Configuration d'une stratégie d'inspection SSL sur le système Cisco FireSIGHT

Contenu

Introduction

La fonction d'inspection SSL vous permet soit de bloquer le trafic chiffré sans l'inspecter, soit d'inspecter le trafic chiffré ou décrypté avec un contrôle d'accès. Ce document décrit les étapes de configuration pour configurer une stratégie d'inspection SSL sur Cisco FireSIGHT System.

Conditions préalables

Components Used

- Cisco FireSIGHT Management Center
- Appareils Cisco Firepower 7000 ou 8000
- Version 5.4.1 ou ultérieure du logiciel

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.

Avertissement : Si vous appliquez une stratégie d'inspection SSL sur votre périphérique

géré, elle peut affecter les performances du réseau.

Configurations

Vous pouvez configurer une stratégie d'inspection SSL pour déchiffrer le trafic de la manière suivante :

1. Décryptage et démission :

- Option 1 : Utilisez FireSIGHT Center en tant qu'autorité de certification racine, ou
- Option 2 : Demandez à une autorité de certification interne de signer votre certificat, ou
- Option 3 : Importer un certificat et une clé CA

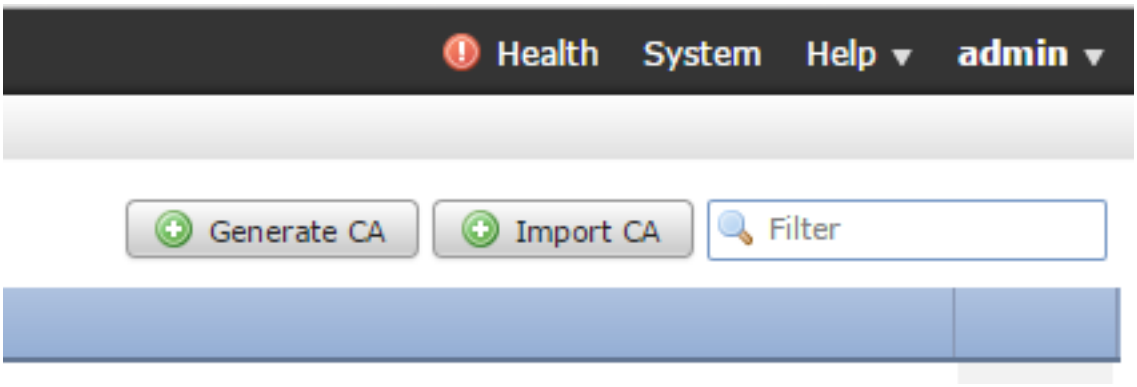
2. Décrypter avec le certificat connu :

- Connectez-vous à FireSIGHT Management Center, puis accédez à **Objets**.
- Sur la page **Objets**, développez l'**ICP** et sélectionnez **AC internes**.

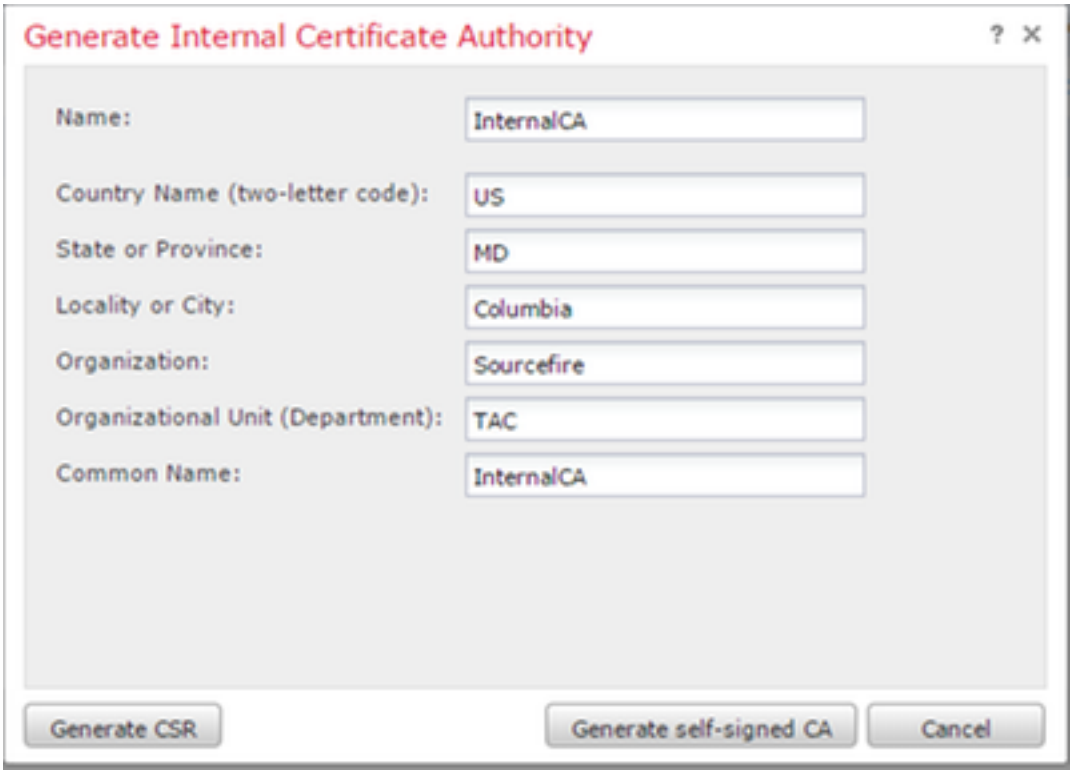
1. Décryptage et démission

Option 1 : Utiliser FireSIGHT Center en tant qu'autorité de certification racine

i. Cliquez sur **Generate CA**.



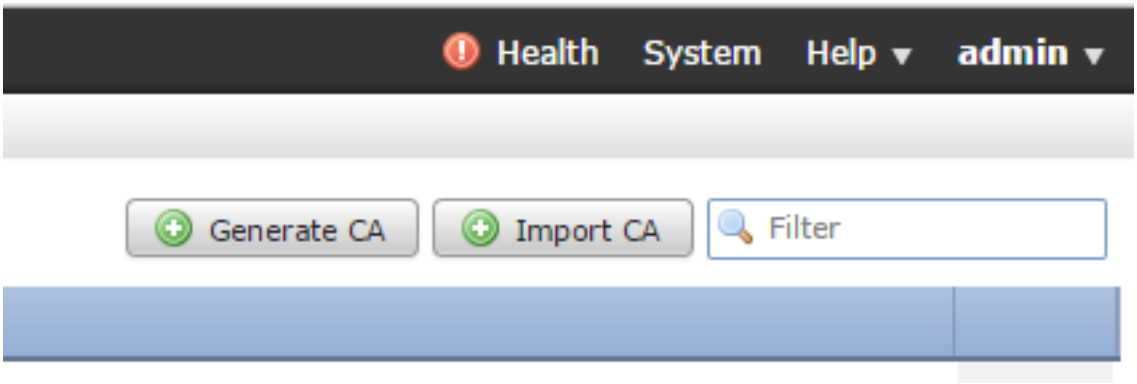
ii. Complétez les informations pertinentes



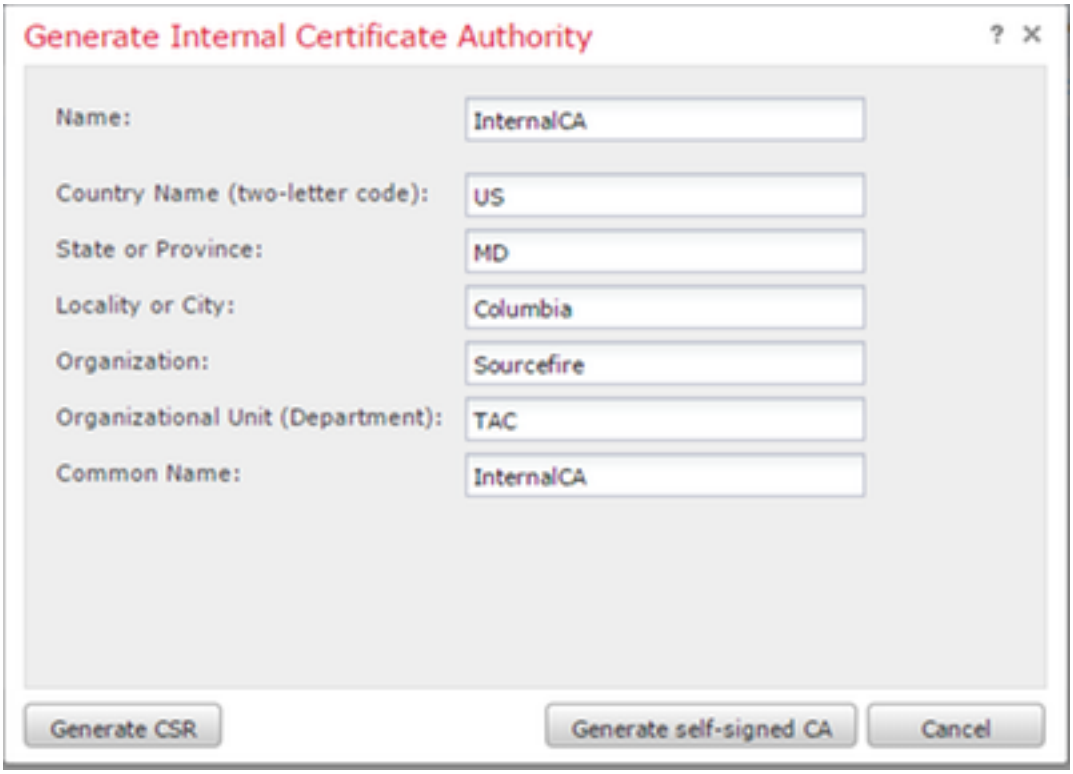
iii. Cliquez sur **Générer une autorité de certification auto-signée**.

Option 2 : Faire signer votre certificat par une autorité de certification interne

i. Cliquez sur **Generate CA**.

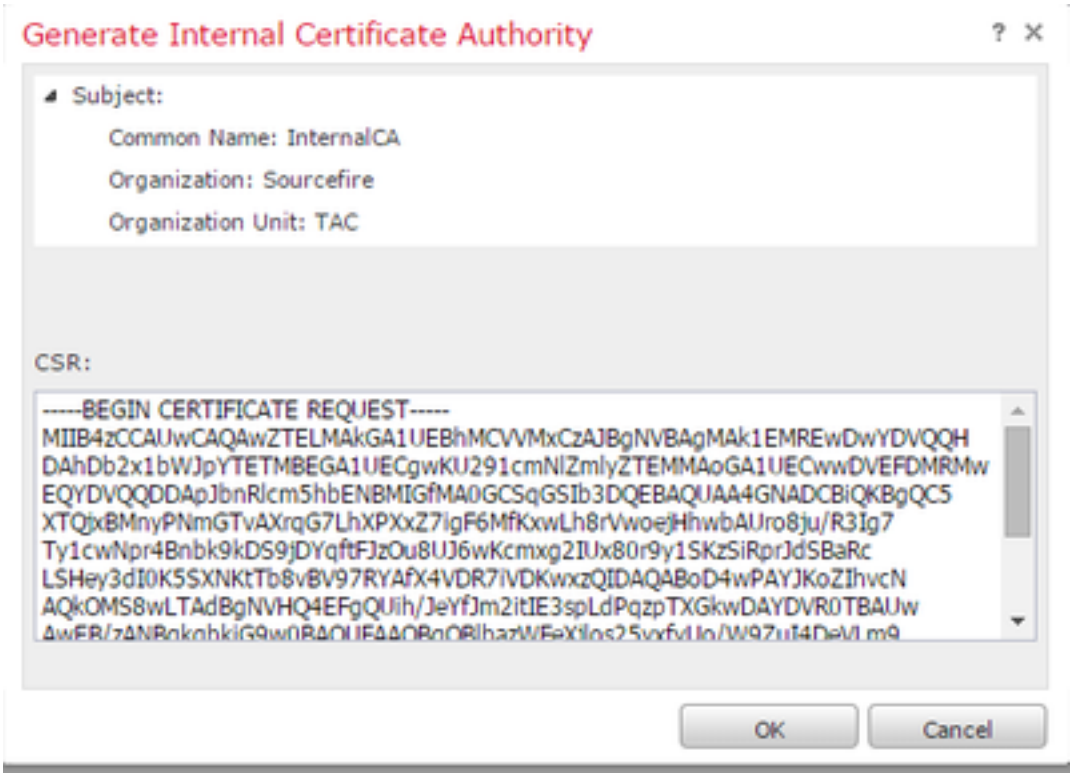


ii. Complétez les informations pertinentes.



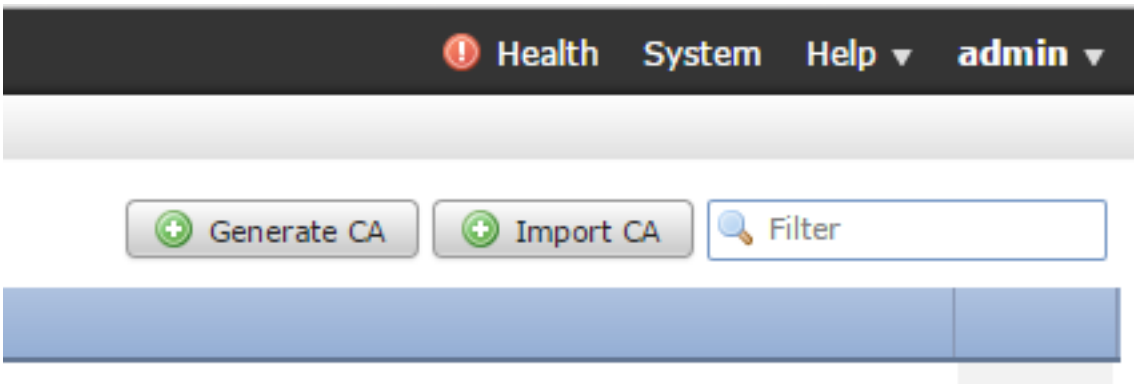
Note: Vous devrez peut-être contacter votre administrateur AC pour déterminer s'il dispose d'un modèle pour la demande de signature.

iii. Copiez l'intégralité du certificat, y compris la — DEMANDE DE CERTIFICAT DE DÉBUT— et —DEMANDE DE CERTIFICAT DE FIN— puis enregistrez-la dans un fichier texte avec l'extension .req.



Note: Votre administrateur AC demande une autre extension de fichier en plus de .req.

Option 3 : Importer un certificat et une clé CA

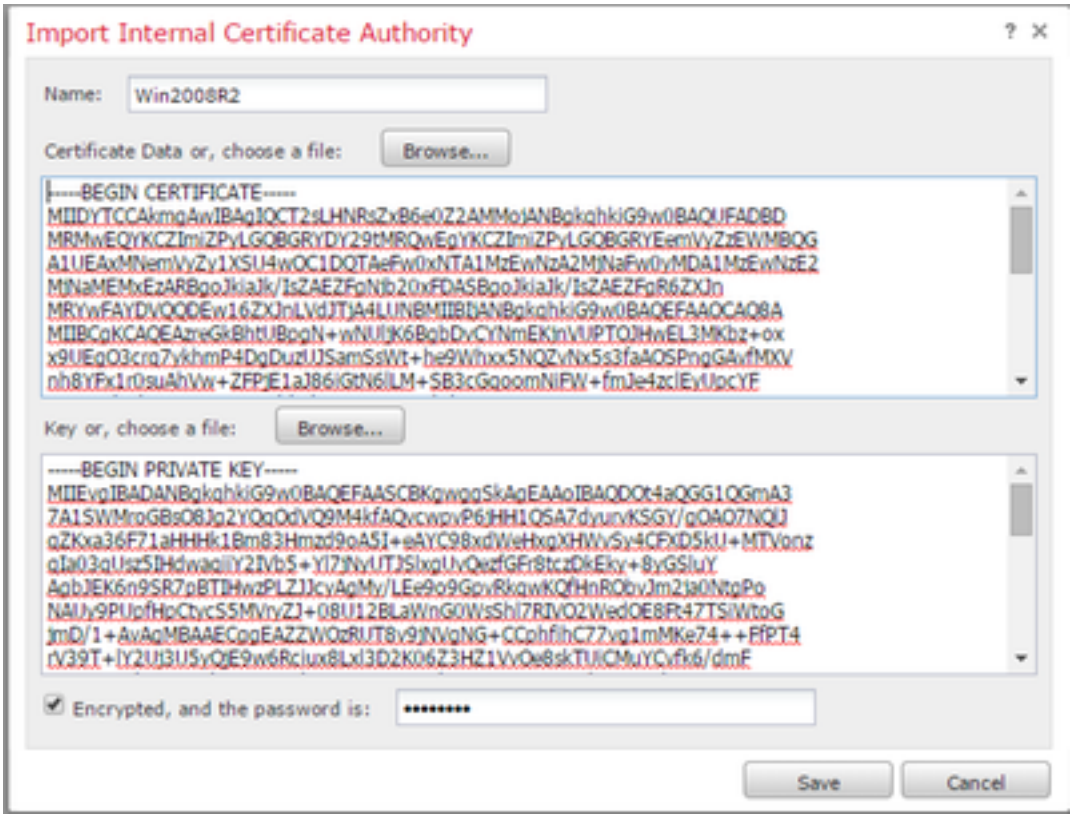


i. Cliquez sur **Importer une autorité de certification**.

ii. Accédez au certificat ou collez-le.

iii. Accédez à ou collez dans la clé privée.

iv. Cochez la case chiffrée et saisissez un mot de passe.



Note: S'il n'y a pas de mot de passe, cochez la case chiffrée et laissez-la vide.

2. Décrypter avec la clé connue

Importation d'un certificat connu (alternative au déchiffrement et au décodage)

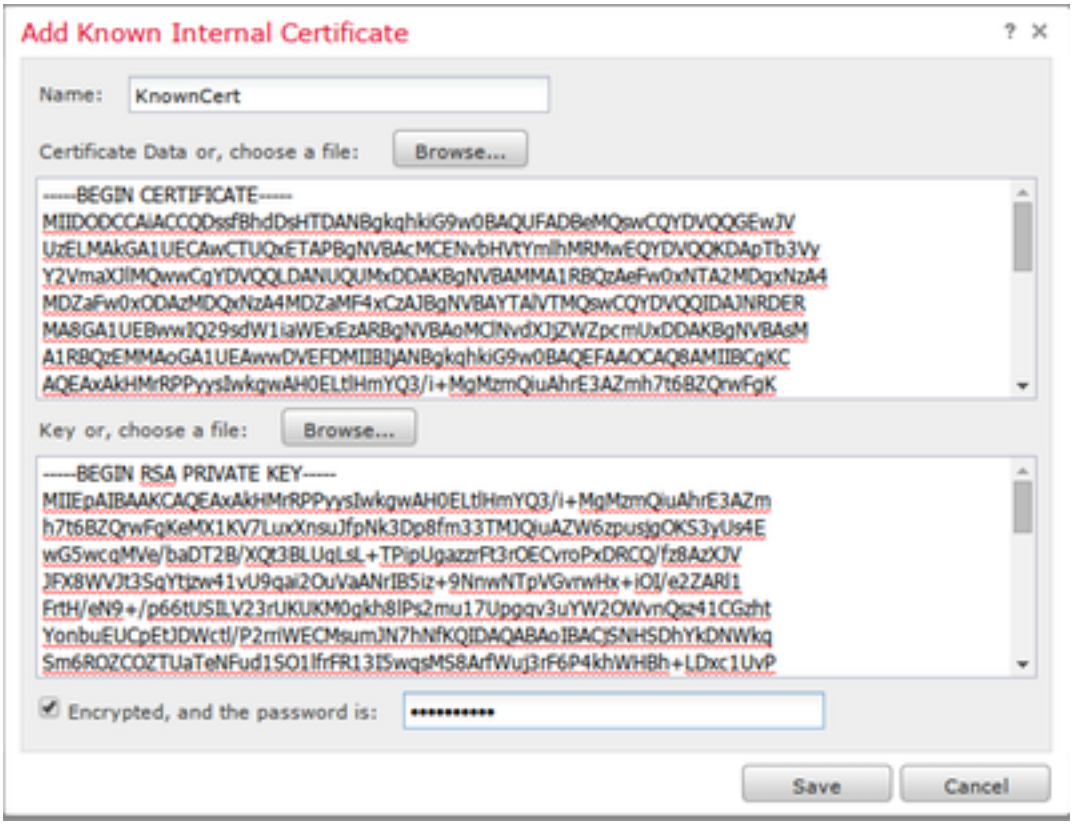
i. Dans la page Objets à gauche, développez PKI et sélectionnez Certs internes.

ii. Cliquez sur **Ajouter un certificat interne**.

iii. Accédez au certificat ou collez-le.

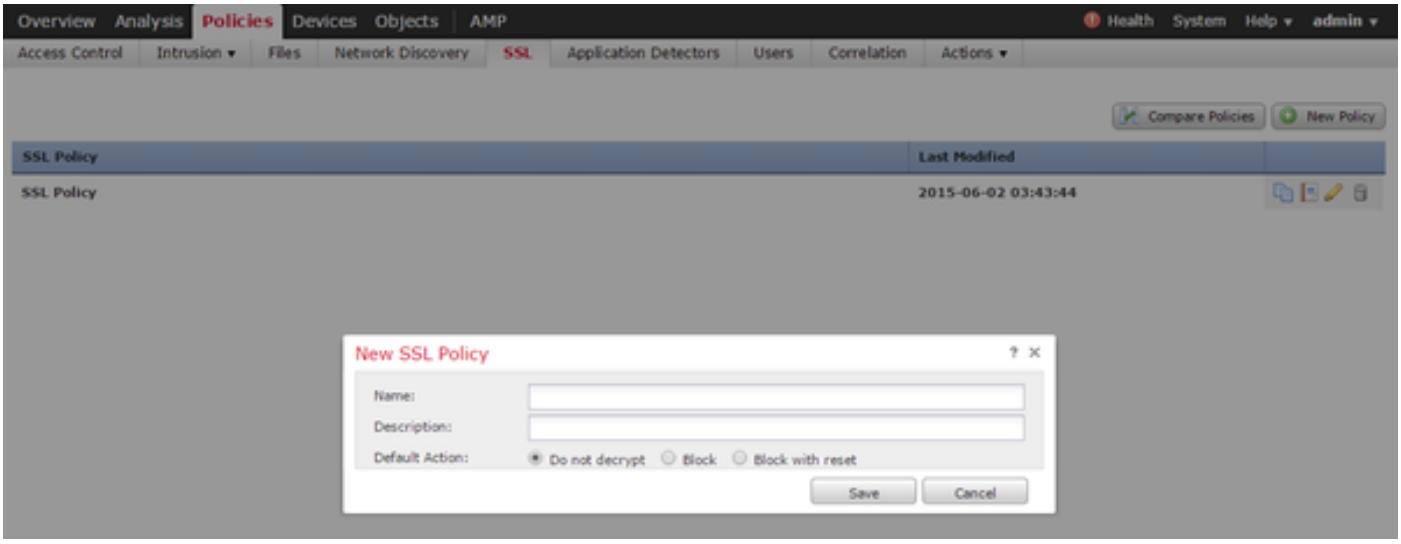
iv. Accédez à ou collez dans la clé privée.

v. Cochez la case **Chiffrée** et saisissez un mot de passe.



Note: S'il n'y a pas de mot de passe, laissez la zone **Chiffrée** vide.

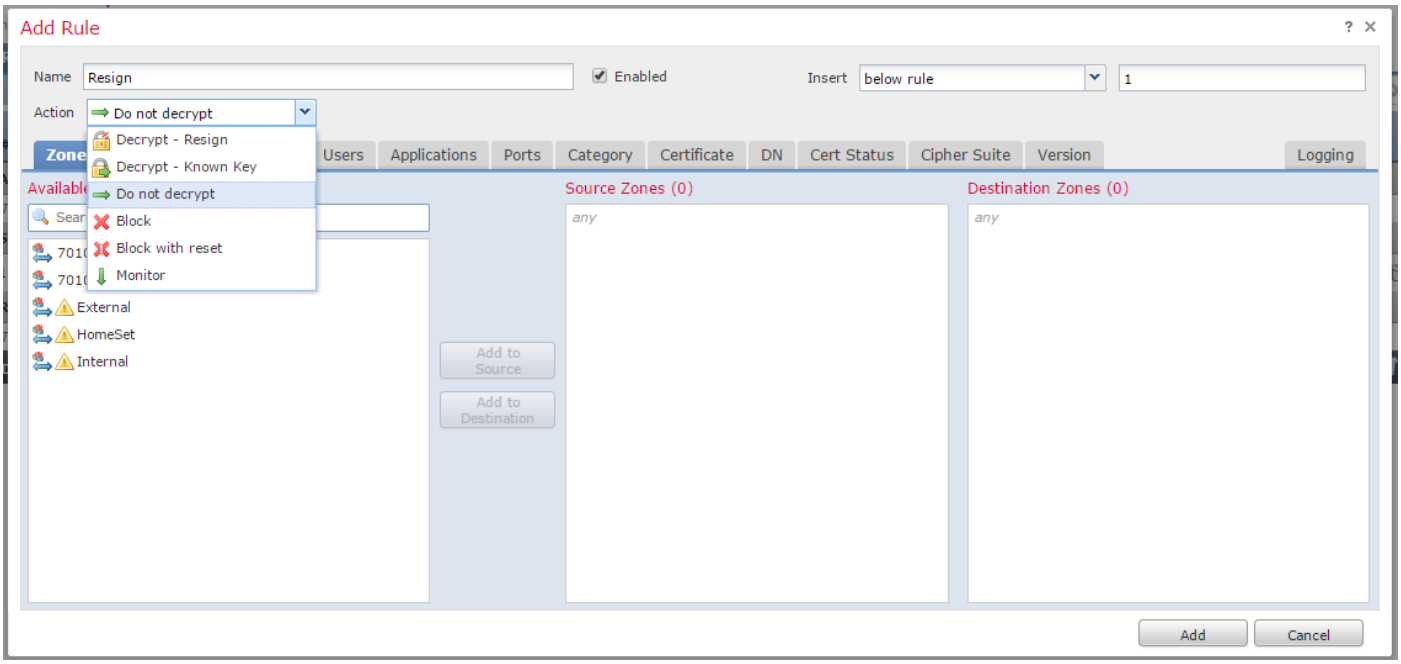
4. Accédez à **Stratégies > SSL**, puis cliquez sur **Nouvelle stratégie**.



