IPsec over TCP non riesce quando il traffico passa attraverso l'ASA

Sommario

Introduzione

I client VPN Cisco che si connettono a un headend VPN utilizzando IPsec su TCP possono connettersi all'headend correttamente, ma in seguito la connessione non riesce. In questo documento viene descritto come passare a IPsec su UDP o all'incapsulamento IPsec ESP nativo per risolvere il problema.

Operazioni preliminari

Requisiti

Per risolvere questo problema specifico, i client VPN Cisco devono essere configurati per connettersi a un dispositivo headend VPN tramite IPsec su TCP. Nella maggior parte dei casi, gli amministratori di rete configurano l'ASA in modo che accetti le connessioni dei client VPN Cisco sulla porta TCP 1000.

Componenti usati

Le informazioni di questo documento si basano su Cisco VPN Client.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Problema

Quando il client VPN è configurato per IPsec su TCP (cTCP), il software client VPN non risponderà se viene ricevuto un ACK TCP duplicato che richiede al client VPN di ritrasmettere i dati. Se si verifica una perdita di pacchetti tra il client VPN e l'headend ASA, è possibile che venga generato un ACK duplicato. La perdita intermittente dei pacchetti è una realtà abbastanza comune su Internet. Tuttavia, poiché gli endpoint VPN non utilizzano il protocollo TCP (si ricordi che utilizzano cTCP), gli endpoint continueranno a trasmettere e la connessione continuerà.

In questo scenario si verifica un problema se è presente un altro dispositivo, ad esempio un firewall, che tiene traccia della connessione TCP in modo statico. Poiché il protocollo cTCP non implementa completamente un client TCP e gli ACK duplicati del server non ricevono una risposta, è possibile che altri dispositivi in linea con questo flusso di rete scarichino il traffico TCP. La perdita di pacchetti deve verificarsi sulla rete causando la mancanza di segmenti TCP, che attiva il problema.

Questo non è un bug, ma un effetto collaterale della perdita di pacchetti sulla rete e del fatto che il protocollo cTCP non è un TCP reale. La tecnologia cTCP tenta di emulare il protocollo TCP incapsulando i pacchetti IPsec in un'intestazione TCP, ma questa è l'estensione del protocollo.

Questo problema si verifica in genere quando gli amministratori di rete implementano un'ASA con un IPS o eseguono una sorta di ispezione dell'applicazione sull'ASA che determina il funzionamento del firewall come proxy TCP completo della connessione. In caso di perdita di pacchetti, l'ASA invierà un ACK per i dati mancanti per conto del server o del client TCP c, ma il client VPN non risponderà mai. Poiché l'appliance ASA non riceve mai i dati che si aspetta, la comunicazione non può continuare. Di conseguenza, la connessione non riesce.

Soluzione

Per risolvere il problema, eseguire una delle azioni seguenti:

- Passare da IPsec su TCP a IPsec su UDP o eseguire l'incapsulamento nativo con il protocollo ESP.
- Passare al client AnyConnect per la terminazione VPN, che usa uno stack di protocolli TCP completamente implementato.
- Configurare l'ASA in modo che applichi il bypass stato-tcp per questi flussi IPsec/TCP specifici. In questo modo vengono sostanzialmente disattivati tutti i controlli di sicurezza per le connessioni che soddisfano il criterio di bypass stato-tcp, ma le connessioni funzioneranno fino a quando non sarà possibile implementare un'altra risoluzione dall'elenco. Per ulteriori informazioni, fare riferimento a Linee guida e limitazioni per il bypass dello stato del protocollo TCP.
- Identificare l'origine della perdita di pacchetti e adottare le misure correttive necessarie per impedire che i pacchetti IPsec/TCP vengano trasmessi sulla rete. Ciò è generalmente impossibile o estremamente difficile poiché la causa del problema è in genere la perdita di pacchetti su Internet e le cadute non possono essere evitate.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems