强化无线网络的五个技巧

目标

无线电是创建无线网络的无线接入点(WAP)的物理组件。WAP和无线路由器上的无线电设置控制无线电的行为，并确定设备传输的信号。尽管Wi-Fi网络非常方便，但它可能会因占用了太多带宽的无线客户端而变得脆弱，并且如果不能适当地保护它，可能会增加安全风险。建议使用以下设置来提高安全性：

- 启用数据封装
- 仅允许已知设备通过介质访问控制(MAC)过滤连接到网络
- 定期更改无线网络密码
- 启用内置防火墙
- 隐藏服务集标识符(SSID)

本文旨在提供有助于保护无线网络安全的提示。

适用设备

- RV系列
- 无线接入点
- Cisco 统一通信

强化您的无线网络

启用数据封装

无线网络设备通常支持某种类型的加密，以便能够安全地连接到无线网络。尽可能使用Wi-Fi保护访问(WPA)或Wi-Fi保护访问2(WPA2)，因为它们通过高级加密标准(AES)加密方法提供更好的安全性。每个设备启用数据加密的步骤略有不同。有关在无线路由器上启用无线安全的指南，请单击此处。有关在接入点上启用无线安全的指南，请单击此处。

仅允许具有MAC过滤的已知设备

通过MAC地址过滤，您可以列出连接到网络的无线客户端的MAC地址，从而有效地创建仅已知设备列表。然后，您可以根据需要授予或拒绝设备访问网络。不在列表中的MAC地址将自动从条件中排除。每个设备启用MAC地址过滤的步骤略有不同。有关在无线路由器上启用MAC过滤的指南，请单击此处。有关在无线接入点上启用MAC过滤的指南，请单击此处。

定期更改无线网络密码

设置无线网络密码是保护无线网络的最简单方法。它们通常需要与网络中的其他无线接入点同步，以实现无缝无线连接。无线网络密码通常需要定期更改，以确保只有授权设备连接到网络。设置无线网络密码的步骤因设备而异。有关如何在路由器上配置无线设置的指南，请单击此处。有关更改接入点密码的指南，请点击此处。

启用内置防火墙

许多无线路由器（如RV130W Wireless-N VPN路由器）都内置了防火墙，可防止恶意流量进

入您的网络。启用防火墙的步骤因设备而异。有关在路由器上启用防火墙的指南，请单击此处。

隐藏SSID

禁用SSID广播会使设备在搜索无线网络时看不到您的网络。与设置无线密码类似，隐藏SSID使连接到无线网络更加困难，因为必须在设备上手动配置连接。禁用SSID广播的步骤因设备而异。有关在接入点上禁用SSID广播的指南，请单击此处。有关在无线路由器上禁用SSID广播的指南，请单击此处。

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）。