

Network security

Sicurezza informatica

v 2.0.1 ~ mar 2021



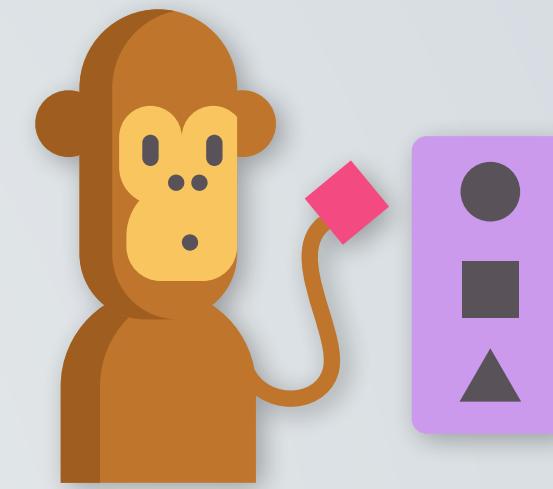
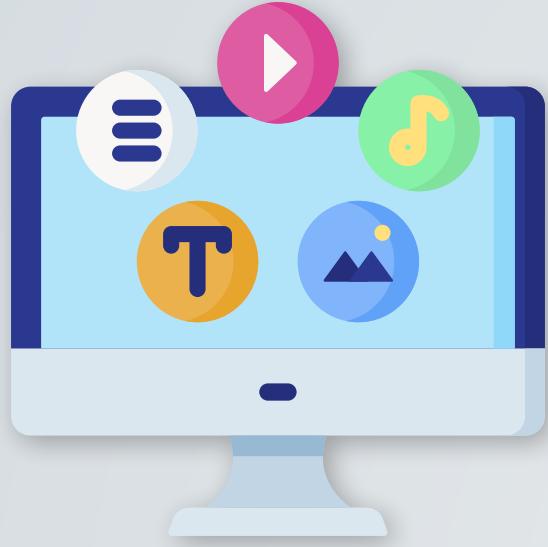
Prof. Marco Farina

marco.farina@its-ictpiemonte.it

t.me/marcofarina

in collaborazione con:

Considerazioni sulla web security



Complessità

I contenuti web sono straordinariamente complessi e possono nascondere problemi di sicurezza.

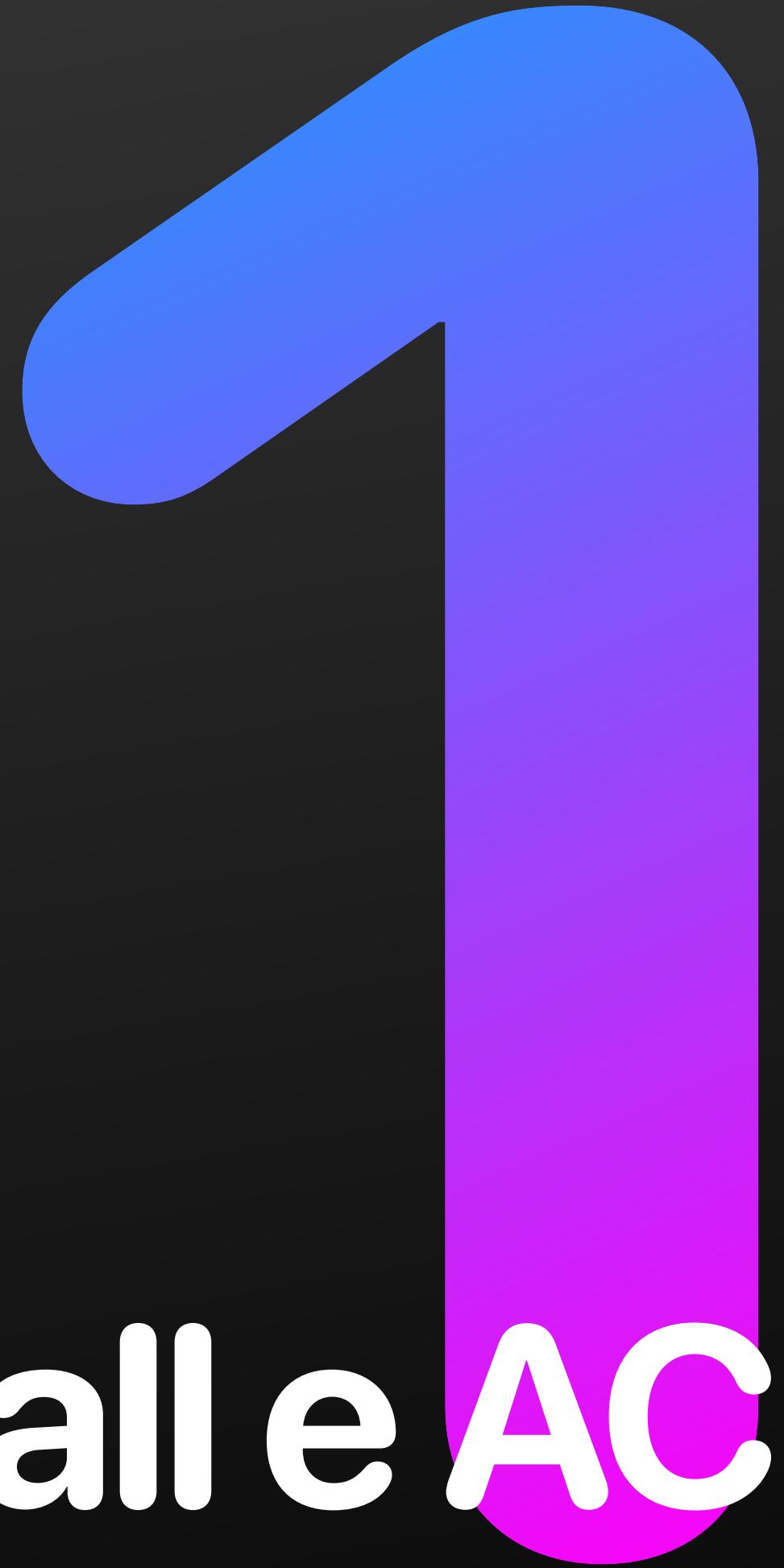
Escalation

I server web possono essere exploitati e usati come trampolino verso la rete aziendale interna.

Utonti

Gli utenti tipici dei servizi web non sono addestrati alle tematiche della security.

La sicurezza del web passa anche dalla difesa del network.



Firewall e ACL

Firewall: muro di fuoco?

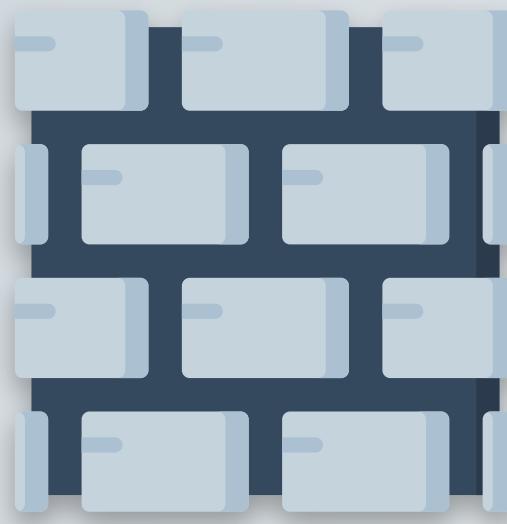


Non facciamo confusione:
"Muro di Fuoco" è un carta di
Magic: the Gathering™.

Il *firewall* è il muro o **porta tagliafuoco**. Il suo compito è isolare e compartmentare una struttura di rete.

Rappresenta la prima linea di difesa perimetrale della struttura di rete.

Cos'è un firewall?



È un componente della sicurezza perimetrale della rete avente lo scopo di controllare gli accessi alle risorse di un sistema filtrando tutto il traffico che tale sistema scambia con l'esterno.

Ma il firewall non è un software?



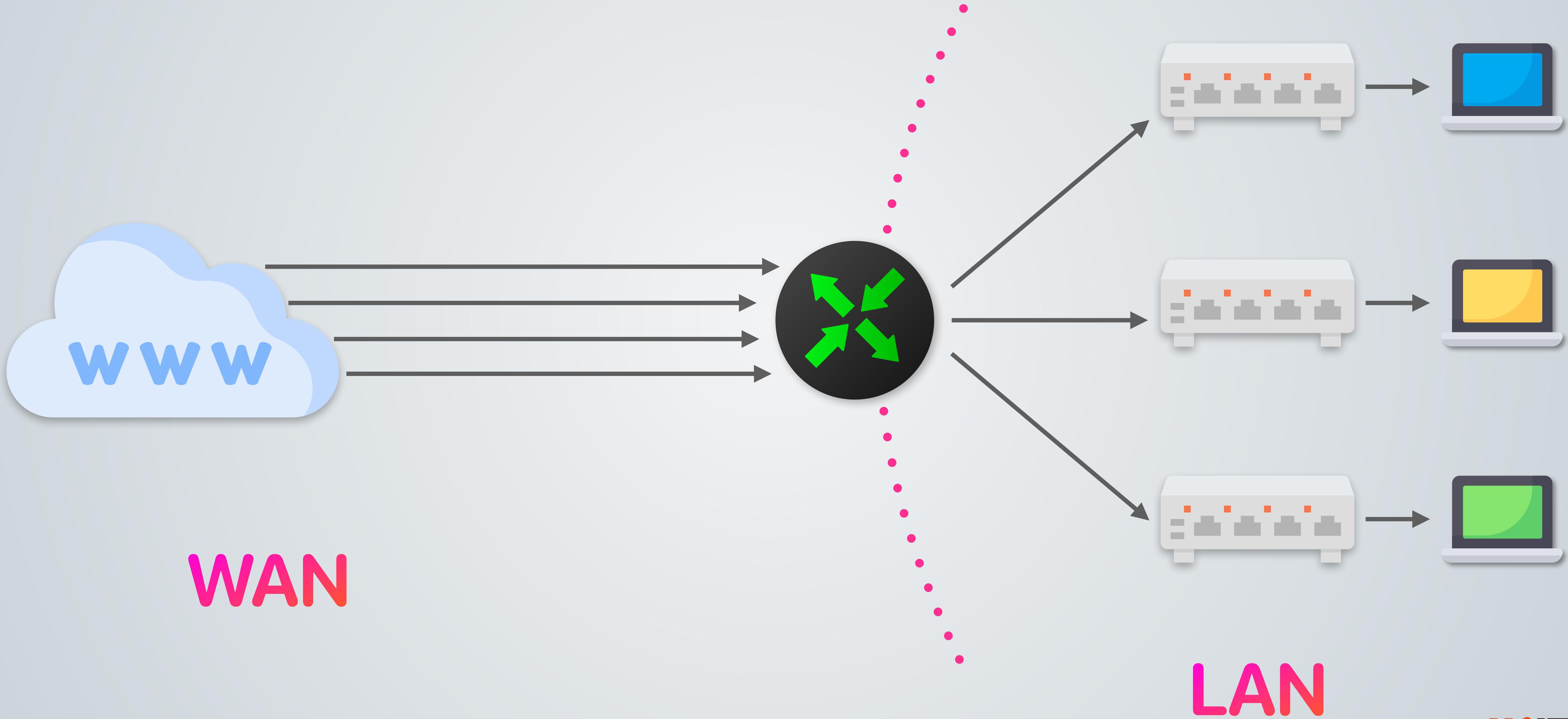
Pros:

- Economico / gratuito
- Facile da utilizzare
- Ottimi risultati
- Soluzione personale

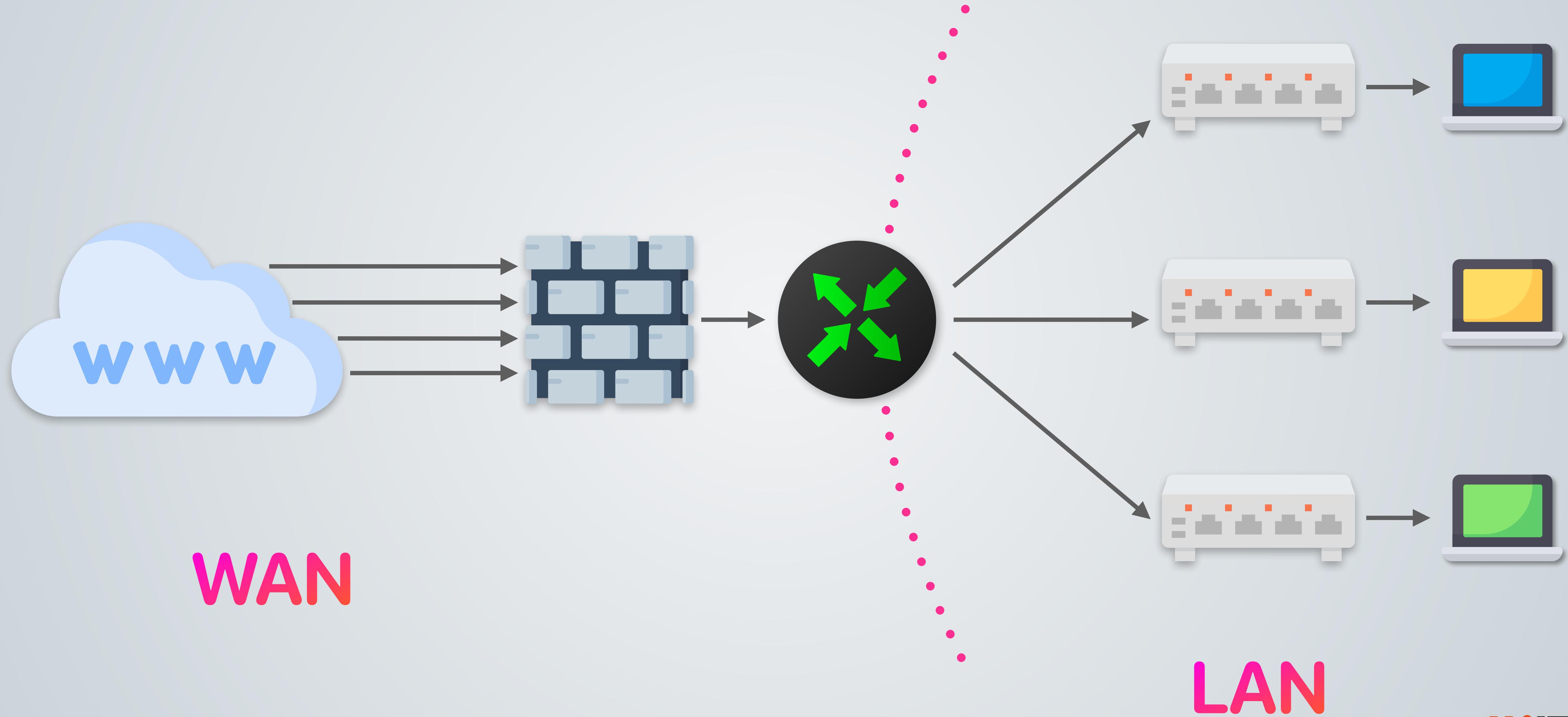
Cons:

- Non protegge la rete
- Troppo semplice
- Da aggiornare su ogni device
- Non adatto alle aziende

Network firewall

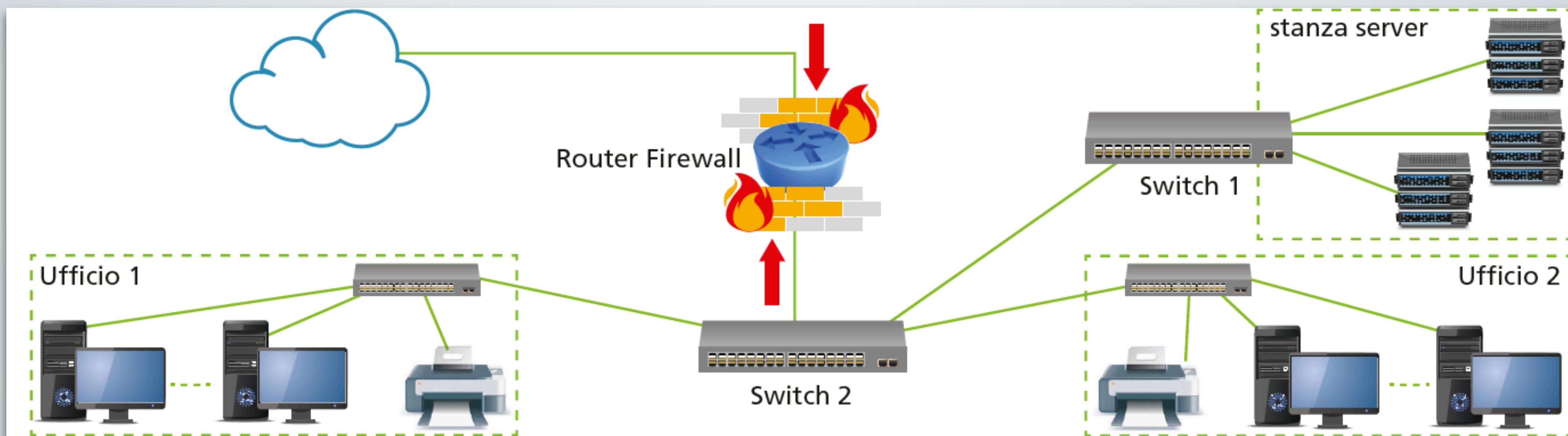


Network firewall



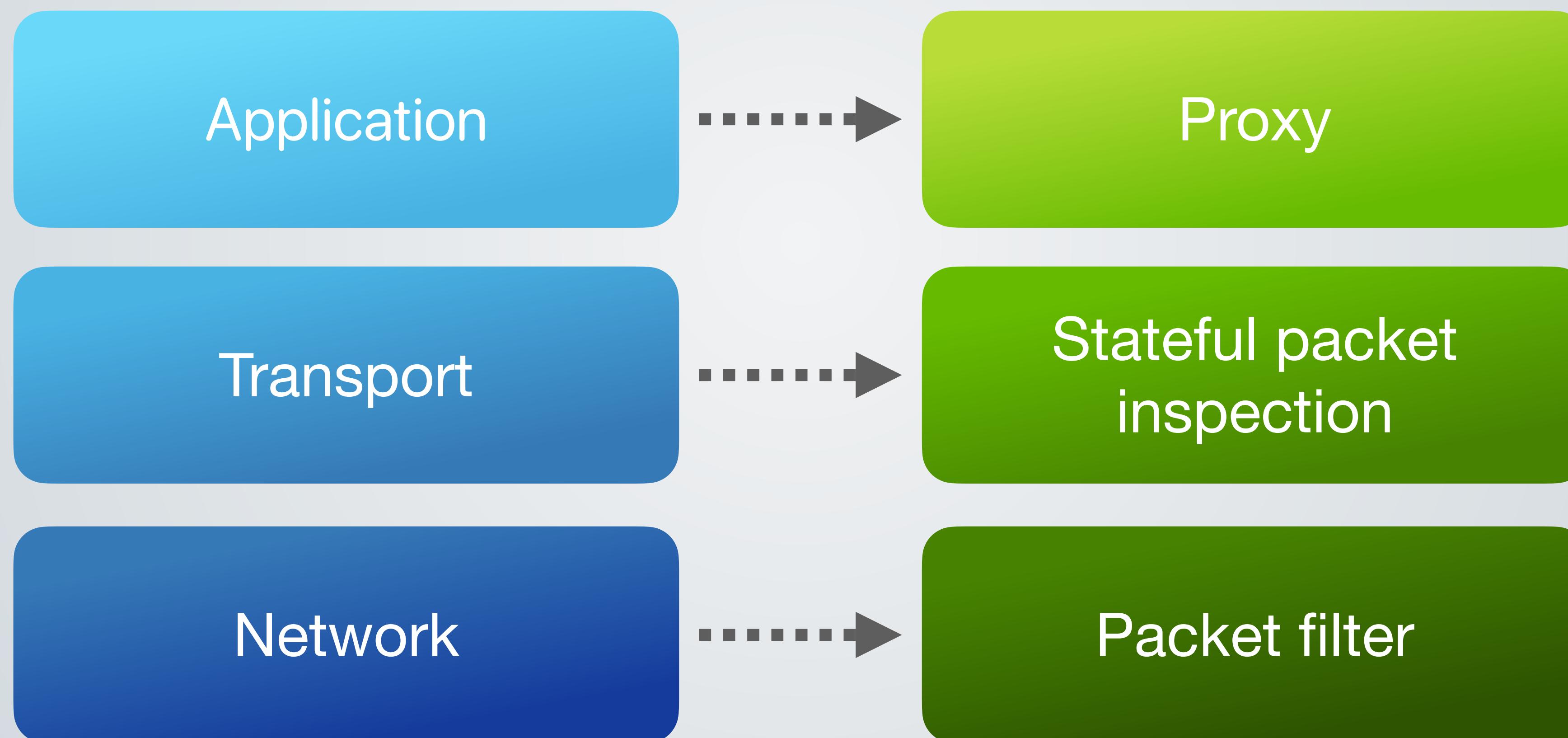
Network firewall

Il firewall filtra tutti i pacchetti entranti e uscenti attraverso regole prestabilite (*policy*) che contribuiscono alla sicurezza della rete stessa.



Firewall

I firewall si possono distinguere in **tre categorie** in base al livello dello stack TCP/IP cui operano:



Packet filter router

- Lavora a **livello network** e filtra a seconda degli header (network e transport): sorgente e destinazione (IP e MAC), numero di porta, protocollo a livello superiore.
- Decide se accettare o meno i pacchetti tramite un algoritmo di scelta basato su regole applicate in ordine di priorità: le **Access Control List**.

Pros:

- Trasparenza per l'utente
- Velocità del controllo
- Immediatezza di configurazione
- Topologia interna mascherata

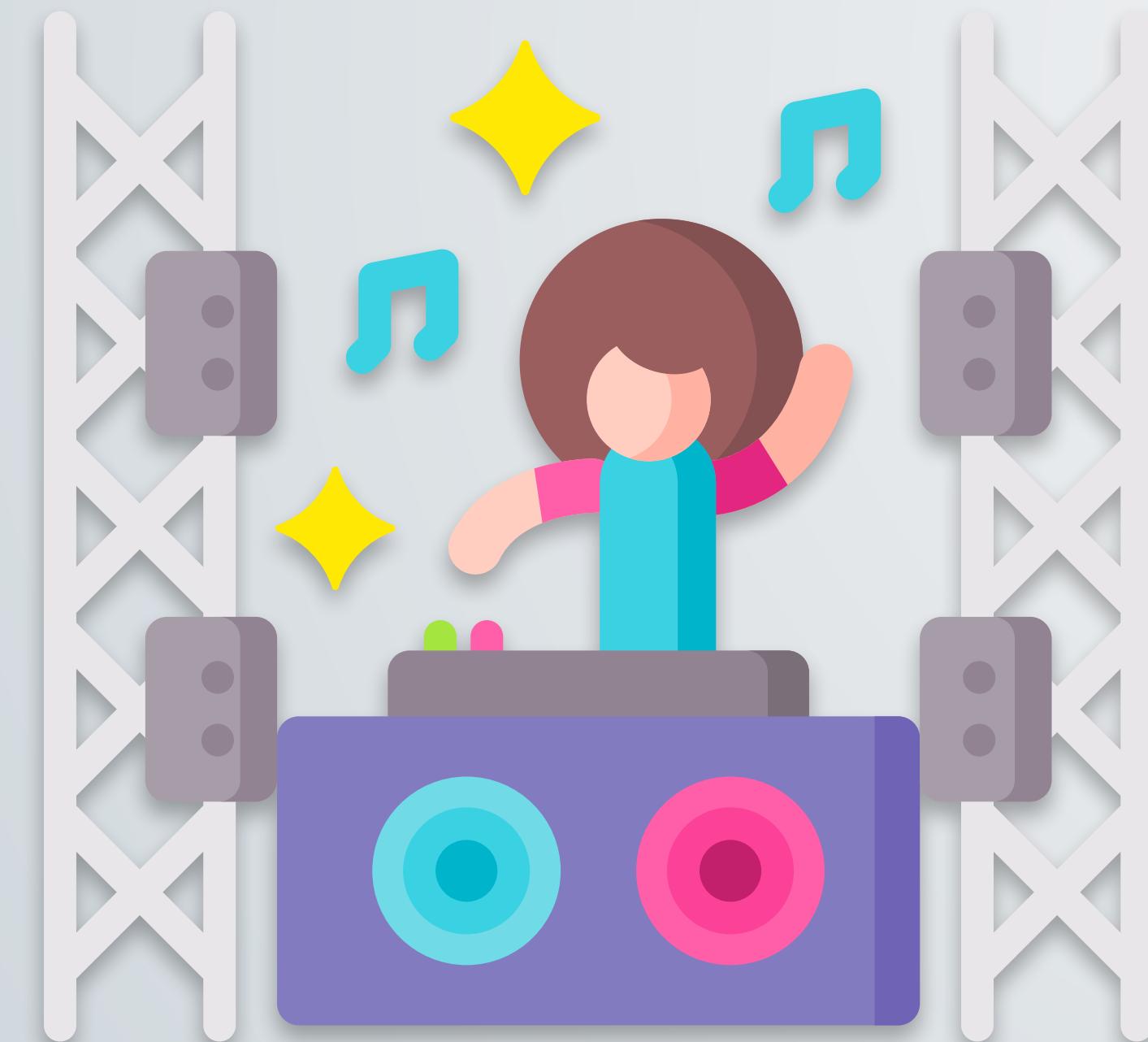
Cons:

- Lavora a basso livello
- Non permette servizi aggiuntivi
- Logging limitato
- Vulnerabile allo spoofing
- Testing molto complesso

Access Control List

Open policy

Tutto è permesso tranne ciò che sta nella lista dei divieti.



Closed policy

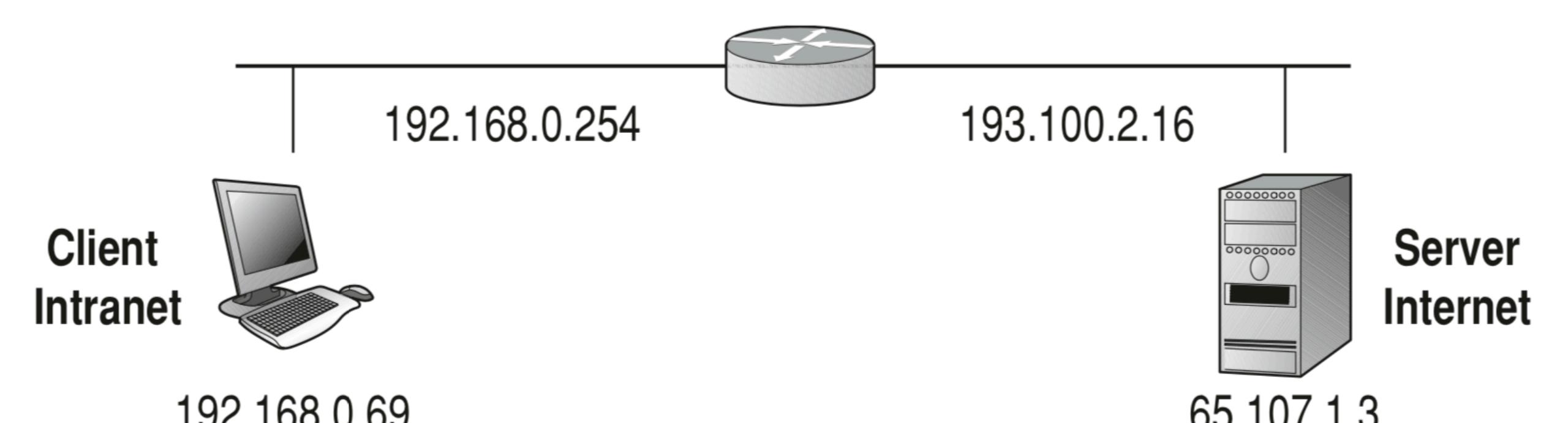
Tutto è vietato tranne ciò che sta nella lista dei permessi.



Access Control List

Le ACL possono essere scritte e modificate tramite configurazione esplicita dell'admin della rete.

Nr. Regola	Azione	Source Address	Source Port	Destination Address	Destination Port
1	allow	any	any /TCP	65.107.1.3	80/TCP
2	allow	65.107.1.3	80/TCP	localhost	any /TCP
3	reject	any	any	any	any



Access Control List: esempio

Per permettere soltanto il traffico sulla porta 80 e 443 le regole di filtraggio dovranno essere:

Nr. Regola	Azione (Rule)	Host Esterno	Porta	Host Interno	Porta	Descrizione
1	accept	any	any	localhost	80	traffico Web HTTP
2	accept	any	any	localhost	443	traffico Web HTTPS
3	deny	any	any	any	any	default

Stateful packet inspection

- Agisce a livello Transport: controlla lo stato della connessione TCP.
- Analizza header e contenuto.
- Compila una tabella di stato per ogni connessione in cui memorizza indirizzi IP, interfacce di rete e stato della connessione.

Pros:

- Buon rapporto prestazioni/sicurezza
- Protezione da IP spoofing e session hijacking
- Filtraggio dei singoli pacchetti

Cons:

- Protocollo unico (TCP)
- Auditing limitato
- Servizi offerti limitati
- Testing complicato

Application layer firewall

- Intercettazione a livello Application, valuta il contenuto dei pacchetti permettendo o bloccando il traffico in base alle policy.
- Riconosce comandi specifici delle applicazioni, offre un alto livello di protezione a scapito della velocità della rete.
- Sono tipicamente realizzati tramite **proxy server**.

Pros:

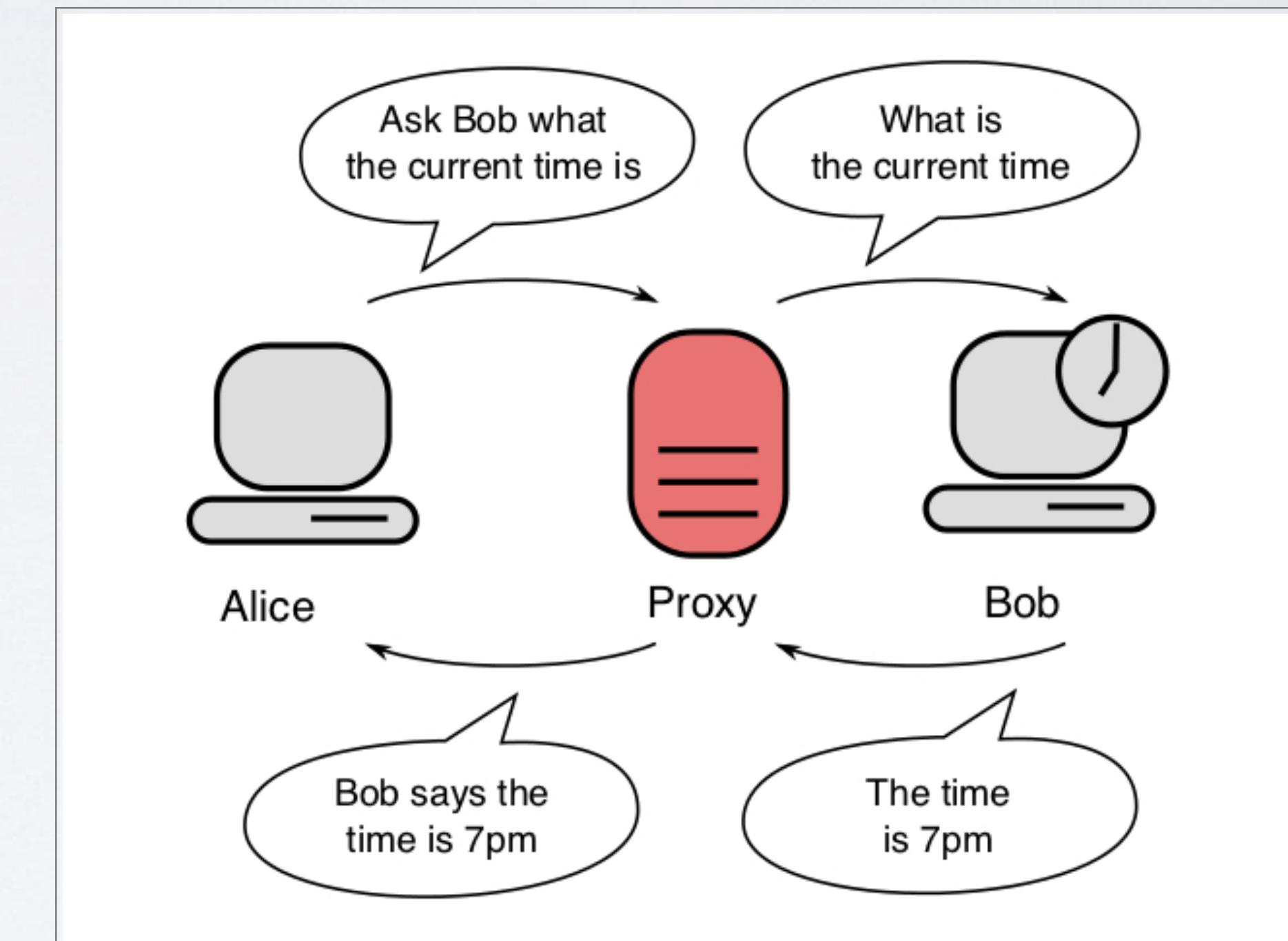
- Controllo completo
- Log dettagliati
- Sicurezza in caso di crash
- User-friendly
- Filtraggio dei contenuti
- Caching

Cons:

- Configurazione dei singoli host
- Un proxy per servizio
- Basse performance

Proxy Server

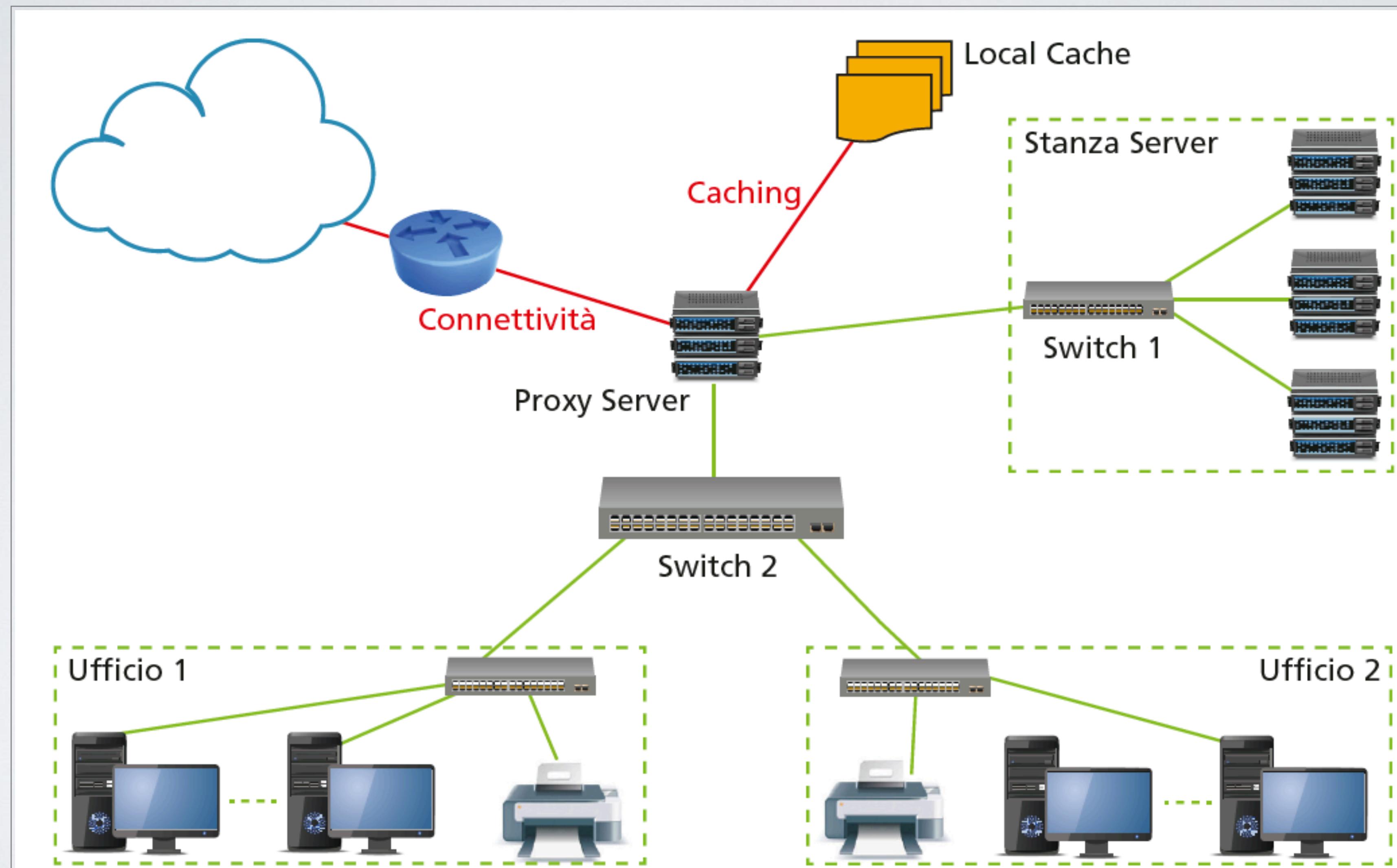
- Un proxy è un programma (in esecuzione su un semplice computer o su un apparato hardware) che si interpone tra un client e un server facendo da tramite.
- Lavorano a livello Application.
- Il compito principale è garantire connettività, caching e filtraggio ai client collegati ai fini dell'efficienza e del controllo della rete.



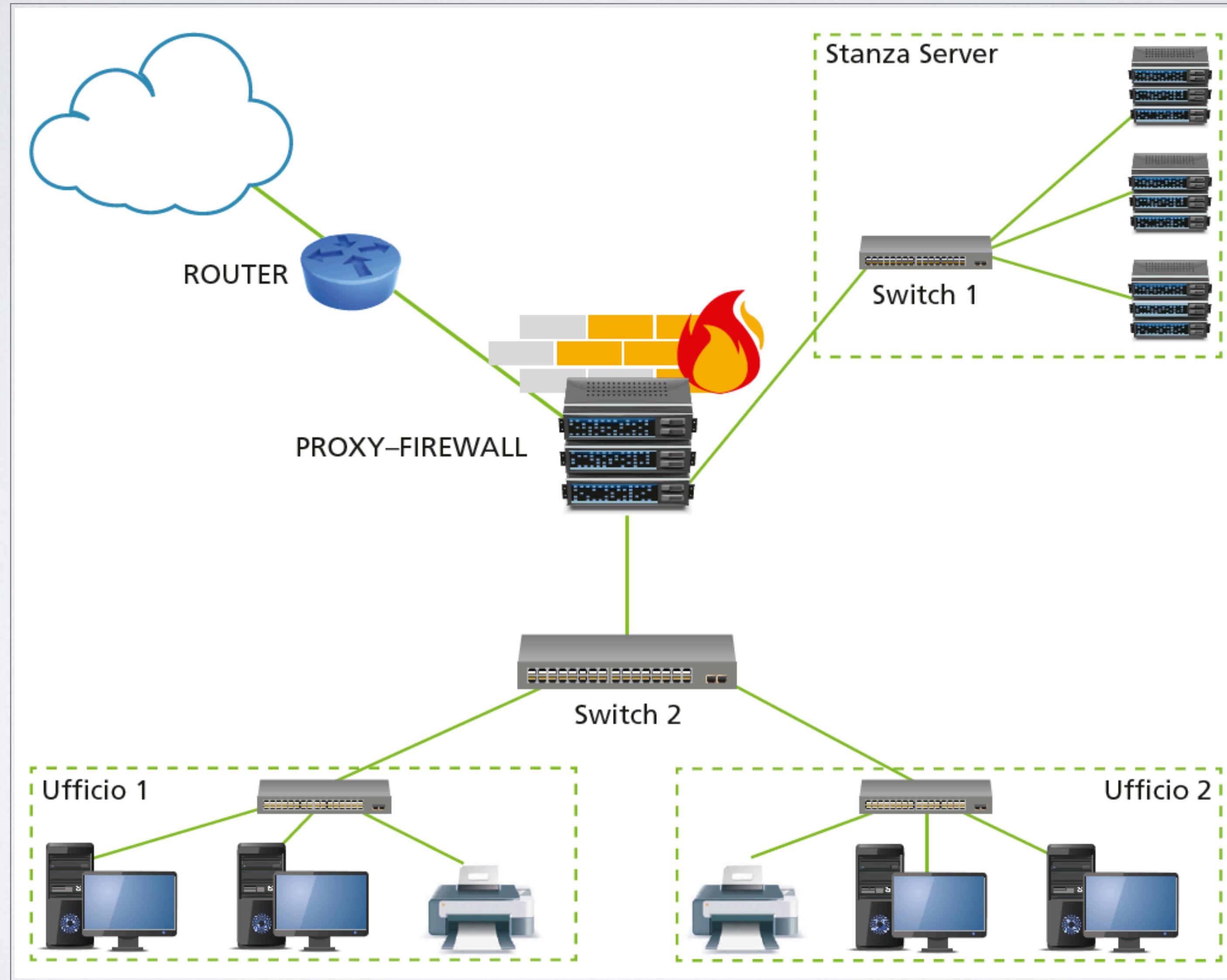


Sicurezza delle architetture web

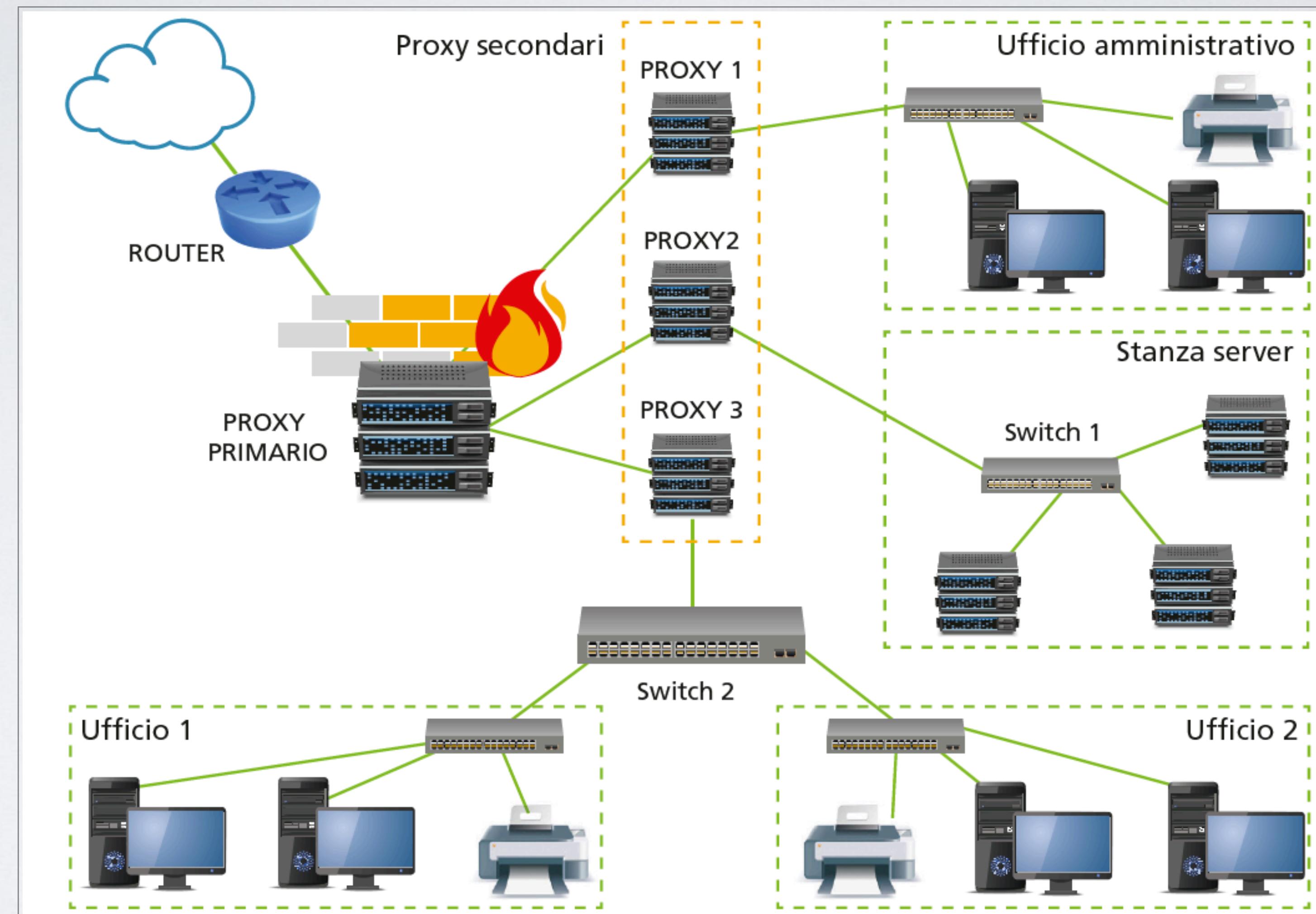
Proxy Server



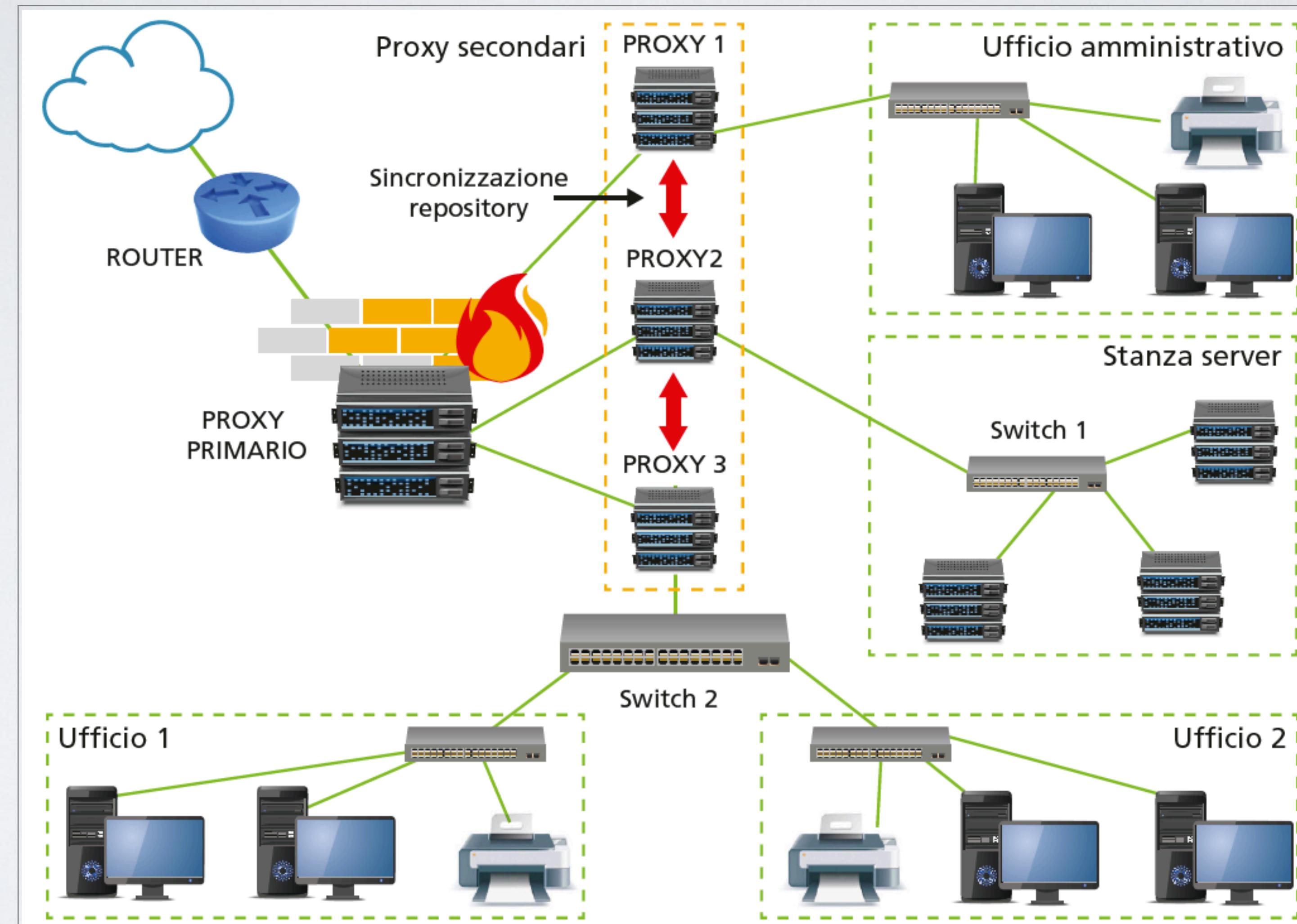
Single proxy topology



Multiple Proxy Vertically Topology



Multiple Proxy Horizontally Topology



Demilitarized Zone

Nei casi più semplici, le uniche due zone, LAN e WAN, sono sui due lati del firewall.

In molti casi, però, è necessaria la creazione di una terza zona, detta DMZ, Demilitarized Zone.

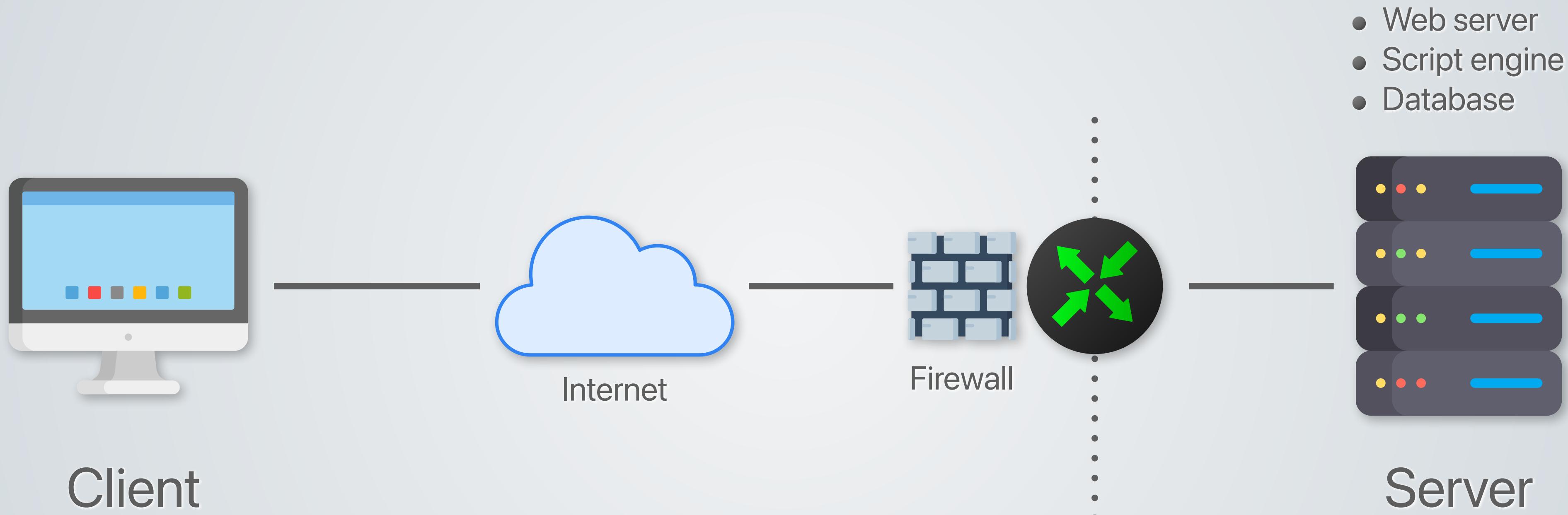
Si tratta di un'area in cui sia il traffico WAN sia quello LAN sono fortemente limitati e controllati.

Tale configurazione viene normalmente utilizzata per permettere ai server posizionati sulla DMZ di fornire servizi all'esterno senza compromettere la sicurezza della rete aziendale interna, per esempio:

- posta elettronica;
- Application Server.

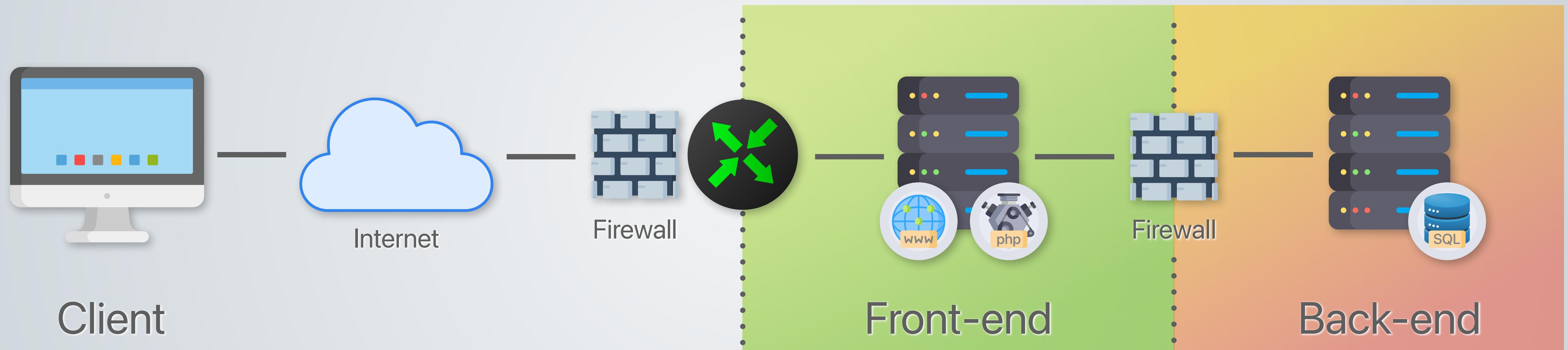
Le architetture web

2-tier



Le architetture web

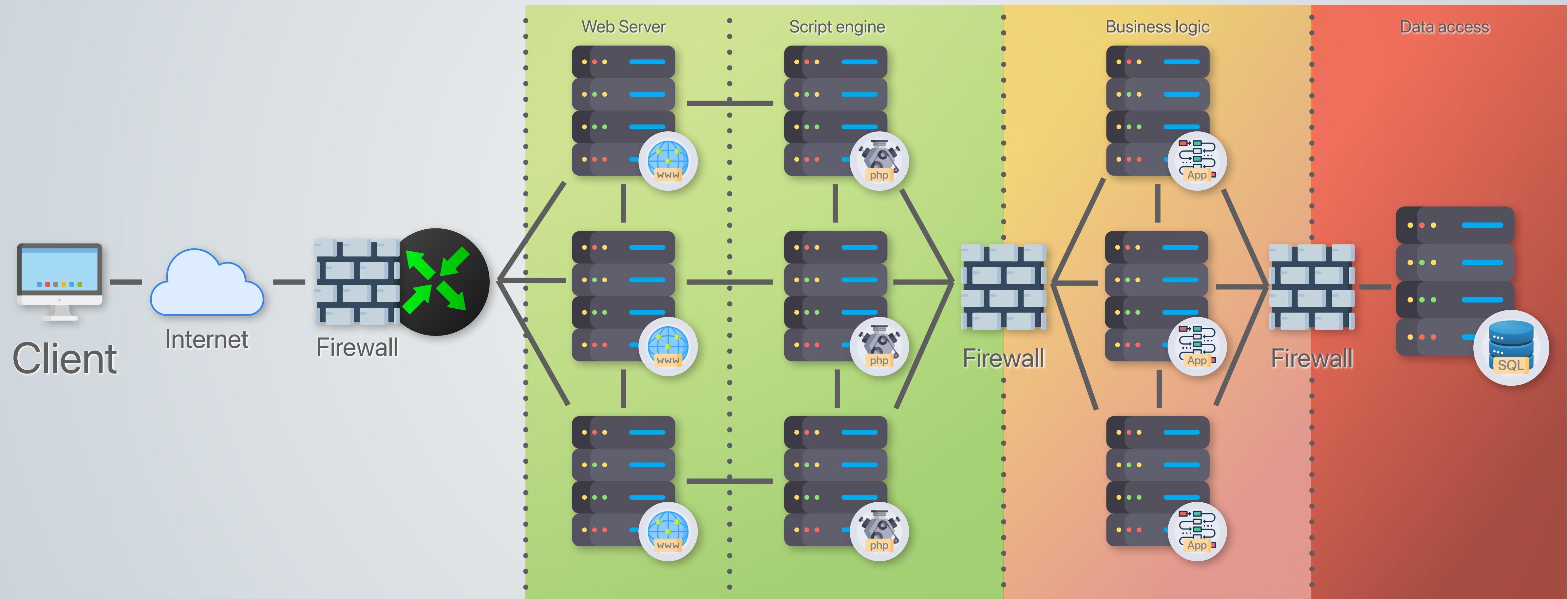
3-tier



Demilitarized Zone

Le architetture web

n-tier



Demilitarized Zone

Back-end