Cisco Web セキュリティ アプライアンス 10 v1.2

最終更新日:2018 年 3 月 14 日

このデモンストレーションについて

WSA AsyncOS 10.1 リリースで導入された機能を実演して紹介するには、Cisco Web セキュリティ アプライアンス 10 v1.2 を使用してください。また、Cisco Advanced Web Security Reporting(AWSR)リリース 6.2 で導入されたカスタム レポートの実演も可能です。

この事前設定済みの WSA 10 のデモンストレーションは、以下のセクションとシナリオで構成されます。

要件

次の表に、本デモンストレーションに必要な要件の概要を示します。

表 1. 要件

必須	オプション
● ラップトップ	● Cisco AnyConnect®

このソリューションについて

Cisco Web セキュリティ アプライアンスは、インターネット トラフィックを傍受および監視するとともに、ポリシーを適用することによって、マルウェア、機密データ損失、生産性低下、その他のインターネット ベースの脅威から社内ネットワークを保護することに役立ちます。1 つのソリューションで、高度な脅威防御、高度なマルウェア防御（AMP）、アプリケーションの可視性と制御（AVC）、洞察力に富んだレポート、セキュアなモビリティなどの機能を兼ね備えています。また、Web トラフィックの保護とコントロールを行いながら、導入を単純化し、コストを削減します。

新しい AsyncOS 10 リリースでは、リファラー ヘッダー バイパスのサポート、外部フィード処理、中間証明書サポートのほか、ユーザ エージェント リストの更新、AMP プライベート クラウド サポート、AMP レポートの強化の新機能が追加されています。

WSA 10.0 リリースの詳細については、下記のリンクを参照してください。

セキュリティ レクチャー：https://youtu.be/Uvpeb2Chr3Y [英語]

リリース ノート：https://www.cisco.com/c/dam/en/us/td/docs/security/wsa/wsa_10-0/WSA_10x_Release_Notes.pdf [英語]

トポロジ

このコンテンツには、スクリプト形式のシナリオと、ソリューションの機能を実例で示すために事前設定されたユーザとコンポーネントが含まれています。コンポーネントのほとんどは、管理ユーザ アカウントを使用して任意の設定が可能です。コンポーネントへのアクセスに使用する IP アドレスとユーザ アカウント資格情報は、アクティブ セッションの [トポロジ（Topology）] メニューのコンポーネント アイコンをクリックして確認するか、それらを必要とするシナリオ内の手順で確認できます。

図 1. dCloud のトポロジ

表 2. 機器の詳細

名前	説明	ホスト名（FQDN）	IP アドレス	ユーザ名	パスワード
WSA-HQ1 プロキシ	WSA-HQ プロキシ		198.18.133.55:8080	admin	C1sco12345
Active Directory	Active Directory		198.18.133.1	administrator	C1sco12345
Workstation 1	クライアント マシン		198.18.133.36	wsaproxy	C1sco12345
AWSR	アドバンスト Web セキュリティ レポート		198.18.133.56:8888	administrator	C1sco12345

はじめに

プレゼンテーションの前に

Cisco dCloud では、実際の対象者の前でプレゼンテーションを行う前に、アクティブなセッションを使用して、このドキュメントのタスクを実施しておくことを強く推奨します。そうすることで、ドキュメントとコンテンツの構成に慣れることができます。

場合によっては、環境を元の構成にリセットするため、このガイドに従った後に新しいセッションをスケジュールする必要があります。

プレゼンテーションを成功させるためには、入念な準備が不可欠です。

次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。

1. dCloud セッションを開始します。[手順を見る]

注: セッションがアクティブになるまで最長で 10 分かかることがあります。

2. 最適なパフォーマンスを得るには、**Cisco AnyConnect VPN** [手順を見る] および**ラップトップのローカル RDP クライアント** [手順を見る] を使用してワークステーションに接続します。
   - ワークステーション 1:**198.18.133.36**、ユーザ名:**dcloud\wsaproxy**、パスワード:**C1sco12345**

注: Cisco dCloud リモート デスクトップ クライアントを使用してワークステーションに接続することもできます [手順を見る] 。dCloud リモート デスクトップ クライアントは、最小限の操作でアクティブ セッションにアクセスする場合に最適です。ただし、この方法には、接続ができない場合や、パフォーマンスが悪い場合があります。

シナリオ 1.　WSA - スタンドアロン（明示型モード）

手順

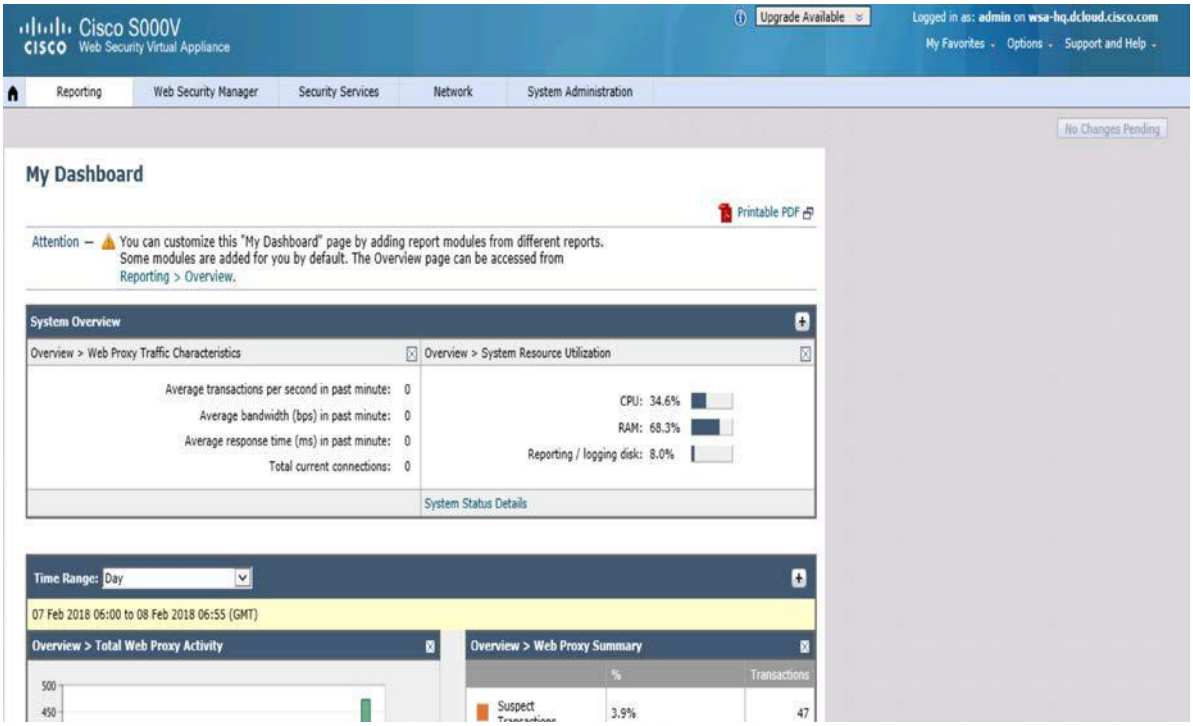
注:このシナリオでは、アプライアンスとトラフィックを区別するために複数のブラウザを使用しています。IE を使用するアプライアンスへのアクセス用として、URL ショートカットに簡単にアクセスできるブックマークが Wkstn1 の Firefox ブラウザにあらかじめ設定されています。

1. **Wkstn1** デスクトップで、タスクバーから **Firefox** ブラウザと **Internet Explorer** ブラウザの両方を開きます。

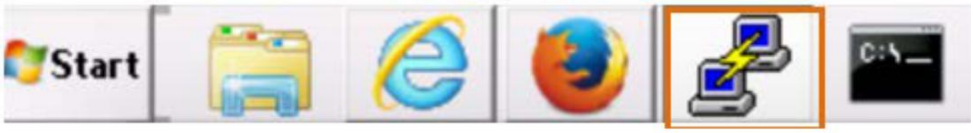
注:IE には、WSA 管理のショートカットが **WSA-HQ** として含まれています。また、WSA は現在、明示プロキシ モードに設定されています。つまり、Firefox ブラウザでは手動によるプロキシ設定が有効になっています。

2. [ログイン（Login）] をクリックし、ユーザ名：**admin**、パスワード：**C1sco12345** で WSA-HQ にアクセスします。

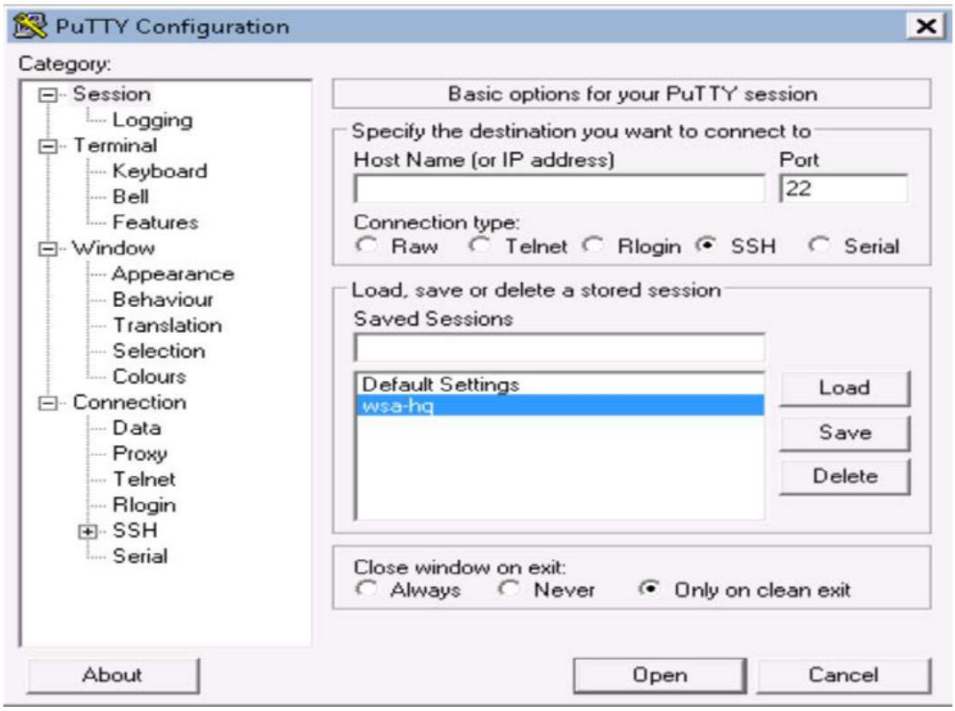
3. ログインが成功すると、WSA の [ダッシュボード（Dashboard）] ページが表示されます。



