server intermedio tra il computer dell'utente e il server web

un sistema in cui l’elaborazione delle informazioni è distribuita su più calcolatori anziché centralizzata su una singola macchina

conserva in memoria i file e le pagine Internet maggiormente visitate, rendendo in tal modo più rapida la loro consultazione.

* Fornire l'anonimato durante la navigazione [Internet](https://it.wikipedia.org/wiki/Internet) (es. sistema [TOR](https://it.wikipedia.org/wiki/Tor_(software)))
* Memorizzare una copia locale degli oggetti web richiesti in modo da poterli fornire nuovamente senza effettuare altri accessi ai server di destinazione (**HTTP caching proxy**)
* Creare una "barriera di difesa" (Firewall) verso il web, agendo da filtro per le connessioni entranti ed uscenti e monitorando, controllando e modificando il traffico interno
* Un server proxy che trasmette richieste e risposte senza modificarle è detto **gateway** o **tunneling proxy**
* Un forward proxy è un proxy volto a internet usato per recuperare dati da un vastissimo campo di risorse (generalmente ovunque su internet)
* Un [reverse proxy](https://it.wikipedia.org/wiki/Reverse_proxy) è anch'esso rivolto ad internet ed è usato *front-end* per controllare e proteggere gli accessi ai server su una rete privata. Ha inoltre diverse mansioni quali bilanciamento del carico, autenticazione, decrittazione e caching

**Controllo del contenuto**

Un proxy web atto al filtraggio del contenuto consente il controllo amministrativo sul contenuto che può essere trasmesso in una o entrambe le direzioni attraverso il proxy. È comunemente usato sia nelle organizzazioni commerciali che non-commerciali (soprattutto scuole) per garantire che l'utilizzo di Internet sia conforme ad una accettabile politica di utilizzo.

#### Aggirare filtri e censura

Se il server di destinazione filtra i contenuti basandosi sull'origine della richiesta, l'uso di un proxy può aggirare questo filtro. Ad esempio, un server che usa la geolocalizzazione dell'indirizzo IP per restringere il campo dei suoi servizi a determinati Paesi, può eseguire l'accesso usando un server proxy localizzato in uno dei Paesi a cui è consentito accedere.

I proxy web sono il mezzo più comune di aggirare censure governative nonostante non più del 3% degli utenti di internet usi strumenti atti a questo scopo[[3]](https://it.wikipedia.org/wiki/Proxy#cite_note-3).

#### Accessi e intercettazioni

I proxy possono essere installati in modo da intercettare dati sul flusso tra computer client e il web. Tutti i contenuti inviati - incluse le password inviate e cookies utilizzati - possono essere catturati e analizzati da parte del proxy. Per questo motivo, le password per i servizi online (come webmail e bancari) devono sempre essere scambiati attraverso una connessione protetta crittograficamente come SSL.

### Proxy contro NAT

La maggior parte delle volte, con il termine proxy ci si riferisce ad un'applicazione di livello 7 della [pila ISO/OSI](https://it.wikipedia.org/wiki/Modello_OSI). In ogni modo, esistono altri modi di "proxare": uno di questi è attraverso il livello 3 (della pila ISO/OSI) è conosciuto come Network Address Translation ([NAT](https://it.wikipedia.org/wiki/Network_address_translation)). Le differenze tra queste due tecnologie di realizzare proxy sono il livello in cui operano e la procedura di configurazione dei client e dei server che adottano.

Nella configurazione del client per il proxy di livello 3 (NAT) è sufficiente configurare il gateway. Per quello di livello 7 invece, la destinazione dei pacchetti che genera il client deve essere sempre il server proxy, che legge ogni pacchetto e trova la destinazione reale.

Il NAT poiché opera a livello 3 richiede meno risorse rispetto al proxy di livello 7, ma è allo stesso tempo meno flessibile.