ゾーンのフィルタの設定

この章では、ゾーンのフィルタを設定する方法について説明します。WBM を使用すると、ゾーン トラフィックを処理するためのフィルタを設定できます。

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

Detector では、ゾーン フィルタを使用して、取得するゾーン トラフィック フローのコピーを管理します。Detector は、ゾーン フィルタを使用して次の機能を実行できます。

- 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
- Detector の異常の検出機能をバイパスする

一連のゾーン フィルタを設定して、Detector にトラフィックの管理と DDoS 攻撃の検出に関するゾーン固有の規則を指定することができます。ゾーンのフィルタの設定を変更すると、変更した内容がただちに有効になります。

Detector は、次のタイプのフィルタを使用します。

- 動的フィルタ：（Detector の動作）Detector は、攻撃の進行中にトラフィック フローの分析結果として動的フィルタを作成します。動的フィルタに従って、Detector はイベントを Detector の syslog に記録するか、Guard をアクティブにしてゾーン保護を実施します。動的フィルタは有効期間が限定されており、Detector は攻撃が終了するとこれらを削除します。動的フィルタは、ユーザが追加または削除できます。

  （Cisco Guard の動作）Cisco Guard は、攻撃の進行中にトラフィック フローの分析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。Cisco Guard は、動的フィルタをゾーンのトラフィックおよび DDoS 攻撃のタイプに合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、Cisco Guard は攻撃が終了するとこれらを削除します。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 フィルタを使用すると、特定のトラフィック フローを Detector が処理しなくなります。信頼されたトラフィックを Detector の異常検出 機能に送信しないようにして、Detector がそれを分析できないようにします。
- 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 フィルタを使用すると、Detector で特定のトラフィック フローのパケットをカウントしたり、悪意のあるトラフィックの送信元を特定することができます。このフィルタは、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。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。

GUARD ゾーン テンプレートを使用してゾーンを作成した場合、そのゾーン設定にはユーザ フィルタのセットが含まれています。Detector 上にユーザ フィルタを設定した後、Cisco Guard にゾーン設定をコピーできます。ユーザ フィルタは Cisco Guard のみで使用され、トラフィック フローに特定の保護レベルを適用します。Cisco Guard が攻撃を分析する十分な時間を得るまで、ユーザ フィルタは、攻撃に対する最初の防御手段を提供します。Cisco Guard が攻撃を分析したら、動的フィルタの生成を開始します。Cisco 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、より重大なアクションを持つフィルタが選択されます。

ユーザ フィルタの管理

ユーザ フィルタは、Cisco Guard だけが使用します。Detector 上にユーザ フィルタを設定した後、Cisco Guard にゾーン設定をコピーできます。次の手順は、GUARD ゾーン テンプレートを使用して作成したゾーンの設定にユーザ フィルタを追加または削除する方法を示しています。Cisco 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。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。

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、GUARD ゾーン テンプレートを使用して作成した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。

ゾーンが GUARD ゾーン テンプレートから作成されたことを確認するには、ゾーンのメイン メニューから **Configuration > General** を選択します。ゾーン テンプレートの名前が GUARD で始まることを確認します。

ステップ 2　ゾーンのメイン メニューの **Configuration > Filters > 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　**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。
Fragments	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。 • **without**：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。 • **with**：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。 • *：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。

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
Rate	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 **unlimit** を選択します。
Burst	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じ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）。
Action	特定のトラフィックに対してユーザ 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。 • **permit**：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機能とゾンビ防止保護メカニズムによって処理され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。 • **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 アクションを使用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 フローを認証する場合に使用します。HTTP トラフィック フローには basic/redirect アクションを使用することをお勧めします。 • **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。

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 （続き）	• **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 SIP エンドポイント間のボイス データを送信する VoIP[3] プロトコルを認証します。 • **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する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 着信接続では、Cisco Guard はプロキシの役割を果たします。着信 IP アドレスに基づく ACL[4]、アクセス ポリシー、またはロードバランシング ポリシーをネットワークで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。 • **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。

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）

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

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 に設定されたときにすべてのユーザ フィルタを削除し、その後ゾーン設定を Cisco Guard にコピーする場合、保護されていないトラフィックがゾーンに渡されます。

ステップ 1　ナビゲーション ペインで、GUARD ゾーン テンプレートを使用して作成した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。

ゾーンが GUARD ゾーン テンプレートから作成されたことを確認するには、ゾーンのメイン メニューから **Configuration > General** を選択します。ゾーン テンプレートの名前が GUARD で始まることを確認します。

ステップ 2　ゾーンのメイン メニューの **Configuration > Filters > 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** をクリックしてユーザ フィルタを削除します。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

次の手順は、Detector のバイパス フィルタを追加または削除する方法を示しています。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 > Filters > 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の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	Detector は、Detector の異常検出機能をバイパスして、指定した IP アドレスからゾーンへ直接トラフィックを転送します。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。

表 5-2　バイパス フィルタのパラメータ（続き）

パラメータ	説明
Source subnet	Detector は、Detector の異常検出機能をバイパスして、指定したサブネットからゾーンへ直接トラフィックを転送します。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	Detector は、Detector の異常検出機能をバイパスし、指定したプロトコルを使用してゾーンへ直接トラフィックを転送します。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	Detector は、Detector の異常検出機能をバイパスし、指定したゾーンの宛先ポートへトラフィックを転送します。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	Detector は指定したトラフィック タイプを処理します。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。 • **without**：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。 • **with**：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。 • *****：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。

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 > Filters > 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 フィルタは、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。

（注） フレックスコンテンツ フィルタは、CPU 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 Detector 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。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を保護するため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. プロトコルとポート　パラメータの値に基づいて、パケットをフィルタリングします。
2. Expression の値に基づいて、パケットをフィルタリングします。
3. 残ったパケットに対して、Pattern の値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 フィルタの式の構文について

tcpdump 式は、バークリー パケット フィルタ形式をとり、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 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* 引数と *port* 引数を使用することをお勧めします。

式には、1 つ以上の要素があります。通常、要素は ID（名前または番号）と、その前に付く 1 つまたは複数の修飾子で構成されます。

修飾子には次の 3 つのタイプがあります。

- 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** タイプの修飾子がデフォルトです。
- 方向修飾子：転送方向を定義します。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 **src or dst** がデフォルトです。
- プロトコル修飾子：照合を特定のプロトコルに限定します。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、タイプに適用したすべてのプロトコルが照合されます。たとえば、ポート 53 は TCP または UDP のポート 53 を意味します。

表 5-3 に、フレックスコンテンツ フィルタの式の要素の説明を示します。

表 5-3　フレックスコンテンツ フィルタの式の要素

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。

表 5-3　フレックスコンテンツ フィルタの式の要素（続き）

パラメータ	説明
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。プロトコル名はキーワードでもあります。プロトコル名を入力する場合は、エスケープ文字としてバックスラッシュ（\）を名前の前に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 5-4 に、tcpdump 式の規則を示します。

表 5-4 に、tcpdump 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	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* の値で指定されます。 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、フィールド内のバイト数を示します。この引数は 1、2、または 4 となります。デフォルトは 1 です。

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。

```
ip[6:2]&0x1fff=0
```

次の例は、すべての TCP RST パケットをカウント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。この表現は、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。特殊文字とは、特殊な意味を持ち、Detector がパターン式に対して実行する照合のタイプを指定する文字です。フレックスコンテンツ フィルタは、パターン式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。

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
.*	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（\）と一致し、1 つのバックスラッシュとピリオド（\.）はピリオド（.）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、必ず 2 桁である必要があります。たとえば、\x41 というパターンは 16 進値 A 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\.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 > Filters > 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 フィルタの説明を示します。
Protocol	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。 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。 http://www.iana.org/assignments/protocol-numbers
Dst 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。 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。 http://www.iana.org/assignments/port-numbers
Expression	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 フィルタ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。

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
Pattern	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。
Match Case	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。
Start Offset	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。
End Offset	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。
Action	Detector 上で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。 アクションを Action ドロップダウン リストから選択します。 • **count**：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。
Guard Action	トラフィックに対して Cisco Guard 上で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。GUARD ゾーン テンプレートを使用してゾーンを作成した場合、このフィールドが適用されます。 アクションを Action ドロップダウン リストから選択します。 • **count**：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。 • **drop**：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。

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
State	フレックスコンテンツ フィルタの動作状態を指定します。 動作状態を State ドロップダウン リストから選択します。 • **enable** : Detector はフィルタをトラフィック フローに適用し、一致が検出されると設定されたアクションを実行します。 • **disable** : Detector は、フィルタをトラフィック フローに適用しません。

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。このゾーンが GUARD ゾーン テンプレートを使用して作成された場合、設定ファイルの Cisco Guard 部分と Detector 部分の両方に Flex-Content フィルタが保存されます。
- **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 > Filters > 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。

このゾーンが GUARD ゾーン テンプレートを使用して作成された場合、設定ファイルの Cisco Guard 部分と Detector 部分の両方から Flex-Content フィルタが削除されます。