AnyConnect VPNセッション中のポート53での過剰なDNS要求

内容

お問い合わせ内容

リモートアクセスVPN(RA-VPN)を実装すると、Cisco AnyConnectを介して接続しているユーザは、セカンダリDNSサーバに対する多数のDNS要求をポート53で生成します。この動作は、VPNトンネルに接続されたすべてのユーザのActivity Monitorで確認され、トンネルで多数の許可された要求がフラッディングされます。ユーザがゼロトラストアクセス(ZTA)経由で接続する場合、この過剰なDNSアクティビティは発生せず、問題がAnyConnect VPNの接続方法に特に関連していることを示します。

環境

- 製品ファミリ：セキュアなアクセス
- 実装：リモートアクセスVPNの導入
- 比較環境：ゼロトラストアクセス(ZTA) – 同じDNSフラッディング動作が発生しない

解決策

過剰なDNS要求を調査するには、ログの収集と分析を行って、DNSフラッディング動作の根本原因を特定する必要があります。ログ収集には、各パケットのPIDを含むパケットキャプチャの収集が含まれ、エンドポイント上のどのアプリケーションがトラフィックを生成しているかを判別し、Process Monitorの出力を生成します。

原因

分析によれば、この量のDNSトラフィックが予想されます。

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。