目次

概要

このドキュメントでは、コマンドライン インターフェイス（CLI）と IDS Device Manager（IDM）を備えた Cisco Intrusion Prevention System（IPS）のイベント アクション フィルタを使用してシグニチャを調整する方法について説明します。

前提条件

要件

この資料は Cisco IPS がインストールされている仮定し、ときちんとはたらきます。

使用するコンポーネント

この文書に記載されている情報はソフトウェア バージョン 5.0 および それ以降を実行する IDS/IPS デバイスに Cisco 4200 シリーズ基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

検知時のアクション フィルター

検知時のアクション フィルターの概要

検知時のアクション フィルターは規則正しく並べられたリストおよびリストのフィルターを上下に移動できると同時に処理されます。

フィルターはセンサーがセンサーがすべての操作を行うか、または全体のイベントを取除くように要求しないでイベントに応じてある特定の操作を行うようにしました。 フィルターはイベントからの操作の削除によってはたらきます。 フィルタはイベントからすべての操作を効果的に取除くイベントを消費します。

注スイープする シグニチャをフィルタリングするとき、Cisco は宛先アドレスをフィルタリングしないことを推奨します。 複数の 宛て先アドレスがある場合、フィルタを一致するのに最後のアドレスだけが使用されています。

特定の操作をイベントから取除きか、または全体のイベントを廃棄し、センサーによってこれからの プロセスを防ぐために検知時のアクション フィルターを設定できます。 フィルター用のグループ アドレスに定義した検知時のアクション 変数を使用できます。 検知時のアクション 変数を設定する方法のプロシージャに関しては検知時のアクション 変数 セクションの削除を追加し、編集し、参照して下さい。

注ドル記号 ($) とストリングよりもむしろ変数を使用することを示すために変数に前書きして下さい。 さもなければ、 受け取ります。

CLI を使用する検知時のアクション フィルター構成

検知時のアクション フィルターを設定するためにこれらのステップを完了して下さい:

1. アドミニストレーター特権があるアカウントの CLI へのログイン。
2. 検知時のアクション ルール サブモードを入力して下さい:`sensor#configure terminal sensor(config)#service event-action-rules rules1 sensor(config-eve)#`
3. フィルタ名前を作成して下さい:`sensor(config-eve)#filters insert name1 begin`検知時のアクション フィルターを指名するために **name1 を、name2**、等使用して下さい。 **開始を**使用して下さい **| end | 非アクティブ | 前に |** キーワード 規定 するため**後**フィルタをどこに挿入したいと思うか。
4. このフィルタの値を規定 して下さい:シグニチャ ID 範囲を規定 して下さい:`sensor(config-eve-fil)#signature-id-range 1000-1005`デフォルトは 900 から 65535 です。サブシグニチャ ID 範囲を規定 して下さい:`sensor(config-eve-fil)#subsignature-id-range 1-5`デフォルトは 0 から 255 です。攻撃者 アドレス範囲を規定 して下さい:`sensor(config-eve-fil)#attacker-address-range 10.89.10.10-10.89.10.23`デフォルトは 255.255.255.255 へ 0.0.0.0 です。対象アドレス範囲を規定 して下さい:`sensor(config-eve-fil)#victim-address-range 192.56.10.1-192.56.10.255`デフォルトは 255.255.255.255 へ 0.0.0.0 です。対象ポート範囲を規定 して下さい:`sensor(config-eve-fil)#victim-port-range 0-434`デフォルトは 0 から 65535 です。OS 関連性を規定 して下さい:`sensor(config-eve-fil)#os-relevance relevant`デフォルトは 0 から 100 です。範囲を評価するリスクを規定 して下さい。`sensor(config-eve-fil)#risk-rating-range 85-100`デフォルトは 0 から 100 です。取除く操作を規定 して下さい:`sensor(config-eve-fil)#actions-to-remove reset-tcp-connection`拒否操作をフィルタリングする場合、ほしい拒否操作のパーセントを設定 して下さい:`sensor(config-eve-fil)#deny-attacker-percentage 90`デフォルトは 100 です。ディセーブルにか有効に されるにフィルタのステータスを規定 して下さい。`sensor(config-eve-fil)#filter-item-status {enabled | disabled}`デフォルトは有効に なります。一致パラメータの停止を規定 して下さい。`sensor(config-eve-fil)#stop-on-match {true | false}`この項目が一致する場合**本当**センサーをフィルターを処理することを止めるように言います。 この項目が一致しても**偽**センサーをフィルターを処理し続けるように言います。このフィルタを説明するために使用したいと思うコメントを追加して下さい:`sensor(config-eve-fil)#user-comment NEW FILTER`
5. フィルタの設定を確認して下さい:`sensor(config-eve-fil)#show settings` NAME: name1 ---------- signature-id-range: 1000-10005 default: 900-65535

```
subsignature-id-range: 1-5 default: 0-255      attacker-address-range: 10.89.10.10-10.89.10.23
default: 0.0.0.0-255.255.255.255      victim-address-range: 192.56.10.1-192.56.10.255 default:
0.0.0.0-255.255.255.255      attacker-port-range: 0-65535 <defaulted>      victim-port-range: 1-343
default: 0-65535      risk-rating-range: 85-100 default: 0-100      actions-to-remove: reset-tcp-
connection default:      deny-attacker-percentage: 90 default: 100      filter-item-status: Enabled
default: Enabled      stop-on-match: True default: False      user-comment: NEW FILTER default:
os-relevance: relevant default: relevant|not-relevant|unknown   ----------------------------------
------------senor(config-eve-fil)#
```

