仮想アプライアンスを除外するためのCisco ASA回避機能の設定

内容

はじめに

このドキュメントでは、脅威検出コンポーネントから仮想アプライアンスを除外するようにCisco ASAを設定する方法について説明します。Cisco ASA脅威検出コンポーネントは、DNSおよびその他のプロトコルでパケットインスペクションを実行します。Umbrellaサポートでは、この機能がシスコの仮想アプライアンスと競合しないように、次のASA設定変更を推奨しています。

- この記事で説明されているように、仮想アプライアンスを脅威検出「排除」機能から除外します。
- DNS暗号化(DNScrypt)を許可するように仮想アプライアンス(VA)をDNSパケットインスペクションから除外します。これについては、Cisco ASAファイアウォールがDNScryptをブロックするをご覧ください。

脅威検出の「回避」機能

「Shun」機能を有効にすると、ASAは脅威検出ルールをトリガーする送信元IPアドレスを完全にブロックできます。詳細については、シスコの記事「ASA脅威検出機能および設定」を参照してください。

仮想アプライアンスは、通常、非常に多数のDNSクエリをUmbrella DNSリゾルバに送信します。リゾルバへの接続にローカルの問題（一時的なネットワークの停止や遅延など）がある場合、これらのクエリは失敗する可能性があります。送信されるクエリーの量が非常に多いため、ごく一部の失敗でもASAは仮想アプライアンスを回避します。その結果、一定期間DNSが完全に停止します。

仮想アプライアンスの除外

注：この記事で紹介するコマンドは、あくまで参考用であり、実稼働環境に変更を加える前にシスコの専門家に相談することを推奨します。

CLIの場合：

- アプライアンスIPを排除から除外するには、次のコマンドを実行します。**no shun <src_ip>**

ASDMインターフェイス経由：

- Configuration > Firewall > Threat Detectionの順に選択します。
- アプライアンスのIPアドレスが排除されないようにするには、「Networks excluded from shun」フィールドにアドレスを入力します。複数のアドレスまたはサブネットをカンマで区切って入力できます。

アプライアンスが「排除」されているかどうかを確認する

これらの手順に従わないと、状況によってはアプライアンスが「排除」され、DNSが停止する可能性があります。

仮想アプライアンスに外部接続がない場合、Cisco ASAコンソールはイベントを次のようにログに記録します。

4|Jun 06 2014 14:00:42|401004：回避パケット：192.168.1.3 ==> 208.67.222.222 on interface inside
4|Jun 06 2014 14:00:42|401004：回避パケット：192.168.1.3 ==> 208.67.222.222 on interface inside

現在排除されているIPアドレスのリストを表示するには、ASAで**show shun**

現在排除されているIPアドレスをただちにクリアするには、ASAで**clear shun**

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。