CS-MARS : Exemple de configuration d'ajout à CS-MARS d'un capteur IPS Cisco comme périphérique de création de rapports

Contenu

Introduction

Ce document explique comment préparer un périphérique Cisco Secure de Système de prévention d'intrusion (IPS) et tous les capteurs virtuels configurés agir en tant que des périphériques d'enregistrement à la surveillance de sécurité Cisco, à l'analyse, et au système de réponse (CS-MARS).

Conditions préalables

Conditions requises

Pour les périphériques 5.x, 6.x, et 7.x de Cisco IPS, TROUBLE des tractions les logs utilisant SDEE au-dessus de SSL. Par conséquent, le MARS doit avoir accès HTTPS au capteur. Afin de préparer le capteur, vous devez permettre au serveur HTTP sur le capteur, TLS d'enable de permettre l'accès HTTPS, et vous assurez que l'adresse IP du MARS est définie comme hôte permis, un qui peut accéder au capteur et tirer des événements. Si les capteurs ont été configurés pour permettre l'accès des hôtes ou des sous-réseaux limités sur le réseau, vous pouvez employer les **ip_address de liste d'accès/**commande de **netmask** afin d'activer cet accès.

Composants utilisés

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

- Périphérique Cisco Secure de MARS qui exécute la version de logiciel 4.2.x et plus tard
- Périphérique IPS de gamme Cisco 4200 qui exécute la version de logiciel 6.0 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

Cette configuration peut également être utilisée avec ces capteurs :

- IPS-4240
- IPS-4255
- IPS-4260
- IPS-4270-20

Conventions

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

Configurez

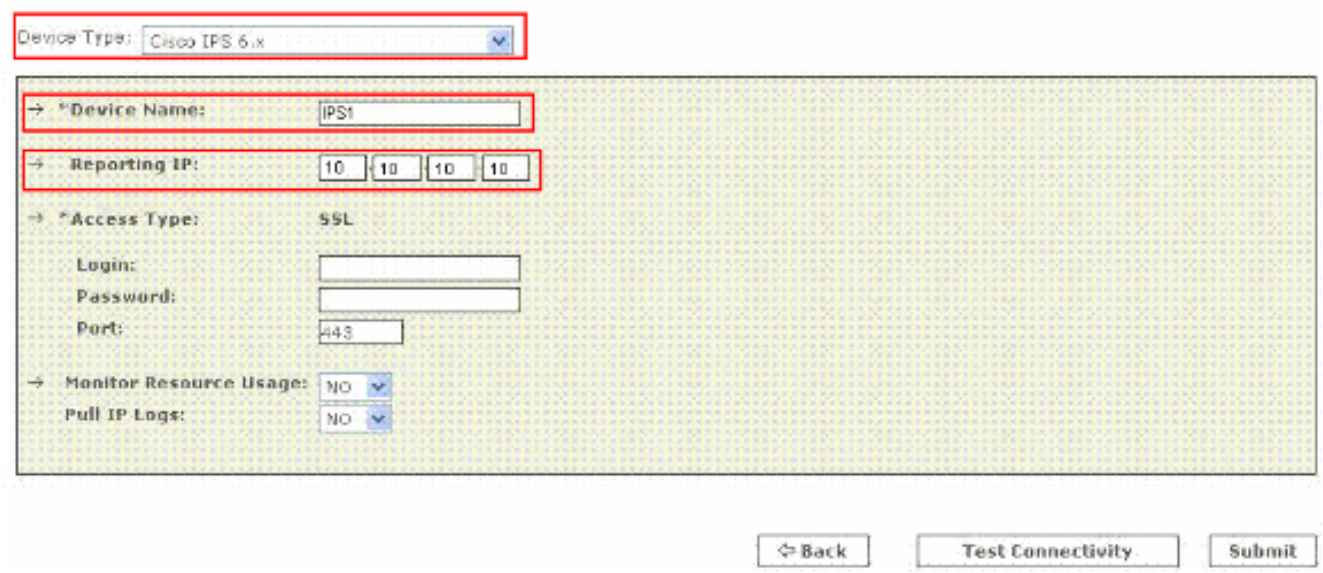
Dans cette section, vous êtes présenté avec les informations sur la façon dont ajouter et configurer un capteur Cisco Secure de Système de prévention d'intrusion (IPS) à un périphérique de surveillance de sécurité Cisco, d'analyse, et de système de réponse (CS-MARS).

Ajoutez et configurez un périphérique 6.x ou 7.x de Cisco IPS dans le MARS

Quand vous définissez un périphérique 6.x ou 7.x de Cisco IPS dans le MARS, vous pouvez découvrir tous les capteurs virtuels configurés sur le périphérique. Quand vous découvrez ces capteurs virtuels, ceci permet au MARS pour séparer les événements signalés par le capteur virtuel. Il te permet également pour accorder la liste de réseaux surveillés à chaque capteur virtuel, qui améliore la précision de l'enregistrement désiré.

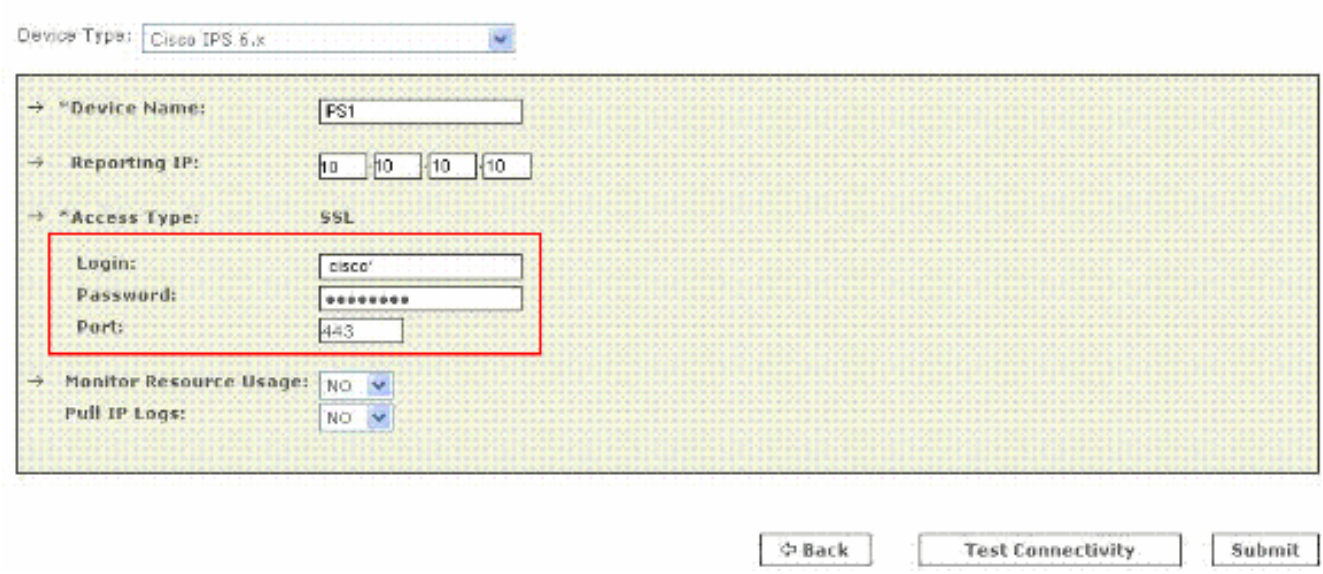
Terminez-vous ces étapes afin d'ajouter et configurer un périphérique 6.x ou 7.x de Cisco IPS dans le MARS :

1. Choisissez l'**admin > le système installés > des périphériques de Sécurité et de moniteur**. Puis, cliquez sur en fonction **Add**.
2. Choisissez le **Cisco IPS 6.x ou le Cisco IPS 7.x de la** liste de type de périphérique. Entrez dans maintenant l'adresse Internet du capteur dans le **champ Device Name** comme affiché ici. IPS1 est le nom du périphérique utilisé dans cet exemple. La valeur de nom du périphérique doit être identique au nom configuré de capteur.



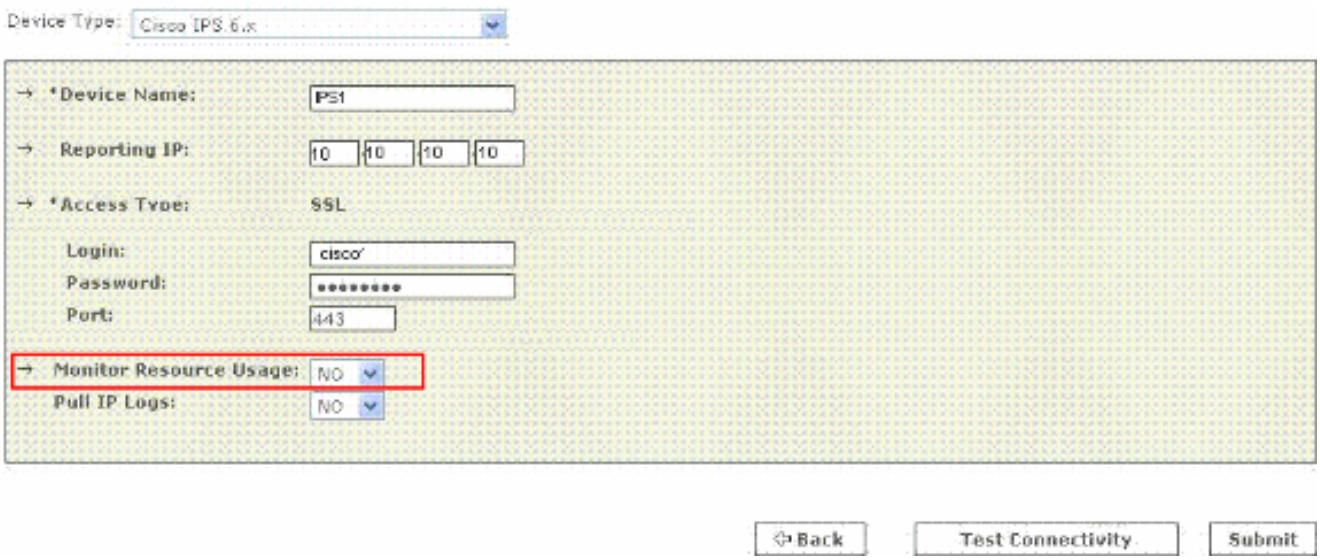
Écrivez maintenant l'adresse IP administrative dans le domaine **signalant IP**. L'adresse IP d'enregistrement est la même adresse que l'adresse IP administrative.

3. Dans le **domaine de procédure de connexion**, écrivez le nom d'utilisateur associé avec le compte administratif qui est utilisé pour accéder au périphérique d'enregistrement. Maintenant, dans le **domaine de mot de passe**, entrez le mot de passe associé avec le nom d'utilisateur spécifié dans le **domaine de procédure de connexion**. **Le nom d'utilisateur** est **Cisco** et le **mot de passe** utilisé est **cisco123** dans cet exemple. Introduisez également le nombre de port TCP sur lequel l'exécution de web server sur le capteur écoute dans le **domaine de port**. Le port du par défaut HTTPS est
443.

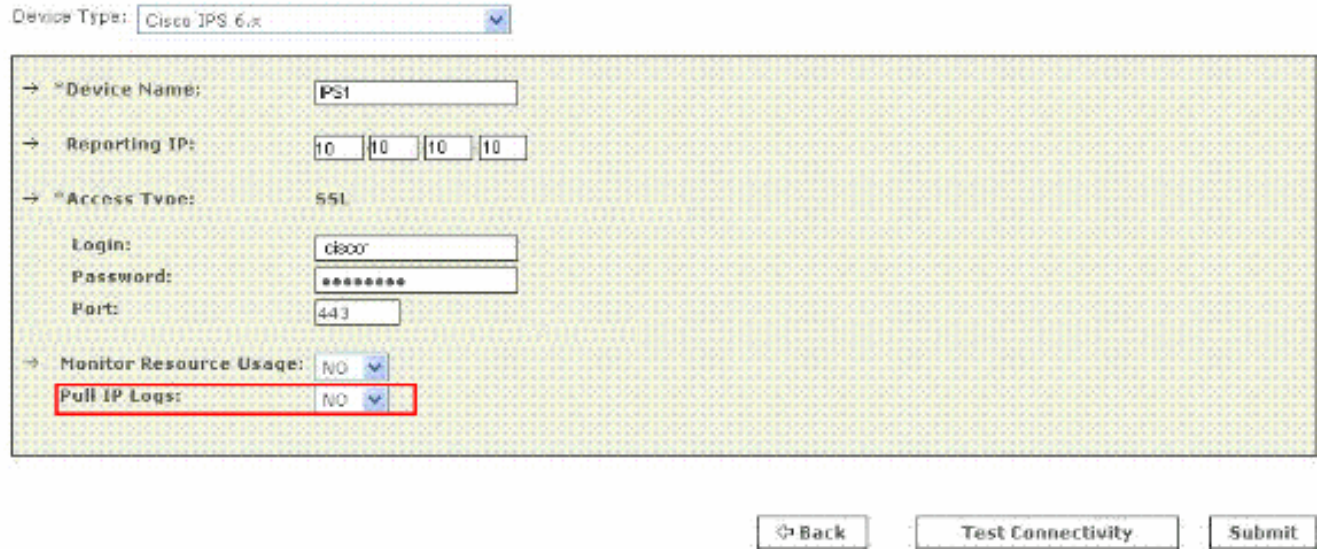


Remarque: Tandis qu'il est possible de configurer le HTTP seulement, le MARS exige HTTPS.

4. Vérifiez maintenant qu'**AUCUN** chosed dans la liste d'**utilisation de ressource en moniteur**. Tandis que l'option d'utilisation de ressource en moniteur apparaît à cette page, elle ne fonctionne pas pour le Cisco
IPS.

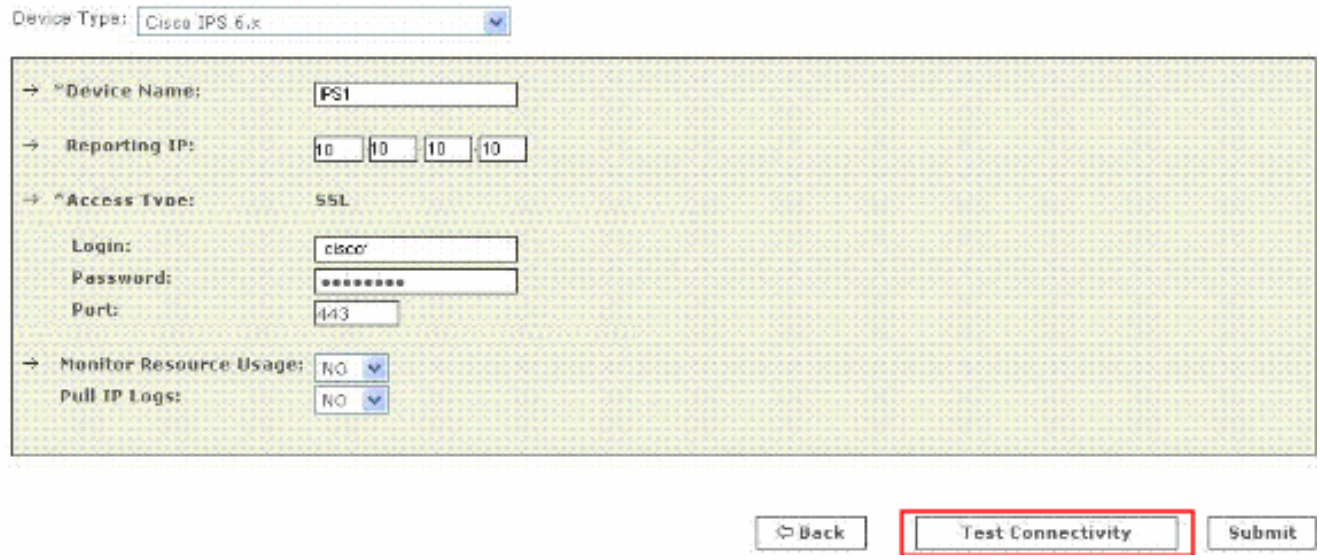


5. Afin de tirer les logs IP du capteur, choisissez **oui de la** liste de **logs IP de traction**. C'est une fonctionnalité facultative, qui peut être utilisée s'il y a lieu.

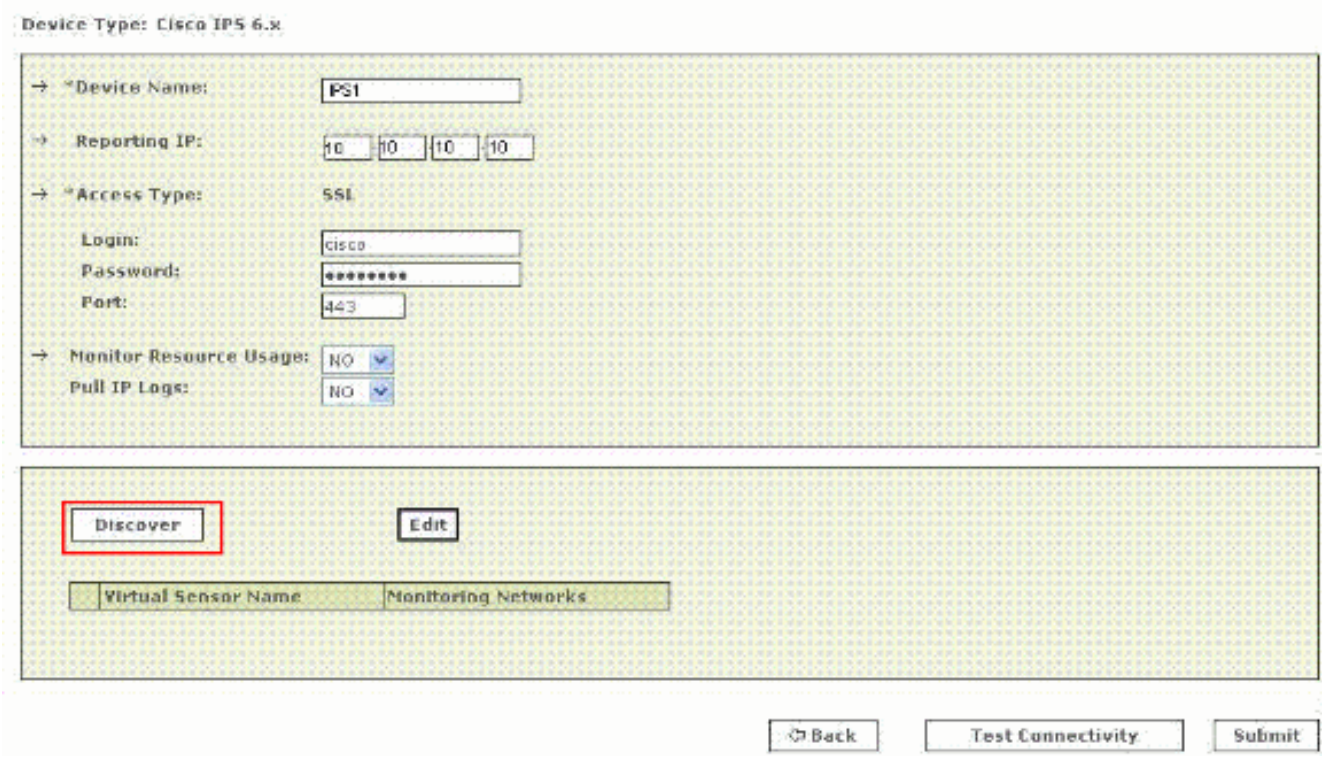


Cette configuration applique au capteur entier, qui inclut ces logs générés pour des alertes virtuelles de capteurs.

6. Cliquez sur la **Connectivité de test** afin de vérifier la configuration et activer la détection des capteurs virtuels.

