

Crittografia e sicurezza delle reti

Firewall

Cosa è un Firewall

- Un punto di controllo e monitoraggio
- Collega reti con diversi criteri di affidabilità e delimita la rete da difendere
- Impone limitazioni ai servizi di rete disponibili
 - solo il traffico autorizzato attraversa la rete
- Eseguono controllo e verifica degli accessi
- E' immune da attacchi

Cosa fa un Firewall

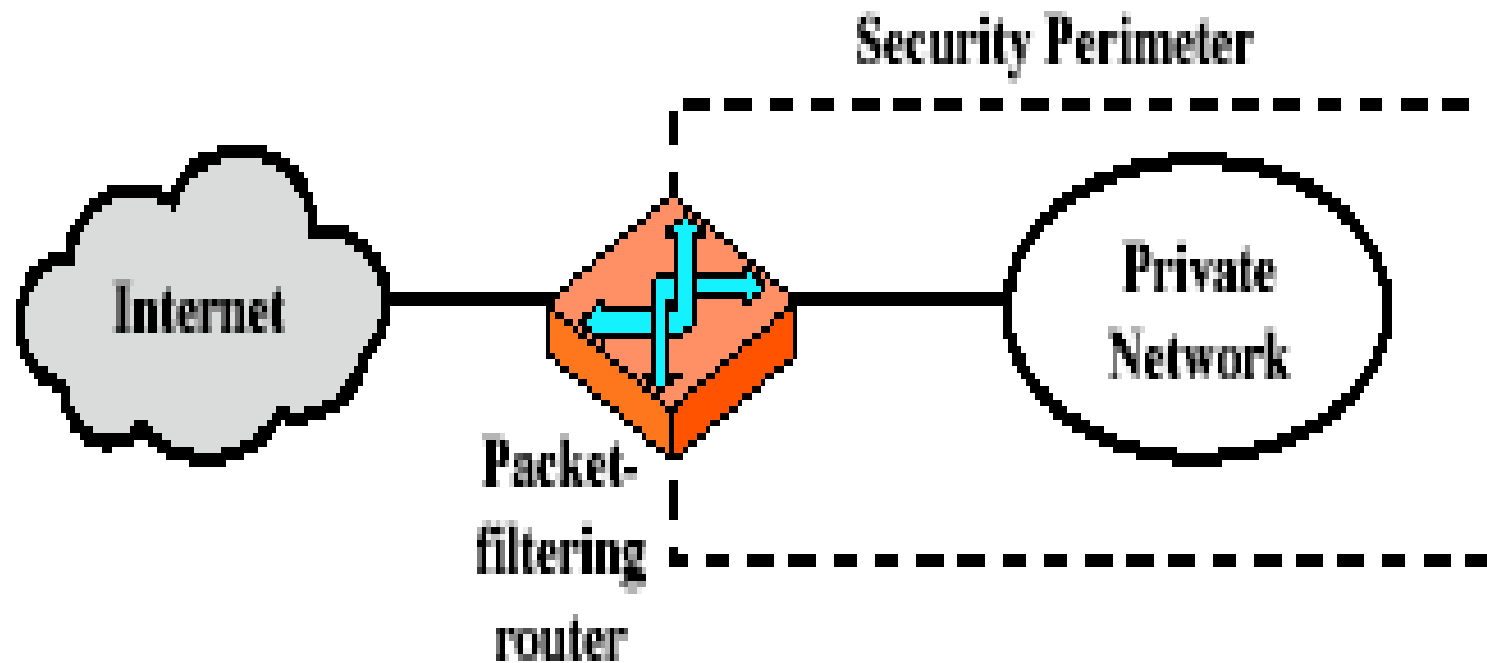
Oltre a limitare il traffico dall'esterno all'interno

- Controllo di banda
- Controllo traffico da rete interna
 - giochi, pornografia, attività non aziendali
- Privatezza
 - non fa vedere dimensioni interne rete o eventuali risorse

Limiti dei Firewall

- Non proteggono da attacchi che li oltrepassano
 - modem, organizzazioni fidate, servizi fidati (es. SSL/SSH)
- Non proteggono da attacchi dall'interno
- Non proteggono dal trasferimento di tutti i possibili virus e worm
 - grande varietà di SO e di virus

Firewalls - Packet Filters



(a) Packet-filtering router

Firewalls - Packet Filters

Esamina ciascun pacchetto IP e utilizza regole per autorizzare/vietare passaggio (non si considera il contesto)

- Regole basate su (ind sorg, porta sorg, ind dest, porta dest, flag)
- Politiche di default
 - ciò che non è espressamente vietato è permesso
 - ciò che non è espressamente permesso è vietato

Firewalls - Packet Filters

Esempi di regole

- può bloccare le richieste di connessioni TCP provenienti dalla rete esterna (tutti i SYN provenienti dall'esterno vengono scartati),
- pacchetti provenienti dall'interno destinati alla porta 80 www sono accettati
- pacchetti dall'interno verso porta 25 (smtp)

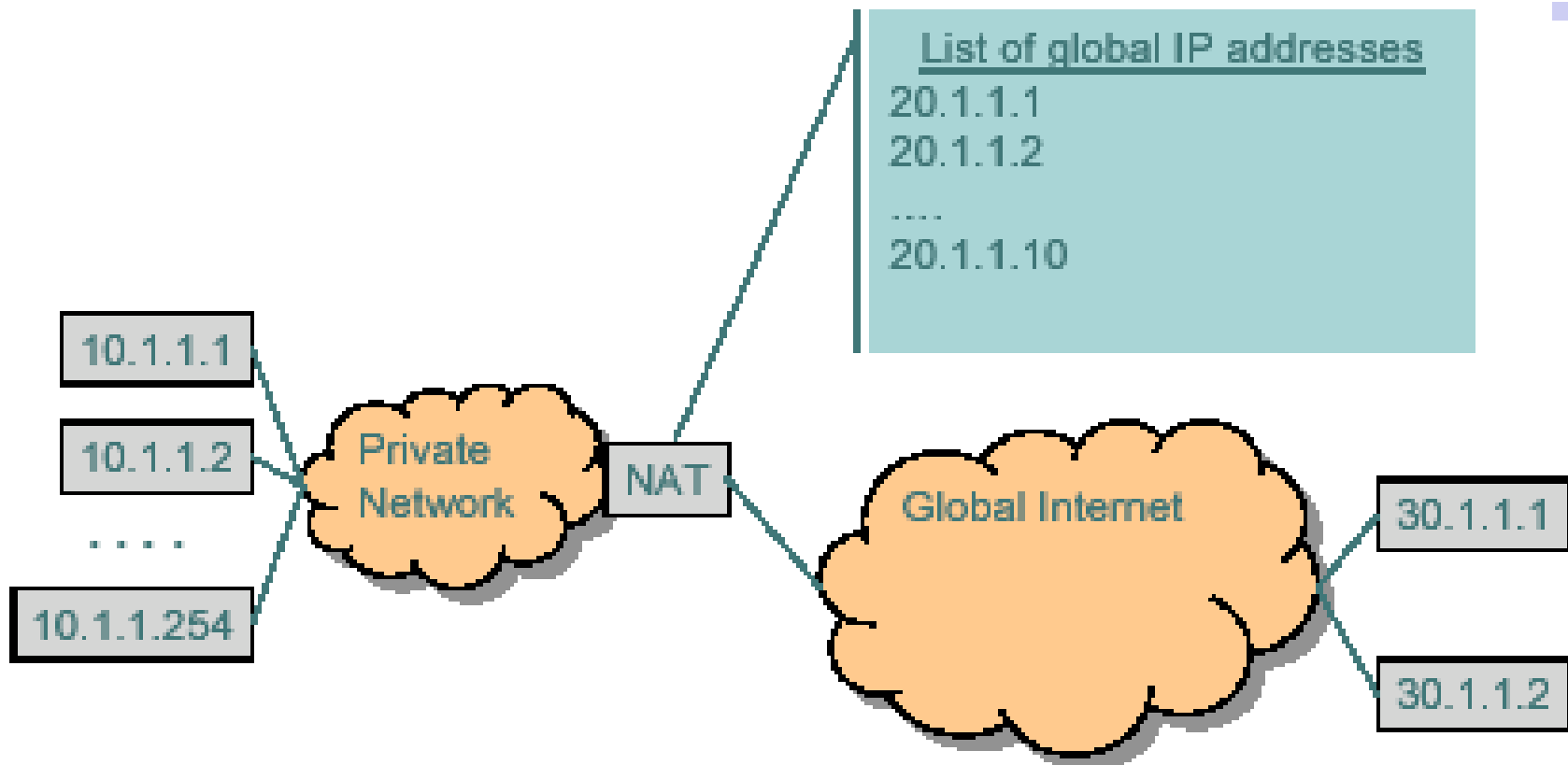
Nota Bene per UDP non c'è modo di controllare le conversazioni attive (non c'è handshaking) o di applicare regole sull'indirizzo sorgente (UDP è facilmente "spoofabile")

NAT - Network Address Translation

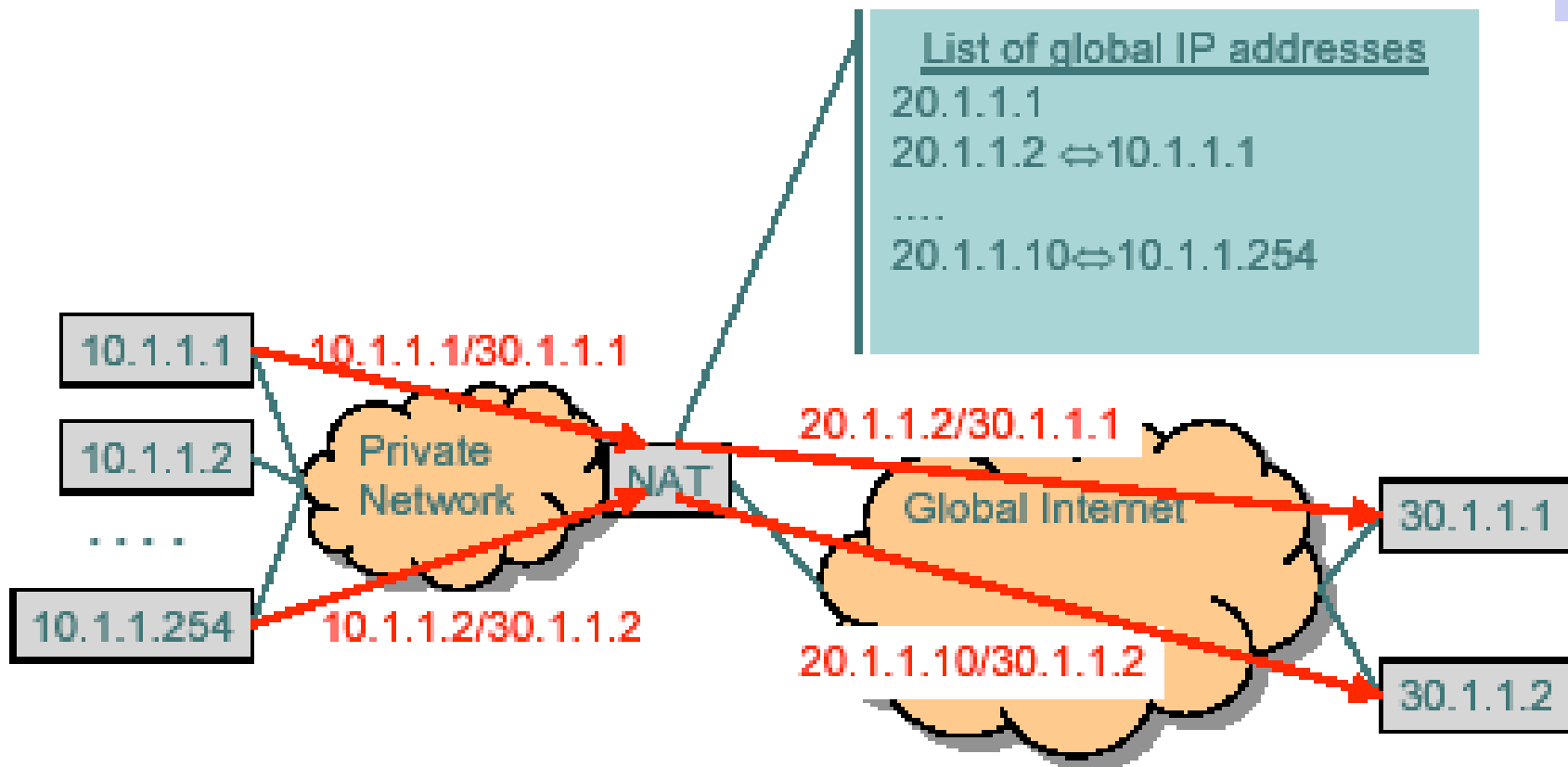
NAT inventati per risolvere il problema dell'esaurimento degli indirizzi IP

- non è più un problema rilevante oggi (sia per uso di NAT che di politiche migliori per non sprecarli)
- utilizzo per filtrare i messaggi

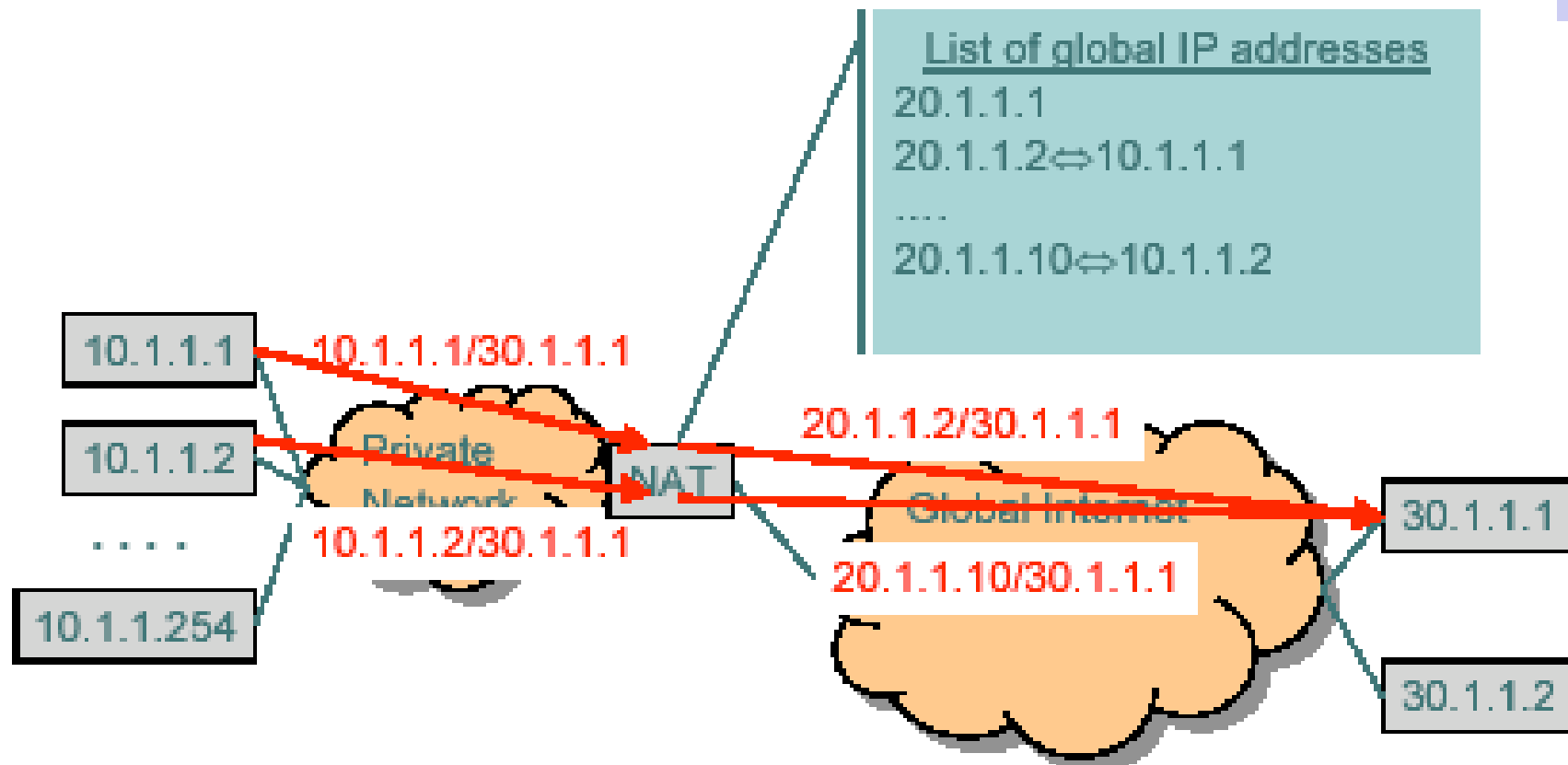
NAT - indirizzi



NAT - accessi



NAT - accessi contemporanei

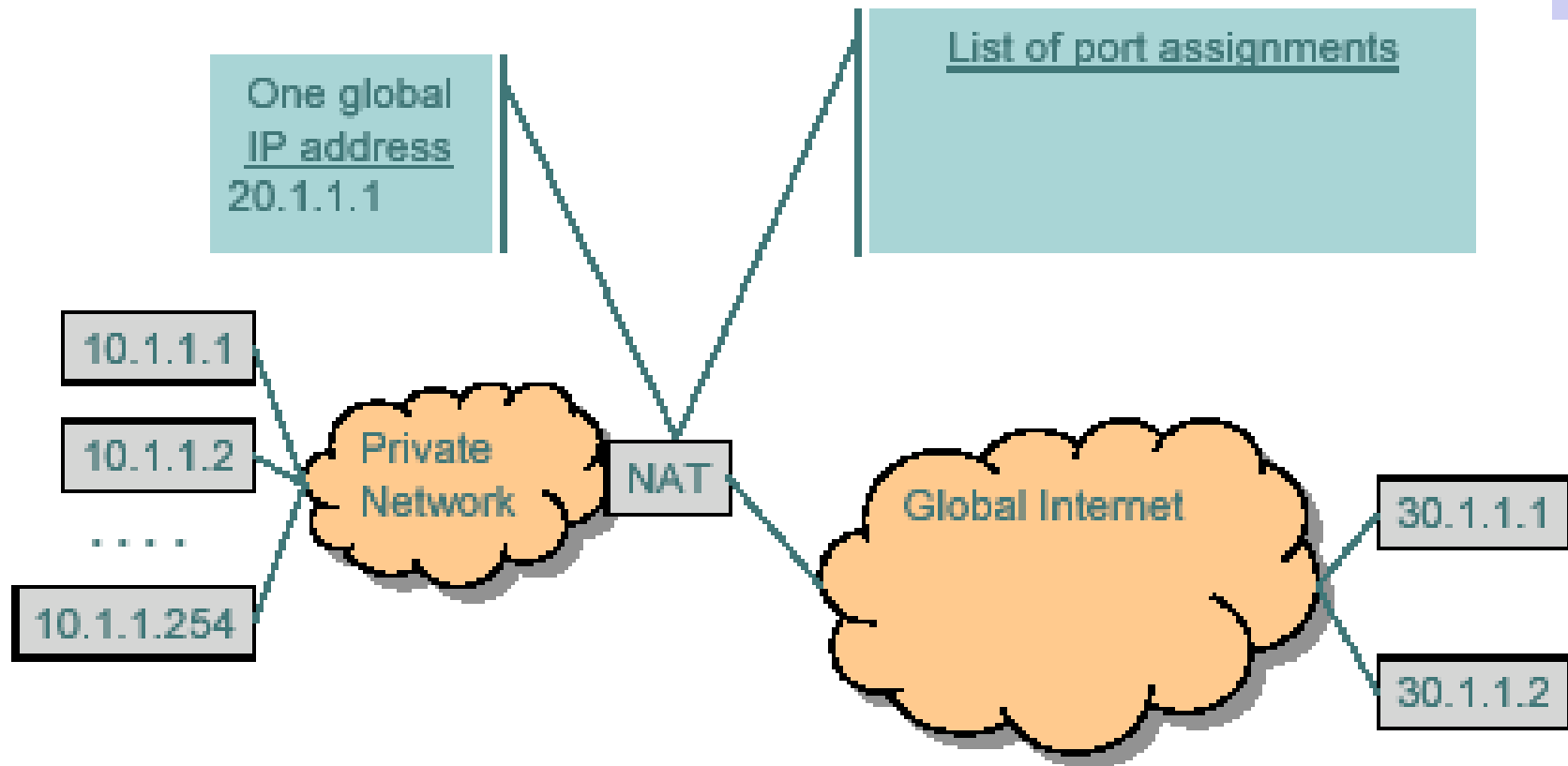


NAT - Problemi

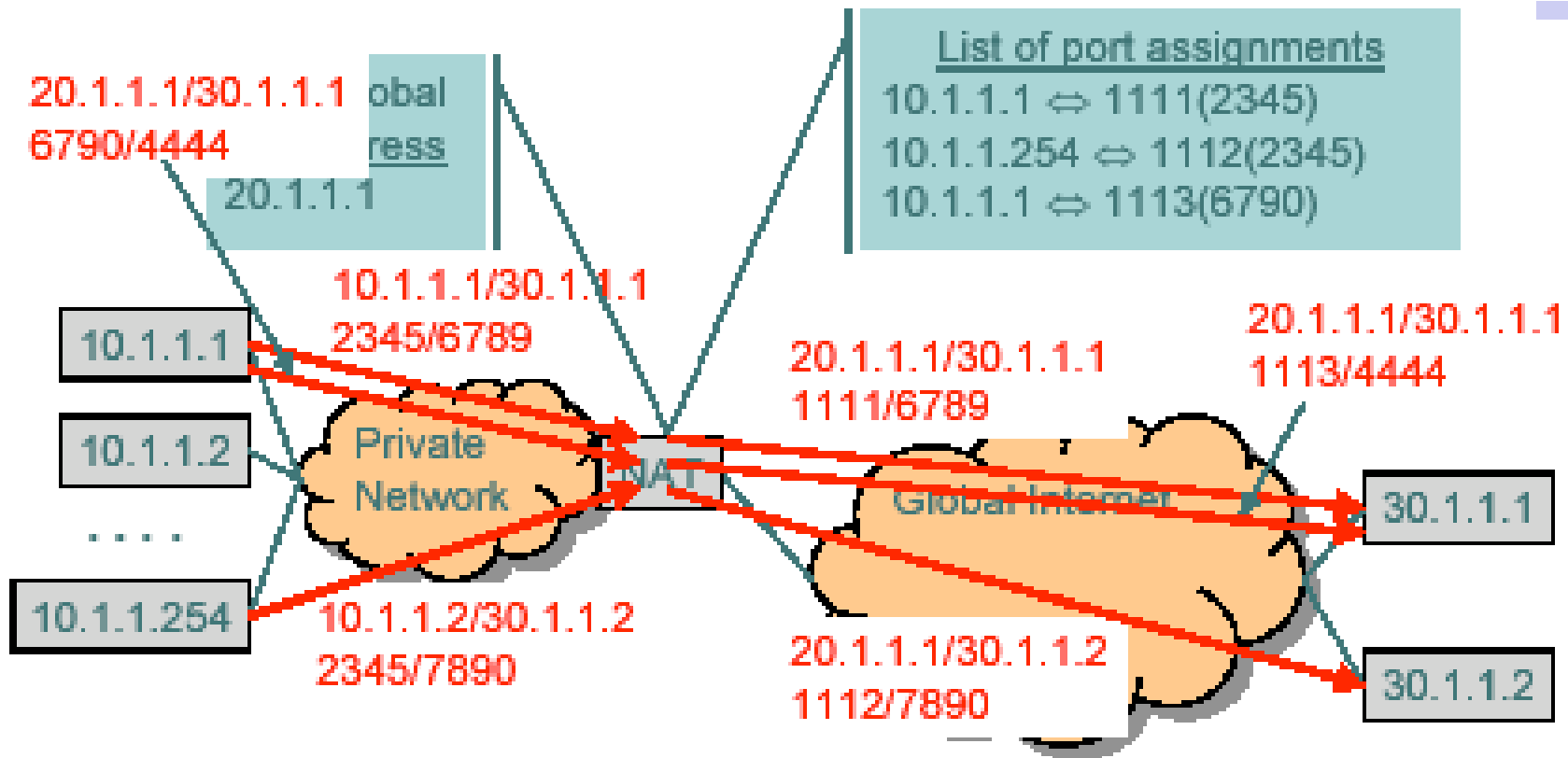
Problemi con il Web

- Si assume che un solo indirizzo globale può supportare decine di host (pochi utenti poche richieste per utente)
- Web:
 - molti accessi contemporanei
 - uso di porte (detto anche port translation - NAT)

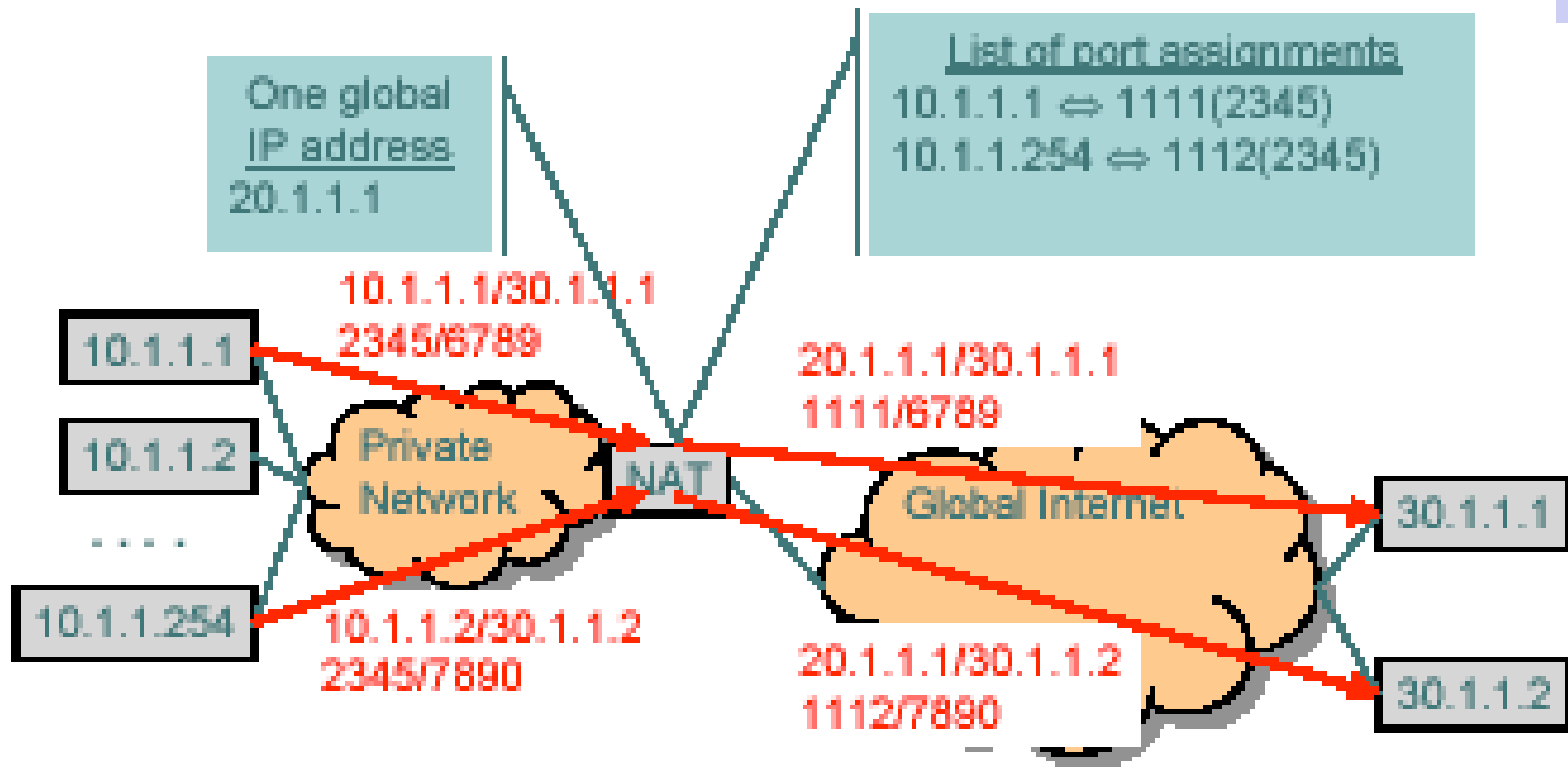
NAT - utilizzo attuale



NAT - accessi contemporanei



NAT - accessi contemporanei



NAT - vantaggi non previsti

- Il NAT impedisce l'accesso dall'esterno alla rete interna
- Privatezza
 - su numero di host all'interno
 - difficoltà a individuare specifici host
 - filtraggio informazioni da/per interno rete

Nota Bene Se si trova il modo per far inviare traffico dall'interno, a quel punto il NAT non fornisce nessun tipo di protezione; utilizzo di firewall

Firewall: con stato e senza stato (stateless e stateful)

- Firewall iniziali (packet filter) sono stateless
 - IP spoofing
 - considera informazioni limitate sullo stato della connessione (es. per TCP si considera solo SYN)
 - quindi pacchetti TCP non SYN sono ammessi anche se dovrebbero essere bloccati
 - Non esiste concetto di conversazione
- Firewall moderni sono stateful
 - mantengono lista dei flussi ammessi
 - più complessi da gestire

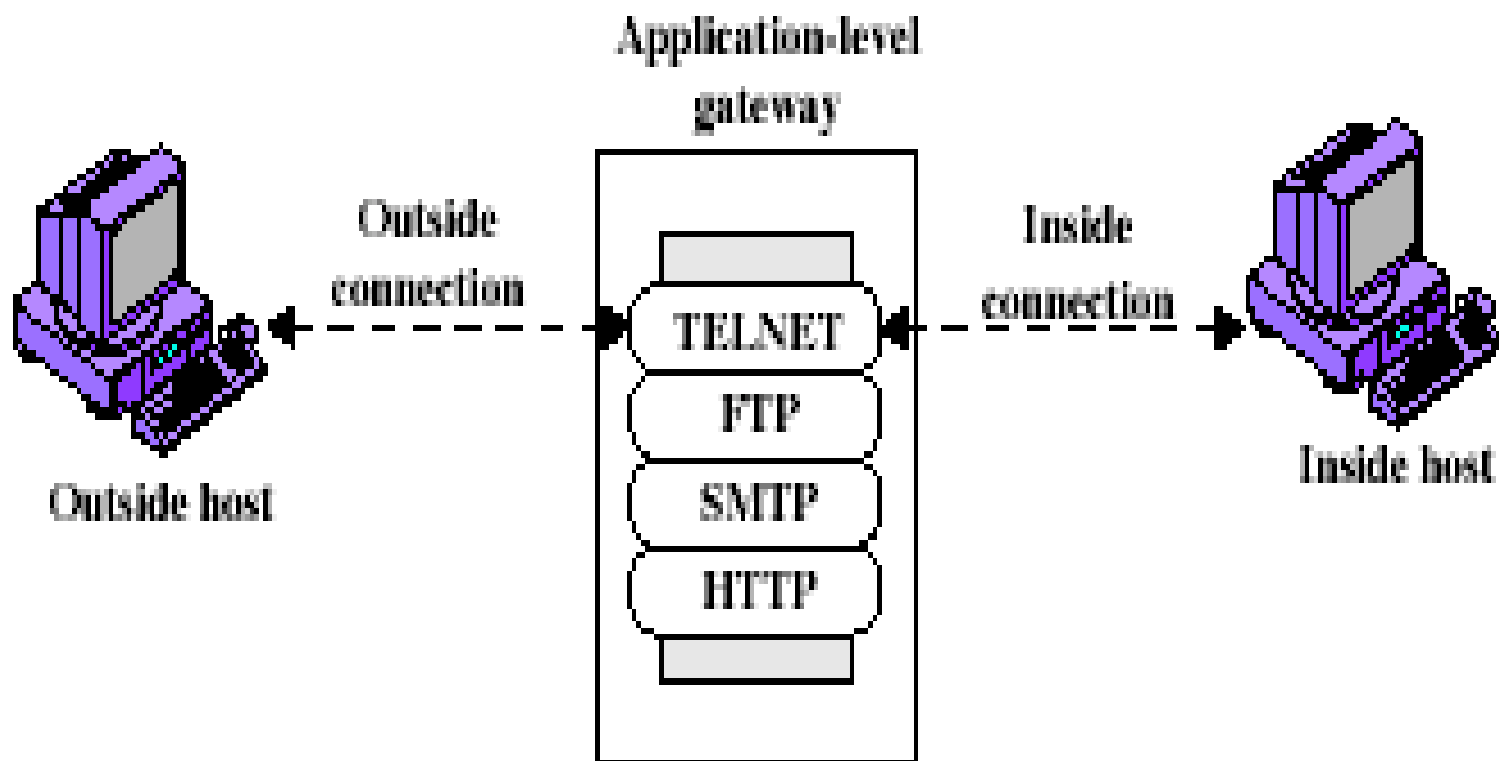
Firewall - Stateful Packet Filters

Esamina ciascun pacchetto nel contesto e mantiene lo stato delle conversazioni e applica regole anche in funzione di esso; ad esempio,

- può decidere di accettare pacchetti dall'esterno solo se le conversazioni sono iniziate dall'interno mantiene informazione su sessioni client-server
- verifica che ogni pacchetto appartenga ad una sessione autorizzata

Migliore capacità di individuare pacchetti anomali (che non appartengono a sessioni autorizzate)

Firewalls - Application Level Gateway

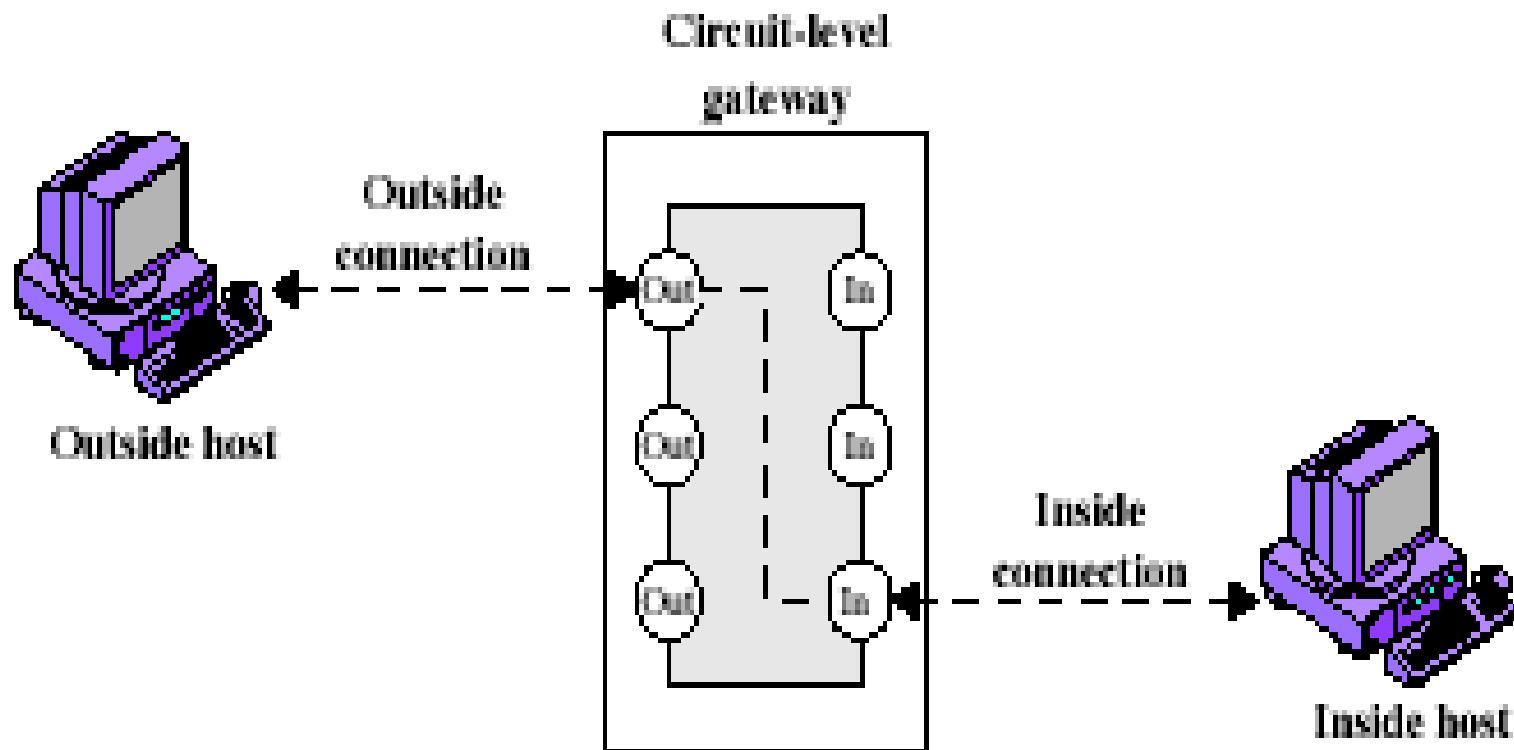


(b) Application-level gateway

Firewalls - Application Level Gateway (proxy)

- Usa una applicazione specifica
- Ha pieno accesso al protocollo
 - utente richiede il servizio
 - la richiesta viene accettata/ rifiutata
 - richieste accettate vengono servite
- Necessita un proxy server per ciascun servizio

Firewalls - Circuit Level Gateway



(c) Circuit-level gateway

Firewalls - Circuit Level Gateway

- Realizza due connessioni TCP
- Impone sicurezza limitando le connessioni autorizzate

Come accedere dall'esterno

Come gestire server della rete trusted che devono essere raggiunti dall'esterno ? (il server di posta SMTP deve ricevere mail da Internet, il sito web deve essere accessibile,...

Soluzione: apro un "buco" sul firewall che inoltra il traffico proveniente dall'esterno destinato alla porta 25, al server di posta; ...analogo per WWW

E' sufficiente ?

Come accedere dall'esterno

Aprire un 'buco' può creare problemi

- Il traffico proveniente dall'esterno può andare solo verso la porta 25 del server SMTP (o 80 del web server) ma:
- I software che girano su queste macchine sono attaccabili
- Un hacker può prendere il controllo della macchina e a quel punto può fare quello che vuole sulla macchina stessa, o attaccare la rete interna (il firewall non ha modo di accorgersene)

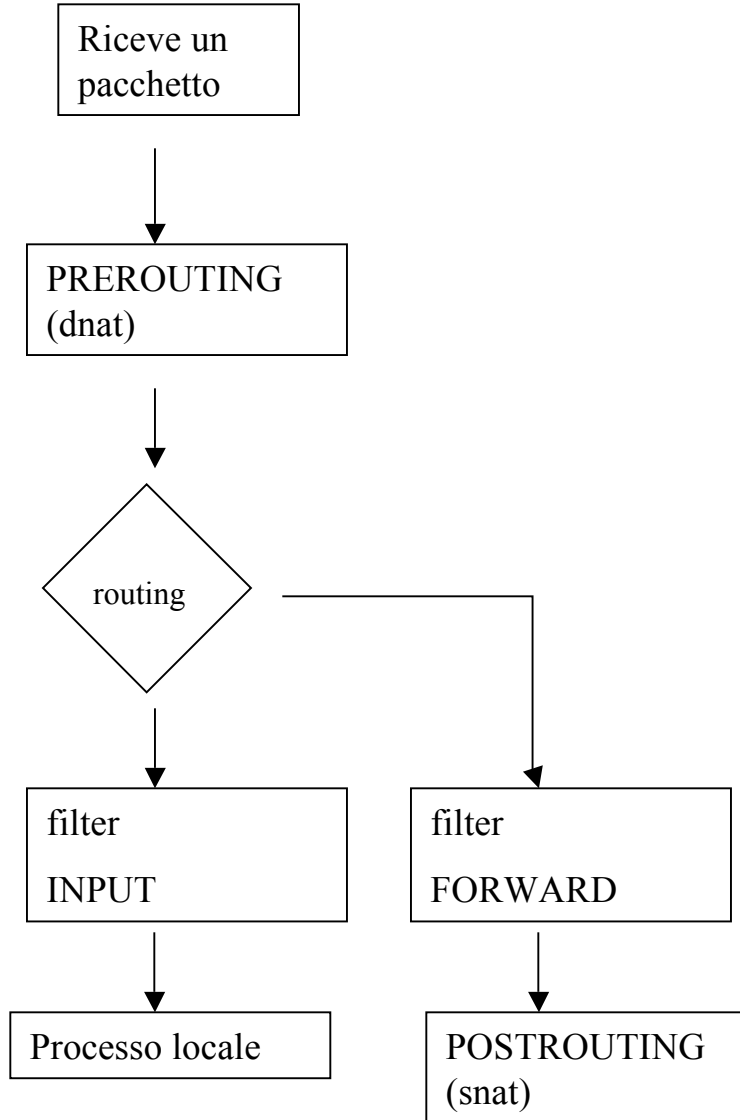
Come accedere dall'esterno

Creo una zona 'demilitarizzata' (DMZ)

- I server che devono essere raggiunti dall'esterno sono in una zona speciale aperta detta DMZ (DeMilitarised Zone); si possono avere anche più livelli di DMZ
- Gli utenti esterni possono accedere alla DMZ ma non alla rete interna

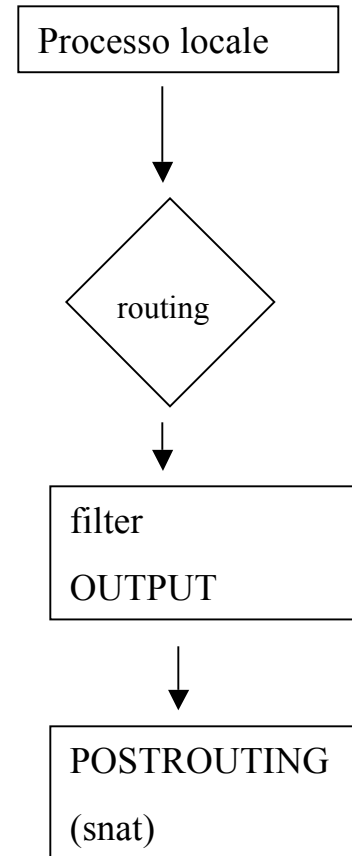
Ovviamente, bisogna fare attenzione al traffico che passa dalla DMZ alla rete interna: se un hacker prende il controllo del server sulla DMZ non deve poter entrare sulla rete interna

IPTABLES



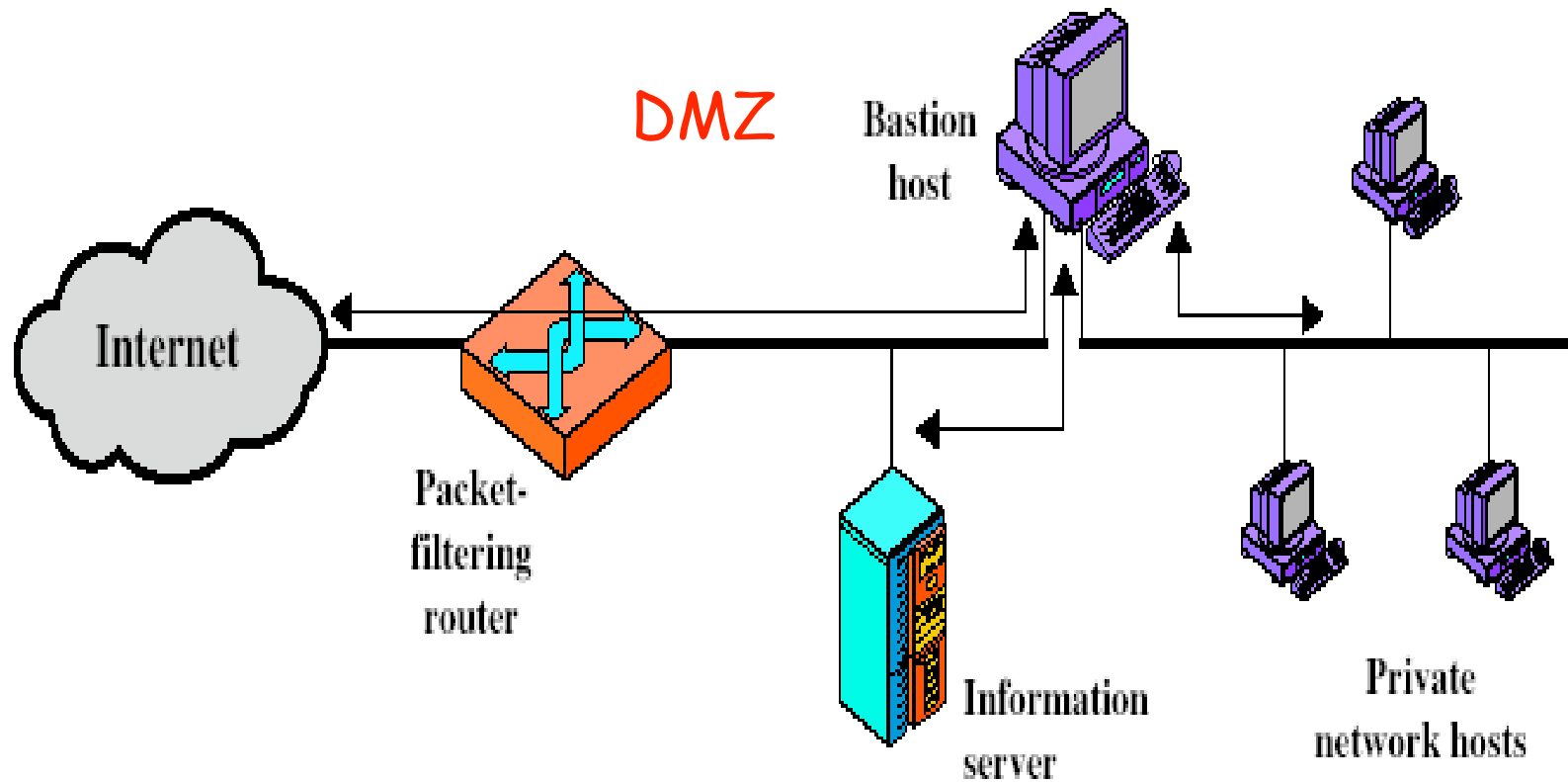
Pacchetti ricevuti dal fw e destinati a processi interni (e.g. ho un web server sulla stesso server del fw)

Pacchetti che attraversano il fw (e.g. dalla rete trusted alla rete untrusted, dalla rete untrusted alla DMZ)



