# Gebruik van RSA Token Server en SDI-protocol voor ASA en ACS

## Inhoud



## Inleiding

Dit document beschrijft de procedures voor het opsporen en verhelpen van problemen bij de RSA-verificatie Manager, die kan worden geïntegreerd met de Cisco adaptieve security applicatie (ASA) en de Cisco Secure Access Control Server (ACS).

De RSA Verificatiebeheer is een oplossing die het ÉÉN Wachtwoord van de Tijd (OTP) voor Verificatie verstrekt. Dat wachtwoord wordt elke 60 seconden gewijzigd en kan slechts eenmaal worden gebruikt. Het ondersteunt zowel hardware- als software-penningen.

## Voorwaarden

### Vereisten

Cisco raadt u aan basiskennis van deze onderwerpen te hebben:

- Cisco ASA CLI-configuratie
- Cisco ACS-configuratie

### Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- Cisco ASA-software, versie 8.4 en hoger
- Cisco Secure ACS, versie 5.3 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Theorie

De RSA server kan met RADIUS of het eigen RSA protocol worden benaderd: SDI. Zowel de ASA als de ACS kunnen beide protocollen (RADIUS, SDI) gebruiken om toegang te krijgen tot de RSA.

Vergeet niet dat de RSA kan worden geïntegreerd met Cisco AnyConnect Secure Mobility Client wanneer een softwaretoken wordt gebruikt. Dit document richt zich uitsluitend op de integratie van ASA en ACS. Raadpleeg voor meer informatie over AnyConnect het gedeelte Gebruikmakend van SDI-verificatie van de Cisco AnyConnect Secure Mobility Client Administrator Guide, release 3.1.

## RSA via RADIUS

RADIUS heeft één groot voordeel ten opzichte van SDI. Op de RSA, is het mogelijk om specifieke profielen (genaamd groepen op ACS) aan gebruikers toe te wijzen. Deze profielen hebben specifieke RADIUS-kenmerken gedefinieerd. Na succesvolle authenticatie bevat het RADIUS-Accept bericht dat van de RSA wordt teruggestuurd die eigenschappen. Op basis van deze eigenschappen neemt het ACS aanvullende besluiten. Het meest voorkomende scenario is het besluit om de toewijzing van de ACS-groep te gebruiken om specifieke RADIUS-kenmerken, gerelateerd aan het profiel op de RSA, in kaart te brengen aan een specifieke groep op de ACS. Met deze logica is het mogelijk het hele vergunningsproces van de RSA naar de ACS te verplaatsen en nog steeds de granulaire logica te handhaven, zoals in de RSA.

## RSA via SDI

SDI heeft twee belangrijke voordelen ten opzichte van RADIUS. De eerste is dat de hele sessie versleuteld is. Het tweede is de interessante opties die de SDI-agent biedt: zij kan vaststellen of de storing is ontstaan omdat de authenticatie of autorisatie is mislukt of omdat de gebruiker niet werd gevonden .

Deze informatie wordt door het ACS gebruikt in actie voor de identiteit. Bijvoorbeeld, het zou

kunnen doorgaan voor "gebruiker not found" maar het zou kunnen weigeren voor "authenticatie faalde".

Er is nog een verschil tussen RADIUS en SDI. Wanneer een apparaat voor netwerktoegang zoals ASA SDI gebruikt, voert het ACS alleen verificatie uit. Wanneer het RADIUS gebruikt, voert het ACS verificatie, autorisatie en accounting (AAA) uit. Dit is echter geen groot verschil. Het is mogelijk om SDI voor authenticatie en RADIUS te configureren voor accounting voor dezelfde sessies.

# SDI-protocol

Standaard gebruikt SDI User Datagram Protocol (UDP) 5500. SDI gebruikt een symmetrische encryptie-toets, vergelijkbaar met de RADIUS-toets, om sessies te versleutelen. Deze toets wordt opgeslagen in een knooppunt-geheim bestand en is verschillend voor elke SDI-client. Dat bestand wordt handmatig of automatisch ingezet.

> Opmerking: ACS/ASA ondersteunt handmatige implementatie niet.

Voor het automatische uitzettingsknooppunt wordt het geheime bestand automatisch gedownload na de eerste succesvolle verificatie. Het knoopsgeheim wordt versleuteld met een sleutel die is afgeleid van de gebruikerscode en andere informatie. Dit creëert een aantal mogelijke beveiligingsproblemen, zodat de eerste verificatie lokaal moet worden uitgevoerd en het gecodeerde protocol (Secure Shell [SSH], niet telnet) moet worden gebruikt om ervoor te zorgen dat de aanvaller dat bestand niet kan onderscheppen en decrypteren.

# Configuratie

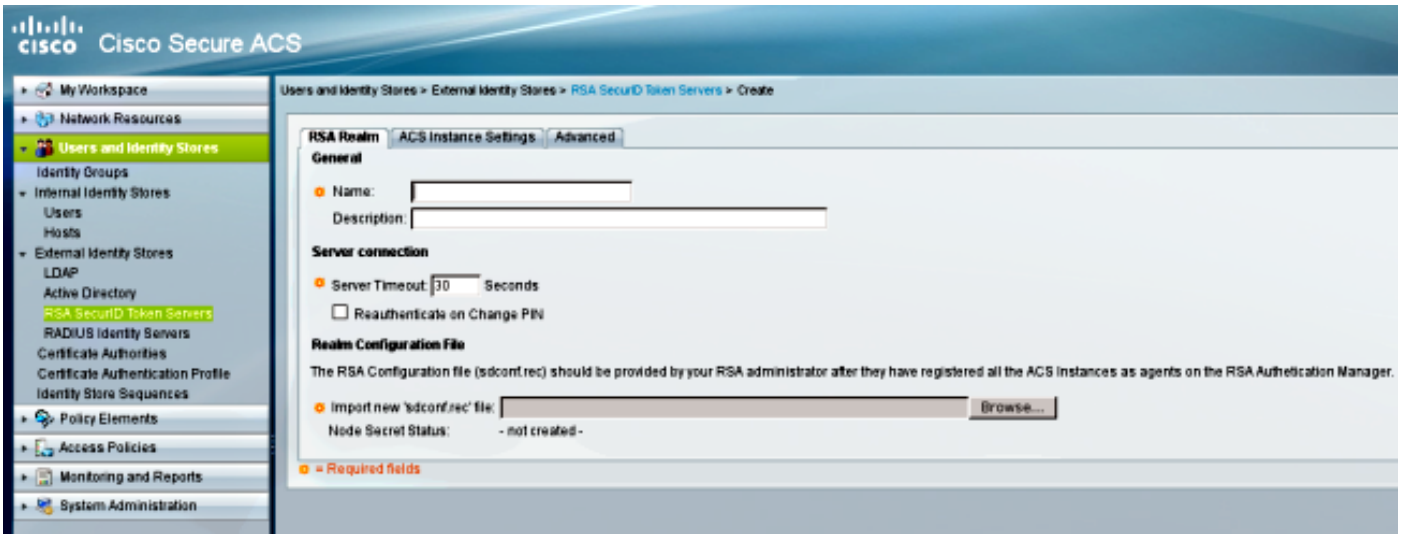
> Opmerkingen:
>
> Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.
>
> De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met **show.** Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**
>
> Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met **debug opgeeft.**

## SDI op ACS

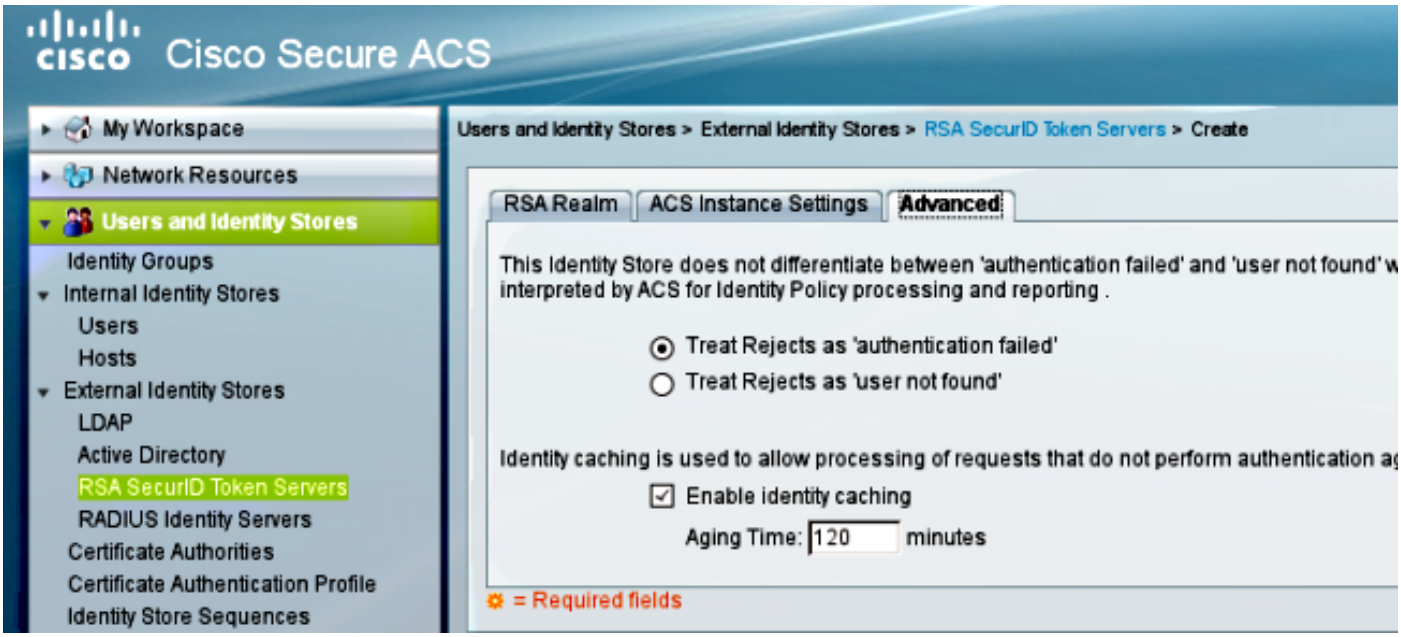
Het wordt ingesteld in **gebruikers en identiteitsopslag > Externe Identity Store > RSA Secure ID Token Server**.

De RSA heeft meerdere replica-servers, zoals de secundaire servers voor de ACS. Het is niet nodig om alle adressen daar te plaatsen, behalve het **sdconf.rec** bestand dat door de RSA-

beheerder wordt geleverd. Dit bestand bevat het IP-adres van de primaire RSA-server. Na het eerste succesvolle authenticknooppunt wordt het geheime bestand gedownload samen met de IP-adressen van alle RSA-replica's.




Om "user not found" te onderscheiden van "Authenticatie defect" kiest u instellingen in het **Advanced** tabblad:




Het is ook mogelijk om de standaard routing (load balances) mechanismen tussen meerdere RSA-servers (primaire en replica's) te wijzigen. Verander het met het **sdopts.rec** bestand dat door de RSA-beheerder is geleverd. In ACS wordt het geüpload in **gebruikers en identiteitsopslag > Externe Identity Store > RSA Secure ID Token Server > ACS-instinctinstellingen**.

Voor clusterimplementatie moet de configuratie worden gerepliceerd. Na de eerste succesvolle authenticatie gebruikt elk ACS-knooppunt zijn eigen knooppunt geheim gedownload van de primaire RSA-server. Het is belangrijk om te onthouden om de RSA te configureren voor alle ACS-knooppunten in de cluster.

