Configuration de la réinitialisation TCP IPS avec IME

Contenu

Introduction

Ce document discute la configuration de la Réinitialisation TCP de Système de prévention d'intrusion (IPS) utilisant le Manager Express IPS (IME). Des capteurs IME et IPS sont utilisés pour gérer un routeur de Cisco pour la Réinitialisation TCP. Quand vous passez en revue cette configuration, souvenez-vous ces éléments :

- Installez le capteur et assurez-vous les travaux de capteur correctement.
- Faites l'envergure d'interface de reniflement au routeur en dehors de l'interface.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

logiciel suivantes :

- Cisco IPS Manager Express 7.0
- Capteur 7.0(0.88)E3 de Cisco IPS
- Routeur de Cisco IOS® avec la version du logiciel Cisco IOS 12.4

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.

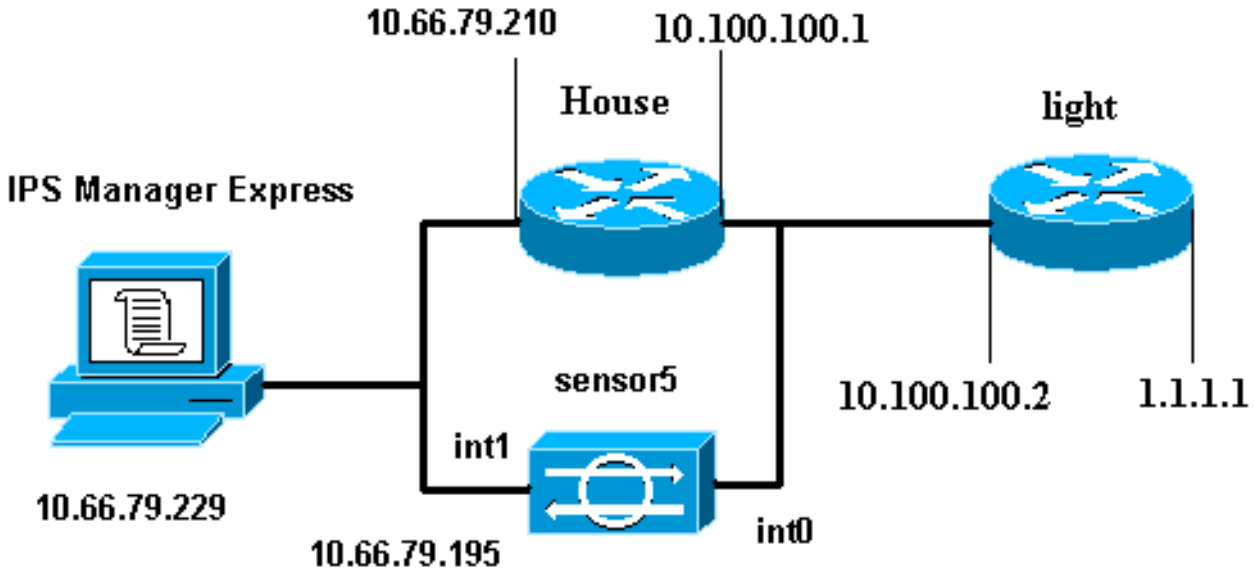
Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez

Diagramme du réseau

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



Configurations

Ce document utilise les configurations indiquées ici.

- Lumière du routeur
- Routeur House

Lumière du routeur

```
Current configuration : 906 bytes
!
version 12.4
```

```
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 10.100.100.2 255.255.255.0
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
10.100.100.1 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 : 939 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname house ! logging queue-limit 100 enable password
cisco ! ip subnet-zero ! ! no ip cef no ip domain lookup
! ip audit notify log ip audit po max-events 100 ! ! no
voice hpi capture buffer no voice hpi capture
destination ! ! ! ! interface FastEthernet0/0 ip address
10.66.79.210 255.255.255.224 duplex auto speed auto !
interface FastEthernet0/1 ip address 10.100.100.1
255.255.255.0 duplex auto speed auto ! interface ATM1/0
no ip address shutdown no atm ilmi-keepalive ! ip
classless ip route 0.0.0.0 0.0.0.0 10.66.79.193 ip route
1.1.1.0 255.255.255.0 10.100.100.2 no ip http server no
ip http secure-server ! ! ! ! call rsvp-sync ! ! mgcp
profile default ! ! line con 0 exec-timeout 0 0 line aux
0 line vty 0 4 exec-timeout 0 0 password cisco login
line vty 5 15 login ! ! end
```

Commencez la configuration de capteur

Terminez-vous ces étapes pour commencer la configuration du capteur.

1. Si c'est votre première fois de se connecter dans le capteur, vous devez entrer dans **Cisco** comme nom d'utilisateur et **Cisco** comme mot de passe.
2. Quand les systèmes invite vous, changent votre mot de passe.**Remarque:** Cisco123 est un mot de dictionnaire et n'est pas autorisé dans le système.
3. Tapez l'**installation** et terminez-vous le système invite afin d'installer les paramètres de base pour les capteurs.
4. Entrez les informations suivantes :`sensor5#setup --- System Configuration Dialog --- !--- At any point you may enter a question mark '?' for help. !--- Use ctrl-c to abort the configuration dialog at any prompt. !--- Default settings are in square brackets '[]'. Current Configuration: networkParams ipAddress 10.66.79.195 netmask 255.255.255.224 defaultGateway 10.66.79.193 hostname Corp-IPS telnetOption enabled !--- Permit the IP`

```
address of workstation or network with IME accessList ipAddress 10.66.79.0 netmask
255.255.255.0 exit timeParams summerTimeParams active-selection none exit exit service
webServer general ports 443 exit exit
```

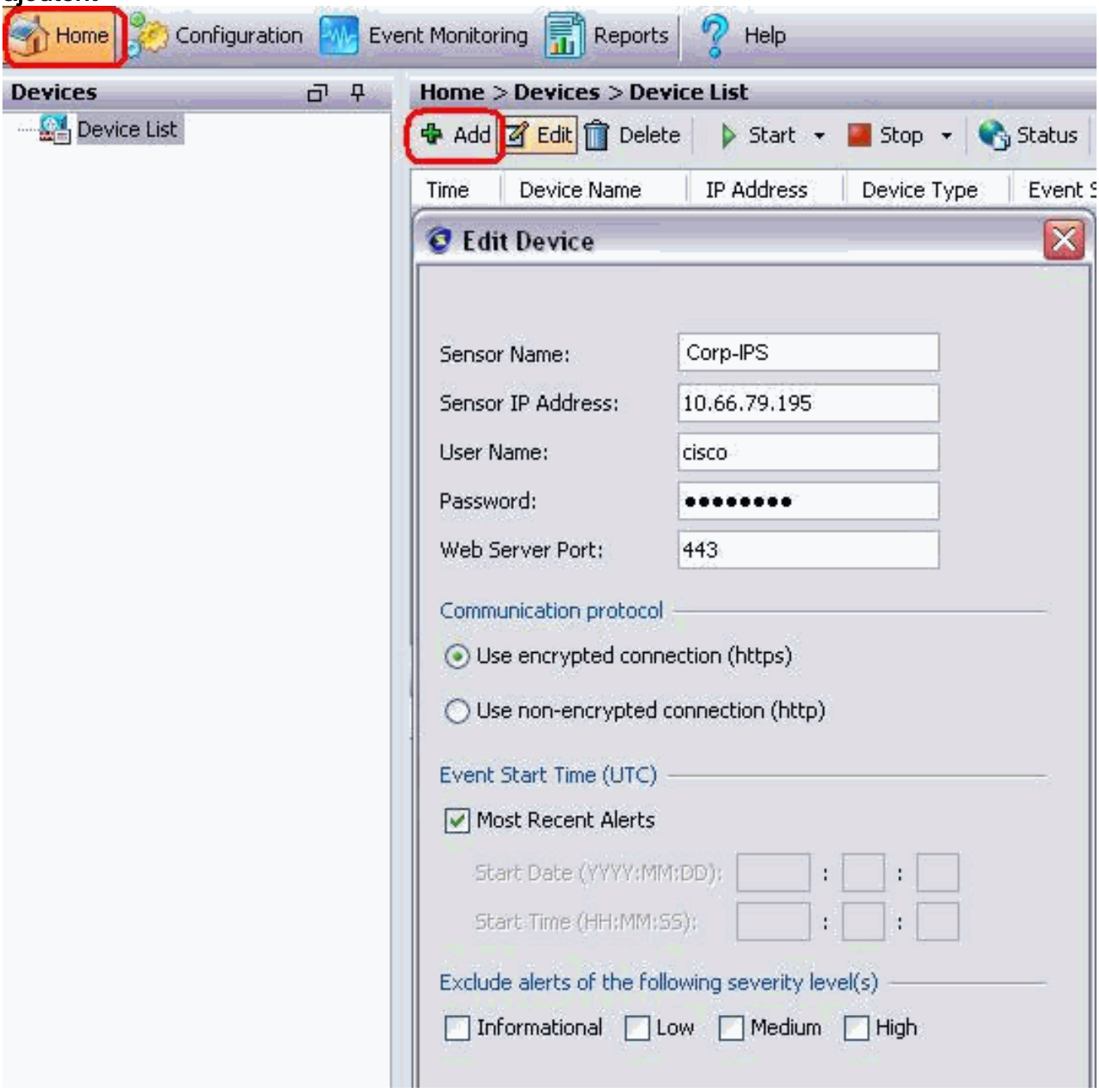
5. Enregistrez la configuration.Il peut prendre quelques minutes pour que le capteur sauvegarde la configuration.
```
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.

Enter your selection[2]: 2
```

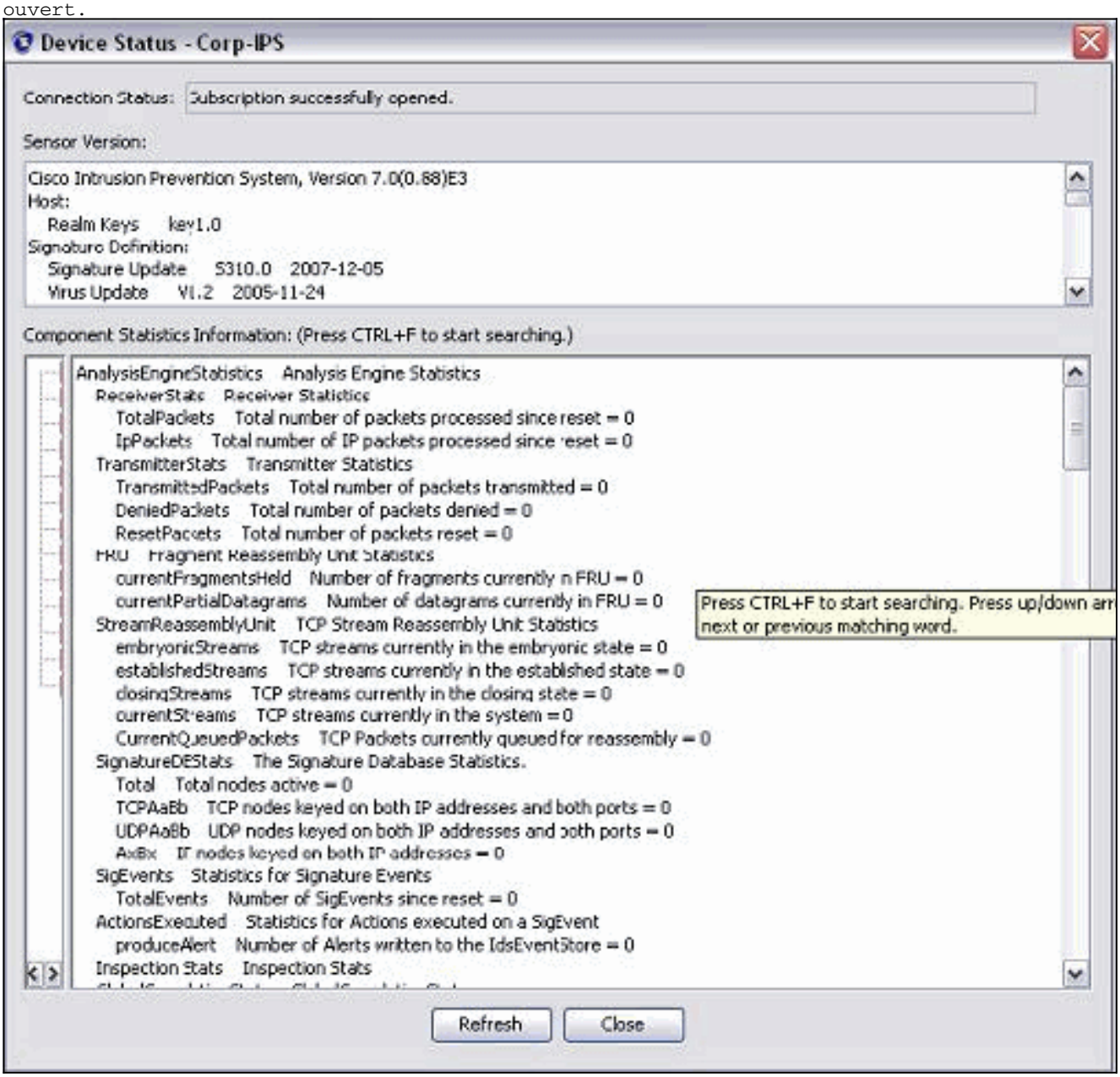
Ajoutez le capteur dans l'IME

Terminez-vous ces étapes afin d'ajouter le capteur dans l'IME :

1. Allez au PC Windows, qui a installé le Manager Express IPS, et ouvrez le Manager Express IPS.
2. Choisissez **à la maison > ajoutent**.



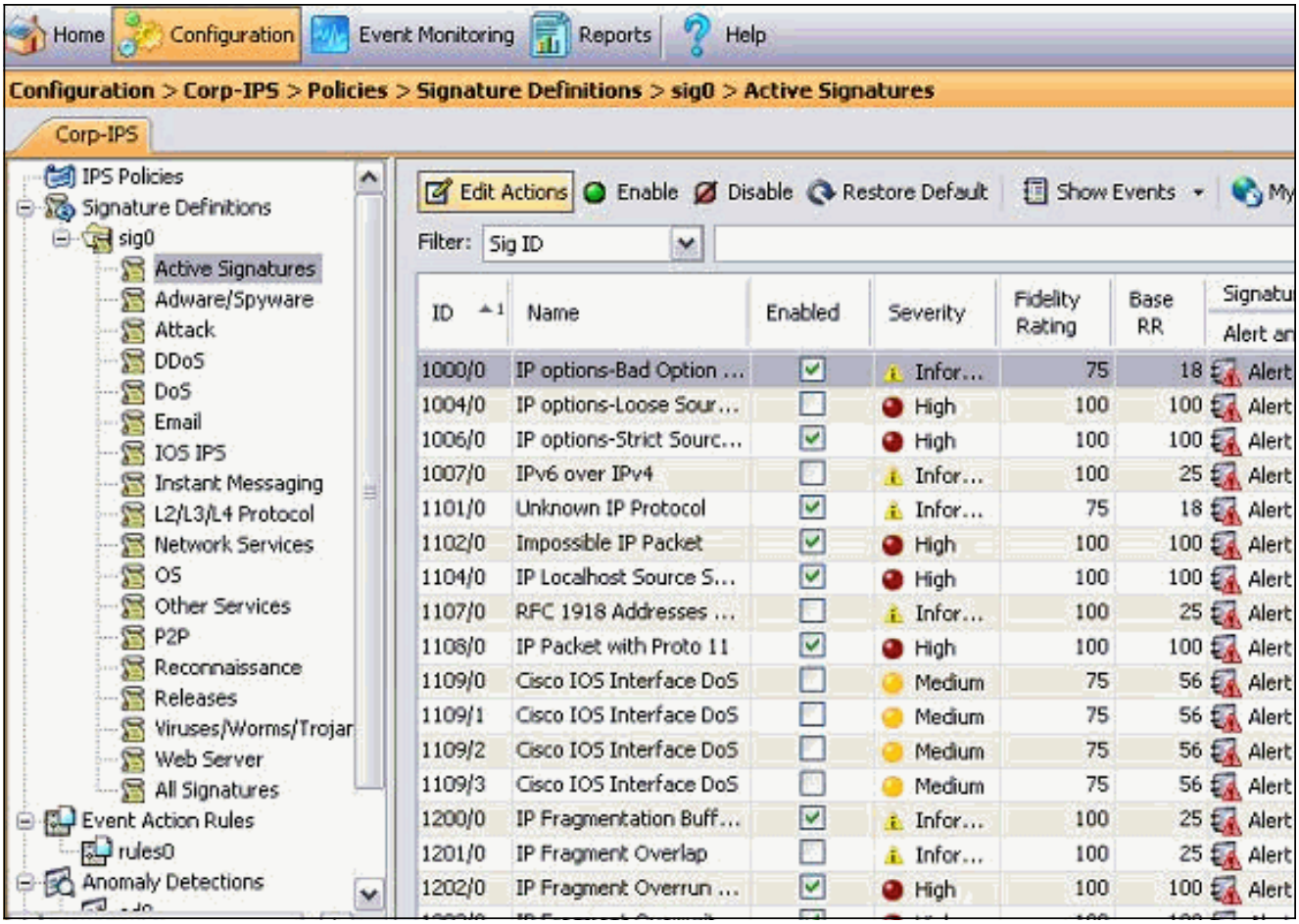
3. Saisissez ces informations et cliquez sur OK afin de terminer la configuration.
4. Choisissez les **périphériques > le Corp.-IPS** afin de vérifier l'état de capteur et puis cliquer avec le bouton droit afin de choisir l'**état des périphériques**.Assurez-vous que vous pouvez voir l'`abonnement avec succès ouvert.`



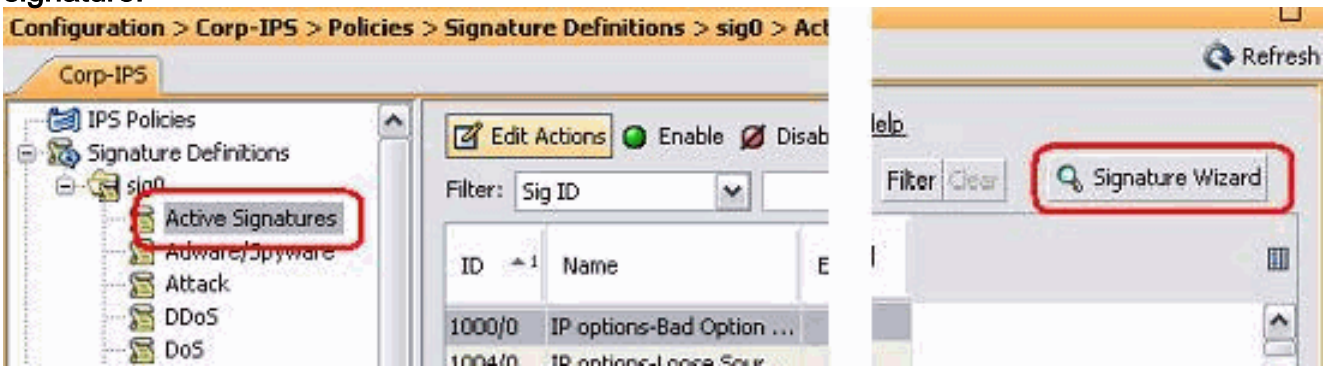
Configurez la Réinitialisation TCP pour le routeur Cisco IOS

Terminez-vous ces étapes afin de configurer la Réinitialisation TCP pour le routeur Cisco IOS :

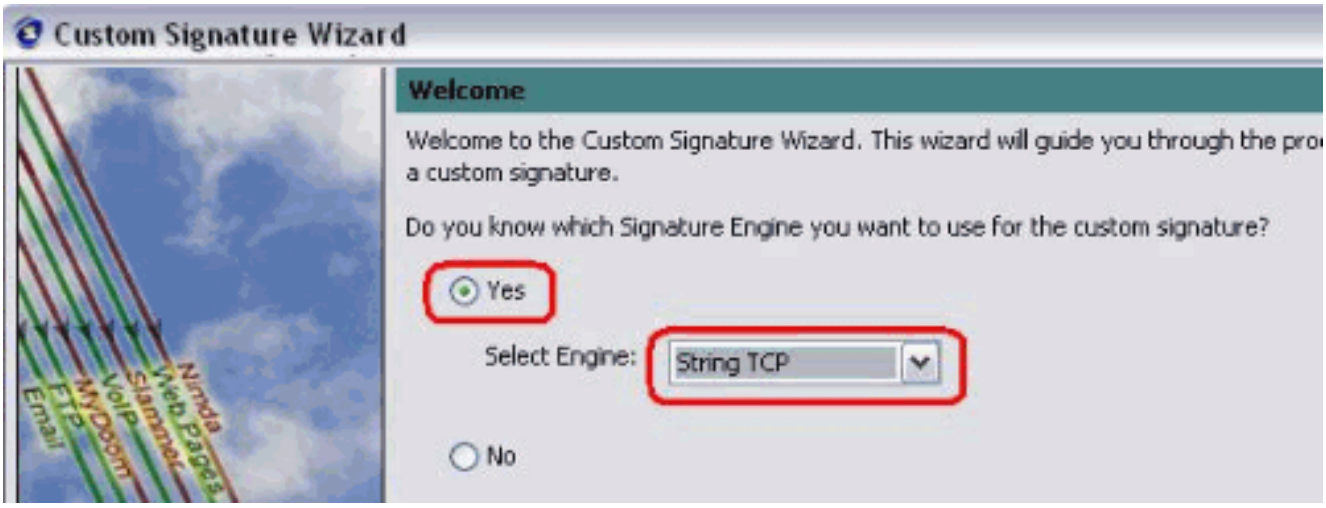
1. Du PC IME, ouvrez votre navigateur Web et allez à **https://10.66.79.195**.
2. Cliquez sur OK afin de recevoir le certificat HTTPS téléchargé du capteur.
3. Dans la fenêtre de connexion, écrivez **Cisco** pour le nom d'utilisateur et **123cisco123** pour le mot de passe.Cette interface de gestion IME apparaît :



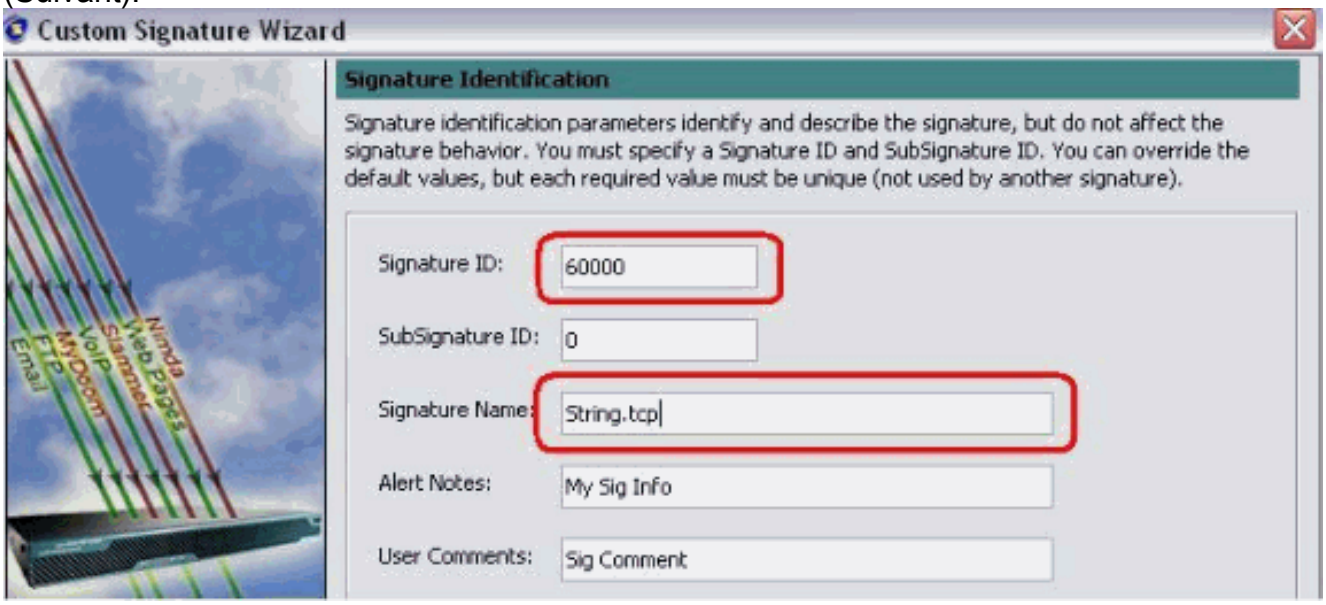
4. De l'onglet de configuration, cliquez sur les **signatures actives**.
5. Cliquez sur alors l'**assistant de signature.**



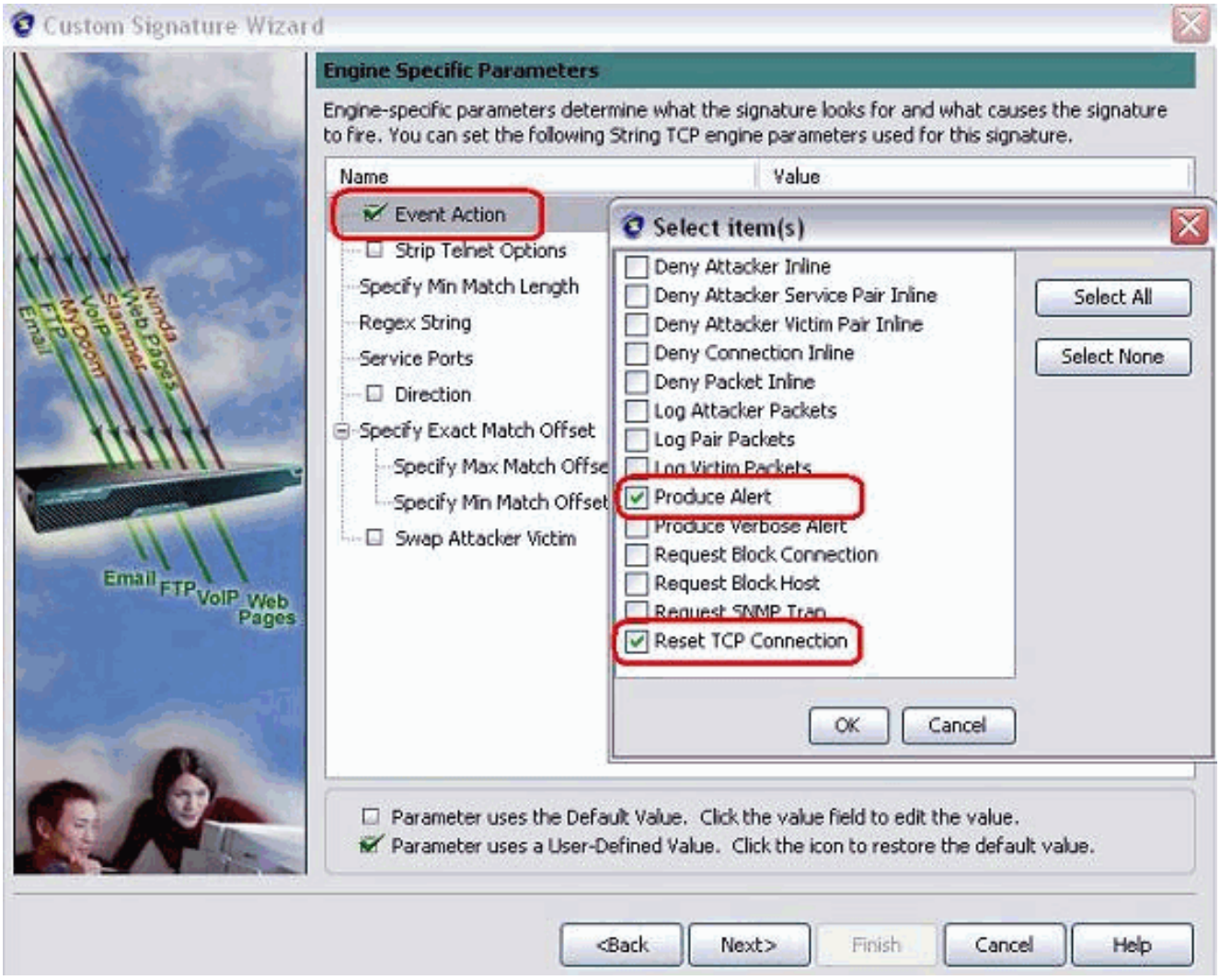
6. Dans l'assistant, choisissez **oui** et choisissez le **TCP de chaîne** comme engine de signature. Cliquez sur **Next** (Suivant).



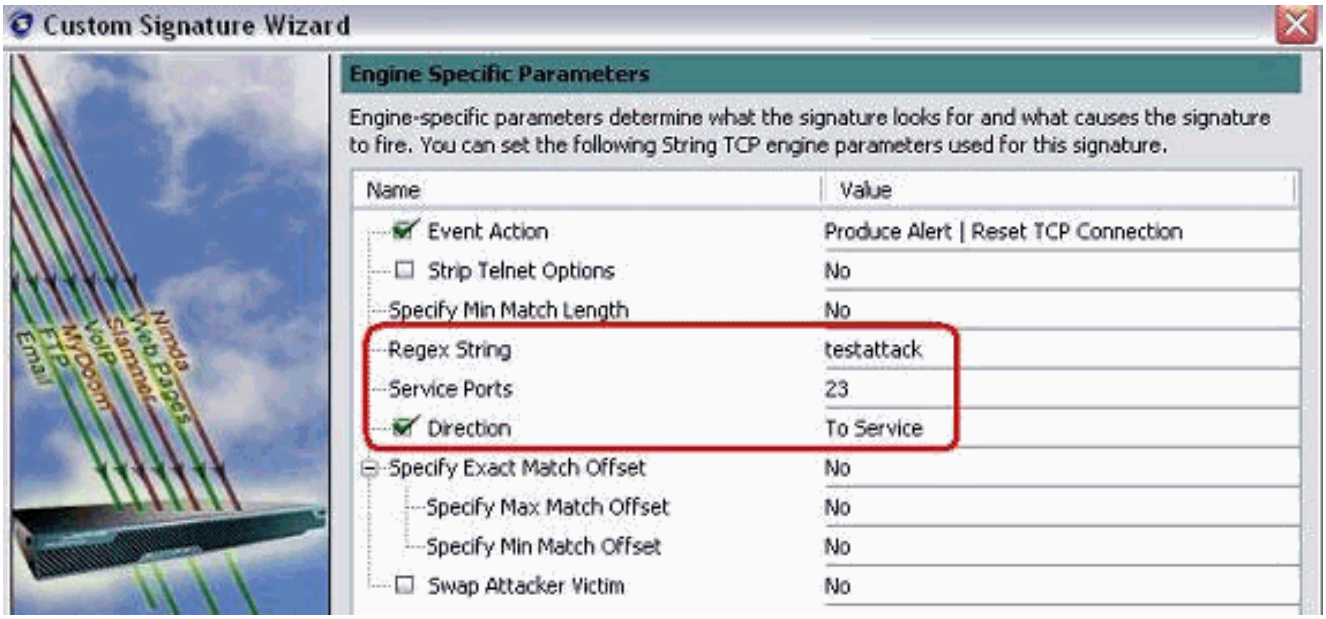
7. Vous pouvez laisser ces informations comme efdault ou écrire votre propres ID de signature, nom de signature et notes en utilisateur. Cliquez sur **Next** (Suivant).



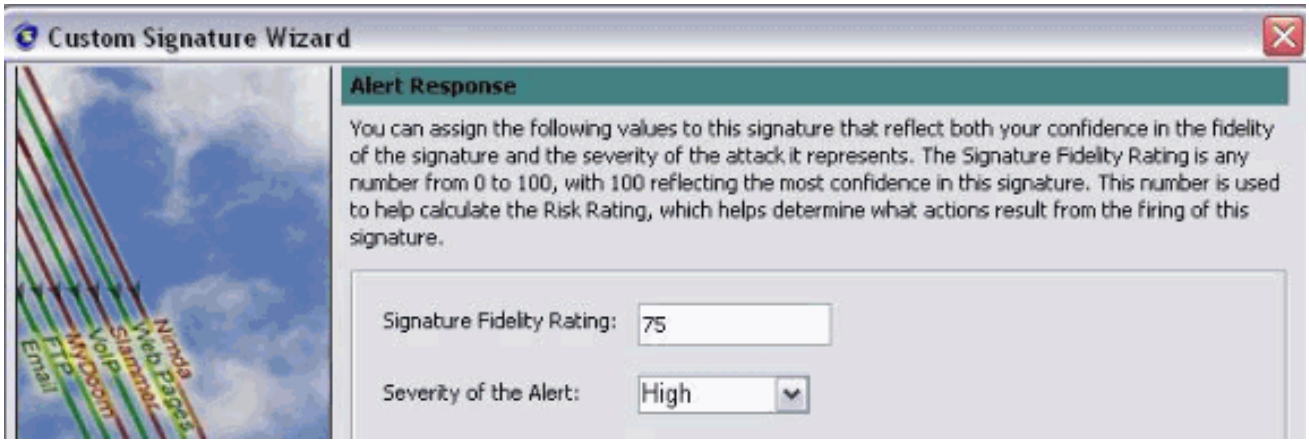
8. Choisissez l'**action d'événement**, et choisissez l'**alerte de produit** et **remettez à l'état initial la connexion TCP**. Cliquez sur OK et afin de continuer alors **ensuite**.



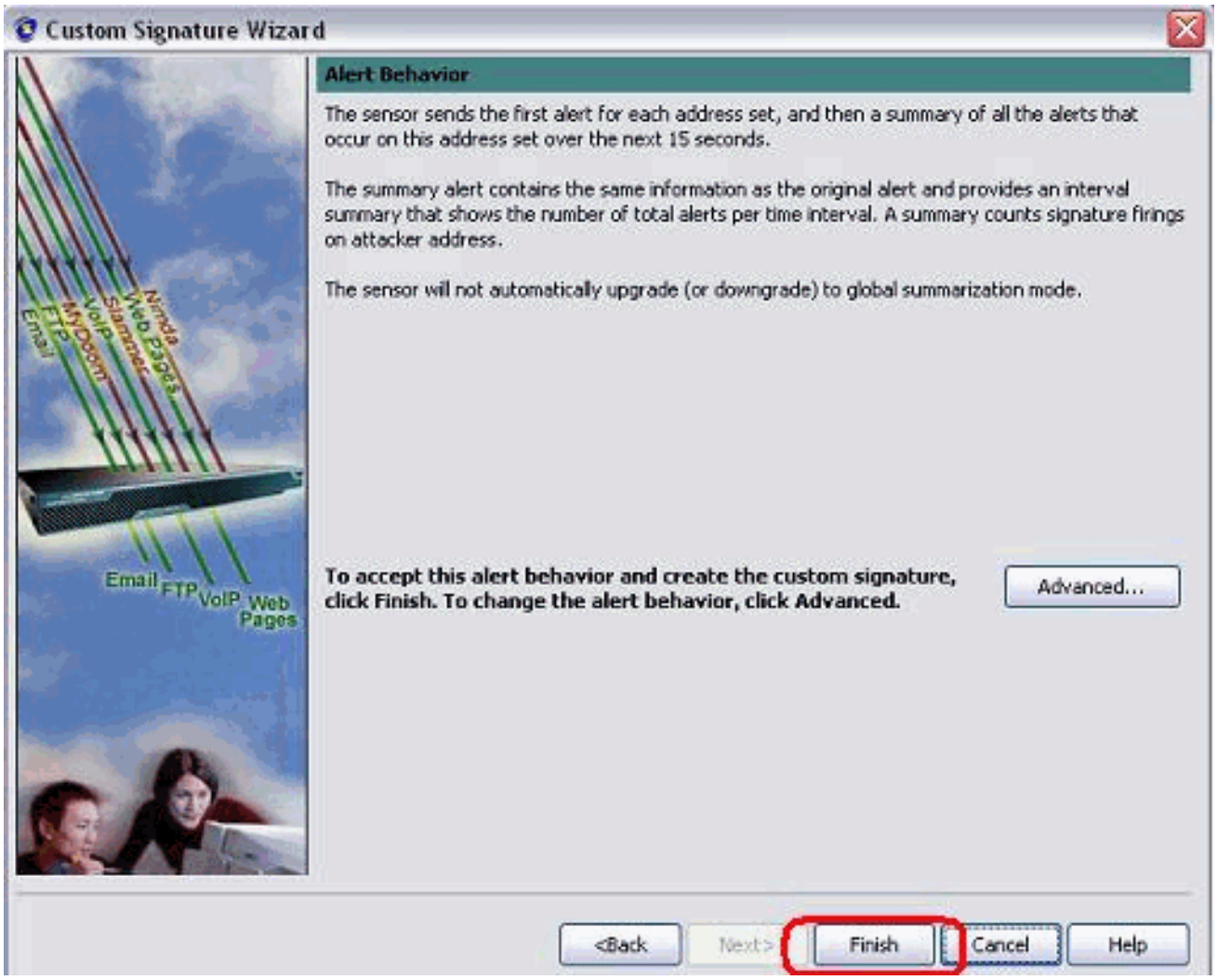
9. Écrivez une expression régulière, et le `testattack` est utilisé dans cet exemple. Écrivez **23** pour des ports de service, choisissez **d'entretenir** pour la direction, et cliquez sur Next afin de continuer.



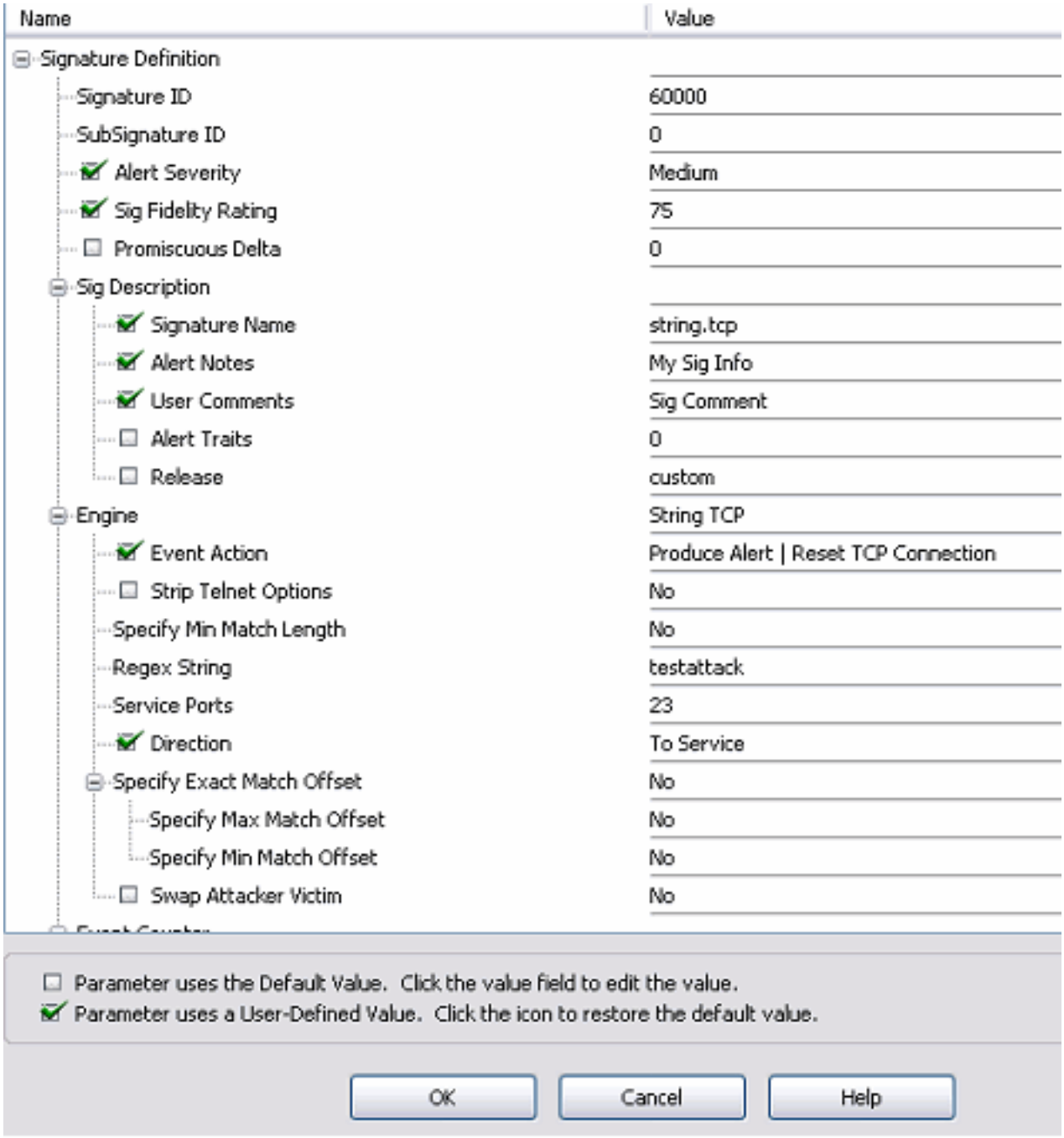
10. Vous pouvez laisser ces informations en tant que par défaut. Cliquez sur **Next** (Suivant).



11. Cliquez sur Finish afin de terminer l'assistant.



12. Choisissez la **configuration > le sig0 > les signatures actives** afin de localiser la signature de création récente près d'**ID de Sig** ou de **nom de Sig**. Cliquez sur Edit afin de visualiser la signature.



13. Cliquez sur OK après que vous confirmiez et cliquez sur le **bouton Apply** afin d'appliquer la signature au capteur.

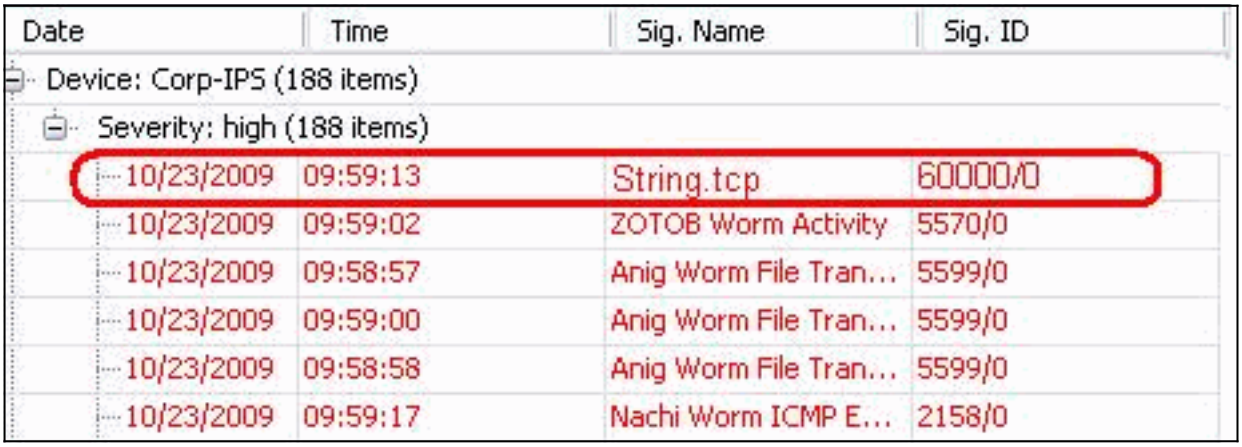
Vérifiez

Lancez l'attaque et la Réinitialisation TCP

Terminez-vous ces étapes afin de lancer l'attaque et la Réinitialisation TCP :

1. Avant que vous lanciez l'attaque, allez à l'**IME**, choisissez la **surveillance d'événement > vue relâchée d'attaques** et choisissez le capteur du côté droit.
2. De la lumière du routeur, le telnet à la Chambre de routeur et écrivent le **testattack**.Frappez le **<space>** ou le **<enter>** afin de remettre à l'état initial votre session de telnet.`light#`**`telnet 10.100.100.1`** `Trying 10.100.100.1 ... Open User Access Verification Password: house>en Password: house#`**`testattack [Connection to 10.100.100.1 closed by foreign host]`** *`!--- Telnet session has been reset due to the !--- signature "String.tcp" triggered.`*

3. Du tableau de bord du visualisateur d'événements IPS, l'alarme rouge apparaît une fois que l'attaque est
lancée.



Date	Time	Sig. Name	Sig. ID
Device: Corp-IPS (188 items)			
Severity: high (188 items)			
10/23/2009	09:59:13	String.tcp	60000/0
10/23/2009	09:59:02	ZOTOB Worm Activity	5570/0
10/23/2009	09:58:57	Anig Worm File Tran...	5599/0
10/23/2009	09:59:00	Anig Worm File Tran...	5599/0
10/23/2009	09:58:58	Anig Worm File Tran...	5599/0
10/23/2009	09:59:17	Nachi Worm ICMP E...	2158/0

Dépannez

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

Conseils

Utilisez ces conseils de dépannage :

- L'évitement établit du port de commandement et de contrôle de reprogrammer le Listes de contrôle d'accès (ACL) de routeur. Les remises de TCP sont envoyées de l'**interface de reniflement du** capteur. Quand vous **set span** dans le commutateur, utilisez la commande du **set span <src_mod/src_port><dest_mod/dest_port>** avec les deux paquets entrant activés comme affiché ici.`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`** `Multicast : enabled`
- Si les remises de TCP fonctionnent, vérifiez si l'alarme est déclenchée pour la Réinitialisation TCP de type d'action. Si l'alarme apparaît, vérifiez que le type de signature est placé à la Réinitialisation TCP.Ouvrez une session utilisant le compte des services su pour enraciner et émettre cette commande. Cette commande suppose que l'interface de détection est placée à eth0.`[root@sensor1 root]#`**`tcpdump -i eth0 -n`** **Remarque:** Cent remises de TCP obtiennent envoyé à la victime/à cible alors cent obtiennent envoyé à l'attaquant/au client.Voici un exemple de sortie :

```
03:06:00.598777 64.104.209.205.1409 >
 10.66.79.38.telnet: R 107:107(0) ack 72 win 0
03:06:00.598794 64.104.209.205.1409 >
 10.66.79.38.telnet: R 108:108(0) ack 72 win 0

03:06:00.599360 10.66.79.38.telnet >
 64.104.209.205.1409: R 72:72(0) ack 46 win 0
03:06:00.599377 10.66.79.38.telnet >
 64.104.209.205.1409: R 73:73(0) ack 46 win 0
```

Informations connexes

- Page de support Cisco Secure de prévention des intrusions
- Documentation pour le système de prévention des intrusions Cisco Secure
- Support et documentation techniques - Cisco Systems