Comprendre comment Umbrella empêche les attaques DDoS

Table des matières

Introduction

Ce document décrit comment Umbrella fournit une protection contre une attaque par déni de service distribué.

Informations générales

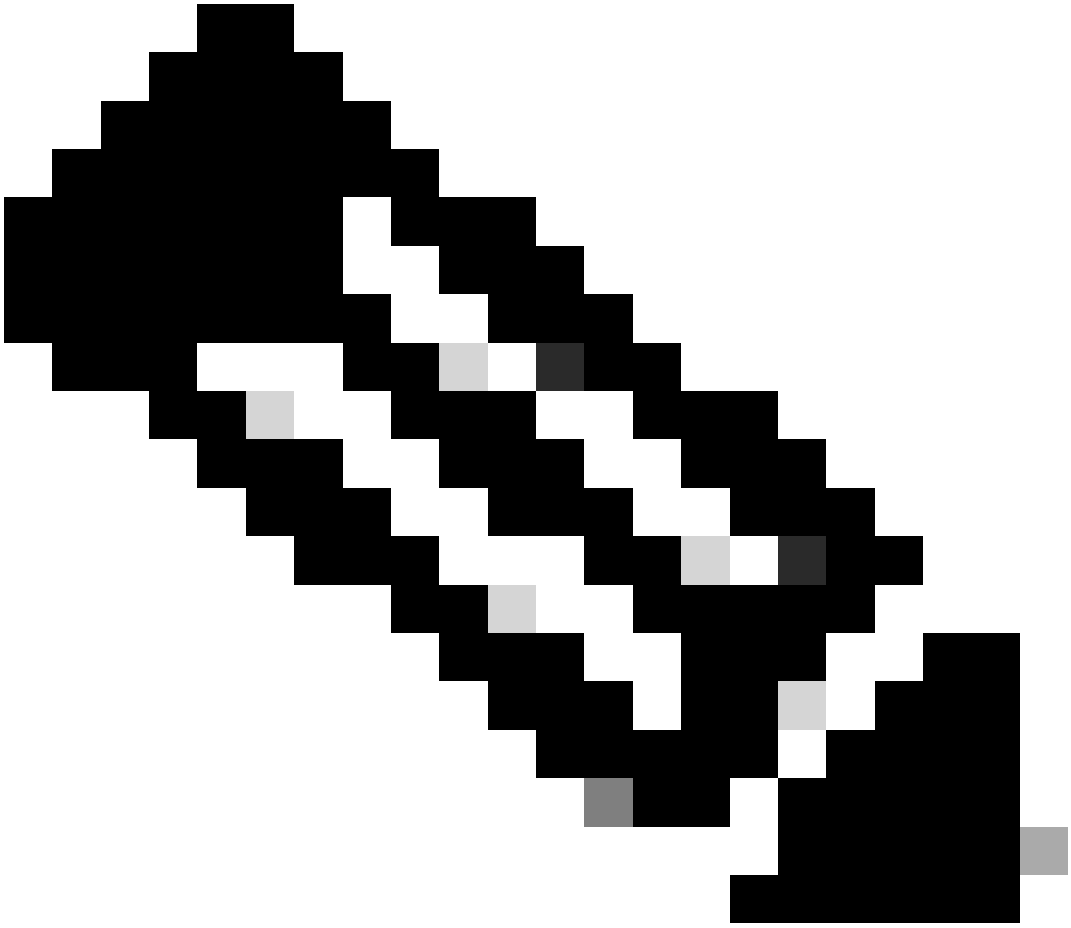
Une attaque par déni de service distribué (DDoS) ou DDoS (Distributed Denial-of-service attack) est une méthode par laquelle des pirates malveillants, utilisant des réseaux d'ordinateurs infectés, peuvent saturer le trafic vers un site ou un service en ligne pour rendre la cible indisponible.

Les services fournis par Umbrella incluent la protection contre les rappels de commande et de contrôle et les programmes malveillants dans la catégorie Sécurité pour la prévention. Cela permet d'éviter que votre infrastructure ne soit utilisée comme rampe de lancement pour des attaques DDoS sur d'autres entreprises en empêchant les programmes malveillants et, plus important encore, en contenant le rappel de commande et de contrôle via une résolution DNS récursive.

Fonctionnement de Umbrella

Lorsqu'un ordinateur malveillant tente d'attaquer un autre site par une attaque DDOS, Umbrella l'empêche d'atteindre ce site. En empêchant les ordinateurs de votre réseau étendu, y compris les ordinateurs en itinérance, de participer à une attaque de rappel de commande et de contrôle, votre entreprise peut éviter d'être considérée comme une source possible de ce type d'attaque.

Certains types d'attaques peuvent être atténués par Umbrella, comme l'attaque contre DynDNS en raison de notre technologie SmartCache qui met en cache le plus récemment connu "bon" IP lorsque les enregistrements DNS d'un site Web deviennent indisponibles.



Remarque : Pour plus d'informations sur l'attaque contre DynDNS, consultez : http://www.theregister.co.uk/2016/10/21/dns_devastation_as_dyn_dies_under_denialofservice_atta

En raison de la manière dont notre service est structuré, les services DNS d'Umbrella ne peuvent pas se protéger contre les attaques DDoS qui ciblent des serveurs DNS faisant autorité ou des serveurs Web depuis l'extérieur.

Pour des attaques telles que, nous recommandons un service qui fournit ou gère un pare-feu d'application Web et un DNS faisant autorité. CloudFlare est un exemple de service complémentaire de ce type.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.