Probleme mit der SWG-Proxyverbindung für sicheren Zugriff für PAC-Datei beheben

Inhalt

Problem

Bei dem Versuch, über Cisco Secure Access mit der SWG-Proxy-URL swg-url-proxy-https-8xxxx.sseproxy.qq.opendns.com auf Websites zuzugreifen, traten Verbindungsfehler auf.

Zu den spezifischen Symptomen gehören:

- Bei Webanfragen (z. B. an https://www.google.com) sind Verbindungsfehler in Browsern aufgetreten.
- Datenverkehr wurde nicht in Aktivitätssuchprotokollen angezeigt
- Zurücksetzen des Servers von der Client-Quell-IP/Client-Ausgangs-IP in Richtung der Ziel-Endpunkte:
    - k8s-sigpro-sigpro-c10eb6eb-38fbeb0455191ac5.elb.eu-central-1.amazonaws.com
    - k8s-sigpro-sigpro-f8f3d861-14341dd91e659675.elb.eu-central-1.amazonaws.com
- Beginn der Ausgaben gegen 09:30 Uhr MESZ
- Die DNS-Auflösung für den SWG-Hostnamen funktionierte ordnungsgemäß.
- Telnet-Verbindungen zu swg-url-proxy-https-8xxxx.sseproxy.qq.opendns.com auf Port 443 waren erfolgreich
- Die äußere Firewall blockierte keine Verbindungen zu den Ziel-IPs.

Die Paketerfassungsanalyse ergab TCP-RST-Pakete, die vom Proxy übermittelt wurden. Dies zeigt die Beendigung der Verbindung auf Proxy-Ebene an.

Umwelt

- Technologie: Cisco Secure Access (SSE)
- Komponente: Sicheres Web-Gateway (SWG)
- SWG-Proxy-URL: swg-url-proxy-https-8385532.sseproxy.qq.opendns.com
- Betroffene Ports: 443 und 80
- Ursprüngliche NAT-IP: 20 x x x x
- Aktualisierte NAT-IP: 21.x.x.x
- AWS ELB-Endpunkte in z. B.: EU-Zentral- oder Ost-Region
- WPAD-Konfiguration Weiterleiten von Browsern an den SWG-Proxy

Auflösung

Das Problem wurde durch die Aktualisierung der Zulassungslistenkonfiguration auf die richtige NAT-IP-Adresse behoben.

Die in den nächsten Abschnitten beschriebenen Schritte wurden durchgeführt, um das Problem zu identifizieren und zu beheben.

Schritt 1: Diagnosedatenerfassung

Erfassung von Paketerfassungen und WPAD-Skriptkonfiguration zur Analyse des Datenverkehrsflusses und der Proxykonfiguration.

Darüber hinaus war der Haupthinweis https://policy.test.sse.cisco.com zeigte "401 unauthorized" Fehler. Das bedeutet, dass die HTTP-Verbindungsanforderung auf den Proxy trifft, der Proxy jedoch den Benutzerdatenverkehr nicht anhand seiner OrgID und anderer Metadatendetails authentifizieren kann, um die Richtlinie anzuwenden und den Datenverkehr zuzulassen.

Phase 2: Datenverkehrsanalyse

Die Analyse der Paketerfassung ergab Folgendes:

- TCP-RST-Pakete wurden vom Proxy gesendet
- Fehlerhafter Datenverkehr wurde nicht in den Aktivitätssuchprotokollen angezeigt
- Die Quell-IP im Datenverkehrsfluss hatte sich geändert.

Schritt 3: NAT-IP-Adressidentifizierung

Die Untersuchung ergab, dass sich die öffentliche NAT-IP-Adresse von 20.x.x.x in 21.x.x.x geändert hatte. Die geänderte IP wurde als registriertes Netzwerk in der CSA-Benutzeroberfläche hinzugefügt. Der SWG-Datenverkehr begann für die PAC-Dateibereitstellung zu funktionieren, nachdem die richtige IP im CSA-Portal registriert wurde.

Schritt 4: Zulassungslisten-Konfigurationsupdate

Zulassen von Datenverkehr von der neuen NAT-IP-Adresse 21.x.x.x anhand der Zulassungsliste/Firewall-Regeln aktualisiert

Schritt 5: Verifizierung

Nach der Aktualisierung der Zulassungsliste mit der neuen NAT-IP-Adresse wurde der normale Secure Access-Datenverkehrsfluss wiederhergestellt, und Webanfragen funktionierten über den SWG-Proxy ordnungsgemäß.

Ursache

Die Ursache hierfür war eine Änderung der öffentlichen NAT-IP-Adresse des Benutzers von 20.x.x.x in 21.x.x.x. Der SWG-Proxy für sicheren Zugriff wurde so konfiguriert, dass nur der Datenverkehr von der ursprünglichen IP-Adresse zugelassen wird. Dadurch wird die Verbindung zurückgesetzt, wenn der Datenverkehr von der neuen IP-Adresse eingeht. Darüber hinaus war der Haupthinweis https://policy.test.sse.cisco.com zeigte "401 unauthorized" Fehler, die auf http-Verbindungsanforderung trifft auf Proxy, dies wird auch durch PCAP bestätigt, aber Proxy nicht in der Lage, Benutzerdatenverkehr auf der Grundlage ihrer OrgID und anderen Metadaten Details zu

authentifizieren, um Richtlinie anzuwenden und den Datenverkehr zuzulassen. Dies führte dazu, dass der Proxy Verbindungen mit TCP-RST-Paketen abschloss und so die Verarbeitung erfolgreicher Webanfragen verhinderte.

Neue NAT-IP in der CSA-Benutzeroberfläche des Benutzers unter dem registrierten Netzwerk hinzugefügt, um das Problem des Web-Datenverkehrsflusses für die SWG-PAC-Datei zu beheben.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.