Excessive DNS Requests on Port 53 During AnyConnect VPN Sessions

Contents

Issue

After implementing Remote Access VPN (RA-VPN), users connecting via Cisco AnyConnect are generating dozens of DNS requests on port 53 to the secondary DNS server. This behavior is observed in the Activity Monitor for all users connected to the VPN tunnel and results in numerous allowed requests flooding the tunnel. This excessive DNS activity is not occurring when users connect via Zero Trust Access (ZTA), indicating that the issue is specifically related to the AnyConnect VPN connection method.

Environment

- Product Family: Secure Access
- Implementation: Remote Access VPN deployment
- Comparison environment: Zero Trust Access (ZTA) - not experiencing the same DNS flooding behavior

Resolution

Investigating the excessive DNS requests requires log collection and analysis to identify the root cause of the DNS flooding behavior. The log collection includes collecting packet capture that includes PID for each packet to determine what application on an endpoint is generating the traffic and Process Monitor output.

Cause

The analysis showed this amount of DNS traffic is expected.

Related Content

- Cisco Technical Support & Downloads