

Problema di connettività del tunnel IPsec di accesso sicuro con il router Versa Networks a causa della negoziazione ESN

Sommario

Problema

Durante la distribuzione di Cisco Secure Access in una succursale che utilizza il router Versa-Network come dispositivo periferico, sono stati rilevati problemi di connettività nonostante entrambi i tunnel IPsec risultassero operativi. T

I sintomi specifici includono:

- Nessuna connettività dalla filiale a Cisco Secure Access
- Accesso a Internet tramite route statiche non funzionante
- Rilevato traffico crittografato unidirezionale (solo in uscita per accesso protetto)
- Statistiche del router che mostrano i pacchetti in uscita inviati ma non i pacchetti in entrata ricevuti
- Funzionamento bidirezionale di Dead Peer Detection tra il router SD-WAN e Secure Access
- Valori SPI (Security Parameter Index) per la corrispondenza corretta del traffico in uscita
- Lo sfarfallio del tunnel (reimpostazione) non ha risolto il problema di connettività
- Le acquisizioni dei pacchetti e gli screenshot hanno confermato la mancanza di traffico in entrata
- La modifica delle cifrature del tunnel da CBC a GCM non ha risolto il problema

Dalle indagini è emerso che il traffico non è stato in grado di decrittografare il lato Cisco a causa di errori di checksum tracciati sulla funzionalità ESN (Extended Sequence Number) del router Versa.

Ambiente

- Distribuzione Cisco Secure Access
- Versa-Networks Router come dispositivo periferico
- Configurazione tunnel IP-Identity
- Configurazione del tunnel IPsec con tentativi di cifratura CBC e GCM

Risoluzione

La risoluzione prevedeva la disabilitazione della negoziazione ESN (Extended Sequence Number) sul router Versa per impedire errori di checksum che causavano errori di decrittografia sull'headend Cisco Secure Access.

Procedura di risoluzione

Passaggio 1: Identificazione della root cause

L'indagine ha stabilito che il router Versa stava negoziando il numero ESN (Extended Sequence Number), il che stava causando la ricezione di errori di checksum da parte dell'headend Cisco Secure Access e la mancata decrittografia dei pacchetti creati con ESN.

Passaggio 2: Disabilitazione di ESN su router Versa

Contattare il supporto Versa Networks o l'amministratore del router per disabilitare i controlli ESN e la negoziazione sulla configurazione del router Versa. In questo modo viene risolto il bug Versa noto che causa la negoziazione non corretta di ESN.

Passaggio 3: Verifica connettività

Dopo aver disattivato la negoziazione ESN, verificare che il flusso del traffico bidirezionale sia stato stabilito e che la connettività completa tra la filiale e Secure Access e Internet sia stata ripristinata.

Passaggio 4: Monitora flusso traffico

Verificare che le statistiche sui pacchetti in entrata e in uscita sul router mostrino un flusso di traffico corretto in entrambe le direzioni, a conferma della corretta risoluzione del problema di traffico unidirezionale.

Causa

La causa principale è stata identificata come bug noto delle reti Versa (ID bug di supporto Versa: 12437 - ESN non deve essere negoziato da VOS) in cui il router Versa negozia in modo errato la funzionalità ESN (Extended Sequence Number) durante la definizione del tunnel IPsec. In seguito alla negoziazione ESN, l'headend Cisco Secure Access riceve i pacchetti con errori di checksum, impedendo la corretta decrittografia e determinando un flusso di traffico unidirezionale. Il router Versa invia correttamente i pacchetti in uscita, ma il traffico di ritorno non può essere elaborato correttamente a causa degli errori di decrittografia ESN.

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).