IDS 디렉터를 사용하여 TCP 재설정 구성

목차

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

소개

이 문서에서는 전송된 문자열이 "testattack"인 경우 시도된 텔넷의 TCP 재설정을 관리되는 라우터가 포함된 주소 범위로 전송하도록 Intrusion Detection System(IDS, 이전의 NetRanger) Director 및 Sensor를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 구성을 고려할 때 다음 사항을 기억하십시오.

- 이 컨피그레이션을 수행하기 전에 센서를 설치하고 센서가 제대로 작동하는지 확인합니다.
- 스니핑 인터페이스가 관리되는 라우터의 외부 인터페이스로 확장되는지 확인합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IDS Director 2.2.3
- Cisco IDS 센서 3.0.5
- Cisco IOS® Router 소프트웨어 릴리스 12.2.6

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.

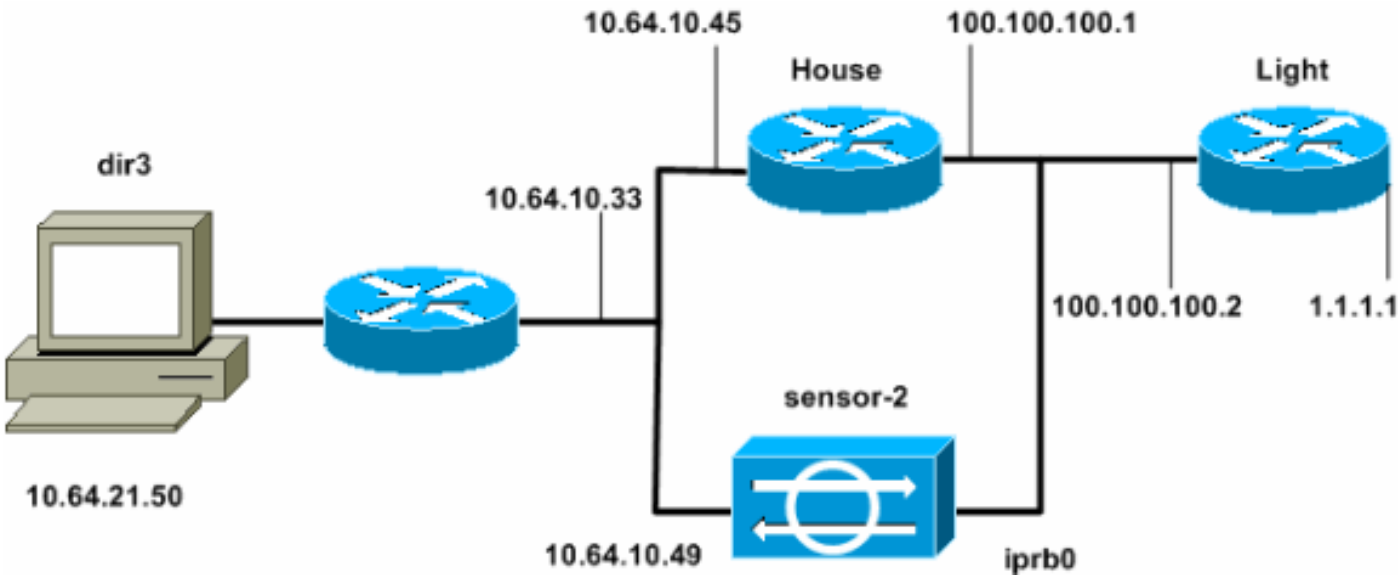
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 이 문서에 사용된 명령에 대한 추가 정보를 찾으려면 명령 조회 도구(등록된 고객만 해당)를 사용합니다.

네트워크 다이어그램

이 문서에서는 이 다이어그램에 표시된 네트워크 설정을 사용합니다.



구성

이 문서에서는 이러한 구성을 사용합니다.

- 라우터 표시등
- 라우터 하우스

라우터 표시등

```
Current configuration : 906 bytes
!
version 12.2
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 100.100.100.2 255.255.255.0
 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 0.0.0.0 100.100.100.1
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 : 2187 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname house
!
enable password cisco
!
!
!
ip subnet-zero
!
!
fax interface-type modem
mta receive maximum-recipients 0
!
!
!
!
interface FastEthernet0/0
 ip address 100.100.100.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.64.10.45 255.255.255.224
 duplex auto
 speed auto
!
!
!
interface FastEthernet4/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.64.10.33
ip route 1.1.1.0 255.255.255.0 100.100.100.2
ip http server
ip pim bidir-enable
!
!
!
snmp-server manager
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
```

```
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
!
!
end

house#
```

센서 구성

센서를 구성하려면 다음 단계를 완료합니다.

