

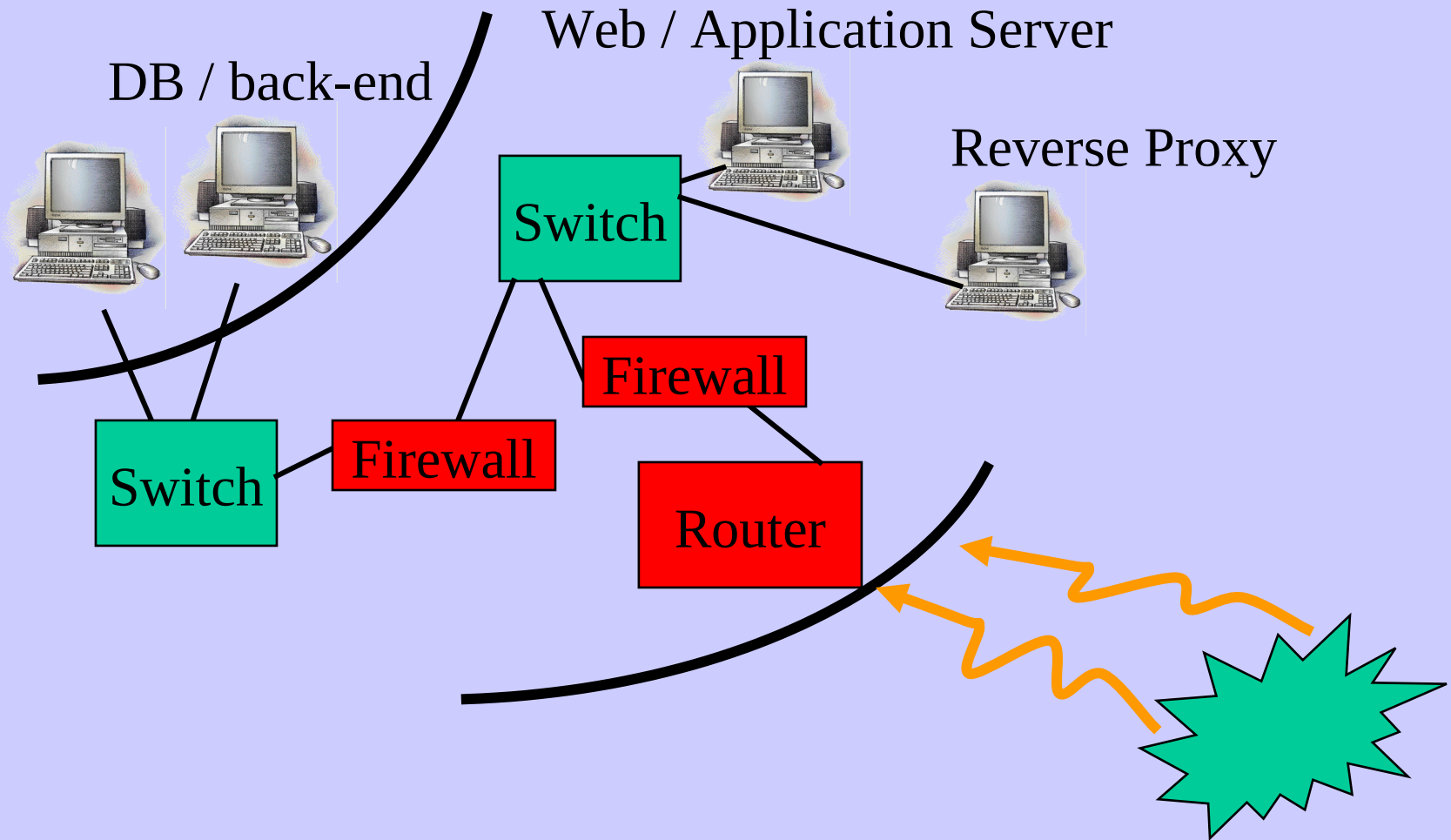
Sicurezza Applicativa: due esempi

Prof. Francesco Bergadano

Dipartimento di Informatica

Universita' di Torino

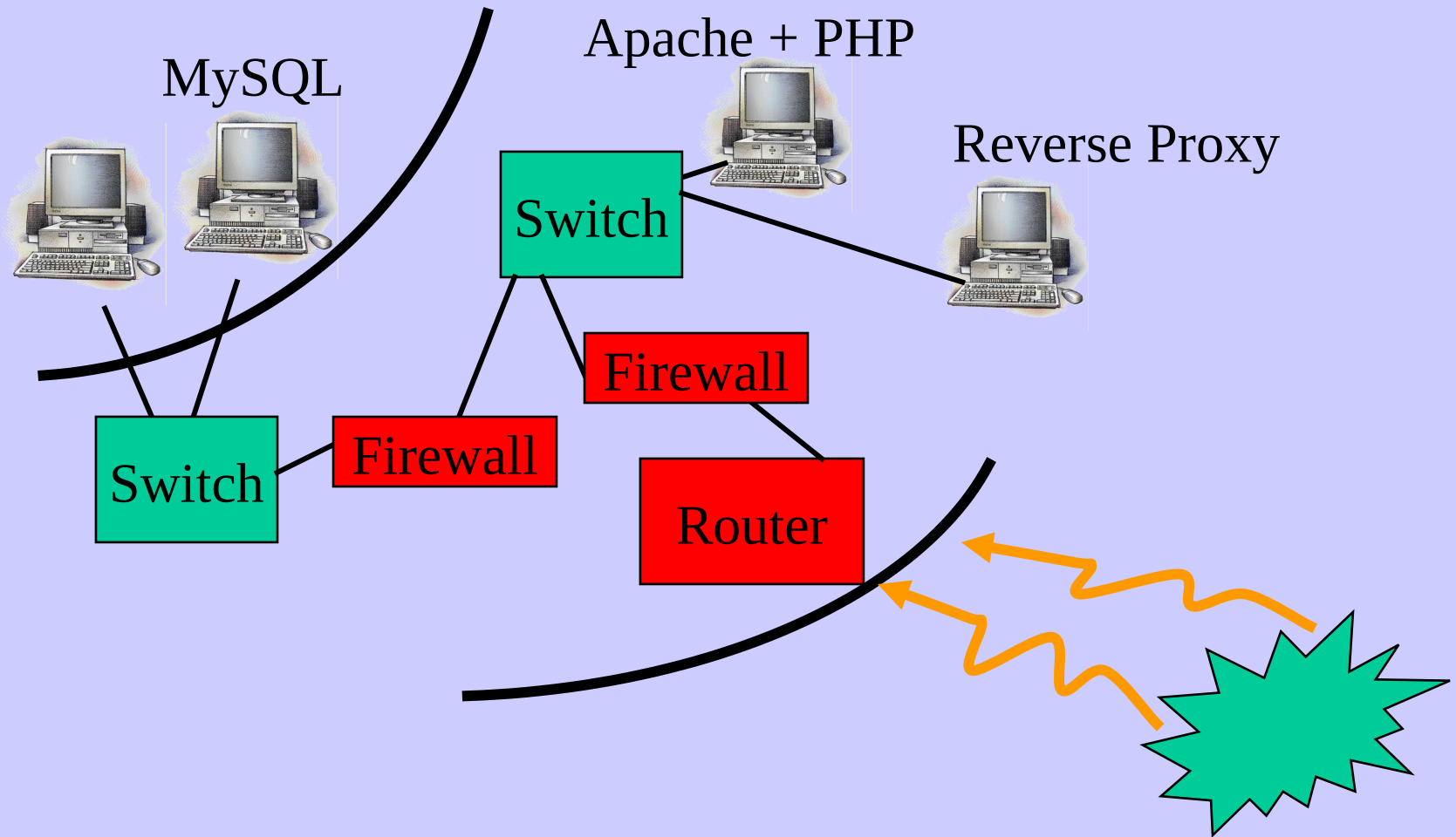
Una possibile architettura



Un esempio

1. **Rete protetta da firewall esterno e reverse proxy**
2. **Una semplice applicazione (http e php) che autentica l'utente con password e risponde con dati riservati**
3. **Un semplice data base (mysql)**
4. **Una vulnerabilità che non può essere fermata dai firewall e 'passa' attraverso i canali cifrati (es. VPN o HTTPS).**

Architettura per l'esempio



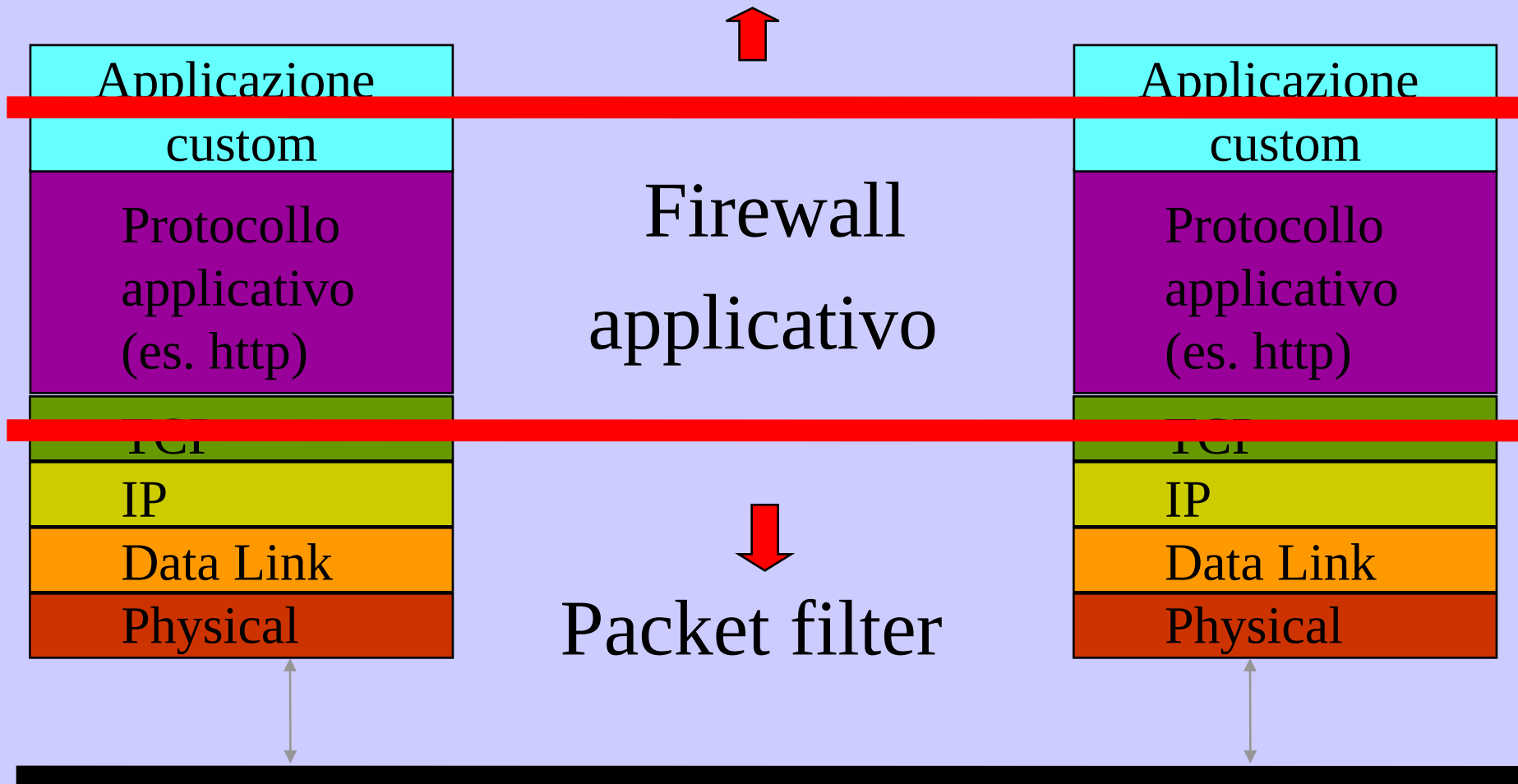
Un primo esempio (vedi 2 immagini a parte)

- Tabella “nomi” e DB “prova” su DB MySQL (con PHPMyAdmin)
- Server Apache con PHP
- File start.php con un form
- File a.php con la gestione del form e la lettura dei dati da DB, quindi visualizzazione della risposta

Un secondo esempio (vedi immagine a parte)

- Sito “A” con Server Apache e PHP
- Un secondo sito “B” malevolo, esterno
- Un link che trae in inganno l’utente
- File start.php con un form
- File a.php con la gestione del form
- File b.php sul sito esterno
- File input.txt con lo script da inserire in start

Sicurezza applicativa



Conclusione

*L'esempio di SQL Injection non può
in generale essere fermato dai
firewall, né essere evitato mediante
encryption o autenticazione di
messaggio, idem per XSS*