Configurer la connexion au module Firepower pour les événements système/trafic à l'aide d'ASDM (gestion intégrée)

Contenu

Introduction

Ce document décrit les événements système/trafic du module Firepower et diverses méthodes d'envoi de ces événements à un serveur de journalisation externe.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance du pare-feu ASA (Adaptive Security Appliance), ASDM (Adaptive Security Device Manager).
- Connaissances de l'appliance Firepower.

- Syslog, connaissance du protocole SNMP.

Components Used

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

- Modules ASA Firepower (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) exécutant le logiciel version 5.4.1 et ultérieure.
- Module ASA Firepower (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) exécutant le logiciel version 6.0.0 et ultérieure.
- ASDM 7.5(1) et plus.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Type d'événements

Les événements du module Firepower peuvent être classés en deux types : -

1. Événements de trafic (événements de connexion/d'intrusion/événements de veille de sécurité/événements SSL/programmes malveillants/événements de fichiers).
2. Événements système (événements du système d'exploitation Firepower).

Configuration

Configuration d'une destination de sortie

Étape 1. Configuration du serveur Syslog

Pour configurer un serveur Syslog pour les événements de trafic, accédez à **Configuration > ASA Firepower Configuration > Policies > Actions Alerts** et cliquez sur le menu déroulant **Créer une alerte** et choisissez l'option **Créer une alerte Syslog.** Saisissez les valeurs du serveur Syslog.

Name : spécifiez le nom qui identifie de manière unique le serveur Syslog.

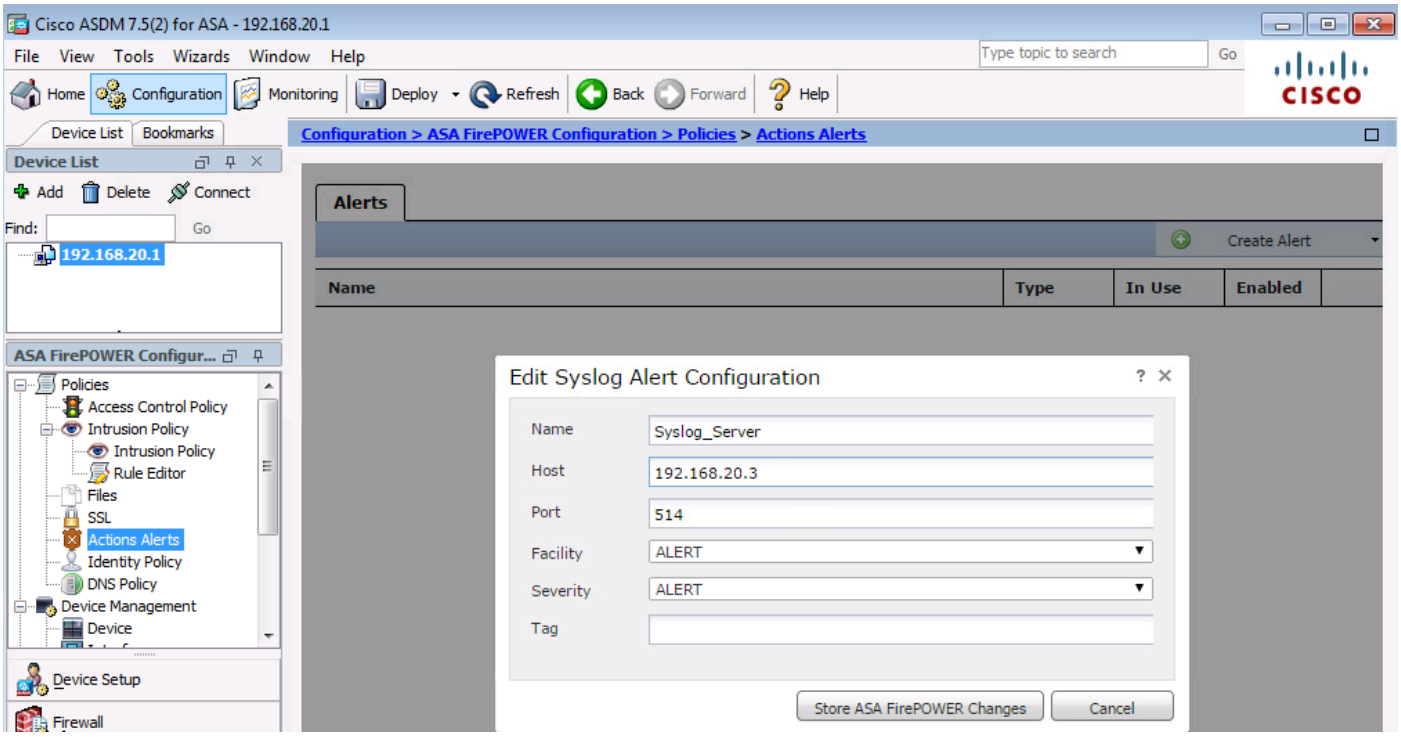
Hôte : spécifiez l'adresse IP/le nom d'hôte du serveur Syslog.

