Umbrellaの非ブラウザアプリケーションのトラブルシューティング

内容

はじめに

このドキュメントでは、Cisco Umbrellaの非ブラウザアプリケーションをトラブルシューティングする方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco Umbrellaに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

この記事では、UmbrellaセキュアWebゲートウェイで機能するように非ブラウザアプリケーションを設定するためのベストプラクティスとトラブルシューティングの手順について説明します。

ほとんどの場合、設定の変更は必要ありません。ただし、特定のアプリケーションはセキュリティ/インスペクション機能（SSL復号化など）と正常に連携しないため、Webプロキシでアプリケーション機能を実現するには例外を追加する必要があります。これは、Umbrella SWGおよびその他のWebプロキシソリューションに適用されます。

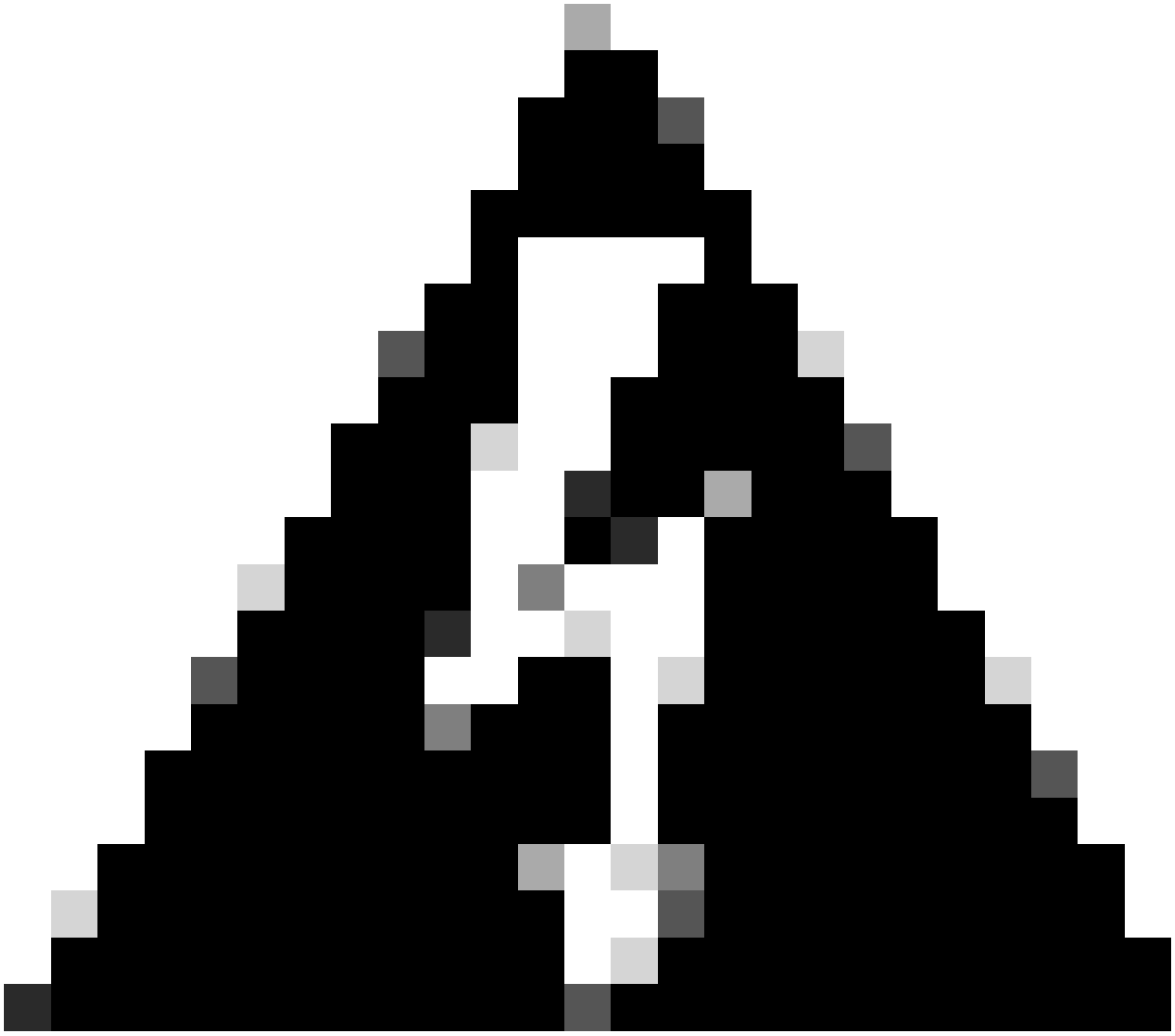
これは、アプリケーションのWebサイト/ブラウザバージョンは機能するが、アプリケーションのデスクトップ/モバイルバージョンは機能しない状況で役立ちます。

互換性の問題

次の理由により、アプリケーションに互換性がない可能性があります。

包括ルートCAのインストール	Cisco UmbrellaルートCAは、エラーのないTLS接続に対して常に信頼されている必要があります。 • 解決策：非Webアプリケーションの場合、Cisco UmbrellaルートCAがシステム/ローカルマシン証明書ストアで信頼されていることを確認します。
証明書ピニング	証明書ピニング(PKP)は、TLSハンドシェイクを検証するために、アプリケーションが正確なリーフ（またはCA証明書）の受信を期待する場合に使用します。 アプリケーションは、Webプロキシによって生成された証明書を受け入れることができません。また、SSL暗号化解除機能と互換性がありません。 • 解決策:選択的復号化リスト(表の後の警告を参照)を使用して、SSL復号化からアプリケーションまたはドメインをバイパスします。 証明書ピニングの影響を受けることが判明しているアプリケーションの詳細については、「公開キーピニング/証明書ピニング」を参照してください。
TLSバージョンのサポート	アプリケーションは、セキュリティ上の理由からSWGでサポートされていない古いTLSバージョン/暗号を使用できます。 • 解決策:外部ドメイン機能(PAC/AnyConnect)またはVPN除外（トンネル）を使用して、Umbrellaにトラフィックが送信されないようにします(表の後の警告を参照)。
非Webプロトコル	一部のアプリケーションは非http(s)プロトコルを使用しますが、SWGによって代行受信される一般的なWebポートを介してこのデータを送信します。SWGはこのトラフィックを理解できません。 • 解決策：ソフトウェアが使用する宛先アドレスまたはIP範囲を判断するには、アプリケーションベンダーに問い合わせてください。 このソフトウェアは、外部ドメイン(PAC/AnyConnect)またはVPN除外（トンネル）を使用してSWGから除外する必要があります(表の後の警告を参照)。

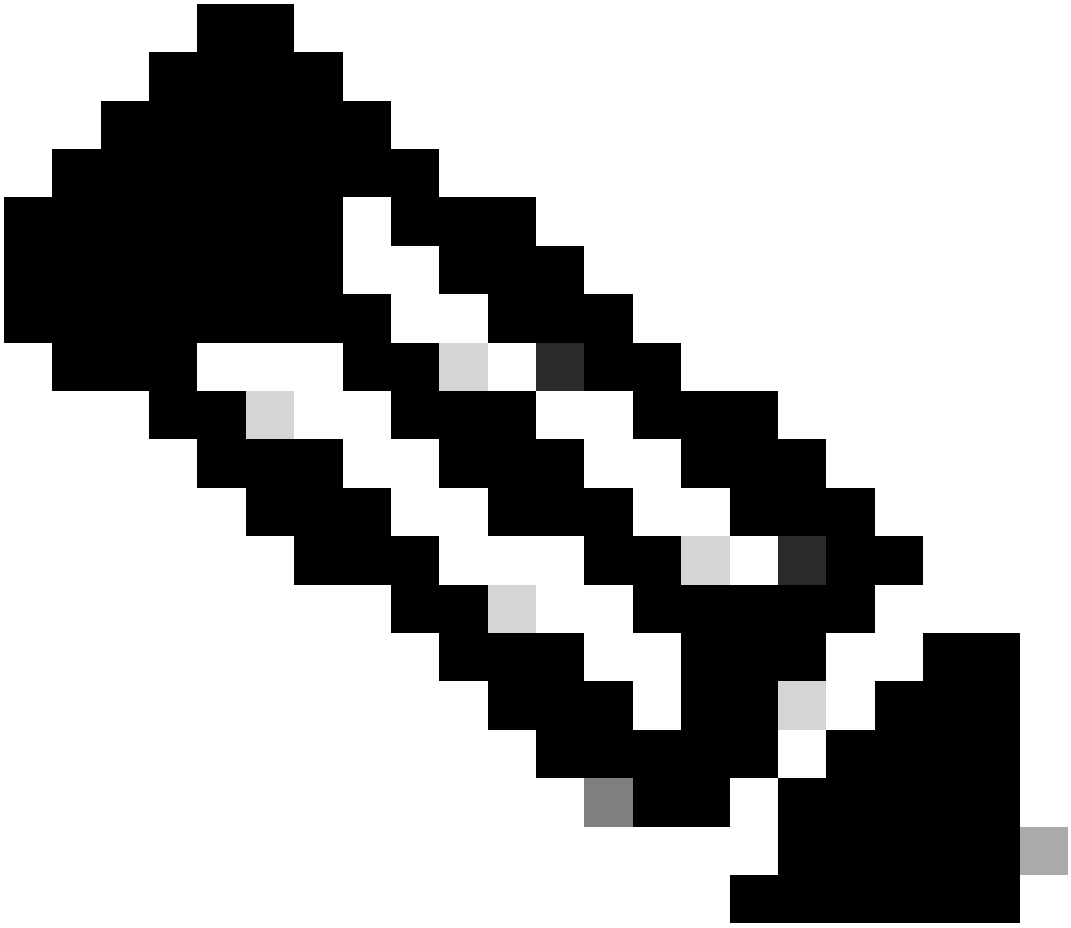
SAML認証	ブラウザ以外のほとんどのアプリケーションは、SAML認証を実行できません。UmbrellaはSAMLの非ブラウザアプリケーションをチャレンジしないため、ユーザ/グループベースのフィルタリングポリシーは一致しません。 • 解決策：非ブラウザアプリケーションで使用するためにユーザ情報をキャッシュできるように、IPサロゲート機能を有効にします。 • 代替: (ユーザやグループではなく) ネットワークまたはトンネルのIDに基づくWebルールでアプリケーションやドメインを許可します。
HTTP範囲要求	一部のアプリケーションでは、データのダウンロード時にHTTPの「バイト範囲」要求を使用します。つまり、一度にダウンロードされるのはファイルの小さなチャンクだけです。これらの要求は、SWGのセキュリティ上の理由により無効にされています。この手法は、アンチウイルス検出のバイパスにも使用できるためです。 • ソリューション(HTTPS):選択的な復号化リストを使用して、包括的なSSL復号化*からアプリケーションまたはドメインをバイパスします。 • 解決策(HTTP)：アンチウイルススキャン*でアプリケーションまたはドメインをバイパスし、WebルールとOverride Securityオプションを使用します。 • 代替：組織で範囲要求をデフォルト*で有効にする場合は、Umbrellaサポートに連絡してください。
明示的なプロキシの互換性	一部のアプリケーションはシステムプロキシ設定 (PACファイルなど) を尊重せず、通常は明示的なWebプロキシと互換性がありません。これらのアプリケーションは、PACファイルの導入ではUmbrella SWGを介してルーティングされません。 • 解決策：アプリケーションは、ローカルネットワークファイアウォール経由で許可されている必要があります。 許可する宛先/ポートの詳細については、アプリケーションベンダーに問い合わせてください。



警告：これらの例外を作成すると、アンチウイルススキャン、DLPスキャン、テナント制御、ファイルタイプ制御、URLインスペクションなどのセキュリティ検査機能が無効になる可能性があります。 これらのファイルのソースを信頼できる場合にのみ、これを行ってください。アプリケーションに対するビジネスニーズを、これらの機能を無効にした場合のセキュリティへの影響と比較検討する必要があります。

Microsoft 365アプリケーション

Microsoft 365互換機能により、SSL復号化およびポリシー適用機能から多数のMicrosoftドメインが自動的に除外されます。この機能を有効にすると、デスクトップバージョンのMicrosoftアプリケーションの問題を解決できます。 詳細については、「グローバル設定の管理」を参照してください。

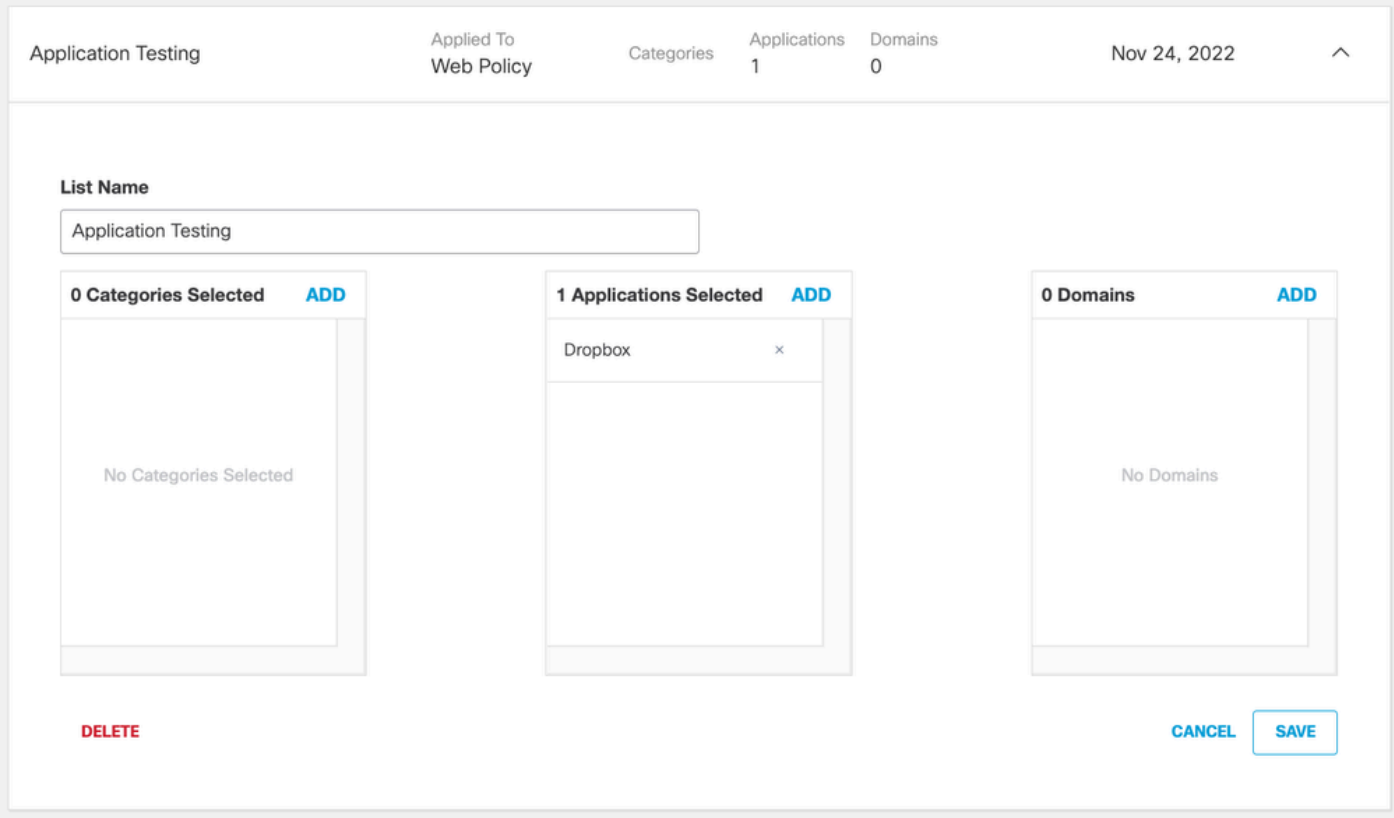