1. 사용자 이름 **루트** 및 비밀번호 **공격**을 사용하여 10.64.10.49(IDS 센서)에 텔넷을 **지정합니다**.
2. sysconfig-**sensor를 입력합니다**.
3. 프롬프트가 표시되면 다음 예와 같이 컨피그레이션 정보를 입력합니다.

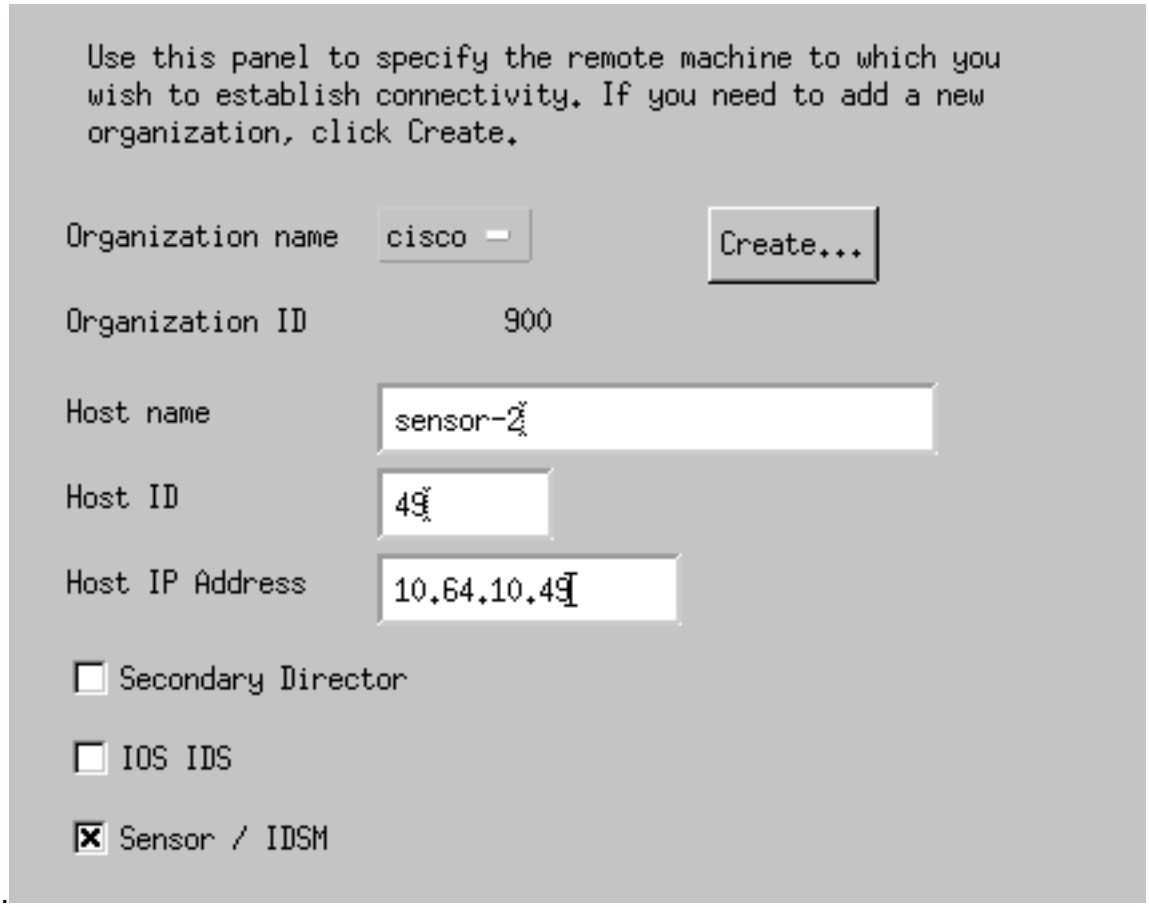
```
1 - IP Address:  10.64.10.49
2 - IP Netmask:  255.255.255.224
3 - IP Host Name:  sensor-2
4 - Default Route:  10.64.10.33
5 - Network Access Control
          64.
          10.
6 - Communications Infrastructure
Sensor Host ID:  49
Sensor Organization ID:  900
Sensor Host Name:  sensor-2
Sensor Organization Name:  cisco
Sensor IP Address:  10.64.10.49
IDS Manager Host ID:  50
IDS Manager Organization ID:  900
IDS Manager Host Name:  dir3
IDS Manager Organization Name:  cisco
IDS Manager IP Address:  10.64.21.50
```

4. 메시지가 표시되면 컨피그레이션을 저장하고 센서가 재부팅되도록 합니다.

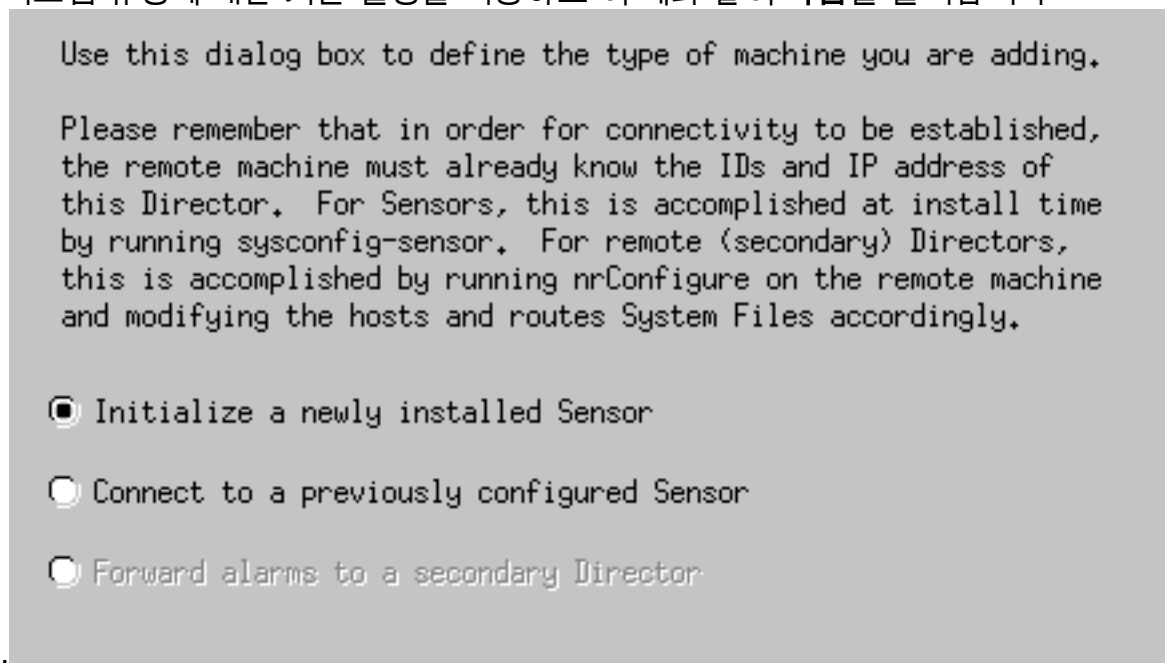
디렉터에 센서 추가

이 단계를 완료하여 센서를 디렉터에 추가합니다.

