ゾーンのフィルタの設定

この章では、Cisco Guard（Guard）のフィルタの設定方法について説明します。

この章は、次の項で構成されています。

概要

ゾーン フィルタは、Guard が特定のトラフィック フローを処理する方法を定義します。トラフィック フローをカスタマイズし、DDoS 防止保護操作を制御するようにフィルタを設定できます。

ゾーン フィルタを使用すると、Guard は次の機能を実行できます。

- 異常がないかゾーン トラフィックを分析する。
- 基本レベルまたは強化レベルの保護を適用し、異常なトラフィックから正当なトラフィックを分離して取り出す。
- 異常なパケットをドロップする。
- トラフィックを直接ゾーンに転送し、Guard の保護機能をバイパスする。

Guard には、次のタイプのフィルタがあります。

- ユーザ フィルタ：必要な保護レベルを指定されたトラフィック フローに適用します。このフィルタは、異常なトラフィックや悪意のあるトラフィックが検出されたときに Guard が最初に実行するアクションを定義します。ゾーン設定には、多様なタイプの攻撃を処理できるオンデマンドの保護用に設定された、デフォルトのユーザ フィルタのセットが含まれています。ユーザ フィルタを変更すると、Guard の保護機能をカスタマイズし、攻撃の疑いがある場合の Guard によるトラフィック フローの処理規則を設定できます。

  詳細については、P.6-24 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：Guard が特定のトラフィック フローを処理しないようにする。

  信頼できるトラフィックが Guard の保護機能を通らないように誘導して、Guard が信頼できるトラフィックを分析しないようにし、直接ゾーンに転送できます。

  詳細については、P.6-20 の「バイパス フィルタの設定」を参照してください。
- フレックスコンテンツ フィルタ：特定のトラフィック フローをカウントまたはドロップします。IP ヘッダーや TCP ヘッダー内のフィールドに基づいたフィルタリング、ペイロード コンテンツに基づいたフィルタリング、複雑なブール式に基づいたフィルタリングなどの非常に柔軟なフィルタリング機能があります。

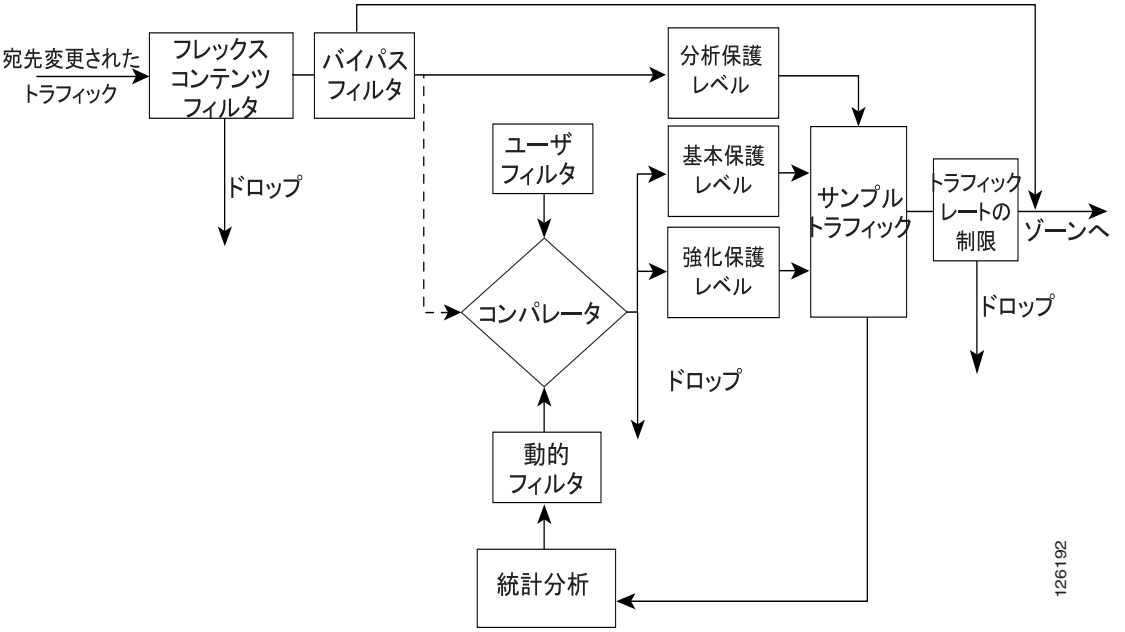
  詳細については、P.6-5 の「フレックスコンテンツ フィルタの設定」を参照してください。

- 動的フィルタ：必要な保護レベルを指定されたトラフィック　フローに適用する。Guard は、トラフィック フロー分析に基づいて動的フィルタを作成し、ゾーン トラフィックや DDoS 攻撃（分散型サービス拒絶攻撃）のタイプに合せて常に動的フィルタ セットを修正しています。動的フィルタは有効期間が限定されており、攻撃が終了すると削除されます。

  詳細については、P.6-32 の「動的フィルタの設定」を参照してください。

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またはリモートのネットワーク検知 DDoS 要素、たとえば Cisco Traffic Anomaly Detector（Detector）などによってゾーン保護がイネーブルになると、Guard はゾーンのトラフィックを分析します。

Guard は、ゾーンに流れるトラフィックのレートを監視します。定義済みのレートを超過するトラフィックはドロップされ、正当なトラフィックはゾーンに転送されます。Guard は、ゾーンのトラフィックの統計分析を行い、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、動的に変化するゾーンのトラフィック特性や変化する DDoS 攻撃のタイプに合せて保護措置を調整します。

トラフィック フローの統計分析を行うために、Guard 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、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である（トラフィック フローがポリシーのしきい値を超えた）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。

Guard は、異常なトラフィックを識別すると次の処理を実行します。

1. 攻撃を処理するアクションが設定された動的フィルタの作成を開始する。デフォルトでは、Guard は、すべての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追加します。Guard が十分な時間を費やして攻撃を分析するまでは、ユーザ フィルタが、新たに発生する DDoS 攻撃を第一線で防御します。
2. Guard 内部でのトラフィックのフローを変更する。異常なトラフィックは、破線で示されているように、コンパレータに流れます。コンパレータとは、動的フィルタとユーザ フィルタから入力を受け取るコンポーネントです。コンパレータは、フローに一致する最初のユーザ フィルタを動的フィルタと比較し、提案された中で最も強力な保護措置を選択します。コンパレータは関連する保護レベルを適用し、トラフィックを認証します。

動的フィルタは有効期間が限定されており、攻撃が終了すると削除されます。デフォルトでは、Guard はシステム管理者がゾーン保護を非アクティブにするまでゾーンを保護します。

フレックスコンテンツ フィルタの設定

フレックスコンテンツ フィルタは、パケット ヘッダー内のフィールドまたはパケット ペイロードのパターンに基づいて、ゾーン トラフィックをフィルタリングします。着信トラフィックに現れているパターンに基づいて攻撃を識別できます。これらのパターンでは、既知のワームまたは一定のパターンを持つフラッド攻撃が識別可能です。

（注） フレックスコンテンツ フィルタは大量の CPU リソースを消費します。フレックスコンテンツ フィルタは Guard のパフォーマンスに影響を及ぼす可能性があるため、使用を制限することをお勧めします。指定のポートに送信される TCP トラフィックなど、動的フィルタによって識別できる特定の攻撃からの保護にフレックスコンテンツ フィルタを使用する場合は、動的フィルタを使用してトラフィックをフィルタリングすることをお勧めします。

フレックスコンテンツ 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する場合、および特定の悪意のあるトラフィックの送信元を識別する場合に使用します。

フレックスコンテンツ フィルタは、次の順序でフィルタリング基準を適用します。

1. プロトコルとポートのパラメータ値に基づいてパケットをフィルタリングする。
2. tcpdump 式の値に基づいてパケットをフィルタリングする。
3. 残りのパケットに対して pattern-expression の値を使用してパターン マッチングを実行する。

この項では、次のトピックについて取り上げます。

- フレックスコンテンツ フィルタの追加
- フレックスコンテンツ フィルタの表示
- フレックスコンテンツ フィルタの削除
- フレックスコンテンツ フィルタの状態の変更

フレックスコンテンツ フィルタの追加

フレックスコンテンツ フィルタは、行番号の昇順でアクティブになります。新しいフレックスコンテンツ フィルタを追加する場合は、リストの適切な位置に配置してください。

Guard は、アクションがドロップであるフレックスコンテンツ フィルタにトラフィックが一致すると、フレックスコンテンツ フィルタのアクティブ化を停止します。

フレックスコンテンツ 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　フレックスコンテンツ　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.6-16 の「フレックスコンテンツ フィルタの表示」を参照してください。

ステップ 2　現在の行番号が連番の場合は、ゾーン設定モードで次のコマンドを入力して、新しいフレックスコンテンツ フィルタを挿入できるようにフレックスコンテンツ フィルタの番号を順に増加させます。

```
flex-content-filter renumber [start [step]]
```

表 6-1 に、**flex-content-filter renumber** コマンドの引数を示します。

表 6-1　flex-content-filter renumber コマンドの引数

パラメータ	説明
start	（オプション）フレックスコンテンツ 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）フレックスコンテンツ 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　（オプション）進行中の攻撃や以前に記録した攻撃のパターン式をフィルタリングするには、**show packet-dump signatures** コマンドを使用して、Guard をアクティブにして攻撃のシグニチャを生成します。

詳細については、P.12-32 の「パケットダンプ キャプチャ ファイルからの攻撃シグニチャの生成」を参照してください。

ステップ 4　次のコマンドを入力して、新しいフレックスコンテンツ フィルタを追加します。

```
flex-content-filter row-num {disabled | enabled} {drop | count}
protocol port [start start-offset [end end-offset]] [ignore-case]
expression tcpdump-expression pattern pattern-expression
```

表 6-2 に、**flex-content-filter** コマンドの引数とキーワードを示します。

表 6-2　flex-content-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。行番号はフィルタの ID で、これによって複数のフレックスコンテンツ フィルタの優先順位が定まります。Guard は、行番号の昇順でフィルタを操作します。
disabled	フィルタの状態をディセーブルに設定します。フィルタはトラフィックを監視しません。
enabled	フィルタの状態をイネーブルに設定します。Guard はトラフィックを監視し、フィルタに一致するフロー上でアクション（ドロップまたはカウント）を実行します。 これがデフォルトの状態です。
drop	フィルタに一致するフローをドロップします。
count	フィルタに一致するフローをカウントします。

表 6-2　flex-content-filter コマンドの引数とキーワード（続き）

パラメータ	説明
protocol	特定のプロトコルからのトラフィック。すべてのプロトコルを指定するには、アスタリスク（*）を使用します。0 ～ 255 の整数を入力します。 指定可能なプロトコル番号については、次に示す Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）の Web サイトを参照してください。 http://www.iana.org/assignments/protocol-numbers
port	特定の宛先ポート宛てのトラフィック。0 ～ 65535 の整数を入力します。特定のポート番号を定義するには、特定のプロトコル番号を定義する必要があります。 すべての宛先ポートを指定するには、アスタリスク（*）を使用します。プロトコル番号を 6（TCP）または 17（UDP）に設定する場合に、アスタリスクを使用できます。 指定可能なポート番号については、次に示す Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）の Web サイトを参照してください。 http://www.iana.org/assignments/port-numbers
start-offset	パケット ペイロードの先頭から、*pattern-expression* 引数のパターン マッチングを開始する位置までのオフセット（バイト単位）。デフォルトは 0（ペイロードの先頭）です。0 ～ 1800 の整数を入力します。 **show packet-dump signatures** コマンドの出力からパターンをコピーする場合は、この引数をコマンドの出力の Start Offset フィールドからコピーします。

表 6-2　flex-content-filter コマンドの引数とキーワード（続き）

パラメータ	説明
end-offset	パケット ペイロードの先頭から、*pattern-expression* 引数のパターン マッチングを終了する位置までのオフセット（バイト単位）。デフォルトは、パケット長（ペイロードの末尾）です。0 ～ 1800 の整数を入力します。 **show packet-dump signatures** コマンドの出力からパターンをコピーする場合は、この引数をコマンドの出力の End Offset フィールドからコピーします。
ignore-case	*pattern-expression* 引数で大文字と小文字が区別されないようにします。 デフォルトでは、*pattern-expression* 引数では大文字と小文字が区別されます。
tcpdump-expression	パケットと照合する式。式はバークリー パケット フィルタの形式です。詳細および設定例については、P.6-11　の「tcpdump 式の構文の設定」を参照してください。 式でスペースを使用する場合は、式を引用符（“ ”）で囲みます。 空の式を入力するには、二重引用符（“”）を使用します。 式で引用符を使用するには、引用符（\”）の前にバックスラッシュ（\）をエスケープ文字として使用します。 （注）　tcpdump 式の構文については、ヘルプを使用できません。

表 6-2　flex-content-filter コマンドの引数とキーワード（続き）

パラメータ	説明
pattern-expression	パケット ペイロードと照合する正規表現のデータ パターン。詳細については、P.6-15 の「パターン式構文の設定」を参照してください。 **show packet-dump signatures** コマンドを使用すると、Guard をアクティブにしてシグニチャを生成できます。P.12-32 の「パケットダンプ キャプチャ ファイルからの攻撃シグニチャの生成」を参照してください。 式でスペースを使用する場合は、式を引用符（“ ”）で囲みます。 空の式を入力するには、二重引用符（“ ”）を使用します。 式で引用符を使用するには、引用符（\”）の前にバックスラッシュ（\\）をエスケープ文字として使用します。 **（注）** パターン式の構文については、ヘルプを使用できません。

フィルタの状態はいつでも変更できます。詳細については、P.6-18 の「フレックスコンテンツ フィルタの状態の変更」を参照してください。

フィルタ アクションはいつでも変更できます。詳細については、P.6-17 の「フレックスコンテンツ フィルタの削除」を参照してください。

次の例は、フレックスコンテンツ フィルタを設定する方法を示しています。

```
user@GUARD-conf-zone-scannet# flex-content-filter enabled count * *
expression “ip[6:2] & 0x1fff=0” pattern
“/ HTTP/1\.1\ x0D\0AAccept: .*/.*\x0D\x0AAccept-Language:
en*\x0D\x0AAccept-Encoding: gzip, deflate\x0D\x0AUser-Agent:
Mozilla/4\.0”
```

この項では、次のトピックについて取り上げます。

tcpdump 式の構文の設定

tcpdump 式はバークリー パケット フィルタ形式で、パケットと照合する式を指定します。

（注） 宛先ポートとプロトコルに基づいてトラフィックをフィルタリングする場合は、tcpdump 式を使用できます。ただし、パフォーマンスへの影響を考慮し、これらの基準でトラフィックをフィルタリングする場合は、フレックスコンテンツ フィルタで *protocol* 引数と *port* 引数を使用することをお勧めします。

式は 1 つ以上の要素からなります。通常、要素は ID（名前または番号）と ID の前に付く 1 つ以上の修飾子からなります。

修飾子には次の 3 つがあります。

- タイプ修飾子：ID（名前または番号）を定義します。指定可能なタイプは、**host**、**net**、および **port** です。**host** タイプ修飾子がデフォルトです。
- 方向修飾子：転送の方向を定義します。指定可能な方向は、**src**、**dst**、**src or dst**、および **src and dst** です。方向修飾子は **src or dst** がデフォルトです。
- プロトコル修飾子：特定のプロトコルへの照合を制限します。指定可能なプロトコルは **ether**、**ip**、**arp**、**rarp**、**tcp**、および **udp** です。プロトコル修飾子を指定しない場合、該当するタイプに適用されるすべてのプロトコルが照合されます。たとえば、ポート 53 とは、TCP または UDP のポート 53 を意味します。

表 6-3 に、tcpdump 式の要素を示します。

表 6-3　tcpdump 式の要素

要素	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。プロトコル名もキーワードです。プロトコル名を入力する場合は、プロトコル名の前にバックスラッシュ（\）をエスケープ文字として使用する必要があります。
expr relop expr	特定の式に適合するトラフィック。表 6-4 に、tcpdump 式の規則を示します。

表 6-4 に、tcpdump 式の規則を示します。

表 6-4　フレックスコンテンツ フィルタの式の規則

式の規則	説明
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。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* 値で指定します。 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*] *size* 引数はオプションで、フィールドのバイト数を指定します。この引数に可能な値は 1、2 または 4 です。デフォルトは 1 です。

次の方法により、式の要素を組み合せることができます。

- 要素と演算子の集まりを丸カッコで囲む：演算子は、通常のバイナリ演算子（+、-、*、/、&、|）と長さ演算子です。

（注）　式でカッコを使用するには、カッコの前にバックスラッシュをエスケープ文字として使用します（\(）。

- 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。

バークリー パケット フィルタの設定オプションの詳細については、次のサイトにアクセスしてください。

http://www.freesoft.org/CIE/Topics/56.htm.

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。

```
user@GUARD-conf-zone-scannet# flex-content-filter enabled count * *
expression ip[6:2]&0x1fff=0 pattern ""
```

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。

```
user@GUARD-conf-zone-scannet# flex-content-filter enabled drop * *
expression tcp[13]&4!=0 pattern ""
```

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。

```
user@GUARD-conf-zone-scannet# flex-content-filter enabled count * *
expression "icmp [0]!=8 and icmp[0] != 0" pattern ""
```

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。

```
user@GUARD-conf-zone-scannet# flex-content-filter enabled count * *
expression "tcp and dst port 80 and not src port 1000" pattern ""
```

パターン式構文の設定

パターン式とは、一連の文字を含んだ文字列を記述した正規表現です。パターン式は、一連の文字列をその要素を実際にリストせずに表現します。パターン式は、一般文字と特殊文字で構成されます。一般文字には、特殊文字とは見なされない印刷可能な ASCII 文字がすべて含まれます。特殊文字は特殊な意味を持つ文字で、Guard がパターン式に対して実行するマッチングのタイプを指定します。フレックスコンテンツ フィルタは、パターン式とパケットの内容（パケット ペイロード）を照合します。たとえば、version 3.1、version 4.0、および version 5.2 という 3 つの文字列は、version .*\..* というパターンで表現できます。

表 6-5 に、使用可能な特殊文字を示します。

表 6-5　パターン式で使用する特殊文字

特殊文字	説明
.*	0 個またはそれ以上の文字を含んでいる文字列と照合します。たとえば、goo.*s は、goos、goods、good for ddos などと照合します。
\	特殊文字から特別な意味を取り除きます。特殊文字を文字列の中で 1 つの文字パターンとして使用するには、各文字の先頭にバックスラッシュ（\）を入力して特殊な意味を取り除きます。たとえば、2 つのバックスラッシュ（\\）は 1 つのバックスラッシュ（\）と照合し、1 つのバックスラッシュとピリオド（\.）は 1 つのピリオドと照合します。 文字として使用するアスタリスク（*）の前にもバックスラッシュを配置する必要があります。
\xHH	16 進値と照合します。H は 16 進数の数字で、大文字と小文字は区別されません。16 進数の値は 2 桁である必要があります。たとえば、\x41 は 16 進数の値 A と照合します。

デフォルトでは、パターン式では大文字と小文字が区別されます。パターン式で大文字と小文字を区別しないようにするには、**flex-content-filter** コマンドに **ignore-case** キーワードを指定します。詳細については、P.6-6 の「フレックスコンテンツ フィルタの追加」を参照してください。

次の例は、パケット ペイロードに特殊なパターンを持つパケットをドロップする方法を示しています。この例のパターンは、Slammer ワームから抽出されました。*protocol*、*port*、および *tcpdump-expression* パラメータは特定のものでなくてもかまいません。

```
user@GUARD-conf-zone-scannet# flex-content-filter enabled drop * *
expression " " pattern
\x89\xE5Qh\.dllhel32hkernQhounthickChGetTf\xB91l
Qh32\.dhws2_f\xB9etQhsockf\xB9toQhsend\xBE\x18\x10\xAEB
```

フレックスコンテンツ フィルタの表示

フレックスコンテンツ フィルタを表示するには、ゾーン設定モードで次のコマンドを入力します。

show flex-content-filters

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

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

フィールド	説明
Row	フレックスコンテンツ フィルタの優先順位を指定します。
State	フィルタの状態（イネーブルまたはディセーブル）を示します。
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。
Protocol	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。
Port	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。
Start	パケット ペイロードの先頭から、パターン マッチングを開始する位置までのオフセット（バイト単位）。このオフセットは、*pattern* フィールドに適用されます。

表 6-6　show flex-content-filters コマンドのフィールドの説明（続き）

フィールド	説明
End	パケット ペイロードの先頭から、パターン マッチングを終了する位置までのオフセットを指定します（バイト単位）。このオフセットは、*pattern* フィールドに適用されます。
Match-case	フィルタと一致するパターン式で、大文字と小文字が区別されるのか、またはされないのかを指定します。 yes の場合は大文字と小文字が区別され、no の場合は区別されません。
TCPDump-expression	パケットと照合する tcpdump 式をバークリー パケット フィルタ形式で指定します。tcpdump 式の構文については、P.6-11 の「tcpdump 式の構文の設定」を参照してください。
Pattern-filter	パケット ペイロードと照合する正規表現のデータ パターンを指定します。パターン式の構文については、P.6-15 の「パターン式構文の設定」を参照してください。
RxRate (pps)	このフィルタで測定される現在のトラフィック レートをパケット / 秒で指定します。

フレックスコンテンツ フィルタの削除

フレックスコンテンツ フィルタを削除またはディセーブルにして、Guard がフィルタ式に基づくパケットのフィルタリングをしないようにすることができます。詳細については、P.6-18 の「フレックスコンテンツ フィルタの状態の変更」を参照してください。

フレックスコンテンツ 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　**show flex-content-filters** コマンドを使用してフレックスコンテンツ フィルタのリストを表示し、削除するフレックスコンテンツ フィルタの行番号を確認します。

次の例は、フレックスコンテンツ フィルタのリストを表示する方法を示しています。

```
user@GUARD-conf-zone-scannet# show flex-content-filters
```

詳細については、P.6-16 の「フレックスコンテンツ フィルタの表示」を参照してください。

ステップ 2　**no flex-content-filter** *row-num* コマンドを入力して、フレックスコンテンツ フィルタを削除します。

row-num 引数には、削除するフレックスコンテンツ フィルタの行番号を指定します。すべてのフレックスコンテンツ フィルタを削除するには、*row-num* 引数としてアスタリスク（*****）を入力します。

次の例は、フレックスコンテンツ フィルタを削除する方法を示しています。

```
user@GUARD-conf-zone-scannet# no flex-content-filters 5
```

フレックスコンテンツ フィルタの状態の変更

フレックスコンテンツ フィルタをディセーブルにすると、Guard はフィルタ式に基づくパケットのフィルタリングと、特定の種類のトラフィックのフィルタリングを実行しなくなります（フィルタはフレックスコンテンツ フィルタのリストに保持されます）。

その後、Guard が指定されたトラフィックをフィルタリングするように再設定できます（フィルタの再設定は不要）。あるいは、フレックスコンテンツ フィルタを削除することもできます。詳細については、P.6-17 の「フレックスコンテンツ フィルタの削除」を参照してください。

フレックスコンテンツ フィルタの状態を変更するには、次の手順を実行します。

ステップ 1　フレックスコンテンツ　フィルタのリストを表示し、状態を変更するフレックスコンテンツ フィルタの行番号を確認します。

詳細については、P.6-16 の「フレックスコンテンツ フィルタの表示」を参照してください。

ステップ 2　次のコマンドを入力して、フレックスコンテンツ フィルタの状態を変更します。

flex-content-filter *row-num* {**disabled** | **enabled**}

row-num 引数には、フレックスコンテンツ フィルタの行番号を指定します。

次の例は、フレックスコンテンツ フィルタをディセーブルにする方法を示しています。

```
user@GUARD-conf-zone-scannet# flex-content-filters 5 disabled
```

バイパス フィルタの設定

バイパス フィルタは、Guard の保護機能（スプーフィング防止機能とゾンビ防止機能を含む）を適用しないという保護ポリシーの決定をサポートし、指定されたトラフィックを直接ゾーンに転送します。

（注）　Guard は、バイパス フィルタを通過したトラフィックをゾーンに注入します。その際、**rate-limit** コマンドによって定められたトラフィック レート制限は適用されません。

この項では、次のトピックについて取り上げます。

- バイパス フィルタの追加
- バイパス フィルタの表示
- バイパス フィルタの削除

バイパス フィルタの追加

バイパス フィルタを追加するには、ゾーン設定モードで次のコマンドを入力します。

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

表 6-7 に、**bypass-filter** コマンドの引数を示します。

表 6-7　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。
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 IP アドレスを示すには、アスタリスク（*）を使用します。

表 6-7　bypass-filter コマンドの引数（続き）

パラメータ	説明
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。サブネット 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。すべてのプロトコルを示すには、アスタリスク（*）を使用します。 指定可能なプロトコル番号については、次に示す Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）の Web サイトを参照してください。 http://www.iana.org/assignments/protocol-numbers
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。すべての宛先ポートを示すには、アスタリスク（*）を使用します。 指定可能なポート番号については、次に示す Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）の Web サイトを参照してください。 http://www.iana.org/assignments/port-numbers
fragments-type	（オプション）断片化されたトラフィックをフィルタが処理するかどうかを指定します。断片化には、次の 3 つのタイプがあります。 • **no-fragments**：断片化されていないトラフィック • **fragments**：断片化されたトラフィック • **any-fragments**：断片化されたトラフィックと断片化されていないトラフィック デフォルトは、**no-fragments** です。

（注） fragments-type と dest-port を両方指定することはできません。fragments-type を設定するには、dest-port にアスタリスク（*）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、ゾーン設定モードで次のコマンドを入力します。

show bypass-filters

表 6-8 に、**show bypass-filters** コマンドの出力フィールドを示します。

表 6-8　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。
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。
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サブネット マスク。
Proto	フィルタが処理するトラフィックのプロトコル番号。
DPort	フィルタが処理するトラフィックの宛先ポート。
Frg	フィルタが処理する断片化の設定。 • yes : フィルタは断片化されたトラフィックを処理します。 • no : トラフィックは断片化されていないトラフィックを処理します。 • any : フィルタは断片化されたトラフィックと断片化されていないトラフィックを処理します。
RxRate (pps)	このフィルタが測定する現在のトラフィック レート（パケット / 秒）。

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。

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　ゾーン設定モードで次のコマンドを入力して、バイパス フィルタを削除します。

no bypass-filter *row-num*

row-num 引数には、削除するバイパス 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、アスタリスク（*）を入力します。

次の例は、バイパス フィルタを削除する方法を示しています。

```
user@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、必要な保護レベルを指定されたトラフィック フローに適用したり、指定されたトラフィックをドロップしたりします。このフィルタは、異常なトラフィックや悪意のあるトラフィックが検出されたときに Guard が最初に実行するアクションを定義します。

ゾーン設定には、多様なタイプの攻撃を処理できるオンデマンドの保護用に設定された、デフォルトのユーザ フィルタのセットが含まれています。ユーザ フィルタを変更すると、Guard の保護機能をカスタマイズし、攻撃の疑いがある場合の Guard による特定のトラフィック フローの処理規則を設定できます。

Guard は、ゾーン宛のトラフィックを継続的に分析します。異常なトラフィック パターンを検出すると、攻撃の処理方法を定義する動的フィルタの作成を開始します。デフォルトでは、Guard は、すべての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追加します。Guard が十分な時間を費やして攻撃を分析するまでは、ユーザ フィルタが、新たに発生する DDoS 攻撃を第一線で防御します。

Guard は、特定のトラフィック フローの処理方法を決定する前に、ユーザ フィルタと動的フィルタの両方を検査します。Guard は、フローに一致する最初のユーザ フィルタを動的フィルタと比較し、提案された中で最も強力な保護措置を選択します。この適切な保護レベルをトラフィック フローに適用し、トラフィックの認証を行います。動的フィルタまたはユーザ フィルタが実行するアクションは、重大度レベルの大きい順に、drop、strong、basic、permit です。アクションが redirect/zombie および block-unauthenticated である動的フィルタは、同じタイプのトラフィックを処理するユーザ フィルタが存在している場合でも適用されます。これは、これらの動的フィルタは Guard の認証メカニズムに影響を与えて、トラフィック フローには直接の影響を与えないためです。

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。新しいユーザ フィルタを追加する場合は、リストの適切な位置に配置することが重要です。

表 6-9 に、ユーザ フィルタで実行可能なアクションを示します。

表 6-9　ユーザ フィルタのアクション

アクション	説明
basic/default	TCP 以外のトラフィック フローを認証します。
basic/dns-proxy	TCP DNS トラフィック フローを認証します。
basic/redirect	HTTP 経由のアプリケーションを認証します。
basic/reset	TCP 経由のアプリケーションを認証します。HTTP トラフィック フローには basic/redirect のアクションを実行することをお勧めします。
basic/safe-reset	TCP 接続のリセットを許容しない TCP アプリケーション トラフィック フローを認証します。HTTP トラフィック フローには basic/redirect のアクションを実行することをお勧めします。
basic/sip	SIP[1] 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/RTCP[2] 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 VoIP[3] アプリケーションを認証します。
drop	トラフィック フローをドロップします。
permit	フローの統計分析を行わないようにします。また、スプーフィング防止やゾンビ防止の保護機能がこのフローを処理しないようにします。他の保護メカニズムでは処理されないため、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。
strong	トラフィック フローに対する強化認証をイネーブルにします。強化認証が必要な場合や、それまでのフィルタがアプリケーションに適していないと考えられる場合にこのフィルタを使用します。認証は、各接続に対して行われます。 TCP 着信接続では、Guard はプロキシの役割を果たします。ネットワーク内の着信 IP アドレスに基づいた ACL[4]、アクセス ポリシー、またはロードバランシング ポリシーを使用している場合は、接続に強化認証アクションを使用しないでください。

1. SIP = Session Initiation Protocol
2. RTP/RTCP = Real-Time Transport Protocol/Real-Time Control Protocol
3. VoIP = Voice over IP
4. ACL = Access Control List（アクセス コントロール リスト）

この項では、次のトピックについて取り上げます。

- ユーザ フィルタの追加
- ユーザ フィルタの表示
- ユーザ フィルタの削除

ユーザ フィルタの追加

ユーザ フィルタを追加するには、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.6-29 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　現在の行番号が連番の場合は、次のコマンドを入力して、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。

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

表 6-10 に、**user-filter renumber** コマンドの引数を示します。

表 6-10　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 ～ 10000 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 ～ 1000 の整数。デフォルトは 10 です。

ステップ 3　次のコマンドを入力して、新しいユーザ フィルタを追加します。

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

表 6-11 に、**user-filter** コマンドの引数を示します。

表 6-11　user-filter コマンドの引数

パラメータ	説明
row-num	1 ～ 1000 の固有な番号。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まります。Guard は、行番号の昇順でフィルタを操作します。
filter-action	特定のトラフィック タイプに対してフィルタが実行するアクション。詳細については、表 6-9 を参照してください。
src-ip	特定の IP アドレスからのトラフィック。すべての IP アドレスを指定するには、アスタリスク（*）を使用します。
ip-mask	（オプション）特定のサブネットからのフロー。サブネットマスクには、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	特定のプロトコルからのトラフィック。すべてのプロトコルを指定するには、アスタリスク（*）を使用します。 指定可能なプロトコル番号については、次に示す Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）の Web サイトを参照してください。 http://www.iana.org/assignments/protocol-numbers
dest-port	特定の宛先ポートへのトラフィック。すべての宛先ポートを指定するには、アスタリスク（*）を使用します。 指定可能なポート番号については、次に示す Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）の Web サイトを参照してください。 http://www.iana.org/assignments/port-numbers

表 6-11　user-filter コマンドの引数（続き）

パラメータ	説明
fragments-type	（オプション）トラフィックのタイプ。トラフィックのタイプは次のいずれかになります。 • **no-fragments**：断片化されていないトラフィック • **fragments**：断片化されたトラフィック • **any-fragments**：断片化されたトラフィックと断片化されていないトラフィック デフォルトは、**no-fragments** です。
rate	レート制限を指定する 64 より大きい整数。ユーザ フィルタは、トラフィックをこのレートに制限します。単位は、*units* パラメータで指定します。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、*units* パラメータで指定される単位に応じて、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。*burst* リミットは、最大で *rate* リミットの 8 倍まで指定可能です。
units	レート制限の単位。単位は次のいずれかになります。 • **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 ずつ変更する方法と、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。このユーザ フィルタは、トラフィック フロー レートを 600 pps に、バースト サイズを 400 パケットに制限しています。

```
user@GUARD-conf-zone-scannet# user-filter renumber 10 5
user@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、ゾーン設定の一部です。ユーザ フィルタを表示するには、ゾーン設定モードで **show** コマンドまたは **show running-config** コマンドを使用します。

ヒント　ユーザ フィルタの設定をディスプレイの先頭に表示するには、**show** コマンドまたは **show running-config** コマンドに **| begin USER FILTERS** オプションを指定して使用します。

表 6-12 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示します。

表 6-12　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。
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。
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。
Proto	フィルタが処理するトラフィックのプロトコル番号。
DPort	フィルタが処理するトラフィックの宛先ポート。

表 6-12　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
Frg	フィルタが処理するトラフィックのタイプ。トラフィックのタイプは次のいずれかになります。 • **yes**：断片化されたトラフィック • **no**：断片化されていないトラフィック • **any**：断片化されたトラフィックと断片化されていないトラフィック
RxRate (pps)	このフィルタが測定する現在のトラフィック レート（単位 pps）。
Action	特定のトラフィック タイプに対してフィルタが実行するアクションを指定します。詳細については、表 6-9 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。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。
Burst	フィルタが特定のフローに許可するトラフィックのバースト リミット。単位は、*Units* フィールドで指定される単位に応じて、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。

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。

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。

注意　ポリシー　アクションが　to-user-filter　に設定されている場合にすべてのユーザ フィルタを削除すると、保護されていないトラフィックはゾーンに渡されます。詳細については、P.7-32 の「ポリシー アクションの設定」を参照してください。

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　ゾーン設定モードで次のコマンドを入力して、ユーザ フィルタを削除します。

```
no user-filter row-num
```

row-num 引数には、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、アスタリスク（*）を入力します。

次の例は、すべてのユーザ フィルタを削除する方法を示しています。

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

動的フィルタの設定

動的フィルタは必要な保護レベルをトラフィック フローに適用し、攻撃の処理方法を定義するものです。Guard は、ゾーン トラフィックに異常があると判断すると（フローがゾーン ポリシーのしきい値を超えたときに発生する）、動的フィルタを作成し、この動的フィルタ セットを常にゾーン トラフィックや DDoS 攻撃のタイプに適合させます。動的フィルタは有効期間が限定されており、攻撃が終了すると削除されます。Guard は、すべてのゾーンで同時にアクティブな動的フィルタを最大 150,000 個サポートします。

デフォルトでは、Guard は、すべての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。Guard が十分な時間を費やして攻撃を分析するまでは、ユーザ フィルタが、新たに発生する DDoS 攻撃を第一線で防御します。

Guard は、特定のトラフィック フローの処理方法を決定する前に、ユーザ フィルタと動的フィルタの両方を検査します。コンパレータは、フローに一致する最初のユーザ フィルタを動的フィルタと比較し、提案された中で最も強力な保護措置を選択します。この適切な保護レベルをトラフィック フローに適用し、トラフィックの認証を行います。動的フィルタとユーザ フィルタが実行するアクションは、重大度レベルの大きい順に、drop、strong、basic、permit です。アクションが redirect/zombie および block-unauthenticated である動的フィルタは、同じタイプのトラフィックを処理するユーザ フィルタが存在している場合でも適用されます。これは、これらの動的フィルタは Guard の認証機能に影響を及ぼしますが、トラフィック フローには直接影響を及ぼさないためです。

動的フィルタを追加できるのは、ゾーン保護がイネーブルになっている場合のみです。

表 6-13 に、動的フィルタで実行可能なさまざまなアクションを示します。

表 6-13　動的フィルタのアクション

アクション	説明
drop	トラフィックをドロップします。
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機能を適用します。

表 6-13　動的フィルタのアクション（続き）

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。
block-unauthenticated-basic	基本保護レベルのスプーフィング防止機能を機能拡張したもので、認証されなかったトラフィック フローをドロップします。
block-unauthenticated-strong	強化保護レベルのスプーフィング防止機能を機能拡張したもので、認証されなかったトラフィック フローをドロップします。
block-unauthenticated-dns	DNS スプーフィング防止機能で認証されなかった、DNS UDP サーバに向かうトラフィック（プロトコルが UDP、ポートが 53 のもの）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します。

動的フィルタは、アクティブな状態が一定時間持続するよう設定されています。動的フィルタのタイムアウトに関するパラメータは、フィルタがどのように作成されたかによって、次のいずれかの方法で設定されます。

- ゾーン　ポリシーによって作成された動的フィルタ：動的フィルタのタイムアウトは、ポリシーのタイムアウトに設定されています。ポリシーによって作成される追加の動的フィルタのタイムアウトを変更するには、ポリシー設定モードで **timeout** コマンドを入力して、この動的フィルタを作成したポリシーのタイムアウトを変更します。
- ユーザ定義の動的フィルタ：動的フィルタのタイムアウトは、**dynamic-filter** コマンドの *exp-time* 引数を指定して定義します。

動的フィルタのタイムアウト期限が切れると、Guard は、現在のトラフィック状態に基づいて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と決定した場合、フィルタはさらにある期間アクティブのままになります。動的フィルタの非アクティブ化の詳細につい

ては、P.6-41 の「動的フィルタの非アクティブ化」を参照してください。

この項では、次のトピックについて取り上げます。

- 動的フィルタの表示
- 動的フィルタの追加
- 動的フィルタの削除
- 動的フィルタの作成防止
- 動的フィルタの非アクティブ化

動的フィルタの表示

Guard が作成した動的フィルタを表示することができます。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 1 つ表示します。
- **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。

保留動的フィルタを表示するには、**show recommendations** コマンドを使用します。保留動的フィルタの詳細については、第 10 章「インタラクティブ保護モードの使用方法」を参照してください。

表 6-14 に、**show dynamic-filters** コマンドの引数とキーワードを示します。

表 6-14　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 ID[1]。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、動的フィルタの完全なリストを表示します。
details	動的フィルタを詳細に表示します。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 6-14　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（pps）の昇順で表示します。

1. ID = 識別番号

（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、動的フィルタに関するすべてのリストを確認してください。

次の例は、動的フィルタを詳細に表示する方法を示しています。

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

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

表 6-15　show dynamic-filters コマンドの出力フィールドの説明

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 6-13 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** コマンドで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。

表 6-15　show dynamic-filters コマンドの出力フィールドの説明（続き）

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	フィルタが断片化されたトラフィックを処理するかどうかを指定します。 • **yes**：フィルタは断片化されたトラフィックを処理します。 • **no**：フィルタは断片化されていないトラフィックを処理します。 • **any**：フィルタは、断片化されたトラフィックと断片化されていないトラフィックの両方を処理します。
RxRate (pps)	このフィルタで測定される現在のトラフィック レートを pps で指定します。

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。

表 6-16 に、**show dynamic-filters details** コマンドの追加出力フィールドを示します。

表 6-16　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 で非スプーフィング攻撃が発生すると、ポート 80 からのトラフィックだけでなく、最初の発信元 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。攻撃フローは、Source IP、Source Mask、Proto、Dport、および Frg フィールドで構成されています。これらのフィールドについては、表 6-15 で説明しています。
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	動的フィルタを作成したポリシーを指定します。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。

動的フィルタの追加

ゾーンの攻撃中に、動的フィルタを追加してゾーン保護を操作することができます。

動的フィルタを追加するには、ゾーン設定モードで次のコマンドを入力します。

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

複数の動的フィルタを追加するには、**dynamic-filter** コマンドを複数使用します。

表 6-17 に、**dynamic-filter** コマンドの引数を示します。

表 6-17　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 6-13 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	フィルタを無期限でアクティブにします。保護が終了すると、フィルタは削除されます。
src-ip	特定の発信元 IP アドレスからのトラフィック。IP アドレスをドット区切り　10　進表記で入力します（たとえば 192.168.100.1）。すべての IP アドレスを指定するには、アスタリスク（*****）を使用します。
ip-mask	（オプション）特定のサブネットからのフロー。サブネット マスクをドット区切り 10 進表記で入力します（たとえば 255.255.255.0）。サブネット 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。

表 6-17　dynamic-filter コマンドの引数とキーワード（続き）

パラメータ	説明
protocol	特定のプロトコルからのトラフィック。すべてのプロトコルを指定するには、アスタリスク（*）を使用します。 指定可能なプロトコル番号については、次に示す Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）の Web サイトを参照してください。 http://www.iana.org/assignments/protocol-numbers
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。すべての宛先ポートを指定するには、アスタリスク（*）を使用します。 指定可能なポート番号については、次に示す Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）の Web サイトを参照してください。 http://www.iana.org/assignments/port-numbers
fragments-type	（オプション）フィルタが機能するトラフィック タイプ。断片化には、次の 3 つのタイプがあります。 • **no-fragments**：断片化されていないトラフィック • **fragments**：断片化されたトラフィック • **any-fragments**：断片化されたトラフィックと断片化されていないトラフィック デフォルトは、**no-fragments** です。

次の例は、トラフィックをユーザ トラフィックに誘導する、有効期限が 600 秒の動的フィルタを追加する方法を示しています。

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

動的フィルタの削除

動的フィルタを削除しても、削除が有効になっている期間は限られています。これは、ゾーン保護がイネーブルのときは、Guard が新しい動的フィルタの設定を続行するためです。Guard が動的フィルタを作成しないようにする方法の詳細については、P.6-40 の「動的フィルタの作成防止」を参照してください。

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　ゾーン設定モードで次のコマンドを入力して、関連する動的フィルタを削除します。

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

dynamic-filter-id 引数には、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、アスタリスク（*）を使用します。

次の例は、動的フィルタを削除する方法を示しています。

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

動的フィルタの作成防止

不要な動的フィルタが作成されないようにするには、次のいずれかのアクションを実行します。

- 動的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.7-22 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特定するには、P.6-34 の「動的フィルタの表示」を参照してください。
- 目的のトラフィック フローにバイパス フィルタを設定します。詳細については、P.6-20 の「バイパス フィルタの設定」を参照してください。

- 不要な動的フィルタを作成するポリシーのしきい値を増分します。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。

動的フィルタの非アクティブ化

動的フィルタのタイムアウト期限が切れると、Guard は、現在のトラフィック状態に基づいて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と決定した場合、フィルタはさらにある期間アクティブのままになります。

動的フィルタは、次のいずれか 1 つの条件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。この項の次のコマンドを参照してください。
- 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）、filter-rate 終了しきい値（この項で次に示すコマンドを参照）が次の両方の値以上である。
  - 動的フィルタの現在のトラフィック レート
  - ユーザが設定した期間内の動的フィルタの平均トラフィック　レートこの期間は、ポリシーのタイムアウト パラメータで定義されます。詳細については、P.7-31 の「ポリシーのタイムアウトの設定」を参照してください。

（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、ゾーン設定モードで次のコマンドを入力します。

filter-termination zone-malicious-rate *threshold*

threshold 引数には、ゾーンの悪意のあるトラフィックのしきい値を pps 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。

動的フィルタのレート終了しきい値を設定するには、ゾーン設定モードで次のコマンドを入力します。

filter-termination filter-rate *threshold*

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

次の例は、動的フィルタの終了レートを設定する方法を示しています。

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