# Secure Access ZTNA Configuration Sync-fout met SSL-decodering en netwerktunnels

## Inhoud

## uitgifte

Cisco Secure Client Zero Trust Access (ZTA) schrijft zich met succes in, maar faalt tijdens de configuratiesynchronisatie met HTTP 502-reacties en de status van de "BadResponse"-serverconnectiviteit. De DART-logs van het Windows 11-eindpunt tonen succesvolle inschrijving, maar herhaalde configuratie-synchronisatiefouten. Het probleem treedt alleen op wanneer het eindpunt is verbonden met het bedrijfsnetwerkpad met behulp van Secure Access/Umbrella-proxy met Meraki AutoVPN-tunnels, terwijl hetzelfde eindpunt met succes de configuratiesynchronisatie op een thuisnetwerk zonder proxy- of tunnelinfrastructuur voltooit.

## milieu

- Cisco Secure Client ZTA versie 5.1.16.4434
- Windows 11 Enterprise-eindpunt
- Meraki MX toestellen met AutoVPN integratie
- Secure Access (SSE) met Network Tunnels Gateway (NTG)
- Overkoepelende DNS en Secure Access Web Security
- SSL-decryptie en HTTPS-inspectie ingeschakeld op bedrijfsnetwerkpad
- Systeem geleverd Niet-ontsleutelen lijst (DND) niet initieel geconfigureerd

## resolutie

De configuratie synchronisatie fout werd opgelost door het implementeren van de juiste SSL decryptie bypasses voor ZTA-gerelateerde domeinen bij het gebruik van Network Tunnels met Secure Access.

## Stap 1: Identificeer de impact van SSL-decodering

Controleer of SSL-decodering de configuratie sync-fouten veroorzaakt door activiteitslogboeken in Secure Access te bekijken voor decoderingsevenementen met betrekking tot ZTA-domeinen.

## Stap 2: Systeemgeleverde DND-lijst configureren

Wanneer u Network Tunnels Gateway (NTG) met Secure Access gebruikt, moet het DND-systeem worden ingeschakeld om ZTA-gerelateerd verkeer van SSL-inspectie te omzeilen.

Navigeer naar Dashboard voor beveiligde toegang > Beveiligd > Lijsten niet decoderen en wijzig de opgegeven systeemlijst Niet decoderen.

## Stap 3: Maak een beveiligingsprofiel voor ZTA-domeinen

Voeg de vereiste ZTA-gerelateerde domeinen toe aan een nieuw beveiligingsprofiel met behulp van de DND-lijst met systeemgegevens:

- zpc.sse.cisco.com
- *.zpc.sse.cisco.com
- ztna.sse.cisco.com
- acme.sse.cisco.com
- devices.api.umbrella.com

## Stap 4: Pas het beveiligingsprofiel toe op de testregel

Wijs het nieuw gemaakte beveiligingsprofiel met de ZTA-domeinbypasses toe aan een testregel om de configuratie te valideren.

### Stap 5: Configuratiesynchronisatie valideren

Test ZTA-inschrijving en synchronisatie van de configuratie van het bedrijfsnetwerk. De synchronisatie kan nu met succes worden voltooid zonder HTTP 502-fouten.

### Stap 6: Coördineren met Meraki Team

Voor uitgebreide dekking, coördineer met Meraki-ondersteuning om officiële ZTA-gerelateerde URL's en domeinen te valideren die kunnen worden overgeslagen van Secure Access-inspectie. Verwijs naar deze Meraki documentatie:

- Upstream Firewall-regels voor cloudconnectiviteit
- Meraki Dashboard URL Update - PCI-conformiteit

## Oorzaak

De configuratie-synchronisatiefout werd veroorzaakt door SSL-decodering en proxy van Zero Trust Access-verkeer op het bedrijfsnetwerk. Wanneer Network Tunnels Gateway (NTG) wordt gebruikt met Secure Access, moeten ZTA-gerelateerde domeinen worden omzeild met behulp van de System provided Do Not Decrypt List (DND). Zonder deze bypass-configuratie wijzigt SSL-inspectie certificaatketens en interfereert het met de communicatie van het ZTA-controlevlak, waardoor de client HTTP 502-reacties ontvangt tijdens configuratiesynchronisatiepogingen.

## Gerelateerde inhoud

- Problemen met Secure Access Decryption en SSL oplossen
- Secure Access Zero Trust Client-gebaseerde inschrijvingsservices

- ZTA-domeinvereisten voor beveiligde toegang
- Problemen met inschrijvingsfouten voor beveiligde toegang oplossen
- Problemen met synchronisatie van beveiligde clientconfiguratie oplossen
- Gedetailleerde ZTNA-logboeken verzamelen voor probleemoplossing
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.