



ポリシー テンプレートと ポリシーの設定

この章では、Cisco Anomaly Guard Module (Guard モジュール) のポリシー、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、ポリシーとポリシー テンプレート パラメータの設定方法を示します。

この章には、次の項があります。

- [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](#)
- [ポリシーの監視](#)
- [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](#)

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、Guard は、特定のトラフィック タイプの処理に関する定義を持っています。これらの定義をポリシーといいます。ポリシーは、Guard 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 パターンに合わ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、Guard 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、Guard モジュールは 2 つのフェーズのラーニング プロセスでゾーンのトラフィックをラーニングします。Guard モジュールは、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 脅威に対する保護のために Guard モジュールが必要とする保護面を扱います。

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

Guard 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、Guard 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、Guard モジュールの分析保護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 8-1 に、ポリシー名の例を示します。

図 8-1 ポリシー名

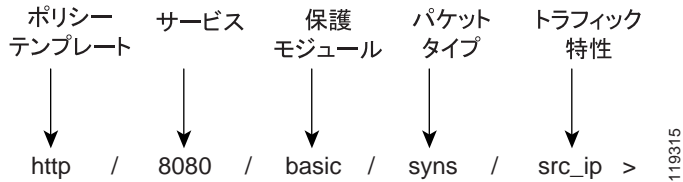


表 8-1 で、ポリシー名のセクションについて詳しく説明します。

表 8-1 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 脅威に対する保護のために Guard モジュールが必要とする保護面を扱います。詳細については、 P.8-5 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	保護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.8-14 の「サービス」 を参照してください。
保護モジュール	Guard モジュールがトラフィック フローの処理に使用する保護モジュールを示します。詳細については、 P.8-18 の「保護モジュール」 を参照してください。
パケット タイプ	Guard モジュールが監視するパケット タイプを示します。詳細については、 P.8-18 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	Guard モジュールがポリシーの集約に使用するトラフィック 特性を示します。詳細については、 P.8-20 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、保護モジュール、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、Guard モジュールは、より限定的なポリシーを使用してフローを分析します。たとえば、TCP サービスに関連するポリシーでは、HTTP 関連のポリシーによって処理される HTTP サービスが除外されます。

ポリシー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.8-21](#) 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

Guard 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 プロセスは次の 2 つのフェーズで構成されます。これらのフェーズで Guard はゾーンのトラフィックをラーニングし、特定のゾーン トラフィックの特性に対応します。

- 1. ポリシー構築フェーズ：**このフェーズでは、Guard 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 Guard を通過し、Guard 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、Guard はゾーンのサービスのトラフィック レートに合わせてポリシーしきい値を調整します。トラフィックが透過的に Guard を通過し、Guard 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.6-13](#) 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。Guard 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、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ときに、Guard モジュールによって一連のポリシー テンプレートがゾーン設定に組み込まれます。

表 8-2 で、Guard モジュールのポリシー テンプレートについて説明します。GUARD_DEFAULT ゾーン テンプレートを使用して新しいゾーンを作成するときに、Guard モジュールによってこれらのポリシー テンプレートが組み込まれます。

表 8-2 ポリシー テンプレート

ポリシー テンプレート	構築される一連のポリシーの関連先
<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 8-2 ポリシー テンプレート (続き)



ポリシー テンプレート	構築される一連のポリシーの関連先
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)。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。</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、<i>notify</i> 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 および 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、<i>notify</i> 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	Guard 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。

表 8-2 ポリシー テンプレート (続き)

ポリシー テンプレート	構築される一連のポリシーの関連先
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。
tcp_services	HTTP 関連のポート (ポート 80 やポート 8080 など) 以外のポート上の TCP サービス。
tcp_services_ns	TCP サービス。デフォルトでは、このポリシー テンプレートから作成されるポリシーは、IRC ポート (666X)、SSH、および Telnet に関連するものになります。このポリシー テンプレートは、Guard モジュールで強化保護メカニズムを使用することが必要なアクションを持つポリシーを作成しません。
udp_services	UDP サービス。



(注) Guard は、まず専用ポート 6660 ~ 6670 および 21 ~ 23 上の TCP トラフィックのインジケータになります。

- これらのポート上でトラフィックがトレースされる場合、tcp_services_ns ポリシー テンプレートがポリシー グループを構築し、tcp_services ポリシー テンプレートが他のポート上の TCP サービスを担当します。
- これらのポート上でトラフィックがトレースされない場合、tcp_services_ns ポリシー テンプレートは動作しません。

