Uso di RSA Token Server e del protocollo SDI per ASA e ACS

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Teoria](#)
[RSA via RADIUS](#)
[RSA via SDI](#)
[Protocollo SDI](#)
[Configurazione](#)
[SDI su ACS](#)
[SDI su ASA](#)
[Risoluzione dei problemi](#)
[Nessuna configurazione dell'agente su RSA](#)
[Nodo segreto danneggiato](#)
[Nodo in modalità sospesa](#)
[Account bloccato](#)
[Problemi di MTU (Maximum Transition Unit) e frammentazione](#)
[Pacchetti e debug per ACS](#)
[Informazioni correlate](#)

Introduzione

In questo documento vengono descritte le procedure di risoluzione dei problemi per RSA Authentication Manager, che può essere integrato con Cisco Adaptive Security Appliance (ASA) e Cisco Secure Access Control Server (ACS).

RSA Authentication Manager è una soluzione che fornisce OTP (One Time Password) per l'autenticazione. La password viene modificata ogni 60 secondi e può essere utilizzata una sola volta. Supporta token hardware e software.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Configurazione Cisco ASA CLI
- Configurazione Cisco ACS

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- Software Cisco ASA, versione 8.4 e successive
- Cisco Secure ACS, versione 5.3 e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Teoria

Èpossibile accedere al server RSA con RADIUS o il protocollo RSA proprietario: SDI Per accedere a RSA, sia l'ASA che l'ACS possono usare entrambi i protocolli (RADIUS, SDI).

Tenere presente che quando si usa un token software, RSA può essere integrato con Cisco AnyConnect Secure Mobility Client. Questo documento si concentra esclusivamente sull'integrazione tra ASA e ACS. Per ulteriori informazioni su AnyConnect, fare riferimento alla sezione Using SDI Authentication nel manuale Cisco AnyConnect Secure Mobility Client Administrator Guide, versione 3.1.

RSA via RADIUS

RADIUS offre un grande vantaggio rispetto a SDI. Su RSA, è possibile assegnare profili specifici (chiamati gruppi su ACS) agli utenti. Per tali profili sono stati definiti attributi RADIUS specifici. Dopo l'autenticazione, il messaggio RADIUS-Accept restituito da RSA contiene questi attributi. In base a tali attributi, l'ACS prende ulteriori decisioni. Lo scenario più comune è la decisione di utilizzare la mappatura dei gruppi ACS per mappare gli attributi RADIUS specifici, correlati al profilo sull'RSA, a un gruppo specifico sull'ACS. Con questa logica, è possibile spostare l'intero processo di autorizzazione da RSA ad ACS e mantenere comunque la logica granulare, come su RSA.

RSA via SDI

SDI offre due vantaggi principali rispetto a RADIUS. La prima è che l'intera sessione è crittografata. Il secondo riguarda le interessanti opzioni fornite dall'agente SDI: è in grado di determinare se l'errore si è verificato perché l'autenticazione o l'autorizzazione non è riuscita o perché l'utente non è stato trovato.

Queste informazioni vengono usate da ACS in azione per l'identità. Ad esempio, potrebbe

continuare per "utente non trovato" ma rifiutare per "autenticazione non riuscita".

C'è un'altra differenza tra RADIUS e SDI. Quando un dispositivo di accesso alla rete come ASA usa l'interfaccia SDI, l'ACS esegue solo l'autenticazione. Quando si utilizza RADIUS, ACS esegue l'autenticazione, l'autorizzazione e l'accounting (AAA). Tuttavia, questa non è una grande differenza. È possibile configurare SDI per l'autenticazione e RADIUS per l'accounting per le stesse sessioni.

Protocollo SDI

Per impostazione predefinita, SDI utilizza il protocollo UDP (User Datagram Protocol) 5500. Per crittografare le sessioni, SDI utilizza una chiave di crittografia simmetrica simile alla chiave RADIUS. Tale chiave viene salvata in un file segreto del nodo ed è diversa per ogni client SDI. Il file viene distribuito manualmente o automaticamente.

> **Nota:** ACS/ASA non supporta la distribuzione manuale.

Per il nodo di distribuzione automatica, il file segreto viene scaricato automaticamente dopo la prima autenticazione riuscita. Il segreto del nodo viene crittografato con una chiave derivata dal passcode dell'utente e da altre informazioni. Ciò crea alcuni possibili problemi di sicurezza, quindi la prima autenticazione deve essere eseguita localmente e usare un protocollo crittografato (Secure Shell [SSH], non telnet) per assicurarsi che l'autore dell'attacco non possa intercettare e decrittografare il file.

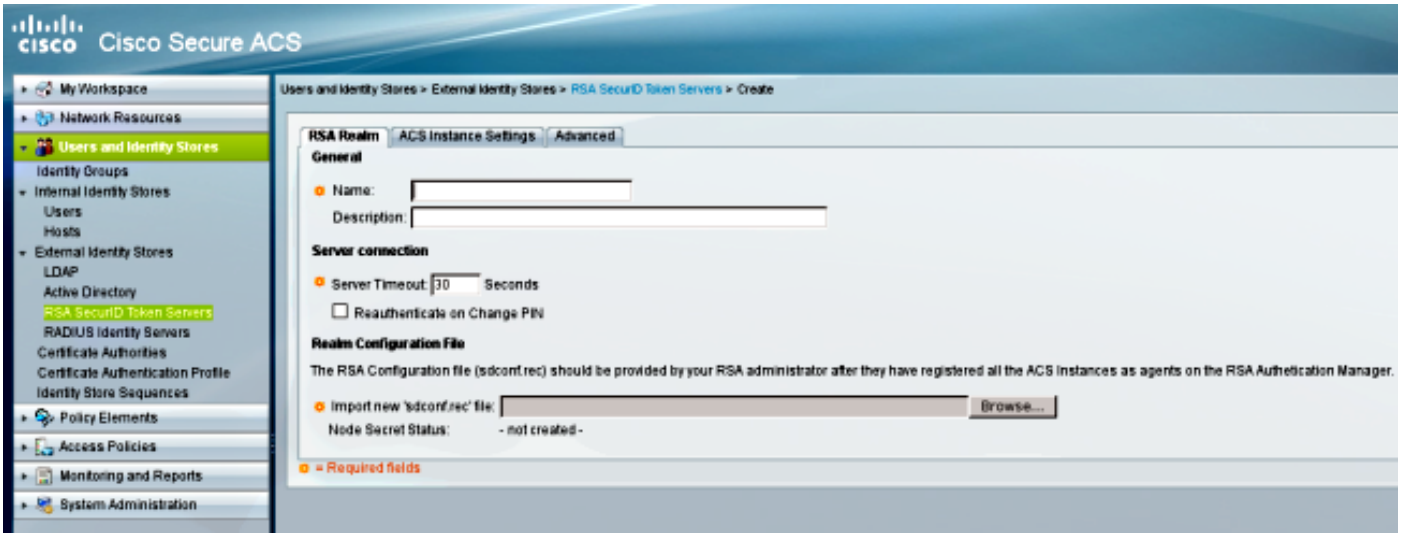
Configurazione

> **Note:**
>
> per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).
>
> Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi **show.** Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**
>
> consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug.**

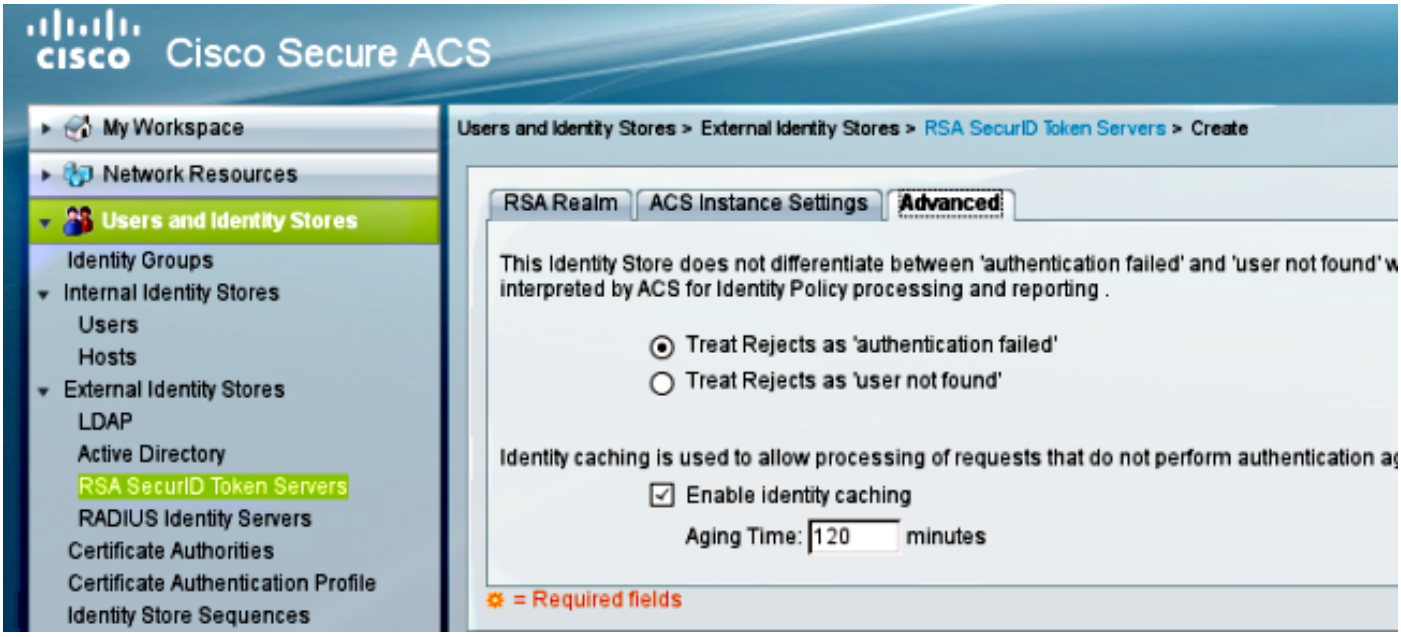
SDI su ACS

Èconfigurato in **Utenti e archivi identità > Archivio identità esterno > Server token RSA Secure ID**.

RSA dispone di più server di replica, come i server secondari per ACS. Non è necessario inserire tutti gli indirizzi, ma solo il file **sdconf.rec** fornito dall'amministratore RSA. Questo file include l'indirizzo IP del server RSA principale. Dopo il primo nodo di autenticazione riuscito, il file segreto viene scaricato insieme agli indirizzi IP di tutte le repliche RSA.



Per distinguere tra "utente non trovato" e "errore di autenticazione", scegliere le impostazioni nella scheda **Avanzate**:



Èinoltre possibile modificare i meccanismi di routing predefiniti (bilanciamento del carico) tra più server RSA (principali e repliche). Modificarlo con il file **sdopts.rec** fornito dall'amministratore RSA. In ACS, viene caricato in **Users and Identity Stores > External Identity Store > RSA Secure ID Token Server > ACS Instance Settings**.

Per la distribuzione cluster, è necessario replicare la configurazione. Dopo la prima autenticazione riuscita, ogni nodo ACS utilizza il proprio segreto del nodo scaricato dal server RSA primario. È importante ricordare di configurare RSA per tutti i nodi ACS nel cluster.

SDI su ASA

L'ASA non consente il caricamento del file **sdconf.rec**. E, come ACS, consente solo l'installazione automatica. L'ASA deve essere configurata manualmente in modo da puntare al server RSA principale. Non è necessaria una password. Una volta completato il primo nodo di autenticazione, il file segreto viene installato (file con estensione sdi su flash) e altre sessioni di autenticazione vengono protette. Vengono scaricati anche gli indirizzi IP degli altri server RSA.

Di seguito è riportato un esempio:

```
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
```

