Web セキュリティ アプライアンス ラボ v1

最終更新日：2018 年 6 月 26 日

このラボについて

このラボは、Web セキュリティ アプライアンスの導入方法を理解し、ASyncOS v10.1 の最新の機能セットを確認できるように作成されています。ここでは、Cisco Web セキュリティ アプライアンスのさまざまな機能を制御するポリシーの設定、管理およびレポート作成を行います。典型的な導入に基づいた、一般的な設定、トラブルシューティング、レポート作成の演習となっており、アクセプタブル ユース ポリシー、Web セキュリティ、アプリケーションの可視性、オンボックスのレポート作成といった機能がカバーされています。ラボ参加者は、3 時間の制限時間内にラボを完了できるようにしてください。このラボでは、シナリオ 11 を除くすべてのタスクを **WSA-HQ1** で実行します。

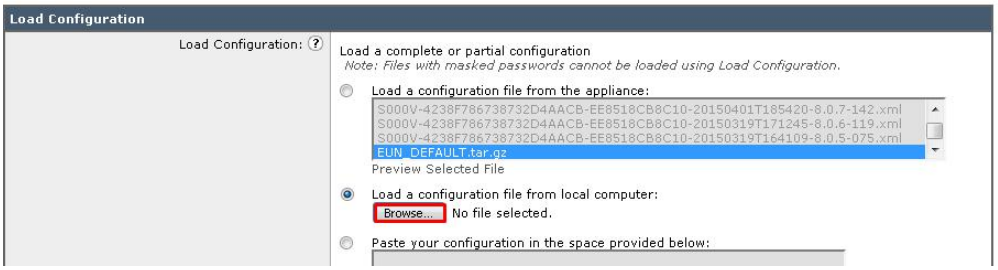
この Web セキュリティ アプライアンス デモンストレーション ガイドには、次の内容が含まれています。

カスタマイズ オプション

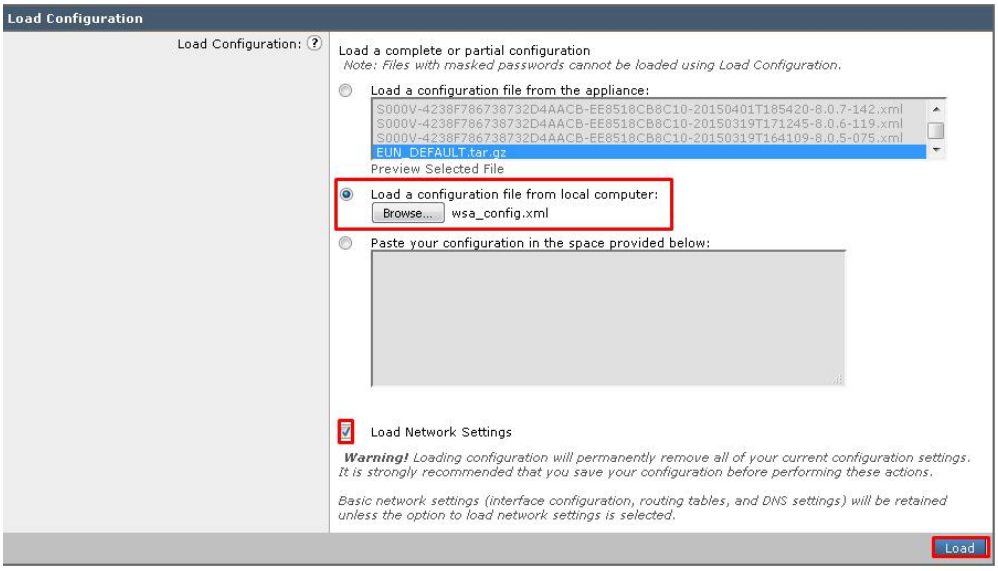
WSA の基本的な設定に精通している上級ユーザの場合、次の手順を実行して設定をロードし、シナリオ 3 に直接進むこともできます。シナリオ 1 と 2 で実施する内容は次のとおりです。

- ネットワークの設定
- 認証レルムの作成
- 基本認証および NTLMSSP 用の ID プロファイルの作成
- カテゴリをブロックするアクセス ポリシーの設定
- HTTPS インスペクション

- プライマリ クライアント マシン（wkst1）にログインします。
- Firefox を開き、プライマリ WSA（WSA-HQ1 - https://198.19.10.51）にアクセスします。
- ユーザ名「admin」、パスワード「ironport」でログインします。
- [システム管理（System Administration）] > [設定ファイル（Configuration File）] の順に移動します。
- [設定をロード（Load Configuration）] で [ローカルコンピュータから設定ファイルをロードする（Load a configuration file from your local computer）] を選択し、[参照（Browse）] をクリックします。



- デスクトップから **wsa_config.xml** を選択します。
- [ネットワーク設定をロード（Load Network Settings）] のチェックボックスが選択されていることを確認し、[ロード（Load）] をクリックします。



- ポップアップで [続行（continue）] をクリックし、成功メッセージが表示されたら右上の [変更を確定（Commit Changes）] をクリックします。
- これで設定がロードされました。
- ログイン用のクレデンシャルは、ユーザ名「**admin**」、パスワード「**ironport**」となります。

要件

次の表に、このデモンストレーションの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

Web セキュリティに対する高度な脅威に対抗するには、すべてのエンドポイント上やエンドポイント間に強力な保護機能と一貫した制御が必要です。保護対象には、モバイル デバイス、Web アプリケーション、モバイル アプリケーション、Web ブラウザが含まれます。そこで、Cisco® Web セキュリティ アプライアンスが必要になります。Cisco WSA を使用すれば、Web トラフィックの保護と制御という課題に、簡単かつ迅速に対処できます。

Cisco WSA は、オールインワンの安全性の高い Web ゲートウェイで、強力な保護、包括的な制御、および投資価値を提供します。また、競争力のある幅広い Web セキュリティ導入オプションを提供し、そのどれもがシスコの市場をリードするグローバル脅威インテリジェンス インフラストラクチャを備えています。

Web セキュリティ アプライアンスには、Advanced Malware Protection（AMP）、Cognitive Threat Analytics（CTA）、Application Visibility and Control（AVC）、アクセプタブル ユース ポリシー、情報豊富なレポート、安全性の高いモビリティが統合されています（図 1）。それらすべてを、管理が容易な単一のプラットフォームで利用できます。物理アプライアンスとしての Web セキュリティ アプライアンスは、メンテナンスの必要がほとんどないため運用コストが低く、遅延も少なくなっています。高度に分散したネットワークでも、Cisco Web セキュリティ仮想アプライアンスにより、必要なときに必要な場所で、同じレベルの厳重な仮想バージョンの Web セキュリティを導入できます。

http://www.cisco.com/web/JP/product/hs/security/ipweb/index.html

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管理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 クレデンシャルは、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するか、それらを必要とするシナリオ内の手順を調べることで確認できます。

図 1. dCloud のトポロジ

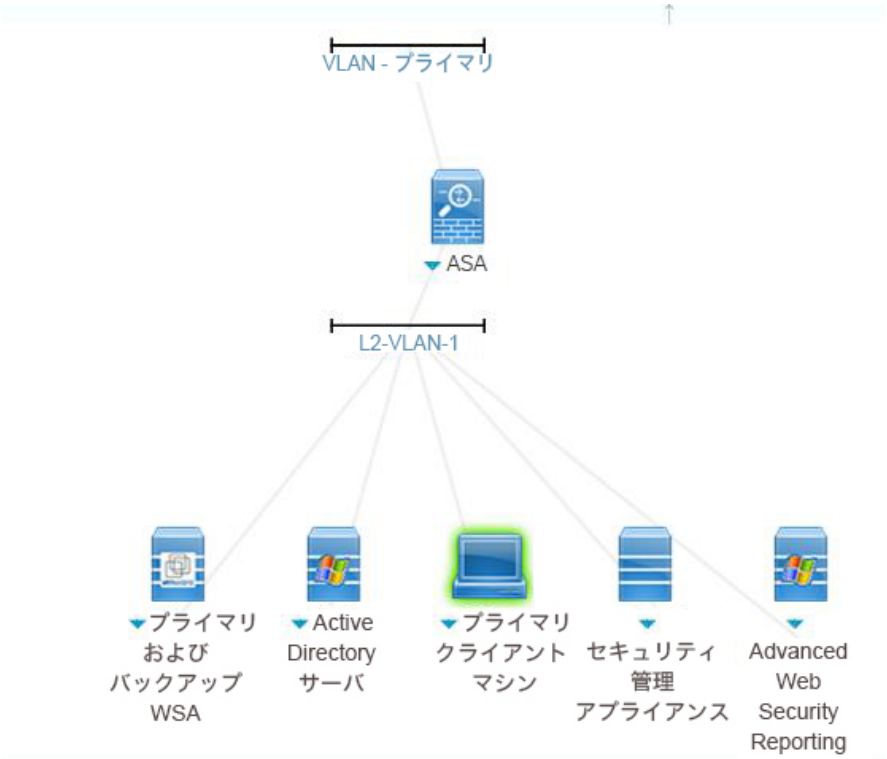


表 2. 機器の詳細

名前	説明	ホスト名（FQDN）	IP アドレス	ユーザ名	パスワード
WSA 1	プライマリ WSA（v. 10.1）	wsa-hq1.dcloud.cisco.com	198.19.10.51	admin	IronPort
WSA 2	セカンダリ WSA（v. 10.1）	wsa-hq2.dcloud.cisco.com	198.19.10.52	admin	C1sco12345
Workstation 1	プライマリ クライアント マシン	wkst1.dcloud.cisco.com	198.19.10.36	dCloud\wsaproxy	C1sco12345
Workstation 2	セカンダリ クライアント マシン	wkst3.dcloud.cisco.com	198.18.133.36	dcloud\connector	C1sco12345
AD サーバ	Active Directory サーバ	ad1.dcloud.cisco.com	198.19.10.1	dcloud\administrator	C1sco12345
AWSR	Advanced Web Security Reporting		198.19.10.56	admin	C1sco12345
SMA	セキュリティ管理アプライアンス	sma.dcloud.cisco.com	198.19.10.55	admin	C1sco12345
ESXi サーバ	ESXi ホスティング サーバ		198.19.10.31	root	C1sco12345

はじめに

以下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、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ために、**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：**198.19.10.36**、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] [英語]。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、この方法では、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 の基本設定とテスト

はじめに

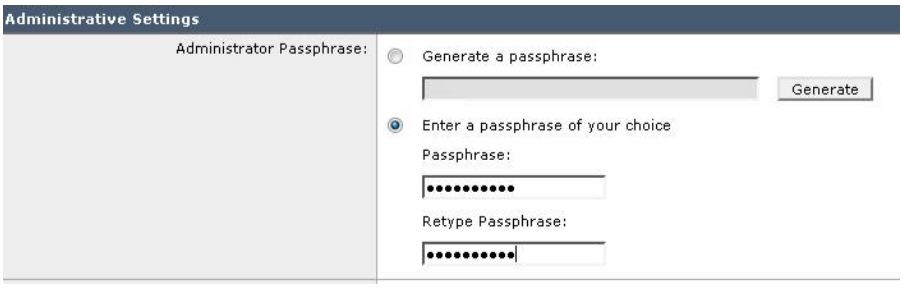
このシナリオでは、WSA の基本設定とテストを行います。ラボでその他のシナリオを進めるためには、ここで実施する内容が**必須**となります。このラボは複数のタスクに分かれています。上級ユーザや WSA の基本設定に精通しているユーザの場合は、このシナリオの内容を VMWare スナップショットからロードしてもかまいません。「カスタマイズ オプション」のセクションに手順が記載されています。

タスク A：システム セットアップ

手順

1. **プライマリ クライアント マシン**で Firefox を開き、次のようにして WSA 管理 GUI に接続します。
    a. https://198.19.10.51:8443 にアクセスするか、[ブックマーク（Bookmarks）] ツールバーで WSA-HQ1 のショートカットをクリックします。
    b. ユーザ名「**admin**」、パスワード「**ironport**」でログインします。
2. WSA GUI で、[システム管理（System Administration）] > [システムセットアップウィザード（System Setup Wizard）] に移動します。
3. [デフォルトシステムホスト名（Default System Hostname）] が **wsa-hq1.dcloud.cisco.com** になっていることを確認します。
4. DNS サーバが **198.19.10.1** に設定されていることを確認します。
5. [NTP サーバ（NTP Server）] が **time.sco.cisco.com** であることを確認します。
6. [タイムゾーン（Time Zone）] を次のように設定します。[地域（Region）] – [アメリカ（America）]、[国（Country）] – [アメリカ合衆国（United States）]、[タイムゾーン/GMT オフセット（Time Zone / GMT Offset）] – [太平洋（ロサンゼルス）（Pacific (Los_Angeles)）]
7. [操作のアプライアンスモード（Appliance Mode of Operation）] で [標準（Standard）] が選択されていることを確認し、[次へ（Next）] をクリックします。
8. [ネットワークコンテキスト（Network Context）] メニューで、もう一度 [次へ（Next）] をクリックします。
9. [ネットワークインターフェイスと配線（Network Interfaces and Wiring）] メニューで IPv4 アドレスとして **198.19.10.51/24** が入力されていることを確認します。[次へ（Next）] をクリックします。
10. [レイヤ 4 トラフィックモニタ配線（Layer 4 Traffic Monitor Wiring）] メニューで [デュプレックスタップ（Duplex TAP）] が選択されていることを確認します。[次へ（Next）] をクリックします。
11. [デフォルトゲートウェイ（Default Gateway）] が **198.19.10.254** に設定されていることを確認します。[次へ（Next）] をクリックします。
12. [レイヤ 4 スイッチもしくはデバイスなし（Layer 4 Switch or No Device）] が選択されていることを確認して、[次へ（Next）] をクリックします。

13. [管理用設定（Administrative Settings）] で [任意のパスフレーズを入力（Enter a passphrase of your choice）] を選択し、「**Cisco123$**」 と入力します。



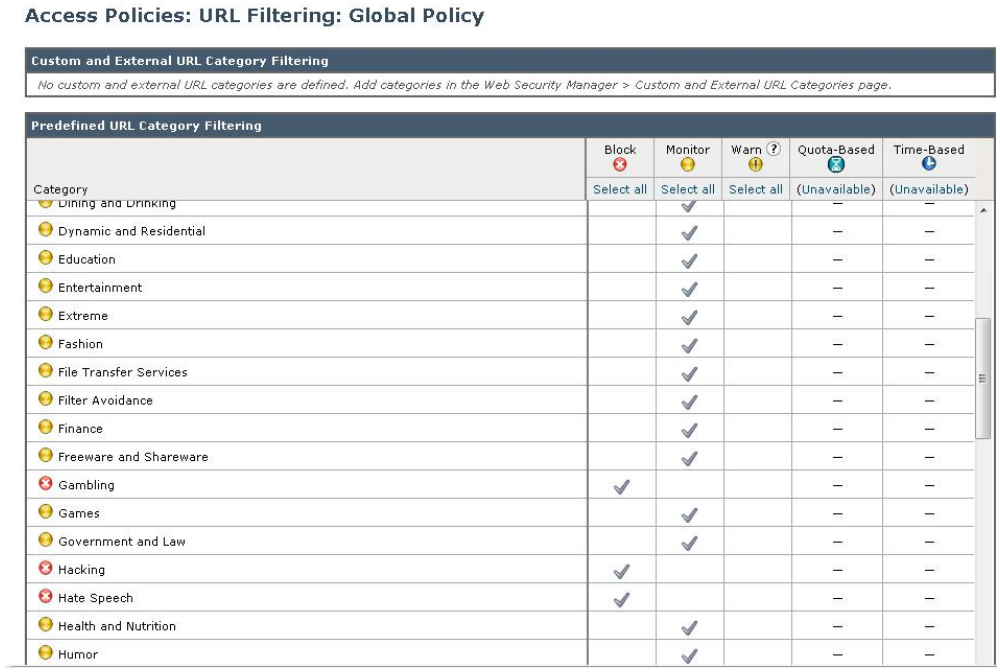
14. 電子メールアドレスとして operator@wsalab.com を設定します。
15. [オートサポート（AutoSupport）] と [ネットワーク参加（NetworkParticipation）] をオフにして、[次へ（Next）] をクリックします。
16. [マルウェアとスパイウェアのスキャン（Malware and Spyware Scanning）] の [検出されたマルウェアに対するアクション（Action for Detected Malware）] で [ブロック（Block）] オプション ボタンを選択し（それ以外はデフォルトのままにします）、[次へ（Next）] をクリックします。
17. 設定を確認し、推奨設定と比較して不適切と思われる設定がある場合は、右側の [編集（Edit）] をクリックして編集します。[この設定をインストール（Install This Configuration）] をクリックして初期設定をインストールします。
18. この時点では、WSA によって新しい FQDN にリダイレクトされます。証明書エラーを確認してアクセスを許可した後は、[システムセットアップの次のステップ（System Setup Next Steps）] ウィンドウが表示されます。IP 経由で WSA UI に再度アクセスすることもできます（https://198.19.10.51:8443/）。

注：システム セットアップ ウィザードが正しく実行され、設定が有効になっていることを確認するには、WSA GUI で [セキュリティサービス（Security Services）] > [Web プロキシ（Web Proxy）] の順に移動します。[基本設定（Basic Settings）] の [HTTP ポート（HTTP Ports）] と [プロキシ（Proxy）] が、それぞれ 80、3128 と [有効（Enabled）] になっていることを確認します。何らかの理由でプロキシが無効になっている場合は、システム セットアップ ウィザードを再実行する必要があります。

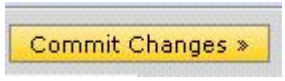
タスク B：アクセプタブル ユース ポリシーの適用

手順

1. [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）] を選択します。
2. [URL フィルタ（URL Filtering）] 列のテキスト [モニタ：79（Monitor: 79）] をクリックします。
3. 不適切であると思われるカテゴリは、[ブロック（Block）] 列をクリックしてブロックします。



4. [Gambling] は必ずブロックしてください – このカテゴリは、ラボでアクセプタブル ユース ポリシーをテストするために使用します。
5. ページ下部にある [送信（Submit）] ボタンをクリックします（変更を送信すると非アクティブな設定が構成されます。これは後で確定または破棄することができます）。
6. WSA GUI の右上の黄色いボタンをクリックします。

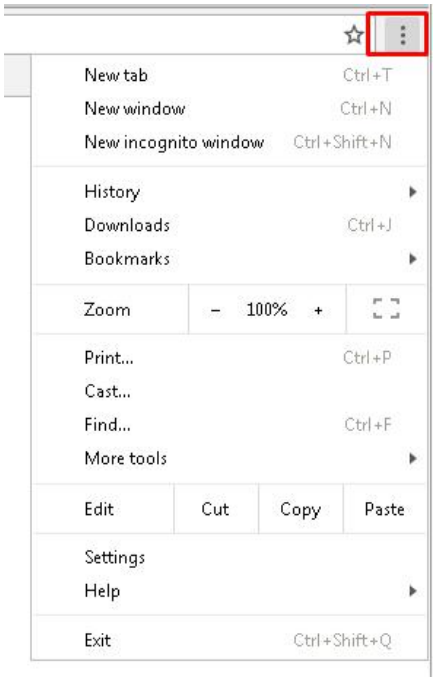


7. 変更する理由を入力し、[変更を確定（Commit Changes）] をクリックします。

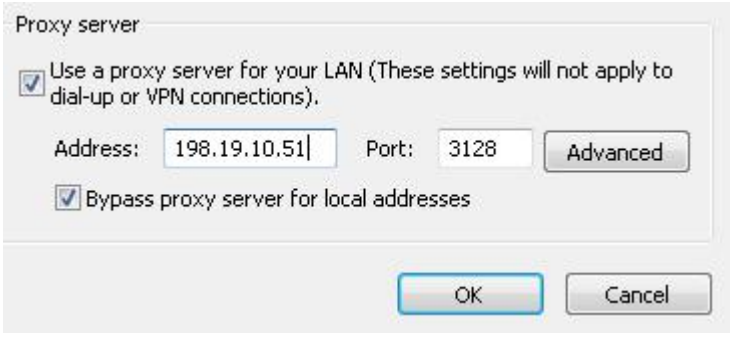
タスク C：プロキシ機能の確認

手順

1. Chrome ブラウザを開き、プロキシが WSA に設定されていることを確認します。
2. [オプション（options）] ボタン（右上にある、縦に並んだ 3 つの点）をクリックします。

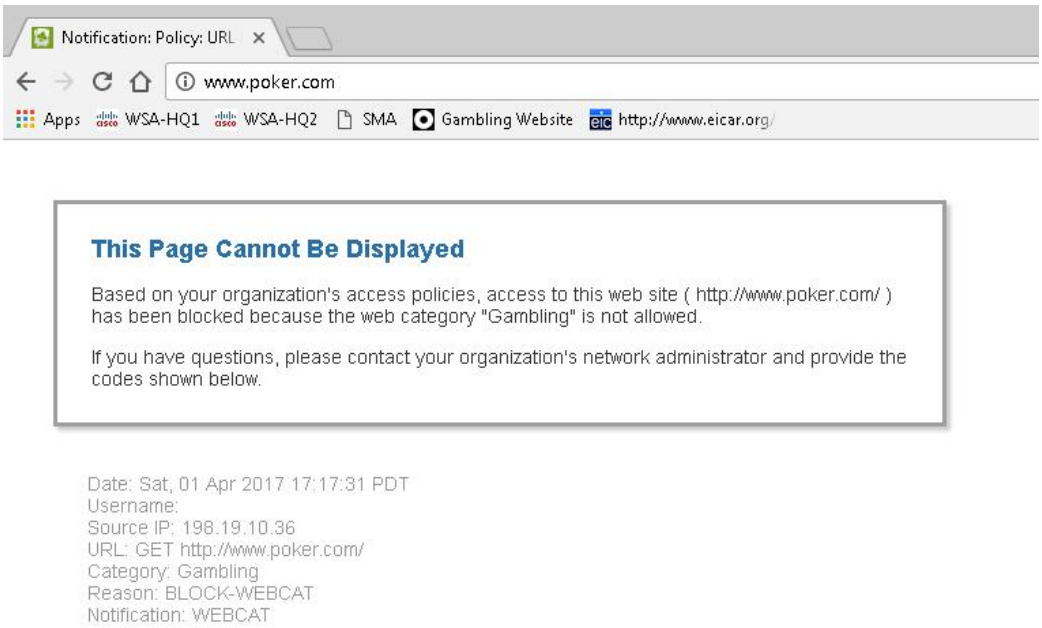


3. [設定（Settings）] をクリックした後、下方向にスクロールして、ハイパーリンク [詳細設定を表示する…（Show advanced settings…）] をクリックします。
4. [ネットワーク（Network）] で [プロキシ設定の変更…（Change proxy settings…）] をクリックします。
5. [接続（Connections）] > [LAN の設定（LAN Settings）] で、プロキシが次のように設定されていることを確認します。



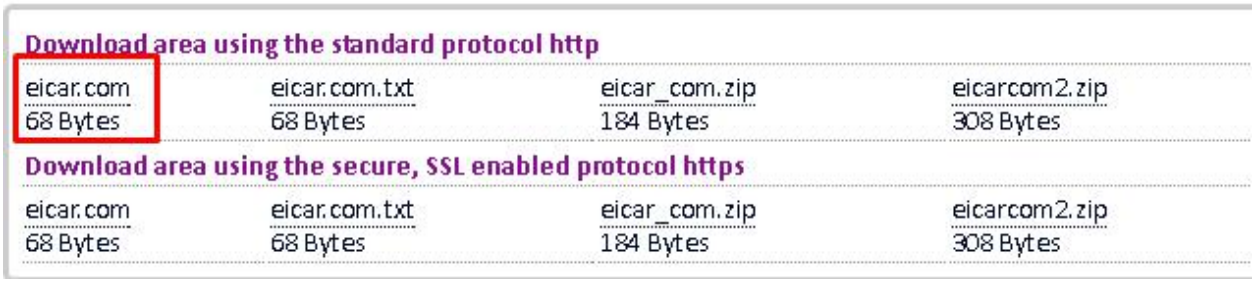
6. [OK] を 2 回クリックします。
7. 許可された Web サイト（例：http://www.yahoo.com）にアクセスします。アクセス可能なはずです。

8. 今度は、許可されていない Web サイト（例：http://poker.com）にアクセスします。ブロックされるはずです。



9. [ブックマーク（Bookmarks）] ツールバーから eicar.org のブックマークを選択します。

10. [ダウンロードエリア（Download area）] が表示されるまで下方向にスクロールして、標準の http として [eicar.com] テストファイルをクリックします。ブロックされるはずです。



11. 次に、www.ihaveabadreputation.com にアクセスします。ブロックされて [エンドユーザ通知（End User Notification）] ページが表示されるはずです。

タスク D：CLI を使用してプロキシ アクセス ログを確認する

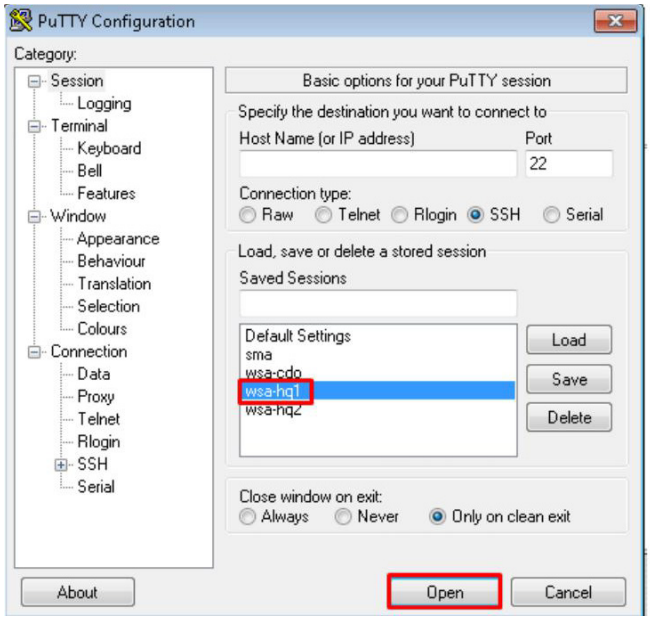
手順

ポリシー設定のトラブルシューティングにとって最も重要なログは、プロキシ アクセス ログです。ラボ全体でこのアクセス ログを確認していきます。現時点では、リアルタイムにこのログを見る方法を学びます。

1. S シリーズに SSH で接続します。

   a. デスクトップにある [putty.exe] アイコンをダブルクリックします。 

   b. 「**wsa-hq1**」という定義済みのセッションがあります。これにより、SSH を介して各自の WSA に接続されます。



   c. WSA にログインします。

2. WSA CLI を使用してログを表示するには 2 つの方法があります。

   a. WSA CLI に「**tail accesslogs**」と入力します。終了するには、**Ctrl+C** を押します。

   b. 「tail」と入力すると、設定済みのログのリストが表示されます。ここで、確認するログに対応する番号を入力できます。[アクセスログ（Access Logs）] で [1] を選択します。

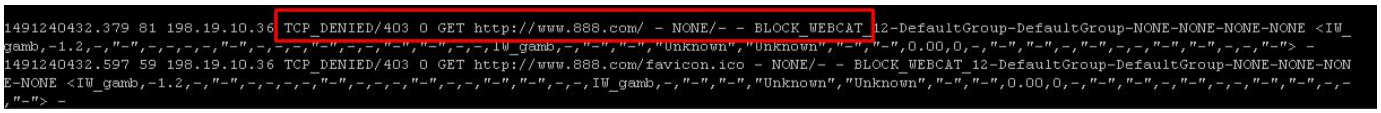
注：まれに、tail accesslogs コマンドの出力に 10 ~ 30 秒程度の遅延が発生することがあります。WSA でのログの記録はリアルタイムですが、出力のみが若干遅延します。

3. Chrome を使用して http://poker.com にアクセスし、アクセス ログと HTTP ヘッダーの両方を確認します。このアクセスは、先ほどのラボで作成したアクセス ポリシーによりブロックされます。アクセス ログ etail ntry で、次の文字列を確認します。

    a. **TCP_DENIED** – 実行結果またはキャッシュ結果コード

    b. **403** – HTTP 応答コード

    c. **BLOCK_WEBCAT** – ACL デシジョン タグ

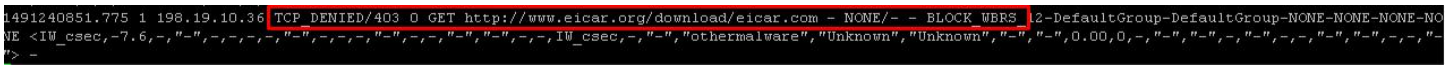


4. Chrome を使用して、eicar テスト ウイルスのダウンロードを再度試みます。アクセス ログと HTTP ヘッダーの両方を確認します。WSA のアクセス ログ エントリで、次の文字列を確認します。

    a. TCP_DENIED – 実行結果またはキャッシュ結果コード

    b. 403 – HTTP 応答コード

    c BLOCK_WBRS – ACL デシジョン タグ



タスク E：プロキシ認証

手順

1. WSA GUI で、[ネットワーク（Network）] > [認証（Authentication）] に移動し、[レルムを追加...（Add Realm...）] をクリックします。

    a. [レルム名（Realm Name）] に「ADrealmDC1」と入力します。

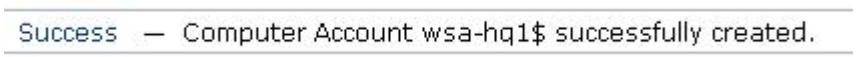
    b. [認証サーバタイプとスキーム（Authentication Server Type and Scheme(s)）] で、[Active Directory] （[Kerberos]、[NTLMSSP] または [基本認証（Basic Authentication）]）を選択します。

    c. [Active Directory サーバ（Active Directory Server）] に「**198.19.10.1**」と入力します。

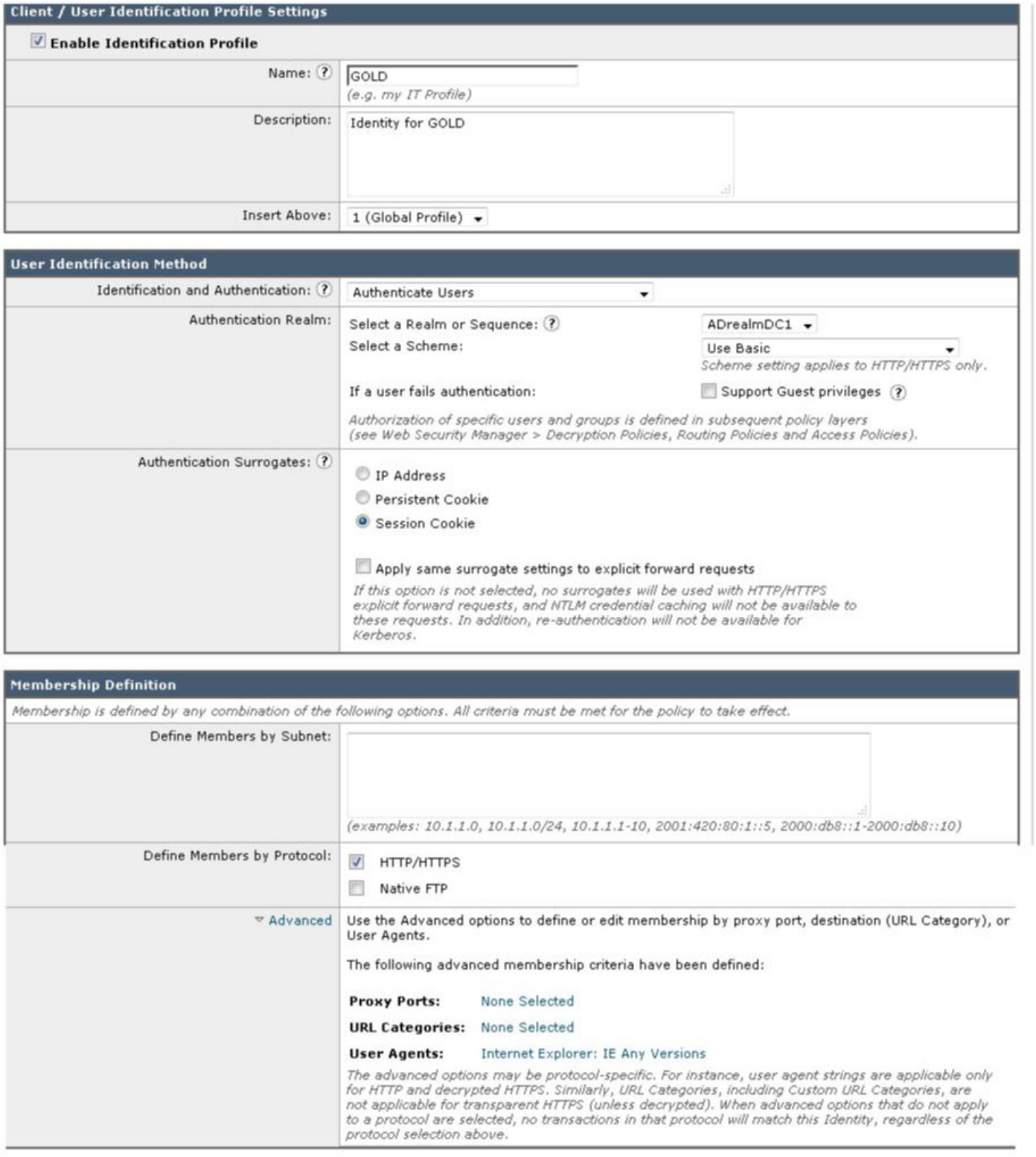
    d. [Active Directory ドメイン（Active Directory Domain）] に「**dcloud.cisco.com**」と入力します。

    e. [ドメインへの参加（Join Domain）] をクリックして、次のクレデンシャルを入力します – ユーザ名「**Administrator**」、パスワード「**C1sco12345**」

    f. すべて成功すると、「Success – Computer Account gold$ successfully created（成功 – コンピュータ アカウント gold$ が正常に作成されました）」というメッセージが表示されます。



2. [テスト開始（Start Test）] ボタンをクリックします。
    a. テストが正常に完了したら、[送信（Submit）] ボタンをクリックします。
    b. エラー メッセージが表示されたら、トラブルシューティングを行い、ホスト名や AD サーバなどを確認してください。
    c. 変更を確定し、[コメント（Comments）] セクションに「AD レルムの作成（AD Realm created）」と入力します。
3. WSA ドメインの新しい ID を作成します。
    a. WSA GUI で、[Web セキュリティマネージャ（Web Security Manager）] > [識別プロファイル（Identification Profiles）] に移動します。
    b. [識別プロファイルの追加...（Add Identification Profile...）] をクリックします。
    c. [名前（Name）] フィールドでは dCloud を使用します。[説明（Description）] テキスト ボックスに適切な説明を入力します。
    d. [識別と認証（Identification and Authentication）] ドロップダウンをクリックして [ユーザの認証（Authenticate Users）] を選択します。
    e. [レルムまたはシーケンスを選択（Select a Realm or Sequence）] では、すでに [ADrealmDC1] が選択されています。
    f. [スキームの選択（Select a Scheme）] では [基本認証を利用（Use Basic）] を選択し、[認証サロゲート（Authenticate Surrogate）] には [セッションクッキー（Session Cookie）] を選択します。
    g. [明示的フォワードリクエストに同じサロゲート設定を適用（Apply same surrogate settings to explicit forward requests）] をオンにします。
    h. [詳細設定（Advanced）] をクリック後、[ユーザエージェント（User Agents）] の [選択なし（None Selected）] をクリックします。
    i. [共通ユーザエージェント（Common User Agents）] で、[ブラウザ（Browsers）] をクリックし、[任意のバージョンの IE（IE Any Versions）] を選択します。下方向へスクロールして、[完了（Done）] をクリックします。
    j. 次のスクリーンショットのような設定になっているはずです。完了したら、[送信（Submit）] をクリック後、[変更を確定（Commit Changes）] をクリックします。



注：[送信（Submit）] をクリックすると警告メッセージが表示されます。理想的な ID プロファイルの順序に関するメッセージを確認します。

4. [グローバル ID の認証（Authentication for Global Identity）] を有効にします。
    a. WSA GUI で、[Web セキュリティ マネージャ（Web Security Manager）] > [識別プロファイル（Identification Profiles）] に移動します。[グローバル識別プロファイル（Global Identification Profile）] をクリックします。
    b. [識別と認証（Identification and Authentication）] ドロップダウン メニューから、[ユーザの認証（Authenticate Users）] を選択します。
    c. [レルムまたはシーケンスを選択（Select a Realm or Sequence）] ドロップダウン メニューから、[すべてのレルム（All Realms）] を選択します。
    d. [スキームの選択（Select a Scheme）] ドロップダウン メニューから、[NTLMSSP 認証を利用（Use NTLMSSP）] または[基本認証を利用（Use Basic）] を選択します。
    e. [認証サロゲート（Authentication Surrogate）] として [セッションクッキー（Session Cookie）] を選択します。
    f. ページの右下にある [送信（Submit）] ボタンをクリックします。警告を無視します。
    g. 右上の黄色い [変更を確定 >>（Commit Changes >>）] ボタンをクリックします。
    h. コメントを入力します。例：プロキシ認証を設定（Configured proxy authentication）
    i. [変更内容を確定（Commit Changes）] をクリックします。

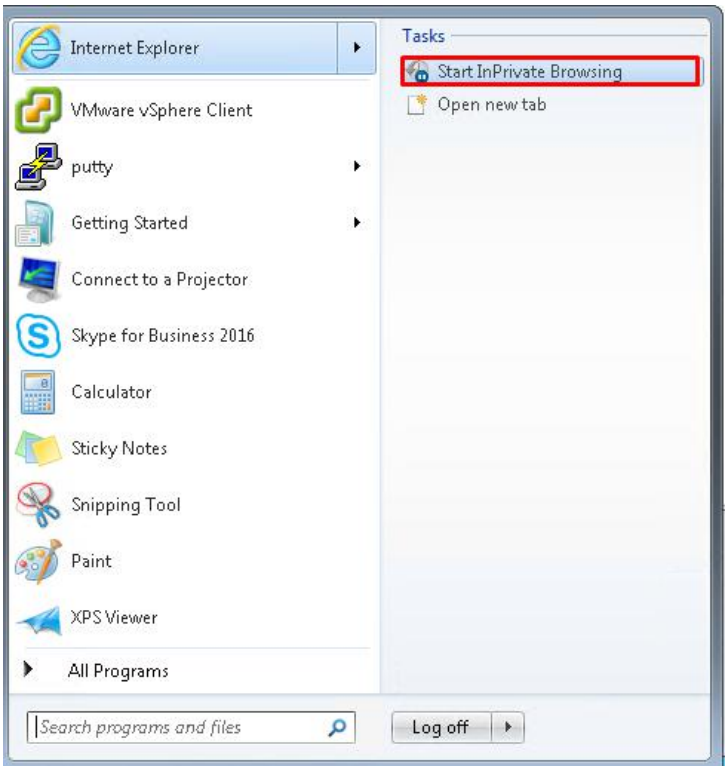
タスク E：認証設定のテスト

手順

1. Chrome を開きます。任意の URL をいくつかテストします。
2. www.poker.com にアクセスします。ログインに使用している AD ユーザ名が表示されます。

3. CLI を利用して、認証済みユーザの ID がアクセス ログに記載されていることを確認します。

4. [スタート（Start）] から、プライベート閲覧モードで Internet Explorer を開きます。



5. www.poker.com にアクセスします。ユーザ名「**wsaproxy**」、パスワード「**C1sco12345**」を入力します。ブロックされるはずです。
6. ギャンブル サイトにアクセスします。ここでも自分のユーザ名が表示されます。

注：次にデモストレーションする双方向認証は、WSA によって実行されます。グローバル ポリシーが NTLMSSP を使用するよう設定されていたため、認証は透過的に実行されました。GOLD の ID プロファイルが [基本（Basic）] に設定され、Internet Explorer のみに適用される設定になっていたため、IE を開いたときにログインが要求されました。

シナリオ 2.　HTTPS インスペクションの使用

タスク A：HTTPS プロキシ設定

はじめに

Web トラフィックをキャプチャして制御を適用するには、HTTPS プロキシの設定が不可欠です。暗号化されている Web サイトの増加に伴い、この機能は多くの顧客環境で必須の機能になっています。

手順

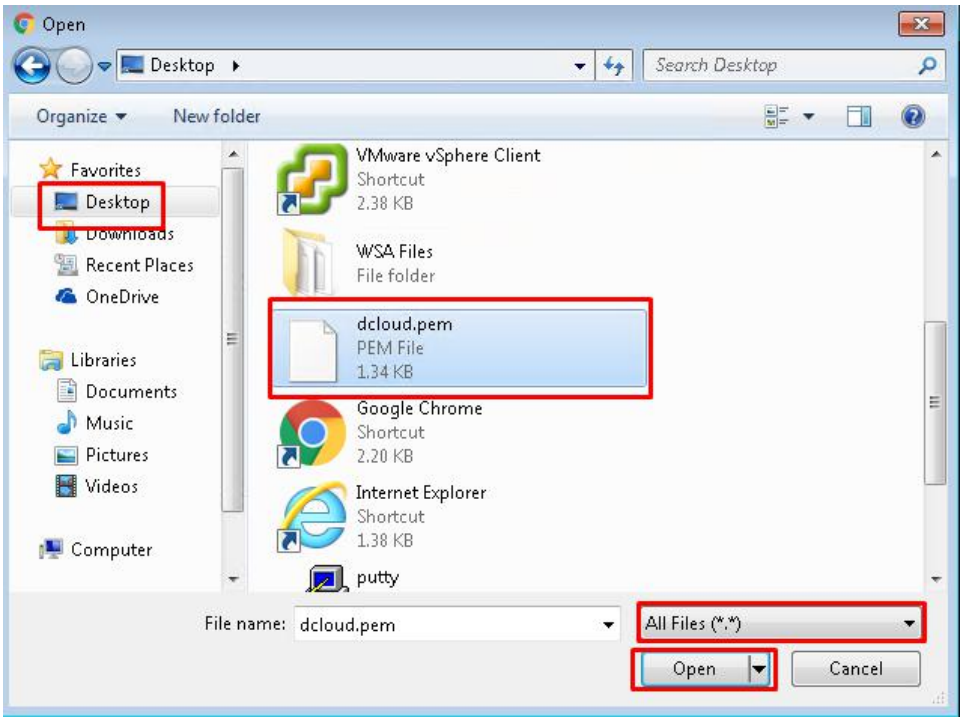
1. [Web セキュリティマネージャ（Web Security Manager）] > [アクセスポリシー（Access Policies）] から、[URL フィルタ（URL Filtering）] の下のリンクをクリックします。[ソーシャルネットワー キング（Social Networking）] カテゴリを [ブロック（Block）] に設定します。[送信（Submit）] をクリック後、[変更を確定（Commit Changes）] をクリックします。
2. HTTPS インスペクションの必要性をデモします。HTTPS を利用したファイル ダウンロードが検査されていないことを確認します。
    a. Chrome を使用して **https://www.facebook.com** にアクセスします。
    b. このページの読み込みは失敗します。最初の HTTPS リクエストが暗号化されていなかったため、WSA がこの最初の接続をブロックしたからです。ただし、アクセスしたページが完全に暗号化されているため、対応するブロック ページは表示されません。HTTPS ブロッキングを適切に利用するには、HTTPS インスペクションを有効にする必要があります。
3. HTTPS プロキシを有効化し設定します。
    a. [セキュリティサービス（Security Services）] > [HTTPS プロキシ（HTTPS Proxy）] に移動します。[設定の有効化と編集...（Enable and Edit Settings...）] をクリックします。
    b. HTTPS プロキシ使用許諾に同意します。
    c. [HTTPS プロキシ設定（HTTPS Proxy Settings）] で、[生成された証明書と鍵を使用（Use Generated Certificate and Key）] を選択し、[新しい証明書と鍵を生成（Generate New Certificate and Key）] ボタンをクリックします。次の図のようにパラメータを追加して、完了したら [生成（Generate）] をクリックします。

d. [証明書をダウンロード（Download Certificate）] リンクを右クリックして [リンクに名前を付けて保存..（Save Link As..）] を選択し、.pem ファイルの名前を「**dcloud**」とします。デスクトップに保存します。

e. 新しいタブを開き、**chrome://settings** と入力します。下方向にスクロールして、[詳細設定を表示する…（Show advanced settings…）] をクリックします。

f. HTTPS/SSL が表示されるまで下方向にスクロールし、[証明書の管理...（Manage Certificates…）] をクリックします。

g. [証明書（Certificates）] ウィンドウで、[インポート（Import）] > [次へ（Next）] の順にクリックします。[証明書インポートウィザード（Certificate Import Wizard）] ウィンドウで、[参照（Browse）] をクリックします。[デスクトップ（Desktop）] を選択し、ドロップダウンから [すべてのファイル（All files）] を選択します。最後に、dcloud.pem ファイルを選択し、[開く（Open）] をクリックします。



h. 次のウィンドウで、もう一度 [次へ（Next）] をクリックします。[証明書ストア（Certificate Store）] ウィンドウで、[すべての証明書を次のストアに配置する（Place all certificates in the following store）] を選択し、[参照（Browse）] をクリックします。[証明書ストアを選択（Select Certificate Store）] ウィンドウから [信頼できるルート認証機関（Trusted Root Certification Authorities）] を選択します。[OK] をクリックします。

i. [次へ（Next）] をクリック後、[終了（Finish）] をクリックします。セキュリティ警告が表示されたら、[はい（Yes）] をクリックします。

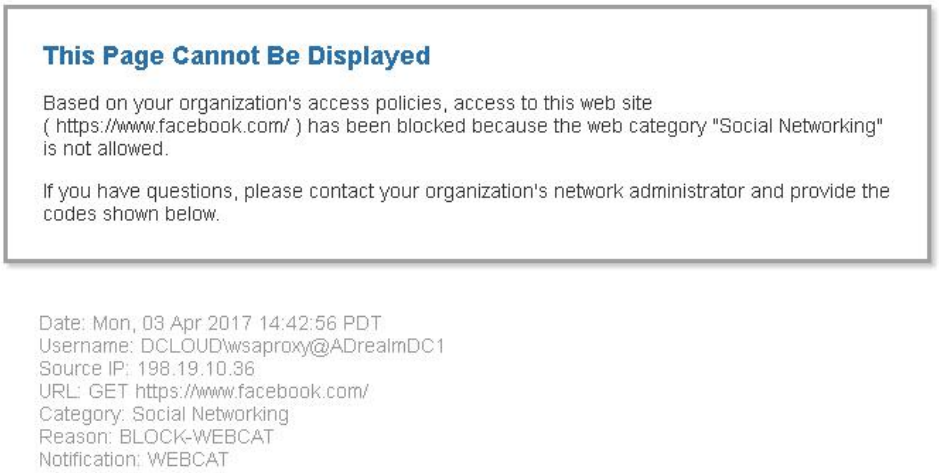
j. WSA UI に戻り、下方向にスクロールして、[HTTPS プロキシ設定（HTTPS Proxy Settings）] メニューで [送信（Submit）] をクリックします。変更を確定します。

