ポリシー テンプレートとポリシーの設定

この章では、Guard のポリシーとポリシー構造について説明します。また、ポリシー 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。

- Guard のポリシー
- ポリシー テンプレート
- ポリシーのセクション
- ポリシーの設定
- スナップショットの作成とポリシーの比較
- ポリシーの監視

Guard のポリシー

ポリシーは、Guard 統計エンジンの構成要素です。ポリシーは、特定のトラフィック フローを測定し、しきい値超過が発生した場合にフローに対してアクションを実行するメカニズムです。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 がゾーンのトラフィックと比較する基礎となります。

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 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。Detector は、定義済みのポリシー テンプレートを使用します。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 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。

ポリシー構造

Guard 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 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 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 7-1 に、ポリシー名の例を示します。

図 7-1　ポリシー名

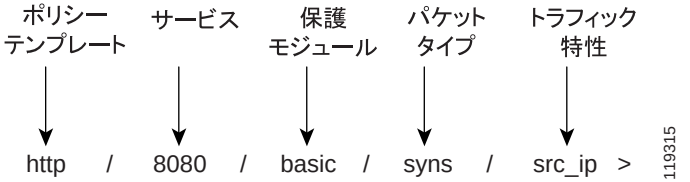

表 7-1 で、ポリシー名のセクションについて詳しく説明します。

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	ポリシーの生成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 が必要とする保護面を扱います。詳細については、P.7-5 の「ポリシー テンプレート」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.7-13 の「サービス」を参照してください。
保護モジュール	Guard 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.7-15 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 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.7-16 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 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.7-17 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 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.7-18 の「ポリシーの設定」を参照してください。

ポリシーの作成

Guard 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 Guard はゾーンのトラフィックをラーニングし、特定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 のポリシー テンプレートを使用して、ゾーンのポリシーが作成されます。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、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が調整されます。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.5-11 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

ポリシー テンプレートはポリシー構築の指針となる規則の集まりで、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）やアプリケーション（http など）や目的（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。DEFAULT ゾーン テンプレートでゾーンを定義する場合、Guard によってこのようなポリシー テンプレートが使用されます。

表 7-2 で、Guard のポリシー テンプレートについて説明します。

表 7-2　ポリシー テンプレート

ポリシー テンプレート	簡単な説明
dns_tcp	DNS-TCP プロトコル トラフィックに関連するポリシーのグループを生成します。
dns_udp	DNS-UDP プロトコル トラフィックに関連するポリシーのグループを生成します。
fragments	断片化されたトラフィックに関連するポリシーのグループを生成します。
http	デフォルトでポート 80（またはユーザによって設定された他のポート）を通過する HTTP トラフィックに関連するポリシーのグループを生成します。

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	簡単な説明
ip_scan	IP スキャニング（送信元 IP がゾーン内の多くの宛先 IP にアクセスしようとする状況）に関連するポリシーのグループを生成します。このポリシー テンプレートは、ゾーンがサブネットとして定義されてい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です。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。 これらのポリシーはリソースを多く消費し、パフォーマンスに影響を及ぼす可能性があるため、注意して使用する必要があります。
other_protocols	TCP と UDP 以外のプロトコルに関連するポリシーのグループを生成します。
port_scan	ポート スキャニング（送信元 IP がゾーン上の多くのポートにアクセスしようとする状況）に関連するポリシーのグループを生成します。 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です。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。 これらのポリシーはリソースを多く消費し、パフォーマンスに影響を及ぼす可能性があるため、注意して使用する必要があります。
tcp_connections	TCP 接続の特性に関連するポリシーのグループを生成します。
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 接続に関連するポリシーのグループを生成します。
tcp_outgoing	ゾーンによって開始された TCP 接続に関連するポリシーのセットを生成します。

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	簡単な説明
tcp_ratio	異なるタイプの TCP パケット間の比率に関連するポリシーのセットを生成します。たとえば、SYN パケット対 FIN/RST パケットなど。
tcp_services	HTTP 関連（ポート 80 や 8080 など）以外のポート上の TCP サービスに関連するポリシーのグループを生成します。
tcp_services_ns	TCP サービスに関連するポリシーのグループを生成します。デフォルトでは、このポリシーは IRC ポート（666X）、ssh、および telnet に関連します。このポリシー テンプレートは、トラフィック フローを強化保護モジュールに誘導するアクションを持つポリシーを作成しません。
udp_services	UDP サービスに関連するポリシーのグループを生成します。

（注）　Cisco 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関連します。

- これらのポート上でトラフィックがトレースされる場合、tcp_services_ns ポリシー テンプレートはそのポリシー グループを生成し、tcp_services ポリシー テンプレートは他のポート上の TCP サービスに関連します。
- 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。
- このポリシーにサービスを追加できます。

Cisco Guard には、TCP プロキシのスプーフィング防止が使用され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、このようなテンプレートを使用できます。

TCP_NO_PROXY ゾーン テンプレートでゾーンを定義する場合、Guard によって、表 7-3 で説明するポリシー テンプレートが使用されます。Guard は、http、tcp_connections、および tcp_outgoing のポリシーをそれぞれ http_ns、tcp_connections_ns、および tcp_outgoing_ns のポリシーに置き換えます。

表 7-3 で、TCP_NO_PROXY 用の Guard ポリシーについて説明します。

表 7-3　Guard TCP_NO_PROXY 用の ポリシー

ポリシー テンプレート	簡単な説明
tcp_connections_ns	TCP 接続の特性に関連するポリシーのグループを生成します。ただし、このポリシー テンプレートは、トラフィック フローを強化保護モジュールに誘導するアクションを持つポリシーを作成しません。
tcp_outgoing_ns	ゾーンによって開始された TCP 接続に関連するポリシーのグループを生成します。ただし、このポリシー テンプレートは、トラフィック フローを強化保護モジュールに誘導するアクションを持つポリシーを作成しません。
http_ns	デフォルトでポート 80（またはユーザによって設定された他のポート）を通過する HTTP トラフィックに関連するポリシーのグループを生成します。ただし、このポリシー テンプレートは、トラフィック フローを強化保護モジュールに誘導するアクションを持つポリシーを作成しません。

ヒント　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 プロンプトでコマンド **policy-template** 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 フェーズ中、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。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 フローを処理する追加のポリシーを作成するものもあります。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：指定したポリシー テンプレートから Guard によって生成されるポリシーの最大数を定義します。
- 最小しきい値：Guard でサービスをランク付けするために超える必要のある最小しきい値を定義します。
- ポリシー テンプレートの状態：Guard が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 テンプレート設定コマンド モードに入ります。次のように入力します。

policy-template *policy-template-name*

引数 *policy-template-name* には、目的のポリシー 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、Guard 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。

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

（注）　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 プロンプトで **show**　コマンドを使用してください。

サービスの最大数

このパラメータは、指定したポリシー テンプレートでポリシーが作成されるサービスの最大数を定義します。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、tcp_services など、サービスを検出するポリシー テンプレートだけに定義できます。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。

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、次のように入力します。

max-services *max-services*

引数 *max-services* は、サービスの最大数を定義する整数です。

（注）　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。

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

最小しきい値

このパラメータは、サービスの最小トラフィック量のしきい値を定義します。このしきい値を超えると、Guard 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生成します。

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生成するポリシー 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。

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、次のように入力します。

min-threshold *min-threshold*

引数 *min-threshold* は、最小しきい値レート（pps）を定義する整数です。同時接続および syn/fin 比率を測定する場合、しきい値は接続の合計数です。

次の例を参考にしてください。

```
admin@GUARD-conf-zone-scannet-policy_template-http# min-threshold 12
```

ポリシー テンプレートの状態

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。そのため、保護に大きな支障をきたす恐れがあります。

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。次のように入力します。

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

表 7-4 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 7-4　policy-template コマンドの引数とキーワード

パラメータ	説明
policy-template-name	ポリシー テンプレート名。詳細については、表 7-1 を参照してください。
max-services	指定したポリシー テンプレートから Guard によって生成されるポリシーの最大数。詳細については、P.7-10 の「サービスの最大数」を参照してください。
min-threshold	Guard 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。詳細については、P.7-11 の「最小しきい値」を参照してください。
disabled	ポリシー テンプレートをディセーブルにして、ポリシーが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」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」を参照してください。

（注）　Guard が現在の値を変更しないようにするには、max-services または min-threshold パラメータに -1 という値を入力してください。

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。

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

ポリシーのセクション

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
- 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

このセクションは、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 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。

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。

サービスの追加

ポリシー構築フェーズで検出されたサービス以外のサービスをポリシー テンプレートに追加して、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、指定したポリシー テンプレートから作成されたすべてのポリシーに追加されます。新しいサービスは、デフォルト値で定義されます。しきい値を手動で定義できます。ただし、しきい値調整フェーズを実行し（詳細については、P.5-15 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。

次のポリシー テンプレートに新しいサービスを追加できます。

- http
- other protocols
- tcp_services
- tcp_services_ns
- udp_services

（注）　http、tcp_services、tcp_services_ns、および udp_services の場合、追加するサービスはポート番号を指定します。other_protocols の場合、追加するサービスはプロトコル番号を指定します。

サービスを追加するには、ポリシー テンプレート プロンプトで次のように入力します。

add-service *service-num*

または

ゾーン プロンプトで次のように入力します。

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

表 7-5 で、**policy-template** コマンドの引数について説明します。

表 7-5　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。

```
admin@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。

ポリシーからサービスを削除するには、ポリシー テンプレート プロンプトで次のように入力します。

remove-service *service-num*

または

ゾーン プロンプトで次のように入力します。

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

policy-template コマンドの引数については、表 7-5 を参照してください。

（注）　サービスを削除すると、Guard 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。

次の例を参考にしてください。

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

保護モジュール

このセクションは、Guard 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 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 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。
- **強化**：この保護モジュールでは、Guard 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。

メカニズムをアクティブにした後、Guard は引き続きトラフィックを分析します。Guard は、ゾーン宛てのクリーンな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

このセクションは、Guard 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 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 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 7-6 で、Guard が監視するパケット タイプについて説明します。

表 7-6　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 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。
syns	同期パケット。つまり、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。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

このセクションは、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、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。

表 7-7 で、Guard が監視するトラフィック特性について説明します。

表 7-7　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_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。
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。
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_net	送信元サブネット 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。
dst_port	特定のゾーン ポート宛てのトラフィック。
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。
src_ip_many_dst_ips	これは、IP スキャニングに使用されるキーです。1 つの IP から多くのゾーン IP アドレスに宛てたトラフィック。
src_ip_many_ports	これは、ポート スキャニングに使用されるキーです。1 つの IP から多くのゾーン ポートに宛てたトラフィック。

ポリシーの設定

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の判断に役立ちます。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 パス プロンプトで **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 プロンプトで次のように入力します。

policy *policy-path*

引数 *policy-path* には、ポリシー パス セクションを指定します。詳細については、P.7-2 の「ポリシー構造」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。

```
admin@GUARD-conf-zone-scannet# policy dns_tcp/*/analysis/syns/global
admin@GUARD-conf-zone-scannet-policy-/dns_tcp/*/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.7-20 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.7-21 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.7-24 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.7-25 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.7-26 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、およびしきい値は、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。高レベルのポリシー 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。

ヒント　Guard では、コマンド **show policies details** および **show policies statistics** 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 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。

すべてのポリシー パラメータの同時設定

1 つのコマンドですべてのポリシー パラメータを設定できます。ゾーン プロンプトで次のように入力します。

policy *policy-path threshold action timeout state* [*proxy-threshold*]

表 7-8 で、**policy** コマンドの引数について説明します。

表 7-8　policy コマンドの引数

パラメータ	説明
policy-path	ポリシー パス セクションです。詳細については、「ポリシー構造」を参照してください。
threshold	このしきい値を超えると、Guard がアクションを実行します。詳細については、P.7-21 の「ポリシーのしきい値の設定」を参照してください。
action	トラフィック超過の結果としてポリシーが実行するアクション。詳細については、P.7-25 の「アクションの設定」を参照してください。

表 7-8　policy コマンドの引数（続き）

パラメータ	説明
timeout	ポリシーのアクションが有効な最小期間。詳細については、P.7-24 の「タイムアウトの設定」を参照してください。
state	ポリシーの状態。詳細については、P.7-20 の「ポリシーの状態の変更」を参照してください。
proxy-threshold	プロキシしきい値。詳細については、P.7-24 の「プロキシしきい値の設定」を参照してください。

（注）　Guard が現在の値を変更しないようにするには、threshold、timeout、および proxy-threshold パラメータに **–1** を入力してください。

次の例では、ポリシー *dns_tcp/53/analysis/pkts/dst_ip* のパラメータを設定しています。しきい値が *300* に、ポリシーのタイムアウトが *360* 秒に、ポリシーのアクションが *filter/drop* に、ポリシーの状態が *active* に設定されます。

```
admin@GUARD-conf-zone-scannet# policy dns_tcp/53/analysis/pkts/dst_ip
300 filter/drop 360 active
```

ポリシーの状態の変更

Guard 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。したがって、ポリシーに適切なしきい値が適用されるようにするには、ポリシーが新しいしきい値調整ラーニング フェーズを経る必要があります。

注意　ポリシーがディセーブルになると、他のポリシーは、ディセーブルになったポリシーの対象トラフィックを自分達に属するとみなします。すべてのポリシーが新しいしきい値調整ラーニング フェーズを経てから、保護モードで適用されるよう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、関連するポリシー セクションに対して次のように入力します。

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

注意　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 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。この操作により、ポリシーが再度アクティブになることがあります。

次の例を参考にしてください。

```
admin@GUARD-conf-zone-scannet-policy-/dns_tcp/*/analysis/syns# state
disabled
```

ポリシーのしきい値の設定

このパラメータは、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。しきい値超過が発生すると、ポリシーはアクションを実行してゾーンを保護します。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ます。しきい値は、しきい値調整ラーニング フェーズで調整されます。次のポリシーを除いて、しきい値は packets per second（pps; パケット / 秒）で測定されます。

- **tcp_connections**：接続数で測定されます。
- **tcp_ratio**：比率で測定されます。

ポリシーのしきい値を設定するには、次のように入力します。

threshold *threshold*

引数 *threshold* には、ポリシーのしきい値を指定します。

次の例を参考にしてください。

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

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。

しきい値に係数を掛けるには、次のように入力します。

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

表 7-9 で、**policy thresh-mult** コマンドの引数について説明します。

表 7-9　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	しきい値に掛ける実数。

次の例を参考にしてください。

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

特定の IP しきい値の設定

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送信元　IP　または送信元サブネットで、アクションが drop であるポリシー。
- トラフィック特性が宛先 IP で、アクションが to-user-filters、strong、notify、または drop であるポリシー。

特定の IP しきい値を設定するには、次のように入力します。

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

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

表 7-10　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 5 つ設定できます。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。

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。

```
admin@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 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 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_connection、および tcp_connection_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_connection 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、次のように入力します。

proxy-threshold *proxy-threshold*

引数 *proxy-threshold* には、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。

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。

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

タイムアウトの設定

このパラメータは、ポリシーのアクションが有効な最小期間を定義します。タイムアウトになると、Guard は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ブ化タイムアウトが新たにゼロから再びカウントされます。詳細については、P.6-24 の「動的フィルタの非アクティブ化」を参照してください。

タイムアウトを設定するには、次のように入力します。

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

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

表 7-11　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。関連するゾーン プロンプトで **policy set-timeout** コマンドを使用します。

アクションの設定

このパラメータは、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、次のように入力します。

action *policy-action*

表 7-12 で、ポリシーのアクションについて説明します。

表 7-12　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	スプーフィ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	ドロップするトラフィックをドロップ保護モジュールに誘導するフィルタを追加します。

表 7-12　ポリシーのアクション（続き）

ポリシーのアクション	簡単な説明
notify	ユーザにしきい値超過を通知します。
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。

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、関連するゾーン プロンプトで **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。

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。

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

インタラクティブ ステータスの設定

このパラメータは、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、保護中にインタラクティブ モードのゾーンだけに適用できます。詳細については、第 8 章「インタラクティブ推奨モード」を参照してください。

インタラクティブ ステータスを設定するには、次のように入力します。

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

表 7-13 で、**interactive-status** コマンドのキーワードについて説明します。

表 7-13　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が自動的に受け入れられます。これは、推奨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 はこのような推奨事項を表示しません。
always-ignore	Guard は、このポリシーによって作成される動的フィルタを無視します。ポリシーは動的フィルタを生成しません。 Guard 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を、ユーザが決める必要があります。Guard 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。

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。

次の例を参考にしてください。

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

スナップショットの作成とポリシーの比較

ラーニング フェーズ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。Guard はこのデータを新しいゾーンとして保存します。スナップショットをゾーンまたは別のスナップショットと比較して、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。

Guard 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。

ヒント　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撮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、スナップショットをゾーンとして使用できます。

ポリシーを比較してラーニング プロセスの結果を確認するには、次の手順を実行します。

ステップ 1　ゾーンのラーニング パラメータのスナップショットを保存します。

（注）　**snapshot** コマンドは、ゾーンがラーニング フェーズである場合にだけ使用できます。

次のように入力します。

snapshot *zone-name new-zone-name*

表 7-14 で、**snapshot** コマンドの引数について説明します。

表 7-14　snapshot コマンドの引数

パラメータ	説明
zone-name	ラーニング パラメータが保存されるゾーンの名前。
new-zone-name	新しいゾーンの名前。Guard は、ラーニングした現在のポリシーとしきい値をこの名前で保存します。

スナップショットにより、新しいゾーンが作成されます。スナップショットのパラメータを確認した後、または 2 つのスナップショットを比較した後、スナップショットを削除できます。また、スナップショットを保持し、元のゾーンを削除することもできます。

ステップ 2　スナップショットのパラメータとゾーンのパラメータを比較して、ポリシー、サービス、およびしきい値の違いをトレースします。ゾーンは、スナップショットが撮られたベース ゾーンでも、別のゾーンでもかまいません。次のように入力します。

```
diff zone-name zone-name [percent]
```

表 7-15 で、**diff** コマンドの引数について説明します。

表 7-15　diff コマンドの引数

パラメータ	説明
zone-name	ラーニング パラメータが比較されるゾーンの名前。
percent	（オプション）Guard は、このパーセンテージを超えて異なるすべてのパラメータをトレースします。デフォルトは 100% で、Guard は比較対象ゾーンのすべての違いをトレースします。

次の例を参考にしてください。

```
admin@GUARD# snapshot scannet scannet-8am
```

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ソース ゾーンから現在のゾーンにコピーできます。このようにして、ラーニング 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。

注意　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てください。

ソース ゾーンからサービスをコピーするには、次のように入力します。

copy-services *src-zone-name* [*service-path*]

表 7-16 で、**copy-services** コマンドの引数とキーワードについて説明します。

表 7-16　copy-services コマンドの引数とキーワード

パラメータ	説明
src-zone-name	ポリシーのコピー元のゾーン名。
service-path	コピーするサービス。サービス パスの形式は、次のいずれかです。 • **policy-template**：ポリシー テンプレートから作成されたすべてのポリシーをコピーします。 • **policy-template/service-num**：ポリシー テンプレートから作成されたポリシーの中で、特定のサービスを持つポリシーをすべてコピーします。

デフォルトでは、すべてのポリシーがコピーされます。

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ポリシーを、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。

```
admin@GUARD-conf-zone-scannet# copy-services webnet tcp_connections/
```

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。

次の作業を行うことができます。

- 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できます。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します。リストのポリシーだけを設定できます。

ゾーンのポリシーを表示するには、次のように入力します。

show policies

（注）　Guard は、現在のゾーン ポリシーだけを表示します。ポリシー構築ラーニング 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 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、このコマンドを発行してもそのポリシーは表示されません。

表 7-17 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 7-17　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。詳細については、P.7-2 の「ポリシー構造」を参照してください。
State	ポリシーの状態。詳細については、P.7-20 の「ポリシーの状態の変更」を参照してください。

表 7-17　show policies コマンド出力のフィールド説明（続き）

フィールド	簡単な説明
IStatus	ポリシーのインタラクティブ ステータス。詳細については、P.7-26 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。
Threshold	ポリシーのしきい値。このしきい値を超えると、ゾーンを保護するために Guard がアクションを実行します。詳細については、P.7-21 の「ポリシーのしきい値の設定」を参照してください。
Proxy	ポリシーのプロキシしきい値。詳細については、P.7-24 の「プロキシしきい値の設定」を参照してください。
List	ポリシーに定義されている特定の IP しきい値の数。詳細については、P.7-23 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。詳細については、P.7-25 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。詳細については、P.7-24 の「タイムアウトの設定」を参照してください。

特定のポリシーの詳細を表示するには、**show policies details** コマンドを使用します。

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 は、ゾーンに転送されたトラフィック フローの中で、保護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。

（注）　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、次のように入力します。

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

表 7-18 で、**show policies statistics** コマンドの引数について説明します。

表 7-18　show policies statistics コマンドの引数

パラメータ	説明
policy-path	ポリシーのグループを定義します。詳細については、P.7-2 の「ポリシー構造」を参照してください。
num-entries	表示するエントリの数。Guard は、最大の値を持つポリシーを表示します。

Guard は、3 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 7-19 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 7-19　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	ポリシーの集約に使用されたトラフィック特性。たとえば、ポリシー *tcp_services/any/analysis/syns/dst_ip* の場合、キーは宛先 IP アドレスです。ポリシーの集約に使用されたトラフィック特性が global である場合、キーには N/A と表示されます。詳細については、表 7-6 を参照してください。
Policy	ポリシー名。詳細については、P.7-2 の「ポリシー構造」を参照してください。

表 7-19　show policies statistics コマンド出力テーブルのフィールド説明（続

テーブル	説明
1 つの出力テーブルのフィールド	
Rate	トラフィック レートを測定するポリシー。Guard は、ポリシーを通過するトラフィックのレートをパケット / 秒（pps）単位で表示します。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。
Connection	接続または送信元 IP アドレスの数を測定するポリシー。この情報は、ポリシー tcp_connections および次のパケット タイプで使用できます。 • **in_nodata_conns**：分析保護モジュールの場合 • **in_conns**：強化保護モジュールの場合
Ratio	フラグ付きのパケット間の比率を測定するポリシー。Guard は、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表示します。この情報は、syn_by_fin ポリシーだけで使用できます。

（注）　Guard は、データを含まないテーブルを表示しません。

例

admin@GUARD-conf-zone-scannet# **show policies statistics**

```
Key              Rate         Policy
192.168.100.34   1.29         tcp_not_auth/any/strong/pkts/dst_ip
N/A              1.29         tcp_not_auth/any/strong/pkts/global
192.168.100.44   0.03         http/80/basic/syns/src_ip
... ... ...

Key              Connections  Policy
... ... ...
192.168.100.35   1.91   tcp_connections/any/strong/in_conns/src_ip
N/A              1.91   tcp_connections/any/strong/in_conns/global
192.168.100.45   1.67   tcp_connections/any/strong/in_conns/src_ip
... ... ...
```