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

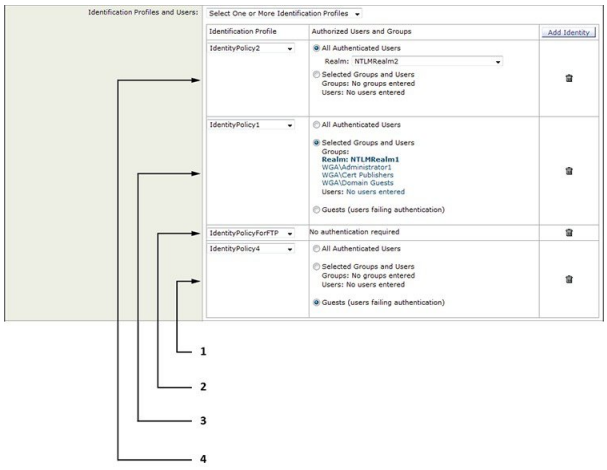
AsyncOS はすべてのトランザクションに識別プロファイルを割り当てます。

- 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。

オプション	説明
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。
- （任意）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
- （任意）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。
- （任意）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。

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。
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化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

ID の有効化/無効化

始める前に

- 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。

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。

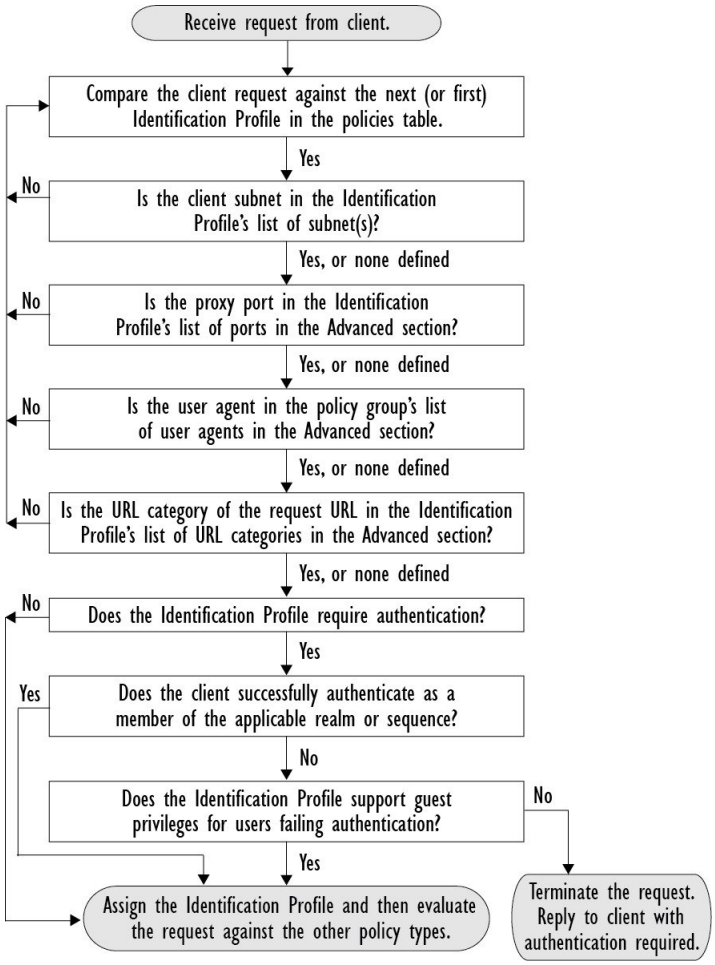
ステップ 4 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

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。

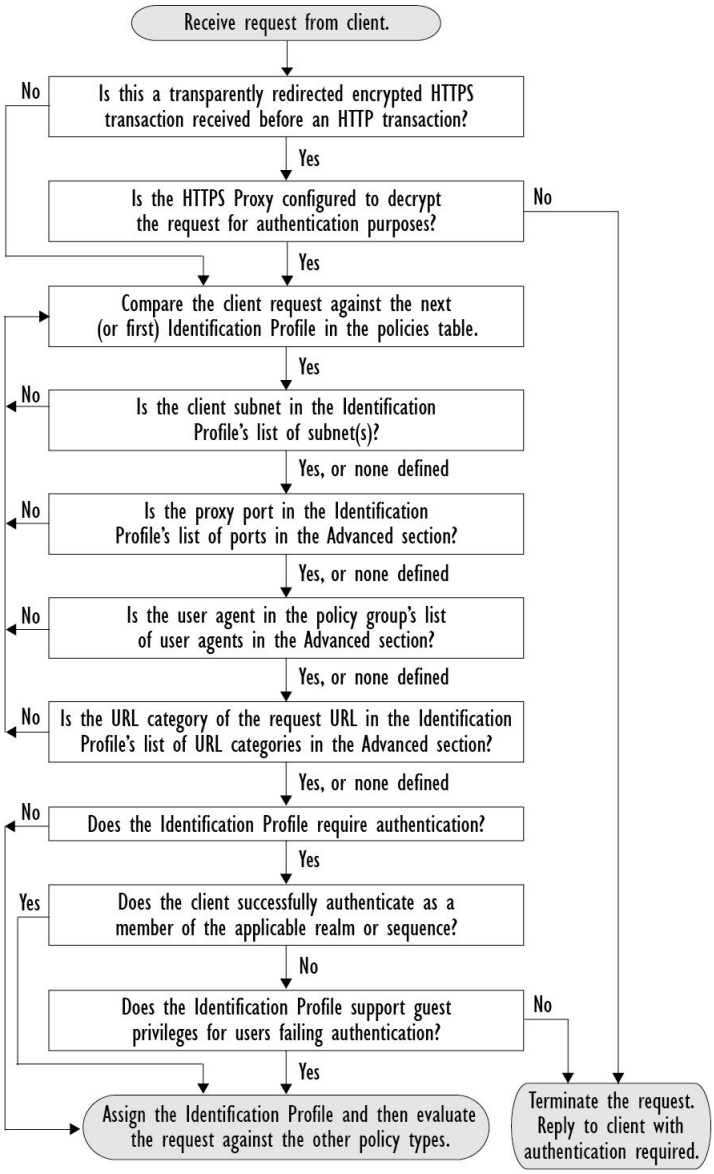
- 認証サロゲートなし
- 認証サロゲートとしての IP アドレス
- 透過的要求を使用する認証サロゲートとしてのクッキー
- 明示的要求を使用する認証サロゲートとしてのクッキー（クレデンシャルの暗号化がイネーブルになっている場合）

図 *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。

図 *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。

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。