配置DNS隧道VPN安全类别

目录

简介

本文档介绍如何在Umbrella中配置DNS隧道VPN安全类别。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Umbrella DNS。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

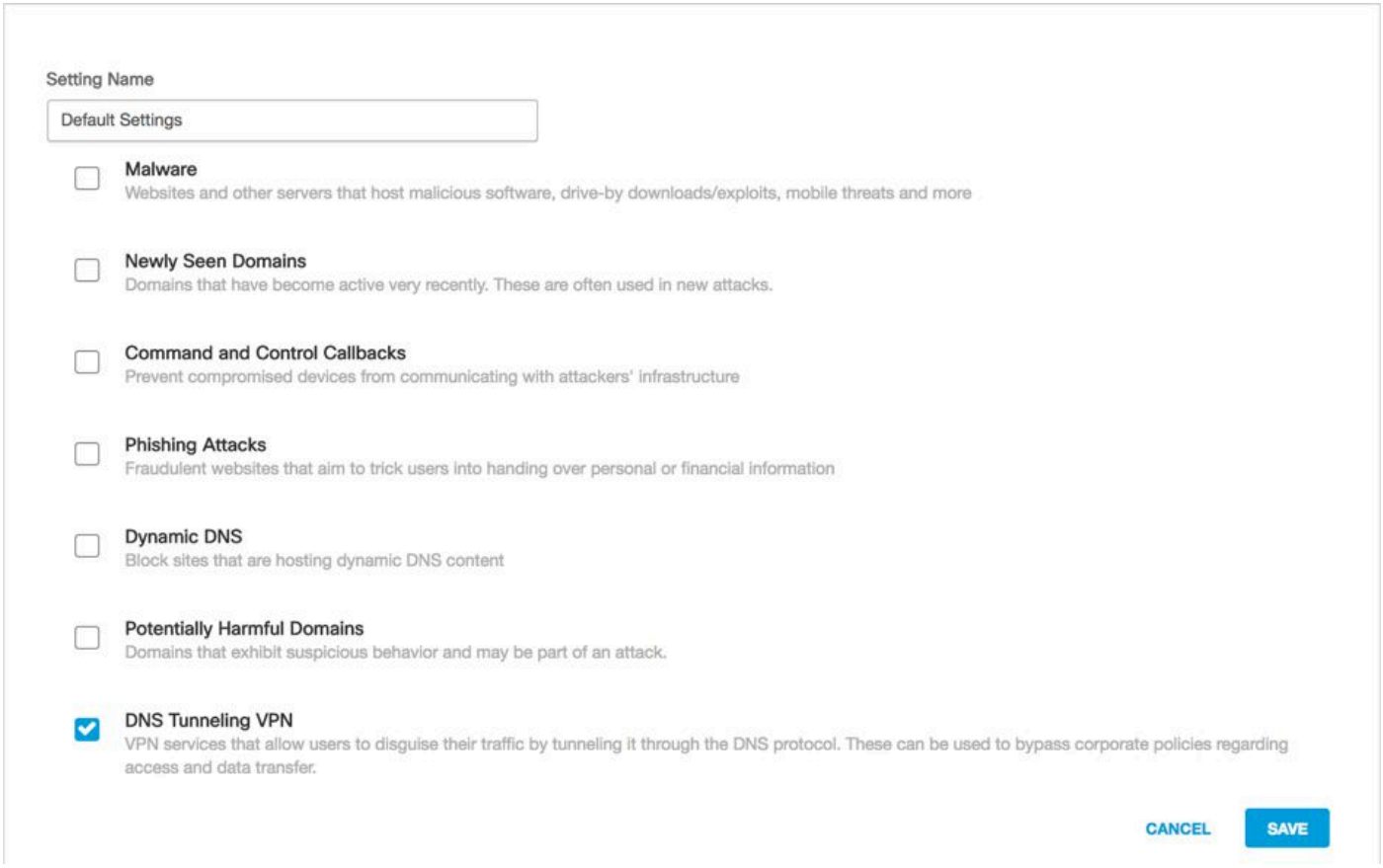
概述

DNS隧道VPN将与DNS隧道VPN服务关联的服务器分类到可以阻止或允许并报告的安全类别下。这些服务允许最终用户将传出流量伪装为DNS查询，从而可能违反可接受使用、数据丢失保护或安全策略。因此，这些服务会带来潜在的安全威胁，并降低您环境中的整体可视性。

通过这种安全类别提供即时可视性，您可以降低DNS隧道风险以及潜在的数据丢失。您可以完全阻止此类别，或仅监控报告中的结果；这样可以灵活地确定解决问题的正确方法，具体取决于您的风险承受能力、可接受的使用或人力资源政策。

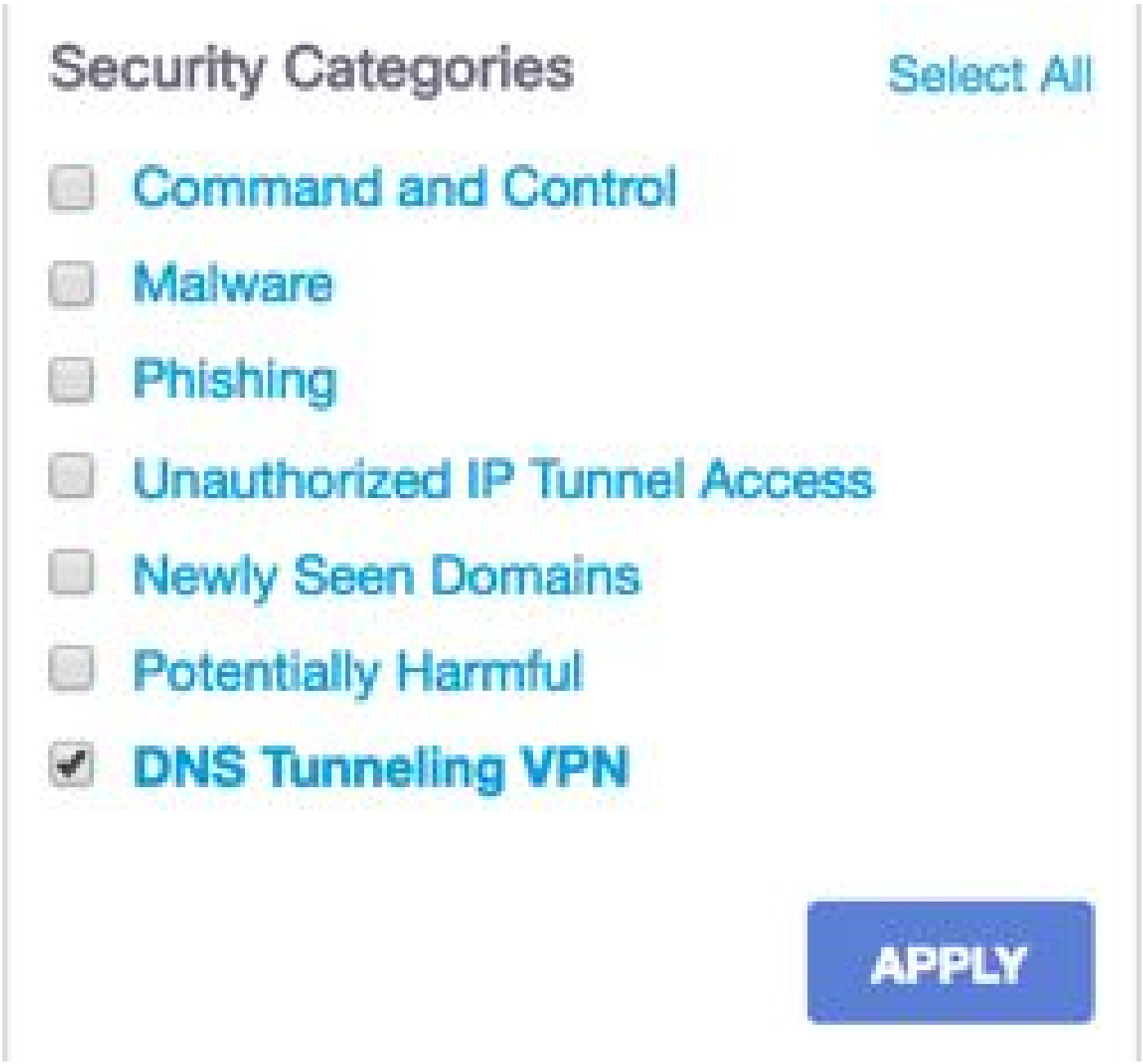
打开DNS隧道VPN

可以像启用Policies > Security Settings下的任何其他安全类别一样启用此安全类别，然后编辑现有安全设置。或者，可以在策略配置向导自身中完成：



115014823666

DNS隧道可通过活动搜索报告进行过滤：



115015008983

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）。