Serveur de jetons RSA et utilisation de Protocol de SDI pour l'ASA et l'ACS

Contenu

Introduction

Ce document décrit des procédures de dépannage pour le gestionnaire d'authentification RSA, qui peut être intégré avec l'appliance de sécurité adaptable Cisco (ASA) et le Cisco Secure Access Control Server (ACS).

Le gestionnaire d'authentification RSA est une solution qui fournit l'un mot de passe de temps (OTP) pour l'authentification. Que le mot de passe est changé toutes les 60 secondes et peut être utilisé seulement une fois. Il prend en charge des jetons de matériel et de logiciel.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de Cisco ASA CLI
- Configuration de Cisco ACS

Composants utilisés

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

- Logiciel de Cisco ASA, version 8.4 et ultérieures
- Cisco Secure ACS, version 5.3 et ultérieures

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.

Théorie

Le serveur RSA peut être accédé à avec le RAYON ou le protocole de propriété industrielle RSA : SDI. L'ASA et l'ACS peuvent employer les deux protocoles (RAYON, SDI) afin d'accéder à la RSA.

Souvenez-vous que la RSA peut être intégrée avec le Client à mobilité sécurisé Cisco AnyConnect quand un jeton de logiciel est utilisé. Ce document se concentre seulement sur l'intégration ASA et ACS. Pour plus d'informations sur AnyConnect, référez-vous à la section de utilisation d'authentification de SDI du guide de l'administrateur de Client à mobilité sécurisé Cisco AnyConnect, version 3.1.

RSA par l'intermédiaire du RAYON

Le RAYON a un grand avantage par rapport au SDI. Sur la RSA, il est possible d'assigner des profils spécifiques (appelés des groupes sur ACS) aux utilisateurs. Ces profils ont des attributs RADIUS spécifiques définis. Après l'authentification réussie, le message de Rayon-recevoir retourné de la RSA contient ces attributs. Basé sur ces attributs, l'ACS prend des décisions supplémentaires. Le scénario le plus commun est la décision d'employer le mappage de groupe ACS afin de tracer des attributs RADIUS spécifiques, liés au profil sur la RSA, à un groupe spécifique sur l'ACS. Avec cette logique, il est possible de déplacer le processus entier d'autorisation de la RSA à l'ACS et de mettre à jour toujours la logique granulaire, comme sur la RSA.

RSA par l'intermédiaire de SDI

Le SDI a deux avantages principaux par rapport au RAYON. Le premier est que la session entière est chiffrée. Le deuxième est les options intéressantes que l'agent de SDI fournit : il peut déterminer si la panne est créée parce que l'authentification ou l'autorisation a manqué ou parce que l'utilisateur n'a pas été trouvé.

Ces informations sont utilisées par l'ACS dans l'action pour l'identité. Par exemple, il pourrait continuer pour le « utilisateur non trouvé » mais l'anomalie pour le « échec de l'authentification. »

Il y a une plus de différence entre le RAYON et le SDI. Quand un périphérique d'accès au réseau comme l'ASA utilise le SDI, l'ACS exécute seulement l'authentification. Quand il utilise le RAYON, l'ACS exécute l'authentification, autorisation, rendant compte (AAA). Cependant, ce n'est pas une grande différence. Il est possible de configurer le SDI pour l'authentification et le RAYON pour expliquer les mêmes sessions.

SDI Protocol

Par défaut, le SDI utilise le Protocole UDP (User Datagram Protocol) 5500. Le SDI utilise une clé de chiffrement symétrique, semblable à la clé de RAYON, afin de chiffrer des sessions. Que la clé est enregistrée dans un fichier secret de noeud et est différente pour chaque client de SDI. Ce fichier est déployé manuellement ou automatiquement.

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

Pour le noeud automatique de déploiement, le fichier secret est téléchargé automatiquement après la première authentification réussie. Le secret de noeud est chiffré avec une clé dérivée d'autres informations de l'utilisateur du code de passage et. Ceci crée quelques problèmes de sécurité possibles, ainsi la première authentification devrait être exécutée localement et protocole chiffré par utilisation (sécurisez le shell [SSH], pas le telnet) afin de s'assurer que l'attaquant ne peut pas intercepter et déchiffrer ce fichier.

Configuration

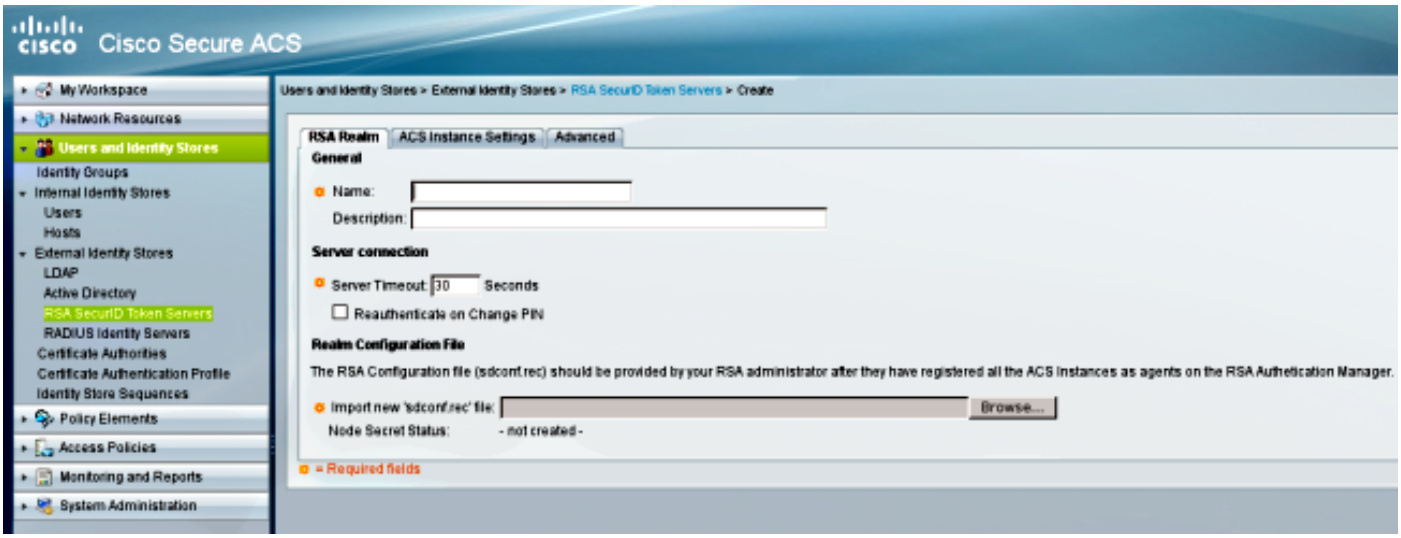
> Remarques :
>
> Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.
>
> L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter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

SDI sur ACS

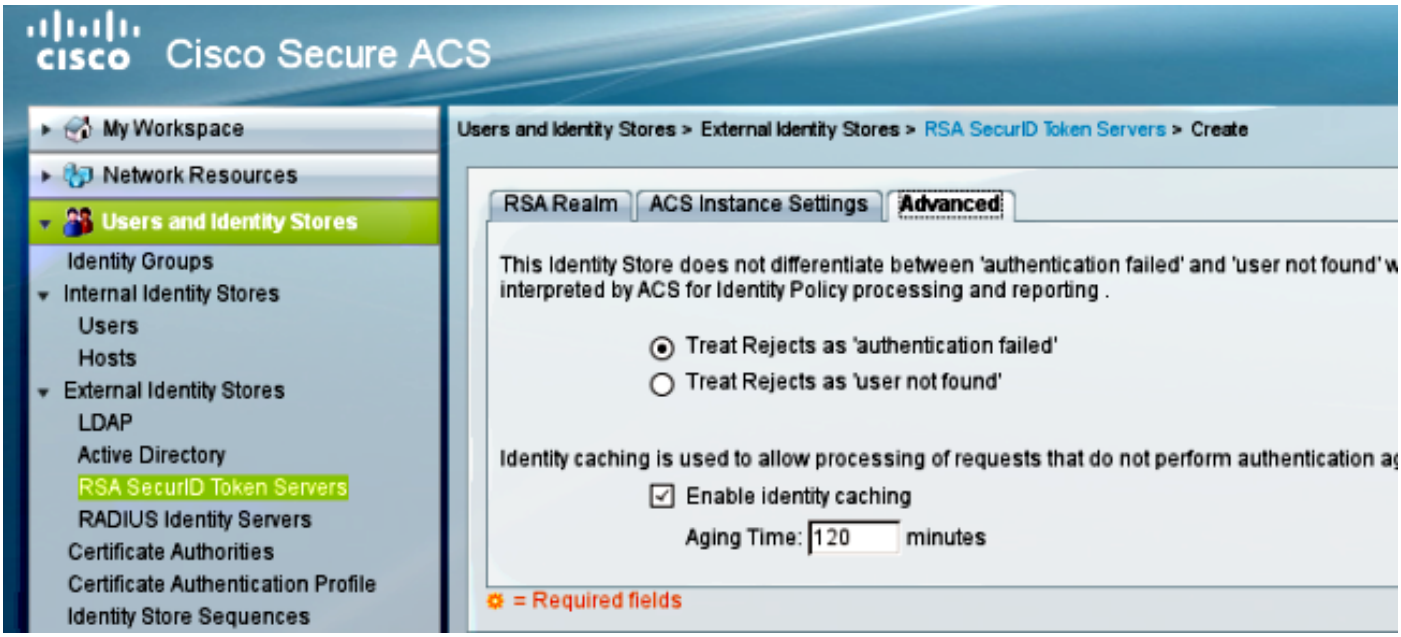
Il est configuré dans les **utilisateurs et l'identité enregistre > mémoire externe d'identité > serveurs de jetons sécurisés d'ID RSA**.

La RSA a de plusieurs serveurs de reproduction, tels que les serveurs secondaires pour l'ACS. Il n'y a aucun besoin de mettre toutes les adresses là, juste le **fichier sdconf.rec** fourni par

l'administrateur RSA. Ce fichier inclut l'adresse IP du serveur primaire RSA. Après le premier noeud réussi d'authentification, le fichier secret est téléchargé avec les adresses IP de toutes les reproductions RSA.



Afin de différencier le « utilisateur non trouvé » du « échec d'authentification, » choisissez les configurations dans l'**onglet Avancé** :



Il est également possible de changer les mécanismes par défaut de routage (Équilibrage de charge) entre de plusieurs serveurs RSA (primaires et des reproductions). Changez-le avec le **fichier sdopts.rec** fourni par l'administrateur RSA. Dans ACS, il est téléchargé dans des **mémoires d'identité d'**Usersand **> mémoire externe d'identité > serveurs de jetons sécurisés d'ID RSA > des configurations d'exemple ACS.**

Pour le déploiement de batterie, la configuration devrait être répliquée. Après la première authentification réussie, chaque noeud ACS utilise son propre secret de noeud téléchargé du serveur primaire RSA. Il est important de se souvenir pour configurer la RSA pour tous les Noeuds ACS dans la batterie.

SDI sur l'ASA

L'ASA ne permet pas le téléchargement du **fichier sdconf.rec**. Et, comme l'ACS, il tient compte du déploiement automatique seulement. L'ASA doit être configurée manuellement afin d'indiquer le serveur primaire RSA. Un mot de passe n'est pas nécessaire. Après le premier noeud réussi d'authentification, le fichier secret est installé (fichier .sdi sur l'éclair) et d'autres sessions d'authentification sont protégées. Également l'adresse IP d'autres serveurs RSA sont téléchargées.

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 l'authentification réussie, la commande de **<aaa-server-group> d'AAA-serveur de SDI** ou d'**exposition de protocole d'AAA-serveur d'exposition** affiche tous les serveurs RSA (s'il y a plus d'un), alors que l'**exposition exécutent des** expositions de commande seulement l'adresse IP primaire :

```
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
```

Dépannez

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

Aucune configuration d'agent sur la RSA

Dans de nombreux cas après que vous installiez une nouvelle ASA ou changiez l'adresse IP ASA, il est facile d'oublier d'apporter les mêmes modifications sur la RSA. L'adresse IP d'agent sur la RSA doit être mise à jour pour tous les clients qui accèdent à la RSA. Puis, le nouveau secret de noeud est généré. Le même s'applique à l'ACS, particulièrement aux Noeuds secondaires parce qu'elles ont différentes adresses IP et la RSA doit leur faire confiance.

Noeud secret corrompu

Parfois le fichier secret de noeud sur l'ASA ou la RSA devient corrompu. Puis, il est le meilleur de retirer la configuration d'agent sur la RSA et de l'ajouter de nouveau. Vous devez également faire le même processus sur l'ASA/ACS - retirez et ajoutez la configuration de nouveau. En outre, supprimez le fichier .sdi sur l'éclair, de sorte que dans la prochaine authentification, un nouveau fichier .sdi soit installé. Le déploiement secret de noeud automatique devrait se produire une fois que c'est complet.

Noeud en mode interrompu

Parfois un des Noeuds est en mode interrompu, qui est provoqué par par aucune 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 interrompu, l'ASA n'essaye pas de n'envoyer aucun paquet à ce noeud ; il doit avoir un état **CORRECT** pour cela. Le serveur défaillant est mis dans le mode actif de nouveau après le temporisateur mort. Le pour en savoir plus, se rapportent à la section de commande de réactivation-mode dans la référence de commandes de gamme de Cisco ASA, le guide 9.1.

Dans de tels scénarios, il est le meilleur de retirer et ajouter la configuration d'AAA-serveur pour ce groupe afin de déclencher ce serveur dans le mode actif de nouveau.

Compte verrouillé

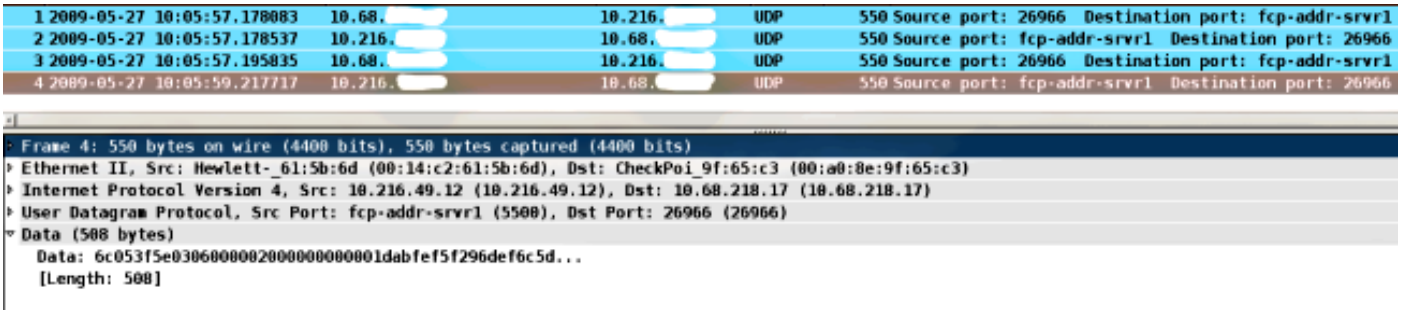
Après que le multiple relance, la RSA pourrait verrouiller hors du compte. Il est facilement vérifié la RSA avec des états. Sur l'ASA/ACS, les états affichent seulement la « authentification défaillante. »

Questions et fragmentation maximum d'unité de transition (MTU)

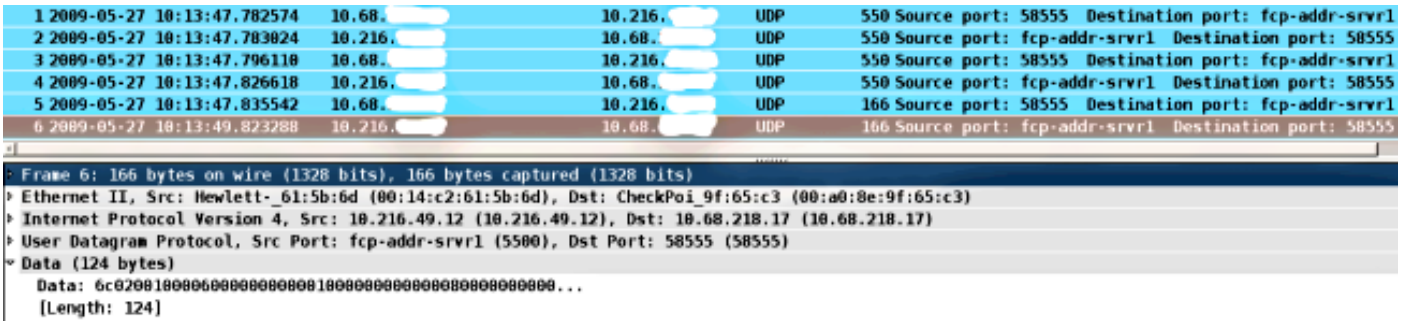
Le SDI utilise l'UDP comme transport, pas découverte de chemin de MTU. Également le trafic UDP n'a pas le bit du Don't Fragment (DF) réglé par défaut. Parfois pour de plus grands paquets, il pourrait y avoir des problèmes de fragmentation. Il est facile de renifler le trafic sur la RSA (l'appliance et le virtual machine [VM] utilisent Windows et utilisent Wireshark). Complétez le même processus sur l'ASA/ACS et comparez. En outre, RAYON de test ou WebAuthentication sur la RSA afin de la comparer au SDI (afin de rétrécir vers le bas le problème).

Paquets et debugs pour ACS

Puisque la charge utile de SDI est chiffrée, la seule manière de dépanner les captures est de comparer la taille de la réponse. S'il est plus petit que 200 octets, il pourrait y a un problème. Un échange typique de SDI implique quatre paquets, qui est de 550 octets, mais cela pourrait changer avec la version serveur RSA :



En cas de problèmes, c'est habituellement plus de quatre paquets permutés et plus petites tailles :



En outre, les logs ACS sont tout à fait clairs. Voici le SDI typique ouvre une session l'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 en gestionnaire d'authentification RSA
- Section de support de serveur RSA/SDI du guide de configuration de gamme de Cisco ASA 5500 utilisant le CLI, les 8.4 et les 8.6
- Section Serveur RSA SecurID du guide utilisateur pour le Système de contrôle d'accès sécurisé Cisco 5.4
- Support et documentation techniques - Cisco Systems