Port : spécifiez le numéro de port du serveur Syslog.

Installation : Sélectionnez une installation configurée sur votre serveur Syslog.

Gravité : sélectionnez une gravité configurée sur votre serveur Syslog.

Balise : spécifiez le nom de la balise que vous voulez afficher avec le message Syslog.



Étape 2.Configuration du serveur SNMP

Pour configurer un serveur d'interruption SNMP pour les événements de trafic, accédez à **Configuration ASDM > Configuration ASA Firepower > Politiques > Actions Alertes** et cliquez sur le menu déroulant **Créer une alerte** et choisissez l'option **Créer une alerte SNMP.**

Name : spécifiez le nom qui identifie de manière unique le serveur d'interruption SNMP.

Serveur d'interruption : spécifiez l'adresse IP/le nom d'hôte du serveur d'interruption SNMP.

Version : le module Firepower prend en charge SNMP v1/v2/v3. Sélectionnez la version SNMP dans le menu déroulant.

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

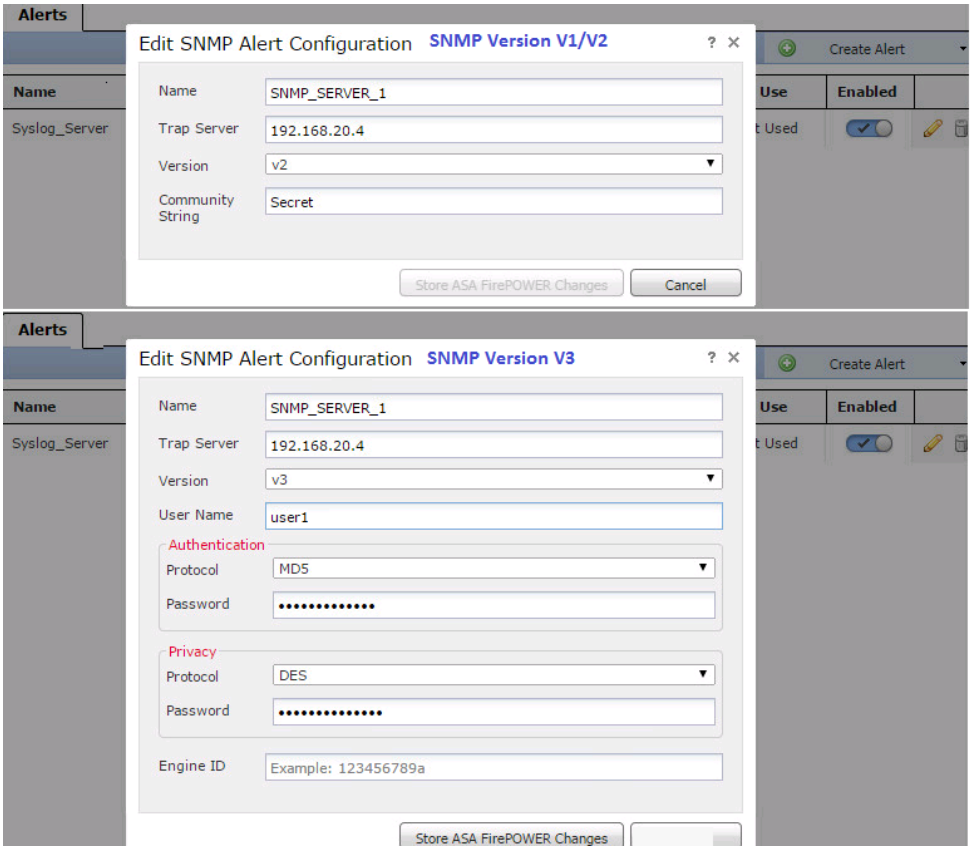
Nom d'utilisateur : Si vous sélectionnez v3 dans l'option **Version**, le système invite le champ **Nom d'utilisateur**. Spécifiez le nom d'utilisateur.

Authentification : cette option fait partie de la configuration SNMP v3. Il fournit une authentification basée sur le hachage

àl'aide d'algorithmes MD5 ou SHA. Dans le menu déroulant **Protocole**, sélectionnez l'algorithme de hachage et saisissez

mot de passe dans l'option **Mot de passe**. Si vous ne souhaitez pas utiliser cette fonction, sélectionnez l'option **Aucun**.

Confidentialité : Cette option fait partie de la configuration SNMP v3. Il fournit le chiffrement à l'aide de l'algorithme DES. Dans le menu déroulant **Protocole**, sélectionnez l'option **DES** et saisissez le mot de passe dans le champ **Mot de passe**. Si vous ne souhaitez pas utiliser la fonction de chiffrement des données, sélectionnez l'option **Aucun**.



Configuration de l'envoi des événements de trafic

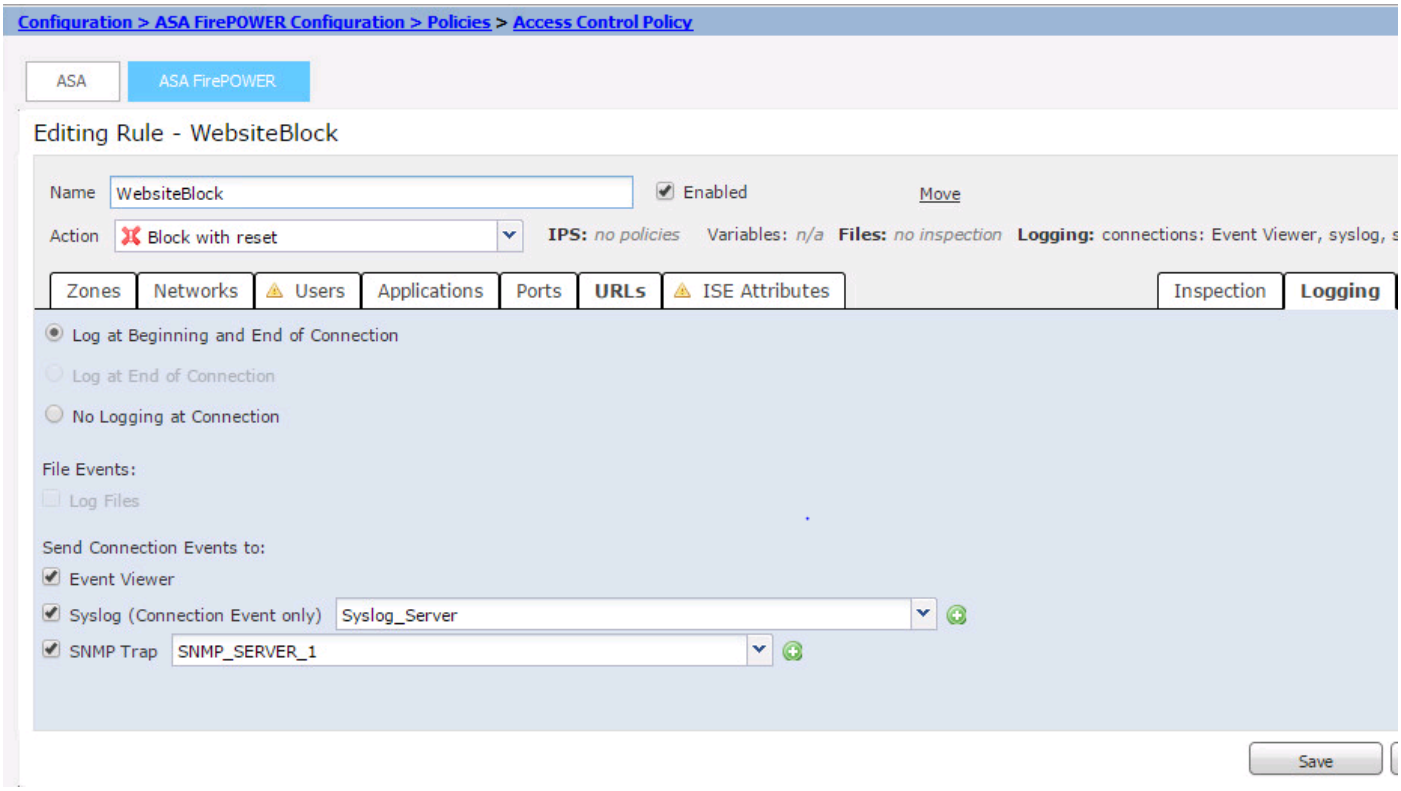
Activer la journalisation externe pour les événements de connexion

Les événements de connexion sont générés lorsque le trafic atteint une règle d'accès avec la journalisation activée. Afin d'activer la journalisation externe pour les événements de connexion, naviguez jusqu'à **(Configuration ASDM > Configuration ASA Firepower > Stratégies > Stratégie de contrôle d'accès)** modifiez la **règle d'accès** et naviguez jusqu'à l'option **de journalisation**.

Sélectionnez l'option de journalisation **log au début et à la fin de la connexion** ou **log à la fin de la connexion**. Accédez à l'option **Envoyer des événements de connexion à** et indiquez où envoyer les événements.

Afin d'envoyer des événements à un serveur Syslog externe, sélectionnez **Syslog**, puis sélectionnez une réponse d'alerte Syslog dans la liste déroulante. Vous pouvez éventuellement ajouter une réponse d'alerte Syslog en cliquant sur l'**icône** Ajouter.

Pour envoyer des événements de connexion à un serveur d'interruptions SNMP, sélectionnez **Interruption SNMP**, puis sélectionnez une réponse d'alerte SNMP dans la liste déroulante. Vous pouvez éventuellement ajouter une réponse d'alerte SNMP en cliquant sur l'**icône** Ajouter.



Activer la journalisation externe pour les événements d'intrusion

Des événements d'intrusion sont générés lorsqu'une signature (règles de renversement) correspond à un trafic malveillant. Afin d'activer la journalisation externe pour les événements d'intrusion, accédez à **Configuration ASDM > Configuration ASA Firepower > Stratégies > Stratégie d'intrusion > Stratégie d'intrusion.** Créez une nouvelle stratégie d'intrusion ou modifiez la stratégie d'intrusion existante.Accédez à **Paramètres avancés > Réponses externes.**

Afin d'envoyer des événements d'intrusion à un serveur SNMP externe, sélectionnez l'option **Enabled** dans **SNMP Alerting**, puis cliquez sur l'option **Edit**.

Type de déroutement : Le type de déroutement est utilisé pour les adresses IP qui apparaissent dans les alertes. Si votre système de gestion de réseau affiche correctement le type d'adresse INET_IPV4, vous pouvez le sélectionner en tant que binaire. Sinon, sélectionnez String.

Version SNMP : Sélectionner **Version 2** ou **Version 3** bouton radio.

Option SNMP v2

Serveur de déroutement : Spécifiez l'adresse IP/le nom d'hôte du serveur d'interruptions SNMP, comme illustré dans cette image.

Chaîne de communauté : Spécifiez le nom de la communauté.

