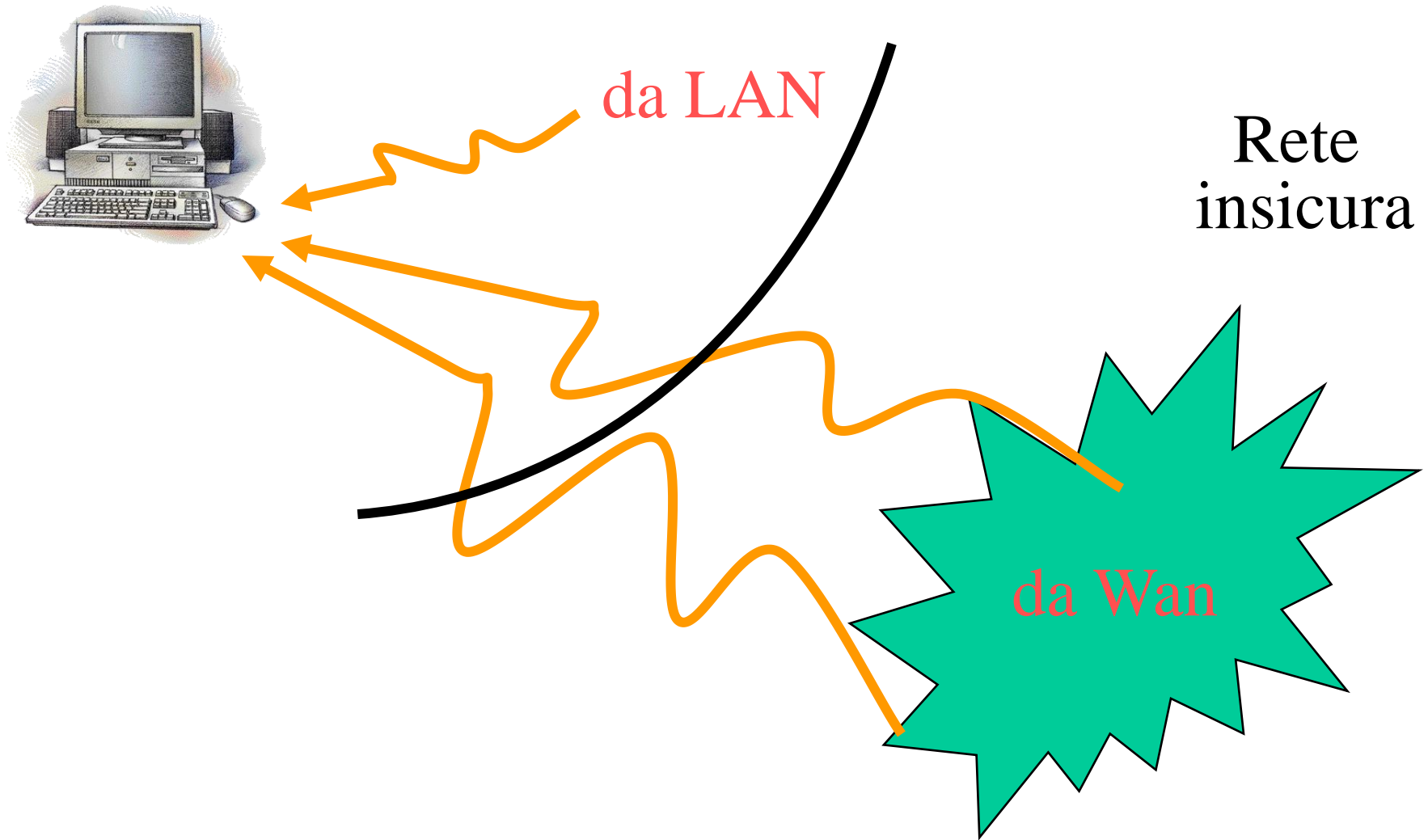


Protezione LAN con un Firewall

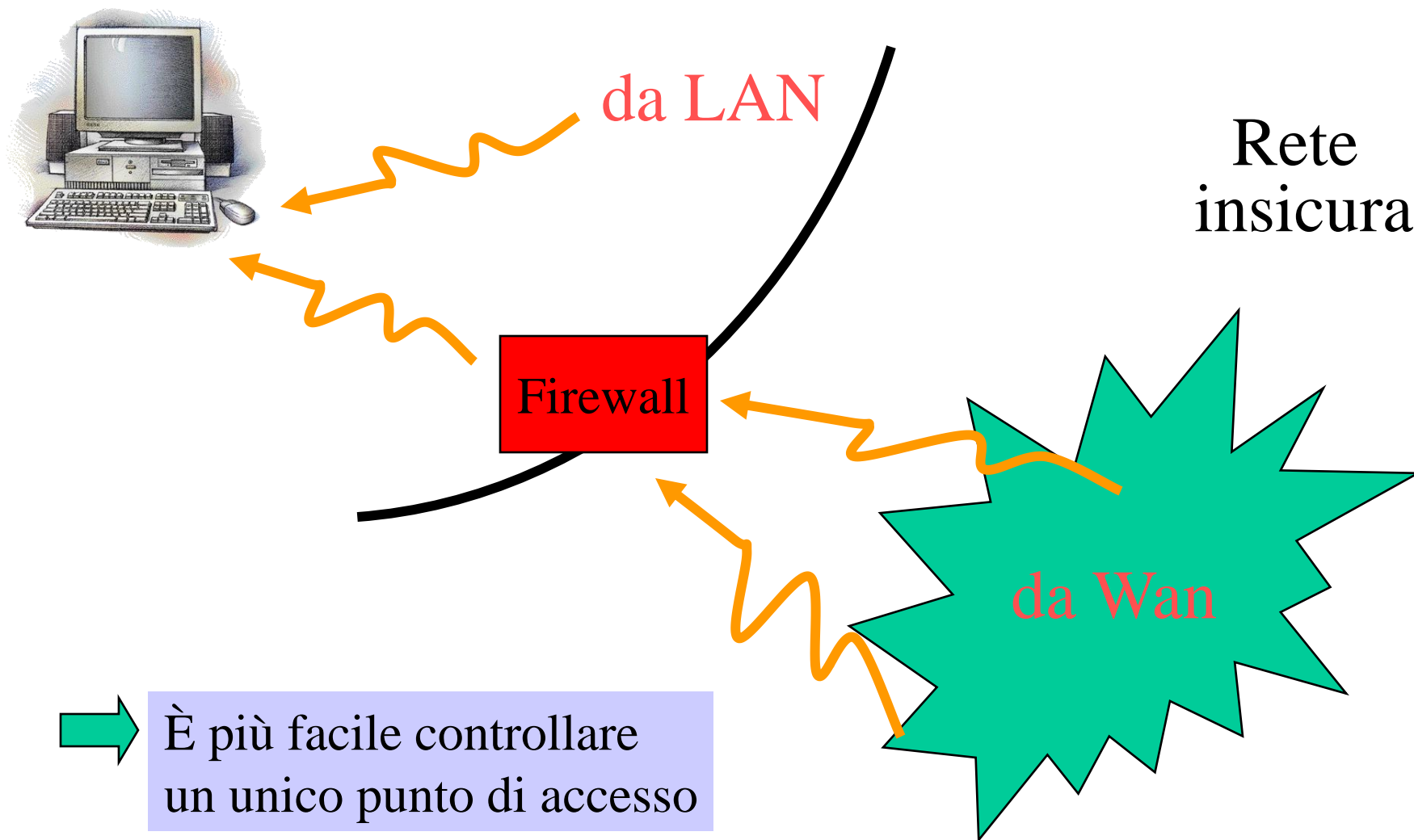
Prof. Francesco Bergadano

**Dipartimento di Informatica
Università di Torino**

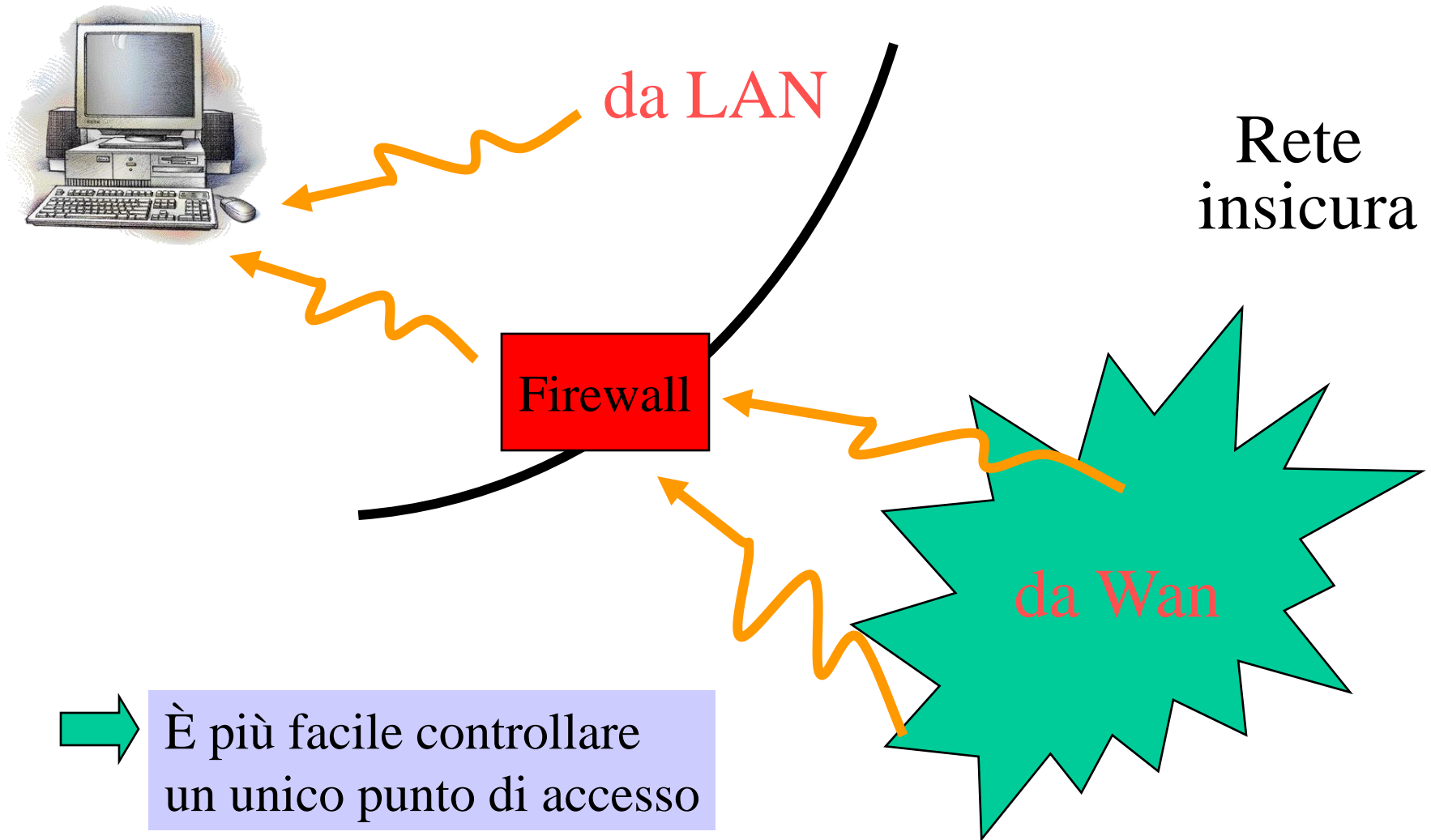
Sicurezza Rete Locale (LAN)



Sicurezza Rete Locale (LAN)



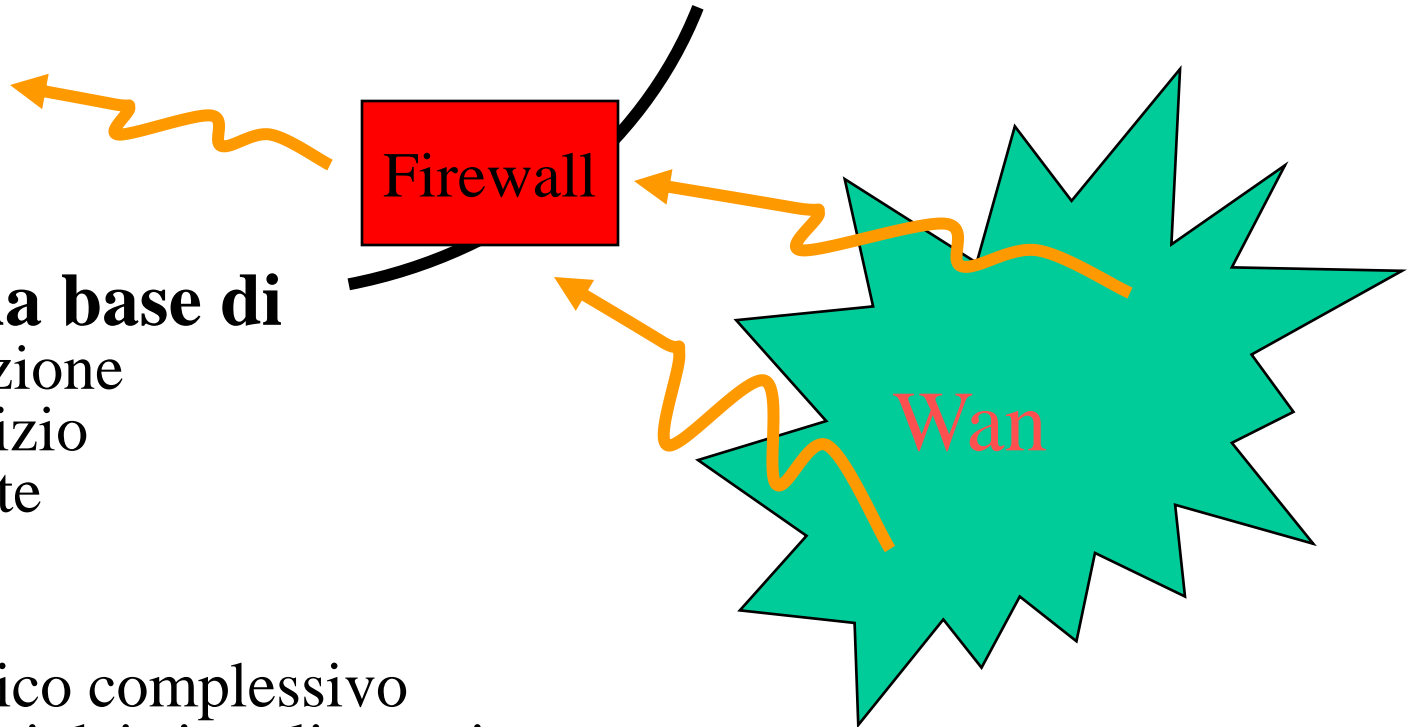
Perché?



Perché un firewall

- **In una LAN alcuni computer sono poco controllati e mal configurati**
- **Basta controllare un computer per accedere facilmente al resto della LAN**
 - **mediante falsificazione di messaggi ARP**
 - **mediante spoofing a livello DNS**
 - **con sniffing di password**

Funzioni del Firewall



Filtro sulla base di
direzione
servizio
utente

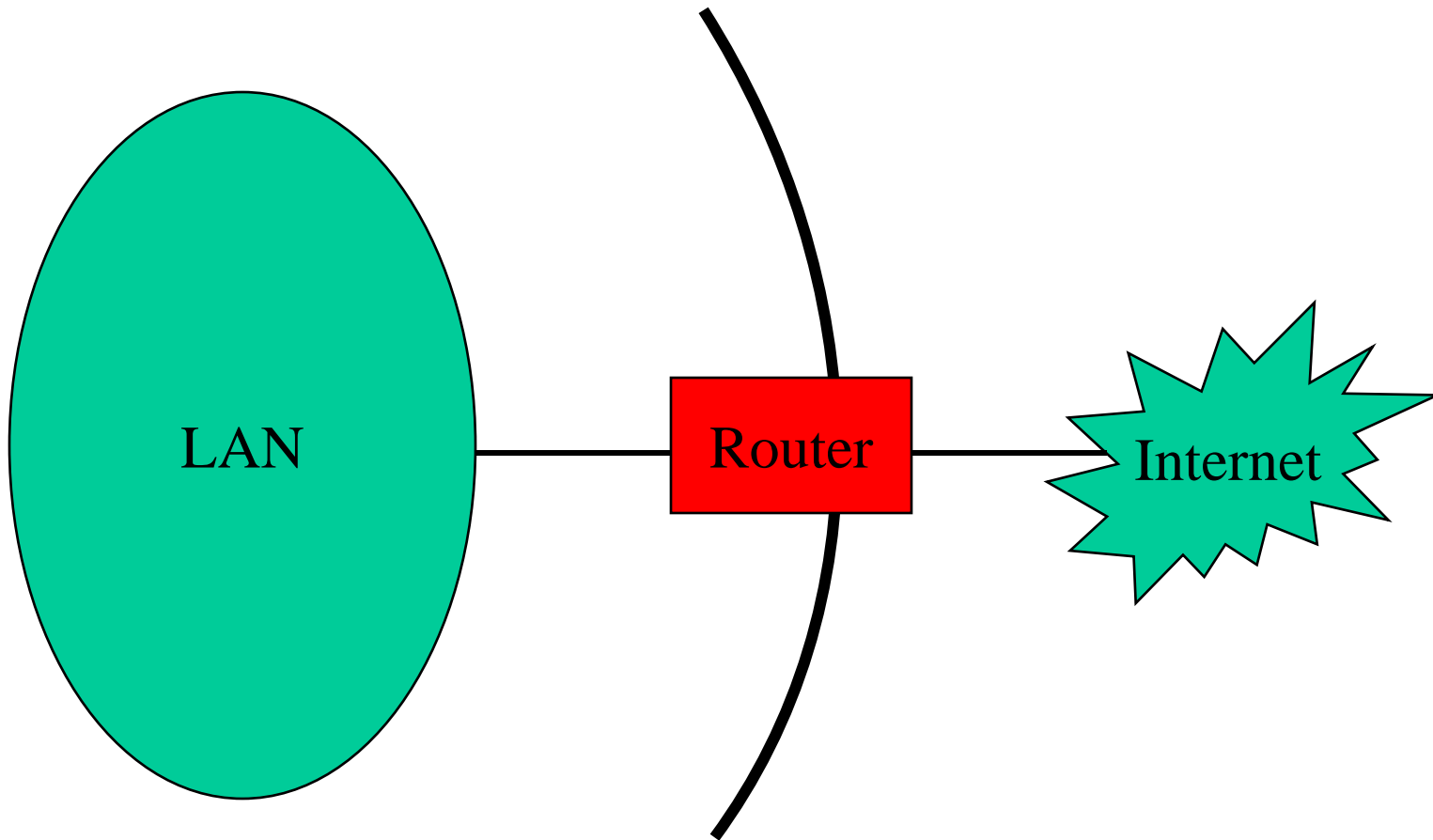
Log di
traffico complessivo
azioni dei singoli utenti

Generazione allarmi

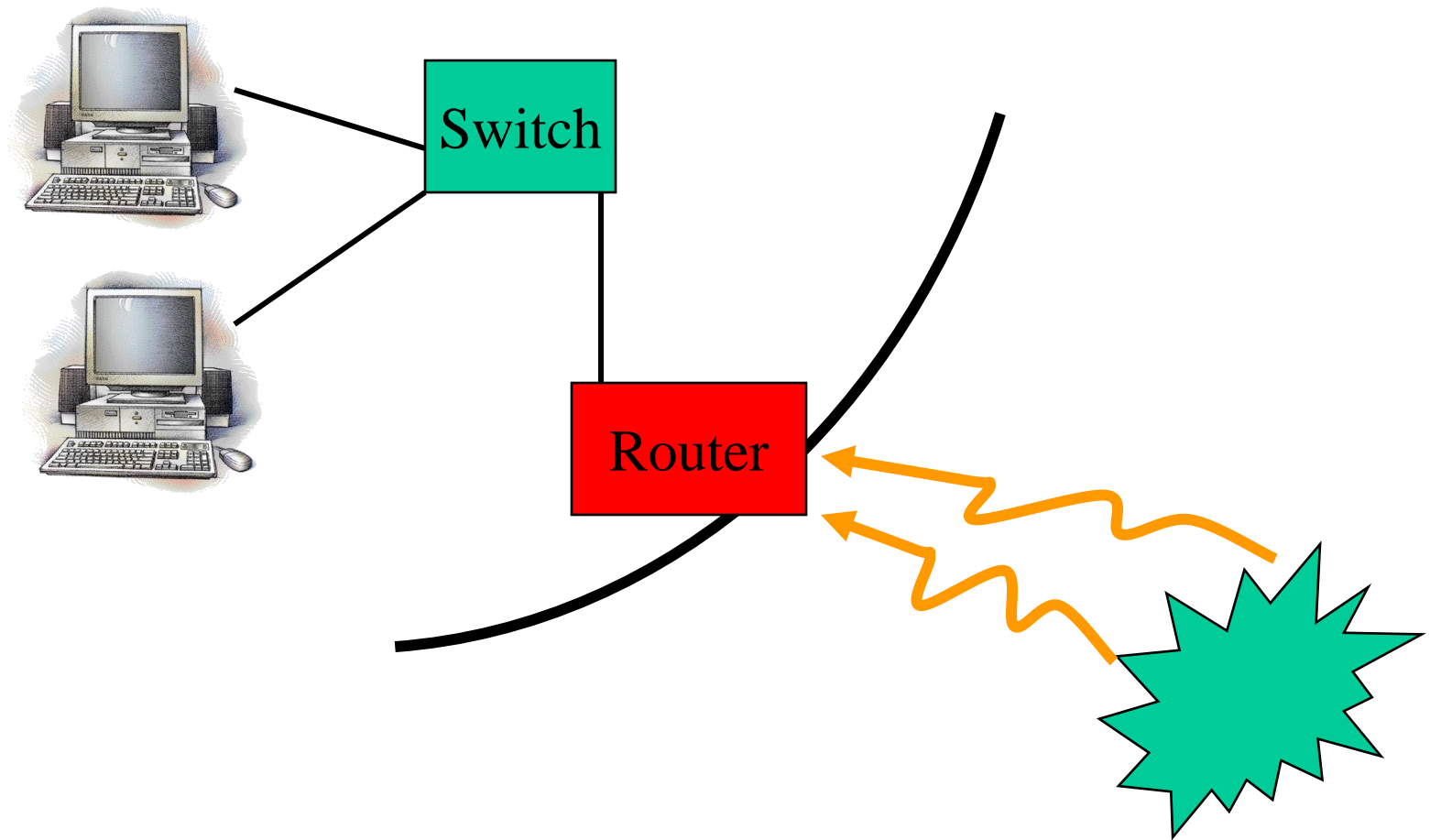
Configurazione Firewall

- **Screening router**
- **Dual-homed gateway**
- **Screened host gateway**
- **Screened subnet**

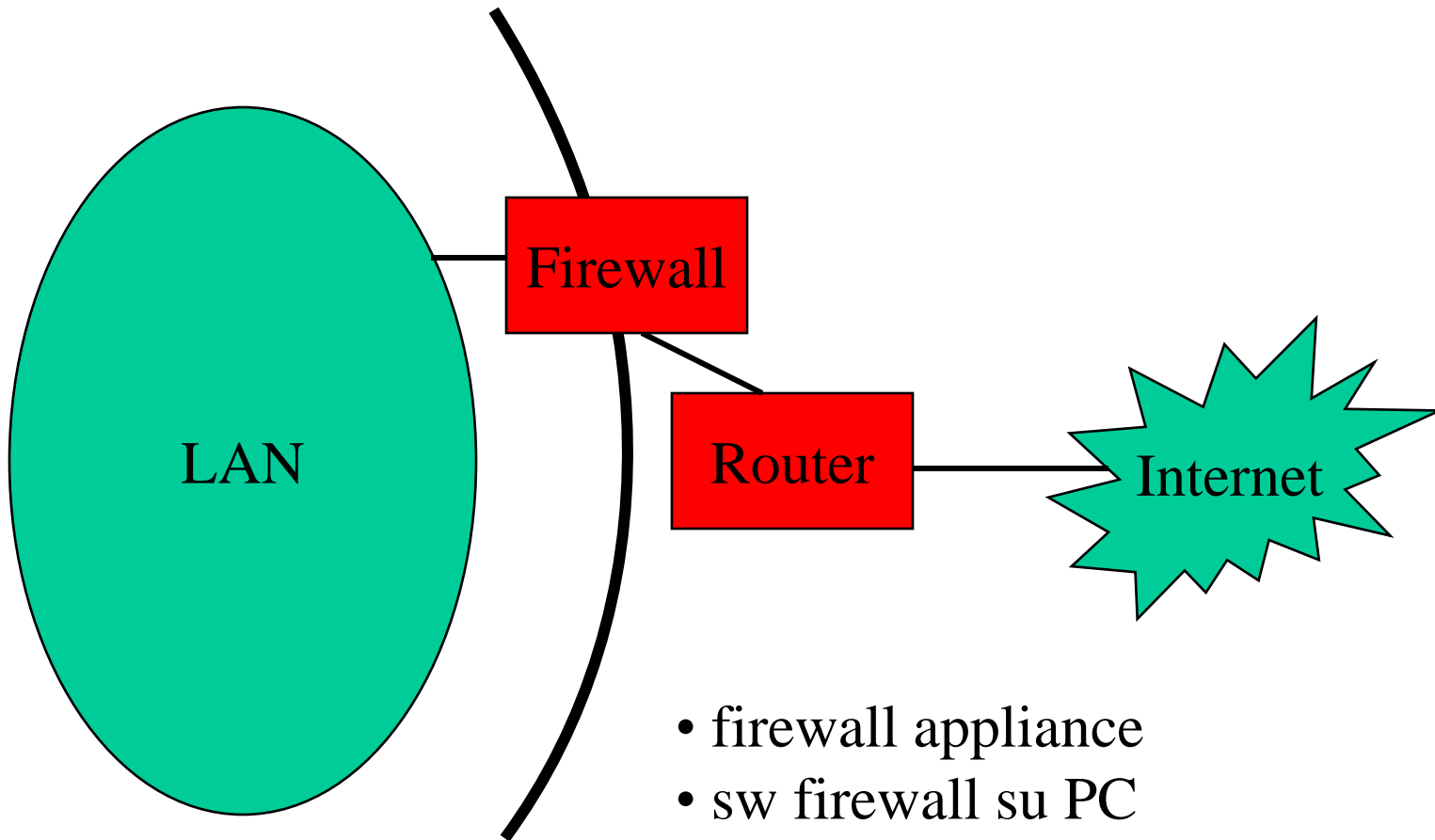
Screening Router



Screening Router

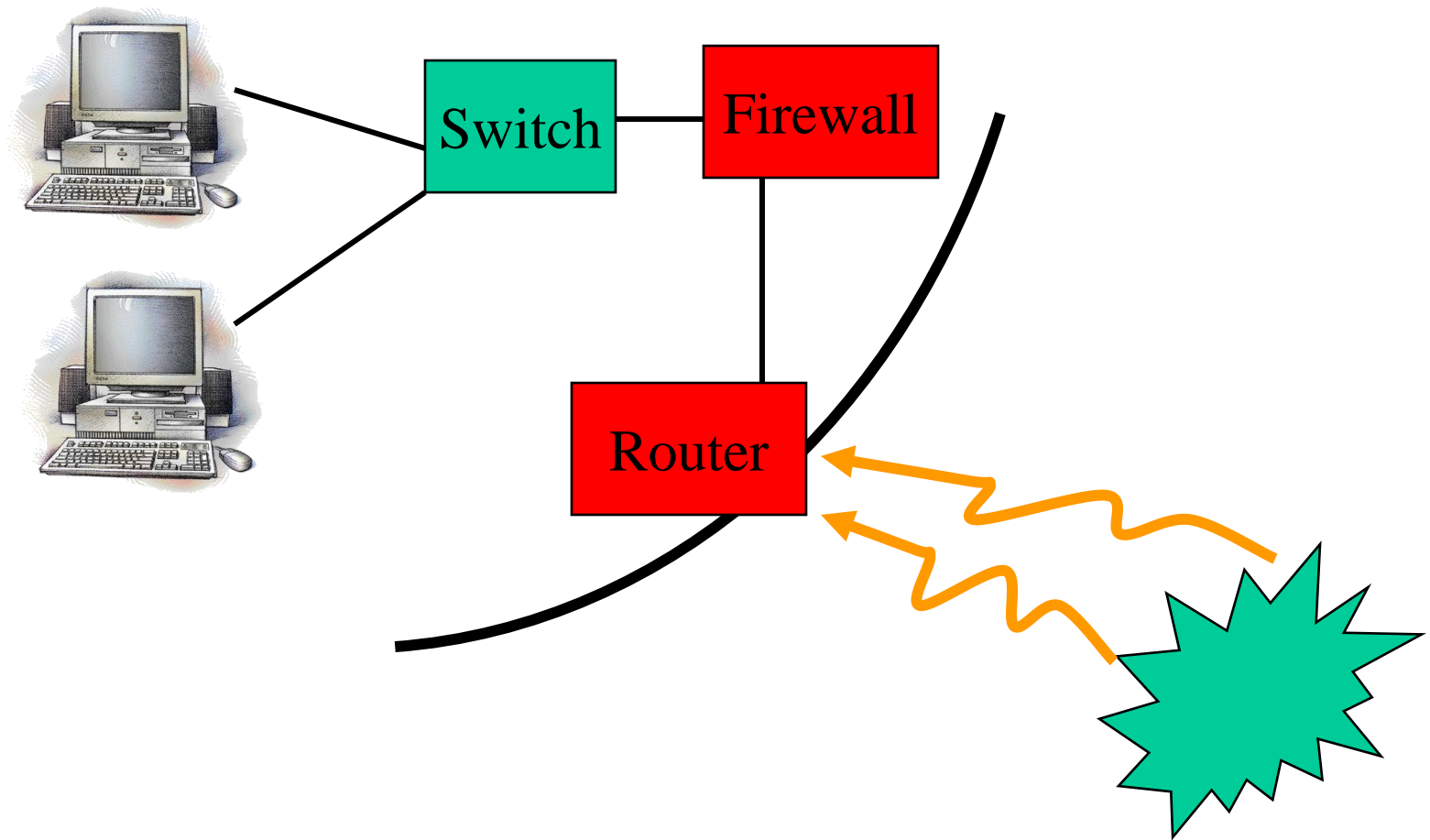


Dual homed gateway

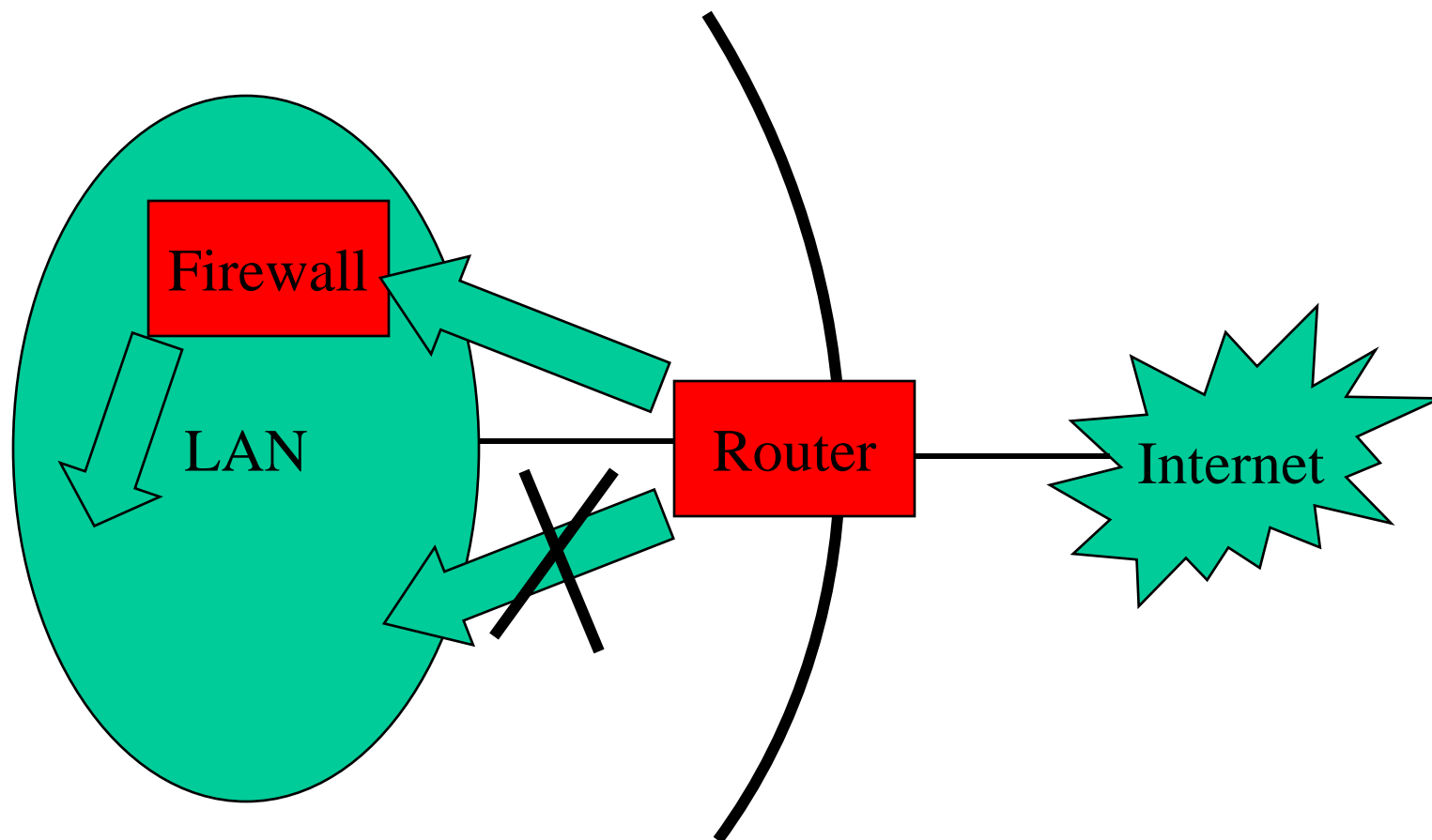


- firewall appliance
- sw firewall su PC
- sw firewall su Calcolatore Custom

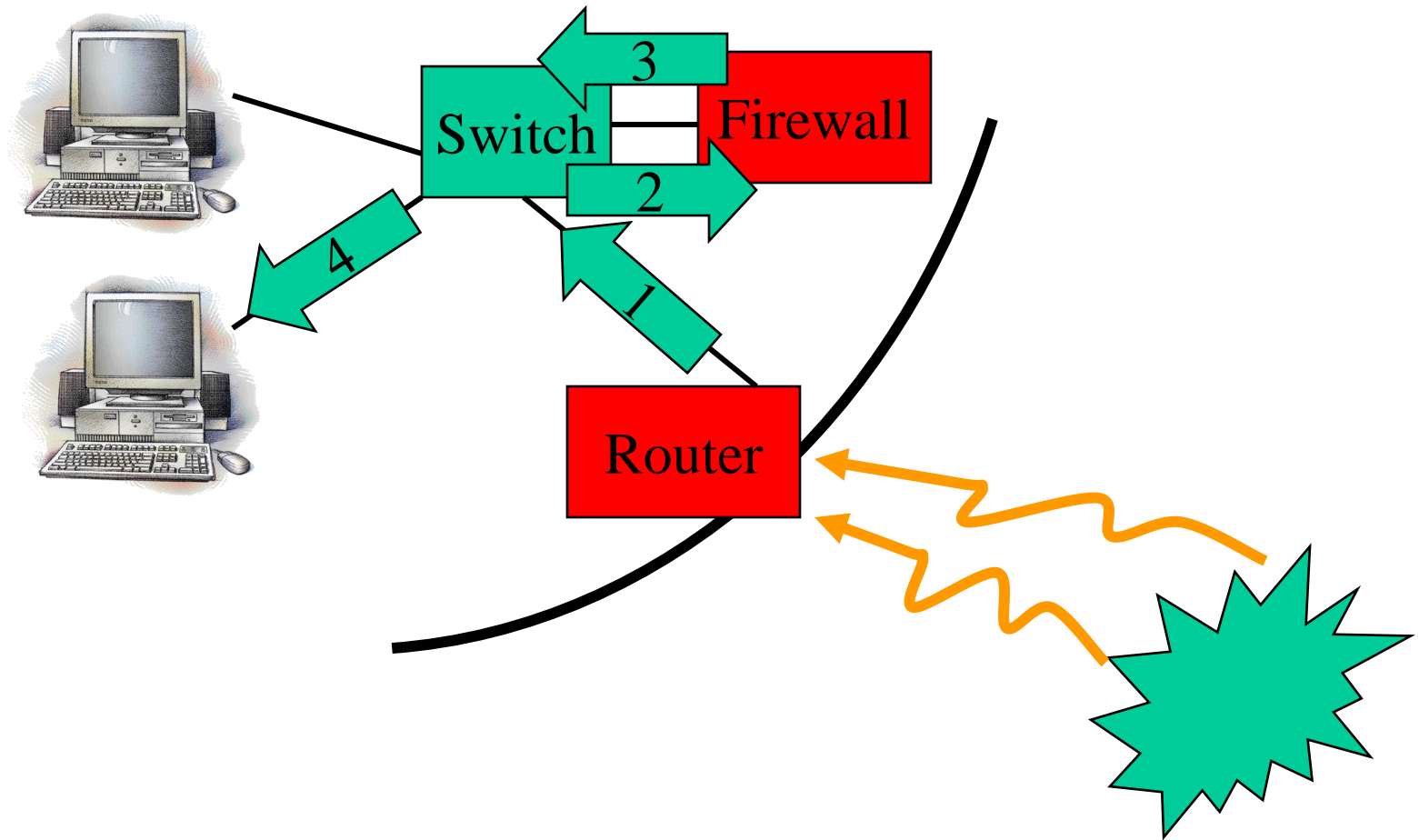
Dual homed gateway



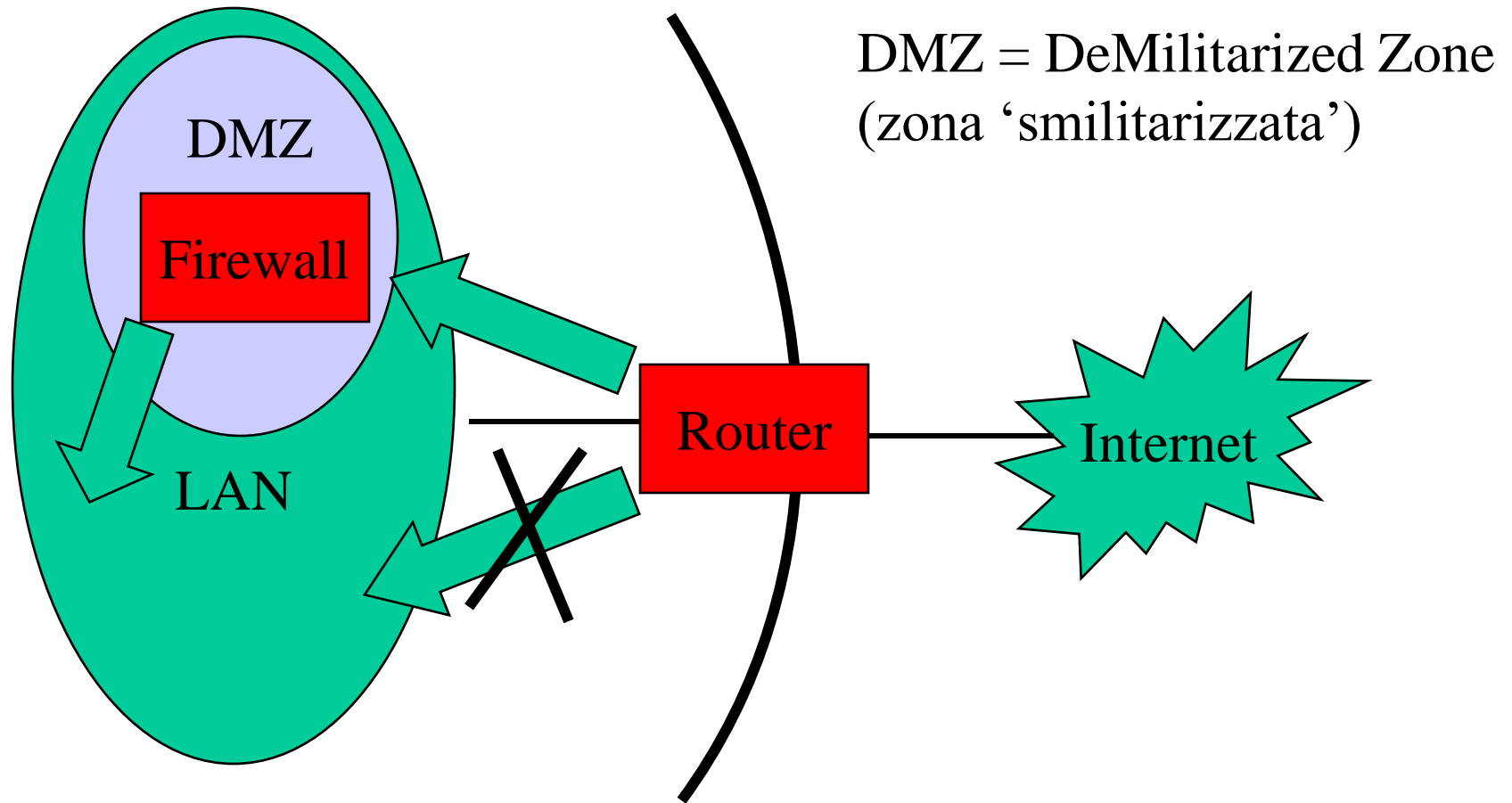
Screened host gateway



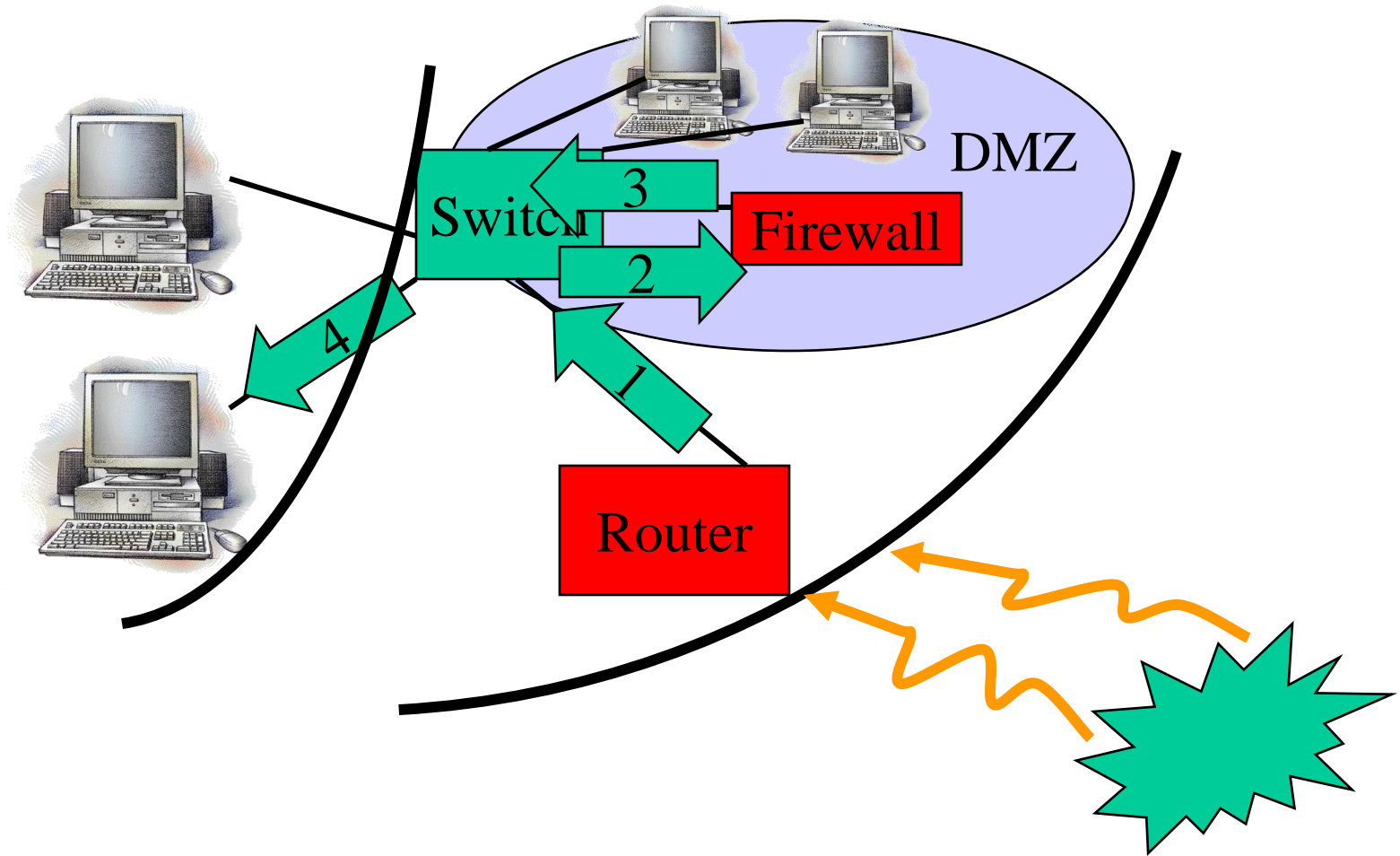
Screened host gateway



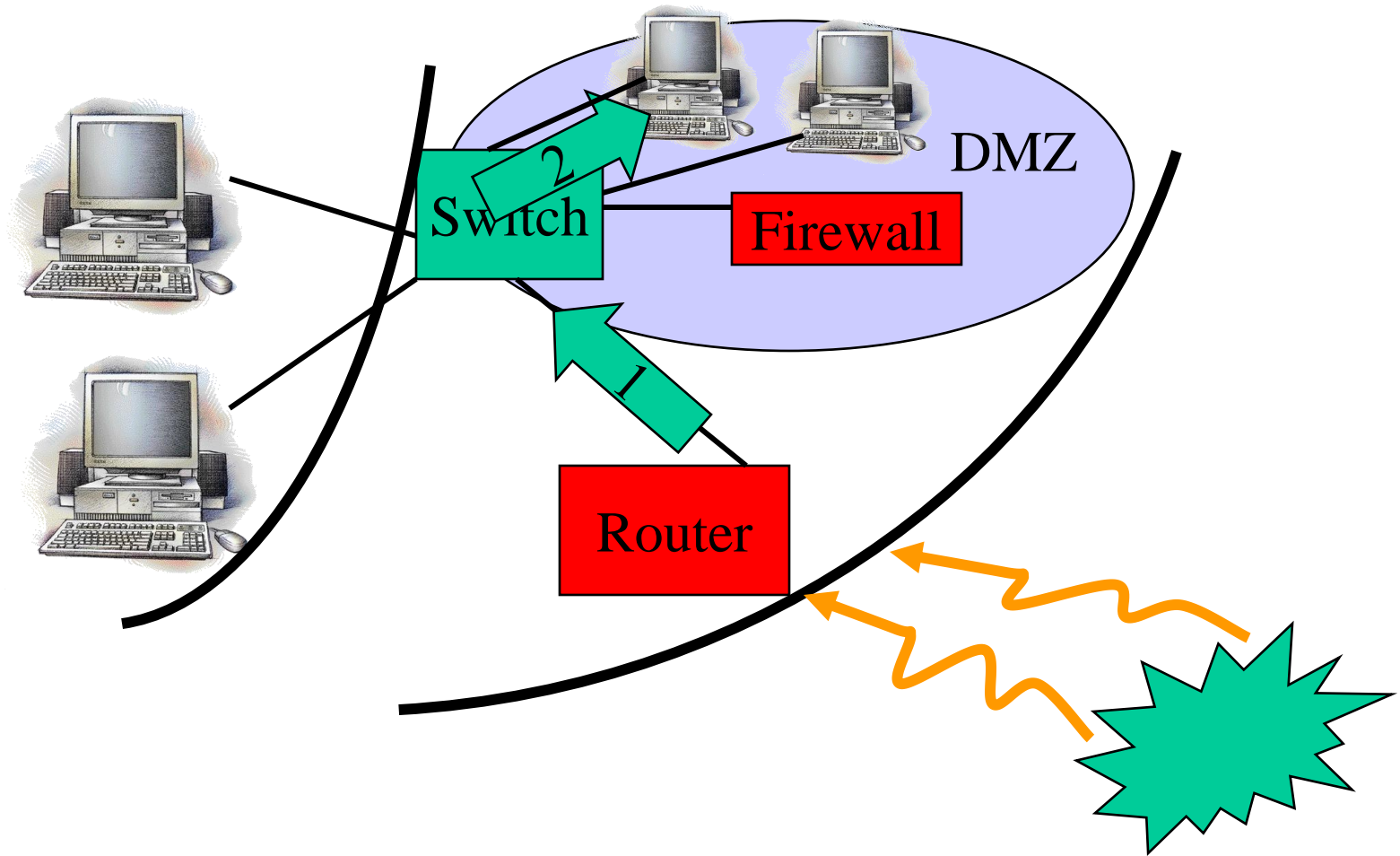
Screened subnet (1 firewall single homed)



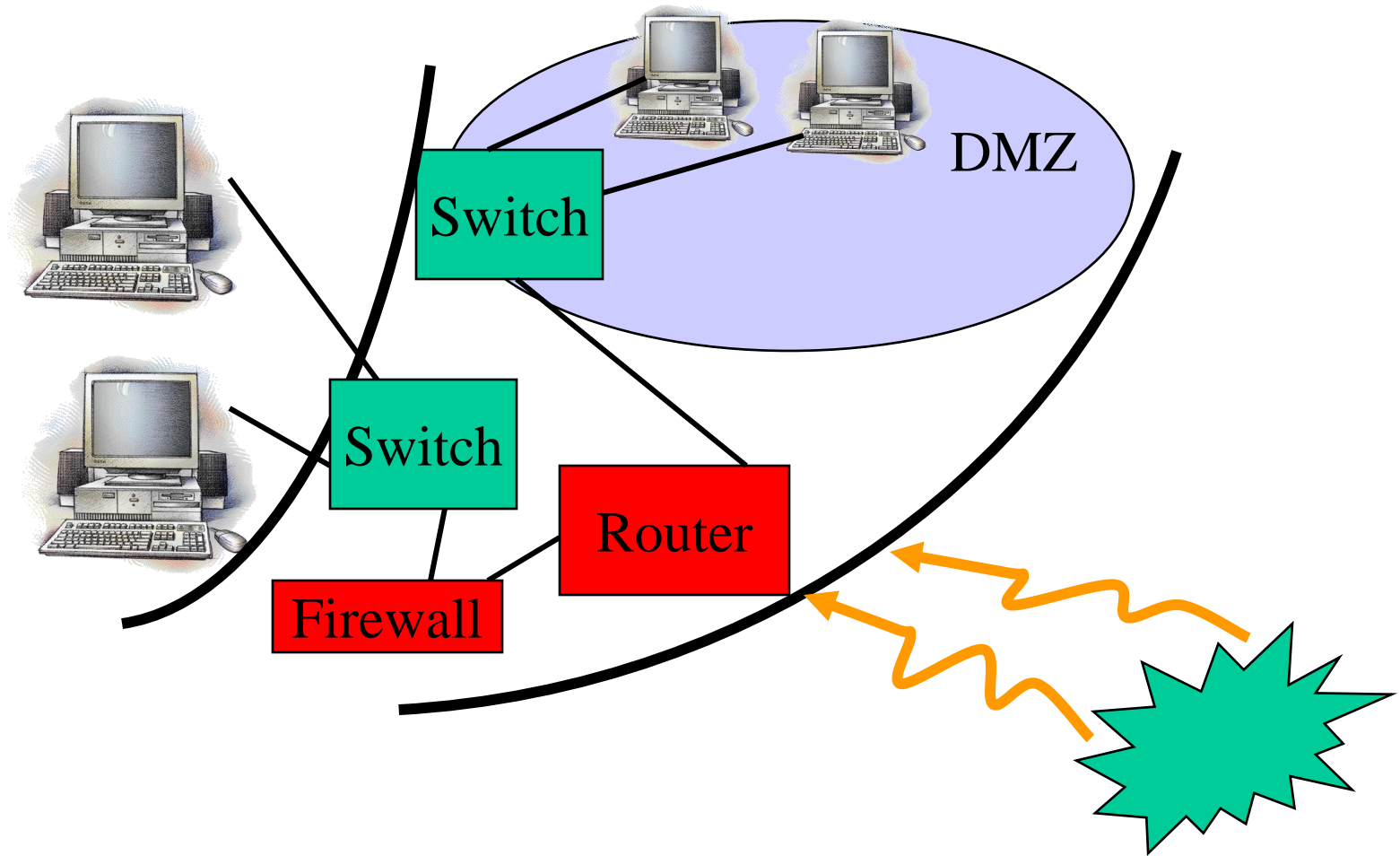
Screened subnet (1 firewall single homed)



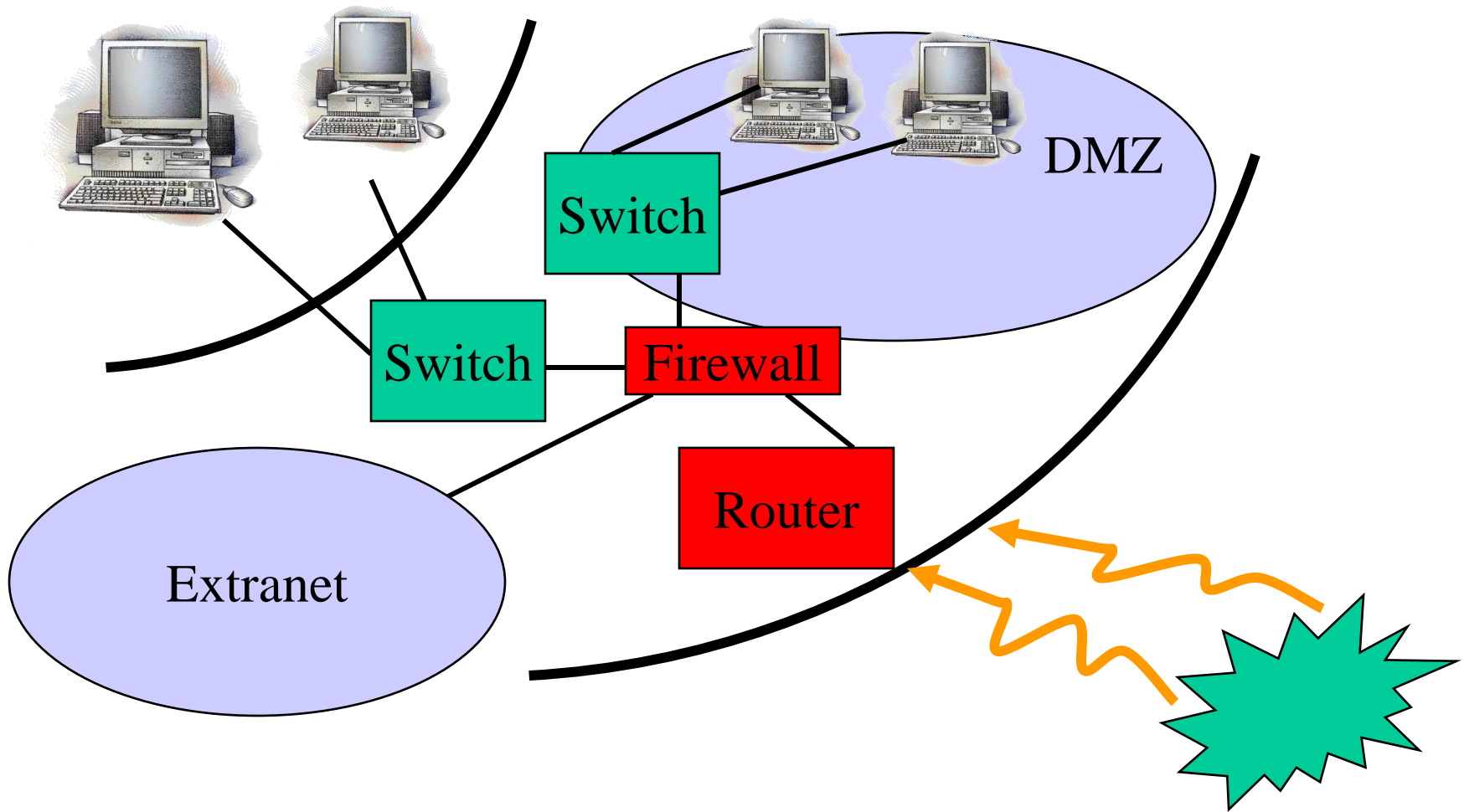
Screened subnet (1 firewall single homed)



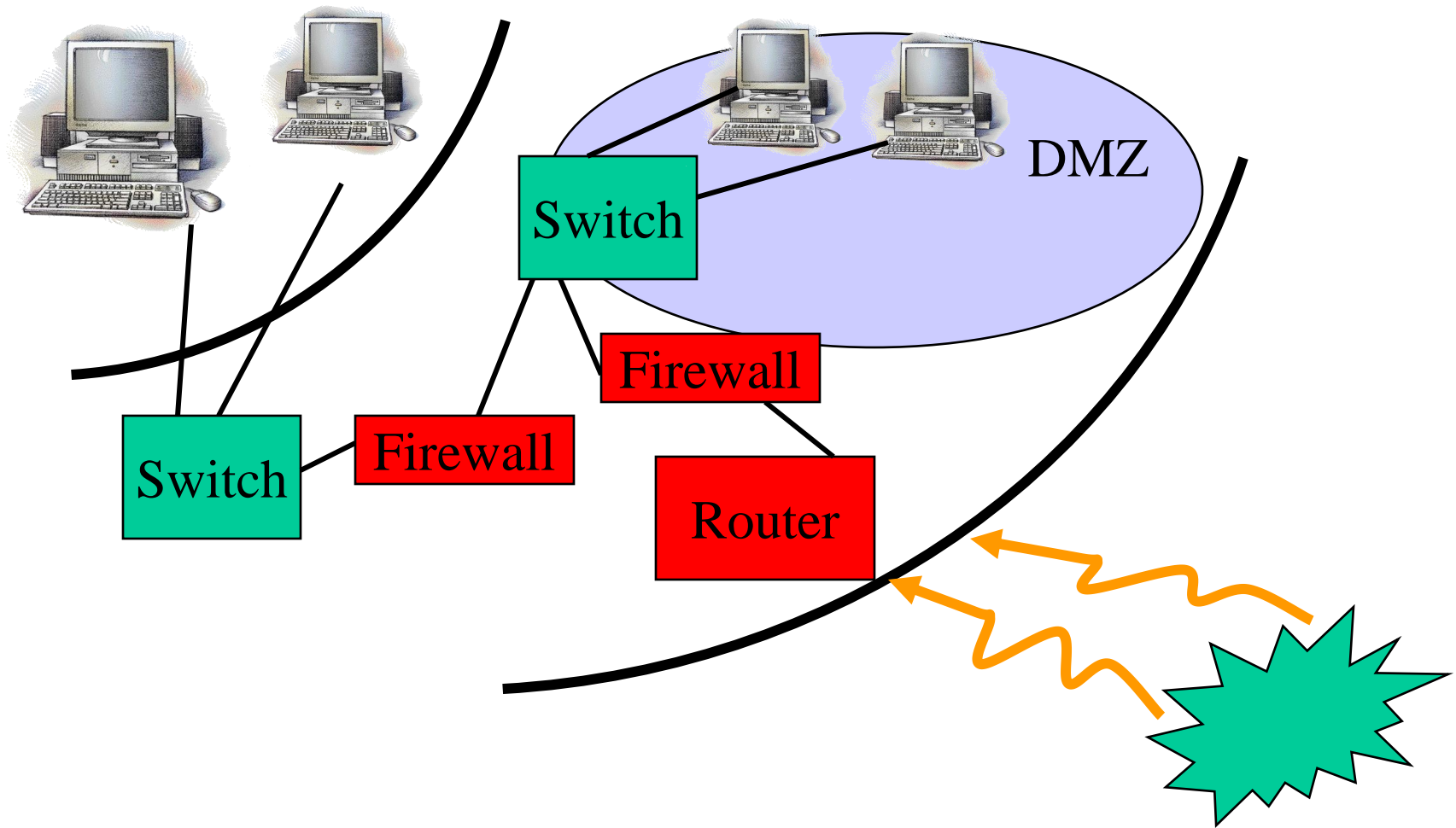
Screened subnet (1 firewall dual homed)



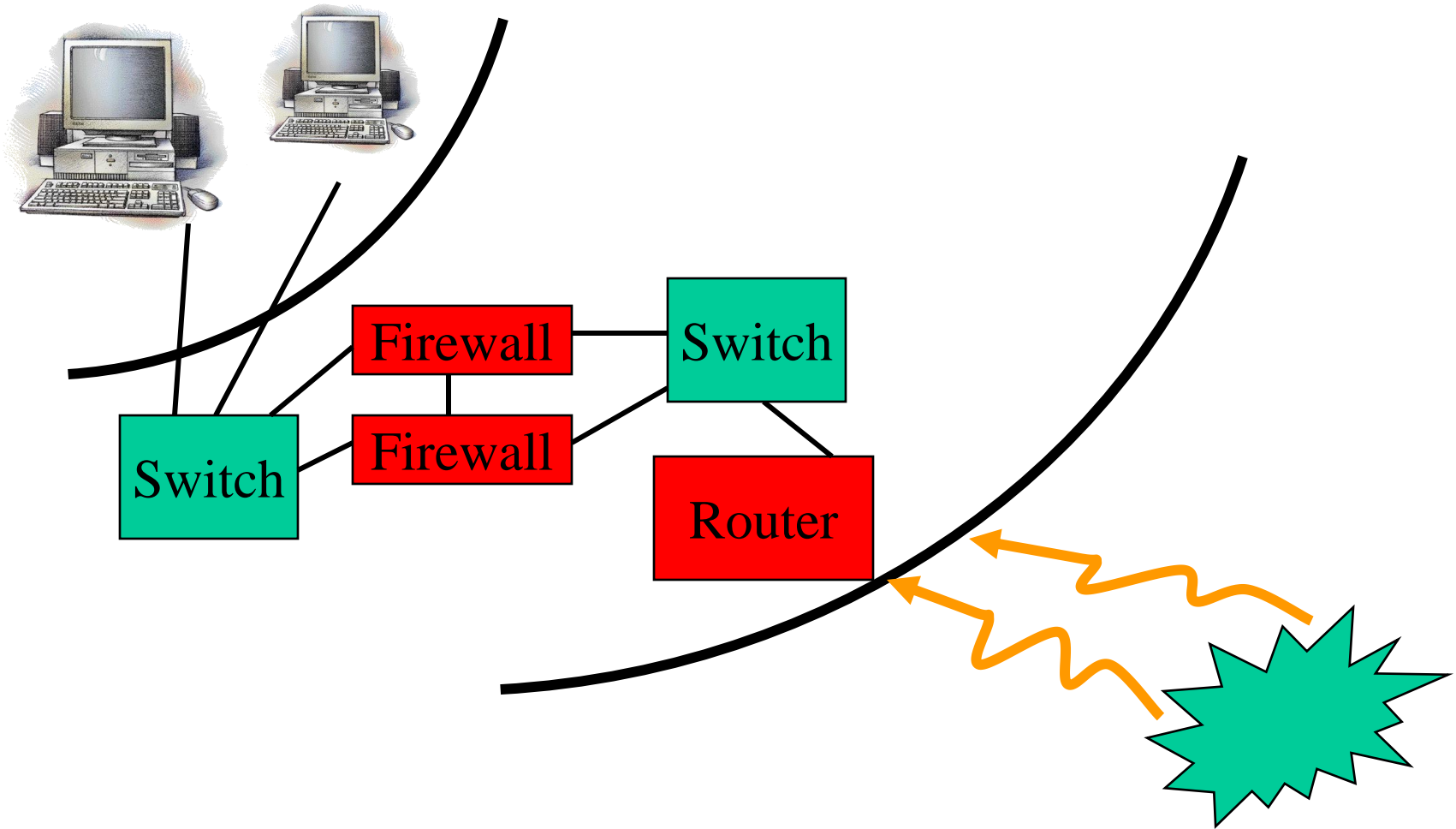
Screened subnet (1 firewall 4 interfaces)



Firewall in cascata



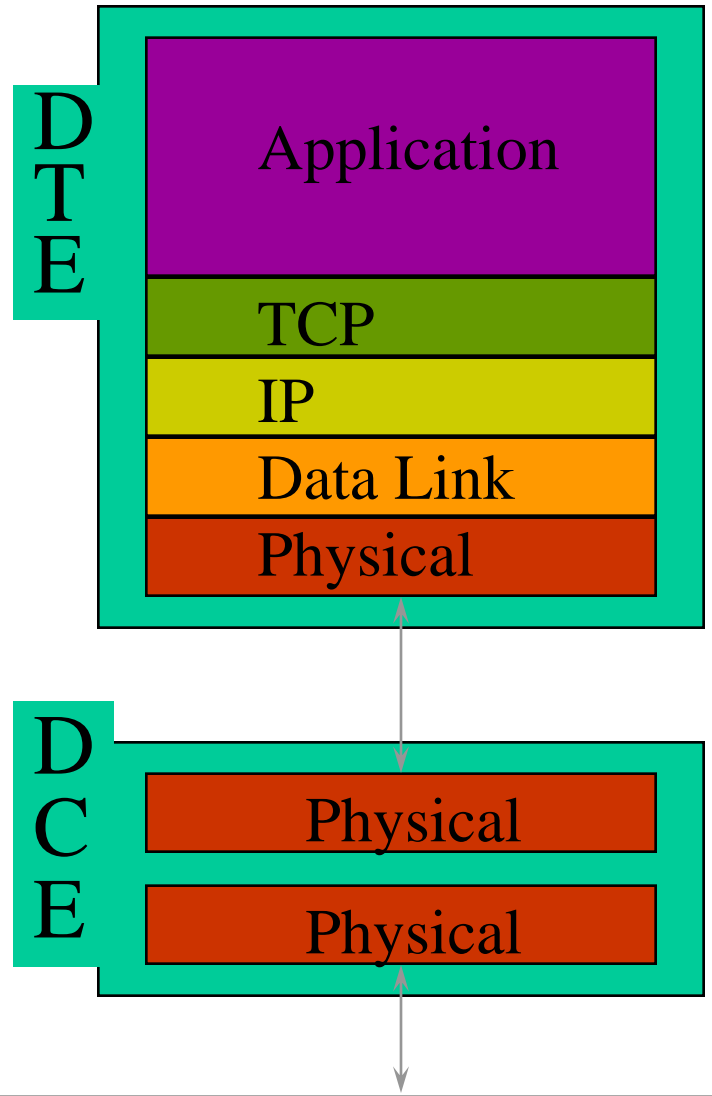
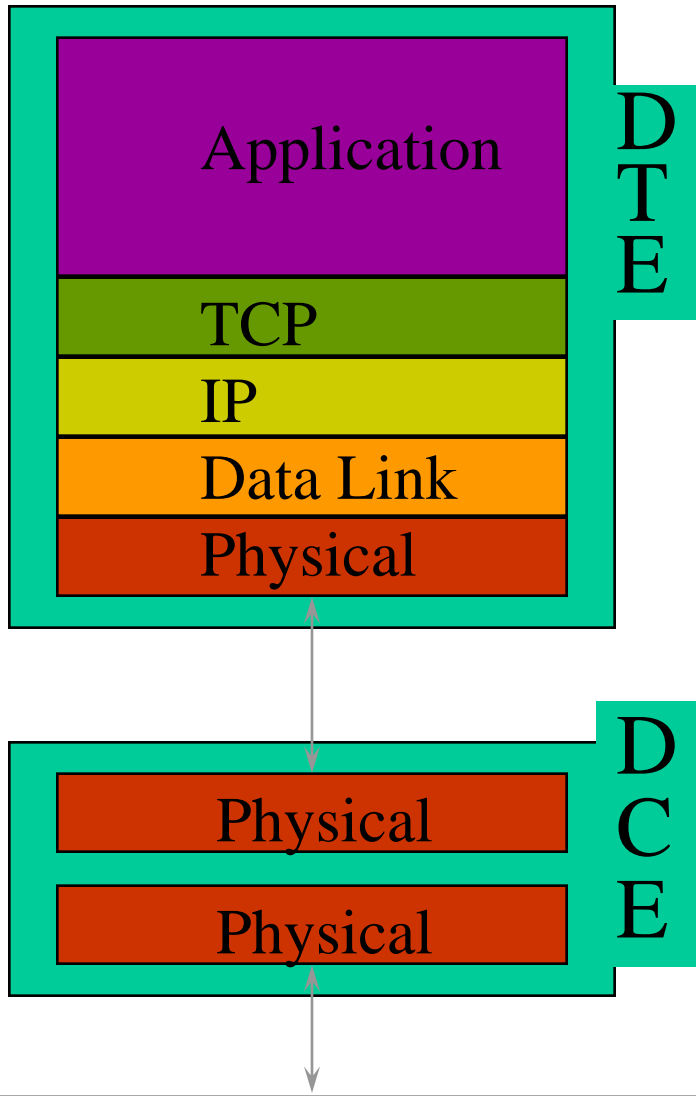
High availability

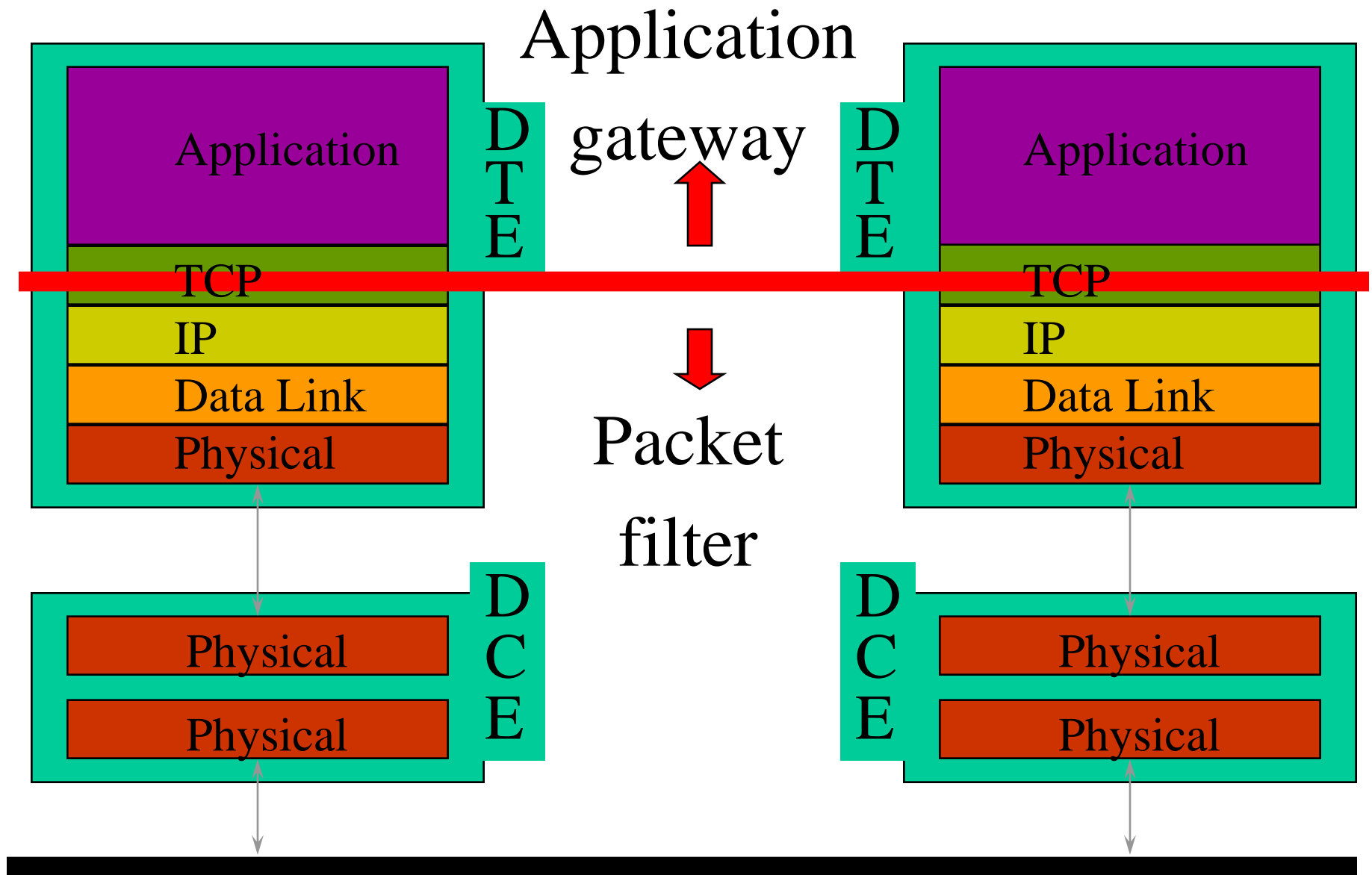


Tipi di Firewall

- **Un router che filtra pacchetti (packet filter)**
- **Un calcolatore attraverso il quale il traffico passa e viene filtrato e registrato a livello applicativo (application proxy)**

livelli TCP/IP





Packet Filter

Filtra in base a:

- **Direzione del pacchetto (da o verso l'esterno)**
- **Direzione della connessione TCP (da o verso l'esterno)**
- **Indirizzo IP sorgente e destinazione**
- **Servizio = porta sorgente e porta destinazione:**
 - SMTP = porta 25
 - HTTP = porta 80
 - FTP = porta 21

Alcune porte note (well-known)

Meglio permettere

20	TCP	dati FTP
21	TCP	controllo FTP
23	TCP	telnet
25	TCP	SMTP
53	UDP	DNS
53	TCP	DNS
80	TCP	HTTP
110	TCP	POP-3

Meglio bloccare

43	TCP	whois
67	UDP	bootp
69	UDP	tftp
79	TCP	finger
161	UDP	SNMP
521	TCP	exec
517	UDP	talk
540	TCP	uucp

un problema importante nella configurazione di un firewall riguarda la frammentazione IP. Infatti se un pacchetto viene frammentato in pezzi molto piccoli, ogni parte può essere tanto ridotta da non includere neanche l'header TCP e quindi la porta utilizzata nel firewall per filtrare.

Questo succede per frammenti di poco più di 20 byte, che sono comunque ingiustificati rispetto a qualsiasi MTU. Tali frammenti corti devono quindi essere tagliati.

Esempio di filtro su router - I

Access Control List (ACL)

action	prot	srcaddr	srcp	dstaddr	dstp	flags
allow	TCP	130.192.239.0	*	*	23	*
allow	TCP	*	23	130.192.239.0	*	ACK

Permette Telnet dall'interno (130.192.239.*) verso l'esterno

Impedisce connessioni Telnet dall'esterno verso l'interno

In mancanza di altre regole impedisce ogni altra connessione da e verso l'esterno.

Esempio di filtro su router - I

Access Control List (ACL)

action	prot	srcaddr	srcp	dstaddr	dstp	flags
allow	TCP	130.192.239.0	*	*	80	*
allow	TCP	*	80	130.192.239.0	*	ACK

Permette HTTP dall'interno (130.192.239.*) verso l'esterno

Impedisce connessioni HTTP dall'esterno verso l'interno

FTP

porta 20 (dati) e porta 21 (controllo)

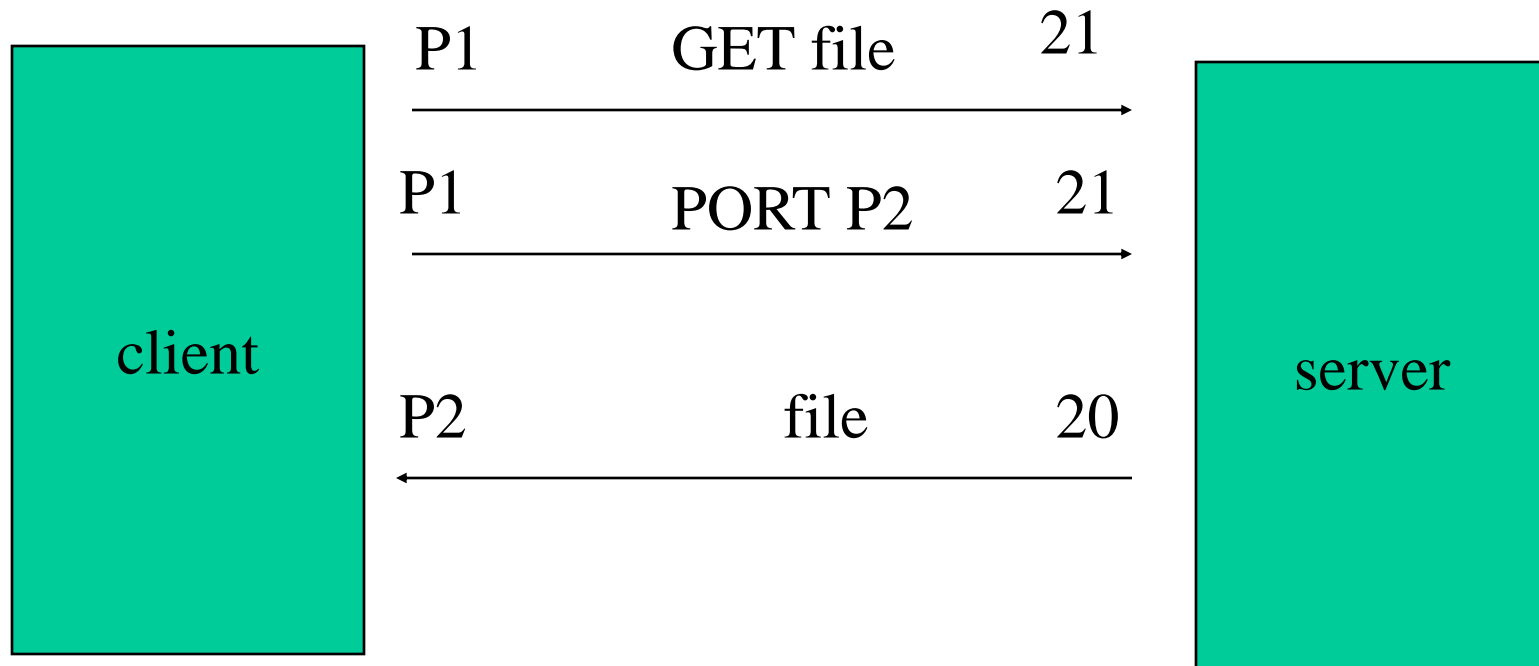
collegamento iniziale al server FTP su porta 21

file transfer richiesto dal client con 'GET' e 'PORT'

client FTP aspetta dati sulla porta indicata


traferimento file da porta 20 remota a porta indicata

FTP



Esempio di filtro su router - II

action	prot	srcaddr	srcp	dstaddr	dstp	flags
allow	TCP	130.192.239.0	*	*	21	*
allow	TCP	*	21	130.192.239.0	*	ACK
allow	TCP	130.192.239.0	*	*	20	*
allow	TCP	*	20	130.192.239.0	*	ACK



Permette FTP dall'interno (130.192.239.*) verso l'esterno

Permette traffico da applicazioni custom

Soluzione per FTP

- **vietare FTP**
- **firewall / filtro ‘application aware’ o ‘stateful’ (quindi con memoria - ricorda la porta dati lato client e permette la connessione solo su quella porta e su quell’indirizzo)**
- **usare FTP modificato**

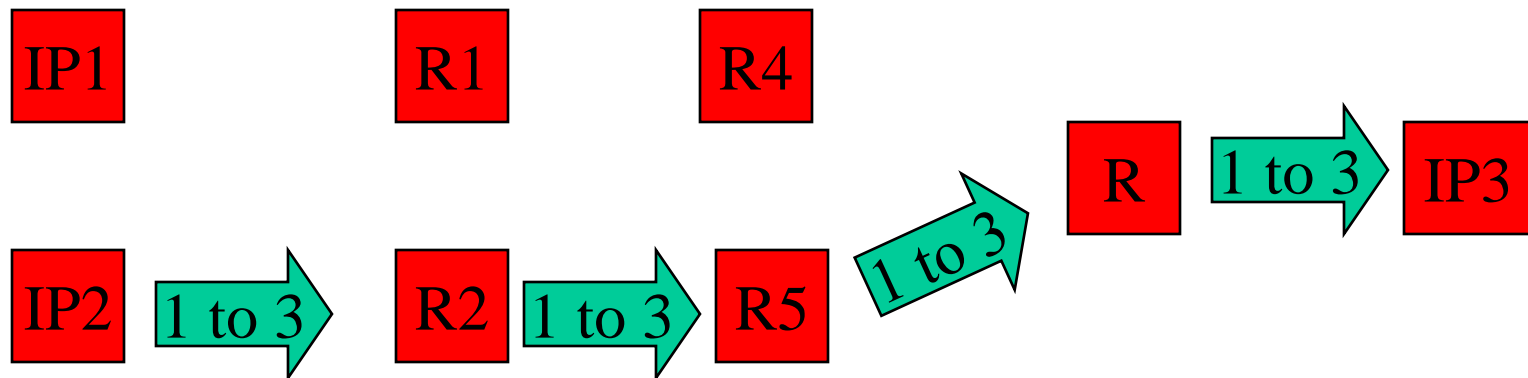
Esempio di filtro su router - III

action	prot	srcaddr	srcp	dstaddr	dstp	flags
deny	*	130.192.239.0	*	130.192.239.0	*	*

Blocca il traffico proveniente dall'esterno verso l'interno, ma con un indirizzo di provenienza che risulta interno, cosa impossibile, indice di address spoofing.

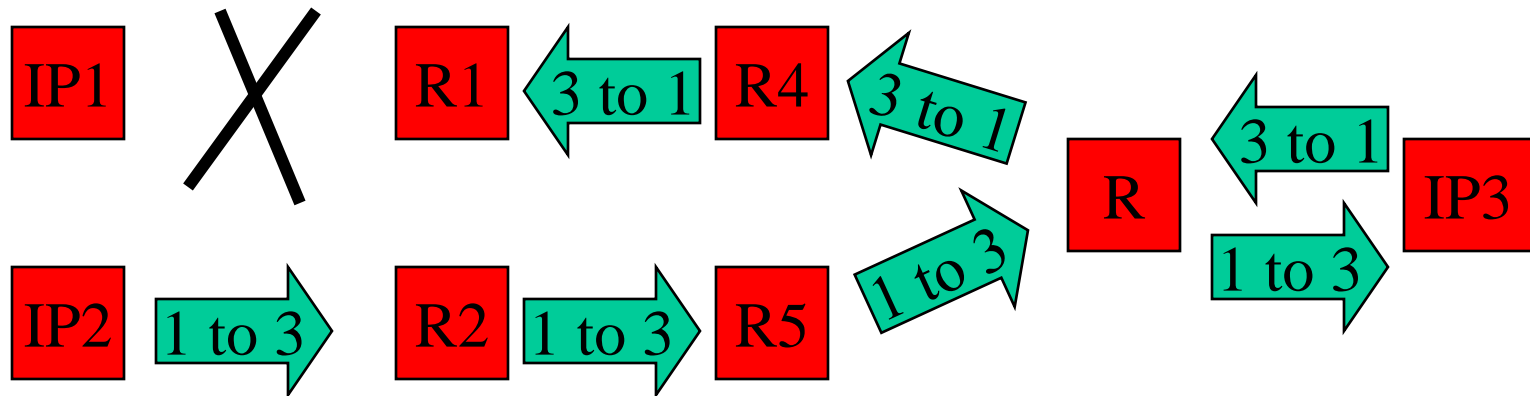
Packet Filter

Un'altra importante regola è bloccare tutti i pacchetti con l'opzione di source routing (permette IP spoofing con TCP su WAN)

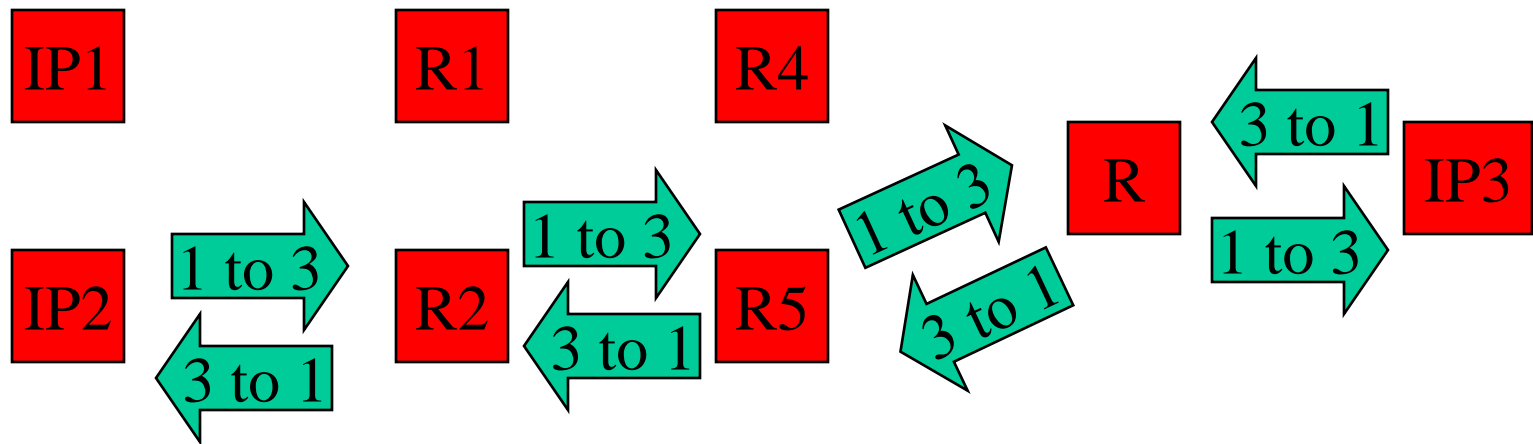


Packet Filter

Un'altra importante regola è bloccare tutti i pacchetti con l'opzione di source routing (permette IP spoofing con TCP su WAN)



Con source routing l'address spoofing diventa possibile



Packet Filter

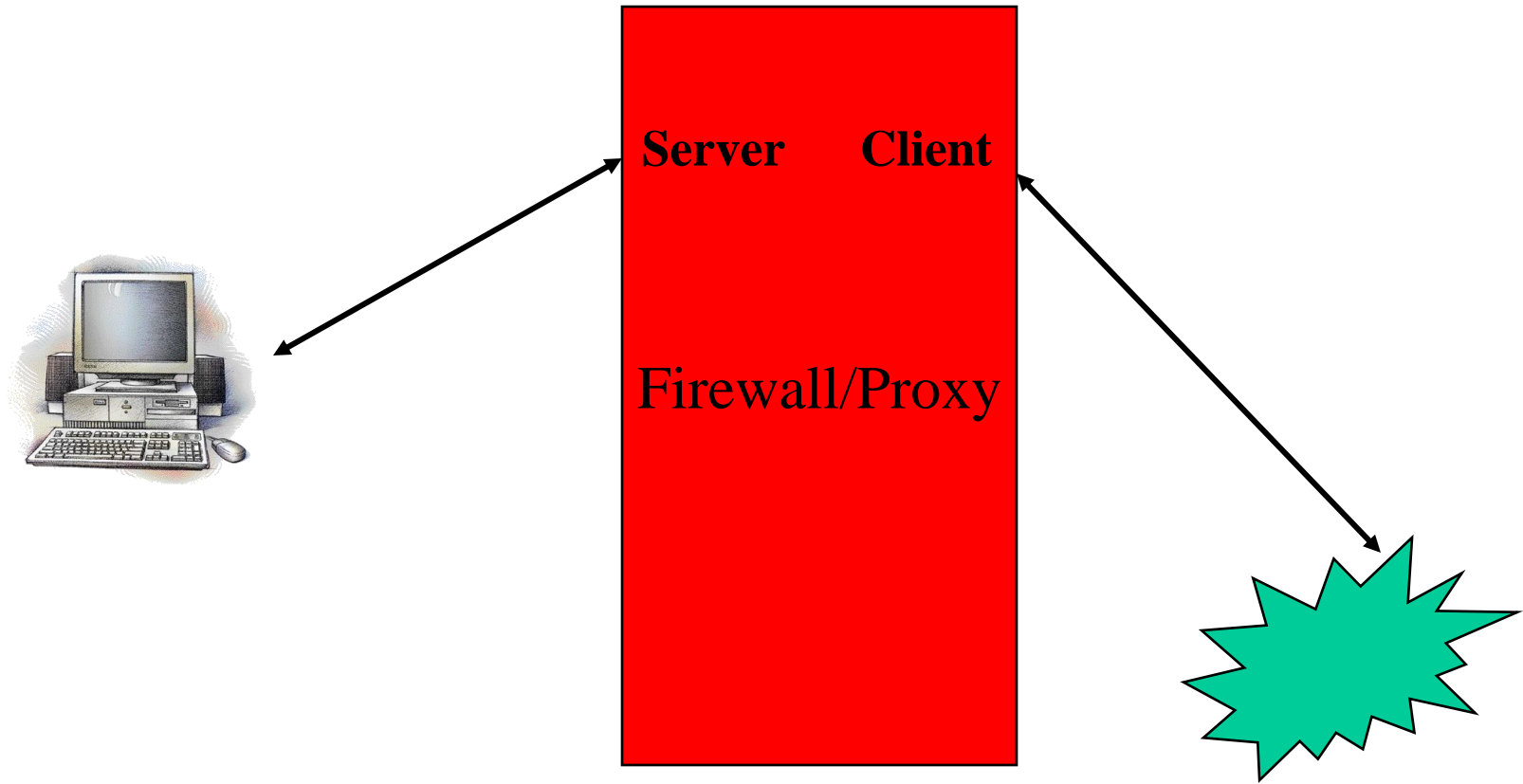
- **Nessuna modifica alle applicazioni (trasparenza)**
- **Economico (realizzato su router)**
- **Alte prestazioni**
- **Difficoltà con alcuni protocolli**
- **Non selettivo rispetto agli utenti**
- **Non mantiene log**
- **Difficile monitorare gli attacchi mentre avvengono**

Firewall di livello applicativo

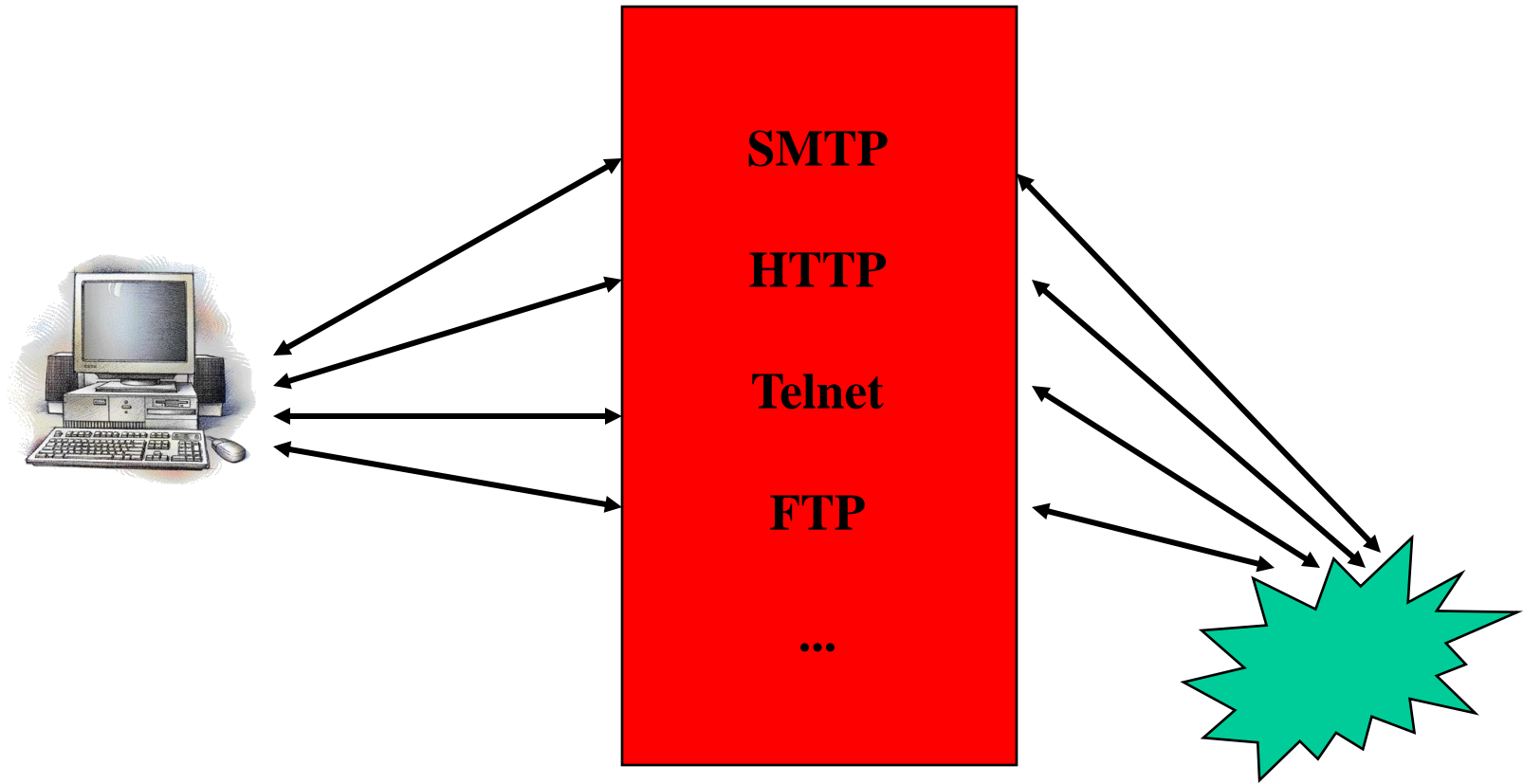
**Le connessioni dirette tra interno
ed esterno sono proibite**

**Solo le connessioni attraverso il
firewall sono possibili**

Firewall come Proxy



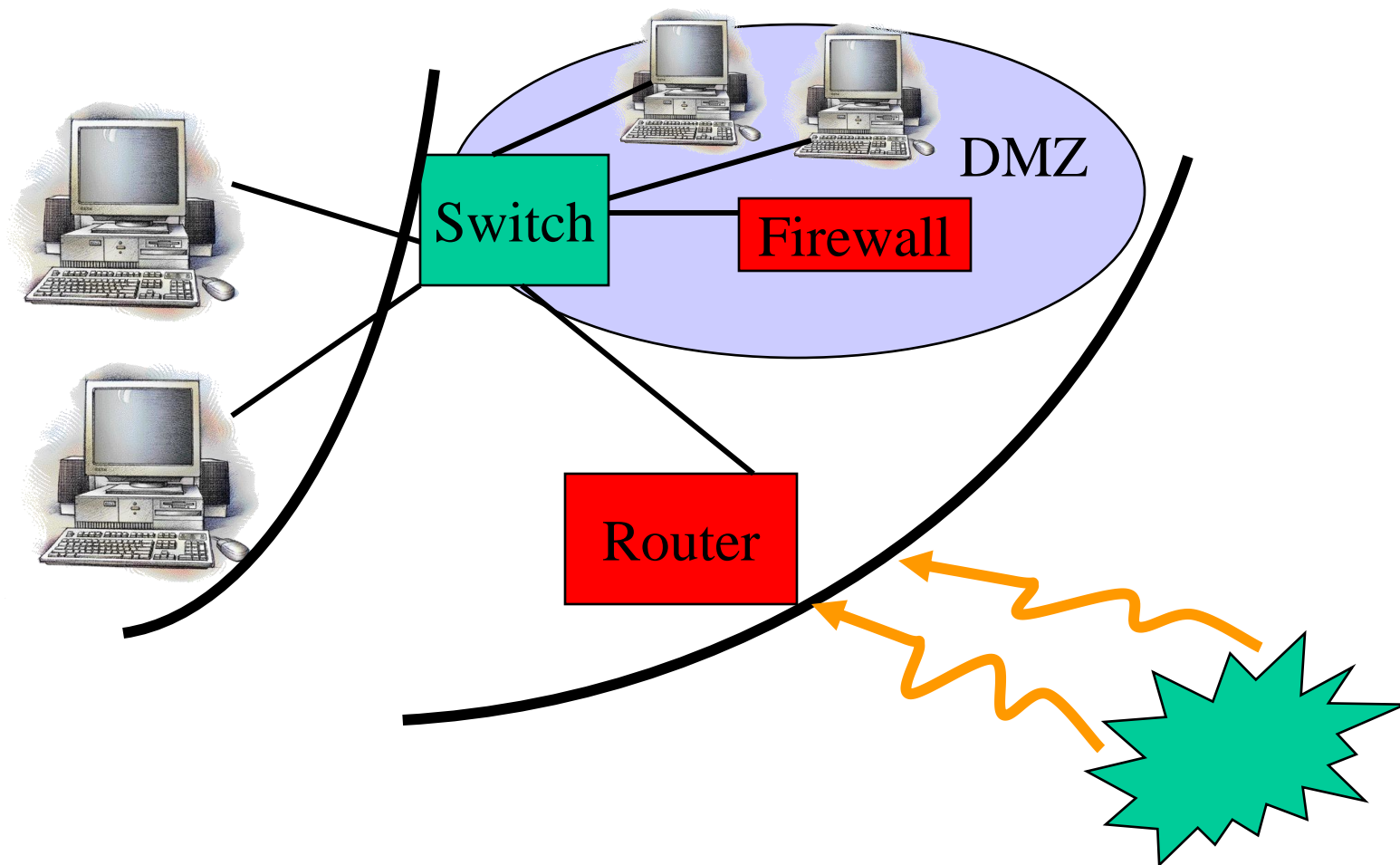
Ogni servizio deve essere configurato



Firewall di livello applicativo

- **Non trasparente**
- **Richiede un host dedicato**
- **Prestazioni medie**
- **Sicuro**
- **E' in grado di riferire il traffico agli utenti**
- **Mantiene log sofisticati**

Un firewall può anche mascherare gli indirizzi IP interni (livello IP o come proxy)

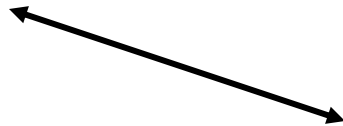


Mascheramento indirizzi interni a livello IP (Network Address Translation - NAT)

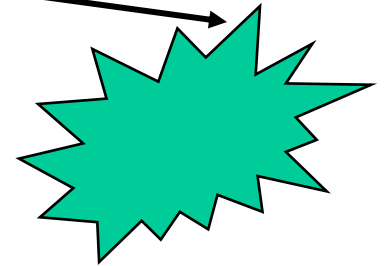
10.10.10.1



10.10.10.2



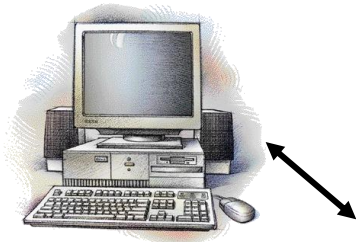
192.10.43.1



Port Address Translation – PAT

Network Addr & Port Transl. - NAT

10.10.10.1 / port 2034



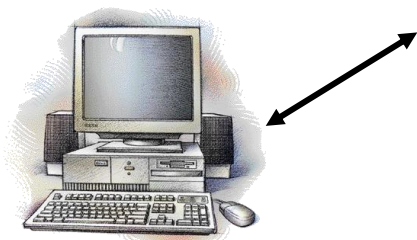
192.10.43.1 / port 2101



NAT device

10.10.10.1/2034 - 192.10.43.1/2101

10.10.10.3/2068 - 192.10.43.1/2102



10.10.10.3 / port 2068

Gestione del Firewall

- **Una macchina affidabile e veloce, in manutenzione, se possibile con fault-tolerance / high availability (HA), oppure una appliance**
- **Sistema operativo e servizi ‘minimi’**
- **No utenti, no NIS, no NFS**
- **Massima attenzione nella protezione di file, password, chiavi crittografiche**
- **esaminare file di log**

Attenzione! Il firewall non risolve tutto

- non evita il problema di password deboli
- non filtra traffico via modem
- non tratta attacchi dall'interno
- non evita problemi di sicurezza sui servizi e sui protocolli aperti verso l'esterno

e, in generale,

- non protegge da virus o simile portato su dischetto
- evitare il 'denial of service'