IPSec sobre TCP falla cuando el tráfico fluye a través de ASA

Contenido

Introducción

Los Cisco VPN Clients que se conectan a una cabecera VPN mediante IPSec sobre TCP pueden conectarse correctamente a la cabecera, pero la conexión falla después de un tiempo. Este documento describe cómo cambiar a IPSec sobre UDP o a la encapsulación IPSec ESP nativa para resolver el problema.

Antes de comenzar

Requirements

Para encontrar este problema específico, los Cisco VPN Clients deben configurarse para conectarse a un dispositivo de cabecera VPN usando IPSec sobre TCP. En la mayoría de los casos, los administradores de red configuran el ASA para aceptar las conexiones de Cisco VPN Client sobre el puerto TCP 10000.

Componentes Utilizados

La información de este documento se basa en Cisco VPN Client.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Problema

Cuando el cliente VPN se configura para IPsec sobre TCP (cTCP), el software cliente VPN no responderá si se recibe un TCP ACK duplicado solicitando al cliente VPN que retransmita datos. Se podría generar un ACK duplicado si hay pérdida de paquetes en algún lugar entre el cliente VPN y la cabecera ASA. La pérdida intermitente de paquetes es una realidad bastante común en Internet. Sin embargo, dado que los terminales VPN no utilizan el protocolo TCP (recuerde que están utilizando cTCP), los terminales seguirán transmitiendo y la conexión continuará.

En esta situación, se produce un problema si hay otro dispositivo, como un firewall que rastrea la conexión TCP con estado. Dado que el protocolo cTCP no implementa completamente un cliente TCP y los ACK duplicados del servidor no reciben una respuesta, esto puede hacer que otros dispositivos en línea con este flujo de red descarten el tráfico TCP. La pérdida de paquetes debe producirse en la red, lo que hace que falten los segmentos TCP, lo que desencadena el problema.

Esto no es un error, sino un efecto secundario de ambas pérdidas de paquetes en la red y el hecho de que cTCP no es un TCP real. El cTCP intenta emular el protocolo TCP al ajustar los paquetes IPSec dentro de un encabezado TCP, pero ese es el alcance del protocolo.

Este problema suele ocurrir cuando los administradores de red implementan un ASA con un IPS, o realizan algún tipo de inspección de la aplicación en el ASA que hace que el firewall actúe como un proxy TCP completo de la conexión. Si hay pérdida de paquetes, el ASA ACK por los datos faltantes en nombre del servidor o cliente cTCP, pero el cliente VPN nunca responderá. Dado que el ASA nunca recibe los datos que espera, la comunicación no puede continuar. Como resultado, la conexión falla.

Solución

Para resolver este problema, realice cualquiera de estas acciones:

- Cambie de IPsec sobre TCP a IPsec sobre UDP, o encapsulación nativa con el protocolo ESP.
- Cambie al cliente AnyConnect para la terminación de VPN, que utiliza una pila de protocolo TCP completamente implementada.
- Configure el ASA para aplicar tcp-state-bypass para estos flujos IPSec/TCP específicos. Esto básicamente inhabilita todas las verificaciones de seguridad de las conexiones que coinciden con la política tcp-state-bypass, pero permitirá que las conexiones funcionen hasta que se pueda implementar otra resolución de esta lista. Para obtener más información, consulte Pautas y Limitaciones de Omisión de Estado TCP.
- Identifique el origen de la pérdida de paquetes y tome medidas correctivas para evitar que los paquetes IPSec/TCP caigan en la red. Esto suele ser imposible o extremadamente difícil, ya que el disparador del problema suele ser la pérdida de paquetes en Internet y las caídas no se pueden prevenir.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems