アクセス制御

この章で説明する内容は、次のとおりです。

ポリシーの適用に対するエンドユーザーの分類

この章で説明する内容は、次のとおりです。

ユーザーおよびクライアント ソフトウェアの分類：概要

識別プロファイルによるユーザーおよびユーザーエージェント（クライアント ソフトウェア）の分類は、以下の目的のために行われます。

- ポリシーの適用に対するトランザクション要求をグループ化します（SaaS を除く）。
- 識別および認証の要件の指定

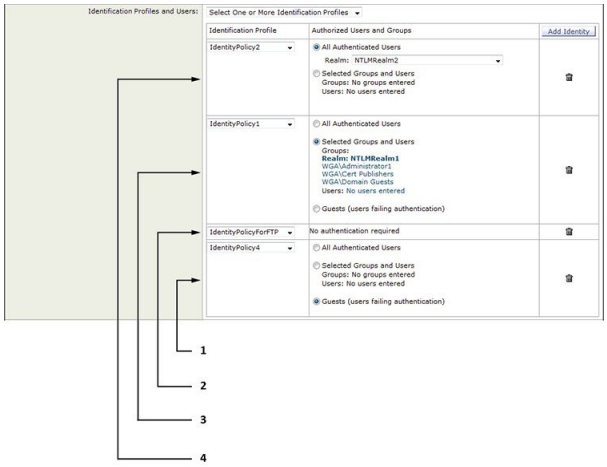
AsyncOS はすべてのトランザクションに識別プロファイルを割り当てます。

- カスタム識別プロファイル：AsyncOSは、そのアイデンティティの条件に基づいてカスタム プロファイルを割り当てます。
- グローバル識別プロファイル：AsyncOS は、カスタム プロファイルの条件を満たさないトランザクションにグローバルプロファイルを割り当てます。デフォルトでは、グローバル プロファイルには認証が必要ありません。

AsyncOS は最初から順番に識別プロファイルを処理します。グローバル プロファイルは最後のプロファイルです。

識別プロファイルには 1 つの条件だけを含めることができます。複数の条件を含む識別プロファイルはすべての条件を満たす必要があります。

1 つのポリシーによって複数の識別プロファイルを要求できます。



1	この識別プロファイルは、認証に失敗したユーザーにゲストアクセスを許可し、それらのユーザーに適用されます。
2	この識別プロファイルには、認証は使用されません。
3	この識別プロファイルで指定されたユーザー グループは、このポリシーで認証されます。
4	この識別プロファイルでは認証シーケンスが使用され、このポリシーがシーケンス内の 1 つのレルムに適用されます。

ユーザーおよびクライアントソフトウェアの分類：ベストプラクティス

- 一般的な識別プロファイルを少数作成して、すべてのユーザーまたは少数の大きなユーザー グループに適用します。より詳細に管理する場合は、プロファイルではなくポリシーを使用します。

- 一意の条件で識別プロファイルを作成します。
- 透過モードで展開する場合は、認証をサポートしていないサイトの識別プロファイルを作成します。「認証のバイパス」を参照してください。

識別プロファイルの条件

これらのトランザクションの特性は、以下の識別プロファイルの定義に使用できます。

オプション	説明
サブネット（Subnet）	クライアントサブネットは、ポリシーのサブネットリストに一致している必要があります。
プロトコル（Protocol）	トランザクションで使用されるプロトコル（HTTP、HTTPS、SOCKS、またはネイティブ FTP）
ポート（Port）	要求のプロキシポートは、識別プロファイルのポートリストに記載されている必要があります（リストに記載がある場合）。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。
ユーザー エージェント（User Agent）	要求を行うユーザーエージェント（クライアントアプリケーション）は、識別プロファイルのユーザーエージェントリストに記載されている必要があります（リストに記載がある場合）。一部のユーザー エージェントは認証を処理できないため、認証を必要としないプロファイルを作成する必要があります。ユーザーエージェントには、アップデータやブラウザ（Internet Explorer、Mozilla Firefox など）などのプログラムが含まれています。
URL カテゴリ（URL Category）	要求 URL の URL カテゴリは、識別プロファイルの URL カテゴリ リストに記載されている必要があります（リストに記載がある場合）。
認証要件（Authentication requirements）	識別プロファイルが認証を必要とする場合は、クライアントの認証クレデンシャルが識別プロファイルの認証要件と一致する必要があります。

ユーザーおよびクライアント ソフトウェアの分類

始める前に

- 認証レルムを作成します。Active Directory 認証レルムの作成（NTLMSSP および基本）またはLDAP 認証レルムの作成を参照してください。
- 識別プロファイルへの変更を確定するときに、エンドユーザーを再認証する必要あるので注意してください。

- クラウド コネクタ モードの場合は、追加の識別プロファイル オプション（マシン ID）を使用できます。ポリシーの適用に対するマシンの識別を参照してください。
- （オプション）認証シーケンスを作成します。認証シーケンスの作成を参照してください
- （オプション）識別プロファイルにモバイル ユーザーを含める場合は、セキュア モビリティをイネーブルにします。
- （オプション）認証サロゲートについて理解しておきます。識別済みユーザーの追跡を参照してください。

手順

ステップ 1 [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）] を選択します。

ステップ 2 [プロファイルの追加（Add Profile）] をクリックしてプロファイルを追加します。

ステップ 3 [識別プロファイルの有効化（Enable Identification Profile）] チェックボックスを使用して、このプロファイルをイネーブルにするか、プロファイルを削除せずにただちにディセーブルにします。

ステップ 4 [名前（Name）] に一意のプロファイル名を割り当てます。

ステップ 5 [説明（Description）] は任意です。

ステップ 6 [上に挿入（Insert Above）] ドロップダウン リストから、このプロファイルを配置するポリシー テーブル内の位置を選択します。

（注）
認証を必要とする最初の識別プロファイルの上に、認証を必要としない識別プロファイルを配置します。

ステップ 7 [ユーザー識別方式（User Identification Method）] セクションで、識別方式を選択して関連パラメータを指定します。表示されるオプションは、選択した方法によって異なります。

a) [ユーザー識別方式（User Identification Method）] ドロップダウン リストから識別方式を選択します。

オプション	説明
認証/識別を免除（Exempt from authentication/identification）	ユーザーは基本的に IP アドレスによって識別されます。追加のパラメータは必要ありません。
認証済みユーザー（Authenticate users）	ユーザーは入力した認証クレデンシャルによって識別されます。
ISE によってユーザーを透過的に識別（Transparently identify users with ISE）	ISE サービスがイネーブルの場合に使用できます（[ネットワーク（Network）] > [Identity Services Engine]）。これらのトランザクションの場合、ユーザー名および関連するセキュリティ グループ タグは Identity Services Engine から取得されます。ISE-PIC 展開では、ISE グループとユーザー情報が受信されます。詳細については、ISE/ISE-PIC サービスを統合するためのタスクを参照してください。

オプション	説明
認証レルムによってユーザーを透過的に識別（Transparently identify users with authentication realm）	このオプションは、1 つ以上の認証レルムが透過的識別をサポートするように定義されている場合に使用できます。

（注）
少なくとも 1 つの識別プロファイルに認証または透過的識別が設定されている場合、ポリシー テーブルでは、ユーザー名、ディレクトリ グループ、セキュリティ グループ タグを使用してポリシー メンバーシップを定義できます。

（注）
Context Directory Agent（CDA）はサポートされなくなりました。同じ機能を実現するために、透過的なユーザー識別のために ISE/ISE-PIC を設定することをお勧めします。

将来のリリースでは CDA を設定するオプションは使用できなくなります。

詳細については、https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/bulletin-c25-2428601.htmlを参照してください。

b) 選択した方式に適したパラメータを指定します。この表に示したすべてのセクションが選択ごとに表示されるわけではありません。

認証レルムまたはゲスト特権へのフォールバック（Fallback to Authentication Realm or Guest Privileges）	ユーザー認証を ISE から取得できない場合： • [ゲスト権限をサポート（Support Guest Privileges）]：トランザクションは続行を許可され、すべての識別プロファイルのゲストユーザーと後続のポリシーを照合します。 • [トランザクションをブロック（Block Transactions）]：ISE で識別できないユーザーにインターネット アクセスを許可しません。 • [ゲスト特権をサポート（Support Guest privileges）]：無効なクレデンシャルにより認証に失敗したユーザーにゲストアクセスを許可する場合、このチェックボックスをオンにします。

認証レルム （Authentication Realm）	

	[レルムまたはシーケンスを選択（Select a Realm or Sequence）]：定義済みの認証レルムまたはシーケンスを選択します。 [スキームの選択（Select a Scheme）]：認証スキームを選択します。 • [Kerberos]：クライアントは Kerberos チケットによって透過的に認証されます。 • [基本（Basic）]：クライアントは常にユーザーにクレデンシャルを要求します。ユーザーがクレデンシャルを入力すると、通常は、入力したクレデンシャルの保存について指定するチェックボックスがブラウザに表示されます。ユーザーがブラウザを開くたびに、クライアントはクレデンシャルの入力を要求するか、または以前に保存したクレデンシャルを再送信します。 クレデンシャルは、保護されていないクリアテキスト（Base64）として送信されます。クライアントと Secure Web Appliance間でのパケットキャプチャにより、ユーザー名やパスフレーズが開示される可能性があります。 • [NTLMSSP]：クライアントは、Windows のログイン クレデンシャルを使用して透過的に認証します。ユーザーはクレデンシャルの入力を要求されません。 ただし、以下の場合、クライアントはユーザーにクレデンシャルの入力を求めます。 • Windows クレデンシャルによる認証が失敗した。 • ブラウザのセキュリティ設定が原因で、クライアントが Secure Web Applianceを信頼しない。 クレデンシャルは、3 ウェイ ハンドシェイク（ダイジェスト形式の認証）により安全に送信されます。パスフレーズが接続を介して送信されることはありません。 • [ヘッダーベースの認証（Header Based Authentication）]：クライアントおよび Secure Web Applianceは、ユーザーを認証済みと見なし、認証またはユーザークレデンシャルの再入力を求めません。X-Authenticated機能は、 Secure Web Applianceがアップストリームデバイスとして動作する場合に機能します。 認証が成功すると、ダウンストリームデバイスは、X-Authenticated-UserおよびX-Authenticated-Groups（オプション）拡張HTTP ヘッダーを介して、ユーザー名とユーザーグループ（オプション）を Secure Web Applianceに送信します。 X-Authenticated-Groups ヘッダーは、アプライアンスで [アクセス ポリシーの照合に X-Authenticate-Groups ヘッダー/カスタム ヘッダー内のグループを使用（Custom Header for matching Access PoliciesUse Groups in X-Authenticate-Groups Header/Custom Header for matching Access Policies）]

	オプション（[ネットワーク認証（Network Authentication）] > [グローバル設定の編集（Edit Global Settings ）] > ）を設定している場合にのみ考慮されます。 （注） X-Authenticated ヘッダーは、アクセス ポリシーまたはルーティング ポリシーにのみ適用できます。ただし、[ヘッダー ベースの認証（Header Based Authentication）] が有効になっている識別プロファイルの復号ポリシーへの関連付けは照合されません。 • [ゲスト特権をサポート（Support Guest privileges）]：無効なクレデンシャルにより認証に失敗したユーザーにゲストアクセスを許可する場合、このチェックボックスをオンにします。
グループ認証のレルム（Realm for Group Authentication）	• [レルムまたはシーケンスを選択（Select a Realm or Sequence）]：定義済みの認証レルムまたはシーケンスを選択します。

認証サロゲート（Authentication Surrogates）	認証の成功後にトランザクションをユーザーに関連付ける方法を指定します（オプションは Web プロキシの展開モードにより異なります）。 • [IPアドレス（IP Address）]：Web プロキシは、特定の IP アドレスの認証済みユーザーを追跡します。透過的ユーザー識別の場合は、このオプションを選択します。 • [永続的なクッキー（Persistent Cookie）]：Web プロキシは、アプリケーションごとに各ユーザー用に永続的クッキーを生成することにより、特定のアプリケーション上の認証済みユーザーを追跡します。アプリケーションを終了してもクッキーは削除されません。 • [セッションクッキー（Session Cookie）]：Web プロキシは、アプリケーションごとに各ドメインの各ユーザー用に永続的クッキーを生成することにより、特定のアプリケーション上の認証済みユーザーを追跡します。（ただし、ユーザーが同じアプリケーションから同じドメインに対して異なるクレデンシャルを指定した場合、クッキーは上書きされます）。アプリケーションを終了するとクッキーは削除されます。 • [サロゲートなし（No Surrogate）]：Web プロキシは、サロゲートを使用してクレデンシャルをキャッシュせず、新しい TCP 接続ごとに認証済みユーザーを追跡します。このオプションを選択すると、Web インターフェイスは適用されくなったその他の設定をディセーブルにします。このオプションは、明示的な転送モードに設定し、[ネットワーク（Network）] > [認証（Authentication）] ページでクレデンシャルの暗号化をディセーブルにしたときにのみ使用できます。 • [明示的フォワード要求に同じサロゲート設定を適用（Apply same surrogate settings to explicit forward requests）]：透過的要求に使用するサロゲートを明示的要求に適用する場合にオンにします（クレデンシャルの暗号化が自動的にイネーブルになります。）このオプションは、Web プロキシがトランスペアレント モードで展開されている場合にのみ表示されます。 （注） • [グローバル認証設定（Global Authentication Settings）] で、すべての要求に対する認証サロゲートのタイムアウト値を定義できます。 • 異なる認証サロゲート（IP アドレス、永続的 Cookie、セッション Cookie など）を使用するように識別プロファイルを設定した場合、アクセスは、他のサロゲートと識別プロファイルが一致しても、IP アドレスサロゲートを使用して認証されます。

ステップ 8 [メンバーシップの定義（Membership Definition）] セクションで、選択した識別方式に適したメンバーシップ パラメータを指定します。以下の表に示すオプションは、すべてのユーザー識別方式で使用できるわけではありません。

メンバーシップの定義（**Membership Definition**）	
ユーザーの場所別メンバーの定義（Define Members by User Location）	この識別プロファイルの適用対象として、**[ローカルユーザーのみ（Local Users Only）]**、**[リモートユーザーのみ（Remote Users Only）]**、または [両方（Both）] を設定します。ここでの選択は、この識別プロファイルで使用可能な認証設定に影響します。
サブネット別メンバの定義（Define Members by Subnet）	この識別プロファイルを適用するアドレスを入力します。IP アドレス、CIDR ブロック、およびサブネットを入力できます。 **（注）** 何も入力しない場合は、すべての IP アドレスにこの識別プロファイルが適用されます。
プロトコル別メンバの定義（Define Members by Protocol）	この識別プロファイルを適用するプロトコルを選択します。適用するすべてのプロトコルを選択してください。 • [HTTP/HTTPS]：基礎のプロトコルとして HTTP または HTTPS を使用するすべての要求に適用されます。これには、FTP over HTTP、および HTTP CONNECT を使用してトンネリングされるその他のプロトコルも含まれます。 • [ネイティブFTP（Native FTP）]：ネイティブ FTP 要求にのみ適用されます。 • [SOCKS]：SOCKS ポリシーにのみ適用されます。

マシン ID によるメンバーの定義（Define Members by Machine ID）	• [このポリシーではマシンIDを使用しないでください（Do Not Use Machine ID in This Policy）]：ユーザーはマシン ID によって識別されません。 • [マシンIDをベースにしたユーザー認証ポリシーの定義（Define User Authentication Policy Based on Machine ID）]：ユーザーは基本的にマシン ID によって識別されます。 [マシングループ（Machine Groups）] 領域をクリックして、[認証済みマシン グループ（Authorized Machine Groups）] ページを表示します。 追加する各グループごとに、[ディレクトリ検索（Directory Search）] フィールドに追加するグループの名前を入力し、[追加（Add）] をクリックします。リストからグループを削除するには、グループを選択して [削除（Remove）] をクリックします。 [完了（Done）] をクリックして前のページに戻ります。 [マシンID（Machine IDs）] 領域をクリックして、[認証済みマシン（Authorized Machines）] ページを表示します。 [認証済みマシン（Authorized Machines）] フィールドで、ポリシーに関連付けるマシン ID を入力し、[完了（Done）] をクリックします。 **（注）** マシン ID による認証はコネクタ モードのみでサポートされ、Active Directory が必要です。

詳細設定	このセクションを展開して、追加のメンバーシップ要件を定義します。 • [プロキシポート（Proxy Ports）]：Web プロキシへのアクセスに使用する 1 つ以上のプロキシ ポートを指定します。ポート番号をカンマで区切って入力します。明示的な転送接続の場合、プロキシ ポートはブラウザで設定されます。 透過接続の場合は、宛先ポートと同じです。 ポート別の ID の定義は、アプライアンスが明示的な転送モードで展開されている場合、またはクライアントがアプライアンスに明示的に要求を転送する場合に最もよく機能します。クライアント要求が透過的にアプライアンスにリダイレクトされる場合は、ポート別の ID の定義によって一部の要求が拒否されることがあります。 • [URLカテゴリ（URL Categories）]：ユーザー定義または定義済みの URL カテゴリを選択します。デフォルトでは、両方のメンバーシップが除外されます。つまり、[追加（Add）]列で選択されていない限り、Web プロキシはすべてのカテゴリを無視します。 URL カテゴリによってメンバーシップを定義する必要がある場合、そのカテゴリに対する認証要求から除外する必要のあるときは ID グループにのみ定義します。 • [ユーザー エージェント（User Agents）]：クライアント要求で見つかったユーザー エージェントごとにポリシー グループ メンバーシップを定義します。一般的に定義されているエージェントを選択するか、正規表現を使用して独自のブラウザを定義できます。 また、これらのユーザー エージェントの指定を含めるか除外するかも指定します。つまり、メンバーシップの定義に選択したユーザー エージェントのみを含めるか、選択したユーザー エージェントを明確に除外するかどうかを指定します。

ステップ 9 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

次のタスク

- エンドユーザー クレデンシャルの取得の概要
- ポリシー タスクによる Web 要求の管理：概要 （100 ページ）

ID の有効化/無効化

Before you begin

- 識別プロファイルをディセーブルにすると、関連するポリシーからその識別プロファイルが削除されるので注意してください。
- 識別プロファイルを再度イネーブルにしても、その識別プロファイルはポリシーに再び関連付けられません。

Procedure

ステップ 1 [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）] を選択します。

ステップ 2 識別プロファイル テーブルのプロファイルをクリックして、そのプロファイルの [識別プロファイル（Identification Profile）] ページを開きます。

ステップ 3 [クライアント/ユーザー識別プロファイルの設定（Client/User Identification Profile Settings）] の真下にある [識別プロファイルの有効化（Enable dentification IProfile）] をオンまたはオフにします。

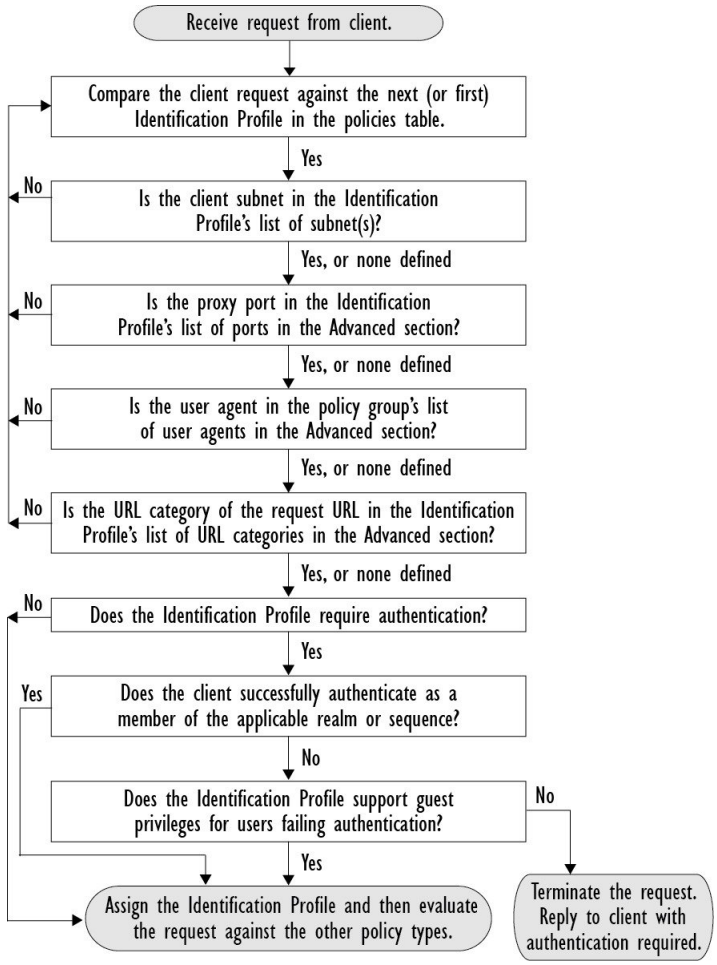
ステップ 4 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

識別プロファイルと認証

次の図に、識別プロファイルが次を使用するように設定されているときに、Webプロキシがクライアント要求を識別プロファイルに対して評価する方法を示します。

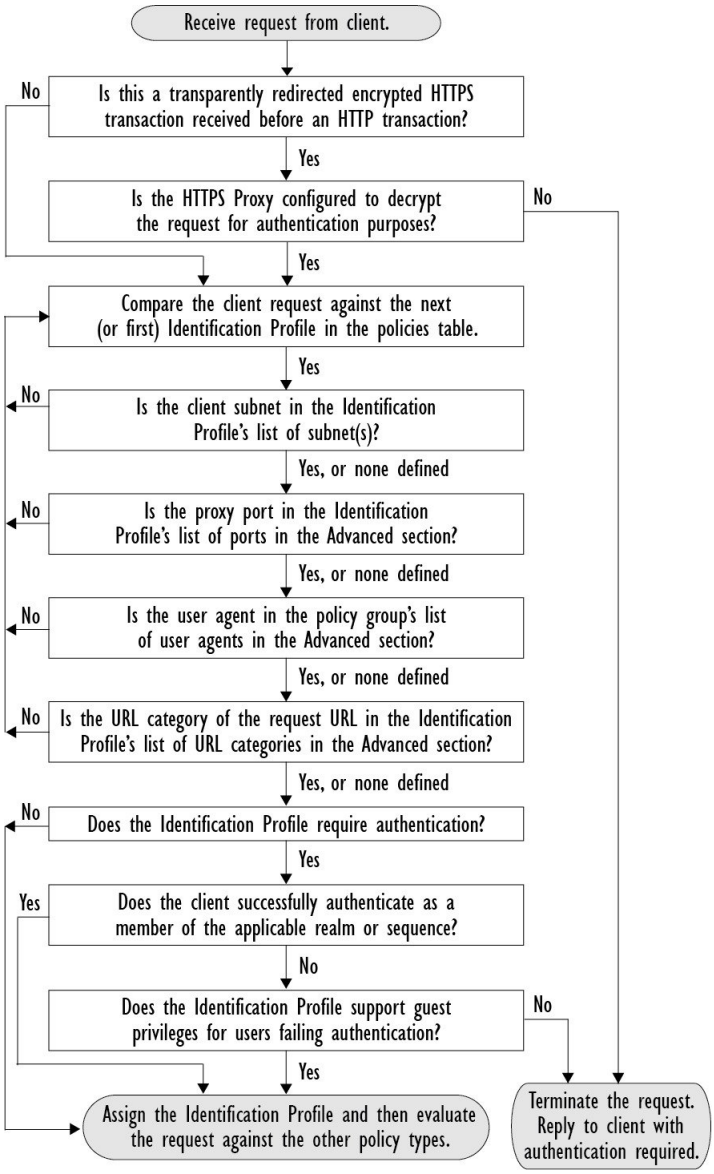
- 認証サロゲートなし
- 認証サロゲートとしての IP アドレス
- 透過的要求を使用する認証サロゲートとしてのクッキー
- 明示的要求を使用する認証サロゲートとしてのクッキー（クレデンシャルの暗号化がイネーブルになっている場合）

Figure 1: 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



次の図に、識別プロファイルが認証サロゲートとして Cookie を使用し、クレデンシャルの暗号化を有効にして、要求が明示的に転送されるように設定されているときに、Web プロキシがクライアント要求を識別プロファイルに対して評価する方法を示します。

Figure 2: 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



識別プロファイルのトラブルシューティング

識別プロファイルでのサロゲートタイプのトラブルシューティング

Cisco Web セキュリティアプライアンスが IP アドレスと Cookie ベースの認証サロゲートの両方を使用するように設定されていて、エンドユーザーからのアクセスが両方のアイデンティティに一致する場合、IPアドレスはCookieベースの認証サロゲートをオーバーライドします。

共有および個別コンピューターの両方を使用するネットワークでは、IPアドレスとサブネットに基づいて2つの異なる識別プロファイルを作成することをお勧めします。これにより、IPまたは Cookie 認証サロゲートが使用されるかどうかが決まります。

ポリシーの適用に対する URL の分類

この章で説明する内容は、次のとおりです。

URL トランザクションの分類の概要

グループ ポリシーを使用して、疑わしいコンテンツが含まれている Web サイトへのアクセスを制御するセキュリティ ポリシーを作成できます。ブロック、許可、または復号されるサイトは、各グループ ポリシーのカテゴリ ブロッキングを設定する際に選択するカテゴリに応じて決まります。URL カテゴリに基づいてユーザー アクセスを制御するには、Cisco Web Usage Controls を有効にする必要があります。これは、ドメインプレフィックスとキーワード分析を使用して URL を分類するマルチレイヤ URL フィルタリング エンジンです。

以下のタスクを実行するときに、URL カテゴリを使用できます。

オプション	方法
ポリシー グループ メンバーシップの定義	URL と URL カテゴリの照合, on page 19
HTTP、HTTPS、および FTP 要求へのアクセスの制御	URL カテゴリによるトランザクションのフィルタリング, on page 29
特定のホスト名と IP アドレスを指定する、ユーザー定義のカスタム URL カテゴリの作成	カスタム URL カテゴリの作成および編集, on page 41

失敗した URL トランザクションの分類

動的コンテンツ分析エンジンは、アクセス ポリシーのみを使用して Web サイトへのアクセスを制御する場合に URL を分類します。ポリシー グループ メンバーシップを判別する場合や、復号ポリシーまたはシスコ データ セキュリティ ポリシーを使用して Web サイトへのアクセスを制御する場合は、URL を分類しません。その理由は、このエンジンが宛先サーバーからの応答コンテンツを分析することによって機能するからです。そのため、サーバーから応答をダウンロードする前の要求時に行う必要がある決定では、このエンジンを使用できません。

未分類 URL の Web レピュテーション スコアが WBRS の許可範囲内にある場合、AsyncOS は動的コンテンツ分析を行わずに要求を許可します。

動的コンテンツ分析エンジンは URL を分類した後、カテゴリの評価と URL を一時キャッシュに格納します。これによって、以降のトランザクションで以前の応答のスキャンを利用することができ、応答時ではなく要求時にトランザクションを分類できます。

動的コンテンツ分析エンジンをイネーブルにすると、トランザクションのパフォーマンスに影響することがあります。ただし、ほとんどのトランザクションは Cisco Web 利用の制御 URL カテゴリ データベースを使用して分類されるので、動的コンテンツ分析エンジンは通常、トランザクションのごく一部に対してのみ呼び出されます。

動的コンテンツ分析エンジンのイネーブル化

Note

- ダイナミック コンテンツ分析（DCA）はデフォルトで無効になり、AsyncOS 15.2.x 以降のバージョンではサポートされなくなりました。DCA の機能は、Talos Web フィルタリング サービスに置き換えられます。Talos Web フィルタリング サービスは、年間 50 億を超える悪意のあるドメインと URL をブロックし、新しいドメインと URL の検出と分類の速度と精度を向上させます。これにより、SWA アプライアンスに対する Talos の頻繁な更新とともに DCA の必要性をなくし、未分類の Web サイト情報を最小限に抑えることができ、WSA ユーザーによりパフォーマンスの高いソリューションを提供します。
- 定義済みの URL カテゴリを使用して、アクセス ポリシー（またはアクセス ポリシーで使用される ID）でポリシー メンバーシップを定義できます。また、アクセス ポリシーにより同じ URL カテゴリに対してアクションを実行できます。ID とアクセス ポリシー グループ メンバーシップを判別するときに、要求の URL を未分類にすることも可能です。ただし、サーバーから応答を受信した後で動的コンテンツ分析エンジンで分類する必要があります。Cisco Web Usage Controls は動的コンテンツ分析によるカテゴリ評価を無視し、残りのトランザクションに対する URL の評価は「未分類」のままになります。ただし、それ以降のトランザクションは引き続き、新しいカテゴリ評価を利用できます。

Procedure

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 Cisco Web Usage Controls を有効にします。

ステップ 3 動的コンテンツ分析エンジンを**クリック**してイネーブルにします。

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）]）。

未分類の URL

未分類の URL とは、定義済みの URL カテゴリにも付属のカスタム URL カテゴリにも一致しない URL です。

Note ポリシー グループのメンバーシップを判別するときに、カスタム URL カテゴリは、ポリシー グループのメンバーシップに対して選択されている場合にのみグループに含まれていると見なされます。

一致しないカテゴリと見なされたトランザクションはすべて、[レポート（Reporting）] > [URL カテゴリ（URL Categories）] ページで [分類されてない URL（Uncategorized URL）] として報告されます。未分類 URL の多くは、内部ネットワーク内の Web サイトへの要求から生じま

す。カスタム URL カテゴリを使用して内部 URL をグループ化し、内部 Web サイトに対するすべての要求を許可することを推奨します。これによって、[分類されてないURL（Uncategorized URL）] として報告される Web トランザクションの数が減少し、内部トランザクションが [バイパスされたURLフィルタリング（URL Filtering Bypassed）] 統計情報の一部として報告されるようになります。

関連項目

- フィルタリングされない未分類のデータについて, on page 56。
- カスタム URL カテゴリの作成および編集, on page 41。

URL と URL カテゴリの照合

URL フィルタリング エンジンはクライアント要求の URL と URL カテゴリを照合するときに、まず、ポリシー グループに含まれているカスタム URL カテゴリと照合して URL を評価します。要求の URL がグループに含まれているカスタム カテゴリと一致しない場合、URL フィルタリング エンジンはその URL を定義済みの URL カテゴリと比較します。URL がカスタム URL カテゴリにも定義済みの URL カテゴリにも一致しない場合、要求は未分類になります。

Note ポリシー グループのメンバーシップを判別するときに、カスタム URL カテゴリは、ポリシー グループのメンバーシップに対して選択されている場合にのみグループに含まれていると見なされます。

特定の Web サイトが割り当てられているカテゴリを確認するには、未分類の URL と誤って分類された URL の報告, on page 19の URL に移動します。

関連項目

- 未分類の URL, on page 18。

未分類の URL と誤って分類された URL の報告

未分類の URL および誤分類された URL をシスコに報告できます。シスコでは、複数の URL を同時に送信できる URL 送信ツールをシスコの Web サイトで提供しています。

- https://talosintelligence.com/tickets
  - 送信された URL のステータスを確認するには、このページの [送信された URL のステータス（Status on Submitted URLs）] タブをクリックします。
  - また、URL 送信ツールを使用して、URL に割り当てられている URL カテゴリを検索できます。
- https://www.talosintelligence.com/reputation_center/support
  - クレームを送信するには、シスコアカウントにログインする必要があります。URL、IP、またはドメインに関するクレームを送信できます。

- Web レピュテーション情報を検索するには、[レピュテーションセンター検索（Reputation Center Search）] ボックスを使用します。

URL カテゴリ データベース

URLが分類されるカテゴリは、フィルタリングカテゴリデータベースによって決定されます。Secure Web Applianceは各 URL フィルタリング エンジンごとに情報を収集し、個別のデータベースに保持します。フィルタリングカテゴリデータベースは、Ciscoアップデートサーバーから定期的にアップデートを受信します。

URL カテゴリ データベースには、シスコ内部およびインターネットのさまざまなデータ要素とデータ ソースが格納されています。要素の 1 つであるオープン ディレクトリ プロジェクトからの情報は、時々検討されて当初のものから大幅に変更されます。

特定の Web サイトが割り当てられているカテゴリを確認するには、未分類の URL と誤って分類された URL の報告, on page 19の URL に移動します。

関連項目

- 手動による URL カテゴリ セットの更新 , on page 28

URL フィルタリング エンジンの設定

デフォルトでは、Cisco Web 利用の制御 URL フィルタリング エンジンはシステム セットアップ ウィザードでイネーブルになります。

Procedure

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 [グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3 [使用許可コントロールを有効にする（Enable Acceptable Use Controls）] プロパティがイネーブルになっていることを確認します。

ステップ 4 次の Cisco Web Usage Controls のいずれかを選択します。

a. アプリケーション制御を有効にする

Note
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。

- [アプリケーションの表示およびコントロールを有効にする（Enable Application Visibility and Control (AVC)） を有効にする：300 以上のアプリケーションがあります
- [アプリケーションの検出およびコントロールを有効にする（Application Discovery and Control (ADC)）]： 3000 以上のアプリケーションがあります

b. ダイナミックコンテンツ分析エンジンを有効にする

c. 複数の URL カテゴリの有効化

Note
複数の URL カテゴリ機能は、アクセスポリシーのみに適用されます。複数の URL カテゴリ機能を復号ポリシーおよび識別プロファイルに適用することはできません。

ステップ 5 URL フィルタリングエンジンを利用できない場合に、Web プロキシが使用すべきデフォルトのアクション（[モニター（Monitor）] または [ブロック（Block）]）を選択します。デフォルトは [モニター（Monitor）] です。

ステップ 6 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

URL カテゴリ セットの更新の管理

事前定義された URL カテゴリのセットは、新しい Web のトレンドと進化する使用パターンに合わせて時々更新されます。URL カテゴリ セットの更新は、新規 URL の追加や誤分類 URL の再マッピングによる変更とは異なります。カテゴリ セットの更新によって既存のポリシーの設定が変更されることがあるため、対処が必要になります。URL カテゴリ セットの更新は製品のリリース間で行われ、AsyncOS のアップグレードは必要ありません。

これらに関する情報は、以下の URL から入手できます：
http://www.cisco.com/en/US/products/ps10164/prod_release_notes_list.html。

以下のアクションを実行します。

実行する時期	方法
更新が実行される前 （初期設定の一部としてこれらのタスクを実行します）	URL カテゴリ セットの更新による影響について , on page 21 URL カテゴリ セットの更新の制御 , on page 27 新規および変更されたカテゴリのデフォルト設定 , on page 28 カテゴリおよびポリシーの変更に関するアラートの受信 , on page 29
更新が実行された後	URL カテゴリ セットの更新に関するアラートへの応答 , on page 29

URL カテゴリ セットの更新による影響について

URL カテゴリ セットの更新は、既存のアクセス ポリシー、復号ポリシー、シスコ データ セキュリティ ポリシー、および ID に以下のような影響を与えます。

- URL カテゴリ セットの変更によるポリシー グループ メンバーシップへの影響 , on page 22
- URL カテゴリ セットの更新によるポリシーのフィルタリング アクションへの影響 , on page 22

URL カテゴリ セットの変更によるポリシー グループ メンバーシップへの影響

このセクションの内容は、URL カテゴリによって定義できるメンバーシップを含んでいるすべてのポリシー タイプ、および ID に該当します。ポリシー グループ メンバーシップが URL カテゴリによって定義されている場合、カテゴリ セットへの変更は以下のような影響を及ぼす可能性があります。

- メンバーシップの唯一の条件であったカテゴリが削除された場合、ポリシーまたは ID はディセーブルになります。

ポリシーのメンバーシップを定義していた URL カテゴリが変更され、それに伴って ACL リストも変更された場合は、Web プロキシが再起動します。

URL カテゴリ セットの更新によるポリシーのフィルタリング アクションへの影響

URL カテゴリ セットの更新により、ポリシーの動作が以下のように変更される可能性があります。

変更内容	ポリシーおよび ID への影響
新しいカテゴリが追加された場合	新しい URL カテゴリでは、[ポリシー設定（Policy Configuartion）] ページの [更新カテゴリのデフォルトアクション（Default Action for Update Categories）] オプションから次のいずれかのアクションが選択されます。 • [最小の制限（Least Restrictive）] • [最大の制限（Most Restrictive）] アクションは、新しいカテゴリに対してデフォルトで設定されます。[アクセスポリシー（Access Policies）] および [シスコデータセキュリティポリシー（Cisco Data Security Policies）] で、次の手順を実行します。 • [最大の制限（Most Restictive）] は [ブロック（Block）] • [最小の制限（Lease Restictive）] は [モニタ（Monitor）] Web トラフィックタップ（WTT）ポリシー： • [最大の制限（Most Restictive）] は [タップ（Tap）] • [最小の制限（Least Restictive）] は [タップなし（No Tap）] [復号ポリシー（Decryption Policies）]： • [最大の制限（Most Restictive）] は [ブロック（Block）] • [最小の制限（Least Restictive）] は [パススルー（Pass Through）]

変更内容	ポリシーおよび ID への影響
カテゴリが削除された場合	削除されたカテゴリに関連付けられていたアクションは削除されます。 ポリシーが削除されたカテゴリにのみ依存していた場合、そのポリシーはディセーブルになります。 ポリシーが依存している ID が削除されたカテゴリにのみ依存していた場合、そのポリシーはディセーブルになります。
カテゴリの名前が変更された場合	既存のポリシーの動作に対する変更はありません。
カテゴリが分割された場合	1 つのカテゴリが複数の新規カテゴリとなることがあります。新しいカテゴリアクションは、[更新カテゴリのデフォルトアクション（Default Action for Update Categories）] から選択されます。

変更内容	ポリシーおよび ID への影響
複数の既存のカテゴリがマージされた場合	

変更内容	ポリシーおよび ID への影響
	ポリシーの元のカテゴリすべてに同じアクションが割り当てられていた場合、マージされたカテゴリには元のカテゴリと同じアクションが含まれます。元のカテゴリすべてが [グローバル設定を使用（Use Global Setting）] に設定されていた場合、マージされたカテゴリも [グローバル設定を使用（Use Global Setting）] に設定されます。 ポリシーの元のカテゴリにさまざまなアクションが割り当てられていた場合、マージされたカテゴリに割り当てられるアクションは、そのポリシーの [分類されてないURL（Uncategorized URLs）] の設定によって決まります。 • [分類されてないURL（Uncategorized URLs）] が [ブロック（Block）]（または [グローバル設定を使用（Use Global Settings）]（グローバル設定が [ブロック（Block）] のとき））に設定されている場合は、元のカテゴリにおいて最も制限が厳しいアクションがマージされたカテゴリに適用されます。 • [分類されてないURL（Uncategorized URLs）] が [ブロック（Block）] 以外（または [グローバル設定を使用（Use Global Settings）] 以外（グローバル設定が [ブロック（Block）] 以外のとき））に設定されている場合は、元のカテゴリにおいて最も制限が緩いアクションがマージされたカテゴリに適用されます。 この場合、以前ブロックされていたサイトにユーザがアクセスできるようになる可能性があります。 ポリシー メンバーシップが URL カテゴリによって定義されており、マージに関連する一部のカテゴリ、または [分類されてないURL（Uncategorized URLs）] のアクションがポリシー メンバーシップの定義に含まれていない場合は、欠落している項目に対してグローバルポリシーの値が使用されます。 制限の厳しさの順位は以下のとおりです（すべてのアクションをすべてのポリシー タイプで使用できるわけではありません）。 • ブロック（Block） • ドロップ（Drop） • 復号（Decrypt） • 警告（Warn） • 時間ベース（Time-based） • モニター（Monitor） • パススルー（Pass Through） **Note**

変更内容	ポリシーおよびIDへの影響
	マージされたカテゴリに基づいている時間ベースのポリシーでは、元のカテゴリのいずれかに関連付けられているアクションが選択されます。（時間ベースのポリシーでは、制限が最も厳しいまたは最も緩いアクションが明確ではないことがあります）。

関連項目

- マージされたカテゴリ：例 , on page 26。

マージされたカテゴリ：例

以下の例は、ポリシーの [URLフィルタリング（URL Filtering）] ページの設定に基づいてマージされたカテゴリを示しています。

元のカテゴリ1	元のカテゴリ2	分類されてないURL	マージされたカテゴリ
モニター（Monitor）	モニター（Monitor）	(N/A)	モニター（Monitor）
ブロック（Block）	ブロック（Block）	(N/A)	ブロック（Block）
グローバル設定を使用（Use Global Settings）	グローバル設定を使用（Use Global Settings）	(N/A)	グローバル設定を使用（Use Global Settings）
警告（Warn）	ブロック（Block）	モニター（Monitor） 元のカテゴリにおいて最も制限が緩いアクションを使用。	警告（Warn）
モニター（Monitor）	• ブロック（Block）または • グローバル設定を使用（Use Global Settings）（グローバルが [ブロック（Block）] に設定されている場合）	• ブロック（Block）または • グローバル設定を使用（Use Global Settings）（グローバル設定が [ブロック（Block）] の場合） 元のカテゴリにおいて最も制限が厳しいアクションを使用。	ブロック（Block）

元のカテゴリ 1	元のカテゴリ 2	分類されてない URL	マージされたカテゴリ
ブロック（Block）	• モニタ（Monitor）または • グローバル設定を使用（Use Global Settings）（グローバルが [モニタ（Monitor）] に設定されている場合）	• モニタ（Monitor）または • グローバル設定を使用（Use Global Settings）（グローバル設定が [モニタ（Monitor）] の場合） 元のカテゴリにおいて最も制限が緩いアクションを使用。	モニター（Monitor）
メンバーシップが URL カテゴリによって定義されているポリシーの場合： モニター（Monitor）	カテゴリのアクションがポリシーで指定されておらず、カテゴリのグローバルポリシーの値が [ブロック（Block）]。	未分類の URL のアクションがポリシーで指定されておらず、未分類の URL のグローバル ポリシーの値が [モニタ（Monitor）]。	モニター（Monitor）

URL カテゴリ セットの更新の制御

デフォルトでは、URL カテゴリ セットの更新は自動的に行われます。ただし、これらの更新によって既存のポリシー設定が変更される可能性があるため、すべての自動更新をディセーブルにすることを推奨します。

オプション	方法
更新をディセーブルにした場合は、[システム管理（System Administration）]>[アップグレードとアップデートの設定（Upgrade and Update Settings）] ページの [アップデートサーバ（リスト）（Update Servers (list)）] セクションで、記載されているすべてのサービスを手動で更新する必要があります。	手動による URL カテゴリ セットの更新 , on page 28 および セキュリティ サービスのコンポーネントの手動による更新
すべての自動更新をディセーブルにします	アップグレードおよびサービス アップデートの設定。

Note CLI を使用する場合は、更新間隔をゼロ（0）に設定して更新をディセーブルにします。

手動による URL カテゴリ セットの更新

Note

- 進行中の更新を中断しないでください。
- 自動更新をディセーブルにした場合は、必要に応じて手動で URL カテゴリ セットを更新できます。

Procedure

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 アップデートが利用可能かどうかを確認します。

[使用許可コントロールエンジンの更新（Acceptable Use Controls Engine Updates）] テーブルの [Cisco Web利用の制御 - Webカテゴリのカテゴリリスト（Cisco Web Usage Controls - Web Categorization Categories List）] を参照してください。

ステップ 3 更新するには、[今すぐ更新（Update Now）] をクリックします。

新規および変更されたカテゴリのデフォルト設定

URL カテゴリ セットの更新によって、既存のポリシーの動作が変更されることがあります。URL カテゴリ セットが更新された場合に対応できるように、ポリシーを設定する際は、特定の変更に対してデフォルトの設定を指定しておく必要があります。新しいカテゴリが追加された場合や既存のカテゴリが新しいカテゴリにマージされた場合、それらのカテゴリに対する各ポリシーのデフォルト アクションは、そのポリシーの **[更新カテゴリのデフォルトアクション（Default Action for Update Categories）]** の設定に影響されます。

既存の設定の確認または変更の実行

Procedure

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）] を選択します。

ステップ 2 各アクセス ポリシー、復号ポリシー、シスコ データ セキュリティ ポリシーに対して、[URL フィルタリング（URL Filtering）] リンクをクリックします。

ステップ 3 [分類されてないURL（Uncategorized URLs）] に対して選択されている設定を確認します。

What to do next

関連項目

- URL カテゴリ セットの更新によるポリシーのフィルタリング アクションへの影響 , on page 22。

カテゴリおよびポリシーの変更に関するアラートの受信

カテゴリ セットの更新によって、以下の 2 種類のアラートがトリガーされます。

- カテゴリの変更についてのアラート
- カテゴリ セットの変更によって変更またはディセーブル化されたポリシーに関するアラート

Procedure

ステップ 1 [システム管理（System Administration）] > [アラート（Alerts）] を選択します。

ステップ 2 [受信者の追加（Add Recipient）] をクリックして電子メール アドレス（または、複数の電子メール アドレス）を追加します。

ステップ 3 受信するアラートの [アラートタイプ（Alert Types）] と [アラートの重大度（Alert Severities）] を決定します。

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）]）。

URL カテゴリ セットの更新に関するアラートへの応答

カテゴリ セットの変更に関するアラートを受信した場合は、以下を実行する必要があります。

- カテゴリがマージ、追加、削除された後、ポリシーと ID が引き続きポリシーの目的に合致していることを確認します。さらに
- 新しいカテゴリや分割によるカテゴリの細分化を活用できるように、ポリシーと ID を変更することを検討します。

関連項目

- URL カテゴリ セットの更新による影響について , on page 21

URL カテゴリによるトランザクションのフィルタリング

URL フィルタリング エンジンを使用して、アクセス ポリシー、復号ポリシー、データ セキュリティ ポリシーのトランザクションをフィルタリングできます。ポリシー グループの URL カテゴリを設定する際は、カスタム URL カテゴリ（定義されている場合）と定義済み URL カテゴリのアクションを設定できます。

設定できる URL フィルタリング アクションは、ポリシー グループのタイプに応じて異なります。

オプション	方法
アクセス ポリシー（Access Policies）	アクセス ポリシー グループの URL フィルタの設定, on page 30
復号ポリシー（Decryption Policies）	復号ポリシー グループの URL フィルタの設定, on page 34
シスコ データ セキュリティ ポリシー（Cisco Data Security Policies）	データ セキュリティ ポリシー グループの URL フィルタの設定, on page 35

関連項目

- アクセス ポリシーでのトラフィックのリダイレクト, on page 53
- ユーザーへの警告と続行の許可, on page 54
- カスタム URL カテゴリの作成および編集, on page 41
- URL カテゴリ セットの更新によるポリシーのフィルタリング アクションへの影響, on page 22

アクセス ポリシー グループの URL フィルタの設定

ユーザー定義のアクセス ポリシー グループおよびグローバル ポリシー グループに対して URL フィルタリングを設定できます。

Procedure

ステップ 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。

ステップ 2 ポリシー テーブルで、編集するポリシー グループの [URL フィルタ（URL Filtering）] 列にあるリンクをクリックします。

ステップ 3 （任意）[カスタムURLカテゴリのフィルタリング（Custom URL Category Filtering）] セクションで、このポリシーのアクションの実行対象となるカスタム URL カテゴリを追加できます。

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 4 [カスタム URL カテゴリのフィルタリング（Custom URL Category Filtering）] セクションで、含まれている各カスタム URL カテゴリのアクションを選択します。

アクション	説明
グローバル設定を使用（Use Global Settings）	グローバル ポリシー グループで設定されているこのカテゴリ用のアクションを使用します。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。 ユーザー定義のポリシー グループにのみ適用されます。 **Note** カスタム URL カテゴリがグローバル アクセス ポリシーから除外されている場合、ユーザー定義のアクセス ポリシーに含まれているカスタム URL カテゴリのデフォルト アクションは、[グローバル設定を使用（Use Global Settings）] ではなく、[モニター（Monitor）] になります。カスタム URL カテゴリがグローバル アクセス ポリシーで除外されている場合は、[グローバル設定を使用（Use Global Settings）] を選択できません。
ブロック（Block）	Web プロキシは、この設定に一致するトランザクションを拒否します。
リダイレクト（Redirect）	当初の宛先がこのカテゴリの URL であるトラフィックを、指定された場所にリダイレクトします。このオプションを選択すると、[リダイレクト先（Redirect To）] フィールドが表示されます。すべてのトラフィックをリダイレクトする URL を入力します。
許可（Allow）	このカテゴリの Web サイトに対してクライアント要求を常に許可します。 許可された要求は、以降のすべてのフィルタリングとマルウェア スキャンをバイパスします。 この設定は信頼できる Web サイトに対してのみ使用してください。この設定は内部サイトに対して使用することをお勧めします。
モニター（Monitor）	Web プロキシは、要求を許可せず、ブロックもしません。代わりに、他のポリシー グループ制御設定（Web レピュテーション フィルタリングなど）と照合して、クライアント要求の評価を続行します。
警告（Warn）	当初、Web プロキシは要求をブロックして警告ページを表示しますが、ユーザーは警告ページのハイパーテキスト リンクをクリックすることで続行できます。 **Note** YouTube カテゴリ フィルタリングでは、どのカテゴリの警告アクションを選択しても、警告メッセージなしでそのカテゴリのビデオを表示できます。これは想定された動作です。
クォータベース（Quota-Based）	個々のユーザーが、指定されたボリュームまたは時間クォータに達すると、警告が表示されます。クォータに達すると、ブロック ページが表示されます。時間範囲およびクォータ, on page 125を参照してください。

アクション	説明
時間ベース（Time-Based）	Web プロキシは、指定された時間範囲内で要求をブロックまたはモニターします。時間範囲およびクォータ, on page 125を参照してください。

ステップ 5 [事前定義された URL カテゴリのフィルタリング（Predefined URL Category Filtering）] セクションで、各カテゴリに対して以下のいずれかのアクションを選択します。

- グローバル設定を使用（Use Global Settings）
- モニター（Monitor）
- 警告（Warn）
- ブロック（Block）
- 時間ベース（Time-Based）
- クォータベース（Quota-Based）

ステップ 6 [分類されてない URL（Uncategorized URLs）] セクションで、定義済みまたはカスタムの URL カテゴリに分類されない 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。この設定により、URL カテゴリ セットの更新で生じた新規カテゴリとマージ カテゴリのデフォルト アクションも決まります。

ステップ 7 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

What to do next

- 埋め込み/参照コンテンツのブロックの例外, on page 32

埋め込み/参照コンテンツのブロックの例外

Web サイトに、別のカテゴリに分類されているコンテンツまたはアプリケーションとみなされるコンテンツが埋め込まれているか、参照している可能性があります。たとえば、ニュース Web サイトには、ストリーミングビデオとして分類され、アプリケーション YouTube と識別されるコンテンツが含まれることがあります。デフォルトでは、埋め込まれたコンテンツは、埋め込まれている Web サイトに関係なく、独自のカテゴリまたはアプリケーションに対して選択されたアクションに基づいてブロックまたは監視されます。この表を使用して、例外を設定します（たとえば、ニュース Web サイトまたはイントラネットを表すカスタムカテゴリから参照されるすべてのコンテンツを許可する場合）。

Note アプリケーション参照コンテンツの設定は、利用可能な Application Control Engine によって異なります。Application Control Engine が変更された場合は、アプリケーション参照コンテンツを確認してください。

Note 埋め込みコンテンツに対する要求には、通常、要求が発信されるサイトのアドレスが含まれます（要求の HTTP ヘッダーの「referer」フィールドとして知られています）。このヘッダー情報を使用して、参照コンテンツの分類が決定されます。

この機能を使用して、埋め込み/参照コンテンツのデフォルト アクションに対する例外を定義できます。たとえば、ニュース Web サイトまたはイントラネットを表すカスタム カテゴリのすべての埋め込み/参照コンテンツを許可することができます。

Note Referer ベースの例外は、アクセス ポリシーでのみサポートされます。HTTPS トラフィックでこの機能を使用するには、アクセス ポリシーで例外を定義する前に、例外用に選択する URL カテゴリの HTTPS 復号を設定する必要があります。HTTPS 復号の設定については、復号ポリシー グループの URL フィルタの設定, on page 34を参照してください。この機能と HTTPS 復号の使用に関する詳細については、埋め込み/参照コンテンツのブロックの例外に対する条件および制約事項を参照してください。

Procedure

ステップ 1 特定のアクセス ポリシーの [URL フィルタリング（URL Filtering）] ページ（アクセス ポリシー グループの URL フィルタの設定, on page 30を参照）で、[埋め込みおよび参照コンテンツのブロックの例外（Exceptions to Blocking for Embedded/Referred Content）] セクションの [例外の有効化（Enable Except）] をクリックします。

ステップ 2 [これらのカテゴリごとに参照コンテンツの例外を設定（Set Exception for Content Referred by These Categories）] 列の [クリックしてカテゴリを選択（Click to select categories）] リンクをクリックして、URL フィルタリング カテゴリの参照の例外の選択ページを開きます。

ステップ 3 [定義済みおよびカスタム URL カテゴリ（Predefined and Custom URL Categories）] リストから、この参照の例外を定義するカテゴリを選択し、[完了（Done）] をクリックしてこのアクセス ポリシーの [URL フィルタリング（URL Filtering）] ページに戻ります。

ステップ 4 [この参照コンテンツの例外を設定（Set Exception for this Referred Content）] ドロップダウン リストから例外のタイプを選択します。

- [すべての埋め込み/参照コンテンツ（All embedded/referred content）]：コンテンツのカテゴリに関係なく、指定したカテゴリ タイプのサイトのすべての埋め込み/参照コンテンツはブロックされません。
- [選択した埋め込み/参照コンテンツ（Selected embedded/referred content）]：このオプションを選択した後、指定した URL カテゴリから発信された場合はブロックしない特定のカテゴリおよびアプリケーションを選択します。
- [すべての埋め込み/参照コンテンツの例外（All embedded/referred content except）]：このオプションを選択すると、ここで指定する URL カテゴリおよびアプリケーションを除いて、指定したカテゴリ タイプのサイトのすべての埋め込み/参照コンテンツはブロックされません。つまり、ここで指定するタイプはブロックされたままになります。

Note
[参照元の例外（Referrer Exception）] オプションは、カスタム URL カテゴリがアクセスポリシーに含まれていない場合でもデフォルトで有効になっています。

ステップ 5 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

What to do next

[レポート（Reporting）] ページ（[URL カテゴリ（URL Categories）]、[ユーザー（Users）]、および [Web サイト（Web Sites）]）や [概要（Overview）] ページの関連チャートに表示される表およびチャートに、「Referrer によって許可される」トランザクション データを表示するように選択できます。チャート表示オプションの選択の詳細については、チャート化するデータの選択を参照してください。

復号ポリシー グループの URL フィルタの設定

ユーザー定義の復号ポリシー グループおよびグローバル復号ポリシー グループに対して URL フィルタリングを設定できます。

Procedure

ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] > [復号ポリシー（Decryption Policies）] を選択します。

ステップ 2 ポリシー テーブルで、編集するポリシー グループの [URL フィルタ（URL Filtering）] 列にあるリンクをクリックします。

ステップ 3 （任意）[カスタムURLカテゴリのフィルタリング（Custom URL Category Filtering）] セクションで、このポリシーのアクションの実行対象となるカスタム URL カテゴリを追加できます。

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 4 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。

アクション	説明
グローバル設定を使用（Use Global Setting）	グローバル復号ポリシー グループで設定されているこのカテゴリ用のアクションを使用します。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。 ユーザー定義のポリシー グループにのみ適用されます。 カスタム URL カテゴリがグローバル復号ポリシーから除外されている場合、ユーザー定義の復号ポリシーに含まれているカスタム URL カテゴリのデフォルト アクションは、[グローバル設定を使用（Use Global Settings）] でなく、[モニター（Monitor）] になります。カスタム URL カテゴリがグローバル復号ポリシーから除外されている場合は、[グローバル設定を使用（Use Global Settings）] を選択できません。
パススルー（Pass Through）	トラフィック コンテンツを検査せずに、クライアントとサーバー間の接続をパススルーします。
モニター（Monitor）	Web プロキシは、要求を許可せず、ブロックもしません。代わりに、他のポリシー グループ制御設定（Web レピュテーション フィルタリングなど）と照合して、クライアント要求の評価を続行します。
復号（Decrypt）	接続を許可しますが、トラフィック コンテンツを検査します。アプライアンスはトラフィックを復号し、プレーン テキスト HTTP 接続であるかのように、復号したトラフィックにアクセス ポリシーを適用します。接続を復号し、アクセス ポリシーを適用することにより、トラフィックをスキャンしてマルウェアを検出できます。
ドロップ（Drop）	接続をドロップし、サーバーに接続要求を渡しません。アプライアンスは接続をドロップしたことをユーザーに通知しません。

Note
HTTPS 要求の特定の URL カテゴリをブロックする場合は、復号ポリシー グループのその URL カテゴリを復号することを選択し、次に、アクセス ポリシー グループの同じ URL カテゴリをブロックすることを選択します。

ステップ 5 [分類されてない URL（Uncategorized URLs）] セクションで、定義済みまたはカスタムの URL カテゴリに分類されない 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。

この設定により、URL カテゴリ セットの更新で生じた新規カテゴリとマージ カテゴリのデフォルト アクションも決まります。

ステップ 6 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

データ セキュリティ ポリシー グループの URL フィルタの設定

ユーザー定義のデータ セキュリティ ポリシー グループおよびグローバル ポリシー グループに対して URL フィルタリングを設定できます。

Procedure

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）]>[シスコデータセキュリティ（Cisco Data Security）]を選択します。

ステップ 2 ポリシー テーブルで、編集するポリシー グループの [URL フィルタ（URL Filtering）] 列にあるリンクをクリックします。

ステップ 3 （任意）[カスタムURLカテゴリのフィルタリング（Custom URL Category Filtering）] セクションで、このポリシーのアクションの実行対象となるカスタム URL カテゴリを追加できます。

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 4 [カスタムURLカテゴリのフィルタリング（Custom URL Category Filtering）]セクションで、各カスタム URL カテゴリのアクションを選択します。

アクション	説明
グローバル設定を使用（Use Global Setting）	グローバル ポリシー グループで設定されているこのカテゴリ用のアクションを使用します。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。 ユーザー定義のポリシー グループにのみ適用されます。 カスタム URL カテゴリがグローバル シスコ データセキュリティ ポリシーから除外されている場合、ユーザー定義のシスコ データセキュリティ ポリシーに含まれているカスタム URL カテゴリのデフォルト アクションは、[グローバル設定を使用（Use Global Settings）] でなく、[モニター（Monitor）] になります。カスタム URL カテゴリがグローバルなシスコ データ セキュリティ ポリシーから除外されている場合は、[グローバル設定を使用（Use Global Settings）] を選択できません。
許可（Allow）	このカテゴリの Web サイトに対してアップロード要求を常に許可します。カスタム URL カテゴリにのみ適用されます 許可された要求は以降のすべてのデータ セキュリティ スキャンをバイパスし、アクセス ポリシーに対して評価されます。 この設定は信頼できる Web サイトに対してのみ使用してください。この設定は内部サイトに対して使用することをお勧めします。

アクション	説明
モニター（Monitor）	Webプロキシは、要求を許可せず、ブロックもしません。代わりに、他のポリシーグループ制御設定（Web レピュテーション フィルタリングなど）と照合して、アップロード要求の評価を続行します。
ブロック（Block）	Web プロキシは、この設定に一致するトランザクションを拒否します。

Note
ファイルサイズの上限を無効にしない場合、URL フィルタリングで [許可（Allow）] または [モニター（Monitor）] オプションが選択されているときに、 Secure Web Applianceで最大ファイルサイズの検証が続行されます。

ステップ 5 [事前定義された URL カテゴリのフィルタリング（Predefined URL Category Filtering）] セクションで、各カテゴリに対して以下のいずれかのアクションを選択します。

- グローバル設定を使用（Use Global Settings）
- モニター（Monitor）
- ブロック（Block）

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 サイトへのアップロード要求に対して実行するアクションを選択します。この設定により、URL カテゴリ セットの更新で生じた新規カテゴリとマージ カテゴリのデフォルト アクションも決まります。

ステップ 7 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

What to do next

関連項目

- URL カテゴリ セットの更新によるポリシーのフィルタリング アクションへの影響, on page 22。

YouTube の分類

YouTube 分類機能により、YouTube のカスタム URL カテゴリを作成し、YouTube カスタムカテゴリに関するポリシーを設定することで、アクセスを保護および制御することができます。

（注） 特定の YouTube カテゴリをブロックする時間ベースのアクセスポリシールールを設定する場合：

- 設定した時間ベースのルールは、アクセスポリシーの設定時にすでに開かれて再生されているビデオには適用されません。
- ルールは、ルールを設定した後に新しく開いたビデオにのみ適用されます。

（注）

- googleapis.com がアップストリームプロキシまたはアップストリーム ファイアウォールでブロックされていないことを確認します。Cisco アップデートサーバーと WBNP テレメトリサーバーに例外を設定している場合は、googleapis.com にも同様に設定します。
- 次のビデオは、ブロックされる YouTube のカテゴリに属する場合でもブロックされません。
  - チャンネルの studio.youtube.com ページに表示されるビデオサムネイル。
  - Google の検索結果に表示されるビデオサムネイル。
  - YouTube ショート ビデオ カテゴリが断続的に機能しなくなる場合があります。

YouTube 分類機能を設定するには、次の作業を実行します。

手順	タスク	トピックおよび手順へのリンク
1.	www.youtube.com と m.youtube.com を使用して、YouTube のカスタムおよび外部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 （41 ページ）。
2.	YouTube のカスタムおよび外部 URL カテゴリを復号ポリシーに追加します。	復号ポリシー グループの URL フィルタの設定 （34 ページ）。
3.	YouTube 分類機能を有効にします。	YouTube 分類機能の有効化 （39 ページ）。

手順	タスク	トピックおよび手順へのリンク
4.	YouTube のカスタムおよび外部 URL カテゴリにアクセスポリシーを適用します。	アクセス ポリシー グループの URL フィルタの設定 （30 ページ）。 （注） [アクセスポリシー（Access Policies）] > [URLフィルタリング（URL Filtering）] ページの [YouTubeカテゴリのフィルタリング（YouTube Category Filtering）] セクションで、「ブロック、モニター、または警告」アクションを設定する必要があります。

YouTube 分類機能の有効化

始める前に

- HTTPS プロキシを有効にします（[セキュリティサービス（Security Services）] > [HTTPS プロキシ（HTTPS Proxy）] ）。
- [使用許可コントロール（Acceptable Use Controls）] を有効にします（[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）]）。
- www.youtube.com と m.youtube.com を使用してカスタムおよび外部 URL カテゴリを設定します（[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）]）。
- YouTube のカスタム URL カテゴリと外部 URL カテゴリを使用し、アクションを [復号（decrypt）] にして復号ポリシーを設定します。
- YouTube 用の Google API サービスを使用して Google API キーを生成します。Google API キーを生成するには、次の手順を実行します。
  1. Google アカウントのクレデンシャルを使用して https://console.developers.google.com/ にログインします（個人の Google アカウントの使用は推奨されません）。
  2. プロジェクトを作成します。
  3. [API とサービスの有効化（Enable APIs and Services）] で、[YouTube Data API v3] を有効にします。
  4. ウィザードを使用して API キーを生成するか、または [API とサービス（APIs & Services）] の下にある [クレデンシャル（Credentials）] オプションを使用します。

（注） ウィザードを使用して API キーを生成するには、[YouTube Data API v3] で次の手順を実行します。

1. [APIの呼び出し元（Where will you be calling the API from?）] ドロップダウンリストから、[その他の非UI（Other non-UI）]（cron job、daemon など）を選択します。
2. [アクセスするデータ（What data will you be accessing）] セクションで、[パブリックデータ（Public data）] を選択します。
3. [必要なクレデンシャル（What credentials do I need?）] をクリックし、次に [完了（Done）] をクリックします。

手順

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 [グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3 YouTube の分類の横にある [有効化（Enable）] チェックボックスをオンにします。

ステップ 4 Google API サービスを使用して生成した API キーを入力します。

YouTube 分類機能を有効にする前に、Google API サービスを使用して API キーを生成する必要があります。

ステップ 5 クエリタイムアウトを入力して、アプライアンスと YouTube API サーバー間のタイムアウト期間を設定します。

ステップ 6 YouTube カテゴリトラフィックが通過するルーティングテーブルを選択します。

- データ（Data）：P1 および P2 インターフェイス用
- 管理（Management）：M1 インターフェイス用

（注）
デフォルトのルーティングテーブルはデータです。上記の 2 つのオプションは、データと管理サービス用に 2 つの個別のルーティングテーブルを設定した場合にのみ使用できます（[ネットワーク（Network）] > [インターフェイス（Interfaces）]）。

ステップ 7 変更を送信し、保存します。

カスタム URL カテゴリの作成および編集

特定のホスト名と IP アドレスを指定する、カスタムおよび外部のライブフィード URL カテゴリを作成できます。また、既存の URL カテゴリを編集したり削除することができます。これらのカスタム URL カテゴリを同じアクセス ポリシー グループ、復号ポリシー グループ、またはシスコ データ セキュリティ ポリシー グループに含めて、各カテゴリに異なるアクションを割り当てると、より上位のカスタム URL カテゴリのアクションが優先されます。

Note これらの URL カテゴリ定義で使用できる外部ライブフィードファイルは 30 までに制限されており、各ファイルに格納できるエントリ数は最大 5000 です。外部フィードエントリを増やしたり、正規表現エントリの数が膨大になったりすると、パフォーマンスの低下につながります。

Secure Web Appliance では、先頭に文字「c_」が付加されたカスタム URL カテゴリ名の最初の 4 文字が、アクセス ログで使用されます。Sawmill を使用してアクセス ログを解析する場合は、カスタム URL カテゴリの名前に注意してください。カスタム URL カテゴリの最初の 4 文字にスペースが含まれていると、Sawmill はアクセス ログ エントリを正しく解析できません。代わりに、最初の 4 文字にはサポートされる文字のみを使用します。カスタム URL カテゴリの完全な名前をアクセス ログに記録する場合は、%XF フォーマット指定子をアクセス ログに追加します。

Note DNS が複数の IP を Web サイトに解決し、それらの IP の 1 つがカスタムブロックリストに登録されている場合、 Secure Web Appliance はカスタムブロックリストへの登録の有無にかかわらずすべての IP の Web サイトをブロックします。

Before you begin

[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。

Procedure

ステップ 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）] を選択します。

ステップ 2 カスタム URL カテゴリを作成するには、[カテゴリを追加（Add Category）] をクリックします。既存のカスタム URL カテゴリを編集するには、URL カテゴリの名前をクリックします。

ステップ 3 次の情報を入力します。

設定	説明
カテゴリ名（Category Name）	この URL カテゴリの識別子を入力します。この名前は、ポリシー グループに URL フィルタリングを設定するときに表示されます。
リスト順（List Order）	カスタム URL カテゴリのリストで、このカテゴリの順序を指定します。リスト内の最初の URL カテゴリに「1」を入力します。 URL フィルタリング エンジンでは、指定した順序でカスタム URL カテゴリに対してクライアント要求が評価されます。
カテゴリ タイプ（Category Type）	[ローカル カスタム カテゴリ（Local Custom Category）] または [外部ライブフィード カテゴリ（External Live Feed Category）] を選択します。
着信サービス一覧（Routing Table）	[管理（Management）] または [データ（Data）] を選択します。この選択は、「分割ルーティング」が有効にされている場合にのみ行うことができます。つまり、ローカル カスタム カテゴリでは選択できません。分割ルーティングの有効化については、ネットワーク インターフェイスのイネーブル化または変更を参照してください。

設定	説明
サイト/フィードファイルの場所（Sites / Feed File Location）	[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）] を選択した場合、カスタム [サイト（Sites）] を指定します。 • このカスタム カテゴリのサイト アドレスを 1 つまたは複数入力します。複数のアドレスは、改行またはカンマで区切って入力します。これらのアドレスの形式は、次のいずれかにします。 • IPv4 アドレス。10.1.1.0 など • IPv6 アドレス。2001:0db8:: など • IPv4 CIDR アドレス。10.1.1.0/24 など • IPv6 CIDR アドレス。2001:0db8::/32 など • ドメイン名。example.com など • ホスト名。crm.example.com など • .example.com などのドットで始まる部分的なホスト名は、ドメインのすべてのサブドメイン（www.example.com、mail.example.com など）と一致しますが、ルートドメイン自体（example.com）とは一致しません。ルートドメインとそのサブドメインの両方を含めるには、example.com と .example.com の両方を指定します。 • 正規表現は、次に示すように [詳細設定（Advanced）] セクションで入力できます。 **Note** • Cisco Secure Web Appliance では、サイトのアドレスに非 ASCII 文字を使用できません。 • 複数のカスタム URL カテゴリで同じアドレスを使用することは可能ですが、カテゴリがリストされる順序は相互関係によります。同じポリシーにこれらのカテゴリを含めて、それぞれに異なるアクションを定義する場合、カスタム URL カテゴリ テーブルの 1 番上にリストされるカテゴリに定義されたアクションが適用されます。 • （オプション）[URLのソート（Sort URLs）] をクリックして、[サイト（Sites）] フィールド内のすべてのアドレスをソートします。 **Note** アドレスをソートした後は、元の順序に戻すことができません。

設定	説明
除外サイト	[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）] を選択した場合は、既存のフィード ファイルから除外するサイトを入力します。複数のアドレスは、改行またはカンマで区切って入力します。これらのアドレスの形式は、次のいずれかにします。 • IPv6 アドレス（2001:0db8::/32 など） • IPv4 アドレス（10.1.1.0 など） • CIDR IPv6 アドレス（2001:0db8::/32 など） • CIDR IPv4 アドレス（10.1.1.0/24 など） • ドメイン名。example.com など • ホスト名。crm.example.com など • .example.com などのドットで始まる部分的なホスト名は、ドメインのすべてのサブドメイン（www.example.com、mail.example.com など）と一致しますが、ルートドメイン自体（example.com）とは一致しません。ルートドメインとそのサブドメインの両方を含めるには、example.com と .example.com の両方を指定します。

設定	説明
フィードの場所（Feed Location）（続き）	

設定	説明
	[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）] を選択した場合、[フィード ファイルの場所（Feed File Location）] 情報を入力します。つまり、このカスタム カテゴリのアドレスが含まれるファイルの場所を指定して、そのファイルをダウンロードします。 **a.** [シスコのフィード形式（Cisco Feed Format）] または [Office 365のフィード形式（Office 365 Feed Format）]、または [Office 365 Webサービス（Office 365 Web Service）] を選択してから、適切なフィード ファイルの情報を入力します。 • [シスコのフィード形式（Cisco Feed Format）] : • 使用するトランスポート プロトコル（HTTPS または HTTP）を選択してから、ライブフィードファイルのURLを入力します。このファイルはカンマ区切り値（.csv）形式のファイルでなければなりせん。このファイルの詳細については、外部フィードファイルの形式, on page 49を参照してください。 • 必要に応じて、[詳細設定（Advanced）] セクションの [認証（Authentication）] にクレデンシャルを入力します。指定したフィードサーバに接続するために使用するユーザ名とパスフレーズを入力します。 • [Office 365 のフィード形式（Office 365 Feed Format）] : • [Office 365 フィードの場所（Office 365 Feed Location）] に、ライブフィード ファイルの場所（URL）を入力します。 このファイルは、XML ファイル形式でなければなりません。このファイルの詳細については、外部フィードファイルの形式, on page 49を参照してください。 • **Office 365 Webサービス（Office 365 Web Service）** Web サービスの URL を入力します。ClientRequestId が含まれておらず、JSON 形式である必要があります。アプライアンスはClientRequestId を自動的に生成します。 **b.** [シスコのフィード形式（Cisco Feed Format）] および [Office 365のフィード形式（Office 365 Feed Format）] の場合は、[ファイルの取得（Get File）] をクリックして、フィードサーバとの接続をテストし、フィードファイルを解析してサーバからダウンロードします。 [ファイルの取得（Get File）] ボタンの下にあるテキスト ボックスに、進捗状況が表示されます。エラーが発生した場合は、その問題が示されるので、問題を修正してから再試行します。発生する可能性のあるエラーについては、外部ライブフィード ファイルのダウンロードに関する問題を参照してください。 [Office 365 Webサービス（Office 365 Web Service）] の場合は、[テスト開始（Start Test）] をクリックし、サービスを開始してURLおよびIPをダウンロードします。

設定	説明
	Note これらの URL カテゴリ定義で使用できる外部ライブフィードは最大 30 です。また、各ファイルに格納できるエントリ数は最大 5000 に制限されています。外部フィードエントリの数を増やすと、パフォーマンスの低下につながります。 **Tip** ライブフィード カテゴリの変更を保存した後、[カスタムおよび外部 URL カテゴリ（Custom and External URL Categories）] ページ（[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 [フィードの内容（Feed Content）] 列でこのエントリに対応する [表示（View）] をクリックすると、ダウンロードしたシスコ フィード形式または Office 365 フィード形式のファイルに含まれているアドレスを表示するウィンドウが開きます。
詳細設定（Advanced）	[カテゴリ タイプ（Category Type）] に [ローカル カスタム カテゴリ（Local Custom Category）] を選択した場合、このセクションに、追加のアドレス セットを指定する正規表現を入力できます。 正規表現を使用して、入力したパターンと一致する複数のアドレスを指定できます。 **Note** • URL フィルタリング エンジンでは、まず [サイト（Sites）] フィールドに入力したアドレスと URL が比較されます。トランザクションの URL が [サイト（Sites）] フィールドの入力値と一致した場合は、ここで入力した式との比較は行われません。 • URL パスを正規表現として追加するときは、スペース文字の代わりに「%20」を使用します。正規表現として使用する場合、URL パスにスペース文字を含めることはできません。 • Cisco Secure Web Appliance では、正規表現に非 ASCII 文字を使用できません。 正規表現の使用方法については、正規表現, on page 57を参照してください。
詳細設定（正規表現の除外）	[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）] を選択した場合は、既存のフィード ファイルから除外する正規表現を入力します。エントリは、フィードファイルの既存の正規表現と正確に一致する必要があります。

設定	説明
フィードの自動更新（Auto Update the Feed）	フィードの更新オプションを選択します。 • **[自動更新しない（Do not auto update）]** • [n HH:MM 間隔（Every *n* HH:MM）]。たとえば、5 分間隔の場合は 00:05 と入力します。ただし、頻繁に更新すると Secure Web Appliance のパフォーマンスに影響することに注意してください。 **Note** リロードして再公開するたびに、使用可能なフィードファイルが現在ダウンロードされているファイルと同じであっても、アプライアンスは使用可能なフィードファイルをダウンロードし、ダウンロード時間を更新します。

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）]）。

What to do next

関連項目

- 正規表現, on page 57。
- アクセス ログのカスタマイズ。
- カスタム URL カテゴリおよび外部 URL カテゴリに関する問題

カスタムおよび外部 URL カテゴリのアドレス形式とフィード ファイル形式

カスタムおよび外部 URL カテゴリを作成および編集する場合は、1 つ以上のネットワーク アドレスを指定する必要があります。**ローカル カスタム カテゴリ**のアドレスを指定するのか、それとも**外部ライブ フィード カテゴリ**のフィードファイル形式で指定するのかは問いません。各インスタンスでは、複数のアドレスを改行またはカンマで区切って入力することがます。これらのアドレスの形式は、次のいずれかにします。

- IPv4 アドレス。10.1.1.0 など
- IPv6 アドレス。2001:0db8:: など
- IPv4 CIDR アドレス。10.1.1.0/24 など
- IPv6 CIDR アドレス。2001:0db8::/32 など
- ドメイン名。example.com など
- ホスト名。crm.example.com など
- .example.com などのドットで始まる部分的なホスト名は、ドメインのすべてのサブドメイン（www.example.com、mail.example.com など）と一致しますが、ルートドメイン自体

（example.com）とは一致しません。ルートドメインとそのサブドメインの両方を含めるには、example.com と .example.com の両方を指定します。

- 指定したパターンと一致する複数のアドレスを指定する正規表現（正規表現の仕様の詳細については、正規表現 （57 ページ）を参照）

（注） 複数のカスタム URL カテゴリで同じアドレスを使用することは可能ですが、カテゴリがリストされる順序は相互関係によります。同じポリシーにこれらのカテゴリを含めて、それぞれに異なるアクションを定義する場合、カスタム URL カテゴリ テーブルの 1 番上にリストされるカテゴリに定義されたアクションが適用されます。

外部フィードファイルの形式

カスタム カテゴリおよび外部の URL カテゴリを作成および編集する場合に、[カテゴリタイプ（Category Type）] で [外部ライブ フィード カテゴリ（External Live Feed Category）] を選択する場合は、フィード形式（[シスコ フィード形式（Cisco Feed Format）] または [Office 365 フィード形式（Office 365 Feed Format）]）を選択して、該当するフィード ファイル サーバの URL を指定する必要があります。

フィード ファイルごとに予測される形式は、次のとおりです。

- シスコ フィード形式（Cisco Feed Format）：カンマ区切り値（.csv）ファイル（.csv 拡張子の付いたテキスト ファイル）を指定する必要があります。.csv ファイルの各エントリは、アドレス/カンマ/アドレスタイプの形式で、独立した行に記述する必要があります（`www.cisco.com,site` や `ad2.*\.com,regex` など）。有効なアドレスタイプは `site` と `regex` です。次に、シスコ フィード形式の .csv ファイルの一部を示します。

```
www.cisco.com,site

\.xyz,regex

ad2.*\.com,regex

www.trafficholder.com,site

2000:1:1:11:1:1::200,site
```

（注） ファイル内の `site` エントリの一部として `http://` または `https://` を含めないでください。エラーが発生します。つまり、`www.example.com` は正しく解析されますが、`http://www.example.com` ではエラーが発生します。

