Problemen met SWG-proxyverbindingen voor PAC-bestand oplossen

Inhoud

uitgifte

Gebruikers hebben verbindingsfouten ondervonden bij pogingen om toegang te krijgen tot websites via Cisco Secure Access met behulp van de SWG (Secure Web Gateway) proxy-URL swg-url-proxy-https-8xxxx.sseproxy.qq.opendns.com.

De specifieke symptomen omvatten:

- Webverzoeken (zoals naar https://www.google.com) faalden met verbindingsfouten in browsers
- Verkeer werd niet weergegeven in activiteitenlogboeken
- Serverresets werden waargenomen vanaf de clientbron IP/Client Egress IP naar de eindpunten van de bestemming:
    - k8s-sigpro-sigpro-c10eb6eb-38fbeb0455191ac5.elb.eu-central-1.amazonaws.com
    - k8s-sigpro-sigpro-f8f3d861-14341dd91e659675.elb.eu-central-1.amazonaws.com
- De problemen begonnen rond 09:30 uur CEST
- De DNS-resolutie voor de SWG-hostnaam functioneerde correct
- Telnet-verbindingen met swg-url-proxy-https-8xxxx.sseproxy.qq.opendns.com op poort 443 waren succesvol
- De externe firewall blokkeerde geen verbindingen met de IP-adressen van de bestemming

Packet capture analyse onthulde TCP RST-pakketten afkomstig van de proxy, wat wijst op het beëindigen van de verbinding op proxyniveau.

milieu

- Cisco Secure Access (SSE)
- Onderdeel: Secure Web Gateway (SWG)
- SWG-proxy-URL: swg-url-proxy-https-8385532.sseproxy.qq.opendns.com
- Getroffen havens: 443 en 80
- Oorspronkelijke NAT IP: 20.x.x.x
- Bijgewerkt NAT IP: 21.x.x.x
- AWS ELB-eindpunten in voor bijv.: EU-centraal of VS-oostelijk gebied
- WPAD-configuratie die browsers naar SWG-proxy leidt

resolutie

Het probleem is opgelost door de allow-list configuratie bij te werken om het juiste NAT IP-adres op te nemen.

De stappen die in de volgende secties worden beschreven, zijn genomen om het probleem te identificeren en op te lossen.

Stap 1: Diagnostische gegevensverzameling

Collected packet captures en WPAD script configuratie om de verkeersstroom en proxy configuratie te analyseren.

Daarnaast was de belangrijkste aanwijzing dat https://policy.test.sse.cisco.com "401 ongeautoriseerde" fout vertoonde. Wat betekent dat http-verbindingsverzoek op proxy slaat, maar proxy niet in staat is om gebruikersverkeer te verifiëren op basis van hun OrgID en andere metagegevens om beleid toe te passen en het verkeer toe te staan.

Stap 2: Verkeersanalyse

Analyse van de packet capture onthulde:

- TCP RST-pakketten werden verzonden vanaf de proxy
- In de logboeken voor het zoeken naar activiteiten is het falende verkeer niet weergegeven
- De bron-IP in de verkeersstroom was veranderd

Stap 3: NAT IP-adresidentificatie

Uit onderzoek bleek dat het openbare IP-adres van de NAT was veranderd van 20.x.x.x naar 21.x.x.x. Gewijzigd IP werd toegevoegd als geregistreerd netwerk in de gebruiker CSA UI, SWG-verkeer begon te werken voor PAC-bestandsimplementatie na het registreren van de juiste IP in de CSA-portal.

Stap 4: Configuratie-update toestaan

Bijgewerkt met de allow-list/firewall regels om verkeer vanaf het nieuwe NAT IP-adres 21.x.x.x toe te staan.

Stap 5: Verificatie

Na het bijwerken van de allow-lijst met het nieuwe NAT IP-adres, werd de normale Secure Access-verkeersstroom hersteld en begonnen webverzoeken correct te functioneren via de SWG-proxy.

Oorzaak

De hoofdoorzaak was een wijziging in het openbare IP-adres van de gebruiker NAT van 20.x.x.x

naar 21.x.x.x. De SWG-proxy voor beveiligde toegang is zo geconfigureerd dat alleen verkeer vanaf het oorspronkelijke IP-adres wordt toegestaan, waardoor de verbinding opnieuw wordt ingesteld wanneer verkeer van het nieuwe IP-adres wordt ontvangen. Daarnaast was de belangrijkste aanwijzing dat https://policy.test.sse.cisco.com "401 ongeautoriseerde" fout vertoonde, die verwijst naar http connect request is hitting naar proxy, dit wordt ook bevestigd door PCAP, maar proxy kan gebruikersverkeer niet verifiëren op basis van hun OrgID en andere metagegevens om het beleid toe te passen en het verkeer toe te staan. Dit resulteerde in de proxy die verbindingen met TCP RST-pakketten beëindigde, waardoor succesvolle webverzoeken niet konden worden verwerkt.

Toegevoegd de nieuwe NATed IP in gebruiker CSA UI onder geregistreerd netwerk om web traffic flow probleem voor SWG PAC-bestand op te lossen.

Gerelateerde inhoud

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.