インターネット要求を制御するポリシーの作成

この章で説明する内容は、次のとおりです。

ポリシーの概要：代行受信されたインターネット要求の制御

ユーザーが Web 要求を作成すると、設定されている Secure Web Applianceが要求を代行受信し、最終結果を得るまでに要求が通過するプロセスを管理します。最終結果は特定の Web サイトや電子メールにアクセスすることであったり、さらにはオンラインアプリケーションにアクセスすることであったりします。 Secure Web Applianceのポリシーを設定する際に、ユーザーからの要求の基準とアクションを定義するためにポリシーが作成されます。

ポリシーは、 Secure Web Applianceが Web 要求を識別および制御する手段です。クライアントが Web 要求をサーバーに送信すると、Web プロキシはその要求を受信して評価し、要求が属しているポリシー グループを判定します。その後、ポリシーで定義されているアクションが要求に適用されます。

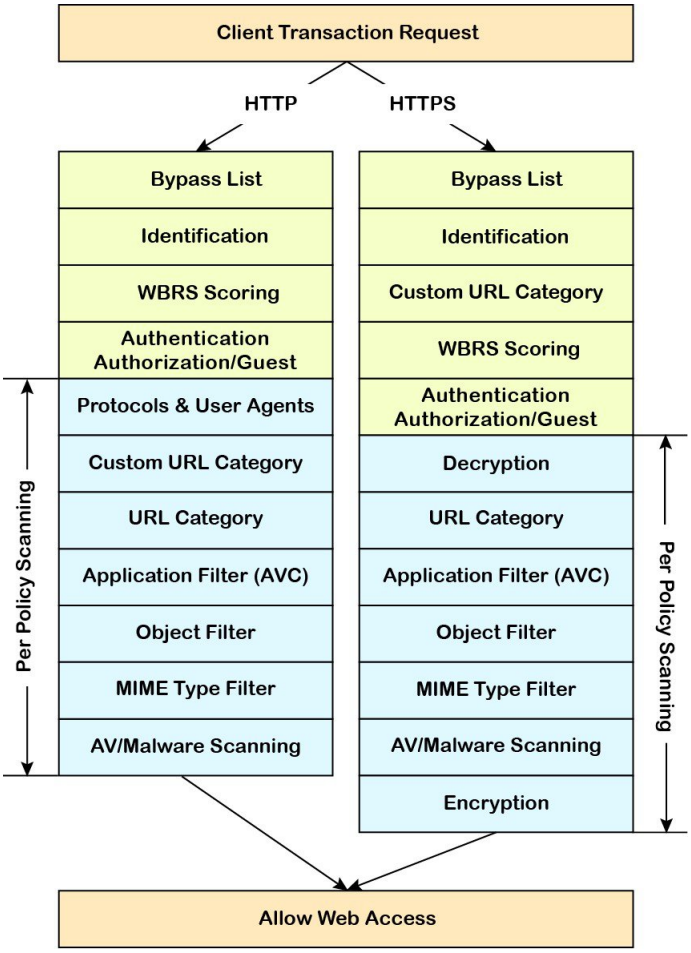
Secure Web Applianceは複数のポリシータイプを使用して、Web 要求のさまざまな側面を管理します。ポリシータイプは独自にトランザクションを全面管理するか、追加の処理のために他のポリシー タイプにトランザクションを渡します。ポリシー タイプは、実行する機能（アクセス、ルーティング、セキュリティなど）によってグループ化できます。

AsyncOS は、アプライアンスからの不要な外部通信を避けるために、外部の依存関係を評価する前にポリシーに基づいてトランザクションを評価します。たとえば、未分類の URL をブロックするポリシーによってトランザクションがブロックされた場合、そのトランザクションが DNS エラーによって失敗することはありません。

代行受信された HTTP/HTTPS 要求の処理

次の図に、代行受信された Web 要求がアプライアンスによって処理される場合のフローを示します。

図 *1 : HTTP/HTTPS* トランザクション フロー



さまざまなトランザクション処理フローを示した次の図も参照してください。

- 識別プロファイルと認証プロセス：サロゲートおよび IP ベースのサロゲートなし

- 識別プロファイルと認証プロセス：Cookie ベースのサロゲート
- 図 2：アクセス ポリシーのポリシー グループ トランザクション フロー （8 ページ）
- 復号化ポリシーのポリシー グループ トランザクション フロー
- HTTPS トラフィックの制御

ポリシー タスクによる Web 要求の管理：概要

手順	ポリシーによるWeb要求管理のタスク リスト	関連項目および手順へのリンク
1	認証レルムを設定して一定の順序に配置する	認証レルム
2	（アップストリーム プロキシの場合）プロキシ グループを作成する	アップストリーム プロキシのプロキシ グループの作成
2	（任意）カスタム クライアント アプリケーションを作成する	クライアント アプリケーション （26 ページ）
3	（任意）カスタムURL カテゴリを作成する	カスタム URL カテゴリの作成および編集
4	識別プロファイルを作成する	ユーザーおよびクライアント ソフトウェアの分類
5	（任意）時間範囲を作成し、時間帯によってアクセスを制限する	時間範囲およびクォータ （27 ページ）
[6]	ポリシーを作成して順序付ける	• ポリシーの作成 （8 ページ） • ポリシーの順序 （7 ページ）

ポリシーによる Web 要求の管理：ベスト プラクティス

Active Directory ユーザー オブジェクトを使用して Web 要求を管理する場合は、基準としてプライマリ グループを使用しないでください。Active Directory ユーザー オブジェクトにはプライマリ グループは含まれません。

ポリシー

- ポリシー タイプ （4 ページ）
- ポリシーの順序 （7 ページ）
- ポリシーの作成 （8 ページ）

ポリシー タイプ

ポリシー タイプ	要求タイプ	説明	タスクへのリンク
アクセス（Access）	• HTTP • 復号化されたHTTPS • FTP	HTTP、FTP、復号化HTTPSの着信トラフィックをブロック、許可、またはリダイレクトします。 HTTPS プロキシがディセーブルの場合、アクセス ポリシーは暗号化された着信 HTTPSトラフィックも管理します。	ポリシーの作成 （8ページ）
SOCKS	• SOCKS	Socks 通信要求を許可またはブロックします。	ポリシーの作成 （8ページ）
アプリケーション認証（Application Authentication）	• アプリケーション	Software as a Service（SaaS）アプリケーションへのアクセスを許可または拒否します。 シングル サイン オンを使用してユーザーを認証し、アプリケーションへのアクセスをただちにディセーブルにすることによってセキュリティを向上させます。 ポリシーのシングルサインオン機能を使用するには、 Secure Web ApplianceをIDプロバイダーとして設定し、SaaS の証明書とキーをアップロードまたは作成する必要があります。	SaaS アプリケーション認証ポリシーの作成
暗号化HTTPS 管理（Encrypted HTTPS Management）	• HTTPS	HTTPS 接続を復号化、パススルー、またはドロップします。 AsyncOS は、その後の処理のために、復号化したトラフィックをアクセス ポリシーに渡します。	ポリシーの作成 （8ページ）

ポリシー タイプ	要求タイプ	説明	タスクへのリンク
データ セキュリティ（Data Security）	• HTTP • 復号化されたHTTPS • FTP	Web へのデータのアップロードを管理します。データ セキュリティ ポリシーは発信トラフィックをスキャンし、宛先とコンテンツに基づいて、トラフィックがデータ アップロードの社内規則に準じていることを確認します。スキャンのために外部サーバーに発信トラフィックをリダイレクトする外部 DLP ポリシーとは異なり、データセキュリティポリシーは、 Secure Web Applianceを使用してトラフィックをスキャンし、評価します。	ポリシーの作成 （8 ページ）
外部 DLP（データ漏洩防止）（External DLP (Data Loss Prevention)）	• HTTP • 復号化されたHTTPS • FTP	サードパーティの DLP システムを実行しているサーバーに発信トラフィックを送信します。DLP システムはトラフィックをスキャンし、トラフィックがデータ アップロードに関する社内規則に準拠していることを確認します。データのアップロードも管理するデータセキュリティポリシーとは異なり、外部 DLP ポリシーは Secure Web Applianceをスキャン作業から解放します。これによって、アプライアンスのリソースが解放され、サードパーティ製ソフトウェアによって提供されるその他の機能を活用できるようになります。	ポリシーの作成 （8 ページ）
発信マルウェア スキャン（Outbound Malware Scanning）	• HTTP • 復号化されたHTTPS • FTP	悪意のあるデータを含んでいる可能性があるデータのアップロード要求をブロック、モニター、または許可します。 ネットワークにすでに存在しているマルウェアが外部ネットワークに送信されるのを防止します。	ポリシーの作成 （8 ページ）

ポリシー タイプ	要求タイプ	説明	タスクへのリンク
ルーティング	• HTTP • HTTPS • FTP	Web トラフィックをアップストリーム プロキシを介して送信するか、または宛先サーバーに送信します。既存のネットワーク設計を保護したり、 Secure Web Applianceからの処理をオフロードしたり、サードパーティのプロキシシステムから提供される追加機能を活用したりするために、アップストリームプロキシを介してトラフィックをリダイレクトできます。 複数のアップストリームプロキシが使用可能な場合、 Secure Web Applianceはロードバランシング技術を使用して、それらのプロキシにデータを分散できます。 クライアントの送信元 IP アドレスを保持するか、あるいは Web プロキシ IP または IP スプーフィングプロファイルを使用してカスタム IP に変更します。	ポリシーの作成 （8 ページ）

各ポリシー タイプはポリシー テーブルを使用して、ポリシーを保存および管理します。各ポリシー テーブルには、ポリシー タイプのデフォルト アクションを保守管理する、定義済みのグローバル ポリシーが用意されています。必要に応じて、追加のユーザー定義ポリシーが作成され、ポリシー テーブルに追加されます。ポリシーは、ポリシー テーブルのリストに記載されている順序で処理されます。

個々のポリシーには、ポリシーが管理するユーザー要求のタイプおよび要求に対して実行するアクションが定義されています。各ポリシー定義には 2 つのメイン セクションがあります。

- **[識別プロファイルとユーザー（Identification Profiles and Users）]**：識別プロファイルは、ポリシーのメンバーシップ基準で使用されます。Web トランザクションを識別するためのさまざまなオプションが含まれているので特に重要です。また、ポリシーと多くのプロパティを共有します。
- [詳細設定（Advanced）]：ポリシーの適用対象となるユーザーの識別に使用される基準。1 つ以上の基準をポリシーで指定でき、基準を満たすにはすべてが一致する必要があります。

- [プロトコル（Protocols）]：さまざまなネットワーク デバイス間でデータを転送できるようにします（http、https、ftp など）。
- [プロキシポート（Proxy Ports）]：要求が Web プロキシへのアクセスに使用する番号付きのポート。
- [サブネット（Subnets）]：要求が発信された、接続ネットワーク デバイスの論理グループ（地理的な場所、ローカル エリア ネットワーク（LAN）など）。
- [時間範囲（Time Range）]：時間範囲を作成すると、ポリシーでそれを使用し、要求が行われた時間帯に基づいて Web 要求を識別したり、Web 要求にアクションを適用できます。時間範囲は、個々のユニットとして作成されます。
- [URLカテゴリ（URL Categories）]：URL カテゴリは Web サイトの定義済みまたはカスタムのカテゴリです（ニュース、ビジネス、ソーシャル メディアなど）。これらを使用して、Web 要求を識別したり、Web 要求にアクションを適用できます。
- [ユーザー エージェント（User Agents）]：要求の作成に使用されるクライアント アプリケーション（アップデータや Web ブラウザなど）があります。ユーザー エージェントに基づいてポリシーの基準を定義したり、制御設定を指定できます。認証からユーザー エージェントを除外することもできます。これは、クレデンシャルの入力を求めることができないアプリケーションで役立ちます。カスタム ユーザー エージェントを定義できますが、これらの定義を他のポリシーで再利用することはできません。

（注） 複数のメンバーシップ基準を定義した場合、クライアント要求は、ポリシーに一致するために、すべての基準を満たす必要があります。

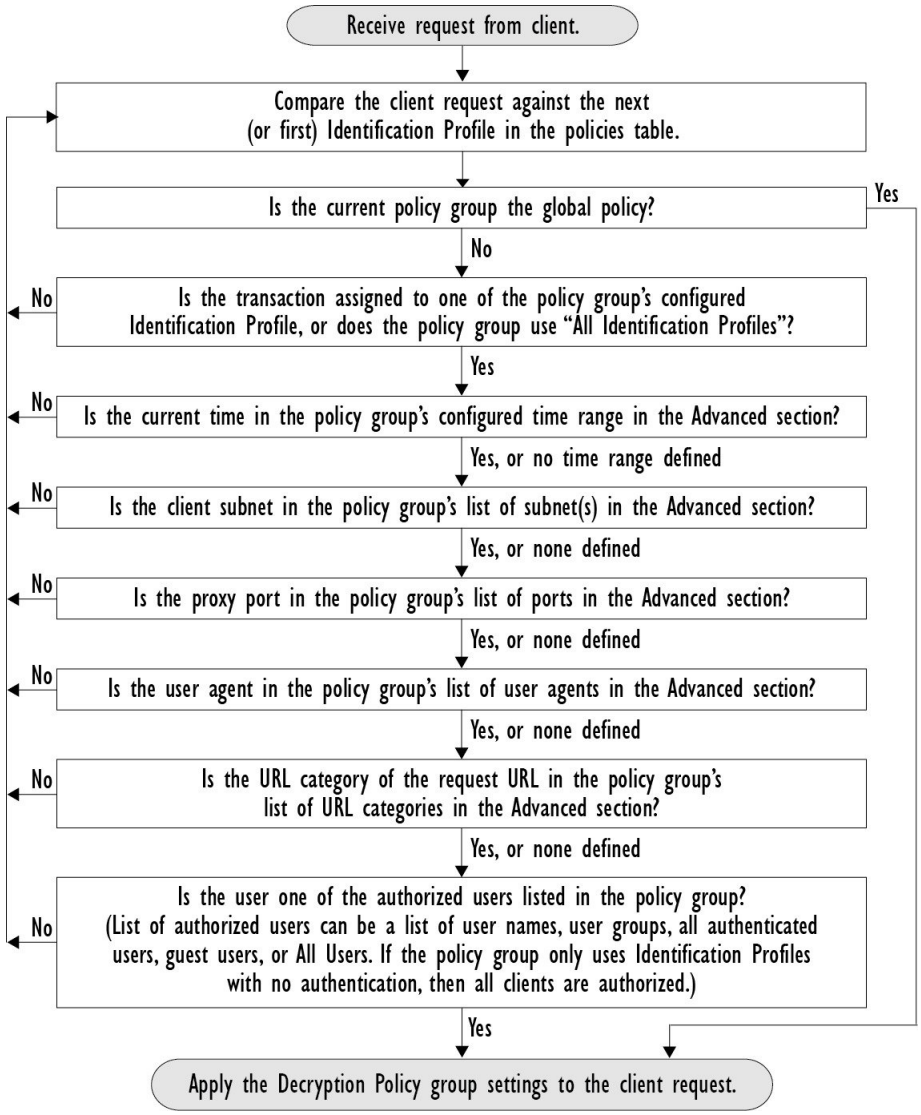
ポリシーの順序

ポリシー テーブルにポリシーを記載する順序によって、Web 要求に適用されるポリシーの優先順位が決まります。Web 要求との照合はテーブルの最上位のポリシーから順に行われ、要求がポリシーに一致した時点で照合は終了します。テーブル内のそれ以降のポリシーは処理されません。

ユーザ定義のポリシーが Web 要求と一致しない場合、そのポリシー タイプのグローバル ポリシーが適用されます。グローバル ポリシーは常にポリシー テーブルの最後に配置され、順序変更できません。

次の図に、アクセス ポリシー テーブルを介したクライアント要求のフローを示します。

図 *2:* アクセス ポリシーのポリシー グループ トランザクション フロー



ポリシーの作成

始める前に

- 該当するプロキシをイネーブルにします。
  - Web プロキシ（HTTP、復号されたHTTPS、および FTP 用）
  - HTTPS プロキシ（HTTPS Proxy）
  - SOCKS プロキシ（SOCKS Proxy）
- 関連する識別プロファイルを作成します。

- ポリシーの順序 （7 ページ）について理解しておきます。
- （暗号化された HTTPS のみ）証明書とキーをアップロードまたは作成します。
- （データ セキュリティのみ）Ciscoデータ セキュリティ フィルタの設定をイネーブルにします。
- （外部 DLP のみ）外部 DLP サーバを定義します。
- （ルーティングのみ） Secure Web Applianceに対して関連するアップストリームプロキシを定義します。
- （任意）関連するクライアント アプリケーションを作成します。
- （任意）関連する時間範囲を作成します。時間範囲およびクォータ （27 ページ）を参照してください。
- （任意）関連する URL カテゴリを作成します。カスタム URL カテゴリの作成および編集を参照してください。

ステップ 1 [ポリシー設定（Policy Settings）] セクションで、[アイデンティティを有効化（Enable Identity）] チェックボックスを使用してこのポリシーをイネーブルにするか、ポリシーを削除せずにただちにディセーブルにします。

ステップ 2 [名前（Name）] に一意のポリシー名を割り当てます。

ステップ 3 [説明（Description）] は任意です。

ステップ 4 [上に挿入（Insert Above）] ドロップダウン リストで、このポリシーを表示するテーブル内の位置を選択します。

（注） ポリシーを配置します。最上位のものが最も制限が厳しく、最下位のものが最も緩くなります。詳細については、ポリシーの順序 （7 ページ）を参照してください。

ステップ 5 [ポリシーの有効期限（Policy Expires）] エリアで、[ポリシーの有効期限の設定（Set Expiration for Policy）] チェック ボックスをオンにして、ポリシーの有効期限を設定します。設定するポリシーの有効期限の日時を入力します。設定期限を越えると、ポリシーは自動的に無効になります。

（注） システムは 1 分ごとにポリシーをチェックして、1 分間に有効期限が切れるポリシーを無効にします。たとえば、ポリシーが 11:00 に期限が切れるように設定されている場合、ポリシーは最大で 11:01 までに無効になります。

ポリシーの有効期限機能は、アクセス ポリシー、復号ポリシー、およびWebトラフィック タップ ポリシーにのみ適用されます。

ポリシーの有効期限の 3 日前にメールが届き、有効期限にもう一度メールが届きます。

（注） アラートを受信するには、[システム管理（System Administration）] > [アラート（Alerts）] を使用して、ポリシーの有効期限アラートを有効にする必要があります。ポリシーの期限切れアラートを参照してください

Cisco コンテンツ セキュリティ管理アプライアンスを使用してポリシーの有効期限を設定することもできます。設定された有効期限が過ぎるとポリシーは失効しますが、Cisco コンテンツ セキュリティ管理アプライアンスの GUI では無効と表示されません。

ポリシーの有効期限機能を設定した後、有効期限はアプライアンスのローカル時間の設定に基づいて期限切れとなります。

ステップ 6 [ポリシーメンバの定義（Policy Member Definition）]セクションで、ユーザおよびグループのメンバーシップの定義方法を選択します。[識別プロファイルとユーザ（Identification Profiles and Users）] リストから、以下のいずれかを選択します。

- [すべての識別プロファイル（All Identification Profiles）]：このポリシーを既存のすべてのプロファイルに適用します。少なくとも 1 つの [詳細設定（Advanced）] オプションを定義する必要があります。
- [1つ以上の識別プロファイルを選択（Select One or More Identification Profiles）]：個々の識別プロファイルを指定するためのテーブルが表示されます。1 行ごとに 1 つのプロファイル メンバーシップ定義が含まれています。

ステップ 7 [すべての識別プロファイル（All Identification Profiles）] を選択した場合：

a) 以下のいずれか 1 つのオプションを選択して、このポリシーを適用する承認済みユーザとグループを指定します。

- [すべての承認済みユーザ（All Authenticated Users）]：認証または透過的 ID によって識別されたすべてのユーザ。
- [選択されたグループとユーザ（Selected Groups and Users）]：指定したユーザとグループが使用されます。

  指定した **ISE セキュリティ グループ タグ**（SGT）や指定したユーザを追加または編集するには、次の適切なラベルのリンクをクリックします。たとえば、現在指定しているユーザのリストを編集するには、そのリストをクリックします。詳細については、ポリシーのセキュリティ グループ タグの追加と編集 （12 ページ）を参照してください。

  ISE を使用する場合、ISE セキュリティ グループ タグを追加または編集できます。これは ISE-PIC 導入ではサポートされていません。指定した **ISE グループ**を追加または編集するには、次のラベルのリンクをクリックします。このオプションは、ISE-PIC に固有です。

- [ゲスト（Guests）]：ゲストとして接続されているユーザと認証に失敗したユーザ。
- [すべてのユーザ（All Users）]：すべてのクライアント。承認済みかどうかは問いません。このオプションを選択する場合は、少なくとも 1 つの [詳細設定（Advanced）] オプションを設定する必要があります。

ステップ 8 [1つ以上の識別プロファイルを選択（Select One or More Identification Profiles）] を選択すると、プロファイル選択テーブルが表示されます。

a) [識別プロファイル（Identity Profiles）] 列の [識別プロファイルの選択（Select Identification Profile）] ドロップダウン リストから、識別プロファイルを選択します。

b) このポリシーを適用する承認済みユーザとグループを指定します。

- [すべての承認済みユーザ（All Authenticated Users）]：認証または透過的 ID によって識別されたすべてのユーザ。
- [選択されたグループとユーザ（Selected Groups and Users）]：指定したユーザとグループが使用されます。

  指定した ISE セキュリティ グループ タグ（SGT）や指定したユーザを追加または編集するには、適切なラベルのリンクをクリックします。たとえば、現在指定しているユーザのリストを編集するには、そのリストをクリックします。詳細については、ポリシーのセキュリティ グループ タグの追加と編集 （12 ページ）を参照してください。
- [ゲスト（Guests）]：ゲストとして接続されているユーザと認証に失敗したユーザ。

c) プロファイル選択テーブルに行を追加するには、[識別プロファイルの追加（Add Identification Profile）] をクリックします。行を削除するには、その行のゴミ箱アイコンをクリックします。

必要に応じて、ステップ (a) から (c) を繰り返して必要な識別プロファイルを追加します。

ステップ 9 [詳細設定（Advanced）] セクションを展開し、追加のグループ メンバーシップ基準を定義します（[ポリシーメンバの定義（Policy Member Definition）] セクションで選択したオプションによっては、このステップは任意になります。また、設定するポリシーのタイプによっては、以下のオプションの一部を使用できません）。

高度なオプション	説明
プロトコル	このポリシーを適用するプロトコルを選択します。[その他のすべて（All others）] は、選択されていないすべてのプロトコルを意味します。関連付けられている識別プロファイルを特定のプロトコルに適用すると、このポリシーもそれらのプロトコルに適用されます
プロキシ ポート（Proxy Ports）	特定のポートを使用して Web プロキシにアクセスするトラフィックにのみ、このポリシーが適用されます。1 つ以上のポート番号を入力します。複数のポートはカンマで区切ります。 明示的な転送接続のために、ブラウザに設定されたポートです。 透過接続の場合は、宛先ポートと同じです。 （注） 関連付けられている識別プロファイルを特定のプロキシポートにのみ適用している場合は、ここにプロキシ ポートを入力できません。
サブネット（Subnets）	特定のサブネットのトラフィックにのみこのポリシーが適用されます。[サブネット指定（Specify subnets）] を選択し、サブネットをカンマで区切って入力します。 サブネットによってさらにフィルタリングしない場合は、[選択したアイデンティティからのサブネットを使用（Use subnets from selected Identities）] をオンのままにしておきます。 （注） 関連する ID を特定のサブネットに適用すると、このポリシーの適用を ID が適用されるアドレスのサブセットに限定できます。

高度なオプション	説明
時間範囲（Time Range）	ポリシー メンバーシップに時間範囲を適用できます。 • [時間範囲（Time Range）]：前に定義した時間範囲を選択します（時間範囲およびクォータ （27 ページ））。 • [時間範囲の一致（Match Time Range）]：このオプションを使用して、この時間範囲を含めるか除外するかを指定します。つまり、指定した範囲内のみを照合するか、指定した範囲を除くすべての時間について照合するかを指定します。
URL カテゴリ（URL Categories）	特定の宛先（URL）と URL カテゴリによってポリシー メンバーシップを制限できます。すべての必要なカスタム カテゴリと定義済みカテゴリを選択します。カスタム カテゴリの詳細については、カスタム URL カテゴリの作成および編集を参照してください。
ユーザ エージェント（User Agents）	特定のユーザ エージェントを選択し、このポリシーのユーザ定義の一部として、正規表現を使用してカスタム エージェントを定義できます。 • **[共通ユーザ エージェント（Common User Agents）]** • [ブラウザ（Browsers）]：このセクションを展開して、さまざまな Web ブラウザを選択します。 • [その他（Others）]：このセクションを展開して、アプリケーション アップデータなどの特定の非ブラウザ エージェントを選択します。 • [カスタム ユーザ エージェント（Custom User Agents）]：1 つ以上の正規表現を（1 行に 1 つずつ）入力して、カスタム ユーザ エージェントを定義できます。 • [ユーザ エージェントの一致（Match User Agents）]：このオプションを使用して、これらのユーザ エージェントの指定を含めるか除外するかを指定します。つまり、メンバーシップの定義に選択したユーザ エージェントのみを含めるか、選択したユーザ エージェントを明確に除外するかどうかを指定します。

ポリシーのセキュリティ グループ タグの追加と編集

ポリシーの特定の識別プロファイルに割り当てられているセキュリティ グループ タグ（SGT）のリストを変更するには、[ポリシーの追加または編集（Add/Edit Policy）] ページの [選択されたグループとユーザ（Selected Groups and Users）] リストで、[ISEセキュリティグループタグ（ISE Secure Group Tags）] ラベルの後ろのリンクをクリックします。（ポリシーの作成 （8 ページ） を参照。）このリンクは、[タグが未入力（No tags entered）] または現在割り当てられているタグのリストです。リンクをクリックすると [セキュリティグループタグの追加または編集（Add/Edit Group）] ページが開きます。

現在このポリシーに割り当てられている SGT が [承認済みセキュリティグループタグ（Authorized Secure Group Tags）] セクションに表示されます。接続されている ISE サーバから使用可能な

すべての SGT が、[セキュリティグループタグの検索（Secure Group Tag Search）] セクションに表示されます。

ステップ 1 [承認済みセキュリティグループタグ（Authorized Secure Group Tags）] リストに 1 つ以上の SGT を追加するには、[セキュリティグループタグの検索（Secure Group Tag Search）] セクションに必要事項を入力し、[追加（Add）] をクリックします。

（注）
- すでに追加されている SGT が緑色で強調表示されます。この利用可能な SGT のリストから特定の SGT を検索するには、[検索（Search）] フィールドにテキスト文字列を入力します。
- Secure Web Applianceが ISE/ISE-PIC に接続されている場合、ISE/ISE-PIC からのデフォルト SGT も表示されます。これらの SGT には割り当てられたユーザがありません。正しい SGT を選択したことを確認してください。

ステップ 2 [承認済みセキュリティグループタグ（Authorized Secure Group Tags）] リストから 1 つ以上の SGT を削除するには、削除するエントリを選択し、[削除（Delete）] をクリックします。

ステップ 3 [完了（Done）] をクリックして、[グループの追加または編集（Add/Edit Group）] ページに戻ります。

次のタスク

関連項目

- 時間範囲およびクォータ （27 ページ）
- ポリシーでのクライアント アプリケーションの使用 （26 ページ）

ルーティングポリシーへのルーティング先と IP スプーフィングプロファイルの追加

ルーティングポリシーにルーティング先と IP スプーフィングプロファイルを設定することによって、Web プロキシが Web トラフィックを転送し、送信元 IP アドレスを要求する方法を設定できます。

（注）
- デフォルトでは、アップストリーム プロキシ グループがアプライアンス上に設定されていない場合でも、グローバル ルーティング ポリシーは有効になります。
- IP スプーフィングプロファイルはルーティング先とは関連がないため、個別に設定できます。
- ルーティングポリシーは、アップストリームプロキシを設定せずに有効にすることができます。

（注） セキュリティ管理アプライアンスでルーティングポリシーのアップストリームプロキシグループを設定するには、Secure Web Applianceのコンフィギュレーションファイルを保存し、セキュリティ管理アプライアンスにインポートします。それ以外の場合は、セキュリティ管理アプライアンスはアップストリームプロキシを「見つかりませんでした（Not Found）」として表示し、設定のプッシュ後にルーティングポリシーを無効にします。

ステップ 1 [Web Security Manager] > [ルーティングポリシー（Routing Policies）] を選択します。

ステップ 2 [ルーティングポリシー（Routing Policies）]ページで、アップストリームプロキシグループを設定するルーティングポリシーの [ルーティング先（Routing Destination ）] 列の下にあるリンクをクリックします。

ステップ 3 選択したポリシーに適したアップストリーム プロキシ グループを次から選択します。

アクション	説明
[グローバルポリシー設定を使用する（Use Global Policy Settings）]	Webプロキシは、グローバルポリシーで定義されている設定を使用します。これは、ユーザー定義のポリシー グループのデフォルト アクションです。デフォルトでは、グローバル ルーティング ポリシーのルーティング先は[直接接続（Direct Connection）]として設定されます。 ユーザー定義のポリシー グループにのみ適用されます。
直接接続	Web プロキシは、Web トラフィックを宛先 Web サーバーに直接転送します。
[カスタム アップストリーム プロキシ グループ（Custom upstream proxy group）]	Web プロキシは、Web トラフィックを外部のアップストリーム プロキシ グループにリダイレクトします。アップストリーム プロキシ グループの作成の詳細については、アップストリーム プロキシを参照してください。

ステップ 4 [ルーティングポリシー（Routing Policies）]ページで、IP スプーフィングプロファイルを設定するルーティングポリシーの [IP スプーフィング（IP Spoofing）] 列の下にあるリンクをクリックします。

ステップ 5 選択したポリシーに適した IP スプーフィングプロファイルを次から選択します。

アクション	説明
[グローバルポリシー設定を使用する（Use Global Policy Settings）]	Webプロキシは、グローバルポリシーで定義されている設定を使用します。これは、ユーザー定義のポリシー グループのデフォルト アクションです。グローバル ルーティング ポリシーの場合、IP スプーフィングはデフォルトで無効になっています。 ユーザー定義のポリシー グループにのみ適用されます。
[IP スプーフィングを使用しない（Do No Use IP Spoofing）]	Web プロキシは、要求送信元の IP アドレスを変更し、それ自体のアドレスと一致させてセキュリティを強化します。

アクション	説明
[クライアント IP を使用する（Use Client IP）]	Web プロキシは送信元アドレスを保持するため、 Secure Web 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。
[カスタム スプーフィング プロファイル名（Custom spoofing profile name）]	Web プロキシは、要求の送信元 IP アドレスを選択したカスタム IP スプーフィング プロファイル名に定義されているカスタム IP に変更します。

ステップ 6 変更を [実行（Submit）] して [確定する（Commit）] します。

次のタスク

関連項目

- アップストリーム プロキシ
- Web プロキシの IP スプーフィング

ポリシーの設定

ポリシーテーブルの各行はポリシー定義を表し、各列にはそのポリシー要素の設定ページへのリンクが含まれています。

（注） 以下のポリシー設定コンポーネントについて、URL フィルタリングのみを使用して「警告」オプションを指定できます。

オプション	説明
プロトコルとユーザー エージェント（Protocols and User Agents）	プロトコルへのポリシー アクセスの制御、および特定のクライアント アプリケーション（インスタント メッセージ クライアント、Web ブラウザ、インターネット電話サービスなど）のブロック設定に使用されます。また、特定のポートの HTTP CONNECT 要求をトンネルするようにアプライアンスを設定することもできます。トンネリングがイネーブルの場合、アプライアンスはHTTP トラフィックを、評価せずに、指定されたポート経由で渡します。

オプション	説明
URL フィルタリング（URL Filtering）	AsyncOS for Web では、アプライアンスが、特定の HTTP 要求または HTTPS 要求の URL カテゴリに基づいてトランザクションを処理する方法を設定できます。定義済みのカテゴリ リストを使用して、クォータ ベースまたは時間ベースのフィルタをモニター、ブロック、警告または設定するかを選択できます。 また、カスタム URL カテゴリを作成して、カスタム カテゴリ内の Web サイト用のクォータ ベースまたは時間ベースのフィルタをブロック、リダイレクト、許可、モニター、警告、または適用するかを選択することもできます。カスタム URL カテゴリの作成については、カスタム URL カテゴリの作成および編集 を参照してください。 また、組み込みまたは参照コンテンツのブロックの例外を追加することもできます。
アプリケーション	AVC または ADC エンジンは、アクセプタブル ユース ポリシーのコンポーネントであり、アプリケーションで使用される Web トラフィックを深く理解し、管理できるように、Web トラフィックを検査します。アプリケーションタイプまたは個々のアプリケーションごとにアプリケーションをブロックまたは許可するように、Web プロキシを設定できます。 AsyncOS 15.0 以降では、AVC または ADC エンジンを使用して Web トラフィックを監視できます。デフォルトでは、AVC は有効になっています。 AVC エンジンは ADC エンジンと同じように動作しますが、AVC エンジンは限られた数のアプリケーションをサポートします。また、AVC エンジンでは特定のアプリケーション内の特定のアプリケーション動作（ファイル転送など）に制御を適用できます。設定の詳細については、Web アプリケーションへのアクセスの管理を参照してください （注） ADC アクティビティの設定後に、ADC アプリケーション エンジンは特定のトラフィックのアクティビティ情報を検索または評価します。 ADC 署名データベースの更新により、カテゴリ全体が [ブロック（Block）] に設定されている場合でも、追加された新しいアプリケーションはすべてデフォルトで [モニタ（Monitor）] に設定されます。
オブジェクト	これらのオプションを使用して、Web プロキシがファイルの特性（ファイルのサイズ、ファイルのタイプ、および MIME タイプなど）に基づいてファイルのダウンロードをブロックできるように設定します。一般的に、オブジェクトとは、個々に選択、アップロード、ダウンロード、および処理できる項目です。次に示すような

オプション	説明
マルウェア対策とレピュテーション（Anti-Malware and Reputation）	Web レピュテーション フィルタを使用すると、Web ベースのレピュテーション スコアを URL に割り当て、URL ベースのマルウェアが含まれている可能性を判定できます。マルウェア対策スキャンにより、Web ベースのマルウェアの脅威を識別して阻止します。Secure Endpoint はダウンロードしたファイル内のマルウェアを識別します。 マルウェア対策とレピュテーション ポリシーは、各コンポーネントごとにグローバル設定から継承されます。[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）] では、マルウェア スキャンの判定に基づいてモニターまたはブロックするようにマルウェア カテゴリをカスタマイズしたり、Web レピュテーション スコアのしきい値をカスタマイズすることができます。マルウェア カテゴリはポリシー内でさらにカスタマイズできます。また、ファイル レピュテーション サービスと分析サービス用のグローバル設定項目もあります。 詳細については、アクセス ポリシーにおけるマルウェア対策およびレピュテーションの設定およびファイル レピュテーションと分析機能の設定を参照してください。
HTTP ReWrite プロファイル	HTTP リクエストのカスタム ヘッダー プロファイルを設定し、ヘッダー書き換えプロファイルの下に複数のヘッダーを作成できます。ヘッダー書き換えプロファイル機能を使用すると、認証が成功した後、アプライアンスがユーザとグループの情報を別のアップストリーム デバイスに渡すことができます。アップストリーム プロキシはユーザを認証済みと見なし、追加の認証をバイパスし、定義されたアクセス ポリシーに基づいてユーザにアクセスを提供します。 ポリシーごとの Web プロキシ カスタム ヘッダーを参照してください。

オプション	説明
ポリシーの複製	既存のポリシーに、新しいポリシーで必要な設定のほとんどが含まれている場合は、既存のポリシーを複製してから変更することで時間を節約できます。複製されたポリシーは同じグループ化属性を共有しますが、表示名、IP アドレス、ホスト、ドメイン名などの独自の ID を持っています。 Cisco Secure Web Appliance のクローンオプションを含む次のポリシーは、Cisco Secure Email and Web Manager（SMA）でも管理できます。 • アクセス • 復号化 • ID • ルーティング • 外部 DLP（External DLP） • 発信マルウェア スキャン（Outbound Malware Scanning） • HTTP ReWrite プロファイル • Cisco データ セキュリティ （注） インスタンスで複製できるポリシーは 1 つだけです。
削除（Delete）	作成したポリシーを削除します。

アクセス ポリシー：オブジェクトのブロッキング

[アクセス ポリシー：オブジェクト（Access Policies: Objects）] ページのオプションを使用して、ファイル サイズ、ファイル タイプ、MIME タイプなどのファイル特性に基づきファイルのダウンロードをブロックできます。オブジェクトとは一般的に、個々に選択、アップロード、ダウンロード、および処理できる項目を指します。

個々のアクセス ポリシー、およびグローバル ポリシーによって、さまざまなオブジェクト タイプをブロック対象に指定できます。これらのオブジェクト タイプには、アーカイブ、ドキュメント タイプ、実行可能コード、Web ページ コンテンツなどが含まれます。

ステップ 1 [アクセス ポリシー（Access Policies）] ページ（[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）]）で、編集対象のポリシーを表す行の [オブジェクト（Objects）] 列にあるリンクをクリックします。

ステップ 2 このアクセス ポリシーでブロックするオブジェクトのタイプを選択します。

- [グローバル ポリシー オブジェクト ブロック設定を使用（Use Global Policy Objects Blocking Settings）]：このポリシーでは、グローバル ポリシーに対して定義されているオブジェクト ブロック設定を使用し

ます。これらの設定は、読み取り専用モードで表示されます。設定を変更するには、グローバル ポリシーの設定を編集します。

- [カスタム オブジェクト ブロック設定の定義（Define Custom Objects Blocking Settings）]：このポリシーのすべてのオブジェクト ブロック設定を編集できます。
- [このポリシーのオブジェクト ブロックを無効にする（Disable Object Blocking for this Policy）]：このポリシーのオブジェクトブロックを無効にします。オブジェクトブロックのオプションは表示されません。

ステップ 3 前のステップで [カスタム オブジェクト ブロック設定の定義（Define Custom Objects Blocking Settings）] を選択した場合、[アクセス ポリシー：オブジェクト（Access Policies: Objects）] ページで、必要に応じてオブジェクト ブロックのオプションをオフにします。

オブジェクトのサイズ	ダウンロード サイズに基づいて、オブジェクトをブロックできます。 • [HTTP/HTTPS 最大ダウンロード サイズ（HTTP/HTTPS Max Download Size）]：HTTP/HTTPS ダウンロードの最大オブジェクト サイズを指定するか（指定したサイズより大きいオブジェクトはブロックされます）、HTTP/HTTPS でダウンロードするオブジェクトに最大サイズの制限を設けないことを指定します。 • [FTP 最大ダウンロード サイズ（FTP Max Download Size）]：FTP ダウンロードの最大オブジェクトサイズを指定するか（指定したサイズより大きいオブジェクトはブロックされます）、FTP でダウンロードするオブジェクトに最大サイズの制限を設けないことを指定します。
ブロックするオブジェクトタイプ	
アーカイブ（Archives）	このセクションを展開して、ブロックするアーカイブ ファイイルのタイプを選択します。このリストには、ARC、BinHex、StuffIt などのアーカイブ タイプが含まれます。

検査可能なアーカイブ（**Inspectable Archives**）	

	このセクションを展開して、検査可能なアーカイブ ファイルの特定のタイプを[許可（Allow）]、[ブロック（Block）]、または[検査（Inspect）]します。検査可能なアーカイブとは、 Secure Web Appliance により各ファイルのコンテンツを検査し、ファイル タイプ ブロック ポリシーを適用できるアーカイブファイル（圧縮ファイル）のことです。検査可能なアーカイブ タイプには、7zip、Microsoft CAB、RAR、TAR などが含まれます。 アーカイブの検査には、以下のことが適用されます。 • [検査（Inspect）]とマークされたアーカイブ タイプだけが展開されて検査されます。 • 一度に検査できるアーカイブは1つだけです。同時に検査可能なアーカイブが他にある場合でも、それらのアーカイブは検査されません。 • 検査されるアーカイブに、現在のポリシーで[ブロック（Block）]アクションが割り当てられているファイルタイプが含まれる場合、許可されるファイル タイプが含まれているとしても、アーカイブ全体がブロックされます。 • サポートされないアーカイブ タイプが含まれる検査対象アーカイブは、「スキャン不可（unscannable）」としてマークされます。ブロック対象のアーカイブ タイプが含まれている場合、アーカイブはブロックされます。 • パスワード保護された暗号化アーカイブはサポートされないため、「スキャン不可（unscannable）」としてマークされます。 • 検査可能なアーカイブが不完全であるか破損している場合、「スキャン不可（unscannable）」としてマークされます。 • [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] グローバル設定に指定された [DVS エンジン オブジェクト スキャンの制限（DVS Engine Object Scanning Limits）] の値は、検査可能なアーカイブのサイズにも適用されます。指定されたサイズを超えているオブジェクトは、「スキャン不可（unscannable）」としてマークされます。このオブジェクトサイズ制限については、マルウェア対策とレピュテーション フィルタの有効化を参照してください。 • 「スキャン不可（unscannable）」としてマークされた検査可能なアーカイブは、アーカイブ全体がブロックされるか、許可されるかのいずれかです。 • カスタムの MIME タイプをブロックするようにアクセス ポリシーが設定されており、アーカイブ検査が有効になっている場合。 • アプライアンスがカスタム MIME タイプのファイルを Content-Type ヘッダーの一部として直接ダウンロードしようとすると、アクセスがブロックされます。 • 同じファイルが ZIP/アーカイブ ファイルの一部である場合、アプライアンスはアーカイブを検査し、独自の MIME 評価に基づいて MIME

	タイプを決定します。アプライアンスのエンジンによって評価されるMIMEが設定済みのカスタムMIMEタイプと一致しない場合、コンテンツはブロックされません。 • アプライアンスは設定されたアーカイブを検査できますが、RAR や 7-Zip などの特定のアーカイブを検査することには制限があります。 アーカイブ検査の設定について詳しくは、アーカイブ検査の設定（22ページ）を参照してください。
ドキュメント タイプ（Document Types）	このセクションを展開して、ブロックするテキストドキュメントのタイプを選択します。このリストには、FrameMaker、Microsoft Office、PDF などのドキュメント タイプが含まれます。
実行可能コード（Executable Code）	このセクションを展開して、ブロックする実行可能コードのタイプを選択します。このリストには、Java アプレット、UNIX 実行可能ファイル、Windows 実行可能ファイルが含まれます。
インストーラ（Installers）	ブロックするインストーラのタイプを選択します。このリストには、UNIX/LINUX パッケージが含まれます。
メディア（Media）	ブロックするメディア ファイルのタイプを選択します。このリストには、音声、ビデオ、および写真画像処理フォーマット（TIFF/PSD）が含まれます。
P2P メタファイル（P2P Metafiles）	このリストには BitTorrent リンク（`.torrent`）が含まれます。
Web ページ コンテンツ（Web Page Content）	このリストには、フラッシュおよびイメージが含まれます。
その他（Miscellaneous）	このリストには、カレンダー データが含まれます。
カスタム MIME タイプ	MIMEタイプに基づいてブロックする追加のオブジェクト/ファイルを定義できます。 [ブロックする MIME タイプ(Block Custom MIME Types)] フィールドに、1 つ以上の MIME タイプを入力します。

ステップ 4 **[送信（Submit）]** をクリックします。

アーカイブ検査の設定

個々のアクセス ポリシーで、特定のタイプの検査可能なアーカイブを許可、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、 Secure Web Appliance により各ファイルのコンテンツを検査し、ファイル タイプ ブロック ポリシーを適用できるアーカイブファイル（圧縮ファイル）のことです。個々のアクセス ポリシーでアーカイブ検査を設定する方法に

ついて詳しくは、アクセス ポリシー：オブジェクトのブロッキング （18 ページ）を参照してください。

（注） アーカイブ検査では、ネストされたオブジェクトがディスクに書き込まれて検査されます。ファイルの検査で使用可能なディスク容量は、随時 1 GB です。このディスク使用量の最大サイズを超えるアーカイブ ファイルは、「スキャン不可（unscannable）」としてマークされます。

Secure Web Appliance の [使用許可コントロール（Acceptable Use Controls）] ページには、システム全体の検査可能なアーカイブ設定が表示されます。これらの設定は、アクセスポリシーでアーカイブの抽出と検査が有効にされている場合は常にアーカイブに適用されます。

ステップ 1 [セキュリティ サービス（Security Services）] > [使用許可コントロール（Acceptable Use Controls）] を選択します。

ステップ 2 [アーカイブ設定の編集（Edit Archives Settings）] ボタンをクリックします。

ステップ 3 必要に応じて、検査可能なアーカイブ設定を編集します。

- [カプセル化されたアーカイブの最大抽出数（Maximum Encapsulated Archive Extractions）]：抽出して検査する「カプセル化」されたアーカイブの最大数。つまり、他の検査可能なアーカイブが含まれるアーカイブを検査する最大深さです。カプセル化されたアーカイブとは別のアーカイブ ファイルに含まれるアーカイブのことです。有効な値は 0 ～ 5 です。深さは、最初にネストされているファイルを 1 としてカウントされます。

  外部アーカイブ ファイルは値ゼロのファイルと見なされます。このネストの最大値を超えるファイルがアーカイブに含まれている場合、アーカイブは「スキャン不可（unscannable）」としてマークされます。この設定はパフォーマンスに影響を与えることに注意してください。

- [検査できないアーカイブをブロック（Block Uninspectable Archives）]：このオプションをオンにすると、 Secure Web Appliance は展開して検査できなかったアーカイブをブロックします。

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

トランザクション要求のブロック、許可、リダイレクト

Web プロキシは、トランザクション要求のグループ用に作成されたポリシーに基づいて、Web トラフィックを制御します。

- **[許可（Allow）]**。Web プロキシは、中断のない接続を許可します。許可された接続は、DVS エンジンによってスキャンされていない可能性があります。
- **[ブロック（Block）]**。Web プロキシは、接続を許可せず、ブロックの理由を説明するエンド ユーザー通知ページを表示します。

- **リダイレクト。**Webプロキシは、最初に要求された宛先サーバーへの接続を許可せず、指定された別の URL に接続します（アクセス ポリシーでのトラフィックのリダイレクトを参照）。

（注） 上記のアクションは、Web プロキシがクライアント要求に対して実行する最終アクションです。アクセス ポリシーに対して設定できるモニター アクションは最終アクションではありません。

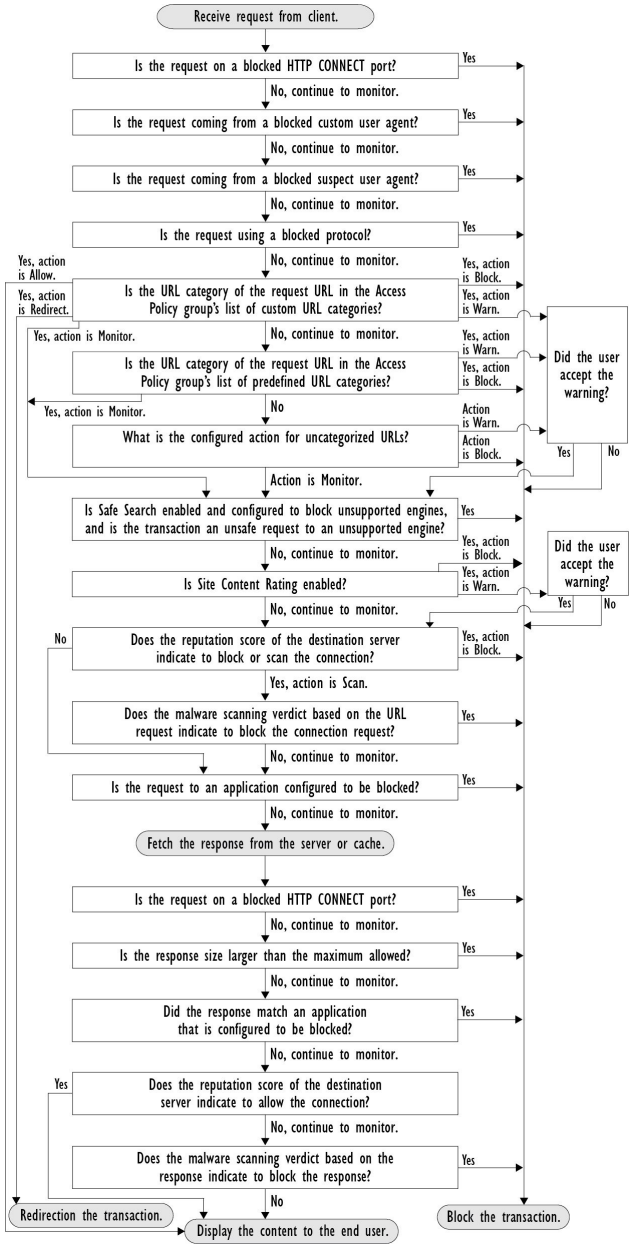
通常、トラフィックは、トランスポートプロトコルに基づいて、さまざまなタイプのポリシーにより制御されます。

ポリシー タイプ	プロトコル				サポートされるアクション			
	HTTP	HTTPS	FTP	SOCKS	ブロック（Block）	許可（Allow）	リダイレクト	モニター（Monitor）
アクセス（Access）	x	x	x		x	x	x	x
SOCKS				x	x	x		
SAAS	x	x						
復号化（Decryption）	x	x						x
データ セキュリティ（Data Security）	x	x	x		x			x
外部 DLP（External DLP）	x	x	x				x	
発信マルウェア スキャン（Outbound Malware Scanning）	x	x	x		x			x
ルーティング	x	x	x				x	

（注） 復号化ポリシーはアクセス ポリシーに優先します。

次の図に、Web プロキシが特定のアクセス ポリシーを要求に割り当てた後に、その要求で実行するアクションを決定する方法を示します。宛先サーバーの Web レピュテーション スコアが評価されるのは 1 回だけですが、その結果は、決定フローの 2 つのポイントで適用されます。

図 *3:* アクセス ポリシーのアクションの適用



クライアント アプリケーション

クライアント アプリケーションについて

クライアント アプリケーション（Web ブラウザなど）は要求を行うために使用されます。クライアント アプリケーションに基づいてポリシー メンバーシップを定義し、制御設定を指定してクライアントアプリケーションの認証を免除することがきます。これは、アプリケーションがクレデンシャルの入力を要求できない場合に役立ちます。

ポリシーでのクライアント アプリケーションの使用

クライアント アプリケーションによるポリシー メンバーシップの定義

ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] メニューからポリシー タイプを選択します。

ステップ 2 ポリシー テーブル内のポリシー名をクリックします。

ステップ 3 [詳細設定（Advanced）] セクションを展開して、[クライアントアプリケーション（Client Applications）] フィールド内のリンクをクリックします。

ステップ 4 クライアント アプリケーションを 1 つ以上定義します。

オプション	方法
定義済みクライアント アプリケーションを選択する	[ブラウザ（Browser）] と [その他（Other）] セクションを展開して、必要なクライアント アプリケーションのチェックボックスをオンにします。 **ヒント** 可能な場合は [すべてのバージョン（Any Version）] オプションだけを選択します。これによって、複数のオプションを選択するよりもパフォーマンスが向上します。
カスタム クライアント アプリケーションを定義する	[カスタムクライアントアプリケーション（Custom Client Applications）] フィールドに適切な正規表現を入力します。必要に応じて、新規行に追加の正規表現を入力します。 **ヒント** 正規表現の例を参照するには、[クライアントアプリケーションのパターン例（Example Client Applications Patterns）] をクリックします。

ステップ 5 （任意）定義したクライアント アプリケーション**以外**のすべてのクライアント アプリケーションにポリシー メンバーシップを基づかせるには、[選択したクライアント アプリケーション以外のすべてに一致（Match All Except The Selected Client Applications Definitions）] オプション ボタンをクリックします。

ステップ 6 [完了（Done）] をクリックします。

クライアント アプリケーションによるポリシー制御設定の定義

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）] メニューからポリシー タイプを選択します。

ステップ 2 ポリシー テーブルで必要なポリシー名を検索します。

ステップ 3 同じ行の [プロトコルとクライアントアプリケーション（Protocols and Client Applications）] 列のセル リンクをクリックします。

ステップ 4 [プロトコルおよびクライアントアプリケーション設定の編集（Edit Protocols and Client Applications Settings）] ペインのドロップダウン リストから、[カスタム設定を定義（Define Custom Settings）] を選択します（まだ設定していない場合）。

ステップ 5 定義するクライアント アプリケーションに対応する [カスタムクライアントアプリケーション（Custom Client Applications）] フィールドに正規表現を入力します。必要に応じて、新規行に追加の正規表現を入力します。

ヒント 正規表現の例を参照するには、[クライアント アプリケーションのパターン例（Example Client Application Patterns）] をクリックします。

ステップ 6 変更を送信し、保存します。

認証からのクライアント アプリケーションの除外

手順

	コマンドまたはアクション	目的
ステップ 1	認証が不要の識別プロファイルを作成する。	ユーザーおよびクライアント ソフトウェアの分類
ステップ 2	除外するクライアントアプリケーションとして識別プロファイルのメンバーシップを設定する。	ポリシーでのクライアントアプリケーションの使用（26 ページ）
ステップ 3	上記の識別プロファイル以外の他のすべての識別プロファイルを、認証が必要なポリシーのテーブルに配置する。	ポリシーの順序 （7 ページ）

時間範囲およびクォータ

ユーザがアクセスできる時間、ユーザの最大接続時間またはデータ量（「帯域幅クォータ」）を制限するために、アクセスポリシーおよび復号ポリシーに時間範囲、時間クォータ、ボリューム クォータを適用できます。

- ポリシーおよび使用許可コントロールの時間範囲 （28 ページ）
- 時間およびボリューム クォータ （29 ページ）

ポリシーおよび使用許可コントロールの時間範囲

時間範囲によって、ポリシーおよび使用許可コントロールを適用する期間を定義します。

（注） 時間範囲を使用して、ユーザ認証が必要な時間帯を定義することはできません。認証要件は識別プロファイルで定義されますが、時間範囲はサポートされません。

• 時間範囲の作成 （28 ページ）

時間範囲の作成

ステップ 1 [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）] を選択します。

ステップ 2 [時間範囲の追加（Add Time Range）] をクリックします。

ステップ 3 時間範囲の名前を入力します。

ステップ 4 [タイム ゾーン（Time Zone）] のオプションを選択します。

- [アプライアンスのタイムゾーン設定を使用（Use Time Zone Setting from Appliance）] - Secure Web Applianceと同じタイムゾーンを使用します。
- [この時間範囲のタイムゾーンを指定（Specify Time Zone for this Time Range）] - [GMTオフセット（GMT Offset）] として、またはその国の地域、国、および特定のタイムゾーンとして、異なるタイム ゾーンを定義します。

ステップ 5 1 つ以上の [曜日（Day of Week）] チェックボックスをオンにします。

ステップ 6 [時刻（Time of Day）] のオプションを選択します。

- [終日（All Day）] - 24 時間中使用できます。
- [開始（From）] と [終了（To）] - 特定の時間範囲を定義します。HH:MM（24 時間形式）で開始時刻と終了時刻を入力します。

ヒント 各時間範囲は、開始時刻と終了時刻の境界を定義します。たとえば、8:00 ～ 17:00 を入力する場合、8:00:00 ～ 16:59:59 に一致しますが 17:00: 00 には一致しません。深夜は、開始時刻が 00:00、終了時刻が 24:00 として指定する必要があります。

ステップ 7 変更を送信し、保存します。

時間およびボリューム クォータ

クォータを使用すると、与えられたデータ量と時間を使い切るまで、個々のユーザはインターネット リソース（またはインターネット リソース クラス）にアクセスできます。AsyncOS は、HTTP、HTTPS、FTP トラフィックに定義されたクォータを適用します。

ユーザが時間またはボリューム クォータに達すると、AsyncOS は最初に警告を表示し、次にブロック ページを表示します。

時間およびボリューム クォータの使用について、以下の点に注意してください。

- AsyncOS が透過モードで展開され、HTTPS プロキシがディセーブルの場合、ポート 443 ではリッスンされず、要求はドロップされます。これは標準の動作です。AsyncOS が明示モードで展開されている場合は、アクセス ポリシーにクォータを設定できます。

  HTTPS プロキシがイネーブルの場合、要求に対して実行可能なアクションは、パススルー、復号、ドロップ、またはモニタとなります。全般的に、復号ポリシーのクォータはパススルー カテゴリにのみ適用されます。

  パススルーの場合は、トンネル トラフィックのクォータを設定するオプションもあります。アクセス ポリシーで設定したクォータは復号トラフィックに適用されるため、復号ではこのオプションは使用できません。

- URL フィルタリングがディセーブルの場合やキーが使用できない場合、AsyncOS は URL のカテゴリを識別できず、[アクセス ポリシー（Access Policy）] > [URL フィルタリング（URL Filtering）] ページは無効になります。したがって、クォータを設定するには、機能キーが存在し、アクセプタブル ユース ポリシーがイネーブルになっている必要があります。
- Facebook や Gmail など、多くの Web サイトでは自動アップデートが頻繁に起こります。使用していないブラウザ ウィンドウやタブでこのような Web サイトを開いたままにしておくと、ユーザの時間およびボリューム クォータが消費され続けます。
- プロキシを再起動すると、ハイパフォーマンスモードは次のようになります。
  - [有効（Enabled）] - 時間とボリュームのクォータはリセットされません。クォータは、設定された時間に基づいて 24 時間以内に自動的に 1 回リセットされます。
  - [無効（Disabled）] - 時間とボリュームのクォータがリセットされます。クォータは自動的に 24 時間以内にリセットされるため、リセットの影響が残るのは現在時刻から 24 時間のみです。設定の変更またはプロキシプロセスのクラッシュが原因でプロキシが再起動する場合があります。
- decrypt-for-EUN オプションがイネーブルの場合でも、HTTPS に対して EUN ページ（警告とブロックの両方）を表示できません。

（注） 複数のクォータを特定のユーザに適用した場合は、常に最も制限が厳しいクォータが適用されます。

- ボリューム クォータの計算 （30 ページ）

• 時間クォータの計算 （30 ページ）
• 時間、ボリューム、および帯域幅のクォータの定義 （30 ページ）

ボリューム クォータの計算

ボリューム クォータの計算方法は次のとおりです。

- HTTP および復号された HTTPS トラフィック：HTTP 要求と応答の本文がクォータの上限に対してカウントされます。要求ヘッダーと応答ヘッダーは上限に対してカウントされません。
- トンネル トラフィック（トンネル化HTTPS を含む）：AsyncOS は、トンネル化トラフィックをクライアントからサーバに（およびその逆に）移動するだけです。トンネル化トラフィックのデータ量全体が、クォータの上限に対してカウントされます。
- FTP：制御接続トラフィックはカウントされません。アップロードおよびダウンロードされたファイルのサイズは、クォータの上限に対してカウントされます。

（注） クライアント側のトラフィックのみがクォータの上限に対してカウントされます。応答がキャッシュから送信された場合でもクライアント側のトラフィックが生成されるため、キャッシュされたコンテンツも上限に対してカウントされます。

時間クォータの計算

時間クォータの計算方法は次のとおりです。

- HTTP および復号された HTTPS トラフィック：同じ URL カテゴリへの各接続時間（確立から切断まで）に 1 分を加えた時間が、時間クォータの上限に対してカウントされます。1 分以内に同じ URL カテゴリに対して複数の要求が行われた場合、それらは 1 つの連続セッションとしてカウントされ、セッションの最後（つまり、少なくとも 1 分の「沈黙」の後）にのみ 1 分が追加されます。
- トンネル トラフィック（トンネル化 HTTPS を含む）：トンネルの実際の期間（確立から切断まで）が、クォータの上限に対してカウントされます。複数の要求に対する上記の計算は、トンネル化トラフィックにも適用されます。
- FTP：FTP 制御セッションの実際の期間（確立から切断まで）が、クォータの上限に対してカウントされます。複数の要求に対する上記の計算は、FTP トラフィックにも適用されます。

時間、ボリューム、および帯域幅のクォータの定義

始める前に

- [セキュリティサービス（Security Services）] > [使用許可コントロール（Acceptable Use Controls）] に移動し、使用許可コントロールをイネーブルにします。
- 毎日の制限としてクォータを適用しない場合は、時間範囲を定義します。

ステップ 1 [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。

ステップ 2 [クォータの追加（Add Quota）] をクリックします。

ステップ 3 [クォータ名（Quota Name）] に一意のクォータ名を入力します。

ステップ 4 時間とボリュームのクォータを毎日リセットするには、[毎日このクォータをリセットする時刻（Reset this quota daily at）]、および [毎日時間とボリュームのクォータをリセットする時刻（Reset Time and Volume quota daily at）] を選択し、フィールドに 12 時間形式で時刻を入力し、メニューから [AM] または [PM] を選択します。または、[事前定義された時間範囲プロファイルを選択します（Select a predefined time range profile）] を選択します。

（注） リセットクォータオプションを使用しても、設定した帯域幅クォータ値はリセットされません。

ステップ 5 時間クォータを設定するには、[時間クォータTime Quota] チェックボックスをオンにして、[時間（hrs）] メニューから時間数を、[分（mins）] メニューから分数を選択し、0 分（常にブロック）から 23 時間 59 分までの時間数を設定します。

ステップ 6 ボリューム クォータを設定するには、フィールドに数字を入力し、メニューから [KB]（キロバイト）、[MB]（メガバイト）、または [GB]（ギガバイト）を選択します。

ステップ 7 帯域幅クォータを設定するには、フィールドに数値を入力し、メニューから [Kbps]（キロバイト/秒）、または [Mbps]（メガバイト/秒）を選択します。

- ただし、同じアクセスポリシーや復号ポリシーに、URL 帯域幅クォータと全体的な Web アクティビティクォータの両方を設定することはできません。
- 全体的な帯域幅制限または AVC 帯域幅制限が有効になっている場合、またはその逆の場合、帯域幅クォータは設定できません。
- キャッシュされたコンテンツも帯域幅クォータで考慮されます。
- クォータプロファイルの編集中は、CDS ポリシーにマッピングされている既存の時間またはボリュームクォータのプロファイルに帯域幅クォータを追加しないでください。
- 復号化ポリシーで Web アクティビティ全体の帯域幅クォータを使用して URL を調整するには、URL をパススルーに設定する必要があります。
- 未分類の URL の場合、詳細な帯域幅制御を介してスロットルするには、次の設定が必要です。
  - アクセスポリシー：復号化ポリシー内の未分類の URL は、アクセスポリシーおよび全体的な Web アクティビティ帯域幅クォータでそれぞれ [復号化/監視（Decrypt/Monitor）] および [監視（Monitor）] に設定されています。
  - 復号化ポリシー：復号化ポリシーの未分類の URL は、パススルーおよび全体的な Web アクティビティの帯域幅クォータに設定されています。

（注） AsyncOS リリース 15.0 にアップグレードする前に帯域幅クォータが設定されたすべてのクォータプロファイルを削除します。

ステップ 8 [送信（Submit）] をクリックし、次に [変更を確定（Commit Changes）] をクリックして変更を適用します。または、[キャンセル（Cancel）] をクリックして変更を破棄します。

次のタスク

（任意）[セキュリティ サービス（Security Services）] > [エンドユーザ通知（End-User Notification）] に移動し、クォータ用のエンドユーザ通知を設定します。

URL カテゴリによるアクセス制御

対応する Web サイトのカテゴリに基づいて、Web 要求を識別してアクションを実行できます。Secure Web Applianceには、多数の定義済み URL カテゴリ（Web ベースの電子メールなど）が用意されています。

定義済みのカテゴリおよびそれらに関連付けられている Web サイトは、 Secure Web Appliance に搭載されているフィルタリングデータベースで定義されます。これらのデータベースは、Cisco によって自動的に最新の状態に維持されます。指定したホスト名と IP アドレスに対してカスタム URL カテゴリを作成することもできます。

URL カテゴリは、要求を識別するポリシーを除くすべてのポリシーで使用できます。また、要求にアクションを適用するポリシー（アクセス、暗号化 HTTPS 管理、データ セキュリティ）でも使用できます。

カスタム URL カテゴリの作成については、カスタム URL カテゴリの作成および編集 を参照してください。

URL カテゴリによる Web 要求の識別

始める前に

- 使用許可コントロールを有効にします（URL フィルタリング エンジンの設定を参照）。
- （任意）カスタム URL カテゴリを作成します（カスタム URL カテゴリの作成および編集を参照）。

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）] メニューからポリシー タイプ（SaaS 以外）を選択します。

ステップ 2 ポリシー テーブル内のポリシー名をクリックします（または新しいポリシーを追加します）。

ステップ 3 [詳細設定（Advanced）] セクションを展開して、[URLカテゴリ（URL Categories）] フィールド内のリンクをクリックします。

ステップ 4 Web 要求の識別に使用する URL カテゴリに対応する [追加（Add）] 列のセルをクリックします。この操作を、カスタム URL カテゴリと定義済み URL カテゴリのリストに対して実行します。

ステップ 5 [完了（Done）] をクリックします。

ステップ 6 変更を送信し、保存します。

URL カテゴリによる Web 要求へのアクション

始める前に

- 使用許可コントロールを有効にします（URL フィルタリング エンジンの設定を参照）。
- （任意）カスタム URL カテゴリを作成します（カスタム URL カテゴリの作成および編集を参照）。

（注） ポリシー内で基準として URL カテゴリを使用している場合、同じポリシー内にアクションを指定する際には、それらのカテゴリだけを使用できます。そのため、下記のオプションの一部が異なっていたり、使用できないことがあります。

ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] メニューから [アクセス ポリシー（Access Policies）]、[Cisco データ セキュリティ ポリシー（Cisco Data Security Policies）]、または [暗号化 HTTPS 管理（Encrypted HTTPS Management）] のいずれかを選択します。

ステップ 2 ポリシー テーブルで必要なポリシー名を検索します。

ステップ 3 同じ行の [URLフィルタリング（URL Filtering）] 列のセル リンクをクリックします。

ステップ 4 （任意）カスタム URL カテゴリを追加します。

a) [カスタムカテゴリの選択（Select Custom Categories）] をクリックします。

b) このポリシーに含めるカスタム URL カテゴリを選択して、[適用（Apply）] をクリックします。

URL フィルタリング エンジンでクライアント要求と照合するカスタム URL カテゴリを選択します。URL フィルタリング エンジンは、クライアント要求と含まれているカスタム URL カテゴリを比較します。除外されたカスタム URL カテゴリは無視されます。URL フィルタリング エンジンは、定義済みの URL カテゴリよりも前に、含まれているカスタム URL カテゴリとクライアント要求の URL を比較します。

ポリシーに含まれているカスタム URL カテゴリは、[カスタムURLカテゴリのフィルタリング（Custom URL Category Filtering）] セクションに表示されます。

ステップ 5 カスタムおよび定義済みの各 URL カテゴリのアクションを選択します。

（注） 使用可能なアクションは、カスタム カテゴリと定義済みカテゴリとでは異なり、ポリシー タイプによっても異なります。

ステップ 6 [分類されてないURL（Uncategorized URLs）] セクションで、定義済み URL カテゴリにもカスタム URL カテゴリにも該当しない Web サイトへのクライアント要求に対して実行するアクションを選択します。

ステップ 7 変更を送信し、保存します。

リモートユーザー

リモート ユーザーについて

Cisco AnyConnect セキュアモビリティはネットワーク境界をリモートエンドポイントまで拡張し、 Secure Web Applianceにより提供される Web フィルタリングサービスの統合を実現します。

リモート ユーザーおよびモバイル ユーザーは Cisco AnyConnect Secure VPN（仮想プライベート ネットワーク）クライアントを使用して、適応型セキュリティ アプライアンス（ASA）との VPN セッションを確立します。ASA は、IP アドレスとユーザー名によるユーザー識別情報とともに、Web トラフィックを Secure Web Applianceに送信します。 Secure Web Applianceは、トラフィックをスキャンしてアクセプタブル ユース ポリシーを適用し、セキュリティ上の脅威からユーザを保護します。セキュリティ アプライアンスは、安全と判断された、ユーザーが受け入れ可能なすべてのトラフィックを返します。

セキュア モビリティがイネーブルの場合は、ID とポリシーを設定し、ユーザーの場所に応じてユーザーに適用できます。

- **リモートユーザー。**これらのユーザーは、VPN を使用してリモート ロケーションからネットワークに接続されます。Cisco ASA と Cisco AnyConnect クライアントの両方が VPN アクセスに使用されている場合、 Secure Web Applianceはリモート ユーザを自動的に識別します。それ以外の場合は、 Secure Web Applianceの管理者が IP アドレスの範囲を設定して、リモート ユーザを指定する必要があります。
- **ローカル ユーザー。**これらのユーザーは、有線またはワイヤレスでネットワークに接続されます。

Secure Web Applianceを Cisco ASA と統合すると、認証されたユーザ名によりユーザを透過的に識別するように設定して、リモート ユーザのシングル サインオンを実現できます。

リモート ユーザーの ID を設定する方法

タスク	解説場所
1. リモート ユーザーの ID を設定する。	リモート ユーザーの ID の設定 （35 ページ）

タスク	解説場所
2. リモート ユーザーの ID を作成する。	ユーザーおよびクライアント ソフトウェアの分類 **1.** [ユーザーの場所別メンバーの定義（Define Members by User Location）] セクションで、[ローカルユーザーのみ（Local Users Only）] を選択します。 **2.** [認証ごとにメンバを定義（Define Members by Authentication）] セクションで、[Cisco ASA統合を通じてユーザーを透過的に識別する（Identify Users Transparently through Cisco ASA Integration）] を選択します。
3. リモート ユーザーのポリシーを作成する。	ポリシーの作成　（8 ページ）

リモート ユーザーの ID の設定

ステップ 1 [セキュリティサービス（Security Services）]>[AnyConnectセキュアモビリティ（AnyConnect Secure Mobility）] で、[有効（Enable）] をクリックします。

ステップ 2 AnyConnect セキュア モビリティのライセンス契約書の条項を読み、[同意する（Accept）] をクリックします。

ステップ 3 リモート ユーザーの識別方法を設定します。

オプション	説明	この他の手順
[IPアドレス（IP Address）]	リモート デバイスに割り当てられているとアプライアンスが見なす IP アドレスの範囲を指定します。	**1.** [IP 範囲（IP Range）] フィールドに IP アドレスの範囲を入力します。 **2.** ステップ 4 に進みます。

オプション	説明	この他の手順
Cisco ASA 統合（Cisco ASA Integration）	Secure Web Applianceが通信する 1 つ以上の Cisco ASA を指定します。Cisco ASAは IP アドレスとユーザーのマッピングを保持し、その情報を Secure Web Applianceに伝達します。Web プロキシはトランザクションを受信すると、IP アドレスを取得し、IP アドレスとユーザーのマッピングをチェックしてユーザーを特定します。Cisco ASA と統合してユーザーを特定する場合は、リモート ユーザーのシングル サイン オンをイネーブルにできます。	**1.** Cisco ASA のホスト名または IP アドレスを入力します。 **2.** ASA へのアクセスに使用するポート番号を入力します。Cisco ASA のデフォルト ポート番号は 11999 です。 **3.** クラスタ内に複数の Cisco ASA が設定されている場合は、[行の追加（Add Row）] をクリックし、クラスタ内の各 ASA を設定します。 （注） 2 つの Cisco ASA が高可用性に設定されている場合は、アクティブな Cisco ASA の 1 つのホスト名または IP アドレスのみを入力します。 **4.** Cisco ASA のアクセス パスフレーズを入力します。 （注） ここで入力するパスフレーズは、指定した Cisco ASA 用に設定されているアクセス パスフレーズと一致する必要があります。 **5.** （任意）[テスト開始（Start Test）] をクリックして、 Secure Web Applianceが設定されている Cisco ASAに接続できることを確認します。

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

（注） Secure Web Applianceで [ユーザーの場所別メンバーの定義（Define Members by User Location）] オプションを有効にするには、AnyConnectセキュリティモビリティを有効にします（[セキュリティサービス（Security Services）] > [AnyConnect Security Mobility]）。デフォルトでは、このオプションは Cisco Content Security Management Appliance（[Web] > [設定マスター（Configuration Master）] > [識別プロファイル（Identification Profiles）]）で使用できます。[ユーザーの場所別メンバーの定義（Define Members by User Location）] オプションを使用してセキュリティ管理アプライアンスで識別プロファイルを設定し、その設定を AnyConnectセキュリティモビリティが有効になっていない Secure Web Applianceに公開すると、その識別プロファイルは無効になります。

ASA のリモート ユーザー ステータスと統計情報の表示

Secure Web Applianceが ASA と統合されている場合は、以下のコマンドを使用してセキュアモビリティに関連する情報を表示します。

コマンド	説明
`musstatus`	このコマンドにより、以下の情報が表示されます。 • Secure Web Applianceと各 ASA との接続ステータス。 • Secure Web Applianceと各 ASA との接続時間（分単位）。 • 各 ASA からのリモート クライアントの数。 • サービス対象のリモート クライアントの数。これは、 Secure Web Applianceを介してトラフィックの受け渡しを行ったリモート クライアントの数です。 • リモート クライアントの合計数。

ポリシーに関するトラブルシューティング

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。