を使用してトラフィックを管理しているネットワークでは、このポリシー アクションがネットワーク問題を引き起こす可能性があるためです。
to-user-filters	トラフィックをユーザ フィルタに転送するフィルタを追加します。 このポリシー アクションは、分析保護レベルのポリシーに設定します。
filter/drop	指定されたトラフィックをドロップするように Guard モジュールに指示するフィルタを追加します。 このポリシー アクションは、Guard モジュールがスプーフィング防止機能を適用した後、トラフィックを監視するポリシーに設定します（基本保護レベルおよび強化保護レベルのポリシー）。このポリシー アクションは、分析保護レベルのポリシーには使用しないことをお勧めします。これは、スプーフィング攻撃を軽減するときに、このアクションによって Guard モジュールが Guard モジュールのフィルタをすべて使用してしまうおそれがあるためです。
redirect/zombie	redirect というアクションを持つすべてのユーザ フィルタの認証機能を強化するフィルタを追加します。 このポリシー アクションは、tcp_connections/any/basic/num_sources/global ポリシーにのみ適用されます。
notify	しきい値を超過した場合に通知します。

1. ACL = Access Control List

次の例は、ポリシー http/80/analysis/syns/src_ip にアクションを設定する方法を示しています。

```
user@GUARD-conf-zone-scannet-policy-/http/80/analysis/syns/src_ip# action drop
```

ポリシー グループのアクションを同時に変更するには、ゾーン設定モードで **policy set-action** コマンドを使用します。

（注）　すべてのアクションがすべてのポリシーで有効なわけではありません。特定のポリシーに有効ではないアクションに対するポリシーのアクションを変更すると、Guard モジュールはエラー メッセージを表示します。

次の例は、すべての dns_tcp ポリシーにアクションを設定する方法を示しています。

```
user@GUARD-conf-zone-scannet# policy dns_tcp/ set-action filter/drop
set action of dns_tcp/ to filter/drop:
16 policy actions set.
```

PPH ポリシーの検出時間パラメータの設定

検出時間のパラメータでは、PPH ポリシーが平均パケット レートを計算する期間を定義します。PPH ポリシーは、ゾーン トラフィックの低レート ゾンビ攻撃を監視し、パケット / 秒単位ではなくパケット / 時単位でトラフィック レートを測定します（「ゾーン ポリシーについて」の項を参照）。

悪意のあるトラフィックと正当なトラフィックを識別するために長いサンプリング期間が必要な場合は、検出時間を長くすることができます。たとえば、1 時間の期間中に正当なユーザと攻撃者が同じ数のパケットを送信することがあります。ただし、2 時間の期間では、正当なユーザがトラフィックの送信を停止してトラフィック レートが低くなる一方、執拗な攻撃者のトラフィック レートは高いままであることがあります。

PPH ポリシーのポリシー パスには、_pph が追加されたパケット タイプ ID が含まれます（たとえば、syns_pph）。ポリシー パスの詳細については、「ポリシー パスについて」の項を参照してください。

検出時間のパラメータを設定するには、次のいずれかのコマンドを使用します。

- **policy** *policy-path* **detection-time** *detection-time-int*：このコマンドはゾーン設定モードで使用します。
- **detection-time** *detection-time-int*：このコマンドはポリシー設定モードで使用します。

detection-time-int 引数には、検出時間を時間単位で指定します。1 ～ 48 の値を入力します。デフォルトは 1 です。

次の例は、ポリシー policy tcps_services/any/strong/reqs_pph/src_ip の検出時間を 8 時間に設定する方法を示しています。

```
user@GUARD-conf-zone-scannet-policy-/tcp_services/any/strong/reqs_pph/src_ip#
detection-time 8
```

ポリシーのインタラクティブ ステータスの設定

インタラクティブ ステータスのパラメータは、ポリシーによって作成される保留動的フィルタのインタラクティブ ステータスを定義します。インタラクティブ ステータスは、ゾーン保護がイネーブルになっていて、ゾーンがインタラクティブ保護モードになっている場合にのみ、ゾーンに適用されます。詳細については、第 11 章「インタラクティブ保護モードの使用方法」を参照してください。

ポリシーによって作成された保留動的フィルタのステータスを、推奨事項のインタラクティブ ステータスに設定した後で、**always-accept** または **always-ignore** に変更するには、**interactive-status** コマンドを使用します。

たとえば、推奨事項のステータスを **always-accept** に設定すると、推奨事項と推奨事項の保留動的フィルタが表示されなくなります。推奨事項または推奨事項によって生成される保留動的フィルタを無視するには、ポリシーのインタラクティブ ステータスを **interactive** または **always-ignore** に変更します。

ポリシー インタラクティブ ステータスを設定するには、ポリシー設定モードで次のコマンドを使用します。

interactive-status {**always-ignore** | **always-accept** | **interactive**}

表 8-16 に、**interactive-status** コマンドのキーワードを示します。

表 8-16　interactive-status コマンドのキーワード

パラメータ	説明
always-accept	ポリシーによって生成される動的フィルタを自動的に受け入れます。このアクションは、ポリシーによって新しい推奨事項が生成されるたびに、自動的に適用されます。 推奨事項は表示されません。
always-ignore	ポリシーによって生成される動的フィルタを自動的に無視します。しきい値を超過しても、ポリシーによって推奨事項が生成されません。 推奨事項は表示されません。
interactive	ポリシーによって生成される動的フィルタを受け入れるか無視するか、ユーザの決定を待ちます。 動的フィルタが推奨事項の一部として表示されます。

次の例は、ポリシー dns_tcp/53/analysis/pkts/src_ip のインタラクティブ ステータスを always-accept に設定する方法を示しています。

```
user@GUARD-conf-zone-scannet-policy-/dns_tcp/53/analysis/pkts/src_ip#
interactive-status always-accept
```

ポリシーの監視

ポリシーを監視して、ポリシーがゾーンのトラフィック量やサービスにどの程度適しているかを確認できます。

この項では、次のトピックについて取り上げます。

- ポリシーの表示
- ポリシーの統計情報の表示

ポリシーの表示

ゾーンのポリシーを表示して、ポリシーがゾーンのトラフィック特性に適しているかどうかを確認できます。ゾーンに構築されたポリシーを表示して、これらのポリシーがゾーンのトラフィックの特性に合せてカスタマイズされていることを確認できます。このリストに表示されるポリシーだけを設定できます。

Guard モジュールは、現在のゾーン ポリシーだけを表示します。ポリシー構築フェーズ中にポリシー テンプレートがディセーブルになっていた場合、Guard モジュールはそのポリシー テンプレートからポリシーを作成しないため、**show policies** コマンドを入力してもポリシーは表示されません。

ゾーン ポリシーを表示するには、ゾーン設定モードで次のコマンドを使用します。

show policies *policy-path*

policy-path 引数には、ポリシー グループを指定します。各ポリシー パス セクションでは、ワイルドカードとしてアスタリスク（*）を使用できます。ポリシー パス セクションを指定しなかった場合、指定していないセクションは Guard モジュールによってワイルドカード（*）と見なされます。たとえば、tcp_services//analysis//global ポリシーでは、サービスとパケット タイプのセクションにワイルドカードが使用されています。

すべてのポリシーの統計情報を表示するには、ポリシー パスにアスタリスク（*）を入力します。

ポリシー パス セクションの詳細については、P.8-2 の「ゾーン ポリシーについて」を参照してください。

次の例は、すべてのゾーン ポリシーを表示する方法を示しています。

```
user@GUARD-conf-zone-scannet# show policies *
```

次の例は、ポート 53 で DNS-over-TCP 同期パケットを監視するすべてのポリシーを表示する方法を示しています。

```
user@GUARD-conf-zone-scannet# show policies dns_tcp/53/*/syns/*
```

表 8-17 に、**show policies** コマンド出力のフィールドを示します。

表 8-17　show policies コマンド出力のフィールドの説明

フィールド	説明
Policy	ポリシー名。ポリシー パス セクションの詳細については、P.8-2 の「ゾーン ポリシーについて」を参照してください。
State	ポリシーの状態。詳細については、P.8-15 の「ポリシーの状態の変更」を参照してください。 act は active、inact は inactive、disab は disabled を指します。

表 8-17　show policies コマンド出力のフィールドの説明（続き）

フィールド	説明
IStatus	ポリシーのインタラクティブ ステータス。詳細については、P.8-23 の「ポリシーのインタラクティブ ステータスの設定」を参照してください。 a-accept は always-accept、a-ignor は always-ignore、interac は interactive を指します。
Threshold	ポリシーのしきい値。このしきい値を超過すると、Guard モジュールはアクションを実行してゾーンを保護します。詳細については、P.8-16 の「ポリシーのしきい値の設定」を参照してください。
Proxy	ポリシーのプロキシしきい値。詳細については、P.8-20 の「プロキシしきい値の設定」を参照してください。
List	ポリシーに定義されている特定の IP しきい値の数。詳細については、P.8-19 の「特定の IP しきい値の設定」を参照してください。
Action	しきい値が超過した場合にポリシーが実行するアクション。詳細については、P.8-21 の「ポリシー アクションの設定」を参照してください。
Timeout	ポリシーのアクションが有効な最小期間。Guard モジュールは、ポリシーによって作成された動的フィルタを非アクティブにするかどうかを、filter-termination しきい値に従って決定します。詳細については、P.8-21 の「ポリシーのタイムアウトの設定」を参照してください。

