Utilisation du serveur de jeton RSA et du protocole SDI pour ASA et ACS

Contenu

Introduction

Ce document décrit les procédures de dépannage de RSA Authentication Manager, qui peuvent être intégrées à Cisco Adaptive Security Appliance (ASA) et à Cisco Secure Access Control Server (ACS).

RSA Authentication Manager est une solution qui fournit le mot de passe OTP (One Time Password) pour l'authentification. Ce mot de passe est modifié toutes les 60 secondes et ne peut être utilisé qu'une seule fois. Il prend en charge les jetons matériels et logiciels.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration CLI de Cisco ASA
- Configuration de Cisco ACS

Components Used

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

- Logiciel Cisco ASA, versions 8.4 et ultérieures
- Cisco Secure ACS, versions 5.3 et ultérieures

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.

Théorie

Le serveur RSA est accessible via RADIUS ou le protocole RSA propriétaire : SDI. L'ASA et l'ACS peuvent utiliser les deux protocoles (RADIUS, SDI) afin d'accéder au RSA.

N'oubliez pas que le RSA peut être intégré au client Cisco AnyConnect Secure Mobility lorsqu'un jeton logiciel est utilisé. Ce document se concentre uniquement sur l'intégration ASA et ACS. Pour plus d'informations sur AnyConnect, reportez-vous à la section Utilisation de l'authentification SDI du Guide d'administration du client Cisco AnyConnect Secure Mobility, version 3.1.

RSA via RADIUS

RADIUS a un grand avantage sur SDI. Sur le RSA, il est possible d'attribuer des profils spécifiques (appelés groupes sur ACS) aux utilisateurs. Ces profils ont des attributs RADIUS spécifiques définis. Après une authentification réussie, le message RADIUS-Accepcept renvoyé par le RSA contient ces attributs. En fonction de ces attributs, l'ACS prend des décisions supplémentaires. Le scénario le plus courant est la décision d'utiliser le mappage de groupe ACS afin de mapper des attributs RADIUS spécifiques, liés au profil sur le RSA, à un groupe spécifique sur l'ACS. Avec cette logique, il est possible de déplacer l'ensemble du processus d'autorisation du RSA vers l'ACS tout en conservant une logique granulaire, comme sur le RSA.

RSA via SDI

SDI présente deux avantages principaux par rapport à RADIUS. La première est que toute la session est chiffrée. La deuxième est l'option intéressante que l'agent SDI propose : il peut déterminer si l'échec est créé en raison d'un échec de l'authentification ou de l'autorisation ou parce que l'utilisateur est introuvable.

Ces informations sont utilisées par l'ACS en action pour l'identité. Par exemple, il peut continuer pour « utilisateur introuvable » mais rejeter pour « échec de l'authentification ».

Il y a une autre différence entre RADIUS et SDI. Lorsqu'un périphérique d'accès au réseau tel qu'ASA utilise SDI, ACS effectue uniquement l'authentification. Lorsqu'il utilise RADIUS, ACS effectue l'authentification, l'autorisation et la comptabilité (AAA). Cependant, ce n'est pas une grande différence. Il est possible de configurer SDI pour l'authentification et RADIUS pour la comptabilisation des mêmes sessions.

Protocole SDI

Par défaut, SDI utilise le protocole UDP (User Datagram Protocol) 5500. SDI utilise une clé de chiffrement symétrique, similaire à la clé RADIUS, afin de chiffrer les sessions. Cette clé est enregistrée dans un fichier secret de noeud et est différente pour chaque client SDI. Ce fichier est déployé manuellement ou automatiquement.

> **Note**: ACS/ASA ne prend pas en charge le déploiement manuel.

Pour le noeud de déploiement automatique, le fichier secret est téléchargé automatiquement après la première authentification réussie. Le secret de noeud est chiffré avec une clé dérivée du code secret de l'utilisateur et d'autres informations. Cela crée des problèmes de sécurité possibles, de sorte que la première authentification doit être effectuée localement et utiliser le protocole chiffré (Secure Shell [SSH], et non telnet) afin de s'assurer que l'attaquant ne peut pas intercepter et déchiffrer ce fichier.

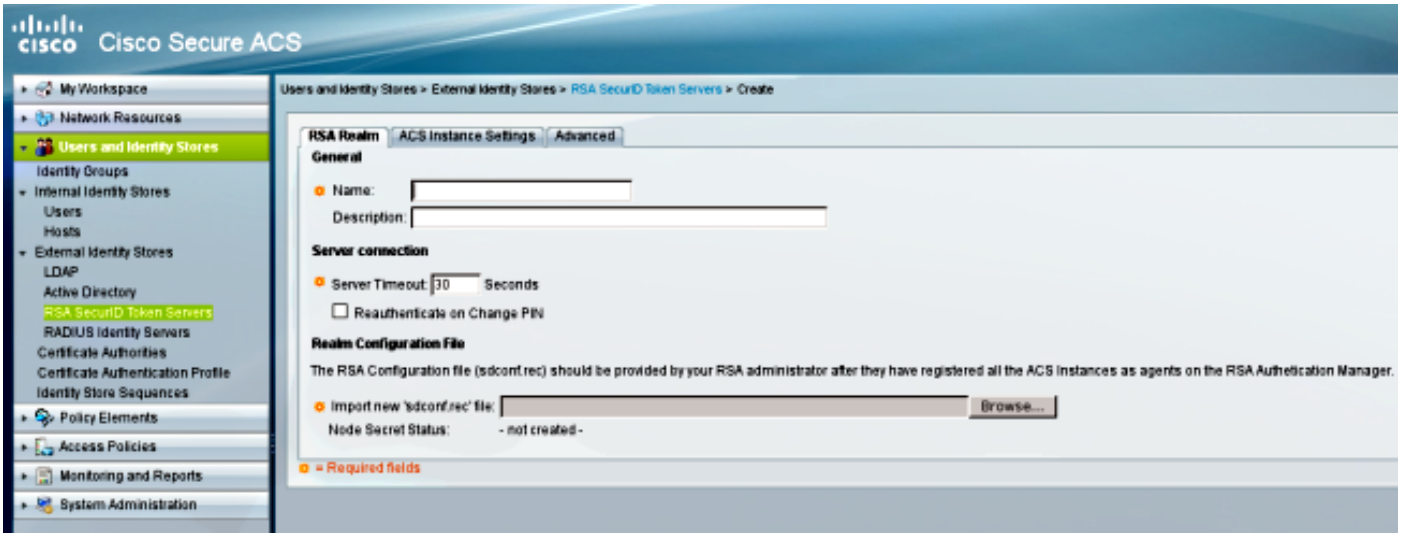
Configuration

> **Remarques :**
>
> Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.
>
> L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .
>
> Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage.

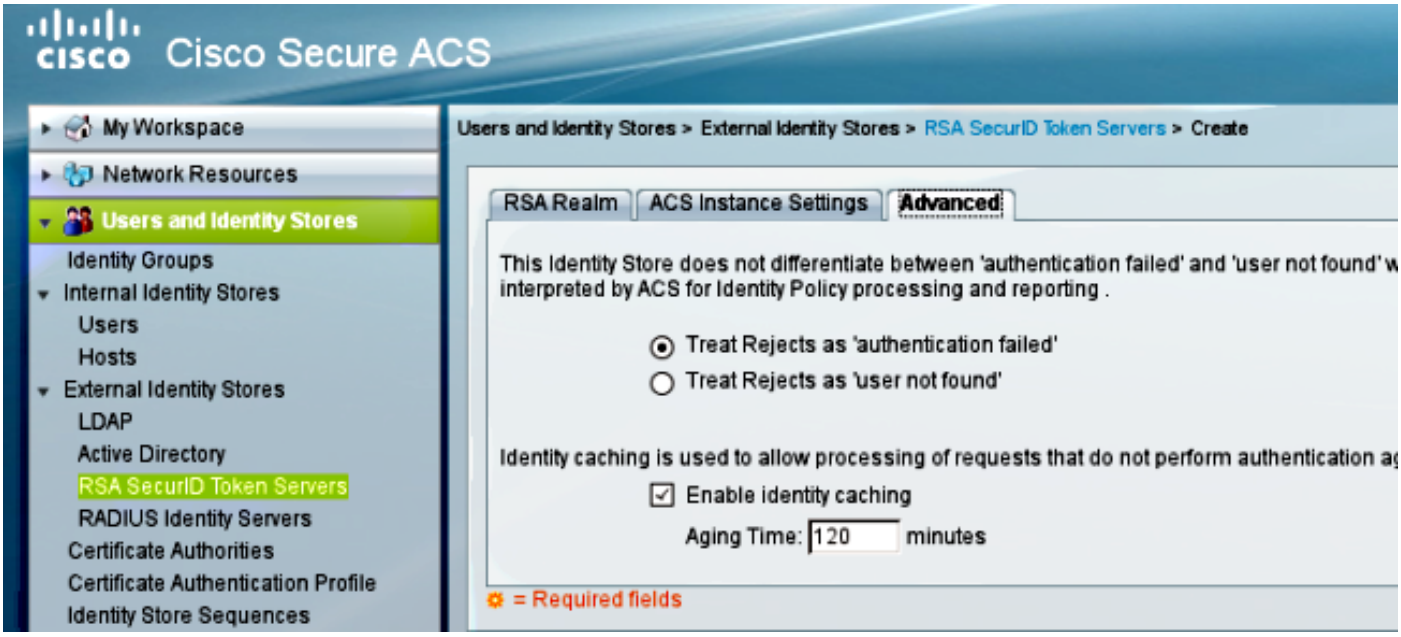
SDI sur ACS

Il est configuré dans **Utilisateurs et magasins d'identités > Banque d'identités externe > Serveurs de jetons RSA Secure ID**.

Le RSA dispose de plusieurs serveurs de réplication, tels que les serveurs secondaires pour l'ACS. Il n'est pas nécessaire d'y placer toutes les adresses, juste le fichier **sdconf.rec** fourni par l'administrateur RSA. Ce fichier inclut l'adresse IP du serveur RSA principal. Après le premier noeud d'authentification réussi, le fichier secret est téléchargé avec les adresses IP de tous les réplicas RSA.



Afin de différencier « utilisateur introuvable » de « échec d'authentification », choisissez les paramètres dans l'onglet **Avancé** :



Il est également possible de modifier les mécanismes de routage par défaut (équilibrage de charge) entre plusieurs serveurs RSA (réplication principale et réplication). Modifiez-le avec le fichier **sdopts.rec** fourni par l'administrateur RSA. Dans ACS, il est téléchargé dans **Utilisateurs et magasins d'identité > Banque d'identité externe > Serveurs de jetons RSA Secure ID > Paramètres d'instance ACS**.

Pour le déploiement de cluster, la configuration doit être répliquée. Après la première authentification réussie, chaque noeud ACS utilise son propre secret de noeud téléchargé à partir du serveur RSA principal. Il est important de ne pas oublier de configurer RSA pour tous les noeuds ACS du cluster.

SDI sur ASA

L'ASA n'autorise pas le téléchargement du fichier **sdconf.rec**. Et, comme l'ACS, il ne permet que le déploiement automatique. L'ASA doit être configuré manuellement pour pointer vers le serveur RSA principal. Aucun mot de passe n'est nécessaire. Après le premier noeud d'authentification réussi, le fichier secret est installé (.sdi file on flash) et les sessions d'authentification

supplémentaires sont protégées. L'adresse IP des autres serveurs RSA est également téléchargée.

Voici un exemple :

```
aaa-server SDI protocol sdi
aaa-server SDI (backbone) host 1.1.1.1
debug sdi 255
test aaa auth SDI host 1.1.1.1 user test pass 321321321
```

Après une authentification réussie, la commande **show aaa-server protocol sdi** ou **show aaa-server <aaa-server-group>** affiche tous les serveurs RSA (s'il y en a plus d'un), tandis que la commande **show run** affiche uniquement l'adresse IP principale :

```
bsns-asa5510-17# show aaa-server RSA
Server Group:    RSA
Server Protocol: sdi
Server Address:  10.0.0.101
Server port:     5500
Server status:   ACTIVE (admin initiated), Last transaction at
10:13:55 UTC Sat Jul 27 2013
Number of pending requests              0
Average round trip time                 706ms
Number of authentication requests       4
Number of authorization requests        0
Number of accounting requests           0
Number of retransmissions               0
Number of accepts                       1
Number of rejects                       3
Number of challenges                    0
Number of malformed responses           0
Number of bad authenticators            0
Number of timeouts                      0
Number of unrecognized responses        0


SDI Server List:
       Active Address:          10.0.0.101
       Server Address:          10.0.0.101
       Server port:             5500
       Priority:                0
       Proximity:               2
        Status:                  OK
       Number of accepts                     0
       Number of rejects                     0
       Number of bad next token codes        0
       Number of bad new pins sent           0
       Number of retries                     0
       Number of timeouts                    0

       Active Address:          10.0.0.102
       Server Address:          10.0.0.102
       Server port:             5500
       Priority:                8
       Proximity:               2
        Status:                  OK
       Number of accepts                     1
       Number of rejects                     0
       Number of bad next token codes        0
       Number of bad new pins sent           0
```

```
        Number of retries                       0
        Number of timeouts                      0
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Aucune configuration d'agent sur RSA

Dans de nombreux cas, après avoir installé un nouvel ASA ou modifié l'adresse IP ASA, il est facile d'oublier d'effectuer les mêmes modifications sur le RSA. L'adresse IP de l'agent sur le RSA doit être mise à jour pour tous les clients qui accèdent au RSA. Ensuite, le nouveau secret de noeud est généré. Il en va de même pour ACS, en particulier pour les noeuds secondaires, car ils ont des adresses IP différentes et le RSA doit leur faire confiance.

Noeud secret endommagé

Parfois, le fichier de noeud secret sur l'ASA ou le RSA devient endommagé. Ensuite, il est préférable de supprimer la configuration de l'agent sur le RSA et de l'ajouter à nouveau. Vous devez également effectuer le même processus sur l'ASA/ACS - supprimer et ajouter à nouveau la configuration. Supprimez également le fichier .sdi sur la mémoire Flash, de sorte que dans l'authentification suivante, un nouveau fichier .sdi soit installé. Le déploiement automatique du secret de noeud doit avoir lieu une fois cette opération terminée.

Noeud en mode Suspendu

Parfois, un des noeuds est en mode suspendu, ce qui est dû à l'absence de réponse de ce serveur :

```
asa# show aaa-server RSA
<.....output ommited"
SDI Server List:
Active Address: 10.0.0.101
Server Address: 10.0.0.101
Server port: 5500
Priority: 0
Proximity: 2
  Status:                  SUSPENDED
```

En mode suspendu, l'ASA n'essaie pas d'envoyer des paquets à ce noeud ; il doit avoir un statut **OK** pour cela. Le serveur défaillant est replacé en mode actif après le compteur d'arrêt. Pour plus d'informations, reportez-vous à la section reactivation-mode command du Guide de référence des commandes de la gamme Cisco ASA, 9.1.

Dans de tels scénarios, il est préférable de supprimer et d'ajouter la configuration AAA-server pour ce groupe afin de déclencher à nouveau ce serveur en mode actif.

Compte verrouillé

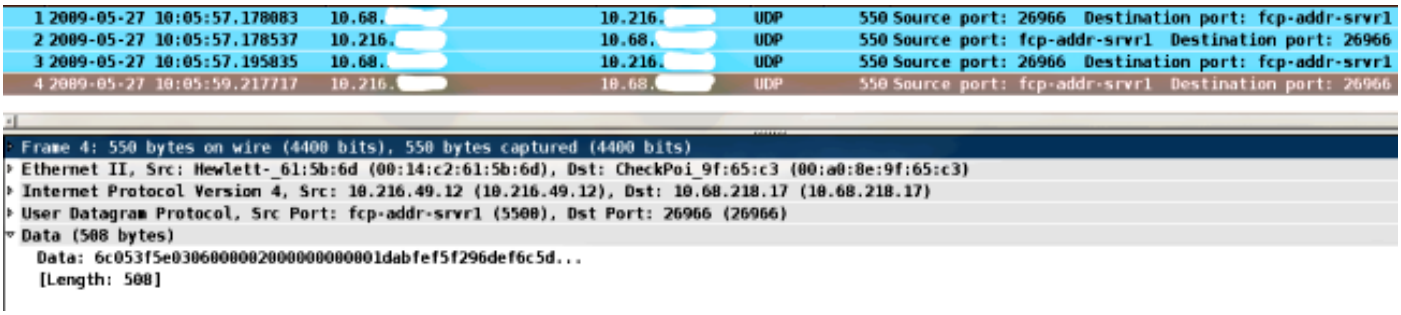
Après plusieurs tentatives, le RSA peut verrouiller le compte. Il est facilement vérifié sur le RSA avec des rapports. Sur l'ASA/ACS, les rapports indiquent uniquement « échec de l'authentification ».

Problèmes liés à l'unité de transition maximale (MTU) et fragmentation

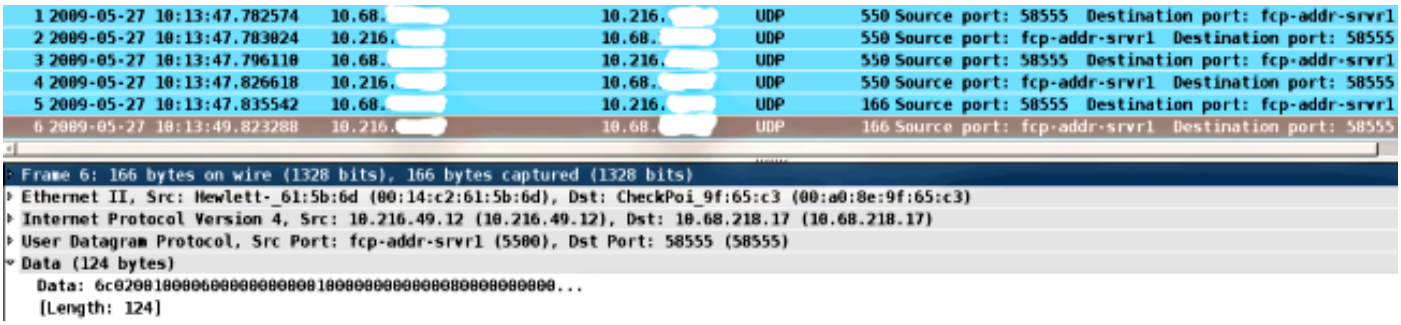
SDI utilise le protocole UDP comme transport et non comme détection de chemin MTU. De même, le bit DF (Don't Fragment) n'est pas défini par défaut sur le trafic UDP. Parfois, pour les paquets plus volumineux, il peut y avoir des problèmes de fragmentation. Il est facile de détecter le trafic sur le RSA (l'appliance et la machine virtuelle [VM] utilisent Windows et Wireshark). Effectuez le même processus sur l'ASA/ACS et comparez. En outre, testez RADIUS ou WebAuthentication sur le RSA afin de le comparer à SDI (afin de réduire le problème).

Paquets et débogages pour ACS

Comme la charge utile SDI est chiffrée, la seule façon de dépanner les captures est de comparer la taille de la réponse. S'il est inférieur à 200 octets, il peut y avoir un problème. Un échange SDI type implique quatre paquets, chacun d'entre eux étant de 550 octets, mais cela peut changer avec la version du serveur RSA :



En cas de problème, il s'agit généralement de plus de quatre paquets échangés et de plus petites tailles :



En outre, les journaux ACS sont assez clairs. Voici des journaux SDI typiques sur ACS :

