UNIX Director에서 차단 설정

목차

소개

Cisco IDS(Intrusion Detection System) Director 및 Sensor를 사용하여 Cisco 라우터를 차단하는 데 사용할 수 있습니다.이 문서에서는 라우터 "집"에서 공격을 탐지하고 이 정보를 디렉터 "dir3"에 전달하기 위해 센서(sensor-2)를 구성합니다. 구성된 후에는 "Light" 라우터에서 공격이 시작됩니다(시그니처 2151인 1024바이트보다 큰 ping 및 시그니처 2152인 ICMP(Internet Control Message Protocol) 플러드). 센서가 공격을 탐지하고 이를 디렉터에게 전달합니다.공격자의 트래픽을 차단하기 위해 ACL(Access Control List)이 라우터에 다운로드됩니다.공격자 가 표시되고 피해자에게 다운로드된 ACL이 표시됩니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- 센서를 설치하고 제대로 작동하는지 확인합니다.
- 스니핑 인터페이스가 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® 라우터(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.

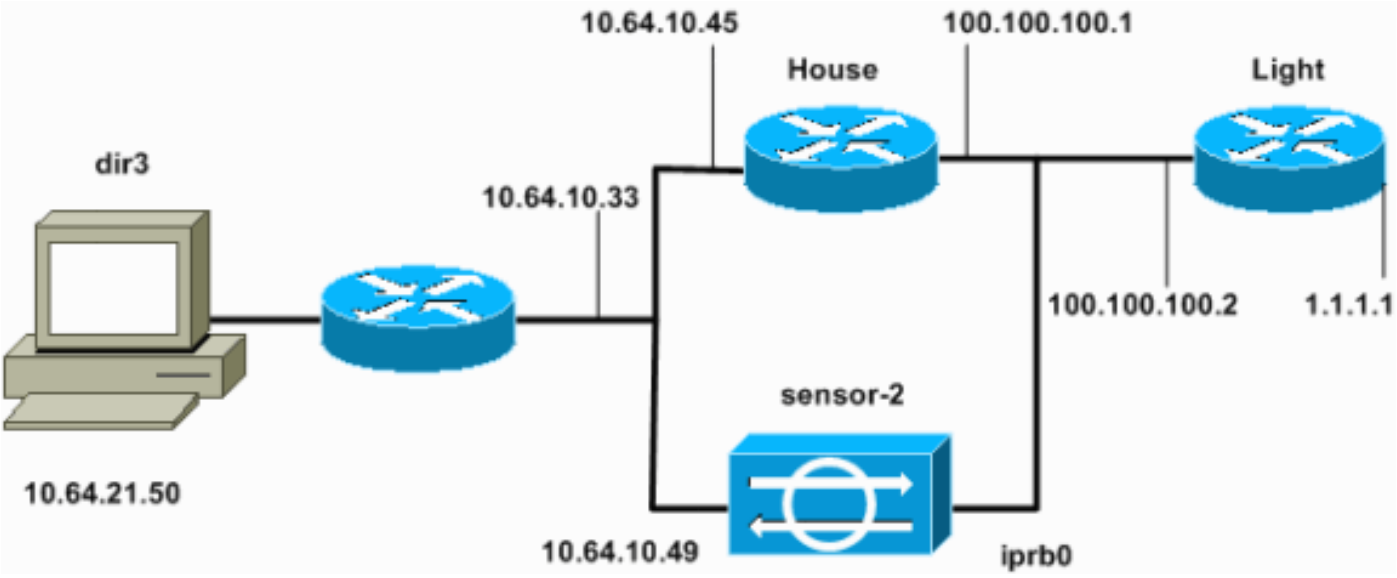
구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

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
!
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
!--- After you configure shunning, IDS Sensor puts this
line in. ip access-group IDS_FastEthernet0/0_in_1 in


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
!
!
!--- After you configure shunning, IDS Sensor puts these
lines in. ip access-list extended IDS_FastEthernet0/0_in
deny ip host 100.100.100.2 any
permit ip host 10.64.10.49 any
 permit ip any any

!
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. 텔넷에서 **10.64.10.49**로 사용자 이름 **루트** 및 비밀번호 **공격**을 **수행합니다**.
2. sysconfig-**sensor를 입력합니다**.
3. 프롬프트가 표시되면 이 예와 같이 컨피그레이션 정보를 입력합니다.

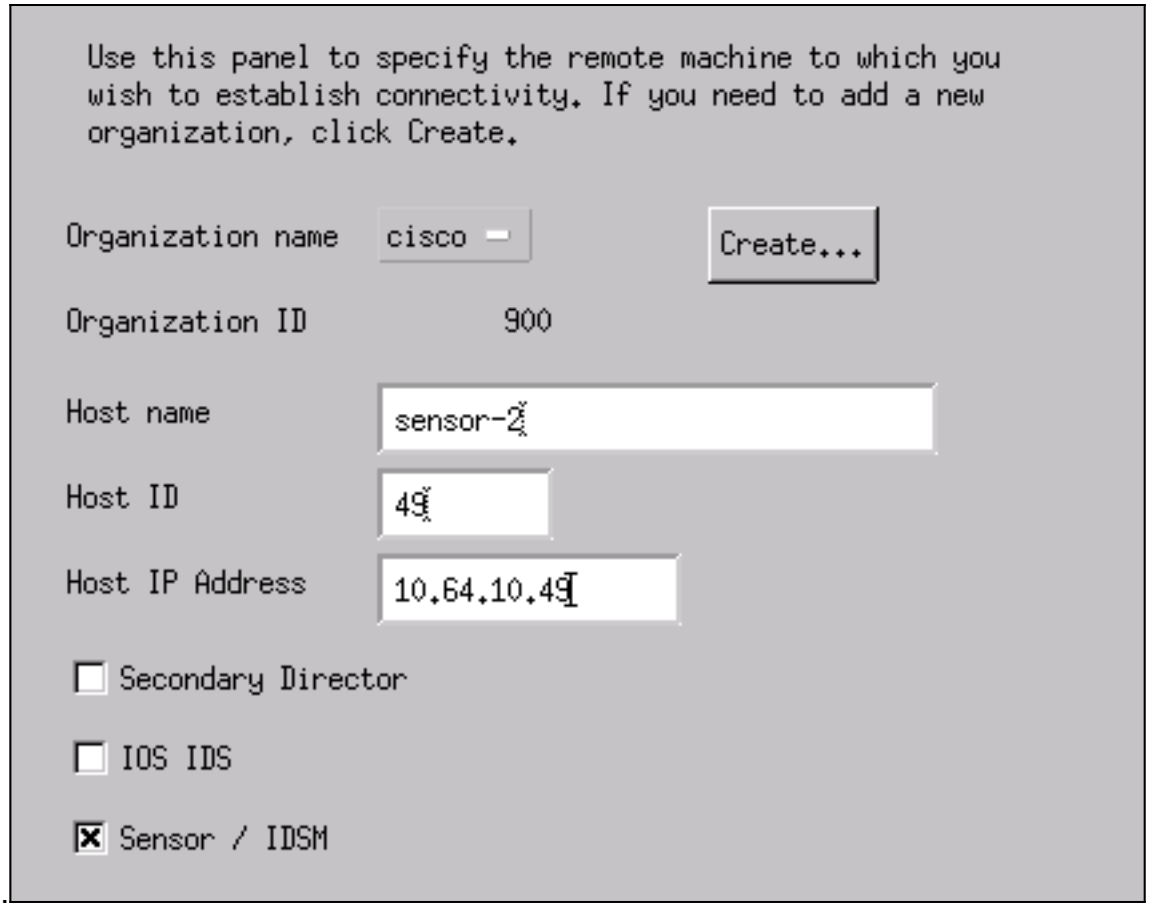
```
1 - IP Address: 10.64.10.49
2 - IP Netmask: 255.255.255.224
3 - IP Host Name:  sensor-2
4 - Default Route     10.64.10.33
5 - Network Access Control
         64.
         10.
6 - Communications Infrastructure
Sensor Host ID: 49
Sensor Organization ID:     900
Sensor Host Name: sensor-2
Sensor Organization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

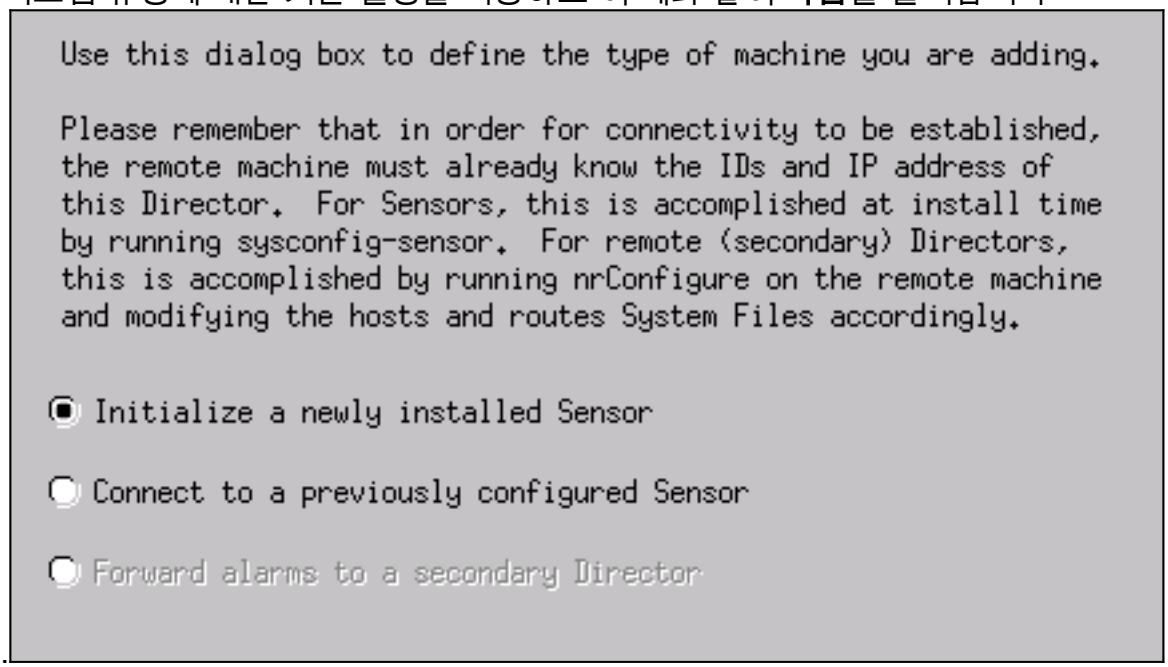
디렉터에 센서 추가

이 단계를 완료하여 센서를 디렉터에 추가합니다.

