Servidor Token RSA y uso del protocolo del SDI para el ASA y el ACS

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Teoría
RSA vía el RADIUS
RSA vía el SDI
Protocolo del SDI
Configuración
SDI en el ACS
SDI en el ASA
Troubleshooting
Ninguna Configuración del agente en el RSA
Nodo secreto corrompido
Nodo en el modo suspendido
Cuenta bloqueada
Problemas y fragmentación máximos de la unidad de la transición (MTU)
Paquetes y debugs para el ACS
Información Relacionada

Introducción

Este documento describe los procedimientos deTroubleshooting para el administrador de la Autenticación RSA, que puede ser integrado con el dispositivo de seguridad adaptante de Cisco (ASA) y el Cisco Secure Access Control Server (ACS).

El administrador de la Autenticación RSA es una solución que proporciona la una contraseña del tiempo (OTP) para la autenticación. Que la contraseña está cambiada cada 60 segundos y se puede utilizar solamente una vez. Soporta ambos tokens del hardware y software.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento básico de estos temas:

- Configuración CLI de Cisco ASA
- Configuración de ACS de Cisco

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Software de Cisco ASA, versión 8.4 y posterior
- Cisco Secure ACS, versión 5.3 y posterior

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Teoría

El servidor RSA se puede acceder con el RADIUS o el protocolo propietario RSA: SDI. El ASA y el ACS pueden utilizar ambos protocolos (RADIUS, SDI) para acceder el RSA.

Recuerde que el RSA se puede integrar con el Cliente de movilidad Cisco AnyConnect Secure cuando se utiliza una ficha de software. Este documento se centra solamente en la integración ASA y ACS. Para más información sobre AnyConnect, refiera a usar Autenticación SDI la sección del guía del administrador del Cliente de movilidad Cisco AnyConnect Secure, la versión 3.1.

RSA vía el RADIUS

El RADIUS tiene una ventaja grande sobre el SDI. En el RSA, es posible asignar los perfiles específicos (llamados los grupos en el ACS) a los usuarios. Esos perfiles tienen atributos de RADIUS específicos definidos. Después de la autenticación satisfactoria, el mensaje del RADIUS-validar vuelto del RSA contiene esos atributos. De acuerdo con esos atributos, el ACS toma las decisiones adicionales. La mayoría del escenario frecuente es la decisión para utilizar la asignación del grupo ACS para asociar los atributos de RADIUS específicos, relacionados con el perfil en el RSA, a un grupo específico en el ACS. Con esta lógica, es posible mover el proceso entero de la autorización desde el RSA al ACS y todavía mantener la lógica granular, como en el RSA.

RSA vía el SDI

El SDI tiene dos ventajas principales sobre el RADIUS. El primer es que la sesión entera está cifrada. El segundo es las opciones interesantes que el agente del SDI proporciona: puede determinar si se crea el incidente porque la autenticación o la autorización falló o porque no encontraron al usuario.

Esta información es utilizada por el ACS en la acción para la identidad. Por ejemplo, podría

continuar para el “usuario no encontrado” pero el rechazo para la “autenticación falló.”

Hay una más diferencia entre el RADIUS y el SDI. Cuando un dispositivo de acceso a la red como el ASA utiliza el SDI, el ACS realiza solamente la autenticación. Cuando utiliza el RADIUS, el ACS realiza la autenticación, autorización, considerando (AAA). Sin embargo, esto no es una diferencia grande. Es posible configurar el SDI para la autenticación y el RADIUS para explicar las mismas sesiones.

Protocolo del SDI

Por abandono, User Datagram Protocol (UDP) 5500 de las aplicaciones del SDI. El SDI utiliza una clave de encripción simétrica, similar a la clave RADIUS, para cifrar las sesiones. Que la clave está guardada en un archivo node secret y es diferente para cada cliente SDI. Ese archivo se despliega manualmente o automáticamente.

> Nota: ACS/ASA no soporta el despliegue manual.

Para el nodo automático del despliegue, el archivo secreto se descarga automáticamente después de la primera autenticación satisfactoria. El secreto de nodo se cifra con una clave derivada de la otra información del usuario de la contraseña y. Esto crea algunos problemas de seguridad posibles, así que la primera autenticación se debe realizar localmente y protocolo cifrado uso (shell seguro [SSH], no el telnet) para asegurarse de que el atacante no puede interceptar y desencriptar ese archivo.

Configuración

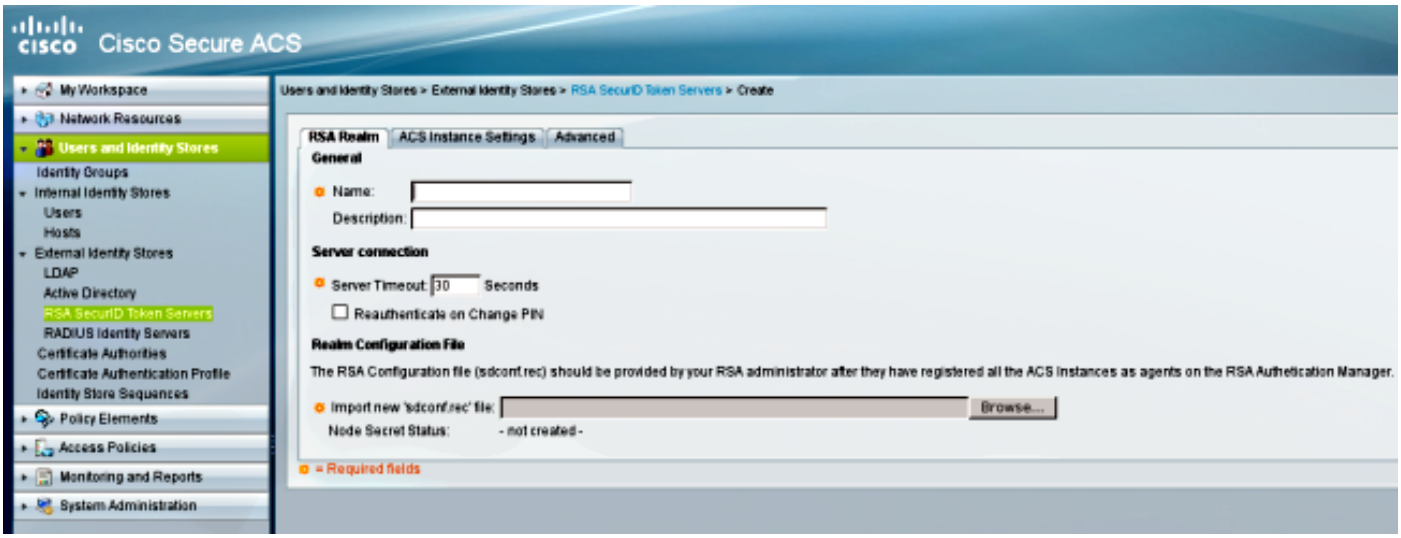
> Notas:
>
> Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.
>
> La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.
>
> Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

SDI en el ACS

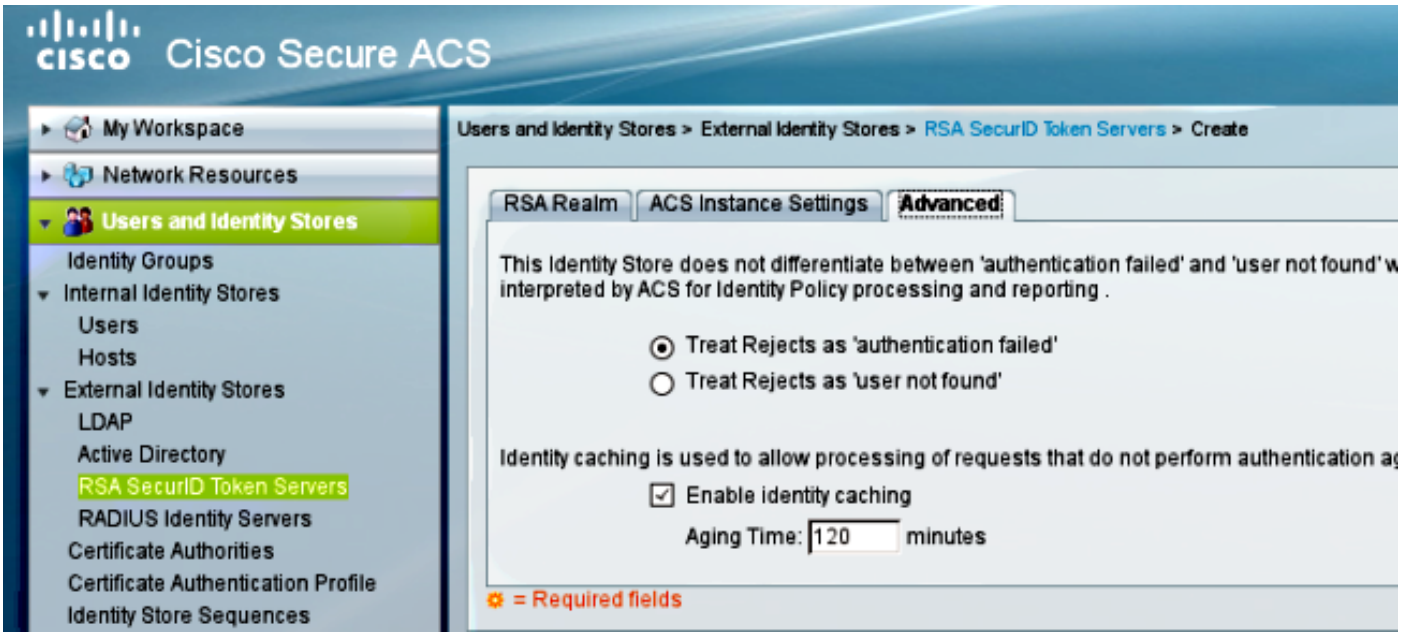
Se configura en los **usuarios y la identidad salva > almacén externo de la identidad > los servidores Token del Secure ID RSA**.

