IPS 5.X et versions ultérieures/IDSM2 : Exemple de configuration de réseaux VLAN en ligne en mode paire à l'aide de l'interface CLI et d'IDM

Contenu

Introduction

L'association des VLAN dans les paires sur une interface physique est connue en tant que mode intégré de paires VLAN. Des paquets reçus sur un des VLAN appareillés sont analysés et expédiés à l'autre VLAN dans les paires. Des paires intégrées VLAN sont prises en charge sur tous les capteurs qui sont compatibles avec le Système de prévention d'intrusion (IPS) 5.1, excepté NM-CIDS, AIP-SSM-10, et AIP-SSM-20.

Le mode intégré de paires VLAN est un mode de détection actif où une interface de détection agit en tant que port de joncteur réseau de 802.1Q, et le capteur exécute le VLAN jetant un pont sur entre les paires de VLAN sur le joncteur réseau. Ceci signifie que le commutateur connecté à l'interface de détection doit être en mode de joncteur réseau.

Le capteur examine le trafic qu'il reçoit sur chaque VLAN dans chaque paire, et peut en avant les paquets sur l'autre VLAN dans les paires ou relâcher le paquet si une tentative d'intrusion est détectée. Vous pouvez configurer un capteur IPS pour jeter un pont sur simultanément jusqu'à 255 paires VLAN sur chaque interface de détection. Le capteur remplace le champ d'ID DE VLAN dans l'en-tête de 802.1Q de chaque paquet reçu par l'ID du de sortie VLAN sur lequel le capteur en avant le paquet. Le capteur relâche tous les paquets reçus sur tous les VLAN qui ne sont pas assignés aux paires intégrées VLAN.

Remarque: Pour IPS-4260, le contournement échec-ouvert de matériel n'est pas pris en charge sur des paires intégrées VLAN. Référez-vous au pour en savoir plus de restrictions de configuration de contournement de matériel.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur le capteur de Système de protection contre les intrusions Cisco qui utilise les 5.1 et plus tard.

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.

Produits connexes

Les informations dans ce document s'appliquent également au Module de services du système de détection d'intrusion (IDSM-2).

Conventions

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

Configuration de capture VACL

Référez-vous à la section configurante de capture VACL de configurer IDSM-2 afin d'envoyer le trafic à l'IDSM sur le commutateur.

Configuration de mode intégrée de paires VLAN

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

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Employez la commande d'**interface_name de physicaux-interface** dans le sous-mode d'interface de service afin de configurer des paires intégrées VLAN utilisant le CLI. Le nom d'interface est FastEthernet ou GigabitEthernet.

Ces options s'appliquent :

- **admin-état {activé | handicapé}** — l'état de lien administratif de l'interface, si l'interface est activée ou désactivée.**Remarque:** Sur tout le fond de panier sentant des interfaces sur tous les modules (IDSM-2 NM-CIDS, et AIP SSM), l'admin-état est placé à activer et est protégé

(vous ne pouvez pas changer la configuration). L'admin-état n'exerce aucun effet (et est protégé) sur l'interface de commandement et de contrôle. Il affecte seulement sentir des interfaces. L'interface de commandement et de contrôle n'a pas besoin d'être activée parce qu'elle ne peut pas être surveillée.

- **ensembles par défaut la** valeur de nouveau à la configuration de paramètres systèmes par défaut.
- **description** — Votre description des paires intégrées d'interface.
- **duplex** — Le paramètre bidirectionnel de l'interface.**automatique** — Place l'interface à l'automatique négocient le duplex.**ensembles complets l'**interface au bidirectionnel simultané.**moitié** — Place l'interface au semi duplex.**Remarque:** L'option duplex est protégée sur tous les modules.
- **NO-** retire une configuration d'entrée ou de sélection.
- **vitesse** — La configuration de débit de l'interface.**automatique** — Place l'interface à l'automatique négocient la vitesse.**10** — Place l'interface à 10 Mo (pour des interfaces TX seulement).**100** — Place l'interface à 100 Mo (pour des interfaces TX seulement).**1000** — Place l'interface à 1 Go (pour des interfaces de gigabit)**Remarque:** L'option de vitesse est protégée sur tous les modules.
- **sous-interface-type** — Spécifie que l'interface est une sous-interface et quel type de sous-interface est défini.**en ligne-VLAN-paires** — Vous permet de définir la sous-interface comme paire de l'en ligne VLAN.**aucun** — Aucune sous-interface définie.
- **sous-interface** — Définit la sous-interface comme paire de l'en ligne VLAN.**vlan1** — Le premier VLAN dans les paires de l'en ligne VLAN.**vlan2** — Le deuxième VLAN dans les paires de l'en ligne VLAN.

Configuration CLI

Terminez-vous ces étapes afin de configurer les configurations de paires de l'en ligne VLAN sur le capteur utilisant le CLI :

1. Ouvrez une session au CLI utilisant un compte avec des privilèges d'administrateur.
2. Écrivez le sous-mode d'interface :
```
sensor#configure terminal
sensor(config)#service interface
sensor(config-int)#
```
3. Vérifiez si des interfaces intégrées existent (le type de sous-interface devrait n'en lire « aucun » si aucune interface intégrée n'a été configurée) :
```
sensor(config-int)#show settings
   physical-interfaces (min: 0, max: 999999999, current: 2)
   ----------------------------------------------
      <protected entry>
      name: GigabitEthernet0/0 <defaulted>
      ----------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <protected>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ----------------------------------------------
            none
            ----------------------------------------------
            ----------------------------------------------
         ----------------------------------------------
```

```
         subinterface-type
         ---------------------------------------------
            none
            ---------------------------------------------
            ---------------------------------------------
         ---------------------------------------------
      ---------------------------------------------
<protected entry>
      name: GigabitEthernet0/1 <defaulted>
      ---------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <defaulted>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ---------------------------------------------
            none
            ---------------------------------------------
            ---------------------------------------------
         ---------------------------------------------
         subinterface-type
         ---------------------------------------------
            none
            ---------------------------------------------
            ---------------------------------------------
         ---------------------------------------------
      ---------------------------------------------
      <protected entry>
      name: GigabitEthernet0/2 <defaulted>
      ---------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <defaulted>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ---------------------------------------------
            none
            ---------------------------------------------
            ---------------------------------------------
         ---------------------------------------------
         subinterface-type
         ---------------------------------------------
            none
            ---------------------------------------------
            ---------------------------------------------
         ---------------------------------------------
      ---------------------------------------------
      <protected entry>
      name: GigabitEthernet0/3 <defaulted>
      ---------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <defaulted>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ---------------------------------------------
            none
            ---------------------------------------------
            ---------------------------------------------
         ---------------------------------------------
         subinterface-type
```

```
         ---------------------------------------------
            none
            ---------------------------------------------
            ---------------------------------------------
         ---------------------------------------------
      ---------------------------------------------
      <protected entry>
      name: Management0/0 <defaulted>
      ---------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <protected>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ---------------------------------------------
            none
            ---------------------------------------------
            ---------------------------------------------
         ---------------------------------------------
         subinterface-type
         ---------------------------------------------
            none
            ---------------------------------------------
            ---------------------------------------------
         ---------------------------------------------
      ---------------------------------------------
   ---------------------------------------------
   command-control: Management0/0 <protected>
   inline-interfaces (min: 0, max: 999999999, current: 0)
   ---------------------------------------------
   ---------------------------------------------
   bypass-mode: auto <defaulted>
   interface-notifications
   ---------------------------------------------
      missed-percentage-threshold: 0 percent <defaulted>
      notification-interval: 30 seconds <defaulted>
      idle-interface-delay: 30 seconds <defaulted>
   ---------------------------------------------
sensor(config-int)#
```

4. Retirez toutes les interfaces intégrées qui utilisent cette interface physique :
   ```
   sensor(config-int)#no inline-interfaces interface_name
   ```

5. Affichez la liste d'interfaces disponibles :
   ```
   sensor(config-int)#physical-interfaces ?
   GigabitEthernet0/0     GigabitEthernet0/0 physical interface.
   GigabitEthernet0/1     GigabitEthernet0/1 physical interface.
   GigabitEthernet0/2     GigabitEthernet0/2 physical interface.
   GigabitEthernet0/3     GigabitEthernet0/3 physical interface.
   Management0/0          Management0/0 physical interface.
   sensor(config-int)#physical-interfaces
   ```

6. Spécifiez une interface :
   ```
   sensor(config-int)#physical-interfaces GigabitEthernet0/2
   ```

7. Activez l'admin-état de l'interface :
   ```
   sensor(config-int-phy)#admin-state enabled
   ```

   L'interface doit être assignée au capteur virtuel et être activée afin de surveiller le trafic.

8. Ajoutez une description de cette interface :

```
sensor(config-int-phy)#description INT1
```

9. Configurez les paramètres bidirectionnels :
```
sensor(config-int-phy)#duplex full
```

   Cette option n'est pas disponible sur des modules.
10. Configurez la vitesse :
```
sensor(config-int-phy)#speed 1000
```

    Cette option n'est pas disponible sur des modules.
11. Installez les paires de l'en ligne VLAN :
```
sensor(config-int-phy)#subinterface-type inline-vlan-pair
sensor(config-int-phy-inl)#subinterface 1
sensor(config-int-phy-inl-sub)#vlan1 52
sensor(config-int-phy-inl-sub)#vlan2 53
```

12. Ajoutez une description pour les paires de l'en ligne VLAN :
```
sensor(config-int-phy-inl-sub)#description pairs vlans 52 and 53
```

13. Vérifiez les configurations de paires de l'en ligne VLAN :
```
sensor(config-int-phy-inl-sub)#show settings
   subinterface-number: 1
   ------------------------------------------------
      description: VLANpair1 default:
      vlan1: 52
      vlan2: 53
   ------------------------------------------------
sensor(config-int-phy-inl-sub)#
```
14. Quittez le sous-mode d'interface :
```
sensor(config-int-phy-inl-sub)#exit
sensor(config-int-phy-inl)#exit
sensor(config-int-phy)#exit
sensor(config-int)#exit
Apply Changes:?[yes]:
```
15. Appuyez sur **entrent** afin d'appliquer les modifications, ou entrent **non** pour les jeter.
16. Écrivez le mode de configuration virtuel de capteur :
```
sensor(config)#service analysis-engine
        sensor(config-ana)#virtual-sensor vs0
```

17. Ajoutez l'interface au virtuel-capteur :
```
sensor(config-ana-vir)#physical-interface GigabitEthernet0/2
subinterface-number 1
```

18. Quittez le sous-mode de virtuel-capteur :
```
sensor(config-ana-vir)#exit
        sensor(config-ana)#exit
        Apply Changes:?[yes]:
```
19. Appuyez sur **entrent** afin d'appliquer les modifications, ou entrent **non** pour les jeter.

Configuration IDM

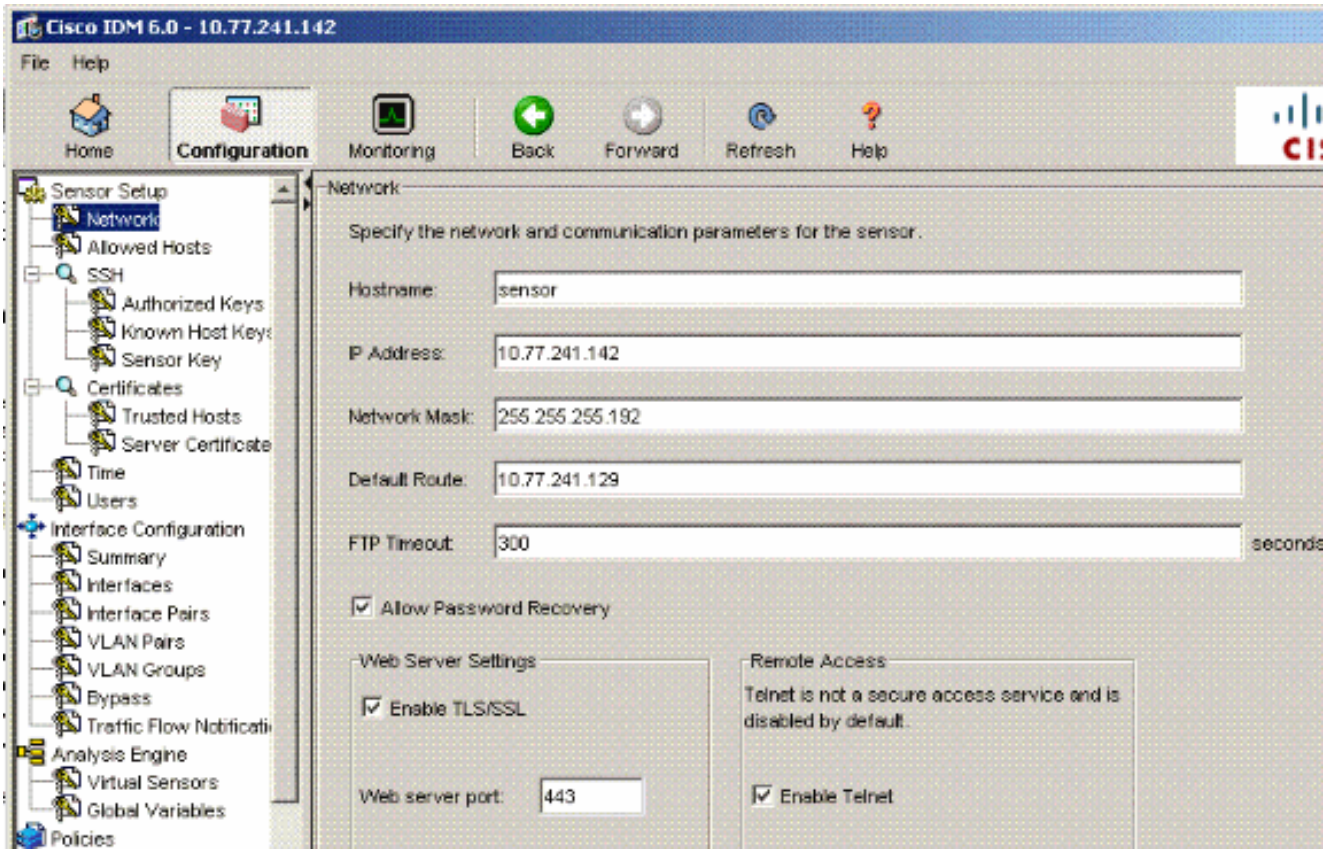
Terminez-vous ces étapes pour configurer les configurations de paires de l'en ligne VLAN sur le capteur utilisant le gestionnaire de périphériques d'ID (IDM) :

1. Ouvrez votre navigateur et écrivez le **<Management_IP_Address_of_IPS> de https://** pour

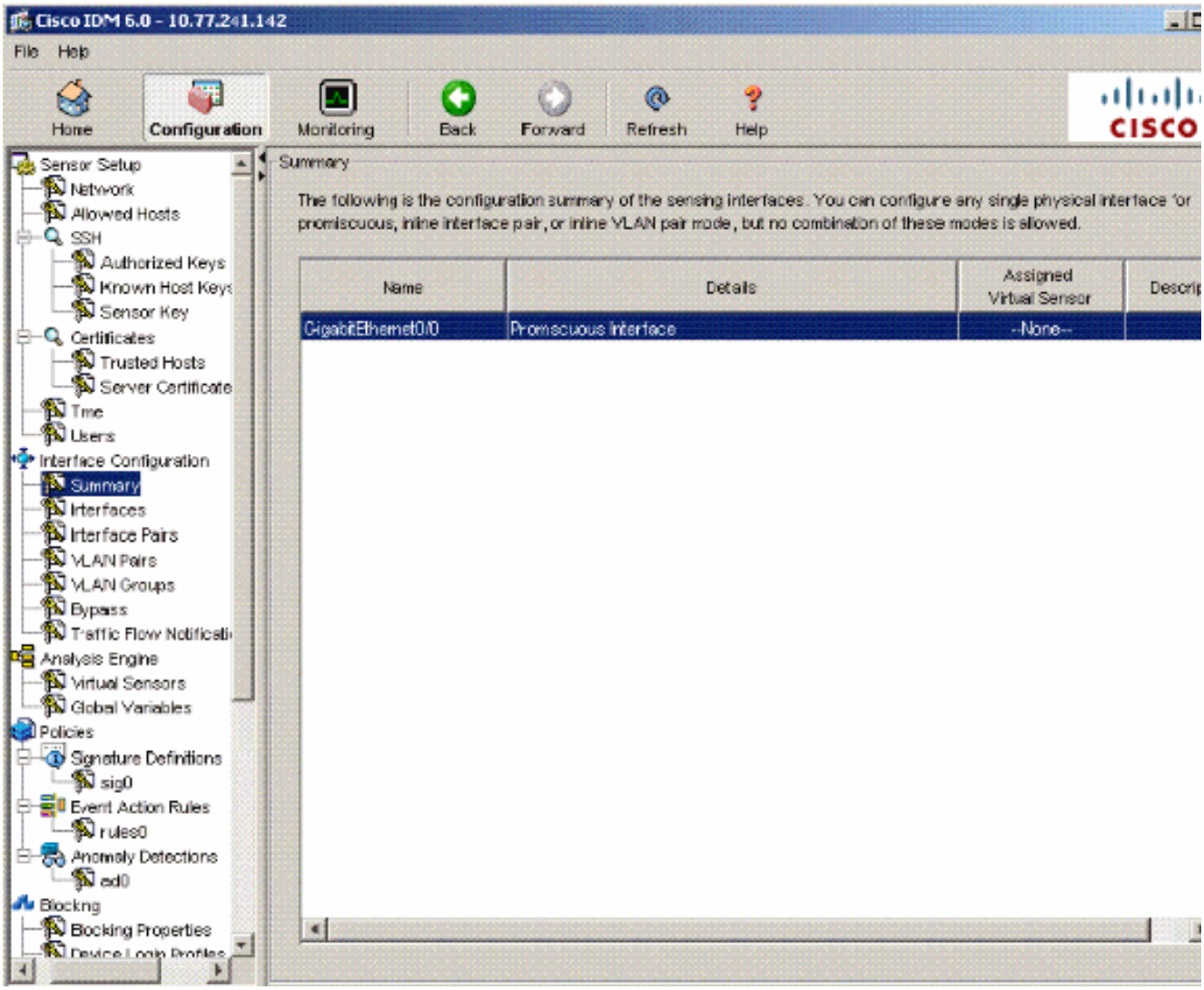
accéder à l'IDM sur l'IPS.

2. Cliquez sur Download le **lanceur IDM et commencez IDM** pour télécharger l'installateur pour l'application.
3. Allez à la page d'accueil afin de visualiser l'information sur le périphérique telle que le nom d'hôte, l'adresse IP, la version, et le modèle.,
   etc.

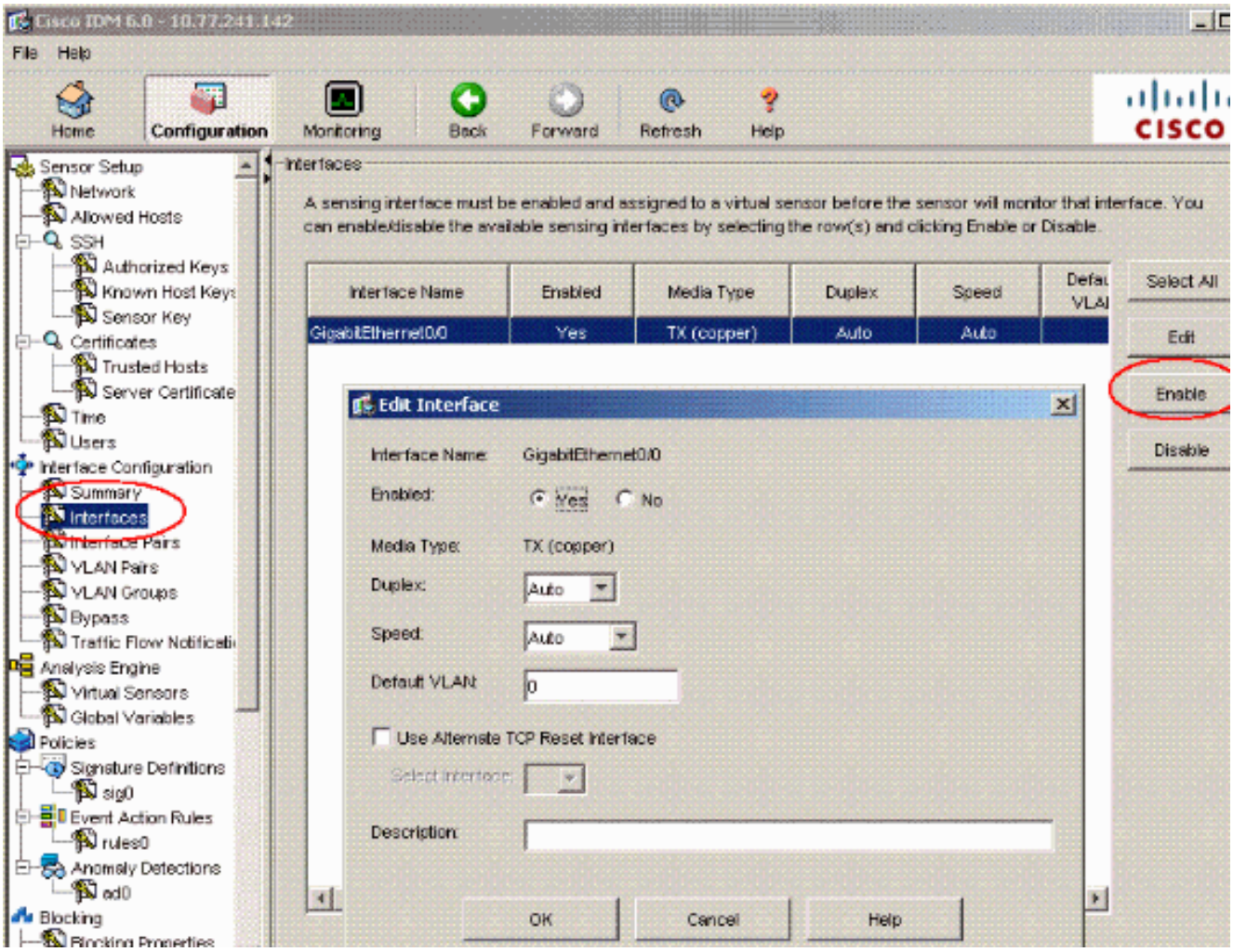
4. Allez à la **configuration > à l'installation de capteur** et cliquez sur le **réseau**. Voici que vous pouvez spécifier l'adresse Internet, l'adresse IP et le default
   route.



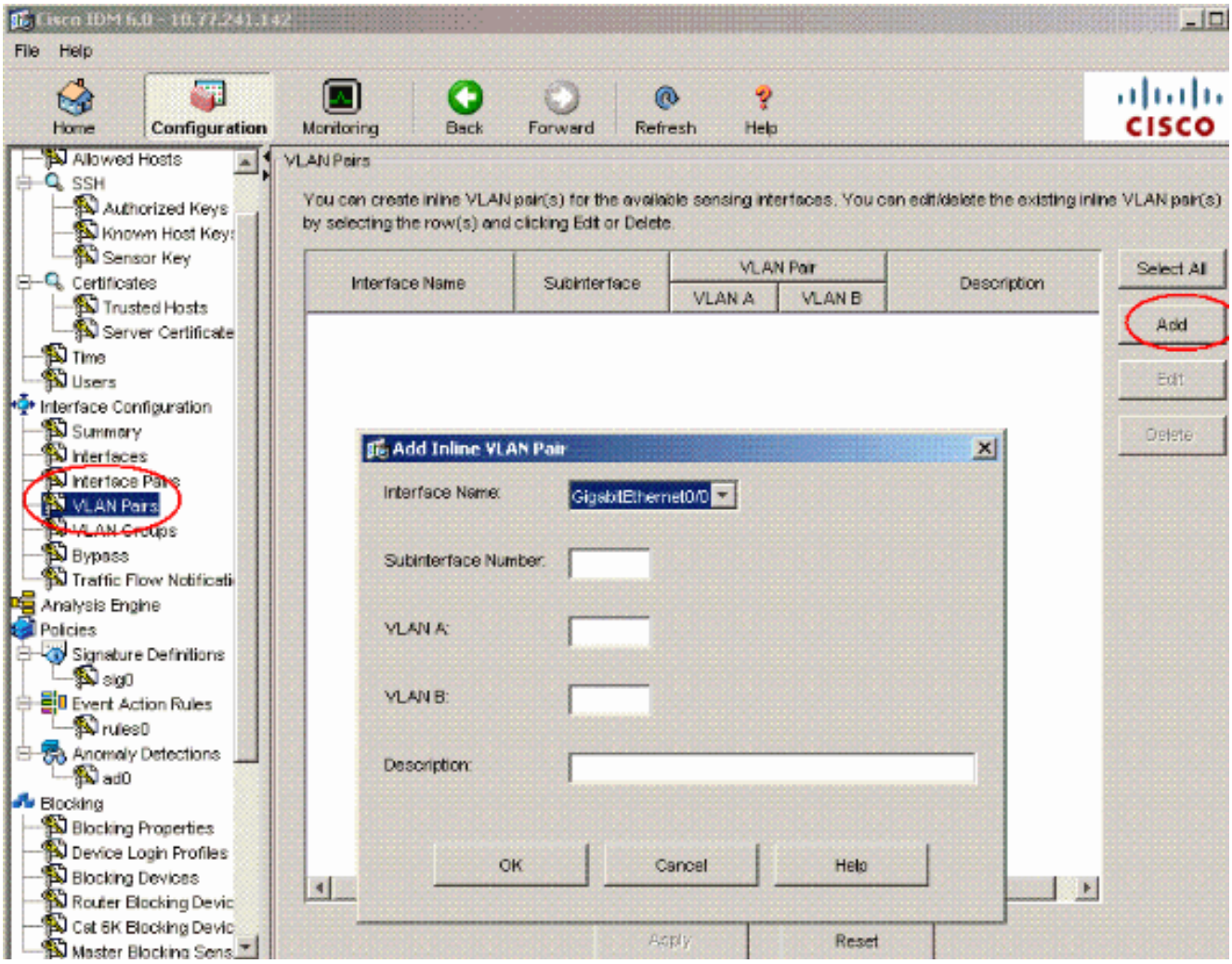
5. Allez à la **configuration > à la configuration d'interface** et cliquez sur le **résumé**.Cette page affiche le résumé de configuration de l'interface de détection.



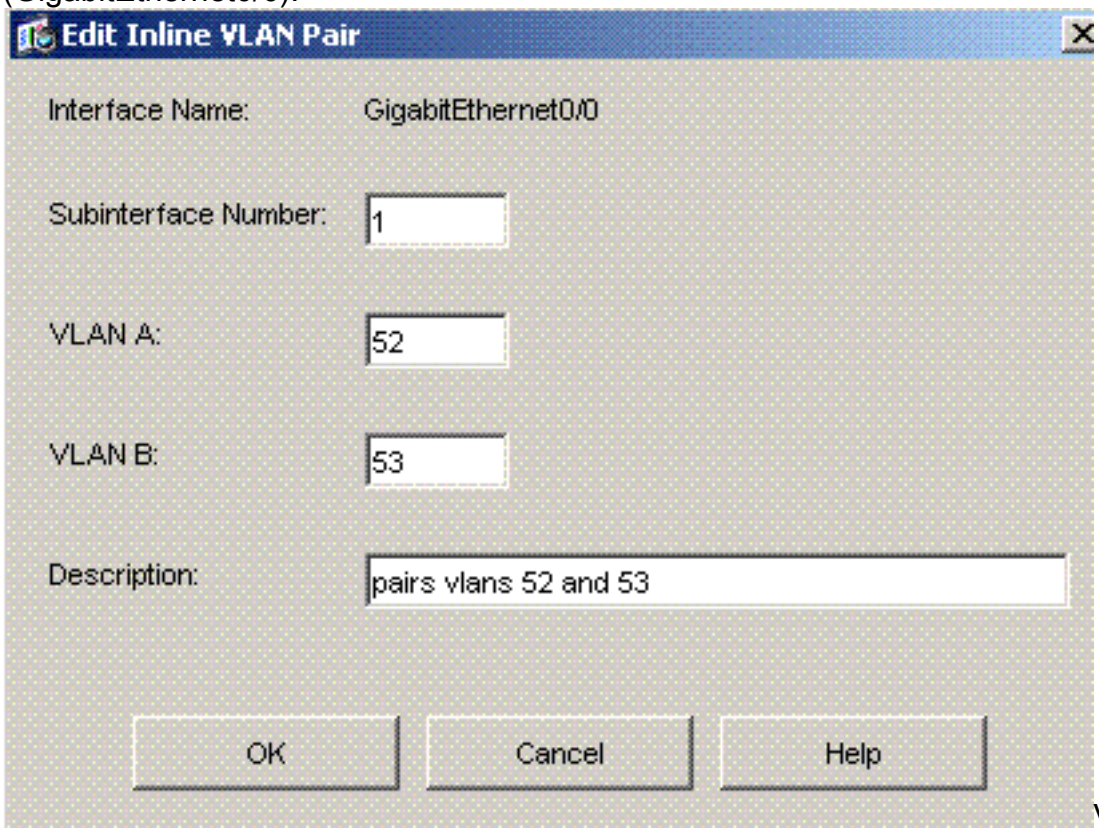
6. Allez à la **configuration > à la configuration d'interface > aux interfaces** et sélectionnez le nom d'interface. Puis, **enable de** clic afin d'activer l'interface de détection. En outre, configurez le duplex, la vitesse et les informations
VLAN.



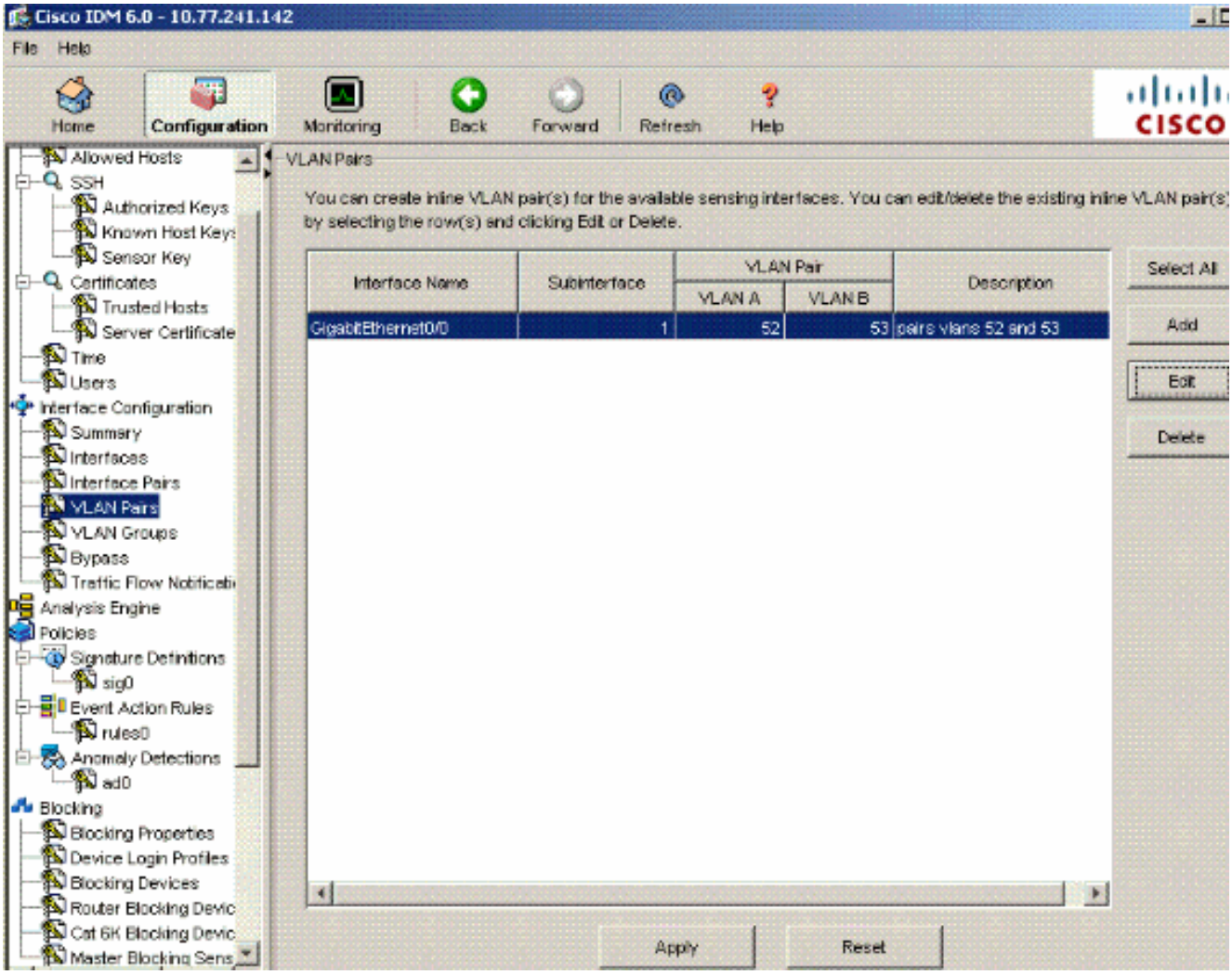
7. Allez à la **configuration > à la configuration d'interface > aux paires VLAN** et cliquez sur Add afin de créer les paires de l'en ligne
VLAN.



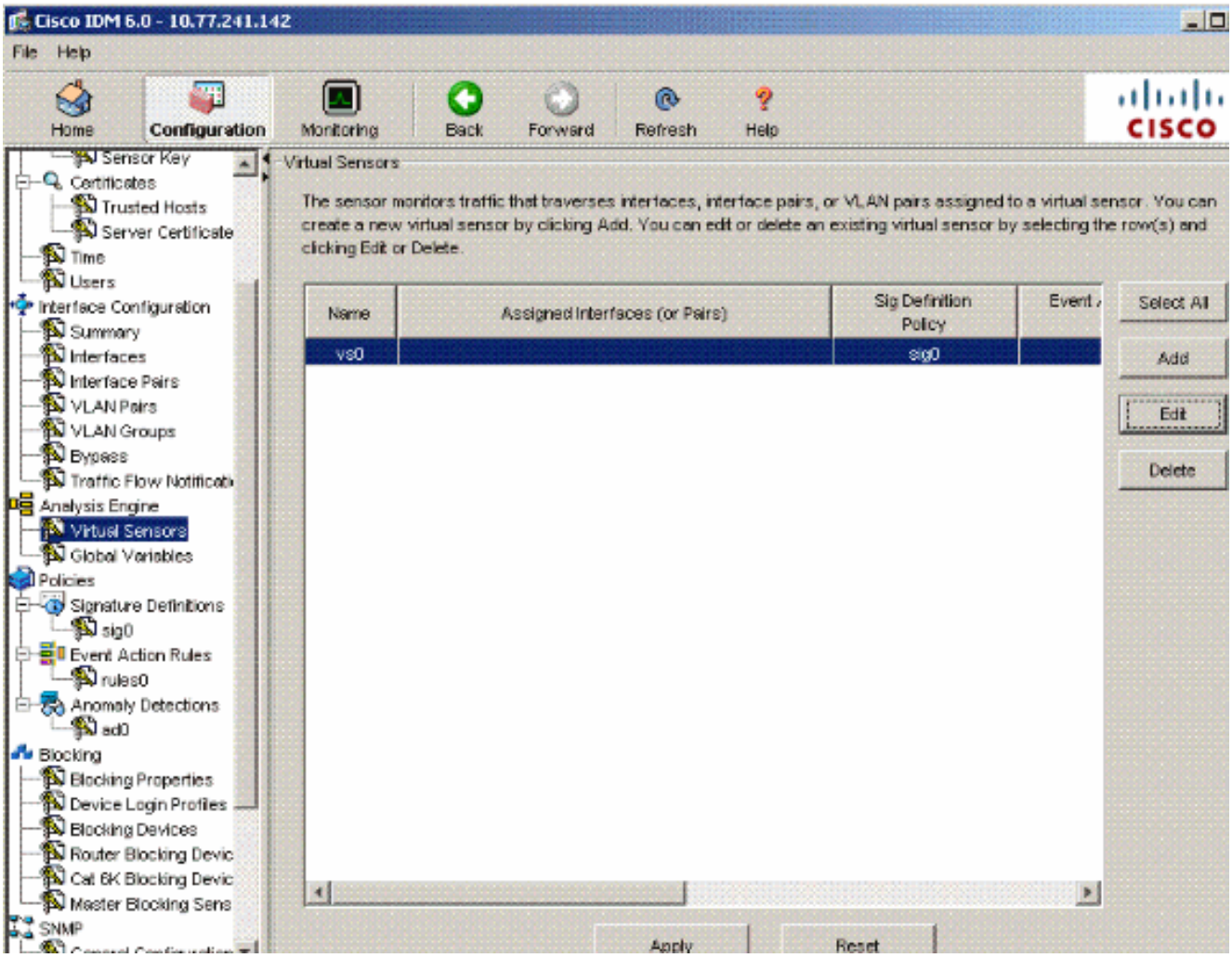
8. Écrivez le numéro de sous-interface, le VLAN A et le VLAN B pour l'interface de détection (GigabitEthernet0/0).



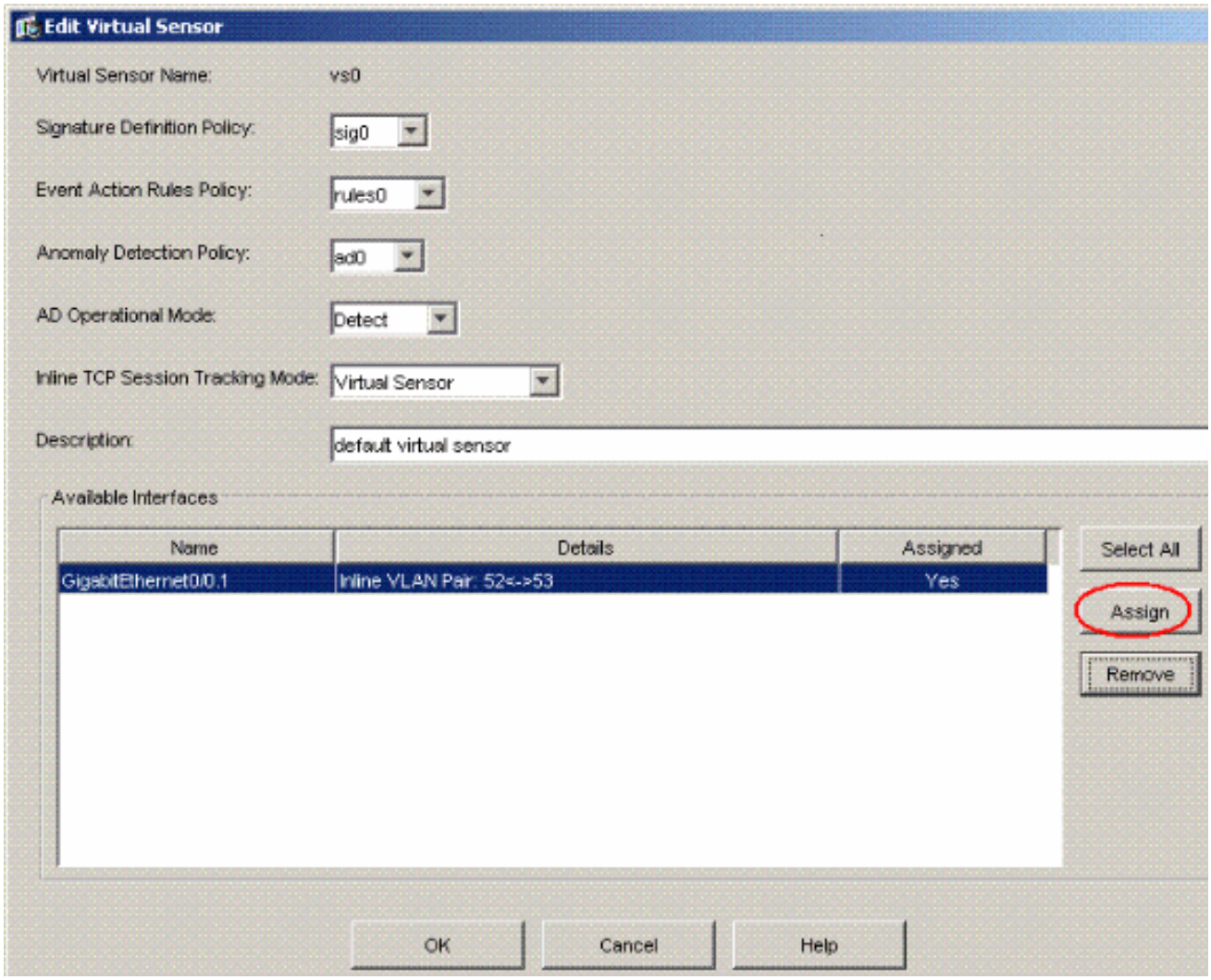
Vous pouvez visualiser le résumé de la configuration de paires de l'en ligne VLAN.



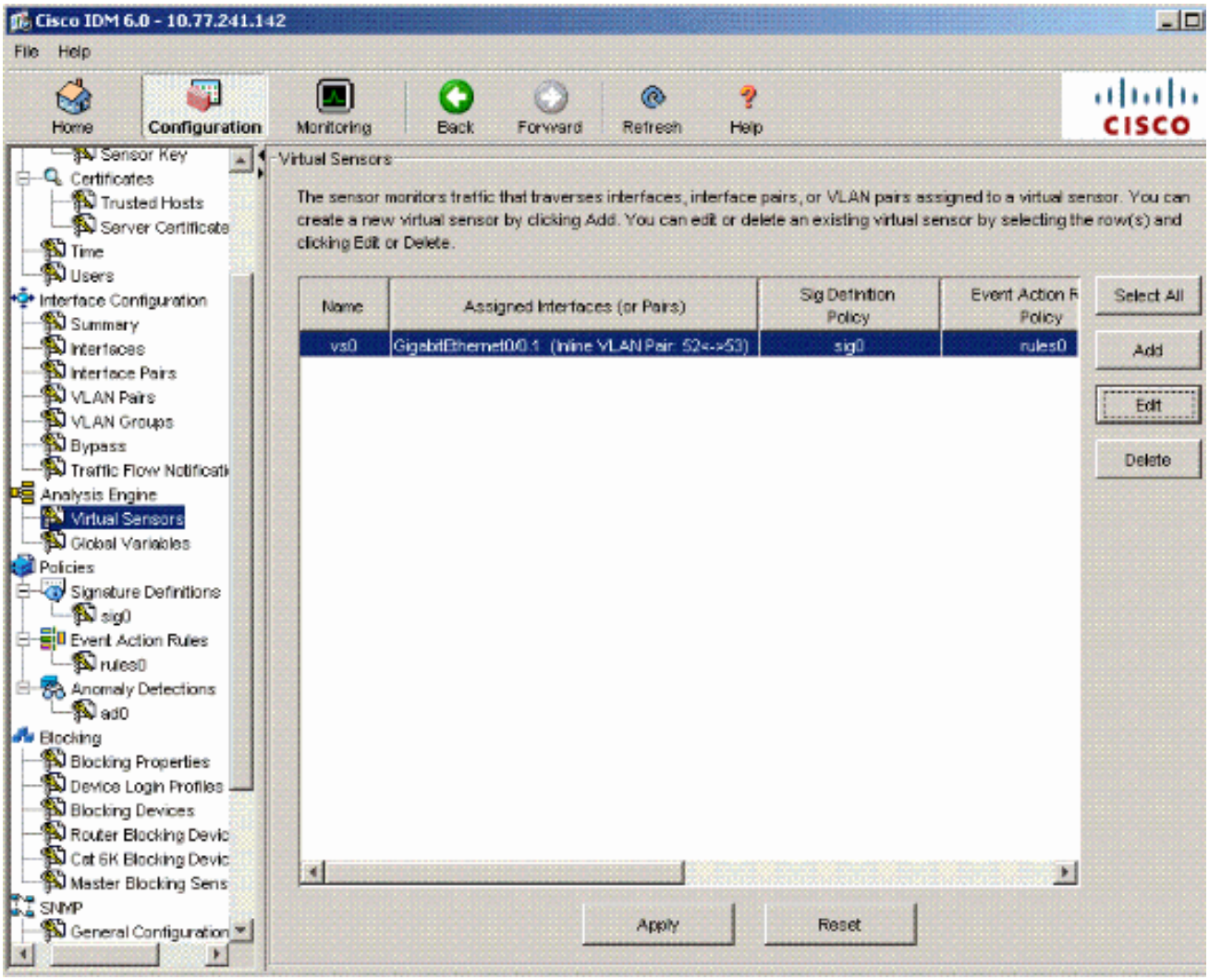
9. Allez à l'**engine de configuration > d'analyse > capteur virtuel** et cliquez sur Edit afin de créer le nouveau capteur
virtuel.



10. Assignez les paires 52 et 53 de l'en ligne VLAN au capteur virtuel vs0.



Visualisez le résumé des informations virtuelles assignées de capteur.



Dépanner

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

Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Système de protection contre les intrusions Cisco
- Détecteurs Cisco, série IPS 4200
- Support et documentation techniques - Cisco Systems