



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](#)
- [ポリシー テンプレートについて](#)
- [ポリシー パスのセクションについて](#)
- [ポリシー パラメータの設定](#)
- [ワーム ポリシーについて](#)
- [ポリシーの監視](#)
- [ポリシー設定のバックアップ](#)

ゾーンポリシーについて

トラフィック フローの統計分析を行うために、Detector モジュールには特定のタイプのトラフィックを処理する定義があります。この定義を、ゾーンポリシーといいます。ゾーンポリシーは Detector モジュールの構成要素で、Detector モジュールがゾーントラフィックを比較する基準になります。ゾーンポリシーは、常にトラフィック フローを測定し、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なもの（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に発生する）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。フィルタ（動的フィルタ）セットを動的に設定して、Detector がリモート Guard リストに定義された Cisco Anomaly Guard Module をアクティブにしてゾーンを保護するか、イベントを自身の syslog に記録します。

ゾーンポリシーを作成するために、Detector モジュールは2つのフェーズでゾーントラフィックをラーニングします。Detector モジュールは事前定義されたテンプレートを使用してポリシーを構築し、それからポリシーのしきい値をラーニングします。各ポリシーテンプレートは、Detector モジュールが特定の DDoS 攻撃（分散型サービス拒絶攻撃）の脅威を検出するために必要なポリシーの作成に使用します。

Detector モジュールがゾーンポリシーを作成したら、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。

ポリシーパスの使用

ゾーンポリシーは、Detector モジュールがゾーントラフィックフローの分析と測定に使用する特性を定義します。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

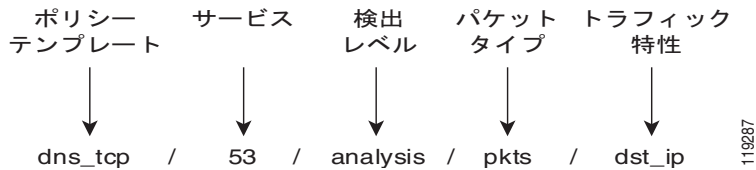


表 7-1 に、ポリシー名のセクションを示します。

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。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.7-5 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	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。詳細については、 P.7-14 の「サービス」 を参照してください。
検出レベル	Detector モジュールがトラフィック フローに適用する検出レベル。詳細については、 P.7-18 の「検出レベル」 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。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。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。

■ ゾーンポリシーについて

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。

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、ポリシーのトリガーを定義し、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定義します。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、次の2つのフェーズで構成されるラーニングプロセスでゾーンポリシーを作成します。これらのフェーズでは、**Detector** モジュールはゾーントラフィックをラーニングし、特定のゾーントラフィック特性に合わせて自己調整します。

1. **ポリシー構築フェーズ**：**Detector** モジュールは、ポリシー テンプレートを使用してゾーンポリシーを構築し、ゾーンが使用する主なサービスを検出します。
2. **しきい値調整フェーズ**：**Detector** モジュールは、ポリシー構築フェーズで検出されたサービスのポリシーしきい値を、ゾーンサービスのトラフィック レートに合わせて調整します。

ラーニング プロセス中、ゾーントラフィックは **Detector** モジュールを透過的に通過します。詳細については、[P.5-14](#) の「[Detector モジュールの Cisco Anomaly Guard Module とのゾーン設定の同期](#)」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。ポリシー構築フェーズ終了時の各テンプレートの出力が、ポリシーの集まりになります。ポリシー テンプレートの名前は、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、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
<code>dns_tcp</code>	DNS-TCP プロトコル トラフィック。
<code>dns_udp</code>	DNS-UDP プロトコル トラフィック。
<code>fragments</code>	断片化されたトラフィック。
<code>http</code>	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	<p>IP スキャン (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。</p> <p>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。</p> <p> (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。</p>
other_protocols	TCP 以外のプロトコルと UDP 以外のプロトコル。
port_scan	<p>ポート スキャン (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)。</p> <p>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。</p> <p> (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。</p>
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 パケット対 FIN/RST パケットなど。

