使用 Cisco IDS Unix Director 避开 IDS PIX

目录

简介

本文描述如何在Cisco IDS Unix Director (以前叫作Netranger导向器)和传感器帮助下配置在PIX的避开。本文假设，传感器和导向器是可操作的，并且传感器的探测接口设置跨过到PIX外部接口。

先决条件

要求

本文档没有任何特定的前提条件。

使用的组件

本文档中的信息基于以下软件和硬件版本。

- Cisco IDS Unix Director 2.2.3
- Cisco IDS UNIX传感器3.0.5
- 与6.1.1的Cisco Secure PIX**注意：** 如果使用6.2.x版本，您能使用安全套接协议(SSH)管理，但是不远程登录。参考的Cisco Bug ID CSCdx55215 (仅限注册用户)欲知详情。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

本部分提供用于配置本文档所述功能的信息。

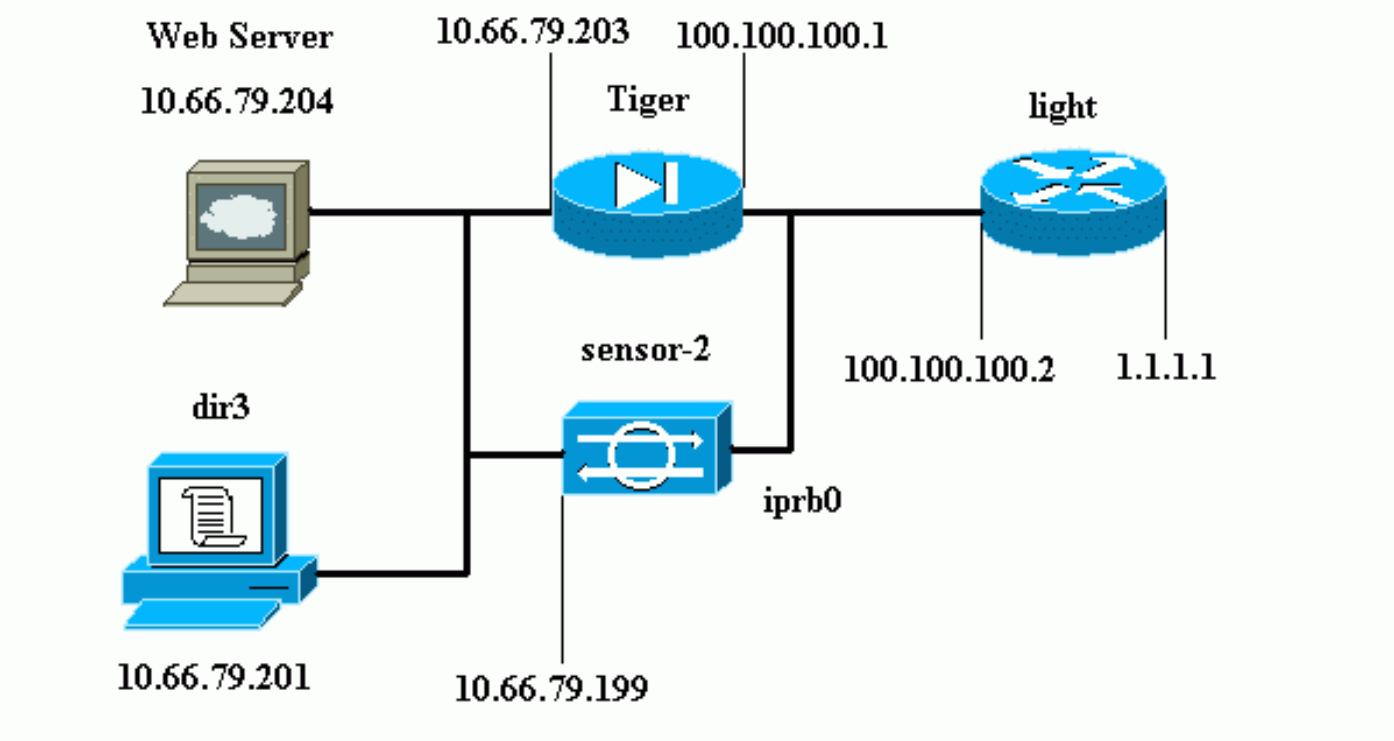
Cisco IDS Unix Director和传感器用于为了管理避开的Cisco Secure PIX。当您考虑此配置时，请记住这些概念：

- 安装传感器并且适当地确保传感器工作。
- 保证探测接口间距对PIX的外部接口。

注意： 为了找到关于用于本文的命令的其他信息，参考命令查找工具(仅限注册用户)。

网络图

本文档使用此网络设置。



配置

本文档使用以下配置。

- 路由器灯
- PIX Tiger

路由器灯
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
```

PIX Tiger

```
PIX Version 6.1(1)
nameif gb-ethernet0 intf2 security10
nameif gb-ethernet1 intf3 security15
nameif ethernet0 outside security0 nameif ethernet1
inside security100 enable password 2KFQnbNIdI.2KYOU
encrypted passwd 9jNfZuG3TC5tCVH0 encrypted hostname
Tiger fixup protocol ftp 21 fixup protocol http 80 fixup
protocol h323 1720 fixup protocol rsh 514 fixup protocol
rtsp 554 fixup protocol smtp 25 fixup protocol sqlnet
1521 fixup protocol sip 5060 fixup protocol skinny 2000
names !--- Allows ICMP traffic and HTTP to pass through
the PIX !--- to the Web Server. access-list 101 permit
icmp any host 100.100.100.100 access-list 101 permit tcp
any host 100.100.100.100 eq www pager lines 24 logging
on logging buffered debugging interface gb-ethernet0
1000auto shutdown interface gb-ethernet1 1000auto
shutdown interface ethernet0 auto interface ethernet1
auto mtu intf2 1500 mtu intf3 1500 mtu outside 1500 mtu
inside 1500 ip address intf2 127.0.0.1 255.255.255.255
ip address intf3 127.0.0.1 255.255.255.255 ip address
outside 100.100.100.1 255.255.255.0 ip address inside
10.66.79.203 255.255.255.224 ip audit info action alarm
ip audit attack action alarm no failover failover
timeout 0:00:00 failover poll 15 failover ip address
intf2 0.0.0.0 failover ip address intf3 0.0.0.0 failover
ip address outside 0.0.0.0 failover ip address inside
0.0.0.0 pdm history enable arp timeout 14400 global
(outside) 1 interface nat (inside) 1 0.0.0.0 0.0.0.0 0 0
!--- Static NAT for the Web Server. static
(inside,outside) 100.100.100.100 10.66.79.204 netmask
255.255.255.255 0 0 access-group 101 in interface
outside route outside 0.0.0.0 0.0.0.0 100.100.100.2 1
route inside 10.66.0.0 255.255.0.0 10.66.79.193 1
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 s0 timeout
uauth 0:05:00 absolute aaa-server TACACS+ protocol
tacacs+ aaa-server RADIUS protocol radius aaa-server
LOCAL protocol tacacs+ no snmp-server location no snmp-
server contact snmp-server community public no snmp-
server enable traps floodguard enable no sysopt route
dnat !--- Allows Sensor Telnet to the PIX from the
inside interface. telnet 10.66.79.199 255.255.255.255
inside telnet timeout 5 ssh timeout 5 terminal width 80
```

```
Cryptochecksum:b4c820ba31fbb3996ca8891503ebacbc : end
```

配置传感器

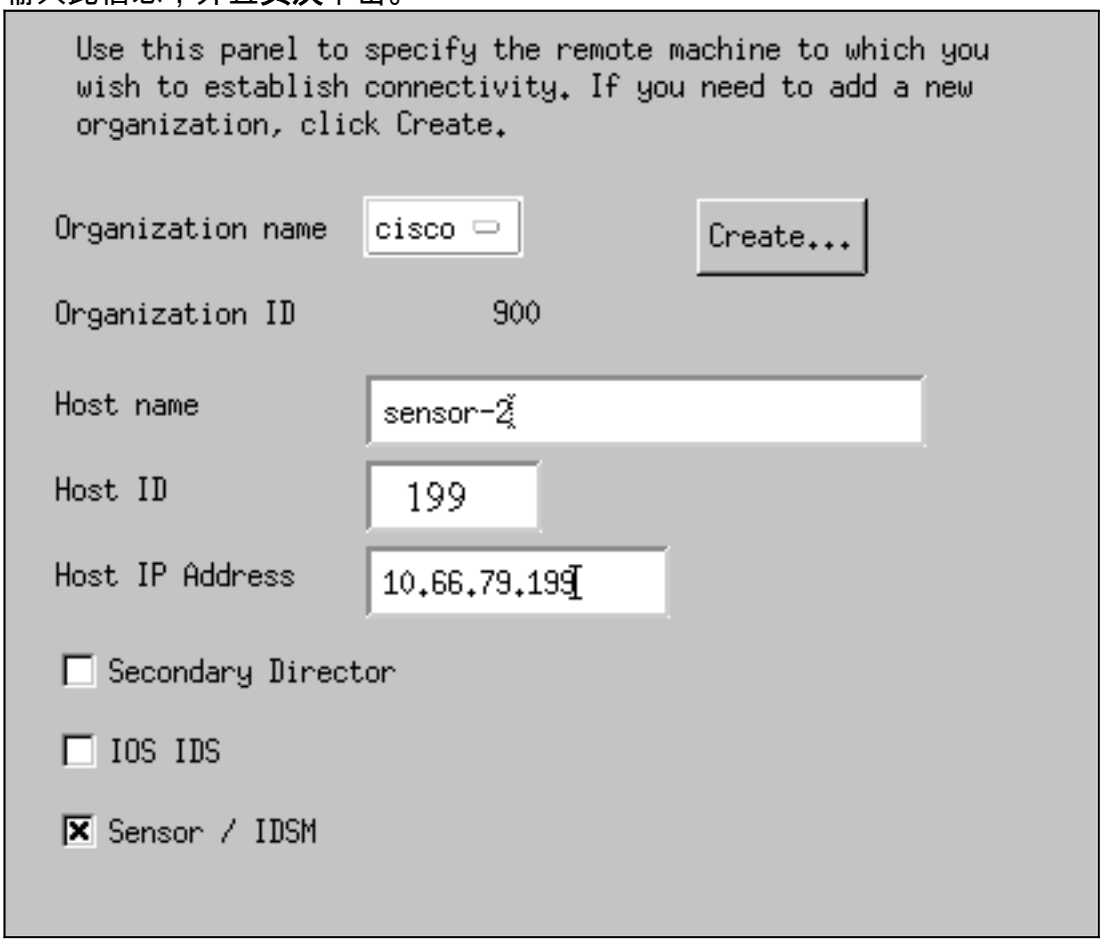
这些步骤描述如何配置传感器。

1. 对**10.66.79.199的**Telnet与用户名根和密码攻击。
2. 回车**sysconfig-sensor**。
3. 输入此信息：IP 地址：**10.66.79.199**IP网络掩码：**255.255.255.224**IP主机命名：**sensor-2**默认路由：**10.66.79.193**网络访问控制**10.**通信基础架构传感器主机ID ：**49**传感器组织ID ：**900**传感器主机名：**sensor-2**传感器组织名称：**cisco**传感器IP地址：**10.66.79.199**IDS管理器主机ID ：**50**IDS管理器组织ID ：**900**IDS管理器主机名：**dir3**IDS管理器组织名称 ：**cisco**IDS管理器IP地址：**10.66.79.201**
4. 保存配置。传感器然后重新启动。

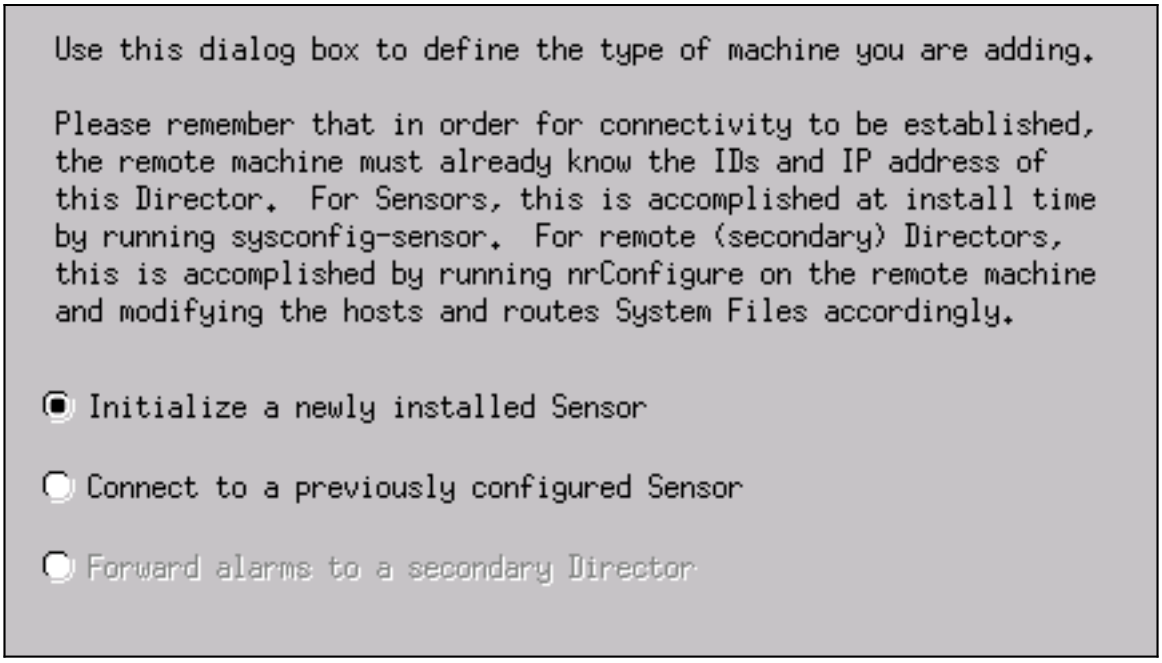
添加传感器到导向器

完成这些步骤为了添加传感器到导向器。

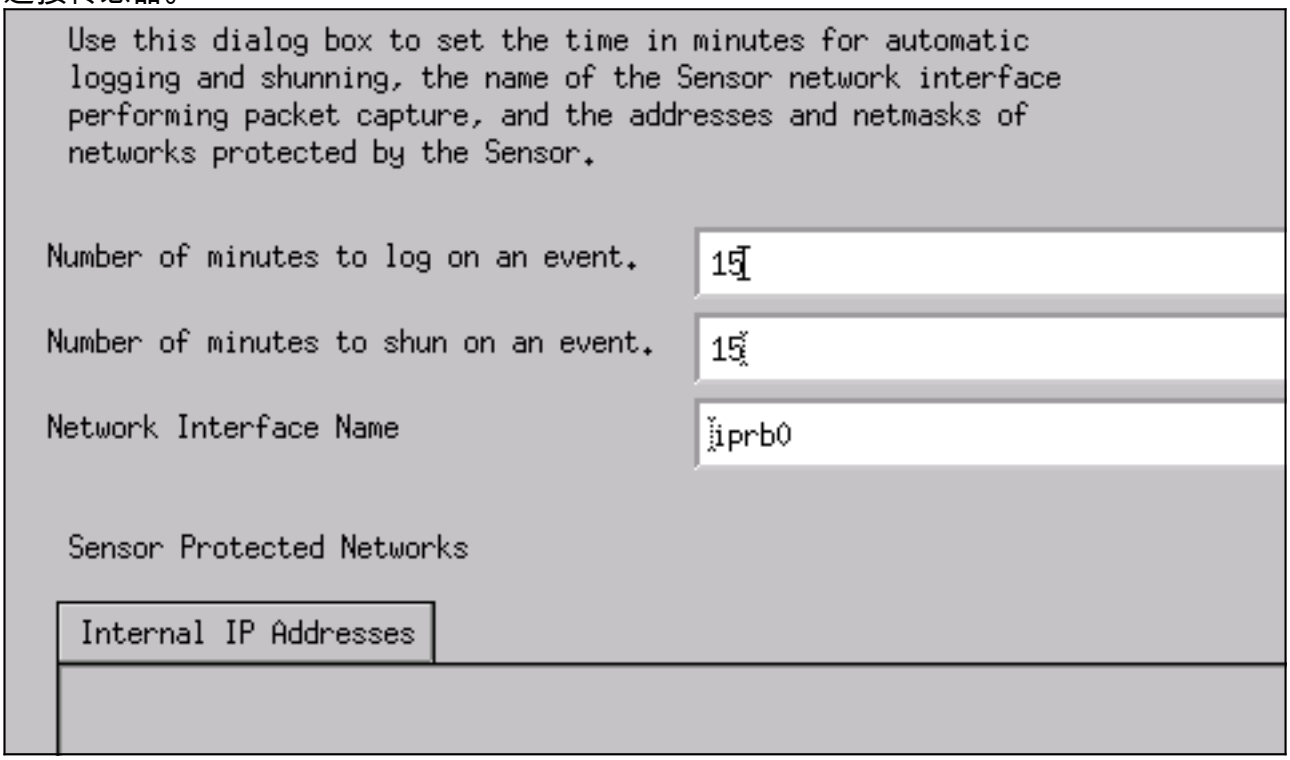
1. 远程登录到与用户名**netrangr**和密码攻击的**10.66.79.201**。
2. 输入**ovw&**为了启动HP OpenView。
3. 在主菜单，请选择**Security > Configure**。
4. 在Netranger配置菜单，请选择**File > Add Host**，并且**其次**单击。
5. 输入此信息，并且**其次**单击。



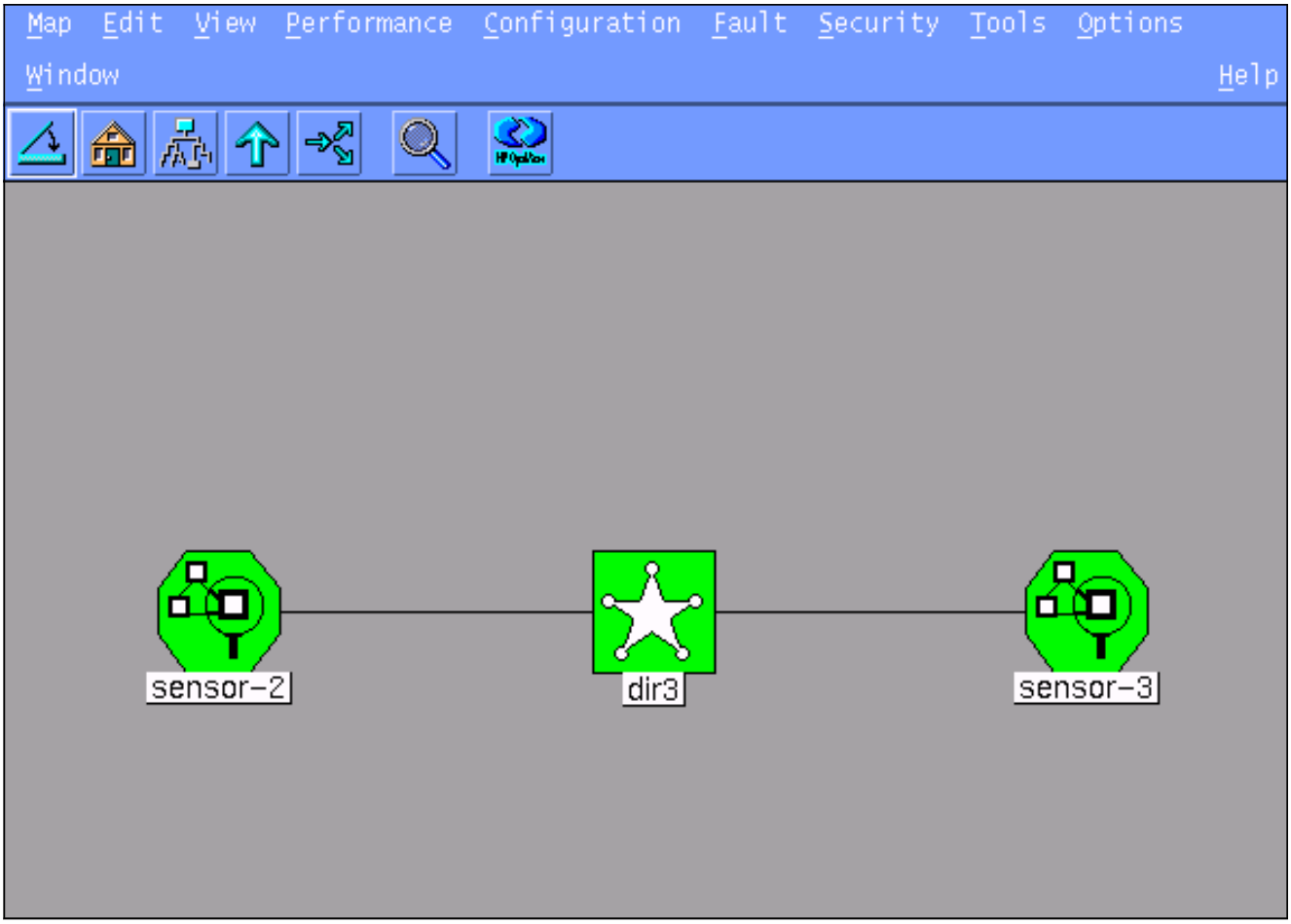
6. 留下默认设置并且**其次**单击。



7. 如果值是可接受，请更改日志并且避开分钟或留下他们作为默认。更改网络接口名字对您的探测接口名称。在本例中，它是"iprb0"。它可以是根据传感器类型或别的"spwr0"，并且您如何连接传感器。



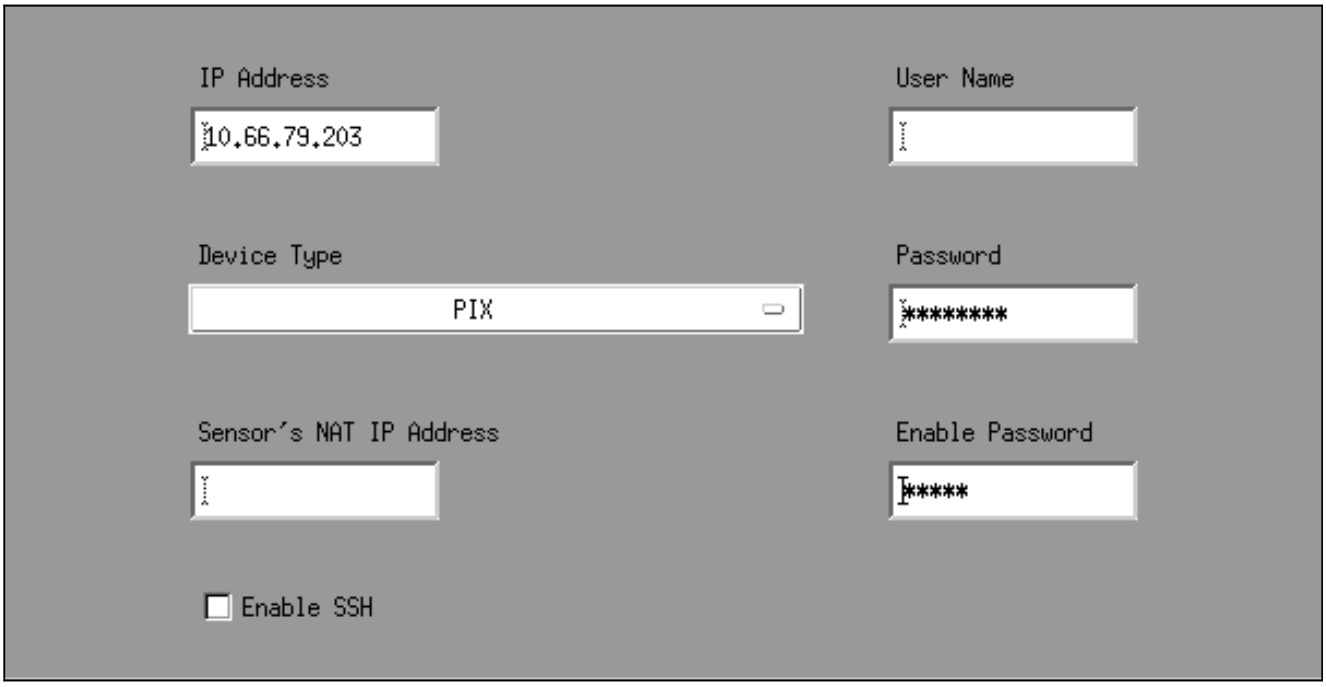
8. **其次请**单击，直到有选项点击**芬通社**。传感器成功地当前添加到导向器。如此示例所显示，从主菜单， **sensor-2**显示。



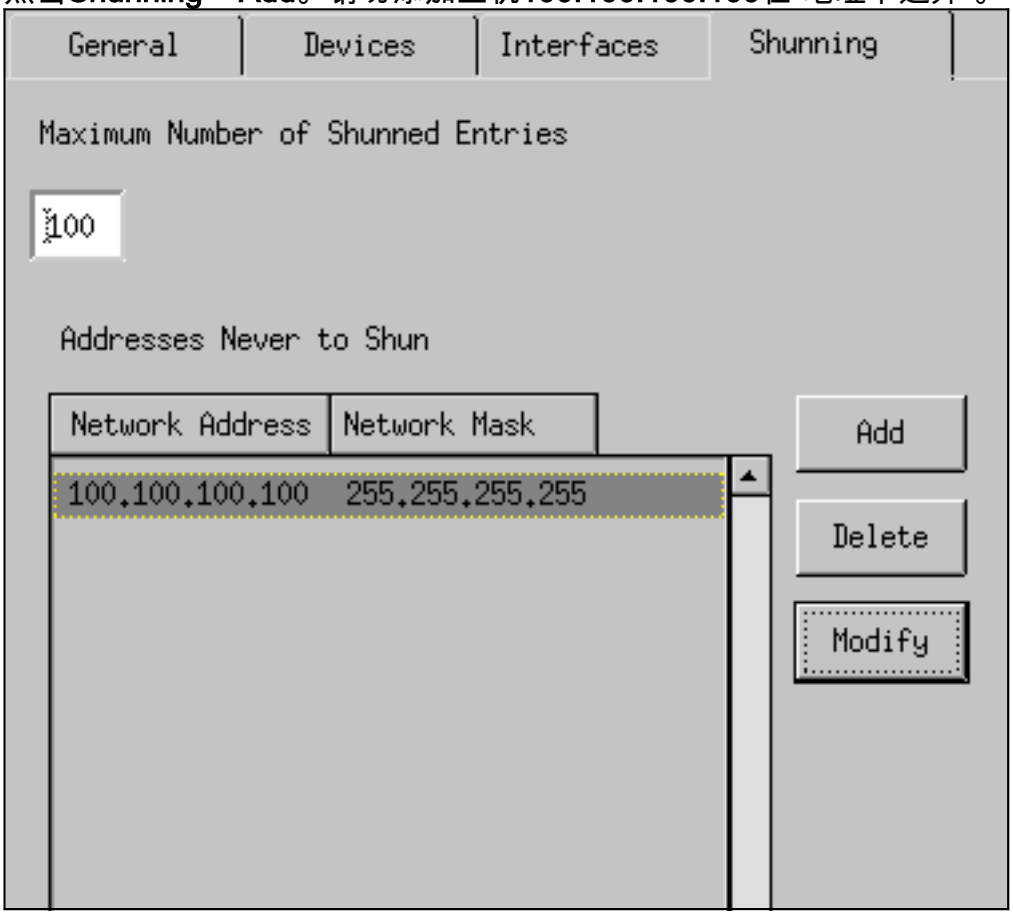
配置PIX的避开

完成这些步骤为了配置PIX的避开。

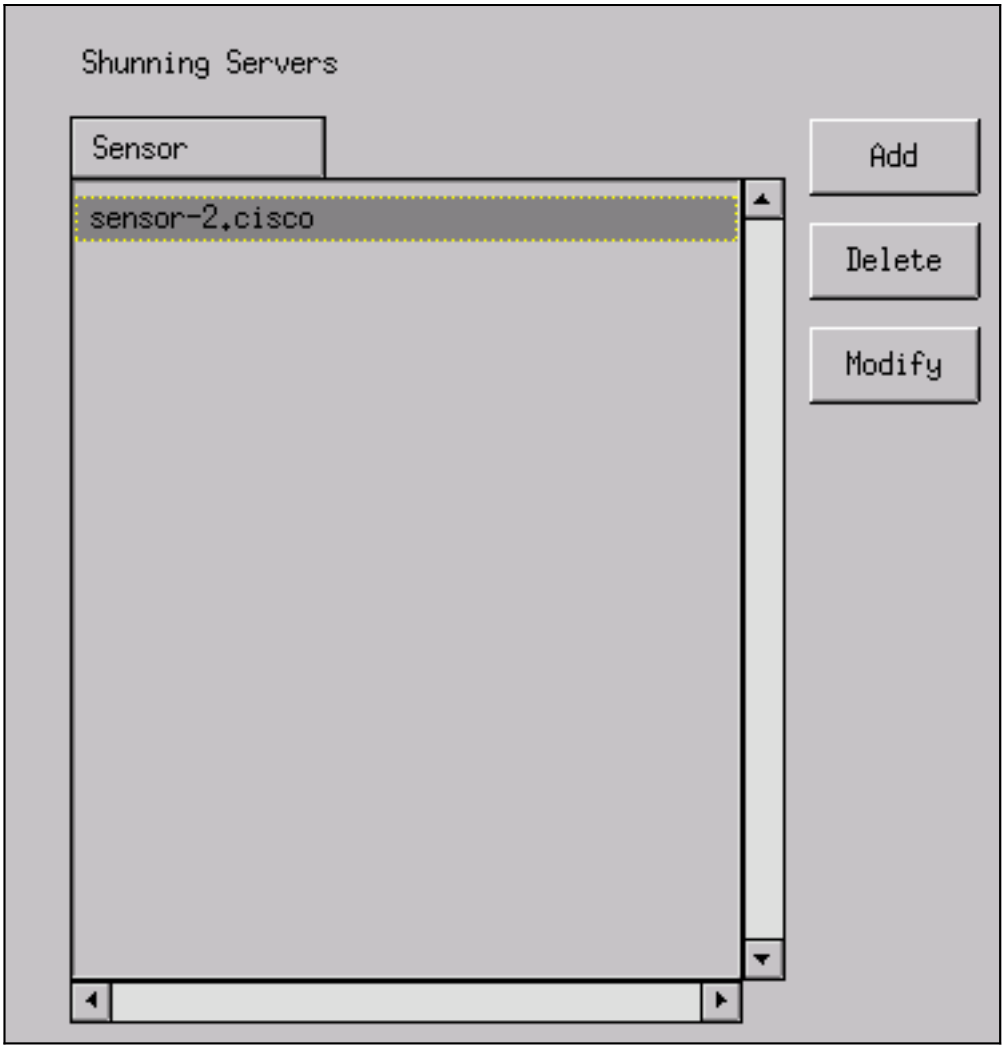
1. 在主菜单，请选择**Security > Configure**。
2. 在Netranger配置菜单，请突出显示**sensor-2**并且双击它。
3. 打开**设备管理**。
4. 如此示例所显示，点击**Devices > Add**并且输入信息。单击 **OK** 以继续。Telnet和特权密码是两“思科”。



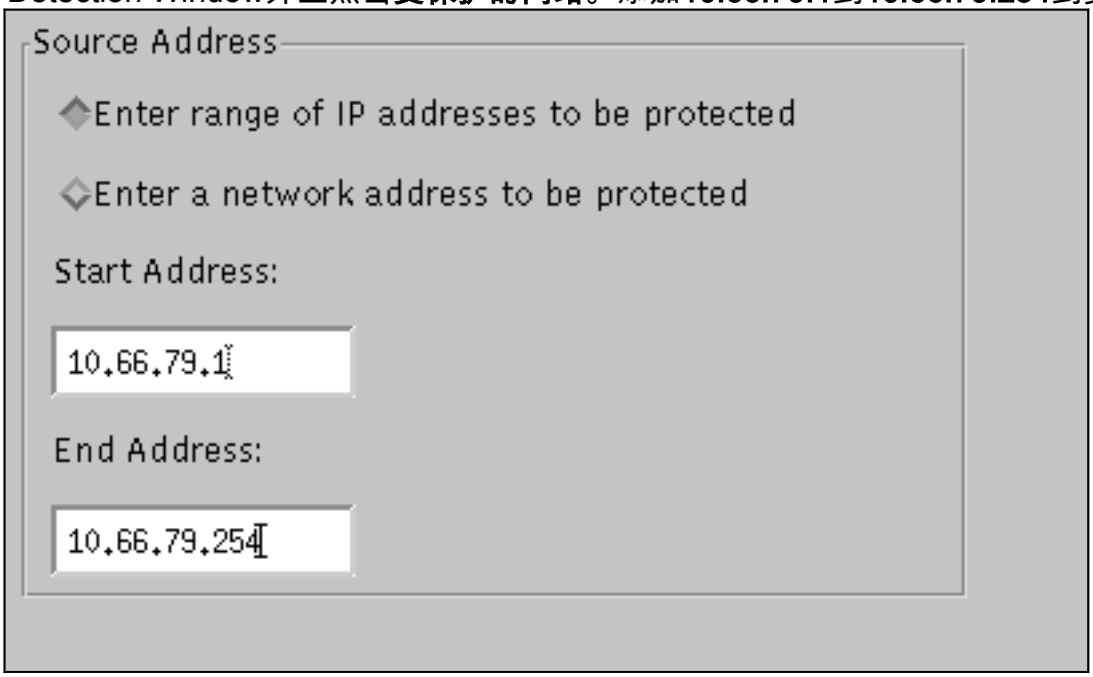
5. 点击**Shunning > Add**。请勿添加主机**100.100.100.100**在“地址下避开”。单击 **OK** 以继续。



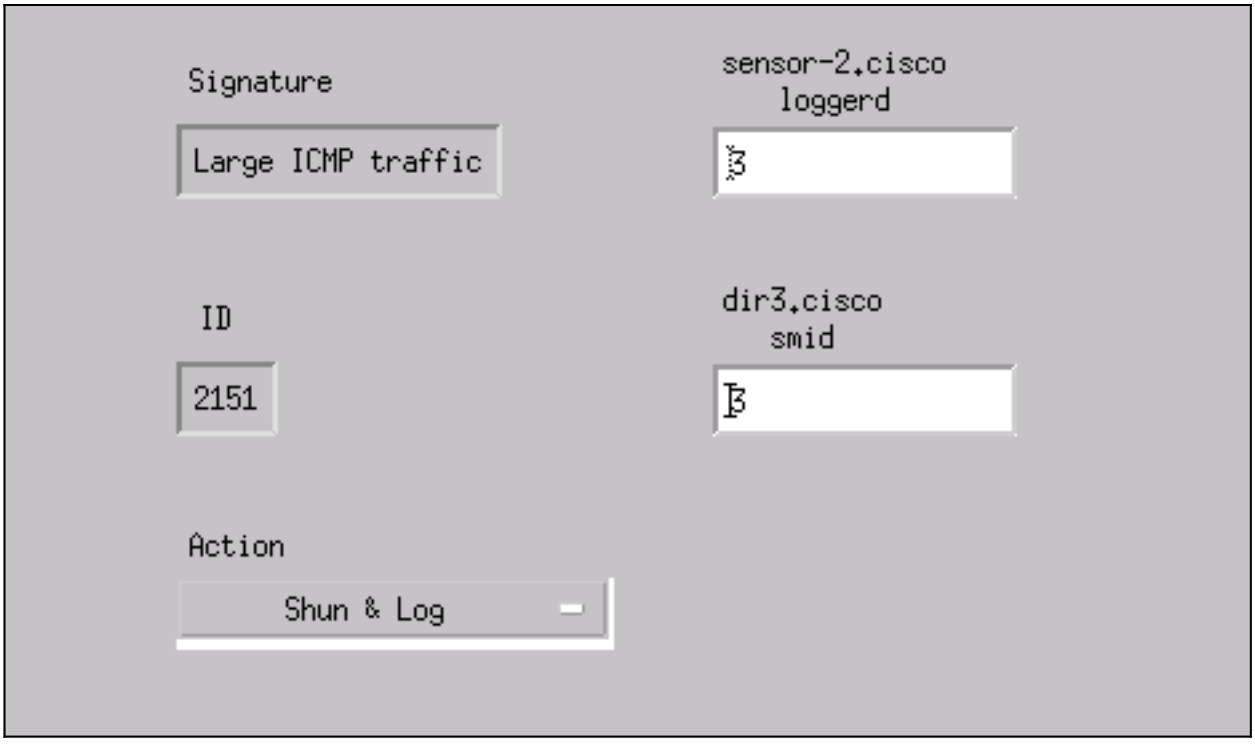
6. 点击**Shunning > Add**并且选择**sensor-2.cisco**作为避开服务器。配置的这部分完成。关上 Device Management窗口。



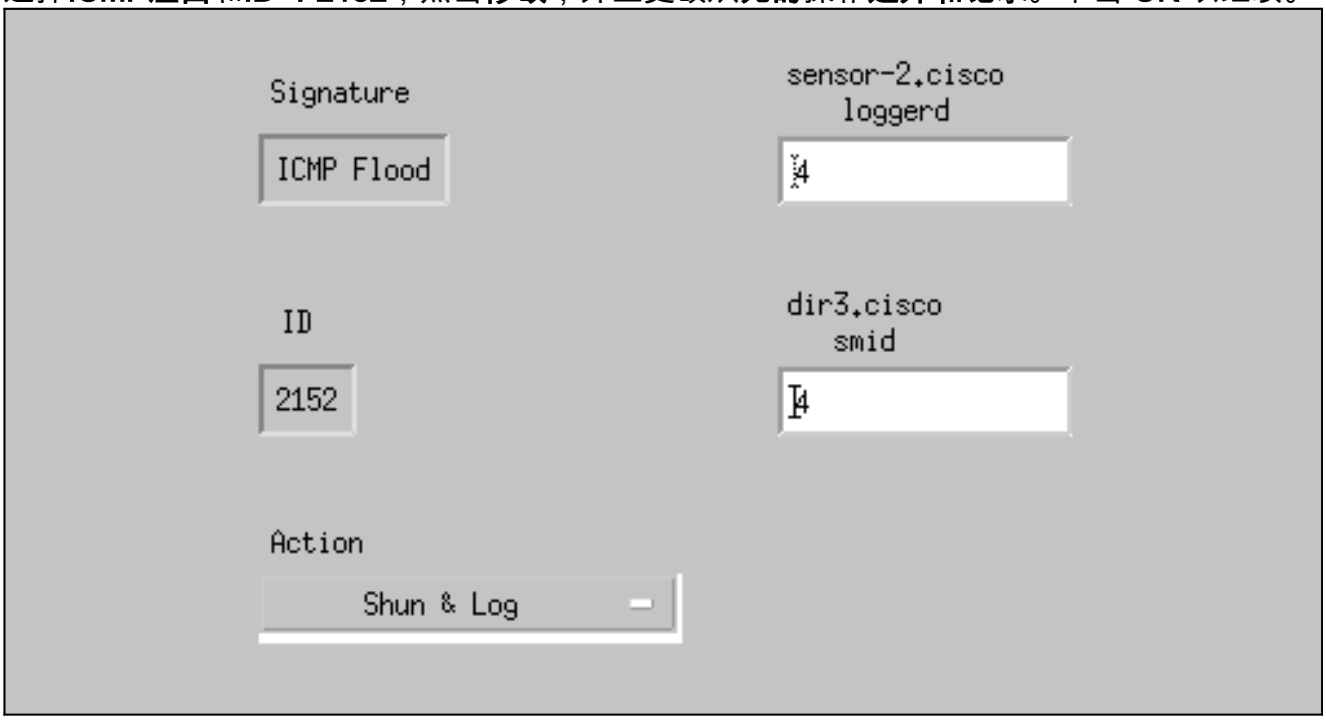
7. 打开Intrusion Detection Window并且点击**受保护的网络**。添加**10.66.79.1**到**10.66.79.254**到受保护的网络。



8. 点击**配置文件**并且选择**手动配置**> Modify**签名**。选择**大ICMP流量**和**ID ：2151**，点击**修改**，并且更改从无的操作**避开和记录**。单击 OK 以继续。

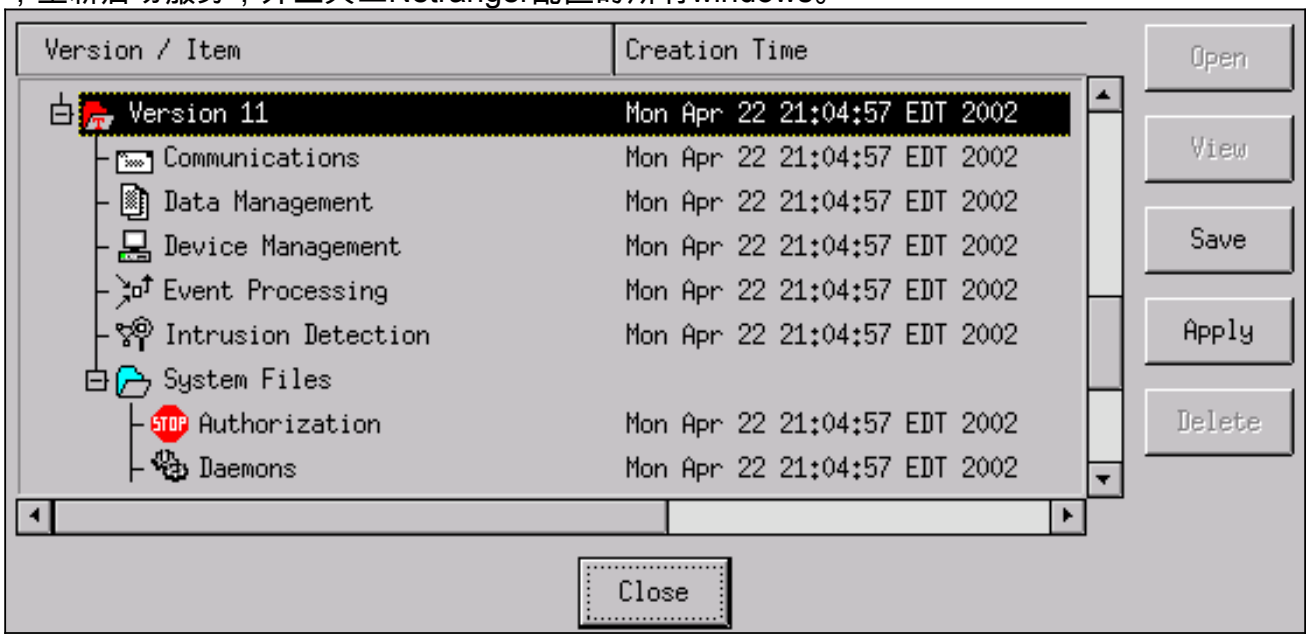


9. 选择**ICMP溢出**和**ID ：2152**，点击**修改**，并且更改从**无的**操作**避开和记录**。单击 **OK** 以继续。



10. 配置的这部分完成。点击OK键为了关上Intrusion Detection Window。
11. 打开**系统文件**文件夹并且打开**Daemons窗口**。保证您启用这些守护程序
    ：

12. 点击OK键为了继续和选择您修改的版本。点击**"Save" >应用**。等待系统告诉您传感器完成，重新启动服务，并且关上Netranger配置的所有windows。



验证

此部分提供帮助您适当地确认您的配置工作的信息。

在您发起攻击前

```
Tiger(config)# show telnet 10.66.79.199 255.255.255.255 inside Tiger(config)# who 0:
10.66.79.199 Tiger(config)# show xlate 1 in use, 1 most used Global 100.100.100.100 Local
10.66.79.204 static Light#ping 100.100.100.100 Type escape sequence to abort. Sending 5, 100-
byte ICMP Echos to 100.100.100.100, timeout is 2 seconds: !!!!! Success rate is 100 percent
(5/5), round-trip min/avg/max = 112/195/217 ms Light#telnet 100.100.100.100 80 Trying
100.100.100.100, 80 ... Open
```

发起攻击和规避

```
Light#ping Protocol [ip]: Target IP address: 100.100.100.100 Repeat count [5]: 100000 Datagram
size [100]: 18000 Timeout in seconds [2]: Extended commands [n]: Sweep range of sizes [n]: Type
escape sequence to abort. Sending 100000, 18000-byte ICMP Echos to 100.100.100.100, timeout is 2
```

```
seconds: !..... Success rate is 4 percent (1/21), round-trip min/avg/max =
281/281/281 ms Light#telnet 100.100.100.100 80 Trying 100.100.100.100, 80 ... % Connection timed
out; remote host not responding Tiger(config)# show shun Shun 100.100.100.2 0.0.0 Tiger(config)#
show shun stat intf2=OFF, cnt=0 intf3=OFF, cnt=0 outside=ON, cnt=2604 inside=OFF, cnt=0
intf4=OFF, cnt=0 intf5=OFF, cnt=0 intf6=OFF, cnt=0 intf7=OFF, cnt=0 intf8=OFF, cnt=0 intf9=OFF,
cnt=0 Shun 100.100.100.2 cnt=403, time=(0:01:00).0 0 0
```

因为避开设置为十五分钟，十五分钟后，它回到正常。

```
Tiger(config)# show shun Tiger(config)# show shun stat intf2=OFF, cnt=0 intf3=OFF, cnt=0
outside=OFF, cnt=4437 inside=OFF, cnt=0 intf4=OFF, cnt=0 intf5=OFF, cnt=0 intf6=OFF, cnt=0
intf7=OFF, cnt=0 intf8=OFF, cnt=0 intf9=OFF, cnt=0 Light#ping 100.100.100.100 Type escape
sequence to abort. Sending 5, 100-byte ICMP Echos to 100.100.100.100, timeout is 2 seconds:
!!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms Light#telnet
100.100.100.100 80 Trying 100.100.100.100, 80 ... Open
```

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- Cisco IDS Director的销售终止
- Cisco IDS传感器软件版本3.x的生命周期结束
- 思科入侵防御系统产品支持
- 思科PIX防火墙软件产品支持
- Cisco Secure PIX 防火墙命令参考
- 技术支持和文档 - Cisco Systems