Azure VPN Client Connection Failure with Secure Access Web Security Enabled

Contents

Issue

After migrating from Umbrella to SSE and enabling Web Security with a newly assigned SIA license, Azure VPN Client connections fail to establish for users when Web Security is enabled. The Azure VPN client connectivity issue affects all clients, preventing them from connecting to the VPN. When the Cisco Secure Access Client is uninstalled from client machines, VPN connectivity is restored, indicating that the Secure Access client is blocking the connection to Azure VPN services.

Disabling Web Security or uninstalling the Cisco Secure Access Client restores VPN connectivity, but this impacts user access to resources over Azure VPN when Web Security protection is needed.

Environment

- Cisco Secure Access (formerly SIA) with Web Security enabled
- Azure VPN Client
- Migration from Umbrella to SSE completed
- Newly assigned SIA license

Resolution

The resolution involves adding the Azure VPN gateway public IP address to the SSE/SWG exception list to prevent traffic interception that blocks VPN connections.

Step 1: Identify the Azure VPN Gateway IP Address

Determine the public IP address of the Azure VPN gateway.

Step 2: Add IP-Based Exception to SSE/SWG

1.- Add the Azure Virtual gateway public IP address to the SSE/SWG exception list in the Cisco Secure Access environment.

2.- Log in to Cisco Secure Access Dashboard - Click Connect - End user Connectivity - Internet Security - Add exception. This prevents the Secure Web Gateway from intercepting and inspecting traffic destined for the Azure VPN gateway.

Step 3: Test VPN Connectivity

After applying the IP-based exception, test the Azure VPN connection to verify that clients can successfully establish VPN connections with Web Security enabled.

Step 4: Expand Testing

Extend testing of the IP-based exception to additional users across the environment to ensure consistent functionality before considering the resolution complete.

Cause

The issue occurs because the Secure Web Gateway (SWG) exception mechanism requires a DNS lookup for a domain to create a domain-to-IP cache entry. When the Azure VPN client connects directly to the IP address without performing a DNS query for the VPN URL, the SWG module cannot map the domain to the IP address. As a result, the SWG continues to inspect and intercept traffic to the IP address, preventing the VPN connection from establishing.

Packet capture analysis showed no DNS queries for the VPN URL and no visible SWG interception traffic for the Azure gateway IP, confirming that the SWG was blocking the connection due to the lack of proper domain-to-IP mapping in its cache.

Related Content

- Cisco Technical Support & Downloads