```
EventHandler,11/03/2013,13:47:58:416,DEBUG,3050957712,Stack: 0xa3de560
Calling backRSAIDStore: Method MethodCaller<RSAIDStore, RSAAgentEvent> in
thread:3050957712,EventStack.cpp:242

AuthenSessionState,11/03/2013,13:47:58:416,DEBUG,3050957712,cntx=0000146144,
sesn=acs-01/150591921/1587,user=mickey.mouse,[RSACheckPasscodeState
::onEnterState],RSACheckPasscodeState.cpp:23
```

```
EventHandler,11/03/2013,13:47:58:416,DEBUG,3002137488,Stack: 0xa3de560
Calling RSAAgent:Method MethodCaller<RSAAgent, RSAAgentEvent> in thread:
3002137488,EventStack.cpp:204

RSAAgent,11/03/2013,13:47:58:416,DEBUG,3002137488,cntx=0000146144,sesn=
acs-01/150591921/1587,user=mickey.mouse,[RSAAgent::handleCheckPasscode],
RSAAgent.cpp:319

RSASessionHandler,11/03/2013,13:47:58:416,DEBUG,3002137488,[RSASessionHandler::
checkPasscode] call AceCheck,RSASessionHandler.cpp:251

EventHandler,11/03/2013,13:48:00:417,DEBUG,2965347216,Stack: 0xc14bba0
Create newstack, EventStack.cpp:27

EventHandler,11/03/2013,13:48:00:417,DEBUG,3002137488,Stack: 0xc14bba0 Calling
RSAAgent: Method MethodCaller<RSAAgent, RSAServerResponseEvent> in
thread:3002137488,EventStack.cpp:204

RSAAgent,11/03/2013,13:48:00:417,DEBUG,3002137488,cntx=0000146144,sesn=acs-01
/150591921/1587,user=mickey.mouse,[RSAAgent::handleResponse] operation completed
with ACM_OKstatus,RSAAgent.cpp:237

EventHandler,11/03/2013,13:48:00:417,DEBUG,3002137488,Stack: 0xc14bba0
EventStack.cpp:37

EventHandler,11/03/2013,13:48:00:417,DEBUG,3049905040,Stack: 0xa3de560 Calling
back RSAIDStore: Method MethodCaller<RSAIDStore, RSAAgentEvent> in thread:
3049905040,EventStack.cpp:242

AuthenSessionState,11/03/2013,13:48:00:417,DEBUG,3049905040,cntx=0000146144,sesn=
acs-01/150591921/1587,user=mickey.mouse,[RSACheckPasscodeState::onRSAAgentResponse]
Checkpasscode succeeded, Authentication passed,RSACheckPasscodeState.cpp:55
```

Informations connexes

- Ressources de RSA Authentication Manager
- Section Support serveur RSA/SDI du Guide de configuration de la gamme Cisco ASA 5500 à l'aide de l'interface de ligne de commande, des versions 8.4 et 8.6
- Section RSA SecurID Server du Guide de l'utilisateur de Cisco Secure Access Control System 5.4
- Support et documentation techniques - Cisco Systems