ゾーンのフィルタの設定

この章では、Guard のフィルタ システムの設定方法と、これらのフィルタを Guard のポリシーに適合させる方法について説明します。

この章には、次の項があります。

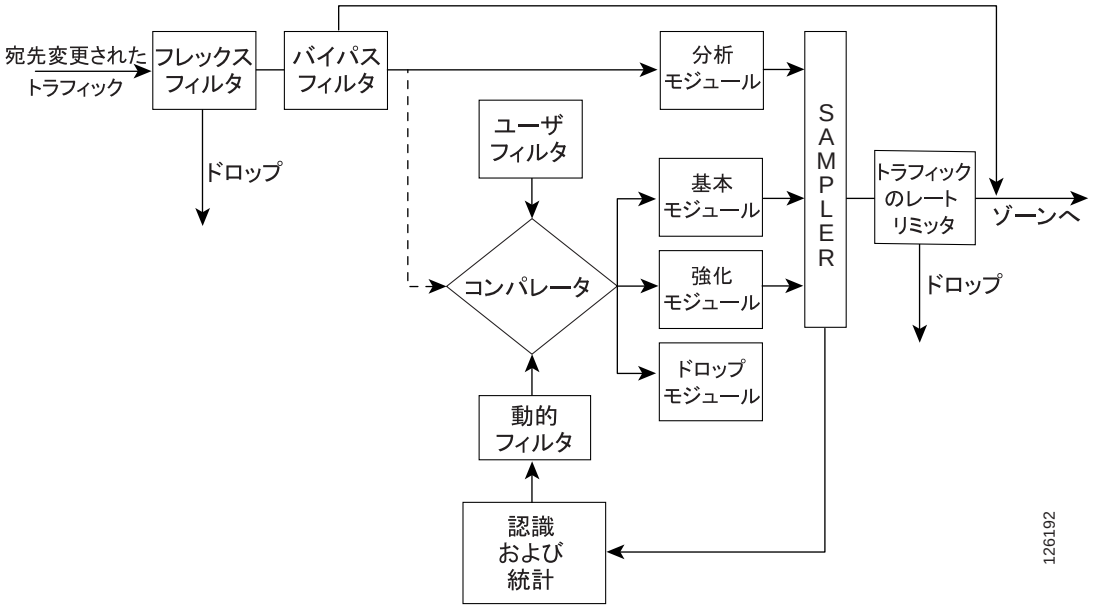
概要

ゾーンのフィルタは、宛先変更されたトラフィックを関連する保護モジュールに誘導するメカニズムです。Guard では、ユーザがフィルタを設定して、カスタマイズされたトラフィック誘導や DDoS 攻撃の防止メカニズムをさまざまに設計できるようになっています。

ゾーンのフィルタ設定の変更は、すぐに反映されます。

図 6-1 に、Guard のフィルタ システムを示します。

図 6-1　Guard のフィルタ システム



ユーザのアクションや、リモートのネットワーク検知 DDoS 要素（Cisco Traffic Anomaly Detector など）によって保護がアクティブになると、Guard はゾーンのトラフィックの宛先を変更します。異常または悪意のあるトラフィックが発見されない場合、トラフィックはゾーンのトラフィックを分析する分析モジュールに直接流れます。フレックス フィルタを使用することにより、Guard が特定のフローをカウントまたはドロップするように設定することができます。バイパス フィルタを使用すると、特定のフローが Guard の保護メカニズムをバイパスするように設定できます。

サンプルでは、トラフィックは認識モジュールに流れています。Guard は、トラフィックをレート リミッタに渡します。定義されたレートを超過したトラフィックは、ここでドロップされます。クリーンになったトラフィックは、再びゾーンに注入されます。

認識モジュールは、クローズド ループのフィードバック サイクルを制御して、Guard の保護措置を動的に変化するゾーンのトラフィック特性に合わせて調整します。Guard は、適切な保護方針を適用して、変化する DDoS 攻撃のタイプとトラフィック フローに対応します。

認識モジュールは、常にトラフィックのフローを測定しているポリシーで構成されます。ポリシーは、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。このようなアクションは、単なる通知の発行から、新しいフィルタ（動的フィルタ）の作成に及びます。

このようにして、Guard は Guard 内部のトラフィック フローを変更します。トラフィックは、破線で示されているように、コンパレータに流れます。コンパレータは、次のフィルタから入力を受け取ります。

- **動的フィルタ**：動的フィルタは、最初に Guard がユーザ フィルタの保護ガイドラインに従うようにします。この一連のフィルタは、ゾーンのトラフィックおよび特定の DDoS 攻撃に合わせて継続的に調整されます。
- **ユーザ フィルタ**：ユーザ フィルタは、デフォルトまたはユーザ定義の保護指示で構成されます。

攻撃時には、動的フィルタとユーザ フィルタの両方を追加できます。

コンパレータは、提案された中で最も厳格な保護措置を選択して、認証のためにトラフィックを関連する保護モジュールに誘導します。

動的フィルタは継続期間が限定されており、攻撃が終了すると消去されます。デフォルトでは、Guard はユーザによって非アクティブにされるまで保護モードのままです。使用されている動的フィルタがなくなり、事前に定義された期間に新しい動的フィルタが追加されなかった場合に、Guard が保護を停止するように設定することができます。詳細については、P.5-19 の「保護の終了の定義」を参照してください。

ユーザは、独自の 保護プリファレンスを定義し、次のフィルタを設定することができます。

- **ユーザ フィルタ**：ユーザ フィルタは、特定のトラフィック フローを関連する Guard の保護モジュールに誘導するために使用されます。ゾーンの設定には、デフォルトのユーザ フィルタのセットが含まれます。ユーザは、このフィルタのセットを変更することができます。詳細については、P.6-14 の「ユーザ フィルタの設定」を参照してください。
- **バイパス フィルタ**：バイパス フィルタは、特定のトラフィック フローが Guard の保護メカニズムによって処理されないようにする場合に使用します。詳細については、P.6-12 の「バイパス フィルタの設定」を参照してください。
- **フレックス フィルタ**：フレックス フィルタは、指定したパケット フローのカウントまたはドロップに使用します。これは、IP および TCP ヘッダーのフィールドに従ったフィルタリングや、コンテンツのバイト数に従ったフィルタリングのように、きわめて柔軟なフィルタ機能を提供するバークリー パケット フィルタです。複雑なブール式を使用できますが、フレックス フィルタを設定できるのはゾーンごとに 1 つだけです。詳細については、P.6-7 の「フレックス フィルタの設定」を参照してください。

フィルタのトラフィック フロー

フィルタが処理するフローを設定する必要があります。表 6-1 に、フィルタのフローの引数を説明します。

詳細については、「バイパス フィルタの設定」、「ユーザ フィルタの設定」、および「動的フィルタの設定」の各項を参照してください。

表 6-1　フィルタのフローの引数

パラメータ	説明
src-ip	特定の IP アドレスからのフローを処理します。**すべて**の場合は、* を入力します。
ip-mask	（オプション）特定のサブネットからのフローを処理します。マスクには、クラス C の値のみを指定できます。デフォルトのサブネットは、255.255.255.255 です。
protocol	特定のプロトコルのフローを処理します。**すべて**の場合は、* を入力します。
dest-port	特定の宛先ポートに向かうトラフィックを処理します。**すべて**の場合は、* を入力します。
fragments-type	（オプション）フィルタが断片化したトラフィックを処理するかどうかを指定します。断片化のタイプは、次のとおりです。 • **no-fragments**：断片化していないトラフィック • **fragments**：断片化したトラフィック • **any-fragments**：断片化したトラフィックと断片化していないトラフィック デフォルトは、**no-fragments** です。

表 6-2 に、フィルタの **show** コマンドのフィールドを説明します。

詳細については、「バイパス フィルタの表示」、「ユーザ フィルタの表示」、および「動的フィルタの表示」を参照してください。

表 6-2　フィルタの show コマンドのフィールドの説明

フィールド	説明
Source IP	フィルタが処理するトラフィックの送信元 IP アドレスを指定します。
Source Mask	フィルタが処理するトラフィックの送信元アドレスのマスクを指定します。
Proto	フィルタが処理するトラフィックのプロトコル番号を指定します。
DPort	フィルタが処理するトラフィックの宛先ポートを指定します。
Frg	フィルタが断片化したトラフィックを処理するかどうかを指定します。 • **yes**：フィルタは断片化したトラフィックを処理します。 • **no**：フィルタは断片化していないトラフィックを処理します。 • **any**：フィルタは、断片化したトラフィックと断片化していないトラフィックの両方を処理します。

送信元 IP アドレス、送信元アドレスのマスク、プロトコル番号、および宛先ポートは、特定のものでなくてもかまいません。アスタリスク（*）は、フィルタがすべてのフィールド値に対して動作するか、フィルタに複数の値が一致したことを示します。

フレックス フィルタの設定

フレックス フィルタは、豊富なフィルタリング機能を持つバークリー パケット フィルタです。フレックス フィルタは、目的のパケット フローをカウントまたはドロップし、トラフィックの特定の悪意ある送信元を明らかにするために使用します。多くのパラメータを持つこのフィルタはきわめて柔軟で、これを使用して特定のトラフィック フローを定義することができます。ただし、フレックス フィルタはリソースを消費するので、設定できるフィルタは 1 つだけです。フレックス フィルタの使用はパフォーマンスに影響を与える場合があるため、注意してください。

バークリー パケット フィルタの設定オプションの詳細な説明については、http://www.freesoft.org/CIE/Topics/56.htm を参照してください。

フレックス フィルタを設定するには、次のように入力します。

flex-filter {drop|count} *parameters*

フレックス フィルタを削除するには、このコマンドの **no** 形を使用します。

引数とキーワードは、次のとおりです。

- **count**：*parameters* によって指定されたフローをカウントします。
- **drop**：*parameters* によって指定されたフローをドロップします。
- *parameters*：フローを定義します。

設定の例については、P.6-10 の「フレックス フィルタの設定例」を参照してください。

表 6-3 に、フレックス フィルタのオプションのパラメータを説明します。

表 6-3　フレックス フィルタのオプションのパラメータ

パラメータ	説明
dst host *host_ip_address*	宛先ホスト IP アドレスへのトラフィック。
src host *host_ip_address*	送信元ホスト IP アドレスからのトラフィック。
host *host_ip_ address*	送信元および宛先の両方のホスト IP アドレスの間のトラフィック。
net *net* **mask** *mask*	特定のネットワークへのトラフィック。
net *net/len*	特定のサブネットへのトラフィック。
dst port *destination_port_number*	宛先ポート番号への TCP または UDP トラフィック。
src port *source_port_number*	送信元ポート番号からの TCP または UDP トラフィック。
port *port_number*	送信元および宛先の両方のポート番号間の TCP または UDP トラフィック。
less *packet_length*	特定のバイト長以下の長さを持つパケット。
greater *packet_length*	特定のバイト長以上の長さを持つパケット。
ip proto *protocol*	ICMP、UDP、または TCP のプロトコル番号を持つパケット。
ip broadcast	ブロードキャスト IP パケット。
ip multicast	マルチキャスト パケット。
ether proto *protocol*	IP、ARP、または RARP などの特定のプロトコル番号またはプロトコル名を持つイーサネット プロトコル パケット。
expr relop expr	特定の式に適合するトラフィック。詳細については、表 6-4 を参照してください。

表 6-4 に、フレックス フィルタの式のルールを説明します。

表 6-4　フレックス フィルタの式のルール

式のルール	
relop	>、<、>=、<=、=、!=
expr	整数の定数（標準の C 構文で表現されたもの）、通常のバイナリ演算子（+、-、*、/、&、|）、長さ演算子、および特殊なパケット データ アクセスで構成される算術式。パケット内のデータにアクセスするには、次の構文を使用します。 *proto* [*expr*: *size*]
proto	インデックス操作用のプロトコル層を指定します。指定可能な値は、**ether**、**ip**、**tcp**、**udp**、または **icmp** です。指定されたプロトコル層までの相対的なバイト オフセットは、expr で指定されます。引数 *size* はオプションです。目的のフィールドのバイト数を示し、1、2、または 4 になります。デフォルトは 1 です。引数 *len* には、パケットの長さを指定します。

次の方法により、プリミティブを組み合せることができます。

- プリミティブとオペレータを小カッコで囲んだグループ（小カッコはシェルの特殊文字であるため、エスケープする必要があります）。
- 否定：**!** または **not** を使用します。
- 連結：**&&** または **and** を使用します。
- 代替：|| または **or** を使用します。

否定は、最も高い優先度を持ちます。代替と連結の優先順位は同じで、左から右に関連付けられます。連結には、並置ではなく、明示的な **and** トークンが必要です。キーワードなしで識別子を指定した場合は、最後に指定されたキーワードが使用されます。

フレックス フィルタの設定例

次の例は、断片化されていないデータグラムと断片化されたデータグラムのフラグメント 0 のみをカウントする方法を示しています。このフィルタは、TCP と UDP のインデックス操作に暗黙的に適用されます。たとえば、tcp[0] は常に TCP ヘッダーの最初のバイトを意味し、中間のフラグメントの最初のバイトを意味することはありません。

```
admin@GUARD-conf-zone-scannet# flex-filter count ip[6:2]&0x1fff=0
```

次の例は、すべての TCP RST パケットをドロップする方法を示しています。

```
admin@GUARD-conf-zone-scannet# flex-filter drop tcp [13] & 4 != 0
```

次の例は、エコー要求およびエコー応答（ping）ではないすべての ICMP パケットをカウントする方法を示しています。

```
admin@GUARD-conf-zone-scannet# flex-filter count icmp[0] != 8 and
icmp[0] != 0
```

次の例は、ポート 80 を宛先とし、ポート 1000 を送信元としないすべての TCP パケットをカウントする方法を示しています。

```
admin@GUARD-conf-zone-scannet# flex-filter count tcp and dst port 80
and not src port 1000
```

フレックス フィルタの表示

フレックス フィルタは、ゾーンの設定の一部です。フレックス フィルタを表示するには、**show** コマンドまたは **show running-config** コマンドを使用します。

次の例を参考にしてください。

```
admin@GUARD-conf-zone-scannet# show
.
.
.
FLEX-FILTER: tcp and dst port 80 and not src port 1000
FLEX-FILTER ACTION: count
FLEX-FILTER COUNTER: 200
.
.
.
```

フレックス フィルタのカウンタは、そのフィルタで処理されたパケットの数を示します。

バイパス フィルタの設定

バイパス フィルタは、Guard の保護メカニズムからの除外という保護ポリシー上の判断をサポートするためのフィルタです。バイパス フィルタは、Guard の動的フィルタ、保護モジュール、およびレート リミッタで特定のトラフィック フローを処理しないようにする場合に使用します。たとえば、信頼されたトラフィック フローが、スプーフィング防止メカニズムやゾンビ防止メカニズムなどの Guard の保護モジュールをバイパスできるようにする場合があります。バイパス フィルタを使用すると、信頼されたトラフィックが Guard の保護メカニズムを通らないように誘導して、そのトラフィックを直接ゾーンに転送することができます。

（注）　バイパス　フィルタによって処理されたトラフィックは、レート　リミッタ　モジュールを通過しません。

バイパス フィルタを設定するには、次のように入力します。

bypass-filter *row-num* ***src-ip*** [***ip-mask***] ***protocol dest-port*** [***fragments-type***]

表 6-5 に、**bypass-filter** コマンドの引数とキーワードを示します。

表 6-5　bypass-filter コマンドの引数

パラメータ	説明
row-num	1 ～ 9,999 の固有な番号を割り当てます。行番号はフィルタの ID で、これによって複数のバイパス フィルタの優先順位が定義されます。Guard は、行番号の昇順でフィルタを操作します。
フローの引数とキーワード	*src-ip*、*ip-mask*、*protocol*、*dest-port*、および *fragments-type* の詳細については、表 6-1 を参照してください。

（注）　fragments-type と dest-port を両方指定することはできません。fragments-type を設定する場合は、dest-port に * を入力してください。

バイパス フィルタの表示

バイパス フィルタを表示するには、次のように入力します。

show bypass-filters

表 6-6 に、**show bypass-filters** コマンドの出力フィールドを示します。

表 6-6　show bypass-filters コマンドのフィールドの説明

フィールド	説明
Row	バイパス フィルタの優先順位を示します。
Filter flow	Source IP、Source Mask、Proto、DPort、Frg の詳細については、表 6-2 を参照してください。
RxRate (pps)	このフィルタについて測定されている現在のトラフィック レートをパケット / 秒（pps）で示します。

バイパス フィルタの削除

バイパス フィルタを削除するには、次の手順を実行します。

ステップ 1　バイパス フィルタのリストを表示し、削除するバイパス フィルタの行番号を確認します。詳細については、前の項、「バイパス フィルタの表示」を参照してください。

ステップ 2　フィルタを削除します。次のように入力します。

```
no bypass-filter row-num
```

引数 *row-num* には、バイパス フィルタの行番号を指定します。すべてのバイパス フィルタを削除するには、* を入力します。

次の例を参考にしてください。

```
admin@GUARD-conf-zone-scannet# no bypass-filter 10
```

ユーザ フィルタの設定

ユーザ フィルタは、ゾーン設定の一部で、DDoS 攻撃の疑いのあるトラフィックの処理方法を定義します。ユーザ フィルタは、Guard の保護をカスタマイズする機能を提供します。ユーザ フィルタを使用すると、攻撃が疑われる場合に特定のトラフィック フローを処理したり、トラフィック フローを関連保護モジュール（Guard のスプーフィング防止メカニズムやゾンビ防止メカニズムなど）に誘導またはドロップする際の指針となる規則を設定することができます。

表 6-7 に、ユーザ フィルタで実行可能なアクションを説明します。

ゾーンの設定には、オンデマンド保護を可能にするデフォルトのユーザ フィルタのセットが含まれます。Guard は、保護されているのゾーンを宛先とするトラフィックを継続的に分析します。Guard は、疑わしいトラフィックを発見すると保護サイクルを開始し、ユーザ フィルタを使用して疑わしいトラフィックをフィルタリングします。

ユーザ フィルタは、行番号の昇順でアクティブになります。したがって、新しいユーザ フィルタを追加する場合には、リストの適切な位置に配置することが重要です。

表 6-7　ユーザ フィルタのアクション

アクション	説明
permit	トラフィックが Guard のスプーフィング防止またはゾンビ防止の保護メカニズムを通らないように誘導する場合に使用します。このフィルタにはレート リミットとバースト リミットを設定することを推奨します。
basic/redirect	HTTP 経由のアプリケーションを認証する場合に使用します。
basic/reset	TCP（HTTP 以外）経由のアプリケーションを認証する場合に使用します。
basic/default	UDP トラフィックを認証する場合や、アクティブにするアクションが不明な場合に使用します。このアクションが指定されたユーザ フィルタは、フローを検査し、実行するアクションを決定します。
basic/dns-proxy	TCP DNS アプリケーションを認証する場合に使用します。

表 6-7　ユーザ フィルタのアクション（続き）

アクション	説明
basic/safe-reset	TCP 接続のリセットを許容しない TCP 経由アプリケーション（HTTP 以外）を認証する場合に使用します。
drop	トラフィック フローをドロップする場合に使用します。
strong	トラフィック フローの強化認証が必要な場合や、それまでのフィルタが該当アプリケーションに適していないと考えられる場合に使用します。認証は、各接続に対して行われます。Guard がプロキシの役割を果たすため、このフィルタは、ACL（アクセス コントロール リスト）を使用しているなど、ネットワークが IP アドレスに従って管理される場合には使用しません。

ユーザ フィルタを設定するには、次の手順を実行します。

ステップ 1　ユーザ フィルタのリストを表示して、リスト内で新しいフィルタを追加する位置を確認します。詳細については、P.6-17 の「ユーザ フィルタの表示」を参照してください。

ステップ 2　現在の行番号が連続したものである場合は、新しいユーザ フィルタを挿入できるようにユーザ フィルタの番号を順に増加させます。次のように入力します。

```
user-filter renumber [start [step]]
```

表 6-8 に、**user-filter renumber** コマンドの引数を示します。

表 6-8　user-filter renumber コマンドの引数

パラメータ	説明
start	（オプション）ユーザ フィルタ リストの新しい開始番号を示す 1 ～ 9,999 の整数。デフォルトは 10 です。
step	（オプション）ユーザ フィルタの各行番号の増分を指定する 1 ～ 999 の整数。デフォルトは 10 です。

ステップ 3　新しいユーザ フィルタを追加します。次のように入力します。

```
user-filter row-num filter-action src-ip [ip-mask] protocol dest-port
[fragments-type] [rate-limit rate burst units]
```

表 6-9 に、**user-filter** コマンドの引数を示します。

表 6-9　user-filter コマンドの引数とキーワード

パラメータ	説明
row-num	1 ～ 9,999 の固有な番号を割り当てます。行番号はフィルタの ID で、これによって複数のユーザ フィルタの優先順位が定義されます。Guard は、行番号の昇順でフィルタを操作します。
filter-action	フィルタが特定のトラフィック タイプに対して実行するアクションを示します。詳細については、表 6-6 を参照してください。
フローの引数とキーワード	*src-ip*、*ip-mask*、*protocol*、*dest-port*、および *fragments-type* の詳細については、表 6-1 を参照してください。
rate	レートの制限を指定する 64 より大きい整数。ユーザ フィルタは、トラフィックを指定されたレートに制限します。単位は、*units* パラメータで指定されます。デフォルトでは、フィルタのトラフィック レートは制限されません。レート リミットは、最大でバースト リミットの 10 倍まで指定可能です。
burst	トラフィックのバースト リミットを指定する 64 より大きい整数。単位は、レートの単位に応じて、ビット、キロビット、キロパケット、メガビット、またはパケットになります。バースト リミットは、最大でレート リミットの 8 倍まで指定可能です。
units	レート リミットの単位を指定します。次の単位を指定できます。 • **bps**：ビット / 秒 • **kbps**：キロビット / 秒 • **kpps**：キロパケット / 秒 • **mbps**：メガビット / 秒 • **pps**：パケット / 秒

次の例は、ユーザ フィルタの番号を 10 から開始してそれぞれ 5 ずつ変更し、行番号 *12* にユーザ フィルタを追加する方法を示しています。このフィルタは、プロトコルが *6*（TCP）で宛先ポート *25*（SMTP）に向かうすべての送信元 IP アドレスからのトラフィックを対象とします。また、このフィルタでは、フローは許可されますが、フロー レートとバースト サイズはそれぞれ *600* パケット / 秒（*pps*）と *400* パケットに制限されています。

```
admin@GUARD-conf-zone-scannet# user-filter renumber 10 5
admin@GUARD-conf-zone-scannet# user-filter 12 permit * 6 25 rate-limit
600 400 pps
```

ユーザ フィルタの表示

ユーザ フィルタは、ゾーンの設定の一部です。ユーザ フィルタを表示するには、ゾーンのプロンプトで、**show** コマンドまたは **show running-config** コマンドを使用します。

表 6-10 に、**show** コマンドの出力におけるユーザ フィルタのフィールドを説明します。

表 6-10　show コマンドにおけるユーザ フィルタのフィールドの説明

フィールド	説明
Row	ユーザ フィルタの優先順位を示します。
Filter flow	Source IP、Source Mask、Proto、DPort、Frg の詳細については、表 6-2 を参照してください。
RxRate (pps)	このフィルタについて測定されている現在のトラフィック レートをパケット / 秒（pps）で示します。
Action	フィルタが特定のトラフィック タイプに対して実行するアクションを示します。詳細については、表 6-6 を参照してください。
Rate	ユーザ フィルタで処理可能なトラフィック レートの制限を示します。レートは、*Units* フィールドで指定された単位で表示されます。

表 6-10　show コマンドにおけるユーザ フィルタのフィールドの説明（続き）

フィールド	説明
Burst	フィルタで特定のフローに対して許可されるトラフィックのバースト リミットを示します。単位は、*Units* フィールドで指定されるレートの単位に応じて、ビット、キロビット、キロパケット、メガビット、またはパケットになります。
Units	レートとバースト レートが表示される単位を示します。

ユーザ フィルタの削除

ユーザ フィルタを削除するには、次の手順を実行します。

ステップ 1　ユーザ フィルタのリストを表示し、削除するユーザ フィルタの行番号を確認します。詳細については、前の項、「ユーザ フィルタの表示」を参照してください。

ステップ 2　フィルタを削除します。次のように入力します。

no user-filter *row-num*

引数 *row-num* には、ユーザ フィルタの行番号を指定します。すべてのユーザ フィルタを削除するには、***** を入力します。

次の例を参考にしてください。

```
admin@GUARD-conf-zone-scannet# no user-filter *
```

注意　すべてのユーザ フィルタを削除する場合、ポリシーのアクションが to-user-filter（詳細については、第 7 章「ポリシー テンプレートとポリシーの設定」を参照）に設定されているときには、保護されていないトラフィックがゾーンに渡されます。

動的フィルタの設定

Guard は、トラフィックの異常を検出する中で宛先変更されたゾーンのトラフィックを分析します。フローがポリシーのしきい値を超過すると、異常が発見されます。ポリシーのしきい値違反を検出すると、Guard は結果を分析して、ゾーンのトラフィックと DDoS 攻撃のタイプに絶えず自身を適合させる一連のフィルタを作成します。このフィルタのセットは、動的フィルタで構成されます。

Guard は、フローを分析し、異常を処理するための追加の動的フィルタを作成し終わるまでの間、トラフィックをユーザ フィルタに誘導する最初の動的フィルタを作成します。動的フィルタとユーザ フィルタは、コンパレータに取り込まれます。コンパレータは、提案された中で最も厳格な保護措置を選択して、認証のためにトラフィックを関連する保護モジュールに誘導します。詳細については、P.6-2 の「概要」を参照してください。

ユーザは、動的フィルタにアクセスし、独自のニーズに合うように設定することができます。

表 6-11 に、動的フィルタで実行可能なさまざまなアクションを説明します。

表 6-11　動的フィルタのアクション

アクション	説明
to-user-filters	ユーザ フィルタにトラフィックを転送します。デフォルトのユーザ フィルタを変更した場合は、これらの動的フィルタを処理するユーザ フィルタが存在することを確認してください。
strong	特定のトラフィックにスプーフィング防止の強化保護メカニズムを適用します。
drop	トラフィックをドロップします。
block-unauthenticated-basic	基本のスプーフィング防止メカニズムで非認証と定義されたトラフィック フローをドロップします。
block-unauthenticated-strong	強化されたスプーフィング防止メカニズムで非認証と定義されたトラフィック フローをドロップします。

表 6-11　動的フィルタのアクション（続き）

アクション	説明
block-unauthenticated-dns	DNS のスプーフィング防止メカニズムで非認証と定義されたトラフィック フロー（DNS サーバに向かうもの）をドロップします。
redirect/zombie	**basic/redirect** のアクションが指定されたすべてのユーザ フィルタの認証を強化するフィルタを追加します。

動的フィルタがタイムアウトになると、Guard はその動的フィルタを非アクティブにするかどうかを判断します。Guard が動的フィルタを非アクティブにしないことを決定した場合は、次の期間に向けてそのフィルタのアクティベーション タイムアウトが再開されます。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。

動的フィルタを追加または削除し、ニーズに合わせて設定することができます。

動的フィルタを追加するには、次のように入力します。

dynamic-filter *action* {***exp-time***|**forever**} ***src-ip*** [***ip-mask***] ***protocol dest-port*** [***fragments-type***]

表 6-12 に、**dynamic-filter** コマンドの引数を示します。

表 6-12　dynamic-filter コマンドの引数とキーワード

パラメータ	説明
action	フィルタが特定のトラフィック フローに対して実行するアクション。詳細については、表 6-10 を参照してください。
exp-time	フィルタがアクティブである期間（秒単位）を指定する、1 ～ 3,000,000 の整数。
forever	フィルタは無限にアクティブになります。保護が終了すると、フィルタは削除されます。
フローの引数とキーワード	*src-ip*、*ip-mask*、*protocol*、*dest-port*、および *fragments-type* の詳細については、表 6-1 を参照してください。

動的フィルタは、すでに保護されているゾーンに対してのみ追加することができます。Guard は、ゾーンの保護が終了すると、そのゾーンの動的フィルタを削除します。

次の例を参考にしてください。

```
admin@GUARD-conf-zone-scannet# dynamic-filter to-user-filters 600
192.128.30.45 255.255.255.252 6 88 no-fragments
```

動的フィルタの表示

Guard によって作成された動的フィルタを表示するには、**show dynamic-filters** コマンドを使用します。このコマンドには、次のオプションが用意されています。

- **show dynamic-filters** [details] : すべての動的フィルタのリストを表示します。
- **show dynamic-filters** *dynamic-filter-id* [details] : 特定の動的フィルタを表示します。
- **show dynamic-filters sort** {action | exp-time | id | filter-rate} : すべての動的フィルタのソートされたリストを表示します。

（注）　保留中のフィルタを表示するには、**show recommendations** コマンドを使用します。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。

表 6-13 に、**show dynamic-filters** コマンドの引数を示します。

表 6-13　show dynamic-filters コマンドの引数とキーワード

パラメータ	説明
dynamic-filter-id	表示する特定の動的フィルタの識別番号（ID）。この整数は Guard によって割り当てられます。フィルタの ID を確認するには、すべての動的フィルタのリストを表示します。
details	動的フィルタの詳細情報を表示します。詳細情報には、攻撃フローに関する追加情報、トリガーとなるレート、およびそのフィルタを作成したポリシーなどがあります。

表 6-13　show dynamic-filters コマンドの引数とキーワード（続き）

パラメータ	説明
action	厳密度の最も高いもの（ドロップ）から低いもの（通知）まで、動的フィルタをアクション別に表示します。
exp-time	動的フィルタを有効期限の昇順で表示します。
id	動的フィルタを ID 番号の昇順で表示します。
filter-rate	動的フィルタをトリガーとなるレートの昇順で表示します。

（注）　Guard は、最大 1,000 個の動的フィルタを表示します。1,000 を超える動的フィルタがアクティブになっている場合は、ログ ファイルまたはゾーンのレポートで動的フィルタの完全なリストを確認してください。

次の例を参考にしてください。

```
admin@GUARD-conf-zone-scannet# show dynamic-filters 876 details
```

表 6-14 に、**show dynamic-filters** コマンドの出力フィールドを説明します。

表 6-14　show dynamic-filters コマンドのフィールドの説明

フィールド	説明
ID	フィルタの識別番号を示します。
Action	フィルタがトラフィック フローに対して実行するアクションを示します。詳細については、表 6-10 を参照してください。
Exp Time	フィルタがアクティブになっている時間を示します。この時間が経過すると、フィルタは **filter-termination** コマンドを使用して定義されたしきい値に従って削除される場合があります。
Filter flow	Source IP、Source Mask、Proto、DPort、Frg の詳細については、表 6-2 を参照してください。
RxRate (pps)	このフィルタについて測定されている現在のトラフィック レートをパケット / 秒（pps）で示します。

表 6-15 に、**show dynamic-filters details** コマンドの出力フィールドを説明します。

表 6-15　show dynamic-filters details コマンドのフィールドの説明

フィールド	説明
Attack flow	軽減が図られた攻撃フローの特性を示します。Dynamic Filters テーブルに表示される軽減が図られた攻撃フローの範囲は、攻撃フローの範囲より広い場合があります。たとえば、ポート 80 に対するスプーフィングを利用しない攻撃では、ポート 80 のトラフィックだけではなく、該当する送信元 IP アドレスからのすべての TCP トラフィックがブロックされます。フロー フィールドの詳細については、表 6-2 を参照してください。
Triggering Rate	ポリシーのしきい値を超過した攻撃フローのレートを示します。
Threshold	攻撃フローによって超過したポリシーのしきい値を示します。
Policy	特定の動的フィルタを作成したポリシーを示します。詳細については、第 7 章「ポリシー テンプレートとポリシーの設定」を参照してください。

動的フィルタの削除

動的フィルタを削除することができます。ただし、削除が有効である期間は限られています。これは、保護モードでは、Guard が動的に変化するトラフィックの状態に保護を適合させるために、新しい動的フィルタを設定し続けるためです。

動的フィルタを削除するには、次の手順を実行します。

ステップ 1　動的フィルタのリストを表示し、削除する動的フィルタの ID を確認します。詳細については、前の項、「動的フィルタの表示」を参照してください。

ステップ 2　フィルタを削除します。次のように入力します。

```
no dynamic-filter dynamic-filter-id
```

引数 *dynamic-filter-id* には、動的フィルタの ID を指定します。すべての動的フィルタを削除するには、* を入力します。

次の例を参考にしてください。

```
admin@GUARD-conf-zone-scannet# no dynamic-filter 876
```

（注）　不要な動的フィルタが再作成されないようにするには、そのフィルタを作成するポリシーを非アクティブにします（詳細については、P.7-20 の「ポリシーの状態の変更」を参照）。不要な動的フィルタを作成したポリシーを調べるには、この章の動的フィルタの表示に関する項を参照してください。または、次のいずれかを実行します。

- 目的のトラフィック フロー用のバイパス フィルタを設定します（詳細については、P.6-12 の「バイパス フィルタの設定」を参照）。
- 不要な動的フィルタを作成したポリシーのしきい値を大きくします（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）。

動的フィルタの非アクティブ化

動的フィルタがタイムアウトになると、Guard はその動的フィルタを非アクティブにするかどうかを判断します。Guard が動的フィルタを非アクティブにしないことを決定した場合は、次の期間に向けてそのフィルタのアクティベーション タイムアウトが再開されます。動的フィルタは、次のいずれかに当てはまる場合に非アクティブになります。

- ゾーンの悪意のあるトラフィック　レートの合計（スプーフィングされたトラフィックとドロップされたトラフィックの合計と等しい）が、zone-malicious-rate 終了しきい値以下である。

- 動的フィルタでトラフィック レートが測定され（フィルタのレート カウンタに N/A と表示されていない）、**かつ** filter-rate 終了しきい値が次の**両方**より大きい。
  - 動的フィルタの現在のトラフィック レート
  - ユーザ定義の期間（ポリシーの Timeout パラメータで定義）中の動的フィルタの平均トラフィック レート

（注） アクション to-user-filters、block-unauthenticated、redirect/zombie、または notify が指定された動的フィルタでは、トラフィック レートは測定されません。

ゾーンの悪意のあるトラフィックのしきい値を設定するには、次のように入力します。

filter-termination zone-malicious-rate *threshold*

引数 *threshold* には、ゾーンの悪意のあるトラフィックのしきい値をパケット / 秒単位で指定します。このトラフィックは、スプーフィングされたトラフィックとドロップされたトラフィックの合計で構成されます。デフォルト値は 50 pps です。

動的フィルタの終了しきい値を設定するには、次のように入力します。

filter-termination filter-rate *threshold*

引数 *threshold* には、動的フィルタのトラフィックのしきい値をパケット / 秒単位で指定します。デフォルト値は 2 pps です。

次の例を参考にしてください。

```
admin@GUARD-conf-zone-scannet# filter-termination zone-malicious-rate 200
admin@GUARD-conf-zone-scannet# filter-termination filter-rate 50
```