Lösen von Verbindungsproblemen mit Azure Virtual Desktop

Inhalt

Problem

Azure Virtual Desktop (AVD)-Verbindungen schlagen fehl, wenn Benutzer über das Büronetzwerk mit aktiviertem Cisco Secure Access auf AVD zugreifen. Dieses spezifische Verhalten wurde beobachtet:

- AVD funktioniert einwandfrei, wenn der Zugriff von einem persönlichen Netzwerk mit deaktiviertem sicherem Zugriff erfolgt.
- AVD funktioniert einwandfrei, wenn der Zugriff vom Büronetzwerk aus ohne sicheren Zugriff erfolgt.
- AVD funktioniert nicht, wenn der Zugriff von einem Netzwerk mit aktiviertem sicherem Zugriff aus erfolgt.

Dieser Verbindungsausfall beeinträchtigt die Zugriffsmöglichkeiten der Benutzer auf ihre virtuellen Desktops und den Produktionsbetrieb. Die Paketerfassungsanalyse zeigte bidirektionalen Datenverkehr sowohl in funktionierenden als auch in nicht funktionierenden Szenarien ohne TCP-Resets oder andere Indikatoren auf Netzwerkebene an, dass Secure Access die AVD-Verbindung terminierte.

Umwelt

- Cisco Secure Access mit ZTNA-Unterstützung (Zero Trust Network Access)
- ZTNA-Profil zur Verwendung von ZTA für alle Internetziele konfiguriert
- Azure Virtual Desktop (AVD)-Bereitstellung, auf die über Microsoft-Endgeräte zugegriffen wird
- Netzwerkumgebung im Büro mit implementiertem Secure Access-Client

- Benutzer, die von Büro- und privaten Netzwerken auf AVD zugreifen

Auflösung

Das Problem wurde behoben, indem der ZTA-Ausnahmeliste Microsoft AVD-bezogene Domänen hinzugefügt wurden, sodass der Secure Access-Client ZTNA für AVD-Datenverkehr umgehen konnte.

Diagnoseanalyse

Die gemeinsame Fehlerbehebungsanalyse ergab, dass das ZTNA-Profil so konfiguriert wurde, dass es ZTA für alle Internetziele verwendet. Dies führte dazu, dass Secure Access den kontinuierlichen WebSocket-Datenverkehr von AVD über den Secure Access-Cloud-Proxy weiterleitete. Dieses Verhalten führte zum Verwerfen von Sitzungen, da Azure Virtual Desktop komplexen, kontinuierlichen Datenverkehr (WebSockets) zum Streamen von Desktop-Sitzungen in Echtzeit verwendet und Cloud-Proxys so konzipiert sind, dass sie Standard-Webseiten prüfen, statt Streaming-Protokolle zu verarbeiten.

Konfigurationsänderung

Diese Microsoft AVD-bezogenen Domänen wurden der ZTA-Ausnahmeliste hinzugefügt:

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

Durch Hinzufügen dieser Domänen zur ZTA-Ausnahmeliste wurde der Secure Access-Client angewiesen, AVD-spezifischen Datenverkehr vollständig zu ignorieren. Auf diese Weise kann AVD-Datenverkehr direkt an Microsoft weitergeleitet werden, wobei der ZTNA-Proxy vollständig umgangen wird. Dies ist genau das, was Microsoft benötigt, damit AVD ordnungsgemäß funktioniert.

Validierung

Nach Anwendung der ZTA-Ausnahmekonfiguration wurde angegeben, dass die AVD-Verbindung während des Überwachungszeitraums normal funktionierte. Die Benutzer konnten über das Büronetzwerk mit aktiviertem sicherem Zugriff erfolgreich auf ihre virtuellen Desktops zugreifen.

Ursache

Die Hauptursache war die ZTNA-Profilkonfiguration, die den gesamten Internetdatenverkehr, einschließlich Azure Virtual Desktop-Verbindungen, abfing. Als der WebSocket-Datenverkehr von AVD zur Überprüfung über den Secure Access Cloud-Proxy geleitet wurde, führte dies zu Verbindungsabbrüchen, da der Proxy nicht für das fortlaufende Streaming von AVD-Sitzungen konzipiert war. AVD erfordert eine direkte Verbindung zu Microsoft-Endgeräten, um stabile Desktop-Streaming-Sitzungen aufrechtzuerhalten.

Verwandte Inhalte

- Für Microsoft Azure Virtual Desktop erforderliche FQDN-Endgeräte
- Fehlerbehebung und Erfassung grundlegender Informationen für Cisco Secure Access
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.