Secure Web ApplianceとUmbrella SWG間のプロキシチェーンの設定

内容

はじめに

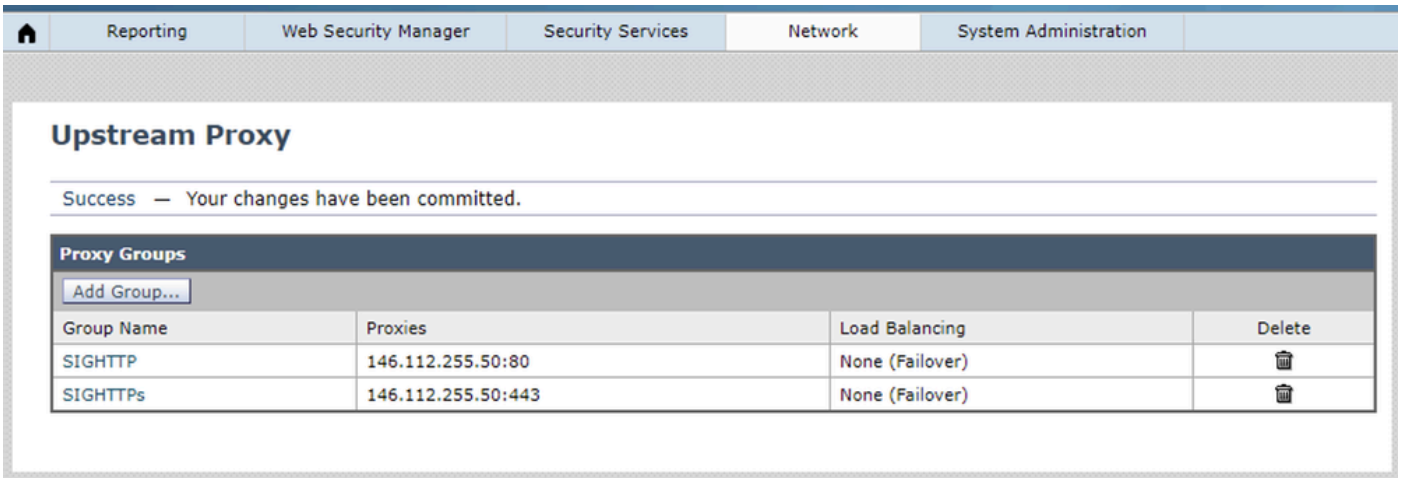
このドキュメントでは、Secure Web Appliance(WSA)とUmbrella Secure Web Gateway(SWG)の間のプロキシチェーンを設定する方法について説明します。

概要

Umbrella SIGはプロキシチェーンをサポートし、ダウンストリームプロキシサーバからのすべてのHTTP/HTTP要求を処理できます。これは、Cisco Secure Web Appliance（以前のCisco WSA）とUmbrella Secure Web Gateway(SWG)の間にプロキシチェーンを実装するための包括的なガイドです。Secure Web ApplianceとSWGの両方の設定が含まれています。

セキュアWebアプライアンスポリシーの設定

1. Network>Upstream Proxyを使用して、SWG HTTPおよびHTTPsリンクをアップストリームプロキシとして設定します。

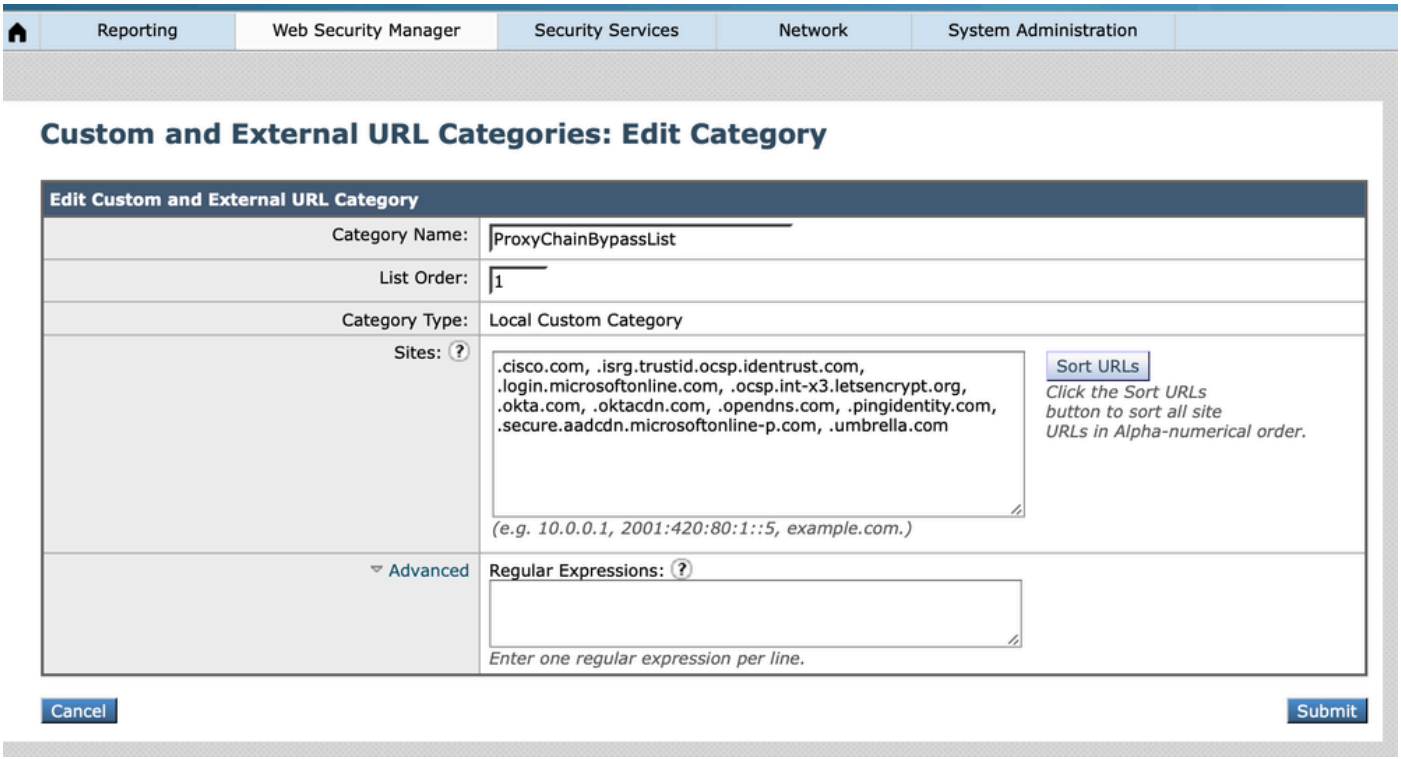


360079596451

2. Web Security Manager>Routing Policyでバイパスポリシーを作成し、提案されたすべての

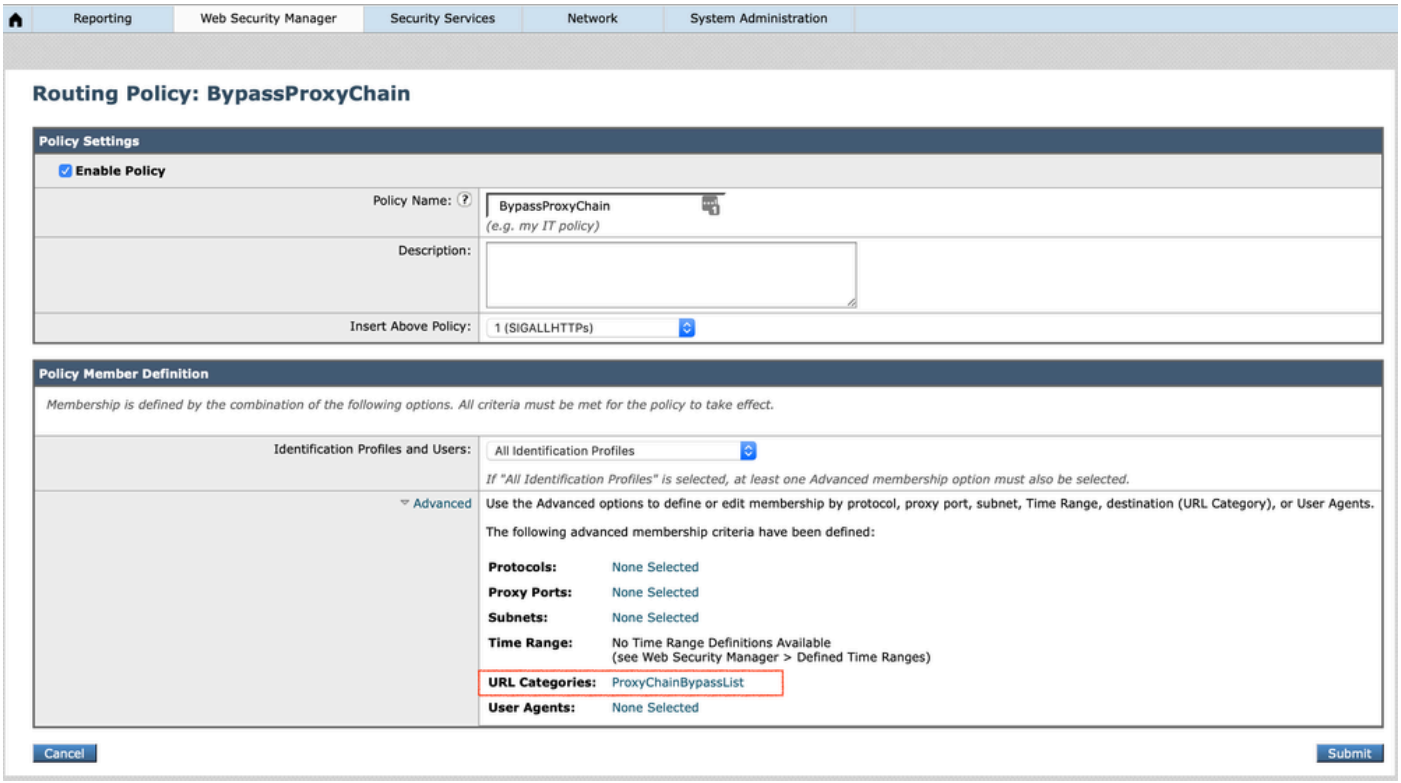
URLをインターネットに直接ルーティングします。バイパスされるすべてのURLは、次のドキュメントに記載されています。[Cisco Umbrella SIGユーザガイド：プロキシチェーンの管理]

- まず、次に示すように、「Web Security Manager>Custom and External URL Categories」に移動して、新しい「カスタムカテゴリ」を作成します。 バイパスポリシーは、「カスタムカテゴリ」に基づいています。



360050592552

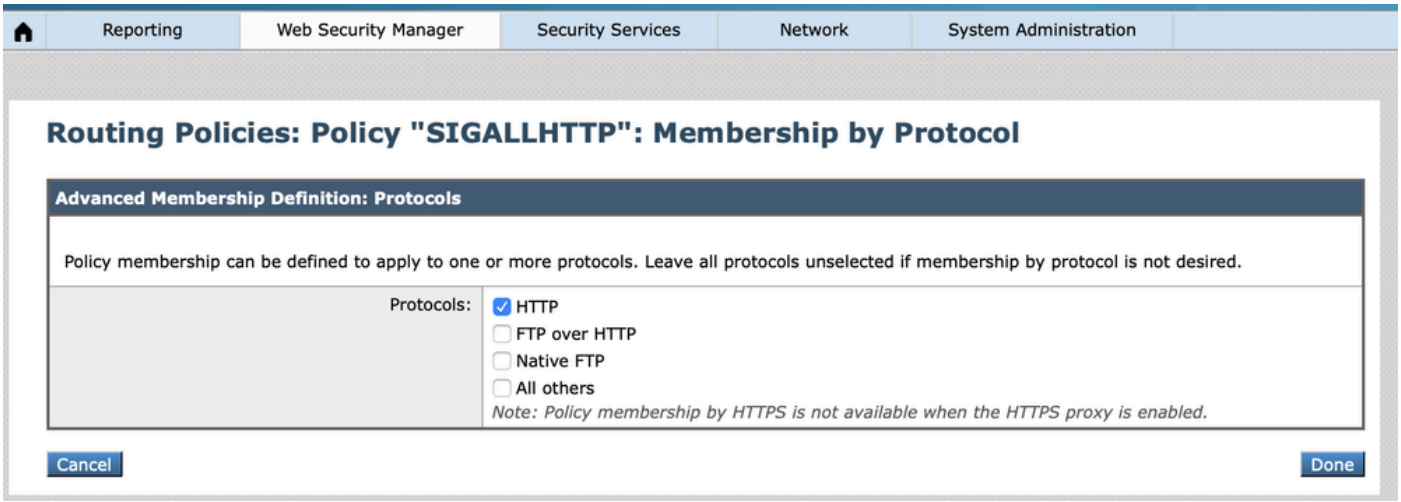
- 次に、Web Security Manager > Routing Policyの順に選択して、新しいバイパスルーティングポリシーを作成します。Secure Web Applianceがポリシーの順序に基づいてポリシーに一致するため、このポリシーが最初のものであることを確認してください。



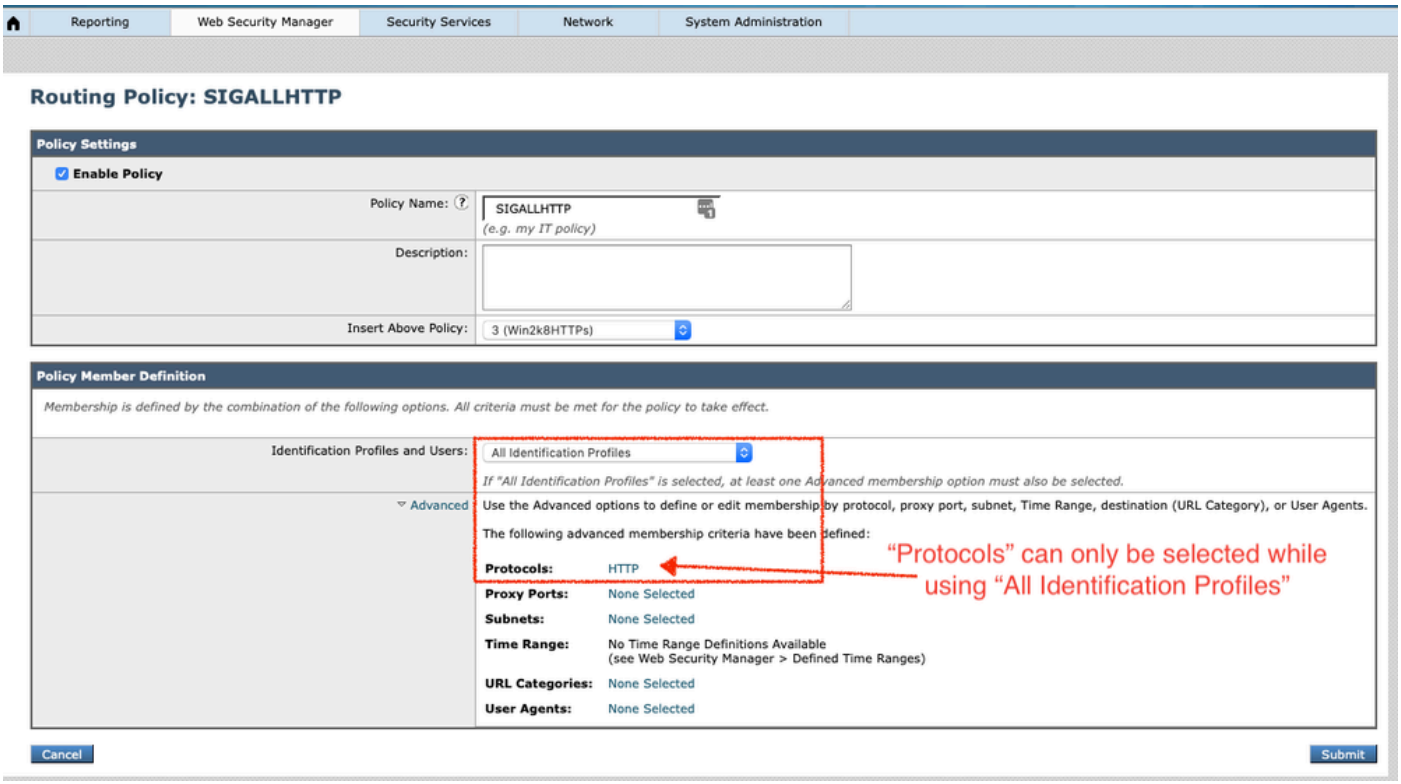
360050703131

3. すべてのHTTP要求の新しいルーティングポリシーを作成します。

- Secure Web Applianceルーティングポリシーメンバ定義では、プロトコルオプションはHTTP、FTP over HTTP、ネイティブFTP、および「その他すべて」で、「すべての識別プロファイル」が選択されています。HTTPにはオプションがないため、すべてのHTTP要求に対してこのルーティングポリシーを実装した後で、HTTP要求のルーティングポリシーを個別に作成します。

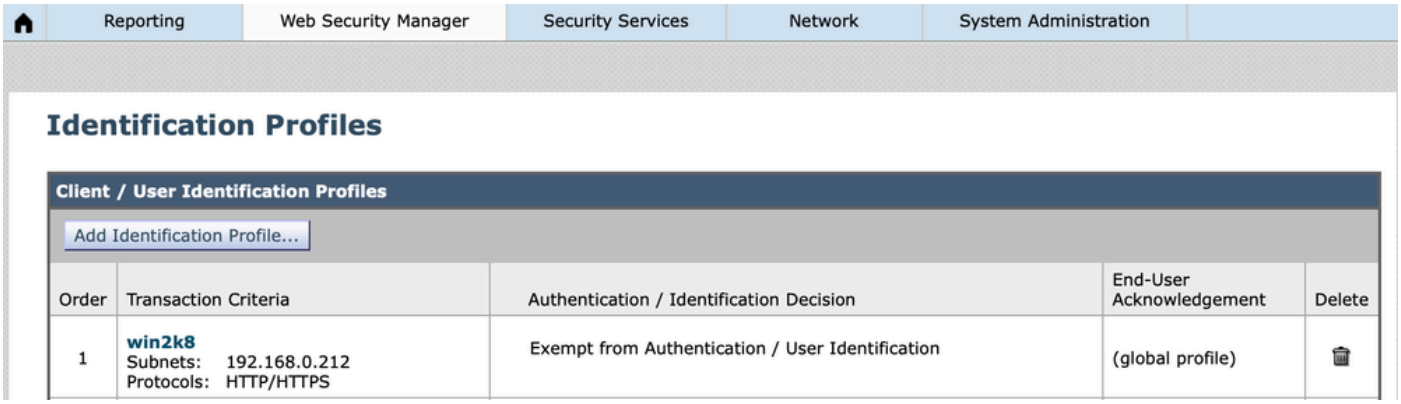


360050592772

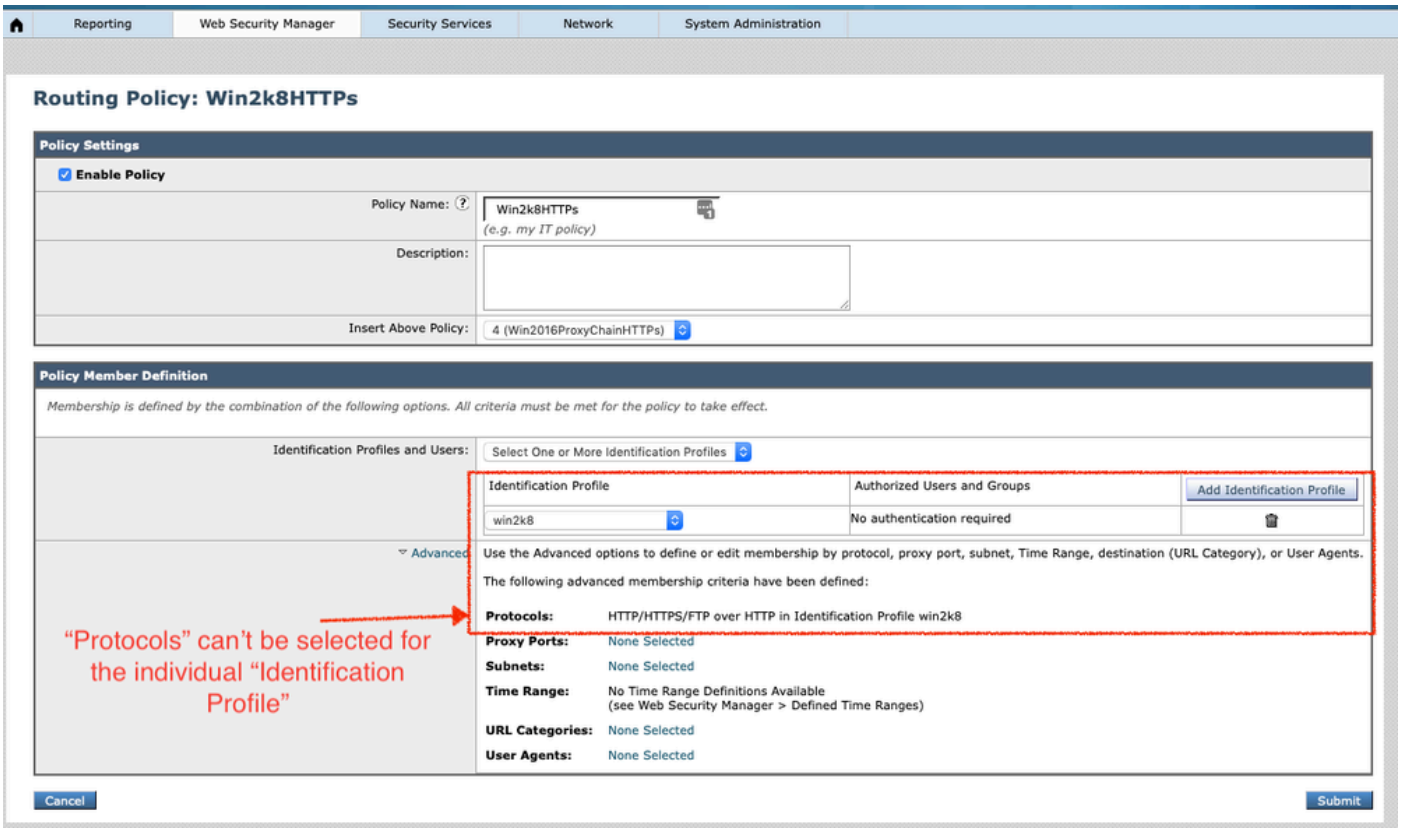


360050589572

4.「IDプロファイル」に基づいて、HTTP要求のルーティングポリシーを作成します。 定義されている「識別プロファイル」の順序に注意してください。これは、Secure Web Applianceが最初の一致の「識別」に一致するためです。この例では、IDプロファイル「win2k8」は内部IPベースのIDです。



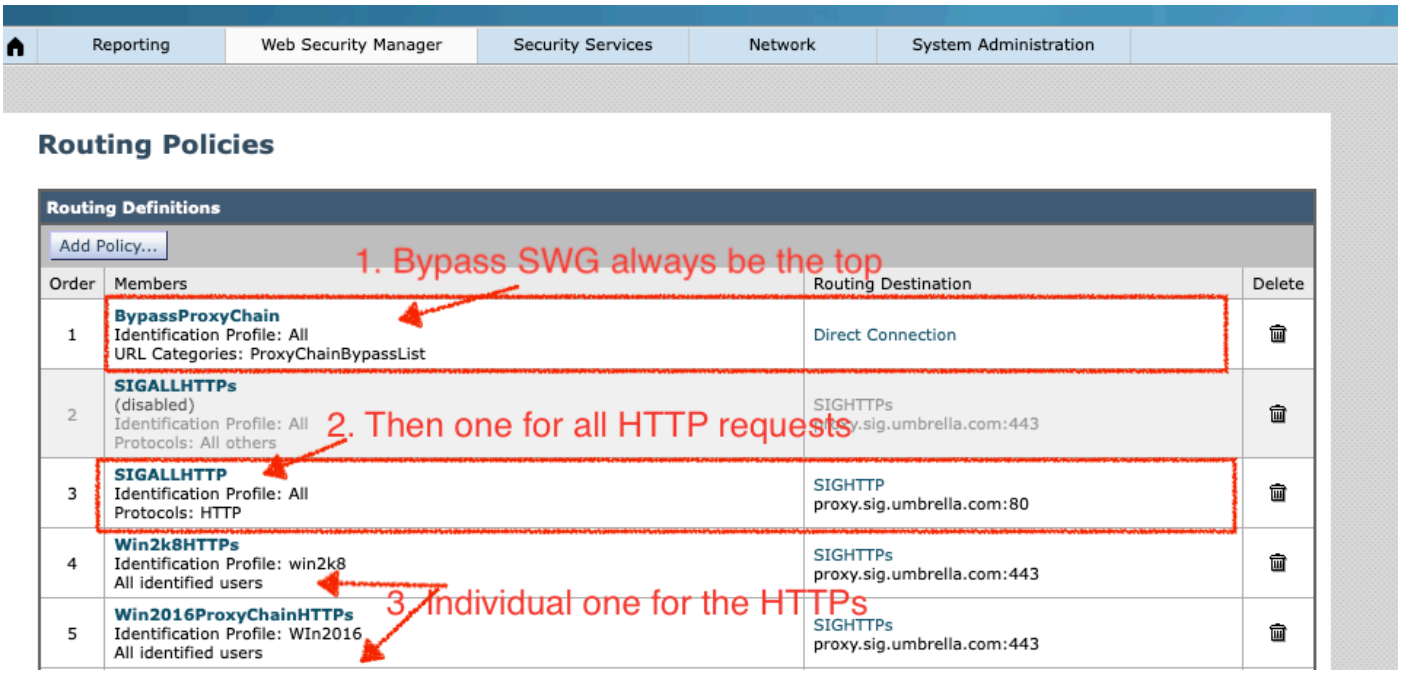
360050703971



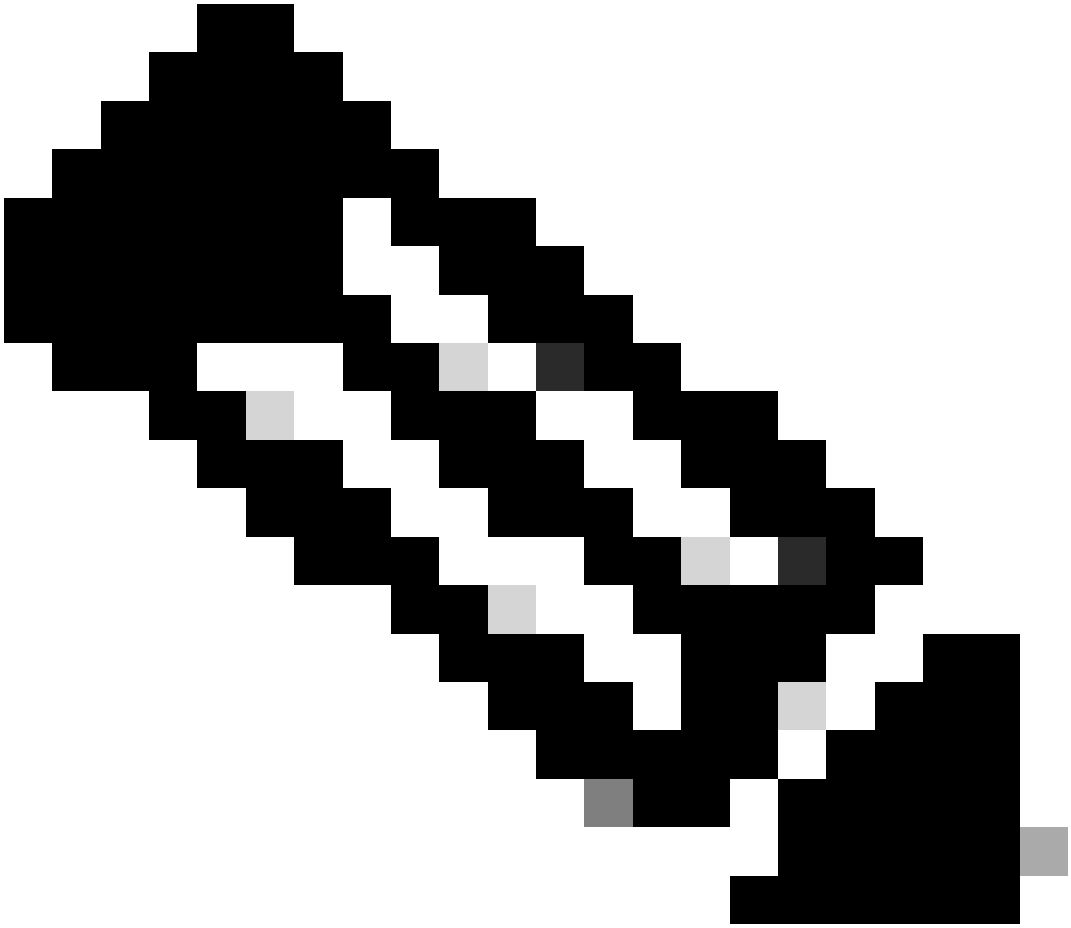
360050700091

5. セキュアWebアプライアンスルーティングポリシーの最終設定：

- Secure Web Applianceは、「トップダウン」方式のルール処理アプローチを使用して、IDおよびアクセスポリシーを評価することに注意してください。 つまり、処理の任意の時点で最初に一致が見つかると、Secure Web Applianceによって実行されるアクションが実行されます。
- さらに、最初にIDが評価されます。クライアントのアクセスが特定のIDに一致すると、セキュアWebアプライアンスは、クライアントのアクセスに一致するIDを使用するように設定されているすべてのアクセスポリシーをチェックします。



360050700131



注：上記のポリシー設定は、明示的なプロキシ導入にのみ適用されます。

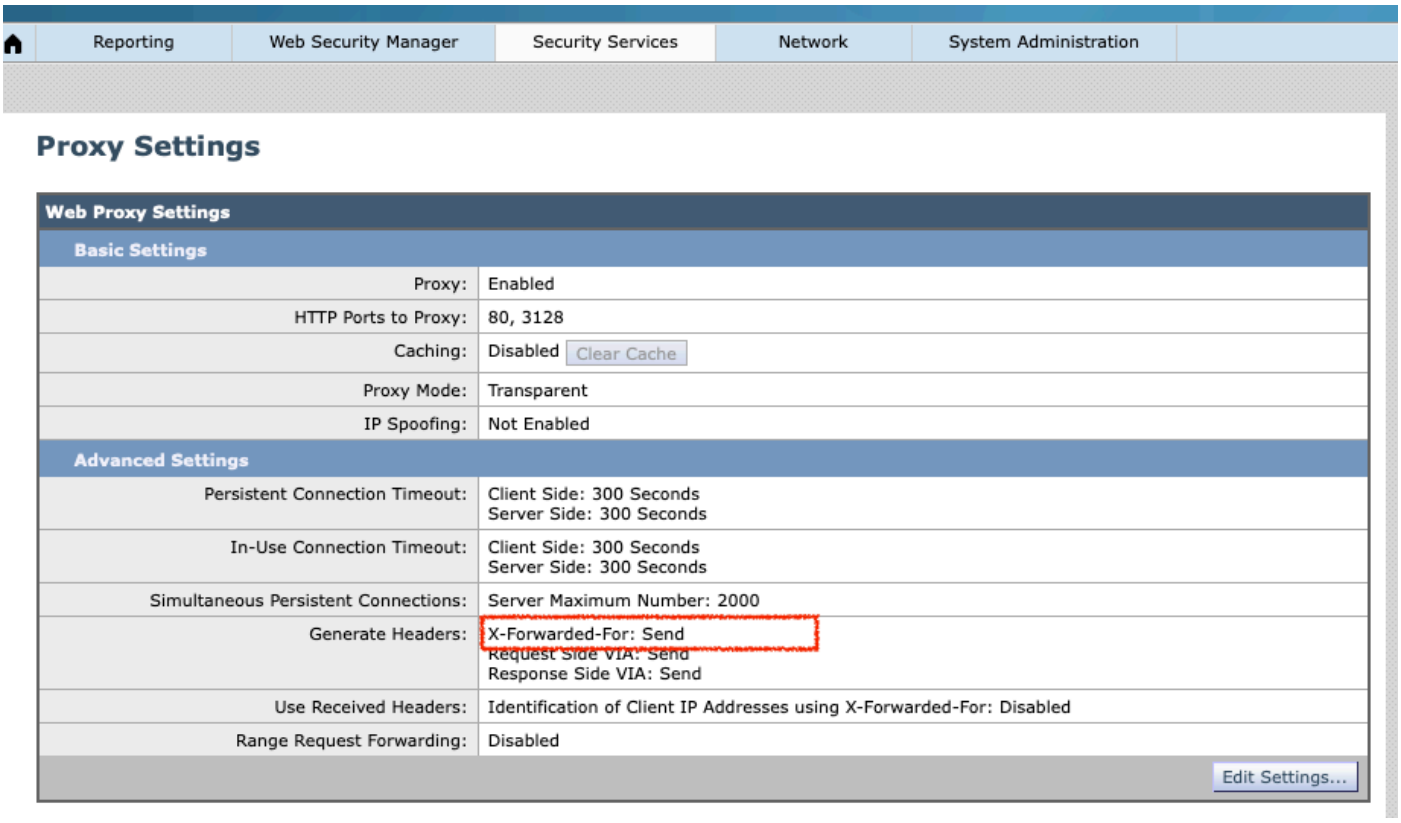
透過的なプロキシ導入

トランスペアレントHTTPSの場合、AsyncOSはクライアントヘッダー内の情報にアクセスできません。そのため、ルーティングポリシーまたはIDプロファイルがクライアントヘッダー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。

1. 透過的にリダイレクトされたHTTPSトランザクションは、次の場合にのみルーティングポリシーと一致します。
   - ルーティングポリシーグループには、URLカテゴリ、ユーザエージェントなどのポリシーメンバーシップ基準が定義されていません。
   - 識別プロファイルには、URLカテゴリ、ユーザエージェントなどのポリシーメンバーシップ基準が定義されていません。
2. いずれかのIDプロファイルまたはルーティングポリシーにカスタムURLカテゴリが定義されている場合、すべての透過的なHTTPSトランザクションはデフォルトルーティングポリシーグループと一致します。
3. トランスペアレントHTTPSトランザクションがデフォルトルーティングポリシーグループに一致する可能性があるため、可能な限り、すべてのIDプロファイルでルーティングポリシーを設定することは避けてください。

1. X-Forwarded-Forヘッダー

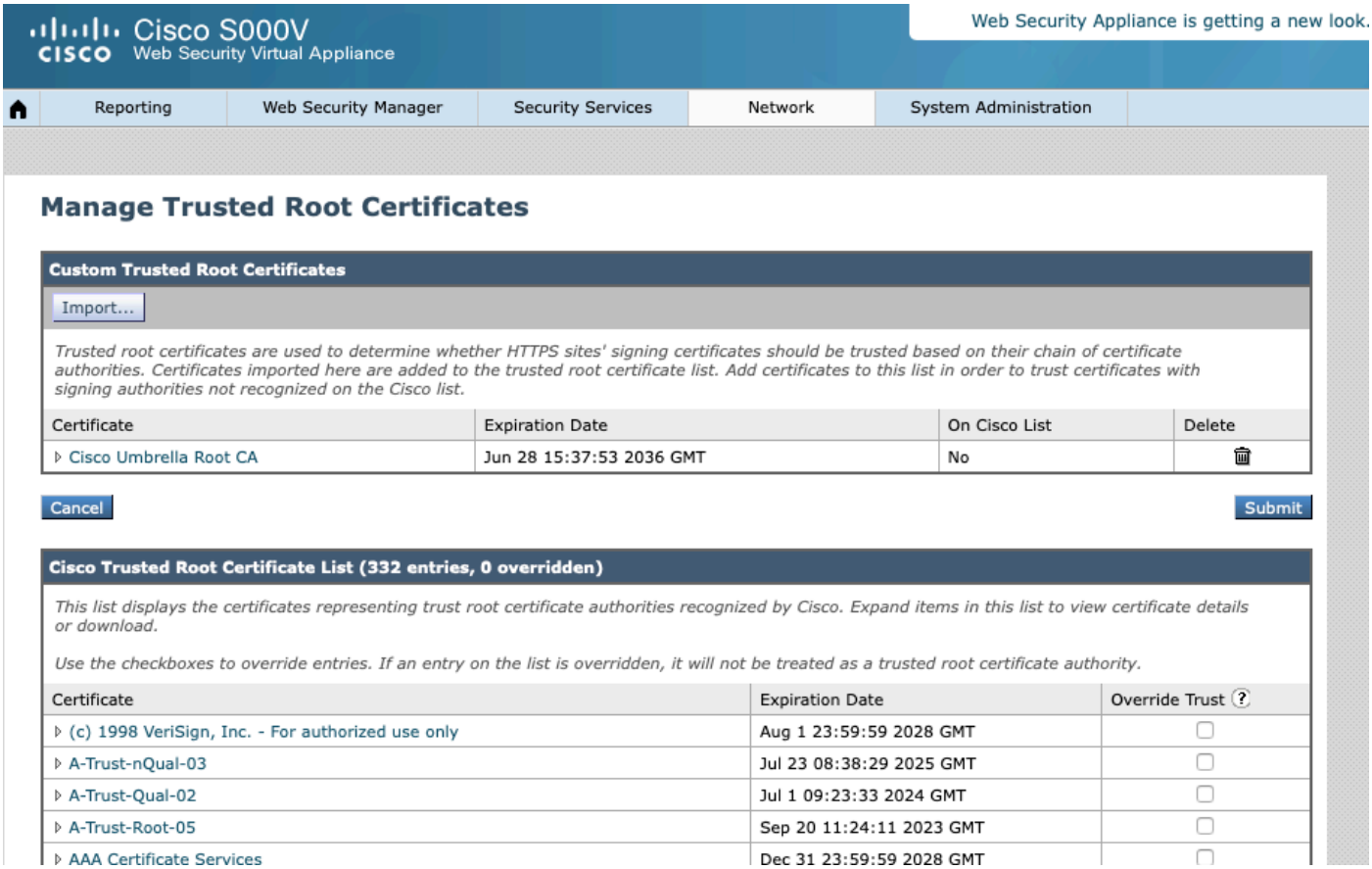
- SWGに内部IPベースのWebポリシーを実装するには、セキュリティサービス>プロキシ設定で、セキュアWebアプライアンスの「X-Forwarded-For」ヘッダーを必ず有効にしてください。



360050700111

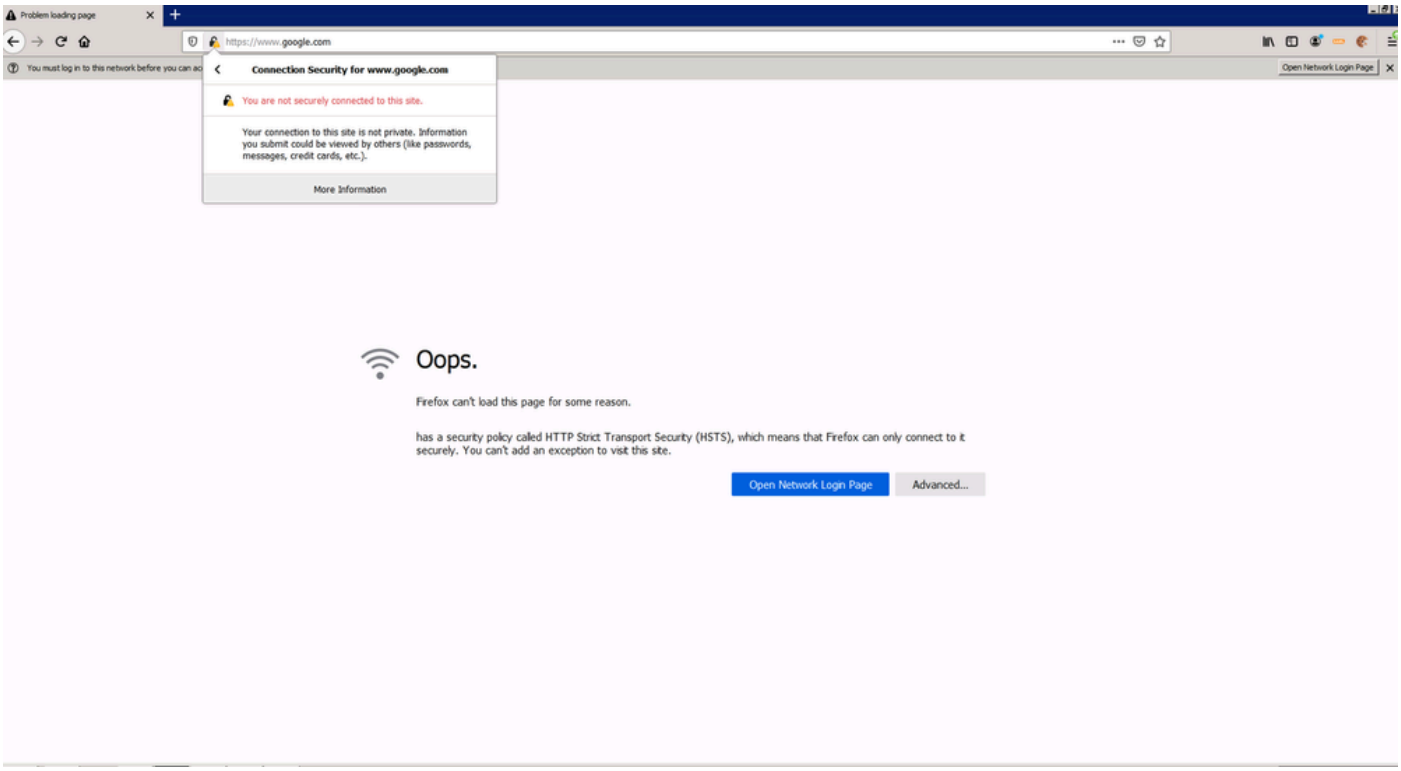
2. HTTP暗号化解除用の信頼されたルート証明書。

- HTTPs復号化がUmbrellaダッシュボードのWeb Policyで有効になっている場合は、Umbrella dashboard> Deployments> Configurationから「Ciscoルート証明書」をダウンロードし、Secure Web Applianceの信頼できるルート証明書にインポートします。



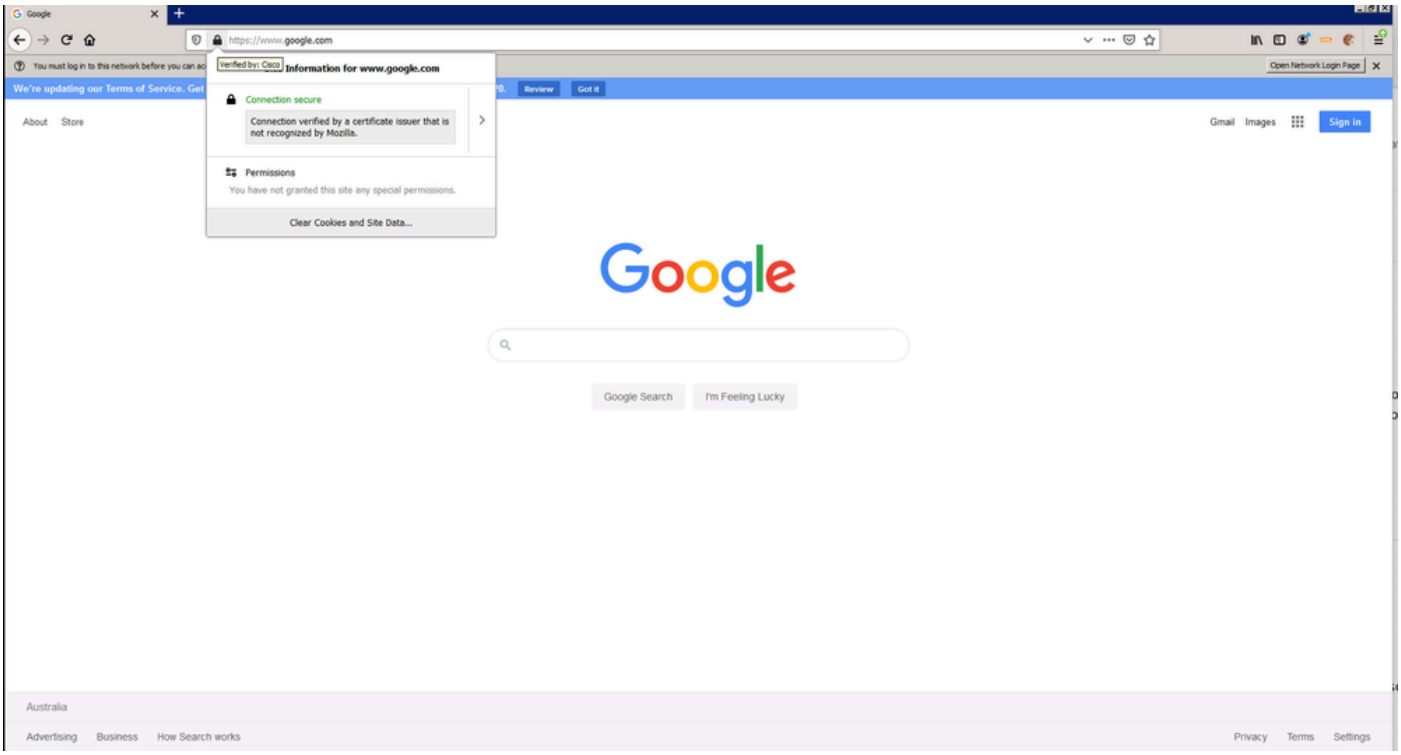
360050589612

- SWG Webポリシーで HTTPs復号化が有効になっている間に「Ciscoルート証明書」が Secure Web Applianceにインポートされていない場合、エンドユーザは次の例のようなエラーを受け取ります。
  - "Oops.（ブラウザ）は何らかの理由でこのページを読み込めません。にはHTTP Strict Transport Security (HSTS)と呼ばれるセキュリティポリシーがあります。つまり、（ブラウザ）は安全に接続することしかできません。このサイトにアクセスするための例外を追加することはできません。
  - 「このサイトに安全に接続されていません。」



360050700171

- これは、Umbrella SWGによって復号化されたHTTPの例です。証明書は、「Cisco」という名前の「Cisco Root Certificate」によって検証されます。



360050700191

UmbrellaダッシュボードでのSWG Webポリシーの設定

内部IPに基づくSWG Webポリシー：

- SWGは内部IPの識別にそのヘッダーを使用するため、セキュアWebアプライアンスで「X-Forwarded-For」ヘッダーを有効にしてください。
- Deployment > Networksで、Secure Web Applianceの出力IPを登録します。
- Deployment > Configuration > Internal Networksの順に選択し、クライアントマシンの内部IPを作成します。「Show Networks」をクリック/選択した後、登録済みのSecure Web Applianceの出力IP（ステップ1）を選択してください。
- ステップ2で作成した内部IPに基づいて新しいWebポリシーを作成します。
- Webポリシーで[SAMLを有効にする]オプションが無効になっていることを確認してください。

ADユーザ/グループに基づくSWG Webポリシー：

- すべてのADユーザとグループがUmbrellaダッシュボードにプロビジョニングされていることを確認します。
- 「SAMLを有効にする」オプションを有効にして、登録されたSecure Web Applianceの出力IPに基づいて新しいWebポリシーを作成します。
- 「Enable SAML」オプションを無効にして、ADユーザ/グループに基づいて新しいWebポリシーを作成します。また、このWebポリシーを手順2で作成したWebポリシーの前に配置する必要があります。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。