Configurer le déchiffrement SSL sur le module FirePOWER à l'aide d'ASDM (On-Box Management)

Contenu

Introduction

Ce document décrit la configuration du déchiffrement SSL (Secure Sockets Layer) sur le module FirePOWER à l'aide d'ASDM (On-Box Management).

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)
- Connaissance de l'appliance FirePOWER
- Connaissance du protocole HTTPS/SSL

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 6.0.0 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

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.

> **Note**: Assurez-vous que FirePOWER Module dispose d'une licence **Protect** pour configurer cette fonctionnalité. Pour vérifier la licence, accédez à **Configuration > ASA FirePOWER Configuration > License**.

Informations générales

Firepower Module déchiffre et inspecte les connexions SSL entrantes et sortantes qui y sont redirigées. Une fois le trafic déchiffré, les applications tunnellisées telles que facebook chat, etc., sont détectées et contrôlées. Les données déchiffrées sont inspectées pour détecter les menaces, le filtrage des URL, le blocage des fichiers ou les données malveillantes.

Décryptage SSL sortant

Le module firepower sert de proxy de transfert pour les connexions SSL sortantes en interceptant les requêtes SSL sortantes et en régénérant un certificat pour le site que l'utilisateur souhaite visiter. L'autorité d'émission est le certificat auto-signé Firepower. Si le certificat de firepower ne fait pas partie d'une hiérarchie existante ou s'il n'est pas ajouté au cache du navigateur d'un client, le client reçoit un avertissement lorsqu'il accède à un site sécurisé. La méthode Decrypt-Resignmethod est utilisée pour effectuer le déchiffrement SSL sortant.

Décryptage SSL entrant

En cas de trafic entrant vers un serveur Web ou un périphérique interne, l'administrateur importe une copie du certificat du serveur protégé et de la clé. Lorsque le certificat du serveur SSL est chargé sur le module firepower et que la stratégie de déchiffrement SSL est configurée pour le trafic entrant, le périphérique déchiffre et inspecte le trafic lors de son transfert. Le module détecte ensuite les contenus malveillants, les menaces et les programmes malveillants circulant sur ce canal sécurisé. En outre, la méthode Decrypt-Known Keymethod est utilisée pour effectuer le déchiffrement SSL entrant.

Configuration pour le déchiffrement SSL

Il existe deux méthodes de déchiffrement du trafic SSL.

- Décrypter - Désigner pour le trafic SSL sortant
- Décryptage - Connu pour le trafic SSL entrant

Décryptage SSL sortant (décryptage - Désignation)

Le module Firepower fait office de MITM (man-in-the-Middle) pour toute négociation SSL pour les serveurs SSL publics. Il désigne le certificat du serveur public avec un certificat CA intermédiaire configuré sur le module firepower.

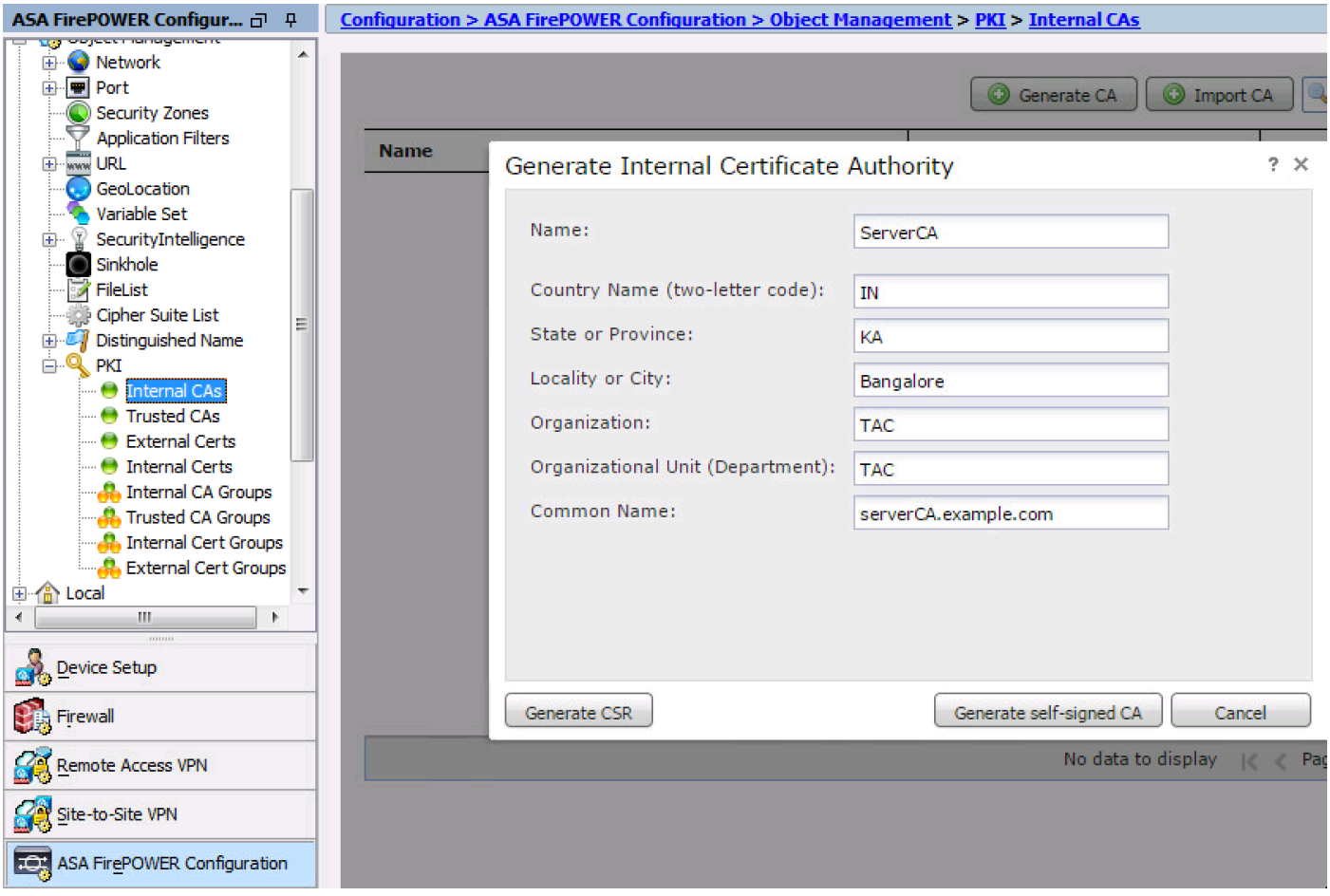
Voici les trois étapes à suivre pour configurer le déchiffrement SSL sortant.

Étape 1. Configurez le certificat CA.

Configurez un certificat auto-signé ou un certificat CA approuvé intermédiaire pour la démission du certificat.

Configurer le certificat CA auto-signé

Afin de configurer le certificat CA auto-signé, accédez à **Configuration > ASA Firepower Configuration > Object Management > PKI > Internal CAs** et cliquez sur **Generate CA**. Le système demande les détails du certificat de l'autorité de certification. Comme le montre l'image, remplissez les détails selon vos besoins.



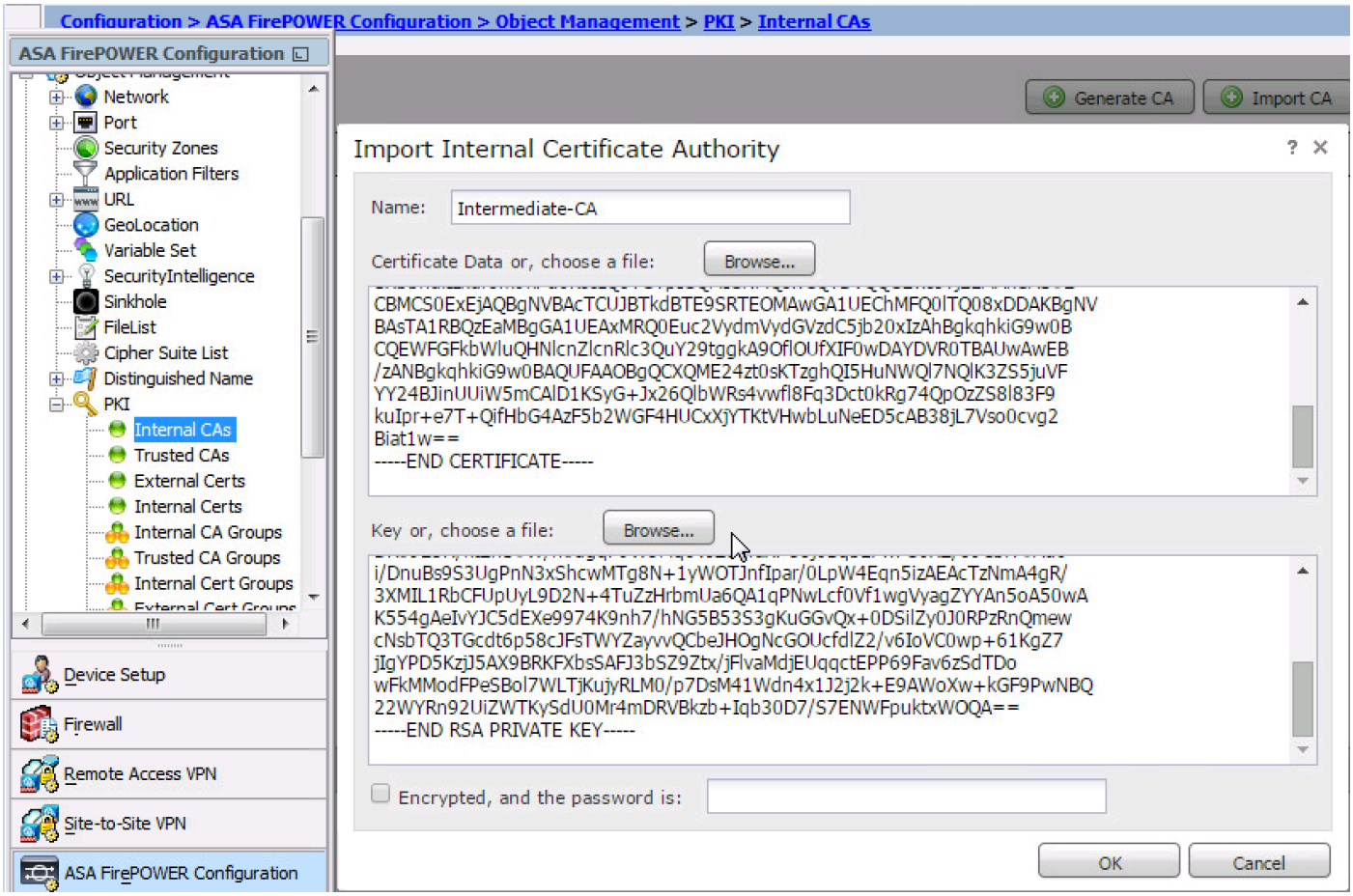
Cliquez sur **Générer une autorité de certification auto-signée** pour générer le certificat d'autorité de certification interne. Cliquez ensuite sur **Generate CSR** pour générer la demande de signature de certificat qui est par conséquent partagée avec le serveur AC à signer.

Configurer le certificat CA intermédiaire

Afin de configurer le certificat d'autorité de certification intermédiaire signé par une autre autorité de certification tierce, accédez à **Configuration > ASA Firepower Configuration > Object Management > PKI > Internal CAs** , puis cliquez sur **Import CA**.

Spécifiez le nom du certificat. Sélectionnez **Parcourir** et télécharger le certificat à partir de l'ordinateur local ou copiez-collez le contenu du certificat dans l'option **Données du certificat**. Afin de spécifier la clé privée du certificat, parcourez le fichier de clé ou copiez-collez la clé dans l'option **Clé**.

Si la clé est chiffrée, activez la case à cocher **Chiffrée** et spécifiez le mot de passe. Cliquez sur **OK** pour enregistrer le contenu du certificat, comme illustré dans l'image :



Étape 2. Configurez la stratégie SSL.

La stratégie SSL définit l'action de déchiffrement et identifie le trafic sur lequel la méthode de déchiffrement Decrypt-Resign est appliquée. Configurez les règles SSL multiples en fonction des besoins de votre entreprise et de la stratégie de sécurité de votre organisation.

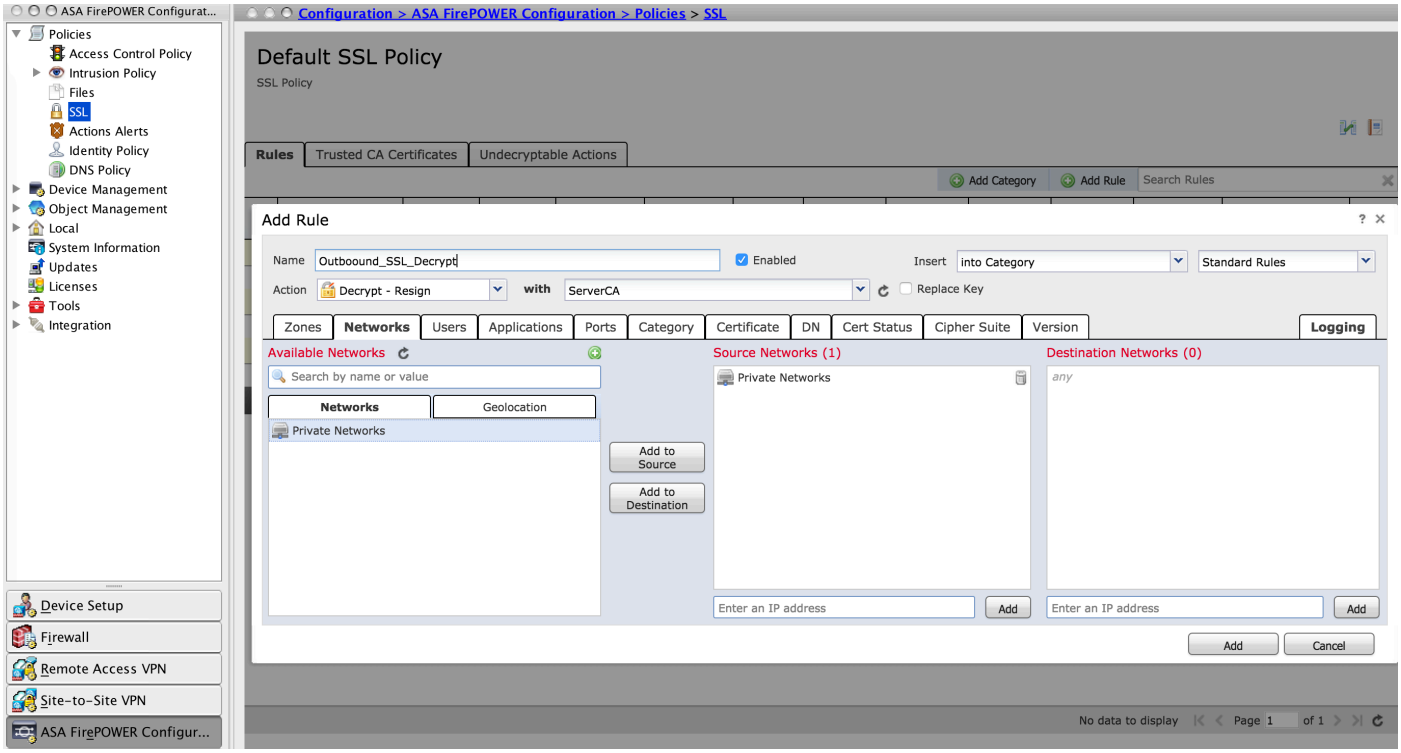
Afin de configurer la stratégie SSL, accédez à **Configure > ASA FirePOWER Configuration > Policies > SSL** et cliquez sur **Add Rule**.

Nom : spécifiez le nom de la règle.

Action : Spécifiez l'action en tant que **Décryptage - Déconnexion** et choisissez le certificat de l'autorité de certification dans la liste déroulante qui est configurée à l'étape précédente.

Définissez des conditions dans la règle pour correspondre au trafic car il existe plusieurs options (zone, réseau, utilisateurs, etc.), spécifiées pour définir le trafic qui doit être déchiffré.

Pour générer les événements du déchiffrement SSL, activez l'option de **journalisation** loggingat, comme indiqué dans l'image :



Cliquez sur **Add** pour ajouter la règle SSL.

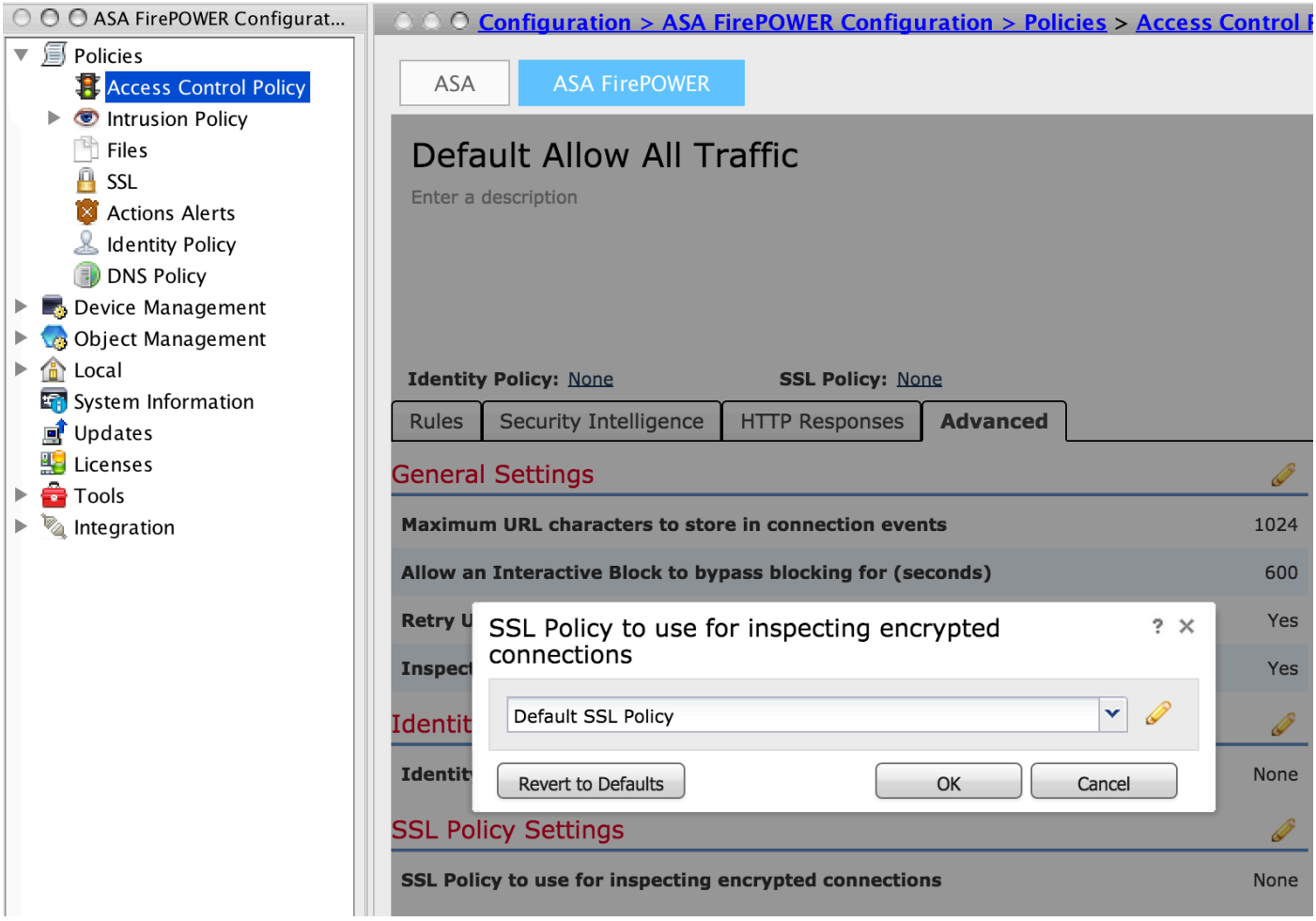
Cliquez sur **Store ASA Firepower Changes** pour enregistrer la configuration de la stratégie SSL.

Étape 3. Configurer la stratégie de contrôle d'accès

Une fois que vous avez configuré la stratégie SSL avec les règles appropriées, vous devez spécifier la stratégie SSL dans le contrôle d'accès pour implémenter les modifications.

Pour configurer la stratégie de contrôle d'accès, accédez à **Configuration > ASA Firepower Configuation > Policies > Access Control.**

Cliquez sur **Aucun** de la **stratégie SSL** ou accédez à **Advanced > SSL Policy Setting.** Spécifiez la stratégie SSL dans la liste déroulante et cliquez sur **OK** pour l'enregistrer, comme indiqué dans l'image :



Cliquez sur **Modifications apportées au pare-feu ASA du magasin** pour enregistrer la configuration de la stratégie SSL.

Vous devez déployer la stratégie de contrôle d'accès sur le capteur. Avant d'appliquer la stratégie, il est indiqué que la **stratégie de contrôle d'accès est obsolète** sur le module. Pour déployer les modifications apportées au capteur, cliquez sur **Déployer** et sélectionnez **l'option Déployer les modifications FirePOWER.** Vérifiez les modifications apportées et cliquez sur **Déployer.**

> **Note**: Dans la version 5.4.x, si vous devez appliquer la stratégie d'accès au capteur, cliquez sur **Apply ASA FirePOWER Changes.**

> **Note**: Accédez à **Monitoring > ASA Firepower Monitoring > Task Status.** Vous pouvez ensuite demander des modifications de configuration pour vous assurer que la tâche est terminée.

Décryptage SSL entrant (décryptage - connu)

La méthode de déchiffrement SSL entrant (Decrypt-Known) est utilisée pour déchiffrer le trafic SSL entrant pour lequel vous avez configuré le certificat de serveur et la clé privée. Vous devez importer le certificat de serveur et la clé privée dans le module Firepower. Lorsque le trafic SSL atteint le module Firepower, il déchiffre le trafic et effectue l'inspection sur le trafic décrypté. Après inspection, le module Firepower chiffre à nouveau le trafic et l'envoie au serveur.

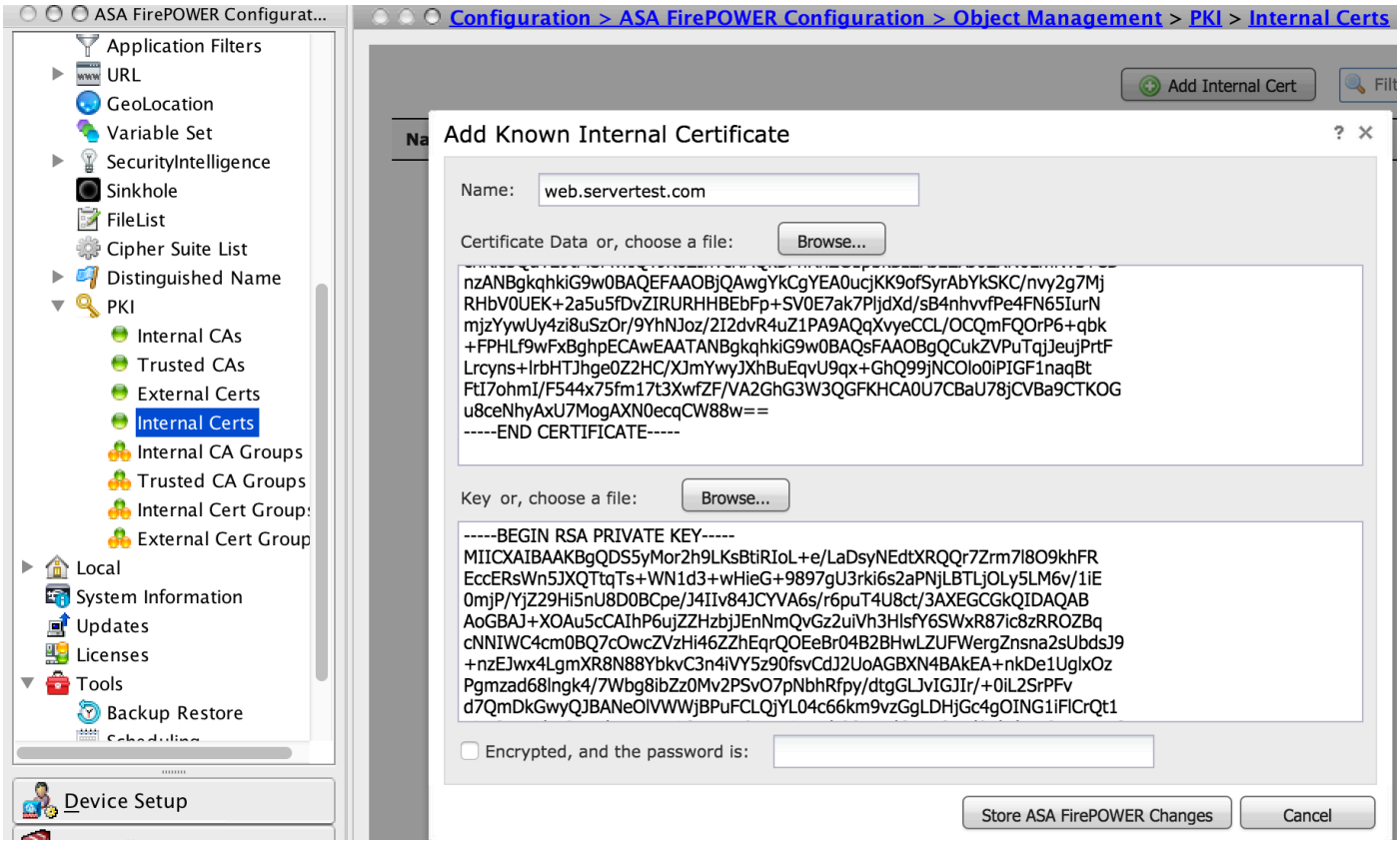
Voici les quatre étapes à suivre pour configurer le déchiffrement SSL sortant :

Étape 1. Importez le certificat et la clé du serveur.

