

合法攔截常見問題

面向服務提供商的思科解決方案如何滿足合法攔截要求？

大多數國家/地區都要求服務提供商與執法部門之間提供切換介面，以滿足全球認可的合法攔截標準。

思科服務供應商網路裝置可作為服務供應商網路中的攔截接入點(IAP)，但並不直接支援向執法部門切換介面。思科服務獨立攔截(SII)架構要求思科的第三方合作夥伴之一提供中介設備，用於管理合法攔截授權、在網路內調配攔截內容以及以適當格式將攔截資訊呈現給執法部門。

基於SII架構的思科網路元素與來自第三方合作夥伴的調解裝置相結合，滿足對服務提供商與執法部門之間的切換介面的合法攔截要求，以獲得最認可的合法攔截標準。

有關各個國家/地區的合法攔截要求的資訊，請參閱：

- [美國:《通訊援助執法法》](#)
- [加拿大:司法部合法訪問常見問題解答](#)
- [英國:2000年《調查權力條例》](#)
- [荷蘭:1998年電信](#)

思科合法攔截架構如何工作？

為了響應支援對其服務提供商客戶進行合法攔截的要求，思科開發了服務獨立攔截(SII)架構。SII架構在充當內容攔截接入點(IAP)的思科裝置和中介裝置之間提供明確定義的開放式介面。SII架構的模組化性質允許服務提供商選擇最合適的調解裝置來滿足特定的網路要求以及執法收集功能的介面基於標準的區域要求。

思科SII架構在資訊[RFC 3924](#)中進行了標準化，並且由思科合作夥伴合法攔截中介裝置和其他裝置供應商提供支援。

我到哪裡諮詢？

有關解決方案功能的資訊，請聯絡您的思科代表。

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）。