強化無線網路的五個技巧

目標

無線電是建立無線網路的無線接入點(WAP)的物理元件。WAP和無線路由器上的無線電設定控制無線電的行為，並確定裝置傳輸的訊號。雖然Wi-Fi網路非常方便，但它可能會因佔用頻寬的無線客戶端而變得脆弱，並且如果不能適當地保護它，則會增加安全風險。建議為增強安全性設定以下設定：

- 啟用資料加密
- 僅允許已知裝置通過介質訪問控制(MAC)過濾連線到網路
- 定期更改無線網路密碼
- 啟用內建防火牆
- 隱藏服務組識別碼(SSID)

本文旨在提供有助於保護無線網路安全的提示。

適用裝置

- RV系列
- 無線存取器
- 思科整合通訊

強化您的無線網路

啟用資料加密

無線網路裝置通常支援某種型別的加密，以便能夠安全地連線到無線網路。儘可能使用Wi-Fi保護訪問(WPA)或Wi-Fi保護訪問2(WPA2)，因為它們使用高級加密標準(AES)加密方法提供更好的安全性。每個裝置啟用資料加密的步驟略有不同。有關在無線路由器上啟用無線安全的指南，請按一下此處。有關在接入點上啟用無線安全的指南，請按一下此處。

僅允許具有MAC過濾的已知裝置

通過MAC地址過濾，您可以列出連線到網路的無線客戶端的MAC地址，從而有效地建立僅已知裝置清單。然後，您可以根據需要授予或拒絕裝置訪問網路。不在清單中的MAC地址將自動從條件中排除。每個裝置啟用MAC地址過濾的步驟略有不同。有關在無線路由器上啟用MAC過濾的指南，請按一下此處。有關在無線接入點上啟用MAC過濾的指南，請按一下此處。

定期更改無線網路密碼

設定無線網路密碼是保護無線網路的最簡單方法。它們通常需要與網路中的其他無線接入點同步，以實現無縫無線連線。無線網路密碼通常需要定期更改，以確保只有經過授權的裝置才能連線到網路。設定無線網路密碼的步驟因裝置的不同而略有不同。有關如何在路由器上配置無線設定的指南，請按一下此處。有關更改接入點密碼的指南，請按一下此處。

啟用內建防火牆

許多無線路由器（如RV130W無線 — N VPN路由器）具有內建防火牆，可防止惡意流量進入您的網路。每個裝置啟用防火牆的步驟略有不同。有關在路由器上啟用防火牆的指南，請按一下此處。

隱藏SSID

禁用SSID廣播可使裝置在搜尋無線網路時看不到您的網路。與設定無線密碼一樣，隱藏SSID使連線到無線網路更加困難，因為需要在裝置上手動配置連線。每個裝置禁用SSID廣播的步驟略有不同。有關在接入點上禁用SSID廣播的指南，請按一下此處。有關在無線路由器上禁用SSID廣播的指南，請按一下此處。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。