Jabber DNS SRV Record Resolution Issues with Cisco Secure Access VPN

Contents

Issue

When implementing Cisco Secure Access VPN, Jabber clients experience connectivity issues due to DNS SRV record resolution conflicts. The problem occurs when Jabber reaches out to two DNS SRV records: one for the CUCM (_cisco-UDS) and one for ExpressWay (_collab-edge). If the CUCM SRV record resolves, regardless of whether it works, Jabber assumes it is on-premises and attempts to connect to the CUCM instead of ExpressWay. This behavior is evident in Jabber logging with the **bEdgeServerFlag = 0** seen in Jabber.log. Additionally, the ExpressWay SRV record fails because it is being sent to the private DNS server that the Secure Client uses for resolution, and the private DNS server does not recursively find this public SRV record.

Environment

- Cisco Secure Access (formerly Cisco AnyConnect Secure Mobility Client)
- Cisco Jabber client
- Cisco Unified Communications Manager (CUCM)
- Cisco ExpressWay for mobile and remote access
- DNS infrastructure with both private and public DNS servers
- VPN tunnel configuration with split tunneling capabilities

Resolution

The issue was resolved by routing Jabber traffic through the VPN tunnel instead of attempting to manually configure the client for ExpressWay connectivity. This approach ensures that Jabber traffic uses the appropriate DNS resolution path and avoids the SRV record conflict that causes the client to incorrectly assume on-premises connectivity.

Troubleshooting Steps

Step 1: Analyze DNS SRV record queries using wireshark packet capture.

```
Use Wireshark filter: dns.qry.type == 33
```

Step 2: Review Jabber logs for edge server flag status

```
Check Jabber.log for: bEdgeServerFlag = 0
```

Step 3: Verify DNS resolution behavior for both SRV records

Check resolution of:

- _cisco-UDS SRV record (CUCM)
- _collab-edge SRV record (ExpressWay)

Solution Implementation

Configure the Cisco Secure Access VPN client to include Jabber traffic in the tunnel rather than allowing it to resolve DNS queries through the local/private DNS server. This ensures that:

- Jabber traffic uses the correct DNS resolution path
- SRV record conflicts are avoided
- ExpressWay connectivity is properly established
- Full Jabber functionality is maintained

This solution is preferred over manually configuring the Jabber client for ExpressWay, which would result in loss of some functionality.

Cause

The root cause is the DNS SRV record resolution logic in Jabber clients. When Jabber starts, it queries for two specific DNS SRV records: _cisco-UDS (for CUCM) and _collab-edge (for ExpressWay). The client decision-making process prioritizes the CUCM SRV record - if this record resolves successfully, Jabber assumes it is operating in an on-premises environment and sets bEdgeServerFlag = 0, regardless of whether the actual CUCM connection works or whether the ExpressWay SRV record also resolves.

In VPN scenarios with split tunneling, the ExpressWay SRV record (_collab-edge) is sent to the private DNS server used by the Secure Client. Since this is typically a public DNS record and the private DNS server does not perform recursive lookups for external records, the ExpressWay SRV resolution fails. This compound issue results in Jabber being unable to establish proper connectivity through either path.

Related Content

- Cisco Technical Support & Downloads