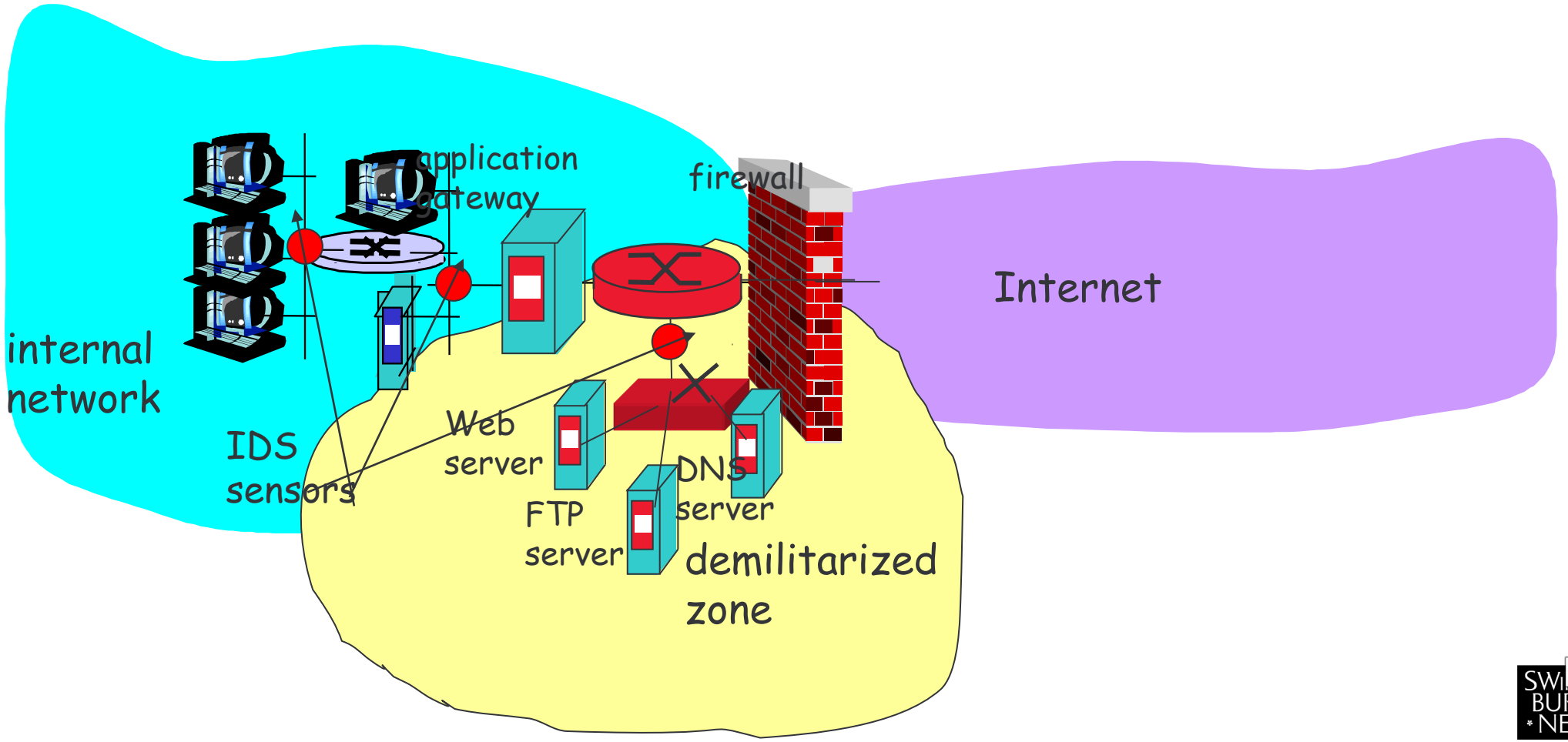
Intrusion Detection

Intrusion detection systems

- a system that monitors network traffic for suspicious activity



IDS Types

- Network Intrusion Detection System (NIDS)
- Host Intrusion Detection System (HIDS)
- Protocol-based Intrusion Detection System (PIDS)
- Application Protocol-based Intrusion Detection System (APIDS)
- Hybrid Intrusion Detection System

Detection Methods

- Signature Based: detect the attacks whose pattern (signature) already exits

- Anomaly Based: detect the unknown malware attacks using machine leraning to create a trustful activity model

Evasions

- Fragmentation
- Avoiding defaults
- Coordinated, low-bandwidth attacks
- Address Spoofing/proxying
- Pattern change evasion

Challenges of IDS

- False Positives (FP)
  - Treat legitimate activity as malicious
- False Negatives (FN)
  - Missing a real risk
- Staffing