# 比较 TACACS+ 和 RADIUS

## 目录


简介

先决条件

- 要求
- 使用的组件
- 规则

背景信息

RADIUS 背景

- 客户端/服务器端模式
- 网络安全
- 灵活的认证机制
- 服务器代码可用性

比较 TACACS+ 和 RADIUS

- UDP 和 TCP
- 数据包加密
- 认证 和 授权
- 多协议支持
- 路由器管理
- 互操作性
- Traffic
  - TACACS+ 流量示例
  - RADIUS 流量示例
- 设备支持
  - 表注释

相关信息


## 简介

本文档介绍并比较用于控制网络访问的两种主流安全协议：Cisco TACACS+ 和 Cisco RADIUS。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档不限于特定的软件和硬件版本。

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。如果您的网络处于活动状态，请确保您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技术提示和格式。

## 背景信息

RFC 2865 中介绍了 RADIUS 规范，RFC 2138 已淘汰。Cisco支持这两种协议。Cisco 的目的不是与 RADIUS 竞争，或鼓励用户使用 TACACS+。您必须选择最符合您需求的解决方案。本文档讨论 TACACS+ 和 RADIUS 之间的区别，使您能够做出合理的选择。

从 1996 年 2 月发行 Cisco IOS® 软件版本 11.1 以后，Cisco 就开始支持 RADIUS 协议。思科继续支持RADIUS并通过新的特性和功能对其进行增强。

在开发 TACACS+ 之前，Cisco 将 RADIUS 作为安全协议进行了认真评估。TACACS+协议中包含许多功能，以满足新的安全市场需求。该协议旨在跟随网络一起发展，能够成为成熟市场中的新安全技术。TACACS+ 协议的底层体系结构与独立身份验证、授权和记帐 (AAA) 体系结构互补。

## RADIUS 背景

RADIUS 是使用 AAA 协议的接入服务器。它是一套分布式安全系统，用于保护远程网络访问和抵御未获授权的网络服务访问。RADIUS 包含三个组件：

- 一套协议，具有使用用户数据报协议 (UDP)/IP 的帧格式。
- 一台服务器
- 客户端

服务器通常在客户端站点的中央计算机上运行，而客户端则驻留在拨号访问服务器中，并可在整个网络中分布。Cisco 将 RADIUS 客户端合并到 Cisco IOS 软件版本 11.1 及更高版本，以及其他设备软件中。

### 客户端/服务器端模式

网络接入服务器 (NAS) 作为 RADIUS 的客户端运行。客户端将用户信息传递到指定的RADIUS服务器，然后对返回的响应执行操作。RADIUS服务器接收用户连接请求，对用户进行身份验证，并返回客户端向用户交付服务所需的所有配置信息。RADIUS 服务器能够担当其他身份验证服务器的代理客户端。

### 网络安全

客户端和 RADIUS 服务器之间的事务通过使用从未在网络上发送的共享密钥进行身份验证。另外，任何用户口令在客户端和 RADIUS 服务器之间都以加密形式发送。这消除了有人在不安全的网络上监听时确定用户密码的可能性。

### 灵活的认证机制

RADIUS 服务器支持多种对用户进行身份验证的方法。当提供用户指定的用户名和原始密码时，它可以支持PPP、密码身份验证协议(PAP)或质询握手身份验证协议(CHAP)、UNIX登录和其他身份验证机制。

### 服务器代码可用性

市场上有许多公开发售和免费提供的服务器代码。Cisco 服务器包括用于 Windows 的 Cisco Secure ACS、用于 UNIX 的 Cisco Secure ACS 以及 Cisco Access Registrar。

## 比较 TACACS+ 和 RADIUS

以下各个部分比较了 TACACS+ 和 RADIUS 的若干功能。

### UDP 和 TCP

RADIUS 使用 UDP，而 TACACS+ 使用 TCP。TCP 提供了几个胜过 UDP 的优点。TCP 提供面向连接的传输，而 UDP 提供尽力传输。RADIUS 需要额外的可编程变量（如重新传输尝试和超时）来补偿尽力传输，但是它缺乏 TCP 传输提供的内置支持水平：

