Configure the Proxy Chain Between the Secure Web Appliance and the Umbrella SWG

Contents

Introduction

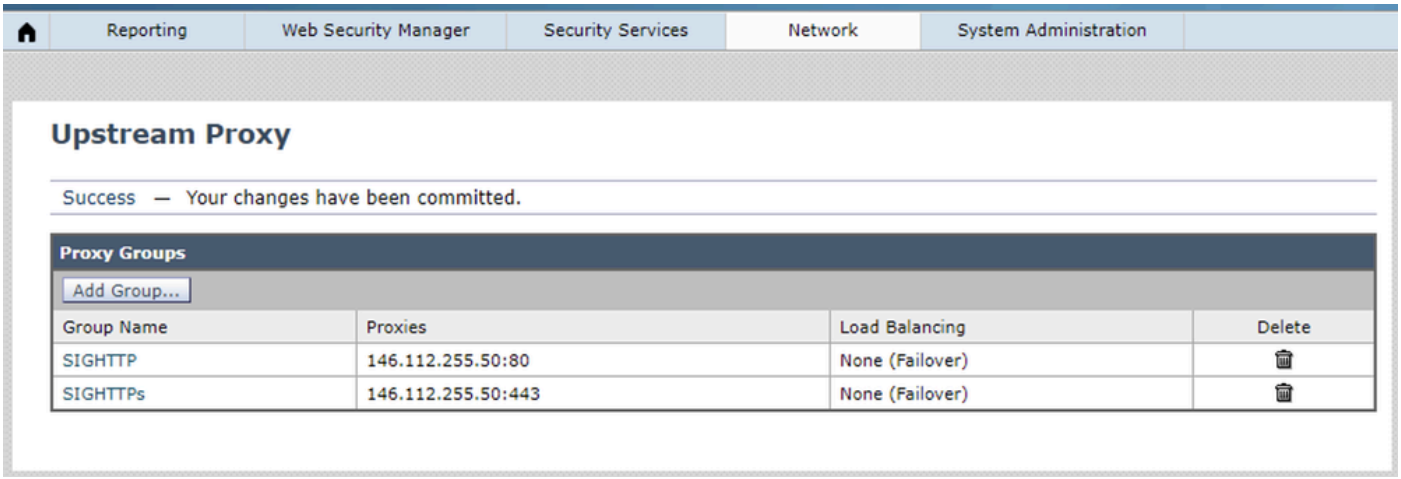
This document describes how to configure the proxy chain between the Secure Web Appliance and the Umbrella Secure Web Gateway (SWG).

Overview

The Umbrella SIG supports the proxy chain and can handle all the HTTP/HTTPs requests from the downstream proxy server. This is a comprehensive guide to implement the proxy chain between Cisco Secure Web Appliance (formerly Cisco WSA) and the Umbrella Secure Web Gateway (SWG), including the configuration for both Secure Web Appliance and SWG.

Secure Web Appliance Policy Configuration

1. Configure the SWG HTTP and HTTPs links as the Upstream Proxy via **Network>Upstream Proxy**.

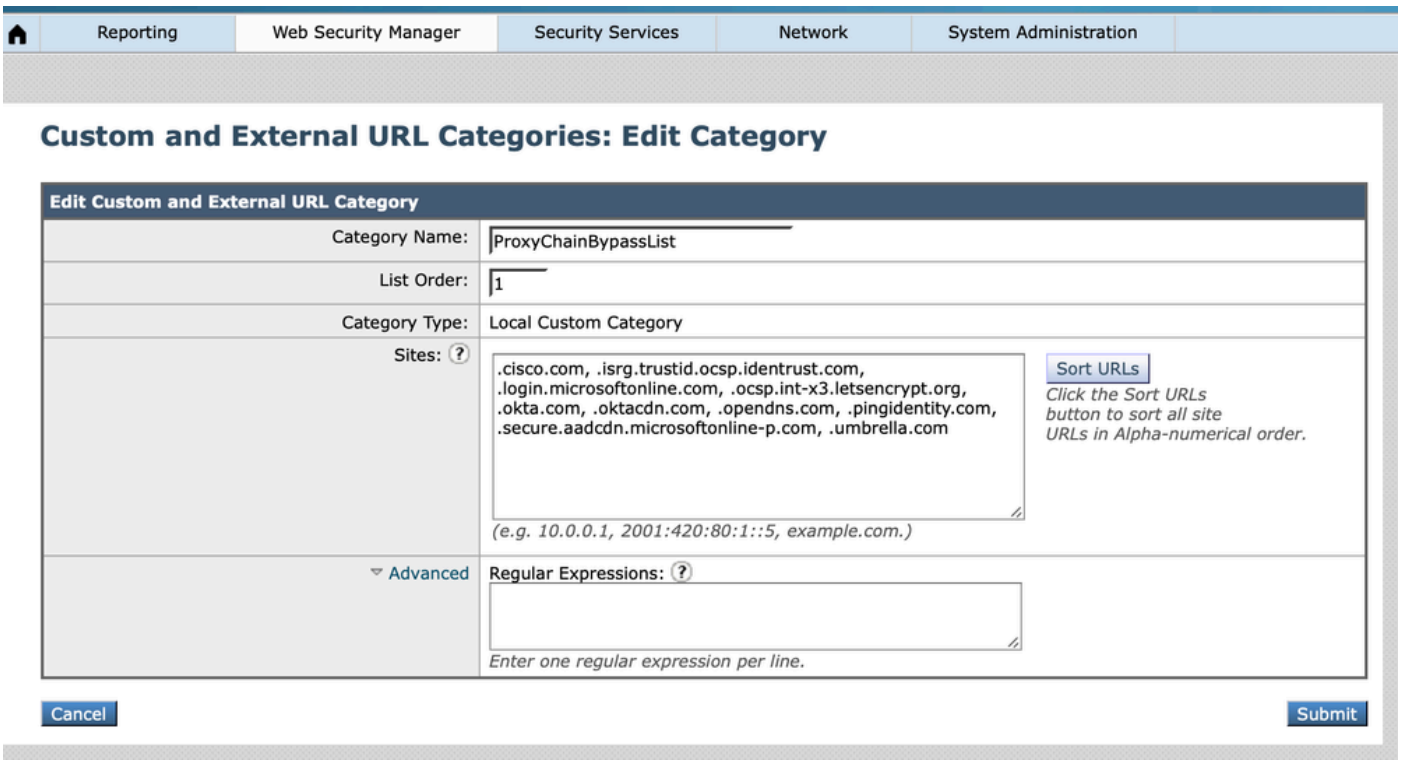


360079596451

2. Create a bypass policy via **Web Security Manager>Routing Policy** to route all suggested URLs to the internet directly. All bypassed URLs can be found in our documentation: Cisco Umbrella SIG User Guide: Manage Proxy Chaining

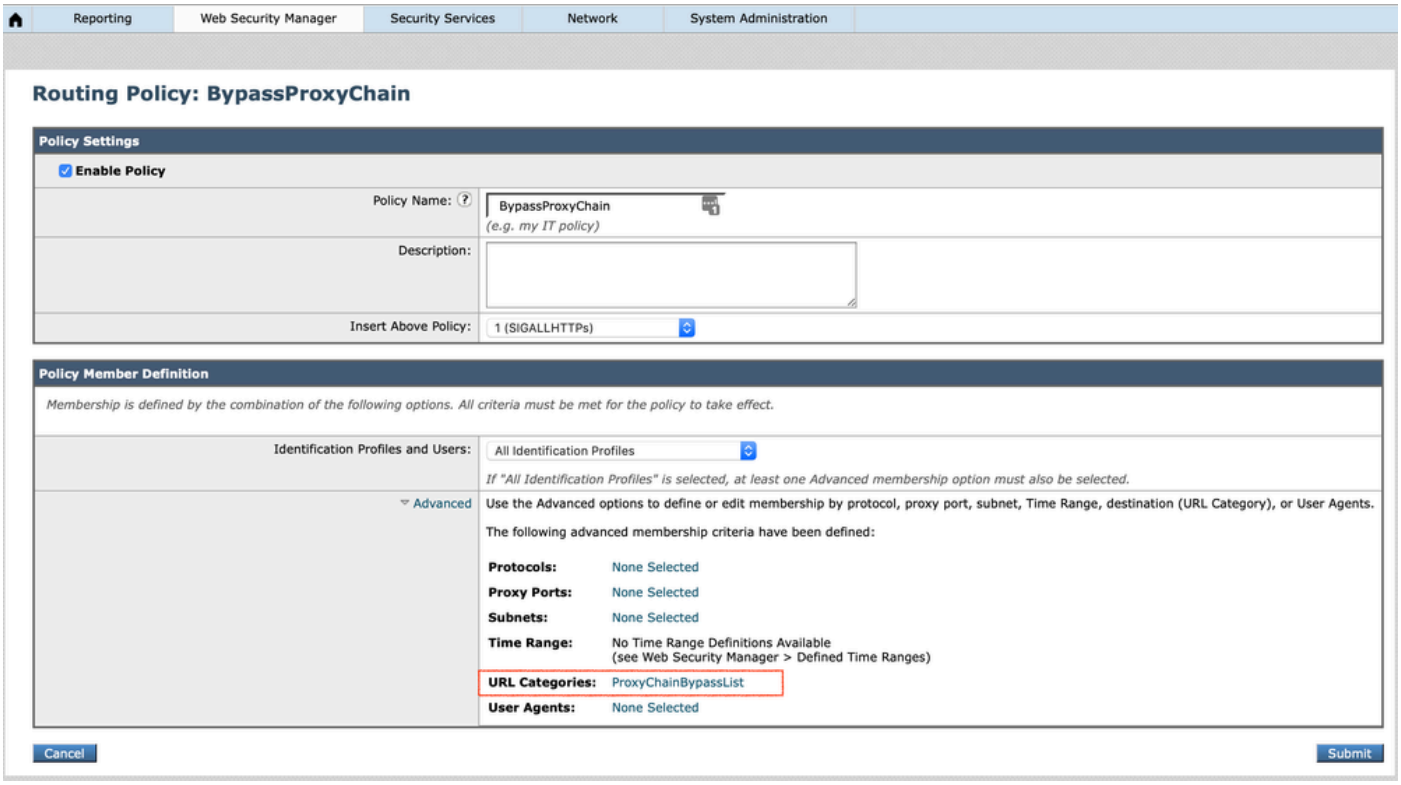
- Start by creating a new "Custom Category" by navigating to **Web Security Manager>Custom and**

External URL Categories as shown here. The bypass policy is based on the "Custom Category."



360050592552

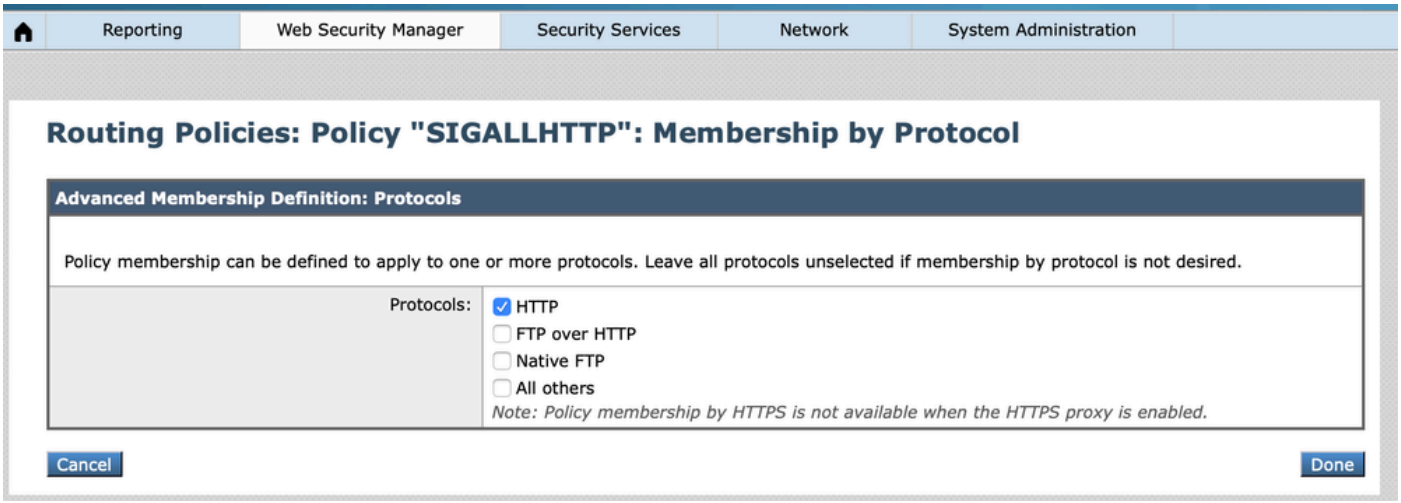
- Next, create a new bypass routing policy by navigating to **Web Security Manager>Routing Policy**. Please make sure this policy is the first one as Secure Web Appliance matches the policy based on the policy order.



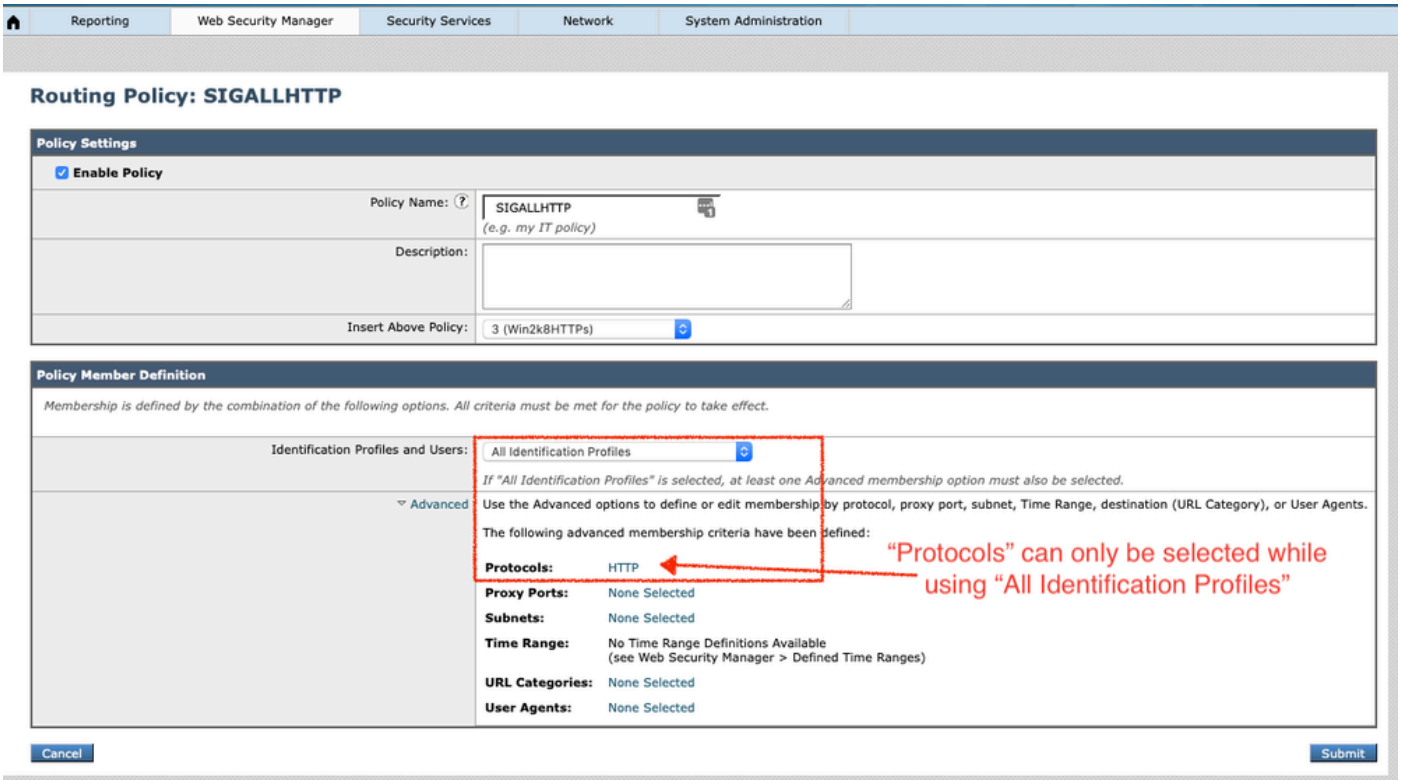
360050703131

3. Create a new routing policy for all HTTP requests.

- In the Secure Web Appliance routing policy member definition, the protocol options are HTTP, FTP over HTTP, Native FTP, and "All others" while "All Identification Profiles" are selected. Since there is no option for HTTPs, create the routing policy for HTTPs request individually after implementing this routing policy for all HTTP requests.

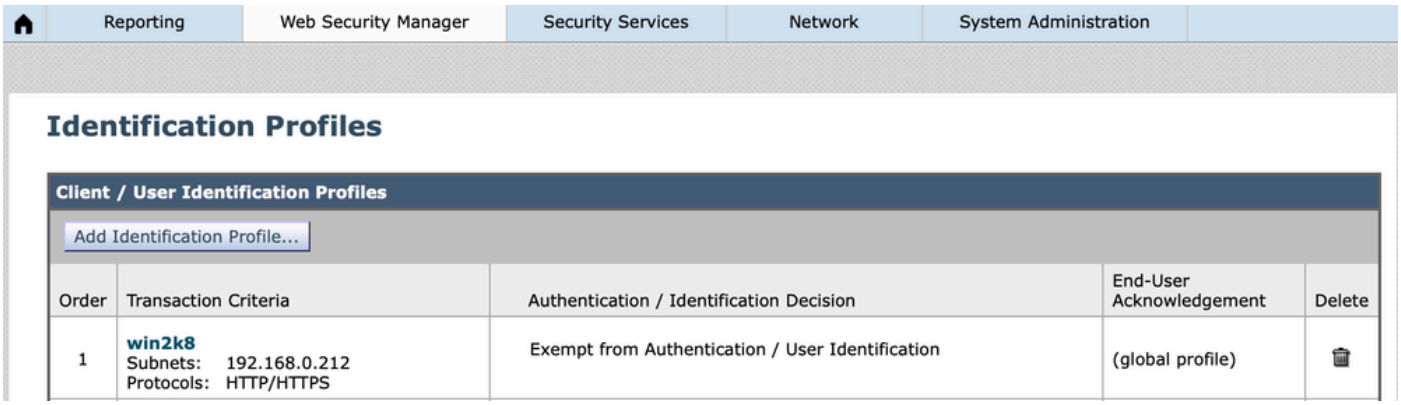


360050592772

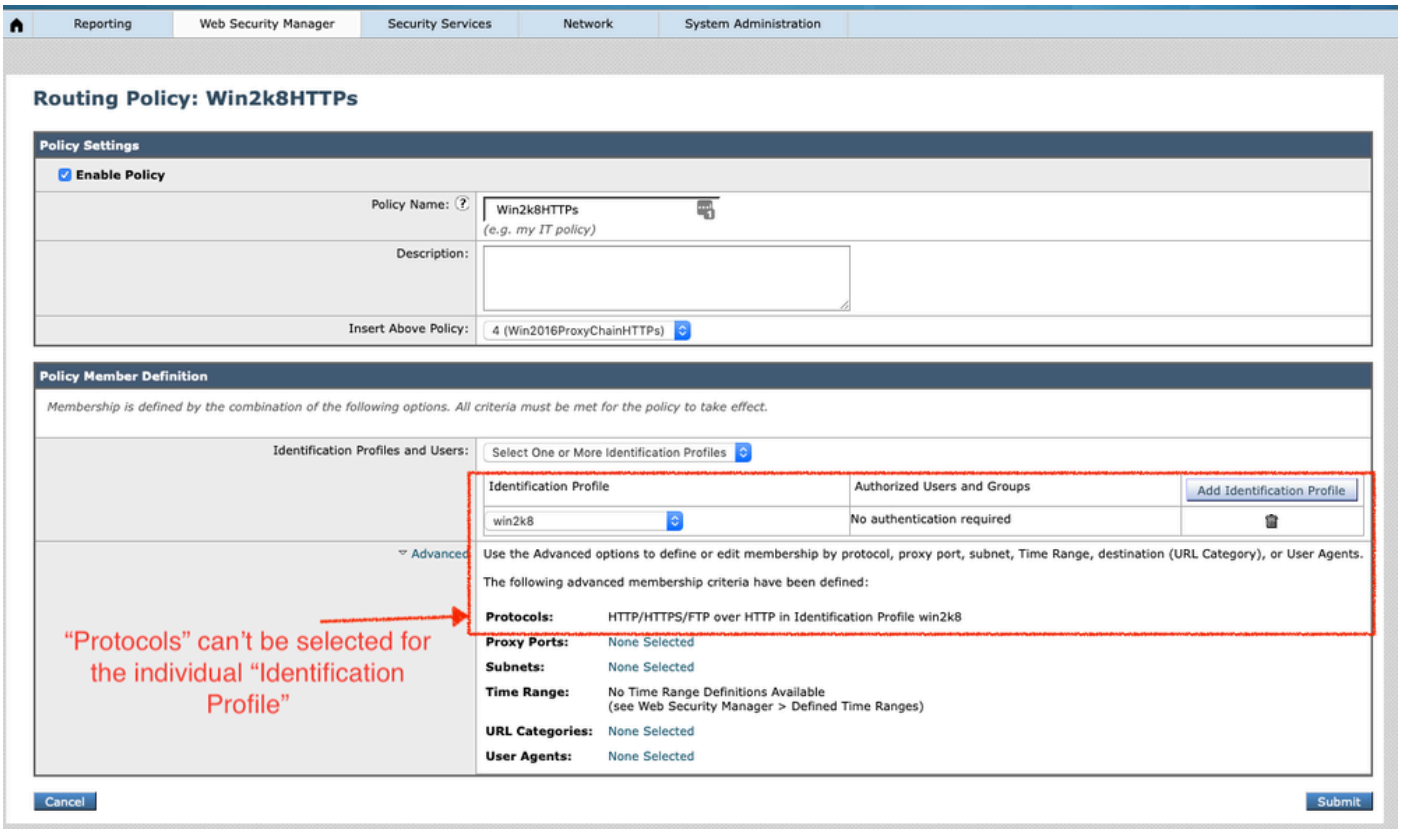


360050589572

4. Create the routing policy for HTTPs requests based on the "Identification Profile." Please be careful with the sequence of the defined "Identification Profile," since the Secure Web Appliance matches the "Identification" for the first match. In this example, the Identification Profile "win2k8" is an internal IP based identity.



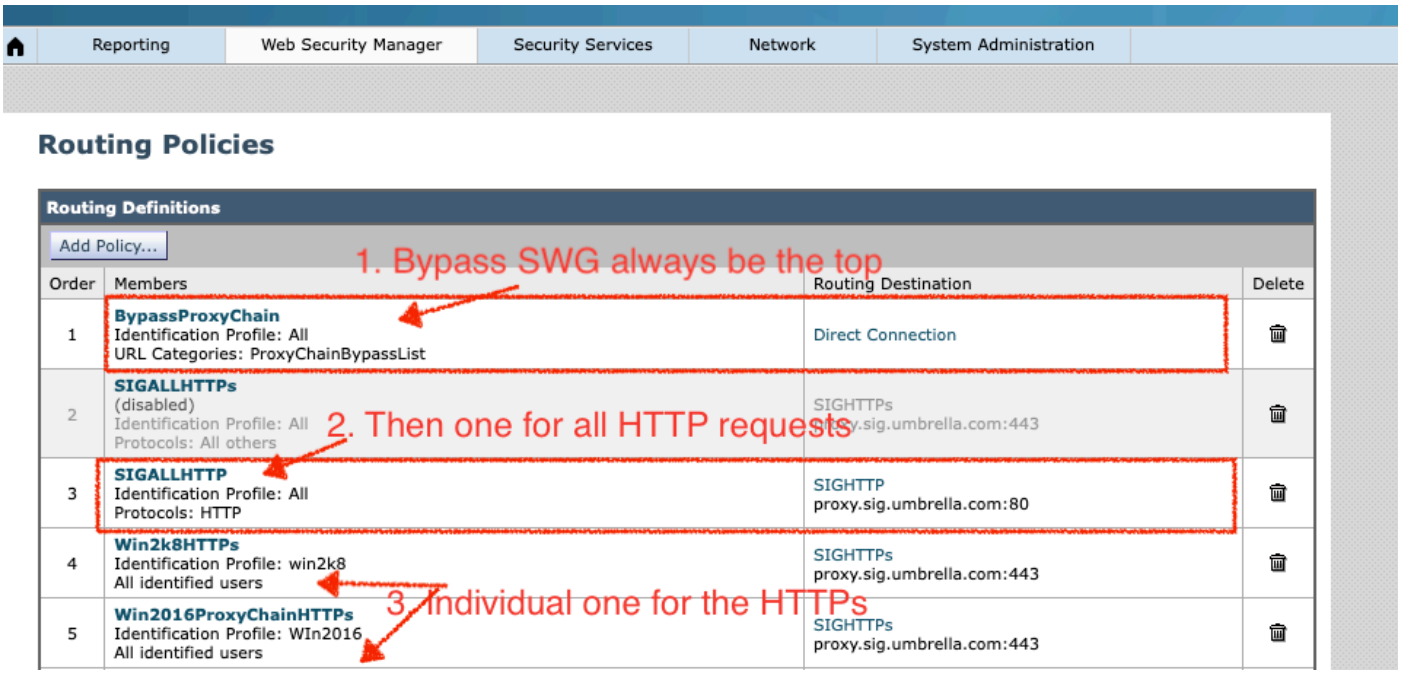
360050703971



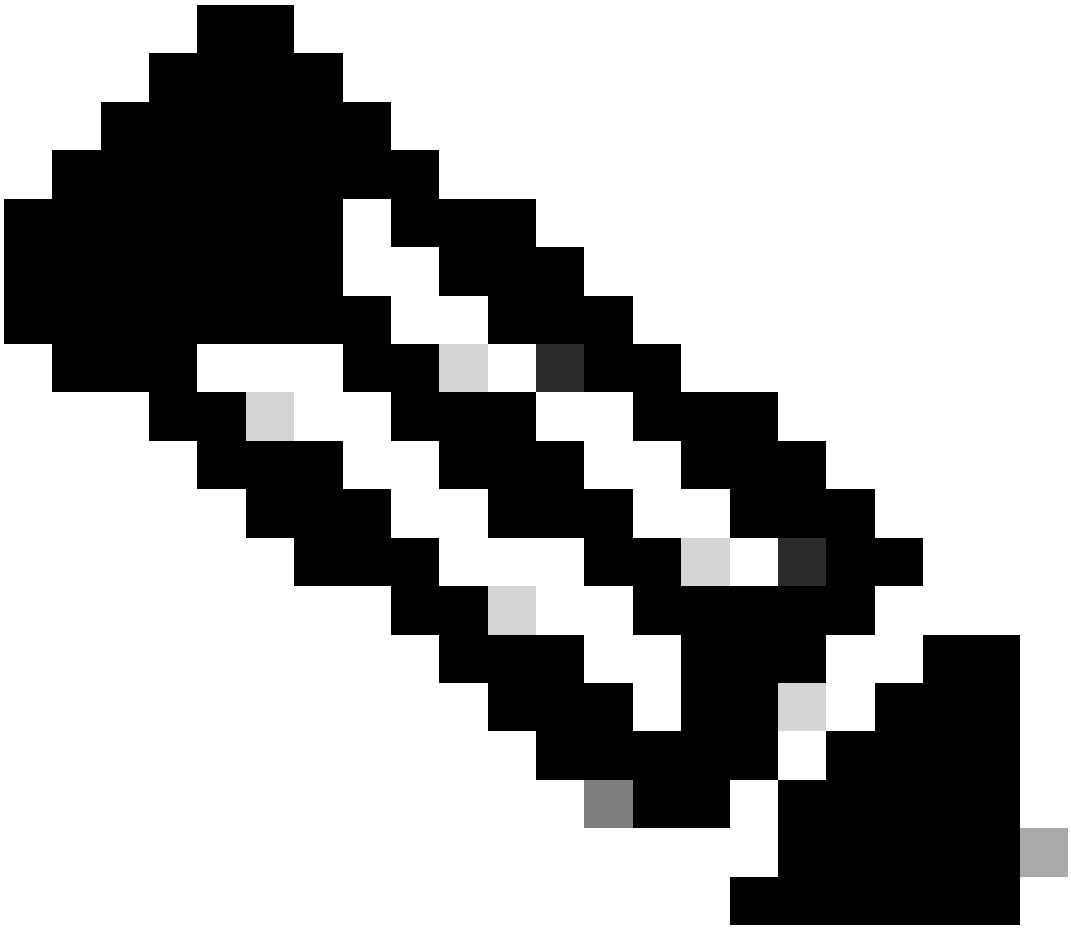
360050700091

5. Final configurations for the Secure Web Appliance Routing Policies:

- Be mindful that Secure Web Appliance evaluates the identities and access policies using a "top down" rule processing approach. This means that the first match made at any point in the processing results in the action taken by Secure Web Appliance.
- Additionally, identities are evaluated first. Once a client's access matches a specific identity, Secure Web Appliance checks all access policies that are configured to use the identity that matches the client's access.



360050700131



Note: The mentioned Policy Configuration is applicable for Explicit Proxy Deployment only.

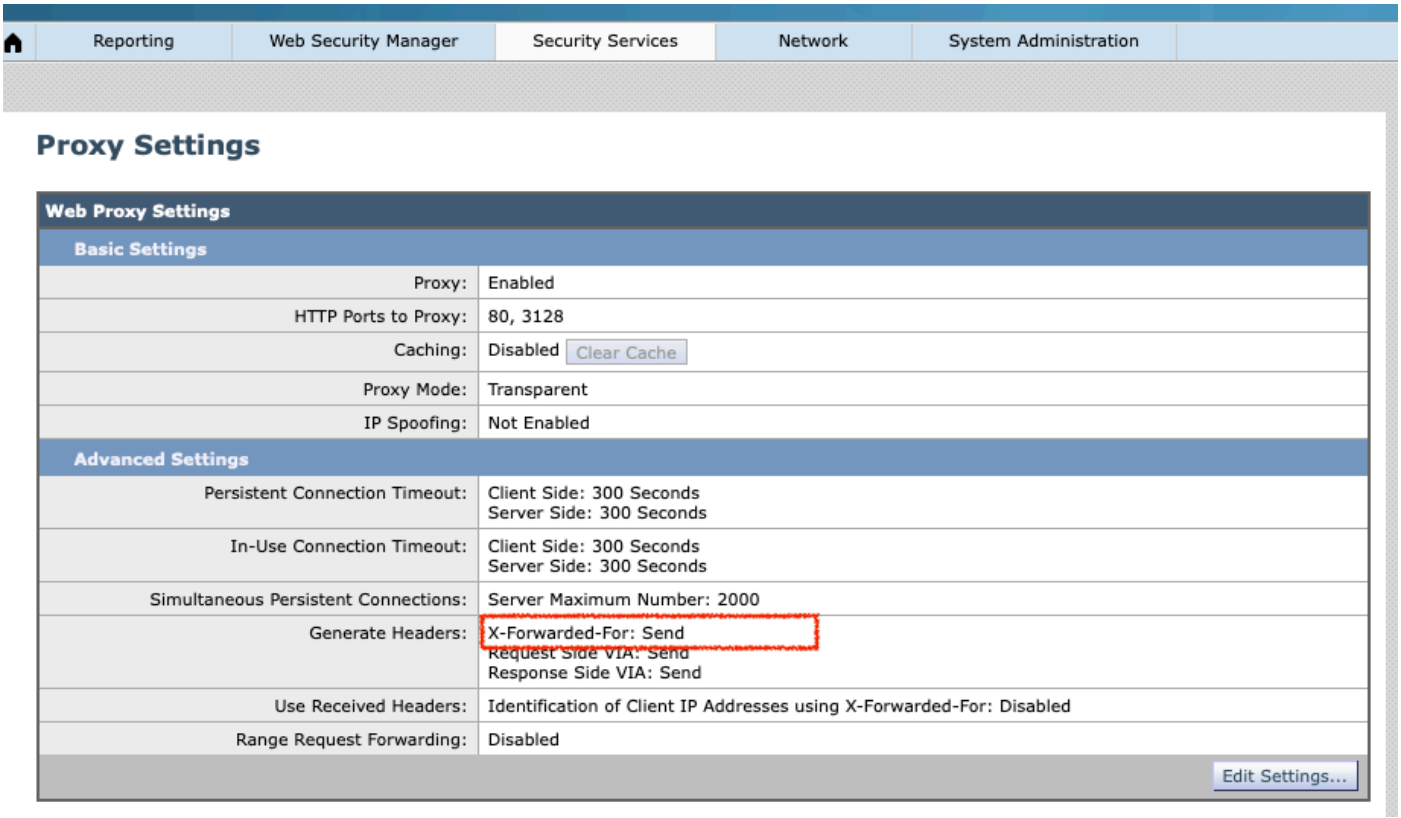
For Transparent Proxy Deployment

In the case of transparent HTTPS, AsyncOS does not have access to information in the client headers. Therefore, AsyncOS cannot enforce routing policies if any routing policy or identification profile relies on the information in the client headers.

1. Transparently redirected HTTPS transactions only matches Routing Policies if:
    - Routing Policy Group does not have a policy membership criteria like URL category, User Agent, and so on defined.
    - Identification Profile does not have a policy membership criteria like URL category, User Agent, and so on defined.
2. If any Identification Profile or Routing Policy has a custom URL category defined, then all the transparent HTTPS transactions matches the Default Routing Policy Group.
3. As much as possible, avoid configuring Routing Policy with All Identification Profiles as this might cause transparent HTTPS transactions to match the Default Routing Policy Group.

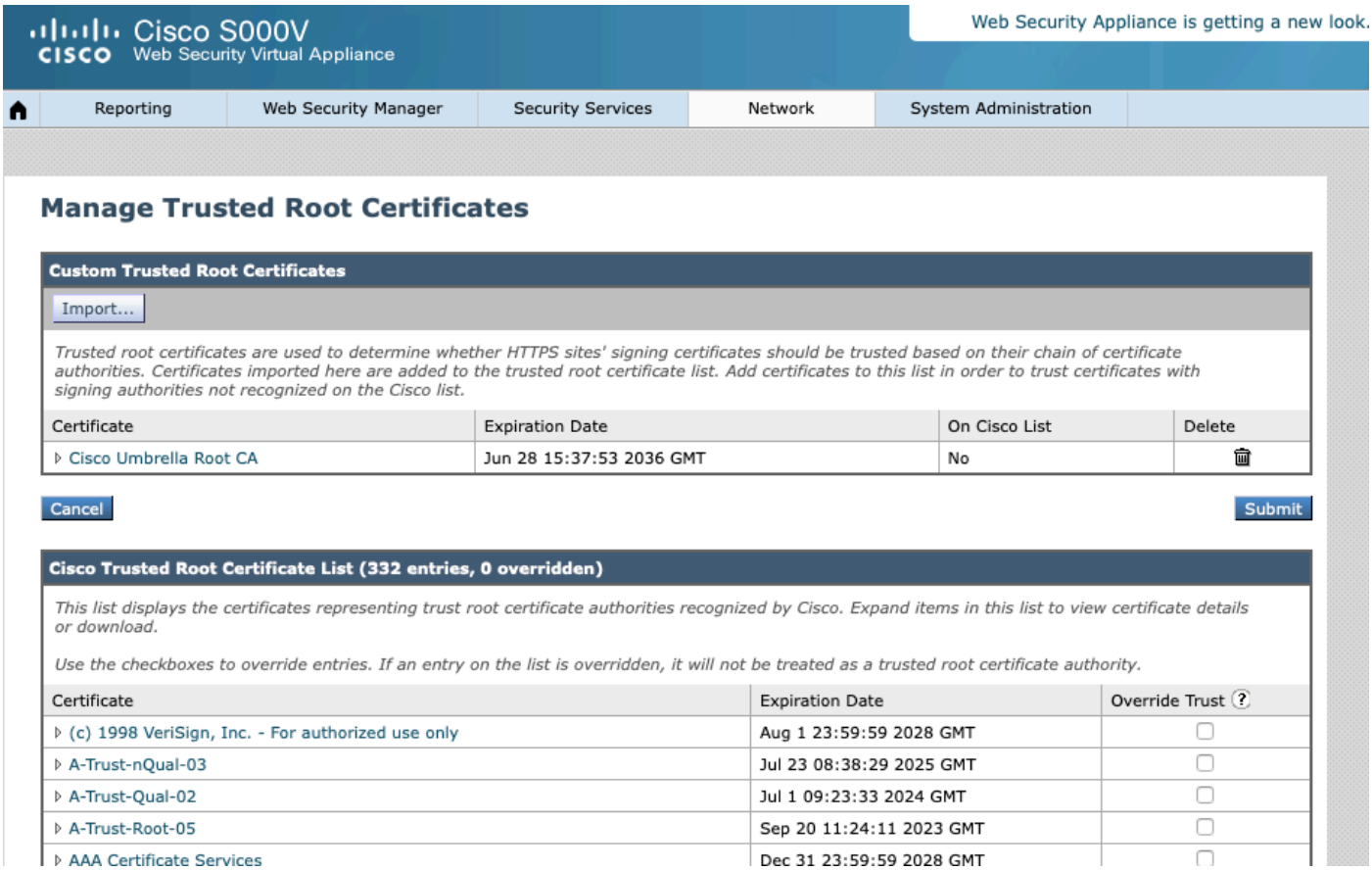
1. X-Forwarded-For Header

- to implement the internal IP based Web Policy in SWG.Make sure to enable the "X-Forwarded-For" header in Secure Web Appliance via **Security Services > Proxy Settings**.



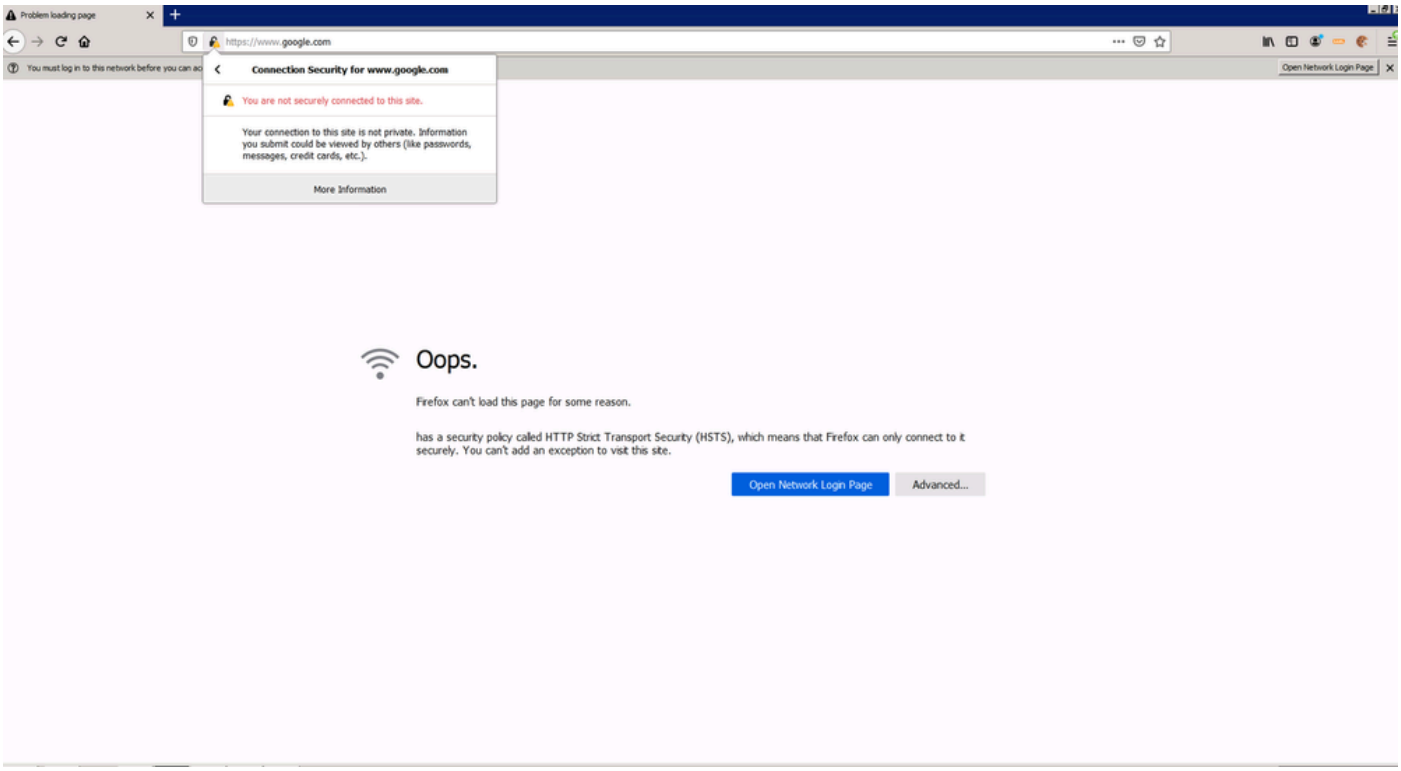
2. Trusted Root Certificate for HTTPs decryption.

- If the HTTPs decryption is enabled at **Web Policy** in the Umbrella dashboard, download "Cisco Root Certificate" from the **Umbrella dashboard> Deployments> Configuration** and import it into the Secure Web Appliance trusted root certificates.



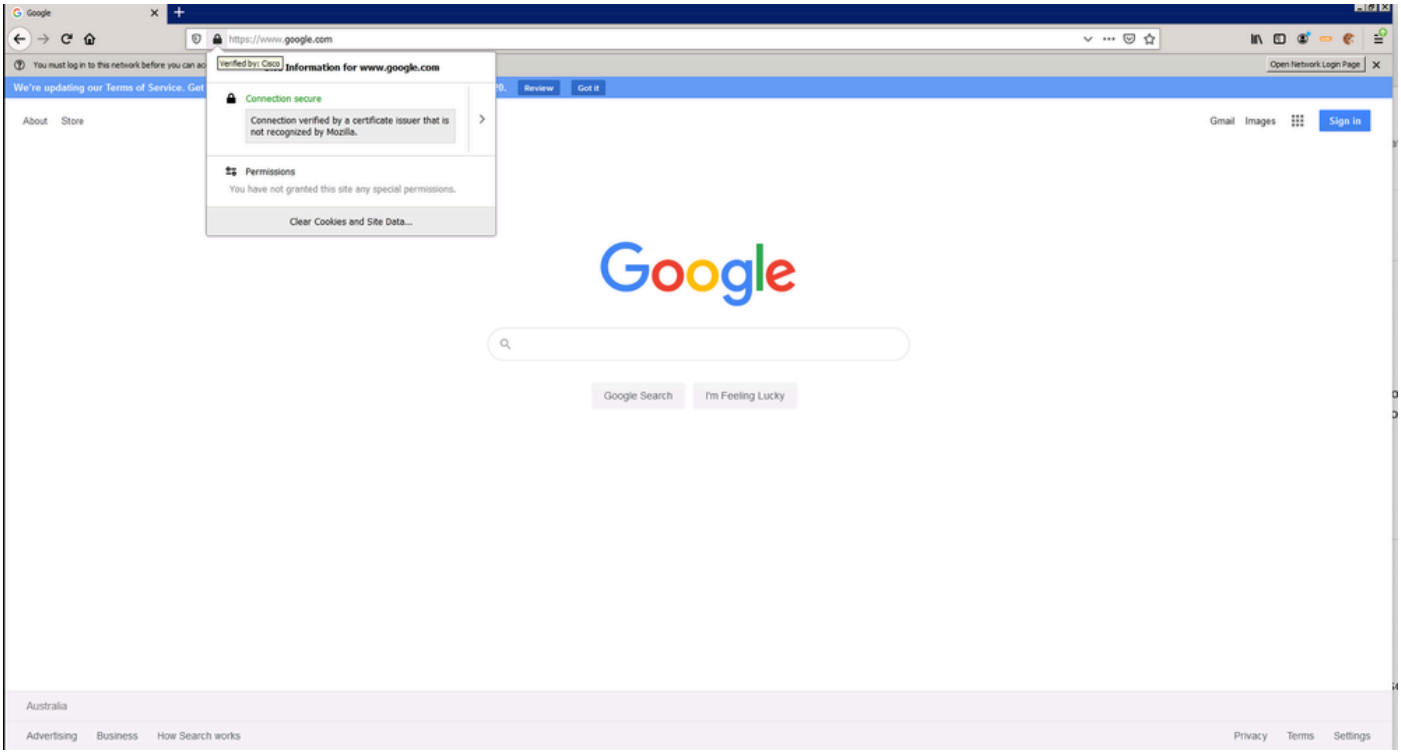
360050589612

- If the "Cisco Root Certificate" has not been imported to the Secure Web Appliance while the HTTPs decryption is enabled at SWG Web Policy, the end-user receives an error similar to this example:
  - "Oops. (browser) cannot load this page for some reason. has a security policy called HTTP Strict Transport Security (HSTS), which means that (browser) can only connect to it securely. You cannot add an exception to visit this site."
  - "You are not securely connected to this site."



360050700171

- This is an example of the HTTPs decrypted by Umbrella SWG. The certificate is verified by the "Cisco Root Certificate" named "Cisco."



360050700191

SWG Web Policy Configuration in Umbrella Dashboard

SWG Web Policy based on internal IP:

- Make sure to enable the "X-Forwarded-For" Header in the Secure Web Appliance, since SWG relies on that to identify the internal IP.
- Register the egress IP of the Secure Web Appliance in **Deployment > Networks**.
- Create an internal IP of the client machine in **Deployment > Configuration > Internal Networks**. Please select the registered Secure Web Appliance egress IP (Step 1) after ticking/selecting "Show Networks."
- Create a new Web Policy based on the internal IP created in Step 2.
- Make sure the "Enable SAML" option is disabled in the Web Policy.

SWG Web Policy based on AD user/group:

- Make sure all AD users and groups are provisioned to the Umbrella dashboard.
- Create a new web policy based on the registered egress IP of the Secure Web Appliance with the "Enable SAML" option enabled.
- Create another new web policy based on the AD user/group with the "Enable SAML" option disabled. Also need to place this web policy ahead of the Web Policy created at Step 2.