Erreur de synchronisation de la configuration ZTNA d'accès sécurisé avec décodage SSL et tunnels réseau

Table des matières

Problème

Cisco Secure Client Zero Trust Access (ZTA) s'inscrit avec succès, mais échoue lors de la synchronisation de la configuration avec les réponses HTTP 502 et l'état de connectivité du serveur « BadResponse ». Les journaux DART du point de terminaison Windows 11 indiquent une inscription réussie, mais des échecs répétés de synchronisation de la configuration. Le problème se produit uniquement lorsque le point d'extrémité est connecté au chemin du réseau d'entreprise à l'aide d'un proxy d'accès sécurisé/Umbrella avec des tunnels Meraki AutoVPN, alors que le même point d'extrémité effectue avec succès la synchronisation de configuration sur un réseau domestique sans infrastructure de proxy ou de tunnel.

Environnement

- Cisco Secure Client ZTA version 5.1.16.4434
- Terminal Windows 11 Entreprise
- Appareils Meraki MX avec intégration AutoVPN
- Accès sécurisé (SSE) avec passerelle de tunnels réseau (NTG)
- Sécurité Web pour le DNS et l'accès sécurisé
- Déchiffrement SSL et inspection HTTPS activés sur le chemin du réseau d'entreprise
- La liste DND (Do Not Decrypt List) fournie par le système n'a pas été configurée initialement

Résolution

L'échec de synchronisation de configuration a été résolu en implémentant des contournements de déchiffrement SSL appropriés pour les domaines liés à ZTA lors de l'utilisation de tunnels réseau avec accès sécurisé.

Étape 1: Identifier l'impact du déchiffrement SSL

Vérifiez que le déchiffrement SSL cause les échecs de synchronisation de configuration en consultant les journaux de recherche d'activité dans Secure Access pour les événements de déchiffrement liés aux domaines ZTA.

Étape 2: Configurer la liste NPD fournie par le système

Lors de l'utilisation de la passerelle de tunnels réseau (NTG) avec accès sécurisé, le service NPD fourni par le système doit être activé pour contourner correctement le trafic lié à ZTA de l'inspection SSL.

Accédez à Secure Access Dashboard > Secure > Do Not Decrypt Lists et modifiez la liste fournie par le système Do Not Decrypt List.

Étape 3: Créer un profil de sécurité pour les domaines ZTA

Ajoutez les domaines ZTA requis à un nouveau profil de sécurité à l'aide de la liste NPD fournie par le système :

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

- devices.api.umbrella.com

Étape 4: Appliquer le profil de sécurité à la règle de test

Attribuez le profil de sécurité nouvellement créé contenant les contournements de domaine ZTA à une règle de test pour valider la configuration.

Étape 5: Valider la synchronisation de configuration

Testez l'inscription ZTA et la synchronisation de la configuration à partir du réseau d'entreprise. La synchronisation peut maintenant s'effectuer sans erreurs HTTP 502.

Étape 6: Coordination avec l'équipe Meraki

Pour une couverture complète, coordonnez-vous avec l'assistance Meraki afin de valider les URL et domaines ZTA officiels qui peuvent être contournés lors de l'inspection Secure Access. Référez-vous à la documentation Meraki :

- Règles de pare-feu en amont pour la connectivité cloud
- Mise à jour des URL du tableau de bord Meraki - Conformité PCI

Motif

L'échec de la synchronisation de la configuration a été causé par le déchiffrement SSL et le proxy du trafic Zero Trust Access sur le réseau d'entreprise. Lorsque la passerelle des tunnels réseau (NTG) est utilisée avec l'accès sécurisé, les domaines associés à ZTA doivent être contournés à l'aide de la liste DND (Do Not Decrypt List) fournie par le système. Sans cette configuration de contournement, l'inspection SSL modifie les chaînes de certificats et interfère avec la communication du plan de contrôle ZTA, amenant le client à recevoir des réponses HTTP 502 pendant les tentatives de synchronisation de la configuration.

Autres informations utiles

- Dépannage du décodage d'accès sécurisé et des problèmes SSL
- Services d'inscription sécurisés basés sur le client Zero Trust
- Configuration requise du domaine ZTA pour un accès sécurisé
- Dépannage des erreurs d'inscription Secure Access
- Dépannage des erreurs de synchronisation de la configuration du client sécurisé
- Collecter des journaux ZTNA détaillés pour le dépannage
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.