4. 復号をテストします。

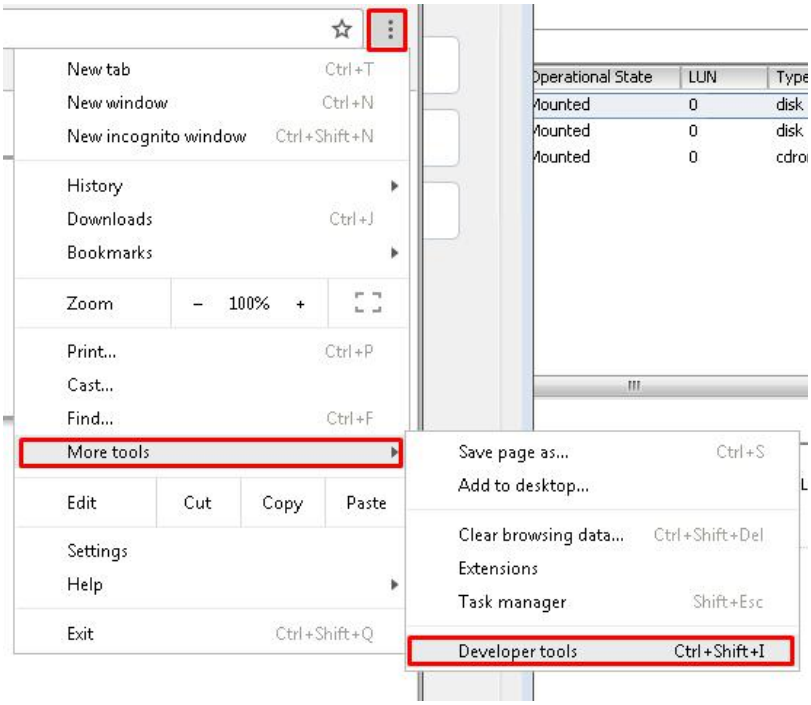
a. Firefox で、www.facebook.com にアクセスします。[URL] フィールドの緑色の鍵のアイコンをクリックします。矢印（>）をクリックして、証明書の詳細を確認します。

b. 上の図では、証明書の提供元は DigiCert 社と示されています。

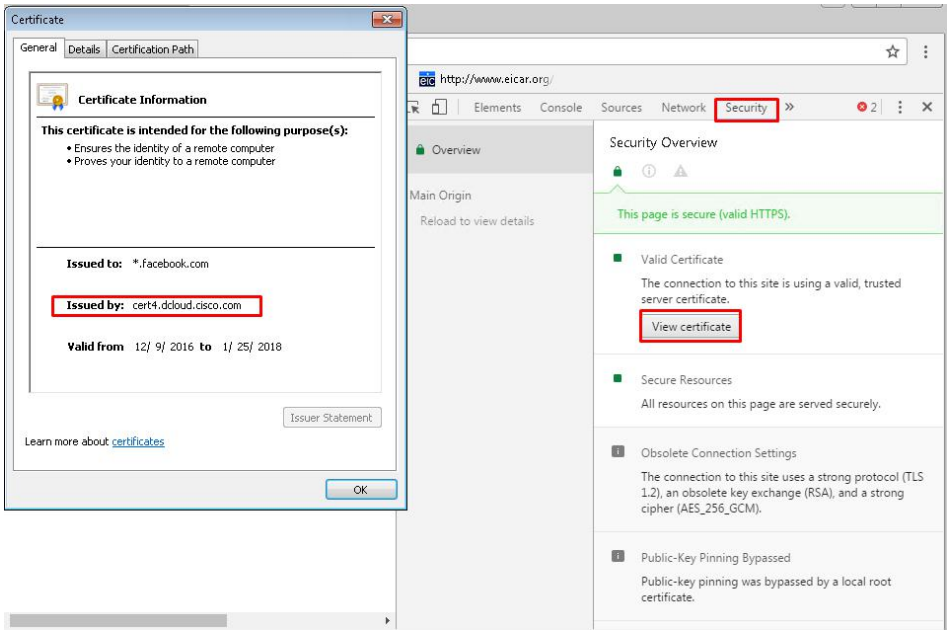
c. Chrome で再び facebook.com にアクセスします。今度はブロック ページが表示されます。



d. Chrome の [設定（settings）] で、[その他のツール（More tools）] > [開発者向けツール（Developer tools）] の順に選択します。



e. 次に、[セキュリティ（Security）] > [証明書の表示（View certificate）] の順にクリックします。



f. 発行される証明書には、WSA で作成したものが表示されるはずです。これにより、WSA が HTTPS トラフィックを正しく復号していることがわかります。

シナリオ 3：アクセプタブル ユース ポリシーの適用

はじめに

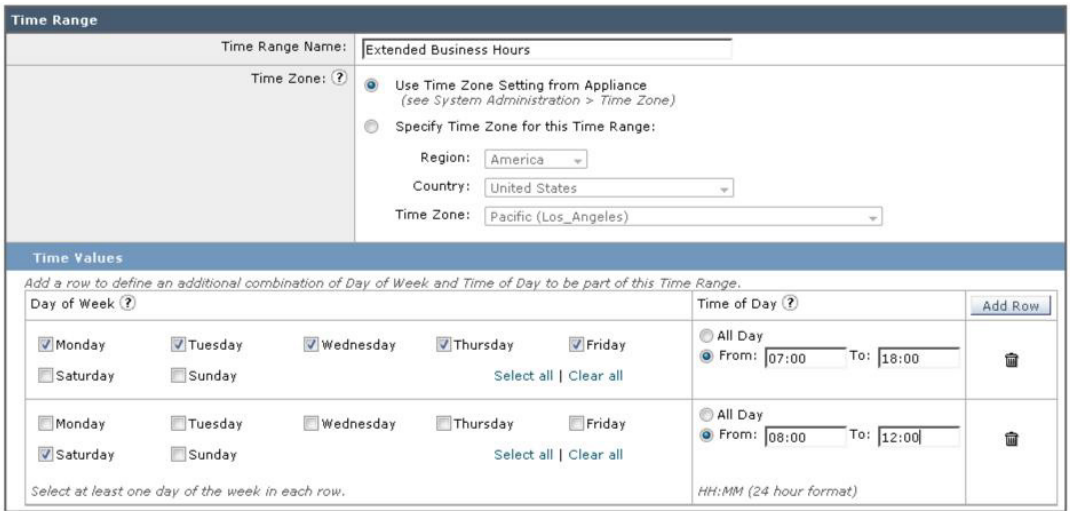
この演習では、アクセプタブル ユース ポリシーの適切な構築方法を理解することが目標となります。このシナリオには、下記の 5 つのタスクがあります。

1. 法律違反や攻撃的なコンテンツを表示するカテゴリをブロックする。
2. 特定のファイル タイプをブロックするアーカイブ検査を設定する。
3. [フィルタリング回避（Filter Avoidance）] および [ピアファイル転送（Peer File Transfer）] カテゴリを [警告（Warn）] に設定する。
4. [業務ピーク時（Peak Business Hours）] では、[ソーシャルネットワーキング（Social Networking）] をブロック（または [モニタ（Monitor）]）に設定する。
5. IP ベースの URL をブロックする。

タスク A：適切なグローバル アクセプタブル ユース ポリシーの作成

手順

1. 就業延長時間帯と業務ピーク時の 2 つの時間範囲を作成します。
    a. WSA GUI で、[Web セキュリティ マネージャ（Web Security Manager）] > [時間範囲およびクォータの定義（Define Time Ranges and Quotas）] に移動します。
    b. [時間範囲の追加（Add Time Range）] をクリックします。
    c. [時間範囲名（Time Range Name）] に「Extended Business Hours」と入力します。
    d. アプライアンスのタイムゾーン設定を利用します。
    e. [時間値（Time Values）] について、[月曜日（Monday）] から [金曜日（Friday）] までのチェックボックスをオンにします。
    f. [時刻（Time of Day）] に、「07:00」から「18:00」と入力します。
    g. [行の追加（Add Row）] をクリックします。
    h. 新しい行で、[土曜日（Saturday）] チェックボックスをオンにします。
    i. 新しい行で、「08:00」から「12:00」と入力します。



j. ページの右下にある [送信（Submit）] ボタンをクリックします。

k. [Add Time Range] をクリックします。

l. [時間範囲名（Time Range Name）] に「Peak Business Hours」と入力します。

m. アプライアンスのタイムゾーン設定を利用します。

n. [時間値（Time Values）] について、[月曜日（Monday）] から [金曜日（Friday）] までのチェックボックスをオンにします。

o. [時刻（Time of Day）] に、「10:00」から「14:00」と入力します。

p. [送信（Submit）] ボタンをクリックし、変更を確定します。

2. グローバル ポリシー（アクセス ポリシー グループ）の URL フィルタを設定します。

a. WSA GUI で、[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）] に移動します。

b. [グローバルポリシー（Global Policy）] 行の [URL フィルタリング（URL Filtering）] 列のテキストをクリックします。

c. 違法・攻撃的なカテゴリがいくつかありますので、それらをブロックしてください。

d. [フィルタリング回避（Filter Avoidance）] および [ピアファイル転送（Peer File Transfer）] カテゴリを [警告（Warn）] に設定します。

e. [ソーシャルネットワー キングカテゴリ（Social Networking Category）] で [時間ベース（Time-Based）] を選択します。

f. [業務ピーク時（Peak Business Hours）] には、[ソーシャルネットワーキング（Social Networking）] をブロック（または[モニタ（Monitor）]）に設定します。

g. [ショッピングカテゴリ（Shopping Category）] で [時間範囲（Time Range）] を選択します。

h. [就業延長時間帯（Extended Business Hours）] には [ショッピング（Shopping）] をブロック（または [警告（Warn）] に設定）します。

i. ページの右下にある [送信（Submit）] ボタンをクリックします。

j. 右上にある黄色い [変更を確定（Commit Changes）] ボタンをクリックします。

k. コメントを入力します。例：グローバル AUP を作成（Created Global AUP）

l. [変更内容を確定（Commit Changes）] をクリックします。

m. 次の URL にアクセスして結果を確認します。

i. www.proxify.com（フィルタリング回避）

ii. www.facebook.com（ソーシャル ネットワー キング）

iii. www.amazon.com（ショッピング）

3. ポリシー トレース ツールを使用して、Social Networking と Gambling に対する時間指定のポリシーをテストします。

a. WSA GUI で、[システム管理（System Administration）] > [ポリシートレース（Policy Trace）] に移動します。

b. [URL] に有効な URL を入力します。例：www.cisco.com。

c. [認証レルム（Authentication Realm）] で、作成したレルムを選択します。

d. [ユーザ名（User Name）] には DCLOUD\wsaproxy と入力します。

e. [詳細（Advanced）] をクリックして詳細設定にアクセスします。

f. [要求の詳細（Request Details）] の [リクエスト時間（Time of Request）] に、[業務ピーク時（Peak Business Hours）] 内の日付と時刻を入力します。

g. [レスポンスの詳細のオーバーライド（Response Detail Overrides）] で、[URL カテゴリ（URL Category）] から [ソーシャルネットワーキング（Social Networking）] を選択します。

h. [一致するポリシーの検索（Find Policy Match）] ボタンをクリックします。

i. 結果がポリシー設定と一致することを確認します。一致しない場合は、エラーをトラブルシューティングして修正します。スクリーンショット例を以下に示します。

Policy Trace

Destination

URL: www.cisco.com

Transaction

Client or User: *To represent a client by IP address, choose "No authentication or Identification" and enter the IP address below. To represent a user identified through an authentication realm, choose the authentication realm and enter the user name.*

Authentication / Identification: ADrealmDC1

Client IP Address:

User Name: DCLOUD\wsaproxy

▽ Advanced

Request Details

Proxy Port:

User Agent:

Time of Request: Date: 04/03/2017 Time: 11:00 (GMT -07:00)

Upload File: Browse... No file selected.

Object Size: *(Add a trailing K, M, or G to indicate size unit)*

MIME Type: Object and MIME Type Reference

Webroot Verdict: Do not override malware verdict

McAfee Verdict: Do not override malware verdict

Sophos Verdict: Do not override malware verdict

Response Detail Overrides

URL Category: Social Networking

Application: Do not override application

Object Size: *(Add a trailing K, M, or G to indicate size unit)*

MIME Type: Object and MIME Type Reference

Web Reputation Score: *(from -10.0 to 10.0)*

Webroot Verdict: Do not override malware verdict

McAfee Verdict: Do not override malware verdict

Sophos Verdict: Do not override malware verdict

Response Detail Overrides

URL Category: Social Networking

Application: Do not override application

Object Size: *(Add a trailing K, M, or G to indicate size unit)*

MIME Type: Object and MIME Type Reference

Web Reputation Score: *(from -10.0 to 10.0)*

Webroot Verdict: Do not override malware verdict

McAfee Verdict: Do not override malware verdict

Sophos Verdict: Do not override malware verdict

Find Policy Match

Results

User Information

User Name: DCLOUD\wsaproxy
Authentication Realm Group Membership: DCLOUD\wsaproxy, DCLOUD\Group Policy Creator Owners, DCLOUD\Domain Users, DCLOUD\Domain Admins, DCLOUD\Enterprise Admins, DCLOUD\Schema Admins, DCLOUD\Organization Management
Secure Group Tag Membership: None
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0

URL Check

WBRS Score: 8.7
URL Category: Social Networking

Policy Match

Cisco Data Security policy: None
Decryption policy: None
Routing policy: None
Identification Profile: DefaultIdentification
Access policy: Global Access Policy

Final Result

Request blocked

Details: Request blocked based on URL category

Trace session complete

4. 以前作成した 2 つの時間クォータに基づき、リクエスト日時と URL カテゴリをさまざまに組み合わせて手順 3a ~ 3i を繰り返します。
5. IP ベースの URL をブロックする：http://67.20.81.143 にアクセスできることを確認します。

注：IP アドレスを識別するためにどのような正規表現を使うかは、簡単な問題ではありません。IP アドレスの表記がさまざま（10 進数表記、16 進数表記、1 整数表記、ドットによる 4 分割表記等）であることが、この問題を難しくしています。さらに、その複雑さから、利用する正規表現によっては WSA のパフォーマンスに影響する可能性があります。この演習では、有効に機能する次のシンプルな表記を使用します。**http://[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+**

6. カスタム URL カテゴリを作成して適用し、IP アドレスで指定された URL をブロックします。
    a. WSA GUI で、[Web セキュリティマネージャ（Web Security Manager）] > [カスタムポリシー要素（Custom Policy Element）] > [カスタムおよび外部 URL カテゴリ（Custom and External URL Categories）] に移動します。
    b. [カテゴリの追加（Add category）] をクリックします。
    c. 「IP based URLs」などのカテゴリ名を入力します。
    d. [正規表現（Regular Expression）] テキストボックスが表示されない場合は、[詳細（Advanced）] 矢印をクリックします。
    e. [正規表現（Regular Expression）] ボックスに「http://[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+」と入力します。
    f. ページの右下にある [送信（Submit）] ボタンをクリック後、[変更を確定（Commit Changes）] をクリックします。
7. 作成したカスタム URL カテゴリがブロックされるように、[グローバルポリシーURL カテゴリ（Global Policy URL Categories）] を設定します。
    a. WSA GUI で、[Web セキュリティマネージャ（Web Security Manager）] > [Web ポリシー（Web Policies）] > [アクセスポリシー（Access Policies）] に移動します。
    b. グローバル ポリシー グループの [URL フィルタリング（URL Filtering）] ボックス内のテキストをクリックします。
    c. [カスタムカテゴリの選択（Select Custom Categories）] ボタンをクリックします。
    d. 作成したカスタム カテゴリについて、[設定の選択（Setting Selection）] ドロップダウン メニューから [ポリシーに含める（Include in policy）] を選択します。
    e. ページの右下にある [適用（Apply）] ボタンをクリックします。
    f. カスタム カテゴリ（IP ベースの URL）の右側の [ブロック（Block）] 列にチェックを入れます。
    g. 変更を送信し、確定します。
8. http://67.20.81.143 にアクセスできないことを確認します（最初にサイトがブロックされない場合は、すべてのブラウザ キャッシュをクリアする必要があります）。アクセス ログでカスタム URL カテゴリの最初の 4 文字を検索します。CLI のアクセス ログに次のように表示されます。

```
1491264101.340 6 198.19.10.36 TCP_DENIED/403 0 GET http://67.20.81.143/ "DCLOUD\wsaproxy@ADrealmDC1"
NONE/- - BLOCK_CUSTOMCAT_12-DefaultGroup-DefaultGroup-NONE-NONE-NONE-NONE <C_IP_b,-,-,"-",-,-,-,-,"-
",-,-,-,"-",-,-,"-","-",-,-,-,-,"-","-","-","-","-","-",0.00,0,-,"-","-",-,"-",-,-,"-","-",-,-,"-"> -
```

タスク B：アーカイブの検査

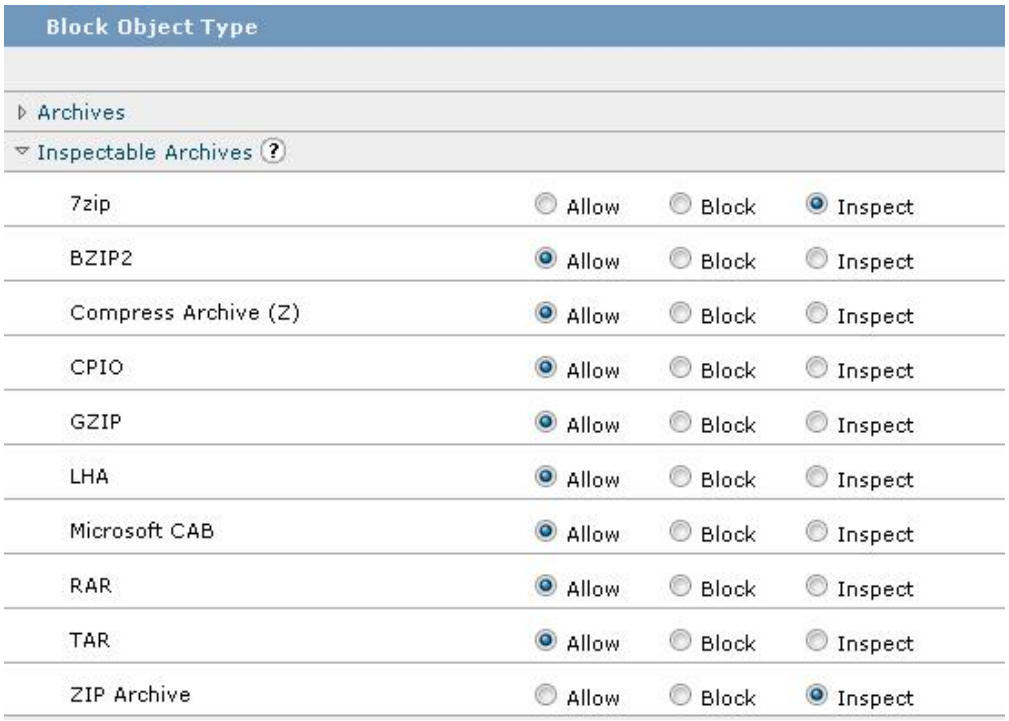
はじめに

個々のアクセス ポリシーについて、検査可能な特定のタイプのアーカイブを許可、ブロック、または検査することができます。検査可能なアーカイブとは、ファイルタイプ ブロック ポリシーを適用するために、WSA が展開してその中に含まれている各ファイルを検査できる、アーカイブまたは圧縮ファイルを指します。

手順

1. [検査可能なアーカイブの設定（Inspectable Archives Settings）] を設定します。
    a. [セキュリティサービス（Security Service）] > [アクセプタブルユースポリシーコントロール（Acceptable Use Controls）] に移動します。
    b. [検査可能なアーカイブの設定（Inspectable Archives Settings）] が表示されるまで下方向にスクロールして、[アーカイブ設定の編集（Edit Archives Settings）] をクリックします。
    c. [カプセル化されたアーカイブの最大展開数（Maximum Encapsulated Archive Extractions）] のデフォルト値は 2 です。この値を 5 に設定します。
    d. [検査不可能なアーカイブをブロック（Block Uninspectable Archives）] のチェックボックスをオンにします。
    e. [送信（Submit）] をクリック後、[変更を確定（Commit Changes）] をクリックします。
2. アーカイブ ファイルのアクセス ポリシーを設定します。
    a. [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。
    b. [グローバルポリシー（Global Policy）] で、[オブジェクト（Objects）] 列の [ブロックされたアイテムなし（No blocked items）] をクリックします。

c. [検査可能なアーカイブ（Inspectable Archives）] オプションを展開します。[ZIP アーカイブ（ZIP Archive）] を [検査（Inspect）] に設定します。

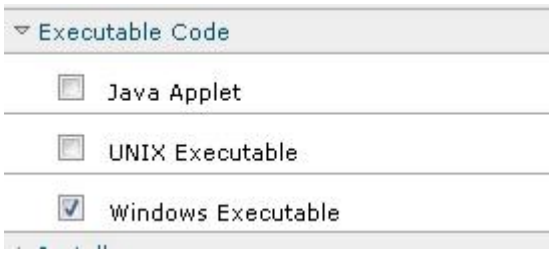


d. [送信（Submit）] をクリック後、[変更を確定（Commit Changes）] をクリックします。

e. Chrome で https://s3-us-west-1.amazonaws.com/testsetupzip/testsetup.zip にアクセスします。**testsetup.zip** ファイルをダウンロードするプロンプトが表示されます。[ダウンロード（Download）] をクリックします。ファイルが正常にダウンロードされます。

f. [グローバルポリシー（Global Policy）] > [オブジェクト（Objects）] に戻ります。[ブロックされたアイテムなし（No Blocked Items）] をもう一度クリックします。

g. [実行可能コード（Executable Code）] を展開し、[Windows 実行可能ファイル（Windows Executable）] を選択します。



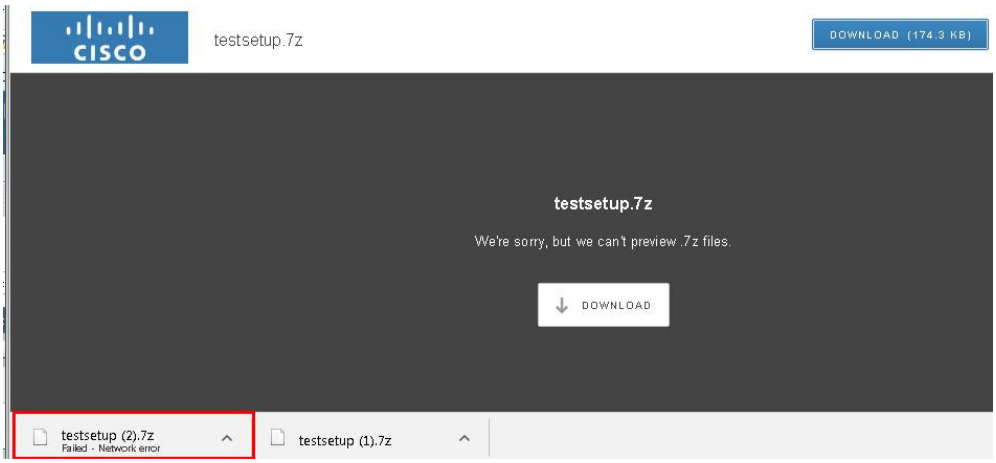
h. 変更を送信して確定します。

3. 変更をテストしてトラッキングします。

a. Putty を開き、WSA CLI に接続します。

b. **tail** を実行し、**3**（archiveinspect_logs）を選択します。

4. Chrome で Box ページを更新するか、https://cisco.box.com/s/mfr48alu4jtgz0dtwpc6w0b808x4zgwx に戻ります。
5. **testsetup.zip** ファイルのダウンロードを再度試みます。今回のダウンロードは失敗するはずです。zip ファイル自体がブロックされない場合は、その中の .exe ファイルがブロックされます。



6. 次のような出力結果が表示されます。Blocked MIME と Inspect MIME タイプのほか、Verdict の内容やブロックされたファイルも確認します。

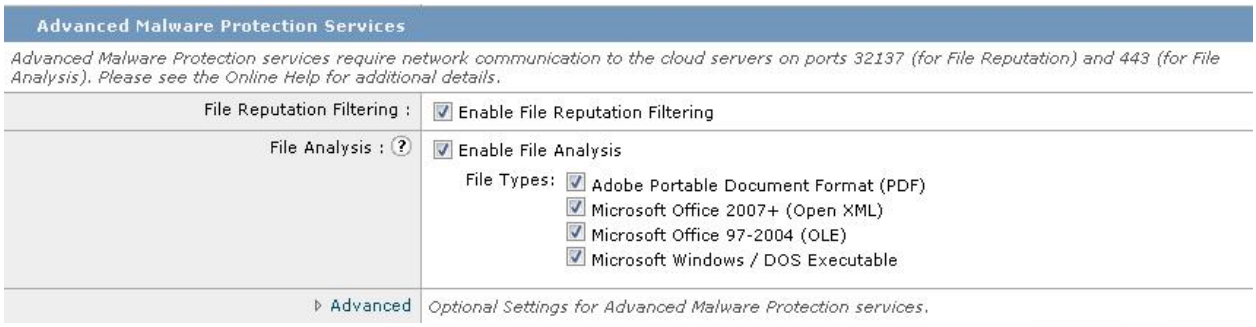
```
05 Apr 2017 19:18:46 (GMT -0700) Info: Request Message from PROX:
05 Apr 2017 19:18:46 (GMT -0700) Info: SoProxId: 152, Method: [Req] RespBodyMimeType: [application/zip; charset=binary]
05 Apr 2017 19:18:46 (GMT -0700) Info: FileName: [download] ResponseBodySize: [178332]Bytes
05 Apr 2017 19:18:46 (GMT -0700) Info: BlockedMimeTypes: [text/x-msdos-batch application/x-dosexec]
05 Apr 2017 19:18:46 (GMT -0700) Info: InspectMimeTypes: [application/zip application/x-7z-compressed]
05 Apr 2017 19:18:46 (GMT -0700) Info: NestLevel: 5, MaxScanSize: [33554432], MaxDiskUse: [1000]MB
05 Apr 2017 19:18:47 (GMT -0700) Info: ------Start of JOBSTATS FileName:[download]------
05 Apr 2017 19:18:47 (GMT -0700) Info: JobID: [5], FileName: [download] JobSize: [178332]
05 Apr 2017 19:18:47 (GMT -0700) Info: Verdict: VERDICT_BLOCKEDMIME  Total Extracted Size [2200]
05 Apr 2017 19:18:47 (GMT -0700) Info: Blocked Mime: [application/x-dosexec], Blocked Filename: [setup.exe]
05 Apr 2017 19:18:47 (GMT -0700) Info: Inspected Nestlevel: [0], Total Nested Archives [0]
05 Apr 2017 19:18:47 (GMT -0700) Info: Num of DataRequests: [11], Files Inspected: [1]
05 Apr 2017 19:18:47 (GMT -0700) Info: Total Job Time: [1094] ms
05 Apr 2017 19:18:47 (GMT -0700) Info: Total Data Download Time: [1088] ms
05 Apr 2017 19:18:47 (GMT -0700) Info: Total UnArchive and Inspection Time: [6] ms
05 Apr 2017 19:18:47 (GMT -0700) Info: ------End of JOBSTATS FileName:[download]------
05 Apr 2017 19:18:47 (GMT -0700) Info: Malloc stats : alloc bytes : 681296, mmap bytes 6174280
```

シナリオ 4：Advanced Malware Protection

タスク A：AMP ファイル レピュテーションとファイル分析の有効化

手順

1. WSA GUI で、[セキュリティサービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] に移動します。
    a. [グローバル設定を編集（Edit Global Settings）] をクリックします（AMP がデフォルトで有効になっていない場合は、次の操作を行って有効化します）。
    b. [高度なマルウェア防御サービス（Advanced Malware Protection Services）] で、[ファイルレピュテーションフィルタを有効にする（Enable File Reputation Filtering）] チェックボックスをオンにします。次の画面で契約に同意します。
    c. もう一度 [グローバル設定を編集...（Edit Global Settings...）] をクリックします。
    d. [高度なマルウェア防御サービス（Advanced Malware Protection Services）] で、[ファイル分析（File Analysis）] チェックボックスをオンにします。次の画面で契約に同意します。
    e. [グローバル設定を編集（Edit Global Settings）] をもう一度クリックします。
    f. [ファイル分析（File Analysis）] の 4 つの [ファイルタイプ（File Types）] をすべて選択します。



    g. [送信（Submit）] をクリック後、[変更を確定（Commit Changes）] をクリックします。

タスク B：アクセス ポリシーでの AMP 制御の設定

手順

1. WSA GUI で、[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）] に移動します。
    a. テーブル下部の [グローバルポリシー（Global Policy）] 行で、[マルウェア対策とレピュテーション（Anti-Malware and Reputation）] 列のテキストをクリックします。
    b. [高度なマルウェア防御設定（Advanced Malware Protection Settings）] で、[ファイルレピュテーションフィルタを有効にする（Enable File Reputation Filtering）] および [ファイル分析を有効にする（Enable File Analysis）] チェックボックスをオンにします。
    c. [悪意のある既知の高リスク ファイル（Known Malicious and High-Risk Files）] については、チェック マークを [ブロック（Block）] に設定します。
    d. ページの下部にある [送信（Submit）] をクリックします。
    e. 変更を完全に確定します（それぞれのページで [変更を確定（Commit Changes）] をクリックします）。

タスク C：ファイル レピュテーション フィルタリングのテスト

手順

1. アクセス ログを別の PuTTY ウィンドウで実行していない場合は、ここで実行できます。アクセス ログの追跡の詳細については、シナリオ 1 を参照してください。
2. Chrome を開きます。
    a. Web サイト http://mysite.science.uottawa.ca/rsmith43/zombies.pdf にアクセスします。
    b. AMP によって PDF がブロックされます。アクセスログには次のエントリが表示されています。

```
1491270162.869 1230 198.19.10.36 TCP_DENIED/403 172449 GET
http://mysite.science.uottawa.ca/rsmith43/zombies.pdf "DCLOUD\wsaproxy@ADrealmDC1"
DIRECT/mysite.science.uottawa.ca application/pdf BLOCK_AMP_RESP_12-DefaultGroup-DefaultGroup-NONE-NONE-
NONE-DefaultGroup <IW_edu,-3.0,0,"-",0,0,0,0,"-",-1,0,-1,"-",0,0,"-","-",-,-,IW_edu,-,"AMP High Risk","-
","Unknown","Unknown","-","-",1121.62,0,-,"Unknown","-
",37,"W32.Zombies.NotAVirus",100,0,"zombies.pdf","00b32c3428362e39e4df2a0c3e0950947c147781fdd3d2ffd0bf5f
96989bb002",3,-,"-"> -
```

タスク D：AMP ファイル レピュテーション レポート

手順

1. WSA GUI で、[レポート（Reporting）] > [高度なマルウェア防御（Advanced Malware Protection）] に移動します。
    a. [時間範囲（Time Range）] を [時間（Hour）] に変更し、ブロックされたトランザクションが zombie.pdf のトランザクションだったことを確認します。出力例のスクリーンショットを以下に示します。

Malware Threat Files

Malware Threat File SHA256	Filenames	Threat Name	File Type	Transactions Monitored	Transactions Blocked
00b32c34...989bb002	zombies.pdf	W32.Zombies.NotAVirus	application/pdf	1	1
Totals (all available data):	--	--	--	1	1

    b. ブロック/モニタされたファイルについて、別のレポート ウィジェットを確認します。[マルウェア脅威ファイル（Malware Threat Files）] テーブルの最初のハッシュ値をクリックします。
    c. 特定のハッシュ値のレポートには、選択したハッシュ値に一致するファイルのダウンロードを試みたすべてのユーザが記載されます。
    d. ページ下部の [一致したファイル（Files Matched）] テーブルに、ダウンロードが試みられたファイルのうち、選択したハッシュ値に一致するファイルが表示されます。いずれかのファイルについてブロックされたトランザクションをクリックすると、ファイルに一致する各トランザクションの詳細な Web トラッキング レポートが表示されます。

タスク E：AMP ファイル分析

手順

1. WSA GUI で、[レポート（Reporting）] > [ファイル分析（File Analysis）] に移動します。
2. 分析済みの各ハッシュ値の横にファイル名が表示されていることを確認します。これも新しい機能です。それぞれの結果の横にある [詳細（Details）] をクリックすると、Web トラッキングにアクセスでき、[結果（Results）] の下に送信元の情報が表示されます。
3. 戻って個々のハッシュ値をクリックすると、[分類/脅威スコア（Classification / Threat Score）] や [一致する署名（Matching signatures）] など、ファイル分析の詳細が表示されます。下部には、分析したファイルの全詳細を確認できる Cisco AMP Threat Grid 用のリンクがあります。
4. 多くの新機能が追加されているので、このセクションを自由に確認してみてください。

シナリオ 5：Cognitive Threat Analytics

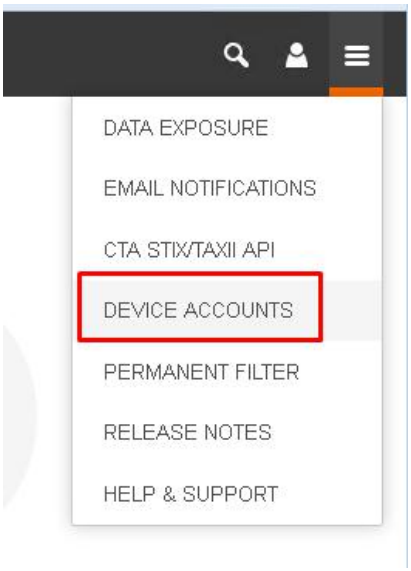
はじめに

Cisco WSA と CTA が統合されたことにより、ふるまいベースの脅威検出を活用して、攻撃の拡散を発見するまでの時間を短縮できるようになりました。この統合により、ふるまい異常検出アルゴリズムおよび信頼モデルを使用して感染の兆候を特定できます。また、機械学習により時間の経過とともに適応していくため、ルールを設定しなくても脅威を検出できるようになります。

タスク A：CTA の設定

手順

1. Firefox から **https://cognitive.cisco.com** にアクセスします。
2. 右上の [顧客ログイン（Customer Login）] をクリックします。
3. ログイン クレデンシャルとして [Web セキュリティ（Web Security）] を選択します。
4. ユーザ名「**ismeet.singh@gmail.com**」、パスワード「**Cisco1234%**」でログインします。
5. [オプション（Options）] タブをクリックし、[デバイスアカウント（Device Accounts）] をクリックします。



6. [デバイスアカウント追加（Add Device Account）] ページが表示されたら、[自動（Automatic）] を選択します。
7. デバイス追加のオプションには、[SCP] と [HTTPS] があります。[SCP] を選択します。
8. WSA[ポッド番号]-SEVTLAB という命名規則に基づいてわかりやすいデバイス名を入力し、[アカウントの追加（ADD ACCOUNT）] をクリックします。たとえば、ポッド番号が 5 の場合、名前は WSA5-SEVTLAB となります。

   注：その名前がすでに使用されている可能性がある場合は、任意の一意の名前を選択してください。

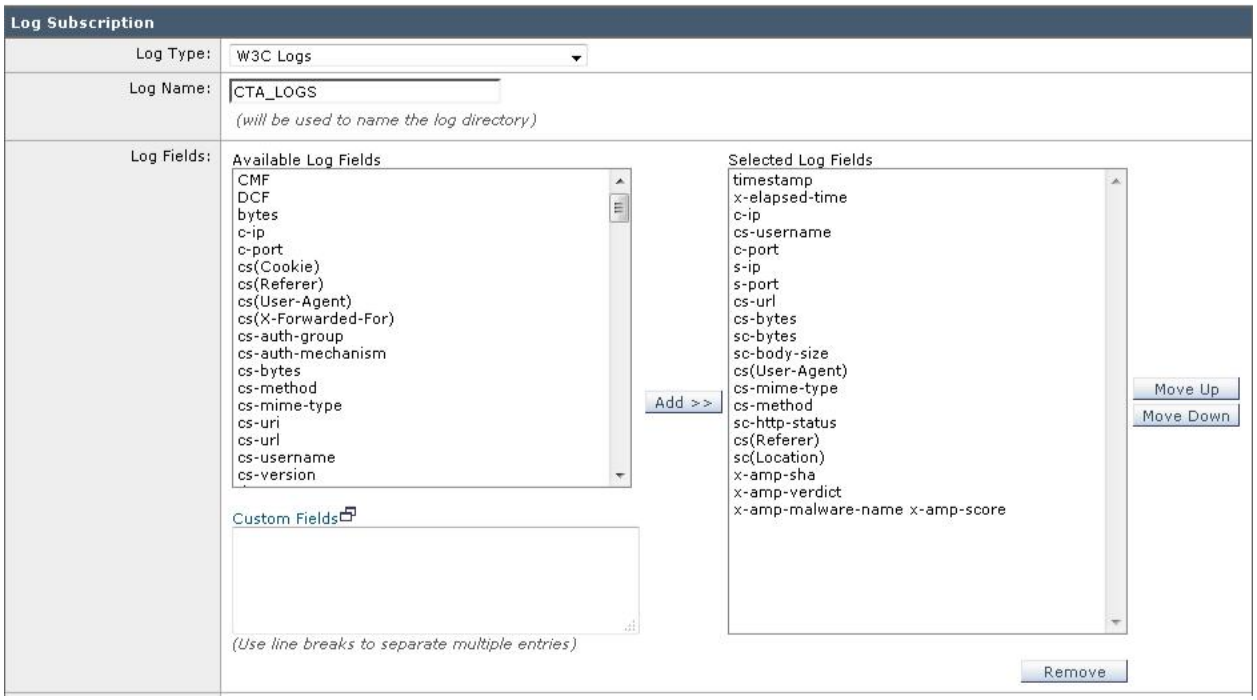
9. 表示された情報を確認します。**このウィンドウは閉じないでください。**演習完了時に、またここに戻ります。

タスク B：WSA の設定

手順

1. WSA UI から [システム管理（System Administration）] > [ログサブスクリプション（Log Subscriptions）] に移動します。
2. [ログサブスクリプションを追加（Add Log Subscription）] をクリックします。
3. [ログタイプ（Log Type）] プルダウンで、[W3C ログ（W3C Logs）] を選択します。
4. [ログ名（Log Name）] フィールドにわかりやすいログ ディレクトリ名を入力します（例：**CTA_LOGS**）。
5. [選択されたログフィールド（Selected Log Fields）] ボックスですべての項目を選択し、[削除（Remove）] をクリックして、事前に選択されたログ フィールドを削除します（タイムスタンプは残ります）。
6. [カスタムフィールド（Custom Fields）] ボックスに、下記の表の項目を入力します。すべての項目を入力したら、[追加（Add）] をクリックします。次の図は、[ログサブスクリプション（Log Subscription）] に表示されるセクションの例です。

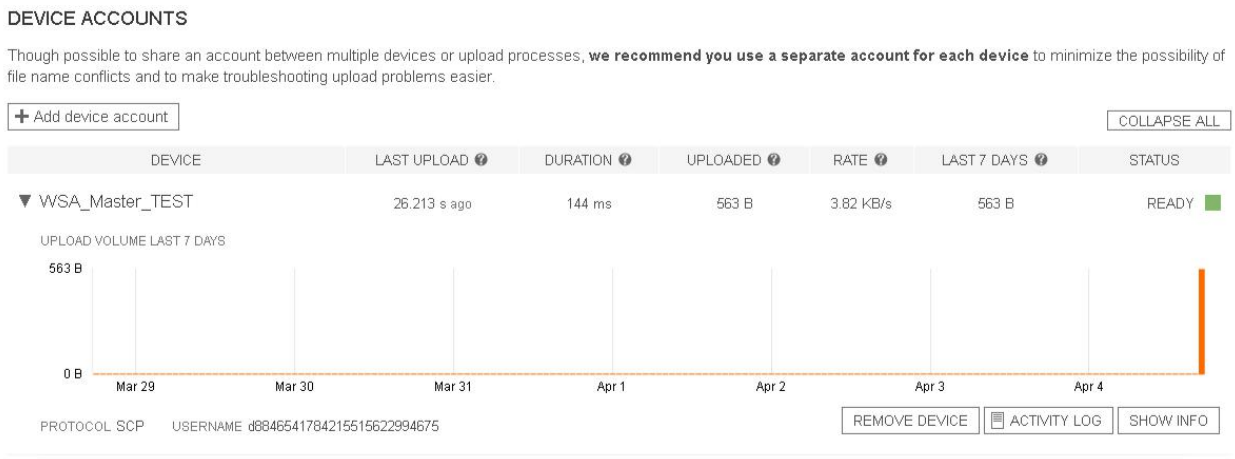
x-elapsed-time
c-ip
cs-username
c-port
s-ip
s-port
cs-url
cs-bytes
sc-bytes
sc-body-size
cs(User-Agent)
cs-mime-type
cs-method
sc-http-status
cs(Referer)
sc(Location)
x-amp-sha
x-amp-verdict
x-amp-malware-name
x-amp-score



7. 次の値を追加します。
    a. [ロールオーバーファイルサイズ（Rollover by File Size）]：500 M
    b. [ロールオーバー時刻（Rollover by Time）]：[カスタム時間間隔（Custom Time Interval）]
    c. [ロールオーバー間隔（Rollover every）]：55 分
    d. [ファイル名（File Name）]：w3c_log
    e. [ログ圧縮（Log Compression）]：[有効（Enable）]
    f. [収集方法（Retrieval Method）]：[リモートサーバでの SCP（SCP on Remote Server）]
        i. [SCP ホスト（SCP Host）]：etr.cloudsec.sco.cisco.com
        ii. [SCP ポート（SCP Port）]：22
        iii. [ディレクトリ（Directory）]：/upload
    g. [ユーザ名（Username）]：Cisco CTA ポータルで自分のデバイス用に生成されたユーザ名を入力します。デバイスユーザ名は大文字と小文字が区別され、プロキシ デバイスごとに異なることに注意してください。
    h. [ホストキーチェックを有効化（Enable Host Key Checking）] チェックボックスをオンにします。
    i. [自動スキャン（Automatically Scan）] オプション ボタンを選択します。
8. [送信（Submit）] をクリックします。
9. ワークステーションで Notepad（メモ帳）を開き、SSH キーをコピーします。
10. [変更を確定（Commit Changes）] をクリックします。[変更を確定（Commit Changes）] ボタンをクリックする前に、わかりやすいコメントを必ず入力してください。
11. SSH キーをコピーしたら、CTA ポータルに戻り、[終了（Finish）] をクリックします。

12. 作成した新しいデバイス インスタンスの横にある [SSH キーを指定（Provide SSH Key）] をクリックします。キーに貼り付けて、[SSH キーを保存（Save SSH Key）] をクリックします。
13. 1 ~ 2 分後に、[オプション（Option）] > [デバイスアカウント（Device Accounts）] の順にクリックします。WSA が登録されると、[ステータス（Status）] が [プロビジョニング（Provisioning）] から [完了（Ready）] に変わります。
14. 正常に接続されていることを検証するために、WSA に戻り [ログサブスクリプション（Log Subscriptions）] をクリックします。
15. 作成したログ サブスクリプションの横にある [ロールオーバー（Rollover）] チェックボックスをクリックします。下方向にスクロールし、[今すぐロールオーバー（Rollover Now）] をクリックします。
16. 成功メッセージが表示されます。

17. CTA ポータルに戻ります。[オプション（Option）] > [デバイスアカウント（Device Accounts）] をもう一度クリックします。今度は、WSA の詳細データが表示され、ログが正常に CTA にアップロードされたことがわかります。

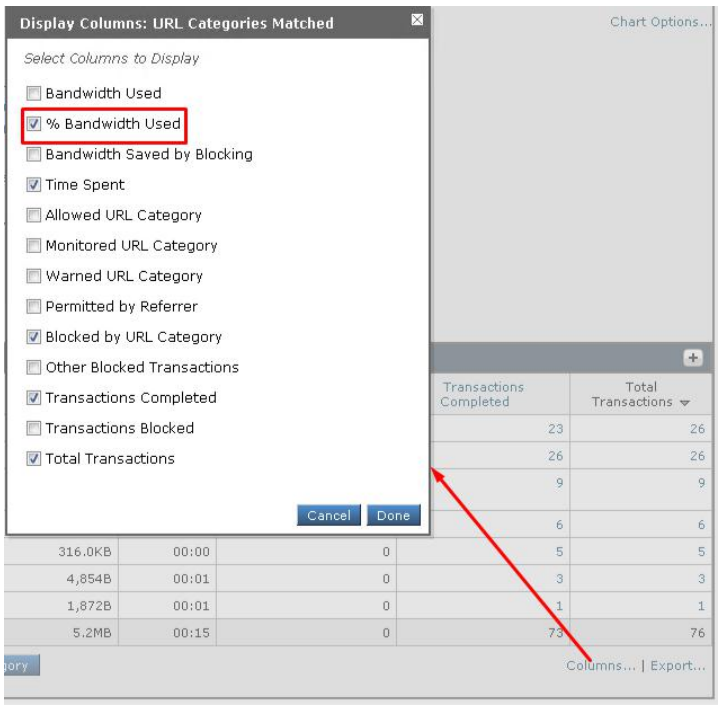


シナリオ 6：レポートおよび Web トラッキング

タスク A：レポートの利用

手順

1. WSA GUI で、[レポート（Reporting）] > [URL カテゴリ（URL Categories）] に移動します。
    a. 全トランザクションでの上位 URL カテゴリを確認します。
    b. ブロックされたトランザクションおよび警告トランザクションでの上位 URL カテゴリを確認します。
    c. [一致した URL カテゴリ（URL Categories Matched）] テーブルで、[使用帯域幅（Bandwidth Used）] を [使用済み帯域幅（%）（%Bandwidth Used）] に変更します。
        i. テーブルの右下の列にある [列...（Columns...）] のテキストをクリックします。
        ii. [使用帯域幅（Bandwidth Used）] チェックボックスをオフにします。[使用済み帯域幅（%）（%Bandwidth Used）] チェックボックスをオンにします。
        iii. [完了（Done）] をクリックします。



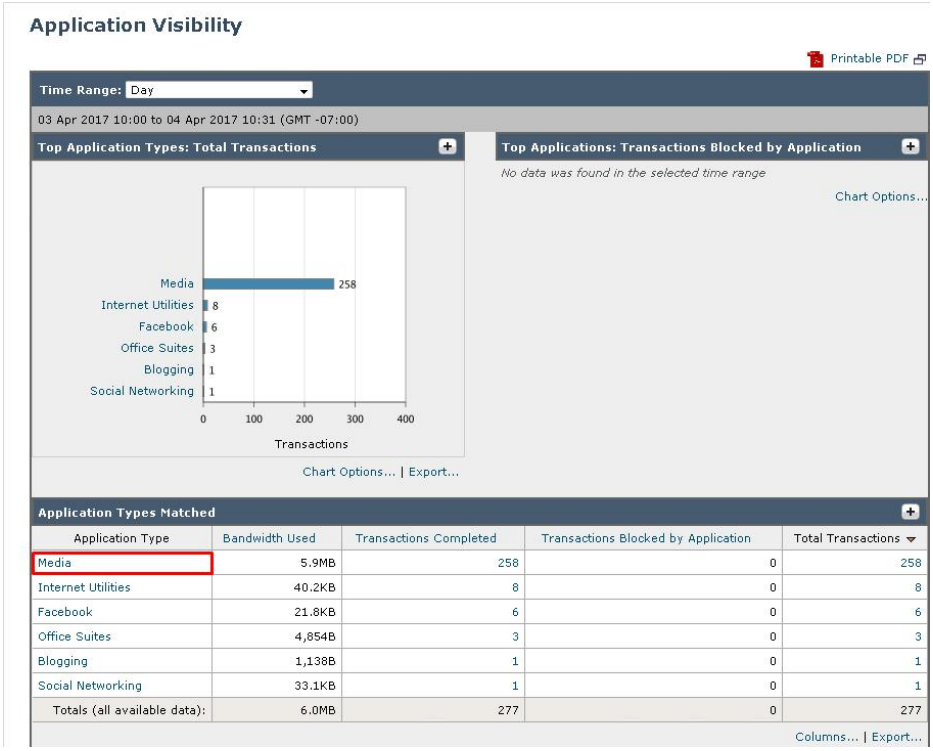
    d. 該当する列の見出しをクリックして、[使用済み帯域幅（%）（% Bandwidth Used）] でテーブルをソートします。
    e. [URL カテゴリ別ブロック数（Blocked by URL Category）] でテーブルをソートし、左側の列にあるカテゴリ名（おそらく「Gambling」）をクリックします。
    f. 全トランザクションでのこのカテゴリの上位サイトと上位ユーザを確認します。
    g. [Web ユーザ（Web Users）] テーブルで、上位ユーザの名前をクリックします。このユーザの詳細情報をメモしてください。

2. アプリケーションの可視性

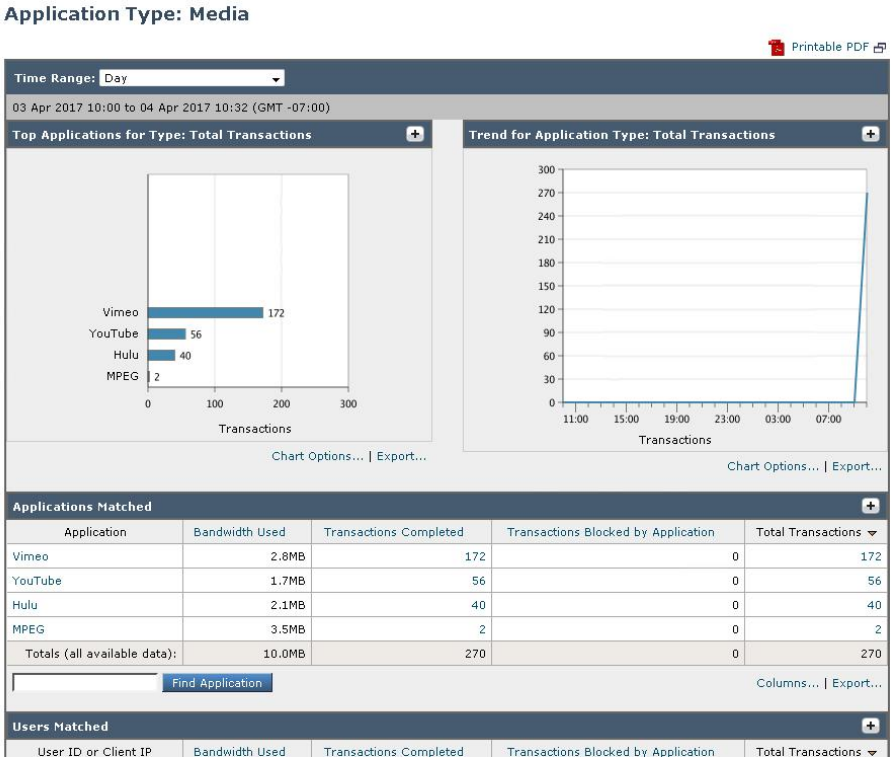
   a. Chrome に移動し、さまざまなビデオ Web サイトを閲覧します（例：youtube.com、hulu.com、vimeo.com、order.hbonow.com）。

   b. WSA GUI で、[レポート（Reporting）] > [アプリケーションの可視化（Application Visibility）] に移動します。

   c. [一致したアプリケーションタイプ（Application Types Matched）] テーブルに [メディア（Media）] と表示されていることを確認します。



d. [メディア（Media）] をクリックします。ストリーミング ビデオ サイトのトランザクションの詳細が表示されます。



3. WSA GUI で、[レポート（Reporting）] > [マルウェア対策（Anti Malware）] に移動します。

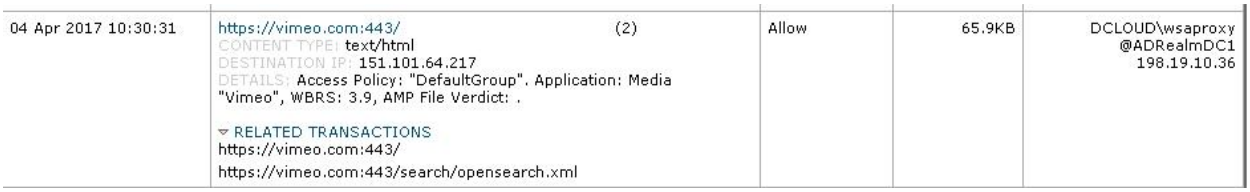
注：[マルウェアの脅威（Malware Threats）] テーブルに EICAR テスト ファイルが表示されています。このファイルが表示されているのは、eicar.com テストファイルのダウンロードを試みたからです。

4. 以下のように、その他のレポートも簡単に確認していきます。
   a. [レポート（Reporting）] > [クライアントマルウェア（Client Malware）]
   b. [レポート（Reporting）] > [ユーザ（Users）]
   c. [レポート（Reporting）] > [Web サイト（Web Sites）]
   d. [レポート（Reporting）] > [Web レピュテーションフィルタ（Web Reputation Filters）]

タスク B：Web トラッキングの活用

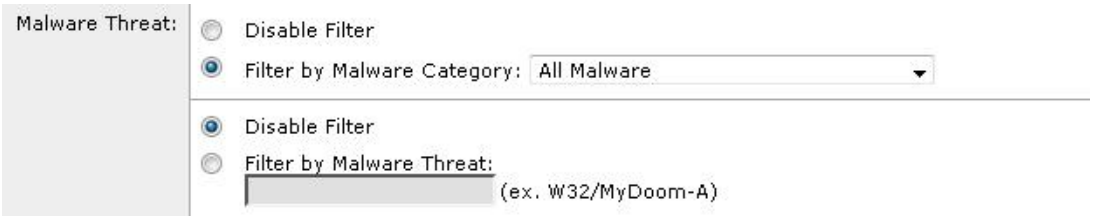
手順

1. WSA GUI で、[レポート（Reporting）] > [Web トラッキング（Web Tracking）] に移動します。[検索（Search）] ボックスで次のように操作します。
    a. [時間範囲（Time Range）] で [日（Day）] を選択します。
    b. [ユーザ/クライアント IP（User/Client IP）] は空白のままにします。
    c. [Web サイト（Website）] には、cisco.com または、以前閲覧した Web サイトを入力します。
    d. [トランザクションタイプ（Transaction Type）] で [すべてのトランザクション（All Transactions）] を選択します。
    e. [検索（Search）] ボタンをクリックします。
    f. [結果（Results）] テーブルで、[詳細の表示...（Display Details...）] テキストをクリックします。
    g. いずれかのトランザクションについて、[関連トランザクション（RELATED TRANSACTIONS）] というテキストをクリックします。
    h. ページに関連付けられた HTML のコンポーネント（イメージ、Javascript など）が表示されることを確認してください。



2. Web トラッキング検索を次のように変更します。[検索（Search）] ボックスで次のように操作します。
    a. [Web サイト（Website）] を空白にします。
    b. [トランザクションタイプ（Transaction Type）] を [ブロック（Blocked）] に変更します。
    c. [検索（Search）] ボタンをクリックします。
    d. [結果（Results）] テーブルで、トランザクションのいずれか 1 つをクリックします。
    e. 脅威の詳細とトランザクションがブロックされた理由を確認してください。

3. Web トラッキング検索を次のように変更します。[検索（Search）] ボックスで次のように操作します。
    a. [トランザクションタイプ（Transaction Type）] を [すべてのトランザクション（All Transactions）] に戻します。
    b. [詳細（Advanced）] をクリックし、詳細な条件を使用してトランザクションを検索します。
        i. [マルウェアの脅威（Malware Threat）] で、[マルウェアのカテゴリでフィルタ（Filter by Malware Category）] オプション ボタンを選択します。
        ii. ドロップダウン メニューから [すべてのマルウェア（All Malware）] を選択します。



    c. [検索（Search）] ボタンをクリックします。
    d. [結果（Results）] ボックスに表示される結果から、さまざまなユーザ トランザクションがブロックされたことがわかります。
4. Web トラッキング検索を次のように変更します。
5. [検索（Search）] ボックスで、[詳細（Advanced）] をクリックし、詳細な条件でトランザクションを検索します。
    a) [高度なマルウェア防御（Advance Malware Protection）] で、[ファイル名でフィルタ（Filter by Filename）] オプション ボタンを選択します。
    b) [ファイル名でフィルタ（Filter by Filename）] テキスト フィールドに「Zombies.pdf」と入力します。
    c) [時間範囲（Time Range）] で [日（Day）] を選択します。
    d) [検索（Search）] ボタンをクリックします。
    e) [結果（Results）] ボックスに次のように表示されます。

Results

Displaying 1 - 3 of 3 items.

Time (GMT -07:00)	Website (count)	Display All Details...	Disposition	Bandwidth	User / Client IP
27 Sep 2016 10:44:05	https://mysite.science.uottawa.ca:443/rsmith43/Zombies.pdf CONTENT TYPE: application/pdf DESTINATION IP: 137.122.152.27 DETAILS: Access Policy: "DefaultGroup". WBRS: 4.9, AMP Verdict: Malware, Malware Threat: W32.Zombies.NotAVirus, Filename: Zombies.pdf, SHA256: 00b32c3428362e39e4df2a0c3e0950947c147781fdd3d2ffd0bf5f96989bb002, AMP File Verdict: Malicious.		Block - AMP	0B	eyetea @ADRealmDC1 10.1.1.101
27 Sep 2016 10:43:18	https://mysite.science.uottawa.ca:443	(2)	Block - AMP	0B	eyetea 10.1.1.101
27 Sep 2016 10:42:52	https://mysite.science.uottawa.ca:443		Block - AMP	0B	eyetea 10.1.1.101

Displaying 1 - 3 of 3 items.

シナリオ 7：リファラ ヘッダー

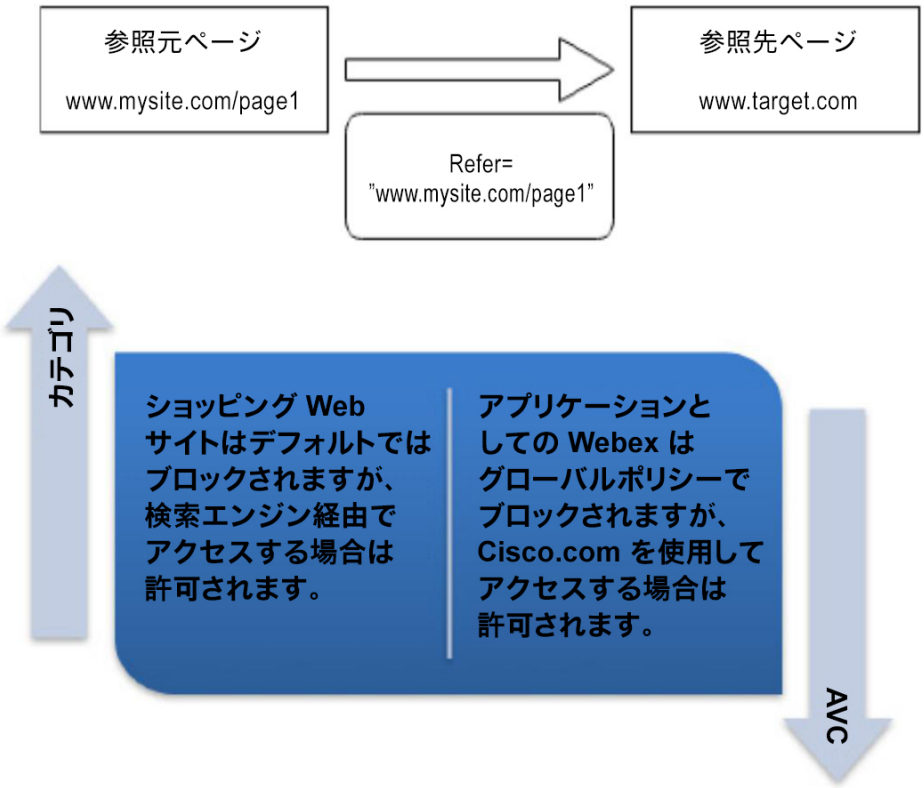
はじめに

リファラとは、現在の Web ページの要求元となった Web ページを特定できる HTTP ヘッダー フィールドのことです。リファラ フィールドを使用して、Web サイトが参照された際の URL を確認したり、アクセス ポリシーを定義したりすることができます。

このラボでは、リファラ ヘッダーを使用して以下の 2 つの使用例に対応しました。

1: **カテゴリ**：事前定義済みブロック カテゴリ/カスタム ブロック カテゴリに含まれている URL であっても、特定のカテゴリから参照される場合、アクセスを有効にする。

2: **AVC**：ブロック対象アプリケーションであっても、特定のカテゴリから参照される場合、アクセスを有効にする。



タスク A：カテゴリ

手順

1. WSA GUI で、[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）] に移動します。
2. [ポリシーを追加（Add Policy）] をクリックします。
3. [ポリシー名（Policy Name）] に、「Referrer Header」という名前を入力します。
4. [識別プロファイルとユーザ（Identification Profiles and Users）] で、[グループとユーザ（Group & Users）] を選択し、[グループが入力されていません（No Group Entered）] をクリックします。
5. [ディレクトリ検索（Directory Search）] で、[DCLOUD\Nurses] を選択し、[追加（Add）] をクリックします。
6. [完了（Done）] をクリックします。
7. [送信（Submit）] をクリックします。
8. 次に、[リファラヘッダーポリシー（Referrer Header Policy）] で、[URL フィルタ（URL Filtering）] をクリックします。
9. [ショッピング（Shopping）] が表示されるまで下方向にスクロールして、[ブロック（Block）] を設定します。
10. [送信（Submit）] をクリック後、コメントを記載してから [変更を確定（Commit Changes）] をクリックします。
11. WSA CLI から、**authcache** コマンドを実行し、続けて flushall コマンドを実行します。

```
wsa-hq1.dcloud.cisco.com> authcache


Choose the operation you want to perform:
- FLUSHALL - Flush all entries from auth cache
- FLUSHUSER - Flush specific user entry from auth cache
- LIST - List all entries from auth cache
- SEARCH - Search all entries from auth cache
[]> flushall

Are you sure that you want to flush all entries? [Y]> Y

2 entries in authentication cache flushed
```

12. IE で、クッキーとユーザ クレデンシャルを消去し、ブラウザを再起動します
13. ユーザ名「**aroberts**」、パスワード「**C1sco12345**」を使用してログインします。
14. www.bestbuy.com または www.Amazon.com にアクセスします。ブロックされ、EUN が表示されます（想定どおりの動作）。
15. ここで [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）] > [リファラヘッダー（Referrer Header）] > [URL フィルタ（URL Filtering）] に戻ります。下方向にスクロールします。[リファラの例外（Referrer Exceptions）] をオンにして有効化します。
16. [これらのカテゴリから参照されるコンテンツに例外を設定する（Set Exception for content Referred by these categories）] で、[カテゴリの選択（Select Categories）] をクリックします。
17. [検索エンジンおよびポータル（Search Engines and Portals）] を選択し、[完了（Done）] をクリックします。

18. 下方向にスクロールし、[この参照コンテンツに例外を設定する（Set Exception for This Referred Content）] の下で、[埋め込み/参照コンテンツ（Embedded/Referred content）] を選択します。
19. [カテゴリの選択（Select Categories）] > [ショッピング（Shopping）] の順にクリックしてから、[完了（Done）] をクリックします（注：ブロック対象はこのカテゴリのみだったため、このカテゴリだけ強調表示されます）。
20. [送信（Submit）] をクリック後、[変更を確定（Commit Changes）] をクリックします。
21. 再度 www.amazon.com にアクセスしてもブロックされます。
22. 次に、www.google.com にアクセスして「amazon」を検索します。
23. 最初に出てきた結果（www.amazon.com）をクリックすると、www.amazon.com にリダイレクトされます（www.google.com を経由しているため、www.amazon.com にアクセス可能になっています）。
24. 次に、リファラ ヘッダーに関するレポートを探すために、下記を実施してレポートをクリックします。
    a. [WSA GUI] > [レポート（Reporting）] > [Web サイト（Web Sites）]
    b. [時間範囲（Time Range）] で [日（Day）] を選択します。
    c. [上位ドメイン（Top Domains）] で、[チャートオプション（Chart Option）] > [リファラにより許可（Permitted by Referrer）] を選択し、[保存（Save）] をクリックします。
    d. これにより、リファラによって許可された上位ドメインが表示されます。
    e. [URL カテゴリ（URL Categories）] の [リファラ（Referrer）] レポートについても、[WSA GUI] > [レポート（Reporting）] > [URL カテゴリ（URL Categories）] の順に実行します。

注：レポートの結果がすぐに表示されない場合は、次のシナリオを完了した後で再度確認してください。これらのレポートが表示されるまで時間がかかる場合があります。

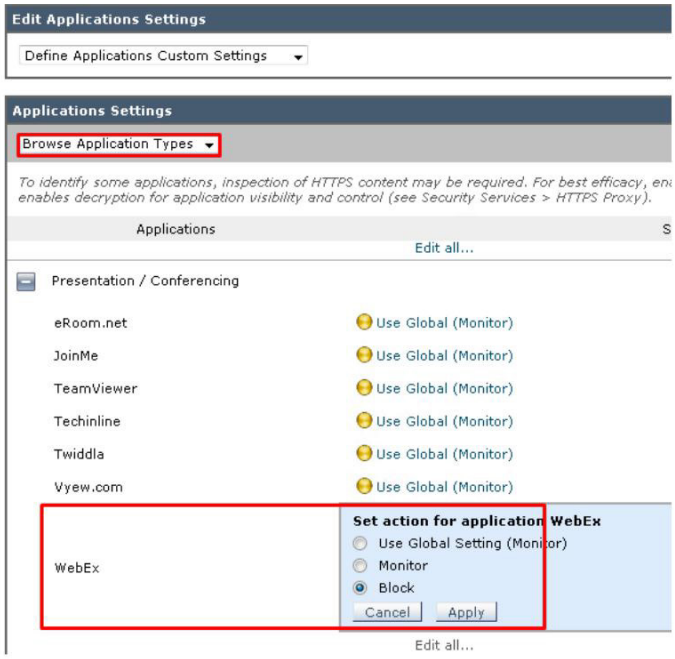
タスク B：AVC

手順

1. アプリケーションとしての Webex をブロックします。
    a. [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）] > [Referrer Header] ポリシーの順に移動し、[アプリケーション（Applications）] の下のリンクをクリックします。

b. [アプリケーション設定の編集（Edit Application Settings）] > [アプリケーションカスタム設定の定義（Define Application Custom Settings）] > [プレゼンテーション/会議（Presentation/Conferencing）] の（+）記号をクリックします。

c. [Webex] の [グローバル設定を使用（モニタ） （Use Global Setting(Monitor)）] を [ブロック（Block）] に変え、[適用（Apply）] をクリック後 [送信（Submit）] をクリックし、[変更を確定（Commit Changes）] を 2 回クリックします。



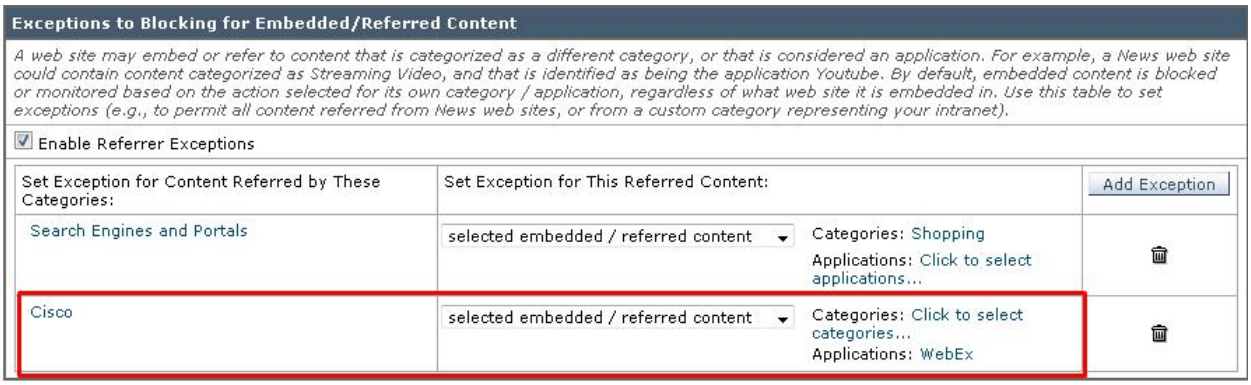
d. www.Webex.com にアクセスすると、AVC によってブロックされます。

2. WSA GUI に戻り、[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 & External URL Categories）] に移動します。[カテゴリの追加（Add category）] をクリックします。
3. [カテゴリ名（Category Name）] に「Cisco」と入力し、[カテゴリタイプ（Category Type）] で [ローカルカスタムカテゴリ（Local Custom Category）] を選択します。
4. [サイト（Sites）] で、[.cisco.com] と [www.webex.com] を選択します（注：Webex は [セルフリファラ（Self Referrer）] として追加されています）。

注：ここに追加するのは www.cisco.com ではなく .cisco とすることに注意してください。これにより、Cisco.com の下にあるサブドメインもすべて対象に含まれることになります。

5. [送信（Submit）] をクリック後、[変更を確定（Commit Changes）] をクリックします。
6. 次に、[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）] > [リファラヘッダー（Referrer Header）] > [URL フィルタ（URL Filtering）] の順に移動します。
7. [リファラの例外（Referrer Exceptions）] が表示されるまで下方向にスクロールします。
8. [例外を追加（Add Exception）] をクリックします。
9. [カテゴリの選択（Select Categories）] をクリックし、[Cisco] を追加します。[完了（Done）] をクリックします。
10. [この参照コンテンツに例外を設定する（Set Exception for This Referred Content）] の下で、[埋め込み/参照コンテンツ（Embedded/Referred content）] を選択します。

11. 次に、[アプリケーション（Application）] で [アプリケーション：Webex（Applications: Webex）] を追加します。[完了（Done）] をクリックします。



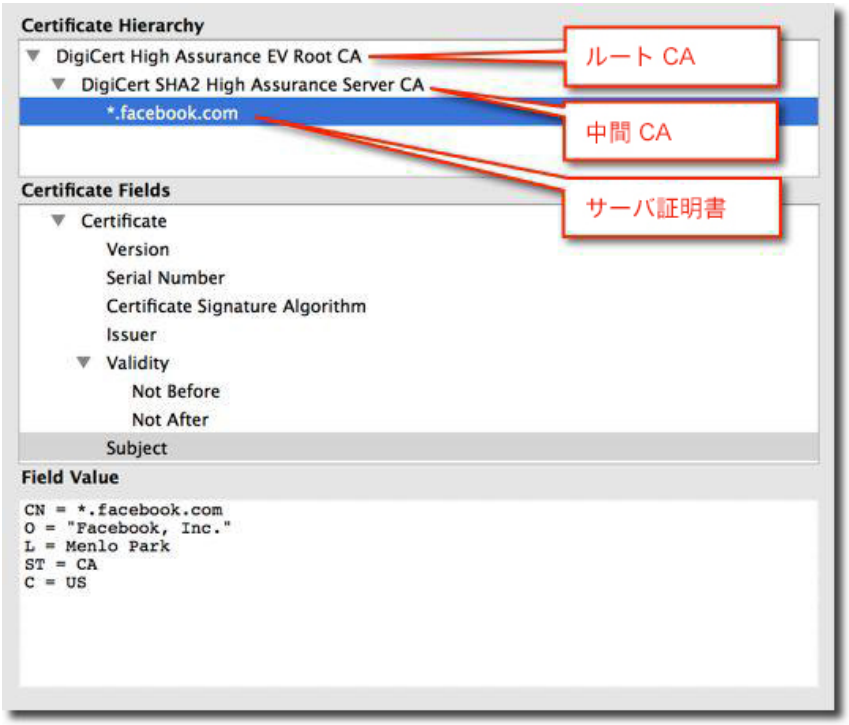
12. [送信（Submit）] をクリック後、[変更を確定（Commit Changes）] をクリックします。
13. IE で www.cisco.com にアクセスし、検索キーワードとして「webexwebex」を入力します。
14. この検索結果で最初に表示される URL は www.webex.com です。
15. この URL をクリックすると webex.com の Web サイトが開きます。
16. 次に、リファラ ヘッダーに関するレポートを探すために、[WSA GUI] > [レポート（Reporting）] > [Web サイト（Web Sites）] の順に移動してレポートをクリックします。
17. [時間範囲（Time Range）] で [日（Day）] を選択し、[上位ドメイン（Top Domains）] の [チャートオプション（Chart Option）] で [リファラにより許可（Permitted by Referrer）] を選択します。これにより、リファラによって許可された上位ドメインが表示されます。
18. [URL カテゴリ（URL Categories）] の [リファラ（Referrer）] レポートについても、[レポート（Reporting）] > [URL カテゴリ（URL Categories）] の順に実行します。

シナリオ 8：中間証明書

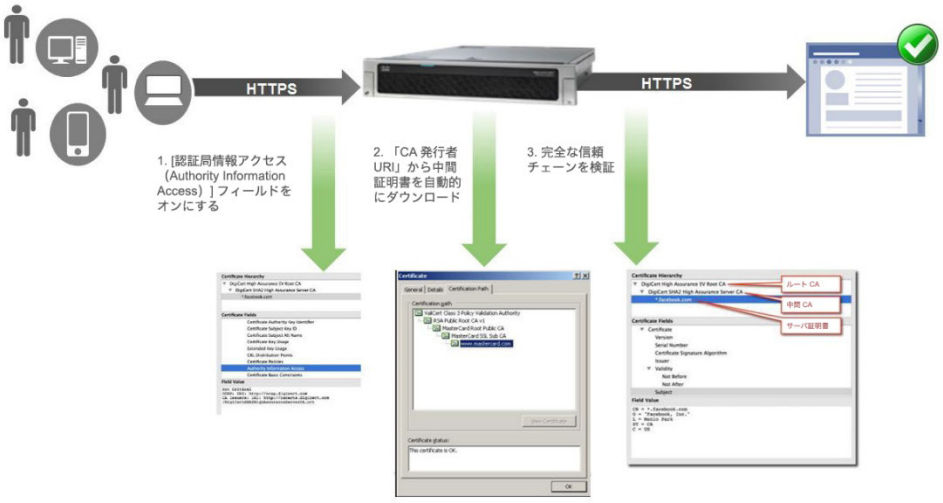
はじめに

HTTPS Web サイトに接続する場合、Web サーバは、SSL 証明書を提示する際に、完全な信頼チェーンを送信することになっています。ただし、Web サーバが信頼チェーンの構築に失敗し、サーバ証明書のみを送信する場合もあります。この場合、信頼チェーンが構築できないため、クライアントはエラーを表示します。

想定される信頼チェーン



証明書が欠落している場合の WSA の動作

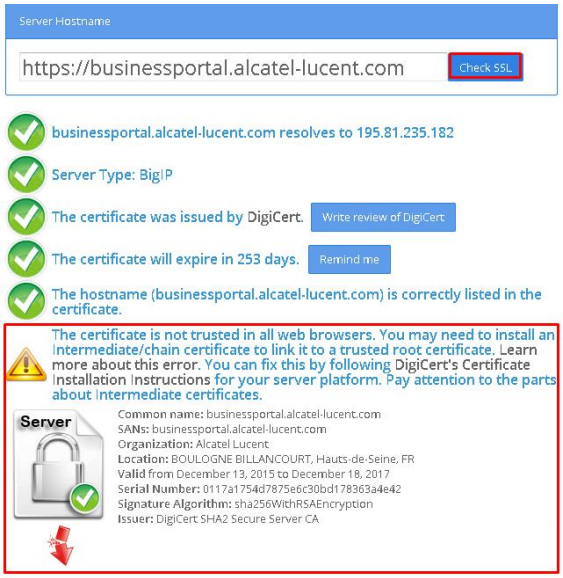


手順

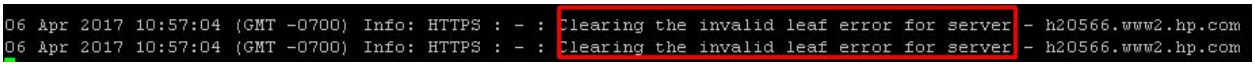
1. Firefox ブラウザを開きます。
2. リンクが壊れているかどうかをテストするため、[URL] > [https://www.sslshopper.com/ssl-checker.html] に移動します。
3. 上記サイトで次のリンクを入力して、リンクが壊れているかどうかをテストします。

https://businessportal.alcatel-lucent.com
https://h20566.www2.hp.com/hpsc/wc/public/home

4. 以下のスクリーンショットのような結果が表示されます。



5. Putty クライアントを開いて wsa-hq1 にログインします。
6. **tail httpslog** を実行します。
7. Chrome を開き、上記リストの Web サイトにアクセスします。どちらのページも正常に読み込めるはずです。
8. 中間証明書が無効または欠落している場合は、CLI コマンドに「Clearing the Invalid leaf error for server - <URL>（サーバ - <URL> の無効なリーフ エラーをクリアしています）」というエラー メッセージが表示されます。



シナリオ 9：サード パーティ フィード

はじめに

この機能により、WSA が外部（またはサード パーティ）のフィード サーバと通信してデータを取得し、それに基づいて WSA 上でポリシーを作成することが可能になります。その後このデータは、フィード内容の変更に応じて定期的に更新されます。

外部のフィード サーバからインポートされたデータは、WSA 上でカスタム URL カテゴリに追加されます。新しいデータが利用可能になるたびに取得され、対応するカスタム URL カテゴリが更新されます。

WSA 管理者は、URL カテゴリに基づいて適切なポリシーを作成できます。設定された URL カテゴリ（ブラックリスト）に一致するトラフィックをブロックするポリシーや、ホワイトリストに一致するトラフィック向けのサービスをバイパスするポリシーなどを作成できます。

WSA は最大 5 つまで外部フィード サーバをサポートします。フィード サーバから取得されて WSA の設定に保存されるデータは、WSA が再起動した後も保持されます。

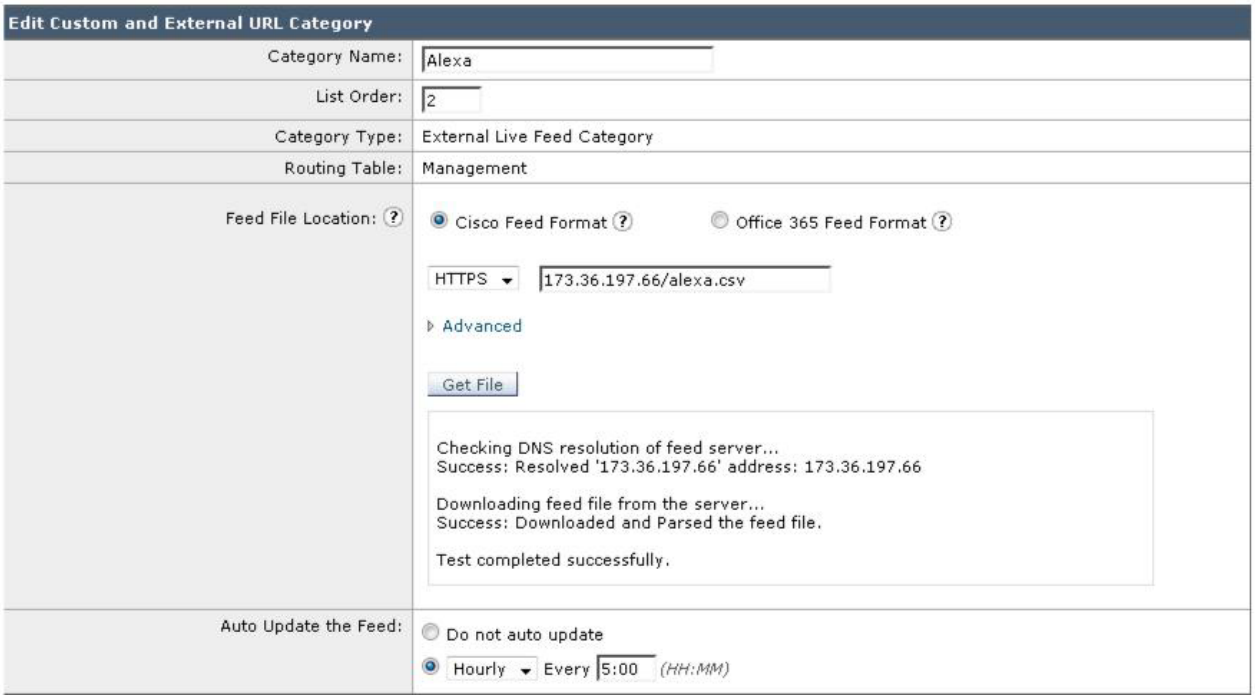
この演習では、Microsoft Office 365 サービス関連の IP と URL のリストが含まれる公式の Office 365 フィードも使用します。

タスク A：サード パーティ フィードとの統合

手順

1. [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）] の順に移動します。
2. [カテゴリを追加（Add Category）] をクリック後、[カテゴリ名（Category Name）] の下の [Alexa] をクリックします。
3. 次に、[カテゴリタイプ（Category Type）] を [外部ライブフィードカテゴリ（External Live Feed Category）] に変更し、[シスコフィード（Cisco Feed）] > [HTTPS] を選択します。
4. [ファイルの取得（Get File）] をクリックします（注：認証は不要です）。

5. [フィードを自動更新（Auto Update the Feed）] で [5 時間ごと（Hourly Every 5）] を選択します。



6. [送信（Submit）] をクリックします。
7. 送信後、[フィードの内容（Feed Content）] > [表示（View）] で表示される内容（外部フィードから取得した全 URL のリスト）を確認し、変更を確定します。
8. 変更確定後、[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。[リファラヘッダー（Referrer Header）] がリストの先頭にあるのを確認します。ない場合は、[グループ（Group）] の下のテキスト [リファラヘッダー（Referrer Header）] をクリックします。このポリシーがリストの先頭に移動したことも確認します。

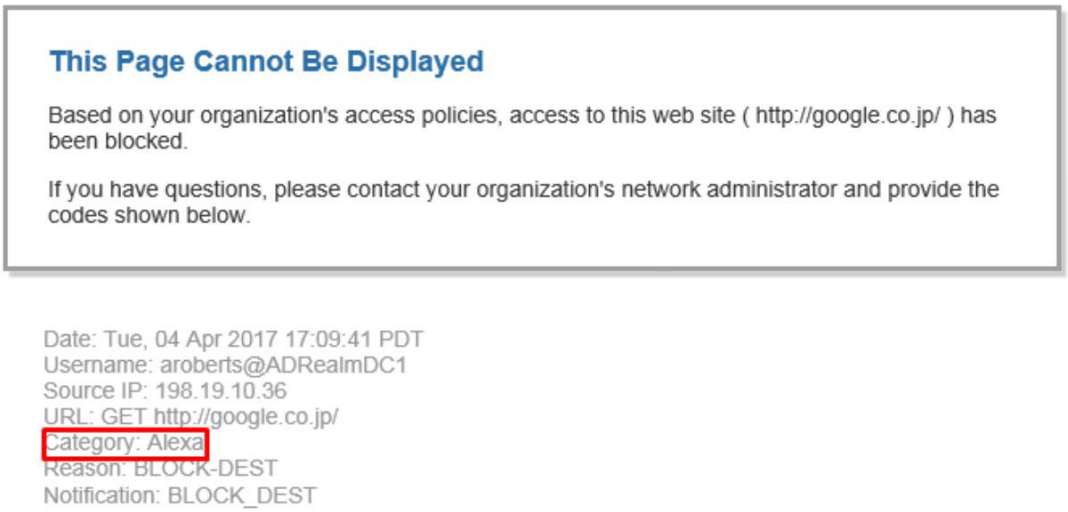
9. もう一度 [Web セキュリティマネージャ（Web Security Manager）] > [アクセスポリシー（Access Policies）] > [リファラヘッダー（Referrer Header）] > [URL フィルタ（URL Filtering）] の順に移動します。
10. [カスタムカテゴリの選択（Select Custom Categories）] > [Alexa] > [ポリシーに含める（Include in Policy）] > [適用（Apply）] の順にクリックします。

11. [グローバル設定をオーバーライド（Override Global Settings）] ペインで [ブロック（Block）] を選択し、[送信（Submit）] をクリック後 [変更を確定（Commit changes）] します。

12. IE で、下記の Web サイトにアクセスします。これらのサイトは、Web セキュリティ アプライアンスによって自動的にブロックされるようになっています。

taobao.com
msn.com
yahoo.co.jp
linkedin.com
google.co.jp
sina.com.cn
weibo.com
Wikipedia.org
yandex.ru

13. これらのサイトはカスタム カテゴリに基づいてブロックされます。

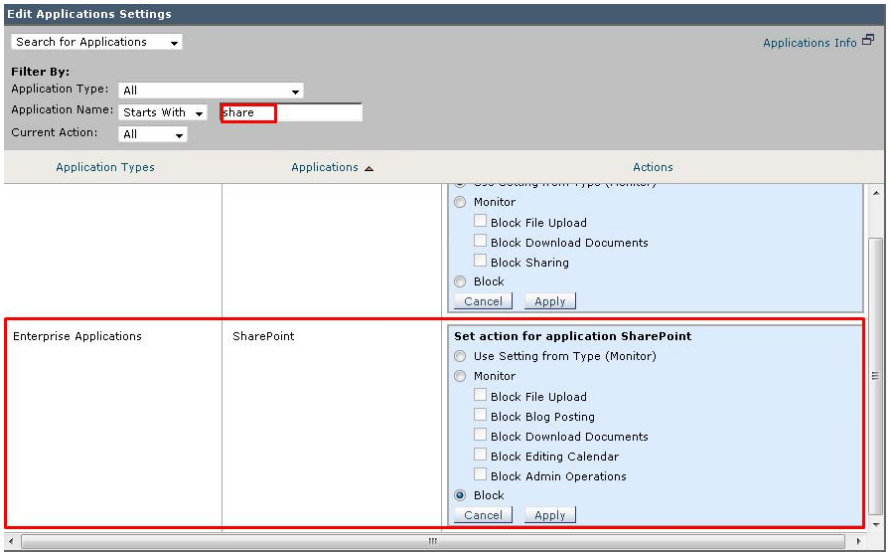


注：このフィードは継続的に更新されているため、上記のうちいくつかのサイトがブロックされない可能性もあります。ただし、ほとんどはブロックされるはずです。

タスク B：Office 365 の互換性

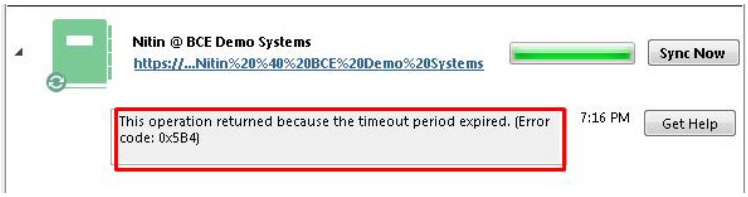
手順

1. Office 365 アプリケーション用に AVC ブロックを設定します。
    a. [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。
    b. [グローバルポリシー（Global Policy）] の [アプリケーション（Applications）] 列をクリックします。
    c. [アプリケーション設定の編集（Edit Application Settings）] が表示されるまで下方向にスクロールし、[アプリケーションを検索（Search for Applications）] を選択します。
    d. テキスト フィールドに「**Sharepoint**」と入力します。
    e. 2 つの [アプリケーションタイプ（Application Types）] に Sharepoint が表示されます。[エンタープライズアプリケーション（Enterprise Applications）] で [ブロック（Block）] を選択して [適用（Apply）] をクリックします。



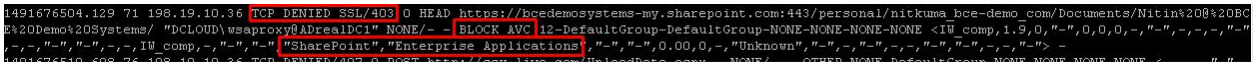
    f. [送信（Submit）] をクリック後、[変更を確定（Commit Changes）] をクリックします。
    g. 次に、タスクバーの [OneNote] アプリケーションをクリックします。 
    h. ページ内の任意の場所にメモを入力します。
    i. [ファイル（File）] に移動し、[同期ステータスの表示（View Sync Status）] をクリックします。
    j. オプション ボタンを [手動同期（Sync manually）] に設定し、[今すぐ同期（Sync Now）] ボタンをクリックします。

k. エラーが表示されます。



l. [閉じる（Close）] をクリックします。

m. オプションで、WSA CLI から **tail accesslogs** を実行できます。次のエントリを確認します。



注：OneNote を含む多くの Office 365 アプリケーションで、クラウドとの同期に Sharepoint サービスが利用されています。アクセス ポリシー内で Sharepoint がブロックされたときに同期プロセスが中断したのは、そのためです。

2. サード パーティ フィードを設定します。

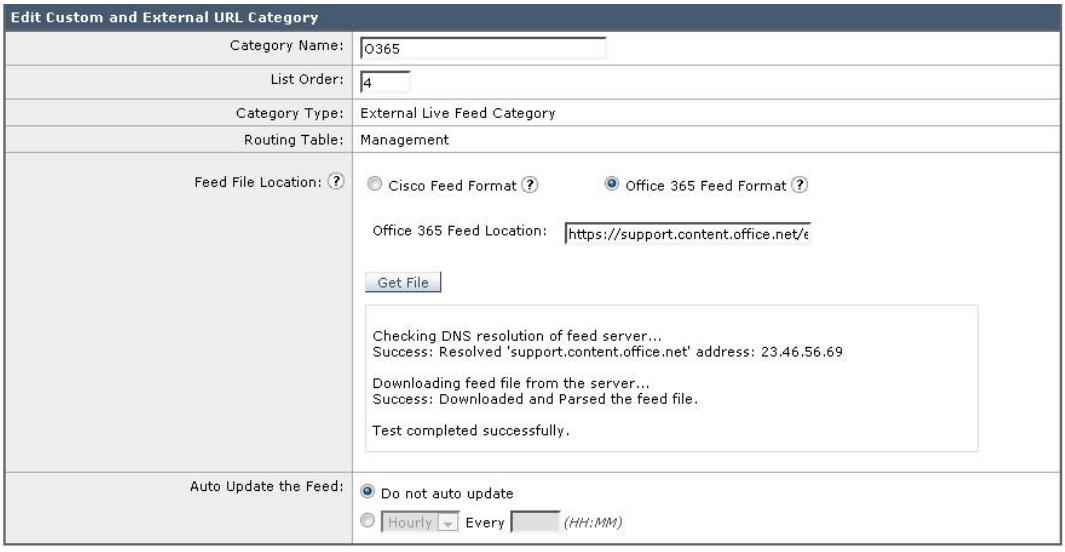
a. [Web セキュリティマネージャ（Web Security Manager）] > [カスタムおよび外部 URL カテゴリ（Custom and External URL Categories）] の順に移動します。

b. [カテゴリの追加…（Add category…）] をクリックします。

c. [カテゴリ名（Category Name）] に「**O365**」と入力し、[カテゴリタイプ（Category Type）] に [外部ライブフィードカテゴリ（External Live Feed Category）] を選択します。

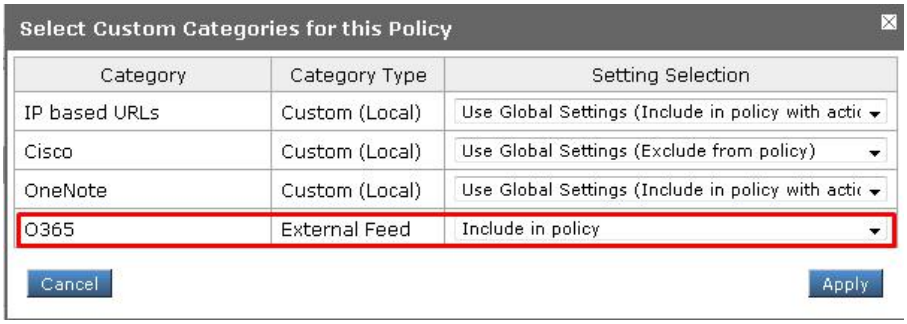
d. [フィードファイルの場所（Feed File Location）] に [Office 365 フィード形式（Office 365 Feed Format）] を選択し、URL「https://support.content.office.net/en-us/static/O365IPAddresses.xml」を入力します。

e. [ファイルの取得（Get File）] をクリックします。成功メッセージが表示されます。

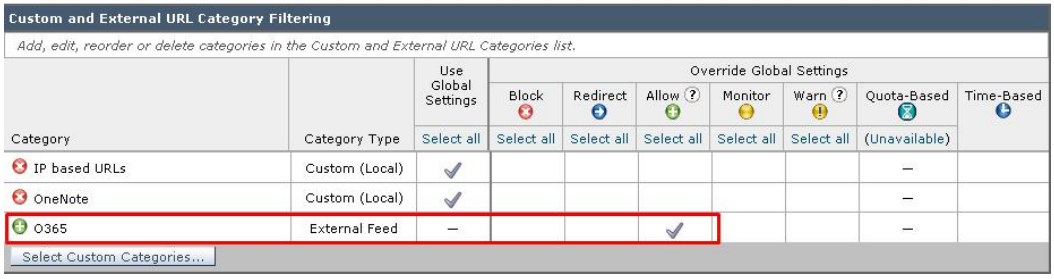


f. [送信（Submit）] をクリック後、[変更を確定（Commit Changes）] をクリックします。

3. アクセス ポリシーを作成します。
    a. [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。
    b. [ポリシーを追加（Add Policy）] をクリックします。
    c. ポリシー名を「**O365**」とします。
    d. [すべての認証済みユーザ（All Authenticated Users）] が選択されていることを確認し、[送信（Submit）] をクリック後、[変更を確定（Commit Changes）] をクリックします。
    e. 新しく作成したポリシーの [URL フィルタ（URL Filtering）] 列をクリックします。
    f. [カスタムカテゴリの選択（Select Custom Categories）] をクリックして、[O365] カテゴリに対して [ポリシーに含める（Include in policy）] を選択し、[適用（Apply）] をクリックします。



    g. [グローバル設定をオーバーライド（Override Global Settings）] オプションを [許可（Allow）] に設定します。



    h. [送信（Submit）] をクリック後、[変更を確定（Commit Changes）] をクリックします。
    i. OneNote に戻り、[ファイル（File）] をクリックします。
    j. [同期ステータスの表示（View Sync Status）] をクリックします。
    k. もう一度、[手動同期（Sync manually）] が選択されていることを確認し、[今すぐ同期（Sync Now）] をクリックします。
    l. 当初のエラーは表示されなくなり、次が表示されます。

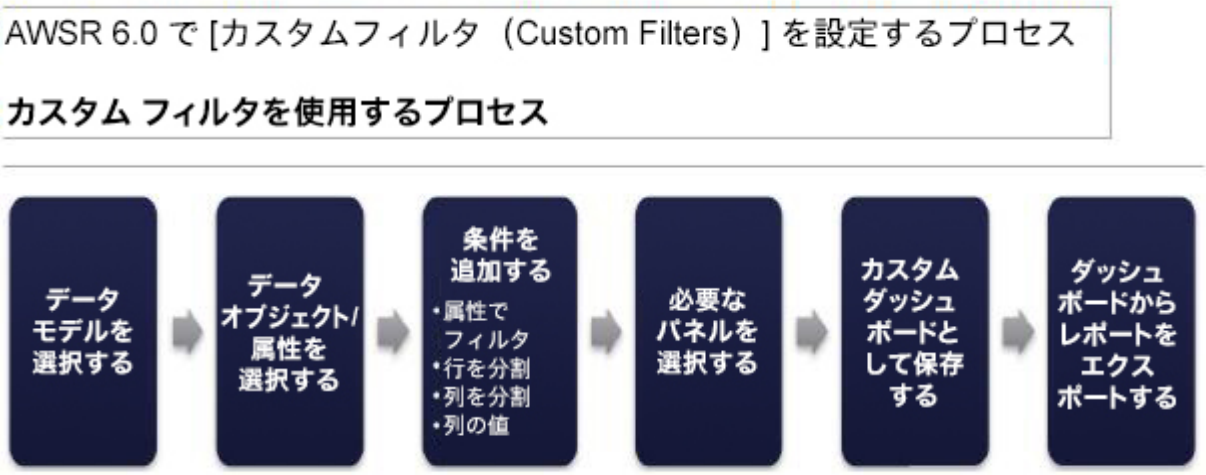
    m. [前回の同期（Last sync）] の時刻は、クライアント マシンの現地時間に一致しています。これで、正常に同期したことがわかります。

n. もう一度 CLI から **tail accesslogs** を実行すると、次のエントリが表示されます。

o. これは、外部フィードからの読み込みを実行したカスタム カテゴリを「許可」に設定したことに基づき、Sharepoint に対する要求が送信されるようになったことを示しています。

シナリオ 10：Advanced Web Security Reporting

はじめに



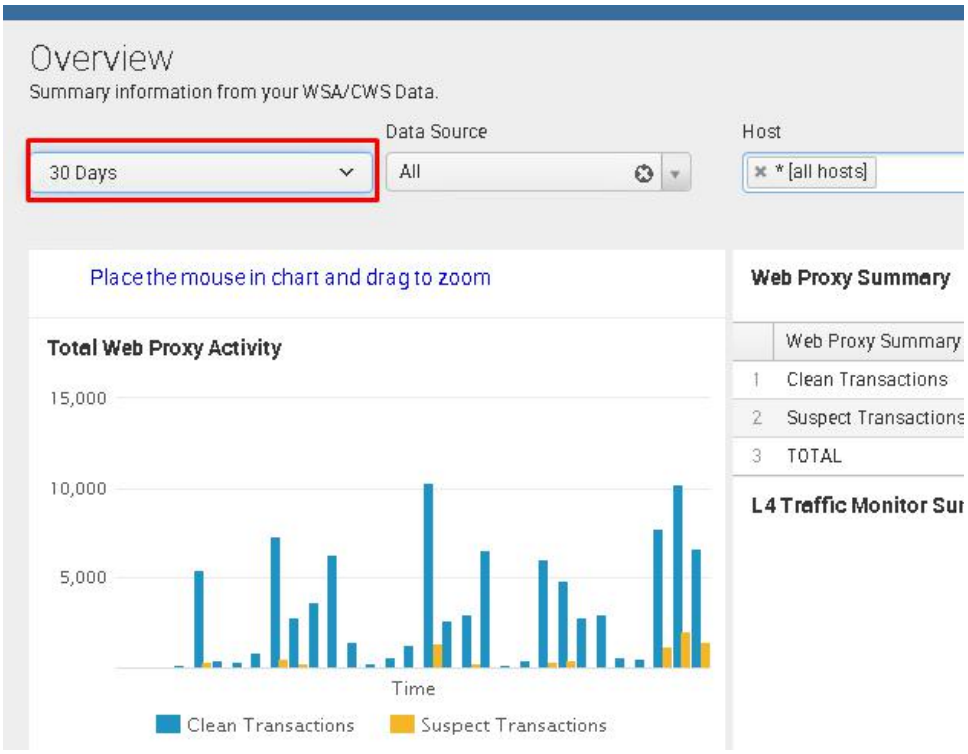
注：このラボでは、AWSR にログを送信するために WSA を設定する方法については取り上げません。その手順については、『AWSR User Guide（AWSR ユーザ ガイド）』を参照してください。
http://www.cisco.com/c/dam/en/us/td/docs/security/wsa/Advanced_Reporting/WSA_Advanced_Reporting_6/Advanced_Web_Security_Reporting_6.pdf 手順の説明はセクション 1-12 から始まります。

タスク A：AWSR での基本的なレポート

手順

1. Advanced Web Security Reporting アプリケーションにログインします。

2. 次のクレデンシャルでログインします。ユーザ名「**admin**」、パスワード「**C1sco12345**」。
3. ログインすると、AWSR の [概要（Overview）] ページが表示されます。デフォルトの期間として [30 日（30 Days）] を選択します。



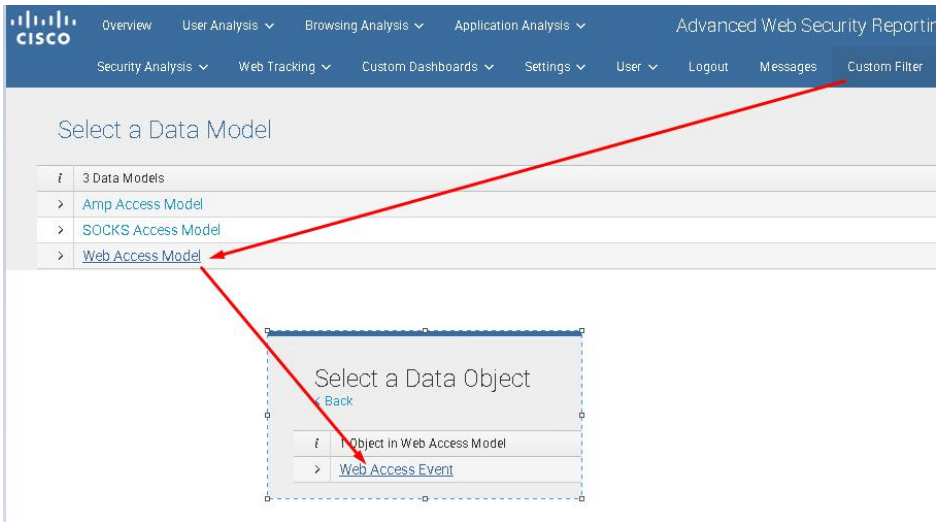
4. [ユーザ分析（User Analysis）]、[閲覧分析（Browsing Analysis）]、[アプリケーション分析（Application Analysis）]、[セキュリティ分析（Security Analysis）]、[Web トラッキング（Web Tracking）] などのさまざまなレポートを確認してみてください。

注：これらのレポートはすべて WSA の類似パターン/トラックに基づいています。

タスク B：カスタム フィルタ：一般的なレポート

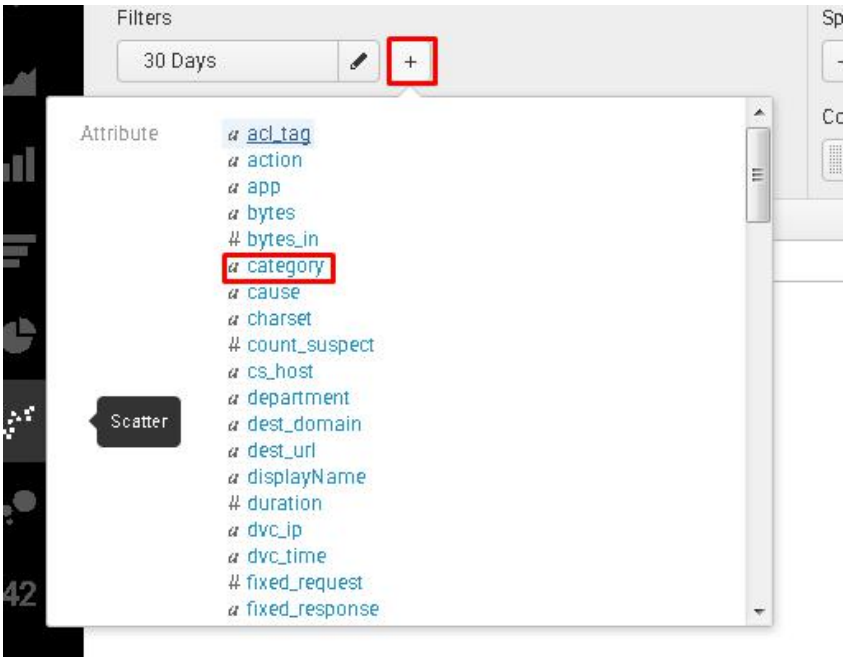
手順

1. [カスタムフィルタ（Custom Filter）] > [Web アクセスモデル（Web Access Model）] > [Web アクセスイベント（Web Access Event）] の順にクリックします。

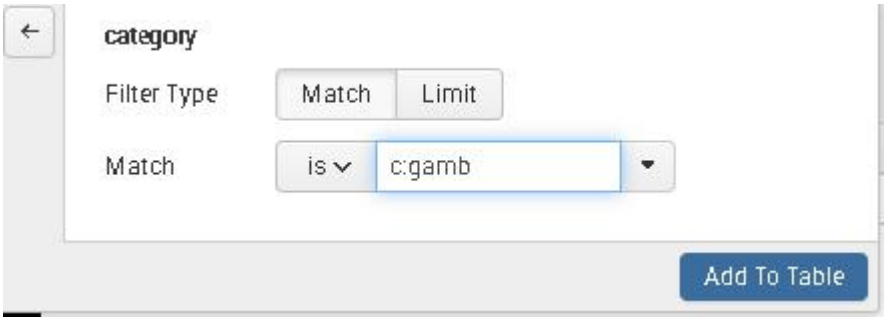


2. [新しいカスタムフィルタ（New Custom Filter）] ウィンドウで、[フィルタ（Filters）] を [常時（All time）] から [30 日（30 Days）] に変更します。

3. フィルタ追加のアイコン（プラス記号）をクリックし、[カテゴリ（category）] を選択します。



4. [フィルタタイプ（Filter Type）] を [一致（Match）] に設定し、[次に一致（Match is）] に対して、文字列 [c:gamb] が設定されていることを確認します。確認後、[テーブルに追加（Add To Table）] をクリックします。このフィルタにより、[ギャンブル（Gambling）] カテゴリの結果のみ表示されるようになります。



5. プラス記号のアイコンをクリックして [行を分割（Split Rows）] ボタンを追加します。

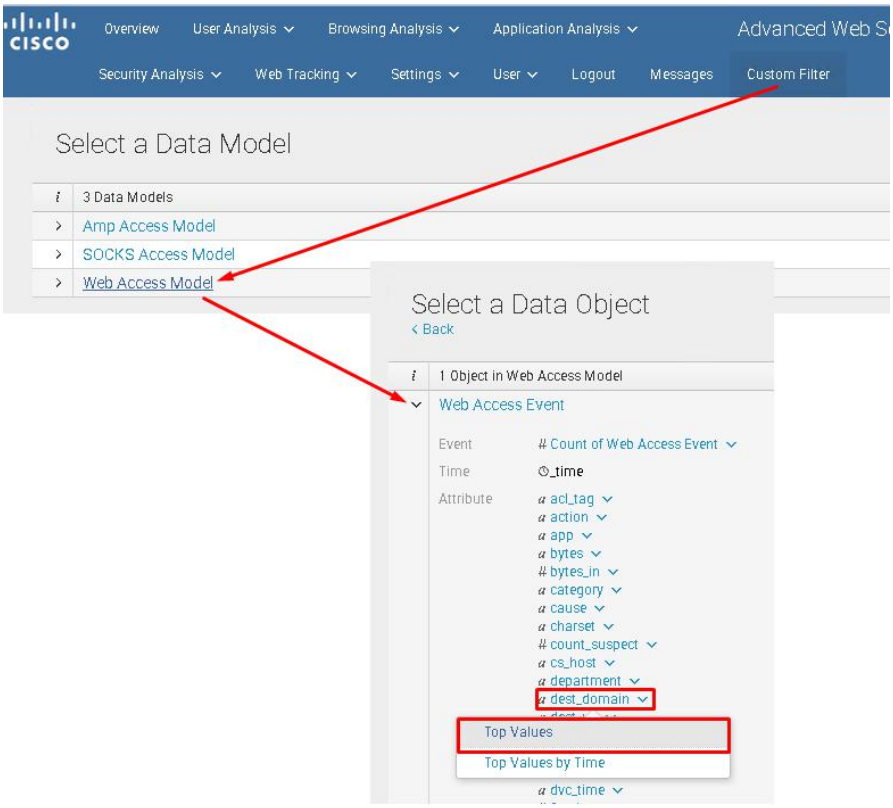
6. 次の属性を追加します。
    a. dest_domain
    b. dvc_ip
    c. user_id_fixed
    d. action
7. **dvc_ip、user_id_fixed、dest_domain、action** の順番になるように行を並べ替えます。

8. 結果を確認します。このレポートには、デバイスの IP、ユーザ名、宛先ドメイン、アクションが記載されています。

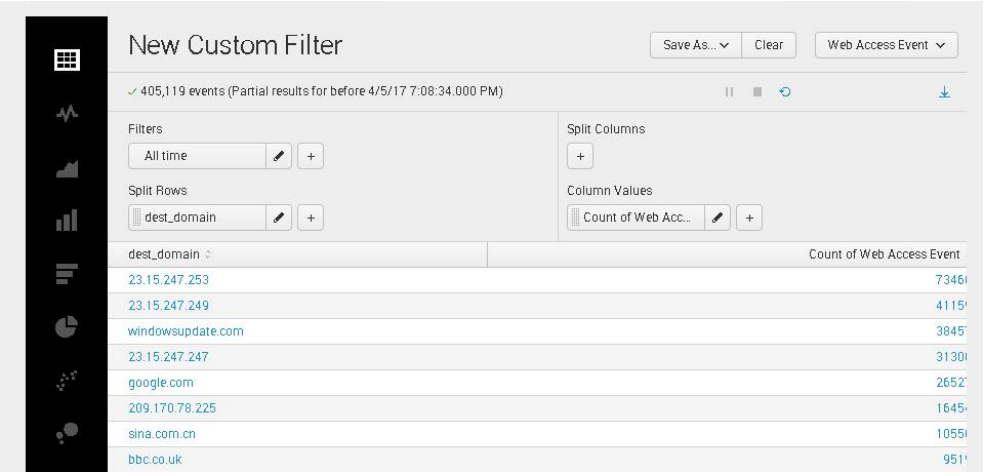
タスク C：カスタム フィルタ：閲覧時間の長い Web サイト

手順

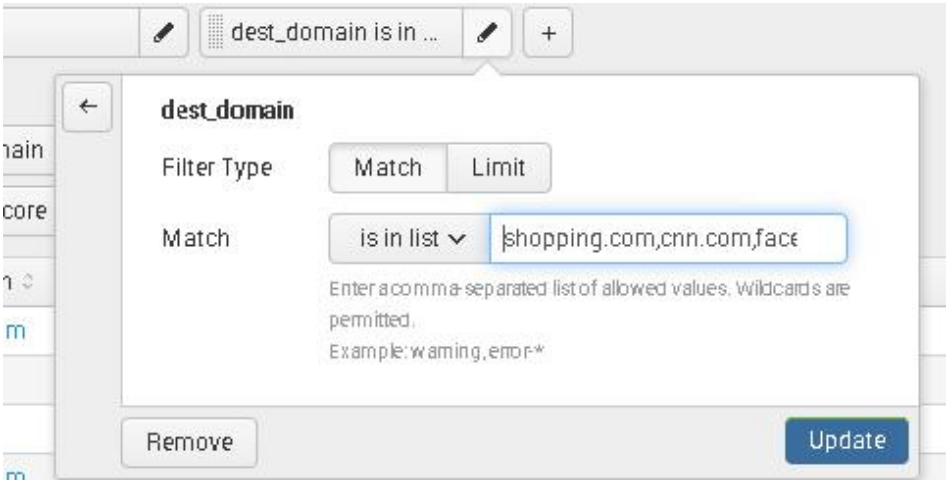
1. この演習では、閲覧時間の長い特定の Web サイト（カスタマイズされたサイト/ドメイン）に関するレポートを管理者が必要としている、という使用例を取り上げます。
2. [カスタムフィルタ（Custom Filter）] をクリックします。
3. [データモデルを選択（Select Data Model）] で [Web アクセスモデル（Web Access Model）] を選択します。
4. リスト ビューをクリックすると。すべてのフィールド/属性のリストが表示されます。
5. [上位の値（Top Values）] に基づいて [dest_domain] を選択します。すべての上位ドメインのリストが表示されます。



6. [新しいカスタムフィルタ（New Custom Filter）] ウィンドウが表示されます。

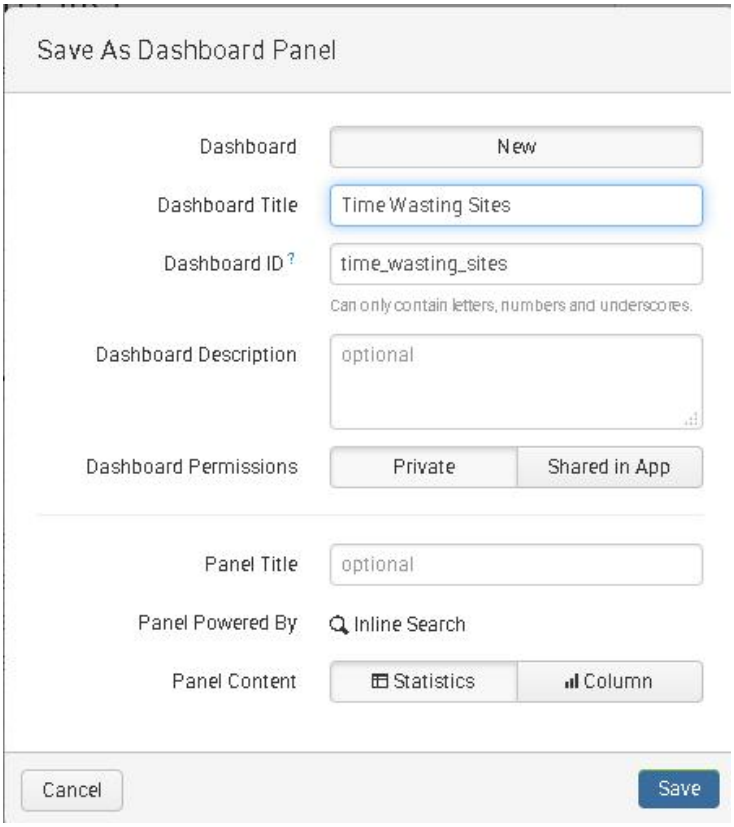


7. [フィルタ（Filters）] の設定を [常時（All Time）] から [30 日間（30 Days）] に変更します。
8. 表示される上位ドメインの数を増やすには、左下の [1 ページあたり 50（50 per Page）] を変更します。
9. 分割された行に、行をさらに追加します（+）。
    a. user_id_fixed
    b. dvc_ip
    c. dest_domain
    d. bytes
10. [フィルタ（Filters）]（+）で [dest_domain] を選択します。
11. [リストに一致（match is in list）] を選択し、**facebook.com**、**cnn.com**、**youtube.com**、**amazon.com**、**netflix.com** の各ドメインを追加します。最後に、[テーブルに追加（Add to Table）] をクリックします。

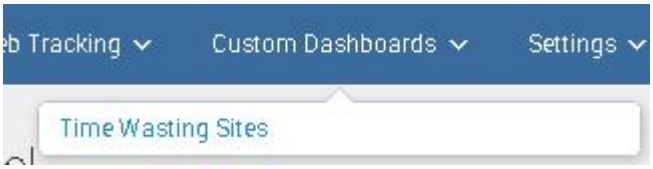


12. ここで [名前を付けて保存（Save As）] > [ダッシュボードパネル（Dashboard Panel）] の順にクリックします。

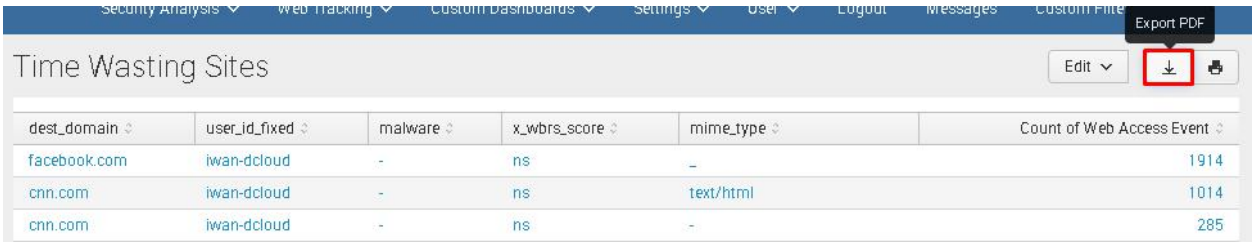
13. **Time Wasting Sites**（閲覧時間の長いサイト）など、わかりやすい名前を入力します。



