Flash intermittente del gruppo di tunnel di rete ad accesso sicuro con il gateway VPN di Azure durante gli eventi di reimpostazione chiavi IKE

Sommario

Problema

In un gruppo di tunnel di rete appena configurato tra Cisco Secure Access e il gateway VPN di Azure viene eseguito il flapping intermittente del tunnel ogni 4 ore circa durante gli eventi di reimpostazione delle chiavi IKE.

Vengono osservati i seguenti messaggi di errore e sintomi specifici:

- Peering BGP interrotto, timer di attesa scaduto
- Avviso: reimpostazione chiave IKE non riuscita
- Tunnel IKE disconnesso

Il flapping del tunnel causa interruzioni periodiche, errori di reimpostazione chiavi IKE, errori di controllo dell'integrità, disconnessioni del tunnel e interruzioni del peering BGP, con un impatto sulla connettività stabile alle risorse di Azure. Gli errori di autenticazione vengono rilevati durante le negoziazioni di reimpostazione chiavi.

Ambiente

- Gruppo tunnel di rete Cisco Secure Access (CSA) configurato per il gateway VPN di Azure
- Tunnel VPN da sito a sito IPsec con IKEv2
- Gateway VPN di Azure con crittografia AES-GCM-256 configurata nei criteri in modalità principale (MM)

- NAT-T (NAT Traversal) abilitato su entrambi i lati con la porta 4500
- Peering BGP configurato tra endpoint
- Durata predefinita SA IKE di 4 ore (2800 secondi)
- Configurazione iniziale della durata della SA IPsec, successivamente modificata in 10800 secondi
- PFS (Perfect Forward Secrecy) non abilitato sul lato Azure

Risoluzione

Il problema è stato risolto tramite una modifica della configurazione per evitare le cifrature AES-GCM nei criteri in modalità principale, in base all'identificazione di un bug nel gateway VPN di Azure.

Passaggio 1: Analisi di debug del gateway VPN di Azure

I debug IKE sono stati raccolti dal lato del gateway VPN di Azure. Questo comportamento è stato rilevato durante i tentativi di reimpostazione delle chiavi:

```
SESSION_ID :{} Remote x.x.x.x:500: Local x.x.x.x:500: [SEND]Sending IPSec policy Payload for tunnel Id
SESSION_ID :{} Remote x.x.x.x:4500: Local x.x.x.x:4500: [SEND][CHILD_SA MM_REKEY] Sending IKE rekey res
SESSION_ID :{} Remote x.x.x.x:4500: Local x.x.x.x:4500: [LOCAL_MSG] IKE Tunnel closed for tunnelId x3 w
```

Passaggio 2: Identificazione della root cause

Il supporto di Azure ha analizzato gli errori di reimpostazione chiavi. L'analisi di Azure ha rilevato che quando Azure avvia MM-REKEY con AES-GCM-256, il pacchetto di reimpostazione chiavi non è valido. Il dispositivo locale non risponde alla richiesta di rigenerazione della chiave non valida. Il tunnel verrà disconnesso.

Passaggio 3: Implementazione della soluzione alternativa di configurazione

In base ai suggerimenti forniti da Azure, è stata implementata questa riduzione:

- Rimuovere le cifrature AES-GCM dai criteri in modalità principale (MM) nella configurazione di Network Tunnel Group.
- Configurare metodi di crittografia alternativi che non utilizzano la modalità GCM.

Fare riferimento al passo 17 in https://securitydocs.cisco.com/docs/csa/olh/121327.dita.

Passaggio 4: Opzioni di mitigazione alternative

Azure ha inoltre fornito strategie di mitigazione aggiuntive che è possibile considerare:

- Configurare la durata di MM locale su un valore maggiore di 2800 secondi in modo che Azure avvii sempre la reimpostazione delle chiavi.
- Impostare il gateway VPN di Azure sulla modalità solo risponditore con una durata dell'associazione di sicurezza locale inferiore alla durata di Azure.

Causa

La causa principale è un bug nel gateway VPN di Azure che influisce sulle operazioni di reimpostazione delle chiavi AES-GCM. Quando Azure avvia una richiesta MM-REKEY utilizzando AES-GCM-256, il pacchetto di rigenerazione delle chiavi non è valido e il dispositivo Cisco Secure Access locale non risponde alla richiesta di rigenerazione delle chiavi non valida. Il risultato sono errori di rigenerazione delle chiavi IKE, errori di autenticazione e conseguenti disconnessioni del tunnel.

Azure ha confermato che si tratta di un bug esistente e ha documentato una correzione pianificata in una versione futura del gateway destinata a metà 2026.

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).