Uso del Protocolo SDI y del Servidor Token RSA para ASA y ACS

Contenido

Introducción

Este documento describe los procedimientos de solución de problemas para el administrador de autenticación RSA, que se pueden integrar con el dispositivo de seguridad adaptable (ASA) de Cisco y el servidor de control de acceso seguro (ACS) de Cisco.

RSA Authentication Manager es una solución que proporciona la contraseña única (OTP) para la autenticación. Esa contraseña se cambia cada 60 segundos y sólo se puede utilizar una vez. Admite tokens de hardware y software.

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos básicos sobre estos temas:

- configuración CLI de Cisco ASA
- configuración de Cisco ACS

Componentes Utilizados

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

- Software Cisco ASA, versión 8.4 y posteriores
- Cisco Secure ACS, versión 5.3 y posteriores

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.

Teoría

Se puede acceder al servidor RSA con RADIUS o el protocolo RSA propietario: SDI. Tanto el ASA como el ACS pueden utilizar ambos protocolos (RADIUS, SDI) para acceder al RSA.

Recuerde que RSA se puede integrar con Cisco AnyConnect Secure Mobility Client cuando se utiliza un token de software. Este documento se centra únicamente en la integración de ASA y ACS. Para obtener más información sobre AnyConnect, consulte la sección Uso de la Autenticación SDI de la Guía del Administrador de Cisco AnyConnect Secure Mobility Client, versión 3.1.

RSA a través de RADIUS

RADIUS tiene una gran ventaja sobre SDI. En RSA, es posible asignar perfiles específicos (llamados grupos en ACS) a los usuarios. Esos perfiles tienen atributos RADIUS específicos definidos. Después de una autenticación exitosa, el mensaje RADIUS-Accept devuelto desde el RSA contiene esos atributos. Sobre la base de esos atributos, el ACS toma decisiones adicionales. El escenario más común es la decisión de utilizar el mapeo de grupo ACS para mapear atributos RADIUS específicos, relacionados con el perfil en el RSA, a un grupo específico en el ACS. Con esta lógica, es posible mover todo el proceso de autorización de RSA a ACS y mantener la lógica granular, como en el RSA.

RSA vía SDI

SDI tiene dos ventajas principales sobre RADIUS. La primera es que toda la sesión está cifrada. El segundo es las opciones interesantes que proporciona el agente SDI: puede determinar si se ha creado la falla porque la autenticación o la autorización fallaron o porque no se encontró al usuario.

Esta información es utilizada por el ACS en acción para la identidad. Por ejemplo, podría continuar con "el usuario no se encontró" pero rechazar por "la autenticación falló".

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

Protocolo SDI

De forma predeterminada, SDI utiliza el protocolo de datagramas de usuario (UDP) 5500. SDI utiliza una clave de cifrado simétrica, similar a la clave RADIUS, para cifrar sesiones. Esa clave se guarda en un archivo secreto de nodo y es diferente para cada cliente SDI. Ese archivo se implementa de forma manual o automática.

> **Nota:** ACS/ASA no admite la implementación manual.

Para el nodo de implementación automática, el archivo secreto se descarga automáticamente después de la primera autenticación correcta. El secreto de nodo se cifra con una clave derivada del código de acceso del usuario y otra información. Esto crea algunos posibles problemas de seguridad, por lo que la primera autenticación debe realizarse localmente y utilizar el protocolo cifrado (Secure Shell [SSH], no Telnet) para asegurarse de que el atacante no pueda interceptar y descifrar ese archivo.

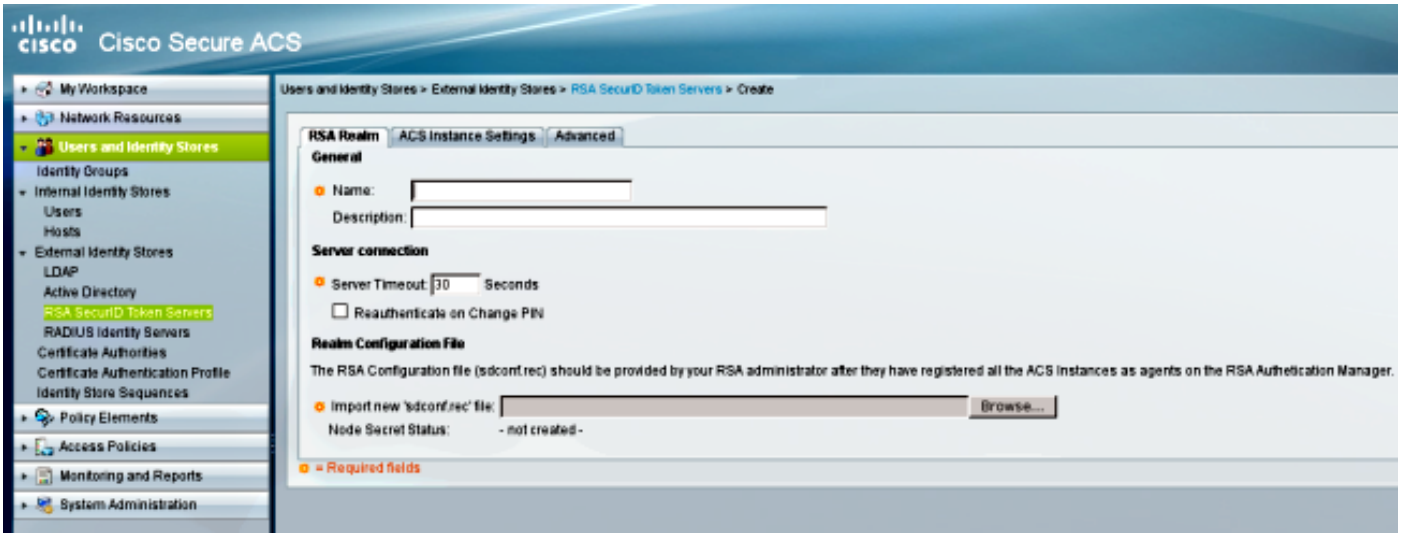
Configuración

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

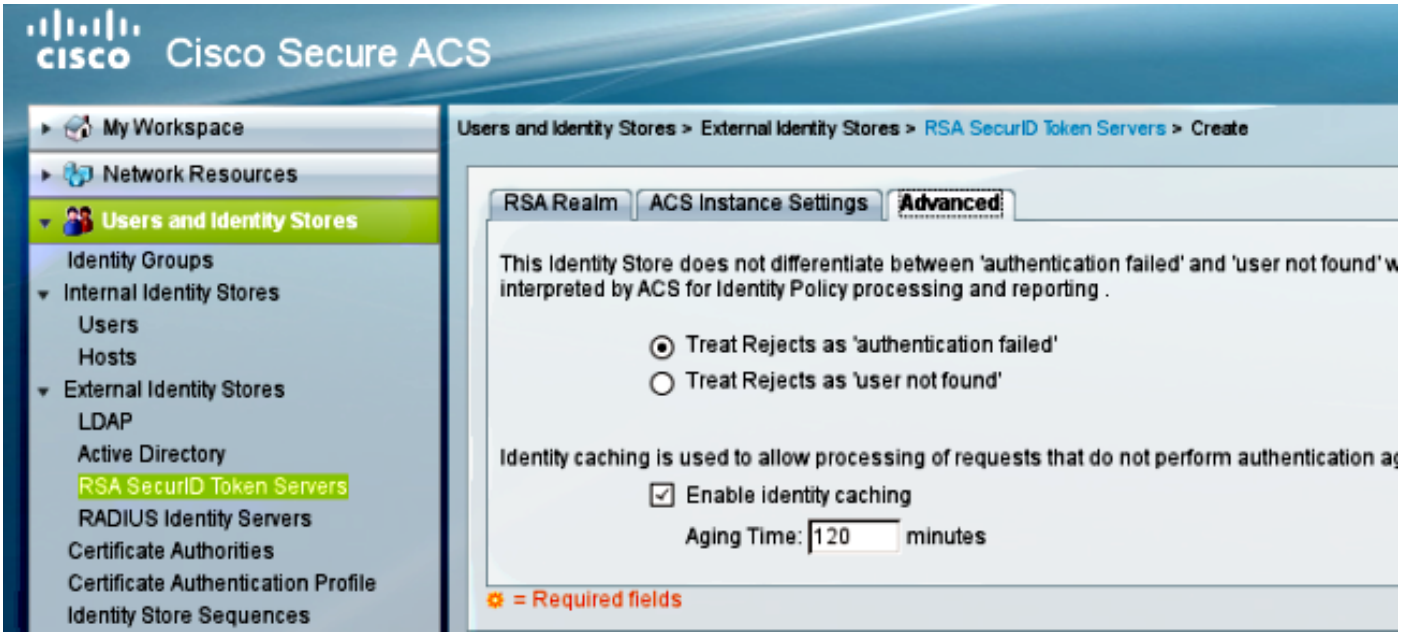
SDI en ACS

Se configura en **Usuarios y Almacenes de Identidad > Almacén de Identidad Externa > Servidores Token de ID Seguros RSA**.

El RSA tiene varios servidores de réplica, como los servidores secundarios para el ACS. No hay necesidad de poner todas las direcciones allí, sólo el archivo **sdconf.rec** proporcionado por el administrador RSA. Este archivo incluye la dirección IP del servidor RSA primario. Después del primer nodo de autenticación exitoso, el archivo secreto se descarga junto con las direcciones IP de todas las réplicas RSA.



Para diferenciar "usuario no encontrado" de "falla de autenticación", elija la configuración en la pestaña **Avanzado**:



También es posible cambiar los mecanismos de routing predeterminados (equilibrio de carga) entre varios servidores RSA (primarios y réplicas). Cámbielo con el archivo **sdopts.rec** proporcionado por el administrador RSA. En ACS, se carga en **Usuarios y Almacenes de Identidad > Almacén de Identidad Externa > Servidores Token de Id. Seguro RSA > Configuración de Instancia ACS**.

Para la implementación del clúster, la configuración debe replicarse. Después de la primera autenticación exitosa, cada nodo ACS utiliza su propio secreto de nodo descargado del servidor RSA primario. Es importante recordar configurar el RSA para todos los nodos ACS en el clúster.

SDI en ASA

El ASA no permite la carga del archivo **sdconf.rec**. Y, al igual que el ACS, permite la implementación automática solamente. El ASA debe configurarse manualmente para apuntar al servidor RSA primario. No se necesita una contraseña. Después del primer nodo de autenticación exitoso, se instala el archivo secreto (archivo .sdi en flash) y se protegen las sesiones de autenticación adicionales. También se descargan las direcciones IP de otros servidores RSA.

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 una autenticación exitosa, el comando **show aaa-server protocol sdi** o **show aaa-server <aaa-server-group>** muestra todos los servidores RSA (si hay más de uno), mientras que el comando **show run** muestra solamente la dirección IP primaria:

```
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
```

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

No hay configuración de agente en RSA

En muchos casos, después de instalar un nuevo ASA o cambiar la dirección IP de ASA, es fácil olvidar realizar los mismos cambios en el RSA. La dirección IP del agente en el RSA debe actualizarse para todos los clientes que acceden al RSA. A continuación, se genera el nuevo secreto de nodo. Lo mismo se aplica al ACS, especialmente a los nodos secundarios porque tienen diferentes direcciones IP y el RSA necesita confiar en ellos.

Nodo secreto dañado

A veces el archivo de nodo secreto en el ASA o RSA se daña. A continuación, es mejor quitar la configuración del agente en RSA y agregarla de nuevo. También debe realizar el mismo proceso en ASA/ACS: elimine y agregue la configuración de nuevo. Además, elimine el archivo .sdi en la memoria flash, de modo que en la siguiente autenticación se instale un nuevo archivo .sdi. Una vez que se complete esta implementación, se debe realizar una implementación automática de nodo secreto.

Nodo en modo suspendido

A veces uno de los nodos se encuentra en modo suspendido, lo que se debe a la ausencia de 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 paquetes a ese nodo; necesita tener un estado **OK** para eso. El servidor fallido se pone en modo activo nuevamente después del temporizador muerto. Para obtener más información, consulte la sección comando reactivation-mode en la Referencia de Comandos de Cisco ASA Series, guía 9.1.

En tales escenarios, es mejor quitar y agregar la configuración AAA-server para ese grupo para activar ese servidor nuevamente en el modo activo.

Cuenta bloqueada

Después de varios reintentos, RSA podría bloquear la cuenta. Se verifica fácilmente en el RSA

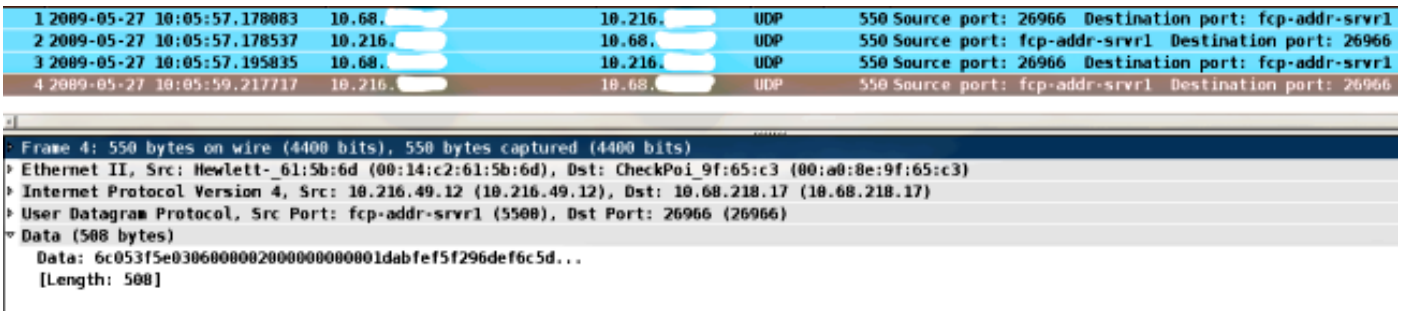
con informes. En ASA/ACS, los informes sólo muestran "autenticación fallida".

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

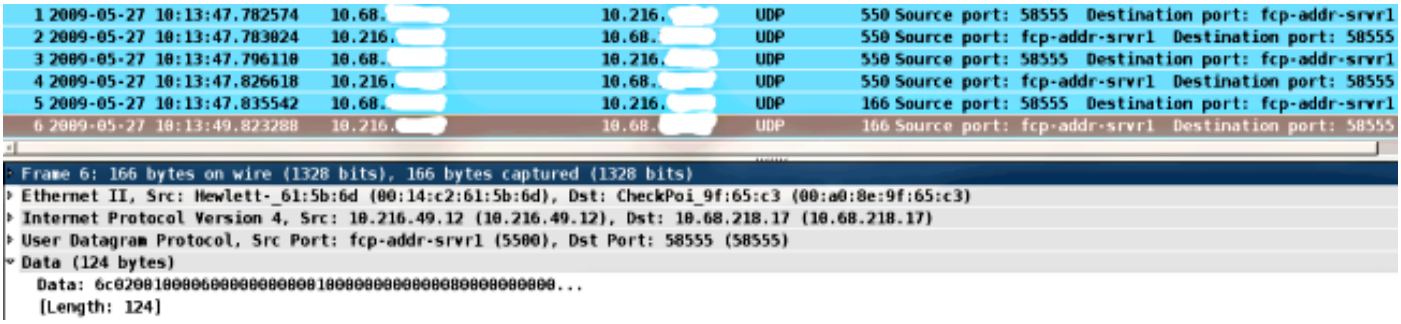
SDI utiliza UDP como transporte, no como detección de ruta MTU. Además, el tráfico UDP no tiene el bit Don't Fragment (DF) configurado de forma predeterminada. A veces, para los paquetes más grandes, puede haber problemas de fragmentación. Es fácil detectar el tráfico en RSA (tanto el dispositivo como la máquina virtual [VM] utilizan Windows y Wireshark). Complete el mismo proceso en ASA/ACS y compare. Además, pruebe RADIUS o WebAuthentication en el RSA para compararlo con SDI (para reducir el problema).

Paquetes y Debugs para ACS

Debido a que la carga útil SDI está cifrada, la única manera de resolver problemas de las capturas es comparar el tamaño de la respuesta. Si es menor a 200 bytes, podría haber un problema. Un intercambio SDI típico implica cuatro paquetes, cada uno de los cuales es de 550 bytes, pero que podría cambiar con la versión del servidor RSA:



En caso de problemas, suele haber más de cuatro paquetes intercambiados y tamaños más pequeños:



Además, los registros ACS son bastante claros. Estos son los registros SDI típicos en 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 de RSA Authentication Manager
- Sección Soporte de Servidor RSA/SDI de la Guía de Configuración de Cisco ASA 5500 Series con CLI, 8.4 y 8.6
- sección RSA SecurID Server de la Guía del Usuario para Cisco Secure Access Control System 5.4
- Soporte Técnico y Documentación - Cisco Systems