O IPsec sobre o TCP falha quando o tráfego corre através do ASA

Índice

Introdução

Os Cisco VPN Clients conectados a um headend de VPN usando IPsec over o TCP podem se conectar satisfatoriamente ao headend, mas a conexão falha após algum tempo. Este documento descreve como comutar para IPsec over UDP ou encapsulamento do ESP do IPSec nativo para resolver o problema.

Antes de Começar

Requisitos

A fim encontrar este problema específico, os Cisco VPN Client devem ser configurados para conectar a um dispositivo do fim de cabeçalho de VPN usando o IPsec sobre o TCP. Na maioria de exemplos, os administradores de rede configuram o ASA para aceitar conexões do Cisco VPN Client sobre a porta TCP 10000.

Componentes Utilizados

A informação neste documento é baseada no Cisco VPN Client.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Problema

Quando o cliente VPN estiver configurado para o IPsec sobre TCP (cTCP), o software do cliente VPN não responderá se uma duplicata TCP ACK é pedir recebido o cliente VPN retransmitir dados. Uma duplicata ACK pôde ser gerada se há uma perda de pacotes em algum lugar entre o cliente VPN e o final do cabeçalho ASA. A perda de pacotes intermitente é uma realidade razoavelmente comum no Internet. Contudo, desde que os pontos finais de VPN não estão usando o protocolo de TCP (aviso que estão usando o cTCP), os valores-limite continuarão a transmitir e a conexão continuará.

Nesta encenação, um problema ocorre se há um outro dispositivo tal como um Firewall que segue a conexão de TCP statefully. Desde que o protocolo do cTCP não executa inteiramente um cliente TCP e o server ACK duplicados não recebe uma resposta, este pode fazer com que os outros dispositivos na linha deste córrego da rede deixem cair o tráfego TCP. A perda de pacotes deve ocorrer na rede que faz com que os segmentos TCP vão faltar, que provoca o problema.

Este é um não erro, mas um efeito secundário da perda de pacotes na rede e do fato de que o cTCP não é um TCP real. O cTCP tenta emular o protocolo de TCP envolvendo os pacotes de IPsec dentro de um cabeçalho de TCP, mas aquela é a extensão do protocolo.

Esta edição ocorre tipicamente quando os administradores de rede executam um ASA com um IPS, ou faz alguma meio inspeção de aplicativo no ASA que faz com que o Firewall atue como um proxy completo TCP da conexão. Se há uma perda de pacotes, o ASA ACK para os dados faltantes em nome do server ou do cliente do cTCP, mas o cliente VPN nunca responderá. Desde que o ASA nunca recebe os dados que está esperando, uma comunicação não pode continuar. Em consequência, a conexão falha.

Solução

A fim resolver este problema, execute qualqueras um ações:

- Comute do IPsec sobre o TCP ao IPsec sobre o UDP, ou do encapsulamento nativo com o protocolo ESP.
- Comute ao cliente de AnyConnect para a terminação VPN, que usa uma pilha de protocolos inteiramente executada TCP.
- Configurar o ASA para aplicar o TCP-estado-desvio para estes fluxos específicos IPsec/TCP. Isto desabilita essencialmente todas as verificações de segurança para as conexões que combinam a política do TCP-estado-desvio, mas permitirá que as conexões trabalhem até que uma outra definição desta lista possa ser executada. Para mais informação, refira diretrizes e limitações do desvio do estado TCP.
- Identifique a fonte da perda de pacotes, e tome a ação corretiva a fim impedir que os pacotes IPsec/TCP deixem cair na rede. Isto é geralmente impossível ou extremamente difícil desde que o disparador à edição é geralmente perda de pacotes no Internet, e as gotas não podem ser impedidas.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems