F5 Load Balancer DNS Forwarding Configuration for Secure Access

Contents

Issue

DNS resolution was not working when using an F5 load balancer as the client DNS server during Umbrella to Secure Access migration. When DNS requests hit the Virtual IP (VIP), the F5 load balancer successfully forwarded packets to backend DNS forwarders, but hostnames were not resolving on endpoint machines. The DNS resolution worked fine when using a virtual appliance directly as the client DNS server, indicating the issue was specific to the F5 load balancer configuration.

Packet captures revealed that DNS replies were using the virtual appliance IP address instead of the expected F5 VIP address. The client computer was expecting DNS replies to come from the F5 VIP address , but instead received replies from the backend virtual appliance IP address.

Environment

- Cisco Umbrella to Secure Access migration environment
- F5 load balancer with DNS load balancing VIP configured
- Multiple DNS forwarders as backend servers
- Virtual appliances serving as DNS servers
- Client endpoints requiring DNS resolution through the load balancer

Resolution

The issue was resolved by configuring the F5 load balancer to properly act as a proxy between the client computers and the virtual appliances. The key configuration change involved enabling Source Network Address Translation (SNAT) with auto-map functionality.

Diagnostic Steps Performed

Step 1: Verify DNS resolution behavior

DNS resolution was tested using both the F5 load balancer VIP and direct virtual appliance connections to isolate the issue.

Step 2: Capture and analyze DNS traffic

Packet captures were performed to analyze the DNS request and response flow through the F5 load balancer.

Step 3: Identify source address mismatch

Analysis revealed that DNS replies contained the virtual appliance IP address instead of the F5 VIP address, causing client confusion.

Configuration Change

Step 1: Access F5 load balancer configuration

Navigate to the F5 load balancer management interface to modify the DNS VIP configuration.

Step 2: Enable SNAT auto-map

Configure SNAT (Source Network Address Translation) to auto-map on the F5 load balancer. This ensures that the F5 device properly proxies DNS requests and responses between clients and backend DNS servers.

Step 3: Verify configuration

After implementing the SNAT auto-map configuration, DNS resolution began working correctly through the F5 load balancer.

Cause

The root cause was improper Source Network Address Translation (SNAT) configuration on the F5 load

balancer. Without SNAT auto-map enabled, the F5 device was not properly acting as a proxy for DNS traffic. This caused DNS responses to be sent directly from the backend virtual appliances to the client computers, using the virtual appliance IP address as the source instead of the expected F5 VIP address. Client computers expected DNS responses to originate from the same IP address they sent their requests to (the F5 VIP), but were receiving responses from different IP addresses (the backend servers), causing DNS resolution failures.

Related Content

- Configure F5 GTM Load Balancing
- Cisco Technical Support & Downloads