了解Umbrella如何防止DDoS攻击

目录

简介

本文档介绍Umbrella如何针对分布式拒绝服务攻击提供保护。

背景信息

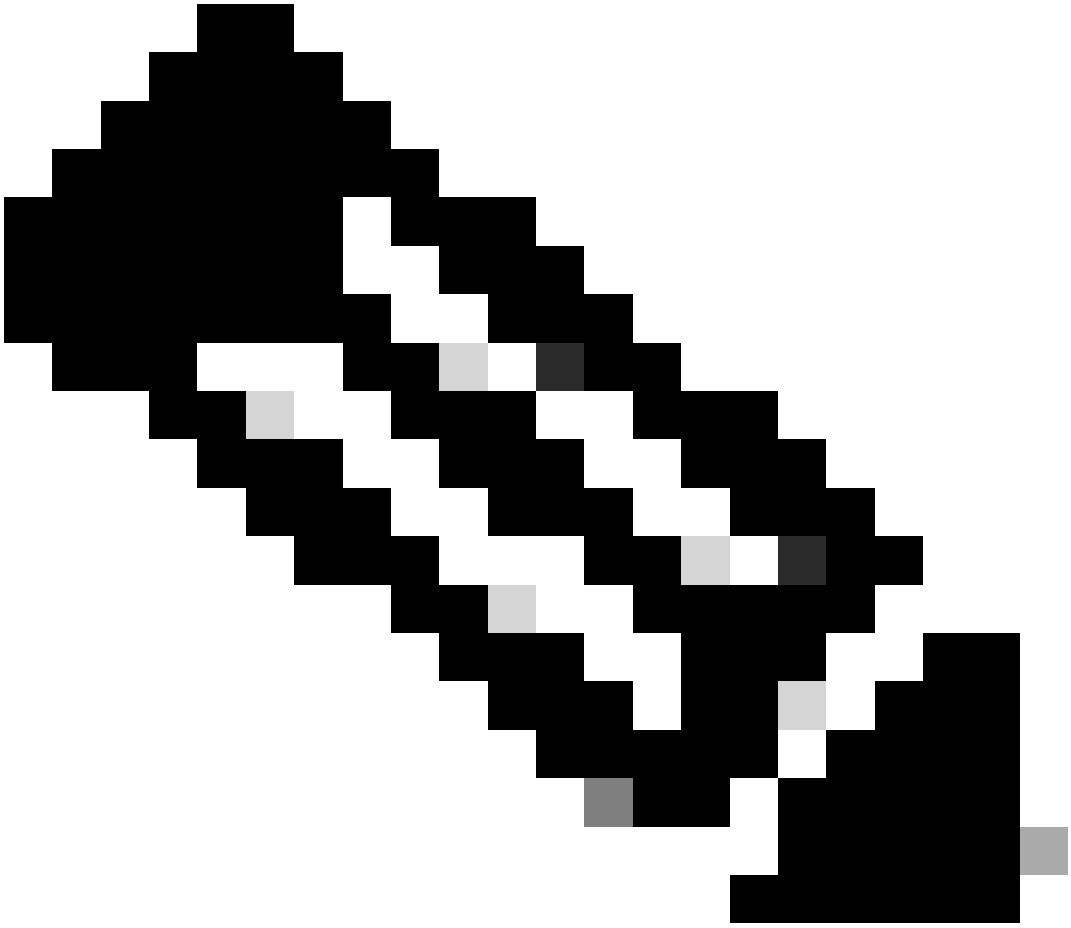
DDoS或分布式拒绝服务攻击（DDoS attack，简称DDoS攻击）是一种方法，恶意攻击者利用受感染的计算机网络，可以使流向在线站点或服务的流量达到饱和，从而使目标不可用。

Umbrella提供的服务包括针对命令和控制回拨以及针对防御安全类别下的恶意软件的防护。通过防止恶意软件，更重要的是通过递归DNS解析包含命令和控制回拨功能，这有助于防止您的基础设施被用作其他公司的DDoS攻击的启动平台。

Umbrella的工作原理

当具有恶意软件的计算机尝试使用DDOS攻击其他站点时，Umbrella会阻止其访问该站点。通过阻止扩展网络中的计算机（包括漫游计算机）参与命令和控制回叫攻击，您的组织可以避免被视为此类攻击的可能来源。

Umbrella可以缓解某些类型的攻击，例如对DynDNS的攻击，因为我们的SmartCache技术在网站的DNS记录不可用时缓存最近已知的“良好”IP。



注意：有关针对DynDNS的攻击的详细信息，请参阅
：http://www.theregister.co.uk/2016/10/21/dns_devastation_as_dyn_dies_under_denialofservice_at

由于我们的服务采用结构化方式，Umbrella的DNS服务无法防御针对外部权威DNS服务器或Web服务器的DDoS攻击。

对于此类攻击，我们建议提供或管理Web应用防火墙和授权DNS的服务。CloudFlare就是这种补充服务的例子。

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）。