Configurez le module ouvrant une session de FirePOWER pour des événements du trafic de système utilisant ASDM (la Gestion de Sur-case)

Contenu

Introduction

Ce document décrit des événements du trafic du système du module de FirePOWER et la diverse méthode d'envoyer ces événements à un serveur se connectant externe.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance du Pare-feu ASA (appliance de sécurité adaptable), ASDM (Adaptive Security Device Manager).
- La connaissance d'appareils de FirePOWER.

- Syslog, la connaissance de protocole SNMP.

Composants utilisés

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

- Version de logiciel courante 5.4.1 des modules ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) et en haut.
- Version de logiciel courante 6.0.0 du module ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) et en haut.
- ASDM 7.5(1) et en haut.

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.

Informations générales

Type d'événements

Des événements de module de FirePOWER peuvent être classés par catégorie dans deux types : -

1. Événements du trafic (événements de connexion/événements d'intrusion/événements de renseignements de sécurité Events/SSL/événements de malware/fichier).
2. Événements de système événements du système d'exploitation (de FirePOWER (SYSTÈME D'EXPLOITATION)).

Configurez

Configurer une destination de sortie

Étape 1. Configuration du serveur de Syslog

Pour configurer un serveur de Syslog pour des événements du trafic, naviguer vers la **configuration > la configuration ASA FirePOWER > les stratégies > les alertes d'actions** et cliquer sur le menu déroulant d'**alerte de création** et choisir l'option **créent l'alerte de Syslog.** Écrivez les valeurs pour le serveur de Syslog.

Nom : Spécifiez le nom qui identifie seulement le serveur de Syslog.

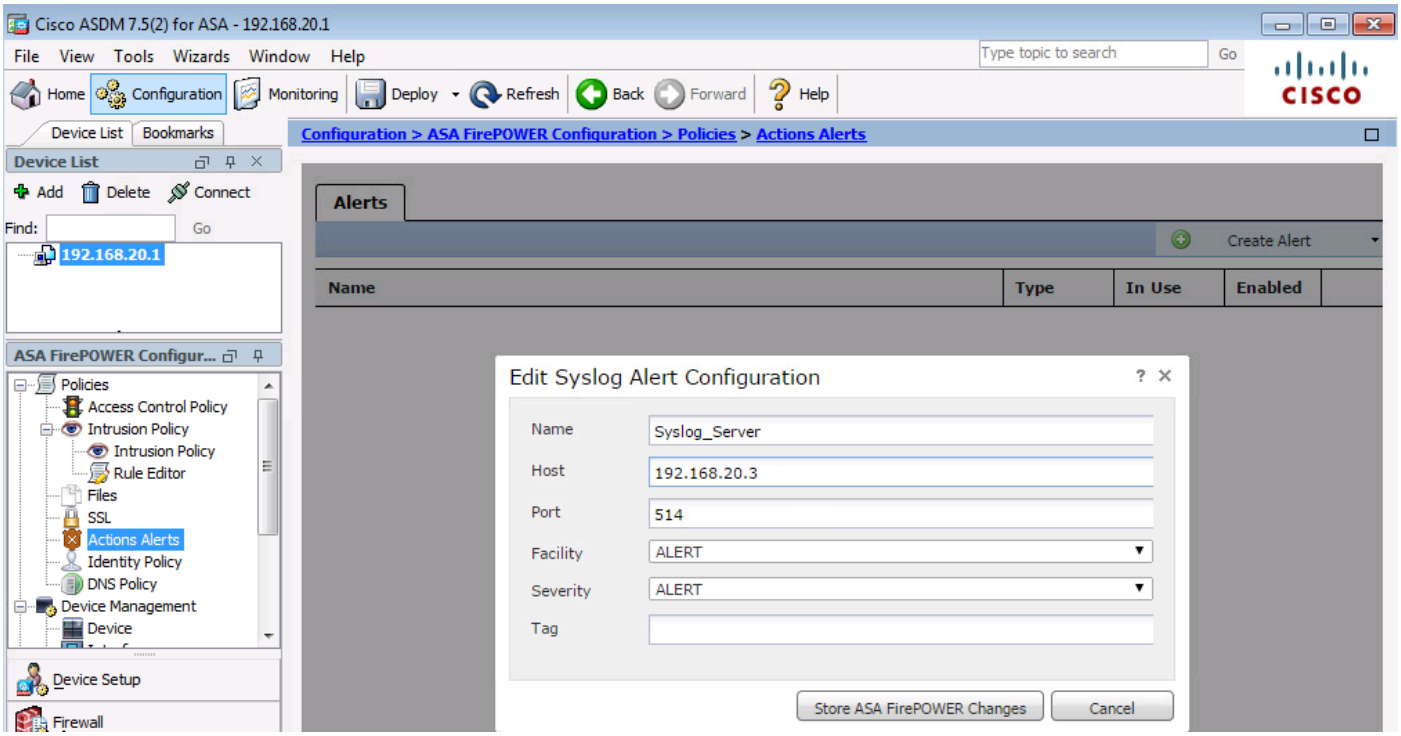
Hôte : Spécifiez l'adresse IP/adresse Internet du serveur de Syslog.

Port : Spécifiez le numéro de port du serveur de Syslog.

Installation : Sélectionnez n'importe quelle installation qui est configurée sur votre serveur de Syslog.

Sévérité : Sélectionnez n'importe quelle sévérité qui est configurée sur votre serveur de Syslog.

Balise : Spécifiez le nom de balise que vous voulez apparaître avec le message de Syslog.



Configuration du serveur de l'étape 2.SNMP

Pour configurer un serveur de déroutement SNMP pour des événements du trafic, naviguer vers la **configuration ASDM > la configuration ASA FirePOWER > les stratégies > les alertes d'actions** et cliquer sur le menu déroulant d'**alerte de création** et choisir l'option **créent l'alerte SNMP.**

Nom : Spécifiez le nom qui identifie seulement le serveur de déroutement SNMP.

Serveur de déroutement : Spécifiez l'adresse IP/adresse Internet du serveur de déroutement SNMP.

Version : Le module de FirePOWER prend en charge SNMP v1/v2/v3. Sélectionnez la version SNMP du menu de baisse vers le bas.

Chaîne de la Communauté : Si vous sélectionnez v1 ou v2 dans l'option de **version**, spécifiez le nom de communauté SNMP.

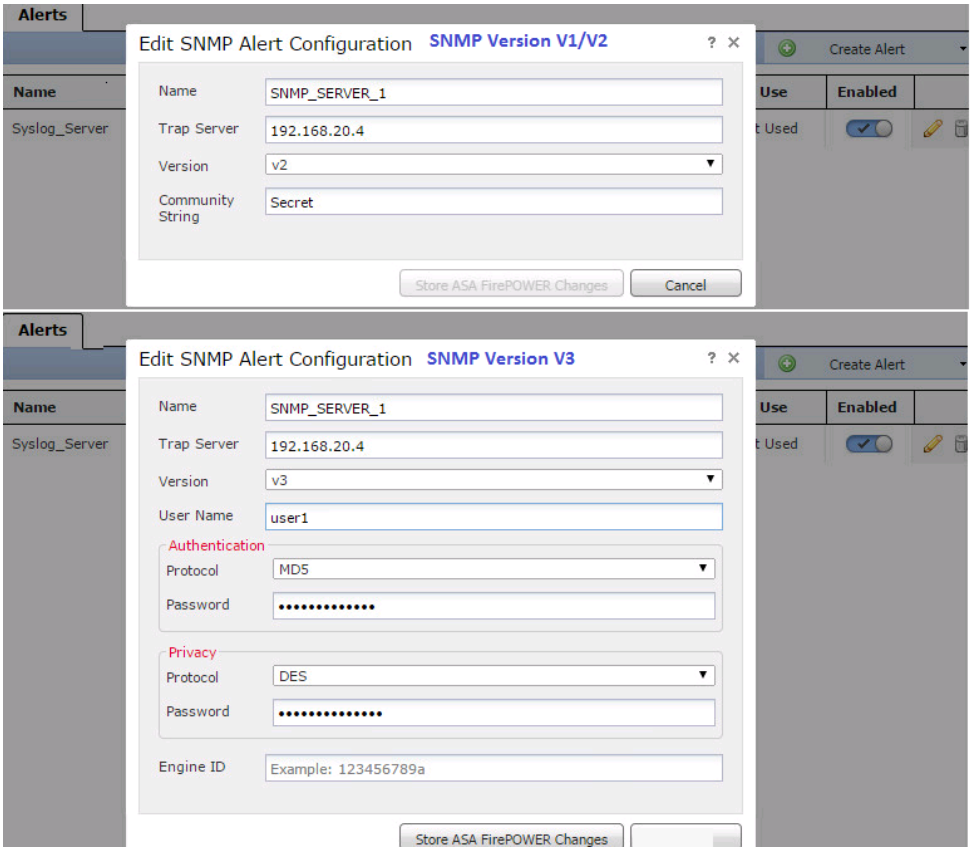
Nom d'utilisateur : Si vous sélectionnez v3 dans l'option de **version**, le **champ User Name de** systèmes invite. Spécifiez le nom d'utilisateur.

Authentification : Cette option est une partie de configuration SNMP v3. Il fournit l'authentification basée sur les informations parasites

algorithme utilisant des algorithmes de MD5 ou de SHA. Dans **Protocol** relâchez vers le bas le menu sélectionnent l'algorithme de hachage et entrent

mot de passe dans l'option de **mot de passe**. Si vous ne voulez pas utiliser cette caractéristique, alors n'en sélectionnez **aucun** option.

Intimité : Cette option est une partie de configuration SNMP v3. Il fournit le cryptage utilisant l'algorithme DES. Dans le menu de baisse de **Protocol** sélectionnez l'option comme **DES&** entrent le mot de passe dans le domaine de **mot de passe**. Si vous ne voulez pas utiliser la caractéristique de chiffrement de données, alors n'en choisissez **aucun** option.



Configuration pour envoyer les événements du trafic

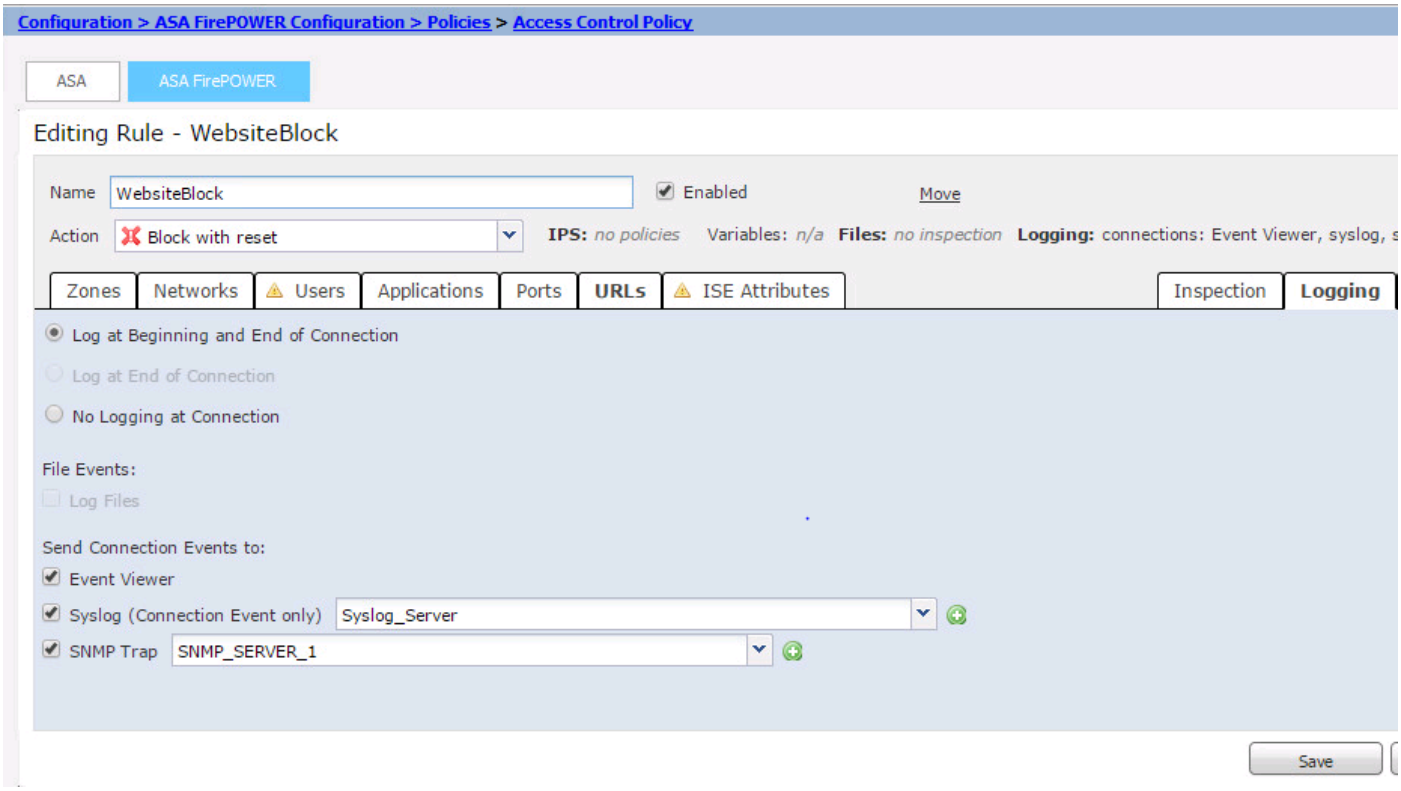
Se connecter externe d'enable pour des événements de connexion

Des événements de connexion sont générés quand le trafic frappe une règle d'accès avec le logging enabled. Afin d'activer se connecter externe pour des événements de connexion, naviguez vers **(configuration ASDM > configuration ASA FirePOWER > stratégies > stratégie de contrôle d'accès)** éditent la **règle d'accès** et naviguent vers **se connecter l'**option.

Sélectionnez le **log** se connectant d'option au **début et l'extrémité de la connexion** ou **connectez-vous à l'extrémité de la connexion**. Naviguez **pour envoyer des événements de connexion à l'**option et pour spécifier où envoyer des événements.

Afin d'envoyer des événements à un serveur externe de Syslog, à un **Syslog** choisi, et puis sélectionner une réponse d'alerte de Syslog de la liste déroulante. Sur option, vous pouvez ajouter une réponse d'alerte de Syslog en cliquant sur l'**icône d'**ajouter.

Pour envoyer des événements de connexion à un serveur de déroutement SNMP, à un **déroutement** choisi **SNMP**, et puis sélectionner une réponse d'alerte SNMP de la liste déroulante. Sur option, vous pouvez ajouter une réponse d'alerte SNMP en cliquant sur l'**icône d'**ajouter.



Se connecter externe d'enable pour des événements d'intrusion

Des événements d'intrusion sont générés quand une signature (reniflez les règles) apparie du trafic malveillant. Afin d'activer se connecter externe pour des événements d'intrusion, naviguez vers la **configuration ASDM > la configuration ASA FirePOWER > la stratégie d'intrusion de Policies> > la stratégie d'intrusion.** Créez une nouvelle stratégie d'intrusion ou éditez l'intrusion existante Policy.Navigate au **paramètre avancé** > des **réponses externes.**

Afin d'envoyer des événements d'intrusion à un serveur externe SNMP, l'option **activée** choisie dans le **SNMP alertant** et puis cliquer sur l'option d'**éditer**.

Type de déroutement : Le type de déroutement est utilisé pour les adresses IP qui apparaissent dans les alertes. Si votre système d'administration de réseaux rend correctement le type de l'adresse INET_IPV4, alors vous pouvez sélectionner comme binaire. Autrement, choisi en tant que chaîne.

Version SNMP : Sélectionnez la case d'option de **version 2** ou de **version 3**.

Option SNMP v2

Serveur de déroutement : Spécifiez l'adresse IP/adresse Internet du serveur de déroutement SNMP, suivant les indications de cette image.

Chaîne de la Communauté : Spécifiez le nom de communauté.

Option SNMP v3

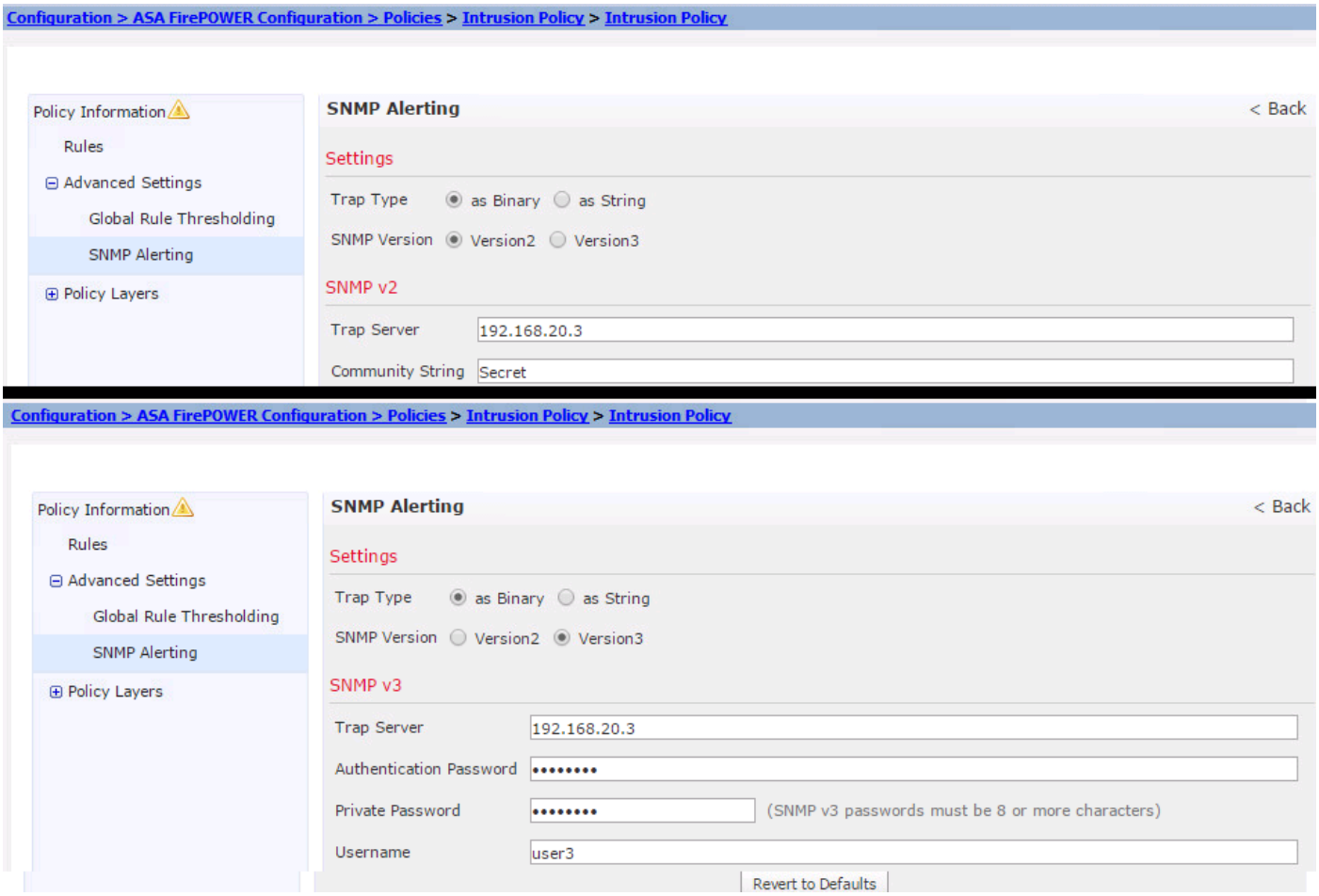
Serveur de déroutement : Spécifiez l'adresse IP/adresse Internet du serveur de déroutement SNMP, suivant les indications de cette image.

Mot de passe d'authentification : Specifypassword a exigé pour l'authentification. SNMP v3

emploie la fonction d'informations parasites pour authentifier le mot de passe.

Mot de passe privé : Spécifiez le mot de passe pour le cryptage. SNMP v3 emploie le chiffre par bloc de Norme de chiffrement de données (DES) pour chiffrer ce mot de passe.

Nom d'utilisateur : Spécifiez le nom d'utilisateur.



Afin d'envoyer des événements d'intrusion à un serveur externe de Syslog, l'option choisie **activée** dans le **Syslog alertant** alors cliquent sur l'option d'**éditer**, suivant les indications de cette image.

Hôte de journalisation : Spécifiez l'adresse IP/adresse Internet du serveur de Syslog.

Installation : Sélectionnez n'importe quelle installation qui est configurée sur votre serveur de Syslog.

Sévérité : Sélectionnez n'importe quelle sévérité qui est configurée sur votre serveur de Syslog.

