CHAPTER 7

ポリシー テンプレートとポリシーの設定

この章では、Cisco Traffic Anomaly Detector（Detector 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。

この章には、Detector モジュールの関連製品である Cisco Guard（Guard）についての記述があります。Guard は、DDoS 攻撃（分散型サービス拒絶攻撃）を検出して軽減するデバイスです。Guard は、ゾーン トラフィックが通過する際に攻撃トラフィックをドロップして正常なトラフィックをネットワークに戻し、ゾーン トラフィックをクリーンにします。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できます。また、Detector モジュールは Guard とゾーン設定を同期させることができます。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。

ゾーン ポリシーについて

Detector 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。
- 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 フローがポリシーのしきい値を超え、悪意のあるトラフィックまたは異常なトラフィックであることを示した場合に、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ています。フローがポリシーのしきい値を超えると、ポリシーはフィルタ（動的フィルタ）セットを動的に設定して、イベントを自身の syslog に記録するか、リモート Guard リストで定義した Guard をアクティブにします。Guard は、アクティブになると、攻撃を軽減してゾーンを保護します。

各ゾーン設定には、ポリシーのセットが含まれています。事前定義されたゾーン テンプレートを使用して新しいゾーンを作成する場合、Detector 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、Detector 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、Detector 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）。Detector 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。Detector 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。Detector モジュールがゾーン ポリシーを作成および調整を行ったら、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 フローを定義している場合、Detector 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 テンプレートについて

ポリシー テンプレートとは、Detector 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 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場合、Detector モジュールのゾーン設定には一連のポリシー テンプレートが用意されています。

この項では、次のトピックについて取り上げます。

- 各種ポリシー テンプレートのタイプについて
- ポリシー テンプレート パラメータの設定

各種ポリシー テンプレートのタイプについて

表 7-1 で、Detector 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。DETECTOR_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場合、Detector モジュールには次のポリシー テンプレートが用意されています。

表 7-1　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、Detector 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。

表 7-1　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
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、Detector 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	Detector 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。
tcp_ratio	異なるタイプの TCP パケット間の比率（たとえば、SYN パケットと FIN/RST パケットの比率）。
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。
udp_services	UDP サービス。

Detector 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 7-2 に、特定のゾーン テンプレートに基づいて Detector 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 7-2　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
DETECTOR_WORM	worm_tcp：TCP ワームを特定するポリシーのグループを構築します。TCP ポリシーは、ワーム攻撃を管理します。この攻撃では、1 つまたは複数の送信元 IP アドレスから、多数の宛先 IP アドレスに対する多数の未確立の接続が同一ポート上に作成されます。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。 Detector モジュールは、ポリシー構築フェーズではなく、ラーニング プロセスのしきい値調整フェーズで、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 パラメータの 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。詳細については、P.7-23 の「ワーム ポリシーについて」を参照してください。

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。Detector モジュールは、表 7-3 に示すポリシー テンプレートを使用して tcp_connections と tcp_outgoing のポリシー テンプレートを http_ns、

tcp_connections_ns および tcp_outgoing_ns policies 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 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 7-3 に、Detector 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 7-3　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。

ポリシー テンプレート パラメータの設定

ラーニング プロセス中、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。Detector 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 Detector 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。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、*any* というサービスを備えた追加のポリシーを作成するものもあります。

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：Detector 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：Detector 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 : Detector 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 パラメータである、サービスの最大数と最小しきい値は、worm_tcp ポリシー テンプレートには影響しません。

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 7-1 を参照してください。

このコマンドを実行すると、Detector モジュールはポリシー テンプレート設定モードに入ります。

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@DETECTOR-conf-zone-scannet# policy-template http
user@DETECTOR-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
- 最小しきい値の設定
- ポリシー テンプレートの状態の設定
- すべてのポリシー テンプレート パラメータの同時設定

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。Detector モジュールは、各サービスのトラフィック量のレベルによってサービスをランク付けします。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。Detector 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 Detector 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。

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 Detector 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、Detector 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、Detector 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@DETECTOR-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、Detector 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異常検出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_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@DETECTOR-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。Detector モジュールが、ディセーブルになっているポリシー テンプレートをポリシー構築フェーズ中に使用してポリシーを作成することはできません。

注意　ポリシー テンプレートをディセーブルにすると、ゾーン異常検出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、Detector モジュールはそのポリシー テンプレートに関連するゾーン トラフィックを検出できません。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、Detector 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@DETECTOR-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 7-4 に、**policy-template** コマンドの引数とキーワードを示します。

表 7-4　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 7-5 を参照してください。
max-services	Detector 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。 Detector 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.7-6 の「サービスの最大数の設定」を参照してください。
min-threshold	Detector 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。 Detector 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.7-7 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.7-7 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.7-7 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@DETECTOR-conf-zone-scannet# policy-template tcp_services 3 -1 enabled
```

ポリシー パスについて

ポリシーの名前はセクションで構成されており、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、Detector モジュールの分析検出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 7-1 に、ゾーン ポリシー名の例を示します。

図 7-1　ポリシー名

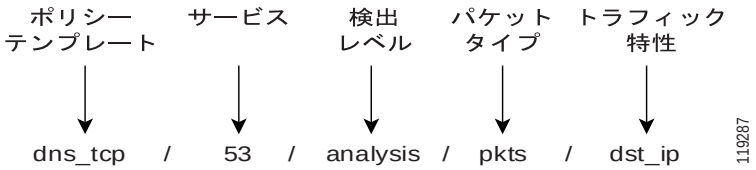

表 7-5 に、ポリシー名のセクションを示します。

表 7-5　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 攻撃の脅威の検出のために Detector 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.7-3 の「ポリシー テンプレートについて」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。
検出レベル	Detector モジュールがトラフィック フローに適用する Detect レベル。Detect 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。
パケット タイプ	Detector 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	Detector 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、検出レベル、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
- Detector モジュールが監視するパケット タイプについて
- Detector 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 フローを定義している場合、Detector 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異常検出にするために、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　Detector 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 ポリシーへのサービスの追加またはゾーン ポリシーからのサービスの削除を行うと、Detector モジュールはそのゾーン ポリシーに未調整のマークを付けます。ゾーン異常検出とラーニング 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、Detector 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.8-8 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.8-12 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.8-8 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、tcp_services_ns、または worm_tcp

  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の場合。
- **policy-template** *policy-template-name* **add-service** *service-num*：ゾーン設定モードの場合。

表 7-6 に、**add-service** コマンドの引数を示します。

表 7-6　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 7-1 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@DETECTOR-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。Detector 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*：このコマンドはポリシー テンプレート設定モードで使用します。
- **policy-template** *policy-template-name* **remove-service** *service-num*：このコマンドはゾーン設定モードで使用します。

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

表 7-7　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 7-1 を参照してください。

注意　サービスを削除すると、Detector 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、ゾーン異常検出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アクティブにすると、同じサービスが再度追加される場合があります。

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

Detector モジュールが監視するパケット タイプについて

Detector 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、Detector モジュールが TCP ハンドシェイクを実行してパケット接続をすでに確認しているパケットのこと）
- パケット方向（着信接続など）

表 7-8 で、Detector 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 7-8　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。
non_estb_conns	未確立の接続。失敗したゾーンの着信接続。応答が受信されなかった TCP 接続要求（SYN パケット）です。
out_pkts	ゾーンの着信 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。

表 7-8　パケット タイプ（続き）

パケット タイプ	説明
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。Detector 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	同じ検出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。

Detector 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。

/53/analysis/pkts/dst_ip and /53/analysis/pkts/src_ip

表 7-9 に、Detector モジュールが監視するトラフィック特性を示します。

表 7-9　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。
scanners	特定の宛先ポート上でゾーン宛先 IP アドレスをスキャンする送信元 IP アドレスの数のヒストグラム。詳細については、P.7-23 の「ワーム ポリシーについて」を参照してください。
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 プロセスが完了したら、特定のポリシー パラメータ（ポリシーの状態、ポリシーのしきい値、ポリシーのタイムアウト、ポリシーのアクション、およびポリシーのインタラクティブ状態）を表示し、そのポリシー パラメータがゾーン トラフィックに適してい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。

ポリシー パラメータの設定を表示するには、ポリシー設定モードで次のコマンドを使用します。

show

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。詳細については、P.7-2 の「ゾーン ポリシーについて」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、/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@DETECTOR-conf-zone-scannet# policy /53/analysis/syns/global
user@DETECTOR-conf-zone-scannet-policy-//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 Detector 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、Detector 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」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
- ポリシーのアクションの設定
- 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）　Detector 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、ゾーン異常検出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**}

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

注意　ポリシーを非アクティブまたはディセーブルにすると、ゾーン ポリシーが機能しなくなるおそれがあります。そのため、ゾーン異常検出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。このしきい値を超過すると、ポリシーはポリシー アクションによって定義された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 / 秒で測定されます。

- num_soruces：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。
- worm_tcp：しきい値は、送信元 IP からスキャンできるゾーン宛先 IP アドレスの最大数として測定されます。

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.7-17 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：Detector 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.7-18 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：Detector 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.7-19 の「特定の IP 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：Detector 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.7-17 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：Detector 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.7-17 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 /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@DETECTOR-conf-zone-scannet-policy-//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。Detector 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 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@DETECTOR-conf-zone-scannet-policy-//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.7-2 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@DETECTOR-conf-zone-scannet# policy 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。Detector 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。Detector 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.8-12 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 7-10 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 7-10　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.7-2 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 Detector モジュールがポリシー テンプレート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@DETECTOR-conf-zone-scannet# policy  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。Detector 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 7-11 に、**policy thresh-mult** コマンドの引数とキーワードを示します。

表 7-11　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 7-1 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@DETECTOR-conf-zone-scannet# policy */*/*/*/src_ip thresh-mult 0.5
```

（注）　Detector モジュールは、後続のしきい値調整フェーズでしきい値を変更する場合があります。Detector 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.7-17 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したときに Detector モジュールが誤って攻撃として検出するのを防ぐには、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持つポリシーを設定します。

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 アドレスで構成されるゾーン）があり、そのゾーンの一部にのみ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 アドレスを対象とするトラフィックに適用するしきい値を設定できる。

宛先 IP（dest_ip）というトラフィック特性を持つポリシーだけに、特定の IP しきい値を設定できます。

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 ...*]：このコマンドはゾーン設定モードで使用します。
- **threshold-list** *ip threshold* [*ip threshold ...*]：このコマンドはポリシー設定モードで使用します。

表 7-12 に、**threshold-list** コマンドの引数を示します。

表 7-12　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 7-1 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。

Detector 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.8-12 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@DETECTOR-conf-zone-scannet-policy-/http/80/analysis/syns/src_ip# threshold-list
10.10.10.2 500 10.10.15.2 500
```

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。

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 7-13 に、**timeout** コマンドの引数とキーワードを示します。

表 7-13　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。

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

ポリシーのアクションの設定

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 7-14 に、ポリシー アクションを示します。

表 7-14　ポリシーのアクション

ポリシーのアクション	説明
notify	しきい値を超過した場合に通知します。
remote-activate	しきい値超過が発生すると、リモート Guard をアクティブにします。リモート Guard はリモート Guard リストに定義されています。詳細については、P.9-6 の「ゾーンを保護するためのリモート Guard のアクティブ化」を参照してください。

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@DETECTOR-conf-zone-scannet-policy-/http/80/analysis/syns/src_ip# action
remote-activate
```

