SSL VPNトラフィックとの競合を回避するためのSWGの設定

内容

はじめに

このドキュメントでは、代行受信されたポートを使用して、Secure Web Gateway(SWG)とSSL VPN間の非互換性の問題を解決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。

問題

AnyConnect用のUmbrella SWGでは、SWGエージェントが代行受信したポート（TCP 443など）を使用する特定のSSL VPNで、非互換性の問題が発生する可能性があります。AnyConnect SWGがカバレッジのアクティブ化と適用に失敗する可能性があります。SWGがアクティブで、VPNトラフィックがSWGを通過する際に、ネットワークの信頼性が低下したり、使用できなくなったりすることがあります。このシナリオでは、非Webトラフィックはドロップされます。この問題は、ポート80および443を使用するすべてのSSL VPNに影響します。

解決方法

SWGがVPNトラフィックを代行受信しないようにするには、VPNドメインとIPアドレスにバイパスを設定します。

1. Umbrellaダッシュボードで、Access Deployments > Domain Management > External Domainsの順に移動します。

2. VPNヘッドエンドサーバのドメインとIPアドレスを外部ドメインリストに追加します。IPエントリにより、SWGエージェントが多数の接続を使用してVPNトラフィックを代行受信することがなくなります。

3. 新しい設定が反映されるまで1時間かかります。

SWGでSSL VPNを使用するには、次の手順を実行します。

1. VPNドメインを外部ドメインリストに追加します。

2. VPNヘッドエンドドメインがDNS検索サフィックスである場合、クライアントは接続の間、自動的にこのドメインを追加します。

3. VPNヘッドエンドのIPアドレスまたはIP範囲を外部ドメインリストに追加します。

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。