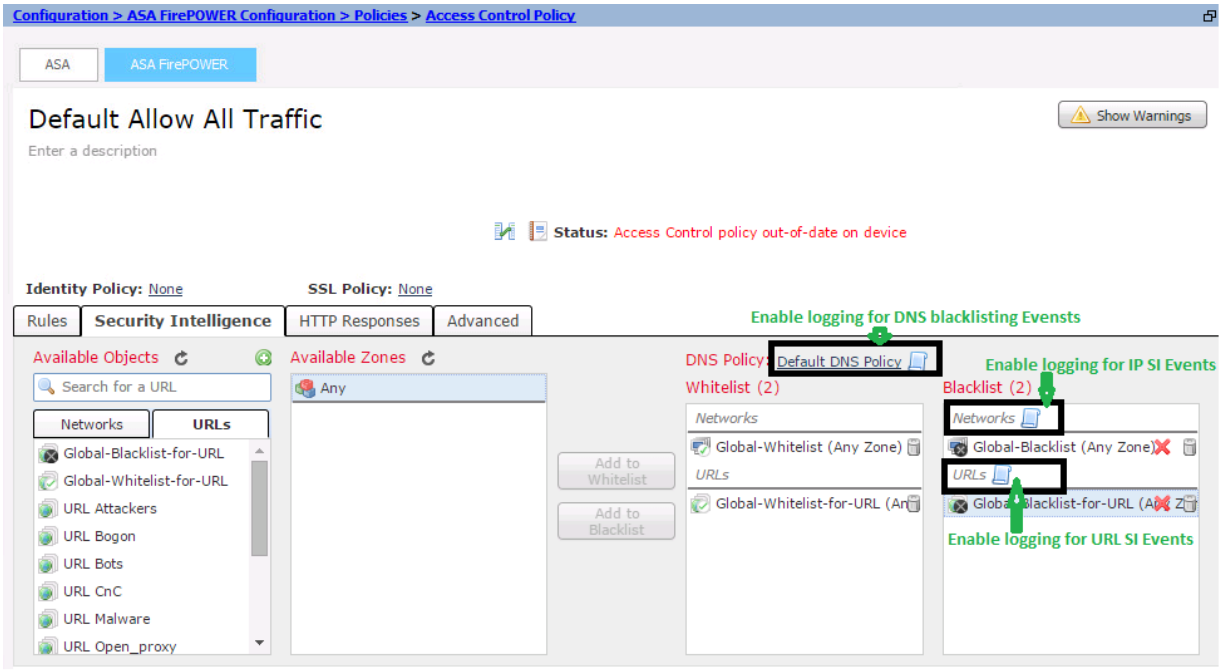
Activez se connecter externe pour des renseignements de sécurité de la Sécurité Intelligence/URL de la sécurité IP Intelligence/DNS

Des événements de **renseignements de sécurité de la Sécurité Intelligence/URL de la sécurité IP Intelligence/DNS** sont générés quand le trafic apparie n'importe quelle base de données de renseignements de sécurité d'adresse IP/nom de domaine /URL. Afin d'activer se connecter externe pour des événements de renseignements de sécurité IP URL/DNS, naviguez vers **(configuration ASDM > configuration ASA FirePOWER > stratégies > stratégie > renseignements de sécurité de contrôle d'accès)**,

Cliquez sur l'**icône** suivant les indications de l'image pour activer se connecter pour des renseignements de sécurité IP/DNS/URL. Cliquer sur l'icône incite une boîte de dialogue pour activer se connecter et option pour envoyer les événements au serveur externe.

Afin d'envoyer des événements à un serveur externe de Syslog, à un **Syslog** choisi, et puis sélectionner une réponse d'alerte de Syslog de la liste déroulante. Sur option, vous pouvez ajouter une réponse d'alerte de Syslog en cliquant sur l'icône d'ajouter.

Afin d'envoyer des événements de connexion à un serveur de déroutement SNMP, à un **déroutement** choisi **SNMP**, et puis sélectionner une réponse d'alerte SNMP de la liste déroulante. Sur option, vous pouvez ajouter une réponse d'alerte SNMP en cliquant sur l'icône d'ajouter.



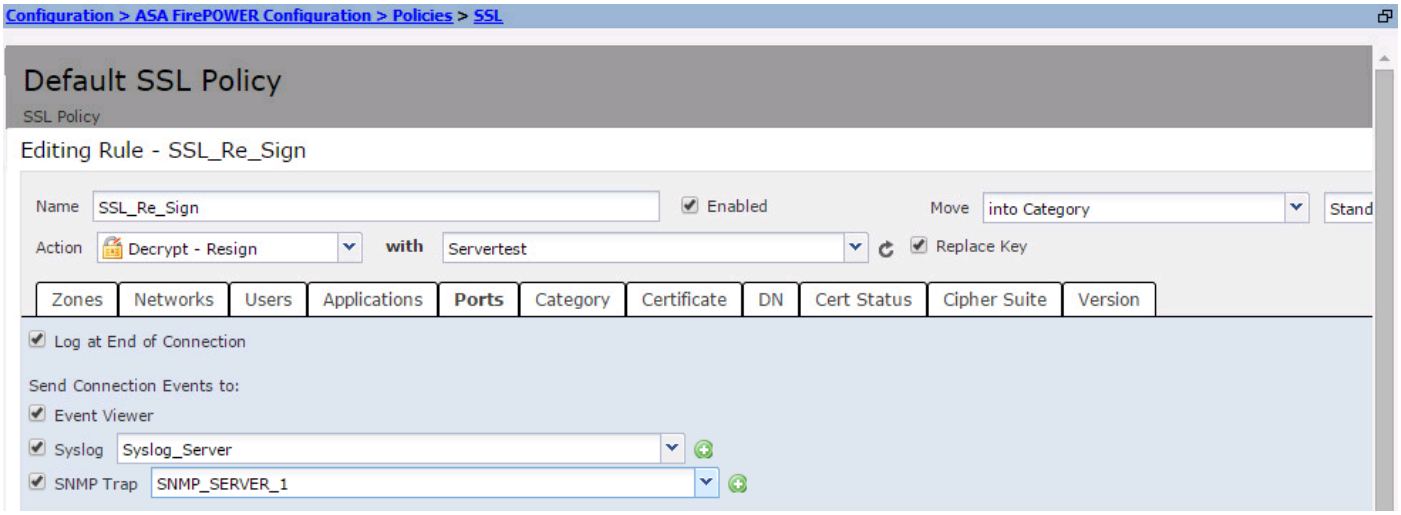
Se connecter externe d'enable pour des événements SSL

Des événements SSL sont générés quand le trafic apparie n'importe quelle règle dans la stratégie SSL, dans laquelle se connecter est activé. Afin d'activer se connecter externe pour le trafic SSL, naviguez vers la **configuration ASDM > la configuration > les stratégies > le SSL ASA FirePOWER.** Éditez exister ou créez une nouvelle règle et naviguez vers **se connecter l'**option. Sélectionnez le **log à la fin de la possibilité de connexion**.

Naviguez alors **pour envoyer des événements de connexion à** et pour spécifier où envoyer les événements.

Pour envoyer des événements à un serveur externe de Syslog, à un **Syslog** choisi, et puis sélectionner une réponse d'alerte de Syslog de la liste déroulante. Sur option, vous pouvez ajouter une réponse d'alerte de Syslog en cliquant sur l'icône d'ajouter.

Pour envoyer des événements de connexion à un serveur de déroutement SNMP, à un **déroutement** choisi **SNMP**, et puis sélectionner une réponse d'alerte SNMP de la liste déroulante. Sur option, vous pouvez ajouter une réponse d'alerte SNMP en cliquant sur l'icône d'ajouter.



Configuration pour envoyer les événements de système

Se connecter externe d'enable pour des événements de système

Les événements de système affichent le statut de système d'exploitation de FirePOWER. Le SNMP Manager peut être utilisé pour voter ces événements de systèmes.

Pour configurer le serveur SNMP afin de voter des événements de système de module de FirePOWER, vous devez configurer une stratégie de système qui fait les informations disponibles dans MIB de firePOWER (Management Information Base) qui peut être voté par le serveur SNMP.

Naviguez vers la **configuration ASDM > la configuration ASA FirePOWER > la stratégie de gens du pays > de système** et cliquez sur le **SNMP**.

Version SNMP : Le module de FirePOWER prend en charge SNMP v1/v2/v3. Spécifiez la version SNMP.

