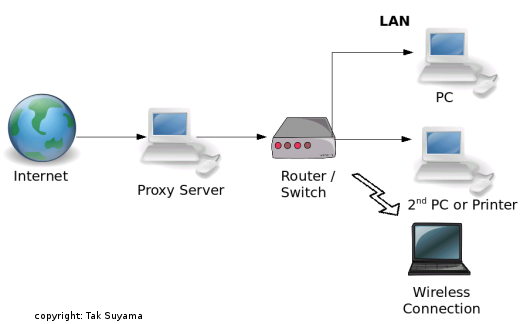
**Proxy HTTP**



Un caso in cui viene spesso usato un proxy è la navigazione [web](http://it.wikipedia.org/wiki/Web) (denominato proxy [HTTP](http://it.wikipedia.org/wiki/Hyper_Text_Transfer_Protocol) dal nome del protocollo usato).[[3]](http://it.wikipedia.org/wiki/Proxy#cite_note-2)

Per utilizzare un proxy è possibile configurare il client in modo che si colleghi al proxy invece che al server, oppure definire un **proxy trasparente**; in questo caso, a seconda della configurazione, alcune connessioni (ad esempio quelle HTTP) vengono automaticamente indirizzate al proxy senza che sia necessario configurare un client (quindi l'impostazione rimane attiva anche cambiando client).

Un proxy può essere usato per una o più delle seguenti ragioni:

* **connettività**: per permettere ad una [rete privata](http://it.wikipedia.org/w/index.php?title=Rete_privata&action=edit&redlink=1) di accedere all'esterno è possibile configurare un computer in modo che faccia da proxy tra gli altri computer e [Internet](http://it.wikipedia.org/wiki/Internet), in modo da mantenere un unico computer connesso all'esterno, ma permettere a tutti di accedere. In questa situazione, solitamente il proxy viene usato anche come [firewall](http://it.wikipedia.org/wiki/Firewall).
* [**caching**](http://it.wikipedia.org/wiki/Cache): un proxy può immagazzinare per un certo tempo i risultati delle richieste di un utente, e se un altro utente effettua le stesse richieste può rispondere senza dover consultare il server originale. Collocando il proxy in una posizione "vicina" agli utenti, questo permette un miglioramento delle prestazioni ed una riduzione del consumo di [ampiezza di banda](http://it.wikipedia.org/wiki/Ampiezza_di_banda).
* **monitoraggio**: un proxy può permettere di tenere traccia di tutte le operazioni effettuate (ad esempio, tutte le pagine web visitate), consentendo statistiche ed osservazioni dell'utilizzo della rete che possono anche violare la [privacy](http://it.wikipedia.org/wiki/Privacy) degli utenti.
* **controllo**: un proxy può applicare regole definite dall'[amministratore di sistema](http://it.wikipedia.org/wiki/Amministratore_di_sistema) per determinare quali richieste inoltrare e quali rifiutare, oppure limitare l'[Ampiezza di banda](http://it.wikipedia.org/wiki/Ampiezza_di_banda) utilizzata dai client, oppure filtrare le pagine Web in transito, ad esempio bloccando quelle il cui contenuto è ritenuto offensivo in base a determinate regole.
* [**privacy**](http://it.wikipedia.org/wiki/Privacy): un proxy può garantire un maggiore livello di privacy mascherando il vero [indirizzo IP](http://it.wikipedia.org/wiki/Indirizzo_IP) del client in modo che il server non venga a conoscenza di chi ha effettuato la richiesta.

Quando la configurazione della rete consente di collegarsi ad internet solamente attraverso un proxy, non sono ovviamente utilizzabili molti tipi di applicazioni basate su protocolli non supportati dal proxy, ad esempio:

* **Giochi on-line**
* **webcam**: la ricezione e l'invio di immagini tramite webcam con programmi di [messaggistica istantanea](http://it.wikipedia.org/wiki/Messaggistica_istantanea)
* browser che non supportano la configurazione di un proxy. Questo caso è frequente su dispositivi particolari come [console](http://it.wikipedia.org/wiki/Console_(sistema_per_videogiochi)) per videogiochi o telefoni cellulari.
* servizi [VoIP](http://it.wikipedia.org/wiki/VoIP)
* applicazioni di [file sharing](http://it.wikipedia.org/wiki/File_sharing)

Talune di queste applicazioni sono state modificate per poter far passare il proprio traffico incapsulato in HTTP e quindi per poterlo veicolare in un proxy.

**Proxy HTTP e anonimato**

I server esterni a cui si collega il client quando si utilizza un proxy vedranno generalmente l'[indirizzo IP](http://it.wikipedia.org/wiki/Indirizzo_IP) del proxy (e non quello del client). Se l'uso di un proxy garantisce una relativa privacy del client (il server esterno, o chi analizzi il traffico diretto ad esso, non potrà infatti conoscere l'indirizzo IP del client), può impedire la connessione a quei siti che utilizzino l'indirizzo IP del client per scopi di autenticazione o di riconoscimento delle sessioni (come ad esempio nei collegamenti agli sportelli bancari on-line).

Il protocollo [HTTP](http://it.wikipedia.org/wiki/Hyper_Text_Transfer_Protocol) prevede però che un proxy possa inserire nelle richieste che inoltra al server degli [header](http://it.wikipedia.org/wiki/Header) standardizzati, che permettono di riconoscere che la richiesta è stata inoltrata da un proxy, e possono contenere anche l'indirizzo IP del client, che in questo modo può essere noto ad un server opportunamente configurato. Quando viene usata questa funzionalità, il server web "si fida" dell'indirizzo del client inviatogli dal proxy, e non può in alcun modo verificare questa informazione. L'amministratore di un server proxy può decidere se inviare o meno questi header determinando quindi il livello di anonimato del proxy.

I proxy HTTP, a seconda dell'anonimato che riescono a fornire, possono essere suddivisi in:

* **NOA** (*non anonymous proxy*) **proxy non anonimi** (o "trasparenti"): Modificano alcuni header trasmessi dal browser e ne aggiungono altri, mostrano anche l'indirizzo IP reale del richiedente. Sono molto facili da riconoscere da parte del server web.
* **ANM** (*anonymous proxy server*) **proxy anonimi**: non trasmettono l'IP del richiedente, ma modificano o aggiungono alcuni header. Sono pertanto facilmente riconoscibili.
* **HIA** (*high anonymous proxy*) **proxy altamente anonimi** (o "*elite*"): non trasmettono l'IP del richiedente e non modificano gli header della richiesta. Sono difficili da riconoscere attraverso i normali controlli.
* **Proxy distorcenti**: trasmettono un IP casuale, diverso da quello del richiedente e modificano o aggiungono alcuni header. Solitamente vengono scambiati per proxy Anonimi, ma offrono una protezione maggiore, in quanto il server web vede le richieste di un utente provenienti da indirizzi IP diversi.

Esistono programmi che, basandosi sulla tecnologia [peer to peer](http://it.wikipedia.org/wiki/P2P) forniscono funzionalità di proxy "anonimizzante" (un proxy che non inoltra al server l'indirizzo IP del client).

Il protocollo HTTP è *stateless*, ovvero una richiesta non lascia alcuno stato nel server. Tuttavia, per realizzare applicazioni web complesse, sono stati sviluppati meccanismi a livello superiore come i [cookies](http://it.wikipedia.org/wiki/Cookies) per costruire "sessioni". Questi meccanismi possono permettere al server web di ottenere informazioni sul client nonostante gli sforzi fatti dal proxy per difenderne l'anonimato, in particolare possono permettere di riconoscere un utente di un server web anche se questi si collega da reti totalmente diverse.

Per vedere se il proxy server consente una navigazione anonima, ossia se non rivela l'IP del client a nessun altro server della rete, è bene effettuare un "[Who-is](http://it.wikipedia.org/wiki/Whois)". Il server del sito per il Who-is deve restituire l'IP del proxy server; se invece, rende visibile un IP diverso, presumibilmente si tratta di quello del client, e il test è fallito.

**Proxy CGI**

Un proxy CGI consiste in un sito web attraverso il quale è possibile navigare in rete. Per utilizzare un proxy CGI occorre collegarsi ad un apposito sito web che ci permette, dopo aver digitato nel campo apposito l'indirizzo web che si vuole visitare, di collegarci ad esso in modo anonimo. Su internet è possibile trovare liste di siti CGI.

* Vantaggi:

1. permettono all'utente di scegliere quali dati inviare al server (cookies, tipo di browser, etc.) nascondendo l'IP
2. permettono ad un utente di rete (che non abbia i diritti di amministratore per modificare le impostazioni del browser o del sistema operativo), di bypassare le restrizioni di navigazione imposte ed operare on-line in modo anonimo

* Svantaggi

1. un proxy CGI potrebbe non poter gestire autonomamente cookies, referer e javascript

**Note** [[modifica](http://it.wikipedia.org/w/index.php?title=Proxy&action=edit&section=8)]

1. [**^**](http://it.wikipedia.org/wiki/Proxy#cite_ref-0) (**EN**) Bradley Mitchell. [*Proxy Servers Tutorial - About Proxy Servers*](http://compnetworking.about.com/cs/proxyservers/a/proxyservers.htm). about.com. URL consultato in data 20-5-2012.
2. [**^**](http://it.wikipedia.org/wiki/Proxy#cite_ref-1) (**EN**) [*SIP: Session Initiation Protocol - 16. Proxy Behavior*](http://tools.ietf.org/html/rfc3261#section-16). ietf.org. URL consultato in data 20-5-2012.
3. [**^**](http://it.wikipedia.org/wiki/Proxy#cite_ref-2) (**EN**) [*Hypertext Transfer Protocol - HTTP/1.1 - 8.1.3 Proxy Servers*](http://tools.ietf.org/html/rfc2616#section-8.1.3). ietf.org. URL consultato in data 20-5-2012.

# FIREWALL

**Definizione e funzionalità**

Una prima definizione chiusa di firewall è la seguente: *Apparato di rete* [*hardware*](http://it.wikipedia.org/wiki/Hardware) *o* [*software*](http://it.wikipedia.org/wiki/Software) *che, opportunamente configurato o settato, filtra tutti i* [*pacchetti*](http://it.wikipedia.org/wiki/Pacchetto_(reti)) *entranti ed uscenti, da e verso una rete o un* [*computer*](http://it.wikipedia.org/wiki/Computer)*, secondo regole prestabilite che contribuiscono alla* [*sicurezza*](http://it.wikipedia.org/wiki/Sicurezza_informatica) *della stessa agendo in maniera centralizzata.*

In realtà un firewall può essere realizzato con un semplice computer (con almeno due [schede di rete](http://it.wikipedia.org/wiki/Scheda_di_rete) e software apposito), può essere una funzionalità logica inclusa in un [router](http://it.wikipedia.org/wiki/Router) oppure può essere un apparato specializzato. Esistono inoltre i cosiddetti "firewall personali", che sono programmi installati sui normali calcolatori, che filtrano solamente i pacchetti che entrano ed escono da quel calcolatore; in tal caso viene utilizzata una sola scheda di rete.

La funzionalità principale in sostanza è quella di creare un filtro sulle [connessioni](http://it.wikipedia.org/wiki/Connessione_(informatica)) entranti ed uscenti, in questo modo il dispositivo innalza il livello di sicurezza della rete e permette sia agli utenti interni che a quelli esterni di operare nel massimo della sicurezza. Il firewall agisce sui pacchetti in transito da e per la zona interna potendo eseguire su di essi operazioni di:

* controllo;
* modifica;
* monitoraggio.

Questo grazie alla sua capacità di "aprire" il [pacchetto](http://it.wikipedia.org/wiki/Pacchetto_(reti)) [IP](http://it.wikipedia.org/wiki/Internet_Protocol) per leggere le informazioni presenti sul suo [header](http://it.wikipedia.org/wiki/Header), e in alcuni casi anche di effettuare verifiche sul contenuto o [payload](http://it.wikipedia.org/wiki/Payload) del pacchetto.

**Personal Firewall o Firewall Software**

Oltre al firewall a protezione perimetrale ne esiste un secondo tipo, definito "*Personal Firewall*", che si installa direttamente sui sistemi da proteggere (per questo motivo è chiamato anche Firewall [Software](http://it.wikipedia.org/wiki/Software)). In tal caso, un buon firewall effettua anche un controllo di tutti i programmi che tentano di accedere ad Internet presenti sul computer nel quale è installato, consentendo all'utente di impostare delle regole che possano concedere o negare l'accesso ad Internet da parte dei programmi stessi, questo per prevenire la possibilità che un programma malevolo possa connettere il computer all'esterno pregiudicandone la sicurezza.

Il principio di funzionamento differisce rispetto a quello del firewall perimetrale in quanto, in quest'ultimo, le regole che definiscono i flussi di traffico permessi vengono impostate in base all'[indirizzo IP](http://it.wikipedia.org/wiki/Indirizzo_IP) sorgente, quello di destinazione e la [porta](http://it.wikipedia.org/wiki/Porta_(reti)) attraverso la quale viene erogato il servizio, mentre nel personal firewall all'utente è sufficiente esprimere il consenso affinché una determinata applicazione possa interagire con il mondo esterno attraverso il protocollo IP.

Da sottolineare che l'aggiornamento di un firewall è importante ma non è così vitale come invece lo è l'aggiornamento di un [antivirus](http://it.wikipedia.org/wiki/Antivirus), in quanto le operazioni che il firewall deve compiere sono sostanzialmente sempre le stesse. È invece importante creare delle regole che siano corrette per decidere quali programmi devono poter accedere alla rete esterna e quali invece non devono.

**Vantaggi e svantaggi**

Rispetto ad un firewall perimetrale, il personal firewall è eseguito sullo stesso [sistema operativo](http://it.wikipedia.org/wiki/Sistema_operativo) che dovrebbe proteggere, ed è quindi soggetto al rischio di venir disabilitato da un [malware](http://it.wikipedia.org/wiki/Malware) che prenda il controllo del calcolatore con diritti sufficienti. Inoltre, la sua configurazione è spesso lasciata a utenti finali poco esperti.

A suo favore, il personal firewall ha accesso ad un dato che un firewall perimetrale non può conoscere, ovvero può sapere quale applicazione ha generato un pacchetto o è in ascolto su una determinata porta, e può basare le sue decisioni anche su questo, ad esempio bloccando una connessione [SMTP](http://it.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol) generata da un virus e facendo passare quella generata da un'altra applicazione.

**Filtraggio dei contenuti**

Una funzione che alcuni firewall prevedono è la possibilità di filtrare ciò che arriva da [internet](http://it.wikipedia.org/wiki/Internet) sulla base di diversi tipi di criteri non relativi alla sicurezza informatica, ma volti a limitare gli utilizzi della rete sulla base di decisioni "politiche", in particolare vietando la connessione a determinate categorie di [siti internet](http://it.wikipedia.org/wiki/Sito_web):

* contenuti non adatti ai minori (ad esempio in una rete domestica, o destinata ai frequentatori di una scuola o biblioteca)
* contenuti non pertinenti all'attività lavorativa (in una rete aziendale)
* contenuti non ritenuti accettabili da organi di [censura](http://it.wikipedia.org/wiki/Censura), su base [politica](http://it.wikipedia.org/wiki/Politica) o [religiosa](http://it.wikipedia.org/wiki/Religione).
* siti che permettono di pubblicare informazioni sfuggendo alla censura di un regime totalitario (in particolare [blog](http://it.wikipedia.org/wiki/Blog))

Alcune nazioni arrivano a filtrare tutto il traffico internet proveniente dal proprio territorio nazionale nel tentativo di controllare il flusso di informazioni.

Spesso l'attivazione di questa funzionalità è demandata a software e/o hardware aggiuntivi appartenenti alla categoria dell'[URL filtering](http://it.wikipedia.org/w/index.php?title=URL_filtering&action=edit&redlink=1). Ai firewall viene però richiesto di impedire che gli utenti aggirino tali limitazioni.

**Limitazioni**

Il firewall è solo uno dei componenti di una strategia di [sicurezza informatica](http://it.wikipedia.org/wiki/Sicurezza_informatica), e non può in generale essere considerato sufficiente:

* la sua configurazione è un compromesso tra usabilità della rete, sicurezza e risorse disponibili per la manutenzione della configurazione stessa (le esigenze di una rete cambiano rapidamente)
* una quota rilevante delle minacce alla sicurezza informatica proviene dalla rete interna (portatili, virus, connessioni abusive alla rete, dipendenti, accessi [VPN](http://it.wikipedia.org/wiki/Virtual_Private_Network), [reti wireless](http://it.wikipedia.org/wiki/Reti_wireless) non adeguatamente protette)

**Tipologie**

Tipologie di firewall, in ordine crescente di complessità:

* Il più semplice è il **packet filter**, che si limita a valutare gli [header](http://it.wikipedia.org/wiki/Header_file) di ciascun pacchetto, decidendo quali far passare e quali no sulla base delle regole configurate. Ciascun pacchetto viene valutato solamente sulla base delle regole configurate, e per questo un firewall di questo tipo è detto anche **stateless**. Alcuni packet filter, analizzando i flag dell'header [TCP](http://it.wikipedia.org/wiki/Transmission_Control_Protocol), sono in grado di discriminare un pacchetto appartenente ad una "connessione TCP stabilita (established)" rispetto a quelli che iniziano una nuova connessione, ma non sono in grado di riconoscere un pacchetto malevolo che finga di appartenere ad una connessione TCP stabilita. Molti [router](http://it.wikipedia.org/wiki/Router) posseggono una funzione di packet filter.
* Un firewall di tipo [stateful inspection](http://it.wikipedia.org/wiki/Filtraggio_stateful_dei_pacchetti), tiene traccia di alcune relazioni tra i pacchetti che lo attraversano, ad esempio ricostruisce lo stato delle connessioni TCP.
* I firewall di tipo **deep inspection** effettuano controlli fino al livello 7 della pila ISO/OSI, ovvero valutano anche il contenuto applicativo dei pacchetti, ad esempio riconoscendo e bloccando i dati appartenenti a [virus](http://it.wikipedia.org/wiki/Virus_(informatica)) o [worm](http://it.wikipedia.org/wiki/Worm) noti in una sessione [HTTP](http://it.wikipedia.org/wiki/Hyper_Text_Transfer_Protocol) o [SMTP](http://it.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol).
* I cosiddetti **Application Layer Firewall** sono apparati che intercettano le connessioni a [livello applicativo](http://it.wikipedia.org/wiki/Livello_applicazioni). A questa categoria appartengono i [proxy](http://it.wikipedia.org/wiki/Proxy). In tali casi, la configurazione della rete privata non consente connessioni dirette verso l'esterno, ma il proxy è connesso sia alla rete privata che alla rete pubblica, e permette alcune connessioni in modo selettivo, e solo per i protocolli che supporta.

La sintassi della configurazione di un firewall in molti casi è basata su un meccanismo di [lista di controllo degli accessi](http://it.wikipedia.org/wiki/Lista_di_controllo_degli_accessi) (ACL), che possono essere statiche (quindi modificabili solo tramite configurazione esplicita) o dinamiche (cioè che possono variare in base allo stato interno del sistema, come ad esempio nel [Port knocking](http://it.wikipedia.org/wiki/Port_knocking)).

Una funzione spesso associata al firewall è quella di [NAT](http://it.wikipedia.org/wiki/Network_address_translation) (traduzione degli indirizzi di rete), che può contribuire a rendere inaccessibili i calcolatori sulla rete interna.

Molti firewall possono registrare tutte le operazioni fatte (logging), effettuare registrazioni più o meno selettive (ad esempio, registrare solo i pacchetti che violano una certa regola, non registrare più di N pacchetti al secondo), e tenere statistiche di quali regole sono state più violate.

La registrazione integrale dell'attività di un firewall può facilmente assumere dimensioni ingestibili, per cui spesso si usa il logging solo temporaneamente per diagnosticare problemi, o comunque in modo selettivo (logging dei soli pacchetti rifiutati o solo di alcune regole). Tuttavia, l'analisi dei log di un firewall (o anche dei contatori delle varie regole) può permettere di individuare in tempo reale tentativi di intrusione.

Talvolta ad un firewall è associata anche la funzione *rilevamento delle intrusioni (*[*IDS*](http://it.wikipedia.org/wiki/Intrusion_detection_system)*)*, un sistema basato su euristiche che analizza il traffico e tenta di riconoscere possibili attacchi alla sicurezza della rete, e può anche scatenare reazioni automatiche da parte del firewall ([Intrusion prevention system](http://it.wikipedia.org/wiki/Intrusion_prevention_system)).

**Vulnerabilità**

Una delle vulnerabilità più conosciute di un firewall di fascia media è l'[HTTP tunneling](http://it.wikipedia.org/wiki/HTTP_tunneling), che consente di bypassare le restrizioni Internet utilizzando comunicazioni [HTTP](http://it.wikipedia.org/wiki/Hyper_Text_Transfer_Protocol) solitamente concesse dai firewall. Altra tipica vulnerabilità è la [dll injection](http://it.wikipedia.org/wiki/Dll_injection), ovvero una tecnica utilizzata da molti [trojan](http://it.wikipedia.org/wiki/Trojan), che sovrascrive il codice maligno all'interno di librerie di sistema utilizzate da programmi considerati *sicuri*. L'informazione riesce ad uscire dal computer in quanto il firewall, che di solito controlla i processi e non le librerie, crede che l'invio ad Internet lo stia eseguendo un programma da lui ritenuto sicuro, ma che di fatto utilizza la libreria contaminata. Alcuni firewall hanno anche il controllo sulla variazione delle librerie in memoria ma è difficile capire quando le variazioni sono state fatte da virus.

# GATEWAY

**Descrizione**

*Gateway* è un termine generico che indica il [servizio](http://it.wikipedia.org/wiki/Servizio) di inoltro dei pacchetti verso l'esterno; il dispositivo [hardware](http://it.wikipedia.org/wiki/Hardware) che porterà a termine questo compito è tipicamente un [router](http://it.wikipedia.org/wiki/Router). Nelle reti più semplici è presente un solo *gateway* che inoltra tutto il traffico diretto all'esterno verso la rete [internet](http://it.wikipedia.org/wiki/Internet). In reti più complesse in cui sono presenti parecchie [subnet](http://it.wikipedia.org/wiki/Subnet), ognuna di queste fa riferimento ad un *gateway* che si occuperà di [instradare](http://it.wikipedia.org/wiki/Instradamento) il [traffico](http://it.wikipedia.org/wiki/Traffico_(telecomunicazioni)) dati verso le altre sottoreti o a rimbalzarlo ad altri *gateway*.

Spesso i *gateway* non si limitano a fornire la funzionalità di base di *routing*, ma integrano altri servizi da e verso la rete locale come [proxy DNS](http://it.wikipedia.org/wiki/Proxy_DNS), [firewall](http://it.wikipedia.org/wiki/Firewall), [NAT](http://it.wikipedia.org/wiki/Network_address_translation) etc, che sono appunto servizi di strato di rete più elevato ovvero applicativo.

**Principio di funzionamento**

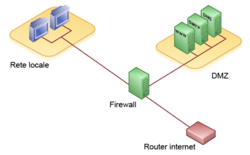
* Un [computer](http://it.wikipedia.org/wiki/Computer) connesso alla rete locale confronta i primi [bit](http://it.wikipedia.org/wiki/Bit) dell'indirizzo di destinazione (quelli che corrispondono a bit "1" nella propria [subnet mask](http://it.wikipedia.org/wiki/Subnet_mask)) dei dati da inviare con il [network prefix](http://it.wikipedia.org/w/index.php?title=Network_prefix&action=edit&redlink=1) (già noto) del proprio [indirizzo IP](http://it.wikipedia.org/wiki/Indirizzo_IP):
  + se corrispondono, significa che il computer di destinazione è sulla stessa rete locale;
  + se invece non corrispondono, il computer d'origine invia i dati al *gateway* predefinito, il quale si occuperà del loro successivo instradamento verso la rete remota di destinazione.
  + non possono stare in una rete 2 computer con lo stesso IP (conflitto IP; il secondo arrivato disattiva la propria scheda di rete)

# Demilitarized zone

Da Wikipedia, l'enciclopedia libera.

Vai a: [navigazione](http://it.wikipedia.org/wiki/Demilitarized_zone#mw-head), [cerca](http://it.wikipedia.org/wiki/Demilitarized_zone#p-search)

|  |  |
| --- | --- |
|  |  |

[](http://it.wikipedia.org/wiki/File:Demilitarized_Zone_Diagram_it.png)

[http://bits.wikimedia.org/static-1.20wmf12/skins/common/images/magnify-clip.png](http://it.wikipedia.org/wiki/File:Demilitarized_Zone_Diagram_it.png)

Diagramma di una rete che utilizza una DMZ creata utilizzando un firewall a tre connessioni (three-legged firewall).

Una **DMZ** (**demilitarized zone**) è un segmento isolato di [LAN](http://it.wikipedia.org/wiki/LAN) (una "[sottorete](http://it.wikipedia.org/wiki/Sottorete)") raggiungibile sia da [reti](http://it.wikipedia.org/wiki/Rete_informatica) interne sia esterne ma caratterizzata dal fatto che gli [host](http://it.wikipedia.org/wiki/Host) attestati sulla DMZ hanno possibilità limitate di connessione verso host specifici della rete interna.[[1]](http://it.wikipedia.org/wiki/Demilitarized_zone#cite_note-0)[[2]](http://it.wikipedia.org/wiki/Demilitarized_zone#cite_note-1)

Tale configurazione viene normalmente utilizzata per permettere ai [server](http://it.wikipedia.org/wiki/Server) posizionati sulla DMZ di fornire servizi all'esterno senza compromettere la [sicurezza](http://it.wikipedia.org/wiki/Sicurezza_informatica) della rete aziendale interna nel caso una di tali macchine sia sottoposta ad un [attacco informatico](http://it.wikipedia.org/wiki/Danneggiamento_informatico): per chi si connette dall'esterno dell'organizzazione la DMZ è infatti una sorta di "strada senza uscita" o "vicolo cieco".

Solitamente sulla DMZ sono infatti collegati i [server](http://it.wikipedia.org/wiki/Server) *pubblici* (ovvero quei server che necessitano di essere raggiungibili dall'esterno della rete aziendale - ed anche dalla [internet](http://it.wikipedia.org/wiki/Internet) - come, ad esempio, server [mail](http://it.wikipedia.org/wiki/Mail), [webserver](http://it.wikipedia.org/wiki/Webserver) e server [DNS](http://it.wikipedia.org/wiki/Domain_Name_System)) che rimangono in tal modo separati dalla LAN interna, evitando di comprometterne l'[integrità](http://it.wikipedia.org/w/index.php?title=Integrit%C3%A0&action=edit&redlink=1).

Una DMZ può essere creata attraverso la definizione di *policies* distinte su uno o più [firewall](http://it.wikipedia.org/wiki/Firewall).

Le connessioni dalle reti esterne verso la DMZ sono solitamente controllate tramite una tipologia di [NAT](http://it.wikipedia.org/wiki/Network_address_translation) chiamata "[port forwarding](http://it.wikipedia.org/wiki/Port_forwarding)" o "port mapping"[[3]](http://it.wikipedia.org/wiki/Demilitarized_zone#cite_note-2), implementata sul sistema che agisce da firewall.

Oltre al summenzionato firewall, di tipo packet filter (ossia che opera a [livello di trasporto](http://it.wikipedia.org/wiki/Livello_di_trasporto) - layer quattro della [pila ISO/OSI](http://it.wikipedia.org/wiki/Open_Systems_Interconnection)), è possibile implementare un differente approccio, impiegando un servizio di "[reverse proxy](http://it.wikipedia.org/wiki/Proxy)", operante all'interno di un cosiddetto 'application layer firewall', che agisce a [livello applicativo](http://it.wikipedia.org/wiki/Livello_applicazioni) (layer sette della pila ISO/OSI).

Il "reverse proxy", invece di fornire un servizio applicativo agli utenti interni ad una rete locale -tipico del proxy comune-, provvede a fornire un accesso (indiretto) a risorse interne alla rete locale (in DMZ in questo caso), provenienti da una rete esterna (tipicamente internet).