Sicherer Zugriff ZTNA-Konfiguration Synchronisierungsfehler mit SSL-Verschlüsselung und Netzwerktunneln

Inhalt

Problem

Cisco Secure Client Zero Trust Access (ZTA) wurde erfolgreich registriert, schlägt jedoch bei der Konfigurationssynchronisierung mit HTTP 502-Antworten und dem Verbindungsstatus "BadResponse" des Servers fehl. Die DART-Protokolle des Windows 11-Endpunkts zeigen eine erfolgreiche Registrierung, aber wiederholte Fehler bei der Konfigurations-Synchronisierung. Das Problem tritt nur auf, wenn der Endpunkt über einen Secure Access/Umbrella-Proxy mit Meraki AutoVPN-Tunneln mit dem Firmennetzwerkpfad verbunden ist, während derselbe Endpunkt die Konfigurationssynchronisierung in einem Heimnetzwerk ohne Proxy oder Tunnelinfrastruktur erfolgreich abschließt.

Umwelt

- Cisco Secure Client ZTA Version 5.1.16.4434
- Windows 11 Enterprise-Endgerät
- Meraki MX-Appliances mit AutoVPN-Integration
- Secure Access (SSE) mit Network Tunnels Gateway (NTG)
- Umbrella DNS und Secure Access Web Security
- SSL-Entschlüsselung und HTTPS-Prüfung im Firmennetzwerkpfad aktiviert
- Vom System bereitgestellte Do Not Decrypt List (DND) nicht anfänglich konfiguriert

Auflösung

Der Fehler bei der Konfigurations-Synchronisierung wurde behoben, indem bei Verwendung von Netzwerktunneln mit sicherem Zugriff korrekte SSL-Verschlüsselungs-Umgehungen für ZTA-bezogene Domänen implementiert wurden.

Schritt 1: Auswirkungen der SSL-Entschlüsselung ermitteln

Überprüfen Sie die Aktivitätssuchprotokolle in Secure Access auf Entschlüsselungsereignisse in Bezug auf ZTA-Domänen, um sicherzustellen, dass die SSL-Entschlüsselung zu Fehlern bei der Konfigurationssynchronisierung führt.

Phase 2: Vom System bereitgestellte DND-Liste konfigurieren

Bei Verwendung von Network Tunnels Gateway (NTG) mit sicherem Zugriff muss das vom System bereitgestellte DND aktiviert werden, um ZTA-bezogenen Datenverkehr von der SSL-Überprüfung richtig zu umgehen.

Navigieren Sie zu Secure Access Dashboard > Secure > Do Not Decrypt Lists, und ändern Sie die vom System bereitgestellte Do Not Decrypt-Liste.

Schritt 3: Sicherheitsprofil für ZTA-Domänen erstellen

Fügen Sie die erforderlichen ZTA-bezogenen Domänen mithilfe der vom System bereitgestellten DND-Liste einem neuen Sicherheitsprofil hinzu:

- zpc.sse.cisco.com
- * .zpc.sse.cisco.com
- ztna.sse.cisco.com
- acme.sse.cisco.com

- devices.api.umbrella.com

Schritt 4: Sicherheitsprofil auf Testregel anwenden

Weisen Sie das neu erstellte Sicherheitsprofil mit den ZTA-Domänenumgehungen einer Testregel zu, um die Konfiguration zu validieren.

Schritt 5: Validierung der Konfigurations-Synchronisierung

ZTA-Anmeldung und -Konfiguration über das Unternehmensnetzwerk testen Die Synchronisierung kann jetzt erfolgreich ohne HTTP 502-Fehler abgeschlossen werden.

Schritt 6: Zusammenarbeit mit dem Meraki-Team

Für eine umfassende Abdeckung sollten Sie sich mit dem Meraki-Support abstimmen, um offizielle ZTA-bezogene URLs und Domänen zu validieren, die bei der Prüfung des sicheren Zugriffs umgangen werden können. Verweisen Sie auf diese Meraki-Dokumentation:

- Upstream-Firewall-Regeln für Cloud-Verbindungen
- Meraki Dashboard URL-Aktualisierung - PCI-Konformität

Ursache

Der Fehler bei der Konfigurationssynchronisierung wurde durch die SSL-Verschlüsselung und die Proxyfunktion für den Verkehr mit nicht vertrauenswürdigem Zugriff im Unternehmensnetzwerk verursacht. Wenn Network Tunnels Gateway (NTG) mit sicherem Zugriff verwendet wird, müssen ZTA-bezogene Domänen mithilfe der vom System bereitgestellten DND (Do Not Decrypt List) umgangen werden. Ohne diese Umgehungskonfiguration ändert die SSL-Prüfung Zertifikatsketten und beeinträchtigt die Kommunikation auf ZTA-Kontrollebene, sodass der Client HTTP 502-Antworten während der Konfigurations-Synchronisierungsversuche empfängt.

Verwandte Inhalte

- Fehlerbehebung bei Problemen mit sicherer Zugriffsentschlüsselung und SSL
- Sicherer Zugriff Zero Trust Client-basierte Registrierungsservices
- ZTA-Domänenanforderungen für sicheren Zugriff
- Fehlerbehebung bei Problemen mit der Anmeldung für sicheren Zugriff
- Fehler beim Synchronisieren der Konfiguration des sicheren Clients
- Sammeln detaillierter ZTNA-Protokolle zur Fehlerbehebung
- 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.