

Konfigurieren der Proxykette zwischen der sicheren Web-Appliance und der Umbrella SWG

Inhalt

[Einleitung](#)

[Überblick](#)

[Richtlinienkonfiguration für sichere Web-Appliance](#)

[Für transparente Proxy-Bereitstellung](#)

[SWG-Webrichtlinienkonfiguration im Umbrella Dashboard](#)

Einleitung

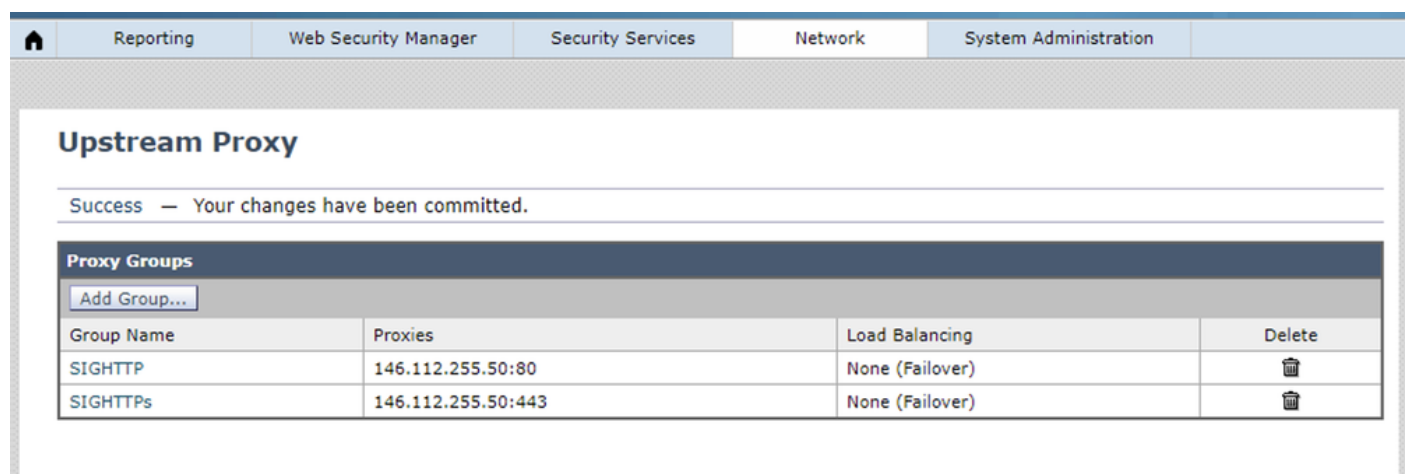
In diesem Dokument wird beschrieben, wie die Proxykette zwischen der sicheren Webappliance und dem Umbrella Secure Web Gateway (SWG) konfiguriert wird.

Überblick

Umbrella SIG unterstützt die Proxy-Kette und kann alle HTTP/HTTPs Anfragen vom Downstream Proxy-Server verarbeiten. Dies ist ein umfassender Leitfaden zur Implementierung der Proxy-Kette zwischen der [Cisco Secure Web Appliance \(ehemals Cisco WSA\)](#) und dem [Umbrella Secure Web Gateway \(SWG\)](#), einschließlich der Konfiguration für die Secure Web Appliance und die SWG.

Richtlinienkonfiguration für sichere Web-Appliance

1. Konfigurieren Sie die SWG HTTP- und HTTPs-Links als Upstream-Proxy über Netzwerk>Upstream-Proxy.



The screenshot shows the 'Upstream Proxy' configuration page in the Umbrella dashboard. The top navigation bar includes 'Reporting', 'Web Security Manager', 'Security Services', 'Network', and 'System Administration'. The main content area has a title 'Upstream Proxy' and a success message: 'Success — Your changes have been committed.' Below this is a table titled 'Proxy Groups' with an 'Add Group...' button. The table has four columns: 'Group Name', 'Proxies', 'Load Balancing', and 'Delete'. There are two rows of data:

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

2. Erstellen Sie eine Umgehungsrichtlinie über Websicherheits-Manager>Routingrichtlinie, um alle vorgeschlagenen URLs direkt an das Internet weiterzuleiten. Alle umgeleiteten URLs finden Sie in unserer Dokumentation: [Cisco Umbrella SIG Benutzerhandbuch: Verwalten der Proxy-Verkettung](#)

- Erstellen Sie zunächst eine neue "benutzerdefinierte Kategorie", indem Sie wie hier dargestellt zu "Websicherheits-Manager>Benutzerdefinierte und externe URL-Kategorien" navigieren. Die Umgehungsrichtlinie basiert auf der "benutzerdefinierten Kategorie".

The screenshot shows the 'Edit Custom and External URL Category' form. The form has a header bar with the title 'Edit Custom and External URL Category'. Below the header, there are several input fields: 'Category Name' (containing 'ProxyChainBypassList'), 'List Order' (containing '1'), and 'Category Type' (set to 'Local Custom Category'). The 'Sites' field is a large text area containing a list of domains: '.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'. To the right of the 'Sites' field is a 'Sort URLs' button with a tooltip that says 'Click the Sort URLs button to sort all site URLs in Alpha-numerical order.' Below the 'Sites' field is an 'Advanced' section with a 'Regular Expressions' field. The 'Regular Expressions' field has a placeholder text 'Enter one regular expression per line.' At the bottom of the form are 'Cancel' and 'Submit' buttons.

Edit Custom and External URL Category	
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

- Erstellen Sie anschließend eine neue Umgehungs-Routingrichtlinie, indem Sie zu Websicherheits-Manager > Routingrichtlinie navigieren. Stellen Sie sicher, dass es sich um die erste Richtlinie handelt, da die sichere Web-Appliance mit der Richtlinie in der Reihenfolge der Richtlinien übereinstimmt.

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.

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:
(see Web Security Manager > Defined Time Ranges)

URL Categories:

User Agents:

360050703131

3. Erstellen Sie eine neue Routingrichtlinie für alle HTTP-Anfragen.

- In der Mitglieddefinition der Richtlinie für das Routing der sicheren Webappliance lauten die Protokolloptionen HTTP, FTP über HTTP, Natives FTP und "Alle anderen", während "Alle Identifikationsprofile" ausgewählt sind. Da es keine Option für HTTPs gibt, erstellen Sie die Routingrichtlinie für HTTPs-Anforderungen einzeln, nachdem Sie diese Routingrichtlinie für alle HTTP-Anforderungen implementiert haben.

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"

360050589572

4. Erstellen Sie die Routingrichtlinie für HTTP-Anforderungen auf Basis des "Identification Profile" (Identifikationsprofils). Seien Sie vorsichtig mit der Abfolge des definierten "Identifikationsprofils", da die sichere Web-Appliance der "Identifikation" für die erste Übereinstimmung entspricht. In diesem Beispiel ist das Identifikationsprofil "win2k8" eine interne IP-basierte Identität.

Reporting Web Security Manager Security Services Network System Administration

Identification Profiles

Client / User Identification Profiles

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)	Delete

360050703971

Reporting Web Security Manager Security Services Network System Administration

Routing Policy: Win2k8HTTPs

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:

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

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

Cancel Submit

360050700091

5. Endgültige Konfigurationen für die Routing-Richtlinien der sicheren Web-Appliance:

- Beachten Sie, dass die sichere Web-Appliance die Identitäten und Zugriffsrichtlinien mit einem "Top-Down"-Regelverarbeitungsansatz auswertet. Dies bedeutet, dass die erste Übereinstimmung, die an einem beliebigen Punkt in der Verarbeitung vorgenommen wird, zu der von der sicheren Web-Appliance durchgeführten Aktion führt.
- Zusätzlich werden Identitäten zuerst ausgewertet. Sobald der Zugriff eines Clients mit einer bestimmten Identität übereinstimmt, überprüft die sichere Webappliance alle Zugriffsrichtlinien, die so konfiguriert sind, dass sie die Identität verwenden, die mit dem Zugriff des Clients übereinstimmt.

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

Anmerkung: Die genannte Richtlinienkonfiguration gilt nur für die explizite Proxy-Bereitstellung.

Für transparente Proxy-Bereitstellung

Im Fall von transparentem HTTPS hat AsyncOS keinen Zugriff auf Informationen im Client-Header. Daher kann AsyncOS keine Routingrichtlinien erzwingen, wenn eine Routingrichtlinie oder ein Identifizierungsprofil auf den Informationen in den Client-Headern beruht.

1. Transparent umgeleitete HTTPS-Transaktionen stimmen nur mit Routingrichtlinien überein, wenn:
 - Für die Routing-Richtliniengruppe sind keine Kriterien für die Richtlinienmitgliedschaft wie URL-Kategorie, Benutzer-Agent usw. definiert.
 - Für das Identifizierungsprofil sind keine Kriterien für die Richtlinienmitgliedschaft wie URL-Kategorie, Benutzer-Agent usw. definiert.
2. Wenn für ein Identifizierungsprofil oder eine Routing-Richtlinie eine benutzerdefinierte URL-Kategorie definiert wurde, stimmen alle transparenten HTTPS-Transaktionen mit der Standardroutingrichtliniengruppe überein.
3. Vermeiden Sie so weit wie möglich die Konfiguration der Routing-Richtlinie mit allen Identifikationsprofilen, da dies dazu führen kann, dass transparente HTTPS-Transaktionen mit der standardmäßigen Routing-Richtliniengruppe übereinstimmen.

1. X-Forwarded-For-Header

- um die interne IP-basierte Webrichtlinie in SWG zu implementieren. Stellen Sie sicher, dass Sie den Header "X-Forwarded-For" in der sicheren Webappliance über Sicherheitsdienste > Proxy-Einstellungen aktivieren.

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. Vertrauenswürdiges Stammzertifikat für HTTP-Entschlüsselung.

- Wenn die HTTP-Entschlüsselung unter Webrichtlinie im Umbrella Dashboard aktiviert ist, laden Sie "Cisco Root Certificate" vom Umbrella Dashboard> Deployments> Configuration herunter, und importieren Sie es in die vertrauenswürdigen Stammzertifikate der Secure Web Appliance.

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)

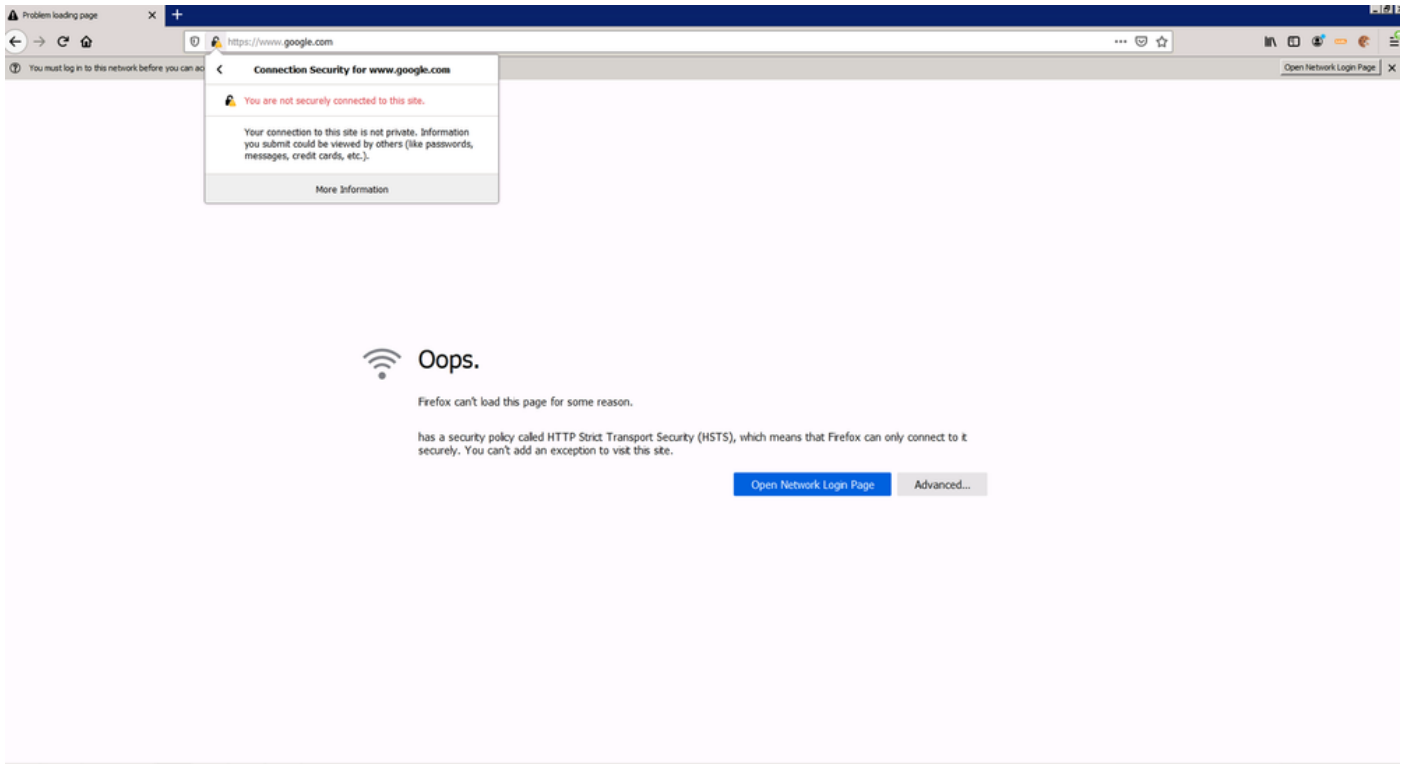
This list displays the certificates representing trust root certificate authorities recognized by Cisco. Expand items in this list to view certificate details or download.

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	☐

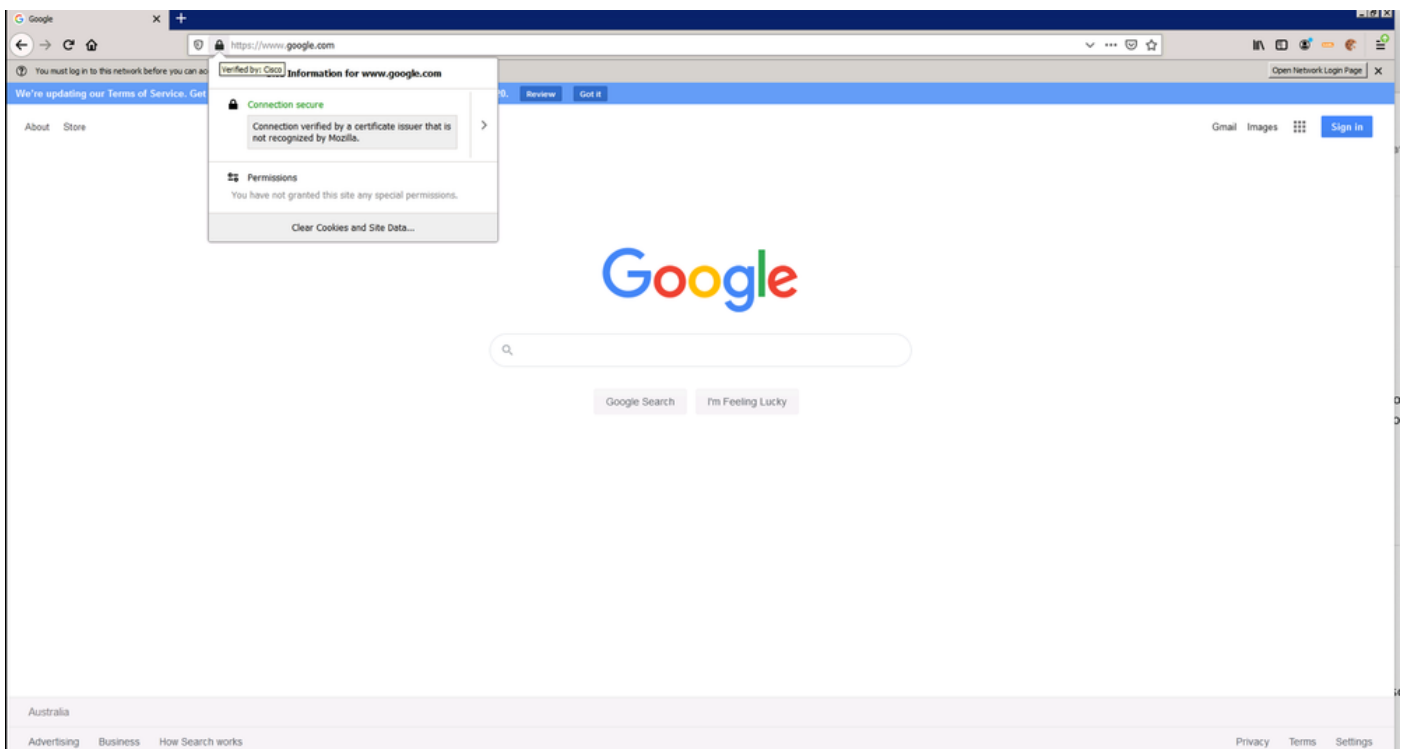
360050589612

- Wenn das "Cisco Root Certificate" nicht in die sichere Web-Appliance importiert wurde, während die HTTP-Entschlüsselung in der SWG-Webrichtlinie aktiviert ist, erhält der Endbenutzer einen ähnlichen Fehler wie in diesem Beispiel:
 - "Hoppla. (Browser) kann diese Seite aus irgendeinem Grund nicht laden. verfügt über eine Sicherheitsrichtlinie mit der Bezeichnung HTTP Strict Transport Security (HSTS), was bedeutet, dass (Browser) nur eine sichere Verbindung zu dieser herstellen kann. Sie können keine Ausnahme hinzufügen, um diese Website aufzurufen."
 - "Sie sind nicht sicher mit dieser Website verbunden."



360050700171

- Dies ist ein Beispiel für die von Umbrella SWG entschlüsselten HTTPs. Das Zertifikat wird durch das "Cisco Root Certificate" mit dem Namen "Cisco" verifiziert.



360050700191

SWG-Webrichtlinienkonfiguration im Umbrella Dashboard

SWG-Webrichtlinie auf Basis der internen IP:

- Stellen Sie sicher, dass Sie den "X-Forwarded-For"-Header in der sicheren Web-Appliance aktivieren, da sich die SWG bei der Identifizierung der internen IP darauf verlässt.
- Registrieren Sie die Ausgangs-IP der sicheren Web-Appliance unter Bereitstellung > Netzwerke.
- Erstellen Sie eine interne IP-Adresse des Client-Computers unter Deployment > Configuration > Internal Networks (Bereitstellung > Konfiguration > Interne Netzwerke). Wählen Sie die registrierte Ausgangs-IP der sicheren Web-Appliance (Schritt 1) aus, nachdem Sie "Netzwerke anzeigen" angekreuzt bzw. ausgewählt haben.
- Erstellen Sie eine neue Web-Richtlinie auf Basis der in Schritt 2 erstellten internen IP.
- Stellen Sie sicher, dass die Option "SAML aktivieren" in der Webrichtlinie deaktiviert ist.

SWG-Webrichtlinie basierend auf AD-Benutzer/Gruppe:

- Stellen Sie sicher, dass alle AD-Benutzer und -Gruppen für das Umbrella Dashboard bereitgestellt werden.
- Erstellen Sie eine neue Webrichtlinie, die auf der registrierten Ausgangs-IP-Adresse der sicheren Web-Appliance basiert, und aktivieren Sie die Option "SAML aktivieren".
- Erstellen Sie eine neue Webrichtlinie auf Basis des AD-Benutzers bzw. der AD-Gruppe, wobei die Option "SAML aktivieren" deaktiviert ist. Sie müssen diese Webrichtlinie auch vor die in Schritt 2 erstellte Webrichtlinie stellen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.