Uso do protocolo SDI e do servidor de token RSA para ASA e ACS

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Teoria](#)
[RSA via RADIUS](#)
[RSA via SDI](#)
[Protocolo SDI](#)
[Configuração](#)
[SDI no ACS](#)
[SDI no ASA](#)
[Troubleshoot](#)
[Nenhuma configuração de agente no RSA](#)
[Nó secreto corrompido](#)
[Nó em modo suspenso](#)
[Conta bloqueada](#)
[Problemas de MTU (Maximum Transition Unit, Unidade máxima de transição) e fragmentação](#)
[Pacotes e depurações para ACS](#)
[Informações Relacionadas](#)

Introduction

Este documento descreve os procedimentos de solução de problemas do RSA Authentication Manager, que pode ser integrado ao Cisco Adaptive Security Appliance (ASA) e ao Cisco Secure Access Control Server (ACS).

O RSA Authentication Manager é uma solução que fornece a senha única (OTP) para autenticação. Essa senha é alterada a cada 60 segundos e pode ser usada apenas uma vez. Suporta tokens de hardware e software.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento básico sobre estes tópicos:

- configuração do Cisco ASA CLI
- configuração do Cisco ACS

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Software Cisco ASA, versão 8.4 e posterior
- Cisco Secure ACS, Versão 5.3 e posterior

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.

Teoria

O servidor RSA pode ser acessado com RADIUS ou o protocolo RSA proprietário: SDI. O ASA e o ACS podem usar ambos os protocolos (RADIUS, SDI) para acessar o RSA.

Lembre-se de que o RSA pode ser integrado ao Cisco AnyConnect Secure Mobility Client quando um token de software é usado. Este documento concentra-se exclusivamente na integração do ASA e do ACS. Para obter mais informações sobre o AnyConnect, consulte a seção Uso da autenticação SDI do Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.1.

RSA via RADIUS

O RADIUS tem uma grande vantagem sobre o SDI. No RSA, é possível atribuir perfis específicos (chamados de grupos no ACS) aos usuários. Esses perfis têm atributos RADIUS específicos definidos. Após a autenticação bem-sucedida, a mensagem RADIUS-Accept retornada do RSA contém esses atributos. Com base nesses atributos, o ACS toma decisões adicionais. O cenário mais comum é a decisão de usar o mapeamento de grupo ACS para mapear atributos RADIUS específicos, relacionados ao perfil no RSA, para um grupo específico no ACS. Com essa lógica, é possível mover todo o processo de autorização do RSA para o ACS e ainda manter a lógica granular, como no RSA.

RSA via SDI

O SDI tem duas vantagens principais sobre o RADIUS. A primeira é que toda a sessão é criptografada. A segunda são as opções interessantes que o agente SDI oferece: ele pode determinar se a falha foi criada porque a autenticação ou a autorização falhou ou porque o usuário não foi encontrado.

Essas informações são usadas pelo ACS em ação para identificação. Por exemplo, ele pode continuar para "usuário não encontrado", mas rejeitar para "falha na autenticação".

Há mais uma diferença entre RADIUS e SDI. Quando um dispositivo de acesso à rede como o ASA usa SDI, o ACS executa somente a autenticação. Quando usa RADIUS, o ACS executa autenticação, autorização, contabilização (AAA). Mas não é uma grande diferença. É possível configurar SDI para autenticação e RADIUS para contabilização das mesmas sessões.

Protocolo SDI

Por padrão, o SDI usa o User Datagram Protocol (UDP) 5500. O SDI usa uma chave de criptografia simétrica, semelhante à chave RADIUS, para criptografar sessões. Essa chave é salva em um arquivo secreto de nó e é diferente para cada cliente SDI. Esse arquivo é implantado manual ou automaticamente.

> **Note**: O ACS/ASA não oferece suporte à implantação manual.

Para o nó de implantação automática, o arquivo secreto é baixado automaticamente após a primeira autenticação bem-sucedida. O segredo do nó é criptografado com uma chave derivada da senha do usuário e outras informações. Isso cria alguns possíveis problemas de segurança, portanto, a primeira autenticação deve ser executada localmente e usar o protocolo criptografado (Secure Shell [SSH], não telnet) para garantir que o invasor não possa interceptar e descriptografar esse arquivo.

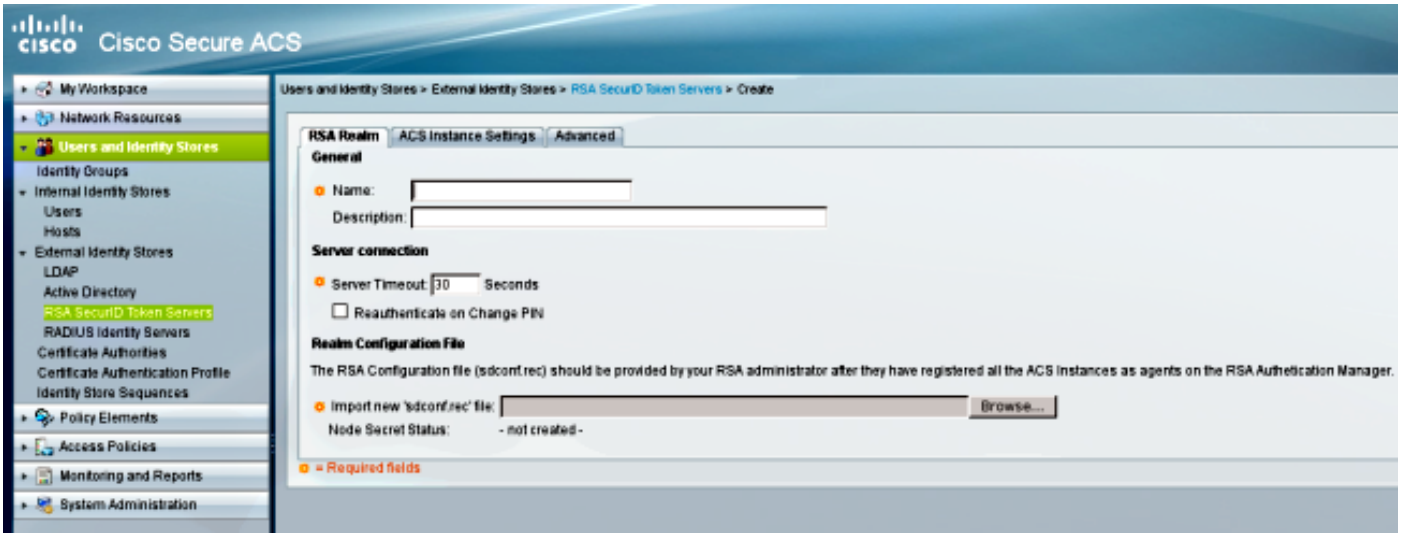
Configuração

> **Notas:**
>
> Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.
>
> A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..
>
> Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug.**

