# Citrix Secure Web Gateway 12.1

**Machine translated content**

## Disclaimer

La versión oficial de este contenido está en inglés. Para mayor comodidad, parte del contenido de la documentación de Cloud Software Group solo tiene traducción automática. Cloud Software Group no puede controlar el contenido con traducción automática, que puede contener errores, imprecisiones o un lenguaje inadecuado. No se ofrece ninguna garantía, ni implícita ni explícita, en cuanto a la exactitud, la fiabilidad, la idoneidad o la precisión de las traducciones realizadas del original en inglés a cualquier otro idioma, o que su producto o servicio de Cloud Software Group se ajusten a cualquier contenido con traducción automática, y cualquier garantía provista bajo el contrato de licencia del usuario final o las condiciones de servicio, o cualquier otro contrato con Cloud Software Group, de que el producto o el servicio se ajusten a la documentación no se aplicará en cuanto dicha documentación se ha traducido automáticamente. Cloud Software Group no se hace responsable de los daños o los problemas que puedan surgir del uso del contenido traducido automáticamente.

# Contents



# Notas de la versión

April 27, 2021

Las notas de la versión del producto Citrix Secure Web Gateway se recogen en las notas de la versión principales de un dispositivo Citrix ADC. Consulte Notas de versión de Citrix ADC.

# Plataformas de hardware y software compatibles

April 27, 2021

El dispositivo Citrix Secure Web Gateway (SWG) está disponible actualmente como dispositivo de hardware y como dispositivo virtual. Las especificaciones detalladas están disponibles en la hoja de datos, que está disponible en www.citrix.com. Pase el puntero del mouse sobre **Productos** y, en la lista **Redes**, seleccione **Citrix Secure Web Gateway**.

Antes de instalar el dispositivo SWG, asegúrese de que dispone de las licencias correctas. Cada dispositivo en una configuración de alta disponibilidad requiere su propia licencia. Para obtener información acerca de las licencias, consulte Requisitos de licencia. Para obtener información acerca de la alta disponibilidad, consulte el tema Introducción a la alta disponibilidad.

## Dispositivo de hardware (MPX)

- Citrix SWG MPX 14020/14030/14040
- Citrix SWG MPX 14020-40G/14040-40G
- Citrix SWG MPX 14060-40S/14080-40S/14100-40S

## Dispositivo virtual (VPX)

- Citrix SWG VPX 200
- Citrix SWG VPX 1000
- Citrix SWG VPX 3000
- Citrix SWG VPX 5000
- Citrix SWG VPX 8000
- Citrix SWG VPX 10G
- Citrix SWG VPX 15G
- Citrix SWG VPX 25G

### Dispositivo de hardware (SDX)

Las instancias SWG se pueden aprovisionar en cualquier plataforma SDX instalando la licencia "SDX 2-Instance Add-On Pack for Secure Web Gateway". Con una instalación de licencia, puede aprovisionar dos instancias SWG en un dispositivo SDX. Puede aprovisionar más instancias SWG en el dispositivo agregando más licencias. Para obtener más información sobre el aprovisionamiento de una instancia de Citrix SWG, consulte Aprovisionar instancias de Citrix ADC.

## Requisito de licencia

April 27, 2021

Una licencia le da acceso a un conjunto de funciones en un dispositivo Citrix Secure Web Gateway (SWG).

El marco de licencias de Citrix le permite centrarse en obtener el máximo valor de los productos Citrix. El proceso de asignación de licencias es muy sencillo. En la Utilidad de configuración SWG (GUI), puede utilizar el número de serie de hardware (HSN) o el código de activación de licencia (LAC) para asignar las licencias. Si ya existe una licencia en el equipo local, puede cargarla en el dispositivo.

Para todas las demás funciones, como devolver o reasignar su licencia, debe utilizar el portal de licencias (que también puede utilizar para la asignación inicial de licencias si lo prefiere). Para obtener más información sobre el portal de licencias, consulte http://support.citrix.com/article/CTX131110.

Puede asignar licencias parcialmente según sea necesario para su implementación. Por ejemplo, si el archivo de licencia contiene diez licencias, pero el requisito actual es solo para seis licencias, puede asignar seis licencias ahora y asignar licencias adicionales más adelante. No puede asignar más del número total de licencias presentes en el archivo de licencia.

Antes de utilizar el dispositivo SWG, debe instalar las siguientes licencias mediante la GUI o la CLI:

- **Licencia de Citrix Secure Web Gateway**
  - La licencia de Citrix SWG Platform es el requisito mínimo para utilizar el dispositivo MPX SWG y para implementar la instancia VPX en diferentes hipervisores, como XenServer, VMware ESX, Microsoft Hyper-V y Linux-KVM.
  - Para las plataformas SDX, se requiere al menos una licencia de paquete adicional SWG para sesiones simultáneas SDX 10K para aprovisionar una instancia de Citrix SWG en un dispositivo Citrix ADC SDX.
- **Licencia de función de inteligencia de amenazas URL**. Esta licencia es necesaria para el uso de las funciones de filtrado de URL, categorización de URL y puntuación de reputación de URL.

### Requisitos previos

Para utilizar el número de serie de hardware o el código de activación de licencia para asignar las licencias:

- Debe poder acceder a dominios públicos a través del dispositivo. Por ejemplo, el dispositivo debería poder acceder a `www.citrix.com`. El software de asignación de licencias accede internamente al portal de licencias de Citrix para su licencia. Para tener acceso a un dominio público, puede utilizar un servidor proxy o configurar un servidor DNS y, en el dispositivo Citrix ADC, configurar una dirección NSIP o una dirección IP de subred (SNIP).
- Su licencia debe estar vinculada a su hardware, o debe tener un código de activación de licencia (LAC) válido. Citrix envía su LAC por correo electrónico cuando compra una licencia.

### Licencias para dispositivos en una configuración de alta disponibilidad

Debe adquirir una licencia independiente para cada dispositivo en un par de alta disponibilidad (HA). Asegúrese de que el mismo tipo de licencia está instalado en ambos dispositivos.

En un dispositivo Citrix ADC SDX, puede configurar una configuración de alta disponibilidad (HA) entre dos instancias SWG del mismo dispositivo. Sin embargo, Citrix recomienda configurar una configuración de alta disponibilidad entre dos instancias SWG en diferentes dispositivos Citrix ADC SDX.

### Asigne e instale sus licencias

Puede asignar e instalar sus licencias mediante la interfaz gráfica de usuario. La instalación de las licencias mediante la CLI requiere copiar las licencias en el directorio /nsconfig/license/.

#### Asigne sus licencias mediante la GUI de Citrix SWG

1. En un explorador web, escriba la dirección IP del dispositivo Citrix SWG.
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. En la ficha **Configuración**, vaya a **Sistema** > **Licencias**.
4. En el panel de detalles, haga clic en **Administrar licencias**, haga clic en **Agregar nueva licencia** y, a continuación, seleccione una de las siguientes opciones:
    - **Utilice el número de serie**. El software obtiene internamente el número de serie del dispositivo y utiliza este número para mostrar sus licencias.
    - **Utilice el código de activación de licencia**. Citrix envía por correo electrónico el código de activación de la licencia (LAC) de la licencia que compró. Introduzca el LAC en el cuadro de texto.

Si no quiere configurar la conectividad a Internet en el dispositivo Citrix ADC, puede utilizar un servidor proxy. Seleccione Conectar a través del servidor proxy y especifique la dirección IP y el puerto del servidor proxy.

5. Haga clic en **Obtener licencias**.
6. Seleccione el archivo de licencia que quiere utilizar para asignar sus licencias.
7. En la columna **Asignar**, introduzca el número de licencias que se asignarán. A continuación, haga clic en **Obtener**.
8. Haga clic en **Reiniciar** para que la licencia surta efecto.
9. En el cuadro de diálogo **Reiniciar**, haga clic en **Aceptar**.

#### Instale sus licencias mediante la GUI de Citrix SWG

1. En un explorador web, escriba la dirección IP del dispositivo Citrix SWG (por ejemplo, `http://192.168.100.1`).
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. En la ficha **Configuración**, vaya a **Sistema** > **Licencias**.
4. En el panel de detalles, haga clic en **Administrar licencias**.
5. Haga clic en **Agregar nueva licencia** y, a continuación, seleccione **Cargar archivos de licencia**.
6. Haga clic en **Examinar**. Vaya a la ubicación de los archivos de licencias, seleccione el archivo de licencias y, a continuación, haga clic en **Abrir**.
7. Haga clic en **Reiniciar** para aplicar la licencia.
8. En el cuadro de diálogo **Reiniciar**, haga clic en **Aceptar**.

#### Instale sus licencias mediante la CLI de Citrix SWG

1. Abra una conexión SSH al dispositivo Citrix SWG mediante un cliente SSH, como PuTTY.
2. Inicie sesión en el dispositivo mediante las credenciales de administrador.
3. Cambie al símbolo del shell y copie los nuevos archivos de licencia en el subdirectorio de licencias del directorio nsconfig. Si el subdirectorio no existe, créelo antes de copiar los archivos.

**Ejemplo**:

```
    login: nsroot

    Password: nsroot

```

```
    Last login: Mon Aug  4 03:37:27 2008 from 10.102.29.9

    Done

    > shell

    Last login: Mon Aug  4 03:51:42 from 10.103.25.64

    root@ns# mkdir /nsconfig/license

    root@ns# cd /nsconfig/license
<!--NeedCopy-->
```

Copie los nuevos archivos de licencia en este directorio.

> **Nota**
>
> La CLI no le pide que reinicie el dispositivo para activar las licencias. Ejecute el comando **reboot -w** para reiniciar el sistema o ejecute el comando **reboot** para reiniciar el sistema normalmente.

## Verifique las funciones con licencia

Antes de utilizar una función, asegúrese de que su licencia es compatible con la función.

### Verifique las funciones con licencia mediante la interfaz gráfica de usuario de Citrix SWG

1. En un explorador web, escriba la dirección IP del dispositivo Citrix SWG (por ejemplo, `http://192.168.100.1`).
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. Vaya a **Sistema** > **Licencias**.
   La pantalla tiene una marca de verificación verde junto a cada función con licencia.

### Verifique las funciones con licencia mediante la CLI de Citrix SWG

1. Abra una conexión SSH al dispositivo Citrix SWG mediante un cliente SSH, como PuTTY.
2. Inicie sesión en el dispositivo mediante las credenciales de administrador.
3. En el símbolo del sistema, escriba el comando sh ns license para mostrar las funciones admitidas por la licencia.

**Ejemplo**:

```
> licencia sh

        Estado de licencia:

```

```
                              Registro Web: NO

                          Protección contra sobretensiones: NO

                            Equilibrio de carga: SÍ

                ...

               Proxy de reenvío: SÍ

                          Intercepción SSL: SÍ

                           Número de modelo ID: 25000

                            Modo de licencia: Local

  Completado
```

### Habilitar o inhabilitar una función

Cuando utilice el dispositivo Citrix Secure Web Gateway por primera vez, debe habilitar una función antes de poder usarla. Si configura una función antes de habilitarla, aparecerá un mensaje de advertencia. La configuración se guarda, pero no se aplica hasta que se habilite la función.

#### Habilitar una función mediante la interfaz gráfica de usuario de Citrix SWG

1. En un explorador web, escriba la dirección IP del dispositivo Citrix SWG (por ejemplo, `http://192.168.100.1`).
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. Vaya a **Sistema** > **Configuración** > **Configurar funciones avanzadas**.
4. Seleccione las funciones (por ejemplo, Proxy de reenvío, Intercepción SSL y Filtrado de URL) que desea habilitar.

#### Habilitar una función mediante la CLI de Citrix SWG

En el símbolo del sistema, escriba los siguientes comandos para habilitar una función y verificar la configuración:

```
enable feature <FeatureName>

show feature
```

En el siguiente ejemplo se muestra cómo habilitar las funciones de interceptación SSL, proxy de reenvío y filtrado de URL.

```
> enable feature forwardProxy sslinterception urlfiltering

 Done

 >show feature

    Feature                        Acronym              Status

        -------                        -------              ------

 1)     Web Logging                    WL                   OFF

 2)     Surge Protection               SP                   OFF

...

...

36)    URL Filtering                  URLFiltering         ON

37)    Video Optimization             VideoOptimization    OFF

38)    Forward Proxy                  ForwardProxy         ON

39)    SSL Interception               SSLInterception      ON

Done
<!--NeedCopy-->
```

> **Nota**
>
> Si la clave de licencia no está disponible para una función, aparece el siguiente mensaje de error para esa función:
>
> ERROR: Funciones no autorizadas

## Instalación

April 27, 2021

Un dispositivo Citrix Secure Web Gateway (SWG) debe estar instalado correctamente y tener acceso a Internet para poder comenzar a configurarlo para proteger su empresa.

Para obtener información acerca de la instalación y la configuración inicial del dispositivo de hardware, consulte Configuración del hardware SWG.

Un dispositivo virtual Citrix SWG (VPX) es compatible con diferentes plataformas de virtualización.

Para obtener información acerca de los hipervisores compatibles e instrucciones para implementar un dispositivo VPX, consulte Implementar una instancia de Citrix ADC VPX.

## Introducción a un dispositivo Citrix ADC MPX y VPX SWG

April 27, 2021

Después de instalar el dispositivo de hardware (MPX) o software (VPX) y realizar la configuración inicial, estará listo para configurarlo como un dispositivo de puerta de enlace web seguro para recibir tráfico.

**Importante**:

- La comprobación OCSP requiere una conexión a Internet para comprobar la validez de los certificados. Si el dispositivo no es accesible desde Internet mediante la dirección NSIP, agregue listas de control de acceso (ACL) para realizar NAT desde la dirección NSIP a la dirección IP de la subred (SNIP). El SNIP debe ser accesible desde Internet. Por ejemplo:

```
add ns acl a1 ALLOW -srcIP = <NSIP> -destIP "!="
    10.0.0.0-10.255.255.255

set rnat a1 -natIP <SNIP>

apply acls
<!--NeedCopy-->
```

- Especifique un servidor de nombres DNS para resolver nombres de dominio. Para obtener más información, consulte Configuración inicial.
- Asegúrese de que la fecha del dispositivo está sincronizada con los servidores NTP. Si la fecha no está sincronizada, el dispositivo no puede comprobar de manera efectiva si un certificado de servidor de origen está caducado.

Para utilizar el dispositivo Citrix SWG, debe realizar las siguientes tareas:

- Agregue un servidor proxy en modo explícito o transparente.
- Habilitar la intercepción SSL.
  - Configure un perfil SSL.
  - Agregue y vincule directivas SSL al servidor proxy.
  - Agregue y vincule un par de claves de certificado de CA para la intercepción SSL.

**Nota:** Un dispositivo Citrix SWG configurado en modo proxy transparente puede interceptar solo los protocolos HTTP y HTTPS. Para omitir cualquier otro protocolo, como telnet, debe agregar la siguiente directiva de escucha en el servidor virtual proxy.

El servidor virtual ahora acepta solo el tráfico entrante HTTP y HTTPS.

```
set cs vserver transparent-pxy1 PROXY * * -cltTimeout 180 -Listenpolicy
    "CLIENT.TCP.DSTPORT.EQ(80) || CLIENT.TCP.DSTPORT.EQ(443)"`
<!--NeedCopy-->
```

Es posible que deba configurar las siguientes funciones, dependiendo de la implementación:

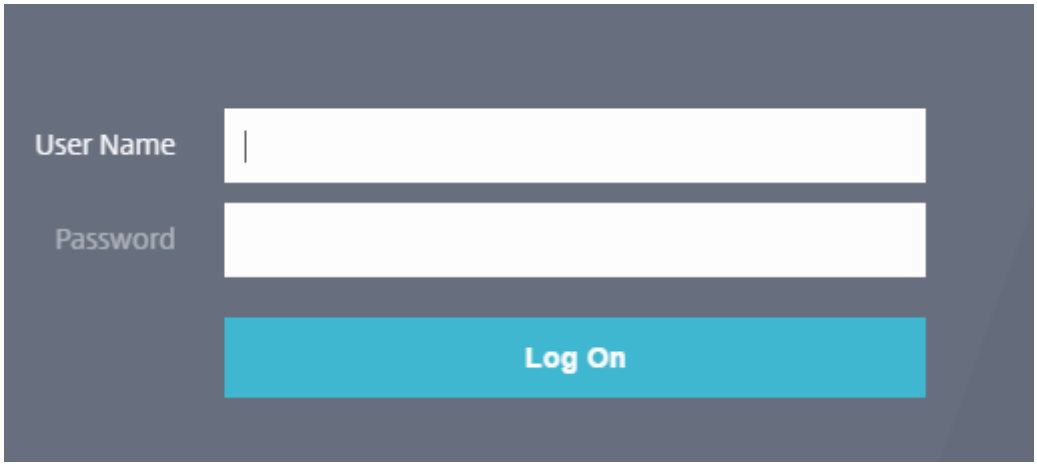
- Servicio de autenticación (recomendado): Para autenticar a los usuarios. Sin el Servicio de autenticación, la actividad del usuario se basa en la dirección IP del cliente.
- Filtrado de URL: Para filtrar las URL por categorías, puntuación de reputación y listas de URL.
- Análisis: Para ver la actividad del usuario, los indicadores de riesgo del usuario, el consumo de ancho de banda y las transacciones desglosadas en Citrix Application Delivery Management (ADM).

**Nota:** SWG implementa la mayoría de los estándares HTTP y HTTPS típicos seguidos de productos similares. Esta implementación se realiza sin ningún explorador específico en mente y es compatible con los exploradores más comunes. SWG ha sido probado con exploradores comunes y versiones recientes de Google Chrome, Internet Explorer y Mozilla Firefox.

### Asistente de puerta de enlace web segura

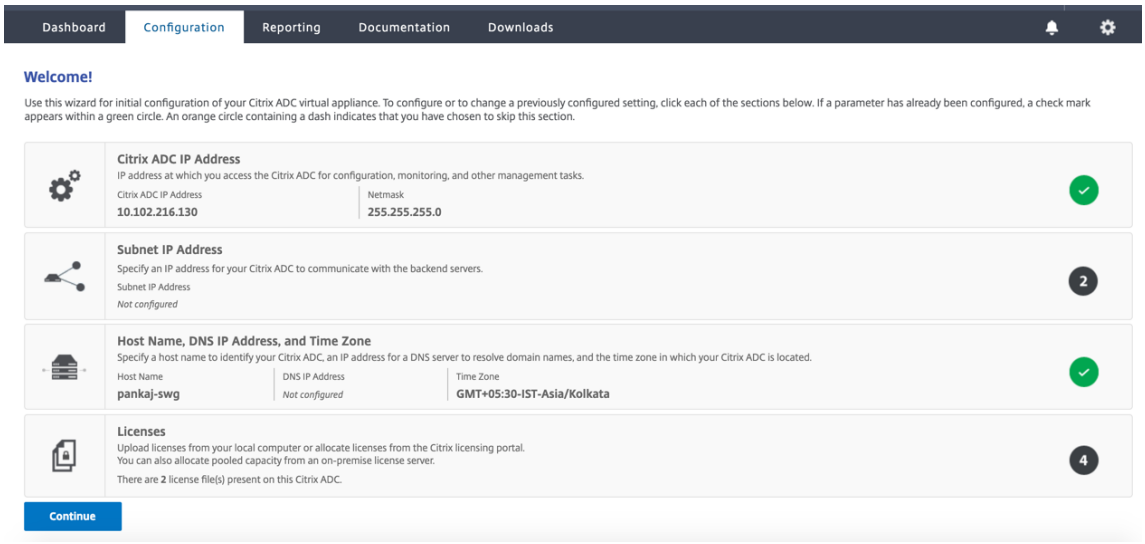
El asistente SWG proporciona a los administradores una herramienta para administrar toda la implementación SWG mediante un explorador web. Ayuda a guiar a los clientes para crear un servicio SWG rápidamente y ayuda a simplificar la configuración siguiendo una secuencia de pasos bien definidos.

1. Abra su explorador web e introduzca la dirección NSIP que especificó durante la configuración inicial. Para obtener más información acerca de la configuración inicial, consulte Configuración inicial.
2. Introduzca su nombre de usuario y contraseña.



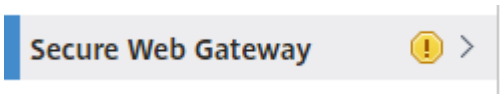

 

3. Si no ha especificado una dirección IP de subred (SNIP), aparecerá la siguiente pantalla.

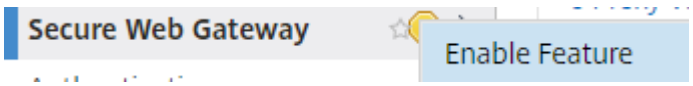



En Dirección IP de subred, introduzca una dirección IP y una máscara de subred. La marca de verificación en un círculo verde indica que el valor está configurado.

4. En **Nombre de host**, **Dirección IP DNS y Zona horaria**, agregue la dirección IP de un servidor DNS para resolver nombres de dominio y especifique la zona horaria.
5. Haga clic en **Continuar**.
6. (Opcional) Es posible que vea un signo de exclamación, como se indica a continuación:




Esta marca indica que la función no está habilitada. Para habilitar la función, haga clic con el botón secundario en la función y, a continuación, haga clic en **Habilitar**




7. En el panel de navegación, haga clic en **Secure Web Gateway**. En **Introducción**, haga clic en **Asistente para puerta de Secure Web Gateway**.


8. Siga los pasos del asistente para configurar la implementación.

### Agregar una directiva de escucha al servidor proxy transparente

1. Vaya a **Secure Web Gateway** > **Servidores proxy**. Seleccione el servidor proxy transparente y haga clic en **Modificar**.
2. Modifique **la configuración básica** y haga clic en **Más**.
3. En **Prioridad de escucha**, escriba 1.
4. En **Expresión de directiva de escucha**, escriba la siguiente expresión:

```
(CLIENT.TCP.DSTPORT.EQ(80)||CLIENT.TCP.DSTPORT.EQ(443))
<!--NeedCopy-->
```

   Esta expresión asume puertos estándar para el tráfico HTTP y HTTPS. Si ha configurado puertos diferentes, por ejemplo 8080 para HTTP o 8443 para HTTPS, modifique la expresión para reflejar esos puertos.

### Limitaciones

SWG no se admite en una configuración de clúster, en particiones de administración y en un dispositivo FIPS de Citrix ADC.

## Introducción a una instancia SWG en un dispositivo Citrix ADC SDX

April 27, 2021

El dispositivo Citrix ADC SDX es una plataforma multiarrendatario en la que puede aprovisionar y administrar varias instancias de Citrix ADC. El dispositivo SDX aborda los requisitos de informática en la nube y de multiarrendamiento al permitir a un único administrador configurar y administrar el dispositivo y delegar la administración de cada instancia alojada en los arrendatarios. El dispositivo SDX permite al administrador del dispositivo proporcionar a cada arrendatario las siguientes ventajas. Se dan a continuación:

- Una instancia completa. Cada instancia tiene los siguientes privilegios:
  - Recursos de memoria y CPU dedicados
  - Un espacio separado para entidades
  - La independencia para ejecutar el lanzamiento y la construcción de su elección
  - Independencia del ciclo de vida
- Una red completamente aislada. El tráfico destinado a una instancia en particular se envía solo a esa instancia.

Si aún no ha instalado el dispositivo Citrix ADC SDX, consulte Instalación de hardware para obtener información sobre la instalación del dispositivo.

Debe utilizar el servicio de administración para realizar la configuración inicial del dispositivo Citrix ADC SDX. Para obtener más información, consulte Introducción a la interfaz de usuario de Management Service.

Puede aprovisionar instancias de Citrix SWG en el dispositivo Citrix ADC SDX de la misma manera que aprovisionaría una instancia de Citrix ADC VPX. Para aprovisionar una instancia SWG en un dispositivo SDX, debe instalar una licencia "SDX: 10K sesiones simultáneas SWG add-on pack". Esta licencia es similar a los paquetes de instancias SDX para VPX, pero es exclusiva de las instancias SWG. Para obtener más información sobre el aprovisionamiento de instancias de Citrix ADC, consulte Aprovisionar instancias de Citrix ADC.

Para configurar la instancia de Citrix SWG para que reciba tráfico, siga las instrucciones indicadas en Introducción a un dispositivo Citrix SWG.

## Modos de proxy

April 27, 2021

El dispositivo Citrix Secure Web Gateway (SWG) actúa como proxy de cliente para conectarse a Internet y aplicaciones SaaS. Como proxy, acepta todo el tráfico y determina el protocolo del tráfico. A menos que el tráfico sea HTTP o SSL, se reenvía al destino tal como está. Cuando el dispositivo recibe una solicitud de un cliente, intercepta la solicitud y realiza algunas acciones, como la autenticación de usuarios, la categorización de sitios y la redirección. Utiliza directivas para determinar qué tráfico permitir y qué tráfico bloquear.

El dispositivo mantiene dos sesiones diferentes, una entre el cliente y el proxy y la otra entre el proxy y el servidor de origen. El proxy se basa en directivas definidas por el cliente para permitir o bloquear el tráfico HTTP y HTTPS. Por lo tanto, es importante que defina directivas para eludir los datos confidenciales, como la información financiera. El dispositivo ofrece un amplio conjunto de atributos de tráfico de capa 4 a capa 7 y atributos de identidad de usuario para crear directivas de administración de tráfico.

Para el tráfico SSL, el proxy verifica el certificado del servidor de origen y establece una conexión legítima con el servidor. A continuación, emula el certificado del servidor, lo firma con un certificado de CA instalado en Citrix SWG y presenta el certificado de servidor creado al cliente. Debe agregar el certificado de CA como certificado de confianza al explorador del cliente para que la sesión SSL se establezca correctamente.

El dispositivo admite modos proxy transparentes y explícitos. En el modo proxy explícito, el cliente

debe especificar una dirección IP en su explorador, a menos que la organización inserte la configuración en el dispositivo del cliente. Esta dirección es la dirección IP de un servidor proxy configurado en el dispositivo SWG. Todas las solicitudes del cliente se envían a esta dirección IP. Para proxy explícito, debe configurar un servidor virtual de conmutación de contenido de tipo PROXY y especificar una dirección IP y un número de puerto válido.

Proxy transparente, como su nombre lo indica, es transparente para el cliente. Es decir, es posible que los clientes no sean conscientes de que un servidor proxy está mediando sus solicitudes. El dispositivo SWG está configurado en una implementación en línea y acepta de forma transparente todo el tráfico HTTP y HTTPS. Para proxy transparente, debe configurar un servidor virtual de conmutación de contenido de tipo PROXY, con asteriscos (*) como dirección IP y puerto. Al utilizar el asistente Secure Web Gateway en la GUI, no es necesario especificar una dirección IP ni un puerto.

> **Nota**
>
> Para interceptar protocolos distintos de HTTP y HTTPS en modo proxy transparente, debe agregar una directiva de escucha y vincularla al servidor proxy.

### Configurar proxy de reenvío SSL mediante la CLI de Citrix SWG

En el símbolo del sistema, escriba:

```
add cs vserver <name> PROXY <ipaddress> <port>
<!--NeedCopy-->
```

**Argumentos**:

**Nombre**:

Nombre del servidor proxy. Debe comenzar con un carácter alfanumérico o de subrayado (_) ASCII y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), en (@), igual (=) y guión (-). No se puede cambiar después de crear el servidor virtual CS.

El siguiente requisito solo se aplica a la CLI:

Si el nombre incluye uno o más espacios, enciérrelo entre comillas dobles o simples (por ejemplo, “mi servidor”o “mi servidor”).

Este es un argumento obligatorio. Longitud máxima: 127

**Dirección IP**:

Dirección IP del servidor proxy.

**puerto**:

Número de puerto para el servidor proxy. Valor mínimo: 1

**Ejemplo de proxy explícito**:

```
add cs vserver swgVS PROXY 192.0.2.100 80
<!--NeedCopy-->
```

**Ejemplo de proxy transparente**:

```
add cs vserver swgVS PROXY * *
<!--NeedCopy-->
```

### Agregar una directiva de escucha al servidor proxy transparente mediante la GUI de Citrix SWG

1. Vaya a **Secure Web Gateway** > **Servidores proxy**. Seleccione el servidor proxy transparente y haga clic en **Modificar**.
2. Modifique **la configuración básica** y haga clic en **Más**.
3. En **Prioridad de escucha**, escriba 1.
4. En **Expresión de directiva de escucha**, escriba la siguiente expresión:

```
(CLIENT.TCP.DSTPORT.EQ(80)||CLIENT.TCP.DSTPORT.EQ(443))
<!--NeedCopy-->
```

> **Nota**
>
> Esta expresión asume puertos estándar para el tráfico HTTP y HTTPS. Si ha configurado puertos diferentes, por ejemplo 8080 para HTTP o 8443 para HTTPS, modifique la expresión anterior para especificar esos puertos.

## Intercepción SSL

April 27, 2021

Un dispositivo Citrix Secure Web Gateway (SWG) configurado para la intercepción SSL actúa como proxy. Puede interceptar y descifrar el tráfico SSL/TLS, inspeccionar la solicitud no cifrada y permitir que un administrador aplique las reglas de cumplimiento y las comprobaciones de seguridad. Intercepción SSL utiliza una directiva que especifica qué tráfico interceptar, bloquear o permitir. Por ejemplo, el tráfico hacia y desde sitios web financieros, como los bancos, no debe ser interceptado, pero se puede interceptar otro tráfico, y los sitios de la lista negra pueden identificarse y bloquearse. Citrix recomienda configurar una directiva genérica para interceptar tráfico y directivas más específicas para omitir parte del tráfico.

El cliente y el proxy Citrix SWG establecen un protocolo de enlace HTTPS/TLS. El proxy SWG establece otro protocolo de enlace HTTPS/TLS con el servidor y recibe el certificado del servidor. El proxy verifica el certificado del servidor en nombre del cliente y también comprueba la validez del certificado del servidor mediante el Protocolo de estado del certificado en línea (OCSP). Regenera el certificado de servidor, lo firma mediante la clave del certificado de CA instalado en el dispositivo y lo presenta al cliente. Por lo tanto, se utiliza un certificado entre el cliente y el dispositivo Citrix ADC, y otro certificado entre el dispositivo y el servidor back-end.

> **Importante**
>
> El certificado de CA que se utiliza para firmar el certificado de servidor debe estar preinstalado en todos los dispositivos cliente, de modo que el cliente confíe en el certificado de servidor regenerado.

Para el tráfico HTTPS interceptado, el servidor proxy SWG descifra el tráfico saliente, accede a la solicitud HTTP de texto claro y puede utilizar cualquier aplicación de Capa 7 para procesar el tráfico, por ejemplo, mirando la URL de texto sin formato y permitiendo o bloqueando el acceso sobre la base de la directiva corporativa y la reputación de URL. Si la decisión de directiva es permitir el acceso al servidor de origen, el servidor proxy reenvía la solicitud recifrada al servicio de destino (en el servidor de origen). El proxy descifra la respuesta del servidor de origen, accede a la respuesta HTTP de texto sin cifrar y, opcionalmente, aplica cualquier directiva a la respuesta. A continuación, el proxy vuelve a cifrar la respuesta y la reenvía al cliente. Si la decisión de directiva es bloquear la solicitud al servidor de origen, el proxy puede enviar una respuesta de error, como HTTP 403, al cliente.

Para realizar la interceptación SSL, además del servidor proxy configurado anteriormente, debe configurar lo siguiente en un dispositivo SWG:

- Perfil SSL
- Directiva SSL
- Almacén de certificados de CA
- Almacenamiento automático y almacenamiento en caché de errores SSL

## Perfil SSL

April 27, 2021

Un perfil SSL es una colección de configuraciones SSL, como cifrados y protocolos. Un perfil es útil si tiene una configuración común para diferentes servidores. En lugar de especificar la misma configuración para cada servidor, puede crear un perfil, especificar la configuración en el perfil y, a continuación, enlazar el perfil a diferentes servidores. Si no se crea un perfil SSL front-end personalizado, el perfil front-end predeterminado está enlazado a entidades del lado cliente. Este perfil le permite

configurar los parámetros para administrar las conexiones del lado del cliente. Para la intercepción SSL, debe crear un perfil SSL y habilitar la intercepción SSL (SSLi) en el perfil. Un grupo de cifrado predeterminado está enlazado a este perfil, pero puede configurar más cifrados para adaptarse a su implementación. Debe enlazar un certificado de CA SSLi a este perfil y, a continuación, enlazar el perfil a un servidor proxy. Para la interceptación SSL, los parámetros esenciales de un perfil son los que se utilizan para comprobar el estado OCSP del certificado del servidor de origen, activar la renegociación del cliente si el servidor de origen solicita la renegociación y verificar el certificado del servidor de origen antes de volver a utilizar la sesión SSL front-end. Debe utilizar el perfil backend predeterminado al comunicarse con los servidores de origen. Establezca los parámetros del lado del servidor, como conjuntos de cifrado, en el perfil de back-end predeterminado. No se admite un perfil de back-end personalizado.

Para ver ejemplos de la configuración SSL más utilizada, consulte "Perfil de muestra"al final de esta sección.

El soporte de cifrado/protocolo difiere en la red interna y externa. En las tablas siguientes, la conexión entre los usuarios y un dispositivo SWG es la red interna. La red externa se encuentra entre el dispositivo e Internet.

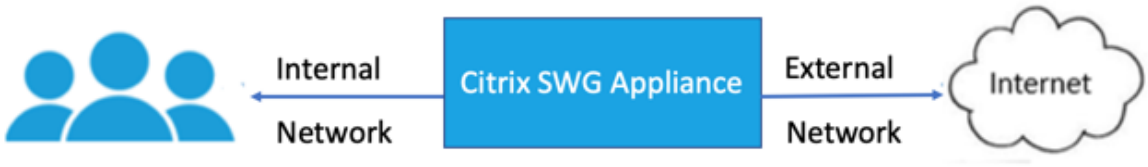



Tabla 1: Tabla de compatibilidad de cifrados/protocolos para la red interna

| (cifrado/protocolo) /Plataforma | MPX (N3) * | VPX |
|---|---|---|
| TLS 1.1/1.2 | 12,1 | 12,1 |
| ECDHE/DHE (Ejemplo TLS1-ECDHE-RSA-AES128-SHA) | 12,1 | 12,1 |
| AES-GCM (Ejemplo TLS1.2-AES128-GCM-SHA256) | 12,1 | 12,1 |
| Cifras SHA-2 (Ejemplo TLS1.2-AES-128-SHA256) | 12,1 | 12,1 |
| ECDSA (Ejemplo TLS1-ECDHE-ECDSA-AES256-SHA) | 12,1 | 12,1 |

Tabla 2: Tabla de compatibilidad de cifrados/protocolos para la red externa

| (cifrado/protocolo) /Plataforma | MPX (N3) * | VPX |
|---|---|---|
| TLS 1.1/1.2 | 12,1 | 12,1 |
| ECDHE/DHE (Ejemplo TLS1-ECDHE-RSA-AES128-SHA) | 12,1 | 12,1 |
| AES-GCM (Ejemplo TLS1.2-AES128-GCM-SHA256) | 12,1 | 12,1 |
| Cifras SHA-2 (Ejemplo TLS1.2-AES-128-SHA256) | 12,1 | 12,1 |
| ECDSA (Ejemplo TLS1-ECDHE-ECDSA-AES256-SHA) | 12,1 | No se admite |

* Utilice el comando **sh hardware** (show hardware) para identificar si el dispositivo tiene chips N3.

**Ejemplo**:

```
sh hardware

Platform: NSMPX-22000 16\*CPU+24\*IX+12\*E1K+2\*E1K+4*CVM N3 2200100

Manufactured on: 8/19/2013

CPU: 2900MHZ

Host Id: 1006665862

Serial no: ENUK6298FT

Encoded serial no: ENUK6298FT

Done
<!--NeedCopy-->
```

### Agregue un perfil SSL y habilite la intercepción SSL mediante la CLI de Citrix SWG

En el símbolo del sistema, escriba:

```
add ssl profile <name> -sslinterception ENABLED -ssliReneg ( ENABLED | DISABLED )-ssliOCSPCheck ( ENABLED | DISABLED )-ssliMaxSessPerServer <positive_integer>
```

**Argumentos**:

Intercepción**SSLIntercepción**:

Habilitar o inhabilitar la interceptación de sesiones SSL.

Valores posibles: ENABLED, DISABLED

Valor predeterminado: DISABLED

**SSLIreneg**:

Habilitar o inhabilitar la activación de la renegociación del cliente cuando se recibe una solicitud de renegociación del servidor de origen.

Valores posibles: ENABLED, DISABLED

Valor predeterminado: ENABLED

Comprobación**SSLIOCSPCheck**:

Habilitar o inhabilitar la comprobación de OCSP para un certificado de servidor de origen.

Valores posibles: ENABLED, DISABLED

Valor predeterminado: ENABLED

**sslimaxsessperServer**:

Número máximo de sesiones SSL que se almacenarán en caché por servidor de origen dinámico. Se crea una sesión SSL única para cada extensión SNI recibida del cliente en un mensaje de saludo de cliente. La sesión coincidente se utiliza para la reutilización de la sesión del servidor.

Valor predeterminado: 10

Valor mínimo: 1

Valor máximo: 1000

**Ejemplo**:

```
1  add ssl profile swg_ssl_profile  -sslinterception ENABLED
2
3  Done
4
5  sh ssl profile swg_ssl_profile
6
7  1)    Name: swg_ssl_profile (Front-End)
8
9                 SSLv3: DISABLED               TLSv1.0: ENABLED  TLSv1
                      .1: ENABLED  TLSv1.2: ENABLED
10
11                Client Auth: DISABLED
12
13                Use only bound CA certificates: DISABLED
14
15                Strict CA checks:                                NO
16
17                Session Reuse: ENABLED
                     Timeout: 120 seconds
18
```

```
19                  DH: DISABLED
20
21                  DH Private-Key Exponent Size Limit: DISABLED
                        Ephemeral RSA: ENABLED
                        Refresh Count: 0
22
23                  Deny SSL Renegotiation
                        ALL
24
25                  Non FIPS Ciphers: DISABLED
26
27                  Cipher Redirect: DISABLED
28
29                  SSL Redirect: DISABLED
30
31                  Send Close-Notify: YES
32
33                  Strict Sig-Digest Check: DISABLED
34
35                  Push Encryption Trigger: Always
36
37                  PUSH encryption trigger timeout:              1 ms
38
39                  SNI: DISABLED
40
41                  OCSP Stapling: DISABLED
42
43                  Strict Host Header check for SNI enabled SSL sessions:
                                NO
44
45                  Push flag:             0x0 (Auto)
46
47                  SSL quantum size:                             8 kB
48
49                  Encryption trigger timeout           100 mS
50
51                  Encryption trigger packet count:                45
52
53                  Subject/Issuer Name Insertion Format: Unicode
54
55                  SSL Interception: ENABLED
56
57                  SSL Interception OCSP Check: ENABLED
58
59                  SSL Interception End to End Renegotiation: ENABLED
60
61                  SSL Interception Server Cert Verification for Client
                        Reuse: ENABLED
62
63                  SSL Interception Maximum Reuse Sessions per Server:  10
64
65                  Session Ticket: DISABLED              Session Ticket
                        Lifetime: 300 (secs)
```

```
66
67                  HSTS: DISABLED
68
69                  HSTS IncludeSubDomains: NO
70
71                  HSTS Max-Age: 0
72
73                  ECC Curve: P_256, P_384, P_224, P_521
74
75 1)             Cipher Name: DEFAULT Priority :1
76
77                  Description: Predefined Cipher Alias
78
79 Done
80 <!--NeedCopy-->
```

### Enlazar un certificado de CA de interceptación SSL a un perfil SSL mediante la CLI de Citrix SWG

En el símbolo del sistema, escriba:

```
bind ssl profile <name> -ssliCACertkey <ssli-ca-cert >
```

**Ejemplo**:

```
1  bind ssl profile swg_ssl_profile -ssliCACertkey swg_ca_cert
2
3  Done
4
5  sh ssl profile swg_ssl_profile
6
7  1)             Name: swg_ssl_profile (Front-End)
8
9                   SSLv3: DISABLED               TLSv1.0: ENABLED  TLSv1
                       .1: ENABLED  TLSv1.2: ENABLED
10
11                  Client Auth: DISABLED
12
13                  Use only bound CA certificates: DISABLED
14
15                  Strict CA checks:                                 NO
16
17                  Session Reuse: ENABLED
                       Timeout: 120 seconds
18
19                  DH: DISABLED
20
21                  DH Private-Key Exponent Size Limit: DISABLED
                       Ephemeral RSA: ENABLED
                       Refresh Count: 0
22
```

```
23                  Deny SSL Renegotiation
                       ALL
24
25                  Non FIPS Ciphers: DISABLED
26
27                  Cipher Redirect: DISABLED
28
29                  SSL Redirect: DISABLED
30
31                  Send Close-Notify: YES
32
33                  Strict Sig-Digest Check: DISABLED
34
35                  Push Encryption Trigger: Always
36
37                  PUSH encryption trigger timeout:              1 ms
38
39                  SNI: DISABLED
40
41                  OCSP Stapling: DISABLED
42
43                  Strict Host Header check for SNI enabled SSL sessions:
                                NO
44
45                  Push flag:             0x0 (Auto)
46
47                  SSL quantum size:                             8 kB
48
49                  Encryption trigger timeout           100 mS
50
51                  Encryption trigger packet count:                45
52
53                  Subject/Issuer Name Insertion Format: Unicode
54
55                  SSL Interception: ENABLED
56
57                  SSL Interception OCSP Check: ENABLED
58
59                  SSL Interception End to End Renegotiation: ENABLED
60
61                  SSL Interception Server Cert Verification for Client
                       Reuse: ENABLED
62
63                  SSL Interception Maximum Reuse Sessions per Server:  10
64
65                  Session Ticket: DISABLED              Session Ticket
                       Lifetime: 300 (secs)
66
67                  HSTS: DISABLED
68
69                  HSTS IncludeSubDomains: NO
70
71                  HSTS Max-Age: 0
```

```
72
73                  ECC Curve: P_256, P_384, P_224, P_521
74
75 1)            Cipher Name: DEFAULT Priority :1
76
77                  Description: Predefined Cipher Alias
78
79 1)            SSL Interception CA CertKey Name: swg_ca_cert
80
81 Done
82 <!--NeedCopy-->
```

### Enlazar un certificado de CA de interceptación SSL a un perfil SSL mediante la GUI de Citrix SWG

1. Vaya a **Sistema** > **Perfiles** > **Perfil SSL**.
2. Haga clic en **Agregar**.
3. Especifique un nombre para el perfil.
4. Habilite la **intercepción de sesiones SSL**.
5. Haga clic en **OK**.
6. En **Configuración avanzada**, haga clic en **Clave de certificado**.
7. Especifique una clave de certificado de CA SSLi para enlazar al perfil.
8. Haga clic en **Seleccionar** y, a continuación, haga clic en **Vincular**.
9. Opcionalmente, configure los cifrados para que se adapten a su implementación.
    - Haga clic en el icono de edición y, a continuación, haga clic en **Agregar**.
    - Seleccione uno o más grupos de cifrado y haga clic en la flecha derecha.
    - Haga clic en **OK**.
10. Haga clic en **Done**.

### Enlazar un perfil SSL a un servidor proxy mediante la GUI de Citrix SWG

1. Desplácese hasta **Secure Web Gateway** > **Servidores proxy**y agregue un nuevo servidor o seleccione un servidor que desee modificar.
2. En **Perfil SSL**, haga clic en el icono de edición.
3. En la lista **Perfil SSL**, seleccione el perfil SSL que creó anteriormente.
4. Haga clic en **OK**.
5. Haga clic en **Done**.

**Perfil de muestra**:

```
Name: swg_ssl_profile (Front-End)

                SSLv3: DISABLED               TLSv1.0: ENABLED  TLSv1
                   .1: ENABLED  TLSv1.2: ENABLED

                Client Auth: DISABLED

                Use only bound CA certificates: DISABLED

                Strict CA checks:                                NO

                Session Reuse: ENABLED
                   Timeout: 120 seconds

                DH: DISABLED

                DH Private-Key Exponent Size Limit: DISABLED
                   Ephemeral RSA: ENABLED
                   Refresh Count: 0

                Deny SSL Renegotiation
                   ALL

                Non FIPS Ciphers: DISABLED

                Cipher Redirect: DISABLED

                SSL Redirect: DISABLED

                Send Close-Notify: YES

                Strict Sig-Digest Check: DISABLED

                Push Encryption Trigger: Always

                PUSH encryption trigger timeout:             1 ms

                SNI: DISABLED

                OCSP Stapling: DISABLED

                Strict Host Header check for SNI enabled SSL sessions:
                                        NO

                Push flag:             0x0 (Auto)

                SSL quantum size:                            8 kB

                Encryption trigger timeout           100 mS

                Encryption trigger packet count:               45

```

```
47                  Subject/Issuer Name Insertion Format: Unicode
48
49                  SSL Interception: ENABLED
50
51                  SSL Interception OCSP Check: ENABLED
52
53                  SSL Interception End to End Renegotiation: ENABLED
54
55                  SSL Interception Maximum Reuse Sessions per Server:  10
56
57                  Session Ticket: DISABLED              Session Ticket
                       Lifetime: 300 (secs)
58
59                  HSTS: DISABLED
60
61                  HSTS IncludeSubDomains: NO
62
63                  HSTS Max-Age: 0
64
65                  ECC Curve: P_256, P_384, P_224, P_521
66
67 1)             Cipher Name: DEFAULT Priority :1
68
69                  Description: Predefined Cipher Alias
70
71 1)             SSL Interception CA CertKey Name: swg_ca_cert
72 <!--NeedCopy-->
```

## Infraestructura de directivas SSL para interceptación SSL

April 27, 2021

Una directiva actúa como un filtro en el tráfico entrante. Las directivas del dispositivo Citrix Secure Web Gateway (SWG) ayudan a definir cómo administrar las conexiones y solicitudes con proxy. El procesamiento se basa en las acciones configuradas para esa directiva. Es decir, los datos de las solicitudes de conexión se comparan con una regla especificada en la directiva y la acción se aplica a las conexiones que coinciden con la regla (expresión). Después de definir una acción para la directiva y crear la directiva, enlazarla a un servidor proxy para que se aplique al tráfico que fluye a través de ese servidor proxy.

Una directiva SSL para intercepción SSL evalúa el tráfico entrante y aplica una acción predefinida a las solicitudes que coinciden con una regla (expresión). La decisión de interceptar, omitir o restablecer una conexión se toma en función de la directiva SSL definida. Puede configurar una de las tres acciones para una directiva: Intercepción, BYPASS o RESET. Especifique una acción al crear una directiva. Para poner en práctica una directiva, debe vincularla a un servidor proxy del dispositivo. Para especificar que una directiva está destinada a la interceptación SSL, debe especificar el tipo (punto

de enlace) como INTERCEPT_REQ cuando vincule la directiva a un servidor proxy. Al desvincular una directiva, debe especificar el tipo como INTERCEPT_REQ.

> **Nota**:
>
> El servidor proxy puede decidir interceptar solo si especifica una directiva.

La interceptación de tráfico puede basarse en cualquier atributo de enlace SSL. El más utilizado es el dominio SSL. El dominio SSL suele ser indicado por los atributos del protocolo de enlace SSL. Puede ser el valor del indicador de nombre del servidor extraído del mensaje de saludo del cliente SSL, si está presente, o el valor del nombre alternativo del servidor (SAN) extraído del certificado del servidor de origen. La directiva SSLi en Citrix SWG presenta un atributo especial denominado DETECTED_DOMAIN, que facilita a los clientes crear directivas de interceptación basadas en el dominio SSL desde el certificado del servidor de origen. El cliente puede hacer coincidir el nombre de dominio con una cadena, una lista de direcciones URL (conjunto de direcciones URL o `patset`) o una categoría de URL derivada del dominio.

### Crear una directiva SSL mediante la CLI de Citrix SWG

En el símbolo del sistema, escriba:

```
add ssl policy <name> -rule <expression> -action <string>
<!--NeedCopy-->
```

**Ejemplos**:

Los ejemplos siguientes son para directivas con expresiones que utilizan el atributo `detected_domain` para buscar un nombre de dominio.

No intercepte tráfico a una institución financiera, como XYZBANK

```
add ssl policy pol1 -rule client.ssl.detected_domain.contains("XYZBANK"
    ) -action BYPASS
<!--NeedCopy-->
```

No permita que un usuario se conecte a YouTube desde la red corporativa.

```
add ssl policy pol2 -rule client.ssl.client.ssl.detected_domain.
    url_categorize(0,0).category.eq ("YouTube") -action RESET
<!--NeedCopy-->
```

Interceptar todo el tráfico de usuario.

```
add ssl policy pol3 – rule true – action INTERCEPT
<!--NeedCopy-->
```

Si el cliente no quiere utilizar detected_domain, puede utilizar cualquiera de los atributos de enlace SSL para extraer e inferir el dominio.

Por ejemplo, no se encuentra un nombre de dominio en la extensión SNI del mensaje de saludo del cliente. El nombre de dominio debe tomarse del certificado del servidor de origen. Los ejemplos siguientes son para directivas con expresiones que comprueban si hay un nombre de dominio en el nombre del sujeto del certificado del servidor de origen.

Interceptar todo el tráfico de usuario a cualquier dominio de Yahoo.

```
1 add ssl policy pol4 -rule client.ssl.origin_server_cert.subject.
     contains("yahoo")  – action INTERCEPT
2 <!--NeedCopy-->
```

Intercepte todo el tráfico de usuarios de la categoría “Compras/Retail”.

```
1 add ssl policy pol_url_category -rule client.ssl.origin_server_cert.
     subject.URL_CATEGORIZE(0,0).CATEGORY.eq("Shopping/Retail") -action
     INTERCEPT
2 <!--NeedCopy-->
```

Intercepte todo el tráfico de usuario a una URL sin categoría.

```
1 add ssl policy pol_url_category -rule client.ssl.origin_server_cert.
     subject.url_categorize(0,0).category.eq("Uncategorized") -action
     INTERCEPT
2 <!--NeedCopy-->
```

Los siguientes ejemplos son para directivas que coinciden con el dominio con una entrada de un conjunto de direcciones URL.

Intercepte todo el tráfico de usuario si el nombre de dominio en SNI coincide con una entrada en el conjunto de URL “top100”.

```
1 add ssl policy pol_url_set  -rule client.ssl.client_hello.SNI.
     URLSET_MATCHES_ANY("top100") -action INTERCEPT
2 <!--NeedCopy-->
```

Intercepte todo el tráfico de usuario del nombre de dominio si el certificado del servidor de origen coincide con una entrada del conjunto de direcciones URL “top100”.

```
1 add ssl policy pol_url_set  -rule client.ssl.origin_server_cert.subject
     .URLSET_MATCHES_ANY("top100") -action INTERCEPT
2 <!--NeedCopy-->
```

### Crear una directiva SSL en un servidor proxy mediante la GUI SWG

1. Vaya a **Secure Web Gateway > SSL > Directivas**.
2. En la ficha **Directivas SSL**, haga clic en **Agregar** y especifique los siguientes parámetros:
   - Nombre de directiva
   - Acción de directiva: Seleccione entre interceptar, omitir o restablecer.

- Expresión

3. Haga clic en **Crear**.

### Enlazar una directiva SSL a un servidor proxy mediante la CLI SWG

En el símbolo del sistema, escriba:

```
bind ssl vserver <vServerName> -policyName <string> -priority <
    positive_integer> -type  INTERCEPT_REQ
<!--NeedCopy-->
```

**Ejemplo**:

```
bind ssl vserver <name> -policyName pol1 -priority 10 -type
    INTERCEPT_REQ
<!--NeedCopy-->
```

### Enlazar una directiva SSL a un servidor proxy mediante la GUI de Citrix SWG

1. Vaya a **Secure Web Gateway > Servidores virtuales proxy**.
2. Seleccione un servidor virtual y haga clic en **Modificar**.
3. En **Configuración avanzada**, haga clic en **Directivas SSL**.
4. Haga clic dentro del cuadro **Directiva SSL**.
5. En **Seleccionar directiva**, seleccione una directiva para enlazar.
6. En **Tipo**, seleccione **INTERCEPT_REQ**.
7. Haga clic en **Vincular** y, a continuación, haga clic en **Aceptar**.

### Desenlazar una directiva SSL a un servidor proxy mediante la línea de comandos

En el símbolo del sistema, escriba:

```
unbind ssl vserver <vServerName> -policyName <string> -type
    INTERCEPT_REQ
<!--NeedCopy-->
```

### Expresiones SSL utilizadas en directivas SSL para SWG

| Expresión | Descripción |
| --- | --- |
| `CLIENT.SSL.CLIENT_HELLO.SNI.*` | Devuelve la extensión SNI en un formato de cadena. Evalúe la cadena para ver si contiene el texto especificado. Ejemplo: Client.ssl.client_hello.sni.contains("xyz.com") |
| `CLIENT.SSL.ORIGIN_SERVER_CERT.*` | Devuelve un certificado, recibido de un servidor back-end, en un formato de cadena. Evalúe la cadena para ver si contiene el texto especificado. Ejemplo: Client.ssl.origin_server_cert.subject.contains("xyz.com") |
| `CLIENT.SSL.DETECTED_DOMAIN.*` | Devuelve un dominio, ya sea de la extensión SNI o del certificado del servidor de origen, en un formato de cadena. Evalúe la cadena para ver si contiene el texto especificado. Ejemplo: Client.ssl.detected_domain.contains("xyz.com") |

## Almacén de certificados de intercepción SSL

April 27, 2021

Un certificado SSL, que es una parte integral de cualquier transacción SSL, es un formulario de datos digitales (X509) que identifica a una empresa (dominio) o a un individuo. Una entidad emisora de certificados (CA) emite un certificado SSL. Una CA puede ser privada o pública. Las aplicaciones que llevan a cabo transacciones SSL confían en los certificados emitidos por las CA públicas, como Verisign. Estas aplicaciones mantienen una lista de CA en las que confían.

Como proxy de reenvío, un dispositivo Citrix Secure Web Gateway (SWG) realiza cifrado y descifrado del tráfico entre un cliente y un servidor. Actúa como un servidor para el cliente (usuario) y como un cliente para el servidor. Antes de que un dispositivo pueda procesar el tráfico HTTPS, debe validar la identidad de un servidor para evitar transacciones fraudulentas. Por lo tanto, como cliente del servidor de origen, el dispositivo debe comprobar el certificado del servidor de origen antes de aceptarlo. Para comprobar el certificado de un servidor, todos los certificados (por ejemplo, certificados raíz e intermedios) que se utilizan para firmar y emitir el certificado de servidor deben estar presentes en el dispositivo. Un conjunto predeterminado de certificados de CA está preinstalado en un dispositivo. Citrix SWG puede utilizar estos certificados para verificar casi todos los certificados

comunes del servidor de origen. Este conjunto predeterminado no se puede modificar. Sin embargo, si la implementación requiere más certificados de CA, puede crear un paquete de dichos certificados e importarlo al dispositivo. Un paquete también puede contener un solo certificado.

Al importar un paquete de certificados al dispositivo, el dispositivo descarga el paquete desde la ubicación remota y, tras comprobar que el paquete contiene solo certificados, lo instala en el dispositivo. Debe aplicar un paquete de certificados antes de poder utilizarlo para validar un certificado de servidor. También puede exportar un paquete de certificados para modificarlo o almacenarlo en una ubicación sin conexión como copia de seguridad.

### Importe y aplique un paquete de certificados de CA en el dispositivo mediante la CLI de Citrix SWG

En el símbolo del sistema, escriba:

```
1 import ssl certBundle <name> <src>
2 <!--NeedCopy-->
```

```
1 apply ssl certBundle <name>
2 <!--NeedCopy-->
```

```
1 show ssl certBundle
2 <!--NeedCopy-->
```

**ARGUMENTOS**:

**Nombre**:

Nombre que se va a asignar al paquete de certificados importados. Debe comenzar con un carácter alfanumérico o de subrayado (_) ASCII y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), en (@), igual (=) y guión (-). El siguiente requisito solo se aplica a la CLI:

Si el nombre incluye uno o más espacios, enciérrelo entre comillas dobles o simples (por ejemplo, “mi archivo”o “mi archivo”).

Longitud máxima: 31

**src**:

URL que especifica el protocolo, el host y la ruta de acceso, incluido el nombre de archivo, al paquete de certificados que se va a importar o exportar. Por ejemplo, `http://www.example.com/cert\\_bundle\\_file`.

**NOTA**: La importación falla si el objeto que se va a importar está en un servidor HTTPS que requiere autenticación de certificado de cliente para el acceso.

Longitud máxima: 2047

**Ejemplo**:

```
import ssl certbundle swg-certbundle http://www.example.com/cert_bundle
<!--NeedCopy-->
```

```
apply ssl certBundle swg-certbundle
<!--NeedCopy-->
```

```
show ssl certbundle

            Name : swg-certbundle(Inuse)

            URL : http://www.example.com/cert_bundle

    Done
<!--NeedCopy-->
```

### Importar y aplicar un paquete de certificados de CA en el dispositivo mediante la GUI de Citrix SWG

1. Vaya a **Secure Web Gateway** > **Introducción** > **Paquetes de certificados**.
2. Lleve a cabo una de las siguientes acciones:
   - Seleccione un paquete de certificados de la lista.
   - Para agregar un nuevo paquete de certificados, haga clic en “+”y especifique un nombre y una dirección URL de origen. Haga clic en **OK**.
3. Haga clic en **OK**.

### Quitar un paquete de certificados de CA del dispositivo mediante la CLI

En el símbolo del sistema, escriba:

```
remove certBundle <cert bundle name>
<!--NeedCopy-->
```

**Ejemplo**:

```
remove certBundle mytest-cacert
<!--NeedCopy-->
```

### Exportar un paquete de certificados de CA desde el dispositivo mediante la CLI de Citrix SWG

En el símbolo del sistema, escriba:

```
export certBundle <cert bundle name> <Path to export>
<!--NeedCopy-->
```

**ARGUMENTOS**:

**Nombre**:

Nombre que se va a asignar al paquete de certificados importados. Debe comenzar con un carácter alfanumérico o de subrayado (_) ASCII y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), en (@), igual (=) y guión (-). El siguiente requisito solo se aplica a la CLI:

Si el nombre incluye uno o más espacios, enciérrelo entre comillas dobles o simples (por ejemplo, "mi archivo"o "mi archivo").

Longitud máxima: 31

**src**:

URL que especifica el protocolo, el host y la ruta de acceso, incluido el nombre de archivo, al paquete de certificados que se va a importar o exportar. Por ejemplo, `http://www.example.com/cert\\_bundle\\_file`.

**NOTA**: La importación falla si el objeto que se va a importar está en un servidor HTTPS que requiere autenticación de certificado de cliente para el acceso.

Longitud máxima: 2047

**Ejemplo**:

```
export certBundle mytest-cacert http://192.0.2.20/
<!--NeedCopy-->
```

### Importar, aplicar y verificar un paquete de certificados de CA desde el almacén de certificados de CA de Mozilla

En el símbolo del sistema, escriba:

```
> import certbundle mozilla_public_ca https://curl.haxx.se/ca/cacert.
   pem
Done
<!--NeedCopy-->
```

Para aplicar el paquete, escriba:

```
> apply certbundle mozilla_public_ca
Done
<!--NeedCopy-->
```

Para verificar el paquete de certificados en uso, escriba:

```
> sh certbundle | grep mozilla
    Name : mozilla_public_ca (Inuse)
<!--NeedCopy-->
```

### Limitación

Los paquetes de certificados no se admiten en una instalación de clúster ni en un dispositivo con particiones.

## Error SSL autoaprendizaje

April 27, 2021

El dispositivo Citrix SWG agrega un dominio a la lista de omitir SSL si el modo de aprendizaje está activado. El modo de aprendizaje se basa en el mensaje de alerta SSL recibido de un cliente o de un servidor de origen. Es decir, el aprendizaje depende del cliente o servidor que envíe un mensaje de alerta. No se aprende si no se envía un mensaje de alerta. El dispositivo se entera de si se cumple alguna de las condiciones siguientes:

1. Se recibe una solicitud de certificado de cliente del servidor.
2. Se recibe una de las siguientes alertas como parte del apretón de manos:
    - CERTIFICADO BAD_
    - UNSUPPORTED_CERTIFICATE
    - CERTIFICATE_REVOCADO
    - CERTIFICATE_CADUCADO
    - CERTIFICATE_UNKNOWN
    - UNKNOWN_CA (Si un cliente utiliza anclar, envía este mensaje de alerta si recibe un certificado de servidor).
    - HANDSHAKE_FAILURE

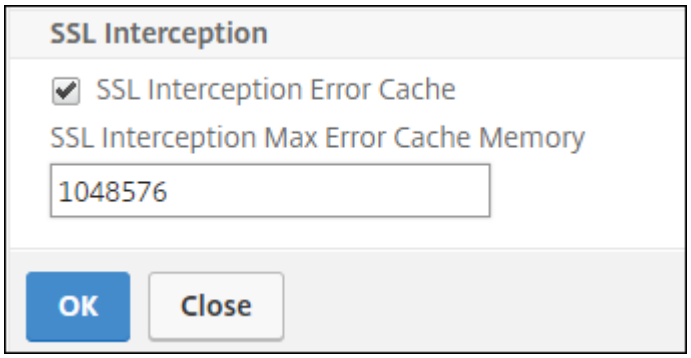
Para habilitar el aprendizaje, debe habilitar la caché de errores y especificar la memoria reservada para esto.

### Habilitar el aprendizaje mediante la GUI de Citrix SWG

1. Vaya a **Secure Web Gateway** > **SSL**.

2. En **Configuración**, haga clic en **Cambiar la configuración avanzada de SSL**.
3. En **Intercepción SSL**, seleccione **Caché de Error de Intercepción SSL**.
4. En **SSL Interception Max Error Cache Memory**, especifique la memoria (en bytes) que quiere reservar.




5. Haga clic en **OK**.

### Habilitar el aprendizaje mediante la CLI de Citrix SWG

En el símbolo del sistema, escriba:

```
set ssl parameter -ssliErrorCache ( ENABLED | DISABLED )-ssliMaxErrorCacheMem
 <positive_integer>
```

**Argumentos**:

**SSLIErrorCache**:

```
Habilite o inhabilite el aprendizaje dinámico y almacene en
    caché la información aprendida para tomar decisiones
    posteriores para interceptar u omitir solicitudes. Cuando
    se habilita, el dispositivo realiza una búsqueda en caché
    para decidir si se omite la solicitud.

Valores posibles: `ENABLED, DISABLED`

Valor predeterminado: `DISABLED`
```

**sslimaxErrorcachemem**:

```
Especifique la memoria máxima, en bytes, que se puede
    utilizar para almacenar en caché los datos aprendidos.
    Esta memoria se utiliza como caché LRU para que las
    entradas antiguas se sustituyan por entradas nuevas después
    de agotar el límite de memoria establecido. Un valor de
    0 decide el límite automáticamente.

Valor predeterminado: 0
```

```
4
5           Valor mínimo: 0
6
7           Valor máximo: 4294967294
```

## Gestión de la identidad del usuario

April 27, 2021

Un número cada vez mayor de infracciones de seguridad y la creciente popularidad de los dispositivos móviles han puesto de relieve la necesidad de garantizar que el uso de Internet externo se ajuste a las directivas corporativas y que solo los usuarios autorizados accedan a los recursos externos proporcionados por el personal corporativo. Identity Management lo hace posible verificando la identidad de una persona o un dispositivo. No determina qué tareas puede realizar el individuo ni qué archivos puede ver el individuo.

Una implementación Secure Web Gateway (SWG) identifica al usuario antes de permitir el acceso a Internet. Todas las solicitudes y respuestas del usuario son inspeccionadas. Se registra la actividad del usuario y los registros se exportan a Citrix Application Delivery Management (ADM) para generar informes. En Citrix ADM, puede ver las estadísticas sobre las actividades del usuario, las transacciones y el consumo de ancho de banda.

De forma predeterminada, solo se guarda la dirección IP del usuario, pero puede configurar el dispositivo Citrix SWG para que registre más detalles sobre el usuario y utilice esta información de identidad para crear directivas de uso de Internet más ricas para usuarios específicos.

El dispositivo Citrix ADC admite los siguientes modos de autenticación para una configuración de proxy explícito.

- **Protocolo ligero de acceso a directorios (LDAP)**. Autentica al usuario a través de un servidor de autenticación LDAP externo. Para obtener más información, consulte Directivas de autenticación LDAP.
- **RADIO**. Autentica al usuario a través de un servidor RADIUS externo. Para obtener más información, consulte Directivas de autenticación RADIUS.
- **TACACS+** Autentica al usuario a través de un servidor externo de autenticación del sistema de control de acceso de controlador de acceso de Terminal Access Controller (TACACS). Para obtener más información, consulte Directivas de autenticación.
- **Negociar**. Autentica al usuario a través de un servidor de autenticación Kerberos. Si hay un error en la autenticación Kerberos, el dispositivo utiliza la autenticación NTLM. Para obtener más información, consulte Negociar directivas de autenticación.

En el caso de proxy transparente, solo se admite actualmente la autenticación LDAP basada en IP. Cuando se recibe una solicitud de cliente, el proxy autentica al usuario comprobando una entrada para la dirección IP del cliente en el directorio activo y crea una sesión basada en la dirección IP del usuario. Sin embargo, si configura el atributo ssonameAttribute en una acción LDAP, se crea una sesión mediante el nombre de usuario en lugar de la dirección IP. Las directivas clásicas no se admiten para la autenticación en una configuración de proxy transparente.

> **Nota**
>
> Para proxy explícito, debe establecer el nombre de inicio de sesión LDAP en `sAMAccountName`. Para proxy transparente, debe establecer el nombre de inicio de sesión LDAP en `networkAddress` y `attribute1` en `sAMAccountName`.

**Ejemplo de proxy explícito**:

```
add authentication ldapAction swg-auth-action-explicit -serverIP
    10.105.157.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "
    CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
    freebsd123$ -ldapLoginName sAMAccountName
<!--NeedCopy-->
```

**Ejemplo de proxy transparente**:

```
add authentication ldapAction swg-auth-action-explicit -serverIP
    10.105.157.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "
    CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
    freebsd123$ -ldapLoginName networkAddress -authentication disable -
    Attribute1 sAMAccountName
<!--NeedCopy-->
```

### Configurar la autenticación de usuario mediante la CLI de Citrix SWG

En el símbolo del sistema, escriba:

```
add authentication vserver <vserver name> SSL

bind ssl vserver <vserver name> -certkeyName <certkey name>

add authentication ldapAction <action name> -serverIP <ip_addr> -
    ldapBase <string> -ldapBindDn <string> -ldapBindDnPassword -
    ldapLoginName <string>

add authentication Policy <policy name> -rule <expression> -action <
    string>

bind authentication vserver <vserver name> -policy <string> -priority <
    positive_integer>

```

```
set cs vserver <name> -authn401 ON -authnVsName <string>
<!--NeedCopy-->
```

**Argumentos**:

**Nombre del servidor virtual**:

Nombre del servidor virtual de autenticación al que se va a enlazar la directiva.

Longitud máxima: 127

**Tipo de servicio**:

Tipo de protocolo del servidor virtual de autenticación. Siempre SSL.

Valores posibles: SSL

Valor predeterminado: SSL

**Nombre de acción**:

Nombre de la nueva acción LDAP. Debe comenzar con una letra, un número o un carácter de subrayado (_) y debe contener solo letras, números y el guión (-), punto (.) libra (#), espacio (), en (@), igual (=), dos puntos (:) y caracteres de subrayado. No se puede cambiar después de agregar la acción LDAP. El siguiente requisito solo se aplica a la CLI:

Si el nombre incluye uno o más espacios, enciérrelo entre comillas dobles o simples (por ejemplo, "mi acción de autenticación"o "mi acción de autenticación").

Longitud máxima: 127

**ServerIP**:

Dirección IP asignada al servidor LDAP.

**LdapBase**:

Base (nodo) desde el que iniciar las búsquedas LDAP. Si el servidor LDAP se está ejecutando localmente, el valor predeterminado de base es dc=netscaler, dc=com. Longitud máxima: 127

**LDAPBindDN**:

Nombre completo (DN) que se utiliza para enlazar al servidor LDAP.

Valor predeterminado: `cn=Manager,dc=netscaler,dc=com`

Longitud máxima: 127

**ldapBinddnPassword**:

Contraseña utilizada para enlazar al servidor LDAP.

Longitud máxima: 127

**ldaploginName**:

Atributo de nombre de inicio de sesión LDAP. El dispositivo Citrix ADC utiliza el nombre de inicio de sesión LDAP para consultar servidores LDAP externos o Active Directories. Longitud máxima: 127

**Nombre de la directiva**:

Nombre de la directiva de autenticación avanzada. Debe comenzar con una letra, un número o un carácter de subrayado (_) y debe contener solo letras, números y el guión (-), punto (.) libra (#), espacio (), en (@), igual (=), dos puntos (:) y caracteres de subrayado. No se puede cambiar después de crear la directiva AUTENTICACIÓN. El siguiente requisito solo se aplica a la CLI:

Si el nombre incluye uno o más espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, "mi directiva de autenticación"o "mi directiva de autenticación").

Longitud máxima: 127

**regla**:

Nombre de la regla, o una expresión de sintaxis predeterminada, que la directiva utiliza para determinar si se intenta autenticar al usuario con el servidor AUTENTICACIÓN.

Longitud máxima: 1499

**acción**:

Nombre de la acción de autenticación que se va a realizar si la directiva coincide.

Longitud máxima: 127

**prioridad**:

Entero positivo que especifica la prioridad de la directiva. Un número inferior especifica una prioridad más alta. Las directivas se evalúan en el orden de sus prioridades y se aplica la primera directiva que coincide con la solicitud. Debe ser único dentro de la lista de directivas enlazadas al servidor virtual de autenticación.

Valor mínimo: 0

Valor máximo: 4294967295

**Ejemplo**:

```
add authentication vserver swg-auth-vs SSL

Done

bind ssl vserver explicit-auth-vs -certkeyName ns-swg-ca-certkey

Done

add authentication ldapAction swg-auth-action-explicit -serverIP
    192.0.2.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "CN=
    Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword zzzzz
     -ldapLoginName sAMAccountName
```

```
10
11 Done
12
13 add authenticationpolicy swg-auth-policy -rule true -action swg-auth-
      action-explicit

      Done
14
15 bind authentication vserver swg-auth-vs -policy swg-auth-policy -
      priority 1
16
17 Done
18
19 set cs vserver testswg -authn401 ON -authnVsName swg-auth-vs
20
21 Done
22 <!--NeedCopy-->
```

### Habilitar el registro de nombres de usuario mediante la CLI de Citrix SWG

En el símbolo del sistema, escriba:

```
1 set appflow param -AAAUserName ENABLED
2 <!--NeedCopy-->
```

**Argumentos**:

`AAAUserName`

Habilitar el registro de nombres de usuario de AppFlow AAA.

Valores posibles:`ENABLED`, `DISABLED`

Valor predeterminado: `DISABLED`

**Ejemplo**:

```
1 set appflow param -AAAUserName ENABLED
2 <!--NeedCopy-->
```

## Filtrado de URL

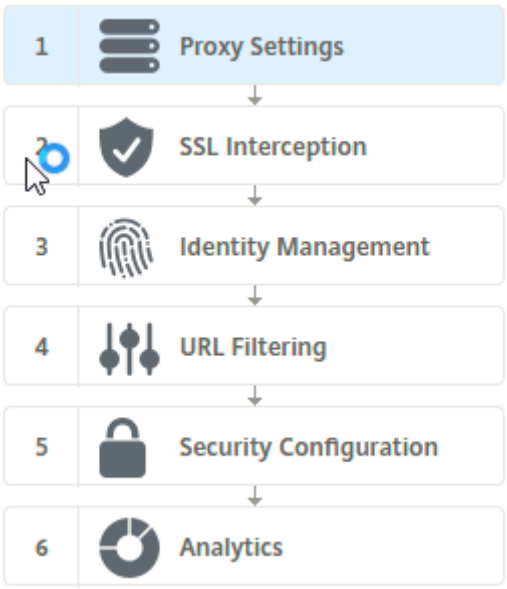
April 27, 2021

El filtrado de URL proporciona un control basado en directivas de sitios web mediante el uso de la información contenida en las URL. Esta función ayuda a los administradores de red a supervisar y controlar el acceso de los usuarios a sitios web maliciosos de la red.

## Introducción

Si es un usuario nuevo y desea configurar el filtrado de URL, debe completar la configuración SWG inicial. Para comenzar con el filtrado de URL, primero debe iniciar sesión en el asistente de Citrix SWG. El asistente le guiará por una serie de pasos de configuración antes de aplicar las directivas de filtrado de URL.




> **Nota**
>
> Antes de comenzar, asegúrese de que tiene instalada una licencia válida de función de URL Threat Intelligence en el dispositivo. Si utiliza una versión de prueba, asegúrese de adquirir una licencia válida para seguir mediante esta función en el dispositivo SWG.

### Iniciar sesión en el asistente SWG

El asistente de Citrix SWG le guía a través de una serie de tareas de configuración simplificadas y el panel derecho muestra la secuencia de flujo correspondiente. Puede utilizar este asistente para aplicar directivas de filtrado de URL a una lista de direcciones URL o a una lista predefinida de categorías.

### Paso 1: Configurar la configuración del proxy

Primero debe configurar un servidor proxy a través del cual el cliente accede a la puerta de enlace SWG. Este servidor es de tipo SSL, y funciona en modo explícito o transparente. Para obtener más información acerca de la configuración del servidor proxy, consulte Modos de proxy.

#### Paso 2: Configurar la intercepción SSL

Después de configurar el servidor proxy, debe configurar el proxy de intercepción SSL para interceptar el tráfico cifrado en el dispositivo Citrix SWG. En el caso del filtrado de URL, el proxy SSL intercepta el tráfico y bloquea la URL en la lista negra mientras que el resto del tráfico se puede omitir. Para obtener más información acerca de cómo configurar la intercepción SSL, consulte Intercepción SSL.

#### Paso 3: Configurar la administración de identidades

Un usuario se autentica antes de que se le permita iniciar sesión en la red empresarial. La autenticación proporciona la flexibilidad necesaria para definir directivas específicas para un usuario o un grupo de usuarios, en función de sus funciones. Para obtener más información acerca de la autenticación de usuarios, consulte Administración de identificación de usuario

#### Paso 4: Configurar el filtrado de URL

El administrador puede aplicar una directiva de filtrado de URL mediante la función Categorización de URL o mediante la función Lista de URL.

Categorización de URL. Controla el acceso a sitios web y páginas web filtrando el tráfico sobre la base de una lista predefinida de categorías.

Lista de URL. Controla el acceso a sitios web y páginas web de la lista negra denegando el acceso a direcciones URL que se encuentren en un conjunto de direcciones URL importadas en el dispositivo.

#### Paso 5: Configurar la configuración de seguridad

Este paso le permite configurar una puntuación de reputación y permitir a los usuarios controlar el acceso a los sitios web denegando el acceso si la puntuación es demasiado baja. Su puntuación de reputación puede variar de uno a cuatro, y puede configurar el umbral en el que la puntuación se vuelve inaceptable. Para puntuaciones que superen el umbral, puede seleccionar una acción de directiva para permitir, bloquear o redirigir el tráfico. Para obtener más información, consulte Configuración de seguridad.

#### Paso 6: Configurar análisis SWG

Este paso le permite activar el análisis SWG para categorizar el tráfico web, registrar la categoría URL en los registros de transacciones de usuario y ver análisis de tráfico. Para obtener más información acerca de SWG Analytics, consulte Analytics.

**Paso 7: Haga clic en Listo para completar la configuración inicial y continuar administrando la configuración de filtrado de URL**

# Lista de URL

April 27, 2021

La función Lista de URL permite a los clientes empresariales controlar el acceso a sitios web específicos y categorías de sitios web. La función filtra sitios web aplicando una directiva de respuesta vinculada a un algoritmo de coincidencia de URL. El algoritmo hace coincidir la URL entrante con un conjunto de URL que consta de hasta un millón (1.000.000) de entradas. Si la solicitud de dirección URL entrante coincide con una entrada del conjunto, el dispositivo utiliza la directiva de respuesta para evaluar la solicitud (HTTP/HTTPS) y controlar el acceso a ella.

## Tipos de conjuntos de direcciones URL

Cada entrada de un conjunto de URL puede incluir una URL y, opcionalmente, sus metadatos (categoría de URL, grupos de categorías o cualquier otro dato relacionado). Para las direcciones URL con metadatos, el dispositivo utiliza una expresión de directiva que evalúa los metadatos. Para obtener más información, consulte Conjunto de URL.

Citrix SWG admite conjuntos de URL personalizados. También puede utilizar conjuntos de patrones para filtrar las URL.

**Conjunto de URL personalizado.** Puede crear un conjunto de direcciones URL personalizado con un máximo de 1.000.000 entradas de URL e importarlo como archivo de texto en el dispositivo.

**Juego de patrones.** Un dispositivo SWG puede utilizar conjuntos de patrones para filtrar direcciones URL antes de conceder acceso a sitios web. Un conjunto de patrones es un algoritmo de coincidencia de cadenas que busca una coincidencia exacta de cadenas entre una URL entrante y hasta 5000 entradas. Para obtener más información, consulte Conjunto de patrones.

Cada URL de un conjunto de URL importado puede tener una categoría personalizada en forma de metadatos de URL. Su organización puede alojar el conjunto y configurar el dispositivo SWG para que actualice periódicamente el conjunto sin necesidad de intervención manual.

Una vez actualizado el conjunto, el dispositivo Citrix ADC detecta automáticamente los metadatos y la categoría está disponible como expresión de directiva para evaluar la dirección URL y aplicar una acción como permitir, bloquear, redirigir o notificar al usuario.

### Expresiones de directiva avanzadas utilizadas con conjuntos de direcciones URL

En la tabla siguiente se describen las expresiones básicas que puede utilizar para evaluar el tráfico entrante.

1. `.URLSET_MATCHES_ANY`: Evalúa `TRUE` si la URL coincide exactamente con cualquier entrada en el conjunto de URL.
2. `.GET_URLSET_METADATA()`: La expresión `GET_URLSET_METADATA()` devuelve los metadatos asociados si la URL coincide exactamente con cualquier patrón dentro del conjunto de URL. Se devuelve una cadena vacía si no hay coincidencia.
3. `.GET_ URLSET_METADATA().EQ(<METADATA)- .GET_ URLSET_METADATA().EQ (<METADATA)`
4. `.GET_URLSET_METADATA ().TYPECAST_LIST_T(',').GET(0).EQ()`: Evalúa `TRUE` si los metadatos coincidentes se encuentran al principio de la categoría. Este patrón se puede utilizar para codificar campos separados dentro de los metadatos, pero solo coinciden con el primer campo.
5. `HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL)`: Se une a los parámetros host y URL, que luego se puede utilizar como un para la coincidencia.

### Tipos de acción del respondedor

> **Nota:** En la tabla, `HTTP.REQ.URL` se generaliza como `<URL expression>`.

En la tabla siguiente se describen las acciones que se pueden aplicar al tráfico entrante de Internet.

| Acción del Respondedor | Descripción |
|---|---|
| Permitir | Permitir que la solicitud acceda a la URL de destino. |
| Redirigir | Redirigir la solicitud a la URL especificada como destino. |
| Bloquear | Denegar la solicitud. |

### Requisitos previos

Debe configurar un servidor DNS si importa un conjunto de direcciones URL desde una dirección URL de nombre de host. Esto no es necesario si utiliza una dirección IP.

En el símbolo del sistema, escriba:

```
add dns nameServer ((<IP> [-local])| <dnsVserverName>)[-state (
ENABLED | DISABLED )] [-type <type>] [-dnsProfileName <string>]
```

**Ejemplo**:

```
add dns nameServer 10.140.50.5
```

## Configurar una lista de direcciones URL

Para configurar una lista de direcciones URL, puede utilizar el asistente de Citrix SWG o la interfaz de línea de comandos (CLI) de Citrix ADC. En el dispositivo Citrix SWG, primero debe configurar la directiva de respuesta y, a continuación, enlazar la directiva a un conjunto de direcciones URL.

Citrix recomienda utilizar el asistente de Citrix SWG como opción preferida para configurar una lista de direcciones URL. Utilice el asistente para enlazar una directiva de respondedor a un conjunto de direcciones URL. Alternativamente, puede enlazar la directiva a un conjunto de patrones.

### Configurar una lista de direcciones URL mediante el asistente Citrix SWG

Para configurar la lista de direcciones URL para el tráfico HTTPS mediante la GUI de Citrix SWG:

1. Inicie sesión en el dispositivo Citrix SWG y vaya a la página **Secured Web Gateway**.
2. En el panel de detalles, realice una de las acciones siguientes:
    a) Haga clic en **Asistente para puerta de enlace web segura** para crear una nueva configuración SWG con la función Lista de direcciones URL.
    b) Seleccione una configuración existente y haga clic en **Modificar**.
3. En la sección **Filtrado de URL**, haga clic en **Modificar**.
4. Active la casilla **Lista de direcciones URL** para habilitar la función.
5. Seleccione una directiva de **lista de direcciones URL** y haga clic en **Enlazar**.
6. Haga clic en **Continuar** y, a continuación, en **Listo**.

Para obtener más información, consulte Cómo crear una directiva de lista de direcciones URL.

### Configurar una lista de direcciones URL mediante la CLI de Citrix SWG

Para configurar una lista de direcciones URL, haga lo siguiente.

1. Configure un servidor virtual proxy para el tráfico HTTP y HTTPS.
2. Configure la intercepción SSL para interceptar el tráfico HTTPS.
3. Configure una lista de direcciones URL que contenga un conjunto de direcciones URL para el tráfico HTTP.
4. Configure la lista de direcciones URL que contiene el conjunto de direcciones URL para el tráfico HTTPS.
5. Configure un conjunto de direcciones URL privadas.

> **Nota**
>
> Si ya ha configurado un dispositivo SWG, puede omitir los pasos 1 y 2 y configurarlo con el paso 3.

**Configuración de un servidor virtual proxy para el tráfico de Internet** El dispositivo Citrix SWG admite servidores virtuales proxy transparentes y explícitos. Para configurar un servidor virtual proxy para el tráfico de Internet en modo explícito, haga lo siguiente:

1. Agregue un servidor virtual SSL proxy.
2. Enlazar una directiva de respondedor al servidor virtual proxy.

Para agregar un servidor virtual proxy mediante la CLI de Citrix SWG:

En el símbolo del sistema, escriba:

```
add cs vserver <name> <serviceType> <IPAddress> <port>
<!--NeedCopy-->
```

**Ejemplo**:

```
add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180
<!--NeedCopy-->
```

Para enlazar una directiva de respuesta a un servidor virtual proxy mediante la CLI de Citrix SWG:

```
bind ssl vserver <vServerName> -policyName <string> [-priority <
   positive_integer>]
<!--NeedCopy-->
```

> **Nota**
>
> Si ya ha configurado el interceptor SSL como parte de la configuración de Citrix SWG, puede omitir el siguiente procedimiento.

**Configurar la intercepción SSL para el tráfico HTTPS** Para configurar la intercepción SSL para el tráfico HTTPS, haga lo siguiente:

1. Enlazar un par de claves de certificado de CA al servidor virtual proxy.
2. Habilite el perfil SSL predeterminado.
3. Cree un perfil SSL front-end y enlaza al servidor virtual proxy y habilite la interceptación SSL en el perfil SSL front-end.

Para enlazar un par de claves de certificación de CA al servidor virtual proxy mediante la CLI de Citrix SWG:

En el símbolo del sistema, escriba:

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName>
<!--NeedCopy-->
```

Para configurar un perfil SSL front-end mediante la CLI de Citrix SWG:

En el símbolo del sistema, escriba:

```
set ssl parameter -defaultProfile ENABLED

add ssl profile <name> -sslInterception ENABLED -ssliMaxSessPerServer <
   positive_integer>
<!--NeedCopy-->
```

Para enlazar un perfil SSL front-end a un servidor virtual proxy mediante la CLI de Citrix SWG

En el símbolo del sistema, escriba:

```
set ssl vserver <vServer name>  -sslProfile <name>
<!--NeedCopy-->
```

**Configurar una lista de direcciones URL importando un conjunto de direcciones URL para el tráfico HTTP** Para obtener información acerca de cómo configurar un conjunto de direcciones URL para el tráfico HTTP, consulte Conjunto de URL.

**Realizar coincidencia explícita de subdominio** Ahora puede realizar una coincidencia explícita de subdominio para un conjunto de direcciones URL importadas. Para hacer esto, se agrega un nuevo parámetro, "SubDomainExactMatch"al comando **`import`** `policy URLset`.

Al habilitar el parámetro, el algoritmo de filtrado de URL realiza una coincidencia explícita de subdominio. Por ejemplo, si la dirección URL entrante es `news.example.com` y si la entrada del conjunto de direcciones URL es `example.com`, el algoritmo no coincide con las direcciones URL.

En el símbolo del sistema, escriba:

```
import policy urlset <name> [-overwrite] [-delimiter <character>][-
rowSeparator <character>] -url [-interval <secs>] [-privateSet][-
subdomainExactMatch] [-canaryUrl <URL>]
```

**Ejemplo**

```
import policy urlset test -url http://10.78.79.80/top-1k.csv -privateSet
 -subdomainExactMatch -interval 900
```

**Configurar un conjunto de direcciones URL para el tráfico HTTPS** Para configurar un conjunto de URL para el tráfico HTTPS mediante la CLI de Citrix SWG

En el símbolo del sistema, escriba:

```
add ssl policy <name> -rule <expression> -action <string> [-undefAction
    <string>] [-comment <string>]
<!--NeedCopy-->
```

**Ejemplo**:

```
add ssl policy pol1 -rule "client.ssl.client_hello.SNI.
   URLSET_MATCHES_ANY("top1m") -action INTERCEPT
<!--NeedCopy-->
```

**Para configurar un conjunto de direcciones URL para el tráfico HTTPS mediante el asistente de Citrix SWG** Citrix recomienda utilizar el asistente de Citrix SWG como opción preferida para configurar una lista de direcciones URL. Utilice el asistente para importar un conjunto de direcciones URL personalizado y enlazar a una directiva de respondedor.

1. Inicie sesión en el dispositivo **Citrix SWG** y vaya a **Secured Web Gateway > Filtrado de URL > Listas de URL**.
2. En el panel de detalles, haga clic en **Agregar.**
3. En la página **Directiva de lista de direcciones URL**, especifique el nombre de la directiva.
4. Seleccione una opción para importar un conjunto de direcciones URL.
5. En la página de separador **Directiva de lista de direcciones** URL, active la casilla de verificación **Importar conjunto de direcciones URL** y especifique los siguientes parámetros de conjunto de direcciones URL.

    a) Nombre de conjunto de direcciones URL: Nombre del conjunto de direcciones URL personalizado.
    b) URL: Dirección web de la ubicación en la que se accede al conjunto de direcciones URL.
    c) Sobrescribir (Overwrite): Sobrescribir un conjunto de direcciones URL importado previamente.
    d) Delimitador: Secuencia de caracteres que delimita un registro de archivo CSV.
    e) Separador de filas: Separador de filas utilizado en el archivo CSV.
    f) Intervalo: Intervalo en segundos, redondeado al número de segundos más cercano igual a 15 minutos, en el que se actualiza el conjunto de direcciones URL.
    g) Conjunto privado: Opción para impedir la exportación del conjunto de direcciones URL.
    h) URL Canary: URL interna para comprobar si el contenido del conjunto de URL debe mantenerse confidencial. La longitud máxima de la URL es de 2047 caracteres.

6. Seleccione una acción de respuesta en la lista desplegable.
7. Haga clic en **Crear** y **cerrar**.

**Configurar un conjunto de direcciones URL privadas** Si configura un conjunto de direcciones URL privadas y mantiene su contenido confidencial, es posible que el administrador de red no conozca

las direcciones URL incluidas en la lista negra del conjunto. En estos casos, puede configurar una URL Canary y agregarla al conjunto de direcciones URL. Mediante la URL Canary, el administrador puede solicitar que se utilice el conjunto de direcciones URL privadas para cada solicitud de búsqueda. Puede consultar la sección del asistente para obtener descripciones de cada parámetro.

Para importar un conjunto de URL mediante la CLI de Citrix SWG:

En el símbolo del sistema, escriba:

```
1 import policy urlset <name> [-overwrite] [-delimiter <character>] [-
     rowSeparator <character>] -url <URL> [-interval <secs>] [-privateSet
     ] [-canaryUrl <URL>]
2 <!--NeedCopy-->
```

**Ejemplo**:

```
1 import policy urlset test1 –url http://10.78.79.80/alytra/top-1k.csv -
     private -canaryUrl http://www.in.gr
2 <!--NeedCopy-->
```

#### Mostrar conjunto de direcciones URL importadas

Ahora puede mostrar conjuntos de direcciones URL importados además de conjuntos de direcciones URL agregados. Para hacer esto, se agrega un nuevo parámetro "importado"al comando "show urlset". Si habilita esta opción, el dispositivo muestra todos los conjuntos de direcciones URL importados y distingue los conjuntos de direcciones URL importados de los conjuntos de direcciones URL agregados.

En el símbolo del sistema, escriba:

```
show policy urlset [<name>] [-imported]
```

**Ejemplo**

```
show policy urlset -imported
```

### Configurar la mensajería del registro de auditoría

El registro de auditoría le permite revisar una condición o una situación en cualquier fase del proceso de lista de direcciones URL. Cuando un dispositivo Citrix ADC recibe una dirección URL entrante, si la directiva de respondedor tiene una expresión avanzada de directiva de conjunto de direcciones URL, la función de registro de auditoría recopila información de conjunto de direcciones URL en la URL y almacena los detalles como un mensaje de registro para cualquier destino permitido por el registro de auditoría.

1. El mensaje de registro contiene la siguiente información:
2. Marca de tiempo.

3. Tipo de mensaje de registro.
4. Niveles de registro predefinidos (Crítico, Error, Aviso, Advertencia, Informativo, Depuración, Alerta y Emergencia).
5. Información de mensajes de registro, como el nombre de conjunto de direcciones URL, la acción de directiva o la dirección URL.

Para configurar el registro de auditoría para la función Lista de URL, debe completar las siguientes tareas:

1. Habilitar registros de auditoría.
2. Acción de mensaje Crear registro de auditoría.
3. Establecer la directiva de respuesta de lista de URL con la acción de mensaje Registro de auditoría.

Para obtener más información, consulte el tema Registro de auditoría.

## Semántica de patrones de URL

April 27, 2021

En la tabla siguiente se muestran los patrones de URL utilizados para especificar la lista de páginas que quiere filtrar. Por ejemplo, el patrón www.example.com/bar solo coincide con una página en www.example.com/bar. Para que coincidan todas las páginas cuya URL comience por 'www.example.com/bar', agregue un asterisco (*) al final de la URL.

### Semántica para el patrón de URL para que coincida con la asignación de metadatos

La semántica de coincidencia de patrones está disponible en formato de tabla. Para obtener más información, consulte la página PDF Semántica de patrones.

## Asignar categorías de URL

April 27, 2021

Una lista de categorías y grupos de categorías de terceros. Para obtener más información, consulte la página Asignación de categorías de URL.

# Caso de uso: Filtrado de URL mediante el uso de un conjunto de URL personalizado

April 27, 2021

Si es un cliente de empresa que busca una forma de controlar el acceso a sitios web y categorías de sitios web específicos, puede hacerlo mediante un conjunto de direcciones URL personalizado enlazado a una directiva de respuesta. La infraestructura de red de su organización puede utilizar un filtro de URL para bloquear el acceso a sitios web malintencionados o peligrosos, como sitios web con adultos, violencia, juegos, drogas, directivas o portales de empleo. Además de filtrar las direcciones URL, puede crear una lista personalizada de direcciones URL e importarla al dispositivo SWG. Por ejemplo, las directivas de su organización podrían requerir el bloqueo del acceso a determinados sitios web, como las redes sociales, los portales de compras y los portales de trabajo.

Cada URL de la lista puede tener una categoría personalizada en forma de metadatos. La organización puede alojar la lista de direcciones URL como una dirección URL establecida en el dispositivo Citrix SWG y configurar el dispositivo para que actualice periódicamente el conjunto sin necesidad de intervención manual.

Una vez actualizado el conjunto, el dispositivo Citrix ADC detecta automáticamente los metadatos y la directiva de respuesta utiliza los metadatos de URL (detalles de categoría) para evaluar la dirección URL entrante y aplicar una acción como permitir, bloquear, redirigir o notificar al usuario.

Para implementar esta configuración en la red, puede realizar las siguientes tareas:

1. Importar un conjunto de URL personalizado
2. Agregar un conjunto de URL personalizado
3. Configurar una lista de URL personalizada en el asistente de Citrix SWG

**Para importar un conjunto de URL personalizado mediante la CLI de Citrix SWG**:

En el símbolo del sistema, escriba:

**import policy urlset** <name> [**-overwrite**] [-**delimiter** <character>] [-**rowSeparator** <character>] -**url** <URL> [**-interval** <secs>] [**-privateSet**] [**-canaryUrl** <URL>]

```
importación de la directiva de urlset test1 ——url http://10.78.79.80/
    alytra/top-1k.csv
```

**Para agregar un conjunto de URL personalizado mediante la CLI de Citrix SWG**:

**En el símbolo del sistema, escriba:**

add urlset <urlset_name>

```
Add urlset test1
```

### Configurar una lista de direcciones URL mediante el asistente Citrix SWG

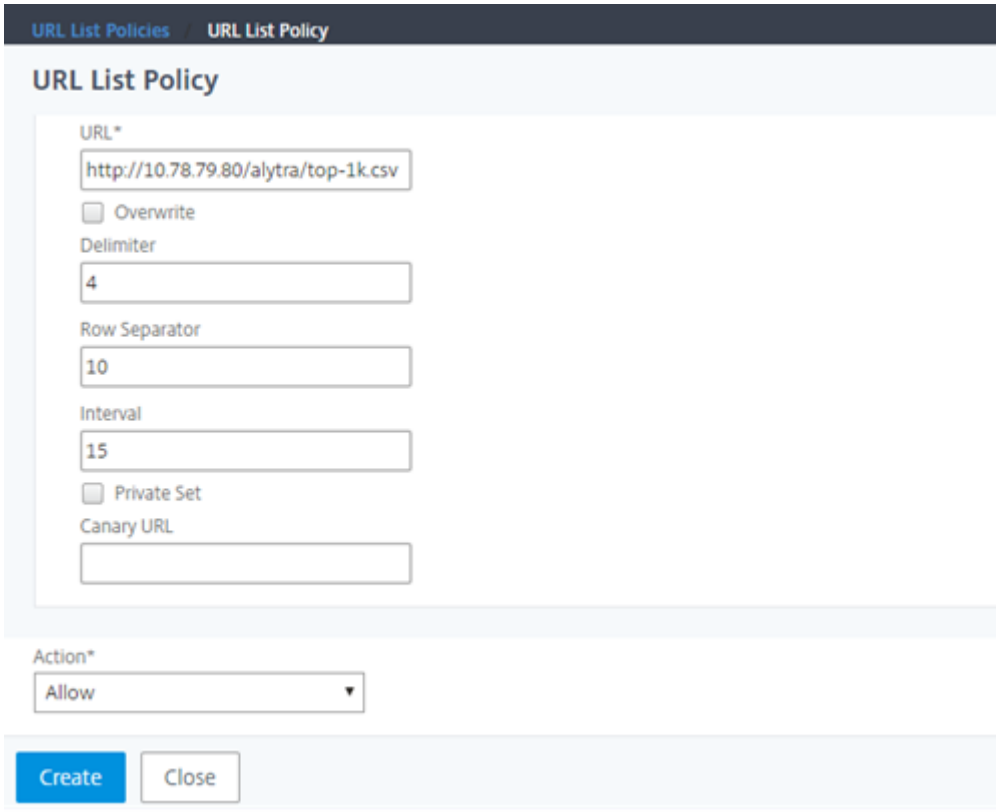
Citrix recomienda utilizar el asistente de Citrix SWG como opción preferida para configurar una lista de direcciones URL. Utilice el asistente para importar un conjunto de direcciones URL personalizado y vincularlo a una directiva de respuesta.

1. Inicie sesión en el dispositivo **Citrix SWG** y vaya a **Secured Web Gateway > Filtrado de URL > Listas de URL**.
2. En el panel de detalles, haga clic en **Agregar.**
3. En la página **Directiva de lista de direcciones URL**, especifique el nombre de la directiva.
4. Seleccione una opción para importar un conjunto de direcciones URL.
5. En la página de separador **Directiva de lista de direcciones** URL, active la casilla de verificación **Importar conjunto de direcciones URL** y especifique los siguientes parámetros de conjunto de direcciones URL.

    a) Nombre de conjunto de direcciones URL: Nombre del conjunto de direcciones URL personalizado.
    b) URL: Dirección web de la ubicación en la que se accede al conjunto de direcciones URL.
    c) Sobrescribir (Overwrite): Sobrescribir un conjunto de direcciones URL importado previamente.
    d) Delimitador: Secuencia de caracteres que delimita un registro de archivo CSV.
    e) Separador de filas: Separador de filas utilizado en el archivo CSV.
    f) Intervalo: Intervalo en segundos, redondeado a los 15 minutos más próximos, en los que se actualiza el conjunto de direcciones URL.
    g) Conjunto privado: Opción para impedir la exportación del conjunto de direcciones URL.
    h) Canary URL: URL interna para comprobar si el contenido del conjunto de URL debe mantenerse confidencial. La longitud máxima de la URL es de 2047 caracteres.

6. Seleccione una acción de respuesta en la lista desplegable.
7. Haga clic en **Crear** y **cerrar**.




### Semántica de metadatos para conjuntos de URL personalizados

Para importar un conjunto de direcciones URL personalizadas, agregue las direcciones URL a un archivo de texto y enlácelo a una directiva de respuesta para bloquear las direcciones URL de redes sociales.

Los siguientes son ejemplos de direcciones URL que puede agregar al archivo de texto:

cnn.com, Noticias

bbc.com, Noticias

google.com, motor de búsqueda

yahoo.com, motor de búsqueda

facebook.com, Redes sociales

twitter.com, Redes Sociales

### Configurar una directiva de respuesta para bloquear las direcciones URL de redes sociales mediante la CLI de Citrix ADC

**add responder action** act_url_unauthorized respondwith “‘HTTP/1.1 451 Unavailable For Legal Reasons\r\n\r\nURL is NOT authorized\n’”

**add responder policy** pol_url_meta_match ‘HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).GET_URLSET_META “u1”).EQ(“Social Media”)’act_url_meta_match

## Categorización de URL

April 27, 2021

La categorización de URL restringe el acceso de los usuarios a sitios web específicos y categorías de sitios web. Como servicio suscrito ofrecido por Citrix Secure Web Gateway (SWG), la función permite a los clientes empresariales filtrar el tráfico web mediante una base de datos de categorización comercial. La base de datos tiene un gran número (miles de millones) de URL clasificadas en diferentes categorías, como redes sociales, juegos de azar, contenido para adultos, nuevos medios de comunicación y compras. Además de la categorización, cada URL tiene una puntuación de reputación actualizada basada en el perfil de riesgo histórico del sitio. Para filtrar el tráfico, puede configurar directivas avanzadas basadas en categorías, grupos de categorías (como Terrorismo, Drogas ilegales) o puntuaciones de reputación del sitio.

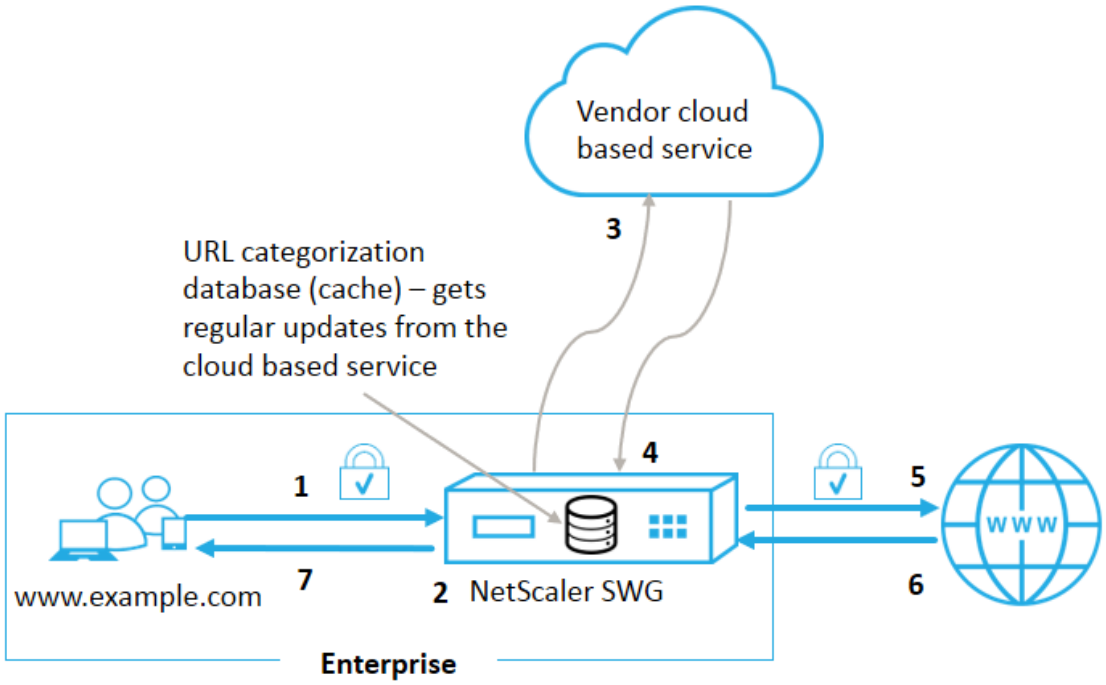
Por ejemplo, puede bloquear el acceso a sitios peligrosos, como sitios conocidos por estar infectados con malware, y restringir de forma selectiva el acceso a contenido como contenido para adultos o medios de transmisión de entretenimiento para usuarios empresariales. También puede capturar los detalles transaccionales del usuario y los detalles del tráfico saliente para supervisar el análisis del tráfico web en el servidor Citrix ADM.

Citrix ADC carga o descarga datos desde el `NetSTAR` dispositivo preconfigurado `nsv10.netstar-inc.com` y `incompasshybridpc.netstar-inc.com` se utiliza como host en la nube de forma predeterminada para las solicitudes de categorización de la nube. El dispositivo utiliza su dirección NSIP como dirección IP de origen y 443 como puerto de destino para la comunicación.

### Cómo funciona la categorización de URL

La siguiente figura muestra cómo se integra el servicio de categorización de URL de Citrix SWG con una base de datos comercial de categorización de URL y servicios en la nube para realizar actualizaciones frecuentes.




Los componentes interactúan de la siguiente manera:

1. Un cliente envía una solicitud de URL enlazada a Internet.
2. El proxy de Citrix SWG aplica una aplicación de directivas a la solicitud en función de los detalles de categoría (por ejemplo, categoría, grupo de categorías y puntuación de reputación de sitio) recuperados de la base de datos de categorización de URL. Si la base de datos devuelve los detalles de la categoría, el proceso salta al paso 5.
3. Si la base de datos no tiene los detalles de categorización, la solicitud se envía a un servicio de búsqueda basado en la nube mantenido por un proveedor de categorización de URL. Sin embargo, el dispositivo no espera una respuesta, sino que la dirección URL se marca como sin categoría y se realiza una aplicación de directivas (vaya al paso 5). El dispositivo continúa supervisando los comentarios de las consultas en la nube y actualiza la caché para que las futuras solicitudes puedan beneficiarse de la búsqueda en la nube.
4. El dispositivo SWG recibe los detalles de la categoría URL (categoría, grupo de categorías y puntuación de reputación) del servicio basado en la nube y los almacena en la base de datos de categorización.
5. La directiva permite la URL y la solicitud se envía al servidor de origen. De lo contrario, el dispositivo descarta, redirige o responde con una página HTML personalizada.
6. El servidor de origen responde con los datos solicitados al dispositivo SWG.
7. El dispositivo envía la respuesta al cliente.

### Caso de uso: Uso de Internet bajo cumplimiento corporativo para las empresas

Puede utilizar la función Filtrado de URL para detectar e implementar directivas de cumplimiento para bloquear sitios que infrinjan el cumplimiento corporativo. Estos pueden ser sitios como adultos, medios de transmisión, redes sociales que podrían considerarse no productivas o consumir exceso de ancho de banda de Internet en una red empresarial. Bloquear el acceso a estos sitios web puede mejorar la productividad de los empleados, reducir los costes operativos para el uso del ancho de banda y reducir la sobrecarga del consumo de red.

### Requisitos previos

La función Categorización de URL funciona en una plataforma Citrix SWG solo si tiene un servicio de suscripción opcional con capacidades de filtrado de URL e inteligencia de amenazas para Citrix Secure Web Gateway. La suscripción permite a los clientes descargar las categorías de amenazas más recientes para sitios web y, a continuación, aplicar esas categorías en Secure Web Gateway. La suscripción está disponible para aplicaciones de hardware y versiones de software (VPX) de Secure Web Gateway.
Antes de habilitar y configurar la característica, debe instalar las siguientes licencias:
**CNS_Webf_Sserver_Retail.lic**

**CNS_XXXXX_SERVER_SWG_Retail.lic.**

Donde, XXXXX es el tipo de plataforma, por ejemplo: V25000

### Expresiones de directiva del respondedor

En la tabla siguiente se enumeran las diferentes expresiones de directiva que se pueden utilizar para comprobar si se debe permitir, redirigir o bloquear una dirección URL entrante.

1. <text>. URL_CATEGORIZE (<min_reputation>, <max_reputation>): Devuelve un objeto URL_CATEGORY. Si <min_reputation> es mayor que 0, el objeto devuelto no contiene una categoría con una reputación inferior a <min_reputation>. Si <max_reputation> es mayor que 0, el objeto devuelto no contiene una categoría con una reputación mayor que <max_reputation>. Si la categoría no se resuelve de manera oportuna, se devuelve el valor undef.
2. <url_category>. CATEGORY(): Devuelve la cadena de categoría para este objeto. Si la URL no tiene una categoría, o si la URL está mal formada, el valor devuelto es “Unknown. “
3. <url_category>. CATEGORY_GROUP(): Devuelve una cadena que identifica el grupo de categorías del objeto. Se trata de una agrupación de categorías de nivel superior, que es útil en operaciones que requieren información menos detallada sobre la categoría de URL. Si la URL no tiene una categoría, o si la URL está mal formada, el valor devuelto es “Unknown. “

4. <url_category>. REPUTATION(): Devuelve la puntuación de reputación como un número de 0 a 5, donde 5 indica la reputación más riesgosa. Si existe la categoría "Desconocido", el valor de reputación es 1.

**Tipos de directivas**:

1. Directiva para seleccionar las solicitudes de direcciones URL que se encuentran en la categoría Motor de búsqueda: `add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0). CATEGORY().EQ("Search Engine")`
2. Directiva para seleccionar las solicitudes de URL que se encuentran en el grupo de categoría Adulto: `add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0). CATEGORY_GROUP().EQ("Adult")'`
3. Directiva para seleccionar solicitudes de URL del motor de búsqueda con una puntuación de reputación inferior a 4: `add responder policy p2 'HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL).URL_CATEGORIZE(4,0).HAS_CATEGORY("Search Engine")`
4. Directiva de selección de solicitudes para el motor de búsqueda y las URL de Shopping: `add responder policy p3 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL). URL_CATEGORIZE(0,0).CATEGORY().EQ ("good_categories")`
5. Directiva para seleccionar solicitudes de direcciones URL del motor de búsqueda con una puntuación de reputación igual o superior a 4: `add responder policy p5 'CLIENT .SSL.DETECTED_DOMAIN.URL_CATEGORIZE(4,0). CATEGORY().EQ("Search Engines")`
6. Directiva para seleccionar las solicitudes de direcciones URL que se encuentran en la categoría Motor de búsqueda y compararlas con un conjunto de direcciones URL: `' HTTP.REQ. HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0). CATEGORY(). EQ("Search Engine")&& HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL). URLSET_MATCHES_ANY("u1")'`

### Tipos de directivas de respondedor

Hay dos tipos de directivas que se utilizan en la función de categorización de URL y cada uno de estos tipos de directivas se explica a continuación:

| Tipo de directiva | Descripción |
|---|---|
| Categoría URL | Categorizar el tráfico web y en función de los resultados de la evaluación bloquea, permite o redirige el tráfico. |

| Tipo de directiva | Descripción |
| --- | --- |
| Puntuación de reputación de URL | Determina la puntuación de reputación del sitio web y le permite controlar el acceso en función del nivel de umbral de puntuación de reputación establecido por el administrador. |

## Configurar categorización de URL

Para configurar la categorización de direcciones URL en un dispositivo Citrix SWG, haga lo siguiente:

1. Habilitar el filtrado de URL.
2. Configure un servidor proxy para el tráfico Web.
3. Configure la intercepción SSL para el tráfico Web en modo explícito.
4. Configure la memoria compartida para limitar la memoria caché.
5. Configure los parámetros de categorización de URL.
6. Configure la categorización de URL mediante el asistente de Citrix SWG.
7. Configure los parámetros de categorización de URL mediante el asistente SWG.
8. Configurar la ruta de base de datos inicial y el nombre del servidor en la nube

### Paso 1: Habilitar el filtrado de URL

Para habilitar la categorización de URL, habilite la función de filtrado de URL y habilite los modos de categorización de URL.

Para habilitar la categorización de URL mediante Citrix SWG: CLI

En el símbolo del sistema, escriba:

```
enable ns feature URLFiltering
```

```
disable ns feature URLFiltering
```

### Paso 2: Configurar un servidor proxy para el tráfico web en modo explícito

El dispositivo Citrix SWG admite servidores virtuales proxy transparentes y explícitos. Para configurar un servidor virtual proxy para el tráfico SSL en modo explícito, haga lo siguiente:

1. Agregue un servidor proxy.
2. Enlazar una directiva SSL al servidor proxy.

Para agregar un servidor proxy mediante la CLI de Citrix SWG

En el símbolo del sistema, escriba:

```
add cs vserver <name> [-td <positive_integer>] <serviceType>  [-
    cltTimeout <secs>]
<!--NeedCopy-->
```

**Ejemplo:**

```
add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180
<!--NeedCopy-->
```

**Enlazar una directiva SSL a un servidor virtual proxy mediante la CLI de Citrix SWG**

```
bind ssl vserver <vServerName> -policyName <string> [-priority <
    positive_integer>]
<!--NeedCopy-->
```

**Paso 3: Configurar la intercepción SSL para el tráfico HTTPS**

Para configurar la intercepción SSL para el tráfico HTTPS, haga lo siguiente:

1. Enlazar un par de claves de certificado de CA al servidor virtual proxy.
2. Configure el perfil SSL predeterminado con parámetros SSL.
3. Enlazar un perfil SSL front-end al servidor virtual proxy y habilitar la intercepción SSL en el perfil SSL front-end.

Para enlazar un par de claves de certificación de CA al servidor virtual proxy mediante la CLI de Citrix SWG

En el símbolo del sistema, escriba:

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName> -
    CA  – skipCAName
<!--NeedCopy-->
```

Para configurar el perfil SSL predeterminado mediante la CLI de Citrix SWG

En el símbolo del sistema, escriba:

```
set ssl profile <name> -denySSLReneg <denySSLReneg> -sslInterception (
    ENABLED | DISABLED) -ssliMaxSessPerServer positive_integer>
<!--NeedCopy-->
```

**Enlazar un perfil SSL front-end a un servidor virtual proxy mediante la CLI de Citrix SWG**

En el símbolo del sistema, escriba:

```
set ssl vserver <vServer name>  -sslProfile ssl_profile_interception
<!--NeedCopy-->
```

**Paso 4: Configurar la memoria compartida para limitar la memoria caché**

Para configurar la memoria compartida para limitar la memoria caché mediante la CLI de Citrix SWG

En el símbolo del sistema, escriba:

```
set cache parameter [-memLimit <megaBytes>]
<!--NeedCopy-->
```

Donde, el límite de memoria configurado para el almacenamiento en caché se establece como 10 MB.

**Paso 5: Configurar los parámetros de categorización de URL**

Para configurar los parámetros de categorización de URL mediante la CLI de Citrix SWG

En el símbolo del sistema, escriba:

```
set urlfiltering parameter [-HoursBetweenDBUpdates <positive_integer>]
   [-TimeOfDayToUpdateDB <HH:MM>]
<!--NeedCopy-->
```

**Ejemplo**:

```
Set urlfiltering parameter  – urlfilt_hours_betweenDB_updates 20
<!--NeedCopy-->
```

**Paso 6: Configure la categorización de URL mediante el asistente de Citrix SWG**

Para configurar la categorización de URL mediante la GUI de Citrix SWG

1. Inicie sesión en el dispositivo Citrix SWG y vaya a la página **Secured Web Gateway**.
2. En el panel de detalles, realice una de las acciones siguientes:
   a) Haga clic en **Asistente para puerta de enlace web segura** para crear una nueva configuración.
   b) Seleccione una configuración existente y haga clic en **Modificar**.
3. En la sección **Filtrado de URL**, haga clic en **Modificar**.

4. Active la casilla de verificación **Categorización de URL** para habilitar la función.
5. Seleccione una directiva de **categorización de URL** y haga clic en **Enlazar**.
6. Haga clic en **Continuar** y, a continuación, en **Listo**.

Para obtener más información acerca de la directiva de categorización de URL, consulte Cómo crear una directiva de categorización de URL.

#### Paso 7: Configuración de parámetros de categorización de URL mediante el Asistente SWG

Para configurar los parámetros de categorización de URL mediante la GUI de Citrix SWG

1. Inicie sesión en el dispositivo **Citrix SWG** y vaya a **Secured Web Gateway > Filtrado de URL**.
2. En la página **Filtrado de URL**, haga clic en **el enlace Cambiar configuración de filtrado de URL**.
3. En la página **Configuración de parámetros de filtrado de URL**, especifique los siguientes parámetros.
    a) Horas entre actualizaciones de base de datos. Horas de filtrado de URL entre las actualizaciones de la base de datos. Valor mínimo: 0 y Valor máximo: 720.
    b) Hora del día para actualizar la base de datos. URL Filtrado hora del día para actualizar la base de datos.
    c) Host en la nube. La ruta URL del servidor en la nube.
    d) Ruta de base de datos de semilla. Ruta de acceso URL del servidor de búsqueda de base de datos semilla.
4. Haga clic en **Aceptar** y **Cerrar**.

**Configuración de ejemplo:**

```
enable ns feature LB CS SSL IC RESPONDER AppFlow URLFiltering

enable ns mode FR L3 Edge USNIP PMTUD

set ssl profile ns_default_ssl_profile_frontend -denySSLReneg NONSECURE
    -sslInterception ENABLED -ssliMaxSessPerServer 100

add ssl certKey swg_ca_cert -cert ns_swg_ca.crt -key ns_swg_ca.key

set cache parameter -memLimit 100

add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180

add responder action act1 respondwith ""HTTP/1.1 200 OK\r\n\r\n" + http
   .req.url.url_categorize(0,0).reputation + "\n""

add responder policy p1 "HTTP.REQ.URL.URL_CATEGORIZE(0,0).CATEGORY.eq("
   Shopping/Retail") || HTTP.REQ.URL.URL_CATEGORIZE(0,0).CATEGORY.eq("
   Search Engines & Portals
```

```
16
17 ")" act1
18
19 bind cs vserver starcs_PROXY -policyName p1 -priority 10 -
      gotoPriorityExpression END -type REQUEST
20
21 add dns nameServer 10.140.50.5
22
23 set ssl parameter -denySSLReneg NONSECURE -defaultProfile ENABLED -
      sigDigestType RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384 RSA-
      SHA512 -ssliErrorCache ENABLED
24
25 -ssliMaxErrorCacheMem 100000000
26
27 add ssl policy pol1 -rule "client.ssl.origin_server_cert.subject.
      URL_CATEGORIZE(0,0).CATEGORY.eq("Search Engines & Portals")"" -
      action INTERCEPT
28
29 add ssl policy pol3 -rule "client.ssl.origin_server_cert.subject.ne("
      citrix")" -action INTERCEPT
30
31 add ssl policy swg_pol -rule "client.ssl.client_hello.SNI.
      URL_CATEGORIZE(0,0).CATEGORY.ne("Uncategorized")" -action INTERCEPT
32
33 set urlfiltering parameter -HoursBetweenDBUpdates 3 -
      TimeOfDayToUpdateDB 03:00
34 <!--NeedCopy-->
```

**Configurar la ruta de base de datos inicial y el nombre del servidor en la nube**

Ahora puede configurar la ruta de acceso de base de datos semilla y el nombre del servidor de búsqueda en la nube para establecer manualmente el nombre del servidor de búsqueda en la nube y la ruta de la base de datos semilla. Para ello, se agregan dos nuevos parámetros, “CloudHost”y “SeedDBPath”, al comando de parámetros de filtrado de URL.

En el símbolo del sistema, escriba:

```
set urlfiltering parameter [-HoursBetweenDBUpdates <positive_integer
>] [-TimeOfDayToUpdateDB <HH:MM>] [-LocalDatabaseThreads <positive_integer
>] [-CloudHost <string>] [-SeedDBPath <string>]
```

**Ejemplo**

```
set urlfiltering parameter -HoursBetweenDBUpdates 3 -TimeOfDayToUpdateDB
 03:00 –CloudHost localhost –SeedDBPath /mypath
```

La comunicación entre un dispositivo Citrix ADC y NetSTAR puede requerir un servidor de nombres de dominio. Puede probar mediante una consola simple o una conexión telnet desde el dispositivo.

**Ejemplo:**

```
root@ns# telnet nsv10.netstar-inc.com 443
Trying 1.1.1.1...
Connected to nsv10.netstar-inc.com.
Escape character is '^]'.

root@ns# telnet incompasshybridpc.netstar-inc.com 443
Trying 10.10.10.10...
Connected to incompasshybridpc.netstar-inc.com.
Escape character is '^]'.
<!--NeedCopy-->
```

### Configurar la mensajería del registro de auditoría

El registro de auditoría le permite revisar una condición o una situación en cualquier fase del proceso de categorización de URL. Cuando un dispositivo Citrix ADC recibe una dirección URL entrante, si la directiva de respuesta tiene una expresión de filtrado de URL, la característica de registro de auditoría recopila la información del conjunto de URL en la dirección URL y la almacena como mensajes de registro para cualquier destino permitido por el registro de auditoría.

- Dirección IP de origen (la dirección IP del cliente que realizó la solicitud).
- Dirección IP de destino (la dirección IP del servidor solicitado).
- URL solicitada que contiene el esquema, el host y el nombre de dominio (http://www.example.com.
- Categoría de URL que devuelve el marco de filtrado de URL.
- Grupo de categoría de URL devuelto por el marco de filtrado de URL.
- Número de reputación de URL devuelto por el marco de filtrado de URL.
- Acción de registro de auditoría realizada por la directiva.

Para configurar el registro de auditoría para la función Lista de URL, debe completar las siguientes tareas:

1. Habilitar registros de auditoría.
2. Acción de mensaje Crear registro de auditoría.
3. Establecer la directiva de respuesta de lista de URL con la acción de mensaje Registro de auditoría.

Para obtener más información, consulte el tema Registro de auditoría.

### Almacenamiento de errores mediante mensajería SYSLOG

En cualquier etapa del proceso de filtrado de URL, si se produce un error a nivel del sistema, el dispositivo Citrix ADC utiliza el mecanismo de registro de auditoría para almacenar registros en el archivo ns.log. Los errores se almacenan como mensajes de texto en formato SYSLOG para que un administrador pueda verlo más adelante en un orden cronológico de ocurrencia de eventos. Estos registros

también se envían a un servidor SYSLOG externo para su archivado. Para obtener más información, consulte artículo CTX229399.

Por ejemplo, si se produce un error al inicializar el SDK de filtrado de URL, el mensaje de error se almacena en el siguiente formato de mensajería.

```
Oct 3 15:43:40 <local0.err> ns URLFiltering[1349]: Error initializing
 NetStar SDK (SDK error=-1). (status=1).
```

El dispositivo Citrix ADC almacena los mensajes de error en cuatro categorías de error diferentes:

- **Error de descarga**. Si se produce un error al intentar descargar la base de datos de categorización.
- **Fallo de integración**. Si se produce un error al integrar una actualización en la base de datos de categorización existente.
- **Error de inicialización**. Si se produce un error al inicializar la función de categorización de URL, establecer parámetros de categorización o finalizar un servicio de categorización.
- **Error de recuperación**. Si se produce un error cuando el dispositivo recupera los detalles de categorización de la solicitud.

### Mostrar resultado de categorización de URL a través de la interfaz de comandos

La categorización de URL le permite introducir una URL y recuperar resultados de categorización (como categoría, grupo y puntuación de reputación) de la base de datos de categorización de URL de terceros de NetSTAR.

Cuando se introduce una dirección URL, la función de filtrado de URL recupera y muestra el resultado de la categorización en la interfaz de comandos. Al introducir otras direcciones URL, el dispositivo excluye las direcciones URL más antiguas de la lista y muestra el resultado de las tres direcciones URL más recientes.

Para mostrar el resultado de categorías URL hasta tres direcciones URL, siga estos pasos:

1. Agregar URL de categorización de URL
2. Mostrar detalles de categorización de URL hasta tres direcciones URL
3. Borrar los datos de categorización de URL.

#### Para agregar URL de categorización de filtrado de URL

Para agregar una dirección URL y recuperar sus detalles de categorización, haga lo siguiente:
En el símbolo del sistema, escriba:

```
add urlfiltering categorization –Url <string>
```

**Ejemplo:**

```
add urlfiltering categorization –Url www.facebook.com
```

**Para mostrar detalles de categorización de URL hasta tres direcciones URL**

En el símbolo del sistema, escriba:

```
> show urlfiltering categorization
```

**Ejemplo:**

```
1 show urlfiltering categorization
2 Url: http://www.facebook.com    Categorization: Facebook,Social
     Networking,1
3 Url: http://www.google.com      Categorization: Search Engines &
     Portals,Search,1
4 Url: http://www.citrix.com      Categorization: Computing & Internet,
     Computing & Internet,1
5 Done
6 <!--NeedCopy-->
```

**Configuración de ejemplo:**

```
1  add urlfiltering categorization -url www.facebook.com
2  Done
3  show urlfiltering categorization
4  Url: http://www.facebook.com    Categorization: Facebook,Social
      Networking,1
5  Done
6
7  add urlfiltering categorization -url www.google.com
8  Done
9  show urlfiltering categorization
10 Url: http://www.facebook.com    Categorization: Facebook,Social
      Networking,1
11 Url: http://www.google.com      Categorization: Search Engines &
      Portals,Search,1
12 Done
13
14 add urlfiltering categorization -url www.citrix.com
15 Done
16 show urlfiltering categorization
17 Url: http://www.facebook.com    Categorization: Facebook,Social
      Networking,1
18 Url: http://www.google.com      Categorization: Search Engines &
      Portals,Search,1
19 Url: http://www.citrix.com      Categorization: Computing & Internet,
      Computing & Internet,1
20 Done
21
22 add urlfiltering categorization -url www.in.gr
23 Done
24 show urlfiltering categorization
```

```
Url: http://www.google.com      Categorization: Search Engines &
    Portals,Search,1
Url: http://www.citrix.com      Categorization: Computing & Internet,
    Computing & Internet,1
Url: http://www.in.gr   Categorization: Search Engines & Portals,Search
    ,1 Done
<!--NeedCopy-->
```

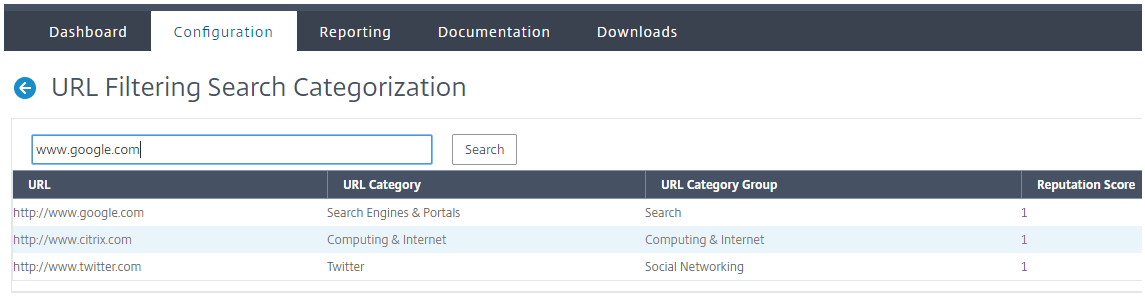
**Para borrar el resultado de categorización de URL**

En el símbolo del sistema, escriba:

```
clear urlfiltering categorization
done

show urlfiltering categorization
done
<!--NeedCopy-->
```

### Mostrar el resultado de categorización de URL a través de la interfaz gráfica de usuario

1. En el panel de navegación, expanda **Secure Web Gateway** > **Filtrado de URL**.
2. En el panel de detalles, haga clic en **Filtrado de URL Enlace categorización de búsqueda** en la sección **Herramientas**.
3. En la página **Filtrado de URL categorización de búsqueda**, introduzca una solicitud de URL y haga clic en **Buscar**.




4. El dispositivo muestra el resultado de categoría de la dirección URL solicitada y de las dos solicitudes de URL anteriores.

## Configuración de seguridad

April 27, 2021

La función Configuración de seguridad le permite configurar la directiva de seguridad para filtrar direcciones URL. El tema Puntuación de reputación de URL proporciona detalles conceptuales y de configuración para filtrar direcciones URL en función de su puntuación de reputación.

Puede utilizar ICAP para la inspección remota de contenido.

### Puntuación de reputación de URL

La función Categorización de URL utiliza la puntuación de reputación de URL para proporcionar un control basado en directivas para bloquear sitios web de alto riesgo. Para obtener más información, consulte Puntuación de reputación de URL.

### Uso de ICAP para la inspección remota de contenido

El tráfico HTTPS se intercepta, desencripta y se envía a los servidores ICAP para la inspección de contenido para comprobaciones antimalware y prevención de fugas de datos.

## Puntuación de reputación de URL

April 27, 2021

La función Categorización de URL proporciona un control basado en directivas para restringir las direcciones URL incluidas en la lista negra. Puede controlar el acceso a sitios web en función de la categoría de URL, la puntuación de reputación o la categoría de URL y la puntuación de reputación. Si un administrador de red supervisa a un usuario que accede a sitios web de alto riesgo, puede utilizar una directiva de respuesta vinculada a la puntuación de reputación de URL para bloquear dichos sitios web de riesgo.

Al recibir una solicitud de dirección URL entrante, el dispositivo recupera la puntuación de categoría y reputación de la base de datos de categorización de direcciones URL. En función de la puntuación de reputación devuelta por la base de datos, el dispositivo asigna una calificación de reputación a los sitios web. El valor puede variar de 1 a 4, donde 4 es el tipo de sitios web más arriesgado, como se muestra en la siguiente tabla.

| Clasificación de reputación de URL | Comentario de reputación |
|---|---|
| 1 | Sitio limpio |
| 2 | Sitio desconocido |

| Clasificación de reputación de URL | Comentario de reputación |
|---|---|
| 3 | Potencialmente peligroso o afiliado a un sitio peligroso |
| 4 | Sitio malintencionado |

### Caso de uso: Filtrar por puntuación de reputación de URL

Considere una organización empresarial con un administrador de red que supervisa las transacciones de usuario y el consumo de ancho de banda de red. Si el malware puede entrar en la red, el administrador debe mejorar la seguridad de los datos y controlar el acceso a sitios web malintencionados y peligrosos que acceden a la red. Para proteger la red contra dichas amenazas, el administrador puede configurar la función de filtrado de URL para permitir o denegar el acceso por puntuación de reputación de URL.

Para obtener más información acerca de cómo supervisar el tráfico saliente y las actividades de usuario en la red, consulte Analítica SWG.

Si un empleado de la organización intenta acceder a un sitio web de redes sociales, el dispositivo SWG recibe una solicitud de URL y consulta la base de datos de categorización de URL para recuperar la categoría URL como redes sociales y una puntuación de reputación 3, lo que indica un sitio web potencialmente peligroso. A continuación, el dispositivo comprueba la directiva de seguridad configurada por el administrador, como bloquear el acceso a sitios con una calificación de reputación de 3 o más. A continuación, aplica la acción de directiva para controlar el acceso al sitio web.

Para implementar esta función, debe configurar la puntuación de reputación de URL y los niveles de umbral de seguridad mediante el asistente de Citrix SWG.

**Configuración de la puntuación de reputación mediante la GUI de Citrix SWG**:

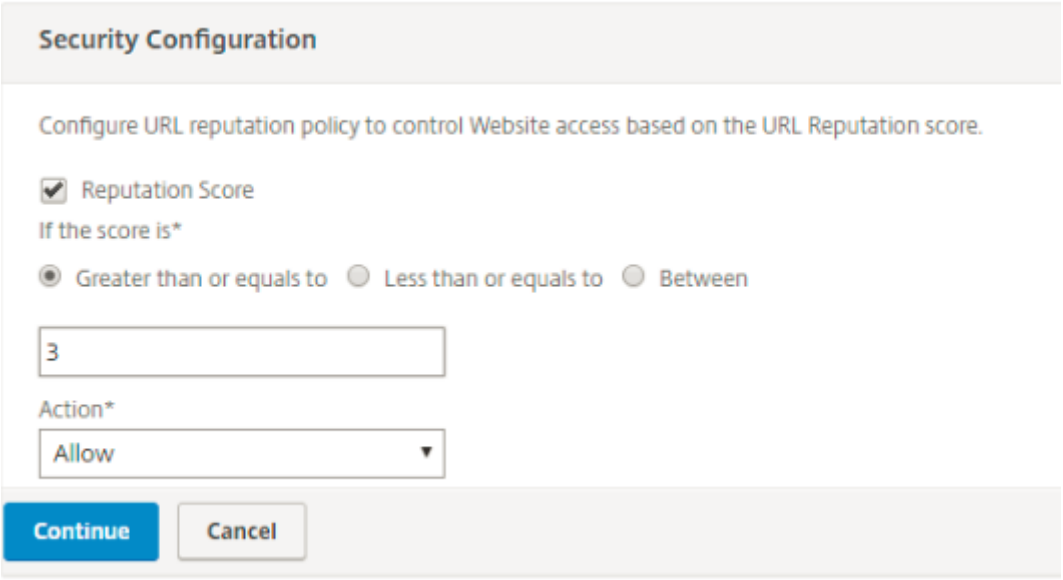
Citrix recomienda utilizar el asistente de Citrix SWG para configurar la puntuación de reputación y los niveles de seguridad. En función del umbral configurado, puede seleccionar una acción de directiva para permitir, bloquear o redirigir el tráfico.

1. Inicie sesión en el dispositivo **Citrix SWG** y desplácese hasta **Secure Web Gateway**.
2. En el panel de detalles, haga clic en **Asistente para puerta de enlace web segura**.
3. En la página **Configuración de Secure Web Gateway**, especifique la configuración del servidor proxy SWG.
4. Haga clic en **Continuar** para especificar otros parámetros, como la intercepción de SSL y la administración de identificación.
5. Haga clic en **Continuar** para acceder a la sección **Configuración de seguridad**.

6. En la sección **Configuración de seguridad**, active la casilla de verificación **Puntuación de reputación** para controlar el acceso en función de la puntuación de reputación de URL.
7. Seleccione el nivel de seguridad y especifique el valor del umbral de puntuación de reputación:
    a) Mayor o igual a: Permite o bloquea un sitio web si el valor de umbral es mayor o igual que N, donde N oscila entre uno y cuatro.
    b) Menor o igual a: Permite o bloquea un sitio web si el valor de umbral es menor o igual a N, donde N oscila entre uno y cuatro.
    c) Entre: Permite o bloquea un sitio web si el valor de umbral está entre N1 y N2 y el rango es de uno a cuatro.
8. Seleccione una acción de respuesta en la lista desplegable.
9. Haga clic en **Continuar** y Cerrar.

En la siguiente imagen se muestra la sección Configuración de seguridad del asistente de Citrix SWG. Habilite la opción Puntuación de reputación de URL para configurar la configuración de directiva.




## Uso de ICAP para la inspección remota de contenido

April 27, 2021

El Protocolo de Adaptación de Contenido de Internet (ICAP) es un protocolo abierto simple y ligero. Normalmente se utiliza para transportar mensajes HTTP entre el proxy y los dispositivos que proporcionan soporte antimalware y servicios de prevención de fugas de datos. ICAP ha creado una interfaz estándar para la adaptación de contenidos para permitir una mayor flexibilidad en la distribución de contenidos y para proporcionar un servicio de valor agregado. Un cliente ICAP reenvía solicitudes y

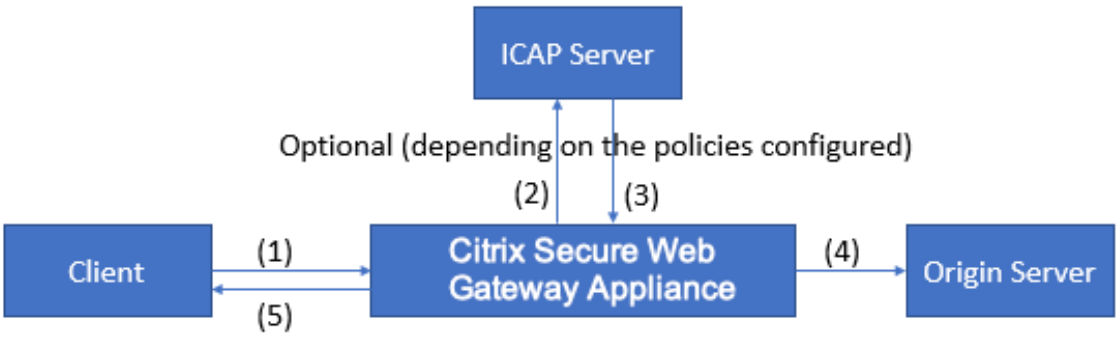
respuestas HTTP a un servidor ICAP para su procesamiento. El servidor ICAP realiza alguna transformación en las solicitudes y envía respuestas al cliente ICAP, con la acción adecuada en la solicitud o respuesta.

### Uso de ICAP en el dispositivo Citrix Secure Web Gateway

> **Nota**
>
> La función de inspección de contenido requiere una licencia SWG Edition.

El dispositivo Citrix Secure Web Gateway (SWG) actúa como cliente ICAP y utiliza directivas para interactuar con servidores ICAP. El dispositivo se comunica con servidores ICAP de terceros que se especializan en funciones como antimalware y prevención de fugas de datos (DLP). Cuando utiliza ICAP en un dispositivo SWG, también se analizan los archivos cifrados. Los proveedores de seguridad anteriormente omitieron estos archivos. El dispositivo realiza la interceptación SSL, descifra el tráfico del cliente y lo envía al servidor ICAP. El servidor ICAP comprueba si hay detección de virus, malware o spyware, inspección de fugas de datos o cualquier otro servicio de adaptación de contenido. El dispositivo actúa como proxy, descifra la respuesta del servidor de origen y la envía en texto sin formato al servidor ICAP para su inspección. Configure directivas para seleccionar el tráfico que se envía a los servidores ICAP.

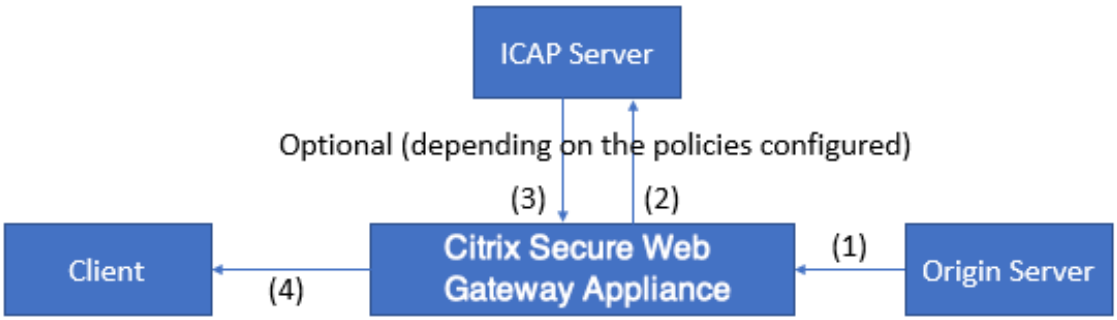
**El flujo del modo de solicitud funciona de la siguiente manera**:




(1) El dispositivo Citrix SWG intercepta las solicitudes del cliente. (2) El dispositivo reenvía estas solicitudes al servidor ICAP, según las directivas configuradas en el dispositivo. (3) El servidor ICAP responde con un mensaje que indica "No se requiere adaptación", error o solicitud modificada. El dispositivo (4) reenvía el contenido al servidor de origen solicitado por el cliente o (5) devuelve un mensaje apropiado al cliente.

**El flujo del modo de respuesta funciona de la siguiente manera**:




(1) El servidor de origen responde al dispositivo Citrix SWG. (2) El dispositivo reenvía la respuesta al servidor ICAP, basándose en las directivas configuradas en el dispositivo. (3) El servidor ICAP responde con un mensaje que indica "No se requiere adaptación", error o solicitud modificada. (4) Dependiendo de la del servidor ICAP, el dispositivo reenvía el contenido solicitado al cliente o envía un mensaje apropiado.

### Configuración de ICAP en el dispositivo Citrix Secure Web Gateway

En los siguientes pasos se explica cómo configurar ICAP en el dispositivo Citrix SWG.

1. Habilite la función de inspección de contenido.
2. Configurar un servidor proxy.
3. Configure un servicio TCP que represente el servidor ICAP. Para establecer una conexión segura entre el dispositivo SWG y el servicio ICAP, especifique el tipo de servicio como SSL_TCP. Para obtener más información acerca de ICAP seguro, consulte la sección "ICAP seguro"más adelante en esta página.
4. Opcionalmente, agregue un servidor virtual de equilibrio de carga para equilibrar la carga de los servidores ICAP y vincular el servicio ICAP a este servidor virtual.
5. Configure un perfil ICAP personalizado. El perfil debe incluir el URI o la ruta de servicio para el servicio ICAP y el modo ICAP (solicitud o respuesta). No hay perfiles predeterminados ICAP similares a los perfiles predeterminados HTTP y TCP.
6. Configure una acción de inspección de contenido y especifique el nombre del perfil ICAP. Especifique el nombre del servidor virtual de equilibrio de carga o el nombre del servicio TCP/SSL_TCP en el parámetro nombre del servidor.
7. Configure una directiva de inspección de contenido para evaluar el tráfico del cliente y vincularlo al servidor proxy. Especifique la acción de inspección de contenido en esta directiva.

#### Configurar ICAP mediante la CLI

Configure las siguientes entidades:

1. Habilite la función.

   ```
   enable ns feature contentInspection
   ```

2. Configurar un servidor proxy.

   ```
   add cs vserver <name> PROXY <IPAddress>
   ```

   **Ejemplo**:

   ```
   add cs vserver explicitswg PROXY 192.0.2.100 80
   ```

3. Configure un servicio TCP para representar los servidores ICAP.

   ```
   add service <name> <IP> <serviceType> <port>
   ```

   Especifique el tipo de servicio como SSL_TCP para una conexión segura con el servidor ICAP.

   **Ejemplo**:

   ```
   add service icap_svc1 203.0.113.100 TCP 1344
   add service icap_svc 203.0.113.200 SSL_TCP 11344
   ```

4. Configure un servidor virtual de equilibrio de carga.

   ```
   add lb vserver <name> <serviceType> <IPAddress> <port>
   ```

   **Ejemplo**:

   ```
   add lbvserver lbicap TCP 0.0.0.0 0
   ```

   Enlazar el servicio ICAP al servidor virtual de equilibrio de carga.

   ```
   bind lb vserver <name> <serviceName>
   ```

   **Ejemplo**:

   ```
   bind lb vserver lbicap icap_svc
   ```

5. Añada un perfil ICAP personalizado.

   ```
   add ns icapProfile <name> -uri <string> -Mode ( REQMOD | RESPMOD
   )
   ```

   **Ejemplo**:

   ```
   add icapprofile icapprofile1 -uri /example.com -Mode REQMOD
   ```

   **Parámetros**

   **name**

   Nombre de un perfil ICAP. Debe comenzar con un carácter alfanumérico o de subrayado (_) ASCII y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), signo en (@), signo igual (=) y guión (-).

Usuarios de CLI: Si el nombre incluye uno o más espacios, enciérrelo entre comillas dobles o simples (por ejemplo, “mi perfil icap”o “mi perfil icap”).

Longitud máxima: 127

**uri**

URI que representa la ruta del servicio ICAP.

Longitud máxima: 511 caracteres

**Modo**

Modo ICAP. Los ajustes disponibles funcionan de la siguiente manera:

- REQMOD: En el modo de modificación de solicitud, el cliente ICAP reenvía una solicitud HTTP al servidor ICAP.
- RESPMOD: en el modo de modificación de la respuesta, el servidor ICAP reenvía una respuesta HTTP desde el servidor de origen al servidor ICAP.

  Valores posibles: REQMOD, RESPMOD

6. Configure una acción para realizar si la directiva devuelve true.

```
add contentInspection action <name> -type ICAP -serverName <
string> -icapProfileName <string>
```

**Ejemplo**:

```
add contentInspection action CiRemoteAction -type ICAP -serverName
 lbicap -icapProfileName icapprofile1
```

7. Configure una directiva para evaluar el tráfico.

```
add contentInspection policy <name> -rule <expression> -action <
string>
```

**Ejemplo**:

```
add contentInspection policy CiPolicy -rule true -action CiRemoteAction
```

8. Enlazar la directiva al servidor proxy.

```
bind cs vserver <vServerName> -policyName <string> -priority <
positive_integer> -type [REQUEST | RESPONSE]
```

**Ejemplo**:

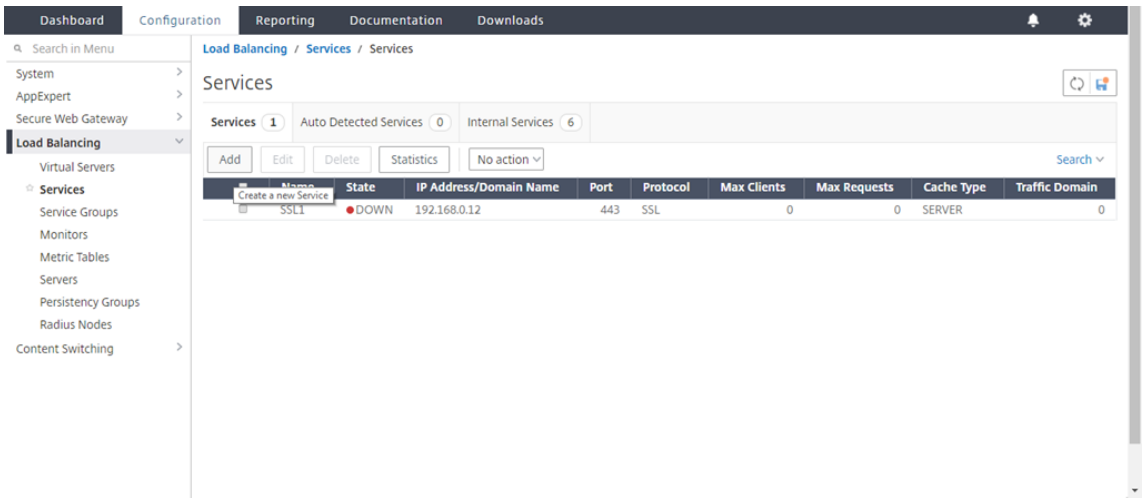
```
bind cs vserver explicitswg -policyName CiPolicy -priority 200 -
type REQUEST
```

### Configurar ICAP mediante la GUI

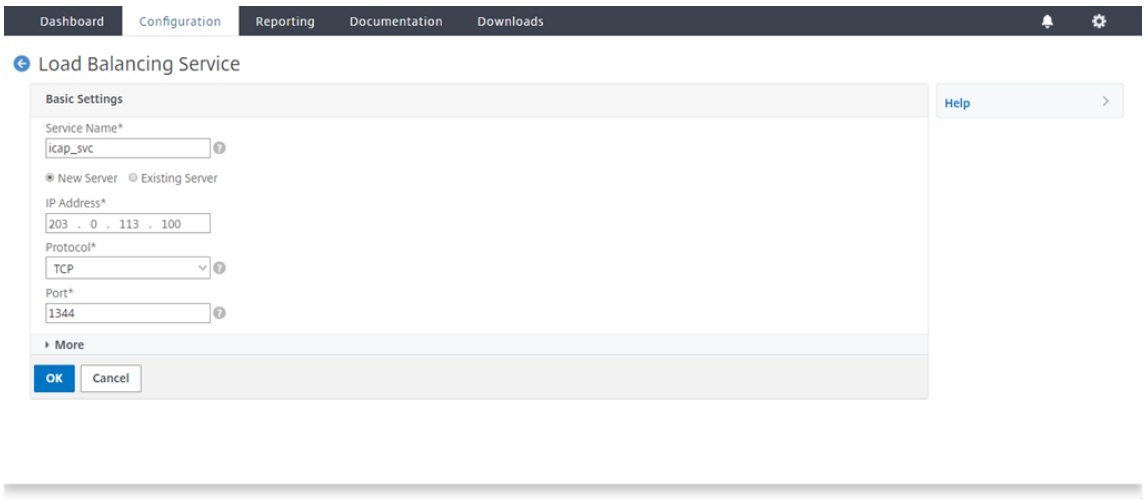
Siga estos pasos:

1. Desplácese hasta **Equilibrio de carga** > **Servicios** y haga clic en **Agregar**.



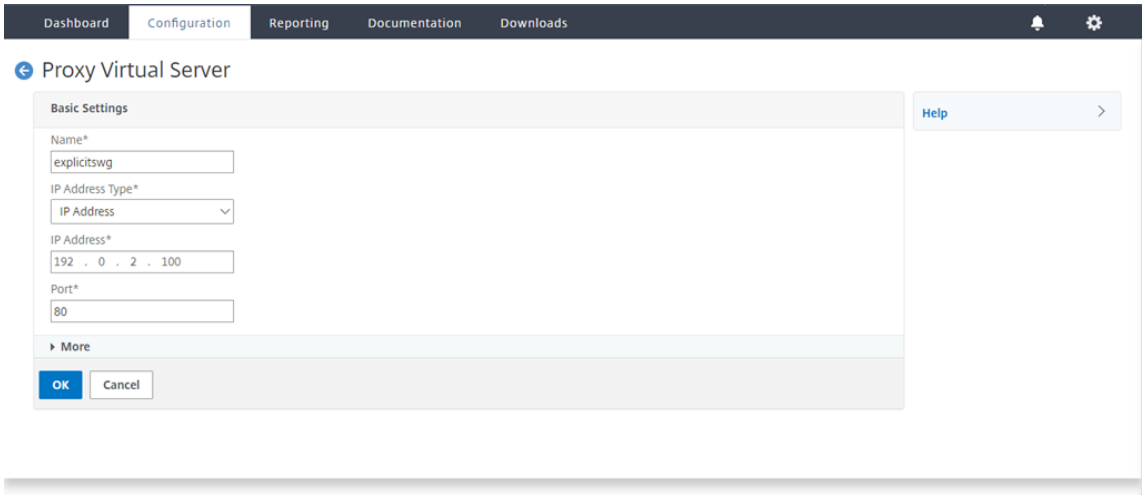

2. Escriba un nombre y una dirección IP. En **Protocolo**, seleccione **TCP**. En **Puerto**, escriba **1344**. Haga clic en **OK**.

   Para una conexión segura con los servidores ICAP, seleccione el protocolo TCP_SSL y especifique el puerto como 11344.

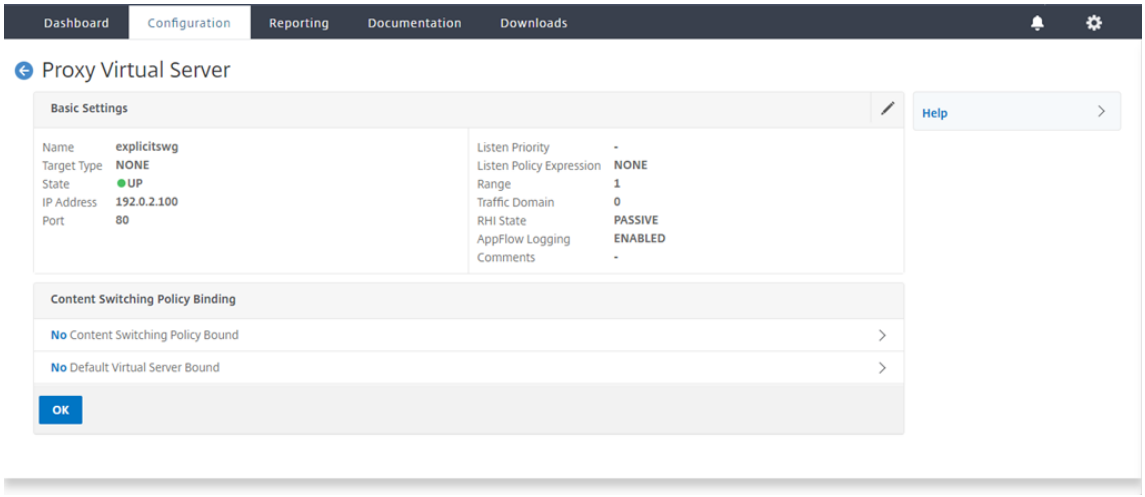



3. Vaya a **Secure Web Gateway** > **Proxy Virtual Servers**. Agregue un servidor virtual proxy o seleccione un servidor virtual y haga clic en **Modificar**. Después de introducir los detalles, haga clic en **Aceptar**.

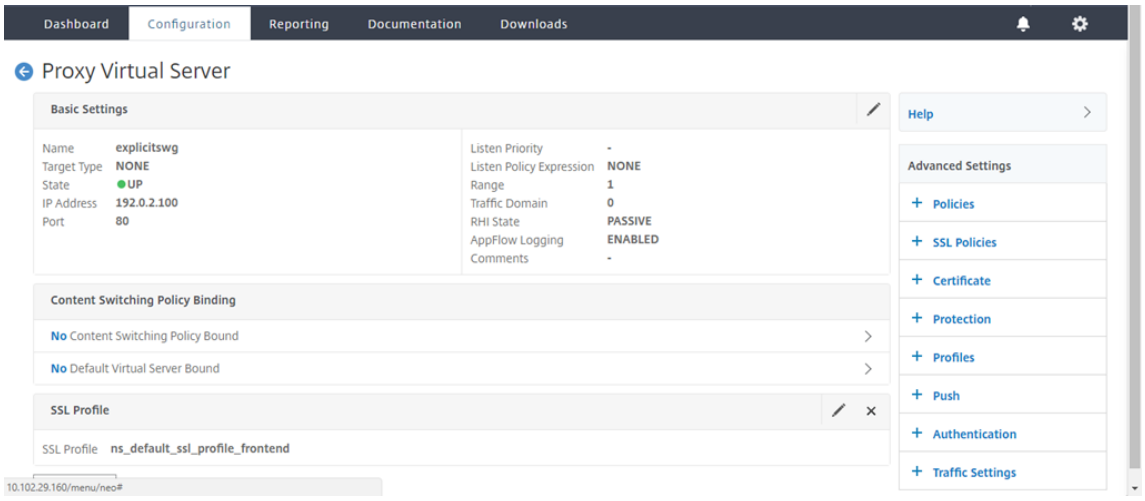
 




Vuelva a hacer clic en **Aceptar**.

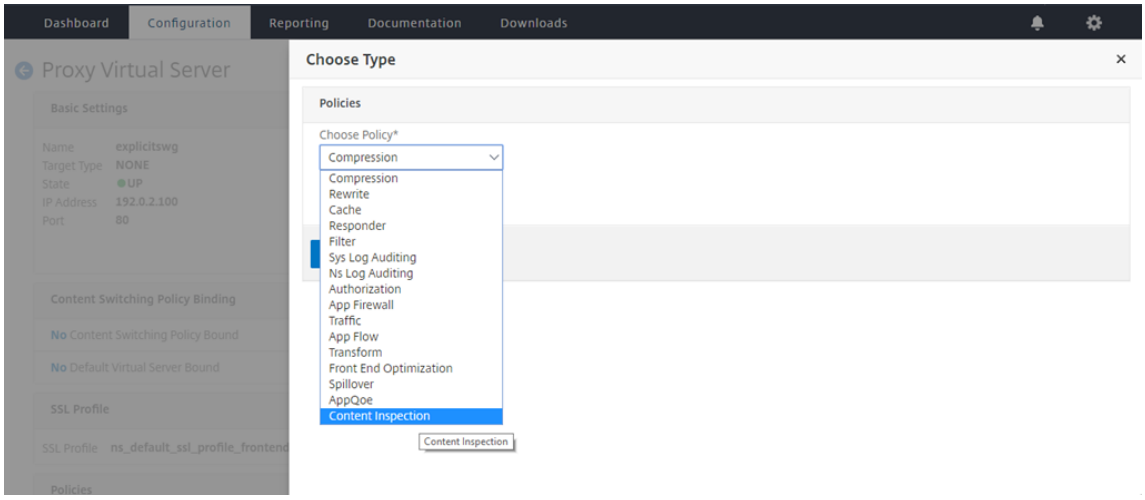



4. En **Configuración avanzada**, haga clic en **Directivas**.

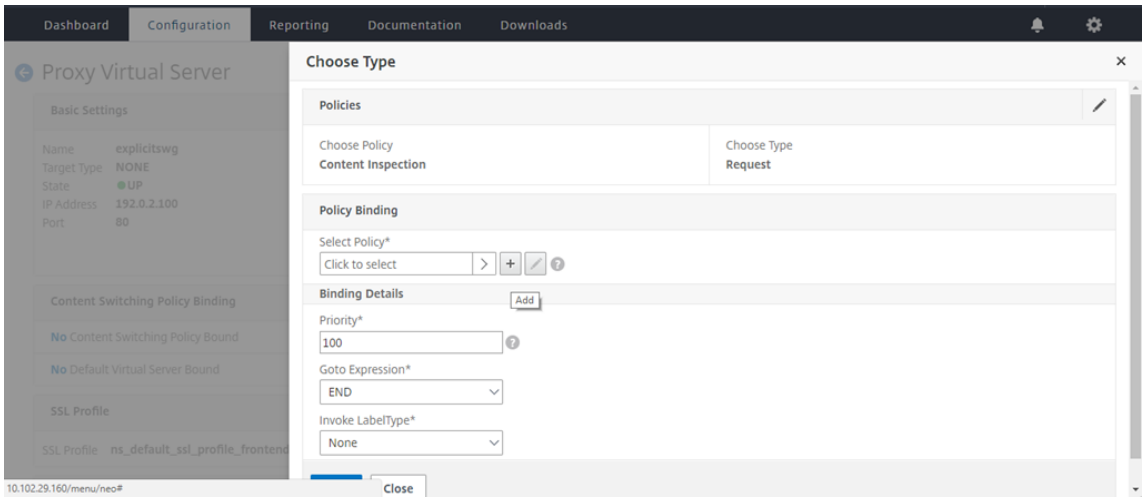



5. En **Elegir directiva**, seleccione **Inspección de contenido**. Haga clic en **Continuar**.

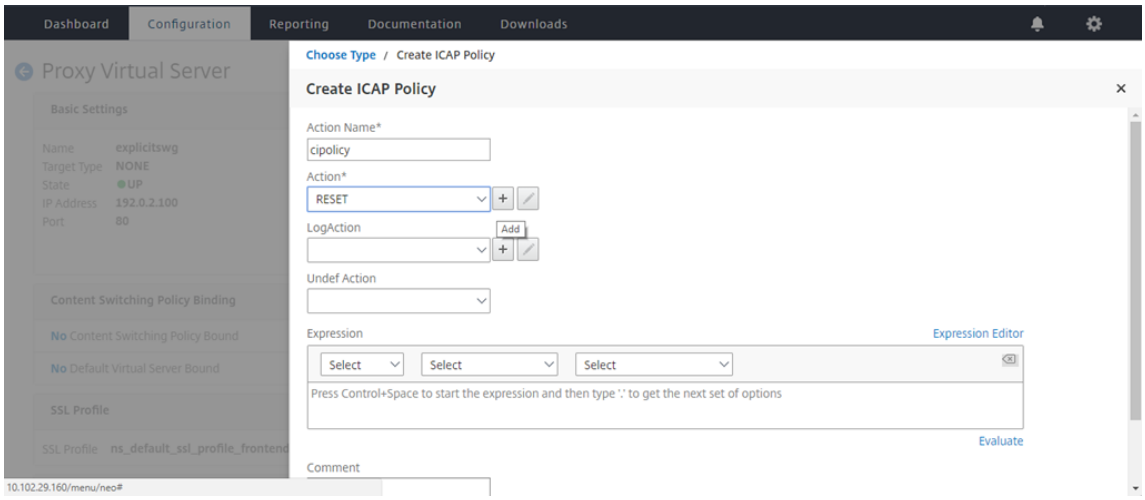
 




6. En **Seleccionar directiva**, haga clic en el signo “+”para agregar una directiva.

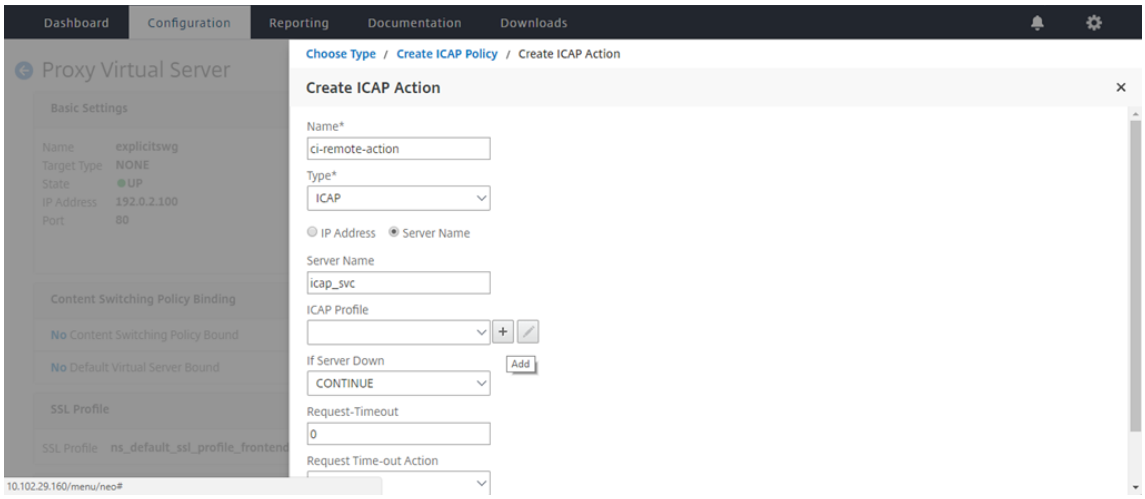



7. Introduzca un nombre para la directiva. En **Acción**, haga clic en el signo “+”para agregar una acción.

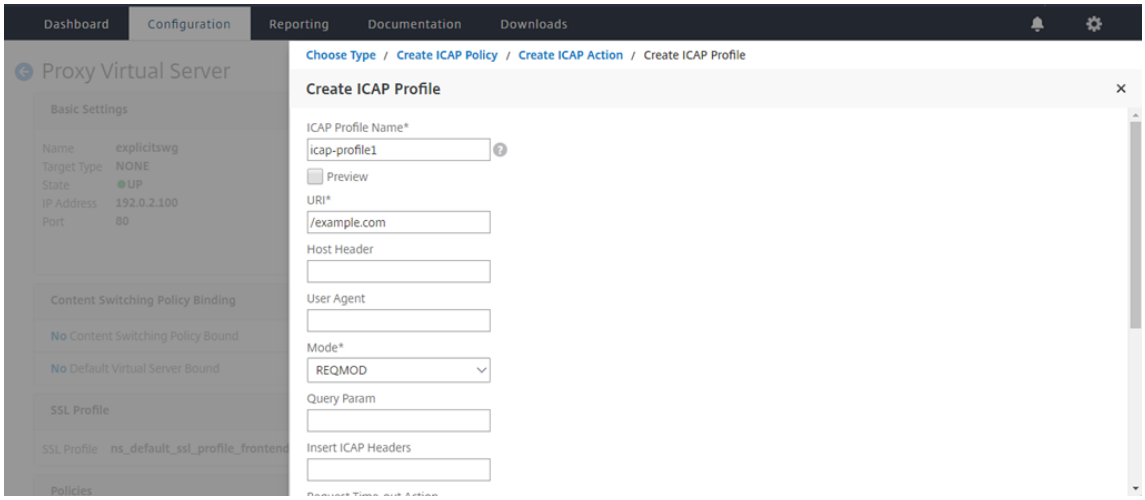


8. Escriba un nombre para la acción. En **Nombre del servidor**, escriba el nombre del servicio TCP creado anteriormente. En **Perfil ICAP**, haga clic en el signo “+”para agregar un perfil ICAP.

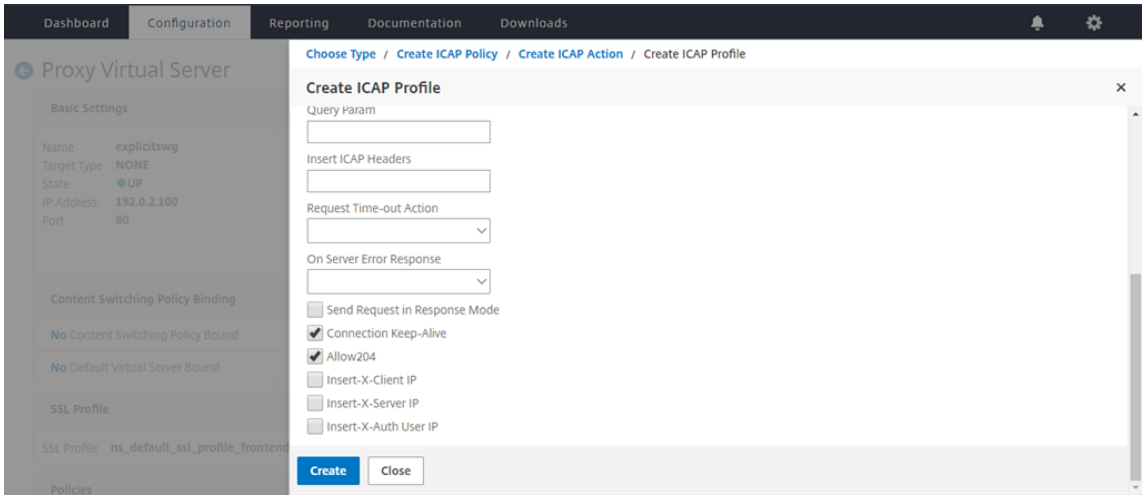



9. Escriba un nombre de perfil, URI. En **Modo**, seleccione **REQMOD**.

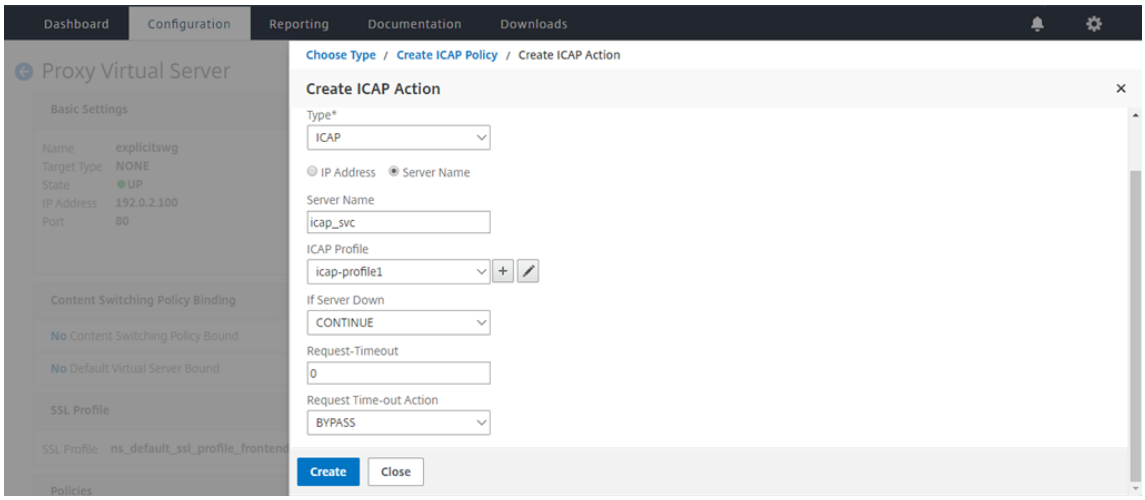



10. Haga clic en **Crear**.

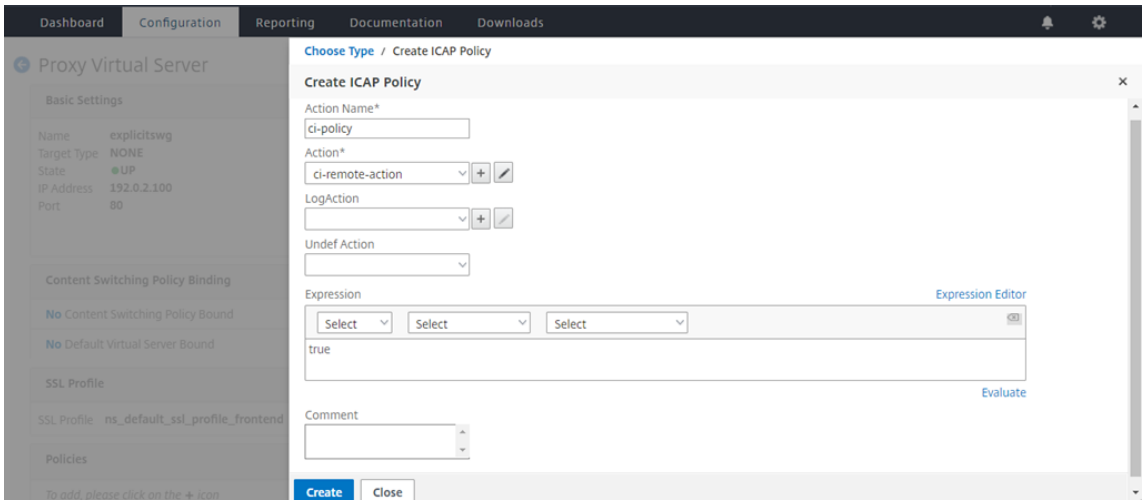
 




11. En la página **Crear acción ICAP**, haga clic en **Crear**.

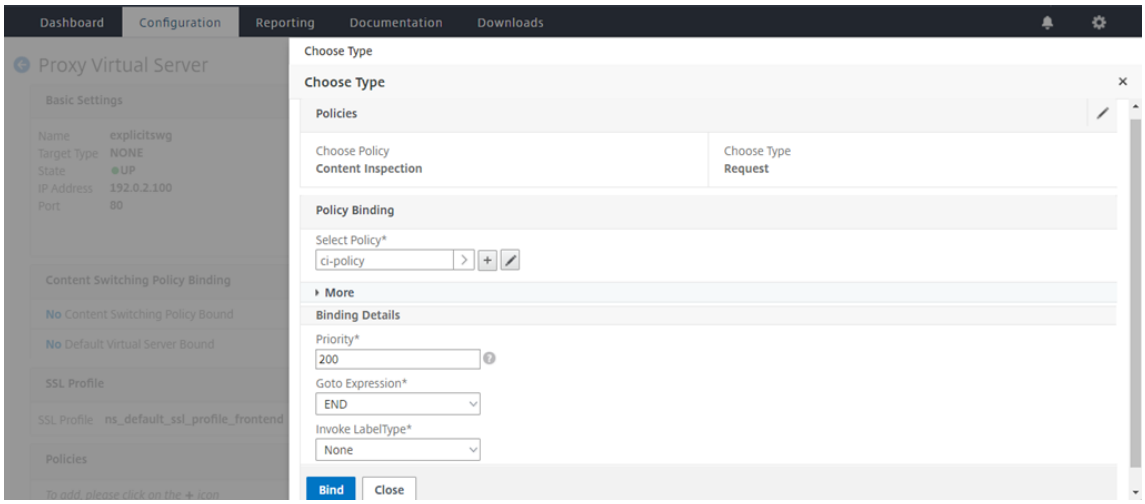



12. En la página **Crear directiva ICAP**, escriba true en el **Editor de expresiones**. A continuación, haga clic en **Crear**.

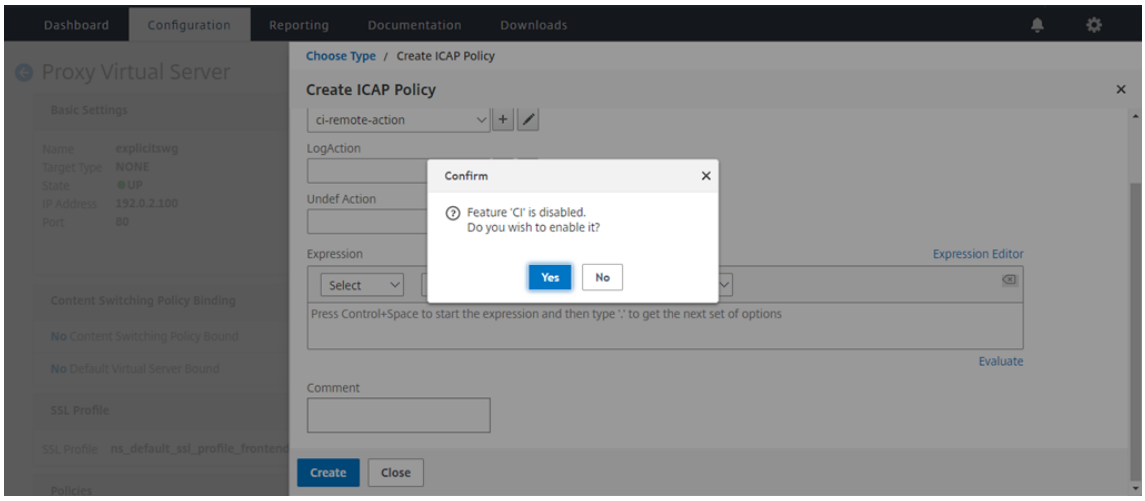


13. Haga clic en **Bind**.

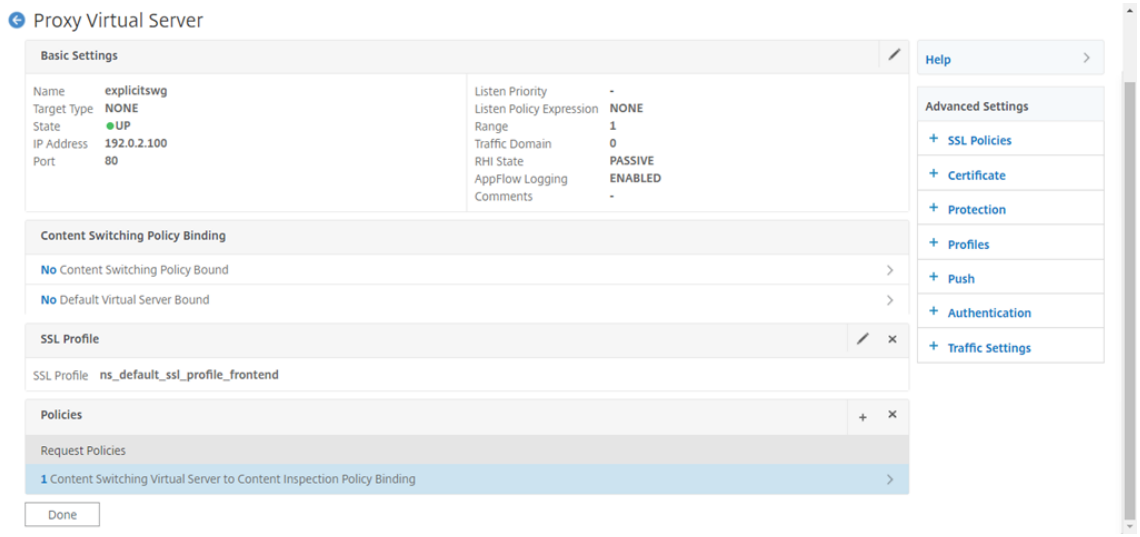



14. Cuando se le pida que active la función de inspección de contenido, seleccione **Sí**.




15. Haga clic en **Done**.




## ICAP seguro

Puede establecer una conexión segura entre el dispositivo SWG y los servidores ICAP. Para ello, cree un servicio SSL_TCP en lugar de un servicio TCP. Configure un servidor virtual de equilibrio de carga de tipo SSL_TCP. Enlazar el servicio ICAP al servidor virtual de equilibrio de carga.

### Configurar ICAP seguro mediante la CLI

En el símbolo del sistema, escriba:

- `add service <name> <IP> SSL_TCP <port>`
- `add lb vserver <name> <serviceType> <IPAddress> <port>`
- `bind lb vserver <name> <serviceName>`

**Ejemplo**:

```
1 add service icap_svc 203.0.113.100 SSL_TCP 1344
2
3 add lbvserver lbicap SSL_TCP 0.0.0.0 0
4
5 bind lb vserver lbicap icap_svc
6 <!--NeedCopy-->
```

### Configurar ICAP seguro mediante la interfaz gráfica de usuario

1. Desplácese hasta **Equilibrio de carga** > **Servidores virtuales** y haga clic en **Agregar**.
2. Especifique un nombre para el servidor virtual, la dirección IP y el puerto. Especifique el protocolo como SSL_TCP.

3. Haga clic en **OK**.
4. Haga clic dentro de la sección **Enlace de servicio de servidor virtual de equilibrio de carga** para agregar un servicio ICAP.
5. Haga clic en “+”para agregar un servicio.
6. Especifique un nombre de servicio, una dirección IP, un protocolo (SSL_TCP) y un puerto (el puerto predeterminado para ICAP seguro es 11344).
7. Haga clic en **OK**.
8. Haga clic en **Done**.
9. Haga clic en **Bind**.
10. Haga clic en **Continuar** dos veces.
11. Haga clic en **Done**.

### Limitaciones

No se admiten las siguientes características:

- Almacenamiento en caché de respuesta ICAP.
- Insertando encabezado X-auth-User-URI.
- Insertar la solicitud HTTP en la solicitud ICAP en RESPMOD.

## Integración con IPS o NGFW como dispositivos en línea

April 27, 2021

Los dispositivos de seguridad como el sistema de prevención de intrusiones (IPS) y el firewall de próxima generación (NGFW) protegen los servidores contra ataques de red. Estos dispositivos pueden inspeccionar el tráfico en vivo y, por lo general, se implementan en el modo en línea de capa 2. Citrix Secure Web Gateway (SWG) proporciona seguridad a los usuarios y a la red empresarial al acceder a recursos en Internet.

Un dispositivo Citrix SWG se puede integrar con uno o más dispositivos en línea para evitar amenazas y proporcionar protección de seguridad avanzada. Los dispositivos en línea pueden ser cualquier dispositivo de seguridad, como IPS y NGFW.

Algunos casos de uso en los que puede beneficiarse con el dispositivo Citrix SWG y la integración de dispositivos en línea son:

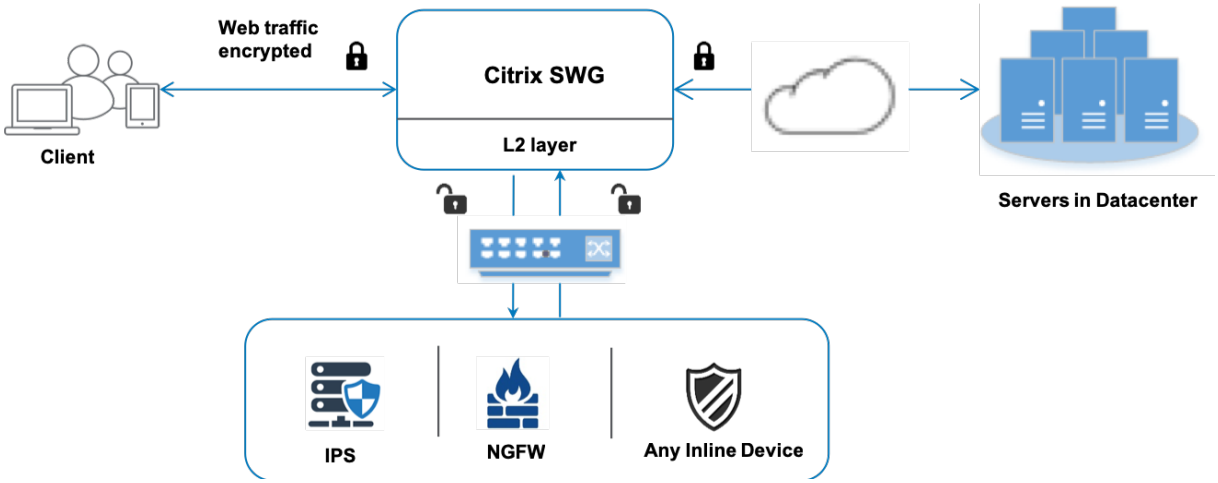
- **Inspección del tráfico cifrado:** la mayoría de los dispositivos IPS y NGFW evitan el tráfico cifrado, lo que puede dejar a los servidores vulnerables a los ataques. Un dispositivo Citrix SWG puede descifrar el tráfico y enviarlo a los dispositivos en línea para su inspección. Esta integración mejora la seguridad de la red del cliente.

- **Descarga de dispositivos en línea del procesamiento TLS/SSL: El procesamiento** TLS/SSL es costoso, lo que puede resultar en una alta utilización de CPU en dispositivos IPS o NGFW si también descifran el tráfico. Un dispositivo Citrix SWG ayuda a descargar el procesamiento TLS/SSL de los dispositivos en línea. Como resultado, los dispositivos en línea pueden inspeccionar un mayor volumen de tráfico.
- **Equilibrio de carga de dispositivos en línea:** si ha configurado varios dispositivos en línea para administrar el tráfico pesado, un dispositivo Citrix SWG puede equilibrar la carga y distribuir el tráfico de manera uniforme a estos dispositivos.
- **Selección inteligente del tráfico:** en lugar de enviar todo el tráfico al dispositivo en línea para su inspección, el dispositivo realiza una selección inteligente del tráfico. Por ejemplo, omite el envío de archivos de texto para su inspección a los dispositivos en línea.

### Integración de Citrix SWG con dispositivos en línea

El siguiente diagrama muestra cómo se integra un Citrix SWG con dispositivos de seguridad en línea.




Cuando integra dispositivos en línea con el dispositivo Citrix SWG, los componentes interactúan de la siguiente manera:

1. Un cliente envía una solicitud a un dispositivo Citrix SWG.
2. El dispositivo envía los datos al dispositivo en línea para la inspección de contenido en función de la evaluación de directivas. Para el tráfico HTTPS, el dispositivo descifra los datos y los envía en texto sin formato al dispositivo en línea para la inspección del contenido.

> **Nota:**
>
> Si hay dos o más dispositivos en línea, la carga del dispositivo equilibra los dispositivos y envía el tráfico.

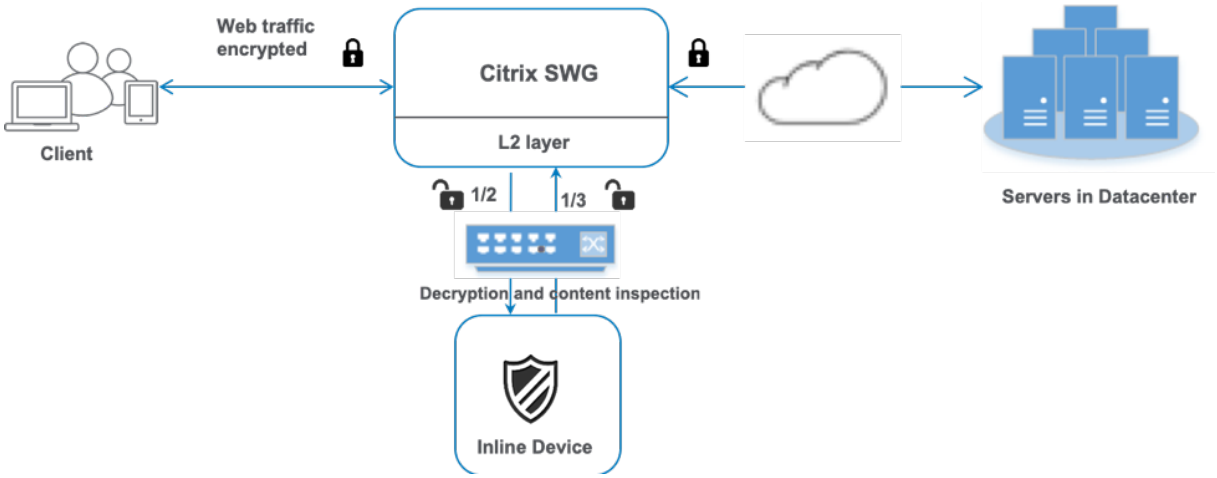
3. El dispositivo en línea inspecciona los datos en busca de amenazas y decide si quiere eliminar, restablecer o enviar los datos al dispositivo.
4. Si hay amenazas de seguridad, el dispositivo modifica los datos y los envía al dispositivo.
5. Para el tráfico HTTPS, el dispositivo vuelve a cifrar los datos y reenvía la solicitud al servidor back-end.
6. El servidor back-end envía la respuesta al dispositivo.
7. El dispositivo vuelve a descifrar los datos y los envía al dispositivo en línea para su inspección.
8. El dispositivo en línea inspecciona los datos. Si hay amenazas de seguridad, el dispositivo modifica los datos y los envía al dispositivo.
9. El dispositivo vuelve a cifrar los datos y envía la respuesta al cliente.

## Configuración de la integración de dispositivos en línea

Puede configurar un dispositivo Citrix SWG con un dispositivo en línea de tres maneras diferentes, como se indica a continuación:

### Caso 1: Uso de un único dispositivo en línea

Para integrar un dispositivo de seguridad (IPS o NGFW) en modo en línea, debe habilitar la inspección de contenido y el reenvío basado en MAC (MBF) en modo global en el dispositivo SWG. A continuación, agregue un perfil de inspección de contenido, un servicio TCP, una acción de inspección de contenido para que los dispositivos en línea restablezcan, bloqueen o descarten el tráfico basándose en la inspección. Agregue también una directiva de inspección de contenido que el dispositivo utiliza para decidir el subconjunto de tráfico que se va a enviar a los dispositivos en línea. Por último, configure el servidor virtual proxy con la conexión de capa 2 habilitada en el servidor y vincule la directiva de inspección de contenido a este servidor virtual proxy.



Siga estos pasos:

1. Habilite el modo de reenvío basado en Mac (MPF).
2. Habilite la función de inspección de contenido.
3. Agregue un perfil de inspección de contenido para el servicio. El perfil de inspección de contenido contiene la configuración del dispositivo en línea que integra el dispositivo SWG con un dispositivo en línea.
4. (Opcional) Agregue un monitor TCP.

   > **Nota:**
   >
   > Los dispositivos transparentes no tienen una dirección IP. Por lo tanto, para realizar comprobaciones de estado, debe vincular explícitamente un monitor.

5. Agregar un servicio. Un servicio representa un dispositivo en línea.
6. (Opcional) Enlazar el servicio al monitor TCP.
7. Agregue una acción de inspección de contenido para el servicio.
8. Agregue una directiva de inspección de contenido y especifique la acción.
9. Agregue un servidor virtual de proxy HTTP o HTTPS (cambio de contenido).
10. Enlazar la directiva de inspección de contenido al servidor virtual.

**Configuración mediante la CLI** Escriba los siguientes comandos en el símbolo del sistema. Los ejemplos se dan después de la mayoría de los comandos.

1. Habilitar MBF.

   ```
   enable ns mode mbf
   <!--NeedCopy-->
   ```

2. Habilite la función.

   ```
   enable ns feature contentInspection
   <!--NeedCopy-->
   ```

3. Agregar un perfil de inspección de contenido.

   ```
   add contentInspection profile <name> -type InlineInspection -
       egressInterface <interface_name> -ingressInterface <
       interface_name>[-egressVlan <positive_integer>] [-ingressVlan <
       positive_integer>]
   <!--NeedCopy-->
   ```

   **Ejemplo:**

```
add contentInspection profile ipsprof -type InlineInspection -
    ingressinterface "1/2" -egressInterface "1/3"
<!--NeedCopy-->
```

4. Agregar un servicio. Especifique una dirección IP ficticia que no sea propiedad de ninguno de los dispositivos, incluidos los dispositivos en línea. Establezca `use source IP address` (USIP) en YES. Ajuste `useproxyport` en NO. Apague el monitor de salud. Active la supervisión de estado solo si vincula este servicio a un monitor TCP. Si vincula un monitor a un servicio, establezca la opción TRANSPARENTE del monitor en ON.

```
add service <service_name>  <IP> TCP <Port> -
    contentinspectionProfileName <Name>  -healthMonitor NO  -usip
    YES  – useproxyport NO
<!--NeedCopy-->
```

**Ejemplo:**

```
add service ips_service 198.51.100.2 TCP * -healthMonitor YES -
    usip YES -useproxyport NO -contentInspectionProfileName ipsprof

<!--NeedCopy-->
```

5. Agregar una acción de inspección de contenido.

```
add contentInspection action <name> -type INLINEINSPECTION -
    serverName <string>
<!--NeedCopy-->
```

**Ejemplo:**

```
add contentInspection action ips_action -type INLINEINSPECTION -
    serverName ips_service
<!--NeedCopy-->
```

6. Agregar una directiva de inspección de contenido.

```
add contentInspection policy <name> -rule <expression> -action <
    string>
<!--NeedCopy-->
```

**Ejemplo:**

```
add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE("
    CONNECT")" -action ips_action
<!--NeedCopy-->
```

7. Agregue un servidor virtual proxy.

```
add cs vserver <name> PROXY <IPAddress> <port> -cltTimeout <secs>
    -Listenpolicy <expression> -authn401 ( ON | OFF ) -authnVsName
    <string> -l2Conn ON
```

```
<!--NeedCopy-->
```

**Ejemplo:**

```
add cs vserver transparentcs PROXY * * -cltTimeout 180 -
   Listenpolicy exp1 -authn401 on -authnVsName swg-auth-vs-trans-
   http -l2Conn ON
<!--NeedCopy-->
```

8. Enlazar la directiva al servidor virtual.

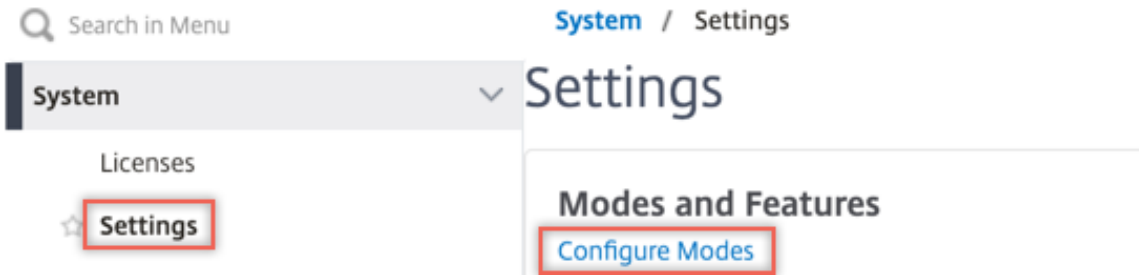
```
bind cs vserver <name> -policyName <string> -priority <
   positive_integer> -gotoPriorityExpression <expression> -type
   REQUEST
<!--NeedCopy-->
```

**Ejemplo:**

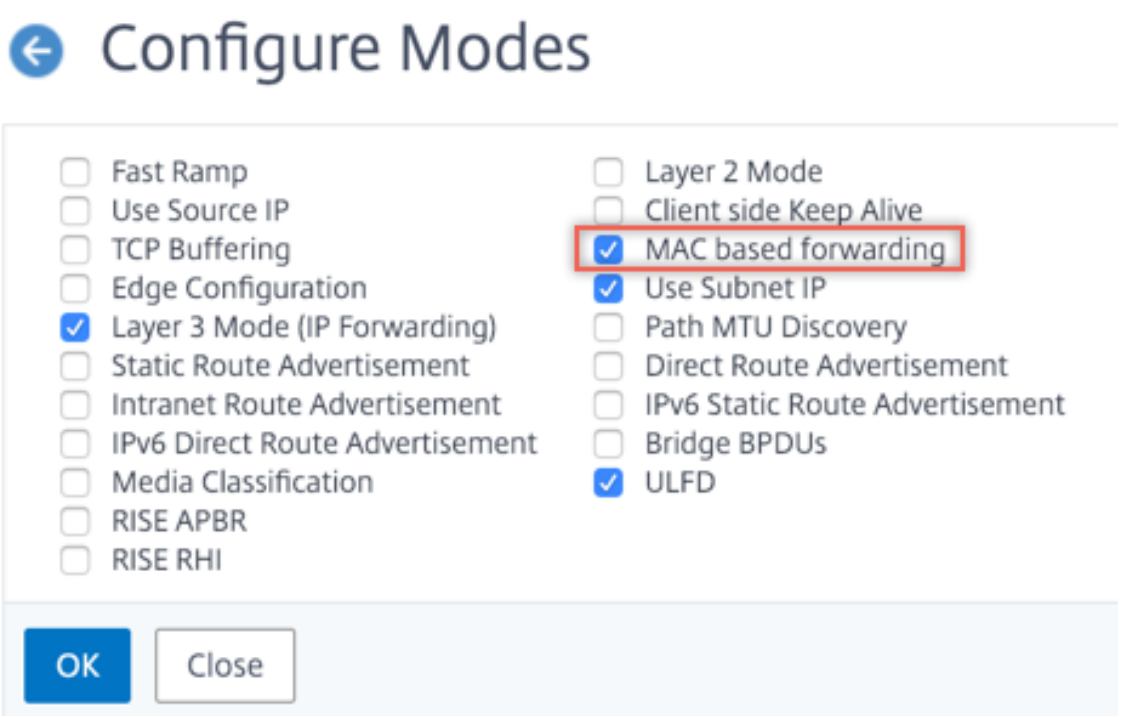
```
bind cs vserver explicitcs -policyName ips_pol -priority 1 -
   gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```

### Configuración mediante la GUI

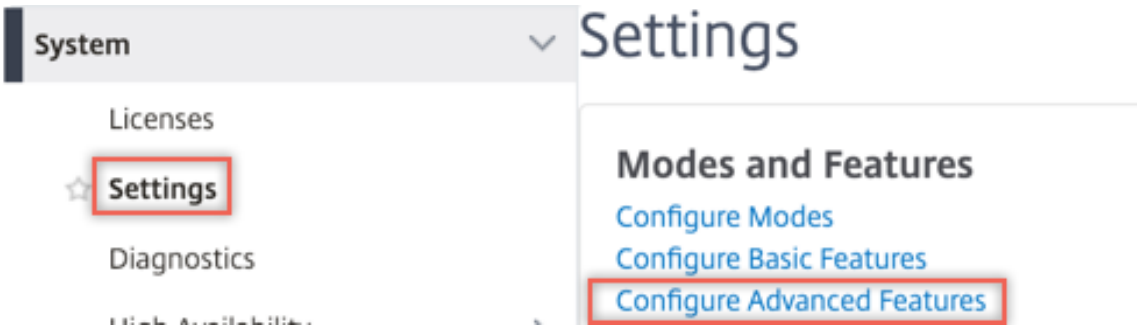
1. Vaya a **Sistema > Configuración**. En **Modos y funciones**, haga clic en **Configurar modos**.



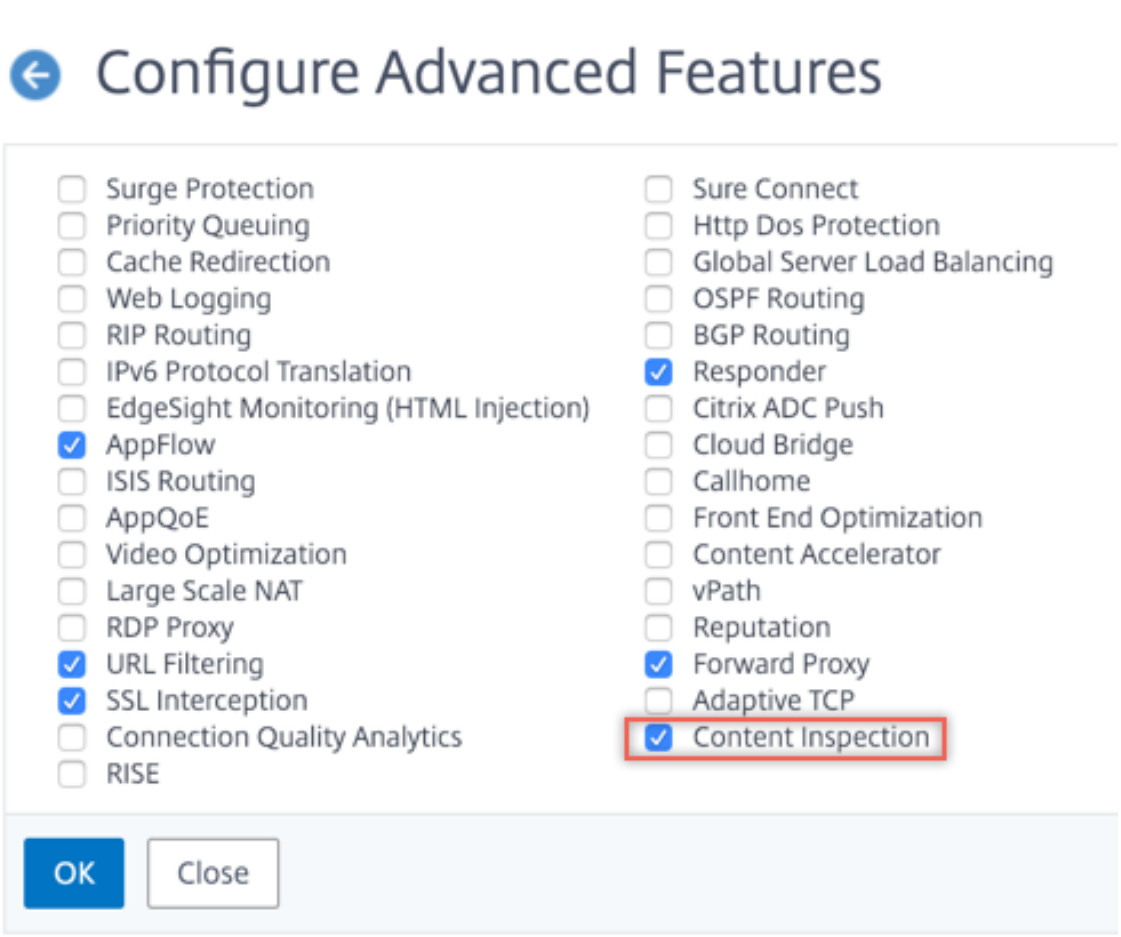

 



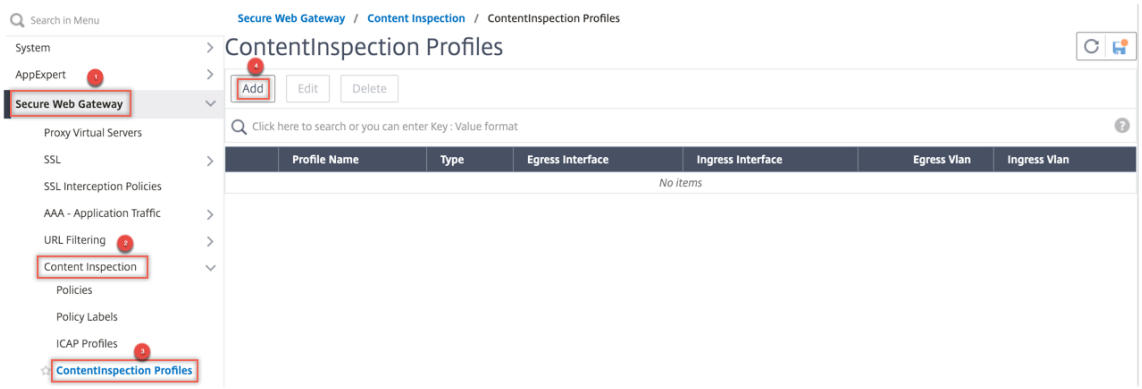

2. Vaya a **Sistema > Configuración**. En **Modos y funciones**, haga clic en **Configurar funciones avanzadas**.





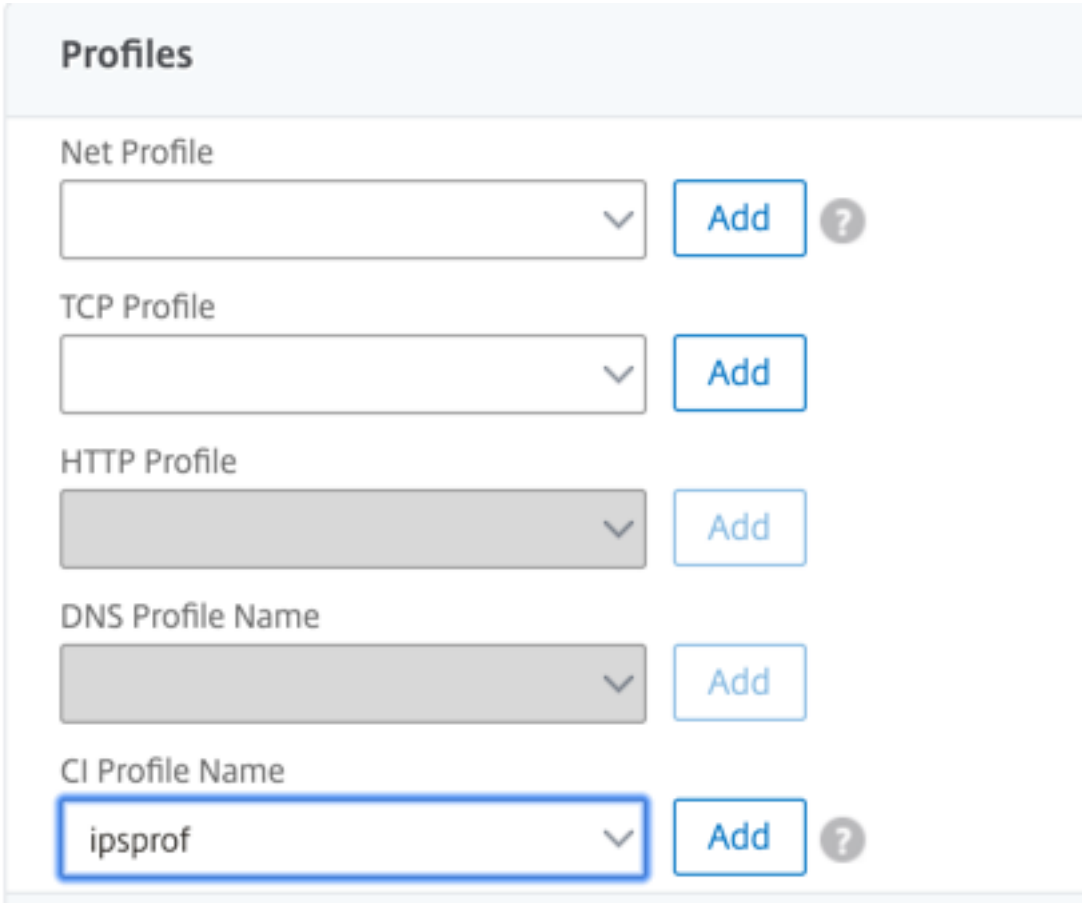

3. Vaya a **Secure Web Gateway > Inspección de contenido > Perfiles de inspección de contenido**. Haga clic en **Agregar**.

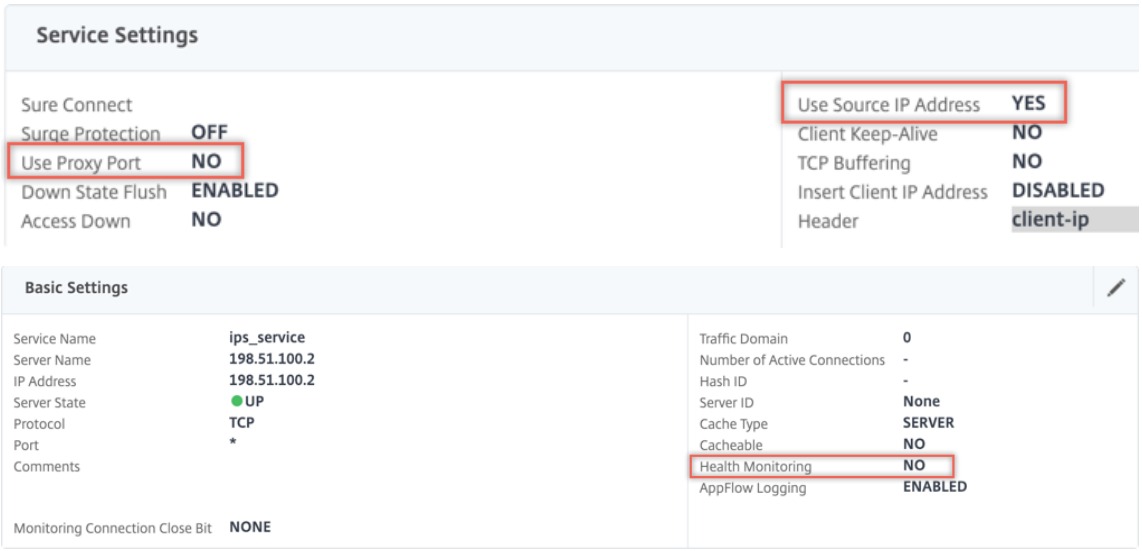



4. Desplácese hasta **Equilibrio de carga > Servicios > Agregar** y agregar un servicio. En **Configuración avanzada**, haga clic en **Perfiles**. En la lista **Nombre de perfil de CI**, seleccione el perfil de inspección de contenido creado anteriormente. En **Configuración del servicio**, establezca **Usar dirección IP de origen**en YES y **Usar puerto proxy**en No. En **Configuración básica**, establezca **Supervisión del estado**en NO. Active la supervisión de estado solo si vincula este ser-

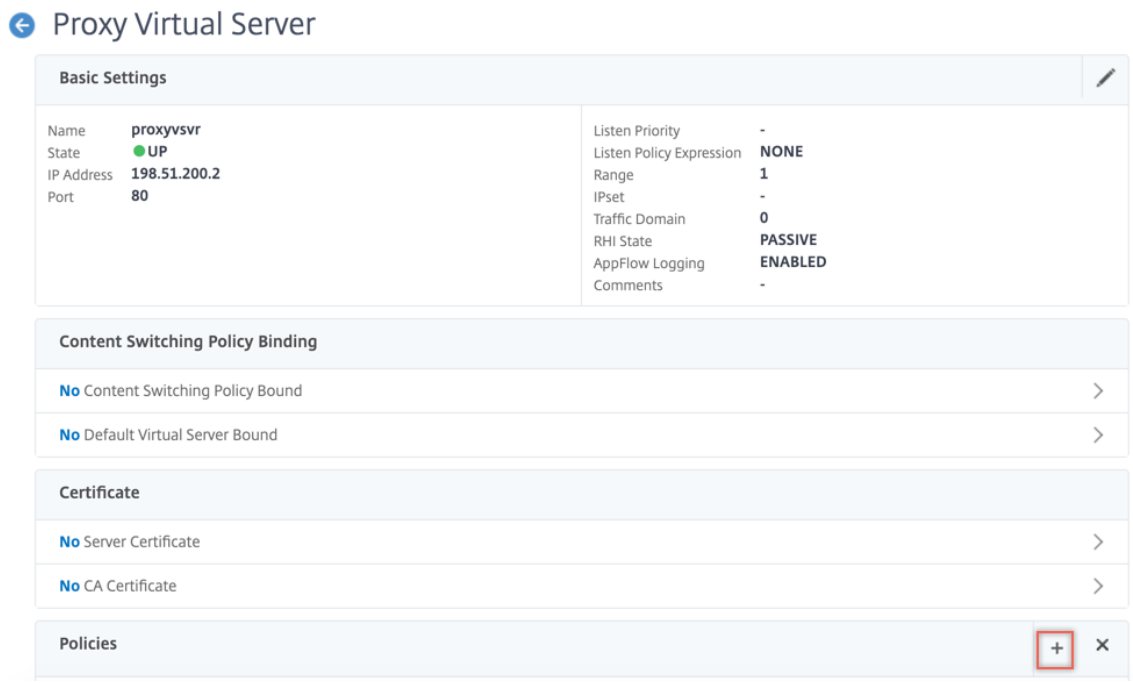
vicio a un monitor TCP. Si vincula un monitor a un servicio, establezca la opción TRANSPARENTE en monitor en ON.



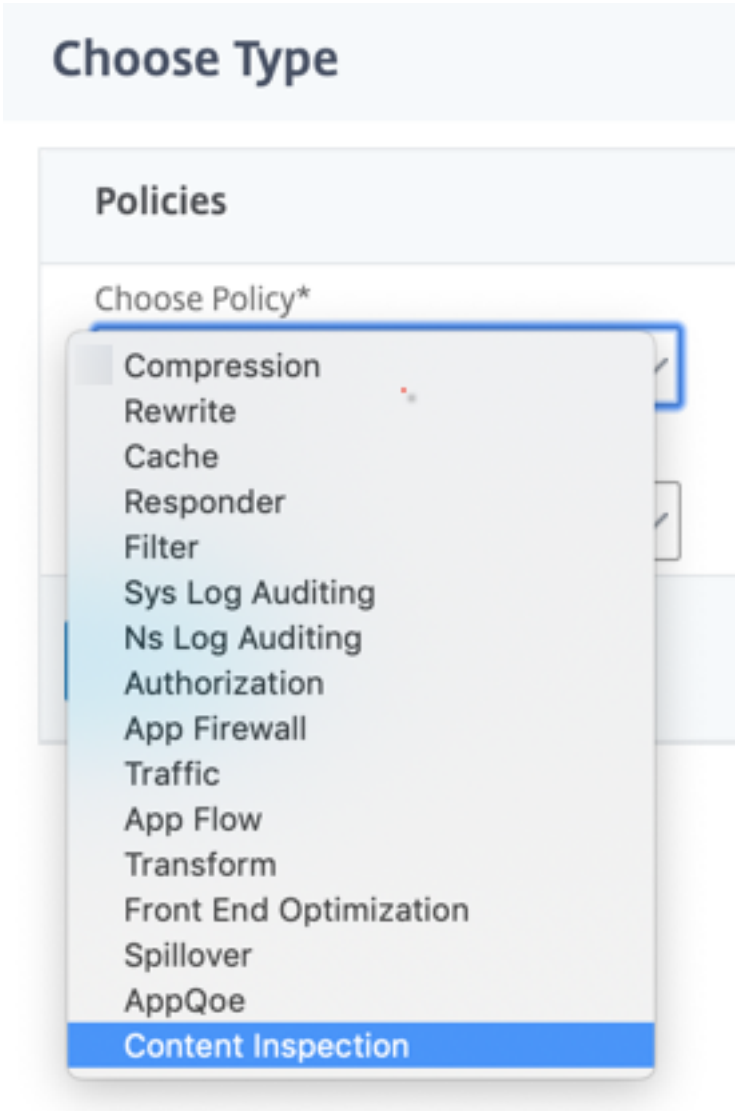

5. Vaya a **Secure Web Gateway > Servidores virtuales Proxy > Agregar**. Especifique un nombre, una dirección IP y un puerto. En **Configuración avanzada**, seleccione **Directivas**. Haga clic en el signo “+”.



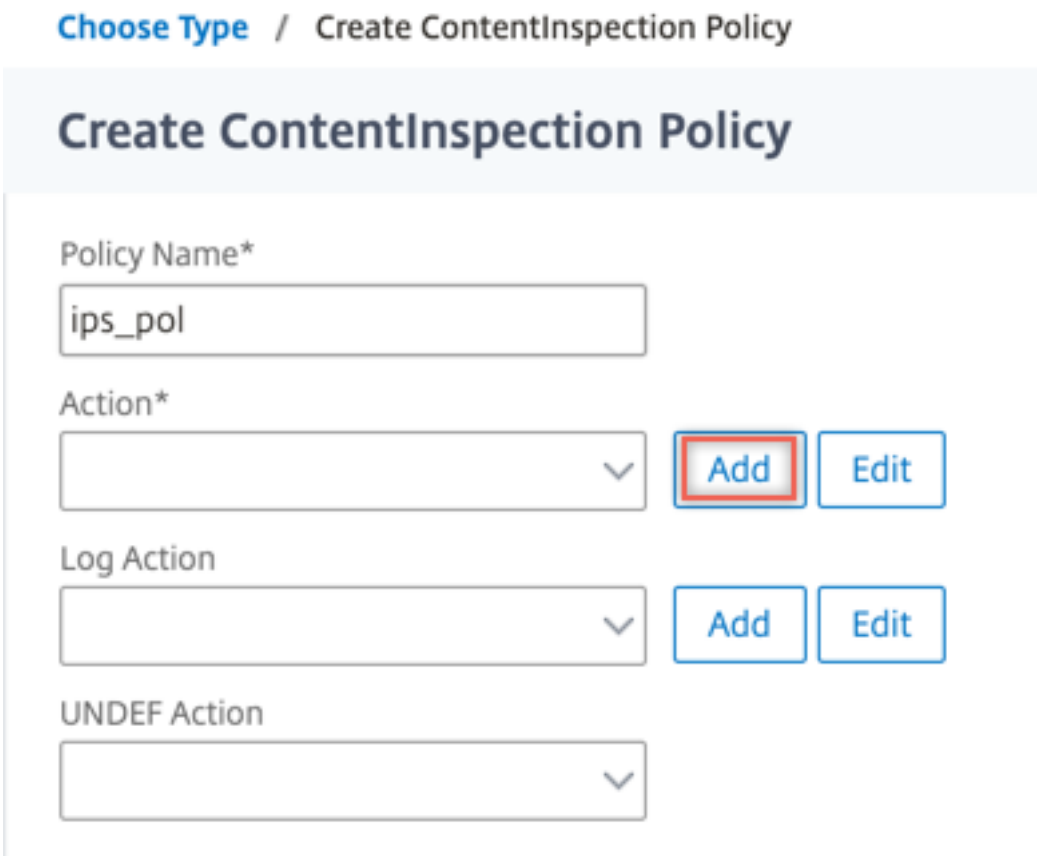

6. En **Elegir directiva**, seleccione **Inspección de contenido**. Haga clic en **Continuar**.



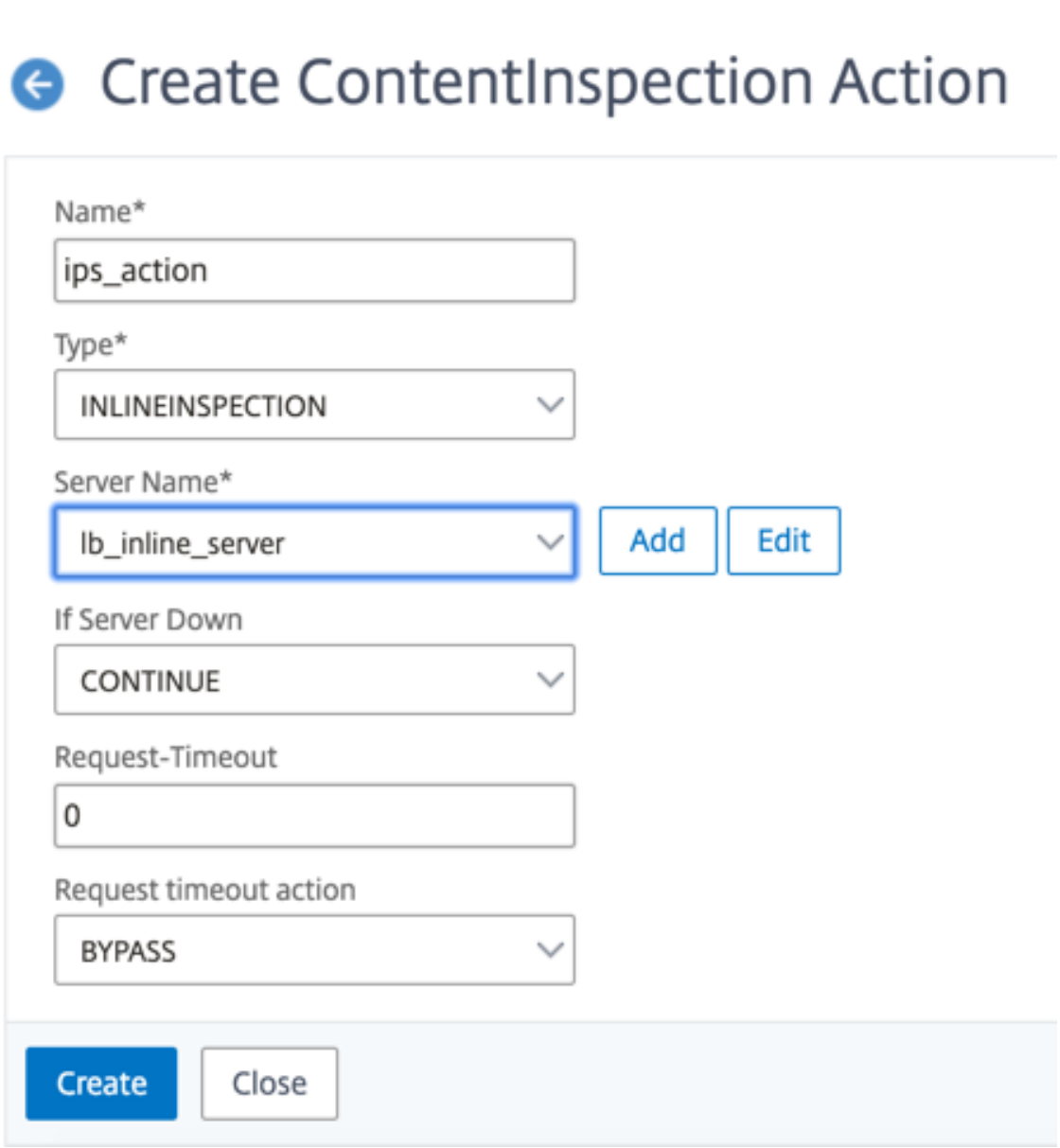

7. Haga clic en **Agregar**. Especifique un nombre. En **Acción**, haga clic en **Agregar**.



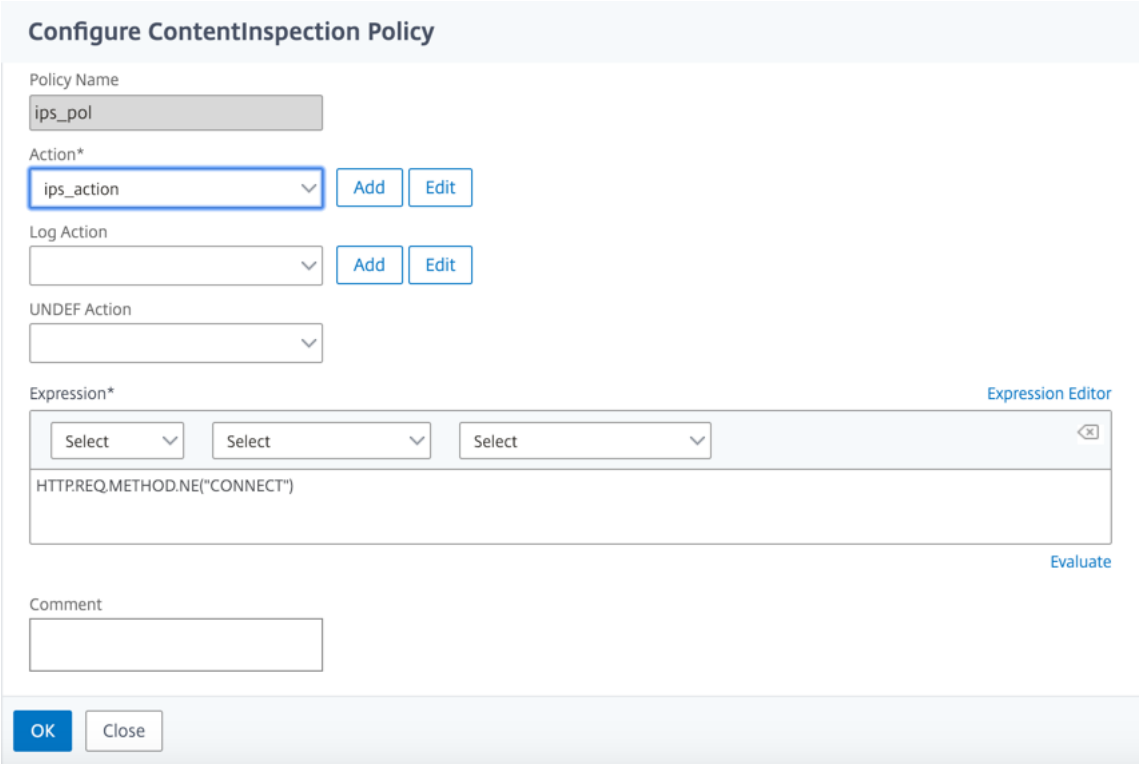

8. Especifique un nombre. En **Tipo**, seleccione **INLINEINSPECTION**. En **Nombre del servidor**, seleccione el servicio TCP creado anteriormente.




9. Haga clic en **Crear**. Especifique la regla y haga clic en **Crear**.

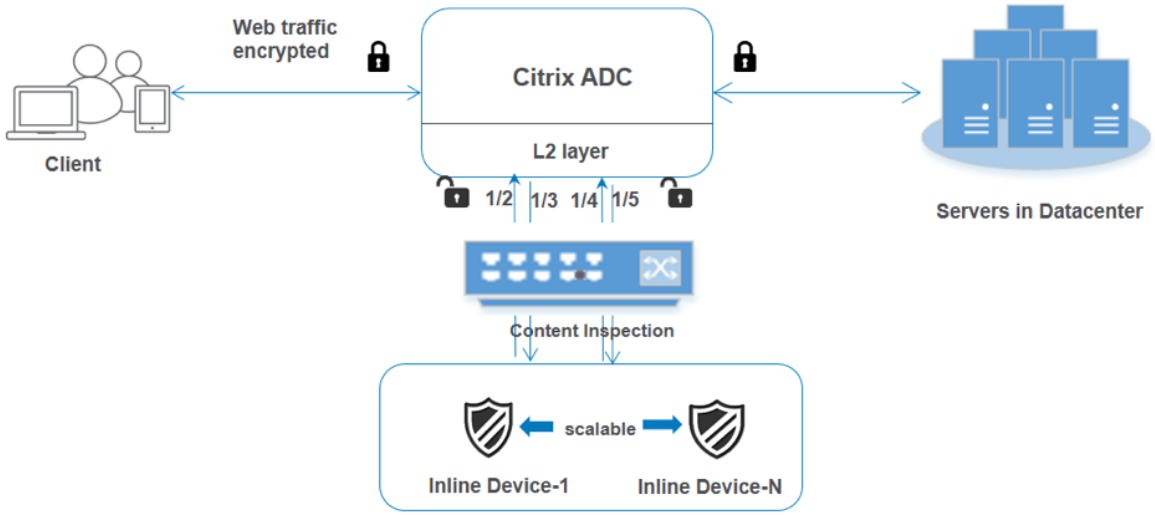



10. Haga clic en **Bind**.
11. Haga clic en **Done**.

### Caso 2: Equilibrio de carga de varios dispositivos en línea con interfaces dedicadas

Si utiliza dos o más dispositivos en línea, puede equilibrar la carga de los dispositivos mediante diferentes servicios de inspección de contenido con interfaces dedicadas. En este caso, la carga del dispositivo Citrix SWG equilibra el subconjunto de tráfico enviado a cada dispositivo a través de una interfaz dedicada. El subconjunto se decide en función de las directivas configuradas. Por ejemplo, es posible que los archivos TXT o de imagen no se envíen para su inspección a los dispositivos en línea.




La configuración básica sigue siendo la misma que en el caso 1. Sin embargo, debe crear un perfil de inspección de contenido para cada dispositivo en línea y especificar la interfaz de entrada y salida en cada perfil. Agregue un servicio para cada dispositivo en línea. Agregue un servidor virtual de equilibrio de carga y especifíquelo en la acción de inspección de contenido. Realice los siguientes pasos adicionales:

1. Agregue perfiles de inspección de contenido para cada servicio.
2. Agregue un servicio para cada dispositivo.
3. Agregue un servidor virtual de equilibrio de carga.
4. Especifique el servidor virtual de equilibrio de carga en la acción de inspección de contenido.

**Configuración mediante la CLI** Escriba los siguientes comandos en el símbolo del sistema. Se dan ejemplos después de cada comando.

1. Habilitar MBF.

```
enable ns mode mbf
<!--NeedCopy-->
```

2. Habilite la función.

```
enable ns feature contentInspection
<!--NeedCopy-->
```

3. Agregar perfil 1 para el servicio 1.

```
add contentInspection profile <name> -type InlineInspection -
    egressInterface <interface_name> -ingressInterface <
    interface_name>[-egressVlan <positive_integer>] [-ingressVlan <
    positive_integer>]
```

```
<!--NeedCopy-->
```

**Ejemplo:**

```
add contentInspection profile ipsprof1 -type InlineInspection -
    ingressInterface "1/2" -egressInterface "1/3"
<!--NeedCopy-->
```

4. Agregar perfil 2 para el servicio 2.

```
add contentInspection profile <name> -type InlineInspection -
    egressInterface <interface_name> -ingressInterface <
    interface_name>[-egressVlan <positive_integer>] [-ingressVlan <
    positive_integer>]
<!--NeedCopy-->
```

**Ejemplo:**

```
add contentInspection profile ipsprof2 -type InlineInspection -
    ingressInterface "1/4" -egressInterface "1/5"
<!--NeedCopy-->
```

5. Agregar servicio 1. Especifique una dirección IP ficticia que no sea propiedad de ninguno de los dispositivos, incluidos los dispositivos en línea. Establezca `use source IP address` (USIP) en YES. Ajuste `useproxyport` en NO. Apague el monitor de salud. Active la supervisión de estado solo si vincula este servicio a un monitor TCP. Si vincula un monitor a un servicio, establezca la opción TRANSPARENTE del monitor en ON.

```
add service <service_name>  <IP> TCP <Port> -
    contentinspectionProfileName <Name>  -healthMonitor NO  -usip
    YES  – useproxyport NO
<!--NeedCopy-->
```

**Ejemplo:**

```
add service ips_service1 192.168.10.2 TCP * -healthMonitor NO -
    usip YES -useproxyport NO -contentInspectionProfileName
    ipsprof1
<!--NeedCopy-->
```

6. Agregar servicio 2. Especifique una dirección IP ficticia que no sea propiedad de ninguno de los dispositivos, incluidos los dispositivos en línea. Establezca `use source IP address` (USIP) en YES. Ajuste `useproxyport` en NO. Apague el monitor de salud. Active la supervisión de estado solo si vincula este servicio a un monitor TCP. Si vincula un monitor a un servicio, establezca la opción TRANSPARENTE del monitor en ON.

```
add service <service_name>  <IP> TCP <Port> -
    contentinspectionProfileName <Name>  -healthMonitor NO  -usip
    YES  – useproxyport NO
<!--NeedCopy-->
```

**Ejemplo:**

```
add service ips_service2 192.168.10.3 TCP * -healthMonitor NO -
   usip YES -useproxyport NO  -contentInspectionProfileName
   ipsprof2
<!--NeedCopy-->
```

7. Agregue un servidor virtual de equilibrio de carga.

```
add lb vserver <LB_VSERVER_NAME> TCP <IP> <port>
<!--NeedCopy-->
```

**Ejemplo:**

```
add lb vserver lb_inline_vserver TCP 192.0.2.100 *
<!--NeedCopy-->
```

8. Enlazar los servicios al servidor virtual de equilibrio de carga.

```
bind lb vserver <LB_VSERVER_NAME> <service_name>
bind lb vserver <LB_VSERVER_NAME> <service_name>
<!--NeedCopy-->
```

**Ejemplo:**

```
bind lb vserver lb_inline_vserver ips_service1
bind lb vserver lb_inline_vserver ips_service2
<!--NeedCopy-->
```

9. Especifique el servidor virtual de equilibrio de carga en la acción de inspección de contenido.

```
add contentInspection action <name> -type INLINEINSPECTION -
   serverName <string>
<!--NeedCopy-->
```

**Ejemplo:**

```
add contentInspection action ips_action -type INLINEINSPECTION -
   serverName lb_inline_vserver
<!--NeedCopy-->
```

10. Agregar una directiva de inspección de contenido. Especifique la acción de inspección de contenido en la directiva.

```
add contentInspection policy <name> -rule <expression> -action <
   string>
<!--NeedCopy-->
```

**Ejemplo:**

```
add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE("
   CONNECT")" -action ips_action
```

```
<!--NeedCopy-->
```

11. Agregue un servidor virtual proxy.

```
add cs vserver <name> PROXY <IPAddress> <port> -l2Conn ON
<!--NeedCopy-->
```

**Ejemplo:**

```
add cs vserver transparentcs PROXY * * -l2Conn ON
<!--NeedCopy-->
```

12. Enlazar la directiva de inspección de contenido al servidor virtual.

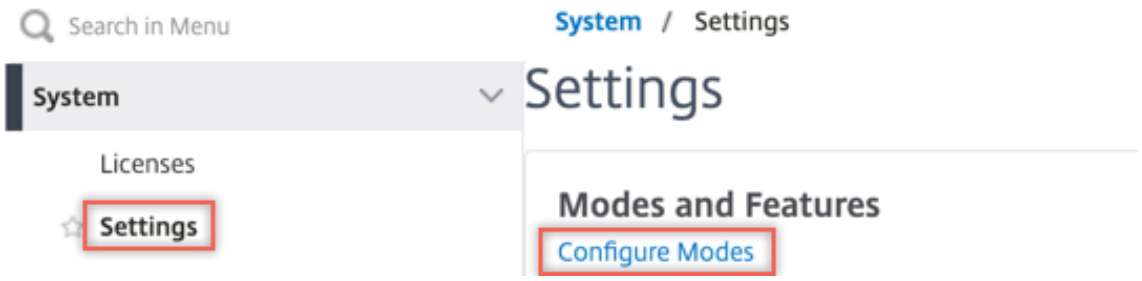
```
bind cs vserver <name> -policyName <string> -priority <
    positive_integer> -gotoPriorityExpression <expression> -type
    REQUEST
<!--NeedCopy-->
```

**Ejemplo:**

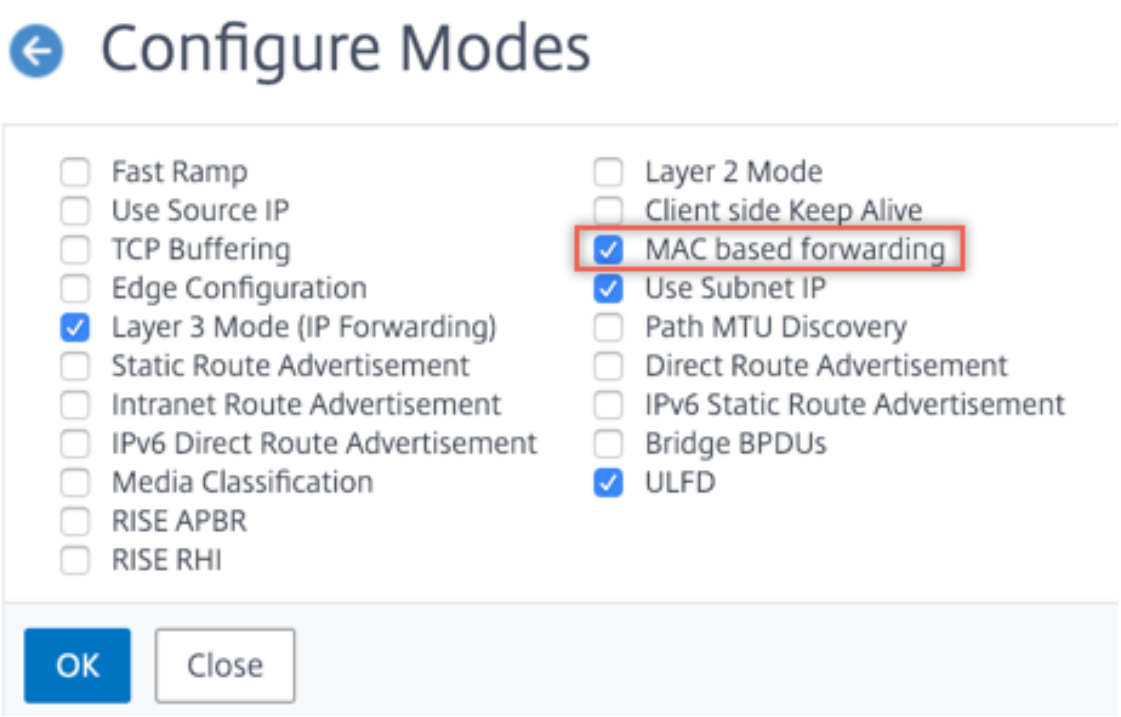
```
bind cs vserver explicitcs -policyName ips_pol -priority 1 -
    gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```

### Configuración mediante la GUI

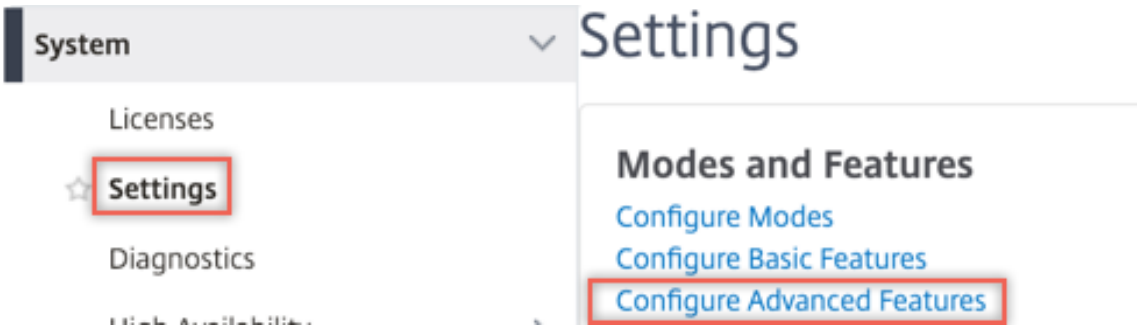
1. Vaya a **Sistema > Configuración**. En **Modos y funciones**, haga clic en **Configurar modos**.



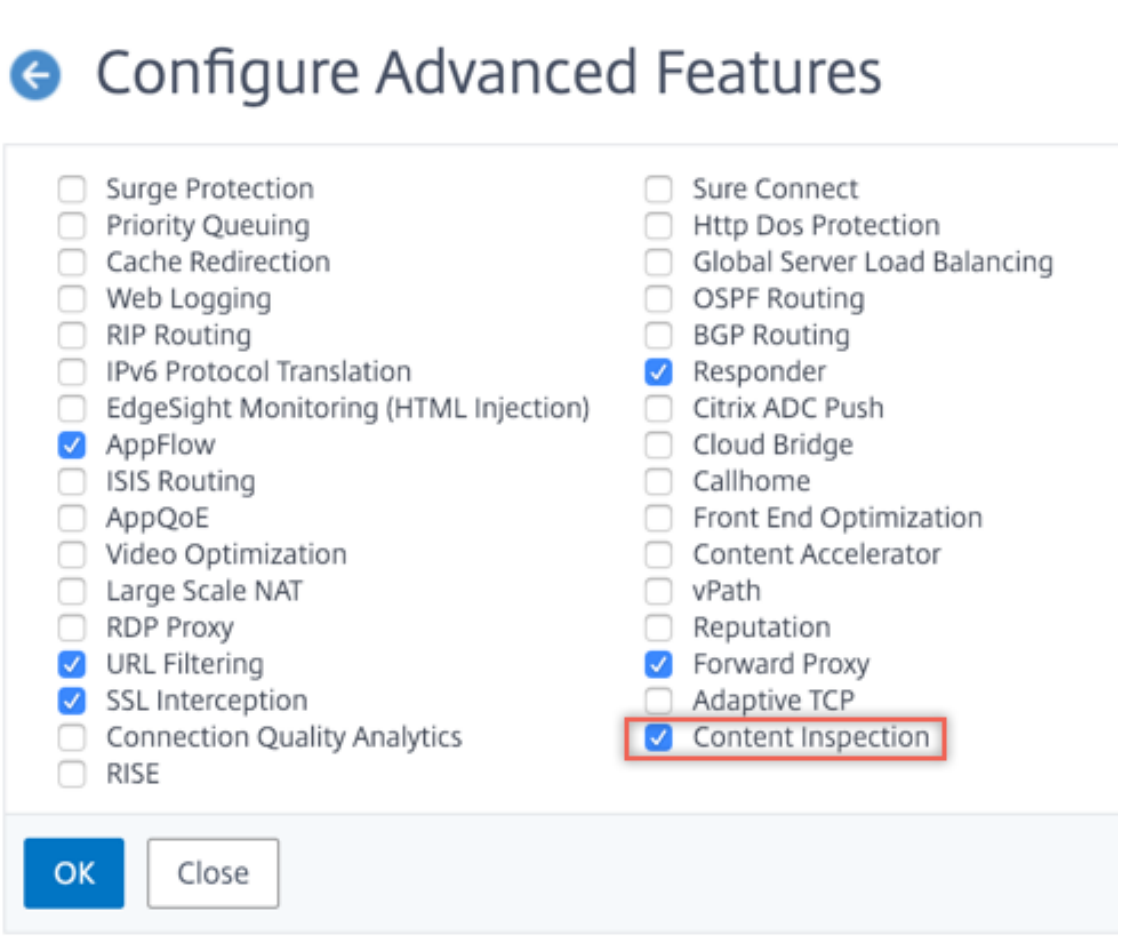

 



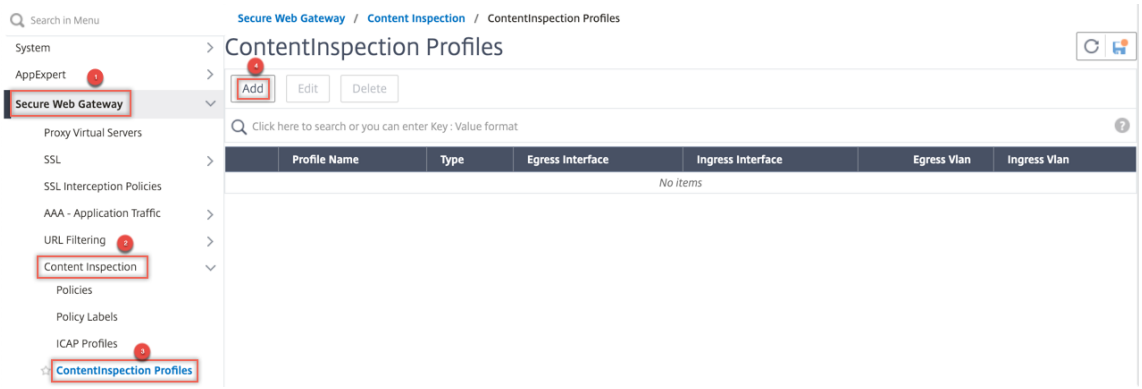

2. Vaya a **Sistema > Configuración**. En **Modos y funciones**, haga clic en **Configurar funciones avanzadas**.



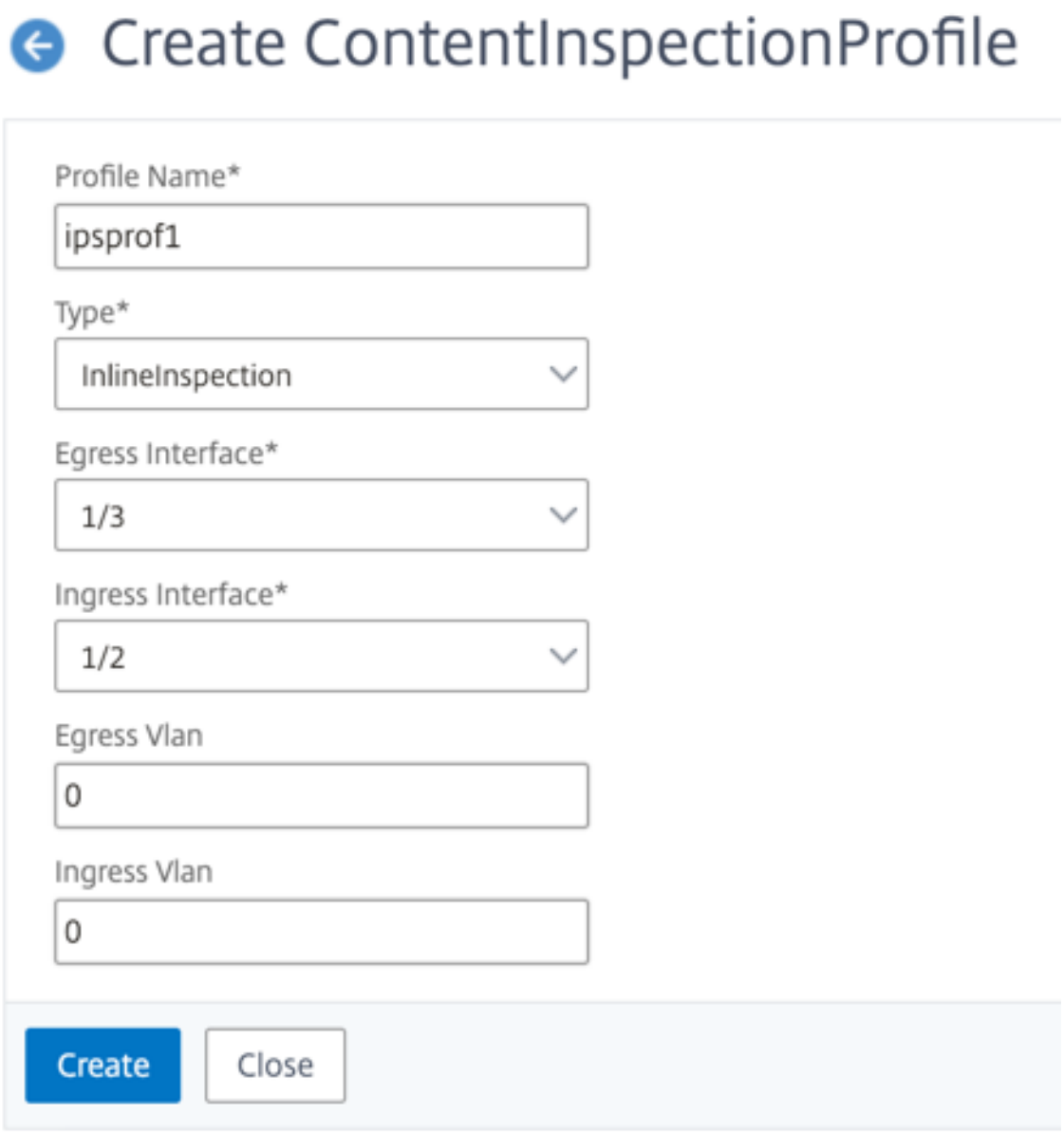



3. Vaya a **Secure Web Gateway > Inspección de contenido > Perfiles de inspección de contenido**. Haga clic en **Agregar**.




Especifique las interfaces de entrada y salida.

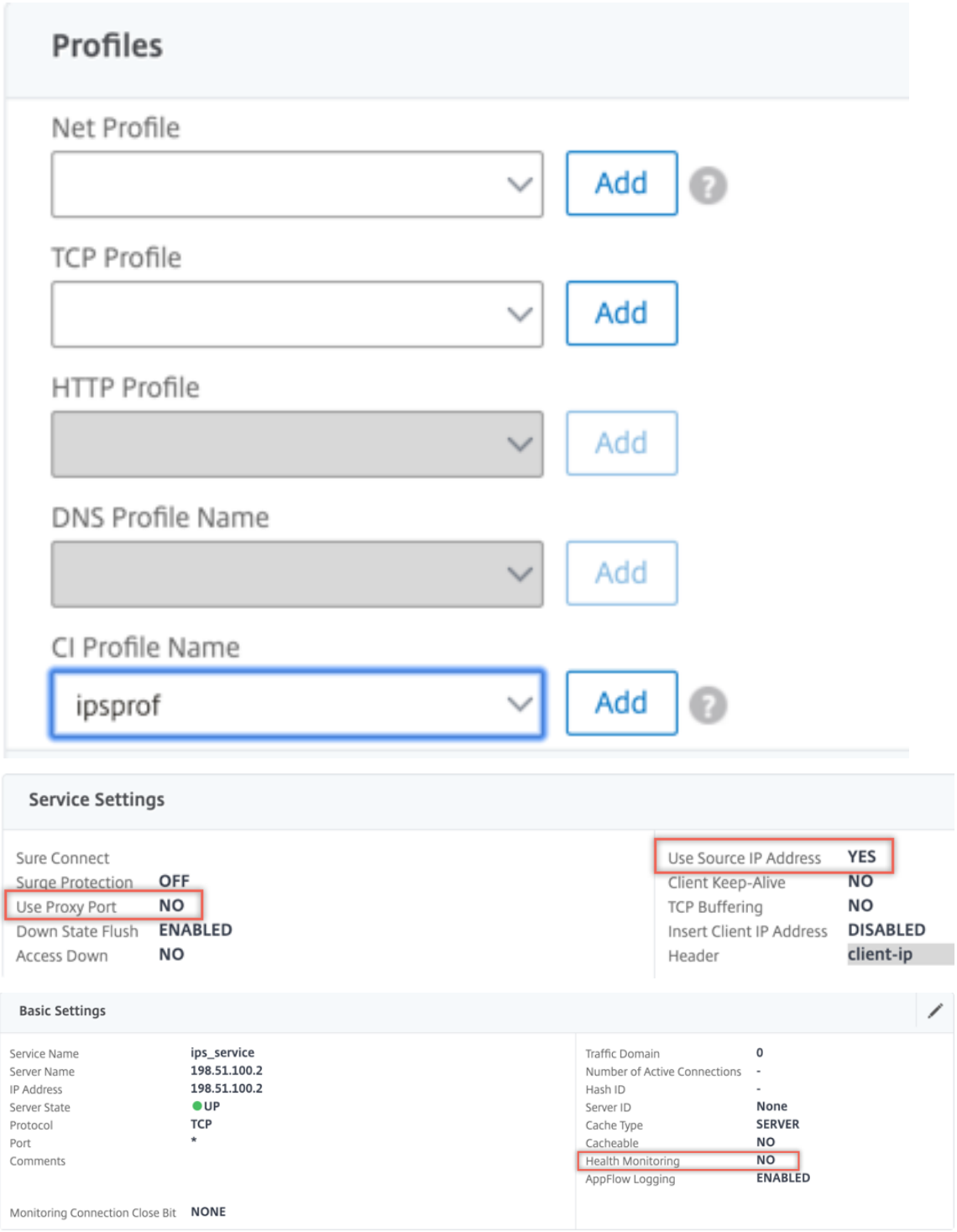
 




Cree dos perfiles. Especifique una interfaz de entrada y salida diferente en el segundo perfil.

4. Desplácese hasta **Equilibrio de carga > Servicios > Agregar** y agregar un servicio. En **Configuración avanzada**, haga clic en **Perfiles**. En la lista **Nombre de perfil de CI**, seleccione el perfil de inspección de contenido creado anteriormente. En **Configuración del servicio**, establezca **Usar dirección IP de origen**en YES y **Usar puerto proxy**en No. En **Configuración básica**, establezca **Supervisión del estado**en NO. Active la supervisión de estado solo si vincula este servicio a un monitor TCP. Si vincula un monitor a un servicio, establezca la opción TRANSPARENTE en monitor en ON.

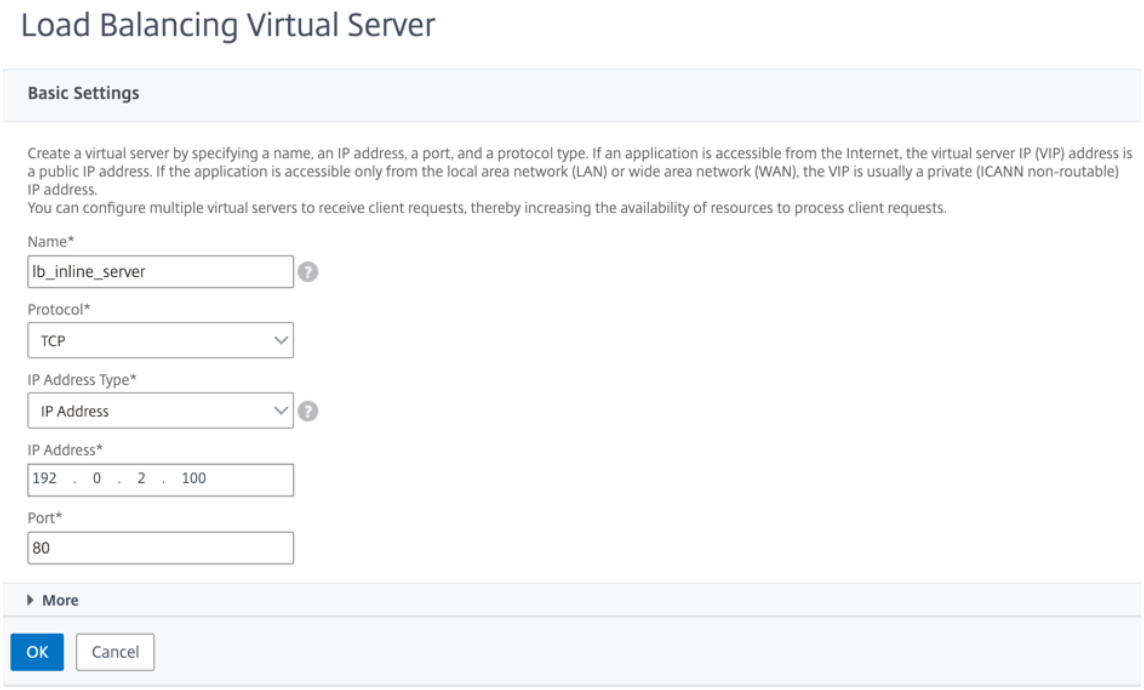
 




Cree dos servicios. Especifique direcciones IP ficticias que no pertenecen a ninguno de los dispositivos, incluidos los dispositivos en línea.

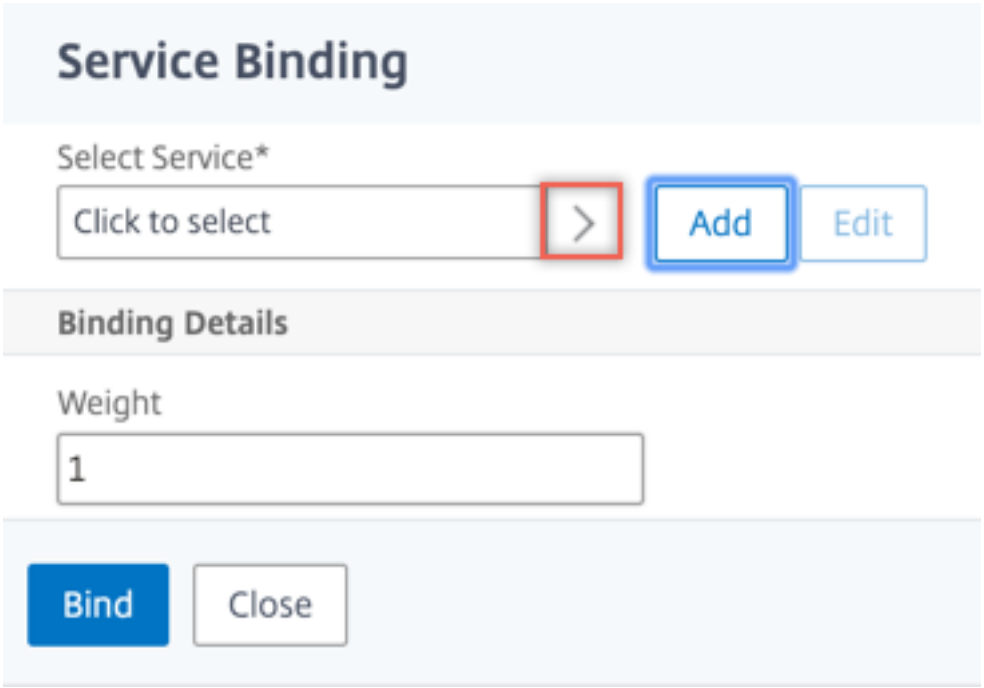
5. Desplácese hasta **Equilibrio de carga > Servidores virtuales > Agregar**. Cree un servidor virtual de equilibrio de carga TCP.

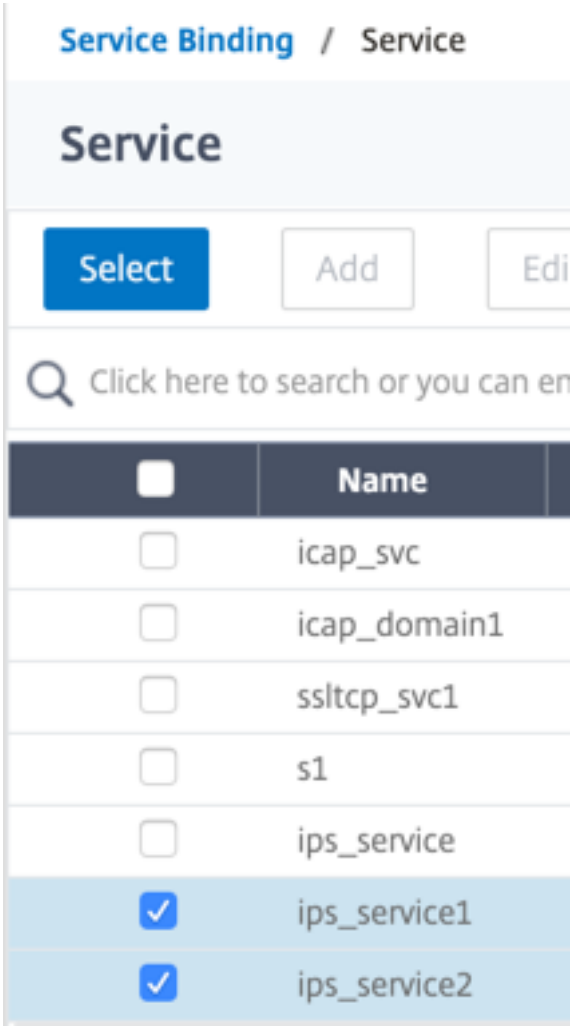



Haga clic en **OK**.

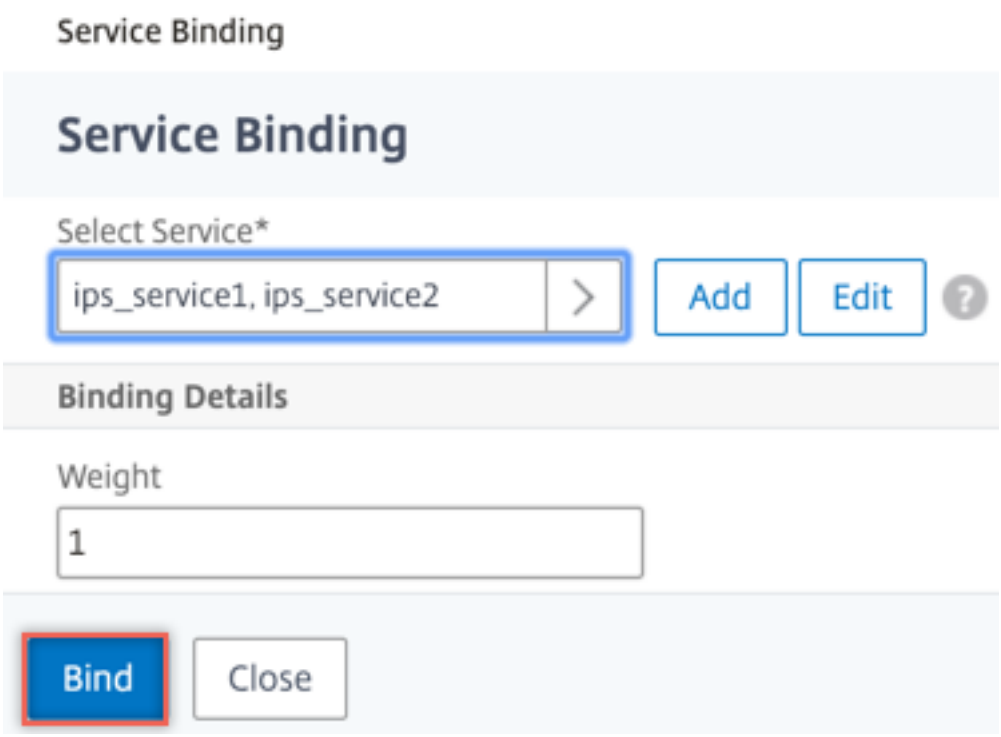
6. Haga clic dentro de la sección **Enlace del servicio de servidor virtual de equilibrio de carga**. En **Enlace de servicio**, haga clic en la flecha **de Seleccionar servicio**. Seleccione los dos servicios creados anteriormente y haga clic en **Seleccionar**. Haga clic en **Bind**.



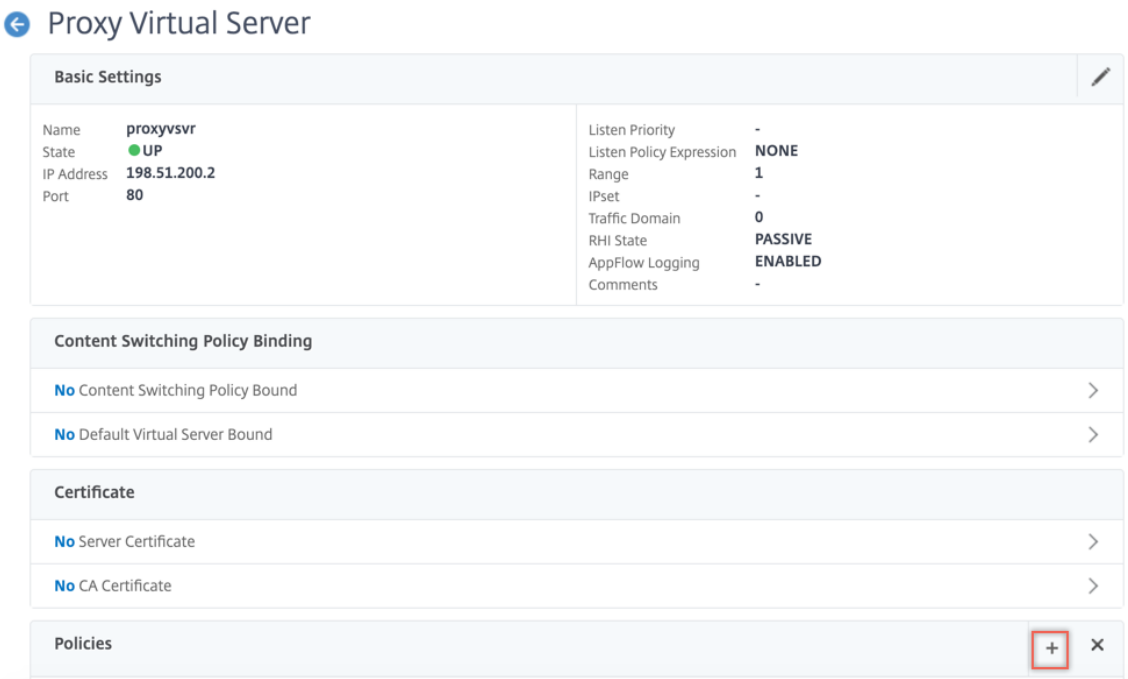

 



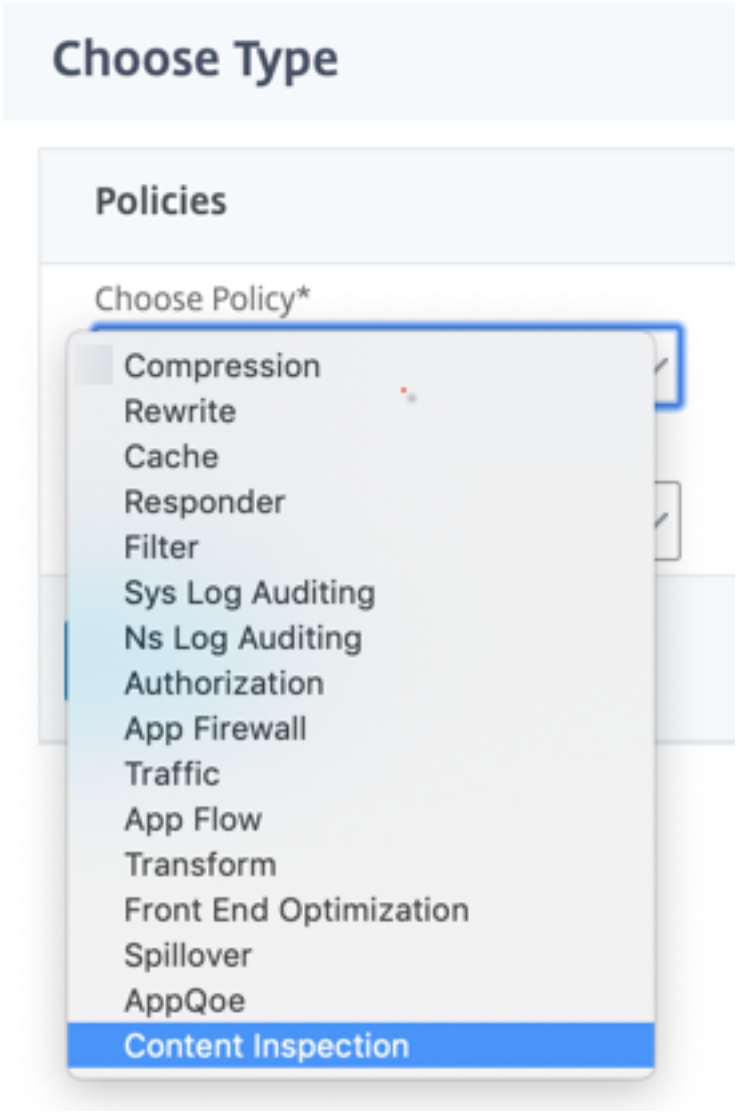



7. Vaya a **Secure Web Gateway > Servidores virtuales Proxy > Agregar**. Especifique un nombre, una dirección IP y un puerto. En **Configuración avanzada**, seleccione **Directivas**. Haga clic en el signo "+".



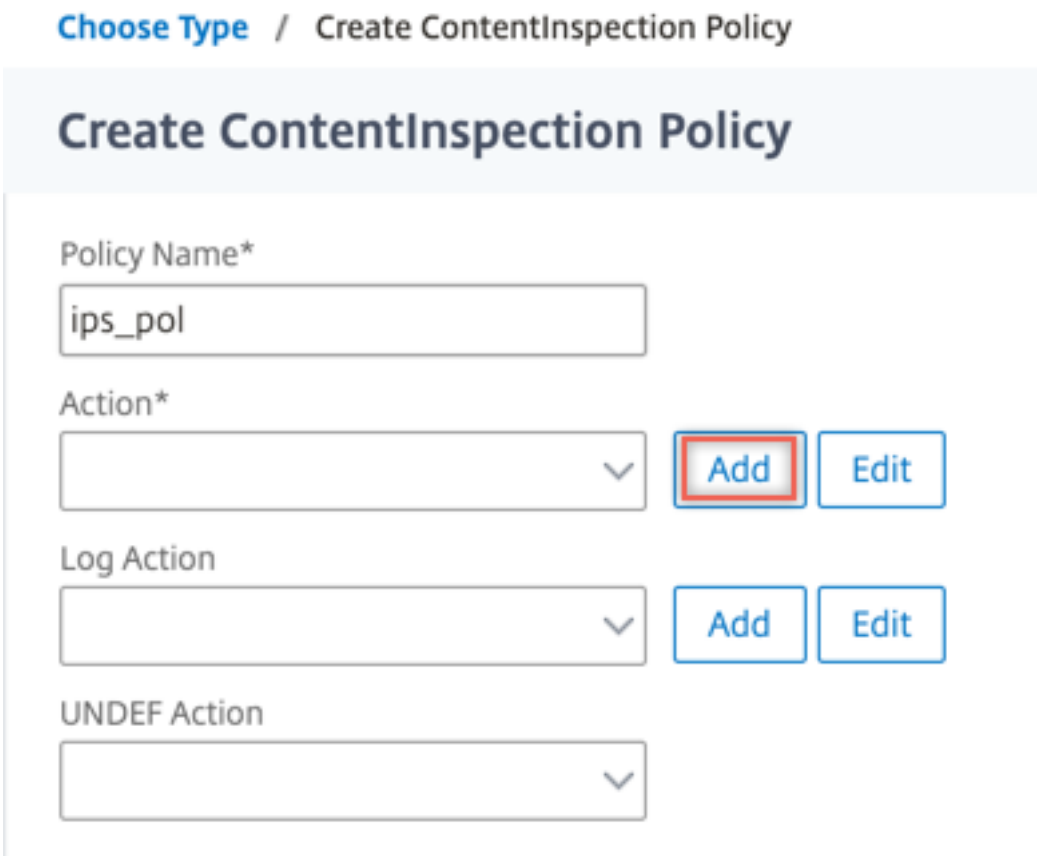

8. En **Elegir directiva**, seleccione **Inspección de contenido**. Haga clic en **Continuar**.



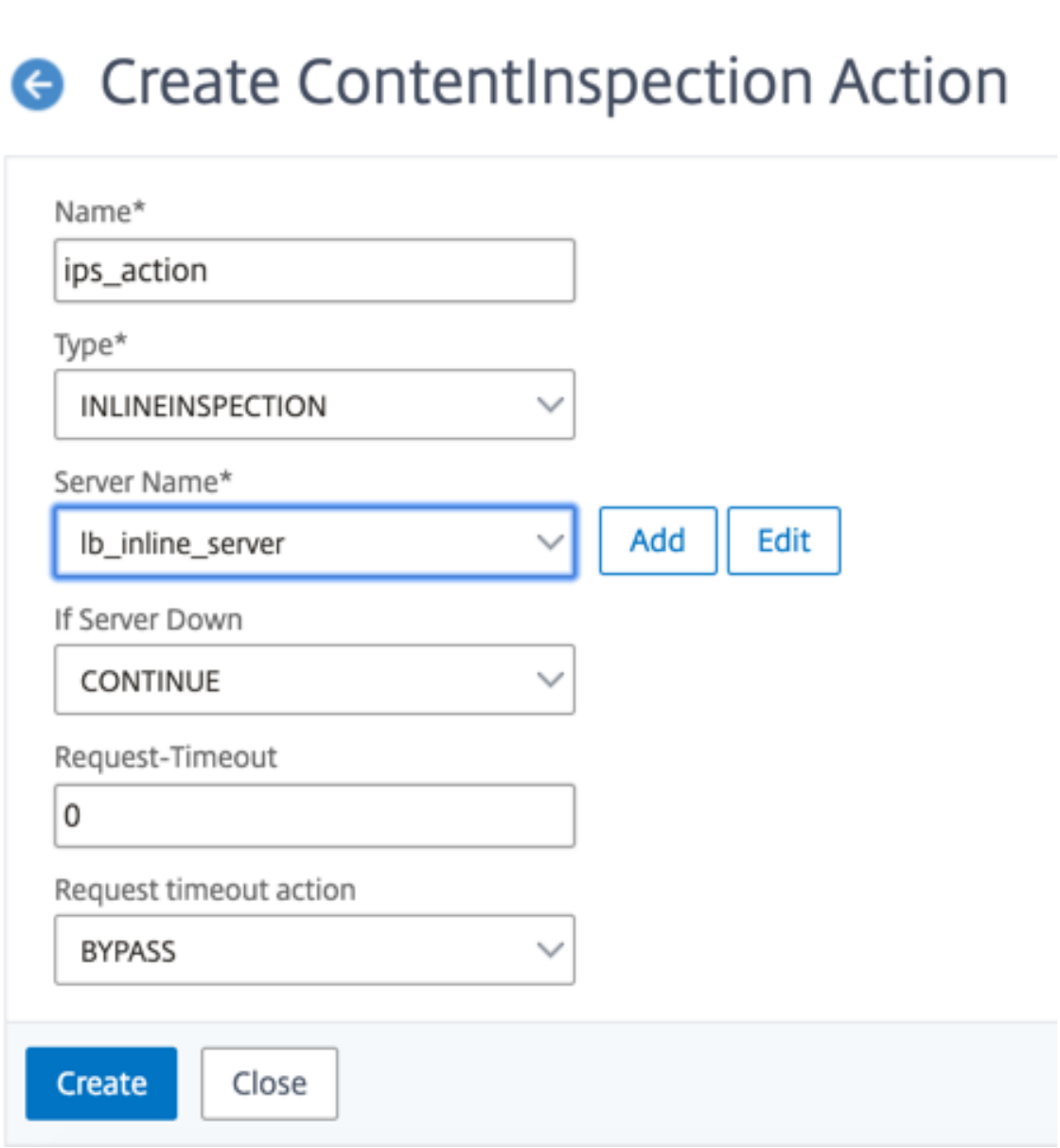

9. Haga clic en **Agregar**. Especifique un nombre. En **Acción**, haga clic en **Agregar**.



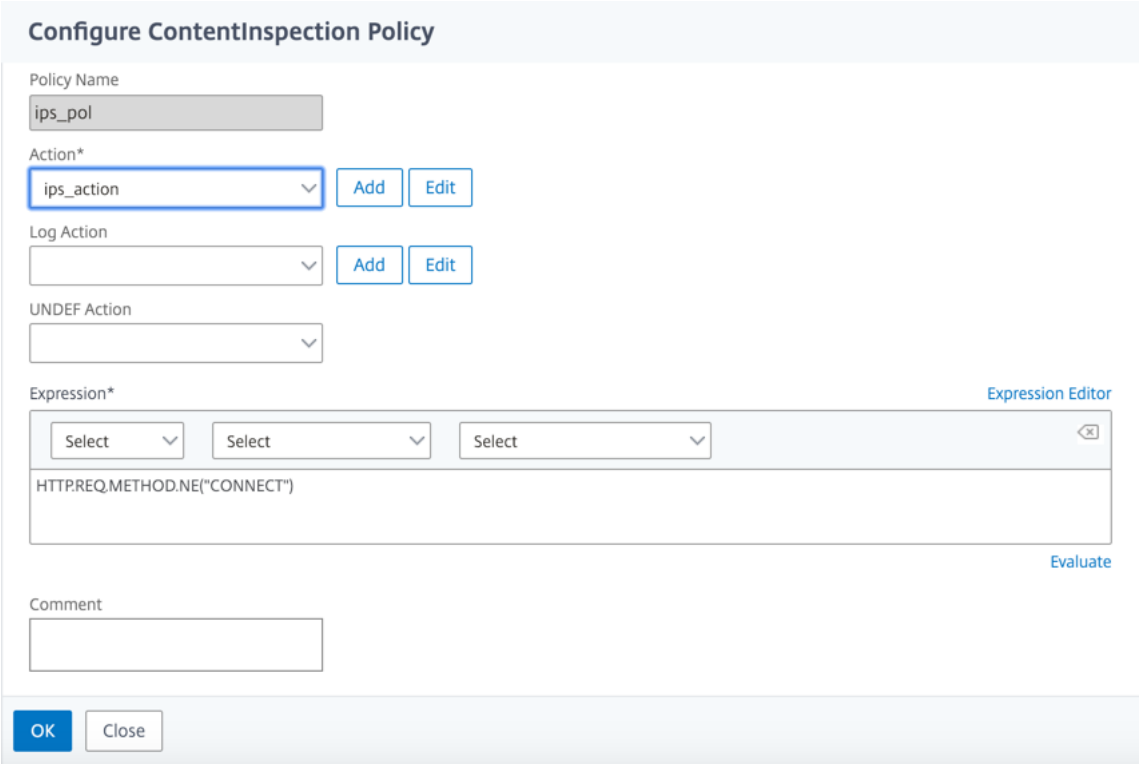

10. Especifique un nombre. En **Tipo**, seleccione **INLINEINSPECTION**. En **Nombre del servidor**, seleccione el servidor virtual de equilibrio de carga creado anteriormente.




11. Haga clic en **Crear**. Especifique la regla y haga clic en **Crear**.

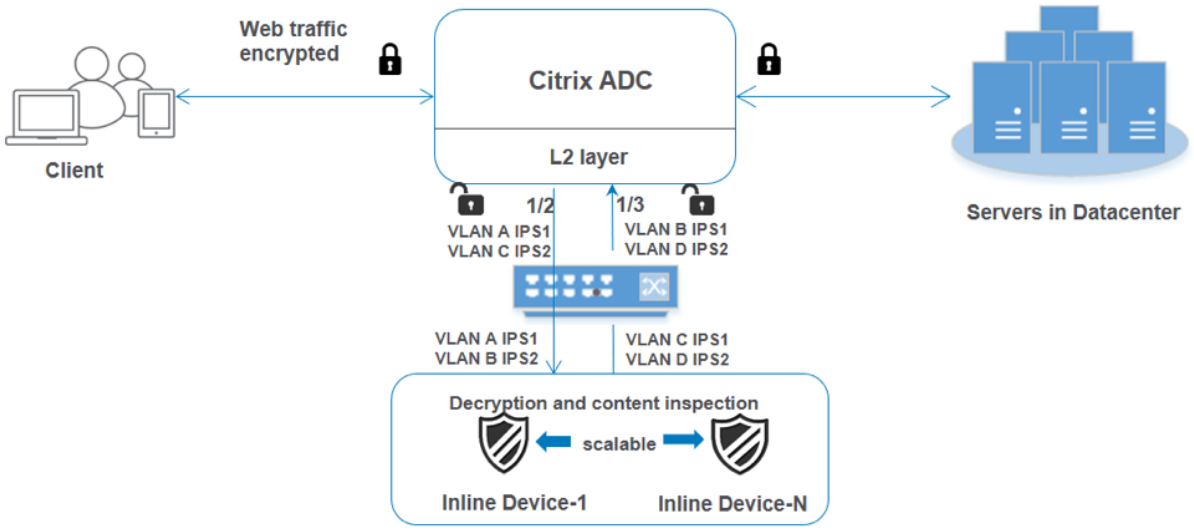



12. Haga clic en **Bind**.
13. Haga clic en **Done**.

### Caso 3: Equilibrio de carga de varios dispositivos en línea con interfaces compartidas

Si utiliza dos o más dispositivos en línea, puede equilibrar la carga de los dispositivos mediante diferentes servicios de inspección de contenido con interfaces compartidas. En este caso, la carga del dispositivo Citrix SWG equilibra el subconjunto de tráfico enviado a cada dispositivo a través de una interfaz compartida. El subconjunto se decide en función de las directivas configuradas. Por ejemplo, es posible que los archivos TXT o de imagen no se envíen para su inspección a los dispositivos en línea.




La configuración básica sigue siendo la misma que en el caso 2. Para este caso, vincule las interfaces a diferentes VLAN para segregar el tráfico de cada dispositivo en línea. Especifique las VLAN en los perfiles de inspección de contenido. Realice los siguientes pasos adicionales:

1. Enlazar las interfaces compartidas a diferentes VLAN.
2. Especifique las VLAN de entrada y salida en los perfiles de inspección de contenido.

**Configuración mediante la CLI** Escriba los siguientes comandos en el símbolo del sistema. Se dan ejemplos después de cada comando.

1. Habilitar MBF.

```
enable ns mode mbf
<!--NeedCopy-->
```

2. Habilite la función.

```
enable ns feature contentInspection
<!--NeedCopy-->
```

3. Enlazar las interfaces compartidas a diferentes VLAN.

```
bind vlan <id> -ifnum <interface> -tagged
<!--NeedCopy-->
```

**Ejemplo:**

```
bind vlan 100  – ifnum 1/2 tagged
bind vlan 200  – ifnum 1/3 tagged
bind vlan 300  – ifnum 1/2 tagged
```

```
4 bind vlan 400 –ifnum 1/3 tagged
5 <!--NeedCopy-->
```

4. Agregar perfil 1 para el servicio 1. Especifique las VLAN de entrada y salida en el perfil.

```
1 add contentInspection profile <name> -type InlineInspection -
      egressInterface <interface_name> -ingressInterface <
      interface_name>[-egressVlan <positive_integer>] [-ingressVlan <
      positive_integer>]
2 <!--NeedCopy-->
```

**Ejemplo:**

```
1 add contentInspection profile ipsprof1 -type InlineInspection -
      egressInterface "1/3" -ingressinterface "1/2" –egressVlan 100
      -ingressVlan 300
2 <!--NeedCopy-->
```

5. Agregar perfil 2 para el servicio 2. Especifique las VLAN de entrada y salida en el perfil.

```
1 add contentInspection profile <name> -type InlineInspection -
      egressInterface <interface_name> -ingressInterface <
      interface_name>[-egressVlan <positive_integer>] [-ingressVlan <
      positive_integer>]
2 <!--NeedCopy-->
```

**Ejemplo:**

```
1 add contentInspection profile ipsprof2 -type InlineInspection -
      egressInterface "1/3" -ingressinterface "1/2" –egressVlan 200
      -ingressVlan 400
2 <!--NeedCopy-->
```

6. Agregar servicio 1.

```
1 add service <service_name>  <IP> TCP <Port> -
      contentinspectionProfileName <Name>  -healthMonitor NO  -usip
      YES –useproxyport NO
2 <!--NeedCopy-->
```

**Ejemplo:**

```
1 add service ips_service1 192.168.10.2 TCP * -healthMonitor NO -
      usip YES -useproxyport NO -contentInspectionProfileName
      ipsprof1
2 <!--NeedCopy-->
```

7. Agregar servicio 2.

```
1 add service <service_name>  <IP> TCP <Port> -
      contentinspectionProfileName <Name>  -healthMonitor NO  -usip
      YES –useproxyport NO
2 <!--NeedCopy-->
```

**Ejemplo:**

```
add service ips_service2 192.168.10.3 TCP * -healthMonitor NO -
   usip YES -useproxyport NO -contentInspectionProfileName
   ipsprof2
<!--NeedCopy-->
```

8. Agregue un servidor virtual de equilibrio de carga.

```
add lb vserver <LB_VSERVER_NAME> TCP <IP> <port>
<!--NeedCopy-->
```

**Ejemplo:**

```
add lb vserver lb_inline_vserver TCP 192.0.2.100 *
<!--NeedCopy-->
```

9. Enlazar los servicios al servidor virtual de equilibrio de carga.

```
bind lb vserver <LB_VSERVER_NAME> <service_name>
bind lb vserver <LB_VSERVER_NAME> <service_name>
<!--NeedCopy-->
```

**Ejemplo:**

```
bind lb vserver lb_inline_vserver ips_service1
bind lb vserver lb_inline_vserver ips_service2
<!--NeedCopy-->
```

10. Especifique el servidor virtual de equilibrio de carga en la acción de inspección de contenido.

```
add contentInspection action <name> -type INLINEINSPECTION -
   serverName <string>
<!--NeedCopy-->
```

**Ejemplo:**

```
add contentInspection action ips_action -type INLINEINSPECTION -
   serverName lb_inline_vserver
<!--NeedCopy-->
```

11. Agregar una directiva de inspección de contenido. Especifique la acción de inspección de contenido en la directiva.

```
add contentInspection policy <name> -rule <expression> -action <
   string>
<!--NeedCopy-->
```

**Ejemplo:**

```
add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE("
   CONNECT")" -action ips_action
```

```
<!--NeedCopy-->
```

12. Agregue un servidor virtual proxy.

```
add cs vserver <name> PROXY <IPAddress> <port> -l2Conn ON
<!--NeedCopy-->
```

**Ejemplo:**

```
add cs vserver transparentcs PROXY * * -l2Conn ON
<!--NeedCopy-->
```

13. Enlazar la directiva de inspección de contenido al servidor virtual.

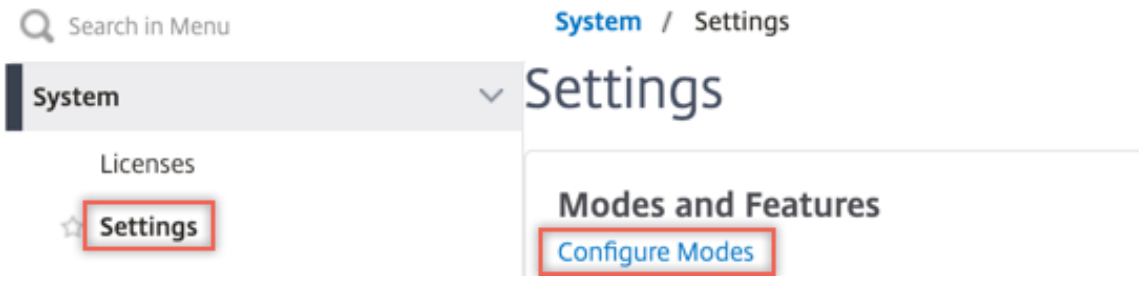
```
bind cs vserver <name> -policyName <string> -priority <
    positive_integer> -gotoPriorityExpression <expression> -type
    REQUEST
<!--NeedCopy-->
```

**Ejemplo:**

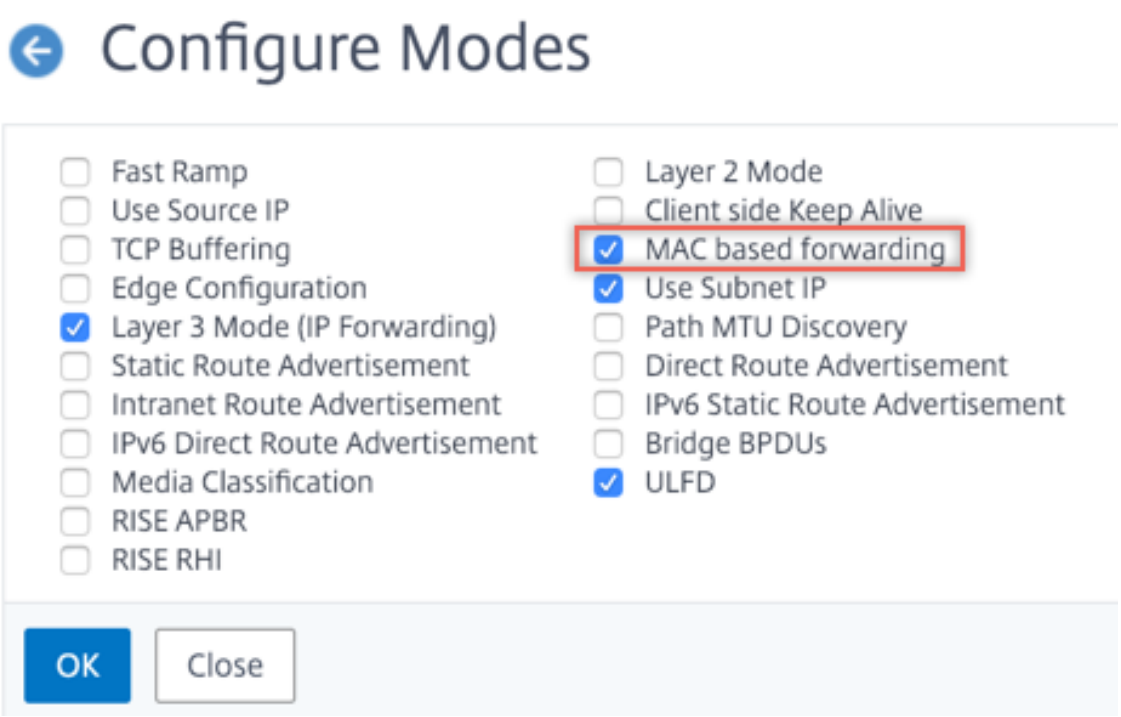
```
bind cs vserver explicitcs -policyName ips_pol -priority 1 -
    gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```

### Configuración mediante la GUI

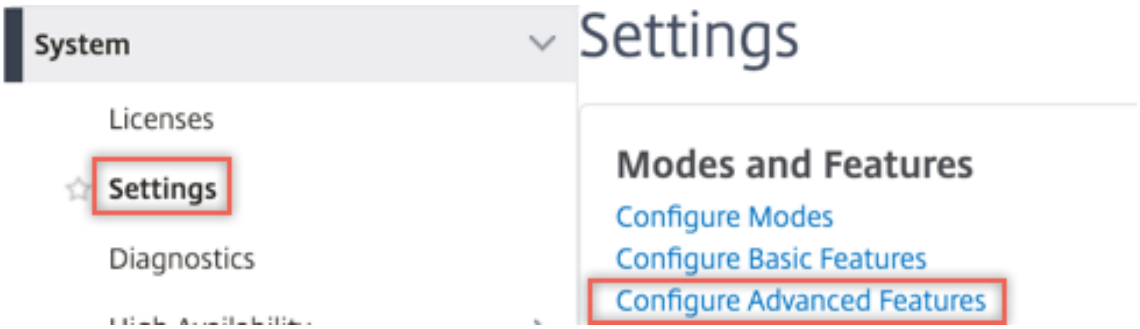
1. Vaya a **Sistema > Configuración**. En **Modos y funciones**, haga clic en **Configurar modos**.



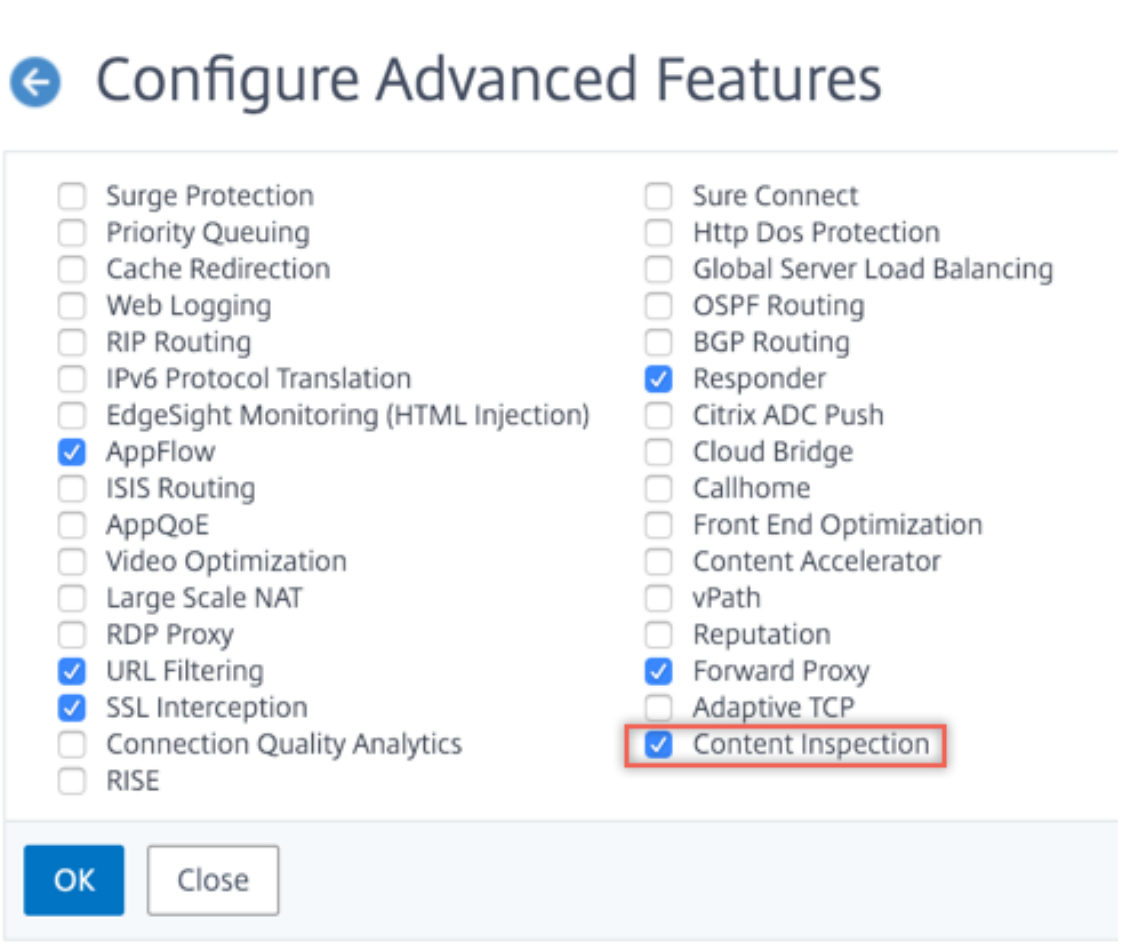

 




2. Vaya a **Sistema > Configuración**. En **Modos y funciones**, haga clic en **Configurar funciones avanzadas**.

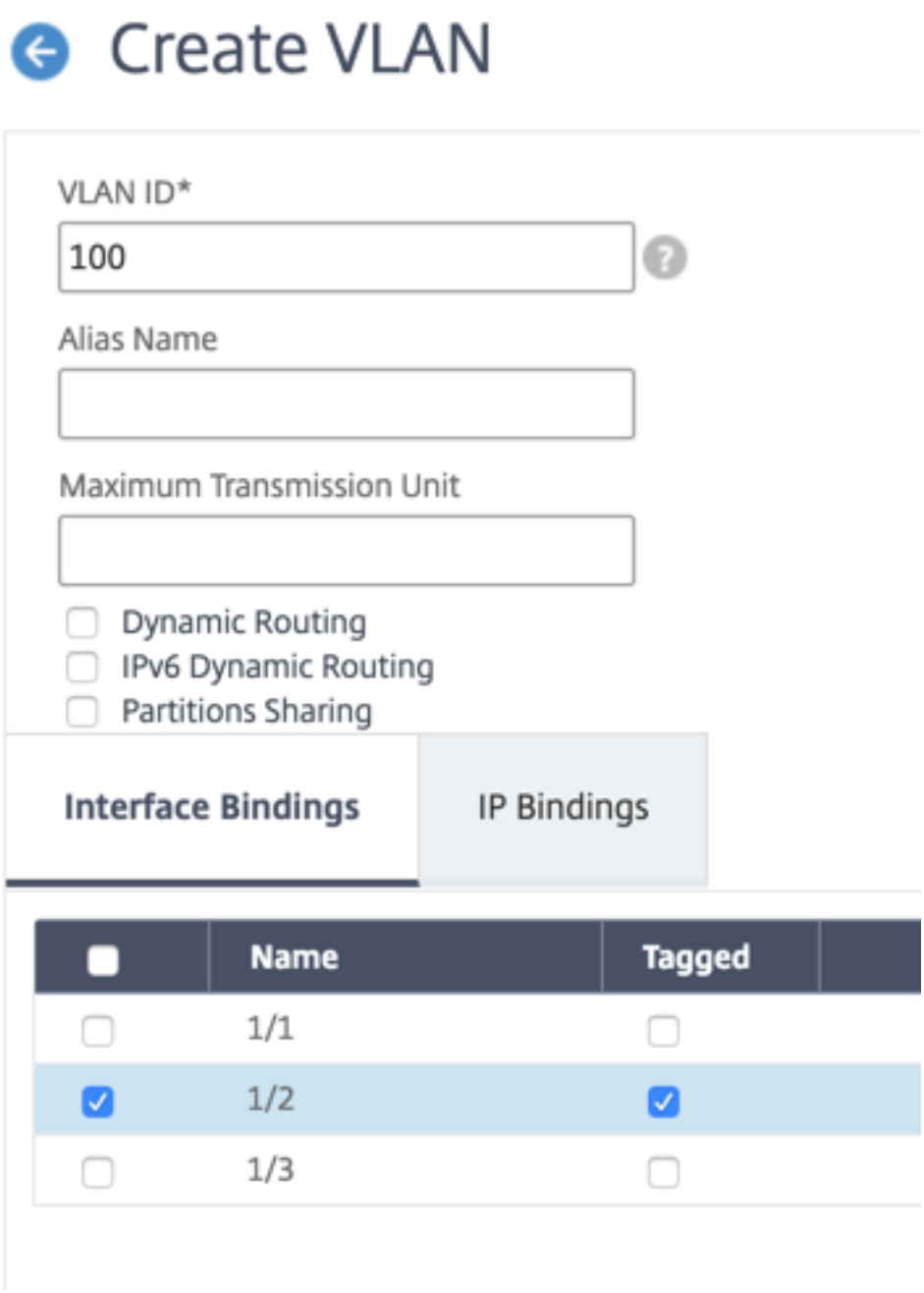


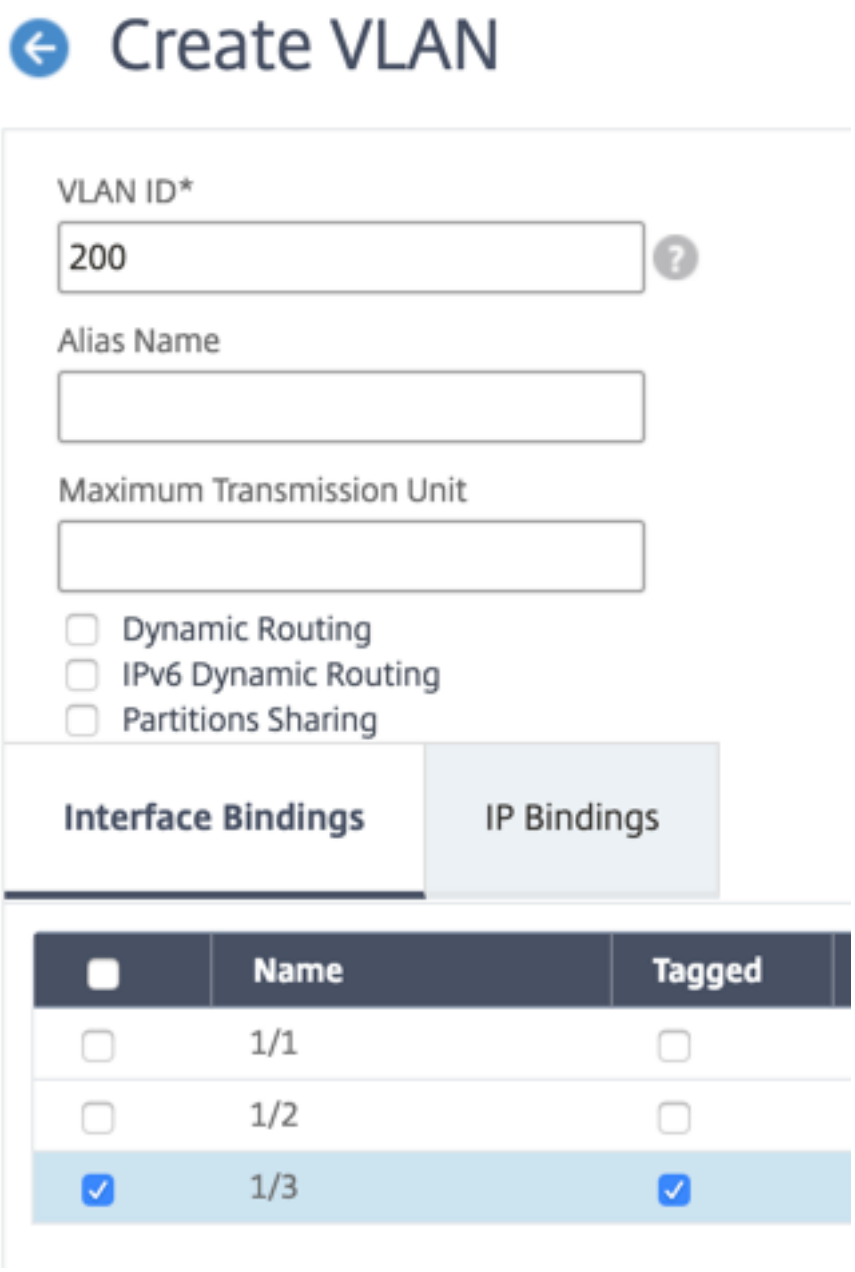



3. Vaya a **Sistema > Red > VLAN > Agregar**. Agregue cuatro VLAN y etiquetarlas a las interfaces.

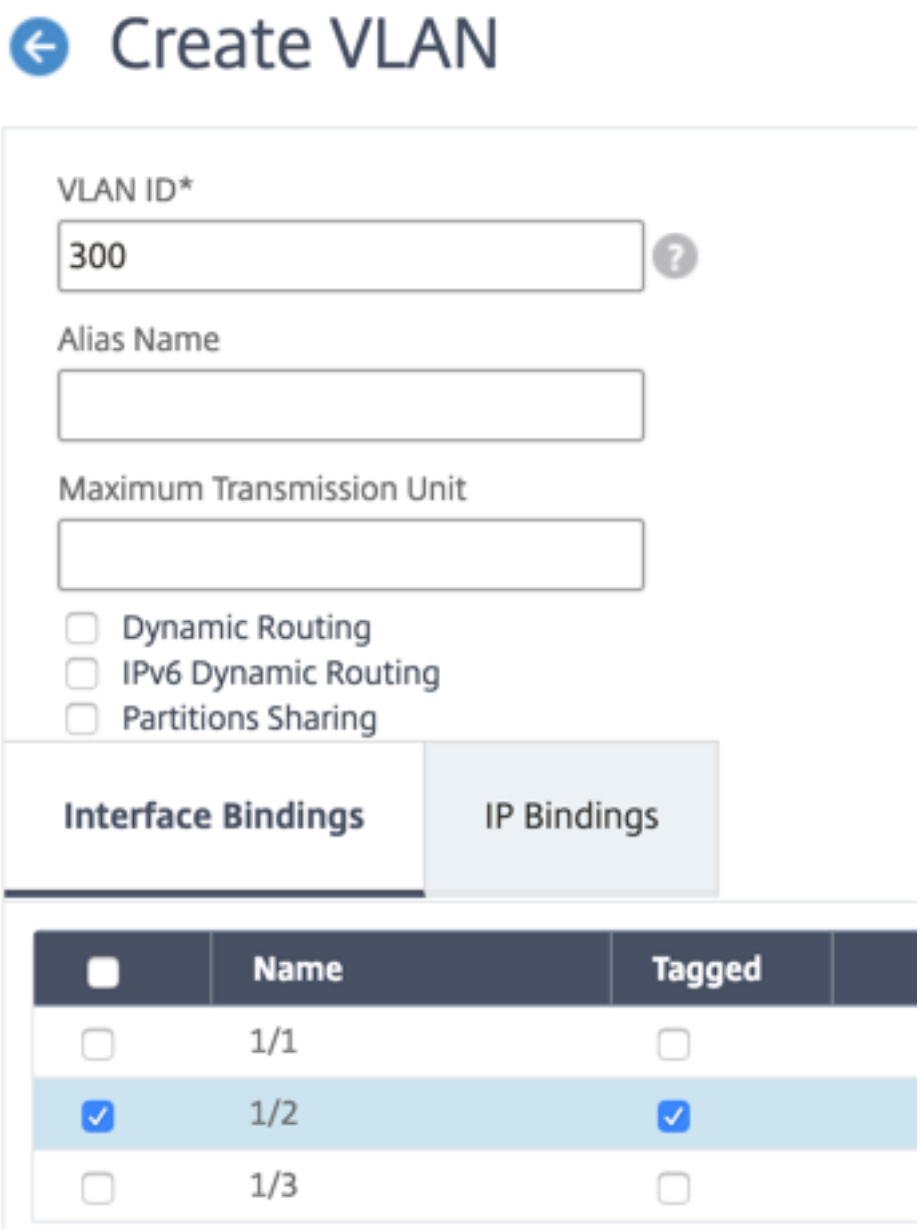
 



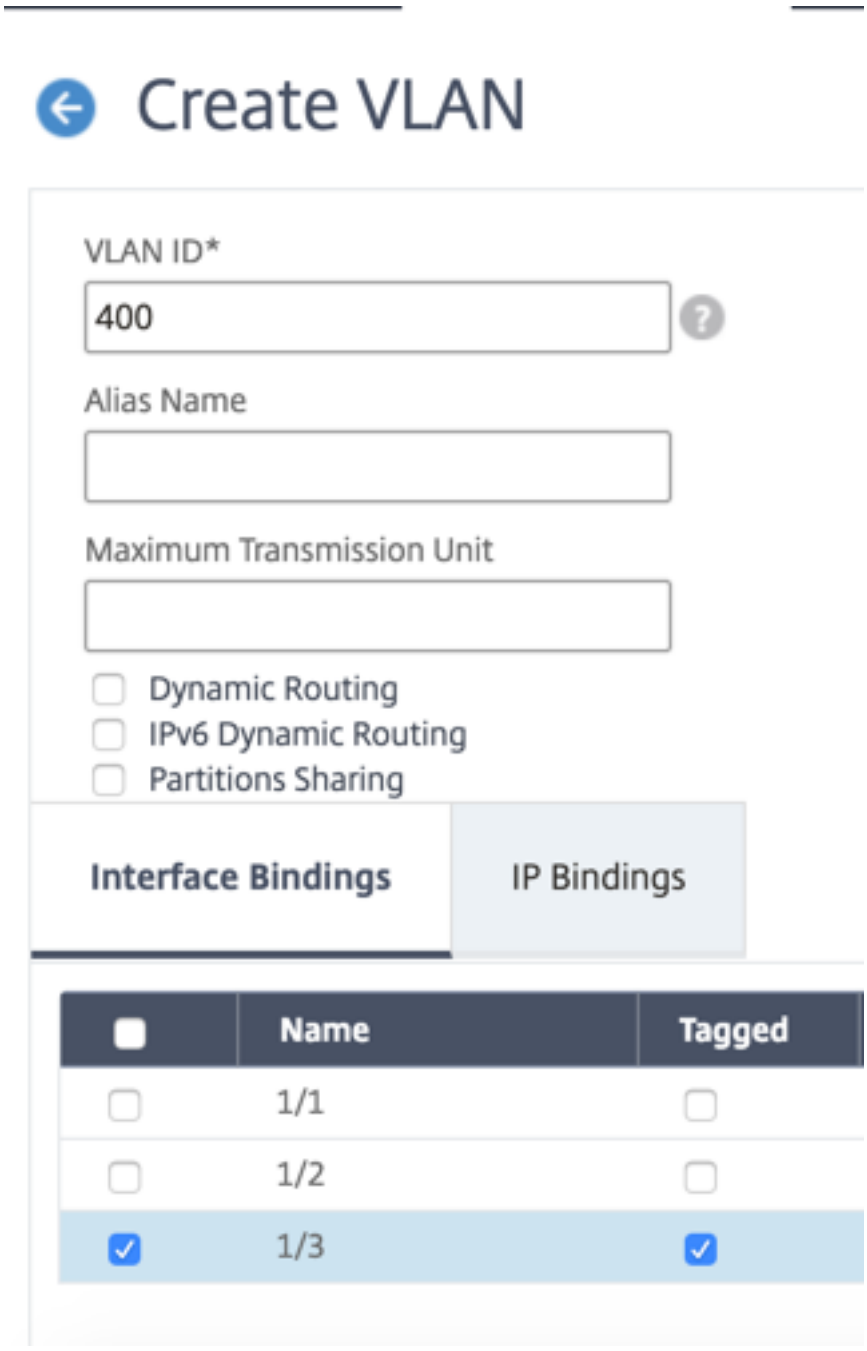

 



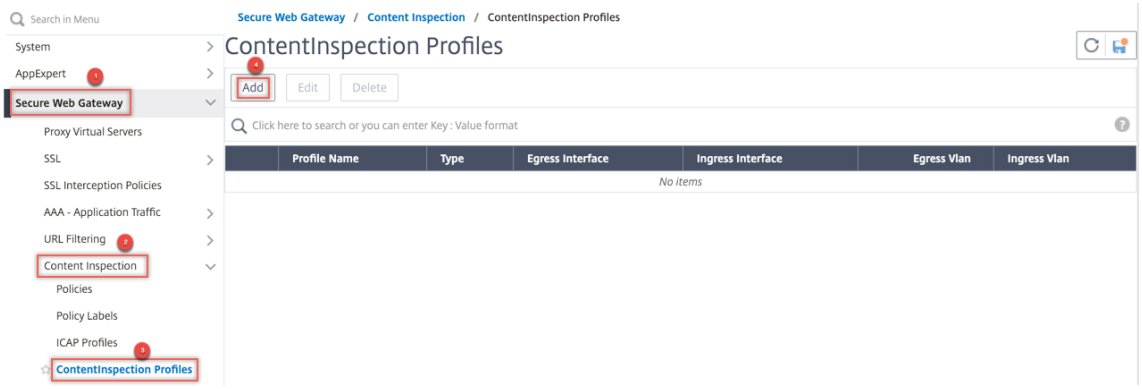


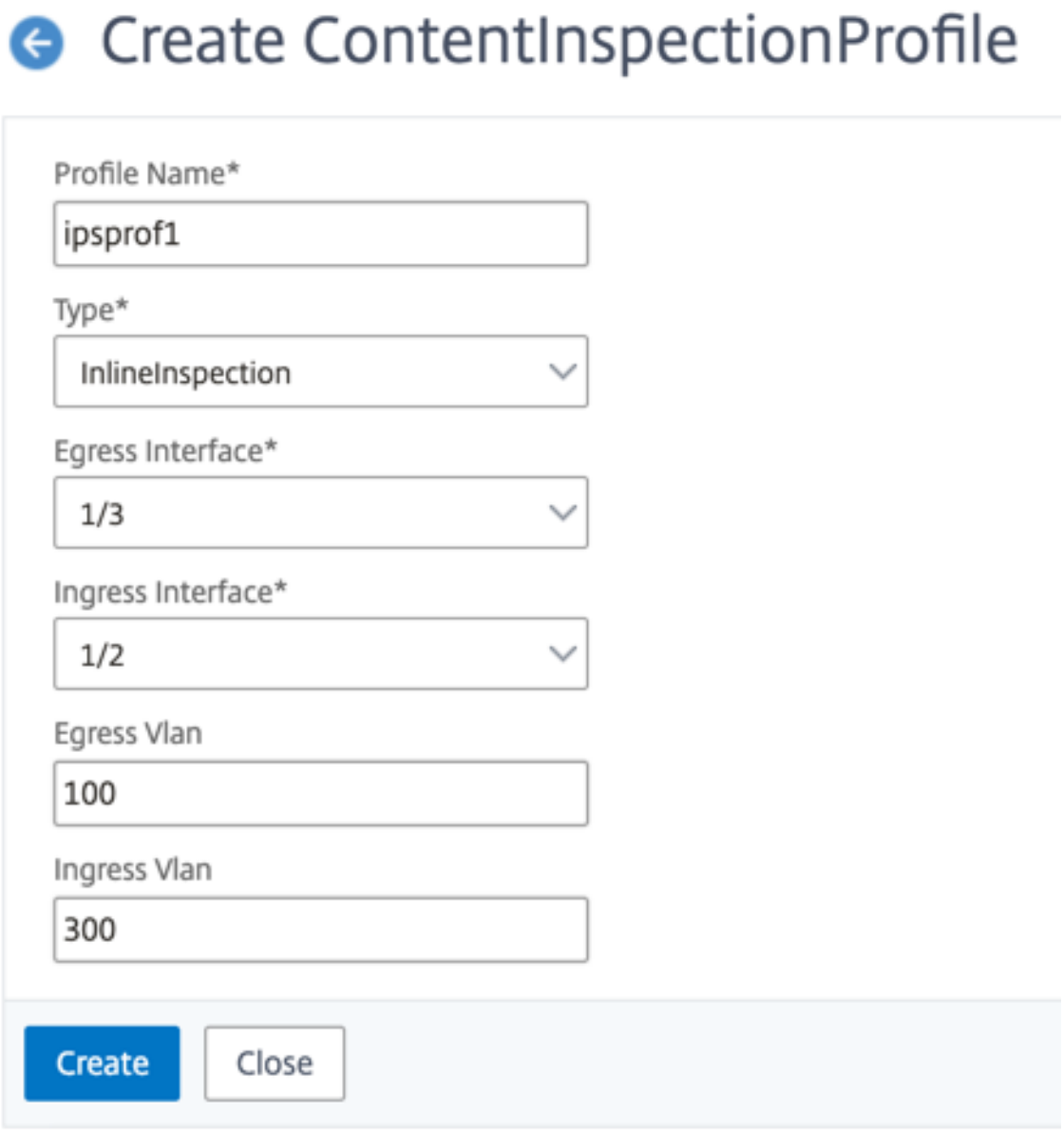



4. Vaya a **Secure Web Gateway > Inspección de contenido > Perfiles de inspección de contenido**. Haga clic en **Agregar**.

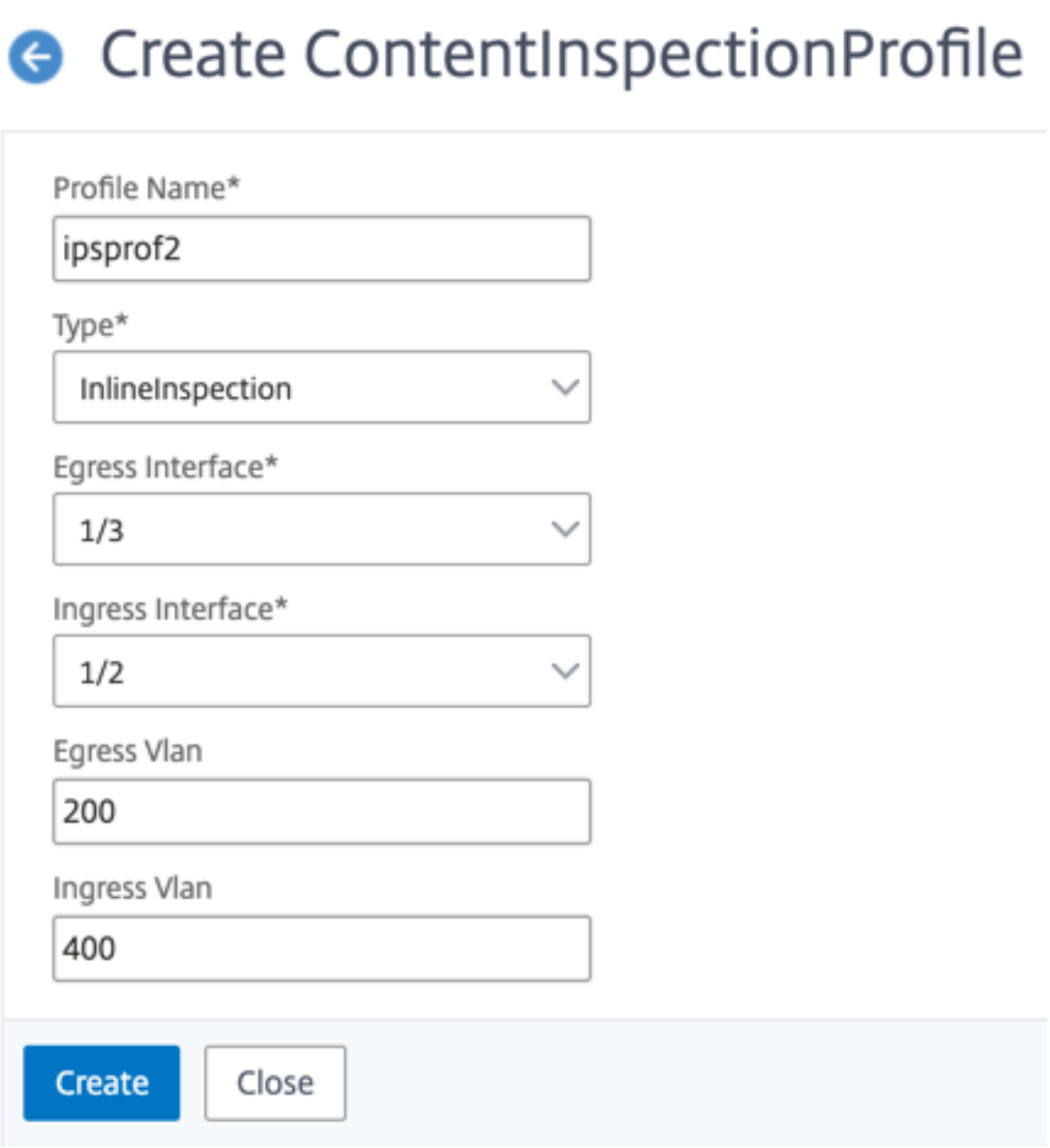



Especifique las VLAN de entrada y salida.



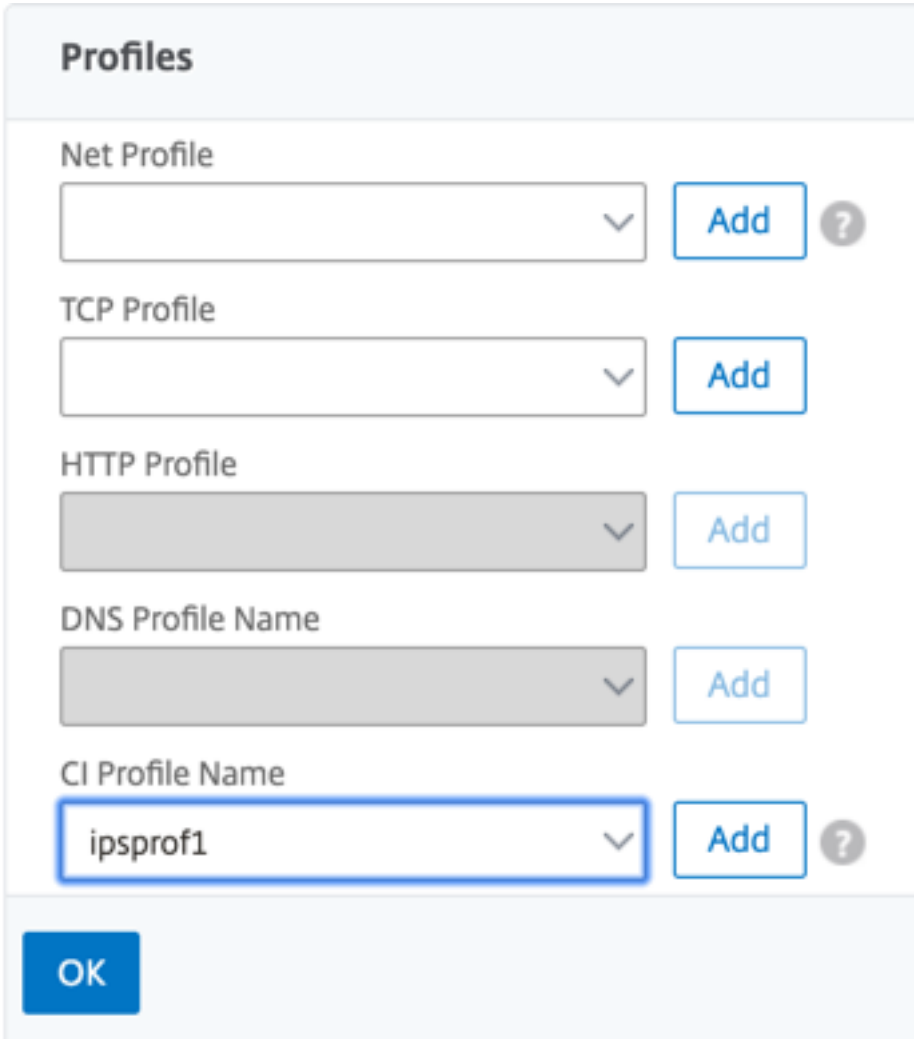
Cree otros perfiles. Especifique una VLAN de entrada y salida diferente en el segundo perfil.



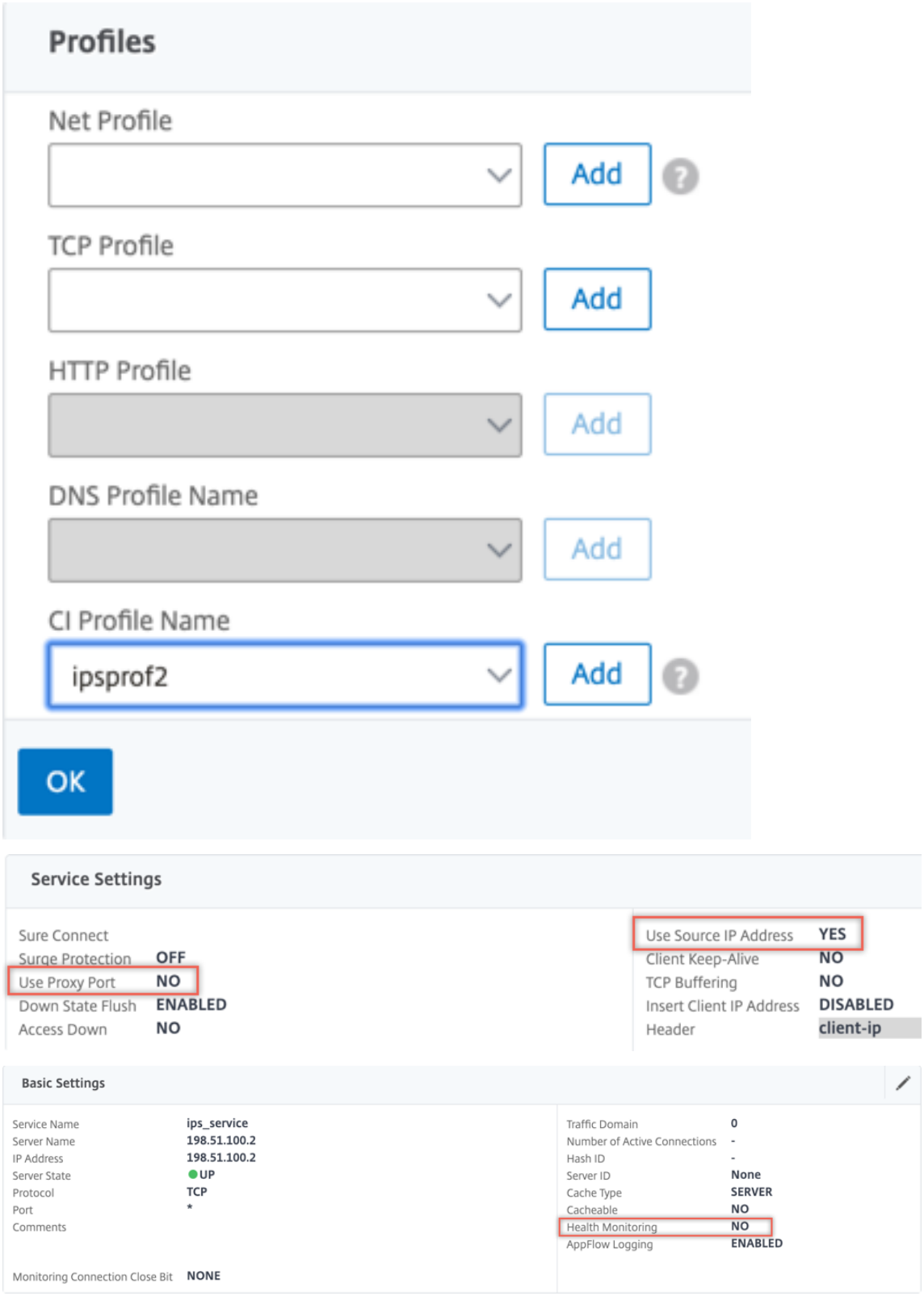

5. Desplácese hasta **Equilibrio de carga > Servicios > Agregar** y agregar un servicio. En **Configuración avanzada**, haga clic en **Perfiles**. En la lista **Nombre de perfil de CI**, seleccione el perfil de inspección de contenido creado anteriormente. En **Configuración del servicio**, establezca **Usar dirección IP de origen**en YES y **Usar puerto proxy**en No. En **Configuración básica**, establezca **Supervisión del estado**en NO.

   Cree dos servicios. Especifique direcciones IP ficticias que no pertenecen a ninguno de los dispositivos, incluidos los dispositivos en línea. Especifique el perfil 1 en el servicio 1 y el perfil 2 en el servicio 2.

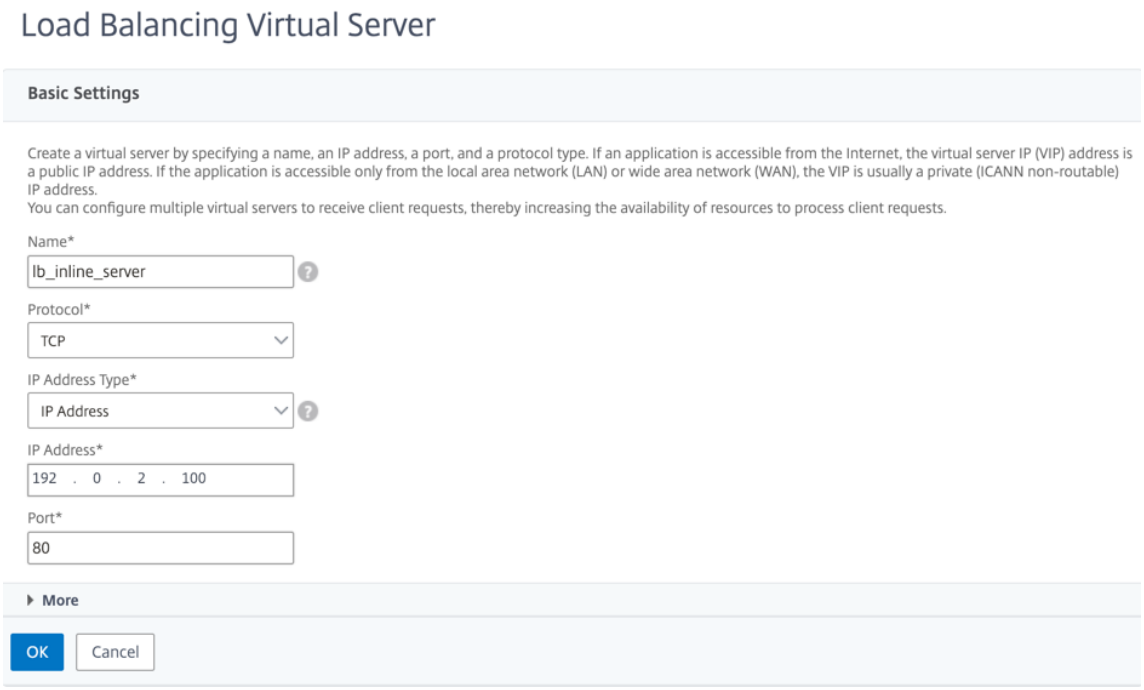




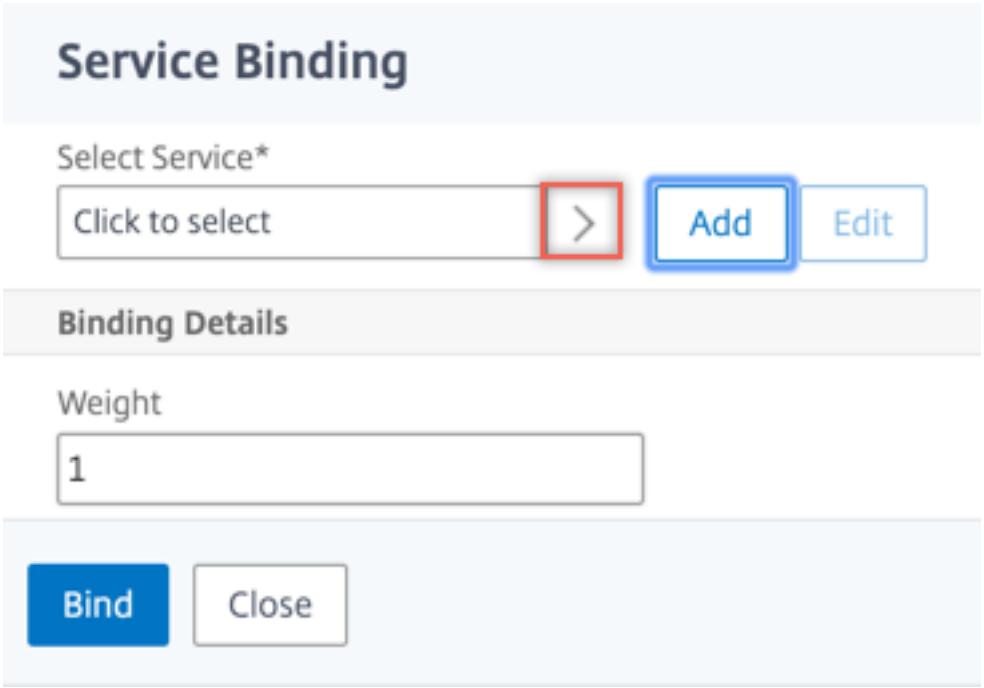

6. Desplácese hasta **Equilibrio de carga > Servidores virtuales > Agregar**. Cree un servidor virtual de equilibrio de carga TCP.

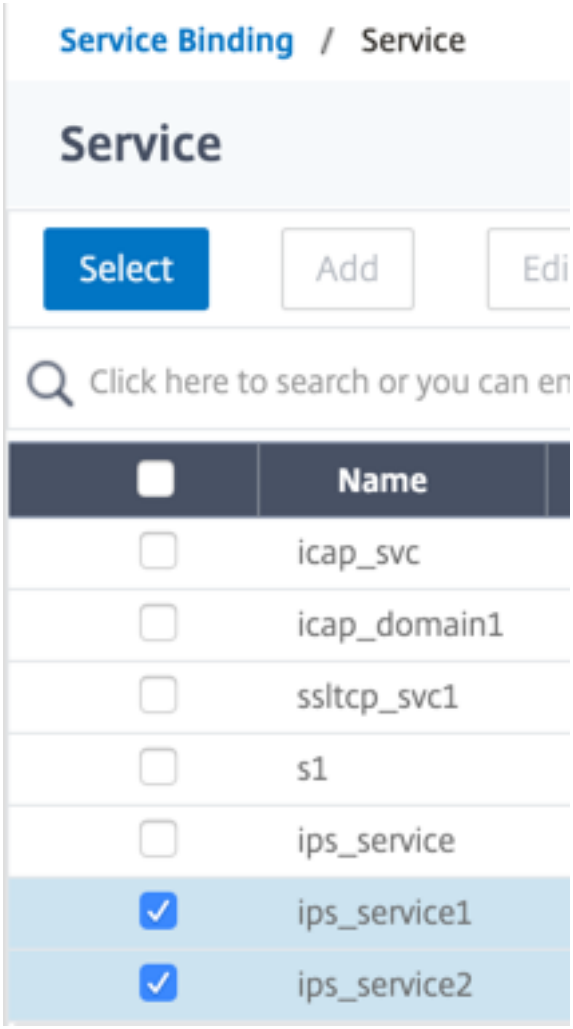



Haga clic en **OK**.

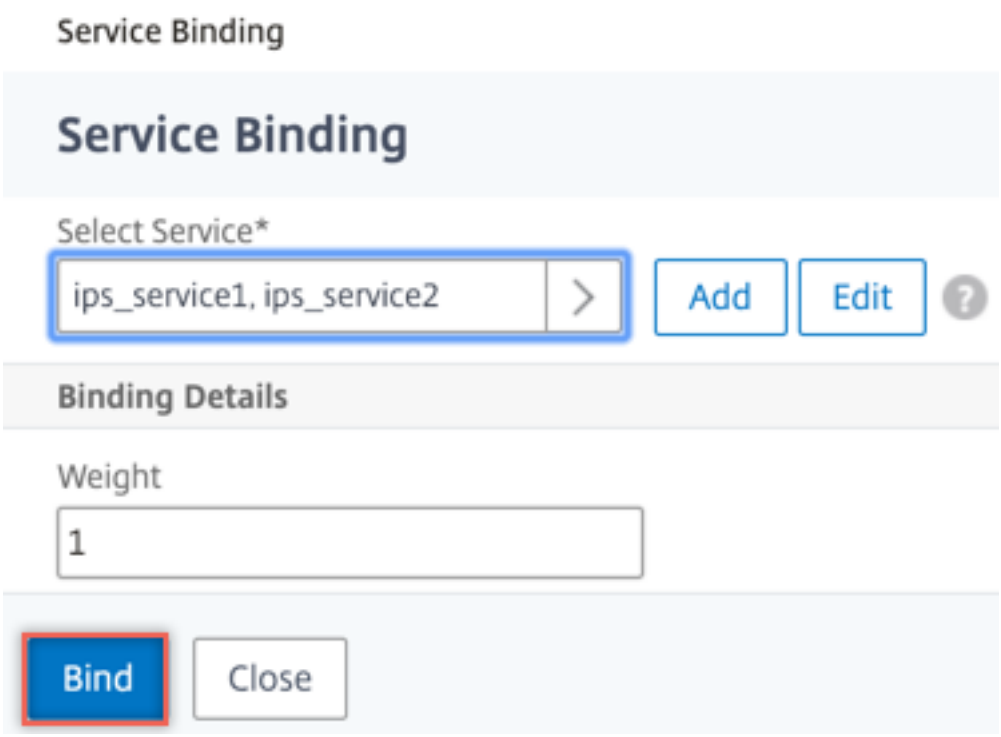
7. Haga clic dentro de la sección **Enlace del servicio de servidor virtual de equilibrio de carga**. En **Enlace de servicio**, haga clic en la flecha **de Seleccionar servicio**. Seleccione los dos servicios creados anteriormente y haga clic en **Seleccionar**. Haga clic en **Bind**.



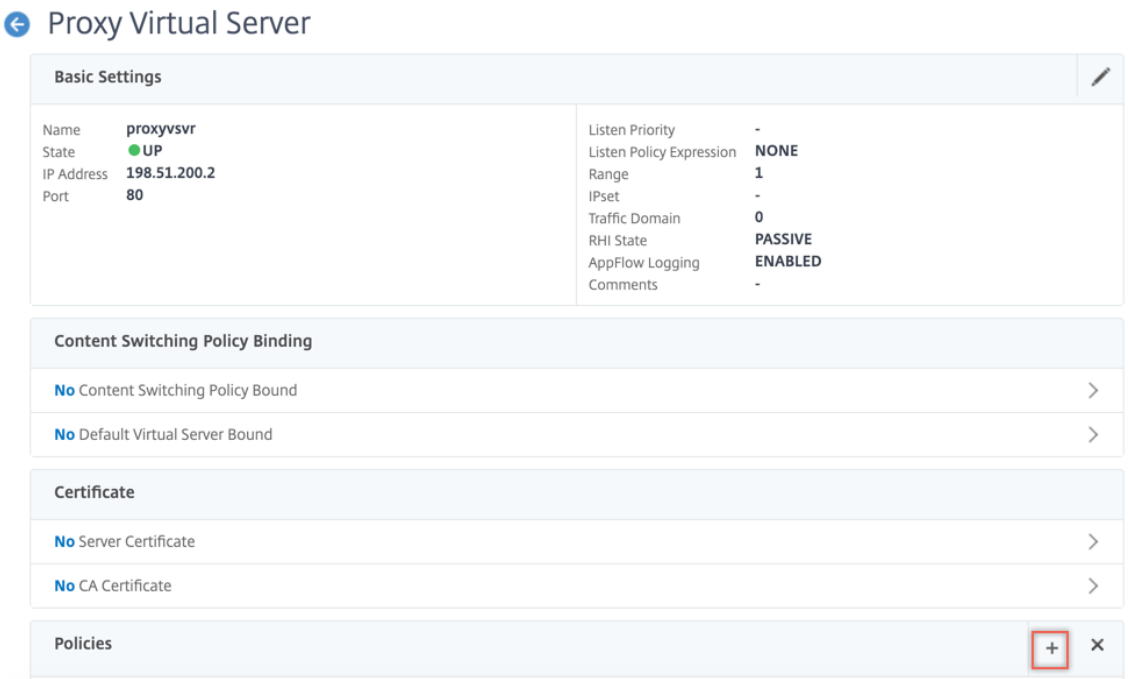

 



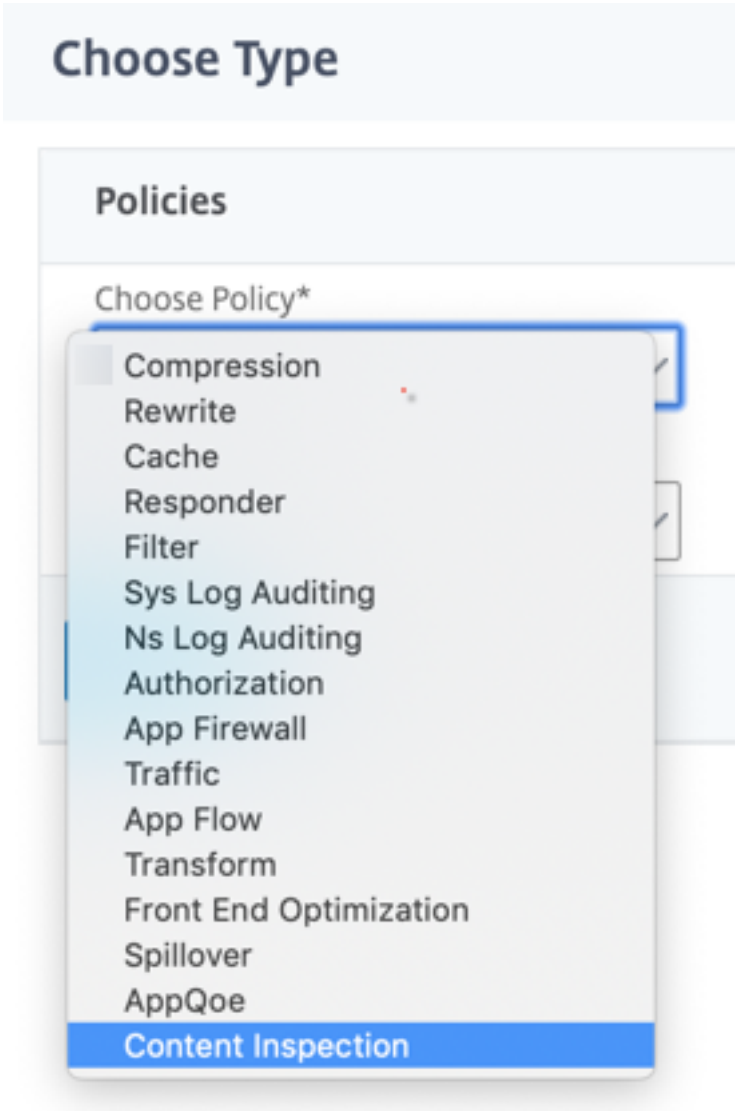



8. Vaya a **Secure Web Gateway > Servidores virtuales Proxy > Agregar**. Especifique un nombre, una dirección IP y un puerto. En **Configuración avanzada**, seleccione **Directivas**. Haga clic en el signo “+”.



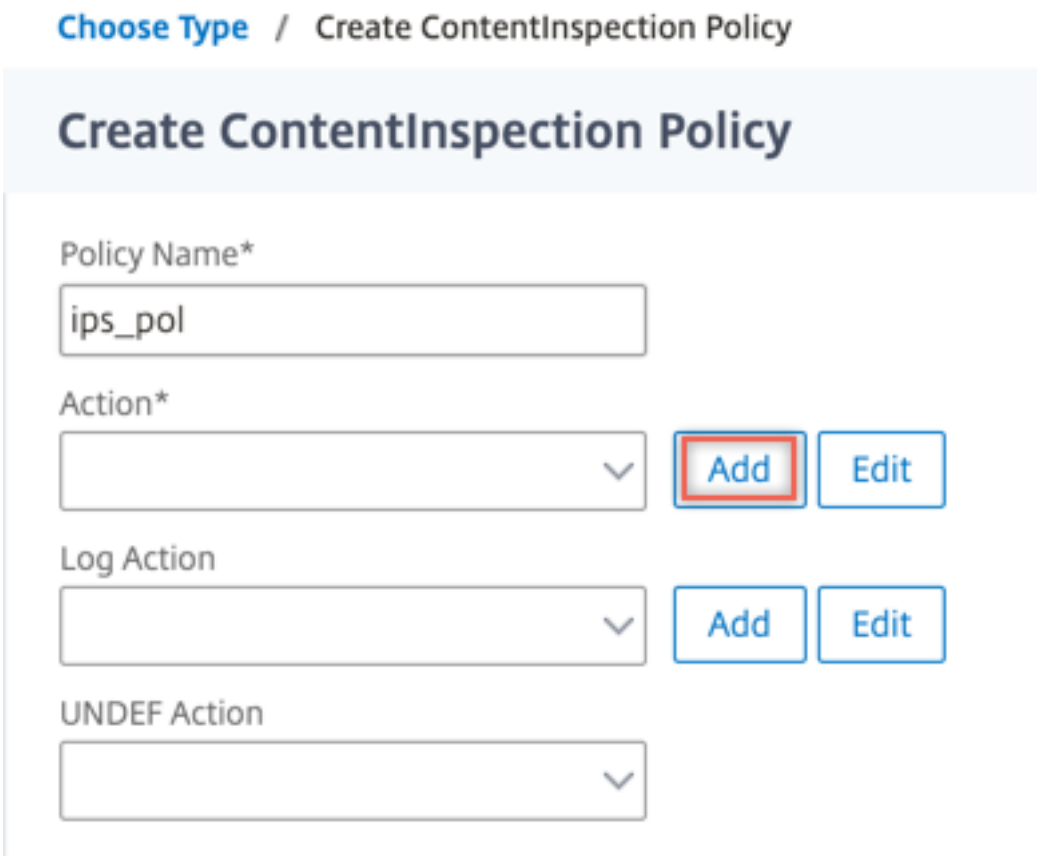

9. En **Elegir directiva**, seleccione **Inspección de contenido**. Haga clic en **Continuar**.



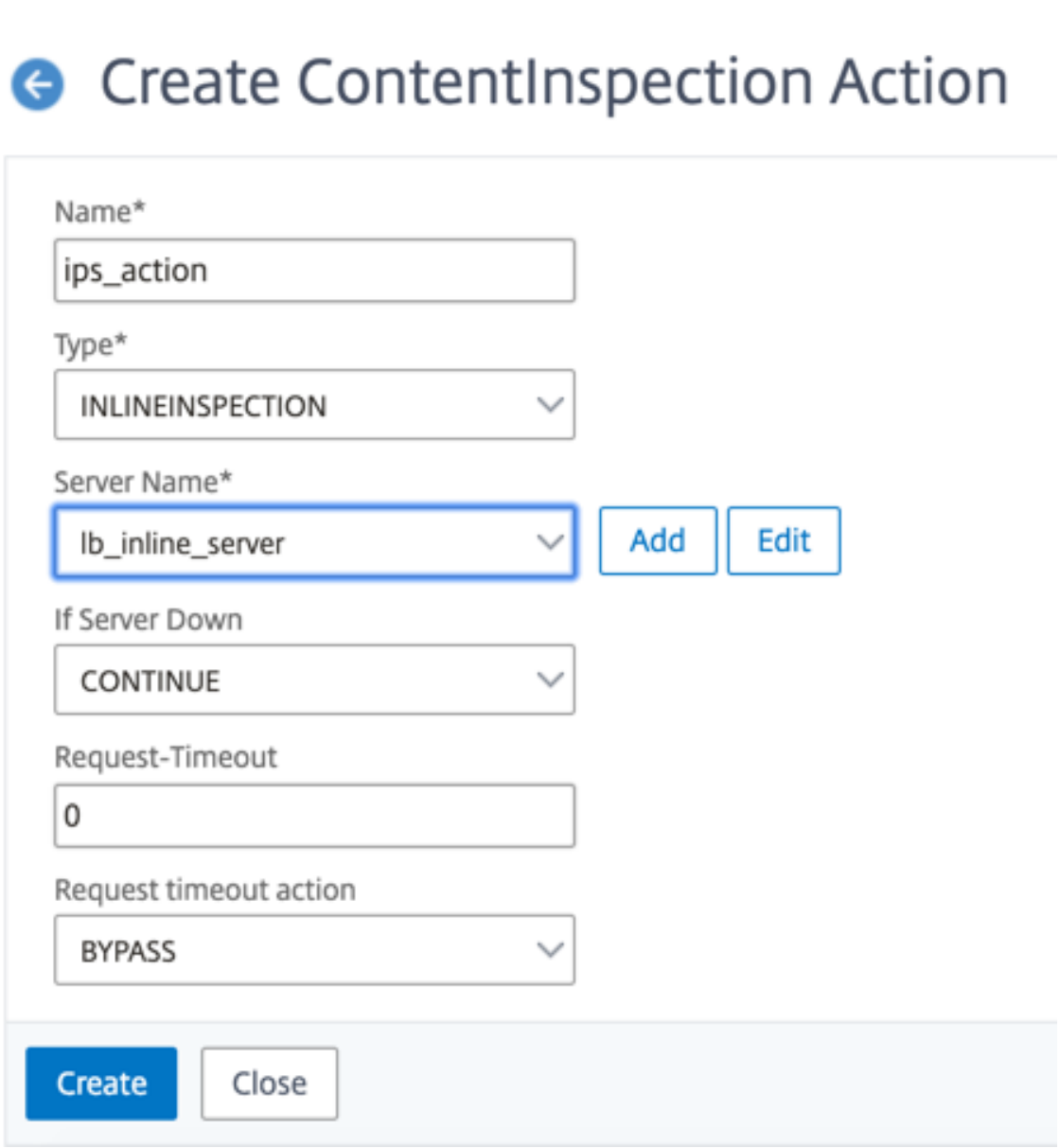

10. Haga clic en **Agregar**. Especifique un nombre. En **Acción**, haga clic en **Agregar**.



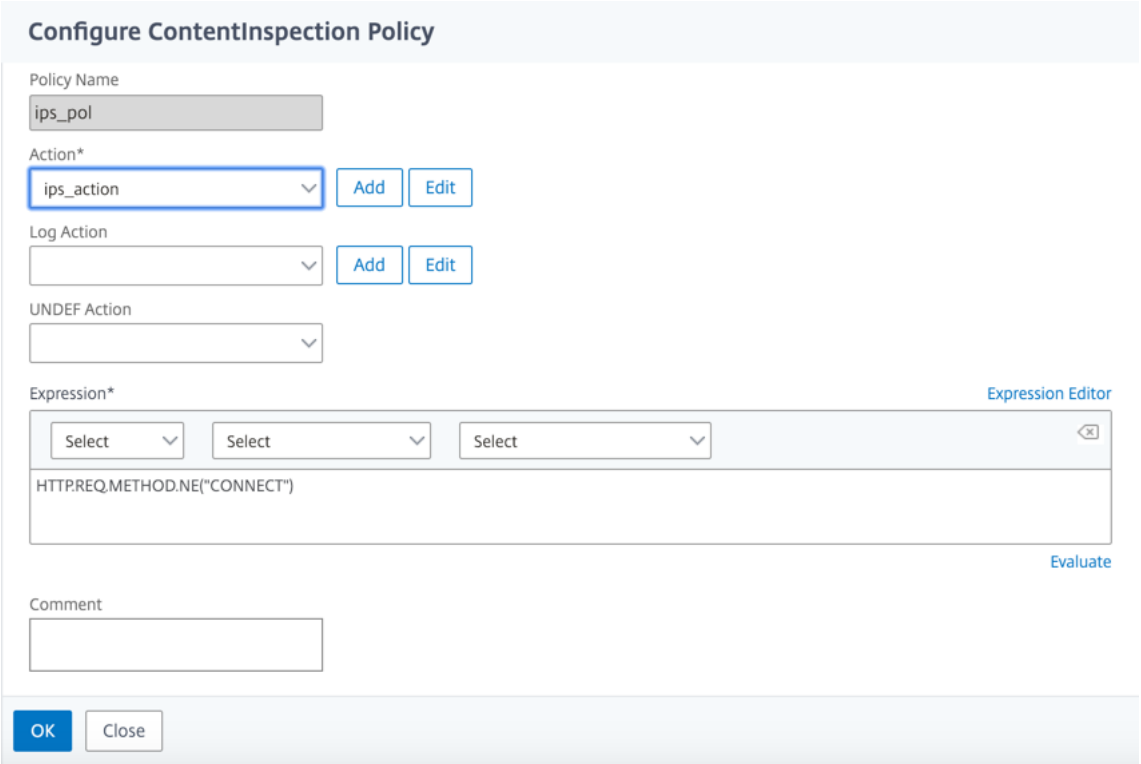

11. Especifique un nombre. En **Tipo**, seleccione **INLINEINSPECTION**. En **Nombre del servidor**, seleccione el servidor virtual de equilibrio de carga creado anteriormente.




12. Haga clic en **Crear**. Especifique la regla y haga clic en **Crear**.




13. Haga clic en **Bind**.
14. Haga clic en **Done**.

## Analytics

April 27, 2021

En el dispositivo Citrix SWG, se registran todos los registros de usuario y los registros posteriores. Cuando integra Citrix Application Delivery Management (ADM) con el dispositivo Citrix SWG, la actividad del usuario registrado y los registros posteriores del dispositivo se exportan a Citrix ADM mediante logstream.

Citrix ADM recopila y presenta información sobre las actividades de los usuarios, como los sitios web visitados y el ancho de banda gastado. También informa sobre el uso del ancho de banda y las amenazas detectadas, como malware y sitios de phishing. Puede utilizar estas métricas clave para supervisar la red y realizar acciones correctivas con el dispositivo Citrix SWG. Para obtener más información, consulte Análisis de Citrix Secure Web Gateway.

Para integrar el dispositivo Citrix SWG con Citrix ADM:

1. En el dispositivo Citrix SWG, al configurar Secure Web Gateway, habilite Analytics y proporcione los detalles de la instancia de Citrix ADM que desea utilizar para análisis.

2. En Citrix ADM, agregue el dispositivo Citrix SWG como instancia a Citrix ADM. Para obtener más información, consulte Agregar nuevas instancias a Citrix ADM.

## Caso de uso: Hacer que el acceso a Internet empresarial sea compatible y seguro

April 27, 2021

El director de seguridad de red en una organización financiera quiere proteger la red empresarial de cualquier amenaza externa proveniente de la web en forma de malware. Para ello, el director necesita obtener visibilidad en el tráfico cifrado que de otro modo se omite y controlar el acceso a sitios web maliciosos. El director debe hacer lo siguiente:

- Intercepte y examine todo el tráfico, incluido SSL/TLS (tráfico cifrado), que entra y sale de la red empresarial.
- Evite la interceptación de solicitudes a sitios web que contengan información confidencial, como información financiera del usuario o correos electrónicos.
- Bloquear el acceso a URL dañinas identificadas como que ofrecen contenido dañino o para adultos.
- Identifique a los usuarios finales (empleados) de la empresa que acceden a sitios web malintencionados y bloquee el acceso a Internet para estos usuarios o bloquee las direcciones URL dañinas.

Para lograr todo lo anterior, el director puede configurar un proxy en todos los dispositivos de la organización y señalarlo a Citrix Secure Web Gateway (SWG), que actúa como servidor proxy en la red. El servidor proxy intercepta todo el tráfico cifrado y no cifrado que pasa a través de la red empresarial. Solicita la autenticación del usuario y asocia el tráfico con un usuario. Se pueden especificar categorías de URL para bloquear el acceso a sitios web Ilegal/Nocivo, Adulto y Malware y SPAM.

Para lograr lo anterior, configure las siguientes entidades:

- Servidor de nombres DNS para resolver nombres de host.
- Dirección IP de subred (SNIP) para establecer una conexión con los servidores de origen. La dirección SNIP debe tener acceso a Internet.
- Servidor proxy en modo explícito para interceptar todo el tráfico HTTP y HTTPS saliente.
- Perfil SSL para definir la configuración SSL, como cifrados y parámetros, para las conexiones.
- par de claves de certificado de CA para firmar el certificado de servidor para la intercepción SSL.
- Directiva SSL para definir los sitios web a interceptar y omitir.
- Autenticación del servidor virtual, la directiva y la acción para garantizar que solo los usuarios válidos tengan acceso.

- Appflow Collector para enviar datos a Citrix Application Delivery Management (ADM).

Se enumeran los procedimientos CLI y GUI para esta configuración de ejemplo. Se utilizan los siguientes valores de ejemplo. Reemplácelos con datos válidos para direcciones IP, certificado SSL y clave, y parámetros LDAP.

| Nombre | Valores utilizados en la configuración de ejemplo |
|---|---|
| Dirección NSIP | 192.0.2.5 |
| Dirección IP de subred | 198.51.100.5 |
| Dirección IP del servidor virtual LDAP | 192.0.2.116 |
| Dirección IP del servidor de nombres DNS | 203.0.113.2 |
| Dirección IP del servidor proxy | 192.0.2.100 |
| Dirección IP MAS | 192.0.2.41 |
| Certificado de CA para intercepción SSL | ns-swg-ca-certkey (certificado: Ns_swg_ca.crt y clave: Ns_swg_ca.key) |
| DN base LDAP | CN=Usuarios, DC=CTXNSSFB, DC=COM |
| DN de enlace LDAP | CN=Administrador, CN=Usuarios, DC=CTXNSSFB, DC=COM |
| Contraseña de DN de enlace LDAP | Zzzzzz |

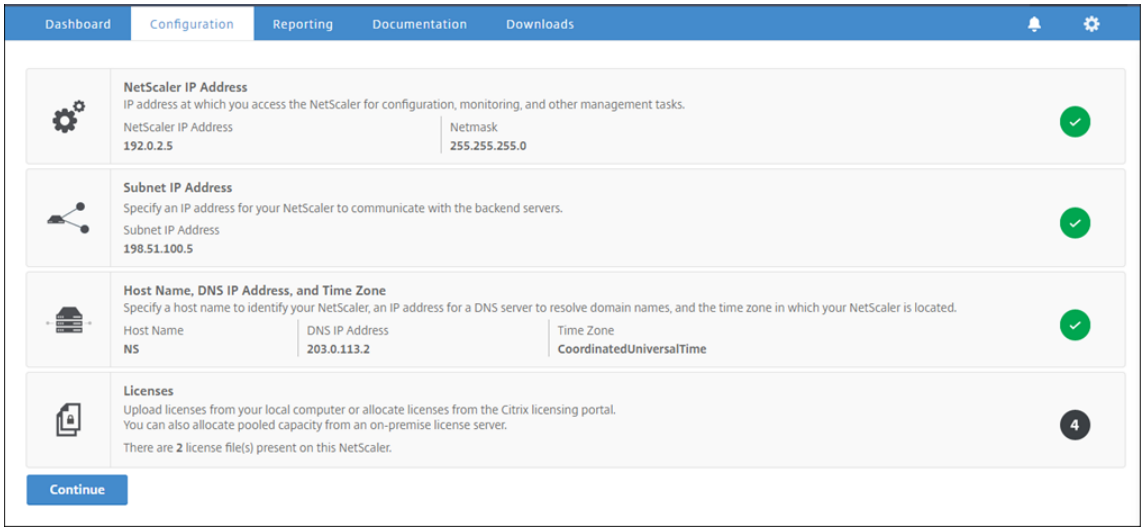
## Uso del asistente de puerta de enlace web segura para configurar la interceptación y el examen del tráfico hacia y desde la red empresarial

Para crear una configuración para interceptar y examinar el tráfico cifrado, además del otro tráfico hacia y desde una red, es necesario configurar la configuración de proxy, la configuración de SSLi, la configuración de autenticación de usuario y la configuración de filtrado de URL. Los siguientes procedimientos incluyen ejemplos de los valores introducidos.

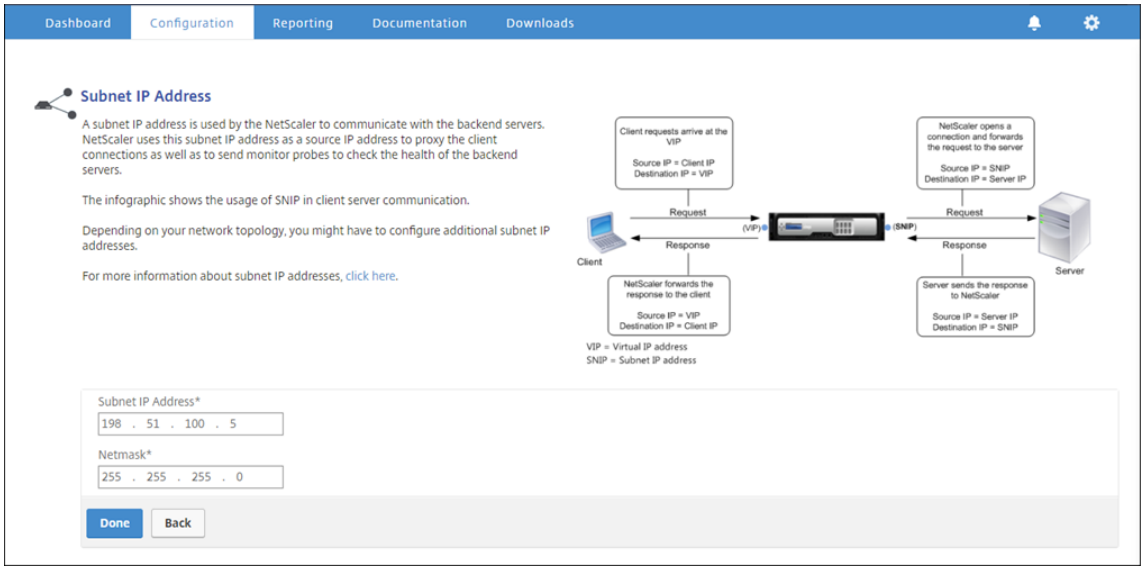
### Configurar la dirección de SNIP y el servidor de nombres DNS

1. En un explorador web, escriba la dirección NSIP. Por ejemplo, `http://192.0.2.5`.
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador. Aparecerá la siguiente pantalla.

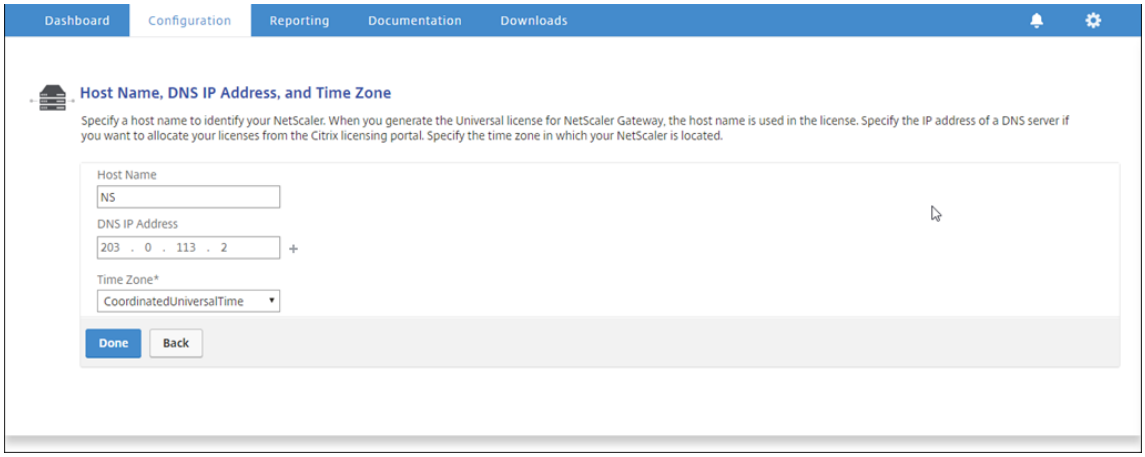



3. Haga clic dentro de la sección **Dirección IP de subred** e introduzca una dirección IP.




4. Haga clic en **Done**.
5. Haga clic dentro de la sección **Nombre de host, Dirección IP DNS y Zona horaria** e introduzca valores para estos campos.

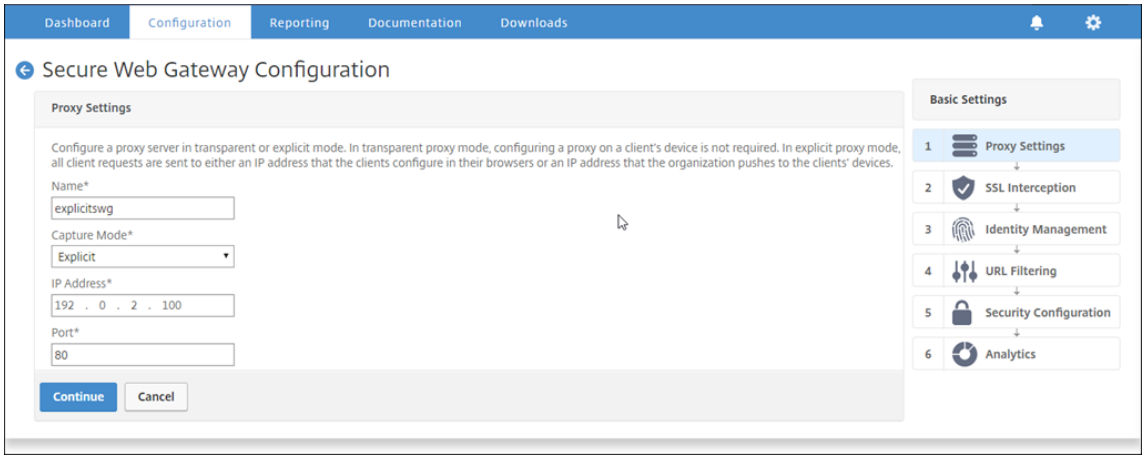
 




6. Haga clic en **Listo** y, a continuación, en **Continuar**.

## Configurar la configuración del proxy

1. Desplácese hasta **Secure Web Gateway** > **Asistente para Secure Web Gateway**.
2. Haga clic en **Comenzar** y, a continuación, haga clic en **Continuar**.
3. En el cuadro de diálogo **Configuración de proxy**, escriba un nombre para el servidor proxy explícito.
4. En **Modo de captura,** seleccione **Explícito**.
5. Introduzca una dirección IP y un número de puerto.

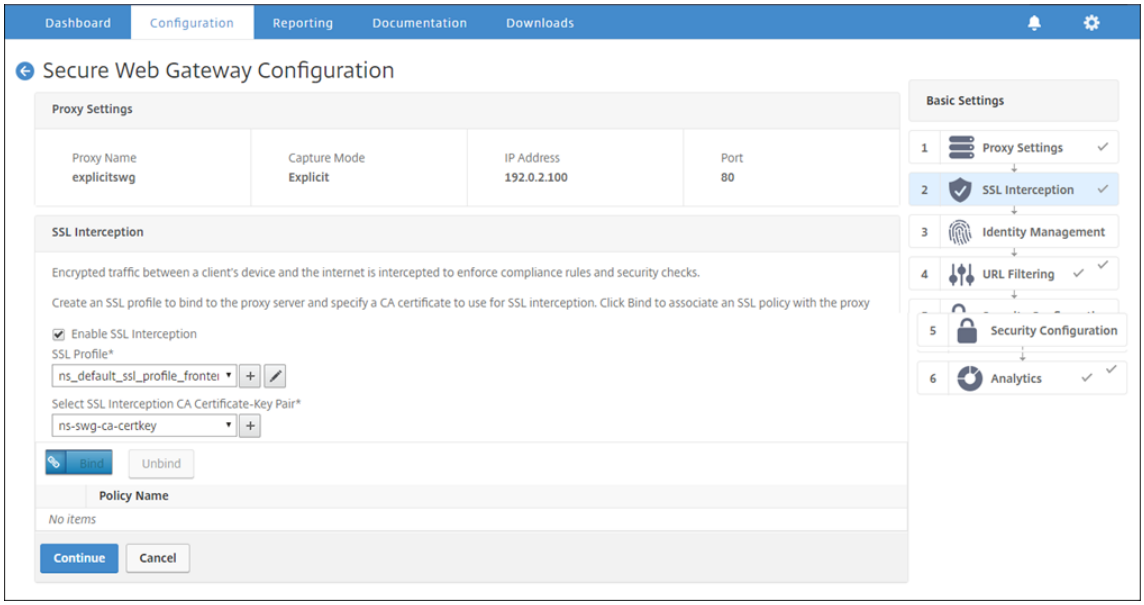



6. Haga clic en **Continuar**.

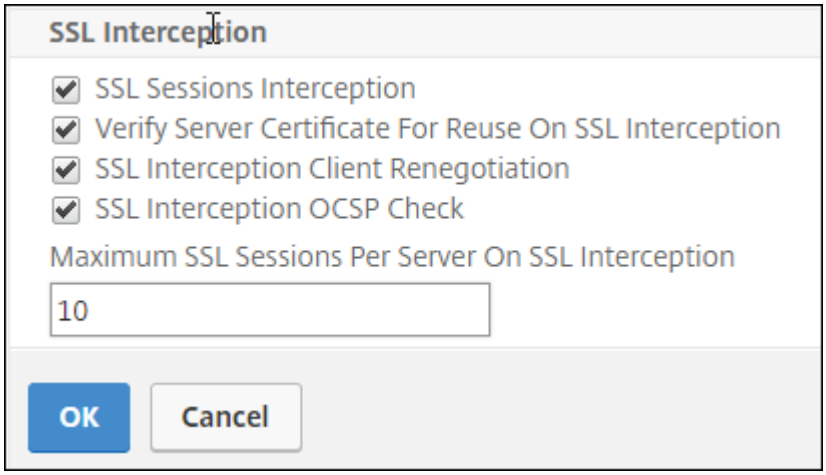
## Configurar la configuración de intercepción SSL

1. Seleccione **Habilitar intercepción SSL**.

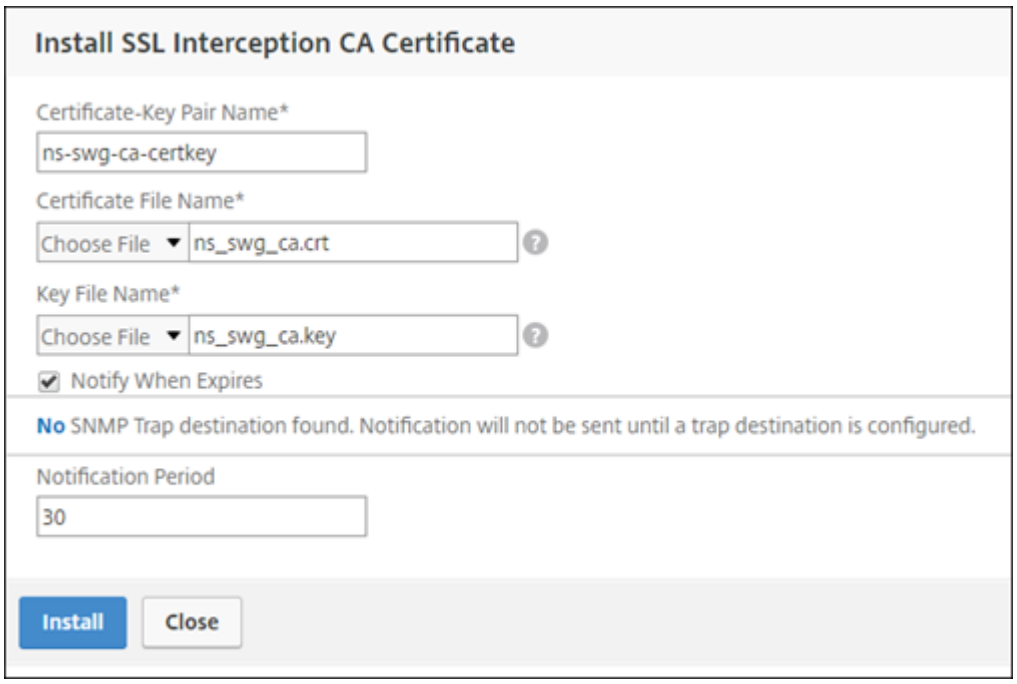



2. En **Perfil SSL**, haga clic en "+"para agregar un nuevo perfil SSL front-end y habilitar la **intercepción de sesiones SSL**en este perfil.

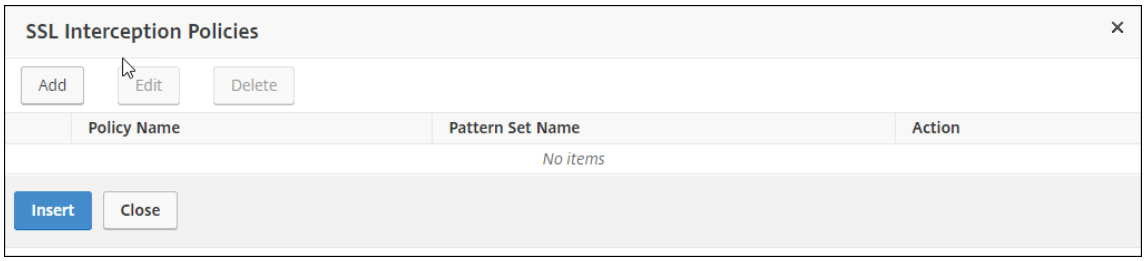



3. Haga clic en **Aceptar** y, a continuación, haga clic en **Listo**.
4. En **Seleccionar par de claves de certificado de CA de intercepción SSL**, haga clic en "+"para instalar un par de claves de certificado de CA para intercepción de SSL.

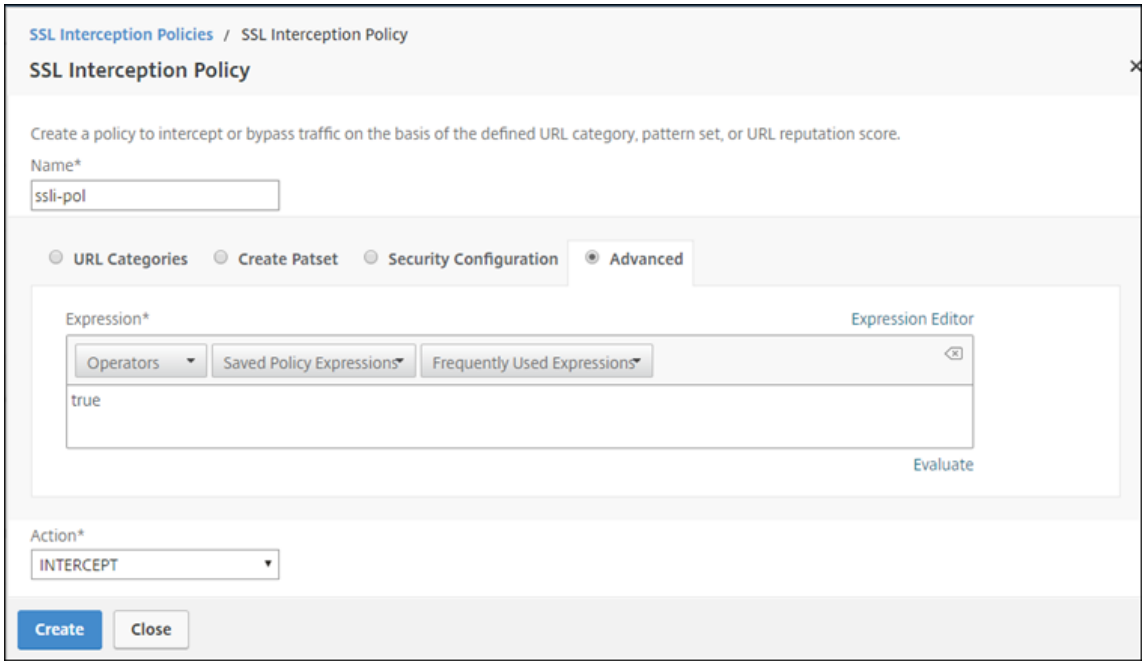



5. Haga clic en **Instalar** y, a continuación, haga clic en **Cerrar**.
6. Agregue una directiva para interceptar todo el tráfico. Haga clic en **Vincular** y, a continuación, haga clic en **Agregar**.



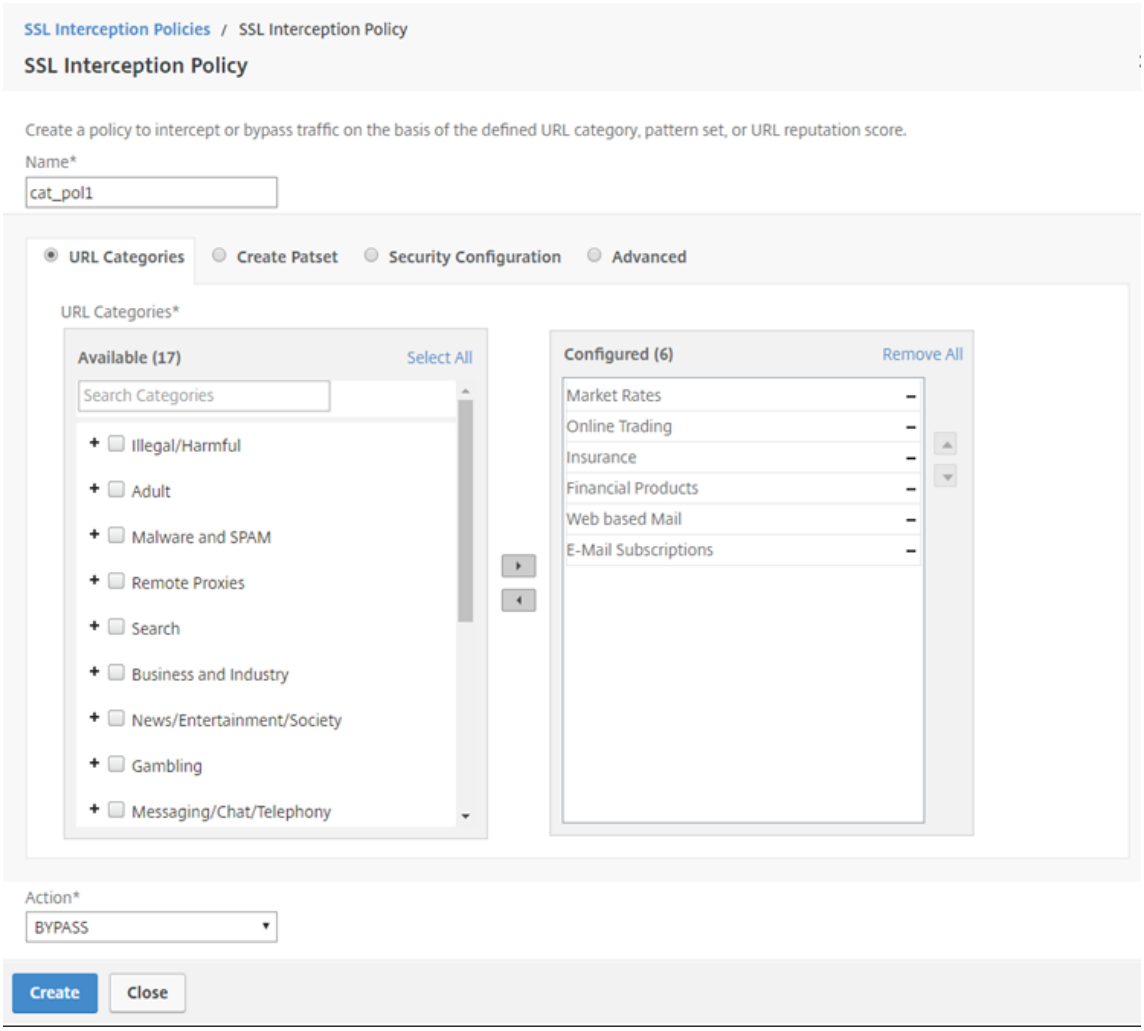

7. Escriba un nombre para la directiva y seleccione **Avanzadas**. En el editor de expresiones, escriba true.
8. En **Acción**, seleccione **INTERCEPCIÓN**.

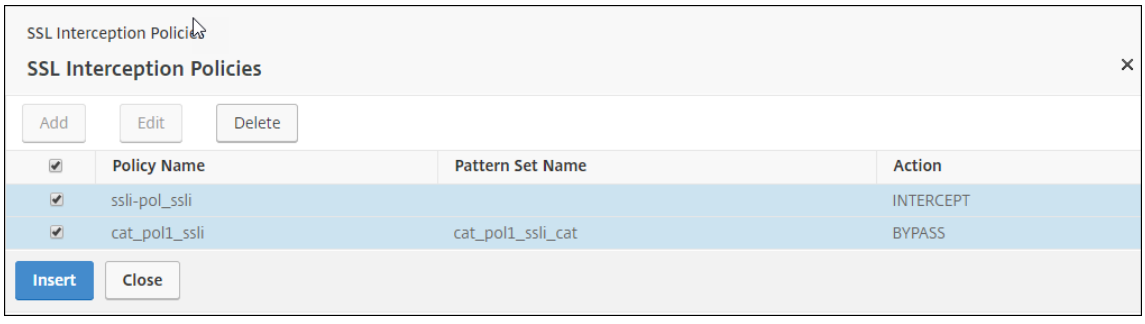



9. Haga clic en **Crear** y, a continuación, haga clic en **Agregar** para agregar otra directiva para omitir la información confidencial.
10. Escriba un nombre para la directiva y, en **Categorías de URL**, haga clic en **Agregar**.
11. Seleccione las categorías **Finanzas** y **Correo electrónico** y muévalas a la lista **Configurada**.
12. En **Acción**, seleccione **PASIVAR**.

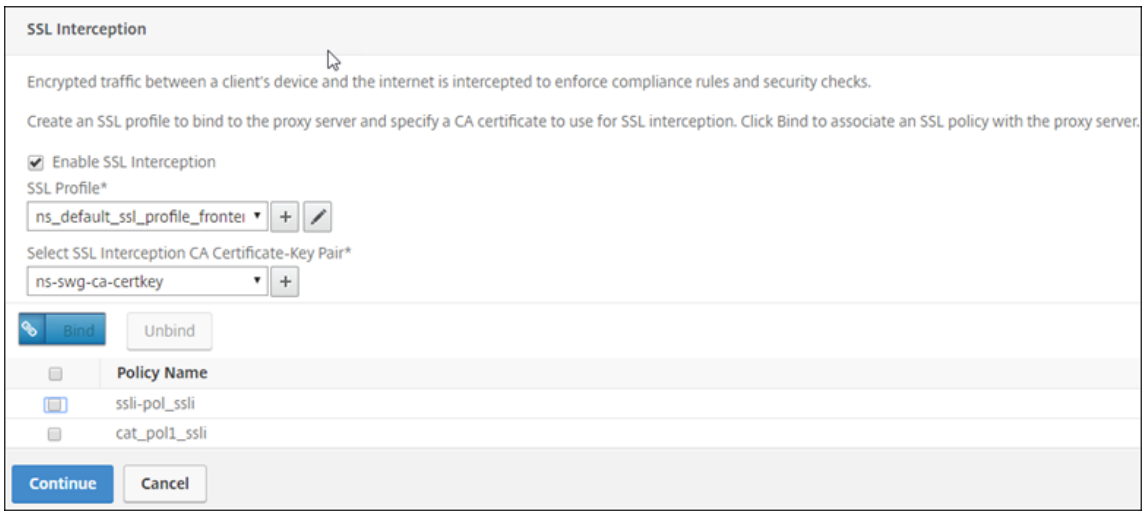



13. Haga clic en **Crear**.
14. Seleccione las dos directivas creadas anteriormente y haga clic en **Insertar**.



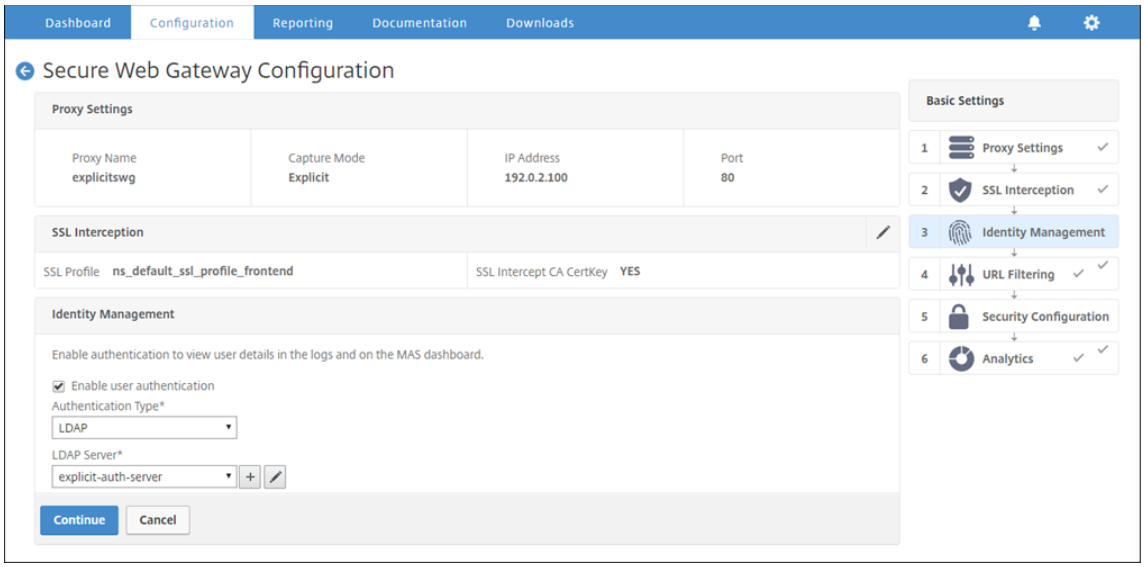

15. Haga clic en **Continuar**.



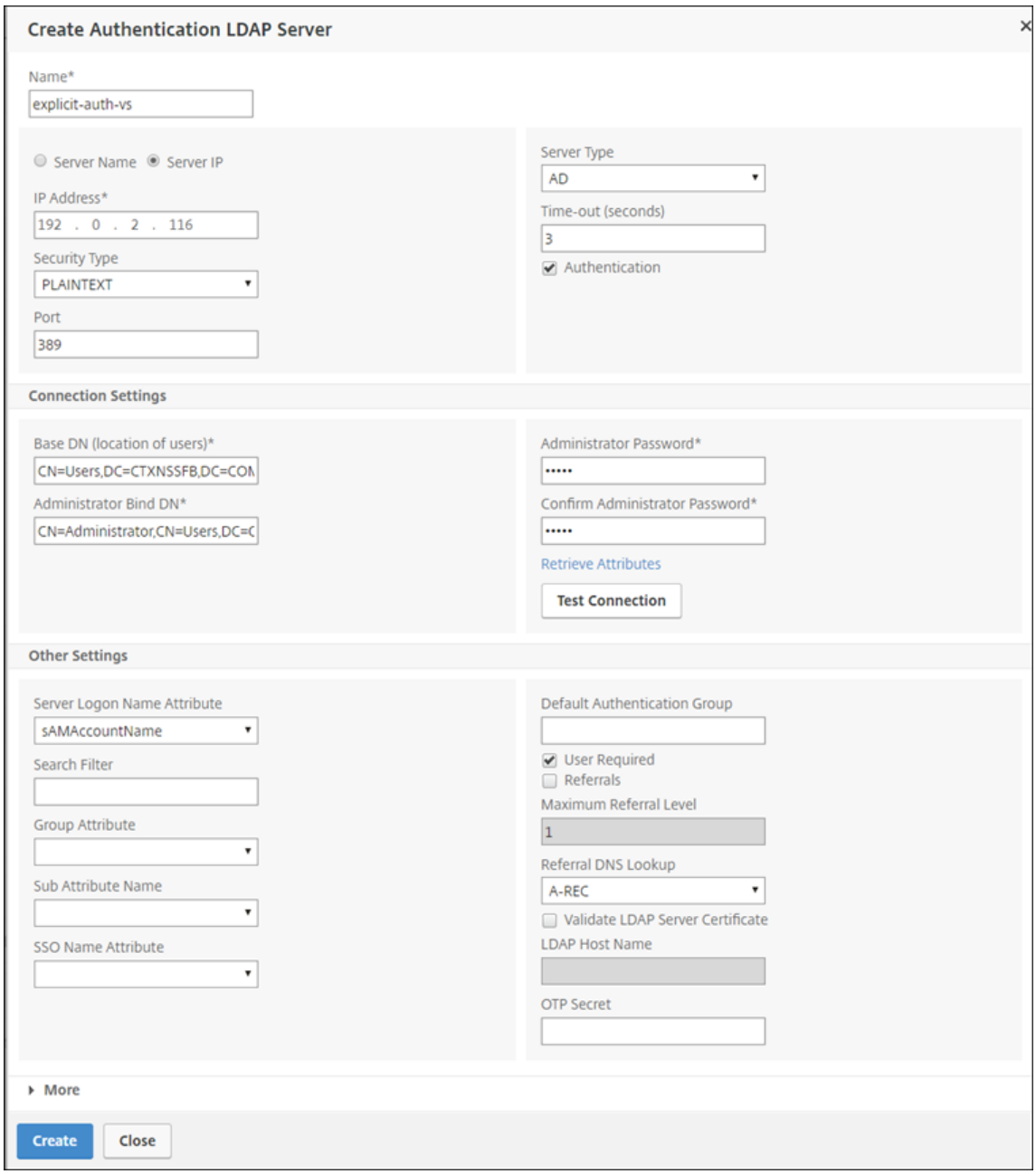

## Configurar la configuración de autenticación de usuario

1. Seleccione **Habilitar autenticación de usuario**. En el campo **Tipo de autenticación**, seleccione **LDAP**.




2. Agregue detalles del servidor LDAP.

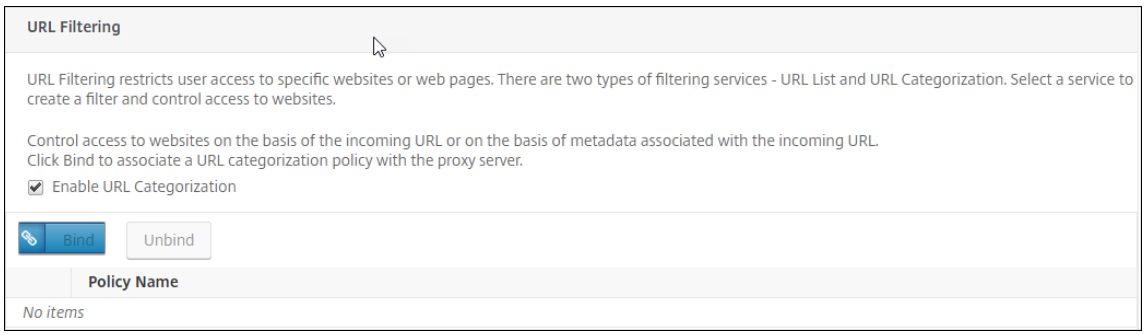



3. Haga clic en **Crear**.
4. Haga clic en **Continuar**.

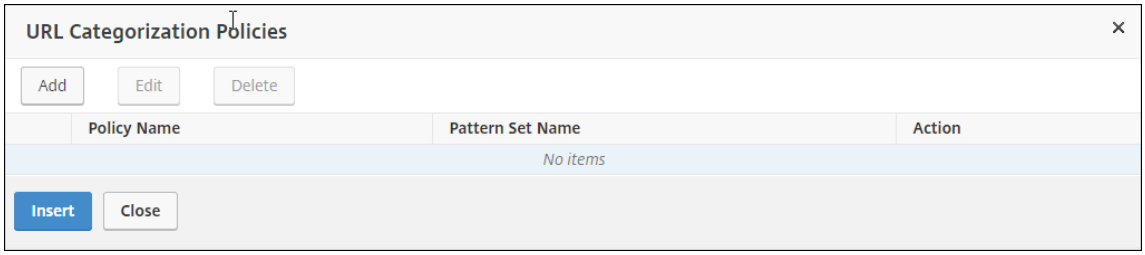
## Configurar opciones de filtrado de URL

1. Seleccione **Habilitar categorización de URL y,** a continuación, haga clic en **Vincular**.

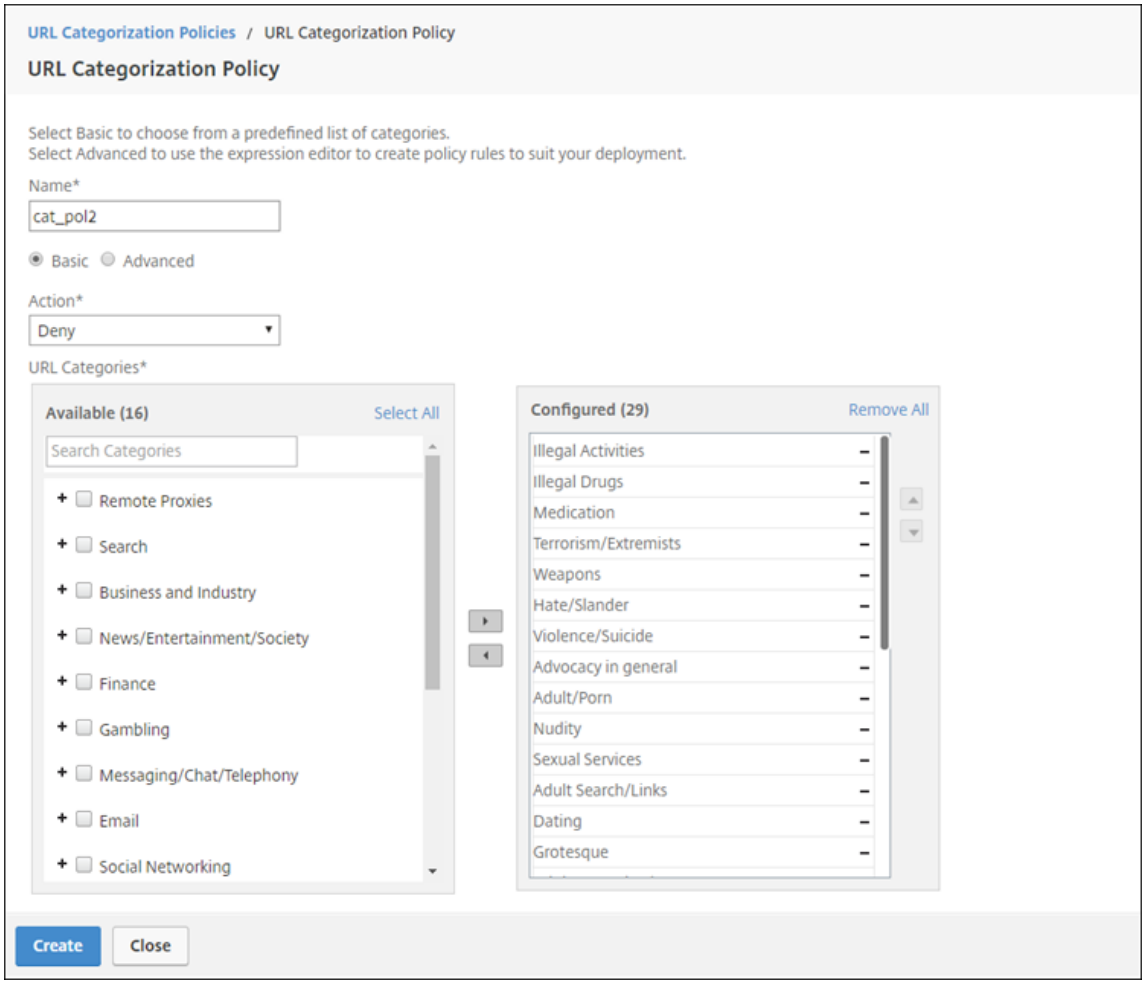



2. Haga clic en **Agregar**.

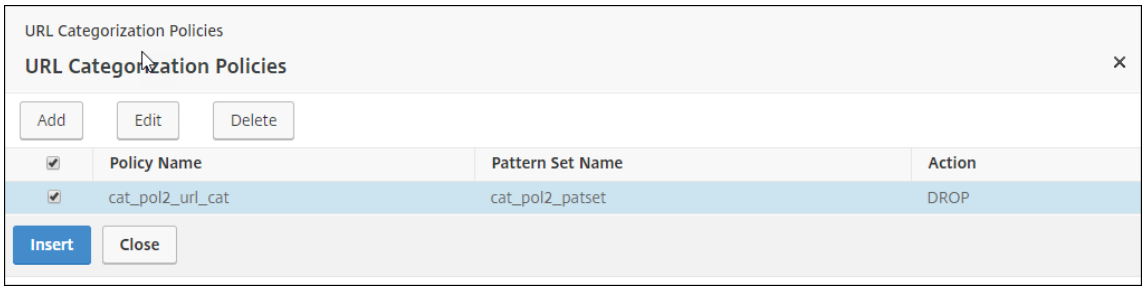



3. Introduzca un nombre para la directiva. En **Acción**, seleccione **Denegar**. Para **Categorías de URL**, seleccione **Ilegal o nocivo**, **Adulto** y **Malware y SPAM**, y muévalos a la lista **Configurada**.

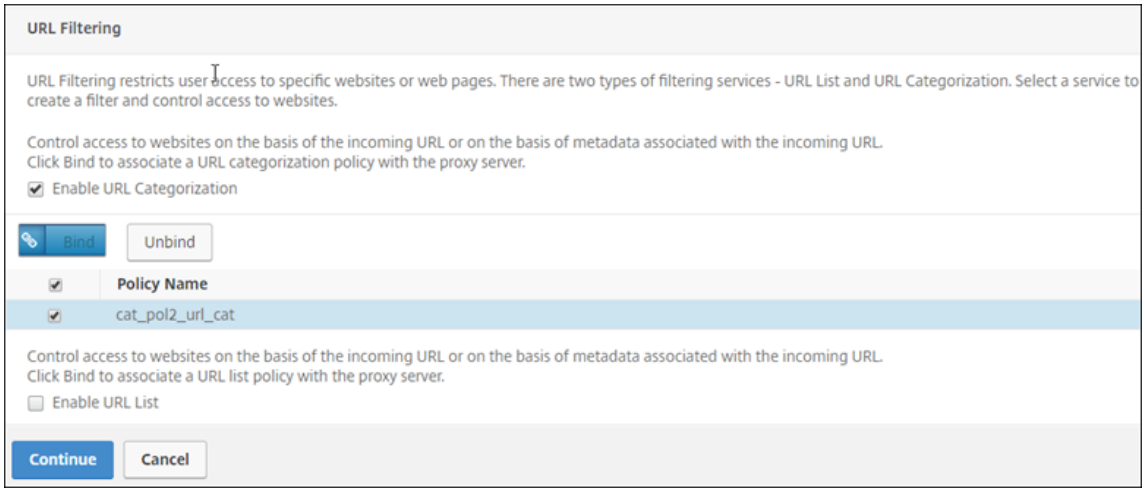



4. Haga clic en **Crear**.
5. Seleccione la directiva y, a continuación, haga clic en **Insertar**.

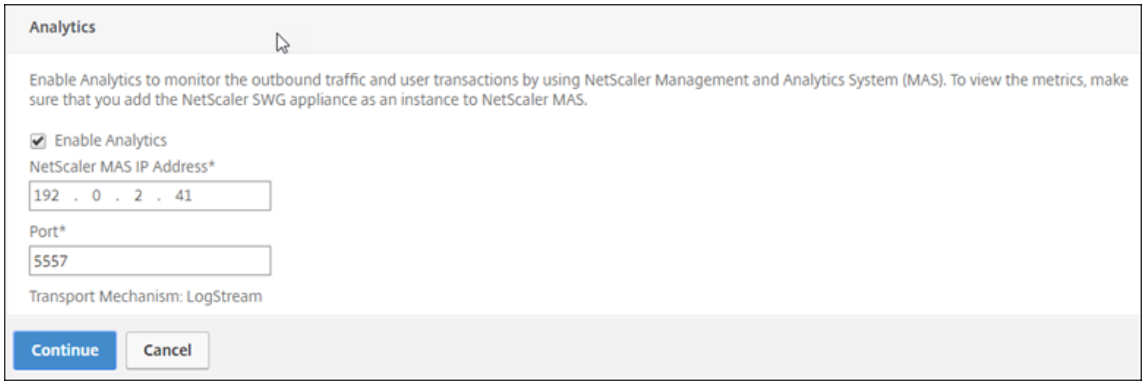



6. Haga clic en **Continuar**.

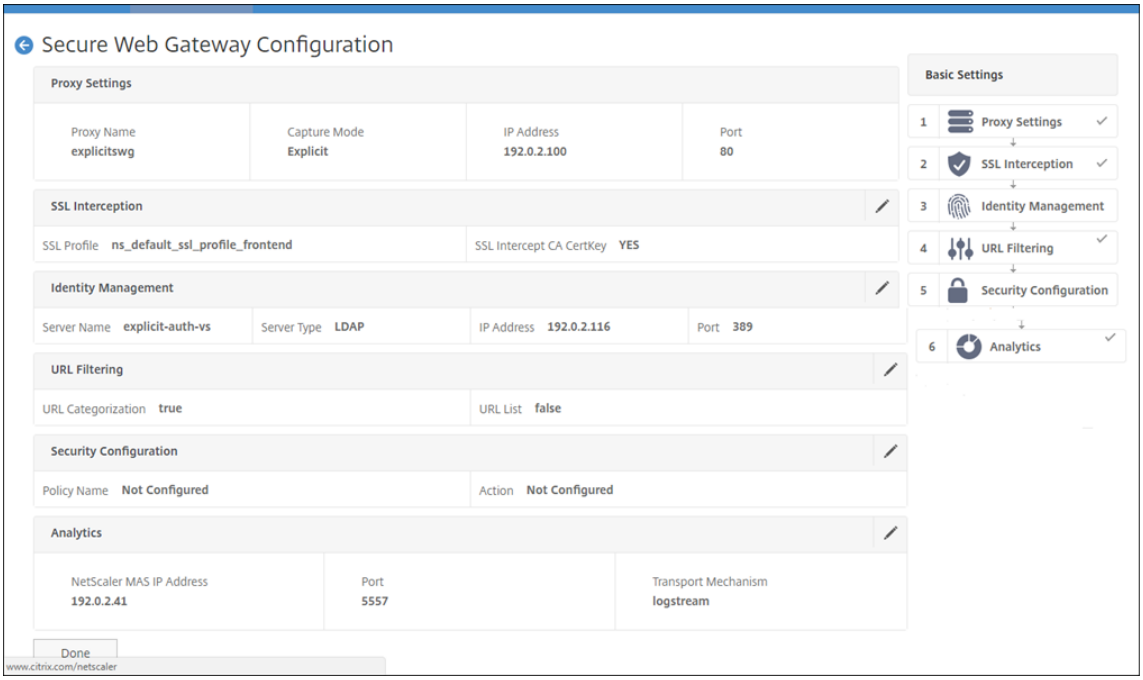



7. Haga clic en **Continuar**.
8. Haga clic en **Habilitar análisis**.
9. Introduzca la dirección IP de Citrix ADM y, para **Port**, especifique 5557.




10. Haga clic en **Continuar**.
11. Haga clic en **Done**.




Utilice Citrix ADM para ver métricas clave para los usuarios y determinar lo siguiente:

- Comportamiento de navegación de los usuarios de su empresa.
- Categorías de URL a las que acceden los usuarios de su empresa.
- Exploradores utilizados para acceder a las URL o dominios.

Utilice esta información para determinar si el sistema del usuario está infectado por malware o para comprender el patrón de consumo de ancho de banda del usuario. Puede ajustar las directivas de su dispositivo Citrix SWG para restringir estos usuarios o bloquear algunos sitios web más. Para obtener más información sobre cómo ver las métricas en MAS, consulte el caso de uso "Inspecting Endpoints" en Casos de uso MAS.

> **Nota**
>
> Establezca los siguientes parámetros mediante la CLI.

```
set syslogparams -sslInterception ENABLED

set cacheparameter -memLimit 100

set appflow param -AAAUserName ENABLED
<!--NeedCopy-->
```

### Ejemplo CLI

El siguiente ejemplo incluye todos los comandos utilizados para configurar la interceptación y el examen del tráfico hacia y desde la red empresarial.

**Configuración general**:

```
    add ns ip 192.0.2.5 255.255.255.0

    add ns ip 198.51.100.5 255.255.255.0 -type SNIP

    add dns nameServer 203.0.113.2

    add ssl certKey ns-swg-ca-certkey -cert ns_swg_ca.crt -key
       ns_swg_ca.key

    set syslogparams -sslInterception ENABLED

    set cacheparameter -memLimit 100

    set appflow param -AAAUserName ENABLED
<!--NeedCopy-->
```

**Configuración de autenticación**:

```
add authentication vserver explicit-auth-vs SSL

bind ssl vserver explicit-auth-vs -certkeyName ns-swg-ca-certkey

add authentication ldapAction swg-auth-action-explicit -serverIP
   192.0.2.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "CN=
   Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
   zzzzzz -ldapLoginName sAMAccountName

add authenticationpolicy swg-auth-policy -rule true -action swg-auth-
   action-explicit

bind authentication vserver explicit-auth-vs -policy swg-auth-policy -
   priority 1
<!--NeedCopy-->
```

**Configuración de servidor proxy e intercepción SSL**:

```
add cs vserver explicitswg PROXY 192.0.2.100 80 -Authn401 ENABLED -
   authnVsName explicit-auth-vs

set ssl parameter -defaultProfile ENABLED

add ssl profile swg_profile -sslInterception ENABLED

bind ssl profile swg_profile -ssliCACertkey ns-swg-ca-certkey

set ssl vserver explicitswg -sslProfile swg_profile

add ssl policy ssli-pol_ssli -rule true -action INTERCEPT

bind ssl vserver explicitswg -policyName ssli-pol_ssli -priority 100 -
   type INTERCEPT_REQ
```

```
<!--NeedCopy-->
```

**Configuración de categorías de URL**:

```
add ssl policy cat_pol1_ssli -rule "client.ssl.client_hello.SNI.
    URL_CATEGORIZE(0,0).GROUP.EQ("Finance") || client.ssl.client_hello.
    SNI.URL_CATEGORIZE(0,0).GROUP.EQ("Email")" -action BYPASS

bind ssl vserver explicitswg -policyName cat_pol1_ssli -priority 10 -
    type INTERCEPT_REQ

add ssl policy cat_pol2_ssli -rule "client.ssl.client_hello.sni.
    url_categorize(0,0).GROUP.EQ("Adult") || client.ssl.client_hello.sni
    .url_categorize(0,0).GROUP.EQ("Malware and SPAM") || client.ssl.
    client_hello.SNI.URL_CATEGORIZE(0,0).GROUP.EQ("Illegal/Harmful")" -
    action RESET

bind ssl vserver explicitswg -policyName cat_pol2_ssli -priority 20 -
    type INTERCEPT_REQ
<!--NeedCopy-->
```

**Configuración de AppFlow para extraer datos en Citrix ADM**:

```
add appflow collector _swg_testswg_apfw_cl -IPAddress 192.0.2.41 -port
    5557 -Transport logstream

set appflow param -templateRefresh 60 -httpUrl ENABLED -AAAUserName
    ENABLED -httpCookie ENABLED -httpReferer ENABLED -httpMethod ENABLED
     -httpHost ENABLED -httpUserAgent ENABLED -httpContentType ENABLED -
    httpVia ENABLED -httpLocation ENABLED -httpDomain ENABLED -
    cacheInsight ENABLED -urlCategory ENABLED

add appflow action _swg_testswg_apfw_act -collectors
    _swg_testswg_apfw_cl -distributionAlgorithm ENABLED

add appflow policy _swg_testswg_apfw_pol true _swg_testswg_apfw_act

bind cs vserver explicitswg -policyName _swg_testswg_apfw_pol -priority
     1
<!--NeedCopy-->
```

## Caso de uso: Hacer que la red empresarial sea segura mediante el uso de ICAP para la inspección remota de malware

April 27, 2021

El dispositivo Citrix Secure Web Gateway (SWG) actúa como proxy e intercepta todo el tráfico del cliente. El dispositivo utiliza directivas para evaluar el tráfico y reenvía las solicitudes de cliente al

servidor de origen en el que reside el recurso. El dispositivo descifra la respuesta del servidor de origen y reenvía el contenido de texto sin formato al servidor ICAP para una comprobación antimalware. El servidor ICAP responde con un mensaje que indica "No se requiere adaptación", error o solicitud modificada. Dependiendo de la respuesta del servidor ICAP, el contenido solicitado se reenvía al cliente o se envía un mensaje apropiado.

Para este caso de uso, debe realizar alguna configuración general, configuración relacionada con la intercepción SSL y proxy, y configuración ICAP en el dispositivo Citrix SWG.

### Configuración general

Configure las siguientes entidades:

- Dirección NSIP
- Dirección IP de subred (SNIP)
- Servidor de nombres DNS
- Par de claves de certificado de CA para firmar el certificado de servidor para la intercepción SSL

### Configuración de servidor proxy e intercepción SSL

Configure las siguientes entidades:

- Servidor proxy en modo explícito para interceptar todo el tráfico HTTP y HTTPS saliente.
- Perfil SSL para definir la configuración SSL, como cifrados y parámetros, para las conexiones.
- Directiva SSL para definir reglas para interceptar tráfico. Establezca en true para interceptar todas las solicitudes del cliente.

Para obtener más información, consulte los siguientes temas:

- Modos de proxy
- Intercepción SSL

En la siguiente configuración de ejemplo, el servicio de detección de antimalware reside en `www.example.com`.

**Ejemplo de configuración general**:

```
add ns ip 192.0.2.5 255.255.255.0

add ns ip 198.51.100.5 255.255.255.0 -type SNIP

add dns nameServer 203.0.113.2

add ssl certKey ns-swg-ca-certkey -cert ns_swg_ca.crt -key ns_swg_ca.
    key
<!--NeedCopy-->
```

**Ejemplo de configuración de intercepción SSL y servidor proxy**:

```
add cs vserver explicitswg PROXY 192.0.2.100 80 –Authn401 ENABLED –
    authnVsName explicit-auth-vs

set ssl parameter -defaultProfile ENABLED

add ssl profile swg_profile -sslInterception ENABLED

bind ssl profile swg_profile -ssliCACertkey ns-swg-ca-certkey

set ssl vserver explicitswg -sslProfile swg_profile

add ssl policy ssli-pol_ssli -rule true -action INTERCEPT

bind ssl vserver explicitswg -policyName ssli-pol_ssli -priority 100 -
    type INTERCEPT_REQ
<!--NeedCopy-->
```

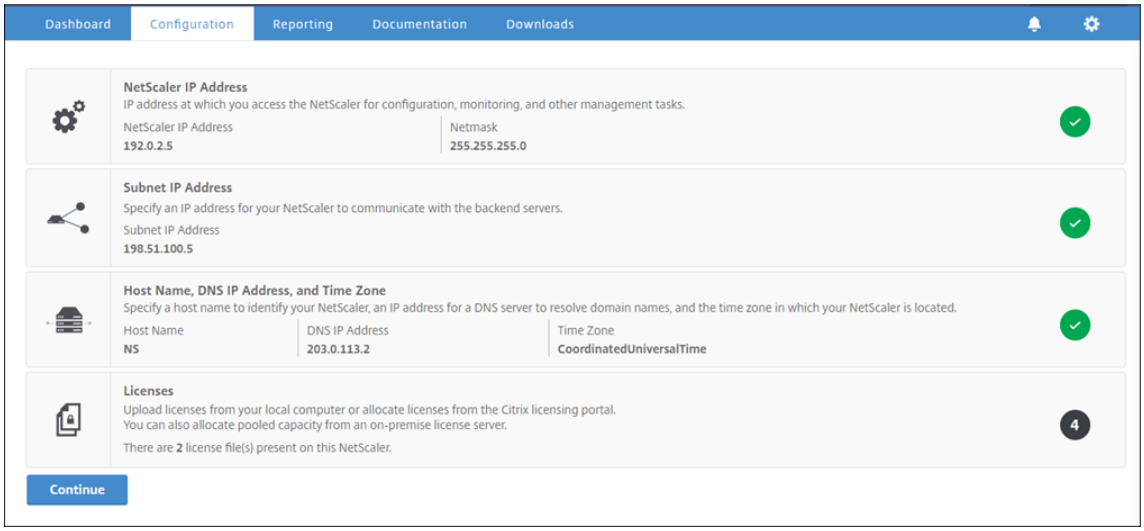
**Ejemplo de configuración ICAP**:

```
add service icap_svc 203.0.113.225 TCP 1344

enable ns feature contentinspection

add icapprofile icapprofile1 -uri /example.com -Mode RESMOD

add contentInspection action CiRemoteAction -type ICAP -serverName
    icap_svc -icapProfileName icapprofile1

add contentInspection policy CiPolicy -rule "HTTP.REQ.METHOD.NE("
    CONNECT")" -action CiRemoteAction

bind cs vserver explicitswg -policyName  CiPolicy -priority 200 -type
    response
<!--NeedCopy-->
```

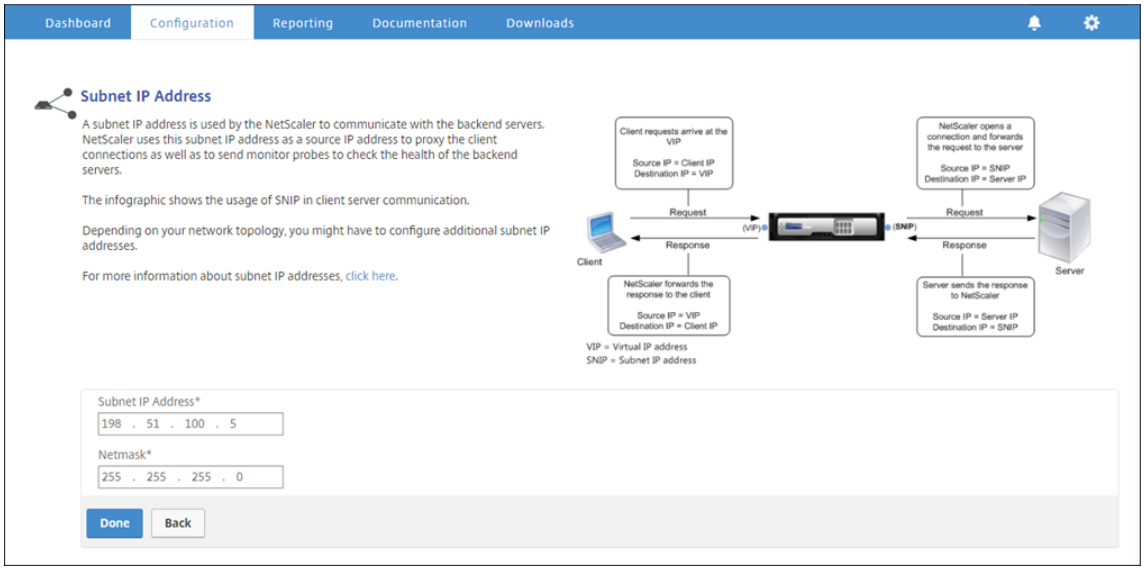
### Configurar la dirección de SNIP y el servidor de nombres DNS

1. En un explorador web, escriba la dirección NSIP. Por ejemplo, `http://192.0.2.5`.
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador. Aparecerá la siguiente pantalla.  Si no aparece la pantalla siguiente, vaya a la sección Configuración del proxy.

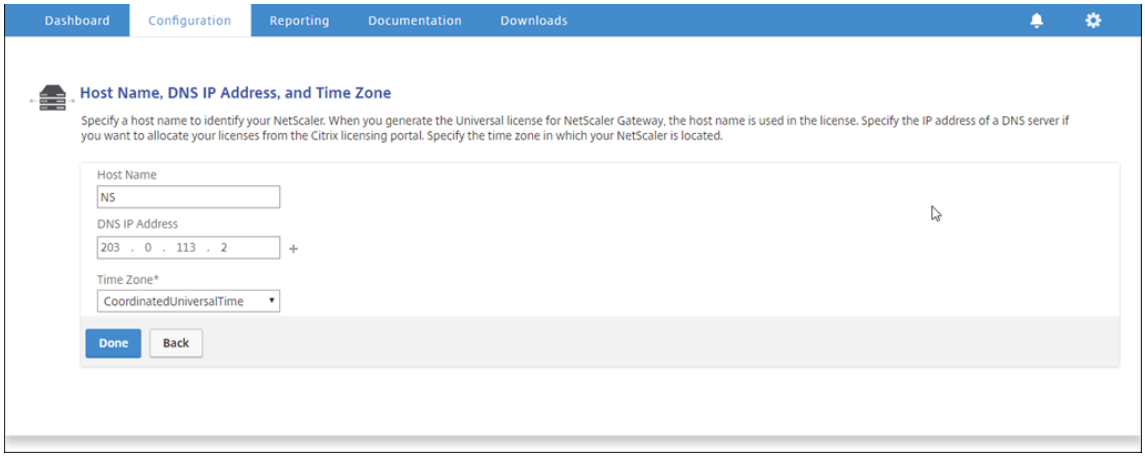



3. Haga clic dentro de la sección **Dirección IP de subred** e introduzca una dirección IP.




4. Haga clic en **Done**.
5. Haga clic dentro de la sección **Nombre de host, Dirección IP DNS y Zona horaria** e introduzca valores para estos campos.

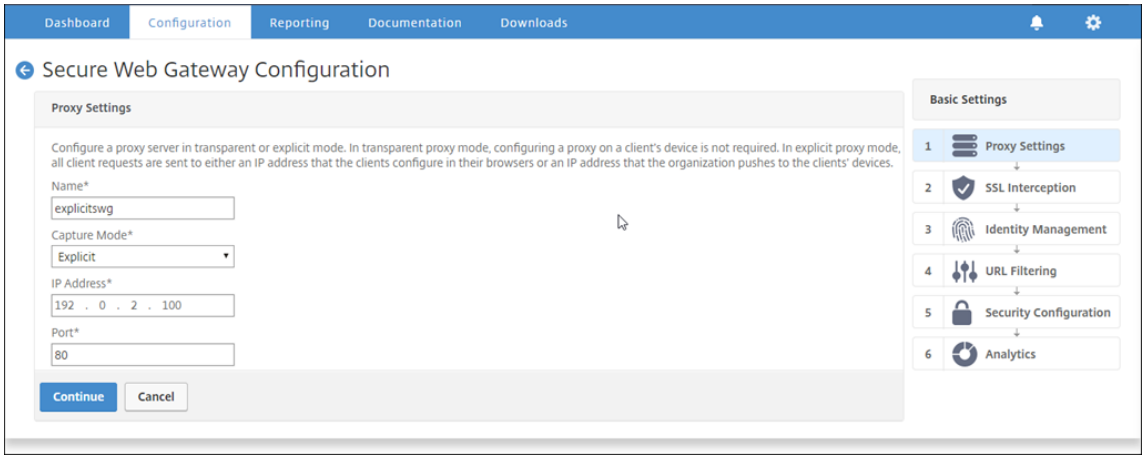
 




6. Haga clic en **Listo** y, a continuación, en **Continuar**.

## Configurar la configuración del proxy

1. Desplácese hasta **Secure Web Gateway** > **Asistente para Secure Web Gateway**.
2. Haga clic en **Comenzar** y, a continuación, haga clic en **Continuar**.
3. En el cuadro de diálogo **Configuración de proxy**, escriba un nombre para el servidor proxy explícito.
4. En **Modo de captura,** seleccione **Explícito**.
5. Introduzca una dirección IP y un número de puerto.

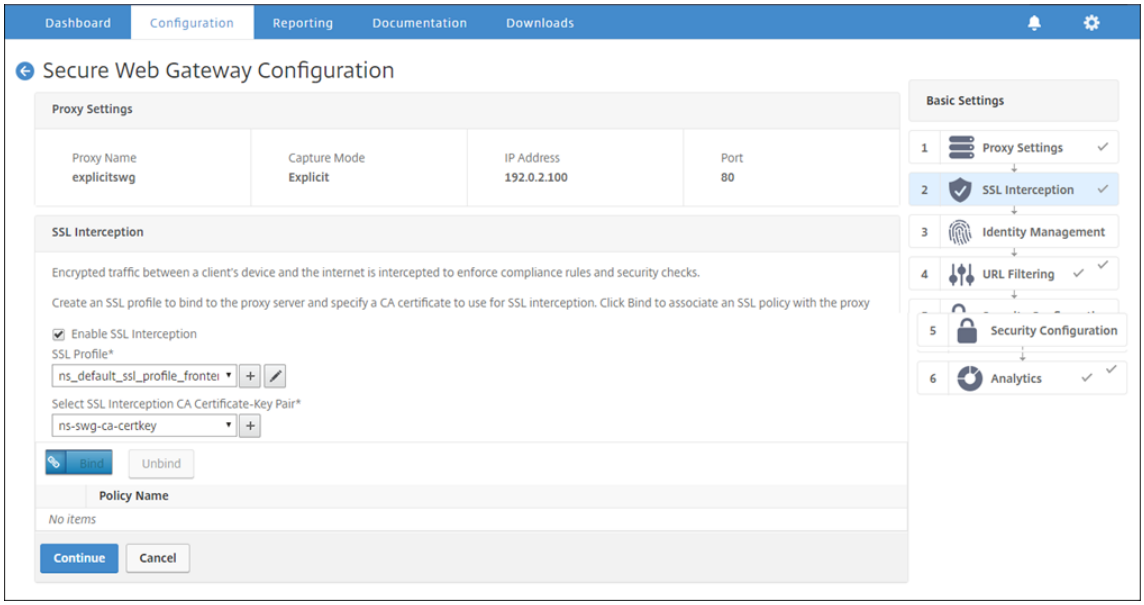



6. Haga clic en **Continuar**.

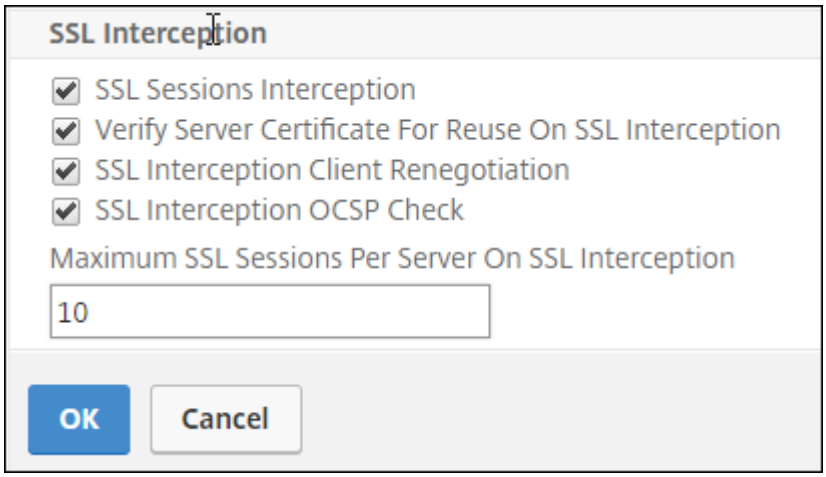
## Configurar la configuración de intercepción SSL

1. Seleccione **Habilitar intercepción SSL**.

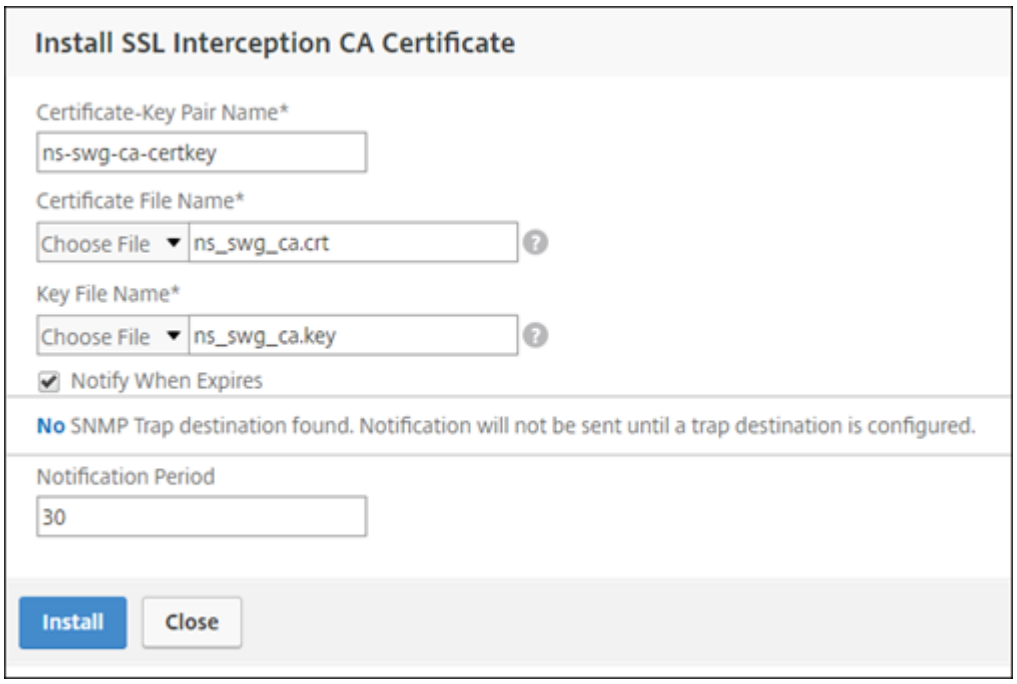



2. En **Perfil SSL**, seleccione un perfil existente o haga clic en "+"para agregar un nuevo perfil SSL front-end. Habilite la **intercepción de sesiones SSL** en este perfil. Si selecciona un perfil existente, omita el siguiente paso.




3. Haga clic en **Aceptar** y, a continuación, haga clic en **Listo**.
4. En **Seleccionar par de claves de certificado de CA de interceptación SSL**, seleccione un certificado existente o haga clic en "+"para instalar un par de claves de certificado de CA para la interceptación de SSL. Si selecciona un certificado existente, omita el siguiente paso.

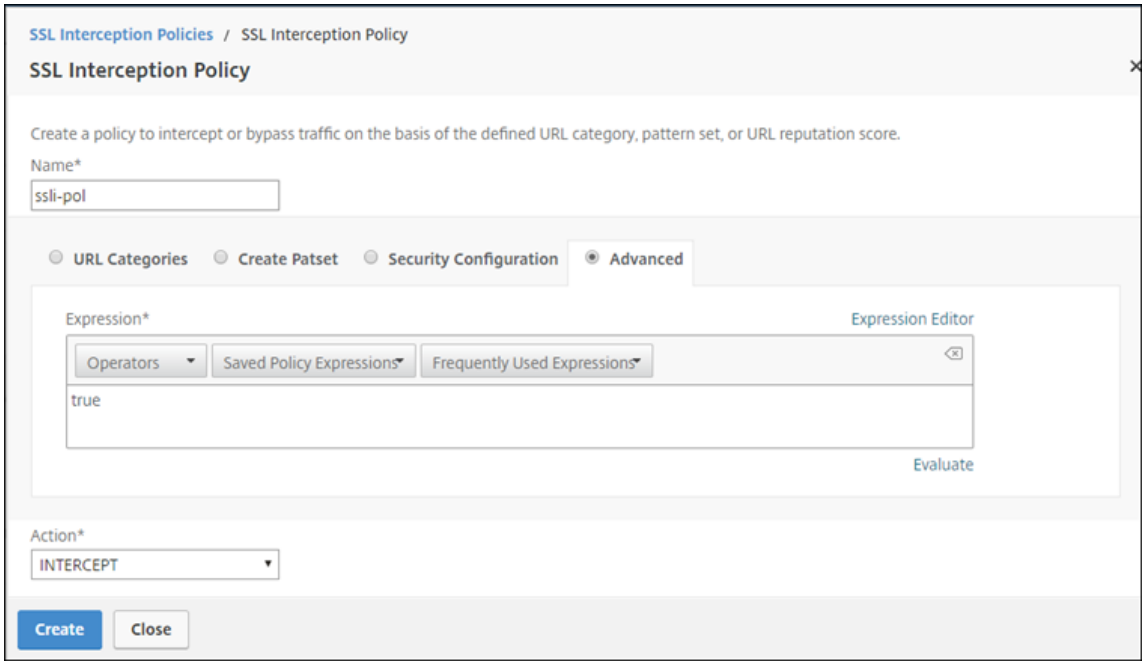
 




5. Haga clic en **Instalar** y, a continuación, haga clic en **Cerrar**.
6. Agregue una directiva para interceptar todo el tráfico. Haga clic en **Bind**. Haga clic en **Agregar** para agregar una nueva directiva o seleccione una existente. Si selecciona una directiva existente, haga clic en **Insertar** y omita los tres pasos siguientes.


7. Escriba un nombre para la directiva y seleccione **Avanzadas**. En el editor de expresiones, escriba true.
8. En **Acción**, seleccione **INTERCEPCIÓN**.

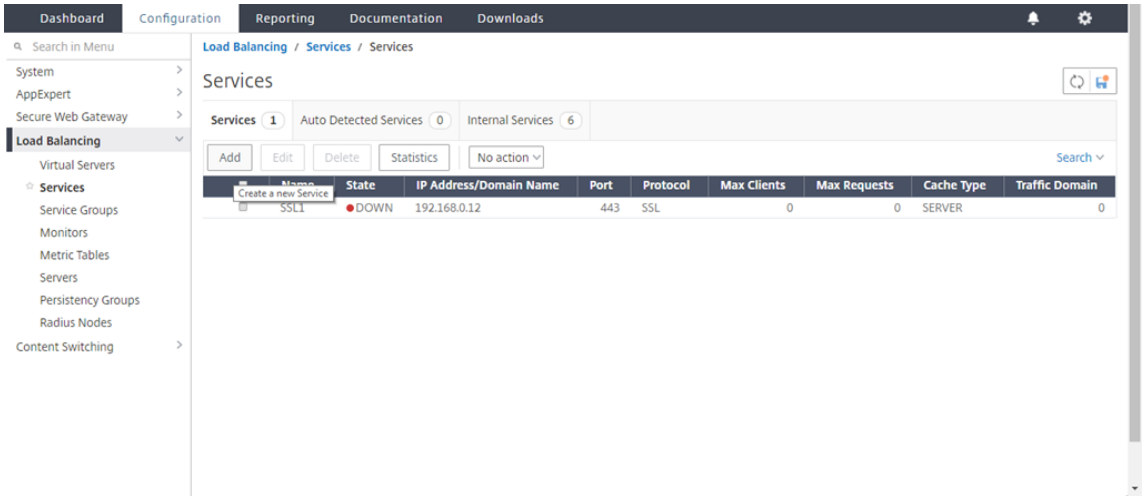
 




9. Haga clic en **Crear**.
10. Haga clic en **Continuar** cuatro veces y, a continuación, haga clic en **Listo**.

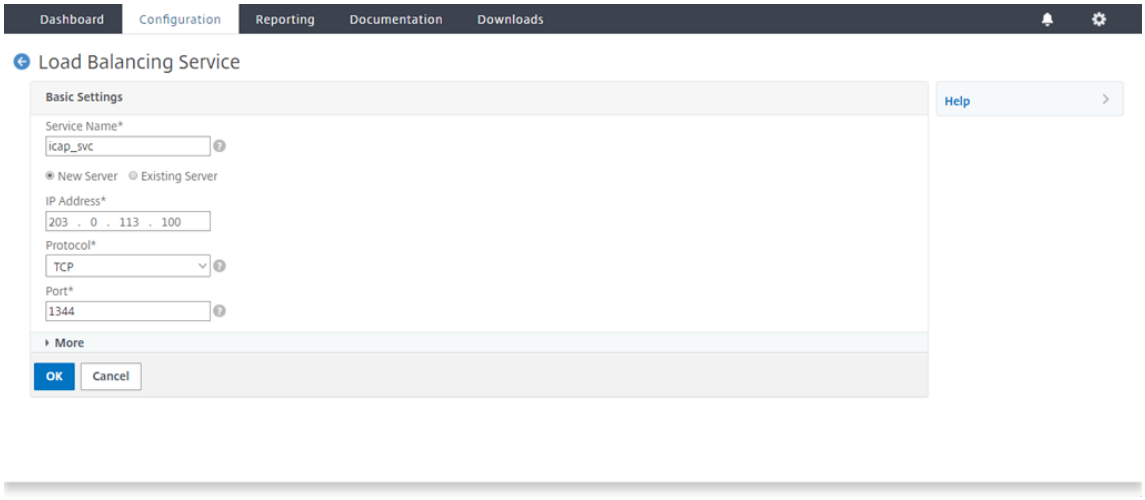
## Configurar la configuración de ICAP

1. Desplácese hasta **Equilibrio de carga** > **Servicios** y haga clic en **Agregar**.

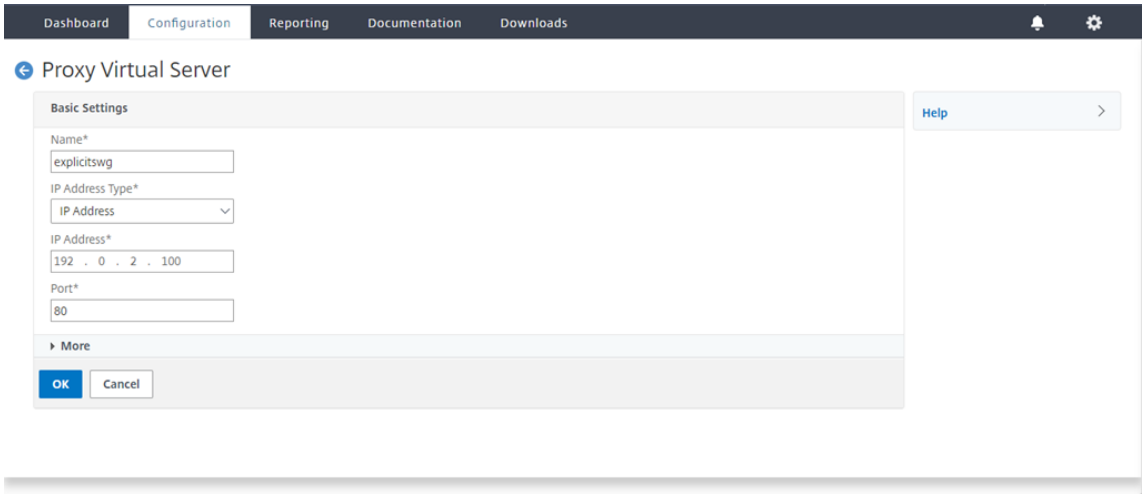



2. Escriba un nombre y una dirección IP. En **Protocolo**, seleccione **TCP**. En **Puerto**, escriba **1344**. Haga clic en **OK**.

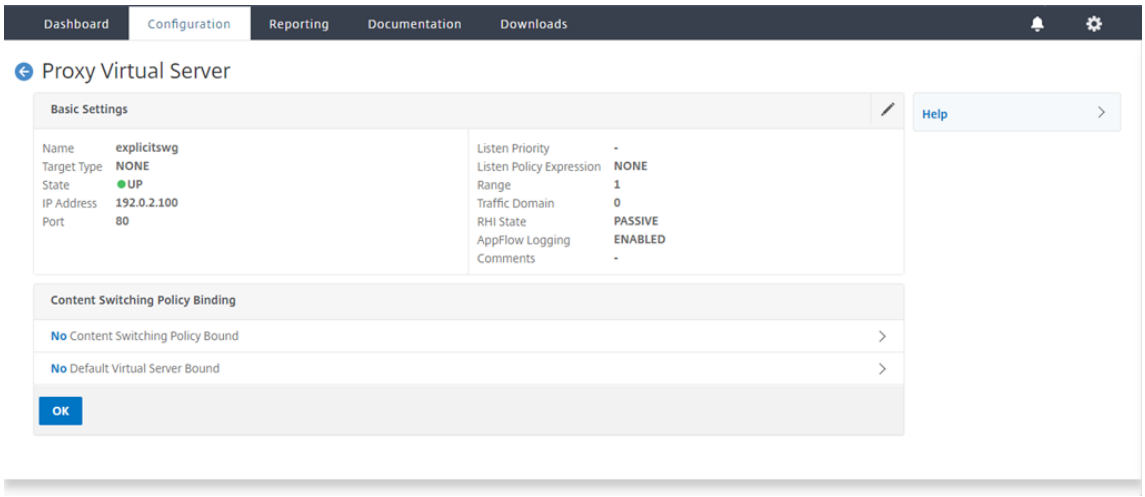
 




3. Vaya a **Secure Web Gateway** > **Proxy Virtual Servers**. Agregue un servidor virtual proxy o seleccione un servidor virtual y haga clic en **Modificar**. Después de introducir los detalles, haga clic en **Aceptar**.

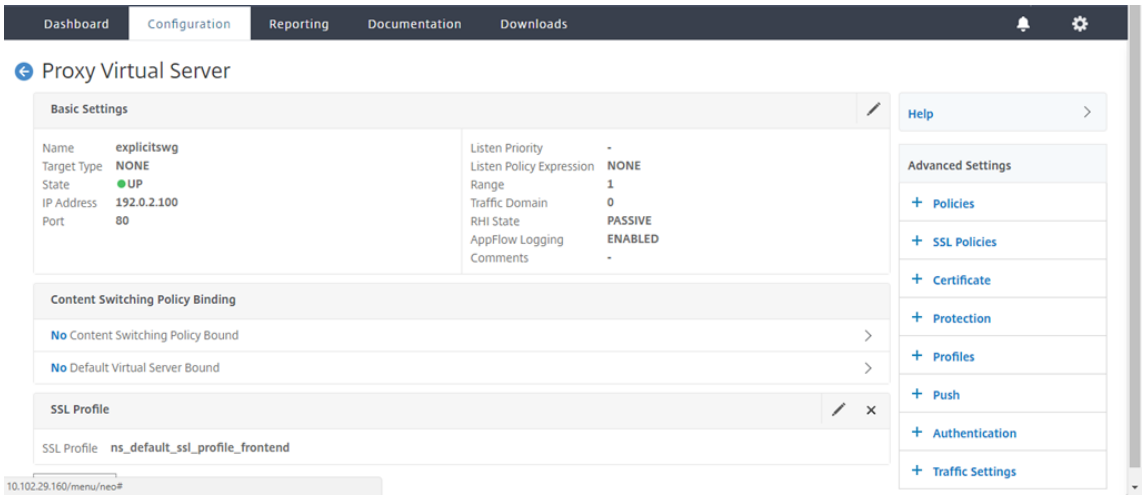



Vuelva a hacer clic en **Aceptar**.

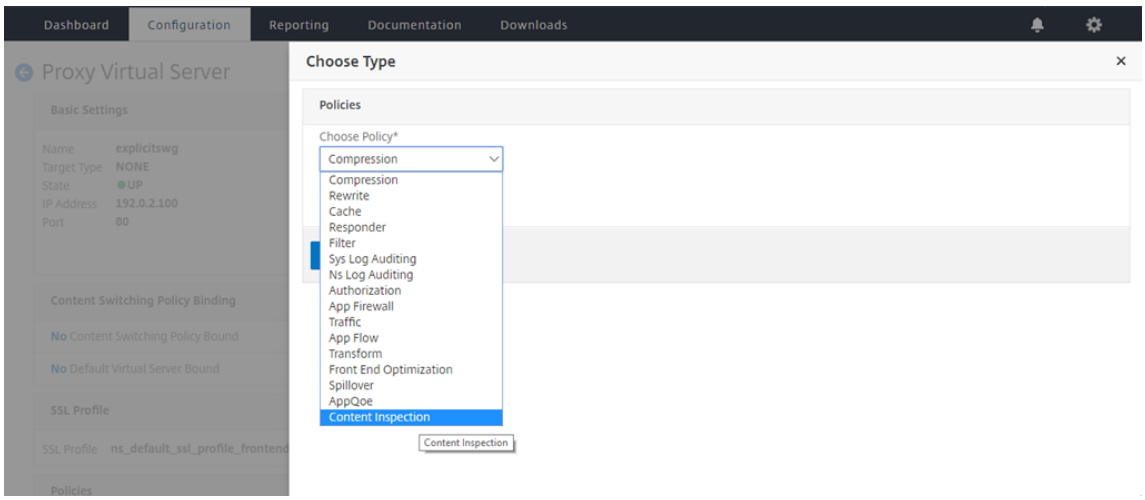


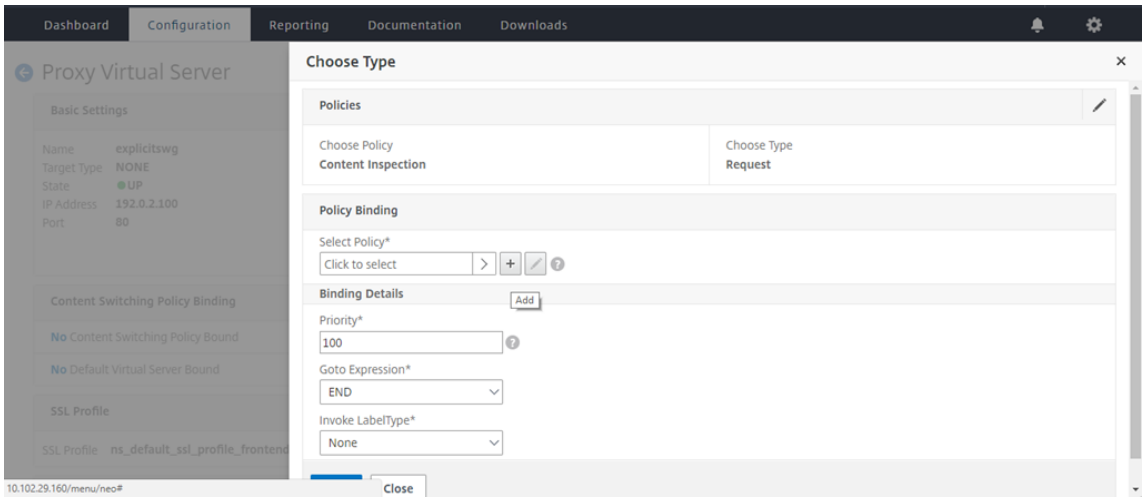
4. En **Configuración avanzada**, haga clic en **Directivas**.




5. En **Elegir directiva**, seleccione **Inspección de contenido**. Haga clic en **Continuar**.

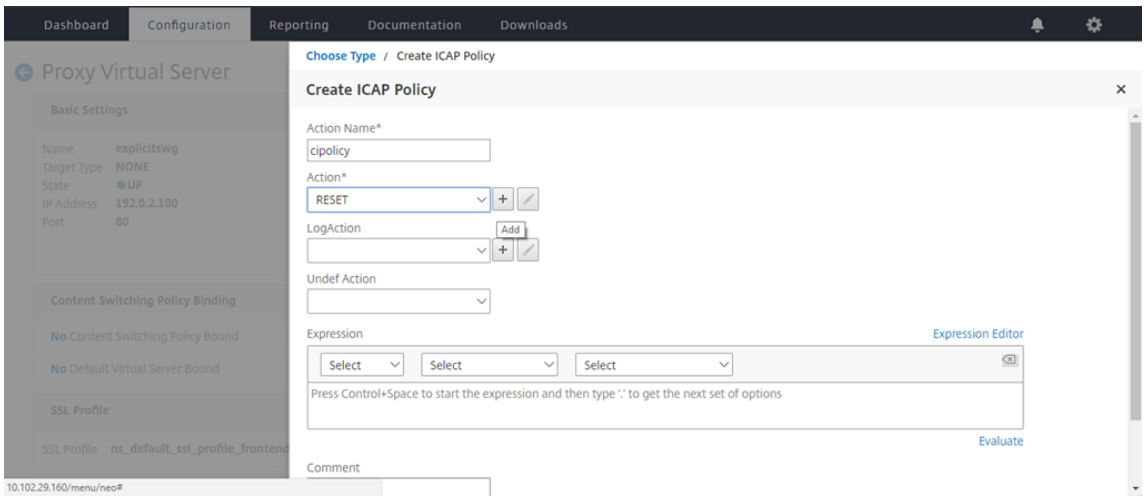



6. En **Seleccionar directiva**, haga clic en el signo “+”para agregar una directiva.

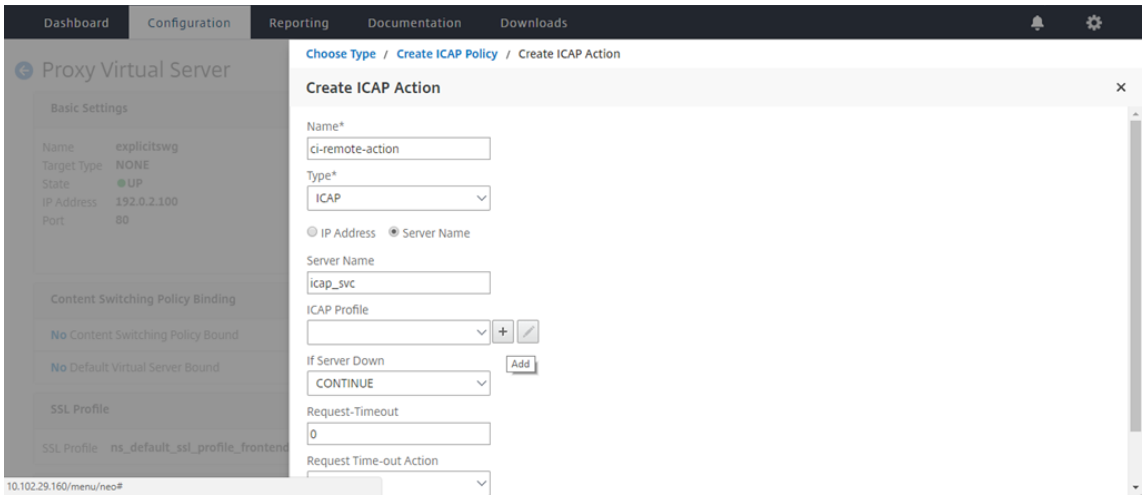


7. Introduzca un nombre para la directiva. En **Acción**, haga clic en el signo "+"para agregar una acción.

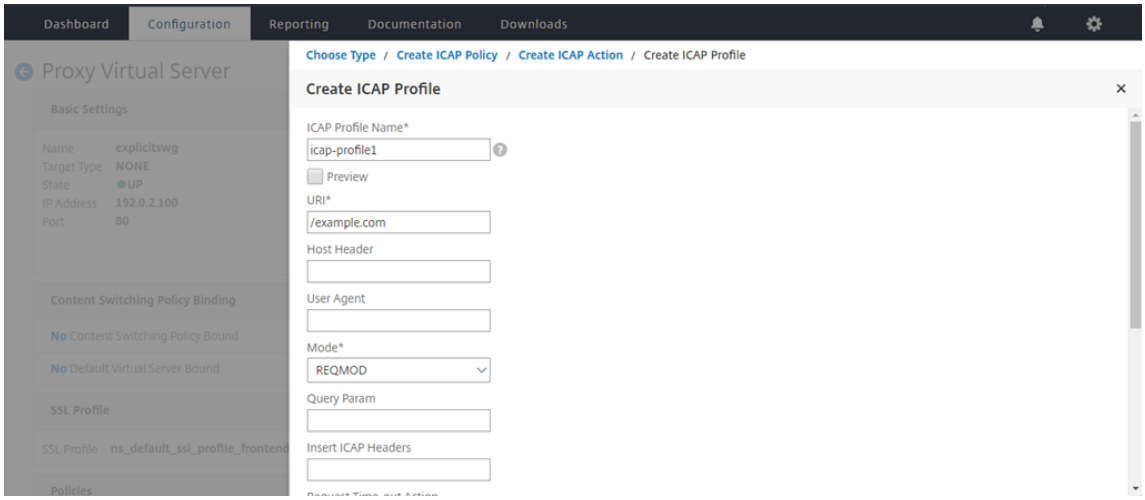



8. Escriba un nombre para la acción. En **Nombre del servidor**, escriba el nombre del servicio TCP creado anteriormente. En **Perfil ICAP**, haga clic en el signo "+"para agregar un perfil ICAP.

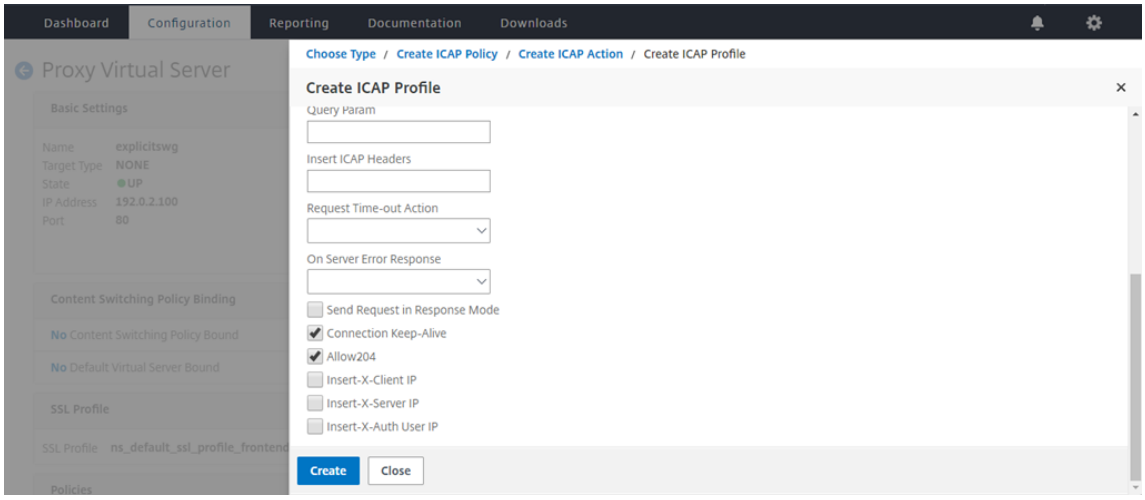



9. Escriba un nombre de perfil, URI. En **Modo**, seleccione **REQMOD**.

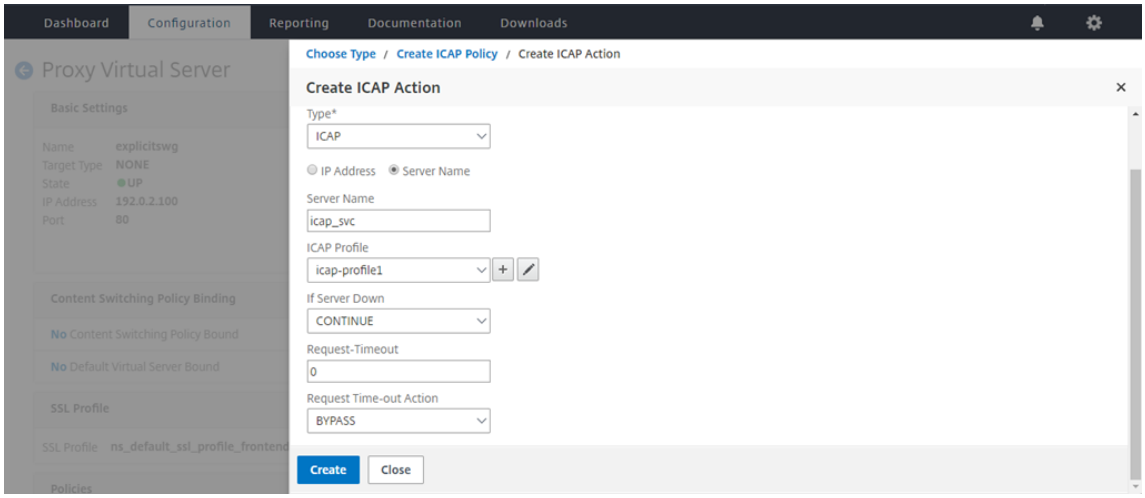
 




10. Haga clic en **Crear**.



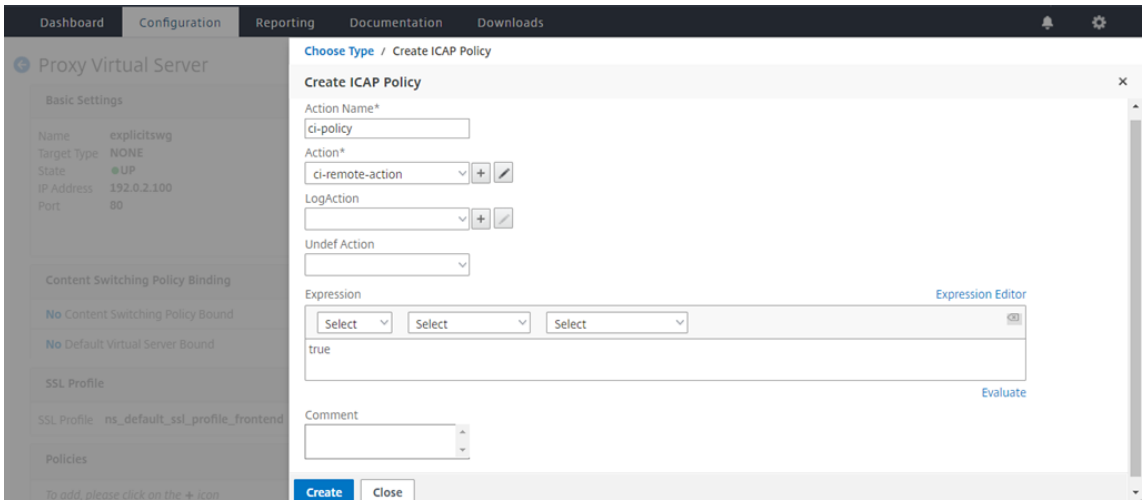

11. En la página **Crear acción ICAP**, haga clic en **Crear**.



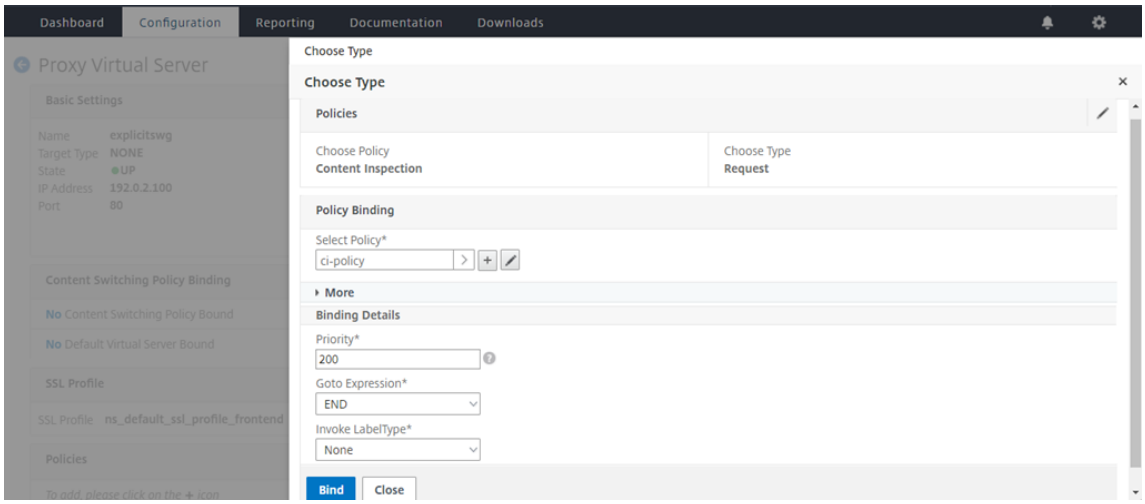

12. En la página **Crear directiva ICAP**, escriba true en el **Editor de expresiones**. A continuación,

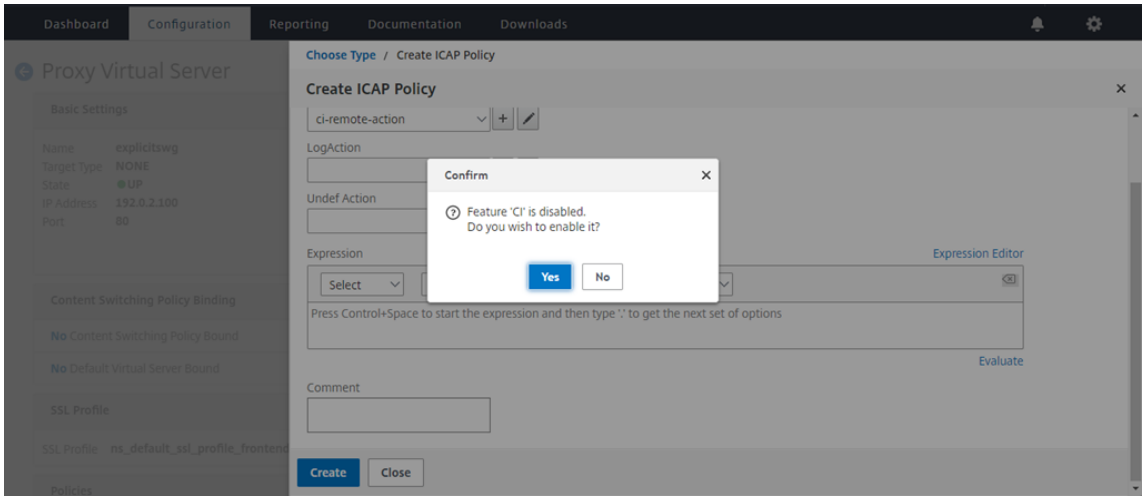
haga clic en **Crear**.




13. Haga clic en **Bind**.

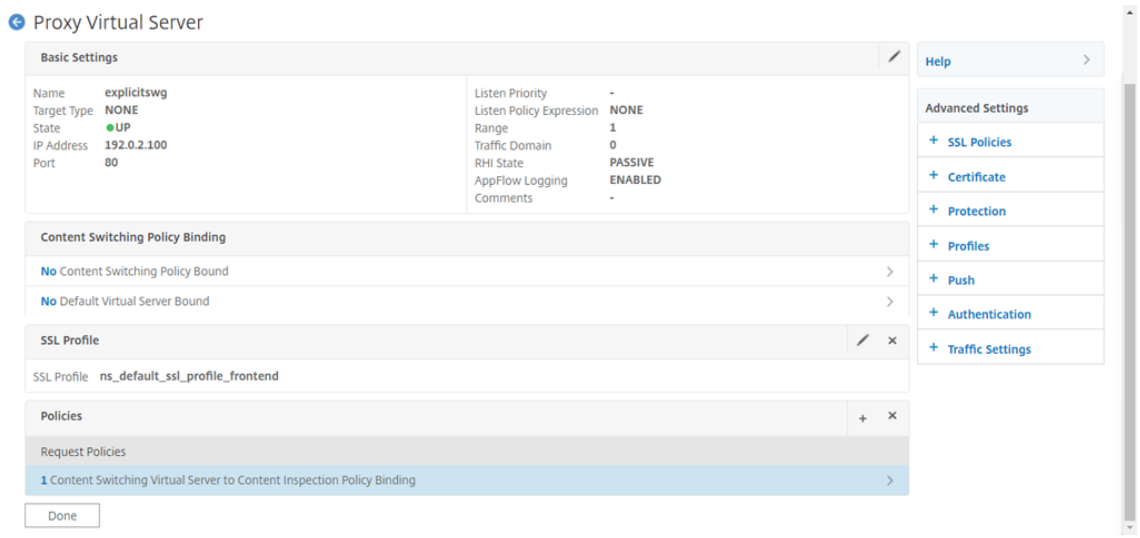



14. Si se le solicita que habilite la función de inspección de contenido, seleccione **Sí**.



15. Haga clic en **Done**.




## Ejemplo de transacciones ICAP entre el dispositivo Citrix SWG y el servidor ICAP en RESPMOD

**Solicitud del dispositivo Citrix SWG al servidor ICAP**:

```
RESPMOD icap://10.106.137.15:1344/resp ICAP/1.0

Host: 10.106.137.15

Connection: Keep-Alive

Encapsulated: res-hdr=0, res-body=282

HTTP/1.1 200 OK

Date: Fri, 01 Dec 2017 11:55:18 GMT

Server: Apache/2.2.21 (Fedora)

Last-Modified: Fri, 01 Dec 2017 11:16:16 GMT

ETag: "20169-45-55f457f42aee4"

Accept-Ranges: bytes

Content-Length: 69

Keep-Alive: timeout=15, max=100

Content-Type: text/plain; charset=UTF-8

X5O!P%@AP[4\PZX54(P^)7CC)7 }
```

```
 $EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
<!--NeedCopy-->
```

**Respuesta del servidor ICAP al dispositivo Citrix SWG**:

```
ICAP/1.0 200 OK

Connection: keep-alive

Date: Fri, 01 Dec, 2017 11:40:42 GMT

Encapsulated: res-hdr=0, res-body=224

Server: IWSVA 6.5-SP1_Build_Linux_1080 $Date: 04/09/2015 01:19:26 AM$

ISTag: "9.8-13.815.00-3.100.1027-1.0"

X-Virus-ID: Eicar_test_file

X-Infection-Found: Type=0; Resolution=2; Threat=Eicar_test_file;

HTTP/1.1 403 Forbidden

Date: Fri, 01 Dec, 2017 11:40:42 GMT

Cache-Control: no-cache

Content-Type: text/html; charset=UTF-8

Server: IWSVA 6.5-SP1_Build_Linux_1080 $Date: 04/09/2015 01:19:26 AM$

Content-Length: 5688

<html><head><META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset
   =UTF-8"/>

...

...

</body></html>
<!--NeedCopy-->
```

## Artículos de procedimientos

May 4, 2020

A continuación se presentan algunas instrucciones de configuración o casos de uso funcionales disponibles como artículos “Cómo”para ayudarle a administrar su implementación de SWG.

### Filtrado de URL



## Cómo crear una directiva de categorización de URL

April 27, 2021

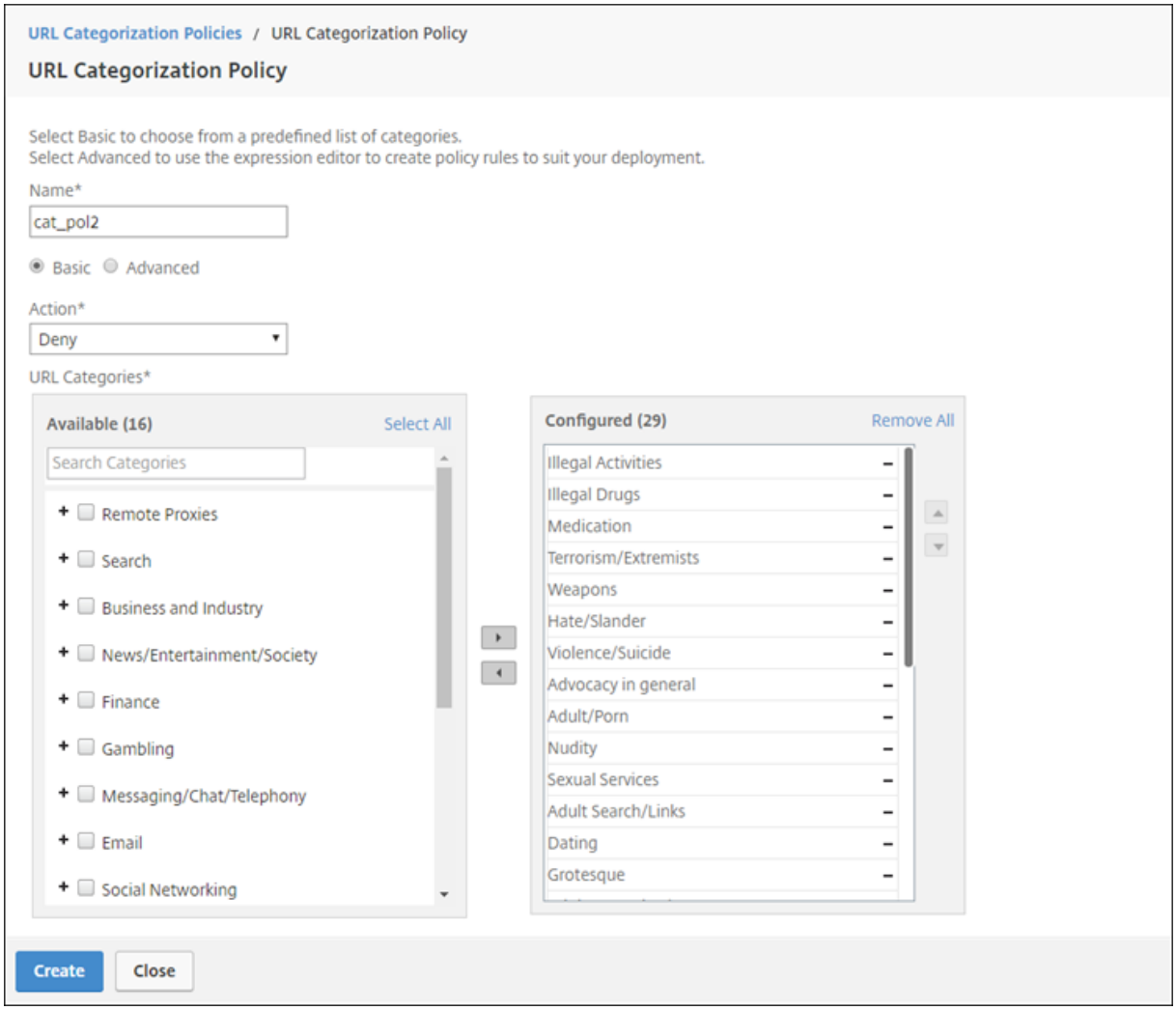
Como administrador de red, es posible que quiera bloquear categorías específicas de sitios web para el acceso de los usuarios. Para ello, cree una directiva de categorización de URL y vincule la directiva con una lista predefinida de categorías a las que desea restringir el acceso.

Por ejemplo, es posible que quiera restringir el acceso a todos los sitios web de redes sociales según las directivas de la organización. En tal caso, debe crear una directiva de categorización y vincularla a la lista predefinida de sitios web de categoría de redes sociales.

Para crear una directiva de categorización de URL mediante el método básico:

1. Inicie sesión en el dispositivo **Citrix SWG** y vaya a **Secured Web Gateway > Filtrado de URL > Categorización de URL**.
2. En el panel de detalles, haga clic en **Agregar** para acceder a la página **Directiva de categorización de URL** y especificar los siguientes parámetros.
    a) **Directiva de categorización de URL**. Nombre de la directiva de respondedor.
    b) **Básico**. Seleccione Configurar mediante una lista predefinida de categorías.
    c) **Acción**. Una acción para controlar el acceso a la URL.
    d) **Categorías de URL**. Lista predefinida de categorías para seleccionarla y agregarla a una lista configurada.
3. Haga clic en **Crear** y **cerrar**.



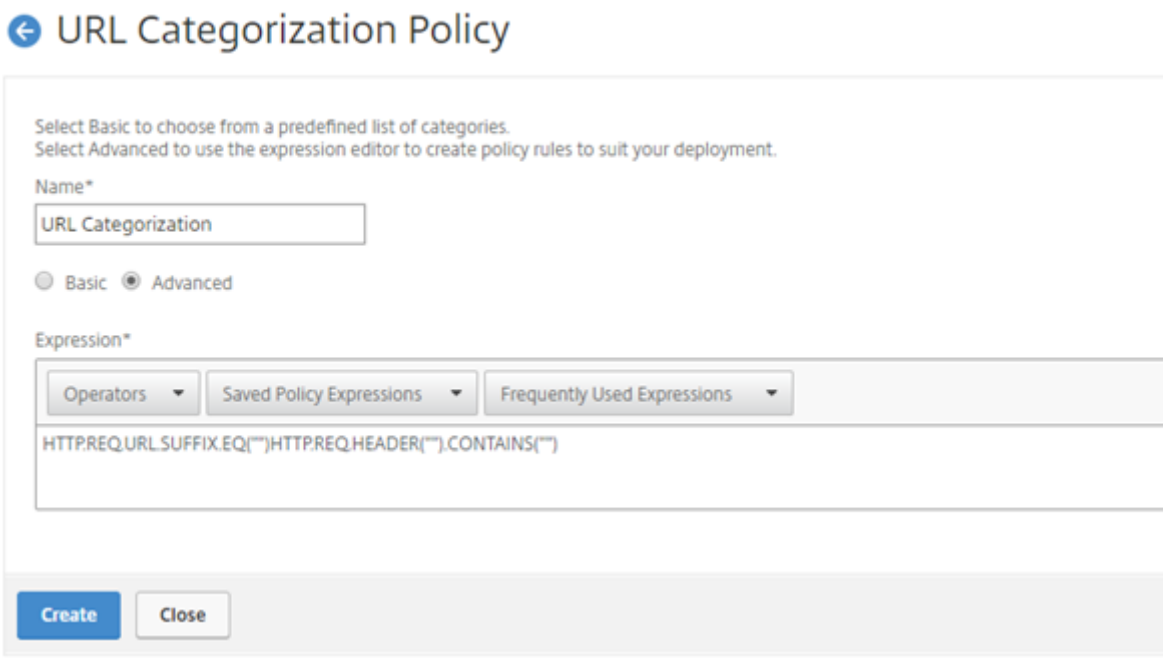

Para crear una directiva de categorización de URL mediante el método avanzado:

1. Para configurar una nueva directiva de categorización de URL mediante categorización avanzada.
2. Haga clic en **Agregar**.
3. En la página **Directiva de categorización de URL**, especifique los siguientes parámetros.

    a) **Directiva de categorización de URL**. Nombre de la directiva de respondedor.
    b) **Avanzado**. Configure la directiva mediante expresiones personalizadas.

4. Haga clic en **Crear** y **cerrar**.




## Cómo crear una directiva de lista de direcciones URL

April 27, 2021

Como administrador de red, es posible que quiera bloquear categorías específicas de sitios web para el acceso de los usuarios. Para ello, cree una directiva de lista de direcciones URL y vincule la directiva con un conjunto de direcciones URL importado en el dispositivo como archivo de texto. El conjunto de direcciones URL es una colección de sitios web que prefiere filtrar.

Por ejemplo, es posible que quiera restringir el acceso a todos los sitios web de malware según las directivas de la organización. En tal situación, debe crear una directiva de lista de direcciones URL y vincularla a un conjunto de direcciones URL importado en el dispositivo.

Para configurar una directiva de lista de direcciones URL:

1. Inicie sesión en el dispositivo **Citrix SWG** y vaya a **Secured Web Gateway > Filtrado de URL > Listas de URL**.
2. En el panel de detalles, haga clic en **Agregar.**
3. En la página **Directiva de lista de direcciones URL**, especifique el nombre de la directiva.
4. Seleccione una opción para importar un conjunto de direcciones URL o crear un conjunto de patrones y, a continuación, realice uno de los procedimientos que siguen el último paso de este procedimiento.
5. Seleccione una acción de respuesta en la lista desplegable.

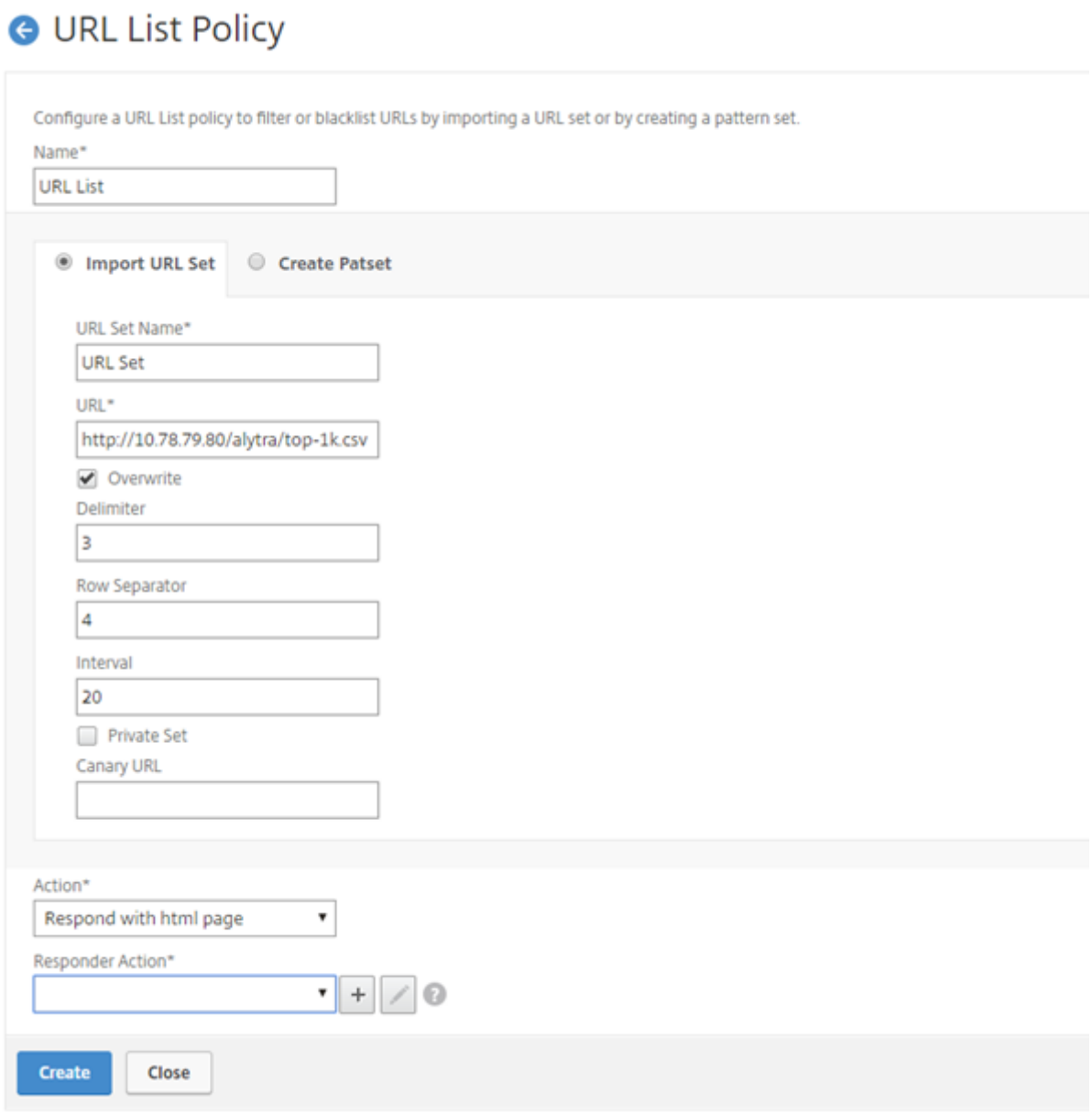
6. Haga clic en **Crear** y **cerrar**.

Para importar un conjunto de URL personalizado o un conjunto de URL de terceros:

1. En la página de separador **Directiva de lista de direcciones** URL, active la casilla de verificación **Importar conjunto de direcciones URL** y especifique los siguientes parámetros de conjunto de direcciones URL.

    a) **Nombre del conjunto de direcciones URL**: Nombre del conjunto de direcciones URL.
    b) **URL**: Dirección web de la ubicación en la que se accede al conjunto de direcciones URL.
    c) **Sobrescribir**: Sobrescribe el conjunto de direcciones URL importadas anteriormente.
    d) **Delimitador**: Secuencia de caracteres que delimita un registro de archivo CSV.
    e) **Separador de filas**: Separador de filas utilizado en el archivo CSV.
    f) **Intervalo**: Intervalo en segundos, redondeado a los 15 minutos más próximos, en los que se actualiza el conjunto de direcciones URL.
    g) **Conjunto privado**: Opción para impedir la exportación del conjunto de direcciones URL.
    h) **Canary URL**: URL interna para comprobar si el contenido del conjunto de URL debe mantenerse confidencial. La longitud máxima de la URL es de 2047 caracteres. Para obtener más información acerca de la URL Canary, consulte la sección Configuración de un conjunto de direcciones URL privadas.



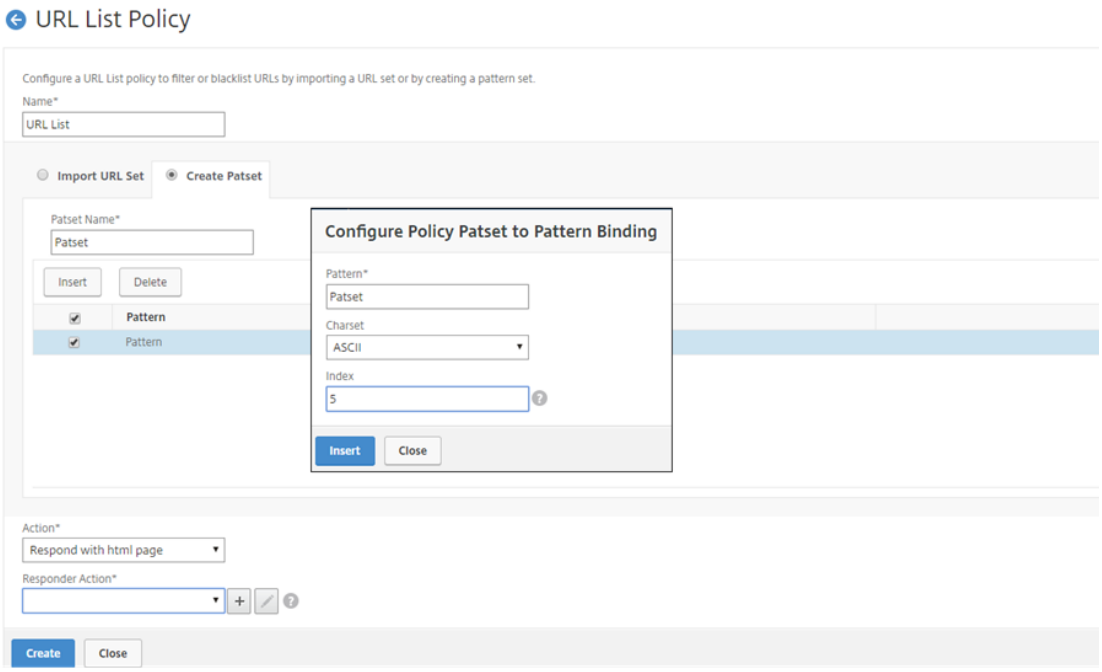

Para crear un conjunto de patrones:

1. En la página de separador **Crear patrón**, introduzca un nombre para el conjunto de patrones.
2. Haga clic en **Insertar** para crear un patrón.
3. En la página **Configure Policy Patset to Patset to Pattern Binding**, establezca los siguientes parámetros.

    a) **Patrón**—Cadena de caracteres que constituye un patrón
    b) **Juego de caracteres**: Tipo de juego de caracteres: Formato ASCII o UTF_8
    c) **Índice**: Valor de índice asignado por el usuario, desde 1 hasta 4294967290

4. Haga clic en **Insertar** para agregar el conjunto de patrones y, a continuación, en **Cerrar**.




## Cómo incluir en la lista blanca una URL excepcional

April 27, 2021

Cuando utiliza un filtro de URL para poner en la lista negra una categoría de sitios web, es posible que tenga que incluir en la lista blanca o permitir un sitio web específico como excepción. Por ejemplo, si prefiere incluir en la lista negra sitios web de juegos pero prefiere incluir únicamente en la lista blanca www.supersports.com, debe crear un conjunto de parches con una directiva de lista de direcciones URL y, a continuación, enlazar la directiva al servidor proxy con una mayor prioridad que otras directivas vinculadas.

### Para crear un conjunto de patrones mediante el asistente de Citrix SWG

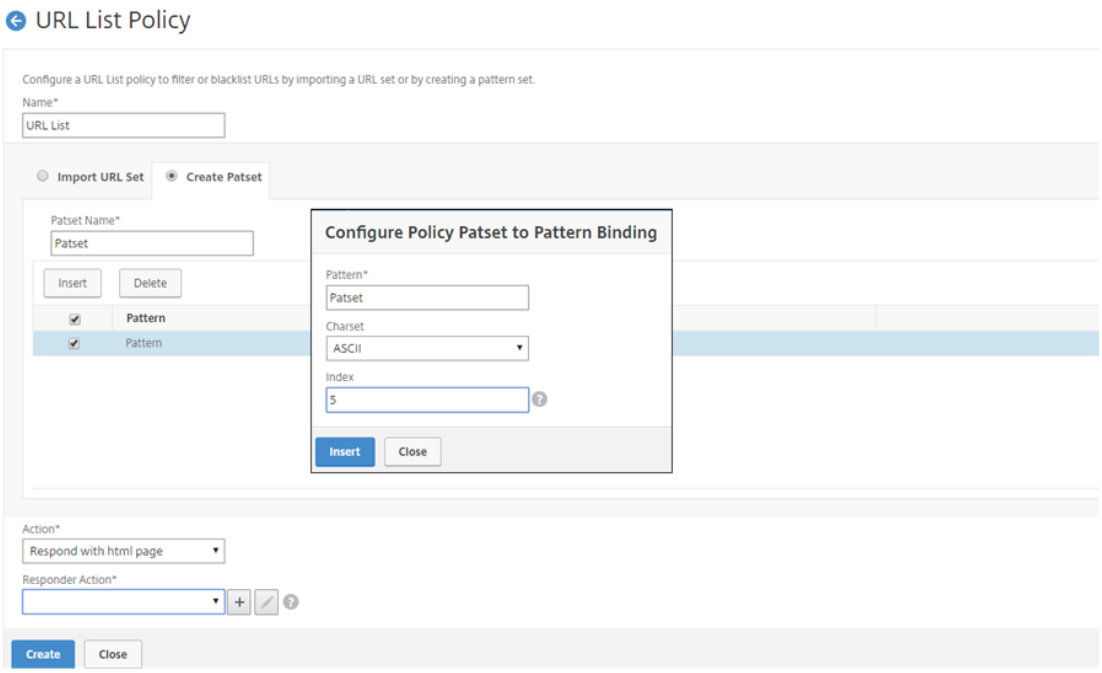
1. Inicie sesión en el dispositivo **Citrix SWG** y vaya a **Secured Web Gateway > Filtrado de URL > Listas de URL**.
2. En el panel de detalles, haga clic en **Agregar.**
3. En la página **Directiva de lista de direcciones URL**, especifique el nombre de la directiva.
4. Seleccione una opción para importar un conjunto de direcciones URL o crear un conjunto de patrones.
5. En la página de separador **Crear patrón**, introduzca un nombre para el conjunto de patrones.
6. Haga clic en **Insertar** para crear un patrón.

7. En la página **Configure Policy Patset to Patset to Pattern Binding**, establezca los siguientes parámetros.

    a) **Patrón**: Cadena de caracteres que constituye un patrón.
    b) **Charset**: Eltipo de conjunto de caracteres define como formato ASCII o UTF_8.
    c) **Índice**: Valor de índice asignado por el usuario, desde 1 hasta 4294967290

8. Haga clic en **Insertar** para agregar el conjunto de patrones y haga clic en **Cerrar**.




Para establecer la prioridad de la expresión de directiva mediante la GUI de Citrix SWG:

1. Inicie sesión en el dispositivo **Citrix SWG** y vaya a **Secure Web Gateway > Proxy Virtual Servers**.
2. En la página de detalles, seleccione un servidor y haga clic en **Modificar**.
3. En la página **Servidores virtuales proxy**, vaya a la sección **Directivas** y haga clic en el icono del lápiz para modificar los detalles.
4. Seleccione la directiva de conjunto de parches que ha creado y, en la página **Enlace de directivas**, especifique el valor de prioridad inferior a otras directivas enlazadas.
5. Haga clic en **Vincular** y **Listo**.

## Cómo bloquear el sitio web de la categoría de adultos

April 27, 2021

Como cliente de empresa, es posible que desee bloquear sitios web pertenecientes al grupo de categoría Adulto. Esto se hace configurando una directiva de respuesta que selecciona las solicitudes pertenecientes a una categoría adulta y bloquea el acceso a dichas direcciones URL de la lista negra.

### Configurar categorización de URL para bloquear sitios web pertenecientes a la categoría de adultos

Para configurar una directiva y bloquear sitios web adultos mediante la CLI:

En el símbolo del sistema, escriba el siguiente comando:

```
1 \*\*add responder policy\*\* <name> <rule> <respondwithhtml> [<
     undefAction>] [-comment <string>] [-logAction <string>] [-
     appflowAction <string>]
2 <!--NeedCopy-->
```

**Ejemplo**:

```
1     add responder policy p1  ‘ HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).
        URL_CATEGORIZE(0,0). GROUP.EQ("Adult") ’
2 <!--NeedCopy-->
```

#### Configurar la categorización de URL para bloquear sitios web para adultos mediante el asistente Citrix SWG

Para bloquear categorías de adultos mediante el asistente Citrix SWG

1. Inicie sesión en el dispositivo **Citrix SWG** y desplácese hasta **Secure Web Gateway**.
2. En el panel de detalles, haga clic en **Asistente para puerta de enlace web segura**.
3. En la página **Configuración de Secure Web Gateway**, especifique la configuración del servidor proxy SWG.
4. Haga clic en **Continuar** para especificar otros parámetros, como la intercepción de SSL y la administración de identificación.
5. Haga clic en **Continuar** para acceder a la sección **Filtrado de URL**.
6. Active la casilla de verificación **Habilitar categorización de URL** para habilitar la función.
7. Haga clic en Vincular para acceder al control deslizante **Directivas de categorización de URL**.
8. Seleccione una directiva y haga clic en **Insertar** para enlazar la directiva.
9. Seleccione la directiva de respuesta para bloquear sitios web para adultos.
10. Para agregar una directiva nueva, haga clic en **Agregar** para acceder a la página **Directiva de categorización de direcciones URL** y realice una de las acciones siguientes.

    a) Para configurar una directiva mediante la categorización básica, haga clic en **Agregar**.

i. En la página **Directiva de categorización de URL**, especifique los siguientes parámetros.

A. Directiva de categorización de URL. Nombre de la directiva de respondedor.
B. Básico. Configure la directiva mediante el método de configuración básico.
C. Acción. Una acción para controlar el acceso a la URL.
D. Categorías de URL. Seleccione Categoría Adulto en la lista predefinida.

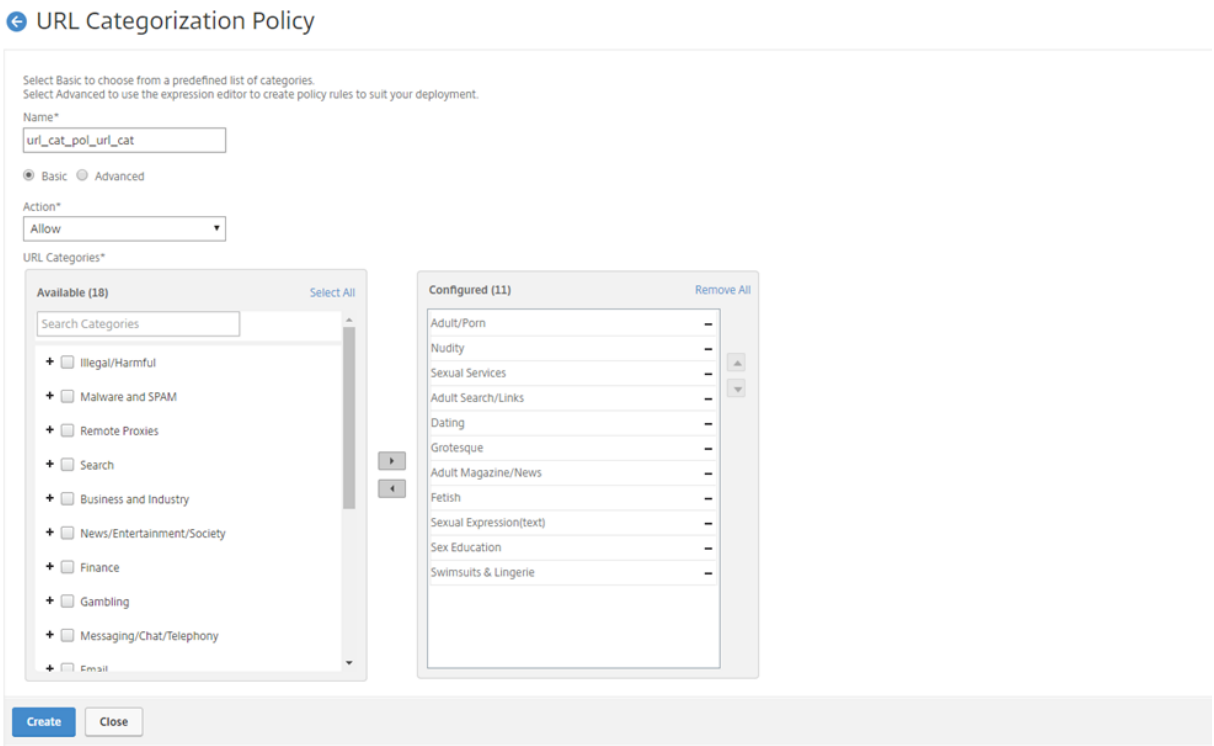
11. Haga clic en **Crear** y **cerrar**.

a) Para configurar una nueva directiva de categorización de URL mediante categorización avanzada, haga clic en **Agregar**.

i. En la página **Directiva de categorización de URL**, especifique los siguientes parámetros.

A. **Directiva de categorización de URL**. Nombre de la directiva de respondedor.
B. **Avanzado**. Configure la directiva para bloquear las solicitudes del grupo de categoría Adulto.

12. Haga clic en **Crear** y **cerrar**.



## System

April 27, 2021

Las funciones del sistema proporcionan información conceptual e instrucciones de configuración que puede consultar al configurar un dispositivo Citrix SWG.

En la siguiente tabla se describen las funciones de un dispositivo Citrix SWG.

Operaciones básicas: Detalles de configuración y operación a nivel del sistema de un dispositivo Citrix ADC.

Autenticación y autorización: Detalles de configuración en la creación de usuarios, grupos de usuarios y directivas de comandos, y la asignación de directivas a cuentas de usuario

Configuración de TCP: Detalles de configuración del perfil TCP y las capacidades TCP en un dispositivo Citrix ADC.

Configuración HTTP: Detalles de configuración del perfil HTTP y las capacidades HTTP en un dispositivo Citrix ADC.

SNMP: Un protocolo de administración de red que supervisa el dispositivo Citrix ADC y responde rápidamente a los problemas del dispositivo.

Registro de auditoría: Un protocolo estándar para registrar los estados del dispositivo Citrix ADC y la información de estado recopilada por varios módulos en el kernel y en los demonios de nivel de usuario. Para el registro de auditoría, puede utilizar el protocolo SYSLOG o NSLOG o ambos.

Call Home: Un sistema de notificación para supervisar y resolver condiciones de error críticas en un dispositivo Citrix SWG.

Herramienta de generación de informes: Interfaz web a la que se accede desde un dispositivo Citrix SWG para ver los informes de rendimiento del sistema como gráficos.

## Redes

April 27, 2021

En los temas siguientes se proporciona información de referencia conceptual e instrucciones de configuración para las características de red que puede desear configurar en un dispositivo Citrix SWG.

- Direcciones IP Direcciones IP propiedad de Citrix ADC y sus detalles de configuración.
- Interfaces Acceso y configuración del dispositivo Citrix SWG.

- Listas de control de acceso (ACL) Diferentes tipos de listas de control de acceso utilizadas en dispositivos Citrix ADC, con detalles de configuración.
- Enrutamiento IP Los diferentes protocolos de enrutamiento IP utilizados en un dispositivo Citrix ADC.
- Protocolo de Internet versión 6 (IPv6) Compatibilidad con el protocolo de Internet en un dispositivo Citrix ADC y cómo funciona el dispositivo como nodo IPv6.
- VXLAN Compatibilidad con Virtual Extensible Local Area Network (VXLAN) en la infraestructura de red Citrix ADC y cómo VXLAN superpone las redes de Capa 2 en una infraestructura de Capa 3 encapsulando tramas de Capa 2 en UDP paquetes.

## AppExpert

April 27, 2021

En los temas siguientes se proporciona información conceptual e instrucciones de configuración para las funciones de AppExpert que puede que desee configurar en un dispositivo Citrix SWG.

Conjuntos de patrones y conjuntos de datos: Expresiones de directiva para realizar operaciones de coincidencia de cadenas en un gran conjunto de patrones de cadenas.

Dependiendo del tipo de patrón que desee hacer coincidir, puede utilizar una de las siguientes características para implementar la coincidencia de patrones:

- Un conjunto de patrones es una matriz de patrones indexados utilizados para la coincidencia de cadenas durante la evaluación de directivas de sintaxis predeterminada. Ejemplo de un conjunto de patrones: Tipos de imagen {svg, bmp, png, gif, tiff, jpg}.
- Un conjunto de datos es una forma especializada de conjunto de patrones. Es una matriz de patrones de tipos número (entero), dirección IPv4 o dirección IPv6.

Variables: Objetos que almacenan información en forma de tokens y son utilizados por acciones de directiva de respuesta.

Las variables son de dos tipos como se indica a continuación:

- Variables Singleton. Puede tener un solo valor de uno de los siguientes tipos: Ulong y text (tamaño máximo). El tipo ulong es un entero de 64 bits sin signo, el tipo de texto es una secuencia de bytes y el tamaño máximo es el número máximo de bytes en la secuencia.
- Asignar variables. Los mapas contienen valores asociados con las claves: Cada par clave-valor se denomina entrada de mapa. La clave de cada entrada es única dentro del mapa.

Directivas y expresiones: Las directivas controlan el tráfico web que entra en un dispositivo Citrix SWG. Una directiva utiliza una expresión lógica, también denominada regla, para evaluar solicitudes, respuestas u otros datos, y aplica una o varias acciones determinadas por el resultado de la evaluación. Como alternativa, una directiva puede aplicar un perfil, que define una acción compleja.

Responder: Directiva que envía respuestas basadas en quién envía la solicitud, de dónde se envía, y otros criterios con implicaciones de seguridad y gestión del sistema. La función es simple y rápida de usar. Al evitar la invocación de funciones más complejas, reduce los ciclos de CPU y el tiempo dedicado al manejo de solicitudes que no requieren procesamiento complejo. Para el manejo de datos confidenciales, como información financiera, si desea asegurarse de que el cliente utiliza una conexión segura para navegar por un sitio web, puede redirigir la solicitud a una conexión segura mediante el protocolo HTTPS.

Reescribir: Directiva que reescribe la información en las solicitudes y respuestas manejadas por el dispositivo Citrix SWG. La reescritura puede ayudar a proporcionar acceso al contenido solicitado sin exponer detalles innecesarios sobre la configuración real del sitio web.

Conjuntos de URL: Expresiones de directiva avanzada para poner en lista negra un millón de entradas de URL. Para evitar el acceso a sitios web restringidos, un dispositivo Citrix SWG utiliza un algoritmo de coincidencia de URL especializado. El algoritmo utiliza un conjunto de direcciones URL que puede contener una lista de direcciones URL de hasta un millón (1.000.000) de entradas en la lista negra. Cada entrada puede incluir metadatos que definen categorías de URL y grupos de categorías como patrones indexados. El dispositivo también puede descargar periódicamente direcciones URL de conjuntos de URL altamente confidenciales administrados por agencias de aplicación de Internet (con sitios web gubernamentales) u organizaciones independientes de Internet.

## SSL

April 27, 2021

En los siguientes temas se proporciona información de referencia conceptual e instrucciones de configuración para las características SSL que puede desear configurar en un dispositivo Citrix SWG.

- Certificados
- Listas de revocación de certificados (CRL)
- Directivas SSL
- Respondedor OCSP

# Preguntas frecuentes

April 27, 2021

P: ¿Qué plataformas de hardware son compatibles con Citrix Secure Web Gateway (SWG)?

**A.** Citrix SWG está disponible en las siguientes plataformas de hardware:

- Citrix SWG MPX 14020/14030/14040
- Citrix SWG MPX 14020-40G/14040-40G
- Citrix SWG MPX 14060-40S/14080-40S/14100-40S
- Citrix SWG MPX 5901/5905/5910
- Citrix SWG MPX/SDX 8905/8910/8920/8930
- Todas las plataformas SDX basadas en Cavium N2 y N3

P: ¿Cuáles son los dos modos de captura que puedo establecer al crear un proxy en el dispositivo SWG?

**A.** La solución SWG admite modos proxy explícitos y transparentes. En modo proxy explícito, los clientes deben especificar una dirección IP y un puerto en sus navegadores, a menos que la organización inserte la configuración en el dispositivo del cliente. Esta dirección es la dirección IP de un servidor proxy configurado en el dispositivo SWG. Proxy transparente, como su nombre lo indica, es transparente para el cliente. El dispositivo SWG está configurado en una implementación en línea y el dispositivo acepta de forma transparente todo el tráfico HTTP y HTTPS.

P: ¿Citrix SWG tiene un asistente de configuración?

**A.** Sí. El asistente se encuentra en el nodo SWG de la utilidad de configuración.

P: ¿Qué funciones de Citrix ADC se utilizan al configurar Citrix SWG?

**A.** Respondedor, AAA-TM, conmutación de contenido, SSL, proxy de reenvío, intercepción SSL y filtrado de URL.

P: ¿Qué métodos de autenticación son compatibles con Citrix SWG?

**A.** En el modo proxy explícito, se admiten los métodos de autenticación LDAP, RADIUS, TACACS+ y NEGOTIATE. En modo transparente, solo se admite la autenticación LDAP.

P: ¿Es necesario instalar el certificado de CA en el dispositivo cliente?

**A.** Sí. El dispositivo Citrix SWG emula el certificado del servidor de origen. Este certificado de servidor debe estar firmado por un certificado de CA de confianza, que debe instalarse en los dispositivos de los clientes para que el cliente pueda confiar en el certificado de servidor regenerado.

P: ¿Puedo usar una licencia de Citrix ADC Platform en la plataforma Citrix SWG?

**A.** No. La plataforma Citrix SWG requiere su propia licencia de plataforma.

P: ¿Se admite HA para una implementación de Citrix Secure Web Gateway?

**A.** Sí.

P: ¿Qué archivo contiene los registros de Citrix SWG?

**A.** El archivo ns.log registra la información de Citrix SWG. Debe habilitar el registro mediante la CLI o la GUI. En el símbolo del sistema, escriba: **set syslogparams -ssli Enabled**.

En la GUI, vaya a **Sistema** > **Auditoría**. En **Configuración**, haga clic en **Cambiar configuración de Syslog de auditoría**. Seleccione **Intercepción SSL**.

P: ¿Qué comandos nsconmsg puedo usar para solucionar problemas?

**A.** Puede utilizar uno de los siguientes comandos o ambos:

```
1 nsconmsg -d current -g ssli
2 <!--NeedCopy-->
```

```
1 nsconmsg -d current -g err
2 <!--NeedCopy-->
```

P: Si el paquete de certificados está integrado, ¿cómo obtengo actualizaciones?

**A.** El último paquete se incluye en la compilación. Para obtener actualizaciones, póngase en contacto con el Soporte técnico de Citrix.

P: ¿Se pueden capturar datos en Citrix ADM desde Citrix SWG?

**A.** Sí. Debe habilitar **Analytics** en el asistente Secure Web Gateway.

**Importante**: Asegúrese de que está utilizando la misma compilación 12.0 para MAS y SWG.

P: ¿Qué es el servicio de filtrado de URL?

**A.** El filtrado de URL es un filtro de contenido web que controla el acceso a una lista de sitios web y páginas web restringidos. El filtro restringe el acceso de los usuarios a contenido inapropiado en Internet según la categoría URL, los grupos de categorías y la puntuación de reputación. Un administrador de red puede supervisar el tráfico web y bloquear el acceso de los usuarios a sitios web de alto riesgo. Puede implementar la función mediante la categorización de URL o la función Lista de URL basada en la aplicación de directivas. Para obtener más información, consulte el tema Filtrado de URL.

P: ¿Cómo encaja el filtrado de URL en Citrix SWG?

**A**. El filtrado de URL aprovecha el dispositivo Citrix SWG para controlar el acceso a sitios web específicos. El dispositivo SWG en el borde de la red actúa como proxy para interceptar el tráfico web y realizar acciones como autenticación, inspección, almacenamiento en caché y redirección. A continuación, el filtro controla el acceso a sitios web mediante la función Categorización de URL o Lista de URL con aplicación de directivas.

P: ¿Con qué frecuencia se actualiza la base de datos de categorización de URL?

**A.** Si utiliza la función de categorización de URL para controlar el acceso a sitios web restringidos, debe actualizar periódicamente la base de datos de categorización con los datos más recientes del servicio de proveedor basado en la nube. Para actualizar la base de datos, la interfaz gráfica de usuario de Citrix SWG le permite configurar los parámetros de filtrado de URL, como Horas entre actualizaciones de base de datos"o "Hora del día para actualizar la base de datos.

P: ¿Qué casos de uso son los más adecuados para el servicio de filtrado de URL en la actualidad?

**A**. A continuación se presentan algunos de los casos de uso dirigidos a clientes empresariales:

- Filtrado de URL por puntuación de reputación de URL
- Control del uso de Internet bajo Cumplimiento corporativo para empresas
- Filtrado de URL mediante la lista de direcciones URL personalizadas

P: ¿Existe un límite de memoria para el almacenamiento en caché en el servicio de categorización de URL?

**A.** Sí. El límite de memoria para el almacenamiento en caché se establece como 10 GB y solo puede configurarlo a través de la interfaz CLI.

P: ¿Qué devuelve la base de datos de categorización de URL si ninguna categoría coincide con la solicitud entrante?

**A.** Si la solicitud entrante no coincide con una categoría o si la dirección URL está mal formada, el dispositivo marca la dirección URL como "Sin categoría"y envía la solicitud al servicio basado en la nube mantenido por el proveedor de categorización. El dispositivo continúa supervisando los comentarios de las consultas en la nube y actualiza la caché para que las futuras solicitudes puedan beneficiarse de la búsqueda en la nube.

P: ¿Qué es una puntuación de reputación de URL y cómo se controla el acceso a sitios web maliciosos en función de la puntuación de reputación?

**A.** Una puntuación de reputación de URL es una calificación que Citrix SWG asigna a un sitio web. El valor puede variar de 1 a 4, donde 4 es un sitio web malicioso y 1 es un sitio web limpio. Si un administrador de red supervisa a un usuario que accede a sitios web de alto riesgo, el acceso a dichos sitios se controla en función de la puntuación de reputación de URL y el nivel de seguridad que haya configurado en el dispositivo Citrix SWG. Para obtener más información, consulte Puntuación de reputación de URL.

P: Si filtra sitios web mediante un conjunto de direcciones URL pero filtra incorrectamente un sitio web específico, ¿cuál es el proceso para habilitar sitios web excepcionales?

**A**. El filtrado de URL utiliza una directiva de respuesta para controlar el acceso a sitios Web. Para incluir en la lista blanca una URL específica como excepción, en el asistente SWG, cree una directiva de conjunto de parches y agregue la URL excepcional con la acción "permitir". Una vez creada la directiva, salga del asistente y siga estos pasos:

Para cambiar la prioridad de una expresión de política mediante la GUI de Citrix SWG:

1. Inicie sesión en el dispositivo **Citrix SWG** y vaya a **Secure Web Gateway > Proxy Virtual Servers**.
2. En la página de detalles, seleccione un servidor y haga clic en **Modificar**.
3. En la página **Servidores virtuales proxy**, vaya a la sección **Directivas** y haga clic en el icono del lápiz para modificar los detalles.
4. Seleccione la directiva de conjunto de parches y, en la página **Enlace de directivas**, especifique el valor de prioridad inferior a otras directivas enlazadas.
5. Haga clic en **Vincular** y **Listo**.

P: ¿Cuáles son las ventajas clave de utilizar la función de filtrado de URL de Citrix SWG?

**A.** La función de filtrado de URL es fácil de implementar, configurar y usar. Proporciona los siguientes beneficios y permite a los clientes empresariales:

- Supervisar el tráfico web y la transacción del usuario
- Filtra el malware y las amenazas de seguridad transmitidas por Internet.
- Controlar el acceso no autorizado a sitios web maliciosos.
- Implemente directivas de seguridad corporativas para controlar el acceso a datos restringidos.

P: Si utiliza una función Lista de direcciones URL para filtrar sitios web, ¿cómo modificar una directiva de lista de direcciones URL?

**A.** Puede modificar una directiva de lista de direcciones URL mediante el asistente de Citrix SWG sobrescribiendo o eliminando la lista importada enlazada a la directiva de respuesta.

P: ¿Qué contienen los metadatos asociados a una URL?

**A.** Cada URL de la base de datos de categorización tiene asociados metadatos. Los metadatos contienen una categoría de URL, un grupo de categorías y una información de puntuación de reputación. Por ejemplo, si la URL es un portal de compras, los metadatos serán Compras, Compras y venta minorista y 1 respectivamente.

Utilice las siguientes expresiones para obtener estos valores para la URL entrante. Las expresiones se dan a continuación:

```
URL_CATEGORIZE(0,0).CATEGORY
<!--NeedCopy-->
```

```
URL_CATEGORIZE(0,0).GROUP
<!--NeedCopy-->
```

```
URL_CATEGORIZE(0,0).REPUTATION
<!--NeedCopy-->
```

P: ¿Qué tipo de licencia y suscripción necesita para la función de categorización de URL?

**A.** La función de categorización de URL requiere un servicio de suscripción de URL Threat Intelligence (disponible durante un año o tres años) con Citrix SWG edition.

P: ¿Cuáles son las formas en que puedo configurar el filtrado de URL?

**A.** Hay dos formas de configurar el filtrado de URL. Puede hacerlo a través de la interfaz de comandos de Citrix SWG o a través del asistente de Citrix SWG. Citrix recomienda utilizar el asistente para configurar directivas de filtrado.

P: ¿Cuáles son los tipos de categorías de URL que puede bloquear?

**A.** La base de datos de categorización de URL contiene millones de direcciones URL con metadatos. El administrador puede configurar una directiva de respuesta para decidir qué categorías de URL se pueden bloquear y qué categorías de URL se pueden permitir para el acceso de los usuarios. Para obtener información sobre la asignación de categorías de URL, consulte la página Categorías de asignación.

P: ¿Qué debemos hacer si no podemos acceder a los servidores de Origin que utilizan WebSocket, como whatsapp?

Debe habilitar WebSocket en el perfil HTTP predeterminado.

En la CLI, escriba:

```
1 > set httpprofile nshttp_default_profile -webSocket ENABLED
2 <!--NeedCopy-->
```

¿Qué es ICAP?

ICAP significa Protocolo de Adaptación de Contenido de Internet.

¿Qué versión de Citrix SWG admite ICAP?

ICAP es compatible con Citrix SWG versión 12.0 compilación 57.x y versiones posteriores.

¿Cuáles son los dos modos ICAP compatibles con Citrix SWG?

Se admiten el modo de modificación de solicitud (`REQMOD`) y el modo de modificación de respuesta (`RESPMOD`).

¿Cuál es el puerto predeterminado para ICAP?

`1344`.