- Office 365 フィード形式（Office 365 Feed Format）：Microsoft Office 365 サーバ、または保存先のローカル サーバに配置された XML ファイルです。Office 365 サービスが提供するもので、変更することはできません。ファイル内のネットワーク アドレスは、`products` > `product` > `addresslist` > `address` の構造に従う XML タグで囲まれます。現在の実装では

addresslist 型には IPv6、IPv4、または URL（ドメインや正規表現を含むことも可）を指定できます。次に、Office 365 フィード ファイルのスニペットを示します。

```
<products updated="4/15/2016">
   <product name="o365">
      <addresslist type="IPv6">
         <address>2603:1040:401::d:80</address>
         <address>2603:1040:401::a</address>
         <address>2603:1040:401::9</address>
      </addresslist>
      <addresslist type="IPv4">
         <address>13.71.145.72</address>
         <address>13.71.148.74</address>
         <address>13.71.145.114</address>
      </addresslist>
      <addresslist type="URL">
         <address>*.aadrm.com</address>
         <address>*.azurerms.com</address>
         <address>*.cloudapp.net2</address>
      </addresslist>
   </product>
   <product name="LYO">
      <addresslist type="URL">
         <address>*.broadcast.skype.com</address>
         <address>*.Lync.com</address>
      </addresslist>
   </product>
 </products>
```

アダルト コンテンツのフィルタリング

一部の Web 検索や Web サイトからアダルト コンテンツをフィルタリングするように、 Secure Web Applianceを設定できます。AVC エンジンは、URL や Web クッキーを書き換えてセーフ モードを有効化することで、特定の Web サイトに実装されているセーフ モード機能を利用し、セーフ サーチやサイト コンテンツ レーティングを適用します。

以下の機能によってアダルト コンテンツをフィルタリングします。

オプション	説明
セーフ サーチの適用（Enforce safe searches）	発信検索要求がセーフ サーチ要求として検索エンジンに表示されるように、 Secure Web Applianceを設定することができます。これにより、ユーザーが検索エンジンを使用して使用許可ポリシーを回避するのを防止できます。
サイトコンテンツ レーティングの適用（Enforce site content ratings）	一部のコンテンツ共有サイトでは、独自のセーフ サーチ機能を適用するか、アダルト コンテンツへのアクセスをブロックするか、または両方を実行することによって、サイトのアダルト コンテンツへのユーザーによるアクセスを制限しています。この分類機能は、一般的にコンテンツ レーティングと呼ばれています。

Note セーフ サーチ機能またはサイト コンテンツ レーティング機能がイネーブルになっているアクセス ポリシーは、安全なブラウジング アクセス ポリシーと見なされます。

セーフ サーチおよびサイト コンテンツ レーティングの適用

Note セーフ サーチおよびサイト コンテンツ レーティングを有効にすると、安全に参照するために、AVC エンジンがアプリケーションを識別する役割を果たすようになります。条件の 1 つとして、AVC エンジンは応答本文をスキャンし、検索アプリケーションを検出します。その結果、アプライアンスは範囲ヘッダーを転送しません。

Procedure

ステップ 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。

ステップ 2 [URL フィルタリング（URL Filtering）] 列にある、アクセス ポリシー グループまたはグローバル ポリシー グループのリンクをクリックします。

ステップ 3 ユーザー定義のアクセス ポリシーを編集する場合、[コンテンツ フィルタ（Content Filtering）] セクションの [コンテンツ フィルタ カスタム設定を定義（Define Content Filtering Custom Settings）] を選択します。

ステップ 4 [セーフ サーチを有効にする（Enable Safe Search）] チェックボックスをオンにして、セーフ サーチ機能をイネーブルにします。

ステップ 5 Secure Web Applianceのセーフ サーチ機能で現在サポートされていない検索エンジンからユーザをブロックするかどうかを選択します。

ステップ 6 [サイトコンテンツ評価を有効にする（Enable Site Content Rating）] チェックボックスをオンにして、サイト コンテンツ レーティング機能をイネーブルにします。

ステップ 7 サポート対象のコンテンツ レーティング Web サイトからのアダルト コンテンツをすべてブロックするか、エンドユーザー URL フィルタリング警告ページを表示するかを選択します。

Note
サポート対象のいずれかの検索エンジンの URL、またはサポート対象のいずれかのコンテンツ レーティング Web サイトの URL が、[許可（Allow）] アクションが適用されているカスタム URL カテゴリに含まれている場合、検索結果はブロックされず、すべてのコンテンツが表示されます。

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

What to do next

関連項目

- ユーザーへの警告と続行の許可, on page 54。

アダルト コンテンツ アクセスのロギング

デフォルトでは、アクセス ログには安全なブラウジング スキャンの判定が含まれており、判定は各エントリの山カッコ内に記載されています。安全なブラウジング スキャンの判定は、セーフ サーチまたはサイト コンテンツ レーティング機能がトランザクションに適用されているかどうかを示します。安全なブラウジング スキャンの判定変数をアクセス ログや W3C アクセス ログに追加することもできます。

- アクセス ログ：%XS
- W3C アクセス ログ：x-request-rewrite

値	説明
ensrch	元のクライアント要求が安全ではなく、セーフ サーチ機能が適用されました。
encrt	元のクライアント要求が安全ではなく、サイト コンテンツ レーティング機能が適用されました。
unsupp	元のクライアント要求がサポートされていない検索エンジン向けでした。
err	元のクライアント要求は安全ではありませんが、エラーのためにセーフ サーチ機能もサイト コンテンツ レーティング機能も適用されませんでした。
-	機能がバイパスされたため（トランザクションがカスタム URL カテゴリで許可された場合など）、またはサポートされていないアプリケーションで要求が実行されたため、セーフ サーチ機能もサイト コンテンツ レーティング機能もクライアント要求に適用されませんでした。

セーフ サーチまたはサイト コンテンツ レーティング機能によってブロックされた要求には、アクセス ログで以下のいずれかの ACL デシジョン タグが使用されます。

- BLOCK_SEARCH_UNSAFE
- BLOCK_CONTENT_UNSAFE
- BLOCK_UNSUPPORTED_SEARCH_APP
- BLOCK_CONTINUE_CONTENT_UNSAFE

関連項目

- ACL デシジョン タグ。

アクセス ポリシーでのトラフィックのリダイレクト

最初の宛先がカスタム URL カテゴリの URL であるトラフィックを指定する場所にリダイレクトするように Secure Web Applianceを設定できます。これにより、宛先サーバーではなく、アプライアンスでトラフィックをリダイレクトできます。カスタム アクセス ポリシー グループまたはグローバル ポリシー グループのトラフィックをリダイレクトできます。

Before you begin

トラフィックをリダイレクトするには、少なくとも 1 つのカスタム URL カテゴリを定義する必要があります。

Procedure

ステップ 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。

ステップ 2 [URL フィルタリング（URL Filtering）] 列にある、アクセス ポリシー グループまたはグローバル ポリシー グループのリンクをクリックします。

ステップ 3 [カスタムURLカテゴリのフィルタリング（Custom URL Category Filtering）] セクションで、[カスタムカテゴリの選択（Select Custom Categories）] をクリックします。

ステップ 4 [このポリシーのカスタムカテゴリを選択（Select Custom Categories for this Policy）] ダイアログボックスで、リダイレクトするカスタム URL カテゴリに対して [ポリシーに含める（Include in policy）] を選択します。

ステップ 5 [適用（Apply）] をクリックします。

ステップ 6 リダイレクトするカスタム カテゴリの [リダイレクト（Redirect）] 列をクリックします。

ステップ 7 [リダイレクト先（Redirect to）] フィールドにトラフィックのリダイレクト先の URL を入力します。

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

Note
トラフィックをリダイレクトするようにアプライアンスを設定する場合は、無限ループにならないように注意してください。

What to do next

関連項目

• カスタム URL カテゴリの作成および編集, on page 41

ロギングとレポート

トラフィックをリダイレクトすると、本来の要求対象である Web サイトのアクセス ログ エントリに REDIRECT_CUSTOMCAT から始まる ACL タグが付けられます。以降、アクセス ログ（通常は次の行）にリダイレクト先の Web サイトのエントリが表示されます。

[レポート（Reporting）] タブに表示されるレポートでは、リダイレクトされたトランザクションは [許可（Allowed）] と示されます。

ユーザーへの警告と続行の許可

サイトが組織の利用規定を満たしていないことをユーザーに警告できます。認証によりユーザー名が使用可能になっている場合、アクセス ログではユーザー名によってユーザーが追跡され、ユーザー名が使用できない場合は IP アドレスによって追跡されます。

以下のいずれかの方法を使用して、ユーザーに警告したり、続行を許可することができます。

- アクセス ポリシー グループの URL カテゴリに対して [警告（Warn）] アクションを選択します。または
- サイト コンテンツ レーティング機能をイネーブルにして、アダルト コンテンツにアクセスするユーザーをブロックする代わりに、ユーザーに警告します。

[エンドユーザー フィルタリング警告（End-User Filtering Warning）] ページの設定

Note

- 「警告して継続」機能は、HTTP トランザクションと復号された HTTPS トランザクションに対してのみ機能します。ネイティブ FTP トランザクションでは機能しません。
- URL フィルタリング エンジンは、特定の要求についてユーザーに警告する場合に、Web プロキシがエンドユーザーに送信する警告ページを提供します。ただし、すべての Web サイトでエンドユーザーに警告ページが表示されるわけではありません。表示されない場合、ユーザーは [警告（Warn）] オプションが割り当てられている URL からブロックされます。引き続きそのサイトにアクセスするチャンスは与えられません。

Procedure

ステップ 1 [セキュリティ サービス（Security Services）] > [ユーザー通知（End-User Notification）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [エンドユーザー フィルタリング警告（End-User Filtering Warning）] ページで以下の設定項目を設定します。

オプション	方法
警告の時間間隔（Time Between Warning）	[警告の時間間隔（Time Between Warning）] では、Web プロキシが、ユーザーごとに各 URL カテゴリに対して、[エンドユーザー フィルタリング警告（End-User Filtering Warning）] ページを表示する頻度を指定します。 この設定は、ユーザー名によって追跡されるユーザーと IP アドレスによって追跡されるユーザーに適用されます。 30 ～ 2678400 秒（1 ヵ月）の任意の値を指定します。デフォルトは 1 時間（3600 秒）です。
カスタム メッセージ（Custom Message）	カスタムメッセージは、ユーザーによって入力されるテキストであり、すべての [エンドユーザーフィルタリング警告（End-User Filtering Warning）] ページに表示されます。 いくつかの単純な HTML タグを組み込み、テキストを書式設定できます。

ステップ 4 [送信（Submit）] をクリックします。

What to do next

関連項目

- アダルト コンテンツのフィルタリング, on page 50
- 通知ページ上のカスタム メッセージ
- エンド ユーザー URL フィルタリング警告ページの設定

時間ベースの URL フィルタの作成

Secure Web Applianceが特定のカテゴリの URL の要求を日時別に処理する方法を設定できます。

Before you begin

[Web セキュリティ マネージャ（Web Security Manager）] > [定義済み時間範囲（Defined Time Range）] に移動し、1 つ以上の時間範囲を定義します。

Procedure

ステップ 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。

ステップ 2 ポリシー テーブルで、編集するポリシー グループの [URL フィルタ（URL Filtering）] 列にあるリンクをクリックします。

ステップ 3 時間範囲に基づいて設定するURL カテゴリ（カスタムまたは定義済み）に対して、[時間ベース（Time-Based）] を選択します。

ステップ 4 [時間範囲内（In Time Range）] フィールドで、URL カテゴリに使用する定義済みの時間範囲を選択します。

ステップ 5 [アクション（Action）] フィールドで、定義した時間範囲内でこの URL カテゴリのトランザクションに割り当てるアクションを選択します。

ステップ 6 [それ以外の場合（Otherwise）] フィールドで、定義した時間範囲外でこの URL カテゴリのトランザクションに割り当てるアクションを選択します。

ステップ 7 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

What to do next

関連項目

- 時間範囲およびクォータ, on page 125

URL フィルタリング アクティビティの表示

[レポート（Reporting）] > [URLカテゴリ（URL Categories）] ページには、一致した上位の URL カテゴリとブロックされた上位の URL カテゴリに関する情報を含む、総合的な URL 統計情報が表示されます。また、帯域幅の節約と Web トランザクションに関するカテゴリ固有のデータも表示されます。

関連項目

- エンドユーザーのアクティビティをモニターするレポートの生成

フィルタリングされない未分類のデータについて

[レポート（Reporting）] > [URL カテゴリ（URL Categories）] ページで URL 統計情報を検討する際は、以下のデータの解釈方法を理解しておくことが大切です。

データ タイプ	説明
URL フィルタリングのバイパス（URL Filtering Bypassed）	URL フィルタリングの前に実行されるポリシー、ポートおよび管理ユーザ エージェントのブロッキングを示します。
分類されてないURL（Uncategorized URL）	URL フィルタリング エンジンに照会したが、カテゴリが一致しなかったすべてのトランザクションを表しています。

アクセス ログへの URL カテゴリの記録

アクセス ログ ファイルでは、各エントリのスキャン判定情報セクションにトランザクションの URL カテゴリが記録されます。

関連項目

- ログによるシステム アクティビティのモニター。

- URL カテゴリについて, on page 61。

正規表現

Secure Web Applianceで使用される正規表現構文は、他の Velocity パターン マッチング エンジンの実装で使用される正規表現構文とはやや異なっています。また、アプライアンスは、バックスラッシュによるスラッシュのエスケープはサポートしていません。正規表現でスラッシュを使用する必要がある場合は、バックスラッシュなしでスラッシュを入力します。

Note 技術的には、AsyncOS for Web では Flex 正規表現アナライザが使用されています。

正規表現は以下の個所で使用できます。

- **アクセス ポリシーのカスタム URL カテゴリ。**アクセス ポリシー グループで使用するカスタム URL カテゴリを作成する際は、正規表現を使用して、入力パターンと一致する複数の Web サーバを指定できます。正規表現で使用できる最大文字数は、Webセキュリティの脆弱性を制限するため、2048 文字に設定されています。
- **ブロックするカスタム ユーザ エージェント。**アクセス ポリシー グループをブロックするようにアプリケーションを編集する際は、ブロックする特定のユーザエージェントを正規表現を使用して入力できます。

Note 広範な文字照合を実行する正規表現はリソースを消費し、システムパフォーマンスに影響を与える可能性があります。したがって、正規表現は慎重に適用する必要があります。

関連項目

- カスタム URL カテゴリの作成および編集, on page 41

正規表現の形成

正規表現は、一般的に、表現における「一致」を利用するルールです。これらを適用することで、特定の URL 宛先や Web サーバーに一致させることができます。たとえば、以下の正規表現は `blocksite.com` を含むパターンに一致します。

```
\.blocksite\.com
```

以下の正規表現の例を考えてください。

```
server[0-9]\.example\.com
```

この例では、`server[0-9]` は `example.com` ドメインの `server0`、`server1`、`server2`、…、`server9` と一致します。

以下の例では、正規表現は downloads ディレクトリ内の `.exe`、`.zip`、`bin` で終わるファイルに一致します。

```
/downloads/.*\.(exe|zip|bin)
```

Note 空白または英数字以外の文字を含む正規表現は、ASCII 引用符で囲む必要があります。

検証エラーを回避するための注意事項

重要：63 文字以上を返す正規表現は失敗し、無効なエントリのエラーが生成されます。必ず、63 文字以上を返す可能性がない正規表現を作成してください。

検証エラーを最小限に抑えるため、以下の注意事項に従ってください。

- 可能な限り、ワイルドカードやカッコで囲んだ式ではなく、リテラル式を使用してください。リテラル式とは、「`It's as easy as ABC123`」のような基本的に加工されていないテキストです。この式は、「`It's as easy as [A-C]{3}[1-3]{3}`」を使用するよりも失敗する可能性が低くなります。後者の式では、結果として非決定性有限オートマトン（NFA）エントリが生じるため、処理時間が大幅に長くなる可能性があります。
- エスケープしていないピリオドの使用は可能な限り避けてください。ピリオドは特別な正規表現文字であり、改行文字以外のあらゆる文字に一致します。たとえば、「`url.com`」などの実際のピリオドと一致させたい場合は、「`url\.com`」のように \ 文字を使用してピリオドをエスケープします。エスケープされたピリオドはリテラル入力と見なされるので、問題が生じません。
- ピリオドの後に 63 文字以上を返すパターン内のエスケープされていないピリオドは、パターンマッチングエンジンによって無効化されます。その影響についてのアラートがユーザーに送信され、パターンを修正または置換するまで更新のたびにアラートを受信し続けます。

  可能な限り、エスケープしていないピリオドではなく、より具体的な一致パターンを使用してください。たとえば、後ろに 1 つの数字が続く URL に一致させるには、「`url.`」ではなく、「`url[0-9]`」を使用します。
- 長い正規表現内でエスケープしていないピリオドを使用することは、特に問題を引き起こすので、避ける必要があります。たとえば、「`Four score and seven years ago our fathers brought forth on this continent, a new nation, conceived in Liberty, and dedicated to the proposition that all men are created .qual`」はエラーを引き起こす可能性があります。ピリオドを含む「`.qual`」をリテラルの「`equal`」に置き換えると問題が解決します。

  また、パターン内でエスケープしていないピリオドを使用し、パターン マッチング エンジンでそのピリオドが無効化されると、63 文字以上が返されます。パターンを修正するか、置き換えてください。

- 正規表現を終了または開始する場合は「*」は使用できません。また、URL に一致させるために正規表現で「./」を使用したり、その式の最後にドットを使用することはできません。
- ワイルドカードとカッコの組み合わせは、問題を引き起こす可能性があります。この組み合わせをできる限り使用しないようにしてください。たとえば、「id:[A-F0-9]{8}-[A-F0-9]{4}-[A-F0-9]{4}-[A-F0-9]{4}-[A-F0-9]{12}\) Gecko/20100101 Firefox/9\.0\.1\$」はエラーになる可能性がありますが、「Gecko/20100101 Firefox/9\.0\.1\$」はエラーになりません。後者の式にはワイルドカードやカッコで囲まれた式が含まれておらず、また、どちらの式でもエスケープされたピリオドが使用されています。

  ワイルドカードやカッコで囲まれた式を排除できない場合は、式のサイズと複雑さを減らすようにしてください。たとえば、「[0-9a-z] {64}」ではエラーが発生する可能性があります。「[0-9]{64}」や「[0-9a-z]{40}」のように、より短いまたはより単純な表現に変更すると、問題が解決します。

エラーが発生した場合は、ワイルドカード（「*」、「+」、「.」など）やカッコで囲まれた式に前述のルールを適用して、問題を解決してください。

Note CLI オプション advancedproxyconfig > miscellaneous > Do you want to enable URL lower case conversion for velocity regex? を使用して、大文字と小文字を区別しないマッチングの場合に小文字に変換するデフォルトの正規表現変換をイネーブルまたはディセーブルにすることができます。このオプションは、大文字と小文字の区別が重要な状況で問題が発生する場合に使用します。このオプションの詳細については、Secure Web Appliance CLI コマンドを参照してください。

正規表現の文字テーブル

メタ文字	説明
.	改行文字（0x0A）を除く任意の文字と一致します。たとえば、正規表現 r.t は文字列 rat、rut、r t と一致しますが、root とは一致しません。 長いパターン内、特に長いパターンの途中でエスケープしていないピリオドを使用する場合は、慎重に行ってください。詳細については、検証エラーを回避するための注意事項, on page 58を参照してください。
*	直前の正規表現の 0 回または複数回の出現と一致します。たとえば、.* は任意の文字列と一致し、「[0-9]*」は任意の数字と一致します。 このメタ文字を使用する場合（特にピリオドと一緒に使用する場合）は、慎重に使用してください。エスケープされていないピリオドを含むパターンは、ピリオドが無効になると 63 文字以上を返します。詳細については、検証エラーを回避するための注意事項, on page 58を参照してください。

メタ文字	説明
\	エスケープ文字。以下のメタ文字を通常の文字として扱うための文字です。たとえば、\^ は、行の先頭ではなく、キャレット記号（^）と一致させる場合に使用します。同様に、\. は、任意の 1 文字ではなく、実際のピリオドと一致させる場合に使用します。
^	行の先頭と一致します。たとえば、正規表現 ^When in matches は、「When in the course of human events」の先頭と一致しますが、「What and when in the」とは一致しません。
$	行または文字列の末尾と一致します。たとえば、b$\. は末尾が「b.」のあらゆる行または文字列と一致します。
+	直前の正規表現の 1 回以上の出現と一致します。たとえば、正規表現 9+ は 9、99、および 999 と一致します。
?	直前の正規表現の 0 回または 1 回の出現と一致します。たとえば、colou?r は、「u」 が任意であるため、「colour」と「color」のどちらとも一致します。
( )	左右のカッコの間の式を 1 つのグループとして扱い、他のメタ文字の範囲を制限します。たとえば、(abc)+ は文字列「abc」の 1 回以上の出現と一致します。「abcabcabc」や「abc123」とは一致しますが、「abab」や「ab123」とは一致しません。
|	論理和（OR）：前のパターンまたは後ろのパターンと一致します。たとえば、(him|her) は、行「it belongs to him」や「it belongs to her」と一致し、「it belongs to them」とは一致しません。
[ ]	カッコで囲まれた文字列の 1 文字に一致します。たとえば、正規表現 r[aou]t は、「rat」、「rot」、「rut」と一致し、「ret」とは一致しません。 文字の範囲は先頭文字、ハイフン、および終了文字で指定します。たとえば、パターン [0-9] は任意の数字と一致します。複数の範囲も指定できます。パターン [A-Za-z] は大文字または小文字を示しています。範囲外（補集合）の文字を照合するには、左角カッコの後に先頭文字を示すキャレット記号を使用します。たとえば、式 [^269A-Z] は 2、6、9、および大文字以外の文字と一致します。

メタ文字	説明
{ }	前のパターンと一致する回数を指定します。 次に例を示します。 D{1,3} は、文字 D が 1 ～ 3 回出現する場合に一致します。 前のパターンが特定の回数（{n}）または特定回数以上（{**n**,}）出現する場合に一致します。たとえば、式 A[0-9]{3} は後ろに 3 桁の数字が続く「A」と一致します。つまり、「A123」とは一致しますが、「A1234」とは一致しません。式 [0-9]{4,} は 4 桁以上の任意の数字と一致します。
“...”	引用符で囲まれた文字を文字どおりに解釈します。

URL カテゴリについて

ここでは、Cisco Web Usage Controls の URL カテゴリのリストを示します。表には URL カテゴリ名の省略形も記載されています。これらの省略形は、アクセス ログ ファイル エントリの [Web レピュテーション フィルタリング（Web Reputation Filtering）] や [マルウェア対策スキャン（Anti-malware Scanning）] セクションに表示されることがあります。

Note アクセス ログでは、Cisco Web Usage Controls の URL カテゴリの各省略形の前にプレフィックス「IW_」が付いています。つまり、「art」カテゴリは「IW_art」となります。

URL カテゴリ	省略形	コード	説明	URL の例
アダルト（Adult）	adlt	1006	アダルト コンテンツを指しますが、ポルノだけではありません。アダルト向けのナイトクラブ（ストリップ クラブ、スワッピング クラブ、同伴サービス、ストリッパーなど）、セックスに関する全般情報（ポルノとは限らない）、性器ピアス、アダルト向けの製品やグリーティング カード、健康や疾病関連以外の性行為に関する情報なども含まれることがあります。	www.adultentertainmentexpo.com www.sincerelynot.com

URL カテゴリ	省略形	コード	説明	URL の例
アドバタイズメント（Advertisements）	adv	1027	Web ページに表示されることの多いバナー広告やポップアップ広告。広告コンテンツを提供しているその他の広告関連 Web サイト。広告サービスおよび広告営業は、[事業および産業（Business and Industry）] カテゴリに分類されます。	www.adforce.com www.doubleclick.com
アルコール（Alcohol）	alc	1077	嗜好品としてのお酒、ビールやワインの醸造、カクテルのレシピ、リキュール販売、ワイナリー、ブドウ園、ビール工場、アルコール類の販売元など。アルコール中毒は [健康と薬（Health and Medicine）] カテゴリに分類されます。バーおよびレストランは[飲食（Dining and Drinking）] カテゴリに分類されます。	www.samueladams.com www.whisky.com
動物とペット	ペット	1107	国内の動物、家畜、介助動物、ペット、およびそれらの世話に関する情報。獣医サービス、医療、および動物の健康。ペットと動物のトレーニング、水族館、動物園、および動物のショー。保護施設、人道支援団体、動物中心のチャリティー、保護区域、ハチの管理、トレーニング、および牧畜。恐竜や絶滅した動物。	www.petmd.com www.wheatenorg.uk
芸術（Arts）	art	1002	画廊および展示会、芸術家および芸術作品、写真、文学および書籍、舞台芸術および劇場、ミュージカル、バレエ、美術館、デザイン、建築。映画およびテレビは [エンターテイメント（Entertainment）] に分類されます。	www.moma.org www.nga.gov
占星術（Astrology）	astr	1074	占星術、ホロスコープ、占い、数霊術、霊能者による助言、タロット。	www.astro.com www.astrology.com

URL カテゴリ	省略形	コード	説明	URL の例
オークション（Auctions）	auct	1088	オンラインまたはオフラインのオークション、オークション会社、オークション案内広告など。	www.craigslist.com www.ebay.com
ビジネスおよび産業（Business and Industry）	busi	1019	マーケティング、商業、企業、ビジネス手法、労働力、人材、運輸、給与、セキュリティとベンチャーキャピタル、オフィス用品、産業機器（プロセス用機器）、機械と機械系、加熱装置、冷却装置、資材運搬機器、包装装置、製造、立体処理、金属製作、建築と建築物、旅客輸送、商業、工業デザイン、建築、建築資材、出荷と貨物（貨物取扱業務、トラック輸送、運送会社、トラック輸送業者、貨物ブローカと輸送ブローカ、優先サービス、荷高と貨物のマッチング、追跡とトレース、鉄道輸送、海上輸送、ロードフィーダサービス、移動と保管）。	www.freightcenter.com www.ge.com
大麻	cann	1109	大麻の快楽的および医療的消費に重点を置いた Web サイト。サイトには、マーケティング、法律および規制の問題に関する議論、成長と生産、道具、研究、大麻産業への投資が含まれる場合があります。ディスペンサリー、カンナビノイド（CBD油、THC など）ベースの製品も含まれています。	www.localproduct.co www.oregonbc.com
チャットおよびインスタントメッセージ（Chat and Instant Messaging）	chat	1040	Web ベースのインスタント メッセージングおよびチャット ルーム。	www.icq.com www.e-chat.co
不正および盗用（Cheating and Plagiarism）	plag	1051	不正行為を助長し、学期末論文（盗用したもの）などの書物を販売したりします。	www.bestessays.com www.superiorpapers.com
児童虐待コンテンツ（Child Abuse Content）	cprn	1064	世界中の違法な児童性的虐待コンテンツ。	—

