# O IPsec sobre TCP falha quando o tráfego flui pelo ASA

## Contents



## Introduction

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

### Requirements

Para encontrar esse problema específico, os Cisco VPN Clients devem ser configurados para se conectar a um dispositivo de headend de VPN usando IPsec sobre TCP. Na maioria dos casos, os administradores de rede configuram o ASA para aceitar conexões do Cisco VPN Client na porta TCP 10000.

### Componentes Utilizados

As informações neste documento são baseadas no Cisco VPN Client.

### Conventions

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

## Problema

Quando o cliente VPN é configurado para IPsec sobre TCP (cTCP), o software cliente VPN não responderá se um TCP ACK duplicado for recebido solicitando que o cliente VPN retransmita dados. Uma ACK duplicada pode ser gerada se houver perda de pacotes entre o cliente VPN e o headend ASA. A perda intermitente de pacotes é uma realidade bastante comum na Internet. No entanto, como os terminais VPN não estão usando o protocolo TCP (lembre-se de que estão usando o cTCP), os terminais continuarão transmitindo e a conexão continuará.

Nesse cenário, um problema ocorre se houver outro dispositivo, como um firewall, rastreando a conexão TCP de forma estável. Como o protocolo cTCP não implementa totalmente um cliente TCP e ACKs duplicados de servidor não recebem uma resposta, isso pode fazer com que outros dispositivos em linha com esse fluxo de rede descartem o tráfego TCP. A perda de pacotes deve ocorrer na rede, causando a perda de segmentos TCP, o que desencadeia o problema.

Isso não é um bug, mas um efeito colateral da perda de pacotes na rede e do fato de que o cTCP não é um TCP real. O cTCP tenta emular o protocolo TCP empacotando os pacotes IPsec dentro de um cabeçalho TCP, mas essa é a extensão do protocolo.

Esse problema normalmente ocorre quando os administradores de rede implementam um ASA com um IPS ou fazem alguma inspeção de aplicativo no ASA que faz com que o firewall atue como um proxy TCP completo da conexão. Se houver perda de pacotes, o ASA irá ACK para os dados ausentes em nome do servidor ou cliente cTCP, mas o cliente VPN nunca responderá. Como o ASA nunca recebe os dados que espera, a comunicação não pode continuar. Como resultado, a conexão falha.

### Solução

Para resolver esse problema, execute qualquer uma destas ações:

- Mude de IPsec sobre TCP para IPsec sobre UDP ou encapsulamento nativo com o protocolo ESP.
- Mude para o cliente AnyConnect para terminação de VPN, que usa uma pilha de protocolo TCP totalmente implementada.
- Configure o ASA para aplicar o tcp-state-bypass para esses fluxos IPsec/TCP específicos. Isso desabilita essencialmente todas as verificações de segurança para as conexões que correspondem à política de desvio de estado do tcp, mas permitirá que as conexões funcionem até que outra resolução dessa lista possa ser implementada. Para obter mais informações, consulte Diretrizes e Limitações de Desvio de Estado de TCP.
- Identifique a origem da perda de pacotes e tome medidas corretivas para evitar que os pacotes IPsec/TCP sejam descartados na rede. Isso geralmente é impossível ou extremamente difícil, pois o desencadeador do problema é geralmente a perda de pacotes na Internet, e as quedas não podem ser evitadas.

## Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems