ゾーンのフィルタの設定

この章では、Cisco Anomaly Guard Module（Guard モジュール）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。ユーザは、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することができます。

Guard モジュールでは、次のタイプのフィルタが使用されます。

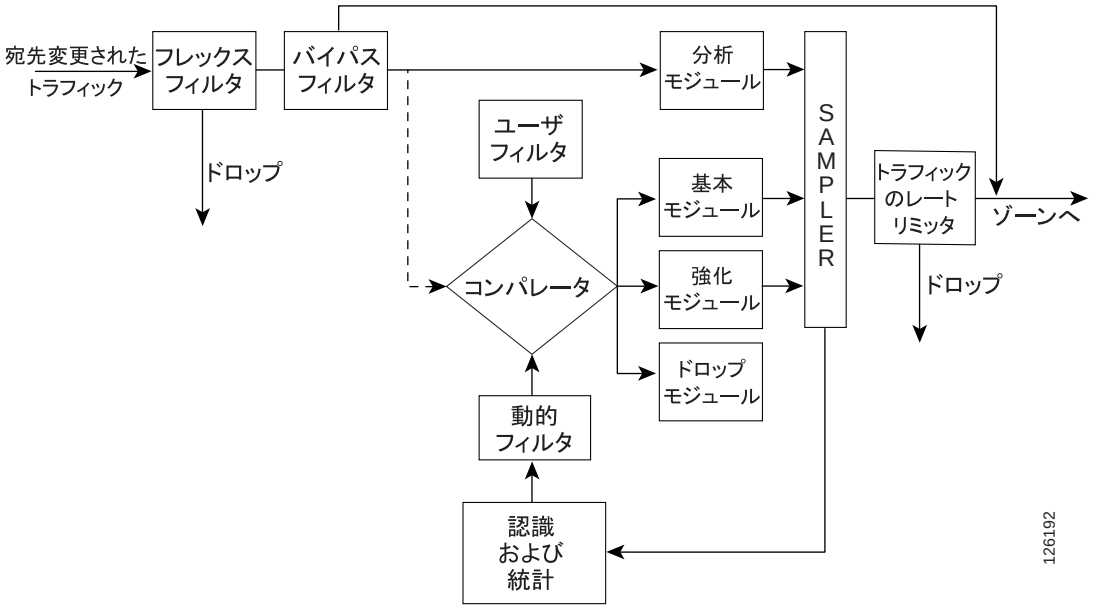
- **ユーザ フィルタ**：ユーザ フィルタは、特定のトラフィック フローを関連する Guard の保護モジュールに誘導します。このフィルタは、異常なトラフィックや悪意のあるトラフィックが検出されたときに Guard が最初に実行するアクションを定義します。ゾーン設定には、多様なタイプの攻撃を処理できるオンデマンドの保護用に設定された、デフォルトのユーザ フィルタのセットが含まれています。ユーザ フィルタを変更すると、Guard の保護モジュールの機能をカスタマイズし、攻撃の疑いがある場合のトラフィック フロー処理規則を設定できます。詳細については、P.7-24 の「ユーザ フィルタの設定」を参照してください。
- **バイパス フィルタ**：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防止します。

  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、そのトラフィックを直接ゾーンに転送できます。

  詳細については、P.7-21 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**：フレックスコンテンツ フィルタは、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。フレックスコンテンツ フィルタは、バークリー パケット フィルタとパターン フィルタを組み合せたもので、IP ヘッダーと TCP ヘッダーのフィールドに基づいたフィルタリングやペイロード コンテンツ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、および複雑なブール式をユーザに提供します。詳細については、P.7-7 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**：動的フィルタは、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します。Guard は、トラフィック フローを分析した結果として動的フィルタを作成します。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 攻撃に合せて継続的に調整されます。動的フィルタは有効期間が限定されており、攻撃が終了すると消去されます。詳細については、P.7-31 の「動的フィルタの設定」を参照してください。

図 7-1 に、Guard モジュールのフィルタ システムを示します。

図 7-1　Guard モジュールのフィルタ 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 Module など）によってゾーンの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 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、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。

Guard モジュールは異常なトラフィックを識別すると、次のように動作します。

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。Guard モジュールは、デフォルトでは、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 モジュールが十分な時間をかけて攻撃を分析するまでの間、ユーザ フィルタは新たに発生する DDoS 攻撃に対して最初の防御策を提供します。
2. Guard モジュール内部のトラフィック 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。コンパレータは、動的フィルタとユーザ フィルタから入力を受け取ります。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。そして、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。

動的フィルタは有効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、ユーザがゾーンの保護を非アクティブにするまで Guard モジュールはゾーンを保護します。

フィルタのトラフィック フロー

フィルタが処理するトラフィック フローを設定する必要があります。表 7-1 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 7-1　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 IP アドレスを示すには、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。

表 7-1　フィルタのフローの引数（続き）

パラメータ	説明
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。断片化のタイプは、次のとおりです。 • **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。

表 7-2 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 7-2　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。

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 フィルタを使用すると、パケット ヘッダー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できます。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。そ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。ただし、フレックスコンテンツ フィルタはリソースを大量に消費します。フレックスコンテンツ フィルタはパフォーマンスに影響を及ぼす可能性があるため、十分に注意して使用することをお勧めします。特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、バークリー パケット フィルタとパターン フィルタを組み合せたもので、豊富なフィルタリング機能を持っています。

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
- TCPDump 式の構文について
- パターン式の構文について
- 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。したがって、新しいフレックスコンテンツ 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。

トラフィックが drop アクションを持つフレックスコンテンツ フィルタに一致すると、Guard モジュールは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.7-18 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　現在の行番号が連続したものである場合は、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。次のコマンドを入力します。

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

表 7-3 に、**flex-filter renumber** コマンドの引数を示します。

表 7-3　flex-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）進行中の攻撃または以前記録した攻撃のパターン式をフィルタリングする場合、Guard モジュールをアクティブ化し、**show packet-dump signatures** コマンドを使用して攻撃のシグニチャを生成することができます。詳細については、P.11-28 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　新しいフレックスコンテンツ　フィルタを追加します。次のコマンドを入力します。

```
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 7-4 に、**flex-filter** コマンドの引数とキーワードを示します。

表 7-4　flex-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義されます。Guard モジュールは、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に関連付けられません。
enabled	フィルタの状態をイネーブルに設定します。フィルタはトラフィックに関連付けられ、一致が検出されるとアクションを実行します。 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 7-4　flex-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。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	特定の宛先ポートに向かうトラフィックを処理します。0 ～ 65,535 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示すには、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）に設定する場合のみ、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、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。このオフセットは、*pattern* フィールドに適用されます。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 7-4　flex-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、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。このオフセットは、*pattern* フィールドに適用されます。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を指定します。式はバークリー パケット フィルタの形式です。詳細および設定の例については、P.7-13 の「TCPDump 式の構文について」を参照してください。 式にスペースが含まれる場合は、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。 式に引用符を含めるには、バックスラッシュ（\）をエスケープ文字として使用します。 TCPDump 式の構文については、ヘルプを使用できません。

表 7-4　flex-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 パターンを指定します。詳細については、P.7-16 の「パターン式の構文について」を参照してください。 Guard モジュールをアクティブ化し、**show packet-dump signatures** コマンドを使用してシグニチャを生成することができます。P.11-28 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。 式にスペースが含まれる場合は、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。 式に引用符を含めるには、バックスラッシュ（\）をエスケープ文字として使用します。 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。

- フレックスコンテンツ フィルタは最初に、*protocol* および *port* に基づいてパケットをフィルタリングする。
- 次に、*tcpdump-expression* を適用する。
- フレックスコンテンツ フィルタは、残りのパケットに対して *pattern-expression* を使用してパターン マッチングを実行する。

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.7-20 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.7-19 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。

次の例を参考にしてください。

```
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"
```

TCPDump 式の構文について

TCPDump 式は、パケットを照合する式を指定します。式はバークリー パケット フィルタの形式です。

（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 の式を使用できます。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。

表 7-5 に、フレックスコンテンツ フィルタの式のパラメータの説明を示します。

表 7-5　フレックスコンテンツ フィルタのパラメータ

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。

表 7-5　フレックスコンテンツ フィルタのパラメータ（続き）

パラメータ	説明
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 7-6 を参照してください。

表 7-6 に、フレックスコンテンツ フィルタの式の規則の説明を示します。

表 7-6　フレックスコンテンツ フィルタの式の規則

式の規則	
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*]

表 7-6　フレックスコンテンツ フィルタの式の規則（続き）

式の規則	
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。*size* 引数はオプションです。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。*len* 引数には、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。

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、http://www.freesoft.org/CIE/Topics/56.htm を参照してください。

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 ""
```

パターン式の構文について

パターン（正規表現）は、一連の文字を含んだ文字列を記述したものです。パターンには、パターンの要素を実際に列挙するのではなく、一連の文字列を記述します。パターンは、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 文字が含まれます。特殊文字は、どのようなマッチングを実行するのかを示します。フレックスコンテンツ フィルタは、このパターンをパケットの内容（パケットのペイロード）と照合します。たとえば、*version 3.1*、*version 4.0*、および *version 5.2* の 3 つの文字列は、*version* .*\..* というパターンで記述されます。

特殊文字とは、特殊な意味を持つ文字で、Guard モジュールが式に対してどのような照合を実行するのかを指定する文字です。表 7-7 で、使用できる特殊文字について説明します。

表 7-7　フレックスコンテンツ パターン フィールドの説明

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一致します。たとえば、パターン *goo.*s* は *goos*、*goods*、*good for ddos* などと一致します。
\	特殊文字が持つ特殊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、シーケンス \\ は \ と一致し、シーケンス \. は . と一致します。 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 進値と一致します。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 進値は 2 桁で入力する必要があります。たとえば、\x41 は A と一致します。

デフォルトでは、パターン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が区別されないようにするには、**ignore-case** キーワードを使用します。P.7-8 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、パケットのペイロードに特定のパターンが含まれている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たものです。プロトコル、ポート、および tcpdump 式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\xB9ll
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 7-8 に、**show flex-content-filters** コマンドの出力フィールドを示します。

表 7-8　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示します。
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）。
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	フィルタが一致するパターンで大文字と小文字が区別されるかどうかを示します（この引数は、*pattern* フィールドに適用されます）。 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。

表 7-8　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
TCPDump-expression	パケットと照合する式をバークリー 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.7-13 の「TCPDump 式の構文について」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 フィルタの構文については、P.7-16 の「パターン式の構文について」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 pps で示します。

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 フィルタを削除できます。または、フレックスコンテンツ フィルタをディセーブルにして、Guard モジュールがフィルタの式に基づいてパケットをフィルタリングしないように設定できます。詳細については、P.7-20 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　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。詳細については、P.7-18 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　フレックスコンテンツ フィルタを削除します。次のコマンドを入力します。

```
no flex-content-filter row-num
```

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。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、アスタリスク（*）を入力します。

次の例を参考にしてください。

```
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 フィルタの状態を変更できます。フレックスコンテンツ フィルタをディセーブルにして、Guard モジュールがフィルタの式に基づいてパケットをフィルタリングしないように設定できます。フィルタは Guard モジュールのフレックスコンテンツ フィルタ リストに残ったままになります。このようにして、ある種類のトラフィックに対する Guard モジュールのフィルタリングを停止することができます。その後で、もう一度指定されたトラフィックをフィルタリングするように Guard モジュールを設定できます。このとき、フィルタを再設定する必要はありません。また、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.7-19 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.7-18 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　フレックスコンテンツ　フィルタの状態を変更します。次のコマンドを入力します。

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。

次の例を参考にしてください。