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。

次の例は、すべての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@DETECTOR-conf-zone-scannet# policy / set-action remote-activate
set action of / to remote-activate:
4 policy actions set.
```

PPH ポリシーの検出時間パラメータの設定

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）。検出時間のパラメータでは、ポリシーがトラフィック レートを特定するためにパケットをカウントする期間（時間単位）を定義します。

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@DETECTOR-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、ゾーン異常検出がイネーブルになっていて、ゾーンがインタラクティブ検出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 10 章「インタラクティブ検出モードの使用方法」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-accept** | **always-ignore** | **interactive**}

表 7-15 に、**interactive-status** コマンドのキーワードを示します。

表 7-15　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。 Detector モジュールはこのような動的フィルタを推奨事項の一部として表示します。

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

ワーム ポリシーについて

インターネット ワームは、自動化された、自己伝搬する侵入性のエージェントであり、自身のコピーを作成して容易に配布します。ワームは、脆弱なホストを攻撃して感染させた後、そのホストを基点として他の脆弱なターゲットを攻撃します。次に、ネットワーク検査形式（一般的にはスキャン）を使用して他のターゲットを探し、次のターゲットに伝搬します。スキャニング ワームは、脆弱なホストを見つけるために、探索するアドレスのリストを生成し、その後ホストにアクセスします。Code Red ワーム、Sasser ワーム、Blaster ワーム、および Slammer ワームはすべて、この方法で蔓延する知名度の高いワームの例です。

Detector モジュールは、ゾーン ネットワークがスキャンされていることを示す、異常なトラフィック パターンを通じてワームを識別することで TCP ワーム攻撃を検出することができます。Detector モジュールは、TCP ワーム攻撃が進行中でない場合であっても、ネットワークにはスキャナーが存在する場合があると想定しています。このモジュールは、特定のポート上で、多くのゾーン宛先 IP アドレスに対する未確立の接続（SYN/ACK 応答パケットが識別されなかった着信 SYN パケット）の開始側である送信元 IP アドレスを、スキャナーとして識別します。

ゾーン トラフィックを分析するために、Detector モジュールは周波数データが含まれたテーブルを使用します。このテーブルはネットワーク スキャナーのヒストグラムとして知られています。Detector モジュールは、最初に、攻撃が進行中でないときにゾーンのネットワークをラーニングし、次に同時スキャナーのヒストグラムを作成します。ヒストグラムには、特定の数のゾーン宛先 IP アドレスを同時にスキャンするスキャナーの数が記載されます。Detector モジュールは、特定の数より多くのゾーン宛先 IP アドレスにアクセスするスキャナーの数を測定します。

Detector モジュールは、次の 2 つのタイプのしきい値を使用して、ワームのトラフィック特性を分析します。

- スキャニングしきい値：単一の送信元 IP アドレスからスキャンできるゾーン IP アドレスの最大数を定義します。このしきい値は、ポリシーのしきい値によって定義されます。
- ヒストグラムしきい値：指定された数を超えるゾーン IP アドレスをスキャンできる送信元 IP アドレスの最大数を定義します。

Detector モジュールは、攻撃が進行中でないときにラーニングしたヒストグラムとの偏差がある場合にワーム攻撃と判断します（つまり、その場合は、定義された数を超えるゾーン宛先 IP アドレスを同時にスキャンする送信元 IP アドレスの数が超過しています）。詳細については、P.7-24 の「ワーム攻撃の識別」を参照してください。

ワーム ポリシーは、次の点で、他のポリシーと異なっています。

- Detector モジュールは、ポリシー構築フェーズ中ではなく、しきい値調整フェーズ中にワーム ポリシーの新しいサービスをラーニングするため、しきい値調整フェーズ中に、ワーム ポリシーに追加された新しいサービス（ポート）が表示される場合があります。
- **any** サービスは、Detector モジュールに特定のポリシーが存在しないポートに関連付けられます。たとえば、Detector モジュールに、worm_tcp/80 と worm_tcp/50 のポリシーが存在する場合、worm_tcp/any ポリシーは、ポート 50 または 80 を宛先としないトラフィックをすべて監視します。他のポリシーとは異なり、**any** サービスは、指定されていないポートすべてに対するトラフィックを集約しません。Detector モジュールは、ゾーン トラフィックを監視するとき、スキャンされるポートごとに別個の内部ヒストグラムを保持しています。次に、このヒストグラムを **any** サービスのヒストグラムと比較します。

この項では、次のトピックについて取り上げます。

ワーム ポリシーの設定

worm_tcp ポリシー テンプレートは、DETECTOR_WORM ゾーン テンプレートだけで使用できます。

TCP ワームを管理するポリシーは、worm_tcp ポリシー テンプレート、non_estb_conns パケット タイプ、およびスキャナーのトラフィック特性から構築されます。

ポリシー設定モードで次のコマンドを入力すると、ヒストグラムを設定し、スキャニングしきい値を変更することができます。

histogram *num-dst-ips num-src-ips* [*num-dst-ips num-src-ips...*]

表 7-16 に、**histogram** コマンドの引数を示します。

表 7-16　histogram コマンドの引数

パラメータ	説明
num-dst-ips	スキャンされたゾーン宛先 IP アドレスの数。*num-dst-ips* の値は 5、20、および 100 で、システム定義になっています。*num-dst-ips* ごとに定義される *num-src-ips* の値は変更できます。
num-src-ips	ヒストグラムのしきい値。このしきい値を超過すると、ポリシーはポリシー アクション パラメータによって定義されたアクションを実行します。しきい値には、指定された数（*num-dst-ips*）のゾーン宛先 IP アドレスをスキャンできる送信元 IP アドレスの数を指定します。

ヒストグラムしきい値をすべて 1 つのコマンドで入力できます。

次の例は、すべての頻度についてヒストグラムしきい値を設定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet- worm_tcp/445/analysis/non_estb_conns/scanners#
histogram 5 99 20 80 50 8 100 1
```

