

ESNネゴシエーションによるVersa Networks RouterとのセキュアアクセスIPSecトンネル接続の問題

内容

お問い合わせ内容

Versa-Network Routerをエッジデバイスとして使用するブランチオフィスでのCisco Secure Accessの導入時に、両方のIPSecトンネルが動作可能に見えたにもかかわらず、接続の問題が発生しました。

具体的な症状は次のとおりです。

- ブランチからCisco Secure Accessへの接続がない
- スタティックルート経由のインターネットアクセスが機能しない
- 監視された単方向暗号化トラフィック（セキュアアクセスへの発信のみ）
- 送信パケットは送信されているが、受信パケットがないことを示すルータ統計情報
- SD-WANルータとSecure Accessの間で双方向に機能するデッドピア検出
- 発信トラフィックを正しく照合するためのセキュリティパラメータインデックス(SPI)値
- トンネルフラッピング（リセット）では、接続の問題は解決されませんでした
- パケットキャプチャとスクリーンショットにより、着信トラフィックがないことを確認
- トンネル暗号をCBCからGCMに変更しても、問題は解決しなかった

調査の結果、チェックサムエラーが原因でCisco側でのトラフィックの復号化に失敗したことが判明しました。これは、VersaルータがESN（拡張シーケンス番号）機能をネゴシエートしたためです。

環境

- シスコセキュアアクセスの導入
- エッジデバイスとしてのVersa-Networksルータ
- IP-IPトンネルの設定
- CBCとGCMの両方の暗号試行を使用したIPsecトンネル設定

解決策

この問題を解決するには、Versaルータで拡張シーケンス番号(ESN)ネゴシエーションを無効にして、Cisco Secure Accessヘッドエンドで復号化障害を引き起こしていたチェックサムエラーを防止する必要がありました。

問題解決の手順

ステップ1：根本原因の特定

調査の結果、VersaルータがESN（拡張シーケンス番号）をネゴシエートしていることが判明しました。これにより、Cisco Secure Accessヘッドエンドはチェックサムエラーを受信し、ESN構築パケットの復号化に失敗しました。

手順2:VersaルータのESNを無効にする

Versa Networksサポートまたはルータ管理者に連絡して、Versaルータ設定のESNチェックとネゴシエーションを無効にしてください。これにより、ESNが不適切にネゴシエートされる原因となる、既知のVersaの不具合が解決されます。

ステップ3：接続の確認

ESNネゴシエーションを無効にした後、双方向トラフィックフローが確立され、ブランチからセキユアアクセスおよびインターネットへの完全な接続が復元されたことを確認します。

ステップ4：トラフィックフローのモニタ

ルータの着信パケットと発信パケットの両方の統計情報が、両方向で適切なトラフィックフローを示していることを確認し、単方向トラフィックの問題が正常に解決されたことを確認します。

原因

根本原因は、既知のVersa Networksのバグ (Versa support bug ID:122437 - ESNはVOSによってネゴシエートされない) として特定されており、このバグでは、IPSecトンネルの確立中にVersaルータが拡張シーケンス番号(ESN)機能を誤ってネゴシエートします。このESNネゴシエーションにより、Cisco Secure Accessヘッドエンドはチェックサムエラーのあるパケットを受信するようになり、適切な復号化が妨げられ、結果として単方向トラフィックフローが発生します。Versaルータは発信パケットを正常に送信しますが、ESN関連の復号化の失敗が原因でリターントラフィックを適切に処理できません。

関連コンテンツ

- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。