Atelier Pratique 1 :

Le Forward Proxy avec Squid

Présenté par : Rachid Bouselama

Superviseur : Mr Lahcen AIT IBOUREK

Le Monde des Proxys : Votre Gardien Numérique

Dans le paysage numérique actuel, comprendre comment les informations transitent sur Internet est crucial. Au cœur de cette compréhension se trouve le concept de mandataire, ou proxy. Ce rôle d'intermédiaire est essentiel pour la sécurité, la performance et le contrôle de votre infrastructure réseau.

Introduction

Qu'est-ce qu'un Mandataire (Proxy) ?

Définition Clé

Un mandataire (proxy) est un serveur intermédiaire qui agit entre un utilisateur (client) et Internet. Il ne s'agit pas d'une connexion directe, mais d'un point de passage stratégique.

Mécanisme Simplifié

Le client envoie sa demande au proxy, qui la transmet au site web. Le proxy reçoit ensuite la réponse du site et la retourne au client.

Rôle Fondamental

Le proxy agit au nom du client, comme un véritable représentant, dissimulant ainsi l'identité réelle du demandeur tout en assurant des fonctions essentielles.

Ce fonctionnement, bien que simple en apparence, est la pierre angulaire de nombreuses stratégies de réseau, visant à contrôler, sécuriser et optimiser l'accès à Internet.

Fonctionnalités & Avantages

Les Rôles Multiples et Avantages Stratégiques d'un Proxy

Sécurité Renforcée

Un proxy peut bloquer activement les sites web malveillants et protéger les utilisateurs contre les menaces telles que le phishing, les malwares et les attaques ciblées, agissant comme un bouclier numérique.

Filtrage de Contenu

Il permet d'interdire l'accès à certaines catégories de sites (réseaux sociaux, streaming) et d'appliquer des règles de navigation précises en fonction de l'utilisateur, du groupe ou de l'horaire, garantissant une utilisation conforme aux politiques internes.

Optimisation des Performances

Grâce à la mise en cache des pages web déjà consultées, le proxy accélère la navigation pour les requêtes répétées et réduit significativement la consommation de bande passante, améliorant l'expérience utilisateur et l'efficacité du réseau.

Contrôle et Traçabilité

Chaque connexion est enregistrée dans des journaux (logs), offrant aux administrateurs réseau une visibilité complète sur l'utilisation d'Internet, essentielle pour l'audit, la conformité et l'identification des anomalies.

Ces fonctionnalités rendent les proxys indispensables dans les environnements professionnels, éducatifs et administratifs, où la gestion du réseau est une priorité absolue.

Types de Proxys

Le Forward Proxy : Contrôle Client-Side

Positionnement Stratégique

Le Forward Proxy est placé côté client, entre les utilisateurs du réseau interne et Internet. C'est le point de passage obligé pour toute requête sortante.

Fonctionnement Détaillé

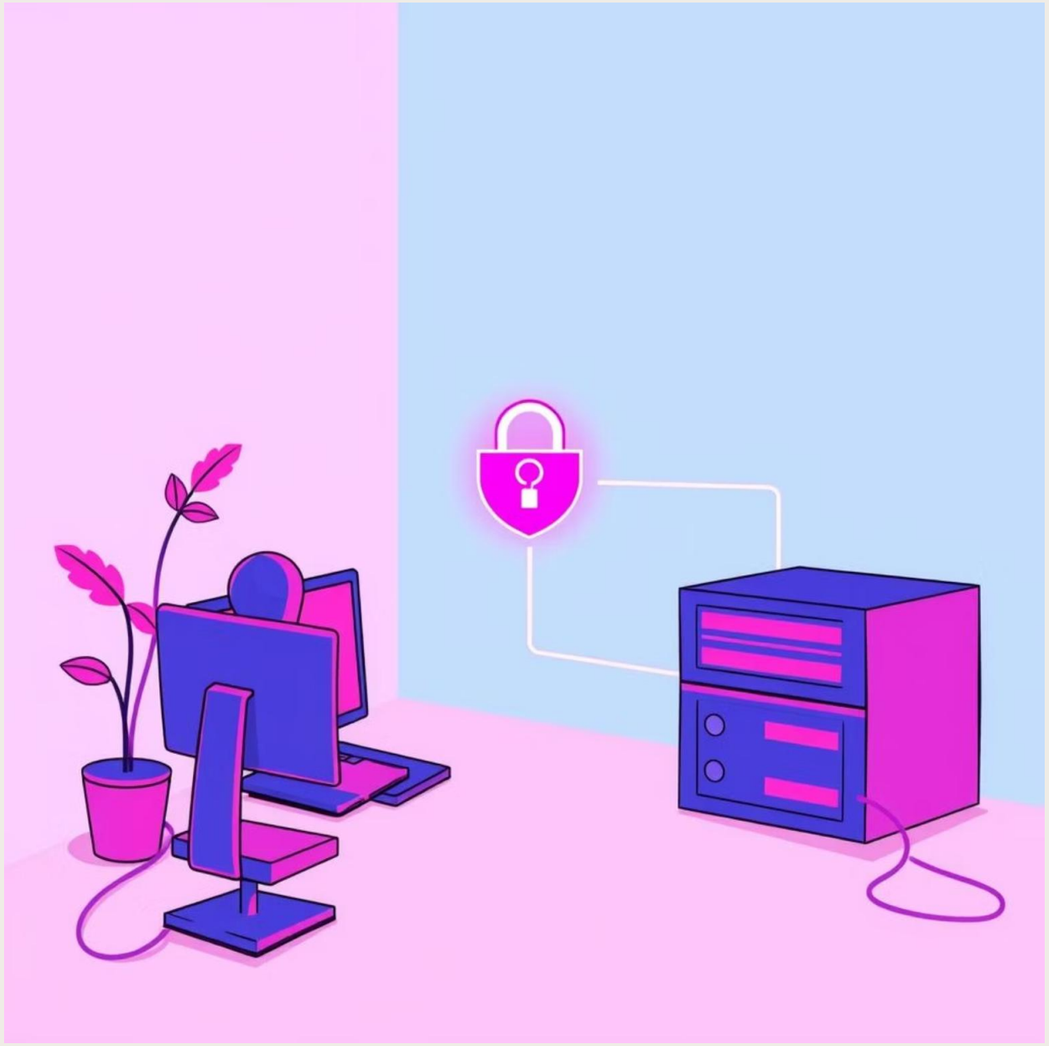
Toutes les requêtes des utilisateurs passent par ce proxy. Il prend ensuite des décisions cruciales : autoriser ou bloquer l'accès, enregistrer les activités, et accélérer la navigation grâce au cache.

Objectifs Principaux

- Contrôler finement l'accès à Internet et filtrer le contenu inapproprié.
- Améliorer les performances en réduisant la latence et la consommation de bande passante.
- Masquer les adresses IP des utilisateurs pour préserver leur confidentialité en ligne.

Exemple Concret

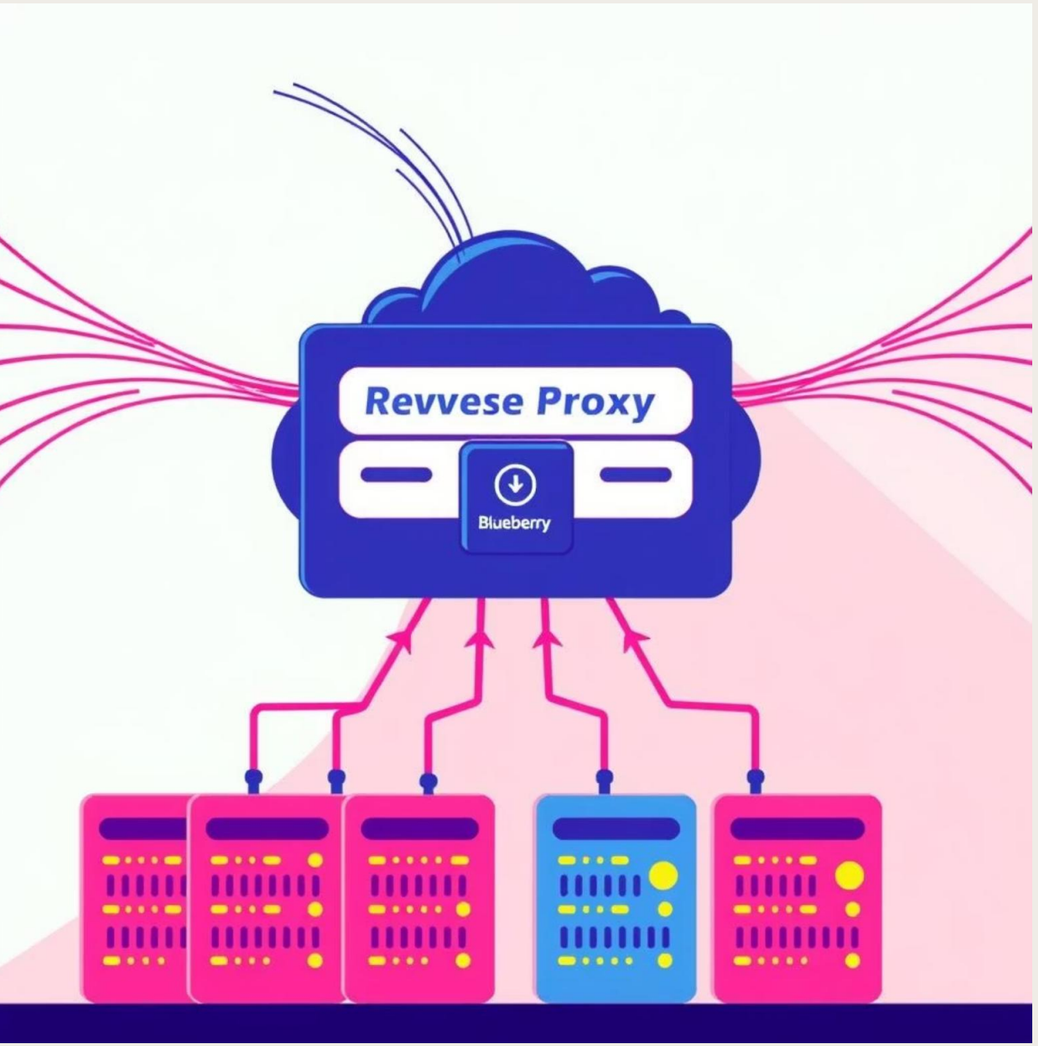
Un logiciel tel que **Squid** est un exemple courant de Forward Proxy, largement utilisé dans les entreprises.



Le Forward Proxy protège et contrôle les utilisateurs internes, garantissant une navigation sécurisée et conforme aux politiques de l'organisation.

Types de Proxys

Le Reverse Proxy : Protection Serveur-Side



Localisation Essentielle

Le Reverse Proxy est positionné côté serveur, agissant comme une façade devant un ou plusieurs serveurs web internes.

Processus Opérationnel

Les clients externes (sur Internet) se connectent au Reverse Proxy, qui ensuite redirige la requête vers le serveur interne approprié, rendant les serveurs réels invisibles et protégés.

Bénéfices Clés

- Répartition de charge (Load Balancing) pour distribuer les requêtes et éviter la surcharge d'un serveur.
- Protection accrue des serveurs contre les attaques externes en masquant leur identité.
- Amélioration des performances par la mise en cache et la centralisation du chiffrement SSL/HTTPS.

Solutions Populaires

Des outils comme **Nginx**, **HAProxy** et **Traefik** sont des exemples puissants de Reverse Proxys.

Le Reverse Proxy protège et optimise les serveurs web, assurant haute disponibilité et performance face aux requêtes externes.

Comparaison

Proxy vs. VPN : Deux Protecteurs, des Rôles Distincts

Bien que les proxys et les VPNs soient tous deux des intermédiaires, leurs objectifs et leurs modes de fonctionnement diffèrent fondamentalement.

Niveau d'Action	Application (Web)	Réseau complet
Chiffrement	Partiel ou non	Total du trafic
Trafic Protégé	Principalement le web	Tout le trafic
Usage Principal	Filtrage, contrôle, cache	Sécurité, confidentialité, accès distant

Comprendre ces différences est crucial pour choisir la solution adaptée à vos besoins spécifiques : gestion et contrôle du réseau pour le proxy, ou sécurité et confidentialité globales pour le VPN.

Proxy : Un Pilier de la Cybersécurité d'Entreprise

Défense contre les Menaces

Le proxy est une première ligne de défense, bloquant l'accès aux sites connus pour héberger des malwares, du phishing ou d'autres cybermenaces avant qu'elles n'atteignent le réseau interne.

Conformité et Politiques

Il permet d'appliquer des politiques de sécurité et d'utilisation d'Internet, essentielles pour la conformité réglementaire (RGPD, etc.) et pour prévenir la fuite de données sensibles.

Prévention des Fuites de Données

En contrôlant les données qui sortent du réseau, un proxy peut aider à identifier et à prévenir les tentatives d'exfiltration d'informations confidentielles, volontaires ou accidentelles.

Pour les administrateurs réseau, le proxy n'est pas qu'un outil de gestion, c'est un composant fondamental d'une stratégie de cybersécurité robuste et proactive.

Impact du Proxy sur la Productivité et la Bande Passante

Accélération de la Navigation

Grâce à son mécanisme de cache, le proxy réduit le temps de chargement des pages fréquemment visitées, améliorant ainsi l'efficacité et la productivité des employés.

Optimisation de la Bande Passante

En servant les requêtes depuis son cache, le proxy diminue le trafic vers Internet, libérant de la bande passante pour les applications critiques et réduisant les coûts de connexion.

Réduction des Distractions

Le filtrage de contenu permet de bloquer l'accès aux sites non professionnels, aidant les employés à rester concentrés sur leurs tâches et à minimiser les distractions.

L'intégration d'un proxy dans l'architecture réseau est un investissement qui se traduit par des gains tangibles en termes de performance opérationnelle et de gestion des ressources.

Considérations pour le Déploiement et la Gestion

01

Choix du Type de Proxy

Évaluer si un Forward, Reverse, ou une combinaison est nécessaire en fonction des objectifs : contrôle utilisateur, protection serveur, ou les deux.

02

Configuration des Règles

Définir des politiques de filtrage claires et granulaires (sites, horaires, utilisateurs) pour équilibrer sécurité et flexibilité.

03

Maintenance et Monitoring

Assurer une surveillance régulière des logs, des performances du cache et des mises à jour logicielles pour garantir l'efficacité et la sécurité continue.

04

Évolutivité

Planifier la capacité du proxy pour gérer l'augmentation du trafic et des utilisateurs, assurant une performance optimale à long terme.

Un déploiement réussi d'un proxy nécessite une planification minutieuse et une gestion proactive pour maximiser ses bénéfices et minimiser les risques.

Le Proxy : Un Actif Indispensable

> Le mandataire (proxy) est bien plus qu'un simple relais. C'est un outil polyvalent et stratégique qui, correctement implémenté, devient un pilier essentiel de toute infrastructure réseau moderne. Il assure la sécurité, optimise les performances et offre un contrôle inégalé sur les flux de données, protégeant ainsi vos actifs les plus précieux et garantissant une expérience numérique fluide et sécurisée pour tous.

Merci de votre attention.

Objectif de l'Atelier : Forward Proxy avec Squid

Cet atelier pratique vise à maîtriser la mise en œuvre d'un Forward Proxy à l'aide de Squid, une solution essentielle pour le contrôle de l'accès Internet en environnement d'entreprise.

Installer et Configurer

Apprendre à installer Squid et à configurer un proxy HTTP.

Bloquer et Autoriser

Mettre en place des règles de filtrage pour bloquer des sites spécifiques et autoriser uniquement le réseau interne.

Tester et Valider

Vérifier le bon fonctionnement du proxy et des règles de filtrage depuis un poste client.

Squid est un pilier de la gestion d'accès Internet en entreprise, garantissant sécurité et conformité.

Architecture et Préparation de l'Environnement

Pour cet atelier, nous allons simuler un environnement réseau typique avec un serveur proxy dédié et un réseau de clients internes.

Serveur Proxy

- **Nom :** srv-proxy01
- **Adresse IP :** 192.168.1.100
- **Rôle :** Point de passage obligatoire pour l'accès Internet.

Clients

- **Réseau :** 192.168.1.0/24
- **Accès :** Via le proxy uniquement.
- **Schéma Logique :** Clients → Squid Proxy → Internet

Pré-requis Techniques

Serveur Debian

Une machine virtuelle ou physique avec Debian installé.

Accès Root/Sudo

Nécessaire pour les installations et configurations système.

Connexion Internet

Fonctionnelle pour le téléchargement des paquets.

Le proxy sera le seul point de sortie autorisé vers Internet pour le réseau client, garantissant un contrôle total.

Étape 1 : Installation de Squid et Sauvegarde

Cette première étape cruciale consiste à installer le serveur proxy Squid sur notre machine Debian et à sécuriser la configuration initiale.

Installation de Squid sur srv-proxy01

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

Ces commandes mettent à jour les listes de paquets et installent Squid de manière non interactive.

Sauvegarde de la Configuration Originale

Avant toute modification, il est impératif de sauvegarder le fichier de configuration par défaut de Squid.

```
sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.bak
```

1

Réversibilité

Permet de revenir facilement à la configuration d'origine en cas de problème.

2

Bonne Pratique

Une étape fondamentale de toute administration système responsable.

Squid est maintenant installé et prêt à être configuré selon nos besoins de filtrage.

Administrateur : Invite de commandes - ssh root@192.168.217.141

```
Microsoft Windows [version 10.0.26200.7462]
(c) Microsoft Corporation. Tous droits réservés.

C:\Windows\System32>ssh root@192.168.217.141
root@192.168.217.141's password:
Linux srv-dns02 6.12.57+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.57-1 (2025-11-05) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Dec  7 21:51:03 2025 from 192.168.217.1
root@srv-dns02:~# sudo apt update
Réception de : 1 http://security.debian.org/debian-security trixie-security InRelease [43,4 kB]
Atteint : 2 http://deb.debian.org/debian trixie InRelease
Réception de : 3 http://deb.debian.org/debian trixie-updates InRelease [47,3 kB]
Réception de : 4 http://security.debian.org/debian-security trixie-security/main Sources [117 kB]
Réception de : 5 http://security.debian.org/debian-security trixie-security/main amd64 Packages [94,0 kB]
Réception de : 6 http://security.debian.org/debian-security trixie-security/main Translation-en [59,1 kB]
361 ko réceptionnés en 0s (1 030 ko/s)
1 paquet peut être mis à jour. Exécutez « apt list --upgradable » pour le voir.
root@srv-dns02:~# sudo apt update && sudo apt install squid -y
Atteint : 1 http://deb.debian.org/debian trixie InRelease
Atteint : 2 http://security.debian.org/debian-security trixie-security InRelease
Atteint : 3 http://deb.debian.org/debian trixie-updates InRelease
1 paquet peut être mis à jour. Exécutez « apt list --upgradable » pour le voir.
Installation de :
  squid
```

Étape 2 : Configuration du Filtrage (ACL) dans Squid

Le cœur de la politique d'accès Internet réside dans la configuration des Listes de Contrôle d'Accès (ACL) dans le fichier `/etc/squid/squid.conf`.

Configuration Minimale Expliquée

Nous allons définir les règles qui permettront de bloquer certains sites web et d'autoriser uniquement le trafic provenant de notre réseau interne.

```
# Définir le réseau local autorisé
acl local_network src 192.168.1.0/24

# Définir les sites interdits
acl restricted_sites dstdomain .facebook.com .instagram.com .twitter.com

# Règles d'accès
http_access deny restricted_sites
http_access allow local_network

# Refuser tout le reste
http_access deny all

# Port d'écoute du proxy
http_port 3128
```

acl (Access Control List)

Permet de définir des critères (qui, quoi, où) pour le filtrage du trafic.

http_access

Applique les règles ACL définies, en spécifiant si l'accès est autorisé ou refusé.

Ordre d'importance

Squid évalue les règles de haut en bas. La première règle qui correspond est appliquée. Il est donc crucial de placer les règles les plus spécifiques ou les règles de refus avant les règles plus génériques d'autorisation.

Avec cette configuration, les réseaux sociaux spécifiés seront bloqués pour les utilisateurs du réseau `192.168.1.0/24`, et tout autre accès non explicitement autorisé sera refusé.

Administrateur : Invite de commandes - ssh root@192.168.217.141

GNU nano 8.4 /etc/squid/squid.conf

```
# Définir le réseau local
acl local_network src 192.168.1.0/24

# Définir les sites interdits
acl restricted_sites dstdomain .facebook.com .instagram.com .twitter.com

# Règles d'accès
http_access deny restricted_sites
http_access allow local_network
http_access deny all

# Port d'écoute
http_port 3128
```

[Lecture de 13 lignes]

^G Aide	^O Écrire	^F Chercher	^K Couper	^T Exécuter	^C Emplacement	M-U Annuler
^X Quitter	^R Lire fich.	^\ Remplacer	^U Coller	^J Justifier	^/ Aller ligne	M-E Refaire

Étape 3 : Application des Changements et Tests Client

Après avoir configuré Squid, il est temps d'appliquer les nouvelles règles et de vérifier que le proxy fonctionne comme prévu depuis un poste client.

Redémarrage et Vérification de Squid

Pour que les nouvelles configurations soient prises en compte, Squid doit être redémarré. Nous vérifierons ensuite son statut.

```
sudo systemctl restart squid
sudo systemctl status squid
```

Test Côté Client (Exemple avec Linux)

Sur un poste client du réseau 192.168.1.0/24, configurez la variable d'environnement pour utiliser le proxy.

```
export http_proxy="http://192.168.1.100:3128"
```

Site Autorisé

```
curl -I http://www.google.com
```

Résultat attendu : Code HTTP **200 OK**.

Site Bloqué

```
curl -I http://www.facebook.com
```

Résultat attendu : Code HTTP **403 Forbidden**.

Résultat Final

Félicitations ! Votre Forward Proxy est désormais opérationnel, filtrant l'accès Internet selon les règles définies.

Windows PowerShell | Windows PowerShell

```
X-Squid-Error: ERR_DNS_FAIL 0
Vary: Accept-Language
Content-Language: en
Cache-Status: proxy;detail=mismatch
Via: 1.1 proxy (squid/6.13)
Connection: keep-alive

root@client:~# curl -I http://www.google.com
HTTP/1.1 200 OK
Content-Type: text/html; charset=ISO-8859-1
Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-mazvvd_qsQJF7VMNFvxumg' 'strict
-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
-hp
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Date: Sun, 04 Jan 2026 09:26:33 GMT
Server: gws
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Expires: Sun, 04 Jan 2026 09:26:33 GMT
Cache-Control: private
Set-Cookie: AEC=AaJma5sw96hH1aH3F6U0SqG5-2o_v9pS46RC2KTW96PXwD62u81euoKB9lU; expires=Fri, 03-Jul-2026 09:26:33 GMT; path
=/; domain=.google.com; Secure; HttpOnly; SameSite=lax
Set-Cookie: NID=527=LevbFhiODd14V_6FNAtvIu81ZZmePmicD_D0h_3BVel-Bc-u7If-XCqnkey1fXksqnKjY
dpBlVs9FFUKduGGHsNfHLEe9u8F5fyonQON1JV7x6xLZHBXnBt9JI-eRGOhCdAjLHhIzovdznAPrXQtE6wWGKQFGfs
; expires=Mon, 06-Jul-2026 09:26:33 GMT; path=/; domain=.google.com; HttpOnly
Cache-Status: proxy;detail=mismatch
Via: 1.1 proxy (squid/6.13)
Connection: keep-alive

root@client:~#
```

Windows PowerShell | Windows PowerShell

```
i, 03-Jul-2026 09:26:33 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax
Set-Cookie: NID=527=LevbFhiODd14V_6FNAtvIu81ZZmePmicD_D0h_3BVel-Bc-u7If-XCqnkey1fXksqnK
jYWiTlWG8k-x-0ti9hpXwvxO6IEV552GTdpBlVs9FFUKduGGHsNfHLEe9u8F5fyonQON1JV7x6xLZHBXnBt9JI-
eRGOhCdAjLHhIzovdznAPrXQtE6wWGKQFGfsbFWGfhXDaaupAnbIFybAzyL5UGcetQ; expires=Mon, 06-Jul
-2026 09:26:33 GMT; path=/; domain=.google.com; HttpOnly
Cache-Status: proxy;detail=mismatch
Via: 1.1 proxy (squid/6.13)
Connection: keep-alive

root@client:~# curl -I http://www.facebook.com
HTTP/1.1 403 Forbidden
Server: squid/6.13
Mime-Version: 1.0
Date: Sun, 04 Jan 2026 09:28:49 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 3061
X-Squid-Error: ERR_ACCESS_DENIED 0
Vary: Accept-Language
Content-Language: en
Cache-Status: proxy
Via: 1.1 proxy (squid/6.13)
Connection: keep-alive

root@client:~#
```

Windows PowerShell

Windows PowerShell

```
 GNU nano 8.4                /etc/nginx/sites-available/load-balancer *
upstream backend_servers {
    # Stratégie par défaut : Round Robin (un par un)
    server 192.168.1.10:80;  # srv-web-01
    server 192.168.1.11:80;  # srv-web-02
}

server {
    listen 80;
    server_name www.innov-tech.com;

    location / {
        proxy_pass http://backend_servers;
        # Transmettre l'IP réelle du client aux serveurs web
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    }
}



^G Aide       ^O Écrire     ^F Chercher   ^K Couper     ^T Exécuter   ^C Emplacement
^X Quitter    ^R Lire fich. ^\ Remplacer  ^U Coller     ^J Justifier  ^/ Aller ligne
```