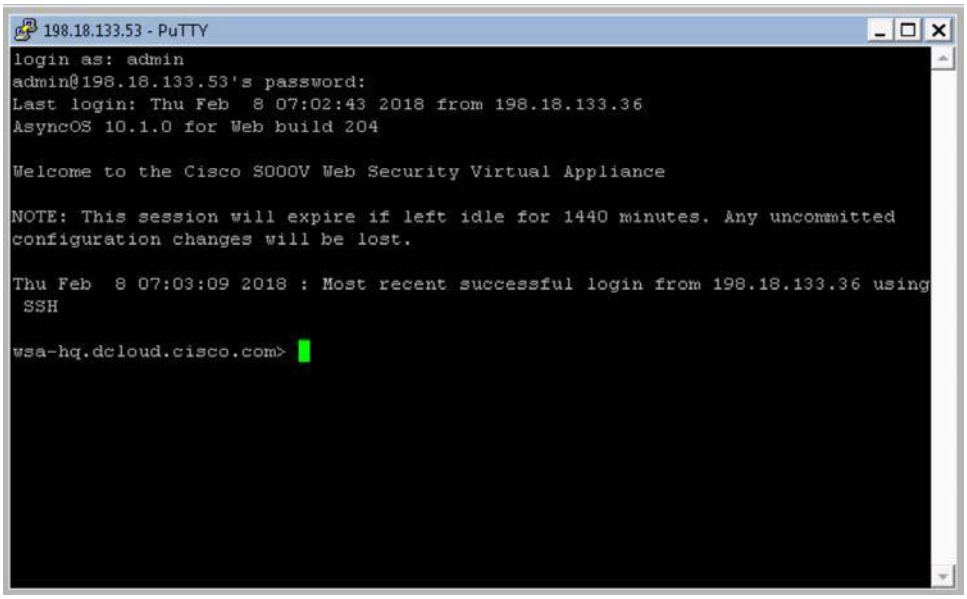
4. タスクバーのショートカットから WSA の PuTTY クライアントにログインします。



5. wsa-hq というショートカットをクリックします。



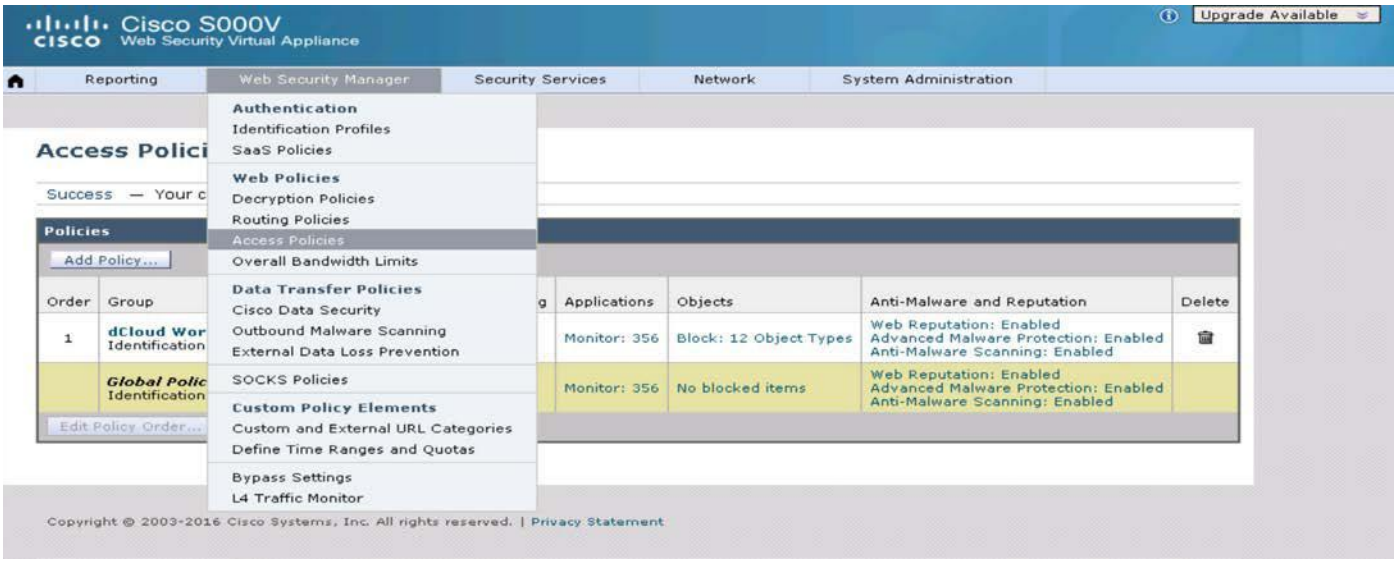
6. ユーザ名：**admin**、パスワード：**C1sco12345** でログインします。



基本 URL カテゴリ – 構成、ポリシー チェック、レポート

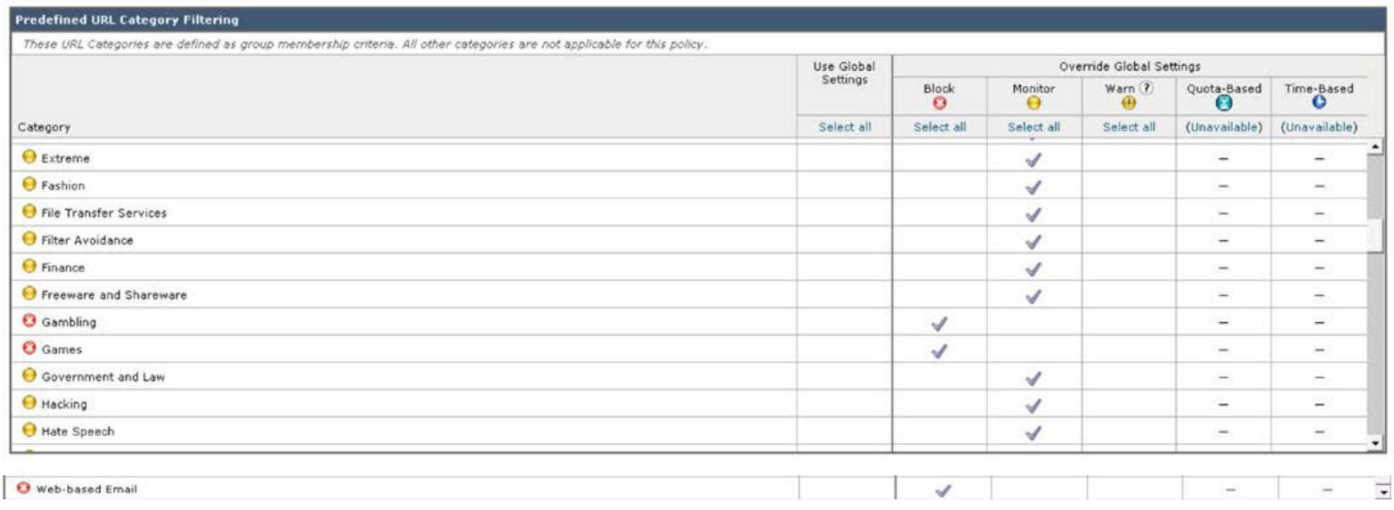
ポリシー チェック

1. WSA アプライアンスの GUI インターフェイスにログオンし、[Web セキュリティマネージャ（Web Security Manager）] > [アクセスポリシー（Access Policies）] の順に移動します。



2. [アクセスポリシー（Access Policies）] で、[dCloud ワークステーション（dCloud Workstation）] の [URL フィルタ（URL Filtering）] タブをクリックします。

3. [ゲーム（Games）]、[ギャンブル（Gambling）]、[Web ベースの電子メール（Web Based Email）] の URL カテゴリがブロックに設定されているのを確認します。