- 无论后端身份验证机制（TCP确认）的负载和速度如何，TCP使用都会在（大约）网络往返时间(RTT)内单独确认已收到请求。
- TCP通过重置(RST)提供崩溃或停止服务器的即时指示。 如果使用长期保持的 TCP 连接，就能确定服务器在何时崩溃、在何时恢复服务。UDP 不能显示发生故障的服务器、慢速服务器和不存在的服务器之间的差别。
- 使用TCP Keepalive时，可以根据实际请求在带外检测服务器崩溃。可以同时维护与多台服务器的连接，您只需将消息发送到已知已启用且运行的服务器。
- TCP更具扩展性，能够适应网络规模的扩大和拥塞的增加。

### 数据包加密

RADIUS 仅对从客户端到服务器的访问请求数据包中的口令加密。数据包的剩余部分未加密。其他信息，如用户名、获得授权的服务和记帐，可以被第三方捕获。

TACACS+ 会加密数据包的整个正文，但留下标准的 TACACS+ 报头。报头内的字段指示正文是否被加密。使用未加密的数据包正文有助于进行调试。然而在正常操作期间，为了实现更安全的通信，会完全加密数据包的正文。

### 认证 和 授权

RADIUS 结合了身份验证和授权。RADIUS 服务器向客户端发送的访问接受数据包中包含授权信息。这样就很难分离身份验证和授权。

TACACS+ 使用分离 AAA 的 AAA 体系结构。这就使独立的身份验证解决方案仍然可使用 TACACS+ 进行授权和记帐。例如，使用 TACACS+，就可以使用 Kerberos 身份验证和 TACACS+ 授权和记帐。在Kerberos服务器上进行NAS身份验证后，它将向TACACS+服务器请求授权信息，而无需重新进行身份验证。NAS 会通知 TACACS+ 服务器，它已经在 Kerberos 服务器上成功通过身份验证，然后服务器就会提供授权信息。

会话期间，如果需要进行额外的授权检查，则接入服务器会与 TACACS+ 服务器进行核对，确定是否授予了用户使用特定命令的权限。这样可以在取消身份验证机制关联时更好地控制可在访问服务器上执行的命令。

## 多协议支持

RADIUS 不支持这些协议：

- AppleTalk 远程访问 (ARA) 协议
- NetBIOS 帧协议控制协议
- Novell 异步服务接口 (NASI)
- X.25 PAD 连接

TACACS+ 提供多协议支持。

## 路由器管理

RADIUS 不允许用户控制哪些命令可以、哪些不可以在路由器上执行。所以，RADIUS 不能用于路由器管理，也不能灵活地适应终端服务。

TACACS+ 提供两种方法来基于每位用户或每个组控制路由器命令授权。第一种方法是为命令分配权限级别，并安排路由器通过 TACACS+ 服务器来验证用户是否已在指定的权限级别内授权。第二种方法是在 TACACS+ 服务器中明确基于每位用户或每个组指定允许的命令。

## 互操作性

由于 RADIUS 请求注解 (RFC) 有多种解释，因此遵循 RADIUS RFC 不能保证互操作性。即使一些供应商实现了 RADIUS 客户端，也并不意味着它们具备互操作性。Cisco 实现了大多数 RADIUS 属性，并将不断加入更多。如果客户端在其服务器中仅使用标准RADIUS属性，则只要这些供应商实施相同的属性，它们就可以在多个供应商之间运行。然而，许多供应商实施的扩展都是专有属性。如果客户端使用这些供应商特定的扩展属性之一，则互操作性是不可能的。

## Traffic

由于 TACACS+ 和 RADIUS 之间存在上述差别，在客户端和服务器之间生成的流量数会有所不同。这些示例说明当 TACACS+ 和 RADIUS 与身份验证、exec 授权、命令授权（RADIUS 无法实现）、exec 记帐和命令记帐（RADIUS 无法实现）一起用于路由器管理时，客户端与服务器之间产生的流量。

TACACS+ 流量示例

此示例假设当用户远程登录到路由器、执行命令并退出路由器时，使用TACACS+登录身份验证、执行授权、命令授权、开始 — 停止exec记帐，以及命令记帐：

RADIUS 流量示例

本示例假设当用户远程登录到路由器、执行命令并退出路由器（其他管理服务不可用）时，使用RADIUS实施登录身份验证、执行授权和开始 — 停止EXEC记帐。

## 设备支持

下表列出了各种设备对选定平台支持的 TACACS+ 和 RADIUS AAA。包括已添加支持的软件版本。如果您的产品未在此列表中，请查看产品发行版本注释以了解详细信息。

| Cisco 设备 | TACACS+ 身份验证 | TACACS+ 授权 | TACACS+ 记帐 | RADIUS 身份验证 | RADIUS 授权 | RADIUS 记帐 |
|---|---|---|---|---|---|---|
| 思科Aironet[1] | 12.2(4)JA | 12.2(4)JA | 12.2(4)JA | 所有接入点 | 所有接入点 | 所有接入点 |
| Cisco IOS®软件[2] | 10.33 | 10.33 | 10.333 | 11.1.1 | 11.1.14 | 11.1.15 |
| Cisco 缓存引擎 | — | — | — | 1.5 | 1.56 | — |
| Cisco Catalyst 交换机 | 2.2 | 5.4.1 | 5.4.1 | 5.1 | 5.4.14 | 5.4.15 |
| Cisco CSS 11000 内容服务交换机 | 5.03 | 5.03 | 5.03 | 5.0 | 5.04 | — |
| Cisco CSS 11500 内容服务交换机 | 5.20 | 5.20 | 5.20 | 5.20 | 5.204 | — |
| Cisco PIX 防火墙 | 4.0 | 4.07 | 4.28,5 | 4.0 | 5.27 | 4.28,5 |
| Cisco Catalyst 1900/2820 交换机 | 8.x企业版[9] | — | — | — | — | — |
| Cisco Catalyst 2900XL/3500XL 交换机 | 11.2.(8)SA6[10] | 11.2.(8)SA6[10] | 11.2.(8)SA6[10] | 12.0(5)WC5[11] | 12.0(5)WC5[11,4] | 12.0(5)WC5[11,5] |
| Cisco VPN 3000集中器[6] | 3.0 | 3.0 | — | 2.012 | 2.0 | 2.012 |
| Cisco VPN 5000 集中器 | — | — | — | 5.2X[12] | 5.2X[12] | 5.2X[12] |

表注释

1. 除了 Cisco IOS 软件版本 12.2(4)JA 或更高版本以外，仅限无线客户端的终端，不包括管理流量。在 Cisco IOS 软件版本 12.2.(4)JA 或更高版本中，可以对无线客户端的终端和管理流量进行身份验证。
2. 检查Software Advisor以了解Cisco IOS软件中的平台支持。
3. 在Cisco IOS软件版本发布之前不实施命令记帐 11.1.6.3.
4. 无命令授权。
5. 无命令记帐。
6. 仅限 URL 阻塞，不包括管理流量。
7. 通过 PIX 的非 VPN 流量的授权。

   注意：版本5.2 — 访问列表支持访问控制列表(ACL)RADIUS供应商特定属性(VSA)或TACACS+授权VPN流量在PIX版本6.1终止 — 支持ACL RADIUS属性11授权VPN流量在PIX版本6.2.2终止 — 支持可下载ACL和RADIUS授权VPN流量在PIX版本6.2终止 — 支持通过TACACS+授权PIX管理流量。<

8. 仅限通过 PIX 的非 VPN 流量的记帐，不包括管理流量。

   注意：版本 5.2 - 支持对通过 PIX 的 VPN 客户端 TCP 数据包进行记帐。

9. 仅限企业版软件。
10. 需要 8M 闪存用于映像。
11. 仅限 VPN 终端。

注意：只有注册的思科用户才能访问内部思科工具和信息。

# 相关信息

- RADIUS支持
- TACACS/TACACS+支持/身份验证协议
- 请求注解 (RFC)
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。