Dopo l'autenticazione, il comando **show aaa-server protocol sdi** o **show aaa-server <aaa-server-group>**visualizza tutti i server RSA (se ne esistono più di uno), mentre il comando **show run** visualizza solo l'indirizzo IP primario:

```
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
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Nessuna configurazione dell'agente su RSA

In molti casi, dopo aver installato una nuova appliance ASA o modificato l'indirizzo IP dell'appliance, è facile dimenticare di apportare le stesse modifiche sull'appliance RSA. L'indirizzo IP dell'agente sull'RSA deve essere aggiornato per tutti i client che accedono all'RSA. Viene quindi generato il nuovo segreto del nodo. Lo stesso vale per l'ACS, soprattutto per i nodi secondari, in quanto hanno indirizzi IP diversi e RSA deve considerarli attendibili.

Nodo segreto danneggiato

A volte il file del nodo segreto sull'appliance ASA o sull'appliance RSA risulta danneggiato. Quindi, è meglio rimuovere la configurazione dell'agente su RSA e aggiungerla di nuovo. La stessa procedura deve essere eseguita anche sull'appliance ASA/ACS, quindi rimuovere e aggiungere nuovamente la configurazione. Inoltre, eliminare il file .sdi sul flash, in modo che nella successiva autenticazione, un nuovo file .sdi sia installato. Al termine della distribuzione automatica del segreto del nodo.

Nodo in modalità sospesa

A volte uno dei nodi è in modalità sospesa, a causa della mancata risposta da tale 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 modalità sospesa, l'ASA non tenta di inviare alcun pacchetto a quel nodo; lo stato deve essere **corretto**. Il server in errore viene riattivato dopo la disattivazione del timer. Per ulteriori informazioni, consultare la sezione sulla modalità di riattivazione nella guida di riferimento dei comandi della serie Cisco ASA, versione 9.1.

In questi scenari, è consigliabile rimuovere e aggiungere la configurazione del server AAA per il gruppo in modo da attivare nuovamente il server in modalità attiva.

Account bloccato

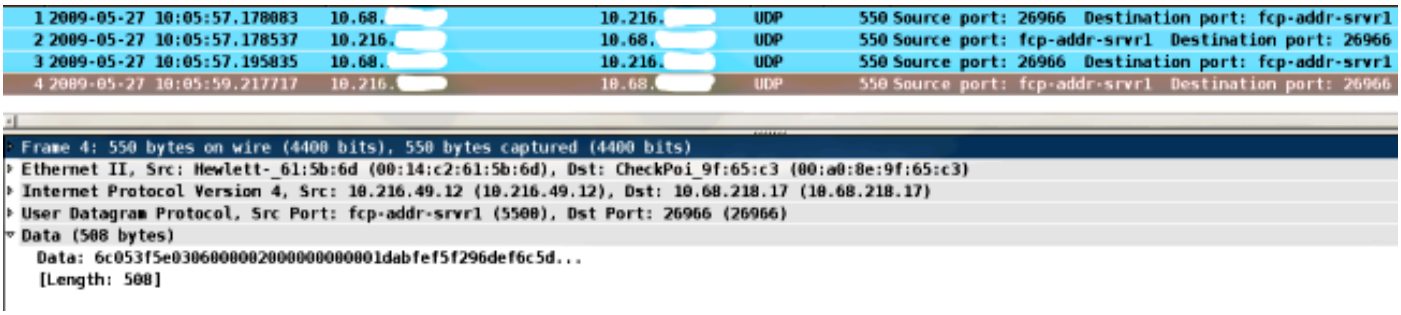
Dopo più tentativi, RSA potrebbe bloccarsi dall'account. È facilmente verificabile su RSA tramite report. Sull'appliance ASA/ACS, i report visualizzano solo "autenticazione non riuscita".

Problemi di MTU (Maximum Transition Unit) e frammentazione

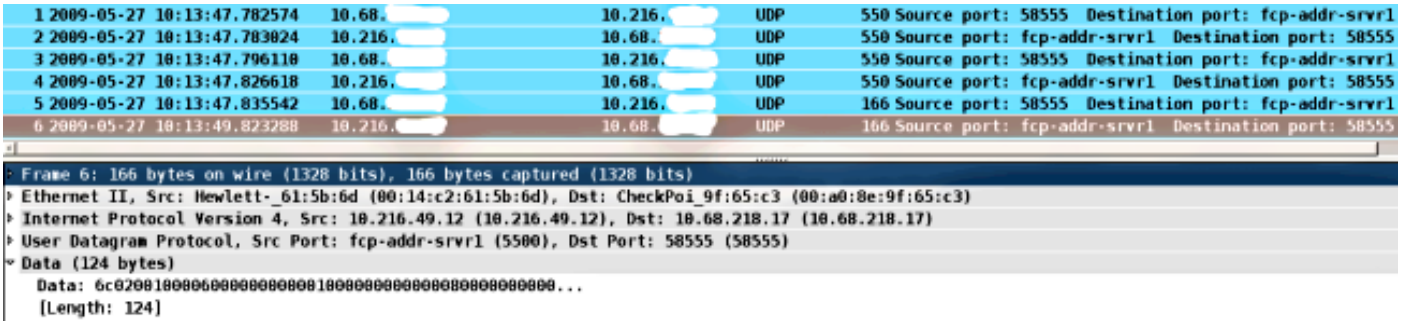
L'interfaccia SDI utilizza UDP come trasporto, non come rilevamento del percorso MTU. Inoltre, per impostazione predefinita, il bit "non frammentare" (DF, Don't Fragment) non è impostato per il traffico UDP. A volte, per i pacchetti di dimensioni maggiori, possono verificarsi problemi di frammentazione. È facile sniffare il traffico su RSA (sia l'appliance che Virtual Machine [VM] utilizzano Windows e Wireshark). Completare la stessa procedura sull'appliance ASA/ACS e confrontarla. Inoltre, verificare RADIUS o WebAuthentication su RSA per confrontarlo con SDI (per limitare il problema).

Pacchetti e debug per ACS

Poiché il payload SDI è crittografato, l'unico modo per risolvere i problemi relativi alle clip è confrontare le dimensioni della risposta. Se è inferiore a 200 byte, potrebbe essersi verificato un problema. Uno scambio SDI tipico coinvolge quattro pacchetti, ognuno dei quali è di 550 byte, ma questo potrebbe cambiare con la versione del server RSA:



In caso di problemi, generalmente vengono scambiati più di quattro pacchetti e dimensioni inferiori:



Inoltre, i log ACS sono abbastanza chiari. Di seguito sono riportati i log SDI tipici sull'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
```

Informazioni correlate

- Risorse di RSA Authentication Manager
- Sezione Supporto server RSA/SDI della guida alla configurazione di Cisco ASA serie 5500 dall'interfaccia CLI (Command Line Interface), 8.4 e 8.6
- Sezione RSA SecurID Server della Guida per l'utente di Cisco Secure Access Control System 5.4
- Documentazione e supporto tecnico – Cisco Systems