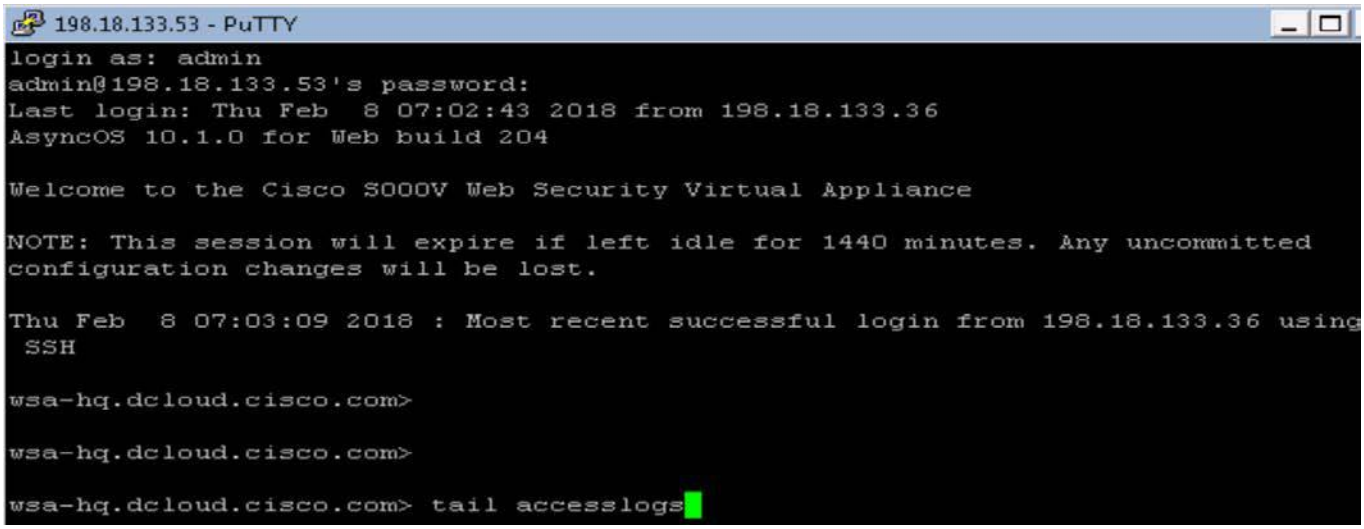
ゲーム URL のブロック

1. Firefox ブラウザと PuTTY クライアントを使用して同じテストを行います（リアルタイム ログ）。

2. Firefox で [ゲーム（Games）] のショートカットをクリックして、PuTTY のログを確認します。

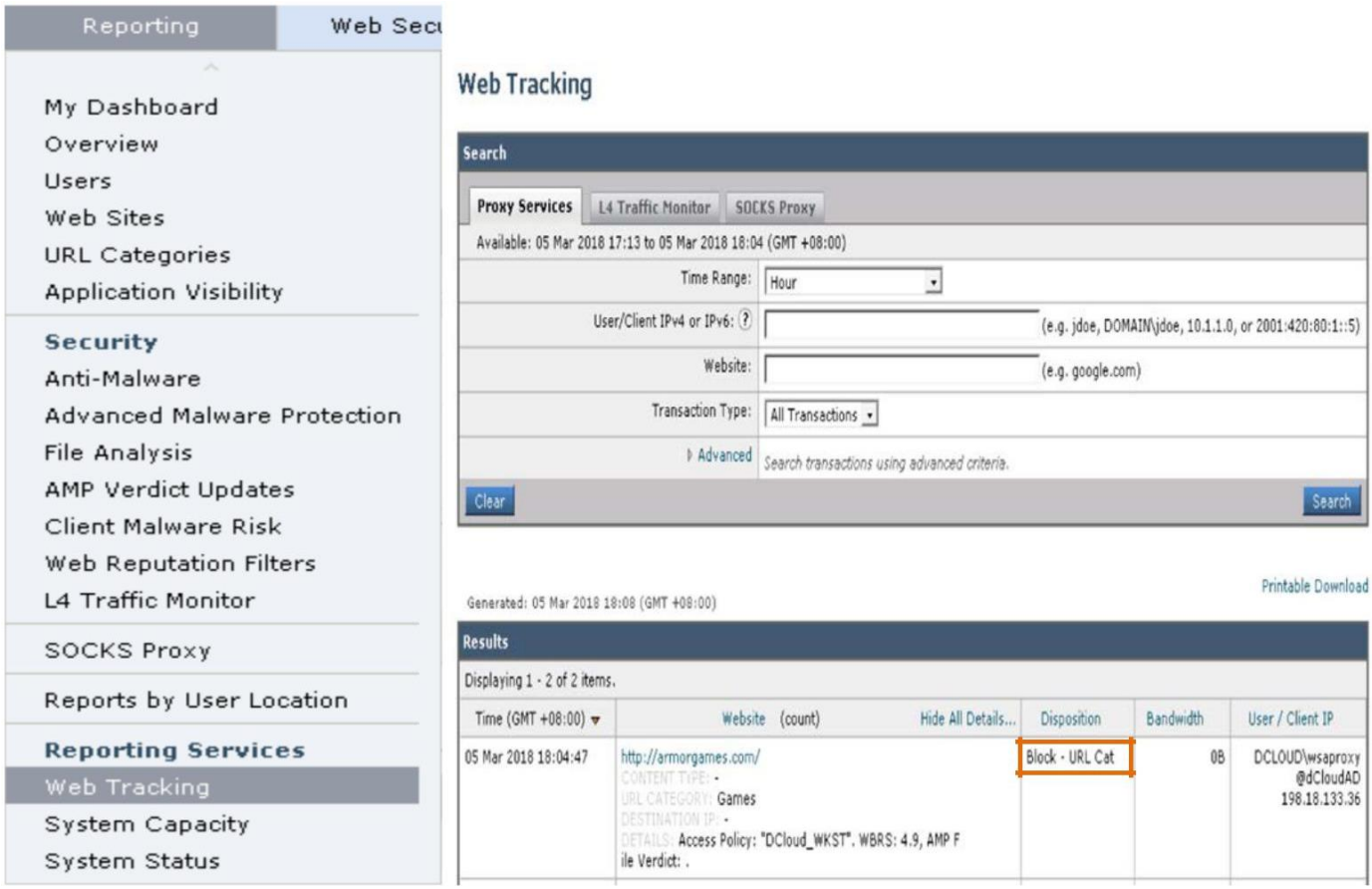
Date: Mon, 05 Mar 2018 18:01:21 +08
Username: DCLOUD\wsaproxy@dCloudAD
Source IP: 198.18.133.36
URL: GET http://armorgames.com/
Category: Games
Reason: BLOCK-WEBCAT
Notification: WEBCAT

3. WSA の PuTTY クライアントで、WSA の PuTTY クライアントからのアクセス ログに tail コマンドを実行します。



4. PuTTY でアクセス ログをスクロールして、www.gogy.com というゲーム URL を探します。

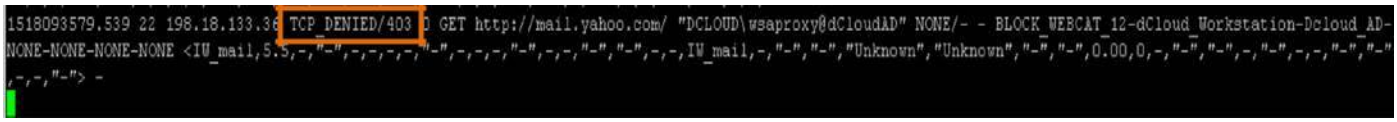
5. WSA で [Web トラッキング（Web Tracking）] レポートが表示されます。



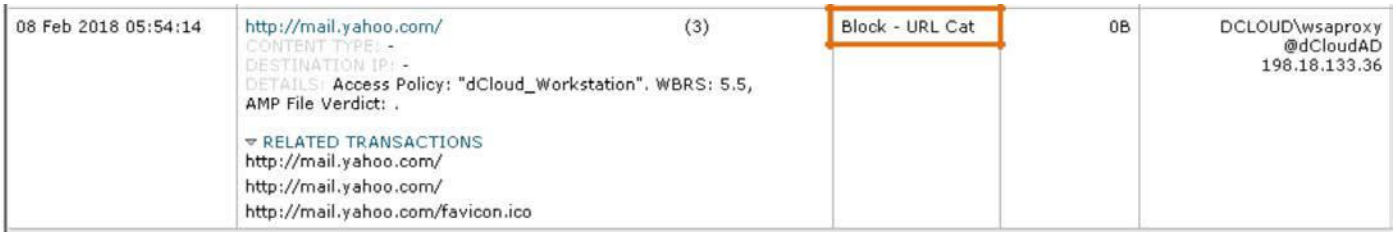
Web メール トラフィックのブロック

6. たとえば Yahoo メールを例として（および例外としても）使用する場合、Firefox で [Yahoo メール（Yahoo Mail）] ショートカットをクリックし、PuTTY のログで Web メール カテゴリがブロックされていることを確認します。

7. アクセス ログをスクロールして mail.yahoo.com を探します。

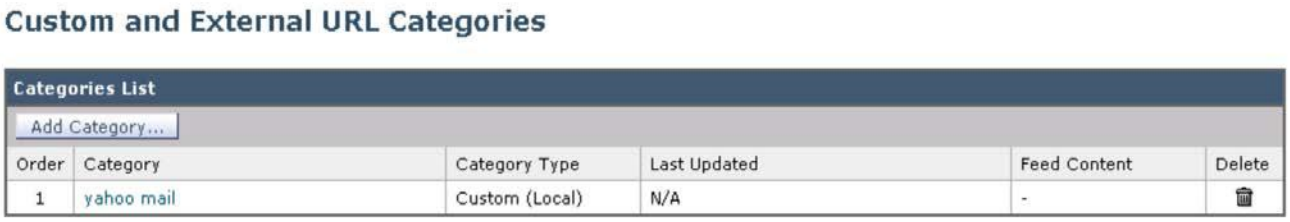


8. 同様に、[Web トラッキング（Web Tracking）] もスクロールして mail.yahoo.com を探します。

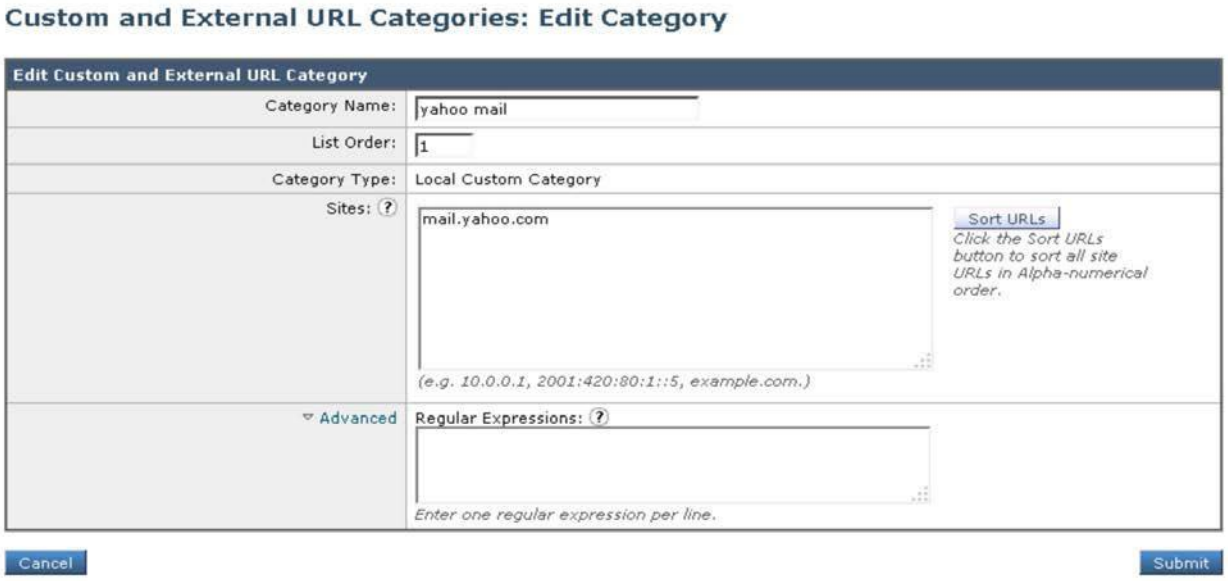


Yahoo メールの例外の作成と、ポリシーへのマッピング

1. **Yahoo メール**は許可するが Web メール一般はブロックするという例外を作成するために、カスタム URL カテゴリを有効にします。
2. [Web セキュリティマネージャ（Web Security Manager）] > [カスタムおよび外部 URL カテゴリ（Custom and External URL Categories）] の順に選択します。
3. テーブル内に Yahoo メールが表示されています。



4. 編集して、mail.yahoo.com がアクティブになっているのを確認します。



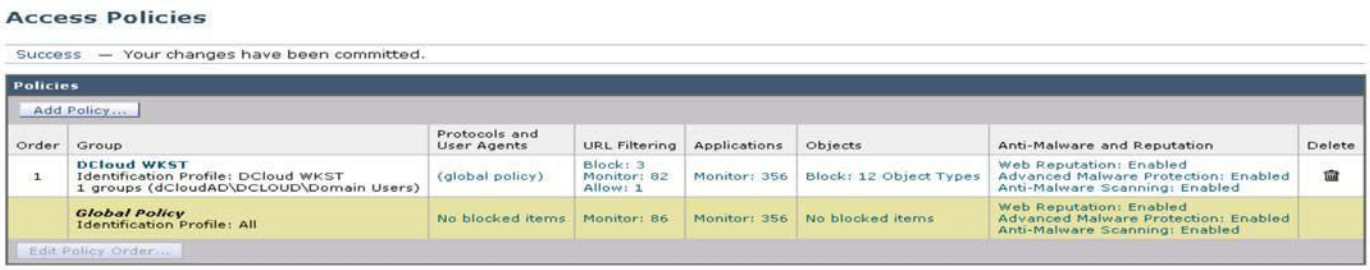
5. **dCloud ワークステーション**の [アクセスポリシー（Access Policy）] でカスタム ポリシーを有効にするには、[URL フィルタ（URL Filtering）] の下の [ブロック/モニタ（Block/Monitor）] をクリックします。

6. [URL フィルタ（URL Filtering）] で、[カスタムカテゴリの選択（Select Custom Categories）] をクリックします。

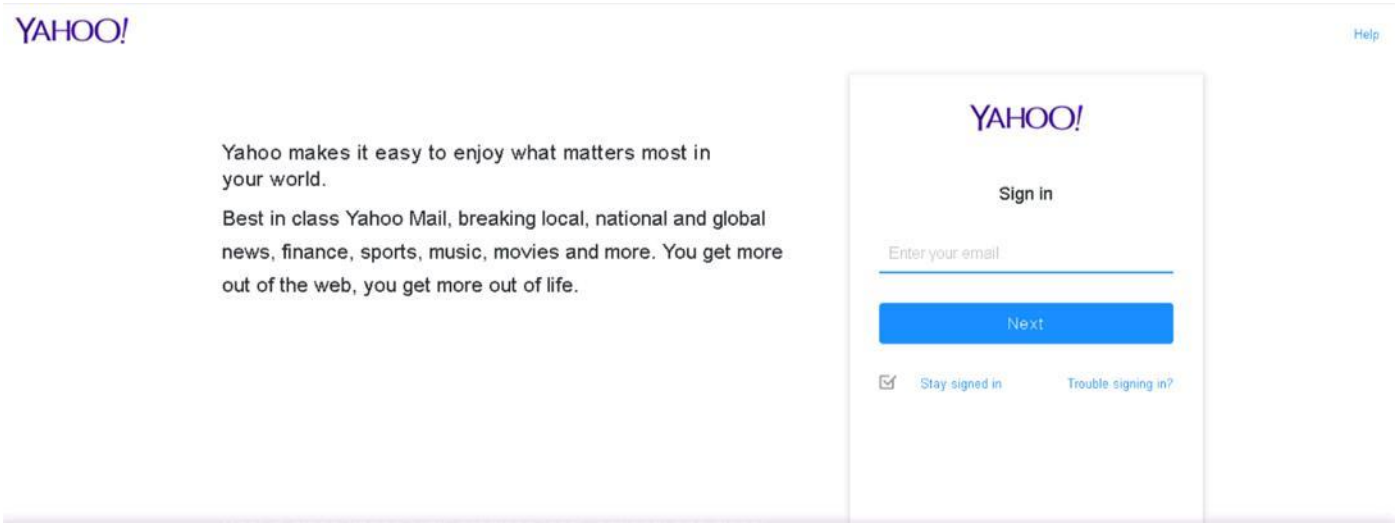
7. [Yahoo メール（Yahoo mail）] カテゴリで [ポリシーに含める（Include in policy）] を選択します。

8. [グローバル設定を上書き（Override Global Settings）] のアクションとして [許可（Allow）] を選択します。

9. 送信し、WSA で変更を確定します。

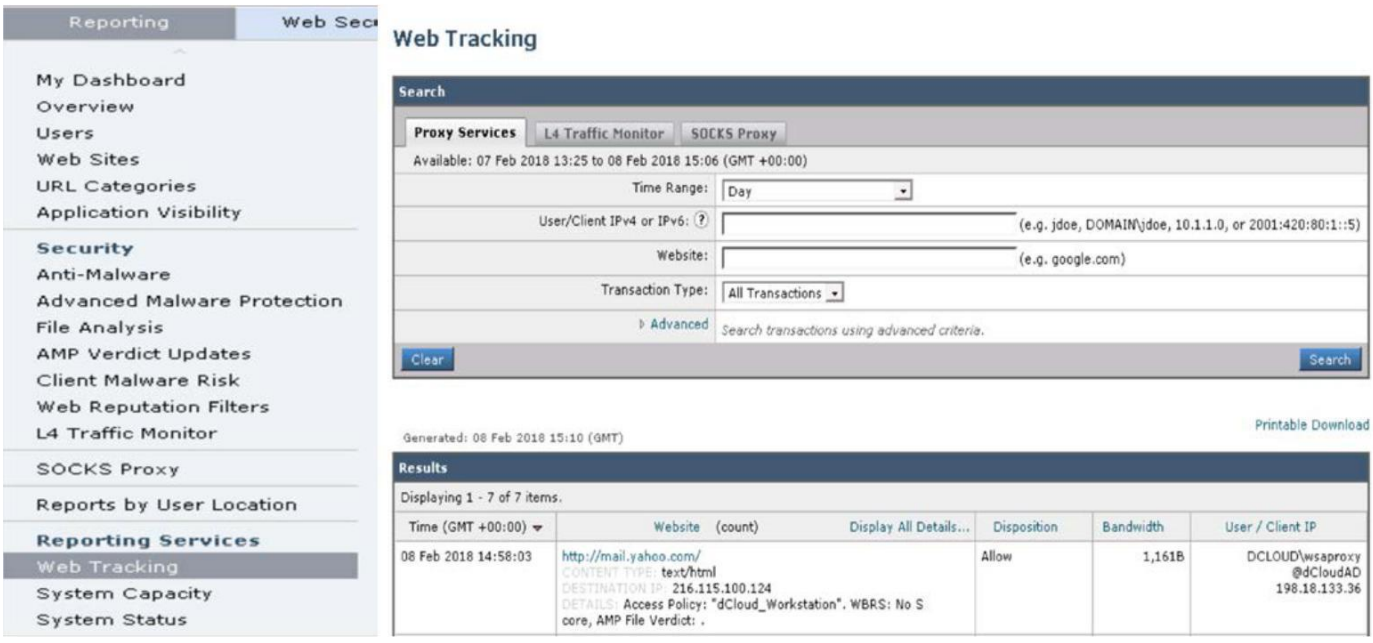


10. Firefox ブラウザから Yahoo メールにアクセスします。



11. WSA PuTTY ログでアクションを確認します。

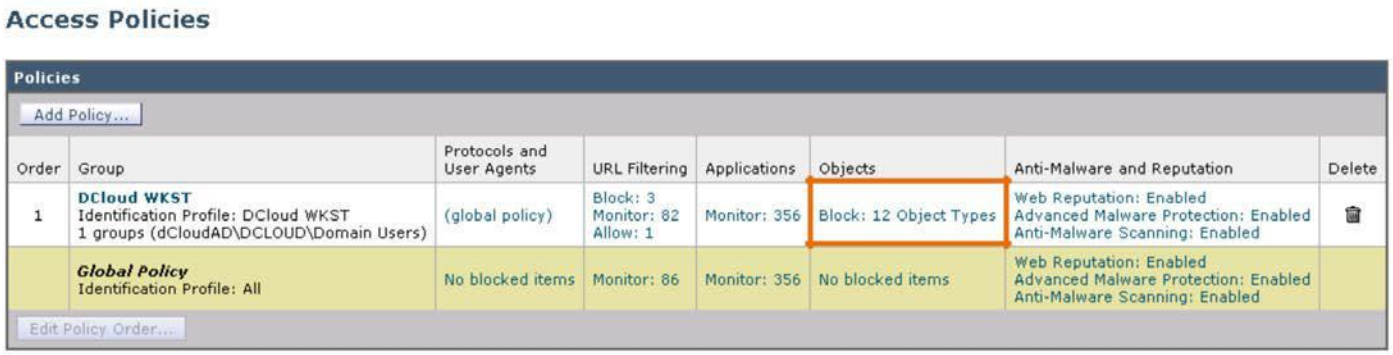
12. または、[Web トラッキング（Web Tracking）] で **mail.yahoo.com** のログを探すこともできます。



