

Cisco IDS Unix Directorを使用するIDS PIX遮断

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[Sensor の設定](#)

[Director への Sensor の追加](#)

[PIX のためのシャニングを設定して下さい](#)

[確認](#)

[攻撃を開始する前に](#)

[攻撃 および シャニングを開始して下さい](#)

[トラブルシューティング](#)

[関連情報](#)

概要

この資料に Cisco IDS Unix ディレクタ (以前 Netranger ディレクターとして知られている) およびセンサーの助けによって PIX のシャニングを設定する方法を記述されています。この資料はセンサーおよびディレクターが正常に動作して、センサーの探知インターフェイスが PIX outside インターフェイスに及ぶために設定されると仮定します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IDS Unix ディレクタ 2.2.3
- Cisco IDS UNIX センサー 3.0.5
- 6.1.1 の CiscoセキュアPIX注: 6.2.x バージョンを使用する場合、Secure Shell Protocol (SSH) 管理を使用し、Telnet で接続しないことができます。Cisco バグ ID [CSCdx55215](#)

([登録ユーザのみ](#)) を詳細については参照して下さい。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

設定

このセクションでは、このドキュメントで説明する機能を設定するための情報を提供します。

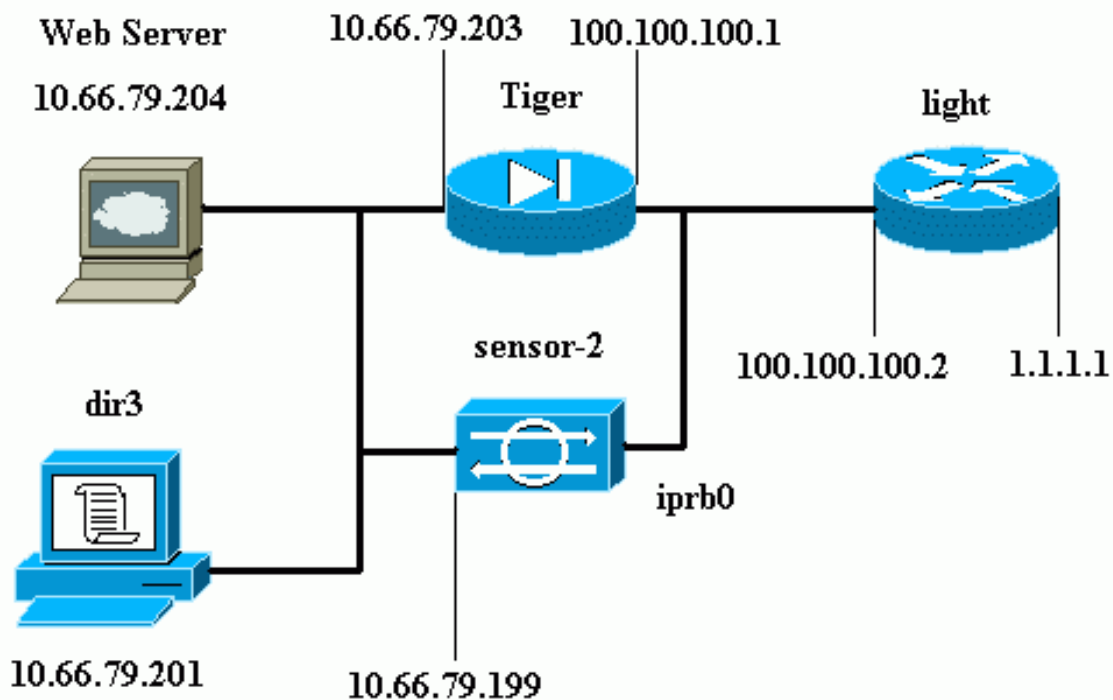
Cisco IDS Unix ディレクタおよびセンサーはシャニングのための Cisco セキュアPIX を管理するために使用されます。この設定を考慮するとき、これらの概念を覚えて下さい:

- センサーをインストールし、センサー作業をきちんと確かめて下さい。
- PIX の outside インターフェイスのように探知インターフェイス スパンして下さい。

注: この資料で使用されるコマンドのその他の情報を見つけるために [Command Lookup Tool](#) ([登録ユーザのみ](#)) を参照して下さい。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



設定

このドキュメントでは、次の設定を使用します。

- [Router Light](#)
- [PIX トリガ](#)

Router Light

```

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 トリガ

```

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
```

Sensor の設定

これらのステップはセンサーを設定する方法を記述します。

1. ユーザ名 ルートおよびパスワード攻撃を用いる 10.66.79.199 への Telnet。
2. **sysconfig-sensor** を入力して下さい。
3. 次の情報を入力します。IP Address : 10.66.79.199IP ネットマスク: 255.255.255.224IP ホスト名前: **sensor-2**デフォルト ルート: 10.66.79.193ネットワーク アクセス制御10.コミュニケーション インフラストラクチャセンサー ホストID: 49センサー組織ID: 900センサー ホスト名: **sensor-2**センサー組織名: **cisco**センサー IP アドレス: 10.66.79.199IDS マネージャ ホストID: 50IDS マネージャ組織ID: 900IDS マネージャ ホスト名: **dir3**IDS マネージャ組織名: **cisco**IDS マネージャ IP アドレス: 10.66.79.201
4. 設定を保存します。センサーそしてリブート。

Director への Sensor の追加

ディレクターにセンサーを追加するためにこれらのステップを完了して下さい。

1. ユーザ名 **netrangr** およびパスワード攻撃を用いる 10.66.79.201 に Telnet で接続して下さい。
2. HP OpenView を起動させるために **ovw&** を入力して下さい。
3. メインメニューでは、Security > Configure の順に選択して下さい。
4. Netranger Configuration メニューでは、File > Add Host の順に選択し、『Next』をクリックして下さい。
5. この情報を入力し、『Next』をクリックして下さい。

Use this panel to specify the remote machine to which you wish to establish connectivity. If you need to add a new organization, click Create.

Organization name

Organization ID

Host name

Host ID

Host IP Address

Secondary Director

IOS IDS

Sensor / IDSM

6. デフォルト設定を残し、『Next』をクリックして下さい。

Use this dialog box to define the type of machine you are adding.

Please remember that in order for connectivity to be established, the remote machine must already know the IDs and IP address of this Director. For Sensors, this is accomplished at install time by running `sysconfig-sensor`. For remote (secondary) Directors, this is accomplished by running `nrConfigure` on the remote machine and modifying the `hosts` and `routes` System Files accordingly.

Initialize a newly installed Sensor

Connect to a previously configured Sensor

Forward alarms to a secondary Director

7. 値が受諾可能である場合ログを変更し、分を排除するか、またはデフォルトとして残して下さい。探知インターフェイスの名前にネットワークインターフェイスの名前を変更して下さい。この例では「iprb0」です。それはセンサーをどのように接続するかセンサタイプに基づく「spwr0」または何か他のもののどれであり。

Use this dialog box to set the time in minutes for automatic logging and shunning, the name of the Sensor network interface performing packet capture, and the addresses and netmasks of networks protected by the Sensor.

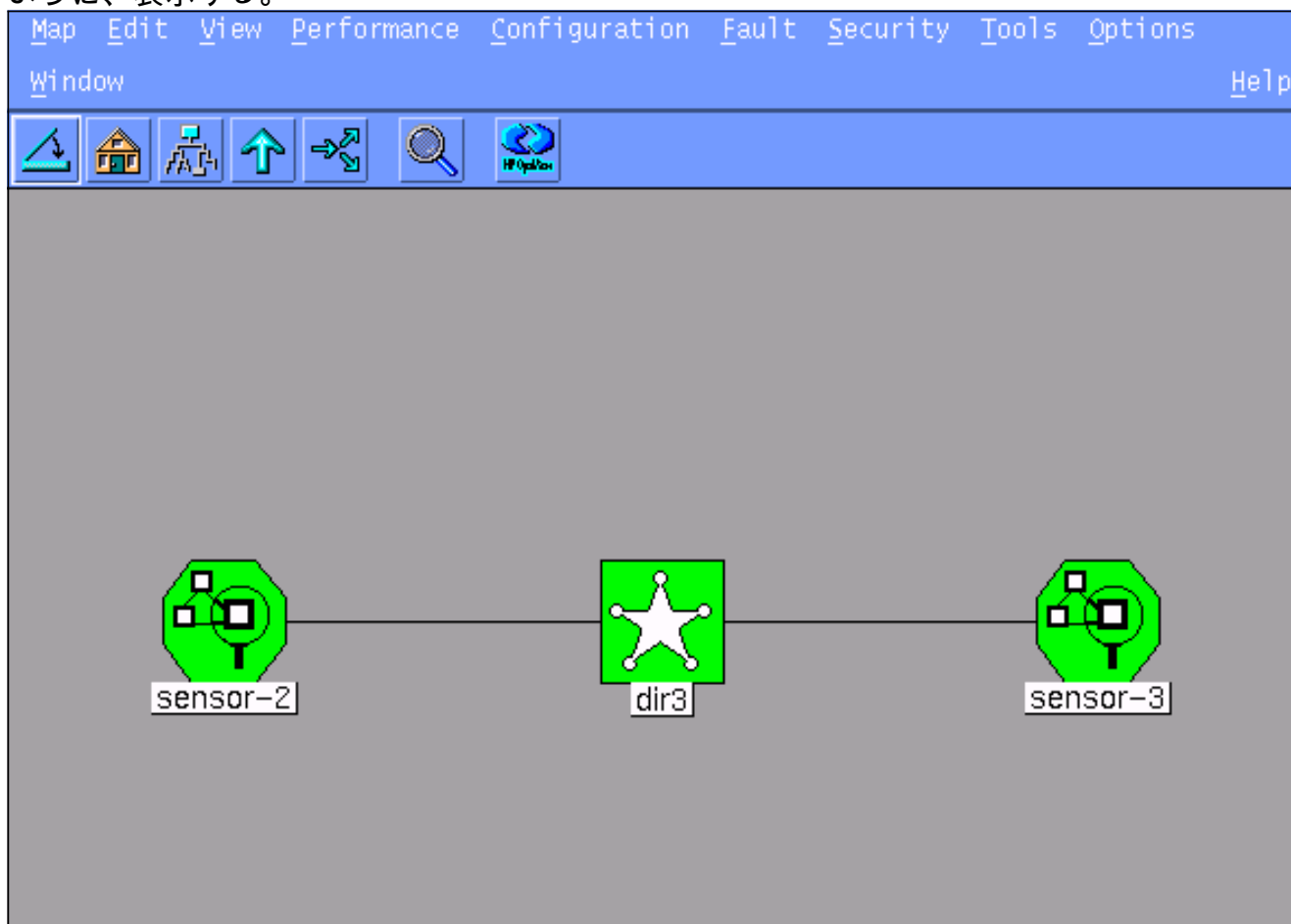
Number of minutes to log on an event,

Number of minutes to shun on an event,

Network Interface Name

Sensor Protected Networks

8. 『Finish』 をクリック する オプションになるまで 『Next』 をクリック して下さい。センサーはディレクターに今追加に成功します。メインメニューから、**sensor-2** はこの例に示すように、表示する。



[PIX のための設定シャニング](#)

PIX のためのシャニングを設定するためにこれらのステップを完了して下さい。

1. メインメニューでは、Security > Configure の順に選択して下さい。
2. Netranger Configuration メニューでは、**sensor-2** を強調表示し、ダブルクリックして下さい。
3. Device Management を開きます。
4. この例に示すように情報を Devices > Add の順にクリックし、入力して下さい。[OK] をクリックして続行します。Telnet およびイネーブルパスワードは両方とも「Cisco」です。

IP Address: 10.66.79.203

User Name: [empty]

Device Type: PIX

Password: *****

Sensor's NAT IP Address: [empty]

Enable Password: *****

Enable SSH

5. Shunning > Add の順にクリックして下さい。決して追加しないで下さい排除するために「アドレスの下でホスト 100.100.100.100 を」。[OK] をクリックして続行します。