現在のヒストグラム設定を表示するには、**show policies** コマンドを使用します。

単一の送信元 IP アドレスからスキャンできるゾーン IP アドレスの最大数を設定できます（スキャニングしきい値）。この数を設定するには、**threshold** コマンドを使用します。詳細については、P.7-16 の「ポリシーのしきい値の設定」を参照してください。

特定のポートのヒストグラムしきい値を指定するには、**add-service** コマンドを使用して、特定のポート番号のサービスを、*worm_tcp* ポリシー テンプレートから作成されたポリシーすべてに追加します。詳細については、P.7-10 の「サービスの追加」を参照してください。

ワーム攻撃の識別

Detector モジュールは、スキャニングしきい値とヒストグラムしきい値の 2 つのタイプのしきい値を使用して、ワームのトラフィック特性を分析します。詳細については、P.7-23 の「ワーム ポリシーについて」を参照してください。

ヒストグラムしきい値を超えると、Detector モジュールは、指定されていない送信元 IP アドレス（*）を持つ動的フィルタを作成します。この動的フィルタは、ワーム攻撃が進行中であることを示します。動的フィルタのポリシーのしきい値は、超過したヒストグラムしきい値を指定します。Detector モジュールは、動的フィルタのポリシーしきい値と等しい新しい内部のスキャニングしきい値を定義します。

ゾーン宛先 IP アドレスをスキャンする送信元 IP アドレスは、ワームに感染したホストの IP アドレスです。ゾーンが攻撃中の場合、ワームに感染した各ホストがスキャンするゾーン宛先 IP アドレスの数が、新しい内部のスキャニングしきい値によって定義された最大数を超えると、動的フィルタが作成されます。Detector モジュールは、動的フィルタのアクションによって定義されたこれらの攻撃フローに対して作用します。

たとえば、ポリシーのしきい値（スキャニングしきい値）が 300 の場合、ポート 445 に関するポリシー スキャナーのヒストグラムは表 7-17 のようになり、Detector モジュールは、350 個のゾーン宛先 IP アドレスをスキャンするスキャナーを識別した場合、マス スキャナーが検出されたことを示す動的フィルタを作成します。ただし、このスキャナーからは、ワーム攻撃が進行中かどうかはまだわかりません。

表 7-17　ヒストグラム例

Number of source IP addresses	10	5	2
Number of Destination IP addresses	5	20	100

Detector モジュールが、ポート 445 で 50 個より多くのゾーン宛先 IP アドレスを同時にスキャンする 6 個の送信元 IP アドレスを識別すると、指定されていない送信元 IP アドレス（*）を持つ動的フィルタを worm_tcp ポリシーから作成します。この動的フィルタは Detector モジュールがポート 445 に対するワーム攻撃を識別したことを示します。動的フィルタのポリシーしきい値である 50 が、新しい内部のスキャニングしきい値に指定されるため、Detector モジュールはスキャナーのしきい値定義を小さくします。この結果、Detector モジュールは新しいスキャニングしきい値（50）を超過してスキャンする送信元 IP アドレスごとに追加の動的フィルタを作成します。

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。

Detector 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、Detector 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 Detector 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.7-2 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@DETECTOR-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@DETECTOR-conf-zone-scannet# show policies dns_tcp/53/*/syns/*
```

表 7-18 に、**show policies** コマンド出力のフィールドを示します。

表 7-18　show policies コマンド出力のフィールド説明

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.7-2 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.7-15 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 7-18　show policies コマンド出力のフィールド説明（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.7-22 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。トラフィック レートがこのしきい値を超えると、Detector モジュールが、そのポリシーと関連付けられたアクションを実行します。詳細については、P.7-16 の「ポリシーのしきい値の設定」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.7-19 の「特定の IP しきい値の設定」を参照してください。ワームに関連するポリシーの場合は、ヒストグラムを表す H が表示されます。詳細については、P.7-23 の「ワーム ポリシーについて」を参照してください。
Action	トラフィックがそのポリシーのしきい値を超えた場合に Detector モジュールが実行するアクション。詳細については、P.7-20 の「ポリシーのアクションの設定」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。Detector 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.7-20 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

単一またはグループのゾーン ポリシーを通過するトラフィックのレートを表示し、サービス タイプおよびトラフィック量がゾーンのトラフィックを表すかどうかを判断できます。Detector 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 7-19 に、**show policies statistics** コマンド出力の引数を示します。

表 7-19　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 Detector 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.7-2 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。Detector 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@DETECTOR-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@DETECTOR-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@DETECTOR-conf-zone-scannet# show policies */*/*/*/global statistics
```

表 7-20 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。Detector 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、Detector モジュールはそのテーブルを表示しません。

表 7-20　show policies statistics コマンド出力テーブルのフィールド説明

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。 ワームに関連するポリシー（worm_tcp/any/analysis/non_estb_conns/scanners など）の場合、キーは、ゾーンのネットワーク アドレスをスキャンする送信元 IP アドレス、コロン、およびスキャンされている宛先ポートになります。この例では、192.128.100.3:70 と表示されます。 詳細については、表 7-8 を参照してください。
Policy	ポリシー名。詳細については、P.7-2 の「ゾーン ポリシーについて」を参照してください。

表 7-20　show policies statistics コマンド出力テーブルのフィールド説明（続き）

カラム	説明
Rate	ポリシーを通過し、パケット / 秒（pps）単位で計測されるトラフィックのレート。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。
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、Detector 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）。
Connection	同時接続の数。この情報は、パケット タイプが in_nodata_conns の tcp_connections ポリシーについてのみ表示されます。
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。
Dst IPs	スキャンされたゾーン宛先 IP アドレスの数。この情報は、worm_tcp ポリシーだけで使用できます。

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