IPS 6.X et versions ultérieures/IDSM2 : Exemple de configuration de paires d'interfaces en ligne à l'aide d'IDM

Contenu

Introduction

Le fonctionnement en mode intégré de paires d'interface met le Système de prévention d'intrusion (IPS) directement dans la circulation et affecte des débits de transfert de paquet, qui les rend plus lents quand la latence est ajoutée. Ceci permet au capteur pour arrêter des attaques ainsi il relâche le trafic malveillant avant qu'il atteigne la cible destinée, ainsi il fournit un service protecteur. Sont non seulement les informations de traitement intégrées de périphérique sur les couches 3 et 4, mais elles analysent également le contenu et la charge utile des paquets pour des attaques incluses plus sophistiquées (couches 3 7). Cette analyse plus profonde permet le système d'identifier et arrêter et/ou bloquer les attaques qui traversent normalement un périphérique traditionnel de Pare-feu.

En mode intégré de paires d'interface, un paquet entre par la première interface des paires sur le capteur et la deuxième interface des paires. Le paquet est envoyé à la deuxième interface des paires à moins que ce paquet soit refusé ou modifié par une signature.

Remarque: Vous pouvez configurer AIM-IPS et AIP SSM pour actionner l'en ligne quoique ces modules aient seulement une interface de détection.

Remarque: Si les interfaces appareillées sont connectées au même commutateur, vous devriez les configurer sur le commutateur comme ports d'accès avec l'accès différent VLAN pour les deux ports. Autrement, le trafic ne traverse pas l'interface intégrée.

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 Cisco IPS qui utilise l'interface de ligne de commande 6.0 et le gestionnaire de périphériques de système de prévention des intrusions (IDM) 6.0.

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.

L'interface intégrée appareille la configuration

Employez la commande de *nom d'en ligne*-**interfaces** dans le sous-mode d'interface de service afin de créer des paires intégrées d'interface.

Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Remarque: L'AIP SSM est configuré pour le mode interface intégré de Cisco ASA CLI et pas du Cisco IPS CLI.

Ces options s'appliquent :

- *nom d'en ligne*-**interfaces** — Nom des paires intégrées logiques d'interface**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
- *interface_name* **interface1** — La première interface dans les paires intégrées d'interface
- *interface_name* **interface2** — La deuxième interface dans les paires intégrées d'interface
- **NO-** retire une configuration d'entrée ou de sélection
- **admin-état {activé | handicapé}** — l'état de lien administratif de l'interface, si l'interface est activée ou désactivée.