ポリシーの統計情報の表示

1 つのゾーン ポリシーまたはゾーン ポリシーのグループを通過するトラフィックのレートを表示したり、サービスタイプおよびボリュームがゾーン トラフィックを表すかどうかを判断したりすることができます。Guard モジュールは、ゾーンに転送されたトラフィック フローの中で、ポリシーによって測定された最も高いレートを持ついくつかのトラフィック フローを表示します。レートは、トラフィックのサンプルに基づいて計算されます。

ポリシーの統計情報を表示するには、ゾーン設定モードで次のコマンドを使用します。

show policies *policy-path* **statistics** [*num-entries*]

表 8-18 に、**show policies statistics** コマンド出力の引数を示します。

表 8-18　show policies statistics コマンドの引数

パラメータ	説明
policy-path	統計情報を表示するポリシーのグループ。 各ポリシー パス セクションでは、ワイルドカード文字としてアスタリスク（*）を使用できます。ポリシー パス セクションを指定しないと、指定していないセクションが Guard モジュールによってワイルドカード（*）と見なされます。たとえば、tcp_services//analysis//global ポリシーでは、サービスとパケット タイプのセクションにワイルドカードが使用されています。 すべてのポリシーの統計情報を表示するには、ポリシー パスにアスタリスク（*）を入力します。 ポリシー パス セクションの詳細については、P.8-2 の「ゾーン ポリシーについて」を参照してください。
num-entries	（オプション）表示するエントリの数。1 ～ 100 の数字を入力します。Guard モジュールは、最大の値を持つポリシーを表示します。

次の例は、すべてのゾーン ポリシーの統計情報を表示する方法を示しています。

```
user@GUARD-conf-zone-scannet# show policies * statistics
```

次の例は、ポート 53 で DNS-over-TCP 同期パケットを監視するすべてのポリシーの統計情報を表示する方法を示しています。

```
user@GUARD-conf-zone-scannet# show policies dns_tcp/53/*/syns/*
```

次の例は、ゾーンのグローバル トラフィックの統計情報を表示する方法を示しています。

```
user@GUARD-conf-zone-scannet# show policies */*/*/*/global statistics
```

表 8-19 に、**show policies statistics** コマンド出力テーブルのフィールドを示します。Guard モジュールは出力をソートし、4 つのテーブル Rates、Rates (pph)、Connections、および Ratios に出力を表示します。各テーブルの情報は値によってソートされ、テーブルの一番上に最大値が表示されます。テーブルに何も情報が含まれていない場合、Guard モジュールはそのテーブルを表示しません。

表 8-19　show policies statistics コマンド出力テーブルのフィールドの説明

カラム	説明
Key	キー（ポリシーの集約に使用されたトラフィック特性）。 たとえば、tcp_services/any/analysis/syns/dst_ip ポリシーの場合、キーは宛先 IP アドレス（dst_ip）です。ポリシーの集約に使用されたトラフィック特性が global である場合、キーには N/A と表示されます。詳細については、表 8-8 を参照してください。
Policy	ポリシー名。詳細については、P.8-2 の「ゾーン ポリシーについて」を参照してください。
Rate	トラフィック レートをパケット / 秒（pps）単位で測定するポリシーによって確認されたトラフィック レート。
Rate (pph)	トラフィック レートをパケット / 時（pph）単位で測定するポリシーによって確認されたトラフィック レート。攻撃の最初の 1 時間を過ぎてからコマンドを入力すると、Guard モジュールは、過去 2 時間の平均パケット / 時レートを表示します。 このフィールドは、PPH ポリシーをイネーブルにした場合にだけ表示されます。デフォルトでは、PPH ポリシーはディセーブルになっています（「ポリシーの状態の変更」の項を参照）。
Connections	同時接続の数。 この情報は、tcp_connections ポリシーおよび次のパケット タイプについてのみ表示されます。 • in_conns：強化保護レベル用 • in_nodata_conns：分析保護レベル用
Ratio	SYN フラグの付いたパケット数と FIN/RST フラグの付いたパケット数の比率。この情報は、syn_by_fin ポリシーでのみ使用できます。

ポリシー設定のバックアップ

現在のゾーン ポリシーは、ゾーン設定モードで **snapshot threshold-selection cur-thresholds** コマンドを使用していつでもバックアップできます。

次の例は、現在のポリシー設定をバックアップするために、スナップショットを作成する方法を示しています。

```
user@GUARD-conf-zone-scannet# snapshot threshold-selection cur-thresholds
```