Servidor de tokens RSA e de protocolo SDI uso para o ASA e o ACS

Índice

Introdução

Este documento descreve procedimentos de Troubleshooting para o gerente da autenticação de RSA, que pode ser integrado com a ferramenta de segurança adaptável de Cisco (ASA) e o Serviço de controle de acesso Cisco Secure (ACS).

O gerente da autenticação de RSA é uma solução que forneça a uma senha do tempo (OTP) para a autenticação. Que a senha está mudada cada 60 segundos e pode ser usada somente uma vez. Apoia ambos os tokens do hardware e software.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento básico destes assuntos:

- Configuração de CLI de Cisco ASA
- Configuração ACS de Cisco

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Software de Cisco ASA, versão 8.4 e mais recente
- Cisco Secure ACS, versão 5.3 e mais recente

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Teoria

O server RSA pode ser alcançado com RAIO ou o protocolo proprietário RSA: SDI. o ASA e o ACS podem usar ambos os protocolos (RAIO, SDI) a fim alcançar o RSA.

Recorde que o RSA pode ser integrado com o Cliente de mobilidade Cisco AnyConnect Secure quando um token de software for usado. Este documento centra-se unicamente sobre a integração ASA e ACS. Para obter mais informações sobre de AnyConnect, refira a seção de utilização da Autenticação SDI do guia do administrador do Cliente de mobilidade Cisco AnyConnect Secure, a liberação 3.1.

RSA através do RAIO

O RAIO tem uma vantagem grande sobre o SDI. No RSA, é possível atribuir os perfis específicos (chamados grupos no ACS) aos usuários. Aqueles perfis têm os atributos RADIUS específicos definidos. Após a autenticação bem sucedida, a mensagem da Raio-aceitação retornada do RSA contém aqueles atributos. Baseado naqueles atributos, o ACS faz decisões adicionais. A maioria de cenário comum é a decisão para usar o mapeamento do grupo ACS a fim traçar os atributos RADIUS específicos, relativos ao perfil no RSA, a um grupo específico no ACS. Com esta lógica, é possível mover o processo inteiro da autorização do RSA para o ACS e manter ainda a lógica granulada, como no RSA.

RSA através do SDI

O SDI tem duas vantagens principal sobre o RAIO. O primeiro é que a sessão inteira está cifrada. O segundo é as opções interessantes que o agente SDI fornece: pode determinar se a falha é criada porque a autenticação ou a autorização falharam ou porque o usuário não foi encontrado.

Esta informação é usada pelo ACS na ação para a identidade. Por exemplo, poderia continuar para o “usuário não encontrado” mas a rejeição para a “autenticação falhou.”

Há uma mais diferença entre o RAIO e o SDI. Quando um dispositivo do acesso de rede como o ASA usa o SDI, o ACS executa somente a autenticação. Quando usa o RAIO, o ACS executa a autenticação, autorização, explicando (AAA). Contudo, esta não é uma diferença grande. É possível configurar o SDI para a autenticação e o RAIO para esclarecer as mesmas sessões.

Protocolo SDI

Àrevelia, o SDI usa o User Datagram Protocol (UDP) 5500. O SDI usa uma chave de criptografia simétrica, similar à chave do RAIO, a fim cifrar sessões. Que a chave salvar em um arquivo do segredo de nó e é diferente para cada cliente de SDI. Esse arquivo é distribuído manualmente ou automaticamente.

> Nota: ACS/ASA não apoia o desenvolvimento manual.

Para o nó automático do desenvolvimento, o arquivo secreto é transferido automaticamente após a primeira autenticação bem sucedida. O segredo de nó é cifrado com uma chave derivada da outra informação do usuário da senha e. Isto cria algumas questões de segurança possíveis, assim que a primeira autenticação deve ser executada localmente e protocolo cifrado uso ([SSH], não telnet do Secure Shell) a fim assegurar-se de que o atacante não possa interceptar e decifrar esse arquivo.

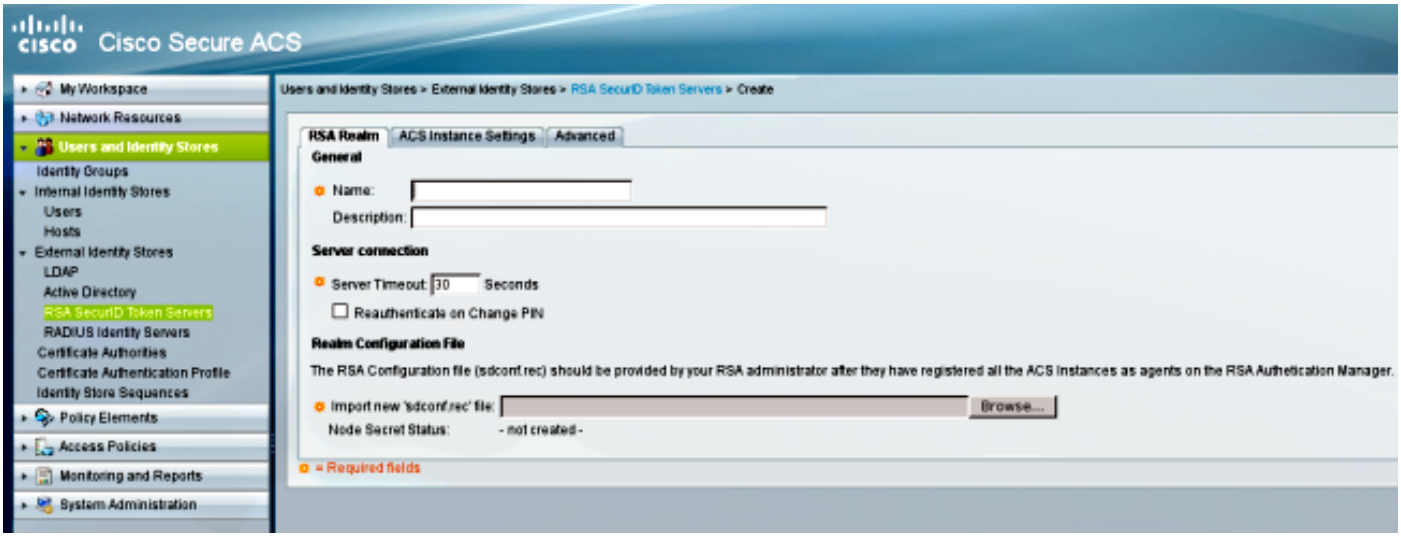
Configuração

> Notas:
>
> Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.
>
> A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.
>
> Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

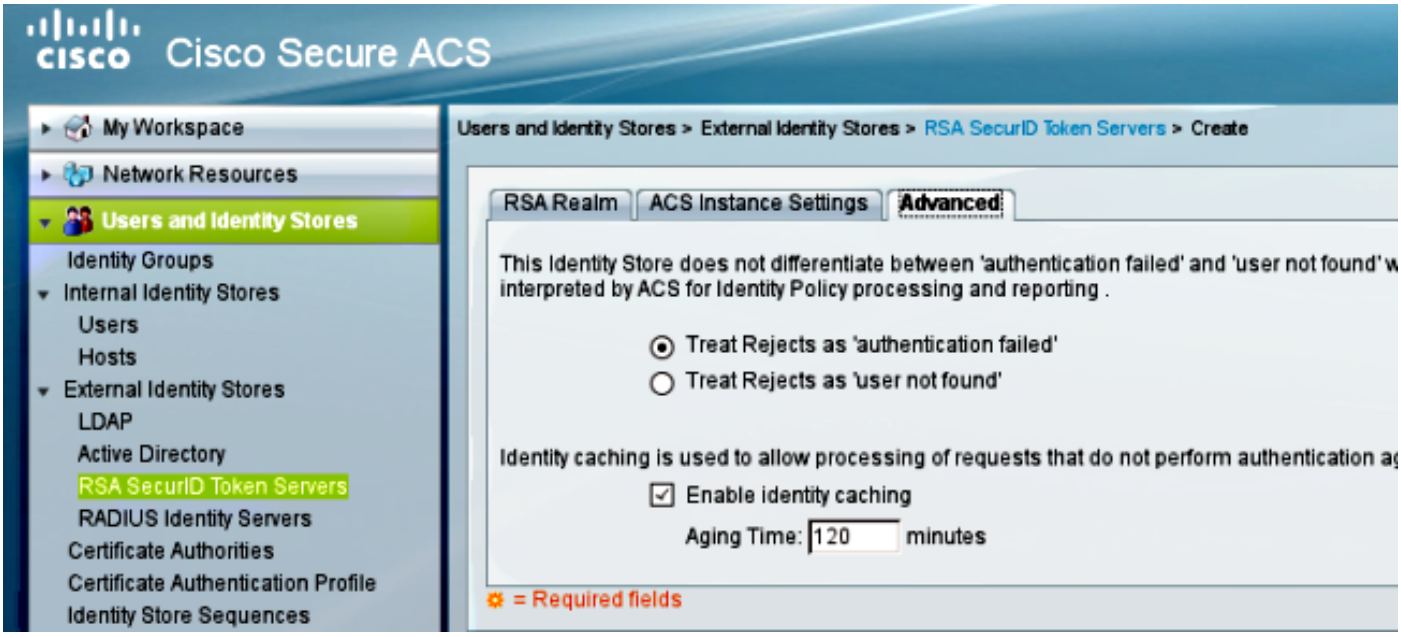
SDI no ACS

Éconfigurado nos **usuários e a identidade armazena > loja externo da identidade > de Secure ID RSA servidores de tokens**.

O RSA tem servidores de réplica múltiplos, tais como os servidores secundários para o ACS. Não há nenhuma necessidade de pôr lá todos os endereços, apenas o **arquivo sdconf.rec** fornecido pelo administrador RSA. Este arquivo inclui o endereço IP de Um ou Mais Servidores Cisco ICM NT do server preliminar RSA. Após o primeiro nó da autenticação bem sucedida, o arquivo secreto é transferido junto com os endereços IP de Um ou Mais Servidores Cisco ICM NT de todas as réplicas RSA.



A fim diferenciar o “usuário não encontrado” da “falha de autenticação,” escolhe ajustes no **guia avançada**:



Éigualmente possível mudar os mecanismos do roteamento padrão (Balanceamento de carga) entre os server múltiplos RSA (preliminares e réplicas). Mude-o com o **arquivo sdopts.rec** fornecido pelo administrador RSA. No ACS, é transferido arquivos pela rede em **lojas da identidade de** Usersand **> loja externo da identidade > de Secure ID RSA servidores de tokens > de exemplo ACS ajustes.**

Para o desenvolvimento do conjunto, a configuração deve ser replicated. Após a primeira autenticação bem sucedida, cada nó ACS usa seu próprio segredo de nó transferido do server preliminar RSA. É importante recordar configurar o RSA para todos os Nós ACS no conjunto.

SDI no ASA

O ASA não permite a transferência de arquivo pela rede do **arquivo sdconf.rec**. E, como o ACS, permite o desenvolvimento automático somente. O ASA precisa de ser configurado manualmente a fim apontar ao server preliminar RSA. Uma senha não é precisada. Após o primeiro nó da autenticação bem sucedida, o arquivo secreto é instalado (arquivo .sdi no flash) e umas sessões mais adicionais da autenticação são protegidas. O endereço IP de Um ou Mais Servidores Cisco

ICM NT de outros server RSA é transferido igualmente.

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 **protocolo sdi do AAA-server da mostra** ou o comando do **<aaa-server-group> do AAA-server da mostra** mostram todos os server RSA (se há mais de um), quando o **comando show run** mostrar somente o endereço IP primário:

```
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 seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

Nenhuma configuração de agente no RSA

Em muitos casos depois que você instala um ASA novo ou muda o endereço IP de Um ou Mais Servidores Cisco ICM NT ASA, é fácil esquecer fazer as mesmas mudanças no RSA. O endereço IP de Um ou Mais Servidores Cisco ICM NT do agente no RSA precisa de ser atualizado para todos os clientes que alcançam o RSA. Então, o segredo do novo nó é gerado. O mesmo aplica-se ao ACS, especialmente aos Nós secundários porque tem endereços IP de Um ou Mais Servidores Cisco ICM NT diferentes e o RSA precisa dos confiar.

Nó secreto corrompido

Às vezes o arquivo secreto do nó no ASA ou no RSA torna-se corrompido. Então, é o melhor remover a configuração de agente no RSA e adicionar-la outra vez. Você igualmente precisa de fazer o mesmo processo no ASA/ACS - remova e adicionar a configuração outra vez. Também, suprima do arquivo .sdi no flash, de modo que na autenticação seguinte, um arquivo novo .sdi seja instalado. O desenvolvimento automático do segredo de nó deve ocorrer uma vez que este está completo.

Nó no modo suspendido

Às vezes um dos Nós reage do modo suspendido, que é causado por nenhuma resposta desse 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
```

No modo suspendido, o ASA não tenta enviar nenhuns pacotes a esse nó; precisa de ter um estado **APROVADO** para aquele. O servidor falho é posto no modo ativo outra vez após o temporizador inoperante. Para mais informação, refira o comando section reactivation-MODE na referência de comandos da série de Cisco ASA, o guia 9.1.

Em tais encenações, é o melhor remover e adicionar a configuração do servidor AAA para esse grupo a fim provocar outra vez esse server no modo ativo.

Conta travada

Depois que múltiplo as novas tentativas, o RSA puderam travar fora da conta. Verifica-se

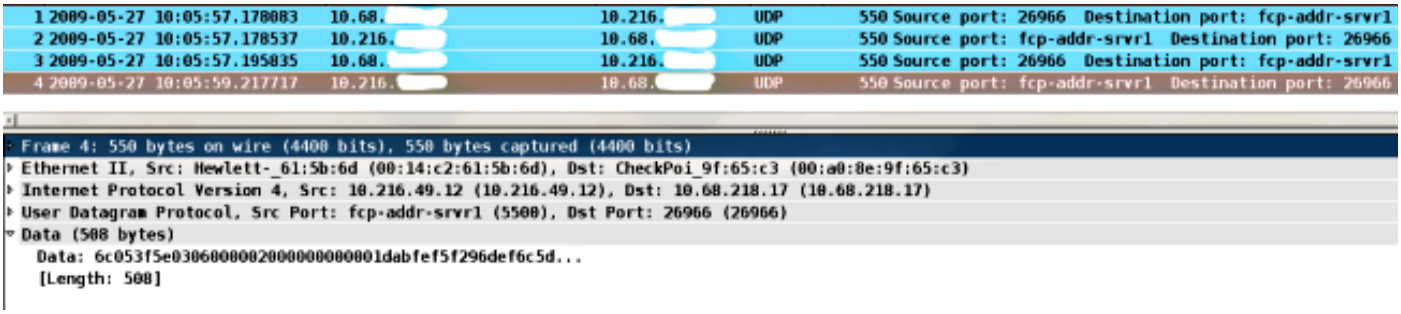
facilmente no RSA com os relatórios. No ASA/ACS, os relatórios mostram somente a “autenticação falha.”

Edições e fragmentação máximas da unidade da transição (MTU)

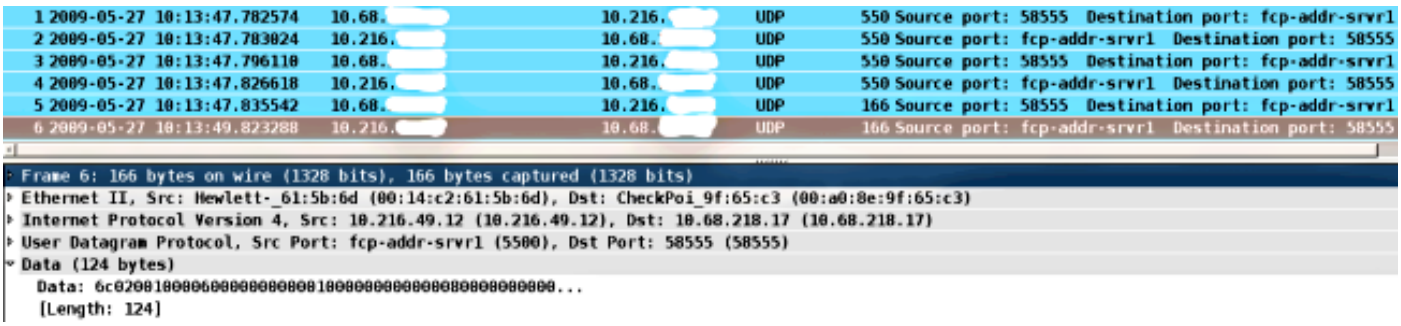
O SDI usa o UDP como o transporte, não descoberta de caminho MTU. Igualmente o tráfego UDP não tem don't fragment (DF) o jogo do bit à revelia. Às vezes para pacotes maiores, pôde haver uns problemas de fragmentação. É fácil aspirar o tráfego no [VM] RSA (o dispositivo e a máquina virtual usam Windows e usam Wireshark). Termine o mesmo processo no ASA/ACS e compare-o. Também, RAIO do teste ou WebAuthentication no RSA a fim compará-lo ao SDI (a fim reduzir para baixo o problema).

Os pacotes e debugam para o ACS

Porque o payload SDI é cifrado, a única maneira de pesquisar defeitos as captações é comparar o tamanho da resposta. Se é menor de 200 bytes, pôde haver um problema. Uma troca típica SDI envolve quatro pacotes, cada qual seja 550 bytes, mas aquela pôde mudar com a versão de servidor RSA:



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



Também, os logs ACS são bastante claros. Está aqui o SDI típico entra o 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 gerente da autenticação de RSA
- Seção do suporte de servidor RSA/SDI do manual de configuração do 5500 Series de Cisco ASA usando o CLI, os 8.4 e os 8.6
- Seção do server do SecurID RSA do Guia do Usuário para o Cisco Secure Access Control System 5.4
- Suporte Técnico e Documentação - Cisco Systems