RSA ASA和ACS的令牌服务器和SDI协议使用情况

目录

简介

本文描述RSA验证管理器的故障排除程序，可以用思科可适应安全工具(ASA)和思科安全访问控制服务器(ACS)集成。

RSA验证管理器是提供一个次密码的解决方案(OTP)为验证。密码更改每60秒，并且可以只一次使用。它支持两个硬件与软件令牌。

先决条件

要求

Cisco 建议您具有以下主题的基础知识：

- 思科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，版本8.4和以上
- Cisco Secure ACS，版本5.3和以上

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服务器可以访问与RADIUS或所有权RSA协议：SDI.ASA和ACS能使用两份协议(RADIUS，SDI)为了访问RSA。

切记RSA可以集成与Cisco AnyConnect安全移动客户端，当使用软件标记。本文独自地着重ASA和ACS集成。关于AnyConnect的更多信息，参考Cisco AnyConnect安全移动客户端管理员指南的使用的SDI Authentication部分，版本3.1。

RSA通过RADIUS

RADIUS有一个大优点超过SDI。在RSA，它是可能的分配特定配置文件(呼叫ACS的组)给用户。那些配置文件有定义的特定RADIUS属性。在成功认证以后，从RSA返回的RADIUS接受消息包含那些属性。凭那些属性， ACS做出另外的决策。多数常见情况是决策使用ACS组映射为了映射特定RADIUS属性，涉及与在RSA的配置文件，对ACS的一特定组。使用此逻辑，移动从RSA的整个授权进程向ACS和仍然维护粒状逻辑，和在RSA是可能的。

RSA通过SDI

SDI有两个主要优点超过RADIUS。第一是全部的会话加密。第二是该有趣的选项SDI代理程序提供：能确定失败是否创建，因为验证或授权失败或，因为未找到用户。

ACS使用此信息在操作标识。例如，它可能为“”验证失败的用户没找到”，但是拒绝继续”。

有在RADIUS和SDI之间的另外一个区别。当一网络接入设备类似ASA使用SDI时， ACS执行仅验证。当它使用RADIUS时， ACS执行验证，授权，认为(AAA)。然而，这不是大差值。配置验证的占的SDI和RADIUS同样会话是可能的。

SDI协议

默认情况下， SDI用途用户数据报协议(UDP) 5500。SDI使用一个对称加密密钥，类似于RADIUS密钥，为了加密会话。密钥在节点秘密文件保存并且为每个SDI客户端是不同的。该文件部

署手工或自动。

> **注意**：ACS/ASA不支持手工的部署。

对于自动部署节点，秘密文件在第一成功认证以后自动地下载。节点秘密加密与从用户的密码和其他信息派生的密钥。这创建一些可能的安全问题，因此应该执行第一验证本地和使用加密的协议(不是Secure Shell [SSH]， telnet)为了保证攻击者不能拦截和解密该文件。

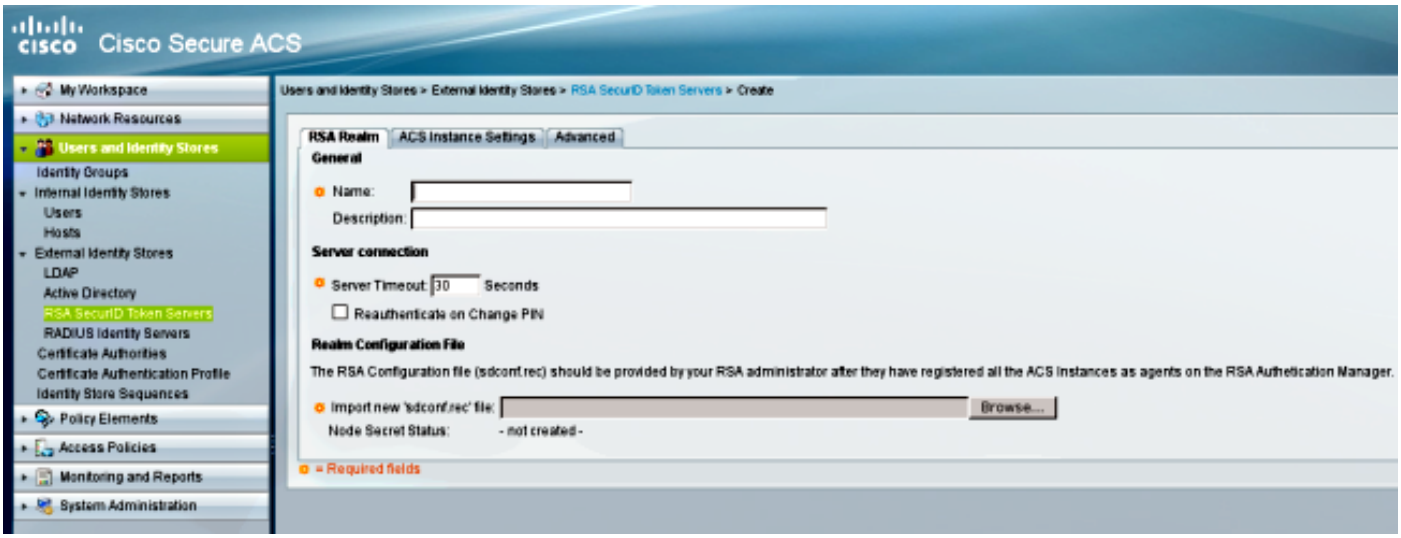
配置

> 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。请使用Output Interpreter Tool为了查看show命令输出分析。
>
> 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

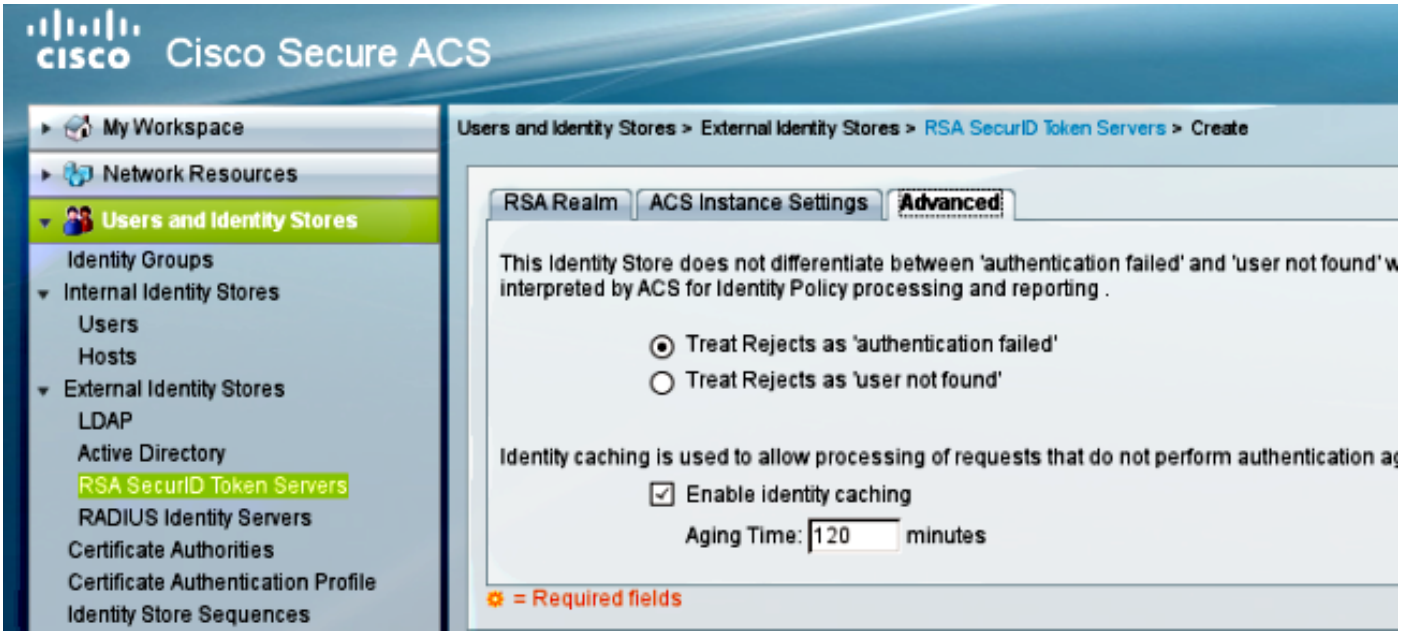
在ACS的SDI

它在**用户配置，并且标识存储>外部标识存储> RSA安全ID令牌服务器。**

RSA有多个复制品服务器，例如ACS的辅助服务器。没有需要放置所有地址那里， RSA管理员提供的**sdconf.rec文件**。此文件包括主要的RSA服务器的IP地址。在第一个成功认证节点以后，秘密文件与所有RSA复制品一起的IP地址下载。



为了区分“从“认证失败没找到的”用户”，请选择在**高级选项卡。的**设置：



更换在多个RSA服务器之间的默认路由(负载均衡)也是可能的机制(主要的和复制品)。随RSA管理员提供的**sdopts.rec文件**改变它。在ACS，它在Usersand**标识存储**上传**>外部标识存储> RSA安全ID令牌服务器> ACS实例设置。**

对于集群部署，应该复制配置。在第一成功认证以后，每个ACS节点使用从主要的RSA服务器下载的其自己的节点秘密。记住配置所有ACS节点的RSA在集群是重要的。

在ASA的SDI

ASA不允许**sdconf.rec文件的**加载。并且，类似ACS，它允许仅自动部署。ASA需要手工配置为了指向主要的RSA服务器。密码不是需要的。在第一个成功认证节点以后，秘密文件安装(在闪存的.sdi文件)，并且更加进一步的验证会话保护。并且其他RSA服务器的IP地址下载。

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
```

在成功认证以后，而**show run命令**显示仅主IP地址， **aaa-server显示协议sdi**或**显示aaa-server <aaa-server-group>**命令显示所有RSA服务器(如果有超过一个)：

```
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。

在RSA的没有代理配置

在许多情况下，在您安装新的ASA或更改ASA IP地址后，忘记做同样变动在RSA是容易的。在RSA的代理程序IP地址需要为访问RSA的所有客户端更新。然后，新节点机密生成。因为他们有不同的IP地址和RSA需要委托他们，同样适用于ACS，特别是对附属节点。

损坏的秘密节点

有时在ASA或RSA的秘密file节点变得损坏。然后，删除在RSA的代理配置和再添加它是最佳的。您也需要执行在ASA/ACS的同一进程-再请删除并且添加配置。并且，请删除在闪存的.sdi文件，因此在下验证，一个新的.sdi文件安装。一旦这完成，自动节点秘密部署应该发生。

在中止模式的节点

有时一节点在中止模式，由从该服务器的无响应造成：

```
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
```

在中止模式， ASA不设法发送任何数据包到该节点;它需要有那的一种**好的**状态。失效的服务器在激活模式再放置在死机计时器以后。欲知更多信息，参考在[Cisco ASA系列命令参考的重新激活模式section命令](#)， 9.1指南。

