IPsec over TCP Fails when Traffic Flows through ASA

Contents

Introduction

Cisco VPN Clients that connect to a VPN headend using IPsec over TCP might connect to the headend fine, but then the connection fails after some time. This document describes how to switch to IPsec over UDP or native ESP IPsec encapsulation in order to resolve the issue.

Before You Begin

Requirements

In order to encounter this specific problem, Cisco VPN Clients must be configured to connect to a VPN headend device using IPsec over TCP. In most instances, network administrators configure the ASA to accept Cisco VPN Client connections over TCP Port 10000.

Components Used

The information in this document is based on Cisco VPN Client.

Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

Problem

When the VPN client is configured for IPsec over TCP (cTCP), the VPN client software will not respond if a duplicate TCP ACK is received asking for the VPN client to re-transmit data. A duplicate ACK might be generated if there is packet loss somewhere between the VPN client and

the ASA headend. Intermittent packet loss is a fairly common reality on the Internet. However, since the VPN endpoints are not using the TCP protocol (recall that they are using cTCP), the endpoints will continue transmitting and the connection will continue.

In this scenario, a problem occurs if there is another device such as a firewall tracking the TCP connection statefully. Since the cTCP protocol does not fully implement a TCP client and server duplicate ACKs do not receive a response, this can cause other devices in-line with this network stream to drop the TCP traffic. Packet loss must occur on the network causing TCP segments to go missing, which triggers the problem.

This is not a bug, but a side effect of both packet loss on the network and the fact that cTCP is not a real TCP. The cTCP tries to emulate the TCP protocol by wrapping the IPsec packets within a TCP header, but that is the extent of the protocol.

This issue typically occurs when network administrators implement an ASA with an IPS, or do some sort of application inspection on the ASA that causes the firewall to act as a full TCP proxy of the connection. If there is packet loss, the ASA will ACK for the missing data on behalf of the cTCP server or client, but the VPN client will never respond. Since the ASA never receives the data it is expecting, communication cannot continue. As a result, the connection fails.

Solution

In order to resolve this problem, perform any of these actions:

- Switch from IPsec over TCP to IPsec over UDP, or native encapsulation with the ESP protocol.
- Switch to the AnyConnect client for VPN termination, which uses a fully implemented TCP protocol stack.
- Configure the ASA to apply tcp-state-bypass for these specific IPsec/TCP flows. This essentially disables all security checks for the connections that match the tcp-state-bypass policy, but will allow the connections to work until another resolution from this list can be implemented. For more information, refer to TCP State Bypass Guidelines and Limitations.
- Identify the source of the packet loss, and take corrective action in order to prevent the IPsec/TCP packets from dropping on the network. This is usually impossible or extremely difficult since the trigger to the issue is usually packet loss on the Internet, and the drops cannot be prevented.

Related Information

- **Technical Support & Documentation - Cisco Systems**