IPsec au-dessus de TCP échoue quand le trafic traverse l'ASA

Contenu

Introduction
Avant de commencer
Conditions requises
Composants utilisés
Conventions
Problème
Solution
Informations connexes

Introduction

Les Clients VPN Cisco qui se connectent à un headend VPN utilisant IPsec au-dessus de TCP pourraient se connecter au bien de headend, mais d'autre part la connexion échouent après une certaine heure. Ce document décrit comment commuter à IPsec au-dessus d'UDP ou d'encapsulation indigène d'IPsec de l'ESP afin de résoudre le problème.

Avant de commencer

Conditions requises

Afin de rencontrer ce problème spécifique, des Clients VPN Cisco doivent être configurés pour se connecter à un périphérique de headend VPN utilisant IPsec au-dessus de TCP. Dans la plupart des exemples, les administrateurs réseau configurent l'ASA pour recevoir des connexions de Client VPN Cisco au-dessus du port TCP 10000.

Composants utilisés

Les informations dans ce document sont basées sur le Client VPN Cisco.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Problème

Quand le client vpn est configuré pour IPsec au-dessus de TCP (cTCP), le logiciel de client VPN ne répondra pas si un TCP en double ACK est demander reçu le client vpn pour retransmettre des données. Un doublon ACK pourrait être généré s'il y a perte de paquets quelque part entre le client vpn et le headend ASA. La perte de paquets intermittente est une réalité assez commune sur l'Internet. Cependant, puisque les points finaux VPN n'utilisent pas le protocole TCP (rappel qu'ils utilisent le cTCP), les points finaux continueront de transmettre et la connexion continuera.

Dans ce scénario, un problème se pose s'il y a un autre périphérique tel qu'un Pare-feu dépistant la connexion TCP statefully. Puisque le protocole de cTCP n'implémente pas entièrement un doublon Acks de client et serveur de TCP ne recevez pas une réponse, ceci peut faire relâcher d'autres périphériques en conformité avec ce flot de réseau le trafic TCP. La perte de paquets doit se produire sur le réseau faisant disparaître des segments de TCP les disparus, qui déclenchent le problème.

Ce n'est pas une bogue, mais un effet secondaire de la perte de paquets sur le réseau et du fait que le cTCP n'est pas un vrai TCP. Les essais de cTCP pour émuler le protocole TCP en enveloppant les paquets d'IPsec dans une en-tête de TCP, mais c'est l'ampleur du protocole.

Cette question se produit typiquement quand les administrateurs réseau implémentent une ASA avec un IPS, ou fait un certain tri d'inspection d'application sur l'ASA qui fait agir le Pare-feu en tant que plein proxy de TCP de la connexion. S'il y a perte de paquets, l'ASA ACK pour les données manquantes au nom du serveur ou du client de cTCP, mais le client vpn ne répondra jamais. Puisque l'ASA ne reçoit jamais les données qu'elle prévoit, la transmission ne peut pas continuer. En conséquence, la connexion échoue.

Solution

Afin de résoudre ce problème, exécutez l'un de ces actions :

- Commutez d'IPsec au-dessus de TCP à IPsec au-dessus d'UDP, ou d'encapsulation indigène avec le protocole de l'ESP.
- Commutez au client d'AnyConnect pour l'arrêt VPN, qui utilise une pile de protocoles entièrement mise en application de TCP.
- Configurez l'ASA pour appliquer le TCP-état-contournement pour ces écoulements de la particularité IPsec/TCP. Ceci désactive essentiellement toute la Sécurité vérifie les connexions qui apparient la stratégie de TCP-état-contournement, mais permettra aux connexions pour fonctionner jusqu'à ce qu'une autre résolution de cette liste puisse être mise en application. Le pour en savoir plus, se rapportent à des instructions et à des limites de contournement d'état de TCP.
- Identifiez la source de perte de paquets, et agissez l'action corrective afin d'empêcher les paquets IPsec/TCP de relâcher sur le réseau. C'est habituellement impossible ou extrêmement difficile puisque le déclencheur à la question est habituellement perte de paquets sur l'Internet, et les baisses ne peuvent pas être empêchées.

Informations connexes

- Support et documentation techniques - Cisco Systems