5 LE TECNICHE NAT E PAT

5.1 NAT (Network Address Translation)

NAT è una tecnica attuata dal router che, nell'intestazione di un pacchetto IP, sostituisce l'indirizzo IP, sorgente o destinazione, con un altro indirizzo. NAT, nel suo impiego più diffuso, viene usato per permettere a una rete locale, che usa una classe di indirizzi privata, di accedere a Internet usando un solo indirizzo pubblico fornito dall'Internet Service Provider (ISP).
Si tratta dunque di condividere Internet su una LAN usando un solo punto di accesso (un solo indirizzo IP pubblico).
Dal punto di vista della sicurezza, anche se non efficace come un firewall, un NAT offre già buone garanzie, proprio perché nasconde gli host interni e non indirizza loro il traffico generico proveniente dall'esterno.

> NAT usa una **tabella** contenente la corrispondenza tra le socket interne ed esterne in uso. Le **socket** non sono altro che l'insieme di protocollo, indirizzo IP e porta di comunicazione usati da mittente e destinatario.

Quando un client richiede una pagina web a 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 il router NAT 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.
Vediamo in FIGURA 15 un esempio in cui supponiamo sia utilizzato il protocollo TCP per tutte le trasmissioni dei pacchetti e che le socket siano limitate a indirizzo IP e numero di porta.

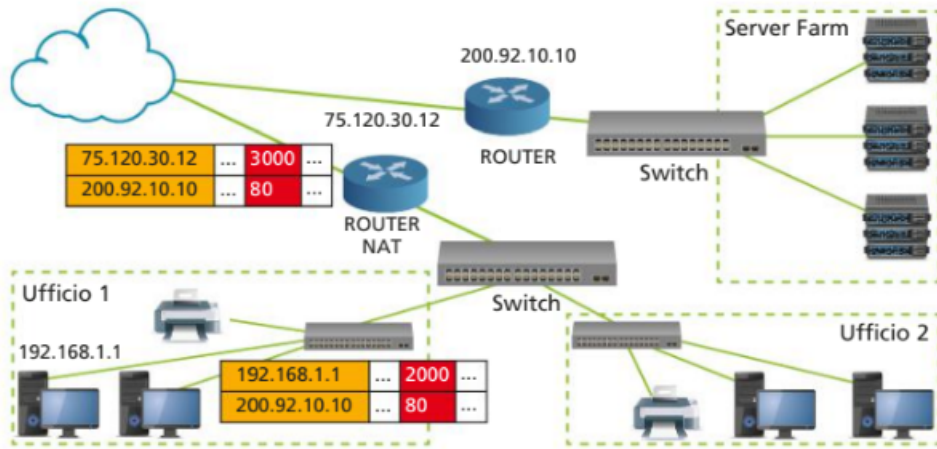


FIGURA 15 Router con funzionalità NAT

Il client con indirizzo privato 192.168.1.1 utilizza la porta 2000 per chiedere una pagina web residente presso una server farm, la quale risponde all'indirizzo pubblico 200.92.10.10 sulla porta 80 (Well Known Port per HTTP). Il router NAT (75.120.30.12) della LAN riceve la richiesta del client e, prima di inoltrare i pacchetti in rete sulla sua porta 3000, modifica l'intestazione dei pacchetti in modo che risultino generati

dal router NAT stesso (**traslazione dell'indirizzo**). Contestualmente, inserisce nella tabella contenente la corrispondenza tra le socket, la relativa corrispondenza:

CLIENT		ROUTER NAT		SERVER DESTINAZIONE
192.168.1.1:2000	↔	75.120.30.12:3000	↔	200.92.10.10:80

La destinazione finale riceverà i pacchetti dal router NAT e restituirà la pagina web richiesta. A quel punto, al router NAT non resterà che consultare la tabella con la corrispondenza delle socket, ripristinare l'indirizzo originario (effettuando un'**altra traslazione** dell'indirizzo) e inoltrare i pacchetti al client della sua LAN che aveva effettuato la richiesta.
Il limite del NAT è che può traslare un solo indirizzo IP per volta, dovendo traslare indirizzo IP e porta abbinati. Quindi se arriva una seconda richiesta per lo stesso server di destinazione, il router NAT non può gestirla avendo già mappato la connessione con quel server sulla porta 3000 dell'esempio ed essendo questa già in uso. È come se si fosse creata una seconda riga, priva di senso, nella tabella di corrispondenza:

CLIENT		ROUTER NAT		SERVER DESTINAZIONE
192.168.1.1:2000	↔	75.120.30.12:3000	↔	200.92.10.10:80
192.168.2.1:2000	↔	75.120.30.12:3000	↔	200.92.10.10:80

In questo caso vale la regola del **rapporto 1:1** tra indirizzo IP del server di destinazione e indirizzo IP del client.
Il router NAT, cioè, non è in grado di distinguere a quale dei due client locali sono destinati, di volta in volta, i pacchetti in arrivo dallo stesso server remoto.
La tecnica PAT supera questa limitazione.

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).

Il NAT presenta 3 funzionalità:
- Static NAT;
- Dynamic NAT;
- Port Address Translation (PAT).

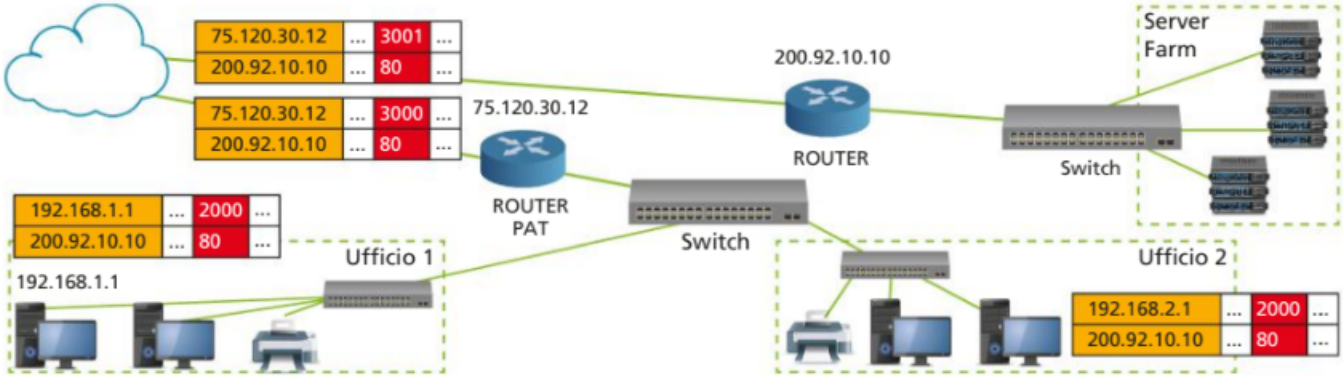
La prima ha a disposizione un solo indirizzo pubblico (IP statico) e a qualunque pacchetto in uscita assegnerà tale indirizzo.
La seconda ha a disposizione un insieme di indirizzi pubblici tra cui sceglierne uno da assegnare ai pacchetti in uscita.
La terza traduce in modo dinamico l'indirizzo delle porte, ovvero guarda alla porta di trasmissione e non agli indirizzi IP degli host. Quest'ultima funzionalità può essere usata in coppia con una della precedenti per ottenere la traslazione dell'indirizzo IP e della porta su ogni pacchetto.

Nella Lezione 9 vedremo nello specifico come realizzare le funzionalità di **NAT statico** e **NAT dinamico**, mediante due esercitazioni con Cisco Packet Tracer.

5.2 PAT (Port Address Translation)

La tecnica PAT consente al router di utilizzare un singolo indirizzo IP per gestire oltre 64.000 connessioni private contemporaneamente (per la precisione, 2^{16} = 65.536 porte diverse indirizzabili). Questo significa che può traslare più indirizzi IP client per un medesimo indirizzo IP destinazione cambiando solo la porta (FIGURA 16). Per il PAT vale la regola del **rapporto 1:N** tra indirizzo IP del server di destinazione e indirizzo IP del client.

