Risoluzione dei problemi di connessione del proxy SWG di accesso sicuro per il file PAC

Sommario

Problema

Gli utenti hanno riscontrato errori di connessione durante il tentativo di accedere ai siti Web tramite Cisco Secure Access utilizzando l'URL proxy SWG (Secure Web Gateway) swg-url-proxy-https-8xxxx.sseproxy.qq.opendns.com.

I sintomi specifici includono:

- Richieste Web (ad esempio a https://www.google.com) non riuscite con errori di connessione nei browser
- Traffico non visualizzato nei log di ricerca attività
- Sono state osservate reimpostazioni del server dall'IP di origine del client/IP di uscita del client verso gli endpoint di destinazione:
    - k8s-sigpro-sigpro-c10eb6eb-38fbeb0455191ac5.elb.eu-central-1.amazonaws.com
    - k8s-sigpro-sigpro-f8f3d861-14341dd91e659675.elb.eu-central-1.amazonaws.com
- I problemi sono iniziati alle 9.30 circa
- La risoluzione DNS per il nome host SWG funzionava correttamente
- Connessioni Telnet a swg-url-proxy-https-8xxxx.sseproxy.qq.opendns.com sulla porta 443 riuscite
- Il firewall esterno non blocca le connessioni agli IP di destinazione

L'analisi dell'acquisizione dei pacchetti ha rivelato i pacchetti TCP RST provenienti dal proxy, indicando la terminazione della connessione a livello di proxy.

Ambiente

- Tecnologia: SSE (Cisco Secure Access)
- Componente: Secure Web Gateway (SWG)
- URL proxy SWG: swg-url-proxy-https-8385532.sseproxy.qq.opendns.com
- Porte interessate: 443 e 80
- IP NAT originale: 20,x,x,x
- IP NAT aggiornato: 21,x,x,x
- AWS-ELB endpoint in per es.: regione ue-centro o usa-est
- Configurazione WPAD indirizzamento dei browser al proxy SWG

Risoluzione

Il problema è stato risolto aggiornando la configurazione dell'elenco di indirizzi consentiti in modo da includere l'indirizzo IP NAT corretto.

Le operazioni descritte nelle sezioni seguenti sono state eseguite per identificare e risolvere il problema.

Passaggio 1: Raccolta dati di diagnostica

Acquisizioni di pacchetti raccolti e configurazione di script WPAD per analizzare il flusso del traffico e la configurazione del proxy.

Oltre a ciò, l'indizio principale era https://policy.test.sse.cisco.com stava mostrando l'errore "401 non autorizzato". Ciò significa che la richiesta di connessione HTTP sta passando al proxy, ma il proxy non è in grado di autenticare il traffico utente in base al proprio OrgID e ad altri dettagli di metadati per applicare i criteri e consentire il traffico.

Passaggio 2: Analisi del traffico

L'analisi dell'acquisizione del pacchetto ha rivelato:

- Pacchetti RST TCP inviati dal proxy
- Nei log di ricerca attività non è visualizzato il traffico che ha generato l'errore
- L'IP di origine nel flusso del traffico è stato modificato

Passaggio 3: Identificazione indirizzo IP NAT

L'inchiesta ha rivelato che l'indirizzo IP pubblico NAT è stato modificato da 20.x.x.x a 21.x.x.x. L'IP modificato è stato aggiunto come rete registrata nell'interfaccia utente CSA dell'utente, il traffico SWG ha iniziato a funzionare per la distribuzione del file PAC dopo la registrazione dell'IP corretto nel portale CSA.

Passaggio 4: Aggiornamento configurazione elenco indirizzi consentiti

Aggiornamento delle regole del firewall/elenco di autorizzazioni per autorizzare il traffico dal nuovo indirizzo IP NAT 21.x.x.x.

Passaggio 5: Verifica

Dopo l'aggiornamento dell'elenco dei permessi con il nuovo indirizzo IP NAT, è stato ripristinato il normale flusso del traffico di accesso sicuro e le richieste Web hanno iniziato a funzionare correttamente tramite il proxy SWG.

Causa

La causa principale è stata una modifica dell'indirizzo IP pubblico NAT dell'utente da 20.x.x.x a

21.x.x.x. Il proxy SWG di accesso sicuro è stato configurato per consentire solo il traffico proveniente dall'indirizzo IP originale, causando la reimpostazione della connessione quando il traffico è arrivato dal nuovo indirizzo IP. Inoltre, l'indizio principale era https://policy.test.sse.cisco.com che mostrava l'errore "401 unauthorized" (401 non autorizzato), che si riferisce alla richiesta di connessione http che sta per raggiungere il proxy, ciò è confermato anche da PCAP, ma il proxy non è in grado di autenticare il traffico degli utenti in base al proprio OrgID e ad altri dettagli sui metadati per applicare la policy e consentire il traffico. Il proxy ha interrotto le connessioni con i pacchetti TCP RST, impedendo l'elaborazione delle richieste Web riuscite.

Aggiunto il nuovo IP NATed nell'interfaccia utente CSA sotto rete registrata per risolvere il problema di flusso del traffico Web per il file SWG PAC.

Contenuto correlato

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).