502 / 504 GATEWAY_TIMEOUT errori durante l'esplorazione di determinati siti

Sommario

Domanda:

Perché vengono visualizzati gli errori 502 / 504 GATEWAY_TIMEOUT durante la navigazione in determinati siti?

Sintomi: Gli utenti ricevono 502 o 504 errori di timeout del gateway da Cisco WSA quando navigano su determinati siti Web

Gli utenti ricevono 502 o 504 errori di timeout del gateway durante l'esplorazione dei siti Web. Nei log degli accessi viene visualizzato 'NONE/504' o 'NONE/502'

Esempio di riga del log degli accessi:

1233658928.496 153185 10.10.70.50 **NONE/504** 1729 GET http://www.example.com/ - DIRECT/www.example.com - .....

Esistono molti motivi per cui WSA potrebbe restituire un errore di timeout del gateway 502 o 504. Sebbene queste risposte di errore siano simili, è importante capire le sottili differenze tra di esse.

Di seguito sono riportati alcuni esempi dei tipi di scenari che possono verificarsi:

- **502:** WSA ha tentato di stabilire una connessione TCP con il server Web, ma non ha ricevuto SYN/ACK.
- **504:** WSA sta ricevendo un TCP reset (RST) che interrompe la connessione con il server Web.
- **504:** WSA non riceve una risposta da un servizio richiesto prima di comunicare con il server Web, ad esempio si è verificato un errore DNS.
- **504:** WSA ha stabilito una connessione TCP con il server Web e ha inviato una richiesta GET, ma non riceve mai la risposta HTTP.

Di seguito sono riportati alcuni esempi di ogni scenario e ulteriori dettagli su potenziali problemi:

502: WSA ha tentato di stabilire una connessione TCP con il server Web, ma non ha ricevuto SYN/ACK.
Se il server Web non risponde ai pacchetti SYN di WSA, dopo un certo numero di tentativi, al client verrà inviato un errore di timeout del gateway 502.

Le cause tipiche sono:
1. Problemi sul server Web o sulla rete del server Web.
2. Un problema di rete sulla rete WSA impedisce ai pacchetti SYN di raggiungere Internet.
3. Un firewall o un dispositivo simile sta ignorando i pacchetti SYN di WSA o il SYN/ACK del server Web
4. Lo spoofing IP è abilitato sul server WSA, ma non è configurato correttamente (nessun reindirizzamento del percorso di ritorno)

Procedura di risoluzione dei problemi:

Il primo passaggio consiste nel verificare se il server WSA può eseguire il ping ICMP sul server Web. A tale scopo, è possibile utilizzare il seguente comando CLI:
WSA> *ping* www.example.com
Se il ping ha esito negativo, non significa che il server non sia attivo. Potrebbe significare che i pacchetti ICMP vengono bloccati da qualche parte nel percorso. Se il ping ha esito positivo, possiamo essere certi che il server WSA disponga di un livello base di connettività di layer 3 al server Web.
Un test telnet verificherà se il server WSA è in grado di stabilire una connessione TCP sulla porta 80 al server Web. Per eseguire un test telnet, vedere le istruzioni riportate più avanti in questo articolo.

Problemi di rete o blocco del firewall
Se il ping ha esito positivo, ma il sistema telnet non funziona, è possibile che un dispositivo di filtraggio, ad esempio un firewall, impedisca al traffico di attraversare la rete. Si consiglia di analizzare i registri del firewall e/o le acquisizioni dei pacchetti dal firewall per ulteriori dettagli.
Lo spoofing IP è abilitato, ma non è configurato correttamente
Se l'inoltro tramite WSA o il test telnet ha esito positivo, significa che WSA è in grado di comunicare direttamente con il server Web, ma se un client esegue l'inoltro tramite WSA con lo spoofing IP, si è verificato un problema.

Senza spoofing IP dei client:
- Il WSA invia un SYN al server Web utilizzando il proprio indirizzo IP come origine. Quando il pacchetto torna indietro, viene indirizzato direttamente al WSA.

Con spoofing IP dei client:
- Il server WSA invia il messaggio SYN, ma utilizza l'indirizzo IP del client come origine. Senza una configurazione di rete speciale, il pacchetto restituito verrà inviato al client anziché al WSA.
- Per utilizzare lo spoofing IP dei client, la rete deve essere configurata in modo specifico per facilitare il reindirizzamento corretto dei pacchetti. Se i pacchetti del percorso di ritorno del server Web vengono inviati al client anziché al server WSA, quest'ultimo non vedrà mai i server SYN/ACK e restituirà al client un errore di timeout del gateway 502.

504: WSA sta ricevendo un TCP reset (RST) che interrompe la connessione con il server Web.

Se il WSA riceve un pacchetto di ripristino TCP nella connessione upstream al server Web, invierà un errore di timeout del gateway 504 al client.

Le cause tipiche sono:
1. Cisco Layer 4 Traffic Monitor (L4TM) impedisce al proxy WSA di connettersi al server Web.

2. Un firewall, un IDS, un IPS o un altro dispositivo di ispezione dei pacchetti sta bloccando il WSA.

Procedura di risoluzione dei problemi:
Determinare innanzitutto se il router TCP RST proviene da L4TM o da un altro dispositivo.
Se L4TM blocca questo traffico, questo verrà visualizzato nei report della GUI in "***Monitor -> L4 Traffic Monitor***". In caso contrario, l'RST proviene da un dispositivo diverso.
Blocco L4TM:
Se L4TM è bloccato, si consiglia di non bloccare le porte su cui è in esecuzione anche il proxy WSA. I motivi sono molteplici:
1. Il proxy WSA visualizza un messaggio di errore descrittivo in caso di problema, anziché limitarsi a reimpostare la connessione tramite TCP. Ciò contribuirà a limitare la confusione da parte degli utenti finali quando sono bloccati.
2. Il proxy WSA può analizzare e bloccare contenuti specifici, mentre L4TM blocca tutto il traffico che corrisponde a un indirizzo IP della blacklist.
Per configurare L4TM in modo che non venga bloccato sulle porte proxy, selezionare "***GUI -> Security Services -> L4 Traffic Monitor***".
Se si tratta di un sito Web notoriamente non valido, ma vi sono motivi per cui il traffico deve essere consentito, il sito può essere elencato in bianco:
"***GUI -> Web Security Manager -> L4 Traffic Monitor -> Allow List***"

Blocco firewall/IDS/IPS:
Se un altro dispositivo della rete blocca la connessione del server Web al server Web, si consiglia di analizzare quanto segue:
1. Registri blocchi firewall
2. Il pacchetto in entrata/in uscita viene acquisito durante il problema

I registri di blocco possono verificare rapidamente se il dispositivo blocca il WSA. A volte un firewall, un IPS o un IDS blocca il traffico e NON lo registra in modo appropriato. In questo caso, l'unico modo per dimostrare da dove proviene l'RST TCP è ottenere le clip in entrata e in uscita dal dispositivo. Se si invia un segnale RST dall'interfaccia in entrata e non ci sono pacchetti in uscita, la causa è sicuramente il dispositivo di sicurezza.

504: WSA ha stabilito una connessione TCP con il server Web e ha inviato una richiesta GET, ma non riceve mai la risposta HTTP.

Se il server WSA invia un comando HTTP GET ma non riceve mai una risposta, invierà al client un errore di timeout del gateway 504.

Le cause tipiche sono:

- Un firewall, IDS, IPS o un altro dispositivo di ispezione dei pacchetti consente la connessione TCP, ma impedisce al contenuto HTTP di raggiungere il server Web. In questo caso, il test telnet può aiutare a isolare il tipo di dati HTTP da bloccare.

I registri dei blocchi del firewall possono verificare rapidamente se e perché il dispositivo blocca il WSA. A volte un firewall, un IPS o un IDS blocca il traffico e NON lo registra in modo appropriato. In questo caso, l'unico modo per dimostrare da dove proviene l'RST TCP è ottenere le clip in entrata e in uscita dal dispositivo. Se si invia un segnale RST dall'interfaccia in entrata e non ci sono pacchetti in uscita, la causa è sicuramente il dispositivo di sicurezza.

Verifica della connettività con un server Web tramite telnet
Dalla CLI di WSA, eseguire il comando **telnet**: WSA> **telnet** Selezionare l'interfaccia da cui si desidera utilizzare telnet. 1. Automatico 2. Gestione (192.168.15.200/24: wsa.hostname.com) 3. P1 (192.168.113.199/24: data.com) [1]> **3** Immettere il nome host remoto o l'indirizzo IP. []> www.example.com Immettere la porta remota. [25]> **80** Sto provando 10.3.2.99... Connesso a www.example.com. Il carattere di escape è '^]'. **Nota**: Il messaggio "Connected" (Connesso) in rosso indica che il protocollo TCP è stato stabilito correttamente tra il server Web e il server WSA. Èpossibile inviare manualmente una richiesta HTTP anche tramite questa sessione telnet. Di seguito è riportata una richiesta di esempio che può essere digitata dopo il messaggio "Connected" (Connesso): — **SCARICA http://www.example.com HTTP/1.1** **HOST: www.example.com** **{Inserire}** — **Nota:** Assicurarsi di aggiungere il ritorno a capo aggiuntivo alla fine, altrimenti il server non risponderà alla richiesta.