IPsec sur TCP échoue lorsque le trafic transite par ASA

Contenu

Introduction

Les clients VPN Cisco qui se connectent à une tête de réseau VPN à l'aide d'IPsec sur TCP peuvent se connecter à la tête de réseau, mais la connexion échoue après un certain temps. Ce document décrit comment passer à IPsec sur UDP ou à l'encapsulation native ESP IPsec afin de résoudre le problème.

Avant de commencer

Conditions requises

Pour faire face à ce problème spécifique, les clients VPN Cisco doivent être configurés pour se connecter à un périphérique de tête de réseau VPN à l'aide d'IPsec sur TCP. Dans la plupart des cas, les administrateurs réseau configurent l'ASA pour accepter les connexions du client VPN Cisco sur le port TCP 10000.

Components Used

Les informations de ce document sont basées sur le client VPN Cisco.

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Problème

Lorsque le client VPN est configuré pour IPsec sur TCP (cTCP), le logiciel client VPN ne répond pas si un ACK TCP en double est reçu demandant au client VPN de retransmettre des données. Un accusé de réception en double peut être généré en cas de perte de paquets entre le client VPN et la tête de réseau ASA. La perte de paquets intermittente est une réalité assez courante sur Internet. Cependant, comme les points d'extrémité VPN n'utilisent pas le protocole TCP (rappelez-vous qu'ils utilisent cTCP), les points d'extrémité continueront à transmettre et la connexion continuera.

Dans ce scénario, un problème se produit s'il existe un autre périphérique, tel qu'un pare-feu qui suit la connexion TCP avec état. Puisque le protocole cTCP n'implémente pas complètement un client TCP et que les ACK dupliqués du serveur ne reçoivent pas de réponse, cela peut entraîner d'autres périphériques en ligne avec ce flux réseau à abandonner le trafic TCP. La perte de paquets doit se produire sur le réseau, entraînant l'absence de segments TCP, ce qui déclenche le problème.

Il ne s'agit pas d'un bogue, mais d'un effet secondaire de la perte de paquets sur le réseau et du fait que cTCP n'est pas un vrai TCP. Le cTCP tente d'émuler le protocole TCP en enveloppant les paquets IPsec dans un en-tête TCP, mais c'est l'étendue du protocole.

Ce problème se produit généralement lorsque les administrateurs réseau implémentent un ASA avec un IPS, ou effectuent une sorte d'inspection d'application sur l'ASA qui fait que le pare-feu agit comme un proxy TCP complet de la connexion. En cas de perte de paquets, l'ASA accepte les données manquantes au nom du serveur ou du client cTCP, mais le client VPN ne répondra jamais. Comme l'ASA ne reçoit jamais les données attendues, la communication ne peut pas se poursuivre. Par conséquent, la connexion échoue.

Solution

Pour résoudre ce problème, effectuez l'une des actions suivantes :

- Passez d'IPsec sur TCP à IPsec sur UDP, ou encapsulation native avec le protocole ESP.
- Basculez vers le client AnyConnect pour terminaison VPN, qui utilise une pile de protocoles TCP entièrement implémentée.
- Configurez l'ASA pour appliquer tcp-state-bypass pour ces flux IPsec/TCP spécifiques. Ceci désactive essentiellement toutes les vérifications de sécurité pour les connexions qui correspondent à la stratégie de contournement d'état tcp, mais permettra aux connexions de fonctionner jusqu'à ce qu'une autre résolution de cette liste puisse être implémentée. Pour plus d'informations, référez-vous à Directives et limitations de contournement d'état TCP.
- Identifiez la source de la perte de paquets et prenez des mesures correctives afin d'empêcher les paquets IPsec/TCP de tomber sur le réseau. Ceci est généralement impossible ou extrêmement difficile, car le déclencheur du problème est généralement la perte de paquets sur Internet, et les pertes ne peuvent pas être évitées.

Informations connexes

- Support et documentation techniques - Cisco Systems