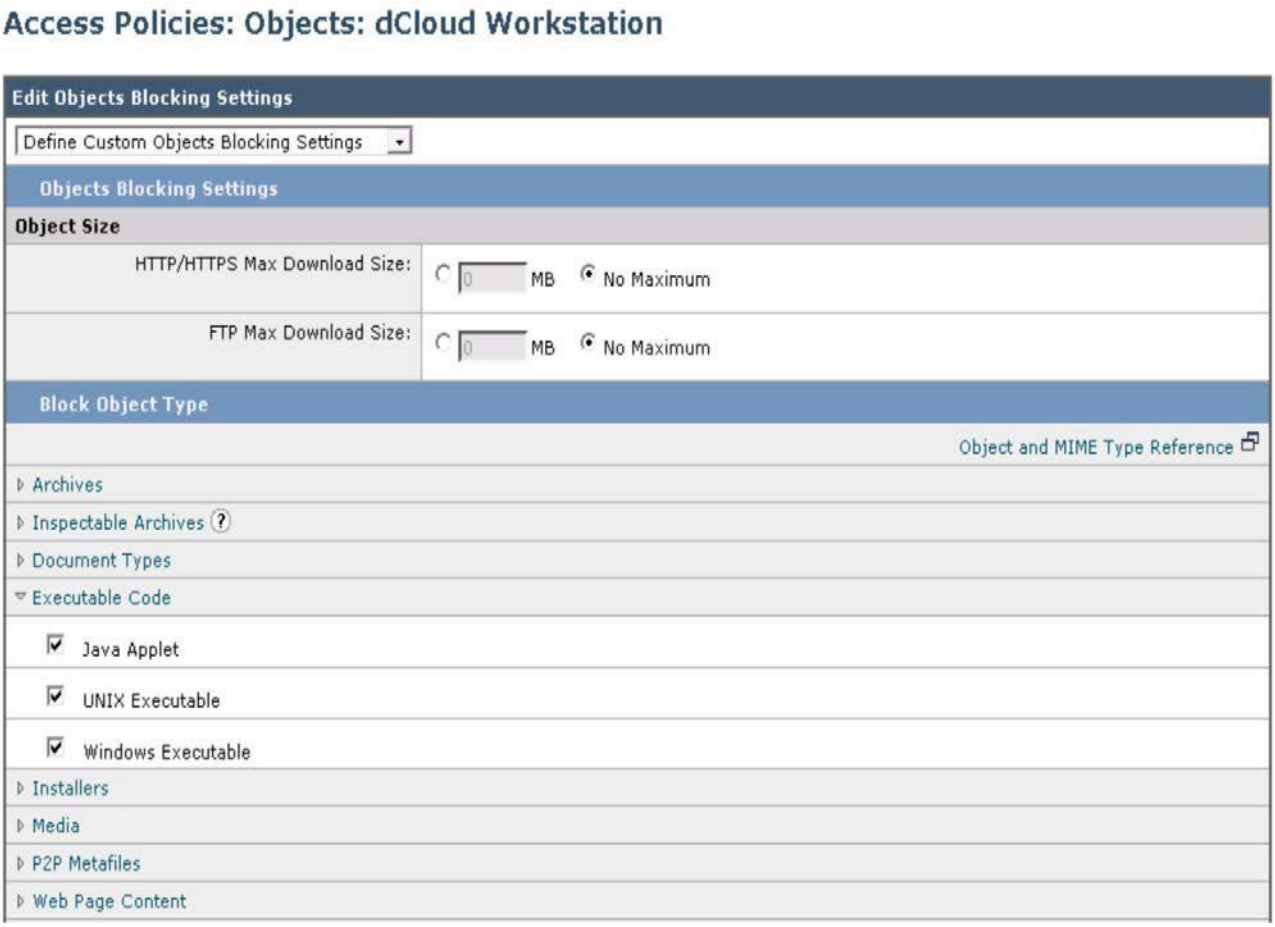
実行可能オブジェクトのブロック

ポリシー チェック

1. dCloud ワークステーションの [アクセスポリシー（Access Policy）] で**実行可能**オブジェクトがブロックされていることを確認します。

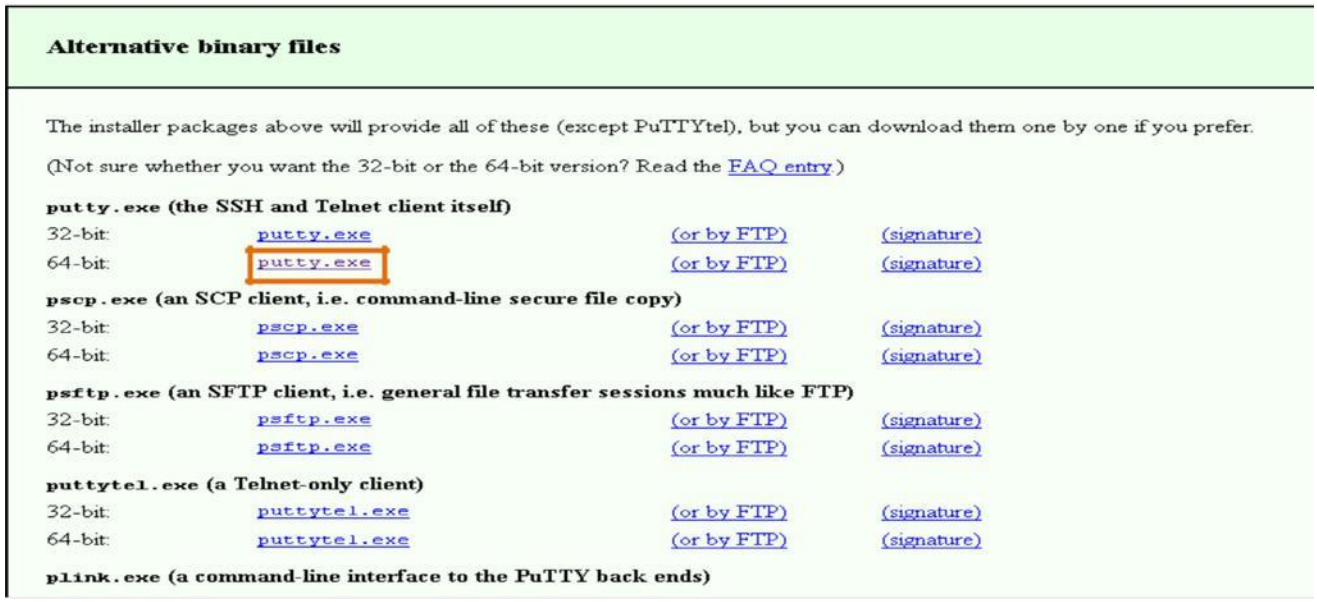


2. [オブジェクト（Objects）] > [ブロック：12 のオブジェクトタイプ（Block:12 Object Types）] の順に選択し、[実行可能コード（Executable Code）] の下のファイルがすべて選択されていることを確認します。



3. Firefox のショートカットから、[PuTTY Exe のダウンロード（Putty Exe Download）] をクリックします。

4. この Web サイトから putty.exe ファイルのダウンロードを試みます。



Alternative binary files

The installer packages above will provide all of these (except PuTTYtel), but you can download them one by one if you prefer.

(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

putty.exe (the SSH and Telnet client itself)

32-bit:	putty.exe	(or by FTP)	(signature)
64-bit:	putty.exe	(or by FTP)	(signature)

pscp.exe (an SCP client, i.e. command-line secure file copy)

32-bit:	pscp.exe	(or by FTP)	(signature)
64-bit:	pscp.exe	(or by FTP)	(signature)

psftp.exe (an SFTP client, i.e. general file transfer sessions much like FTP)

32-bit:	psftp.exe	(or by FTP)	(signature)
64-bit:	psftp.exe	(or by FTP)	(signature)

puttytel.exe (a Telnet-only client)

32-bit:	puttytel.exe	(or by FTP)	(signature)
64-bit:	puttytel.exe	(or by FTP)	(signature)

plink.exe (a command-line interface to the PuTTY back ends)

5. エンド ユーザ通知が表示され、トランザクションがブロックされます。

This Page Cannot Be Displayed

Based on your organization's access policies, access to this web site or download (https://the.earth.li/~sgtatham/putty/0.70/w64/putty.exe) has been blocked because the file type "application/x-dosexec" is not allowed.

If you have questions, please contact your organization's network administrator and provide the codes shown below.

Date: Thu, 08 Feb 2018 15:56:46 GMT
Username: DCLOUD\wsaproxy@dCloudAD
Source IP: 198.18.133.36
URL: GET https://the.earth.li/~sgtatham/putty/0.70/w64/putty.exe
Category: Computers and Internet
Reason: BLOCK-TYPE
Notification: FILE_TYPE

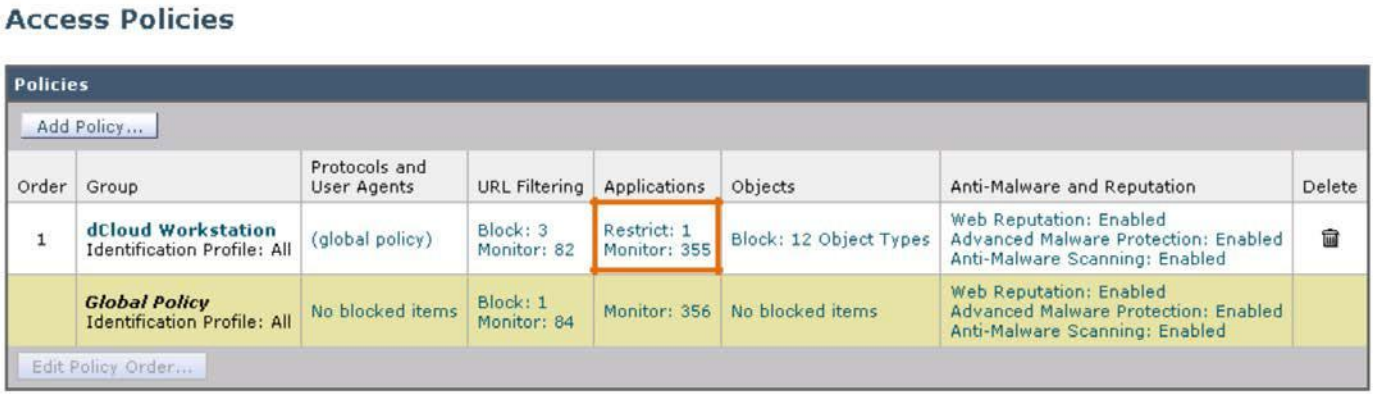
6. PuTTY でアクセス ログをスクロールします。putty.exe がブロックされていることを確認します。

```
1518105439.762 1105 198.18.133.36 TCP_DENIED_SSL/403 0 GET https://the.earth.li:443/~sgtatham/putty/0.70/w64/putty.exe "DCLOUD\wsaproxy@dCloudAD" DIRECT/the.
earth.li application/x-dosexec BLOCK_ADMIN_FILE_TYPE 2-dCloud_Workstation-Dcloud_AD-NONE-NONE-NONE-DefaultGroup <IW_comp,-5.9,0,"-",0,0,0,-,"-",-,-,-,"-",-,
-,"-","-",-,-,IW_comp,-,"-","othermalware","Unknown","Unknown","-","-",0.00,0,-,"Unknown","-",-,"-",-,-,"-","-",-,-,"-"> -
```