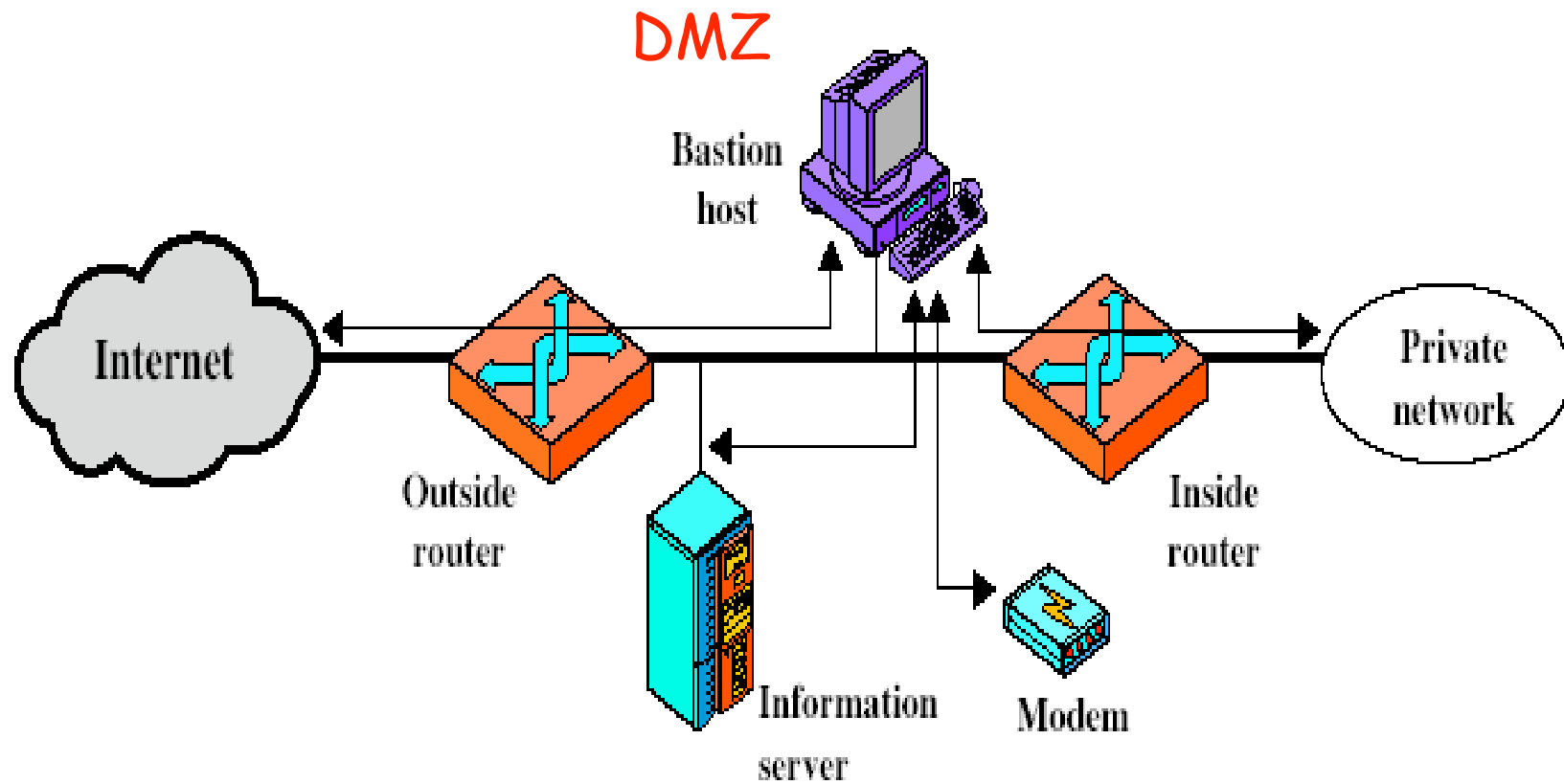
Pacchetti che sono originati dal server su cui risiede il fw (e.g. uso il server del fw anche come postazione di lavoro ed effettuo un telnet, una get http (web) verso la rete un-trusted (internet))

Firewall - Configurazioni



(b) Screened host firewall system (dual-homed bastion host)

Firewall - Configurazioni



(c) Screened-subnet firewall system

Regole di attraversamento

- Valide per pacchetti entrano/ escono dalla rete
- Ogni pacchetto deve attraversare una o più catene
 - Regole di default (accetta o rifiuta)
 - se attraversa indenne una catena passa alla catena successiva
 - durante l'attraversamento può cambiare la sua destinazione (uso di NAT)

Sintassi delle regole

Sintassi delle regole:

```
IPTABLES -t TABLE -A CHAIN -[i|o] IFACE -s x.y.z.w -d a.b.c.d -p  
PROT -m state --state STATE -j ACTION
```

TABLE = nat | filter | ... (tavola indirizzi)

CHAIN = INPUT | OUTPUT | FORWARD | PREROUTING|POSTROUTING
(un pacchetto deve attraversare diverse catene)

IFACE = eth0 | eth1 | ppp0 (interfaccia di rete)

PROT = tcp | icmp | udp

STATE = NEW | ESTABLISHED | RELATED

ACTION = DROP | ACCEPT | REJECT | DNAT | SNAT

Sintassi - esempi

Blocco tutto il traffico proveniente dall'esterno

- Supponiamo sia eth0 l'interfaccia esterna

```
IPTABLES -A FORWARD -i eth0 -j DROP
```

Nota che i pacchetti vengono scartati in modo silenzioso; non si forniscono messaggi in modo da proteggersi in caso di attacchi "flooding" e da non fornire informazioni in caso di attacchi basati su "port scanning"

Sintassi - esempi

Accetto il traffico proveniente dall'esterno se è relativo a connessioni originate dall'interno

Supponiamo sia eth0 l'interfaccia esterna

```
IPTABLES -A FORWARD -i eth0 -m state --state ESTABLISHED -j ACCEPT
```

Nota che si usa lo stato "ESTABLISHED" per usare il connection tracking; lo stato ESTABLISHED non va confuso con lo stato TCP, bensì per iptables è uno stato in cui sono passati pacchetti tra due host in entrambe le direzioni; ad esempio per ICMP i pacchetti request possiedono lo stato NEW, le replay ESTABLISHED

Sintassi - esempi

Lascio aperto l'SSH quando è originato da un indirizzo noto

- Supponiamo sia eth0 l'interfaccia esterna

```
IPTABLES -A INPUT -i eth0 -s 123.123.123.123 -p tcp -  
-dport 22 -j ACCEPT
```

Nota: l'host 123.123.123.123 è l'unico autorizzato a fare connessioni SSH dall'esterno; ovviamente a questo punto la mia sicurezza dipende anche da questo host: se qualcuno si impossessa dell'host 123.123.123.123 può entrare sulla mia rete interna