Risoluzione dei problemi di accesso al sito Web SWG di Secure Web Gateway

Sommario

Questo documento descrive la metodologia strutturata per la diagnosi dei problemi di accesso ai siti Web quando instradati tramite un proxy basato su cloud (Secure Web Gateway/SWG), ma non quando si utilizza Direct Internet Access (DIA).

- Ambito: Si applica sia a Cisco Umbrella SIG che a Cisco Secure Access.

Prerequisiti e avvisi importanti

- Verificare che la risoluzione dei problemi venga eseguita su problemi riproducibili.
- Raccogliere un file HAR (HTTP Archive) e un'acquisizione simultanea dei pacchetti (PCAP) per fornire dati accurati per l'analisi.
- Le modifiche apportate alle policy proxy (ad esempio, ignorando la decrittazione o l'ispezione) possono influire sulla postura di sicurezza; applicare solo per la risoluzione dei problemi o come consigliato.

Identificazione degli errori a livello di proxy

Gli indicatori comuni di interferenza proxy includono:

- 502 Gateway non valido
- Certificato upstream 515 non attendibile
- Certificato upstream 517 revocato
- 403 Vietato
- Certificati revocati
- Mancata corrispondenza del gruppo di crittografia
- Timeout connessione sito Web

Metodologia di risoluzione dei problemi

Passaggio 1: Conferma passaggio traffico al proxy

- Raccolta dati: Generare un file HAR e PCAP quando si verifica il problema.
- Analisi intestazione: Controllare l'intestazione Via nelle risposte HTTP. La presenza di `s_proxy` (proxy Nginx) o `m_proxy` (servizio proxy modulare/MPS) conferma che il traffico è proxy.
- Flusso TCP: In Wireshark, seguire il flusso TCP per verificare che la connessione sia all'IP del proxy, non all'IP di destinazione.

Passaggio 2: Verifica stato decrittografia TLS

- Controllo browser: Fare clic sull'icona del lucchetto nella barra degli indirizzi del browser. Se nella catena di certificati viene visualizzato il certificato Cisco Secure Access Root, l'ispezione HTTPS è attiva.
- Convalida: Creare riferimenti incrociati tra le intestazioni Via nei file HAR/PCAP.
- Comando OpenSSL: Per ispezionare le catene di certificati:
  `openssl s_client -connect www.example.com:443 -showcerts`
  Questo comando controlla la catena di certificati presentata dal server. Eseguirlo da un computer che attraversa il proxy per la convalida diretta.

Passaggio 3: Isolamento e processo di eliminazione

1. Fase A - Test ispezione HTTPS (livello Nginx):
   - Aggiungete il dominio con problemi all'elenco SWG "Do Not Decrypt" (Non decrittografare).
   - Mantieni controllo file abilitato.
   - Se il problema è risolto: La causa principale è probabilmente l'ispezione SSL/TLS Nginx. Analizzare il PCAP per individuare eventuali mancate corrispondenze o problemi SNI. Utilizzare `curl` con e senza proxy per confrontare il comportamento.
   - Se il problema persiste: Procedere alla fase B.
2. Fase B - Ispezione file di test (livello di scansione):
   - Disabilitare Ispezione file per il traffico specifico.
   - Se il problema è risolto: La causa principale risiede nel motore di analisi dei file. Esaminare PCAP e HAR, riprodurre in laboratorio e determinare se il problema è causato da un file specifico o da una firma di digitalizzazione.
   - Se non risolti: contattare il supporto tecnico fornendo registri e risultati completi.

Problemi comuni e codici di errore

Certificato upstream 515 non attendibile

Questo errore si verifica quando il proxy SWG non può convalidare il certificato del server di destinazione. Le cause includono catene di certificati scadute, autofirmate o incomplete.

- Ispezione HTTPS ON + Ispezione file ON: opere di siti web; nessun errore del certificato.
- Ispezione HTTPS ON + Ispezione file OFF: Errore 515, rapporto utente corrispondente.
- Ispezione HTTPS OFF + Ispezione file OFF (dominio nell'elenco Non decrittografare): Nessun problema rilevato.

Dettagli tecnici: Il proxy Nginx potrebbe avere esito negativo se il server upstream utilizza il recupero tramite AIA (Authority Information Access) per i certificati intermedi mancanti, in quanto Nginx non gestisce l'AIA in modo corretto come il servizio proxy di scansione dei file. La mancata corrispondenza di SNI e SAN durante l'handshake TLS può anche causare errori.

Certificato upstream 517 revocato

L'errore 517 indica che il controllo OCSP o CRL del proxy SWG ha rilevato che il certificato del server upstream è stato revocato.

- Risoluzione dei problemi: Utilizzare strumenti esterni quali SSL Labs o OpenSSL per confermare lo stato di revoca.
- Documentazione:
  - Errore 517 nella risoluzione dei problemi Cisco - Certificato upstream revocato
  - Comprendere gli errori comuni di protocollo e certificato

Opzioni di gestione degli errori dei certificati

Cisco Secure Access introdurrà una nuova funzionalità denominata "Opzioni di gestione degli errori dei certificati" per il bypass granulare degli errori senza disabilitare completamente la decrittografia. I domini che attivano errori di certificato a causa dell'ispezione possono essere gestiti utilizzando questa funzione invece di elenchi "Non decrittografare" ampi.
Questa funzione esiste in Umbrella SIG da oggi. Dettagli delle richieste di funzionalità per CSA.

502 Gateway non valido

L'errore 502 indica che il proxy SWG ha ricevuto una risposta non valida dal server upstream mentre agiva come intermediario.

- A valle: Da client a proxy SWG
- A monte: Proxy SWG su server di destinazione

L'errore si verifica sempre nella connessione a monte a causa di errori di protocollo, reimpostazioni TCP o intestazioni in formato non corretto.

Cause comuni 502

- Suite di crittografia SWG non supportate
- Richiesta di autenticazione certificato client
- Intestazioni aggiunte dal proxy SWG

Suite di crittografia non supportate

Causa: Il server richiede una cifratura non supportata da SWG, ad esempio TLS_CHACHA20_POLY1305_SHA256.
Risoluzione: Aggiungere il dominio all'elenco di decrittografia selettiva.

Comandi di test:
Con proxy:

```
curl -x proxy.sig.umbrella.com:80 -v xyz.com:80
curl -x swg-url-proxy-https.sigproxy.qq.opendns.com:443 -vv -k "https://www.cnn.com" >> null
```

Senza proxy:

```
curl -v www.xyz.com:80
```

Mac/Linux:

```
curl -vv -o /dev/null -k -L www.cnn.com
```

Windows:

```
curl -vv -o null -k -L www.cnn.com
```

Richiesta di autenticazione certificato client

Causa: Il server upstream richiede certificati sul lato client che SWG non supporta.
Risoluzione: Ignorare il dominio dal proxy utilizzando l'elenco di gestione dei domini esterni (Umbrella SIG) o ignorare il proxy protetto (Cisco Secure Access). Ignorare solo l'ispezione HTTPS non è sufficiente.

Intestazioni aggiunte dal proxy

Causa: Alcuni server rifiutano le richieste con l'intestazione X-Forwarded-For (XFF) aggiunta da SWG quando l'ispezione HTTPS è abilitata.
Risoluzione: Confronto del comportamento con/senza HTTPS e ispezione dei file. Se l'errore si verifica solo quando è presente XFF, è probabile che il server Web non sia configurato correttamente.

Esempio:
`curl https://www.xyz.com -k –header 'X-Forwarded-For: 1.1.1.1' -o /dev/null -w "Codice di stato: %{http_code}" -s`
Codice stato: 502
`curl https://www.xyz.com -k -o /dev/null -w "Codice di stato: %{http_code}" -s`
Codice stato: 200

L'intestazione XFF viene aggiunta per la geolocalizzazione. Se il server non è in grado di elaborarlo, viene generato un errore 502.

PUA potenzialmente indesiderato o file danneggiati

Se SWG non riesce a eseguire la scansione di un file mediante l'ispezione dei file (ad esempio, file protetti, richiesti da intervalli o danneggiati), blocca il download e segnala - Bloccato - Applicazione potenzialmente indesiderata (file protetto)

- Risoluzione dei problemi: Acquisire un HAR durante l'evento di blocco. Utilizzare Sostituisci protezione come soluzione temporanea. Se il file è danneggiato o dannoso, deve essere corretto all'origine.

Categorie e blocchi della reputazione potenzialmente dannosi

- Utilizzare Talos per verificare la reputazione Web (WBRS). Se un dominio è erroneamente classificato, presentare una richiesta COG Jira a Talos per la revisione. Talos classificato come sicuro o favorevole ma ancora SWG blocco allora abbiamo bisogno di controllare dal servizio Beaker di SWG.

Accesso negato da Akamai per gli IP di uscita SWG

- SWG utilizza IP in uscita condivisi. Se tali siti sono inclusi nella lista nera dei servizi di reputazione IP (ad esempio, Brightcloud), l'accesso a determinati siti potrebbe essere negato.

Problemi noti: Bot e video di accesso a Youtube non disponibili

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).