Configuration du blocage IPS avec IME

Contenu

Introduction

Ce document discute la configuration du Système de prévention d'intrusion (IPS) bloquant avec l'utilisation du Manager Express IPS (IME). Des capteurs IME et IPS sont utilisés pour gérer un routeur de Cisco pour le blocage. Souvenez-vous ces éléments quand vous considérez cette configuration :

- 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.

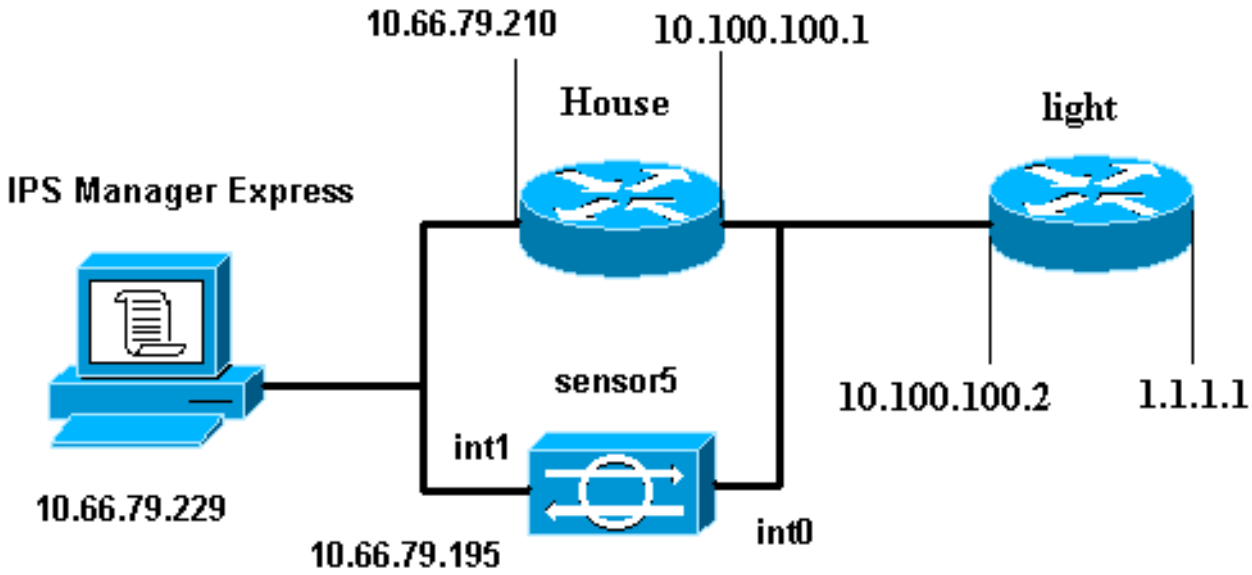
Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez

Diagramme du réseau

Ce document utilise cette configuration du réseau.



Configurations

Ce document utilise les configurations suivantes.

- 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 ip access-group IDS_FastEthernet0/1_in_0
in !--- After you configure blocking, !--- IDS Sensor
inserts this line. 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 ! ! ip access-list extended
IDS_FastEthernet0/1_in_0 permit ip host 10.66.79.195 any
permit ip any any !--- After you configure blocking, !--
- IDS Sensor inserts this line. ! 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 se connectant 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 suivez le système invite pour 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 time: Thu Oct 22 21:19:51 2009 Setup Configuration last modified: Enter host
name[sensor]: Enter IP interface[10.66.79.195/24,10.66.79.193]: Modify current access
list?[no]: Current access list entries: !--- permit the ip address of workstation or
network with IME Permit:10.66.79.0/24 Permit: Modify system clock settings?[no]: Modify
summer time settings?[no]: Use USA SummerTime Defaults?[yes]: Recurring, Date or
Disable?[Recurring]: Start Month[march]: Start Week[second]: Start Day[sunday]: Start
Time[02:00:00]: End Month[november]: End Week[first]: End Day[sunday]: End Time[02:00:00]:
DST Zone[]: Offset[60]: Modify system timezone?[no]: Timezone[UTC]: UTC Offset[0]: Use
NTP?[no]: yes NTP Server IP Address[]: Use NTP Authentication?[no]: yes NTP Key ID[]: 1 NTP
Key Value[]: 8675309
```

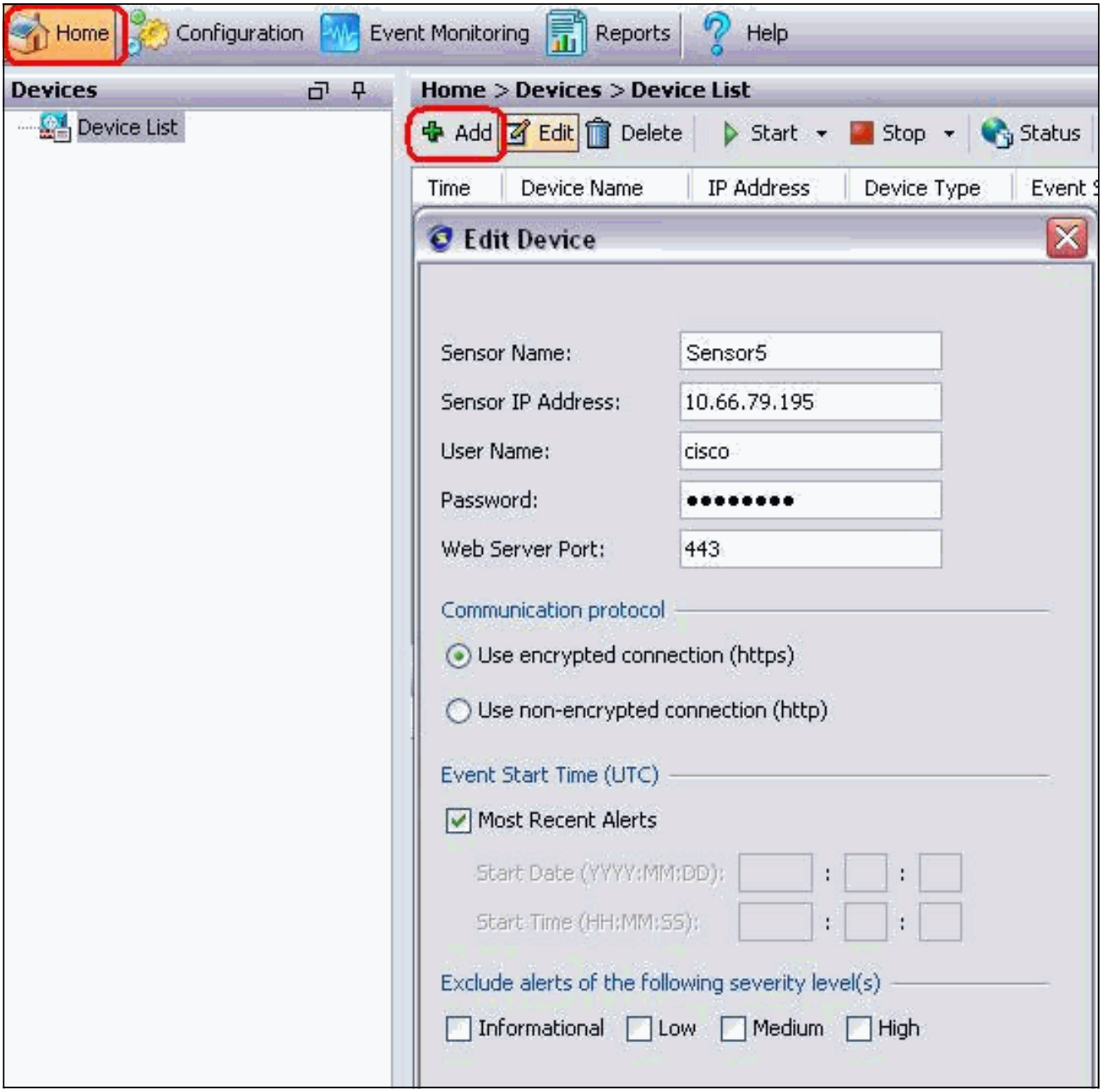
5. Enregistrez la configuration.Il peut prendre quelques minutes pour que le capteur sauvegarde la configuration.
```
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.

Enter your selection[2]: 2
```

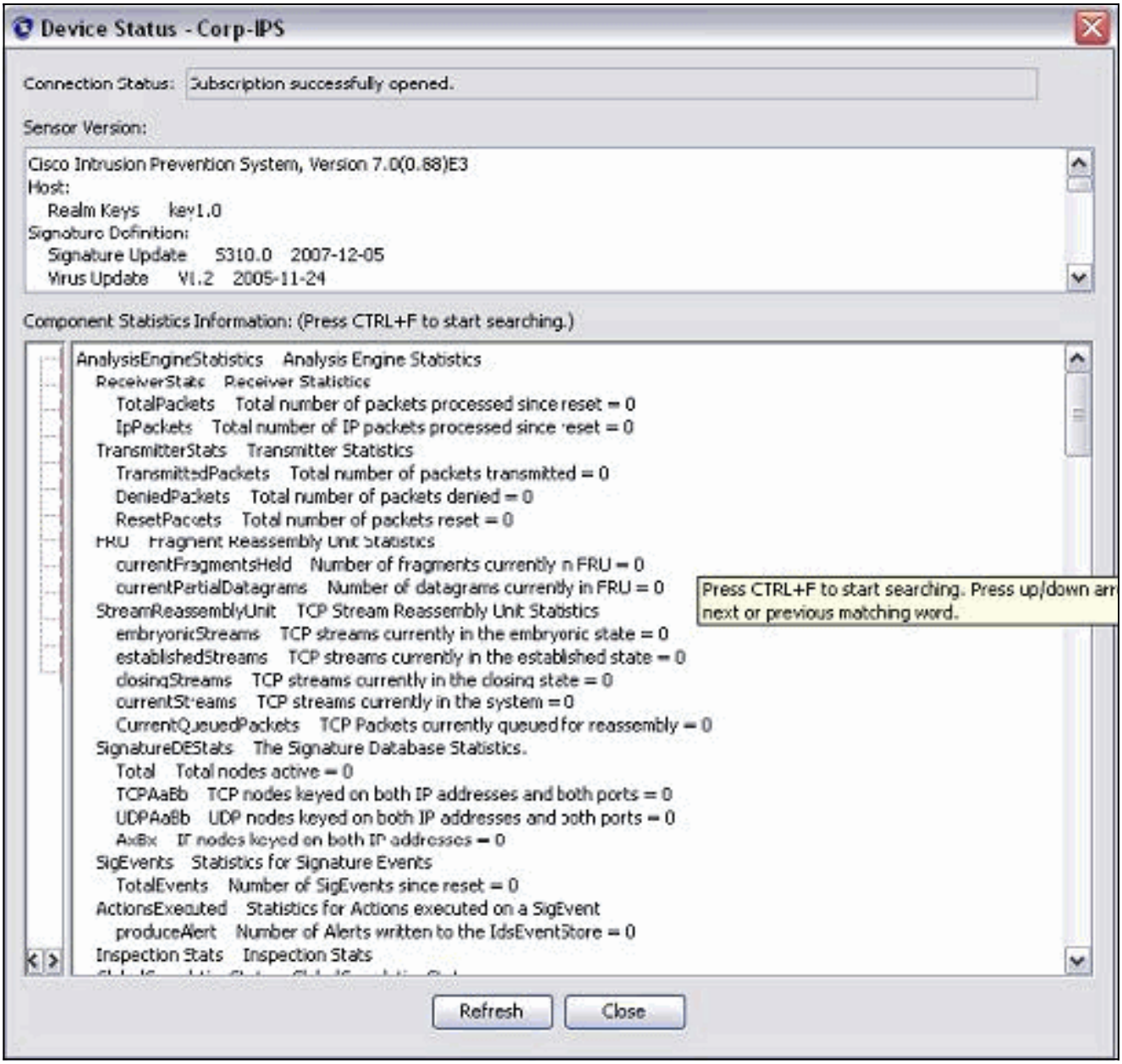
Ajoutez le capteur dans l'IME

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 ouvre le **Manager Express IPS**.
2. Choisissez **à la maison > ajoutent**.
3. Saisissez ces informations et cliquez sur OK afin de terminer la configuration.



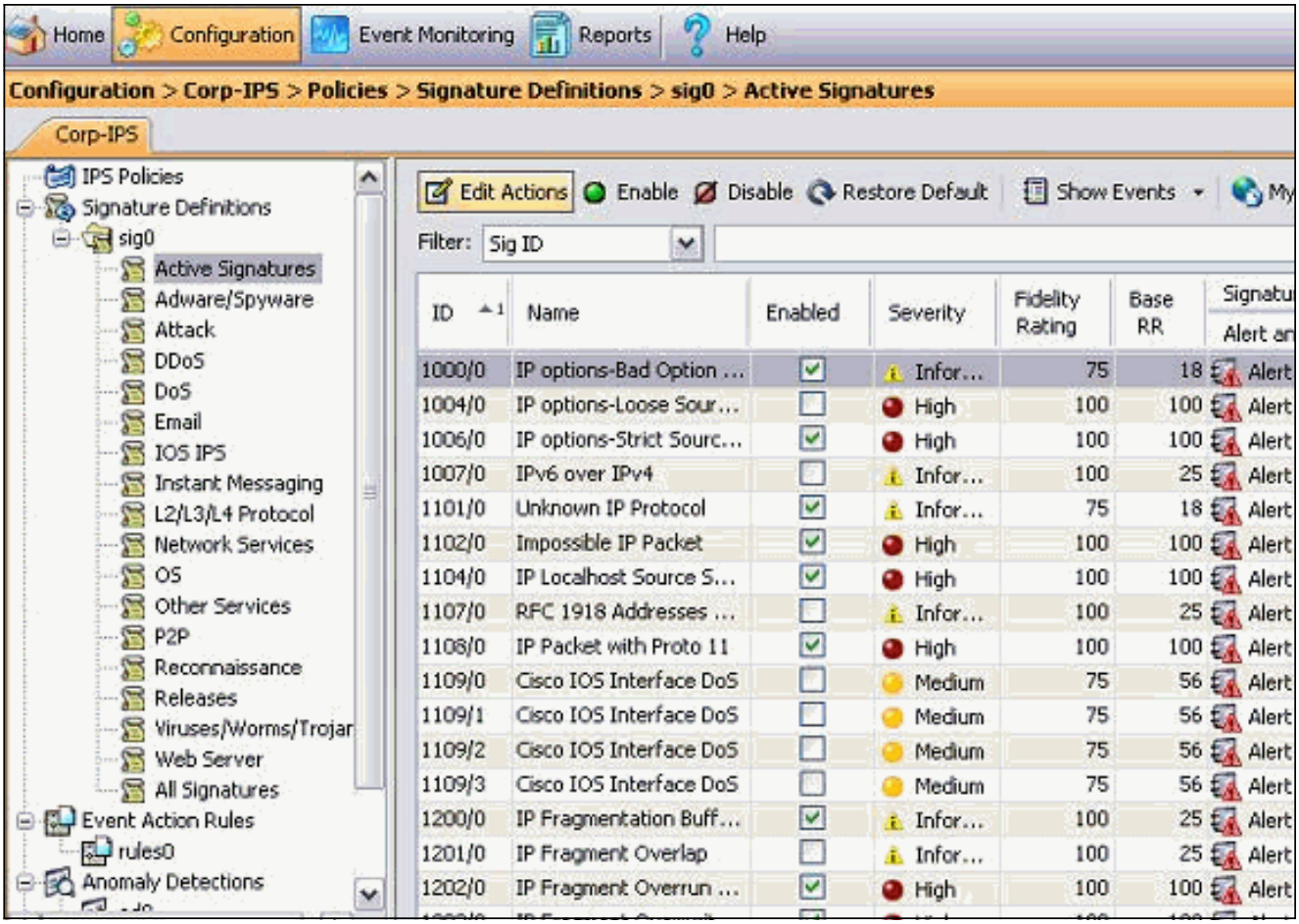
4. Choisissez les **périphériques > le sensor5** afin de vérifier l'état de capteur et puis cliquer avec le bouton droit pour choisir l'**état**.Assurez-vous que vous pouvez voir l'*abonnement avec succès ouvert.*
message.



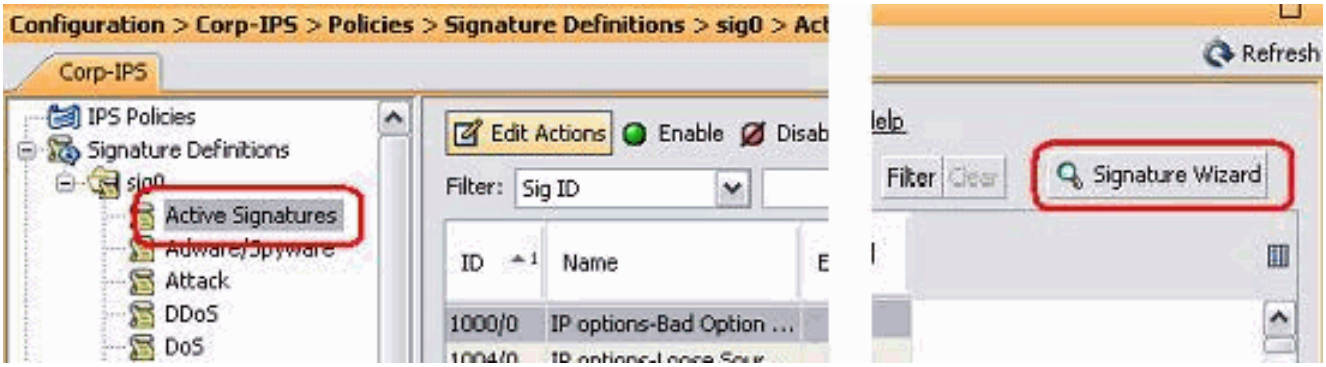
Configurez le blocage pour le routeur Cisco IOS

Terminez-vous ces étapes afin de configurer le blocage pour l'artère de 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
   :

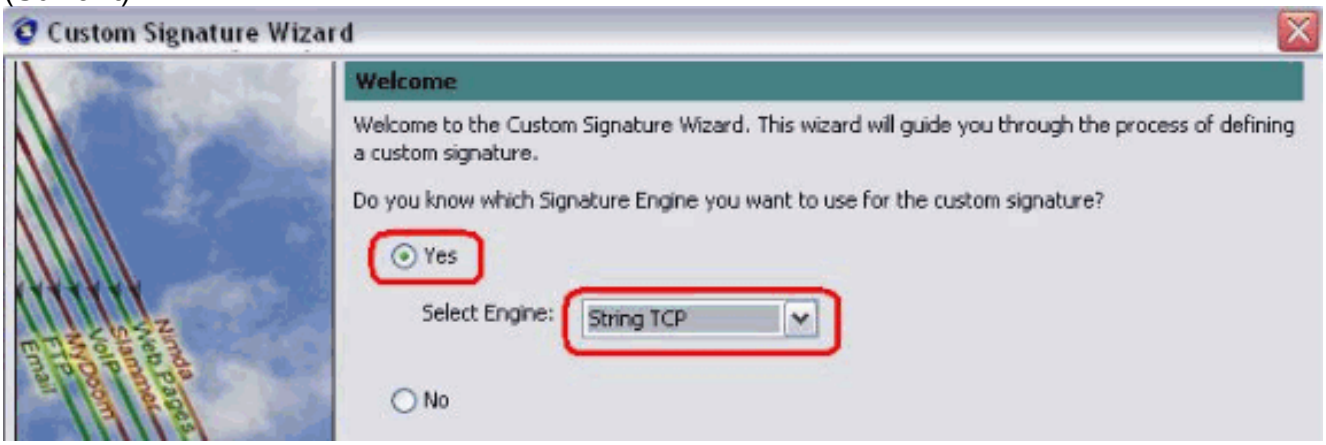


4. De l'onglet de configuration, cliquez sur les **signatures actives**.
5. Puis, **assistant de signature de**
   clic.

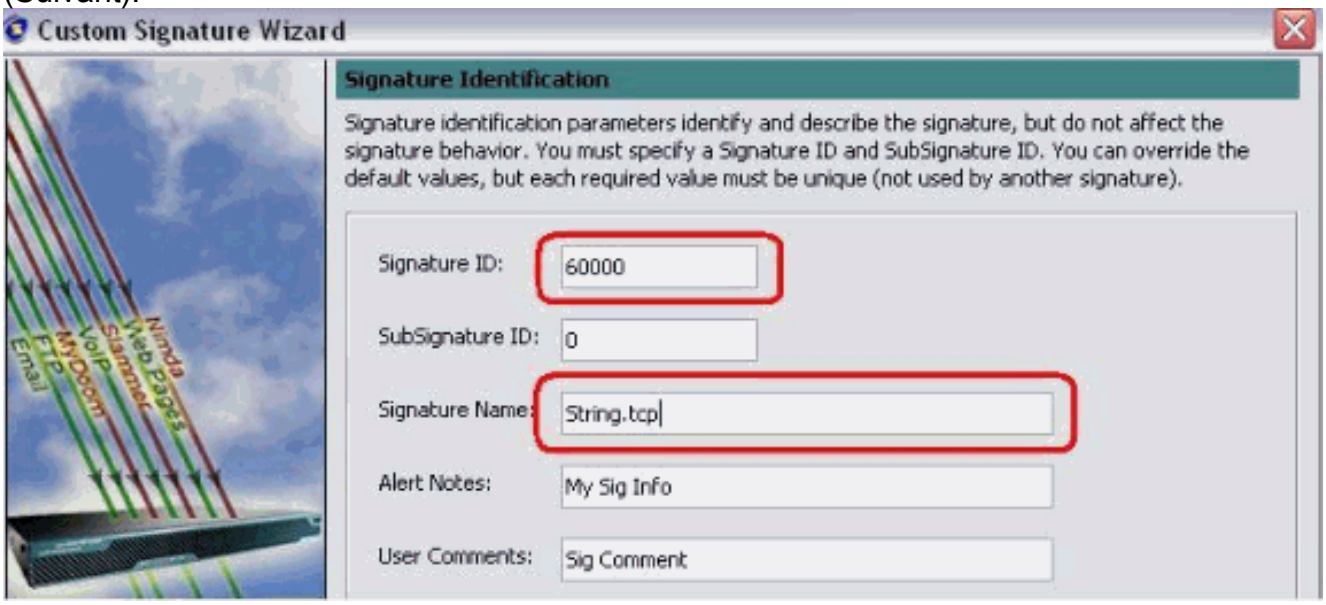


Remarque: Le tir d'écran précédent a été coupé en deux parts en raison de la limite de l'espace.

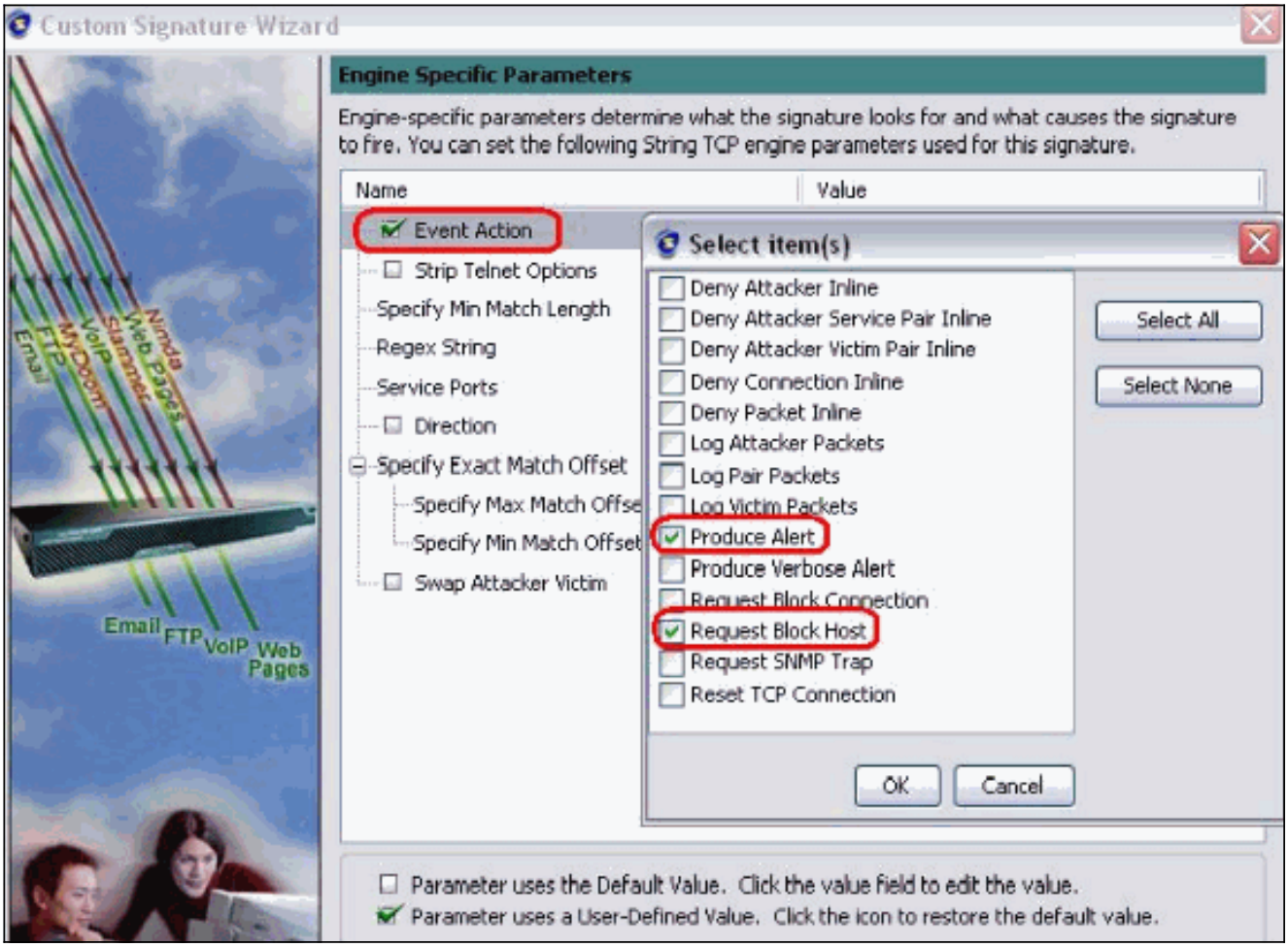
6. Choisissez **oui** et **ficelez le TCP** comme engine de signature. Cliquez sur **Next** (Suivant).



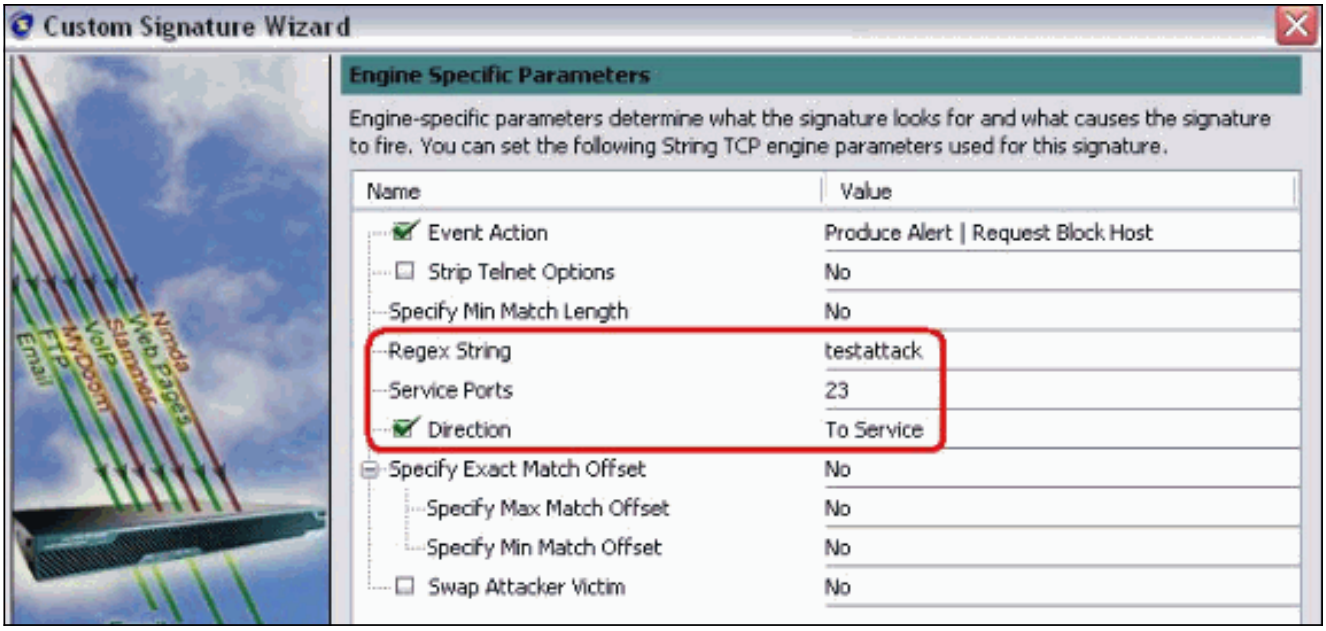
7. Vous pouvez laisser ces informations comme par défaut ou écrire votre propres ID de signature, nom de signature et notes en utilisateur. Cliquez sur **Next** (Suivant).



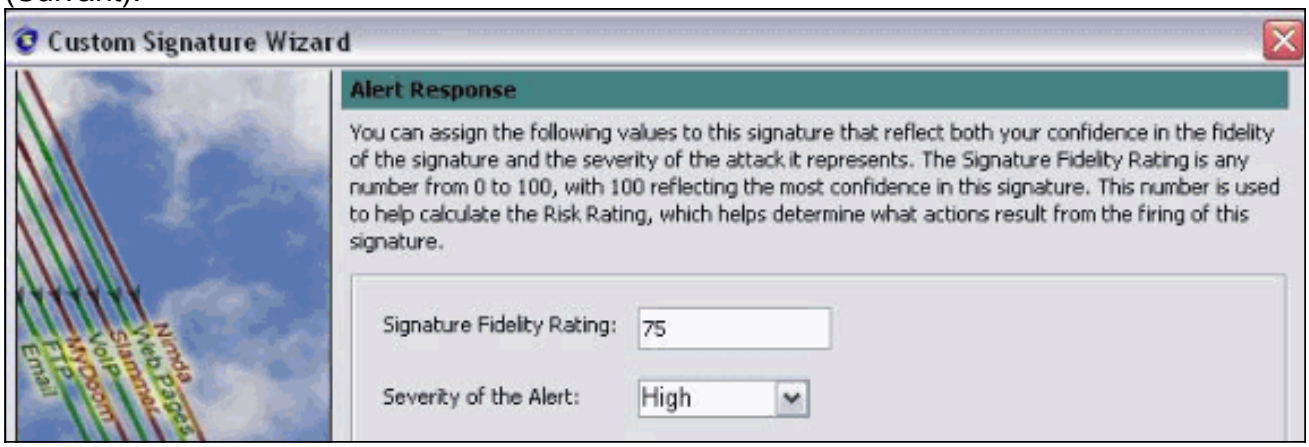
8. Choisissez l'**action d'événement** et choisissez l'**alerte de produit** et l'**hôte de bloc de demande**. Cliquez sur Next afin de continuer.



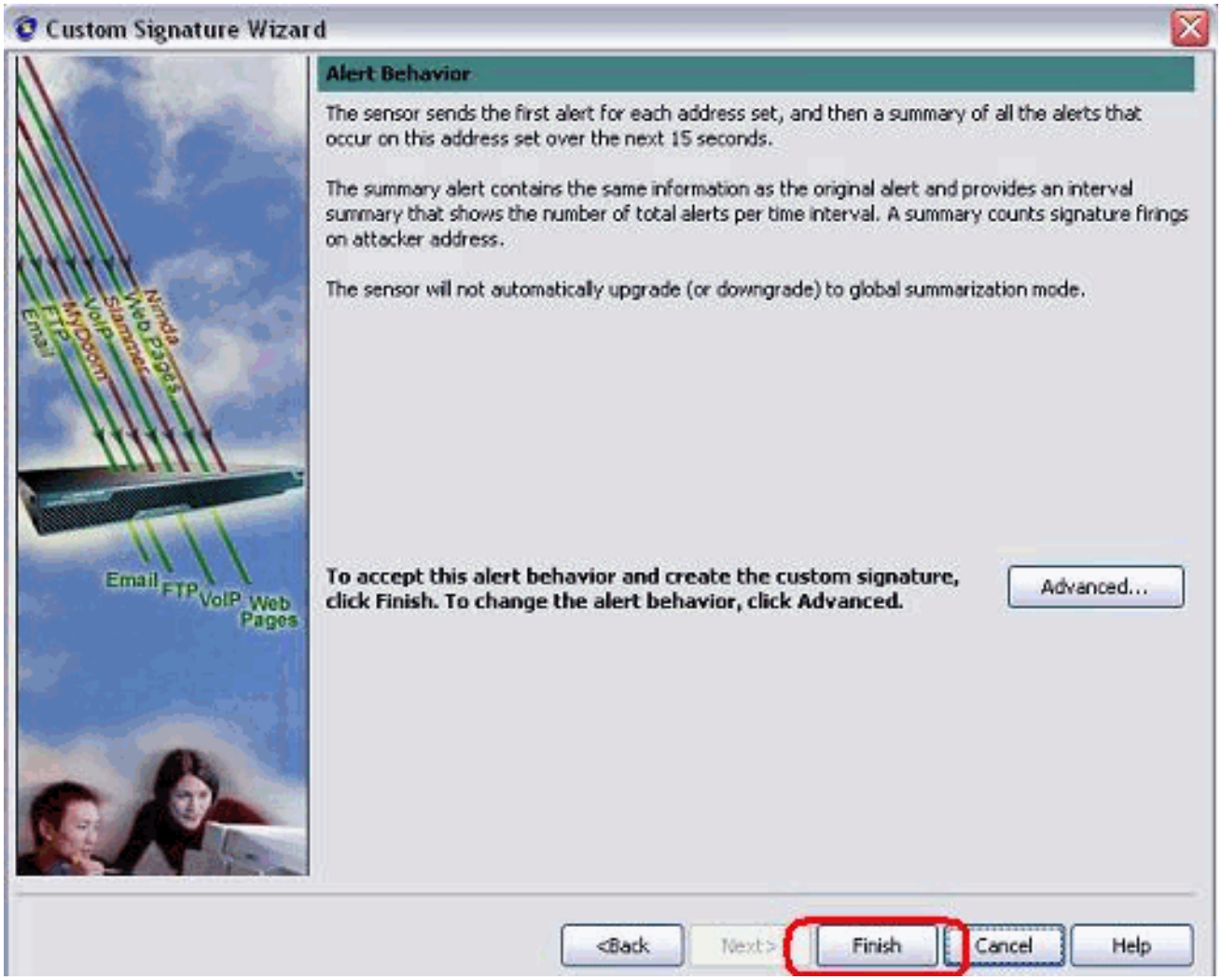
9. Écrivez une expression régulière, qui dans cet exemple est *testattack*, écrivent **23** pour des ports de service, choisissent **d'entretenir** pour la direction, et cliquent sur Next afin de continuer.



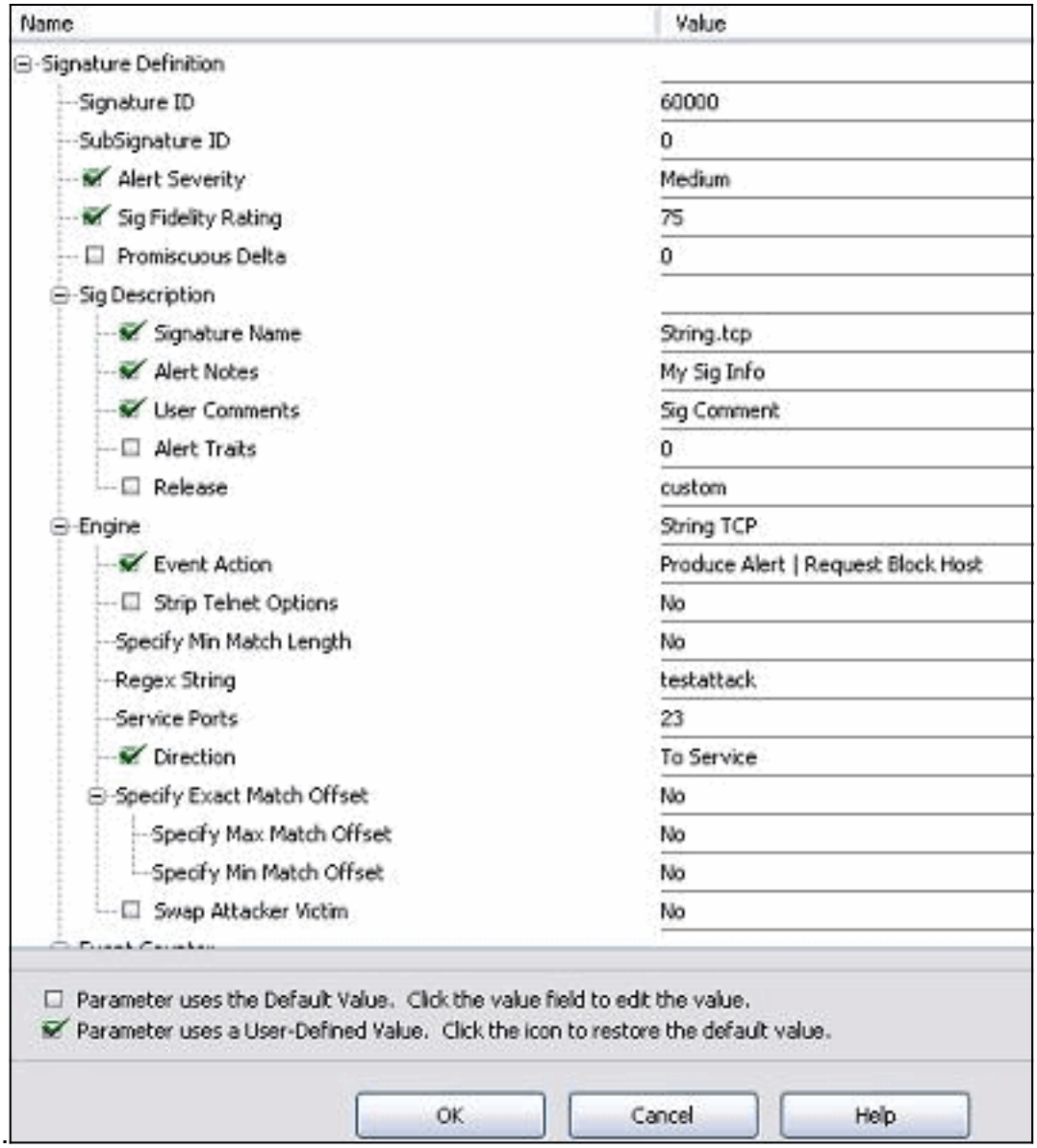
10. Vous pouvez laisser ces informations en tant que par défaut. Cliquez sur **Next** (Suivant).



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

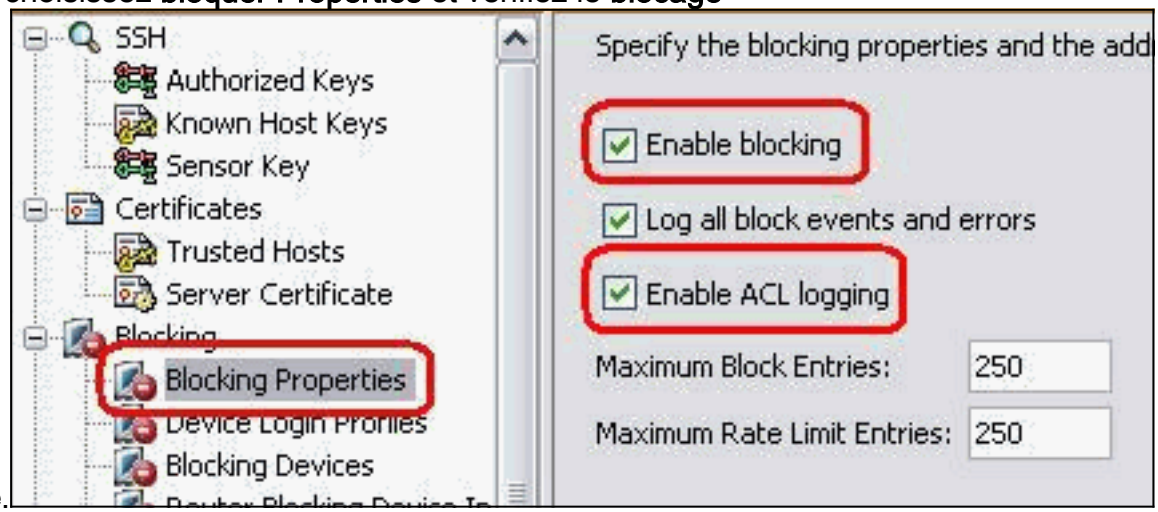


12. Choisissez la **configuration > le sig0 > les signatures actives** dans la commande localisent la signature de création récente près d'**ID de Sig** ou de **nom de Sig**. Cliquez sur Edit afin de visualiser la



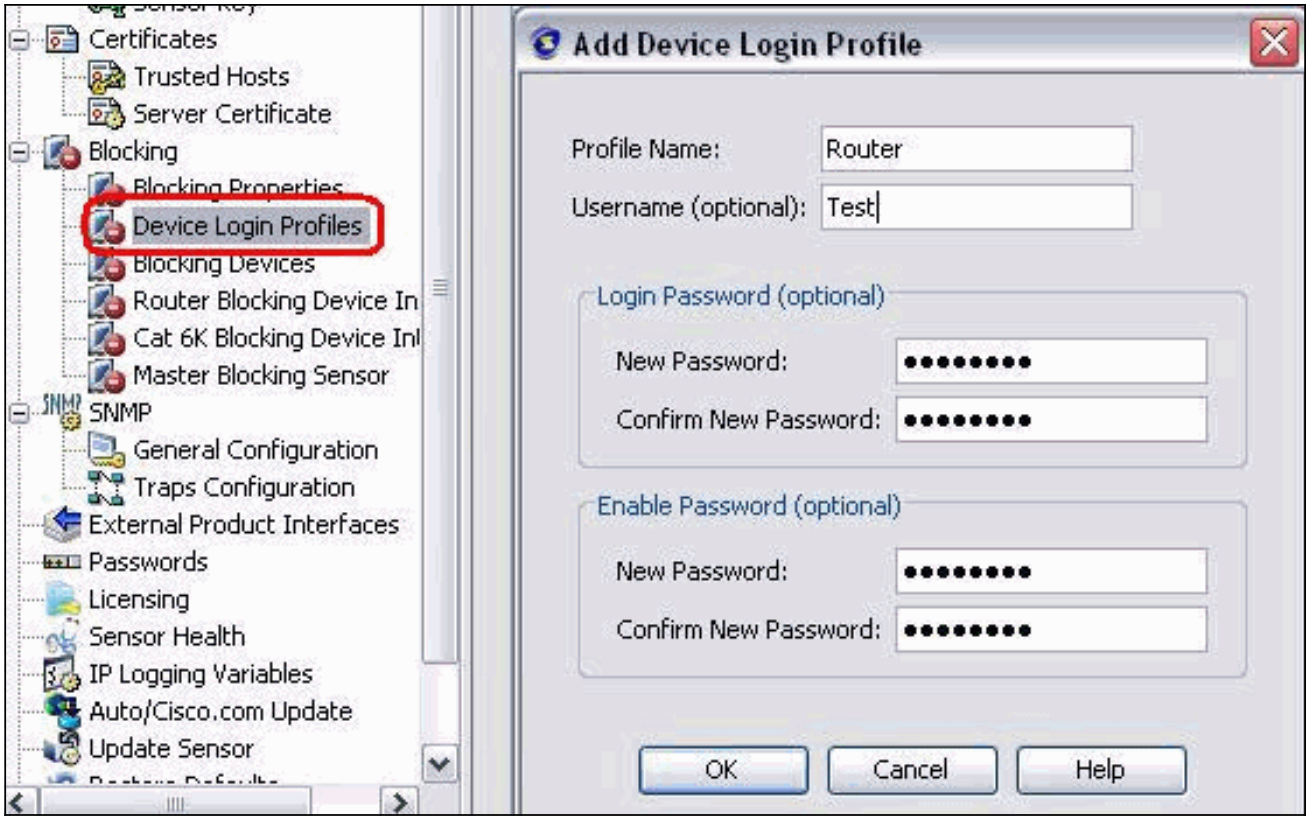
signature.

13. Cliquez sur OK après que vous confirmiez et cliquez sur le **bouton Apply** afin d'appliquer la signature au capteur.
14. De l'onglet de configuration, sous le **blocage de** clic de Gestion de capteur. Du volet gauche, choisissez **bloquer Properties** et vérifiez le **blocage**

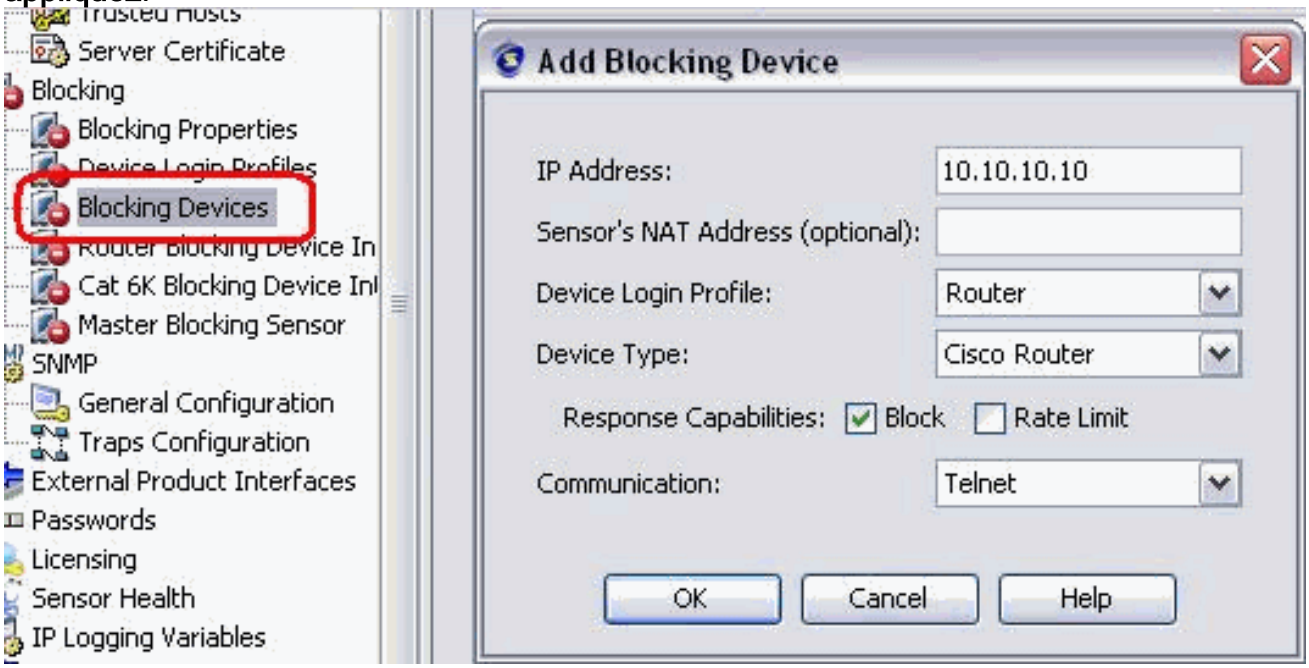


d'enable.

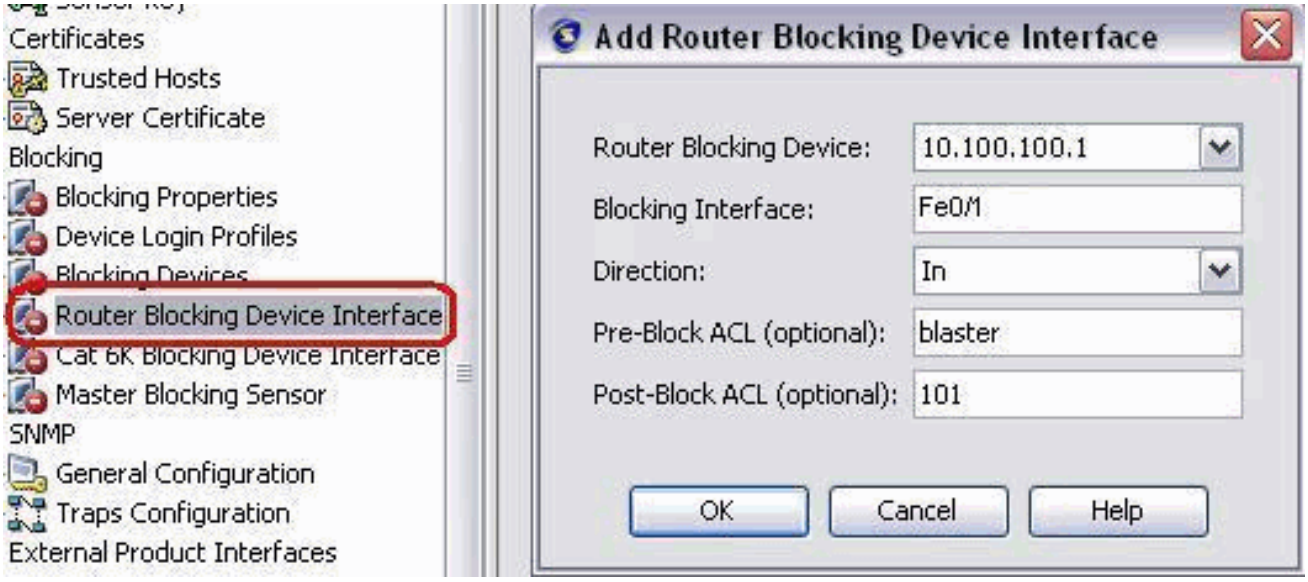
15. Maintenant du volet gauche, allez au **profil de procédure de connexion de périphérique**. Afin de créer un nouveau profil, cliquez sur Add. Une fois créé cliquez sur OK et **appliquez le** capteur et
continuez.



16. L'étape suivante est de configurer le routeur en tant que périphérique en mode bloc. Du volet gauche, choisissez le **périphérique en mode bloc**, cliquent sur Add afin d'ajouter ces informations. Alors cliquez sur OK et **appliquez**.



17. Maintenant du volet gauche configurez les interfaces de périphérique de blocage. Ajoutez les informations, cliquez sur OK et **appliquez**.



Vérifiez

Lancez l'attaque et le blocage

Terminez-vous ces étapes pour lancer l'attaque et le blocage :

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. Le telnet à la Chambre de routeur et vérifient la transmission du serveur avec ces commandes.`house#**show user** Line User Host(s) Idle Location * 0 con 0 idle 00:00:00 226 vty 0 idle 00:00:17 10.66.79.195 house#**show access-list** Extended IP access list IDS_FastEthernet0/1_in_0 permit ip host 10.66.79.195 any permit ip any any (12 matches) house#`
3. De la lumière du routeur, telnet à la Chambre de routeur et au **testattack de** type.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 lost]** *!--- Host 10.100.100.2 has been blocked due to the !--- signature "testattack" triggered.*`
4. Le telnet à la Chambre de routeur et utilisent la **commande access-list d'exposition** comme affiché ici.`house#**show access-list** Extended IP access list IDS_FastEthernet0/1_in_0 10 permit ip host 10.66.79.195 any **20 deny ip host 10.100.100.2 any (71 matches)** 30 permit ip any any`
5. Du tableau de bord du visualisateur d'événements d'ID, 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 :

- Du capteur regardez l'**accès au réseau de statistiques d'exposition** sorti et assurez-vous que l'`état` " est en activité. De la console ou du SSH au capteur, ces informations sont visualisées :
```
sensor5#show statistics network-access Current Configuration AllowSensorShun = false
ShunMaxEntries = 100 NetDevice Type = Cisco IP = 10.66.79.210 NATAddr = 0.0.0.0
Communications = telnet ShunInterface InterfaceName = FastEthernet0/1 InterfaceDirection =
in State ShunEnable = true NetDevice IP = 10.66.79.210 AclSupport = uses Named ACLs State =
Active ShunnedAddr Host IP = 10.100.100.2 ShunMinutes = 15 MinutesRemaining = 12 sensor5#
```
- Assurez-vous que le paramètre de transmission prouve que le protocole correct est utilisé comme le telnet ou le SSH avec 3DES. Vous pouvez essayer un SSH manuel ou le telnet d'un client SSH/Telnet sur un PC afin de vérifier les qualifications de nom d'utilisateur et mot de passe sont correct. Puis l'essai au telnet ou le SSH du capteur lui-même au routeur et voient si vous pouvez ouvrir une session avec succès au routeur.

Informations connexes

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