URL カテゴリ	省略形	コード	説明	URL の例
クラウドおよびデータセンター	serv	1118	組織のアプリケーション、サービス、またはデータ処理をサポートするためにクラウド インフラストラクチャまたはデータセンター ホスティングを提供するために使用されるプラットフォーム。これらのドメインと IP アドレスの分散型という性質のため、コンテンツや所有権に基づいてより具体的なカテゴリを適用することはできません。	www.azurewebsites.net www.s3.amazonaws.com
コンピュータ セキュリティ（Computer Security）	csec	1065	企業ユーザおよび家庭ユーザ向けのセキュリティ製品およびセキュリティ サービス。	www.computersecurity.com www.symantec.com
コンピュータおよびインターネット（Computers and Internet）	comp	1003	コンピュータおよびソフトウェアに関する情報（ハードウェア、ソフトウェア、ソフトウェア サポートなど）、ソフトウェア エンジニア向けの情報、プログラミング、ネットワーク、Web サイト設計、Web およびインターネット全般、コンピュータ科学、コンピュータ グラフィック、クリップアートなど。フリーウェアとシェアウェアは、[フリーウェアおよびシェアウェア（Freeware and Shareware）] カテゴリに分類されます。	www.xml.com www.w3.org

URL カテゴリ	省略形	コード	説明	URL の例
表記法、会議および見本市	expo	1110	特定の業界、市場、または共通の関心をテーマにしたセミナー、見本市、大会、会議。チケットの取得、登録、要約またはプレゼンテーションの提案ガイドライン、ワークショップ、スポンサーの詳細、ベンダーまたは出展者の情報、およびその他のマーケティングまたは販促資料に関する情報が含まれる場合があります。このカテゴリには、アカデミック イベント、プロフェッショナル イベント、ポップカルチャ イベントが含まれます。すべて、一時的または毎年恒例のイベントである傾向があります。	www.thesmallbusinessexpo.com www.makerfaire.com
暗号通貨	Cryp	1111	ユーザが暗号通貨を取引できるオンライン ブローカー業者および Web サイト。分析、解説、アドバイス、業績指標、価格チャートなどの暗号通貨に関する情報。仮想通貨マイニングおよびマイニング ビジネスに関する一般的な情報はこのカテゴリに含まれますが、マイニング アクティビティに直接関係するドメインと IP アドレスは仮想通貨マイニングとして分類されます。	www.coinbase.com www.coinsutra.com
仮想通貨マイニング	mine	1112	暗号通貨マイニングプールにアクティブに参加しているホスト。	www.give-me-coins.com www.slushpool.com
出会い系（Dating）	date	1055	出会い系サイト、結婚紹介所など。	www.eharmony.com www.match.com
デジタル ポストカード（Digital Postcards）	card	1082	デジタルはがきおよび電子カードの送信。	www.hallmarkecards.com www.bluemountain.com
飲食（Dining and Drinking）	food	1061	飲食店、レストラン、バー、居酒屋、パブ、レストラン ガイド、レストラン レビューなど。	www.zagat.com www.experiencethepub.com

URL カテゴリ	省略形	コード	説明	URL の例
DIY プロジェクト（DIY Projects）	diy	1097	エキスパートや専門家の支援を受けずに、物品を作成、改善、変更、装飾、修復するためのガイダンスおよび情報。	www.diy-tips.co.uk www.thisoldhouse.com
DNS トンネリング	tunn	1122	サービスとしてDNSトンネリングを提供するサイト。これらのサービスは、PCまたはモバイル向けのものであり、企業のポリシーおよびインスペクションをバイパスする可能性のあるトラフィックを送信するために、DNS を介して特別に VPN 接続を作成します。	
暗号化された DNS	doht	1113	DNS over HTTPS（DoH）プロトコルまたはDNS over TLSプロトコルを使用した暗号化 DNS リクエスト。これらのプロトコルは通常、エンドユーザによってセキュリティとプライバシーの層として使用されますが、暗号化によってリクエストの宛先が非表示にされ、サードパーティ経由で渡されます。	www.cloudflare-dns.com www.dns。 google.com
ダイナミックおよびレジデンシャル（Dynamic and Residential）	dyn	1091	ブロードバンドリンクのIPアドレス。通常は、ホーム ネットワークへのアクセスを試みているユーザを指します。たとえば、ホーム コンピュータへのリモート セッションの場合などです。	http://109.60.192.55
ダイナミック DNS プロバイダー（Dynamic DNS Provider）	ddns	1114	ダイナミック DNS サービスを使用して、動的に割り当てられた IP アドレスでホストされているエンドポイントから特定のアプリケーションまたはコンテンツに Web 経由でアクセス可能にすることができます。アクセス権は、ダイナミック DNS サービスが所有するドメインのホスト名を介して付与されます。	www.noip.com www.afraid.org

URL カテゴリ	省略形	コード	説明	URL の例
教育（Education）	edu	1001	教育関連の Web サイト。たとえば、学校、短大、大学、教材、教師用資料、技術訓練、職業訓練、オンライン トレーニング、教育問題、教育政策、学資援助、学校助成金、規範、試験など。	www.education.com www.greatschools.org
エンターテイメント（Entertainment）	ent	1093	映画、音楽、バンド、テレビ、芸能人、ファン サイト、エンターテイメント ニュース、芸能界のゴシップ、エンターテイメントの会場などに関する詳細や批評など。[芸術（Arts）] カテゴリとの違いを確認してください。	www.eonline.com www.ew.com
過激（Extreme）	extr	1075	性的暴力または犯罪性のあるもの、暴力および暴力的行為、悪趣味な写真や血まみれの写真（解剖写真など）、犯行現場、犯罪被害者、事故被害者の写真、過度にわいせつな文章や写真、衝撃的な内容の Web サイトなど。	www.car-accidents.com www.crime-scene-photos.com
ファッション（Fashion）	fash	1076	衣料、服飾、美容室、化粧品、アクセサリ、宝飾品、香水、身体改造に関連する図表や文章、タトゥー、ピアス、モデル事務所など。皮膚科関連製品は [健康と薬（Health and Medicine）] カテゴリに分類されます。	www.fashion.net www.styleseat.com
ファイル転送サービス（File Transfer Services）	fts	1071	ダウンロード サービスおよびホスティングによるファイル共有を主目的とするファイル転送サービス	www.sharefile.com www.wetransfer.com
フィルタリング回避（Filter Avoidance）	filt	1025	検出されない匿名の Web 利用を促進および支援する Web サイト。例：cgi、php、および glype を使用した匿名プロキシ サービス。	www.bypassschoolfilter.com www.filterbypass.com

URL カテゴリ	省略形	コード	説明	URL の例
金融（Finance）	fnnc	1015	会計実務、会計士、課税、税、銀行、保険、投資、国家経済、個人資産管理（各種保険、クレジットカード、個人退職金積立計画、遺産相続計画、ローン、住宅ローン）などの金融や財務関連のもの。株は [オンライン トレード（Online Trading）] に分類されます。	www.finance.yahoo.com www.bankofamerica.com
フリーウェアおよびシェアウェア（Freeware and Shareware）	free	1068	フリー ソフトウェアおよびシェアウェア ソフトウェアのダウンロードを提供します。	www.freewarehome.com www.filehippo.com
ギャンブル（Gambling）	gamb	1049	カジノ、オンライン ギャンブル、ブックメーカー、オッズ、ギャンブルに関する助言、ギャンブルの対象となっているレース、スポーツ ブッキング、スポーツ ギャンブル、株式スプレッド ベッティング サービス。ギャンブル中毒に関する Web サイトは、[健康と薬（Health and Medicine）] カテゴリに分類されます。国営宝くじは、[宝くじ（Lotteries）] カテゴリに分類されます。	www.888.com www.gambling.com
ゲーム（Games）	game	1007	さまざまなカード ゲーム、ボード ゲーム、ワード ゲーム、ビデオ ゲーム、戦闘ゲーム、スポーツ ゲーム、ダウンロード型ゲーム、ゲーム批評、攻略本、コンピュータ ゲーム、インターネット ゲーム（ロール プレイング ゲームなど）。	www.games.com www.shockwave.com

URL カテゴリ	省略形	コード	説明	URL の例
生成 AI	gnai	1128	生成 AI とは、人工知能モデルを使用して、ユーザーから提供されたプロンプトに基づき文章、音声、動画、画像などの出力を生成することを主な目的とするサイトを指します。この定義は、より広範なサービス提供の一環として生成 AI を間接的に組み込むだけのテクノロジーを除外します。	https://www.deepseek.com/
政府および法律（Government and Law）	gov	1011	政府 Web サイト、外交関係、政府および選挙に関するニュースや情報、法律家、法律事務所、法律関連の出版物、法律関連の参考資料、裁判所、訴訟事件一覧表、法律関連の協会などの法律分野に関する情報、立法および判例、市民権問題、移民関連、特許、著作権、法執行制度および矯正制度に関する情報、犯罪報道、法的措置、犯罪統計、軍事（軍隊、軍事基地、軍組織）/テロ対策など。	www.usa.gov www.law.com
ハッキング（Hacking）	hack	1050	Web サイト、ソフトウェア、およびコンピュータのセキュリティを回避する方法に関する議論。	www.hackthissite.org www.gohacking.com
ヘイト スピーチ（Hate Speech）	hate	1016	社会集団、肌の色、宗教、性的指向、障がい、階級、民族、国籍、年齢、性別、性同一性を基に、憎悪、不寛容、差別を助長する Web サイト。人種差別を扇動するサイト、性差別、人種差別の神学、人種差別の音楽、ネオナチ組織、特定民族至上主義、ホロコースト否定論。	www.kkk.com www.aryanunity.com

URL カテゴリ	省略形	コード	説明	URL の例
健康と薬	hmed	1104	健康管理、疾病および障がい、医療、病院、医師、医薬品、精神衛生、精神医学、薬理学、エクササイズおよびフィットネス、身体障がい、ビタミン剤およびサプリメント、健康にかかわる性行為（疾病および健康管理）、喫煙、飲酒、薬物使用、健康にかかわるギャンブル（疾病および健康管理）。	www.webmd.com www.health.com
ユーモア（Humor）	lol	1079	ジョーク、スケッチ、コミック、その他のユーモラスなコンテンツ。不快感を与える可能性のあるアダルト ユーモアは [アダルト（Adult）] に分類されます。	www.pun.me www.jokes.com
ハンティング	hunt	1022	職業としての狩猟または魚釣り、またはスポーツとしての狩猟：ガン クラブ、およびその他の狩猟関連のサイト。	www.bulletsafaris.com www.mfha.org
違法行為（Illegal Activities）	ilac	1022	窃盗、不正行為、電話ネットワークへの不法アクセスなどの犯罪を助長するサイト、コンピュータ ウィルス、テロリズム、爆弾、無秩序、殺人や自殺を描写したものやその実行方法を記述した Web サイト。	www.ekran.no www.pyrobin.com
違法ダウンロード（Illegal Downloads）	ildl	1084	著作権契約に違反してソフトウェア保護を回避するための、ソフトウェア、シリアル番号、キー生成ツールなどをダウンロードできる Web サイト。Torrent は [ピアファイル転送（Peer File Transfer）] に分類されます。	www.keygenninja.com www.rootscrack.com
違法ドラッグ（Illegal Drugs）	drug	1047	気晴らしのためのドラッグ、ドラッグ摂取の道具、ドラッグの購入と製造に関する情報。	www.shroomery.org www.hightimes.com

URL カテゴリ	省略形	コード	説明	URL の例
インフラストラクチャおよびコンテンツ配信ネットワーク（Infrastructure and Content Delivery Networks）	infr	1018	コンテンツ配信インフラおよび動的に生成されるコンテンツ、セキュリティで保護されているか、または分類が困難なために細かく分類できない Web サイトなど。	www.akamai.net www.webstat.net
Internet of Things（IoT）	iot	1116	Internet of Things（IoT）およびその他のネットワーク認識型電子機器の設定で、全般的な正常性、アクティビティ、または支援をモニタするために使用されるドメイン。また、これらのサイトでは、ソフトウェアまたはファームウェアの更新を提供したり、デバイスを管理するためのリモート アクセスを許可したりできます。IoT は、プリンタ、テレビ、サーモスタット、システム モニタリング、自動化、スマート アプライアンスなどの製品の消費者とプロフェッショナルの両方のセグメントに存在します。	www.samsungotn.net www.transport.nest.com
インターネット電話（Internet Telephony）	v oip	1067	インターネットを利用した電話サービス。	www.skype.com www.getvoca.com
求職（Job Search）	job	1004	職業に関する助言、履歴書の書き方、面接に関するスキル、就職斡旋サービス、求人データバンク、職業紹介所、人材派遣会社、雇用主の Web サイトなど。	www.careerbuilder.com www.monster.com
下着および水着（Lingerie and Swimsuits）	ling	1031	下着および水着。特にモデルが着用している Web サイト。	www.swimsuits.com www.victoriassecret.com
宝くじ（Lotteries）	lotr	1034	宝くじ、コンテストおよび国が運営する宝くじ。	www.calottery.com www.flalottery.com
[軍（Military）]	mil	1099	武装部隊などの軍隊：軍事基地：軍事組織：テロ対策。	www.goarmy.com www.todaysmilitary.com

URL カテゴリ	省略形	コード	説明	URL の例
携帯電話（Mobile Phones）	cell	1070	ショート メッセージ サービス（SMS）、着信音などの携帯電話用ダウンロード サービス。携帯電話会社の Web サイトは、[ビジネスおよび産業（Business and Industry）] カテゴリに分類されます。	www.cbfsms.com www.zedge.net
博物館	muse	1117	一般的な関心を集めたり、または高い専門性を備えたりするテーマに関する情報を保持することを専門とする、オンラインおよび物理的な博物館と展示品。テーマは、芸術、歴史、科学、または文化的に重要なものです。	www.ushmm.org www.louvre.fr
自然と保護	ncon	1106	天然資源、生態学および自然保護、森林、原生地、植物、草花、森林保護、森林、原生林および林業、森林管理（再生、保護、保全、伐採、森林状態、間伐、計画的火入れ）、農作業（農業、ガーデニング、園芸、造園、種まき、除草、灌漑、剪定、収穫）、環境汚染問題（大気質、有害廃棄物、汚染防止、リサイクル、廃棄物処理、水質、環境産業）に関するサイト。	www.nature.org www.thepottedgarden.co.uk
ニュース（News）	news	1058	ニュース、ヘッドライン、新聞、テレビ局、雑誌、天気、スキー場の状態。	www.cnn.com www.news.bbc.co.uk
非政府組織（Non-Governmental Organizations）	ngo	1087	クラブ、圧力団体、コミュニティ、非営利組織および労働組合などの非政府組織。	www.panda.org www.unions.org
性的でないヌード（Non-Sexual Nudity）	nsn	1060	ヌーディズム、ヌード、自然主義、ヌーディスト キャンプ、芸術的ヌードなど。	www.1001fessesproject.com www.naturistsociety.com
非実用的	nact	1103	検査されたが、到達不能またはカテゴリに割り当てられるコンテンツが不足しているサイト。	—

URL カテゴリ	省略形	コード	説明	URL の例
オンライン コミュニティ（Online Communities）	comm	1024	アフィニティ グループ、Special Interest Group（SIG; 同じ興味を持つ人々の集まり）、Web ニュース グループ、Web 掲示板など。[プロフェッショナルネットワーキング（Professional Networking）] カテゴリまたは[ソーシャルネットワーキング（Social Networking）] カテゴリに分類される Web サイトはここには含まれません。	www.reddit.com www.stackexchange.com
オンライン ドキュメントの共有とコラボレーション	docs	1115	ドキュメントの作成、変換、編集に使用されるクラウドベースのソフトウェア。コラボレーションおよび共有機能は、通常は作成者が設定したアクセス権限で使用できます。ドキュメントはオンラインで保存することも、ダウンロードして使用することもできます。	www.pastebin.com www.docs.google.com
オンライン会議（Online Meetings）	meet	1100	オンライン会議、デスクトップ共有、リモートアクセス、および複数の場所のコラボレーションを容易にするその他のツール。	www.join.me www.teamviewer.com
オンライン ストレージおよびバックアップ（Online Storage and Backup）	osb	1066	バックアップ、共有、およびホスティングを目的とした、オフサイト ストレージおよびピアツーピア型ストレージ	www.adrive.com www.dropbox.com
オンライン トレード（Online Trading）	trad	1028	オンライン証券会社、ユーザがオンラインで株取引できる Web サイト、株式市場、株式、債券、投資信託会社、ブローカー、株式市場の分析と解説、株式審査、株価チャート、IPO、株式分割に関する情報。株式スプレッド ベッティング サービスは [ギャンブル（Gambling）] に分類されます。その他の金融サービスは [財務（Finance）] に分類されます。	www.tdameritrade.com www.etrade.com

URL カテゴリ	省略形	コード	説明	URL の例
業務用電子メール（Organizational Email）	pem	1085	Outlook Web Access（OWA）などで業務用のメールを利用する際に使用する Web サイト。	www.mail.zoho.com www.webmail.edmc.edu
超常現象（Paranormal）	prnm	1101	UFO、幽霊、未確認動物、テレキネシス、都市伝説、神話。	www.ghoststudy.com www.ufocasebook.com
パーク ドメイン（Parked Domains）	park	1092	広告ネットワークの有料リスティング サービスを利用してそのドメインのトラフィックから収益を得ようとする Web サイト、またはドメイン名を販売して収益を得ようと考えている「不正占拠者」が所有する Web サイト。有料広告リンクを返す偽の検索サイトも含まれます。	www.domainzaar.com www.cricketbuzz.com
ピア ファイル転送（Peer File Transfer）	p2p	1056	ピアツーピア型のファイル要求 Web サイト。ファイル転送自体のトラッキングは行いません。	www.bittorrent.com www.torrentdownloads.me
個人サイト（Personal Sites）	pers	1081	個人が運営している個人関連の Web サイト、個人用ホーム ページ サーバ、個人的コンテンツが公開されている Web サイト、特定のテーマがない個人ブログなど。	www.blogmaverick.com www.stallman.org
パーソナル VPN（Personal VPN）	pvpn	1102	バーチャル プライベート ネットワーク（VPN）サイト、または一般的に個人使用向けのツール（法人による使用の可否は場合による）。	www.openvpn.net www.torvpn.com
写真検索と画像	img	1090	画像、写真、クリップ アートの保存と検索を促進します。	www.flickr.com www.photobucket.com
政治（Politics）	pol	1083	政治家、政党、政治、選挙、民主主義、投票などに関連するニュースや情報の Web サイト。	www.politics.com www.gp.org

URL カテゴリ	省略形	コード	説明	URL の例
ポルノ（Pornography）	porn	1054	性的表現が露骨な文章または画像。性的表現が露骨なアニメや漫画、性的表現が露骨な描写全般、フェチ志向の文章や画像、性的表現が露骨なチャット ルーム、セックス シミュレータ、ストリップ ポーカー、アダルト映画、わいせつな芸術、性的表現が露骨な Web メールなど。	www.redtube.com www.youporn.com
ホストとしてのプライベート IP アドレス	piah	1121	URL のホスト部分として使用されるプライベート IP アドレス。プライベート IP アドレスは、境界ルータの背後での内部使用専用であるため、パブリックにルーティングできません。	
プロフェッショナル ネットワーキング（Professional Networking）	pnet	1089	キャリア開発や専門性開発を目的としたソーシャル ネットワーキング。[ソーシャルネットワーキング（Social Networking）] も参照してください。	www.linkedin.com www.europeanpwn.net
不動産（Real Estate）	rest	1045	不動産の検索に役立つ情報、事務所および商業区画、賃貸、アパート、戸建てなどの不動産物件一覧、住宅建築など。	www.realtor.com www.zillow.com
レシピと食品	reci	1105	料理、レシピ、および食品やノンアルコール飲料に関する情報、料理と食品の文化的側面、食生活の説明と守るべきヒント、食品に関する一般的な栄養情報を共有または議論する専門サイト。調理機器および用具の使用および説明。フードセレブ、ライフスタイル、マニアのブログ。	www.allrecipes.com www.seriouseats.com
参照	ref	1017	都道府県および市区町村の案内情報、地図、時刻、参照文献、辞書、図書館など	www.wikipedia.org www.yellowpages.com
地域の制限付きサイト（ドイツ）	xdeu	1125	地方政府の判断により違法である可能性のあるコンテンツが原因でドイツで制限されている URL。	

URL カテゴリ	省略形	コード	説明	URL の例
地域の制限付きサイト（英国）	xgbr	1123	地方政府の判断により違法である可能性があるコンテンツが原因で英国で制限されている URL。	
地域の制限付きサイト（イタリア）	xita	1124	地方政府の判断により違法である可能性のあるコンテンツが原因でイタリアで制限されている URL。	
地域の制限付きサイト（ポーランド）	xpol	1126	地方政府の判断により違法である可能性のあるコンテンツが原因でポーランドで制限されている URL。	www.betsafe62.com www.tornadobet69.com
宗教（Religion）	rel	1086	宗教に関するコンテンツ、宗教に関する情報、宗教団体。	www.religionfacts.com www.religioustolerance.org
SaaS および B2B（SaaS and B2B）	saas	1080	オンライン ビジネス サービス用 Web ポータル、オンライン会議など。	www.netsuite.com www.salesforce.com
子供向け（Safe for Kids）	kids	1057	幼児や児童向けに作成されているか、明示的に幼児や児童向けと認められている Web サイト。	www.discoverykids.com www.nickjr.com
科学技術（Science and Technology）	sci	1012	科学技術（航空宇宙、電子工学、工学、数学など）、宇宙探査、気象学、地理学、環境、エネルギー（化石燃料、原子力、再生可能エネルギー）、通信（電話、電気通信）など。	www.physorg.com www.science.gov
検索エンジンおよびポータル（Search Engines and Portals）	srch	1020	検索エンジンなど、インターネット上の情報にアクセスするための起点となるサイト。	www.bing.com www.google.com
性教育（Sex Education）	sxed	1052	事実に基づいて性的情報を扱う Web サイト、性的健康、避妊、妊娠など	www.avert.org www.scarleteen.com
ショッピング（Shopping）	shop	1005	物々交換、オンライン購入、クーポン、無料提供、事務用品、オンライン カタログ、オンライン モールなど。	www.amazon.com www.shopping.com

URL カテゴリ	省略形	コード	説明	URL の例
ソーシャル ネットワーキング（Social Networking）	snet	1069	ソーシャル ネットワーキング関連。[プロフェッショナルネットワーキング（Professional Networking）] も参照してください。	www.facebook.com www.twitter.com
社会科学（Social Science）	socs	1014	社会に関係する科学と歴史、考古学、文化人類学、カルチュラル スタディーズ、歴史学、言語学、地理学、哲学、心理学、女性学。	www.archaeology.org www.anthropology.net
社会および文化（Society and Culture）	scty	1010	家族および家族関係、民族性、社会組織、家系、高齢者、保育など。	www.childcareaware.org www.familysearch.org
ソフトウェア アップデート（Software Updates）	swup	1053	ソフトウェア パッケージに対する更新プログラムを提供している Web サイト。	www.softwarepatch.com www.windowsupdate.com
スポーツおよびレクリエーション（Sports and Recreation）	sprt	1008	すべてのプロ スポーツおよびアマチュア スポーツ、レクリエーション活動、釣り、ファンタジー スポーツ （ゲーム）、公園、遊園地、レジャープール、テーマ パーク、動物園、水族館、温泉施設など。	www.espn.com www.recreation.gov
ストリーミング オーディオ（Streaming Audio）	aud	1073	リアルタイム ストリーミング オーディオ コンテンツ（インターネット ラジオやオーディオ フィードなど）。	www.live-radio.net www.shoutcast.com
ストリーミング ビデオ（Streaming Video）	vid	1072	リアルタイム ストリーミング ビデオ（インターネット テレビ、Web キャスト、動画共有など）。	www.hulu.com www.youtube.com

URL カテゴリ	省略形	コード	説明	URL の例
テロリズムと暴力的な過激主義	terr	1119	イデオロギーの一環として、死または暴力を助長するテロリストまたは過激派の Web サイト。サイトには、グラフィックや不穏な画像、ビデオおよびテキストが含まれていることがあります。一部のサイトは、テロを支持していないが、暴力的な資料を直接共有している場合もあります。	
タバコ（Tobacco）	tob	1078	愛煙家の Web サイト、タバコ製造会社、パイプ、喫煙製品（違法薬物吸引用でないもの）など。タバコ中毒は [健康と薬（Health and Medicine）] カテゴリに分類されます。	www.bat.com www.tobacco.org
乗り物（Transportation）	trns	1044	個人用の乗り物、自動車およびバイクに関する情報、新車、中古車、オートバイの購入、自動車愛好会、小型船舶、航空機、レジャー用自動車（RV）など。自動車レースおよびバイク レースは [スポーツおよびレクリエーション（Sports and Recreation）] に分類されます。	www.cars.com www.motorcycles.com
旅行（Travel）	trvl	1046	ビジネス旅行と個人旅行、旅行情報、トラベル リソース、旅行代理店、休暇利用のパック旅行、船旅、宿泊施設、交通手段、航空便の予約、航空運賃、レンタカー、別荘など。	www.expedia.com www.lonelyplanet.com
URL 短縮サービス	shrt	1120	長い URL を短縮したり、URL をブランディングしたり、ハイパーリンクの最終的な宛先を隠したりするために使用されるドメイン。	www.bit.ly www.tinyurl.com

URL カテゴリ	省略形	コード	説明	URL の例
武器（Weapons）	weap	1036	一般的な武器の購入および使用に関する情報（銃販売店、銃オークション、銃の案内広告、銃の付属品、銃の展示会、銃の訓練など）、銃に関する全般情報、その他の武器や狩猟関連画像のサイトなども含まれる場合があります。政府の軍に関する Web サイトは、[政府および法律（Government and Law）] カテゴリに分類されます。	www.coldsteel.com www.gunbroker.com
Web キャッシュとアーカイブ	cach	1108	通常、保存またはロード時間の短縮のために格納されるキャッシュまたはアーカイブされた Web コンテンツ。	www.archive.org www.cachedpages.com
Web ホスティング（Web Hosting）	whst	1037	Web サイトのホスティング、帯域幅サービスなど。	www.bluehost.com www.godaddy.com
Web ページ翻訳（Web Page Translation）	tran	1063	Web ページの翻訳。	www.babelfish.com www.translate.google.com
Web-based Email	メールアドレス	1038	Web メール サービス。個人が自分の会社の電子メール サービスを利用するための Web サイトは、[業務用電子メール（Organizational Email）] カテゴリに分類されます。	www.mail.yahoo.com www.outlook.com

関連項目

- URL カテゴリ セットの更新の管理 , on page 21
- 未分類の URL と誤って分類された URL の報告, on page 19

HTTPS トラフィックを制御する復号ポリシーの作成

この章で説明する内容は、次のとおりです。

- ルート証明書 （89 ページ）
- HTTPS トラフィックのルーティング （97 ページ）
- 暗号化/HTTPS/証明書のトラブルシューティング （98 ページ）

HTTPS トラフィックを制御する復号ポリシーの作成：概要

復号ポリシーで、Web プロキシ内の HTTPS トラフィックの処理が定義されます。

- HTTPS トラフィックを復号するタイミング。
- 無効な、または失効したセキュリティ証明書を使用する要求の処理方法。

HTTPS トラフィックを以下のように処理する復号ポリシーを作成できます。

- 暗号化されたトラフィックをパススルーする。
- トラフィックを復号し、HTTP トラフィック用に定義されたコンテンツ ベースのアクセス ポリシーを適用する。これによって、マルウェアスキャンも可能になります

  .
- HTTPS 接続をドロップする。
- Web プロキシがポリシーに対して要求を評価しているときに、要求をモニターする（最終アクションは実行されない）。この評価によって、最終的にドロップ、パススルー、または復号のアクションが実行されます。

Caution **個人識別情報の取り扱いに注意してください。**エンドユーザの HTTPS セッションを復号することを選択した場合は、 Secure Web Applianceのアクセス ログとレポートに個人識別情報が含まれることがあります。管理者は `advancedproxyconfig` CLI コマンドと `HTTPS` サブコマンドを使用して、ログに保存するURIテキストの量を設定できます。URI全体、またはクエリーの部分が除外されたURIの部分的な形式をログに保存できます。ただし、URIからクエリーを削除することを選択した場合でも、個人を特定できる情報は残されたままになる可能性があります。

復号ポリシー タスクによる HTTPS トラフィックの管理の概要

手順	復号ポリシーによる HTTPS トラフィック管理のためのタスク リスト	関連項目および手順へのリンク
1	HTTPS プロキシをイネーブルにする	HTTPS プロキシのイネーブル化, on page 84

手順	復号ポリシーによる HTTPS トラフィック管理のためのタスク リスト	関連項目および手順へのリンク
2	証明書とキーをアップロードまたは生成する	• ルート証明書およびキーのアップロード, on page 92 • HTTPS プロキシ用の証明書およびキーの生成, on page 92
3	復号オプションを設定する	復号オプションの設定, on page 88
5	（任意）無効な証明書の処理を設定する	無効な証明書の処理の設定, on page 93
6	（任意）リアルタイムの失効ステータス チェックをイネーブルにする	リアルタイムの失効ステータス チェックの有効化, on page 95
7	（任意）信頼された証明書とブロックされた証明書を管理する	信頼できるルート証明書, on page 96

復号ポリシーによるHTTPSトラフィックの管理：ベストプラクティス

一般的な復号ポリシー グループを少数作成して、ネットワーク上のすべてのユーザーまたは少数の大きなユーザー グループに適用します。その後、復号された HTTPS トラフィックにきめ細かい管理を適用する必要がある場合は、より具体的なアクセス グループを使用します。

復号ポリシー

アプライアンスは、HTTPS 接続要求に対して、以下のアクションを実行できます。

オプション	説明
モニター（Monitor）	モニター（Monitor）は、最終的に適用される最終アクションを決定するために Web プロキシが他の管理設定に対してトランザクションを評価し続ける必要があることを示す中間のアクションです。
削除（Drop）	アプライアンスは接続をドロップします。サーバーに接続要求を渡しません。アプライアンスは接続をドロップしたことをユーザーに通知しません。

オプション	説明
パススルー（Pass through）	アプライアンスは、トラフィックの内容を検査せずに、クライアントとサーバー間の接続をパススルーします。 ただし、標準のパススルーポリシーを使用している場合、 Secure Web Applianceは要求されたサーバーとのHTTPSハンドシェイクを開始して、このサーバーの有効性をチェックします。有効性チェックでは、サーバー証明書が検証されます。サーバーのチェックが失敗した場合、トランザクションはブロックされます。 特定のサイトの検証チェックをスキップするには、これらのサイトを含むカスタム カテゴリが組み込まれたポリシーを設定して、これらのサイトが信頼できることを示します。これらのサイトは、有効性チェックを受けないでパススルーされます。有効性チェックのスキップを許可するポリシーを設定する場合は、注意してください。
復号（Decrypt）	アプライアンスは、接続を許可しますが、トラフィックの内容を検査します。トラフィックを復号、プレーン テキスト HTTP 接続であるかのように、復号されたトラフィックにアクセス ポリシーを適用します。接続を復号し、アクセス ポリシーを適用することにより、トラフィックをスキャンしてマルウェアを検出できます。

モニター以外のすべての操作は、Webプロキシがトランザクションに適用する「最終アクション」です。最終アクションは、Webプロキシが他の管理設定に対してトランザクションを評価することを停止する操作です。たとえば、復号ポリシーが、無効なサーバー証明書をモニターするように設定されている場合、Webプロキシは、サーバーにある証明書が無効である場合のHTTPSトランザクションの処理方法についての最終決定を行いません。復号ポリシーが、Web レピュテーション スコアが低いサーバーをブロックするように設定されている場合、レピュテーション スコアが低いサーバーに対するすべての要求が URL カテゴリ操作を考慮せずにドロップされます。

次の図に、Web プロキシが復号ポリシー グループに対してクライアント要求を評価する方法を示します。「復号ポリシーアクションの適用」に、復号ポリシーの制御設定を評価するときに Web プロキシで使用する順序が表示されます。Figure 8: アクセス ポリシーのアクションの適用, on page 123には、アクセスポリシーの制御設定を評価するときに Web プロキシで使用する順序が表示されます。

Figure 3: 復号ポリシー アクションの適用

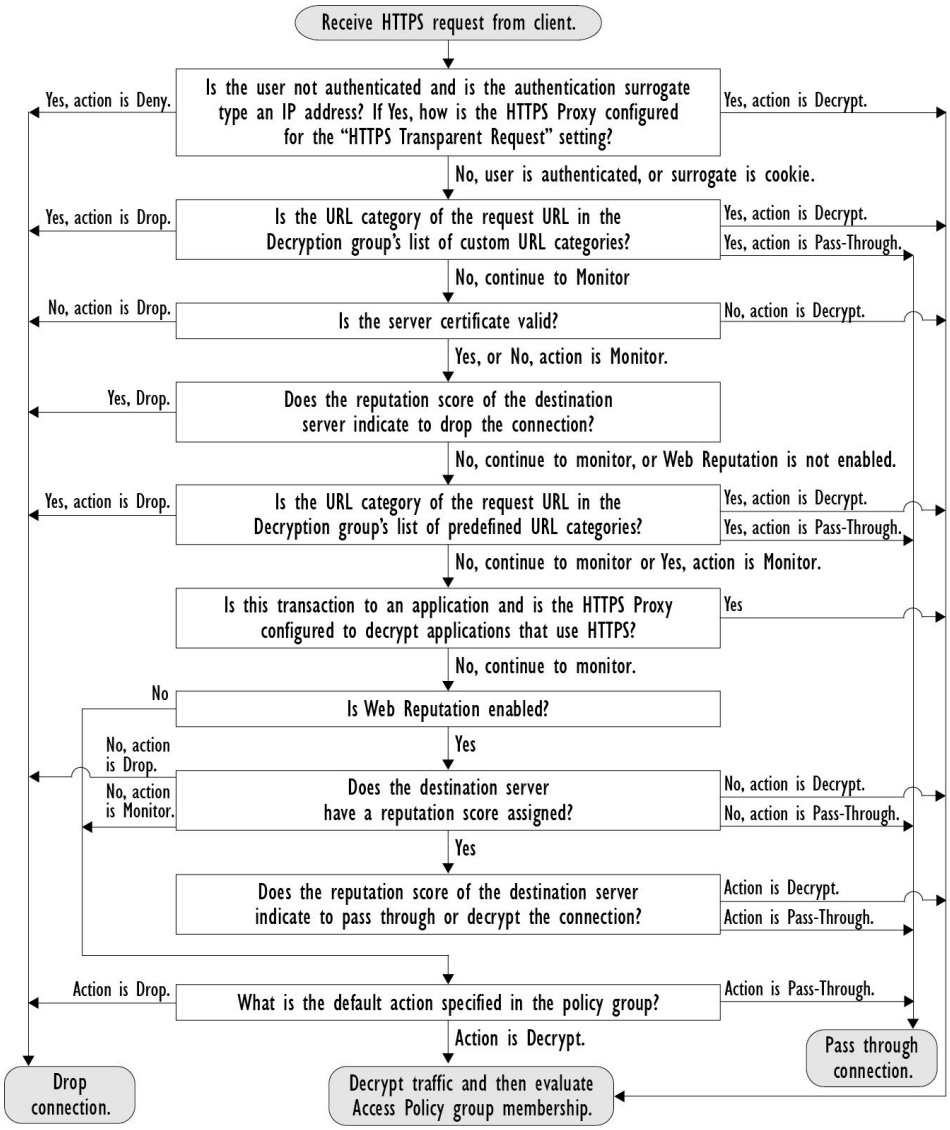
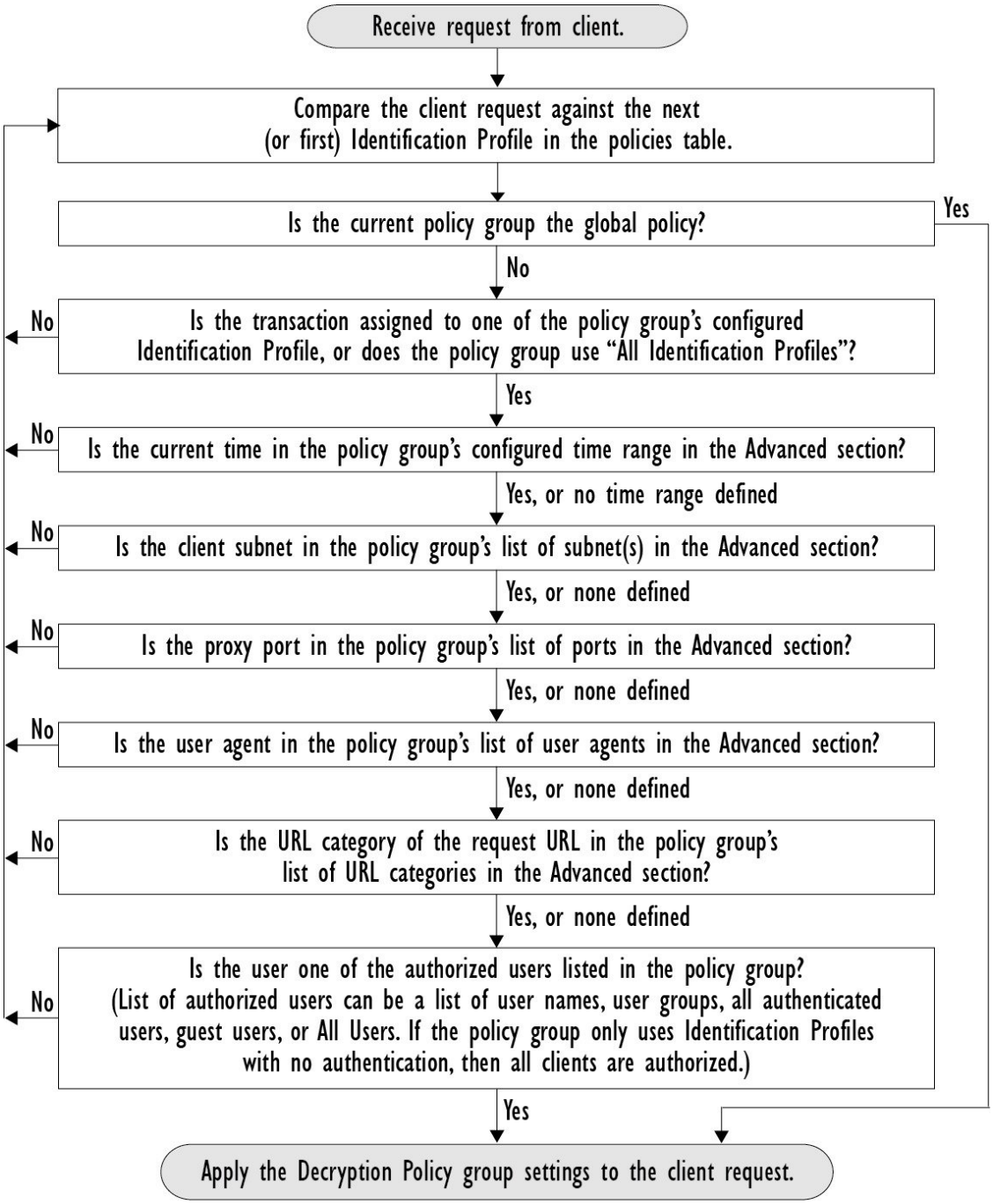


Figure 4: 復号ポリシーのポリシー グループ トランザクション フロー



HTTPS プロキシのイネーブル化

HTTPS トラフィックをモニターして復号するには、HTTPS プロキシをイネーブルにする必要があります。HTTPS プロキシをイネーブルにする場合は、アプライアンスが、ネットワークのクライアント アプリケーションに自己署名済みサーバー証明書を送信するときに使用する

ルート証明書を設定します。組織の既存のルート証明書およびキーをアップロードするか、ユーザーが入力した情報で証明書およびキーを生成するようにアプライアンスを設定することができます。

HTTPS プロキシをイネーブルした後は、すべての HTTPS ポリシー決定が復号ポリシーによって処理されます。また、このページで、サーバー証明書が無効な場合の、アプライアンスによる HTTPS トラフィックの処理も設定できます。

Before you begin

HTTPS プロキシをイネーブルにすると、アクセス ポリシー内の HTTPS 専用のルールがディセーブルになり、Web プロキシは HTTP 用のルールを使用して、復号された HTTPS トラフィックを処理します。

Procedure

ステップ 1 [セキュリティ サービス（Security Services）] > [HTTPS プロキシ（HTTPS Proxy）] に移動し、[設定の有効化と編集（Enable and Edit Settings）] をクリックします。

HTTPS プロキシ ライセンス契約書が表示されます。

ステップ 2 HTTPS プロキシ 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 [HTTPS プロキシを有効にする（Enable HTTPS Proxy）] フィールドがイネーブルであることを確認します。

ステップ 4 [HTTPS ポートからプロキシへ（HTTPS Ports to Proxy）] フィールドに、アプライアンスが HTTPS トラフィックをチェックするポートを入力します。ポート 443 がデフォルト ポートです。

Note
Secure Web Appliance はプロキシとして最大 30 ポートを使用できます。3 ポートは常に FTP プロキシ用に予約されており、27 ポートは HTTP および HTTPS プロキシとして構成できます。

ステップ 5 復号に使用するルート/署名証明書をアップロードまたは生成します。

Note
アップロードされた証明書とキーのペアと、生成された証明書とキーのペアの両方がアプライアンスにある場合は、[署名用ルート証明書（Root Certificate for Signing）] セクションで選択されている証明書とキーのペアのみを使用します。

ステップ 6 [HTTPS 透過的要求（HTTPS Transparent Request）] セクションで、以下のオプションのいずれかを選択します。

- Decrypt the HTTPS request and redirect for authentication（HTTPS 要求を復号して、認証のためにリダイレクトする）
- Deny the HTTPS request（HTTPS 要求を拒否する）

この設定は、認証サロゲートとして IP アドレスを使用するトランザクションだけに、ユーザーがまだ認証されていない場合に適用されます。

Note

このフィールドは、アプライアンスが透過モードで展開されている場合にだけ表示されます。

ステップ 7 [HTTPSを使用するアプリケーション（Applications that Use HTTPS）] セクションで、アプリケーションの可視性とコントロール、およびアプリケーションの検出と制御を向上させるために復号をイネーブルにするかどうか選択します。

Note
署名用ルート証明書がクライアントにインストールされていない場合は、復号により、アプリケーションでエラーが発生することがあります。アプライアンス ルート証明書の詳細については、証明書の検証と HTTPS の復号の管理, on page 91を参照してください。

ステップ 8 変更を送信し、保存します。

What to do next

関連項目

- 証明書の検証と HTTPS の復号の管理, on page 91

HTTPS トラフィックの制御

Secure Web Applianceが復号ポリシー グループに HTTPS 接続要求を割り当てた後、接続要求は、そのポリシー グループの管理設定を継承します。復号ポリシー グループの管理設定で、アプライアンスが接続を復号するか、ドロップするか、またはパススルーするかが決定されます。

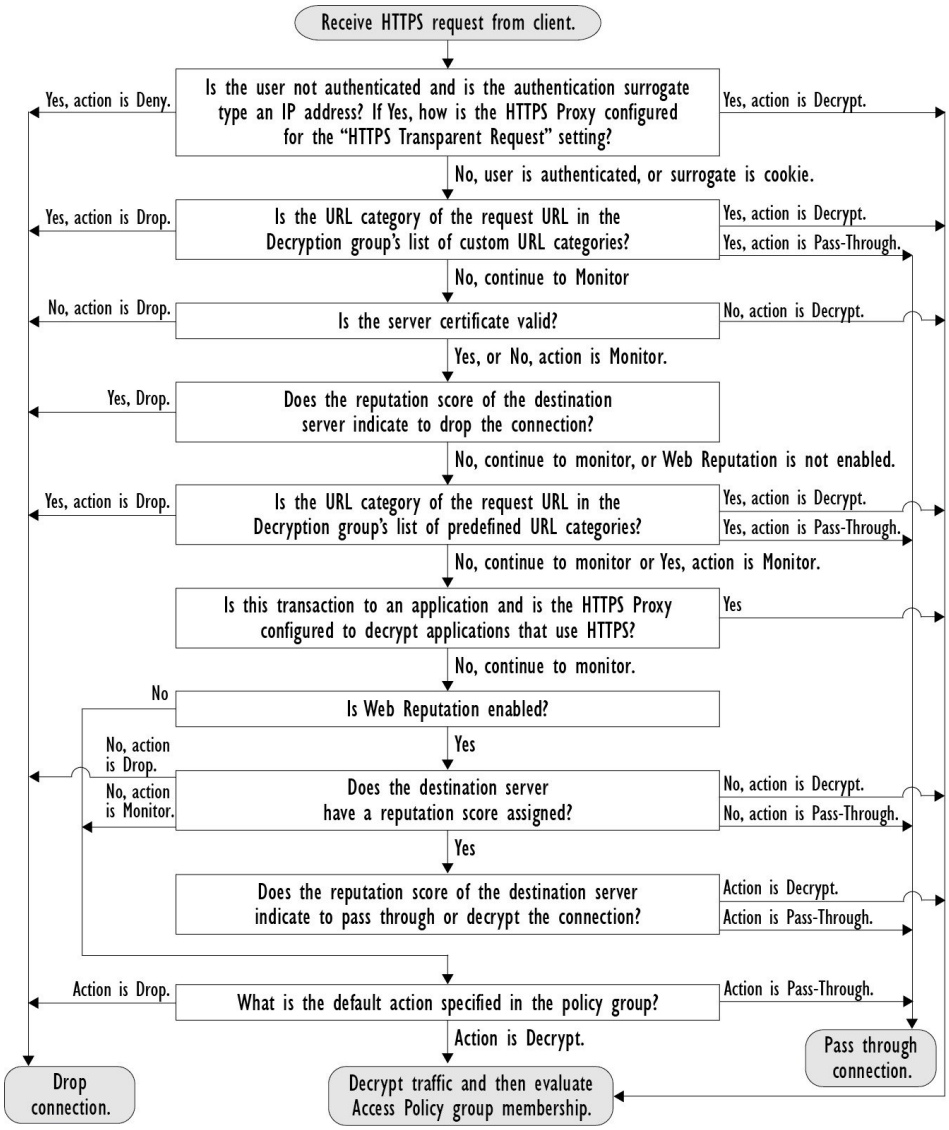
オプション	説明
URL カテゴリ（URL Categories）	定義済みおよびカスタムの各 URL カテゴリについて、HTTPS 要求で実行するアクションを設定できます。[URL フィルタリング（URL Filtering）] 列にある、設定するポリシー グループのリンクをクリックします。 **Note** HTTPS 要求の特定の URL カテゴリをドロップ（エンドユーザー通知なし）するのではなく、ブロック（エンドユーザー通知あり）する場合は、復号ポリシー グループのその URL カテゴリの復号を選択し、その後に、アクセス ポリシー グループの同じ URL カテゴリのブロックを選択します。
Web レピュテーション（Web Reputation）	要求されたサーバーの Web レピュテーション スコアに基づいて、HTTPS 要求に対して実行するアクションを設定できます。[Web レピュテーション（Web Reputation）] 列にある、設定するポリシー グループのリンクをクリックします。

オプション	説明
デフォルト アクション（Default Action）	他に該当する設定がない場合にアプライアンスが実行する必要があるアクションを設定できます。[デフォルト アクション（Default Action）] 列にある、設定するポリシー グループのリンクをクリックします。 **Note** 設定されたデフォルトアクションは、下される決定が、URL カテゴリと Web レピュテーション スコアのどちらにも基づいていない場合にのみ、トランザクションに影響します。Web レピュテーション フィルタリングがディセーブルの場合は、デフォルト アクションが、URL カテゴリの Monitor アクションに一致するすべてのトランザクションに適用されます。Web レピュテーション フィルタリングがイネーブルの場合は、スコアなしのサイトに Monitor アクションが選択されている場合にのみ、デフォルト アクションが使用されます。

Web レピュテーションスコアが高い暗号化トラフィックをバイパスするには、[HTTPSプロキシ設定（HTTPS Proxy Settings）] ページの [復号オプション（Decryption Options）] セクションにある [アプリケーション検出のための復号（Decrypt for Application Detection）] オプションをオフにしてください。

次の図に、アプライアンスが特定の復号ポリシーを HTTPS 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。たとえば、Web レピュテーション スコアのドロップ アクションは、定義済みの URL カテゴリに指定されているあらゆるアクションに優先することに注意してください。

Figure 5: 復号ポリシー アクションの適用



復号オプションの設定

Before you begin

HTTPS プロキシのイネーブル化, on page 84で説明したように、HTTPS プロキシがイネーブルであることを確認します。

Procedure

ステップ 1 [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。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 復号オプションをイネーブルにします。

Note
このオプションを有効化すると、一部のHTTPSアプリケーションの検出効率が向上します。ただし、署名用ルート証明書がクライアントにインストールされていない場合は、復号によりその他の HTTPS アプリケーションでエラーが発生することがあります。使用許可コントロールで ADC または AVC を選択すると、アプリケーション識別のために復号されます。

復号オプション	説明
認証のための復号	この HTTPS トランザクションの前に認証されていないユーザーに復号を許可して、認証されるようにします。
エンドユーザー通知のための復号	AsyncOS がエンド ユーザー通知を表示できるように復号を許可します。 **Note** 証明書が無効であり、無効な証明書をドロップするように設定されている場合は、最初にロギングされたトランザクションのアクションがポリシー トレースの実行時に「復号」されます。
エンドユーザー確認応答のための復号	この HTTPS トランザクションの前に Web のプロキシに確認応答していないユーザーに復号を許可し、AsyncOS がエンドユーザーの確認応答を表示できるようにします。
アプリケーション検出のための復号	AsyncOS が HTTPS アプリケーションを検出する機能を強化します。

認証および HTTPS 接続

HTTPS 接続レイヤでの認証は、以下のタイプの要求で使用できます。

オプション	説明
明示的要求（Explicit requests）	• セキュア クライアント認証がディセーブルである、または • セキュア クライアント認証がイネーブルで、サロゲートが IP ベースである
透過的要求（Transparent requests）	• サロゲートが IP ベースで、認証の復号がイネーブル、または • サロゲートが IP ベースで、クライアントが以前に HTTP 要求を使用して認証されている

ルート証明書

HTTPS プロキシは、アプライアンスにアップロードした秘密キー ファイルとルート証明書を使用して、トラフィックを復号します。アプライアンスにアップロードするルート証明書ファ

イルと秘密キー ファイルは、PEM 形式である必要があります。DER 形式はサポートされていません。

ルート証明書の情報は、以下のように入力できます。

- **生成する。**基本的な設定情報を入力してから、ボタンをクリックすると、アプライアンスが、残りの証明書と秘密キーを生成します。
- **アップロードする。**アプライアンスの外部で作成された証明書ファイルと、それに一致する秘密キー ファイルをアップロードできます。

Note また、ルート認証局によって署名された中間証明書をアップロードすることもできます。Web プロキシがサーバー証明書を模倣すると、アップロードされた証明書とともに、模倣された証明書がクライアントアプリケーションに送信されます。このように、クライアントアプリケーションが信頼するルート認証局によって中間証明書が署名されている限り、アプリケーションは模倣されたサーバー証明書も信頼します。詳細については、証明書およびキーについてを参照してください。

Secure Web Applianceが作成したルート証明書を処理する場合は、以下のいずれかを選択できます。

- **ルート証明書を受け入れるようにユーザーに通知します。**組織内のユーザーに、企業の新しいポリシーについて通知し、組織が提供したルート証明書を、信頼できる認証局として受け入れるように指示できます。
- **クライアント マシンにルート証明書を追加します。**ネットワーク上のすべてのクライアントマシンに、信頼できるルート認証局としてルート証明書を追加できます。そうすれば、クライアントアプリケーションは自動的にルート証明書を持つトランザクションを受け入れるようになります。

Procedure

ステップ 1 [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。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 生成またはアップロードされた証明書の [証明書のダウンロード（Download Certificate）] リンクをクリックします。

Note
クライアント マシンで証明書エラーが表示される可能性を減らすには、 Secure Web Applianceにルート証明書を生成またはアップロードした後に変更を送信してから、クライアント マシンに証明書を配布し、その後にアプライアンスへの変更をコミットします。

証明書の検証と HTTPS の復号の管理

Secure Web Applianceは証明書を検証してから、コンテンツを検査して復号します。

有効な証明書

有効な証明書の条件：

- **有効期限が切れていない。**現在の日付が証明書の有効期間内です。
- **公認の認証局である。**発行認証局は、 Secure Web Applianceに保存されている、信頼できる認証局のリストに含まれています。
- **有効な署名がある。**デジタル署名が、暗号規格に基づいて適切に実装されています。
- **名前が一貫している。**通常名が、HTTP ヘッダーで指定されたホスト名に一致します。
- **失効していない。**発行認証局が証明書を無効にしていません。

関連項目

- リアルタイムの失効ステータス チェックの有効化, on page 95
- 無効な証明書の処理の設定, on page 93
- 証明書失効ステータスのチェックのオプション, on page 94

無効な証明書の処理

アプライアンスは、無効なサーバー証明書に対して、以下のアクションの 1 つを実行できます。

- **切断。**
- **復号。**
- **モニタ。**

複数の理由で無効となる証明書

認識できないルート認証局と期限切れ証明書の両方の理由により無効なサーバー証明書に対して、HTTPS プロキシは、認識できないルート認証局に適用されるアクションを実行します。

それ以外のすべての場合は、同時に複数の理由により無効なサーバー証明書に対して HTTPS プロキシは、制限レベルが最高のアクションから最低のアクションへの順にアクションを実行します。

復号された接続の、信頼できない証明書の警告

Secure Web Applianceが無効な証明書を検出し、接続を復号するように設定されている場合、AsyncOS は、信頼できない証明書を作成します。エンド ユーザは、これを受け入れるか、拒否する必要があります。証明書の一般名は「Untrusted Certificate Warning」です。

この信頼できない証明書を信頼できる証明書のリストに追加すると、エンドユーザーは接続を受け入れるか拒否するかを選択できなくなります。

AsyncOS は、これらの証明書のいずれかを生成するときに、「Signing untrusted key」または「Signing untrusted cert」というテキストのプロキシ ログ エントリを作成します。

ルート証明書およびキーのアップロード

Before you begin

HTTPS プロキシをイネーブルにします。HTTPS プロキシのイネーブル化, on page 84。

Procedure

ステップ 1 [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。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [アップロードされた証明書とキーを使用（Use Uploaded Certificate and Key）] を選択します。

ステップ 4 [証明書（Certificate）] フィールドで [参照（Browse）] をクリックし、ローカルマシンに保存されている証明書ファイルに移動します。

アップロードするファイルに複数の証明書またはキーが含まれている場合、Web プロキシはファイル内の先頭の証明書またはキーを使用します。

ステップ 5 [キー（Key）] フィールドで [参照（Browse）] をクリックし、秘密キー ファイルに移動します。

Note
キーの長さは 512、1024、または 2048 ビットである必要があります。

ステップ 6 キーが暗号化されている場合は、[キーは暗号化されています（Key is Encrypted）] を選択します。

ステップ 7 [ファイルのアップロード（Upload Files）] をクリックして、証明書およびキーのファイルを Secure Web Applianceに転送します。

アップロードされた証明書の情報が [HTTPS プロキシ設定を編集（Edit HTTPS Proxy Settings）] ページに表示されます。

ステップ 8 （任意）[証明書のダウンロード（Download Certificate）] をクリックすると、ネットワーク上のクライアント アプリケーションに証明書を転送できます。

ステップ 9 変更を送信し、保存します。

HTTPS プロキシ用の証明書およびキーの生成

Before you begin

HTTPS プロキシをイネーブルにします。HTTPS プロキシのイネーブル化, on page 84。

Procedure

ステップ 1 [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。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [生成された証明書とキーを使用（Use Generated Certificate and Key）] を選択します。

ステップ 4 [新しい証明書とキーを生成（Generate New Certificate and Key）] をクリックします。

ステップ 5 [証明書とキーを生成（Generate Certificate and Key）] ダイアログボックスで、ルート証明書に表示する情報を入力します。

[共通名（Common Name）] フィールドには、スラッシュ（/）を除く任意の ASCII 文字を入力できます。

ステップ 6 [生成（Generate）] をクリックします。

ステップ 7 生成された証明書の情報が [HTTPS プロキシ設定を編集（Edit HTTPS Proxy Settings）] ページに表示されます。

ステップ 8 （任意）[証明書のダウンロード（Download Certificate）] をクリックすると、ネットワーク上のクライアント アプリケーションに証明書を転送できます。

ステップ 9 （任意）[証明書署名要求のダウンロード（Download Certificate Signing Request）] リンクをクリックすると、証明書署名要求（CSR）を認証局（CA）に送信できます。

ステップ 10 （任意）CA から署名付き証明書を受信した後、それを Secure Web Applianceにアップロードします。この操作は、アプライアンスで証明書を生成した後はいつでも実行できます。

ステップ 11 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

無効な証明書の処理の設定

Before you begin

HTTPS プロキシのイネーブル化, on page 84で説明したように、HTTPS プロキシがイネーブルであることを確認します。

Procedure

ステップ 1 [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。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 証明書エラーのタイプごとに、プロキシの応答（**ドロップ**、**復号**、**モニター**）を定義します。

証明書エラーのタイプ	説明
期限切れ	現在の日付が、証明書の有効範囲外にあります。

証明書エラーのタイプ	説明
ホスト名の不一致	証明書にあるホスト名が、クライアントがアクセスしようとしたホスト名に一致しません。 **Note** 明示的な転送モードで展開されている場合にのみ、Web プロキシはホスト名の照合を実行できます。透過モードで展開されている場合は、宛先サーバーのホスト名がわからない（わかっているのは IP アドレスのみです）ため、ホスト名をサーバー証明書のホスト名と比較できません。
認識できないルート認証局/発行元	ルート認証局または中間認証局が認識されません。
無効な署名証明書	署名証明書に問題があります。
無効なリーフ証明書	リーフ証明書に、拒否、でコード、または不一致などの問題が発生しました。
その他のエラー タイプ	他のほとんどのエラー タイプは、アプライアンスが HTTPS サーバーとの SSL ハンドシェイクを完了できないことが原因です。サーバー証明書の詳細なエラー シナリオに関する情報については、http://www.openssl.org/docs/apps/verify.html を参照してください。

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）]）。

証明書失効ステータスのチェックのオプション

発行認証局が証明書を失効させたかどうかを特定するために、 Secure Web Applianceでは、次の方法で発行認証局をチェックできます。

- **証明書失効リスト（Comodo 証明書のみ）。** Secure Web ApplianceはComodo の証明書失効リストをチェックします。Comodo は、このリストを独自のポリシーに従って更新して維持します。最後に更新された日時によっては、 Secure Web Applianceがチェックした時点では、証明書失効リストが古くなっている可能性があります。
- **オンライン証明書ステータス プロトコル（OCSP）。** Secure Web Applianceが、発行認証局で失効ステータスをリアルタイムでチェックします。発行認証局がOCSP をサポートしている場合は、リアルタイム ステータス チェック用の URL が証明書に含まれています。この機能は、新規インストールではデフォルトでイネーブルになり、更新ではデフォルトでディセーブルになります。

Note Secure Web Applianceは、他のすべての点で有効であることを特定し、OCSP URL を含んでいる証明書の OCSP クエリーのみを実行します。

関連項目

- リアルタイムの失効ステータス チェックの有効化, on page 95
- 無効な証明書の処理の設定, on page 93

リアルタイムの失効ステータス チェックの有効化

Before you begin

HTTPS プロキシがイネーブルであることを確認します。HTTPS プロキシのイネーブル化, on page 84を参照してください。

Procedure

ステップ 1 [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。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [オンライン証明書ステータス プロトコル（OCSP）を有効にする（Enable Online Certificate Status Protocol (OCSP)）] を選択します。

ステップ 4 [OCSP結果処理（Result Handling）] の各プロパティを設定します。

シスコでは、OCSP 結果処理のオプションを、無効な証明書の処理のオプションと同じアクションに設定することを推奨します。たとえば、[モニターする期限切れ証明書（Expired Certificate to Monitor）] を設定する場合は、モニターする失効証明書を設定します。

ステップ 5 （任意）[詳細（Advanced）] 設定セクションを展開し、以下の設定項目を設定します。

フィールド名	説明
OSCP 有効応答キャッシュ タイムアウト（OCSP Valid Response Cache Timeout）	有効なOCSP応答を再確認する前に待機する時間。単位は秒（s）、分（m）、時間（h）、または日（d）。デフォルトの単位は秒です。有効な範囲は 1 秒～ 7 日です。
OSCP 無効応答キャッシュ タイムアウト（OCSP Invalid Response Cache Timeout）	無効なOCSP応答を再確認する前に待機する時間。単位は秒（s）、分（m）、時間（h）、または日（d）。デフォルトの単位は秒です。有効な範囲は 1 秒～ 7 日です。
OSCP ネットワーク エラーキャッシュタイムアウト（OCSP Network Error Cache Timeout）	応答がなかった後に、OCSP 応答側に連絡を再度試みる前に待機する時間。単位は秒（s）、分（m）、時間（h）、または日（d）。有効な範囲は 1 秒～ 24 時間です。

フィールド名	説明
許容されるクロックスキュー（Allowed Clock Skew）	Secure Web Applianceと OCSP 応答側の間で許容される設定時間の差の最大値。単位は秒（s）または分（m）。有効な範囲は 1 秒～ 60 分です。
OSCP 応答待機最大時間（Maximum Time to Wait for OCSP Response）	OCSP 応答側からの応答を待機する時間の最大値。有効な範囲は 1 秒～ 10 分です。OCSP レスポンダを使用できない場合に、HTTPS 要求へのエンドユーザーアクセスの遅延を短縮するには、短い期間を指定します。
OSCP チェックにアップストリームプロキシを使用（Use upstream proxy for OCSP checking）	アップストリーム プロキシのグループ名。
アップストリームプロキシから除外するサーバー（Servers exempt from upstream proxy）	除外するサーバーの IP アドレスまたはホスト名。空白のままにすることもできます。

ステップ 6 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

信頼できるルート証明書

Secure Web Applianceには、信頼できるルート証明書のリストが付属し、これが維持されます。信頼できる証明書を持つ Web サイトでは、復号は必要ありません。

信頼できる証明書のリストに証明書を追加し、機能的に証明書を削除すると、信頼できる証明書のリストを管理できます。 Secure Web Applianceでは、プライマリリストから証明書は削除されませんが、ユーザーが証明書の信頼を無効化できます。これで、信頼できるリストから証明書が機能的に削除されます。

信頼できるリストへの証明書の追加

Before you begin

HTTPS プロキシがイネーブルであることを確認します。HTTPS プロキシのイネーブル化, on page 84を参照してください。

Procedure

ステップ 1 [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。

ステップ 2 [信頼できるルート証明書の管理（Manage Trusted Root Certificates）] をクリックします。

ステップ 3 [インポート（Import）] をクリックします。

ステップ 4 [参照（Browse）] をクリックして証明書ファイルに移動します。

ステップ 5 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

[カスタム信頼済みルート証明書（Custom Trusted Root Certificates）] リストで、アップロードした証明書を探します。

信頼できるリストからの証明書の削除

Procedure

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

ステップ 2 [信頼できるルート証明書の管理（Manage Trusted Root Certificates）] をクリックします。

ステップ 3 リストから削除する証明書に対応する [信頼をオーバーライド（Override Trust）] チェックボックスを選択します。

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）]）。

HTTPS トラフィックのルーティング

クライアントのヘッダーに保存されている情報に基づいてHTTPSトランザクションをルーティングする AsyncOS の機能は限定的であり、透過 HTTPS と明示 HTTPS で異なります。

オプション	説明
透過 HTTPS	透過 HTTPS の場合は、AsyncOS がクライアントのヘッダー情報にアクセスできません。したがって、ルーティングポリシーまたは識別プロファイルがクライアントヘッダー内の情報に依存している場合、AsyncOS はルーティングポリシーを適用できません。
明示 HTTPS	明示 HTTPS の場合、AsyncOS は、クライアント ヘッダー内の以下の情報にアクセスできます。 • URL • 宛先ポート番号 したがって、明示 HTTPS トランザクションでは、URL またはポート番号に基づいてルーティング ポリシーを照合できます。

暗号化/HTTPS/証明書のトラブルシューティング

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

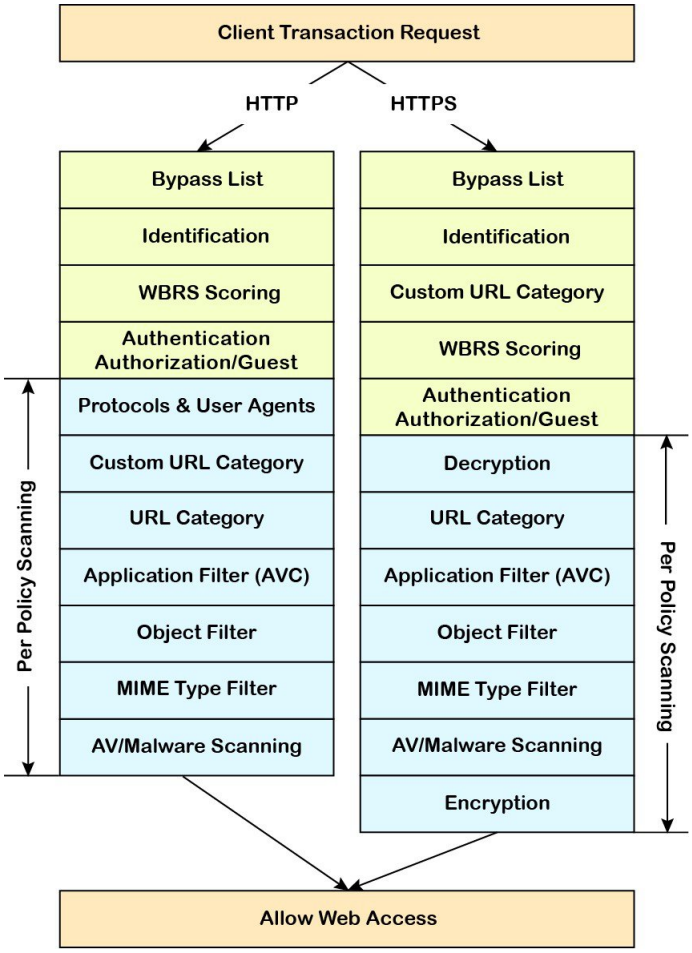
のポリシー タイプにトランザクションを渡します。ポリシー タイプは、実行する機能（アクセス、ルーティング、セキュリティなど）によってグループ化できます。

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。

***Figure 6: 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。

- Figure 1: 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, on page 14
- Figure 2: 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, on page 15

- Figure 7: 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, on page 105
- Figure 4: 復号ポリシーのポリシー グループ トランザクション フロー, on page 84
- HTTPS トラフィックの制御, on page 86

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	（オプション）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, on page 124
3	（オプション）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, on page 41
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, on page 3
5	（オプション）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, on page 125
[6]	ポリシーを作成して順序付ける	• ポリシーの作成 , on page 105 • ポリシーの順序, on page 104

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, on page 101
- ポリシーの順序, on page 104
- ポリシーの作成 , on page 105

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	• HTTP • 復号された HTTPS • FTP	HTTP、FTP、復号 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 , on page 105
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 , on page 105
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, on page 140
暗号化 HTTPS 管理（Encrypted HTTPS Management）	• HTTPS	HTTPS 接続を復号、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 , on page 105

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 , on page 105
外部 DLP（データ漏洩防止）（External DLP (Data Loss Prevention)）	• HTTP • 復号された 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 , on page 105
発信マルウェア スキャン（Outbound Malware Scanning）	• HTTP • 復号された 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 , on page 105

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（Routing）	• 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 , on page 105

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。

Note 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。

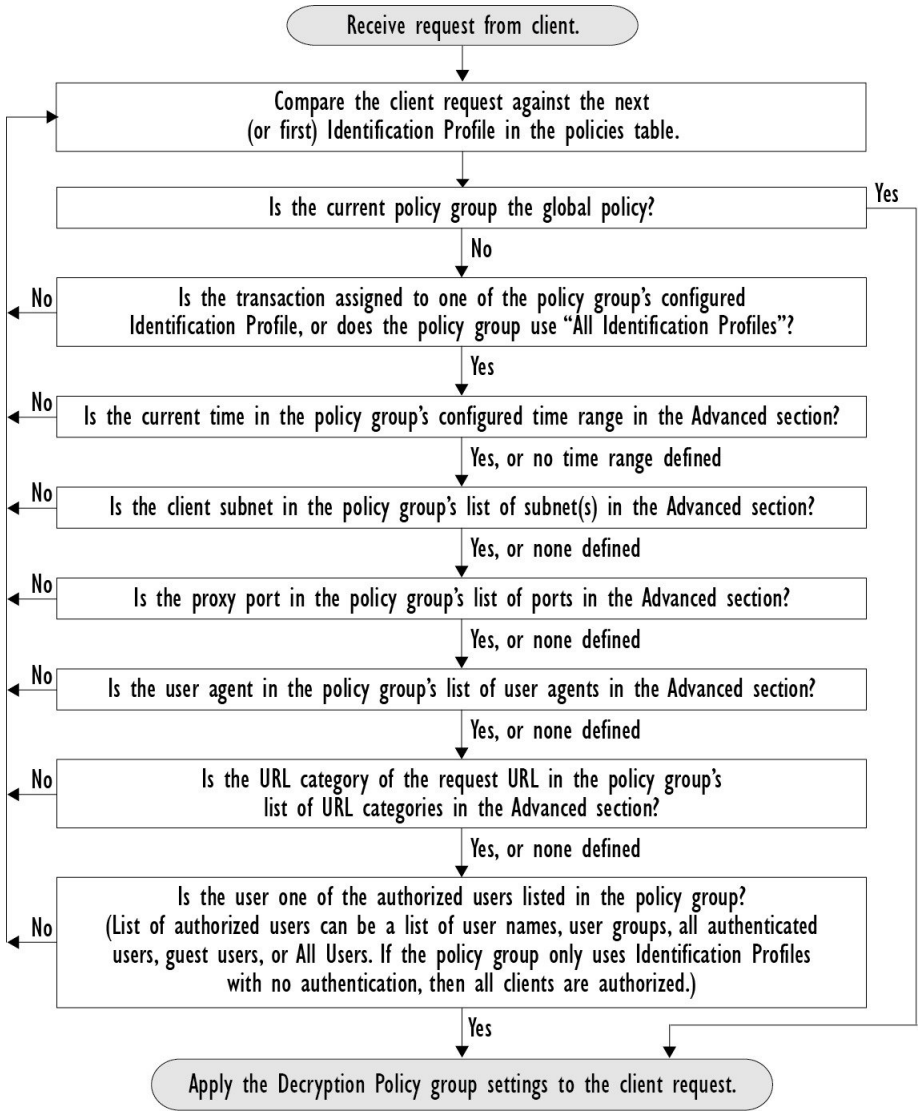
ポリシーの順序

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。

Figure 7: 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

Before you begin

- 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, on page 104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。
- （オプション）関連するクライアント アプリケーションを作成します。
- （オプション）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, on page 125を参照してください。
- （オプション）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, on page 41を参照してください。

Procedure

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。

Note
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, on page 104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。

Note
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。

Note

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, on page 110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, on page 110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（Protocols）	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。 **Note** 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。

高度なオプション	説明
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。 **Note** 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。
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, on page 125）。 • [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, on page 41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 , on page 105 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。

Procedure

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。

Note

- 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。

What to do next

関連項目

- 時間範囲およびクォータ, on page 125
- ポリシーでのクライアント アプリケーションの使用, on page 124

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。

Note

- 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。

Note 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。

Procedure

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（Direct Connection）]	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。
[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。

What to do next

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。

Note 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。
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, on page 41 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。

オプション	説明
アプリケーション（Applications）	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 **Note** 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（Objects）	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。Advanced Malware Protection 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 • ID • ルーティング（Routing） • 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 **Note** 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。

手順

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（120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 [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（116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。

手順

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,on page 53を参照）。

Note 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。

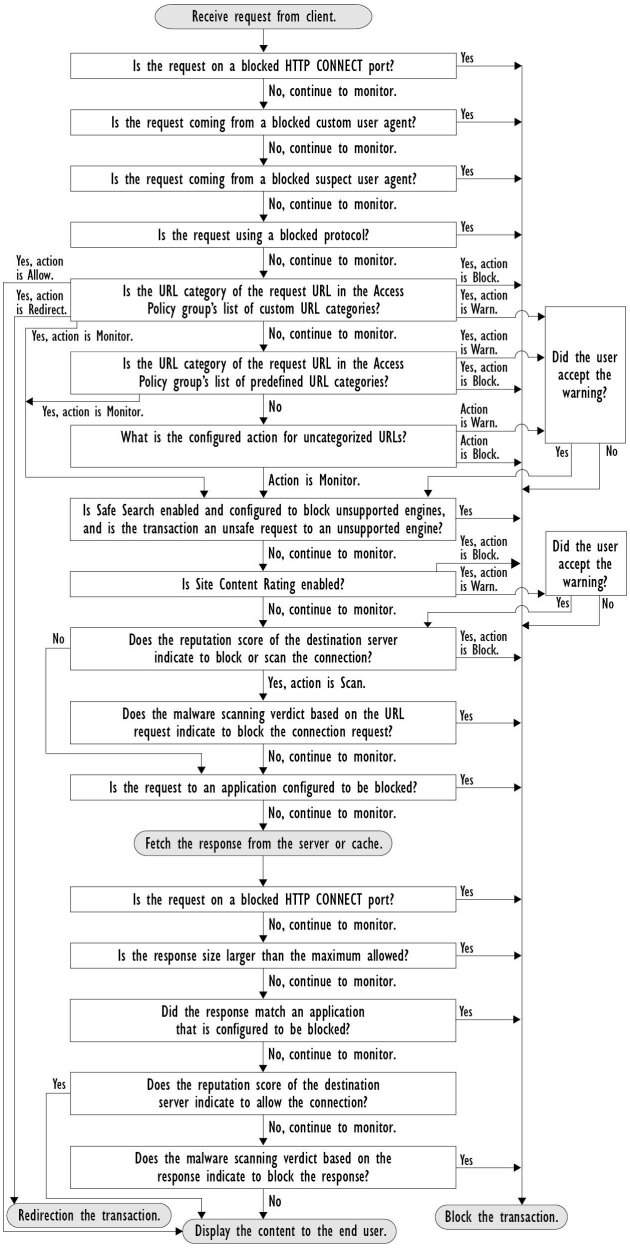
通常、トラフィックは、トランスポートプロトコルに基づいて、さまざまなタイプのポリシーにより制御されます。

ポリシー タイプ	プロトコル（Protocols）				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（Redirect）	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（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（Routing）	x	x	x				x	

Note 復号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。

Figure 8: 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

Procedure

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。 **Tip** 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。 **Tip** 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

Procedure

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。

Tip
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

Procedure

	Command or Action	Purpose
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, on page 3
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, on page 124
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, on page 104

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, on page 126

• 時間およびボリューム クォータ, on page 127

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。

Note 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, on page 126

時間範囲の作成

Procedure

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。

Tip
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。

Note 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, on page 128
- 時間クォータの計算, on page 128

• 時間、ボリューム、および帯域幅のクォータの定義, on page 128

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。

Note 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

Before you begin

- [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。

Procedure

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。

Note
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/監視（Decrypt/Monitor）] および [監視（Monitor）] に設定されています。
  - 復号ポリシー：復号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。

Note

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。

What to do next

（オプション）[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, on page 41 を参照してください。

URL カテゴリによる Web 要求の識別

Before you begin

- 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 , on page 20 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, on page 41 を参照）。

Procedure

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

Before you begin

- 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 , on page 20 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, on page 41を参照）。

Note 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。

Procedure

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。

Note
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, on page 133
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, on page 3 **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 , on page 105

リモート ユーザーの ID の設定

Procedure

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。	**a.** [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。 **b.** 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。	**a.** Cisco ASA のホスト名または IP アドレスを入力します。 **b.** 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。 **c.** 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。 **Note** 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。 **d.** Cisco ASA のアクセス パスフレーズを入力します。 **Note** 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。 **e.** （オプション）[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）]）。

Note
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

• HTTPS に対してアクセス ポリシーを設定できない
• 一部の Microsoft Office ファイルがブロックされない
• DOS の実行可能オブジェクト タイプをブロックすると、Windows OneCare のアップデートがブロックされる
• 識別プロファイルがポリシーから削除される
• ポリシーが適用されない
• HTTPS および FTP over HTTP 要求が、認証を必要としないアクセス ポリシーにのみ一致する
• HTTPS 要求および FTP over HTTP 要求の場合にユーザーがグローバル ポリシーに一致
• ユーザーに誤ったアクセス ポリシーが割り当てられる
• ポリシーのトラブルシューティング ツール：ポリシー トレース

SaaS アクセス コントロール

この章で説明する内容は、次のとおりです。

• SaaS アクセス コントロールの概要 （136 ページ）
• ID プロバイダとしてのアプライアンスの設定 （137 ページ）

- SaaS アクセス コントロールと複数のアプライアンスの使用 （140 ページ）
- SaaS アプリケーション認証ポリシーの作成 （140 ページ）
- シングル サイン オン URL へのエンドユーザー アクセスの設定 （143 ページ）

SaaS アクセス コントロールの概要

Secure Web Applianceは、セキュリティアサーションマークアップ言語（SAML）を使用して、SaaS アプリケーションへのアクセスを許可します。SAML バージョン 2.0 に厳密に準拠している SaaS アプリケーションで動作します。

Cisco SaaS アクセス コントロールによって、以下のことが可能になります。

- SaaS アプリケーションにアクセスできるユーザーおよび場所を制御する。
- ユーザーが組織を退職した時点で、すべての SaaS アプリケーションへのアクセスをただちに無効にする。
- ユーザーに SaaS ユーザー クレデンシャルの入力を求めるフィッシング攻撃のリスクを軽減する。
- ユーザーを透過的にサインインさせるか（シングル サイン オン機能）、ユーザーに認証ユーザー名とパスフレーズの入力を求めるかを選択する。

SaaS アクセスコントロールは、 Secure Web Applianceがサポートしている認証メカニズムを必要とする SaaS アプリケーションでのみ動作します。現在、Web プロキシは「PasswordProtectedTransport」認証メカニズムを使用しています。

SaaS アクセスコントロールをイネーブルにするには、 Secure Web Applianceと SaaS アプリケーションの両方の設定を行う必要があります。

Procedure

	Command or Action	Purpose
ステップ 1	Secure Web Applianceを ID プロバイダーとして設定する。	ID プロバイダとしてのアプライアンスの設定, on page 137
ステップ 2	SaaS アプリケーションの認証ポリシーを作成します。	SaaS アプリケーション認証ポリシーの作成, on page 140
ステップ 3	SaaS アプリケーションをシングル サイン オン用に設定します。	シングル サイン オン URL へのエンドユーザー アクセスの設定, on page 143
ステップ 4	（任意）複数の Secure Web Applianceを設定する。	SaaS アクセス コントロールと複数のアプライアンスの使用, on page 140

ID プロバイダとしてのアプライアンスの設定

Secure Web Applianceを ID プロバイダーとして設定する場合、定義する設定は通信するすべての SaaS アプリケーションに適用されます。 Secure Web Applianceは、作成する各 SAML アサーションに署名するために証明書とキーを使用します。

Before you begin

- （オプション）SAML アサーションに署名するための証明書（PEM 形式）とキーを検索します。
- 各 SaaS アプリケーションに証明書をアップロードします。

Procedure

ステップ 1 [ネットワーク（Network）] > [SaaS の ID プロバイダ（Identity Provider for SaaS）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [SaaS シングルサインオンサービスを有効にする（Enable SaaS Single Sign-on Service）] をオンにします。

ステップ 4 [アイデンティティ プロバイダのドメイン名（Identity Provider Domain Name）] フィールドに仮想ドメイン名を入力します。

ステップ 5 [アイデンティティ プロバイダのエンティティ ID（Identity Provider Entity ID）] フィールドに、一意のテキスト識別子を入力します（URI 形式の文字列を推奨）。

ステップ 6 証明書とキーをアップロードまたは生成します。

方法	この他の手順
証明書およびキーのアップロード	**a.** [アップロードされた証明書とキーを使用（Use Uploaded Certificate and Key）] を選択します。 **b.** [証明書（Certificate] フィールドで [参照（Browse）]をクリックし、アップロードするファイルを検索します。 **Note** Web プロキシは、ファイル内の最初の証明書またはキーを使用します。証明書ファイルは PEM 形式にする必要があります。DER 形式はサポートされていません。 **c.** [キー（Key）] フィールドで [参照（Browse）] をクリックし、アップロードするファイルを指定します。 キーが暗号化されている場合は、[キーは暗号化されています（Key is Encrypted）] を選択します。 **Note** キーの長さは 512、1024、または 2048 ビットである必要があります。秘密キーファイルは PEM 形式でなければなりません。DER 形式はサポートされていません。 **d.** [ファイルのアップロード（Upload File）] をクリックします。 **e.** [証明書をダウンロード（Download Certificate）] をクリックして、 Secure Web Appliance が通信する SaaS アプリケーションに転送する証明書のコピーをダウンロードします。

方法	この他の手順
証明書およびキーの生成	**a.** [生成された証明書とキーを使用（Use Generated Certificate and Key）] を選択します。 **b.** [新しい証明書とキーを生成（Generate New Certificate and Key）] をクリックします。 **1.** [証明書とキーを生成（Generate Certificate and Key）] ダイアログボックスで、署名付き証明書に表示する情報を入力します。 **Note** [共通名（Common Name）] フィールドには、スラッシュ（/）を除く任意の ASCII 文字を入力できます。 **2.** [生成（Generate）] をクリックします。 **c.** [証明書をダウンロード（Download Certificate）] をクリックして、 Secure Web Applianceが通信する SaaS アプリケーションに証明書を転送します。 **d.** （オプション）署名付き証明書を使用するには、[証明書署名要求のダウンロード（Download Certificate Signing Request）]（DCSR）リンクをクリックして、認証局（CA）に要求を送信します。CA から署名付き証明書を受信したら、[参照（Browse）] をクリックし、署名付き証明書の場所に移動します。[ファイルのアップロード（Upload File）] をクリックします。（バグ 37984）

Note
アップロードされた証明書とキーのペアと、生成された証明書とキーのペアの両方がアプライアンスにある場合、アプライアンスは、[署名証明書（Signing Certificate）] セクションで現在選択されている証明書とキーのペアのみを使用します。

ステップ 7 アプライアンスを ID プロバイダとして設定する場合は、設定を書き留めておきます。これらの設定の一部は、SaaS アプリケーションをシングル サイン オン用に設定する際に使用する必要があります。

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

What to do next

SAML アサーションの署名に使用する証明書とキーを指定したら、各 SaaS アプリケーションに証明書をアップロードします。

関連項目

- シングル サイン オン URL へのエンドユーザー アクセスの設定, on page 143

SaaS アクセス コントロールと複数のアプライアンスの使用

Before you begin

ID プロバイダとしてのアプライアンスの設定, on page 137

Procedure

ステップ 1 各 Secure Web Applianceに対して同じ ID プロバイダーのドメイン名を設定します。

ステップ 2 各 Secure Web Applianceに対して同じ ID プロバイダーのエンティティ ID を設定します。

ステップ 3 [ネットワーク（Network）] > [SaaS の ID プロバイダ（Identity Provider for SaaS）] ページで、各アプライアンスに同じ証明書と秘密キーをアップロードします。

ステップ 4 設定する各 SaaS アプリケーションにこの証明書をアップロードします。

SaaS アプリケーション認証ポリシーの作成

Before you begin

- 関連付けられた ID を作成します。
- ID プロバイダを設定します（ID プロバイダとしてのアプライアンスの設定, on page 137を参照）。
- ID プロバイダの署名証明書とキーを入力します（[ネットワーク（Network）] > [SaaS の ID プロバイダ（Identity Provider for SaaS）] > [設定の有効化と編集（Enable and Edit Settings）]）。
- 認証レルムを作成します。認証レルム

Procedure

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

ステップ 2 [アプリケーションの追加（Add Application）] をクリックします。

ステップ 3 以下の設定項目を設定します。

プロパティ	説明
アプリケーション名（Application Name）	このポリシーの SaaS アプリケーションを識別する名前を入力します。各アプリケーション名は一意である必要があります。 Secure Web Applianceは、アプリケーション名を使用して、シングル サインオン URL を生成できます。
説明	（オプション）この SaaS ポリシーの説明を入力します。

プロパティ	説明
サービスプロバイダのメタデータ（Metadata for Service Provider）	このポリシーで参照されるサービスプロバイダを示すメタデータを設定します。サービスプロバイダのプロパティを手動で記述するか、またはSaaSアプリケーションによって提供されるメタデータ ファイルをアップロードできます。 Secure Web Applianceは、SAML を使用して SaaS アプリケーション（サービスプロバイダー）と通信する方法を決定するために、メタデータを使用します。メタデータの適切な設定については、SaaS アプリケーションを参照してください。 キーの手動設定（Configure Keys Manually）：このオプションを選択した場合は、以下を入力します。 • [サービスプロバイダのエンティティID（Service Provider Entity ID）]。SaaS アプリケーションが自身をサービス プロバイダとして識別するために使用するテキスト（通常は URI 形式）を入力します。 • [名前IDの形式（Name ID Format）]。サービス プロバイダに送信する SAML アサーションでアプライアンスがユーザーを識別するために使用する形式を、ドロップダウン リストから選択します。ここで入力する値は、SaaS アプリケーションの対応する設定と一致している必要があります。 • [Assertion Consumer ServiceのURL（Assertion Consumer Service URL）]。 Secure Web Applianceが作成したSAMLアサーションの送信先URLを入力します。SaaS アプリケーションのマニュアルを参照して、使用する適切な URL （ログイン URL）を決定してください。 [ハードディスクからファイルをインポート（Import File from Hard Disk）]：このオプションを選択した場合は、[参照（Browse）] をクリックしてファイルを検索し、[インポート（Import）] をクリックします。 **Note** このメタデータ ファイルは、サービスプロバイダのインスタンスを説明するSAML標準に準拠した XML ドキュメントです。すべての SaaS アプリケーションがメタデータ ファイルを使用するわけではありませんが、使用する場合は、ファイルについて SaaS アプリケーションのプロバイダにお問い合わせください。

プロパティ	説明
ユーザー識別/SaaS SSO の認証（User Identification / Authentication for SaaS SSO）	SaaS シングル サインオンに対してユーザーを識別または認証する方法を指定します。 • ユーザーに対して、常にローカル認証クレデンシャルの入力を求める。 • Web プロキシが透過的にユーザー名を取得した場合に、ユーザーに対してローカル認証クレデンシャルの入力を求める。 • SaaS ユーザーのローカル認証クレデンシャルを使用して、ユーザーを自動的にサインインさせる。 この SaaS アプリケーションにアクセスするユーザーを認証するために、Web プロキシが使用する認証レルムまたはシーケンスを選択します。SaaS アプリケーションに正常にアクセスするには、ユーザーは認証レルムまたは認証シーケンスのメンバーである必要があります。Identity Services Engine を認証に使用しており、LDAP を選択した場合は、SAML ユーザー名と属性のマッピングにレルムが使用されます。
SAML ユーザー名のマッピング（SAML User Name Mapping）	Web プロキシが SAML アサーションでサービス プロバイダにユーザー名を示す方法を指定します。ネットワーク内で使用されているユーザー名を渡すか（[マッピングなし（No mapping）]）、または以下のいずれかの方法で内部ユーザー名を別の形式に変更できます。 • [LDAP クエリー（LDAP query）]。サービス プロバイダに送信されるユーザー名は、1 つ以上の LDAP クエリー属性に基づきます。LDAP 属性フィールドと任意のカスタム テキストを含む式を入力します。属性名は山カッコで囲む必要があります。任意の数の属性を含めることができます。たとえば、LDAP 属性が「user」と「domain」の場合は、<user>@<domain>.com と入力できます。 • [固定ルール マッピング（Fixed Rule Mapping）]。サービス プロバイダに送信されるユーザー名は、前または後ろに固定文字列を追加した内部ユーザー名に基づきます。[式名（Expression Name）] フィールドに固定文字列を入力し、その前または後ろに %s を付けて内部ユーザー名における位置を示します。
SAML 属性マッピング（SAML Attribute Mapping）	（オプション）SaaS アプリケーションから要求された場合は、LDAP 認証サーバーから内部ユーザーに関する追加情報を SaaS アプリケーションに提供できます。各 LDAP サーバー属性を SAML 属性にマッピングします。
認証コンテキスト（Authentication Context）	Web プロキシが内部ユーザーを認証するために使用する認証メカニズムを選択します。 **Note** 認証コンテキストは、ID プロバイダが内部ユーザーの認証に使用した認証メカニズムをサービス プロバイダに通知します。一部のサービス プロバイダでは、ユーザーに SaaS アプリケーションへのアクセスを許可するために特定の認証メカニズムが必要です。サービス プロバイダが ID プロバイダでサポートされていない認証コンテキストを必要とする場合、ユーザーはシングル サイン オンを使用して ID プロバイダからサービス プロバイダにアクセスできません。

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）]）。

What to do next

アプリケーションを設定したのと同じパラメータを使用して、SaaSアプリケーション側にシングル サインオンを設定します。

シングル サイン オン URL へのエンドユーザー アクセスの設定

Secure Web Applianceを ID プロバイダーとして設定し、SaaS アプリケーション用に SaaS アプリケーション認証ポリシーを作成すると、アプライアンスによってシングルサインオン URL（SSO URL）が作成されます。 Secure Web Applianceは SaaS アプリケーション認証ポリシーで設定されたアプリケーション名を使用して、シングルサインオン URL を生成します。SSO URL の形式は以下のとおりです。

http://*IdentityProviderDomainName* /SSOURL/*ApplicationName*

Procedure

ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] > [SaaS ポリシー（SaaS Policies）] ページで、シングルサインオン URL を取得します。

ステップ 2 フロー タイプに応じてエンドユーザーが URL を使用できるようにします。

ステップ 3 IDプロバイダによって開始されるフローを選択すると、アプライアンスはユーザーをSaaSアプリケーションにリダイレクトします。

ステップ 4 サービス プロバイダによって開始されるフローを選択する場合は、この URL を SaaS アプリケーションで設定する必要があります。

- 常に SaaSユーザーにプロキシ認証を要求する。ユーザーは有効なクレデンシャルを入力した後、SaaS アプリケーションにログインします。
- SaaS ユーザーを透過的にサインインさせる。ユーザーは SaaS アプリケーションに自動的にログインします。

Note
アプライアンスが透過モードで展開されている場合に、明示的な転送要求を使用して、すべての認証済みユーザーに対するシングル サイン オン動作を実現するには、ID グループを設定する際に、[明示的転送要求に同じサロゲート設定を適用（Apply same surrogate settings to explicit forward requests）] 設定を選択します。

発信トラフィックでの既存の感染のスキャン

この章で説明する内容は、次のとおりです。

発信トラフィックのスキャンの概要

悪意のあるデータがネットワークから発信されないようにするため、 Secure Web Applianceには発信マルウェアスキャン機能があります。ポリシー グループを使用して、マルウェアのスキャン対象となるアップロード、スキャンに使用するマルウェア対策スキャン エンジン、ブロックするマルウェアのタイプを定義できます。

Cisco Dynamic Vectoring and Streaming（DVS）エンジンは、トランザクション要求がネットワークから発信されるときにそれをスキャンします。Cisco DVS エンジンとの連携により、 Secure Web Applianceでは無意識のうちに悪意のあるデータがアップロードされるのを防止できます。

次の作業を実行できます。

タスク	タスクへのリンク
マルウェアをブロックするポリシーを作成する	アウトバウンド マルウェア スキャン ポリシーの設定, on page 146
発信マルウェア ポリシー グループにアップロード要求を割り当てる	アップロード要求の制御 , on page 148

要求が DVS エンジンによってブロックされた場合のユーザー エクスペリエンス

Cisco DVS エンジンがアップロード要求をブロックすると、Web プロキシはエンドユーザーにブロック ページを送信します。ただし、すべての Web サイトでエンド ユーザーにブロック ページが表示されるわけではありません。一部の Web 2.0 Web サイトでは、静的 Web ページの代わりに JavaScript を使用して動的コンテンツが表示され、ブロック ページが表示されることはありません。そのような場合でも、ユーザーは適切にブロックされているので悪意のあるデータをアップロードすることはありませんが、そのことが Web サイトから通知されない場合もあります。

アップロード要求について

発信マルウェア スキャン ポリシーは、サーバーにデータをアップロードするトランザクション（アップロード要求）に対して、Web プロキシが HTTP 要求と復号 HTTPS 接続をブロックするかどうかを定義します。アップロード要求は、要求本文にコンテンツが含まれているHTTP または復号 HTTPS 要求です。

アップロード要求を受信すると、Web プロキシは要求を発信マルウェア スキャン ポリシー グループと比較して、適用するポリシー グループを決定します。ポリシー グループに要求を割り当てた後、ポリシー グループの設定済み制御設定と要求を比較し、要求をモニターするかブロックするかを決定します。発信マルウェア スキャン ポリシーによる判定で要求をモニターすることが決定されると、要求はアクセス ポリシーに対して評価され、Web プロキシが実行する最終アクションが該当するアクセス ポリシーによって決定されます。

Note サイズがゼロ（0）バイトのファイルのアップロードを試みているアップロード要求は、発信マルウェア スキャン ポリシーに対して評価されません。

グループ メンバーシップの基準

各クライアント要求に ID が割り当てられ、次に、それらの要求が他のポリシー タイプと照合して評価され、タイプごとに要求が属するポリシー グループが判定されます。Web プロキシは、要求のポリシー グループ メンバーシップに基づいて、設定されているポリシー制御設定をクライアント要求に適用します。

Web プロキシは、特定のプロセスを実行してグループ メンバーシップの基準と照合します。グループ メンバーシップの以下の要素が考慮されます。

基準	説明
識別プロファイル（Identification Profile）	各クライアント要求は、**識別プロファイル**に一致するか、認証に失敗するか、ゲストアクセスが許可されるか、または認証に失敗して終了します。
権限を持つユーザー	割り当てられた**識別プロファイル**が認証を必要とする場合に、そのユーザーが発信マルウェア スキャン ポリシー グループの承認済みユーザーのリストに含まれており、ポリシー グループに一致している必要があります。承認済みユーザーのリストには、任意のグループまたはユーザーを指定でき、**識別プロファイル**がゲストアクセスを許可している場合はゲスト ユーザーを指定できます。
詳細オプション（Advanced options）	発信マルウェア スキャン ポリシー グループ メンバーシップの複数の高度なオプションを設定できます。一部のオプション（プロキシ ポート、URL カテゴリなど）は、**識別プロファイル**内に定義することもできます。高度なオプションを**識別プロファイル**内で設定すると、発信マルウェア スキャン ポリシー グループ レベルでは設定できなくなります。

クライアント要求と発信マルウェア スキャン ポリシー グループの照合

Web プロキシは、アップロード要求のステータスを最初のポリシー グループのメンバーシップ基準と比較します。一致した場合、Web プロキシは、そのポリシー グループのポリシー設定を適用します。

一致しない場合は、その以下のポリシー グループとアップロード要求を比較します。アップロード要求をユーザー定義のポリシー グループと照合するまで、Web プロキシはこのプロセスを続行します。ユーザー定義のポリシー グループに一致しない場合は、グローバル ポリシー グループと照合します。Web プロキシは、アップロード要求をポリシー グループまたはグローバル ポリシー グループと照合するときに、そのポリシー グループのポリシー設定を適用します。

アウトバウンド マルウェア スキャン ポリシーの設定

宛先サイトの 1 つ以上のアイデンティティや URL カテゴリなど、複数の条件の組み合わせに基づいてアウトバウンド マルウェア スキャン ポリシー グループを作成できます。ポリシー グループのメンバーシップには、少なくとも 1 つの条件を定義する必要があります。複数の条件が定義されている場合、アップロード要求がポリシー グループと一致するには、すべての条件を満たしていなければなりません。ただし、アップロード要求は設定された ID の 1 つのみと一致する必要があります。

Procedure

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）] > [発信マルウェア スキャン（Outbound Malware Scanning）] を選択します。

ステップ 2 [ポリシーを追加（Add Policy）] をクリックします。

ステップ 3 ポリシー グループの名前と説明（オプション）を入力します。

Note
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。

ステップ 4 [上記ポリシーを挿入（Insert Above Policy）] フィールドで、ポリシー テーブル内のポリシー グループを配置する場所を選択します。

複数のポリシー グループを設定する場合は、各グループに論理的な順序を指定します。

ステップ 5 [識別プロファイルおよびユーザー（Identification Profiles And Users）] セクションで、このポリシー グループに適用する 1 つまたは複数の ID グループを選択します。

ステップ 6 （オプション）[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。

ステップ 7 いずれかの拡張オプションを使用してポリシー グループのメンバーシップを定義するには、拡張オプションのリンクをクリックし、表示されるページでオプションを設定します。

高度なオプション	説明
プロトコル	クライアント要求で使用されるプロトコルによってポリシー グループのメンバーシップを定義するかどうかを選択します。含めるプロトコルを選択します。 [その他のすべて（All others）] は、このオプションの上に一覧表示されていないプロトコルを意味します。 **Note** HTTPS プロキシをイネーブルにすると、復号ポリシーのみが HTTPS トランザクションに適用されます。アクセス、ルーティング、アウトバウンド マルウェア スキャン、データ セキュリティ、外部 DLP のポリシーの場合は、HTTPS プロトコルによってポリシー メンバーシップを定義できません。
プロキシ ポート（Proxy Ports）	Web プロキシへのアクセスに使用するプロキシ ポートで、ポリシー グループ メンバーシップを定義するかどうかを選択します。[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。 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。 クライアント要求がアプライアンスに透過的にリダイレクトされるときにプロキシ ポートでポリシー グループのメンバーシップを定義すると、一部の要求が拒否される場合があります。 **Note** 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、非 ID 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。
サブネット（Subnets）	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するかどうかを選択します。 関連 ID で定義されている可能性のあるアドレスを使用するか、またはここで特定のアドレスを入力することができます。 **Note** 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メンバーシップを定義している場合は、ID で定義されているアドレスのサブセットであるアドレスを、このポリシー グループに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。
URL カテゴリ（URL Categories）	URL カテゴリでポリシー グループのメンバーシップを定義するかどうかを選択します。ユーザー定義または定義済みの URL カテゴリを選択します。 **Note** 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、非 ID 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
ユーザー エージェント（User Agents）	クライアント要求で使用されるユーザー エージェント（アップデータや Web ブラウザなどのクライアント アプリケーション）ごとにポリシー グループ メンバーシップを定義するかどうかを選択します。一般的に定義されているユーザー エージェントを選択するか、正規表現を使用して独自に定義できます。メンバーシップの定義に選択したユーザー エージェントのみを含めるか、選択したユーザー エージェントを明確に除外するかどうかを指定します。 **Note** このポリシー グループに関連付けられている**識別プロファイル**が、この詳細設定によって**識別プロファイル** メンバーシップを定義している場合、非**識別プロファイル** 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。
ユーザーの場所（User Location）	ユーザーのリモートまたはローカルの場所でポリシー グループのメンバーシップを定義するかどうかを選択します。

ステップ 8 変更を送信します。

ステップ 9 アウトバウンド マルウェア スキャン ポリシー グループの管理を設定して、Web プロキシがトランザクションを処理する方法を定義します。

新しいアウトバウンド マルウェア スキャン ポリシー グループは、各制御設定のオプションが設定されるまで、グローバル ポリシー グループの設定を自動的に継承します。

ステップ 10 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

アップロード要求の制御

各アップロード要求は、アウトバウンド マルウェア スキャン ポリシー グループに割り当てられ、そのポリシー グループの制御設定を継承します。Web プロキシは、アップロード要求ヘッダーを受信することにより、要求本文をスキャンする必要があるかどうかを判定するための必要情報を得ます。DVS エンジンは要求をスキャンし、Web プロキシに判定を返します。必要に応じて、エンド ユーザーにブロック ページが表示されます。

Procedure

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）] > [発信マルウェア スキャン（Outbound Malware Scanning）] を選択します。

ステップ 2 [接続先（Destinations）] 列で、設定するポリシー グループのリンクをクリックします。

ステップ 3 [接続先設定の編集（Edit Destination Settings section）] セクションで、ドロップダウン メニューから [接続先スキャンのカスタム設定の定義（Define Destinations Scanning Custom Settings）] を選択します。

ステップ 4 [スキャンする接続先（Destination to Scan）] セクションで、以下のいずれかを選択します。

オプション	説明
どのアップロードもスキャンしない（Do not scan any uploads）	DVS エンジンはアップロード要求をスキャンしません。すべてのアップロード要求がアクセス ポリシーに対して評価されます。
すべてのアップロードをスキャンする（Scan all uploads）	DVS エンジンはすべてのアップロード要求をスキャンします。DVS エンジンのスキャン判定に応じて、アップロード要求はブロックされるか、またはアクセス ポリシーに対して評価されます。
指定したカスタム URL カテゴリへのアップロードをスキャン（Scan uploads to specified custom URL categories）	DVS エンジンは、特定のカスタム URL カテゴリに属するアップロード要求をスキャンします。DVS エンジンのスキャン判定に応じて、アップロード要求はブロックされるか、またはアクセス ポリシーに対して評価されます。 [カスタムカテゴリリストを編集（Edit custom categories list）] をクリックして、スキャンする URL カテゴリを選択します。

ステップ 5 変更を送信します。

ステップ 6 [マルウェア対策フィルタリング（Anti-Malware Filtering）] 列で、ポリシー グループのリンクをクリックします。

ステップ 7 [マルウェア対策設定（Anti-Malware Settings）] セクションで、[マルウェア対策カスタム設定の定義（Define Anti-Malware Custom Settings）] を選択します。

ステップ 8 [Cisco DVS マルウェア対策設定（Cisco DVS Anti-Malware Settings）] セクションで、このポリシー グループに対してイネーブルにするマルウェア対策スキャン エンジンを選択します。

ステップ 9 [マルウェア カテゴリ（Malware Categories）] セクションで、さまざまなマルウェア カテゴリをモニターするかブロックするかを選択します。

このセクションに一覧表示されるカテゴリは、イネーブルにするスキャンエンジンによって異なります。

Note
設定された最大時間に達した場合や、システムで一時的エラーが発生した場合、URL トランザクションはスキャン不可と分類されます。たとえば、スキャンエンジンのアップデート時や AsyncOS のアップグレード時に、トランザクションがスキャン不可と分類されることがあります。マルウェア スキャンの判定が SV_TIMEOUT や SV_ERROR の場合は、スキャン不可のトランザクションと見なされます。

ステップ 10 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

DVS スキャンのロギング

アクセス ログは、DVS エンジンがマルウェアについてアップロード要求をスキャンしたかどうかを示します。各アクセス ログ エントリのスキャン判定情報セクションには、スキャンされたアップロードに対する DVS エンジン アクティビティの値が含まれています。フィールドのいずれかを W3C またはアクセス ログに追加すると、この DVS エンジン アクティビティをより簡単に検索できます。

Table 1: W3C ログのログ フィールドおよびアクセス ログのフォーマット指定子

W3C ログ フィールド	アクセス ログのフォーマット指定子
x-req-dvs-scanverdict	%X2
x-req-dvs-threat-name	%X4
x-req-dvs-verdictname	%X3

DVS エンジンによってアップロード要求がマルウェアと判定され、DVS エンジンがマルウェアのアップロードをブロックするように設定されている場合、アクセス ログの ACL デシジョン タグは BLOCK_AMW_REQ になります。

ただし、DVS エンジンによってアップロード要求がマルウェアと判定され、DVS エンジンがマルウェアをモニターするように設定されている場合、アクセス ログの ACL デシジョン タグは、実際にトランザクションに適用されるアクセス ポリシーによって決まります。

DVS エンジンがマルウェアについてアップロード要求をスキャンしたかどうかを判断するには、各アクセス ログ エントリのスキャン判定情報セクションで、DVS エンジン アクティビティの結果を確認します。

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。