Configurer l'intégration d'Active Directory avec l'appliance Firepower pour l'authentification Single-Sign-On par & Captive Portal

Table des matières

Introduction

Ce document décrit la configuration de l'authentification du portail captif (authentification active) et de l'authentification unique (authentification passive).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Périphériques Sourcefire Firepower
- Modèles de périphériques virtuels
- Service d'annuaire léger (LDAP)
- Agent utilisateur Firepower

Composants utilisés

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

- Firepower Management Center (FMC) version 6.0.0 et ultérieure
- Capteur Firepower 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

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

L'authentification unique ou passive fournit une authentification transparente à un utilisateur pour les ressources réseau et l'accès à Internet sans que plusieurs identifiants d'utilisateur ne se produisent. L'authentification par authentification unique peut être réalisée par l'agent utilisateur Firepower ou par l'authentification du navigateur NTLM.

Remarque : pour l'authentification Captive Portal, l'appliance doit être en mode routé.

Configurer

Étape 1. Configuration de l'agent utilisateur Firepower pour l'authentification unique

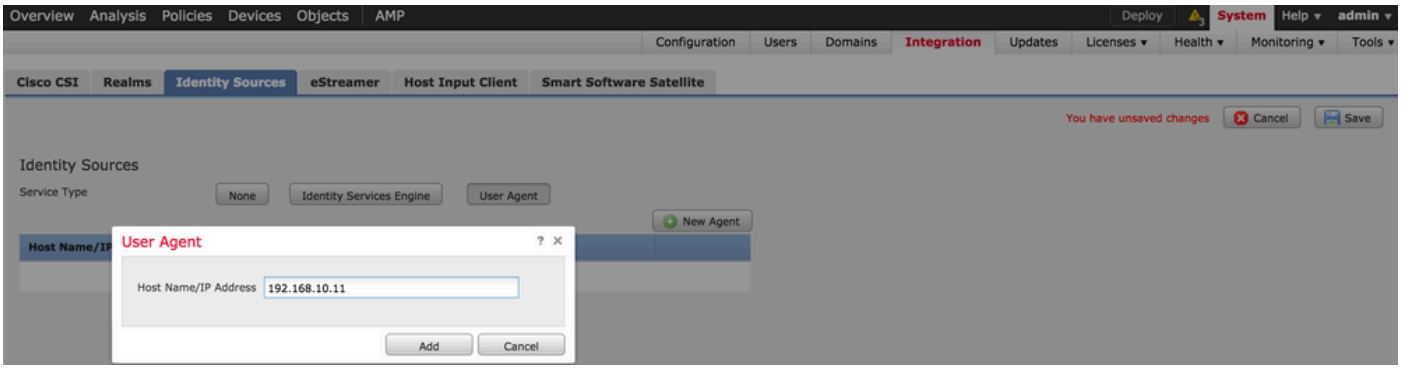
Cet article explique comment configurer Firepower User Agent sur un ordinateur Windows :

Installation et désinstallation de Sourcefire User Agent

Étape 2. Intégration de Firepower Management Center (FMC) à User Agent

Connectez-vous à Firepower Management Center, accédez à System > Integration > Identity Sources. Cliquez sur l'option Nouvel agent. Configurez l'adresse IP du système User Agent et cliquez sur le bouton Add.

Cliquez sur le bouton Save pour enregistrer les modifications.



Étape 3. Intégrer Firepower à Active Directory

Étape 3.1 Création du domaine

Connectez-vous à FMC, accédez à System > Integration > Realm. Cliquez sur l'option 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 Active Directory

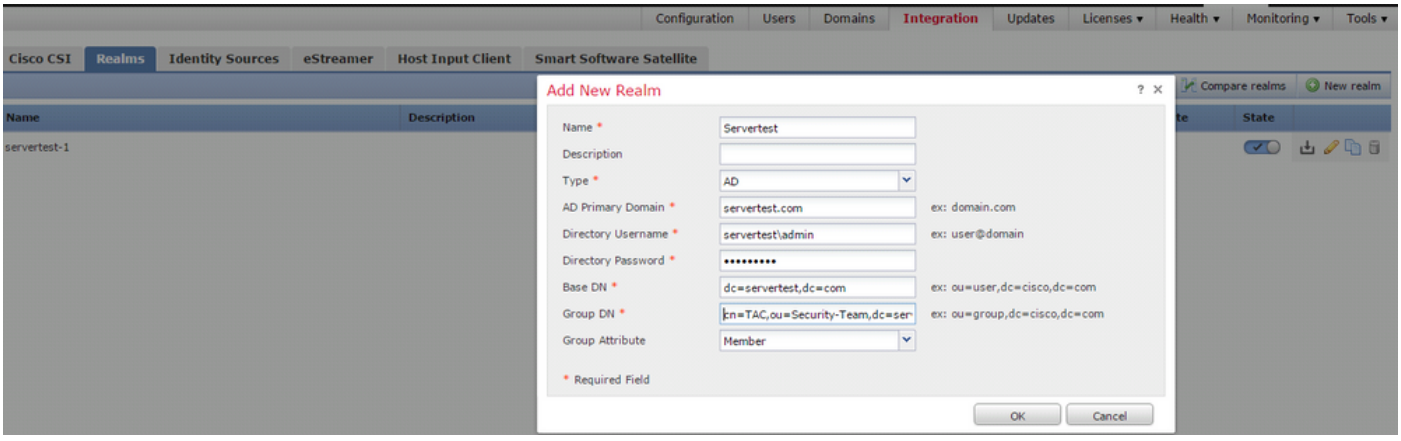
Nom d'utilisateur du répertoire : <username>

Mot de passe du répertoire : <password>

DN de base : domaine ou DN d'unité d'organisation spécifique à partir duquel le système lance une recherche dans la base de données LDAP.

DN de groupe : DN de groupe

Attribut de groupe : Membre



Cet article vous aide à comprendre les valeurs DN de base et DN de groupe.

[Identifier les attributs d'objet LDAP Active Directory]

Étape 3.2 Ajout du serveur d'annuaire

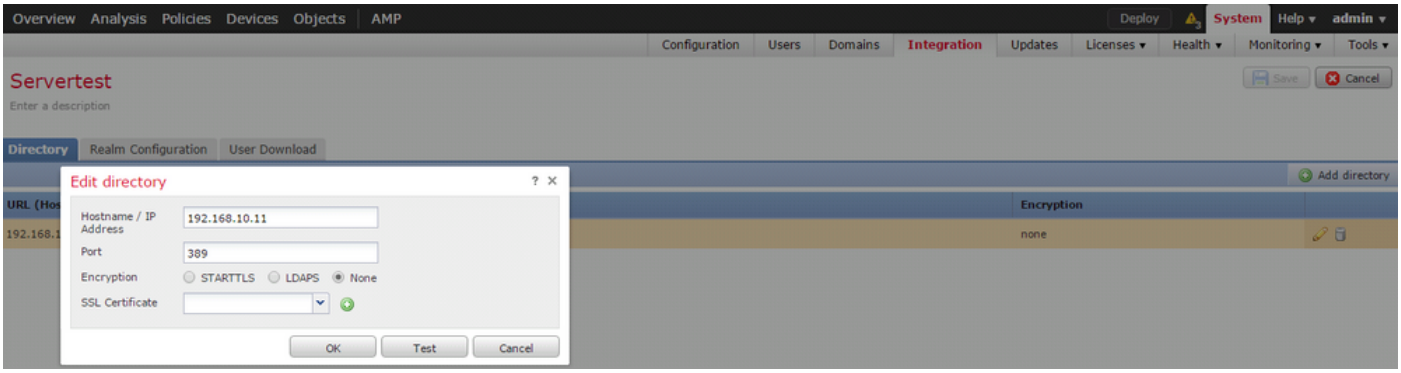
Cliquez sur le bouton Add afin de naviguer à l'étape suivante et ensuite cliquez sur l'option Add directory.

Hostname/IP Address : configurez l'adresse IP/le nom d'hôte du serveur AD.

Port : 389 (numéro de port LDAP Active Directory)

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

article : [Vérification de l'objet d'authentification sur FireSIGHT System pour l'authentification Microsoft AD sur SSL/TLS]



Cliquez sur le bouton Test afin de vérifier si FMC est en mesure de se connecter au serveur AD.

Étape 3.3 Modification de la configuration du domaine

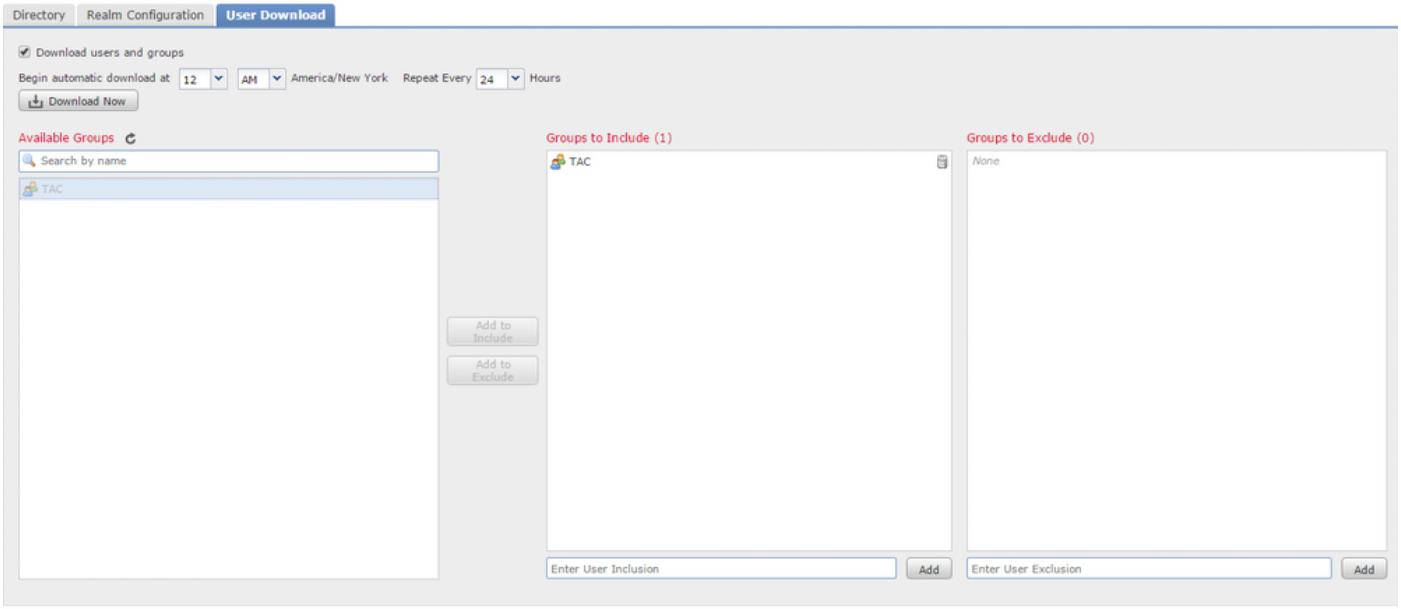
Accédez à Configuration du domaine afin de vérifier la configuration d'intégration du serveur AD et vous pouvez modifier la configuration AD.

Étape 3.4 Téléchargement de la base de données utilisateur

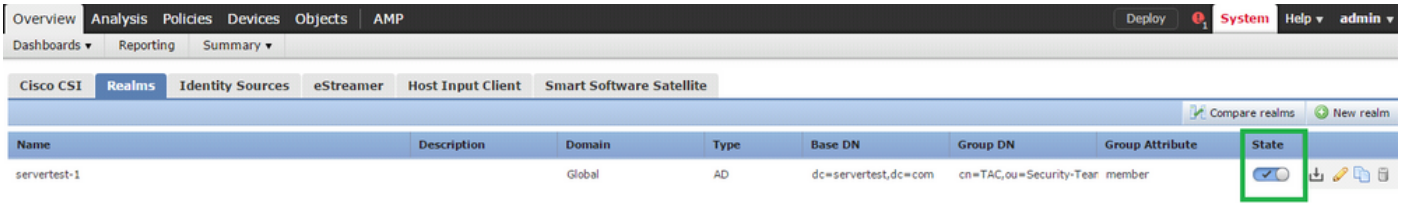
Accédez à l'option Téléchargement utilisateur pour récupérer la base de données utilisateur à partir du serveur AD.

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 FMC contacte AD pour télécharger la base de données utilisateur.

Sélectionnez le groupe et placez-le dans l'option Include pour laquelle vous voulez configurer l'authentification.



Comme l'illustre l'image, activez l'état AD :



Étape 4 : configuration de la stratégie d'identité

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

Étape 4.1 Portail captif (authentification active)

L'authentification active demande un nom d'utilisateur/mot de passe au niveau du navigateur pour identifier une identité utilisateur afin d'autoriser toute connexion. Le navigateur authentifie l'utilisateur avec 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. Les 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 les négocie avec Active Directory via un navigateur Web. Vous devez activer l'authentification NTLM dans le navigateur. L'authentification utilisateur se fait de manière transparente sans invite d'identification. Il offre une expérience d'authentification unique aux utilisateurs.
3. HTTP Negotiate : dans ce type, le système tente de s'authentifier avec NTLM. En cas d'échec, le capteur utilise le type d'authentification HTTP de base comme méthode de

secours et affiche une boîte de dialogue pour les informations d'identification de l'utilisateur.

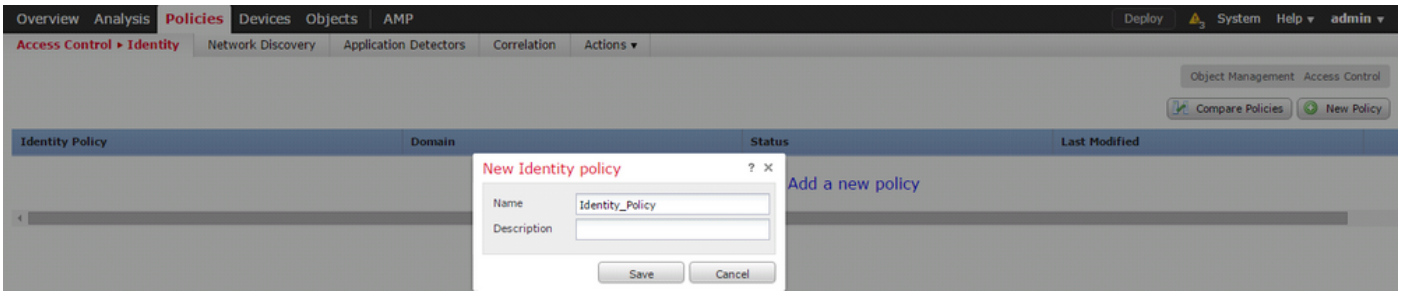
4. Page Réponse HTTP : ce type est similaire au type de base HTTP, mais l'utilisateur est invité à remplir l'authentification dans un formulaire HTML qui peut être personnalisé.

Chaque navigateur dispose d'un moyen spécifique d'activer l'authentification NTLM et, par conséquent, il respecte les consignes du navigateur afin d'activer l'authentification NTLM.

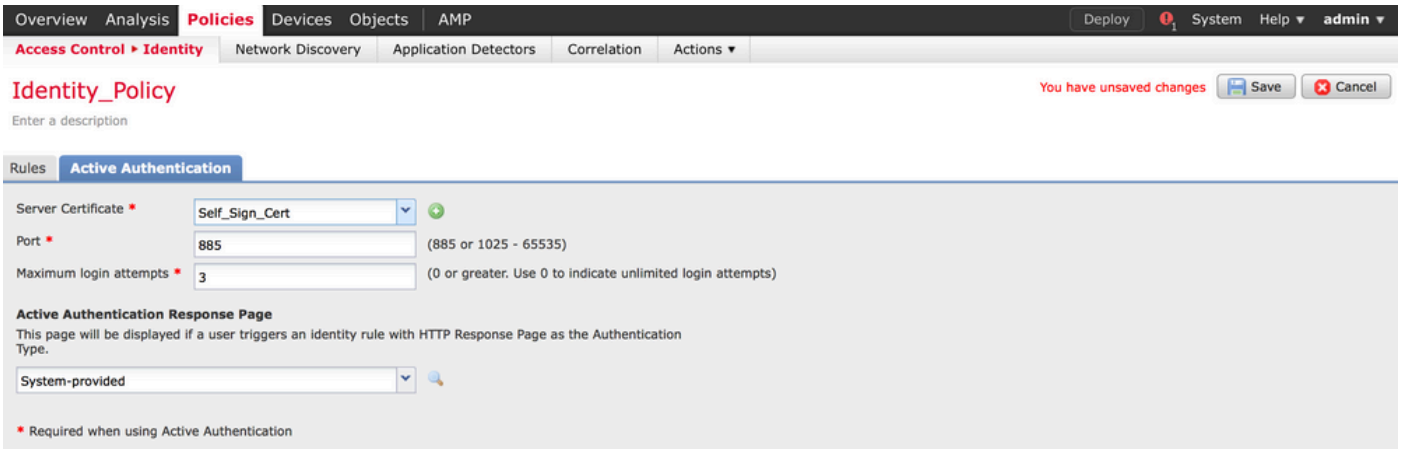
Pour partager de manière sécurisée les informations d'identification avec le capteur routé, vous devez installer un certificat de serveur auto-signé ou un certificat de serveur signé publiquement dans la stratégie d'identité.

```
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 Politiques > Contrôle d'accès > Identité. Cliquez sur Ajouter une stratégie & donnez un nom à la stratégie et enregistrez-la.

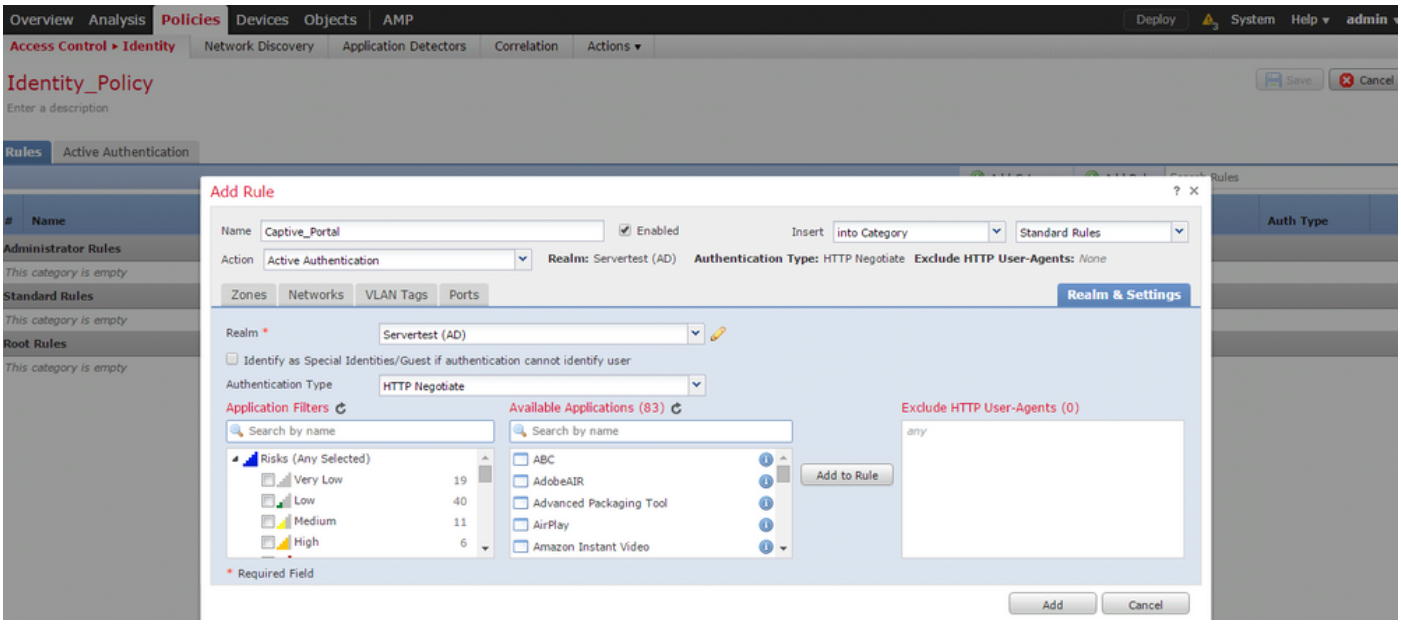


Accédez à l'onglet Active Authentication et dans l'option Server Certificate, cliquez sur l'icône (+) et téléchargez le certificat et la clé privée que vous avez générés à l'étape précédente avec openSSL.



Cliquez maintenant sur le bouton Add rule et donnez un nom à la règle et choisissez l'action comme Active Authentication. Définissez la zone source/destination, le réseau source/destination pour lequel vous souhaitez activer l'authentification de l'utilisateur.

Sélectionnez le domaine, que vous avez configuré à l'étape précédente et le type d'authentification qui convient le mieux à votre environnement.



Configuration ASA pour Captive Portal

Pour le module ASA Firepower, configurez ces commandes sur l'ASA afin de configurer le portail captif.

