IME를 사용하여 IPS TCP 재설정 구성

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[표기 규칙](#)
[구성](#)
[네트워크 다이어그램](#)
[구성](#)
[센서 구성 시작](#)
[IME에 센서 추가](#)
[Cisco IOS 라우터에 대한 TCP 재설정 구성](#)
[다음을 확인합니다.](#)
[공격 및 TCP 재설정 실행](#)
[문제 해결](#)
[팁](#)
[관련 정보](#)

소개

이 문서에서는 IPS Manager Express(IME)를 사용하여 IPS(Intrusion Prevention System) TCP 재설정의 컨피그레이션에 대해 설명합니다. IME 및 IPS 센서는 TCP 재설정을 위한 Cisco 라우터를 관리하는 데 사용됩니다. 이 구성을 검토할 때 다음 항목을 기억하십시오.

- 센서를 설치하고 센서가 제대로 작동하는지 확인합니다.
- 스니핑 인터페이스를 인터페이스 외부의 라우터로 확장합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IPS Manager Express 7.0
- Cisco IPS Sensor 7.0(0.88)E3

- Cisco IOS Software 릴리스 12.4가 포함된 Cisco IOS® 라우터

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.

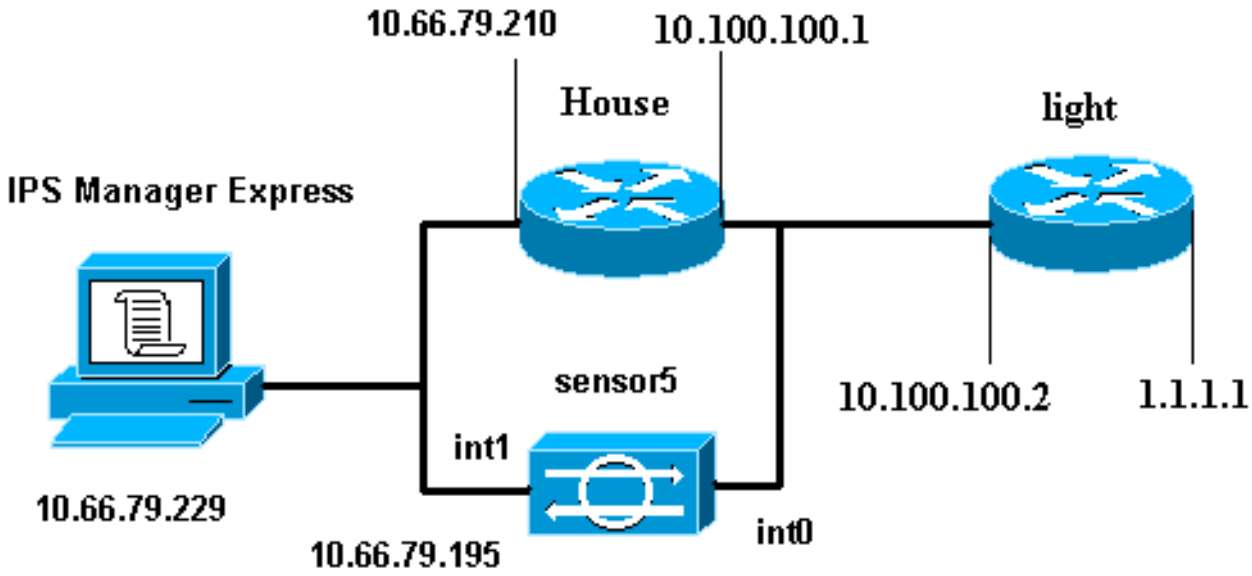
표기 규칙

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

구성

네트워크 다이어그램

이 문서에서는 이 다이어그램에 표시된 네트워크 설정을 사용합니다.



구성

이 문서에서는 여기에 표시된 구성을 사용합니다.

- 라우터 표시등
- 라우터 하우스

라우터 표시등

```
Current configuration : 906 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname light
!
```

```
enable password cisco
!
username cisco password 0 cisco
ip subnet-zero
!
!
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
call rsvp-sync
!
!
!
fax interface-type modem
mta receive maximum-recipients 0
!
controller E1 2/0
!
!
!
interface FastEthernet0/0
 ip address 10.100.100.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 1.1.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface BRI4/0
 no ip address
 shutdown
!
interface BRI4/1
 no ip address
 shutdown
!
interface BRI4/2
 no ip address
 shutdown
!
interface BRI4/3
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.100.100.1
ip http server
ip pim bidir-enable
!
!
dial-peer cor custom
!
!
line con 0
line 97 108
line aux 0
line vty 0 4
 login
!
end
```

라우터 하우스

```
Current configuration : 939 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname house
!
logging queue-limit 100
enable password cisco
!
ip subnet-zero
!
!
no ip cef
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
!
!
interface FastEthernet0/0
 ip address 10.66.79.210 255.255.255.224
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.100.100.1 255.255.255.0
 duplex auto
 speed auto
!
interface ATM1/0
 no ip address
 shutdown
 no atm ilmi-keepalive
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.66.79.193
ip route 1.1.1.0 255.255.255.0 10.100.100.2
no ip http server
no ip http secure-server
!
!
!
!
call rsvp-sync
!
!
mgcp profile default
!
!
line con 0
 exec-timeout 0 0
line aux 0
```

```
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
line vty 5 15
 login
!
!
end
```

센서 구성 시작

센서 구성을 시작하려면 다음 단계를 완료하십시오.

1. 센서에 처음 로그인하는 경우 **cisco**를 사용자 이름으로, **cisco**를 비밀번호로 입력해야 합니다.
2. 시스템이 메시지를 표시하면 비밀번호를 변경합니다.**참고:** Cisco123은 사전 단어이며 시스템에서 허용되지 않습니다.
3. **setup**을 입력하고 시스템 프롬프트를 완료하여 센서의 기본 매개변수를 설정합니다.
4. 다음 정보를 입력합니다.

```
sensor5#setup

    --- System Configuration Dialog ---

!--- At any point you may enter a question mark '?' for help. !--- Use ctrl-c to abort the
configuration dialog at any prompt. !--- Default settings are in square brackets '[]'.


Current Configuration:

networkParams
ipAddress 10.66.79.195
netmask 255.255.255.224
defaultGateway 10.66.79.193
hostname Corp-IPS
telnetOption enabled
!--- Permit the IP address of workstation or network with IME accessList ipAddress
10.66.79.0 netmask 255.255.255.0
exit
timeParams
summerTimeParams
active-selection none
exit
exit
service webServer
general
ports 443
exit
exit
```

5. 컨피그레이션을 저장합니다.센서가 컨피그레이션을 저장하는 데 몇 분 정도 걸릴 수 있습니다.

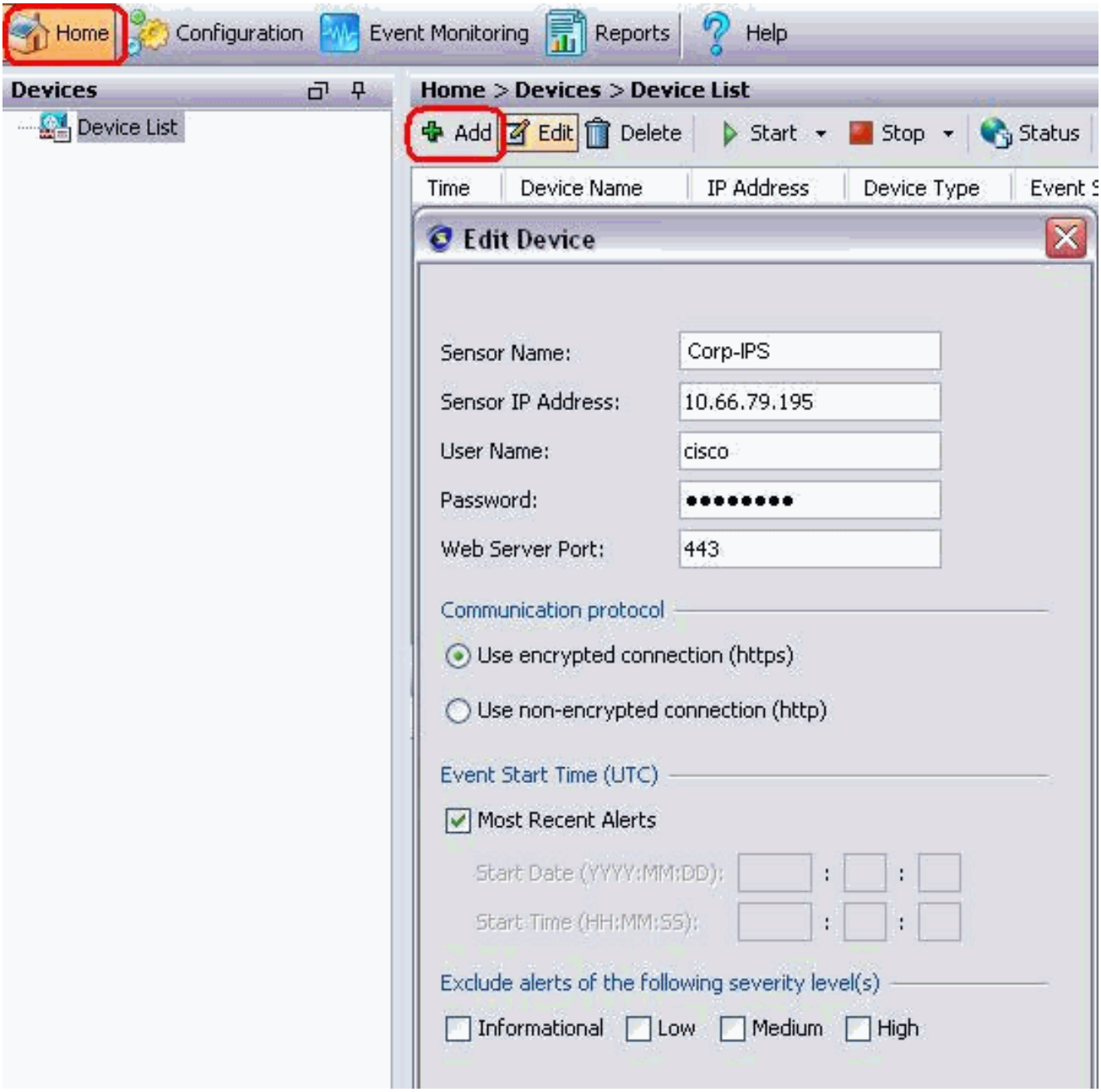
```
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.

Enter your selection[2]: 2
```

IME에 센서 추가

IME에 센서를 추가하려면 다음 단계를 완료합니다.

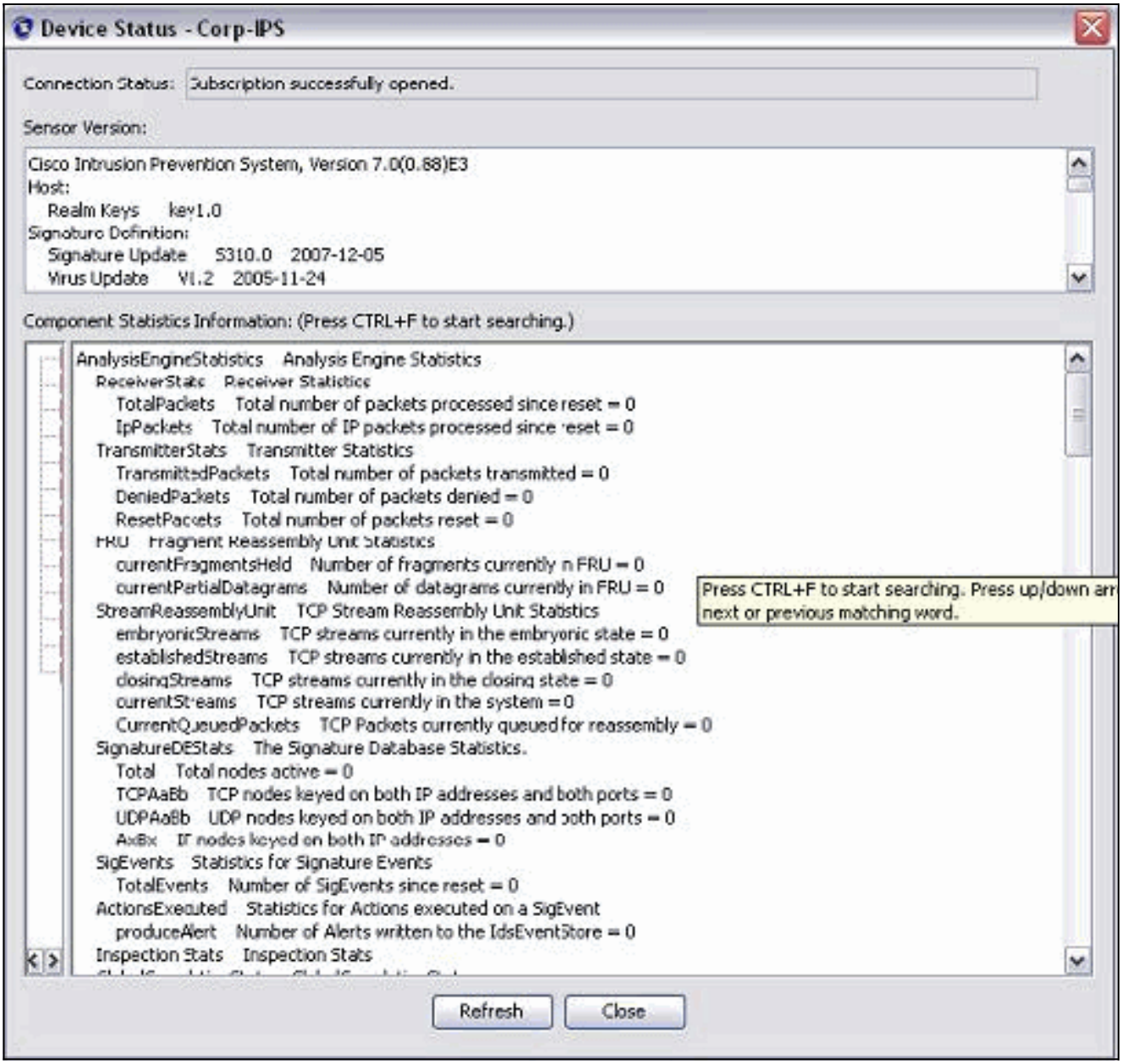
1. IPS Manager Express를 설치한 Windows PC로 이동하여 IPS Manager Express를 엽니다.
2. Home(**홈) > Add(추가)를** 선택합니다

.



3. 이 정보를 입력하고 **OK**(확인)를 클릭하여 컨피그레이션을 완료합니다.
4. Devices(**디바이스) > Corp-IPS**를 선택하여 센서 상태를 확인한 다음 마우스 오른쪽 버튼을 클릭하여 **Device Status(디바이스 상태)**를 선택합니다.Subscription이

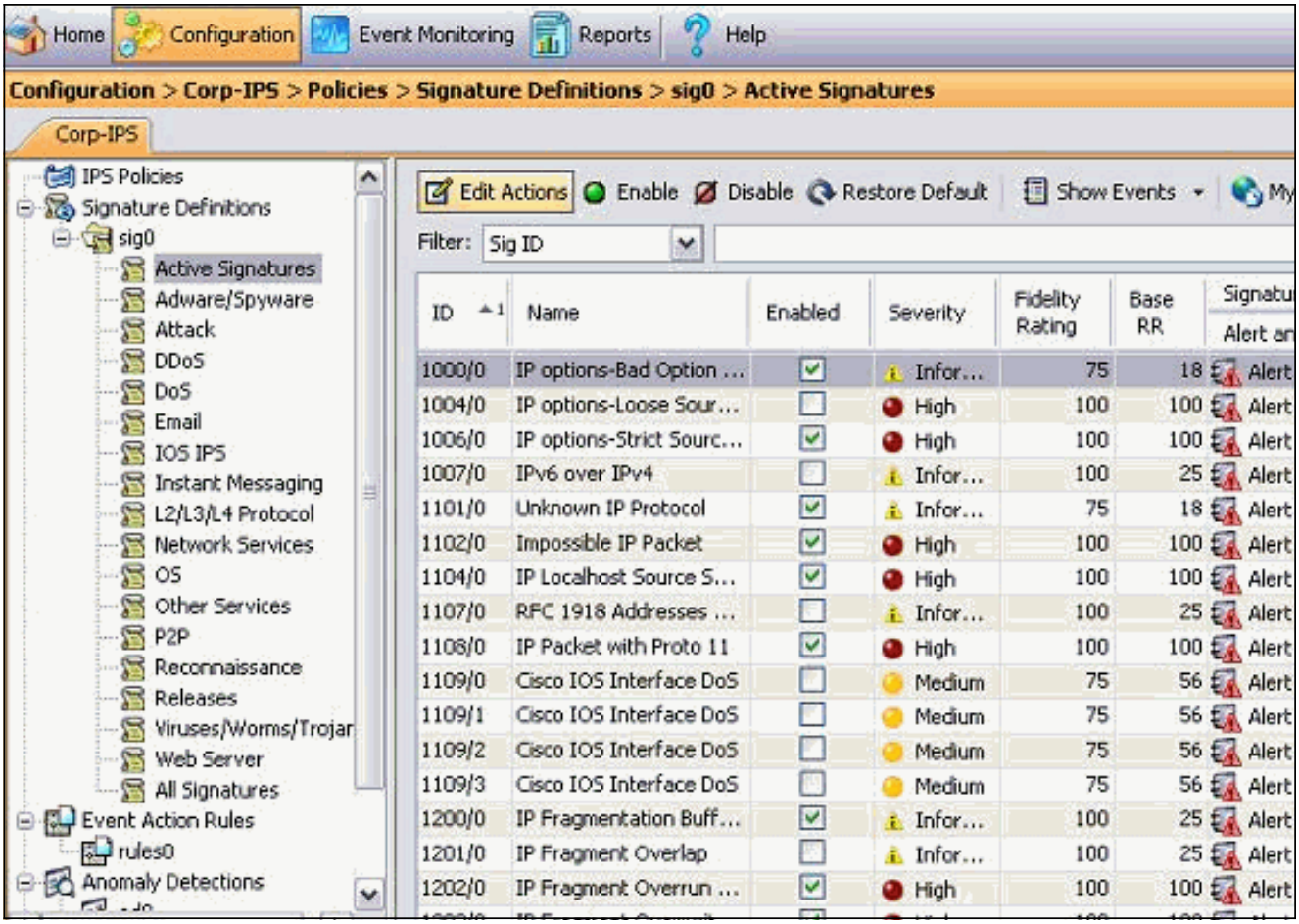
.



Cisco IOS 라우터에 대한 TCP 재설정 구성

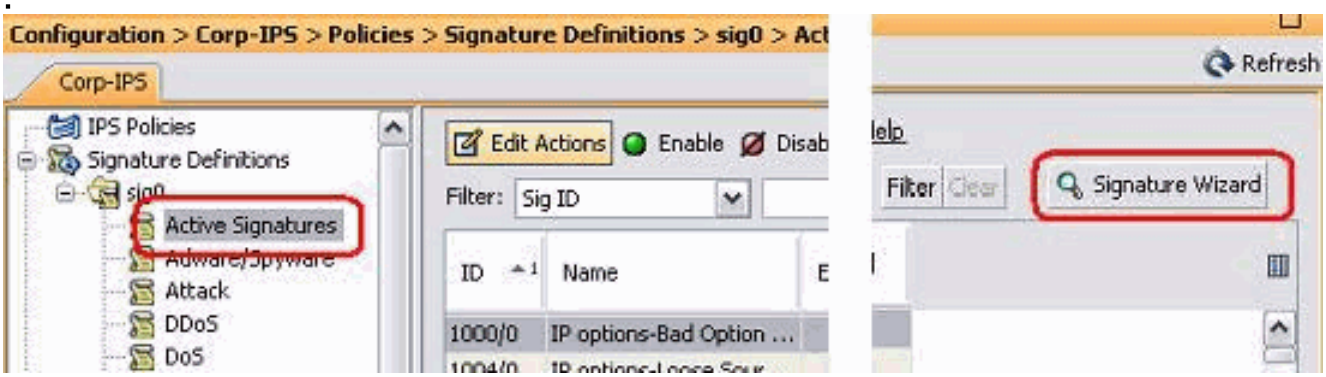
Cisco IOS 라우터에 대한 TCP 재설정을 구성하려면 다음 단계를 완료합니다.

1. IME PC에서 웹 브라우저를 열고 https://10.66.79.195으로 **이동합니다**.
2. 센서에서 다운로드한 HTTPS 인증서를 수락하려면 확인을 클릭합니다.
3. 로그인 창에서 사용자 이름에 **cisco**를 입력하고 **비밀번호는 123cisco123**을 입력합니다.이 IME 관리 인터페이스는 다음과 같이 나타납니다
   .



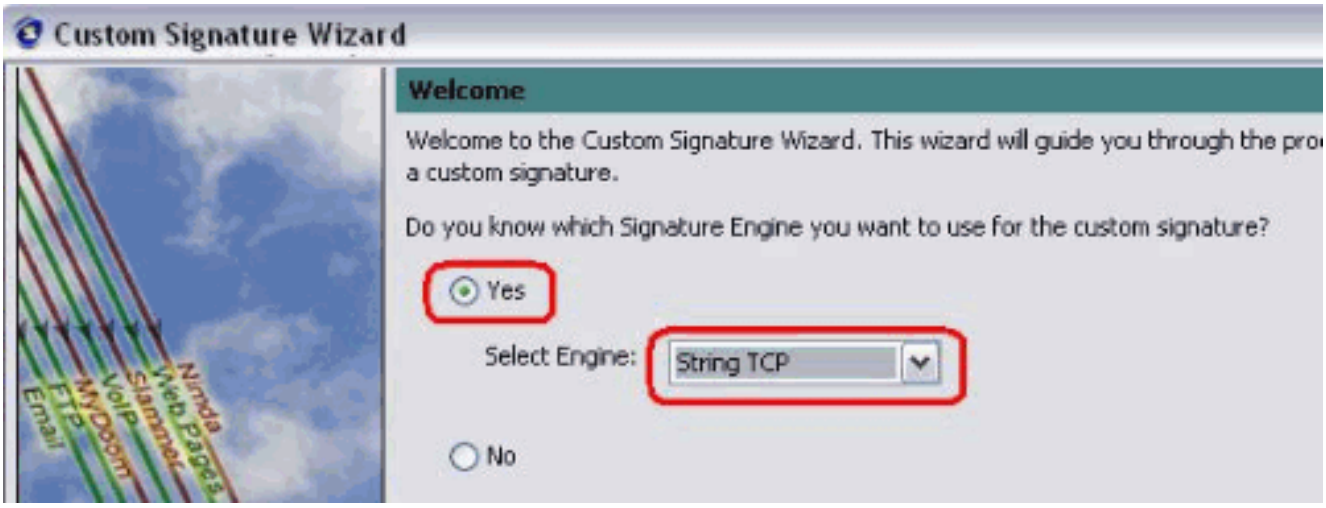
4. Configuration(컨피그레이션) 탭에서 Active **Signatures(활성 서명)를** 클릭합니다.
5. 그런 다음 **Signature Wizard를** 클릭합니다

.



