ASA を経由してトラフィックが流れているときに IPSec over TCP が失敗する

内容

概要

IPSec over TCP を使用して VPN ヘッドエンドに接続する Cisco VPN Client は、ヘッドエンドに正常に接続する可能性がありますが、しばらくすると接続が失敗します。このドキュメントでは、問題を解決するために IPSec over UDP またはネイティブ ESP IPSec カプセル化に切り替える方法について説明します。

はじめに

要件

この問題の発生を確認するには、IPSec over TCP を使用して VPN ヘッドエンド デバイスへ接続するよう Cisco VPN Client を設定する必要があります。ほとんどの場合、ネットワーク管理者は TCP ポート 10000 において Cisco VPN Client の接続を受け入れるよう ASA を設定します。

使用するコンポーネント

このドキュメントの情報は、Cisco VPN Client に基づくものです。

表記法

ドキュメントの表記法の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

問題

VPN クライアントが IPSec over TCP（cTCP）用に設定されている場合、VPN クライアントが

データを再送信するよう要求する重複 TCP ACK を受け取っても、VPN クライアント ソフトウェアは応答しません。VPN クライアントと ASA ヘッドエンド間のどこかでパケット損失がある場合、重複 ACK が生成されることがあります。断続的なパケット損失は、インターネットでよく見られる現象です。ただし、VPN エンドポイントは TCP プロトコルを使用していない（cTCP を使用している）ため、エンドポイントは送信を続行し、接続が継続します。

このシナリオでは、TCP 接続をステートフルに追跡するファイアウォールなどの別のデバイスが存在する場合に、問題が発生します。cTCP プロトコルは TCP クライアントを完全に実装していないこと、およびサーバの重複 ACK は応答を受信しないことが原因となって、同じネットワーク ストリームにつながっている他のデバイスが TCP トラフィックをドロップしてしまうことがあります。TCP セグメントの行先が不明になるネットワークではパケット損失が発生する可能性が高く、これによりこの問題が引き起こされます。

これはバグではありませんが、ネットワーク上でパケット損失が発生していること、および cTCP は本当の TCP ではないということの両方による二次的な影響です。cTCP は IPSec パケットを TCP ヘッダー内にラッピングすることにより TCP プロトコルをエミュレートしようとしますが、これはプロトコルの範囲です。

この問題は通常、ネットワーク管理者が IPS を備えた ASA を実装する場合、または ASA 上で何らかのアプリケーション検査を行うためファイアウォールが接続の完全な TCP プロキシとして機能する場合に、発生します。パケット損失があると、ASA は cTCP サーバまたはクライアントに代わり不明データに対して ACK 応答をしますが、VPN クライアントは応答しません。ASA は想定されているデータを受け取らないため、通信を続けることができません。その結果、接続が失敗します。

解決方法

この問題を解決するには、次のいずれかのアクションを実行します。

- IPSec over TCP から IPSec over UDP へ切り替える。これは ESP プロトコルを使用したネイティブなカプセル化です。
- VPN 終端用の AnyConnect クライアントに切り替える。これは完全に実装された TCP プロトコル スタックを使用しています。
- これらの特定の IPSec/TCP フローに対して TCP 状態バイパスを適用できるように ASA を設定する。これは基本的に、このリストの別の解決策が実装できるようになるまで、TCP 状態バイパス ポリシーと一致する接続に対してすべてのセキュリティ チェックを無効にしますが、接続の機能を許可することになります。詳細については、『TCP ステート バイパスのガイドラインと制限事項』を参照してください。
- パケット損失の原因を特定し、IPSec/TCP パケットがネットワークからドロップしないように是正措置を実行する。多くの場合、この問題はインターネット上のパケット損失によりトリガーされるため、この是正措置を実行することは一般的に不可能であるか、または非常に困難であり、ドロップを回避することはできません。

関連情報

- テクニカル サポートとドキュメント – Cisco Systems