Remote Access Users Unable to Reach Internal Services Over RAVPN

Contents

Issue

Remote Access users using Secure Access were unable to reach internal services, including the Domain Controller at headquarters, while internet access continued to work normally. Users could browse the internet successfully but could not access internal resources such as the Domain Controller over RAVPN (Remote Access VPN).

Environment

- Cisco Secure Access - Secure Client Remote Access (VPN, Posture, Private Resource)
- RAVPN (Remote Access VPN) tunnels reported as up and healthy
- SD-WAN infrastructure in use
- Internal DNS servers at headquarters
- Domain Controller services at headquarters location
- Multiple branch networks connected via the infrastructure

Resolution

The following troubleshooting and resolution steps were performed to address the Remote Access connectivity issue:

Step 1: Packet Capture Analysis

Collect Simultaneous Packet Capture from client and your Edge Device(bidirectional) to analyze traffic flow patterns.

Flow:

RA VPN Client ----------Cisco Secure Access --------Ipsec tunnel ---------- Edge Device ---------Private Resource

- Confirm if DNS queries from clients were successfully reaching Edge Device and being to sent towards DNS server.
- Check if No DNS replies were observed returning from local DNS server to the clients
- Local DNS server was sending a response however those responses never made back to tunnel interface.

Step 2: Root Cause Identification

Based on the packet capture analysis, the issue was identified as a return-path routing problem. The traffic analysis indicated that while DNS queries were successfully reaching the local DNS server through the Cisco Secure Access infrastructure, the return traffic containing DNS responses was not reaching the Remote Access clients due to routing or configuration issues on your Infrastructure.

Step 3: Configuration Review and Remediation

Review and correct the internal network configuration and internal network configuration, specifically focusing on:

- DNS configuration and return traffic routing
- Internal routing policies for VPN return traffic
- Internal network routing configuration
- Missing configuration elements on the Edge Device side

Step 4: Service Restoration Verification

Following the configuration review and corrections, Secure Access functionality was largely restored. Most

Remote Access users regained access to internal services including the Domain Controller at headquarters.

Cause

The root cause was identified as a return-path routing issue within the internal network infrastructure. While DNS queries from Remote Access clients were successfully reaching the local DNS server through the Cisco Secure Access Infrastructure the return traffic containing DNS responses was not properly routed back to the clients. This was caused by missing or incorrect configuration on the internal network infrastructure side that prevented DNS replies and TCP responses from reaching the Remote Access clients over the VPN connection.

Related Content

- Cisco Technical Support & Downloads