



# ゾーンのフィルタの設定

---

この章では、高度なゾーンのフィルタの設定作業を実施する方法について説明します。WBM を使用すると、ゾーンのトラフィックを処理するためのカスタムフィルタ設定を設計できます。

この章は、次の項で構成されています。

- [ゾーンのフィルタの概要](#)
- [ユーザ フィルタの管理](#)
- [バイパス フィルタの管理](#)
- [フレックスコンテンツ フィルタの管理](#)

## ゾーンのフィルタの概要

Guard は、ゾーンを保護するときおよびゾーンのトラフィックをラーニングするときに、ゾーンのフィルタを使用してトラフィック フローを管理します。ゾーンのフィルタによって、Guard で次の機能を実行できるようになります。

- ゾーンのトラフィックに異常がないかどうかを分析する
- 基本または強化保護レベルを適用して悪意のあるトラフィックと正当なトラフィックを区別する
- 悪意のあるパケットをドロップする
- Guard のゾーン保護機能をバイパスして、トラフィックをゾーンに直接転送する

一連のゾーンのフィルタを設定すると、トラフィックの管理と DDoS 攻撃からの保護について、Guard にゾーン固有の規則を指示できます。ゾーンのフィルタの設定を変更すると、その変更がゾーンの設定に保存され、ただちに有効になります。Guard では、次のタイプのトラフィック フィルタを使用します。

- ユーザ フィルタ : Guard には、特定の保護レベルをトラフィック フローに適用する一連のスタティック ユーザ フィルタがあらかじめ設定されています。ユーザ フィルタは、さまざまなタイプの攻撃に対応するように設計されています。

攻撃の進行中、Guard はユーザ フィルタと動的フィルタ（下で説明）の両方を利用してゾーン保護を管理します。ゾーンに対する攻撃が発生すると、Guard は動的フィルタの作成を開始します。このフィルタには、攻撃の進行中に保護プロセスを管理するためのアクションが設定されます。Guard は、十分な時間をかけて攻撃を分析するまでの間、トラフィック フローをユーザ フィルタに誘導するアクションを持った動的フィルタを設定します。ユーザ フィルタは、攻撃に対する最初の防御手段となっており、ユーザ フィルタが持つアクションをトラフィックに適用します。Guard は、攻撃を分析し終わると、独自のアクションを持った動的フィルタの作成を開始して、トラフィック フローに直接適用します。Guard がユーザ フィルタと動的フィルタの両方をトラフィック フローに適用しようとしたときは、強力なほうのアクションを持つフィルタが選択されます。

- 動的フィルタ : Guard は、攻撃進行中のトラフィック 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。ユーザ フィルタと同様に、動的フィルタも特定の保護レベルをトラフィック フローに適用します。Guard は、動的フィルタを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します。動的フィルタは有効期間が限定されており、Guard は攻撃

が終了したときに動的フィルタを消去します。動的フィルタは、ユーザが追加または削除できます。


- **バイパス フィルタ**：ユーザ定義のバイパス フィルタは、特定のトラフィック フローを **Guard** で処理しないようにして、ゾーンに直接転送します。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機能およびゾンビ防止機能を含めて **Guard** の保護機能をバイパスすることを許可できます。
- **フレックスコンテンツ フィルタ**：ユーザ定義のフレックスコンテンツ フィルタは、特定のトラフィック フローのパケットを **Guard** でカウントまたはドロップできるようにします。また、悪意のあるトラフィックの送信元の識別に使用できます。このバークリー パケット フィルタは、IP ヘッダーおよび TCP ヘッダーのフィールドに基づいたフィルタリングや、コンテンツのバイト数に基づいたフィルタリングなど、柔軟なフィルタリング機能を提供します。特定のトラフィック フローにフレックスコンテンツ フィルタを設定できます。設定できるフレックスコンテンツ フィルタは、ゾーンごとに 1 つのみです。フレックスコンテンツ フィルタはリソース消費量が多く、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については、<http://www.freesoft.org/CIE/Topics/56.htm> を参照してください。

## ユーザフィルタの管理

この項の手順では、Guard のユーザフィルタを追加および削除する方法について説明します。Guard は、ユーザフィルタをユーザフィルタリストでの表示順に従ってアクティブにします（図 5-1 を参照）。新しいユーザフィルタを追加するときは、リスト内での新しいフィルタの配置場所を把握しておくことが重要です。

図 5-1 ユーザフィルタ

Zone scannet (interactive) - Protected 

Home > Zone > User filters

	Src IP	Protocol	Dst Port	Fragments	Rate	Burst	Action	Rate (pps)
<input type="checkbox"/>	*	6	80	without			basic/redirect	0.00
<input type="checkbox"/>	*	6	8080	without			basic/redirect	0.00
<input type="checkbox"/>	*	6	8000	without			basic/redirect	0.00

119408

この項では、次の手順について説明します。

- ユーザフィルタの追加
- ユーザフィルタの削除

## ユーザフィルタの追加

新しい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** ナビゲーション ペインでゾーンを選択します。ゾーンのメインメニューが表示されます。
- ステップ 2** ゾーンのメインメニューの **Configuration > User filters** を選択します。ゾーンのユーザフィルタのリストが表示されます（図 5-1 を参照）。
- ステップ 3** **Add** をクリックします。Add Filter Step 1 画面が表示され、ユーザフィルタのリストが示されます。

- ステップ 4** Insert カラムで、ユーザ フィルタを挿入する位置の下にある行をクリックします。Insert Here テキストが表示され、選択した行の上に新しいユーザ フィルタが挿入されることが示されます。
- ステップ 5** Next をクリックします。Add Filter Step 2 画面が表示され、User Filter Form が示されます。
- ステップ 6** 新しいユーザ フィルタのパラメータを設定します。表 5-1 に、User Filter Form に表示されるフィルタ パラメータの説明を示します。

表 5-1 ユーザ フィルタのパラメータ

パラメータ	説明
Source IP	特定の IP アドレスから送信されるトラフィックをユーザ フィルタに転送します。送信元 IP アドレスを入力します。すべての送信元 IP アドレスを指定するには、このフィールドをブランクのままにするか、アスタリスク (*) を入力します。
Source subnet	特定のサブネットから送信されるトラフィックをユーザ フィルタに転送します。サブネットを Source subnet ドロップダウンリストから選択します。
Protocol	特定のプロトコルで送信されるトラフィックをユーザ フィルタに転送します。プロトコル番号を入力します。すべてのプロトコルを指定するには、このフィールドをブランクのままにするか、アスタリスク (*) を入力します。
Dst Port	特定のポートが宛先となっているトラフィックをユーザ フィルタに転送します。宛先ポート番号を入力します。すべての宛先ポートを指定するには、このフィールドをブランクのままにするか、アスタリスク (*) を入力します。

表 5-1 ユーザフィルタのパラメータ (続き)

パラメータ	説明
Fragments	<p>フィルタで処理するトラフィックのタイプを指定します。Fragments ドロップダウン リストから、次のいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• <b>without</b> : ユーザ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。</li> <li>• <b>with</b> : ユーザフィルタは断片化されたトラフィックを処理します。</li> <li>• <b>*</b> : ユーザフィルタは、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。</li> </ul>
Rate	<p>レート リミットを指定します。ユーザフィルタは、トラフィックの量を指定したレート以下に制限します。レート リミットの値を Rate フィールドに入力し、使用する測定単位を Rate ドロップダウン リストから選択します。トラフィック レートをユーザフィルタで制限しない場合は、測定単位として <b>unlimit</b> を選択します。</p>
Burst	<p>トラフィックのバースト リミットを指定します。ユーザフィルタは、Rate に対して選択したものと同一測定単位をバーストにも使用します (このテーブルの Rate を参照)。</p>

表 5-1 ユーザフィルタのパラメータ (続き)

パラメータ	説明
Action	<p>特定のトラフィック タイプに対してユーザ フィルタが実行するアクションを指定します。Action ドロップダウン リストから、次のいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• <b>permit</b> : フローの統計分析を実行せず、このフローをスプーフィング防止保護メカニズムとゾンビ防止保護メカニズムによって処理しない場合に使用します。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。</li> <li>• <b>basic/redirect</b> : 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。</li> <li>• <b>basic/reset</b> : 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 <b>basic/redirect</b> アクションを使用することをお勧めします。</li> <li>• <b>basic/safe-reset</b> : 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 <b>basic/redirect</b> アクションを使用することをお勧めします。</li> <li>• <b>basic/default</b> : TCP 以外のトラフィック フローを認証する場合に使用します。</li> <li>• <b>basic/dns-proxy</b> : TCP DNS トラフィック フローを認証する場合に使用します。</li> <li>• <b>strong</b> : 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するアプリケーションに適用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。</li> </ul> <p>TCP 着信接続では Guard がプロキシの役割を果たすため、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、このような接続にこのアクションを使用しないことをお勧めします。</p> <ul style="list-style-type: none"> <li>• <b>drop</b> : トラフィック フローをドロップする場合に使用します。</li> </ul>

**ステップ 7** 次のいずれかのオプションを選択します。

- **OK** : 新しいユーザフィルタの設定を保存します。User filters 画面が表示されます。
- **Cancel** : 情報を保存せずに User Filters Form を終了します。User filters 画面が表示されます。

## ユーザフィルタの削除



### 注意

ユーザフィルタを削除するときは、Guard のゾーン保護機能が影響を受ける可能性があるため、十分に注意してください。

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** ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。
- ステップ 2** ゾーンのメイン メニューの **Configuration > User filters** を選択します。ゾーンのユーザフィルタのリストが表示されます。
- ステップ 3** 削除するユーザフィルタの隣にあるチェックボックスをオンにします。
- ステップ 4** **Delete** をクリックします。ユーザフィルタのリストからユーザフィルタが削除されます。



## バイパス フィルタの管理

この項の手順では、Guard のバイパス フィルタを追加および削除する方法について説明します。ここに示す手順に従ってバイパス フィルタのリストを表示すると、バイパス フィルタでフィルタリングされた現在のバイパス フィルタ トラフィックのレートが、カウンタにパケット / 秒 (pps) 単位で示されます。

この項では、次の手順について説明します。

- [バイパス フィルタの追加](#)
- [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、次の手順を実行します。

- 
- ステップ 1** ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。
  - ステップ 2** ゾーンのメイン メニューの **Configuration > Bypass filters** を選択します。Bypass filters 画面が表示されます。
  - ステップ 3** **Add** をクリックします。Add bypass filter 画面が表示されます。
  - ステップ 4** 新しいバイパス フィルタのパラメータを設定します。[表 5-2](#) に、Bypass Filter Form に表示されるフィルタ パラメータの説明を示します。

表 5-2 バイパス フィルタのパラメータ

パラメータ	説明
Source IP	Guard は、指定する IP アドレスからのトラフィックについては Guard の保護機能をバイパスして、ゾーンに直接転送します。すべての送信元 IP アドレスを指定するには、このフィールドをブランクのままにするか、アスタリスク (*) を入力します。
Source subnet	Guard は、指定するサブネットからのトラフィックについては Guard の保護機能をバイパスして、ゾーンに直接転送します。サブネットを Source subnet ドロップダウン リストから選択します。
Protocol	Guard は、指定するプロトコルを使用しているトラフィックについては Guard の保護機能をバイパスして、ゾーンに直接転送します。プロトコル番号を入力します。すべてのプロトコルを指定するには、このフィールドをブランクのままにするか、アスタリスク (*) を入力します。
Dst Port	Guard は、指定するゾーン宛先ポートをターゲットとするトラフィックについては Guard の保護機能をバイパスして転送します。宛先ポート番号を入力します。すべての宛先ポートを指定するには、このフィールドをブランクのままにするか、アスタリスク (*) を入力します。
Fragments	<p>フィルタで処理するトラフィックのタイプを指定します。Fragments ドロップダウン リストから、次のいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• <b>without</b> : バイパス 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。</li> <li>• <b>with</b> : バイパス フィルタは断片化されたトラフィックを処理します。</li> <li>• <b>*</b> : バイパス 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。</li> </ul>

**ステップ 5** 次のいずれかのオプションを選択します。

- **OK** : 新しいバイパス フィルタの設定を保存します。Bypass filters 画面が表示されます。
  - **Cancel** : 情報を保存せずに Bypass Filters Form を終了します。Bypass filters 画面が表示されます。
- 

## 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** ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

**ステップ 2** ゾーンのメイン メニューの **Configuration > Bypass filters** を選択します。Bypass filters 画面が表示されます。

**ステップ 3** 削除する各バイパス フィルタの隣にあるチェックボックスをオンにし、**Delete** をクリックします。フィルタのリストからバイパス フィルタが削除されます。表示されているバイパス フィルタをすべて削除するには、Src IP の隣にあるチェックボックスをオンにし、**Delete** をクリックします。

---

## フレックスコンテンツ フィルタの管理

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。このようなパターンによって、一定のパターンを持つ既知のワームやフラッド攻撃を識別できます。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、豊富なフィルタリング機能を持つバークリー パケット フィルタとパターン フィルタを組み合わせたものです。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。