5. Indiquez un nom et sélectionnez une **action par défaut**. La page Éditeur de stratégie SSL s'affiche. La page Éditeur de stratégie SSL fonctionne de la même manière que la page Éditeur de stratégie de contrôle d'accès.

> **Note:** Si vous n'êtes pas sûr de l'**action par défaut**, **Ne pas déchiffrer** est le point de départ recommandé.

6. Sur la page de l'éditeur de stratégie SSL, cliquez sur **Ajouter une règle**. Dans la fenêtre Ajouter une règle, indiquez un nom pour la règle et renseignez toutes les autres informations pertinentes.



La section suivante décrit différentes options de la fenêtre **Ajouter une règle** :

Action

Décrypter - Désigner

- Le capteur agit en tant qu'homme au milieu (MitM) et accepte la connexion avec l'utilisateur, puis établit une nouvelle connexion au serveur. Exemple : Les types d'utilisateur dans https://www.facebook.com dans un navigateur. Le trafic atteint le capteur, le capteur négocie ensuite avec l'utilisateur à l'aide du certificat CA sélectionné et le tunnel SSL A est créé. En même temps, le capteur se connecte à https://www.facebook.com et crée le tunnel SSL B.

- Résultat final : L'utilisateur voit le certificat dans la règle, pas sur facebook.
- Cette action nécessite une autorité de certification interne. Sélectionnez Remplacer la clé si vous souhaitez la remplacer. L'utilisateur recevra le certificat que vous sélectionnez.

  Note: Il ne peut pas être utilisé en mode passif.

Décrypter - Clé connue

- Le capteur possède la clé qui sera utilisée pour déchiffrer le trafic. Exemple : Les types d'utilisateur dans https://www.facebook.com dans un navigateur. Le trafic atteint le capteur, le capteur déchiffre le trafic, puis inspecte le trafic.
- Résultat final : L'utilisateur peut voir le certificat de facebook
- Cette action nécessite un certificat interne. Ceci est ajouté dans **Objets >PKI > Certs internes**.

  Note: Votre organisation doit être propriétaire du domaine et du certificat. Pour l'exemple de facebook.com, la seule façon possible pour l'utilisateur final de voir le certificat de facebook serait si vous possédez réellement le domaine facebook.com (c'est-à-dire que votre société est Facebook, Inc) et que vous possédez le certificat facebook.com signé par une autorité de certification publique. Vous ne pouvez décrypter qu'avec les clés connues des sites appartenant à votre organisation.

Le but principal du déchiffrement de la clé connue est de déchiffrer le trafic en direction de votre serveur https afin de protéger vos serveurs contre les attaques externes. Pour inspecter le trafic côté client vers des sites https externes, vous utiliserez le déchiffrement de la déconnexion car vous ne possédez pas le serveur et vous êtes intéressé par l'inspection du trafic client de votre réseau se connectant à des sites chiffrés externes.

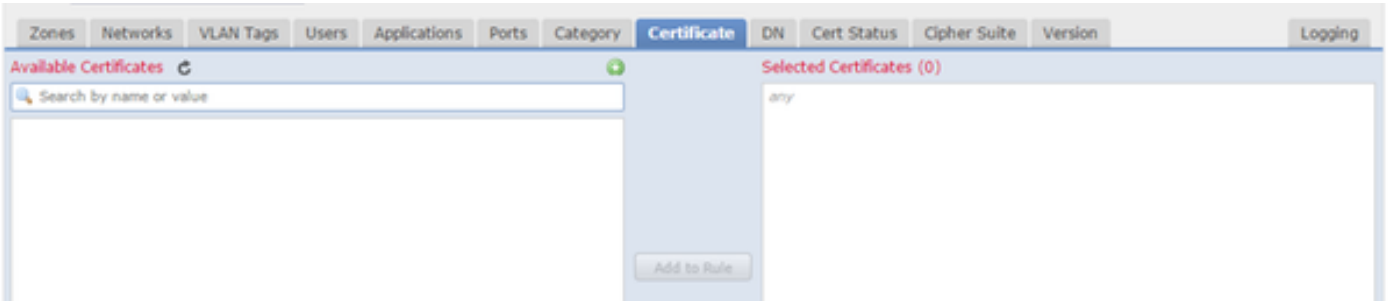
Note: Pour que DHE et ECDHE décryptent, nous devons être en ligne.

Ne pas déchiffrer

Le trafic contourne la stratégie SSL et continue à la stratégie de contrôle d'accès.

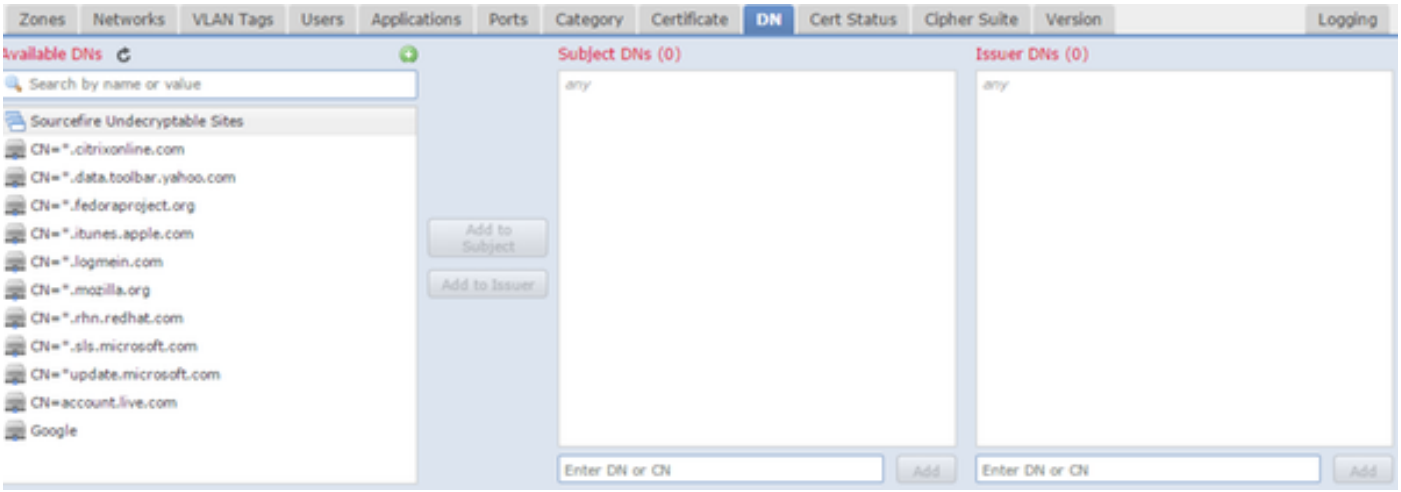
Certificat

La règle correspond au trafic SSL à l'aide de ce certificat particulier.



DN

La règle correspond au trafic SSL à l'aide de certains noms de domaine dans les certificats.

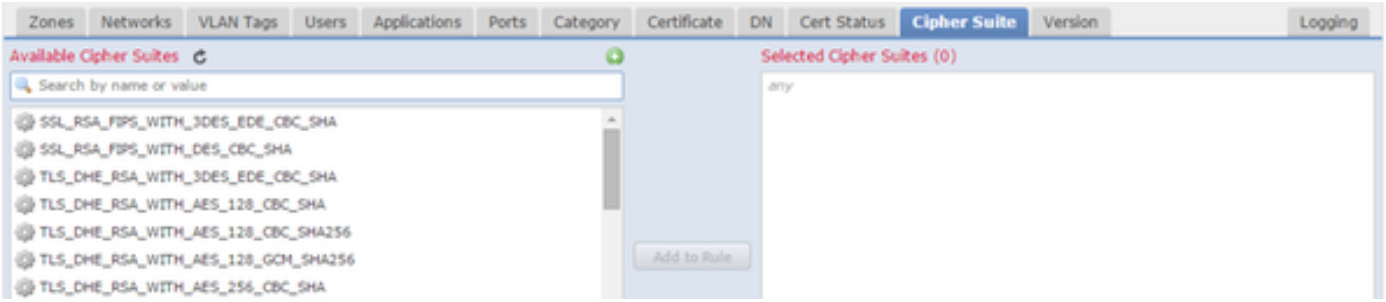


État du certificat

La règle correspond au trafic SSL avec ces états de certificat.

Suite Cipher

La règle correspond au trafic SSL à l'aide de ces suites de chiffrement.



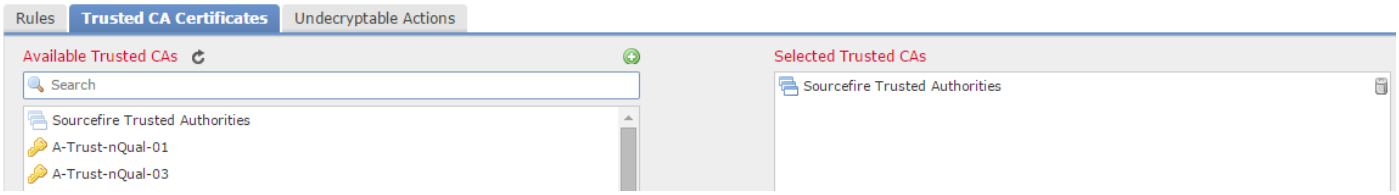
Version

Les règles s'appliquent uniquement au trafic SSL avec les versions sélectionnées de SSL.

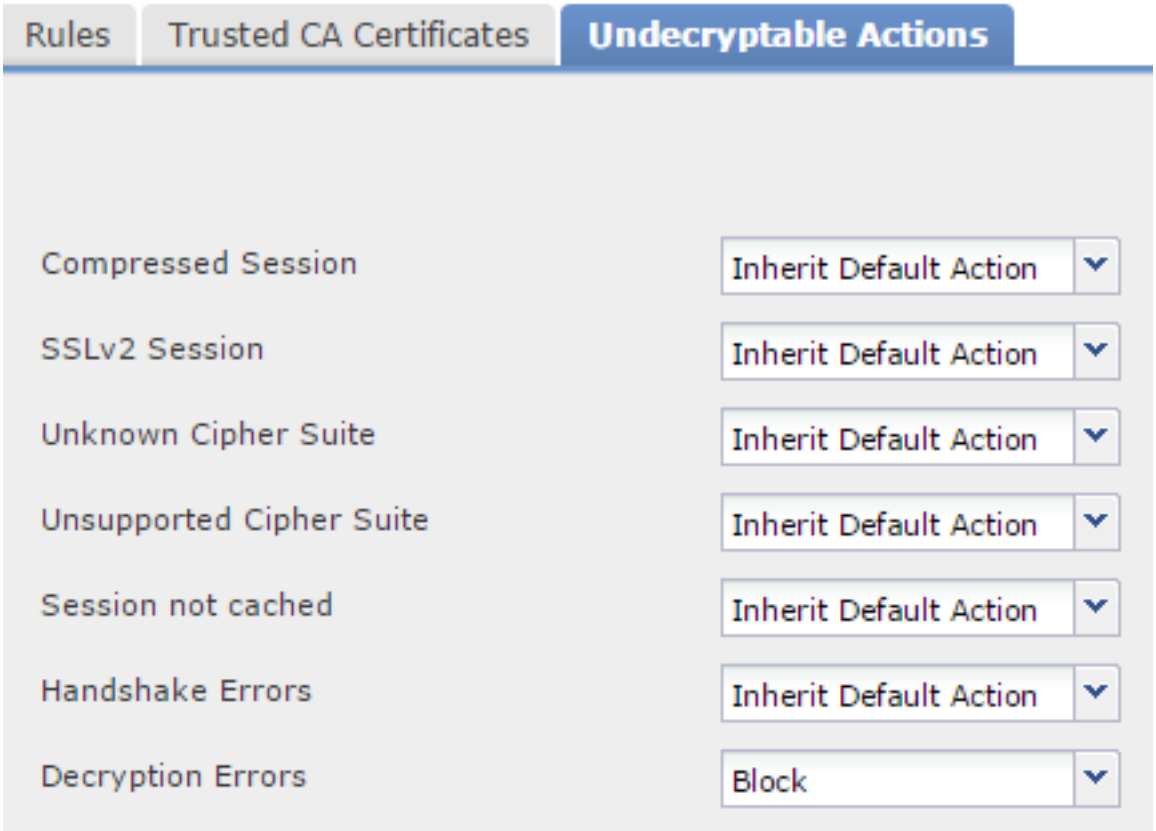
Journalisation

Activez la journalisation pour voir les événements de connexion pour le trafic SSL.

7. Cliquez sur **Certificat CA approuvé**. C'est à cet endroit que l'autorité de certification de confiance est ajoutée à la stratégie.



8. Cliquez sur **Actions non déchiffrables**. Voici les actions pour lesquelles le capteur ne peut pas déchiffrer le trafic. Vous pouvez trouver les définitions dans l'aide en ligne (**Aide > En ligne**) de FireSIGHT Management Center.



- **Session compressée** : La session SSL applique une méthode de compression de données.
- **Session SSLv2** : La session est chiffrée avec SSL version 2. Notez que le trafic est déchiffrable si le message Hello du client est SSL 2.0 et que le reste du trafic transmis est SSL 3.0.

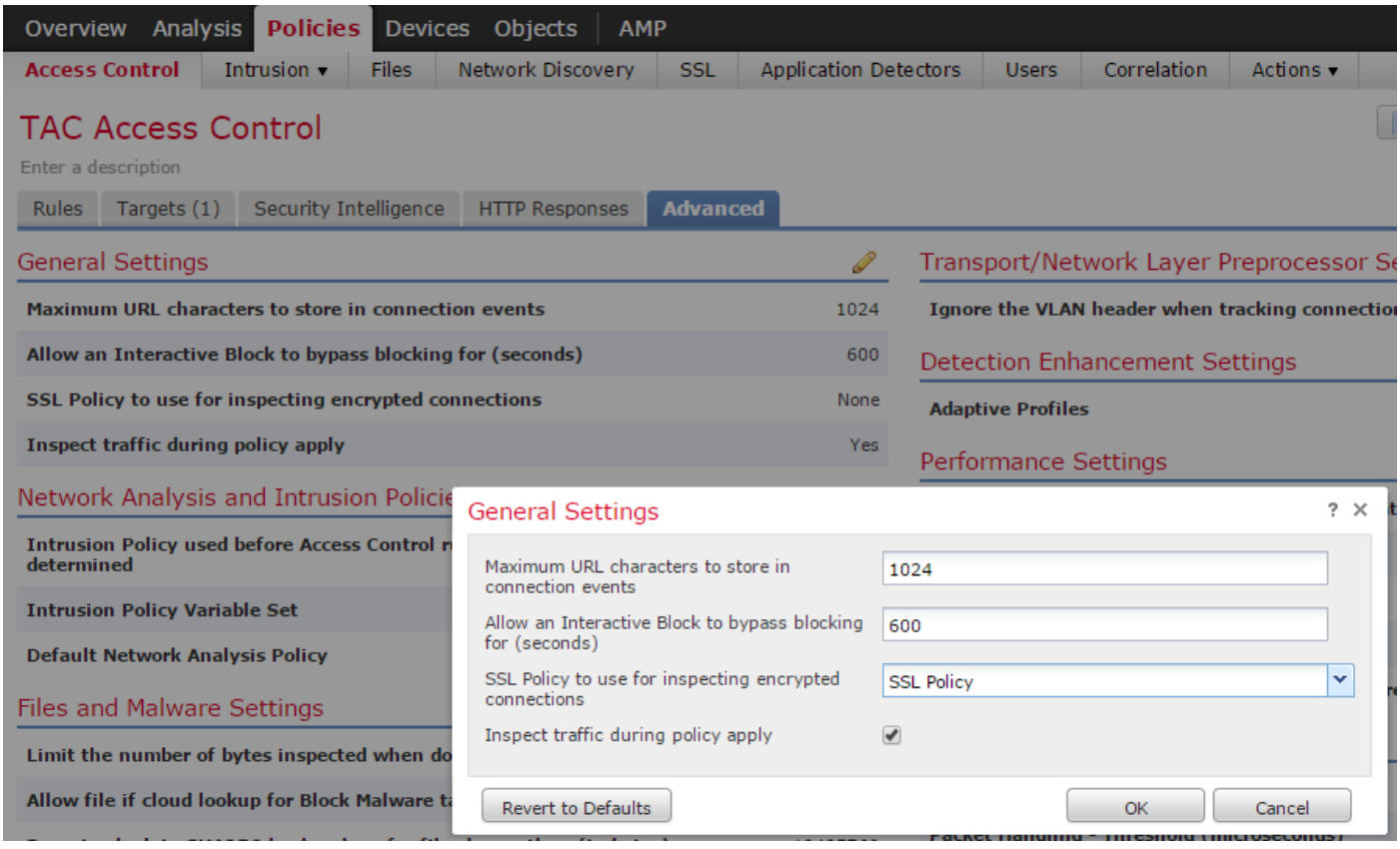
- **Suite de chiffrement inconnue** : Le système ne reconnaît pas la suite de chiffrement.
- **Suite Cipher non prise en charge** : Le système ne prend pas en charge le déchiffrement en fonction de la suite de chiffrement détectée.
- **Session non mise en cache** : La réutilisation de la session SSL est activée, le client et le serveur ont rétabli la session avec l'identificateur de session et le système n'a pas mis cet identificateur en cache.
- **Erreurs de connexion** : Une erreur s'est produite lors de la négociation de la connexion SSL.
- **Erreurs de déchiffrement** : Une erreur s'est produite lors du déchiffrement du trafic.

Note: Par défaut, ils héritent de l'action par défaut. Si votre action par défaut est Bloquer, vous risquez de rencontrer des problèmes inattendus

9. Enregistrez la stratégie.

10. Accédez à **Stratégies > Contrôle d'accès**. Modifiez votre stratégie ou créez une nouvelle stratégie de contrôle d'accès.

11. Cliquez sur **Avancé** et modifiez les **paramètres généraux**.



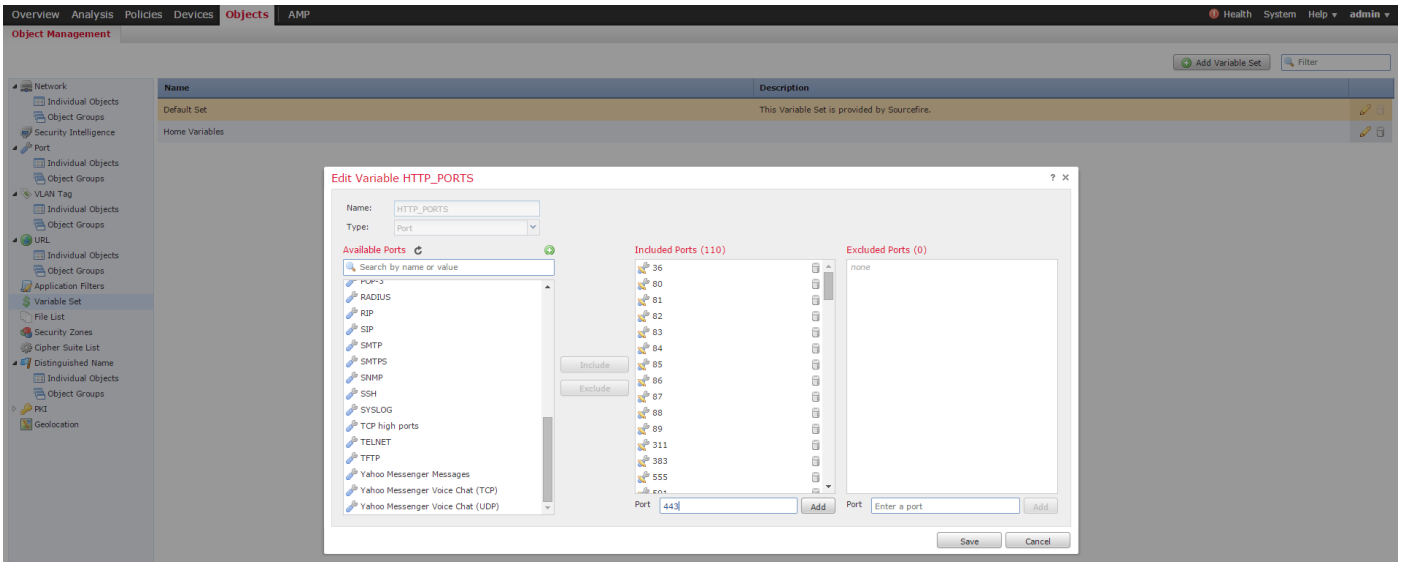
12. Dans le menu déroulant, sélectionnez votre **stratégie SSL**.

13. Cliquez sur **OK** pour enregistrer.

Configurations supplémentaires

Les modifications suivantes doivent être apportées aux stratégies d'intrusion pour une identification correcte :

i. Votre variable $HTTP_PORTS doit inclure le port 443 et tout autre port avec le trafic https qui sera déchiffré par votre stratégie (**Objets > Gestion des objets > Jeu de variables > Modifier** le jeu de variables).



ii. La stratégie d'analyse de réseau qui inspecte le trafic chiffré doit avoir le port 443 (et tout autre port avec le trafic https qui sera décrypté par votre stratégie) inclus dans le champ des ports des paramètres du préprocesseur HTTP. Sinon, aucune des règles http avec modificateurs de contenu http (http_uri, http_header, etc.) ne se déclenchera car cela dépend des ports http définis et les tampons http dans snort ne seront pas renseignés pour le trafic qui ne passe pas par les ports spécifiés.

iii. (Facultatif mais recommandé pour une meilleure inspection) Ajoutez vos ports https aux paramètres **de configuration de flux TCP** dans le champ **Réassemblage de flux sur les deux ports**.

iv. Réappliquer la stratégie de contrôle d'accès révisée pendant une fenêtre de maintenance planifiée.

> **Avertissement :** cette stratégie modifiée peut entraîner des problèmes de performances importants. Il convient de tester cette fonctionnalité en dehors des heures de production afin de réduire les risques de panne ou de performances du réseau.

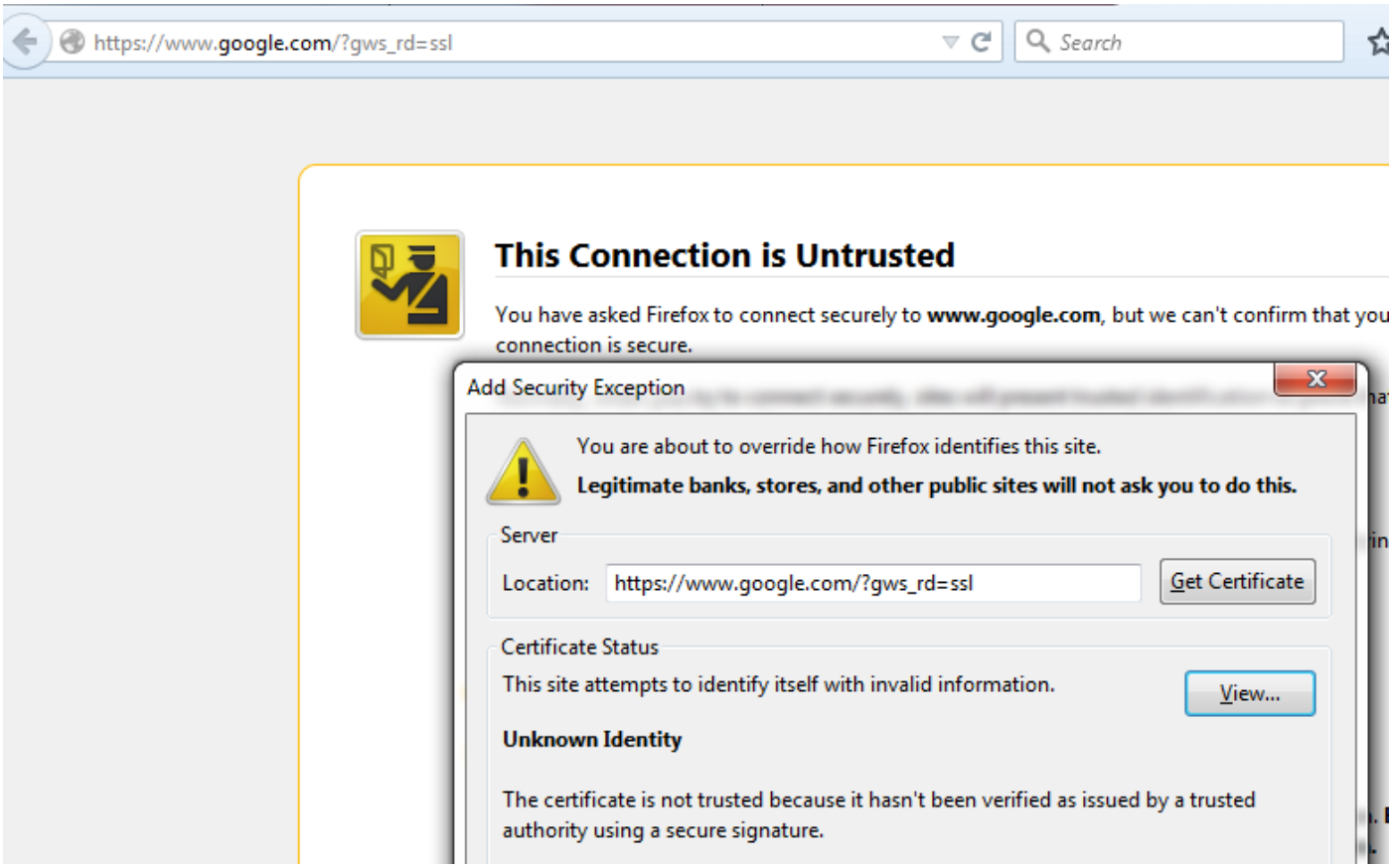
Vérification

Décrypter - Désigner

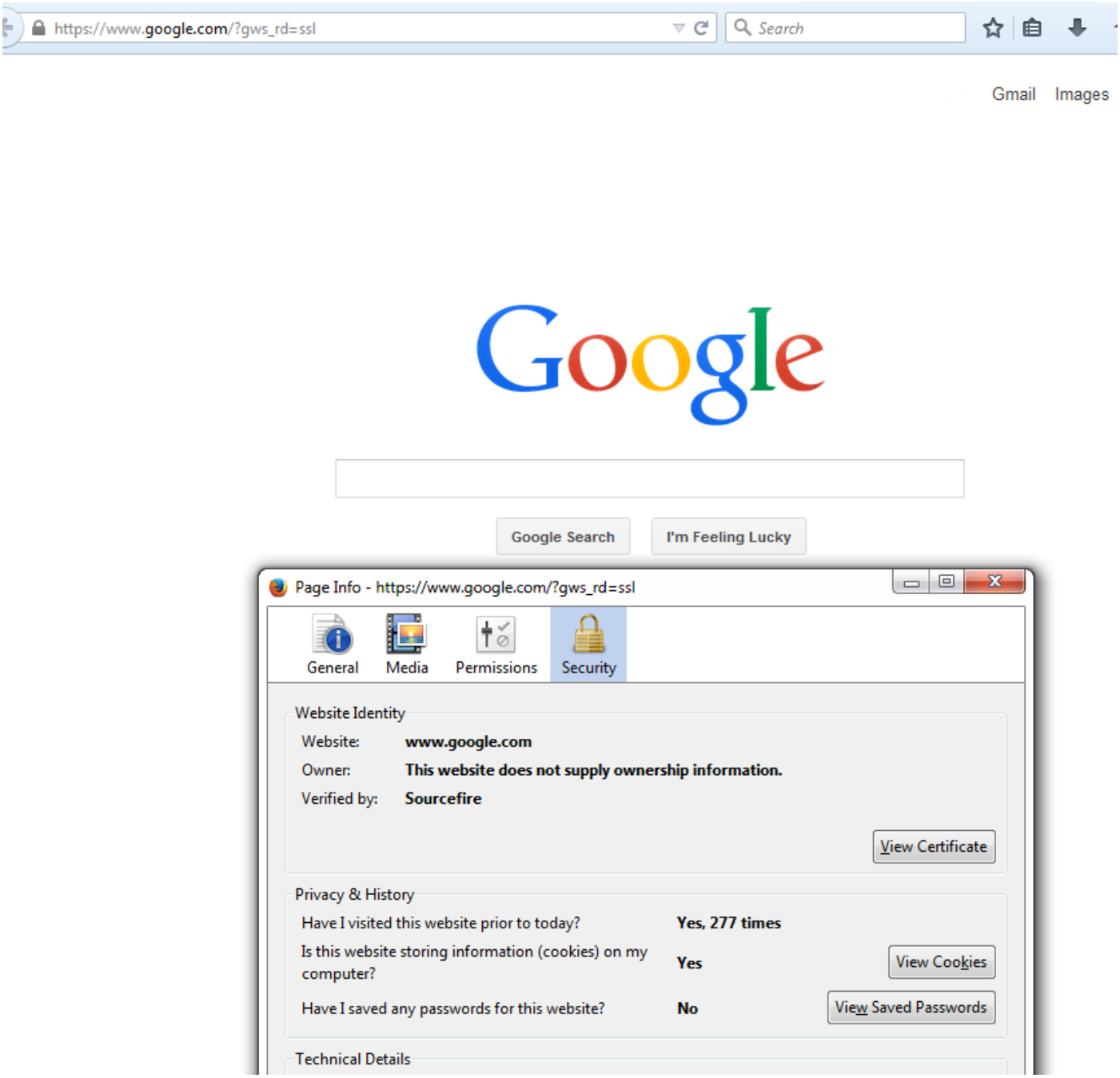
1. Ouvrez un navigateur Web.

> **Remarque :** le navigateur Firefox est utilisé dans l'exemple ci-dessous. Cet exemple peut ne pas fonctionner dans Chrome. Reportez-vous à la section Dépannage pour plus de détails.

2. Accédez à un site Web SSL. Dans l'exemple ci-dessous https://www.google.com est utilisé, les sites Web des institutions financières fonctionneront également. L'une des pages suivantes s'affiche :



Note: La page ci-dessus s'affiche si le certificat lui-même n'est pas approuvé et que le certificat de l'autorité de certification de signature n'est pas approuvé par votre navigateur. Pour savoir comment le navigateur détermine les certificats de CA approuvés, reportez-vous à la section Autorités de certification approuvées ci-dessous.



Note: Si cette page est affichée, vous avez correctement résigné le trafic. Notez la section **Vérifié par : Sourcefire**.

Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN)	www.google.com
Organization (O)	Google Inc
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	13:E3:D5:7D:4E:5F:8F:E7

Issued By

Common Name (CN)	Sourcefire TAC
Organization (O)	Sourcefire
Organizational Unit (OU)	Tac

Period of Validity

Begins On	5/6/2015
Expires On	8/3/2015

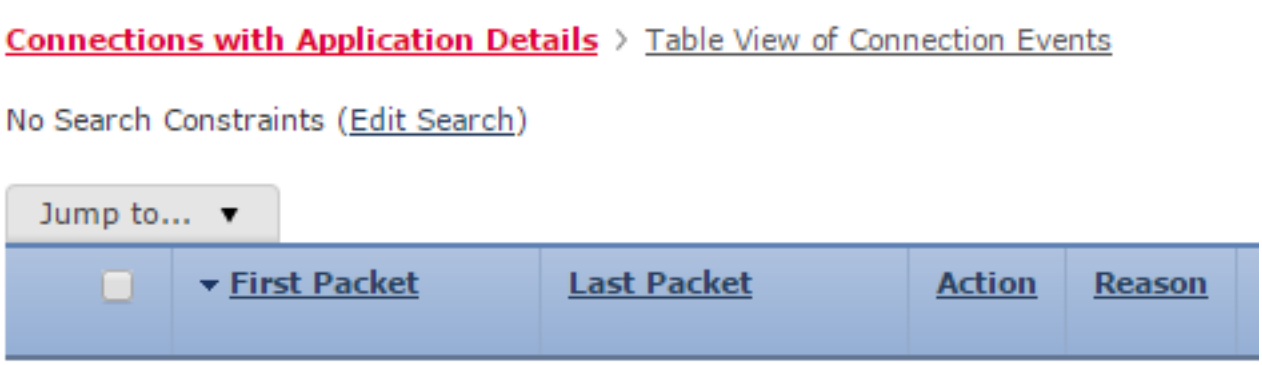
Fingerprints

SHA-256 Fingerprint	20:00:CB:25:13:8B:1F:89:4D:4A:CF:C5:E2:21:38:92: 06:66:00:2E:B7:83:27:72:98:EA:B1:6A:10:B3:67:A1
SHA1 Fingerprint	1B:C2:30:D9:66:84:DB:97:CF:A9:5E:5F:29:DA:4C:3F:13:E9:DE:5D

Note: Voici un aperçu du même certificat.

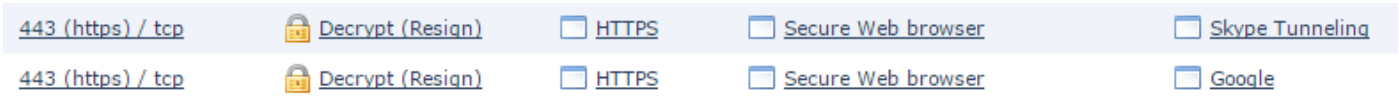
3. Dans Management Center, accédez à **Analysis > Connections > Events**.

4. Selon votre workflow, vous pouvez voir ou non l'option de déchiffrement SSL. Cliquez sur **Vue table des événements de connexion**.



5. Faites défiler la page vers la droite et recherchez l'état SSL. Vous devriez voir des options

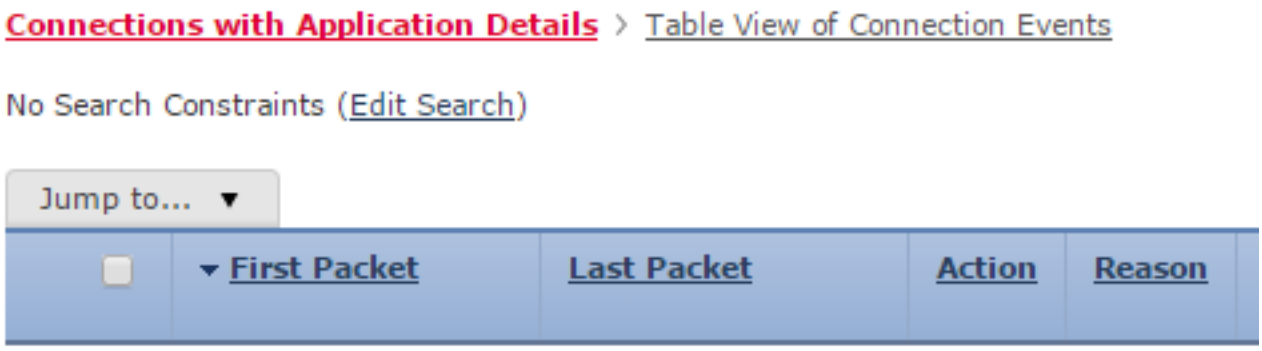
similaires à celles ci-dessous :



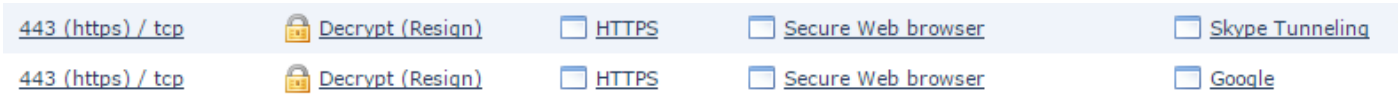
Décrypter - Certificat connu

1. Dans FireSIGHT Management Center, accédez à **Analysis > Connections > Events**.

2. Selon votre workflow, vous pouvez voir ou non l'option de déchiffrement SSL. Cliquez sur **Vue table des événements de connexion**.



3. Faites défiler la page vers la droite et recherchez l'état SSL. Vous devriez voir des options similaires à celles ci-dessous :



Dépannage

Problème 1: Certains sites Web ne peuvent pas être chargés sur le navigateur Chrome

Exemple

www.google.com ne peut pas se charger avec un décryptage - Déconnexion à l'aide de Chrome.

Motif

Le navigateur Google Chrome est capable de détecter des certificats frauduleux pour les propriétés de Google afin d'empêcher les attaques de l'homme du milieu. Si le navigateur Chrome (client) tente de se connecter à un domaine google.com (serveur) et qu'un certificat retourné qui n'est pas un certificat google valide, le navigateur refusera la connexion.

Solution

Si vous rencontrez ce problème, ajoutez une règle **Ne pas déchiffrer** pour DN=*.google.com, *.gmail.com, *.youtube.com. Ensuite, effacez le cache et l'historique du navigateur.

Problème 2: Obtention d'un avertissement/d'une erreur non approuvé dans certains navigateurs

Exemple

Lorsque vous vous connectez à un site à l'aide d'Internet Explorer et de Chrome, vous ne recevez pas d'avertissement de sécurité, mais lorsque vous utilisez le navigateur Firefox, vous devez faire confiance à la connexion chaque fois que vous fermez et rouvrez le navigateur.

Motif

La liste des autorités de certification approuvées dépend du navigateur. Lorsque vous faites confiance à un certificat, celui-ci ne se propage pas dans les navigateurs et l'entrée approuvée ne dure généralement que pendant l'ouverture du navigateur. Une fois fermé, tous les certificats approuvés seront supprimés et la prochaine fois que vous ouvrirez le navigateur et visitez le site, vous devez l'ajouter à nouveau à la liste des certificats approuvés.

Solution

Dans ce scénario, IE et Chrome utilisent tous deux la liste des autorités de certification de confiance dans le système d'exploitation, mais Firefox conserve sa propre liste. Le certificat CA a donc été importé dans le magasin du système d'exploitation mais n'a pas été importé dans le navigateur Firefox. Afin d'éviter d'obtenir l'avertissement de sécurité dans Firefox, vous devez importer le certificat CA dans le navigateur en tant qu'autorité de certification de confiance.

Autorités de certification approuvées

Lorsqu'une connexion SSL est établie, le navigateur vérifie d'abord si ce certificat est approuvé (c'est-à-dire que vous êtes déjà allé sur ce site et que vous lui avez demandé manuellement de faire confiance à ce certificat). Si le certificat n'est pas approuvé, le navigateur vérifie le certificat de l'autorité de certification (AC) qui a vérifié le certificat pour ce site. Si le certificat d'autorité de certification est approuvé par le navigateur, il le considère comme un certificat approuvé et autorise la connexion. Si le certificat de l'autorité de certification n'est pas approuvé, le navigateur affiche un avertissement de sécurité et vous force à ajouter manuellement le certificat en tant que certificat approuvé.

La liste des autorités de certification de confiance dans un navigateur dépend entièrement de la mise en oeuvre du navigateur et chaque navigateur peut remplir sa liste de confiance différemment des autres navigateurs. En général, les navigateurs actuels remplissent une liste de CA approuvées de deux manières :

1. Ils utilisent la liste des autorités de certification approuvées par le système d'exploitation
2. Ils expédient une liste des autorités de certification de confiance avec le logiciel et il est intégré dans le navigateur.

Pour les navigateurs les plus courants, les autorités de certification de confiance sont remplies comme suit :

- **Google Chrome** : Liste des CA fiables du système d'exploitation

- **Firefox** : Tenir à jour sa propre liste de CA de confiance
- **Internet Explorer** : Liste des CA fiables du système d'exploitation
- **Safari** : Liste des CA fiables du système d'exploitation

Il est important de connaître la différence, car le comportement du client varie en fonction de celui-ci. Par exemple, pour ajouter une autorité de certification approuvée pour Chrome et IE, vous devez importer le certificat d'autorité de certification dans le magasin d'autorité de certification approuvé du système d'exploitation. Si vous importez le certificat d'autorité de certification dans le magasin d'autorité de certification approuvé du système d'exploitation, vous n'obtiendrez plus d'avertissement lors de la connexion aux sites avec un certificat signé par cette autorité de certification. Dans le navigateur Firefox, vous devez importer manuellement le certificat d'autorité de certification dans le magasin d'autorité de certification approuvé dans le navigateur lui-même. Après cela, vous n'obtiendrez plus d'avertissement de sécurité lors de la connexion aux sites vérifiés par cette autorité de certification.

Références

- Mise en route des règles SSL