Configuration CLI

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

1. Ouvrez une session au CLI avec un compte qui a 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)#
```

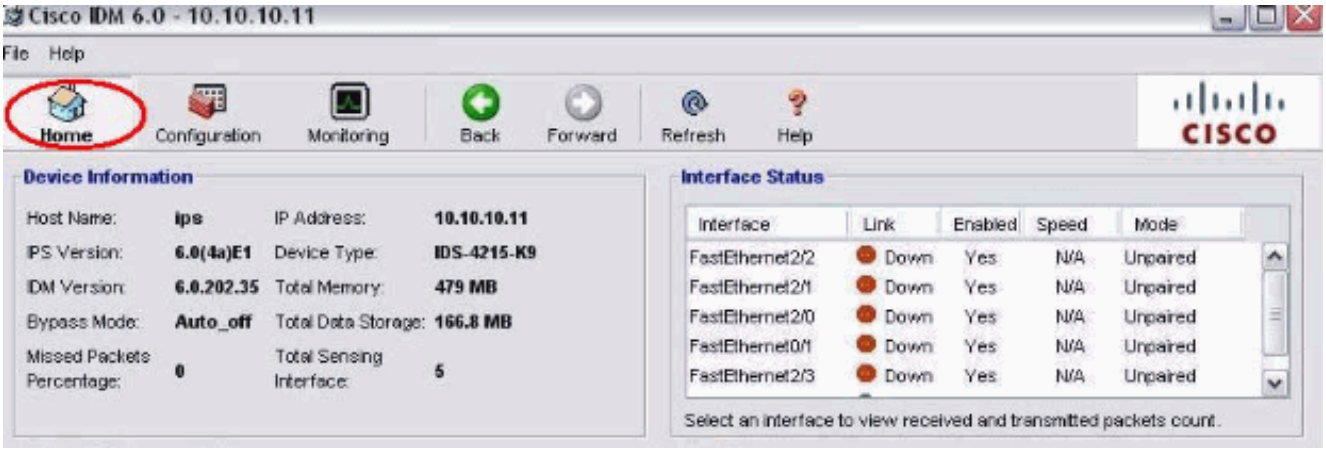
4. Nommez les paires intégrées :`sensor(config-int)#`**`inline-interfaces PAIR1`**
5. Affichez la liste d'interfaces disponibles :`sensor(config-int)#`**`physical-interfaces ?`**
   `GigabitEthernet0/0 GigabitEthernet0/0 physical interface. GigabitEthernet0/1 GigabitEthernet0/1 physical interface. GigabitEthernet0/2 GigabitEthernet0/2 physical interface. GigabitEthernet0/3 GigabitEthernet0/3 physical interface. Management0/0 Management0/0 physical interface. sensor(config-int)#`**`physical-interfaces`**
6. Configurez deux interfaces dans une paire :`sensor(config-int)#`**`interface1 GigabitEthernet0/0`**
   `sensor(config-int-inl)#`**`interface2 GigabitEthernet0/1`** Vous devez assigner l'interface à un capteur virtuel et l'activer avant qu'elle puisse surveiller le trafic. Voir le pour en savoir plus d'étape 10.
7. Ajoutez une description de cette interface :`sensor(config-int-phy)#`**`description PAIR1 Gig0/0 and Gig0/1`**
8. Répétez les étapes 4 à 7 pour toutes les autres interfaces que vous voulez configurer aux paires intégrées d'interface.
9. Vérifiez les configurations :`sensor(config-int-inl)#`**`show settings`** `name: PAIR1 ----------`
   ```
   ------------------------------ description: PAIR1 Gig0/0 & Gig0/1 default: interface1:
   GigabitEthernet0/0 interface2: GigabitEthernet0/1 ----------------------------------------
   ------
   ```
10. Activez les interfaces assignées aux paires d'interface :`sensor(config-int)#`**`exit`**
    `sensor(config-int)#`**`physical-interfaces GigabitEthernet0/0`** `sensor(config-int-phy)#`**`admin-state enabled`** `sensor(config-int-phy)#`**`exit`** `sensor(config-int)#`**`physical-interfaces GigabitEthernet0/1`** `sensor(config-int-phy)#`**`admin-state enabled`** `sensor(config-int-phy)#`**`exit`**
    `sensor(config-int)#`
11. Vérifiez que les interfaces sont activées :`sensor(config-int)#`**`show settings`** `physical-`
    ```
    interfaces (min: 0, max: 999999999, current: 5) ----------------------------------------
    ----- <protected entry> name: GigabitEthernet0/0 ----------------------------------------
    ------ media-type: tx <protected> description: <defaulted> admin-state: enabled default:
    disabled duplex: auto <defaulted> speed: auto <defaulted> default-vlan: 0 <defaulted> alt-
    tcp-reset-interface ---------------------------------------- none ----------------
    ------------------------------ ---------------------------------------- -----------
    ---------------------------------- subinterface-type ----------------------------------
    ----------- none ---------------------------------------- ----------------------
    ---------------------- ---------------------------------------- -----------------
    ---------------------------- <protected entry> name: GigabitEthernet0/1 ----------------
    ------------------------------ media-type: tx <protected> description: <defaulted> admin-
    state: enabled default: disabled duplex: auto <defaulted> speed: auto <defaulted> default-
    vlan: 0 <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> default-vlan: 0 <defaulted> alt-tcp-reset-interface --
    ---------------------------------------- none ----------------------------------
    -------- ---------------------------------------- ----------------------------
    ------------- subinterface-type ---------------------------------------- none ----
    ---------------------------------------- ----------------------------------------
    - ---------------------------------------- ----------------------------------------
    ------- <protected entry> name: GigabitEthernet0/3 <defaulted> ----------------------
    ------------------- media-type: tx <protected> --MORE--
    ```

12. Émettez cette commande afin de supprimer une paire intégrée d'interface et renvoyer les interfaces au mode promiscueux :`sensor(config-int)#no inline-interfaces PAIR1` Vous devez également supprimer les paires intégrées d'interface du capteur virtuel auquel il est assigné.
13. Vérifiez les paires intégrées d'interface a été supprimé :`sensor(config-int)#show settings --- command-control: Management0/0 <protected> inline-interfaces (min: 0, max: 999999999, current: 0) ---------------------------------- ----------- -- bypass-mode: auto <defaulted> interface-notifications --`
14. Quittez le sous-mode de configuration d'interface :`sensor(config-int)#exit Apply Changes:?[yes]:`
15. Appuyez sur **entrent** afin d'appliquer les modifications ou entrer **aucun** afin de les jeter.

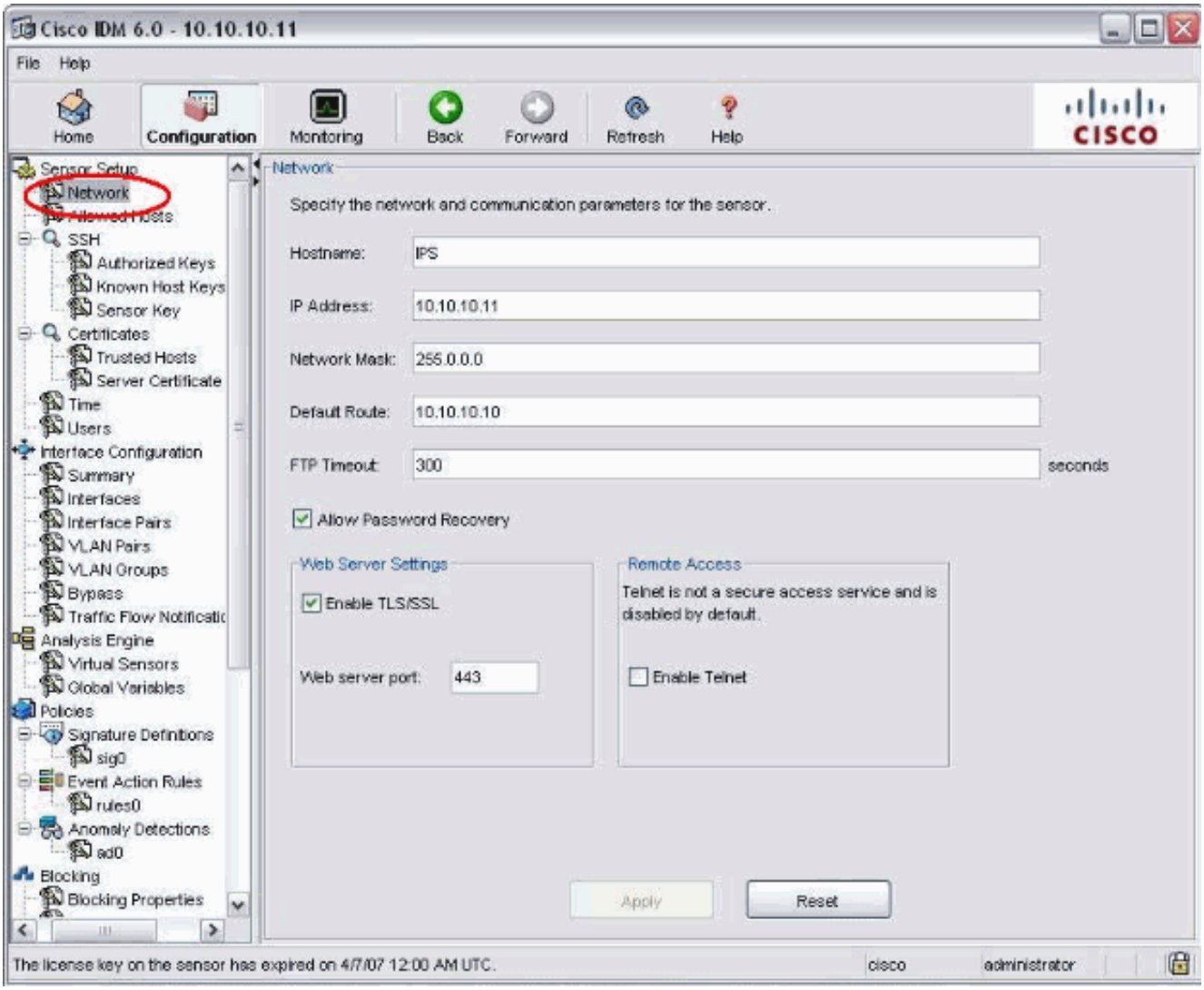
Configuration IDM

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

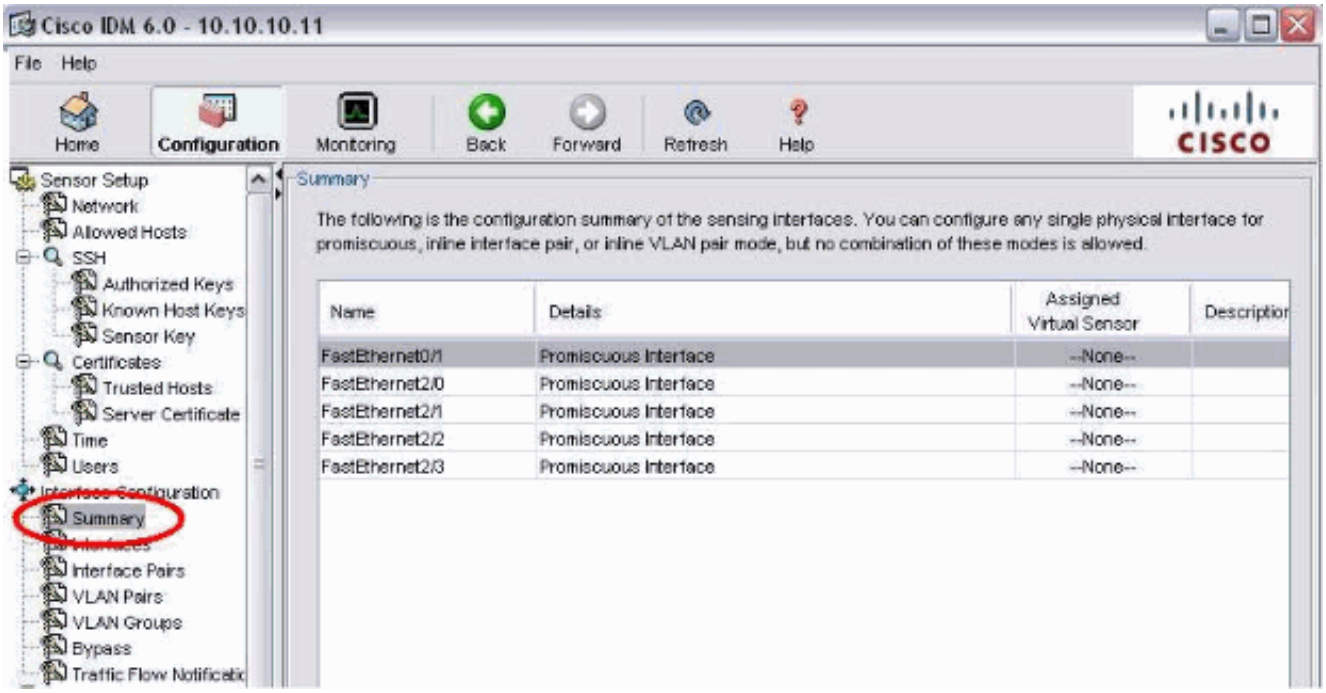
1. Ouvrez votre navigateur et écrivez le **<Management_IP_Address_of_IPS> de https://** pour accéder à l'IDM sur l'IPS.
2. Cliquez sur Download le **lanceur IDM** et **commencez IDM** pour télécharger l'installateur pour l'application.
3. Allez à la page d'accueil afin de visualiser l'information sur le périphérique telle que le nom d'hôte, l'adresse IP, la version, et le modèle.



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.

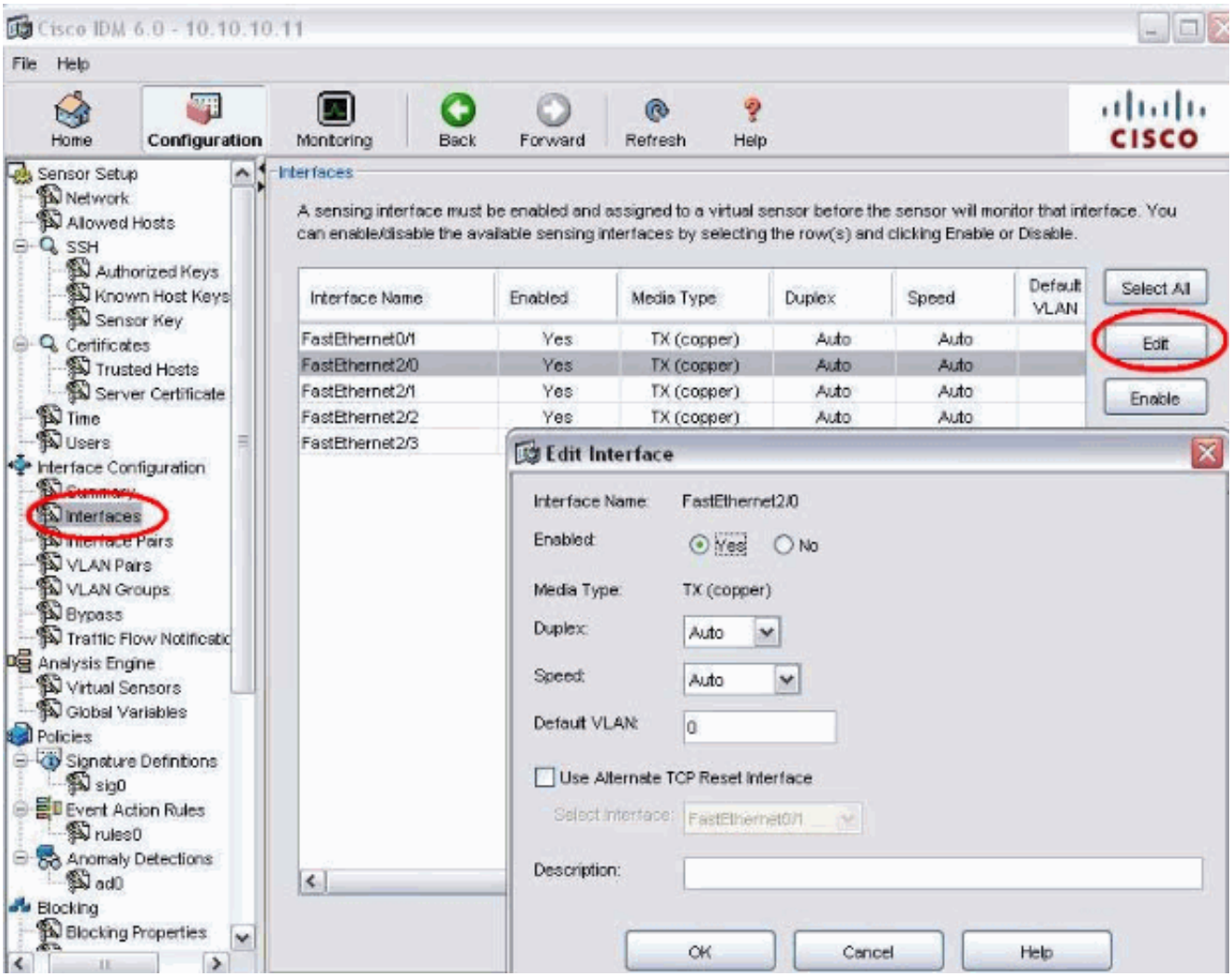


5. Allez à la **configuration > à la configuration d'interface** et cliquez sur le **résumé**.Cette page affiche le résumé de configuration de l'interface de détection
:

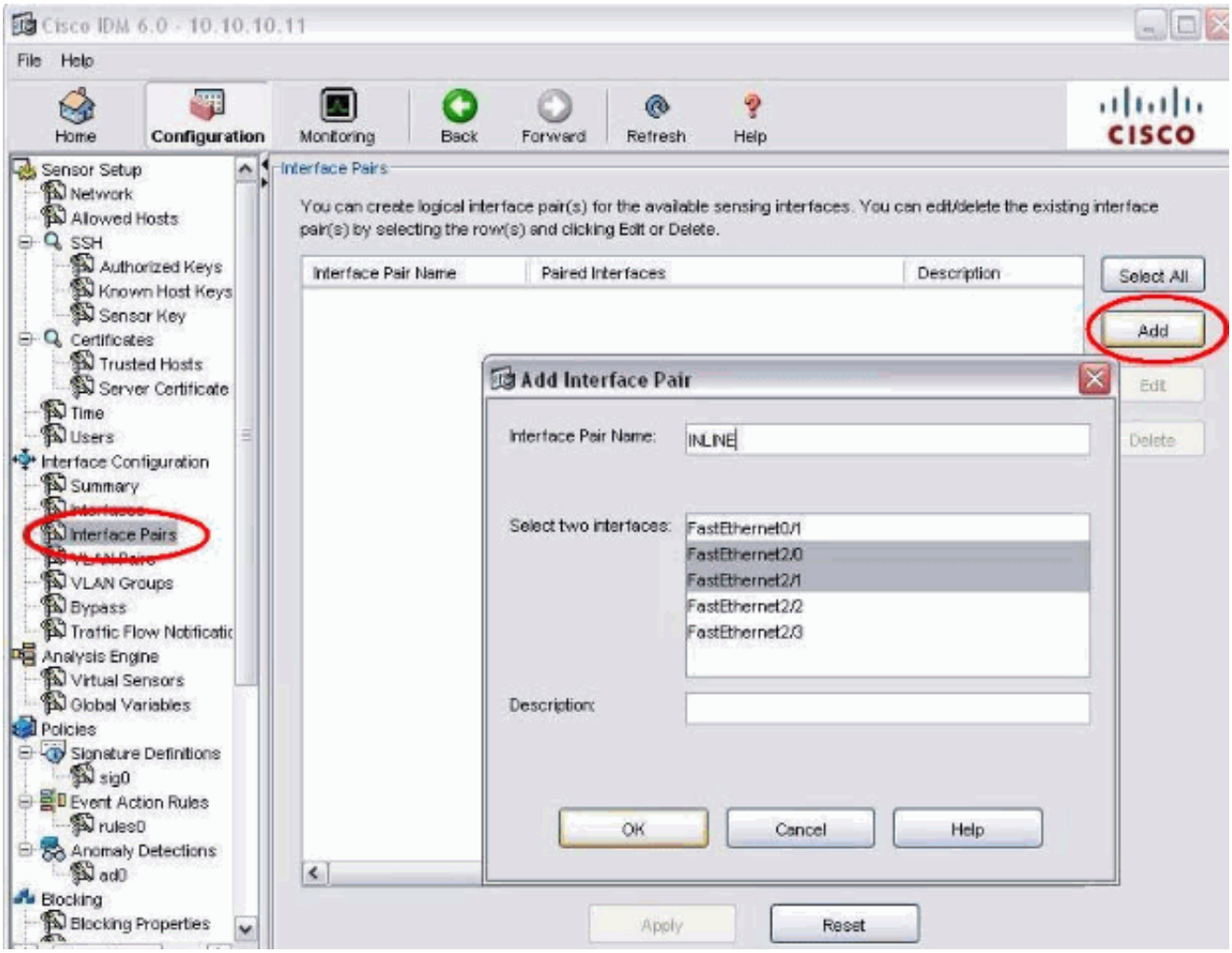


6. Allez à la **configuration > à la configuration d'interface > aux interfaces** et sélectionnez le nom d'interface. Puis, **enable de** clic afin d'activer l'interface de détection. En outre, configurez le duplex, la vitesse et les informations

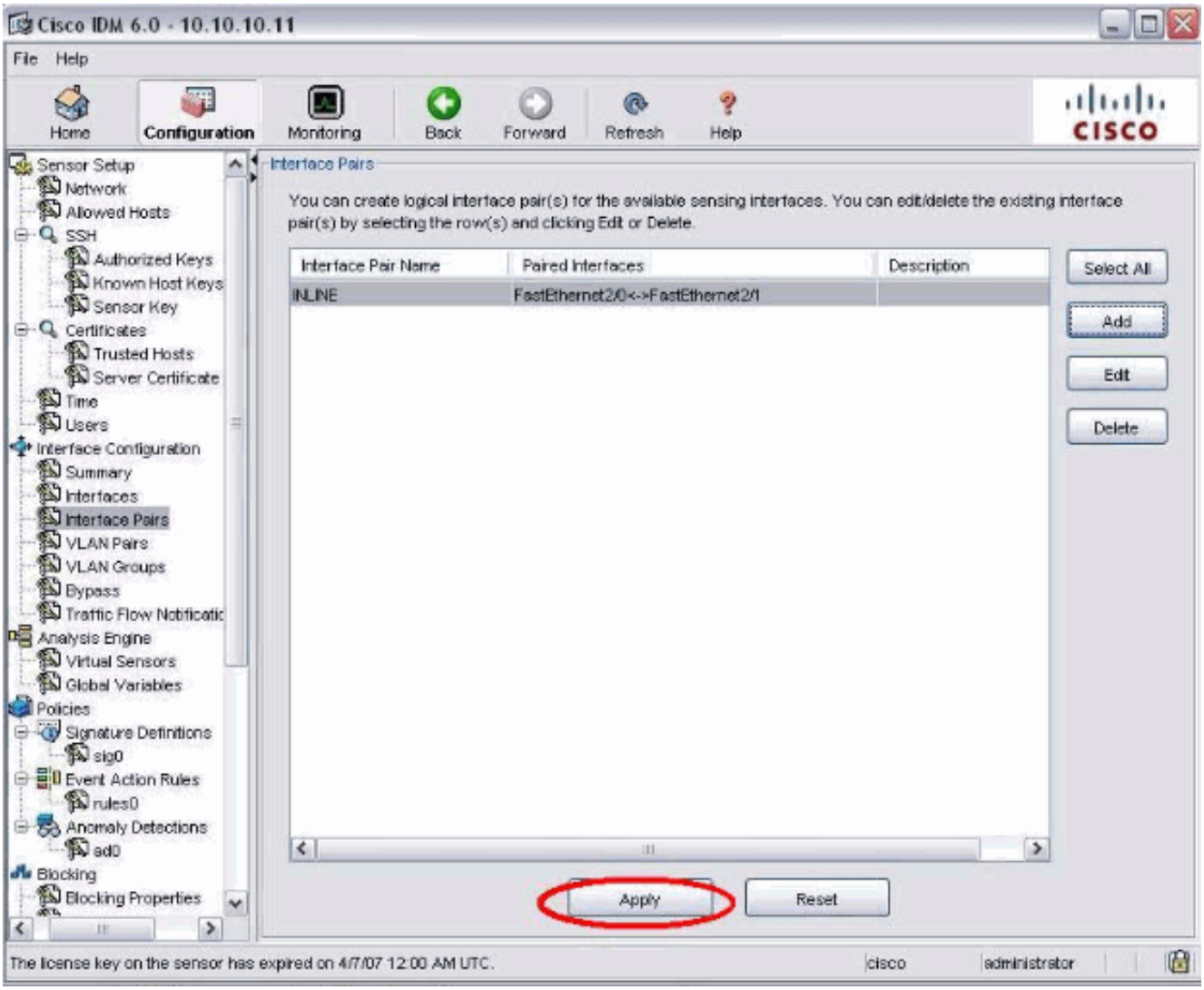
VLAN.



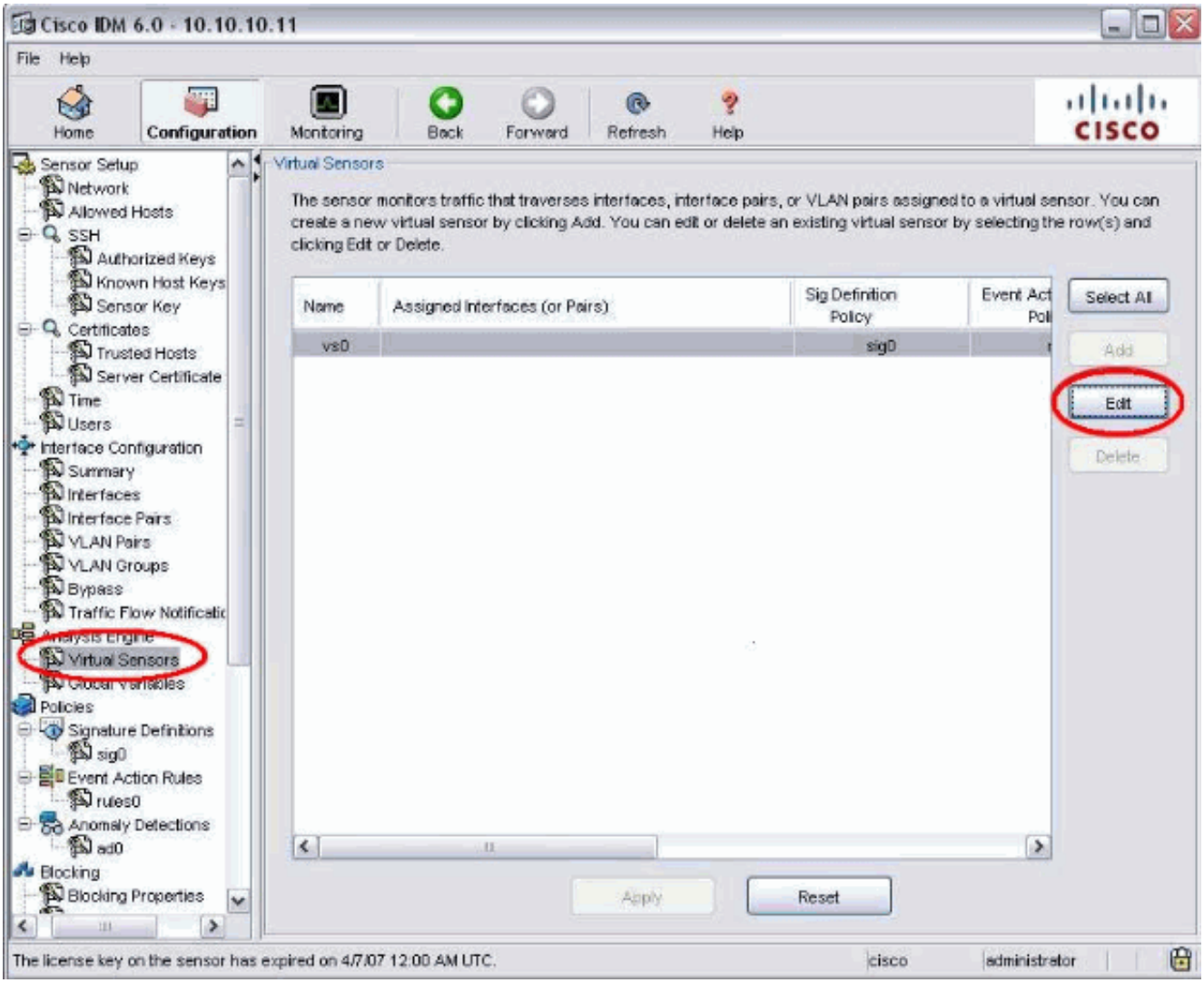
7. Allez aux **paires de configuration > de configuration d'interface > d'interface** et cliquez sur Add afin de créer les paires intégrées.



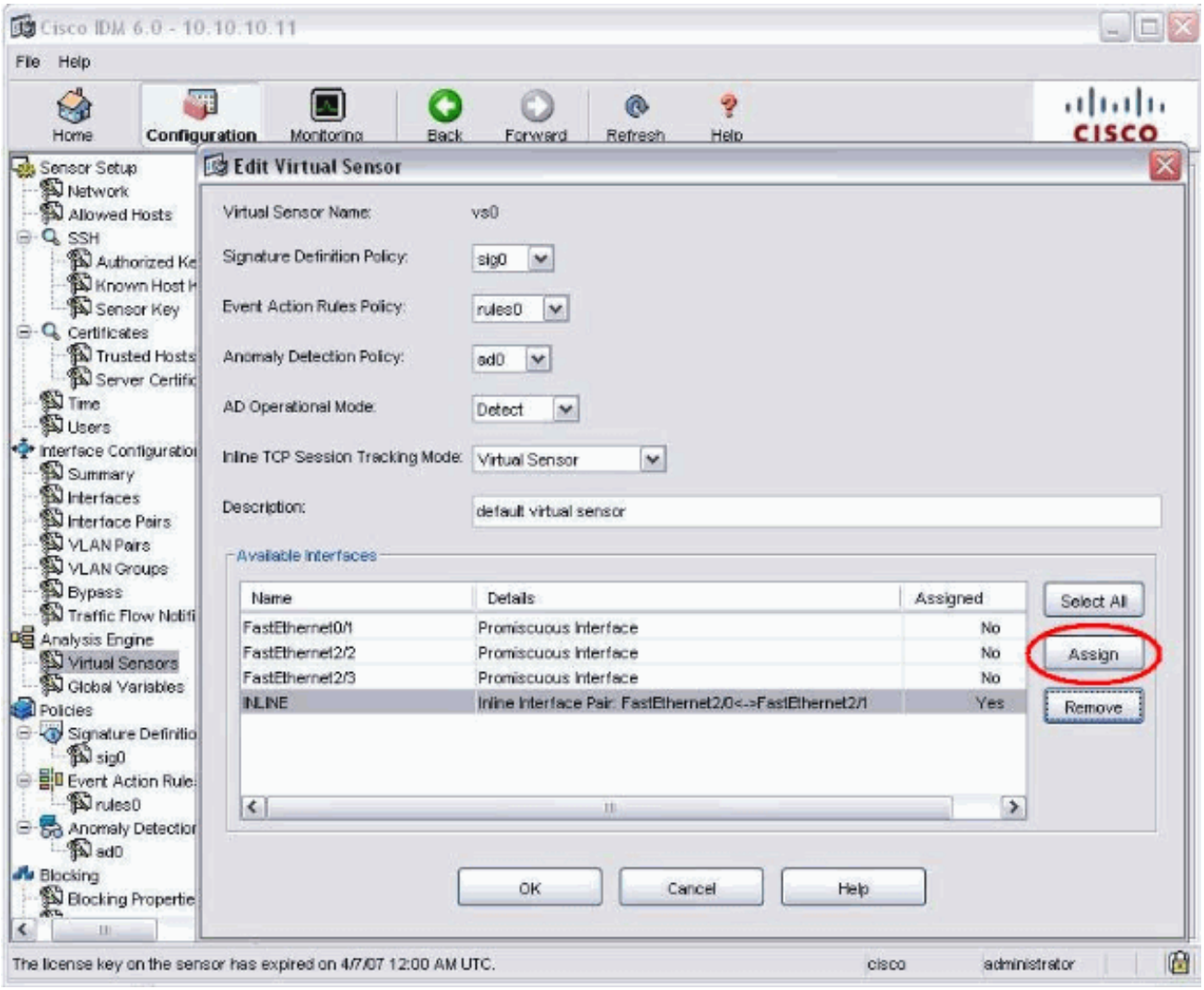
8. Visualisez le résumé de la configuration intégrée de paires et appliquez-le.



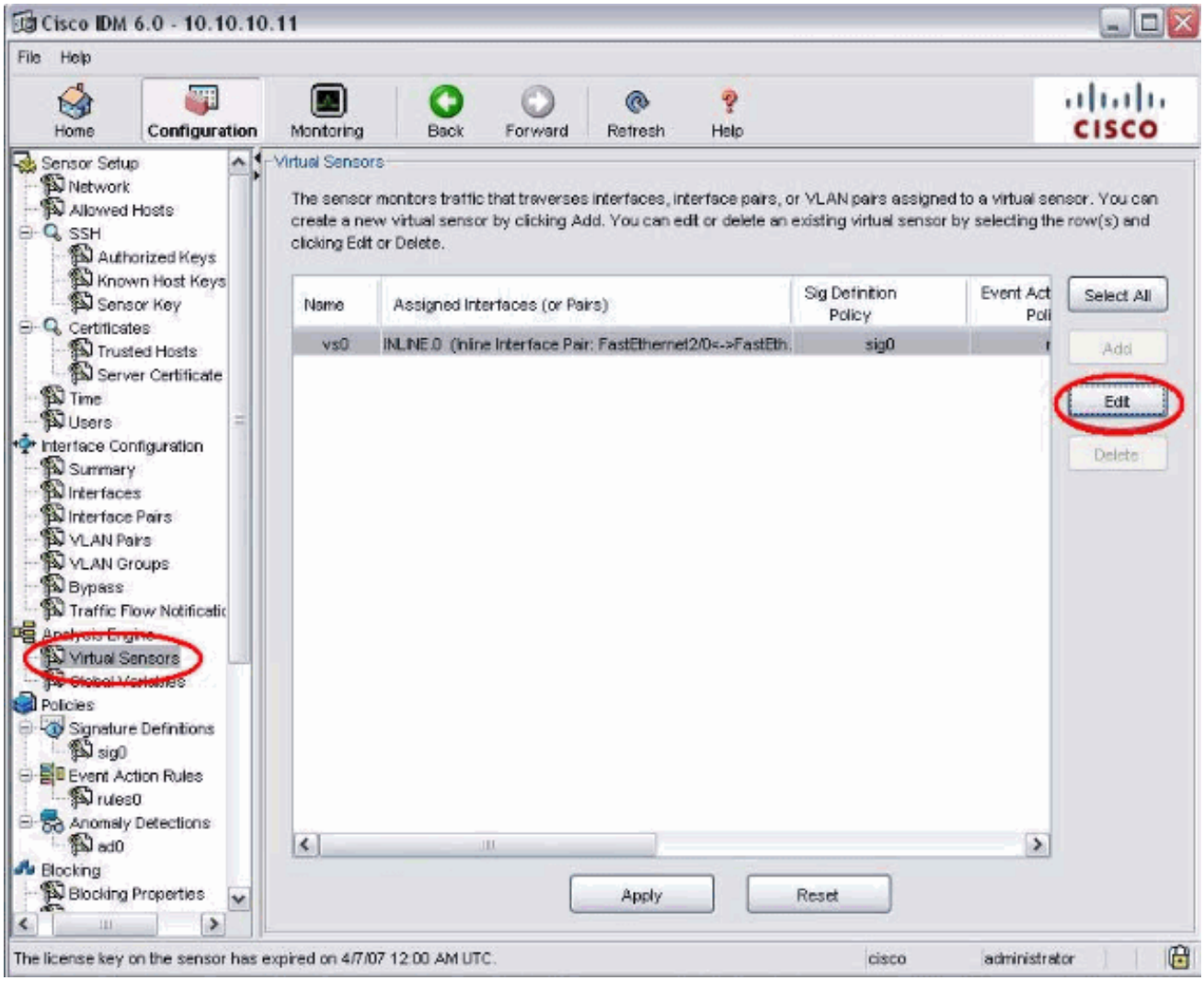
9. Allez à l'**engine de configuration > d'analyse > capteur virtuel** et cliquez sur Edit afin de créer le nouveau capteur
virtuel.



10. Assignez l'**EN LIGNE** intégré de paires au capteur virtuel vs0.



11. Visualisez le résumé des informations virtuelles assignées de capteur.



Configurez le commutateur pour IDSM-2 en mode intégré

Référez-vous à configurer le commutateur de la gamme 6500 de Catalyst pour IDSM-2 dans la section Mode intégrée de configurer IDSM-2 afin de configurer le commutateur pour le mode de l'en ligne IDSM-2.

Dépannez

Problème

Si l'IPS échoue et c'est en ligne configuré, faites les interfaces échouent ouvert (le trafic continue à passer) ou fermé (le trafic est abandonné).

Solution

Vous pouvez configurer l'IPS dans l'état échec-ouvert. Ainsi, si l'IPS échoue il continuera à passer le trafic, mais il pas surveillent le trafic.

Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500

- Système de protection contre les intrusions Cisco
- Détecteurs de la gamme Cisco IPS 4200
- Support et documentation techniques - Cisco Systems