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 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 7-3 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 7-3 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
_WORM	<p>worm_tcp : TCP ワームに関連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。</p> <p>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.7-34 の「ワーム ポリシーについて」を参照してください。</p>
GUARD_SIP	<p>sip_udp : SIP¹ 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/RTCP² を使用して音声データを SIP エンドポイント間で伝送する VoIP³ 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。</p>

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

■ ポリシー テンプレートについて

GUARD_ゾーン テンプレートからゾーンを作成する場合、Cisco Anomaly Guard Module 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 7-4 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、Cisco Anomaly Guard Module 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 7-4 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 7-4 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	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、ゾーン トラフィックは **Detector** 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。**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。

- **サービスの最大数の設定** : **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 7-2](#) 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#
```

■ ポリシー テンプレートについて

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、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 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、ゾーンが使用する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。したがって、こちらの値は正確ではありません。

サービス数を制限すると、目的のトラフィック フロー要件に合わせて 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よりの確に合せることができます。

最小しきい値のパラメータは、正しいゾーン異常検出に不可欠で必ず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*) には設定できません。

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。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トラフィックからゾーンを検出できません。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、**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

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 7-5 に、**policy-template** コマンドの引数とキーワードを示します。

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
<i>policy-template-name</i>	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。
<i>max-services</i>	<p>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。</p> <p>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。</p> <p>詳細については、P.7-10 の「サービスの最大数の設定」を参照してください。</p>
<i>min-threshold</i>	<p>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。</p> <p>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。</p> <p>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。</p>
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.7-12 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.7-12 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](#)
- [サービス](#)
- [検出レベル](#)
- [パケットタイプ](#)
- [トラフィック特性](#)

ポリシー テンプレート

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。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

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。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。

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

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.8-10 の「ポリシーしきい値の調整」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.8-18 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 トラフィックに合わせて調整することをお勧めします。詳細については、P.8-10 の「ポリシーしきい値の調整」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、worm_tcp
このサービスは、ポート番号を表わします。
- other_protocols
このサービスは、プロトコル番号を表わします。



(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。

■ ポリシー パスのセクションについて

次の状況では、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、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
<i>policy-template-name</i>	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。
<i>service-num</i>	プロトコル番号またはポート番号。

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せん。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* (ポリシー テンプレート設定モードの場合)

- **policy-template** *policy-template-name* **remove-service** *service-num* (ゾーン設定モードの場合)

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
<i>policy-template-name</i>	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。
<i>service-num</i>	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**、**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。
- (ネットワーク環境では一般的でないため) イネーブルにしてい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、同じサービスが再度追加される場合があります。

■ ポリシー パスのセクションについて

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
```

検出レベル

Guard は分析検出レベルをトラフィック フローに適用します。



(注) 検出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 Detector 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 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ゾーン着信接続 (データ ペイロードのないパケット)。

表 7-8 パケット タイプ (続き)

パケット タイプ	説明
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。
syms	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。

トラフィック特性

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 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	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	説明
dst_port	特定のゾーン ポート宛でのトラフィック。
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.7-34 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	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 プロセスが完了したら、特定のポリシー パラメータを表示し、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することができます。必要に応じて、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 **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「[ポリシー パスの使用](#)」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@DETECTOR-conf-zone-scannet# policy
dns_tcp/53/analysis/syns/global
user@DETECTOR-conf-zone-scannet-policy-/dns_tcp/53/analysis/syns/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.7-23](#) 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.7-30](#) 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 パラメータの設定

- ポリシーのアクション : P.7-31 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.7-32 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 `tcp_services/analysis/global` 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。

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ため、しきい値を取得しません。したがって、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、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。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-/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@DETECTOR-conf-zone-scannet-policy-/*/*/*global# state notify
```



注意

むやみに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、そのためゾーン異常検出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。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、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 パラメータの設定

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.7-24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.7-27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 アドレス範囲内で、特定の IP 送信元アドレスを設定します。P.7-28の「[特定の IP しきい値の設定](#)」を参照してください。

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.7-25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に固定乗数を設定する
Detector モジュールは、以後のしきい値調整フェーズで、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.7-26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、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@DETECTOR-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。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、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/  
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に設定できます。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「ポリシー パスの使用」](#)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@DETECTOR-conf-zone-scannet# policy dns_tcp learning-params  
fixed-threshold
```