6. 既存のフィルタを編集するため:`sensor(config-eve)#`**`filters edit name1`**
7. パラメータを編集し、詳細についてはステップ 4a によって 4l を参照して下さい。
8. フィルタリストのフィルタを上下に移動するため:`sensor(config-eve-fil)#`**`exit`**`sensor(config-eve)#`**`filters move name5 before name1`**
9. フィルターを移動したことを確認して下さい:`sensor(config-eve-fil)#`**`exit`**`sensor(config-eve)#`**`show settings`**
```
---------------------------------------------   filters (min: 0, max: 4096, current: 5 -
4 active, 1 inactive)   ---------------------------------------------   ACTIVE list-contents   --
-----------------------------------------      NAME: name5      ------------------------------
---------------         signature-id-range: 900-65535 <defaulted>         subsignature-id-range:
0-255 <defaulted>         attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>
victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>         attacker-port-range: 0-65535
<defaulted>         victim-port-range: 0-65535 <defaulted>         risk-rating-range: 0-100
<defaulted>         actions-to-remove: <defaulted>         filter-item-status: Enabled <defaulted>
stop-on-match: False <defaulted>         user-comment: <defaulted>      ---------------------------
--------------------      ------------------------------------------------      NAME: name1      ---
-----------------------------------------         signature-id-range: 900-65535 <defaulted>
subsignature-id-range: 0-255 <defaulted>         attacker-address-range: 0.0.0.0-255.255.255.255
<defaulted>         victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>         attacker-
port-range: 0-65535 <defaulted>         victim-port-range: 0-65535 <defaulted>         risk-rating-
range: 0-100 <defaulted>         actions-to-remove: <defaulted>         filter-item-status: Enabled
<defaulted>         stop-on-match: False <defaulted>         user-comment: <defaulted>      -------
---------------------------------------      ------------------------------------------------
NAME: name2      ------------------------------------------------         signature-id-range: 900-
65535 <defaulted>         subsignature-id-range: 0-255 <defaulted>         attacker-address-range:
0.0.0.0-255.255.255.255 <defaulted>         victim-address-range: 0.0.0.0-255.255.255.255
<defaulted>         attacker-port-range: 0-65535 <defaulted>         victim-port-range: 0-65535
<defaulted>         risk-rating-range: 0-100 <defaulted>         actions-to-remove: <defaulted>
filter-item-status: Enabled <defaulted>         stop-on-match: False <defaulted>         user-
comment: <defaulted>      ------------------------------------------------      --------------------
---------------------------   ------------------------------------------------   INACTIVE list-
contents   ------------------------------------------------------------------------------------------
------sensor(config-eve)#
```

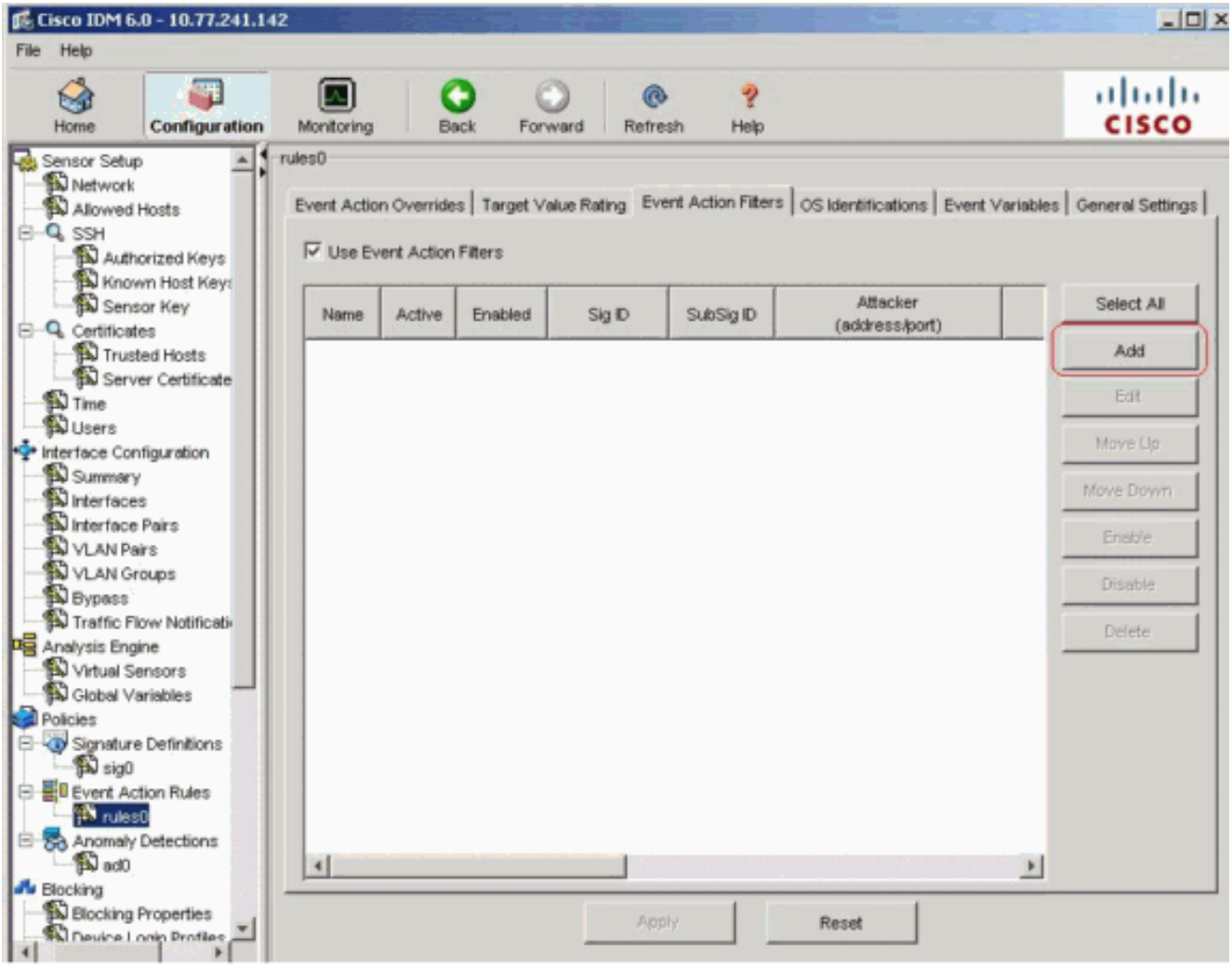
10. フィルタを非アクティブ リストに移動するため:`sensor(config-eve)#`**`filters move name1 inactive`**
11. フィルタが非アクティブ リストに移動したことを確認して下さい:`sensor(config-eve-fil)#`**`exit`**`sensor(config-eve)#`**`show settings`**
```
   ---------------------------------------------
   INACTIVE list-contents   ---------------------------------------------      --------------------
   ---------------------------      NAME: name1      ---------------------------------------------
   signature-id-range: 900-65535 <defaulted>         subsignature-id-range: 0-255 <defaulted>
   attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>         victim-address-range: 0.0.0.0-
   255.255.255.255 <defaulted>         attacker-port-range: 0-65535 <defaulted>         victim-port-
   range: 0-65535 <defaulted>         risk-rating-range: 0-100 <defaulted>         actions-to-remove:
   <defaulted>         filter-item-status: Enabled <defaulted>         stop-on-match: False
   <defaulted>         user-comment: <defaulted>      ---------------------------------------------
   ------------------------------------------------sensor(config-eve)#
```

12. 検知時のアクション ルール サブモードを終了して下さい:`sensor(config-eve)#`**`exit`**`Apply Changes:?[yes]:`
13. 変更を加えるか、またはそれらを廃棄するために入るために『Enter』 を押さない で下さい。

IDM を使用する検知時のアクション フィルター構成

検知時のアクション フィルターを追加し、編集し、削除し、有効に し、ディセーブルにし、移動するためにこれらのステップを完了して下さい:

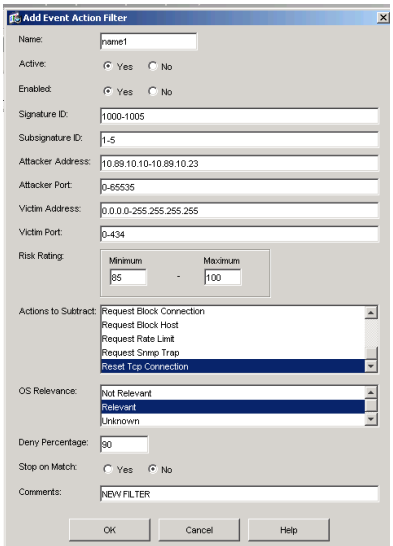
1. 管理者またはオペレータ特権があるアカウントの IDM への口グイン。
2. ソフトウェア バージョンが 6.x である場合 **> 検知時のアクション支配します > rules0 > 検知時のアクション フィルタ** Configuration > Policies の順に選択 して下さい。 ソフトウェア バージョン 5.x に関しては、**> 検知時のアクション支配します > 検知時のアクション フィルタ**『Configuration』 を選択 して下さい。検知時のアクション Filters タブは示されているように現われます。



