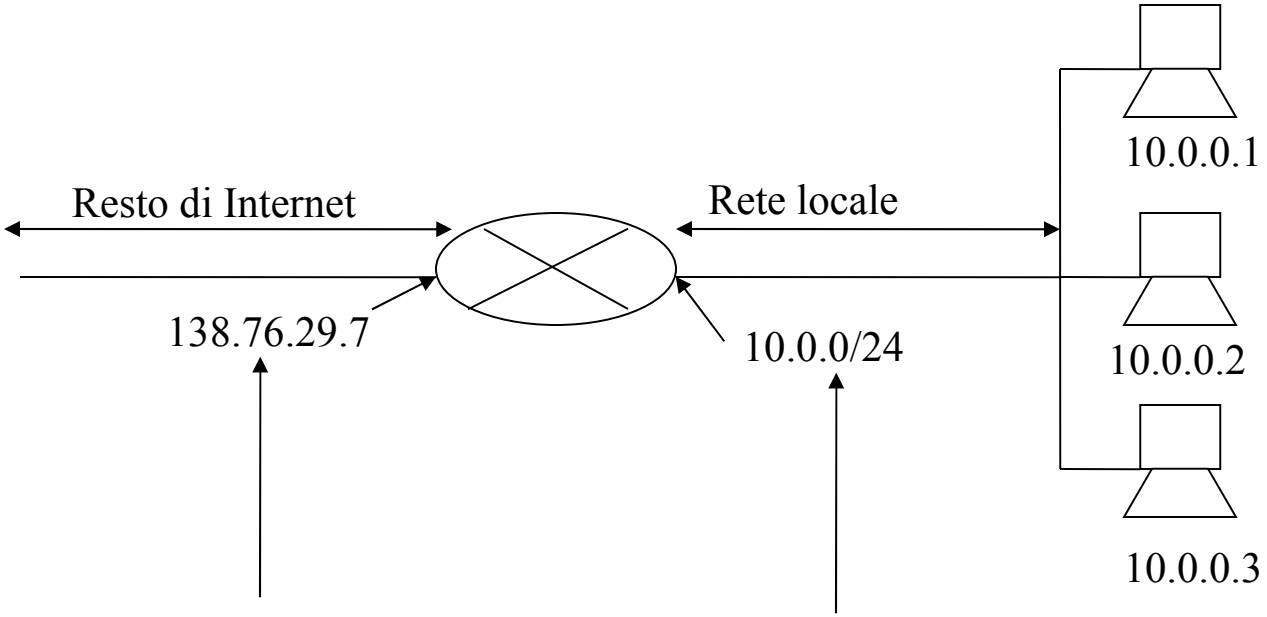
NAT & Firewalls
20/05/2008

NAT(NETWORK ADDRESS TRANSLATION) MOTIVAZIONI

- NAT(Network Address Translation) = Tecnica di filtraggio di pacchetti IP con sostituzione degli indirizzi (mascheramento)
- NAT = Consente la connessione di un insieme di hosts ad Internet utilizzando un unico indirizzo IP
- Vanatggi
  - risparmiare indirizzi IP (in attesa della piena diffusione di IPv6)
  - facilita l'amministazione della rete
  - aumenta la sicurezza

NAT:NETWORK ADDRESS TRANSLATION



Tutti i datagrammi che escono dalla rete hanno lo stesso indirizzo NAT 138.76.29.7, ma diversi numeri di porta

Tutti i datagrammi con sorgente/destinazione in questa sottorete hanno indirizzo 10.0.0/24 come sorgente/destinazione

NETWORK ADDRESS TRANSLATION

Motivazioni

- Risparmio di indirizzi IP: l'ISP attribuisce un solo indirizzo ad un insieme di hosts appartenenti alla stessa organizzazione. L'utente risparmia sul costo della connessione

- Facilità di amministrazione della rete:
  - si possono modificare gli indirizzi nella rete locale senza notificarlo al mondo esterno
  - Si può cambiare ISP senza modificare gli indirizzi della rete locale

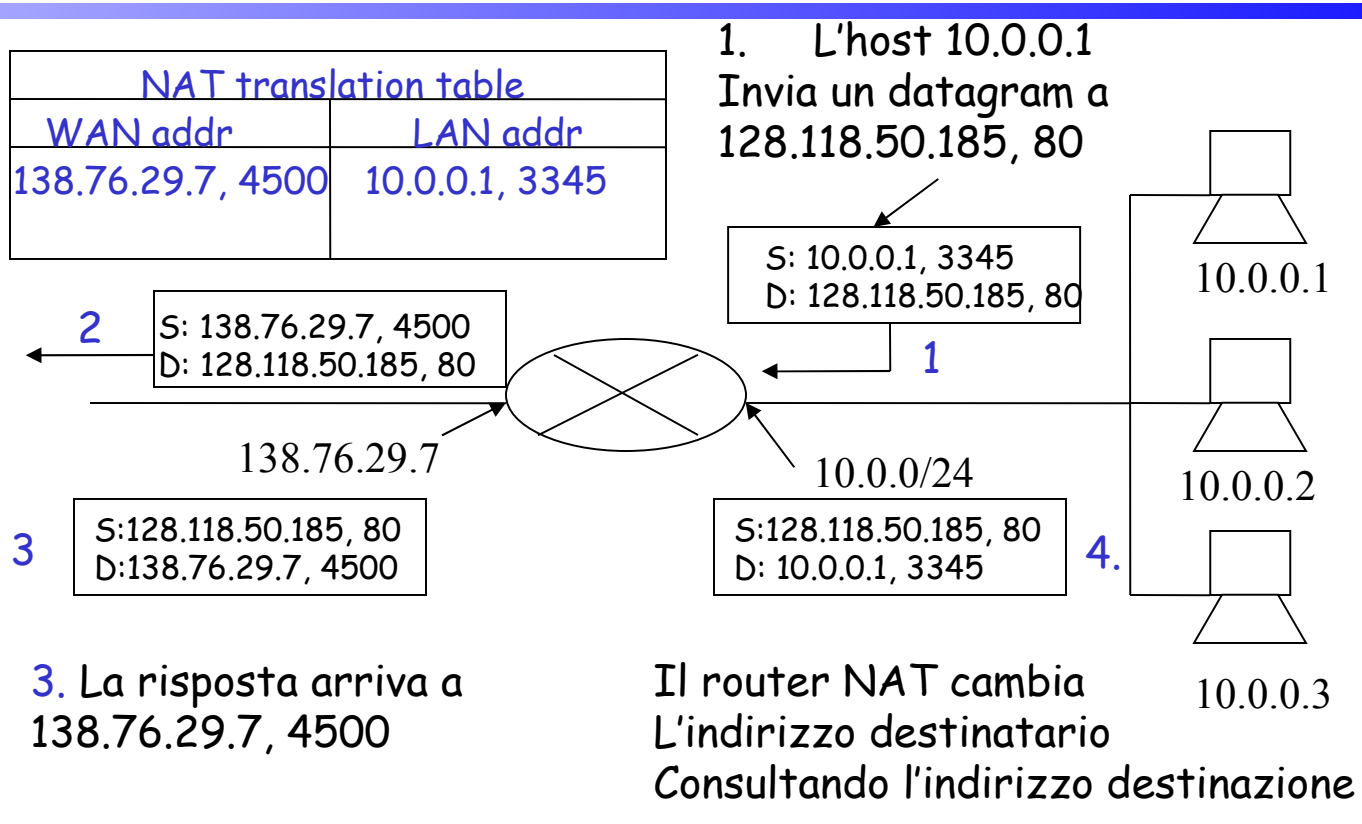
- Sicurezza gli hosts nella rete locale non sono visibili dall'esterno e quindi indirizzabili direttamente dall'esterno

NETWORK ADDRESS TRANSLATION

Funzioni di un router NAT

- sostituire in ogni datagram uscente la coppia (IP sorgente, #porta) con (NAT IP, #nuovaporta) dove #nuovaporta è un nuovo numero di porta generato dal NAT
- registrare in una tabella di traduzione la corrispondenza tra le due coppie
- Sostituire in ogni datagramma entrante la coppia (NAT IP, #nuovaporta) con il corrispondente (IP sorgente, #porta) memorizzato nella tabella di traduzione

NAT:NETWORK ADDRESS TRANSLATION



NETWORK ADDRESS TRANSLATION

- NAT : funziona solo con datagram IP che trasportano pacchetti a livello trasporto spediti mediante il protocollo UDP o il protocollo TCP

- Gli indirizzi assegnati alle sottoreti interne appartengono ad una delle seguenti zone
  - 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16

- Il router opera anche come dispositivo NAT

- Circa 60000 porte con 16 bit

  $\Rightarrow$

  circa 60000 connessioni aperte con un unico indirizzo IP

NETWORK ADDRESS TRANSLATION

- Vantaggi del NAT
  - Topologia della rete non visibile dall'esterno
  - Il NAT opera in modo trasparente per molte applicazioni
  - Spesso combinato con un firewall

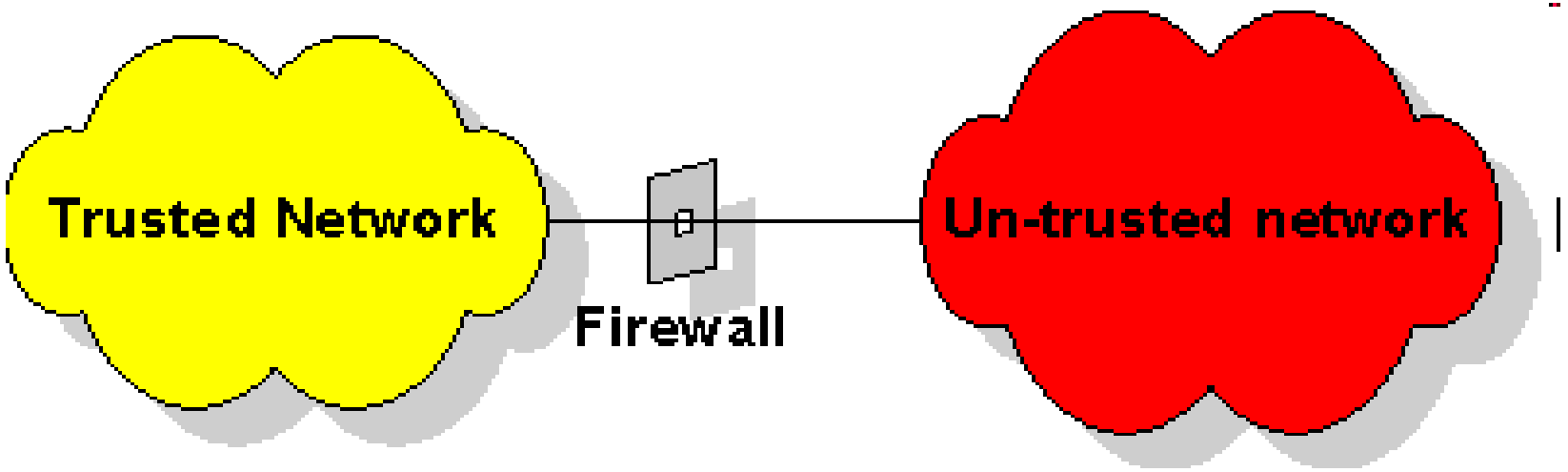
NETWORK ADDRESS TRANSLATION

- Svantaggi del NAT
  - Il router manipola i numeri di porta (livello trasporto), mentre dovrebbe operare solo fine al livello 3 (IP)
  - Rende più complessa la raggiungibilità degli host sulla rete

    $\Rightarrow$

    difficoltà di sviluppo di applicazioni P2P
  - Alcune applicazioni non sono trasparenti al NAT (esempio applicazioni che contengono indirizzi IP e numeri di porta nel payload)
    - Esempio:FTP utilizza due connessioni parallele, una per l'interazione con il server, l'altra per il trasferimento dati da e verso il server.I parametri della seconda (porta su cui spedire i dati) connessione sono inclusi nel payload della prima
- Obiettivo: eliminare NAT con la diffusione di IPv6

FIREWALLS: CARATTERISTICHE PRINCIPALI



- firewall: punto di controllo e di monitoraggio, collega reti con diversi livelli di affidabilità e delimita la rete da difendere (es:isola la rete interna di una organizzazione dalla rete pubblica)
- impone limitazioni ai servizi di rete disponibili (solo il traffico autorizzato attraversa la rete

FIREWALLS: CARATTERISTICHE PRINCIPALI

Una semplice politica di sicurezza:

- Permettere agli utenti della trusted network di accedere a servers esterni (eventualmente scegliendo quali), ma non permettere accessi dall'esterno verso la trusted network (ad esempio ad un server locale)

- Per implementare politiche simili, il firewall deve conoscere
  - L'applicazione a cui ci si intende connettere
  - La direzione della connessione

- Applicazione individuabile mediante il numero di porta (porta di ricezione, es porta 80 per www, porta 25 per e-mail,…)

- Stabilire la direzione della comunicazione può risultare più complesso

FIREWALLS: TIPI

Packet filter:

- analizza separatamente l'header di ogni pacchetto in transito.
- decide quali pacchetti devono/non devono essere inoltrati sulla base di un insieme di regole

Esempio:

< 192.12.13.14, 1234, 128.7.6.5, 80>

Filtrare (non trasmettere) tutti i pacchetti provenienti dalla porta 1234 dell'host 192.12.13.14 , indirizzati alla porta 80 dell'host 128.7.6.5

Regole di filtraggio basate su:

- IP mittente e destinatario,
- porte mittente e destinatario
- flags TCP (SYN,numeri di sequenza,…)

FIREWALLS: TIPI

Packet Filter:

- Le regole possono contenere indirizzi parziali (prefissi, range, wildcards)
- Per specificare le regole: *default deny (ciò che non è espressamente permesso è vietato)*
- Definizione statica/dinamica dei filtri
  - Definizione dinamica dei filtri può risultare necessaria nel caso di default deny, quando il numero di porta su cui viene attivata una connessione può essere stabilito solo dinamicamente

    Esempio: FTP instaura una nuova connessione TCP per ogni file trasferito. Le porte utilizzate sono stabilite al momento della connessione

FIREWALLS: CARATTERISTICHE PRINCIPALI

Packet Filtering, una semplice politica di sicurezza

- Bloccare le richieste di connessione TCP provenienti dalla rete esterna (tutti i SYN provenienti dall'esterno vengono scartati)
- Pacchetti provenienti dall'interno e destinati alla porta 80 (www) vengono accettati
- Pacchetti provenienti dall'interno e destinati alla porta 25 (smtp) vengono accettati

Più difficile definire politiche di sicurezza per UDP

FIREWALLS: TIPI

- Stateful inspection: analizza i pacchetti nel contesto di una sequenza
  - tiene traccia delle relazioni tra i pacchetti
  - consente di implementare politiche di filtraggio più complesse (esempio: riconoscimento di pacchetti TCP anomali che non fanno parte di alcuna connessione)

Esempio: ricorda le sessioni aperte dalla rete verso l'esterno e controlla che tutti i pacchetti che entrano successivamente appartengano ad una delle sessioni aperte

NAT E FIREWALLS

- Il NAT impedisce l'accesso dall'esterno alla rete interna
- Privatezza
  - Su numero di hosts interni
  - Difficoltà ad individuare specifici hosts
  - Può effettuare filtraggio di informazioni
- Ma se una connessione è aperta da un host interno alla rete il NAT non fornisce alcun tipo di protezione. Occorre un firewall.