ASA和ACS的RSA令牌服务器和SDI协议使用

目录

简介

本文档介绍RSA身份验证管理器的故障排除步骤，该管理器可与思科自适应安全设备(ASA)和思科安全访问控制服务器(ACS)集成。

RSA身份验证管理器是提供一次性密码(OTP)进行身份验证的解决方案。该密码每60秒更改一次，只能使用一次。它支持硬件和软件令牌。

先决条件

要求

Cisco 建议您具有以下主题的基础知识：

- Cisco ASA CLI 配置
- Cisco ACS配置

使用的组件

本文档中的信息基于以下软件版本：

- Cisco ASA软件8.4版及更高版本
- 思科安全ACS 5.3版及更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

理论

RSA服务器可以使用RADIUS或专有RSA协议访问：SDI。ASA和ACS都可以使用两种协议(RADIUS、SDI)来访问RSA。

请记住，当使用软件令牌时，RSA可与Cisco AnyConnect安全移动客户端集成。本文档仅重点介绍ASA和ACS集成。有关AnyConnect的详细信息，请参阅《Cisco AnyConnect安全移动客户端管理员指南，版本3.1》的使用SDI身份验证部分。

通过RADIUS的RSA

RADIUS与SDI相比有一大优势。在RSA上，可以将特定配置文件（在ACS上称为组）分配给用户。这些配置文件定义了特定RADIUS属性。身份验证成功后，从RSA返回的RADIUS-Accept消息包含这些属性。ACS根据这些属性做出其他决策。最常见的情况是决定使用ACS组映射，以将与RSA上的配置文件相关的特定RADIUS属性映射到ACS上的特定组。利用此逻辑，可以将整个授权过程从RSA移到ACS，并仍然像在RSA上那样维护精细逻辑。

通过SDI的RSA

SDI与RADIUS相比有两个主要优势。第一个是整个会话已加密。第二个是SDI代理提供的有趣选项：它能够确定是否因身份验证或授权失败或未找到用户而创建故障。

ACS使用此信息进行身份识别。例如，它可以继续为“user not found”，但拒绝为“authentication failed”。

RADIUS和SDI之间还有一个区别。当网络接入设备（如ASA）使用SDI时，ACS仅执行身份验证。当使用RADIUS时，ACS执行身份验证、授权、记帐(AAA)。 然而，这并不是什么大区别。可以为身份验证配置SDI，为相同会话配置RADIUS。

SDI协议

默认情况下，SDI使用用户数据报协议(UDP)5500。SDI使用对称加密密钥（类似于RADIUS密钥）来加密会话。该密钥保存在节点加密文件中，并且每个SDI客户端都不同。该文件是手动或自动部署的。

注意：ACS/ASA不支持手动部署。

对于自动部署节点，在第一次成功身份验证后自动下载加密文件。使用从用户的密码和其他信息派生的密钥对节点密钥进行加密。这会产生一些可能的安全问题，因此，第一次身份验证应在本地执行并使用加密协议（Secure Shell [SSH]，而不是telnet），以确保攻击者无法拦截和解密该文件。

配置

注意：

使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

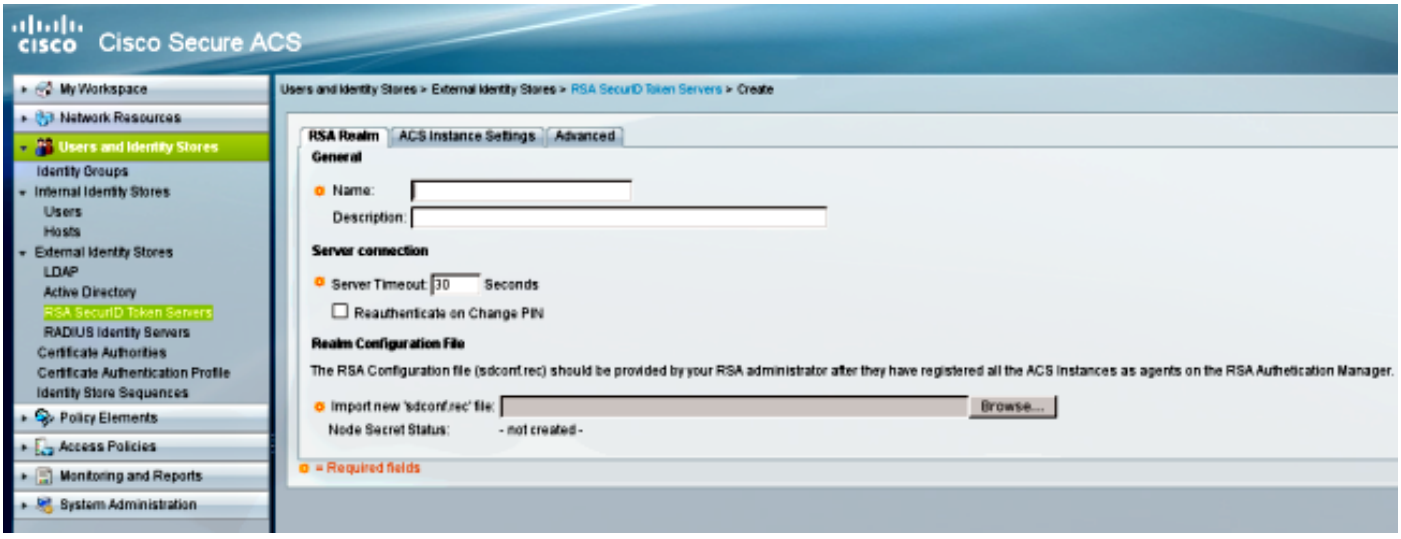
命令输出解释程序工具（仅限注册用户）支持某些 show 命令。使用输出解释器工具来查看 show 命令输出的分析。

使用 **debug 命令之前，请参阅**有关 Debug 命令的重要信息。

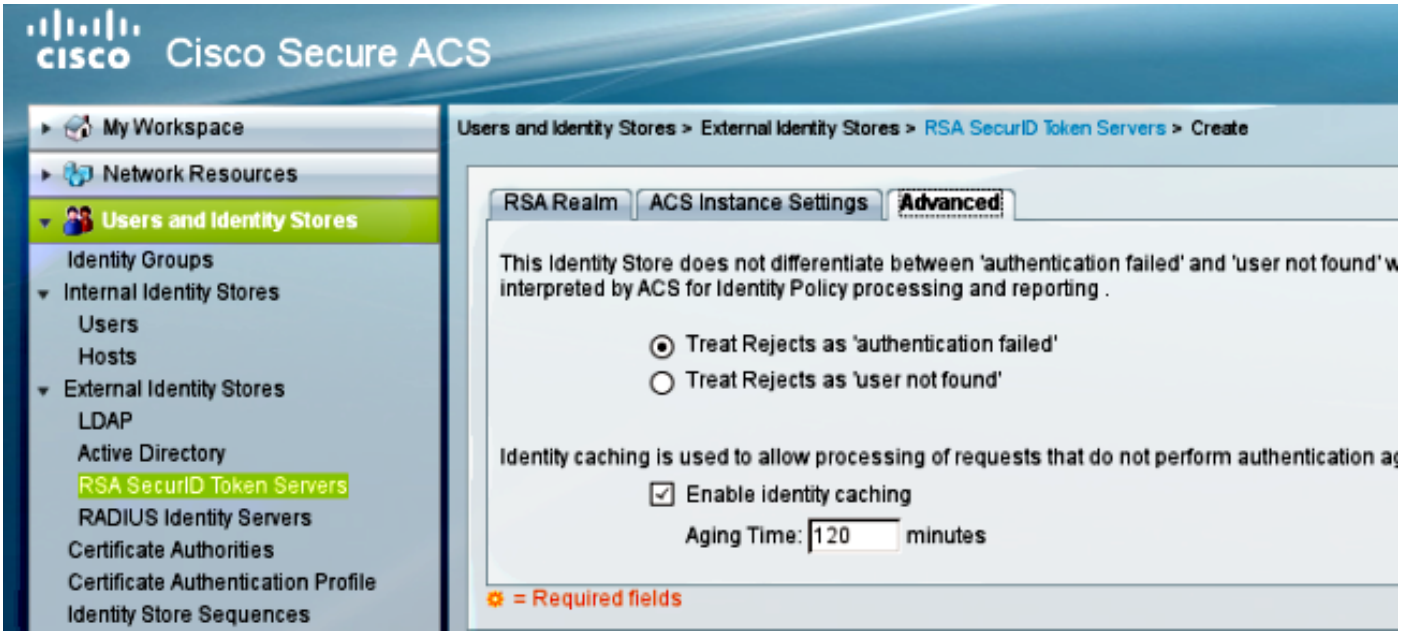
ACS上的SDI

它在用户和身**份库>外部身份库> RSA安全ID令牌服务器中配置**。

RSA有多个副本服务器，例如ACS的辅助服务器。无需将所有地址放在那里，只需RSA管理员提供的**sdconf.rec**文件。此文件包括主RSA服务器的IP地址。在第一个成功的身份验证节点后，将下载加密文件以及所有RSA副本的IP地址。



要区分“user not found”和“authentication failure”，请在“Advanced”选项卡中选**择设置**：



还可以更改多个RSA服务器（主服务器和副本）之间的默认路由（负载均衡）机制。 使用RSA管理员提供的sdopts.rec文件更改它。在ACS中，它上载到“用户和身份库”(Users and Identity Stores)>“外部身份库”(External Identity Store)>“RSA安全ID令牌服务器”(RSA Secure ID Token Servers)>“ACS实例设置”(ACS Instance Settings)。

对于集群部署，应复制配置。首次成功进行身份验证后，每个ACS节点使用从主RSA服务器下载的自己的节点密钥。请务必为集群中的所有ACS节点配置RSA。

ASA上的SDI

ASA不允许上传sdconf.rec文件。与ACS一样，它仅允许自动部署。需要手动配置ASA以指向主RSA服务器。不需要密码。在第一个成功的身份验证节点后，将安装加密文件（闪存上的.sdi文件），并保护进一步的身份验证会话。此外，还会下载其他RSA服务器的IP地址。

示例如下：

```
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
```

成功进行身份验证后，**show aaa-server protocol sdi**或**show aaa-server <aaa-server-group>**命令显示所有RSA服务器（如果有多个），而**show run**命令仅显示主IP地址：

```
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
```

故障排除

本部分提供了可用于对配置进行故障排除的信息。

RSA上没有代理配置

在许多情况下，在安装新ASA或更改ASA IP地址后，很容易忘记对RSA进行相同的更改。RSA上的代理IP地址需要为访问RSA的所有客户端更新。然后，生成新节点密钥。这同样适用于ACS，尤其是辅助节点，因为它们具有不同的IP地址，而RSA需要信任它们。

损坏的加密节点

有时，ASA或RSA上的加密节点文件会损坏。然后，最好删除RSA上的代理配置并重新添加。您还需要在ASA/ACS上执行相同的流程 — 再次删除并添加配置。此外，删除闪存上的.sdi文件，以便在下次身份验证时安装新的.sdi文件。完成后，应进行自动节点加密部署。

处于暂停模式的节点

有时，其中一个节点处于挂起模式，这是由该服务器没有响应引起的：

```
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
```

在暂停模式下，ASA不会尝试向该节点发送任何数据包；它需要有OK状态。故障服务器在死计时器后再次进入活动模式。有关详细信息，请参阅《Cisco ASA系列命令参考9.1指南》中的reactivation-mode命令部分。

在这种情况下，最好删除并添加该组的AAA服务器配置，以便再次将该服务器触发到主用模式。

帐户已锁定

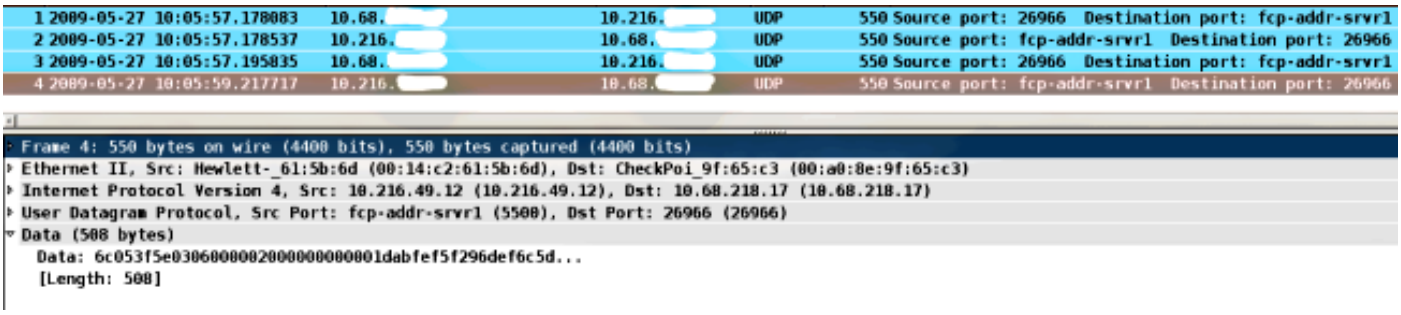
在多次重试后，RSA可能会锁定帐户。在RSA上使用报告轻松检查它。在ASA/ACS上，报告仅显示“失败的身份验证”。

最大转换单元(MTU)问题和分段

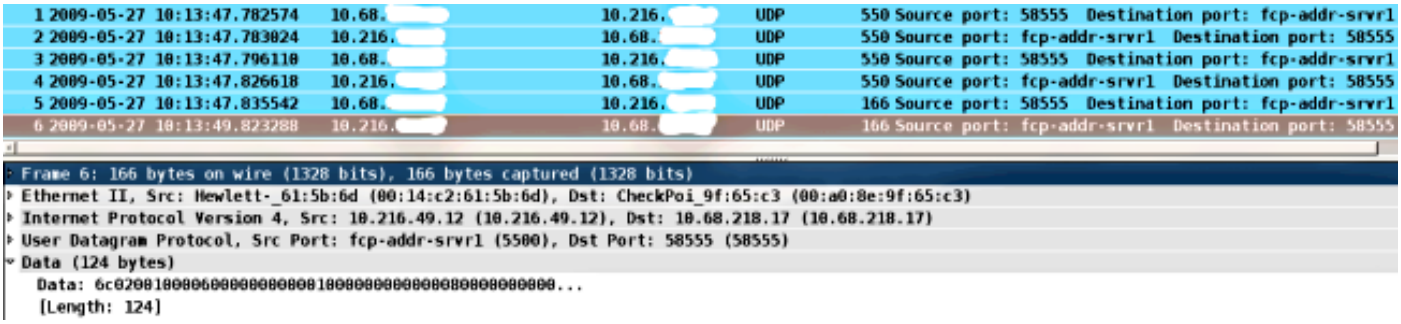
SDI使用UDP作为传输，而不是MTU路径发现。此外，UDP流量在默认情况下没有设置“不分段(DF)”位。有时，对于较大的数据包，可能会出现分段问题。在RSA上嗅探流量非常容易（设备和虚拟机[VM]都使用Windows并使用Wireshark）。 在ASA/ACS上完成相同的流程并进行比较。此外，在RSA上测试RADIUS或WebAuthentication，以将其与SDI进行比较（以缩小问题范围）。

ACS的数据包和调试

由于SDI负载已加密，因此排除捕获故障的唯一方法是比较响应的大小。如果小于200字节，则可能存在问题。典型的SDI交换涉及四个数据包，每个数据包为550字节，但随着RSA服务器版本的变化，这些数据包可能会改变：



在出现问题时，交换的数据包通常超过四个，且大小较小：



此外，ACS日志非常清晰。以下是ACS上的典型SDI日志：

```
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
```

相关信息

- RSA身份验证管理器资源
- 使用CLI、8.4和8.6的《Cisco ASA 5500系列配置指南》的“RSA/SDI服务器支持”部分
- 《思科安全访问控制系统用户指南5.4》的“RSA SecurID Server”部分

- 技术支持和文档 - Cisco Systems