جامعة كارنيجي ميلون في قطر
Carnegie Mellon
QATAR CAMPUS

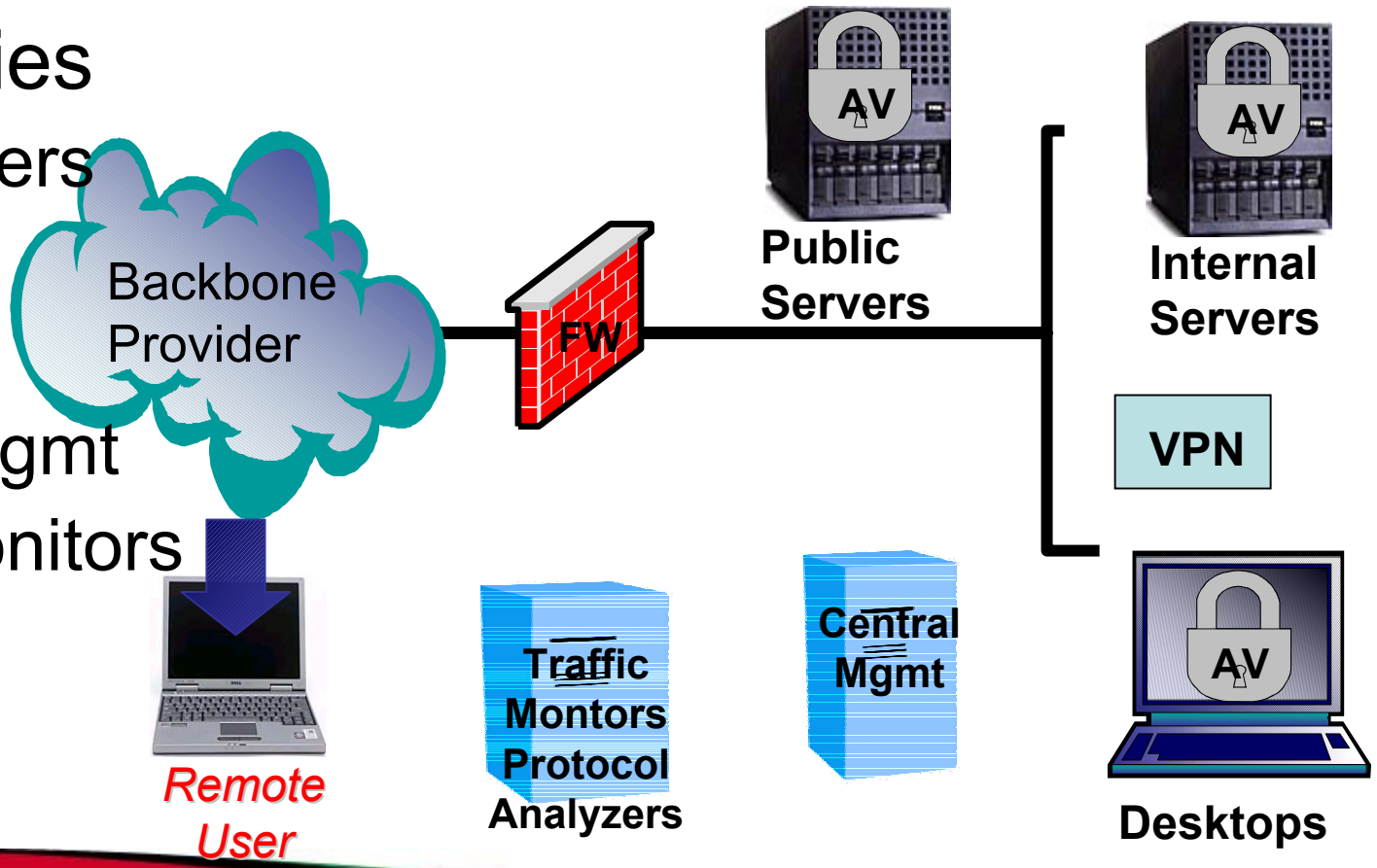
10YR ANNIVERSARY
مؤسسة قطر
Qatar Foundation

Intrusion Prevention

Overview
Cyndi Mills
CIO Carnegie Mellon in Qatar

Intrusion Prevention (history)

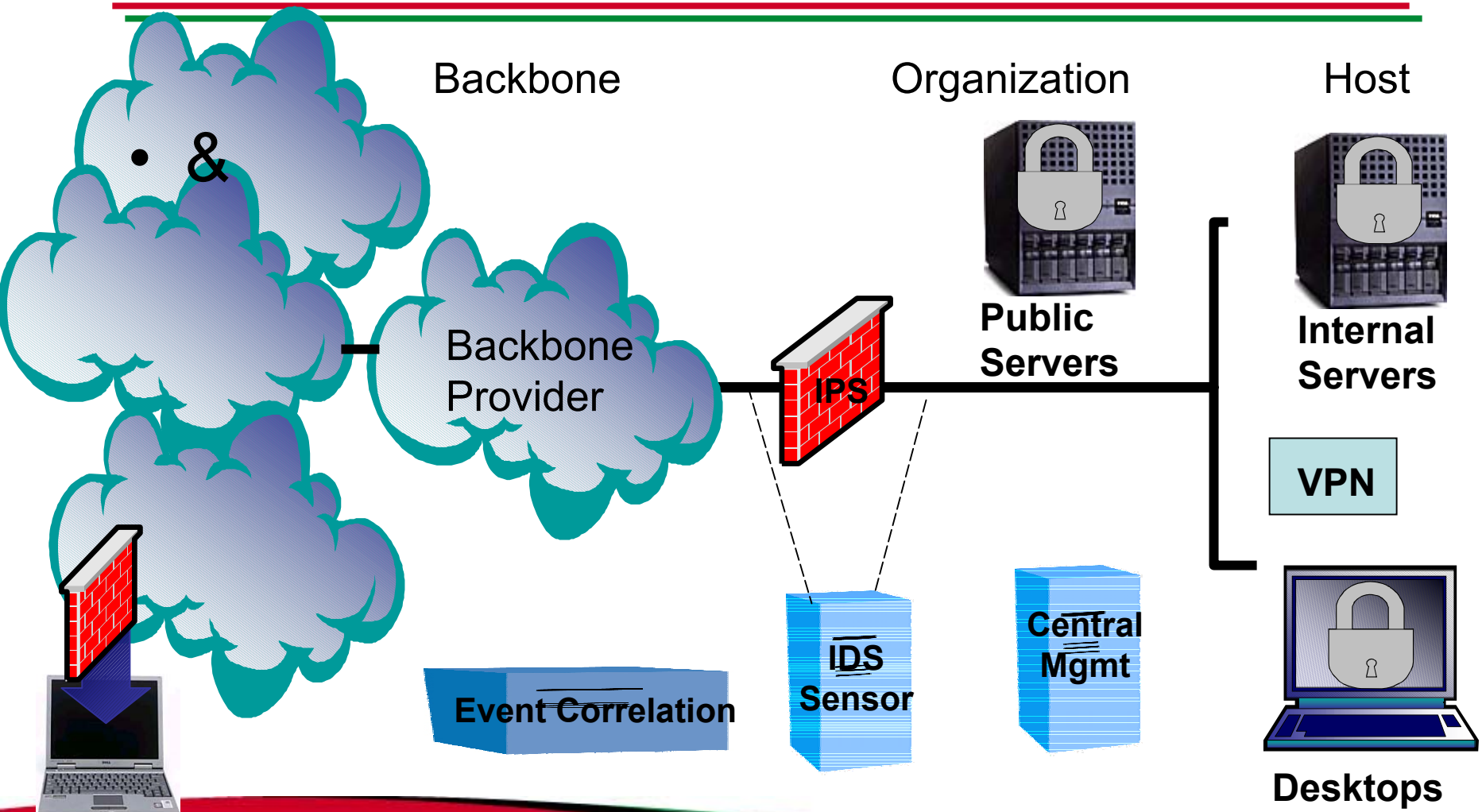
- Technologies
  - Router filters
  - Firewalls
  - Antivirus
  - Central Mgmt
  - Traffic Monitors
  - VPN/PKI



Defense-in-depth players

- Backbone (availability, optimization)
  - Expedite legitimate traffic (no false positives)
  - Remove bulk attacks (e.g. denial-of-service)
- Organization (content, liability)
  - Block attacks (inbound or outbound!)
  - Filter content based on organizational mission
    - (what is “spam” to one is “news” to another)
- Desktop (safe and reliable computing)
  - Protect with antivirus and desktop firewalls / IPS
  - Learn security awareness and best practices

Intrusion Prevention Overview (now)

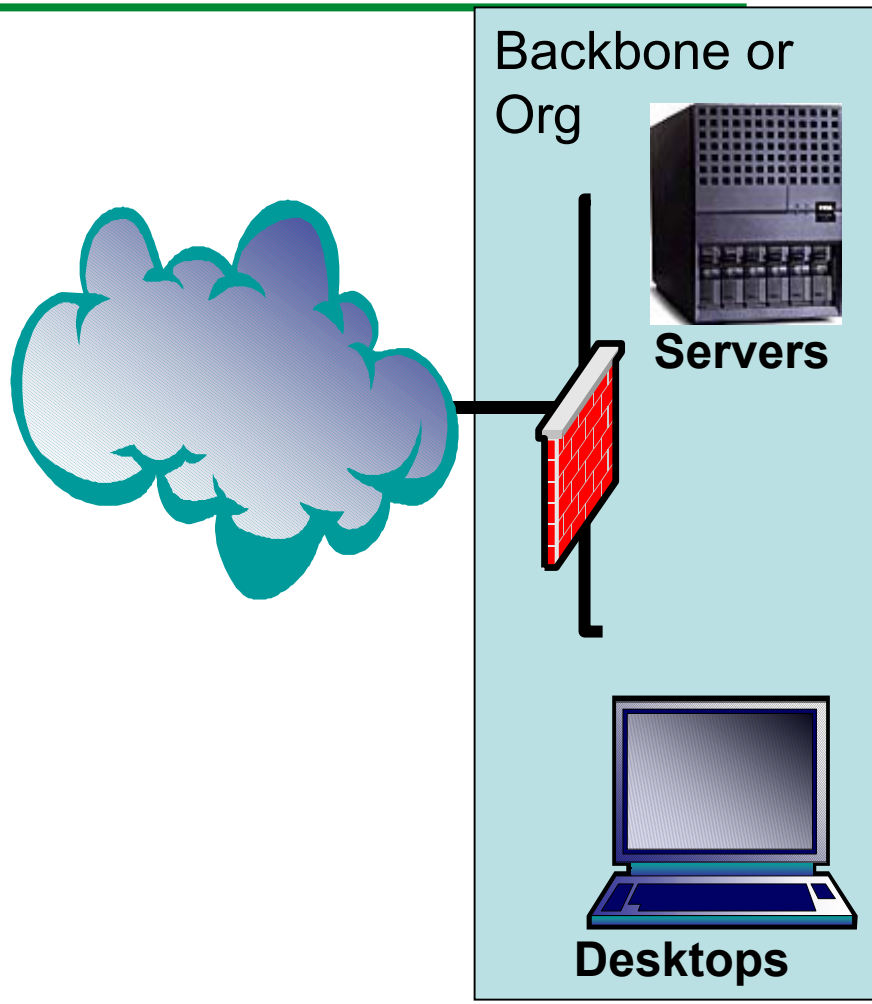


Network Intrusion Prevention adds:

- More Stateful Analysis
  - Protocol Decode with Pattern Matching
    - blocks buffer overflows, protocol defects, program invocations, single packet attacks
  - Traffic/signature normalization
    - block evasions
  - Anomaly Detection
- Heuristic Analysis
  - Port Sweep, Synflood

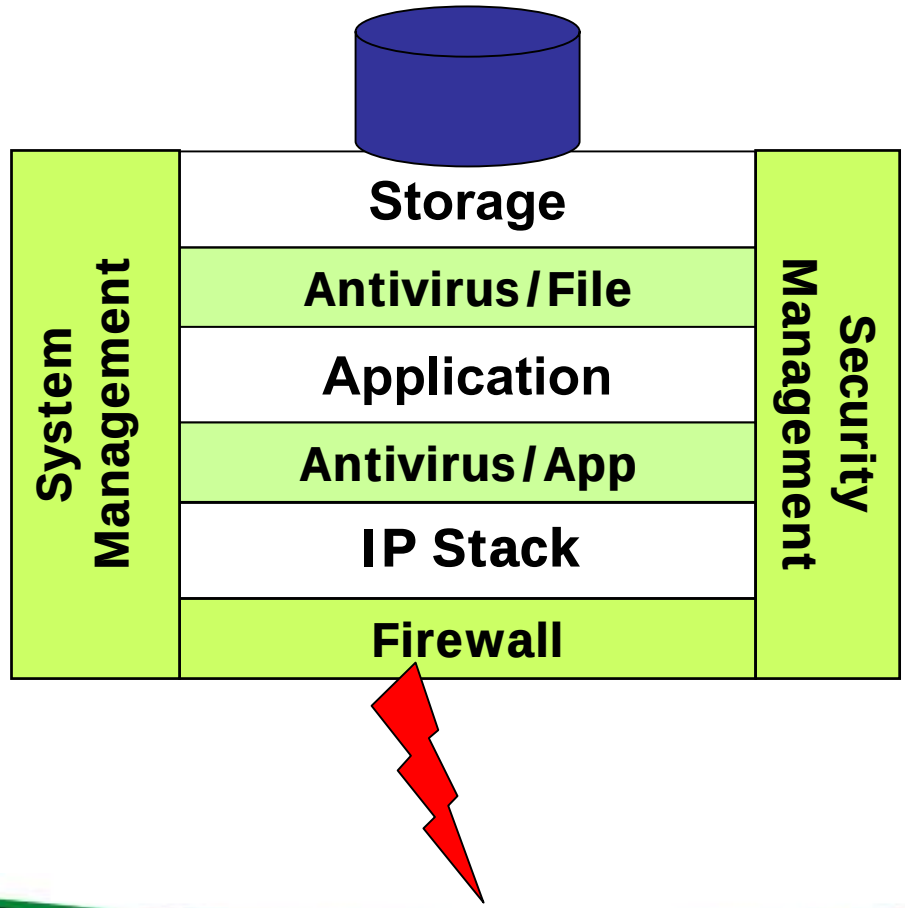
Attack Mitigation (anti-DOS)

- Dividing traffic into “known good”, “known bad”, and “suspicious”
- Resource limiting with thresholds
  - Flood detection
  - Connection limiting
  - Rate limiting

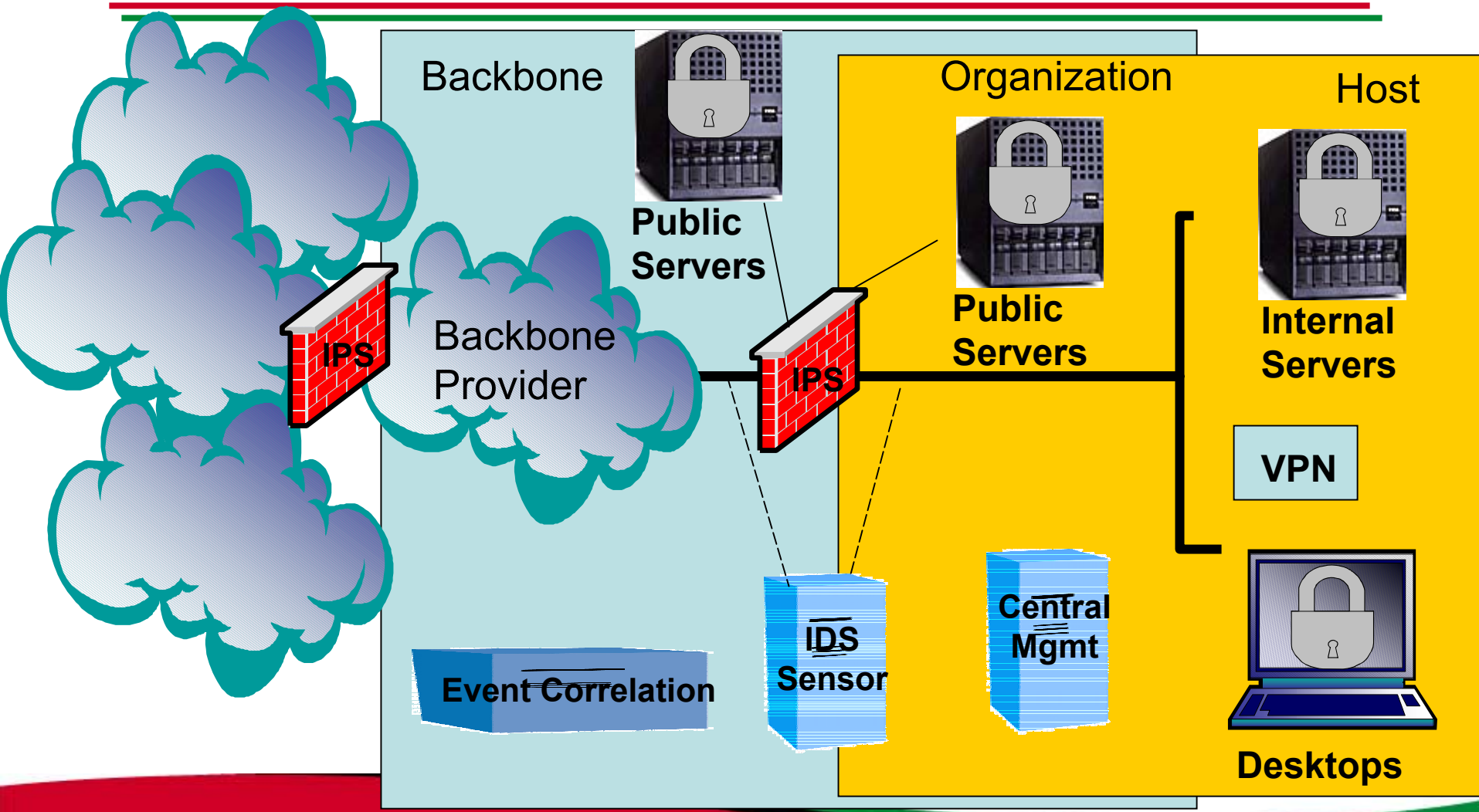


Host Intrusion Prevention

- Antivirus / Spam & Spyware
  - File integrity checking
  - E-mail/download quarantine
  - Application blocking
  - Content filtering
- Host IDS/IPS (System)
  - Logs and audit trails
  - Authentication
  - OS-Intercepts
- Desktop Firewall
  - Stateful Access Control
  - Intrusion Prevention Filters
- Central Management
  - Administration, Configuration, Monitoring



Intrusion Prevention Summary



Further Reading

- NSS
  - http://www.nss.co.uk/
- InfoSecurity Nov 2005 “On the Line” (Gigabit IPS devices)
  - http://informationsecurity.techtarget.com/magPrintFriendly/0,293813,sid42_gci1137925,00.html
- Network World 20 Questions to ask your IPS vendor
  - http://www.networkworld.com/reviews/2004/0216ips20qs.html

Some Evaluation Criteria for IPS

- Where is this product designed to sit on the network?
  - Peformance (latency, throughput, and jitter)?
- Attack-blocking mechanisms
  - rate-based and content/anomaly-based mechanisms?
  - how does this product block (DoS, UDP attacks, buffer overflow attacks, fragmentation attacks, spoofing attacks , application-layer attacks, etc.)?
  - How does this product protect again false positives?
- Reporting and management capabilities?
  - Alerts, logging, interoperability