# ASA 8.3：TACACS认证使用ACS 5.X

## 目录



## 简介

本文提供信息关于怎样配置安全工具验证网络访问的用户。

## 先决条件

### 要求

本文假设，可适应安全工具(ASA)是完全能操作和已配置的允许Cisco Adaptive Security Device Manager (ASDM)或CLI做配置更改。

**注意：** 参考允许HTTPS访问ASDM关于如何允许ASDM远程配置的设备的更多信息。

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco可适应安全工具软件版本8.3和以上
- Cisco Adaptive Security Device Manager版本6.3和以上
- 思科安全访问控制服务器5.x

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。

## 规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

# 配置

本部分提供有关如何配置本文档所述功能的信息。

**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。

## 网络图

本文档使用以下网络设置：

**注意：** 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

## 使用CLI，配置验证的ASA从ACS服务器

执行ASA的这些配置从ACS服务器验证：

```
!--- configuring the ASA for TACACS server ASA(config)# aaa-server cisco protocol tacacs+
ASA(config-aaa-server-group)# exit !--- Define the host and the interface the ACS server is on.
ASA(config)# aaa-server cisco (DMZ) host 192.168.165.29 ASA(config-aaa-server-host)# key cisco
!--- Configuring the ASA for HTTP and SSH access using ACS and fallback method as LOCAL
authentication. ASA(config)#aaa authentication ssh console cisco LOCAL ASA(config)#aaa
authentication http console cisco LOCAL
```

**注意：** 当ACS不是可用的时，请创建ASA的一个本地用户使用**用户名Cisco密码cisco权限15**命令访问与本地认证的ASDM。

## 使用ASDM，配置验证的ASA从ACS服务器

### ASDM 步骤

完成这些步骤为了配置验证的ASA从ACS服务器：

1. 选择**Configuration>设备管理> Users/AAA >AAA服务器组>Add**为了创建**AAA服务器组**。
2. 提供在**添加AAA服务器组**联式窗的**AAA服务器组**细节如显示。使用的协议是**TACACS+**，并且创建的服务器组是**cisco**。单击 **Ok**。
3. 选择**Configuration>设备管理> Users/AAA >AAA服务器组**并且单击**添加在选定组的服务器下**为了添加AAA服务器。
4. 提供在**添加AAA服务器**窗口的**AAA服务器**细节如显示。使用的服务器组是**cisco**。点击OK键，然后单击**应用**。您将看到在ASA和**AAA服务器**配置的**AAA服务器组**。
5. 单击 **Apply**。
6. 选择**Configuration>设备管理> Users/AAA >AAA访问>验证**并且在**HTTP/ASDM**和**SSH旁边**单击复选框。然后，请选择**cisco**作为服务器组并且单击**应用**。

## 配置ACS作为TACACS服务器

完成此步骤为了配置ACS作为TACACS服务器：

1. 选择**网络资源>网络设备和AAA客户端**并且单击**创建**为了添加ASA到ACS服务器。
2. 提供关于**客户端的**必填信息(ASA客户端在这里)并且单击**提交**。添加的此enablesthe ASA到ACS服务器。详细信息包括ASA和**TACACS服务器**详细信息的**IP地址**。您将看到客户端被添加到ACS服务器的**思科**。
3. 选择**用户，并且标识存储>内部标识存储> Users**并且单击**创建**为了创建新用户。
4. 提供**名称、密码和特权密码**信息。**特权密码可选**。完成时，请单击 **Submit**。您将看到用户被添加到ACS服务器的**cisco**。

# 验证

使用本部分可确认配置能否正常运行。

请使用**cisco命令**thetest **aaa-server验证cisco主机192.168.165.29用户名的Cisco密码**检查配置是否适当地工作。此镜像显示验证是成功的，并且连接对ASA的用户由ACS服务器验证。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

# 故障排除

## Error:指示TACACS+在AAA服务器组TACACS的AAA服务器x.x.x.x如失败

此消息意味着思科ASA丢失连接用x.x.x.x服务器。确保您有在TCP 49的一有效连接到从ASA的服务器x.x.x.x。万一有网络延迟，您能也增加在ASA的超时从5的TACACS+服务器的到秒钟所需的数量。ASA不会发送认证请求对失效的服务器x.x.x.x。然而，它在AAA服务器组TACACS将使用下个服务器。

# 相关信息

- Cisco ASA 5500 系列自适应安全设备支持页
- Cisco ASA 5500 系列自适应安全设备命令参考
- Cisco 自适应安全设备管理器
- IPsec 协商/IKE 协议支持页
- 用于 Windows 的 Cisco 安全访问控制服务器
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems