Problème de vérification du fonctionnement du proxy en amont WSA après une interruption du réseau

Table des matières

Problème

Après une interruption prolongée du réseau, un appareil de sécurité Web Cisco (WSA) configuré pour utiliser un proxy en amont spécifié par le nom de domaine complet (FQDN) peut échouer lors de la reprise du transfert du trafic vers un proxy en amont et envoyer le trafic directement à la place. Ce problème se manifeste lorsque le WSA marque le proxy en amont comme « mort » pendant la panne du réseau, mais ne parvient pas à reconnaître quand le proxy en amont redevient disponible, même après la restauration de la connectivité du réseau.

Les symptômes spécifiques observés sont les suivants :

- WSA configuré avec le proxy en amont via FQDN et « Failure Handling = go Direct »
- Interruption à long terme du réseau affectant la connectivité au proxy en amont et au serveur DNS
- Après la restauration du réseau, les journaux d'accès n'affichent aucune balise DEFAULT_PARENT, indiquant que le trafic continue à contourner le proxy en amont
- Le problème se produit sur un appareil WSA alors qu'un autre dans le même environnement fonctionne normalement

Environnement

- Appliance de sécurité Web Cisco (WSA) série S
- AsyncOS 14.5.2-011 (version concernée)
- Matériel : S695

- Proxy en amont configuré avec spécification FQDN
- Gestion des échecs configurée en tant que « go direct »
- Environnement réseau avec infrastructure de commutation L2

Résolution

Ce problème est résolu en mettant à niveau AsyncOS vers une version qui contient le correctif pour CSCwi13124. Ce bogue a été corrigé dans les versions AsyncOS suivantes :

- AsyncOS 15.5.0-566
- AsyncOS 15.5.0-710

Solution temporaire pour les versions actuelles

Pour les environnements qui ne peuvent pas être mis à niveau immédiatement, une atténuation temporaire est disponible en ajustant le délai d'inactivité maximal pour vérifier les proxies en amont qui ne répondent pas :

Étape 1: Accédez à l'interface de ligne de commande et accédez à la configuration avancée du proxy :

```
cli -> advancedproxyconfig -> MISCELLANEOUS
```

Étape 2: Modifiez le paramètre Délai d'inactivité maximal :

```
"Enter maximum idle timeout for checking unresponsive upstream proxy (in seconds)"
```

Étape 3: Réduisez la valeur maximale par défaut (86400 secondes/24 heures) à une valeur plus petite pour réduire le temps entre les vérifications d'intégrité.

Méthode De Récupération Immédiate

Si le problème affecte actuellement le flux de trafic, la commande suivante peut immédiatement restaurer la fonctionnalité de proxy en amont :

Étape 1: Accédez au menu de diagnostic :

```
CLI > diagnostic > PROXY > kick
```

Le processus proxy est alors redémarré et les opérations proxy en amont normales sont restaurées.

Procédure de validation et de test

Pour vérifier si le problème est présent ou a été résolu après une mise à niveau, passez en revue les étapes suivantes :

Étape 1: Établir une surveillance de base

Surveillez les journaux d'accès et les journaux de proxy pour confirmer que WSA envoie du trafic au proxy en amont. Vérifiez que le trafic atteint le côté proxy en amont.

Étape 2: Simuler une interruption du réseau

Après avoir confirmé le flux de trafic normal vers le proxy en amont, déconnectez ces connexions :

- Connexion WSA au proxy en amont
- Connexion WSA au serveur DNS

Étape 3: Surveillance de la détection des défaillances

Vérifiez les journaux du proxy et du système pour les indicateurs suivants :

- Le journal du proxy peut afficher le proxy en amont comme « ... déclaré mort »
- Le journal système peut afficher « Critique : Nombre maximal d'échecs d'interrogation du serveur DNS atteint..."

Étape 4: Conserver l'état Perturbé

Sans redémarrer le processus proxy, conservez l'état déconnecté à partir de l'étape 2 et continuez à générer des demandes pendant environ 10 heures.

Étape 5: Restaurer la connectivité

Au bout d'environ 10 heures, restaurez les connexions qui ont été déconnectées à l'étape 2.

Étape 6: Surveiller le comportement de récupération

Une fois l'étape 5 terminée, surveillez les journaux d'accès et les journaux proxy sans redémarrer le processus proxy :

- Dans un système fixe : Le trafic reprend en passant par le proxy en amont et les journaux du proxy affichent des transitions d'état normales
- Dans un système affecté : Les journaux d'accès indiquent que le trafic continue à contourner le proxy en amont, et les journaux du proxy n'affichent pas les messages « ... était malade, maintenant sain » ou « ... était sain, maintenant malade »

Motif

La cause première de ce problème est une faille logique dans le mécanisme de contrôle d'intégrité du proxy en amont. Lorsque WSA détermine qu'un proxy en amont configuré est « mort » (ne répond pas), il implémente un algorithme de réémission temporisée exponentielle qui double l'intervalle de contrôle d'intégrité après chaque échec. Cet intervalle peut atteindre un maximum de 24 heures (86400 secondes).

Ce problème se produit lorsque le proxy en amont redevient disponible au cours de l'un de ces intervalles étendus. Même si le proxy a récupéré et répond normalement, WSA n'effectuera pas de contrôle d'intégrité tant que l'intervalle de temps configuré ne sera pas écoulé. Cela peut entraîner jusqu'à 24 heures de routage direct continu du trafic au lieu de reprendre l'utilisation du proxy en amont.

Ce comportement affecte les configurations WSA où :

- Le proxy en amont est spécifié par le nom d'hôte DNS/FQDN (et non par l'adresse IP)
- La gestion des échecs est définie sur « Go Direct »
- Les interruptions réseau étendues affectent la connectivité du serveur proxy en amont et du serveur DNS

ID de bogue Cisco : CSCwi13124

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.