

RADIUS、TACACS+、和 Cisco 安全域剥离

目录

[简介](#)

[开始使用前](#)

[规则](#)

[先决条件](#)

[使用的组件](#)

[RADIUS 域剥离](#)

[TACACS+ 域剥离](#)

[Cisco Secure ACS for Windows域剥离](#)

[Cisco Secure UNIX 域剥离](#)

[相关信息](#)

简介

在某些状况下，与“@”符号(username@website.com)的一用户名发送对Cisco IOS软件。当这发生时，有需要剥去域名流入的用户。在这类情况下，使用在路由器的在服务器的定向请求或Cisco安全软件这可能执行。

开始使用前

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

先决条件

本文档没有任何特定的前提条件。

使用的组件

本文档不限于特定的软件和硬件版本。

RADIUS 域剥离

在此配置示例中，假设您配置主机呼叫*website.com*的一个域的路由器。您的RADIUS服务器有10.1.1.1的IP地址。

```
ip host website.com 10.1.1.1
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server directed-request
```

注意： `radius-server directed-request`命令在Cisco IOS软件版本12.0(2)T介绍。

使用此配置，当人命名了 `user@website.com` 需要验证，定向请求代码设法解决域名到IP地址。在这种情况下，`website.com`解决对IP地址10.1.1.1由于本地IP主机语句。路由器为是解决的IP地址然后查寻RADIUS服务器主机线路，并且发送username的认证请求到RADIUS服务器。

[TACACS+ 域剥离](#)

您可用这些命令进行TACACS+的同一进程：

```
ip host website.com 10.1.1.1
tacacs-server host 10.1.1.1
tacacs-server directed-request
```

[Cisco Secure ACS for Windows域剥离](#)

如果需从 `user@website.com` 剥离域，请配置CiscoSecure NT仅验证用户名作为用户通过完成这些步骤：

1. 去 **Interface Configuration > Advanced Options**，选择分布式系统设定，并且单击**提交**。另外，除这一个之外，如果剥离的用户将去服务器，请完成以下步骤：去 **Network Configuration > Network Device Groups > Add Entry** 添加验证、授权和统计(AAA)服务器。去在目标的 **Network Configuration > Network Device Groups** 并且配置来源。
2. 在来源，请去 **Network Configuration > Distribution Table > Add Entry**。配置设置如下：在字符串的字段，请键入域名(`@website.com`)。从**位置**下拉菜单，请选择后缀。(请注意前缀在某些情况下也是可适用的。)从**小条**下拉菜单，请选择是。移动从**AAA Server列表**的服务器向**Forward To列表**。如果剥离名称是去从来源来源(来源和目标是相同的)的含义，来源是“转发的服务器”。如果剥离名称是去从来源一个不同的目标，则目标是“转发的服务器”。
3. 单击**提交**保存设置。

[Cisco Secure UNIX 域剥离](#)

在**AAA > 家用网关访问控制服务器**的域网页，指定这些设置：

- 域名：website.com
- 分隔符：@@
- 域名位置：在
- 域类型：远程

[相关信息](#)

- [远程用户拨入认证系统\(RADIUS\)](#)
- [终端访问控制器访问控制系统 \(TACACS+\)](#)
- [请求注解 \(RFC\)](#)

- [技术支持 - Cisco Systems](#)