合法拦截常见问题

面向服务提供商的思科解决方案如何满足合法拦截要求？

大多数国家/地区都要求服务提供商与执法部门之间的切换界面符合全球认可的合法拦截标准。

思科服务提供商网络设备可在服务提供商网络中用作拦截接入点(IAP)，但并不直接支持向执法部门切换接口。思科服务独立拦截(SII)架构需要来自思科第三方合作伙伴的调解设备，用于管理合法拦截授权、在网络内调配拦截以及以适当格式将拦截信息提供给执法部门。

基于SII架构的思科网络元素与来自第三方合作伙伴的调解设备相结合，可满足最认可的合法拦截标准对服务提供商与执法部门之间切换界面的合法拦截要求。

有关各个国家/地区的合法拦截要求的信息，请参阅：

- 美国:《通信援助执法法》
- 加拿大:司法部合法访问常见问题解答
- 英国:《2000年调查权力法》
- 荷兰:1998年电信

思科合法拦截架构如何工作？

为了响应为其服务提供商客户支持合法拦截的要求，思科开发了服务独立拦截(SII)架构。SII架构在充当内容拦截接入点(IAP)的思科设备和中介设备之间提供明确定义的开放式接口。SII架构的模块化特性允许服务提供商选择最合适的调解设备来满足特定的网络要求以及执法收集功能的接口基于标准的区域要求。

思科SII架构在信息RFC 3924中进行了标准化，并由思科合作伙伴为合法拦截中介设备和其他设备供应商提供支持。

我到哪里咨询？

有关解决方案功能的信息，请联系您的思科代表。

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）。