Cisco Secure Access Fragmented ICMP Packet Handling

Contents

Issue

ICMP echo requests larger than the MTU are not receiving replies when sent with the DF (Don't Fragment) bit disabled. This behavior occurs in two specific scenarios:

- From RAVPN endpoints over the VPN interface when sending ICMP packets that exceed the VPN interface MTU size with the DF bit cleared
- From on-premise endpoints over an IPsec tunnel between a site router and Cisco Secure Access (CSA) when sending ICMP packets that exceed the IPsec tunnel interface MTU size with the DF bit cleared

In both cases, no ICMP responses are received, leading to questions about whether CSA drops fragmented packets with the DF bit disabled.

Environment

- Cisco Secure Access (CSA)
- RAVPN (Remote Access VPN) endpoints
- IPsec tunnels between site routers and CSA
- ICMP traffic exceeding interface MTU sizes
- Fragmented packet scenarios with DF bit cleared

Resolution

Cisco Secure Access drops fragmented packets in both underlay and overlay scenarios. This behavior is documented in the Cisco Secure Access Help documentation, which explicitly states: "Fragmented packets in the underlay or overlay are dropped."

Expected Behavior

Cisco Secure Access is designed to drop fragmented packets regardless of whether they occur in the underlay or overlay network. This applies to:

- ICMP packets sent from RAVPN endpoints that exceed the VPN interface MTU with DF bit cleared
- ICMP packets sent from on-premise endpoints over IPsec tunnels that exceed the tunnel interface MTU with DF bit cleared

This behavior is consistent across all scenarios involving fragmented packets within the Cisco Secure Access infrastructure.

Feature request CSE-I-5739 has been created for this.

Cause

Cisco Secure Access is architected to drop fragmented packets as a security and performance design decision. This behavior is implemented to prevent potential security vulnerabilities and processing overhead associated with packet reassembly in both underlay and overlay network scenarios.

Related Content

- Cisco Secure Access Help Documentation - Fragmented Packet Handling
- Cisco Technical Support & Downloads