ASA 8.3 : Authentification TACACS utilisant ACS 5.X

Contenu

Introduction

Ce document fournit des informations sur la façon dont configurer les dispositifs de sécurité pour authentifier des utilisateurs pour l'accès au réseau.

Conditions préalables

Conditions requises

Ce document suppose que l'appliance de sécurité adaptable (ASA) est complètement opérationnelle et configurée pour permettre au Cisco Adaptive Security Device Manager (ASDM) ou au CLI pour apporter des modifications de configuration.

Remarque: Référez-vous à permettre HTTPS Access pour l'ASDM pour plus d'informations sur la façon permettre le périphérique à configurer à distance par l'ASDM.

Composants utilisés

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

- Version de logiciel 8.3 d'appliance de sécurité adaptable Cisco et plus tard
- Version 6.3 et ultérieures de Cisco Adaptive Security Device Manager
- Cisco Secure Access Control Server 5.x

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Remarque: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

Configurez l'ASA pour l'authentification du serveur ACS utilisant le CLI

Exécutez ces configurations pour l'ASA pour authentifier du serveur ACS :

```
!--- configuring the ASA for TACACS server ASA(config)# aaa-server cisco protocol tacacs+
ASA(config-aaa-server-group)# exit !--- Define the host and the interface the ACS server is on.
ASA(config)# aaa-server cisco (DMZ) host 192.168.165.29 ASA(config-aaa-server-host)# key cisco
!--- Configuring the ASA for HTTP and SSH access using ACS and fallback method as LOCAL
authentication. ASA(config)#aaa authentication ssh console cisco LOCAL ASA(config)#aaa
authentication http console cisco LOCAL
```

Remarque: Créez un utilisateur local sur l'ASA utilisant la commande du privilège 15 de mot de passe cisco de Cisco de nom d'utilisateur d'accéder à l'ASDM avec l'authentification locale quand l'ACS n'est pas disponible.

Configurez l'ASA pour l'authentification du serveur ACS utilisant l'ASDM

Procédure ASDM

Terminez-vous ces étapes afin de configurer l'ASA pour l'authentification du serveur ACS :

1. Choisissez la **configuration > la Gestion de périphériques > l'Users/AAA > les Groupes de serveurs AAA > ajoutent** afin de créer un **Groupe de serveurs AAA**.
2. Fournissez les petits groupes de **Groupe de serveurs AAA** dans la fenêtre de **Groupe de serveurs AAA d'ajouter** comme affichée. Le protocole utilisé est **TACACS+** et le groupe de serveurs créé est **Cisco**.Cliquez sur **OK**.
3. Choisissez la **configuration > la Gestion de périphériques > l'Users/AAA > les Groupes de serveurs AAA** et cliquez sur Add sous des **serveurs au groupe sélectionné** afin d'ajouter le serveur d'AAA.
4. Fournissez les petits groupes de **serveur d'AAA** dans la fenêtre de **serveur d'AAA d'ajouter** comme affichée. Le groupe de serveurs utilisé est **Cisco**.Cliquez sur OK, puis cliquez sur Apply.Vous verrez le **Groupe de serveurs AAA** et le **serveur d'AAA** configurés sur l'ASA.
5. Cliquez sur **Apply**.
6. Choisissez le **Configuration > Device Management > Users/AAA > AAA Access > Authentication** et cliquez sur les cases à côté de **HTTP/ASDM** et de **SSH**. Puis, choisissez **Cisco** en tant que groupe de serveurs et cliquez sur Apply.

Configurez ACS en tant que serveur TACACS

Remplissez cette procédure afin de configurer l'ACS en tant que serveur TACACS :

1. Choisissez les **ressources de réseau > les périphériques de réseau et les clients** et le clic d'**AAA créent** afin d'ajouter l'ASA au serveur ACS.
2. Fournissez l'information requise au sujet du **client** (l'ASA est le client ici) et cliquez sur Submit. Cet enablesthe ASA à obtenir a ajouté au serveur ACS. Les détails incluent l'**adresse IP de l'**ASA et des petits groupes de **serveur TACACS**.Vous verrez le client **Cisco** étant ajouté au serveur ACS.
3. Choisissez les **utilisateurs et l'identité enregistre > identité interne enregistre > des utilisateurs** et le clic **créent** afin de créer un nouvel utilisateur.
4. Fournissez le **nom, le mot de passe, et les** informations de **mot de passe d'enable**. **Le mot de passe d'enable** est **facultatif**. Quand vous terminez, cliquez sur Submit.Vous verrez l'utilisateur **Cisco** étant ajouté au serveur ACS.

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Utilisez la commande de **mot de passe cisco de Cisco de nom d'utilisateur de 192.168.165.29 d'hôte de Cisco d'authentification d'AAA-serveur** thetest de vérifier si la configuration fonctionne correctement. Cette image prouve que l'authentification est réussie et l'utilisateur connecté à l'ASA a été authentifié par le serveur ACS.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Dépannez

Erreur : AAA marquant le serveur x.x.x.x TACACS+ dans des tacacs de Groupe de

serveurs AAA comme MANQUÉS

Ce message signifie que ce Cisco ASA a perdu la Connectivité avec le serveur x.x.x.x. Veillez-vous pour avoir une Connectivité valide sur le TCP 49 au serveur x.x.x.x de l'ASA. Vous pouvez également augmenter le délai d'attente sur l'ASA pour le serveur TACACS+ de 5 au nombre désiré de secondes au cas où il y aurait une latence de réseau. L'ASA n'enverrait pas une demande d'authentification au serveur défaillant x.x.x.x. Cependant, il utilisera le prochain serveur dans les tacacs de Groupe de serveurs AAA.

Informations connexes

- Page d'assistance des appliances de sécurité adaptables de la gamme Cisco ASA 5500
- Références de commandes de Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500
- Cisco Adaptive Security Device Manager
- Page de support de la négociation IPSec/des protocoles IKE
- Cisco Secure Access Control Server pour Windows
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems