Configuration du shunning sur UNIX Director

Contenu

Introduction

Le directeur et le capteur de Detection System de Cisco Intrusion (ID) peuvent être utilisés pour gérer un routeur de Cisco pour l'évitement. Dans ce document, un senseur (sensor-2) est configuré afin de détecter des attaques sur le routeur « Chambre » et afin de communiquer ces informations au directeur "dir3." une fois configuré, une attaque est lancé (le ping de plus en grande partie que 1024 octets, qui est la signature 2151, et d'une inondation d'Internet Control Message Protocol [ICMP], qui est la signature 2152) du routeur la « lumière. » Le senseur détecte l'attaque et communique ceci au directeur. Une liste de contrôle d'accès (ACL) est téléchargée au routeur pour éviter le trafic de l'attaquant. Sur l'attaquant l'`inaccessible d'hôte` est affiché, et sur la victime l'ACL téléchargé est affiché.

Conditions préalables

Conditions requises

Assurez-vous de répondre à ces exigences avant d'essayer cette configuration :

- Installez le capteur et assurez-vous que cela fonctionne correctement.
- Assurez-vous que les envergures d'interface de reniflement au routeur en dehors de l'interface.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

- IDS Director 2.2.3 de Cisco
- Capteur 3.0.5 d'ID de Cisco
- Routeur de Cisco IOS® avec 12.2.6

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.

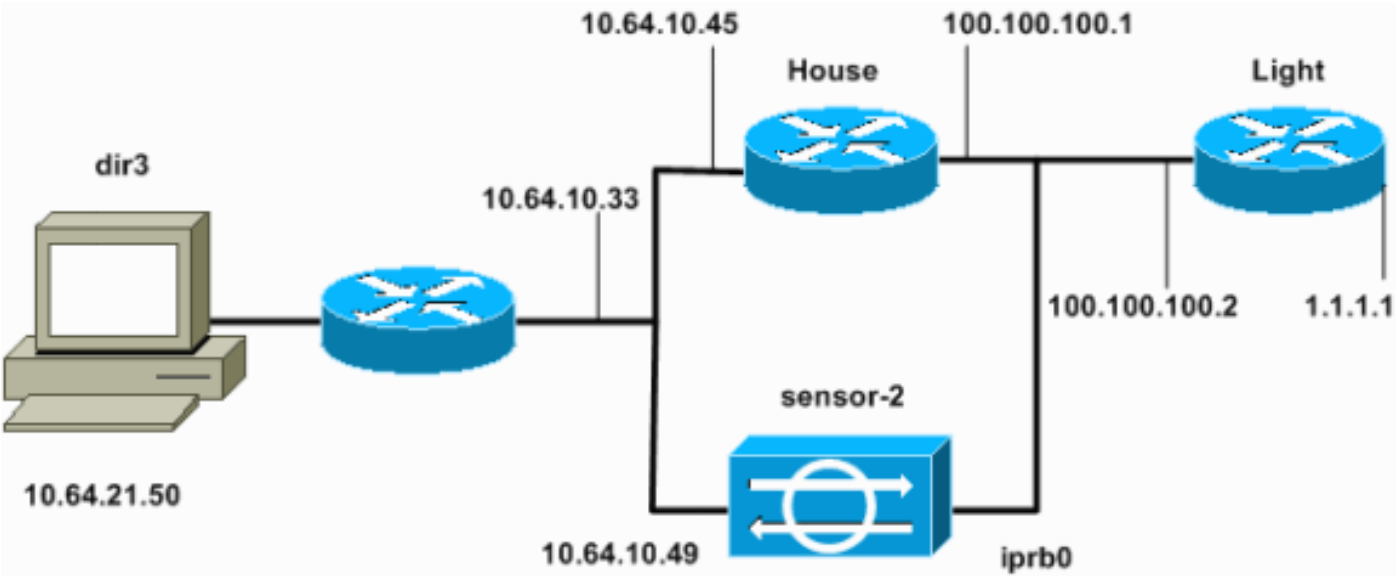
Configurer

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

Remarque: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commande (clients enregistrés seulement).

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant.



Configurations

Ce document utilise les configurations suivantes.

- Lumière du routeur
- Routeur House

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
!
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
```

Routeur House

```
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#
```

Configurez le capteur

Terminez-vous ces étapes pour configurer le capteur.

1. Telnet à **10.64.10.49** avec la **racine de** nom d'utilisateur et l'**attaque de** mot de passe.
2. Entrez dans le sysconfig-**capteur**.
3. Une fois incité, écrivez les informations de configuration, suivant les indications de cet exemple.

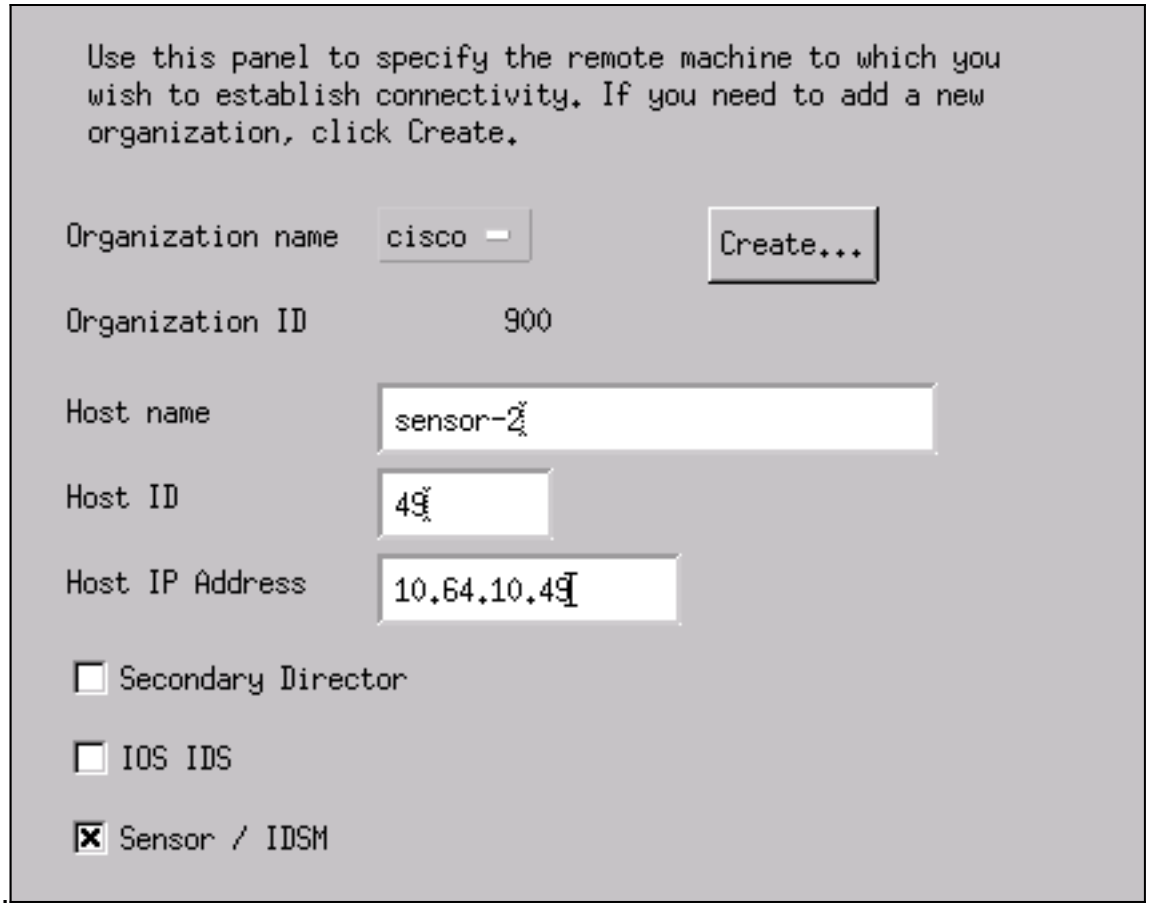
```
1 - IP Address: 10.64.10.49
2 - IP Netmask: 255.255.255.224
3 - IP Host Name:  sensor-2
4 - Default Route     10.64.10.33
5 - Network Access Control
         64.
         10.
6 - Communications Infrastructure
Sensor Host ID: 49
Sensor Organization ID:     900
Sensor Host Name: sensor-2
Sensor Organization 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. Une fois incité, sauvegardez la configuration et permettez au capteur pour redémarrer.

Ajoutez le capteur dans le directeur

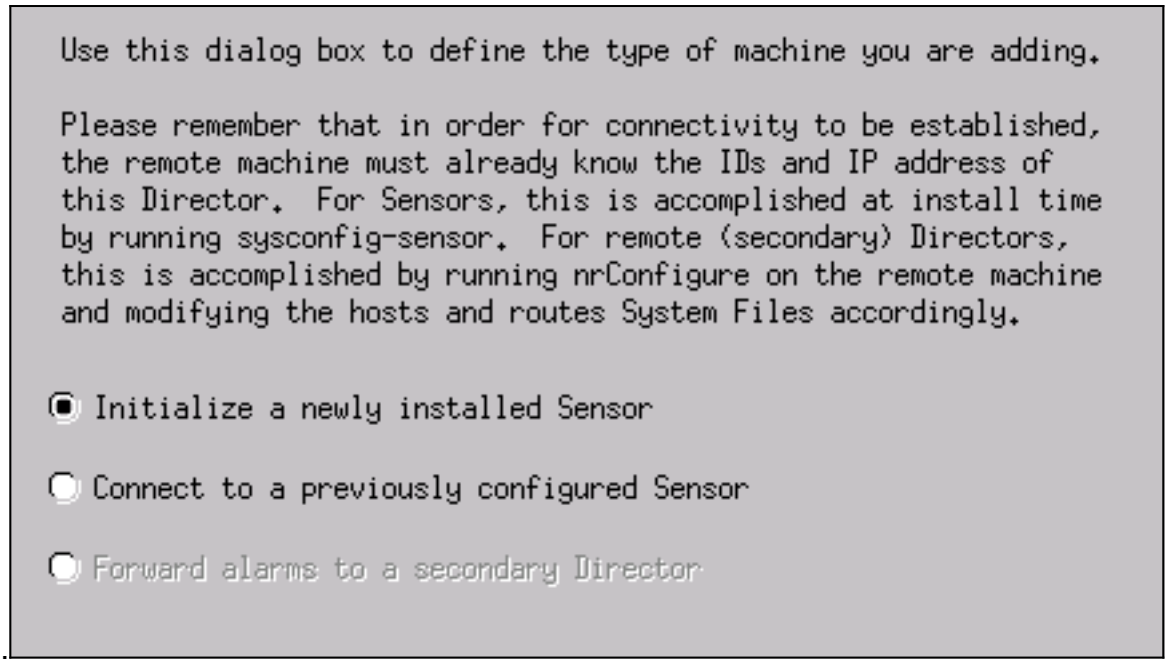
Terminez-vous ces étapes pour ajouter le capteur dans le directeur.

1. Telnet à **10.64.21.50** avec le **netrangr de** nom d'utilisateur et l'**attaque de** mot de passe.
2. Écrivez l'**ovw&** pour lancer le HP OpenView.
3. Dans le menu principal, **Security > Configure** choisi.
4. Dans l'utilitaire de gestion de fichier de configuration, le **fichier** choisi **> ajoutent l'hôte**, et cliquent sur Next.
5. C'est un exemple de la façon compléter les informations



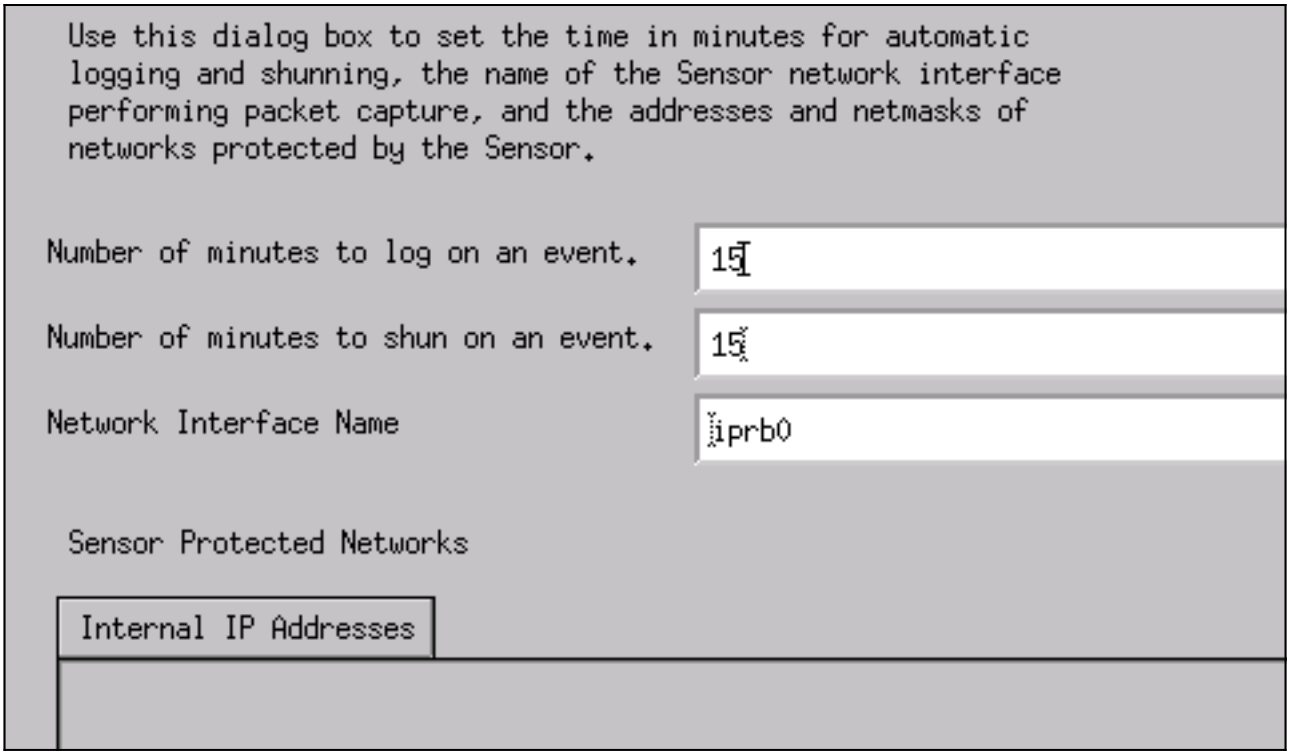
demandées.

6. Recevez la valeur par défaut pour le type d'ordinateur, et cliquez sur Next, suivant les indications de cet

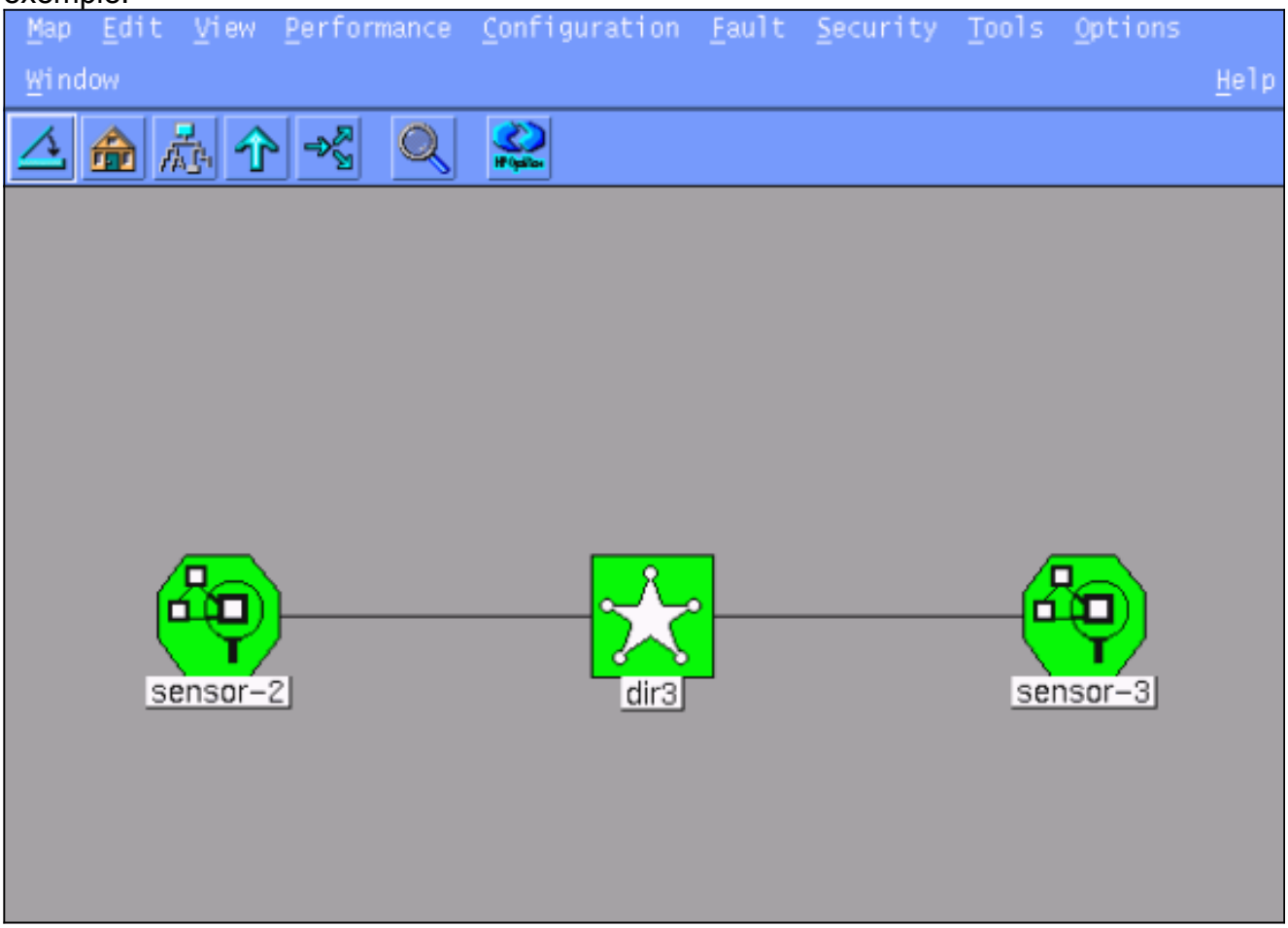


exemple.

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." qu'il peut être "spwr0" ou toute autre chose selon le type de capteur et comment vous connectez votre capteur.



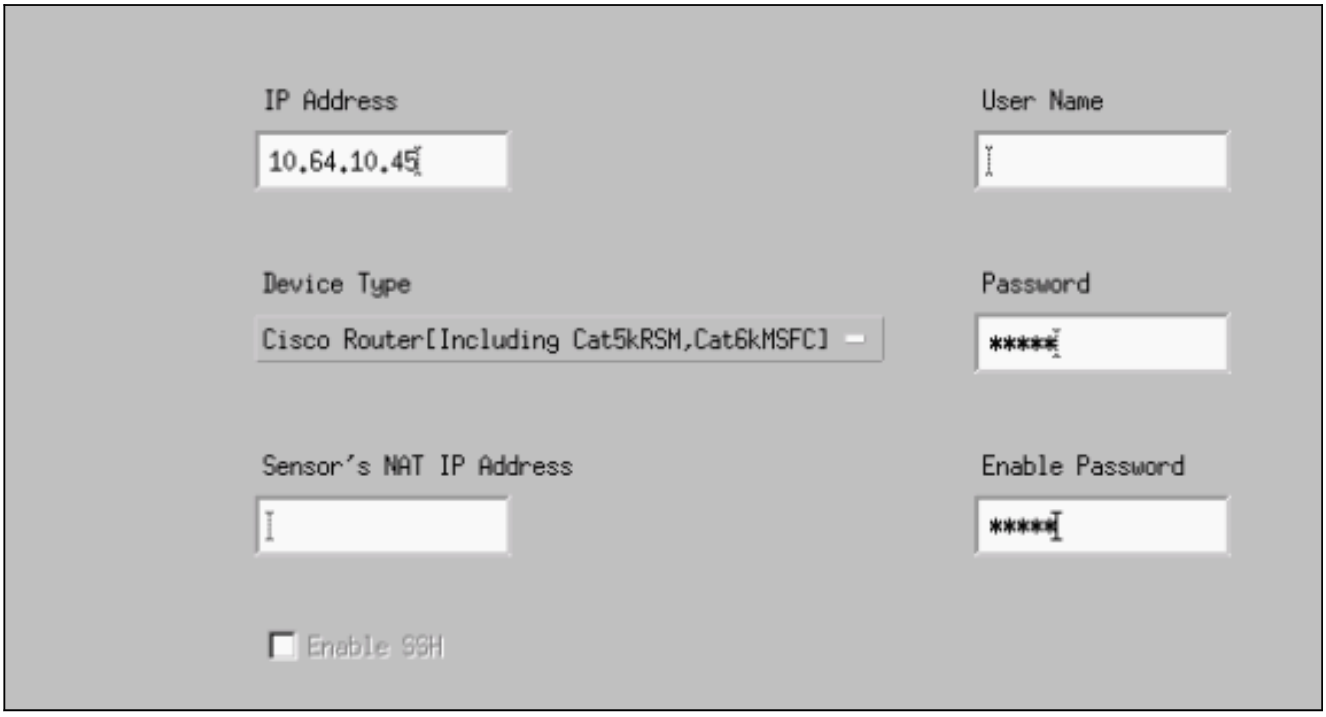
8. Cliquez sur Next jusqu'à ce qu'il y ait une option de cliquer sur Finish.Vous avez avec succès ajouté le capteur dans le directeur. Du menu principal, vous devriez voir `sensor-2`, comme indiqué dans cet
exemple.



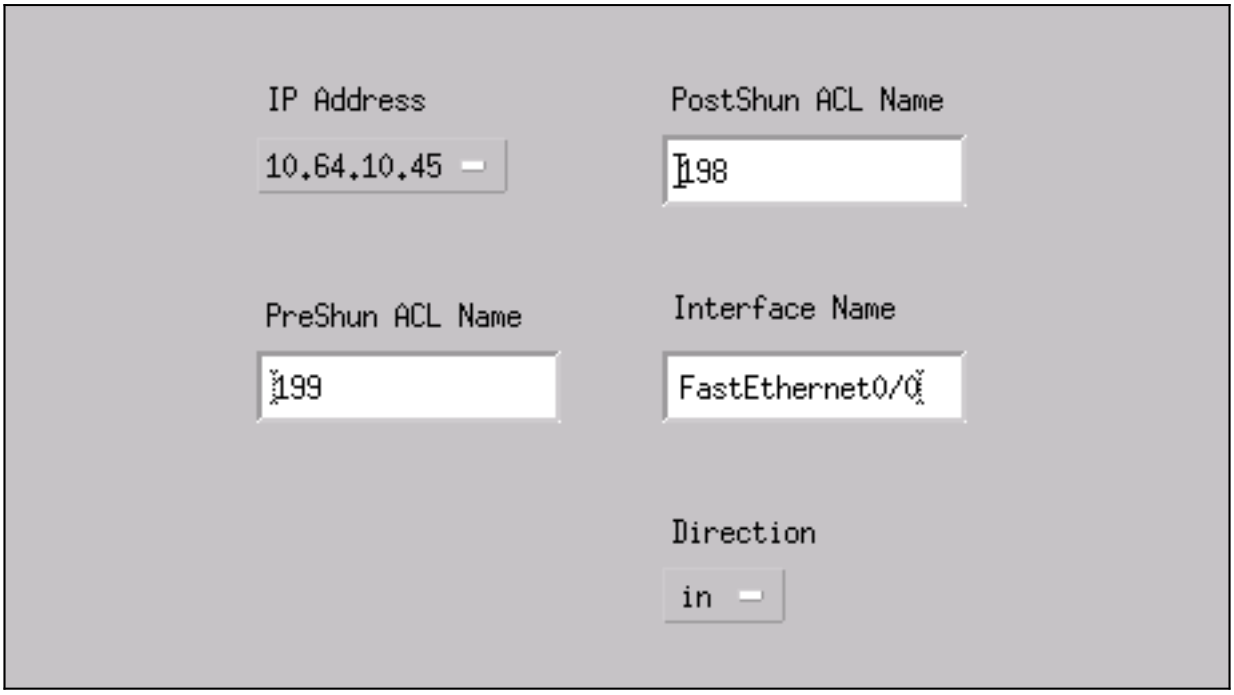
Configurez l'évitement pour le routeur Cisco IOS

Terminez-vous ces étapes pour configurer l'évitement pour le routeur Cisco IOS.

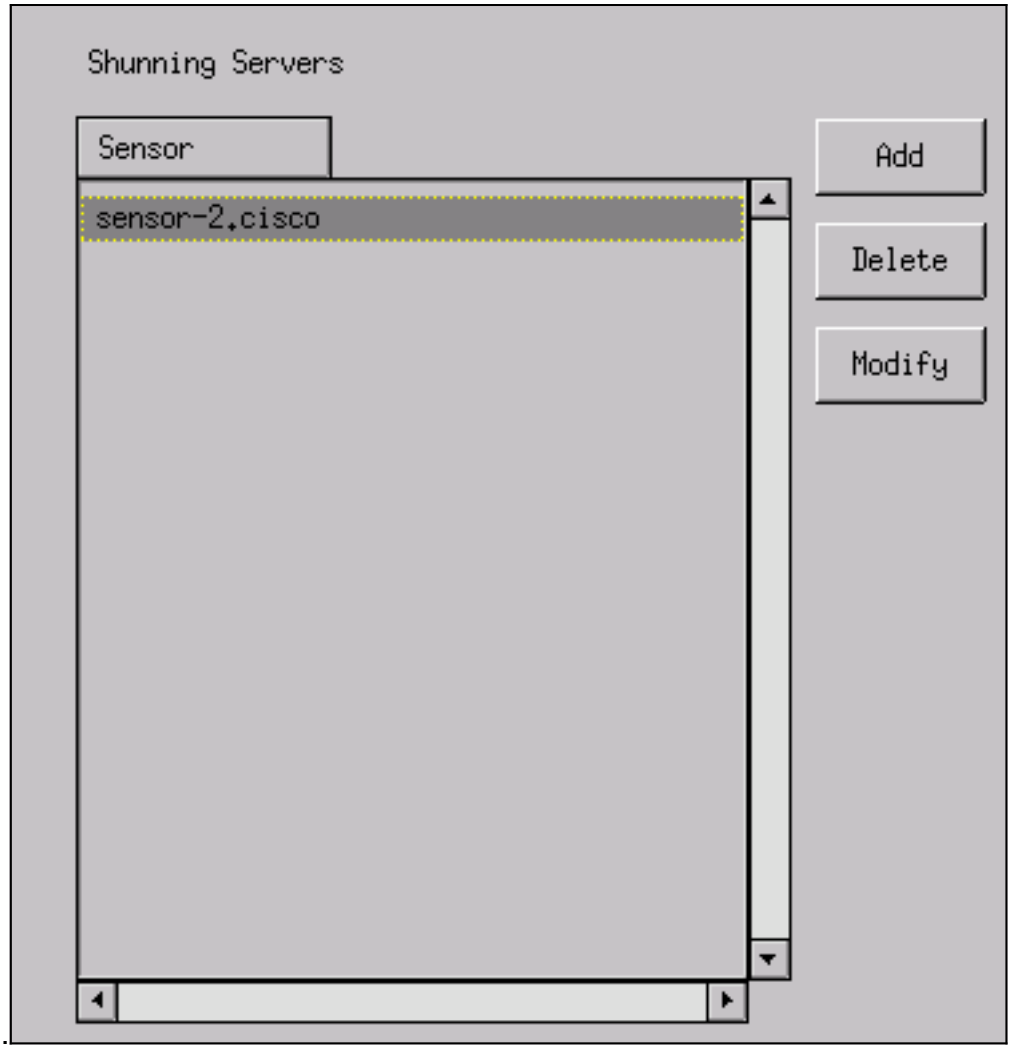
1. Dans le menu principal, **Security > Configure** choisi.
2. Dans l'utilitaire de gestion de fichier de configuration, mettez en valeur **sensor-2** et double-cliquer-le.
3. Ouvrez la **Gestion de périphériques**.
4. Cliquez sur les **périphériques > ajoutent**, et écrivent les informations suivant les indications de cet exemple. Cliquez sur **OK** pour continuer.La correspondance de mots de passe de telnet et d'enable ce qui est dans le routeur la « Chambre. »



5. Cliquez sur les **interfaces > ajoutent**, écrivent ces informations, et cliquent sur OK pour continuer.

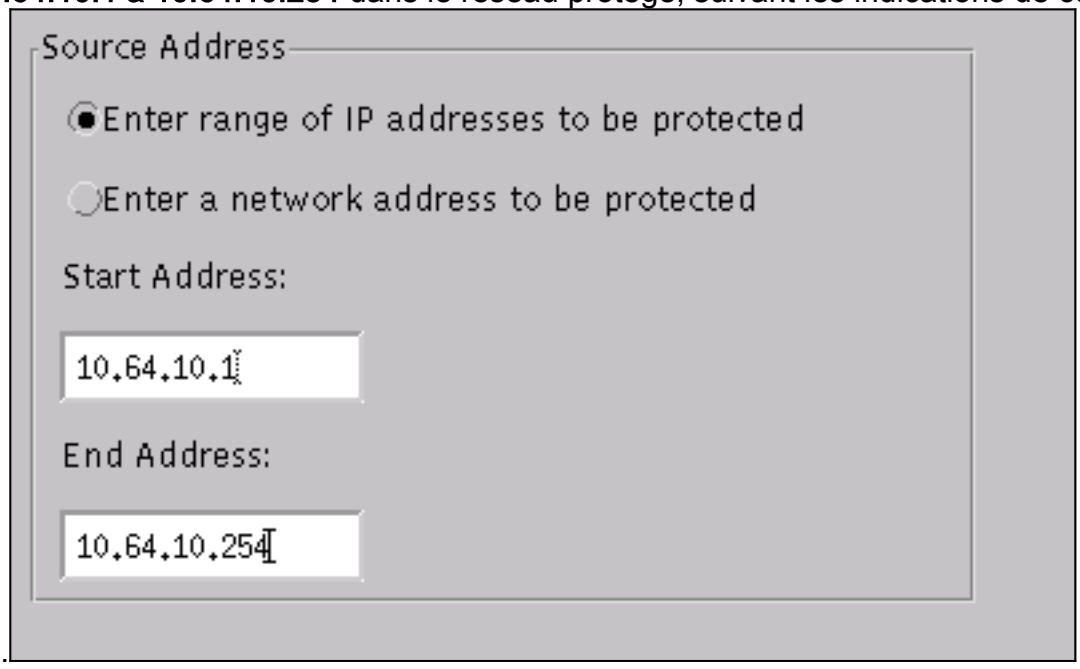


6. Le clic **évitant > ajoutent** et sélectionnent **sensor-2.cisco** en tant que serveur de évitement. Fermez la fenêtre de Gestion de périphériques quand vous êtes de



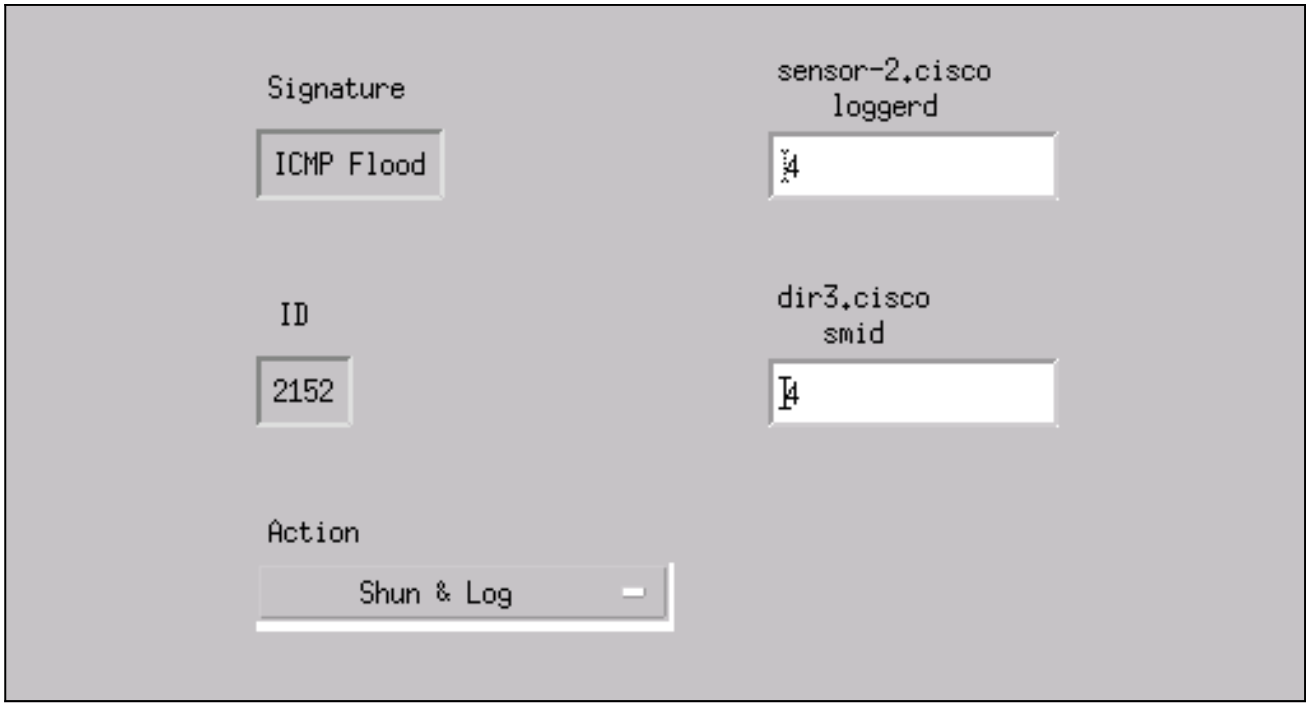
finition.