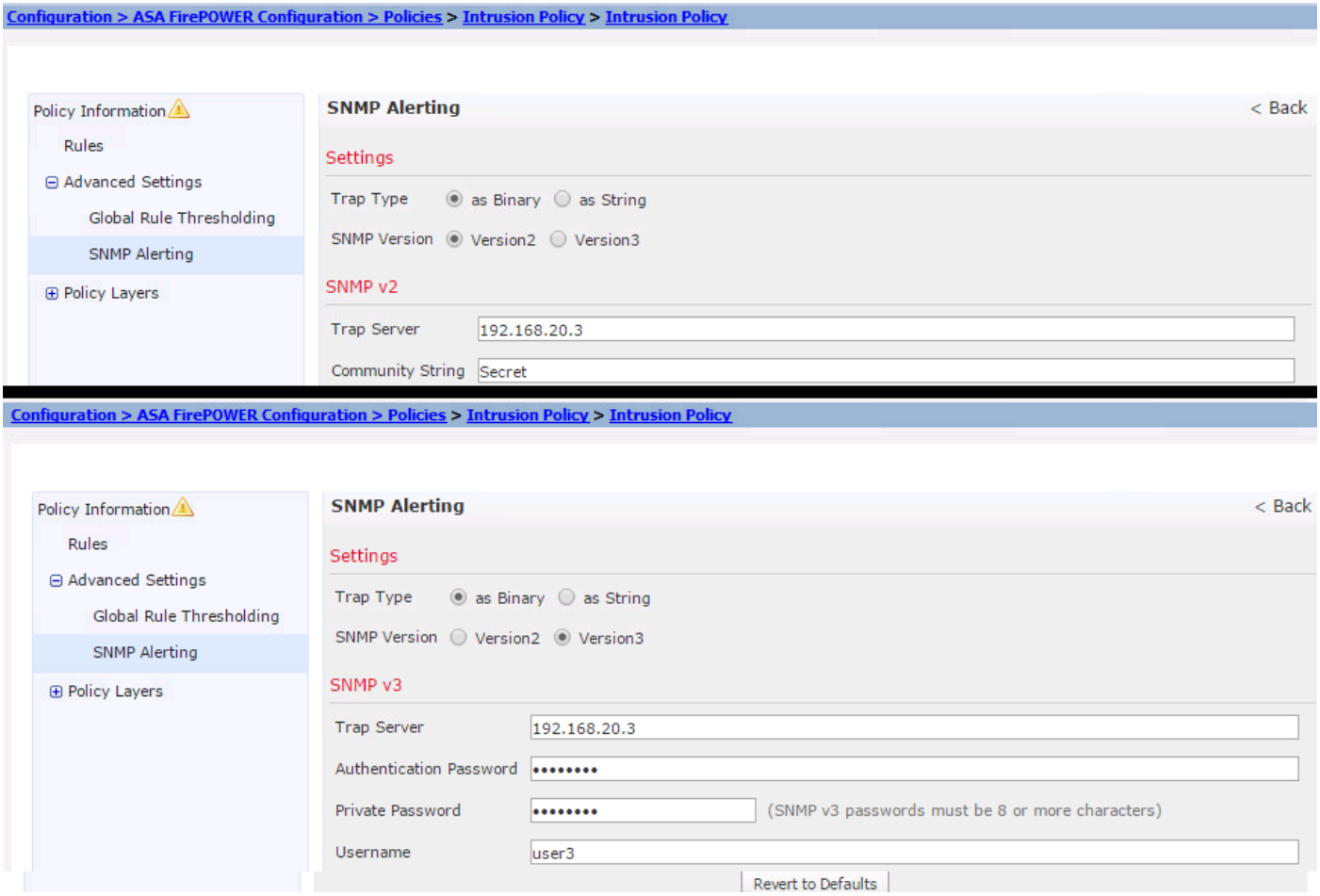
Option SNMP v3

Serveur de déroutement : Spécifiez l'adresse IP/le nom d'hôte du serveur d'interruptions SNMP, comme illustré dans cette image.

Mot de passe d'authentification : Spécifiermot de passe requis pour l'authentification. SNMP v3 utilise la fonction de hachage pour authentifier le mot de passe.

Mot de passe privé : spécifiez le mot de passe pour le chiffrement. SNMP v3 utilise le chiffrement de bloc DES (Data Encryption Standard) pour chiffrer ce mot de passe.

nom de l'utilisateur: Spécifiez le nom d'utilisateur.



Afin d'envoyer des événements d'intrusion à un serveur Syslog externe, sélectionnez l'option **Activée** dans **Syslog Alerte** puis cliquez sur le bouton **Modifier** , comme illustré dans cette image.

Hôte de journalisation : Spécifiez l'adresse IP/le nom d'hôte du serveur Syslog.

Installation : Sélectionner une installation qui est configuré sur votre serveur Syslog.

Gravité : Sélectionnez une gravité configurée sur votre serveur Syslog.

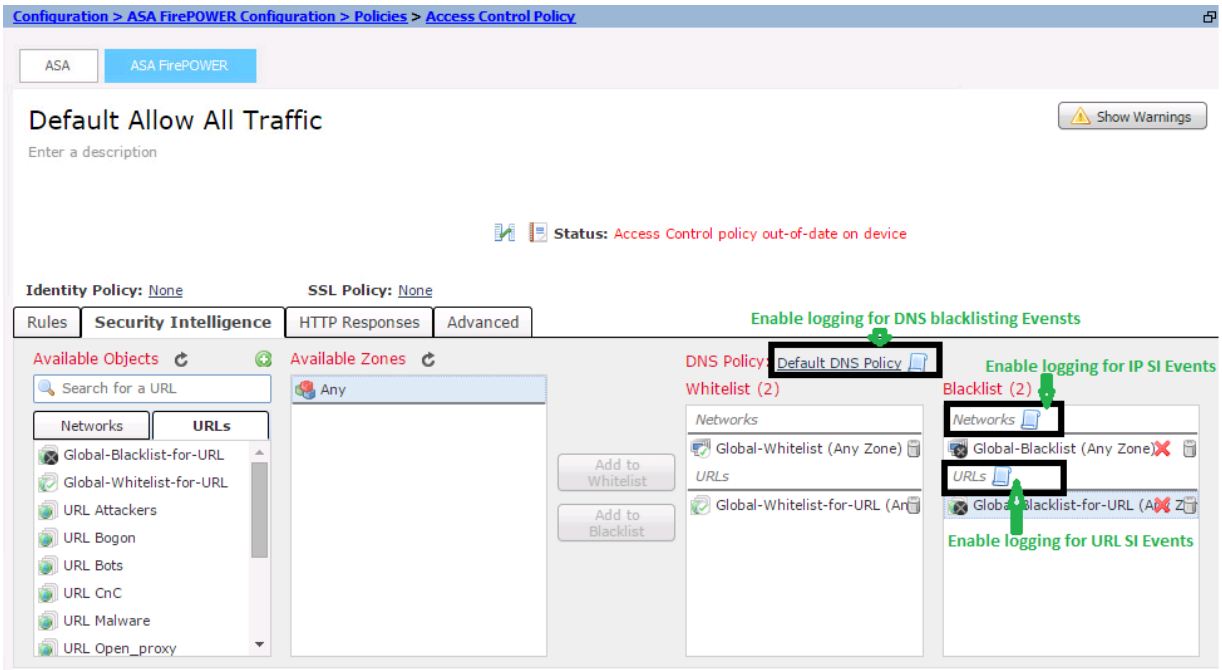
Activer la journalisation externe pour IP Security Intelligence/DNS Security Intelligence/URL Security Intelligence

Les événements **IP Security Intelligence/DNS Security Intelligence/URL Security Intelligence** sont générés lorsque le trafic correspond à n'importe quelle adresse IP/nom de domaine/base de données URL Security Intelligence. Afin d'activer la journalisation externe pour les événements de sécurité IP/URL/DNS, accédez à **(Configuration ASDM > Configuration ASA Firepower > Stratégies > Politique de contrôle d'accès > Intelligence de sécurité)**,

Cliquez sur l'**icône** telle qu'illustrée dans l'image pour activer la journalisation pour IP/DNS/URL Security Intelligence. Cliquez sur l'icône pour afficher une boîte de dialogue permettant d'activer la journalisation et d'envoyer les événements au serveur externe.

Afin d'envoyer des événements à un serveur Syslog externe, sélectionnez **Syslog**, puis sélectionnez une réponse d'alerte Syslog dans la liste déroulante. Vous pouvez éventuellement ajouter une réponse d'alerte Syslog en cliquant sur l'icône Ajouter.

Afin d'envoyer des événements de connexion à un serveur de déroutement SNMP, sélectionnez **déroutement SNMP**, puis sélectionnez une réponse d'alerte SNMP dans la liste déroulante. Vous pouvez éventuellement ajouter une réponse d'alerte SNMP en cliquant sur l'icône Ajouter.



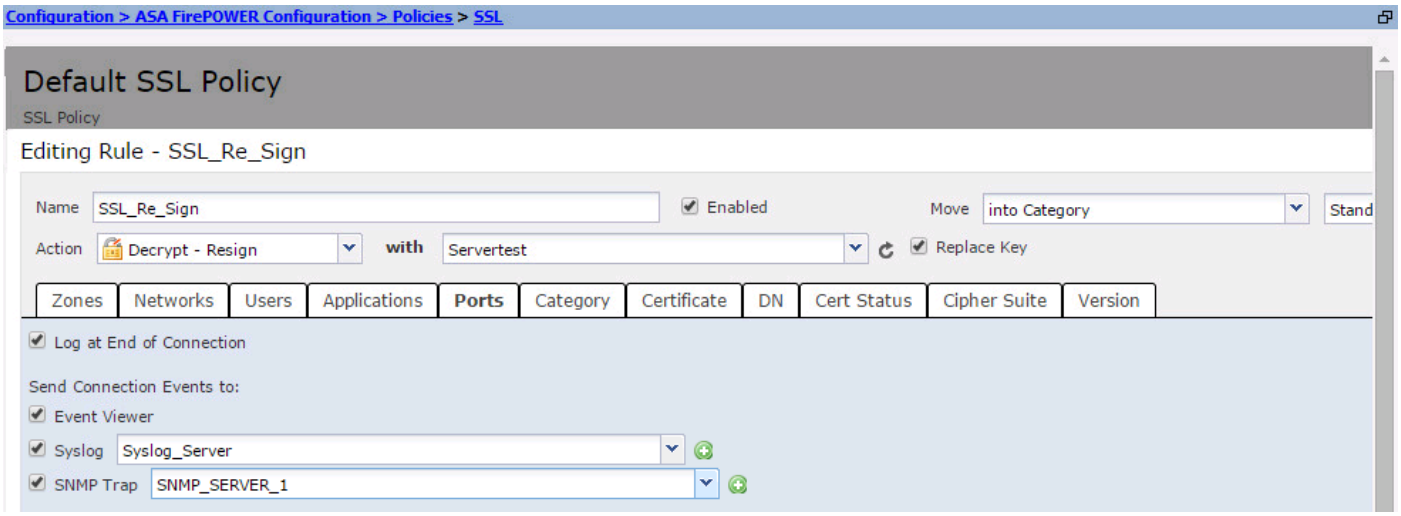
Activer la journalisation externe pour les événements SSL

Les événements SSL sont générés lorsque le trafic correspond à une règle de la stratégie SSL, dans laquelle la journalisation est activée. Afin d'activer la journalisation externe pour le trafic SSL, accédez à **Configuration ASDM > Configuration ASA Firepower > Politiques > SSL.** Modifiez la règle existante ou créez-en une et accédez à l'option **logging**.Sélectionnez **log à la fin de la connexion**.

Naviguez ensuite jusqu'à **Envoyer des événements de connexion à** et indiquez où envoyer les événements.

Pour envoyer des événements à un serveur Syslog externe, sélectionnez **Syslog**, puis sélectionnez une réponse d'alerte Syslog dans la liste déroulante. Vous pouvez éventuellement ajouter une réponse d'alerte Syslog en cliquant sur l'icône Ajouter.

Pour envoyer des événements de connexion à un serveur d'interruptions SNMP, sélectionnez **Interruption SNMP**, puis sélectionnez une réponse d'alerte SNMP dans la liste déroulante. Vous pouvez éventuellement ajouter une réponse d'alerte SNMP en cliquant sur l'icône Ajouter.



Configuration de l'envoi des événements système

Activer la journalisation externe pour les événements système

Les événements système indiquent l'état du système d'exploitation Firepower. Le gestionnaire SNMP peut être utilisé pour interroger ces événements système.

Pour configurer le serveur SNMP afin d'interroger les événements système à partir de Firepower Module, vous devez configurer une stratégie système qui rend les informations disponibles dans la base MIB de Firepower (Management Information Base) qui peut être interrogée par le serveur SNMP.

Accédez à **Configuration ASDM > Configuration ASA Firepower > Local > System Policy** et cliquez sur le **protocole SNMP**.

