Client-basierte ZTNA-Verkehrssteuerung bei sicherem Client

Inhalt

Problem

Client-basierter Zero Trust Network Access (ZTNA) ermöglicht beim Zugriff über FQDN oder direkte IP-Adressen keinen Zugriff auf interne Anwendungen, während dieselben Anwendungen über eine VPN-Verbindung weiterhin erreichbar sind.

Zu den beobachteten spezifischen Symptomen gehören:

- ZTNA (Secure Client) kann interne Anwendungen nicht über FQDN oder direkte IP erreichen, wenn die VPN-Verbindung getrennt wird.
- Der browserbasierte ZTNA-Zugriff funktioniert für dieselben Anwendungen einwandfrei.
- Bei VPN-Ausfall werden in den Aktivitätsprotokollen keine ZTNA-Ereignisse angezeigt. Dies weist darauf hin, dass der Client-Datenverkehr nicht über den ZTNA-Pfad geleitet wird.
- Es wurde überprüft, ob die Definitionen der privaten Apps den vom VPN routbaren Ressourcen mit den richtigen IP-/Port-/FQDN-Konfigurationen übereinstimmen.
- Es wurde bestätigt, dass die ZTNA-Richtlinien mit den Zuweisungen des Testbenutzers und der Testgruppe übereinstimmen.

Das Problem isoliert sich speziell auf den Secure Client ZTNA-Verkehrssteuerungs- oder Durchsetzungsmechanismus, da die browserbasierte ZTNA überprüft, ob Backend-Publishing und -Durchsetzung ordnungsgemäß funktionieren.

Umwelt

- Technologie: Sicherer Zugriff - ZTNA (Zero Trust Network Access)

- Komponenten: Client-basiertes ZTNA, Status, Registrierung, Zugriff auf private Ressourcen
- Sicherer Client mit gleichzeitig vorhandenen VPN-Profilen
- Zugriff auf private Anwendungen über FQDN und direkte IP-Adressierung
- Browserbasierte ZTNA-Funktion funktionierte bestätigt
- Die Richtliniendurchsetzung wird im Modus für die Durchsetzung der meisten Übereinstimmungen konfiguriert.

Auflösung

Die Lösung beinhaltete Konfigurationsanpassungen des ZTA-Profils und die Validierung von Richtlinien. Die in den folgenden Abschnitten beschriebenen Schritte wurden durchgeführt, um die clientbasierte ZTNA-Funktionalität wiederherzustellen.

Schritt 1: Hinzufügen privater Ressourcen zum ZTA-Profil

Private Ressourcen wurden der ZTA-Profilkonfiguration hinzugefügt. Nach dieser Änderung wurden blockierte Ereignisse in den Aktivitätsprotokollen und Screenshots angezeigt, was darauf hinweist, dass der Client-Datenverkehr nun ordnungsgemäß über den ZTNA-Pfad geleitet wurde.

Phase 2: Überprüfung und Tests von Richtlinien

Es wurde eine temporäre Regel für die "beliebige Erlaubnis" hinzugefügt, um den Datenverkehrsfluss zu validieren. Während diese Regel aktiv war, funktionierte der clientbasierte ZTNA-Zugriff ordnungsgemäß. Dies bestätigte, dass der Verkehrssteuerungsmechanismus funktionierte, die Richtliniendurchsetzung jedoch angepasst werden musste.

Schritt 3: Richtlinienanpassung

Die temporäre "permit-any"-Regel wurde entfernt und die spezifischen Zugriffsrichtlinien validiert. Der Zugriff auf die private Ressource wurde über die Zugriffsrichtlinie Private Resources_Cyril im

Modus Most Specific Match Enforcement der Plattform bestätigt.

Schritt 4: Validierung der Konfiguration

Der Benutzer bestätigte, dass der Client-basierte ZTNA-Zugriff nach den Konfigurationsänderungen weiterhin verfügbar war. Das Problem konnte behoben werden, ohne dass weitere Richtlinienänderungen oder Systemänderungen erforderlich waren.

Ursache

Die Ursache dafür war die unvollständige Konfiguration der privaten Ressource im ZTA-Profil. Ohne die entsprechenden, im ZTA-Profil definierten privaten Ressourcen wurde der Client-Datenverkehr nicht über den ZTNA-Erzwingungspfad geleitet, sodass er auf lokale Routing-Mechanismen zurückfiel. Dadurch wird der Datenverkehr die ZTNA-Richtlinien vollständig umgehen. Dies erklärt, warum beim Trennen der VPN-Verbindung keine ZTNA-Ereignisse in den Aktivitätsprotokollen auftraten.

Das Problem war spezifisch für die Client-basierte ZTNA-Verkehrssteuerung, während die browserbasierte ZTNA-Verkehrssteuerung weiterhin funktioniert, da sie einen anderen, ordnungsgemäß konfigurierten Verkehrssteuerungsmechanismus verwendet.

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.