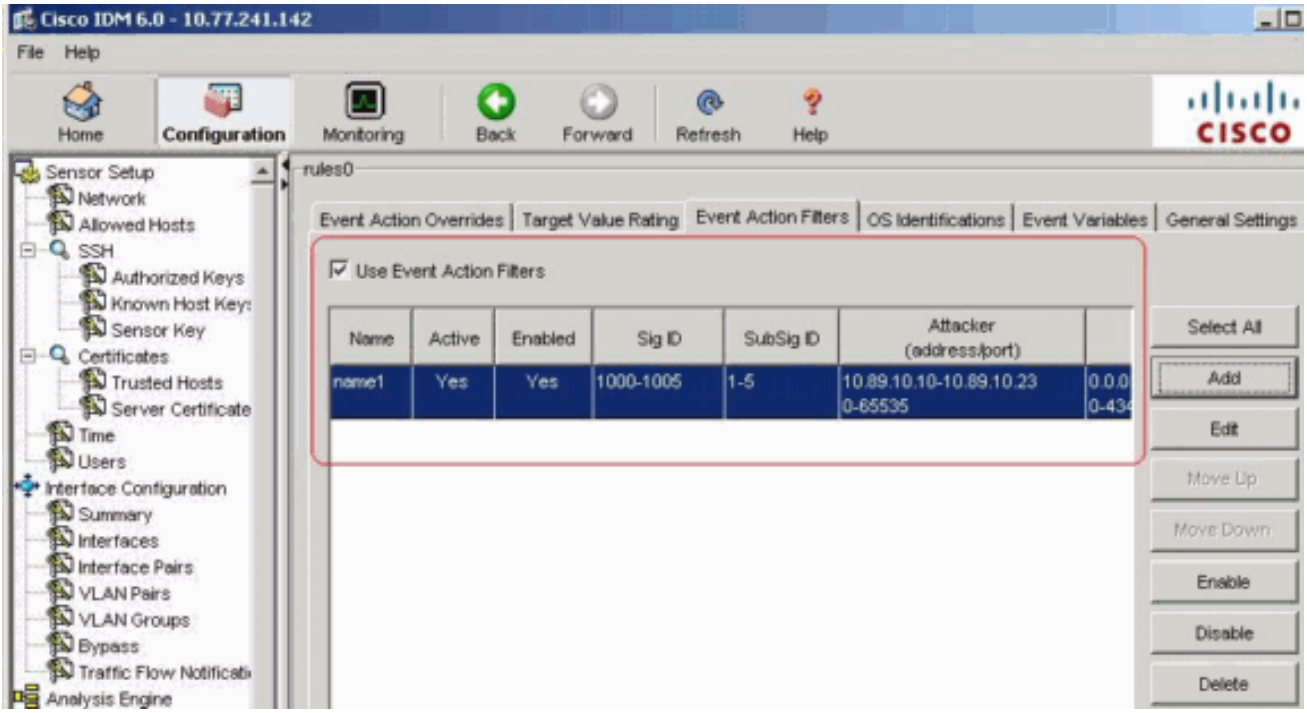
3. 検知時のアクション フィルタを追加するために『Add』 をクリック して下さい。追加検知時のアクション フィルター ダイアログ ボックスは現われます。
4. Name フィールドでは、名前をように検知時のアクション フィルタのための **name1** 入力して下さい。既定値 の 名前は供給されます、より多くのわかりやすい名前にそれを変更できます。
5. アクティブなフィールドで、フィルタリング イベントに対する実施されるようにリストにこのフィルタを追加するために **Yesオプション・ ボタンを**クリックして下さい。
6. Enabled フィールドで、フィルタを有効に するために **Yesオプション・ ボタンを**クリックして下さい。**注**また検知時のアクション Filters タブの**使用 検知時のアクション Filters チェックボックスを**チェックして下さいか、または追加検知時のアクション フィルタ ダイアログ ボックスの **Yes チェックボックスを**チェックするかどうかに関係なく検知時のアクション フィルタのどれもイネーブルになるようになりません。
7. シグニチャ ID フィールドでは、このフィルタが適用するはずであるすべてのシグニチャのシグニチャ ID を入力して下さい。事象変数タブでそれらを定義した場合 1000、1005、または範囲、たとえば、SIG 変数の **1000-1005** か 1 つリストを、たとえば使用、できます。

序文 $ との変数。

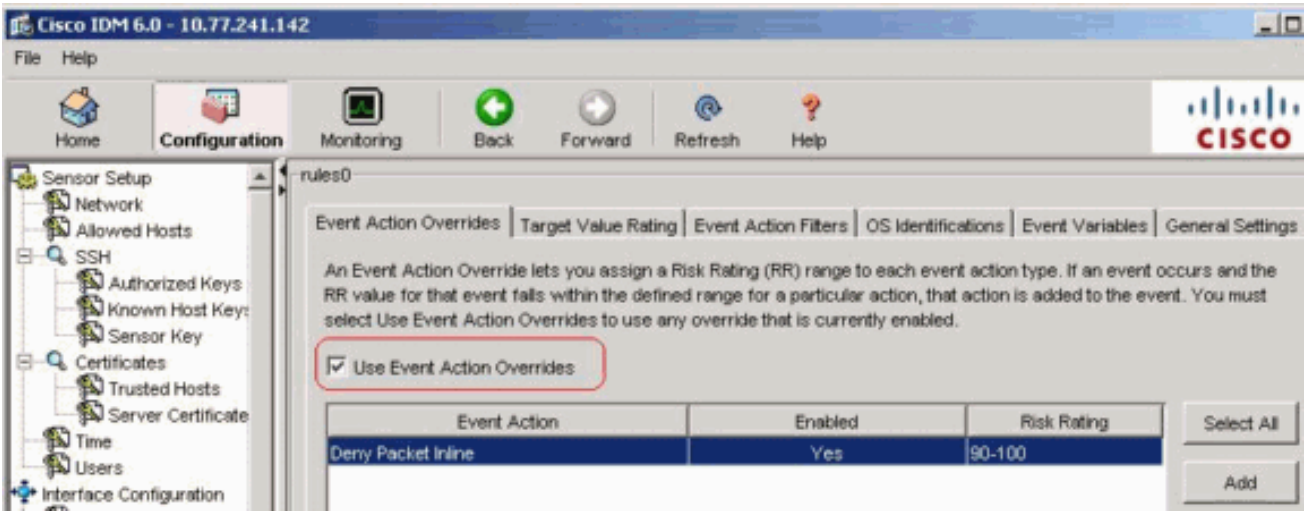
8. サブシグニチャ ID フィールドでは、このフィルタが適用するはずであるサブシグニチャのサブシグニチャ ID を入力して下さい。 たとえば、**1-5**。
9. 攻撃者 Address フィールドでは、ソースホストの IP アドレスを入力して下さい。事象変数タブでそれらを定義した場合変数の 1 つを使用できます。 序文 $ との変数。 また **10.89.10.10-10.89.10.23** アドレス範囲を、たとえば入力する、ことができます。 デフォルトは 0.0.0.0-255.255.255.255 です。
10. 攻撃者 Port フィールドでは、おこるパケットを送信 するために攻撃者によって使用されるポート番号を入力して下さい。
11. 犠牲者 Address フィールドでは、受信者のホストの IP アドレスを入力して下さい。事象変数タブでそれらを定義した場合変数の 1 つを使用できます。 序文 $ との変数。 また **192.56.10.1-192.56.10.255** アドレス範囲を、たとえば入力する、ことができます。 デフォルトは 0.0.0.0-255.255.255.255 です。
12. 犠牲者 Port フィールドでは、おこるパケットを受信するために攻撃の的となるホストによって使用されるポート番号を入力して下さい。 たとえば、**0-434**。
13. フィールドを評価するリスクではこのフィルタのための RR 範囲を入力して下さい。 たとえば、**85-100**。イベントのための RR が規定 する 範囲の内で下れば、イベントはこのフィルタの基準に対して処理されます。
14. ドロップダウン リストを引く操作からこのフィルタにイベントから取除いてほしい操作を選択して下さい。 たとえば、**TCP 接続を**『Reset』 を選択 して下さい。**ヒント**： リストの 1 つの検知時のアクションより『More』 を選択 するために **Ctrl** キーを維持して下さい。
15. OS 関連性ドロップダウン リストで、アラートが対象のために識別された OS に関連しているかどうか知りたいと思うかどうか選択して下さい。 たとえば、**関連した**選択して下さい。
16. 拒否パーセント フィールドでは、拒否攻撃者 機能のために否定するためにパケットのパーセントを入力して下さい。 たとえば、**90**。デフォルトは 100%です。
17. マッチ フィールドの停止では、これらのオプション ボタンの 1 つを選択して下さい:**はい**か。ほしければ検知時のアクションはこの特定のフィルタの操作が取除かれた後処理することを止めるようにコンポーネントをフィルタリングします残るどのフィルターでも処理されません; 従って、追加操作はイベントから取除くことができません。**いいえ**か。追加フィルターを処理し続けたいと思えば
18. コメント欄では、このフィルタの目的のようなこのフィルタと、保存したいと思うまたはなぜ特定の方法でこのフィルタを設定したコメント入力して下さい。 たとえば、**新しいフィルタ**。**ヒント**： 変更を取消し、追加検知時のアクション フィルター ダイアログ ボックスを閉じるために『Cancel』 をクリック して下さい。



19. [OK] をクリックします。新しい検知時のアクション フィルタは示されているように検知時のアクション Filters タブのリストに今現われます。

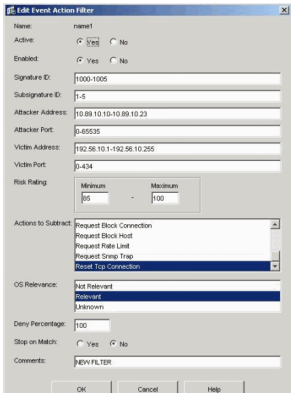


20. 示されているように**使用 検知時のアクション オーバーライド** チェックボックスをチェックして下さい。



注検知時のアクション オーバーライド タブの**使用 検知時のアクション オーバーライド** チェックボックスをチェックして下さいか、または検知時のアクション オーバーライドのどれも値に関係なくイネーブルになるように追加検知時のアクション フィルター ダイアログ ボックスで設定 されるなりません。

21. それを編集するためにリストの既存の検知時のアクション フィルタを選択し次に『Edit』をクリック して下さい。編集検知時のアクション フィルター ダイアログ ボックスは現われます。

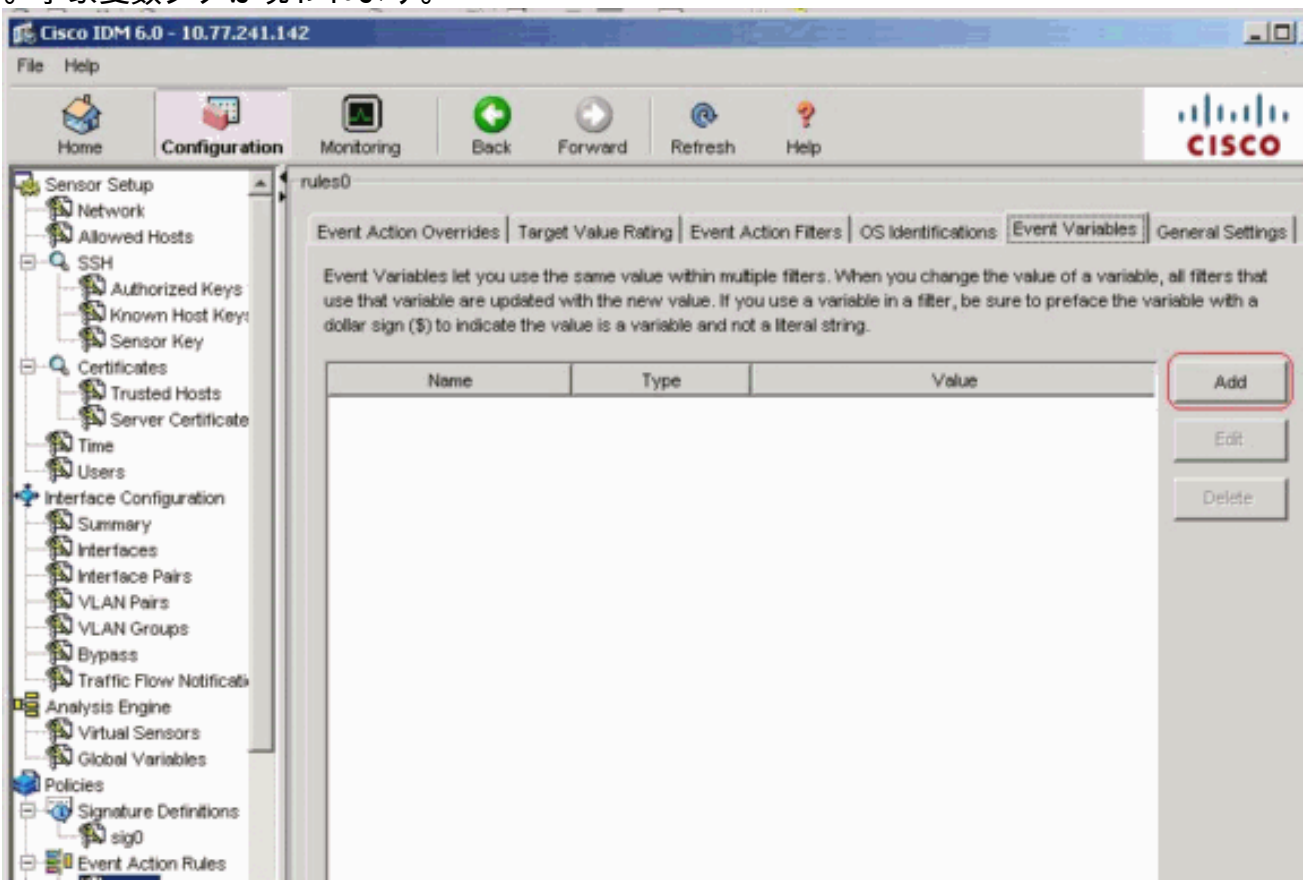


22. 変える必要があるフィールドの値を変更して下さい。フィールドに入力する方法の情報のためのステップ 4 〜 18 を参照して下さい。**ヒント：** 変更を取消し、編集検知時のアクション フィルター ダイアログ ボックスを閉じるために『Cancel』 をクリック して下さい。
23. [OK] をクリックします。編集された検知時のアクション フィルタは検知時のアクション Filters タブのリストに今現われます。
24. **使用 検知時のアクション オーバーライド** チェックボックスをチェックして下さい。**注**検知時のアクション オーバーライド タブの**使用 検知時のアクション オーバーライド** チェックボックスをチェックして下さいか、または検知時のアクション オーバーライドのどれも値に関係なく編集検知時のアクション フィルター ダイアログ ボックスで設定 される 有効に なりません。
25. それを削除するためにリストの検知時のアクション フィルタを選択し次に『Delete』 をクリック して下さい。検知時のアクション フィルタは検知時のアクション Filters タブのリストにもはや現われません。
26. 次に検知時のアクションを移動するためにリストで上下にフィルタリングしそれを選択し、『Move UP』 をクリック するか、または**移動して下さい。ヒント：** 変更を取除くために『Reset』 をクリック して下さい。
27. 変更を加え、修正された設定を保存するために『Apply』 をクリック して下さい。

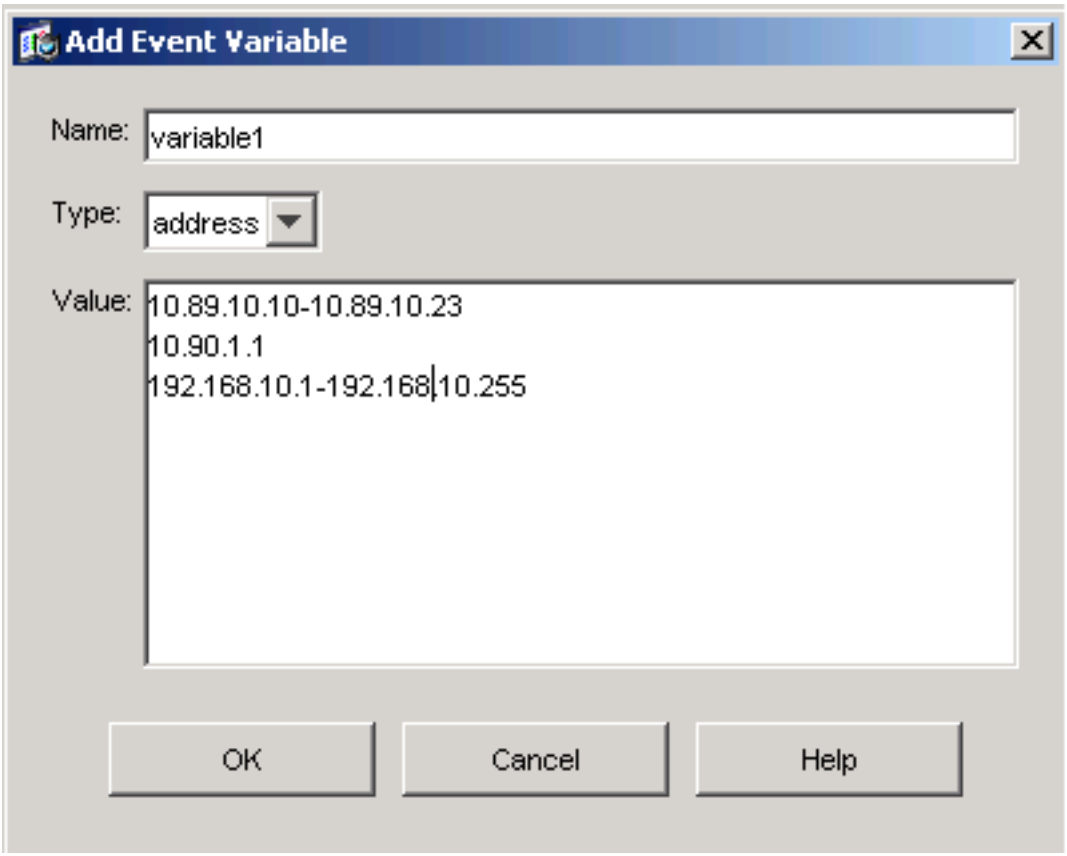
事象変数設定

事象変数を追加し、編集し、削除するためにこれらのステップを完了して下さい:

