Shunning IDS PIX avec Cisco IDS UNIX Director

Contenu

Introduction

Ce document décrit comment configurer l'évitement sur un PIX à l'aide du Directeur Cisco IDS Unix (autrefois connu sous le nom de directeur de Netranger) et du capteur. Ce document suppose que le capteur et le directeur sont opérationnels et l'interface de reniflement du capteur est installée pour la répartir au PIX en dehors de l'interface.

Conditions préalables

Conditions requises

Aucune condition préalable spécifique n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur les versions de logiciel et matériel suivantes :

- Directeur Cisco IDS Unix 2.2.3
- Capteur 3.0.5 des ID UNIX de Cisco
- PIX Cisco Secure avec 6.1.1**Remarque:** Si vous utilisez la version 6.2.x, vous pouvez utiliser la Gestion de Secure Shell Protocol (SSH), mais pas le telnet. Référez-vous à l'ID de bogue

Cisco CSCdx55215 (clients enregistrés seulement) pour de plus amples informations.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Configurer

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

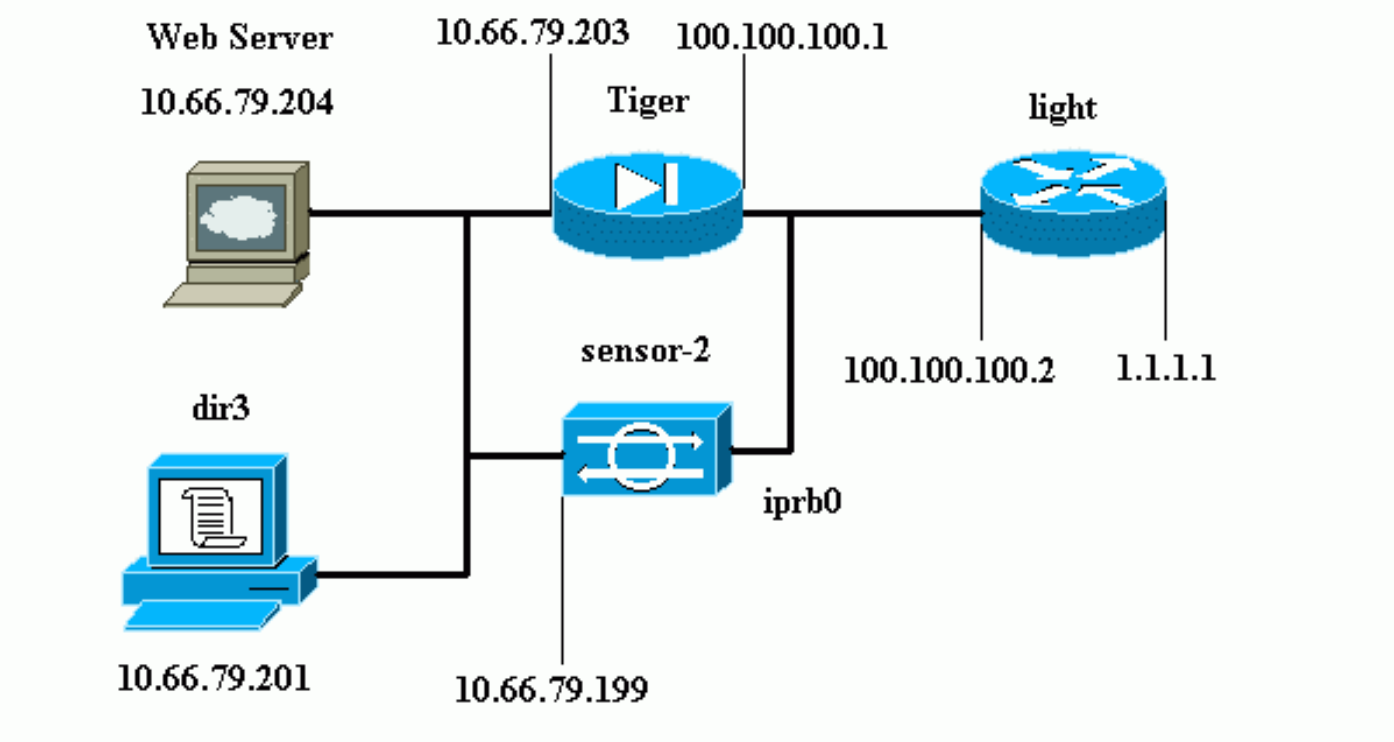
Le Directeur Cisco IDS Unix et le capteur sont utilisés afin de gérer un PIX Cisco Secure pour l'évitement. Quand vous considérez cette configuration, souvenez-vous ces concepts :

- Installez le capteur et assurez-vous les travaux de capteur correctement.
- Assurez-vous que les envergures d'interface de reniflement à l'interface extérieure du PIX.

Remarque: Afin de trouver les informations complémentaires sur les commandes utilisées dans ce document, référez-vous au Command Lookup Tool (clients enregistrés seulement).

Diagramme du réseau

Ce document utilise cette configuration du réseau.



Configurations

Ce document utilise les configurations suivantes.

- Lumière du routeur
- PIX Tiger

Lumière du routeur

```
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
```

Configurez le capteur

Ces étapes décrivent comment configurer le capteur.

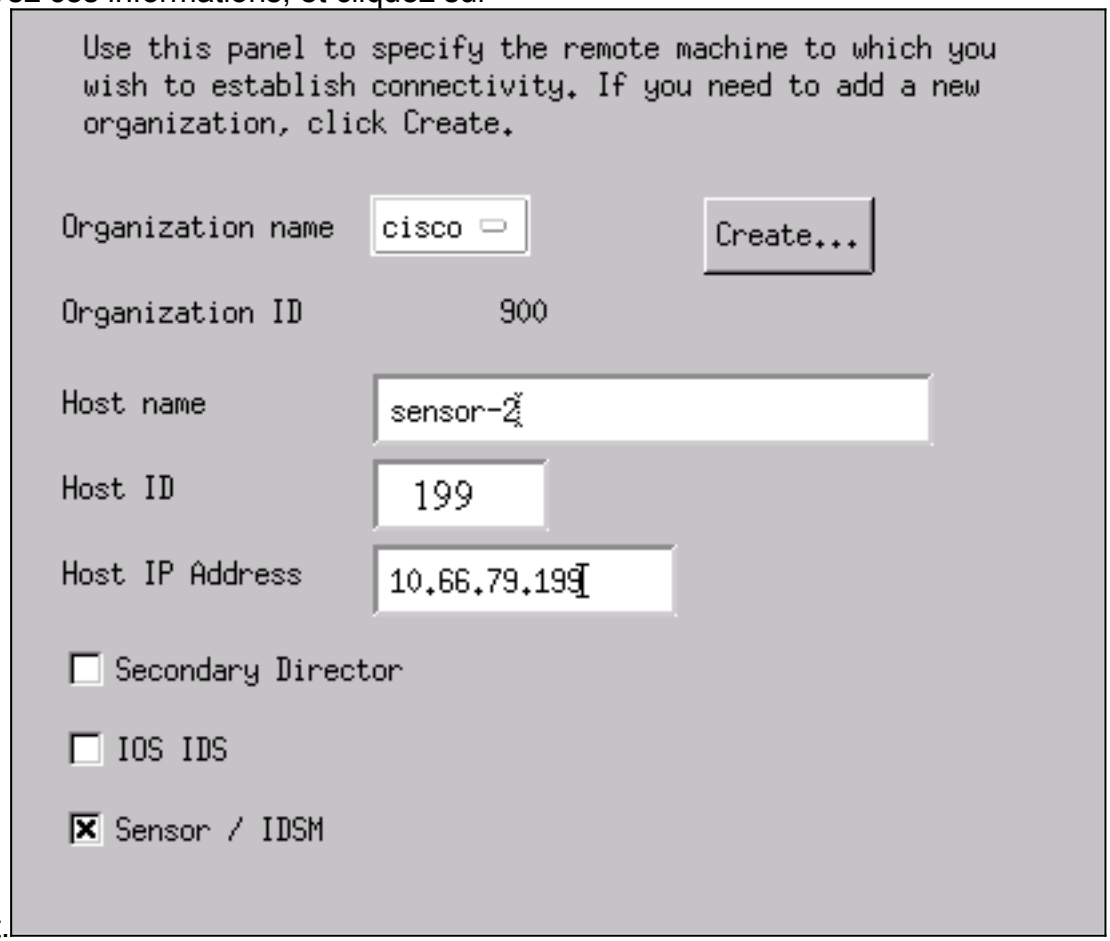
1. Telnet à **10.66.79.199** avec la **racine de** nom d'utilisateur et l'**attaque de** mot de passe.
2. Entrez dans le sysconfig-**capteur**.
3. Entrez les informations suivantes :Adresse IP : **10.66.79.199**Masque de réseau IP : **255.255.255.224**Nom d'hôte IP : **sensor-2**Default route : **10.66.79.193**Contrôle d'accès au réseau**10.**Infrastructure de communicationsID d'hôte de capteur : **49**ID d'organisation de capteur : **900**Nom d'hôte de capteur : **sensor-2**Nom d'organisation de capteur : **Cisco**Adresse IP de capteur : **10.66.79.199**ID d'hôte de gestionnaire d'ID : **50**ID d'organisation de gestionnaire d'ID : **900**Nom d'hôte de gestionnaire d'ID : **dir3**Nom d'organisation de gestionnaire d'ID : **Cisco**Adresse IP de gestionnaire d'ID : **10.66.79.201**
4. Enregistrez la configuration. Les réinitialisations de capteur puis.

Ajoutez le capteur dans le directeur

Terminez-vous ces étapes afin d'ajouter le capteur dans le directeur.

