Resolución de Problemas de Conexión de Proxy SWG de Secure Access para el Archivo PAC

Contenido

Problema

Los usuarios experimentaron fallos de conexión al intentar acceder a sitios web a través de Cisco Secure Access mediante la URL proxy SWG (gateway web segura) swg-url-proxy-https-8xxxx.sseproxy.qq.opendns.com.

Los síntomas específicos incluyeron:

- Las solicitudes web (como https://www.google.com) generaban errores de conexión en los exploradores
- El tráfico no aparecía en los registros de búsqueda de actividad
- Se observaron restablecimientos del servidor desde la IP de salida del cliente/IP de origen del cliente hacia los terminales de destino:
    - k8s-sigpro-sigpro-c10eb6eb-38fbeb0455191ac5.elb.eu-central-1.amazonaws.com
    - k8s-sigpro-sigpro-f8f3d861-14341dd91e659675.elb.eu-central-1.amazonaws.com
- Los problemas comenzaron aproximadamente a las 09:30 AM CEST
- La resolución DNS del nombre de host SWG funcionaba correctamente
- Las conexiones Telnet a swg-url-proxy-https-8xxxx.sseproxy.qq.opendns.com en el puerto 443 se realizaron correctamente
- El firewall exterior no estaba bloqueando las conexiones a las IP de destino

El análisis de captura de paquetes reveló paquetes TCP RST provenientes del proxy, lo que indica la terminación de la conexión en el nivel del proxy.

Entorno

- Tecnología: Cisco Secure Access (SSE)
- Componente: Gateway web seguro (SWG)
- URL de proxy SWG: swg-url-proxy-https-8385532.sseproxy.qq.opendns.com
- Puertos afectados: 443 y 80
- IP NAT original: 20.x.x.x
- IP de NAT actualizada: 21.x.x.x
- Terminales AWS ELB para ex: región eu-central o us-east
- Configuración de WPAD que dirige los navegadores al proxy SWG

Resolución

El problema se resolvió actualizando la configuración de la lista de permitidos para incluir la dirección IP NAT correcta.

Los pasos descritos en las siguientes secciones se tomaron para identificar y resolver el problema.

Paso 1: Recopilación de datos de diagnóstico

Capturas de paquetes recopiladas y configuración de scripts WPAD para analizar el flujo de tráfico y la configuración de proxy.

Además de eso, la pista principal era https://policy.test.sse.cisco.com mostraba el error "401 no autorizado". Lo que significa que la solicitud de conexión http llega al proxy, pero el proxy no puede autenticar el tráfico de usuario en función de su OrgID y otros detalles de metadatos para aplicar la política y permitir el tráfico.

Paso 2: Análisis del tráfico

El análisis de la captura de paquetes reveló:

- Los paquetes RST de TCP se estaban enviando desde el proxy
- Los registros de búsqueda de actividad no mostraron el tráfico fallido
- La IP de origen en el flujo de tráfico ha cambiado

Paso 3: Identificación de dirección IP de NAT

La investigación reveló que la dirección IP pública de NAT había cambiado de 20.x.x.x a 21.x.x.x. La IP cambiada se agregó como red registrada en la interfaz de usuario CSA, el tráfico SWG comenzó a funcionar para la implementación de archivos PAC después de registrar la IP correcta en el portal CSA.

Paso 4: Actualización de configuración de Allow-List

Actualización de las reglas de la lista de permitidos/del firewall para permitir el tráfico desde la nueva dirección IP NAT 21.x.x.x.

Paso 5: Verificación

Después de actualizar la lista de permitidos con la nueva dirección IP de NAT, se restauró el flujo de tráfico de Secure Access normal y las solicitudes web comenzaron a funcionar correctamente a través del proxy SWG.

Causa

La causa raíz fue un cambio en la dirección IP pública NAT del usuario de 20.x.x.x a 21.x.x.x. El

proxy SWG de acceso seguro se configuró para permitir solo el tráfico de la dirección IP original, lo que provoca que la conexión se restablezca cuando el tráfico llega desde la nueva dirección IP. Además de eso, la pista principal era https://policy.test.sse.cisco.com mostraba el error "401 no autorizado", que se refiere a que la solicitud de conexión http está llegando al proxy, esto también lo confirma PCAP, pero el proxy no puede autenticar el tráfico de usuario en función de su OrgID y otros detalles de metadatos para aplicar la política y permitir el tráfico. Esto dio lugar a que el proxy terminara las conexiones con los paquetes RST TCP, lo que impidió que se procesaran las solicitudes web correctas.

Se agregó la nueva IP NATed en la interfaz de usuario CSA de la red registrada para resolver el problema de flujo de tráfico web para el archivo SWG PAC.

Contenido relacionado

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).