Troubleshoot Secure Access SWG Proxy Connection Issues for PAC File

Contents

Issue

Users experienced connection failures when attempting to access websites through Cisco Secure Access using the SWG (Secure Web Gateway) proxy URL swg-url-proxy-https-8xxxx.sseproxy.qq.opendns.com.

The specific symptoms included:

- Web requests (such as to https://www.google.com) were failing with connection errors in browsers
- Traffic was not appearing in activity search logs
- Server resets were observed from the client source IP/Client Egress IP toward destination endpoints:
    - k8s-sigpro-sigpro-c10eb6eb-38fbeb0455191ac5.elb.eu-central-1.amazonaws.com
    - k8s-sigpro-sigpro-f8f3d861-14341dd91e659675.elb.eu-central-1.amazonaws.com
- Issues began at approximately 09:30 AM CEST
- DNS resolution for the SWG hostname was functioning correctly
- Telnet connections to swg-url-proxy-https-8xxxx.sseproxy.qq.opendns.com on port 443 were successful
- The outer firewall was not blocking connections to the destination IPs

Packet capture analysis revealed TCP RST packets coming from the proxy, indicating connection termination at the proxy level.

Environment

- Technology: Cisco Secure Access (SSE)
- Component: Secure Web Gateway (SWG)

- SWG Proxy URL: swg-url-proxy-https-8385532.sseproxy.qq.opendns.com
- Affected Ports: 443 and 80
- Original NAT IP: 20.x.x.x
- Updated NAT IP: 21.x.x.x
- AWS ELB endpoints in for ex: eu-central or us-east region
- WPAD configuration directing browsers to SWG proxy

Resolution

The issue was resolved by updating the allow-list configuration to include the correct NAT IP address.

The steps described in the next sections were taken to identify and resolve the problem.

Step 1: Diagnostic Data Collection

Collected packet captures and WPAD script configuration to analyze the traffic flow and proxy configuration.

In addition to that, main clue was https://policy.test.sse.cisco.com was showing "401 unauthorized" error. Which does meant http connect request is hitting to proxy, but proxy not able to authenticate user traffic based on their OrgID and other meta data details to apply policy and allow the traffic.

Step 2: Traffic Analysis

Analysis of the packet capture revealed:

- TCP RST packets were being sent from the proxy
- Activity search logs did not show the failing traffic
- The source IP in the traffic flow had changed

Step 3: NAT IP Address Identification

Investigation revealed that the NAT public IP address had changed from 20.x.x.x to 21.x.x.x. Changed IP was added as registered network in the user CSA UI, SWG traffic started to work for PAC file deployment after registering correct IP in the CSA portal.

Step 4: Allow-List Configuration Update

Updated the allow-list/firewall rules to permit traffic from the new NAT IP address 21.x.x.x.

Step 5: Verification

After updating the allow-list with the new NAT IP address, normal Secure Access traffic flow was restored and web requests began functioning correctly through the SWG proxy.

Cause

The root cause was a change in the user NAT public IP address from 20.x.x.x to 21.x.x.x. The Secure Access SWG proxy was configured to only allow traffic from the original IP address, causing connection resets when traffic arrived from the new IP address. In addition to that, main clue was https://policy.test.sse.cisco.com was showing "401 unauthorized" error, which refers to http connect request is hitting to proxy, this is confirmed by PCAP as well, but proxy not able to authenticate user traffic based on their OrgID and other meta data details to apply policy and allow the traffic. This resulted in the proxy terminating connections with TCP RST packets, preventing successful web requests from being processed.

Added the new NATed IP in user CSA UI under registered network to resolve web traffic flow issue for SWG PAC file.

Related Content

- Cisco Technical Support & Downloads