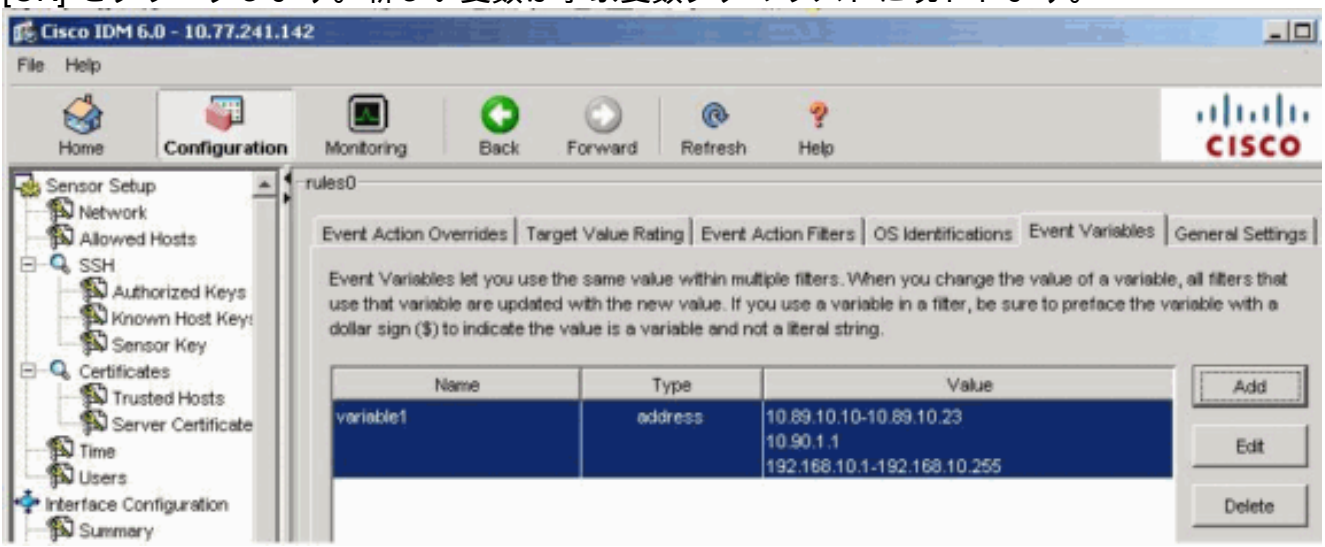
1. ログインする。 たとえば、管理者またはオペレータ特権とアカウントを使用して下さい。
2. ソフトウェア バージョンが 6.x である場合 **> 検知時のアクション支配します > rules0 > 事象変数** Configuration > Policies の順に選択 して下さい。 ソフトウェア バージョン 5.x に関しては、**> 検知時のアクション支配します > 事象変数**『Configuration』 を選択 して下さい。事象変数タブは現われます。



3. 変数を作成するために『Add』 をクリック して下さい。追加可変ダイアログボックスは現われます。
4. Name フィールドでは、この変数の名前を入力して下さい。**注**有効な名前は数か文字しか含まれていない場合があります。 またハイフン (-) かアンダースコア (_) を使用できます。
5. Value フィールドでは、この変数の値を入力して下さい。範囲の完全な IP アドレスか範囲またはセット 規定 して下さい。 次に、例を示します。10.89.10.10-10.89.10.2310.90.1.1192.168.10.1-192.168.10.255**注**デリミタとしてカンマを使用できます。 後ろ の スペースがカンマの後にないことを確かめて下さい。 さもなければ、 メッセージを受け取ります。**ヒント：** 変更を取消し、追加事象変数ダイアログボックスを閉じるために『Cancel』 をクリック して下さい。



6. [OK] をクリックします。新しい変数は事象変数タブのリストに現われます。



7. それを編集するためにリストの既存の変数を選択し次に『Edit』 をクリック して下さい。編集事象変数ダイアログボックスは現われます。
8. Value フィールドでは、値への変更を入力して下さい。
9. [OK] をクリックします。編集された事象変数は事象変数タブのリストに今現われます。**ヒ**

ント： 変更を取除くために『Reset』 を選択 して下さい。

10. 変更を加え、修正された設定を保存するために『Apply』 をクリック して下さい。

関連情報

- Cisco 侵入防御システムに関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems