防止用户使用UltraSurf

目录

简介

本文档介绍如何防止用户使用UltraSurf。

问题

用户通过使用UltraSurf代理绕过内容过滤和安全配置。

原因

UltraSurf结合了多种措施，以允许避开常用的内容过滤解决方案。它使用SSL创建到远程主机的连接，以加密数据并阻止大多数解决方案进行“窥探”。

目前，UltraSurf会进行更改以降低浏览器的安全设置，因为它使用无效的SSL证书建立这些连接。在以前的版本中，UltraSurf使用DNS作为绕过内容过滤解决方案的机制，而Umbrella通过识别这些DNS服务器并阻止对服务器的访问来降低其速度。然而，UltraSurf的开发团队不断推出新版本的软件，因此他们再次改变方法只是时间问题。

解决方案

还可以采取其他措施，包括阻止UltraSurf已知使用的子网。这些地址通常是ISP分配的动态IP地址范围，只有很少甚至没有商务用户的合法用途。此外，在Active Directory环境中，可以使用软件限制策略限制应用。这可用于限制当前和早期版本的UltraSurf软件在您的网络上运行。

发布新版本后，您需要添加其他软件限制策略。还可以限制用户对Internet Explorer的安全选项所做的更改，以防止使用无效的安全证书。我们将继续监控Ultrasurf在每个修订版中进行的版本和更改，并正在研究Umbrella如何帮助防止Ultrasurf访问。

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）。