DNS Server IP Address Configuration for Secure Client Roaming

Contents

Issue

When deploying the Secure Client Roaming module for Secure Access DNS Advantage, users are unable to locate configuration options in the portal to define DNS server IP addresses for client machines. Despite the absence of visible configuration options, all client computers are automatically sending DNS queries to the well-known DNS server IP addresses 208.67.222.222 and 208.67.220.220. Users require clarification on whether these DNS server addresses are:

- Fixed and hard-coded in the Secure Client code with no option to change them
- Pushed to user computers through an alternative mechanism not visible in the portal
- Configurable through a different method or location within the system

Environment

- Cisco Secure Access DNS Advantage product
- Secure Client Roaming module deployment
- Client computers configured with Secure Client
- DNS queries being sent to 208.67.222.222 and 208.67.220.220

Resolution

The DNS server IP addresses 208.67.222.222 and 208.67.220.220 used by the Secure Client Roaming module are part of the standard DNS interception and redirection behavior implemented in Secure Access DNS Advantage. This behavior is documented in the official Cisco documentation regarding DNS interception and redirection functionality.

The DNS server addresses are automatically configured as part of the Secure Client Roaming module's standard operation and do not require manual configuration through the portal interface. The system is designed to automatically direct DNS queries to these specific OpenDNS resolver addresses to ensure proper security filtering and policy enforcement.

For detailed information about this behavior and the underlying mechanisms, users should review the official Cisco documentation that specifically covers DNS interception and redirection behavior within the Secure Access DNS Advantage solution.

Cause

This is the intended design behavior of the Secure Access DNS Advantage product. The DNS server addresses 208.67.222.222 and 208.67.220.220 are automatically implemented as part of the DNS interception and redirection functionality to ensure that all DNS queries from protected endpoints are routed through the Cisco security infrastructure for proper policy enforcement and threat protection.

Related Content

- Cisco documentation regarding DNS interception and redirection behavior for Secure Access DNS Advantage
- Cisco Technical Support & Downloads