El RSA tiene los servidores réplica múltiples, tales como los servidores secundarios para el ACS. No hay necesidad de poner todos los direccionamientos allí, apenas el **archivo sdconf.rec** proporcionado por el administrador RSA. Este archivo incluye la dirección IP del servidor primario

RSA. Después del primer nodo de la autenticación satisfactoria, el archivo secreto se descarga junto con los IP Addresses de todas las reproducciones RSA.



Para distinguir al “usuario no encontrado” de la “falla de autenticación,” elija las configuraciones en la **ficha Avanzadas**:



Es también posible cambiar los mecanismos del ruteo predeterminado (Equilibrio de carga) entre los servidores múltiples RSA (primarios y las reproducciones). Cambíelo con el **archivo sdopts.rec** proporcionado por el administrador RSA. En el ACS, está cargado en los **almacenes de la identidad de** Usersand **> almacén externo de la identidad > los servidores Token del Secure ID RSA > las configuraciones del caso ACS.**

Para el despliegue del cluster, la configuración debe ser replicada. Después de la primera autenticación satisfactoria, cada nodo ACS utiliza su propio secreto de nodo descargado del servidor primario RSA. Es importante recordar configurar el RSA para todos los Nodos ACS en el cluster.

SDI en el ASA

El ASA no permite la carga del **archivo sdconf.rec**. Y, como el ACS, permite el despliegue

automático solamente. El ASA necesita ser configurado manualmente para señalar al servidor primario RSA. Una contraseña no es necesaria. Después del primer nodo de la autenticación satisfactoria, el archivo secreto está instalado (archivo .sdi en el flash) y se protegen sesiones más futuras de la autenticación. También la dirección IP de otros servidores RSA se descarga.

Aquí tiene un ejemplo:

```
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
```

Después de la autenticación satisfactoria, el **sdi del protocolo del AAA-servidor de la demostración** o el comando del **<aaa-server-group> del AAA-servidor de la demostración** muestra todos los servidores RSA (si hay más de uno), mientras que el **comando show run** muestra solamente el IP Address principal:

```
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
```

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

Ninguna Configuración del agente en el RSA

En muchos casos después de que usted instale un nuevo ASA o cambie la dirección IP ASA, es fácil olvidar realizar los mismos cambios en el RSA. La dirección IP del agente en el RSA necesita ser puesta al día para todos los clientes que accedan el RSA. Entonces, se genera el secreto del nuevo nodo. Lo mismo se aplica al ACS, especialmente a los Nodos secundarios porque él tiene diversos IP Addresses y el RSA necesita confiarlos en.

Nodo secreto corrompido

A veces el archivo secreto del nodo en el ASA o el RSA se corrompe. Entonces, es el mejor quitar la Configuración del agente en el RSA y agregarla otra vez. Usted también necesita hacer el mismo proceso en el ASA/ACS - quite y agregue la configuración otra vez. También, borre el archivo .sdi en el flash, para en la autenticación siguiente, instalar un nuevo archivo .sdi. El despliegue automático del secreto de nodo debe ocurrir una vez que éste es completo.

Nodo en el modo suspendido

A veces uno de los Nodos está en el modo suspendido, que es causado por ninguna respuesta de ese servidor:

```
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 el modo suspendido, el ASA no intenta enviar ninguna paquetes a ese nodo; necesita tener un estatus **ACEPTABLE** para eso. Ponen al servidor defectuoso en el modo activo otra vez después del temporizador de emergencia. Para más información, refiera al comando section reactivación-MODE en la referencia de comandos de la serie de Cisco ASA, la guía 9.1.

En tales escenarios, es el mejor quitar y agregar la configuración de servidor AAA para ese grupo para accionar ese servidor en el modo activo otra vez.

Cuenta bloqueada

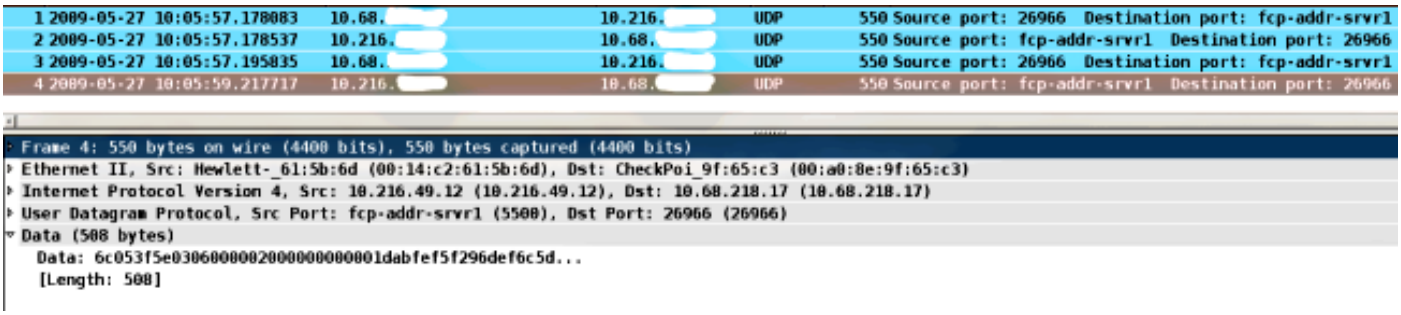
Después de que sea múltiple las recomprobaciones, el RSA pudieran bloquear la cuenta de los. Se comprueba fácilmente el RSA con los informes. En el ASA/ACS, los informes muestran solamente la “autenticación fallida.”

Problemas y fragmentación máximos de la unidad de la transición (MTU)

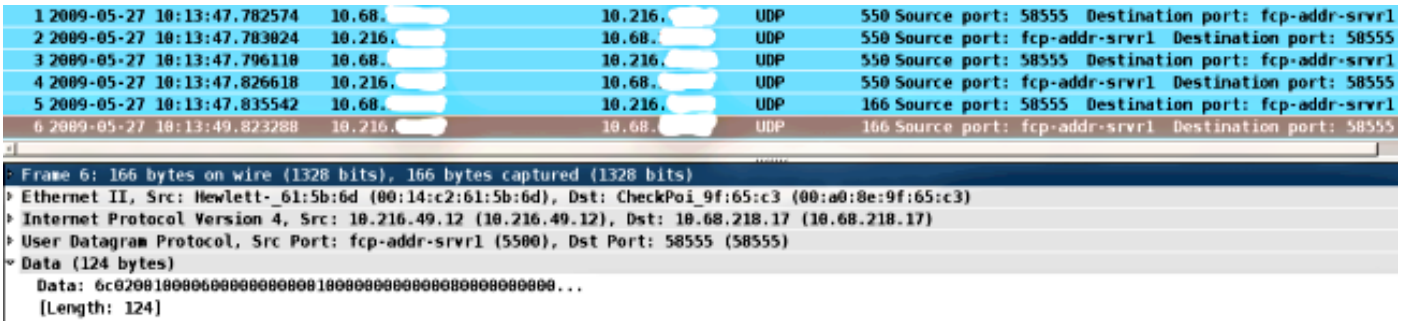
El SDI utiliza el UDP como transporte, no detección de trayecto MTU. También el tráfico UDP no tiene el conjunto de bits del don't fragment (DF) por abandono. A veces para paquetes más grandes, pudo haber problemas de fragmentación. Es fácil oler el tráfico en [VM] RSA (el dispositivo y la máquina virtual utilizan Windows y utilizan Wireshark). Complete el mismo proceso en el ASA/ACS y compare. También, prueba RADIUS o WebAuthentication en el RSA para compararlo al SDI (para estrechar abajo el problema).

Paquetes y debugs para el ACS

Porque se cifra el payload del SDI, la única forma de resolver problemas las capturas es comparar el tamaño de la respuesta. Si es más pequeña de 200 bytes, pudo haber un problema. Un intercambio típico del SDI implica cuatro paquetes, que es 550 bytes, pero ése pudo cambiar con la versión del servidor RSA:



En caso de los problemas, es generalmente más de cuatro paquetes intercambiados y tamaños más pequeños:



También, los registros ACS están muy claros. Aquí está el SDI típico abre una sesión el 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
```

Información Relacionada

- Recursos del administrador de la Autenticación RSA
- Sección del soporte de servidor RSA/SDI de la guía de configuración de las 5500 Series de Cisco ASA que usa el CLI, los 8.4 y los 8.6
- Sección del servidor del SecurID RSA del guía del usuario para el Cisco Secure Access Control System 5.4
- Soporte Técnico y Documentación - Cisco Systems