Understand why Queries for Internal Domains Are Not Logged in Umbrella Insights

Contents

Introduction

This document describes why queries for Internal Domains are not logged.

Overview

When using Umbrella Insights, which includes the Virtual Appliance (VA), all workstations must only have their DNS server settings pointing to the VAs. The VAs must be configured to use your pre-existing internal DNS servers. The dashboard allows you to enter a list of 'Internal Domains' so that when the client makes a DNS query for an internal resource, the VA forwards the request to one of the internal DNS servers. Occasionally we are asked why none of these internal requests appear in the logging.

Explanation

As outlined above, Internal DNS requests received by the VA are forwarded to one of the Internal DNS servers configured on the VA during setup. These can be seen in the console. All being well, the Internal DNS server issues a response and the VA relays this back to the client.

When the client makes a DNS request for a resource that is NOT on the list of Internal Domains, it forwards it out to the Umbrella Anycast IP addresses. This request includes extra data in the DNS query to our resolvers which allows the request to be tied back to an origin. The origin could for example be a UserID hash, a source IP, or a number of other identifying factors that are included in this extended DNS packet. This extra data can be seen by running a specific DNS query from a command line:

```
nslookup -server=208.67.222.222 -type=txt debug.opendns.com.
```

The actual logging of DNS requests takes place on our resolvers. The logging relies on this unique information being appended to the DNS packet. The VA does not log the DNS requests it forwards on. It is first and foremost a recursive DNS server. Once our public resolvers receives a DNS query it uses the extended data sent with the actual query to identify the source, apply the appropriate policy, and log the information of the request and if it was allowed or blocked, which then shows up in the dashboard. As Internal DNS queries never see our resolvers, the logging of them is not possible.