Compartmented Networks: A Corporate Solution for Privacy, Integrity, and Security

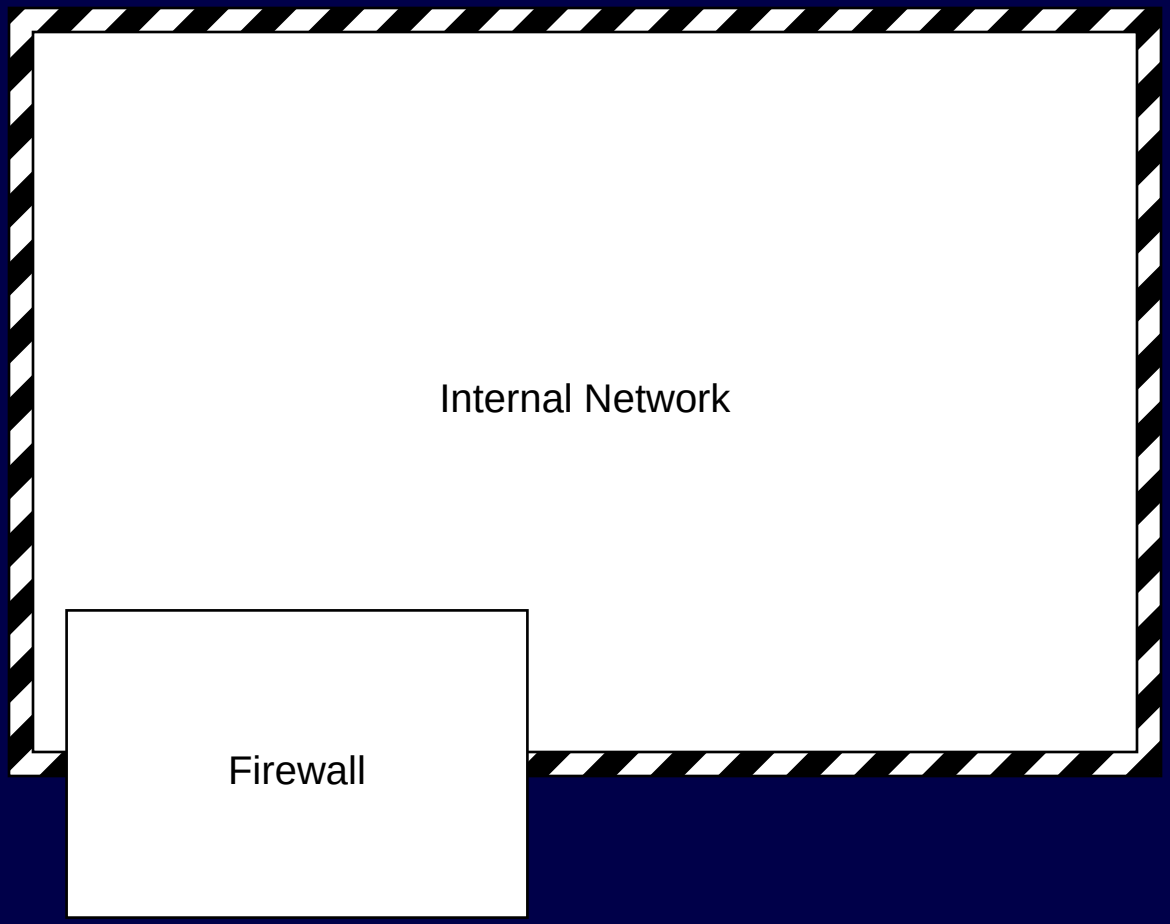
11th Annual NY State Cyber Security Conference

Thursday, June 5, 2008

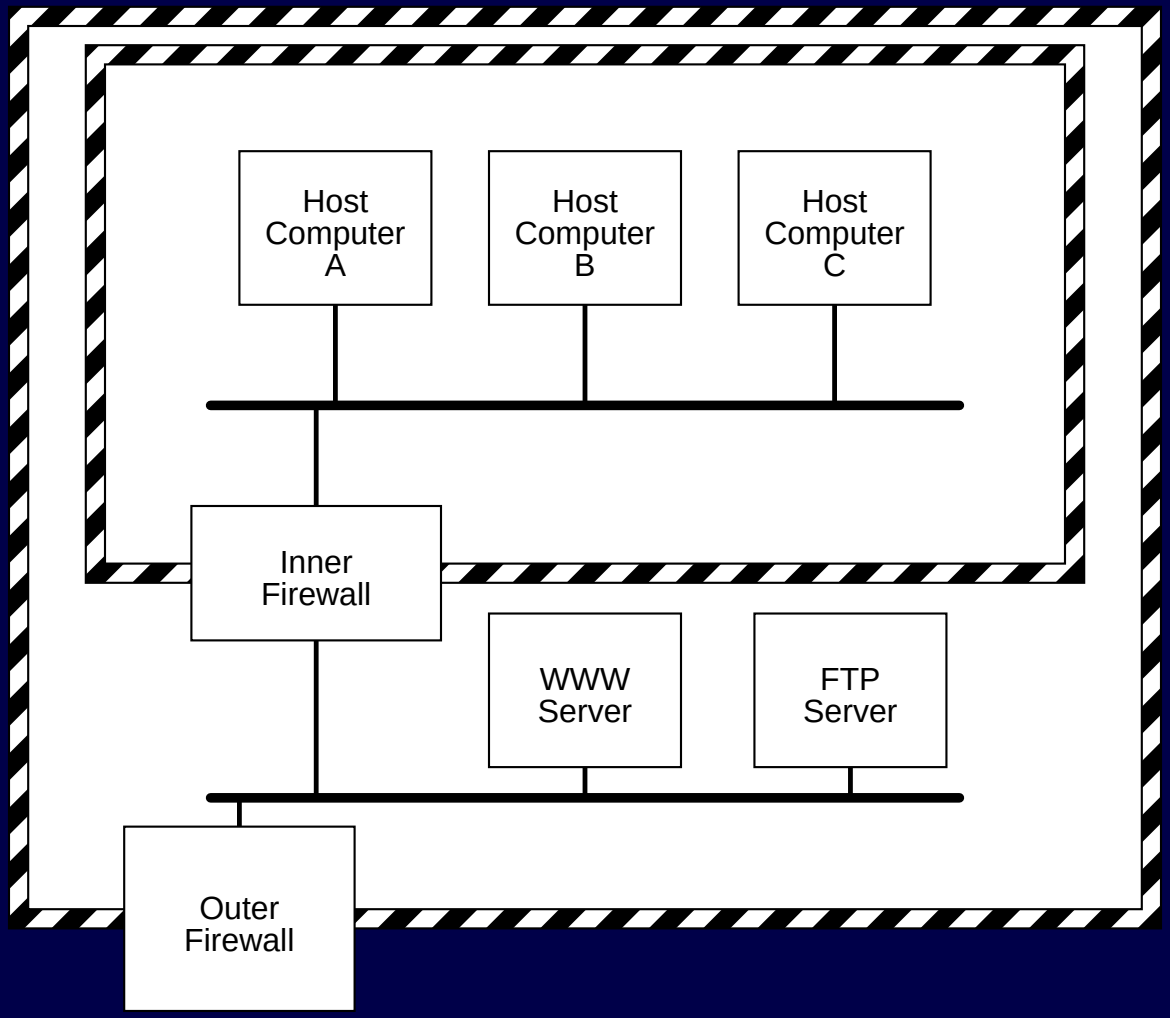
Robert Gezelter Software Consultant
35 – 20 167th Street, Suite 215
Flushing, New York 11358 – 1731
United States of America

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

Canonical Firewall Architecture



Traditional Firewall Architecture with DMZ



Threats:

- There are many players in the network world:
  - Friendlies
  - Bandits – Bad Actor
  - Bogies – ???

Attacks –

- potentially devastating
- not always attributable
- not always actionable

Response –

- may be infeasible
- retaliation (e.g., counter-battery) is illegal
- Defensive Action only

Who is the opposition?

- amateurs
- professionals
- criminals
- rogues
- nation states
  - military forces
  - sponsored

Today's challenges –

- hacking
- ID theft
- information theft
- accountable access

"The world is flat" – Friedman

- this is essentially true
- also means – "The barbarians ARE at the gate"
- you can be attacked from anywhere, at anytime
- flat networks as monolithic security domains are vulnerable
- the original Internet is a prime example

Internet technologies –

- were designed to enable access
- secure, accountable access was NOT part of the context

Electronic intelligence has gone retail

- formerly expensive, capital intensive
- was the provence of nation states
- now easy to do; available to teenagers

Threat detectors detect ALREADY accomplished threats

- IDS, Port scanning identify existing problems
- previously known threats
- previously identified vulnerabilities
- far too late!

Network monitoring –

- compromised media
- rogue switch ports
- information gathering platforms
- ringers

Are these threats credible?

- TJ Maxx – 11/30/2007 (94 million #s)
- Dave and Buster's – 8/2007 (5,000 #s)
- Hannaford/Sweetbay Supermarkets – 3/10/2008 (4.2 million #s)

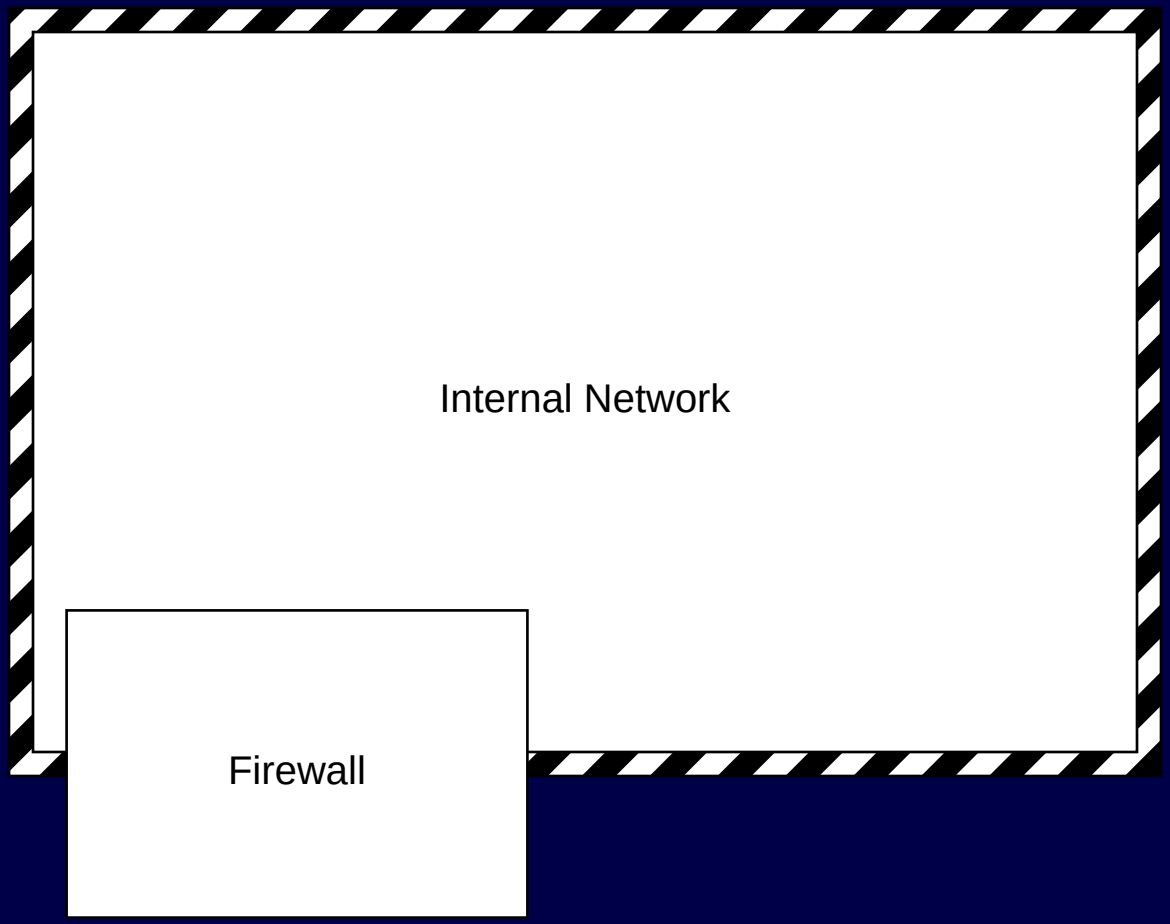
Systematic Breach is the enemy –

- ongoing compromise
- compromised infrastructure
  - networks
  - servers
  - workstations
  - networked devices

Costs –

- TJ Maxx – US$ 10.00/card
  - could easily exceed revenue
  - How many firms can pay US$ 49M+?
  - board-level expense

Canonical Firewall Architecture



Reverse the philosophy –

- the threat is not ennumerable
- there are things that are unknowable

Reactive measures raise alarms AFTER compromise

- intrusion detection
- network monitoring
- virus detection

Trust is Corrosive

- Weakest link
- Once compromised, difficult to recover

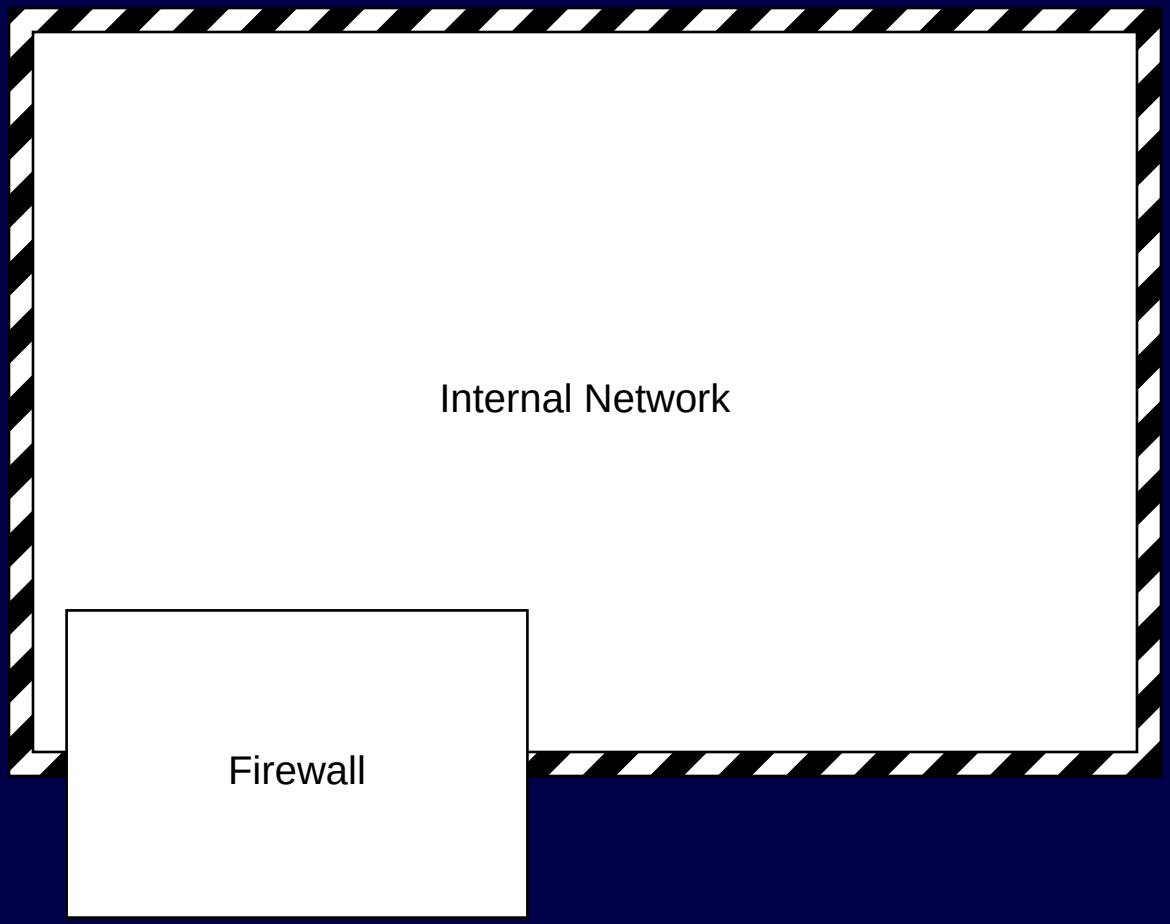
Ubiquitous Connectivity –

- no texture
- different needs for outside access
- have different risks
- What about access within the organization?
  - Production
  - Development
  - Research
  - Confidentiality requirements

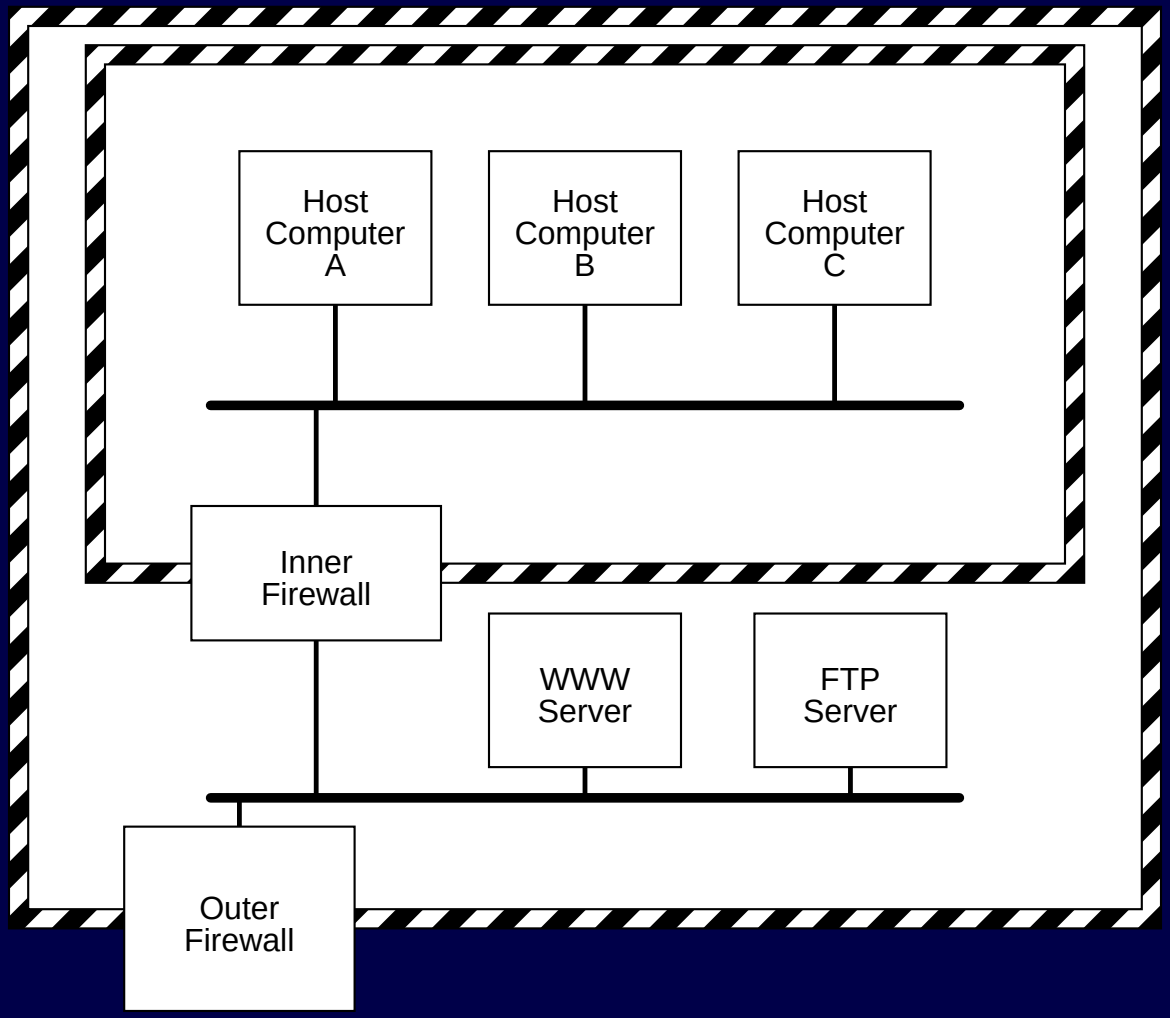
Security Domains

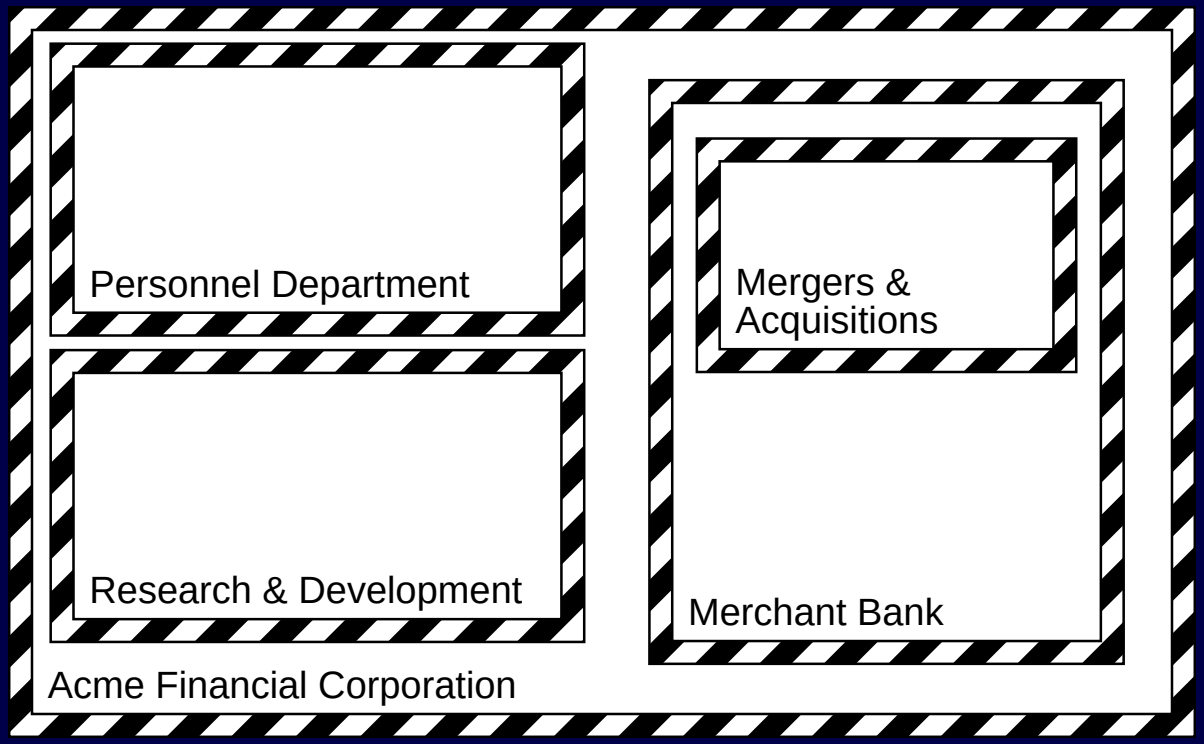
- Security by architecture/structure
- Limit and control trust and delegation
- Monolithic domains cannot factor the problem space
- Sibling and child security domains
- DMZs
- Cul-de-sacs
- pseudo-public access to dial-tone

Canonical Firewall Architecture



Traditional Firewall Architecture with DMZ

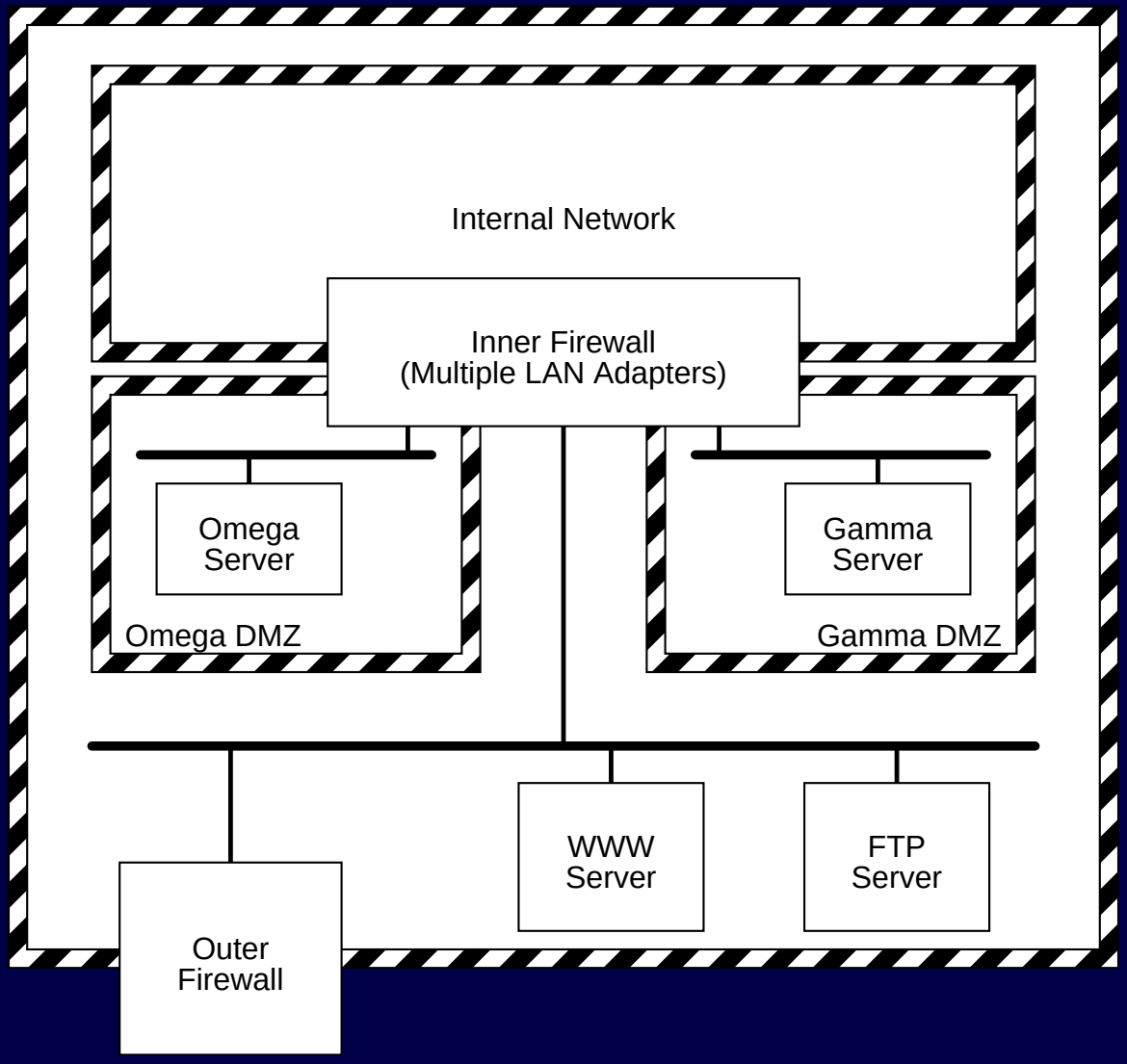




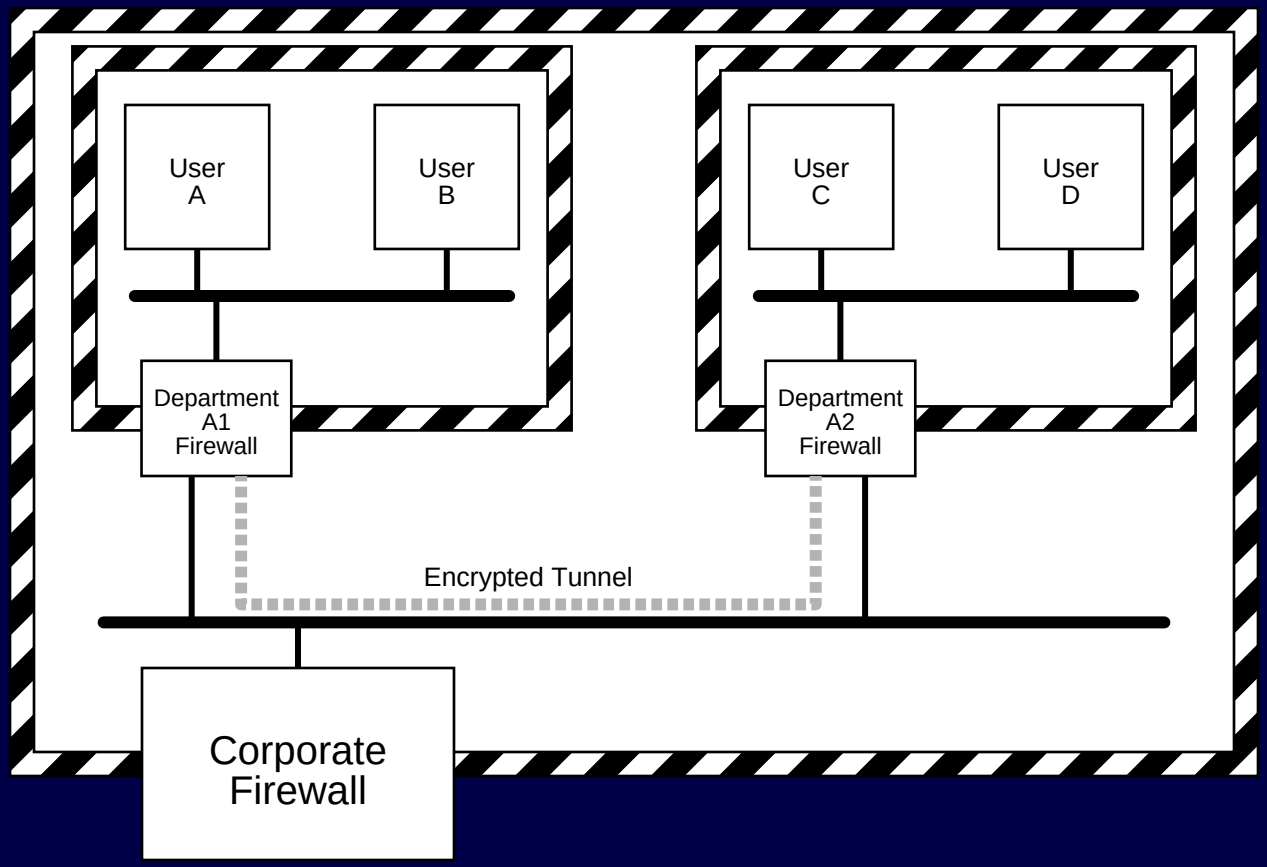
DMZs

- 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



Alternative –

- ubiquitous secure access – presume compromised infrastructure
- outside -> inside – only as needed
- inside -> outside – based on need
- inside is not uniform
  - differential access
  - within (Intranet) and without (Internet)
  - degrees of control and auditing
  - ubiquitous VPN and SSL

Ongoing issues –

- https-based rogue VPN's
- ports do not guarantee traffic

All of engineering & structural design is about safety factors.

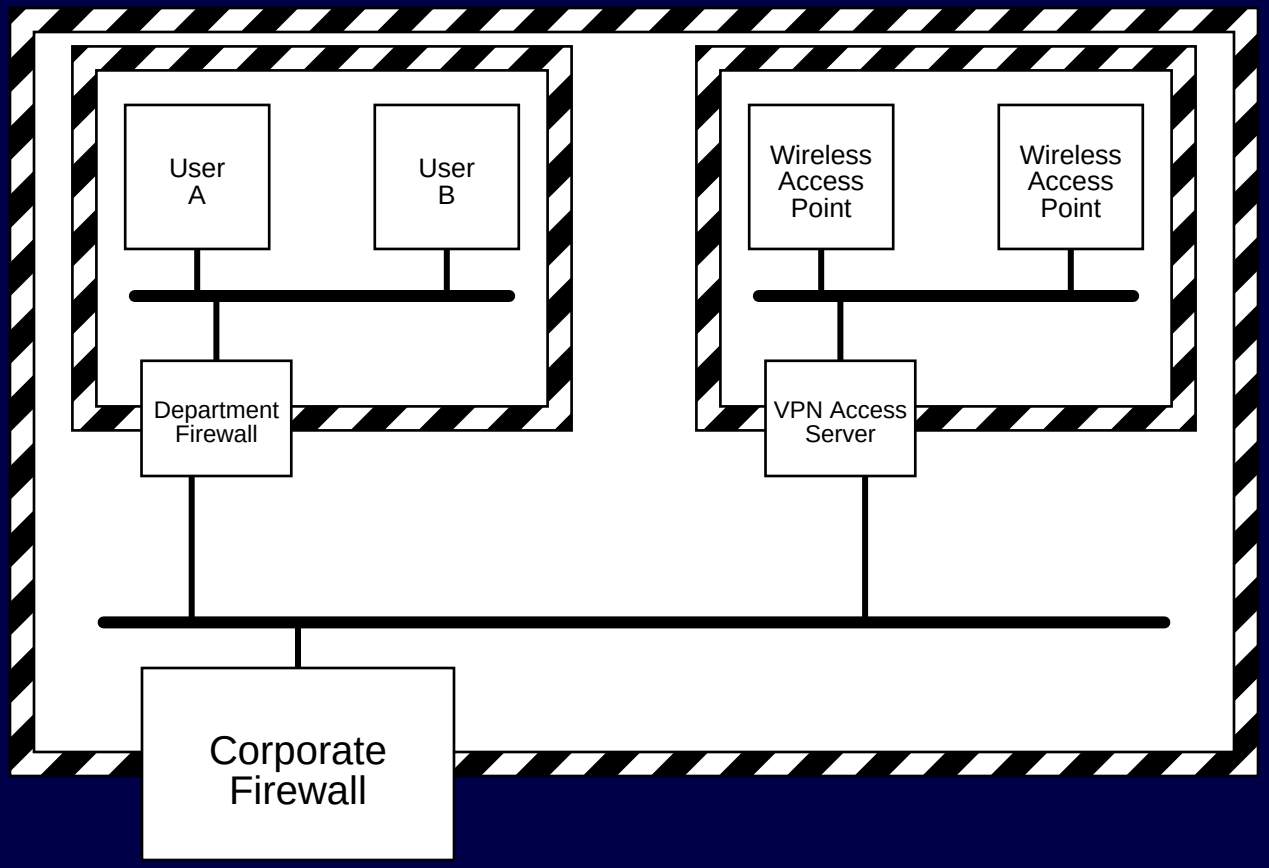
The art of ensuring safety in the face of error, uncertainty, and imperfection.

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

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

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

Summary –

It is sound policy to break a monolithic company network into a collection of nested and sibling networks to enforce proper and safe usage.

This decomposition allows the network topology to accurately reflect policy and provides the needed choke points to enforce policy and control.

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/nyscybersecurity/2008/compartmented.html