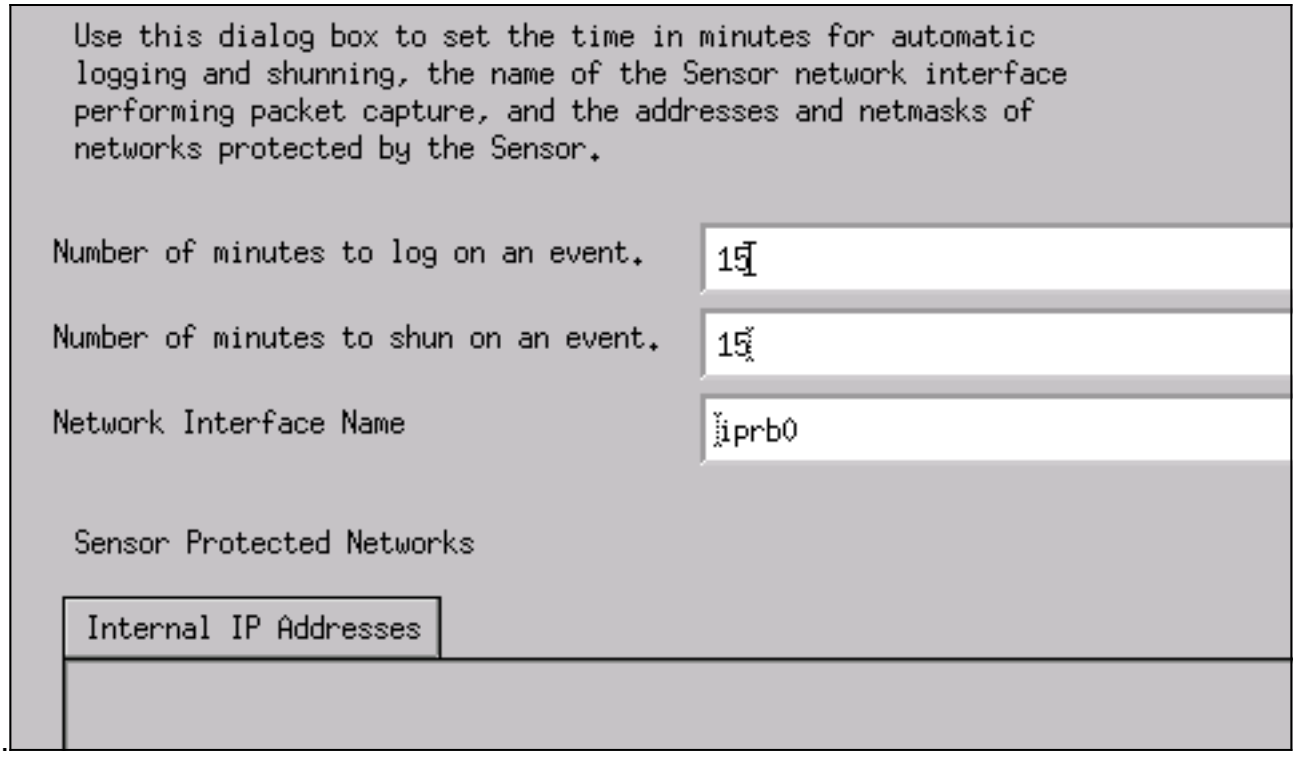
1. 텔넷에서 **10.64.21.50에** 대한 사용자 이름 **netrangr** 및 비밀번호 **공격**.
2. ovw**&**를 입력하여 HP OpenView를 시작합니다.
3. 주 메뉴에서 **보안 > 구성**을 선택합니다.
4. Configuration File Management Utility에서 **File > Add Host를** 선택하고 **Next**를 클릭합니다.
5. 요청된 정보를 입력하는 방법의 예입니다



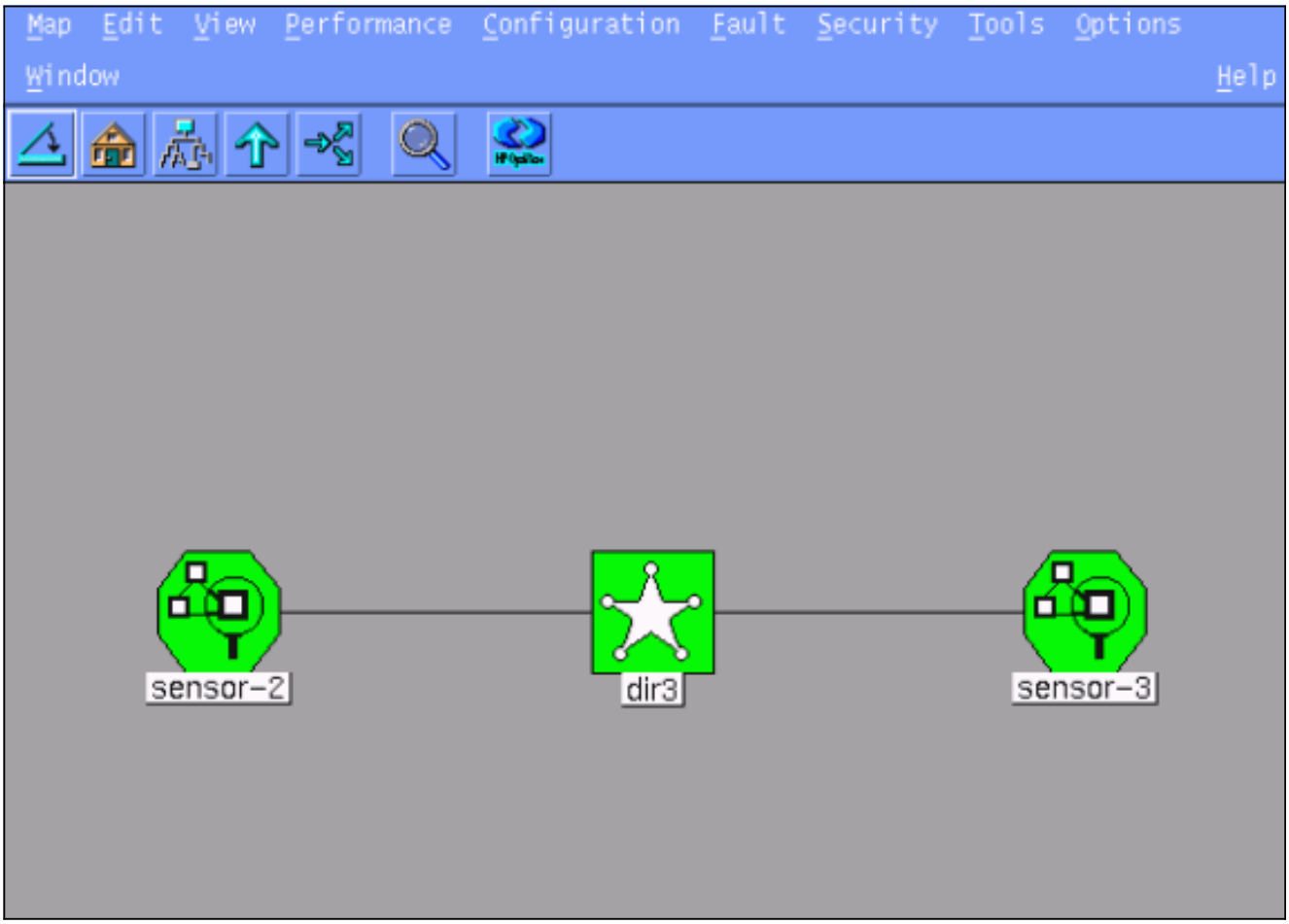
6. 시스템 유형에 대한 기본 설정을 적용하고 이 예와 같이 **다음**을 클릭합니다



7. 로그 및 차단 분을 변경하거나, 값이 허용되는 경우 기본값으로 둡니다.네트워크 인터페이스 이름을 스니핑 인터페이스의 이름으로 변경합니다.이 예에서는 "iprb0"입니다. 센서 유형 및 센서 연결 방법에 따라 "spwr0" 또는 그 밖의 다른 것일 수 있습니다



8. Finish(마침)를 클릭하는 옵션이 있을 때까지 Next(다음)를 **클릭합니다**.센서를 디렉터에 추가했습니다.주 메뉴에서 -2가 이 예와 같이 표시됩니다

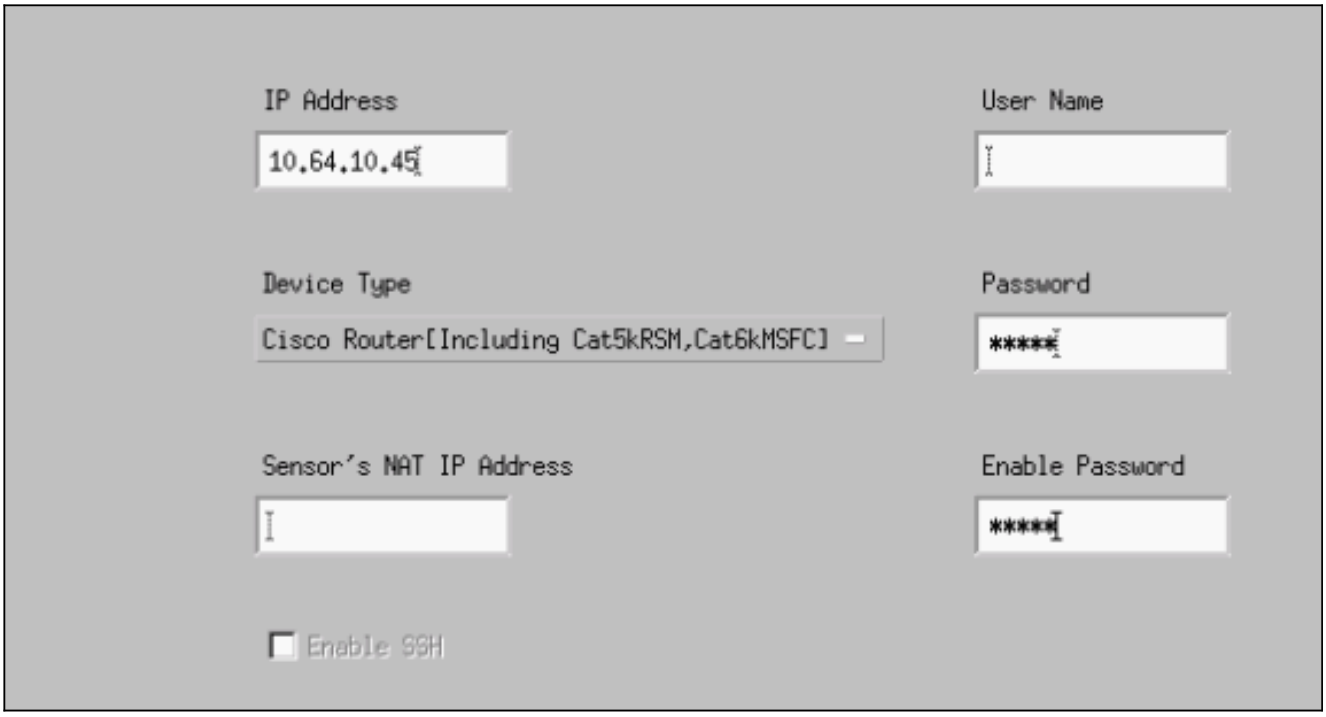


Cisco IOS Router에 대한 차단 구성

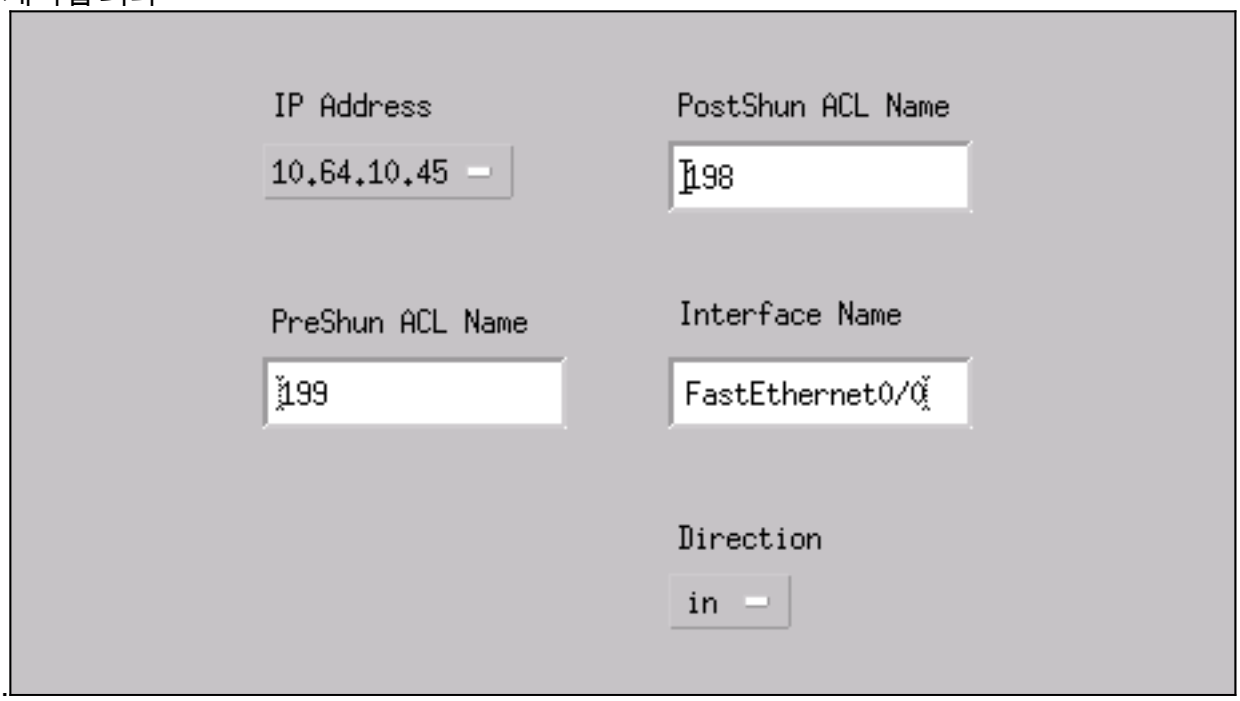
Cisco IOS 라우터에 대한 연결을 구성하려면 다음 단계를 완료합니다.

1. 주 메뉴에서 **보안 > 구성**을 선택합니다.
2. Configuration File Management Utility(컨피그레이션 파일 관리 유틸리티)에서 **sensor-2**를 강조 표시하고 두 번 클릭합니다.
3. 디바이스 **관리를 엽니다**.
4. Devices **> Add**를 클릭하고 이 예와 같이 정보를 입력합니다.OK(**확인**)를 클릭하여 계속합니다 .텔넷 및 enable 비밀번호는 라우터 "House"에 있는 것과 일치합니다

