Configuration de la réinitialisation TCP avec IDS Director

Contenu

Introduction

Ce document décrit comment configurer un IDS (Intrusion Detection System, anciennement NetRanger) Director et Sensor pour envoyer des réinitialisations TCP sur une tentative de Telnet à une plage d'adresses qui incluent le routeur géré si la chaîne envoyée est « testattack ».

Conditions préalables

Conditions requises

Lorsque vous envisagez cette configuration, n'oubliez pas de :

- Installez le capteur et vérifiez qu'il fonctionne correctement avant d'effectuer cette configuration.
- Assurez-vous que l'interface de reniflage s'étend à l'interface externe du routeur géré.

Components Used

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

- Cisco IDS Director 2.2.3
- Capteur Cisco IDS 3.0.5
- Routeur Cisco IOS® exécutant le logiciel version 12.2.6

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

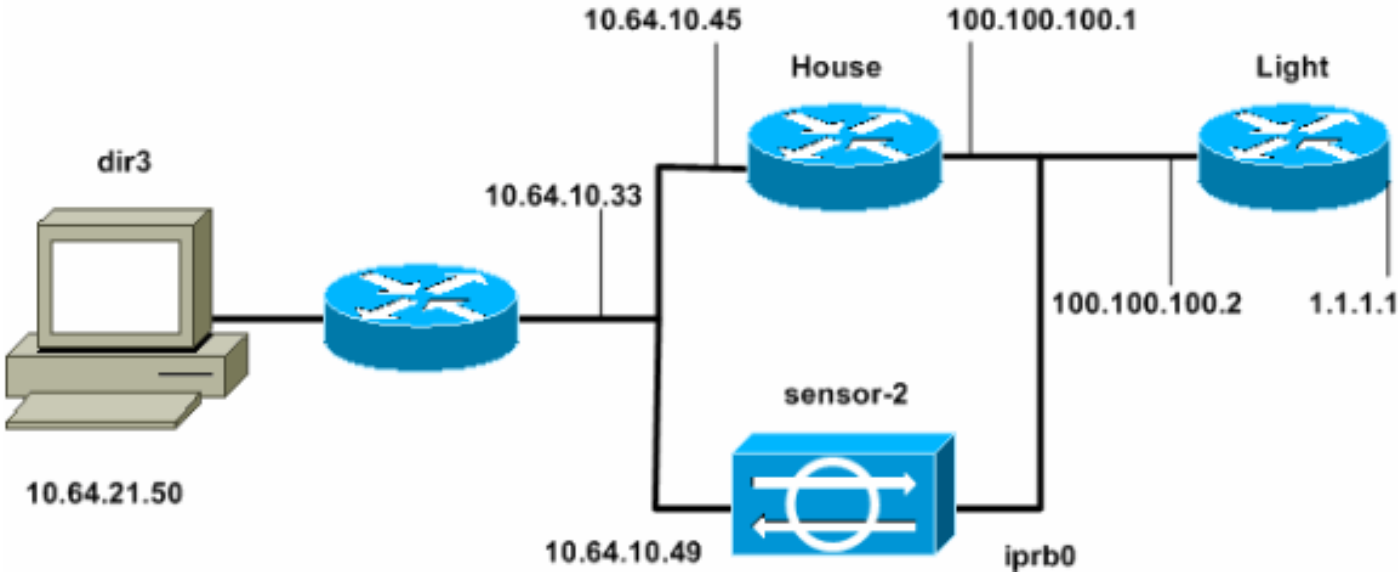
Configuration

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

Remarque : Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez l'outil de recherche de commandes (clients inscrits seulement).

Diagramme du réseau

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



Configurations

Ce document utilise les configurations suivantes.

- Voyant du routeur
- Routeur House

Voyant 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#
```

Configuration du capteur

Suivez ces étapes pour configurer le capteur.

1. Établissez une connexion Telnet à 10.64.10.49 (le capteur IDS) avec le nom d'utilisateur **root** et l'**attaque** par mot de passe.
2. Tapez **sysconfig-capteur**.
3. Lorsque vous y êtes invité, entrez les informations de configuration, comme indiqué dans 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. Lorsque vous y êtes invité, enregistrez la configuration et autorisez le capteur à redémarrer.

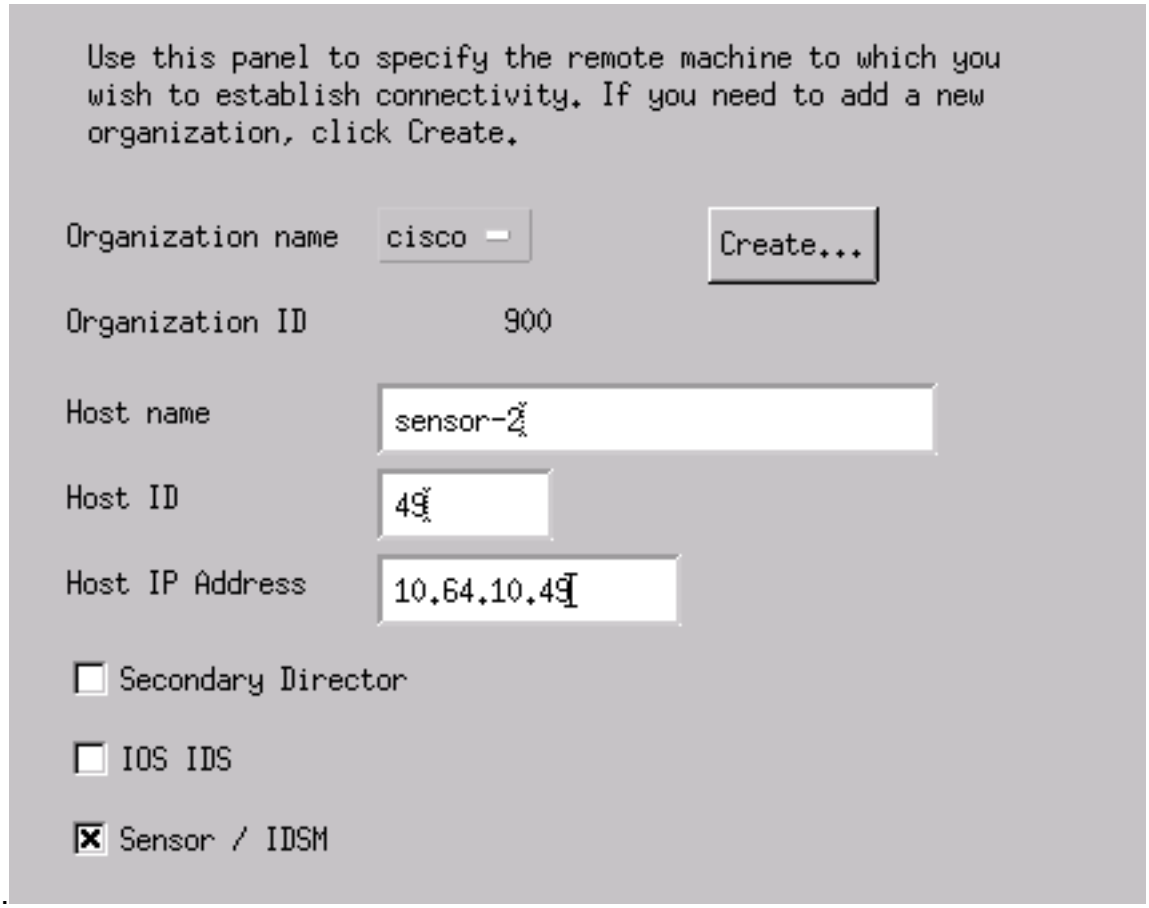
Ajouter le capteur au Director

Complétez ces étapes pour ajouter le capteur au Director.

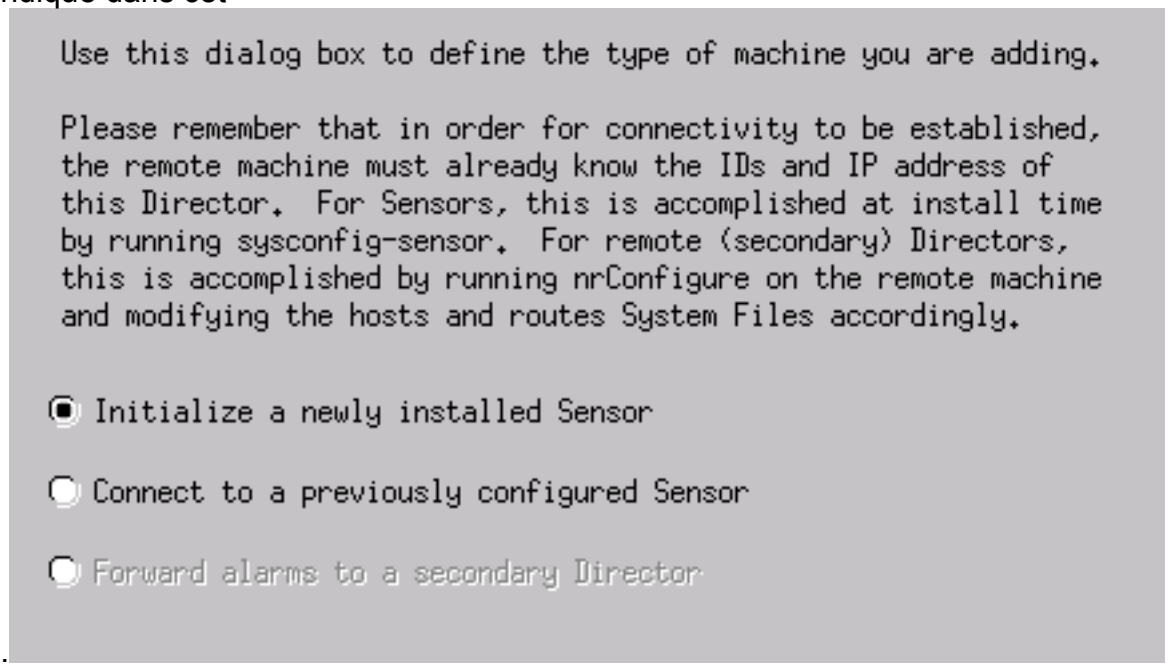
1. Établissez une connexion Telnet vers 10.64.21.50 (IDS Director) avec le nom d'utilisateur **voisin** et l'**attaque par** mot de passe.
2. Tapez **ovw&** pour lancer HP OpenView.
3. Dans le menu principal, accédez à **Security > Configure**.
4. Dans l'utilitaire de gestion des fichiers de configuration, accédez à **file > Add Host** et cliquez

sur **Next**.

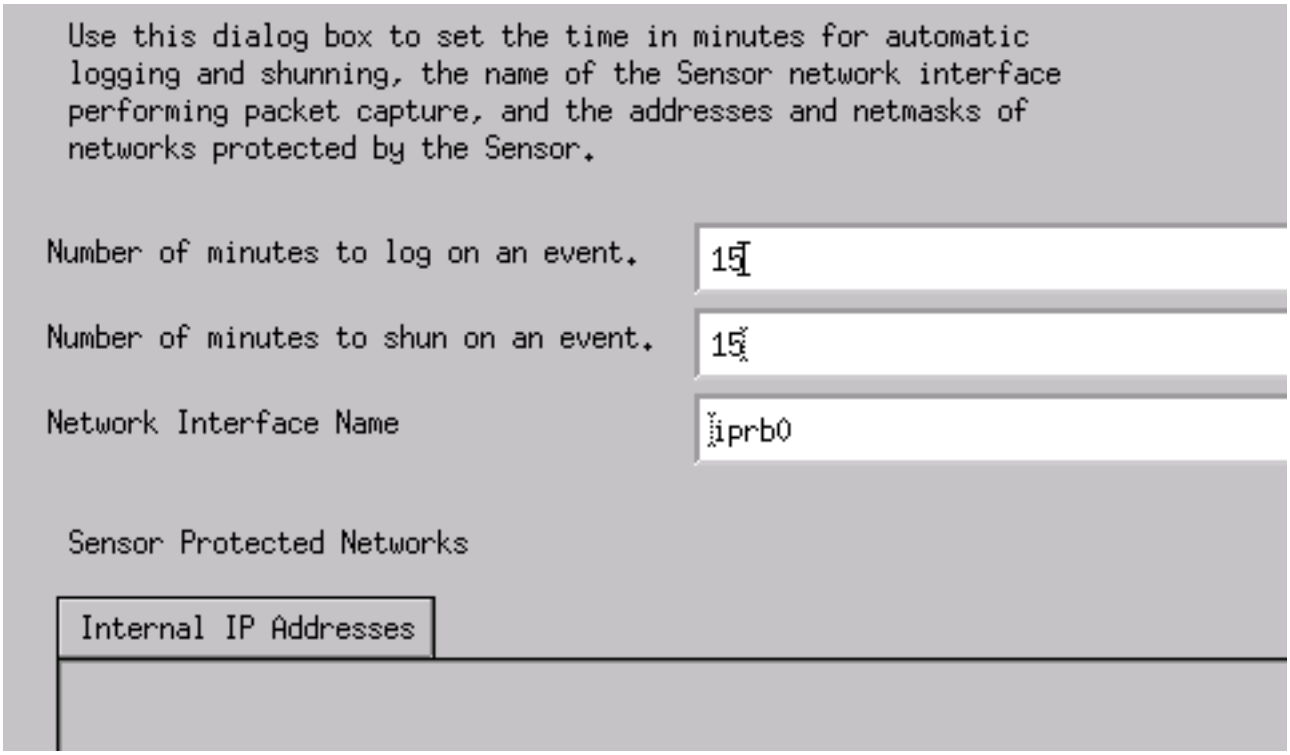
5. Complétez les informations sur l'hôte du capteur, comme indiqué dans cet exemple. Cliquez sur **Next** (Suivant).



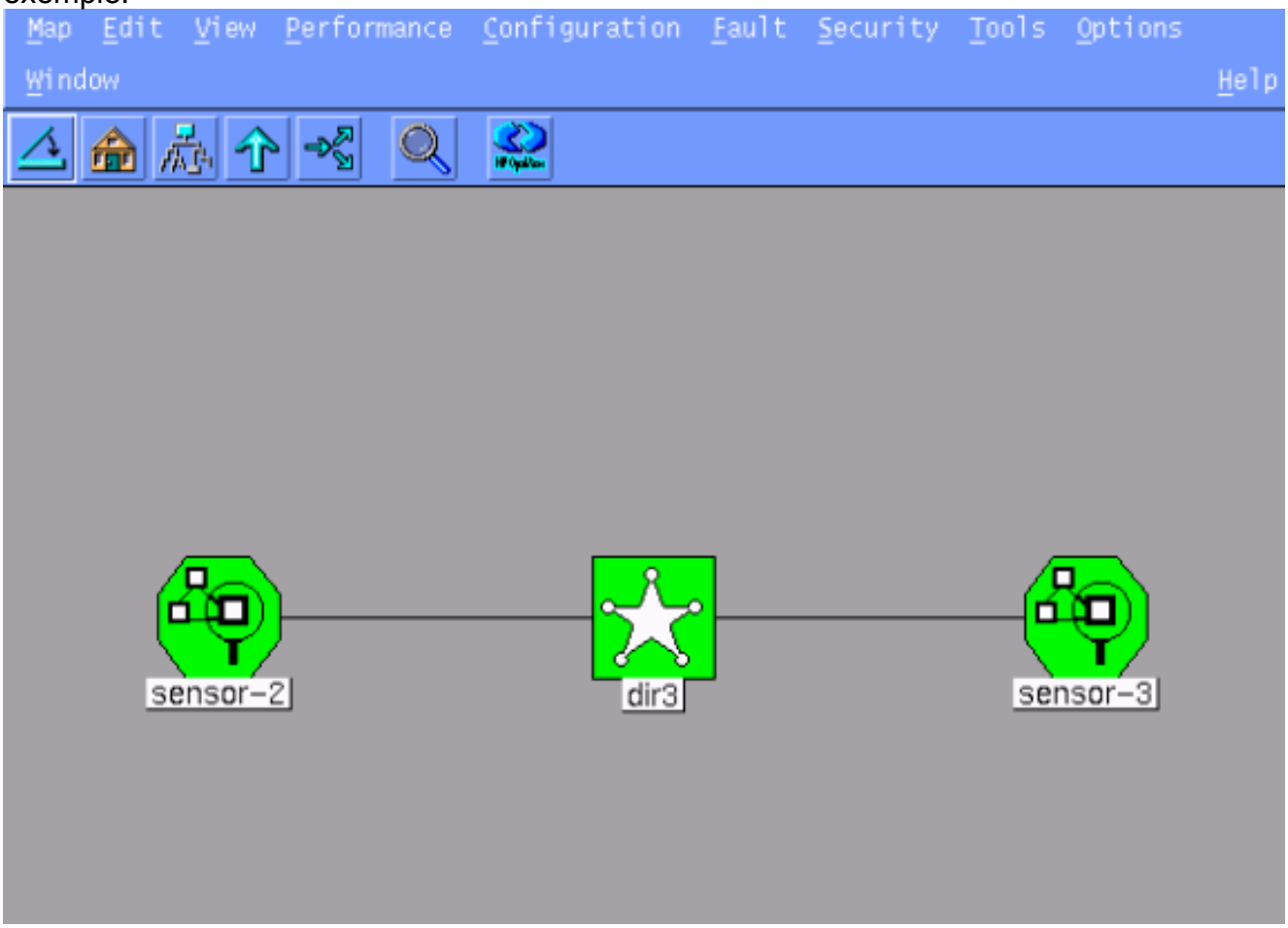
6. Acceptez les paramètres par défaut pour le type de machine, puis cliquez sur **Suivant**, comme indiqué dans cet exemple.



7. Vous pouvez modifier le journal et ignorer les minutes ou accepter les valeurs par défaut. Cependant, vous devez remplacer le nom de l'interface réseau par le nom de votre interface de reniflage. Dans cet exemple, il s'agit de « iprb0 ». Il peut s'agir de « spwr0 » ou de n'importe quoi d'autre selon le type de capteur et la façon dont vous connectez votre capteur.



8. Continuez à cliquer sur **Suivant**, puis cliquez sur **Terminer** pour ajouter le capteur au Director. Dans le menu principal, vous devriez maintenant voir le capteur-2, comme dans cet exemple.

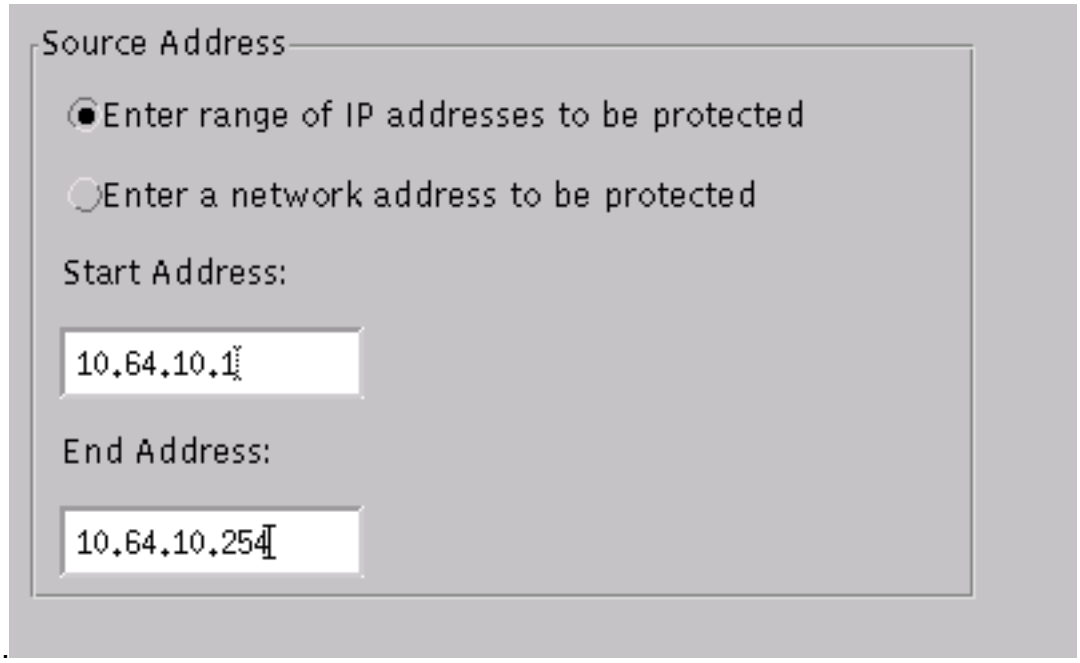


Configuration de la réinitialisation TCP pour le routeur Cisco IOS

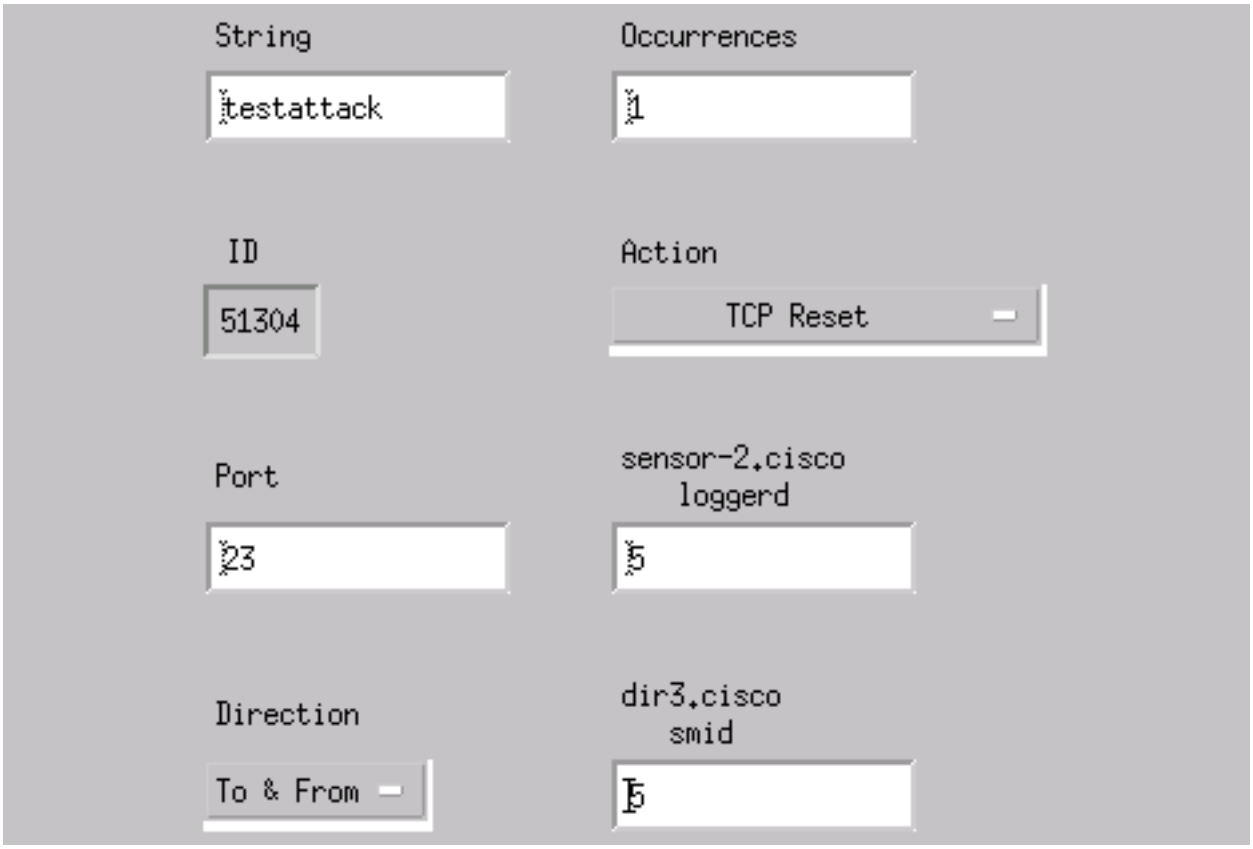
Complétez ces étapes pour configurer la réinitialisation TCP pour le routeur Cisco IOS.

1. Dans le menu principal, accédez à **Security > Configure**.
2. Dans l'utilitaire de gestion des fichiers de configuration, mettez en surbrillance **le capteur-2** et double-cliquez dessus.
3. Ouvrez la gestion des périphériques.
4. Cliquez sur **Périphériques > Ajouter**. Saisissez les informations relatives au périphérique, comme indiqué dans l'exemple suivant. Cliquez sur **OK pour continuer.** Les mots de passe Telnet et enable sont tous deux
   Cisco.

5. Ouvrez la fenêtre Intrusion Detection et cliquez sur **Protected Networks**. Ajoutez la plage d'adresses de 10.64.10.1 à 10.64.10.254 dans le réseau
   protégé.

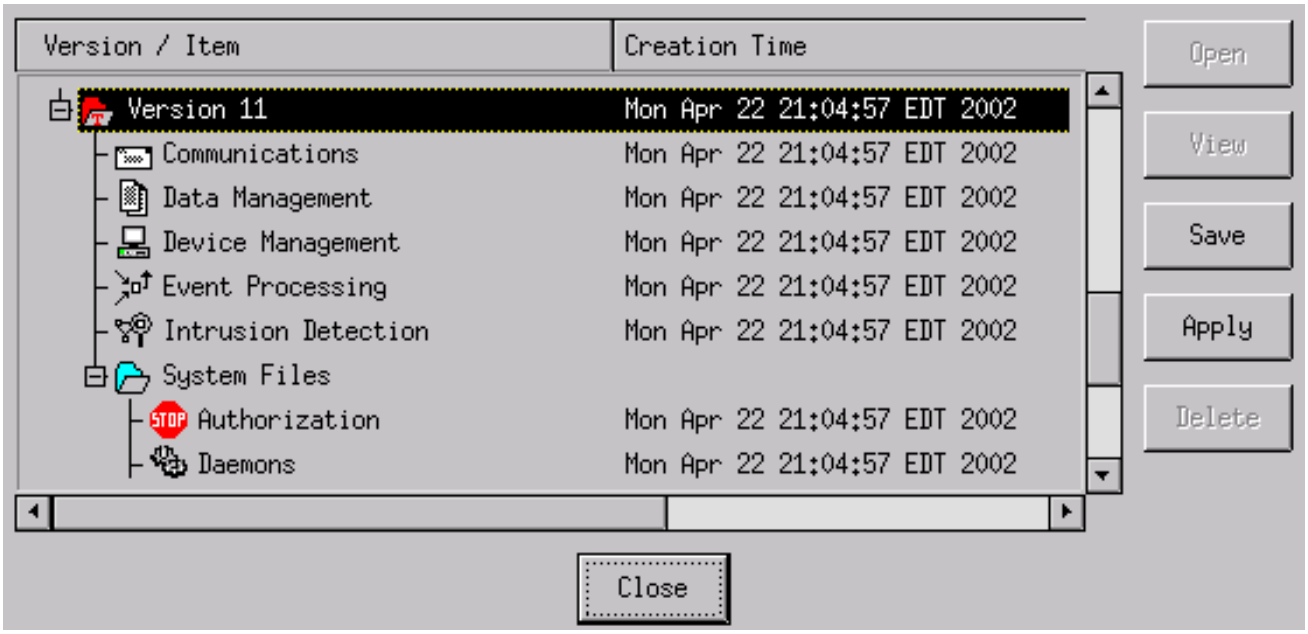


6. Cliquez sur **Profil** et sélectionnez **Configuration manuelle**. Cliquez ensuite sur **Modifier les signatures**. Choisissez **Chaînes correspondantes** avec un ID de 8000. Cliquez sur **Développer > Ajouter** pour ajouter une nouvelle chaîne appelée **testattack**. Entrez les informations de chaîne, comme indiqué dans cet exemple, et cliquez sur **OK** pour continuer.



7. Vous avez terminé cette partie de la configuration. Cliquez sur **OK** pour fermer la fenêtre Intrusion Detection.
8. Ouvrez le dossier Fichiers système, puis la fenêtre Démons. Assurez-vous que ces démons sont activés
   :

9. Cliquez sur **OK pour continuer.**
10. Choisissez la version que vous venez de modifier, cliquez sur **Enregistrer**, puis **Appliquer**. Attendez que le système vous dise que le capteur a terminé le redémarrage des services, puis fermez toutes les fenêtres de la configuration
    Director.



Lancer l'attaque et réinitialiser TCP

Établissez une connexion Telnet de Router Light à Router House et tapez **testattack**. Dès que vous appuyez sur la touche Espace ou Entrée, votre session Telnet se réinitialise. Vous vous connecterez à Router House.

```
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.
```

Vérification

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

Dépannage

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

Établissez une connexion Telnet avec 10.64.10.49, le capteur, en utilisant le nom d'utilisateur **root** et l'**attaque** par mot de passe. Tapez **cd /usr/nr/etc**. Tapez **cat packetd.conf**. Si vous définissez correctement la réinitialisation TCP pour le test, vous devriez voir quatre (4) dans le champ Codes d'action. Ceci indique la réinitialisation TCP comme indiqué dans 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 définissez accidentellement l'action sur « aucun » dans la signature, vous verrez un zéro (0) dans le champ Codes d'action. Cela indique qu'aucune action n'est visible 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 réinitialisations TCP sont envoyées à partir de l'interface de reniflage du capteur. Si un commutateur connecte l'interface Sensor à l'interface externe du routeur géré, lorsque vous configurez à l'aide de la commande **set span** du commutateur, utilisez la syntaxe suivante :

```
set span
```

```
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 d'assistance Cisco Secure Intrusion Prevention