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

## Inhalt



## Einleitung

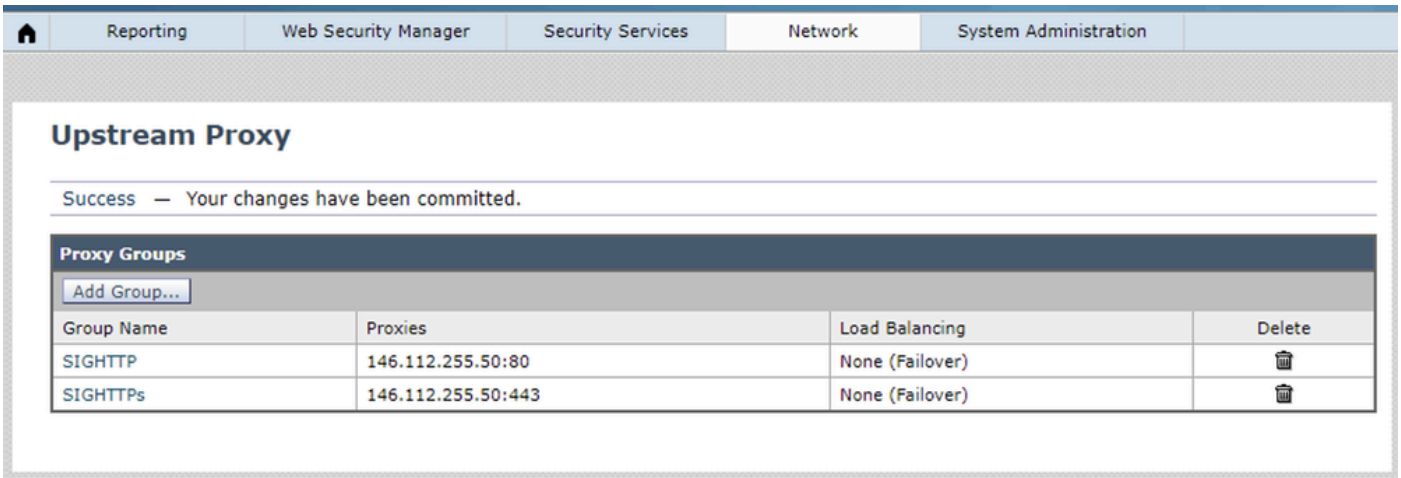
In diesem Dokument wird beschrieben, wie die Proxykette zwischen der sicheren Webappliance und dem Umbrella Secure Web Gateway (SWG) konfiguriert wird.

## 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.

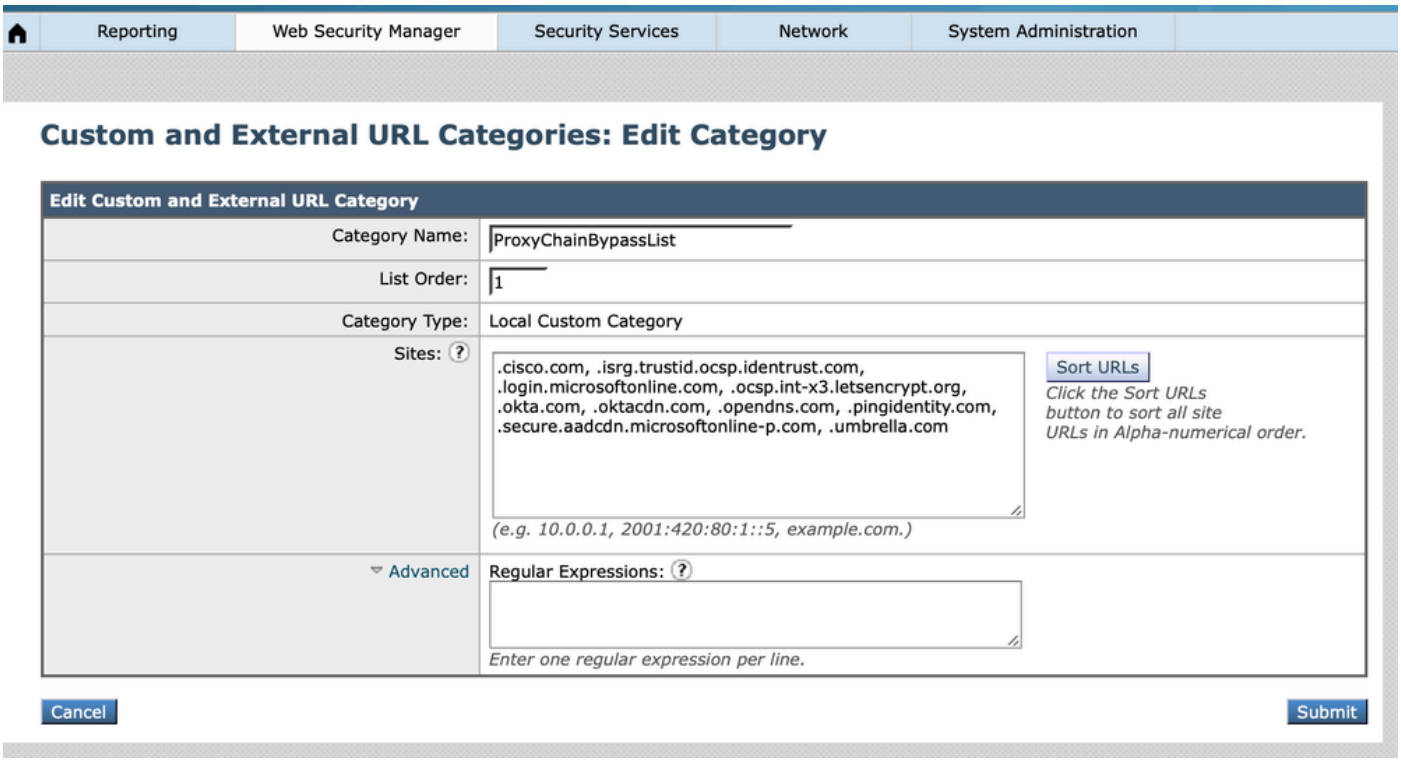
## Richtlinienkonfiguration für sichere Web-Appliance

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



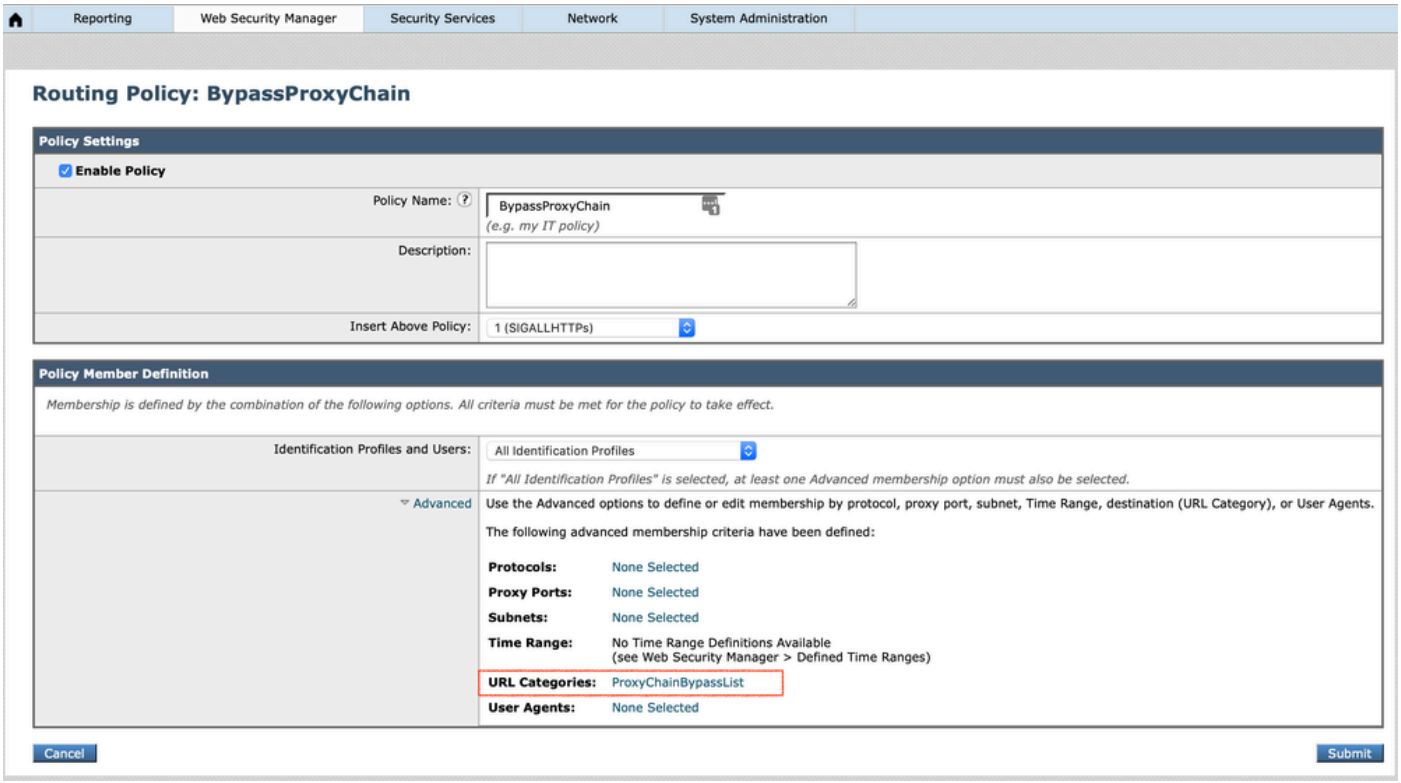
2. Erstellen Sie eine Umgehungsrichtlinie über Websicherheits-Manager>Routingrichtlinie, um alle vorgeschlagenen URLs direkt an das Internet weiterzuleiten. Alle umgeleiteten URLs finden Sie in unserer Dokumentation: [Cisco Umbrella SIG Benutzerhandbuch: Verwalten der Proxy-Verkettung]

- 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".




360050592552

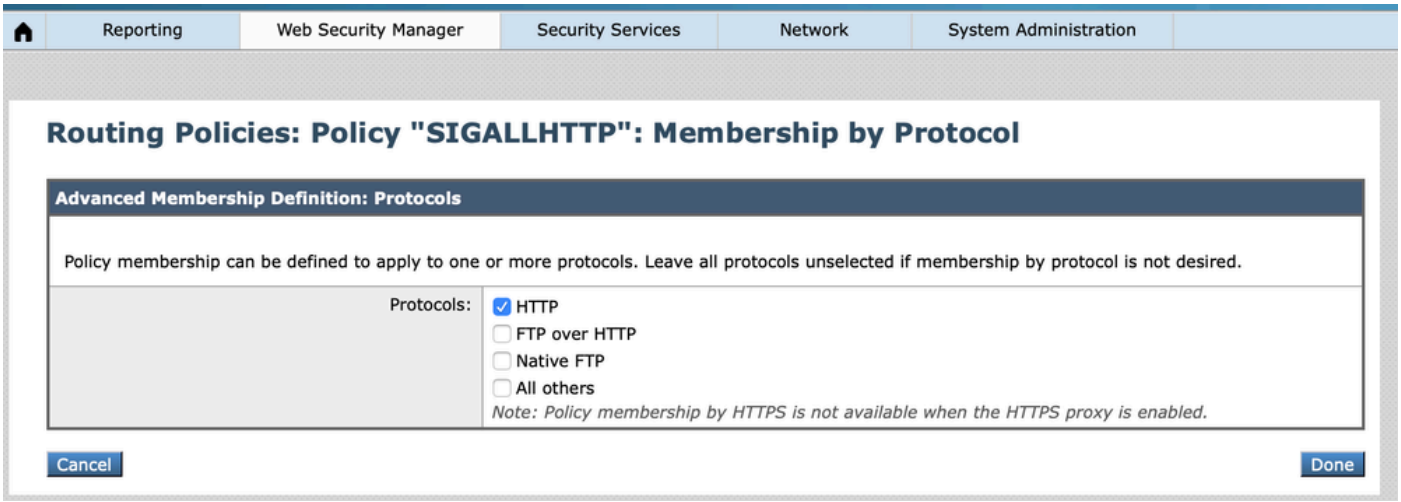
- Erstellen Sie anschließend eine neue Umgehungs-Routingrichtlinie, indem Sie zu Websicherheits-Manager > Routingrichtlinie navigieren. Stellen Sie sicher, dass es sich um die erste Richtlinie handelt, da die sichere Web-Appliance mit der Richtlinie in der Reihenfolge der Richtlinien übereinstimmt.



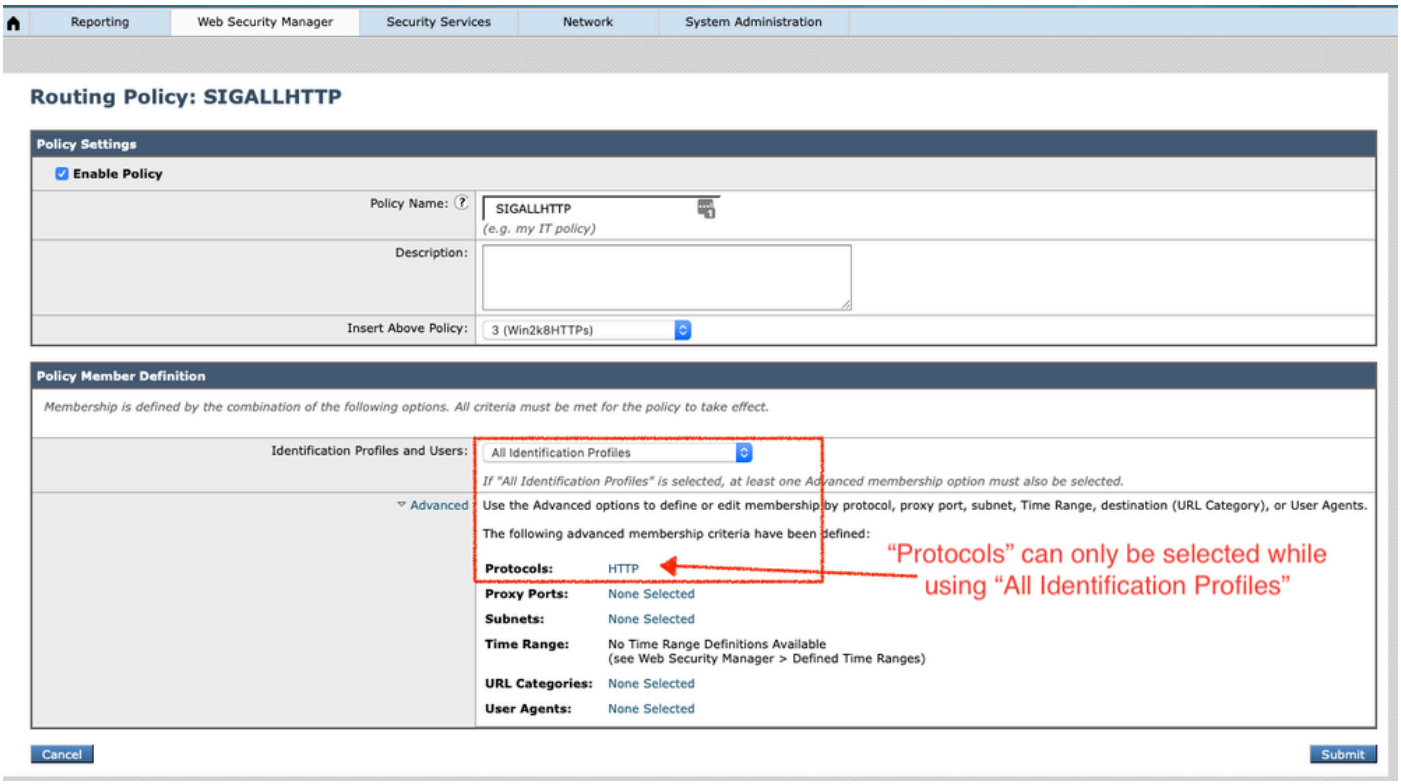

360050703131

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.

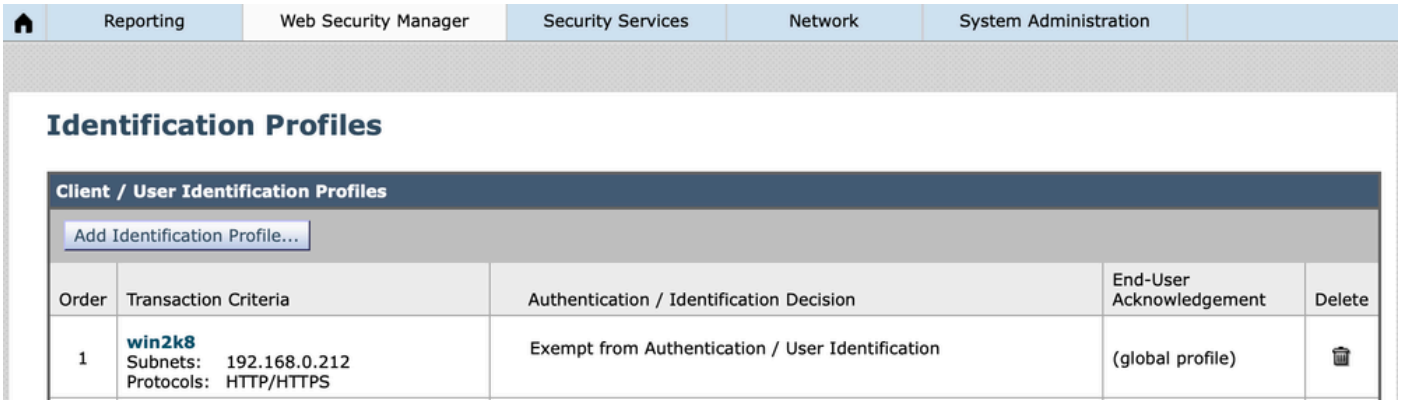



360050592772

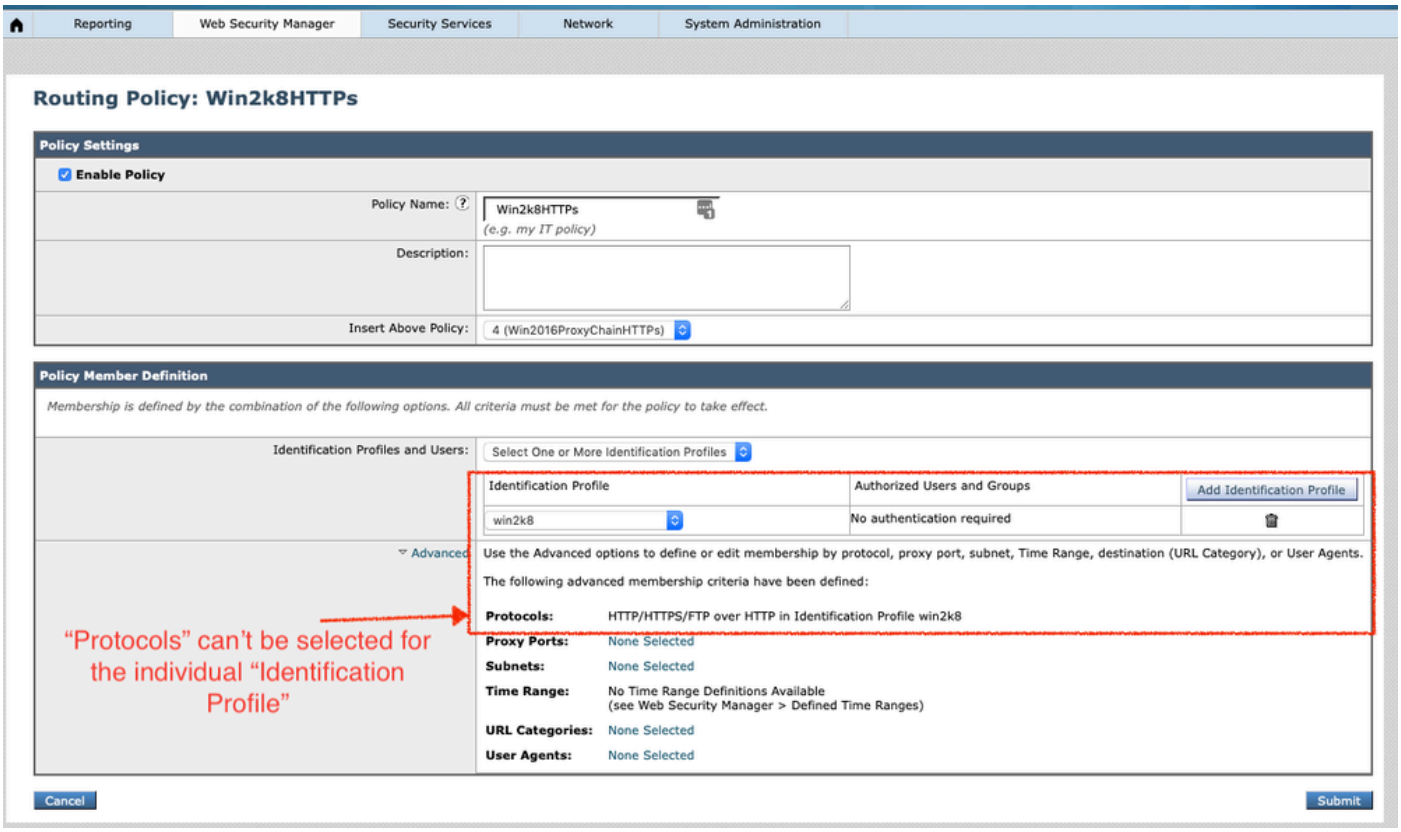



360050589572

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.



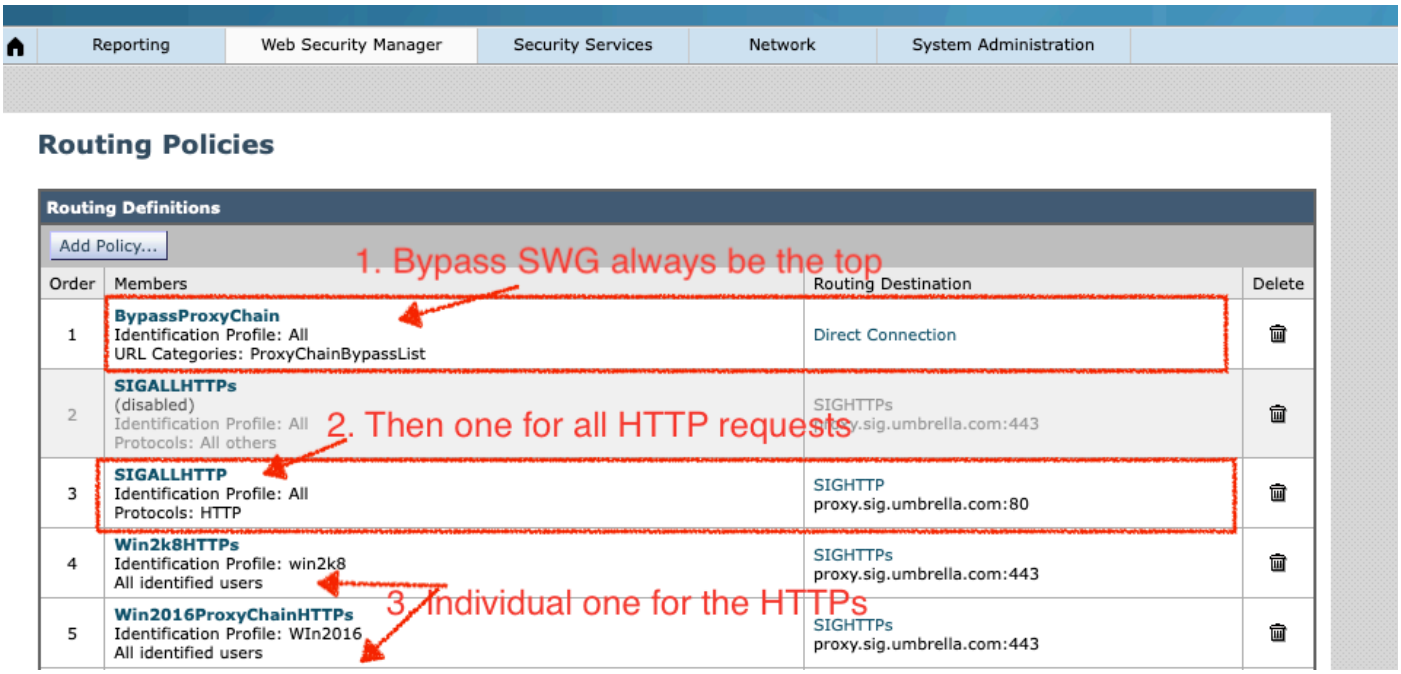

360050703971



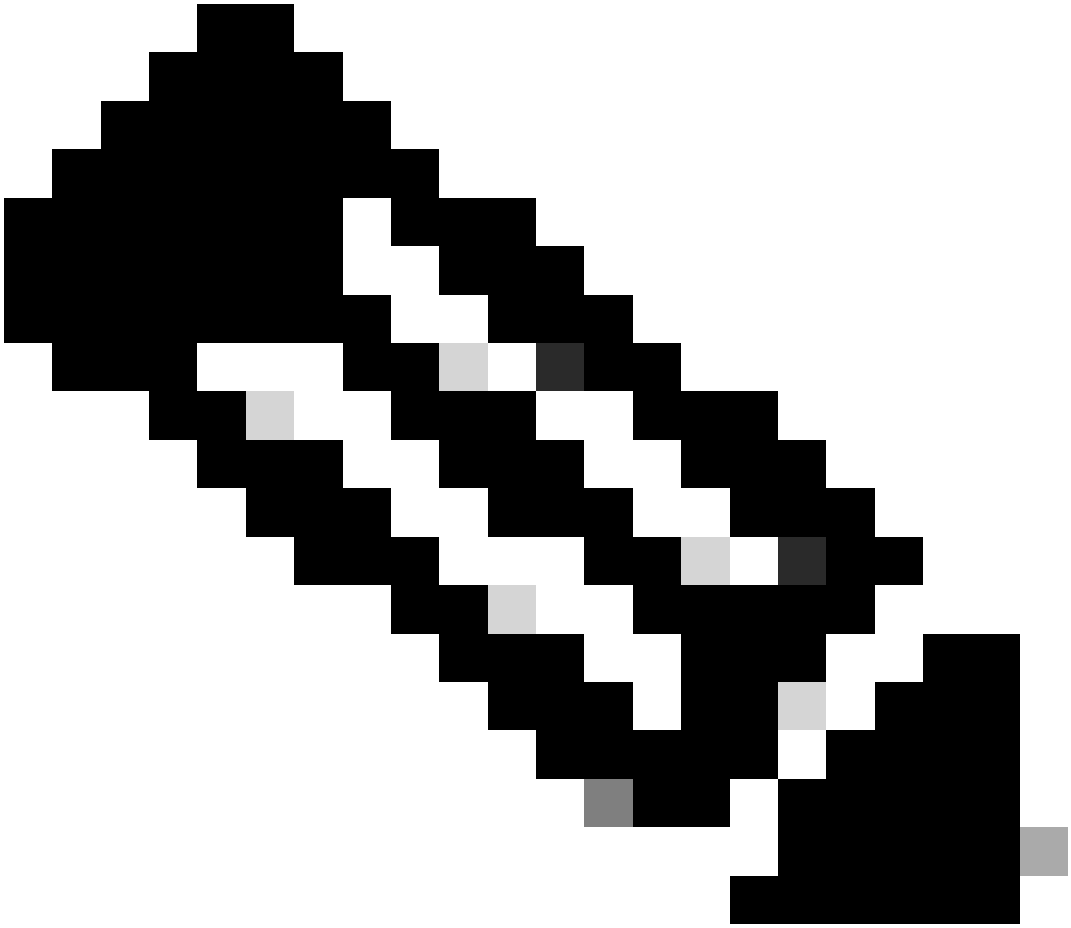

360050700091

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.




360050700131



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

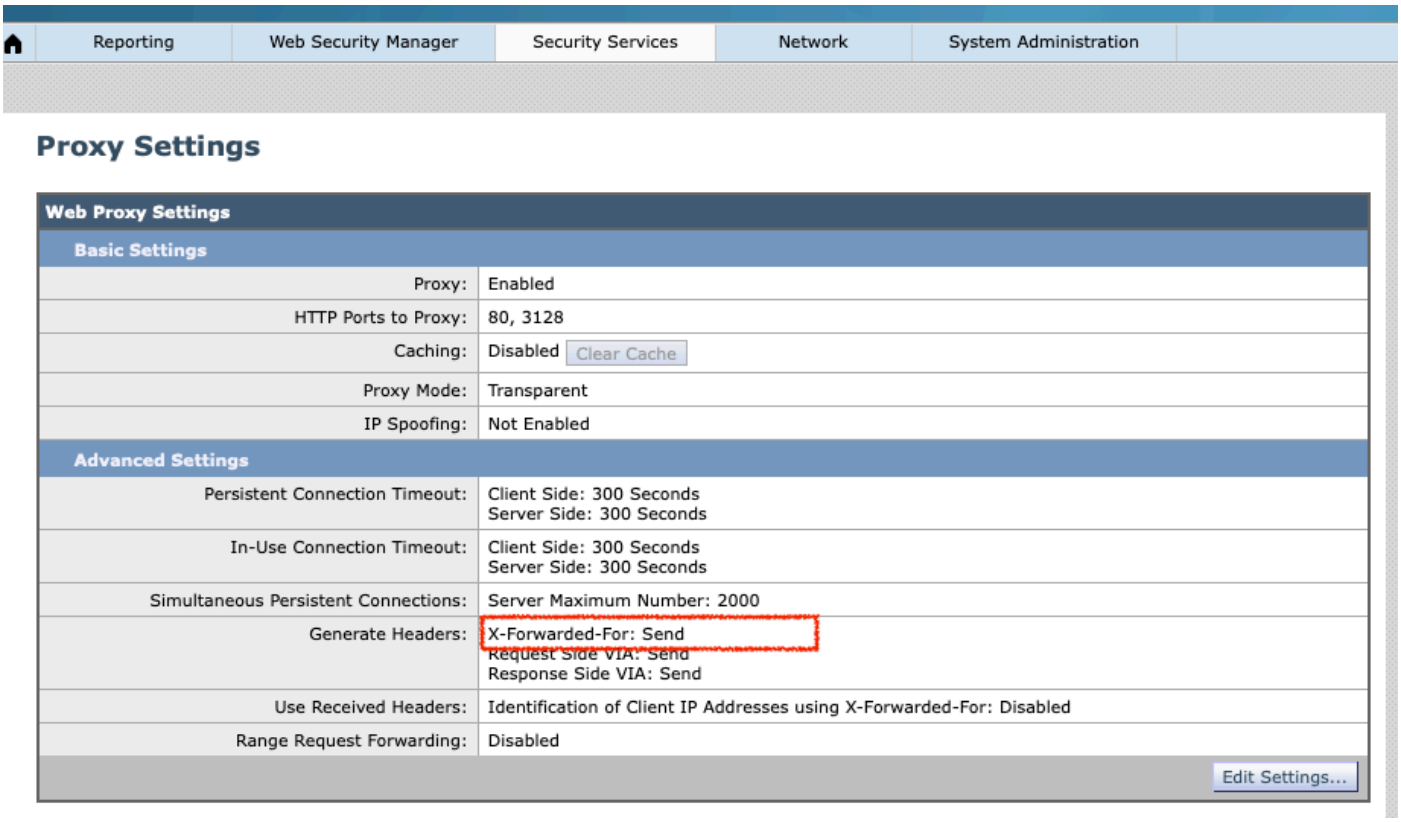
## Für transparente Proxy-Bereitstellung

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

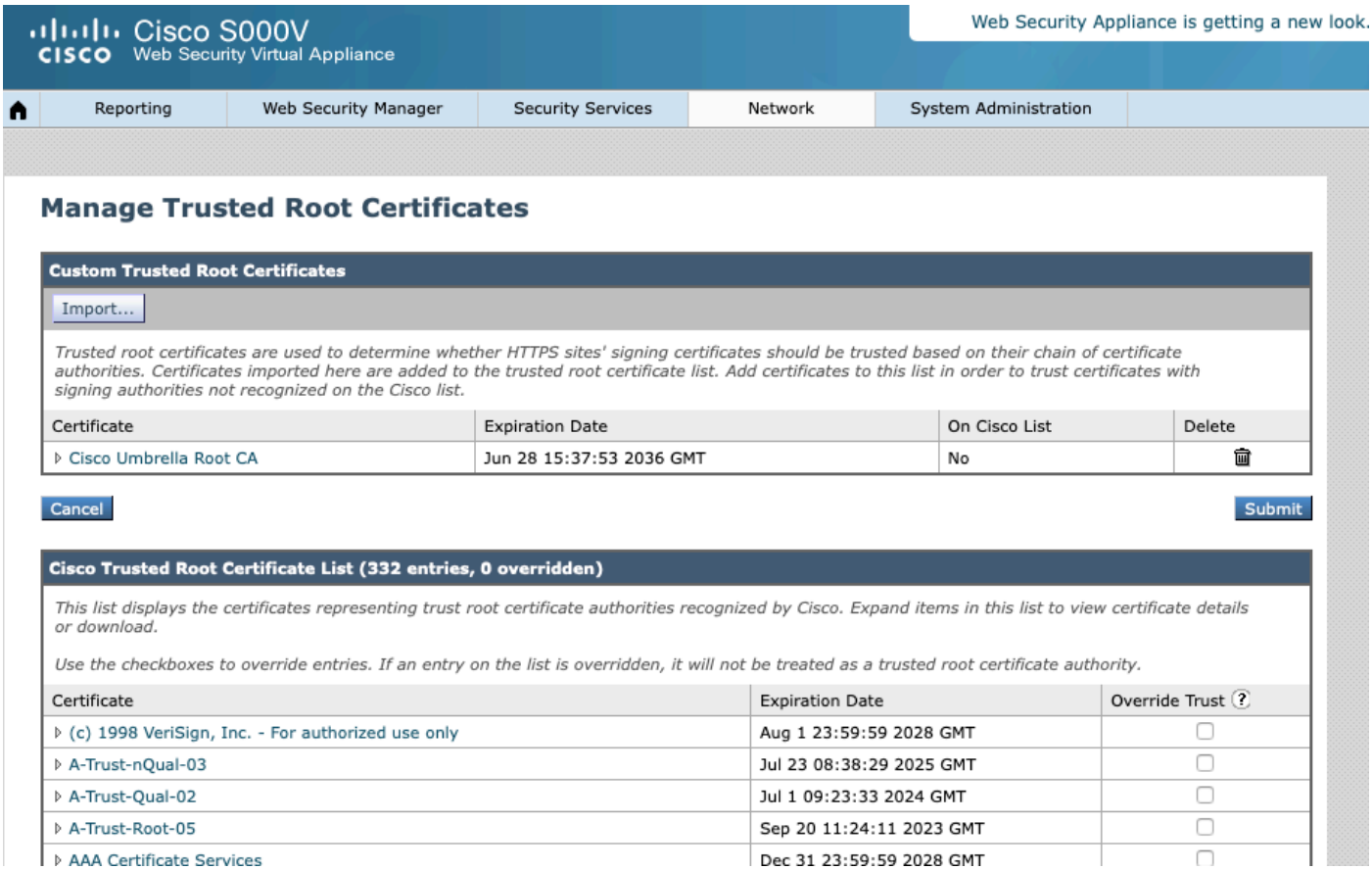
- um die interne IP-basierte Webrichtlinie in SWG zu implementieren.Stellen Sie sicher, dass Sie den Header "X-Forwarded-For" in der sicheren Webappliance über Sicherheitsdienste > Proxy-Einstellungen aktivieren.




