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 Module（Detector モジュール）のポリシー、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、ポリシーおよびポリシー 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、次の項があります。

ポリシーについて

トラフィックの統計分析を実行するため、Detector には特定のタイプのトラフィックを処理する方法についての定義が含まれています。これらの定義をポリシーといいます。ポリシーは、Detector モジュール統計エンジンの構成要素です。各ゾーンには、ゾーンのトラフィック パターンに合せて調整されたポリシーのセットがあります。これらのポリシーは、悪意となる可能性のある異常をトレースするために、Detector モジュールがゾーンのトラフィックと比較する基礎となります。ポリシーは、トラフィック フローを持続的に測定し、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であると判断すると、そのフローに対してアクションを実行します。このアクションは、フローがポリシーのしきい値を超過すると発生します。

ゾーンの特定のトラフィック特性に合ったポリシーを作成するために、Detector モジュールは 2 つのフェーズのラーニング プロセスでゾーンのトラフィックをラーニングします。また、定義済みのポリシー テンプレートを使用してポリシーを構築します。各ポリシー テンプレートは、ポリシーの作成に使用され、特定の DDoS 脅威を検出するために Detector モジュールが必要とする検出面を扱います。

ポリシーの作成後、ポリシーの追加および削除、またはポリシー パラメータの変更を行うことができます。

ポリシー パス構造

Detector モジュールは、ゾーンのトラフィック フローに関する統計分析を行います。各ポリシーは、特定のトラフィック フローを測定します。ポリシーは、Detector モジュールが分析に使用する特性を定義します。ポリシー名はセクションで構成されます。各セクションは、異なるトラフィック特性に関連する異なる役割を示します。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モジュールによって認証され、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、ポリシー名の例を示します。

図 7-1　　ポリシー名

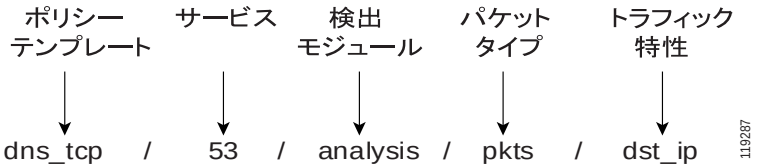

表 7-1 で、ポリシー名のセクションについて詳しく説明します。

表 7-1　　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 テンプレートを示します。各ポリシー テンプレートは、特定の DDoS 脅威を検出するために Detector モジュールが必要とする検出面を扱います。詳細については、P.7-5 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	検出ポリシーに関連するポート番号またはプロトコル番号を示します。詳細については、P.7-14 の「サービス」を参照してください。
検出モジュール	Detector モジュールがトラフィック フローの処理に使用する検出モジュールを示します。詳細については、P.7-18 の「検出モジュール」を参照してください。
パケット タイプ	Detector モジュールが監視するパケット タイプを示します。詳細については、P.7-18 の「パケット タイプ」を参照してください。
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を示します。詳細については、P.7-19 の「トラフィック特性」を参照してください。

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*、*検出モジュール*、および *パケット タイプ*）では、分析するトラフィックのタイプが定義されます。ポリシー パスの最後のセクション（*トラフィック特性*）では、フローの分析方法が定義されます。

ポリシーには、相互依存性および優先度があります。同じトラフィック フローを定義する 2 つのポリシーがある場合、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。

ポリシーの動作面を設定できます。動作面では、何がポリシーをトリガーするか、およびポリシーがアクティブになったときにポリシーが実行するアクションが定義されます。詳細については、P.7-21 の「ポリシー パラメータの設定」を参照してください。

ポリシーの作成

Detector モジュールは、ラーニング プロセスでゾーンのポリシーを作成します。ラーニング プロセスは 2 つのフェーズで構成され、これらのフェーズで Detector はゾーンのトラフィックをラーニングし、特定のゾーンのトラフィック特性に対応します。

1. **ポリシー構築フェーズ**：このフェーズでは、Detector はポリシー テンプレートを使用して、ゾーンのポリシーを構築します。トラフィックが透過的に Detector を通過し、Detector はゾーンによって使用される主なサービスを検出できます。
2. **しきい値調整フェーズ**：このフェーズでは、Detector はゾーンのサービスのトラフィック レートに合せてポリシーのしきい値を調整します。トラフィックが透過的に Detector を通過し、Detector はポリシー構築フェーズ中に検出されたサービスのしきい値を調整できます。

詳細については、P.5-12 の「ゾーン トラフィックの特性のラーニング」を参照してください。

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、ポリシー構築の規則をまとめたものです。Detector モジュールは、ポリシー構築フェーズでポリシー テンプレートを使用してゾーンのポリシーを作成します。ポリシー構築フェーズの終わりの各テンプレートの出力は、ポリシーのグループです。ポリシー テンプレートの名前は、作成されるすべてのポリシーに共通の特性に由来しています。テンプレートの名前として、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）が使用されます。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。

表 7-2 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 7-2　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。

表 7-2　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
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）。このポリシー テンプレートは、定義されたゾーンがサブネットである場合に適しています。 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 および UDP 以外のプロトコル。
port_scan	ポート 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	Detector のスプーフィング防止メカニズム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 パケットの比率に関連するものです。

