Troubleshoot Azure Virtual Desktop Connectivity Issues

Contents

Issue

Azure Virtual Desktop (AVD) connections fail when users access AVD from the office network with Cisco Secure Access enabled. This specific behavior was observed:

- AVD works fine when accessed from a personal network with Secure Access disabled.
- AVD works fine when accessed from the office network without Secure Access.
- AVD does not work when accessed from any network with Secure Access enabled.

This connectivity failure impacts users' ability to access their virtual desktops and affects production business operations. Packet capture analysis showed bidirectional traffic in both working and non-working scenarios with no TCP resets or other network-level indicators that Secure Access was terminating the AVD connection.

Environment

- Cisco Secure Access with Zero Trust Network Access (ZTNA) enabled
- ZTNA profile configured to use ZTA for all internet destinations
- Azure Virtual Desktop (AVD) deployment accessed through Microsoft endpoints
- Office network environment with Secure Access client deployed
- Users accessing AVD from both office and personal networks

Resolution

The issue was resolved by adding Microsoft AVD-related domains to the ZTA Exceptions list, allowing the Secure Access client to bypass ZTNA for AVD traffic.

Diagnostic Analysis

Joint troubleshooting analysis determined that the ZTNA profile was configured to use ZTA for all internet destinations, which caused Secure Access to route AVD's continuous WebSocket traffic through the Secure Access cloud proxy. This behavior led to session drops because Azure Virtual Desktop uses complex, continuous traffic (WebSockets) to stream desktop sessions in real-time, and cloud proxies are designed to inspect standard web pages rather than handle streaming protocols.

Configuration Change

These Microsoft AVD-related domains were added to the ZTA Exceptions list:

```
*.wvd.microsoft.com
*.core.windows.net
*.servicebus.windows.net
*.events.data.microsoft.com
```

By adding these domains to the ZTA Exceptions list, the Secure Access client was instructed to completely ignore AVD-specific traffic. This allows AVD traffic to go directly to Microsoft, bypassing the ZTNA proxy entirely, which is exactly what Microsoft requires for AVD to function properly.

Validation

After applying the ZTA Exceptions configuration, AVD connectivity was reported as working normally during the monitoring period. Users were able to successfully access their virtual desktops from the office network with Secure Access enabled.

Cause

The root cause was the ZTNA profile configuration that intercepted all internet-bound traffic, including Azure Virtual Desktop connections. When AVD's WebSocket traffic was routed through the Secure Access cloud proxy for inspection, it caused connection drops because the proxy was not designed to handle the

continuous streaming nature of AVD sessions. AVD requires direct connectivity to Microsoft endpoints to maintain stable desktop streaming sessions.

Related Content

- Microsoft Azure Virtual Desktop Required FQDN Endpoints
- Troubleshoot and Collect Basic Information for Cisco Secure Access
- Cisco Technical Support & Downloads