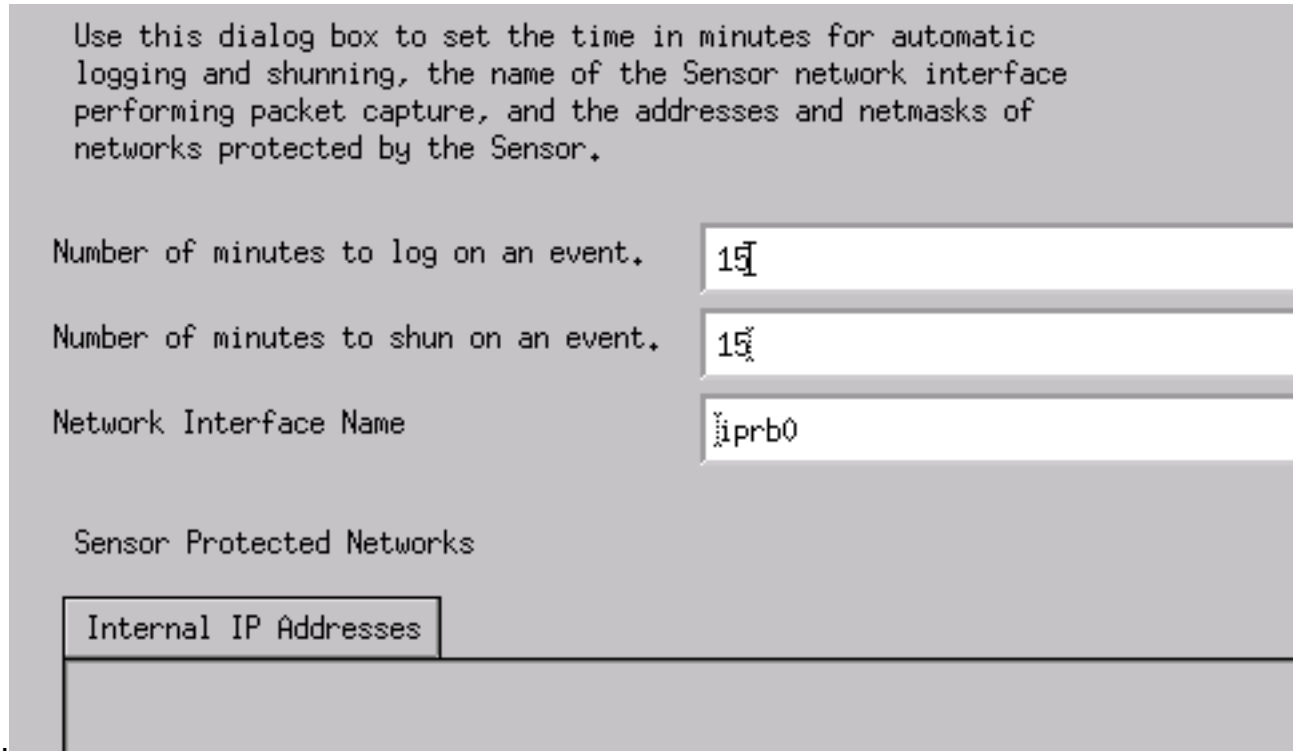
1. 사용자 이름 netrangr 및 비밀번호 **공격**을 사용하여 10.64.21.50(IDS **Director**)에 텔넷.
2. **ovw&를 입력하여** HP OpenView를 시작합니다.
3. 주 메뉴에서 **보안 > 구성**으로 **이동합니다**.
4. Configuration File Management Utility(구성 파일 관리 유틸리티)에서 **file(파일) > Add Host(호스트 추가)**로 이동하고 **Next(다음)**를 클릭합니다.
5. 이 예와 같이 센서 호스트 정보를 완료합니다. Next(**다음)를 클릭합니다**



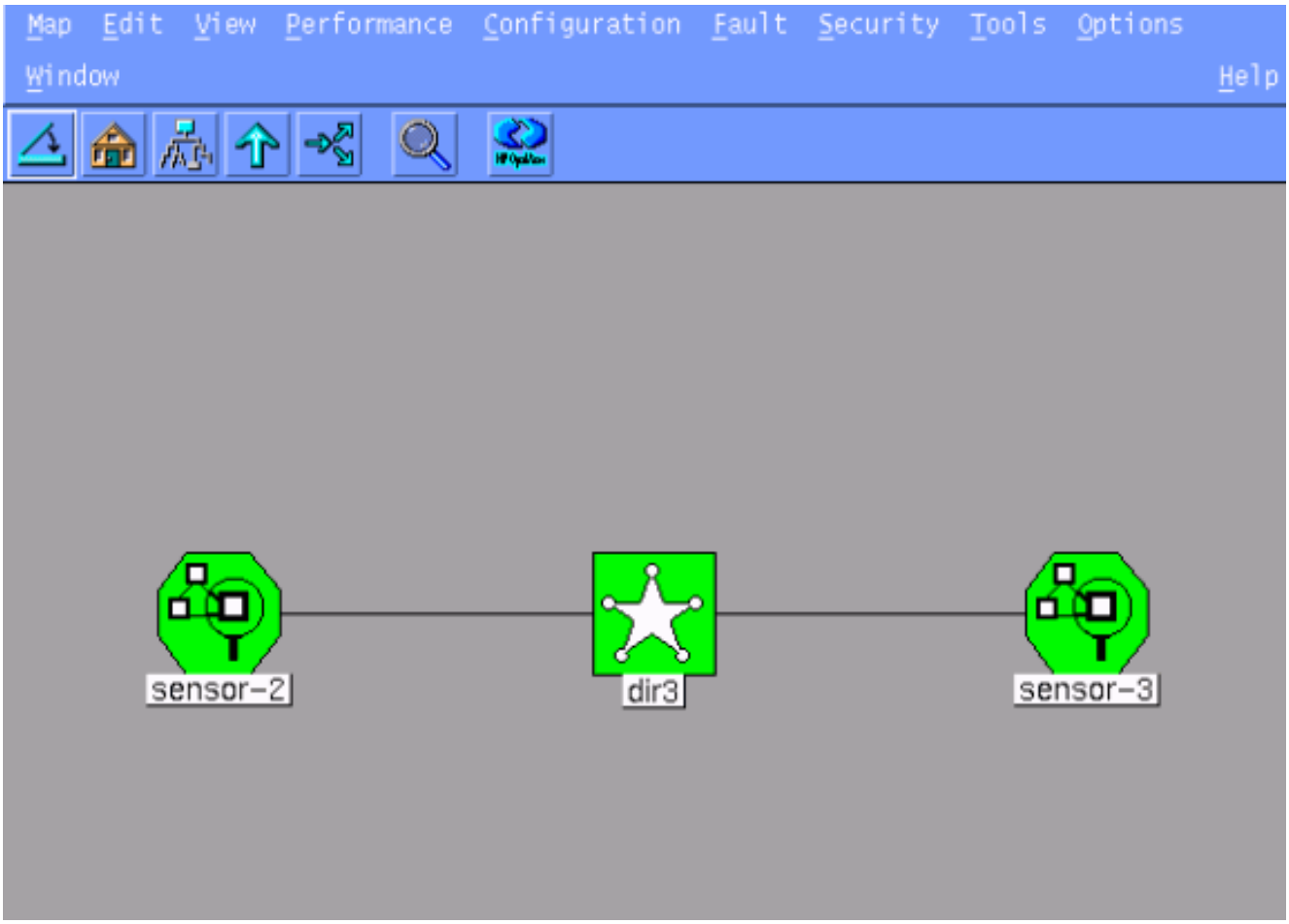
6. 시스템 유형에 대한 기본 설정을 적용하고 이 예와 같이 **다음**을 클릭합니다



7. 로그를 변경하고 분을 사용하지 않거나 기본값을 사용할 수 있습니다. 그러나 네트워크 인터페이스 이름을 스니핑 인터페이스의 이름으로 변경해야 합니다. 이 예에서는 "iprb0"입니다. 센서 유형 및 센서 연결 방법에 따라 "spwr0" 또는 그 밖의 다른 것일 수 있습니다



8. 계속해서 **Next(다음)**를 클릭한 다음 **Finish(마침)를** 클릭하여 센서를 디렉터에 추가합니다. 이제 주 메뉴에서 이 예와 같이 sensor-2가 표시됩니다



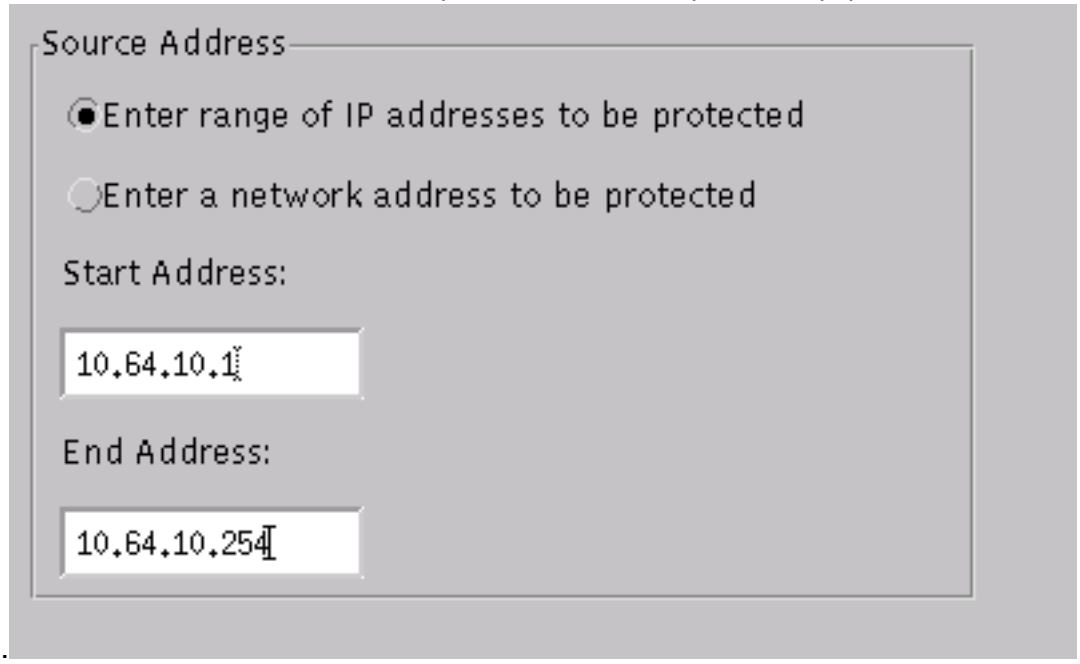
Cisco IOS 라우터에 대한 TCP 재설정 구성

Cisco IOS 라우터에 대한 TCP 재설정을 구성하려면 다음 단계를 완료합니다.

1. 주 메뉴에서 **보안 > 구성**으로 **이동합니다**.
2. Configuration File Management Utility에서 **sensor-2**를 강조 표시하고 두 번 클릭합니다.
3. 장치 관리를 엽니다.
4. Devices **> Add를 클릭합니다**. 다음 예와 같이 디바이스 정보를 입력합니다. OK(**확인**)를 클릭하여 계속합니다. 텔넷과 enable 비밀번호 모두 Cisco입니다

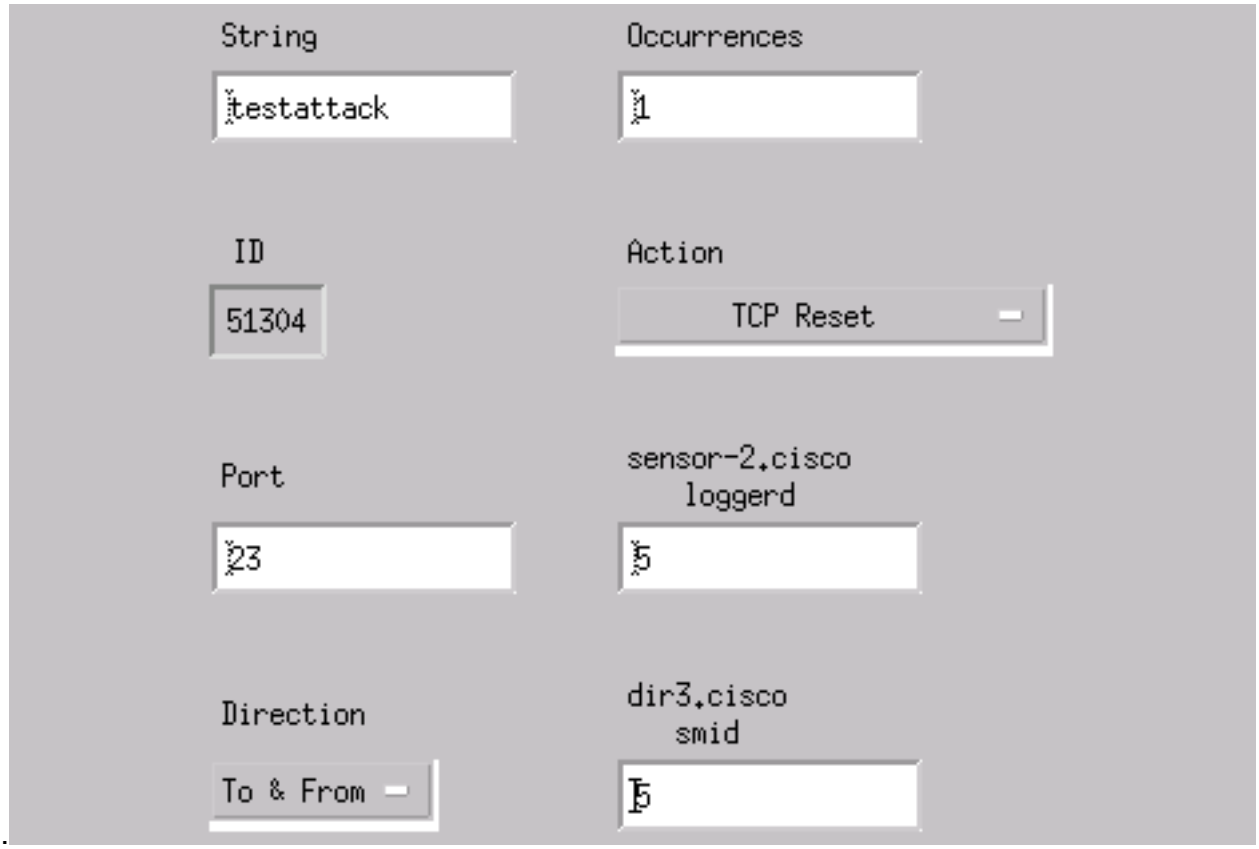
.

5. Intrusion Detection(침입 탐지) 창을 열고 Protected Networks(**보호된 네트워크)를** 클릭합니다. 10.64.10.1~10.64.10.254 범위의 주소를 보호 네트워크에 추가합니다

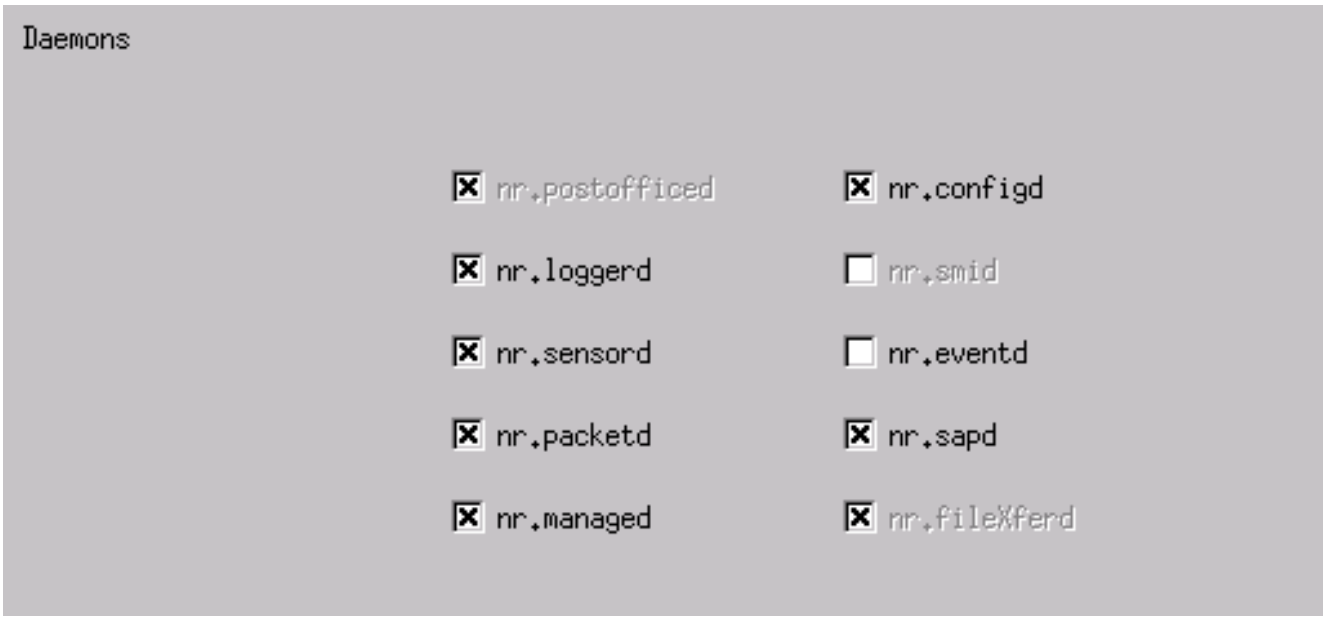


.

