Configuration de la réinitialisation TCP avec IDS Director

Contenu

Introduction

Ce document décrit comment configurer un directeur de système de détection d'intrusion (ID, autrefois NetRanger) et un capteur pour envoyer les remises de TCP sur un telnet tenté à une plage d'adresses qui incluent le routeur géré si la chaîne envoyée est « testattack ».

Conditions préalables

Conditions requises

Quand vu cette configuration, souvenez-vous s'il vous plaît de :

- Installez le capteur et le vérifiez que cela fonctionne correctement avant que vous exécutiez cette configuration.
- Assurez-vous que les envergures d'interface de reniflement au routeur géré 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
- Version de logiciel 12.2.6 courante de routeur de Cisco IOS®

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.

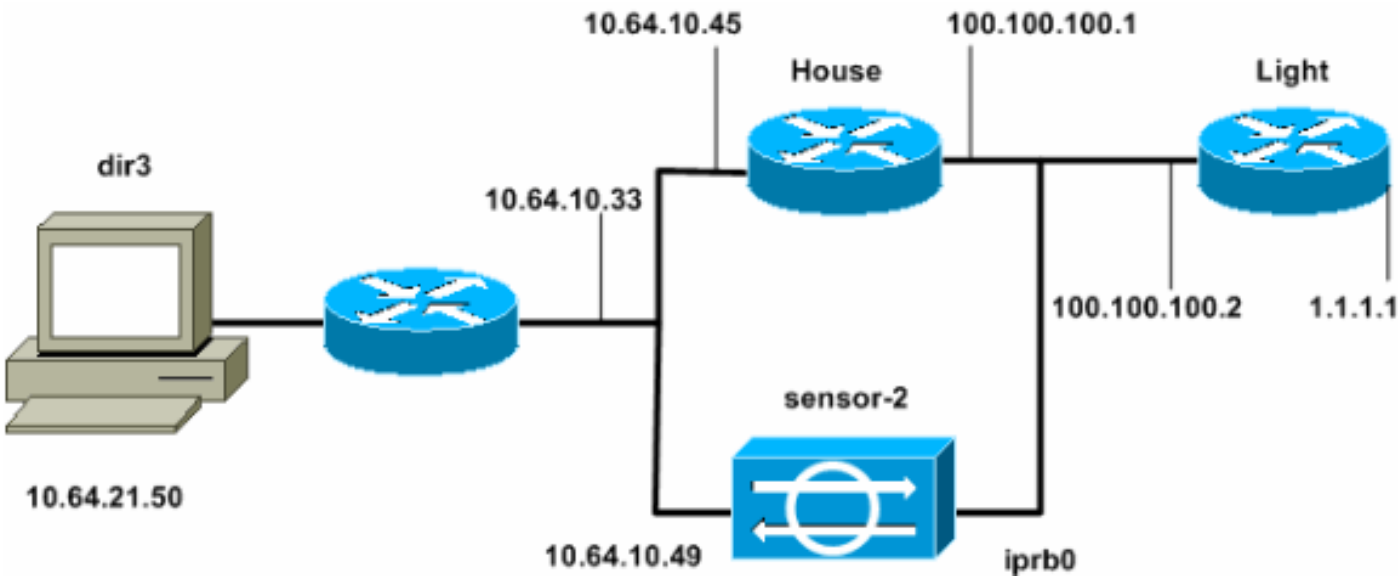
Configurer

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
!
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
```

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
 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
!
!
!
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 (le capteur d'ID) avec la **racine de** nom d'utilisateur et l'**attaque de** mot de passe.
2. **Sysconfig-capteur de** type.
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
```

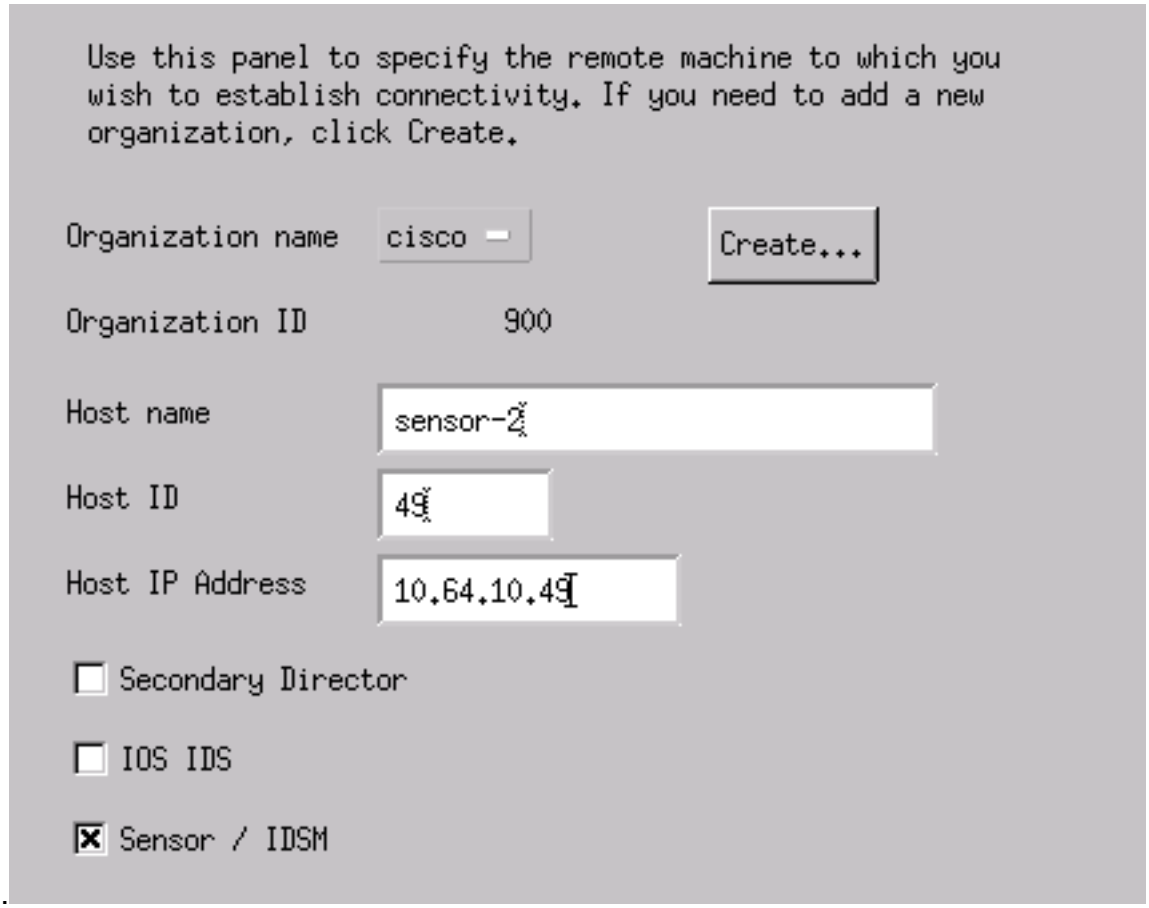
4. Une fois incité, sauvegardez la configuration et permettez au capteur pour redémarrer.

Ajoutez le capteur dans le directeur

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

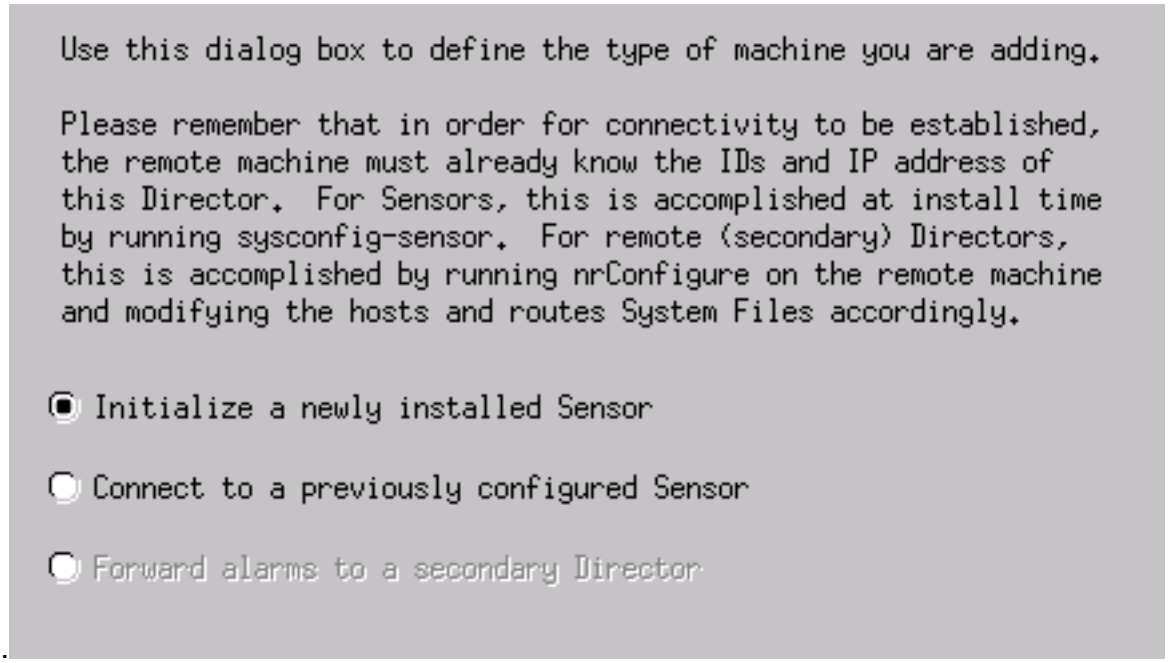
1. Telnet à 10.64.21.50 (l'IDS Director) avec le **netrangr de** nom d'utilisateur et l'**attaque de** mot de passe.

2. **Ovw& de** type pour lancer le HP OpenView.
3. Du menu principal, allez au **Security > Configure**.
4. Dans l'utilitaire de gestion de fichier de configuration, allez **classer > ajoutent l'hôte** et cliquent sur Next.
5. Remplissez les informations d'hôte de capteur, suivant les indications de cet exemple. Cliquez sur **Next**



(Suivant).

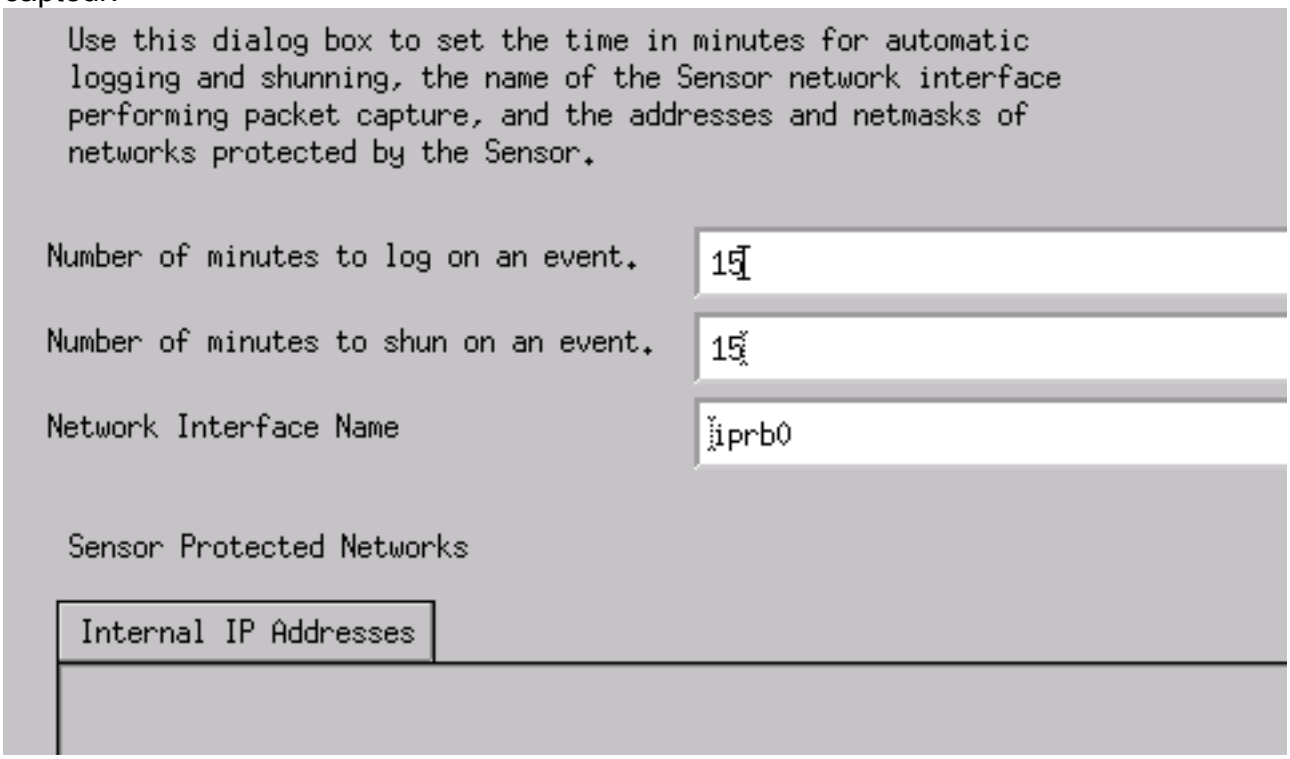
6. Recevez les valeurs par défaut pour le type d'ordinateur, et cliquez sur Next, suivant les indications de cet



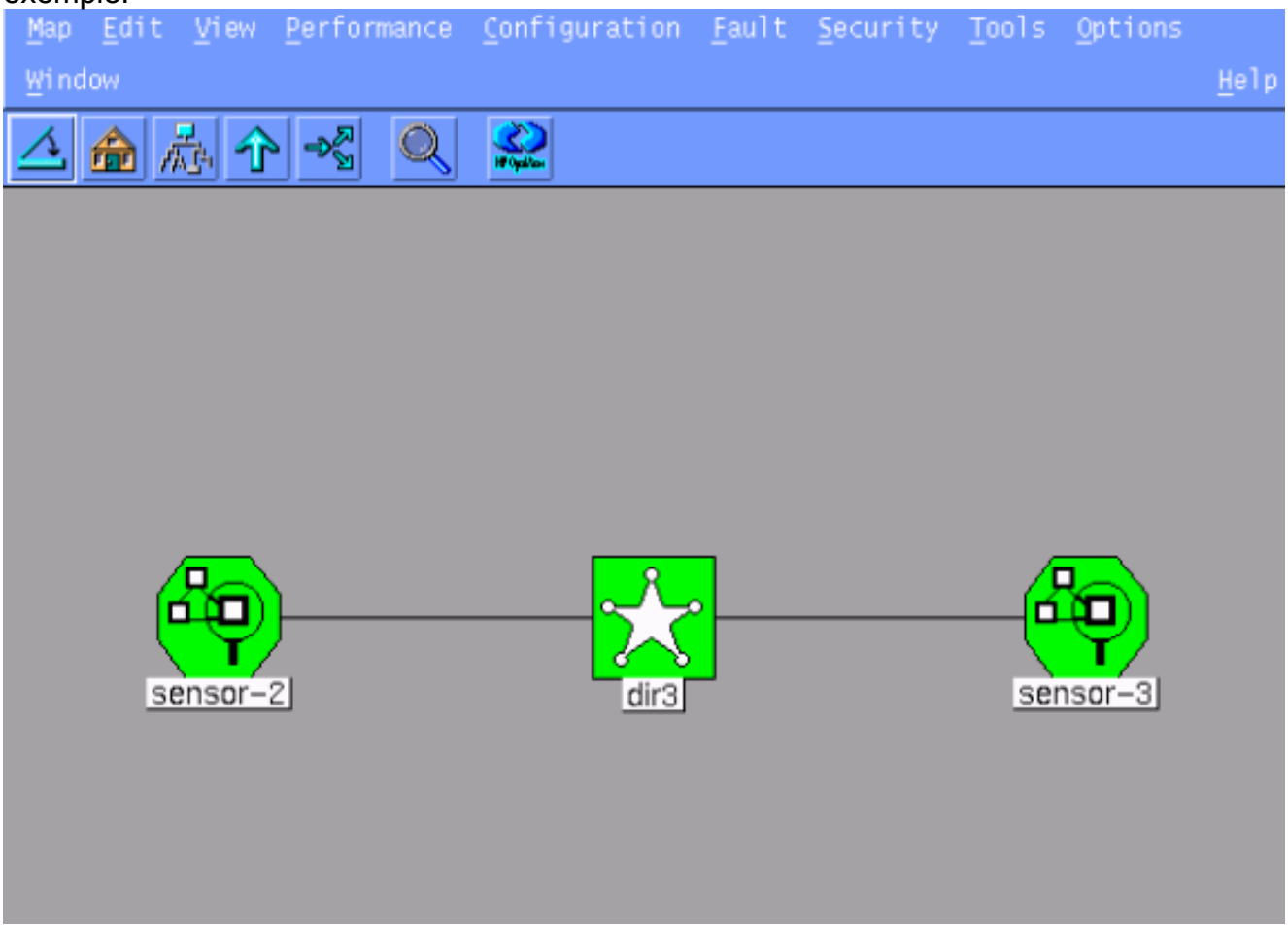
exemple.

7. Vous pouvez changer le log et éviter les minutes ou vous peut recevoir les valeurs par défaut. Cependant, vous devez changer 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

selon le type de capteur et comment vous connectez votre capteur.



8. Continuez à cliquer sur Next et puis cliquer sur Finish pour ajouter le capteur dans le directeur. Du menu principal, vous devriez maintenant voir sensor-2, comme indiqué dans cet exemple.

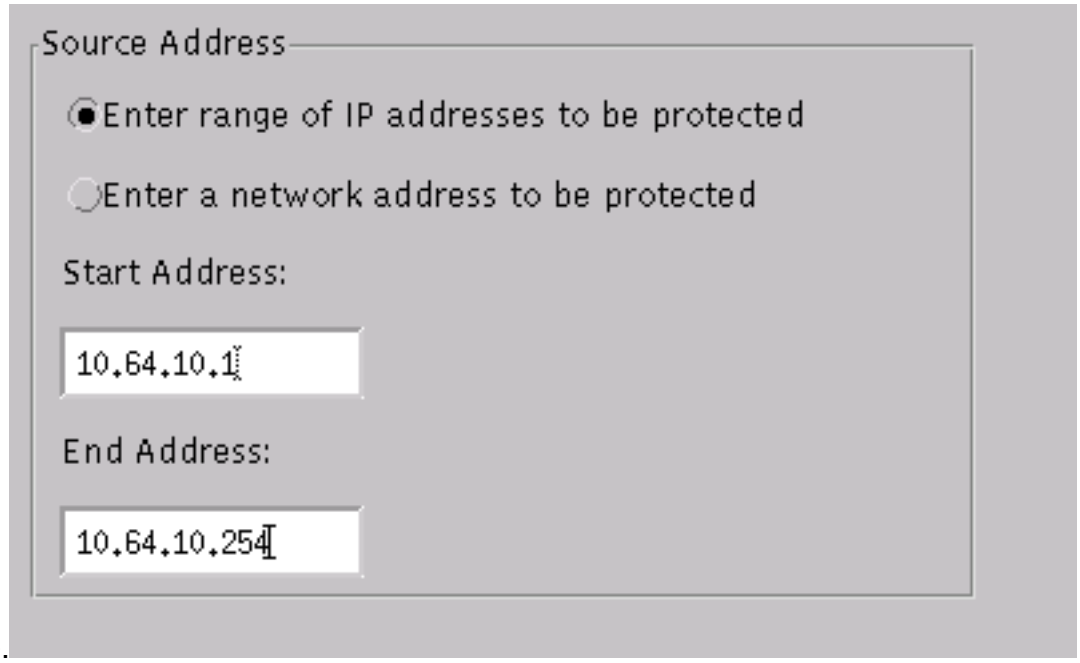


[Configurez la Réinitialisation TCP pour le routeur Cisco IOS]

Terminez-vous ces étapes pour configurer la Réinitialisation TCP pour le routeur Cisco IOS.

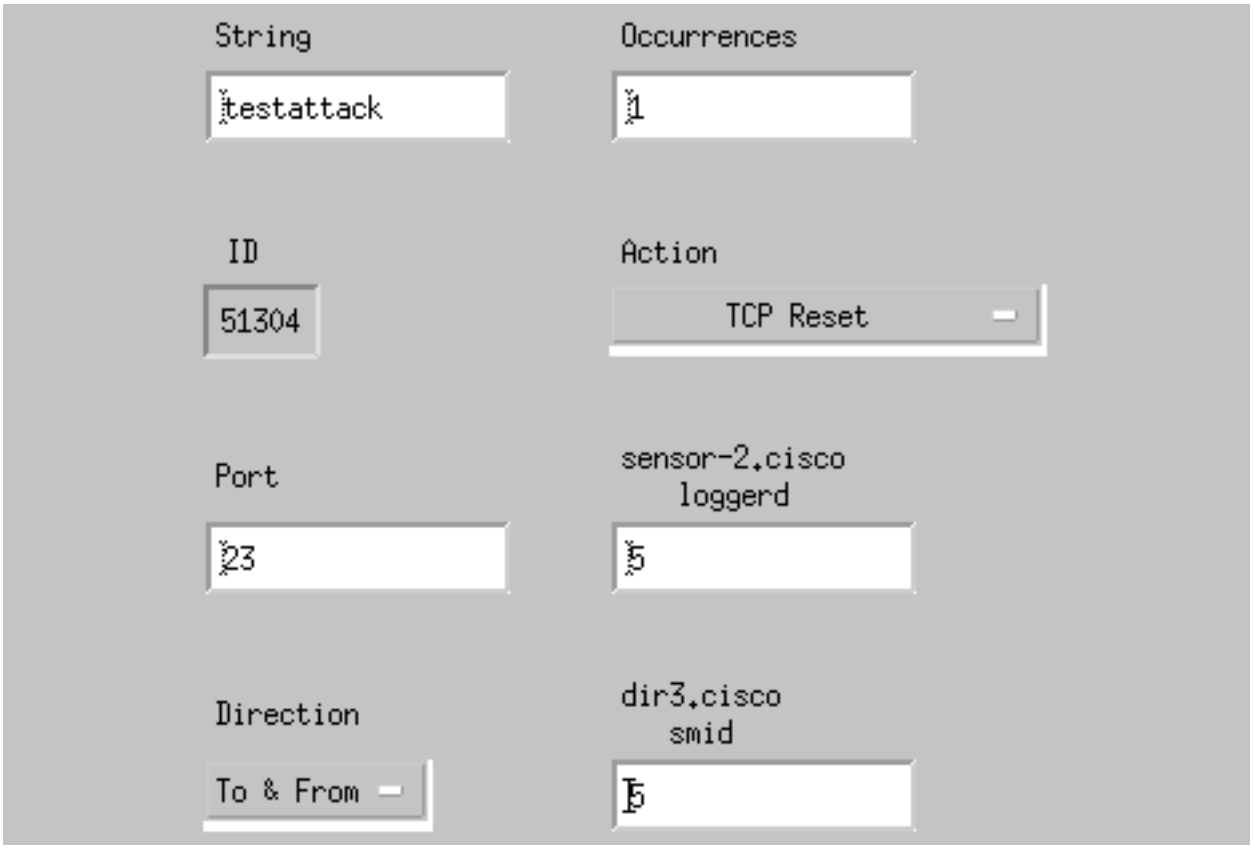
1. Dans le menu principal, allez au **Security > Configure**.
2. Dans l'utilitaire de gestion de fichier de configuration, mettez en valeur **sensor-2** et double-cliquer-le.
3. Ouvrez la Gestion de périphériques.
4. **Les périphériques de** clic **> ajoutent**. Écrivez l'information sur le périphérique, suivant les indications de l'exemple suivant. Cliquez sur **OK** pour continuer. Les mots de passe de telnet et d'enable sont
   Cisco.

5. Ouvrez la fenêtre de détection d'intrusion et cliquez sur les **réseaux protégés**. Ajoutez la plage d'adresses de 10.64.10.1 à 10.64.10.254 dans le réseau
   protégé.



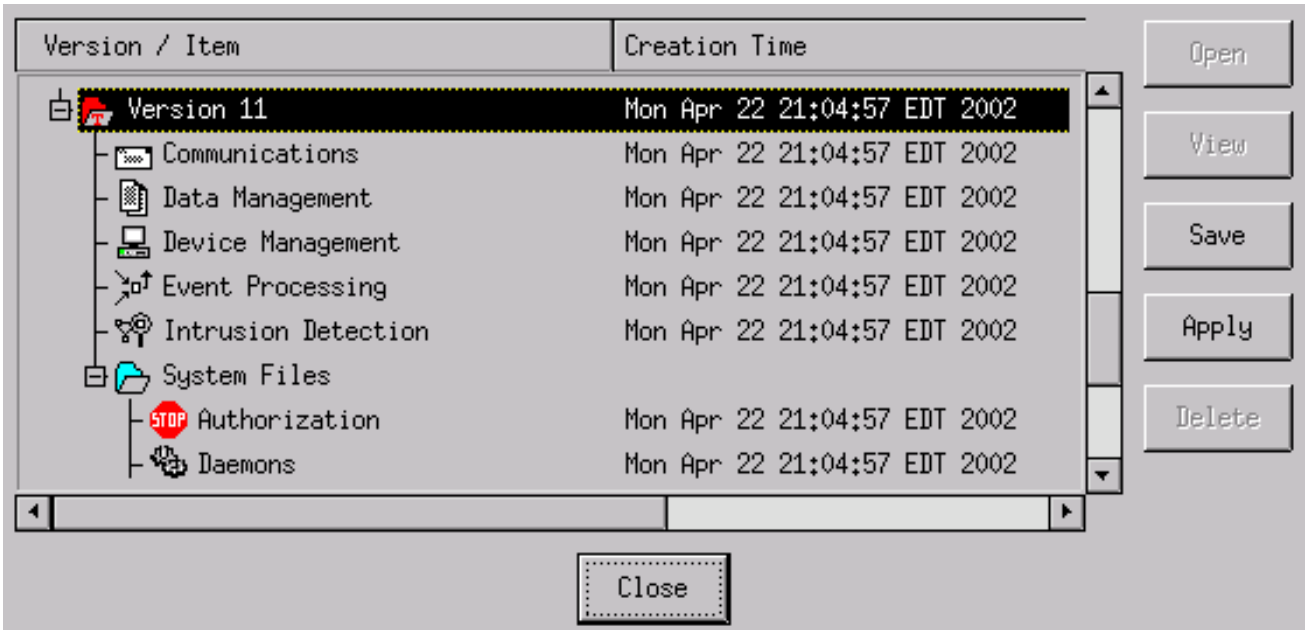
6. **Profil de** clic et **configuration manuelle** choisie. Ensuite, le clic **modifient des signatures**. Choisissez les **chaînes appariées** avec un ID de 8000. Le clic **développent > ajoutent** pour ajouter une nouvelle chaîne appelée le **testattack**. Écrivez les informations de chaîne, suivant les indications de cet exemple, et cliquez sur OK pour

continuer.



7. Vous avez terminé la présente partie de la configuration. Cliquez sur OK pour fermer la fenêtre de détection d'intrusion.
8. Ouvrez le répertoire de fichiers système, puis la fenêtre de démons. Veillez-vous pour faire activer ces démons
:

9. Cliquez sur **OK** pour continuer.
10. Choisissez la version que vous avez juste modifiée, cliquez sur la **sauvegarde** et puis **appliquez**. Attendez le système pour vous dire que le capteur a fini de redémarrer des services, puis ferment toutes les fenêtres pour la configuration de directeur.



Lancez l'attaque et la Réinitialisation TCP

Telnet de lumière du routeur à la Chambre de routeur et au **testattack de** type. Dès que vous avez enfoncé l'espace ou la touche Enter, vos remises de session de telnet. Vous vous connecterez à la Chambre de routeur.

```
light#telnet 10.64.10.45
Trying 10.64.10.45 ... Open

User Access Verification
Password:
house>en
Password:
house#testattack
[Connection to 10.64.10.45 closed by foreign host]
 !--- Telnet session has been reset because the !--- signature testattack was triggered.
```

Vérifier

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépanner

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Telnet à 10.64.10.49, le capteur, utilisant la **racine de** nom d'utilisateur et l'**attaque de** mot de passe. **Cd /usr/nr/etc de** type. **Cat packetd.conf de** type. **Si** vous placez correctement la Réinitialisation TCP pour le testattack, vous devriez voir des quatre (4) dans le domaine de codes d'intervention. Ceci indique la Réinitialisation TCP suivant les indications de cet exemple.

```
netrangr@sensor-2:/usr/nr/etc
>cat packetd.conf | grep "testattack"
RecordOfStringName 51304 23 3 1 "testattack"
SigOfStringMatch 51304 4 5 5 # "testattack"
```

Si vous placez accidentellement l'action à « aucun » dans la signature, vous verrez un zéro (0) dans le domaine de codes d'intervention. Ceci n'indique aucune action comme vu dans cet exemple.

```
netrangr@sensor-2:/usr/nr/etc
>cat packetd.conf | grep "testattack"
RecordOfStringName 51304 23 3 1 "testattack"
SigOfStringMatch 51304 0 5 5 # "testattack"
```

Les remises de TCP sont envoyées de l'interface de reniflement du capteur. S'il y a un commutateur connectant l'interface de capteur à l'interface extérieure du routeur géré, quand vous configurez utilisant la commande de **set span** dans le commutateur, utilisez cette syntaxe :

```
set span <src_mod/src_port><dest_mod/dest_port> both inpkts enable
```

```
banana (enable) set span 2/12 3/6 both inpkts enable
Overwrote Port 3/6 to monitor transmit/receive traffic of Port 2/12
Incoming Packets enabled. Learning enabled. Multicast enabled.
banana (enable)
banana (enable)
banana (enable) show span

Destination     : Port 3/6
!--- Connect to sniffing interface of the Sensor. Admin Source : Port 2/12
!--- Connect to FastEthernet0/0 of Router House. Oper Source : Port 2/12
Direction       : transmit/receive
Incoming Packets: enabled
Learning        : enabled
Multicast       : enabled
```

Informations connexes

- Notes de terrain
- Page de support Cisco Secure de prévention des intrusions