セキュアWebアプライアンスで未知のアプリケーションをブロックする方法

内容

概要

このドキュメントでは、Cisco Secure Web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方法について説明します。

不明なアプリケーションをブロックする方法

これらの方法は、単独または組み合わせて使用できます。

> **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。この情報は、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、ソフトウェアのベンダーに連絡してください。

ユーザエージェント文字列に基づくアプリケーションのブロック

最初の防御は、ユーザエージェント文字列を使用して未知のアプリケーションをブロックすることです。

- ユーザエージェントを **Web Security Manager** > **Access Policies** > **Protocols and User Agents** column <for the required access policy>
- ユーザエージェント文字列を **Block Custom User Agents**（1行につき1つ）。

> **注**：「リファレンス」の下にあるリンクを使用して、ユーザー· エージェントを検索できます。

Application Visibility Controlsに基づくアプリケーションのブロック

Application Visibility Controls(AVC)が有効になっている場合(**GUI > Security Services > Web Reputation and Anti-Malware**)を使用すると、プロキシ、ファイル共有、インターネットユーティリティなどのアプリケーションタイプに基づいてアクセスをブロックできます。この操作は、 **Web Security Manager > Access Policies > Applications** column <for the required access policy>

MIMEタイプに基づくアプリケーションのブロック

ユーザエージェントが存在しない場合は、多目的インターネットメール拡張機能(MIME)タイプを追加できます。

- 下にMIMEタイプを追加 **Web Security Manager** > **Web Access Policies** > **Objects** column <for the required access policy>
- オブジェクト/MIMEタイプを **Block Custom MIME Types** セクション（1行につき1つ） たとえば、BitTorrentアプリケーションをブロックするには、 application/x-bittorrent.

注：MIMEの種類を検索するには、「参照」のリンクを使用します。

アクセスポリシーのURLカテゴリのブロック

[Filter Avoidance]、[Illegal Activities]、[Illegal Downloads]などのカテゴリがアクセスポリシーでブロックされていることを確認します。一部のアプリケーションが接続に既知のURLまたはIPアドレスを使用する場合、関連付けられた事前定義されたURLカテゴリをブロックするか、ドメインに一致するIPアドレス、完全修飾ドメイン名(FQDN)、正規表現を使用してブロックされたカスタムURLカテゴリにを設定します。この操作は、 **Web Security Manager > Access Policies > URL Categories** カラム.

アクセスポリシーでのHTTP CONNECTポートの設定の制限

一部のアプリケーションでは、HTTP CONNECT方式を使用して異なるポートに接続できます。HTTP CONNECTポート設定ドメインの環境で必要な既知のポートまたは特定のポートのみを許可します。

- HTTP CONNECTは、 **Web Security Manager** > **Access Policies** > **Protocols and User Agents** column <for the required access policy>
- 許可ポートを **HTTP CONNECT Ports**.

特定のIPアドレスへのアクセスのブロック

アクセスされている宛先IPアドレスのみを認識しているアプリケーションでは、L4 Traffic Monitor機能を使用して、特定のIPアドレスへのアクセスをブロックできます。宛先IPを **Web Security Manager > L4 Traffic Monitor > Additional Suspected Malware Addresses**.

アプリケーションが使用するユーザエージェントまたはMIMEタイプの検索方法

特定のアプリケーションで使用されているユーザエージェントまたはMIMEタイプがわからない場合は、次のいずれかの手順を実行して情報を検索できます。

- クライアントのマシンでWireShark(Ethereal)を使用してパケットキャプチャを実行し、「http」プロトコルのフィルタを実行します。
- セキュアWebアプライアンスでキャプチャを実行します(**Support and Help** > **Packet Capture**)を選択します。

参考

> **注**：ここに記載されている外部Webサイトは、参照用としてのみ提供されています。リンクとコンテンツはシスコによって制御されず、変更される可能性があります。

ユーザエージェントのリスト

User Agent String.Com(useragentstring.com)

MIMEタイプのリスト

- 一般的なMIMEタイプ(mozilla.org)
- MIMEの種類：MIMEタイプの完全なリスト(w3cub.com)
- MIMEタイプの完全なリスト(sitepoint.com)