DNS Resolution Conflicts Between Cisco Secure Access and Banyan Security App

Contents

Issue

When Cisco Secure Access is deployed concurrently with the Banyan Security App on Windows endpoints, users experience significant DNS resolution slowdowns and timeouts. The specific symptoms include:

- DNS resolution begins to timeout when the Banyan Security App is connected.
- Web pages load very slowly despite eventually resolving.
- The Banyan App starts a local DNS proxy on a loopback interface, similar to Umbrella behavior.
- This DNS proxy configuration interferes with normal DNS resolution behavior.

The issue particularly impacts users who must access external environments while Cisco Secure Access is deployed for their primary network security.

Environment

- Cisco Secure Access deployed with Internet Access components (Roaming Module, VA, DNS, SWG, PAC, IPS, Certificates)
- Banyan Security App running on Windows endpoints
- Users requiring access to external environments through Banyan while maintaining Secure Access connectivity
- DNS proxy services running on loopback interfaces from both applications
- Internal domain bypass already configured in Secure Access for FQDN resolution

Resolution

To resolve the DNS resolution conflicts between Cisco Secure Access and Banyan Security App, implement these approaches:

Primary Resolution Steps

This is a known Cisco Bug ID CSCwr21575 which addresses known DNS proxy conflicts between Cisco Secure Access and third-party security applications that implement local DNS proxies.

Symptom

DNS resolution times out or is significantly delayed.

Conditions

- DNS query intercepted by Cisco Secure Client Umbrella module.
- The primary DNS server is configured to an IP address from the loopback range 127.0.0.0/8 and the DNS query targets that server.
- There is at least one other non-loopback IPv4 DNS server on the same or another adapter.

Workaround

Set the primary DNS server to a non-loopback IP address. The permanent fix is to upgrade Cisco Secure Client to 5.1.13 and above.

Verification and Testing

After implementing the resolution steps, perform this validation:

- Test DNS resolution speed with both Cisco Secure Access and Banyan Security App active
- Verify web page loading times return to acceptable levels
- Confirm that access to external environments through Banyan continues to function
- Validate that internal domain resolution through Secure Access bypass remains operational

Cause

The DNS resolution slowdown is caused by conflicting DNS proxy implementations between Cisco Secure Access and the Banyan Security App. Both applications establish local DNS proxies on loopback interfaces, creating competing DNS resolution paths that result in timeouts and delayed responses.

The Banyan Security App DNS proxy behavior interferes with Cisco Secure Access DNS handling, particularly affecting the order and priority of DNS query processing on Windows endpoints.

Cisco bug ID CSCwr21575 addresses this specific compatibility issue.

Related Content

- Cisco Technical Support & Downloads