FIGURA 16 Router con funzionalità PAT



In questo caso la seconda riga della tabella di corrispondenza permette al router PAT di distinguere a quale client inoltrare i pacchetti in arrivo dal server di destinazione sulle due connessioni aperte rispettivamente sulle porte 3000 e 3001:

CLIENT		ROUTER PAT		SERVER DESTINAZIONE
192.168.1.1:2000	↔	75.120.30.12:3000	↔	200.92.10.10:80
192.168.2.1:2000	↔	75.120.30.12:3001	↔	200.92.10.10:80

5.3 NAT per IPv6

Anche IPv6 implementa una forma di NAT con scopi del tutto diversi dal NAT per IPv4. Con IPv6 non serve più "risparmiare" indirizzi pubblici ma serve 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**: i dispositivi di rete sono in grado di inoltrare pacchetti IPv4 e pacchetti IPv6;
- **conversion**: è considerato il NAT per IPv6 realizzato con il protocollo **NAT-PT** (Network Address Translation - Protocol Translator) che permette la comunicazione tra reti IPv6 e reti IPv4;
- **tunneling per IPv6**: incapsula un pacchetto IPv6 in un pacchetto IPv4, permettendone il trasporto in reti IPv4.

La tecnica del **dual-stack** prevede l'utilizzo del doppio stack IP (FIGURA 17) nella pila di protocolli TCP/IP.

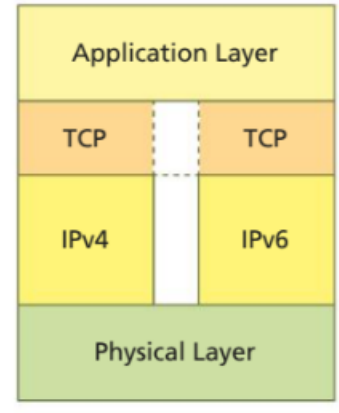


FIGURA 17 Dual-stack

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.

Il dual-stack è senza dubbio una delle tecniche più semplici da implementare, ma presenta alcuni svantaggi. Innanzitutto aumenta la complessità della rete: router e switch devono essere multiprotocollo per funzionare sia con IPv4 che con IPv6 e devono interpretare più istanze dello stesso protocollo. Inoltre non risolve il problema della scarsità degli indirizzi IPv4 poiché secondo la tecnica del dual-stack un'interfaccia dev'essere sempre e comunque dotata dei due indirizzi IPv4 e IPv6. Infine i due indirizzi devono essere entrambi annunciati in Internet e ciò complica e rallenta il routing.

La **conversion** con NAT-PT è un sistema che sfrutta i concetti introdotti dalla tecnologia NAT: infatti esso opera una **conversione** dell'indirizzo IPv6 in indirizzo IPv4 e viceversa secondo le tecniche di un NAT IPv4, permettendo in questo modo a due reti con protocolli IP diversi di poter comunicare tra di loro.
NAT-PT consente quindi la comunicazione diretta tra reti solo IPv6 e reti solo IPv4 come mostrato in FIGURA 18.

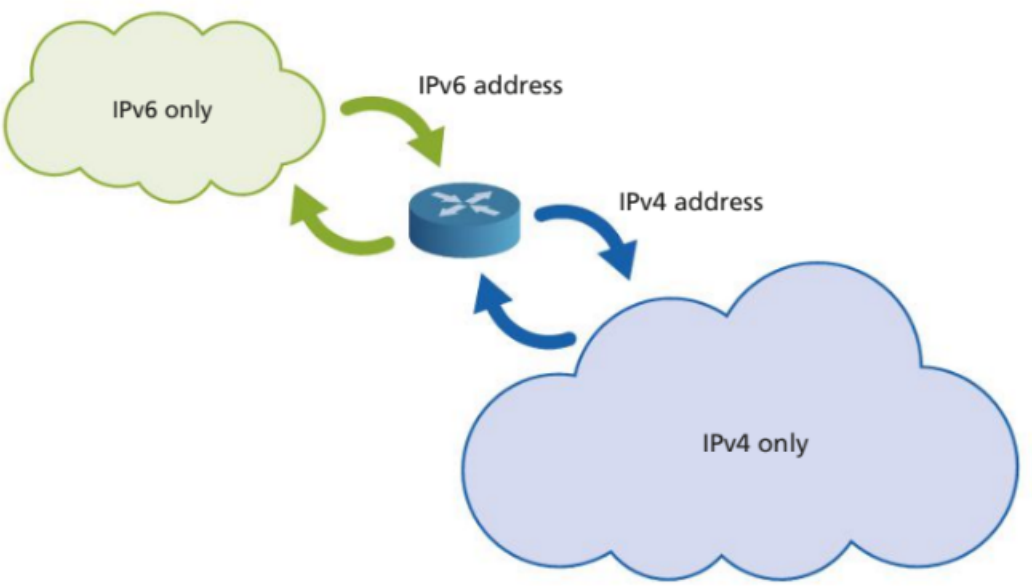


FIGURA 18 Comunicazione diretta IPv4-IPv6

È consigliabile non utilizzare NAT-PT per comunicare tra un host dual-stack e un host solo IPv6 o solo IPv4.
Allo stesso modo è meglio evitare l'uso di NAT-PT in uno scenario in cui una rete solo IPv6 tenta di comunicare con un'altra rete solo IPv6 tramite un backbone IPv4 o viceversa, perché NAT-PT richiede una doppia traduzione degli indirizzi IP.
In presenza di tali scenari è più conveniente utilizzare tecniche di tunneling.

> Tuttavia, se si dispone di una rete interamente IPv6 e ci si connette a un provider IPv6, il NAT non ha senso perché non serve, tranne per il fatto che è possibile eseguire il tunneling tra reti IPv4 su reti IPv6.

La tecnica del **tunneling** è quella più utilizzata per far fronte ai problemi di incompatibilità tra le reti IPv4 e IPv6. Con il tunneling si stabilisce un collegamento point-to-point tra due host.

4to6

Nel tunneling IPv4 di un pacchetto IPv6, i pacchetti IPv6 vengono incapsulati dall'host sorgente in pacchetti IPv4, inviati nel tunnel IPv4 (FIGURA 19) e, una volta giunti a destinazione, l'host ricevente li decapsula per riottenere l'indirizzo in IPv6.

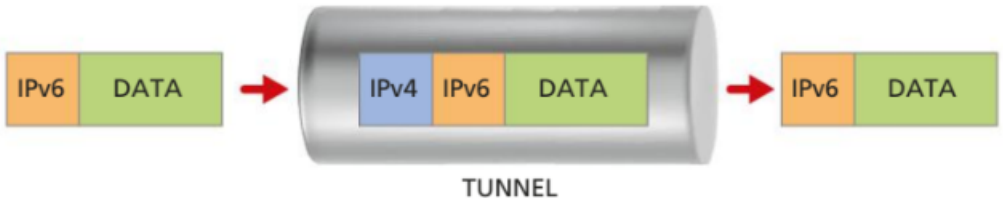


FIGURA 19 Tunnel IPv4 per pacchetti IPv6

Il tunneling IPv4 è di tipo multicast, consentendo ai nodi IPv6 di vedere tutto il resto della rete a cui sono connessi come un'unica rete LAN IPv6 virtuale. Questa tecnica è descritta nella RFC 2529.

IN ENGLISH PLEASE

Network Working Group — B. Carpenter
Request for Comments: 2529 — IBM
Category: Standards Track — C. Jung
3Com
March 1999

Transmission of IPv6 over IPv4 Domains without Explicit Tunnels

Abstract

This memo specifies the frame format for transmission of IPv6 [IPV6] packets and the method of forming IPv6 link-local addresses over IPv4 domains. It also specifies the content of the Source/Target Link-layer Address option used in the Router Solicitation, Router Advertisement, Neighbor Solicitation, and Neighbor Advertisement and Redirect messages, when those messages are transmitted on an IPv4 multicast network.

The motivation for this method is to allow isolated IPv6 hosts, located on a physical link which has no directly connected IPv6 router, to become fully functional IPv6 hosts by using an IPv4 domain that supports IPv4 multicast as their virtual local link. It uses IPv4 multicast as a "virtual Ethernet".

6to4

Viceversa, il tunneling IPv6 su IPv4 è di difficile realizzazione sulle reti globali per le complicazioni che introduce a livello di routing e quindi il suo utilizzo è limitato ad applicazioni e comunicazioni in reti locali più o meno grosse.

È una tecnica di tunnel automatico, descritta dalla RFC 3056 successivamente ampliata dalla RFC 6343. Essa integra nell'indirizzo IPv6 l'indirizzo IPv4 dell'host di destinazione. Il modello parte dall'assunto che un dispositivo utilizza nativamente un indirizzo IPv6 ma opera in un ambiente, per esempio Internet, in cui il fornitore di servizi utilizza IPv4.

IN ENGLISH PLEASE

Internet Engineering Task Force (IETF)
Request for Comments: 6343
Category: Informational
ISSN: 2070-1721

B. Carpenter
Univ. of Auckland

August 2011

Advisory Guidelines for 6to4 Deployment

Abstract

This document provides advice to network operators about deployment of the 6to4 technique for automatic tunneling of IPv6 over IPv4. It is principally addressed to Internet Service Providers (ISPs), including those that do not yet support IPv6, and to Content Providers. Some advice to implementers is also included. The intention of the advice is to minimize both user dissatisfaction and help-desk calls.

Usando un tunnel IPv6, viene generato un indirizzo IPv6 composto nel seguente modo (0 indica il bit più significativo):

- bit 0-15: prefisso 6to4 al valore esadecimale fisso 2002;
- bit 16-47: indirizzo IPv4 espresso in notazione esadecimale; per esempio: 160.1.1.32 diventa A001:0120;
- bit 48-63: identificativo delle sottoreti;
- bit 64-127: identificativo dell'interfaccia fisica.

Il pacchetto così generato viene inviato tramite il tunnel al router di destinazione che è in grado di interpretarlo e preparare un pacchetto IPv4 per l'host cui era indirizzato. Con questa tecnica, un singolo indirizzo IPv4 corrisponde a un indirizzo IPv6 con maschera /48: per esempio, l'indirizzo IPv4 160.1.1.32 equivale al range di indirizzi IPv6 2002: A001:0120::/48.

FISSA LE CONOSCENZE

- In che cosa consiste la tecnica NAT attuata dai router?
- Quali sono le 3 funzionalità del NAT e che caratteristiche hanno?
- In che cosa consiste la tecnica PAT attuata dai router?
- Quali sono i 3 meccanismi per la possibile convivenza di IPv4 e IPv6?
- Che cosa consente di fare NAT-PT?
- In quale caso il NAT su un host IPv6 non serve?
- Che cosa si intende rispettivamente per 4to6 e per 6to4?

6 LA DEMILITARIZED ZONE (DMZ)

6.1 La terza zona

La sicurezza perimetrale si occupa di proteggere una rete nei punti in cui essa è a contatto con il mondo esterno. Dividere la rete in zone è una tecnica che aumenta notevolmente la sicurezza: in base al tipo di traffico e alla funzione si identificano diverse zone.
Nei casi più semplici, le uniche due zone, LAN e WAN, sono attestate sui due lati del firewall.

La **zona LAN** è il segmento privato e protetto: comprende tutti gli host e i server i cui servizi sono riservati all'uso interno.
La **zona WAN** è la parte esterna a cui appartengono gli apparati di routing che sostengono il traffico da e per rete locale, Internet e sedi remote dell'azienda.
In molti casi, però, si rende necessaria la creazione di una terza zona.

> Questa terza zona è 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.

Nel caso più comune si colloca nella DMZ la **posta elettronica**: l'installazione di un server mail all'interno della rete aziendale comporta la pubblicazione del servizio SMTP. In pratica, il server che pubblica il servizio SMTP viene collocato in DMZ ed eventualmente anche la webmail, l'antispam e l'antivirus; in LAN restano il server che ospita il database delle caselle e gli altri servizi.
Altro caso tipico sono gli **Application Server**, che isolano un database residente in LAN ma ne offrono un'interfaccia verso l'esterno.

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.

6.2 Tipi di DMZ

Una DMZ, per esporre all'esterno i servizi di un'azienda, può essere realizzata in due modi:

- **vicolo cieco**: realizzato mediante un firewall con due porte, una verso la LAN e una verso la DMZ, oltre naturalmente alla porta verso la WAN.

La Figura 12 della Lezione 4 ne illustra un esempio: il firewall separa la stanza server (DMZ) dagli uffici (LAN). L'idea è quella di consentire l'accesso dall'esterno (ma anche dall'interno) alla DMZ, garantendo che, una volta raggiunta la DMZ, non si possa accedere alla LAN, cioè agli uffici. Si è cioè entrati in un vicolo cieco da cui si esce solo attraversando la stessa via da cui si è entrati. Dunque, un utente potrà accedere ai servizi che l'azienda rende accessibili dall'esterno (per esempio da Internet) nella DMZ senza mettere in pericolo la sicurezza dei dati presenti nella zona LAN;

- **zona cuscinetto**: creata aggiungendo un secondo firewall, come nella FIGURA 20. L'**external firewall** separa la rete pubblica dalla DMZ; l'**internal firewall** separa la DMZ dalla zona LAN vera e propria. Questo garantisce una sicurezza ancora maggiore dei database presenti in LAN. Chi dall'esterno approda alla DMZ, per attaccare i dati in LAN dovrà superare un secondo firewall dedicato.

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.

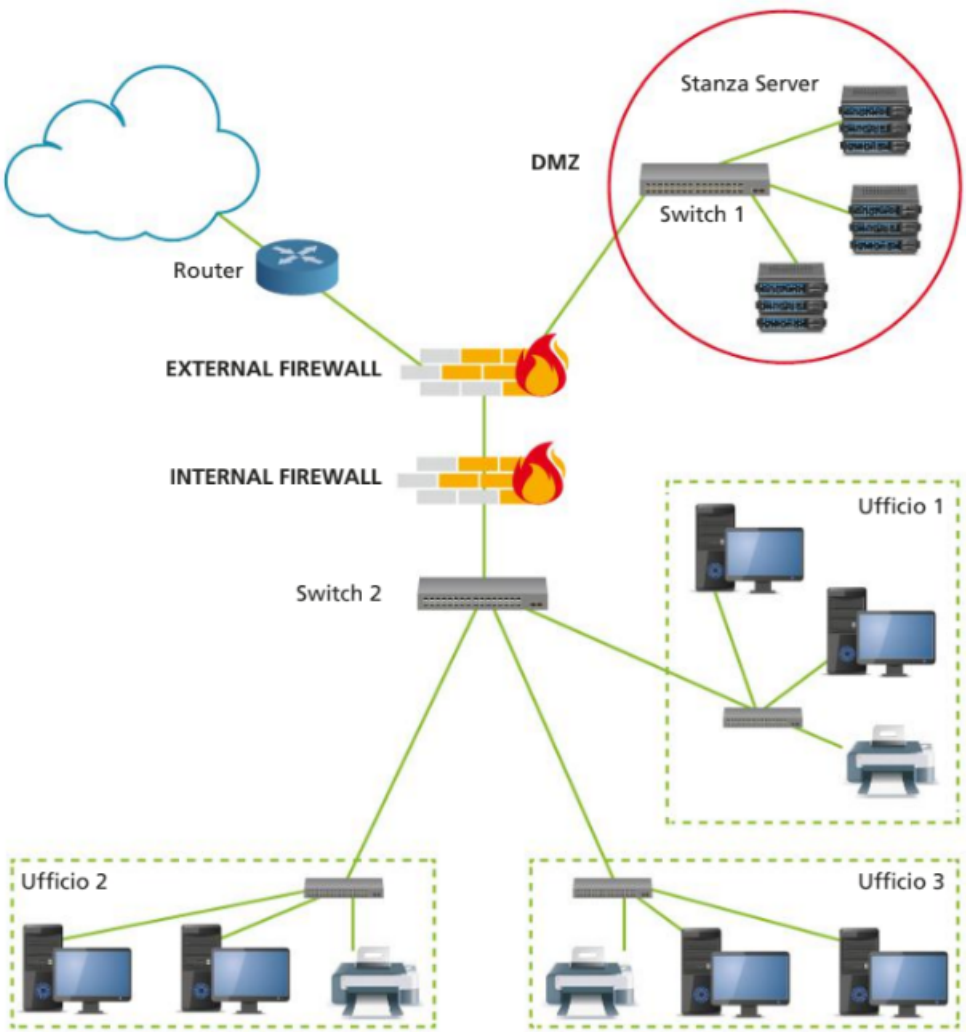


FIGURA 20 DMZ con modalità a zona cuscinetto

FISSA LE CONOSCENZE

- Perché la DMZ è detta terza zona?
- Quali sono i due modi in cui si può realizzare una DMZ e in che cosa differiscono?
- Per che cosa viene normalmente utilizzata la DMZ?