注:Microsoft 365互換性機能では、すべてのMicrosoftドメインが除外されるわけではありません。 Umbrellaは、フィルタリングから除外する必要があるドメインのリストに関するMicrosoftの推奨事項を使用します。詳細については、「新しいOffice 365エンドポイントカテゴリ」を参照してください。

証明書ピニングバイパス

証明書ピニング(PKP)は、アプリケーションの互換性の問題の一般的な原因です。 シスコでは、回避策としてSSL復号化をバイパスするように設定できる、名前付きアプリケーションの包括的なリストを提供しています。選択的復号化は、Policies > Selective Decryption Listsで設定できます。

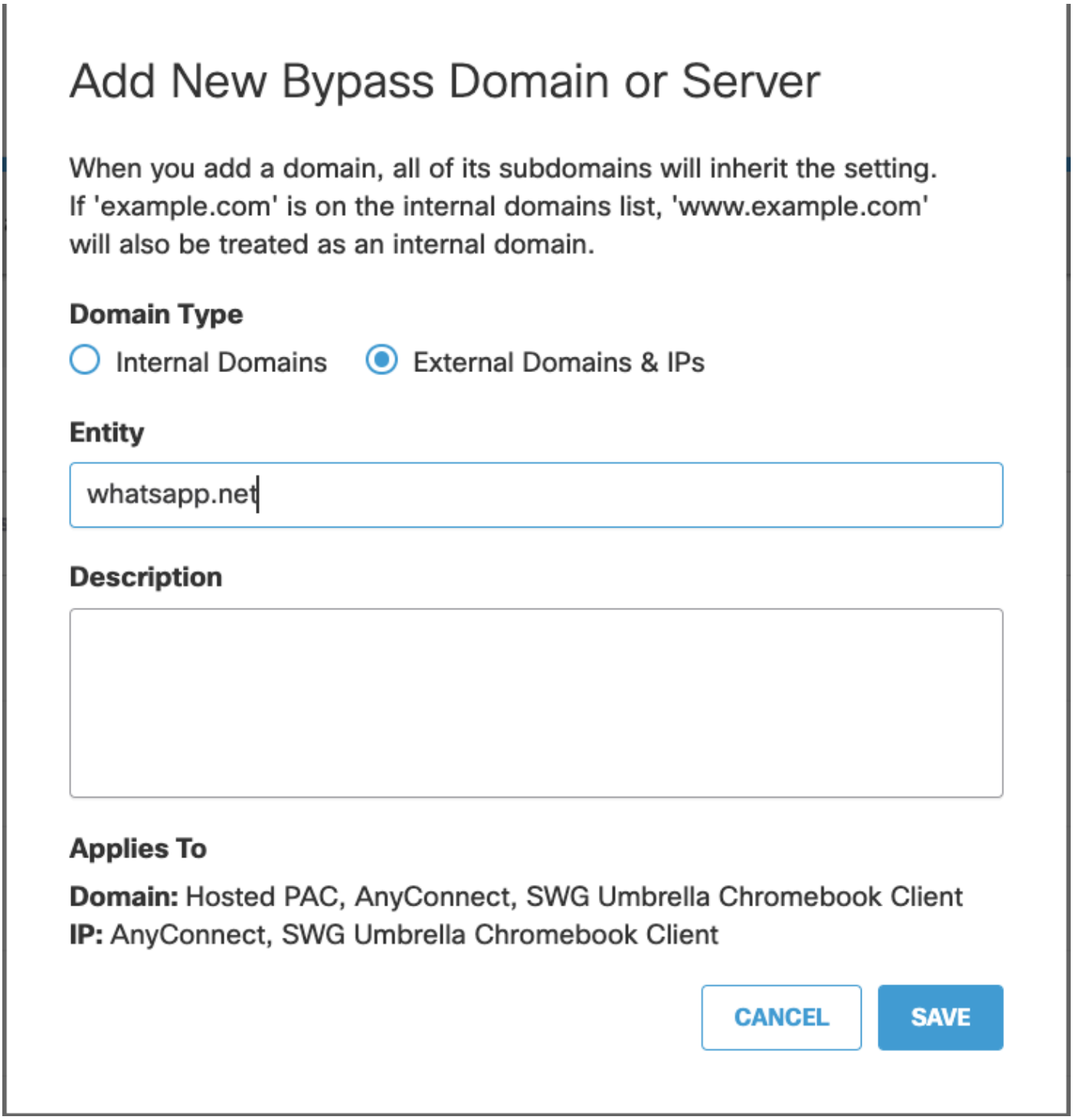
ほとんどの場合、管理者は名前でアプリケーションを除外するだけで、証明書のピニングの問題を解決できます。これは、ドメインのリストを学習または維持しなくても、これらの問題を解決できることを意味します。



または、宛先ドメイン/IPアドレスに基づいてアプリケーションをバイパスすることもできます。アプリケーションベンダーに問い合わせて、ドメイン/IPの該当するリストを確認するか、「証明書のピン留めの除外の識別」を参照してください。

TLS互換性バイパス

レガシーまたはカスタムのTLSバージョンは、アプリケーションの互換性の問題の一般的な原因です。これらの問題は、Deployments > Domain Management > External Domains & IPsでUmbrellaからのトラフィックを除外することで解決できます。 トンネル展開では、VPN設定に例外を追加することによってのみ、トラフィックを除外できます。



アプリケーションベンダーに問い合わせて、除外するドメイン/IPの該当リストを確認するか、「互換性のないTLSバージョンの除外の特定」（この記事の後半）を参照してください。

トラブルシューティング（上級）

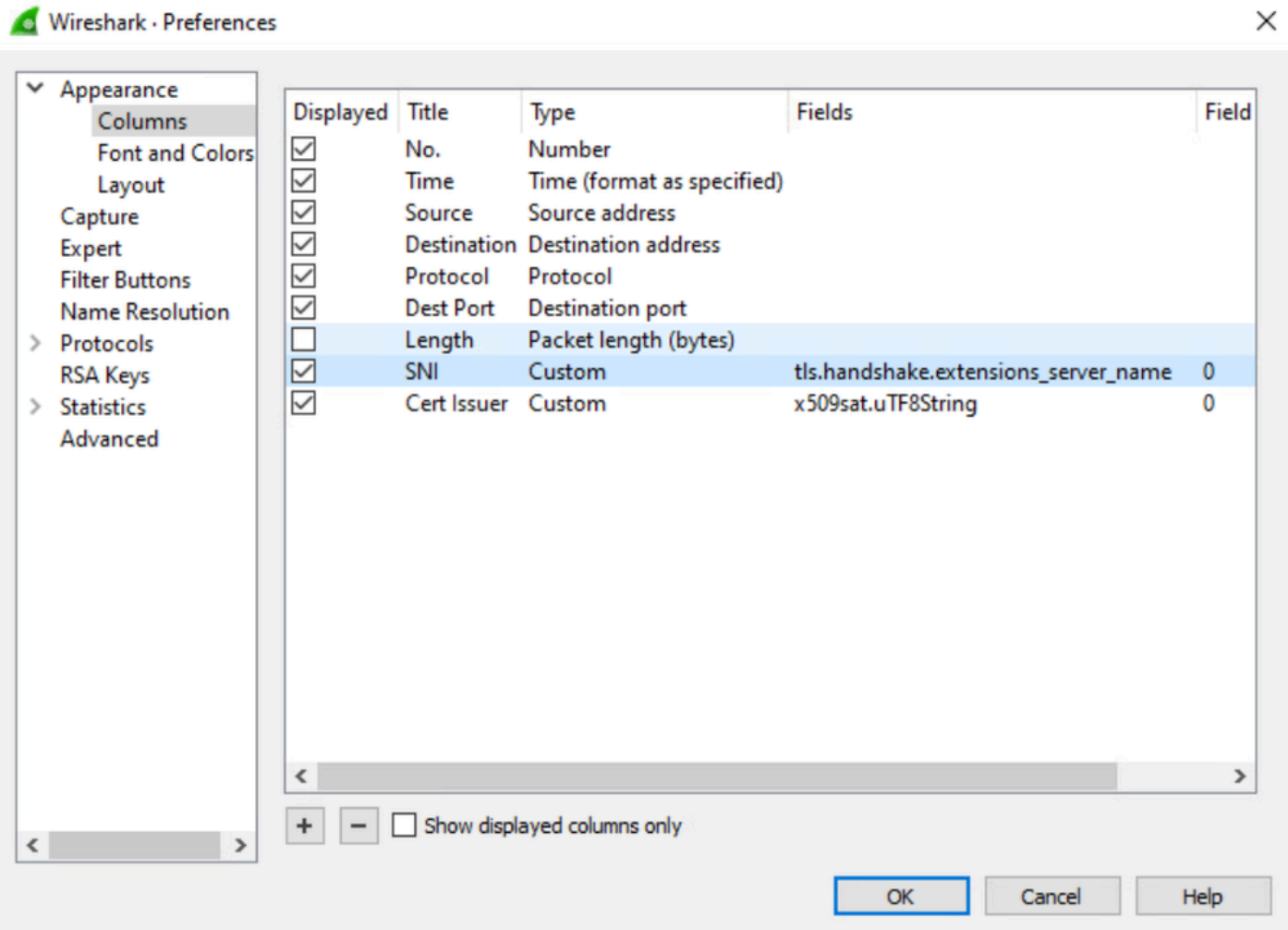
この記事の残りの手順では、トラブルシューティングの目的でWireshark(www.wireshark.org)のパケットキャプチャを使用します。Wiresharkは、カスタム除外の実装に役立つように、アプリケーションによって使用されるドメインを特定するのに役立ちます。開始する前に、Wiresharkで次のカスタム列を追加します。

