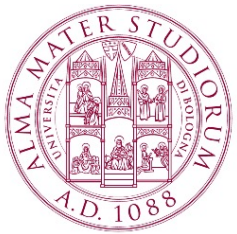
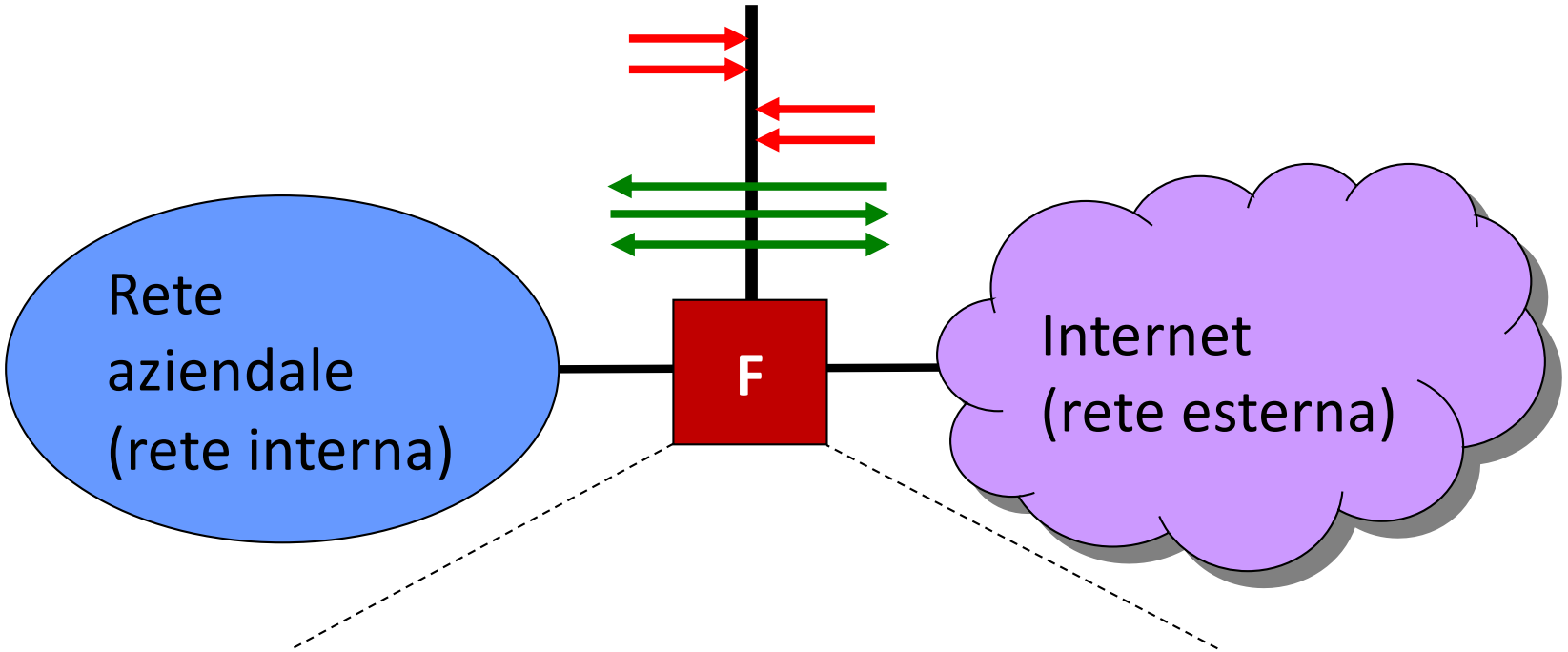


ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

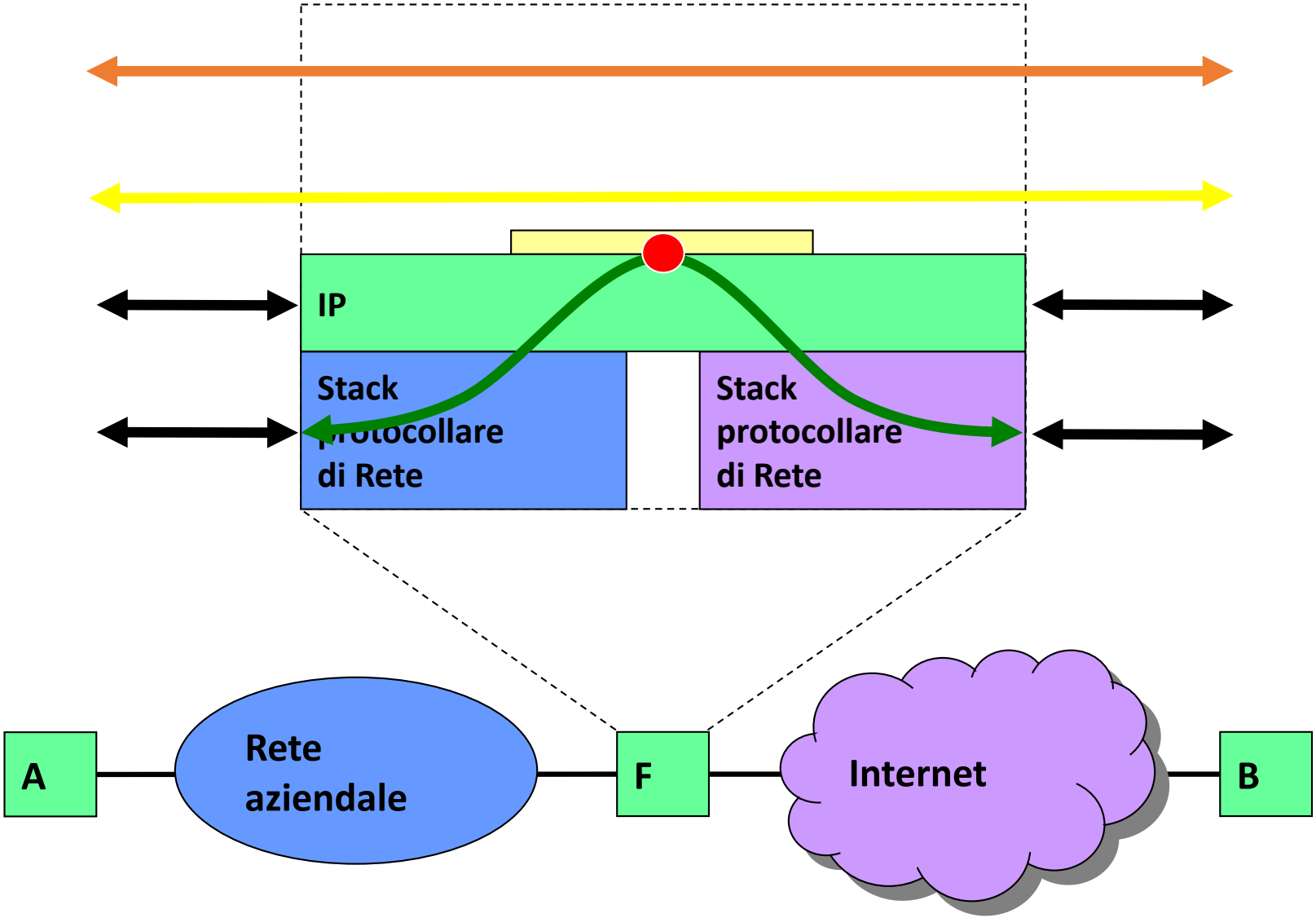
Packet Filter e Firewall

Il firewall



- Il firewall si interpone fra rete interna (da proteggere) e rete esterna (da cui possono provenire le minacce)
- È un apparato che può essere co-localizzato con il gateway
- Permette il passaggio di alcuni pacchetti (frecce verdi) e blocca quello di altri (frecce rosse)

Instradamento selettivo: packet filter



Packet filter

- Prende decisioni in base al contenuto dei campi del protocollo IP
  - IP sorgente
  - IP destinazione
  - Protocollo di livello superiore (campo protocol)
- Tipicamente confronta questi parametri con delle liste di accesso (Access Control List o ACL) che specificano le regole di comportamento
  - ACCEPT: il pacchetto viene instradato correttamente
  - DENY: il pacchetto viene bloccato e cancellato
  - REJECT: il pacchetto viene bloccato e viene inviato un messaggio di errore alla sorgente (similmente a DESTINATION UNREACHABLE)
- Alcuni esempi di regole ACL
  - `deny icmp any host 10.0.1.54`
  - `permit tcp host 10.0.0.37 host 10.1.1.230`
  - `deny icmp 10.0.0.0 0.0.0.255 host 10.0.0.254`

Packet filter e trasporto

- Un packet filter può anche permettere di creare ACL più complesse che includono informazioni prese del livello di trasporto
  - Porta sorgente
  - Porat destinazione
- In questo caso le ACL risultano più articolate
  - `deny 10.0.10.0 0.0.0.255 host 10.0.1.254 80`
  - `permit tcp 10.0.0.37 10.1.1.230`

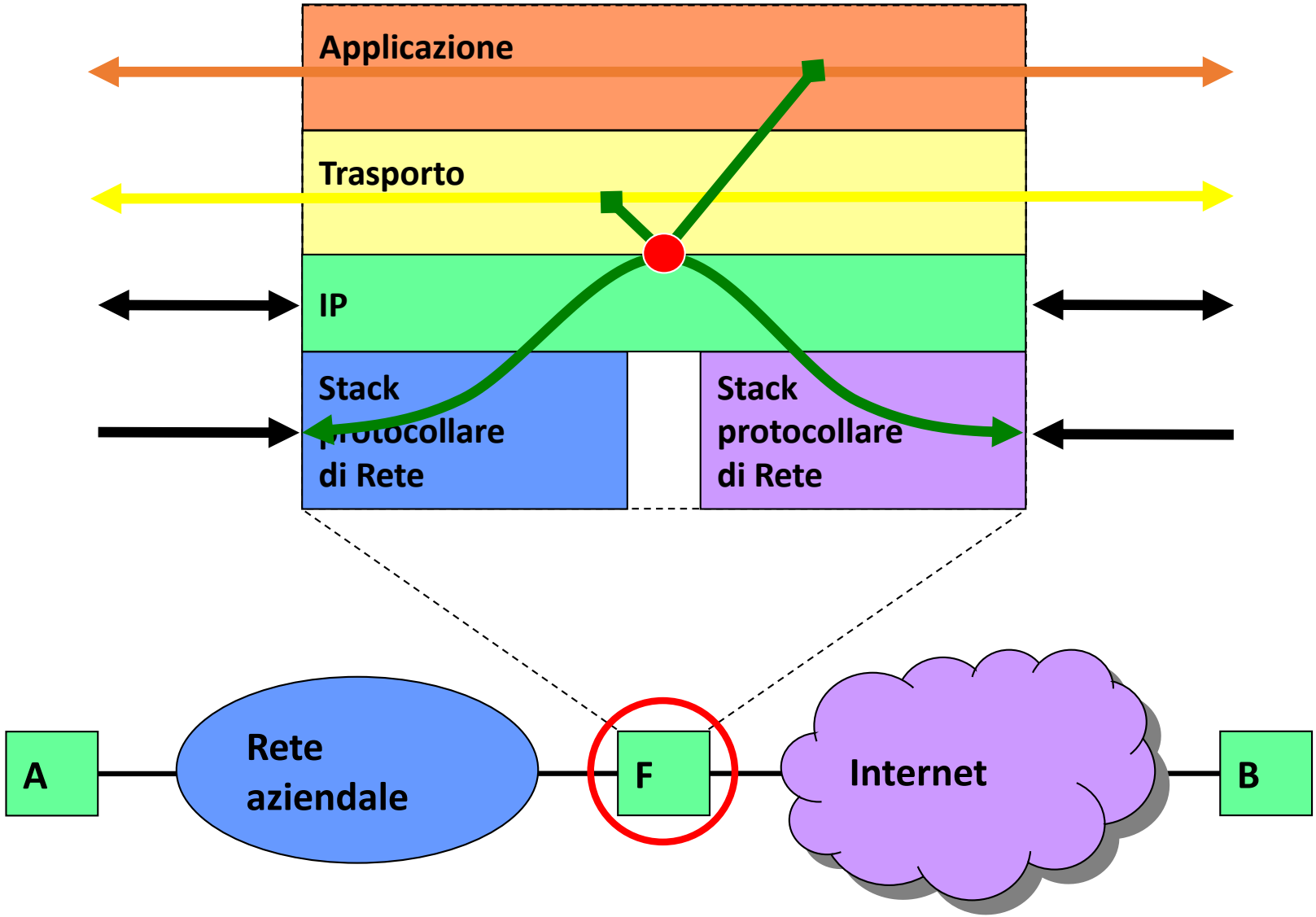
- Il packet filter è comunque un dispositivo «stateless» che controlla pacchetto per pacchetto ma che non tiene conto di possibili correlazioni fra pacchetti successivi
- Questo lo rende facilmente attaccabile per esempio con un semplice *IP spoofing* (modifica dell'indirizzo IP)

Default policy

- Normalmente le ACL vengono consultate sequenzialmente
- La prima regola che risulta vera conclude la lettura e viene applicata

- Un packet filter può essere configurato con una politica di **default**
- Default accept
  - Tutto il traffico può passare escluso quello esplicitamente indicato nella ACL
  - `permit any any`
- Default deny
  - Tutto il traffico viene bloccato escluso quello esplicitamente indicato nella ACL
  - `deny any any`

Stateful Packet Inspection



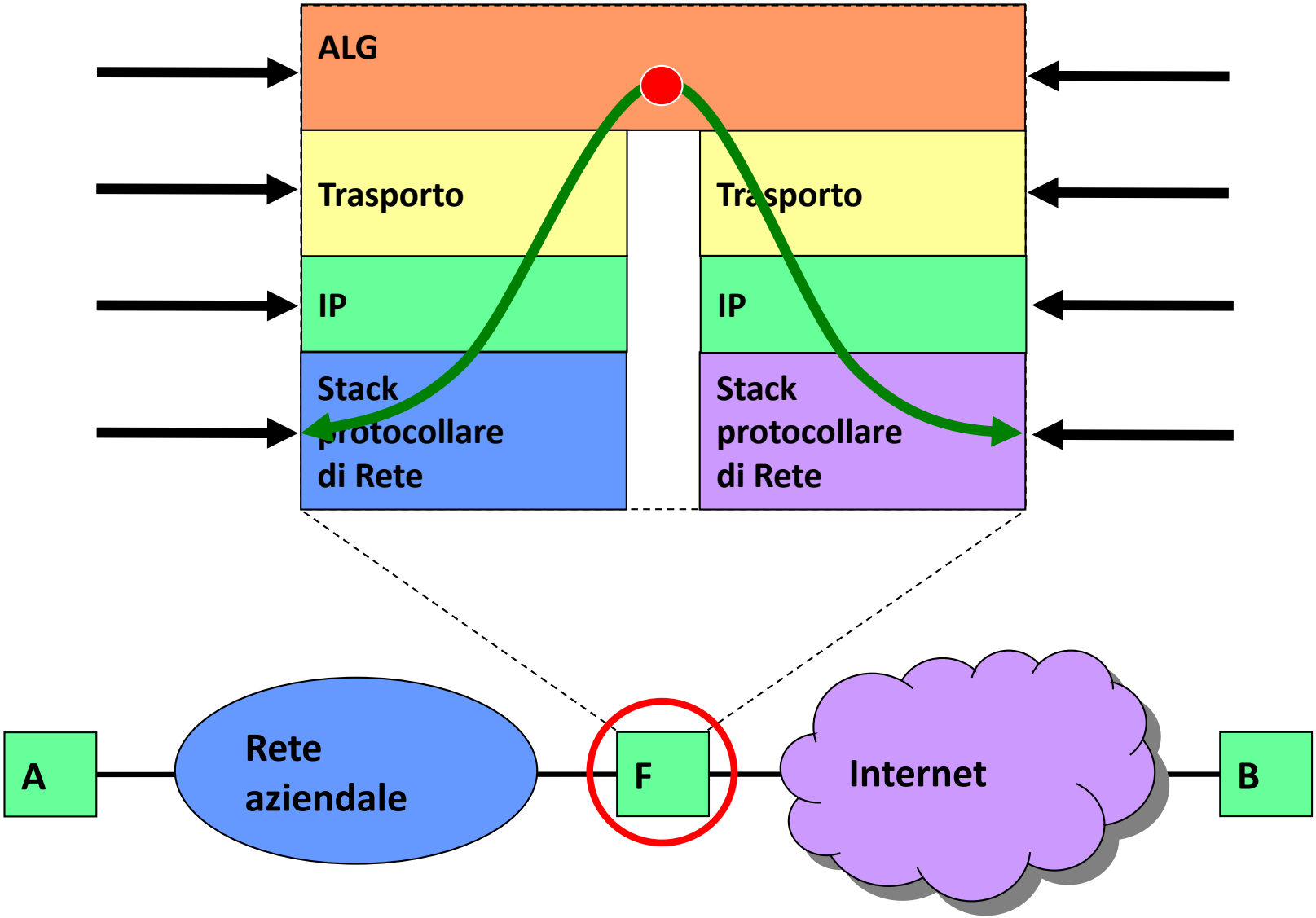
Stateful Packet Inspector

- Simile a un packet filter ma capace di tenere memoria della correlazione fra pacchetti in funzione delle connessioni a livello di trasporto
  - Comprende il three ways handshake del TCP e memorizza le connessioni aperte
  - Permette l'apertura delle connessioni in base alla direzione (incoming – outgoing)

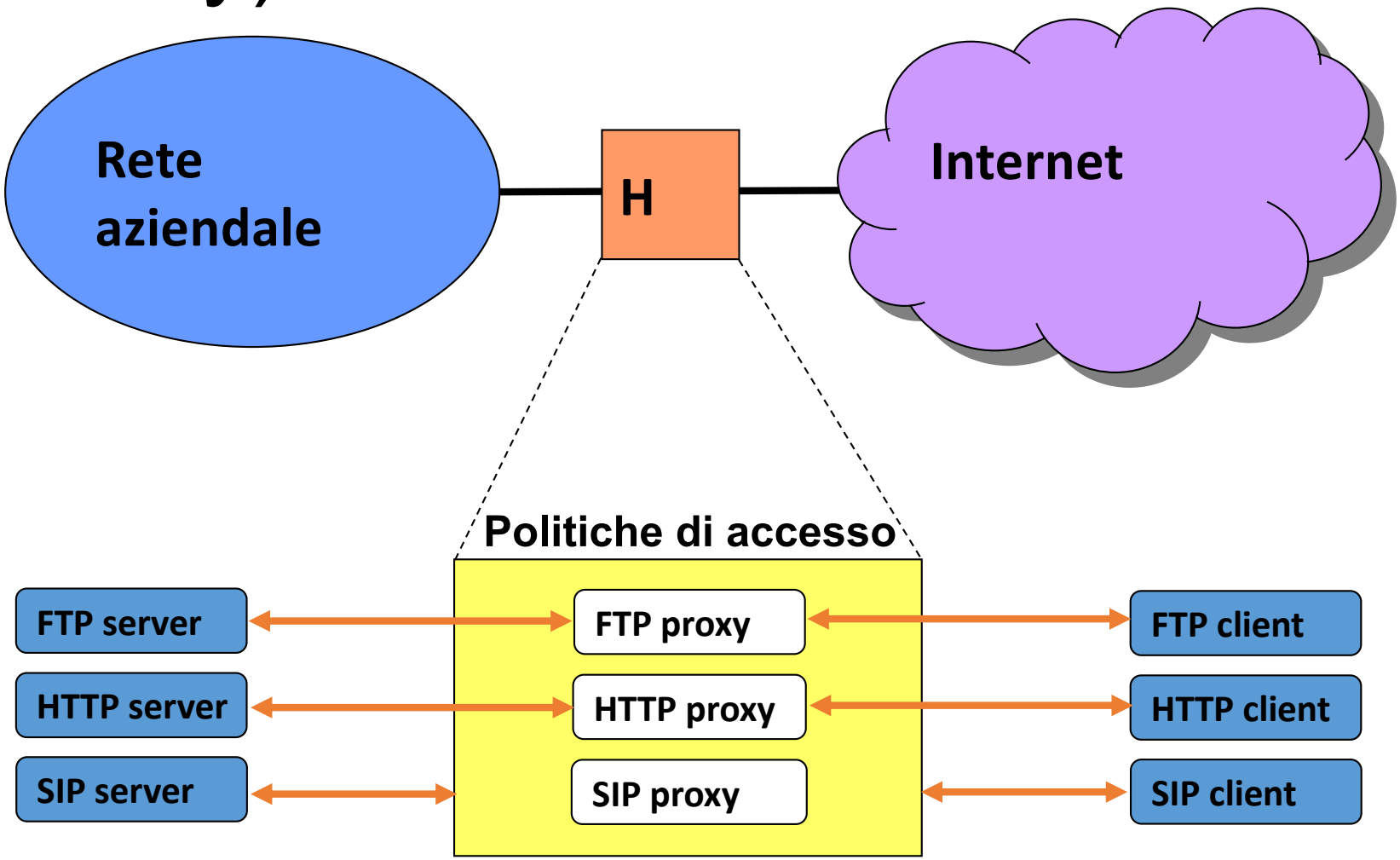
- L'implementazione può anche supportare dinamiche complesse all'interno dello stesso protocollo (dialogo multi connessione)

- Maggiore sicurezza rispetto al semplice packet filter
  - Se permette solo connessioni in uscita, previene azioni di port scanning dalla rete esterna verso la rete interna
  - Blocca tipologie di attacco basate sull'apertura della connessione (SYN flood)

Application Layer Gateway (Proxy)

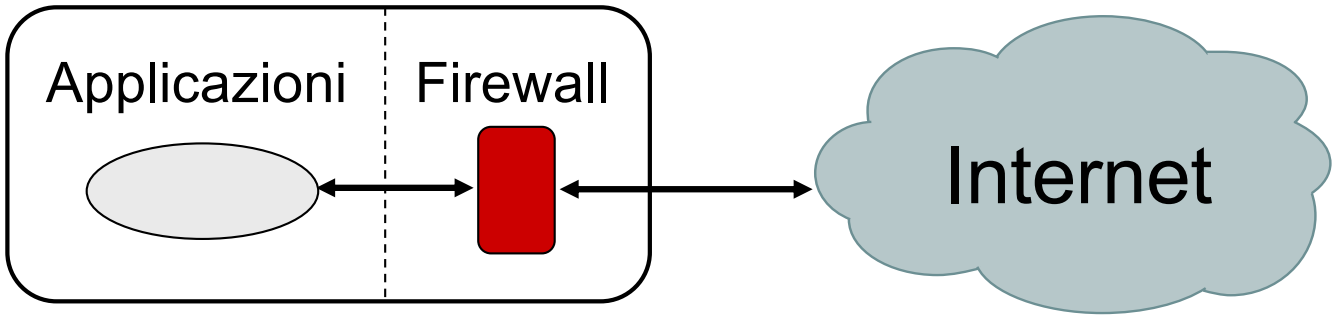


Application Layer Gateway (Proxy)



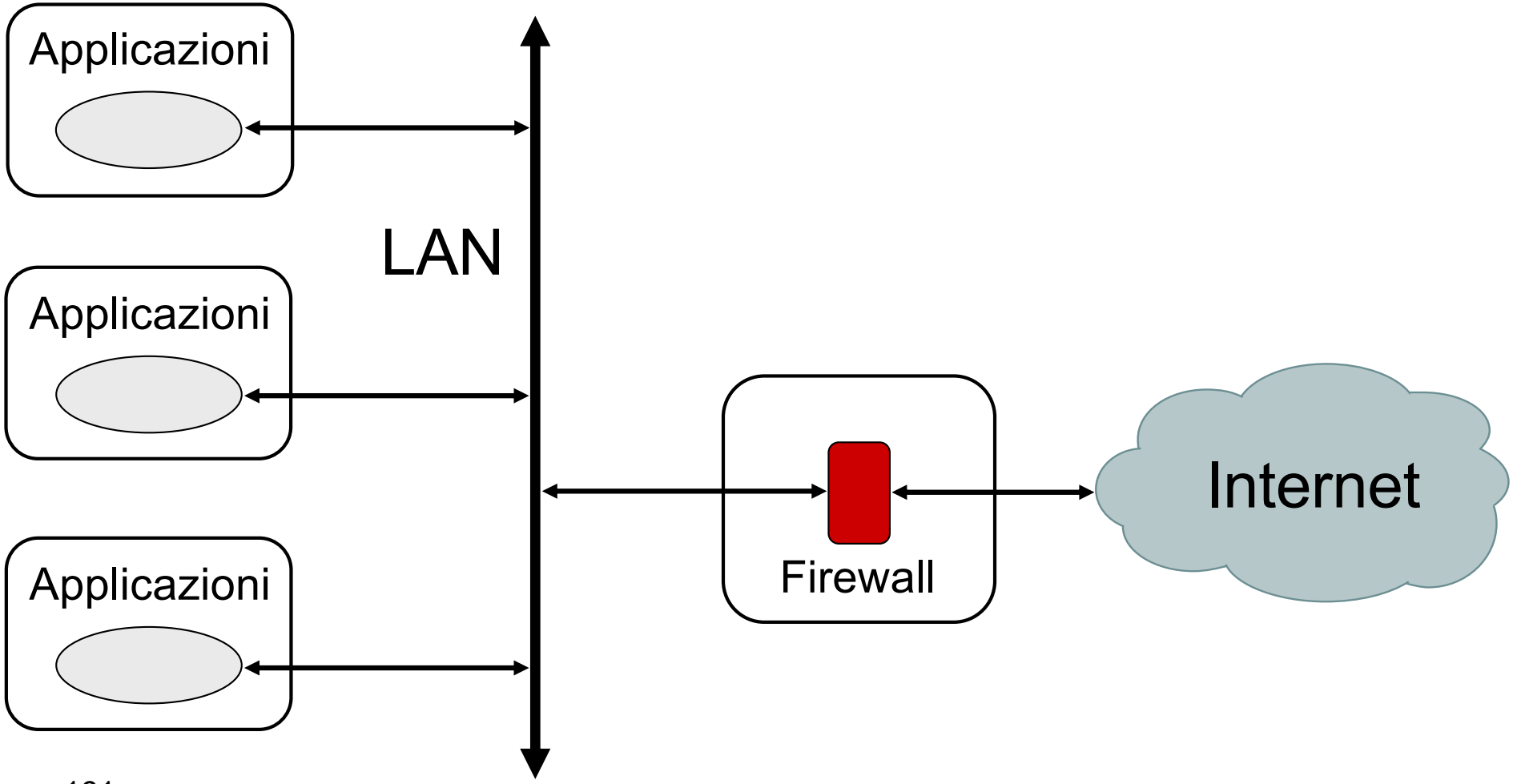
Protezione di host: firewall

- Un firewall è un filtro software/hardware che serve a proteggersi da accessi indesiderati provenienti dall'esterno della rete
- Può essere semplicemente un programma installato sul proprio PC che protegge quest'ultimo da attacchi esterni
  - tipicamente usato in accessi domestici a larga banda (ADSL, FTTH)



Protezione di rete: firewall

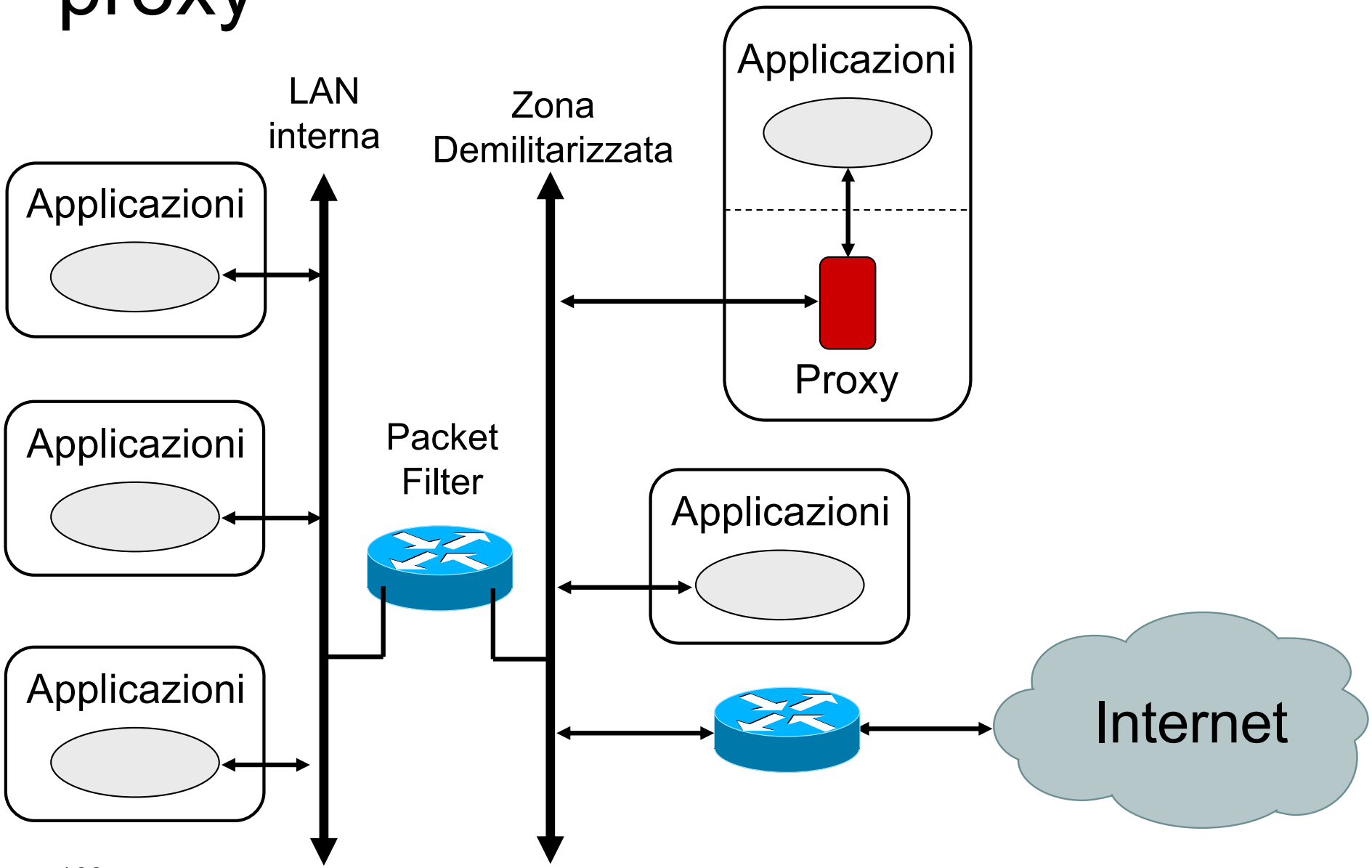
- Oppure può essere una macchina dedicata che filtra tutto il traffico da e per una rete locale



Protezione di rete: firewall

- Tutto il traffico fra la rete locale ed Internet deve essere filtrato dal firewall
- Solo il traffico autorizzato deve attraversare il firewall
- Si deve comunque permettere che i servizi di rete ritenuti necessari siano mantenuti
- Il firewall deve essere per quanto possibile immune da problemi di sicurezza sull'host

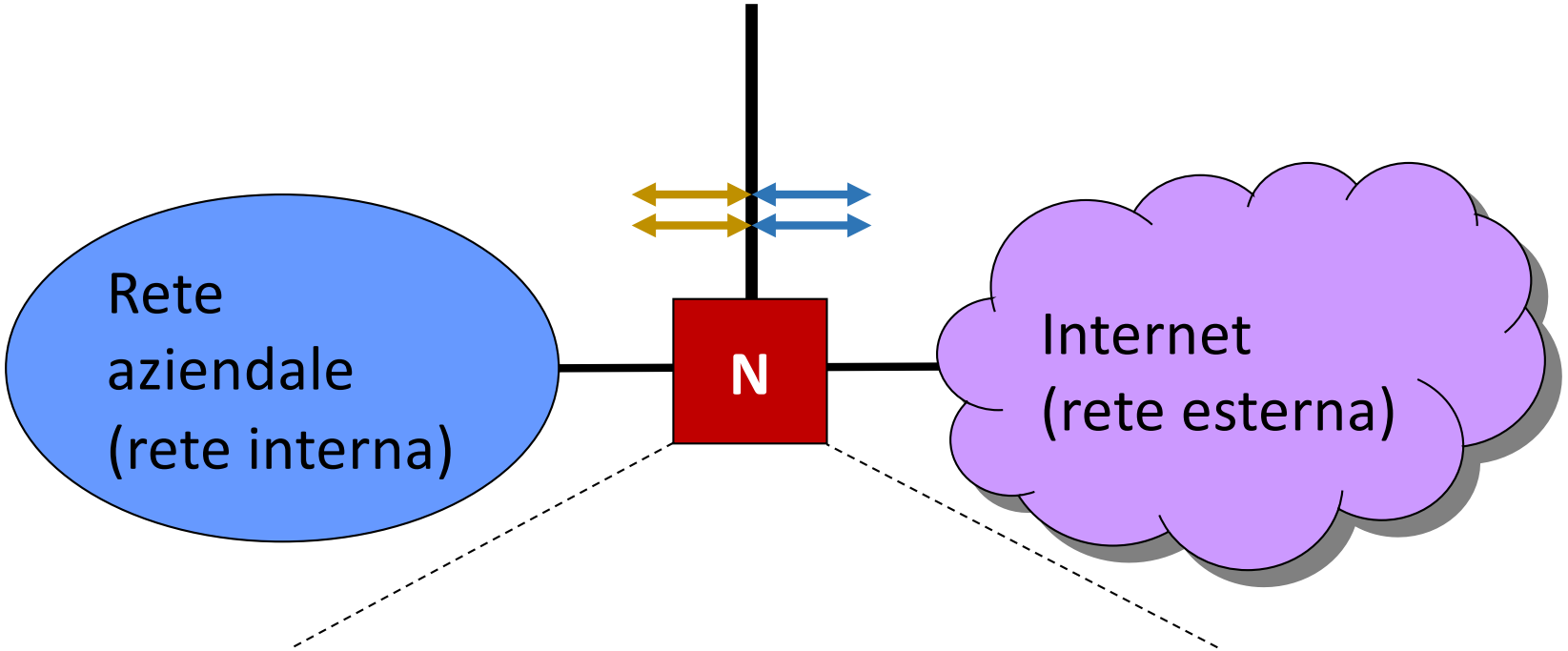
Configurazione di packet filter e proxy



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Network Address Translation

Il Network Address Translation



- Il NAT si interpone fra rete interna e rete esterna
- Analizza e modifica gli header dei pacchetti in ingresso/uscita con lo scopo di cambiare gli indirizzi degli end-point
  - Agisce su numeri IP e su numeri di porta

Indirizzi IP privati

- Le RFC 1918 (for IPv4) and RFC 4193 (for IPv6) definisco degli intervalli di indirizzi IP destinati a reti IP utilizzate da enti per finalità interne e quindi non connesse alla rete globale
- Spazi IPv4 privato:
- 10.0.0.0 a 10.255.255.255 (10.0.0.0/8)
- 172.16.0.0 a 172.31.255.255 (172.16.0.0/12)
- 192.168.0.0 a 192.168.255.255 (192.168.0.0/16)

RFC1918

Hosts within enterprises that use IP can be partitioned into **three categories**:

Category 1: hosts that do not require access to hosts in other enterprises or the Internet at large; hosts within this category may use IP addresses that are unambiguous within an enterprise, but may be ambiguous between enterprises.

Category 2: hosts that need access to a limited set of outside services (e.g., E-mail, FTP, netnews, remote login) which can be handled by mediating gateways (e.g. application layer gateways). For many hosts in this category an unrestricted external access (provided via IP connectivity) may be unnecessary and even undesirable for privacy/security reasons. Just like hosts within the first category, such hosts may use IP addresses that are unambiguous within an enterprise, but may be ambiguous between enterprises.

Category 3: hosts that need network layer access outside the enterprise (provided via IP connectivity); hosts in the last category require IP addresses that are globally unambiguous.

We will refer to the hosts in the first and second categories as "**private**".
We will refer to the hosts in the third category as "**public**".

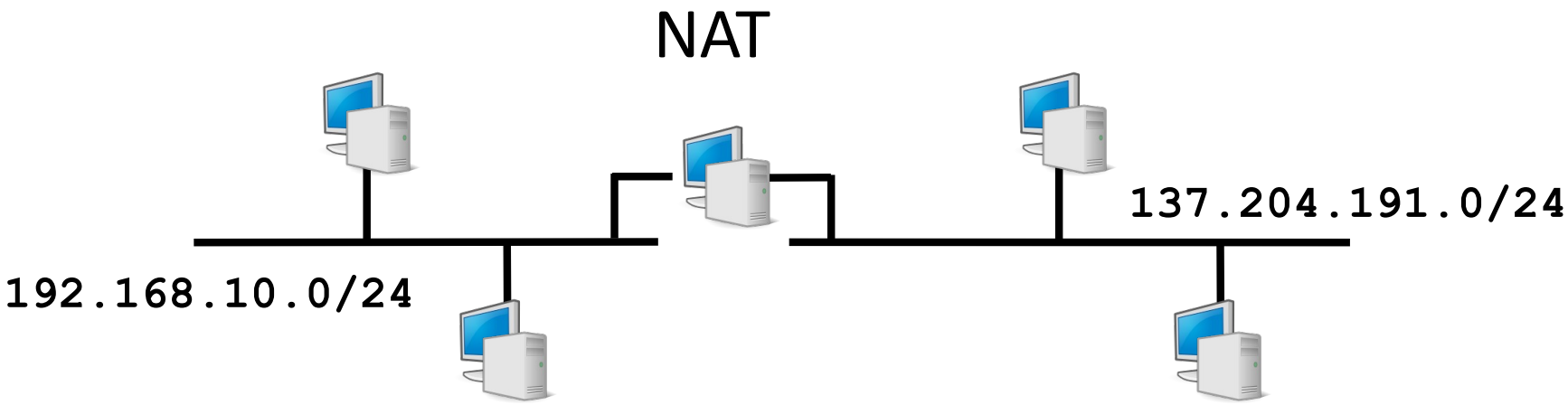
RFC1918

Because private addresses have no global meaning, **routing information about private networks shall not be propagated on inter-enterprise links**, and packets with private source or destination addresses should not be forwarded across such links. Routers in networks not using private address space, especially those of Internet service providers, are expected to be configured **to reject (filter out) routing information about private networks**. If such a router receives such information the rejection shall not be treated as a routing protocol error.

Indirect references to such addresses should be contained within the enterprise. Prominent examples of such references are DNS Resource Records and other information referring to internal private addresses. In particular, Internet service providers should take measures to prevent such leakage.

NAT

- Tecnica per il filtraggio di pacchetti IP con sostituzione degli indirizzi (mascheramento)
  - Indirizzi e porte
- Definito nella RFC 3022 per permettere a reti IP private l'accesso a reti IP pubbliche tramite un apposito gateway
- Utile per il risparmio di indirizzi IP pubblici e il riutilizzo di indirizzi IP privati



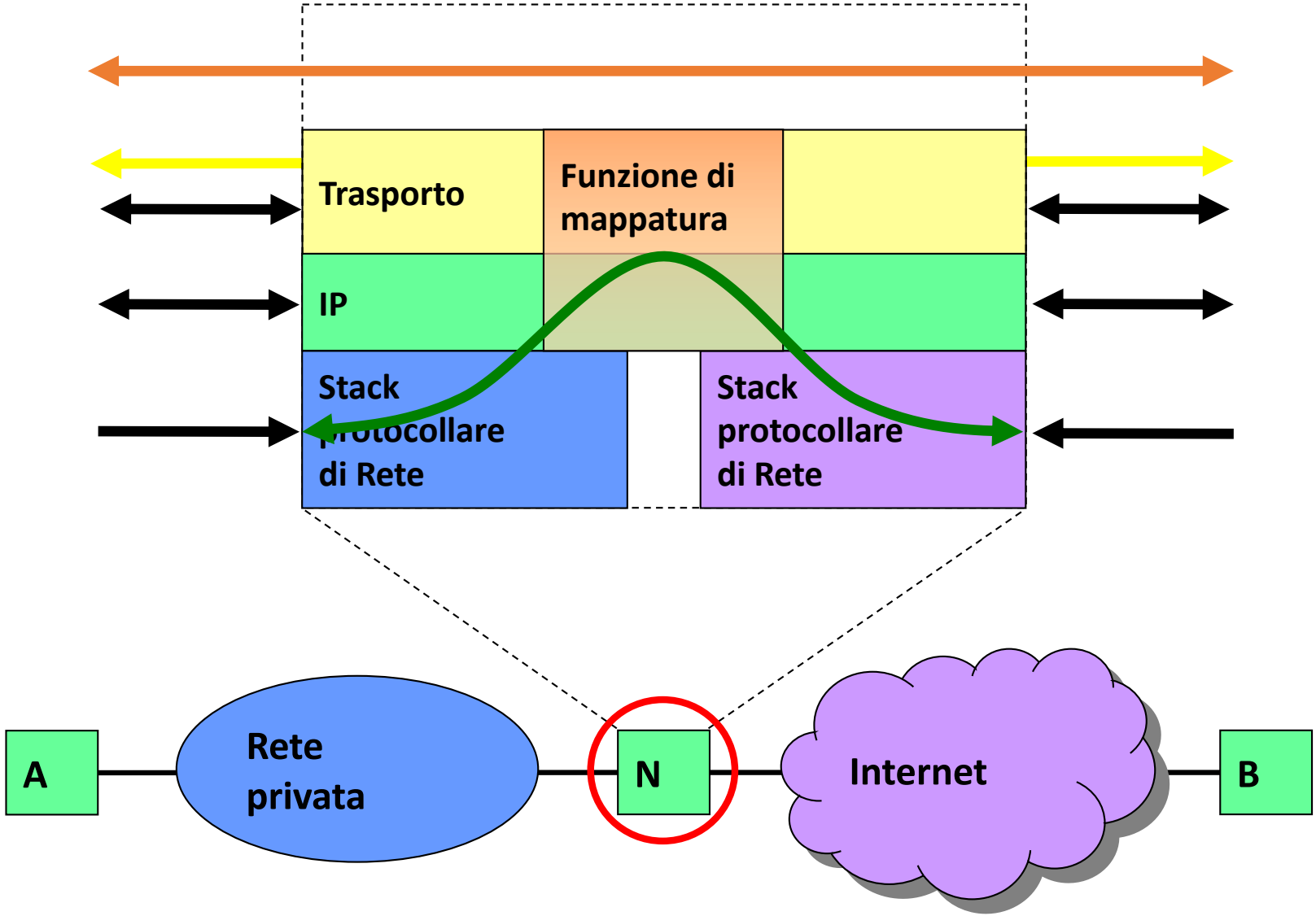
NAT: motivazioni

- Efficiente uso della spazio degli indirizzi
- Condividere uno o pochi indirizzi per accedere alla rete globale

- Security
  - Rendere gli host interni non accessibili dall'esterno
  - Nascondere gli indirizzi e la struttura della rete

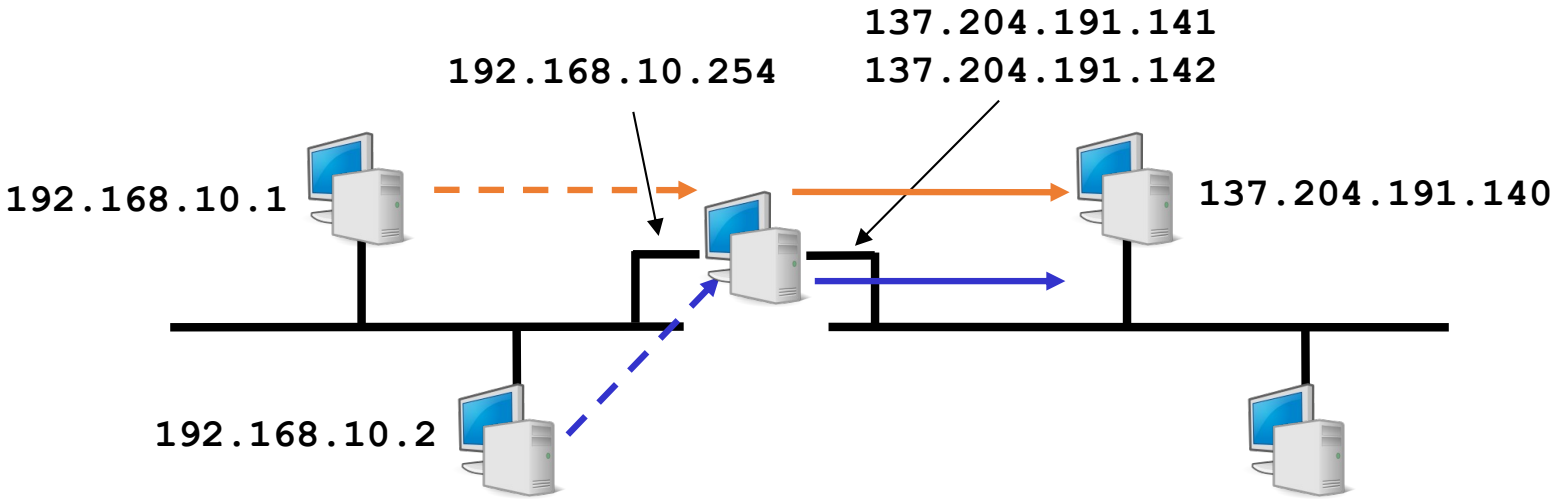
- Include un packet filter, stateful packet inspection configurati dinamicamente

Network (+Port) Address Translator (NAT)



Basic NAT – Conversione di indirizzo

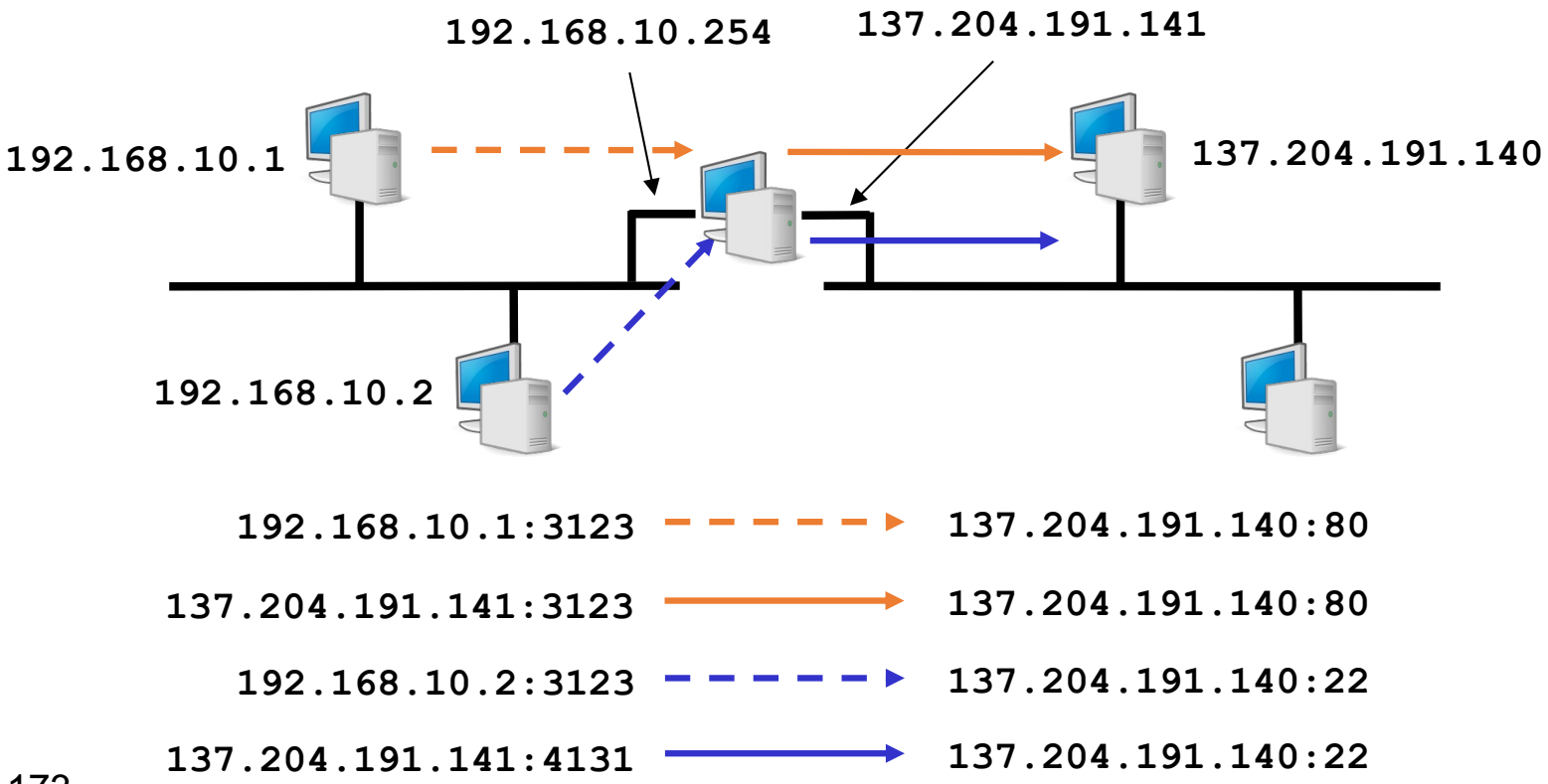
- Il NAT può fornire una semplice conversione di indirizzo IP (statica o dinamica)
- Conversioni contemporanee limitate dal numero di indirizzi IP pubblici a disposizione del gateway NAT



192.168.10.1:3123	⇢	137.204.191.140:80
137.204.191.141:3123	→	137.204.191.140:80
192.168.10.2:5039	⇢	137.204.191.140:22
137.204.191.142:5039	→	137.204.191.140:22

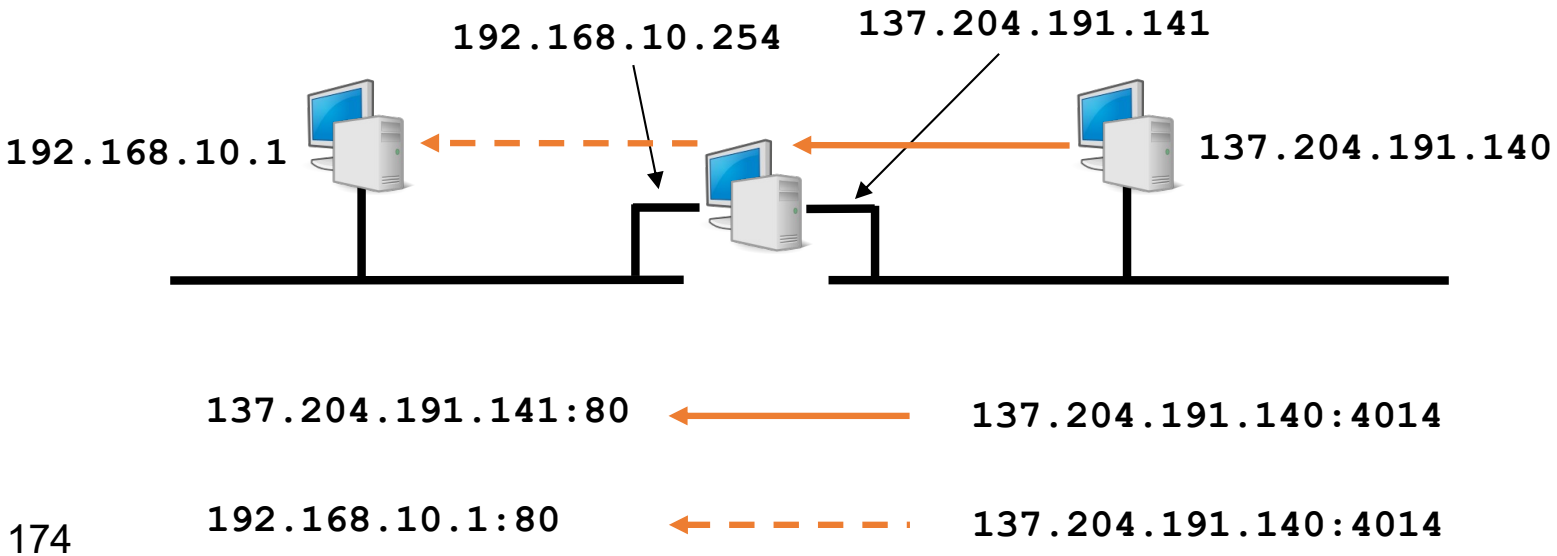
Conversione di indirizzo e porta

- Il NAT può fornire anche conversione di indirizzo IP e porta TCP o UDP
- Conversioni contemporanee possibili anche con un unico indirizzo IP pubblico del gateway NAT



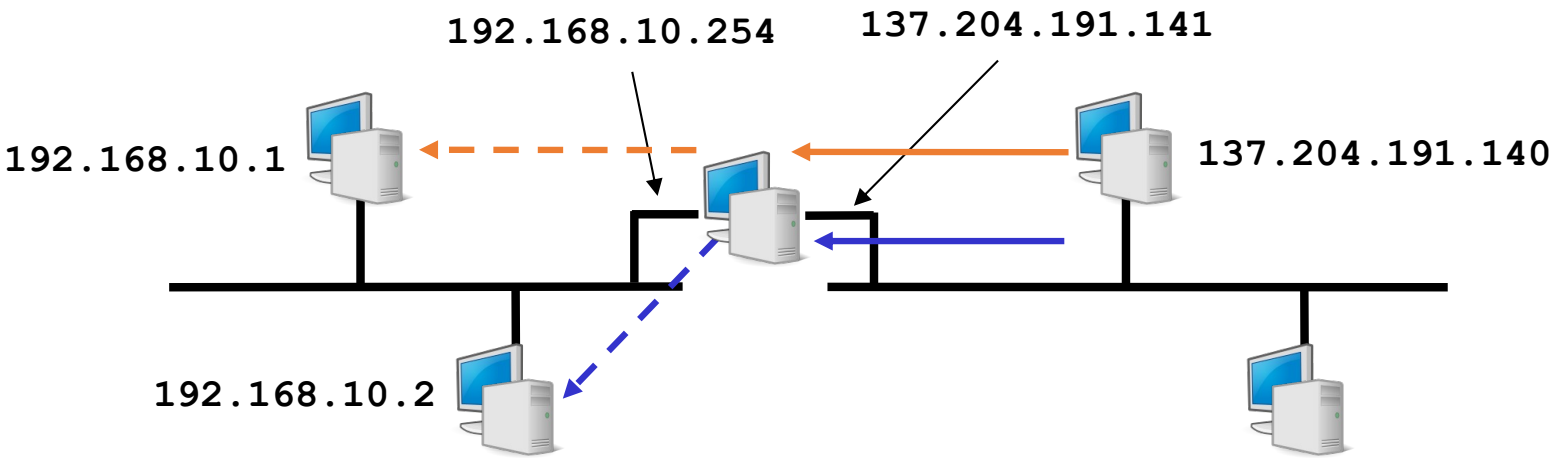
Direzione delle connessioni

- Tipicamente da rete privata verso rete pubblica
  - Il NAT si preoccupa di effettuare la conversione inversa quando arrivano le risposte
  - Registra le corrispondenze in corso in una tabella
- E' possibile contattare dalla rete pubblica un host sulla rete privata?
  - Dipende dal tipo di NAT e dalla relativa configurazione



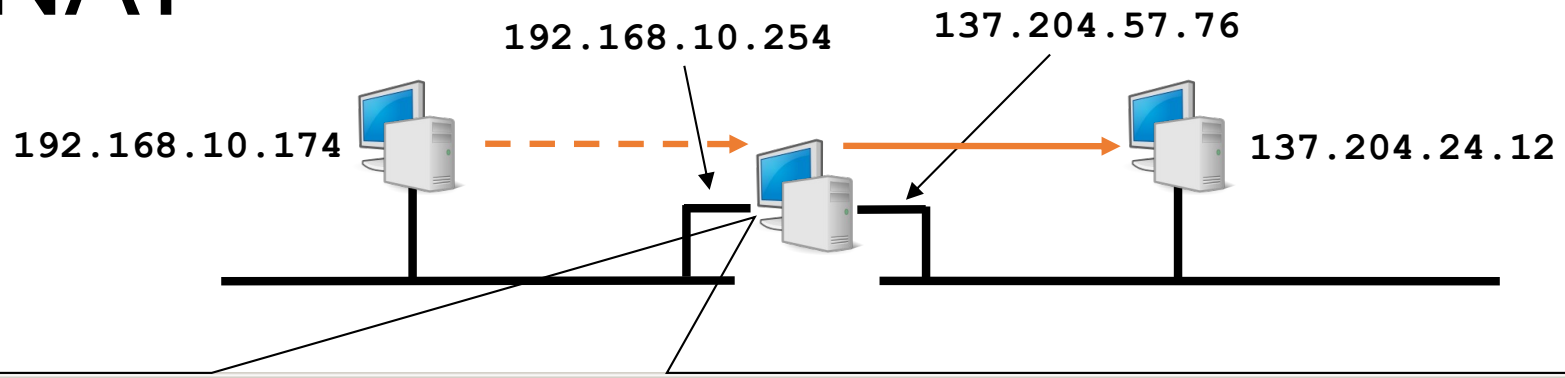
Port forwarding

- Il NAT permette l'ingresso di pacchetti destinati a porte specifiche effettuando la traduzione opportuna



137.204.191.141:80	←	137.204.191.140:4014
192.168.10.1:80	←	137.204.191.140:4014
137.204.191.141:8080	←	137.204.191.140:4015
192.168.10.2:8080	←	137.204.191.140:4015

Analisi di connessioni attraverso NAT

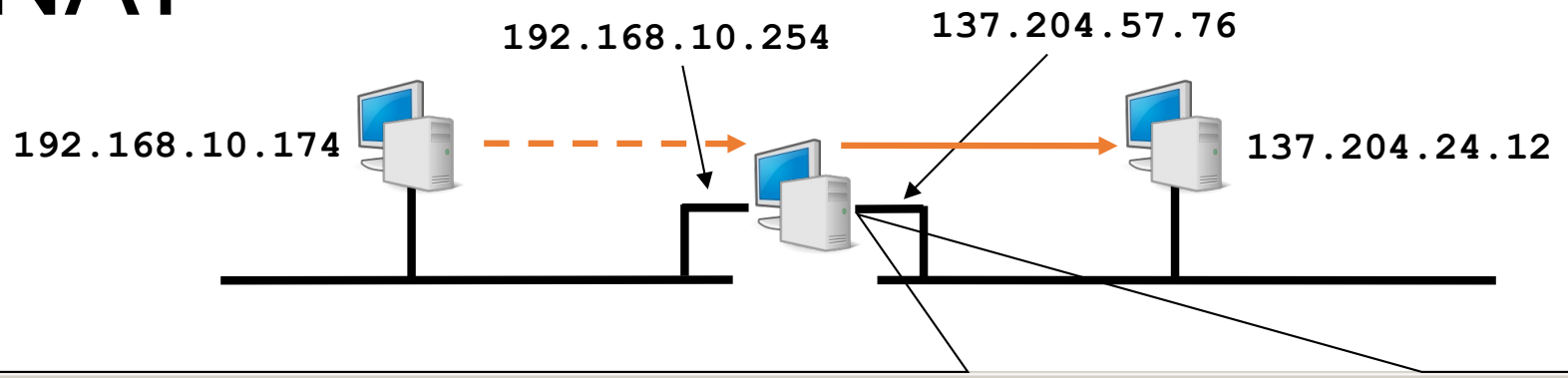


NAT-int.cap - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.10.174	137.204.24.12	HTTP	GET /Ingegneria+Cesena/default.htm HTTP/1.
2	0.034608	137.204.24.12	192.168.10.174	TCP	80 > 3770 [ACK] Seq=3665385073 Ack=46511275 Win=1
3	0.896816	137.204.24.12	192.168.10.174	HTTP	HTTP/1.1 200 OK
4	0.896908	137.204.24.12	192.168.10.174	HTTP	Continuation
5	0.898068	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665387993 Win=6
6	0.899848	137.204.24.12	192.168.10.174	HTTP	Continuation
7	0.899971	137.204.24.12	192.168.10.174	HTTP	Continuation
8	0.900095	137.204.24.12	192.168.10.174	HTTP	Continuation
9	0.900913	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665389453 Win=6
10	0.901066	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665392373 Win=6
11	0.902676	137.204.24.12	192.168.10.174	HTTP	Continuation
12	0.902798	137.204.24.12	192.168.10.174	HTTP	Continuation
13	0.902921	137.204.24.12	192.168.10.174	HTTP	Continuation
14	0.903045	137.204.24.12	192.168.10.174	HTTP	Continuation
15	0.903168	137.204.24.12	192.168.10.174	HTTP	Continuation
16	0.903846	192.168.10.174	137.204.24.12	HTTP	GET /NR/Custom/web/Common/css/stile_main.c
17	0.903848	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665393833 Win=6
18	0.903850	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665396753 Win=6
19	0.904022	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665398213 Win=6
20	0.905643	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665399673 Win=6

Analisi di connessioni attraverso NAT



NAT-ext.cap - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	137.204.57.76	137.204.24.12	HTTP	GET /Ingegneria+Cesena/default.htm HTTP/1.
2	0.034559	137.204.24.12	137.204.57.76	TCP	80 > 3770 [ACK] Seq=3665385073 Ack=46511275 Win=1128
3	0.896736	137.204.24.12	137.204.57.76	HTTP	HTTP/1.1 200 OK
4	0.896859	137.204.24.12	137.204.57.76	HTTP	Continuation
5	0.898045	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665387993 Win=6424
6	0.899803	137.204.24.12	137.204.57.76	HTTP	Continuation
7	0.899925	137.204.24.12	137.204.57.76	HTTP	Continuation
8	0.900050	137.204.24.12	137.204.57.76	HTTP	Continuation
9	0.900889	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665389453 Win=6424
10	0.901042	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665392373 Win=6424
11	0.902630	137.204.24.12	137.204.57.76	HTTP	Continuation
12	0.902752	137.204.24.12	137.204.57.76	HTTP	Continuation
13	0.902875	137.204.24.12	137.204.57.76	HTTP	Continuation
14	0.903000	137.204.24.12	137.204.57.76	HTTP	Continuation
15	0.903122	137.204.24.12	137.204.57.76	HTTP	Continuation
16	0.903836	137.204.57.76	137.204.24.12	HTTP	GET /NR/Custom/web/Common/css/stile_main.c
17	0.903847	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665393833 Win=6424
18	0.903855	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665396753 Win=6424
19	0.903999	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665398213 Win=6424
20	0.905619	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665399673 Win=6424

NAT e applicazioni di rete

- Il NAT è trasparente per l'applicazione
  - Modifica l'intestazione IP e TCP/UDP ma non il payload
- Questo è un problema in alcuni casi specifici
  - Applicazioni non sono trasparenti al NAT
    - Contengono indirizzi IP e numeri di porta nel payload
    - FTP utilizza due connessioni parallele
      - connessione per l'interazione con il server tramite linea di comando (porta TCP 21)
      - connessione per il trasferimento dei dati da e verso il server
      - i parametri della seconda sono specificati nei dati trasmessi dalla prima
  - Il tipo di traffico permesso dipende dal tipo di NAT
    - Full Cone NAT
    - (Port) Restricted Cone NAT
    - Symmetric NAT