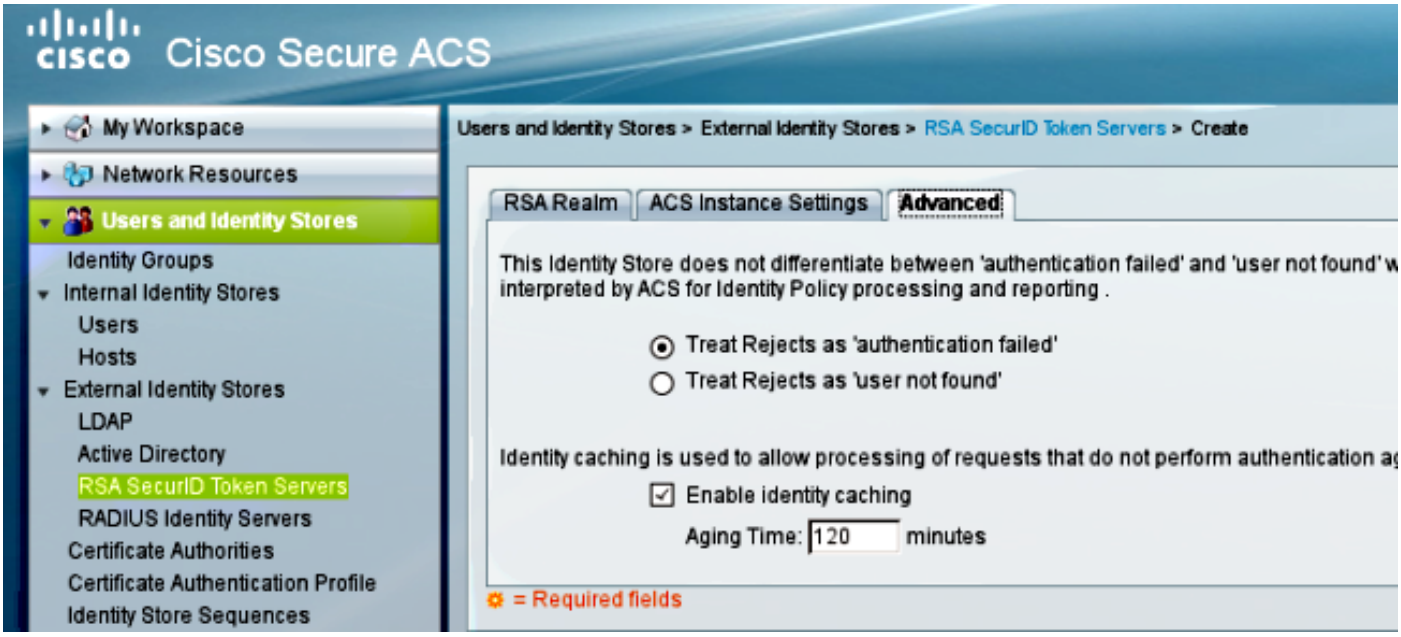
SDI no ACS

Ele é configurado em **Usuários e Repositórios de Identidades > Repositório de Identidades Externas > Servidores de Token de Identificação Segura RSA**.

O RSA tem vários servidores de réplica, como os servidores secundários para o ACS. Não há necessidade de colocar todos os endereços lá, apenas o arquivo **sdconf.rec** fornecido pelo administrador RSA. Esse arquivo inclui o endereço IP do servidor RSA primário. Após o primeiro nó de autenticação bem-sucedido, o arquivo secreto é baixado junto com os endereços IP de todas as réplicas RSA.



Para diferenciar "usuário não encontrado" de "falha de autenticação", escolha as configurações na guia **Avançado**:



Também é possível alterar os mecanismos de roteamento padrão (balanceamento de carga) entre vários servidores RSA (primários e réplicas). Altere-o com o arquivo **sdopts.rec** fornecido pelo administrador RSA. No ACS, ele é carregado em **Usuários e Repositórios de Identidades > Repositório de Identidades Externas > Servidores de Token de Identificação Segura RSA > Configurações de Instância ACS**.

Para implantação de cluster, a configuração deve ser replicada. Após a primeira autenticação bem-sucedida, cada nó ACS usa seu próprio segredo de nó baixado do servidor RSA primário. É importante lembrar de configurar o RSA para todos os nós ACS no cluster.

SDI no ASA

O ASA não permite o upload do arquivo **sdconf.rec**. E, como o ACS, ele permite apenas a implantação automática. O ASA precisa ser configurado manualmente para apontar para o servidor RSA primário. Não é necessária uma senha. Após o primeiro nó de autenticação bem-sucedido, o arquivo secreto é instalado (arquivo .sdi na flash) e outras sessões de autenticação são protegidas. Além disso, o endereço IP de outros servidores RSA é baixado.

Aqui está um exemplo:

```
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
```

Após a autenticação bem-sucedida, o **comando show aaa-server protocol sdi** ou **show aaa-server <aaa-server-group>** mostra todos os servidores RSA (se houver mais de um), enquanto o comando **show run** mostra apenas o endereço IP 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
```

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Nenhuma configuração de agente no RSA

Em muitos casos, após instalar um novo ASA ou alterar o endereço IP do ASA, é fácil esquecer fazer as mesmas alterações no RSA. O endereço IP do agente no RSA precisa ser atualizado para todos os clientes que acessam o RSA. Em seguida, o novo segredo do nó é gerado. O mesmo se aplica ao ACS, especialmente aos nós secundários porque eles têm endereços IP diferentes e o RSA precisa confiar neles.

Nó secreto corrompido

Às vezes, o arquivo de nó secreto no ASA ou no RSA é corrompido. Em seguida, é melhor remover a configuração do agente no RSA e adicioná-la novamente. Você também precisa fazer o mesmo processo no ASA/ACS - remover e adicionar a configuração novamente. Além disso, exclua o arquivo .sdi na memória flash para que, na próxima autenticação, um novo arquivo .sdi seja instalado. A implantação automática de segredo de nó deve ocorrer quando isso for concluído.

Nó em modo suspenso

Às vezes, um dos nós está em modo suspenso, o que é causado por nenhuma resposta desse 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
```

No modo suspenso, o ASA não tenta enviar nenhum pacote para esse nó; ele precisa ter um status **OK** para isso. O servidor com falha é colocado no modo ativo novamente após o temporizador inoperante. Para obter mais informações, consulte a seção de comando do modo de reativação no Guia de referência de comando do Cisco ASA Series, 9.1.

Nesses cenários, é melhor remover e adicionar a configuração do servidor AAA para esse grupo para disparar esse servidor para o modo ativo novamente.

Conta bloqueada

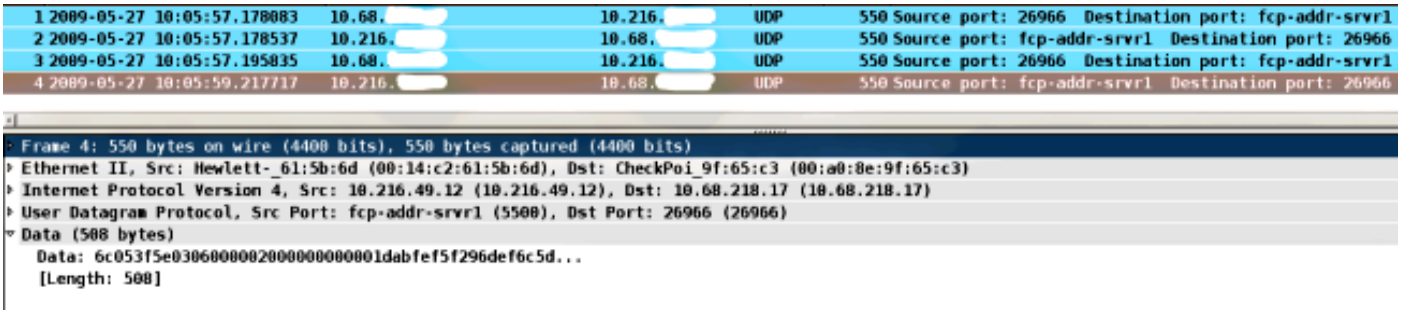
Após várias tentativas, o RSA pode bloquear a conta. Ele é facilmente verificado no RSA com relatórios. No ASA/ACS, os relatórios mostram apenas "falha na autenticação".

Problemas de MTU (Maximum Transition Unit, Unidade máxima de transição) e fragmentação

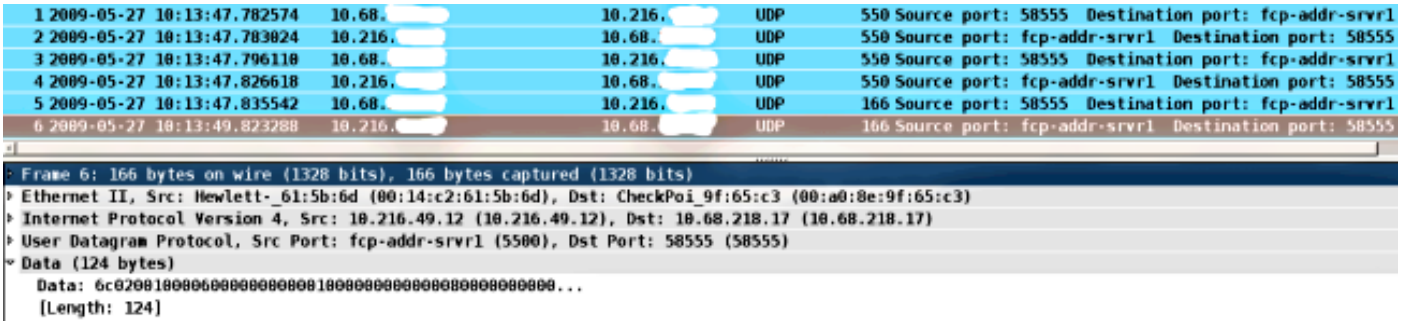
O SDI usa UDP como transporte, não como descoberta de caminho MTU. Além disso, o tráfego UDP não tem o bit Don't Fragment (DF) definido por padrão. Às vezes, para pacotes maiores, pode haver problemas de fragmentação. É fácil detectar tráfego no RSA (tanto o dispositivo quanto a máquina virtual [VM] usam o Windows e o Wireshark). Conclua o mesmo processo no ASA/ACS e compare. Além disso, teste RADIUS ou WebAuthentication no RSA para compará-lo ao SDI (para restringir o problema).

Pacotes e depurações para ACS

Como o payload de SDI é criptografado, a única maneira de solucionar os problemas das capturas é comparar o tamanho da resposta. Se for menor que 200 bytes, pode haver um problema. Uma troca SDI típica envolve quatro pacotes, cada um com 550 bytes, mas isso pode mudar com a versão do servidor RSA:



Em caso de problemas, geralmente são mais de quatro pacotes trocados e tamanhos menores:



Além disso, os registros do ACS são bastante claros. Aqui estão os registros SDI típicos no 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
```

Informações Relacionadas

- Recursos do RSA Authentication Manager
- Seção Suporte ao servidor RSA/SDI do Guia de Configuração do Cisco ASA 5500 Series usando CLI, 8.4 e 8.6
- Seção RSA SecurID Server do Guia do usuário do Cisco Secure Access Control System 5.4
- Suporte Técnico e Documentação - Cisco Systems