General | Devices | Interfaces | Shunning

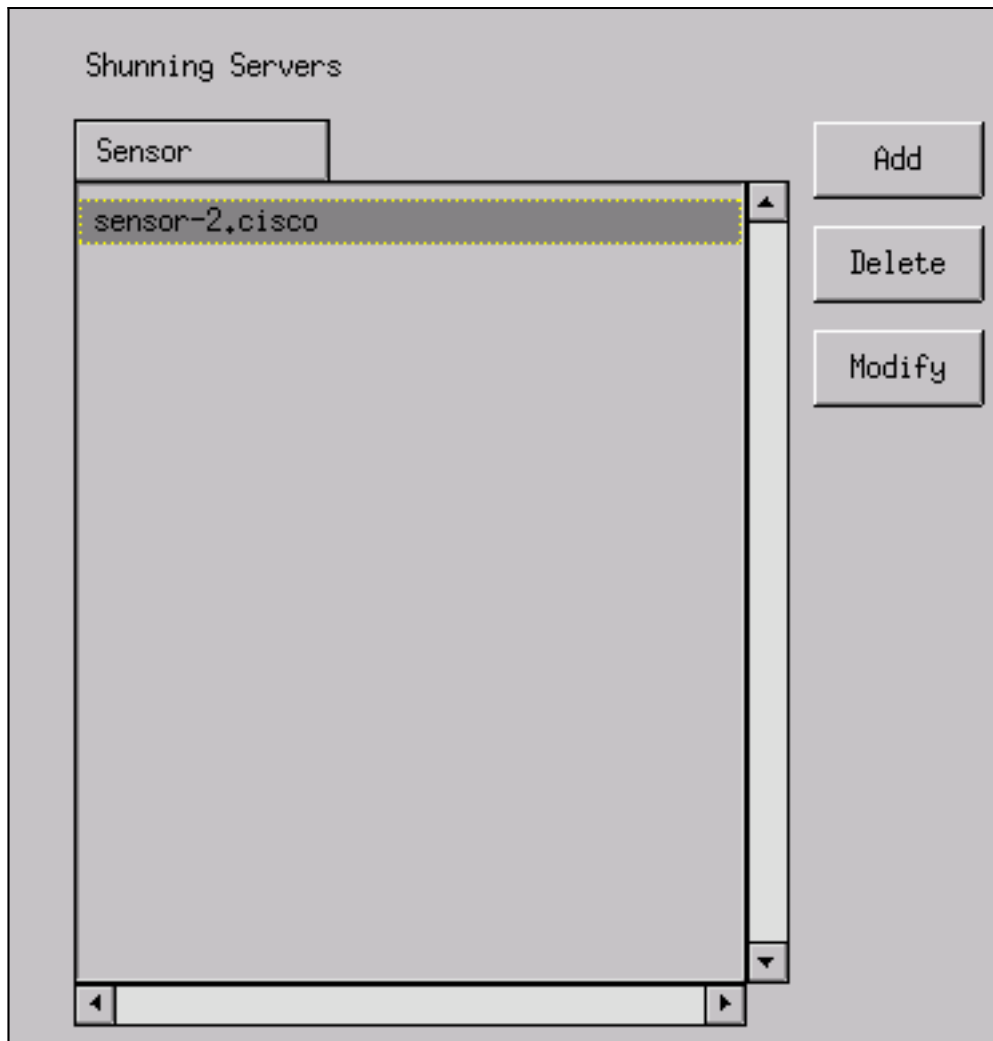
Maximum Number of Shunned Entries: 100

Addresses Never to Shun

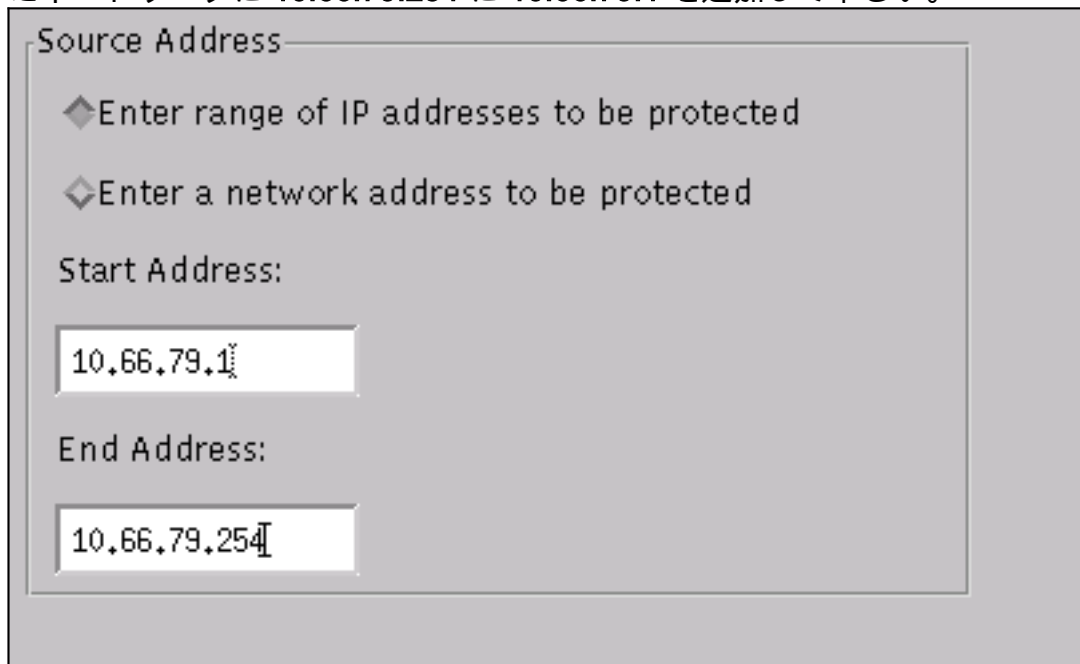
| Network Address | Network Mask |
|-----------------|-----------------|
| 100.100.100.100 | 255.255.255.255 |

Buttons: Add, Delete, Modify

6. シャニングサーバとして **sensor-2.cisco** を Shunning > Add の順にクリックし、選択して下さい。設定のこの一部は完了します。Device Management ウィンドウを閉じて下さい。



7. [Intrusion Detection] ウィンドウを開き、[Protected Networks] をクリックします。保護されたネットワークに 10.66.79.254 に 10.66.79.1 を追加して下さい。



8. 『Profile』 をクリックし、Manual Configuration > Modify Signatures の順に選択して下さい。ID 『Large ICMP Traffic』 を選択すれば: 2151 は排除し、記録することをどれもから、『Modify』 をクリックし、処理を変更します。[OK] をクリックして続行します。

| | |
|--------------------|---------------------------|
| Signature | sensor-2,cisco loggerd |
| Large ICMP traffic | 3 |
| ID | dir3,cisco smid |
| 2151 | 3 |
| Action | |
| Shun & Log | |

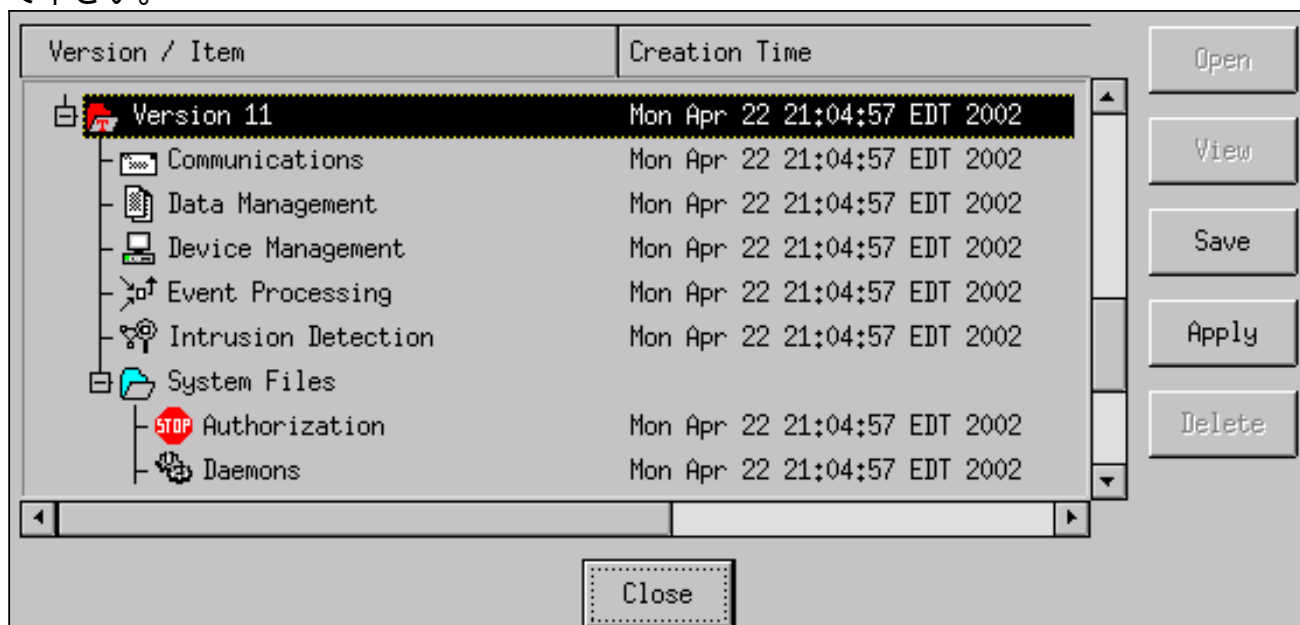
9. ID 『ICMP Flood』 を選択 すれば: 2152 は排除し、記録 することをどれもから、『Modify』 をクリックし、処理を変更します。[OK] をクリックして続行します。

| | |
|------------|---------------------------|
| Signature | sensor-2,cisco loggerd |
| ICMP Flood | 4 |
| ID | dir3,cisco smid |
| 2152 | 4 |
| Action | |
| Shun & Log | |

10. 設定のこの一部は完了しました。Intrusion Detection ウィンドウを閉じるために『OK』 をクリックして下さい。
11. システム ファイル ファイル ホルダーを開き、Daemons ウィンドウを開いて下さい。有効にしましたこれらのデーモンを確認して下さい
- :



12. 続き、ちょうど修正したバージョンを選択するために『OK』をクリックして下さい。『SAVE』をクリックして下さい>適用して下さい。センサーが終了し、サービスを再開し、Netranger 設定のためのすべてのウィンドウを閉じることを言うためにシステムを待つして下さい。



確認

このセクションは情報を提供します設定作業をきちんと確認するのを助ける。

攻撃を開始する前に

```
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
```

攻撃 および シャニングを開始して下さい

```
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
```

15分以降、それは標準にシャニングが15分に設定されるので戻ります。

```
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
```

[トラブルシューティング](#)

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

[関連情報](#)

- [Cisco IDS Director のための終りの販売](#)
- [Cisco IDS センサ ソフトウェア バージョン 3.x のための廃止](#)
- [Cisco 侵入防御システム製品のサポート](#)
- [Cisco PIX Firewall ソフトウェア製品サポート](#)
- [Cisco Secure PIX ファイアウォール コマンド リファレンス](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)