Configure Internal DNS Servers for Umbrella Deployment

Contents

Introduction

Configure the Internal DNS Servers

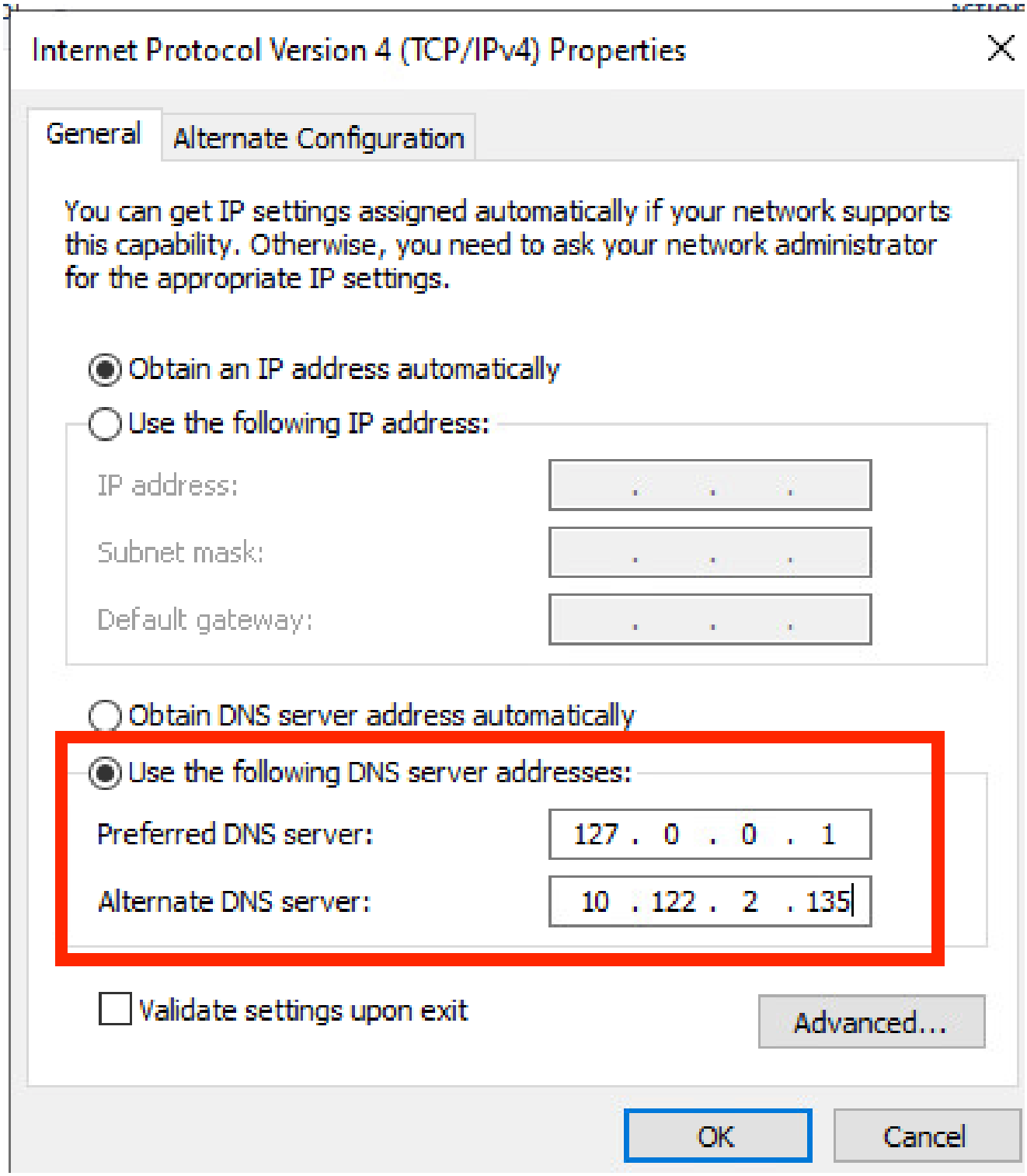
Introduction

This document describes how to configure the internal DNS servers to deploy the VA component of Cisco Umbrella.

Configure the Internal DNS Servers

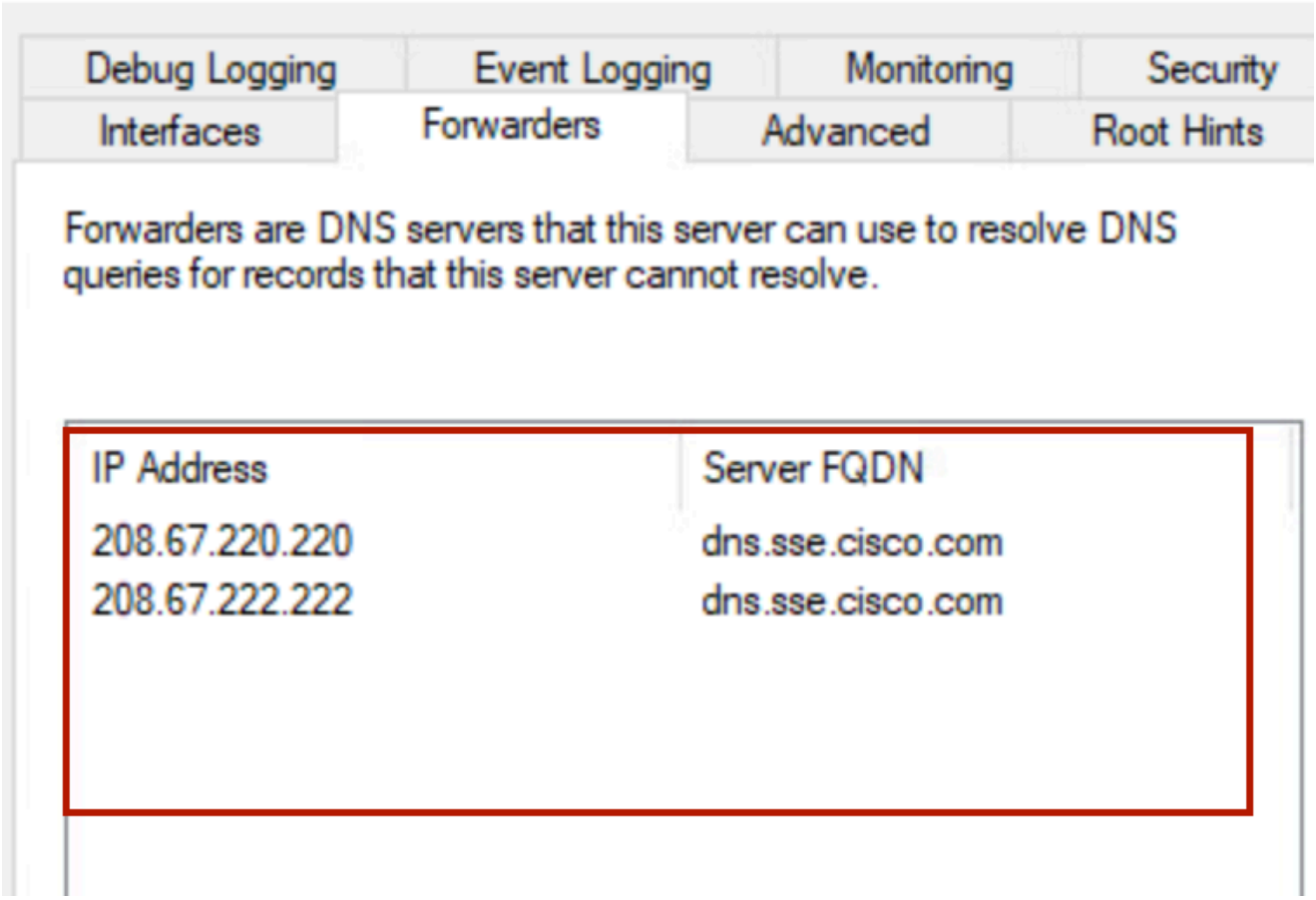
To deploy the virtual appliance (VA) component of Cisco Umbrella, we recommend this DNS configuration on any internal DNS server.

1. In DNS server's network adapter settings, use the loopback address (127.0.0.1) so that the server uses itself for DNS resolution. The second entry must be another internal DNS server.



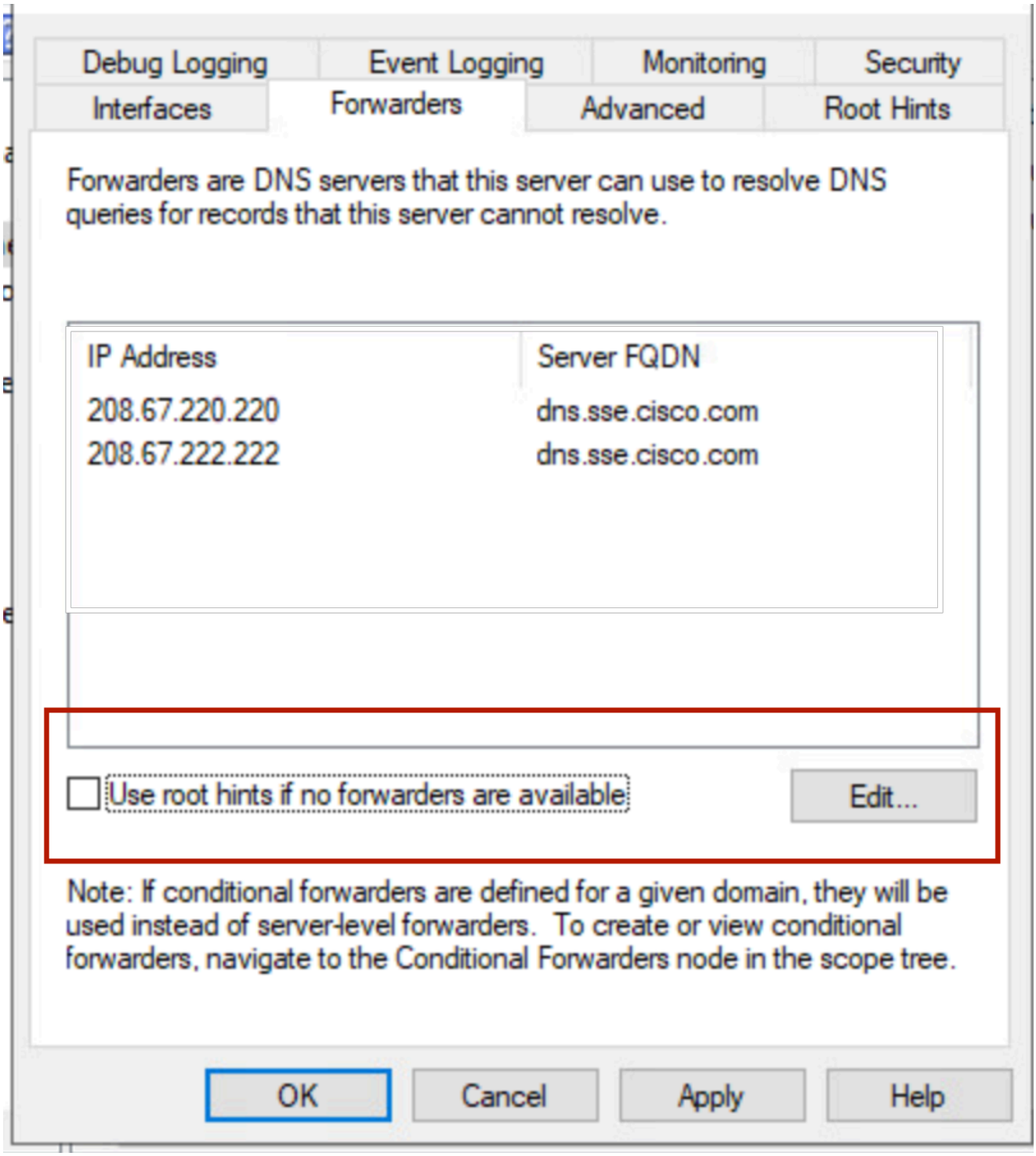
26492560404372

2. In DNS server's forwarder settings, use the Umbrella anycast addresses (208.67.220.220 and 208.67.222.222), and not the virtual appliance IP addresses. Forwarding DNS queries from DNS server to virtual appliances can cause DNS loops, and is not recommended nor supported per https://docs.umbrella.com/deployment-umbrella/docs/6-local-dns-forwarding.

