

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](#)

[概要](#)

[セキュアWebアプライアンスポリシーの設定](#)

[透過的なプロキシ導入](#)

[UmbrellaダッシュボードでのSWG Webポリシーの設定](#)

はじめに

このドキュメントでは、Secure Web Appliance(WSA)とUmbrella Secure Web Gateway(SWG)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/HTTPS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。

Group Name	Proxies	Load Balancing	Delete
SIGHTTP	146.112.255.50:80	None (Failover)	
SIGHTTPs	146.112.255.50:443	None (Failover)	

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。

Reporting	Web Security Manager	Security Services	Network	System Administration										
Custom and External URL Categories: Edit Category Edit Custom and External URL Category <table><tr><td>Category Name:</td><td>ProxyChainBypassList</td></tr><tr><td>List Order:</td><td>1</td></tr><tr><td>Category Type:</td><td>Local Custom Category</td></tr><tr><td>Sites: ?</td><td> .cisco.com, .isrg.trustid.ocsp.identrust.com, .login.microsoftonline.com, .ocsp.int-x3.letsencrypt.org, .okta.com, .oktacdn.com, .opendns.com, .pingidentity.com, .secure.aadcdn.microsoftonline-p.com, .umbrella.com Sort URLs Click the Sort URLs button to sort all site URLs in Alpha-numerical order. (e.g. 10.0.0.1, 2001:420:80:1::5, example.com.) </td></tr><tr><td>Advanced</td><td> Regular Expressions: ? Enter one regular expression per line. </td></tr></table> Cancel Submit					Category Name:	ProxyChainBypassList	List Order:	1	Category Type:	Local Custom Category	Sites: ?	.cisco.com, .isrg.trustid.ocsp.identrust.com, .login.microsoftonline.com, .ocsp.int-x3.letsencrypt.org, .okta.com, .oktacdn.com, .opendns.com, .pingidentity.com, .secure.aadcdn.microsoftonline-p.com, .umbrella.com Sort URLs Click the Sort URLs button to sort all site URLs in Alpha-numerical order. (e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)	Advanced	Regular Expressions: ? Enter one regular expression per line.
Category Name:	ProxyChainBypassList													
List Order:	1													
Category Type:	Local Custom Category													
Sites: ?	.cisco.com, .isrg.trustid.ocsp.identrust.com, .login.microsoftonline.com, .ocsp.int-x3.letsencrypt.org, .okta.com, .oktacdn.com, .opendns.com, .pingidentity.com, .secure.aadcdn.microsoftonline-p.com, .umbrella.com Sort URLs Click the Sort URLs button to sort all site URLs in Alpha-numerical order. (e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)													
Advanced	Regular Expressions: ? Enter one regular expression per line.													

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。

Reporting Web Security Manager Security Services Network System Administration

Routing Policy: BypassProxyChain

Policy Settings

☒ Enable Policy

Policy Name: (e.g. my IT policy)

Description:

Insert Above Policy:

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

If "All Identification Profiles" is selected, at least one Advanced membership option must also be selected.

☒ Advanced Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents. The following advanced membership criteria have been defined:

Protocols:

Proxy Ports:

Subnets:

Time Range:

URL Categories:

User Agents:

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。

Reporting Web Security Manager Security Services Network System Administration

Routing Policies: Policy "SIGALLHTTP": Membership by Protocol

Advanced Membership Definition: Protocols

Policy membership can be defined to apply to one or more protocols. Leave all protocols unselected if membership by protocol is not desired.

Protocols: ☒ HTTP ☐ FTP over HTTP ☐ Native FTP ☐ All others

Note: Policy membership by HTTPS is not available when the HTTPS proxy is enabled.

360050592772

Reporting Web Security Manager Security Services Network System Administration

Routing Policy: SIGALLHTTP

Policy Settings

☒ Enable Policy

Policy Name: (e.g. my IT policy)

Description:

Insert Above Policy:

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

If "All Identification Profiles" is selected, at least one Advanced membership option must also be selected.

Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Protocols: HTTP
 Proxy Ports: None Selected
 Subnets: None Selected
 Time Range: No Time Range Definitions Available
(see Web Security Manager > Defined Time Ranges)
URL Categories: None Selected
 User Agents: None Selected

"Protocols" can only be selected while using "All Identification Profiles"

Cancel Submit

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。

Reporting	Web Security Manager	Security Services	Network	System Administration
Identification Profiles				
Client / User Identification Profiles				
Add Identification Profile...				
Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
1	win2k8 Subnets: 192.168.0.212 Protocols: HTTP/HTTPS	Exempt from Authentication / User Identification	(global profile)	

360050703971

Reporting Web Security Manager Security Services Network System Administration

Routing Policy: Win2k8HTTps

Policy Settings

☒ Enable Policy

Policy Name: Win2k8HTTps
(e.g. my IT policy)

Description:

Insert Above Policy: 4 (Win2016ProxyChainHTTps)

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users: Select One or More Identification Profiles

Identification Profile	Authorized Users and Groups	
win2k8	No authentication required	Add Identification Profile

☒ Advanced

Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents. The following advanced membership criteria have been defined:

Protocols: HTTP/HTTPS/FTP over HTTP in Identification Profile win2k8
Proxy Ports: None Selected
Subnets: None Selected
Time Range: No Time Range Definitions Available
(see Web Security Manager > Defined Time Ranges)
URL Categories: None Selected
User Agents: None Selected

Cancel
Submit

"Protocols" can't be selected for the individual "Identification Profile"

360050700091

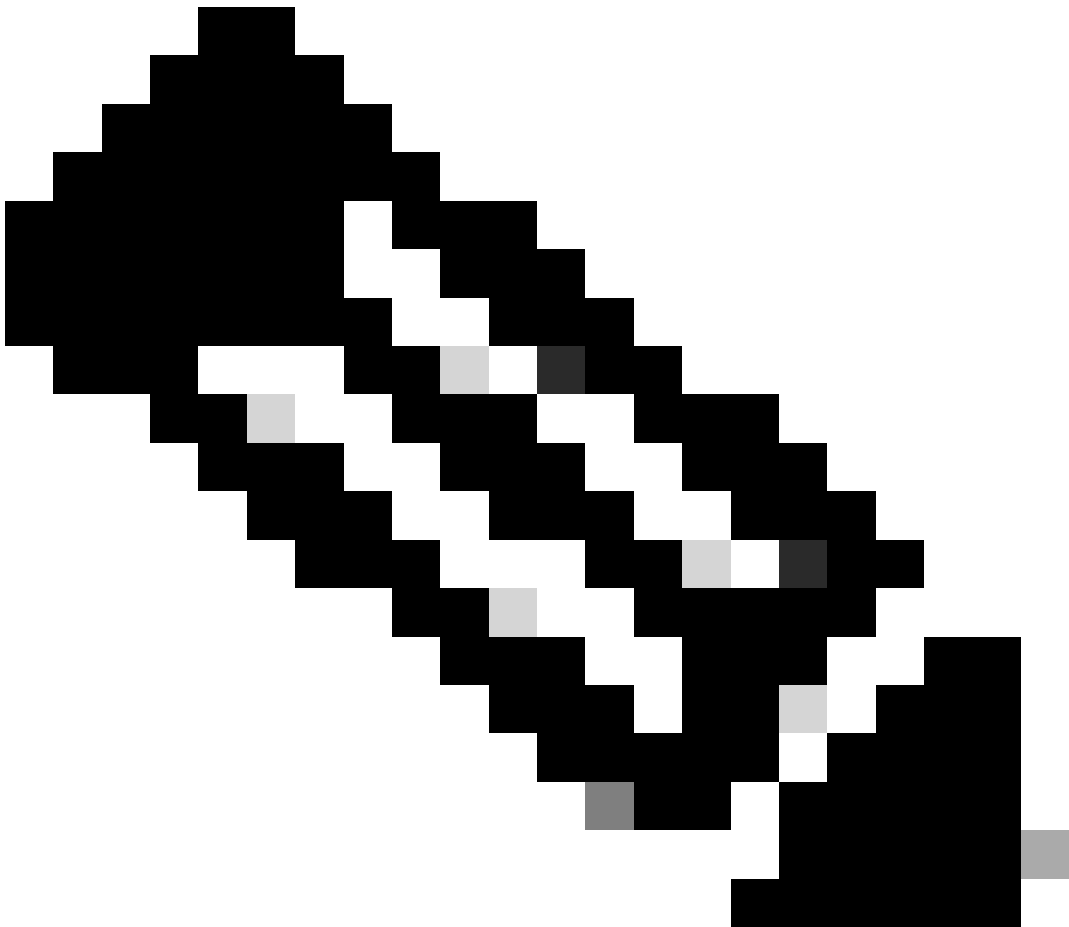
5. セキュアWebアプライアンスルーティングポリシーの最終設定：

- 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り、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。

Routing Policies

Routing Definitions			
Add Policy...			
Order	Members	Routing Destination	Delete
1	BypassProxyChain Identification Profile: All URL Categories: ProxyChainBypassList	Direct Connection	
2	SIGALLHTTPs (disabled) Identification Profile: All Protocols: All others	SIGHTTPs proxy.sig.umbrella.com:443	
3	SIGALLHTTP Identification Profile: All Protocols: HTTP	SIGHTTP proxy.sig.umbrella.com:80	
4	Win2k8HTTPs Identification Profile: win2k8 All identified users	SIGHTTPs proxy.sig.umbrella.com:443	
5	Win2016ProxyChainHTTPs Identification Profile: Win2016 All identified users	SIGHTTPs proxy.sig.umbrella.com:443	

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。

Home

Reporting

Web Security Manager

Security Services

Network

System Administration

Proxy Settings

Web Proxy Settings

Basic Settings

Proxy:	Enabled
HTTP Ports to Proxy:	80, 3128
Caching:	Disabled Clear Cache
Proxy Mode:	Transparent
IP Spoofing:	Not Enabled

Advanced Settings

Persistent Connection Timeout:	Client Side: 300 Seconds Server Side: 300 Seconds
In-Use Connection Timeout:	Client Side: 300 Seconds Server Side: 300 Seconds
Simultaneous Persistent Connections:	Server Maximum Number: 2000
Generate Headers:	X-Forwarded-For: Send Request Side VIA: Send Response Side VIA: Send
Use Received Headers:	Identification of Client IP Addresses using X-Forwarded-For: Disabled
Range Request Forwarding:	Disabled

Edit Settings...

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。

Cisco S000V
Web Security Virtual Appliance

Web Security Appliance is getting a new look.

Home

Reporting

Web Security Manager

Security Services

Network

System Administration

Manage Trusted Root Certificates

Custom Trusted Root Certificates

Import...

Trusted root certificates are used to determine whether HTTPS sites' signing certificates should be trusted based on their chain of certificate authorities. Certificates imported here are added to the trusted root certificate list. Add certificates to this list in order to trust certificates with signing authorities not recognized on the Cisco list.

Certificate	Expiration Date	On Cisco List	Delete
▸ Cisco Umbrella Root CA	Jun 28 15:37:53 2036 GMT	No	

Cancel

Submit

Cisco Trusted Root Certificate List (332 entries, 0 overridden)

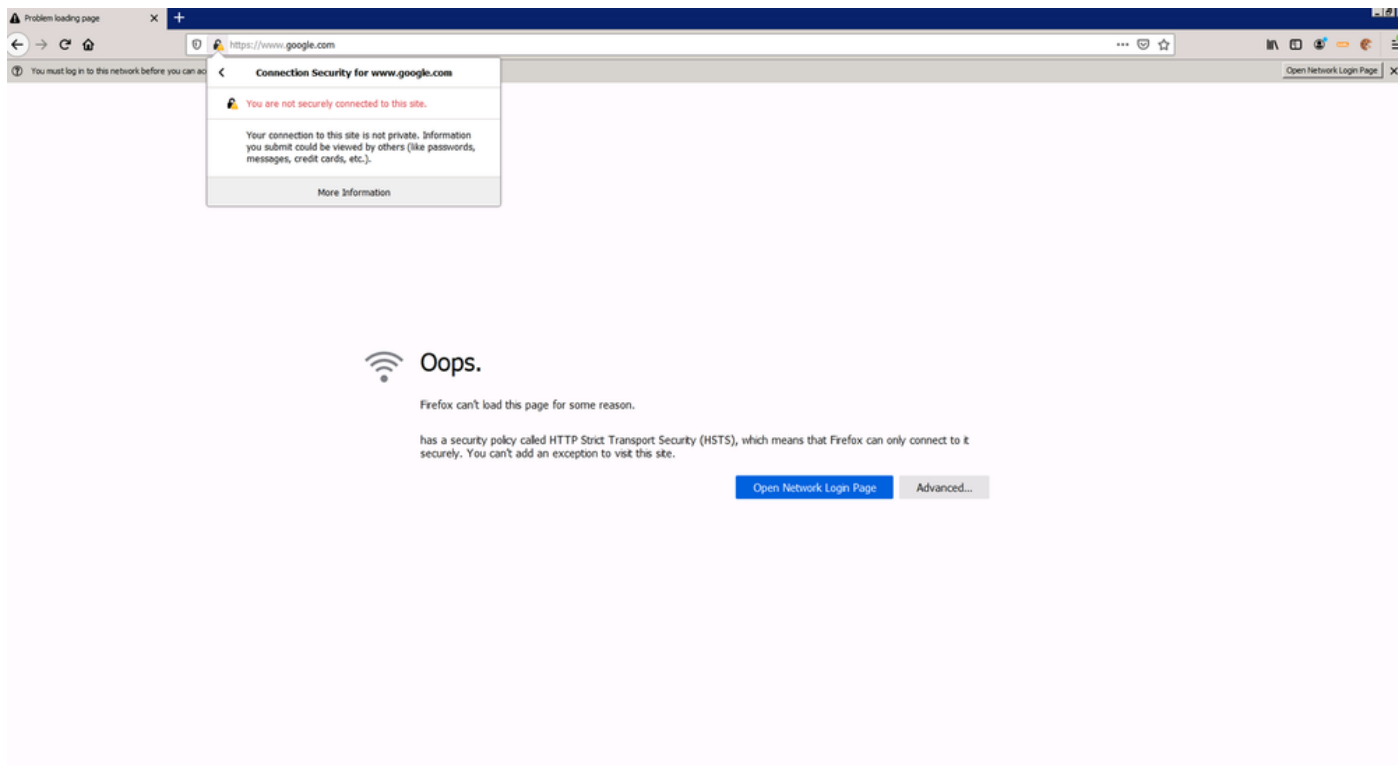
This list displays the certificates representing trust root certificate authorities recognized by Cisco. Expand items in this list to view certificate details or download.

Use the checkboxes to override entries. If an entry on the list is overridden, it will not be treated as a trusted root certificate authority.

Certificate	Expiration Date	Override Trust ?
▸ (c) 1998 VeriSign, Inc. - For authorized use only	Aug 1 23:59:59 2028 GMT	☐
▸ A-Trust-nQual-03	Jul 23 08:38:29 2025 GMT	☐
▸ A-Trust-Qual-02	Jul 1 09:23:33 2024 GMT	☐
▸ A-Trust-Root-05	Sep 20 11:24:11 2023 GMT	☐
▸ AAA Certificate Services	Dec 31 23:59:59 2028 GMT	☐

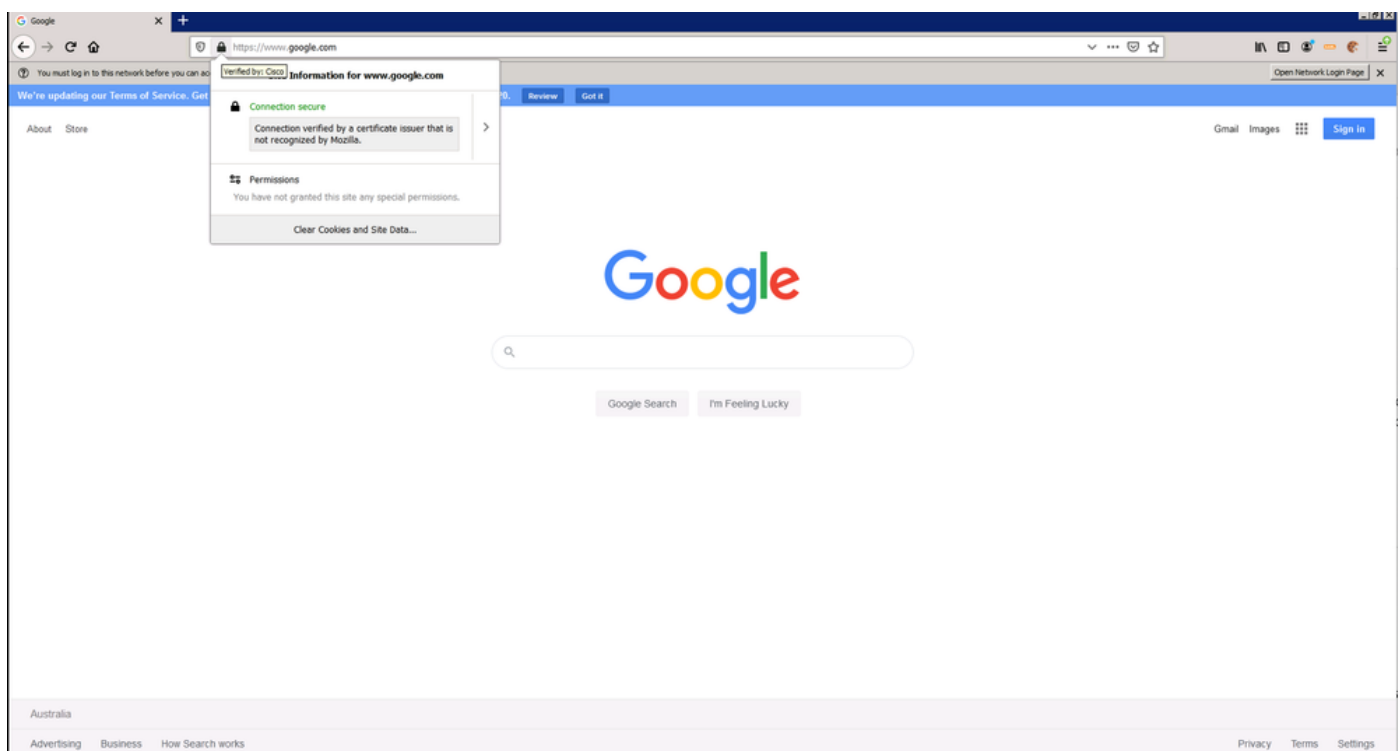
360050589612

- 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。