

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](#)
- [このソリューションについて](#)
- [トポロジ](#)
- [はじめに](#)
- [シナリオ 1: WSA - スタンドアロン \(明示型モード\)](#)
- [シナリオ 2: Advanced Web Security Reporting \(AWSR\)](#)

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 |
|--|---|
| <ul style="list-style-type: none"> • ラップトップ | <ul style="list-style-type: none"> • 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 | アドバンスド 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: **dcloudwsaproxy**、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。

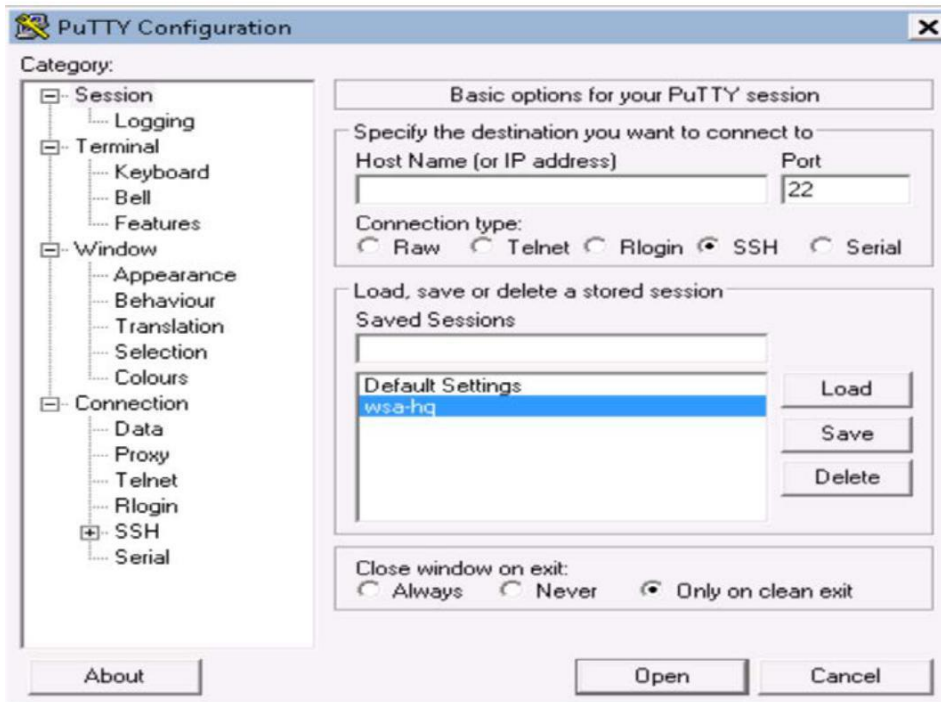
| System Overview | |
|---|--|
| Overview > Web Proxy Traffic Characteristics | Overview > System Resource Utilization |
| Average transactions per second in past minute: 0 | CPU: 34.6% |
| Average bandwidth (bps) in past minute: 0 | RAM: 68.3% |
| Average response time (ms) in past minute: 0 | Reporting / logging disk: 8.0% |
| Total current connections: 0 | |

| Overview > Web Proxy Summary | |
|------------------------------|------|
| Suspect Transactions | 3.9% |
| Transactions | 47 |

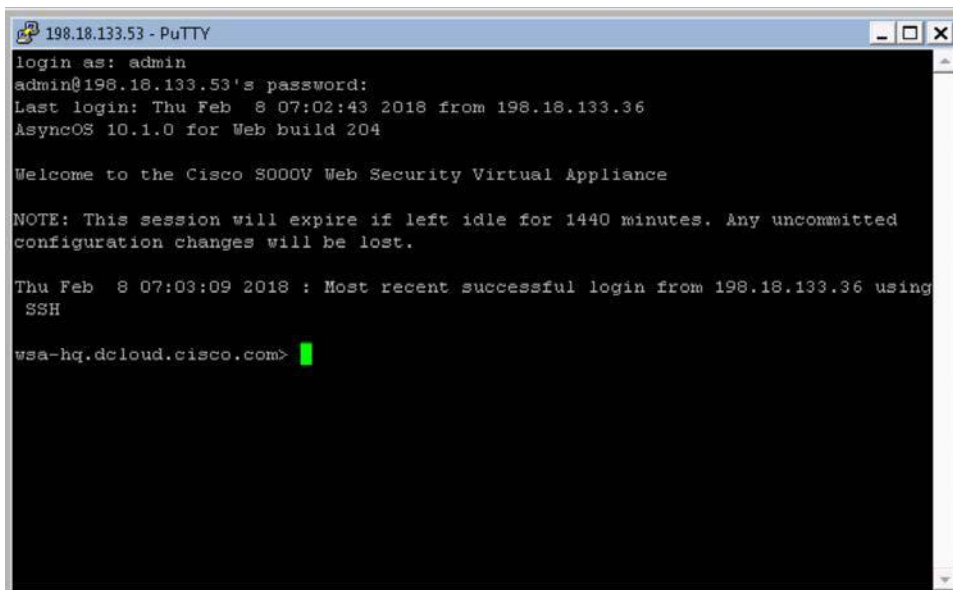
4. タスクバーのショートカットから WSA の PuTTY クライアントにログインします。



5. wsa-hq というショートカットをクリックします。



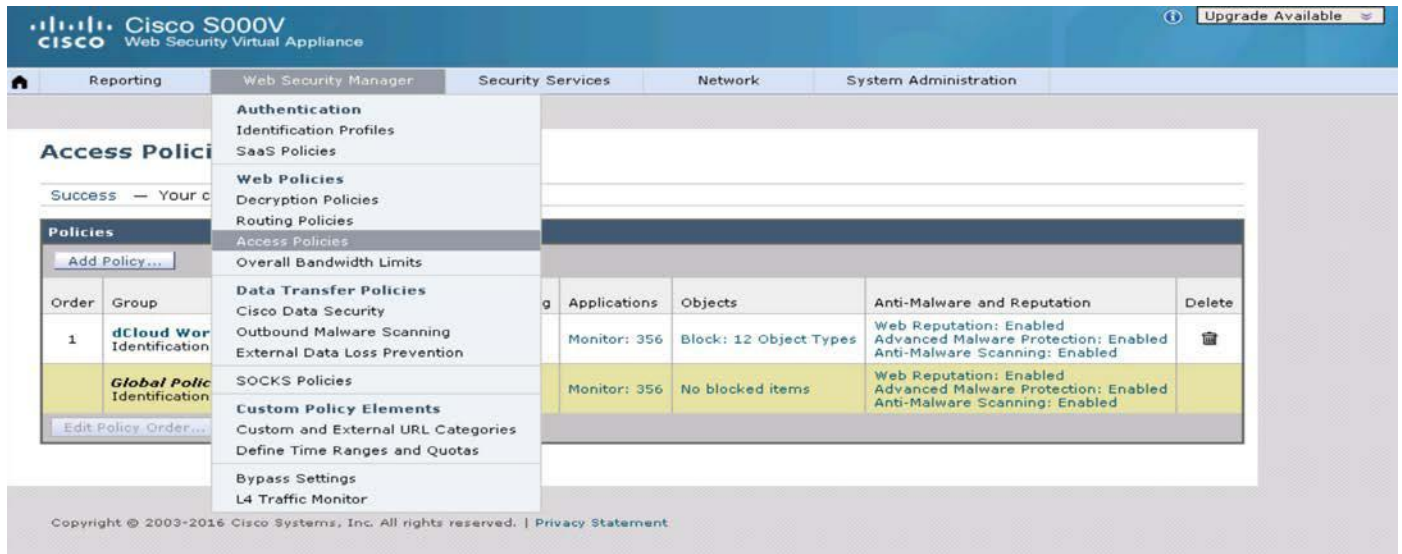
6. ユーザ名:admin、パスワード:C1sco12345 でログインします。



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。

Access Policies

| Order | Group | Protocols and User Agents | URL Filtering | Applications | Objects | Anti-Malware and Reputation | Delete |
|-------|--|---------------------------|-------------------------|--------------|------------------------|---|--------|
| 1 | DCloud WKST Identification Profile: DCloud WKST 1 groups (dCloudAD\DCLLOUD\Domain Users) | (global policy) | Block: 3 Monitor: 82 | Monitor: 356 | Block: 12 Object Types | Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled | |
| | Global Policy Identification Profile: All | No blocked items | Monitor: 86 | Monitor: 356 | No blocked items | Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled | |

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。

| Category | Use Global Settings | Override Global Settings | | | | |
|------------------------|---------------------|--------------------------|---------|----------|---------------|---------------|
| | | Block | Monitor | Warn (?) | Quota-Based | Time-Based |
| Extreme | Select all | | ✓ | | (Unavailable) | (Unavailable) |
| Fashion | | | ✓ | | (Unavailable) | (Unavailable) |
| File Transfer Services | | | ✓ | | (Unavailable) | (Unavailable) |
| Filter Avoidance | | | ✓ | | (Unavailable) | (Unavailable) |
| Finance | | | ✓ | | (Unavailable) | (Unavailable) |
| Freeware and Shareware | | | ✓ | | (Unavailable) | (Unavailable) |
| Gambling | | ✓ | | | (Unavailable) | (Unavailable) |
| Games | | ✓ | | | (Unavailable) | (Unavailable) |
| Government and Law | | | ✓ | | (Unavailable) | (Unavailable) |
| Hacking | | | ✓ | | (Unavailable) | (Unavailable) |
| Hate Speech | | | ✓ | | (Unavailable) | (Unavailable) |
| Web-based Email | | ✓ | | | (Unavailable) | (Unavailable) |

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。



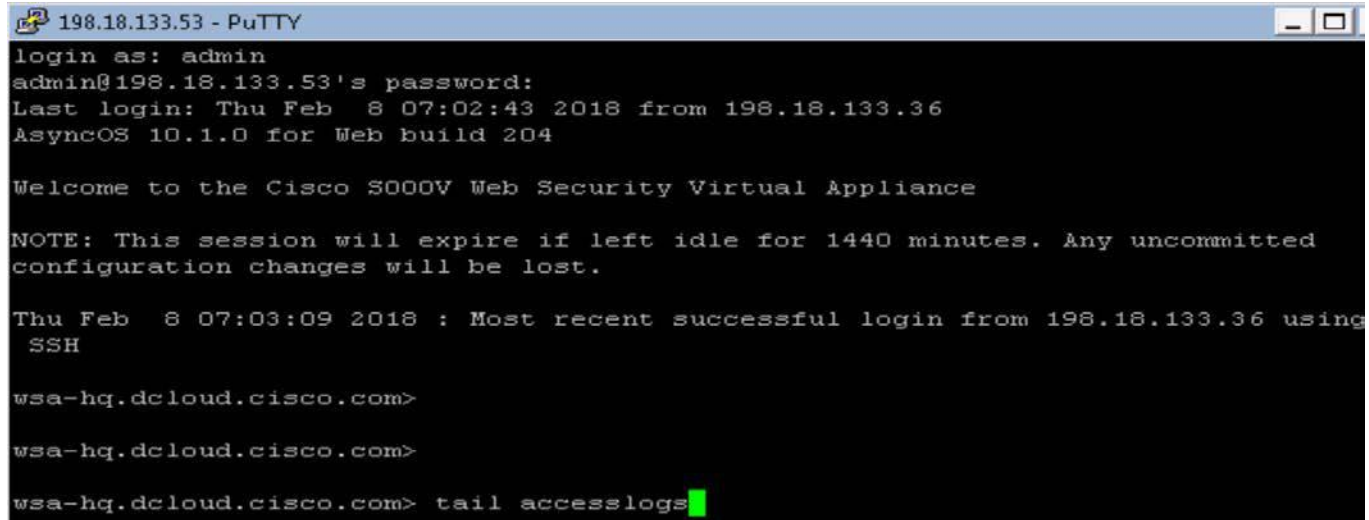
This Page Cannot Be Displayed

Based on your organization's access policies, access to this web site (http://armorgames.com/) has been blocked because the web category "Games" is not allowed.

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

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 Tracking

Search

Proxy Services L4 Traffic Monitor SOCKS Proxy

Available: 05 Mar 2018 17:13 to 05 Mar 2018 18:04 (GMT +08:00)

Time Range: Hour

User/Client IPv4 or IPv6: (e.g. jdoe, DOMAIN\jdoe, 10.1.1.0, or 2001:420:80:1::5)

Website: (e.g. google.com)

Transaction Type: All Transactions

Advanced Search transactions using advanced criteria.

Clear Search

Generated: 05 Mar 2018 18:08 (GMT +08:00) Printable Download

Results

Displaying 1 - 2 of 2 items.

| Time (GMT +08:00) | Website (count) | Hide All Details... | Disposition | Bandwidth | User / Client IP |
|----------------------|---|---------------------|-----------------|-----------|--|
| 05 Mar 2018 18:04:47 | http://armorgames.com/ CONTENT TYPE: - URL CATEGORY: Games DESTINATION IP: - DETAILS: Access Policy: "DCloud_WKST", WBR: 4.9, AMP F ile Verdict: . | | Block - URL Cat | 0B | DCLLOUD\wsaproxy@dCloudAD 198.18.133.36 |

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。



This Page Cannot Be Displayed

Based on your organization's access policies, access to this web site (http://mail.yahoo.com/) has been blocked because the web category "Web-based Email" 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 10:39:59 GMT
 Username: DCLLOUDwsaproxy@dCloudAD
 Source IP: 198.18.133.36
 URL: GET http://mail.yahoo.com/
 Category: Web-based Email
 Reason: BLOCK-WEBCAT
 Notification: WEBCAT

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

Access Policies

| Policies | | | | | | | |
|----------|---|---------------------------|-------------------------|--------------|------------------------|---|--------|
| Order | Group | Protocols and User Agents | URL Filtering | Applications | Objects | Anti-Malware and Reputation | Delete |
| 1 | DCloud WKST Identification Profile: DCloud WKST 1 groups (dCloudAD\DCLLOUD\Domain Users) | (global policy) | Block: 3 Monitor: 82 | Monitor: 356 | Block: 12 Object Types | Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled | |
| | Global Policy Identification Profile: All | No blocked items | Monitor: 86 | Monitor: 356 | No blocked items | Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled | |

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。

Access Policies: URL Filtering: dCloud Workstation

Custom and External URL Category Filtering

No Custom Categories are included for this Policy.

Select Custom Categories...

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。

Select Custom Categories for this Policy

| Category | Category Type | Setting Selection |
|------------|----------------|-------------------|
| yahoo mail | Custom (Local) | Include in policy |

Cancel Apply

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。

Access Policies: URL Filtering: dCloud Workstation

Custom and External URL Category Filtering

Add, edit, reorder or delete categories in the Custom and External URL Categories list.

| Category | Category Type | Use Global Settings | Override Global Settings | | | | | | |
|------------|----------------|---------------------|--------------------------|------------|------------|------------|------------|---------------|---------------|
| | | | Block | Redirect | Allow ? | Monitor | Warn ? | Quota-Based | Time-Based |
| yahoo mail | Custom (Local) | - | Select all | Select all | Select all | Select all | Select all | (Unavailable) | (Unavailable) |

Select Custom Categories...

Cancel Submit

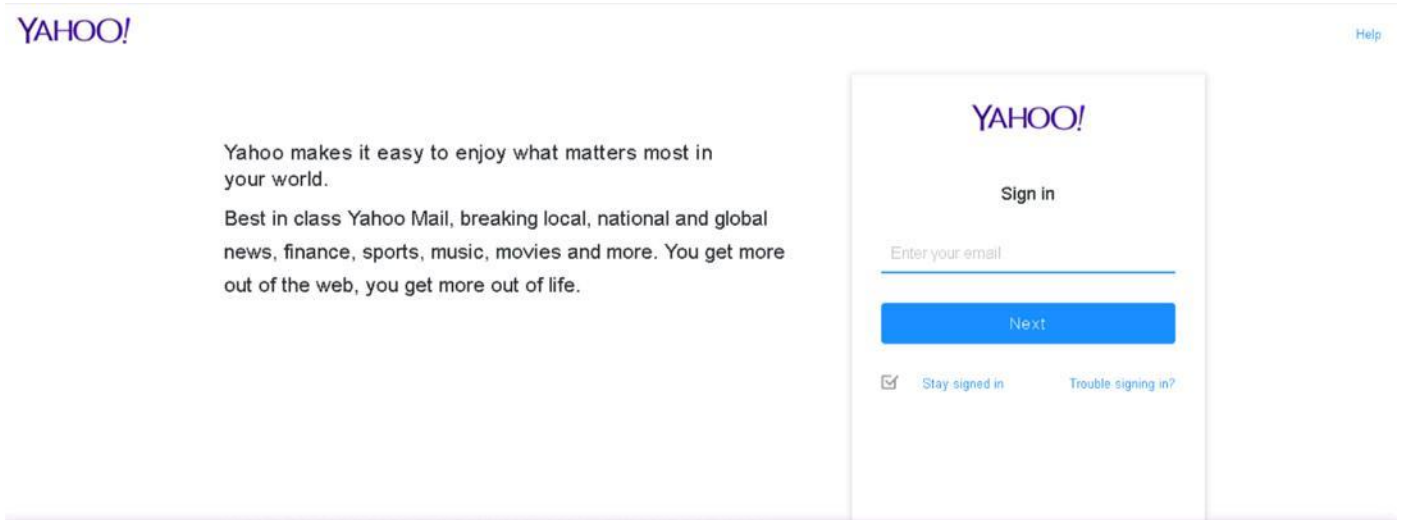
9. 送信し、WSA で変更を確定します。

Access Policies

Success — Your changes have been committed.

| Policies | | | | | | | |
|----------|---|---------------------------|-------------------------------------|--------------|------------------------|---|--------|
| Order | Group | Protocols and User Agents | URL Filtering | Applications | Objects | Anti-Malware and Reputation | Delete |
| 1 | DCloud WKST Identification Profile: DCloud WKST 1 groups (dCloudAD\DCLLOUD\Domain Users) | (global policy) | Block: 3 Monitor: 82 Allow: 1 | Monitor: 356 | Block: 12 Object Types | Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled | |
| | Global Policy Identification Profile: All | No blocked items | Monitor: 86 | Monitor: 356 | No blocked items | Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled | |

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。

Web Tracking

Search

Proxy Services | L4 Traffic Monitor | SOCKS Proxy

Available: 07 Feb 2018 13:25 to 08 Feb 2018 15:06 (GMT +00:00)

Time Range: Day

User/Client IPv4 or IPv6: (e.g. jdoe, DOMAIN\jdoe, 10.1.1.0, or 2001:420:801:1:5)

Website: (e.g. google.com)

Transaction Type: All Transactions

Advanced Search transactions using advanced criteria.

Clear Search

Generated: 08 Feb 2018 15:10 (GMT) Printable Download

Results

Displaying 1 - 7 of 7 items.

| Time (GMT +00:00) | Website (count) | Display All Details... | Disposition | Bandwidth | User / Client IP |
|----------------------|--|------------------------|-------------|-----------|--|
| 08 Feb 2018 14:58:03 | http://mail.yahoo.com/ CONTENT TYPE: text/html DESTINATION IP: 216.115.100.124 DETAILS: Access Policy: "dCloud_Workstation". WBRAS: No S core, AMP File Verdict: . | | Allow | 1,161B | DCLLOUD\wsaproxy@dCloudAD 198.18.133.36 |

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。

Access Policies

| Policies | | | | | | | |
|----------|---|---------------------------|-------------------------------------|--------------|-------------------------------|---|--------|
| Order | Group | Protocols and User Agents | URL Filtering | Applications | Objects | Anti-Malware and Reputation | Delete |
| 1 | DCloud WKST Identification Profile: DCloud WKST 1 groups (dCloudAD\DCLLOUD\Domain Users) | (global policy) | Block: 3 Monitor: 82 Allow: 1 | Monitor: 356 | Block: 12 Object Types | Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled | |
| | Global Policy Identification Profile: All | No blocked items | Monitor: 86 | Monitor: 356 | No blocked items | Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled | |

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。

Access Policies: Objects: dCloud Workstation

| Edit Objects Blocking Settings | |
|--|---|
| Define Custom Objects Blocking Settings ▾ | |
| Objects Blocking Settings | |
| Object Size | |
| HTTP/HTTPS Max Download Size: | <input type="text" value="0"/> MB <input checked="" type="radio"/> No Maximum |
| FTP Max Download Size: | <input type="text" value="0"/> MB <input checked="" type="radio"/> No Maximum |
| Block Object Type | |
| Object and MIME Type Reference | |
| ▸ Archives | |
| ▸ Inspectable Archives [?] | |
| ▸ Document Types | |
| ▾ Executable Code | |
| <input checked="" type="checkbox"/> | Java Applet |
| <input checked="" type="checkbox"/> | UNIX Executable |
| <input checked="" type="checkbox"/> | Windows Executable |
| ▸ Installers | |
| ▸ Media | |
| ▸ P2P Metabytes | |
| ▸ Web Page Content | |

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: D\CLOUD\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。

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。

Access Policies

| Policies | | | | | | | |
|----------------------|---|---------------------------|-------------------------|-----------------------------|------------------------|---|--------|
| Add Policy... | | | | | | | |
| Order | Group | Protocols and User Agents | URL Filtering | Applications | Objects | Anti-Malware and Reputation | Delete |
| 1 | dCloud Workstation Identification Profile: All | (global policy) | Block: 3 Monitor: 82 | Restrict: 1 Monitor: 355 | Block: 12 Object Types | Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled | |
| | Global Policy Identification Profile: All | No blocked items | Block: 1 Monitor: 84 | Monitor: 356 | No blocked items | Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled | |
| Edit Policy Order... | | | | | | | |

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。

Access Policies: Applications Visibility and Control: dCloud Workstation

Edit Applications Settings

Define Applications Custom Settings

Applications Settings

Browse Application Types

Applications Info

To identify some applications, inspection of HTTPS content may be required. For best efficacy, enable the HTTPS Proxy, then select the option that enables decryption for application visibility and control (see Security Services > HTTPS Proxy).

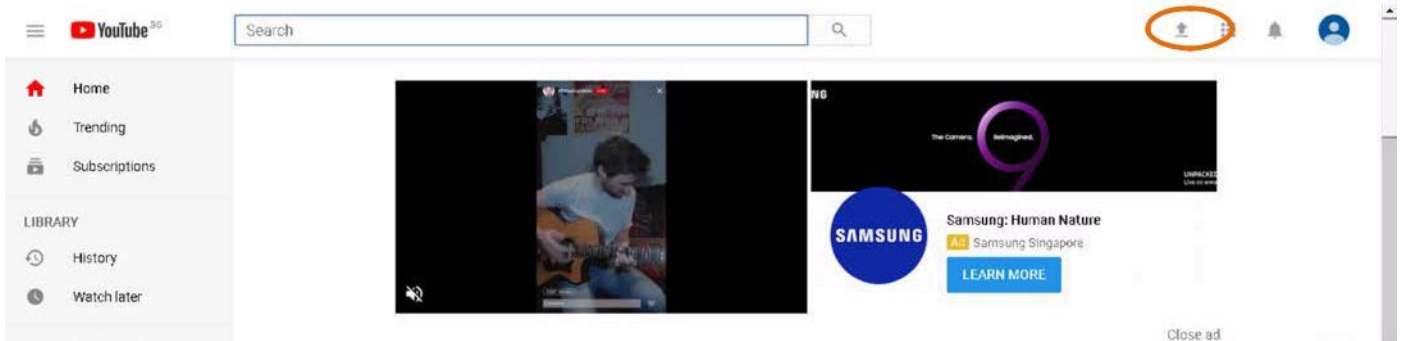
| Applications | Settings |
|--------------|--|
| Youku | <input checked="" type="radio"/> Use Global (Monitor); No Bandwidth Limit |
| YouTube | <div style="border: 1px solid gray; padding: 5px;"> <p>Set action for application YouTube</p> <p><input type="radio"/> Use Global Setting (Monitor); No Bandwidth Limit</p> <p><input checked="" type="radio"/> Monitor</p> <p><input checked="" type="checkbox"/> Block File Upload</p> <p><input type="checkbox"/> Block Posting Text</p> <p><input type="checkbox"/> Block High Definition</p> <p><input type="radio"/> Block</p> <p>Bandwidth Limit: <input checked="" type="radio"/> Use Setting from Type (No Bandwidth Limit)</p> <p><input type="radio"/> No Bandwidth Limit</p> <p>Cancel Apply</p> </div> |

Edit all...

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。

This Page Cannot Be Displayed

Based on your organization's access policies, access to application YouTube of type Media has been blocked.

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

Date: Thu, 08 Feb 2018 20:04:00 GMT
 Username: DCLLOUD\wsaproxy@dCloudAD
 Source IP: 198.18.133.36
 URL: GET https://www.youtube.com/upload
 Category: Streaming Video
 Reason: UNKNOWN
 Notification: AVC

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 | DCLLOUD\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。

Access Policies

| Policies | | | | | | | |
|---------------|--|---------------------------|-------------------------|-----------------------------|------------------------|---|--------|
| Add Policy... | | | | | | | |
| Order | Group | Protocols and User Agents | URL Filtering | Applications | Objects | Anti-Malware and Reputation | Delete |
| 1 | dCloud Workstation Identification Profile: All | (global policy) | Block: 3 Monitor: 82 | Restrict: 1 Monitor: 355 | Block: 12 Object Types | Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled | |
| | Global Policy Identification Profile: All | No blocked items | Block: 1 Monitor: 84 | Monitor: 356 | No blocked items | Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled | |

Edit Policy Order...

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。

Access Policies: Anti-Malware and Reputation Settings: dCloud Workstation

| Web Reputation and Anti-Malware Settings | |
|---|--|
| Define Web Reputation and Anti-Malware Custom Settings <input type="button" value="v"/> | |
| Web Reputation Settings | |
| <i>Web Reputation Filters will automatically block transactions with a low Web Reputation score. For transactions with a higher Web Reputation score, scanning will be performed using the services selected by Adaptive Scanning.</i> | |
| <i>If Web Reputation Filtering is disabled in this policy, transactions will not be automatically blocked based on low Web Reputation Score. Blocking of sites that contain malware or other high-risk content is controlled by the settings below.</i> | |
| <input checked="" type="checkbox"/> Enable Web Reputation Filtering | |

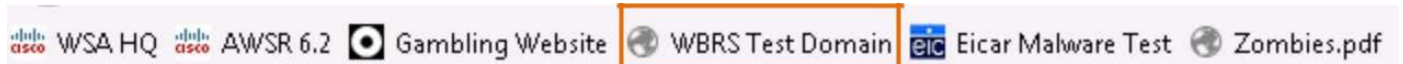
3. さらに、Advance Malware Protection (AMP) も有効化されブロックに設定されているかどうか確認します。

| Advanced Malware Protection Settings | | |
|--|---------|-------------------------------------|
| <input checked="" type="checkbox"/> Enable File Reputation Filtering and File Analysis | | |
| <i>File Reputation Filters will identify transactions containing known malicious or high-risk files. Files that are unknown may be forwarded to the cloud for File Analysis.</i> | | |
| File Reputation | Monitor | Block |
| Known Malicious and High-Risk Files | | <input checked="" type="checkbox"/> |

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 DYS Anti-Malware Settings | | |
|---|------------|-------------------------------------|
| <input checked="" type="checkbox"/> Enable Suspect User Agent Scanning <input checked="" type="checkbox"/> Enable Anti-Malware Scanning (Webroot, McAfee, and Sophos) | | |
| Malware Categories | Monitor | Block |
| | Select all | Select all |
| <input checked="" type="checkbox"/> Adware | | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Browser Helper Object | | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Commercial System Monitor | | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Dialer | | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Generic Spyware | | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Hijacker | | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Other Malware | | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Phishing URL | | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> PUA | | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> System Monitor | | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Trojan Downloader | | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Trojan Horse | | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Trojan Phisher | | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Virus | | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Worm | | <input checked="" type="checkbox"/> |
| Other Categories | Monitor | Block |
| | Select all | Select all |
| <input checked="" type="checkbox"/> Encrypted File | | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Outbreak Heuristics | | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Suspect User Agents | | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Unscannable | | <input checked="" type="checkbox"/> |

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: DCLLOUDwsaproxy@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". WBR S Threat: othermalware, WBR S Threat Reason: Researchers or users identified possible threats. Domain reported and ve rified as serving malware. Domain is associated with risky or offensive content., AMP File Verdict: . | | Block - WBR S: -8.6 | 0B | DCLLOUD\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。

The screenshot shows a Firefox browser window with a bookmark bar containing several items, including 'Eicar Malware Test' which is highlighted with an orange box. Below the browser, the EICAR website is visible, featuring a navigation menu with 'ANTI-MALWARE TESTFILE' selected, a search bar, and a 'DOWNLOAD ANTI-MALWARE TESTFILE' button. A 'MEMBERS AREA' login form is also present on the page.

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。

| Download area using the standard protocol http | | | |
|--|---|--|--|
| eicar.com 68 Bytes | eicar.com.txt 68 Bytes | eicar_com.zip 184 Bytes | eicarcom2.zip 308 Bytes |
| Download area using the secure, SSL enabled protocol https | | | |
| eicar.com 68 Bytes | eicar.com.txt 68 Bytes | eicar_com.zip 184 Bytes | eicarcom2.zip 308 Bytes |

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。

This Page Cannot Be Displayed

Based on your organization's access policies, this web site (<https://secure.eicar.org/eicar.com>) has been blocked because it has been determined to be a security threat to your computer or the organization's network. Malware threat EICAR test file in the category Virus has been found on this site.

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

Date: Thu, 08 Feb 2018 20:57:04 GMT
 Username: DCLLOUD\wsaproxy@dCloudAD
 Source IP: 198.18.133.36
 URL: GET <https://secure.eicar.org/eicar.com>
 Category: Computer Security
 Reason: BLOCK-MALWARE
 Notification: MALWARE_SPECIFIC

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。

[Printable Download](#)

Generated: 08 Feb 2018 21:05 (GMT)

| 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) | Block - Response AMW | 0B | DCLLOUD\wsaproxy@dCloudAD 198.18.133.36 |
| CONTENT TYPE: application/octet-stream DESTINATION IP: 213.211.198.58 DETAILS: Access Policy: "DefaultGroup". Malware Category: Virus, Malware Threat: EICAR test file, WBSR: 1.5, AMP File Verdict: . ▶ RELATED TRANSACTIONS | | | | | |
| 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。

This Page Cannot Be Displayed

Based on your organization's access policies, this web site (<https://mysite.science.uottawa.ca/rsmith43/Zombies.pdf>) has been blocked because it has been determined to be a security threat to your computer or the organization's network. Malware threat W32.Zombies.NotAVirus in the category AMP High Risk has been found on this site.

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

Date: Thu, 08 Feb 2018 21:14:09 GMT
 Username: DCLLOUD\wsaproxy@dCloudAD
 Source IP: 198.18.133.36
 URL: GET <https://mysite.science.uottawa.ca/rsmith43/Zombies.pdf>
 Category: Education
 Reason: UNKNOWN

Notification: MALWARE_SPECIFIC

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。

| | | | | |
|----------------------|--|-------------|----|--|
| 08 Feb 2018 21:14:09 | https://mysite.science.uottawa.ca:443/rsmith43/Zombies.pdf CONTENT TYPE: application/pdf DESTINATION IP: 137.122.152.27 DETAILS: Access Policy: "dCloud_Workstation". WBRs: 1.5, AMP Verdict: Malware, Malware Threat: W32.Zombies.NotAVirus, Filename: Zombies.pdf, SHA256: 00b32c3428362e39e4df2a0c3e0950947c147781fdd3d2ffd0bf5f96989bb002, AMP File Verdict: Malicious. | Block - AMP | 0B | DCLLOUD\wsaproxy@dCloudAD 198.18.133.36 |
|----------------------|--|-------------|----|--|