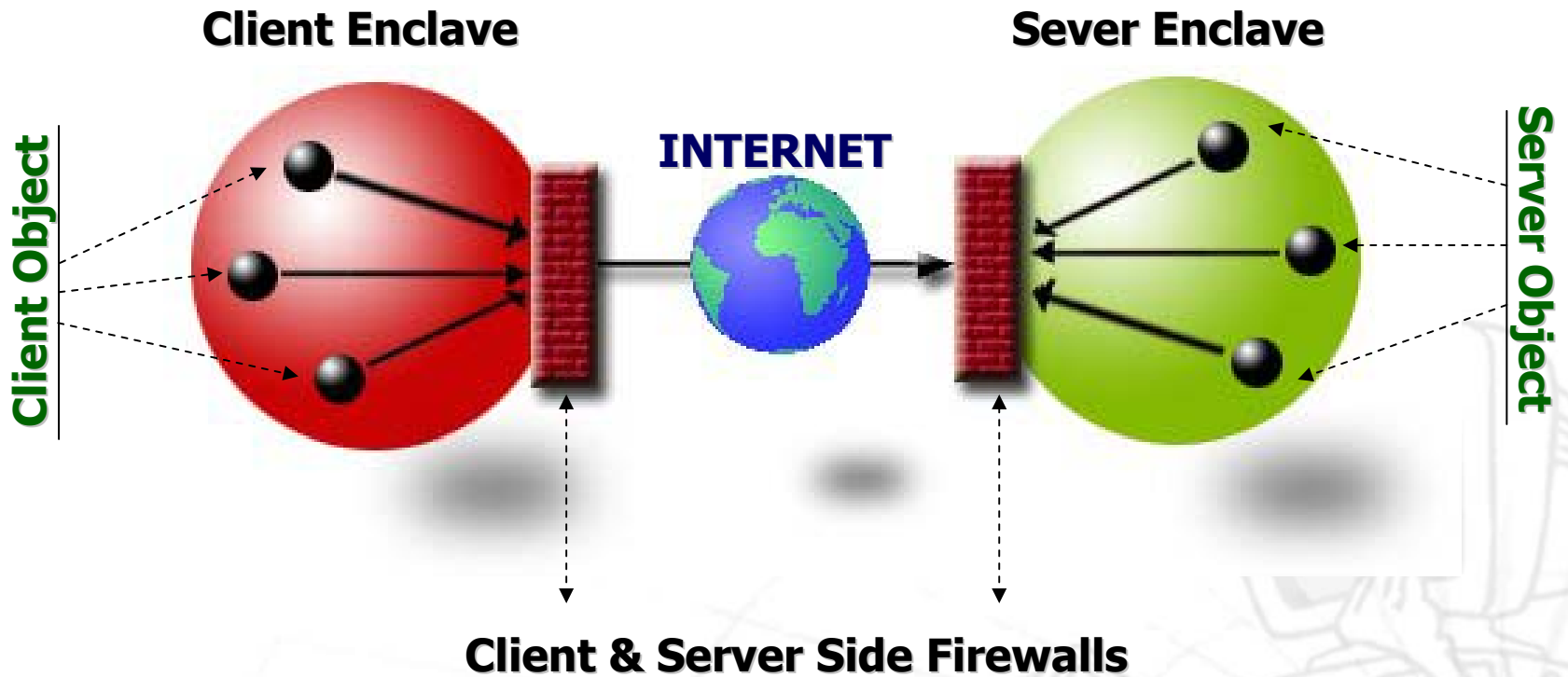


# Architettura CORBA

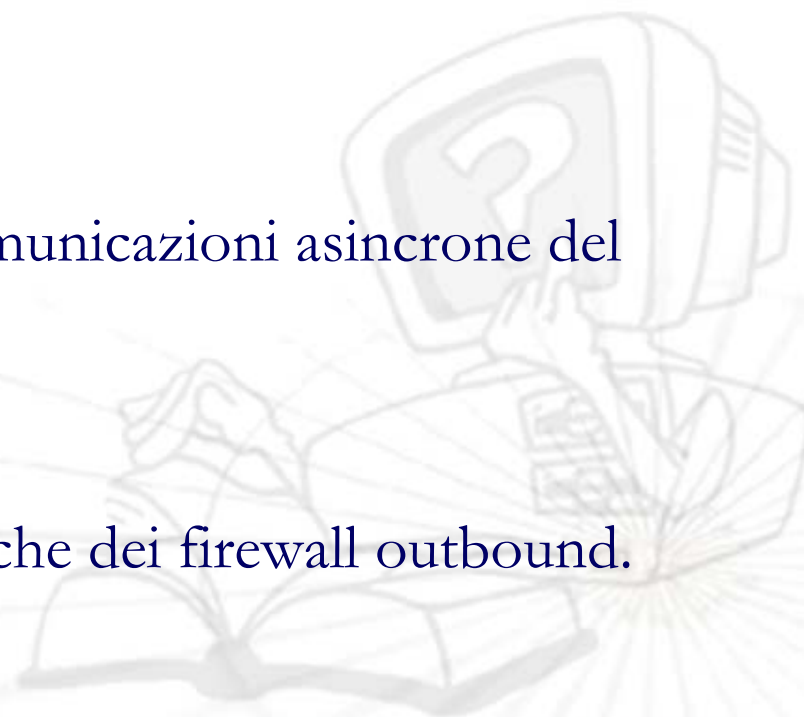
## Aspetti di Sicurezza

- **Security Service** (parte dello standard)
- **Firewall Proposal** (in discussione)



- Indirizzamento: l'IOR contiene il socket (indirizzo IP e porta) del server;
- Se il server è in un'altra enclave, non è raggiungibile direttamente;
- Il Client deve ottenere un indirizzo proxyfied, corrispondente al firewall più vicino;
- Sul Firewall che protegge il client (outbound), la configurazione può essere manuale:
  - `corbaClient -IOOPBindAddr inet:myiioproxy.mynet.com:port-number`
- Sul Firewall che protegge il Server (inbound), la configurazione statica non ha senso (CORBA crea servizi dinamicamente)
- Gli IOR generati dal Server devono contenere informazione aggiuntiva per individuare il firewall

- Nei sistemi Client/Server tradizionali solo il client stabilisce connessioni con il server;
- In CORBA l'ORB è sostanzialmente lo stesso per i client e per i server. Ogni client può fornire servizi;
- Le callbacks sono molto usate per comunicazioni asincrone del server ai client;
- Approccio incompatibile con le politiche dei firewall outbound.



## Crittografia

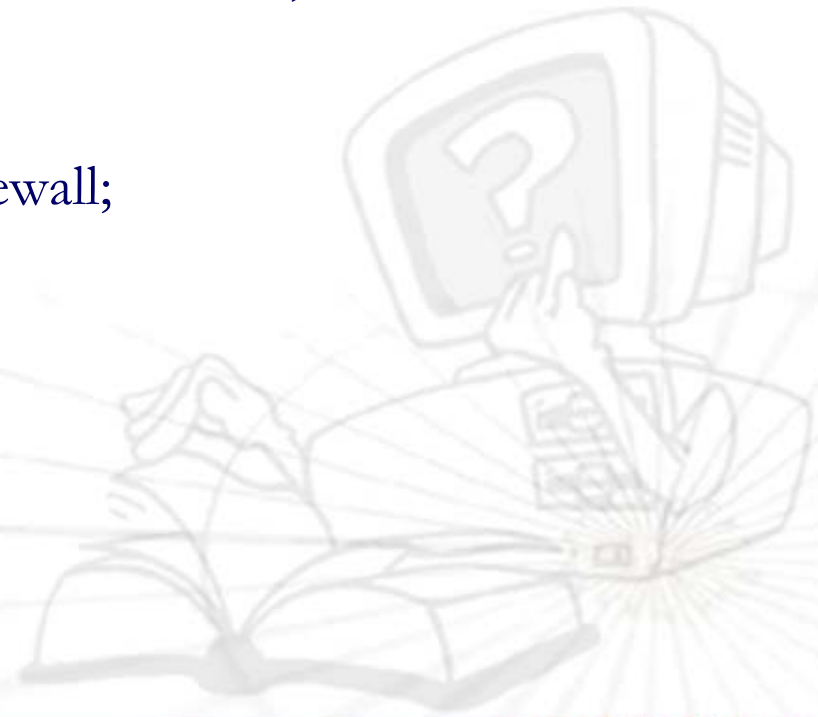
- Le comunicazioni su Internet passano su un mezzo pubblico;
- La sola protezione possibile è la crittografia dei pacchetti (IIOP su SSL).

## Trasparenza

- la presenza del firewall dovrebbe essere il più possibile trasparente agli utenti finali ed agli sviluppatori

La proposta prevede tre approcci possibili:

- Un proxy TCP per applicazioni piuttosto statiche;
- Un proxy SOCKS per client-side firewall;
- Un proxy IIOP a livello applicativo.



- Firewall a livello trasporto: il controllo degli accessi è basato sugli indirizzi IP di client e server;
- Mapping statico tra una porta sul firewall e il socket del servizio CORBA;
- L'IOR del servizio CORBA deve far riferimento al socket del firewall.

Es:

```
./server -IOOPProxyAddr inet:<indirizzo-del-firewall>:<porta-del-proxy>
```



- SOCKS è un meccanismo di proxy standard a livello trasporto (RFC 1928);
- Solitamente già disponibile sul firewall outbound;

## Funzionamento

- Il client chiede al proxy di aprire determinate connessioni;
- Il client deve essere sockified (sostituzione delle network call con le primitive SOCKS);
- Il Client si autentica con il proxy;
- Il Client chiede una connessione verso l'Application Server;
- Il Proxy crea la connessione verso l'application server;
- Client e Server si scambiano i dati attraverso il proxy;
- Meccanismo trasparente al server.

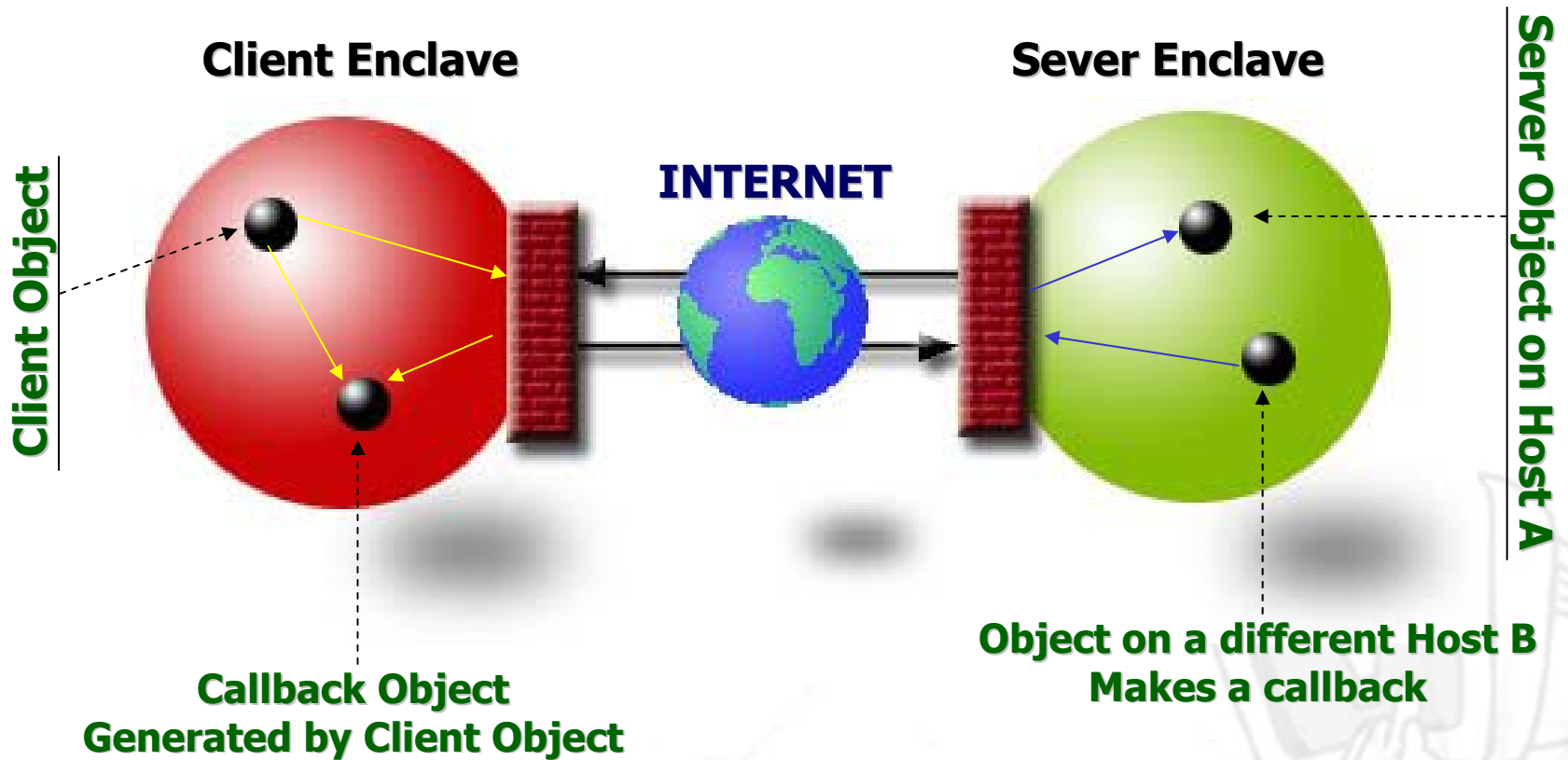


- I firewall a livello trasporto possono effettuare controlli solo sugli indirizzi IP;
- Non possono valutare il contenuto dei pacchetti IIOP;
- Un proxy IIOP può verificare la presenza di IIOP illegale;

ES.

telnet alla porta IIOP

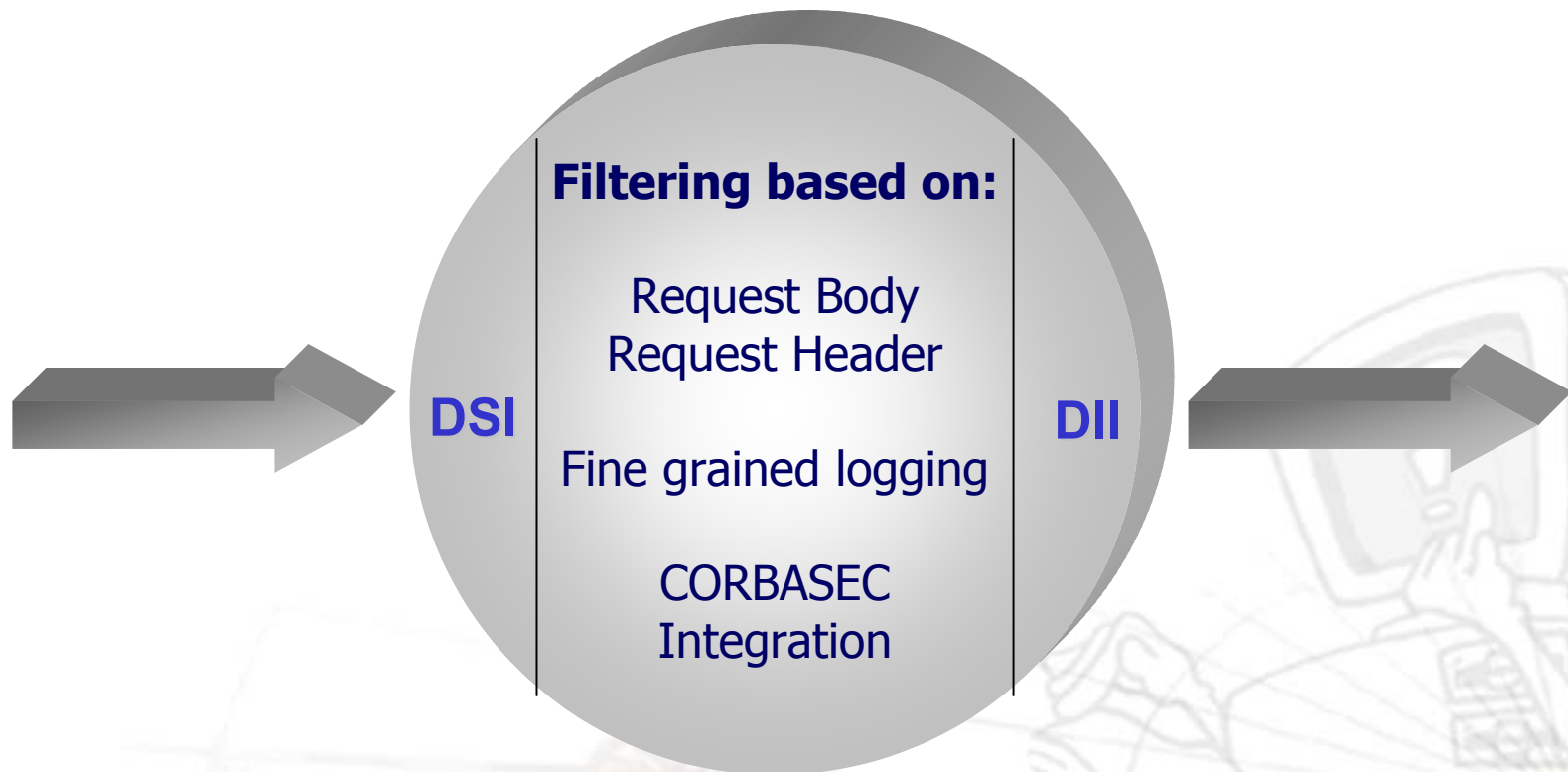




## Soluzioni Possibili:

- Bidiretional GIOP: modificare GIOP per consentire richieste in entrambe le direzioni in un'unica connessione TCP;
- Uso di un IIOP proxy anche per l'inbound firewall.

Questa soluzione non rientra nella proposta OMG



- Usato per superare l'outbound firewall;
- Tecnica inutile in presenza di proxy specifici per http.