.

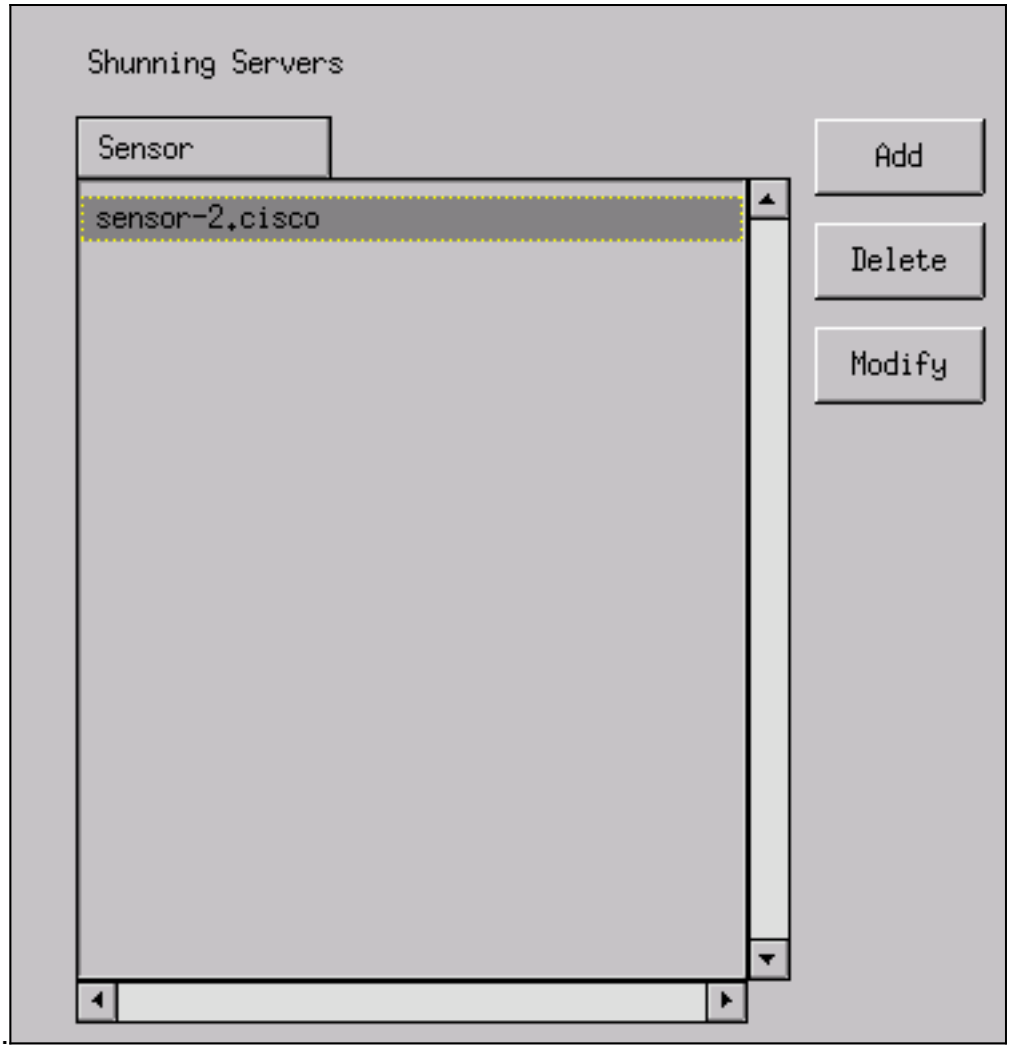


5. Interfaces(**인터페이스) > Add(추가)**를 클릭하고 이 정보를 입력한 다음 **OK(확인)를 클릭하여** 계속합니다



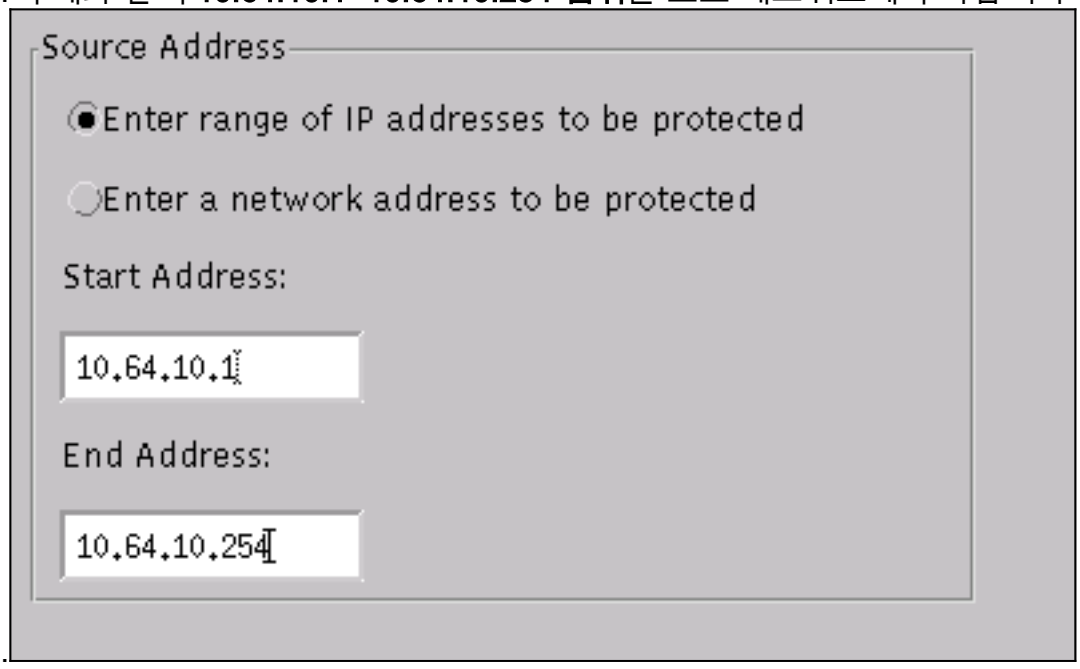
.

6. Covering **> Add**를 클릭하고 **sensor-2.cisco**를 제외 서버로 선택합니다.완료되면 Device Management 창을 닫습니다



.

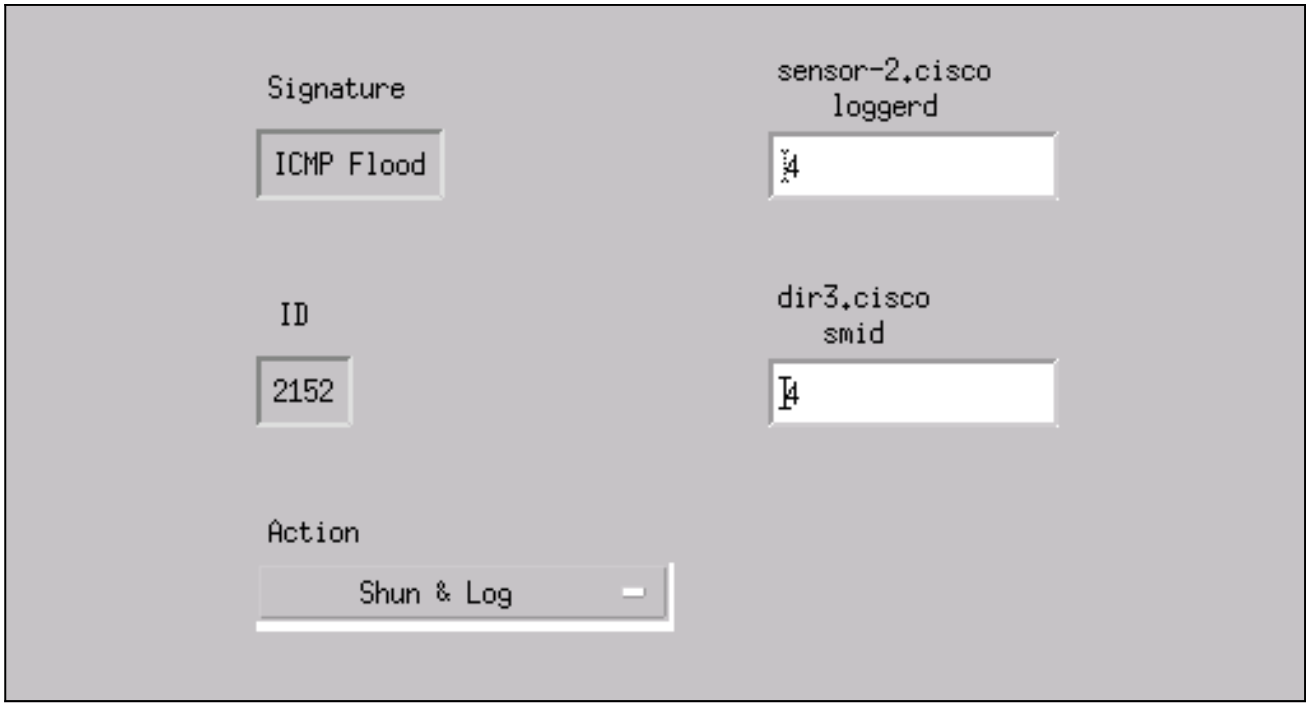
7. Intrusion Detection(침입 탐지) 창을 열고 Protected Networks(**보호된 네트워크)를** 클릭합니다 .이 예와 같이 **10.64.10.1~10.64.10.254 범위**를 보호 네트워크에 추가합니다



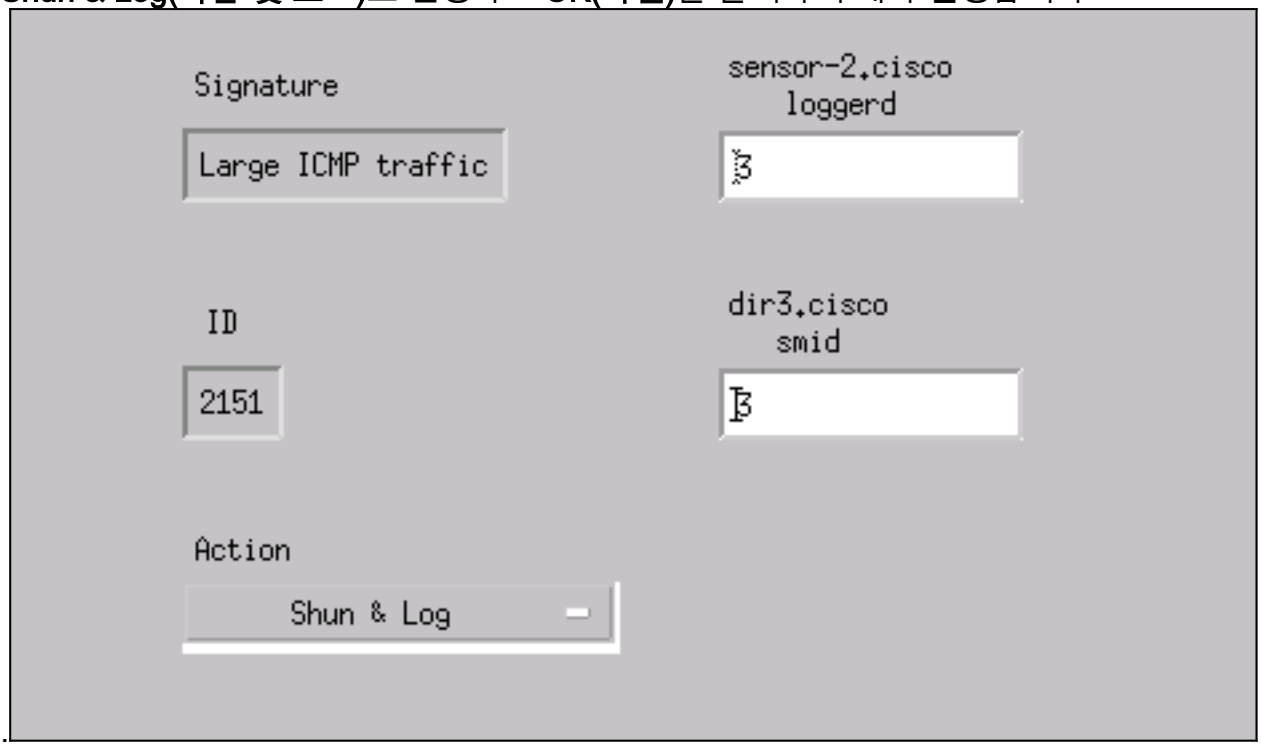
.

8. Profile **> Manual Configuration을 클릭합니다**.
9. Modify **Signatures > Large ICMP Traffic** with ID **2151을 선택합니다**.
10. Modify(**수정)**를 클릭하고 **Action(작업)**을 None(없음)에서 **Shun & Log(차단 및 로그)로 변경한** 다음 **OK(확인)를** 클릭하여 계속 진행합니다

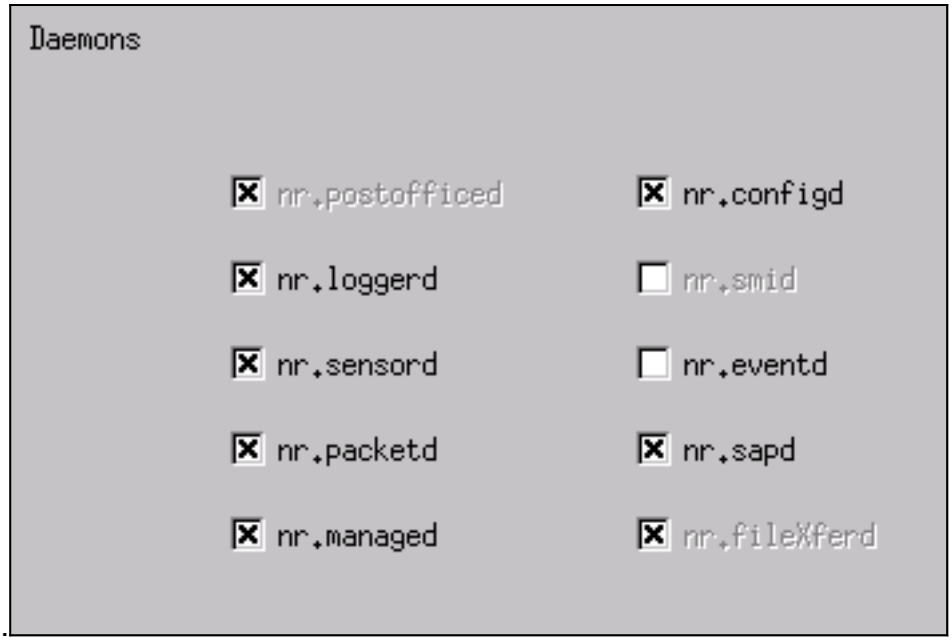
.



11. ID가 **2152**인 **ICMP Flood**를 선택하고 Modify를 **클릭합니다**.Action(작업)을 **None(없음)**에서 **Shun & Log(차단 및 로그)**로 변경하고 **OK(확인)**를 클릭하여 계속 진행합니다



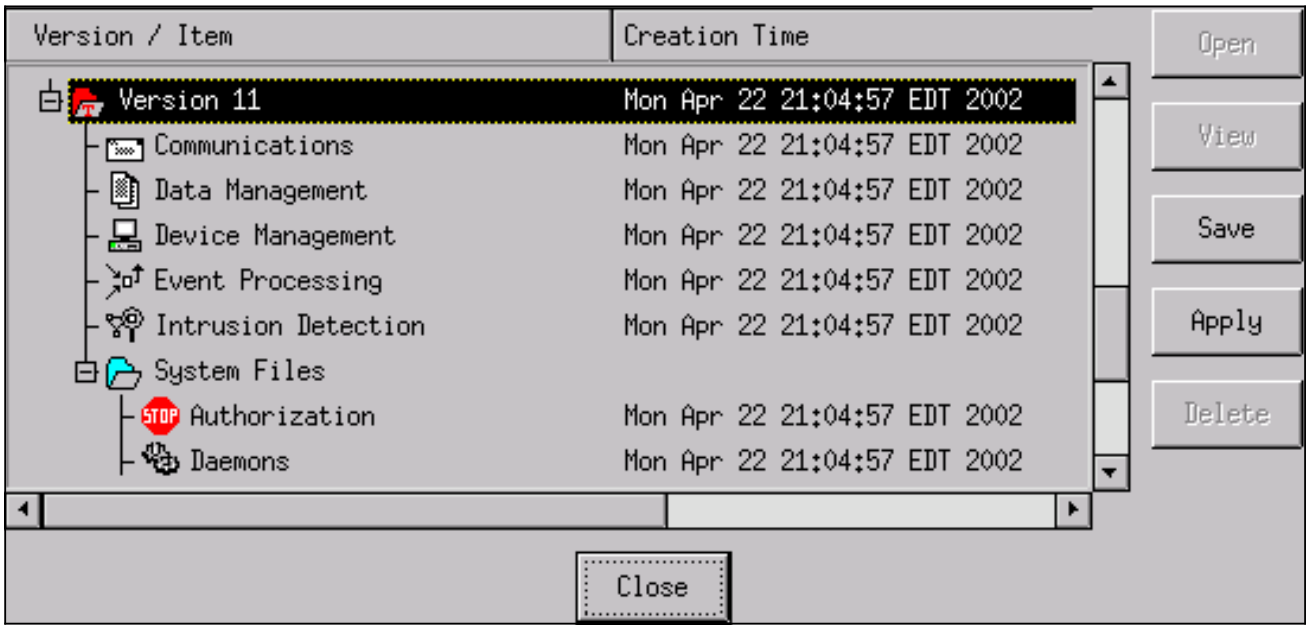
12. OK를 클릭하여 Intrusion Detection 창을 닫습니다.
13. System Files 폴더를 열고 Daemons 창을 엽니다.다음 데몬을 사용하도록 설정했는지 확인



합니다.

14. OK(**확인**)를 클릭하여 계속 진행하고 방금 수정한 버전을 선택한 다음 **Save(저장)**와 Apply(적용)를 **클릭합니다**.시스템이 서비스 재시작을 완료했음을 알려 줄 때까지 기다린 다음 디렉터 구성의 모든 창을 닫습니다

.



다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

- **show access-list** - **access-list** 명령문을 라우터 컨피그레이션에 나열합니다.또한 access-**list** 명령 검색 중에 요소가 일치한 횟수를 나타내는 적중 횟수가 나열됩니다.
- **ping** - 기본 네트워크 연결을 진단하는 데 사용됩니다.

공격이 시작되기 전

공격이 시작되기 전에 다음 명령을 실행합니다.

```
house#show access-list
Extended IP access list IDS_FastEthernet0/0_in_1
    permit ip host 10.64.10.49 any
    permit ip any any (12 matches)
house#

light#ping 10.64.10.45

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.64.10.45, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
light#
```

공격 실행 및 차단

라우터 "Light"에서 피해자 "House"로 공격을 실행합니다. ACL이 적용되면 연결되지 않은 항목이 표시됩니다.

```
light#ping
Protocol [ip]:
Target IP address: 10.64.10.45
Repeat count [5]: 1000000
Datagram size [100]: 18000
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 1000000, 18000-byte ICMP Echos to 10.64.10.45, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.
```

센서가 공격을 감지하고 ACL을 다운로드하면 이 출력이 "House"에 표시됩니다.

```
house#show access-list
Extended IP access list IDS_FastEthernet0/0_in_0
  permit ip host 10.64.10.49 any
  deny ip host 100.100.100.2 any (459 matches)
  permit ip any any
```

이 예와 같이 연결되지 않은 것은 "Light"에 표시됩니다.

```
Light#ping 10.64.10.45
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.64.10.45, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
```

15분 후, "집"은 고소를 15분으로 설정한 상태였기 때문에 정상으로 돌아왔습니다.

```
House#show access-list
Extended IP access list IDS_FastEthernet0/0_in_1
    permit ip host 10.64.10.49 any
    permit ip any any (12 matches)
```

```
house#
```
"조명"은 "하우스"를 ping할 수 있습니다.

```
Light#ping 10.64.10.45

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.64.10.45, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

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