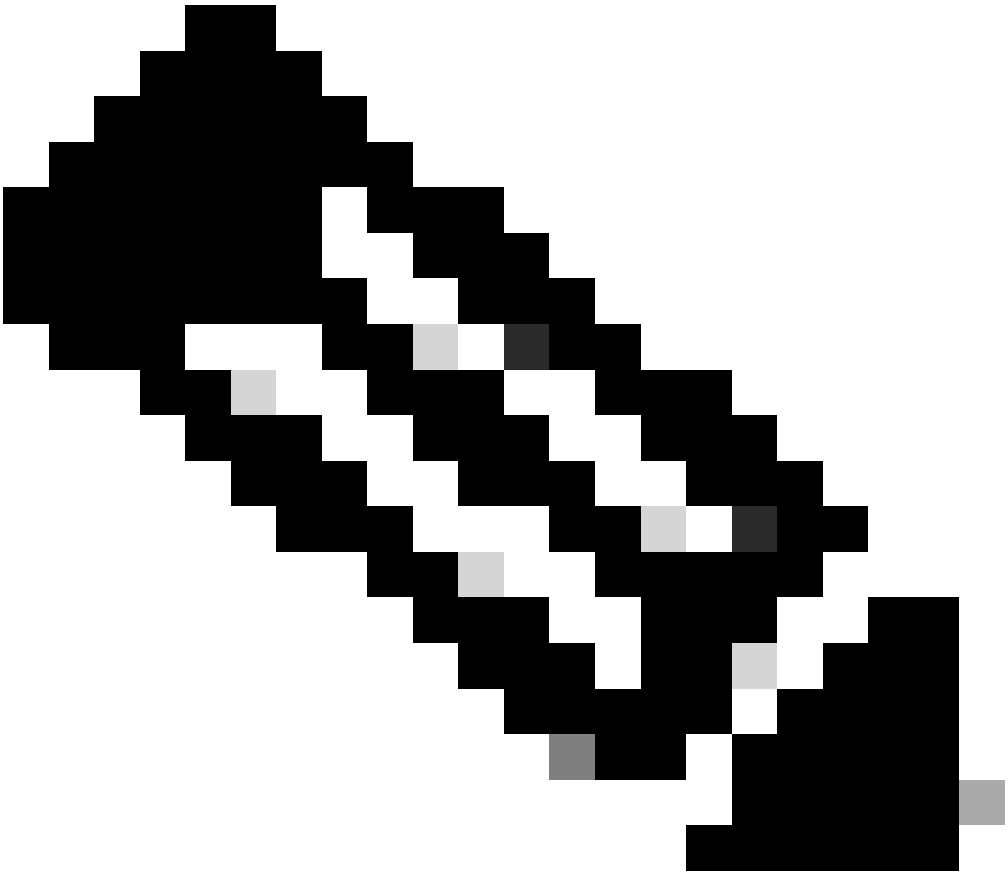


26492637809300

3. If you use a Windows DNS server, consider to uncheck the "Use root hints" option as it can cause DNS traffic to be bypassed in some instances. For more information on this best practice, please reference our article that discusses root hints further.



26492657078036



Note: Whether to use root hints as the last resort in forwarder configuration is up to your discretion. If you uncheck the "Use root hints" option, it is possible that there can be some situations where your DNS server is not able to resolve external domains. You do not have to uncheck the option if you do not feel comfortable doing so.

4. If the server also acts as a mail server, the best option is to point forwarder to your ISP's DNS servers or other recursive resolvers such as those provided by your ISP. We outline potential problems with using Umbrella on mail servers in these articles:
    - Umbrella and Your Email Server
    - Does Umbrella Work with DNSBLS and URIBLS?