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

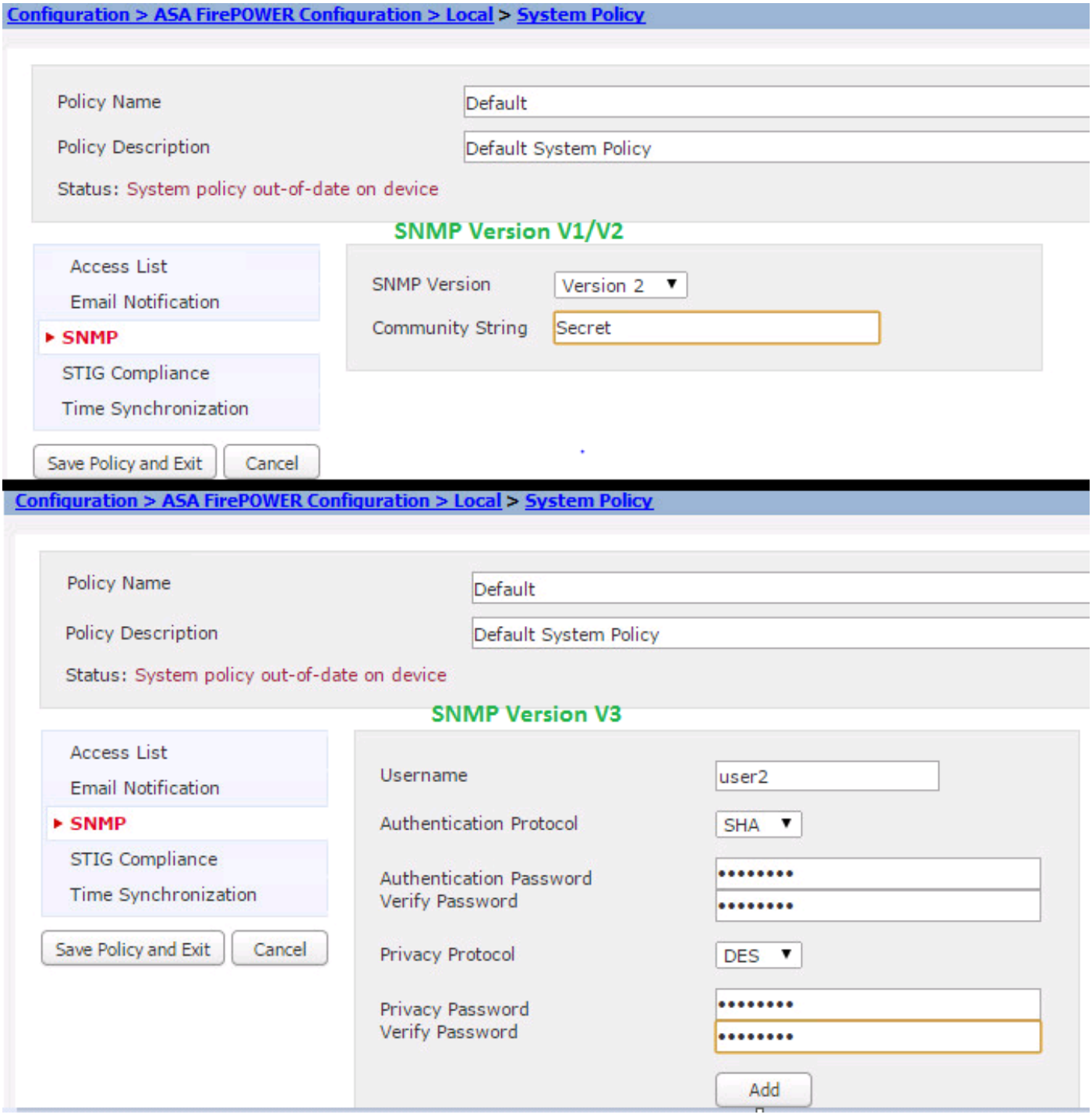
Chaîne de communauté : Si vous sélectionnez **v1/ v2** dans l'option de version SNMP, tapez le nom de la communauté SNMP dans le champ Chaîne de communauté.

username (nom d'utilisateur) : Si vous sélectionnez l'option **v3** dans la version. Cliquez sur le bouton **Ajouter un utilisateur** et spécifiez le **nom d'utilisateur** dans le champ Nom d'utilisateur.

Authentification : cette option fait partie de la configuration SNMP v3. Il fournit une authentification basée sur le code d'authentification des messages hachés à l'aide d'algorithmes MD5 ou SHA. Choisissez **Protocol** pour l'algorithme de hachage et saisissez le mot de passe

dans le champ **Mot de passe**. Si vous ne souhaitez pas utiliser la fonction d'authentification, sélectionnez **Aucune** option.

Confidentialité : Cette option fait partie de la configuration SNMP v3. Il fournit le chiffrement à l'aide de l'algorithme DES/AES. Sélectionnez le protocole de chiffrement et saisissez le mot de passe dans le champ **Mot de passe**. Si vous ne souhaitez pas que la fonction de chiffrement des données soit activée, sélectionnez **Aucune** option.



Remarque: Une base d'informations de gestion (MIB) est un ensemble d'informations organisées de manière hiérarchique. Le fichier MIB (DCEALERT.MIB) pour Firepower Module est disponible à l'emplacement du répertoire (/etc/sf/DCEALERT.MIB) qui peut être récupéré à partir de cet emplacement du répertoire.

Vérification

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

Dépannage

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

Informations connexes

- Support et documentation techniques - Cisco Systems