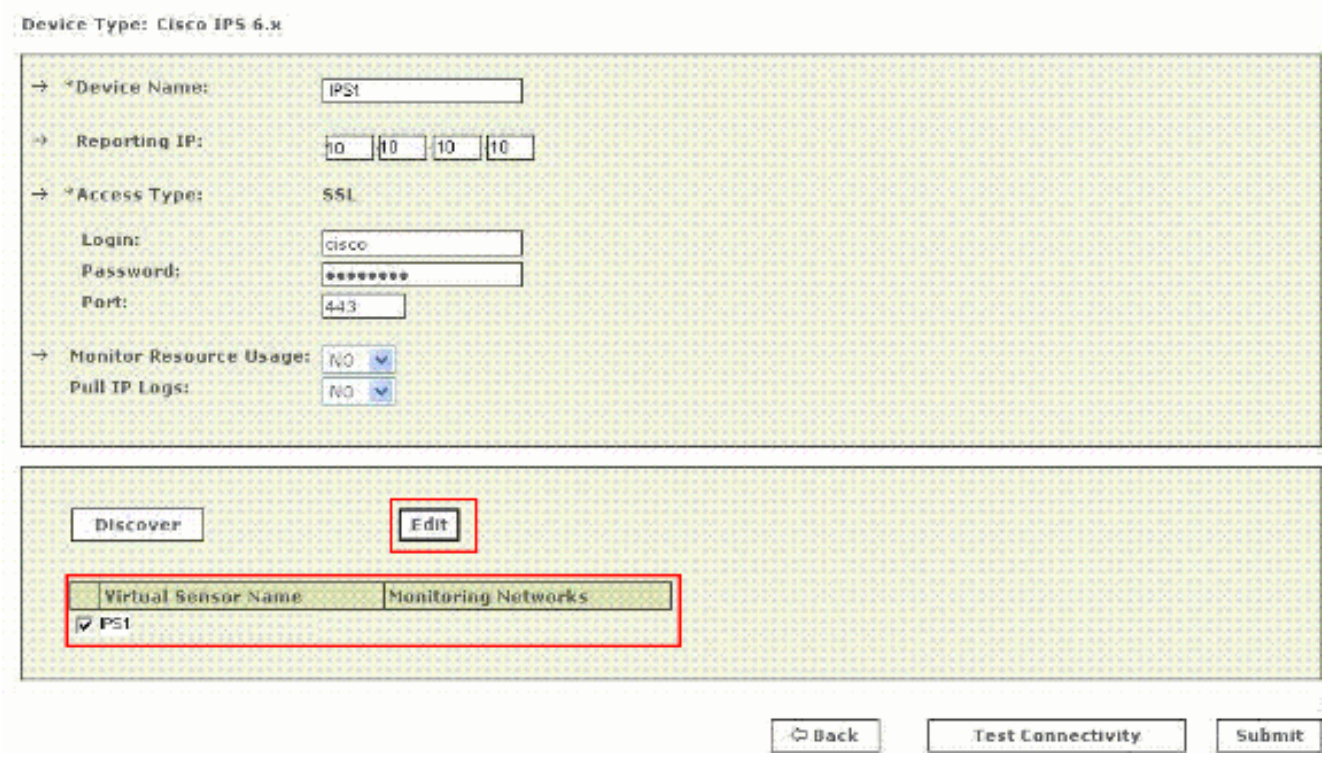


7. Le clic **les découvrent** afin de découvrir tous les capteurs virtuels définis.



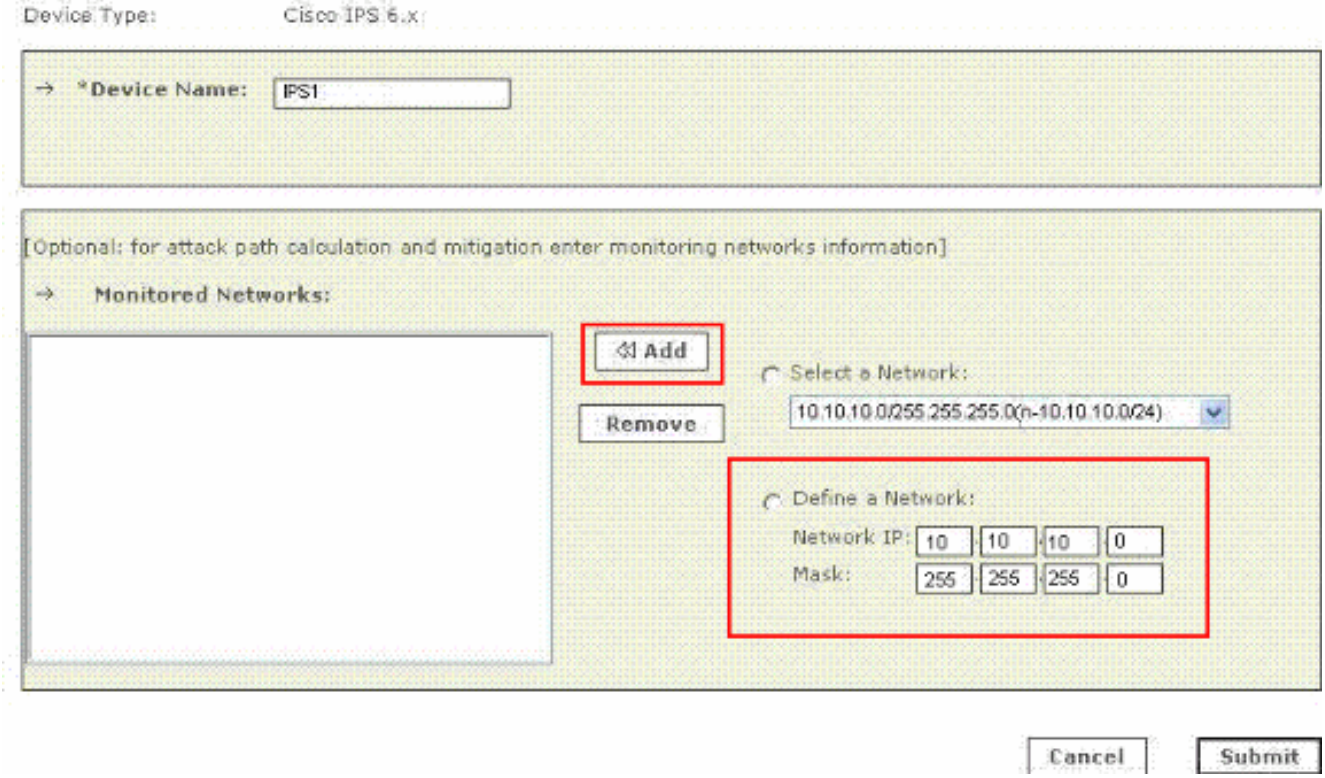
Remarque: Le MARS est inconscient des modifications apportées au capteur. Lorsque vous apportez des modifications aux configurations virtuelles de capteur, vous devez cliquer sur **découvrez à** cette page de configuration de capteur afin de régénérer les détails virtuels de capteur dans le MARS.

