Accès sécurisé Déconnexion intermittente derrière les pare-feu d'entreprise avec erreurs IdleTimeout

Table des matières

- Problème
- Environnement
- Résolution
  - Étape 1: Implémenter la configuration du tampon TTL MX
  - Étape 2: Configurer les exclusions de domaine requises
  - Étape 3: Vérification des autorisations de port et de protocole
  - Étape 4: Surveillance et validation de la résolution
- Motif
- Autres informations utiles

Problème

Les clients Cisco Secure Access subissent des déconnexions intermittentes et des reconnexions immédiates lorsque les terminaux sont connectés au réseau de l'entreprise. Les déconnexions se produisent de manière aléatoire, le client se reconnectant automatiquement après environ 5 secondes. Ce comportement est observé lorsque le trafic Internet est transféré par proxy via Zero Trust Access (ZTA) vers Secure Access à partir de terminaux situés derrière les périphériques Cisco FirePower et Meraki MX.

Le journal des événements Windows capture les erreurs spécifiques « idleTimeout » au cours de ces événements de déconnexion. Le modèle de déconnexion ne se produit pas lorsque les

utilisateurs se connectent à partir de connexions Internet domestiques, ce qui indique que le problème est spécifiquement lié à l'infrastructure réseau de l'entreprise.

Le symptôme crée une interruption de l'activité pour sécuriser la connectivité d'accès à distance pour les utilisateurs qui opèrent dans l'environnement réseau de l'entreprise, alors que les utilisateurs distants ne sont pas affectés par ce problème de connectivité.

Environnement

- Cisco Secure Access - Déploiement Advantage
- Logiciel client Cisco Secure Internet Access (SIA)
- Infrastructure réseau d'entreprise avec les appliances de sécurité Cisco FirePower
- Appareils de sécurité Meraki MX sur le chemin du réseau
- Configuration ZTA (Zero Trust Access) proxy du trafic Internet vers un accès sécurisé
- Terminaux Windows avec fonctionnalité de journalisation des événements
- Scénarios de connectivité mixte : réseau d'entreprise (affecté) et connexions internet domestiques (non affecté)

Résolution

La résolution impliquait la mise en oeuvre de modifications de configuration sur l'appareil Meraki MX et la garantie d'exclusions de domaine et d'allocations de port appropriées pour l'intégration d'accès sécurisé.

Étape 1: Implémenter la configuration du tampon TTL MX

Configurez une mémoire tampon MX TTL sur le périphérique Meraki MX pour résoudre le comportement de mise en cache DNS TTL qui a contribué aux problèmes de déconnexion intermittente. Cette modification de configuration résout les conflits de synchronisation entre la mise en cache de la résolution DNS et les attentes de connectivité du client Secure Access.

Étape 2: Configurer les exclusions de domaine requises

Assurez-vous que ces domaines sont correctement exclus de l'interception et ajoutés aux listes non décryptées sur les périphériques Cisco FirePower et Meraki MX :

- ztna.sse.cisco.com
- zpc.sse.cisco.com
- Domaines de service d'accès sécurisé supplémentaires tels qu'identifiés dans la configuration de la stratégie

Étape 3: Vérification des autorisations de port et de protocole

Configurez l'infrastructure de pare-feu de l'entreprise pour autoriser les ports et protocoles d'accès sécurisé requis via les périphériques FirePower et Meraki MX. Assurez-vous que le trafic vers le port 443 pour les points d'extrémité du service d'accès sécurisé est correctement géré sans interférence d'une inspection de sécurité qui pourrait entraîner des conditions de délai d'attente.

Étape 4: Surveillance et validation de la résolution

Après avoir implémenté la configuration de la mémoire tampon MX TTL, surveillez le comportement du client Secure Access pendant plusieurs jours pour confirmer que le modèle de déconnexion et de reconnexion intermittent a cessé.

Motif

Les déconnexions intermittentes ont été provoquées par des conflits de comportement de mise en cache DNS TTL (Time To Live) entre l'infrastructure réseau de l'entreprise et les attentes du service d'accès sécurisé. L'analyse technique de Cisco a révélé que les valeurs de durée de vie DNS varient en raison du comportement de mise en cache du résolveur, et que les adresses IP alternatives sont un comportement attendu en raison des mécanismes d'équilibrage de charge dans l'architecture de service d'accès sécurisé.

Lorsque des périphériques réseau d'entreprise (Cisco FirePower et Meraki MX) ont traité des réponses DNS pour des terminaux d'accès sécurisé, la mise en cache et la gestion des durées de vie ont créé des décalages temporels qui ont entraîné des conditions de « délai d'inactivité ». Ce conflit de synchronisation a amené le client Secure Access à interpréter la connexion comme étant inactive et à lancer des cycles de déconnexion/reconnexion.

Le problème était spécifique aux environnements réseau d'entreprise, car les connexions Internet domestiques n'implémentent généralement pas le même niveau de mise en cache DNS et d'inspection du trafic qui peut interférer avec la gestion de l'état de la connexion du client Secure Access.

Autres informations utiles

- 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.