Configurer l'intégration Active Directory avec ASDM pour l'authentification unique et l'authentification captive du portail (gestion intégrée)

Contenu

Introduction

Ce document décrit la configuration de l'authentification du portail captif (authentification active) et de l'authentification unique (authentification passive) sur le module Firepower à l'aide d'ASDM (Adaptive Security Device Manager).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance du pare-feu ASA (Adaptive Security Appliance) et de l'ASDM
- Connaissances du module FirePOWER
- Service LDAP (Light Weight Directory Service)
- Agent utilisateur Firepower

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.

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

Captive Portal Authentication ou Active Authentication demande une page de connexion et les informations d'identification de l'utilisateur sont requises pour qu'un hôte puisse accéder à Internet.

L'authentification à connexion unique ou passive permet à un utilisateur d'obtenir une authentification transparente pour les ressources réseau et l'accès à Internet sans saisir plusieurs fois les informations d'identification de l'utilisateur. L'authentification à connexion unique peut être obtenue soit par l'agent utilisateur Firepower, soit par l'authentification du navigateur NTLM.

> **Remarque** : l'authentification du portail captif, ASA doit être en mode routé.

> **Note**: La commande Captive Portal est disponible dans ASA version 9.5(2) et versions ultérieures.

Configuration

Étape 1. Configurez l'agent utilisateur Firepower pour l'authentification unique.

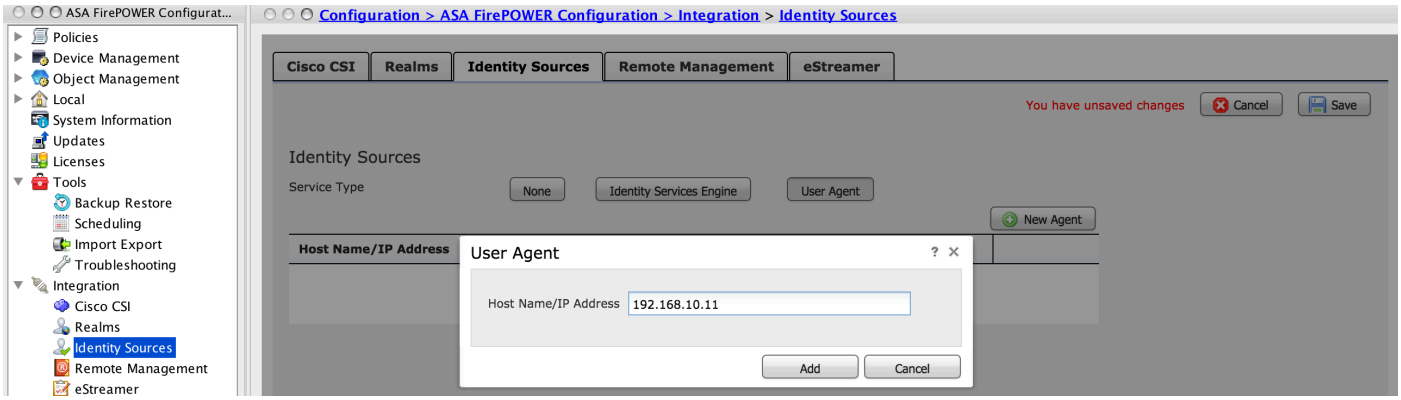
Cet article explique comment configurer Firepower User Agent dans l'ordinateur Windows :

Installation et désinstallation de Sourcefire User Agent

Étape 2. Intégrez le module Firepower (ASDM) à l'agent utilisateur.

Connectez-vous à ASDM, accédez à **Configuration > ASA FirePOWER Configuration > Integration > Identity Sources** et cliquez sur l'option **User Agent**. Après avoir cliqué sur l'option **Agent**

utilisateur et configuré l'adresse IP du système Agent utilisateur. cliquez sur **Ajouter**, comme l'illustre l'image :



Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications.

Étape 3. Intégrer Firepower à Active Directory.

Étape 3.1 - Créez le domaine.

Connectez-vous à ASDM, accédez à **Configuration > ASA FirePOWER Configuration > Integration > Realms.** Cliquez sur **Ajouter un nouveau domaine**.

Nom et description : Donnez un nom/une description pour identifier le domaine de manière unique.

Type : AD

Domaine principal AD : Nom de domaine d'Active Directory (nom NETBIOS).

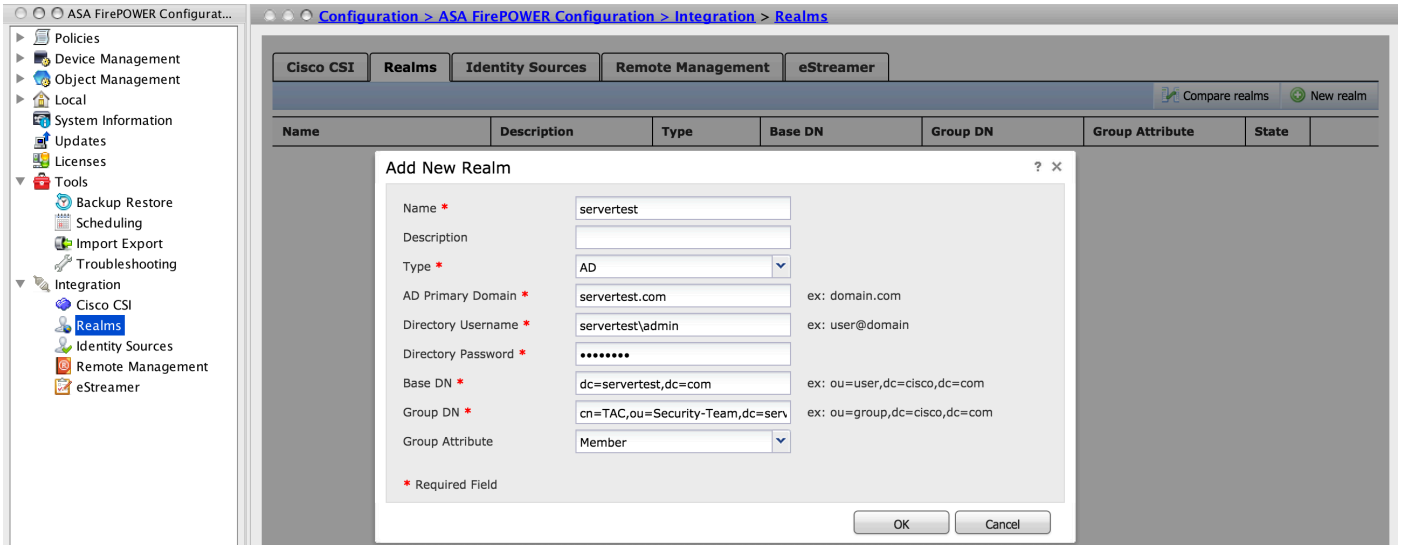
Nom d'utilisateur du répertoire : spécifiez le <*nom d'utilisateur*>.

Mot de passe du répertoire : Spécifiez le <*mot de passe*>.

Nom unique de base : Domaine ou Nom unique d'unité d'organisation spécifique à partir duquel le système lancera une recherche dans la base de données LDAP.

DN du groupe : Spécifiez le DN du groupe.

Attribut de groupe : Spécifiez l'option Member dans la liste déroulante.



Cliquez sur **OK** pour enregistrer la configuration.

Cet article peut vous aider à déterminer les valeurs DN de base et DN de groupe.

[Identifier les attributs d'objet LDAP Active Directory]

Étape 3.2 - Ajoutez l'adresse IP/le nom d'hôte du serveur d'annuaire.

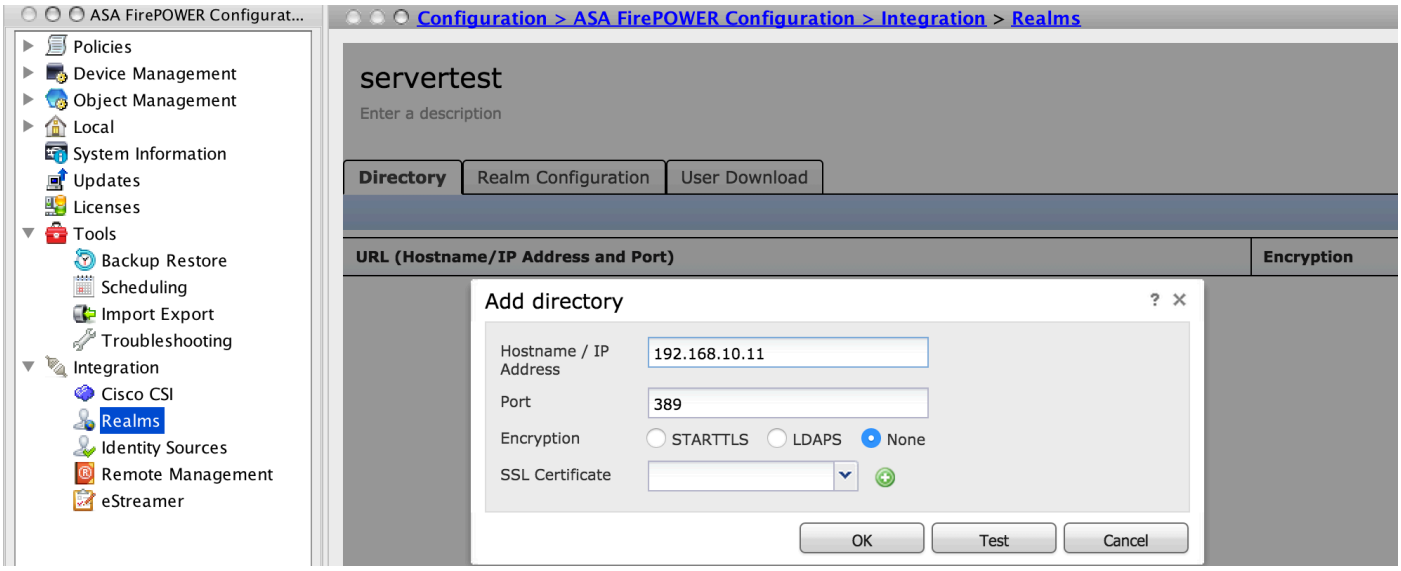
Pour spécifier l'adresse IP/le nom d'hôte du serveur AD, cliquez sur **Ajouter un répertoire**.

Nom d'hôte/Adresse IP : configurez l'adresse IP/nom d'hôte du serveur AD.

Port : spécifiez le numéro de port LDAP Active Directory (389 par défaut).

Certificat de chiffrement/SSL : (facultatif) Pour chiffrer la connexion entre le serveur FMC et AD, reportez-vous à cet article :

[Vérification de l'objet d'authentification sur FireSIGHT System pour l'authentification AD Microsoft sur SSL/T...]



Cliquez sur **Tester** afin de vérifier la connexion de FMC avec le serveur AD. Cliquez maintenant sur **OK** pour enregistrer la configuration.

Étape 3.3 - Modifiez la configuration du domaine.

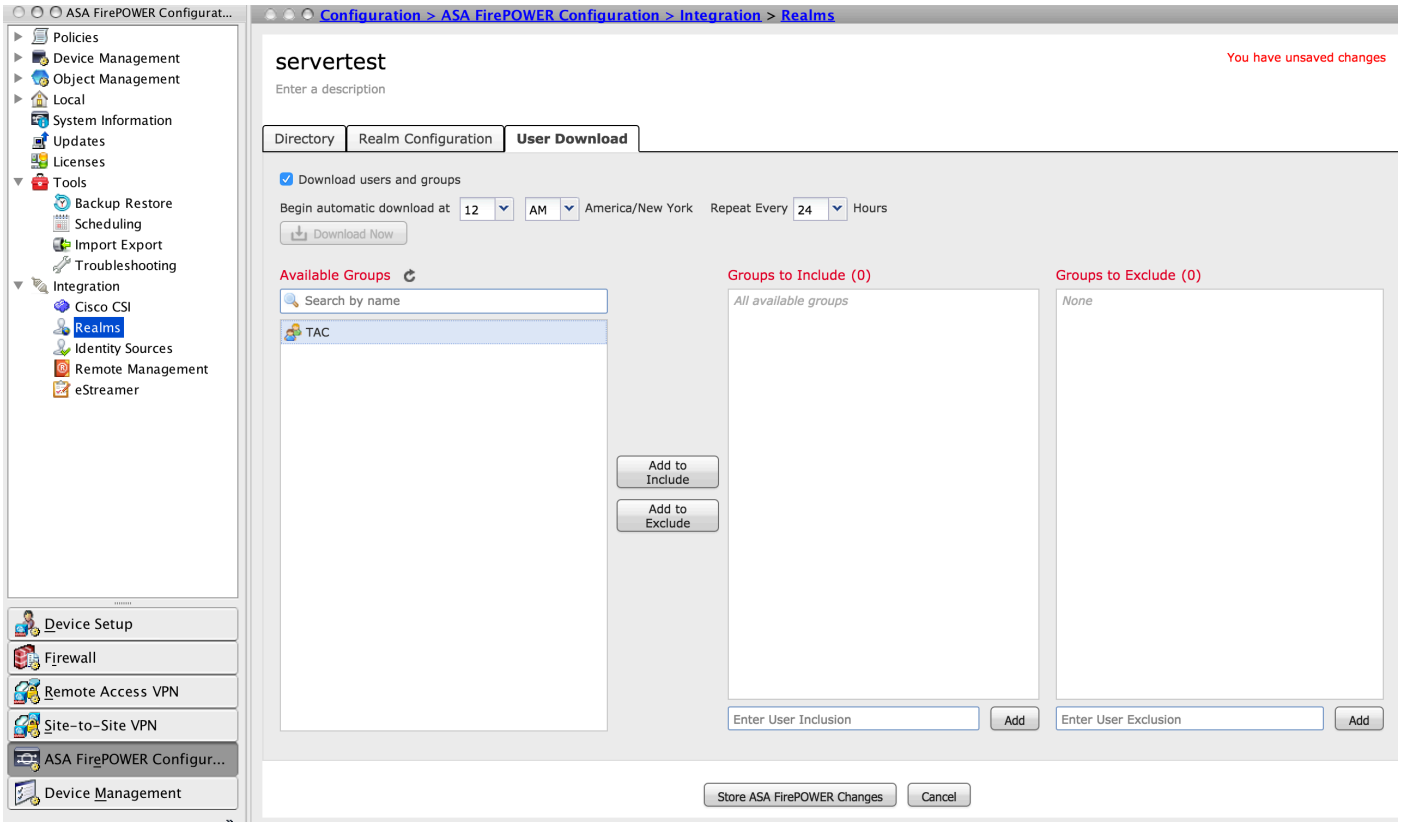
Afin de modifier et de vérifier la configuration d'intégration du serveur AD, accédez à **Configuration de domaine**.

Étape 3.4 - Téléchargez la base de données des utilisateurs.

Accédez à **Téléchargement utilisateur** pour récupérer la base de données utilisateur à partir du serveur AD.

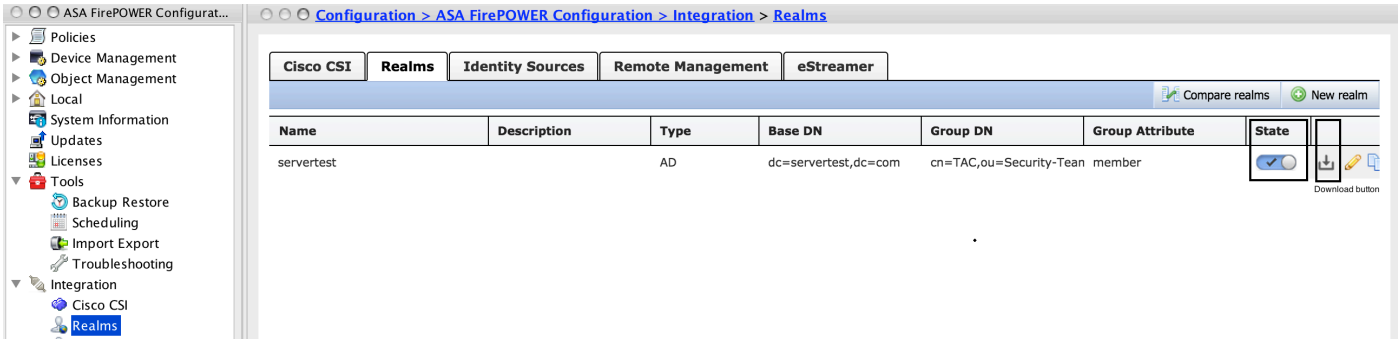
Activez la case à cocher pour télécharger **les utilisateurs et les groupes de téléchargement** et définissez l'intervalle de temps sur la fréquence à laquelle le module Firepower contacte le serveur AD pour télécharger la base de données utilisateur.

Sélectionnez le groupe et ajoutez-le à l'option **Inclure** pour laquelle vous voulez configurer l'authentification. Par défaut, tous les groupes sont sélectionnés si vous ne choisissez pas d'inclure les groupes.



Cliquez sur **Store ASA Firepower Changes** pour enregistrer la configuration du domaine.

Activez l'état du domaine et cliquez sur le bouton de téléchargement pour télécharger les utilisateurs et les groupes, comme illustré dans l'image.



Étape 4. Configurez la stratégie d'identité.

Une stratégie d'identité effectue l'authentification des utilisateurs. Si l'utilisateur ne s'authentifie pas, l'accès aux ressources réseau est refusé. Cela applique le contrôle d'accès basé sur les rôles (RBAC) au réseau et aux ressources de votre entreprise.

Étape 4.1 Portail captif (Authentification active)

Active Authentication demande un nom d'utilisateur et un mot de passe dans le navigateur pour identifier une identité d'utilisateur afin d'autoriser toute connexion. Le navigateur authentifie l'utilisateur en présentant une page d'authentification ou s'authentifie silencieusement avec l'authentification NTLM. NTLM utilise le navigateur Web pour envoyer et recevoir des informations d'authentification. L'authentification active utilise différents types pour vérifier l'identité de l'utilisateur. Différents types d'authentification sont les suivants :

1. **HTTP Basic : dans cette méthode, le navigateur demande des informations d'identification utilisateur.**
2. **NTLM : NTLM utilise les informations d'identification de la station de travail Windows et la négocie avec Active Directory à l'aide d'un navigateur Web. Vous devez activer l'authentification NTLM dans le navigateur. L'authentification utilisateur se produit de manière transparente sans demander d'informations d'identification. Il offre une expérience d'authentification unique aux utilisateurs.**
3. **HTTP Negotiate :** Dans ce type, le système tente de s'authentifier à l'aide de NTLM, s'il échoue, le capteur utilise le type d'authentification HTTP Basic comme méthode de secours et invite une boîte de dialogue pour les informations d'identification de l'utilisateur.
4. **Page de réponse HTTP : Ce type est similaire au type de base HTTP. Cependant, ici, l'utilisateur est invité à remplir l'authentification dans un formulaire HTML qui peut être personnalisé.**

Chaque navigateur dispose d'une façon spécifique d'activer l'authentification NTLM et, par conséquent, vous pouvez suivre les directives du navigateur afin d'activer l'authentification NTLM.

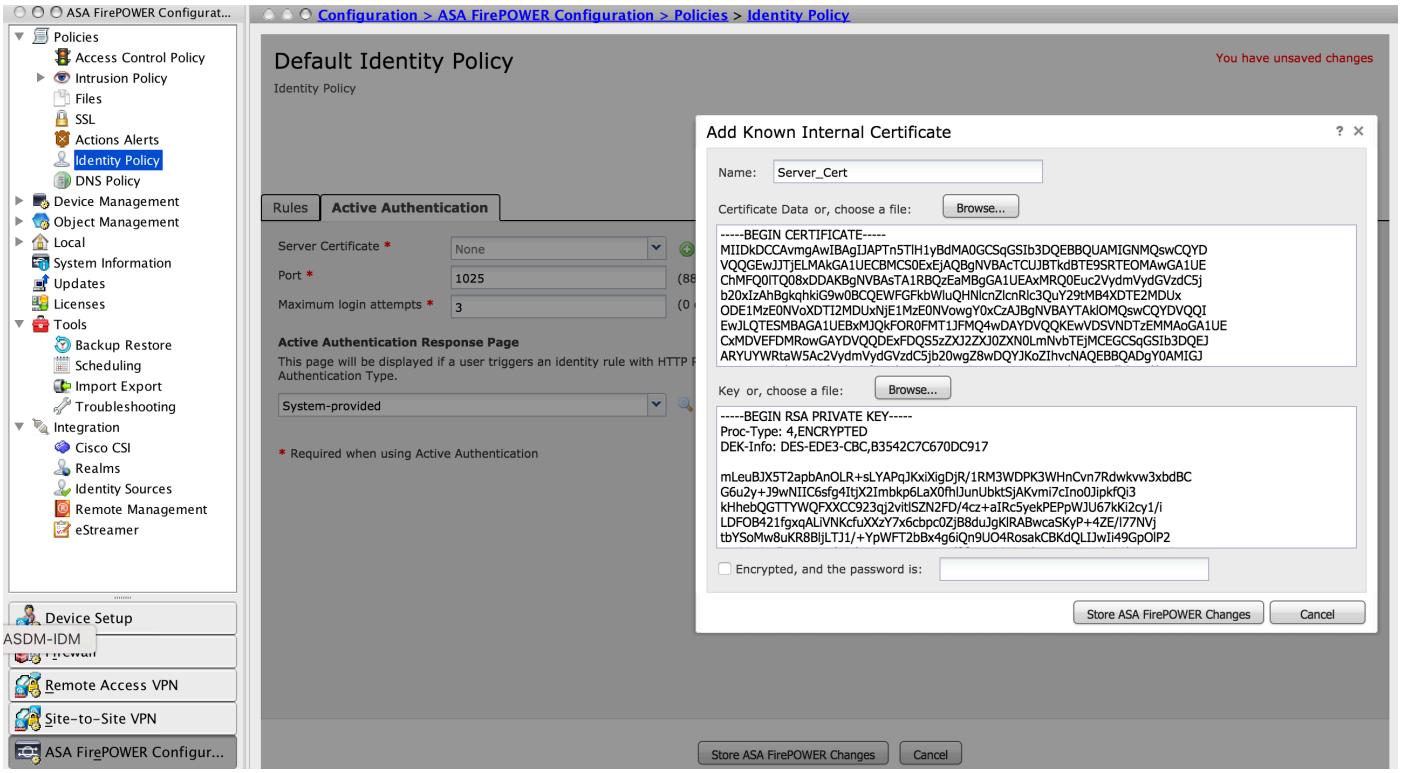
Pour partager en toute sécurité les informations d'identification avec le capteur routé, vous devez installer un certificat de serveur auto-signé ou un certificat de serveur signé publiquement dans la stratégie d'identité.

```
Generate a simple self-signed certificate using openSSL -

Step 1.   Generate the Private key
               openssl genrsa -des3 -out server.key 2048

Step 2.   Generate Certificate Signing Request (CSR)
```

```
openssl req -new -key server.key -out server.csr
```

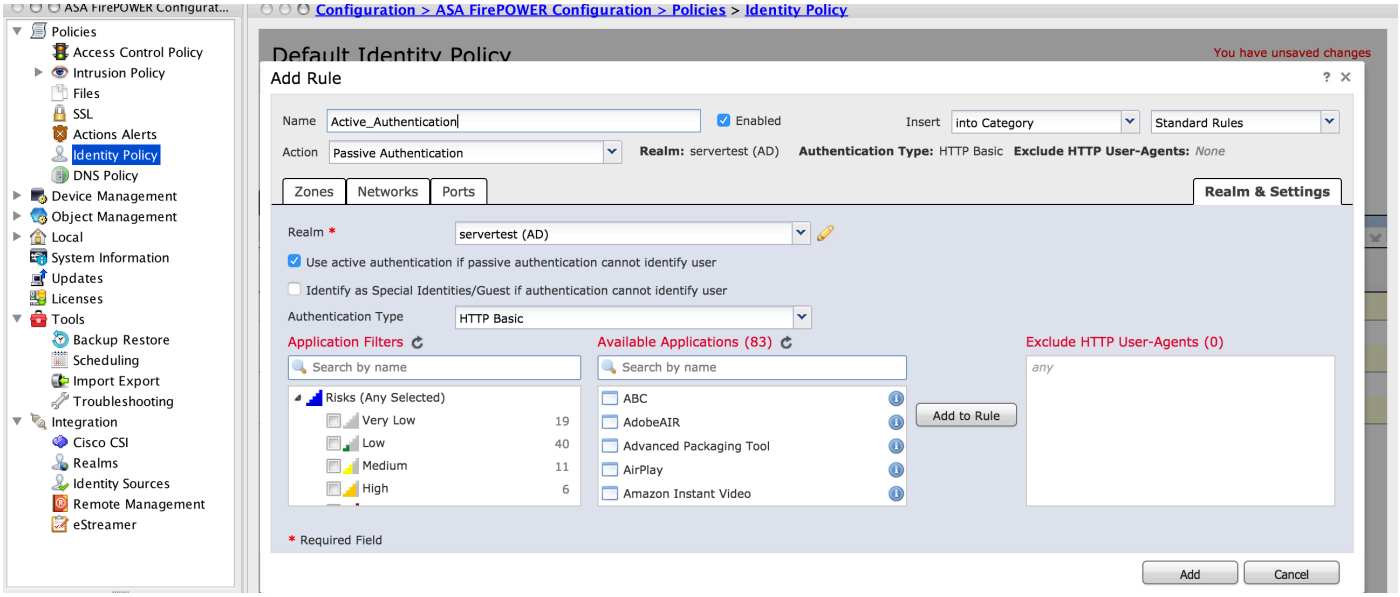
```
Step 3.   Generate the self-signed Certificate.
openssl x509 -req -days 3650 -sha256 -in server.csr -signkey server.key -out server.crt
```

Accédez à **Configuration > ASA FirePOWER Configuration > Policies > Identity Policy**. Maintenant accédez à l'onglet **Authentification active** et dans l'option **Certificat serveur**, cliquez sur l'**icône (+)** et téléchargez le certificat et la clé privée que vous avez générés à l'étape précédente à l'aide d'openSSL, comme illustré dans l'image :



Cliquez maintenant sur **Ajouter une règle** pour donner un nom à la règle et choisissez l'action en tant qu'**Authentification active**. Définissez la zone source/destination, le réseau source/destination pour lequel vous voulez activer l'authentification utilisateur.

Accédez à l'onglet **Domaine et paramètres**. Sélectionnez le **domaine** dans la liste déroulante que vous avez configurée à l'étape précédente et sélectionnez le **type d'authentification** dans la liste déroulante qui convient le mieux à votre environnement réseau.



Étape 4.2 Configuration ASA pour Captive Portal.

Étape 1. Définissez le trafic intéressant qui sera redirigé vers Sourcefire pour inspection.

```
ASA(config)# access-list SFR_ACL extended permit ip 192.168.10.0 255.255.255.0 any
ASA(config)#
ASA(config)# class-map SFR_CMAP
ASA(config-cmap)# match access-list SFR_ACL
```

```
ASA(config)# policy-map global_policy
ASA(config-pmap)# class SFR_CMAP
ASA(config-pmap-c)# sfr fail-open
ASA(config)#service-policy global_policy global
```

Étape 2. Configurez cette commande sur l'ASA afin d'activer le portail captif.

```
ASA(config)# captive-portal interface inside port 1025
```

> **Astuce** : captive-portal peut être activé globalement ou par interface.

> **Astuce** : Assurez-vous que le port du serveur, TCP 1025, est configuré dans l'option de port de l'onglet Authentification active de la stratégie d'identité.

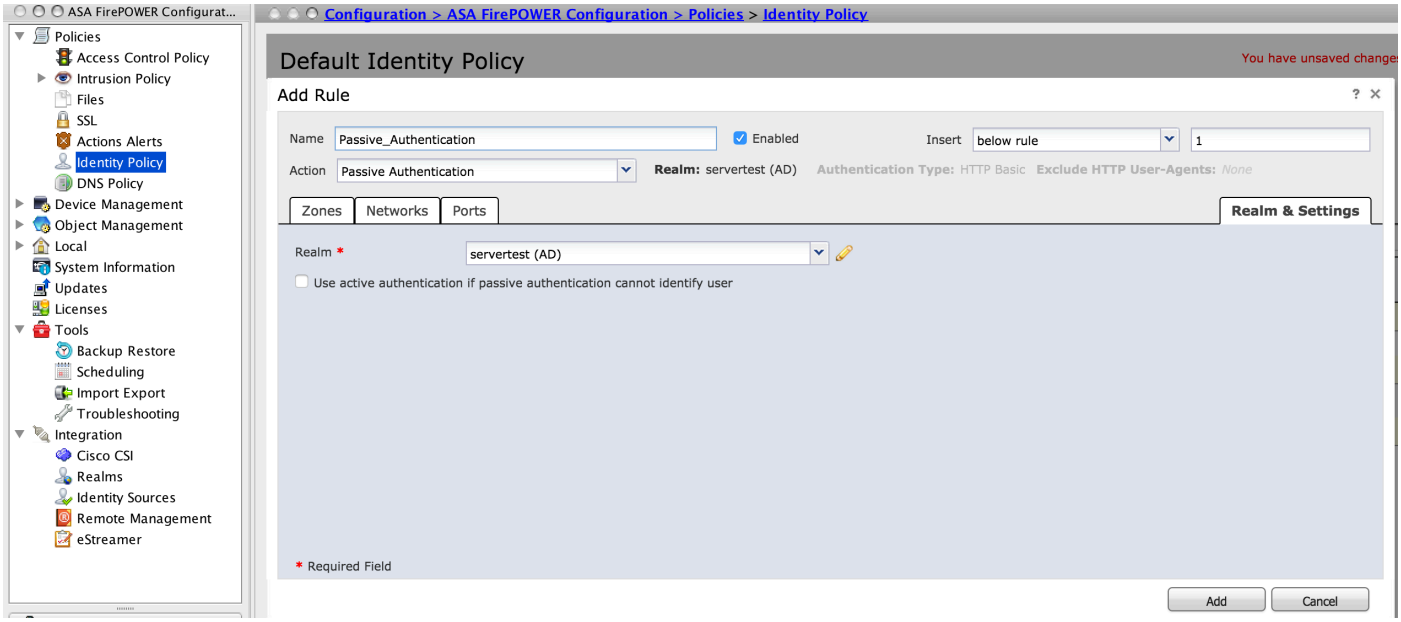
Étape 4.3 Authentification unique (authentification passive).

Dans l'authentification passive, lorsqu'un utilisateur de domaine se connecte et est en mesure d'authentifier la distance administrative, l'agent utilisateur Firepower interroge les détails du mappage utilisateur-IP à partir des journaux de sécurité d'AD et partage ces informations avec Firepower Module. Le module Firepower utilise ces informations afin d'appliquer le contrôle d'accès.

Pour configurer la règle d'authentification passive, cliquez sur **Ajouter une règle** pour donner un nom à la règle, puis choisissez l'**action** comme **authentification passive**. Définissez la zone source/destination, le réseau source/destination pour lequel vous voulez activer l'authentification utilisateur.

Accédez à la **Domaine et paramètres** . Sélectionnez le **Domaine** dans la liste déroulante que vous avez configurée à l'étape précédente.

Vous pouvez choisir la méthode de retour en arrière comme **authentification active si l'authentification passive ne peut pas identifier l'identité de l'utilisateur**, comme illustré dans l'image :

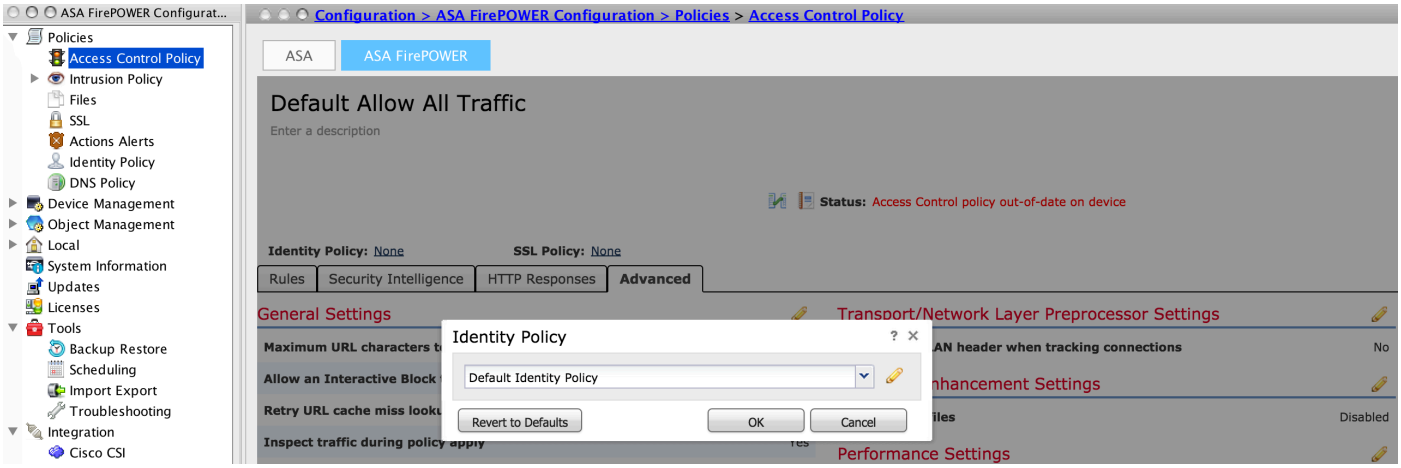


Cliquez maintenant sur **Store ASA Firepower Changes** pour enregistrer la configuration de la stratégie d'identité.

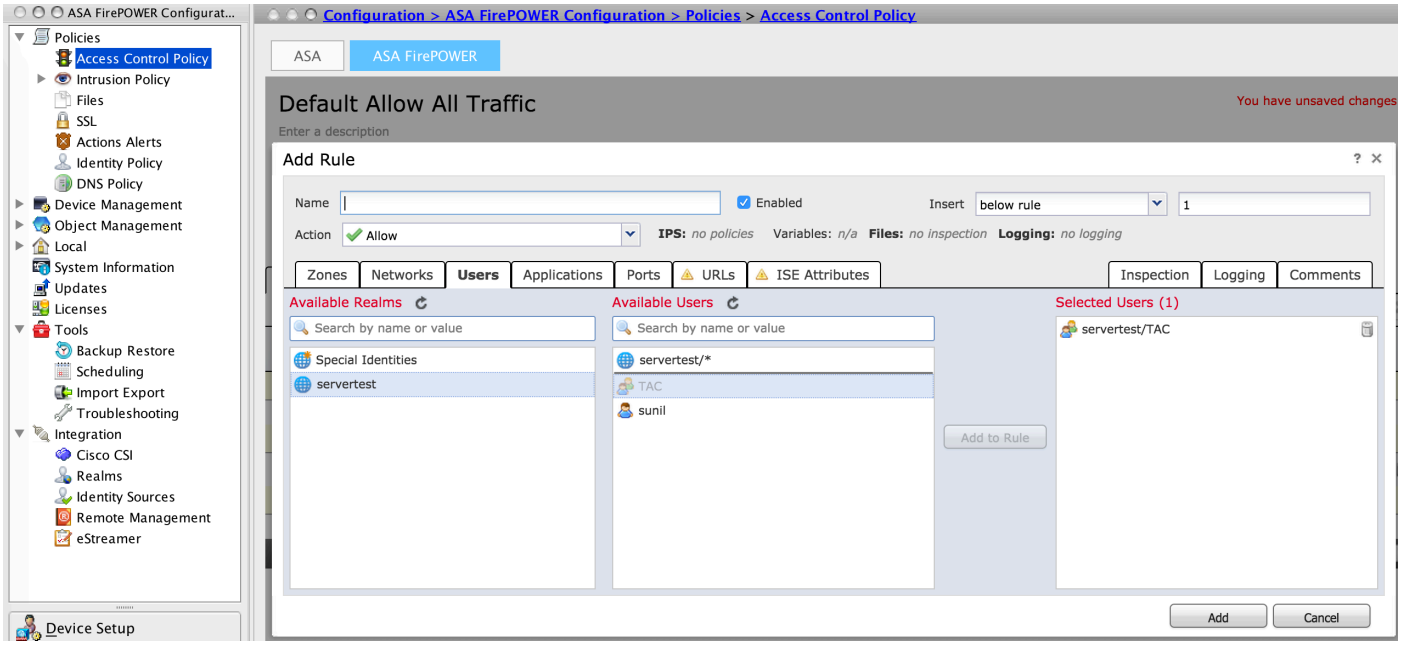
Étape 5. Configurez la stratégie de contrôle d'accès.

Accédez à **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy.**

Cliquez sur la **stratégie d'identité** (dans le coin supérieur gauche), sélectionnez la stratégie d'identification que vous avez configurée à l'étape précédente dans la liste déroulante et cliquez sur **OK**, comme illustré dans cette image.



Cliquez sur **Ajouter une règle** pour ajouter une nouvelle règle, accédez à **Utilisateurs** et sélectionnez les utilisateurs pour lesquels la règle de contrôle d'accès sera appliquée, comme illustré dans cette image, puis cliquez sur **Ajouter**.



Cliquez sur **Modifications apportées au pare-feu ASA du magasin** pour enregistrer la configuration de la stratégie de contrôle d'accès.

Étape 6. Déployez la stratégie de contrôle d'accès.

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

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

> **Note**: Naviguez jusqu'à Monitoring > ASA Firepower Monitoring > Task Status. Assurez-vous que la tâche doit être terminée en appliquant la modification de configuration.

Étape 7. Surveiller les événements utilisateur.

Accédez à **Monitoring > ASA FirePOWER Monitoring > Real-Time Eventil**, pour surveiller le type de trafic utilisé par l'utilisateur.

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Accédez à **Analysis > Users** afin de vérifier le type d'authentification/d'authentification utilisateur/mappage utilisateur-IP/règle d'accès associé au flux de trafic.

Connectivité entre le module Firepower et l'agent utilisateur (authentification passive)

Le module Firepower utilise le port TCP 3306, afin de recevoir les données du journal d'activité de l'utilisateur de l'agent utilisateur.

Afin de vérifier l'état du service du module Firepower, utilisez cette commande dans le FMC.

```
admin@firepower:~$ netstat -tan | grep 3306
```

Exécutez la capture de paquets sur le FMC afin de vérifier la connectivité avec l'Agent utilisateur.

```
admin@firepower:~$ sudo tcpdump -i eth0 -n port 3306
```

Connectivité entre FMC et Active Directory

Le module Firepower utilise le port TCP 389 afin de récupérer la base de données utilisateur à partir de Active Directory.

Exécutez la capture de paquets sur le module Firepower pour vérifier la connectivité avec Active Directory.

```
admin@firepower:~$ sudo tcpdump -i eth0 -n port 389
```

Assurez-vous que les informations d'identification de l'utilisateur utilisées dans la configuration du domaine disposent de privilèges suffisants pour récupérer la base de données utilisateur d'AD.

Vérifiez la configuration du domaine et assurez-vous que les utilisateurs/groupes sont téléchargés et que le délai d'expiration de la session utilisateur est configuré correctement.

Accédez à Surveillance de l'état des tâches de surveillance ASA Firepower et assurez-vous que le téléchargement des tâches par les utilisateurs/groupes s'est terminé correctement, comme illustré dans cette image.

Connectivité entre ASA et système d'extrémité (authentification active)

authentification active, assurez-vous que le certificat et le port sont correctement configurés dans la stratégie d'identité du module Firepower et dans ASA (commande captive-portal). Par défaut, ASA et le module Firepower écoutent sur le port TCP 885 pour l'authentification active.

Afin de vérifier les règles actives et leur nombre de coups, exécutez cette commande sur l'ASA.

```
ASA# show asp table classify domain captive-portal

Input Table
in  id=0x2aaadf516030, priority=121, domain=captive-portal, deny=false
   hits=10, user_data=0x0, cs_id=0x0, flags=0x0, protocol=6
   src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
   dst ip/id=19.19.19.130, mask=255.255.255.255, port=1025, tag=any, dscp=0x0
   input_ifc=inside, output_ifc=identity

Output Table:

L2 - Output Table:

L2 - Input Table:
```

```
Last clearing of hits counters: Never
```

Configuration des politiques et déploiement des politiques

Assurez-vous que les champs Domaine, Type d'authentification, Agent utilisateur et Action sont configurés correctement dans Stratégie d'identité.

Assurez-vous que la stratégie d'identité est correctement associée à la stratégie de contrôle d'accès.

Naviguez jusqu'à Monitoring > ASA Firepower Monitoring > Task Status et assurez-vous que le déploiement de la stratégie se termine correctement.

Dépannage

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

Informations connexes

- Support et documentation techniques - Cisco Systems
- Configurer l'intégration Active Directory avec Firepower Appliance pour l'authentification unique et l'authentification captive du portail