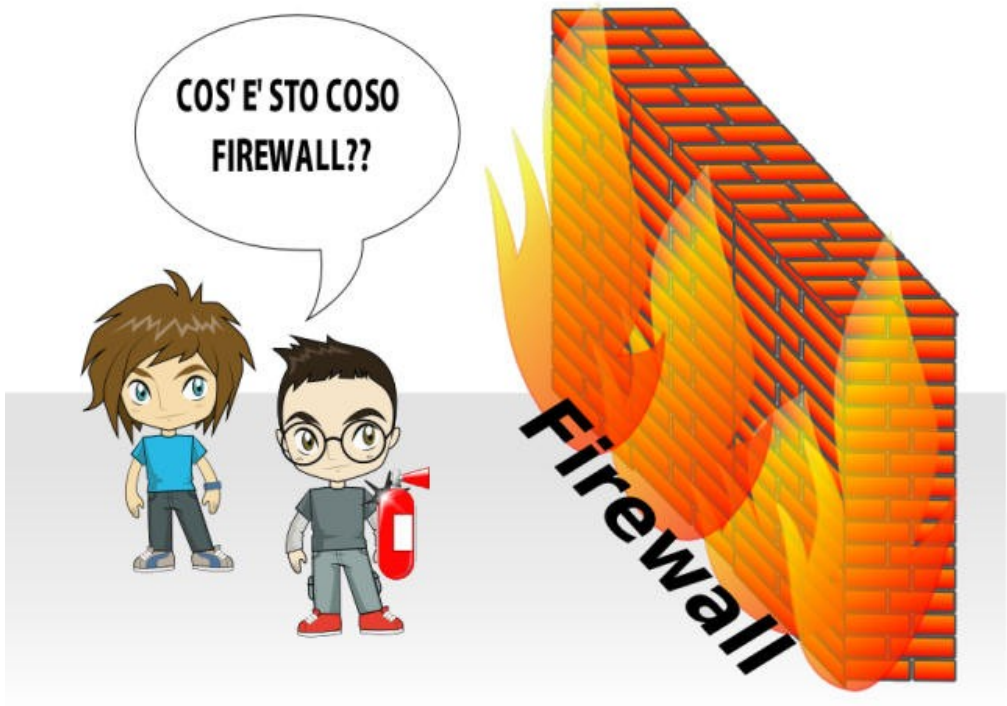
Filtraggio del traffico e protezione delle reti locali



Video

FIREWALL E ACL

Il **firewall** separa la LAN aziendale dalla WAN pubblica filtrando 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.

FIREWALL E ACL

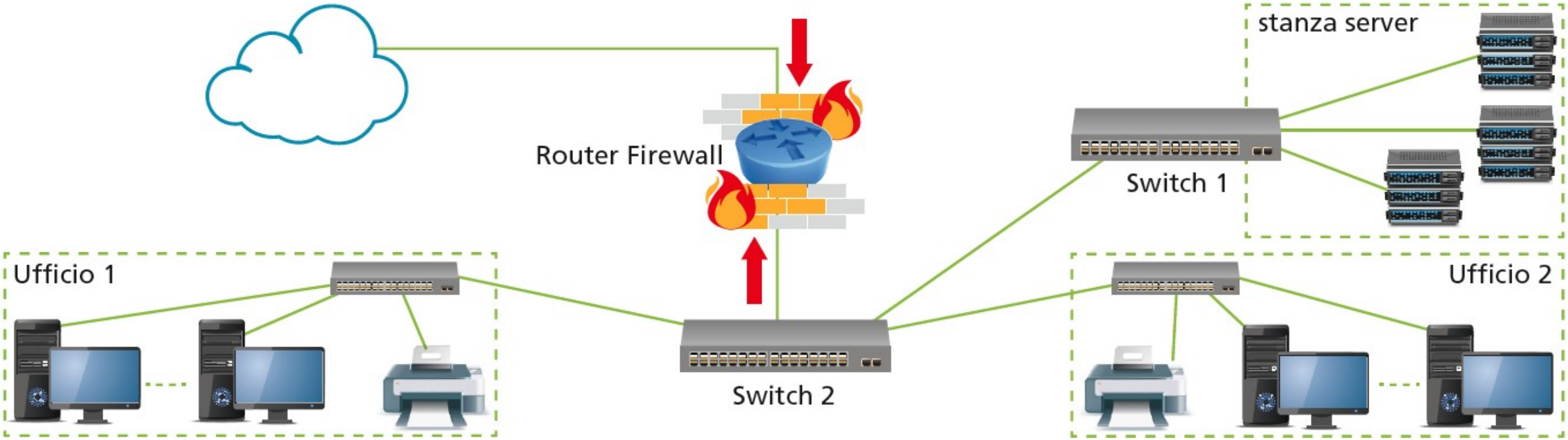
Un firewall può essere realizzato con un PC (con almeno due schede di rete, una per l'input e l'altra per l'output) ed il SW apposito.

Nelle LAN aziendali viene realizzato attraverso una funzionalità logica (**software**) inclusa nel **router** oppure può essere implementato su **hardware dedicato**.

FIREWALL E ACL

La sicurezza di tutta la rete aziendale connessa ad Internet viene ricondotta quindi alla **sicurezza di un ristrettissimo numero di nodi**, molto spesso uno. Solo il nodo in questione, costituito dal firewall appunto, 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 della rete, e delle uscite, per bloccare richieste contrarie alla policy aziendale.

FIREWALL E ACL



Video

FIREWALL E ACL

Nel caso di un'azienda, non disporre di un firewall significa essere esposti a numerosi attacchi e tentativi di intrusione che potrebbero portare alla perdita di dati con considerevoli danni soprattutto in termini di costi e affidabilità.

#prendinota

Esistono anche i cosiddetti firewall personali, cioè programmi installati sui normali elaboratori client, che filtrano solamente i pacchetti che entrano ed escono da quel computer.

FIREWALL E ACL

Caratteristiche principali di un Firewall:

- Strumento efficace per la sicurezza delle reti;
- Presenza di meccanismi per il controllo degli accessi;
- Possibilità di gestire le regole per la sicurezza;
- Configurazione di filtri per l'accesso dei programmi e dei computer di una rete ad Internet;
- Protezione da attacchi di tipo ARP spoofing, port scanning, DoS, SQL slammer, ecc...

FIREWALL E ACL

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

- **Application Level Firewall**;
- **Packet Filter Firewall**;
- **Stateful Packet Inspection Firewall**.

FIREWALL E ACL

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.

FIREWALL E ACL

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).

FIREWALL E ACL

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.

FIREWALL E ACL

La sintassi della configurazione di un firewall è basata su un meccanismo di lista di controllo degli accessi **ACL** (**Access Control List**).

#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.

FIREWALL E ACL

Le ACL permettono di esprimere delle **regole** che determinano l'accesso o meno ad alcune risorse di un sistema informatico da parte dei suoi utenti. Possono essere modificabili tramite configurazione esplicita da parte dell'**amministratore** di sistema o possono variare in base allo stato interno del sistema.

FIREWALL E ACL

Esistono varie **ragioni** per decidere di adoperare le **ACL**:

- Fornire un **livello base di sicurezza**: si possono ad esempio restringere gli accessi ad 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.

FIREWALL E ACL

L'**ordine** con cui le ACL sono scritte è importante poiché esse vengono elaborate dal router-firewall in maniera **sequenziale**: è necessario inserire le condizioni più restrittive all'inizio.

Appena un pacchetto soddisfa una delle condizioni, la valutazione si interrompe ed il resto delle ACL non viene considerato. Il pacchetto viene quindi inoltrato o scartato a seconda dell'istruzione eseguita. Se il pacchetto non soddisfa nessuna delle condizioni viene scartato (l'ultima ACL contiene generalmente l'istruzione ***deny all***)

FIREWALL E ACL

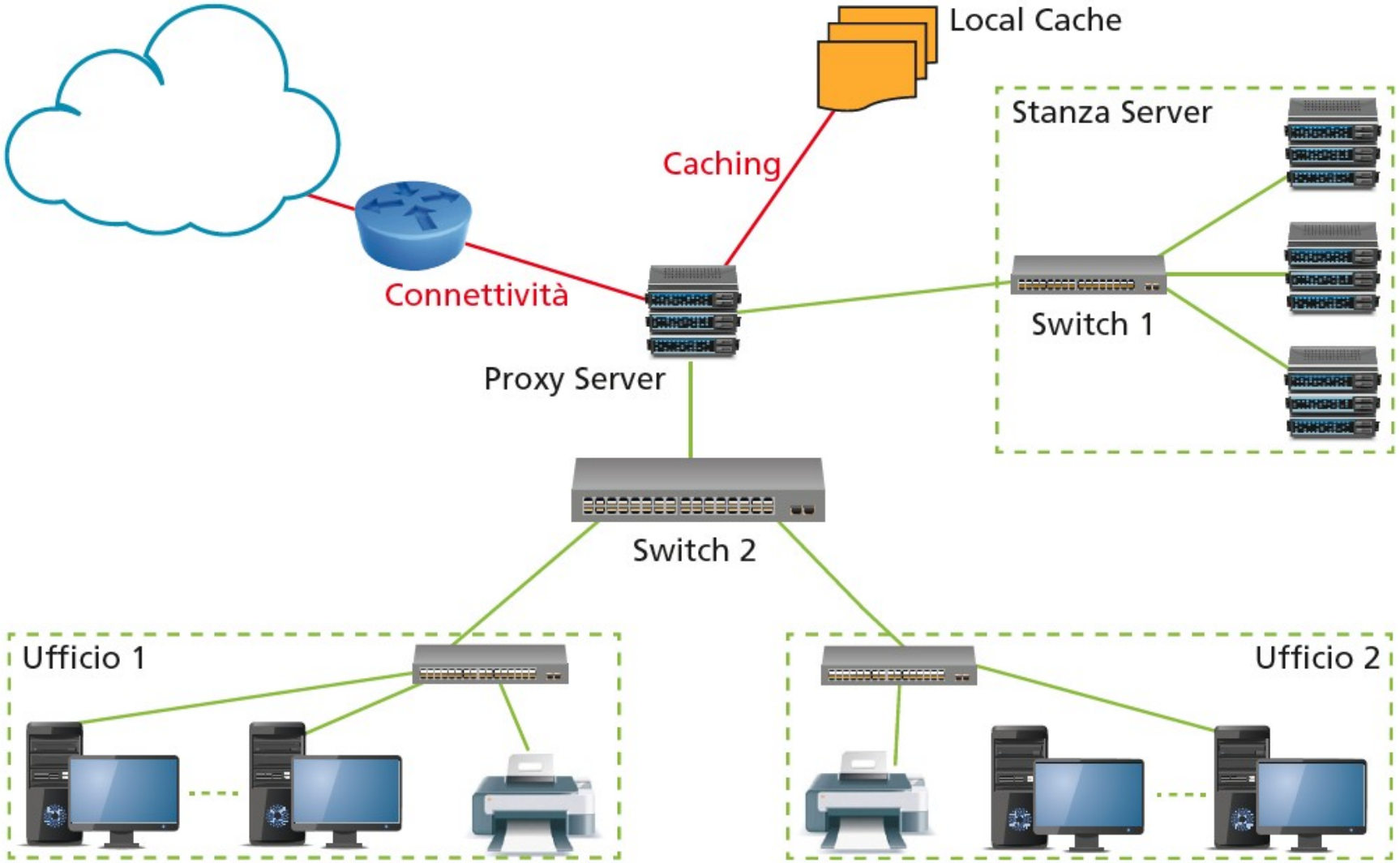
Possiamo avere 2 tipologie di ACL:

- **Standard ACL**: specificano delle limitazioni ai pacchetti guardando esclusivamente l'indirizzo della sorgente e vanno posizionate sull'interfaccia del router il più possibile vicino alla destinazione;
- **Extended ACL**: pongono limitazioni ai pacchetti in base a molte specifiche (protocollo, indirizzo sorgente, indirizzo destinazione, numero di porta).

PROXY SERVER

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

PROXY SERVER



PROXY SERVER

Compiti che possono essere svolti da un Proxy Server:

- **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 Lezione 3 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, può 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;

PROXY SERVER

Compiti che possono essere svolti da un Proxy Server:

- **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).

PROXY SERVER

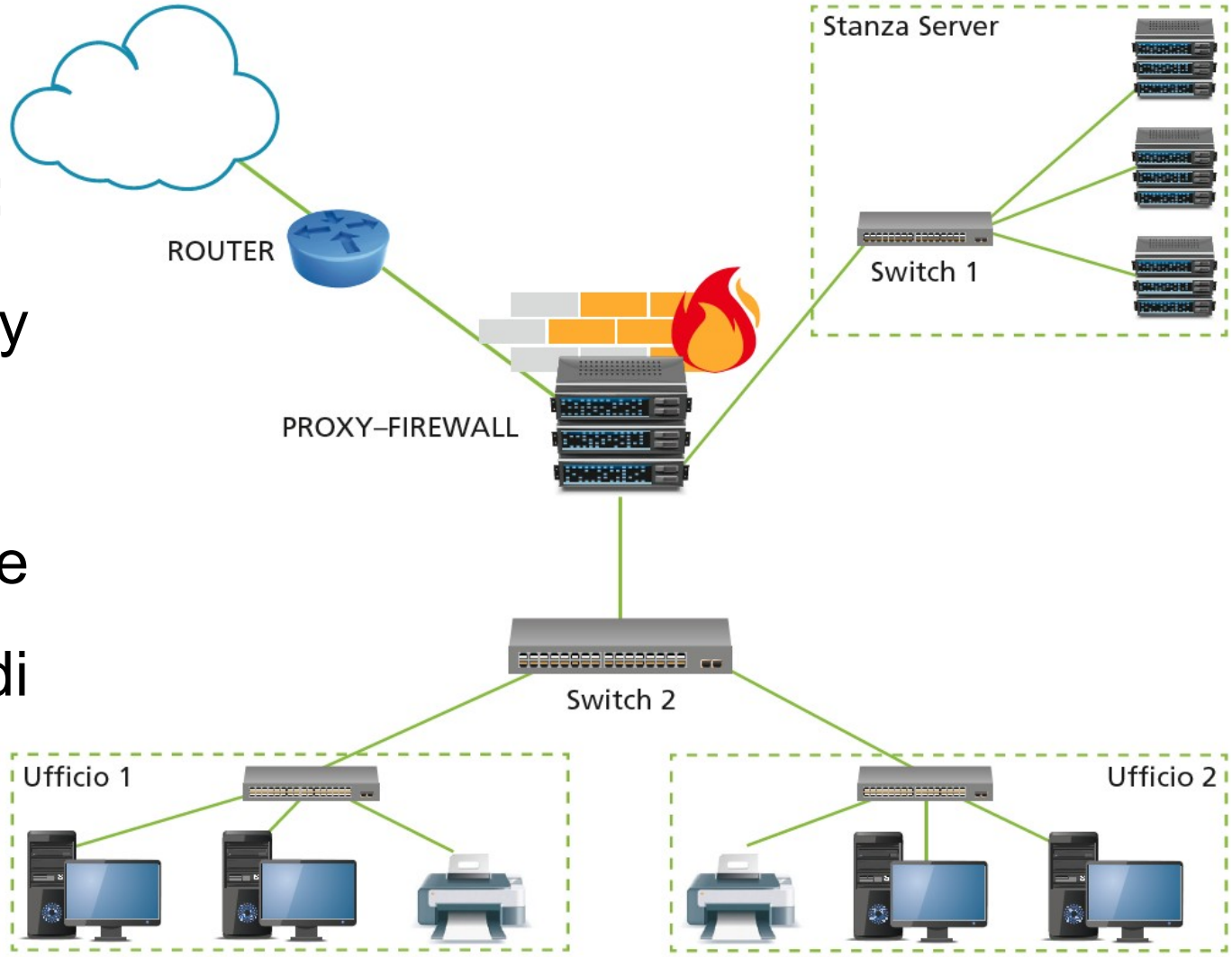
I Proxy Server, in particolare quelli che incorporano funzioni di firewall, possono essere diversamente collocati in base alle esigenze dell'azienda. In generale, si possono individuare 3 categorie di utilizzo prevalenti:

- **Single Proxy Topology**
- **Multiple Proxy Vertically Topology**
- **Multiple Proxy Horizontally Topology**

PROXY SERVER

Single Proxy Topology:

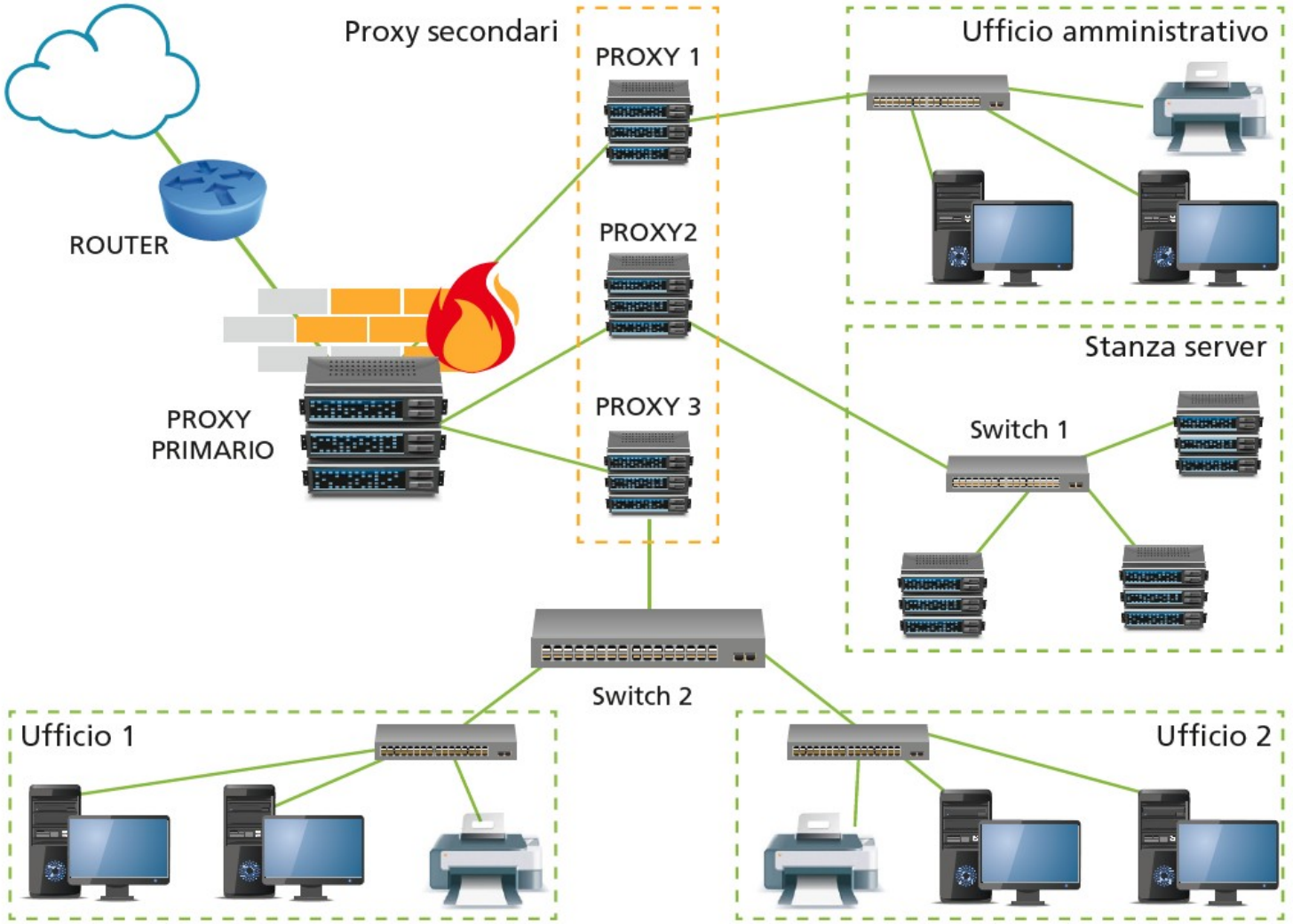
- Utilizza un singolo Proxy Server per l'intera rete;
- Configurazione sufficiente per un piccolo gruppo di client.



PROXY SERVER

Multiple Proxy Vertically Topology:

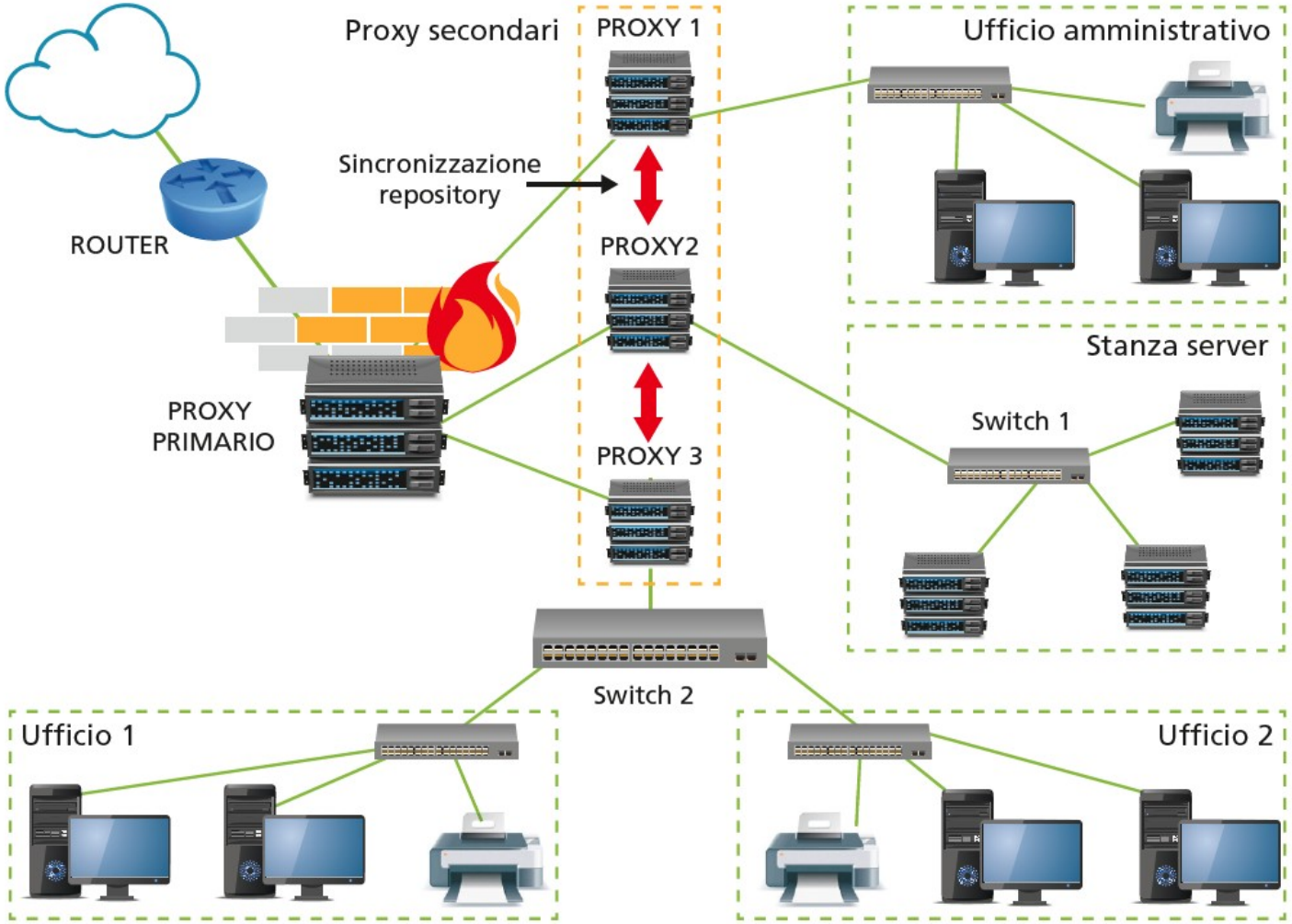
- Reti medio-grandi;
- Più Proxy secondari (ad esempio uno per ogni subnet) dipendenti da un Proxy Primario;
- I client possono avere il filtraggio dei pacchetti personalizzato.



PROXY SERVER

Multiple Proxy Horizontally Topology:

- Consente di bilanciare il carico tra i server in base alle richieste dei client;
- I server secondari sono di pari livello;
- Necessità di sincronizzazione tra i repository dei proxy (SVANTAGGIO).



LE TECNICHE NAT E PAT

NAT (**Network Address Translation**) è una tecnica attuata dal router che, nell'intestazione di un pachetto IP, sostituisce un indirizzo (sorgente o destinazione), con un altro indirizzo. Tale tecnica permette a una rete locale, con classe di indirizzi privata, di accedere ad Internet usando un solo IP fornito dall'ISP.

NAT usa una **tabella** contenente la corrispondenza tra i socket interni ed esterni in uso. Il **socket** è l'insieme di protocollo, indirizzo IP e porta di comunicazione.

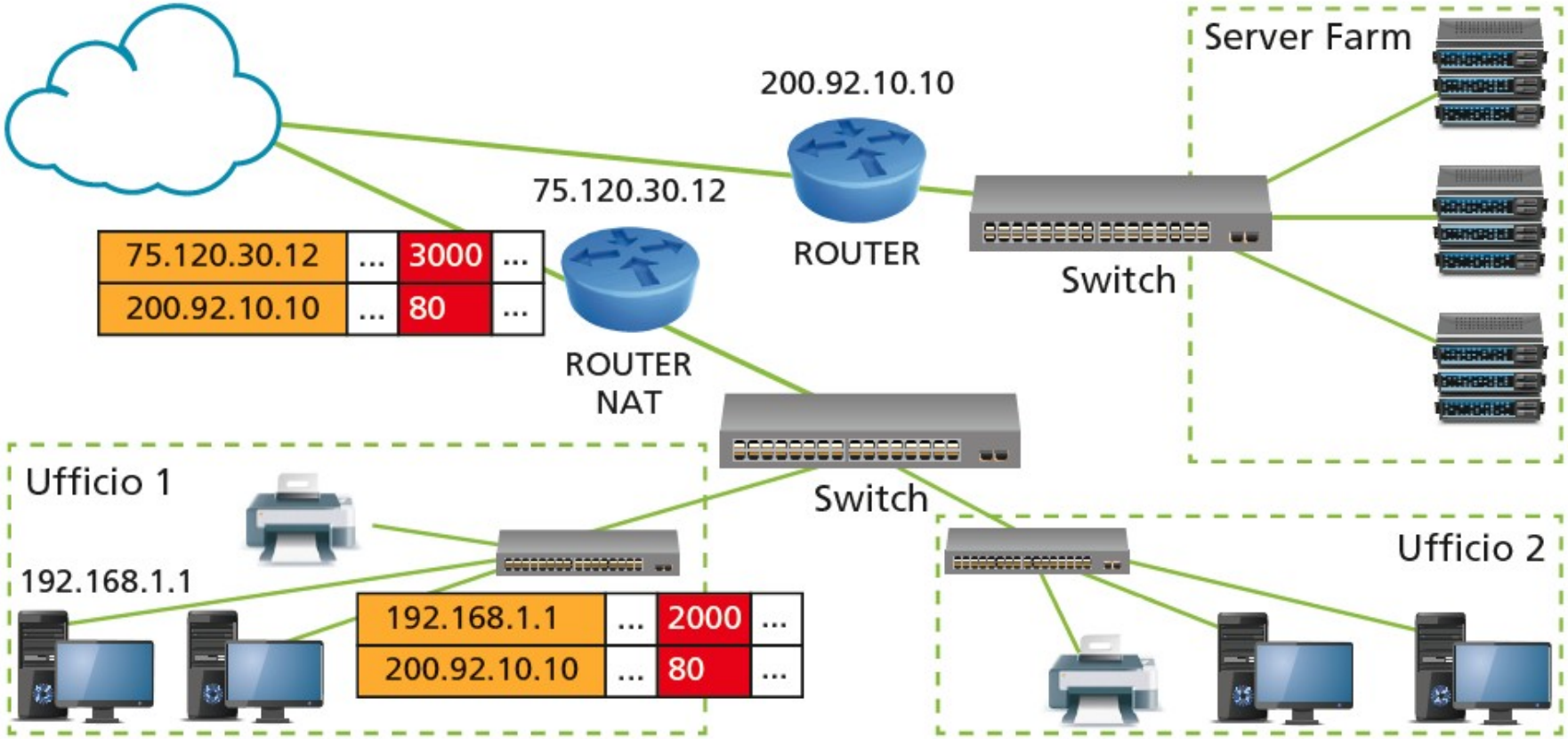
LE TECNICHE NAT E PAT

Quando un client richiede una pagina web ad un server esterno, il suo indirizzo e la sua porta di origine vengono traslati e la corrispondenza viene registrata nella tabella. Quando arriva la risposta dal server esterno, la tabella permette di capire chi voleva quei dati, quindi effettua la traslazione inversa e manda i pacchetti al client richiedente. Tutte le comunicazioni provenienti dall'esterno che non sono state registrate nella tabella, vengono eliminate.

LE TECNICHE NAT E PAT

Router con funzionalità NAT:

rapporto 1:1 tra IP server destinazione e IP client.



LE TECNICHE NAT E PAT

La funzione NAT presenta diversi vantaggi:

- limita il numero di indirizzi IP pubblici necessari per collegare una LAN a Internet;
- mantiene inalterata la configurazione degli host;
- non modifica il funzionamento dei protocolli e delle applicazioni della rete intranet;
- offre una flessibilità elevata grazie allo spazio molto esteso per gli indirizzi privati;
- riduce i costi di accesso a Internet (gli indirizzi pubblici sono concessi a pagamento);
- garantisce maggior sicurezza per i computer della rete locale (dall'esterno non si conosce l'indirizzo IP privato di un host).

LE TECNICHE NAT E PAT

Il NAT presenta 3 funzionalità:

- **Static NAT (**usa un solo indirizzo IP pubblico);
- **Dynamic NAT** (usa un insieme di indirizzi IP pubblici tra cui scegliere);
- **Port Address Translation o PAT** (traduce in modo dinamico l'indirizzo delle porte).

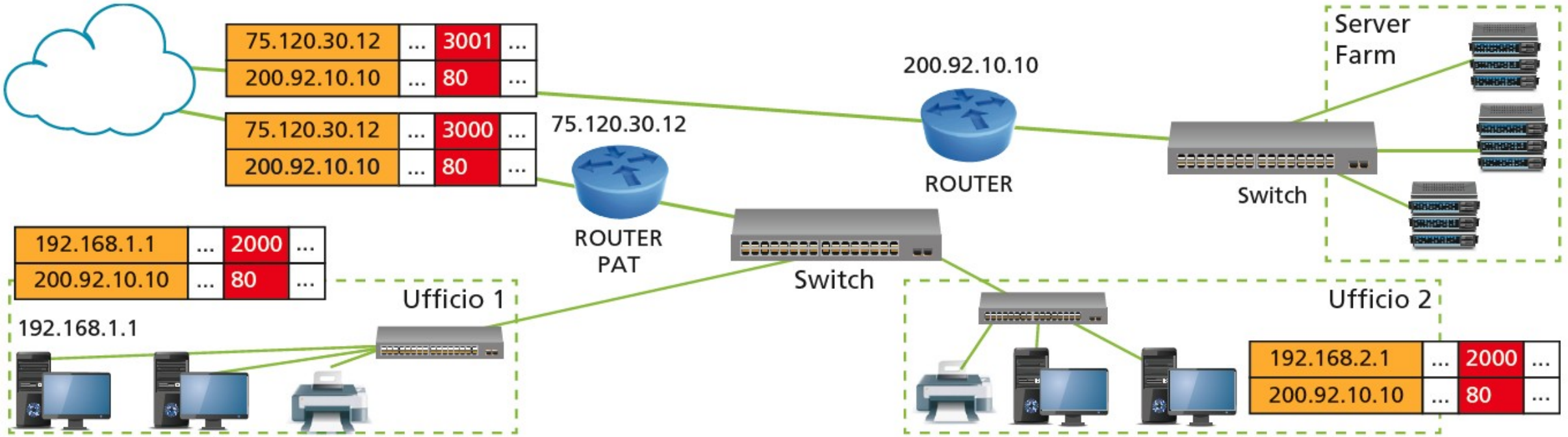
LE TECNICHE NAT E PAT

La tecnica **PAT** (**Port Address Translation)** consente al router di utilizzare un singolo indirizzo IP per gestire oltre 64000 connessioni private contemporaneamente (per la precisione 2^16 = 65536 porte diverse indirizzabili).

Questo vuol dire che può traslare più indirizzi IP client per un medesimo indirizzo IP destinazione cambiando solo la porta.

LE TECNICHE NAT E PAT

Router con funzionalità PAT: rapporto 1:N tra IP server Destinazione e IP client.



NAT per IPv6

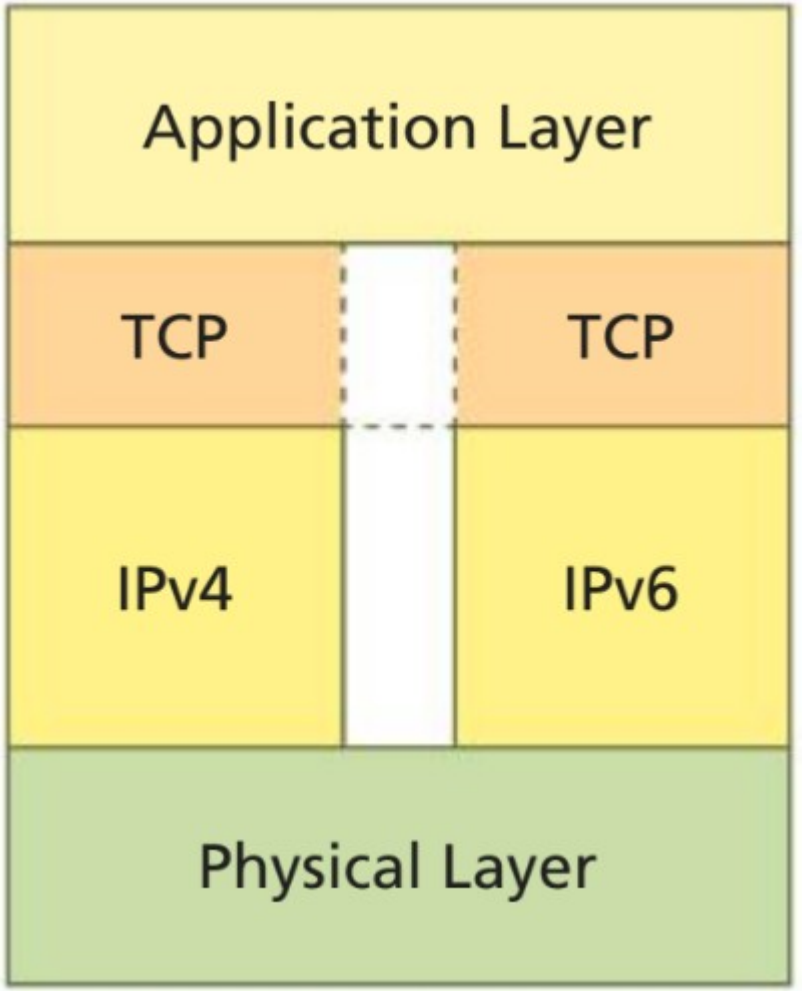
Anche IPv6 implementa una forma di NAT per mettere in comunicazione reti IPv6 con reti IPv4.

Per la fase di transizione da IPv4 a IPv6, IETF ha ipotizzato 3 meccanismi di possibile convivenza:

- **dual-stack**
- **conversion**
- **tunneling per IPv6**

NAT per IPv6: dual-stack

La tecnica **dual-stack** prevede l'utilizzo del doppio stack IP nella pila di protocolli TCP/IP. Questo doppio stack permette di interpretare entrambe le versioni del protocollo IP e quindi di smistare ai livelli superiori il contenuto del pacchetto senza che questi sappiano da quale protocollo IP derivi.



NAT per IPv6: dual-stack

Vantaggi: Semplicità di implementazione.

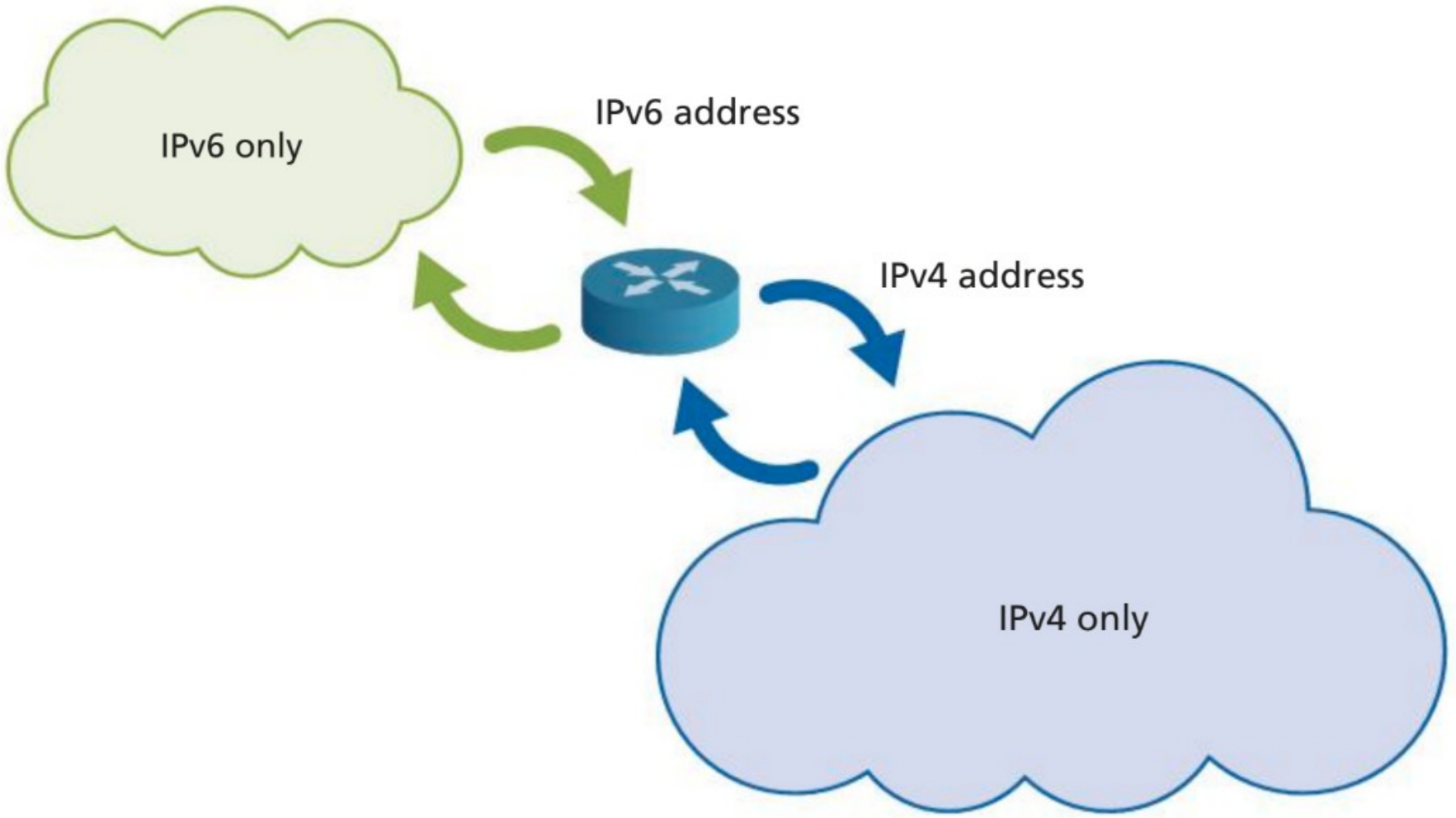
Svantaggi:

- Aumento della complessità della rete (router e switch multiprotocollo);
- Non risolve il problema della scarsità degli indirizzi IP (un'interfaccia deve comunque avere sia l'IPv4 che l'IPv6);
- Routing più lento (entrambi gli IP devono essere annunciati).

NAT per IPv6: conversion

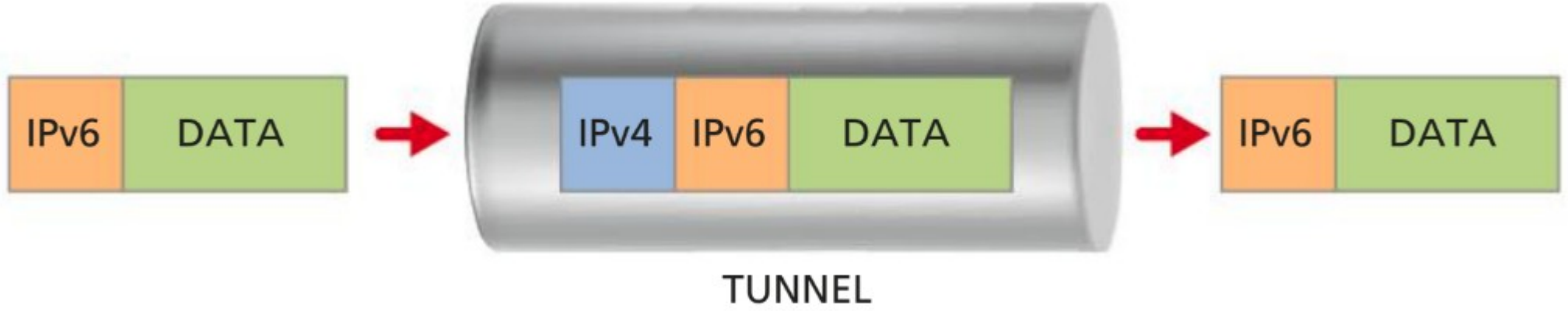
- Il meccanismo della **conversion** è considerato il NAT per IPv6.
- È realizzato con il protocollo **NAT-PT** (Network Address Translation – Protocol Translator) che effettua la conversione dell'indirizzo IPv6 in indirizzo IPv4 e viceversa secondo le tecniche di un NAT IPv4.
- NAT-PT consente la comunicazione diretta tra reti solo IPv6 e reti IPv4.

NAT per IPv6: conversion



NAT per IPv6: tunneling 4to6

Il **tunneling** per IPv6 incapsula un pacchetto IPv6 in un pacchetto IPv4, permettendone il trasporto in reti IPv4.



LA DEMILITARIZED ZONE (DMZ)

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

In molti casi, però, si rende 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.

LA DEMILITARIZED ZONE (DMZ)

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**.

LESSICO

Il **front-end** è la parte di un servizio (per esempio un sito web) visibile agli utenti. Rappresenta quindi l'interfaccia grafica con cui l'utente interagisce con l'azienda (lato client). Il **back-end** è il dietro le quinte, cioè la parte che gli utenti non vedono ma che garantisce la risposta del servizio alle richieste arrivate (lato server).

LA DEMILITARIZED ZONE (DMZ)

Generalmente in DMZ si installano i server detti **front-end**, a cui corrispondono i relativi **back-end** in LAN. In genere un server di front-end comunica solo con il suo back-end, e solo con le porte TCP e/o UDP strettamente necessarie.
Nel malaugurato caso in cui un servizio in LAN sia compromesso in seguito a una vulnerabilità, l'aggressore potrebbe raggiungere anche gli altri host della rete, dato che in LAN non esiste isolamento tra il server e gli altri nodi.

Se lo stesso problema si verificasse in DMZ, l'aggressore avrebbe grosse difficoltà a raggiungere la LAN, poiché il traffico tra i server front-end e back-end è fortemente limitato dal firewall.

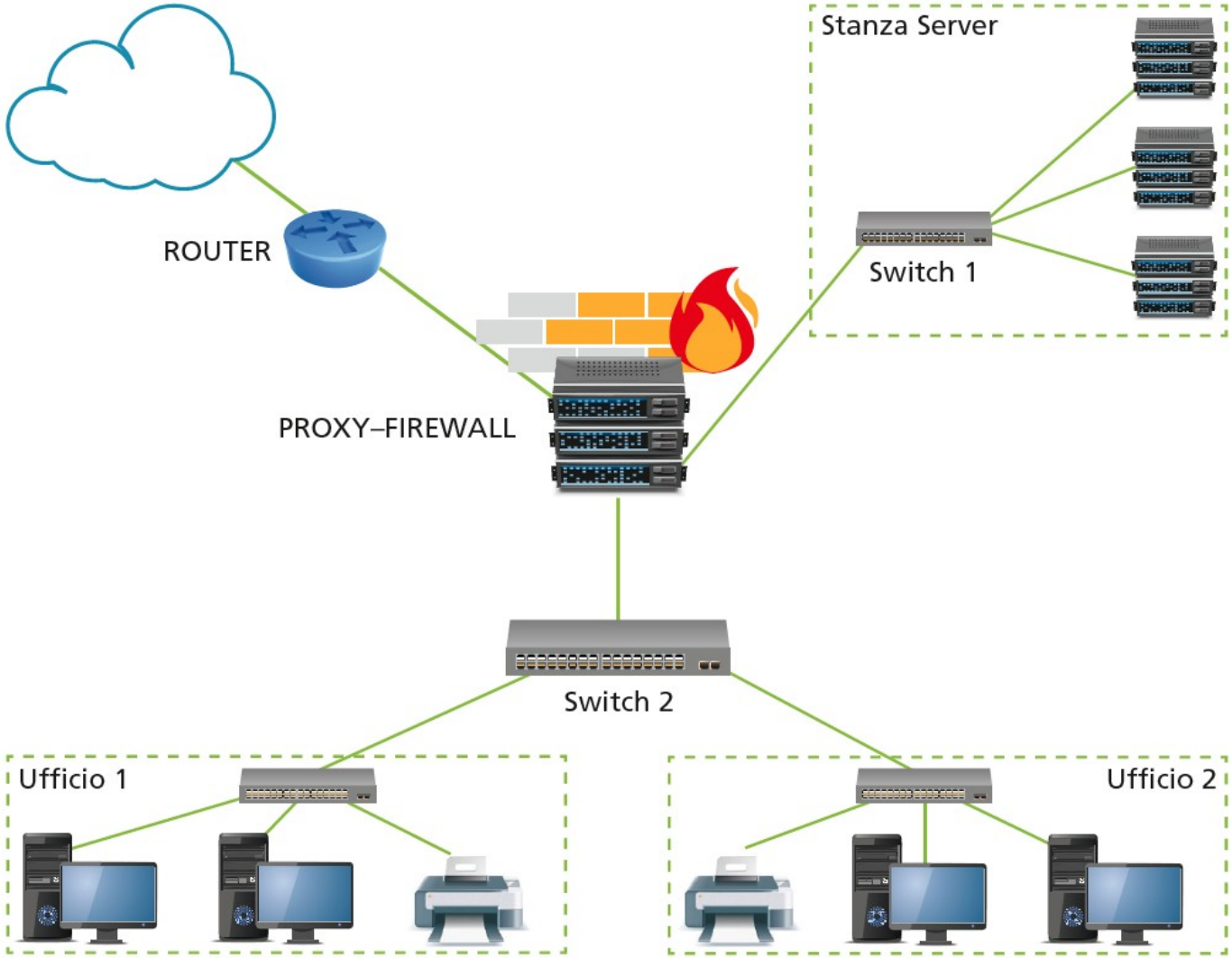
LA DEMILITARIZED ZONE (DMZ)

Una DMZ può essere realizzata in due modi:

- **Vicolo cieco**
- **Zona cuscinetto**

LA DEMILITARIZED ZONE (DMZ)

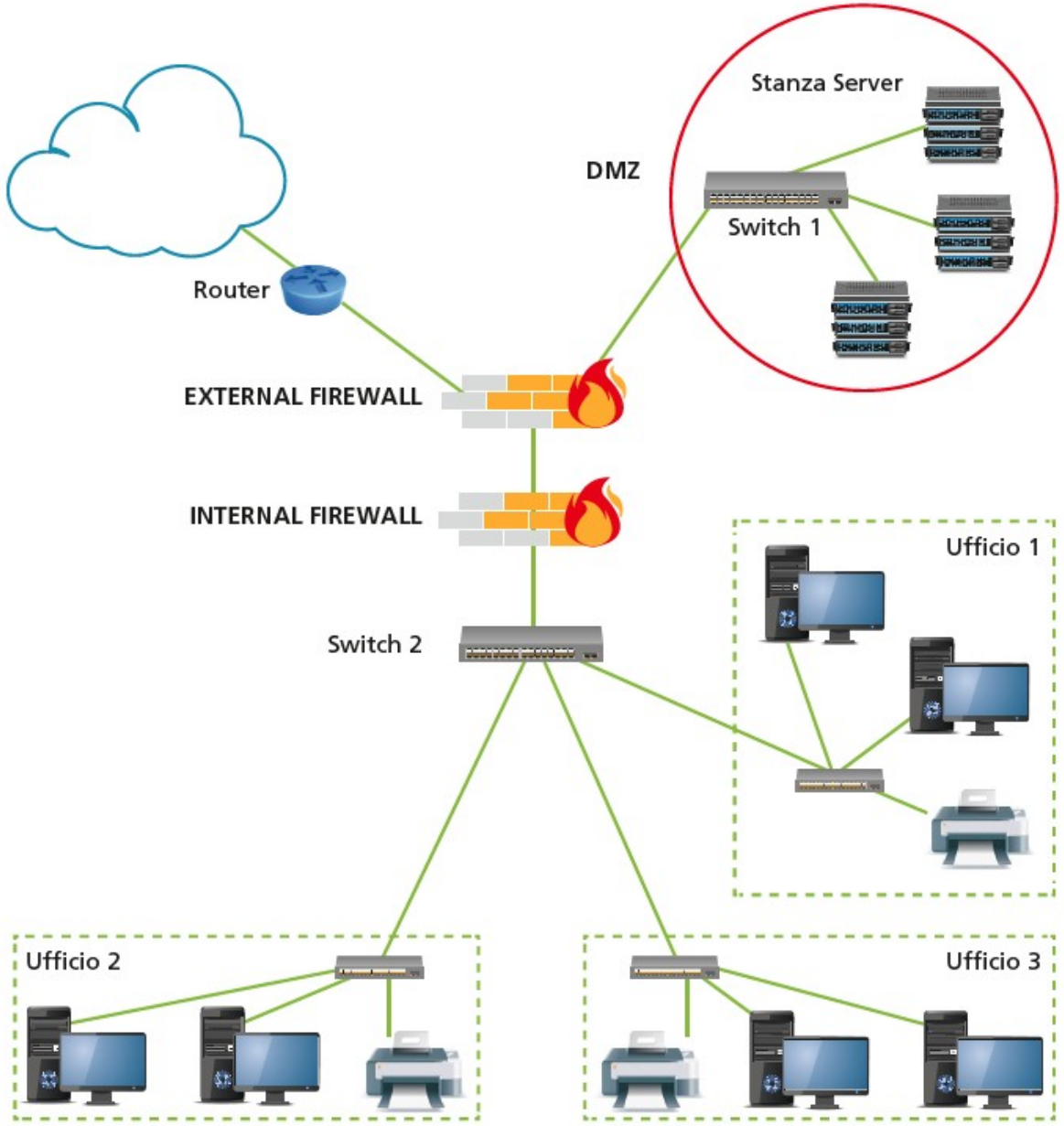
DMZ in modalità **vicolo cieco:** realizzata mediante un firewall con due porte, una verso la LAN (rete che connette gli uffici) e una verso la DMZ (la stanza server), oltre naturalmente alla porta verso la WAN.



LA DEMILITARIZED ZONE (DMZ)

DMZ in modalità **cuscinetto:**

- L'**external firewall** separa la rete pubblica dalla DMZ;
- L'**internal firewall** separa la DMZ dalla zona LAN vera e propria;
- Sicurezza maggiore per i DB presenti in LAN;
- Eventuali tentativi di intrusione in LAN devono superare un secondo firewall.



LA DEMILITARIZED ZONE (DMZ)

Ricapitolando, la DMZ è un'area pubblica protetta, dove il traffico è strettamente regolato da entrambi i lati ed è utile per pubblicare servizi verso l'esterno minimizzando i rischi per la rete interna. La DMZ è una *sottorete* della rete aziendale accessibile dai dipendenti tramite LAN e da utenti esterni tramite Internet. Architetture più complesse possono implicare la presenza di più zone DMZ distinte, ognuna con la sua policy e con il relativo controllo del traffico su tutti i lati. Laddove la sicurezza è vitale, la DMZ è stratificata, cioè sono presenti più di due firewall.