7. Ouvrez la fenêtre de détection d'intrusion, et cliquez sur les **réseaux protégés**. Ajoutez la plage **10.64.10.1 à 10.64.10.254** dans le réseau protégé, suivant les indications de cet

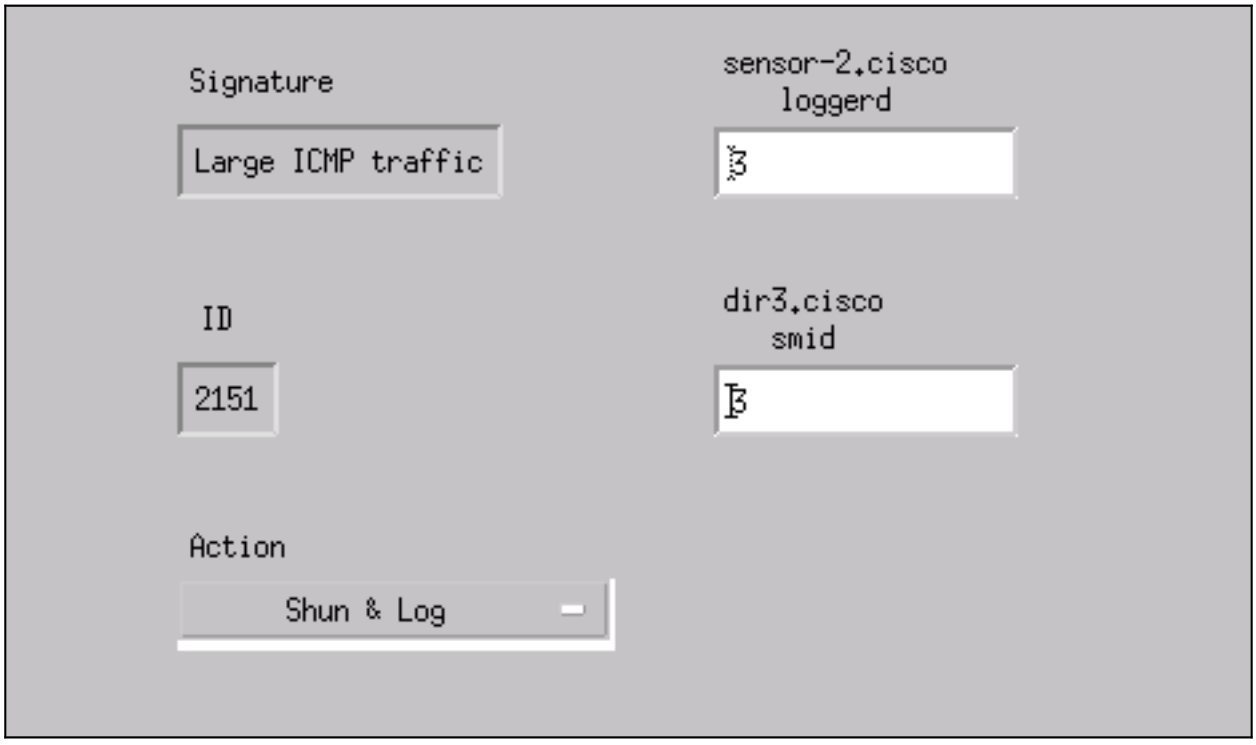


exemple.

8. **Profil > configuration manuelle de** clic.
9. Choisi **modifiez les signatures > le grand trafic d'ICMP** avec un ID de **2151**.
10. Le clic **modifient**, changent l'**action d'**aucun **éviter et se connecter**, et cliquent sur OK pour continuer.

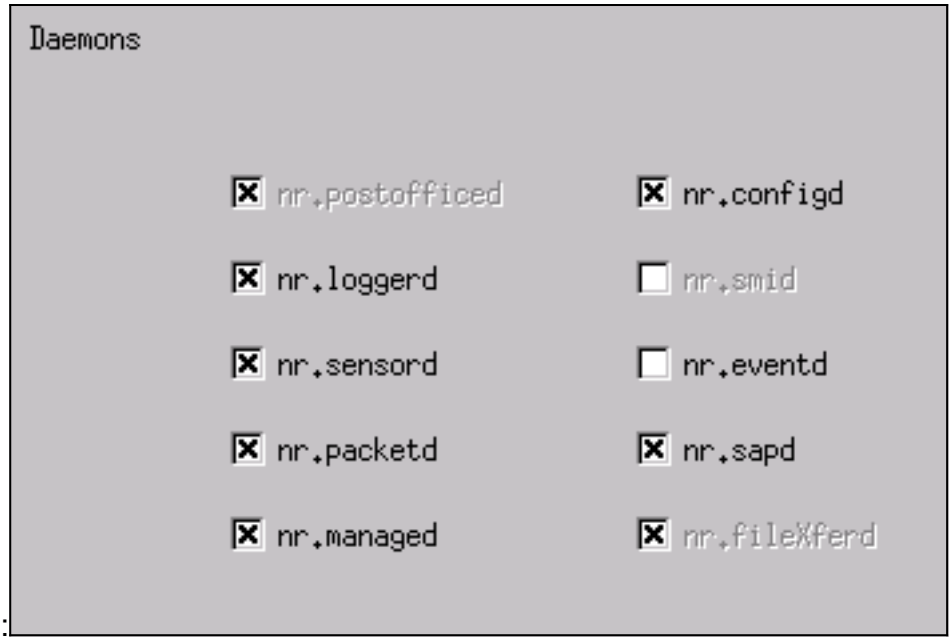


11. Choisissez l'**inondation d'ICMP** avec un ID de **2152**, et le clic **modifient**. Changez l'**action d'**aucun **éviter et se connecter**, et cliquez sur OK pour continuer.

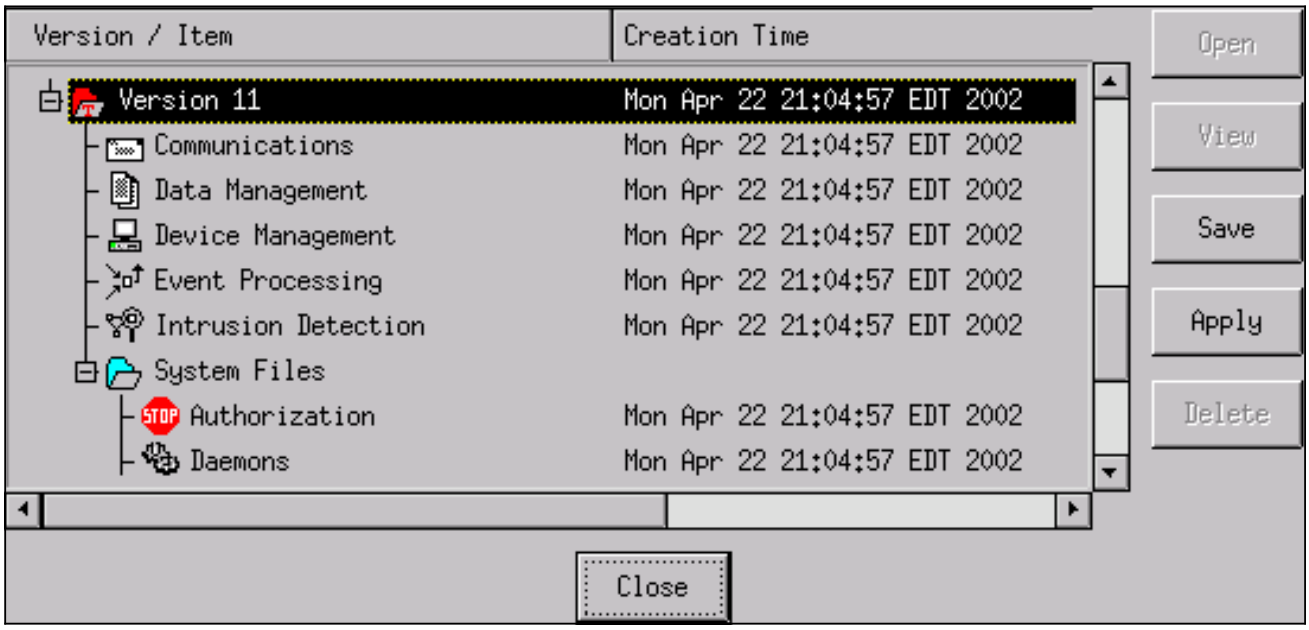


12. Cliquez sur OK pour fermer la fenêtre de détection d'intrusion.
13. Ouvrez le répertoire de fichiers système, et ouvrez la fenêtre de démons.Veillez-vous pour

avoir activé ces démons :



14. Cliquez sur OK pour continuer, pour choisir la version juste modifiée, et pour cliquer sur la **sauvegarde** et puis **pour s'appliquer**.Attendez le système pour te dire le capteur terminé en redémarrant des services, puis fermez toutes les fenêtres pour la configuration de directeur.



Vérifier

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **liste d'accès d'exposition** - Répertorie les déclarations de **commande access-list** en configuration de routeur. Il répertorie également un nombre de hits qui indique que le nombre de fois où un élément a été apparié pendant une recherche de **commande access-list**.
- **ping** - Utilisé pour diagnostiquer la connexion réseau de base.

Avant une attaque est lancé

Avant qu'une attaque soit lancée, émettez ces commandes.

```
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#
```

Lancez l'attaque et l'évitement

Lancez votre attaque à partir du routeur « lumière » à la victime « Chambre. » Quand l'ACL prend l'affect, les unreachables sont vus.

```
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.
```

Une fois que le capteur l'a détecté l'attaque, et l'ACL est téléchargé, et cette sortie est affichée sur la « Chambre. »

```
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
```

Les unreachables sont encore vus sur la « lumière, » suivant les indications de cet exemple.

```
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)
```

Quinze minutes plus tard, la « Chambre » retourne à la normale, parce que l'évitement a été placé à 15 minutes.

```
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#
```

La « lumière » peut cingler la « Chambre. »

```
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
```

Dépanner

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

Informations connexes

- Page de support Cisco Secure de prévention des intrusions
- Support et documentation techniques - Cisco Systems