在这样方案中，删除和添加该组的AAA服务器配置为了再触发该服务器到激活模式是最佳的。

锁定的帐户

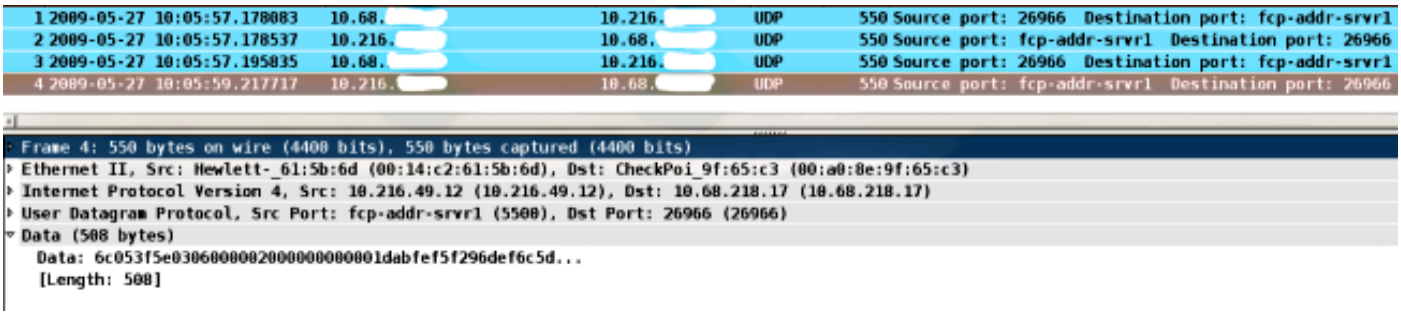
在多个再试后， RSA也许锁定在帐户外面。容易地被检查RSA与报告。在ASA/ACS，报告只显示“失败的认证”。

最大转换单元(MTU)问题和分段

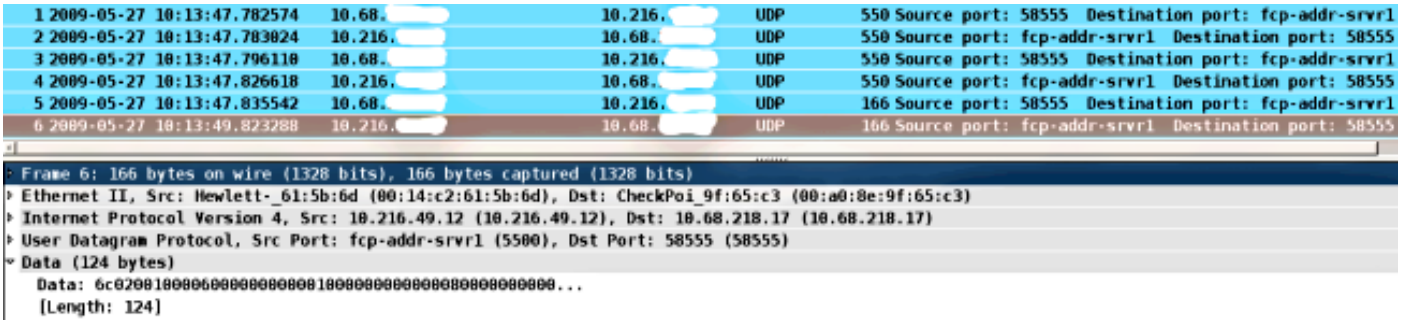
SDI使用UDP作为传输，不是MTU路径发现。默认情况下并且UDP流量没有设置的不要分段(DF)位。有时为更加大的数据包，也许有分段问题。是容易的探测在RSA的流量(设备和虚拟机[VM]使用Windows并且使用Wireshark)。完成在ASA/ACS的同一进程并且比较。并且，测验RADIUS或WebAuthentication在RSA为了比较它到SDI (为了缩小问题)。

数据包和调试ACS的

由于SDI有效负载加密，排除故障捕获的唯一方法是比较答复的大小。如果它小于200个字节，也许有问题。典型SDI交换介入四数据包，其中每一个是550个字节，但是那也许随RSA服务器版本改变：



在问题的情况下，它通常是超过四数据包被交换的和更加小的大小：



并且，ACS日志是相当清楚的。这是典型SDI注册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
```

相关信息

- RSA验证管理器资源
- RSA/SDI Cisco ASA 5500系列配置指南的服务器支持部分使用CLI，8.4和8.6
- RSA用户指南的SecurID服务器部分思科安全访问控制系统的5.4
- 技术支持和文档 - Cisco Systems