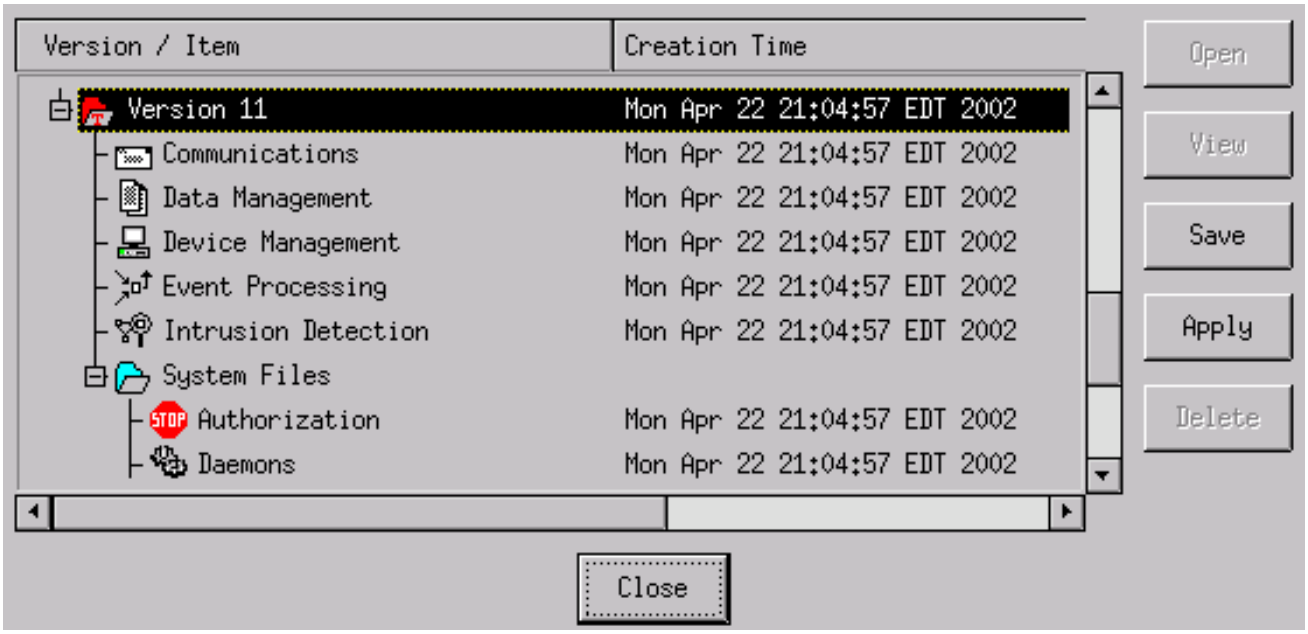
6. Profile(**프로파일**)을 클릭하고 Manual Configuration(**수동 컨피그레이션)을 선택합니다**. 그런 다음 Modify **Signatures를 클릭합니다**. ID가 8000인 Matched Strings를 선택합니다. Expand(**확장) > Add(추가**)를 클릭하여 testattack이라는 새 문자열을 **추가합니다**. 이 예와 같이 문자열 정보를 입력하고 **OK**를 클릭하여 계속합니다



7. 컨피그레이션의 이 부분을 마쳤습니다. OK를 클릭하여 Intrusion Detection 창을 닫습니다.
8. System Files 폴더를 열고 Daemons 창을 엽니다. 다음 데몬이 활성화되었는지 확인합니다
.



9. OK(**확인**)를 클릭하여 계속합니다.
10. 방금 수정한 버전을 선택하고 **저장**을 클릭한 다음 **적용**을 **클릭합니다**. 시스템이 센서 서비스가 다시 시작되었음을 알릴 때까지 기다린 다음 디렉터 구성의 모든 창을 닫습니다
.



공격 및 TCP 재설정 실행

Telnet from Router Light to Router House 및 type testattack**입니다**. Space 또는 Enter 키를 누르면 텔넷 세션이 재설정됩니다. 라우터 하우스에 연결합니다.

```
light#telnet 10.64.10.45
Trying 10.64.10.45 ... Open

User Access Verification
Password:
house>en
Password:
house#testattack
[Connection to 10.64.10.45 closed by foreign host]
 !--- Telnet session has been reset because the !--- signature testattack was triggered.
```

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

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

사용자 이름 **루트**와 비밀번호 **공격**을 사용하여 10.64.10.49에 텔넷을 연결합니다. cd **/usr/nr/etc 를 입력합니다**. cat packetd**.conf를 입력합니다**. 테스트 공격에 대해 TCP 재설정을 올바르게 설정한 경우 Action Codes(작업 코드) 필드에 4개가 표시됩니다. 이 예와 같이 TCP 재설정을 나타냅니다.

```
netrangr@sensor-2:/usr/nr/etc
>cat packetd.conf | grep "testattack"
RecordOfStringName 51304 23 3 1 "testattack"
SigOfStringMatch 51304 4 5 5 # "testattack"
```

서명에 실수로 액션을 "none"으로 설정하면 Action Codes(작업 코드) 필드에 0이 표시됩니다. 이는

이 예제에서 볼 수 있는 작업이 없음을 나타냅니다.

```
netrangr@sensor-2:/usr/nr/etc
>cat packetd.conf | grep "testattack"
RecordOfStringName 51304 23 3 1 "testattack"
SigOfStringMatch 51304 0 5 5 # "testattack"
```

센서의 스니핑 인터페이스에서 TCP 재설정이 전송됩니다. 센서 인터페이스를 관리 라우터의 외부 인터페이스에 연결하는 스위치가 있는 경우 스위치에서 set span 명령을 사용하여 구성할 때 다음 구문을 사용합니다.

set span

```
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
Learning        : enabled
Multicast       : enabled
```

관련 정보

- 필드 알림
- Cisco Secure Intrusion Prevention 지원 페이지