Dépannage des problèmes de connexion proxy SWG d'accès sécurisé pour le fichier PAC

Table des matières

Problème

Les utilisateurs ont rencontré des problèmes de connexion lorsqu'ils ont tenté d'accéder à des sites Web via Cisco Secure Access à l'aide de l'URL proxy SWG (Secure Web Gateway) swg-url-proxy-https-8xxxx.sseproxy.qq.opendns.com.

Les symptômes spécifiques comprenaient :

- Les requêtes Web (telles que vers https://www.google.com) ont échoué avec des erreurs de connexion dans les navigateurs
- Le trafic n'apparaissait pas dans les journaux de recherche d'activité
- Des réinitialisations de serveur ont été observées à partir de l'IP source du client/IP de sortie du client vers les terminaux de destination :
    - k8s-sigpro-sigpro-c10eb6eb-38fbeb0455191ac5.elb.eu-central-1.amazonaws.com
    - k8s-sigpro-sigpro-f8f3d861-14341dd91e659675.elb.eu-central-1.amazonaws.com
- Les problèmes ont commencé vers 09h30 CEST
- La résolution DNS du nom d'hôte SWG fonctionnait correctement
- Les connexions Telnet vers swg-url-proxy-https-8xxxx.sseproxy.qq.opendns.com sur le port 443 ont réussi
- Le pare-feu externe ne bloquait pas les connexions aux adresses IP de destination

L'analyse de capture de paquets a révélé des paquets TCP RST provenant du proxy, indiquant la fin de la connexion au niveau du proxy.

Environnement

- Technologie : Accès sécurisé Cisco (SSE)
- Composant : Passerelle Web sécurisée (SWG)
- URL du proxy SWG : swg-url-proxy-https-8385532.sseproxy.qq.opendns.com
- Ports affectés : 443 et 80
- Adresse IP NAT d'origine : 20.x.x.x
- IP NAT mise à jour : 21.x.x.x
- Points de terminaison AWS ELB dans par exemple : région centre-ue ou est-états-unis
- Configuration WPAD dirigeant les navigateurs vers le proxy SWG

Résolution

Le problème a été résolu en mettant à jour la configuration de la liste de contrôle d'accès pour inclure l'adresse IP NAT correcte.

Les étapes décrites dans les sections suivantes ont été suivies pour identifier et résoudre le problème.

Étape 1: Collecte des données de diagnostic

Captures de paquets collectées et configuration de script WPAD pour analyser le flux de trafic et la configuration du proxy.

En plus de cela, l'indice principal était https://policy.test.sse.cisco.com affichait une erreur « 401 non autorisé ». Ce qui signifie que la requête de connexion http parvient au proxy, mais que le proxy ne peut pas authentifier le trafic utilisateur sur la base de son OrgID et d'autres détails de métadonnées pour appliquer la stratégie et autoriser le trafic.

Étape 2: Analyse du trafic

L’analyse de la capture de paquets a révélé :

- Les paquets TCP RST étaient envoyés à partir du proxy
- Les journaux de recherche d'activité n'affichaient pas le trafic défaillant
- L’adresse IP source dans le flux de trafic a changé

Étape 3: Identification de l'adresse IP NAT

L'enquête a révélé que l'adresse IP publique NAT est passée de 20.x.x.x à 21.x.x.x. L'adresse IP modifiée a été ajoutée en tant que réseau enregistré dans l'interface utilisateur CSA. Le trafic SWG a commencé à fonctionner pour le déploiement de fichiers PAC après l'enregistrement de l'adresse IP correcte dans le portail CSA.

Étape 4: Mise à jour de la configuration Allow-List

Mise à jour des règles de liste d'autorisation/pare-feu pour autoriser le trafic de la nouvelle adresse IP NAT 21.x.x.x.

Étape 5: Vérification

Après la mise à jour de la liste d'autorisation avec la nouvelle adresse IP NAT, le flux de trafic normal d'accès sécurisé a été restauré et les requêtes Web ont commencé à fonctionner correctement via le proxy SWG.

Motif

La cause principale était un changement dans l'adresse IP publique NAT de l'utilisateur de

20.x.x.x à 21.x.x.x. Le proxy SWG d'accès sécurisé a été configuré pour autoriser uniquement le trafic en provenance de l'adresse IP d'origine, ce qui entraîne des réinitialisations de connexion lorsque le trafic arrive de la nouvelle adresse IP. En plus de cela, l'indice principal était https://policy.test.sse.cisco.com affichait une erreur « 401 invalid », qui se réfère à la requête de connexion http qui atteint le proxy, ceci est confirmé par PCAP aussi, mais le proxy ne peut pas authentifier le trafic utilisateur sur la base de son OrgID et d'autres détails de métadonnées pour appliquer la politique et autoriser le trafic. Cela a entraîné l'interruption des connexions du proxy avec les paquets TCP RST, empêchant le traitement des requêtes Web réussies.

Ajout de la nouvelle adresse IP NATed dans l'interface utilisateur CSA sous le réseau enregistré pour résoudre le problème de flux de trafic Web pour le fichier SWG PAC.

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.