

Configuración de Proxy

Configuración de Proxy para Consultas

Anonymous · 27/08/2026

Configuración de Proxy para Consultas

Un **proxy** es un servidor intermediario que actúa como puente entre tu aplicación y los servicios externos. En el contexto de API Gateway, utilizamos proxies para distribuir las consultas, por ejemplo al SII (Servicio de Impuestos Internos), desde diferentes direcciones IP, evitando así posibles restricciones y limitaciones de uso.

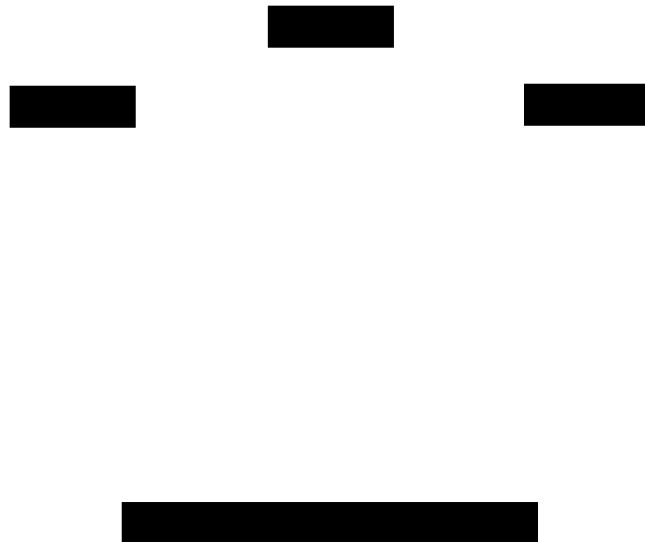
Importante

Cuando cada empresa gestiona sus consultas al SII a través de su propio proxy y dirección IP, se entiende que está haciendo un uso legítimo y responsable de nuestra API. Promovemos y respaldamos la **automatización de consultas tributarias como un derecho fundamental de las empresas** que buscan asegurar el cumplimiento de sus obligaciones fiscales de manera eficiente y transparente.

Riesgo al no utilizar un proxy

El SII puede implementar límites de uso basados en direcciones IP para controlar el acceso a sus servicios. Debido a que API Gateway es la plataforma líder en Chile que ofrece servicios web que el SII no proporciona directamente, debemos procesar un alto volumen de consultas, lo que puede provocar restricciones impuestas por el SII.

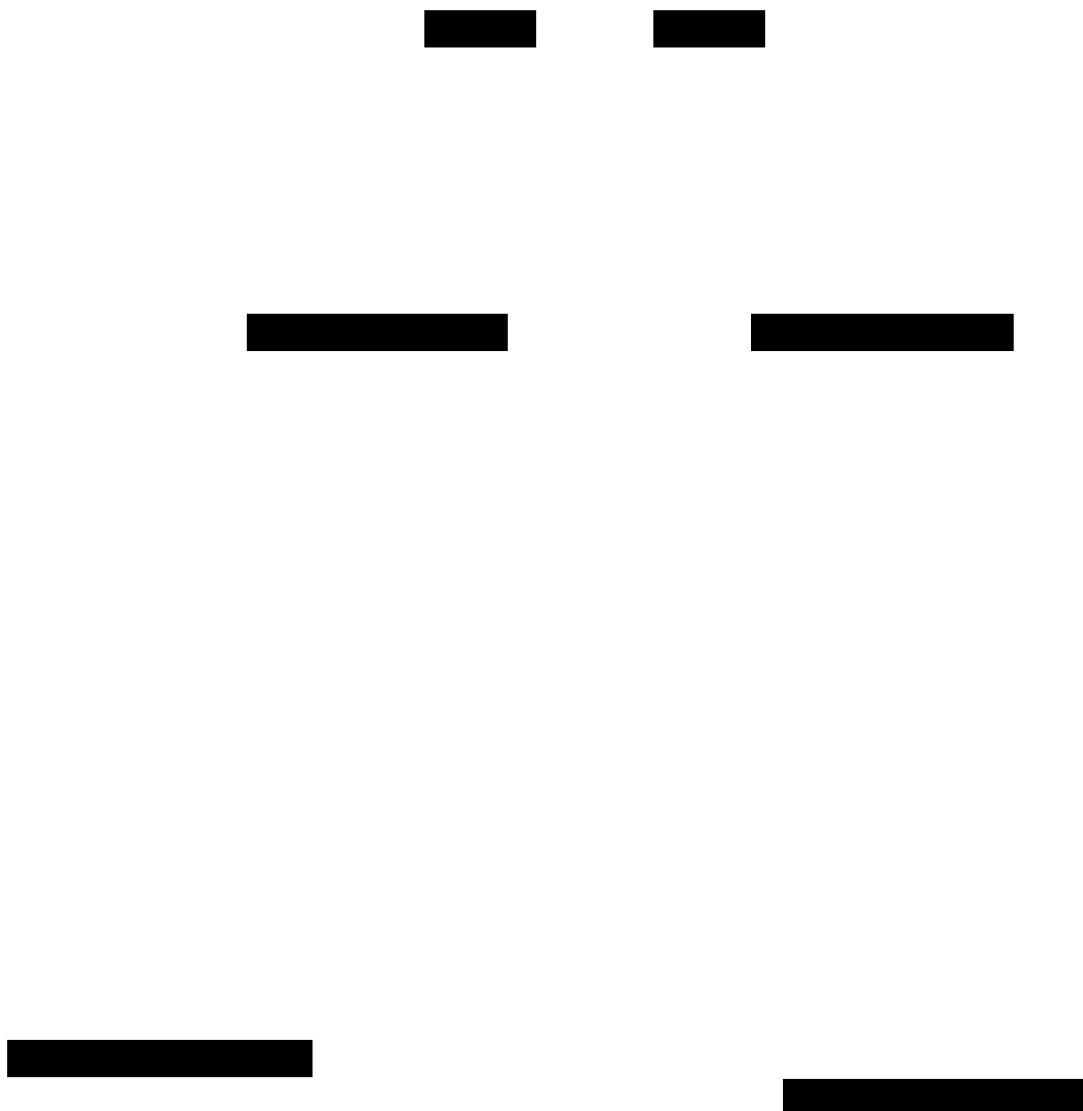
Cuando el SII restringe o limita las consultas desde una IP específica, el riesgo es que afecte a múltiples usuarios. Esto se muestra en el siguiente diagrama:



Funcionamiento del Proxy

Con el proxy, se busca mitigar este problema permitiendo que las consultas se realicen desde direcciones IP diferentes, una por cada empresa/RUT que realiza consultas al SII. Con esto, se distribuye la carga y se minimiza el impacto de las restricciones.

El proxy funciona como un intermediario en la comunicación entre aplicaciones, evitando que una sola dirección IP sea restringida y afecte a múltiples usuarios. Esto se muestra en el siguiente diagrama:



Beneficios del uso de proxy:

- **Aislamiento de restricciones:** Si una IP es limitada, solo afecta a los usuarios de ese proxy específico.
- **Mayor disponibilidad:** Si la IP principal está restringida, los proxies permiten continuar operando.
- **Distribución de carga:** Reduce la presión sobre una sola dirección IP.

Configuración del Proxy

El proxy debe estar ubicado en una red pública accesible desde API Gateway. En este tutorial utilizaremos **Squid**, un proxy HTTP/HTTPS robusto y ampliamente utilizado, pero puedes implementar cualquier solución compatible.

Opciones de despliegue:

- **Servidores propios:** Infraestructura on-premise.
- **Servicios en la nube:** Google Cloud Platform (tiene región en Chile), AWS, Azure, etc.
- **Proveedores locales:** Otros servicios con presencia en Chile.

1. Archivo Docker Compose

Utilizaremos Docker Compose para simplificar la implementación del proxy Squid. Crea un directorio para tu proyecto y dentro de este crea un archivo `docker-compose.yml` con la siguiente configuración:

```
services:
  squid:
    image: ubuntu/squid:latest
    container_name: squid
    restart: unless-stopped
    volumes:
      - "./squid.conf:/etc/squid/squid.conf:ro"
      - "./passwords:/etc/squid/passwords:ro"
    ports:
      - "3128:3128"
```

Nota importante

El puerto 3128 es el puerto estándar de Squid. Si necesitas usar un puerto diferente, asegúrate de modificarlo tanto en el `docker-compose.yml` como en el archivo de configuración `squid.conf`. Este puerto debe ser accesible desde Internet o al menos desde los servidores de API Gateway.

2. Configuración de Squid

Crea el archivo `squid.conf` en el mismo directorio de `docker-compose.yml` con la siguiente

configuración:

```
# Configuración de autenticación.
auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/passwords
auth_param basic realm Proxy

# Definir ACL para usuarios autenticados.
acl authenticated proxy_auth REQUIRED

# Definir ACL para dominios del SII (recomendado para seguridad).
acl sii_domains dstdomain .sii.cl

# AWS API Gateway (usado por eboleta)
acl eboleta_aws_api dstdomain .amazonaws.com

# Previred
acl previred_domains dstdomain .previred.com

# Permitir acceso solo a usuarios autenticados y solo a dominios del SII.
http_access allow authenticated sii_domains
http_access allow authenticated eboleta_aws_api
http_access allow authenticated previred_domains

# Denegar todas las demás solicitudes.
http_access deny all

# Escuchar en el puerto 3128.
http_port 3128
```

Nota de seguridad

La configuración anterior incluye una restricción que limita el uso del proxy únicamente a dominios del SII (.sii.cl), Previred (.previred.com) y eBoleta (.amazonaws.com). Esto es altamente recomendado para evitar el uso no autorizado del proxy para otros fines. Si necesitas acceder a otros dominios a través del proxy, puedes modificar o eliminar la línea `acl sii_domains dstdomain .sii.cl` y cambiar `http_access allow authenticated sii_domains` por `http_access allow authenticated`.

3. Creación de Credenciales

Genera el archivo de contraseñas usando el comando `htpasswd`:

```
htpasswd -c passwords <nombre_usuario> <contraseña>
```

Ejemplo:

```
htpasswd -c passwords admin mi_contraseña_segura
```

Recomendaciones de seguridad:

- Usa contraseñas fuertes (mínimo 12 caracteres).
- Combina mayúsculas, minúsculas, números y símbolos.
- Evita información personal en las credenciales.

4. Iniciar el Servicio

Ejecuta el siguiente comando para iniciar el proxy:

```
docker compose up -d
```

Verifica que el servicio esté funcionando correctamente:

```
docker compose ps
```

Habilitación en API Gateway

Una vez que tu proxy esté funcionando, necesitas configurarlo en API Gateway. Acá hay 2 formas de hacerlo dependiendo de qué versión de API Gateway estés usando:

- **Versión V2:** Acceder a la [configuración de la conexión](#). Recuerda que en la versión 2 la configuración del proxy se debe realizar por cada conexión que tengas activa.
- **Versión Legacy (V1):** Acceder a la [configuración de tu perfil](#).

Independientemente de la versión de API Gateway que estés usando, debes configurar el proxy indicando su URL, la cual tendrá el siguiente formato:

```
http://<nombre_usuario>:<contraseña>@<ip_proxy>:3128
```

Donde los parámetros son:

- `<nombre_usuario>`: El usuario que creaste con `htpasswd`.
- `<contraseña>`: La contraseña correspondiente.
- `<ip_proxy>`: La dirección IP pública de tu servidor proxy.
- `3128`: El puerto de Squid (cambia si usaste uno diferente).

Realización de pruebas

Después de guardar la configuración, API Gateway comenzará a utilizar tu proxy para todas las consultas. Esto significa que las consultas se realizarán desde la IP de tu proxy en lugar de la IP

principal de API Gateway.

Para verificar que la configuración es correcta, realiza una consulta a la API y revisa la cabecera `X-Stats-HttpClientProxy` en la respuesta. Si su valor es `1`, significa que el proxy está siendo utilizado. Si el valor es `0`, el proxy no se está usando; en ese caso, revisa la sección de problemas comunes a continuación.

Problemas Comunes

1. Error de autenticación

- Verifica que las credenciales en API Gateway coincidan con las del archivo `passwords`.
- Confirma que el archivo `passwords` esté correctamente montado en el contenedor.

2. Proxy no accesible

- Verifica que el puerto 3128 esté abierto en el firewall.
- Confirma que la IP del proxy sea accesible desde Internet.
- Revisa los logs de Docker: `docker compose logs squid`.

3. Consultas lentas

- Monitorea el uso de recursos del servidor proxy.
- Considera aumentar los recursos asignados al contenedor.
- Verifica la latencia de red entre API Gateway y tu proxy.

Last updated on 21/08/2026