IPS 5.x 以降： CLI と IDM を使用した、イベント アクション フィルタによるシグニチャの調整

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

このドキュメントは、Cisco IPS がインストールされ、適切に動作することを前提としています。

使用するコンポーネント

このドキュメントの情報は、ソフトウェア バージョン 5.0 以降が稼働する Cisco 4200 シリーズ IDS/IPS デバイスに基づくものです。

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。

イベント アクション フィルタ

イベント アクション フィルタの概要

イベント アクション フィルタは順序リストとして処理され、フィルタはリスト内で上下に移動できます。

フィルタによって、センサーは、イベントに応答して特定のアクションを実行できます。すべてのアクションを実行したり、イベント全体を削除したりする必要はありません。 フィルタは、イベントからアクションを削除することで機能します。 1 つのイベントからすべてのアクションを削除するフィルタは、イベントを効率的に消費します。

注: スイープ シグニチャをフィルタリングする場合は、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。 複数の宛先アドレスがある場合、最後のアドレスだけがフィルタとの照合に使用されます。

特定のアクションをイベントから削除するか、または、イベント全体を破棄してセンサーによる今後の処理を回避するように、イベント アクション フィルタを設定できます。 フィルタに対するアドレスをグループ化するために定義したイベント アクション変数を使用できます。 イベント アクション変数を設定する方法の手順についてはイベント アクション変数セクションの削除を追加、編集、を参照してください。

注: 文字列ではなく変数を使用することを示すために、変数の先頭にはドル記号（$）を付ける必要があります。 「$」を付けないと、「Bad source and destination」エラーが生じます。

CLI を使用したイベント アクション フィルタの設定

イベント アクション フィルタを設定するには、次の手順を実行します。

1. 管理者権限を持つアカウントで CLI にログインします。
2. イベント アクション ルール サブモードを開始します。`sensor#configure terminal sensor(config)#service event-action-rules rules1 sensor(config-eve)#`
3. フィルタ名を作成します。`sensor(config-eve)#filters insert name1 begin` name1、name2 などを使用して、イベント アクション フィルタの名前を指定します。 次のキーワードを使用します。begin | end | inactive | before | キーワードを指定すると、フィルタをどこに実装するか。
4. このフィルタの値を指定します。シグニチャ ID 範囲を指定します。`sensor(config-eve-fil)#signature-id-range 1000-1005` デフォルトは 900 ～65535 です。サブシグニチャ ID 範囲を指定します。`sensor(config-eve-fil)#subsignature-id-range 1-5` デフォルトは 0 ～255 です。攻撃者のアドレス範囲の指定:`sensor(config-eve-fil)#attacker-address-range 10.89.10.10-10.89.10.23` デフォルトは 0.0.0.0 ～ 255.255.255.255 です。攻撃対象のアドレス範囲を指定します。`sensor(config-eve-fil)#victim-address-range 192.56.10.1-192.56.10.255` デフォルトは 0.0.0.0 ～ 255.255.255.255 です。攻撃対象ポート範囲を指定します。`sensor(config-eve-fil)#victim-port-range 0-434` デフォルトは 0 ～65535 です。OS 関連性を指定します。`sensor(config-eve-fil)#os-relevance relevant` デフォルトは 0 ～100 です。リスク レーティング範囲を指定します。`sensor(config-eve-fil)#risk-rating-range 85-100` デフォルトは 0 ～100 です。削除するアクションを指定します。`sensor(config-eve-fil)#actions-to-remove`

reset-tcp-connection 拒否アクションをフィルタリングする場合は、必要な拒否アクションの割合を設定します。sensor(config-eve-fil)#**deny-attacker-percentage 90** デフォルトは 100 です。フィルタのステータスをディセーブルまたはイネーブルのいずれかに指定します。sensor(config-eve-fil)#**filter-item-status {enabled | disabled}** デフォルトではイネーブルになっています。一致パラメータで停止を指定します。sensor(config-eve-fil)#**stop-on-match {true | false}** True を指定すると、このアイテムが一致する場合にセンサーがフィルタの処理を停止します。 False を指定すると、このアイテムが一致する場合であってもセンサーはフィルタの処理を続行します。このフィルタを説明するために使用するコメントを追加します。sensor(config-eve-fil)#**user-comment NEW FILTER**

5. フィルタの設定を確認します。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には、次のようにします。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と4lを参照してください。
8. フィルタ リストでフィルタを上または下に移動するには、次のようにします。sensor(config-eve-fil)#**exit** sensor(config-eve)#**filters move name5 before name1**
9. フィルタが移動されたことを確認します。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 リストに移動するには、次のようにします。sensor(config-eve)#**filters move name1 inactive**
11. フィルタが非アクティブ リストに移動されたことを確認します。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-

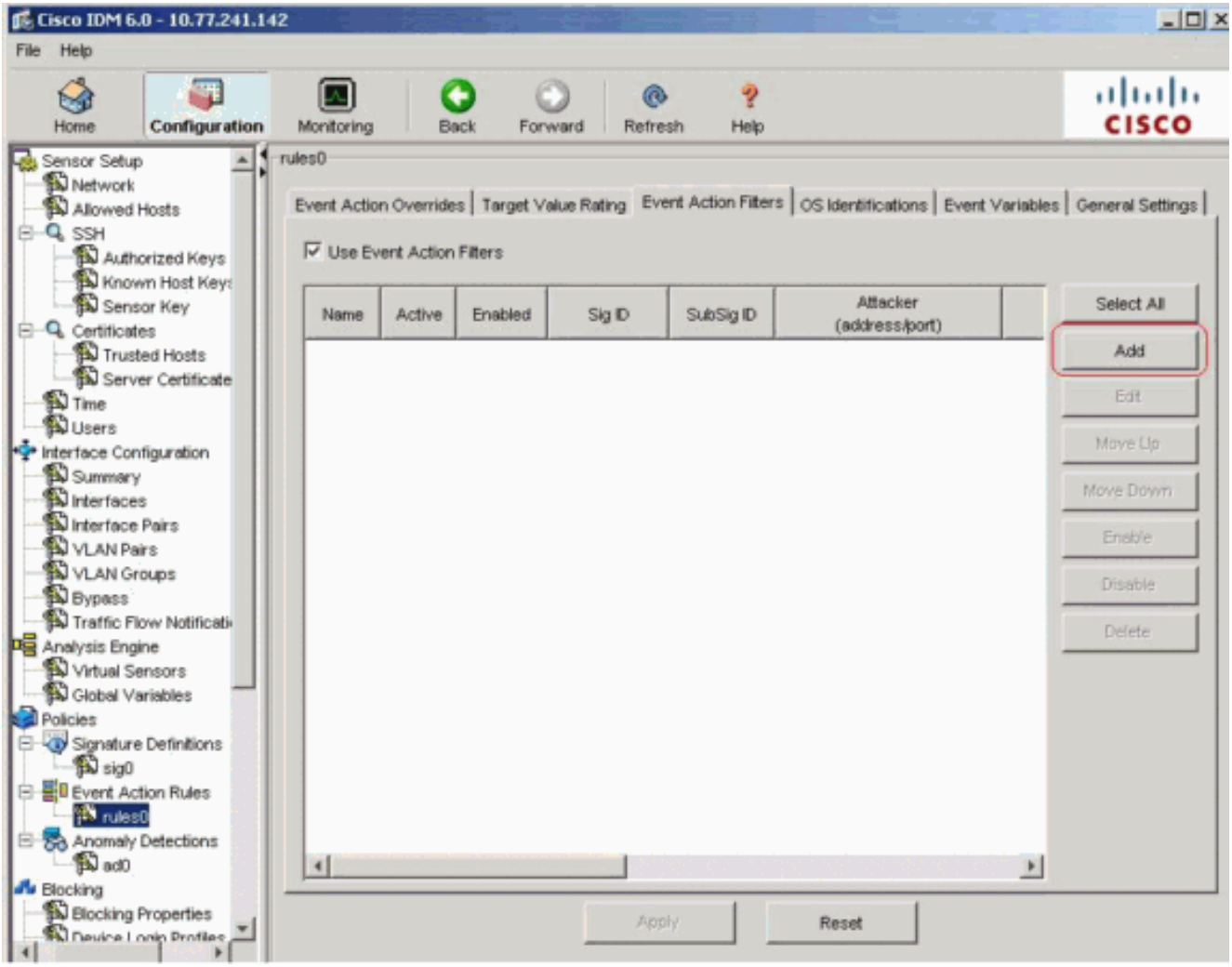
```
255.255.255.255 <defaulted> attacker-port-range: 0-65535 <defaulted> victim-port-range: 0-
65535 <defaulted> risk-rating-range: 0-100 <defaulted> actions-to-remove: <defaulted>
filter-item-status: Enabled <defaulted> stop-on-match: False <defaulted> user-comment:
<defaulted> ---------------------------------------------- ------------------------------
---------------- sensor(config-eve)#
```

12. イベント アクション ルール サブモードを終了します。`sensor(config-eve)#exit Apply Changes:?[yes]:`
13. 変更を適用する場合は Enter キーを押し、変更を廃棄する場合は「no」 を入力します。

IDMを使用した、イベント アクション フィルタ設定

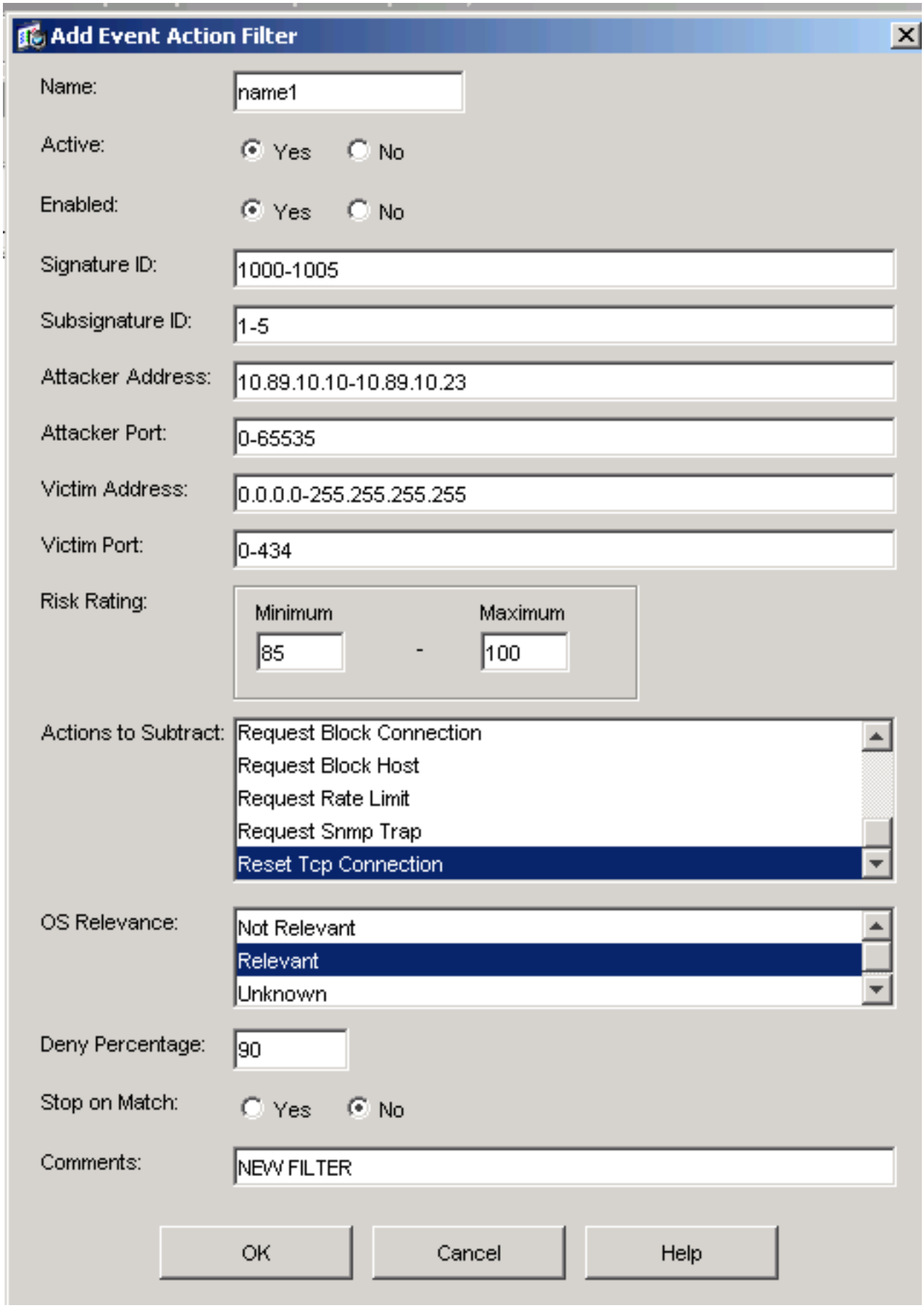
イベント アクション フィルタを追加、編集、削除、有効化および無効化、移動するには、次の手順を実行してください:

1. 管理者権限またはオペレータ権限を持つアカウントを使用して IDM にログインします。
2. ソフトウェア バージョンが6.x.**設定> >イベント アクション ルール** ポリシーrules0 > >イベント アクション フィルタを選択します。 ソフトウェア バージョン5.xでは、設定**>イベント アクション ルール>イベント アクション フィルタを選択します。**イベント アクション フィルタ タブが次のように表示されます。

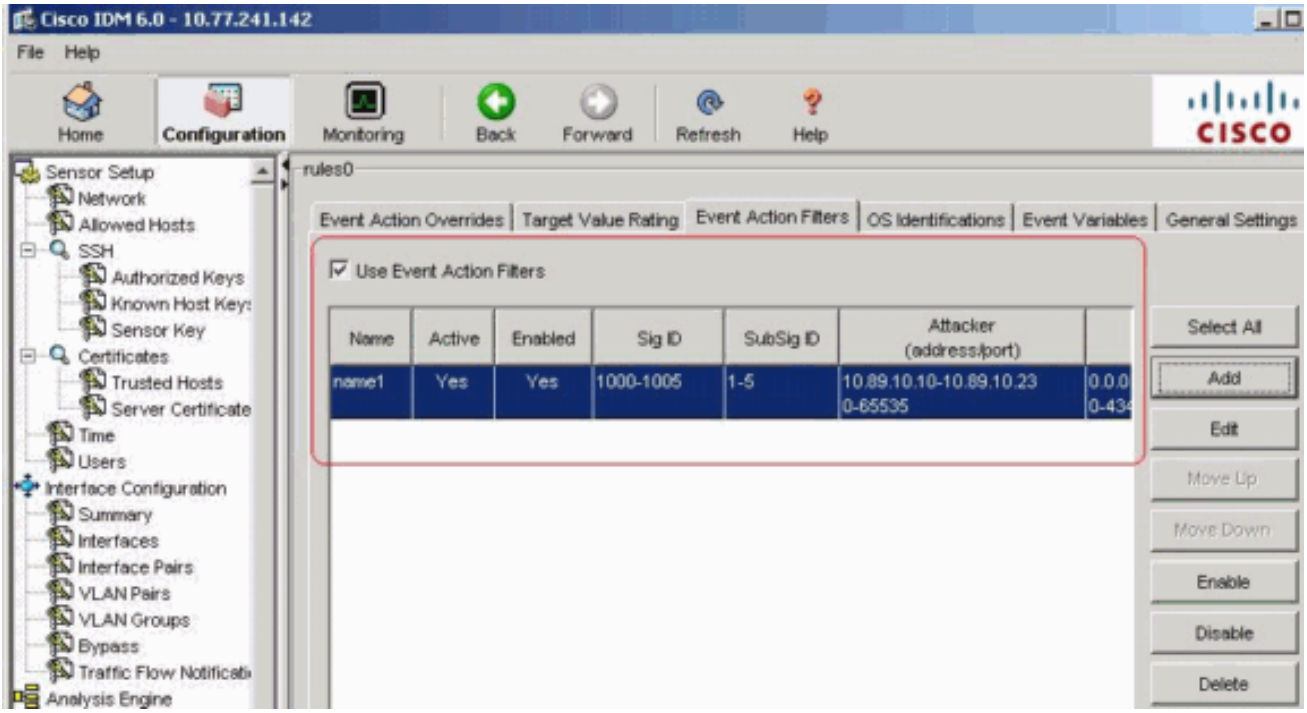


3. [イベント アクション フィルタを追加ます。[Add Event Action Filter] ダイアログボックスが表示されます。
4. [Name] フィールドに、イベント アクション フィルタの名前として、「name1」と入力します。デフォルト名が設定されますが、より意味のある名前に変更できます。
5. [Active] フィールドで、[Yes] オプション ボタンをクリックし、このフィルタをリストに追加して、フィルタリング イベントで有効にします。

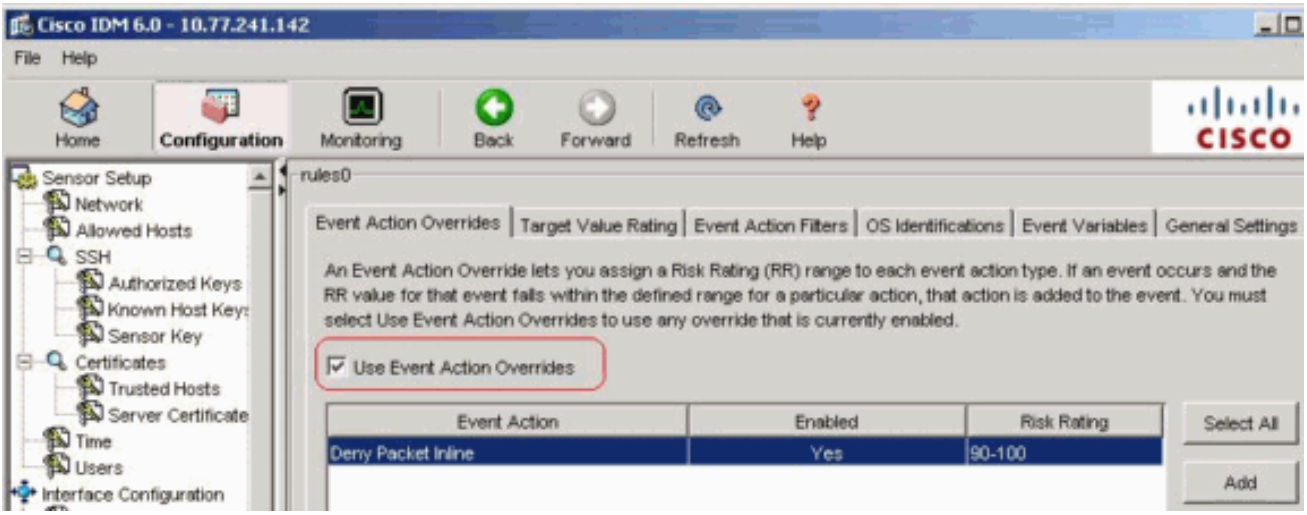
6. [Enabled] フィールドで [Yes] オプション ボタンをクリックし、フィルタをイネーブルにします。**注:** イベント アクション **フィルタ タブの使用の**イベント アクション フィルタのチェックボックスをオンにするか、または追加のイベント アクション フィルタ]ダイアログボックスの[Yes]チェックボックスをオンにするか**イベント アクション フィルタはいずれも有効になるように関係なくなりません。**
7. [Signature ID] フィールドに、このフィルタを適用するすべてのシグニチャのシグニチャ ID を入力します。リスト（例：1000, 1005）または範囲（例：**1000-1005**）の他、[Event Variables] タブで定義したいずれかの SIG 変数を使用できます。 変数の前には $ を付けます。
8. [SubSignature ID] フィールドには、このフィルタを適用するシグニチャのサブシグニチャ ID を入力します。 たとえば **1-5** と入力します。
9. [Attacker IPv4 Address] フィールドに、送信元ホストの IP アドレスを入力します。[Event Variables] タブで変数を定義済みであれば、そのうちの 1 つを使用できます。 変数の前には $ を付けます。 また、アドレスの範囲を入力することもできます（例：**10.89.10.10-10.89**）。 デフォルトは、0.0.0.0-255.255.255.255 です。
10. [Attacker Port] フィールドに、攻撃者が攻撃パケットを送信するために使用するポート番号を入力します。
11. [Victim Address] フィールドに、受信者ホストの IP アドレスを入力します。[Event Variables] タブで変数を定義済みであれば、そのうちの 1 つを使用できます。 変数の前には $ を付けます。 また、アドレスの範囲を入力することもできます（例：**192.56.10.1-192.56.10.255**）。 デフォルトは、0.0.0.0-255.255.255.255 です。
12. [Victim Port] フィールドに、攻撃対象ホストが攻撃パケットを受信するために使用するポート番号を入力します。 たとえば **0-434** と入力します。
13. [Risk Rating] フィールドに、このフィルタの RR 範囲を入力します。 たとえば **85-100** と入力します。イベントの RR が指定した範囲に収まる場合、イベントはこのフィルタの条件に照らして処理されます。
14. ドロップダウン リストから差し引く運用から、このフィルタにイベントから削除するアクションを選択します。 たとえば、Reset TCP Connection**を選択します。ヒント：** リスト**で**複数のイベント アクションを選択するにはCtrlキーを押したままにします。
15. [OS Relevance] ドロップダウン リストで、攻撃対象の OS として特定された OS にアラートが関連するかどうかを知る必要があるかどうかを選択します。 たとえば、[Relevant] を選択します。
16. [Deny Percentage] フィールドに、拒否攻撃者機能で拒否するパケットのパーセンテージを入力します。 たとえば、**90** に設定します。デフォルトは 100% です。
17. [Stop on Match] フィールドに、次のオプション ボタンのいずれかをクリックします。[Yes]：この特定のフィルタのアクションが削除された後に、Event Action Filters コンポーネントでの処理を停止するかどうか。残りのフィルタも処理されません; したがって、ここではイベントから削除できません。追加フィルタを処理することには非
18. [Comments] フィールドに、このフィルタの目的や、このフィルタを特定の方法で設定した理由など、このフィルタとともに保存するコメントを入力します。 たとえば、**新しいフィルタ。ヒント：** 変更を取り消すには、[キャンセル]をクリックして、追加のイベント アクション フィルタ]ダイアログボックスを閉じます。



19. [OK] をクリックします。次のように、新しいイベント アクション フィルタが [Event Action Filters] タブのリストに表示されます。

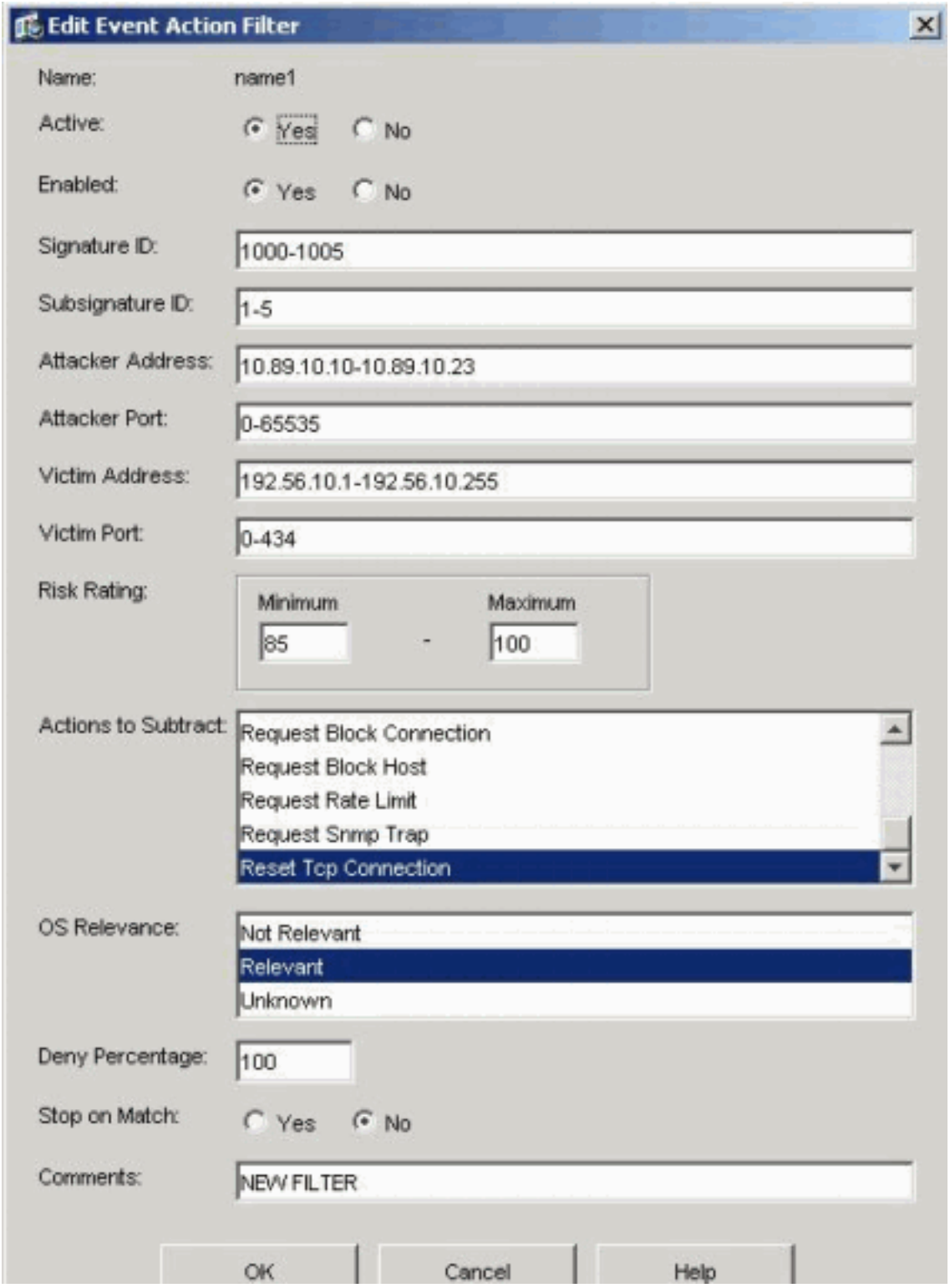


20. 次のよう**に使用のイベント アクション** オーバーライド]チェックボックスをオンにします。



注: [Event Action Overrides] タブの [Use Event Action Overrides] チェックボックスもオンにする必要があります。そうしない場合、[Add Event Action Filter] ダイアログボックスで設定した値にかかわらず、どのイベント アクション フィルタもイネーブルになりません。

21. これを行うには、リストの既存のイベント アクション フィルタを選択し、[Edit]をクリックします。[Edit Event Action Filter] ダイアログボックスが表示されます。



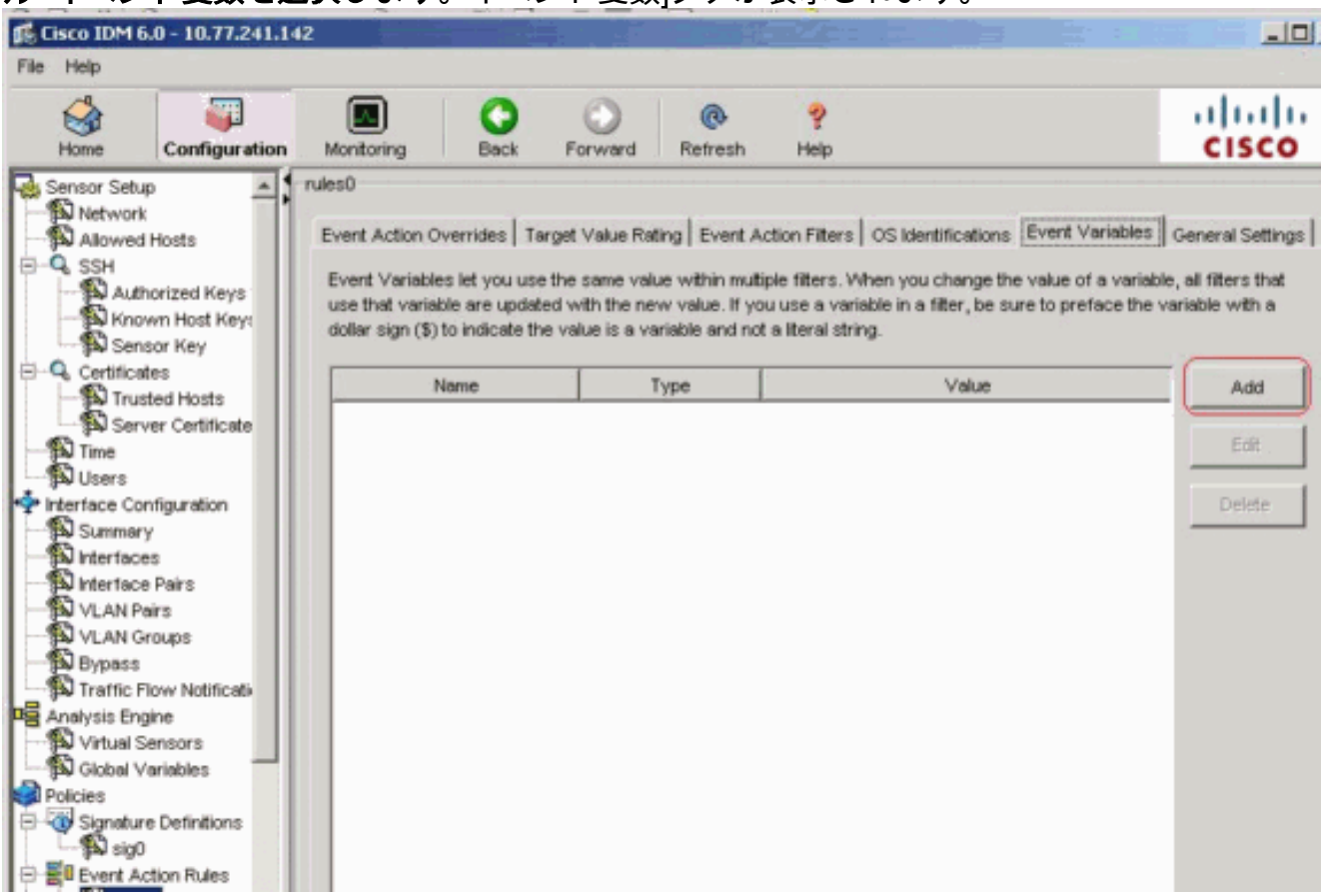
22. 、変更が必要なフィールドの値を変更します。フィールドに入力する方法については、ステップ4 ~ 18を参照してください。**ヒント：** 変更を取り消すには、[キャンセル]をクリックして編集イベント アクション フィルタ]ダイアログボックスを閉じます。
23. [OK] をクリックします。編集後のイベント アクション フィルタが [Event Action Filters] タブのリストに表示されます。
24. [Use Event Action Overrides] チェックボックスをオンにします。**注:** [Event Action Overrides] タブの [Use Event Action Overrides] チェックボックスをオンにする必要があります。そうしない場合、[Edit Event Action Filter] ダイアログ ボックスで設定した値にかかわらず、どのイベント アクション フィルタもイネーブルになりません。
25. これを削除するには、リストのイベント アクション フィルタを選択し、[削除]をクリックします。イベント アクション フィルタが [Event Action Filters] タブのリストに表示されなくなります。

26. イベント アクションを移動するリストでフィルタリング、を選択し、次に移動、クリックするとします。**ヒント：** 変更を削除するには、[Reset]をクリックします。
27. 変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

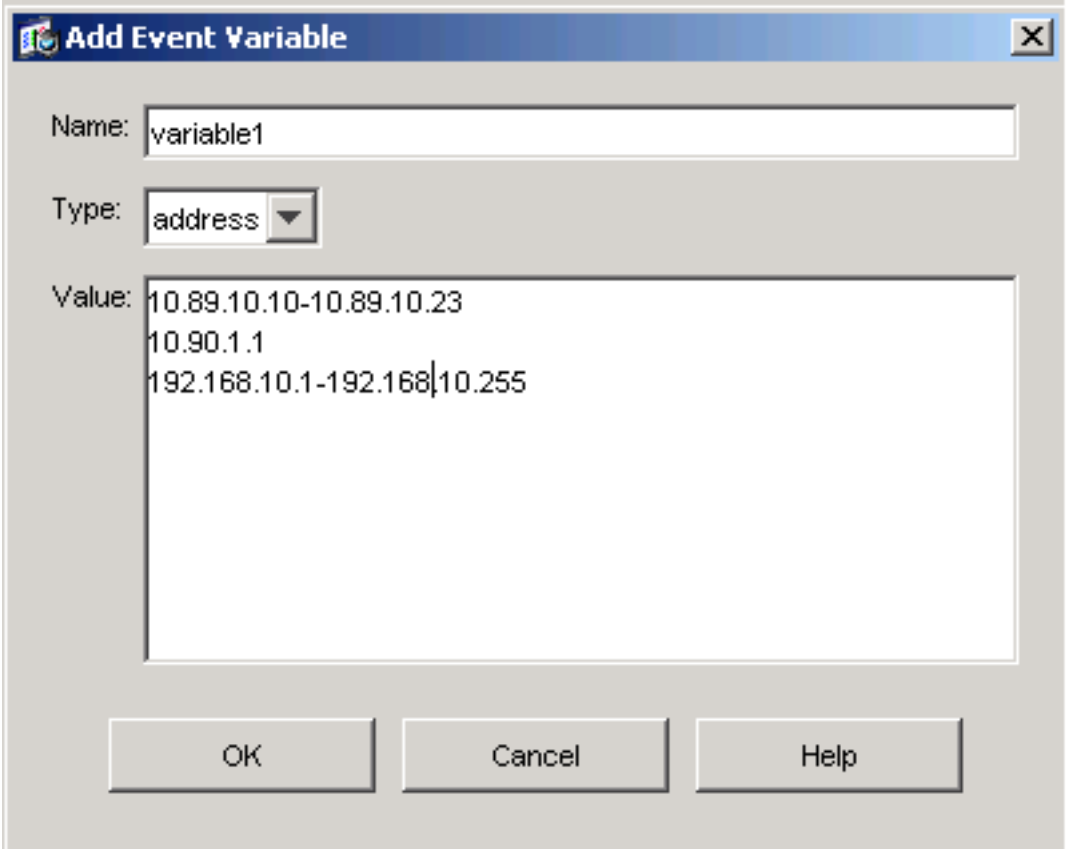
イベント キューの設定

イベント変数を追加、編集、削除するには、次の手順を実行します。

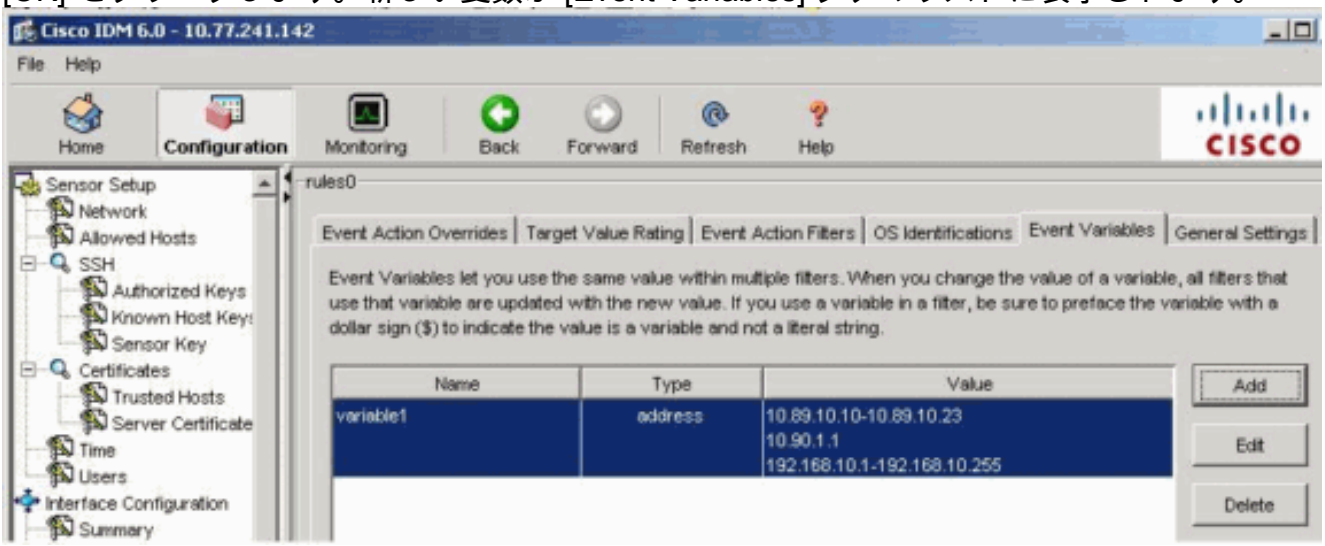
1. ログインする。 たとえば、Administratorまたはオペレータ特権アカウントを使用します。
2. ソフトウェア バージョンが6.x.**設定> >イベント アクション ルール** ポリシーrules0 > >イベント変数を選択します。 ソフトウェア バージョン5.xでは、設定**>イベント アクション ルール>イベント変数を選択します**。イベント変数]タブが表示されます。



3. [Add] をクリックして新しい変数を作成します。[Add Variable] ダイアログボックスが表示されます。
4. [Name] フィールドにこの変数の名前を入力します。**注:** 名前には、数字とアルファベットのみを使用できます。 また、ハイフン (-) またはアンダースコア (_) も使用できます。
5. [Value] フィールドにこの変数の値を入力します。完全な IP アドレス、範囲、複数の範囲を指定します。 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:** デリミタにはカンマが使用できます。 カンマの後にはスペースを入れないでください。 スペースを入力すると、「Validation failed」エラー メッセージを受け取ります。**ヒント：** 変更を取り消すには、[キャンセル]をクリックして、追加のイベント変数]ダイアログボックスを閉じます。



6. [OK] をクリックします。新しい変数が [Event Variables] タブのリストに表示されます。



7. これを行うには、リストの既存の変数を選択して[Edit]をクリックします。[Edit Event Variable] ダイアログボックスが表示されます。
8. [Value]フィールドに値を入力します。
9. [OK] をクリックします。編集したイベント変数が [Event Variables] タブのリストに表示されます。**ヒント：** 変更を削除するには[Resetを選択します。
10. 変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

関連情報

- Cisco Intrusion Prevention System 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