# Configureer de proxyketen tussen de Secure Web Appliance en de overkoepelende SWG

## Inhoud



## Inleiding

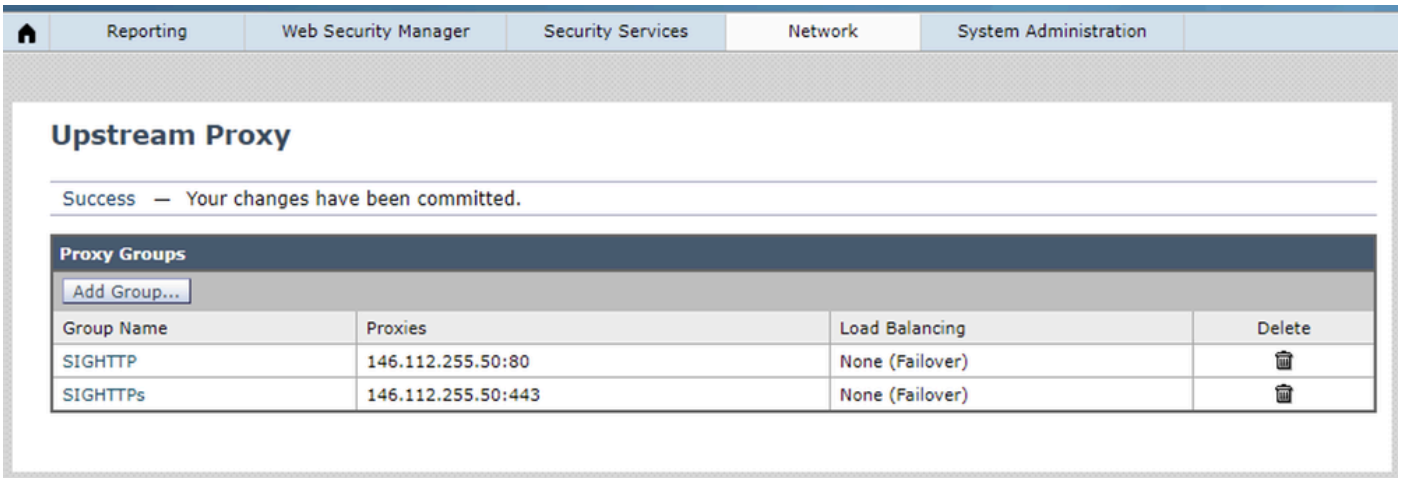
In dit document wordt beschreven hoe u de proxyketen tussen de Secure Web Appliance en de Umbrella Secure Web Gateway (SWG) configureert.

## Overzicht

De Umbrella SIG ondersteunt de proxy-keten en kan alle HTTP / HTTP-verzoeken van de downstream-proxyserver afhandelen. Dit is een uitgebreide handleiding voor de implementatie van de proxyketen tussen Cisco Secure Web Appliance (voorheen Cisco WSA) en de Umbrella Secure Web Gateway (SWG), inclusief de configuratie voor zowel Secure Web Appliance als SWG.

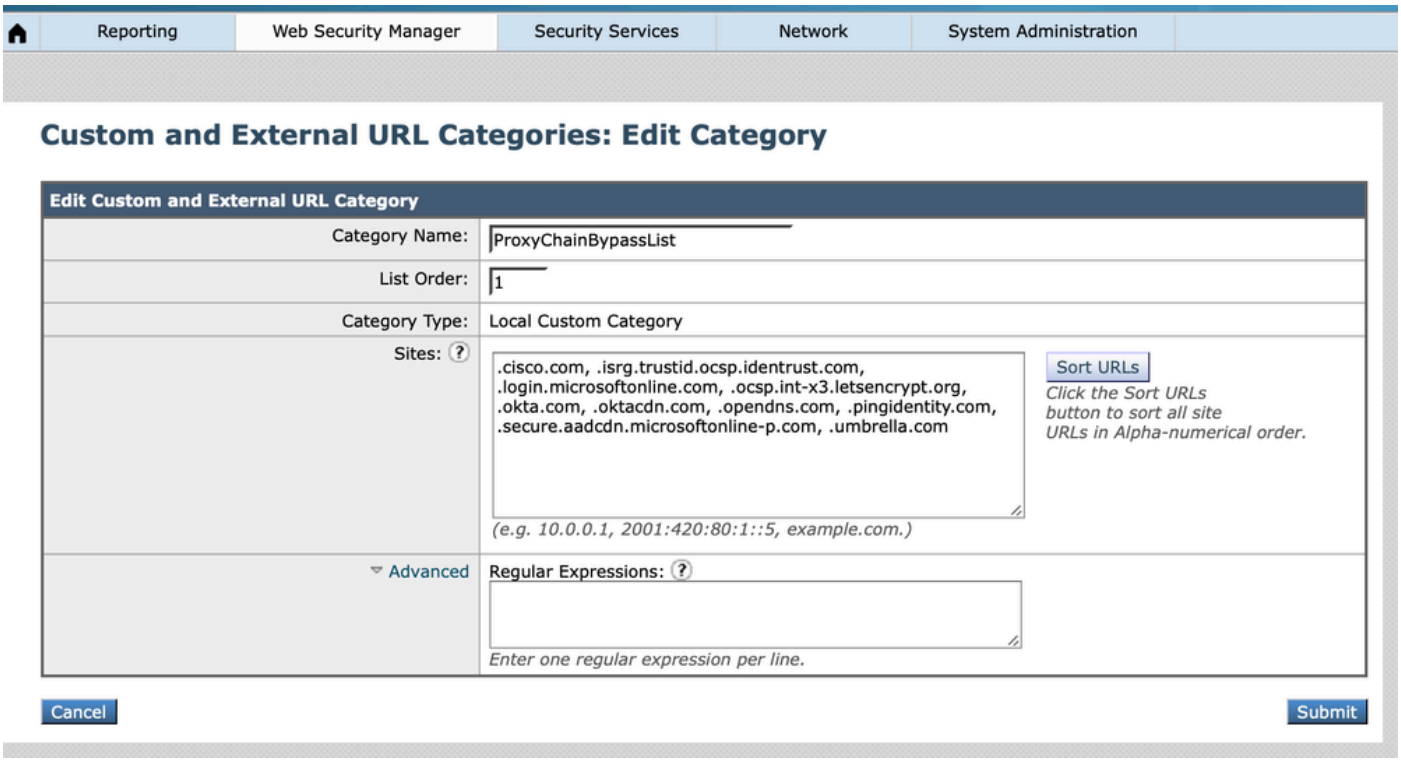
## Beleidsconfiguratie voor veilige webapparaten

1. Configureer de SWG HTTP- en HTTP-koppelingen als de Upstream Proxy via Network>Upstream Proxy.



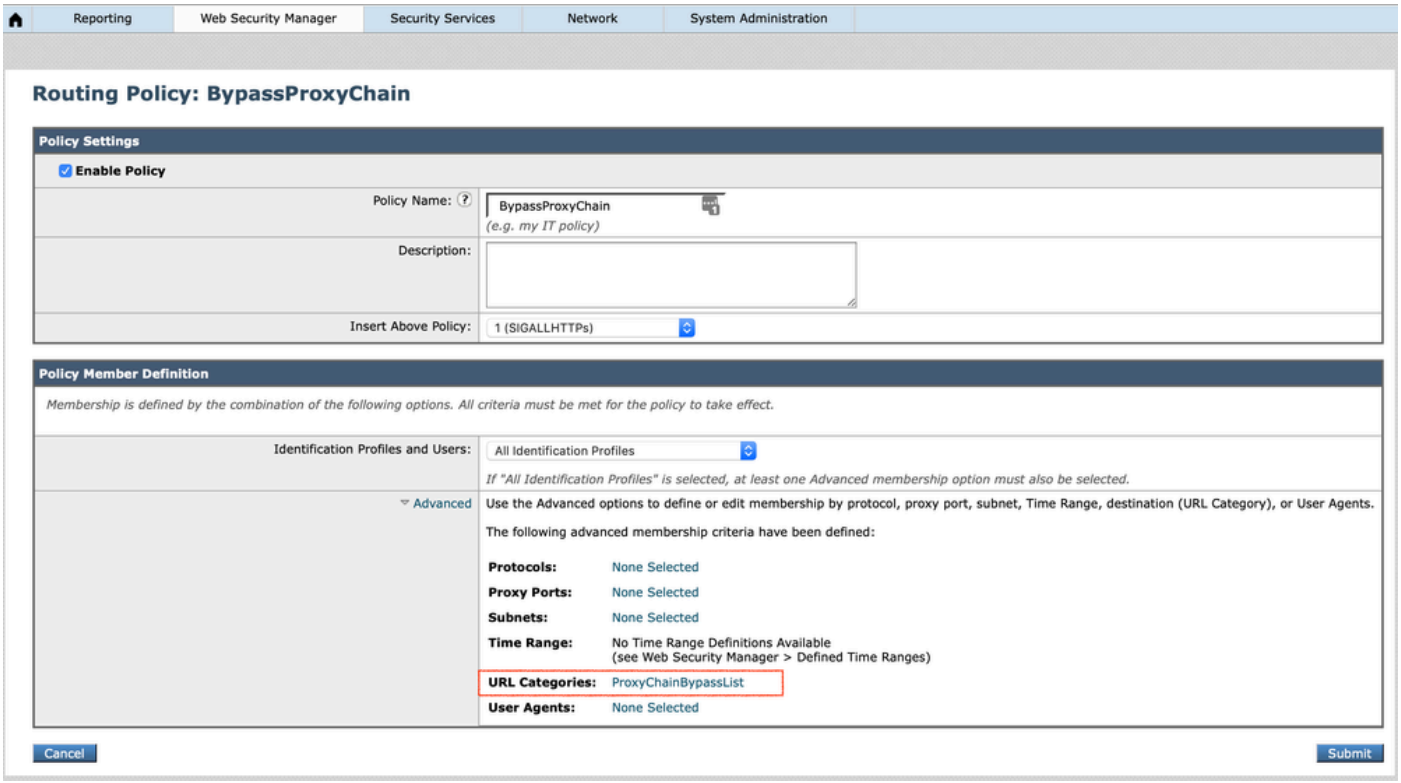
2. Maak een bypassbeleid via Web Security Manager>Routeringsbeleid om alle voorgestelde URL's rechtstreeks naar internet te routeren. Alle omzeilde URL's zijn te vinden in onze documentatie: [Cisco Umbrella SIG User Guide: Manage Proxy Chaining]

- Begin met het maken van een nieuwe "Aangepaste categorie" door te navigeren naar Web Security Manager>Aangepaste en Externe URL-categorieën zoals hier weergegeven. Het bypassbeleid is gebaseerd op de 'Aangepaste rubriek'.




360050592552

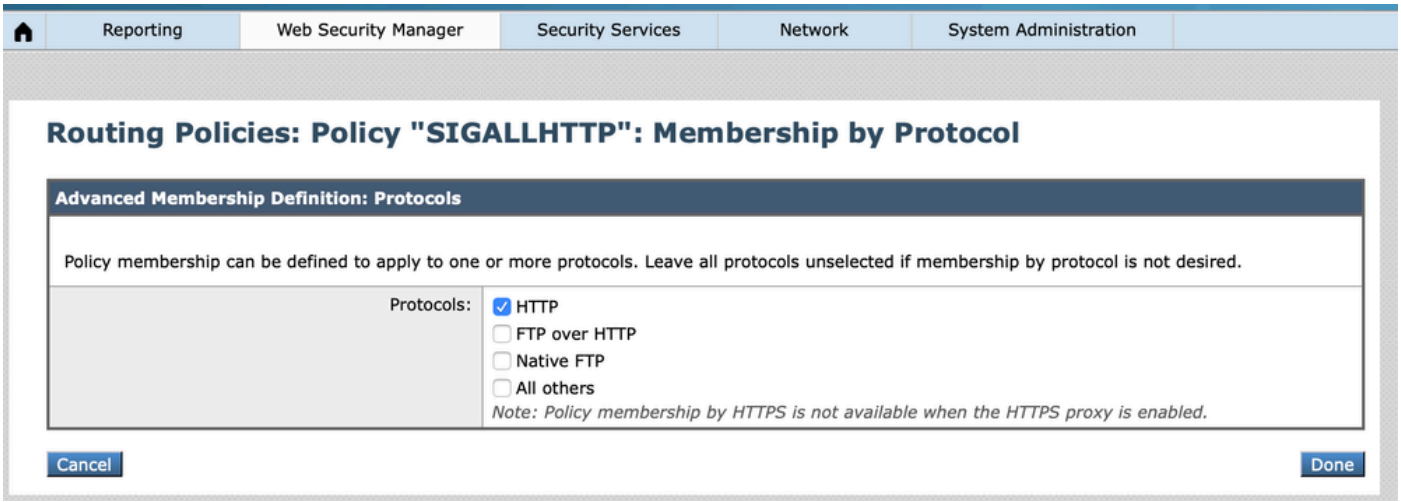
- Maak vervolgens een nieuw bypass-routeringsbeleid door naar Web Security Manager>Routeringsbeleid te navigeren. Zorg ervoor dat dit beleid het eerste beleid is, aangezien Secure Web Appliance overeenkomt met het beleid op basis van de beleidsvolgorde.



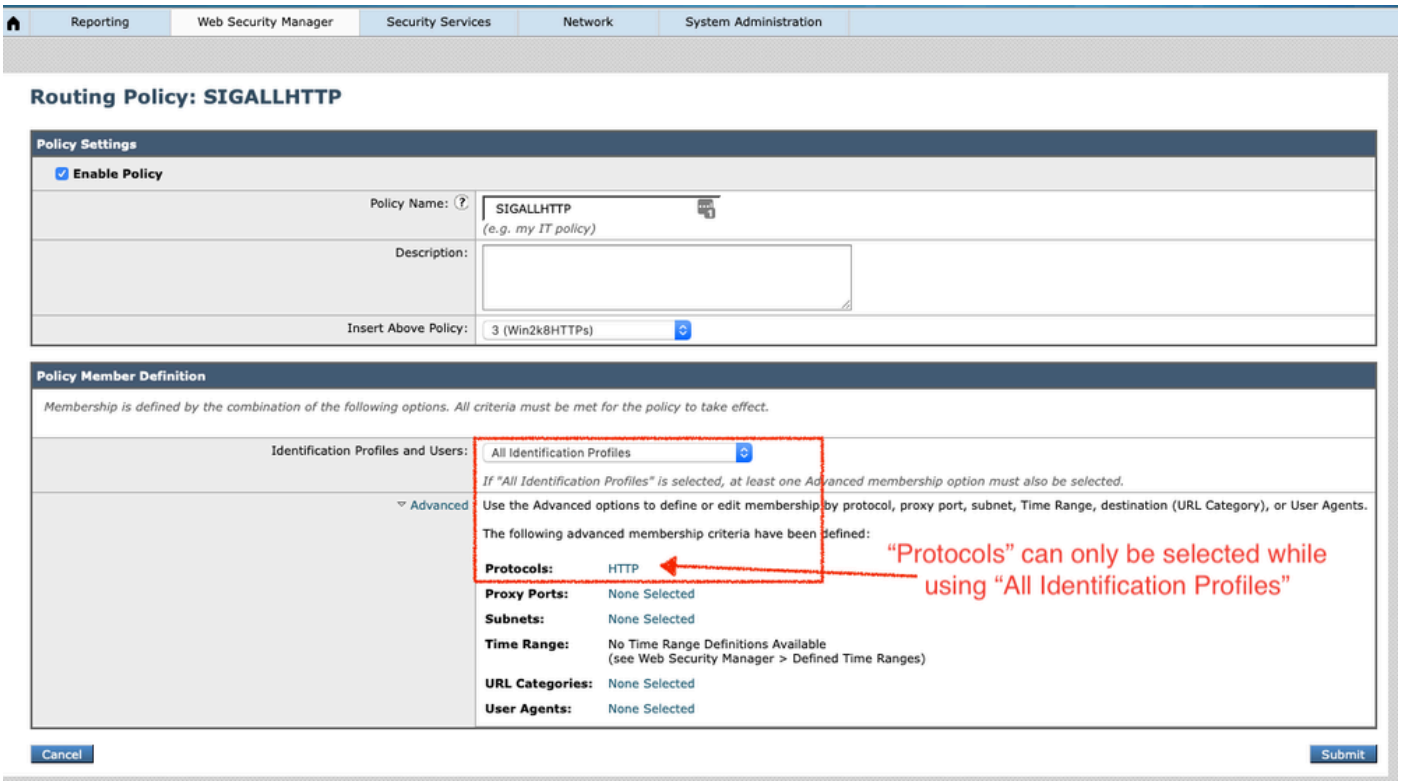

360050703131

3. Maak een nieuw routeringsbeleid voor alle HTTP-verzoeken.

- In de ledendefinitie van het routeringsbeleid voor Secure Web Appliance zijn de protocolopties HTTP, FTP over HTTP, Native FTP en "All others", terwijl "All Identification Profiles" is geselecteerd. Aangezien er geen optie is voor HTTP's, maakt u het routeringsbeleid voor HTTP-aanvragen afzonderlijk nadat u dit routeringsbeleid voor alle HTTP-aanvragen hebt geïmplementeerd.

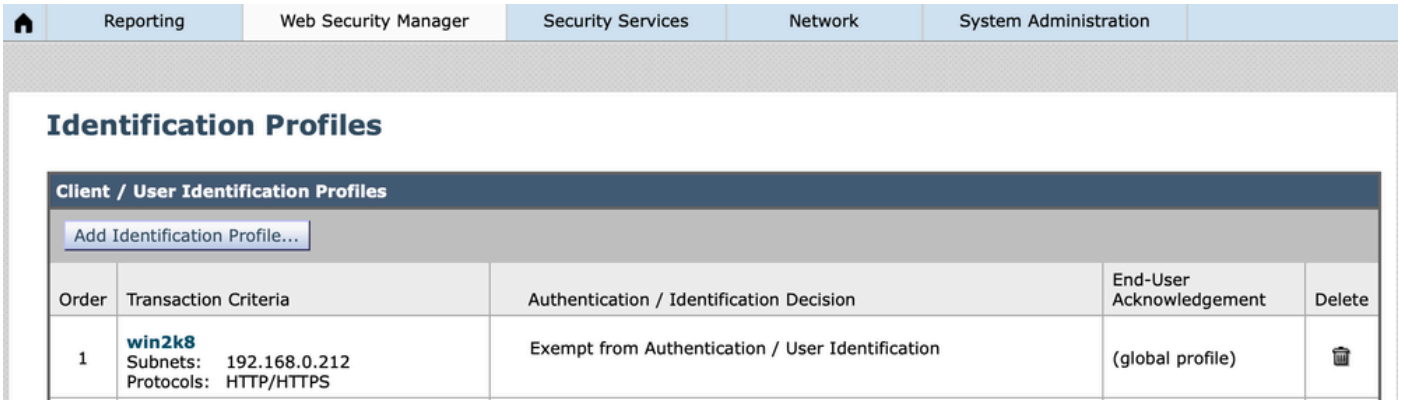



360050592772

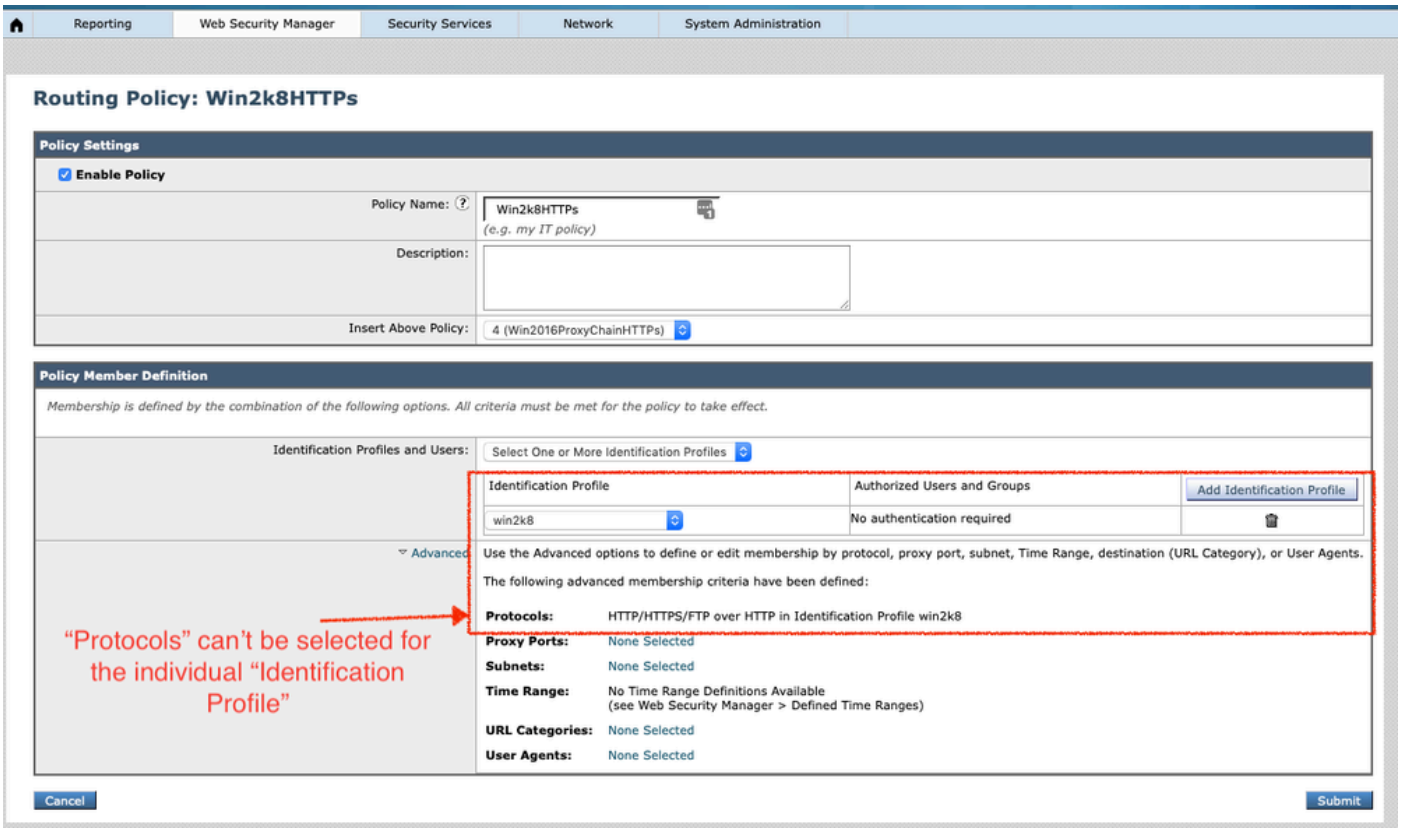



360050589572

4. Maak het routeringsbeleid voor HTTP-verzoeken op basis van het "Identificatieprofiel". Wees voorzichtig met de volgorde van het gedefinieerde "Identificatieprofiel", aangezien het Secure Web Appliance overeenkomt met de "Identificatie" voor de eerste match. In dit voorbeeld is het identificatieprofiel "win2k8" een interne op IP gebaseerde identiteit.



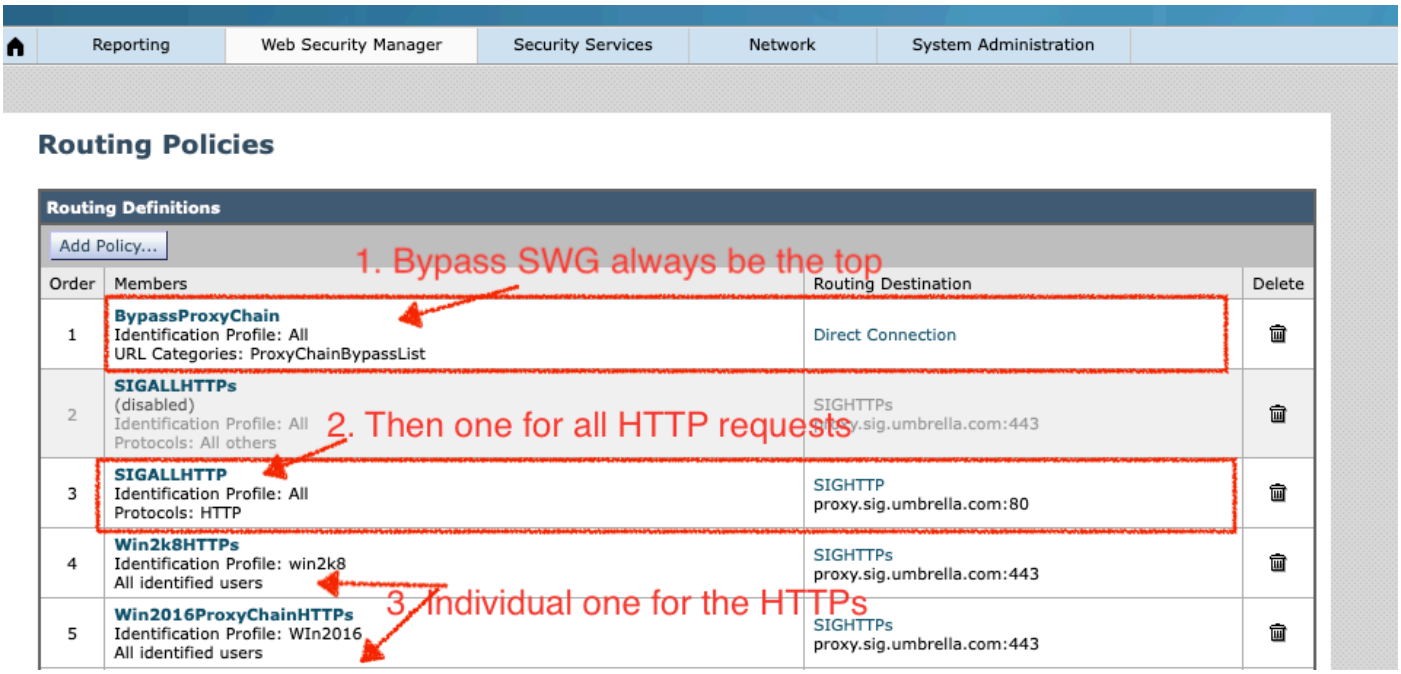

360050703971



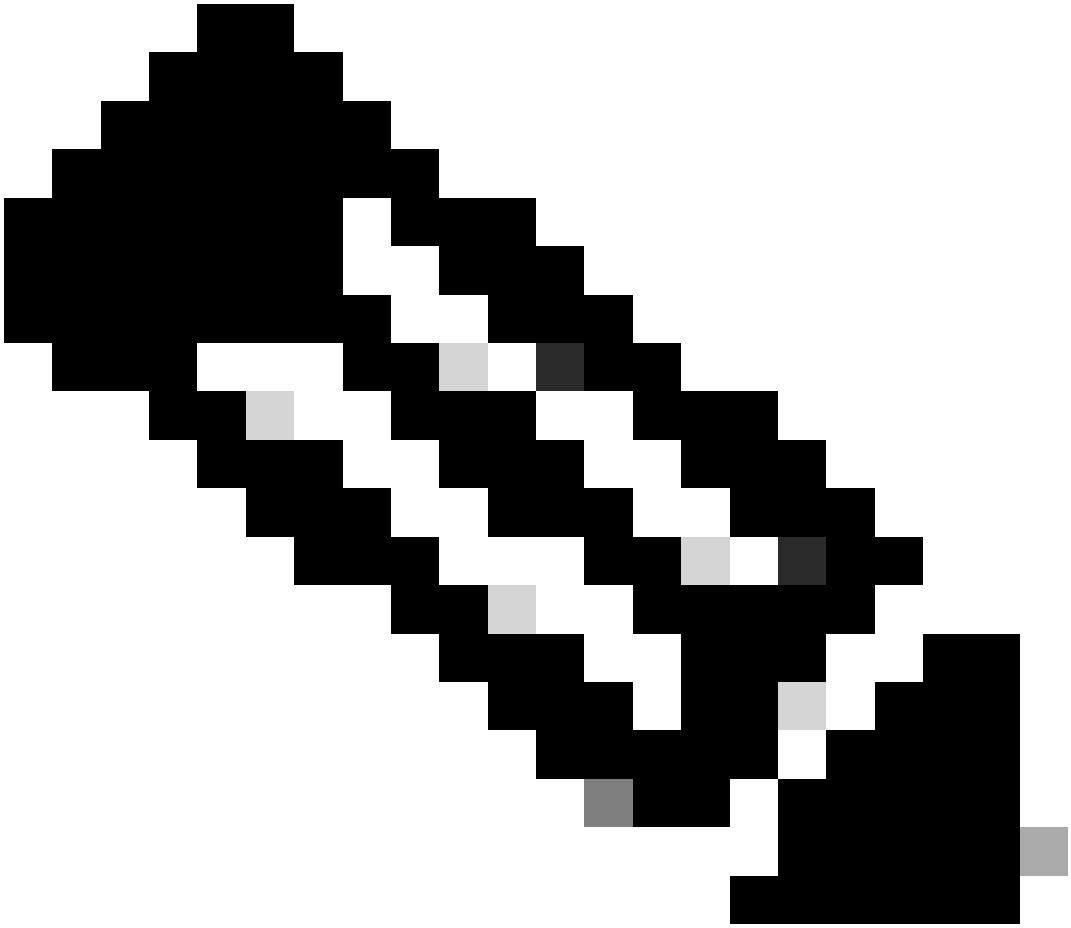

360050700091

5. Definitieve configuraties voor het routeringsbeleid voor veilige webapparaten:

- Houd er rekening mee dat Secure Web Appliance de identiteit en het toegangsbeleid evalueert met behulp van een "top down"-regelverwerkingsaanpak. Dit betekent dat de eerste match die op enig moment in de verwerking wordt gemaakt, resulteert in de actie die door Secure Web Appliance wordt ondernomen.
- Identiteiten worden eerst beoordeeld. Zodra de toegang van een client overeenkomt met een specifieke identiteit, controleert Secure Web Appliance alle toegangsbeleidsregels die zijn geconfigureerd om de identiteit te gebruiken die overeenkomt met de toegang van de client.




360050700131



Opmerking: de vermelde beleidsconfiguratie is alleen van toepassing voor de implementatie van expliciete proxy's.

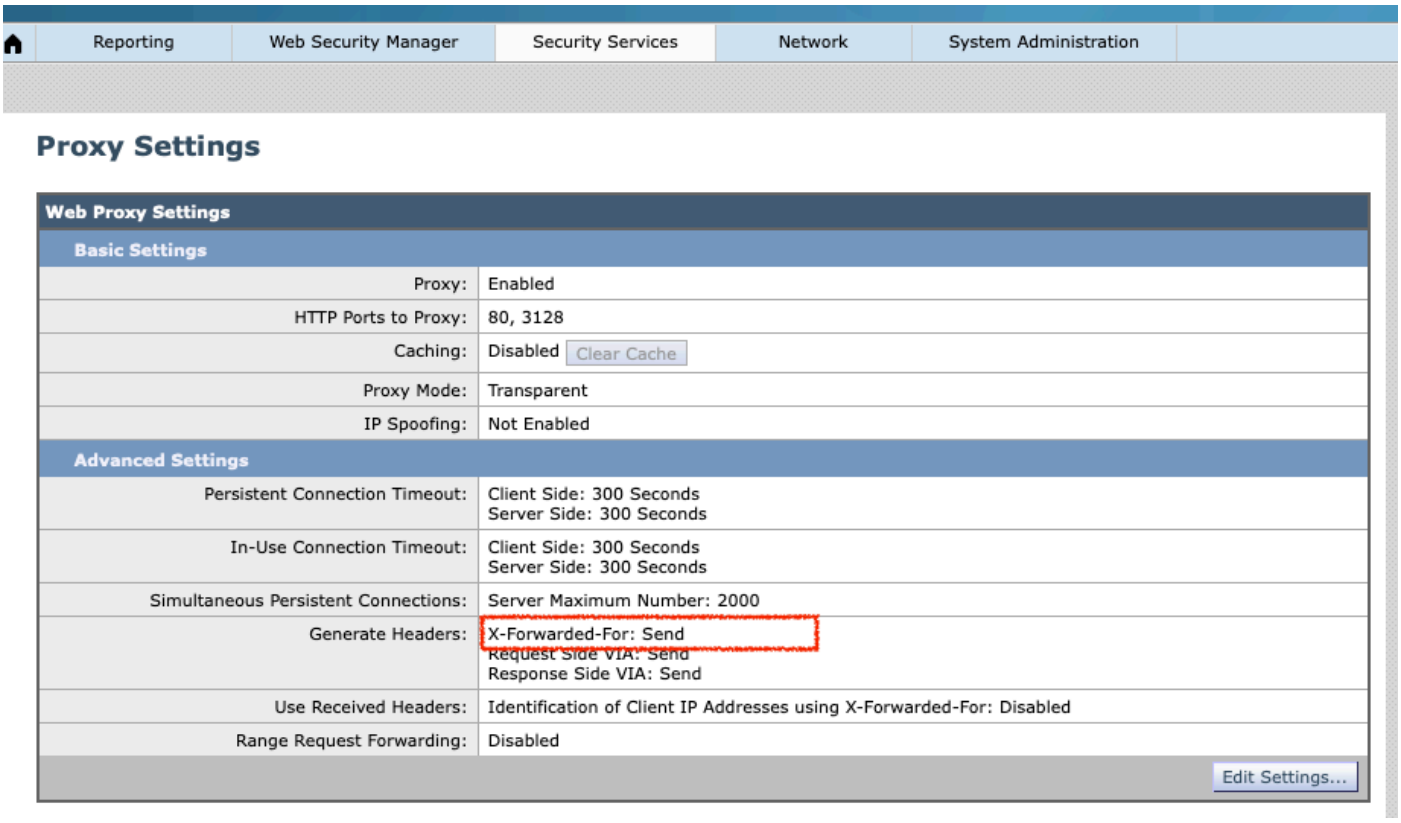
## Voor transparante proxyimplementatie

In het geval van transparante HTTPS heeft AsyncOS geen toegang tot informatie in de clientheaders. Daarom kan AsyncOS geen routeringsbeleid afdwingen als een routeringsbeleid of identificatieprofiel afhankelijk is van de informatie in de kopteksten van de client.

1. Transparant omgeleide HTTPS-transacties komen alleen overeen met het routeringsbeleid als:
    - Routing Policy Group heeft geen lidmaatschapscriteria voor beleid zoals URL-categorie, User Agent, enzovoort.
    - Identificatieprofiel heeft geen lidmaatschapscriteria voor beleid, zoals URL-categorie, User Agent, enzovoort.
2. Als in een identificatieprofiel of routeringsbeleid een aangepaste URL-categorie is gedefinieerd, komen alle transparante HTTPS-transacties overeen met de standaardgroep voor routeringsbeleid.
3. Vermijd zoveel mogelijk het configureren van het routeringsbeleid met alle identificatieprofielen, omdat dit ertoe kan leiden dat transparante HTTPS-transacties overeenkomen met de standaardgroep voor routeringsbeleid.

1. X-forwarding voor koptekst

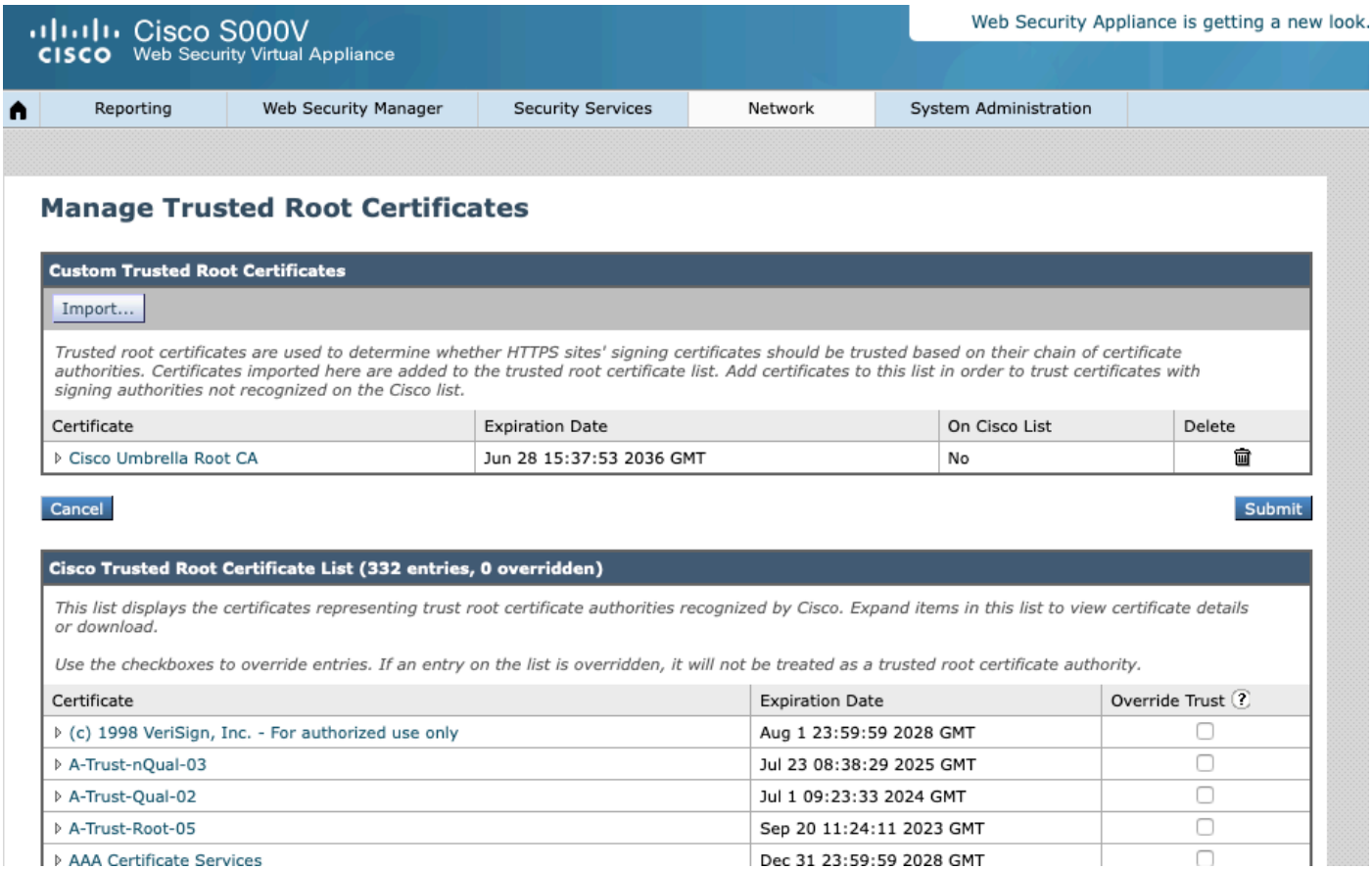
- om het interne IP-gebaseerde webbeleid in SWG te implementeren.Zorg ervoor dat u de koptekst "X-Forwarding-For" inschakelt in Secure Web Appliance via Beveiligingsservices > Proxyinstellingen.




360050700111

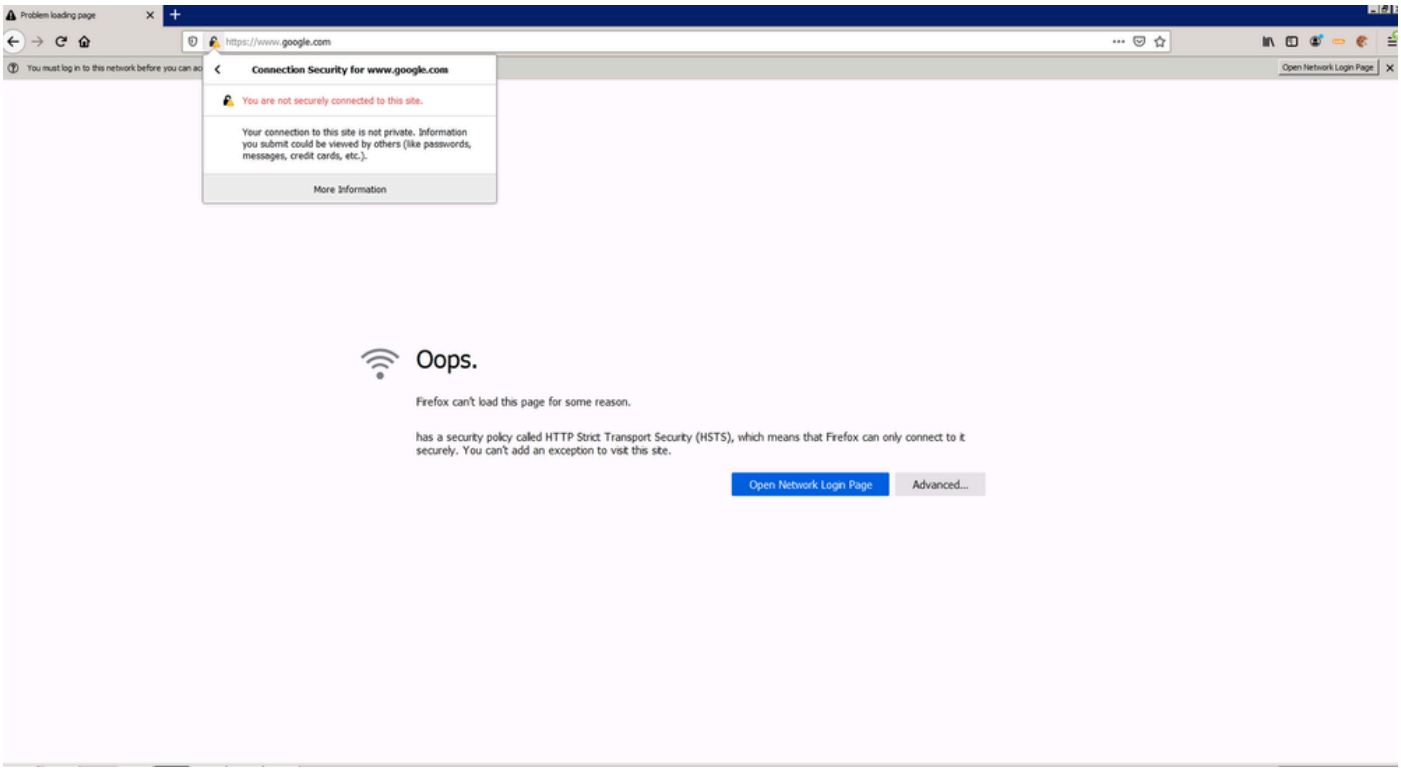
2. Vertrouwd basiscertificaat voor HTTP-decodering.

- Als de HTTP-decodering is ingeschakeld bij Webbeleid in het overkoepelende dashboard, downloadt u "Cisco Root Certificate" van het overkoepelende dashboard> Implementaties> Configuratie en importeert u het in de vertrouwde basiscertificaten van de Secure Web Appliance.



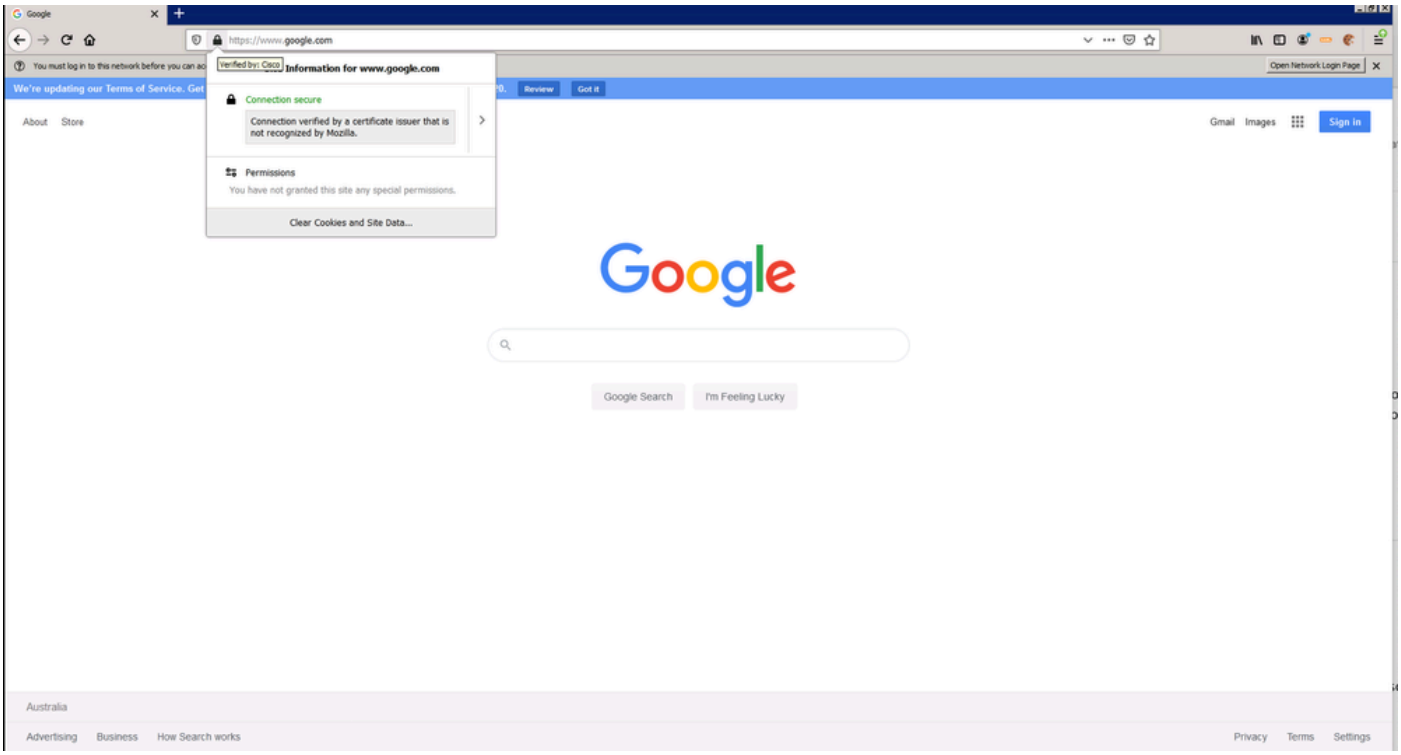

360050589612

- Als het "Cisco Root Certificate" niet is geïmporteerd in de Secure Web Appliance terwijl de HTTPs-decodering is ingeschakeld in SWG Web Policy, krijgt de eindgebruiker een fout die vergelijkbaar is met dit voorbeeld:
  - "Oeps. (browser) kan deze pagina om een of andere reden niet laden. heeft een beveiligingsbeleid genaamd HTTP Strict Transport Security (HSTS), wat betekent dat (browser) er alleen veilig verbinding mee kan maken. Je kunt geen uitzondering toevoegen om deze site te bezoeken."
  - "Je bent niet veilig verbonden met deze site."




360050700171

- Dit is een voorbeeld van de HTTP's die zijn gedecodeerd door Umbrella SWG. Het certificaat wordt geverifieerd door het "Cisco Root Certificate" met de naam "Cisco".




360050700191

# Configuratie van SWG-webbeleid in overkoepelend dashboard

SWG-webbeleid op basis van interne IP:

- Zorg ervoor dat u de "X-Forwarding-For" -header inschakelt in de Secure Web Appliance, omdat SWG daarop vertrouwt om het interne IP-adres te identificeren.
- Registreer de IP-uitgang van de Secure Web Appliance in Implementatie > Netwerken.
- Maak een intern IP-adres van het clientsysteem in Implementatie > Configuratie > Interne netwerken. Selecteer de geregistreerde Secure Web Appliance-uitgang IP (stap 1) nadat u "Netwerken weergeven" hebt aangevinkt/geselecteerd.
- Maak een nieuw webbeleid op basis van het interne IP-adres dat in stap 2 is gemaakt.
- Zorg ervoor dat de optie "SAML inschakelen" is uitgeschakeld in het webbeleid.

SWG-webbeleid op basis van AD-gebruiker/groep:

- Zorg ervoor dat alle AD-gebruikers en -groepen zijn voorzien van het Umbrella-dashboard.
- Maak een nieuw webbeleid op basis van de geregistreerde IP-uitgang van de Secure Web Appliance met de optie "SAML inschakelen" ingeschakeld.
- Maak een ander nieuw webbeleid op basis van de AD-gebruiker/groep met de optie "SAML inschakelen" uitgeschakeld. U moet dit webbeleid ook vóór het webbeleid plaatsen dat in stap 2 is gemaakt.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.