14. 保存すると、[カスタムダッシュボード（Custom Dashboards）] タブが表示されます。



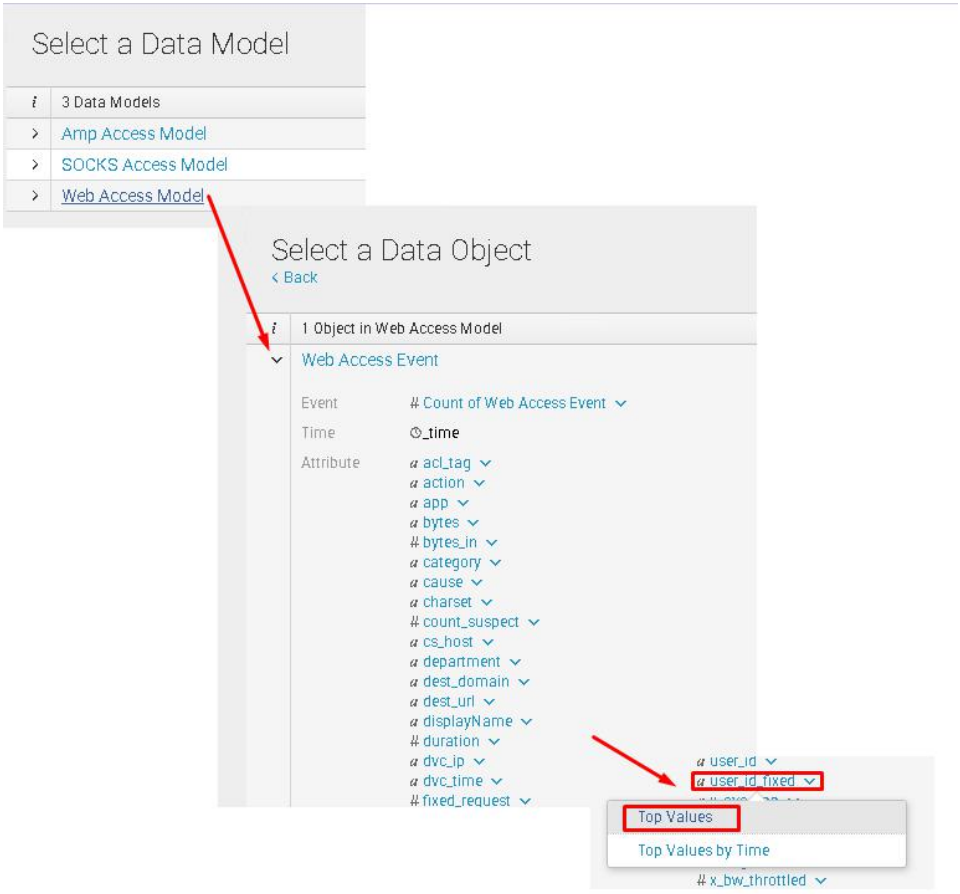
15. [閲覧時間の長いサイト（Time Wasting Sites）] をクリックします。[ダウンロード（Download）] ボタンが表示されます。このレポートを PDF にエクスポートします。



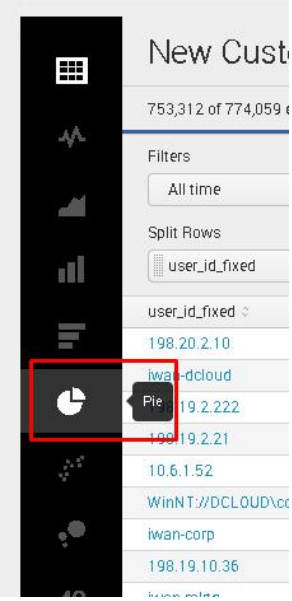
タスク D：カスタム フィルタ：円グラフ パネル

手順

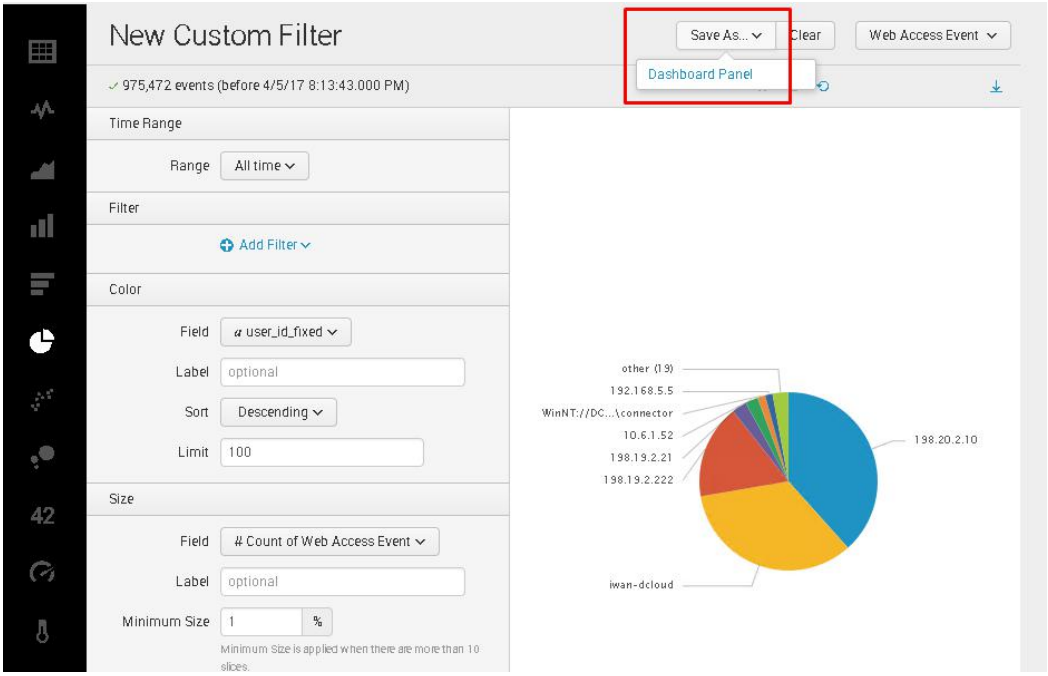
1. [カスタムフィルタ（Custom Filter）] をクリックします。
2. [データ モデルを選択（Select Data Model）] で [Web アクセスモデル（Web Access Model）] を選択します。
3. [上位の値（Top Value）] に基づいて [user_id_fixed] を選択します。すべての上位ユーザ/IP アドレスのリストが表示されます。



4. 左側のパネルから円グラフのアイコンを選択します。

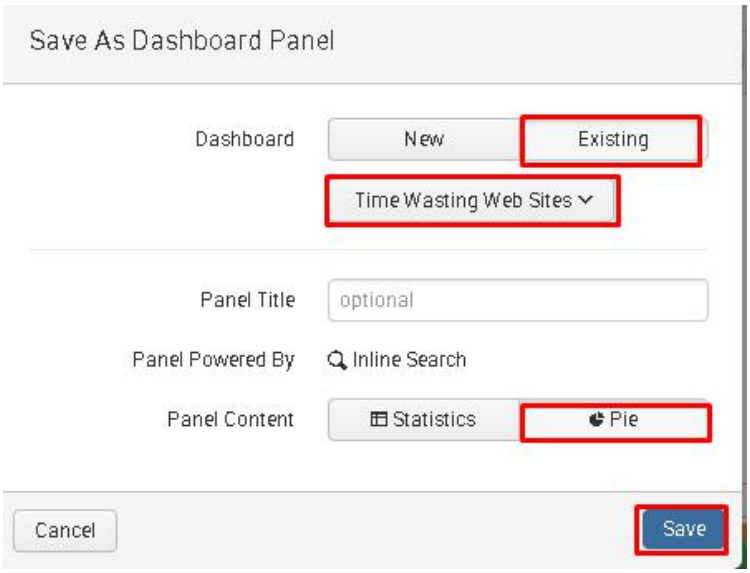


5. データが円グラフで表示されます。
6. 右上で、[名前を付けて保存..（Save As..）] > [ダッシュボードパネル（Dashboard Panel）] の順に選択します。

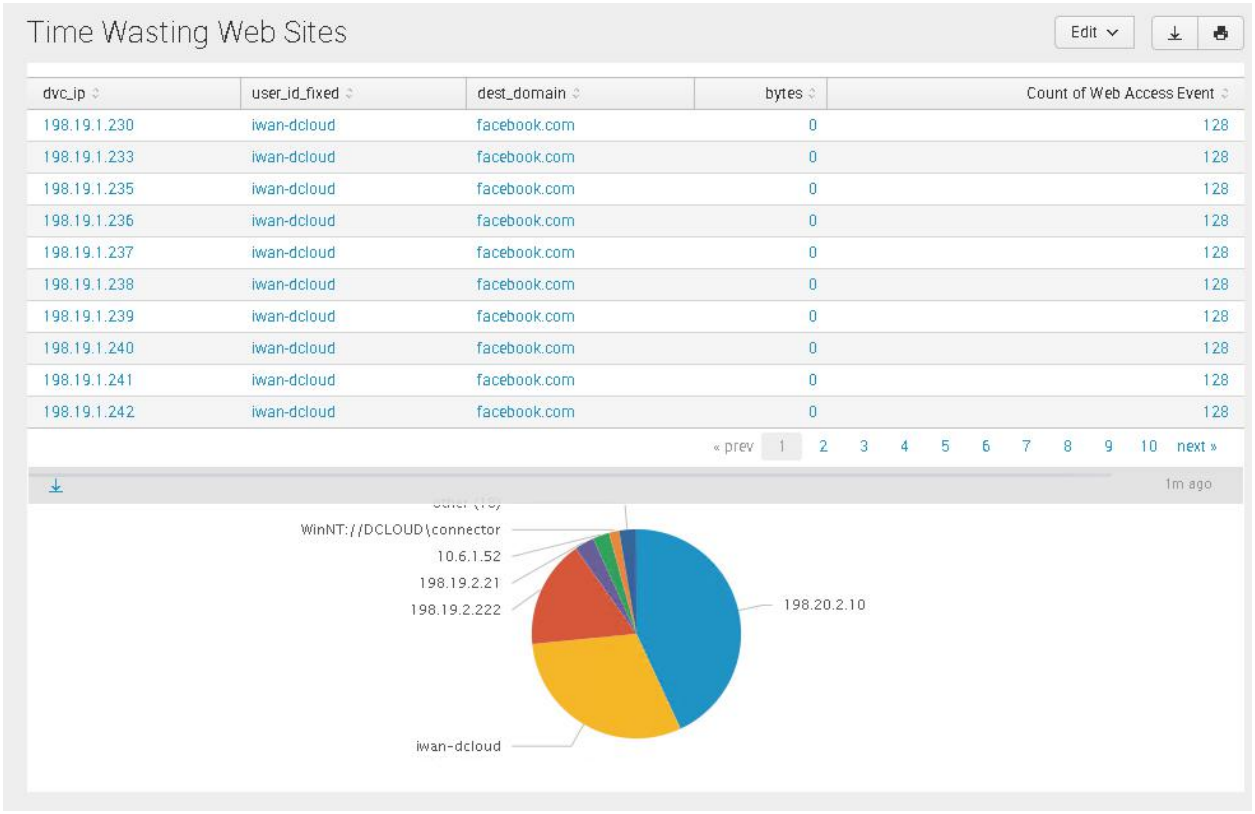


7. [既存（Existing）] を選択し、[Time Wasting Sites] を選択します。
8. [パネルコンテンツ（Panel Content）] が [円（Pie）] になっていることを確認します。

9. [保存（Save）] をクリックしてから [OK] をクリックします。



10. [カスタムダッシュボード（Custom Dashboards）] を再度クリックし、[Time Wasting Sites] を選択します。今度は円グラフのほかに表形式のレポートも表示されます。



シナリオ 11：一元管理型ソフトウェア アップグレード

はじめに

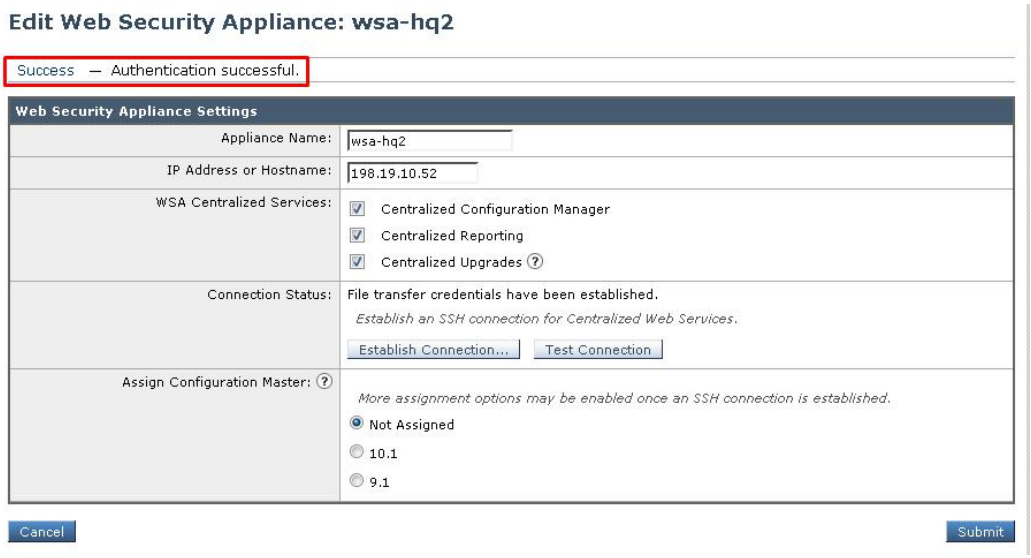
セキュリティ管理アプライアンス（SMA）を導入して WSA や ESA を管理している場合、アップグレード処理はデバイスごとに実施する必要がありました。バージョン 10.1 以降では、管理者が複数のデバイスにアップグレードを同時にプッシュできるようになりました。

タスク A：システム セットアップ

手順

1. 接続を確認します。
    a. ブックマークのリンクを使って SMA にログインするか、https://sma.dcloud.cisco.com にアクセスします。
    b. [管理アプライアンス（Management Appliance）] > [一元管理サービス（Centralized Services）] > [セキュリティアプライアンス（Security Appliances）] の順に移動します。
    c. [セキュリティアプライアンス（Security Appliances）] の下に [wsa-hq2] が表示されます。アプライアンスの名前をクリックします。

d. [接続の確立（Establish Connection）] ボタンをクリックします。ユーザ名「**admin**」、パスワード「**ironport**」を入力します。[接続の確立（Establish Connection）] をもう一度クリックします。成功メッセージが表示されます。



e. 次に、[接続のテスト（Test Connection）] をクリックします。再び成功メッセージが表示されます。

f. [送信（Submit）] をクリック後、[変更を確定（Commit Changes）] をクリックします。

g. [接続確立（Connection Established）] の下に [確立（Yes）] と表示されます。

2. SMA で一元管理型アップグレードを設定します。

   a. [管理アプライアンス（Management Appliance）] > [一元管理サービス（Centralized Services）] > [一元管理型アップグレードマネージャ（Centralized Upgrade Manager）] の順に移動します。

   b. [一元管理型アップグレード（Centralized upgrade）] が [有効（Enabled）] に設定されていることを確認します。設定されている場合はステップ 2c に進みます。設定されていない場合は、[設定の編集（Edit Settings）] をクリックし、[一元管理型アップグレードサービスを有効にする（Enable Centralized upgrade Service）] チェックボックスをオンにします。[送信（Submit）] をクリック後、[変更を確定（Commit Changes）] をクリックします。

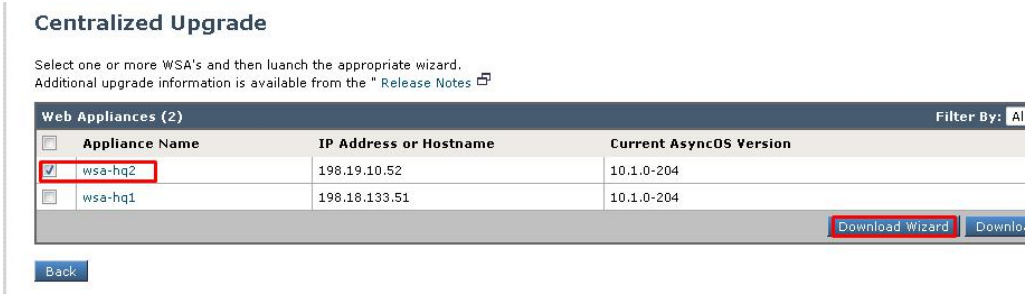
   c. 最後に、[一元管理サービス（Centralized Services）] > [セキュリティアプライアンス（Security Appliances）] で、[wsa-hq2] の [アップグレードマネージャ（Upgrade Manager）] が有効になっていることを確認します。

3. WSA のアップグレード プログラムをダウンロードします。

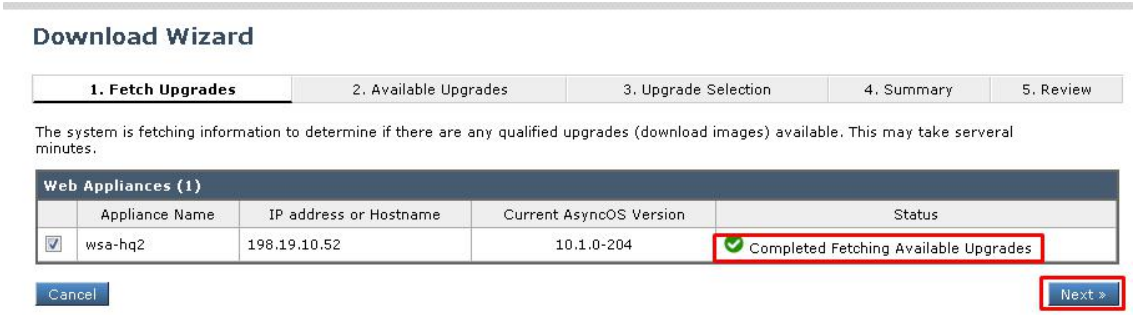
   a. [Web] > [ユーティリティ（Utilities）] > [一元管理型アップグレード（Centralized Upgrade）] の順に移動します。

b. [アプライアンスのアップグレード（Upgrade Appliances）] ボタンをクリックします。リストに [wsa-hq2] と [wsa-hq1] の両方が表示されています。

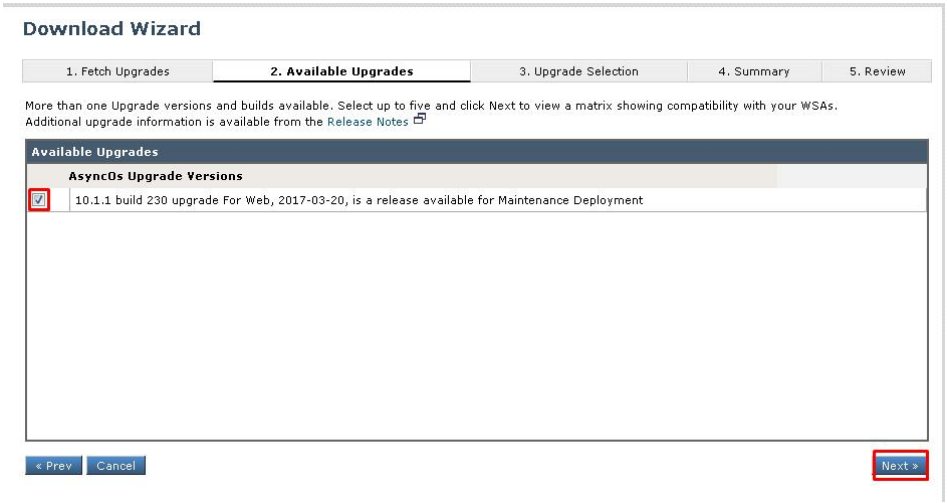
c. [wsa-hq2] を選択し、[ダウンロードウィザード（Download Wizard）] ボタンをクリックします。



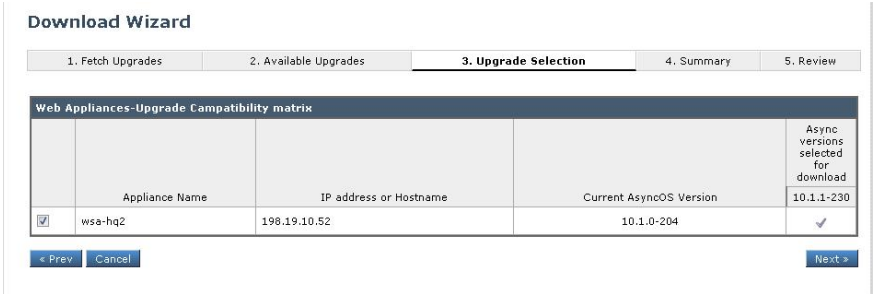
d. [アップグレードの取得（Fetch Upgrades）] 画面が表示されます。正常に完了したら、[次へ（Next）] をクリックします。



e. 利用可能な AsyncOS バージョンを選択し、[次へ（Next）] をクリックします。

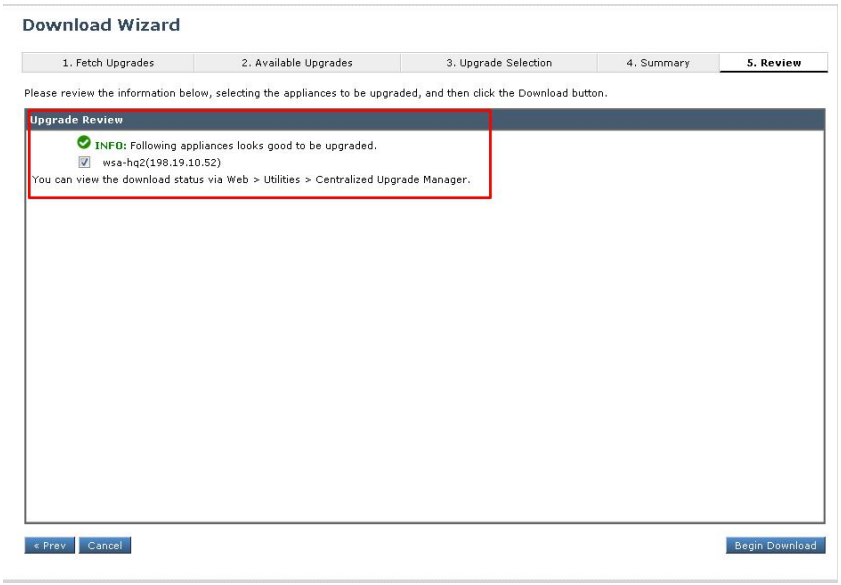


f. 正しい WSA が IP アドレスおよび現在の AsyncOS バージョンと合わせて表示されていることを確認します。確認後、[次へ（Next）] をクリックします。



g. [概要（Summary）] タブで情報を確認して [次へ（Next）] をクリックします。

h. [ダウンロード開始（Begin Download）] ボタンが表示されます。



i. WSA へのダウンロードが開始されます。ラボ インフラストラクチャの帯域幅を確保するため、[キャンセル（Cancel）] をクリック後、[キャンセルを確認（Confirm Cancel）] をクリックします。

注：通常の状況では、[一元管理型アップグレード（Centralized Upgrade）] によって複数の WSA のアップグレードが可能です。

お疲れさまでした。これで、このラボは終了です。

お問い合せ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp