Understand VA Communication with Umbrella and Local DNS

Contents

Introduction

This document describes how the VA communicates with Cisco Umbrella and local DNS.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Introduction

The Virtual Appliance "talks" to both the Umbrella resolvers as well as local DNS, depending on the DNS query and user configuration. Unlike simpler DNS clients, the VA does not prioritize one server over the other, or do a simple round robin. Instead, the VA uses the process outlined here.

This ensures, after an initial query, that the best DNS server is used. This also explains why a DNS query can be slow for one query, but speed up significantly after the first in select scenarios.

Explanation

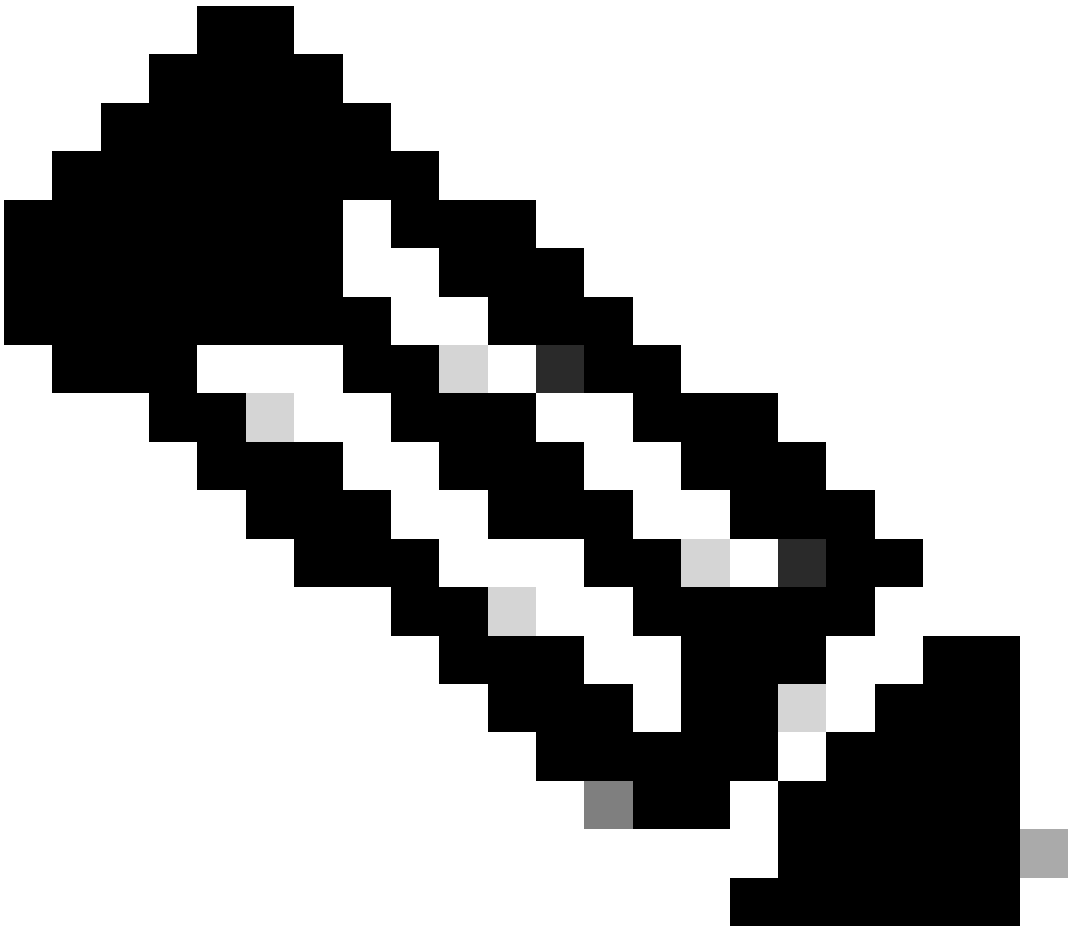
This article specifically refers to the Umbrella Virtual Appliances (VAs). The forwarder queries servers in a random order using an increasing set of timeout values until it gets a response. How it deals with servers that do not respond within the given timeouts is discussed in the rest of this article.

Caches

The VA forwarder maintains an RTT (round trip time) cache for use when deciding if a query can be sent to a server.

The RTT is a measure in seconds of how long it took for Umbrella to get a response from a server. Each time the forwarder sends a query to a server, it caches the RTT for 15 minutes. Once that expires, the RTT is effectively 0 for that server which resets it to the default state of "use this server."

If a server ultimately fails to respond at the highest timeout level, Umbrella tries it once more and then reply to the client with a SERVFAIL if it fails to respond. Any subsequent queries of this nature can be retried against the servers in question according to the current timeout level.



> **Note**: DNS responses are not cached on the VA. The data that is cached is how long an authoritative nameserver takes to respond for a given domain.

This process determines which local DNS server and which of Umbrella's public resolvers respond the quickest, and ensures that it is used rather than doing a round robin every time. This allows for avoiding sending DNS to a local DNS server that went down, for example.