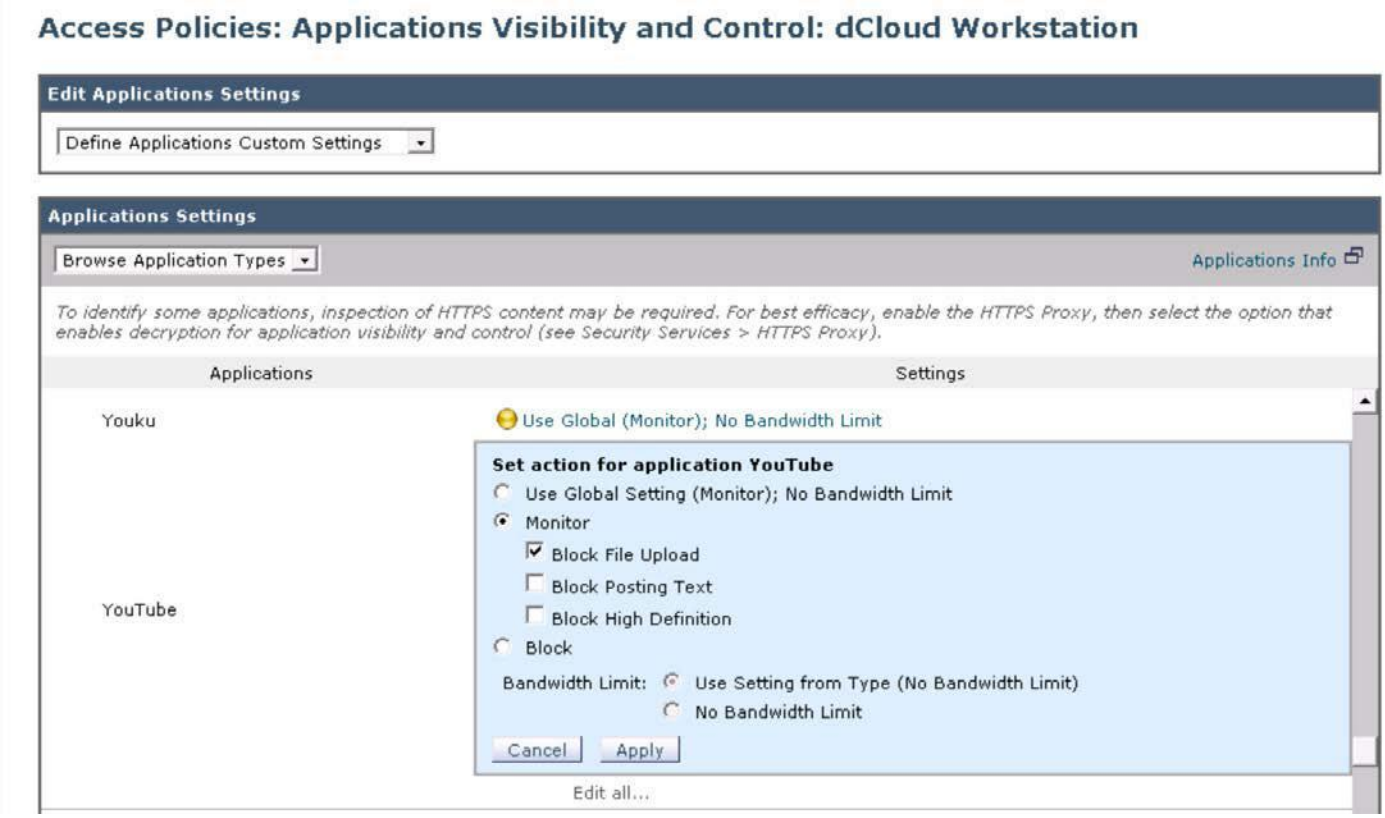
アプリケーションと可視性の制御、トラッキング、レポート

ポリシー チェック

1. dCloud ワークステーションの [アクセスポリシー（Access Policy）] で、[1 つの制限アプリケーション（1 Restrict Application）] をクリックします。



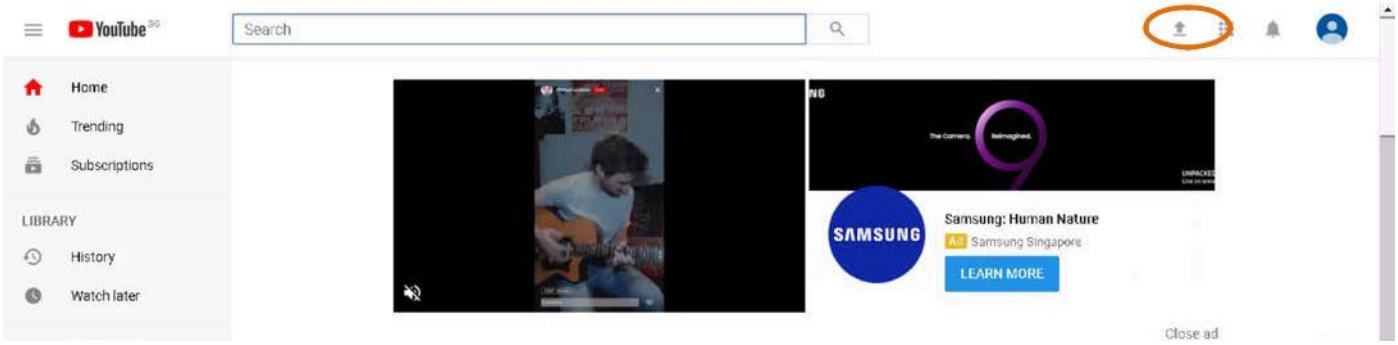
2. [アプリケーション（Applications）] で [メディア（Media）] > [YouTube] までスクロールします。



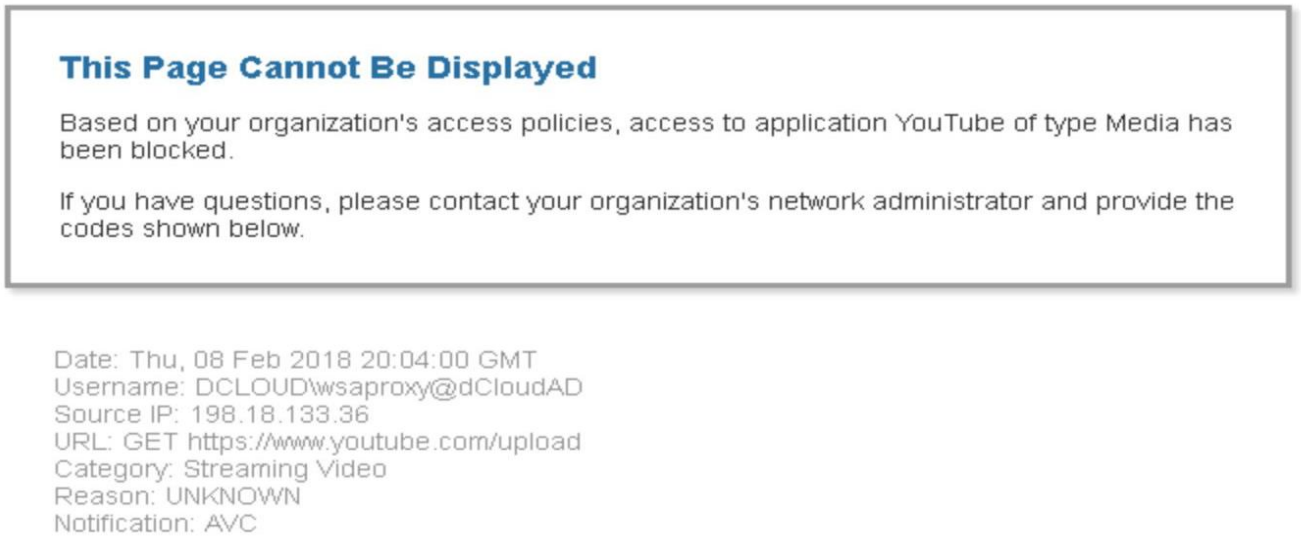
3. [ファイルアップロードをブロック（Block File Upload）] が選択されていることを確認します。

4. Firefox ブラウザの [YouTube] ショートカットをクリックします。

5. [アップロード（Upload）] ボタンをクリックします。



6. AVC コントロールによってアップロードがブロックされていることを確認します。

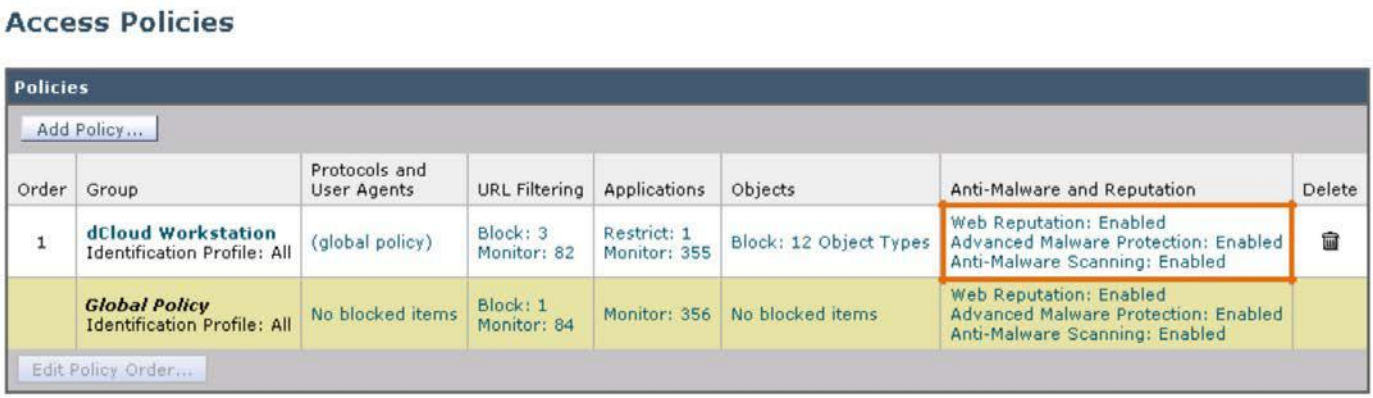


7. [Web トラッキング（Web Tracking）] のレポートの表示を確認します。

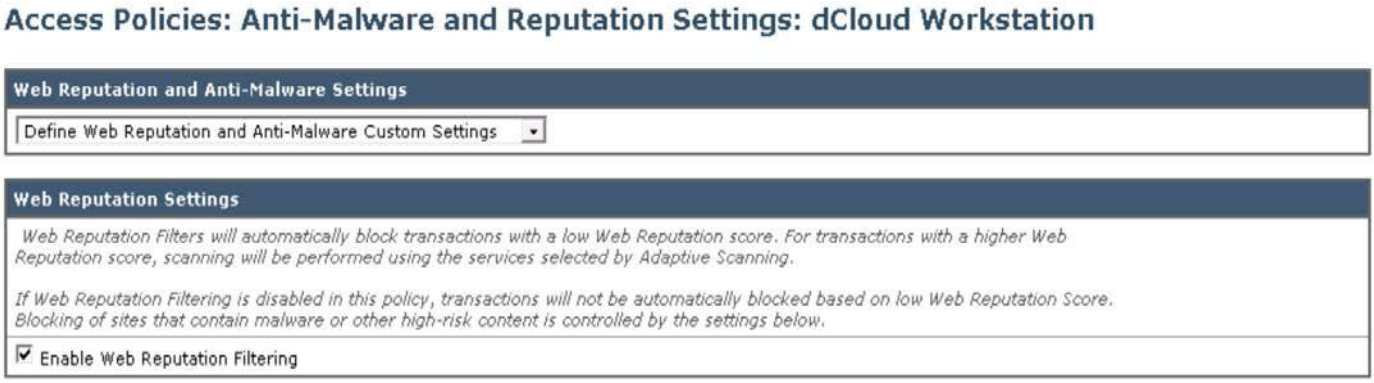
08 Feb 2018 20:04:00	https://www.youtube.com:443/upload CONTENT TYPE: - DESTINATION IP: - DETAILS: Access Policy: "dCloud_Workstation". Application: Media "YouTube", Behavior: Upload, WBRS: 8.0, AMP File Verdict: .	Block - Policy	0B	DCLOUD\wsaproxy @dCloudAD 198.18.133.36

Web レピュテーション、ウイルス対策、Advance Malware Protection（AMP）エンジンによるマルウェア防御

1. dCloud ワークステーションの [アクセスポリシー（Access Policy）] で [マルウェア対策（Anti-Malware）] と [Web レピュテーション（Web Reputation）] が有効になっていることを確認します。

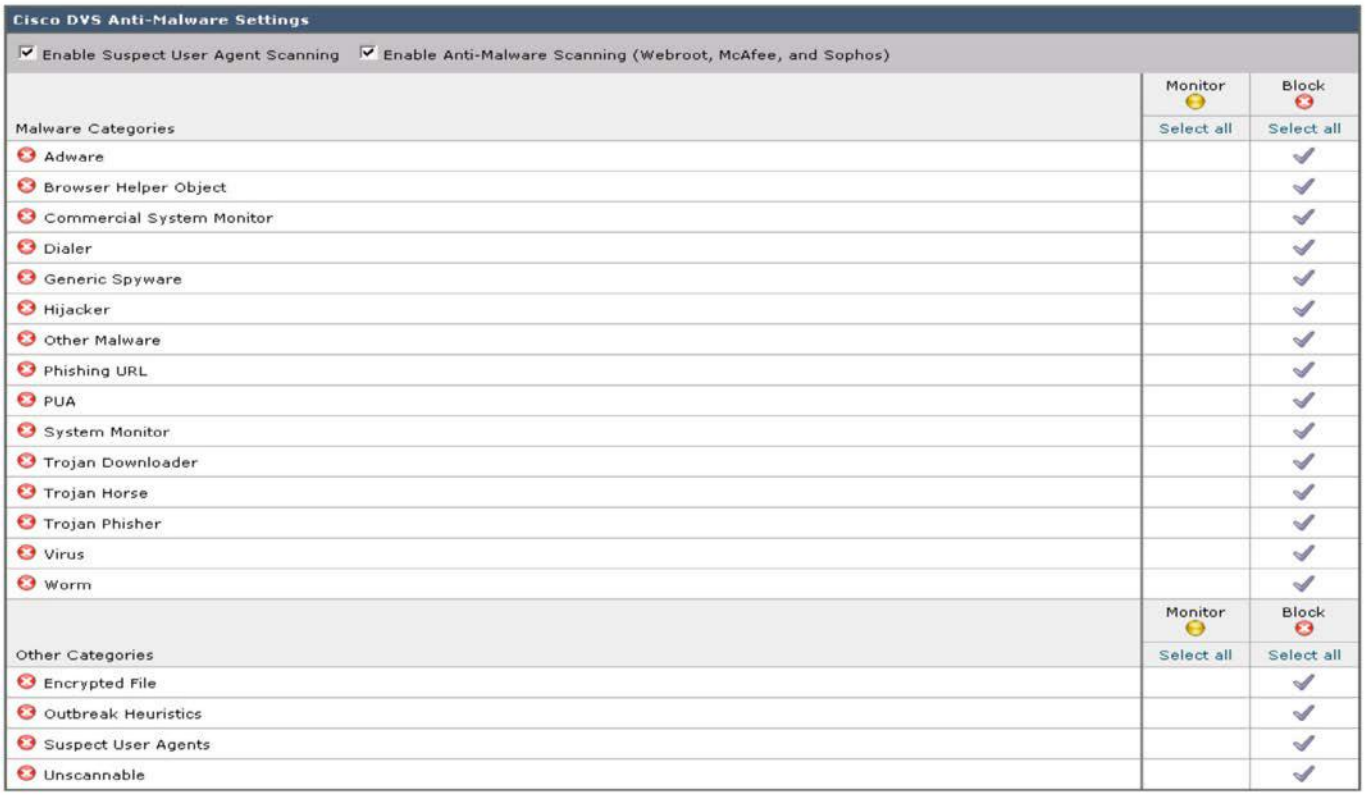


2. [Web レピュテーション：有効（Web Reputation: Enabled）] をクリックして、[Web レピュテーションフィルタを有効にする（Enable Web Reputation Filtering）] が選択されていることを確認します。



3. さらに、Advance Malware Protection（AMP）も有効化されブロックに設定されているかどうか確認します。

4. 最後に、すべてのウイルス対策マルウェア カテゴリがブロックに設定されていることを確認します。



Cisco DVS Anti-Malware Settings

Enable Suspect User Agent Scanning Enable Anti-Malware Scanning (Webroot, McAfee, and Sophos)

Malware Categories	Monitor Select all	Block Select all
Adware		✓
Browser Helper Object		✓
Commercial System Monitor		✓
Dialer		✓
Generic Spyware		✓
Hijacker		✓
Other Malware		✓
Phishing URL		✓
PUA		✓
System Monitor		✓
Trojan Downloader		✓
Trojan Horse		✓
Trojan Phisher		✓
Virus		✓
Worm		✓
Other Categories	**Monitor Select all**	**Block Select all**
Encrypted File		✓
Outbreak Heuristics		✓
Suspect User Agents		✓
Unscannable		✓

5. Firefox ブラウザの [Google.com.com] ショートカットをクリックします。

6. Web レピュテーションによって、ページがブロックされます。

This Page Cannot Be Displayed

Based on your organization's access policies, this web site (http://rk.revolvermaps.com/j/g.jar) has been blocked because it has been determined by Web Reputation Filters to be a security threat to your computer or the organization's network. This web site has been associated with malware/spyware.

If you have questions, please contact your organization's network administrator and provide the codes shown below.

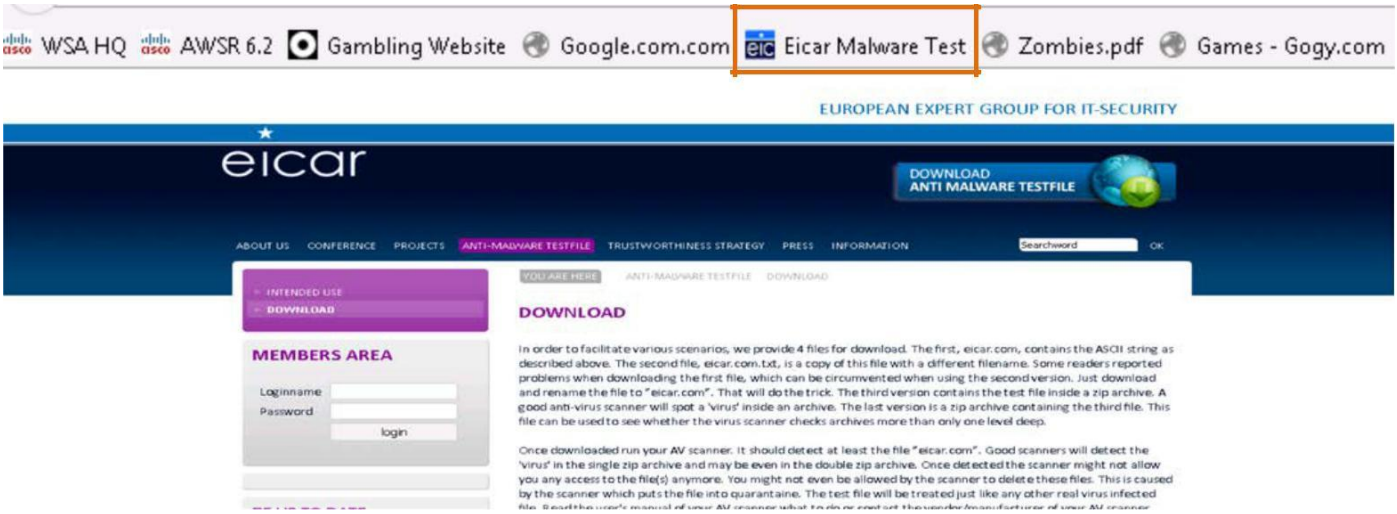
Date: Mon, 05 Mar 2018 18:36:50 +08
Username: DCLOUD\wsaproxy@dCloudAD
Source IP: 198.18.133.36
URL: GET http://rk.revolvermaps.com/j/g.jar
Category: Reference
Reason: BLOCK-MALWARE
Threat Type: othermalware
Threat Reason: Researchers or users identified possible threats. Domain reported and verified as serving malware. Domain is associated with risky or offensive content.
Notification: WBRS

7. [Web レポート（Web Reporting）] では、ブロックされている URL/ドメインのユーザと Web レピュテーション スコアを追跡できます。

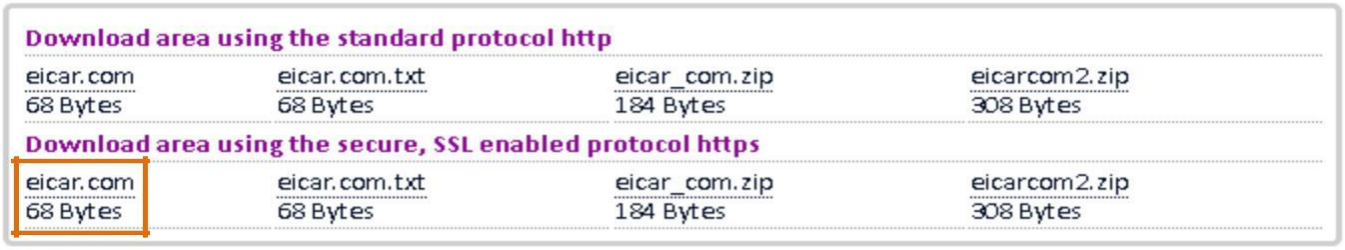
Time (GMT +08:00)	Website (count) Hide All Details...	Disposition	Bandwidth	User / Client IP
05 Mar 2018 18:36:50	http://rk.revolvermaps.com/j/g.jar CONTENT TYPE: - URL CATEGORY: Reference DESTINATION IP: - DETAILS: Access Policy: "DCloud_WKST", WBRS: -8.6, WBRS Threat: othermalware, WBRS Threat Reason: Researchers or users identified possible threats. Domain reported and verified as serving malware. Domain is associated with risky or offensive content., AMP File Verdict: .	Block - WBRS: -8.6	0B	DCLOUD\wsaproxy @dCloudAD 198.18.133.36

ウイルス対策またはマルウェア対策

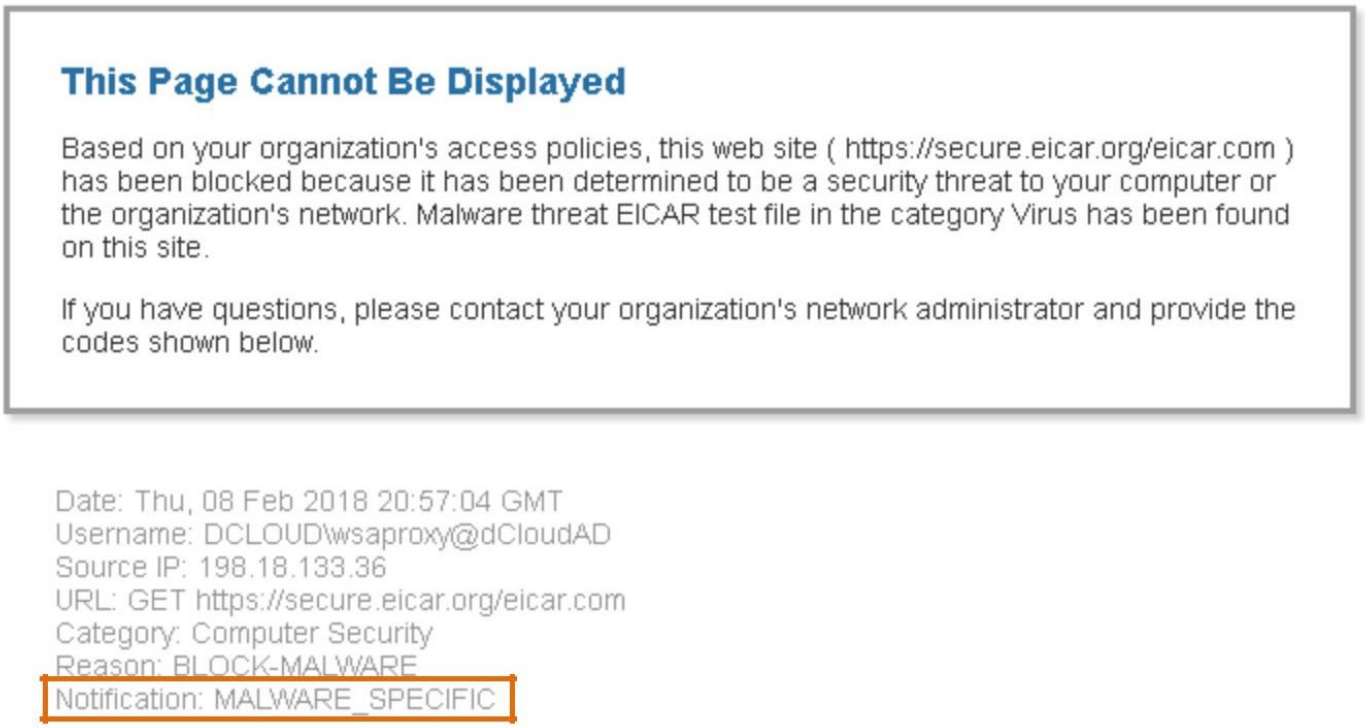
8. Firefox ブラウザの [Eicar Malware Test] ショートカットをクリックします。



9. 最下部までスクロールすると、マルウェア テスト ファイルについて、すべてのファイルがテストされることになっているのがわかります。



10. すべてのマルウェア ファイルがブロックされることを確認します。



11. [Web レポート（Web Reporting）] では、適切なマルウェア カテゴリのユーザとマルウェア対策を追跡できます。

Generated: 08 Feb 2018 21:05 (GMT)

Printable Download

Results

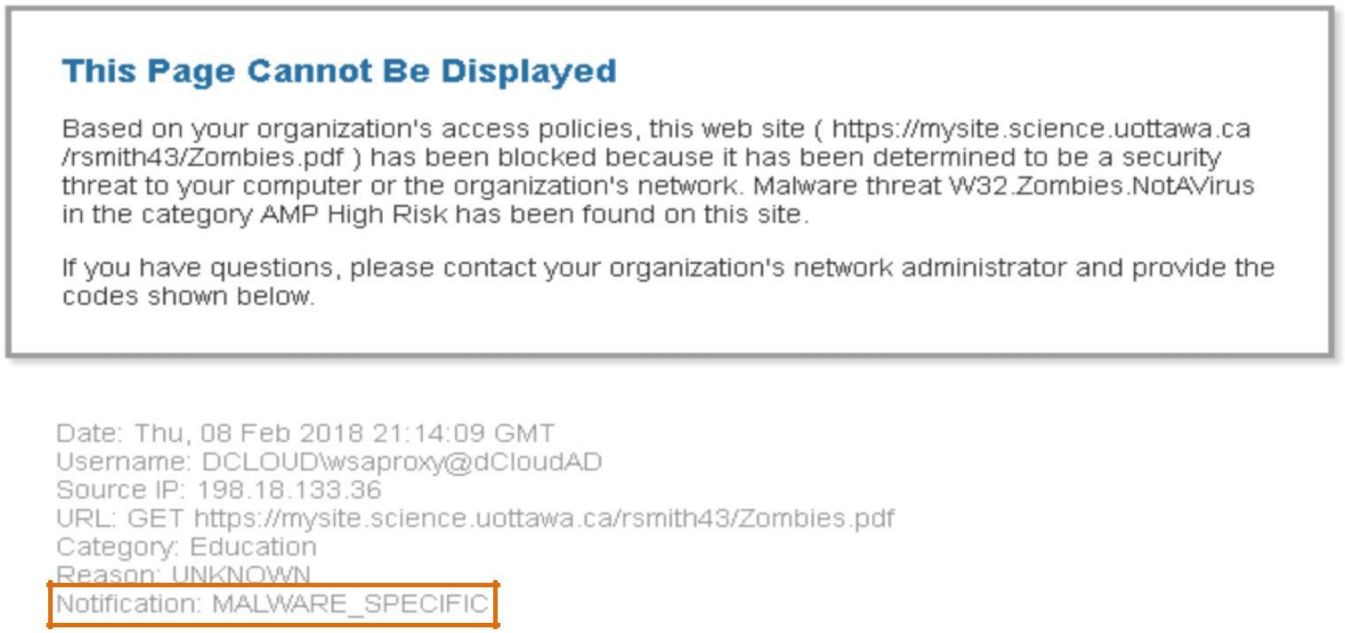
Displaying 1 - 5 of 5 items.

Time (GMT +00:00)	Website (count) Display All Details...	Disposition	Bandwidth	User / Client IP
08 Feb 2018 05:50:32	https://secure.eicar.org:443	Block - Response AMW	0B	wsaproxy 198.18.133.36
08 Feb 2018 05:42:43	https://secure.eicar.org:443	Block - Response AMW	0B	wsaproxy 198.18.133.36
07 Feb 2018 13:27:43	https://secure.eicar.org:443	Block - Response AMW	0B	wsaproxy 198.18.133.36
07 Feb 2018 13:27:33	https://secure.eicar.org:443/eicar.com.txt (2) CONTENT TYPE: application/octet-stream DESTINATION IP: 213.211.198.58 DETAILS: Access Policy: "DefaultGroup". Malware Category: Virus, Malware Threat: EICAR test file, WBRS: 1.5, AMP File Verdict: . ▷ RELATED TRANSACTIONS	Block - Response AMW	0B	DCLOUD\wsaproxy @dCloudAD 198.18.133.36
08 Feb 2018 20:57:04	https://secure.eicar.org:443	Block - Response AMW	0B	wsaproxy 198.18.133.36

Displaying 1 - 5 of 5 items.

12. Firefox ブラウザの [Zombies.pdf] ショートカットをクリックします。

13. このページがブロックされていることを確認します。



14. このファイルが Advance Malware Protection（AMP）エンジンによってブロックされていることが強調表示されます。