Wiresharkによるネットワークトラフィックのキャプチャと分析による診断

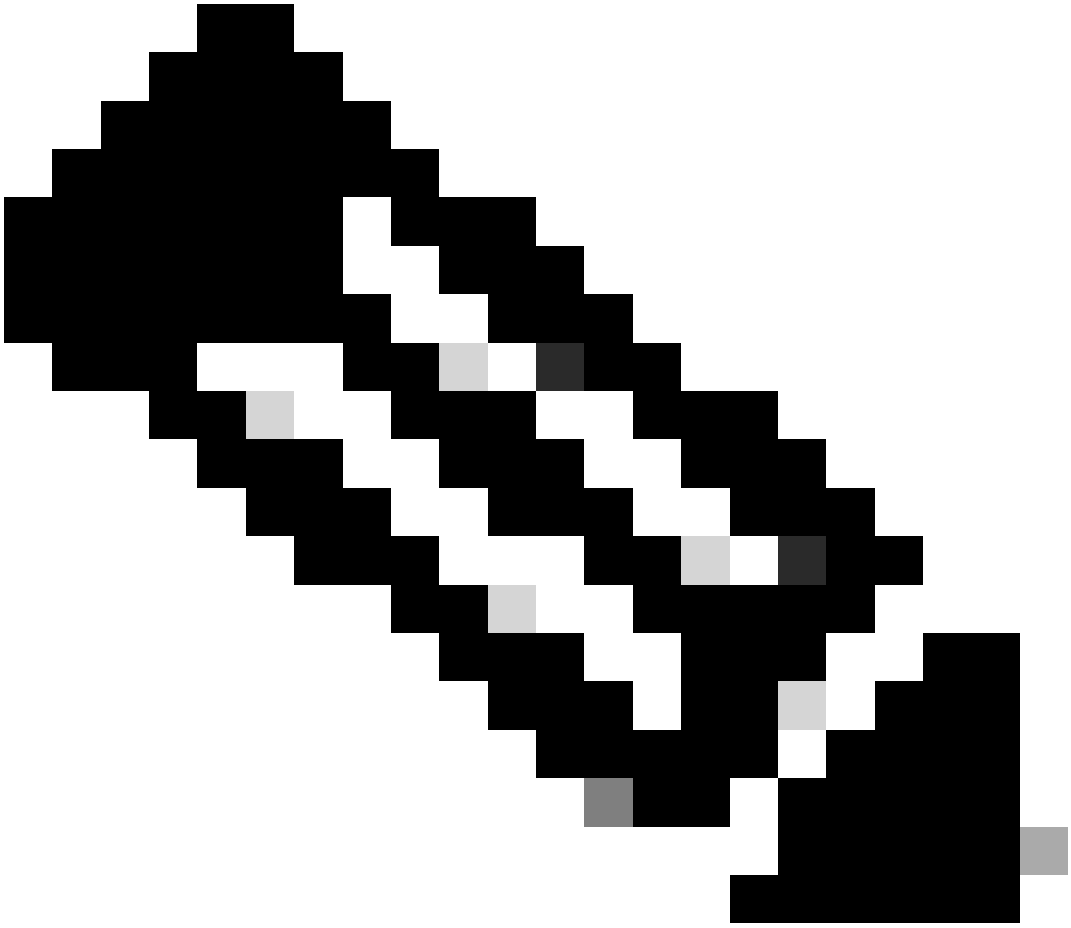
内容

はじめに

このドキュメントでは、Wiresharkを使用してネットワークトラフィックを検出および分析し、診断を行う方法について説明します。

概要

Wiresharkは、パケットキャプチャ（「TCPダンプ」とも呼ばれる）の読み取りと分析に使用できる無料のアプリケーションです。 パケットキャプチャは、ネットワークアダプタを介したすべての通信をパケットレベルで明らかにし、DNS、HTTP、ping、およびその他のトラフィックタイプを表示できるようにします。パケットキャプチャは、詳細なトラブルシューティングの診断ステップとして特に有用であり、SIGの導入により、診断プロセスの基本的な部分となっています。



注:Wiresharkは選択されたアダプタのすべてのトラフィックをキャプチャします。パケットキャプチャには個人を特定できる情報(PII)が含まれていることが多いため、必ずBoxリンクなどの安全な方法を使用して、キャプチャファイルをサポートと共有してください。

Wiresharkの入手

Windows、macOS、またはLinux用のWiresharkは、https://www.wireshark.org/からダウンロードできます。

パケットキャプチャの収集

1. インターネットに接続されているネットワークアダプタを選択し、Wiresharkでキャプチャを開始します。
2. キャプチャ中に、診断したい問題を再現します。

3. 終了したらキャプチャを停止し、ファイルを.pcapとして保存します。

基本的なポートとプロトコル

- ほとんどのパケットは、トランスポート層プロトコルTCPまたはUDPで通信します
  - たとえば、「DNS」はデフォルトでUDPの「上」で実行されます。TCPに障害が発生するとUDPに切り替わる
- HTTPとDNSは、トランスポートプロトコル+ポートの組み合わせで動作する一般的なプロトコルです。

トランスポート層プロトコル	ポート	プロトコル名	用途
TCP	22	SSH	リモートVAアクセス
TCP	25	SMTP	VAモニタリング
IP	50	ESP(Encapsulating Security Payload)	機密性、データ整合性、原点認証
IP	51	AH（認証ヘッダー）	データ整合性、オリジン認証
UDP	53	DNS	DNSのデフォルト
TCP	53	DNS	DNSフェールオーバー
TCP	80	HTTP	Webトラフィック（非暗号化）、API
UDP	123	NTP	VA時間同期
TCP	443	HTTPS	暗号化されたWebトラフィック、API、VAへのADコネクタ
UDP	443	HTTPS	RC暗号化DNSクエリ
UDP	500	IKE	IPSecトンネルネゴシエーション
UDP	4500	NAT-T	IPSecトンネルのNATトラバーサル
TCP	8080	HTTP	VA通信へのADコネクタ

プロトコル名、ポート、およびその使用方法を知っておくと、Wiresharkで関連するトラフィックを特定して分析するのに役立ちます。

基本演算子

Wiresharkでフィルタ文字列を作成する場合は、次の演算子を使用します。

- `==`: Equals (例：`ip.dst==1.2.3.4`)
- `!=`：等しくない(例：`ip.dst!=1.2.3.4`)
- `&&`：および(例：`ip.dst==1.2.3.4 && ip.src==208.67.222.222`)
- `||`：または(例：`ip.dst==1.2.3.4 || ip.dst==1.2.3.5`)

高度なフィルタオプションについては、Wiresharkのドキュメントを参照してください(6.4)。表示フィルタ式の作成

フィルタ

パケットキャプチャには数千のパケットを含めることができます。フィルタを使用すると、特定のトラフィックタイプに重点を置くことができます。

- プロトコル別：
  - `dns`— DNSトラフィックのみを表示
  - `http || dns`— HTTPまたはDNSトラフィックを表示します。
- IPアドレス：
  - `ip.addr==<IP>:<IP>`との間のすべてのトラフィック
  - `ip.src==<IP>:<IP>`からのすべてのトラフィック
  - `ip.dst==<IP>:<IP>`へのすべてのトラフィック
- その他:
  - `tcp.flags.reset==1`— TCPリセット（タイムアウト）のチェック
  - `dns.qry.name contains "[domain]"`：ドメインに一致するDNSクエリ
  - `tcp.port==80 || udp.port==80`：ポート80のTCPまたはUDPトラフィック

パケットの表示と分析

パケットを見つけたら、Wireshark内のセグメントを展開して詳細を分析します。プロトコル構造に精通していると、これらの詳細を解釈し、必要に応じてデータを再構築することもできます。

データストリームの追跡

パケットリストを使用して、要求と応答のペアを検索します。パケットを右クリックし、Follow > TCP Stream、UDP Stream、TLS Stream、またはHTTP Streamを選択して、関連する要求と応答のシーケンスを表示します。

- これは、単一要求プロトコル（DNSなど）よりも、複数の交換（HTTPなど）を含むプロトコルの方が便利です。

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。