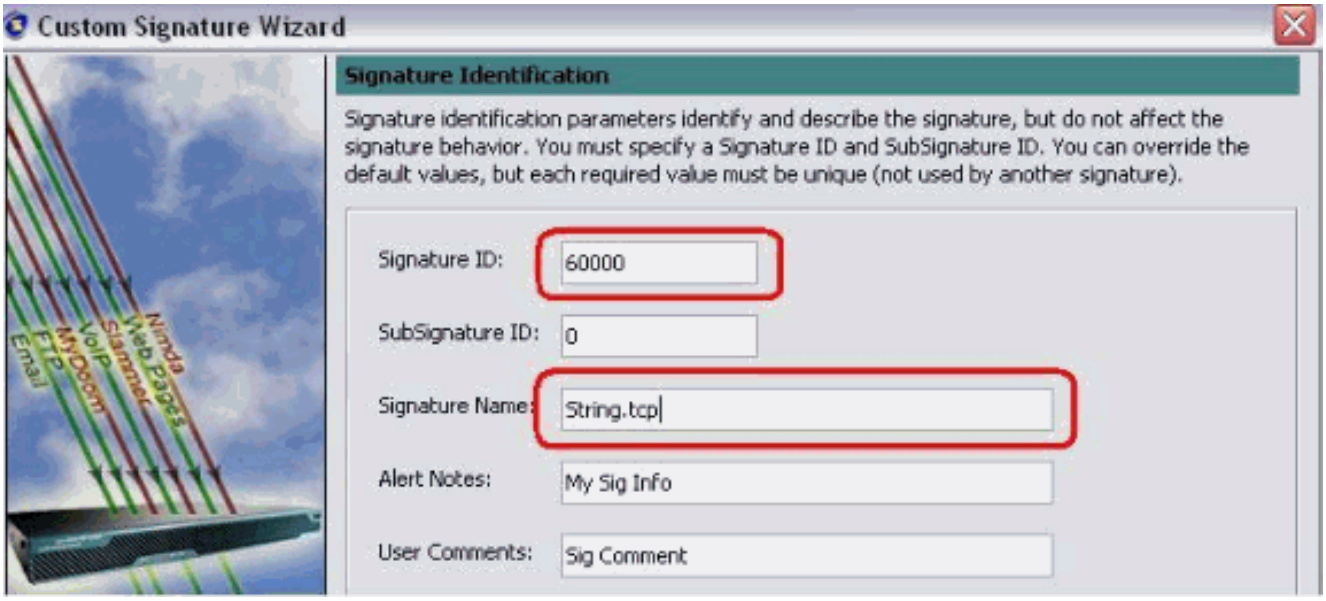
6. 마법사에서 **Yes(예)**를 선택하고 **String TCP**를 Signature 엔진으로 선택합니다. Next(**다음)를 클릭합니다**

.



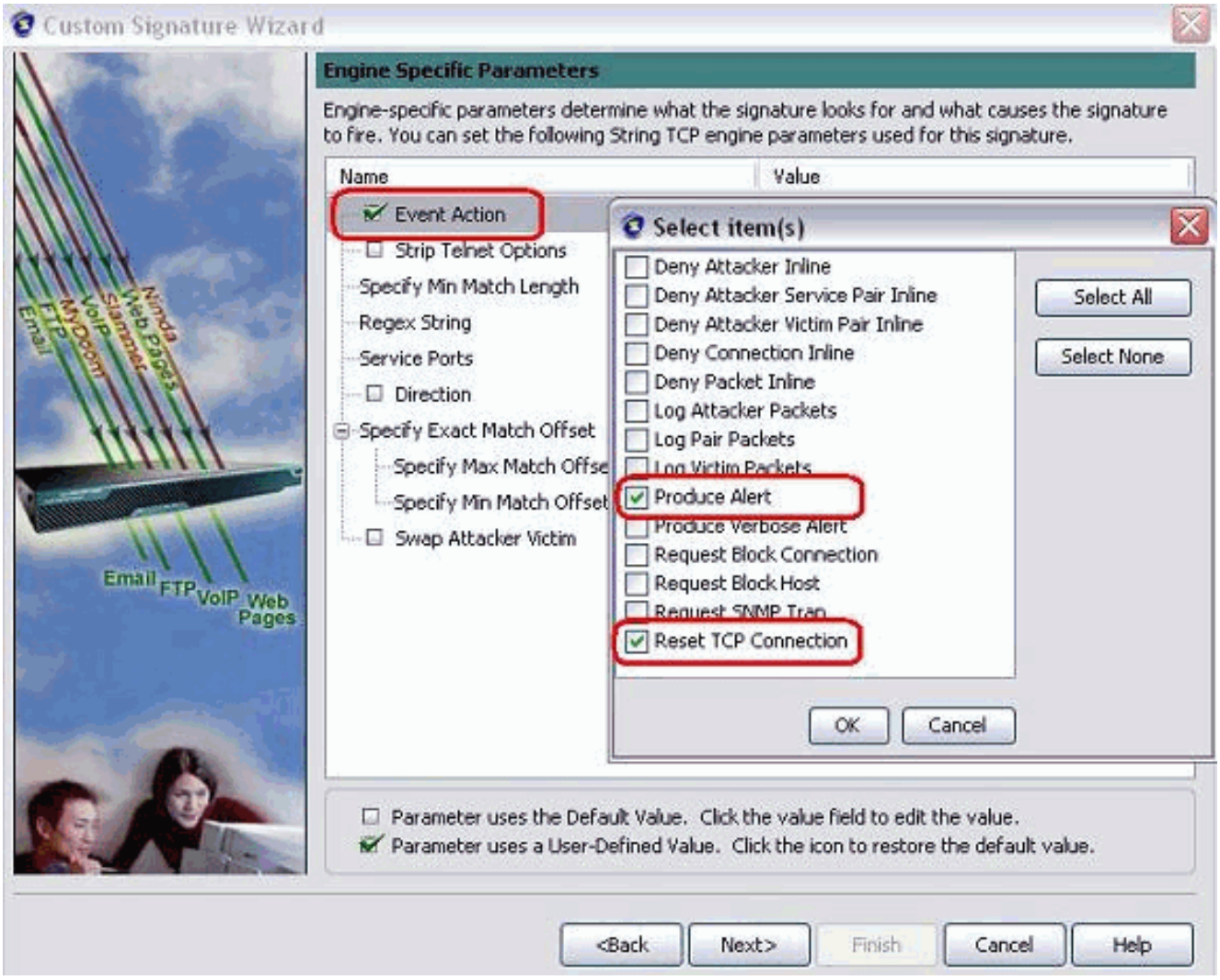
7. 이 정보를 기본값으로 두거나 자신의 서명 ID, 서명 이름 및 사용자 메모를 입력할 수 있습니다. Next(**다음)를 클릭합니다**

.



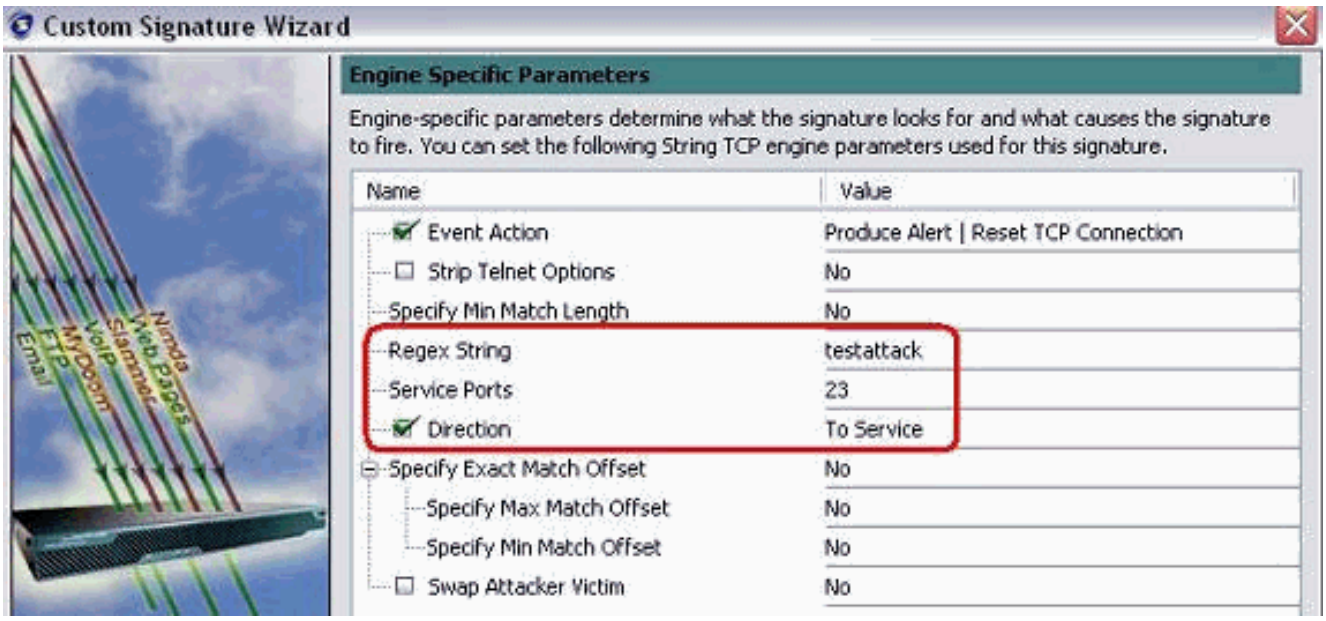
8. Event **Action(이벤트 작업)**을 선택하고 **Produce Alert**(경고 생성) 및 **Reset TCP Connection(TCP 연결 재설정)을 선택합니다**. 계속하려면 **확인**을 클릭한 다음 **다음**을 클릭합니다

.



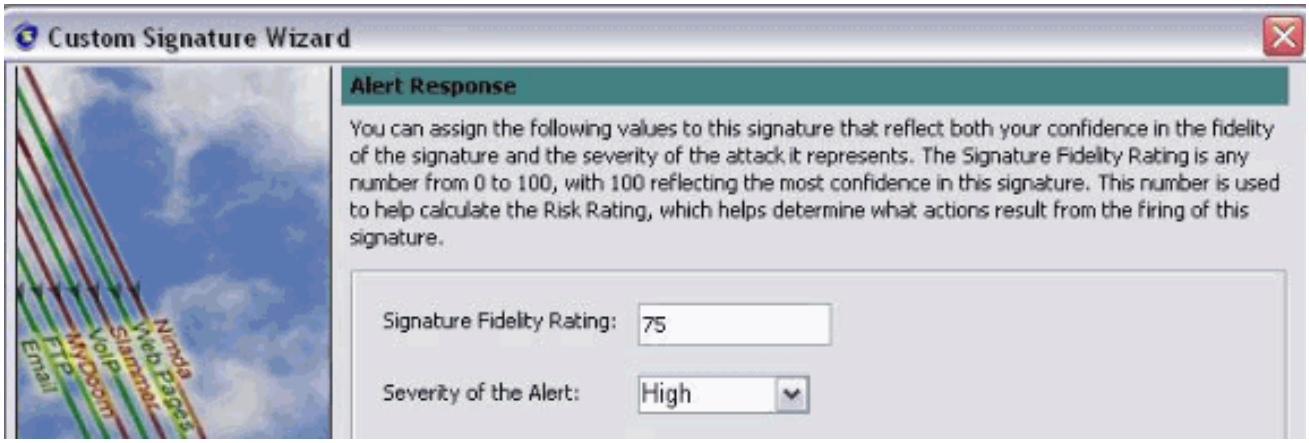
9. Regular Expression을 입력하면 `testattack`이 이 예에 사용됩니다. Service Ports(서비스 포트)에 **23**을 입력하고 **To Service**(서비스) for the Direction(방향)을 선택한 다음 Next(**다음**)를 클릭하여 계속합니다

.



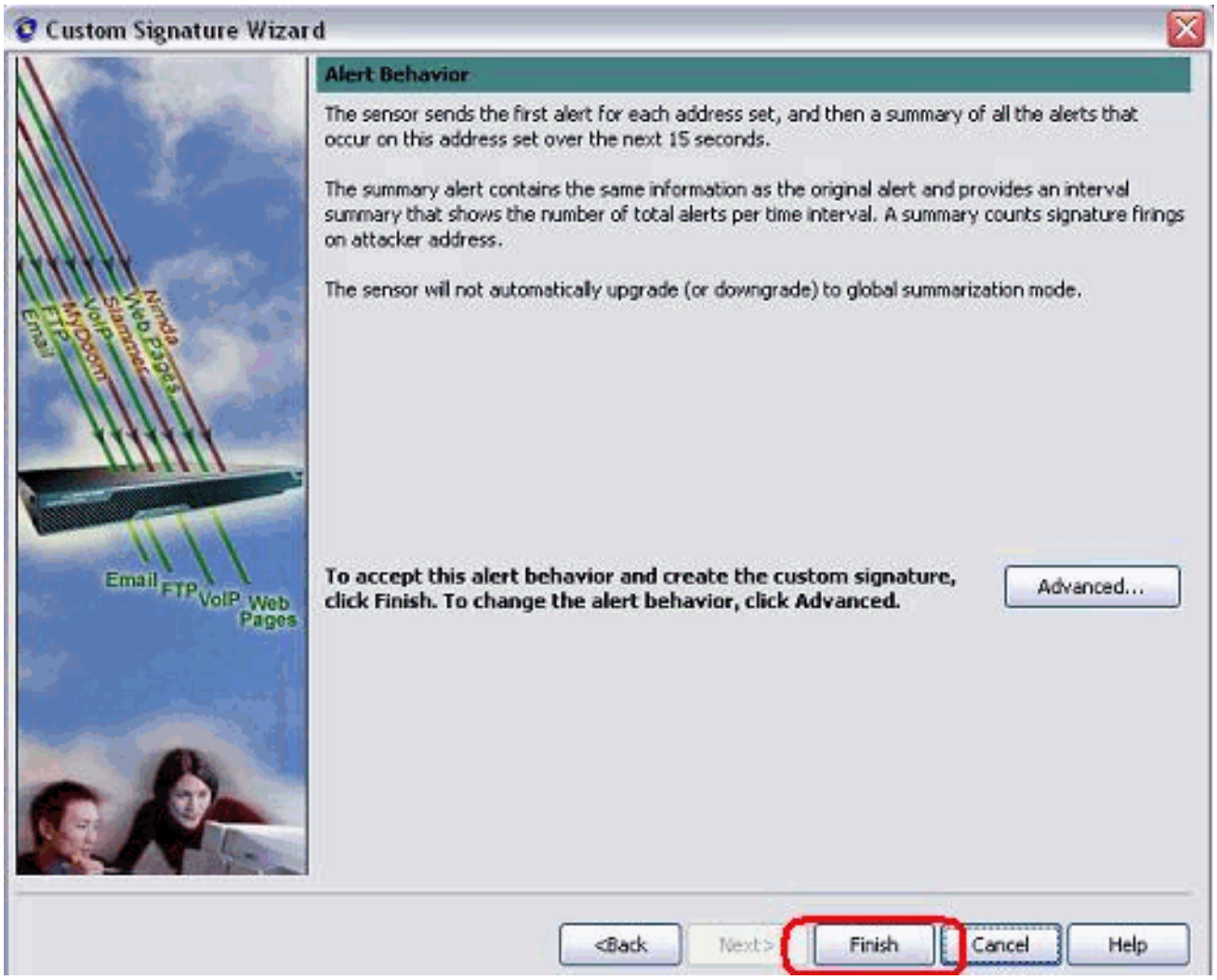
10. 이 정보를 기본값으로 둘 수 있습니다. Next(**다음**)**를 클릭합니다**

.

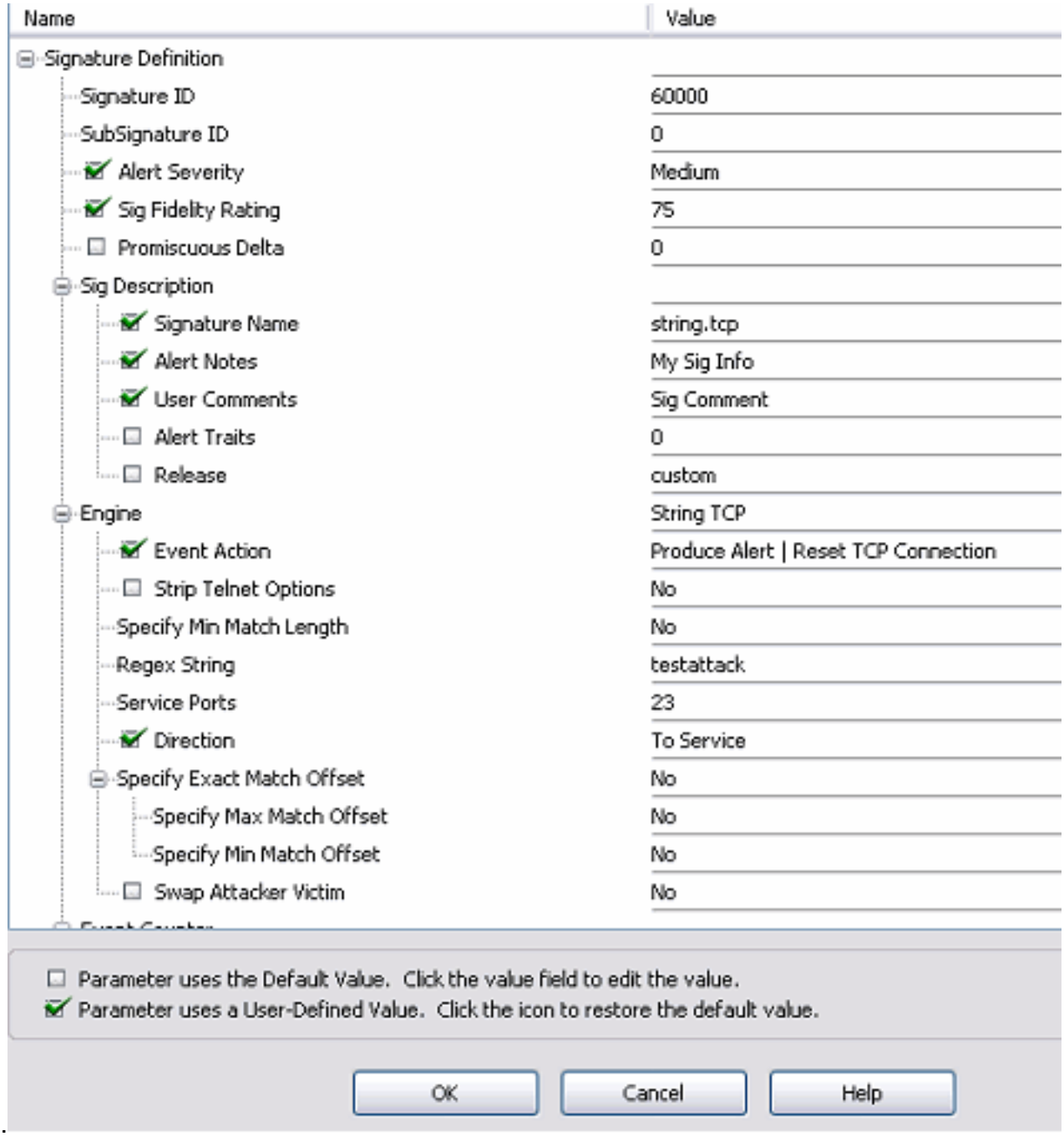


11. **마침**을 클릭하여 마법사를 완료합니다

.



12. Configuration(**컨피그레이션) > sig0 > Active Signatures(활성 시그니처)**를 선택하여 Sig **ID** 또는 Sig Name(서명 이름)으로 새로 생성된 시그니처를 **찾습니다**. Edit(**편집)**를 클릭하여 Signature(시그니처)를 확인합니다



13. 확인 후 **확인**을 클릭하고 **적용** 버튼을 클릭하여 센서에 서명을 적용합니다.

다음을 확인합니다.

공격 및 TCP 재설정 실행

공격 및 TCP 재설정을 시작하려면 다음 단계를 완료하십시오.

1. 공격을 실행하기 전에 **IME**로 이동하여 Event Monitoring(**이벤트 모니터링**) > **Dropped Attacks View(삭제된 공격 보기)를** 선택하고 오른쪽에 있는 센서를 선택합니다.
2. Router Light(라우터 표시등)에서 Telnet to Router House(라우터 하우스)로 이동하여 **testattack을 입력합니다**.텔넷 세션을 재설정하려면 **<space> 또는** <enter>를 누르십시오.

```
light#telnet 10.100.100.1
    Trying 10.100.100.1 ... Open

    User Access Verification
    Password:
```

```
house>en
Password:
house#testattack
[Connection to 10.100.100.1 closed by foreign host]
!--- Telnet session has been reset due to the !--- signature "String.tcp" triggered.
```

3. IPS Event Viewer의 Dashboard(대시보드)에서 공격이 시작되면 빨간색 경보가 나타납니다

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

팁

다음 문제 해결 팁을 사용합니다.

- Bypass는 명령 및 제어 포트에서 작동하여 라우터 ACL(Access Control List)을 다시 프로그래밍합니다. TCP 재설정은 센서의 스니핑 **인터페이스**에서 전송됩니다. 스위치에서 **span을 설정할** 때, **set span <src_mod/src_port><dest_mod/dest_port>** 명령을 사용합니다. 이 명령은 두 수신 패킷을 모두 활성화합니다.

```
banana (enable)set span 2/12 3/6 both inpkts enable
Overwrote Port 3/6 to monitor transmit/receive traffic of Port 2/12
Incoming Packets enabled. Learning enabled. Multicast enabled.
banana (enable)
banana (enable)
banana (enable)show span

Destination      : Port 3/6
!--- connect to sniffing interface of the sensor
Admin Source     : Port 2/12
!--- connect to FastEthernet0/0 of Router House
Oper Source      : Port 2/12
Direction        : transmit/receive
Incoming Packets: enabled
Multicast        : enabled
```

- TCP 재설정이 작동하는 경우 작업 유형 TCP Reset에 대해 경보가 트리거되었는지 확인합니다. 경보가 나타나면 서명 유형이 TCP 재설정으로 설정되어 있는지 확인합니다.root에 service account su를 사용하여 로그인하고 이 명령을 실행합니다. 이 명령은 센싱 인터페이스가 eth0으로 설정된 것으로 가정합니다.

```
[root@sensor1 root]#tcpdump -i eth0 -n
```

참고: 100개의 tcp 재설정이 피해자/타겟으로 전송되고 100개의 TCP가 공격자/클라이언트로 전송됩니다.다음은 출력의 예입니다.

```
03:06:00.598777 64.104.209.205.1409 >
```

```
 10.66.79.38.telnet: R 107:107(0) ack 72 win 0
03:06:00.598794 64.104.209.205.1409 >
 10.66.79.38.telnet: R 108:108(0) ack 72 win 0

03:06:00.599360 10.66.79.38.telnet >
 64.104.209.205.1409: R 72:72(0) ack 46 win 0
03:06:00.599377 10.66.79.38.telnet >
 64.104.209.205.1409: R 73:73(0) ack 46 win 0
```

관련 정보

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