VPN Client Unable to Successfully Verify IP Forwarding Table Modification Error on Secure Client RAVPN Split-Tunnel/Default DNS

Contents

Issue

Mac users experience intermittent failures when attempting CLI authentication to internal applications while connec
and `dig` succeed. The issue occurs randomly and can be temporarily resolved by reconnecting the VPN, after which
tunnel VPN is in use, and Cisco Umbrella is active. The problem does not occur when using Palo Alto GlobalProtect

- Error message: "host not found" on CLI authentication and `curl` commands.
- Error message: VPN client unable to successfully verify IP forwarding table modifications. Domain name serv
- `nslookup` and `dig` commands succeed
- Intermittent connectivity after reconnecting VPN
- Split-tunnel remote access VPN and Umbrella module enabled
- Issue reproducible only with Cisco Secure Client VPN on MacOS devices

Environment

- Product: Cisco Secure Client (CSC) with multiple modules
- Platform: Corporate Mac devices
- VPN Profile Configuration: Remote access VPN Profile - Bypass Secure access - Split-tunnel Mode and DNS mode selected as "Default DNS"
- DNS Filtering: Cisco Umbrella enabled
- Module Versions:
  - Cloud Management v1.0.0.23
  - AnyConnect VPN v5.1.13.177
  - Umbrella v5.1.13.177
  - DART v5.1.13.177
  - Secure Firewall Posture v5.1.13.177
  - Network Visibility Module v5.1.13.177
- Diagnostic Data: DART bundles collected for analysis
- Observed only on Cisco Secure Client VPN (not on Palo Alto GlobalProtect)

Resolution

- During debugging of the VPN profile (`naic.org`) split-tunnel configuration and the AnyConnect VPN routing table on the client side, this behavior was observed:
  - Working scenario - When performing a `nslookup` for the Vault non-prod local domains, DNS requests handled by the DNS servers configured within the VPN profile resolv secured routes.
  - Non-working Scenario - However, when the same DNS requests were handled by the macOS system’s local DNS (192.168.x.x)
  - the private domains resolved to IP range of 34.x.x.x , which led to the connectivity issue. Wireshark cap

- From a design and configuration standpoint, with a split-tunnel VPN profile setup, it is recommended to use split DNS rather than relying on local system DNS/default
- Additionally, the `us-east-eks-amazonaws.com` entry has been added to ensure traffic for this EKS cluster is correctly steered through the remo
- Also discussed was that the RAVPN interface must take precedence over the Umbrella module and should not file containing the Umbrella Organization ID.
- During our troubleshooting process, we have done fresh install of CSC client without Umbrella module, with t

This align with issue resolve when there is no Umbrella module in place. With proper VPN profile configuration inc

The user confirmed that issue has been resolved after modifying the DNS mode to Split tunnel and edited the VPN p

Cause

VPN profile - Bypass Secure Access -
DNS mode supposed to set to Split Tunnel (most commonly seen options from a use case scenarios) and include all

Related Content

- Cisco Technical Support & Downloads