SWAでのMicrosoft Updateトラフィックの範囲要求の設定

内容

はじめに

前提条件

- 要 件
- 使用するコンポーネント

範囲要求

プロキシ環境での範囲要求

Microsoft更新プログラムの範囲要求を有効にする

Microsoft Updateに対してのみ範囲要求を有効にする手順

- ステップ 1：範囲要求の有効化
- ステップ 2Microsoft Updates URLのカスタムURLカテゴリの作成
- ステップ3:（オプション）Microsoft Updatesトラフィックを認証から除外するIDプロファイルを作成します
- ステップ4:（オプション）Microsoft Updatesトラフィックを通過させる復号化ポリシーを作成します
- ステップ 5Microsoft Updatesトラフィックの範囲要求を許可するアクセスポリシーの作成

アクセスログの変更

検証

関連情報

はじめに

このドキュメントでは、Microsoft Updates(MS)トラフィックでSecure Web Appliance(SWA)のRange Request(RRRQ)を使用できるようにする手順について説明します。

前提条件

要 件

次の項目に関する知識があることが推奨されます。

- SWA管理。

次のツールをインストールしておくことを推奨します。

- 物理または仮想SWA
- SWAグラフィカルユーザインターフェイス(GUI)への管理アクセス

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

範囲要求

範囲要求はHTTPプロトコルの機能で、クライアント（Webブラウザやダウンロードマネージャなど）はファイル全体を一度にダウンロードするのではなく、ファイルの特定の部分だけをサーバに要求できます。これは、中断されたダウンロードの再開、メディアのストリーミング、または大きなファイルへの効率的なアクセスに特に役立ちます。クライアントはHTTP要求のRangeヘッダーで必要なバイト範囲を指定し、サーバは範囲要求をサポートする場合は206 Partial Content(PCS)ステータスコードで応答し、要求されたファイルのセグメントだけを配信します。

このメカニズムにより、さまざまなシナリオでパフォーマンスとユーザエクスペリエンスが向上します。たとえば、ビデオストリーミングでは、レンジ要求によってプレーヤーは再生に必要なセグメントのみを取得できるため、帯域幅の使用量が削減され、応答性が向上します。同様に、ダウンロードマネージャは範囲要求を使用してファイルをチャンクに分割し、それらを並行してダウンロードすることで、プロセスを高速化します。範囲要求は、キャッシングおよびプロキシシステムでも重要な役割を果たし、部分的なアップデートを可能にし、冗長なデータ転送を削減します。

プロキシ環境での範囲要求

プロキシ環境では、範囲要求は帯域幅の使用を最適化し、コンテンツ配信の効率を向上させるために重要な役割を果たします。範囲要求が有効な場合、プロキシサーバは要求されたバイトセグメントだけを元のサーバから取得し、それらをローカルにキャッシュできます。これにより、クライアントは、ビデオや大きなファイルの特定のセグメントなどの部分的なコンテンツを要求し、プロキシキャッシュから迅速に受信できます（可能な場合）。また、並列ダウンロードおよび再開機能も有効にします。これらは、帯域幅が限られている環境や遅延が大きい環境で特に役立ちます。

ただし、範囲要求が無効な場合、クライアントが必要とする部分が少なくても、プロキシは発信元サーバからファイル全体をフェッチする必要があります。これにより、不要なデータ転送、プロキシとオリジンサーバの両方の負荷の増加、クライアントの応答時間の遅延が発生します。また、プロキシは部分的なコンテンツを保存または提供できないため、効率的なキャッシング戦略を妨げます。ストリーミングシナリオでは、これによりバッファリングの遅延やユーザエクスペリエンスの低下が発生する可能性があります。範囲要求の無効化は、セキュリティまたはポリシー上の理由で実行できますが、パフォーマンスと柔軟性が犠牲になることがあります。

たとえば、10人のユーザが100MBのファイルからそれぞれ1MBをプロキシサーバ経由でダウンロ

ードするとします。

範囲要求が無効：

範囲要求を無効にすると、プロキシは各ユーザが必要とする1MBのセグメントだけを取得できません。代わりに、要求ごとに元のサーバから100MBのファイル全体をダウンロードする必要があります。その結果、次のことが可能になります。

発信元からプロキシへの合計トラフィック：10 × 100 MB = 1000 MB(1 GB)

クライアントが実際に使用するのはそのデータの10 MBだけです。

残りの990MBは無駄になり、帯域幅の使用が非効率的になり、プロキシおよびオリジンサーバの負荷が増大します。

範囲要求が有効：

範囲要求を有効にすると、プロキシは要求された1 MB/ユーザのみをフェッチします。

発信元からプロキシへの合計トラフィック：10 × 1MB = 10MB

プロキシはこれらのセグメントをキャッシュし、必要に応じて他のユーザに提供できます。

これにより、トラフィックが90分の1に削減され、応答時間が短縮され、リソース使用率が大幅に向上します。

Microsoft更新プログラムの範囲要求を有効にする

範囲要求はパフォーマンスを向上させますが、SWA環境内のセキュリティスキャンとポリシー適用の妨げになります。これらのシステムでは部分的なコンテンツを完全に検査できないためです。この記事では、範囲要求の使用をMicrosoft Updateトラフィックのみに制限します。

⚠ 注意:範囲要求の転送を有効にすると、ポリシーベースのApplication Visibility and Control(AVC)効率が損なわれ、セキュリティが損なわれる可能性があります。

Microsoft Updateに対してのみ範囲要求を有効にする手順

ステップ 1：範囲要求の有効化	ステップ 1.1： GUIから、Security Servicesをクリックし、Web Proxyを選択します。 ステップ 1.2： [Edit Settings] をクリックします。 ステップ 1.3：Enable Range Request Forwardingチェックボックスをオンにします。 ステップ 1.4：[Submit] をクリックします。

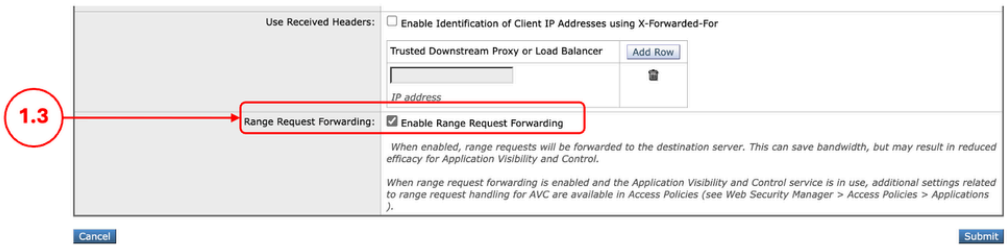
<table>
<tr><td></td><td> 

図 – 範囲要求転送の有効化</td></tr>
<tr><td>ステップ 2Microsoft Updates URLのカスタムURLカテゴリの作成</td><td>ステップ2.1:GUIから、Web Security Managerを選択し、カスタムおよび外部URLカテゴリをクリックします。
ステップ2.2：カテゴリの追加をクリックして、カスタムURLカテゴリを追加します。
手順2.3:一意のCategoryNameを割り当てます。
ステップ2.4:（オプション）説明を追加する。

ステップ 2.5：リスト順から、一番上に配置する最初のカテゴリを選択します。

ステップ 2.6：Category Typeドロップダウンリストから、Local Custom Categoryを選択します。

ステップ 2.7： SitesセクションにMicrosoft Updates URLを追加します。

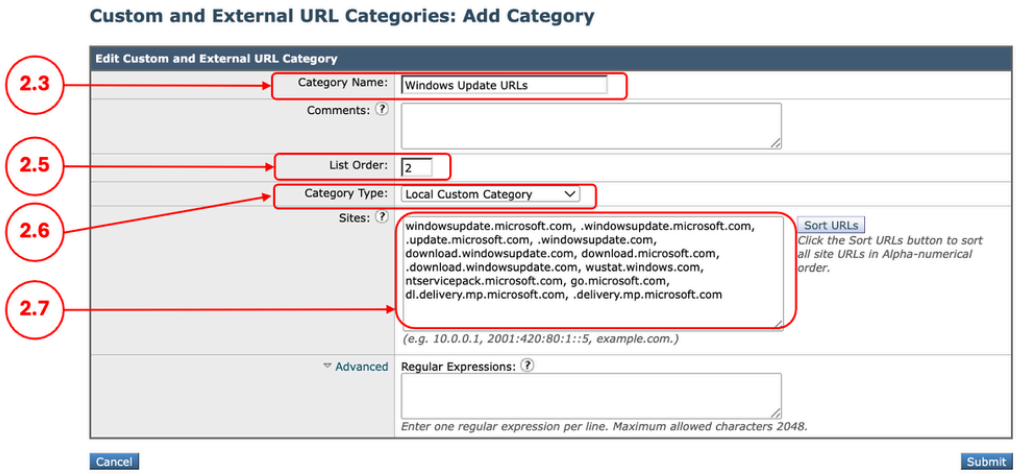
ヒント:Microsoftの更新プログラムの一覧は、次のリンクから確認できます：手順2 - WSUSの構成| Microsoft詳細情報

注意:Microsoftのドキュメントにあるようなurlをコピー/ペーストしないでください。SWA形式として正しく書式設定してください。 詳細については、次のサイトを参照してください。Secure Web ApplianceでのカスタムURLカテゴリの設定 – シスコ

次に例を示します。

http://windowsupdate.microsoft.com ===> windowsupdate.microsoft.com
http://*.windowsupdate.microsoft.com ===> .windowsupdate.microsoft.com

ステップ 2.8： [Submit] をクリックします。</td></tr>
</table>

<table>
<tr>
<td></td>
<td> 

イメージ – カスタムURLカテゴリの作成</td>
</tr>
<tr>
<td>ステップ3: (オプション) Microsoft Updatesトラフィックを認証から除外するIDプロファイルを作成します

注：このアクションは、Microsoft Updatesへのトラフィックに対するSWAの認証負荷を軽減することです。</td>
<td>ステップ3.1:GUIから、Web Security Managerを選択し、Identification Profilesをクリックします。
ステップ3.2：プロファイルを追加するには、Add Profileをクリックします。
ステップ3.3:Enable Identification Profilecheckボックスが選択されていることを確認します。
手順3.4:一意のprofileNameを割り当てます。
ステップ3.5: (任意) 説明を追加する。
ステップ3.6:上記の挿入ドロップダウンリストから、このプロファイルをテーブルのどこに表示するかを選択します。

ステップ 3.7： ユーザ識別方法セクションで、認証/識別から免除を選択します。

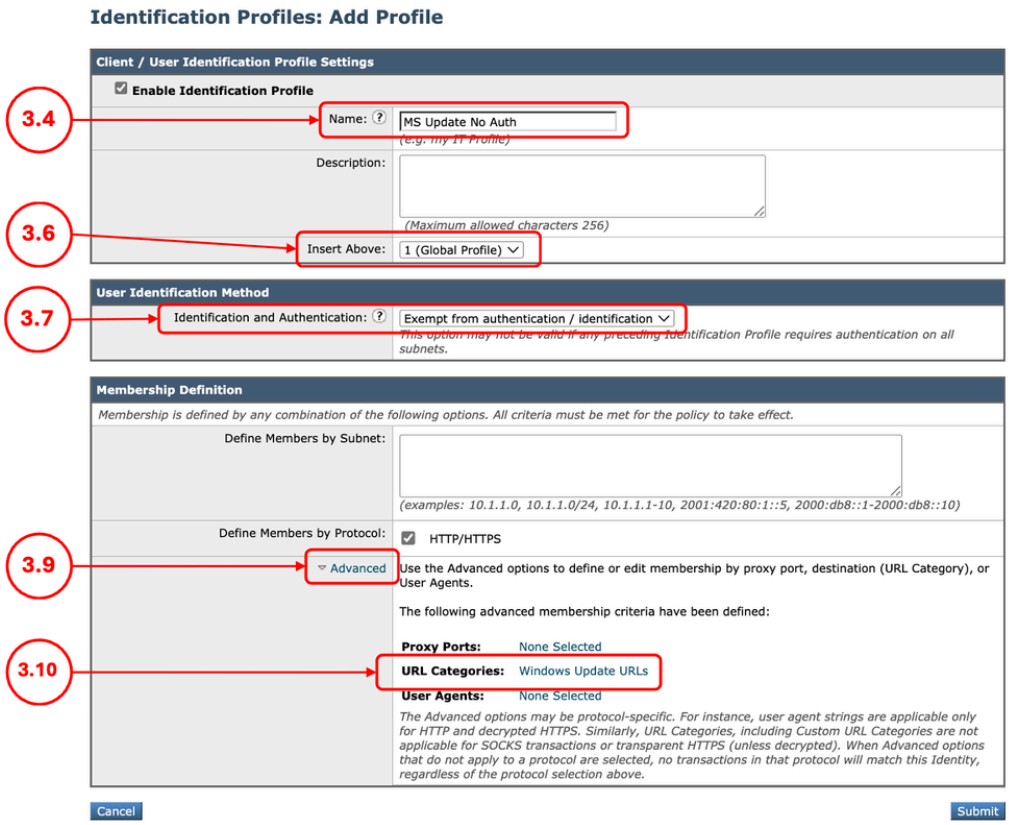
手順3.8.「サブネットによるメンバーの定義」で、特定のユーザに対してMicrosoftトラフィックをパススルーしたい場合は、適用するIPアドレスまたはサブネットを入力します。すべてのIPアドレスを含める場合は、このフィールドを空白のままにします。

ステップ 3.9：Advancedセクションから、Custom URL Categoriesを選択します。

ステップ 3.10：Microsoftアップデート用に作成されたカスタムURLカテゴリを追加します。

ステップ 3.11：[Done] をクリックします。

ステップ 3.12： [Submit] をクリックします。</td>
</tr>
</table>



イメージ – 識別プロファイルの作成

ステップ4: (オプション) Microsoft Updatesトラフィックを通過させる復号化ポリシーを作成します

注:Microsoft Updatesは HTTPを使用し、HTTPSトラフィックはアップデートリンクをプッシュするためのものです。これは、SWAでの復号化の負荷を軽減するためです。

ステップ4.1:GUIから、Web Security Managerを選択し、Decryption Policyをクリックします。

ステップ 4.2： Add Policiesをクリックして、復号ポリシーを追加します。

手順4.3:一意のPolicyNameを割り当てます。
ステップ4.4: (オプション) 説明を追加する。
ステップ4.5:Insert Above Policypolicyドロップダウンリストから、最初のポリシーを選択します。

ステップ4.6:Identification Profiles and Usersで、Select One or more Identification Profilesを選択します。

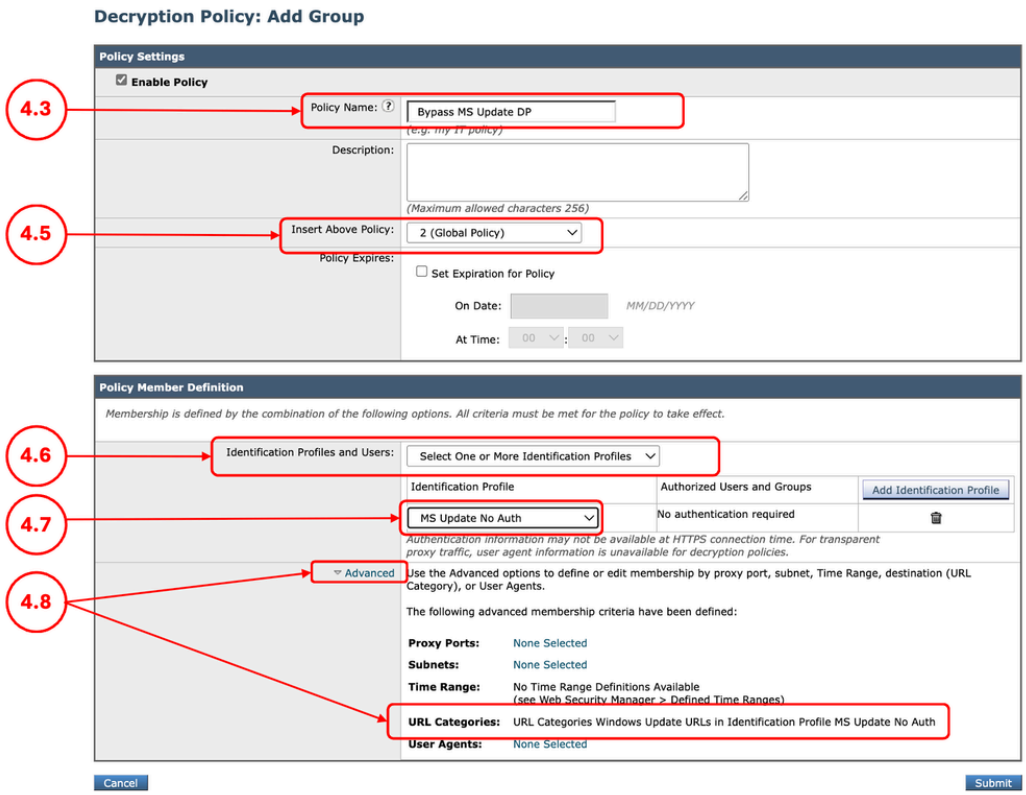
ステップ 4.7：ステップ3で作成したIDプロファイルを選択し、ステップ4.11に進みます。

ステップ 4.8： Windows UpdatesのIDプロファイルを作成していない場合は、AdvancedセクションでCustom URL Categoriesを選択します。

ステップ 4.9：ステップ2でMicrosoftのアップデート用に作成したカスタムURLカテゴリを追加します。

ステップ 4.10：[Done] をクリックします。

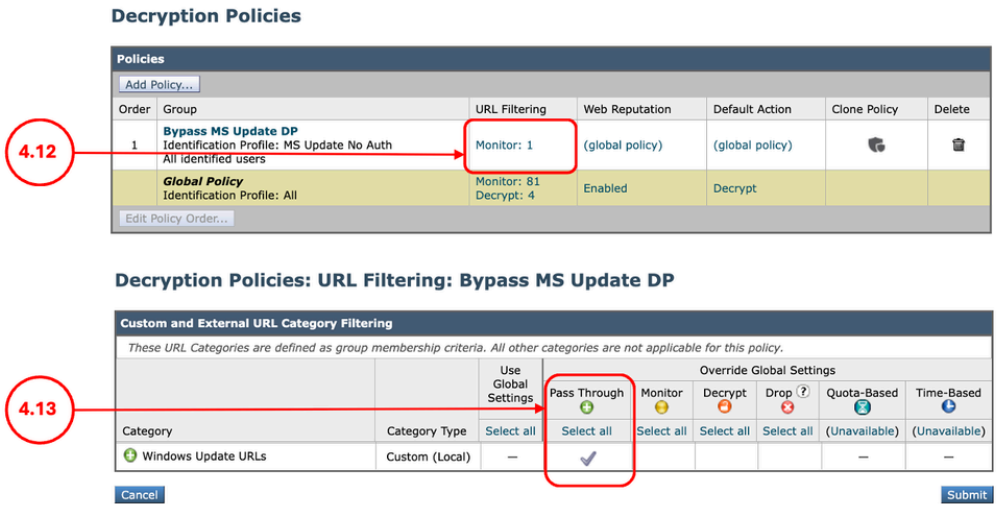
ステップ 4.11： [Submit] をクリックします。



イメージ：復号化ポリシーの作成

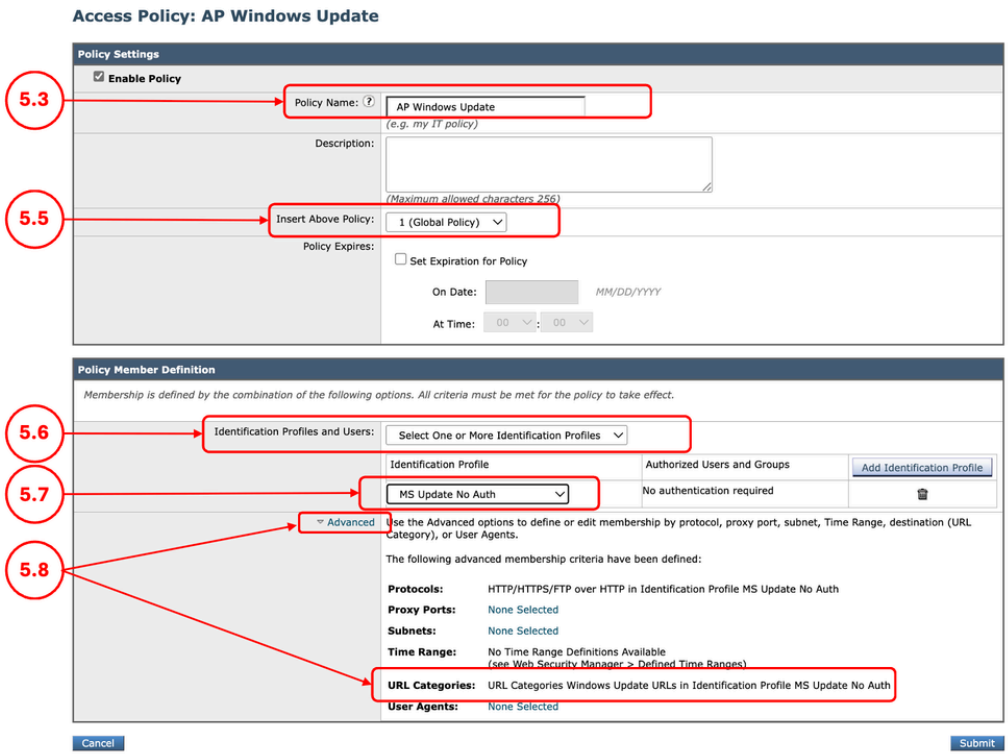
ステップ4.12:復号ポリシーページのURLフィルタリングで、この新しい復号ポリシーに関連付けられているリンクをクリックします。

ステップ4.13:SelectPassには、Microsoft Updates URLカテゴリのアクションがあります。



イメージ：URLカテゴリのアクションのパススルーの設定

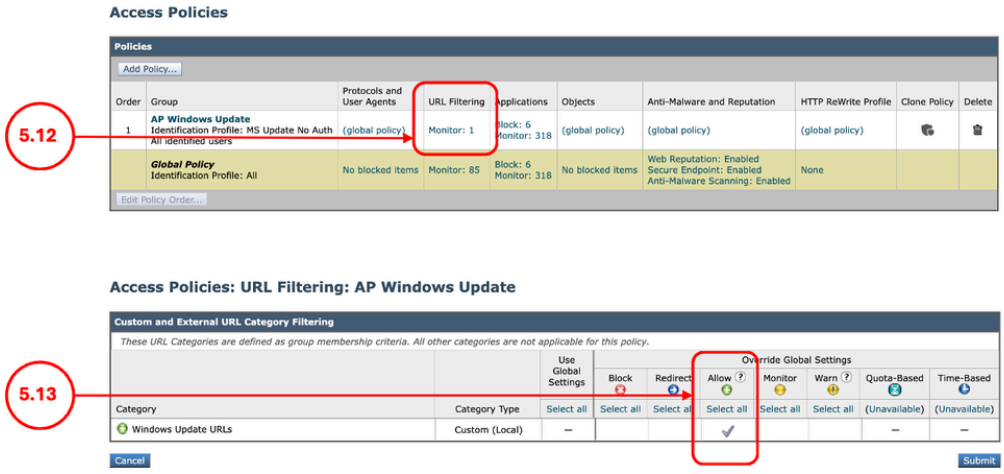
ステップ 4.12：[Submit] をクリックします。

ステップ 5Microsoft Updatesトラフィックの範囲要求を許可するアクセスポリシーの作成	ステップ5.1:GUIから、Web Security Managerをクリックし、Access Policyを選択します。 ステップ 5.2： アクセスポリシーを追加するには、Add Policiesをクリックします。 ステップ5.3:一意のPolicyNameを割り当てます。 ステップ5.4:（オプション）説明を追加する。 ステップ5.5:Insert Above Policypolicyドロップダウンリストから、最初のポリシーを選択します。 ステップ5.6:Identification Profiles and Usersから、Select One or more Identification Profilesを選択します。 ステップ 5.7：ステップ3で作成したIDプロファイルを選択し、ステップ5.11にスキップします。 ステップ 5.8： Windows UpdatesのIDプロファイルを作成していない場合は、AdvancedセクションでCustom URL Categoriesを選択します。 ステップ 5.9：ステップ2でMicrosoftのアップデート用に作成したカスタムURLカテゴリを追加します。 ステップ 5.10：[Done] をクリックします。 ステップ 5.11：[Submit] をクリックします。  イメージ：アクセスポリシーの作成 ステップ 5.12： Access PoliciesページのURL Filteringの下で、この新し

いアクセスポリシーに関連付けられているリンクをクリックします

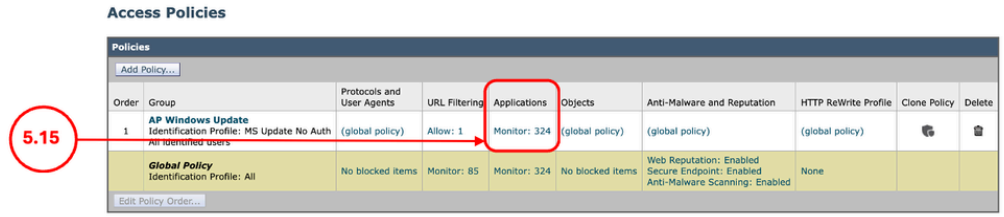
ステップ5.13:Microsoft Updates用に作成したカスタムURLカテゴリのアクションとしてAllowを選択します。

ステップ 5.14：[Submit] をクリックします。



イメージ：URLカテゴリのアクション許可の設定

ステップ 5.15： Access PoliciesページのApplicationsの下で、この新しいアクセスポリシーに関連付けられているリンクをクリックします

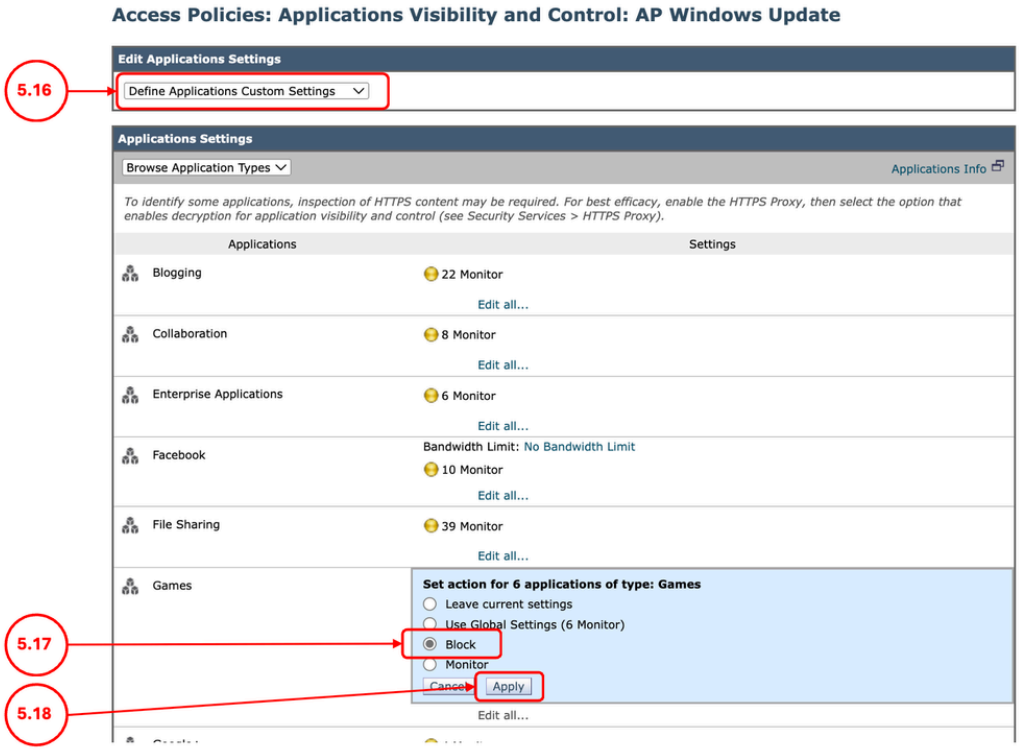


イメージ – Application Visibility and Controlの編集

ステップ 5.16：Edit Applications Settingsセクションで、Define Applications Custom Settingsを選択します。

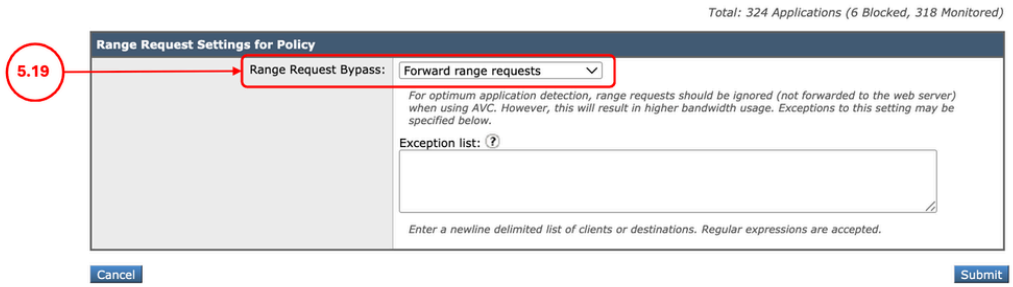
ステップ5.17:アプリケーションの設定セクションで、Gamesアプリケーションのすべてを編集をクリックし、アクションをブロックに設定します。

ステップ 5.18：[APPLY] をクリックします。



イメージ – 1つのアプリケーションアクションをブロックに設定

ステップ 5.19：下にスクロールしてRange Request Settings for Policyセクションに移動し、Forward range requestsが選択されていることを確認します。



イメージ – ポリシーの範囲要求の設定

ステップ 5.20：[Submit] をクリックします。

ステップ5.21:アクセスポリシーページで、アプリケーションの下にあるグローバルポリシーに関連付けられているリンクをクリックします。

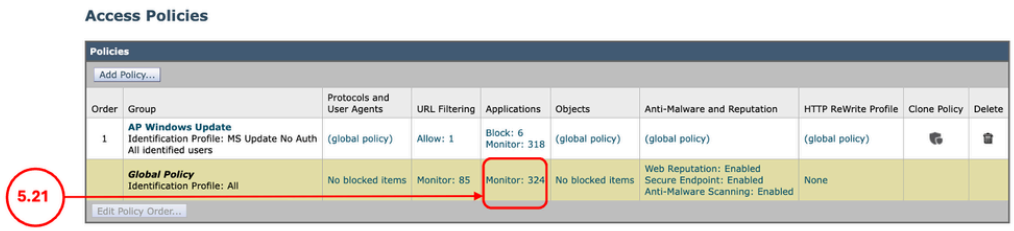


図 – デフォルトのアクセスポリシーアプリケーション設定

	ステップ 5.22：下にスクロールしてRange Request Settings for Policyセクションに移動し、Do Not Forward Range Requestsが選択されていることを確認します。 ステップ 5.23：変更を確定します。

アクセスログの変更

アクセスログからの範囲要求をより詳細に把握するために、次のカスタムフィールドを追加できます。

[クライアントの範囲= %<範囲：]	クライアントが要求した範囲を表示します（バイト）
[content= %>Content-Length:]	ダウンロードされたコンテンツのサイズ（バイト）を表示します

SWAアクセスログにカスタムフィールドを追加する方法の詳細については、「アクセスログのパフォーマンスパラメータの設定」を参照してください。

検証

次のCURLコマンドを使用して、範囲要求をSWAに送信します。

```
curl -vvvk -H "Pragma: no-cache" -x 10.48.48.181:3128 -H 'Range: bytes=0-100' 'http://catalog.sf.dl.del
```

CURLの出力から、HTTP応答がHTTP/1.1 206であることがわかります。

```
> GET http://catalog.sf.dl.delivery.mp.microsoft.com/filestreamingservice/files/f263aa64-f367-42f0-9cad
> Host: catalog.sf.dl.delivery.mp.microsoft.com
> User-Agent: curl/8.7.1
> Accept: */*
> Proxy-Connection: Keep-Alive
> Pragma: no-cache
> Range: bytes=0-100
>
* Request completely sent off
< HTTP/1.1 206 Partial Content
```

アクセスログから、アクションがTCP_CLIENT_REFRESH_MISS/206であることを確認できます

。

```
1773942471.096 14 10.190.0.206 TCP_CLIENT_REFRESH_MISS/206 860 GET http://catalog.sf.dl.delivery.mp.mic
```

関連情報

- AsyncOS 15.0 for Cisco Secure Web Applianceユーザガイド – GD（一般導入）– ポリシー アプリケーションのエンドユーザの分類[Cisco Secure Web Appliance] – シスコ
- Secure Web Applianceでのカスタム URLカテゴリの設定：シスコ
- Cisco Webセキュリティアプライアンス(WSA)でOffice 365トラフィックを認証および復号化から除外する方法：シスコ
- アクセスログのパフォーマンスパラメータの設定
- セキュアなWebアプライアンスのベストプラクティスの使用：シスコ
- Secure Web Applianceでの認証のバイパス：シスコ

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。