I firewall

Un firewall è un dispositivo che permette di filtrare il traffico di rete tra due (o più) interfacce, in base a determinate politiche (policy). L'utilizzo di un firewall rende possibile controllare chi accede ai servizi messi a disposizione dal sistema ed a quali altri sistemi si può accedere, offrendo la sicurezza desiderata ed eventualmente tracciando il traffico in un file, per poterlo controllare successivamente.

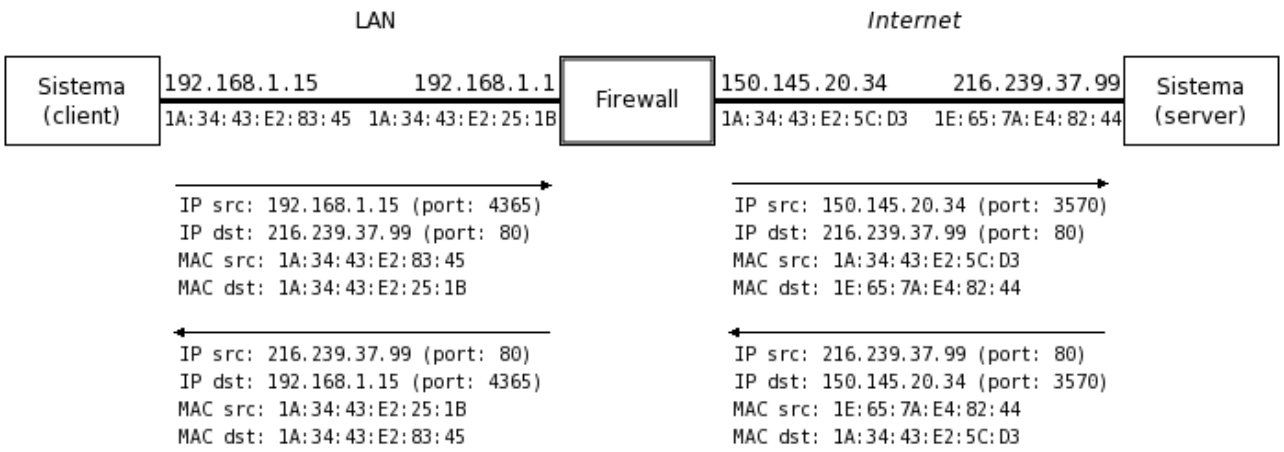
In commercio esistono apparecchi dedicati a svolgere il compito di firewall, spesso denominati firewall hardware per contraddistinguerli dai software che svolgono tale compito su macchine con sistemi operativi multipurpose, utilizzabili cioè per poterci lavorare in generale, che possono avere, come GNU/Linux, un firewall software. Questo non deve trarre in inganno poiché la politica di firewalling è comunque gestita attraverso un insieme di regole che vengono attuate attraverso un software. Esistono essenzialmente due tipologie di firewall:

- **Packet filter** esegue un filtraggio sui pacchetti che lo attraversano, dal livello fisico fino al livello di trasporto dello stack OSI. Ad esempio, un firewall di questo tipo può scartare i pacchetti che arrivano da interfacce di rete con un determinato indirizzo IP, o far passare soltanto il traffico relativo a determinate porte (TCP o UDP).
- **Proxy server** esegue un filtraggio sui pacchetti che lo attraversano, ai livelli più alti dello stack OSI. Un firewall di questo tipo (spesso denominato soltanto proxy server), può permettere, oltre alla gestione di caching delle pagine visitate, anche l'accesso o meno a determinate pagine web basandosi sul contenuto delle stesse.

Un firewall può essere caratterizzato in base alla possibilità di gestire il controllo sui pacchetti che lo attraversano dipendentemente dallo stato della relativa comunicazione. Si identificano così i seguenti tipi di firewall:

- **Stateless** il firewall non tiene conto dello stato della comunicazione, ma analizza i pacchetti isolatamente l'uno dall'altro, senza tener conto di nessuna correlazione tra essi.
- **Stateful** il firewall tiene conto dello stato della comunicazione, permettendo l'analisi dei pachetti in relazione, per esempio, al fatto che la comunicazione tra il mittente ed il destinatario sia già stata iniziata o meno. Un firewall di questo tipo è generalmente più sicuro rispetto ad uno stateless poiché permette di filtrare i pacchetti in maniera più selettiva.

I firewall in genere possono implementare funzionalità di **NAT (Network Address Translation)** e **PAT (Port Address Translation),** che consentono al firewall di modificare automaticamente l'indirizzo IP e/o la porta del mittente o destinatario del pacchetto. Queste funzionalità permettono a più sistemi collegati in una rete privata di poter accedere ad Internet attraverso il firewall.



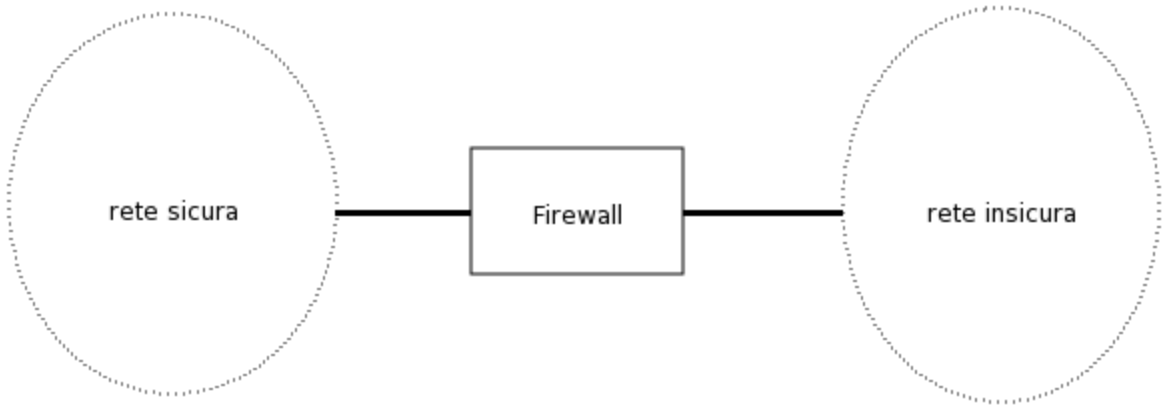
Il firewall infatti provvede a modificare opportunamente gli indirizzi IP del pacchetto. Si supponga che un sistema della rete privata con un interfaccia che ha l'indirizzo IP 192.168.1.15 voglia accedere al sito Internet con indirizzo IP 216.239.37.99. Se il firewall fungesse soltanto da router, il pacchetto inviato dall'interfaccia 192.168.1.15 avrebbe appunto 192.168.1.15 come indirizzo IP del mittente e 216.239.37.99 come indirizzo IP di destinazione. Questo funziona fintantoché il pacchetto arriva al server con interfaccia avente indirizzo IP 216.239.37.99. Ma quando questo provvede a rispondere al mittente (192.168.1.15), il pacchetto viene scartato (letteralmente buttato via) dal primo router ben configurato, poiché l'indirizzo IP 192.168.1.15 si riferisce ad una rete privata e non può essere utilizzato come indirizzo pubblico (per Internet). Quindi, per far comunicare l'interfaccia 192.168.1.15 con il sito 216.239.37.99 il firewall deve essere configurato per funzionare con il meccanismo di NAT: quando il pacchetto con indirizzo IP mittente 192.168.1.15 e destinatario 216.239.37.99 arriva al firewall, questo viene modificato dal firewall stesso che sostituisce l'indirizzo dell'interfaccia del mittente con l'indirizzo IP della sua interfaccia connessa ad Internet (150.145.20.34). Quindi inoltra il pacchetto. Quando l'interfaccia 216.239.37.99 riceve il pacchetto, essa lo elabora e quindi risponde al mittente, cioè all'indirizzo 150.145.20.34 (il firewall), che ricevendo il pacchetto di risposta e ricordandosi che quello si riferisce al pacchetto di richiesta precedentemente inviato dall'interfaccia 192.168.1.15 (questa informazione il firewall l'aveva precedentemente salvata all'interno della sua tabella di NAT) sostituisce l'indirizzo IP del destinatario del pacchetto con 192.168.1.15 (cioè l'indirizzo IP dell'interfaccia che aveva inviato il primo pacchetto) e quindi inoltra il pacchetto sulla LAN, in maniera tale che l'interfaccia 192.168.1.15 possa ricevere la risposta alla sua richiesta.

In questo modo è possibile far accedere ad Internet un insieme di computer connessi in una rete privata, senza dover assegnare ad ognuna delle loro interfacce un indirizzo IP valido per Internet. È chiaro che questo meccanismo permette a più macchine l'accesso ad Internet, ma questo avviene attraverso un'unica interfaccia e quindi le varie macchine si divideranno la banda di comunicazione a disposizione per tale accesso.

L'utilizzo di NAT implica anche il PAT sulla porta sorgente poiché più macchine comunicano con l'esterno. Si supponga ad esempio che una delle macchine presenti nella rete privata invii un pacchetto verso Internet con indirizzo IP del mittente 192.168.1.43 e porta mittente 5012. Il firewall esegue il NAT sostituendo l'indirizzo IP del mittente con quello della sua porta esterna (es. 194.143.24.15) e quindi tenta di inviare il pacchetto verso il destinatario. Se però un'altra macchina della rete privata avesse già instaurato una comunicazione con lo stesso server remoto dalla stessa porta mittente, il firewall deve cambiare la porta mittente (si ricordi che una connessione è univocamente identificata dalla quaterna <indirizzo_IP_mittente, porta_mittente, indirizzo_IP_destinatario, porta_destinatario>).

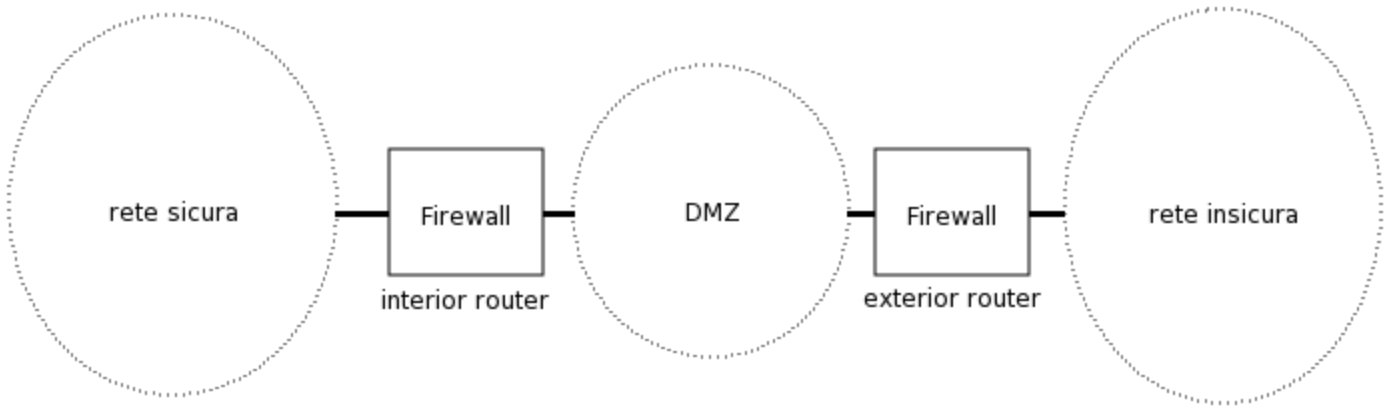
Screening router e DMZ

In genere un firewall viene frapposto tra una rete sicura (LAN) ed una rete insicura (Internet), per gestire le comunicazione che possono avvenire in entrambi i sensi. Tale tipologia di firewall, nota in letteratura anche con il nome screening router (router controllore), consistente essenzialmente da un firewall con due interfacce di rete, è l'architettura più semplice relativamente all'uso di un firewall. Infatti, sebbene il sistema che funge da firewall protegga la rete sicura da quella insicura, esso è l'unica difesa che si ha nei confronti di un attacco esterno: un'intrusione attraverso il firewall permetterà all'attaccante di avere accesso a tutti i sistemi presenti sulla rete sicura.



Utilizzo di un firewall come screening router.

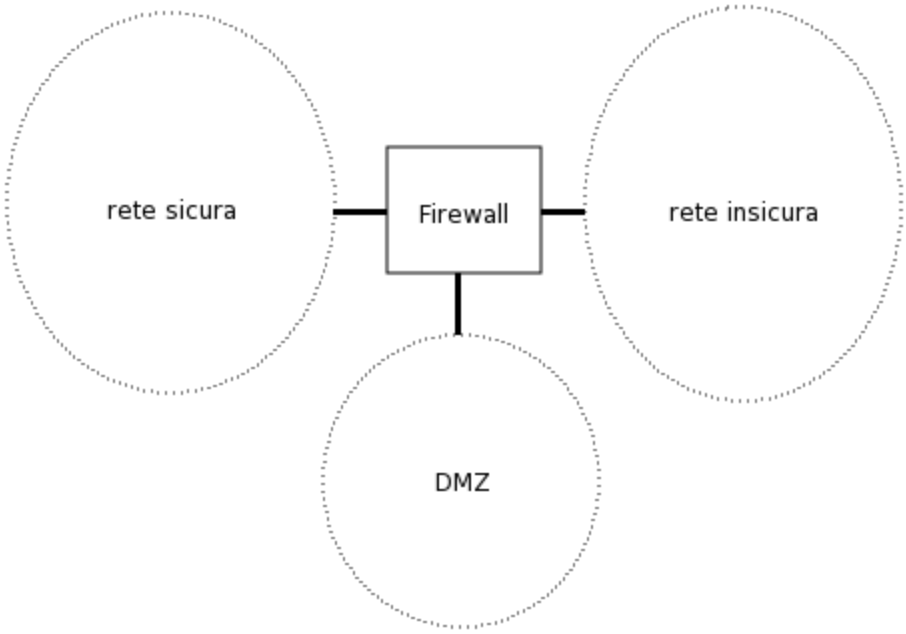
Per ridurre l'accessibilità ai sistemi della rete sicura, è necessario innanzi tutto individuare quali sono i sistemi che devono erogare un servizio verso la rete insicura. Poiché questi devono erogare un servizio, essi devono necessariamente essere raggiungibili dalla rete insicura, mentre gli altri sistemi possono non esserlo affatto. Quindi si può pensare di inserire due screening router in cascata, in modo da individuare tre reti distinte: quella insicura, quella mediamente sicura (in cui ci sono i server che erogano un servizio verso la rete insicura) e quella sicura.



Utilizzo di due firewall come screening router.

La rete mediamente sicura che si è venuta così a delineare è detta anche DMZ (De-Militarized Zone) e funge da rete perimetrale tra la rete insicura e quella sicura. In questo modo un'eventuale intrusione attraverso lo screening router più esterno (exterior router) consente l'accesso ai soli server presenti sulla DMZ, mentre la rete sicura rimane protetta da un ulteriore screening router (interior router). Tale architettura, conosciuta anche con il nome di screened subnet (sottorete controllata) è realizzabile anche per mezzo di un solo firewall con almeno tre interfacce di rete.

Ovviamente un solo firewall presenta il problema del single point of failure (singolo punto critico) sia per quanto riguarda i guasti, che dal punto di vista del rischio di manomissione, ma permette di mantenere logicamente separato il traffico tra le reti in questione e consente un risparmio sia in termini economici che di gestione.



Utilizzo di un firewall con tre interfacce di rete.

Tipologie di Firewall

Un firewall è quindi implementato da un software che serve a difendere un computer o una rete di computer da attacchi informatici . Questi tentativi di intrusione possono consistere in semplici scansioni di porte fino a veri e propri attacchi informatici del tipo DoS (Denial of Service). Gli attacchi tipo DoS hanno lo scopo di mandare fuori servizio una risorsa e questa può essere qualunque cosa come ad esempio la connessione a internet o un server di posta elettronica. Il port scanner, invece, non è un vero e proprio attacco ma consiste nel verificare quali porte sono eventualmente aperte con l'intento di sfruttare particolari vulnerabilità nel sistema operativo in uso o attivare programmi troian.

Il firewall analizza dunque il traffico e blocca tutti i dati che possono risultare pericolosi. Non disporre di un firewall significa essere esposti a numerosi attacchi e tentativi di intrusione. Il firewall diventa così uno dei programmi più efficaci per la gestione della sicurezza delle reti, grazie a meccanismi di controllo degli accessi in accoppiata con la possibilità di gestire delle regole per la sicurezza.

Un firewall è configurabile, si possono aggiungere o rimuovere i filtri, si può gestire l'accesso dei programmi ad Internet e permettere addirittura di decidere quali computer possono avere accesso ad Internet in una rete. Per esempio grazie ad una regola del firewall si può stabilire che solo un computer in una rete può accedere ad Internet, oppure un solo computer può usare il protocollo FTP o ricevere e mandare E-Mail.

I firewall si possono distinguere sostanzialmente in tre categorie: **Application Level Firewall**, **Packet Filter Firewall** e **Hardware Firewall.**

Application Level Firewall (o Proxy Server)

Questo tipo di firewall gestisce il traffico a livello di applicazione. Ciò significa che il firewall si basa su delle regole, prestabilite dall'utente, le quali gestiscono le applicazioni che possono avere accesso ad Internet. Lavorando a livello di applicazione, questo tipo di firewall può riconoscere comandi specifici delle applicazioni; sono i più facili da configurare e gestire, offrono un alto livello

di protezione a scapito però della velocità della rete, che può diminuire a volte anche di parecchio a seconda del traffico di dati da analizzare che essendo in alcuni casi considerevole, può rallentare la connessione.

Packet Filter Firewall

Questo tipo di firewall lavora ai livelli IP e TCP dello schema TCP/IP. Il Packet Filter Firewall quando riceve un pacchetto di dati lo compara con una serie di criteri prima di inoltrarlo o di rimandarlo al mittente. A seconda delle regole, il firewall può ignorare i pacchetti di dati, inoltrarli al sistema o rimandarli al mittente. I parametri che solitamente il packet Filter Firewall controlla nell'header del pacchetto sono l'indirizzo IP di origine e destinazione, numero della porta TCP/UDP di origine e destinazione e protocollo usato.

I Packet Filter Firewall possono usare un processo chiamato Network Address Translation (NAT) che permette di reindirizzare correttamente i pacchetti di rete in uscita dal sistema verso internet. Questo permette di nascondere la struttura della rete interna di una LAN, mascherando il pacchetto uscente come se provenisse da un host differente dal computer della rete interna.

Il packet Filter Firewall è la scelta migliore perché molto veloce e, proprio grazie a questa velocità e "superficialità" del controllo, non grava sulla connessione di rete e non la rallenta. Non è fondamentalmente legato al sistema operativo ma può essere configurato per funzionare su tutta la LAN, se messo alla fonte della connessione ad Internet.

Quindi per esempio, una e-mail contenente un virus può tranquillamente passare attraverso il firewall, se è consentito il traffico POP/SMTP. Non ha grandi possibilità di gestione dei dati all'interno del pacchetto dati, non prende decisioni in base al contenuto del pacchetto. Tutto ciò si trasforma in mancanza di features quali HTTP object caching o URL filtering e non possono filtrare le informazioni che passano dai computer interni verso l'esterno.

Hardware Firewall

I firewall hardware solitamente sono simili ai **Packet filter Firewall**, in quanto lavorano principalmente con la tecnica del **Packet filtering**. Possono usare anche un'altra tecnica chiamata **Stateful Packet Inspection** (SPI). la SPI permette un controllo non solo dell'header del pacchetto dati, bensì permette 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 analizzare lo stato della connessione e compilare le informazioni ottenute su una tabella così le operazioni di filtraggio dei pacchetti sono basate non solo su impostazioni definite dall'amministratore, ma anche sulla base di regole adottate con pacchetti simili scansionati già precedentemente dal firewall.

Network Address Translation

Nel campo delle reti telematiche, il **network address translation** o **NAT**, ovvero *traduzione degli indirizzi di rete*, conosciuto anche come **network masquerading, native address translation**, è una tecnica che consiste nel modificare gli indirizzi IP dei pacchetti in transito su un sistema che agisce da router. Sono molto note anche alcune tipologie specifiche di NAT, come l'*IP masquerading* e il *port forwarding*.

Tipi di NAT

Il NAT è spesso implementato dai router e dai firewall. Si può distinguere tra *source NAT* (SNAT) e *destination NAT* (DNAT), a seconda che venga modificato l'indirizzo sorgente o l'indirizzo destinazione del *pacchetto che inizia una nuova connessione*.

I pacchetti che viaggiano in senso opposto verranno modificati in modo corrispondente, in modo da dare ad almeno uno dei due computer che stanno comunicando l'illusione di parlare con un indirizzo IP diverso da quello effettivamente utilizzato dalla controparte.

Per implementare il NAT, un router ha quindi bisogno di effettuare il tracciamento delle connessioni, ovvero di tenere traccia di tutte le connessioni che lo attraversano. Per "connessione" in questo contesto si intende un flusso bidirezionale di pacchetti tra due host, identificati da particolari caratteristiche a livelli superiori a quello di rete (IP):

- nel caso di TCP è una connessione TCP in senso proprio, caratterizzata da una coppia di porte
- nel caso di UDP, per quanto UDP sia un protocollo di trasporto senza connessione, viene considerata connessione uno scambio di pacchetti UDP tra due host che usi la stessa coppia di numeri di porta.
- altri protocolli vengono gestiti in modo analogo, usando caratteristiche del pacchetto a livelli superiori ad IP per identificare i pacchetti che appartengono ad una stessa connessione.

Source NAT

Nel source NAT, le connessioni effettuate da uno o più computer vengono alterate in modo da presentare verso l'esterno uno o più indirizzi IP diversi da quelli originali. Quindi chi riceve le connessioni le vede provenire da un indirizzo diverso da quello utilizzato da chi le genera...

Storicamente il NAT si è affermato come mezzo per ovviare alla scarsità di indirizzi IP pubblici disponibili, soprattutto in quei paesi che, a differenza degli USA, hanno meno spazio di indirizzamento IP allocato pro-capite.

- Considerato che spesso gli indirizzi IP pubblici hanno un prezzo, per molti utenti Internet questo costo di indirizzi IP extra non sarebbe stato compensato dai benefici che avrebbero potuto ricavare.
- Le tecniche utilizzate per risparmiare indirizzi IP pubblici rendono i calcolatori non direttamente raggiungibili da internet, per cui spesso questa configurazione viene scelta per ragioni di sicurezza.

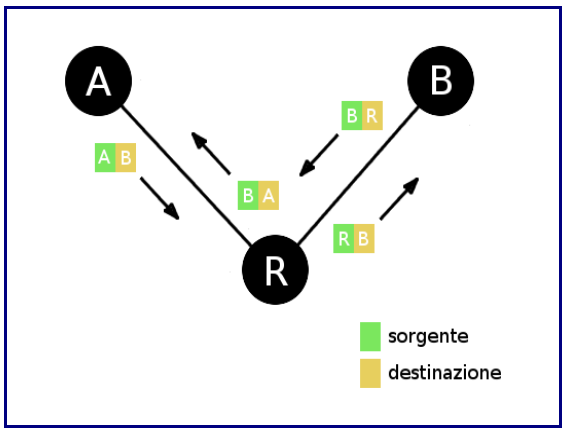
IP masquerading

Viene detto **IP masquerading** (a volte **NAT dinamico**) un caso particolare di source NAT, in cui le connessioni generate da un insieme di computer vengono "presentate" verso l'esterno con un solo indirizzo IP. La tecnica è detta anche *Port Address translation* (PAT), *IP Overloading* o NAPT (Network Address and Port Translation), in quanto vengono modificati non solo gli indirizzi IP ma anche le porte TCP e UDP delle connessioni in transito.

Questo metodo prevede di individuare una rete "interna" (che tipicamente utilizza indirizzi IP

privati) ed una "esterna" (che tipicamente utilizza indirizzi IP pubblici), e permette di gestire solo connessioni che siano originate da host della rete "interna".

Ciascuna connessione TCP o UDP viene gestita individualmente: quando la connessione viene iniziata, la porta sorgente originale può essere modificata, e il router NAT mantiene una tabella di corrispondenze tra porte sull'indirizzo esterno e corrispondenti porte e indirizzi IP privati. Quando riceve un pacchetto TCP o UDP sull'indirizzo IP esterno, consulta la tabella per sapere a quale host interno e su quale porta inviarlo. Il router NAT deve quindi tenere traccia di tutte le connessioni TCP e UDP attive tra la rete interna e quella esterna (e preoccuparsi di eliminare le voci inutilizzate da questa tabella mediante un meccanismo di scadenza). Alcune implementazioni modificano sistematicamente le porte sorgente di tutte le connessioni, utilizzando tipicamente numeri di porte molto alti (tipicamente sopra 61000), altre tendono a mantenere i numeri di porta originali, e li modificano solo se un numero di porta sorgente è utilizzato da due host contemporaneamente.



Un esempio di comunicazione mascherata.

Questa tecnica è spesso usata per collegare le Intranet (reti private sviluppate sul modello di Internet) ad Internet, permettendo di mantenere un piano di indirizzamento IP che non permetterebbe la connessione diretta ad internet, di risparmiare indirizzi IP pubblici e di "nascondere" all'esterno una rete privata. In una intranet, gli host utilizzano normalmente indirizzi IP privati, e necessitano di un dispositivo che possa effettuare la traduzione da indirizzo IP privato (valido nella sola Intranet) ad indirizzo IP pubblico (quindi utilizzabile in Internet), questo dispositivo può essere un host multicollegato che effettui relaying a livello 3 oppure un tipico router.

Alcuni host possono, però, avere la necessità di utilizzare un proprio ben determinato indirizzo pubblico in uscita pur conservando il proprio indirizzo privato. In questo caso tramite il **NAT statico** si può fare una mappatura 1:1 in cui è garantito il mascheramento ma l'unicità dell'host in uscita permette di tradurre solamente l'indirizzo IP sorgente lasciando inalterata la porta TCP/UDP.

Destination NAT

Nel destination NAT, le connessioni effettuate da uno o più computer vengono alterate in modo da venire redirette verso indirizzi IP diversi da quelli originali. Quindi chi effettua le connessioni si collega in realtà con un indirizzo diverso da quello che seleziona.

Possibili usi del *destination NAT*

- Port forwarding: in una configurazione di *masquerading*, può essere necessario che alcuni host o servizi di rete ospitati sulla rete "mascherata" siano accessibili dall'esterno. Per ottenere questo, viene utilizzata una configurazione detta Port forwarding, per cui le connessioni verso una determinata porta TCP o UDP dell'indirizzo esterno vengono redirette

verso un particolare host della rete interna.

- Bilanciamento del carico di lavoro: tramite il *destination NAT* si può realizzare un sistema in cui una connessione destinata ad un indirizzo IP viene reindirizzata a un altro indirizzo scelto tra quelli di un insieme di server che si hanno a disposizione. Questo permette di distribuire il carico di lavoro tra diversi server, migliorando così le prestazioni del servizio di rete offerto dal sistema.
- Gestione dei fallimenti: il *destination NAT* può essere usato per realizzare un sistema ad alta disponibilità. Un sistema di questo tipo deve essere sempre in grado di offrire il servizio di cui è responsabile. Tutti i server sono soggetti a possibili fallimenti. Se si fa uso di un router con *destination NAT*, il router può rilevare il fallimento del server principale e reindirizzare le connessioni a un server secondario, mantenendo così il servizio attivo.
- Trasparenza del servizio di proxy: il *destination NAT* può reindirizzare le connessioni (ad esempio HTTP) a un server speciale, chiamato *proxy*, che ha a disposizione una memoria temporanea in cui memorizza il contenuto di siti web visitati in precedenza. Se la connessione richiesta da un client è verso un indirizzo di cui il proxy ha già a disposizione il contenuto, esso invierà al client i dati richiesta senza la necessità di effettuare una vera connessione a Internet. Questa tecnica è usata dagli Internet Service Provider per ridurre l'uso della banda di trasmissione senza richiedere ai client di configurare il loro browser per il supporto del proxy, anche se ci sono delle controindicazioni.

Double NAT

Talvolta è necessario far comunicare tra loro due LAN, entrambe connesse ad Internet tramite *IP masquerading* (ad esempio, due sedi di una stessa azienda). In questi casi viene generalmente utilizzata una VPN (Virtual Private Network) tra i due router che connettono le reti ad Internet, indirizzando sulla VPN il traffico tra le due LAN.

In alcuni casi però capita che le LAN utilizzino gli stessi range di indirizzi IP, quindi non è possibile collegarle direttamente, ma sarebbe necessario *rinumerare* una delle due reti, ovvero riassegnare indirizzi IP in una diversa sottorete a tutti gli host. Questa operazione è normalmente faticosa, comporta disservizi e spese, per cui spesso si preferisce ricorrere a configurazioni di "double NAT", che nascondono reciprocamente le due reti, permettendo loro di comunicare come se non usassero indirizzi IP sovrapposti.

Le configurazioni di double NAT possono essere descritte come combinazioni di Source e Destination NAT.

Esempi di port forwarding

Come già detto, il port forwarding permette a computer esterni di connettersi a uno specifico computer della rete locale, a seconda della porta usata per la connessione. Ad esempio:

- il forwarding della porta 8000 dal router a un computer interno, permette a quel computer di usare il sistema Shoutcast.
- il forwarding delle porte dalla 6881 alla 6889 dal router a un computer interno, permette a quel computer di usare il sistema di condivisione file BitTorrent.

Operativamente, l'utente dal *browser* del proprio PC con un indirizzo "http:// *IP del router*" accede alle opzioni di configurazione del router, nel quale dichiara una sincronizzazione fra una porta del router e la corrispondente nel proprio PC.

Ad esempio nei programmi di file sharing, si potranno dichiarare le porte TCP1, UDP2, TCP3 (per l'accesso remoto). Le tre porte andranno impostate nel PC come predefinite per i protocolli TCP e UDP, e per l'accesso da remoto; nel *router* in una scheda per il *port forwarding* si dovranno inserire una *start port* del router e una *end port*, quella del PC, che saranno sincronizzate.

Perché il router riconosca il computer, è necessario creare un indirizzo IP statico. L'utente deve configurare sul PC l'ip del router come gateway predefinito, nel router sceglie un indirizzo IP fra quelli disponibili, nella configurazione del router trascrive l'IP scelto nell'elenco degli IP statici e vi aggiorna di conseguenza il range IP degli indirizzi disponibili.

Port triggering

In informatica, il **port triggering** è una tecnica simile al port forwarding, con la differenza che non c'è necessariamente bisogno di conoscere l'indirizzo IP del destinatario. Il port triggering agisce su tutta la LAN o su un intervallo di indirizzi IP (dipende dal modello di router) ed apre una porta non appena sente la richiesta di trasferimento.

Differenze con il port forwarding: Poniamo per esempio che venga usata la porta 5555 per richieste in uscita (upload) e contemporaneamente arrivi una richiesta in entrata sulla stessa porta. Nel port forwarding la richiesta in entrata non potrà passare e dovrà aspettare che la porta si liberi. Invece con il port triggering, il router aprirà temporaneamente un'altra porta (o altre) in modo da evitare le attese. Ecco perché è utile nel gaming online: in questi casi bisogna gestire molte richieste contemporanee in entrata e in uscita; trovare una porta occupata creerebbe ritardi meglio conosciuti come Lag_(informatica).