Web 要求の代行受信

Web 要求の代行受信の概要

Web Security Appliance は、ネットワーク上のクライアントまたは他のデバイスから転送された要求を代行受信します。

アプライアンスは他のネットワーク デバイスと連携してトラフィックを代行受信します。そのようなデバイスとして、一般的なスイッチ、トランスペアレント リダイレクション デバイス、ネットワーク タップ、およびその他のプロキシ サーバまたは Web Security Appliance などがあげられます。

Web 要求の代行受信のためのタスク

手順	タスク	関連項目および手順へのリンク
1.	ベスト プラクティスを検討します。	• Web 要求の代行受信のベスト プラクティス（4-2 ページ）
2.	（任意）以下のネットワーク関連のフォローアップ タスクを実行します。 • アップストリーム プロキシを接続および設定する。 • ネットワーク インターフェイス ポリシーを設定する。 • 透過リダイレクション デバイスを設定する。 • TCP/IP ルートを設定する。 • VLAN の設定。	• アップストリーム プロキシ（2-19 ページ） • ネットワーク インターフェイス（2-21 ページ） • 透過リダイレクションの設定（2-28 ページ） • TCP/IP トラフィック ルートの設定（2-26 ページ） • VLAN の使用によるインターフェイス能力の向上（2-33 ページ）

手順	タスク	関連項目および手順へのリンク
3.	(任意)Web プロキシのフォローアップ タスクを実行します。 • 転送モードまたは透過モードで動作するように Web プロキシを設定する。 • 代行受信するプロトコル タイプに追加のサービスが必要かどうかを決定する。 • IP スプーフィングを設定する。 • Web プロキシ キャッシュを管理する。 • カスタム Web 要求ヘッダーを使用する。 • 一部の要求に対してプロキシをバイパスする。	• Web 要求を代行受信するための Web プロキシ オプション(4-2 ページ) • Web プロキシの設定(4-3 ページ) • Web 要求を代行受信するための Web プロキシ オプション(4-2 ページ) • Web プロキシ キャッシュ(4-5 ページ) • Web プロキシの IP スプーフィング(4-8 ページ) • Web プロキシのバイパス(4-10 ページ)
4.	以下のクライアント タスクを実行します。 • クライアントが Web プロキシに要求をリダイレクトする方法を決定する。 • クライアントとクライアント リソースを設定する。	• Web 要求をリダイレクトするためのクライアント オプション(4-11 ページ) • クライアント アプリケーションによる PAC ファイルの使用(4-12 ページ)
5.	(任意)FTP プロキシを有効化して設定します。	• FTP プロキシ サービス(4-15 ページ)

Web 要求の代行受信のベスト プラクティス

- 必要なプロキシ サービスのみをイネーブルにします。
- Web セキュリティ アプライアンスで定義されているすべての WCCP サービスに対して、同じ転送方式とリターン方式(L2 または GRE)を使用します。これによって、プロキシ バイパス リストが確実に機能します。
- ユーザが企業ネットワークの外部から PAC ファイルにアクセスできないことを確認します。これによって、モバイル ワーカーは、企業ネットワーク上にいるときは Web プロキシを使用し、それ以外の場合は Web サーバに直接接続できます。
- 信頼できるダウンストリーム プロキシまたはロード バランサからの X-Forwarded-For ヘッダーのみが Web プロキシで許可されるようにします。
- 当初は明示的な転送だけを使用していた場合でも、Web プロキシをデフォルトの透過モードのままにしておきます。透過モードでは、明示的な転送要求も許可されます。

Web 要求を代行受信するための Web プロキシ オプション

単独では、Web プロキシは HTTP(FTP over HTTP を含む)および HTTPS を使用する Web 要求を代行受信できます。追加のプロキシ モジュールを利用してプロトコル管理を向上させることができます。

- **FTP プロキシ。**FTP プロキシを使用すると、(HTTP でエンコードされた FTP トラフィックだけでなく)ネイティブ FTP トラフィックを代行受信できます。
- **HTTPS プロキシ。**HTTPS プロキシは HTTPS トラフィックの復号化をサポートしているので、Web プロキシは、暗号化されていない HTTPS 要求をコンテンツ分析のためにポリシーに渡すことができます。

(注)　透過モードでは、HTTPS プロキシがイネーブルでない場合、Web プロキシは透過的にリダイレクトされたすべての HTTPS 要求をドロップします。透過的にリダイレクトされた HTTPS 要求がドロップされた場合、その要求のログ エントリは作成されません。

- **SOCKS プロキシ。**SOCKS プロキシを使用すると、SOCKS トラフィックを代行受信できます。

これらの追加のプロキシのそれぞれが機能するには、Web プロキシが必要です。Web プロキシをディセーブルにすると、これらをイネーブルにできません。

(注)　Web プロキシはデフォルトでイネーブルになります。デフォルトでは、他のプロキシはすべてディセーブルになります。

関連項目

- FTP プロキシ サービス（4-15 ページ）。
- SOCKS プロキシ サービス（4-17 ページ）

Web プロキシの設定

はじめる前に

- Web プロキシをイネーブルにします。

手順 1　[セキュリティ サービス（Security Services）] > [Web プロキシ（Web Proxy）] を選択します。

手順 2　[設定の編集（Edit Settings）] をクリックします。

手順 3　必要に応じて基本的な Web プロキシ設定項目を設定します。

プロパティ	説明
プロキシを設定する HTTP ポート（HTTP Ports to Proxy）	Web プロキシが HTTP 接続をリッスンするポート
HTTP CONNECT ポート（HTTP CONNECT Ports）	ポート アプリケーションは、HTTP 経由で発信トラフィックをトンネリングする場合に使用が許可されます。
キャッシング（Caching）	Web プロキシによるキャッシュをイネーブルにするかディセーブルにするか指定します。 Web プロキシは、パフォーマンスを向上させるためにデータをキャッシュします。

プロパティ	説明
プロキシ モード（Proxy mode）	• [転送（Forward）]：クライアント ブラウザがインターネット ターゲットを指定できるようにします。Web プロキシを使用するように各 Web ブラウザを個々に設定する必要があります。このモードでは、Web プロキシは明示的に転送された Web 要求のみを代行受信できます。 • [透過（Transparent）]（推奨）：Web プロキシがインターネット ターゲットを指定できるようにします。このモードでは、Web プロキシは、透過的または明示的に転送された Web 要求を代行受信できます。
IP スプーフィング（IP Spoofing）	• [IP スプーフィングの無効化（IP Spoofing disabled）]：Web プロキシは、セキュリティを向上させるために、Web プロキシのアドレスと一致するように要求の送信元 IP アドレスを変更します。 • [IP スプーフィングの有効化（IP Spoofing enabled）]：Web プロキシは送信元アドレスを維持するため、Web Security Appliance ではなく送信元クライアントから発信されたように見えます。

手順 4　必要に応じて Web プロキシの詳細設定を設定します。

プロパティ	説明
永続的接続のタイムアウト（Persistent Connection Timeout）	トランザクションが完了し、その他のアクティビティが検出されなかった後に、Web プロキシがクライアントまたはサーバとの接続を開いたままにしておく最大時間（秒単位）。 • [クライアント側（Client side）]。クライアントとの接続のタイムアウト値。 • [サーバ側（Server side）]。サーバとの接続のタイムアウト値。 これらの値を大きくすると、接続が開いたままになっている時間が延長され、接続の開閉に費やされるオーバーヘッドが低減します。ただし、永続的な同時接続の数が最大数に達した場合に Web Proxy が新しい接続を開く機能も低下します。 シスコは、デフォルト値を維持することを推奨します。
使用中接続タイムアウト（In-Use Connection Timeout）	現在のトランザクションが完了していないときに、Web プロキシがアイドル状態のクライアントまたはサーバからのデータをさらに待機する最大時間（秒単位）。 • [クライアント側（Client side）]。クライアントとの接続のタイムアウト値。 • [サーバ側（Server side）]。サーバとの接続のタイムアウト値。
同時永続的接続（サーバ最大数）（Simultaneous Persistent Connections (Server Maximum Number)）	Web プロキシ サーバがサーバに対して開いたままにする接続（ソケット）の最大数。

ヘッダーの生成（Generate Headers）	要求に関する情報をエンコードするヘッダーを生成して追加します。 • **X-Forwarded-For** ヘッダーは、HTTP 要求を発信したクライアントの IP アドレスをエンコードします。 （注）　ヘッダーの転送をオン/オフするには、`advancedproxyconfig` CLI コマンドの Miscellaneous オプション「HTTP X-Forwarded-For ヘッダーを通過させますか?（Do you want to pass HTTP X-Forwarded-For headers?）」を使用します。 （注）　明示的な転送アップストリーム プロキシを使用して、プロキシ認証によりユーザ認証やアクセス制御を管理するには、これらのヘッダーを転送する必要があります。 • **Request Side VIA** ヘッダーは、クライアントからサーバへの要求が通過するプロキシをエンコードします。 • **Response Side VIA** ヘッダーは、サーバからクライアントへの要求が通過するプロキシをエンコードします。
Received ヘッダーの使用（Use Received Headers）	アップストリーム プロキシとして展開された Web プロキシが、ダウンストリームプロキシから送信された X-Forwarded-For ヘッダーを使用してクライアントを識別できるようにします。Web プロキシは、リストに含まれていない送信元からの X-Forwarded-For ヘッダーの IP アドレスを受け入れません。 これをイネーブルにする場合は、ダウンストリーム プロキシまたはロードバランサの IP アドレスが必要です（サブネットやホスト名は入力できません）。
範囲要求の転送（Range Request Forwarding）	範囲要求の転送をイネーブルまたはディセーブルにするには、[範囲要求の転送の有効化（Enable Range Request Forwarding）] チェックボックスを使用します。詳細については、範囲要求の設定（15-4 ページ）を参照してください。

手順 5　変更を送信し、保存します。

関連項目

- Web プロキシ キャッシュ（4-5 ページ）。
- 透過リダイレクションの設定（2-28 ページ）

Web プロキシ キャッシュ

Web プロキシは、パフォーマンスを向上させるためにデータをキャッシュします。AsyncOS には「セーフ」から「アグレッシブ」の範囲の定義済みキャッシュ モードがあり、またカスタマイズしたキャッシングも使用できます。キャッシュ対象から特定の URL を除外することもできます。これを行うには、その URL をキャッシュから削除するか、無視するようにキャッシュを設定します。

Web プロキシ キャッシュのクリア

手順 1　[セキュリティ サービス（Security Services）] > [Web プロキシ（Web Proxy）] を選択します。

手順 2　[キャッシュを消去（Clear Cache）] をクリックしてアクションを確定します。

Web プロキシ キャッシュからの URL の削除

手順 1　CLI にアクセスします。

手順 2　webcache > evict コマンドを使用して、必要なキャッシング エリアにアクセスします。

```
example.com> webcache

Choose the operation you want to perform:
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> evict

Enter the URL to be removed from the cache.
[]>
```

手順 3　キャッシュから削除する URL を入力します。

（注）　URL にプロトコルが含まれていない場合は、URL に http:// が追加されます（たとえば、www.cisco.com は http://www.cisco.com となります）。

Web プロキシによってキャッシュしないドメインまたは URL の指定

手順 1　CLI にアクセスします。

手順 2　webcache -> ignore コマンドを使用して、必要なサブメニューにアクセスします。

```
example.com> webcache

Choose the operation you want to perform:
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> ignore

Choose the operation you want to perform:
- DOMAINS - Manage domains
- URLS - Manage urls
[]>
```

手順 3　管理するアドレス タイプを入力します（DOMAINS または URLS）。

```
[]> urls

Manage url entries:
```

```
Choose the operation you want to perform:
- DELETE - Delete entries
- ADD - Add new entries
- LIST - List entries
[]>
```

手順 4　**add** と入力して新しいエントリを追加します。

```
[]> add

Enter new url values; one on each line; an empty line to finish
[]>
```

手順 5　以下の例のように、1 行に 1 つずつ、ドメインまたは URL を入力します。

```
Enter new url values; one on each line; an empty line to finish
[]> www.example1.com

Enter new url values; one on each line; an empty line to finish
[]>
```

ドメインまたは URL を指定する際に、特定の正規表現（regex）文字を含めることができます。DOMAINS オプションでは、前にピリオドを付けることで、キャッシュ対象からドメインとそのサブドメイン全体を除外できます。たとえば、google.com ではなく、.google.com と入力すると、www.google.com、docs.google.com などを除外することができます。

URLS オプションでは、正規表現文字の全一式を使用できます。正規表現の使用方法については、正規表現（9-27 ページ）を参照してください。

手順 6　値の入力を終了するには、メイン コマンドライン インターフェイスに戻るまで Enter キーを押します。

手順 7　変更を保存します。

Web プロキシのキャッシュ モードの選択

手順 1　CLI にアクセスします。

手順 2　advancedproxyconfig -> caching コマンドを使用して、必要なサブメニューにアクセスします。

```
example.com> advancedproxyconfig

Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
[]> caching
```

```
Enter values for the caching options:

The following predefined choices exist for configuring advanced caching
options:
1. Safe Mode
2. Optimized Mode
3. Aggressive Mode
4. Customized Mode
Please select from one of the above choices:
[2]>
```

手順 3　必要な Web プロキシ キャッシュ設定に対応する番号を入力します。

入力	[モード(Mode)]	説明
1	セーフ	他のモードと比較して、キャッシングが最も少なく、RFC #2616 には最大限準拠します。
2	最適化	キャッシングと RFC #2616 への準拠が適度です。セーフ モードと比較した場合、Last-Modified ヘッダーが存在するときにキャッシング時間が指定されていない場合に、最適化モードでは Web プロキシがオブジェクトをキャッシュします。Web プロキシは、ネガティブ応答をキャッシュします。
3	アグレッシブ	キャッシングが最も多く、RFC #2616 には最小限準拠します。最適化モードと比較した場合、アグレッシブ モードでは、Web プロキシは認証済みコンテンツ、ETag の不一致、および Last-Modified ヘッダーのないコンテンツをキャッシュします。Web プロキシは非キャッシュ パラメータを無視します。
4	カスタマイズド モード	各パラメータを個々に設定します。

手順 4　オプション 4(カスタマイズ モード)を選択した場合は、各カスタム設定の値を入力します(または、デフォルト値のままにします)。

手順 5　メイン コマンド インターフェイスに戻るまで、**Enter** キーを押します。

手順 6　変更を保存します。

関連項目

- Web プロキシ キャッシュ (4-5 ページ)

Web プロキシの IP スプーフィング

デフォルトでは、Web プロキシは要求を転する際に、自身のアドレスに合わせて要求の送信元 IP アドレスを変更します。これによってセキュリティは向上しますが、この動作は IP スプーフィングを実装することによって変更できます。IP スプーフィングを使用すると、要求は送信元アドレスを維持するので、Web Security Appliance からではなく、送信元クライアントから発信されたように見えます。

IP スプーフィングは、透過的または明示的に転送されたトラフィックに対して機能します。Web プロキシが透過モードで展開されている場合、IP スプーフィングを、透過的にリダイレクトされた接続に対してのみイネーブルにするか、すべての接続（透過的にリダイレクトされた接続と明示的に転送された接続）に対してイネーブルにするかを選択できます。明示的に転送された接続で IP スプーフィングを使用する場合は、リターンパケットを Web セキュリティ アプライアンスにルーティングする適切なネットワーク デバイスがあることを確認してください。

IP スプーフィングがイネーブルで、アプライアンスが WCCP ルータに接続されている場合は、2 つの WCCP サービス（送信元ポートに基づくサービスと宛先ポートに基づくサービス）を設定する必要があります。

関連項目

- Web プロキシの設定（4-3 ページ）
- WCCP サービスの設定（2-30 ページ）

Web プロキシのカスタム ヘッダー

特定の発信トランザクションにカスタム ヘッダーを追加して、宛先サーバによる特別な処理を要求できます。たとえば、YouTube for Schools と関係がある場合、カスタム ヘッダーを使用して、YouTube.com へのトランザクション要求を自身のネットワークから発信された、特別な処理を必要とする要求として識別させることができます。

Web 要求へのカスタム ヘッダーの追加

手順 1　CLI にアクセスします。

手順 2　`advancedproxyconfig -> customheaders` コマンドを使用して、必要なサブメニューにアクセスします。

```
example.com> advancedproxyconfig

Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
[]> customheaders

Currently defined custom headers:

Choose the operation you want to perform:
- DELETE - Delete entries
- NEW - Add new entries
- EDIT - Edit entries
[]>
```

手順 3　必要なサブコマンドを入力します。

オプション	説明
削除（Delete）	指定するカスタム ヘッダーを削除します。コマンドで返されたリストのヘッダーに関連付けられている番号を使用して削除するヘッダーを指定します。
新規作成（New）	指定するドメインの使用に提供するヘッダーを作成します。 ヘッダーの例： X-YouTube-Edu-Filter: ABCD1234567890abcdef （この場合の値は、YouTube で提供される固有キーです）。 ドメインの例： youtube.com
編集（Edit）	既存のヘッダーを指定したヘッダーと置き換えます。コマンドで返されたリストのヘッダーに関連付けられている番号を使用して削除するヘッダーを指定します。

手順 4　メイン コマンド インターフェイスに戻るまで、**Enter** キーを押します。

手順 5　変更を保存します。

Web プロキシのバイパス

Web プロキシのバイパス（Web 要求の場合）

特定のクライアントからの透過的要求や特定の宛先への透過的要求が Web プロキシをバイパスするように、Web Security Appliance を設定できます。

Web プロキシをバイパスすることによって、以下のことが可能になります。

- プロキシ サーバへの接続に HTTP ポートを使用しているが、適切に機能しない HTTP 非対応（または独自の）プロトコルが干渉されないようにします。
- ネットワーク内の特定のマシンからのトラフィックが、マルウェアのテスト マシンなど、ネットワーク プロキシおよび組み込みのセキュリティ保護をすべてバイパスすることを確認します。

バイパスは、Web プロキシに透過的にリダイレクトされる要求に対してのみ機能します。Web プロキシは、透過モードでも転送モードでも、クライアントから明示的に転送されたすべての要求を処理します。

Web プロキシのバイパス設定（Web 要求の場合）

手順 1　[Web セキュリティ マネージャ（Web Security Manager）] > [バイパス設定（Bypass Settings）] を選択します。

手順 2　[バイパス設定の編集（Edit Bypass Settings）] をクリックします。

手順 3　Web プロキシをバイパスするアドレスを入力します。

手順 4　変更を送信し、保存します。

Web プロキシのバイパス設定（アプリケーションの場合）

手順 1　[Web セキュリティマネージャ（Web Security Manager）] > [バイパス設定（Bypass Settings）] を選択します。

手順 2　[アプリケーションのスキップ設定を編集（Edit Application Bypass Settings）] をクリックします。

手順 3　スキャンをバイパスするアプリケーションを選択します。

手順 4　変更を送信し、保存します。

Web プロキシ使用規約

Web Security Appliance を設定して、Web アクティビティのフィルタリングとモニタリングが行われていることをユーザに通知できます。アプライアンスは、ユーザが初めてブラウザにアクセスしたときに、一定時間の経過後、エンド ユーザ確認ページを表示します。エンド ユーザ確認ページが表示されたら、ユーザはリンクをクリックして、要求した元のサイトまたは他の Web サイトにアクセスする必要があります。

関連項目

- エンドユーザへのプロキシ アクションの通知

Web 要求をリダイレクトするためのクライアント オプション

クライアントから Web プロキシに明示的に要求を転送することを選択した場合は、それを実行するためのクライアントの設定方法も指定する必要があります。以下の方法から選択します。

- **明示的な設定を使用してクライアントを設定する。**Web プロキシのホスト名とポート番号を使ってクライアントを設定します。設定方法の詳細については、個々のクライアントのマニュアルを参照してください。

（注）　デフォルトでは、Web プロキシ ポートはポート番号 80 と 3128 を使用します。クライアントはいずれかのポートを使用できます。

- **プロキシ自動設定（PAC）ファイルを使用してクライアントを設定する。**PAC ファイルは、Web 要求の送信先をクライアントに指示します。このオプションを使用すると、プロキシの詳細に対する以降の変更を一元管理できます。

PAC ファイルを使用する場合は、PAC ファイルの保存場所とクライアントがそれらを検出する方法を選択する必要があります。

関連項目

- クライアント アプリケーションによる PAC ファイルの使用（4-12 ページ）

クライアント アプリケーションによる PAC ファイルの使用

プロキシ自動設定（PAC）ファイルのパブリッシュ オプション

クライアントがアクセスできる場所に PAC ファイルをパブリッシュする必要があります。有効な場所は以下のとおりです。

- **Web サーバ。**
- **Web Security Appliance セキュリティ アプライアンス。**PAC ファイルを Web Security Appliance に配置できます。これはクライアントでは Web ブラウザとして表示されます。アプライアンスには、さまざまなホスト名、ポート、ファイル名を使用している要求に対応する機能など、PAC ファイルを管理するための追加オプションもあります。
- **ローカル マシン。**クライアントのハード ディスクに PAC ファイルをローカルに配置できます。ただし、この方法は一般的なソリューションとしてお勧めしません（自動 PAC ファイルの検出には適していませんが、テストする場合には有用です）。

関連項目

- Web セキュリティ アプライアンスでの PAC ファイルのホスティング（4-13 ページ）
- クライアント アプリケーションでの PAC ファイルの指定（4-14 ページ）

プロキシ自動設定（PAC）ファイルを検索するクライアント オプション

クライアントに対して PAC ファイルを使用する場合は、クライアントが PAC ファイルを検索する方法を選択する必要があります。以下の 2 つの対処法があります。

- **PAC ファイルの場所をクライアントに設定する。**この PAC ファイルを明確に差し指す URL をクライアントに設定します。
- **PAC ファイルの場所を自動的に検出するようにクライアントを設定する。**DHCP または DNS とともに WPAD プロトコルを使用して PAC ファイルを自動的に検索するようにクライアントを設定します。

PAC ファイルの自動検出

WPAD は、DHCP および DNS ルックアップを使用してブラウザが PAC ファイルの場所を判別できるようにするプロトコルです。

- **DHCP と共に WPAD を使用するには**、DHCP サーバに PAC ファイルの場所の URL と共にオプション 252 を設定します。ただし、すべてのブラウザが DHCP をサポートしているわけではありません。
- **DNS と共に WPAD を使用するには**、PAC ファイルのホスト サーバを指し示すように DNS レコードを設定します。

いずれかまたは両方のオプションを設定できます。WPAD は最初に DHCP を使用して PAC ファイルの検出を試み、検出できなかった場合は DNS を使って試みます。

関連項目

- クライアントでの PAC ファイルの自動検出（4-15 ページ）

Web セキュリティ アプライアンスでの PAC ファイルのホスティング

手順 1　[セキュリティ サービス（Security Services）] > [PAC ファイル ホスティング（PAC File Hosting）] を選択します。

手順 2　[設定の有効化と編集（Enable and Edit Settings）] をクリックします。

手順 3　（任意）以下の基本設定項目を設定します。

オプション	説明
PAC サーバ ポート（PAC Server Ports）	Web Security Appliance が PAC ファイル要求のリッスンに使用するポート。
PAC ファイルの有効期限（PAC File Expiration）	ブラウザ キャッシュで指定されている分数が経過した後に PAC ファイルを期限切れにできます。

手順 4　[PAC ファイル（PAC Files）] セクションで [参照（Browse）] をクリックし、Web Security Appliance にアップロードする PAC ファイルをローカル マシンから選択します。

（注）　選択したファイルの名前が `default.pac` である場合は、ブラウザで場所を設定するときにファイル名を指定する必要がありません。名前が指定されていない場合、Web Security Appliance は `default.pac` というファイルを検索します。

手順 5　[アップロード（Upload）] をクリックして、ステップ 4 で選択した PAC ファイルを Web Security Appliance にアップロードします。

手順 6　（任意）[PAC ファイル サービスを直接提供するホスト名（Hostnames for Serving PAC Files Directly）] セクションで、ポート番号を含まない PAC ファイル要求のホスト名と関連ファイル名を設定します。

オプション	説明
ホストネーム	Web Security Appliance が要求を処理する場合に、PAC ファイル要求に含める必要があるホスト名。要求にはポート番号が含まれていないため、要求は Web プロキシの HTTP ポート（ポート80）を使用して処理され、ホスト名評価から PAC ファイル要求として識別できます。
プロキシ ポートを通じた「GET」要求に対するデフォルト PAC ファイル（Default PAC File for "Get/" Request through Proxy Port）	同じ行のホスト名に関連付けられる PAC ファイル名。ホスト名に対する要求は、ここで指定した PAC ファイルを返します。 アップロード済みの PAC ファイルのみを選択できます。
行を追加（Add Row）	別の行を追加して、追加のホスト名と PAC ファイル名を指定します。

手順 7　変更を送信し、保存します。

クライアント アプリケーションでの PAC ファイルの指定

- クライアントでの PAC ファイルの場所の手動設定（4-14 ページ）
- クライアントでの PAC ファイルの自動検出（4-15 ページ）

クライアントでの PAC ファイルの場所の手動設定

手順 1　PAC ファイルを作成してパブリッシュします。

手順 2　ブラウザの PAC ファイル設定領域に PAC ファイルの場所を示す URL を入力します。

Web Security Appliance が PAC ファイルをホストしている場合、有効な URL 形式は以下のようになります。

```
http://server_address[.domain][:port][/filename] | http://WSAHostname[/filename]
```

WSAHostname は、Web Security Appliance に PAC ファイルをホストするときに設定した [ホスト名（hostname）] の値です。ホストしていない場合、URL の形式は格納場所と（場合によっては）クライアントに応じて異なります。

関連項目

- Web セキュリティ アプライアンスでの PAC ファイルのホスティング（4-13 ページ）

クライアントでの PAC ファイルの自動検出

手順 1　wpad.dat という名前の PAC ファイルを作成し、Web サーバまたは Web Security Appliance にパブリッシュします（DNS と共に WPAD を使用する場合は、Web サーバのルート フォルダにファイルを配置する必要があります）。

手順 2　以下の MIME タイプで .dat ファイルを設定するように Web サーバを設定します。

```
application/x-ns-proxy-autoconfig
```

（注）　Web Security Appliance はこれを自動的に実行します。

手順 3　DNS ルックアップをサポートするには、「wpad」から始まる、内部的に解決可能な DNS 名を作成して（例：wpad.example.com）、wpad.dat ファイルをホストしているサーバの IP アドレスに関連付けます。

手順 4　DHCP ルックアップをサポートするには、DHCP サーバのオプション 252 に wpad.dat ファイルの場所の URL を設定します（例：「http://wpad.example.com/wpad.dat」）。URL には、IP アドレスなど、有効な任意のホスト アドレスを使用できます。特定の DNS エントリは必要ありません。

関連項目

- クライアント アプリケーションによる PAC ファイルの使用（4-12 ページ）
- Web セキュリティ アプライアンスでの PAC ファイルのホスティング（4-13 ページ）
- Firefox で WPAD を使用できない（A-4 ページ）

FTP プロキシ サービス

- FTP プロキシ サービスの概要（4-15 ページ）
- FTP プロキシの有効化と設定（4-16 ページ）

FTP プロキシ サービスの概要

Web プロキシは、以下の 2 種類の FTP 要求を代行受信できます。

- **ネイティブ FTP。**ネイティブ FTP 要求は、専用 FTP クライアントによって生成されます（または、ブラウザで組み込みの FTP クライアントを使用して生成されます）。FTP プロキシが必要です。
- **FTP over HTTP。**ブラウザは、ネイティブ FTP を使用する代わりに、HTTP 要求内に FTP 要求をエンコードすることがあります。FTP プロキシは必要ありません。

関連項目

- FTP プロキシの有効化と設定（4-16 ページ）。
- FTP 通知メッセージの設定（17-10 ページ）

FTP プロキシの有効化と設定

（注）　FTP over HTTP 接続に適用されるプロキシ設定を設定するには、Web プロキシの設定（4-3 ページ）を参照してください。

手順 1　[セキュリティ サービス（Security Services）] > [FTP プロキシ（FTP Proxy）] を選択します。

手順 2　[設定の有効化と編集（Enable and Edit Settings）] をクリックします（表示されるオプションが [設定の編集（Edit Settings）] だけの場合、FTP プロキシは設定済みです。）

手順 3　（任意）基本的な FTP プロキシ設定項目を設定します。

プロパティ	説明
プロキシ リスニング ポート（Proxy Listening Port）	FTP プロキシが FTP 制御接続をリッスンするポート。クライアントは、（FTP サーバに接続するためのポート（通常はポート 21 を使用）としてではなく）FTP プロキシを設定するときにこのポートを使用する必要があります。
キャッシング（Caching）	匿名ユーザからのデータ接続をキャッシュするかどうか。 （注）　匿名ではないユーザからのデータはキャッシュされません。
サーバ側の IP スプーフィング（Server Side IP Spoofing）	FTP プロキシが FTP サーバの IP アドレスをシミュレートできるようにします。これによって、IP アドレスが制御接続とデータ接続で異なる場合に、トランザクションを許可しない FTP クライアントに対応できます。
認証形式（Authentication Format）	FTP クライアントと通信するときに FTP プロキシが使用する認証形式を選択できるようにします。
パッシブ モード データ ポート範囲（Passive Mode Data Port Range）	パッシブ モード接続で FTP プロキシとのデータ接続を確立するために FTP クライアントが使用する TCP ポートの範囲。
アクティブ モード データ ポート範囲（Active Mode Data Port Range）	アクティブ モード接続で FTP プロキシとのデータ接続を確立するために FTP サーバが使用する TCP ポートの範囲。この設定は、ネイティブ FTP および FTP over HTTP 接続の両方に適用されます。 ポート範囲を大きくすると、同じ FTP サーバからのさらに多くの要求に対応できます。TCP セッションの TIME-WAIT 遅延（通常数分）によって、ポートは使用された直後に、*同じ* FTP サーバで再び使用できるようになりません。その結果、所定の FTP サーバは短時間アクティブ モードで *n* 回以上 FTP プロキシに接続できません。ここでは *n* は、このフィールドに指定されたポート数です。
ウェルカム バナー（Welcome Banner）	接続時に FTP クライアントに表示されるウェルカム バナー。次から選択します。 • [FTP サーバメッセージを（FTP server message）]。メッセージは宛先 FTP サーバによって表示されます。このオプションは、Web プロキシが透過モードに設定されている場合にのみ利用でき、透過接続にのみ適用されます。 • [カスタム メッセージ（Custom message）]。このオプションをオンにすると、すべてのネイティブ FTP 接続に対してこのカスタム メッセージが表示されます。オフにした場合は、明示的な転送ネイティブ FTP 接続に使用されます。

手順 4　(任意)FTP プロキシの詳細設定を設定します。

プロパティ	説明
制御接続のタイムアウト(Control Connection Timeouts)	現在のトランザクションが完了していない場合に、アイドル状態の FTP クライアントまたは FTP サーバからの制御接続による通信を、FTP プロキシがさらに待機する最大時間(秒単位)。 • [クライアント側(Client side)]。アイドル状態の FTP クライアントとの制御接続のタイムアウト値。 • [サーバ側(Server side)]。アイドル状態の FTP サーバとの制御接続のタイムアウト値。
データ接続のタイムアウト(Data Connection Timeouts)	現在のトランザクションが完了していない場合に、アイドル状態の FTP クライアントまたは FTP サーバからのデータ接続による通信を、FTP プロキシがさらに待機する時間。 • [クライアント側(Client side)]。アイドル状態の FTP クライアントとのデータ接続のタイムアウト値。 • [サーバ側(Server side)]。アイドル状態の FTP サーバとのデータ接続のタイムアウト値。

手順 5　変更を送信し、保存します。

関連項目

- FTP プロキシ サービスの概要(4-15 ページ)

SOCKS プロキシ サービス

SOCKS プロキシ サービスの概要

Web Security Appliance には、SOCKS トラフィックを処理するための SOCKS プロキシが含まれます。SOCKS ポリシーは、SOCKS トラフィックを制御するアクセス ポリシーと同等です。アクセス ポリシーと同様に、識別プロファイルを使用して、各 SOCKS ポリシーによってどのトランザクションを管理するかを指定できます。SOCKS ポリシーをトランザクションに適用すると、ルーティング ポリシーによってトラフィックのルーティングを管理できます。

SOCKS プロキシでは、以下の点に注意してください。

- SOCKS プロトコルは、直接転送接続のみをサポートしています。
- SOCKS プロキシは、アップストリーム プロキシをサポートしていません(アップストリーム プロキシに転送されません)。

- SOCKS プロキシは、Application Visibility and Control（AVC）、Data Loss Prevention（DLP）、およびマルウェア検出に使用されるスキャニング サービスをサポートしていません。
- SOCKS プロキシは、ポリシー追跡をサポートしていません。
- SOCKS プロキシは、SSL トラフィックを復号化できません。これは、クライアントからサーバにトンネリングします。

SOCKS トラフィックの処理のイネーブル化

はじめる前に

- Web プロキシをイネーブルにします。

手順 1　[セキュリティ サービス（Security Services）] > [SOCKS プロキシ（SOCKS Proxy）] を選択します。

手順 2　[設定の編集（Edit Settings）] をクリックします。

手順 3　[SOCKS プロキシを有効にする（Enable SOCKS Proxy）] を選択します。

手順 4　変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

SOCKS プロキシの設定

手順 1　[セキュリティ サービス（Security Services）] > [SOCKS プロキシ（SOCKS Proxy）] を選択します。

手順 2　[設定の編集（Edit Settings）] をクリックします。

手順 3　[SOCKS プロキシを有効にする（Enable SOCKS Proxy）] を選択します。

手順 4　基本および高度な SOCKS プロキシ設定を設定します。

プロパティ	説明
SOCKS プロキシ（SOCKS Proxy）	イネーブル。
SOCKS コントロール　ポート（SOCKS Control Ports）	SOCKS 要求を受け入れるポート。デフォルトは 1080 です。
UDP リクエスト ポート（UDP Request Ports）	SOCKS サーバがリッスンする必要がある UDP ポート。デフォルトは 16000 ～ 16100 です。
プロキシ ネゴシエーション タイムアウト（Proxy Negotiation Timeout）	ネゴシエーション段階で SOCKS クライアントからデータを送受信するのを待機する時間（秒単位）。デフォルトは 60 です。
UDP トンネル タイムアウト（Tunnel Timeout）	UDP トンネルを閉じる前に UDP クライアントまたはサーバからのデータを待機する時間（秒単位）。デフォルトは 60 です。

SOCKS ポリシーの作成

手順 1　[Web セキュリティ マネージャ（Web Security Manager）] > [SOCKS ポリシー（SOCKS Policies）] を選択します。

手順 2　[ポリシーを追加（Add Policy）] をクリックします。

手順 3　[ポリシー名（Policy Name）] フィールドに名前を割り当てます。

（注）　各ポリシー グループ名は、英数字またはスペース文字のみを含む、一意の名前とする必要があります。

手順 4　（任意）説明を追加します。

手順 5　[上記ポリシーを挿入（Insert Above Policy）] フィールドで、この SOCKS ポリシーに挿入する SOCKS ポリシーの場所を選択します。

（注）　複数の SOCKS ポリシーを設定する場合、各ポリシーの論理的な順序を決定します。照合が適切に行われるように、ポリシーの順序を指定してください。

手順 6　[アイデンティティとユーザ（Identities and Users）] セクションで、このグループ ポリシーに適用する 1 つ以上の ID を選択します。

手順 7　（任意）[詳細（Advanced）] セクションを拡張して、追加のメンバーシップ要件を定義します。

高度なオプション	説明
プロキシ ポート（Proxy Ports）	ブラウザに設定されたポート。 （任意）Web プロキシへのアクセスに使用するプロキシ ポートによってポリシー グループのメンバーシップを定義します。[プロキシ ポート（Proxy Ports）] フィールドに、1 つ以上のポート番号を入力します。複数のポートを指定する場合は、カンマで区切ります。 あるポート上に要求を明示的に転送するように設定されたクライアントのセットがあり、別のポート上に要求を明示的に転送するように設定された別のクライアントのセットがある場合、プロキシ ポート上でポリシー グループのメンバーシップを定義することがあります。 **（注）**　このポリシー グループに関連付けられている ID が この詳細設定によって ID メンバーシップを定義している場合、SOCKS ポリシー グループ レベルではこの設定項目を設定できません。

高度なオプション	説明
サブネット（Subnets）	（任意）サブネットまたは他のアドレスでポリシー グループのメンバーシップを定義します。 関連付けられた ID で定義できるアドレスを使用するか、または特定のアドレスをここに入力できます。 **（注）** ポリシー グループに関連付けられている ID が、アドレスによってグループのメンバーシップを定義している場合は、このポリシー グループに、ID のアドレスのサブセットであるアドレスを入力する必要があります。ポリシー グループにアドレスを追加することにより、このグループ ポリシーに一致するトランザクションのリストを絞り込めます。
時間範囲（Time Range）	（任意）時間範囲別にポリシー グループのメンバーシップを定義します。 1. [時間範囲（Time Range）] から時間範囲を選択します。 2. このポリシー グループが選択した時間範囲内または範囲外の時間に適用されるかどうかを指定します。

手順 8　変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

次の作業

- （任意）SOCKS ポリシーで使用するための ID を追加します。
- SOCKS トラフィックを管理する 1 つ以上の SOCKS ポリシーを追加します。

要求の代替受信に関するトラブルシューティング