8. Choisissez la case à cocher à côté du nom virtuel de capteur et cliquez sur Edit afin de définir les réseaux surveillés pour chaque capteur virtuel. Maintenant la page de module IPS paraît comme affiché ici.



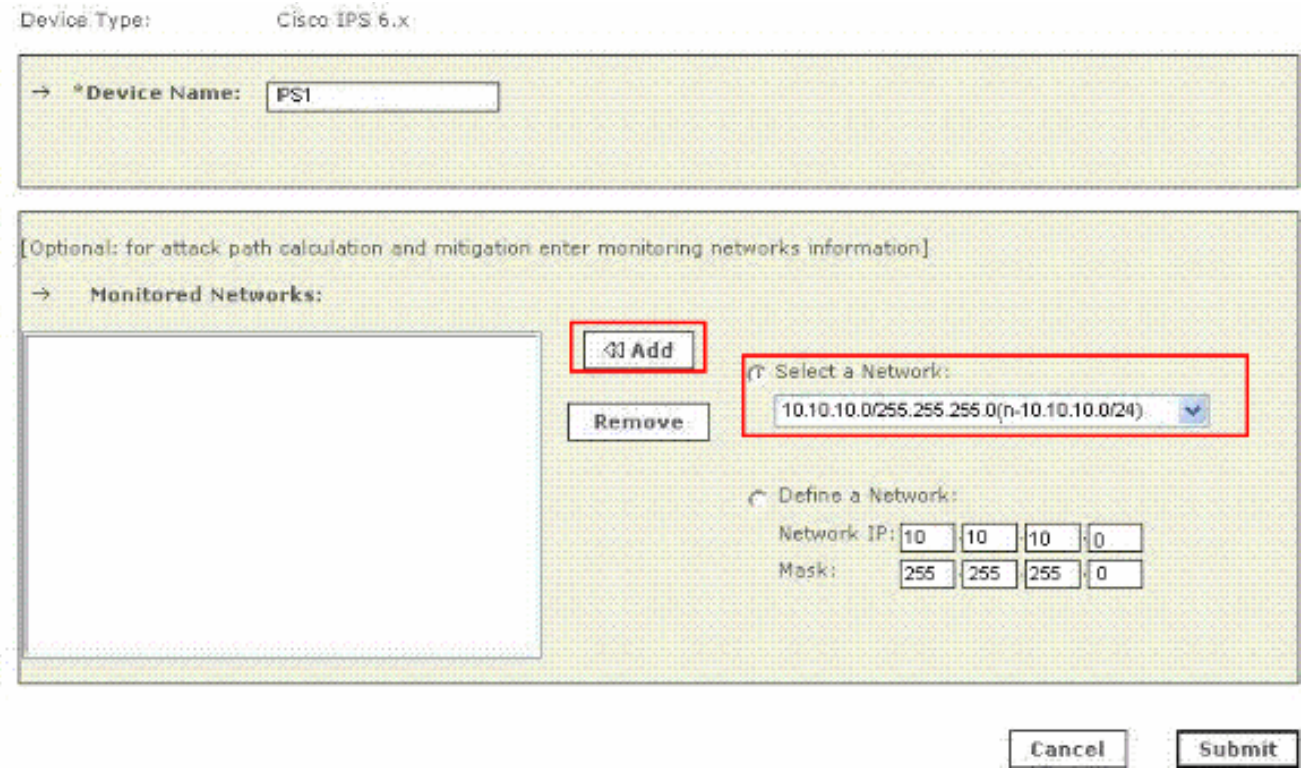
9. Pour le calcul et la réduction de chemin d'attaque, spécifiez les réseaux surveillé par le capteur. Choisissez le **définir une** case d'option de **réseau** afin de définir manuellement le

réseau. Terminez-vous alors ces étapes afin de définir un réseau :Introduisez l'adresse réseau dans le domaine **IP de réseau**.Écrivez la valeur correspondante de masque de réseau dans le domaine de **masque**.Cliquez sur Add afin d'entrer le réseau spécifié dans le champ surveillé de réseaux.Répétez les étapes précédentes s'il y a un besoin de définir plus de
réseaux.



Remarque: C'est une fonctionnalité facultative disponible et peut être ignorée sinon a exigé.

10. Cliquez sur le **choisi une** case d'option de **réseau** dans la commande sélectionnent les réseaux qui sont reliés au périphérique. Terminez-vous alors ces étapes afin de choisir les réseaux :Choisissez un réseau du **choisi une liste des réseaux**.Cliquez sur Add afin d'entrer le réseau spécifié dans le champ surveillé de réseaux.Répétez les étapes précédentes s'il y a un besoin de choisir plus de
réseaux.



Remarque: C'est une fonctionnalité facultative disponible et peut être ignorée sinon a exigé.

11. Répétez l'**étape 8 à l'étape 10** pour chaque capteur virtuel.
12. Cliquez sur Submit afin de sauvegarder vos modifications. Le nom du périphérique apparaît sous la Sécurité et la liste de l'information de surveillance. L'exécution de soumission enregistre les changements des tables de base de données. Mais, il ne charge pas les modifications dans la mémoire temporaire de travail de l'appliance de MARS. Les chargements d'exécution de lancement ont soumis des modifications dans la mémoire temporaire de travail.
13. Le clic **lancent** afin de permettre au MARS de commencer à sessionize des événements de ce périphérique.Le MARS commence à sessionize des événements générés par ce module et à évaluer ces événements utilisant les règles définies d'inspection et de baisse. Tous événements édités par le périphérique au MARS avant que le lancement puisse être questionné avec l'adresse IP d'enregistrement du périphérique comme critère de correspondance. Référez-vous lancent l'enregistrement et les périphériques de réduction. pour plus d'informations sur l'action de lancement.

Vérifiez que le MARS tire des événements d'un périphérique de Cisco IPS

Il est commun pour créer des événements bénins sur le réseau afin de vérifier le flux de données. Terminez-vous ces étapes afin de vérifier le flux de données entre un périphérique de Cisco IPS et le MARS :

1. Sur le périphérique, l'enable et l'alerte de Cisco IPS sur les signatures 2000 et 2004. Les messages ICMP de moniteur de signatures (pings).
2. Cinglez un périphérique sur le sous-réseau sur lequel le périphérique de Cisco IPS écoute. Les événements sont générés et tirés par MARS.
3. Vérifiez que les événements apparaissent dans l'interface web de MARS. Vous pouvez exécuter une requête avec le périphérique de Cisco IPS.

4. Une fois que le flux de données est vérifié, vous pouvez désactiver les 2000 et 2004 signatures sur le périphérique de Cisco IPS.**Remarque:** Si l'exécution de Connectivité de test n'échoue pas pendant la configuration d'un périphérique de Cisco IPS dans l'interface web de MARS, alors des transmissions sont activées. Cette tâche te permet pour vérifier plus loin les alertes sont générées et tirées correctement.

Dépannez

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

Informations connexes

- Page de support de Système de sécurité pour la surveillance, l'analyse et l'intervention de Cisco
- Page de support de Système de protection contre les intrusions Cisco
- Système de sécurité pour la surveillance, l'analyse et l'intervention de Cisco - Les informations sur la compatibilité
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems