Gestione pacchetti ICMP frammentati con Cisco Secure Access

Sommario

Problema

Le richieste echo ICMP più grandi della MTU non ricevono risposte quando vengono inviate con il bit DF (Don't Fragment) disabilitato. Questo comportamento si verifica in due scenari specifici:

- Dagli endpoint VPN sull'interfaccia VPN quando si inviano pacchetti ICMP che superano le dimensioni MTU dell'interfaccia VPN con bit DF annullato
- Dagli endpoint locali su un tunnel IPsec tra un router di sito e Cisco Secure Access (CSA) quando si inviano pacchetti ICMP che superano le dimensioni dell'MTU dell'interfaccia del tunnel IPsec con bit DF annullato

In entrambi i casi, non viene ricevuta alcuna risposta ICMP e ciò porta a domande sull'eventualità che la CSA scarti pacchetti frammentati con il bit DF disabilitato.

Ambiente

- Cisco Secure Access (CSA)
- Endpoint VPN (Remote Access VPN)
- Tunnel IPsec tra router del sito e CSA
- Il traffico ICMP supera le dimensioni MTU dell'interfaccia
- Scenari di pacchetti frammentati con bit DF annullato

Risoluzione

Cisco Secure Access scarta i pacchetti frammentati in entrambi gli scenari di sovrimpressione e sovrapposizione. Questo comportamento è documentato nella documentazione della Guida di

Cisco Secure Access, in cui viene dichiarato esplicitamente: "I pacchetti frammentati nella parte inferiore o superiore vengono scartati."

Comportamento previsto

Cisco Secure Access è progettato per eliminare i pacchetti frammentati indipendentemente dal fatto che si trovino nella rete sottostante o sovrapposta. Ciò si applica a:

- Pacchetti ICMP inviati da endpoint VPN che superano l'MTU dell'interfaccia VPN con bit DF annullato
- Pacchetti ICMP inviati da endpoint locali su tunnel IPsec che superano l'MTU dell'interfaccia del tunnel con bit DF annullato

Questo comportamento è coerente in tutti gli scenari che coinvolgono pacchetti frammentati all'interno dell'infrastruttura Cisco Secure Access.

Per questa operazione è stata creata la richiesta di funzionalità CSE-I-5739.

Causa

L'architettura di Cisco Secure Access è progettata per eliminare i pacchetti frammentati in base a una decisione di progettazione della sicurezza e delle prestazioni. Questo comportamento viene implementato per prevenire potenziali vulnerabilità della sicurezza e sovraccarico di elaborazione associati al riassemblaggio dei pacchetti in scenari di rete sia sovrapposti che sottostanti.

Contenuto correlato

- Documentazione della Guida di Cisco Secure Access - Gestione pacchetti frammentati
- 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).