Umbrella DNS Security Co-existence Issues with Broadcom WSS on macOS

Contents

Issue

The Umbrella module is not intercepting DNS traffic on macOS when co-existing with Broadcom WSS (Web Security Service). When the WSS agent is configured to intercept specific web ports like 80 and 443, the Umbrella DNS security functionality fails to capture all DNS queries. However, when WSS is disabled, Umbrella resumes intercepting DNS traffic as expected. Only certain DNS queries are being processed by Umbrella when WSS is enabled, rather than all DNS traffic being intercepted.

Environment

- Operating System: macOS
- Cisco Umbrella DNS Security module
- Broadcom WSS (Web Security Service) agent
- WSS agent configured to intercept web ports 80 and 443

Resolution

This issue has been analyzed and determined to be an architectural limitation of macOS where DNS Security cannot co-exist with WSS in the current macOS architecture. This limitation applies to both Infoblox and Cisco Umbrella DNS security solutions.

Technical Analysis

The root cause is related to macOS DNS proxy limitations:

- Only one DNS proxy can be active in the system at a time due to macOS limitations
- If DNS resolvers are bound to utunX interfaces or proxy-injected resolvers, then macOS resolves DNS inside the tunnel, not via Umbrella

- When another NEDnsProxyProvider is active on the system on macOS, Umbrella will not intercept DNS traffic

Diagnostic Commands

To verify which DNS resolver is taking priority on macOS, use the following command:

```
scutil --dns
```

This command will show which resolver is marked as: Scoped, Supplemental, or Interface: utunX, helping to identify DNS proxy conflicts.

Workaround Options

For macOS environments, WSS will continue to intercept DNS without any separate DNS Agent. To move forward with DNS security coverage, one option would be to implement to support a Passive Bypass architecture. With this approach, the provider would completely bypass the flow, allowing the traffic to be processed as if the provider was not active.

Cause

The issue is caused by macOS architectural limitations where only one NEDnsProxyProvider can be active on the system at a time. When both Umbrella DNS Security and Broadcom WSS are installed, they compete for DNS proxy control, resulting in WSS taking priority and preventing Umbrella from intercepting DNS traffic. This is a fundamental limitation of the macOS networking stack and affects all DNS security solutions, not just Cisco Umbrella.

Related Content

- Cisco Technical Support & Downloads