360050700111

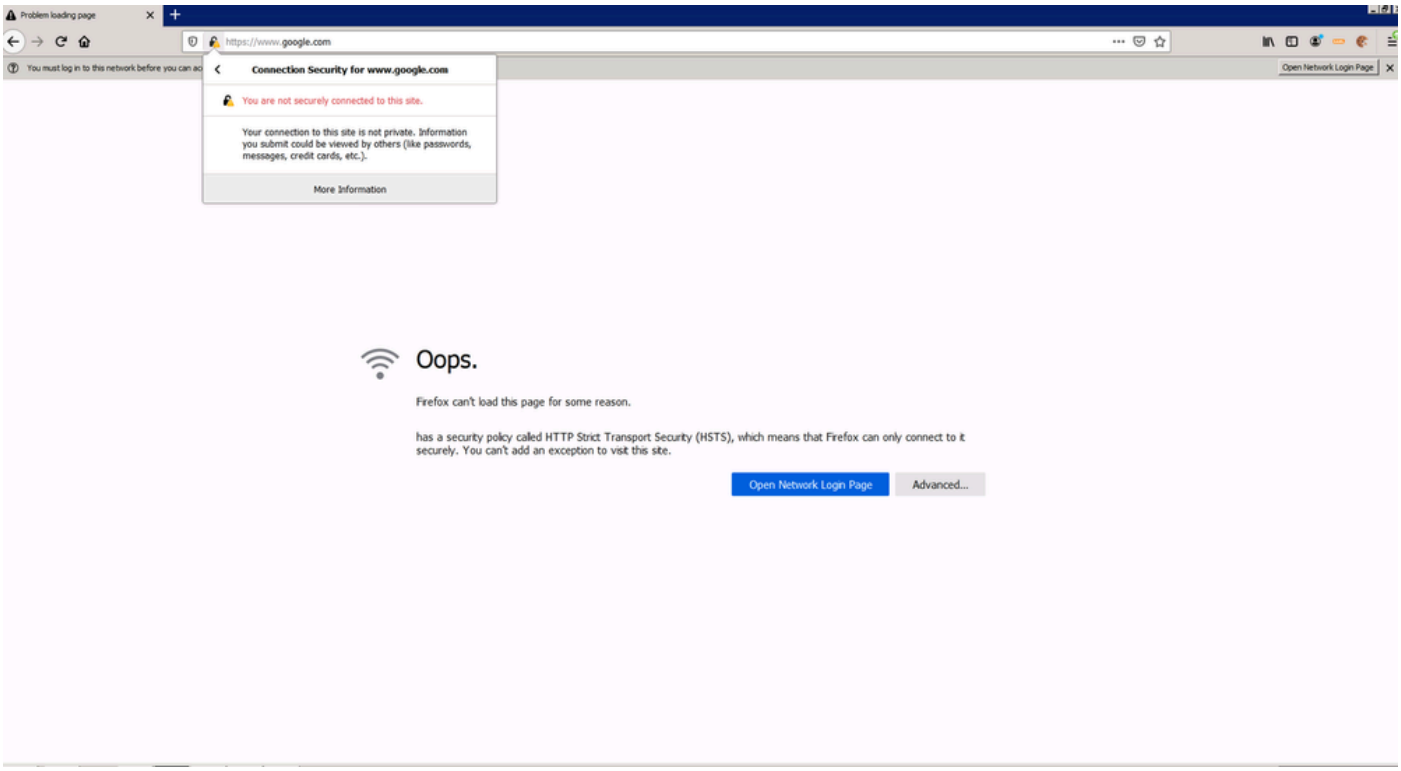
2. Vertrauenswürdiges Stammzertifikat für HTTP-Entschlüsselung.

- 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.



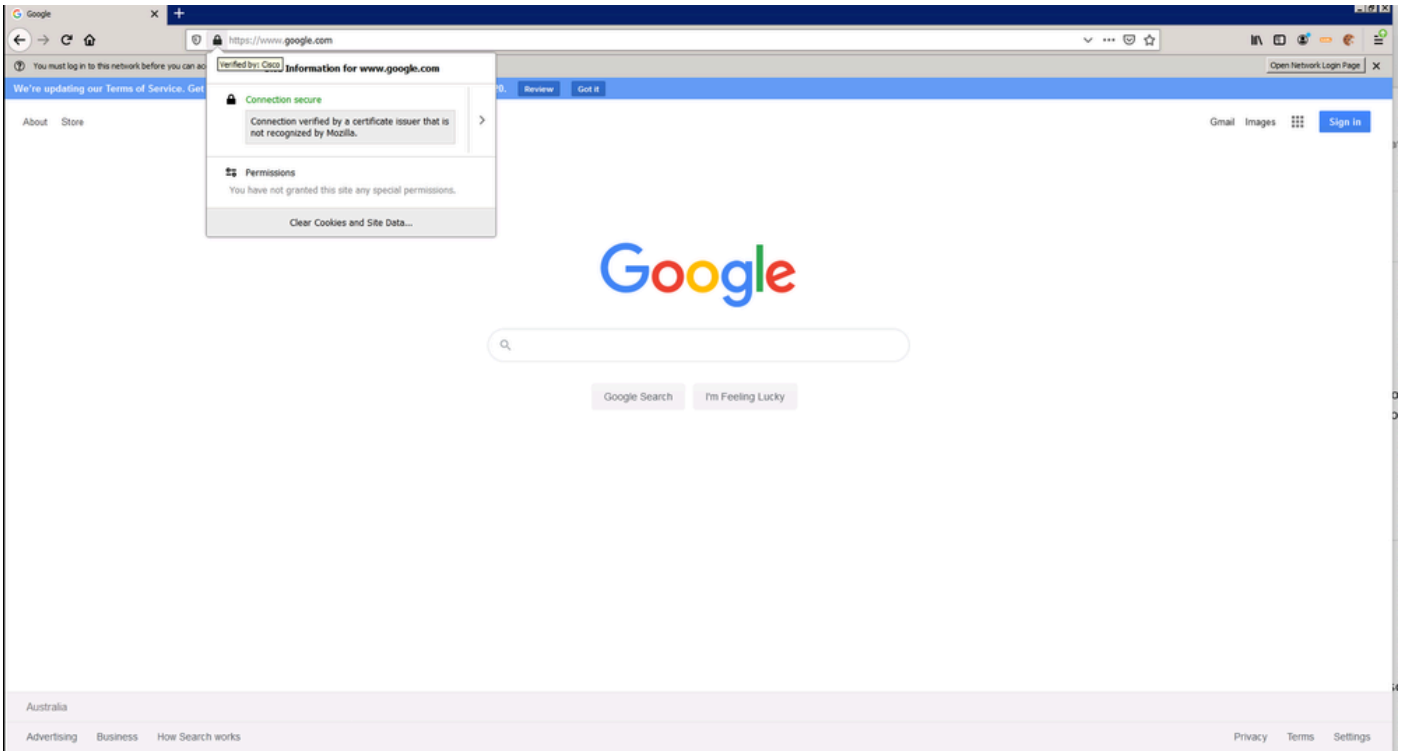

360050589612

- 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.