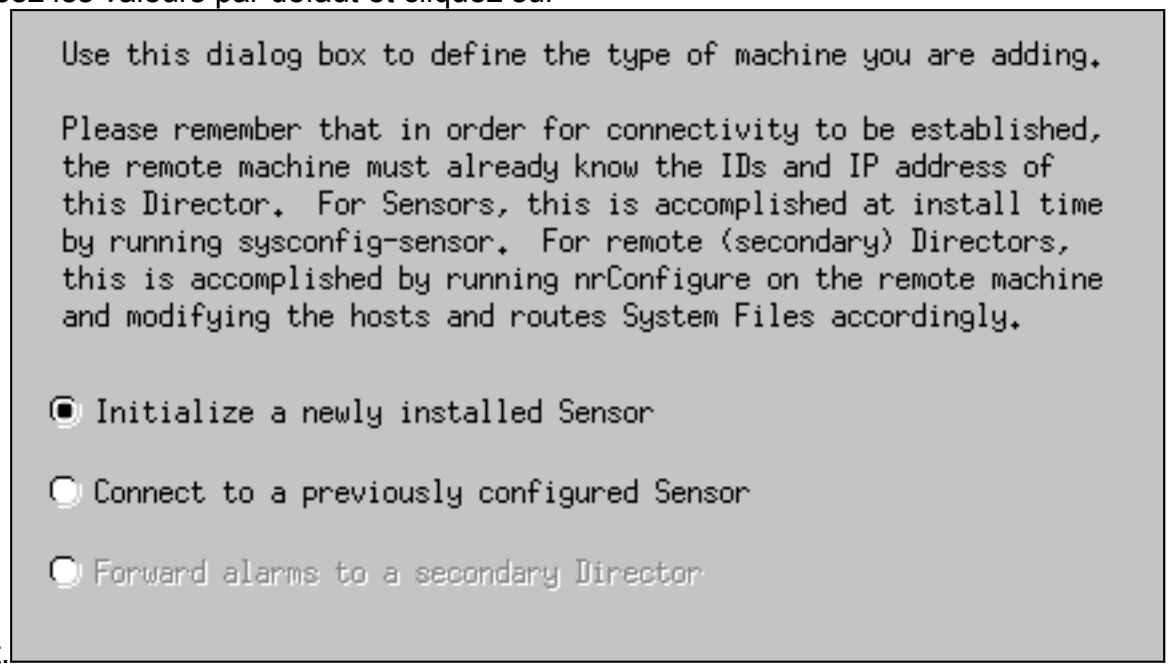
1. Telnet à **10.66.79.201** avec le **netrangr de** nom d'utilisateur et l'**attaque de** mot de passe.
2. Écrivez l'**ovw&** afin de lancer le HP OpenView.

3. Dans le menu principal, **Security > Configure** choisi.
4. Dans le menu de configuration de Netranger, le **fichier** choisi **> ajoutent l'hôte**, et cliquent sur Next.
5. Écrivez ces informations, et cliquez sur



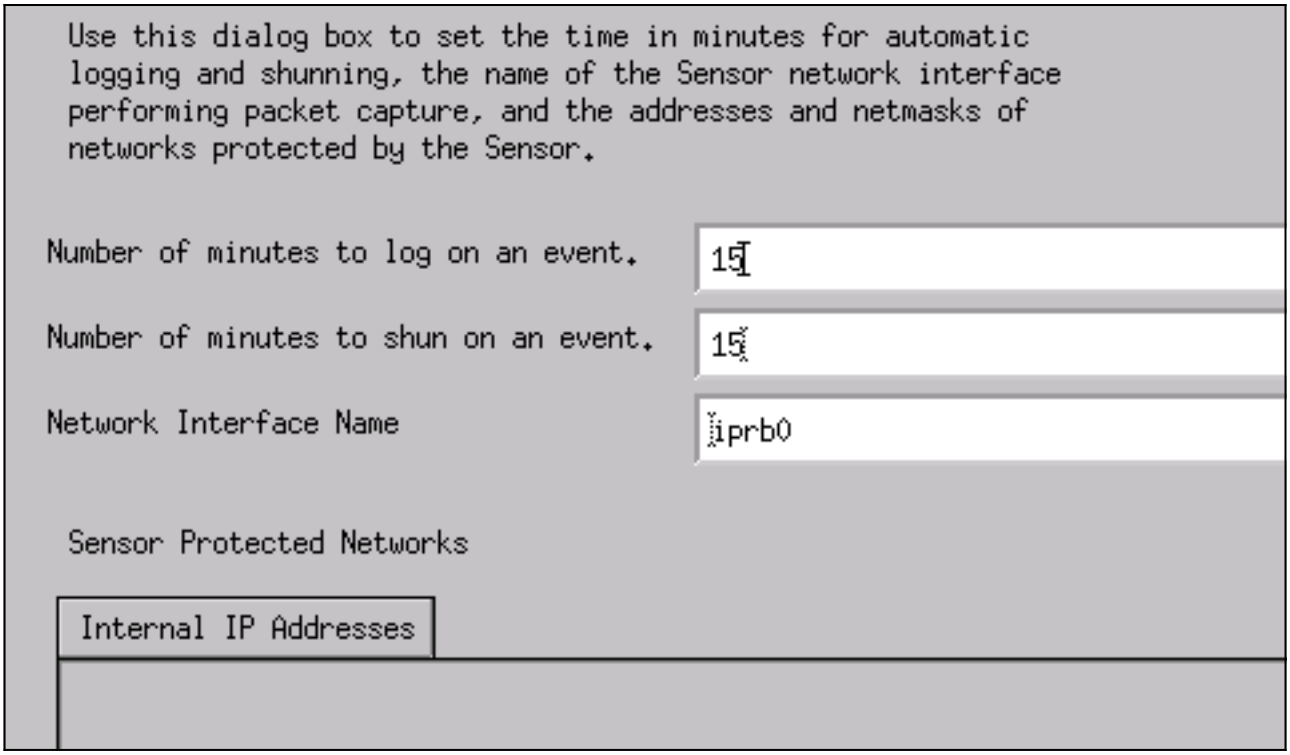
Next.

6. Laissez les valeurs par défaut et cliquez sur

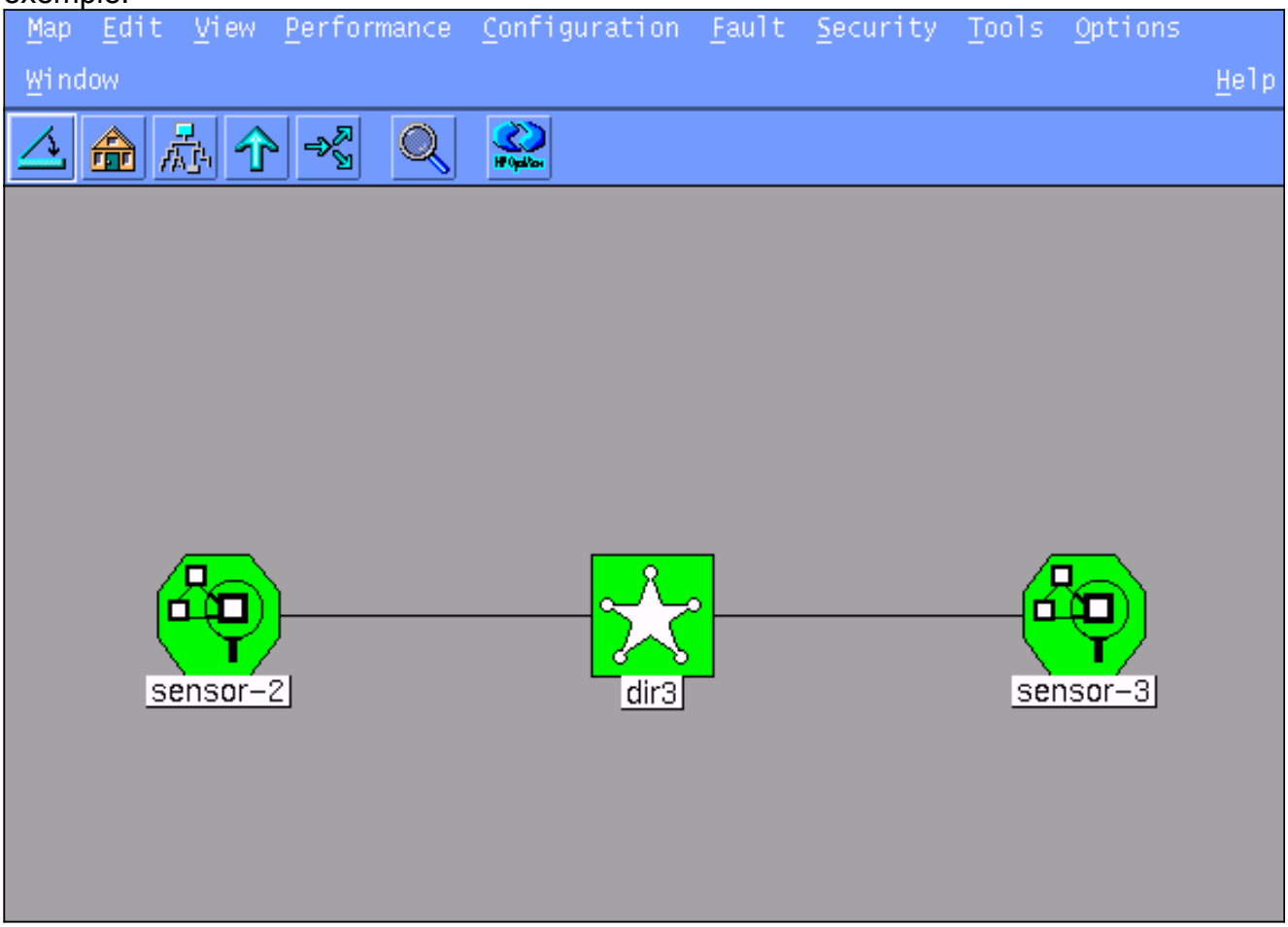


Next.

7. Changez le log et évitez les minutes ou laissez-les comme par défaut si les valeurs sont acceptables. Changez le nom d'interface réseau au nom de votre interface de reniflement. Dans cet exemple, il est "iprb0". Il peut être "spwr0" ou toute autre chose basé sur le type de capteur et comment vous connectez le
capteur.



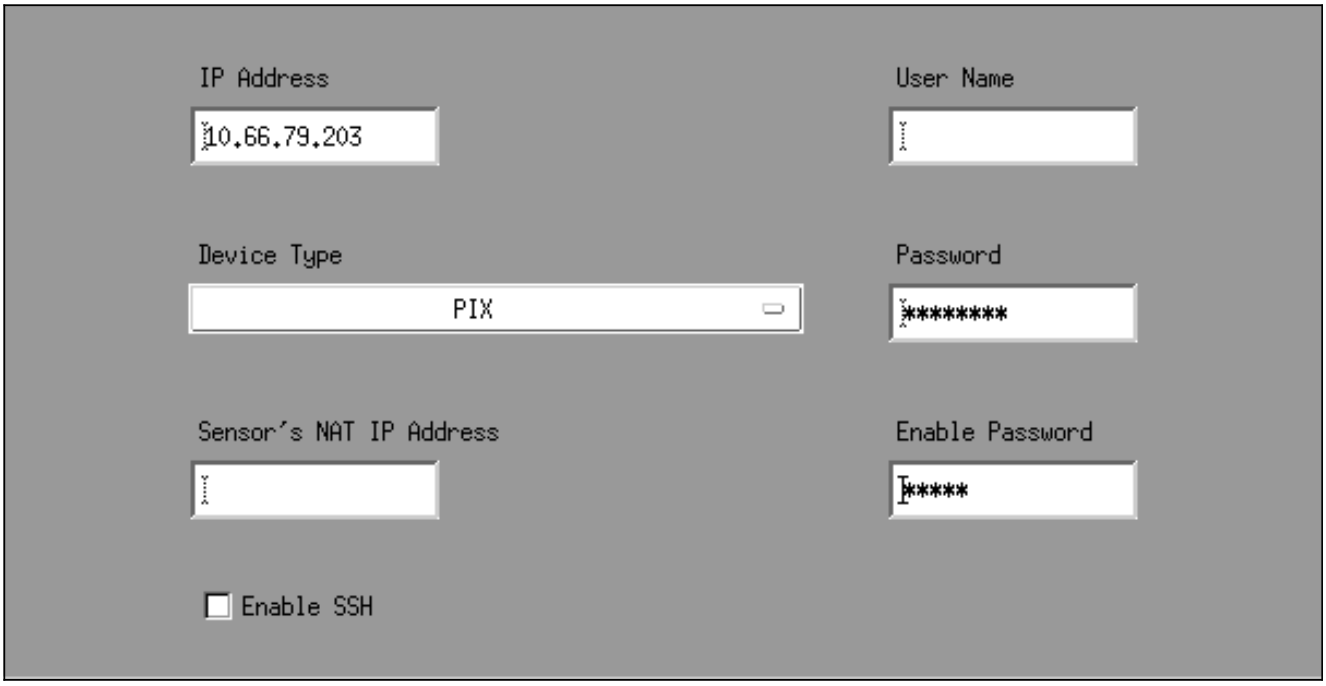
8. Cliquez sur Next jusqu'à ce qu'il y ait une option de cliquer sur Finish.Le capteur est maintenant avec succès ajouté dans le directeur. Du menu principal, **sensor-2** est affiché, suivant les indications de cet
exemple.



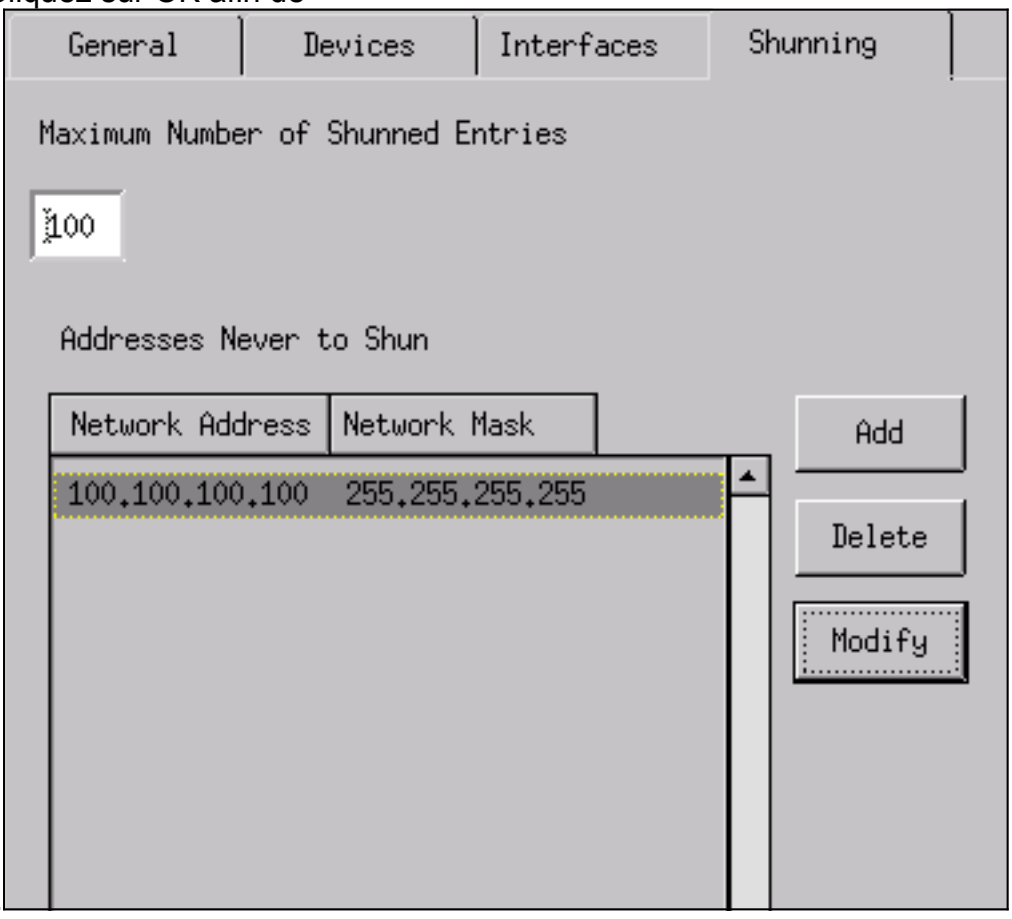
Configurez l'évitement pour PIX

Terminez-vous ces étapes afin de configurer l'évitement pour PIX.

1. Dans le menu principal, **Security > Configure** choisi.
2. Dans le menu de configuration de Netranger, mettez en valeur **sensor-2** et double-cliquer-le.
3. Ouvrez la **Gestion de périphériques**.
4. Cliquez sur les **périphériques > ajoutent** et écrivent les informations suivant les indications de cet exemple. Cliquez sur OK afin de continuer. Le telnet et le mot de passe d'enable sont les deux
« Cisco ».

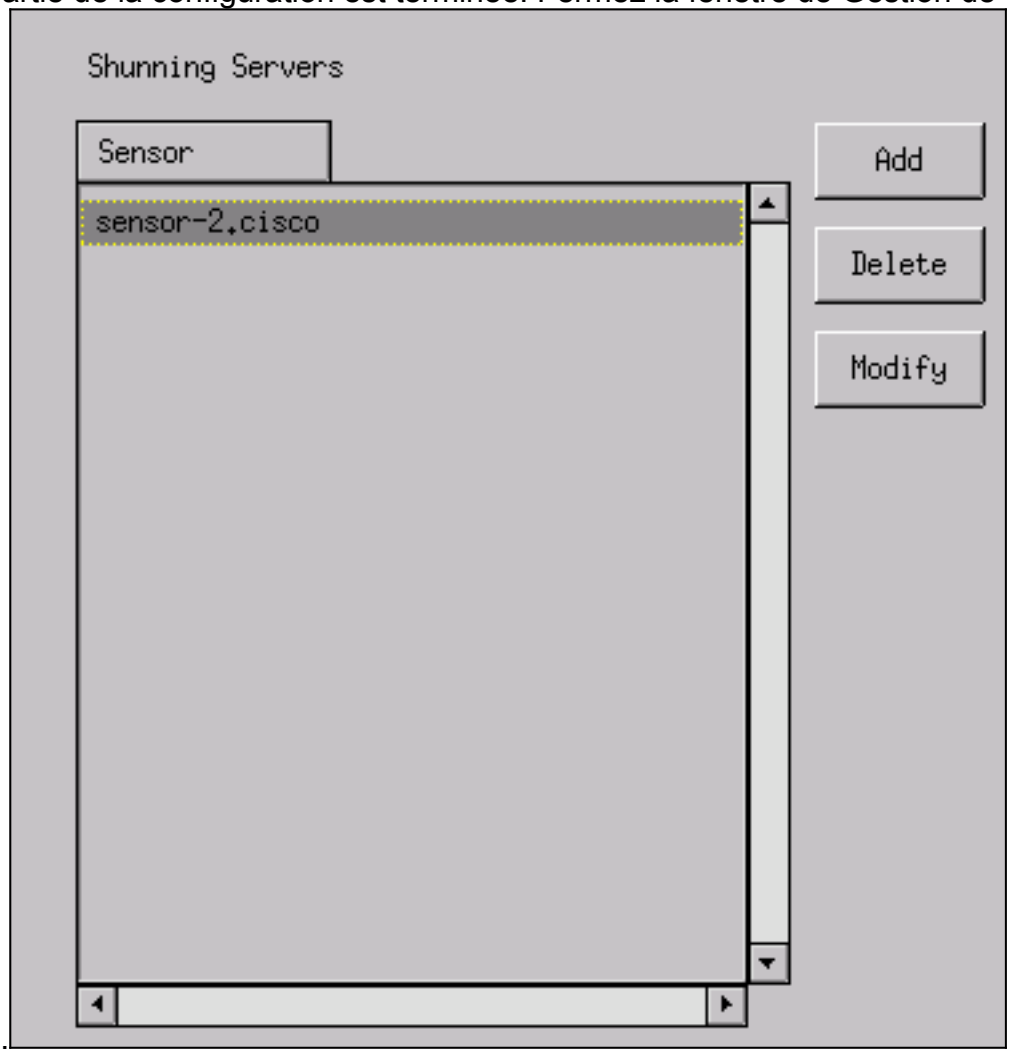


5. Le clic **évitant > ajoutent**. N'ajoutez jamais l'hôte **100.100.100.100** sous des « adresses pour éviter. » Cliquez sur OK afin de continuer.



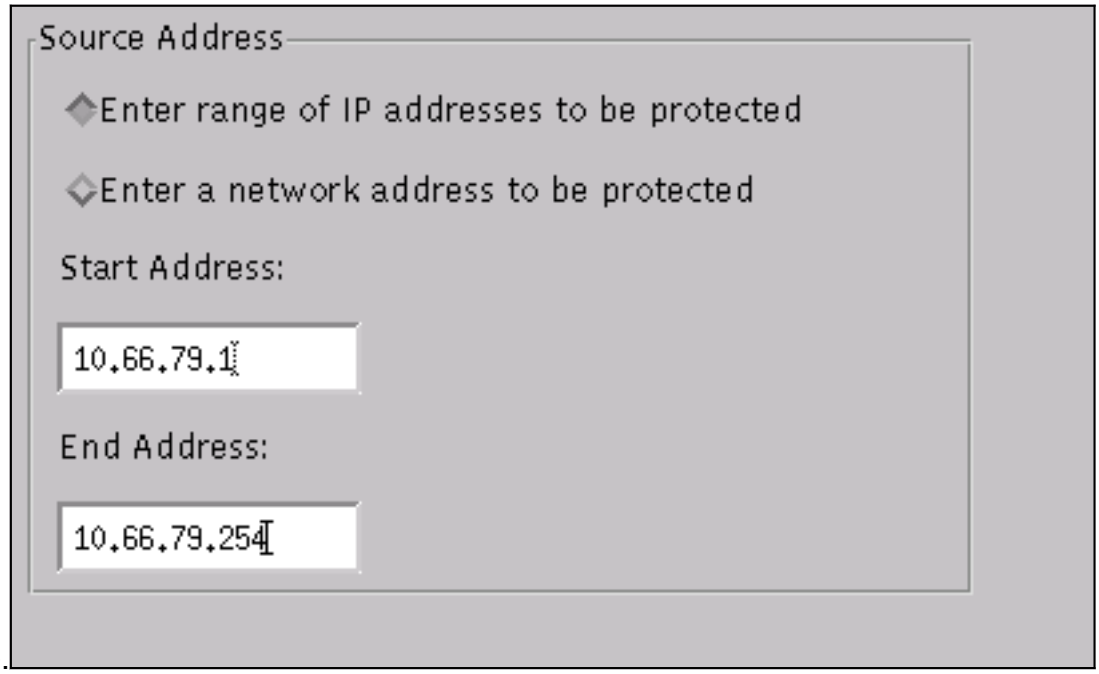
6. Le clic **évitant > ajoutent** et sélectionnent **sensor-2.cisco** en tant que serveurs de évitement.

La présente partie de la configuration est terminée. Fermez la fenêtre de Gestion de



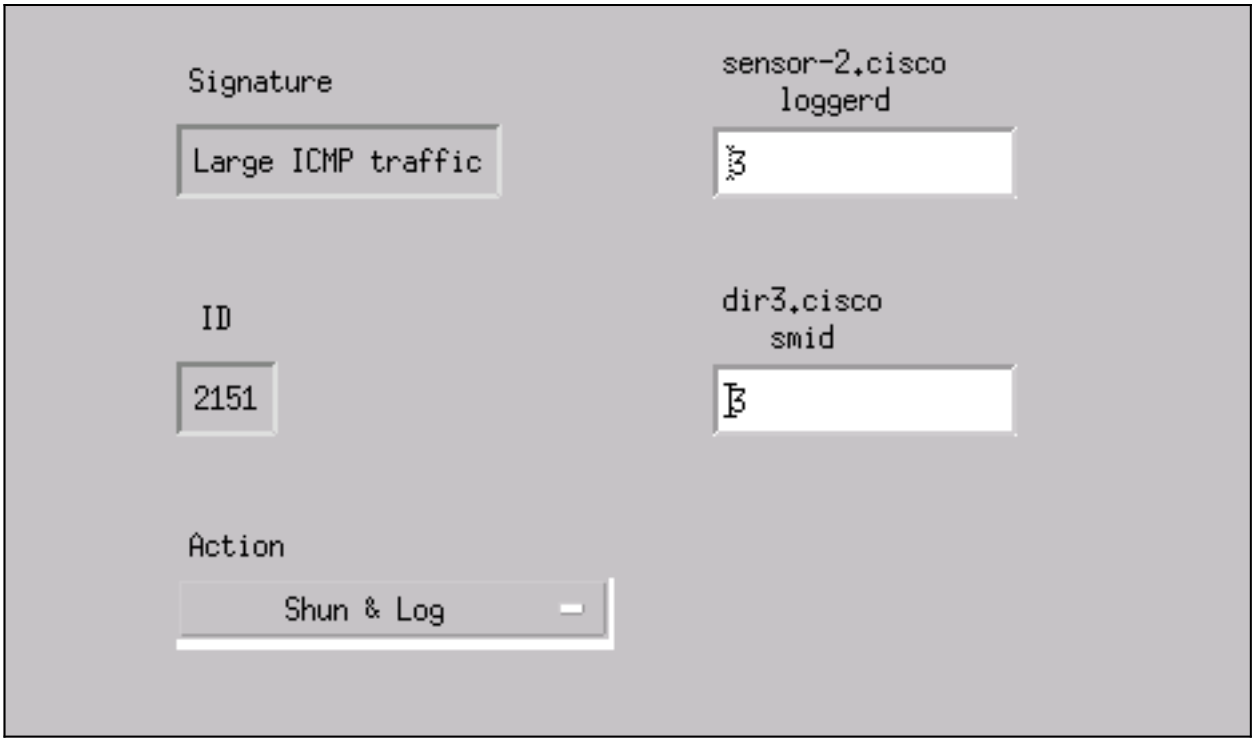
périphériques.

7. Ouvrez la fenêtre de détection d'intrusion et cliquez sur les **réseaux protégés**. Ajoutez **10.66.79.1 à 10.66.79.254** dans le réseau

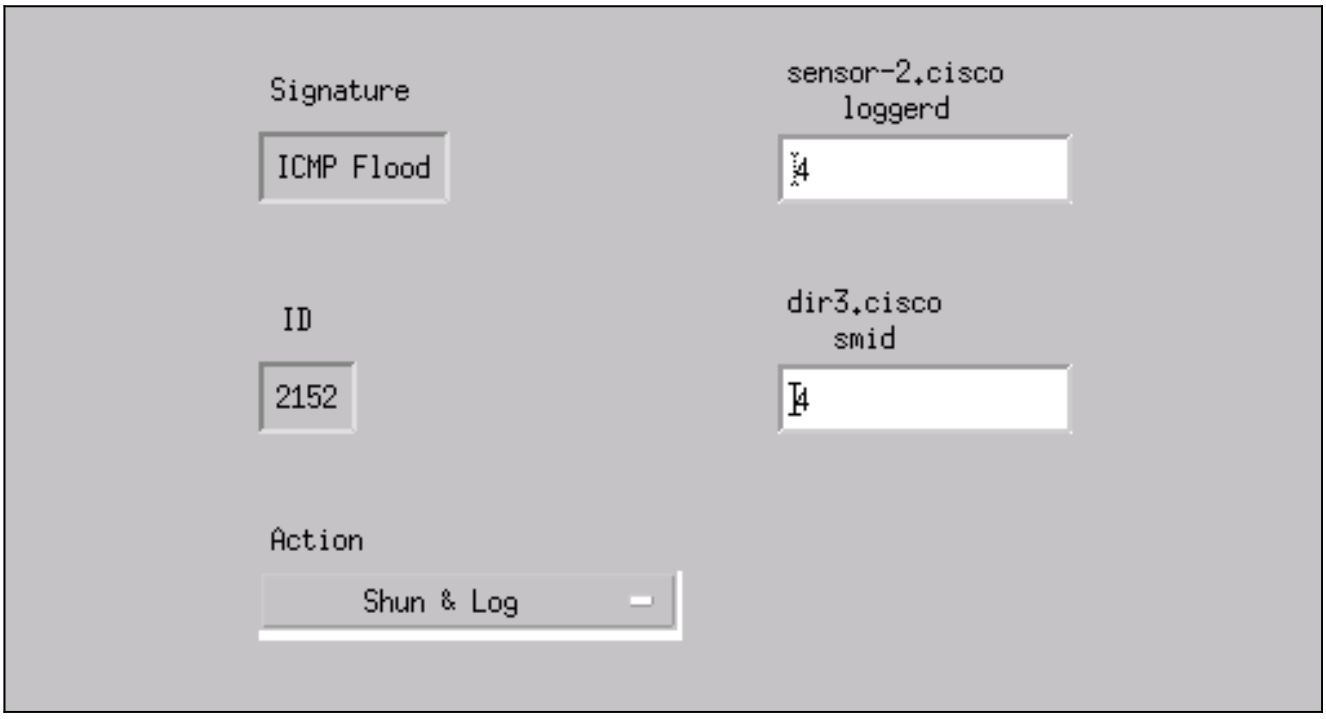


protégé.

8. **Le profil de** clic et la **configuration manuelle** choisie **> modifient des signatures**. Sélectionnez le **grands trafic** et **ID d'ICMP : 2151**, clic **modifient**, et changent l'action d'aucun **éviter et se connecter**. Cliquez sur OK afin de continuer.

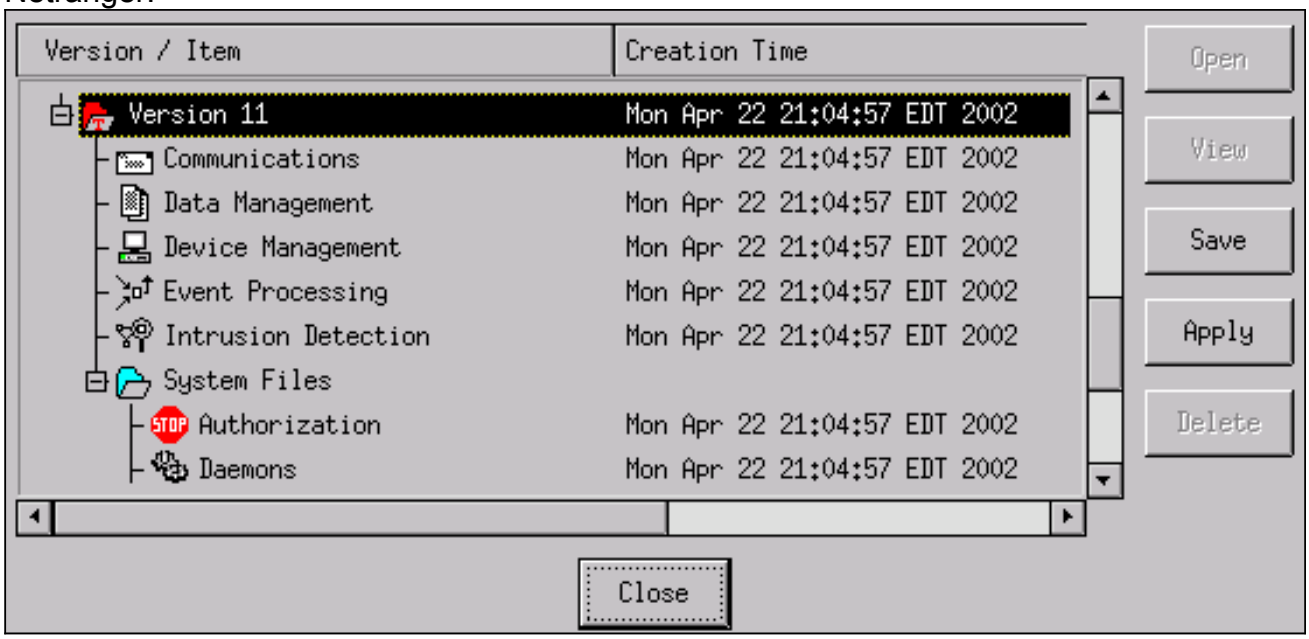


9. **Inondation** choisie et **ID d'ICMP : 2152**, clic **modifient**, et changent l'action d'**aucun éviter et se connecter**. Cliquez sur OK afin de continuer.



10. La présente partie de configuration est complète. Cliquez sur OK afin de fermer la fenêtre de détection d'intrusion.
11. Ouvrez le répertoire de **fichiers système** et ouvrez la fenêtre de **démons**. Assurez que vous avez activé ces démons :

12. Cliquez sur OK afin de continuer, et sélectionner la version que vous avez juste modifiée. **La sauvegarde de** clic > **s'appliquent**. Attendez le système pour vous dire que le capteur est de finition, redémarre des services, et ferme toutes les fenêtres pour la configuration de Netranger.



Vérifier

Cette section fournit les informations qui vous aident à confirmer vos travaux de configuration correctement.

Avant que vous lanciez l'attaque

```
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
```

Lancez l'attaque et l'évitement

```
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
```

Quinze minutes plus tard, il retourne à la normale parce que l'évitement est placé à quinze minutes.

```
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
```

Dépanner

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Fin de commercialisation pour l'IDS Director de Cisco
- Fin de vie pour la version de logiciel 3.x de capteur d'ID de Cisco
- Support produit de Système de protection contre les intrusions Cisco
- Support produit de Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Support et documentation techniques - Cisco Systems