表 7-2　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_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_WORM ゾーン テンプレートを使用してゾーンを定義する場合、Detector モジュールには追加のポリシー テンプレートが用意されています。

表 7-3 で、DETECTOR_WORM に関する Detector のポリシー テンプレートについて説明します。

表 7-3　DETECTOR_WORM 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
worm_tcp	TCP ワーム。このポリシーは、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。このポリシー テンプレートは、主として、IP アドレス定義がサブネットであるゾーンを対象に設計されています。 （注）　このポリシー テンプレートを使用できるのは、DETECTOR_WORM ゾーン テンプレートから作成されたゾーンに対してのみです。 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.7-32 の「ワーム ポリシーについて」を参照してください。

GUARD_TCP_NO_PROXY　ゾーン　テンプレートでゾーンを定義した場合、Detector モジュールは表 7-4 で説明されているポリシー テンプレートを使用します。Detector 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 のポリシー テンプレートでは、強力な保護メカニズムを使用することを Guard モジュールに要求するアクションを持つポリシーは作成されません。

表 7-4 で、GUARD_TCP_NO_PROXY に関する Detector のポリシーを詳しく説明します。

表 7-4　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	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 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** コマンドを入力し、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、ゾーンのトラフィックは Detector 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、ゾーンのトラフィックの特性に応じてポリシーのグループを生成します。Detector では、特定のポリシー テンプレートから Detector が生成するポリシーの最大数を定義できます。Detector は、ポリシー テンプレートに関連す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。次に、Detector は、定義済みの最小しきい値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ピックアップして、各サービスの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ていないすべてのトラフィック フローを処理するために、追加のポリシーを作成します。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。

次のポリシー テンプレート パラメータを設定できます。

- サービスの最大数の設定：Detector がポリシー テンプレートから特定のポリシーを作成するときの対象となるサービスの最大数を定義します。
- 最小しきい値の設定：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の設定：Detector モジュールがポリシー テンプレートからポリシーを生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 パラメータを設定するには、ポリシー テンプレート設定モードに入ります。次のコマンドを入力します。

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 7-2 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。

次の例を参考にしてください。

```
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。

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は、ポリシー テンプレートがピックアップしてポリシーを作成する対象となるサービスの最大数（プロトコル番号やポート番号）を定義します。Detector は、ポリシー テンプレートに関連す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。Detector 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ピックアップして、各サービスのポリシーを作成します。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が、*any* というサービスで追加されることがあります。

（注）　サービスの最大数が大きいほど、ゾーンが使用するメモリが多くなります。

このパラメータは、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。特定のサービスに関連するポリシー テンプレート（サービス 53 に関連する *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）にこのパラメータを設定することはできません。

Detector 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。このトラフィック特性とは、送信元 IP アドレス、宛先 IP アドレス、または送信元ネットです。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すべてのサービスの送信元 IP アドレスのレートを測定します。したがって、こちらの値は精度が劣ります。

サービスの数を制限すると、希望のトラフィック フロー要件に合せて Detector 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、次のコマンドを入力します。

max-services *max-services*

max-services 引数は、Detector がピックアップするサービスの最大数を定義する 2 以上の整数です。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。

次の例を参考にしてください。

```
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 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。

正しいゾーン検出に不可欠であるために常にポリシーを構築するポリシー テンプレート（tcp_services、udp_services、other_protocols、http、および fragments）に、このパラメータを設定することはできません。

このしきい値を設定すると、Detector の検出をゾーンのサービスのトラフィック量に、よりよく適合させることができます。

最小しきい値を設定するには、次のコマンドを入力します。

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（pps）を定義します。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。

次の例を参考にしてください。

```
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

このパラメータは、ポリシー テンプレートの状態を定義します。ポリシー テンプレートは、イネーブルまたはディセーブルにすることができます。ポリシー テンプレートをディセーブルにすると、Detector がポリシー構築フェーズを経ても、ポリシー テンプレートからポリシーが生成されません。

注意　ポリシー テンプレートをディセーブルにすると、Detector はポリシー テンプレートに関連する種類のトラフィックからゾーンを検出できません。このため、検出の実効性が大幅に低下する可能性があります。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 は DNS (UDP) 攻撃からゾーンを保護できなくなります。

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

すべてのポリシー テンプレート パラメータの同時設定

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。次のコマンドを入力します。

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

表 7-5 で、**policy-template** コマンドの引数とキーワードについて説明します。

表 7-5　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 7-1 を参照してください。
max-services	Detector が特定のポリシー テンプレートからポリシーをピックアップおよび構築するときの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.7-9 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.7-11 の「最小しきい値の設定」を参照してください。

表 7-5　policy-template コマンドの引数とキーワード（続き）

パラメータ	説明
disabled	ポリシー テンプレートをディセーブルにして、ポリシーが生成されないようにします。詳細については、P.7-11 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.7-11 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。サービスの最大数は *3* に設定されます。最小しきい値は変更されず（*-1*）、ポリシーの状態は **enabled** に設定されます。

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

ポリシー パスのセクションについて

ポリシー パスは、次のセクションで構成されます。

- ポリシー テンプレート（「ポリシー テンプレートについて」を参照）
- サービス
- 検出モジュール
- パケット タイプ
- トラフィック特性

サービス

サービス セクションは、ポリシーに関連するゾーン アプリケーション ポートまたはプロトコルを示します。ポリシーには、相互依存性および優先度があります。同じトラフィック フローを定義する 2 つのポリシーがある場合、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。

ゾーンの主なサービスに対して特定のポリシーを定義し、検出が最適に調整されたことを保証するようお勧めします。

注意　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。ゾーンが検出およびラーニング動作状態の場合、Detector モジュールは、ユーザによって次のアクションのいずれかが実行されるまでゾーンの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.5-18 の「しきい値の調整」を参照）。
- ゾーン ポリシーを調整済みとしてマークする（P.5-25 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
- サービスの削除

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ポリシーすべてにサービスを追加し、より限定的なポリシーを作成することができます。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ます。新しいサービスは、デフォルト値を使用して定義されます。しきい値を手動で定義することはできますが、しきい値調整フェーズを実行し（詳細については、P.5-18 の「しきい値の調整」を参照）、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。

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、worm_tcp：サービスはポート番号を指定します。
- other_protocols：サービスはプロトコル番号を指定します。

（注）　サービスの追加後にポリシー構築フェーズを実行すると、手動で追加したサービスを新しいサービスが上書きすることがあります。

次の状況において、ポリシー構築を再度実行しない場合は、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、ポリシー テンプレート設定モードで次のコマンドを入力します。

add-service *service-num*

または

ゾーン設定モードで次のコマンドを入力します。

policy-template *policy-template-name* **add-service** *service-num*

表 7-6 で、**policy-template** コマンドの引数について説明します。

表 7-6　policy-template コマンドの引数

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 7-2 を参照してください。
service-num	プロトコル番号またはポート番号。

次の例を参考にしてください。

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

サービスの削除

ポリシー テンプレートに関連する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、ポリシー テンプレート設定モードで次のコマンドを入力します。

remove-service *service-num*

または

ゾーン設定モードで次のコマンドを入力します。

policy-template *policy-template-name* **remove-service** *service-num*

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
policy-template-name	ポリシー テンプレート名。詳細については、表 7-2 を参照してください。
service-num	削除するプロトコル番号またはポート番号。

注意　サービスを削除すると、Detector　モジュールのポリシーがそのサービスのトラフィックに関連できなくなります。そのため、ゾーンの検出に支障をきたす恐れがあります。

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、tcp_services_ns：サービスはポート番号です。
- other_protocols：サービスはプロトコル番号です。

次の状況において、ラーニング プロセスのポリシー構築をアクティブにしない場合は、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。
- イネーブルにするつもりのない（そのネットワーク環境では一般的でないため）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）　サービスの削除後にポリシー構築フェーズを実行すると、そのサービスが再度追加されることがあります。

次の例を参考にしてください。

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

検出モジュール

検出モジュール セクションは、Detector モジュールがトラフィック フローの処理に使用する検出モジュールを示します。このセクションは情報提供用で、検出モジュールを設定することはできません。

分析：この検出モジュールでは、トラフィック フローが介入なしで流れます。

パケット タイプ

パケット タイプ セクションは、Detector モジュールが監視するパケット特性を示します。パケット特性は、次のいずれかです。

- パケット タイプ：たとえば、TCP-SYN パケット
- Detector モジュールによるパケット分析：たとえば、認証されたパケットや、接続が TCP ハンドシェイクを実行していることを Detector モジュールが確認したパケット
- パケットの方向：たとえば、着信接続

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	簡単な説明
auth_pkts	TCP ハンドシェイクまたは UDP 認証を経たパケット。
auth_tcp_pkts	TCP ハンドシェイクを経たパケット。
auth_udp_pkts	UDP 認証を経たパケット。
in_nodata_conns	接続上でデータ転送のないゾーン着信接続（データ ペイロードのないパケット）。
in_conns	ゾーン着信接続。
in_pkts	ゾーンの着信 DNS クエリー パケット。
in_unauth_pkts	ゾーンの認証されていない着信 DNS クエリー。
non_estb_conns	未確立の接続。失敗したゾーン着信接続。応答が受信されなかった TCP 接続要求（SYN パケット）。
out_pkts	ゾーンの着信 DNS 応答パケット。

表 7-8　パケット タイプ（続き）

パケット タイプ	簡単な説明
reqs	データ ペイロードを持つ要求パケット。
syns	同期パケット：TCP SYN フラグの付いたパケット。
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 ハンドシェイクを経なかったパケット。
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。

トラフィック特性

トラフィック特性セクションは、ポリシーの集約に使用されたトラフィック特性を示します。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*、*検出モジュール*、および *パケット タイプ*）では、分析するトラフィックのタイプが定義されます。トラフィック特性では、トラフィック フローを分析する方法が定義されます。したがって、同じトラフィック フローを分析するが、異なる特性に応じてレートを測定する異なるポリシーが存在することがあります。たとえば、*dns_tcp/53/analysis/pkts/dst_ip* と *dns_tcp/53/analysis/pkts/src_ip* です。

表 7-9 で、Detector モジュールが監視するトラフィック特性について説明します。

表 7-9　トラフィック特性

トラフィック特性	簡単な説明
dst_ip	ゾーンの IP アドレス宛てのトラフィック。
dst_ip_ratio	特定の IP アドレス宛ての、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 ポート宛てのトラフィック。
dst_port_ratio	特定のポート宛ての、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。

表 7-9　トラフィック特性（続き）

トラフィック特性	簡単な説明
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	プロトコルに応じて集約された、ゾーン宛てのトラフィック。
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.7-32 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、ゾーン宛てのトラフィック。
src_ip_many_dst_ips	多数のゾーン IP アドレスが同じポートにあることを調査する 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 アドレスに多数のポートがあることを調査する 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、特定のポリシー パラメータを表示できます。ポリシー パラメータを表示すると、ポリシー パラメータがゾーンのトラフィックに適しているかどうかを判断できます。1 つのポリシーまたはポリシーのグループを設定できます。必要に応じて、ポリシー パラメータを設定し、ポリシーをゾーンのトラフィック要件に適合させることができます。

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 **show** コマンドを使用します。

1 つの特定のポリシーまたはポリシーのグループを設定できます。

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入力します。

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「ポリシー パス構造」を参照してください。

（注）　ポリシー パス プロンプトで **policy ..** と入力すると、ポリシー パス階層で 1 レベル上に移動します。

次の例を参考にしてください。

```
user@DETECTOR-conf-zone-scannet# policy http/80/analysis/pkts/global
user@DETECTOR-conf-zone-scannet-policy-/http/80/analysis/pkts/global#
```

次のパラメータを設定できます。

- ポリシーの状態：P.7-22 の「ポリシーの状態の変更」を参照してください。
- ポリシーのしきい値：P.7-24 の「ポリシーのしきい値の設定」を参照してください。
- ポリシーのタイムアウト：P.7-29 の「ポリシーのタイムアウトの設定」を参照してください。

- ポリシーのアクション：P.7-30 の「ポリシーのアクションの設定」を参照してください。
- ポリシーのインタラクティブ ステータス：P.7-30 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。

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 パラメータの引数は、ポリシー パスの各セクションで変更できます。ただし、高レベルのポリシー セクション（ポリシー テンプレート セクションやサービス 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。

Detector モジュールでは、**show policies** コマンドおよび **show policies statistics** コマンドを発行するときに、各ポリシー パス セクションで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（*）とみなされます。
たとえば、ポリシーを *tcp_services//analysis//global* のように指定する場合です。

ポリシーの状態の変更

Detector モジュールのポリシーには、次の 3 つの状態があります。

- **Active**：ポリシーがトラフィックに関連し、しきい値超過が発生するとアクションを実行します。
- **Inactive**：ポリシーがトラフィックに関連し、しきい値を取得しますが、しきい値超過が発生してもアクションを実行しません。したがって、ポリシーが新しいしきい値調整ラーニング フェーズを経るようにする必要はありません。
- **Disabled**：ポリシーがトラフィック フローに関連しないため、しきい値が取得されません。このため、ポリシーに新しいしきい値調整フェーズを実行して、Detector モジュールにポリシーの適切なしきい値を監視させる必要があります。

注意　ポリシーをディセーブルにすると、そのポリシーの対象となっていたトラフィックは、他のポリシーに属するものと見なされます。すべてのポリシーが新しいしきい値調整フェーズを経てから、ゾーン検出をアクティブにすることを強くお勧めします。

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入力します。

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

次の例は、*/dns_tcp/53/analysis/syns* に一致するフローを持つすべてのポリシーの状態をディセーブルに設定する方法を示しています。

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

注意　ポリシーに対して不必要な非アクティブ化またはディセーブル化を行うと、Detector モジュールのポリシーが検出の役割を担わなくなり、ゾーンの検出に支障をきたす恐れがあります。

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、トラフィック フローに応じてポリシーが再設定されます。その結果、ポリシーが再び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 レートを定義します。このしきい値を超過すると、ポリシーはアクションを実行してゾーンを検出します。ポリシーのしきい値は、しきい値調整フェーズで調整されます。

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、pps 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を設定できます。P.7-25 の「ポリシーのしきい値の設定」を参照してください。
- しきい値の乗算を行う：Detector モジュールは、ポリシーの現在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.7-27 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、ゾーンのアドレス範囲内の特定の IP 送信元アドレスに対するしきい値を設定します。P.7-28 の「特定の IP しきい値の設定」を参照してください。

別のしきい値調整フェーズを実行すると、ポリシーのしきい値が変化する場合があります。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、後続のしきい値調整フェーズで、ポリシーのしきい値である proxy-threshold および threshold-list を変更しません。P.7-25 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の固定乗数を設定する**：Detector モジュールは、後続のしきい値調整フェーズで、ポリシーの現在のしきい値、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.7-26 の「しきい値の乗数の設定」を参照してください。

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、次のコマンドを入力します。

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 http/80/analysis/pkts/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-/http/80/analysis/pkts/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である proxy-threshold と threshold-list は、固定値として設定できます。Detector は、ラーニング プロセスのしきい値調整フェーズにおいて新しいしきい値を無視し、現在のしきい値を保持します。この機能により、ポリシーのしきい値を設定しながらも、引き続き他のポリシーのしきい値をラーニングする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入力します。

learning-params fixed-threshold

次の例を参考にしてください。

```
user@DETECTOR-conf-zone-scannet-policy-/http/80/analysis/pkts/global#
learning-params fixed-threshold
```

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。この場合、ゾーン設定モードでコマンドを使用します。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、次のコマンドを入力します。

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「ポリシー パス構造」を参照してください。

次の例を参考にしてください。

```
user@DETECTOR-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-parameters** コマンドを使用するか、ゾーン設定モードで **show policies** *policy-path* **learning-parameters** 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、後続のしきい値調整フェーズの結果を受け入れる前に、ラーニングしたしきい値に指定の乗数を掛けて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.5-24 の「しきい値選択方式の設定」を参照）。

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入力します。

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

表 7-10 で、**learning-params threshold-multiplier** コマンドの引数について説明します。

表 7-10　learning-params threshold-multiplier **コマンドの引数**

パラメータ	説明
policy-path	乗数を掛ける対象のしきい値を持つポリシーのパス。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「ポリシー パス構造」を参照してください。
threshold-multiplier	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、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分にする方法を示しています。

```
user@DETECTOR-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-parameters** コマンドを使用するか、ゾーン設定モードで **show policies** *policy-path* **learning-parameters** コマンドを使用します。

係数によるしきい値の乗算

1 つのポリシーまたはポリシーのグループのしきい値に係数を掛けることができます。このようにして、トラフィック量がゾーンのトラフィックを表さない場合に、1 つのポリシーまたはポリシーのグループのしきい値を増減できます。Detector モジュールは、ポリシーのしきい値、プロキシしきい値、および **policy threshold-list** コマンドを使用して定義されたしきい値を乗算します。

ポリシーのしきい値に係数を掛けるには、次のコマンドを入力します。

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

表 7-11 で、**policy thresh-mult** コマンドの引数について説明します。

表 7-11　policy thresh-mult 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 7-2 を参照してください。
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）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。

次の例を参考にしてください。

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

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 モジュールが後続のしきい値ラーニング フェーズでしきい値を変更でき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.7-25 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-parameters** コマンドを使用するか、ゾーン設定モードで **show policies** *policy-path* **learning-parameters** コマンドを使用します。

特定の IP しきい値の設定

特定の IP しきい値を設定するには、次の方法を使用します。

- ある IP 送信元から大量のトラフィックがあることが分かっている場合は、特定の IP 送信元アドレスに適用するしきい値を設定できます。
- ゾーンの一部だけに宛てた大量のトラフィックがあることが分かっている非同種ゾーン（複数の IP アドレスが定義されているゾーン）の場合は、特定の IP 宛先アドレスに適用するしきい値を設定できます。

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、次のコマンドを入力します。

policy *policy-path* **threshold-list** *ip threshold* [*ip threshold ...*]

表 7-12 で、**policy threshold-list** コマンドの引数について説明します。

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 7-2 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（pps）。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。

しきい値選択方式が new-thresholds に設定されていると、Detector モジュールは後続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場合があります（詳細については、P.5-24 の「しきい値選択方式の設定」を参照）。

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

ポリシーによって生成される動的フィルタがそのアクションを適用する最小期間を定義するタイムアウト パラメータ。

ポリシーのタイムアウトを設定するには、次のコマンドを入力します。

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

表 7-13 で、**timeout** コマンドの引数とキーワードについて説明します。

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。
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指定する 1 ～ 3,000,000 の整数。

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

ポリシーのアクションの設定

アクション パラメータは、しきい値超過が発生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。ポリシーのアクションを設定するには、次のコマンドを入力します。

action *policy-action*

表 7-14 で、ポリシーのアクションについて説明します。

表 7-14　ポリシーのアクション

ポリシーのアクション	簡単な説明
notify	しきい値を超過するとユーザに通知します。
remote-activate	しきい値超過が発生すると、ポリシーはリモート 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.5-45 の「リモート Guard のアクティブ化」および P.4-34 の「日付と時刻の設定」を参照してください。

ポリシーの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、*dns_tcp* に関連するすべてのポリシーの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 dns_tcp/ set-action
remote-activate
set action of dns_tcp/ to remote-activate:
4 policy actions set.
```

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、検出がイネーブルで、ゾーンがインタラクティブ検出モードの場合にのみ、ゾーンに適用できます。詳細については、第 8 章「インタラクティブ検出モード」を参照してください。

現在保護されているゾーンの推奨事項のインタラクティブ ステータスを **always-accept** または **always-ignore** に設定している場合、ポリシーの保留動的フィルタのステータスを変更するには、**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ことを選択するには、ポリシーのインタラクティブ ステータスを **interactive** または **always-accept** に変更します。

ポリシーのインタラクティブ ステータスを設定するには、次のコマンドを入力します。

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

表 7-15 で、**interactive-status** コマンドのキーワードについて説明します。

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。これは、ポリシーによって新しい推奨事項が生成されると必ず、自動的に適用されます。 Detector モジュールはこのような推奨事項を表示しません。
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。ポリシーは、いったんしきい値を超過すると推奨事項を生成しません。 Detector モジュールはこのような推奨事項を表示しません。
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。

次の例を参考にしてください。

```
user@DETECTOR-conf-zone-scannet-policy-/http/80/analysis/pkts/global#
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、自己伝搬する侵入エージェントであり、自身のコピーを容易に配布します。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別の脆弱なターゲットを攻撃します。次に、何らかの手法でネットワークを探索（一般的にはスキャン）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、各アドレスにアクセスします。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 モジュールを使用することにより、TCP ワーム攻撃からゾーンを保護することができます。このモジュールは、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 パターンに従ってワームを識別します。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 モジュールはネットワーク スキャナーのヒストグラムを使用します。Detector モジュールは、攻撃が進行中でないとき（平時）にゾーンのネットワークをラーニングし、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、平時にラーニングしたヒストグラムから偏差がある場合、ワーム攻撃を識別します。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.7-34 の「ワーム攻撃の識別」を参照してください。

これらのポリシーは、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します。したがって、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 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 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 以外を宛先とするトラフィックすべてを監視します。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
- ワーム攻撃の識別

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 *scanners* トラフィック特性から構築されます。

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。ヒストグラムを設定するには、ポリシー設定モードで次のコマンドを入力します。

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

num-dst-ips 引数には、スキャンされたゾーン宛先 IP アドレスの数を指定します。*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 引数には、ヒストグラムしきい値を指定します。しきい値を超過すると、ポリシーはアクションを実行してゾーンを検出します。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.7-24 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。P.7-15 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、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。このしきい値を超えた時点で、Detector モジュールはネットワークにマス スキャナーが存在すると判断します。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わかりません。
- 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。ヒストグラムしきい値を超えた時点で、Detector モジュールはワーム攻撃であると判断します。

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スキャニングしきい値を新しく内部に定義します。

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 scanners ポリシーのヒストグラムは次のようになります。

送信元 IP アドレスの数	10	5	2
宛先 IP アドレスの数	5	20	100

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。

Detector モジュールは、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 policy 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ます。このため、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。その結果、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適切に調整されていることを確認する必要があります。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であった場合、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** コマンドを発行してもそのポリシーは表示されません。

ゾーンのポリシーを表示するには、次のコマンドを入力します。

show policies *policy-path*

policy-path 引数には、ポリシーのグループを指定します。詳細については、P.7-2 の「ポリシー パス構造」を参照してください。すべてのポリシーの統計情報を表示するには、アスタリスク（*）を入力します。

表 7-16 で、**show policies** コマンド出力のフィールドについて説明します。

表 7-16　show policies コマンド出力のフィールド説明

フィールド	簡単な説明
Policy	ポリシー名を示します。詳細については、P.7-2 の「ポリシー パス構造」を参照してください。
State	ポリシーの状態を示します。詳細については、P.7-22 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。
IStatus	ポリシーのインタラクティブ ステータスを示します。詳細については、P.7-30 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を示します。このしきい値を超過すると、Detector モジュールはアクションを実行します。詳細については、P.7-24 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 しきい値の数を示します。詳細については、P.7-28 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。P.7-32 の「ワーム ポリシーについて」を参照してください。
Action	しきい値超過が発生した場合にポリシーが実行するアクションを示します。詳細については、P.7-30 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を示します。Detector モジュールは、filter-termination しきい値に従って、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。詳細については、P.7-29 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 つのポリシーまたは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できます。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、次のコマンドを入力します。

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

表 7-17 で、**show policies statistics** コマンドの引数について説明します。

表 7-17　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を指定します。詳細については、P.7-2 の「ポリシー パス構造」を参照してください。すべてのポリシーの統計情報を表示するには、アスタリスク（*）を入力します。
num-entries	表示するエントリの数を指定します。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。

Detector モジュールは、4 つのテーブルに情報を表示します。各テーブルの情報は値によってソートされ、最大の値が一番上に表示されます。

（注）　Detector モジュールは、データを含まないテーブルを表示しません。

表 7-18 で、**show policies statistics** コマンド出力テーブルのフィールドについて説明します。

表 7-18　show policies statistics コマンド出力テーブルのフィールド説明

テーブル	説明
すべての出力テーブルのフィールド	
Key	キー（ポリシーの集約に使用されたトラフィック特性）を示します。 たとえば、ポリシー *tcp_services/any/analysis/syns/dst_ip* 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。たとえば、*192.128.100.3:70* です。 詳細については、表 7-8 を参照してください。
Policy	ポリシー名を示します。詳細については、P.7-2 の「ポリシー パス構造」を参照してください。
1 つの出力テーブルのフィールド	
Rate	ポリシーを通過するトラフィックのレートを pps で示します。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。
Connection	同時接続の数を示します。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_nodata_conns**：分析検出モジュールの場合
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を示します。この情報は、syn_by_fin ポリシーだけで使用できます。
Dst IPs	スキャンされたゾーン宛先 IP アドレスの数を指定します。この情報は、worm_tcp ポリシーだけで使用できます。

スナップショットを使用したラーニング プロセスの結果の確認

ラーニング プロセス中の任意の段階でラーニング パラメータ（サービス、しきい値、その他のポリシー関連データ）のスナップショットを保存して、後で確認できます。2 つのゾーンのラーニング パラメータまたはスナップショットを比較して、ラーニング プロセスの結果を確認し、ポリシー、サービス、およびしきい値の違いをトレースできます。

ラーニング プロセス中、数時間ごとにスナップショットを保存することをお勧めします。ラーニング プロセス中に攻撃が発生した場合は、スナップショット ポリシーをゾーンに使用できます。スナップショットは、手動で撮ることも、Detector モジュールを設定して、指定した間隔で自動的に撮ることもできます。Detector モジュールは、ゾーンごとに最大 100 個のスナップショットを保存できます。以前のスナップショットは新しいスナップショットに置き換えられます。

スナップショットからポリシーをコピーすることで、必要に応じて、以前のラーニングの結果に基づいてゾーンを設定できます。

この項では、次のトピックについて取り上げます。

- スナップショットの作成
- ラーニングの結果の比較
- スナップショットの表示
- ポリシーのコピー

スナップショットの作成

ゾーン ラーニング パラメータのスナップショットを 1 つだけ保存することも、指定した間隔でスナップショットが自動的に撮られるように Detector モジュールを設定することもできます。Detector モジュールは、スナップショットが撮られている間も、ラーニング フェーズを続行します。

指定した間隔でスナップショットが自動的に撮られるように Detector モジュールを設定する方法の詳細については、P.5-23 の「定期的なアクションの設定」を参照してください。

ゾーンのラーニング パラメータのスナップショットを 1 つ保存するには、ゾーン設定モードで次のコマンドを入力します。

snapshot [**threshold-selection** {**new-thresholds** | **max-thresholds** | **cur-thresholds** | **weighted** *calc-weight*}]

表 7-19 で、**snapshot** コマンドの引数とキーワードについて説明します。

表 7-19　snapshot コマンドの引数とキーワード

パラメータ	説明
threshold-selection	Detector モジュールがスナップショットしきい値の計算に使用する方法を設定します。デフォルトでは、Detector モジュールは、**learning-params threshold-selection** コマンドによって定義された、ゾーンのしきい値選択方式を使用します。ゾーンのデフォルトのしきい値選択方式は、**max-thresholds** です。
new-thresholds	Detector モジュールは、ラーニング プロセスの結果をゾーン設定に保存します。
max-thresholds	Detector モジュールは、現在のポリシーのしきい値をラーニングされたしきい値と比較し、値の大きい方をゾーン設定に保存します。 これがデフォルトの方式です。
weighted *calc-weight*	Detector モジュールは、次の数式に基づいて、保存するポリシーのしきい値を計算します。 しきい値 = (新しいしきい値 * 計算された重み + 現在のしきい値 * (100 - 計算された重み)) / 100
cur-thresholds	Detector モジュールは、ラーニング プロセスの新しいしきい値を無視し、ポリシーの現在のしきい値をスナップショットに保存します。この方式は、バックアップの目的で使用できます。

snapshot コマンドを使用すると、ゾーンのラーニング プロセスの結果が保存されます。この結果には、ゾーンのポリシー、サービス、およびしきい値が含まれます。スナップショットのパラメータを確認するか、2 つのスナップショットを比較するか、またはスナップショットのパラメータを新しいゾーンにコピーし終わったら、スナップショットを削除できます。

snapshot threshold-selection cur-thresholds コマンドを使用すると、現在のゾーン ポリシーをいつでもバックアップできます。

次の例は、ポリシーの現在のしきい値とラーニング プロセスの新しいしきい値のうちで最も大きい値をしきい値として持つ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
max-thresholds
```

グローバル モードでスナップショットを 1 つ保存するには、**snapshot** *zone-name* [**threshold-selection** {**new-thresholds** | **max-thresholds** | **cur-thresholds** | **weighted** *weight*}] コマンドを使用します。

スナップショットを削除するには、**no snapshot** コマンドを使用します。

ラーニングの結果の比較

2 つのスナップショットまたはゾーンのラーニングの結果を比較して、ポリシー、サービス、およびしきい値の違いをトレースできます。

この項では、次のトピックについて取り上げます。

- スナップショットの比較
- ゾーンの比較

スナップショットの比較

2 つのスナップショットを比較するには、ゾーン設定モードで次のコマンドを入力します。

diff snapshots *snapshot-id snapshot-id* [***percent***]

表 7-20 で、**diff** コマンドの引数について説明します。

表 7-20　diff コマンドの引数

パラメータ	説明
snapshot-id	比較対象のラーニング パラメータを持つスナップショットの ID。ゾーンのスナップショットのリストを表示するには、**show snapshots** コマンドを使用します。
percent	（オプション）トレースしきい値。Guard は、2 つのスナップショットを比較した場合、相違点がここに指定したしきい値を超えているポリシーしきい値パラメータをすべてトレースします。デフォルトのパーセンテージは 100% で、Guard は 2 つのスナップショットにおける相違をすべてトレースします。

次の例は、ゾーンのスナップショットを表示し、最新の 2 つのスナップショットを比較する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show snapshots
ID    Time
1     Feb 10 10:32:04
2     Feb 10 10:49:12
3     Feb 10 11:01:50
user@DETECTOR-conf-zone-scannet# diff 2 3
```

グローバル モードでスナップショットを比較するには、**diff** *zone-name* **snapshots** *snapshot-id snapshot-id* [*percent*] コマンドを使用します。

ゾーンの比較

2 つのゾーンのラーニング パラメータを比較するには、グローバル モードまたは設定モードで次のコマンドを入力します。

diff *zone-name zone-name* [***percent***]

表 7-21 で、**diff** コマンドの引数について説明します。

表 7-21　diff コマンドの引数

パラメータ	説明
zone-name	比較対象のラーニング パラメータを持つゾーンの名前。
percent	（オプション）トレースしきい値。Guard は、2 つのゾーンを比較した場合、相違点がここに指定したしきい値を超えているポリシーしきい値パラメータをすべてトレースします。デフォルトのパーセンテージは 100% で、Guard は 2 つのゾーンにおける相違をすべてトレースします。

次の例を参考にしてください。

```
user@DETECTOR# diff scannet scannet-mailserver
```

スナップショットの表示

ゾーンのラーニングの結果を明確に把握するために、ゾーンのスナップショットまたはスナップショット パラメータのリストを表示できます。

ゾーンのスナップショットを表示するには、次のコマンドを入力します。

show snapshots [***snapshot-id*** [**policies** ***policy-path***]]

表 7-22 で、**show snapshots** コマンドの引数とキーワードについて説明します。

表 7-22　show snapshots コマンドの引数とキーワード

パラメータ	説明
snapshots	ゾーンのスナップショットを表示します。スナップショットの ID を指定しない場合、デフォルトでは、ゾーンのスナップショットすべてのリストが表示されます。
snapshot-id	表示対象のラーニング パラメータを持つスナップショットの ID。ポリシーを指定しない場合、デフォルトでは、ゾーンのスナップショットすべてのリストが表示されます。スナップショットの ID を表示するには、**show snapshots** コマンドを使用します。
policy-path	表示対象のポリシーのグループを指定します。詳細については、P.7-2 の「ポリシー パス構造」を参照してください。

グローバル モードでスナップショットを比較するには、**show zone** *zone-name* **snapshots** [*snapshot-id* [**policies** *policy-path*]] コマンドを使用します。

次の例は、ゾーンのスナップショットのリストを表示し、次にスナップショット *2* の *dns_tcp* に関連するポリシーを表示する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show snapshots
ID    Time
1     Feb 10 10:32:04
2     Feb 10 10:49:12
user@DETECTOR-conf-zone-scannet# show snapshots 2 policies dns_tcp
```

show zone *zone-name* **snapshots** *snapshot-id* **policies** *policy-path* コマンド出力のフィールドは、**show policies** コマンド出力のフィールドと同じです。詳細については、P.7-36 の「ポリシーの表示」を参照してください。

表 7-23 で、**show snapshots** コマンド出力のフィールドについて説明します。

表 7-23　show snapshots コマンド出力のフィールドの説明

フィールド	説明
ID	スナップショットの ID。
Time	スナップショットが取得された日時。

ポリシーのコピー

ポリシーの設定または部分的な設定を現在のゾーンにコピーできます。

次の情報をコピーできます。

- サービスをコピーする：ソース　ゾーンから別のゾーンにサービスをコピーできます。このようにして、サービスを検出するためにポリシー構築フェーズを適用せずに、ゾーンのポリシーを設定できます。サービスをゾーンにコピーするには、まず、そのゾーンが同様のトラフィック パターンを持つことを確認します。
- ポリシー パラメータをコピーする：ポリシー パラメータを、ゾーンのスナップショットの 1 つが持つポリシー パラメータに置き換えることができます。このようにして、以前のラーニングの結果に戻すことができます。Detector モジュールは、既存のポリシーのパラメータだけをコピーします。

ゾーンのポリシーをコピーするには、ゾーン設定モードで次のコマンドを入力します。

copy-policies {***snapshot-id*** | *src-zone-name* [*service-path*]}

表 7-24 で、**copy-policies** コマンドの引数とキーワードについて説明します。

表 7-24　copy-policies コマンドの引数とキーワード

パラメータ	説明
snapshot-id	ポリシーのコピー元のスナップショットの ID。スナップショットの ID を表示するには、**show snapshots** コマンドを使用します。
src-zone-name	サービス ポリシーのコピー元のゾーン名。
service-path	コピーされる対象のサービス。サービス パスの形式は、次のいずれかです。 • **policy-template**：ポリシー テンプレートに関連するすべてのポリシーをコピーします。 • **policy-template/service-num**：ポリシー テンプレートおよび指定のサービスに関連するすべてのポリシーをコピーします。 デフォルトでは、すべてのポリシーとサービスがコピーされます。

次の例は、ポリシー テンプレート *tcp_connections* に関連するすべてのサービスを、ゾーン *webnet* から現在のゾーン *scannet* にコピーする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# copy-policies webnet tcp_connections/
```

次の例は、ゾーンのスナップショットのリストを表示し、次に ID が *2* のスナップショットからポリシーをコピーする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show snapshots
ID   Time
1    Feb 10 10:32:04
2    Feb 10 10:49:12
user@DETECTOR-conf-zone-scannet# copy-policies 2
```