## SDI op ASA

De ASA staat het uploaden van het **sdconf.rec**-bestand niet toe. Net als het ACS maakt het alleen

automatische plaatsing mogelijk. De ASA moet handmatig worden ingesteld om naar de primaire RSA-server te wijzen. Er is geen wachtwoord nodig. Na het eerste succesvolle authenticatieknooppunt wordt het geheime bestand geïnstalleerd (.sdi-bestand op flitser) en worden verdere authenticatiesessies beveiligd. Ook het IP-adres van andere RSA-servers wordt gedownload.

Hierna volgt een voorbeeld:

```
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
```

Na succesvolle verificatie **toont** de **opdracht** AAA-**server protocol sdi** of **toont a-server <a-server-group>** alle RSA servers (als er meer dan één zijn), terwijl de opdracht **show run** alleen het primaire IP-adres toont:

```
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
```

# Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

## No Agent-configuratie voor RSA

In veel gevallen nadat u een nieuwe ASA hebt geïnstalleerd of het ASA IP-adres hebt gewijzigd, is het gemakkelijk om dezelfde veranderingen op de RSA te vergeten. Het IP-adres van de Agent op de RSA moet worden bijgewerkt voor alle klanten die toegang hebben tot de RSA. Vervolgens wordt het nieuwe knooppunt-geheim gegenereerd. Het zelfde is van toepassing op ACS, vooral op secundaire knooppunten omdat zij verschillende IP adressen hebben en de RSA moet hen vertrouwen.

## Versleuteld geheim knooppunt

Soms wordt het geheime knooppunt bestand op de ASA of de RSA beschadigd. Vervolgens is het beter om de Agent-configuratie op de RSA te verwijderen en opnieuw toe te voegen. U moet ook hetzelfde proces uitvoeren op de ASA/ACS - en de configuratie opnieuw verwijderen en toevoegen. Verwijder ook het .sdi-bestand op de flitser, zodat in de volgende verificatie een nieuw .sdi-bestand geïnstalleerd is. Automatische geheime implementatie van knooppunten zou moeten plaatsvinden zodra dit is voltooid.

## Knooppunt in verdachte modus

Soms is één van de knooppunten in de gesuspendeerde modus, wat wordt veroorzaakt door geen reactie van die server:

```
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
```

In de gesuspendeerde modus probeert de ASA geen pakketten naar dat knooppunt te verzenden. Daarvoor is een **goede** status nodig. De mislukte server wordt na de dode timer opnieuw in actieve modus gezet. Raadpleeg voor meer informatie het gedeelte Opdracht reactivatie-mode in de Cisco ASA Series Opdrachtreferenties, 9.1 richtlijn.

In dergelijke scenario's is het best om de configuratie van de AAA-server voor die groep te

verwijderen en toe te voegen om die server opnieuw in de actieve modus te activeren.

## Account vergrendeld

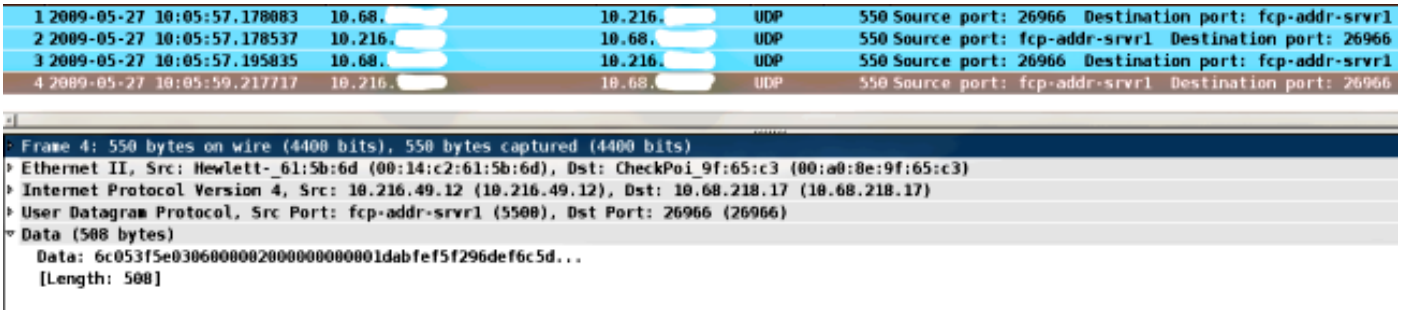
Na meerdere herhalingen kan de RSA buiten de rekening sluiten. Het wordt gemakkelijk gecontroleerd op de RSA met rapporten. Op de ASA/ACS tonen rapporten alleen "mislukte authenticatie".

## Max. doorgifte-eenheid (MTU) - problemen en fragmentatie

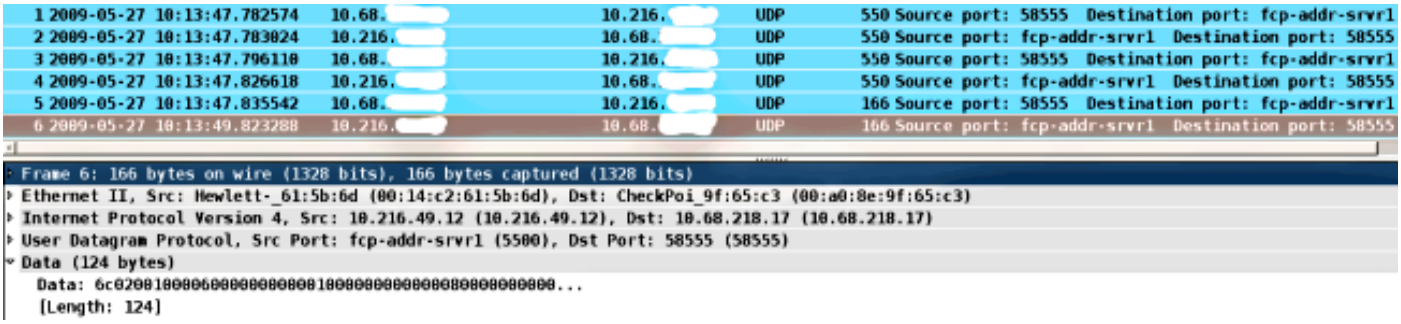
SDI gebruikt UDP als transport, niet als MTU om het pad te ontdekken. Het UDP-verkeer heeft het Don't Fragment (DF)-bit niet standaard ingesteld. Soms zijn er voor grotere pakketten fragmentatieproblemen. U kunt eenvoudig overschakelen op de RSA (zowel het apparaat als de virtuele machine [VM] gebruiken Windows en Wireshark gebruiken). Voltooi hetzelfde proces op de ASA/ACS en vergelijk het. Test ook RADIUS of Webex Verificatie op RSA om het met SDI te vergelijken (om het probleem te beperken).

## Packet- en debugs voor ACS

Omdat SDI payload versleuteld is, is de enige manier om problemen op te lossen de Captures door de grootte van de respons te vergelijken. Als het kleiner is dan 200 bytes, kan er een probleem zijn. Een typische SDI-uitwisseling heeft betrekking op vier pakketten, die elk 550 bytes zijn, maar die met de RSA-serverversie kunnen veranderen:




In geval van problemen is het meestal meer dan vier uitgewisselde pakketten en een kleiner formaat:




De ACS-logboeken zijn ook heel duidelijk. Hier zijn typische SDI-blogs op de 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
```

# Gerelateerde informatie

- RSA-verificatie Manager-bronnen
- Ondersteuning van RSA/SDI-server van het Cisco ASA 5500 Series Configuration Guide uit de CLI, 8.4 en 8.6
- RSA SecureID Server-gedeelte van de gebruikersgids voor Cisco Secure Access Control System 5.4
- Technische ondersteuning en documentatie – Cisco Systems