Servidor proxy transparent

Índex

Un **servidor proxy** és un intermediari entre els dispositius d'una xarxa local i Internet.

Quan un client (ordinador, mòbil, etc.) vol accedir a una pàgina web, en lloc de connectar-se directament al servidor de destinació, la petició passa primer pel proxy, que la reenvia en nom del client i retorna la resposta.

1. Per a què serveix?

Control d'accés --- permet bloquejar webs per categoria, horari o usuari (com fèiem amb SquidGuard).

Caché --- emmagatzema còpies locals del contingut més visitat, reduint el consum d'amplada de banda i accelerant la navegació.

Seguretat --- filtra contingut maliciós, oculta les IP internes de la xarxa i pot inspeccionar el tràfic.

Registre i auditoria --- guarda logs de tota l'activitat de navegació, útil en entorns corporatius o educatius.

Anonimitat --- el servidor de destinació veu la IP del proxy, no la del client.

2. Tipus principals

- **Proxy explícit** --- els clients el configuren manualment al navegador.
- **Proxy transparent** --- intercepta el tràfic automàticament sense que els clients el sàpiguen (el que configuràvem amb Squid).
- **Proxy invers** --- s'usa al costat del servidor per distribuir càrrega o protegir aplicacions web (ex: Nginx, HAProxy).

3. Instal·lació

```
sudo apt update
sudo apt install squid squidguard -y
```

4. Configuració d'Squid (/etc/squid/squid.conf)

```
# Edita el fitxer de configuració principal
sudo nano /etc/squid/squid.conf
```

Aquesta és una configuració bàsica per a proxy transparent:

```
# Port transparent (intercepta el tràfic HTTP)
http_port 3128
http_port 3129 intercept

# Port per a HTTPS transparent (si cal)
https_port 3130 intercept ssl-bump cert=/etc/squid/ssl_cert/myCA.pem
 ↪  key=/etc/squid/ssl_cert/myCA.key

# Xarxa local permesa
acl localnet src 192.168.1.0/24
http_access allow localnet
http_access allow localhost
http_access deny all

# Integració amb SquidGuard
url_rewrite_program /usr/bin/squidGuard -c
 ↪  /etc/squidguard/squidGuard.conf
url_rewrite_children 5

# Logs
access_log /var/log/squid/access.log squid
cache_log /var/log/squid/cache.log

# Cache
cache_dir ufs /var/spool/squid 1000 16 256
maximum_object_size 50 MB
```

5. Configuració d'SquidGuard (/etc/squidguard/squidGuard.conf)

```
sudo nano /etc/squidguard/squidGuard.conf
```

```
# Directori de bases de dades
dbhome /var/lib/squidguard/db
logdir /var/log/squidguard

# Definició de temps
time workhours {
    weekly mtwhf 08:00 - 18:00
}
```

```
# Definició de xarxes
src admin {
    ip 192.168.1.1
}

src users {
    ip 192.168.1.0/24
}

# Llistes negres (blacklists)
dest adult {
    domainlist blacklists/adult/domains
    urllist    blacklists/adult/urls
}

dest ads {
    domainlist blacklists/ads/domains
}

dest social {
    domainlist blacklists/social/domains
}

# Regles d'accés
acl {
    admin {
        pass all
    }

    users within workhours {
        pass !adult !ads all
    }

    users {
        pass !adult !ads !social all
    }

    default {
        pass none
        redirect http://192.168.1.1/blocked.html
    }
}
```

6. Descarregar llistes negres

Pots usar les llistes de **Shallalist** o **URLBlacklist**:

```
# Crear directori
sudo mkdir -p /var/lib/squidguard/db
cd /var/lib/squidguard/db

# Descarregar Shallalist (exemple)
sudo wget http://www.shallalist.de/Downloads/shallalist.tar.gz
sudo tar -xzf shallalist.tar.gz
sudo mv BL blacklists

# Compilar les bases de dades
sudo squidGuard -C all

# Ajustar permisos
sudo chown -R proxy:proxy /var/lib/squidguard/db
```

7. Redirecció de trànsit amb iptables

Per fer el proxy **realment transparent**, has de redirigir el trànsit del port 80 cap a Squid:

```
# Redirigir HTTP (port 80) al port interceptor de Squid
sudo iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j
 ↪  REDIRECT --to-port 3129

# Permetre tràfic de Squid
sudo iptables -A INPUT -p tcp --dport 3129 -j ACCEPT

# Activar IP forwarding
echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward

# Fer-ho persistent
sudo nano /etc/sysctl.conf
# Afegeix: net.ipv4.ip_forward = 1
```

Per fer les regles d'iptables persistents:

```
sudo apt install iptables-persistent -y
sudo netfilter-persistent save
```

8. Iniciar i habilitar els serveis

```
# Verificar configuració de Squid
sudo squid -k parse

# Reiniciar Squid
sudo systemctl restart squid
sudo systemctl enable squid

# Verificar estat
sudo systemctl status squid
```

9. Verificació

```
# Comprovar que Squid escolta als ports correctes
sudo ss -tlnp | grep squid

# Seguir els logs en temps real
sudo tail -f /var/log/squid/access.log
sudo tail -f /var/log/squidguard/squidGuard.log
```

10. Resum de ports

Port	Funció
3128	Proxy estàndard
3129	Intercepció HTTP transparent
3130	Intercepció HTTPS (SSL Bump)

> **Nota:** Per interceptar HTTPS necessites configurar SSL Bump i distribuir el certificat CA als clients, cosa que té implicacions de privacitat i seguretat que cal tenir en compte.

11. Configurar SSL Bump a Squid

SSL Bump permet que Squid intercepti i inspeccioni tràfic HTTPS. Funciona com un “man-in-the-middle” legítim dins la teva xarxa.

11.1. Generar el certificat CA

```
# Crear directori per als certificats
sudo mkdir -p /etc/squid/ssl_cert
sudo chown proxy:proxy /etc/squid/ssl_cert
sudo chmod 700 /etc/squid/ssl_cert

cd /etc/squid/ssl_cert

# Generar clau privada
sudo openssl genrsa -out myCA.key 4096

# Generar certificat CA autosignat (10 anys)
sudo openssl req -new -x509 -days 3650 -key myCA.key -out myCA.pem
 ↪  -subj "/C=ES/ST=Catalunya/L=Barcelona/O=La meva
 ↪  organització/CN=Proxy CA"

# Ajustar permisos
sudo chown proxy:proxy myCA.key myCA.pem
sudo chmod 600 myCA.key
```

11.2. Preparar la caché SSL

```
# Crear directori per a la caché de certificats
sudo mkdir -p /var/spool/squid/ssl_db

# Inicialitzar la base de dades SSL
sudo /usr/lib/squid/security_file_certgen -c -s
 ↪  /var/spool/squid/ssl_db -M 4MB

# Ajustar permisos
sudo chown -R proxy:proxy /var/spool/squid/ssl_db
```

11.3. Configuració de Squid amb SSL Bump

```
# Edita el fitxer squid.conf
sudo nano /etc/squid/squid.conf
```

```
# Ports
http_port 3129 intercept
https_port 3130 intercept ssl-bump cert=/etc/squid/ssl_cert/myCA.pem
 ↪  key=/etc/squid/ssl_cert/myCA.key generate-host-certificates=on
 ↪  dynamic_cert_mem_cache_size=4MB

# Generador de certificats
sslcrtd_program /usr/lib/squid/security_file_certgen -s
 ↪  /var/spool/squid/ssl_db -M 4MB
```

```
sslcrtd_children 5

# Dominis que NO s'han d'interceptar (banques, etc.)
acl no_bump_domains ssl::server_name .bankinter.com
acl no_bump_domains ssl::server_name .caixabank.com
acl no_bump_domains ssl::server_name .lacaixa.com

# Estratègia SSL Bump
ssl_bump splice no_bump_domains   # Deixar passar sense inspeccionar
ssl_bump stare all                # Inspeccionar la resta
ssl_bump bump all

# Verificació de certificats del servidor
sslproxy_cert_error deny all
sslproxy_flags DONT_VERIFY_PEER   # Només si cal per compatibilitat

# Opcions SSL
tls_outgoing_options min-version=1.2
```

11.4. Regles iptables per a HTTPS

```
# Redirigir HTTP
sudo iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j
 ↪  REDIRECT --to-port 3129

# Redirigir HTTPS
sudo iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j
 ↪  REDIRECT --to-port 3130

# Guardar regles
sudo netfilter-persistent save
```

11.5. Distribuir el certificat CA als clients

Linux (Ubuntu/Debian)

```
# Copiar el certificat
sudo cp myCA.pem /usr/local/share/ca-certificates/proxy-ca.crt

# Actualitzar certificats del sistema
sudo update-ca-certificates

# Verificar
ls /etc/ssl/certs/ | grep proxy
```

Windows (GPO per a dominis o manual)

Manual:

```
# Importar via PowerShell (com a administrador)
Import-Certificate -FilePath "myCA.pem" `
    -CertStoreLocation Cert:\LocalMachine\Root
```

Via GPO (recomanat en entorns corporatius):

1. Obre `Administració de directives de grup`
2. Navega a `Configuració de l'equip -> Configuració de Windows -> Configuració de seguretat -> Directrius de clau pública`
3. Fes clic dret a `Autoritats de certificació arrel de confiança`
4. Importa `myCA.pem`

macOS

```
# Via terminal
sudo security add-trusted-cert -d -r trustRoot -k
 ↪  /Library/Keychains/System.keychain myCA.pem
```

O manualment:

1. Obre **Accés a Clauer**
2. Arrossega `myCA.pem` a **Clauer del sistema**
3. Fes doble clic al certificat -> **Confiar** -> **Sempre confiar**

Android

1. Copia `myCA.pem` al dispositiu
2. Ves a **Configuració -> Seguretat -> Instal·lar certificat**
3. Selecciona el fitxer i instal·la'l com a **Certificat CA**

   Android 7+ limita els certificats d'usuari per a apps. Necessites accés root o MDM per a una confiança total.

iOS / iPadOS

1. Envia el fitxer `myCA.pem` per AirDrop o correu
2. Ves a **Configuració -> General -> VPN i gestió de dispositius**
3. Instal·la el perfil
4. Ves a **Configuració -> General -> Quant a -> Confiança de certificats arrel**
5. Activa el certificat

11.6. Verificar que SSL Bump funciona

```
# Reiniciar Squid
sudo systemctl restart squid

# Comprovar logs SSL
sudo tail -f /var/log/squid/access.log | grep CONNECT

# Provar des d'un client (hauria de mostrar l'emissor
# com "La meva organització")
curl -v https://example.com 2>&1 | grep "issuer"
```

11.7. Consideracions importants

Aspecte	Detall
Legalitat	Informa sempre els usuaris que el tràfic és inspeccionat
Privacitat	Evita inspeccionar serveis bancaris, mèdics o personals
Certificate Pinning	Algunes apps (WhatsApp, etc.) fallaran perquè verifiquen el certificat directament
HTTP/3 (QUIC)	Squid no suporta QUIC; bloqueja el port UDP 443 si cal

Versions d'aquest document

- HTML - proxy.html
- PDF - proxy.pdf
- ODT - proxy.odt
- MD - proxy.md