ネットワーク終了設定

この章では、ネットワーク終了機能とその設定方法について説明します。

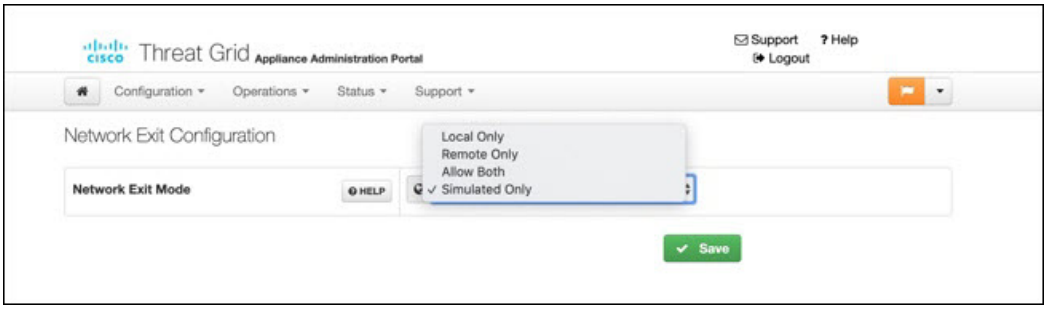
ネットワーク終了の設定

地理的な場所は、マルウェア分析において重要な問題になることがよくあります。マルウェアのいくつかの種類は、地理的な場所によって異なる方法で動作しますが、その他の種類は特定の領域をターゲットにする可能性があります。VPN の概念と同様に、**ネットワーク終了**設定（v2.4.3 以降）により、サンプル分析中に生成されるすべての発信ネットワークがその場所で終了したように表示されます。設定ファイルが自動的に配布されるため、サポートスタッフが手動でインストールまたは更新する必要はありません。

（注） 以前に tg-tunnel を使用していた場合は、v2.4.3 をインストールする前に、4.14.36.142:21413 と 63.97.201.68:21413 へのアウトバウンドトラフィックを許可する必要があります。それ以外の場合は、リモート終了の使用を有効にする前に、該当するトラフィックのみを許可する必要があります。

ステップ 1 OpAdmin ポータルで、**[Configuration] > [Network Exit]** をクリックします。

図 *1*：ネットワーク終了設定



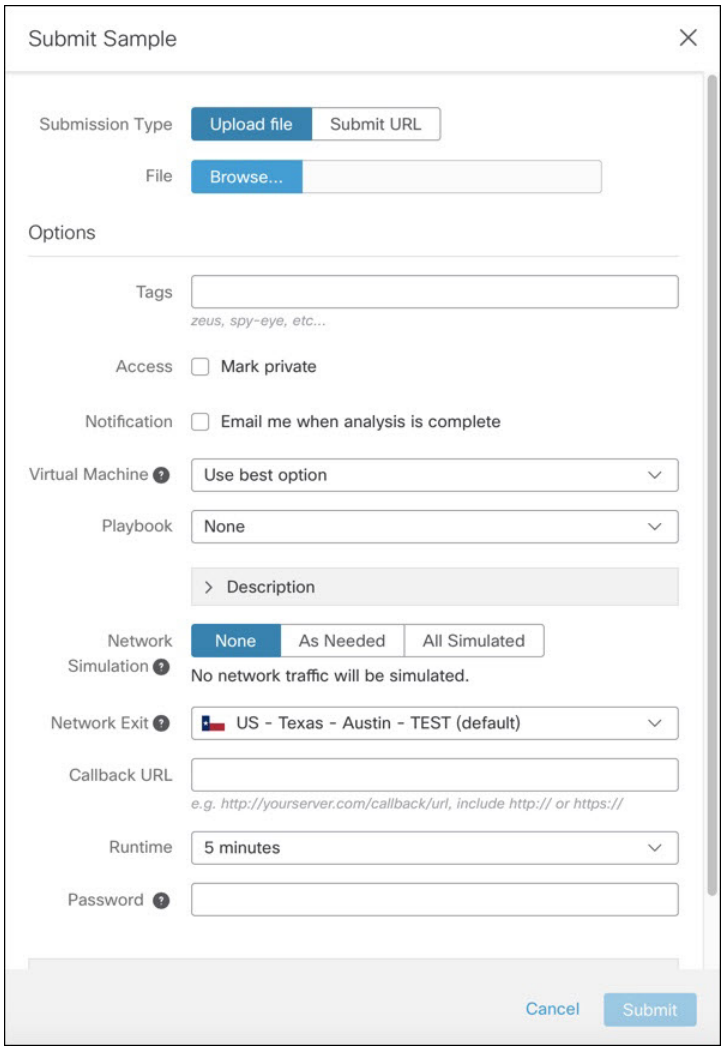
ステップ 2 [**Network Exit Mode**] フィールドで、[**Local Only**]、[**Remote Only**]、[**Allow Both**]、または [**Simulated Only**] を選択します。このフィールドで、UI でサンプルを送信する場合などに、アプリケーションで使用可能にする**ネットワーク終了**オプションを決定します。

[**Local Only**] または [**Remote Only**] を選択した場合、アプリケーションの設定により、ユーザが使用できるのはこれらのオプションのみになります。

[**Simulated Only**] を選択した場合、API ユーザと UI ユーザは、仮想マシンからローカル Threat Grid アプライアンス外の接続先にネットワークトラフィックを送信するオプションを選択できません。

プライベートネットワークへのアクセスは、DNS ルックアップやネットワーク終了が目的であっても許可されません。すべてのマルウェアトラフィックは、設定済みのダーティ DNS サーバを使用して、ダーティインターフェイスから発信されます。

図 *2:* サンプルの送信



（注） 分析中にネットワーク接続をシミュレートする必要が生じることがあります。ネットワーク シミュレーションは、それ以外の方法では（または他の理由で）使用できない可能性があるマルウェアサンプルにネットワークリソースを提示する方法をアナリストに提供します。たとえば、アップストリームサーバにアクセスできない場合、サーバがダウンしている場合、DNS レコードが失われた場合、またはサンプルの実行率と判定率を向上させるためにアウトバウンド接続に対する他の制限が適用されている場合に、ネットワーク接続をシミュレートするネットワーク シミュレーション オプションを選択できます。

さらに、ネットワーク シミュレーションは、エアギャップアプライアンスへの接続方法を少なくともいくつか提供し、それらのアプライアンスに対するサンプルの実行率を改善することができます。

サンプル分析の**ネットワーク シミュレーション**オプションは、Threat Grid Appliance v2.7.1 以降で使用できます。詳細については、Threat Grid Portal UI のオンラインヘルプトピックを参照してください。