■ ポリシー パラメータの設定

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.8-17 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
<i>policy-path</i>	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「ポリシー パスの使用」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 <i>threshold-multiplier</i>	ポリシーのしきい値を乗算します。 <i>threshold-multiplier</i> 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 `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@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-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
<i>policy-path</i>	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。
thresh-mult <i>threshold-multiply-factor</i>	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。

■ ポリシー パラメータの設定

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@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.7-25 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-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分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 モジュールが攻撃を誤っ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持つ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分かっている場合は、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分かっている場合は、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。

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 ...]` (ゾーン設定モードの場合)
- `threshold-list ip threshold [ip threshold ...]` (ポリシー設定モードの場合)

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
<code>policy-path</code>	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。
<code>ip</code>	特定の IP アドレス。
<code>threshold</code>	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。

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.8-17 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。
<i>timeout</i>	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.9-7 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 `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@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、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-accept** 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 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	<p>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。</p> <p>Detector モジュールはこのような推奨事項を表示しません。</p>
always-ignore	<p>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、しきい値を超過すると推奨事項を生成しません。</p> <p>Detector モジュールはこのような推奨事項を表示しません。</p>

表 7-15 interactive-status コマンドのキーワード (続き)

パラメータ	説明
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。スキャンング 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。

- スキャンングしきい値：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.7-37 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 を宛先とする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](#)
- [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。

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、スキャン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
<i>num-dst-ips</i>	スキャンされたゾーン宛先 IP アドレスの数。 <i>num-dst-ips</i> の値は 5、20、および 100 で、システム定義になっています。 <i>num-dst-ips</i> ごとに定義される <i>num-src-ips</i> の値は変更できません。
<i>num-src-ips</i>	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 (<i>num-dst-ips</i>) 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 (スキャンしきい値)。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.7-23 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、スキャン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.7-34 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スキャン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ン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 (スキャンしきい値) 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

■ ワーム ポリシーについて

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ン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ンしきい値 (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わ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 (*) とみなされます。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「[ポリシー パスの使用](#)」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/*/syms/*
```

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	ポリシー名を示します。 ポリシー パス セクションの詳細については、 P.7-2 の「 ポリシー パスの使用 」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.7-32 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.7-23 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。詳細については、 P.7-34 の「 ワーム ポリシーについて 」を参照してください。

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
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を示します。詳細については、P.7-31 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、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.7-30 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、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
<i>policy-path</i>	<p>統計情報を表示するポリシーのグループを指定します。</p> <p>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、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。</p> <p>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。</p> <p>ポリシー パス セクションの詳細については、P.7-2 の「ポリシーパスの使用」を参照してください。</p>
<i>num-entries</i>	<p>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。</p>

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
```

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、テーブルの一番上に最大値が表示されます。

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。

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
すべての出力テーブルのフィールド	
Key	<p>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。</p> <p>たとえば、<code>tcp_services/any/analysis/syns/dst_ip</code> ポリシーの場合、キーは宛先 IP アドレス（<code>dst_ip</code>）です。ポリシーの集約に使用されたトラフィック特性が <code>global</code> である場合、キーには <code>N/A</code> と表示されます。</p> <p>ワームに関連するポリシー（<code>worm_tcp/any/analysis/non_estb_conns/scanners</code> 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、<code>192.128.100.3:70</code> と表示されます。</p> <p>詳細については、表 7-8 を参照してください。</p>
Policy	<p>ポリシー名を示します。</p> <p>詳細については、P.7-2 の「ポリシーパスの使用」を参照してください。</p>
1 つの出力テーブルのフィールド	
Rate	<p>ポリシーを通過し <code>pps</code> 単位で計測されるトラフィックのレートを示します。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。</p>
Connection	<p>同時接続の数を示します。</p> <p>この情報は、パケットタイプが <code>in_nodata_conns</code> の <code>tcp_connections</code> ポリシーについてのみ表示されます。</p>

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
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。



(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。

ポリシー設定のバックアップ

現在のゾーン ポリシーは、**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
```