Afin d'importer le certificat et la clé du serveur, accédez à **Configuration > ASA Firepower Configuration > Object Management > PKI > Internal Certs** et cliquez sur **Add Internal Cert**.

Comme l'illustre l'image, spécifiez le nom du certificat. Sélectionnez **Parcourir** pour sélectionner le certificat à partir de l'ordinateur local ou copiez-collez le contenu du certificat dans les **données du certificat**. Afin de spécifier la clé privée du certificat, parcourez le fichier de clé ou copiez-collez la clé dans l'option **Key**.

Si la clé est chiffrée, activez la case à cocher **Chiffrée** et spécifiez le mot de passe, comme indiqué dans l'image :



Cliquez sur **Store ASA FirePOWER Changes** pour enregistrer le contenu du certificat.

Étape 2. Importer le certificat CA (facultatif).

Pour le certificat de serveur signé par un certificat d'autorité de certification interne intermédiaire ou racine, vous devez importer la chaîne interne de certificats d'autorité de certification dans le module firepower. Une fois l'importation effectuée, le module firepower peut valider le certificat du serveur.

Pour importer le certificat d'autorité de certification, accédez à **Configuration > ASA Firepower Configuration > Object Management > Trusted CAs** et cliquez sur **Add Trusted CA** pour ajouter le certificat d'autorité de certification.

Étape 3. Configurez la stratégie SSL.

La stratégie SSL définit l'action et les détails du serveur pour lesquels vous souhaitez configurer la méthode connue de déchiffrement pour déchiffrer le trafic entrant. Si vous avez plusieurs serveurs internes, configurez plusieurs règles SSL basées sur différents serveurs et le trafic qu'ils gèrent .

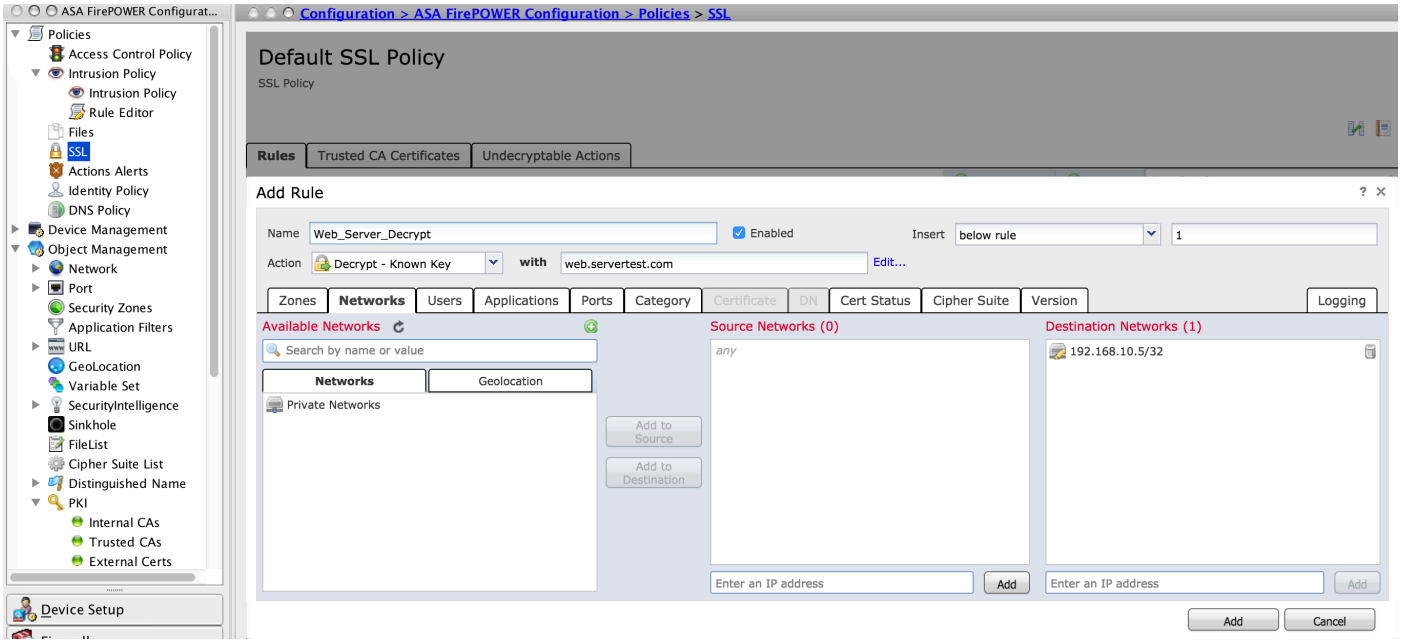
Pour configurer la stratégie SSL, accédez à **Configure > ASA FirePOWER Configuration > Policies > SSL** et cliquez sur **Add Rule**.

Nom : spécifiez le nom de la règle.

Action : Spécifiez l'action comme **Décryptage - connu** et choisissez le certificat de l'autorité de certification dans la liste déroulante qui est configurée à l'étape précédente.

Définissez la condition pour correspondre à ces règles, car plusieurs options (réseau, application, ports, etc.) sont spécifiées pour définir le trafic intéressant du serveur pour lequel vous voulez activer le déchiffrement SSL. Spécifiez l'autorité de certification interne dans **les autorités de certification approuvées sélectionnées dans l'**onglet **Certificat d'autorité de certification approuvée.**

Pour générer les événements de déchiffrement SSL, activez l'option de **journalisation** loggingat.



Cliquez sur **Add** pour ajouter la règle SSL.

Puis cliquez sur **Store ASA Firepower Changes** pour enregistrer la configuration de la stratégie SSL.

Étape 4. Configurez la stratégie de contrôle d'accès.

Une fois que vous avez configuré la stratégie SSL avec les règles appropriées, vous devez spécifier la stratégie SSL dans le contrôle d'accès pour implémenter les modifications.

Pour configurer la stratégie de contrôle d'accès, accédez à **Configuration > ASA Firepower Configuation > Policies > Access Control.**

Cliquez sur l'option **Aucun** en regard de **Stratégie SSL** ou accédez à **Advanced > SSL Policy Setting**, spécifiez la stratégie SSL dans la liste déroulante et cliquez sur **OK** pour l'enregistrer.

Cliquez sur **Modifications apportées au pare-feu ASA du magasin** pour enregistrer la configuration de la stratégie SSL.

Vous devez déployer la stratégie de contrôle d'accès. Avant d'appliquer la stratégie, vous pouvez voir une indication Politique de contrôle d'accès obsolète sur le module. Pour déployer les modifications apportées au capteur, cliquez sur **Déployer** et choisissez **l'option Déployer les modifications FirePOWER.** Vérifiez les modifications apportées et cliquez sur **Déployer** dans la fenêtre contextuelle.

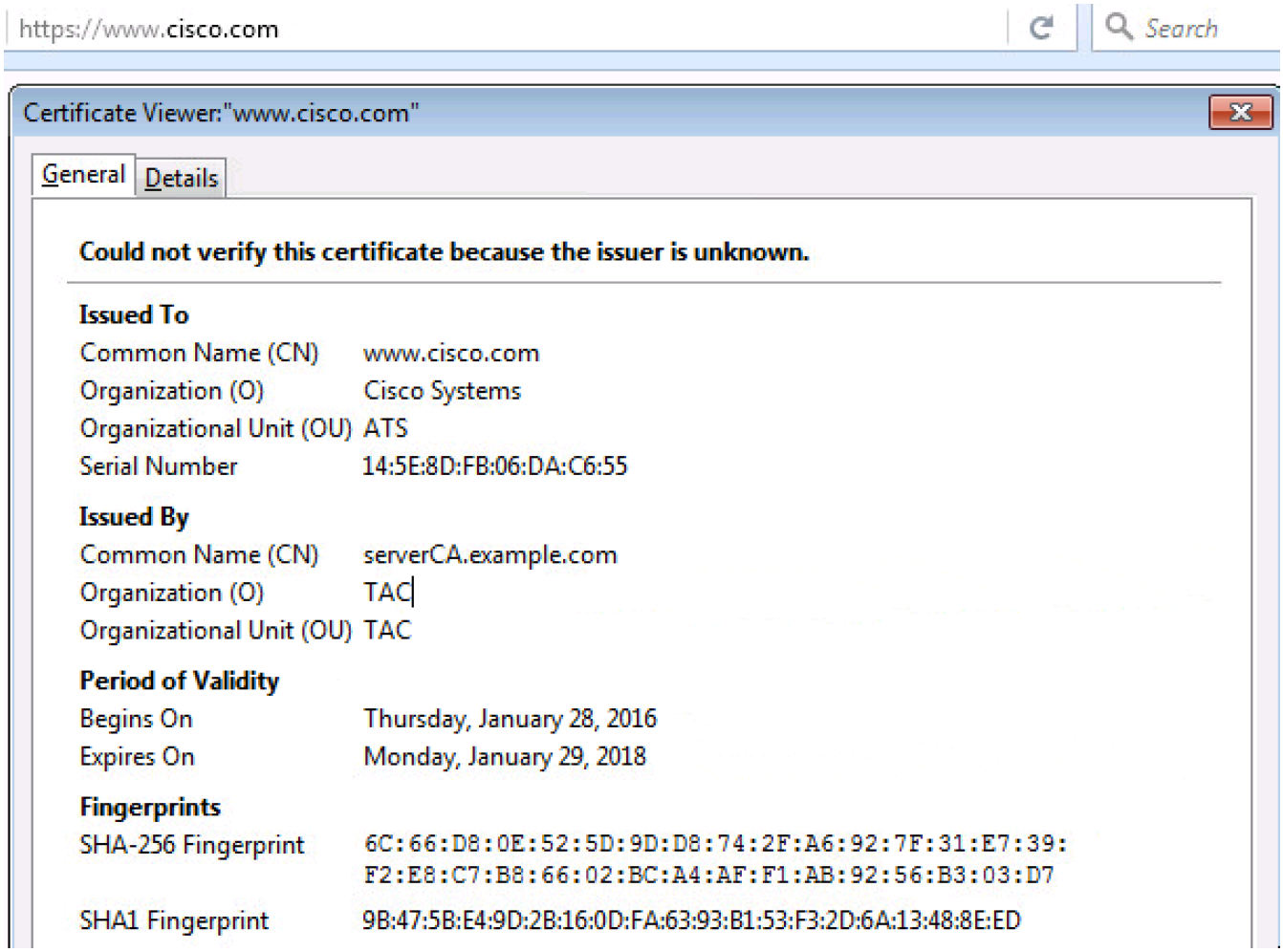
> **Note**: Dans la version 5.4.x, si vous devez appliquer la stratégie d'accès au capteur, cliquez sur **Apply ASA FirePOWER Changes**.

> **Note**: Accédez à **Monitoring > ASA Firepower Monitoring > Task Status.** Vous pouvez ensuite demander des modifications de configuration pour vous assurer que la tâche est terminée.

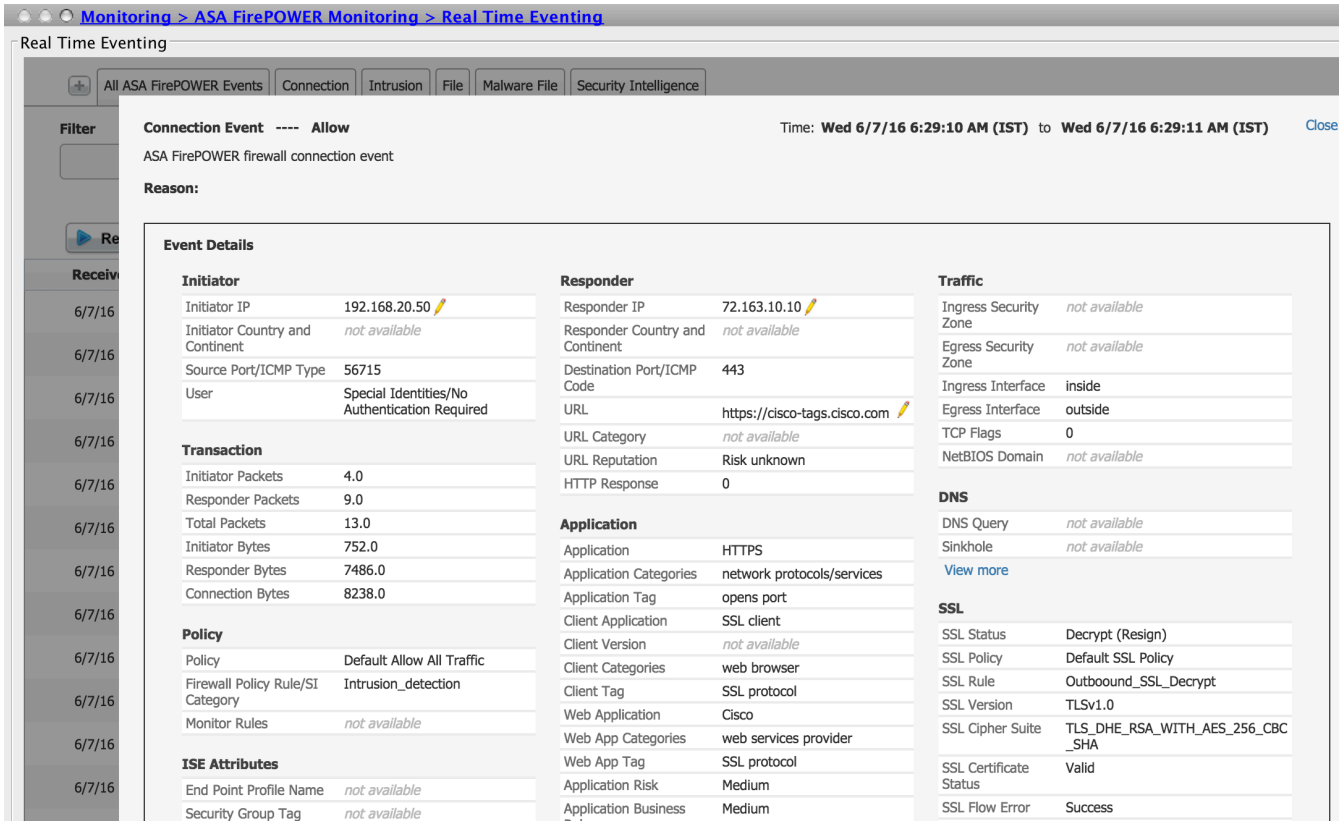
Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

- Pour la connexion SSL sortante, une fois que vous avez parcouru un site Web SSL public à partir du réseau interne, le système affiche un message d'erreur du certificat. Vérifiez le contenu du certificat et vérifiez les informations de l'autorité de certification. Le certificat CA interne que vous avez configuré dans le module Firepower apparaît. Acceptez le message d'erreur pour parcourir le certificat SSL. Pour éviter le message d'erreur, ajoutez le certificat d'autorité de certification dans la liste des autorités de certification de confiance de votre navigateur.



- Vérifiez les événements de connexion pour vérifier quelle stratégie SSL et quelle règle SSL sont affectées par le trafic. Naviguez jusqu'à **Monitoring > ASA FirePOWER Monitoring > Real-Time Evant.**Sélectionnez un événement et cliquez sur **View Details**. Vérifiez les statistiques de déchiffrement SSL.



- Assurez-vous que le déploiement de la stratégie de contrôle d'accès s'est terminé correctement.
- Assurez-vous que la stratégie SSL est incluse dans la stratégie de contrôle d'accès.
- Assurez-vous que la stratégie SSL contient les règles appropriées pour la direction entrante et sortante.
- Assurez-vous que les règles SSL contiennent la condition appropriée pour définir le trafic intéressant.
- Surveillez les événements de connexion pour vérifier la stratégie SSL et la règle SSL.
- Vérifiez l'état du déchiffrement SSL.

Dépannage

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

Informations connexes

- Support et documentation techniques - Cisco Systems