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/地区需要服务提供商和执法机构之间的切换接口才能满足全球公认的合法拦截标准。

思科服务提供商网络设备可以在服务提供商网络内用作拦截接入点(IAP)，但不直接支持向执法部门的切换接口。思科服务独立拦截(SII)架构要求思科的第三方合作伙伴之一提供中介设备，用于管理合法拦截授权、调配网络内的拦截以及以适当格式向执法部门展示拦截信息。

基于SII架构的思科网络元素与来自第三方合作伙伴的中介设备相结合，可满足服务提供商和执法机构之间关于最公认合法拦截标准的切换接口的合法拦截要求。

有关各国合法拦截要求的信息，请参阅：

- 美国:《执法通信协助法》
- 加拿大:司法部合法访问常见问题
- 英国:2000年《调查权力条例》
- 荷兰:1998年电信业

思科合法拦截架构如何工作？

为响应支持其服务提供商客户合法拦截的要求，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)的思科设备与中介设备之间提供明确定义的开放式接口。SII架构的模块化特性使服务提供商能够选择最合适的中介设备来满足特定网络要求和区域性、基于标准的要求，为执法收集功能提供接口。

Cisco SII架构在信息性RFC 3924中进行了标准化，并受思科合作伙伴支持合法拦截调解设备和其他设备供应商的支持。

我在哪里进行咨询？

有关解决方案功能的信息，请联系您的思科代表。