Understand How Umbrella Prevents DDoS Attacks

Contents

Introduction

This document describes how Umbrella provides protection against a distributed denial-of-service attack.

Background Information

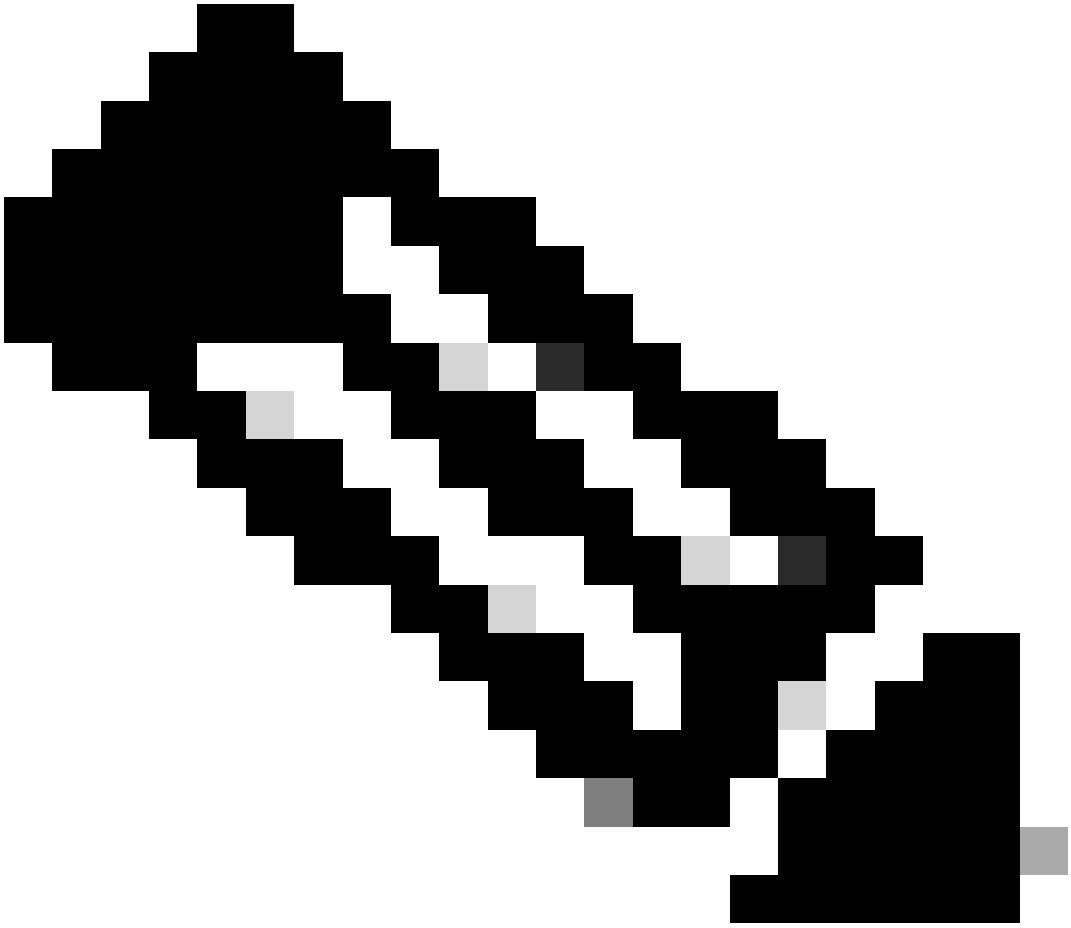
A DDoS or distributed denial-of-service attack (DDoS attack) is a method by which malicious attackers, using networks of infected computers, can saturate traffic to an online site or service to make the target unavailable.

The services provided by Umbrella include protection against Command and Control Callback and malware under the Security Category for Prevention. This helps prevent your infrastructure being used as a launch pad for DDoS attacks onto other companies by preventing malware, and more importantly, containing Command and Control Callback via recursive DNS resolution.

How Umbrella Works

When a computer with malware tries is trying to attack another site with a DDOS attack, Umbrella prevents it from reaching that site. By stopping computers within your extended network, including roaming computers, from participating in a Command and Control Callback attack your organization can avoid being seen as a possible source of this type of attack.

Certain types of attacks can be mitigated by Umbrella, such as the attack against DynDNS because of our SmartCache technology that caches the most recently known 'good' IP when a website's DNS records become unavailable.



Note: For more info on the attack against DynDNS, see: http://www.theregister.co.uk/2016/10/21/dns_devastation_as_dyn_dies_under_denialofservice_attack/.

Due to the way our service is structured, Umbrella's DNS services cannot protect against DDoS attacks that target authoritative DNS servers or Web servers from the outside.

For attacks such, we recommend a service that provides or manages a web application firewall and authoritative DNS. An example of such a complementary service is CloudFlare.