1. www.wireshark.orgからWiresharkをダウンロードします。

2. Edit > Preferences > Columnsの順に移動します。

3. 次のフィールドを使用して、タイプがCustomの列を作成します。

```
http.host
tls.handshake.extensions_server_name
x509sat.uTF8String
```



パケットキャプチャを実行するには、次の手順を実行するか、「Wiresharkによるネットワークトラフィックのキャプチャ」を参照してください。

1. 管理者としてWiresharkを実行します。

2. [キャプチャ] > [オプション]で、関連するネットワークインターフェイスを選択します。

- PAC/トンネル導入の場合は、通常のLANネットワークインターフェイスでキャプチャします。
- AnyConnectの導入では、LANネットワークインターフェイスとループバックインターフェイスでキャプチャします。

3. 問題のあるアプリケーション以外のアプリケーションをすべて終了します。

4. DNSキャッシュをフラッシュします：`ipconfig /flushdns`

5. Wiresharkのキャプチャを開始します。

6. 問題を迅速に再現し、Wiresharkのキャプチャを停止します。

証明書ピニングの除外の識別

証明書のピニングはクライアントに適用されます。つまり、正確な動作と解決手順はアプリケーションごとに異なります。キャプチャ出力で、TLS接続が失敗していることを示す明白な兆候を探します。

- TLS接続がすばやく閉じられるか、リセットされる（RSTまたはFIN）。
- TLS接続が繰り返し再試行されています。
- TLS接続用の証明書がCisco Umbrellaによって発行されているため、復号化されます。

次のWiresharkフィルタの例は、TLS接続の重要な詳細を表示するのに役立ちます。

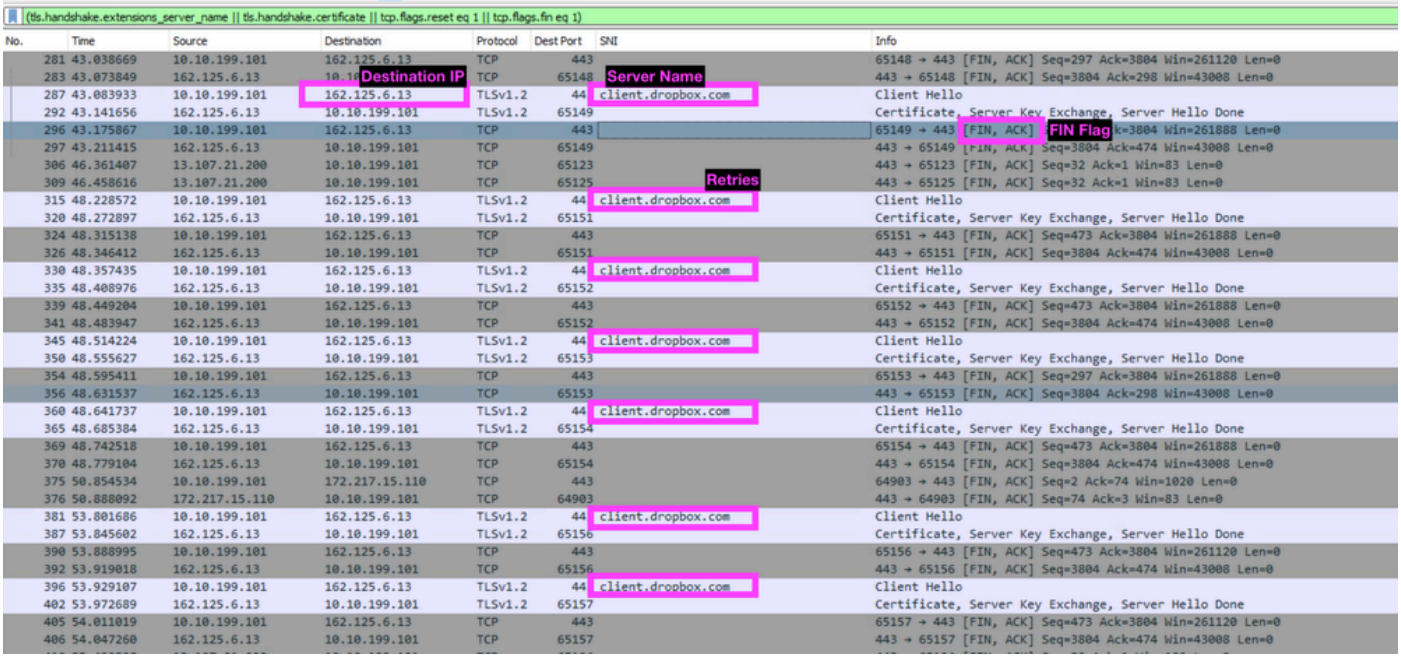
トンネル/接続

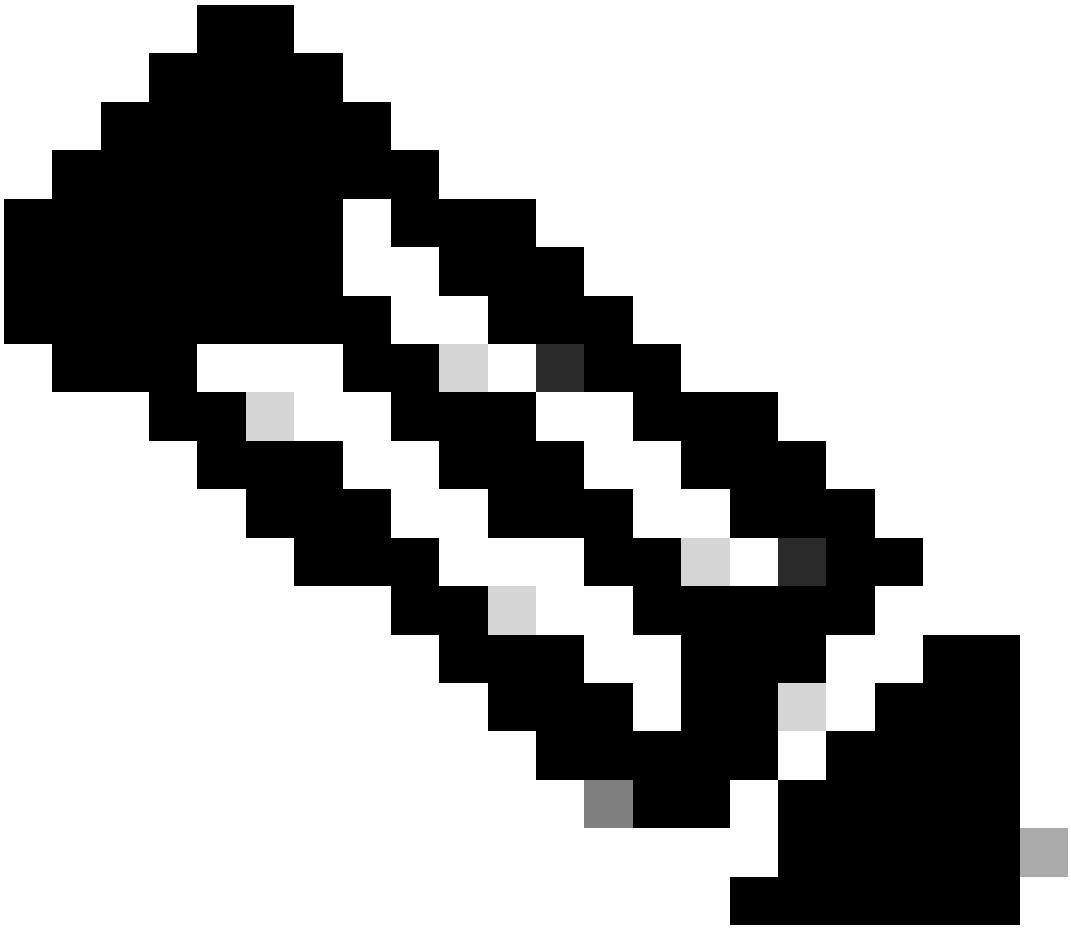
```
tcp.port eq 443 && (tls.handshake.extensions_server_name || tls.handshake.certificate || tcp.flags.rese
```

PAC/プロキシチェーン

```
tcp.port eq 443 && (http.request.method eq CONNECT || tcp.flags.reset eq 1)
```

