Internet Dial Tones & Firewalls: One Policy Does Not Fit All

IEEE Coastal South Carolina Section
Computer & Communications Chapter
Tuesday, June 10, 2003

Robert Gezelter Software Consultant
35 – 20 167th Street, Suite 215
Flushing, New York 11358 – 1731
United States of America

+1 (718) 463 1079
gezelter@rlgsc.com
http://www.rlgsc.com

Information Access Trend

- Online data is more accurate
- Stored/Staged data is obsolete
- Types of data
  - package tracking
  - technical data (private and public)
  - news and financial data
  - government filings
 - interwoven applications using XML

Internet Access has become expected (cont'd)

- WiFi (wireless)
  - coffee shops (Starbucks)
  - bookstores (Borders)
  - airports
  - public spaces (NYC's Bryant Park)
  - conferences
 - 24x7x365 acccess, at will, wherever one is

However, inside enterprises –

- Outside, access is (or is becomming) ubiquitious
- Inside, access is increasing in complexity
- Past model was "gatehouse", hard outside inside was/is fairly soft
- One size fits all, no texture or subtlety

Traditional Simplistic Firewall Architecture

Internal Network
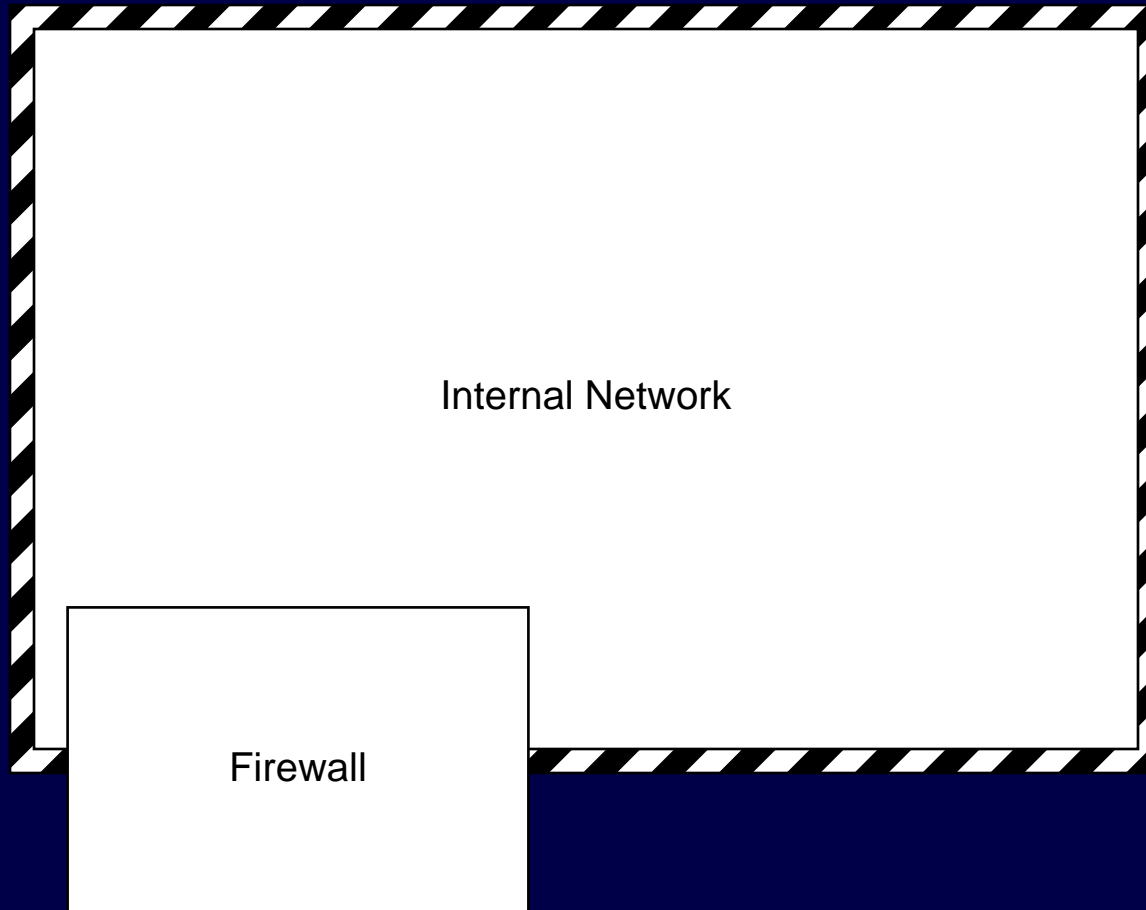
Firewall

Traditional Simplistic Firewall Architecture with DMZ
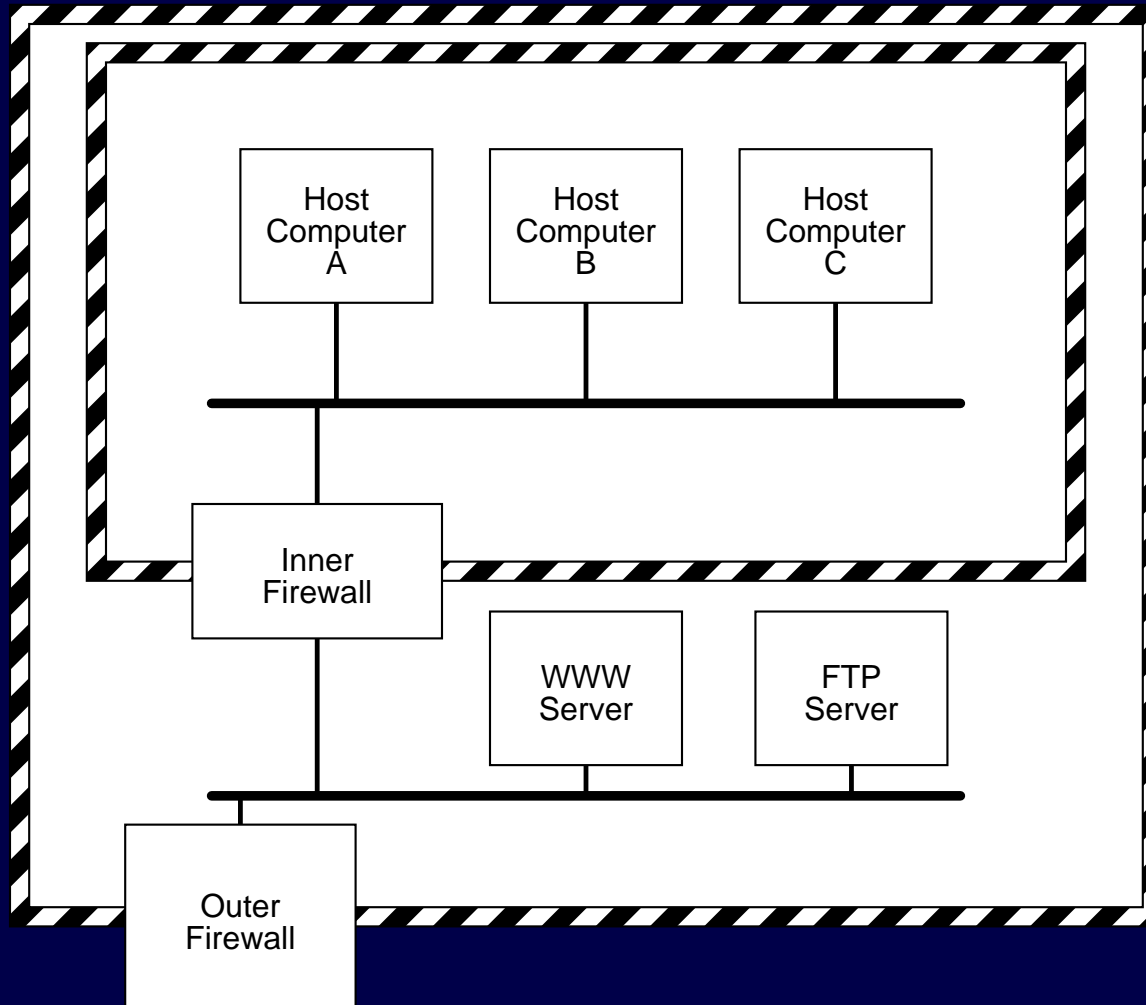
Internal Access Obligations/Restraints

- Internal Security – Pricing, Internal data
- National/Homeland Security
- Regulatory – SEC, FDIC, FRB
- Legal – HIPAA, other protected
- Less monolithic teams

"Inside" Community is more Diverse

- Employees
- Contractors
- Vendors
- Salesman
- Customers
- Colleagues

Technology Concerns

- both wired and WiFi have security concerns

- but, in a sense, the concerns/issues are the same

Security/Access Concerns

- authentication
- privacy/anti-eavesdropping
- bandwidth allocation
- springboard elimination

Security Domains

- Monolithic Domains cannot factor the problem space
- Sibling and Child Security Domains
- DMZs
- Cul-de-sacs
- pseudo-Public access to dial-tone
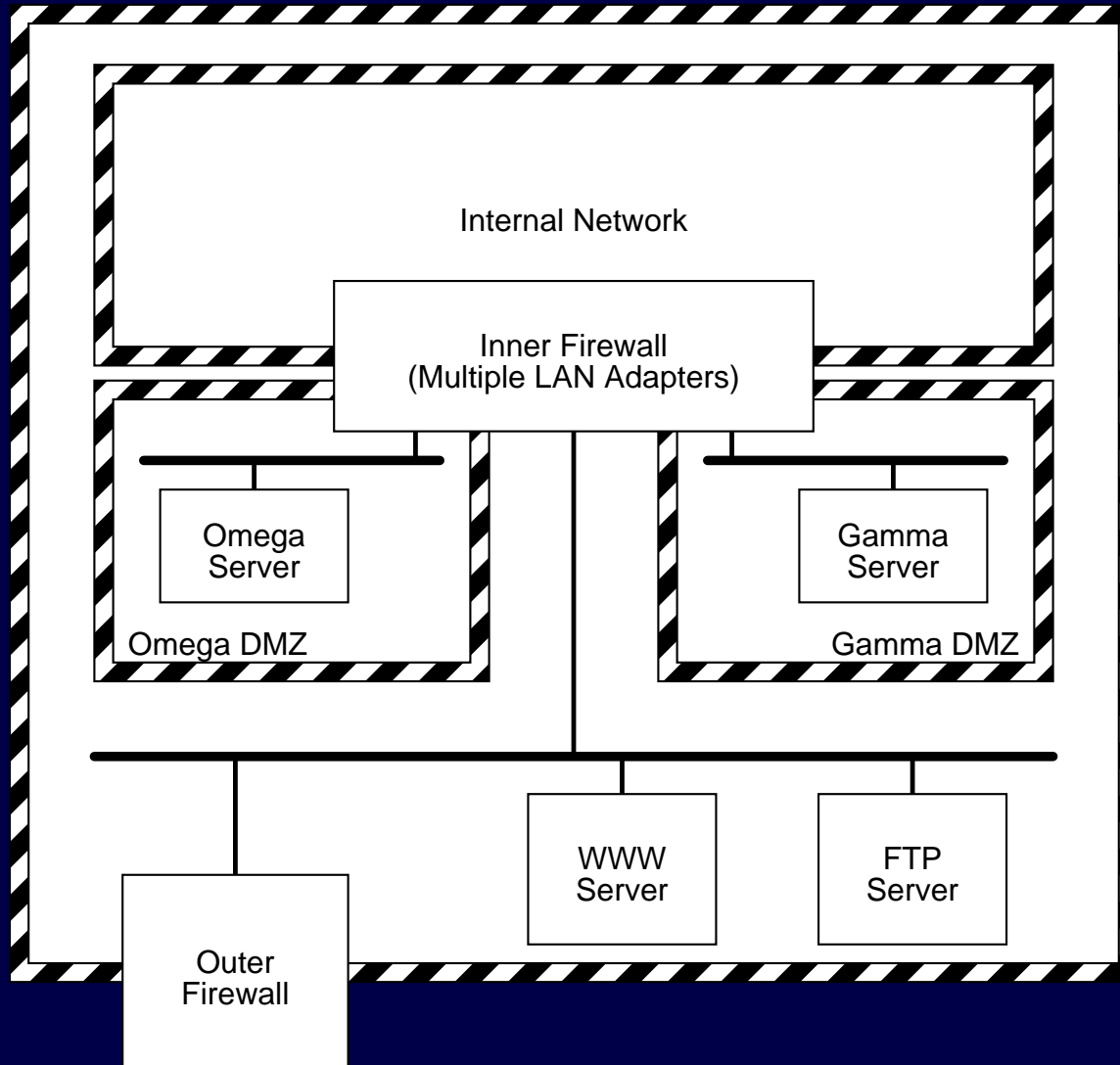- HTTPS/X.509 Certificates within organization
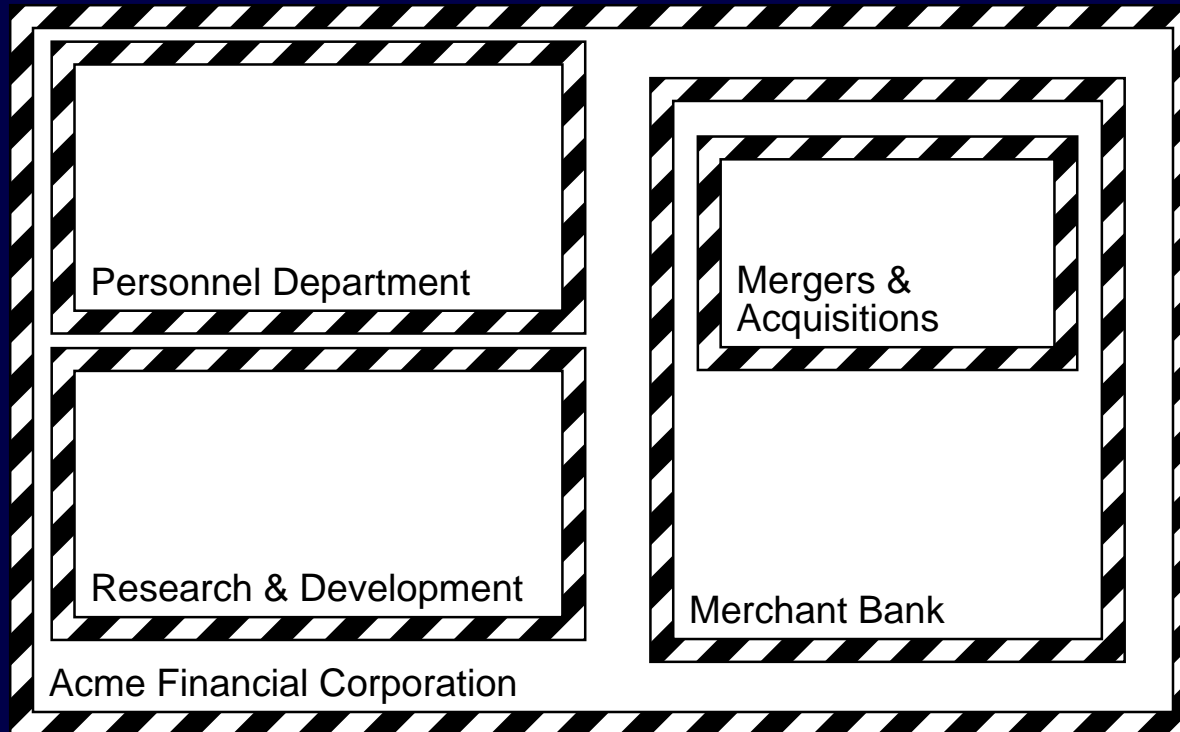
DMZs

- not just between Internet and intranet
- each organization contains many outsiders
- firewalls are internal security partitions

Nested and Sibling Security Domains

Cul-de-sacs

- WAPs are only digital dial-tone
- getting out of a cul-de-sac requires VPN
- extensive use of proxy servers
- assumption of compromised network media

Questions?

Robert Gezelter Software Consultant
35 – 20 167th Street, Suite 215   +1 (718) 463 1079
Flushing, New York 11358 – 1731   gezelter@rlgsc.com
United States of America   http://www.rlgsc.com

Session Notes & Materials:
    http://www.rlgsc.com/ieee/charleston/2003-6/index.html