Understand Best Practices for Installing OpenDNS Umbrella with Websense

Contents

Introduction

This document describes the best practices for installing OpenDNS Umbrella with Websense.

Overview

To ensure you see the full potential of OpenDNS during your evaluation (and afterwards), all non-internal DNS traffic must point to the OpenDNS Global Network. Three Websense environments cause OpenDNS to miss some DNS traffic:

1. On-premises proxy is resolving DNS requests initiated by Web servers (more common)
2. Cloud proxy is resolving DNS requests initiated by Web servers (for hybrid customers using Web Endpoint Agents)
3. On-premises proxy is resolving DNS requests on behalf of clients (less common)

1) On-premises proxy is resolving DNS requests initiated by Web servers

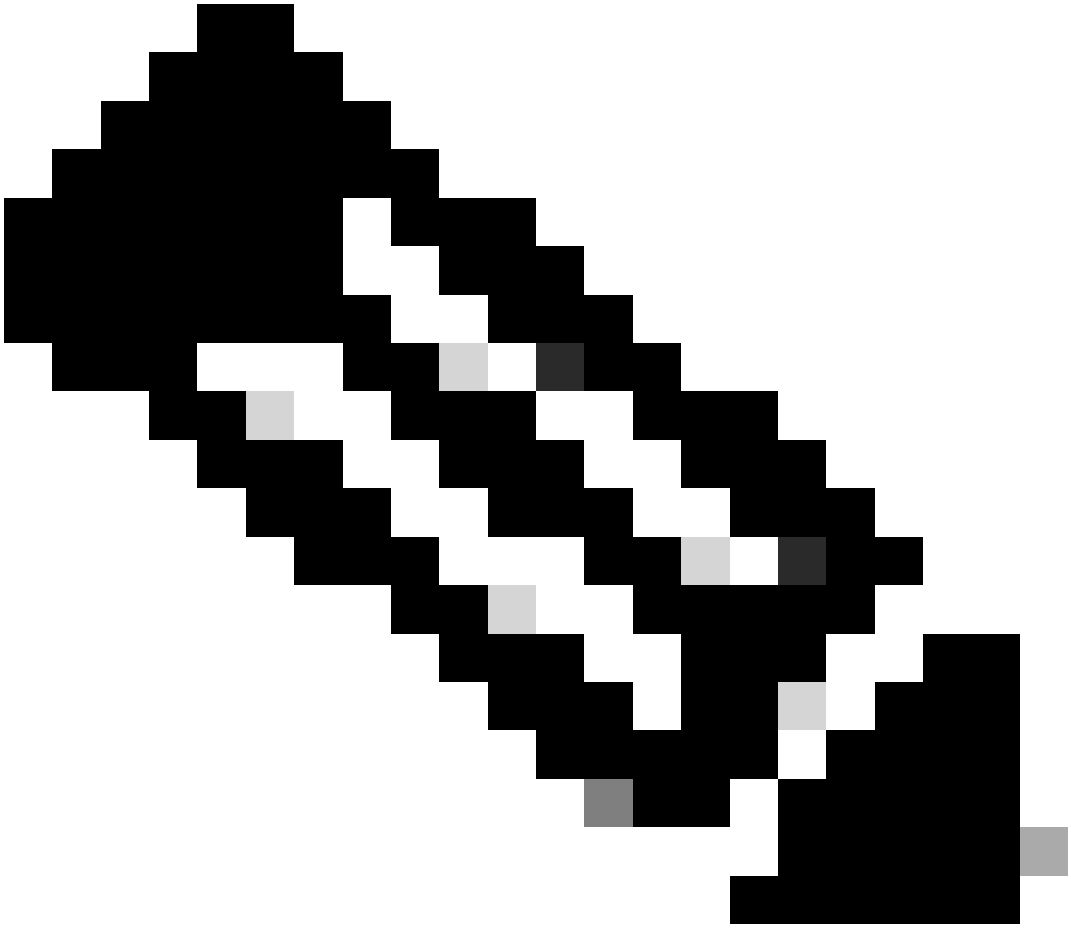
- Websense Content Gateways—deployed either in explicit or transparent proxy mode—can resolve DNS requests initiated after a connection is made with a Web server; depending on its configuration.
- If these DNS requests are resolved from Websense's built-in DNS proxy caching or a different recursive DNS service, OpenDNS is bypassed.
- Please refer to Websense's support materials—linked here for your convenience—to ensure that Websense is configured to always resolve non-internal DNS requests using OpenDNS.
  Content Gateway Manager Help > DNS Resolver > DNS Variables > Using the Split DNS option

2) Cloud proxy is resolving DNS requests initiated by Web servers

- Unfortunately, Websense does not allow its customers to directly change the DNS server settings.
- We are not sure if you can request Websense to manually change the settings to point to OpenDNS.

3) On-premises proxy is resolving DNS requests on behalf of clients

- It happens if the DNS proxy caching option is enabled, but configuring DNS proxy caching is only possible with a L4 switch or a Cisco WCCPv2 device, so it’s not a common environment.
- DNS proxy only answers requests for A and CNAME DNS entries. Other types of requests are not be answered.
- If the hostname to IP address mapping is not in the DNS cache, Content Gateway contacts the DNS server specified in the /etc/resolv.conf file. (Note: Only the first entry in resolv.conf is used, and this might not be the same DNS server for which the DNS request was originally intended.)



Note: The "Always Query Destination" option reduces the number of DNS lookups, and can be enabled if the Content Gateway is not running in both explicit and transparent proxy mode. It configures the proxy to always obtain the original destination IP of incoming requests from the ARM (Adaptive Redirection Module). And use that IP to determine the origin server, instead of doing a DNS lookup on the hostname of the request. Because the client already performed a DNS lookup, proxy does not have to.