この例では、client.dropbox.comに接続を試みた際の証明書ピニングがDropBoxデスクトップアプリケーションに影響します。





注意：必要な除外を追加した後、これらの手順を複数回繰り返して、アプリケーション

で使用されるすべての宛先を識別できます。

互換性のないTLSバージョンの除外の識別

Umbrella SWGでサポートされている必須のTLS1.2+プロトコルを使用しないSSL/TLS接続を探します。これには、レガシープロトコル（TLS1.0以前）や、アプリケーションによって実装されるカスタムプロトコルが含まれます。

このフィルタ例は、初期TLSハンドシェイクパケットとDNSクエリーを表示します。

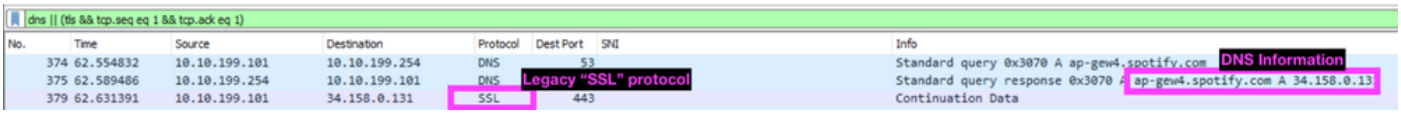
トンネル/AnyConnect

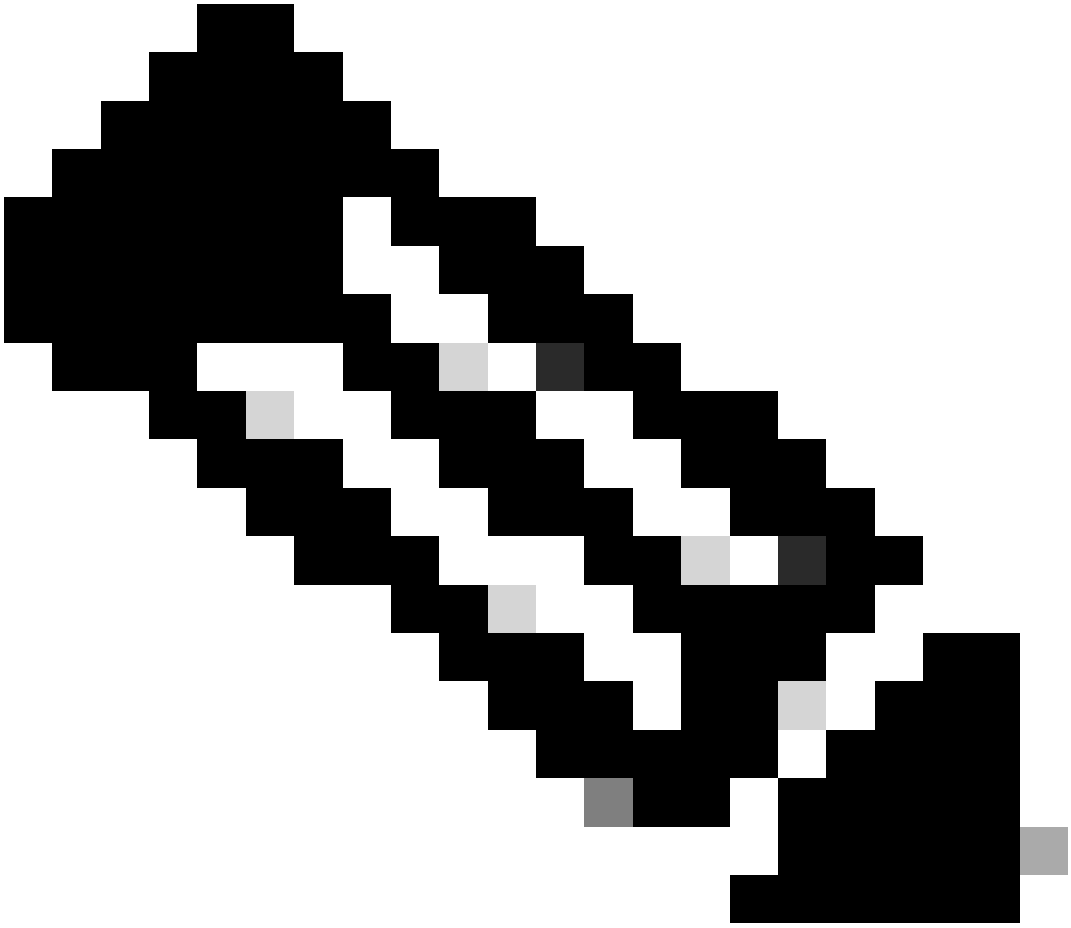
```
dns || (tls && tcp.seq eq 1 && tcp.ack eq 1)
```

PAC/プロキシチェーン

```
dns || http.request.method eq CONNECT
```

この例では、Spotifyデスクトップアプリケーションは、SWG経由で送信できない非標準またはレガシーの「SSL」プロトコルを使用してap-gew4.spotify.comに接続しようとしています。





注意：必要な除外を追加した後、これらの手順を複数回繰り返して、アプリケーションで使用されるすべての宛先を識別できます。

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。