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

Guard には、TCP プロキシのスプーフィング防止メカニズムを使用しないゾーンを保護するための追加のポリシー テンプレートが用意されています。ゾーンが IP アドレスに応じて管理される場合 (Internet Relay Chat (IRC; インターネットリレー チャット) サーバタイプゾーンなど)、またはゾーンでどのようなタイプのサービスが実行されているか分からない場合は、このようなポリシー テンプレートを使用できます。

GUARD_TCP_NO_PROXY ゾーンテンプレートでゾーンを定義する場合、Guard モジュールによって、表 8-3 に示されるポリシー テンプレートが使用されます。Guard モジュールは、http、tcp_connections、および tcp_outgoing のポリシー テンプレートをそれぞれ http_ns、tcp_connections_ns、および tcp_outgoing_ns のポリシー テンプレートに置き換えます。http_ns、tcp_connections_ns、および tcp_outgoing_ns のポリシー テンプレートは、Guard モジュールで強化保護メカニズムを使用することが必要なアクションを持つポリシーを作成しません。

表 8-3 に、GUARD_TCP_NO_PROXY の Guard ポリシーを詳細に説明します。

表 8-3 GUARD_TCP_NO_PROXY のポリシー テンプレート

ポリシー テンプレート	構築される一連のポリシーの関連先
tcp_connections_ns	TCP 接続の特性。
tcp_outgoing_ns	ゾーンによって開始された TCP 接続。
http_ns	ポート 80 (デフォルト) または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 Guard 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。Guard では、特定のポリシー テンプレートから Guard が生成するポリシーの最大数を定義できます。Guard 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 Guard は、定義済みの最小しきい値を超過したサービスの中で最大のトラフィック量を持つ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** : **Guard** 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** : **Guard** モジュールでサービスをランク付けするために超える必要のある最小しきい値を定義します。
- **ポリシー テンプレートの状態の設定** : **Guard** 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 8-2 を参照してください。

このコマンドを実行すると、**Guard** 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@GUARD-conf-zone-scannet# policy-template http  
user@GUARD-conf-zone-scannet-policy_template-http#
```

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

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。**Guard** 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。**Guard** は、定義済みの最小しきい値（*min-threshold* パラメータで定義）を超過したサービスの中で最大のトラフィック量を持つ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。

`Guard` は、ポリシーのトラフィック特性に基づいてサービスへのトラフィック 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ワークです。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 フロー要件に合わせて `Guard` 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、`Guard` がピックアップ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。

次の例を参考にしてください。

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

最小しきい値の設定

最小しきい値のパラメータは、サービスの最小トラフィック量を定義します。このしきい値を超過すると、Guard は、しきい値を超過し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。

このパラメータは、正しいゾーン保護に不可欠であるためにポリシーを常に構築するポリシー テンプレート (`tcp_services`、`tcp_services_ns`、`udp_services`、`other_protocols`、`http`、および `fragments`) には設定できません。

このしきい値を設定すると、Guard の保護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@GUARD-conf-zone-scannet-policy_template-http# min-threshold 12.3
```

ポリシー テンプレートの状態の設定

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、Guard 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、Guard はそのポリシー テンプレートに関連するトラフィックの種類からゾーンを保護できません。このため、保護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 テンプレートについて

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 8-4 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 8-4 **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 8-1 を参照してください。
<i>max-services</i>	Guard がピックアップして特定のポリシー テンプレートからポリシーを構築する対象となるサービスの最大数。 Guard モジュールが現在の値を変更しないように防止するには、-1 を入力します。 詳細については、P.8-9 の「サービスの最大数の設定」を参照してください。
<i>min-threshold</i>	Guard モジュールでサービスをランク付けするために超える必要のある最小しきい値。 Guard モジュールが現在の値を変更しないように防止するには、-1 を入力します。 詳細については、P.8-11 の「最小しきい値の設定」を参照してください。

表 8-4 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.8-11 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.8-11 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@GUARD-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](#)
- [保護モジュール](#)
- [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、Guard モジュールは、より限定的なポリシーを使用してフローを分析します。サービス *any* は、同じポリシー テンプレートから作成された他のサービスと特に一致しないすべてのトラフィックに関連します。

ゾーンの主要サービスに対して最適に調整された保護が可能になるよう、特定のポリシーを定義することをお勧めします。



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。

ゾーンのポリシーにサービスを追加または削除すると、Guard モジュールはゾーンのポリシーを未調整としてマークします。ゾーンが保護およびラーニング動作状態にある場合、次のいずれかの操作が実行されるまで、Guard モジュールはゾーントラフィック内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.6-19](#) の「[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.6-27](#) の「[ポリシーへの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るので、より限定的なポリシーを作成できます。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。このしきい値は手動で定義することもできますが、しきい値調整フェーズを実行し（詳細については、[P.6-19](#)の「[しきい値の調整](#)」を参照）、ポリシーをゾーンのトラフィックに合わ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` : 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）。

■ ポリシー パスのセクションについて

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 8-5 で、**policy-template** コマンドの引数について説明します。

表 8-5 **policy-template** 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 8-2 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。

次の例を参考にしてください。

```
user@GUARD-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。Guard モジュールは、特定のポリシー テンプレートで作成されたすべてのポリシーからサービスを削除します。

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 8-6 で、**remove-service** コマンドの引数について説明します。

表 8-6 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 8-2 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、Guard 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、ゾーンの保護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@GUARD-conf-zone-scannet-policy_template-tcp_services# remove-service 25
```

保護モジュール

保護モジュール セクションは、Guard モジュールがトラフィック フローの処理に使用する保護モジュールを示します。このセクションは情報提供用で、保護モジュールを設定することはできません。Guard モジュールには、次の 3 つの保護モジュールがあります。

- **分析**: この保護モジュールでは、トラフィック フローが介入なしで流れます。
- **基本**: この保護モジュールでは、Guard モジュールの基本的なスプーフィング防止メカニズムが適用されます。Guard モジュールは、各ホストに対して認証を行います。認証は事前に定義された期間で有効です。この期間が経過すると、Guard モジュールはもう一度ホストを認証します。
- **強化**: この保護モジュールでは、Guard モジュールの強力なスプーフィング防止メカニズムが適用されます。Guard モジュールは、各接続に対して認証を行います。

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

パケット タイプ

パケット タイプ セクションは、Guard 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
- Guard 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 Guard 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 8-7 で、Guard モジュールが監視するパケット タイプについて説明します。

表 8-7 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。
num_sources	Guard のスプーフィング防止メカニズムによって認証された、ゾーン宛ての TCP 送信元 IP アドレスを持つパケットの数。
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。Guard モジュールは SYN フラグの付いたパケット数と FIN フラグの付いたパケット数の比率を確認します。
unauth_pkts	TCP ハンドシェイクを経なかったパケット。
pkts	同じ保護レベルの他のどのカテゴリにも入らないすべてのパケット タイプ。

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、保護モジュール、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 8-8 で、Guard 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 8-8 **トラフィック特性**

トラフィック特性	簡単な説明
<code>dst_ip</code>	ゾーンの IP アドレス宛てのトラフィック。
<code>dst_ip_ratio</code>	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。
<code>dst_port</code>	特定のゾーン ポート宛てのトラフィック。
<code>dst_port_ratio</code>	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。
<code>global</code>	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。
<code>protocol</code>	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。
<code>src_ip</code>	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。
<code>src_ip_many_dst_ips</code>	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 スキャンングに使用されます。
<code>src_ip_many_ports</code>	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 スキャン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.8-2](#) 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@GUARD-conf-zone-scannet# policy dns_tcp/53/analysis/syns/global  
user@GUARD-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.8-22](#) 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.8-23](#) 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.8-30](#) の「[ポリシーのタイムアウトの設定](#)」を参照してください。
- ポリシーのアクション：[P.8-31](#) 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 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 : P.8-32 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 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。

Guard 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 Guard モジュールによってワイルドカード (*) と見なされます。

たとえば、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

Guard 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** : ポリシーはトラフィックに関連付けられ、しきい値を超過した場合にアクションを実行します。
- **Inactive** : ポリシーはトラフィックに関連付けられ、しきい値を取得しますが、しきい値を超過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なる必要はありません。
- **Disabled** : ポリシーがトラフィック フローに関連付けられないため、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、Guard モジュールでポリシーの正しいしきい値を監視する必要があります。



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、ゾーン保護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@GUARD-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、Guard モジュールのポリシーが保護の役割を担わなくなり、ゾーンの保護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、ポリシーはゾーンを保護するアクションを実行します。しきい値は、デフォルトで、オンデマンド保護に適する値に設定されています。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。

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.8-24 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 : Guard モジュールは現在のポリシーのしきい値に係数を掛けます。新しい値を固定値として設定しない場合、後続のしきい値調整フェーズでこの値が変更されることがあります。P.8-27 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 : Guard モジュールはゾーンのアドレス範囲内にある特定の IP 送信元アドレスのしきい値を設定します。P.8-28 の「[特定の IP しきい値の設定](#)」を参照してください。
- プロキシしきい値を設定する : Guard モジュールは、プロキシを介して HTTP でゾーンに接続するクライアントのトラフィックのしきい値を設定します。P.8-29 の「[プロキシしきい値の設定](#)」を参照してください。

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

- 固定値としてしきい値を設定する : Guard 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 (proxy-threshold および threshold-list) を変更しません。P.8-25 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 : Guard モジュールは、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、後続のしきい値調整フェーズでポリシーのしきい値を計算します。P.8-26 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 policy dns_tcp/53/analysis/syns/global のしきい値を 300 に設定する方法を示しています。

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


固定値としてのしきい値の設定

ポリシーのしきい値 (`proxy-threshold` および `threshold-list`) を固定値として設定できます。Guard 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@GUARD-conf-zone-scannet-policy-/dns_tcp/53/analysis/syns/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.8-2](#) 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@GUARD-conf-zone-scannet# policy dns_tcp learning-params fixed-threshold
```

ポリシーのラーニング パラメータを表示するには、ポリシー設定モードで **show learning-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。Guard 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。Guard モジュールは設定された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.6-26 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 8-9 で、**learning-params threshold-multiplier** コマンドの引数について説明します。

表 8-9 learning-params threshold-multiplier コマンドの引数

パラメータ	説明
<i>policy-path</i>	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.8-2 の「ポリシー パス構造」を参照してください。
<i>threshold-multiplier</i>	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@GUARD-conf-zone-scanner# 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。Guard 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 8-10 で、**policy thresh-mult** コマンドの引数について説明します。

表 8-10 policy thresh-mult コマンドの引数

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 8-2 を参照してください。
<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。

次の例を参考にしてください。

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

しきい値は、Guard モジュールによって後続のしきい値調整フェーズで変更される場合があります。Guard モジュールによって、しきい値が後続のしきい値ラーニング フェーズで変更されないようにするには、しきい値を固定値として設定します。P.8-25 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。

次のポリシーだけに、特定の IP しきい値を設定できます。

- トラフィック特性が宛先 IP (`dst_ip`) であるポリシー。
- デフォルト ポリシーアクションが `drop` である、トラフィック特性が送信元 IP (`src_ip`) アドレスのポリシー。デフォルト ポリシーアクションは、新しいゾーンを作成するときにポリシーが持っているアクションです。これらのポリシーには、ポリシーアクションを変更する場合でもしきい値のリストを設定できます。

特定の IP しきい値を設定するには、次のコマンドを入力します。

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

表 8-11 で、**policy threshold-list** コマンドの引数について説明します。

表 8-11 policy threshold-list コマンドの引数

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 8-2 を参照してください。
<i>ip</i>	特定の IP アドレス。
<i>threshold</i>	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` に設定されている場合、Guard モジュールによって、ポリシーのしきい値が後続のしきい値調整フェーズで変更される場合があります (P.6-26 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@GUARD-conf-zone-scannet-policy-/http/80/analysis/syns/src_ip#  
threshold-list 10.10.10.2 500 10.10.15.2 500
```

プロキシしきい値の設定

プロキシしきい値パラメータは、プロキシを介して HTTP でゾーンに接続するクライアントのトラフィック レートを定義します。プロキシしきい値により、Guard モジュールおよびユーザは、ポリシーをさまざまな送信元からのトラフィック量に適合させることができます。Guard モジュールはトラフィックをブロックするためだけにプロキシしきい値を使用します。したがってユーザは、強化保護モジュールを持つ、DEFAULT ゾーン テンプレート内のポリシー、および基本保護モジュールを持つ、TCP_NO_PROXY ゾーン テンプレート内のポリシーだけにプロキシしきい値を設定できます。

プロキシしきい値は、`http`、`http_ns`、`tcp_connections`、および `tcp_connections_ns` のポリシーだけに使用できます。ゾーンにアクティブな `http` または `http_ns` ポリシーがある場合にだけ、`tcp_connections` または `tcp_connections_ns` ポリシー テンプレートから作成されたポリシーのプロキシしきい値が有効になります。

プロキシしきい値を設定するには、次のコマンドを入力します。

proxy-threshold proxy-threshold

`proxy-threshold` 引数には、`http` ポリシーおよび `http_ns` ポリシーのプロキシしきい値のトラフィック レート (pps) を指定します。この引数は、`tcp_connections` ポリシーおよび `tcp_connections_ns` ポリシーの接続数でプロキシしきい値を指定します。

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

■ ポリシー パラメータの設定

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

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

ポリシーのタイムアウトの設定

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。

タイムアウト期限が満了すると、Guard はプロセスを実行して、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。Guard が動的フィルタを非アクティブにしないと決定した場合、フィルタのアクティベーションタイムアウトが新たにゼロから再びカウントされます。動的フィルタの非アクティベーションの基準を変更するには、**filter-termination** コマンドを使用します。詳細については、[P.7-38 の「動的フィルタの非アクティブ化」](#)を参照してください。

ポリシーのタイムアウトを設定するには、次のコマンドを入力します。

```
timeout {forever | timeout}
```

[表 8-12](#) 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 8-12 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。この場合、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 8-13 で、ポリシーのアクションについて説明します。

表 8-13 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
block-unauthenticated	事前ハンドシェイクなしの ACK など、スプーフイング防止メカニズムによって認証されなかったトラフィックをブロックするフィルタを追加します。
filter/strong	トラフィックを強化保護モジュール メカニズムに誘導するフィルタを追加します。
to-user-filters	トラフィックをユーザ フィルタに誘導するフィルタを追加します。
filter/drop	特定のトラフィックをドロップするように Guard モジュールを誘導するフィルタを追加します。
redirect/zombie	redirect というアクションを持つすべてのユーザ フィルタの認証機能を強化するフィルタを追加します。
notify	しきい値を超過するとユーザに通知します。

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。



(注)

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

次の例は、*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@GUARD-conf-zone-scannet# policy dns_tcp/ set-action filter/drop
set action of dns_tcp/ to filter/drop:
16 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、保護をイネーブルにし、ゾーンがインタラクティブ保護モードである場合にのみゾーンに適用できます。詳細については、[第 9 章「インタラクティブ保護モード」](#)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 8-14](#) で、**interactive-status** コマンドのキーワードについて説明します。

表 8-14 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。 Guard 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。 Guard 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。 Guard 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@GUARD-conf-zone-scannet-policy-/dns_tcp/53/analysis/pkts/src_ip#  
interactive-status always-accept
```

ポリシーの監視

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

この項では、次のトピックについて取り上げます。

- [ポリシーの表示](#)
- [ポリシーの統計情報の表示](#)

ポリシーの表示

ゾーンのポリシーを表示して、ポリシーがゾーンのトラフィック特性に適しているかどうかを確認できます。ゾーンに構築されたポリシーを表示して、これらのポリシーがゾーンのトラフィックの特性に合わ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せん。

Guard モジュールは、現在のゾーン ポリシーだけを表示します。ポリシー構築フェーズ中にポリシー テンプレートがディセーブルであった場合、Guard モジュールはそのポリシー テンプレートからポリシーを作成しないため、**show policies** コマンドを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.8-2](#)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 8-15](#) 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 8-15 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.8-2 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.8-22 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.8-32 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、Guard モジュールはアクションを実行してゾーンを保護します。詳細については、P.8-23 の「ポリシーのしきい値の設定」を参照してください。
Proxy	ポリシーのプロキシしきい値を示します。詳細については、P.8-29 の「プロキシしきい値の設定」を参照してください。
List	ポリシーに定義されている特定の IP しきい値の数を示します。詳細については、P.8-28 の「特定の IP しきい値の設定」を参照してください。
Action	しきい値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.8-31 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。Guard モジュールは、フィルタの終了しきい値に従って、その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決定します。詳細については、P.8-30 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。Guard モジュールは、ゾーンに転送されたトラフィック フローの中で、ポリシーによって測定された最も高いレートを持ついくつかのトラフィック フローを表示します。レートは、トラフィックのサンプルに基づいて計算されます。

ポリシーの統計情報を表示するには、次のコマンドを入力します。

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

表 8-16 で、**show policies statistics** コマンド出力の引数について説明します。

表 8-16 show policies statistics コマンドの引数

パラメータ	説明
<i>policy-path</i>	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.8-2 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。
<i>num-entries</i>	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。Guard モジュールは、最大の値を持つポリシーを表示します。

Guard 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。

表 8-17 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 8-17 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	<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、ポリシー <code>tcp_services/any/analysis/syns/dst_ip</code> 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 N/A と表示されます。</p> <p>詳細については、表 8-7 を参照してください。</p>
Policy	<p>ポリシー名を示します。詳細については、P.8-2 の「ポリシーパス構造」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。</p>
Connection	<p>同時接続の数を示します。この情報は、<code>tcp_connections</code> 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。</p> <ul style="list-style-type: none"> <code>in_nodata_conns</code> : 分析保護モジュールの場合 <code>in_conns</code> : 強化保護モジュールの場合
Ratio	<p>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、<code>syn_by_fin</code> ポリシーだけで使用できます。</p>



(注) Guard 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。

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取得するか、または Guard モジュールを自動的に指定した間隔でスナップショットを取得するように設定できます。Guard モジュールは、各ゾーンにスナップショットを 100 個まで保存します。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 つ保存することができます。または、自動的に指定した間隔でスナップショットを取得するように Guard モジュールを設定できます。Guard 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。

自動的に指定した間隔でスナップショットを取得するように Guard モジュールを設定する方法の詳細については、[P.6-25](#) 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 8-18 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 8-18 snapshot コマンドの引数とキーワード

パラメータ	説明
threshold-selection	Guard モジュールがスナップショットのしきい値の計算に使用する方式を設定します。デフォルトでは、Guard モジュールは learning-params threshold-selection コマンドで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	Guard 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	Guard モジュールは、ポリシーの現在のしきい値とラーニング済みのしきい値とを比較し、2 つのうちで大きな方の値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	Guard モジュールは、保存するポリシーしきい値を次の式に基づいて計算します。 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	Guard 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、現在のポリシー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。

■ 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

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。

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、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@GUARD-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 8-19 で、**diff** コマンドの引数について説明します。

表 8-19 diff コマンドの引数

パラメータ	説明
<i>snapshot-id</i>	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。
<i>percent</i>	(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@GUARD-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@GUARD-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。

■ 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

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 8-20 で、**diff** コマンドの引数について説明します。

表 8-20 diff コマンドの引数

パラメータ	説明
<i>zone-name</i>	比較対象のラーニング パラメータを持つゾーンの名前。
<i>percent</i>	(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@GUARD# 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 8-21 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 8-21 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。
<i>snapshot-id</i>	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。
<i>policy-path</i>	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.8-2 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@GUARD-conf-zone-scannet# show snapshots
ID    Time
1     Feb 10 10:32:04
2     Feb 10 10:49:12
user@GUARD-conf-zone-scannet# show snapshots 2 policies dns_tcp
```

show zone zone-name snapshots snapshot-id policies policy-path コマンドの出力のフィールドは、**show policies** コマンドの出力のフィールドと同じです。詳細については、P.8-34 の「[ポリシーの表示](#)」を参照してください。

表 8-22 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 8-22 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。Guard モジュールは、既存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 8-23 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 8-23 copy-policies コマンドの引数とキーワード

パラメータ	説明
<i>snapshot-id</i>	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。
<i>src-zone-name</i>	サービス ポリシーのコピー元のゾーン名。
<i>service-path</i>	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。 <ul style="list-style-type: none"> • 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@GUARD-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@GUARD-conf-zone-scannet# show snapshots
ID    Time
1     Feb 10 10:32:04
2     Feb 10 10:49:12
user@GUARD-conf-zone-scannet# copy-policies 2
```

■ 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