Sicherer Zugriff trennt gelegentlich Verbindungen hinter Unternehmens-Firewalls mit IdleTimeout-Fehler

Inhalt

- Problem
- Umwelt
- Auflösung
  - Schritt 1: MX TTL-Pufferkonfiguration implementieren
  - Phase 2: Konfigurieren erforderlicher Domänenausschlüsse
  - Schritt 3: Überprüfung der Port- und Protokollzulagen
  - Schritt 4: Behebung überwachen und validieren
- Ursache
- Verwandte Inhalte

Problem

Cisco Secure Access-Clients werden bei der Verbindung von Endgeräten mit dem Unternehmensnetzwerk zeitweilig getrennt und sofort wieder verbunden. Die Verbindungstrennung erfolgt nach dem Zufallsprinzip, wobei der Client nach etwa 5 Sekunden automatisch wieder eine Verbindung herstellt. Dieses Verhalten wird beobachtet, wenn der Internetdatenverkehr über ZTA (Zero Trust Access) an einen sicheren Zugriff von Endgeräten hinter Cisco FirePower- und Meraki MX-Geräten geleitet wird.

Das Windows-Ereignisprotokoll erfasst bestimmte "idleTimeout"-Fehler während dieser Trennungsereignisse. Das Trennungsmuster tritt nicht auf, wenn Benutzer von privaten

Internetverbindungen eine Verbindung herstellen. Dies weist darauf hin, dass das Problem speziell mit der Netzwerkinfrastruktur des Unternehmens zusammenhängt.

Das Symptom führt zu Unterbrechungen des Geschäftsbetriebs bei der sicheren Remote-Zugriffsverbindung für Benutzer, die in der Netzwerkumgebung des Unternehmens arbeiten, während Remote-Benutzer von diesem Verbindungsproblem nicht betroffen sind.

Umwelt

- Cisco Secure Access - vorteilhafte Bereitstellung
- Cisco Secure Internet Access (SIA) Client-Software
- Netzwerkinfrastruktur des Unternehmens mit Cisco FirePOWER Security Appliances
- Meraki MX Security Appliances im Netzwerkpfad
- ZTA-Konfiguration (Zero Trust Access) zum Proximieren des Internetdatenverkehrs zu sicherem Zugriff
- Windows-Endgeräte mit Ereignisprotokollierungsfunktion
- Gemischte Konnektivitätsszenarien: Firmennetzwerk (betroffen) und private Internetverbindungen (nicht betroffen)

Auflösung

Die Lösung beinhaltete die Implementierung von Konfigurationsänderungen auf dem Meraki MX-Gerät sowie die Sicherstellung der richtigen Domänenausschlüsse und Portfreigaben für die Secure Access-Integration.

Schritt 1: MX TTL-Pufferkonfiguration implementieren

Konfigurieren Sie einen MX-TTL-Puffer auf dem Meraki MX-Gerät, um das Verhalten des DNS-TTL-Caching zu beheben, das zu den Problemen mit der zeitweiligen Verbindungstrennung beigetragen hat. Mit dieser Konfigurationsänderung werden Zeitkonflikte zwischen der

Zwischenspeicherung der DNS-Auflösung und den erwarteten Verbindungen des Secure Access-Clients behoben.

Phase 2: Konfigurieren erforderlicher Domänenausschlüsse

Stellen Sie sicher, dass diese Domänen ordnungsgemäß vom Abfangen ausgeschlossen und nicht entschlüsselten Listen auf Cisco FirePower- und Meraki MX-Geräten hinzugefügt werden:

- ztna.sse.cisco.com
- zpc.sse.cisco.com
- Zusätzliche Dienstdomänen für den sicheren Zugriff, wie in der Richtlinienkonfiguration festgelegt

Schritt 3: Überprüfung der Port- und Protokollzulagen

Konfigurieren Sie die Firewall-Infrastruktur des Unternehmens so, dass die erforderlichen Ports und Protokolle für sicheren Zugriff über FirePower- und Meraki MX-Geräte zugelassen werden. Stellen Sie sicher, dass der Datenverkehr an Port 443 für Endgeräte des Secure Access-Dienstes ordnungsgemäß verarbeitet wird, ohne dass es durch eine Sicherheitsüberprüfung zu Interferenzen kommt, die zu einer Zeitüberschreitung führen können.

Schritt 4: Behebung überwachen und validieren

Nach der Implementierung der MX-TTL-Pufferkonfiguration sollte das Verhalten des Secure Access-Clients mehrere Tage lang überwacht werden, um sicherzustellen, dass das Muster für die zeitweilige Trennung und erneute Verbindung beendet wurde.

Ursache

Die unterbrochenen Verbindungen wurden durch das Zwischenspeicherungsverhalten von DNS TTL (Time To Live) verursacht, das in Konflikt zwischen der Netzwerkinfrastruktur des

Unternehmens und den Erwartungen an den sicheren Zugriff geriet. Die technische Analyse von Cisco hat ergeben, dass die DNS-TTL-Werte aufgrund des Zwischenspeicherungsverhaltens der Resolver variieren. Wechselnde IP-Adressen werden aufgrund von Lastverteilungsmechanismen in der Secure Access-Servicearchitektur erwartet.

Bei der Verarbeitung von DNS-Antworten für Endgeräte mit sicherem Zugriff durch Netzwerkgeräte des Unternehmens (Cisco FirePower und Meraki MX) kam es durch die Zwischenspeicherung und die TTL-Verarbeitung zu Timing-Diskrepanzen, die zu einem "idleTimeout" führten. Dieser Zeitkonflikt hat dazu geführt, dass der Secure Access-Client die Verbindung als inaktiv interpretiert und Verbindungs-/Wiederherstellungszyklen initiiert hat.

Das Problem war speziell auf die Netzwerkumgebung des Unternehmens zugeschnitten, da die privaten Internetverbindungen in der Regel nicht die gleiche Stufe von DNS-Caching und Datenverkehrsprüfung implementieren, die die Verwaltung des Verbindungsstatus des Secure Access-Clients beeinträchtigen kann.

Verwandte Inhalte

- 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.