

Cisco Web セキュリティ アプライアンスで不明なアプリケーションをブロックするにはどうしたらよいですか。

目次

[質問](#)

質問

Cisco Web セキュリティ アプライアンスで不明なアプリケーションをブロックするにはどうしたらよいですか。

注：このナレッジ ベース記事では、シスコによる保守およびサポートの対象でないソフトウェアを参照しています。情報は、利便性のために無償で提供されています。さらにサポートが必要な場合は、ソフトウェア ベンダーに連絡してください。

1. 最初の防御はそのようなアプリケーションをブロックするのに「ユーザ エージェント」ストリングを使用することです。これらののためのすべてのユーザーエージェントをアプリケーション知っていないので、下記のリンクでそれらを検索する必要があります。
Web セキュリティ マネージャ > アクセスポリシー > プロトコルおよびユーザ エージェント のカラムの下で <for 必須アクセス policy> 「ユーザーエージェント」を追加できます。--> Add 「**ブロック カスタム ユーザ エージェント**」の下に「ユーザー エージェント ストリング:」 (行ごとに1つ)。
2. アプリケーション表示制御 (AVC) がイネーブルになっていれば (GUI > Security の下で > Web 評判および反Malware 保守します)、インターネット ユーティリティ プロキシのようなアプリケーションタイプに、ファイル共有に基づいてブロック、アクセスをできます。 **Web セキュリティ マネージャ > アクセスポリシー** の下で > 「**アプリケーションのカラム** <for 必須アクセス policy> これをすることができます。
3. ユーザ エージェントが存在しない場合、MIME 型 (例を追加するように試みることができます: ビット急流アプリケーション)。
Web セキュリティ マネージャ > Web アクセス ポリシー > オブジェクト カラム <for の下で **必須アクセス policy**> 「MIME」型を追加できます。---オブジェクト/パントマイムの > Add は「**ブロック application/x-bittorrent** (行ごとに1) のようなカスタム MIME 型のセクションを打ち込みます。
4. フィルタ無効化のようなカテゴリがアクセスポリシーで、非合法 活動ブロックされるようにして下さい。いくつかのアプリケーションが接続のために既知 URL か IP アドレスを使用する場合、assocaited あらかじめ定義された URL カテゴリをブロックするか、またはブロックされたカスタム URL カテゴリで IP アドレス、FQDN、またはドメインと一致する regex を使用して設定できます。 **Web セキュリティ マネージャ > アクセスポリシー** の下で

> 「URL カテゴリ」カラムこれを行うことができます。

5. いくつかのアプリケーションは異なるポートに接続するのに HTTP 接続応答方式を使用できます。既知ポートだけを許可すれば HTTP の環境で必要とされる特定のポートはポート設定ドメインを接続します。

HTTP 接続応答は **Web セキュリティ マネージャ > アクセスポリシー > プロトコルおよびユーザ エージェントのカラムの下で <for 必須アクセス policy>** 設定することができます。-- 「HTTP 接続応答ポートの下の > Add によって許可されるポート:」

6. アクセスされる宛先 IP アドレスについてだけ確認するアプリケーションの場合関連する IP アドレスのためのアクセスをブロックするのに L4 トラフィック モニタ機能を使用できます。**Web セキュリティ マネージャ > L4 トラフィック モニタの下で > Malware 追加疑われたアドレス宛先 IPS** を追加できます。

「ユーザ エージェント」または「マイム役者型」がある特定のアプリケーションによって使用されているかどれをに気づいていなければ、この情報を見つけるために次のどちらかを行うことができます:

- パケットキャプチャをクライアント マシンの WireShark (Ethereal) と実行し、「http」プロトコルのためにフィルタリングして下さい。
- クライアントの IP アドレスでフィルタリングされる WSA のキャプチャを (「サポートおよびヘルプ」> 「パケットキャプチャの下で」) 実行して下さい。

ユーザ エージェントのリスト:

=====

<http://www.user-agents.org/>

MIME 型のリスト:

=====

<http://www.webmaster-toolkit.com/mime-types.shtml>

<http://www.microsoft.com/technet/isa/2004/plan/commonapplicationsignatures.mspx>