El IPSec sobre el TCP falla cuando el tráfico atraviesa el 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

Requisitos

Para encontrar este problema específico, los Clientes Cisco VPN deben ser configurados para conectar con un dispositivo de la cabecera VPN usando el IPSec sobre el TCP. En la mayoría de los casos, los administradores de la red configuran el ASA para validar las conexiones del Cliente Cisco VPN sobre el puerto TCP 10000.

Componentes Utilizados

La información en este documento se basa en el Cliente Cisco VPN.

Convenciones

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

Problema

Cuando configuran al cliente VPN para el IPSec sobre TCP (cTCP), el software cliente VPN no responderá si un duplicado TCP ACK es el pedir recibido el cliente VPN retransmitir los datos. Un duplicado ACK pudo ser generado si hay pérdida del paquete en alguna parte entre el cliente VPN y el headend ASA. La pérdida del paquete intermitente es una realidad bastante común en Internet. Sin embargo, puesto que los puntos finales de VPN no están utilizando el protocolo TCP (memoria que están utilizando el cTCP), los puntos finales continuarán transmitiendo y la conexión continuará.

En este escenario, un problema ocurre si hay otro dispositivo tal como un Firewall que sigue la conexión TCP statefully. Puesto que el protocolo del cTCP no implementa completamente a un cliente TCP y el servidor ACK duplicados no recibe una respuesta, éste puede hacer los otros dispositivos conforme a esta secuencia de la red caer tráfico TCP. La pérdida del paquete debe ocurrir en la red que hace los segmentos TCP ir a faltar, que acciona el problema.

Éste es un no bug, sino un efecto secundario de la pérdida del paquete sobre la red y del hecho de que el cTCP no es un TCP real. El cTCP intenta emular al protocolo TCP envolviendo los paquetes IPsec dentro de un encabezado TCP, pero ése es el fragmento del protocolo.

Este problema ocurre típicamente cuando los administradores de la red implementan un ASA con un IPS, o hace una cierta clase de Inspección de la aplicación en el ASA que hace el Firewall actuar como proxy lleno TCP de la conexión. Si hay pérdida del paquete, el ASA ACK para los datos que falta en nombre del servidor o del cliente del cTCP, pero el cliente VPN nunca responderá. Puesto que el ASA nunca recibe los datos que está esperando, la comunicación no puede continuar. Como consecuencia, la conexión falla.

Solución

Para resolver este problema, realice ninguno de estos acciones:

- Switch del IPSec sobre el TCP al IPSec sobre el UDP, o encapsulación nativa con el protocolo ESP.
- Switch al cliente de AnyConnect para la terminación VPN, que utiliza una pila del protocolo completamente implementada TCP.
- Configure el ASA para aplicar TCP-estado-puente para estos flujos específicos IPsec/TCP. Esto esencialmente inhabilita todas las revisiones de seguridad para las conexiones que corresponden con la directiva de TCP-estado-puente, pero permitirá que las conexiones trabajen hasta que otra resolución de esta lista pueda ser implementada. Para más información, refiera a las guías de consulta y a las limitaciones de puente del estado TCP.
- Identifique la fuente de la pérdida del paquete, y tome la acción correctiva para evitar que los paquetes IPsec/TCP caigan en la red. Esto es generalmente imposible o extremadamente difícil puesto que el activador al problema es generalmente pérdida del paquete en Internet, y los descensos no pueden ser prevenidos.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems