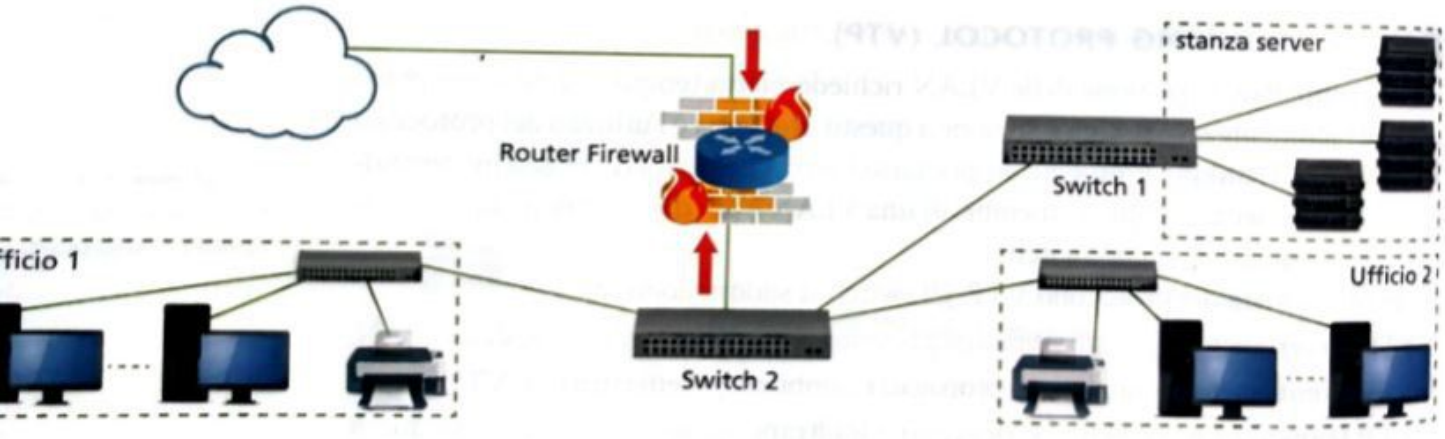
3 IL FIREWALL E LE ACL

3.1 Firewall

Il **firewall** (letteralmente: muro tagliafuoco) è una linea di difesa indispensabile contro le intrusioni di rete poiché agisce come sentinella alla porta di collegamento del computer con una rete esterna come Internet. In pratica separa la LAN aziendale dalla WAN pubblica.

> Il firewall filtra tutti i **pacchetti entranti** e **uscenti**, da e verso una rete o un computer, secondo regole prestabilite (policy) che contribuiscono alla sicurezza della rete stessa.

Un firewall può essere realizzato con un computer (con almeno due schede di rete, una per l'input e l'altra per l'output) e il software apposito.
Nelle LAN aziendali viene realizzato attraverso una funzionalità logica (software) **inclusa nel router** oppure può essere implementato su un apparato **hardware dedicato**.
La sicurezza di tutta una rete aziendale connessa a Internet viene ricondotta quindi alla sicurezza di un ristrettissimo numero di nodi, generalmente uno. Solo il nodo costituito dal firewall risulta essere direttamente collegato a Internet e dunque solo su di esso occorre effettuare le operazioni di controllo degli accessi, contro i tentativi di intrusione nella rete, e delle uscite, per bloccare richieste contrarie alla policy aziendale (FIGURA 10).



RA 10 Router firewall: ecce indicano la direzione iltraggio

Non disporre di un firewall significa essere esposti a numerosi attacchi e tentativi di intrusione.
Nel caso di un semplice sistema casalingo, il danno può essere minimo, ma nel caso di un'azienda, una perdita di dati può risultare un danno considerevole soprattutto in termini di costi e affidabilità.
Il firewall diventa così uno degli strumenti più efficaci per la gestione della sicurezza delle reti, con la possibilità di gestirne le regole e definire i meccanismi di controllo degli accessi.
Un firewall è configurabile e i filtri possono essere aggiunti o rimossi quando serve. È possibile decidere quali programmi o quali host possono avere accesso a Internet da una rete e quali no.

endinota

ono anche i cosiddetti all personali, cioè promi installati sui normali ratori client, che filtrano amente i pacchetti che no ed escono da quel uter.

Per esempio, grazie a una regola del firewall si può stabilire che solo un computer in una rete può accedere a Internet, oppure un solo computer può usare il protocollo FTP o ricevere e mandare email.
Funzioni di sicurezza di alto livello mettono al sicuro la rete da attacchi provenienti dall'esterno ma anche dall'interno. Attacchi di tipo ARP spoofing, port scanning, DoS, Worm.Blaster, Worm.Sasser, SQL slammer, per citare solo i più comuni, sono identificati, intercettati e resi inoffensivi.

3.2 Categorie di firewall

I firewall si possono distinguere sostanzialmente in 3 categorie in base al livello dello stack TCP/IP in cui operano.

1. **Application Level Firewall**: intercetta le trasmissioni a livello Application dello stack TCP/IP. In altre parole, valuta il contenuto applicativo dei pacchetti, per esempio riconoscendo e bloccando i dati appartenenti a virus o worm noti in una sessione HTTP o SMTP. A questa categoria appartengono i **proxy**. Utilizzando un proxy, la configurazione della LAN privata non consente connessioni dirette verso l'esterno: il proxy è connesso sia alla rete privata sia alla rete pubblica e permette alcune connessioni in modo selettivo. In pratica, mediante regole prestabilite dall'amministratore, vengono gestite le applicazioni che hanno accesso a Internet. Lavorando a livello Application, questo tipo di firewall riconosce comandi specifici delle applicazioni e offre un alto livello di protezione a scapito però della velocità della rete.
2. **Packet Filter Firewall**: lavora a livello Network e a livello Transport. Il Packet Filter Firewall è molto più veloce dell'Application Level Firewall in quanto il controllo viene effettuato sui pochi byte di header (20, escluse le opzioni) senza preoccuparsi dell'applicazione (di livello superiore) che ha generato il pacchetto. D'altra parte, questo firewall non ha la possibilità di gestire i dati all'interno del pacchetto. Per esempio, una email contenente un virus può tranquillamente passare attraverso il firewall, se è consentito il traffico POP/SMTP. Questo implica anche che non si possono filtrare le informazioni che passano dai computer interni verso l'esterno. Grazie a questa superficialità nel controllo, però, la connessione di rete non subisce rallentamenti.

   Se collocato alla fonte della connessione a Internet può essere configurato per funzionare su tutta la LAN (router firewall). I parametri che il Packet Filter Firewall controlla nell'header del pacchetto possono essere:

   - l'indirizzo IP di origine e destinazione (header IP);
   - il numero della porta TCP/UDP di origine e destinazione (header TCP/UDP);
   - il protocollo di livello superiore usato (header IP).
3. **Stateful Packet Inspection Firewall:** agisce a livello Transport e permette, oltre al controllo dell'header del pacchetto dati, anche di analizzarne il contenuto per catturare più informazioni rispetto ai semplici indirizzi di origine e destinazione. Un firewall che utilizza questo tipo di tecnologia può controllare lo stato della connessione TCP e compilare le informazioni ottenute su una tabella. In questo modo le operazioni di filtraggio dei pacchetti risulteranno basate sia su impostazioni definite dall'amministratore, sia sulla base di regole adottate per pacchetti simili già scansionati dal firewall. Nel complesso pregi e difetti sono sostanzialmente gli stessi del Packet Filter Firewall.

3.3 Le ACL

La sintassi della configurazione di un firewall in molti casi è basata su un meccanismo di **lista di controllo degli accessi ACL (Access Control List)**.
Le ACL possono essere modificabili tramite configurazione esplicita da parte dell'amministratore di sistema o possono variare in base allo stato interno del sistema.

Le ACL sono un elenco di istruzioni da applicare alle interfacce di un router allo scopo di gestire il traffico, filtrando i pacchetti in entrata e in uscita.

Esistono varie ragioni per decidere di utilizzare le ACL:

- fornire un livello base di sicurezza: si può per esempio restringere gli accessi a una determinata rete o sottorete;
- limitare il traffico e aumentare la performance della rete: si può, infatti, decidere che alcuni pacchetti vengano processati prima di altri;
- decidere quale tipo di traffico può essere trasmesso: si può per esempio permettere l'invio di email e impedire allo stesso tempo il Telnet.

#prendinota

Tra le tecniche di filtraggio più usate vi sono quelle che si basano sulle *whitelist* oppure sulle *blacklist*: le prime elencano in una tabella i soli indirizzi verso cui consentono il passaggio dei pacchetti, bloccando tutti gli altri; le seconde, viceversa, elencano le destinazioni bloccate, consentendo il passaggio dei pacchetti verso tutte le destinazioni non elencate.

Le ACL vengono elaborate dal router in maniera sequenziale in base all'ordine in cui sono state inserite le varie clausole. Appena un pacchetto soddisfa una delle condizioni, la valutazione si interrompe e il resto delle ACL non viene preso in considerazione. Il pacchetto viene quindi inoltrato o eliminato secondo l'istruzione eseguita.
Se il pacchetto non soddisfa nessuna delle condizioni viene scartato (si considera che alla fine di una ACL non vuota ci sia l'istruzione deny any ovvero **nega tutto**). L'ordine con cui sono scritte le ACL è importante: essendo eseguite in sequenza, è necessario inserire le condizioni più restrittive all'inizio.

ACL è quindi un meccanismo usato per esprimere regole complesse che determinano l'accesso o meno ad alcune risorse di un sistema informatico da parte dei suoi utenti.
Le ACL possono essere standard, **Standard ACL**, oppure estese, **Extended ACL**.
Le prime specificano delle limitazioni ai pacchetti guardando esclusivamente l'indirizzo della sorgente e vanno posizionate sull'interfaccia del router il più possibile vicino alla destinazione finale.
Le seconde, invece, pongono le limitazioni ai pacchetti in base a molte specifiche, come il protocollo usato, l'indirizzo di sorgente, l'indirizzo di destinazione e la porta a cui è indirizzato il pacchetto.
La Lezione 8 sarà interamente dedicata alla creazione di ACL standard ed estese mediante Cisco Packet Tracer.

FISSA LE CONOSCENZE

- A che cosa serve il firewall?
- Quali sono le 3 categorie di firewall distinte in base al livello TCP/IP in cui operano?
- Che cosa sono le ACL?
- Quali sono i principali motivi per cui si decide di utilizzare le ACL?
- Perché è importante l'ordine in cui sono scritte le ACL?
- Che differenza c'è tra le ACL standard e quelle estese?

4 IL PROXY SERVER

4.1 I compiti del Proxy Server

Un **proxy** è un programma (in esecuzione su un semplice computer o su un apparato hardware) che si interpone tra un client e un server facendo da tramite. Il client si collega al proxy, invece che al server, e gli invia la richiesta. Il proxy, a sua volta, si collega al server a cui inoltra la richiesta del client. Infine il proxy, ricevuta la risposta, la inoltra al client. I proxy, nella maggior parte dei casi, lavorano a livello Application. Il loro compito principale è garantire la **connettività** e il **caching** ai client a loro collegati ai fini dell'efficienza della rete (FIGURA 11).

Collocare il proxy in una posizione prossima ai client permette un miglioramento delle prestazioni e una riduzione del consumo di banda. Un Proxy Server può essere usato per molti compiti, alcuni già visti nell'Unità 8 del volume del quarto anno affrontando i proxy HTTP (Proxy Web). Nel complesso, le configurazioni del Proxy Server permettono loro di svolgere alcuni compiti che ricordiamo:

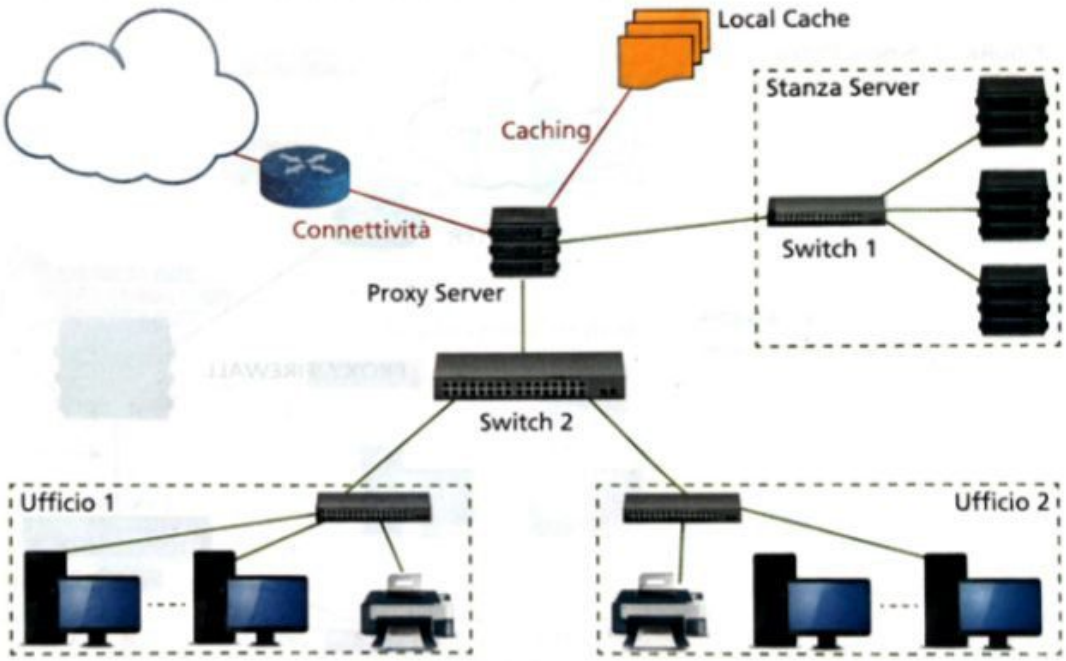


FIGURA 11 Collocazione del Proxy Server ai fini dell'efficienza della rete

- **connettività**: permettere a una intera rete privata di accedere a Internet attraverso un unico computer;
- **privacy**: mascherare il vero indirizzo IP del client in modo che il server remoto non venga a conoscenza di chi ha effettuato la richiesta. Questo compito verrà approfondito nella prossima Lezione 5, dove parleremo del Network Address Translation (NAT);
- **caching**: immagazzinare per un certo tempo i risultati delle richieste di un client e, se un altro client effettua le stesse richieste, rispondere senza dover consultare il server originale;
- **monitoraggio**: tenere traccia di tutte le operazioni effettuate (per esempio, tutte le pagine web visitate), consentendo statistiche e osservazioni dell'utilizzo della rete;
- **amministrazione**: applicare regole definite dall'amministratore di sistema per determinare quali richieste inoltrare e quali rifiutare, oppure limitare l'ampiezza di banda utilizzata dai client, oppure filtrare le pagine web in transito, per esempio bloccando quelle il cui contenuto è ritenuto offensivo in base a determinate regole;
- **filtraggio**: svolgere funzioni di firewall a livello Application, garantendo un alto grado di protezione a scapito della velocità della rete;

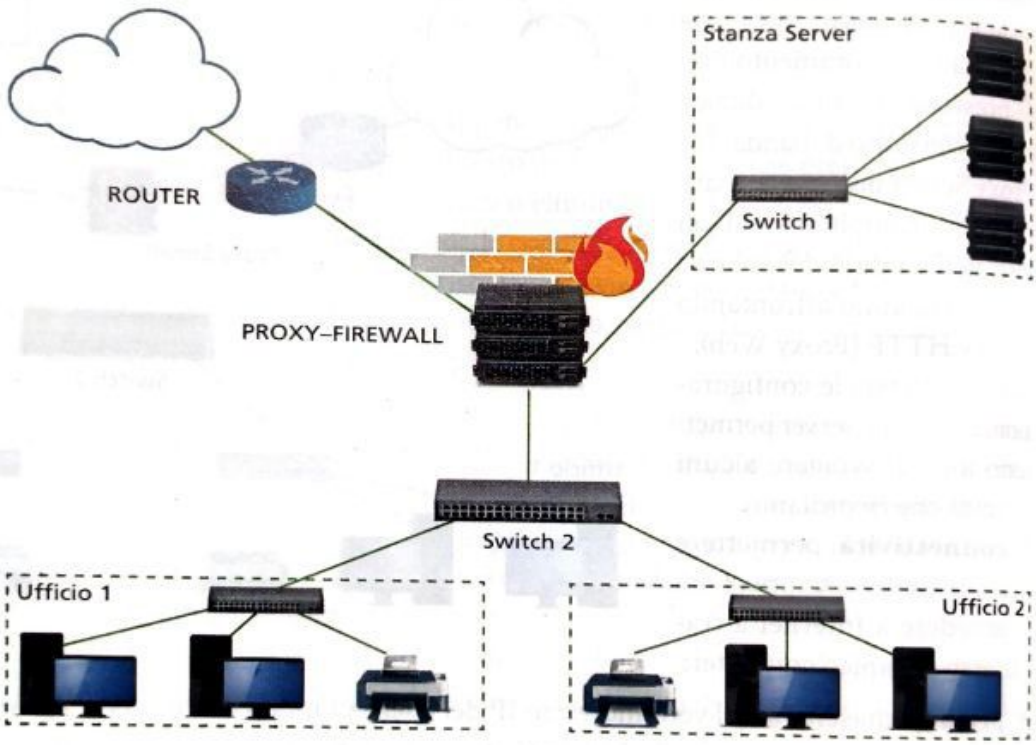
- **restrizioni**: creare una zona neutra (*terza zona*), non appartenente né alla LAN aziendale, né alla WAN, ma dove il traffico LAN e WAN è fortemente limitato e controllato. Questo processo verrà approfondito nella Lezione 6 dove parleremo della DeMilitarized Zone (DMZ).

4.2 Tipi di proxy

I Proxy Server, in particolare quelli che incorporano funzioni di firewall, possono essere diversamente collocati in base alle esigenze dell'azienda. Si possono individuare 3 categorie di utilizzo prevalenti.

1. **Single Proxy Topology**: risulta essere la scelta più semplice in quanto utilizza un singolo Proxy Server per servire l'intera rete (FIGURA 12). Questa configurazione è sufficiente però solo per un piccolo gruppo di client: la performance sarà compromessa appena aumenta il numero di client che richiedono pacchetti.

FIGURA 12 Single Proxy Topology



2. **Multiple Proxy Vertically Topology**: nel caso di reti medio-grandi è preferibile configurare più proxy, per esempio uno per ogni subnet, stabilendo un **proxy primario** a cui gli altri si connettono (FIGURA 13). I **proxy secondari** agiscono come client del primario. Questa tecnica *verticale* consente a qualsiasi client di avere il filtraggio dei pacchetti personalizzato. Il proxy secondario semplicemente guarda nel suo **repository** per vedere se è in grado di risolvere il pacchetto in transito. Se non lo risolve, inoltra il pacchetto al livello superiore, cioè verso il proxy primario. Questa configurazione fa sì che i proxy secondari dipendano dal primario per gli aggiornamenti, così come per i pacchetti personalizzati.
3. **Multiple Proxy Horizontally Topology**: consente di bilanciare il carico tra i server in base alle richieste dei client. In tale caso, le informazioni sul trattamento dei pacchetti personalizzati si distribuiscono ai server di pari livello, in modo da garantirne la risoluzione in locale (FIGURA 14). Lo svantaggio sta nella necessità di sincronizzare il repository di ogni proxy con quello degli altri.

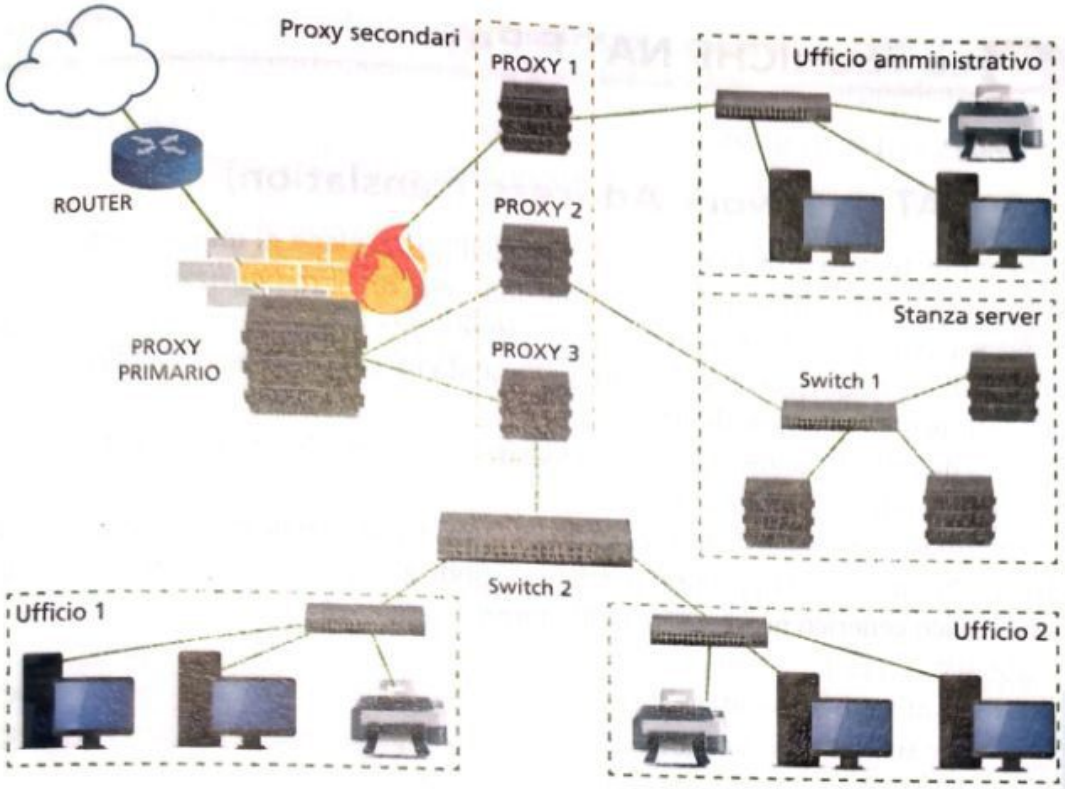


FIGURA 13 Multiple Proxy Vertically Topology

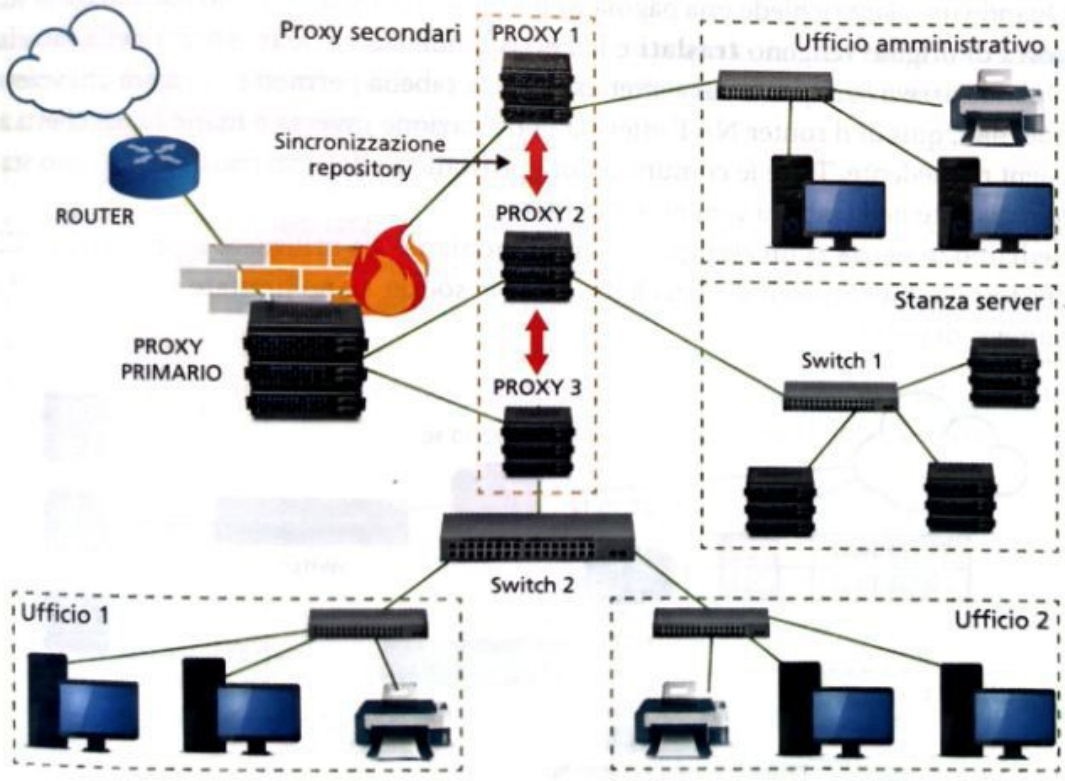


FIGURA 14 Multiple Proxy Horizontally Topology

FISSA LE CONOSCENZE

- Che cos'è un Proxy Server?
- Quali sono i compiti che un Proxy Server può svolgere?
- Quali sono le 3 categorie principali di Proxy Server?