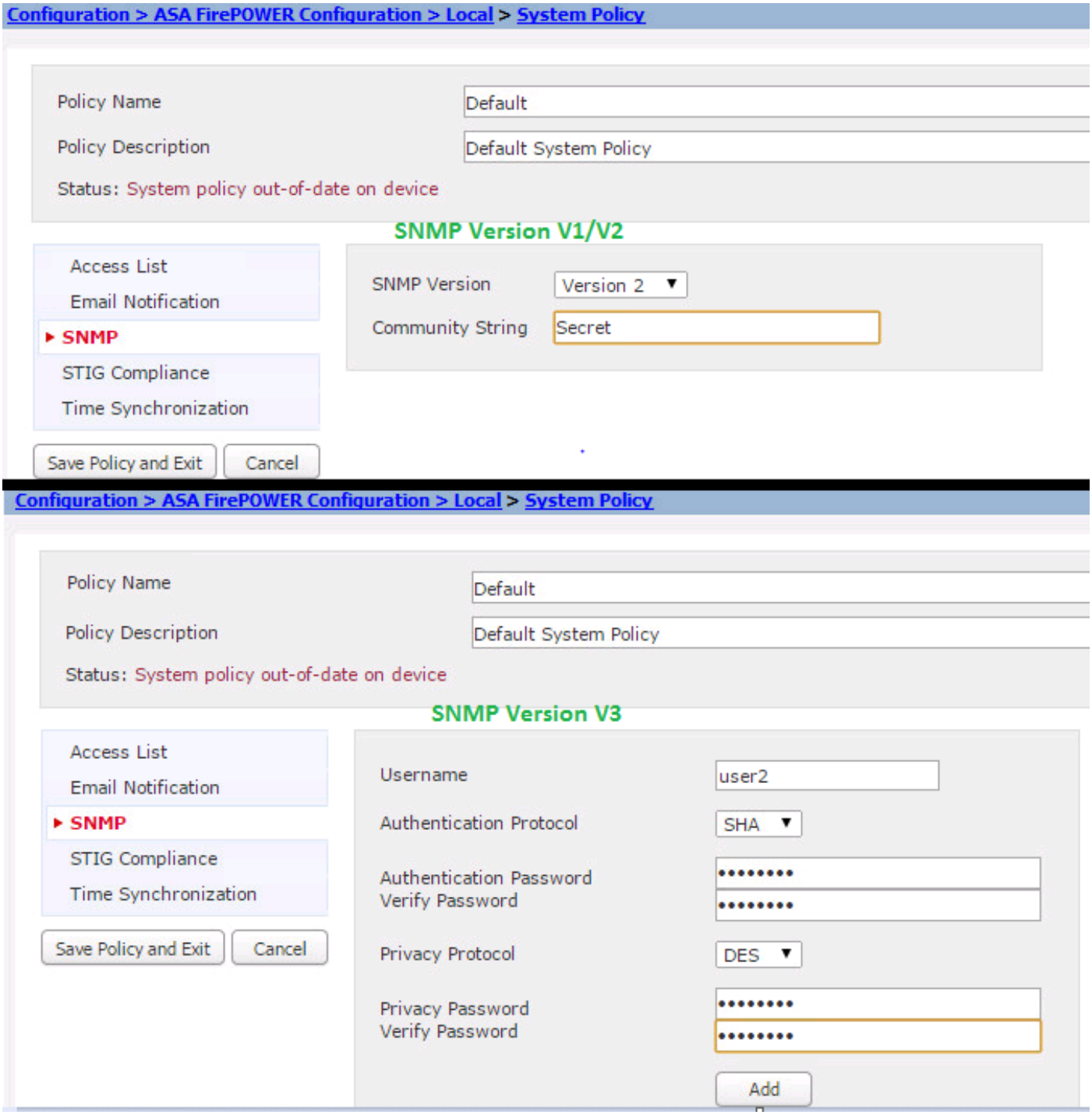
Chaîne de la Communauté : Si vous sélectionnez **v1/ v2** dans l'option de version SNMP, introduisez le nom de la communauté SNMP dans le domaine de chaîne de la Communauté.

Nom d'utilisateur : Si vous sélectionnez l'option **v3** dans l'option de version. Cliquez sur le bouton d'**utilisateur d'ajouter** et spécifiez le **nom d'utilisateur** dans le domaine de nom d'utilisateur.

Authentification : Cette option est une partie de configuration SNMP v3. Il fournit l'authentification basée sur le code haché d'authentification de message utilisant des algorithmes de MD5 ou de SHA. Choisissez **Protocol** pour l'algorithme de hachage et entrez le mot de passe

dans le domaine de **mot de passe**. Si vous ne voulez pas utiliser la fonction d'authentification alors n'en sélectionnez **aucun** option.

Intimité : Cette option est une partie de configuration SNMP v3. Il fournit le cryptage utilisant l'algorithme DES/AES. Le protocole choisi pour le cryptage et entrent le mot de passe dans le domaine de **mot de passe**. Si vous ne voulez pas la caractéristique de chiffrement de données alors n'en choisissez **aucun** option.



Note: Un Management Information Base (MIB) est une collecte d'informations qui est organisé hiérarchiquement. Le fichier MIB (DCEALERT.MIB) pour le module de FirePOWER est disponible à l'emplacement de répertoire (/etc/sf/DCEALERT.MIB) qui peut être cherché de cet emplacement de répertoire.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

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

Informations connexes

- Support et documentation techniques - Cisco Systems