IPS 5.x 이상:CLI 및 IDM을 사용하여 이벤트 작업 필터로 서명 조정

목차

소개

이 문서에서는 CLI(Command Line Interface) 및 IDM(IDS Device Manager)을 사용하여 Cisco IPS(Intrusion Prevention System)의 이벤트 작업 필터로 서명을 조정하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에서는 Cisco IPS가 설치되어 제대로 작동한다고 가정합니다.

사용되는 구성 요소

이 문서의 정보는 소프트웨어 버전 5.0 이상을 실행하는 Cisco 4200 Series IDS/IPS 장치를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

이벤트 작업 필터

이벤트 작업 필터 이해

이벤트 작업 필터는 순서가 지정된 목록으로 처리되며 목록에서 필터를 위 또는 아래로 이동할 수 있습니다.

필터를 사용하면 센서가 모든 작업을 수행하거나 전체 이벤트를 제거하지 않고도 이벤트에 대한 응답으로 특정 작업을 수행할 수 있습니다.필터는 이벤트에서 작업을 제거함으로써 작동합니다.이벤트에서 모든 작업을 제거하는 필터는 이벤트를 효과적으로 소비합니다.

참고: 비우기 시그니처를 필터링할 때 대상 주소를 필터링하지 않는 것이 좋습니다.여러 목적지 주소가 있는 경우 마지막 주소만 필터와 일치시킵니다.

이벤트에서 특정 작업을 제거하거나 전체 이벤트를 삭제하고 센서에서 추가 처리를 방지하도록 이벤트 작업 필터를 구성할 수 있습니다.필터의 주소를 그룹화하기 위해 정의한 이벤트 작업 변수를 사용할 수 있습니다.이벤트 작업 변수를 구성하는 방법에 대한 절차는 이벤트 작업 변수 추가, 편집 및 삭제 섹션을 참조하십시오.

참고: 문자열 대신 변수를 사용함을 나타내려면 변수 앞에 달러 기호($)를 붙여야 합니다.그렇지 않으면 `Bad source  destination  .`

CLI를 사용하여 이벤트 작업 필터 컨피그레이션

이벤트 작업 필터를 구성하려면 다음 단계를 완료합니다.

1. 관리자 권한이 있는 계정으로 CLI에 로그인합니다.
2. 이벤트 작업 규칙 하위 모드를 입력합니다.
   ```
   sensor#configure terminal
   sensor(config)#service event-action-rules rules1
   sensor(config-eve)#
   ```
3. 필터 이름을 만듭니다.
   ```
   sensor(config-eve)#filters insert name1 begin
   ```

   name1, name2 등을 사용하여 이벤트 작업 필터의 이름을 지정합니다.**시작** 사용 **| 끝 | 비활성 | 이전** 필터를 삽입할 위치를 지정하려면 키워드 **| 뒤에** 오십시오.
4. 이 필터의 값을 지정합니다.서명 ID 범위를 지정합니다.
   ```
   sensor(config-eve-fil)#signature-id-range 1000-1005
   ```

   기본값은 900~65535입니다.하위 서명 ID 범위를 지정합니다.
   ```
   sensor(config-eve-fil)#subsignature-id-range 1-5
   ```

   기본값은 0~255입니다.공격자 주소 범위를 지정합니다.
   ```
   sensor(config-eve-fil)#attacker-address-range 10.89.10.10-10.89.10.23
   ```

   기본값은 0.0.0.0~255.255.255.255입니다.피해자 주소 범위를 지정합니다.
   ```
   sensor(config-eve-fil)#victim-address-range 192.56.10.1-192.56.10.255
   ```

   기본값은 0.0.0.0~255.255.255.255입니다.피해자 포트 범위를 지정합니다.
   ```
   sensor(config-eve-fil)#victim-port-range 0-434
   ```

기본값은 0~65535입니다.OS 관련성을 지정합니다.
```
sensor(config-eve-fil)#os-relevance relevant
```

기본값은 0~100입니다.위험 등급 범위를 지정합니다.
```
sensor(config-eve-fil)#risk-rating-range 85-100
```

기본값은 0~100입니다.제거할 작업 지정:
```
sensor(config-eve-fil)#actions-to-remove reset-tcp-connection
```

거부 작업을 필터링하는 경우 원하는 거부 작업의 비율을 설정합니다.
```
sensor(config-eve-fil)#deny-attacker-percentage 90
```

기본값은 100입니다.필터의 상태를 비활성화 또는 사용으로 설정합니다.
```
sensor(config-eve-fil)#filter-item-status {enabled | disabled}
```

기본값은 enabled입니다.match 매개 변수에 stop을 지정합니다.
```
sensor(config-eve-fil)#stop-on-match {true | false}
```

True는 센서에서 이 항목이 일치하는 경우 필터 처리를 중지하도록 지시합니다.False는 센서가 이 항목이 일치하더라도 필터를 계속 처리하도록 지시합니다.이 필터를 설명하기 위해 사용할 주석을 추가합니다.
```
sensor(config-eve-fil)#user-comment NEW FILTER
```

5. 필터의 설정을 확인합니다.

```
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. 기존 필터를 수정하려면

```
sensor(config-eve)#filters edit name1
```

7. 매개 변수를 수정하고 4a~4l 단계를 참조하십시오.
8. 필터 목록에서 필터를 위 또는 아래로 이동하려면

```
sensor(config-eve-fil)#exit
sensor(config-eve)#filters move name5 before name1
```

9. 필터를 이동했는지 확인합니다.

```
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. 필터를 비활성 목록으로 이동하려면

```
sensor(config-eve)#filters move name1 inactive
```

11. 필터가 비활성 목록으로 이동되었는지 확인합니다.

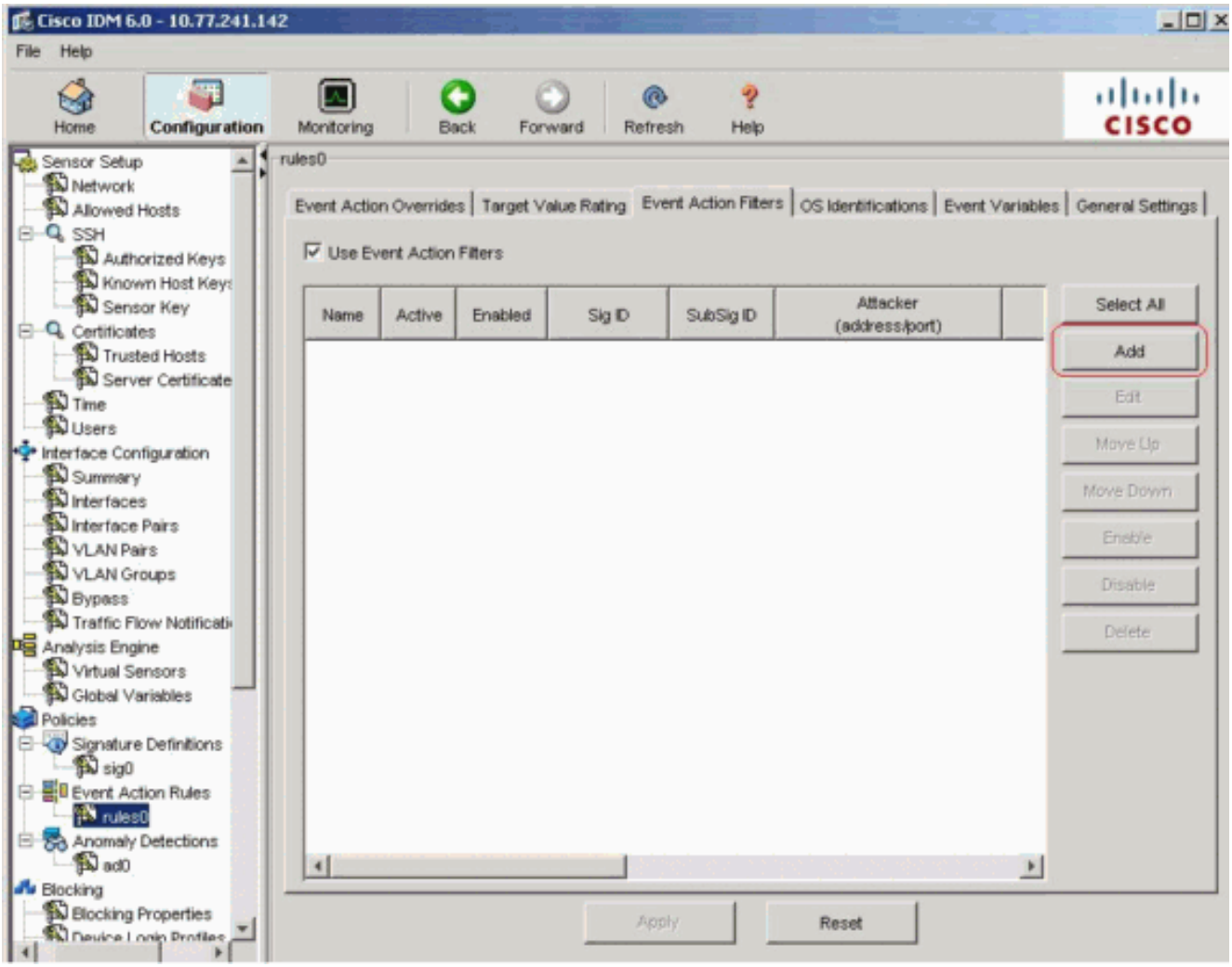
```
sensor(config-eve-fil)#exit
sensor(config-eve)#show settings

   ----------------------------------------------

   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. 이벤트 작업 규칙 하위 모드 종료:
```
sensor(config-eve)#exit
Apply Changes:?[yes]:
```
13. Enter를 눌러 변경 사항을 적용하거나 **no**를 입력하여 취소합니다.

IDM을 사용하는 이벤트 작업 필터 구성

이벤트 작업 필터를 추가, 편집, 삭제, 활성화, 비활성화 및 이동하려면 다음 단계를 완료하십시오.

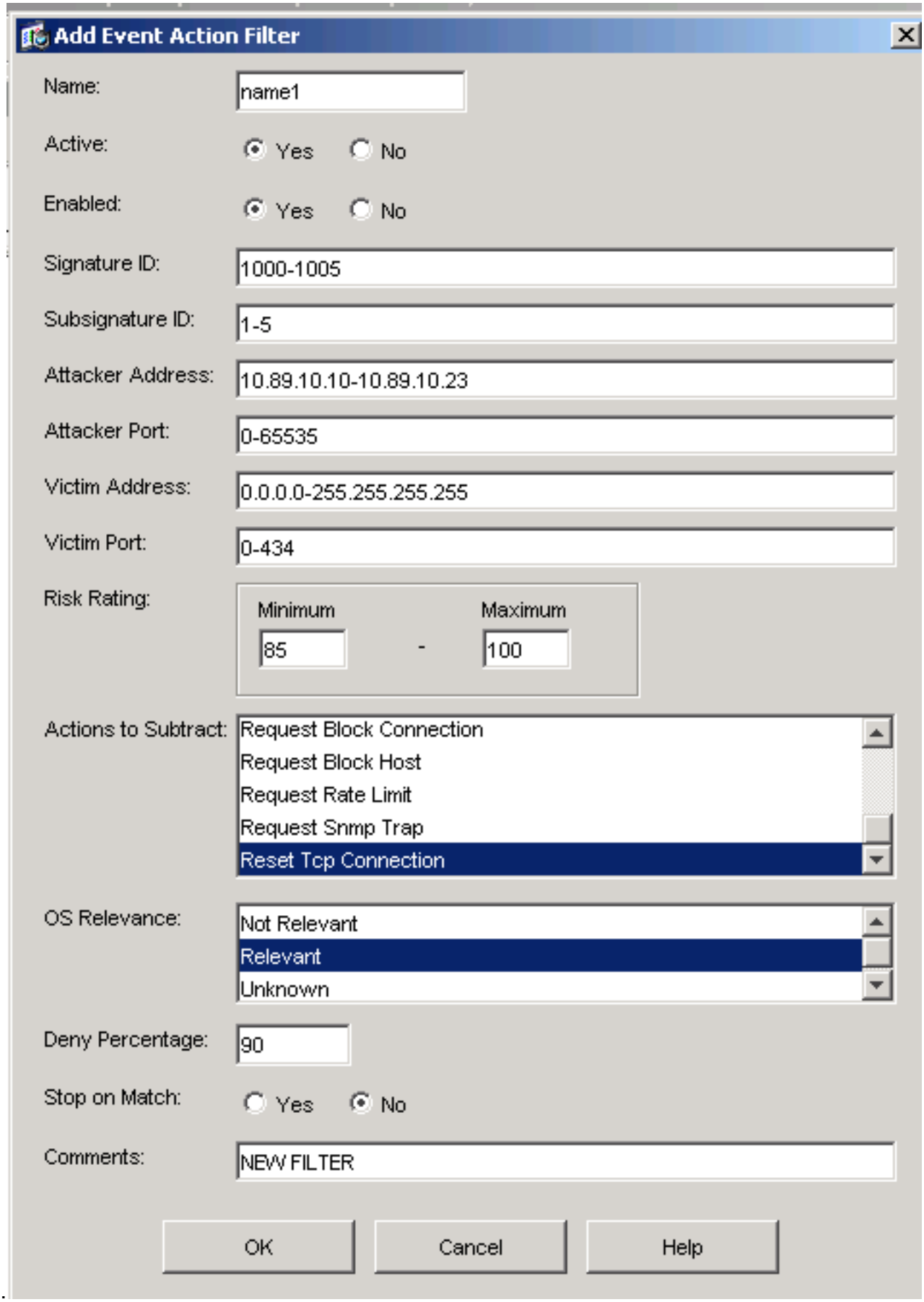
1. 관리자 또는 운영자 권한이 있는 계정으로 IDM에 로그인합니다.
2. 소프트웨어 버전이 6.x인 경우 Configuration **> Policies > Event Action Rules > rules0 > Event Action Filters**를 선택합니다.소프트웨어 버전 5.x의 경우 Configuration(구성) **> Event Action Rules(이벤트 작업 규칙) > Event Action Filters(이벤트 작업 필터)**를 선택합니다.Event Action Filters 탭이 표시된 대로 나타납니다
   .



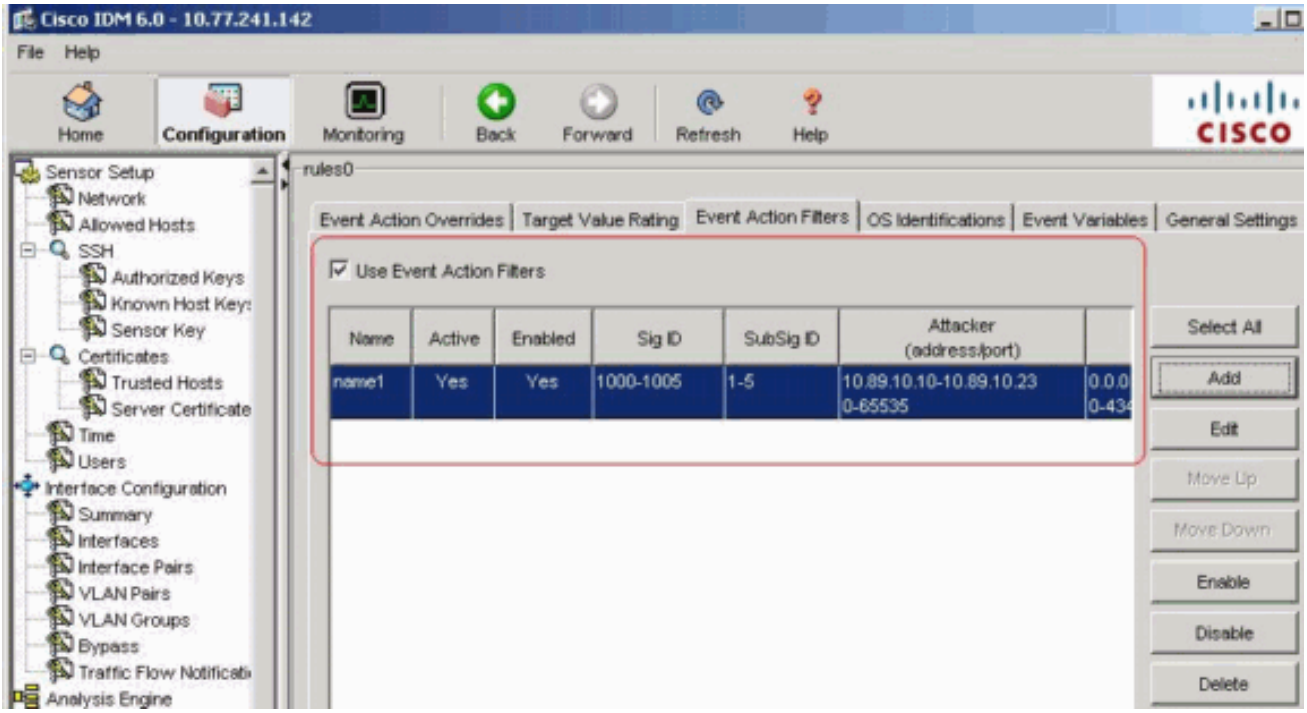
3. 이벤트 작업 필터를 추가하려면 Add를 클릭합니다.Add Event Action Filter 대화 상자가 나타납니다.
4. Name 필드에 이벤트 작업 필터의 이름1을 입력합니다.기본 이름이 제공되지만 더 의미 있는 이름으로 변경할 수 있습니다.
5. Active(활성) 필드에서 **Yes(예)** 라디오 버튼을 클릭하여 이 필터를 목록에 추가하여 이벤트 필터링에 적용합니다.
6. Enabled(활성화됨) 필드에서 **Yes(예)** 라디오 버튼을 클릭하여 필터를 활성화합니다.**참고:** 또한 Event Action Filters(이벤트 작업 필터) 탭에서 Use Event Action Filters(이벤트 작업 필터 **사용**) 확인란을 선택해야 합니다. 그렇지 않으면 Add Event Action Filter(이벤트 작업 필터 추가) 대화 상자에서 Yes(예) 확인란을 선택했는지 여부와 상관없이 이벤트 작업 필터가 활성화되지 않습니다.
7. Signature ID 필드에 이 필터를 적용해야 하는 모든 서명의 서명 ID를 입력합니다.목록(예: 1000, 1005 또는 범위)을 사용할 수 있습니다(예: **1000-1005** 또는 SIG 변수 중 하나).변수 앞에 $ 를 입력합니다.
8. SubSignature ID 필드에 이 필터를 적용할 하위 서명의 하위 서명 ID를 입력합니다.예: **1-5**.
9. Attacker Address 필드에 소스 호스트의 IP 주소를 입력합니다.Event Variables 탭에서 변수를 정의한 경우 변수 중 하나를 사용할 수 있습니다.변수 앞에 $ 를 입력합니다.주소 범위를 입력할 수도 있습니다(예: **10.89.10.10-10.89.10.23**). 기본값은 0.0.0.0-255.255.255.255입니다.
10. 공격자 포트 필드에 공격자가 문제의 패킷을 전송하기 위해 사용하는 포트 번호를 입력합니다.
11. 피해자 주소 필드에 수신자 호스트의 IP 주소를 입력합니다.Event Variables 탭에서 변수를 정의한 경우 변수 중 하나를 사용할 수 있습니다.변수 앞에 $ 를 입력합니다.주소 범위를 입력할 수도 있습니다(예: **192.56.10.1-192.56.10.255**). 기본값은 0.0.0.0-255.255.255.255입니

다.

12. 피해자 포트 필드에 피해자 호스트가 문제의 패킷을 수신하기 위해 사용하는 포트 번호를 입력합니다.예: **0-434**.
13. Risk Rating(위험 등급) 필드에 이 필터의 RR 범위를 입력합니다.예: **85-100**.이벤트에 대한 RR이 지정한 범위 내에 있으면 이 필터의 기준에 따라 이벤트가 처리됩니다.
14. Actions to Subtract 드롭다운 목록에서 이 필터가 이벤트에서 제거할 작업을 선택합니다.예를 들어, Reset **TCP connection을** 선택합니다.**팁:** Ctrl 키를 누른 채 목록에서 둘 이상의 이벤트 작업을 선택합니다.
15. OS Relevance(OS 관련성) 드롭다운 목록에서 해당 경고가 피해자에 대해 식별된 OS와 관련이 있는지 확인할지 여부를 선택합니다.예를 들어, Relevant를 **선택합니다**.
16. Deny Percentage 필드에 공격자 기능을 거부하기 위해 패킷의 비율을 입력합니다.예를 들어, **90**.기본값은 100%입니다.
17. Stop on Match 필드에서 다음 라디오 버튼 중 하나를 선택합니다.**Yes**(예) - 이 특정 필터의 작업이 제거된 후 Event Action Filters(이벤트 작업 필터) 구성 요소가 처리를 중지하도록 하려면남아 있는 필터는 처리되지 않습니다.따라서 이벤트에서 추가 작업을 제거할 수 없습니다.**아니요**—추가 필터를 계속 처리하려는 경우
18. Comments 필드에 이 필터의 목적이나 특정 방법으로 이 필터를 구성한 이유 등 이 필터에 저장할 주석을 입력합니다.예: **NEW FILTER**.**팁: 취소**를 클릭하여 변경 사항을 취소하고 이벤트 작업 필터 추가 대화 상자를 닫습니다

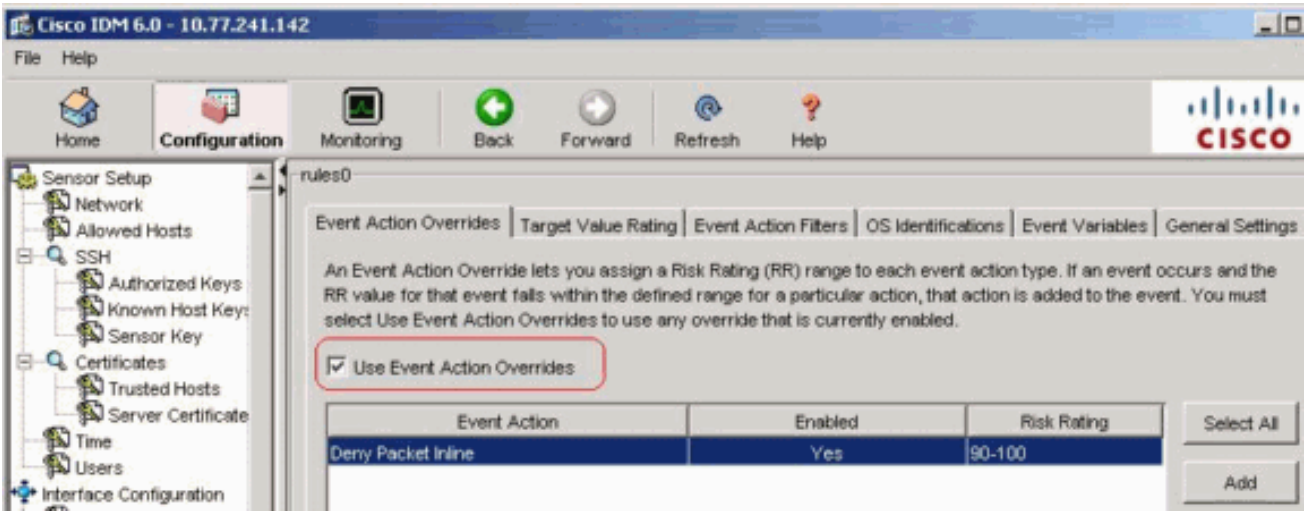


19. **확인**을 **클릭합니다**.이제 새 이벤트 작업 필터가 표시된 대로 Event Action Filters 탭의 목록에 나타납니다
.



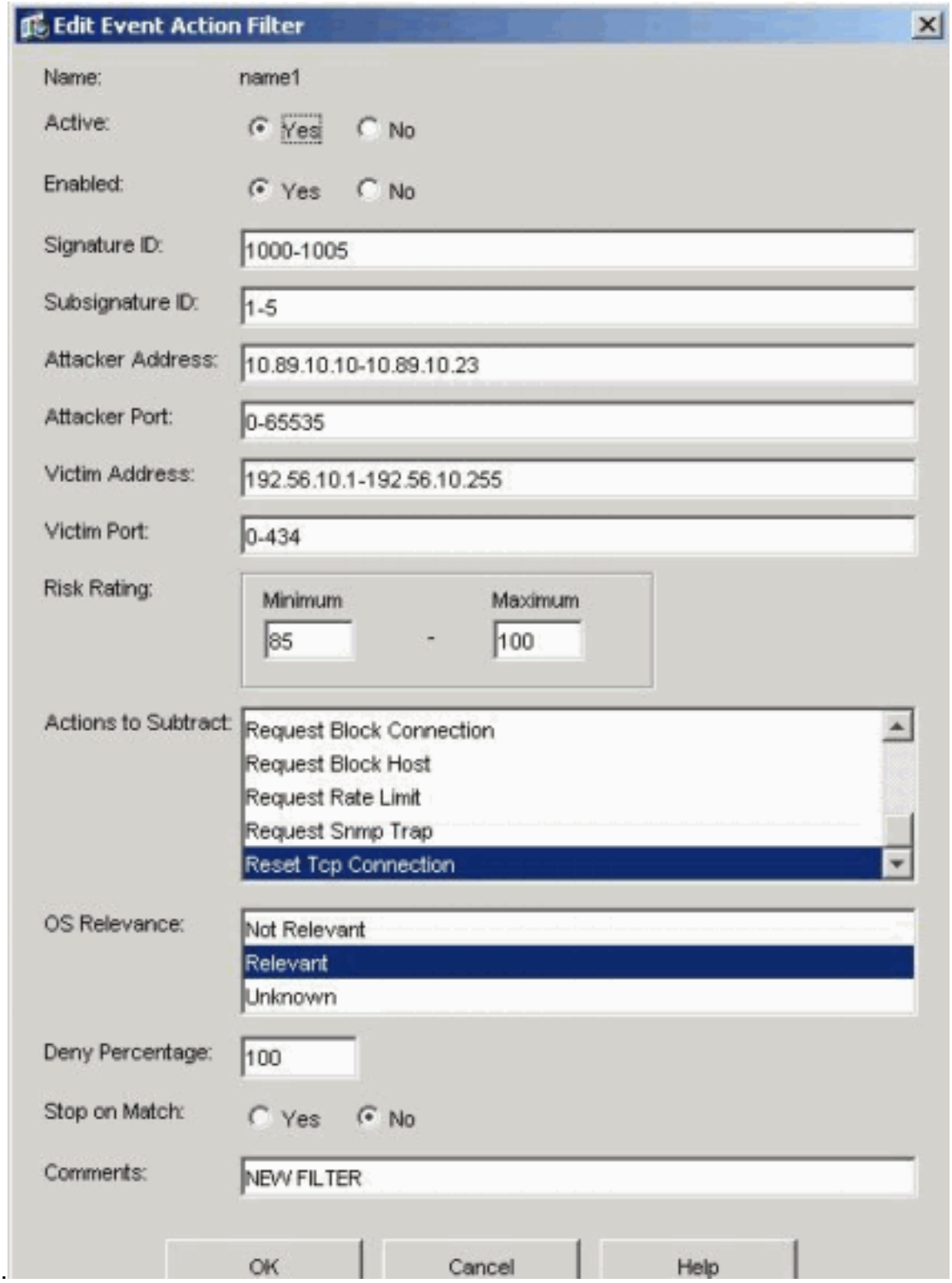
20. 표시된 대로 **Use Event Action Overrides** 확인란을 선택합니다

.



참고: Event Action Overrides(이벤트 작업 재정의) 탭에서 Use Event Action Overrides(이벤트 작업 재정의 사용) 확인란을 선택해야 합니다. 그렇지 않으면 Add Event Action Filter(이벤트 작업 필터 추가) 대화 상자에서 설정한 값과 상관없이 이벤트 작업 재정의가 활성화되지 않습니다.

21. 목록에서 기존 이벤트 작업 필터를 선택하여 수정한 다음 **Edit**를 클릭합니다.Edit Event Action Filter 대화 상자가 나타납니다



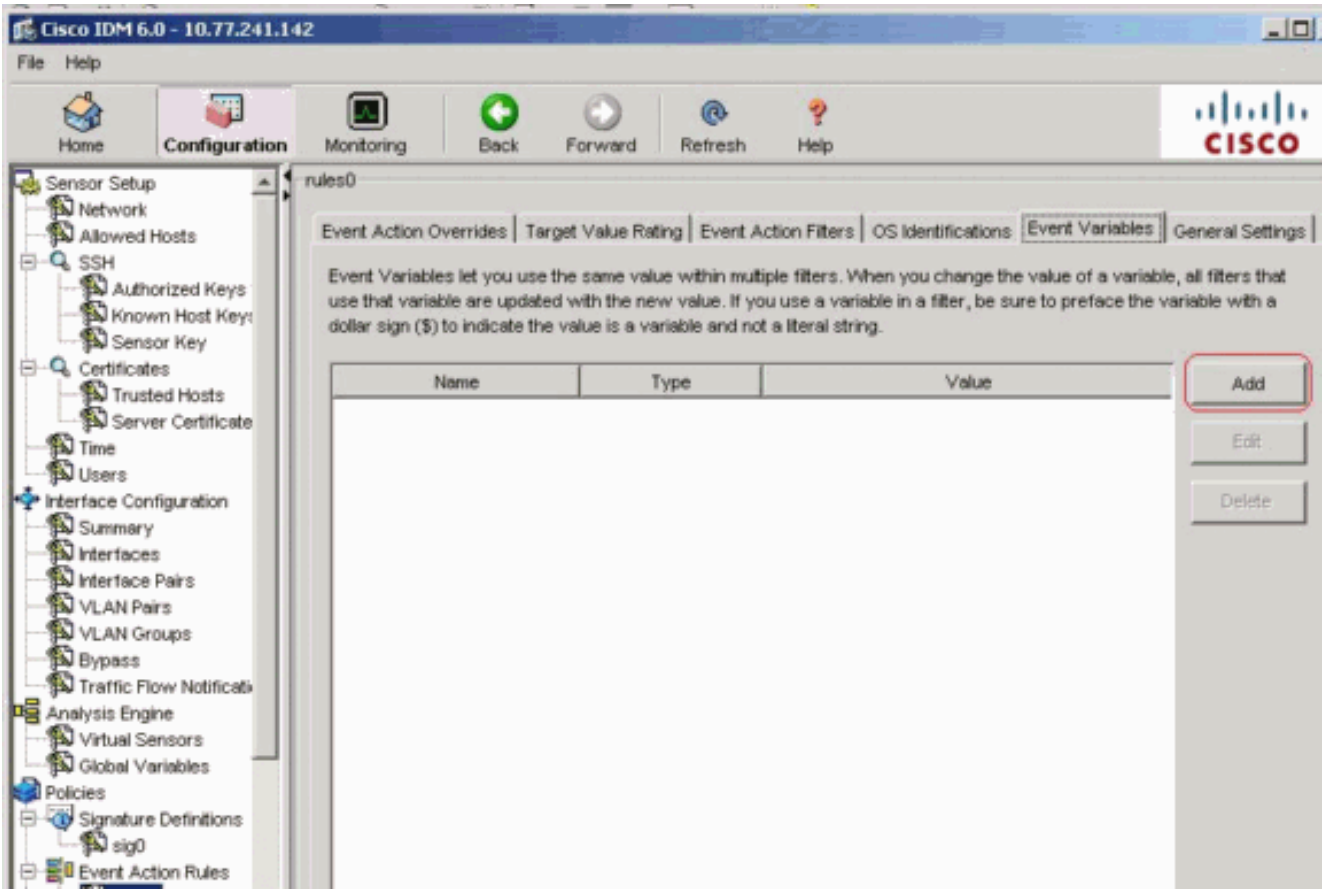
22. 변경해야 할 필드의 값을 변경합니다.필드를 완료하는 방법은 4~18단계를 참조하십시오.**팁: 취소**를 클릭하여 변경 사항을 취소하고 이벤트 작업 필터 편집 대화 상자를 닫습니다.
23. **확인**을 **클릭합니다**.편집한 이벤트 작업 필터가 Event Action Filters 탭의 목록에 나타납니다.
24. Use Event **Action Overrides(이벤트 작업 재정의 사용**) 확인란을 선택합니다.**참고:** Event Action Overrides(이벤트 작업 재정의) 탭에서 Use Event Action Overrides(이벤트 작업 재정의 사용) 확인란을 선택해야 합니다. 그렇지 않으면 Edit Event Action Filter(이벤트 작업 필터 수정) 대화 상자에서 설정한 값과 상관없이 이벤트 작업 재정의가 활성화되지 않습니다.
25. 목록에서 이벤트 작업 필터를 선택하여 삭제한 다음 **삭제**를 클릭합니다.이벤트 작업 필터는 Event Action Filters 탭의 목록에 더 이상 나타나지 않습니다.
26. 이벤트 작업을 이동하려면 목록에서 위 또는 아래로 필터링하고 선택한 다음 위로 **이동** 또는 **아래로 이동을** 클릭합니다.**팁:** 변경 사항을 제거하려면 재설정을 클릭합니다.
27. 변경 사항을 적용하고 수정된 컨피그레이션을 저장하려면 **Apply**를 클릭합니다.

이벤트 변수 구성

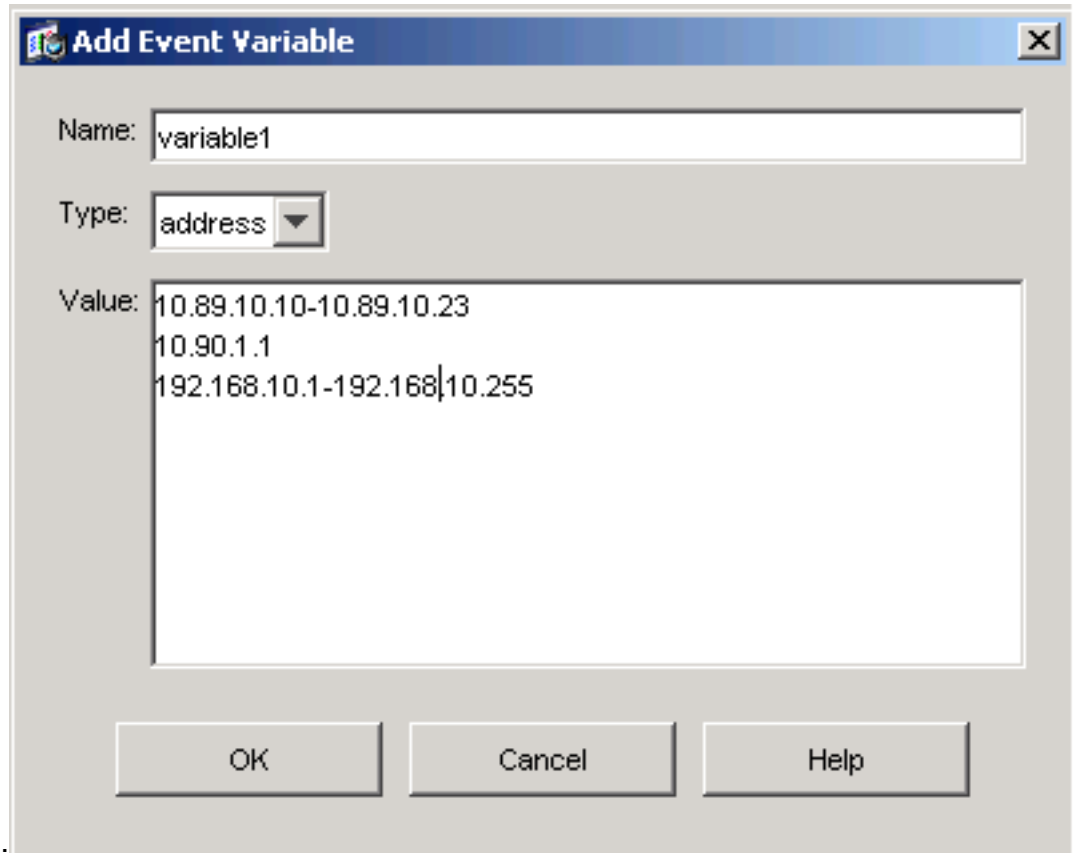
이벤트 변수를 추가, 수정 및 삭제하려면 다음 단계를 완료하십시오.

1. 로그인합니다.예를 들어 관리자 또는 운영자 권한이 있는 계정을 사용합니다.
2. 소프트웨어 버전이 6.x인 경우 **Configuration > Policies > Event Action Rules > rules0 > Event Variables**를 선택합니다.소프트웨어 버전 5.x의 경우 Configuration(구성) **> Event Action Rules(이벤트 작업 규칙) > Event Variables(이벤트 변수)**를 선택합니다.Event Variables 탭이 나타납니다

.

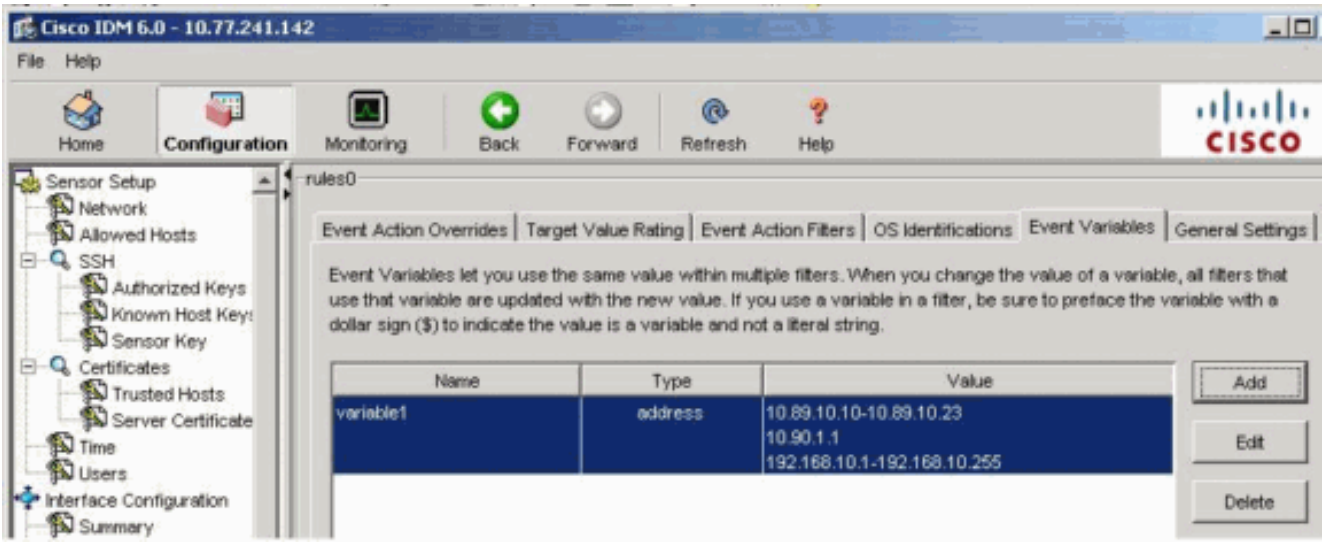


3. 변수를 생성하려면 Add를 클릭합니다.Add Variable 대화 상자가 나타납니다.
4. Name 필드에 이 변수의 이름을 입력합니다.**참고:** 유효한 이름은 숫자나 문자만 포함할 수 있습니다.하이픈(-) 또는 밑줄(_)을 사용할 수도 있습니다.
5. 값 필드에 이 변수의 값을 입력합니다.전체 IP 주소 또는 범위 또는 범위 집합을 지정합니다.예:10.89.10.10-10.89.10.2310.90.1.1192.168.10.1-192.168.10.255**참고:** 쉼표를 구분 기호로 사용할 수 있습니다.쉼표 뒤에 공백이 없어야 합니다.그렇지 않으면 유효성 검사 오류 메시지가 표시됩니다.**팁: 취소**를 클릭하여 변경 사항을 취소하고 이벤트 변수 추가 대화 상자를 닫습니



다.

6. **확인**을 **클릭합니다**.새 변수가 Event Variables 탭의 목록에 나타납니다



7. 목록에서 기존 변수를 선택하여 수정한 다음 **Edit**를 클릭합니다.Edit Event Variable 대화 상자가 나타납니다.
8. 값 필드에 값의 변경 사항을 입력합니다.
9. **확인**을 **클릭합니다**.편집한 이벤트 변수가 Event Variables 탭의 목록에 나타납니다.**팁:** 변경 사항을 제거하려면 재설정을 선택합니다.
10. 변경 사항을 적용하고 수정된 컨피그레이션을 저장하려면 **Apply**를 클릭합니다.

관련 정보

- Cisco Intrusion Prevention System 지원 페이지
- 기술 지원 및 문서 – Cisco Systems