Solucionar problemas de conexão do proxy SWG de acesso seguro para o arquivo PAC

Contents

Problema

Os usuários experimentaram falhas de conexão ao tentar acessar sites através do Cisco Secure Access usando o URL de proxy SWG (Secure Web Gateway) swg-url-proxy-https-8xxxx.sseproxy.qq.opendns.com.

Os sintomas específicos incluíram:

- As solicitações da Web (como https://www.google.com) falhavam devido a erros de conexão nos navegadores
- O tráfego não estava aparecendo nos logs de pesquisa de atividade
- As redefinições do servidor foram observadas do IP de origem do cliente/IP de saída do cliente em direção aos endpoints de destino:
    - k8s-sigpro-sigpro-c10eb6eb-38fbeb0455191ac5.elb.eu-central-1.amazonaws.com
    - k8s-sigpro-sigpro-f8f3d861-14341dd91e659675.elb.eu-central-1.amazonaws.com
- Os problemas começaram aproximadamente às 9h30, horário do Pacífico
- A resolução DNS para o nome de host SWG estava funcionando corretamente
- As conexões Telnet para swg-url-proxy-https-8xxxx.sseproxy.qq.opendns.com na porta 443 foram bem-sucedidas
- O firewall externo não estava bloqueando as conexões aos IPs de destino

A análise de captura de pacotes revelou pacotes TCP RST vindos do proxy, indicando o término da conexão no nível do proxy.

Ambiente

- Tecnologia: Cisco Secure Access (SSE)
- Componente: Gateway da Web seguro (SWG)
- URL do proxy do SWG: swg-url-proxy-https-8385532.sseproxy.qq.opendns.com
- Portas afetadas: 443 e 80
- IP NAT original: 20 x x x
- IP NAT atualizado: 21 x x x
- Endpoints AWS ELB em por ex: região centro-ue ou leste-eua
- Configuração de WPAD direcionando navegadores para o proxy SWG

Resolução

O problema foi resolvido atualizando-se a configuração da lista de permissão para incluir o endereço IP de NAT correto.

As etapas descritas nas próximas seções foram seguidas para identificar e resolver o problema.

Passo 1: Coleta de Dados de Diagnóstico

Capturas de pacotes coletadas e configuração de script WPAD para analisar o fluxo de tráfego e a configuração de proxy.

Além disso, a pista principal era https://policy.test.sse.cisco.com estava mostrando o erro "401 não autorizado". O que significa que a solicitação de conexão http está chegando ao proxy, mas o proxy não pode autenticar o tráfego do usuário com base em seu OrgID e outros detalhes de metadados para aplicar a política e permitir o tráfego.

Passo 2: Análise de tráfego

A análise da captura de pacotes revelou:

- Os pacotes TCP RST estavam sendo enviados do proxy
- Os logs de pesquisa de atividade não mostram o tráfego com falha
- O IP de origem no fluxo de tráfego foi alterado

Passo 3: Identificação de endereço IP de NAT

A investigação revelou que o endereço IP público NAT mudou de 20.x.x.x para 21.x.x.x. O IP alterado foi adicionado como rede registrada na UI CSA do usuário, o tráfego SWG começou a funcionar para a implantação do arquivo PAC depois de registrar o IP correto no portal CSA.

Passo 4: Atualização da configuração da lista de permissões

Regras de lista de permissão/firewall atualizadas para permitir o tráfego do novo endereço IP de NAT 21.x.x.x.

Passo 5: Verificação

Após atualizar a lista de permissão com o novo endereço IP de NAT, o fluxo de tráfego normal do Secure Access foi restaurado e as solicitações da Web começaram a funcionar corretamente através do proxy SWG.

Causa

A causa raiz foi uma alteração no endereço IP público do NAT do usuário de 20.x.x.x para 21.x.x.x. O proxy SWG de acesso seguro foi configurado para permitir apenas o tráfego do endereço IP original, causando redefinições de conexão quando o tráfego chegou do novo endereço IP. Além disso, a pista principal foi https://policy.test.sse.cisco.com estava mostrando o erro "401 não autorizado", que se refere à solicitação de conexão http está atingindo o proxy, isso também é confirmado pelo PCAP, mas o proxy não pode autenticar o tráfego do usuário com

base em seu OrgID e outros detalhes de metadados para aplicar a política e permitir o tráfego. Isso fez com que o proxy encerrasse conexões com pacotes TCP RST, impedindo que solicitações da Web bem-sucedidas fossem processadas.

Adicionado o novo IP com NAT na UI do usuário CSA na rede registrada para resolver o problema de fluxo de tráfego da Web para o arquivo SWG PAC.

Conteúdo relacionado

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.