Omnissa Full Client Connectivity Issues Through Secure Access

Contents

Issue

The Omnissa full client is unable to load virtual desktops when connected through Cisco Secure Access. Users experience connectivity failures when attempting to establish connections to virtual environments using the full client application. However, access through the HTML/web client continues to work normally, indicating that the underlying virtual desktop infrastructure is functional but there is a specific issue affecting the full ability of the client to establish connections through the Cisco Secure Access solution.

Environment

- Technology: Solution Support (SSPT - contract required)
- Sub-technology: Cisco Secure Access
- Product Family: SECACCS
- Software Version: All versions affected
- Client Application: Omnissa full client
- Virtual Desktop Environment: Omnissa virtual desktops
- Network Infrastructure: IPsec tunnels and FTD (Firepower Threat Defense)

Resolution

The resolution involves implementing specific network configuration changes to enable proper routing for the Omnissa full client through Cisco Secure Access. These steps were taken to resolve the connectivity issue:

- Configure split-tunnel settings. Add split-tunnel configurations to allow the Omnissa full client to

establish direct connections to the required destination hosts. This configuration ensures that traffic destined for specific virtual desktop clients is properly routed through the appropriate network paths.

- Implement static route configurations. Configure static routes for the specific clients that need to establish connections to virtual desktops. The key requirement is to configure routes not just to the aggregation server downstream, but directly to the destination hosts that the virtual desktop clients need to reach.
- Clear IPsec tunnels. After implementing the configuration changes, clear the IPsec tunnels on the FTD to ensure that the new routing configurations take effect properly.
- Validate connectivity. Test the Omnissa full client connectivity after implementing the changes to confirm that virtual desktop connections can be established successfully through Cisco Secure Access.

Implementation Schedule

The configuration changes must be implemented during a scheduled maintenance window to minimize impact on users. After implementation, validate both reachability and Omnissa full client connectivity to ensure the resolution is successful.

Cause

The connectivity issue was caused by insufficient routing configurations in the Cisco Secure Access environment. Specifically, the network was configured with routes only to the aggregation server downstream, but lacked the necessary split-tunnel and static route configurations for the specific clients that the Omnissa full client needed to establish connections to. This routing gap prevented the full client from properly reaching the virtual desktop hosts, while the HTML/web client could still function because it used different connection paths that were properly configured.

Related Content

- Cisco Technical Support & Downloads