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. プロトコルと宛先ポートに基づいて、パケットをフィルタリングします。
2. `tcpdump` 式を適用します。
3. 残ったパケットに対して、パターン を使用してパターン マッチングを実行します。

この項は、次の情報と手順で構成されています。

- [フレックスコンテンツの式の構文について](#)
- [フレックスコンテンツ フィルタのパターンの構文について](#)
- [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 フィルタの削除](#)

## フレックスコンテンツの式の構文について

フレックスコンテンツ フィルタの式には、パケットとのパターン マッチングに使用する式を指定します。この式は、バークリー パケット フィルタ形式を使用して定義します。



(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` の式を使用できます。ただし、パフォーマンスを考慮すると、これらの基準に基づいて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 フィルタの `protocol` パラメータと `port` パラメータを使用することをお勧めします。

表 5-3 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 5-3      フレックスコンテンツ フィルタの式のパラメータ**

パラメータ	説明
<b>Destination host IP address</b>	宛先ホスト IP アドレスへのトラフィック。
<b>Source host IP address</b>	送信元ホスト IP アドレスからのトラフィック。
<b>Host IP address</b>	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。
<b>Net mask</b>	特定のネットワークへのトラフィック。
<b>Net net/len</b>	特定のサブネットへのトラフィック。
<b>Destination port number</b>	宛先ポート番号への TCP または UDP トラフィック。
<b>Source port number</b>	送信元ポート番号からの TCP または UDP トラフィック。
<b>Port number</b>	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。
<b>Less packet length</b>	特定のバイト長以下の長さを持つパケット。
<b>Greater packet length</b>	特定のバイト長以上の長さを持つパケット。

表 5-3 フレックスコンテンツ フィルタの式のパラメータ (続き)

パラメータ	説明
<b>IP protocol</b>	ICMP、UDP、または TCP のプロトコル番号を持つパケット。
<b>IP broadcast</b>	ブロードキャスト IP パケット。
<b>IP multicast</b>	マルチキャスト パケット。
<b>Ether protocol</b>	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。
<b>Relop expression</b>	特定の式に適合するトラフィック。詳細については、表 5-4 を参照してください。

表 5-4 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 5-4 フレックスコンテンツ フィルタの式の規則

式の規則	
<b>relop</b>	>、<、>=、<=、=、!=
<b>expression</b>	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。  <i>protocol [expression: size]</i>
<b>protocol</b>	インデックス操作のプロトコル層を指定します。指定可能な値は、 <b>ether</b> 、 <b>ip</b> 、 <b>tcp</b> 、 <b>udp</b> 、または <b>icmp</b> 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、 <i>expression</i> で指定されます。 <i>size</i> パラメータはオプションです。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。 <i>length</i> パラメータには、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わ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許文字であるため、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。

```
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。

```
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。

```
"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。

```
"tcp and dst port 80 and not src port 1000"
```

## フレックスコンテンツ フィルタのパターンの構文について

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、どのような照合を行うかを示します。フレックスコンテンツ フィルタでは、このパターンをパケットのコンテンツ（パケット 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。

特殊文字は、特別な意味を持った文字で、Guard が式でどのような照合を行うかを指定します。表 5-5 に、使用可能な特殊文字の説明を示します。

**表 5-5 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
<code>.*</code>	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 <code>goo.*s</code> は <code>goos</code> 、 <code>goods</code> 、 <code>good for ddos</code> などと一致します。
<code>\</code>	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 ( <code>\</code> ) を入力して特別な意味を取り除きます。たとえば、シーケンス <code>「\」</code> は <code>「\」</code> に、シーケンス <code>「.」</code> は <code>「.」</code> に一致します。  文字として使用するアスタリスク ( <code>*</code> ) の前にもバックスラッシュを配置する必要があります。
<code>\xHH</code>	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 進数の値は、必ず 2 桁である必要があります。たとえば、 <code>「\x41」</code> は <code>「A」</code> に一致します。

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。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。



```
\x89\xE5Qh\.dllhel132hkernQhounthickChGetTf\xB911
Qh32\.dhws2_f\xB9etQhsockf\xB9toQhsend\xBE\x18\x10\xAEB
```

## 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 フィルタを追加するには、次の手順を実行します。

- ステップ 1 ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。
- ステップ 2 ゾーンのメイン メニューの **Configuration > Flex-Content filters** を選択します。Flex-Content filters 画面が表示され、既存のフレックスコンテンツ フィルタのリストが示されます。
- ステップ 3 **Add** をクリックします。Add filter - step 2 画面が表示されます。
- ステップ 4 フレックスコンテンツ フィルタのパラメータを設定します。表 5-6 に、Flex-Content Filter Form に表示されるフィルタ パラメータの説明を示します。

**表 5-6** 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
Description	フレックスコンテンツ フィルタを説明するテキスト。
Protocol	<p>特定のプロトコルを使用しているトラフィックを処理します。0 ~ 255 のプロトコル番号を入力します。すべてのプロトコル タイプを指定するには、アスタリスク (*) を入力します。</p> <p>有効なプロトコル番号のリストについては、次の Internet Assigned Numbers Authority (IANA) の Web サイトを参照してください。</p> <p><a href="http://www.iana.org/assignments/protocol-numbers">http://www.iana.org/assignments/protocol-numbers</a></p>

表 5-6 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
Dst Port	<p>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 の宛先ポート番号を入力します。すべての宛先ポートを指定するには、アスタリスク (*) を入力します。</p> <p>有効なポート番号のリストについては、次の Internet Assigned Numbers Authority (IANA) の Web サイトを参照してください。</p> <p><a href="http://www.iana.org/assignments/port-numbers">http://www.iana.org/assignments/port-numbers</a></p>
Expression	<p>指定した式に基づいてトラフィックをフィルタリングします (「フレックスコンテンツの式の構文について」の項を参照)。180 個 (スペース区切り) までのトークンを使用して文字列を入力します。</p>
Pattern	<p>パケットの内容と照合するための正規表現データ パターンを指定します (「フレックスコンテンツ フィルタのパターンの構文について」の項を参照)。使用するデータ パターンを入力します。</p>
Match Case	<p>データ パターン式で大文字と小文字を区別するかどうかを指定します。大文字と小文字を区別するデータ パターン式として定義するには、チェックボックスをオンにします。</p>
Start Offset	<p>パケットの内容の先頭から、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)。デフォルトは 0 (ペイロードの先頭) です。開始オフセットは、pattern フィールドに適用されます。0 ~ 2047 の整数を入力します。</p>
End Offset	<p>パケットの内容の先頭から、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)。デフォルトは、パケット長 (ペイロードの末尾) です。終了オフセットは、pattern フィールドに適用されます。0 ~ 2047 の整数を入力します。</p>

表 5-6 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
Action	<p>トラフィックに対してフレックスコンテンツ フィルタが実行するアクションを指定します。</p> <p>アクションを Action ドロップダウン リストから選択します。</p> <ul style="list-style-type: none"> <li>• <b>count</b> : フィルタに一致するトラフィック フロー パケットをカウントします。</li> <li>• <b>drop</b> : フィルタに一致するトラフィック フロー パケットをドロップします。</li> </ul>
State	<p>フレックスコンテンツ フィルタの動作状態。</p> <p>動作状態を State ドロップダウン リストから選択します。</p> <ul style="list-style-type: none"> <li>• <b>enable</b> : Guard はフィルタをトラフィック フローに適用し、一致が見つかったら、設定されているアクションを実行します。</li> <li>• <b>disable</b> : Guard は、フィルタをトラフィック フローに適用しません。</li> </ul>

**ステップ 5** 次のいずれかのオプションを選択します。

- **OK** : 新しいフレックスコンテンツ フィルタを保存します。Flex-Content filters 画面が表示されます。
- **Clear** : フォームの情報をデフォルト値に戻し、追加した情報をすべて消去します。
- **Cancel** : 情報を保存せずに Flex-Content filters 画面を終了します。Flex-Content filters 画面が表示されます。

## 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 フィルタを削除するには、次の手順を実行します。

- 
- ステップ 1 ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。
  - ステップ 2 ゾーンのメイン メニューの **Configuration > Flex-Content filters** を選択します。Flex-Content filters 画面が表示され、既存のフレックスコンテンツ フィルタのリストが示されます。
  - ステップ 3 削除する各フレックスコンテンツ フィルタの隣にあるチェックボックスをオンにし、**Delete** をクリックします。フィルタのリストからフレックスコンテンツ フィルタが削除されます。表示されているフレックスコンテンツ フィルタをすべて削除するには、Src IP の隣にあるチェックボックスをオンにし、**Delete** をクリックします。
-