

IKEキー再生成イベント中にSecure Access NetworkトンネルグループがAzure VPN Gatewayで断続的にフラッシングする

内容

お問い合わせ内容

Cisco Secure AccessとAzure VPN Gatewayの間に新しく設定されたネットワークトンネルグループで、IKEキー再生成イベント中に約4時間ごとに断続的なトンネルフラッシングが発生します。

次のような特定のエラーメッセージと症状が見られます。

- BGPピアリングがダウンし、ホールドタイマーが切れました
- アラート：失敗したIKEキー再生成
- IKEトンネル切断

トンネルフラッシングは、定期的な中断、IKEキー再生成の失敗、整合性チェックの失敗、トンネルの切断、およびBGPピアリングドロップを引き起こし、Azureリソースへの安定した接続に影響を与えます。キー再生成ネゴシエーション中に認証エラーが発生します。

環境

- Azure VPN Gatewayに構成されたCisco Secure Access (CSA)ネットワークトンネルグループ
- IKEv2を使用したIPsecサイト間VPNトンネル
- メインモード(MM)ポリシーで構成されたAES-GCM-256暗号化を使用するAzure VPNゲートウェイ

- ポート4500を使用して両側でNAT-T (NATトラバーサル) が有効
- エンドポイント間に設定されたBGPピアリング
- デフォルトのIKE SAライフタイム4時間 (28800秒)
- 初期IPSec SAライフタイム設定、後で10800秒に変更
- Azure側でPFS (Perfect Forward Secrecy)が有効になっていません

解決策

この問題は、Azure VPN GatewayのバグIDに基づき、メインモードポリシーでAES-GCM暗号化を回避するように構成を変更することで解決されました。

手順1: Azure VPN Gatewayデバッグ分析

IKEデバッグがAzure VPN Gateway側から収集され、キー再生成の試行中に次の動作が表示されました：

```
SESSION_ID : {} Remote x.x.x.x:500: Local x.x.x.x:500: [SEND]Sending IPSec policy Payload for tunnel Id  
SESSION_ID : {} Remote x.x.x.x:4500: Local x.x.x.x:4500: [SEND][CHILD_SA MM_REKEY] Sending IKE rekey res  
SESSION_ID : {} Remote x.x.x.x:4500: Local x.x.x.x:4500: [LOCAL_MSG] IKE Tunnel closed for tunnelId x3 w
```

ステップ2：根本原因の特定

Azureサポートがキー再生成エラーを調査しました。Azure分析で、AzureがAES-GCM-256を使用してMM-REKEYを開始すると、キー再生成パケットの形式が正しくないことが確認されました。オンプレミスデバイスが不正なキー再生成要求に応答しないため、トンネルが切断されます。

ステップ3：設定の回避策の実装

Azureの推奨事項に基づいて、この軽減措置が実装されました：

- Network Tunnel Group設定のメインモード(MM)ポリシーからAES-GCM暗号を削除します。
- GCMモードを使用しない代替暗号化方式を設定します。

<https://securitydocs.cisco.com/docs/csa/olh/121327.dita>のステップ17を参照してください。

ステップ4：別の軽減策オプション

また、Azureは以下の緩和策も提供しました。

- オンプレミスのMMの有効期間を28800秒より長く構成して、Azureが常にキー再生成を開始するようにします。
- オンプレミスのSAの有効期間がAzureの有効期間より短い場合、Azure VPN Gatewayを応答側専用モードに設定します。

原因

根本原因は、AES-GCMキー再生成操作に影響を与えるAzure VPN Gatewayのバグです。AzureがAES-GCM-256を使用してMM-REKEYを開始すると、キー再生成パケットの形式が正しくないため、オンプレミスのCisco Secure Accessデバイスが正しくない形式のキー再生成要求に応答しなくなります。その結果、IKEキー再生成の失敗、認証エラー、および後続のトンネル切断が発生します。

Azureは、これを既存のバグとして確認し、2026年半ばを目標とした将来のゲートウェイリリースで予定されている修正を文書化しました。

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。