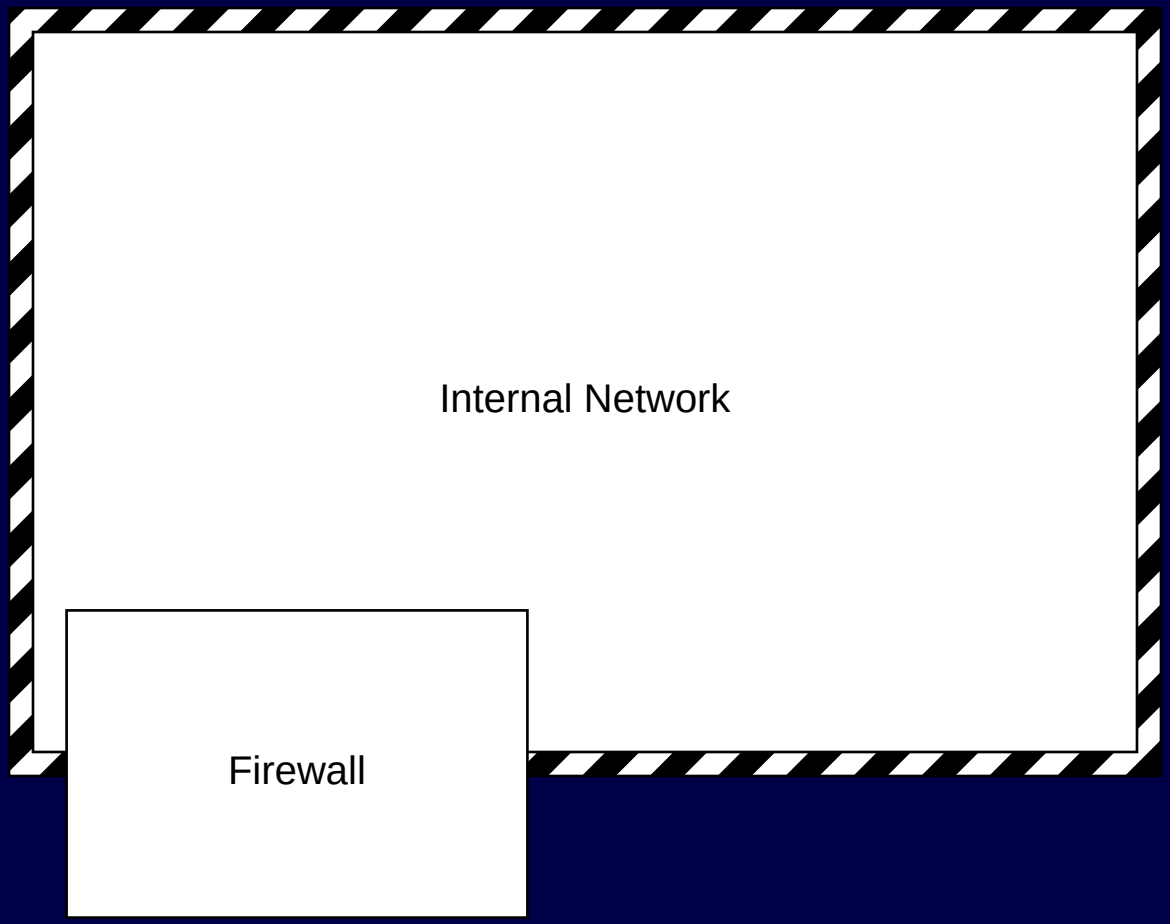
Safe Computing in the Age of Ubiquitous Connectivity

IEEE Computer Society
Los Alamos and Northern New Mexico Chapter
Wednesday, February 22, 2006

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

Canonical Firewall Architecture



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- Stored/Staged data is obsolete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

- Wired Broadband
- Wi-Fi
- Cellular

Internet Access has become expected (cont'd)

- Wi-Fi (wireless)
  - coffee shops (Starbucks/T-Mobile, …)
  - bookstores (Borders/T-Mobile, …)
  - copycenters (Kinko's/T-Mobile, …)
  - airports
  - public spaces (NYC's Bryant Park, …)
  - phone booths (Verizon)
  - conferences
  - 24x7x365 access, at will, wherever one is

Internet Access has become expected (cont'd)

- Cellular Data
  - announced in USA Today, 25 March 2004, page 3B
  - Broadband-class performance
  - Verizon (deploying EV-DO)
  - Sprint (1xEV-DV) +1–2 years
  - Now deployed and useable in many areas

However, inside enterprises –

- Outside, access is (or is becoming) 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
- Levels of Trust (payroll, health, proprietary)
- Ease of breach/theft (e.g., script kiddies)
- Rogue Access Point deployments

The Real Issue – TRUST

- the word TRUST means different things in different contexts
- the word TRUST means different things to different communities
- In human relationships, TRUST is often used in an absolute sense
- In legal contexts, TRUST is a far different concept
- Unsurprisingly, people can often agree on wording easier than the concept

All of engineering & structural design is about safety factors.

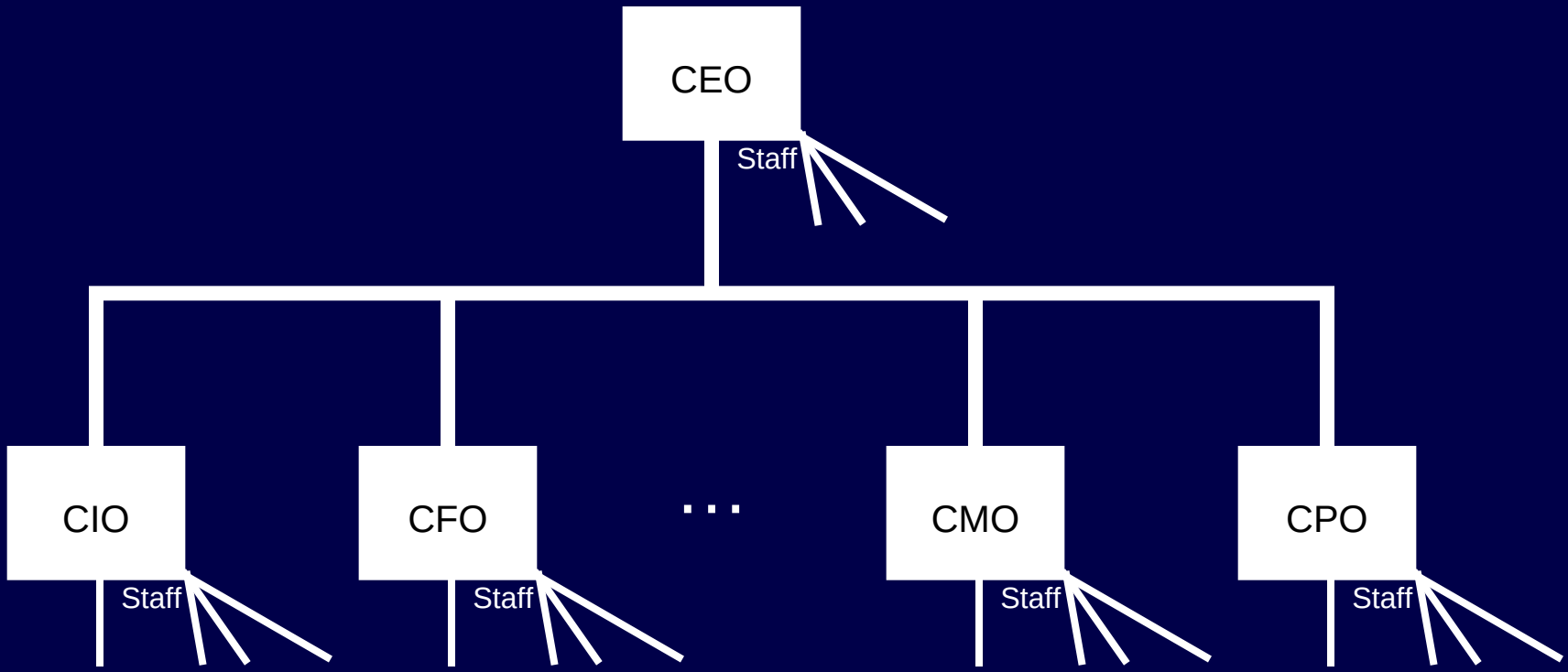
The art of ensuring safety in the face of error, uncertainty, and imperfection.

In God we trust –
All others we polygraph.
– Tom Clancy

Technical TRUST – What does it mean?

- Liability exposure
- Need to know
- Things may not work as planned
- When building houses, carpenters:
  - toe-nail
  - cross-brace
  - hurricane straps

The Modern Corporation



- Access is NOT related to rank
- Access is related to clade, project

Data and Liability –

- R & D
- Deal making
- Client confidentiality/privacy
- For employee's own protection

Goal – Seamless Technical TRUST –

- If you don't breach the barrier, it isn't really there. Is it?
- Insufficent walls create catastrophic failures – the "Titanic/Comet Syndrome"

The Age of Innocence

- Machines were rare
- Inherently restricted access
- Few players, all known to each other

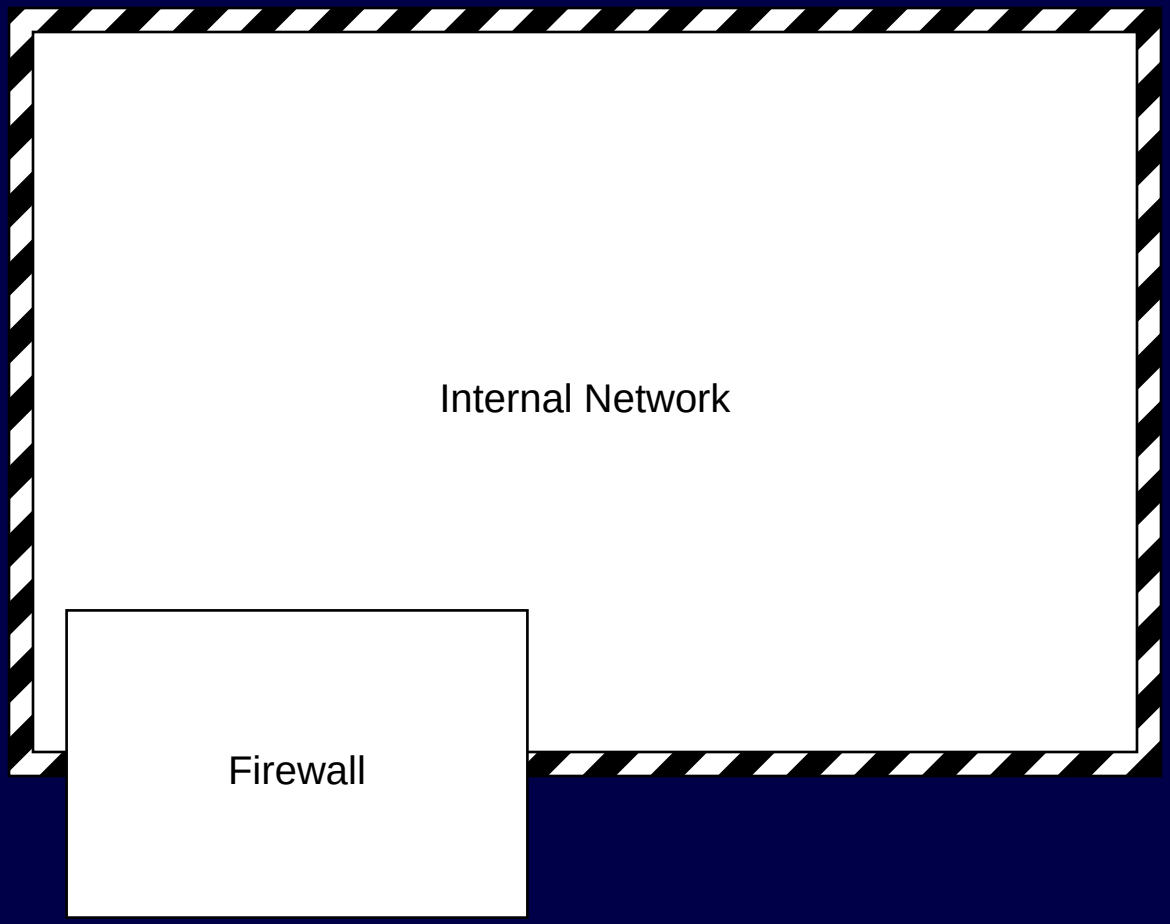
Original Internet – Total TRUST

- No safeguards
- No integrity checks
- No compartmentalization
- Total Net Crash – IMP caused (SEN, 1/1981)
- Trusting server processes (e.g., sendmail)

The Age of Ubiquitous Computing/Connectivity

- Huge number of machines
- Easy access to essentially unrestricted bandwith/connectivity
- Worldwide connectivity – essentially anonymous
- “On the Internet, nobody knows that you are a ‘dog’”

Traditional Simplistic Firewall Architecture



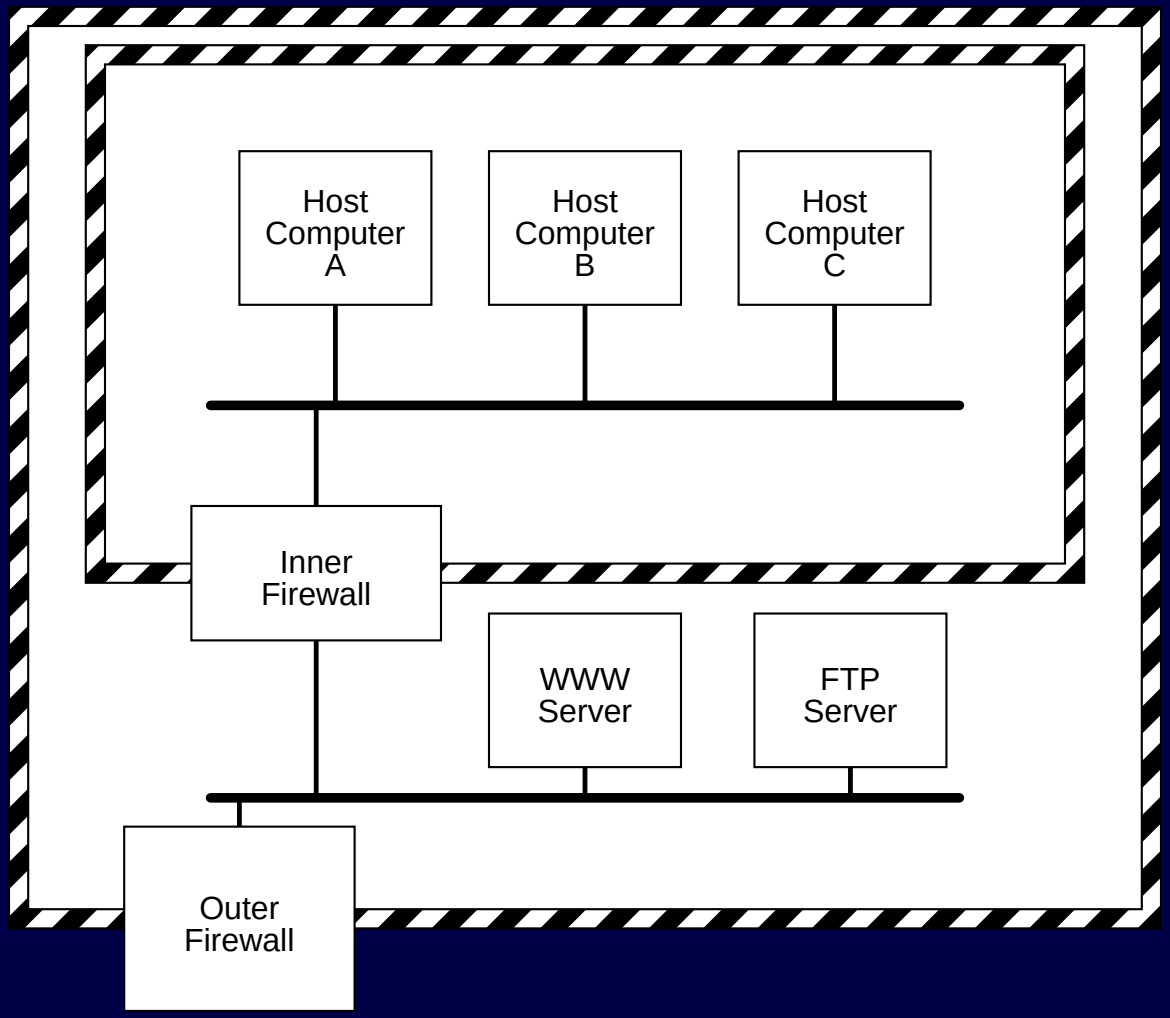
Analyze the Threats

- Internal information control (“Need to know”)
- Curiosity (e.g., celebrity tax returns)
- Insider fraud
- “Loose lips sink ships”
- Criminal
- Visitor-borne contagion

Internal Access Obligations/Restraints

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

Traditional Simplistic Firewall Architecture with DMZ



"Inside" Community is more Diverse

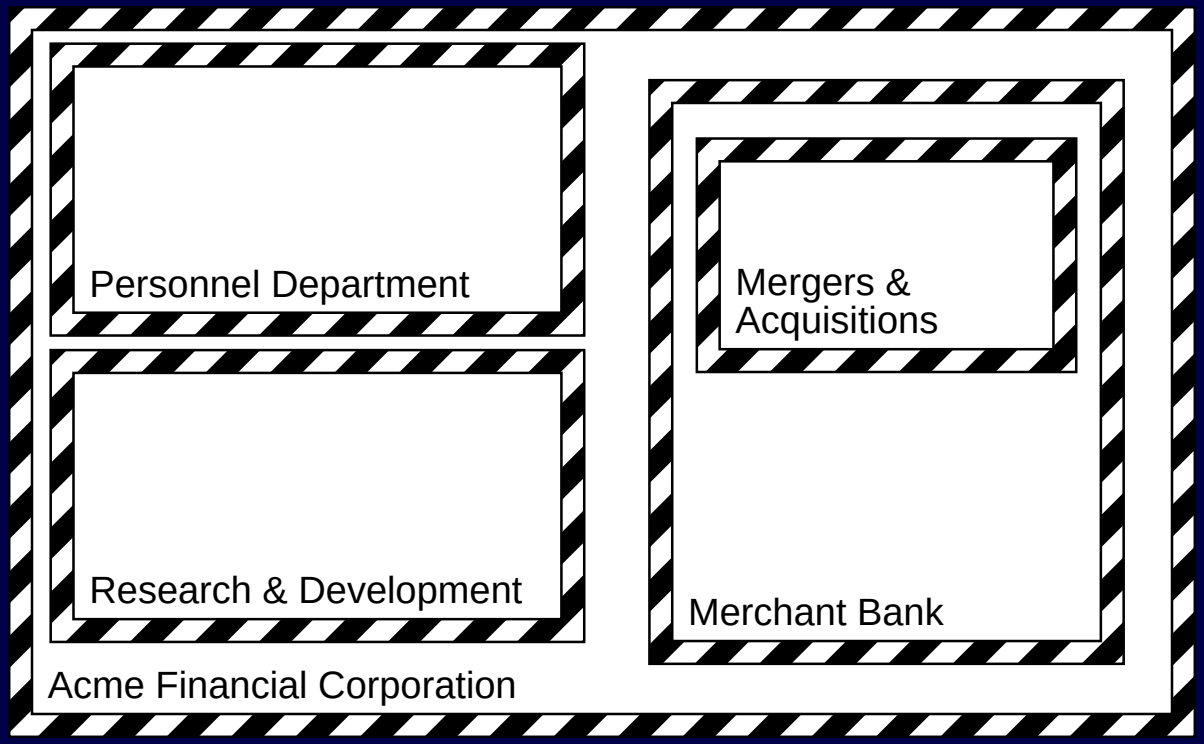
- Employees
- Contractors
- Vendors
- Salesmen
- Customers
- Colleagues
- Regulators
- Interviewees

Technology-based Security Concerns are similar for wired, Wi-Fi, and cellular

- Are wall sockets really secure?
- Passive attack – sniffing/eavesdropping
- Trojan Horse (software/hardware)
- The “Remote Control” syndrome

Security/Access Concerns

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



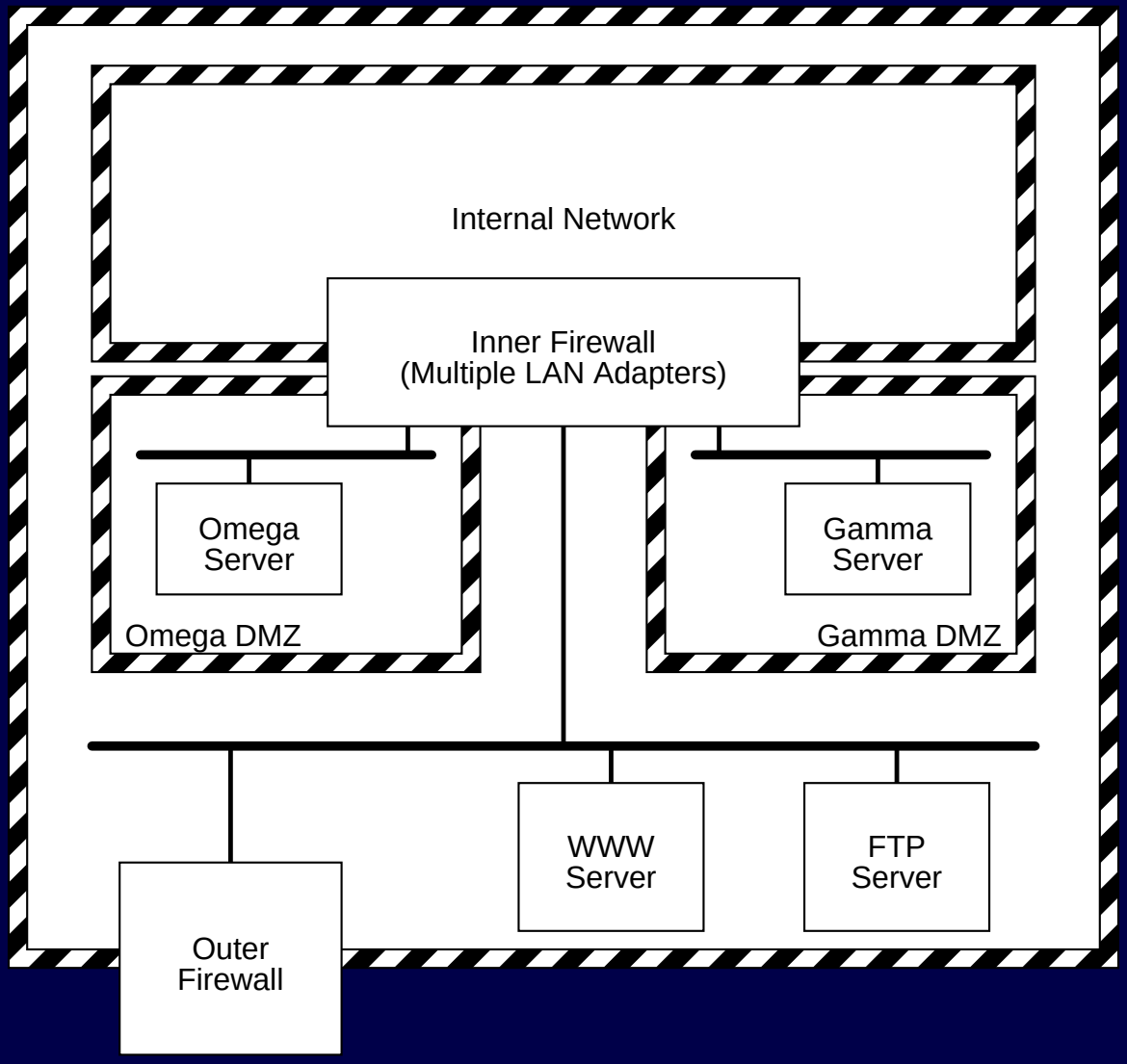
Security Domains

- Security by architecture/structure
- Limit and control trust and delegation
- Monolithic domains cannot factor the problem space
- Sibling and child security domains
- DMZs
- Cul-de-sacs
- pseudo-public access to dial-tone

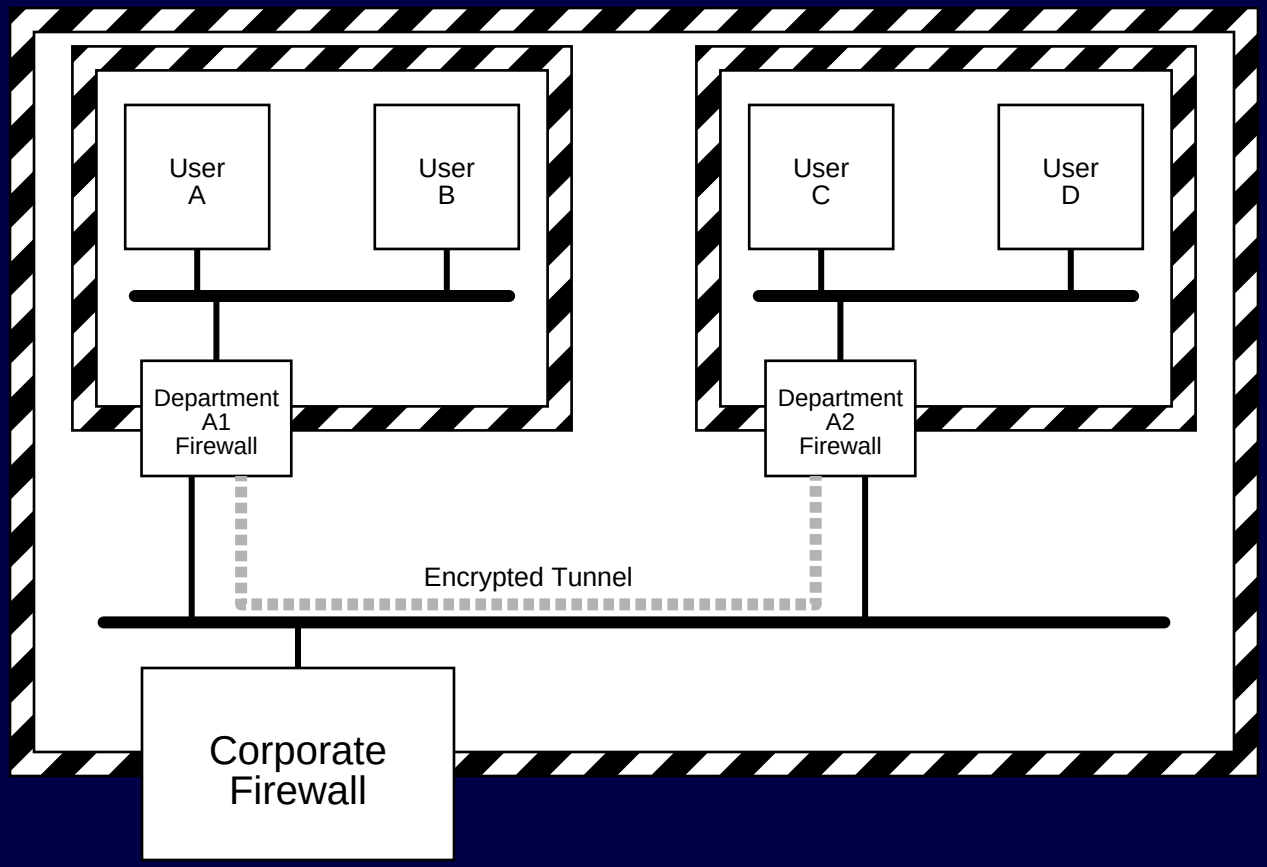
DMZs

- not just between Internet and intranet
- each organization contains many relative outsiders
- firewalls are internal security partitions
- VPNs even within the organization
- X.509 Certificates/HTTPS for intranets when sensitive business/personal information is present

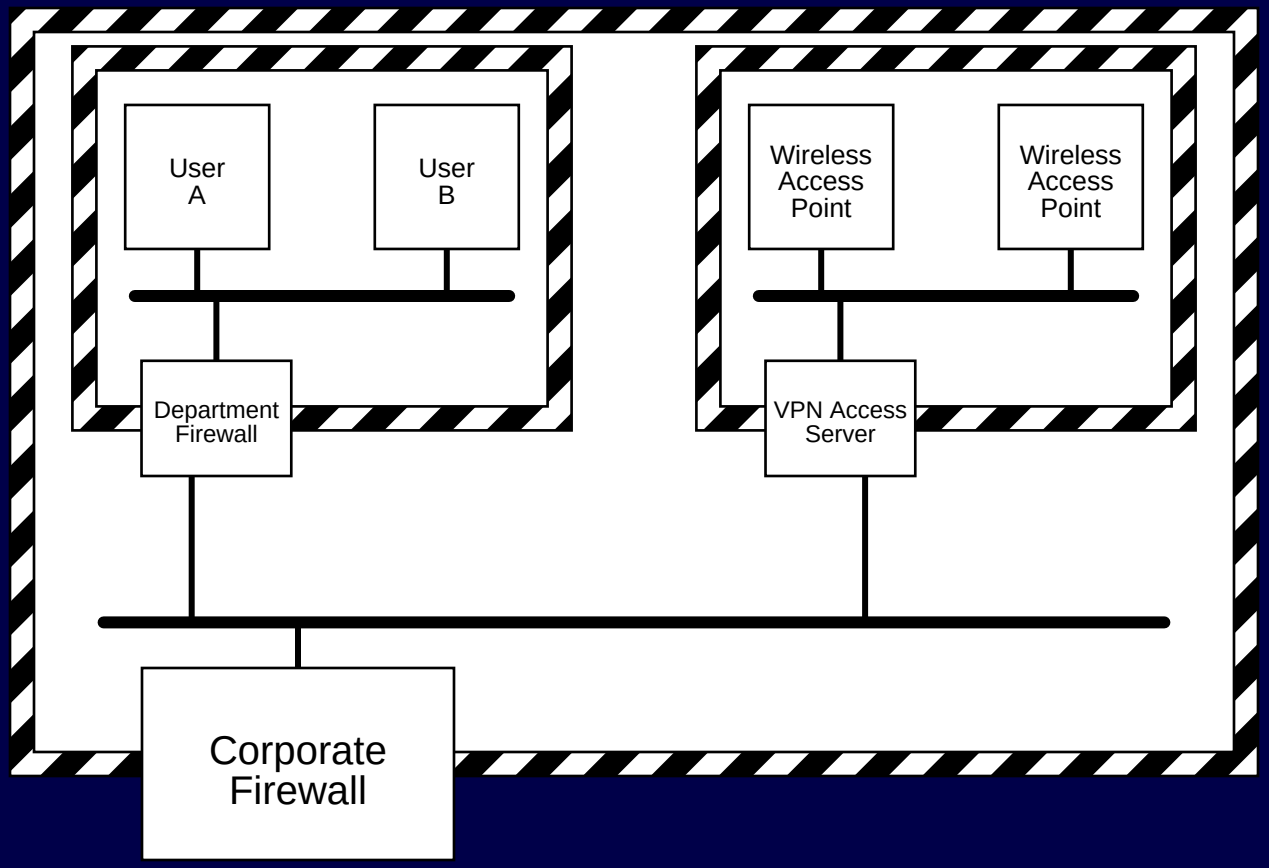
Nested and Sibling Security Domains



VPNs Within the Corporation



Cul-de-sacs provide Dial-Tone



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
- location of WAP relative to gateway
- WPA and WPA2 only address the “last meter” problem

Questions?

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

Session Notes & Materials:
http://www.rlgsc.com/ieee/LosAlamos/2006-02/index.html