```
ASA(config)# captive-portal global port 1055
```

Assurez-vous que le port de serveur, TCP 1055, est configuré dans l'option port de l'onglet Identity Policy Active Authentication.

Afin de vérifier les règles actives et leur nombre de succès, exécutez la commande :

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

Remarque : la commande Captive portal est disponible dans ASA version 9.5(2) et ultérieure.

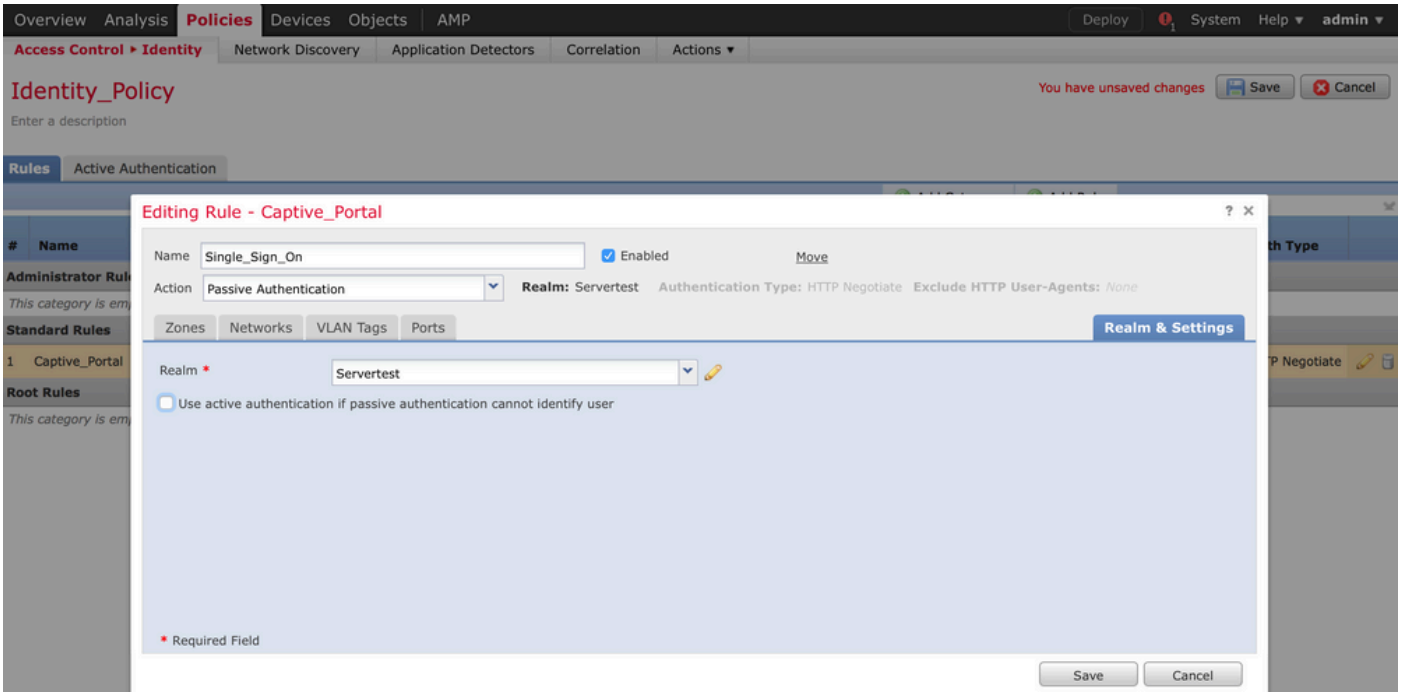
Étape 4.2 Authentification unique (authentification passive)

Dans l'authentification passive, lorsqu'un utilisateur de domaine se connecte et est en mesure d'authentifier AD, l'agent utilisateur Firepower interroge les détails du mappage User-IP à partir des journaux de sécurité d'AD et partage ces informations avec Firepower Management Center (FMC). FMC envoie ces détails au capteur afin d'appliquer le contrôle d'accès.

Cliquez sur le bouton Add rule et donnez un nom à la règle et choisissez l'Action as Passive Authentication. Définissez la zone source/destination, le réseau source/destination pour lequel vous souhaitez activer l'authentification de l'utilisateur.

Sélectionnez le domaine que vous avez configuré à l'étape précédente et le type d'authentification qui correspond le mieux à votre environnement, comme illustré dans cette image.

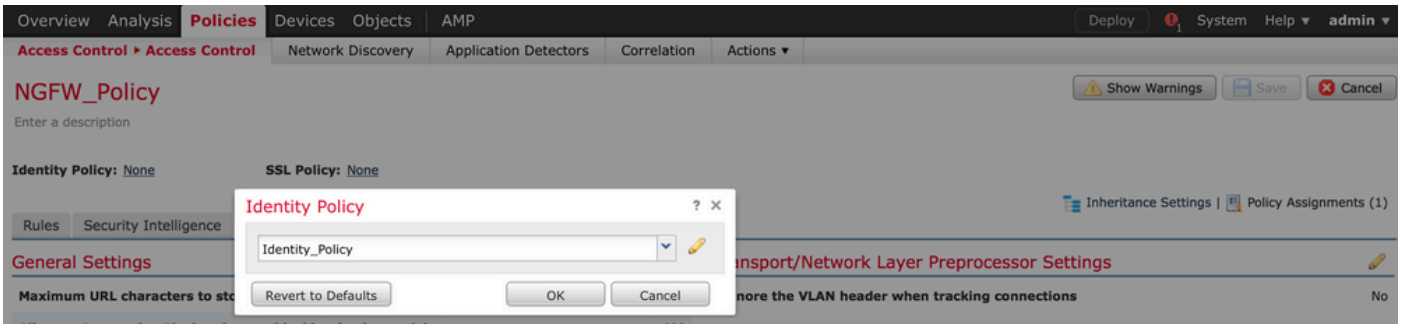
Ici, vous pouvez choisir la méthode de secours comme authentification active si l'authentification passive ne peut pas identifier l'identité de l'utilisateur.



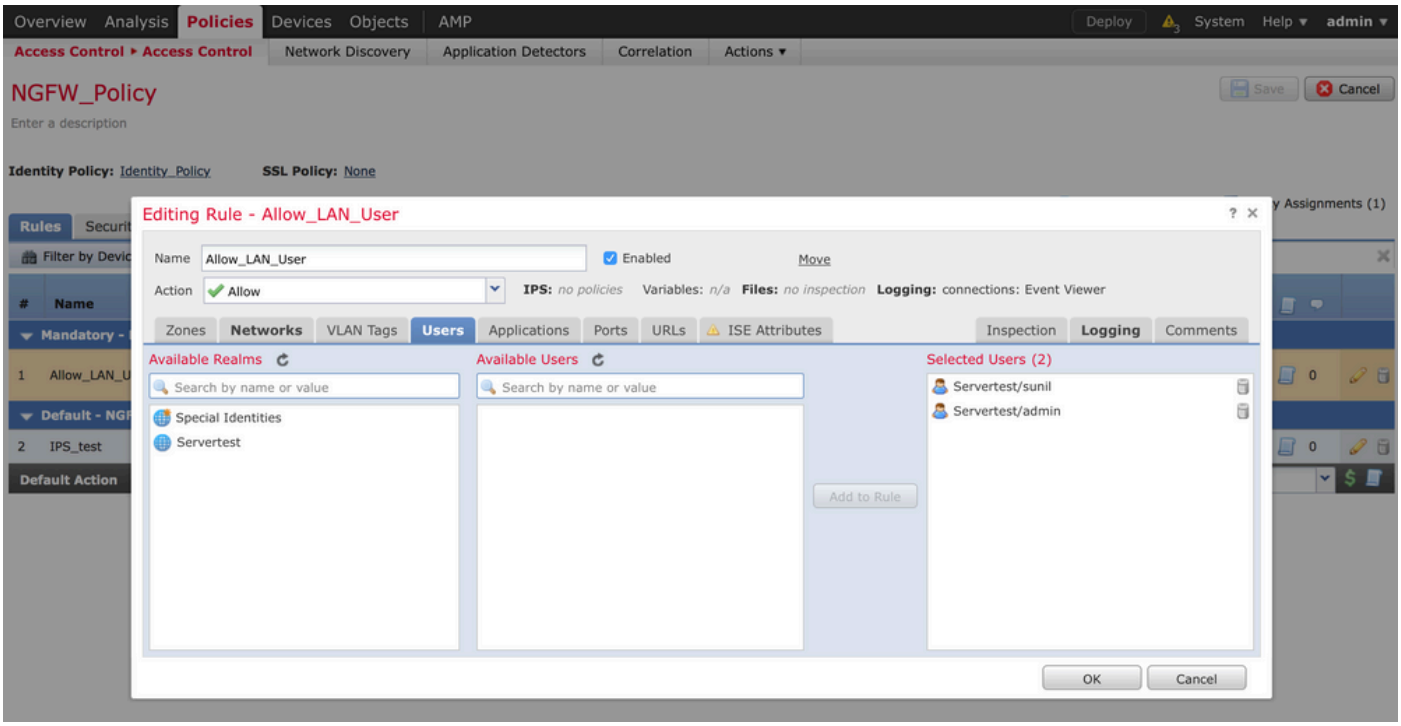
Étape 5. Configuration de la stratégie de contrôle d’accès

Accédez à Policies > Access Control > Create/Edit a Policy.

Cliquez sur la politique d'identité (coin supérieur gauche), choisissez la politique d'identification que vous avez configurée à l'étape précédente et cliquez sur le bouton OK, comme illustré dans cette image.

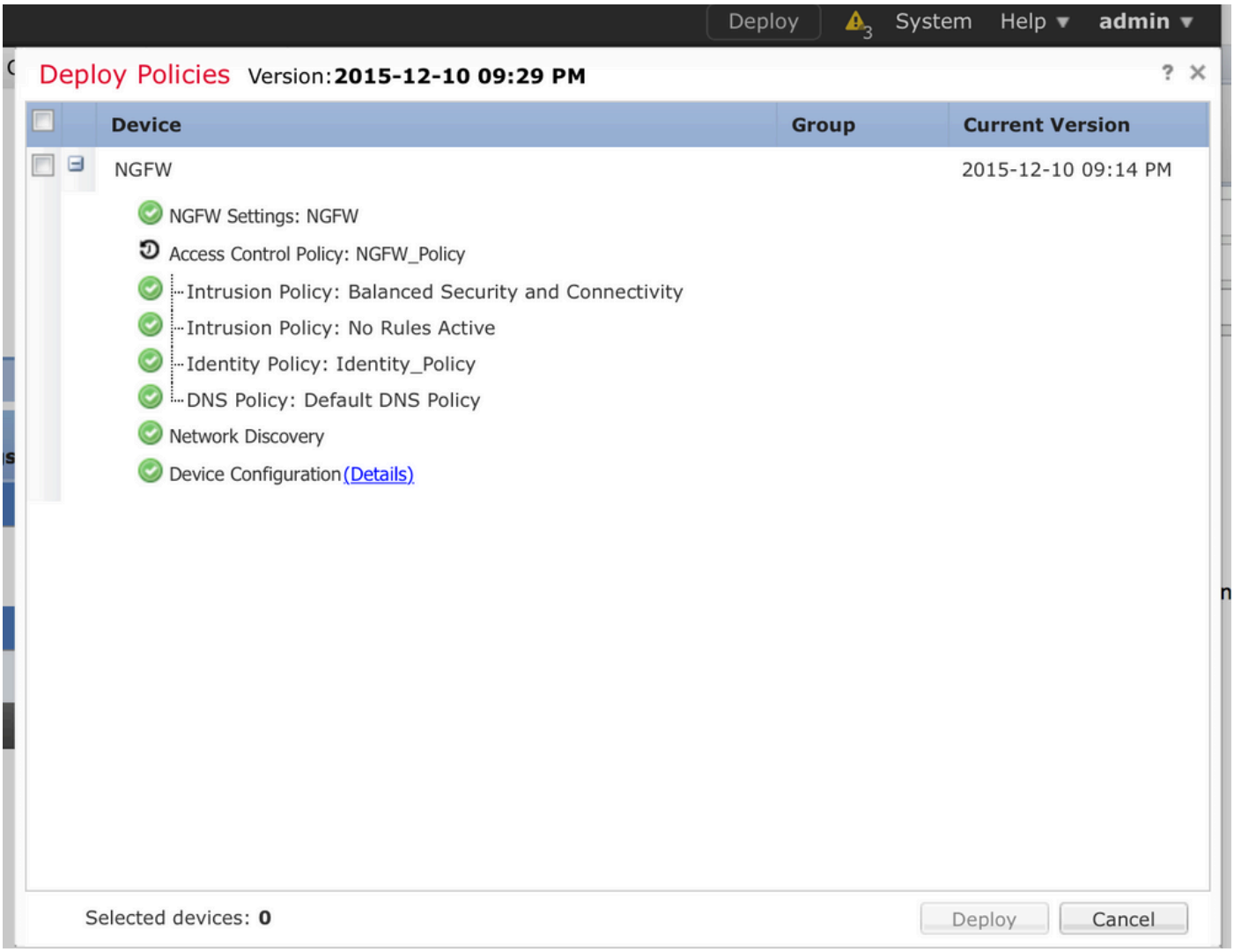


Cliquez sur le bouton Ajouter une règle pour ajouter une nouvelle règle. Accédez à Utilisateurs et sélectionnez les utilisateurs pour lesquels la règle de contrôle d'accès s'applique, comme illustré dans cette image. Cliquez sur OK et cliquez sur Save afin d'enregistrer les modifications.



Étape 6. Déploiement de la stratégie de contrôle d’accès

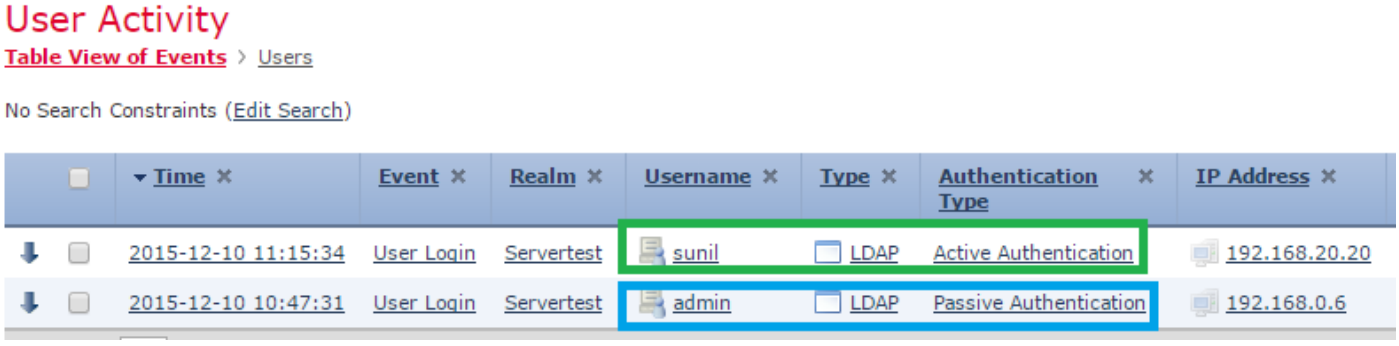
Accédez à l'option Deploy, choisissez le Device et cliquez sur l'option Deploy pour transmettre la modification de configuration au capteur. Surveillez le déploiement de la stratégie à partir de l'option Icône du Centre de messages (icône entre l'option Déployer et Système) et assurez-vous que la stratégie doit s'appliquer correctement, comme illustré dans cette image.



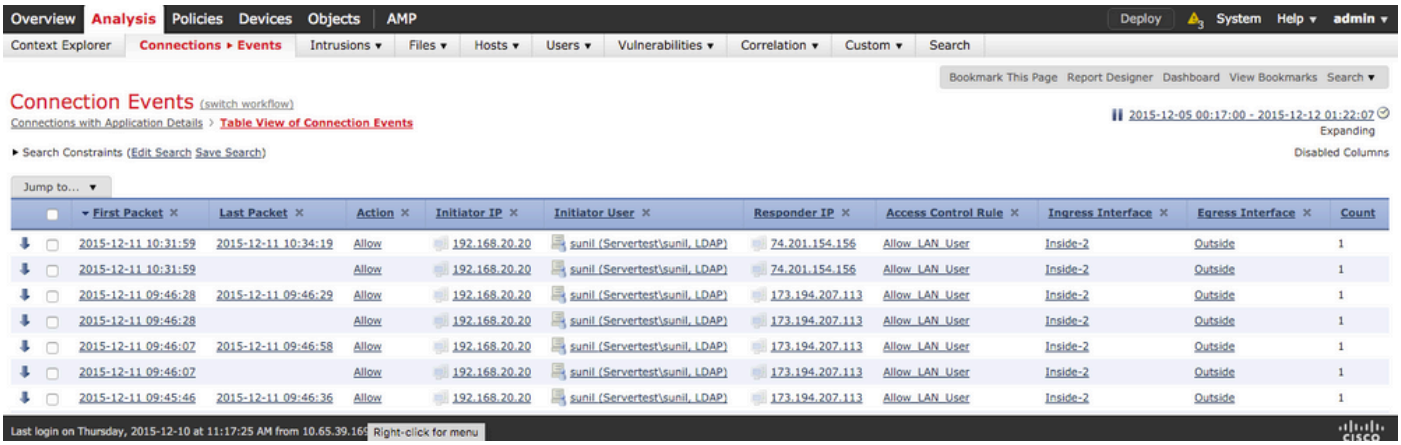
Étape 7. Surveillance des événements utilisateur et des événements de connexion

Les sessions utilisateur actuellement actives sont disponibles dans la section Analysis > Users > Users.

La surveillance de l'activité de l'utilisateur permet de déterminer quel utilisateur a associé à quelle adresse IP et comment l'utilisateur est détecté par le système par authentification active ou passive. Analyse > Utilisateurs > Activité utilisateur



Accédez à Analysis > Connections > Events, pour surveiller le type de trafic qui est utilisé par l'utilisateur.



Vérifiez et dépannez

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

Vérification de la connectivité entre FMC et l'agent utilisateur (authentification passive)

Firepower Management Center (FMC) utilise le port TCP 3306 afin de recevoir les données du journal d'activité utilisateur de l'agent utilisateur.

Afin de vérifier l'état du service FMC, 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
```

Accédez à Analysis > Users > User Activity afin de vérifier si le FMC reçoit les détails de connexion de l'utilisateur de l'agent utilisateur.

Vérification de la connectivité entre FMC et Active Directory

FMC utilise le port TCP 389 afin de récupérer la base de données utilisateur à partir d'Active Directory.

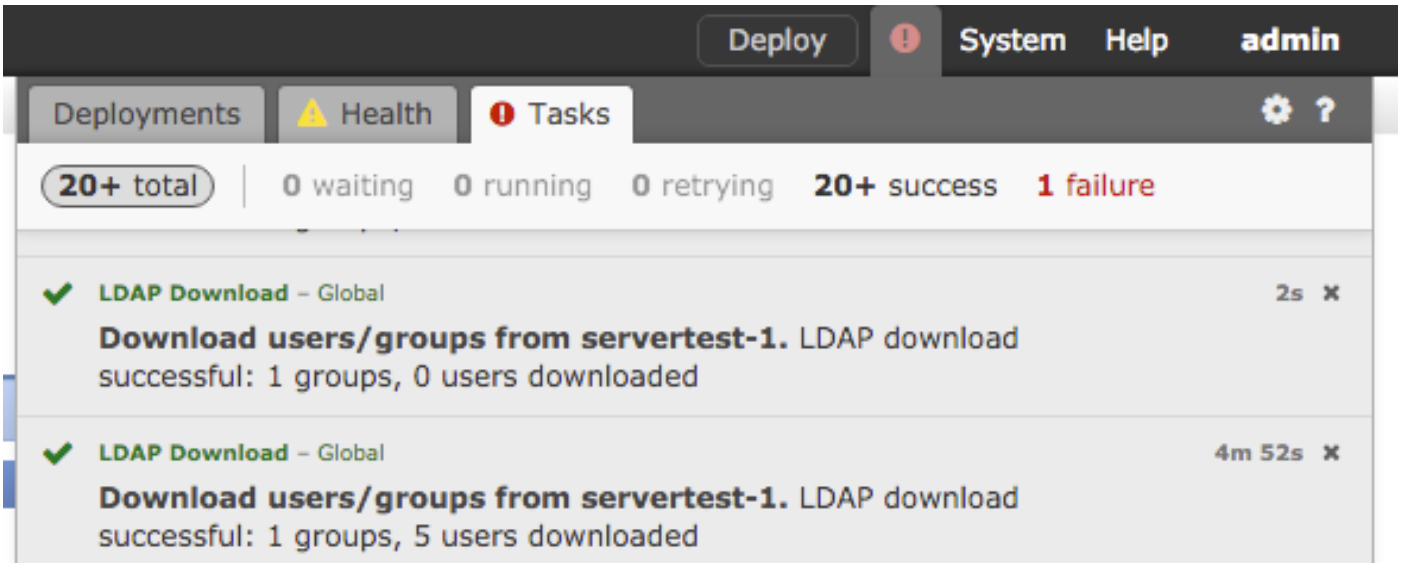
Exécutez la capture de paquets sur le FMC pour vérifier la connectivité avec Active Directory.

```
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 FMC disposent des privilèges suffisants pour extraire la base de données utilisateur AD.

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

Accédez à Centre de messages > Tâches et assurez-vous que la tâche téléchargée par les utilisateurs/groupes se termine correctement , comme illustré dans cette image.



Vérification de la connectivité entre le détecteur Firepower et le système final (authentification active)

Pour l'authentification active, assurez-vous que le certificat et le port sont configurés correctement dans la stratégie d'identité FMC.Par défaut, le capteur Firepower écoute le port TCP 885 pour l'authentification active.

Vérification de la configuration et du déploiement des stratégies

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

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

Accédez à Centre de messages > Tâches et assurez-vous que le déploiement de la stratégie se termine avec succès.

Analyser les journaux des événements

Les événements Connection et User Activity peuvent être utilisés pour diagnostiquer si la connexion de l'utilisateur a réussi ou non.Ces événements

Vous pouvez également vérifier quelle règle de contrôle d'accès est appliquée au flux.

Accédez à Analysis > User pour vérifier les journaux d'événements de l'utilisateur.

Accédez à Analysis > Connection Events pour vérifier les événements de connexion.

Informations connexes

- **Assistance et documentation techniques - Cisco Systems**

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.