Cisco Web セキュリティ アプライアンス（WSA）が Skype トラフィックを処理する方法

目次

質問：

Cisco Web セキュリティ アプライアンス（WSA）が Skype トラフィックを処理する方法

環境： Cisco WSA、Skype

Skype は、独自のインターネット テレフォニー（VoIP）ネットワークです。 Skype は、主にピアツーピア プログラムとして動作するため、中央のサーバと直接通信して動作することはありません。 Skype はさまざまな方法で接続を試みるため、ブロックするのが困難な場合があります。

Skype は、次の順序で接続します。

1. ランダムなポート番号を使用した、他のピアへの直接 UDP パケット
2. ランダムなポート番号を使用した、他のピアへの直接 TCP パケット
3. ポート 80 またはポート 443（またはその両方）を使用した、他のピアへの直接 TCP パケット
4. ポート 433 への HTTP CONNECT を使用した、Web プロキシ経由のトンネル パケット

明示的なプロキシ環境に展開された場合、1 ~ 3 の接続は Cisco WSA に送信されません。 Skype をブロックするには、まずネットワークの別の場所からブロックする必要があります。 Skype の接続手順 1 ~ 3 は、次の手段でブロックできます。

- ファイアウォール： Skype バージョン 1 のブロックには NBAR を使用します。 詳細については、http://ciscotips.wordpress.com/2006/06/07/how-to-block-skype/ を参照してください。
- Cisco IPS（ASA）： Cisco ASA は、シグニチャによって Skype を潜在的に検出してブロックできます。

Skype が明示的なプロキシを使用する場合、Skype は HTTP CONNECT 要求でクライアントの詳細（およびユーザ エージェント文字列を）を故意に提供しません。 このため、Skype と有効な CONNECT 要求を区別することが困難になります。 Skype は常にポート 443 に接続し、宛先アドレスは常に IP アドレスです。

例：

```
CONNECT 10.129.88.111:443 HTTP/1.0
Proxy-Connection: keep-alive
```

次のアクセス ポリシーは、IP アドレスとポート 443 を一致させる WSA によってすべての CONNECT 要求をブロックします。 これは、すべての Skype トラフィックを一致させます。 た

だし、ポート 443 の IP アドレスにトンネリングしようとする Skype 以外のプログラムもブロックされます。

Skype のブロック：HTTPS プロキシが無効化されている明示的な環境

IP およびポート 443 トラフィックを一致させるためのカスタム URL カテゴリを作成します。

1. [Security Manager] -> [Custom URL Categories] -> [Add Custom Category] の順に移動します。
2. [Category Name] に名前を入力し、[Advanced] を展開します。
3. [Regular Expression] ウィンドウに「[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+」と入力します。

アクセス ポリシーで、このカテゴリを拒否に設定します。

1. [Web Security Manager] > [Access Policies] の順に移動します。
2. [URL Categories] 列にある、該当のポリシー グループのリンクをクリックします。
3. [Custom URL Category Filtering] セクションで、新しい Skype カテゴリに対して [Block] を選択します。
4. 変更を送信し、保存します。

注： 明示的な CONNECT 要求は、HTTPS プロキシ サービスが無効になっている場合にのみブロックできます。

WSA の HTTPS 復号化が有効になっている場合、Skype トラフィックが破壊される可能性が最も高くなります。これは、このトラフィックが（CONNECT とポート 443 を使用しているにもかかわらず）純粋な HTTPS トラフィックではないためです。 これにより、WSA によって 502 エラーが生成され、接続が破棄されます。 IP アドレスへの実際の HTTPS Web トラフィックは（WSA で復号化された場合でも）引き続き正常に動作します。

Skype のブロック：HTTPS プロキシが有効化されている明示的または透過的な環境

IP およびポート 443 トラフィックを一致させるためのカスタム カテゴリを作成します。

1. [Security Manager] -> [Custom URL Categories] -> [Add Custom Category] の順に移動します。
2. [Category Name] に名前を入力し、[Advanced] を展開します。
3. [Regular Expression] ウィンドウに「[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+」と入力します。

復号化ポリシーで、このカテゴリを復号化に設定します。

1. [Web Security Manager] > [Decryption Policies] の順に移動します。
2. [URL Categories] 列にある、該当のポリシー グループのリンクをクリックします。
3. [Custom URL Category Filtering] セクションで、新しい Skype カテゴリに対して [Decrypt] を選択します。
4. 変更を送信し、保存します。

注： Skype トラフィックは IP に送信されるため、「未分類の URL」の一部と見なされます。 アクションが復号化か、またはパススルーかに応じて、上記と同じ効果が発生します。