Problema di controllo dello stato del proxy upstream WSA dopo un'interruzione della rete

Sommario

Problema

Dopo un'interruzione prolungata della rete, una appliance Cisco Web Security Appliance (WSA) configurata per utilizzare un proxy upstream specificato da FQDN può non riuscire a riprendere l'inoltro del traffico a un proxy upstream e inviare il traffico direttamente. Questo problema si verifica quando il server WSA contrassegna il proxy upstream come "inattivo" durante l'interruzione della rete, ma non riesce a riconoscere quando il proxy upstream diventa nuovamente disponibile, anche dopo il ripristino della connettività di rete.

I sintomi specifici osservati includono:

- WSA configurato con proxy upstream tramite FQDN e "Gestione errori = go Direct"
- Interruzione della rete a lungo termine che influisce sulla connettività sia al proxy upstream che al server DNS
- Dopo il ripristino della rete, nei log degli accessi non vengono visualizzati i tag DEFAULT_PARENT, a indicare che il traffico continua a ignorare il proxy upstream
- Il problema si verifica su un accessorio WSA, mentre un altro nello stesso ambiente funziona normalmente

Ambiente

- Cisco Web Security Appliance (WSA) serie S
- AsyncOS 14.5.2-01 (versione interessata)
- Hardware: S695
- Proxy upstream configurato con specifica FQDN

- Gestione degli errori configurata come "go Direct"
- Ambiente di rete con infrastruttura switch L2

Risoluzione

Per risolvere il problema, aggiornare AsyncOS a una versione contenente la correzione per CSCwi13124. Il bug è stato risolto nelle seguenti versioni AsyncOS:

- AsyncOS 15.5.0-566
- AsyncOS 15.5.0-710

Soluzione temporanea per le versioni correnti

Per gli ambienti che non possono essere aggiornati immediatamente, è disponibile una riduzione temporanea regolando il timeout massimo di inattività per il controllo dei proxy upstream che non rispondono:

Passaggio 1: Accedere alla CLI e selezionare la configurazione proxy avanzata:

```
cli -> advancedproxyconfig -> MISCELLANEOUS
```

Passaggio 2: Modificare l'impostazione del timeout di inattività massimo:

```
"Enter maximum idle timeout for checking unresponsive upstream proxy (in seconds)"
```

Passaggio 3: Ridurre il valore massimo predefinito (86400 secondi/24 ore) a un valore inferiore per ridurre il tempo tra i controlli di integrità.

Metodo di recupero immediato

Se il problema influisce sul flusso del traffico, il comando successivo può ripristinare immediatamente la funzionalità del proxy upstream:

Passaggio 1: Accedere al menu di diagnostica:

```
CLI > diagnostic > PROXY > kick
```

In questo modo il processo proxy viene riavviato e vengono ripristinate le normali operazioni proxy a monte.

Procedura di convalida e di verifica

Per verificare se il problema è presente o è stato risolto dopo un aggiornamento, esaminare i seguenti passaggi:

Passaggio 1: Definizione monitoraggio di base

Monitorare i log degli accessi e i log proxy per verificare che WSA stia inviando il traffico al proxy upstream. Verificare che il traffico stia raggiungendo il lato proxy upstream.

Passaggio 2: Simula interruzione rete

Dopo aver confermato il normale flusso di traffico verso il proxy upstream, disconnettere le seguenti connessioni:

- Connessione WSA a proxy upstream
- Connessione WSA a server DNS

Passaggio 3: Rilevamento errori monitor

Verificare nei log proxy e nei log di sistema la presenza di questi indicatori:

- Il registro proxy può visualizzare il proxy upstream come "... dichiarato inattivo"
- Nel registro eventi di sistema può essere visualizzato il messaggio "Critico: Raggiunto il

numero massimo di errori durante la query sul server DNS..."

Passaggio 4: Gestisci stato interrotto

Senza riavviare il processo proxy, mantenere lo stato disconnesso dal passaggio 2 e continuare a generare richieste per circa 10 ore.

Passaggio 5: Ripristina connettività

Dopo circa 10 ore, ripristinare le connessioni disconnesse nel passaggio 2.

Passaggio 6: Monitoraggio del comportamento di ripristino

Dopo aver completato il passaggio 5, monitorare i log degli accessi e i log proxy senza riavviare il processo proxy:

- In un sistema fisso: Il traffico riprende a scorrere attraverso il proxy upstream e i log proxy mostrano le normali transizioni di stato
- In un sistema interessato: I log di accesso mostrano il traffico che continua a ignorare il proxy upstream e i log proxy non mostrano i messaggi "... era malato, ora integro" o "... era integro, ora malato"

Causa

La causa principale di questo problema è un difetto logico nel meccanismo di controllo dello stato del proxy a monte. Quando WSA determina che un proxy upstream configurato è "inattivo" (non risponde), implementa un algoritmo di backoff esponenziale che raddoppia l'intervallo di controllo dello stato dopo ogni errore. Questo intervallo può raggiungere un massimo di 24 ore (86400 secondi).

Questo problema si verifica quando il proxy upstream diventa nuovamente disponibile durante uno di questi intervalli estesi. Anche se il proxy è stato ripristinato e risponde normalmente, WSA non eseguirà un controllo di integrità finché non è trascorso l'intero intervallo di tempo configurato. In questo modo, è possibile continuare il routing del traffico diretto fino a 24 ore anziché riprendere l'utilizzo del proxy a monte.

Questo comportamento influisce sulle configurazioni WSA in cui:

- Il proxy upstream è specificato da nome host/FQDN DNS (non indirizzo IP)
- Gestione degli errori è impostata su "go Direct" (Vai direttamente)
- Le interruzioni estese della rete influiscono sia sulla connettività del proxy upstream sia su quella del server DNS

ID bug Cisco: CSCwi13124

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).