Configuración de la cadena de proxy entre el dispositivo web seguro y el SWG de Umbrella

Contenido

Introducción

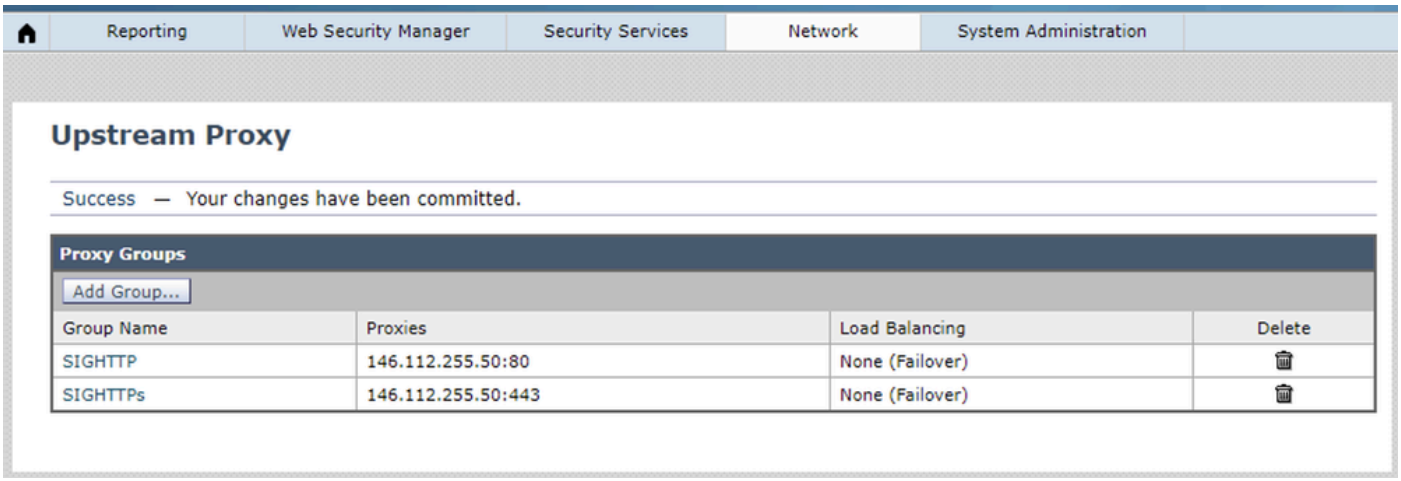
En este documento se describe cómo configurar la cadena de proxy entre Secure Web Appliance y Umbrella Secure Web Gateway (SWG).

Overview

Umbrella SIG soporta la cadena de proxy y puede manejar todas las solicitudes HTTP/HTTPs del servidor proxy de flujo descendente. Esta es una guía completa para implementar la cadena de proxy entre Cisco Secure Web Appliance (anteriormente Cisco WSA) y Umbrella Secure Web Gateway (SWG), incluida la configuración tanto para Secure Web Appliance como para SWG.

Configuración de la política de Secure Web Appliance

1. Configure los links HTTP y HTTPs SWG como el Proxy Upstream vía Red>Proxy Upstream.

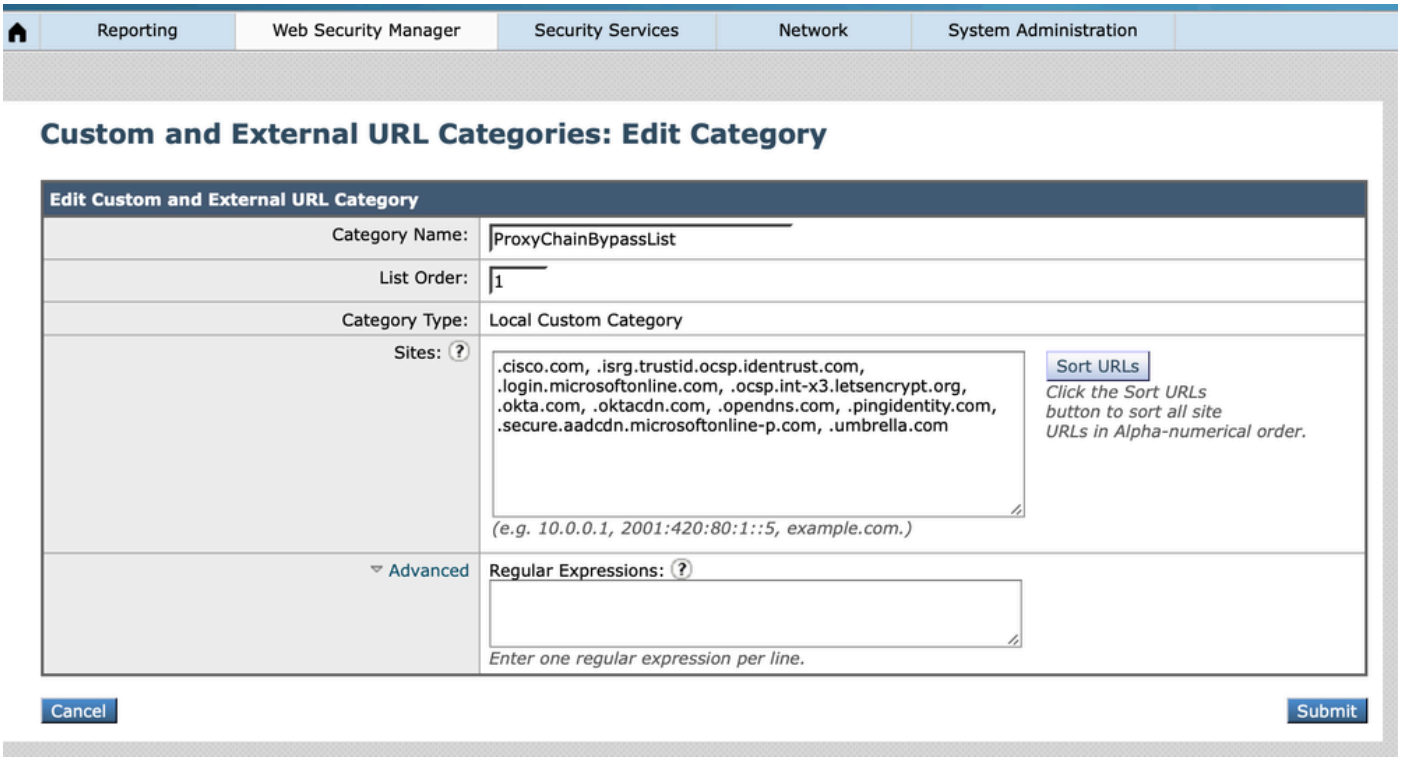


360079596451

2. Cree una política de desvío a través de Web Security Manager>Política de enrutamiento para enrutar todas las URL sugeridas a Internet directamente. Todas las URL omitidas se pueden

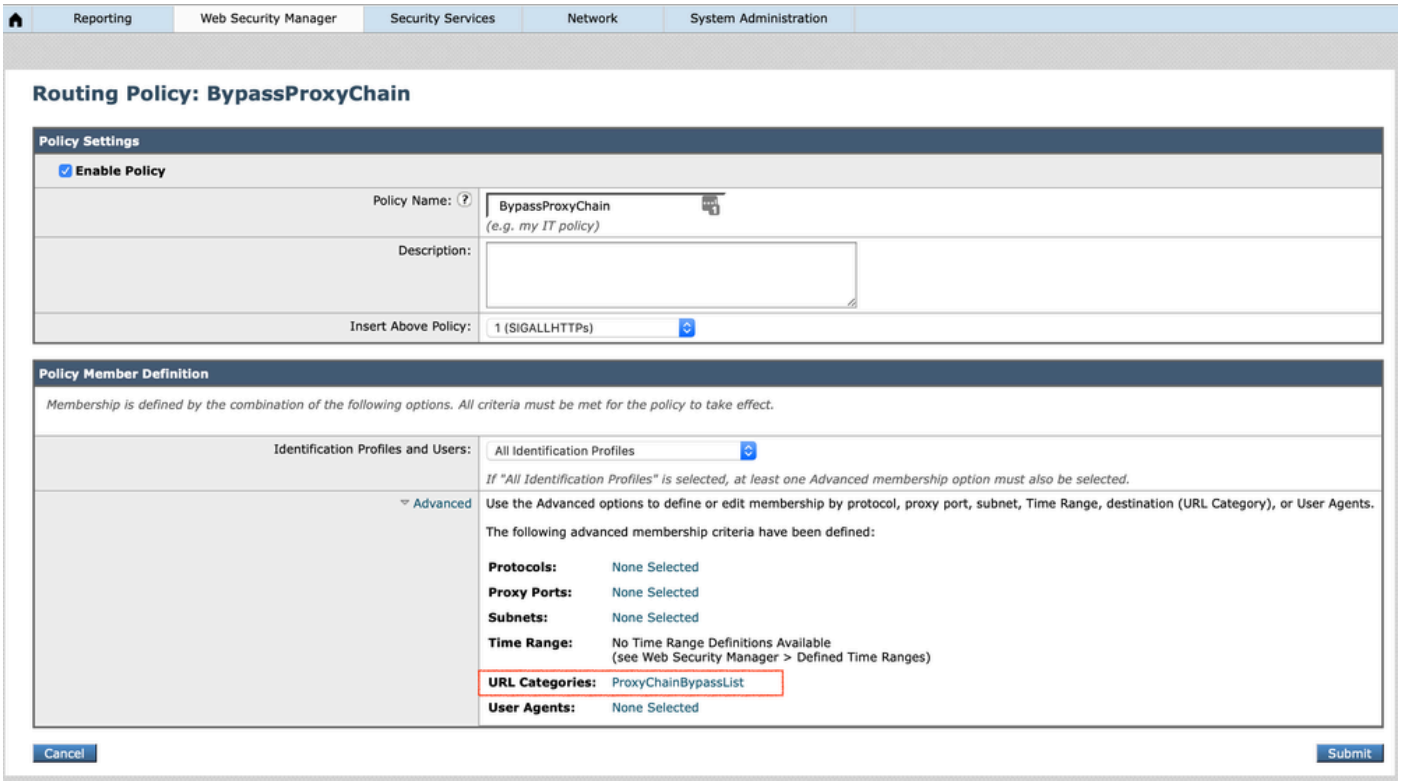
encontrar en nuestra documentación: [Guía del usuario de Cisco Umbrella SIG: Administrar encadenamiento de proxy]

- Comience creando una nueva "Categoría personalizada" navegando hasta Administrador de seguridad web>Categorías de URL externas y personalizadas como se muestra aquí. La política de omisión se basa en la "Categoría personalizada".



360050592552

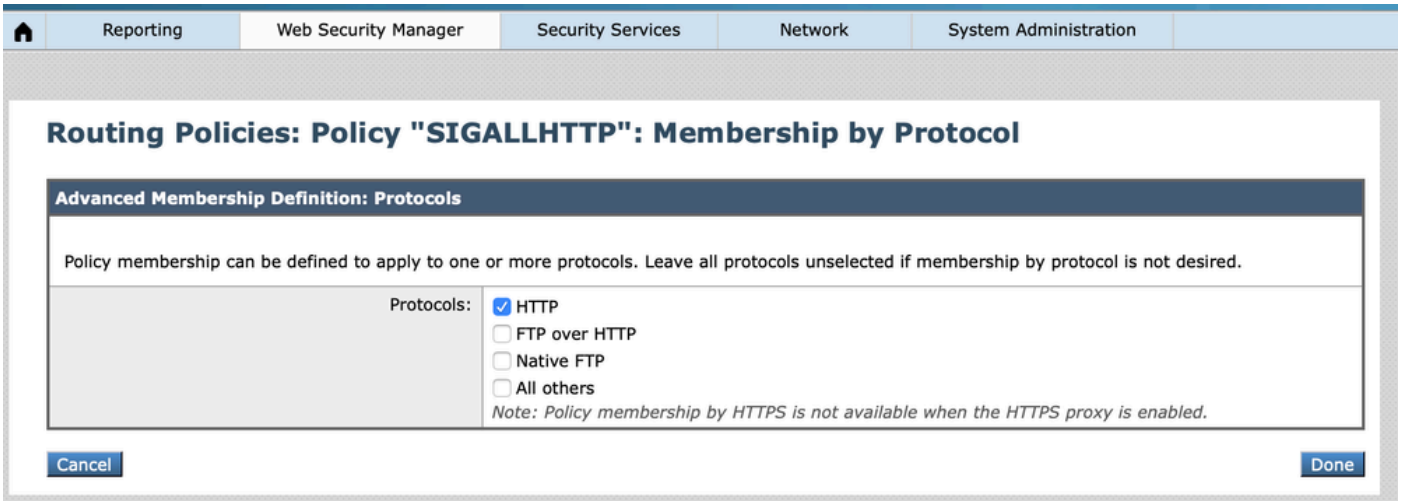
- A continuación, cree una nueva política de enrutamiento de omisión navegando hasta Administrador de seguridad web>Política de enrutamiento. Asegúrese de que esta política es la primera, ya que el dispositivo web seguro coincide con la política basada en el orden de la política.



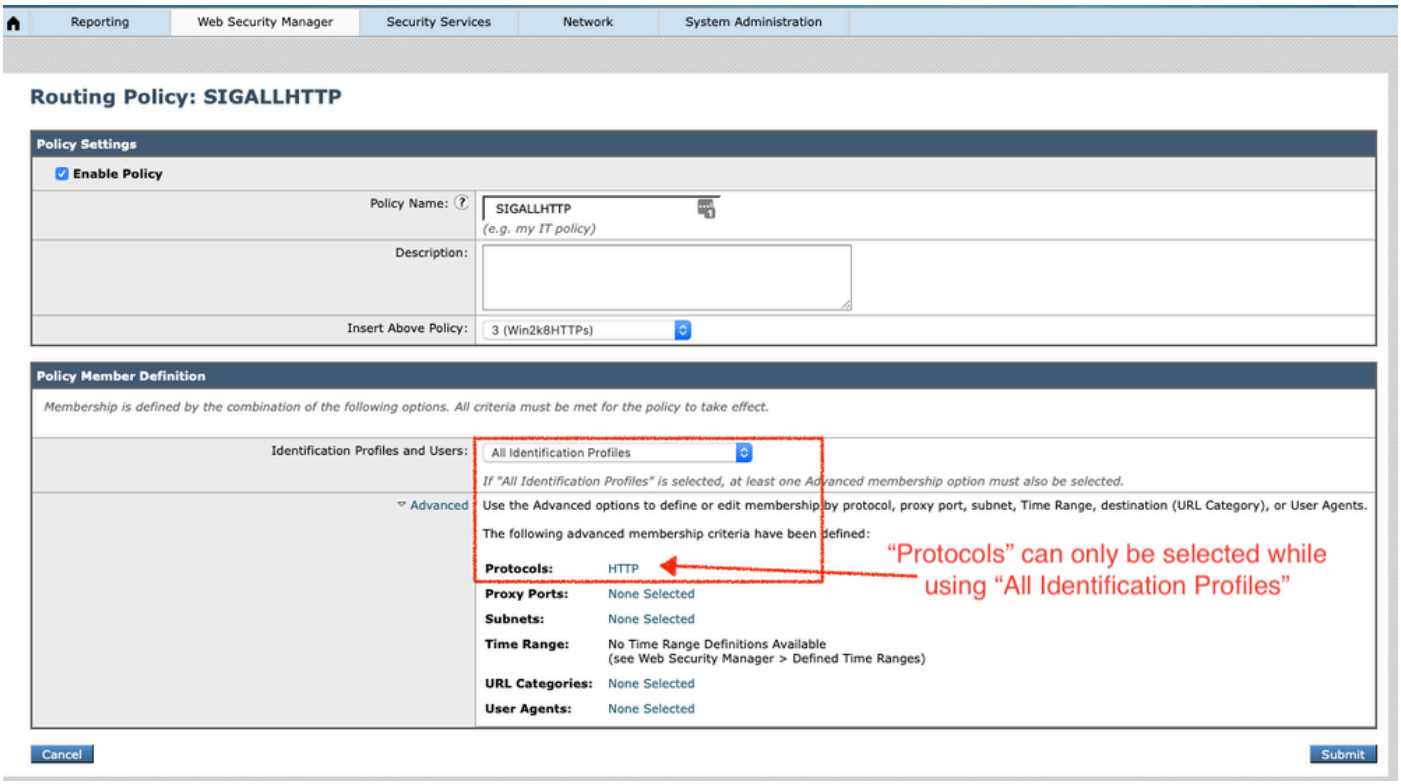
360050703131

3. Cree una nueva política de enrutamiento para todas las solicitudes HTTP.

- En la definición de miembro de la política de routing de Secure Web Appliance, las opciones de protocolo son HTTP, FTP sobre HTTP, FTP nativo y "Todos los demás", mientras que se selecciona "Todos los perfiles de identificación". Dado que no hay ninguna opción para HTTP, cree la política de enrutamiento para la solicitud de HTTP individualmente después de implementar esta política de enrutamiento para todas las solicitudes HTTP.

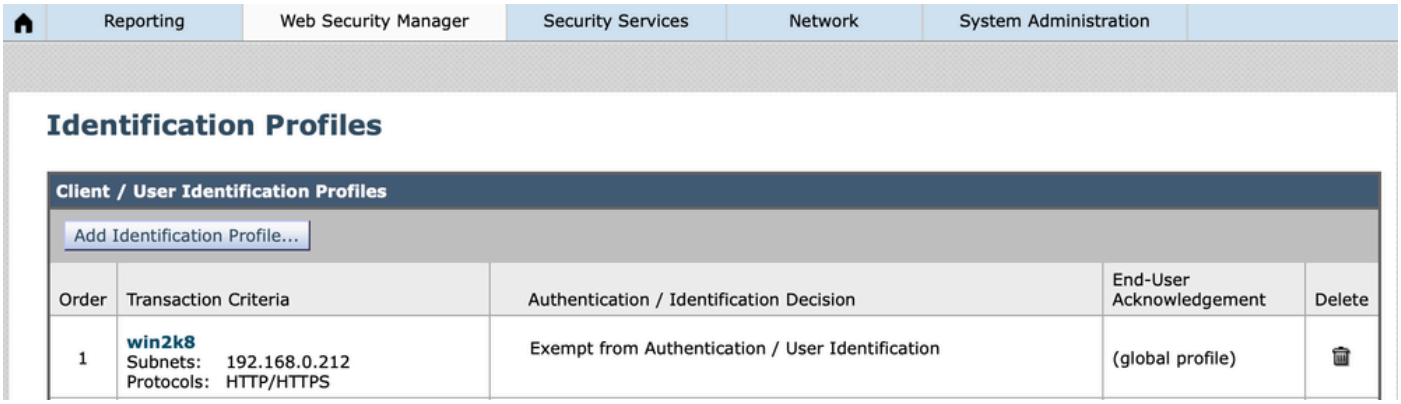


360050592772

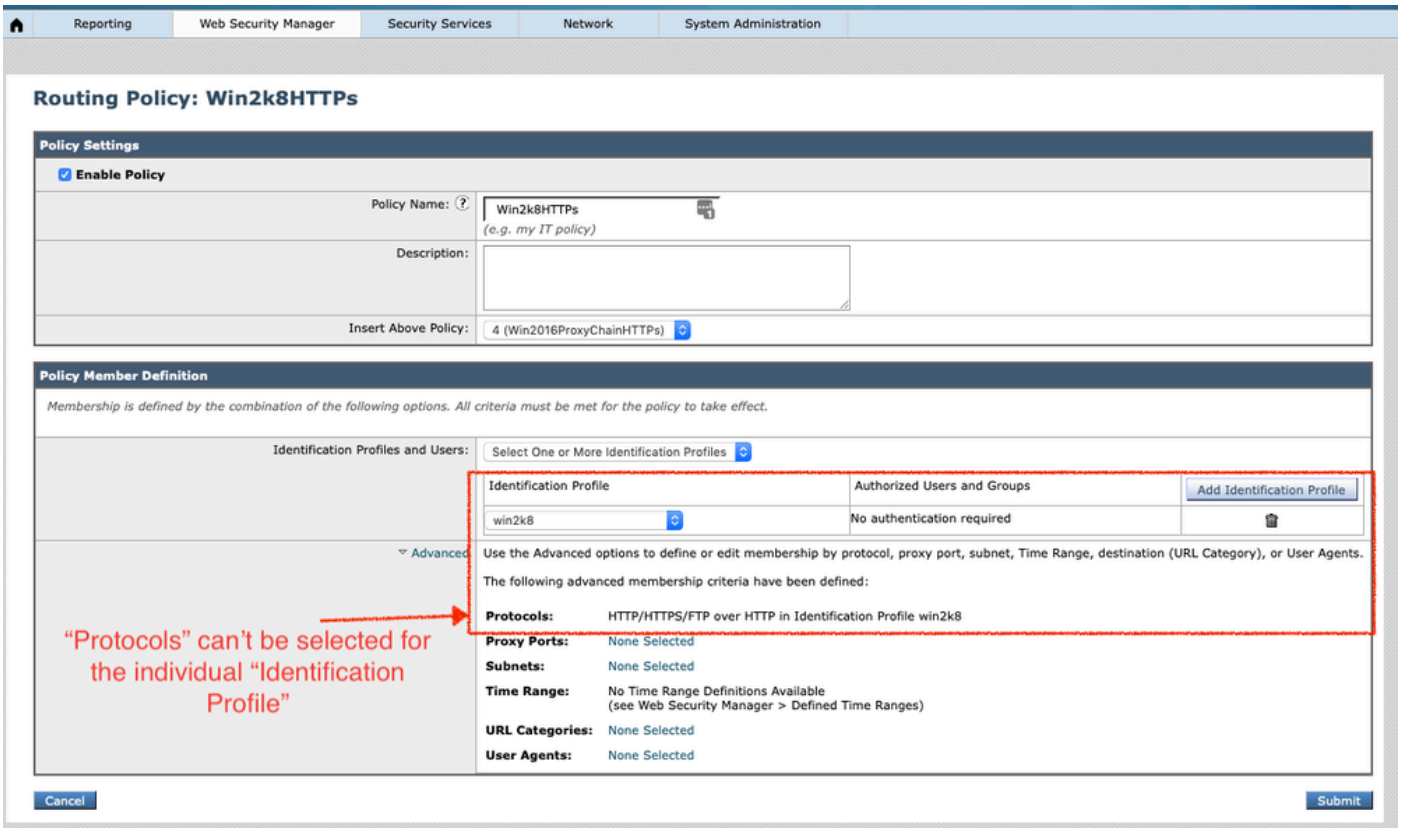


360050589572

4. Cree la política de enrutamiento para las solicitudes HTTP basándose en el "perfil de identificación". Tenga cuidado con la secuencia del "perfil de identificación" definido, ya que el dispositivo web seguro coincide con la "identificación" para la primera coincidencia. En este ejemplo, el perfil de identificación "win2k8" es una identidad interna basada en IP.



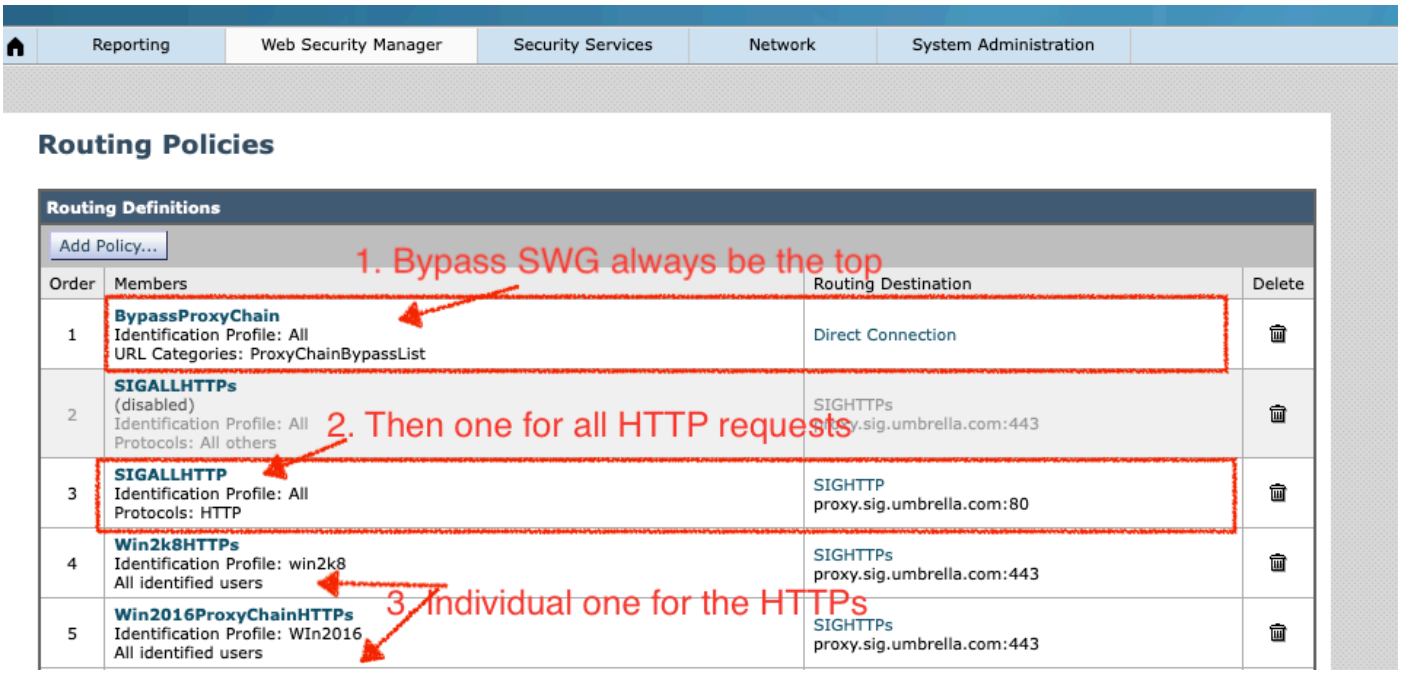
360050703971



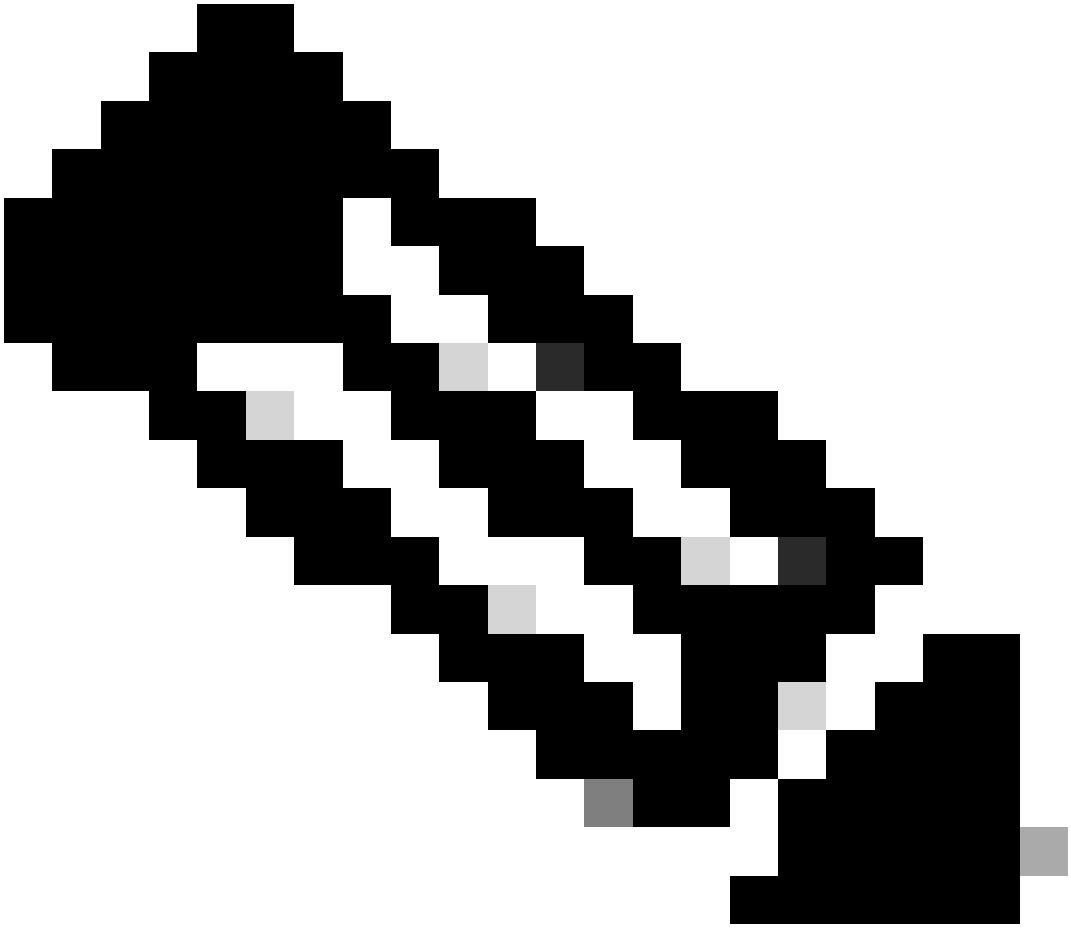
360050700091

5. Configuraciones finales de las políticas de routing de dispositivos web seguros:

- Tenga en cuenta que Secure Web Appliance evalúa las identidades y las políticas de acceso mediante un enfoque de procesamiento de reglas "descendente". Esto significa que la primera coincidencia realizada en cualquier punto del procesamiento tiene como resultado la acción realizada por Secure Web Appliance.
- Además, las identidades se evalúan primero. Una vez que el acceso de un cliente coincide con una identidad específica, Secure Web Appliance comprueba todas las políticas de acceso configuradas para utilizar la identidad que coincide con el acceso del cliente.



360050700131



Nota: La configuración de directiva mencionada sólo se aplica a la implementación de proxy explícito.

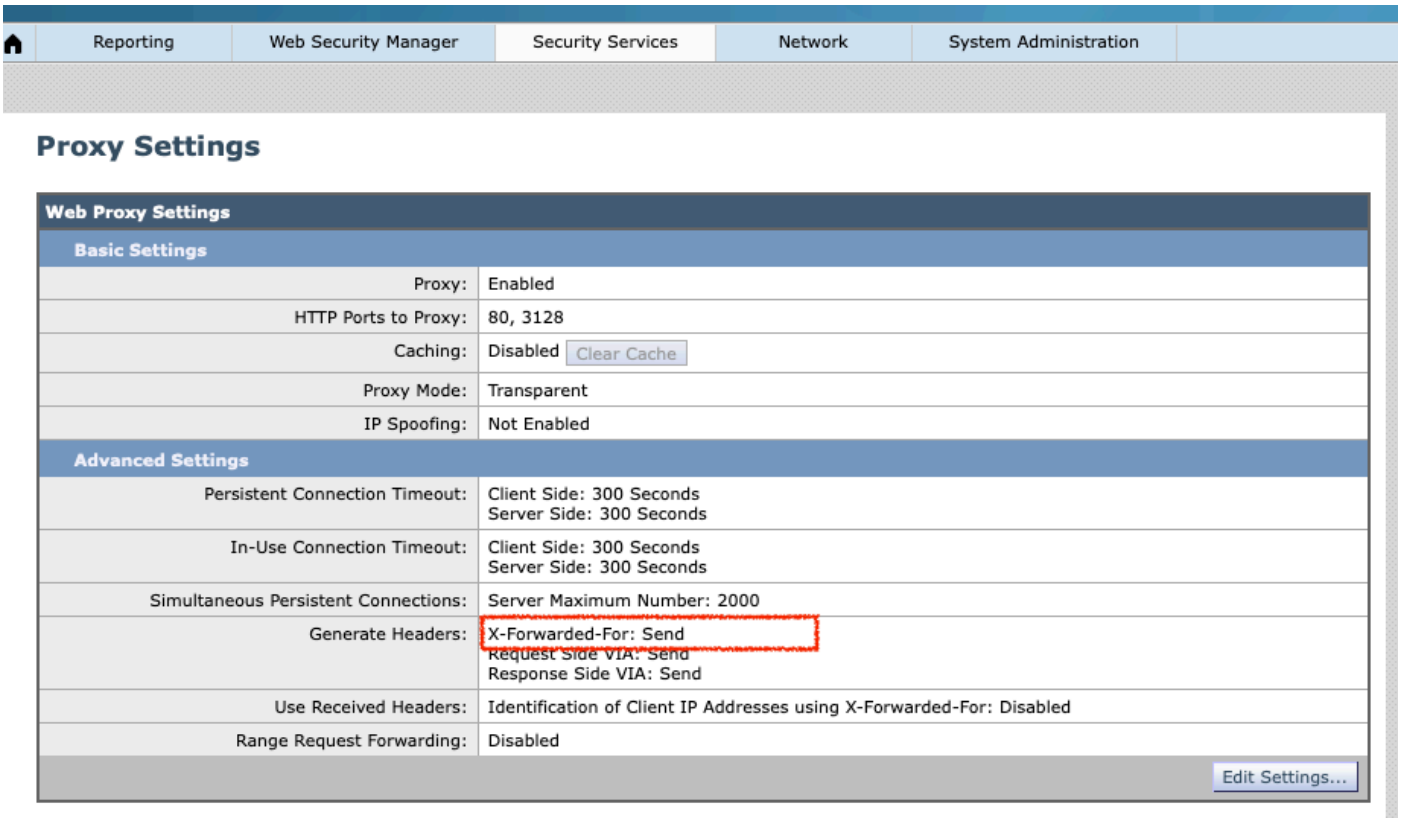
Para una implementación de proxy transparente

En el caso de HTTPS transparente, AsyncOS no tiene acceso a la información de los encabezados de cliente. Por lo tanto, AsyncOS no puede aplicar directivas de enrutamiento si alguna directiva de enrutamiento o perfil de identificación depende de la información de los encabezados de cliente.

1. Las transacciones HTTPS redirigidas de forma transparente sólo coinciden con las políticas de enrutamiento si:
    - El grupo de políticas de enrutamiento no tiene definidos criterios de pertenencia a políticas como la categoría de URL, el agente de usuario, etc.
    - El perfil de identificación no tiene definidos criterios de pertenencia a políticas como la categoría de URL, el agente de usuario, etc.
2. Si algún perfil de identificación o política de enrutamiento tiene definida una categoría de URL personalizada, todas las transacciones HTTPS transparentes coinciden con el grupo de políticas de enrutamiento predeterminado.
3. En la medida de lo posible, evite configurar la política de routing con todos los perfiles de identificación, ya que esto podría hacer que las transacciones HTTPS transparentes coincidieran con el grupo de políticas de routing predeterminado.

1. Encabezado X-Forwarded-For

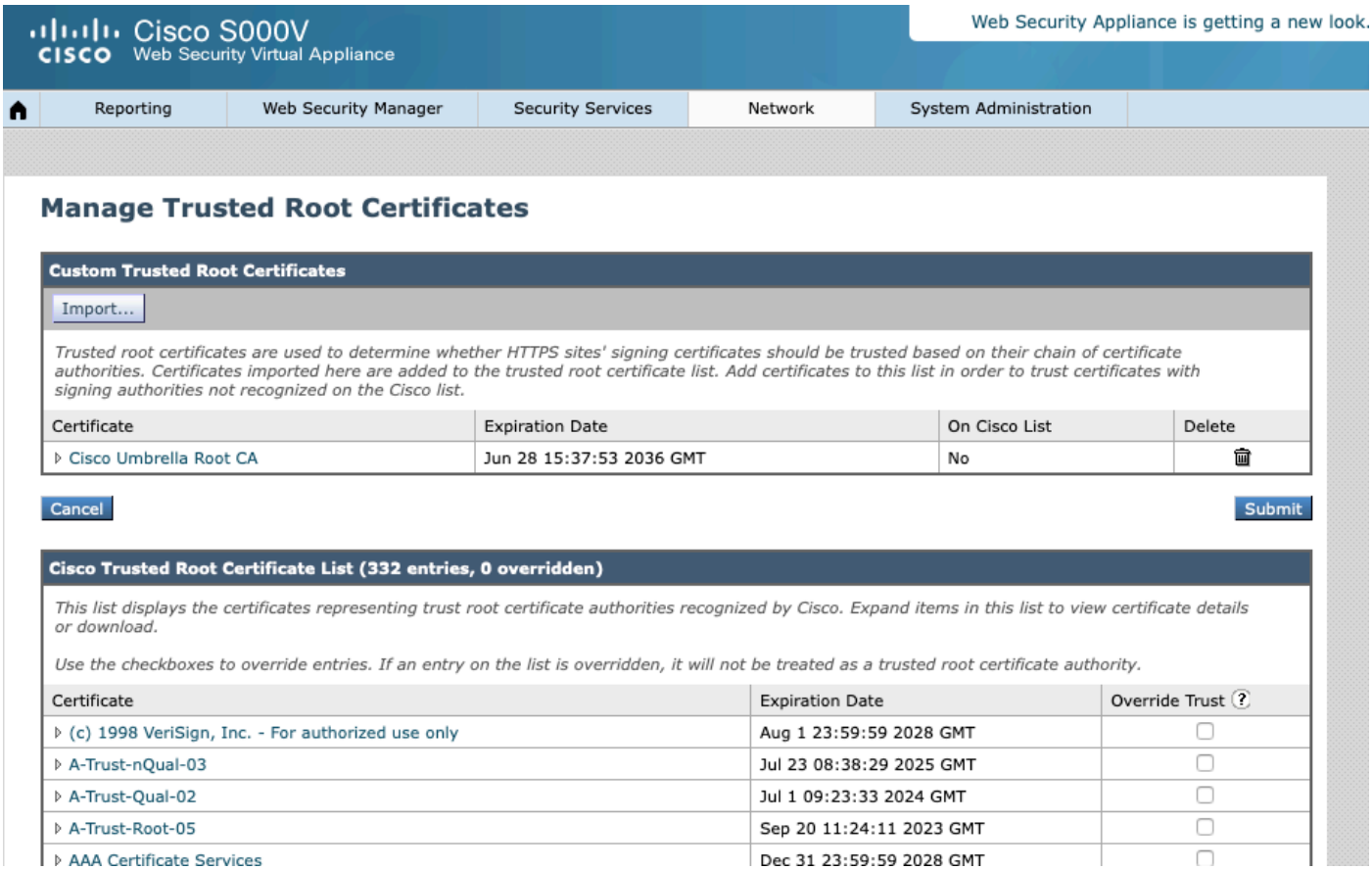
- para implementar la política web interna basada en IP en SWG.Asegúrese de habilitar el encabezado "X-Forwarded-For" en Secure Web Appliance mediante Servicios de seguridad > Configuración de proxy.



360050700111

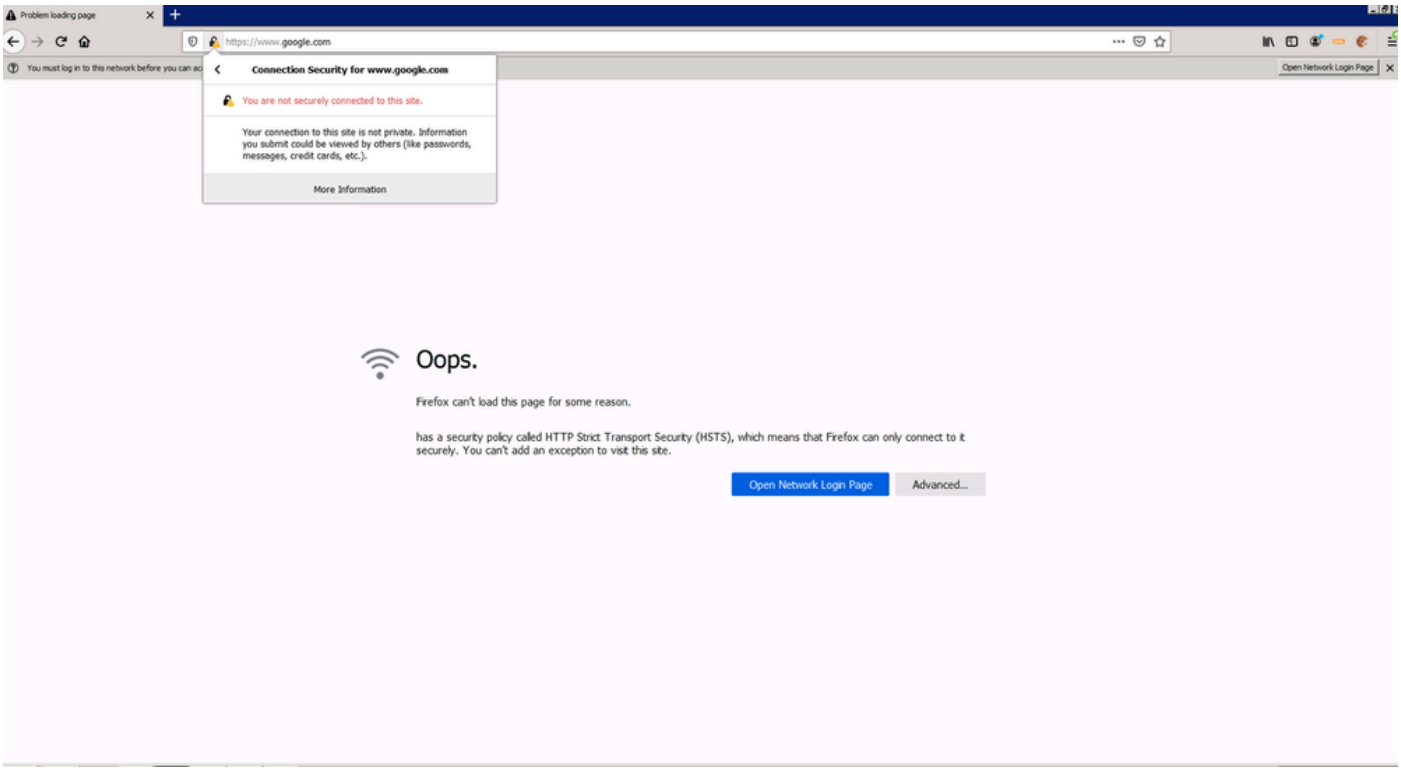
2. Certificado raíz de confianza para el descifrado de HTTPs.

- Si el descifrado de HTTPs está habilitado en Web Policy en el panel de Umbrella, descargue "Cisco Root Certificate" desde el panel de Umbrella> Deployments> Configuration e impórtelo en los certificados raíz de confianza de Secure Web Appliance.



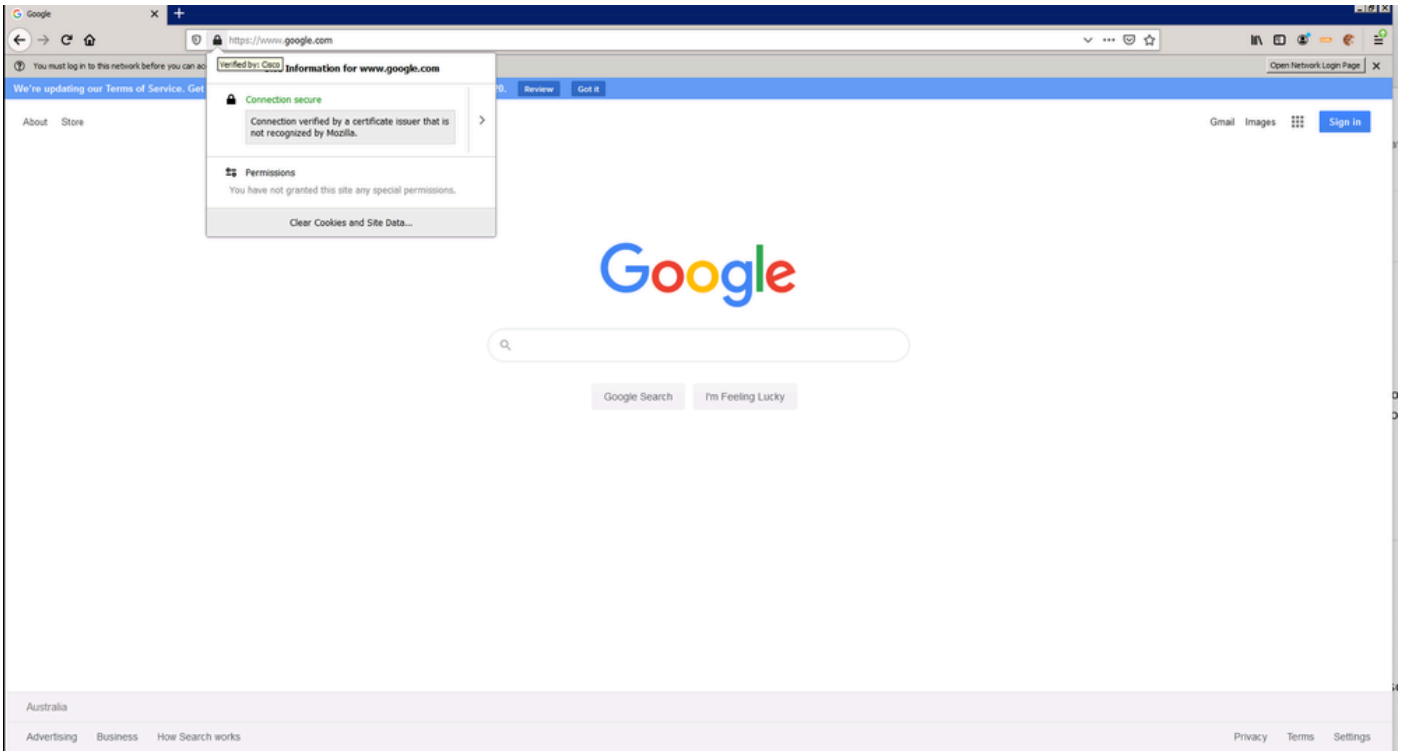
360050589612

- Si el "certificado raíz de Cisco" no se ha importado al dispositivo web seguro mientras el descifrado de HTTPs está habilitado en la política web de SWG, el usuario final recibe un error similar a este ejemplo:
  - "Uy. (navegador) no puede cargar esta página por algún motivo. cuenta con una política de seguridad denominada seguridad de transporte estricta HTTP (HSTS), lo que significa que (navegador) solo puede conectarse a ella de forma segura. No puede agregar una excepción para visitar este sitio."
  - "No está conectado de forma segura a este sitio."



360050700171

- Este es un ejemplo de los HTTP descifrados por Umbrella SWG. El certificado se verifica mediante el "certificado raíz de Cisco" denominado "Cisco".



360050700191

Configuración de la política web de SWG en el panel de Umbrella

Política web SWG basada en IP interna:

- Asegúrese de habilitar el encabezado "X-Forwarded-For" en el dispositivo web seguro, ya que SWG se basa en eso para identificar la IP interna.
- Registre la IP de salida del dispositivo web seguro en Implementación > Redes.
- Cree una IP interna del equipo cliente en Implementación > Configuración > Redes internas. Seleccione la IP de salida del dispositivo web seguro registrado (paso 1) después de marcar/seleccionar "Mostrar redes".
- Cree una nueva política web basada en la IP interna creada en el paso 2.
- Asegúrese de que la opción "Enable SAML" (Activar SAML) esté desactivada en la política web.

Política web SWG basada en usuario/grupo AD:

- Asegúrese de que todos los usuarios y grupos de AD se aprovisionan en el panel de Umbrella.
- Cree una nueva política web basada en la IP de salida registrada del dispositivo web seguro con la opción "Enable SAML" (Activar SAML) activada.
- Cree otra nueva política web basada en el usuario/grupo de AD con la opción "Activar SAML" desactivada. También debe colocar esta política web por delante de la política web creada en el paso 2.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).