```
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 の保護メカニズムを利用しない保護ポリシーの採用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、分析、基本、強化の各保護モジュール、およびレート リミット保護モジュール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 フローについては、スプーフィング防止メカニズムおよびゾンビ防止メカニズムを含めて Guard の保護モジュールをバイパスするように指定できます。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を Guard の保護メカニズムの対象から除外して、ゾーンに直接送信できるようになります。

（注）　バイパス フィルタで処理されるトラフィックは、レート リミット モジュールを経由しません。

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、関連する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 7-9 に、**bypass-filter** コマンドの引数を示します。

表 7-9　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 モジュールは、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	フィルタリングを実行する対象のフロー。*src-ip*、*ip-mask*、*protocol*、*dest-port*、および *fragments-type* の詳細については、表 7-1 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、関連する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 7-10 に、**show bypass-filters** コマンドの出力フィールドを示します。

表 7-10　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	フィルタリングを実行する対象のフローを示します。Source IP、Source Mask、Proto、DPort、Frg の詳細については、表 7-2 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 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　バイパス フィルタを削除します。次のコマンドを入力します。

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

row-num 引数には、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、アスタリスク（*）を入力します。

次の例を参考にしてください。

```
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、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 の保護モジュールの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。ユーザ フィルタは、特定のトラフィック フローを関連する保護モジュール、および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に誘導したり、ドロップしたりできます。

Guard は、ゾーンが宛先になっている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。Guard モジュールは、デフォルトでは、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 モジュールが十分な時間をかけて攻撃を分析するまでの間、ユーザ フィルタは新たに発生する DDoS 攻撃に対して最初の防御策を提供します。

Guard モジュールはユーザ フィルタと動的フィルタの両方を調べた後で、当該トラフィック フローの処理方法を決定します。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。そして、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 redirect/zombie および block-unauthenticated が指定された動的フィルタは、同じタイプのトラフィックを処理するユーザ フィルタがあっても適用されます。動的フィルタは Guard モジュールの認証メカニズムに影響しますが、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。

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 7-11 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。

表 7-11　ユーザ フィルタのアクション

アクション	説明
permit	フローの統計分析を行わないよう、また、スプーフィング防止やゾンビ防止の保護メカニズムがこのフローを処理しないよう防止する場合に使用します。このフローは他の保護メカニズムによって処理されないため、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お勧めします。
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 経由のアプリケーションを認証する場合に使用します。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/default	TCP 経由でないトラフィック フローを認証する場合に使用します。
basic/dns-proxy	TCP DNS トラフィック フローを認証する場合に使用します。
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 フローを認証する場合に使用します。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。
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。 TCP 着信接続については Guard モジュールがプロキシの役割を果たすため、このアクションは、Access Control List（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、このような接続に使用しないことをお勧めします。

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.7-28 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。次のコマンドを入力します。

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

表 7-12 に、**user-filter renumber** コマンドの引数を示します。

表 7-12　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。次のコマンドを入力します。

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

表 7-13 に、**user-filter** コマンドの引数を示します。

表 7-13　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。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 モジュールは、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を指定します。詳細については、表 7-11 を参照してください。
フローの引数とキーワード	フィルタリングを実行する対象のフロー。*src-ip*、*ip-mask*、*protocol*、*dest-port*、および *fragments-type* の詳細については、表 7-1 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、トラフィックをこの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。*rate* リミットは、最大で *burst* 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 リミットの単位。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、特定のフローは許可されますが、フロー レートは *600 pps* に、バースト サイズは *400* パケットにそれぞれ制限されています。

```
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。

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** コマンドを **| begin USER FILTERS** オプションを指定して使用します。

表 7-14 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 7-14　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	フィルタリングを実行する対象のフローを示します。Source IP、Source Mask、Proto、DPort、Frg の詳細については、表 7-2 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 pps で示します。

表 7-14　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
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 7-11 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。
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。次のコマンドを入力します。

```
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、* を入力します。

次の例を参考にしてください。

```
user@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（ポリシーのアクションの詳細については、第 8 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 フローを分析した結果として動的フィルタを作成します。このフィルタは、特定のトラフィック フローを関連する保護モジュールに誘導します。この一連のフィルタは Guard モジュールによって、ゾーンのトラフィックおよび特定の DDoS 攻撃に合せて継続的に調整されます。動的フィルタは有効期間が限定されており、攻撃が終了すると消去されます。

Guard は、トラフィックの異常を検出する中で、ゾーンが宛先になっているトラフィックを継続的に分析します。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。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。

Guard モジュールは、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 モジュールが十分な時間をかけて攻撃を分析するまでの間、ユーザ フィルタは新たに発生する DDoS 攻撃に対して最初の防御策を提供します。

Guard モジュールはユーザ フィルタと動的フィルタの両方を調べた後で、当該トラフィック フローの処理方法を決定します。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。そして、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 redirect/zombie および block-unauthenticated が指定された動的フィルタは、同じタイプのトラフィックを処理するユーザ フィルタがあっても適用されます。動的フィルタは Guard モジュールの認証メカニズムに影響しますが、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 7-15 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 7-15　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メカニズムを適用します。
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	基本的なスプーフィング防止メカニズム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	強力なスプーフィング防止メカニズム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 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、DNS UDP サーバに向かうトラフィック フロー（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、動的フィルタが生成される原因となったポリシーのタイムアウトを変更します。ポリシー設定モードで **timeout** コマンドを使用します。
- 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* 引数を使用して定義します。

動的フィルタのタイムアウト期限が満了すると、Guard は、現在のトラフィックの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。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。

動的フィルタを追加または削除し、ニーズに合せて設定することができます。動的フィルタは、Guard モジュールによって現在保護されているゾーンに対してだけ追加することができます。Guard モジュールは、ゾーンの保護が終了すると、動的フィルタを消去します。

この項では、次のトピックについて取り上げます。

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

動的フィルタの追加

動的フィルタを追加するには、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 7-16 に、**dynamic-filter** コマンドの引数を示します。

表 7-16　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 7-15 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。

表 7-16　dynamic-filter コマンドの引数とキーワード（続き）

パラメータ	説明
forever	フィルタは無限にアクティブです。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	フィルタリングを実行する対象のフロー。*src-ip*、*ip-mask*、*protocol*、*dest-port*、および *fragments-type* の詳細については、表 7-1 を参照してください。

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 モジュール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 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。

（注）　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。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。

表 7-17 に、**show dynamic-filters** コマンドの引数を示します。

表 7-17　show dynamic-filters コマンドの引数

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 モジュール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。
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。

（注）　Guard モジュールは、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。

次の例を参考にしてください。

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

表 7-18 に、**show dynamic-filters** コマンドの出力フィールドを説明します。

表 7-18　show dynamic-filters コマンド出力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 7-15 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済みのしきい値に従って削除される場合があります。
Filter flow	フィルタリングを実行する対象のフローを示します。Source IP、Source Mask、Proto、DPort、Frg の詳細については、表 7-2 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 pps で示します。

表 7-19 に、**show dynamic-filters details** コマンドの追加の出力フィールドを説明します。

表 7-19　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 から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 7-2 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。

表 7-19　show dynamic-filters details コマンドのフィールドの説明（続き）

フィールド	説明
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 8 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、削除が有効になる期間は限られています。Guard モジュールは、ゾーンが保護されている限り、継続的に新しい動的フィルタを設定するためです。

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　関連する動的フィルタを削除します。次のコマンドを入力します。

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（*）を入力します。

次の例を参考にしてください。

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

必要のない動的フィルタが再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.8-22 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発見するには、P.7-34 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 フロー用のバイパス フィルタを設定します（詳細については、P.7-21 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.8-23 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

動的フィルタのタイムアウト期限が満了すると、Guard は、現在のトラフィックの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（この項で次に示すコマンドを参照）。
- 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（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.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。

（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、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。

次の例を参考にしてください。

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