“Holistic” Security: Circles, Pies, or Crystals?

Jim Litchko, IMSI

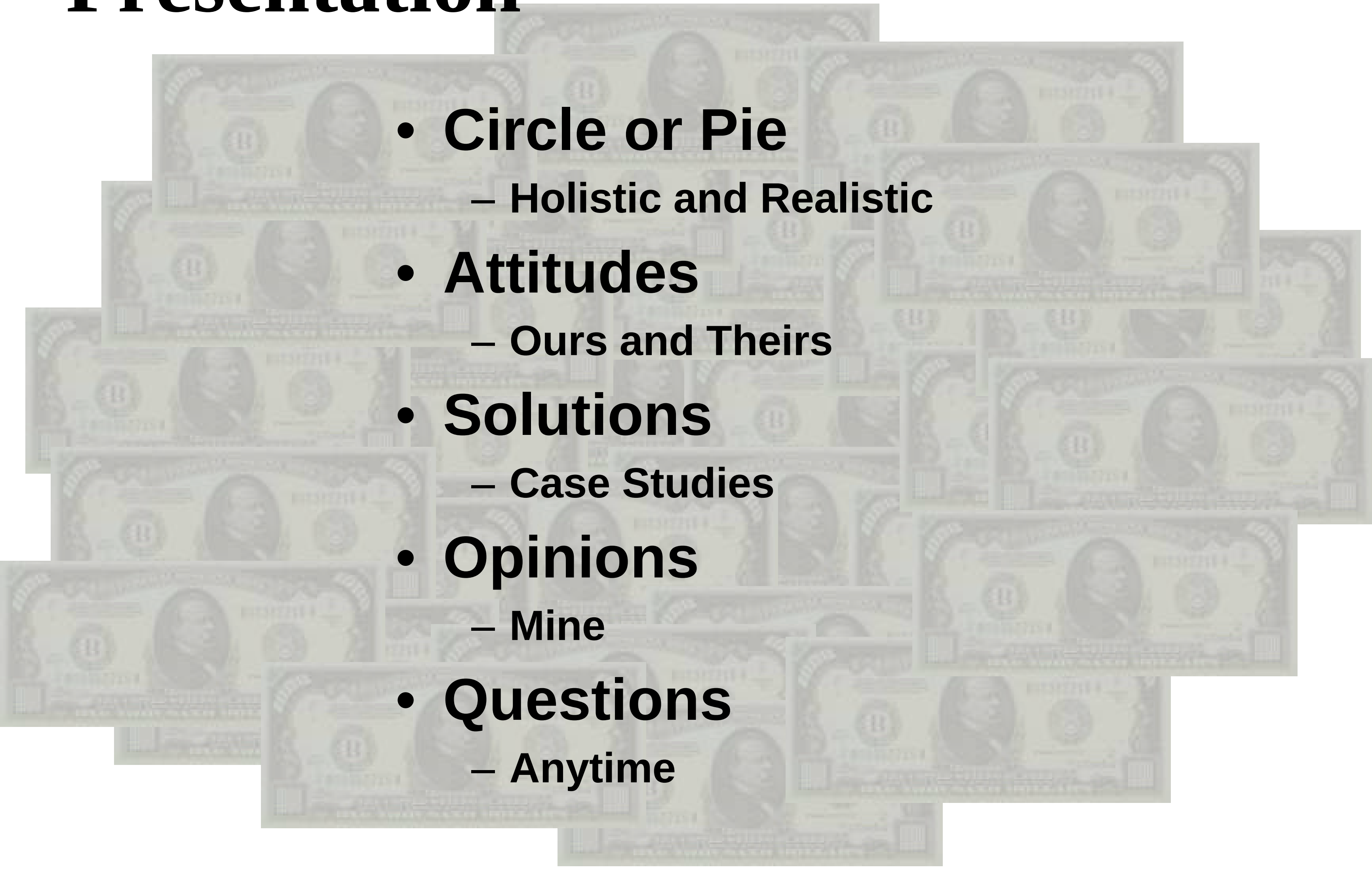
Securing a system is not like plugging a hole in a dam. Throwing a firewall and/or cryptography at the problem is not enough. Using his over twenty years of experience conducting system security reviews, he will identify the most common security misperceptions that he has seen, i.e., “Black Box Solutions”, “MS Evaluation”, “Trust”, “Circle-based Security”, and “KES Principle”. Jim will illustrate how these misperceptions with real-world examples and the resulting impact to the companies they supported.   After this presentation, the audience will understand what is meant by “Holistic” security and the “PIES Concept”, and how they are applied to securing any information system.

“Holistic” Security:

Circles,
Pies, or
Crystals

Jim Litchko
Jim@litchko.com

Presentation



- Circle or Pie
  - Holistic and Realistic
- Attitudes
  - Ours and Theirs
- Solutions
  - Case Studies
- Opinions
  - Mine
- Questions
  - Anytime

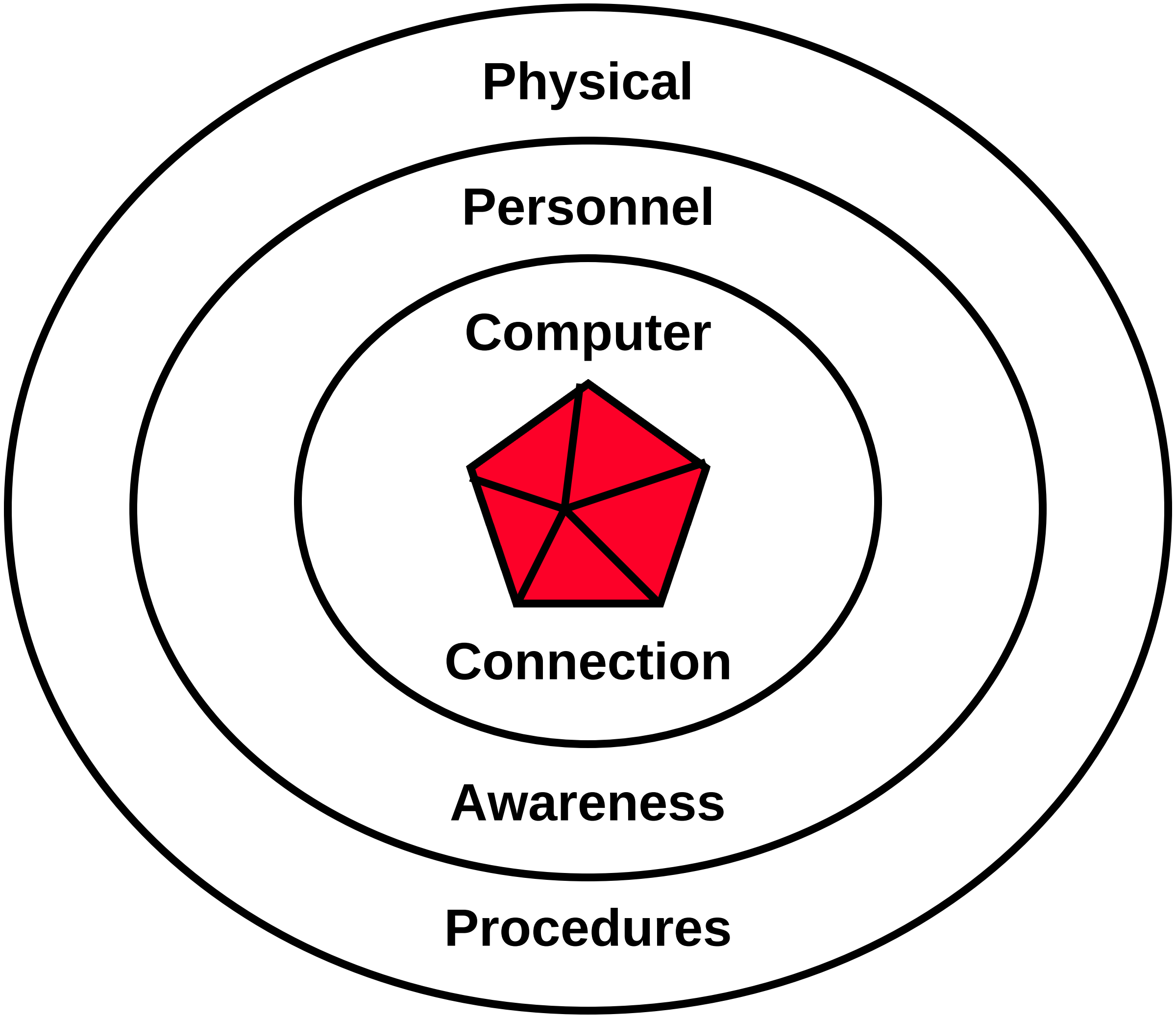
Where can . . .

- Insider is a greater threat then outsiders
- A cup of coffee save you $10,000 - $50,000/hour
- Solve all security problems with on solution - firewall or PKI or . . . .
- A six-pack beer cooler replace a $4,000 fire-proof safe
- Common sense can be replaced by technology

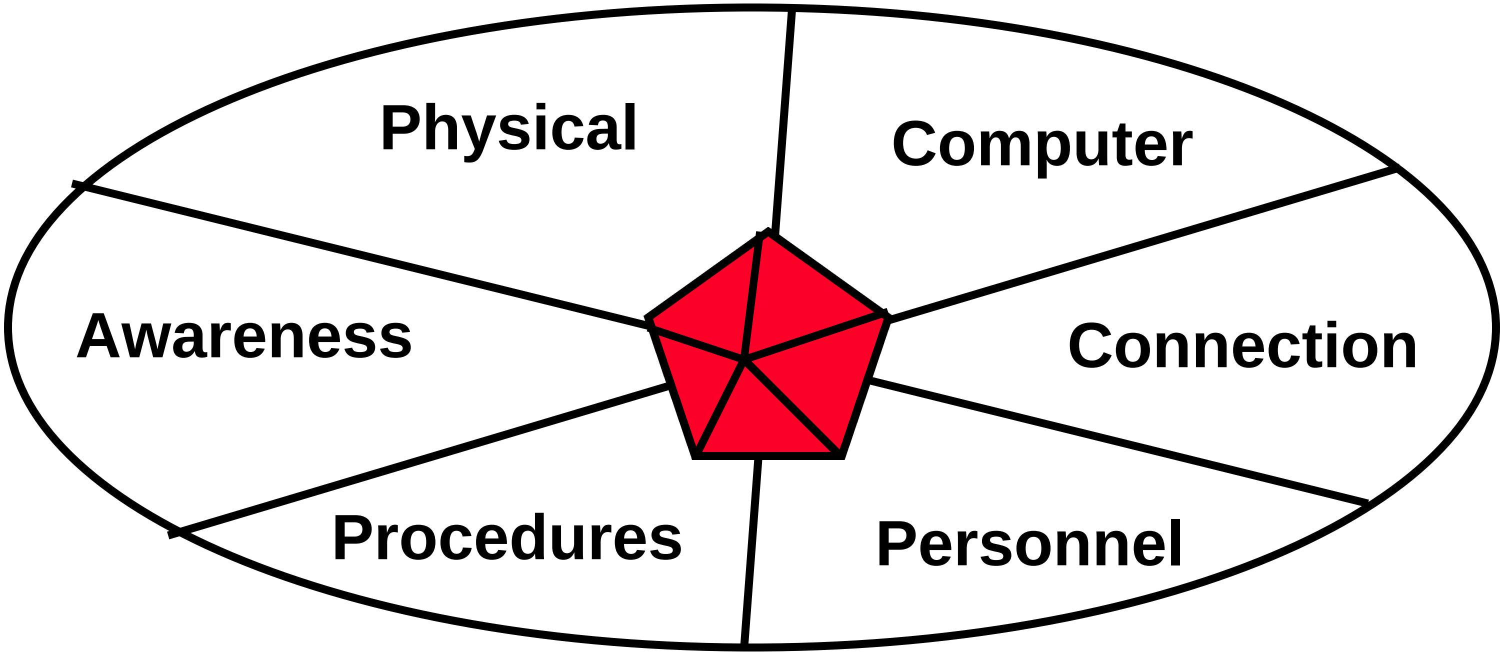
Audience Survey:

- Loses due to Outsider?
- Loses due to Insiders?
- Loses due to CS?

“Fortress” (Circle-based) Security



“Holistic” (Pie-Based) Security

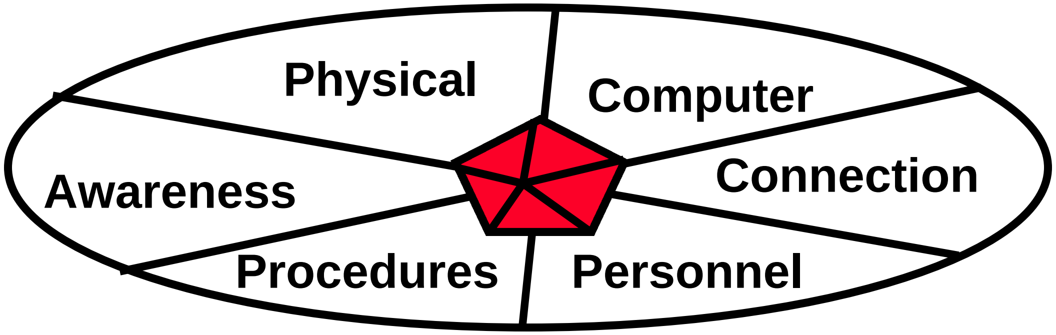


Entry and Departures

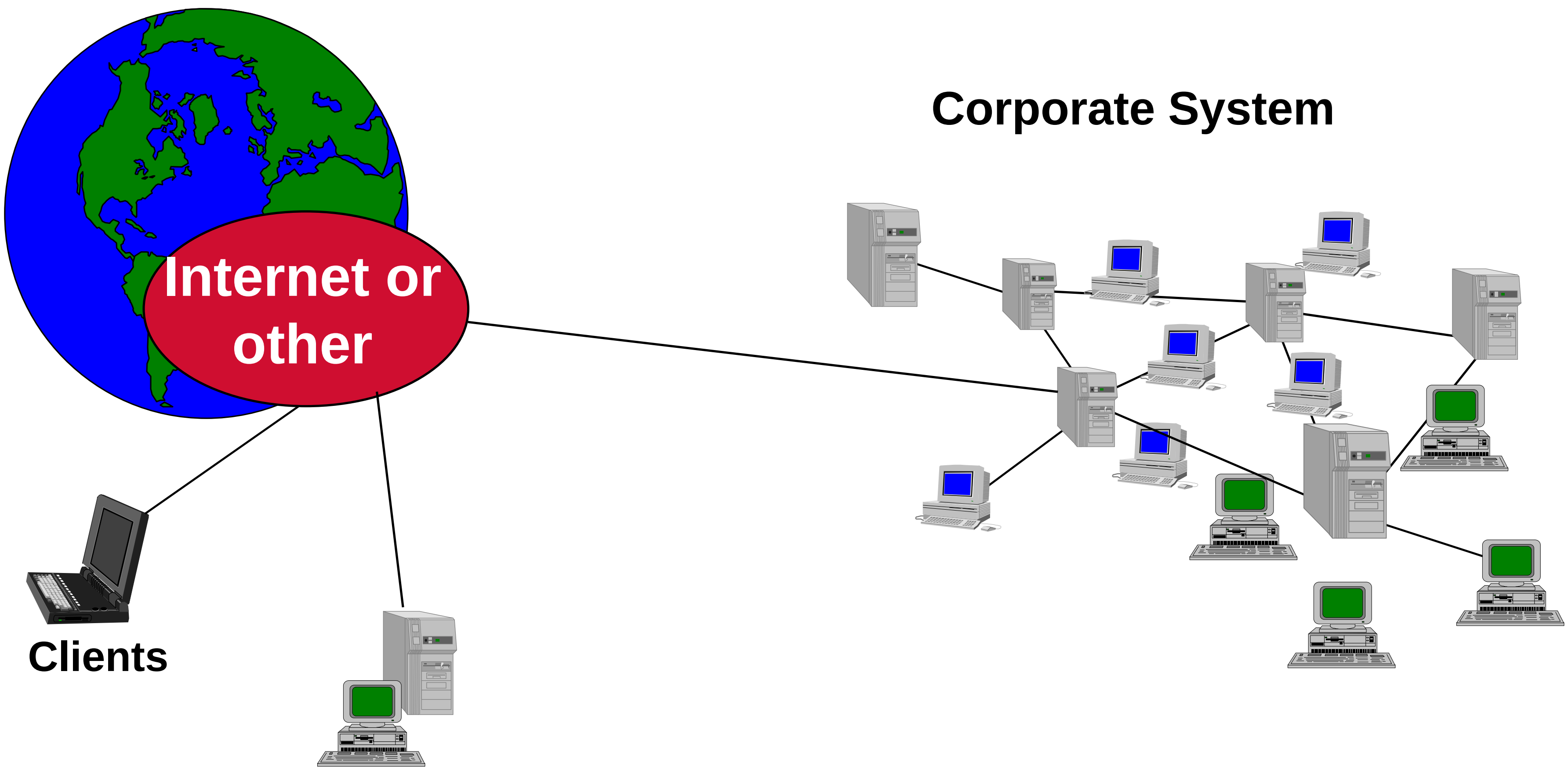
- Initial entry
  - – Last name and first name
  - – Change password on first login
- Departures
  - – Delete account prior to departure, except…..
- Audit Results
  - – 67% continued “first name” past anniversary date
- Personal Experience
  - – Forwarding email continued for months

Attitudes and Perceptions:

- Sailor-Proof
  - – If it is too hard, they will find away around it.
- SNMP is the standard
  - – Not a smoking gun . . . . a bleeding wound is needed.
- What is the aspirin for security:
  - – Firewalls, VPN, PKI, IDS, ...?
  - – Technology will solve all of our problems!
  - – Email monitoring problem solution was policy.



Typical Evolving Network



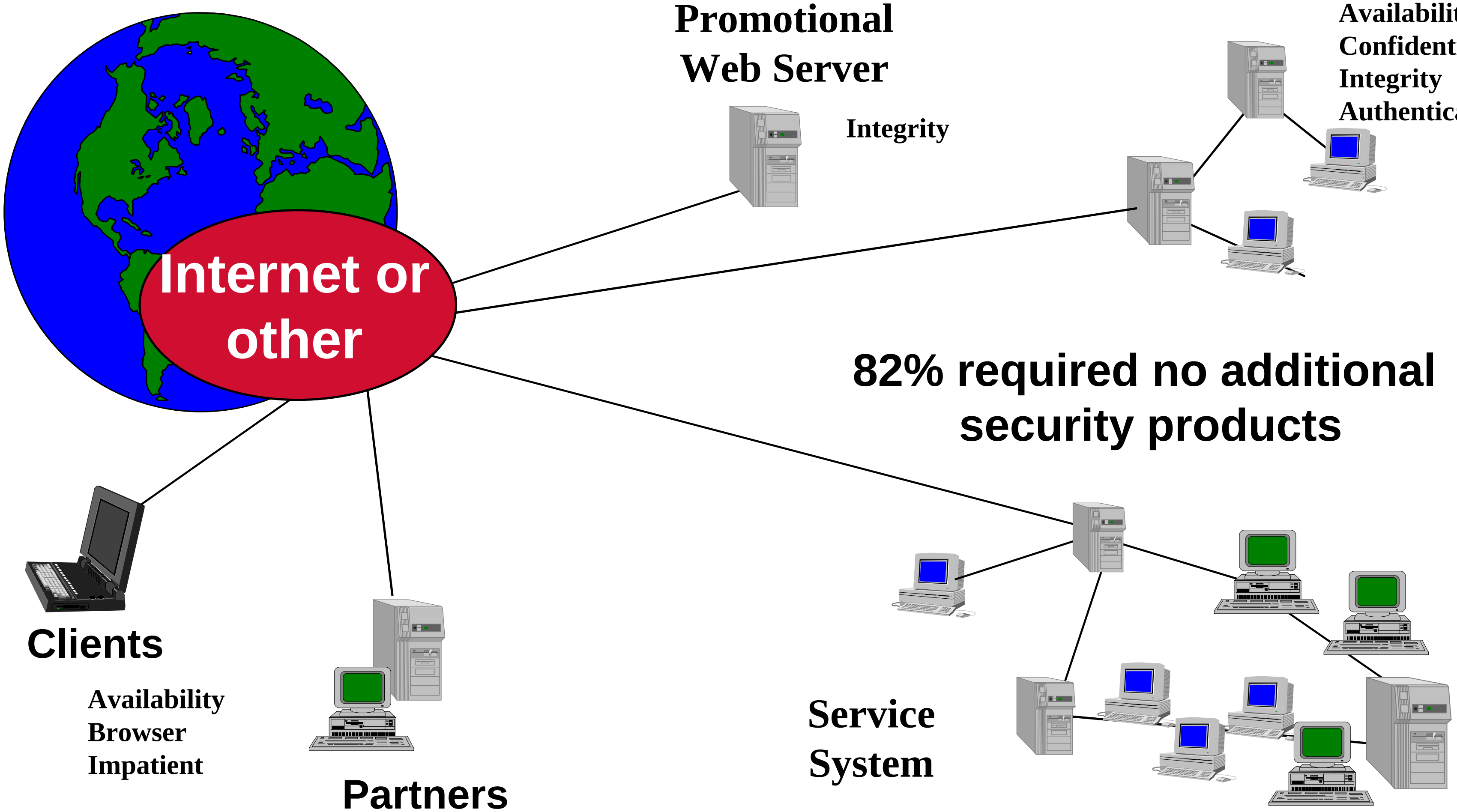
Corporate System

Internet or other

Clients

Partners

Business/Security Requirements



Internet or other

Promotional Web Server

Integrity

Transaction System

Availability
Confidentiality
Integrity
Authentication

82% required no additional security products

Clients

Availability
Browser
Impatient

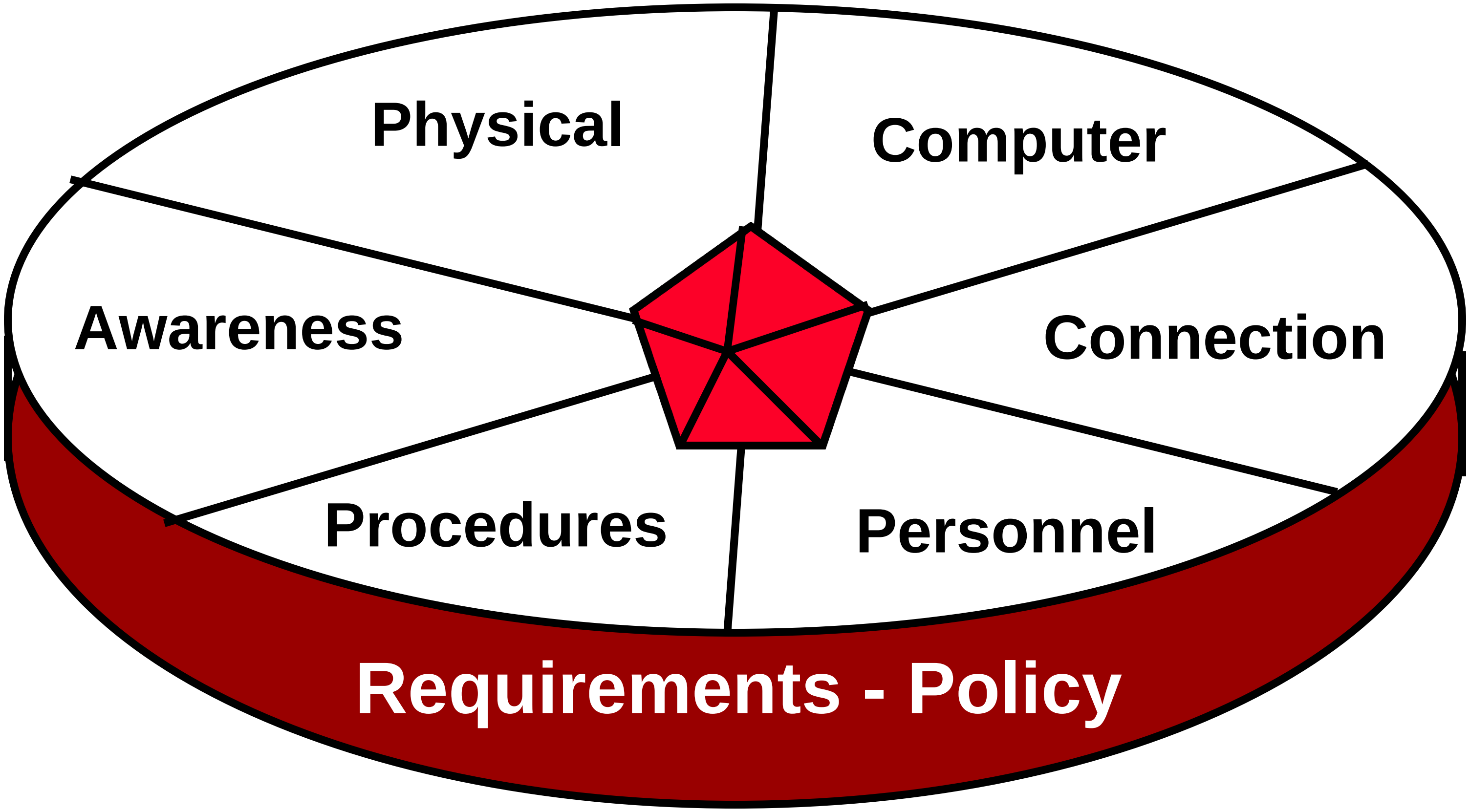
Partners

Confidentiality
Visibility

Service System

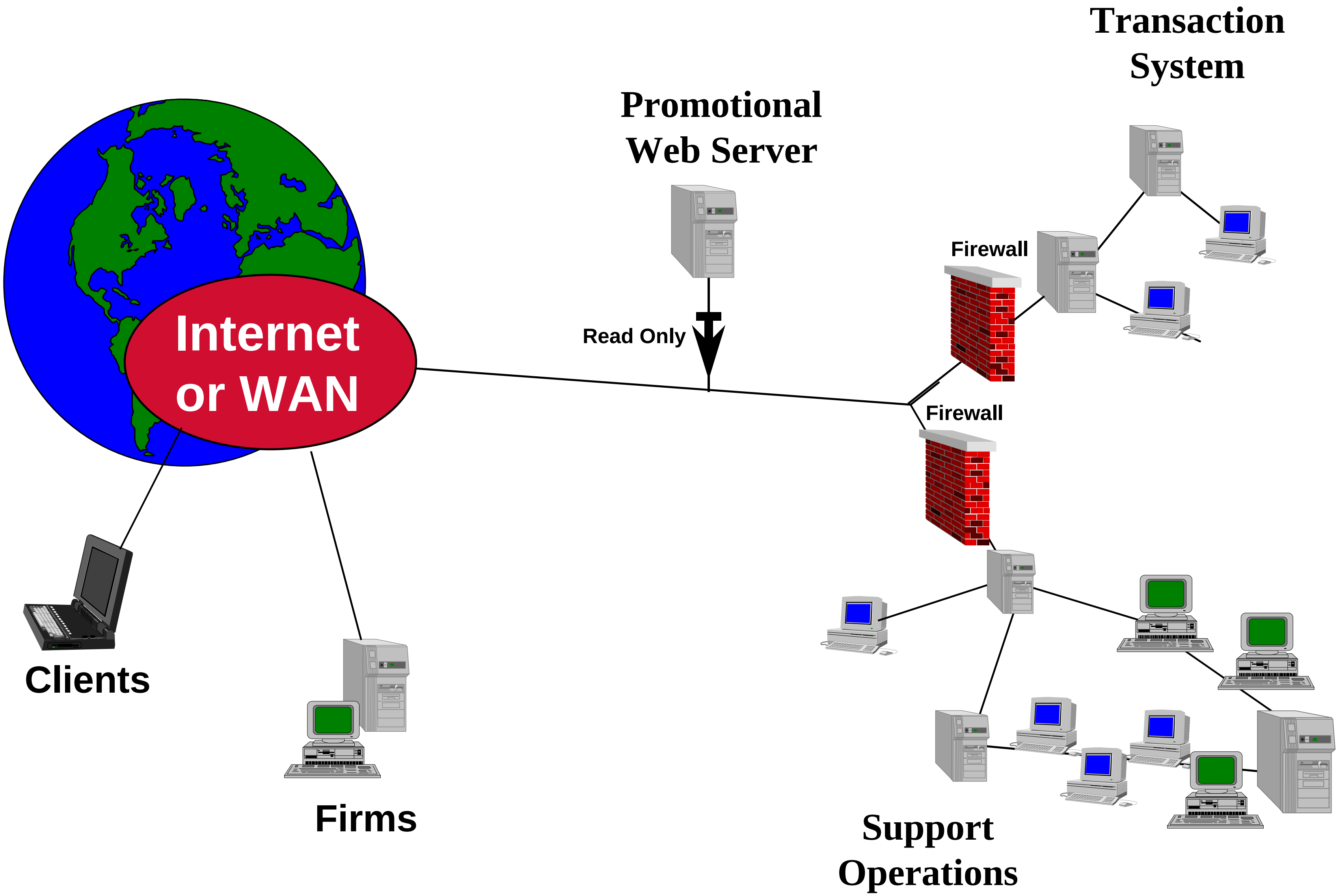
?
Productivity

Policy and Senior Management Support



A firewall is just a door…..Right?

- 50+ complex firewalls for deployment
  - Cost: 50+ x $50,000 = $2.5M
- 3 large government contractors
- How are they to be configured?
  - "Configured? It is a firewall."
- Policy?
  - What do you think the Commanding Officer wants?
  - Policy developed by contractors in 20 minutes.
- Results?


Transaction
System
Promotional
Web Server
Firewall
Internet
or WAN
Read Only
Firewall
Clients
Firms
Support
Operations

Black Box or Crystal Box?

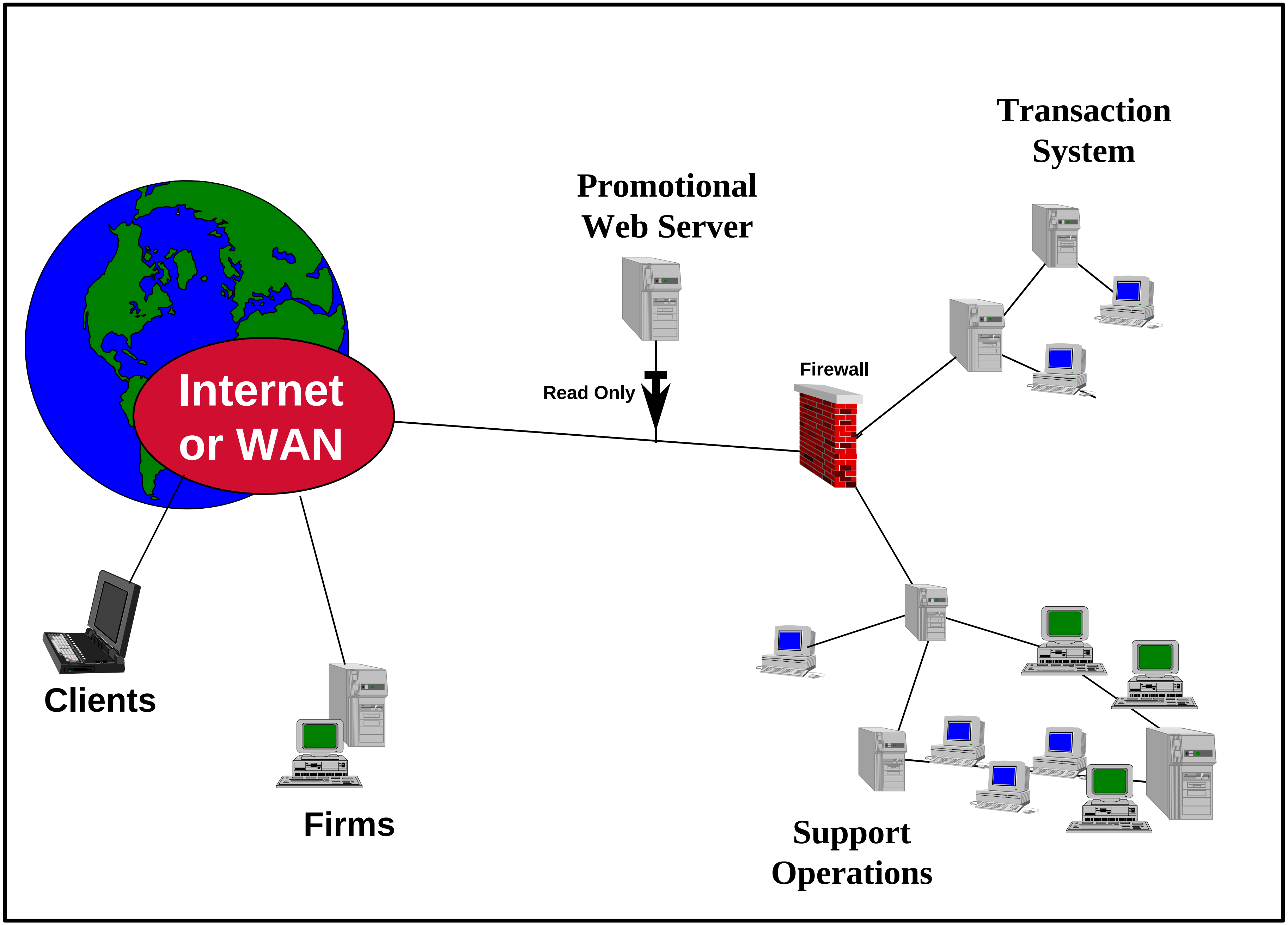
- Crypto algorithms
  - – DES and RSA
  - – Proprietary
- Firewalls
  - – UNIX
  - – NT
- Awareness
  - – KISS
  - – Responsible employees

What and who do we trust? Why?

- Orange Book or Common Criteria
- ICSA
- NSA
- NIST
- Market Share or GUI
- Stock price
- Guarantee
- PKI agent or Bank or ……

KISS - Keep InfoSec Simple

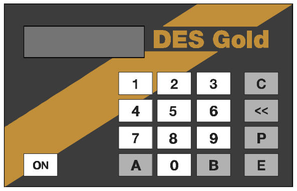
- Firewall is based on simplicity
  - Harden O/S
  - Tight and concise code
- Good and Bad news
  - Firewalls have lots of capabilities
  - Firewalls have lots of capabilities
- Meet “requirement” not the “desirables” or the “potentials”
  - Cost impact
  - Complexity impact - vulnerabilities and cost


Transaction
System
Promotional
Web Server
Internet
or WAN
Read Only
Firewall
Clients
Firms
Support
Operations

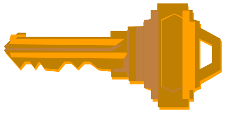
Authentication

- Something that you <u>know</u>:
  - PIN or combination
  - Password
  - Procedure

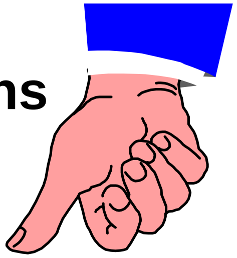
R-38
L-13
R-41



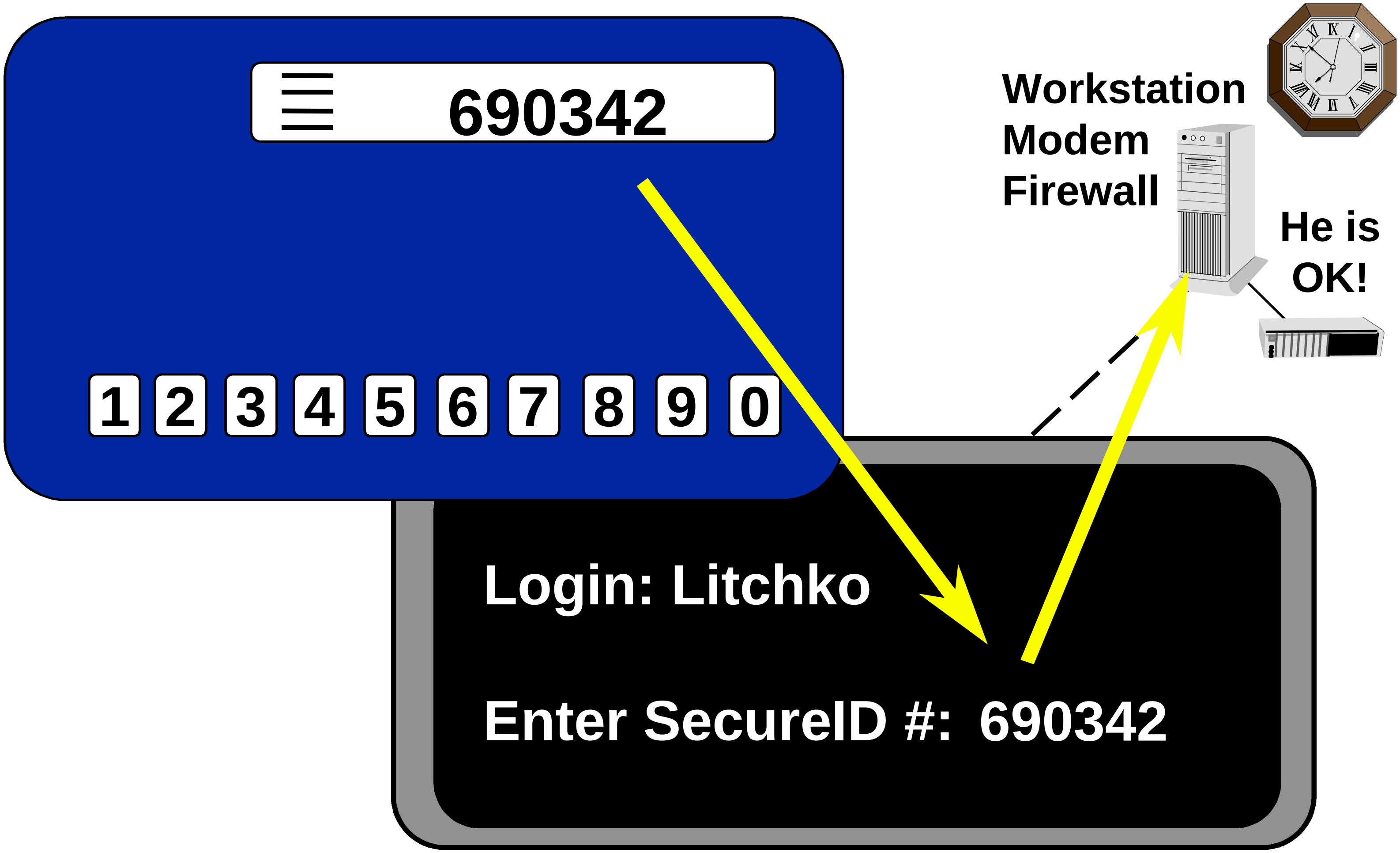
- Something that you <u>have</u>:
  - Badge or ID
  - ATM or Credit card
  - Token



- Something that you <u>are</u>:
  - Finger prints and retina patterns
  - Voice pattern and weight
  - Signature



Password Token .... time based.



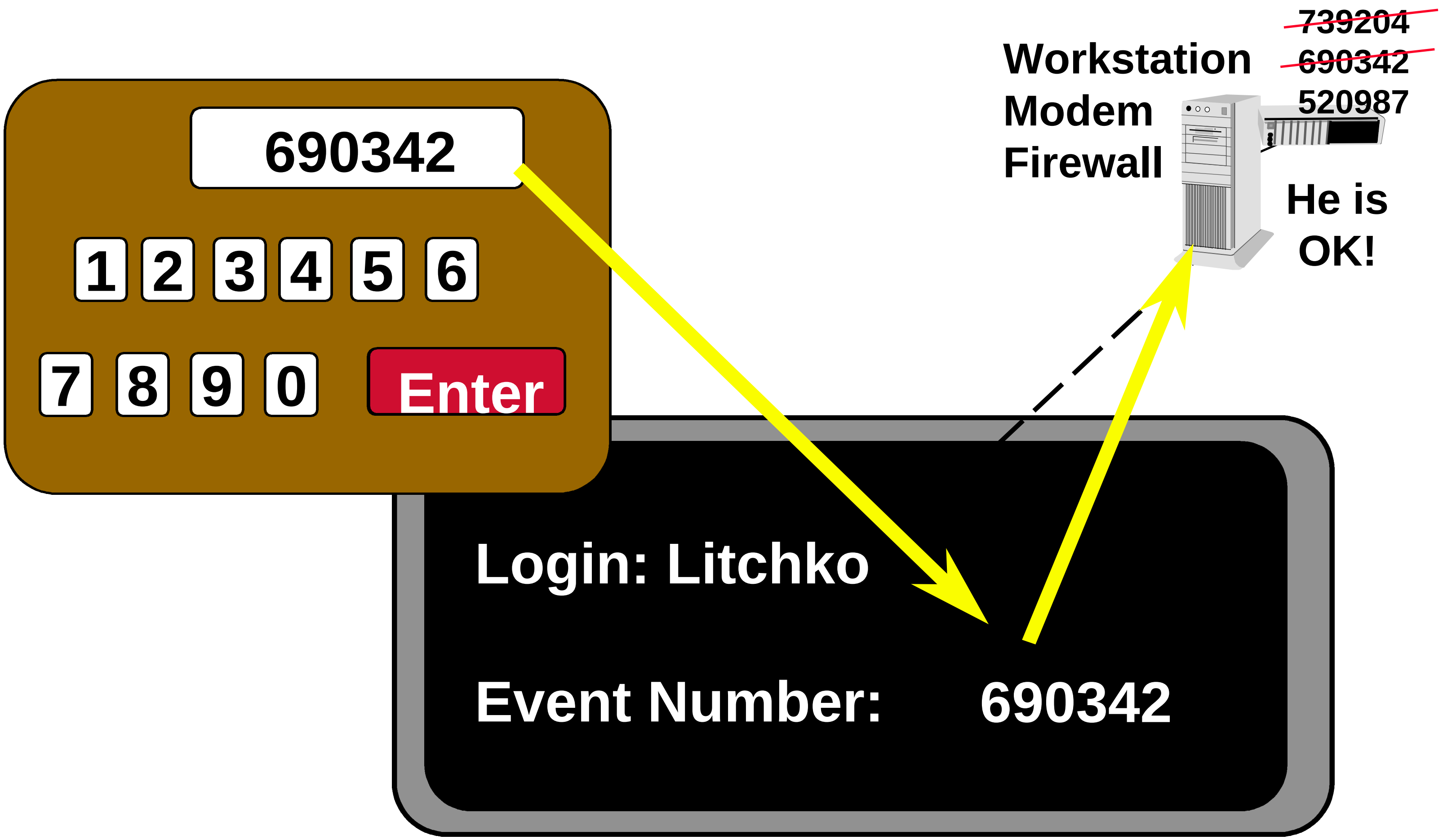
Workstation
Modem
Firewall

He is
OK!

Login: Litchko

Enter SecureID #: 690342

Password Token . . . . . . event based.



690342

1 2 3 4 5 6

7 8 9 0 Enter

Workstation
Modem
Firewall

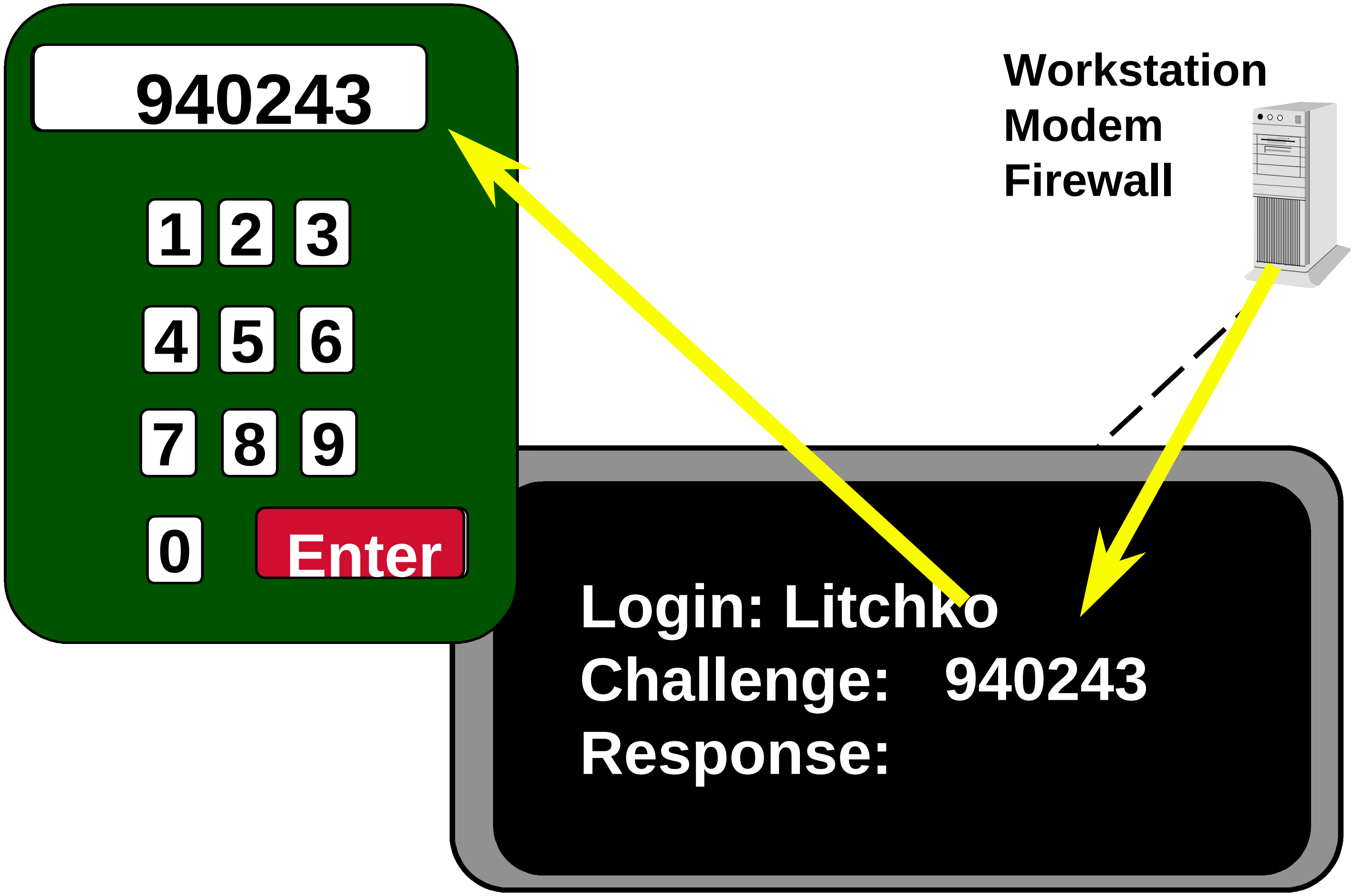
~~739204~~
~~690342~~
520987

He is
OK!

Login: Litchko

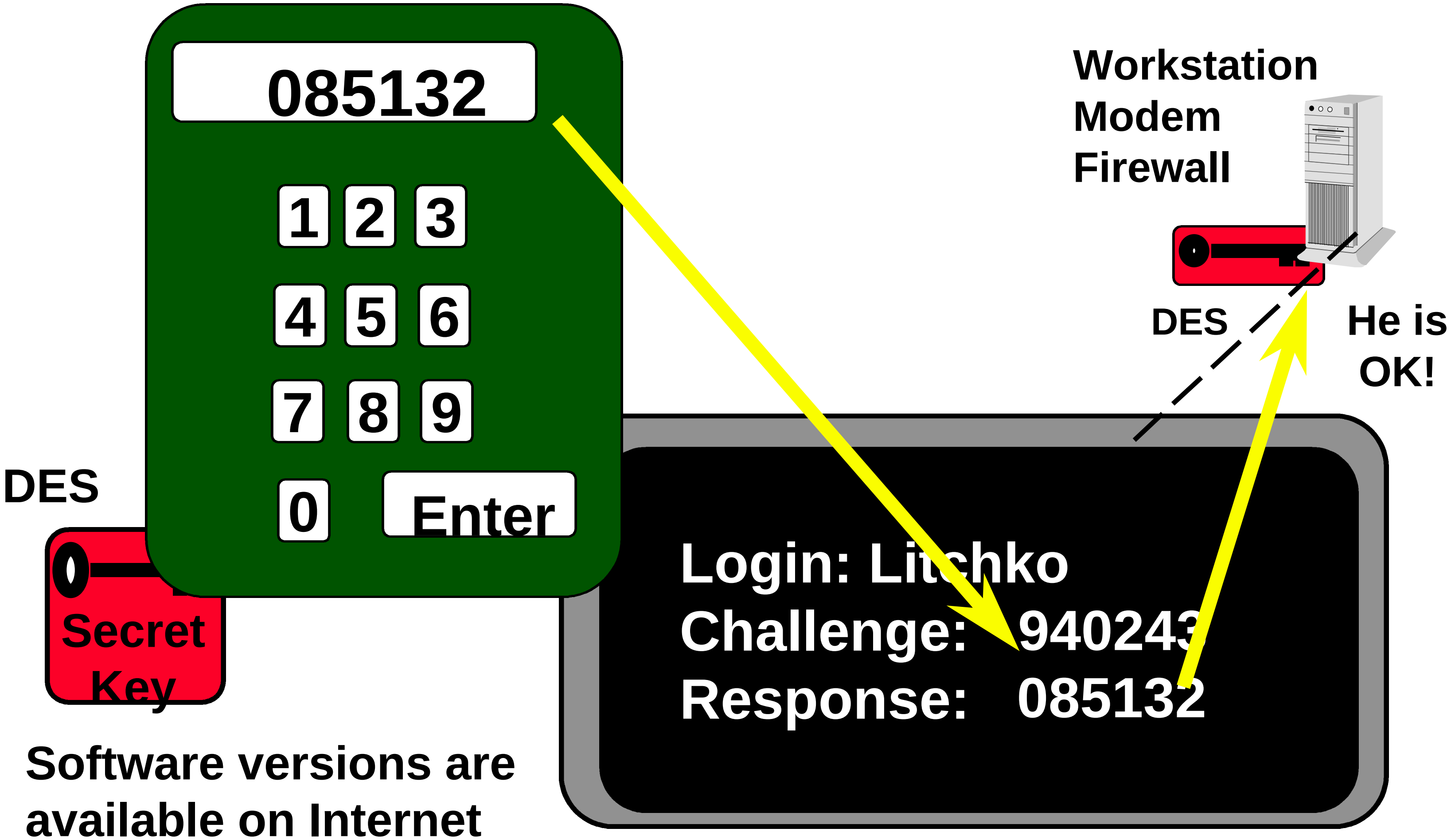
Event Number: 690342

Challenge-Response . . . in a token.



Login: Litchko
Challenge: 940243
Response:

Challenge-Response . . . in a token.



Login: Litchko
Challenge: 940243
Response: 085132

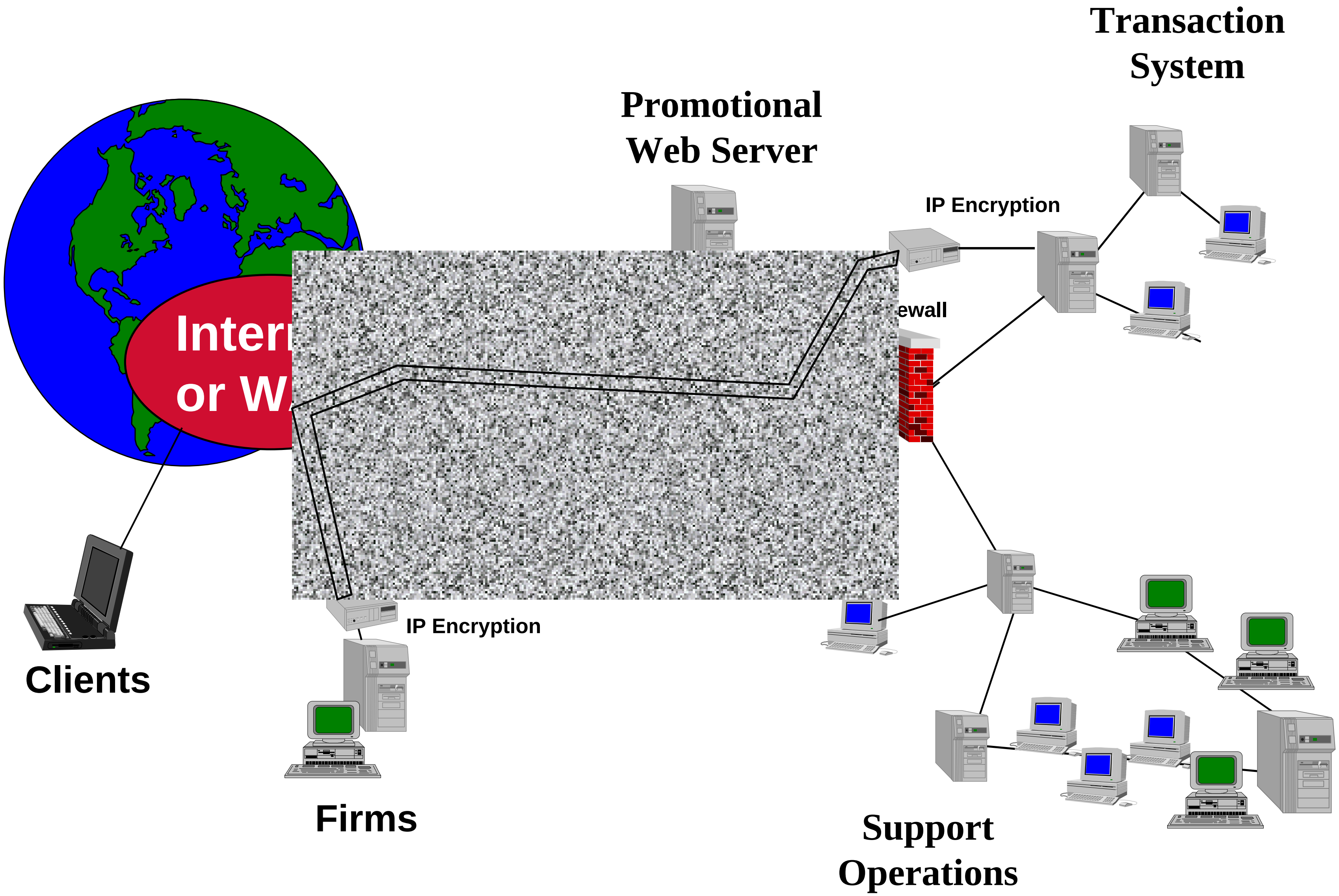
Software versions are available on Internet and from vendors.

Problem

- Subscription Information Service Provider
- Web site distribution
- Computer illiterate users
- Sharing passwords
- $40,000 loss per month
- What is the solution?

PKI is for everyone……is it?

- PKI is “The solution for security”
- Everyone needs a “private key”
  - Authentication - all
  - Signature - some
- Who will be my Certification Authority?
  - Verisign, GTE, NSA, ...
  - Bank
  - Mom
  - Me
- Why?



Transaction System

Promotional Web Server

IP Encryption

Inter

or W

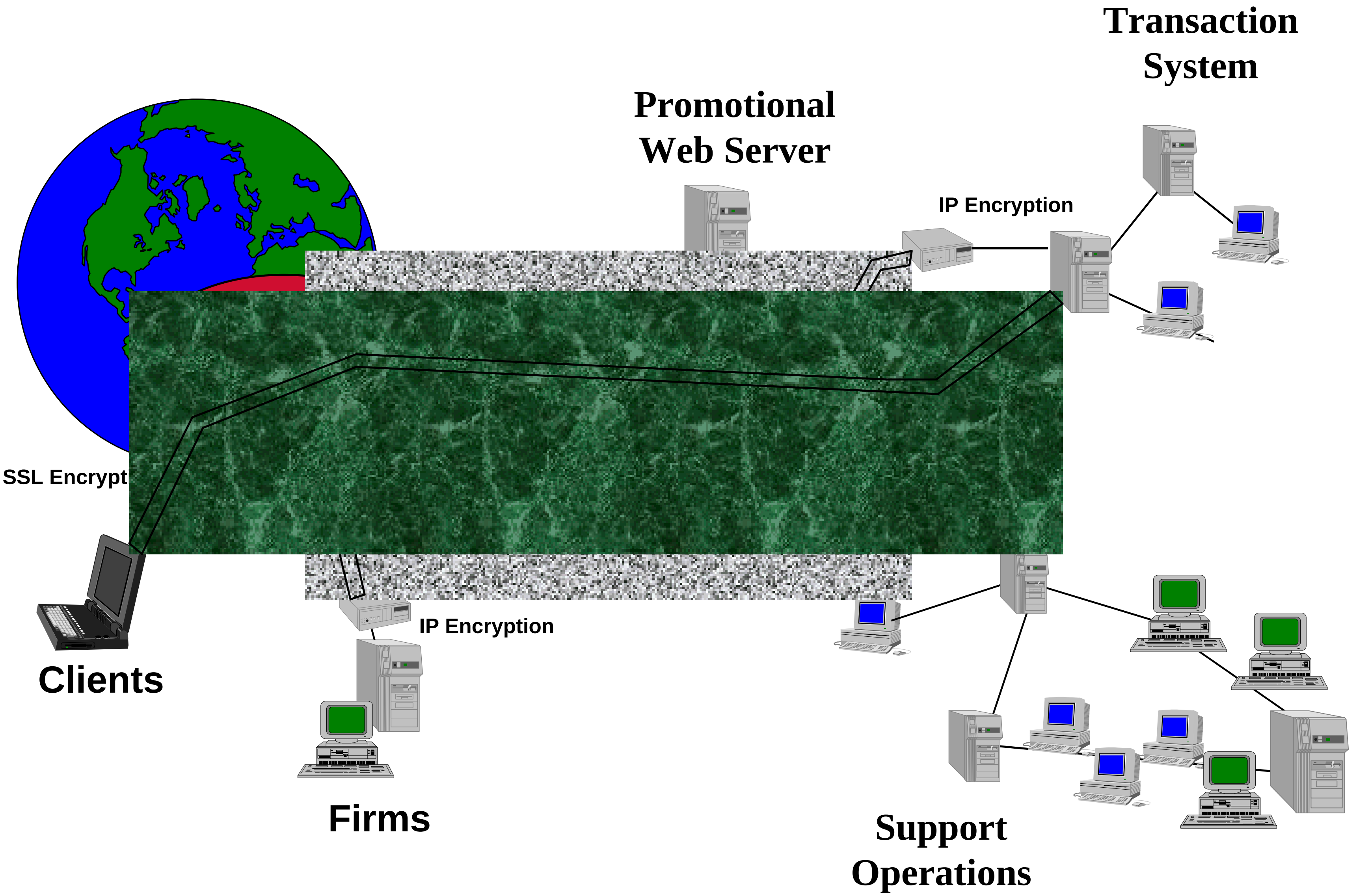
ewall

Clients

IP Encryption

Firms

Support Operations



Transaction System

Promotional Web Server

IP Encryption

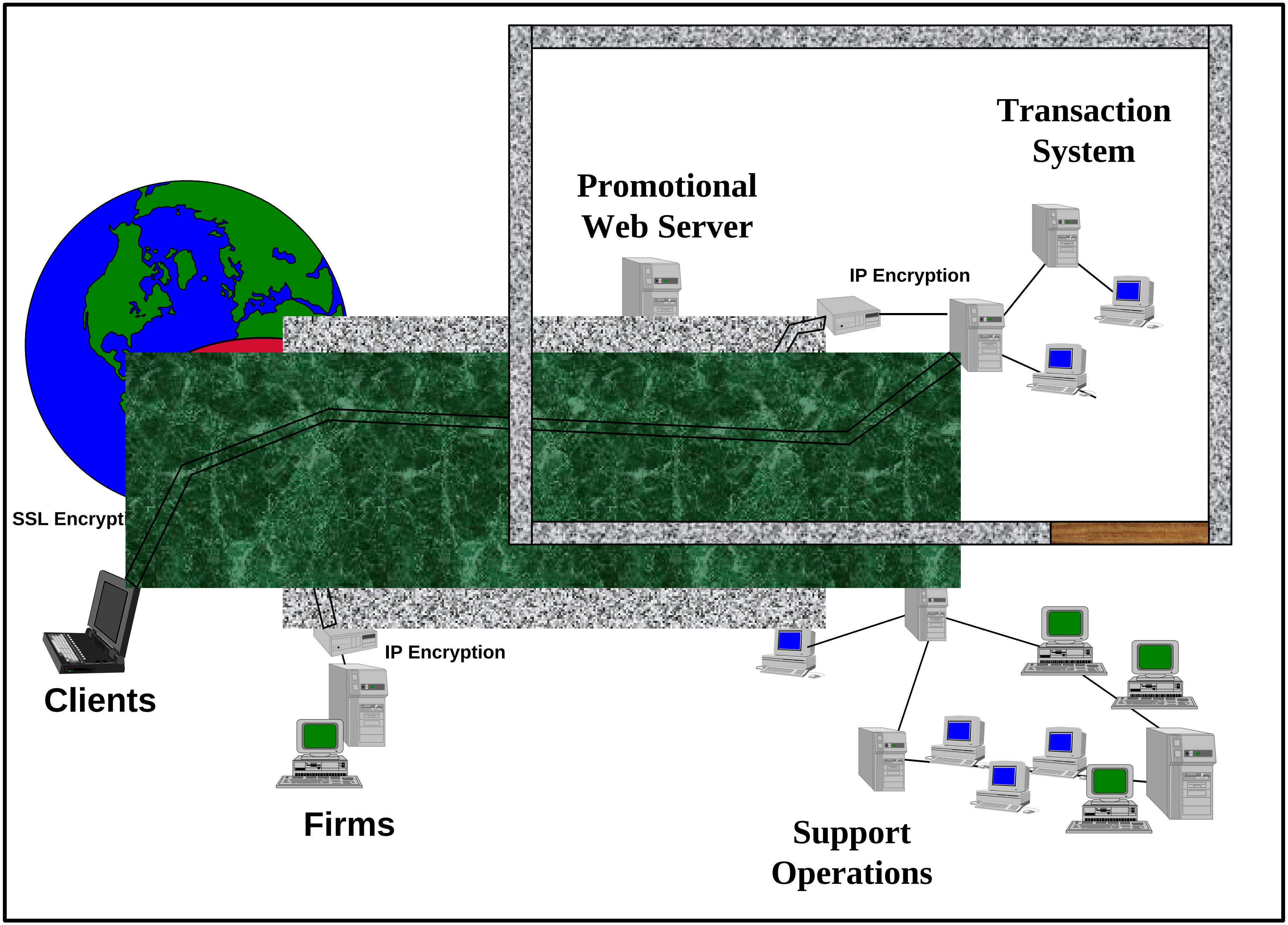
SSL Encrypt

Clients

IP Encryption

Firms

Support Operations



Transaction System

Promotional Web Server

IP Encryption

SSL Encrypt

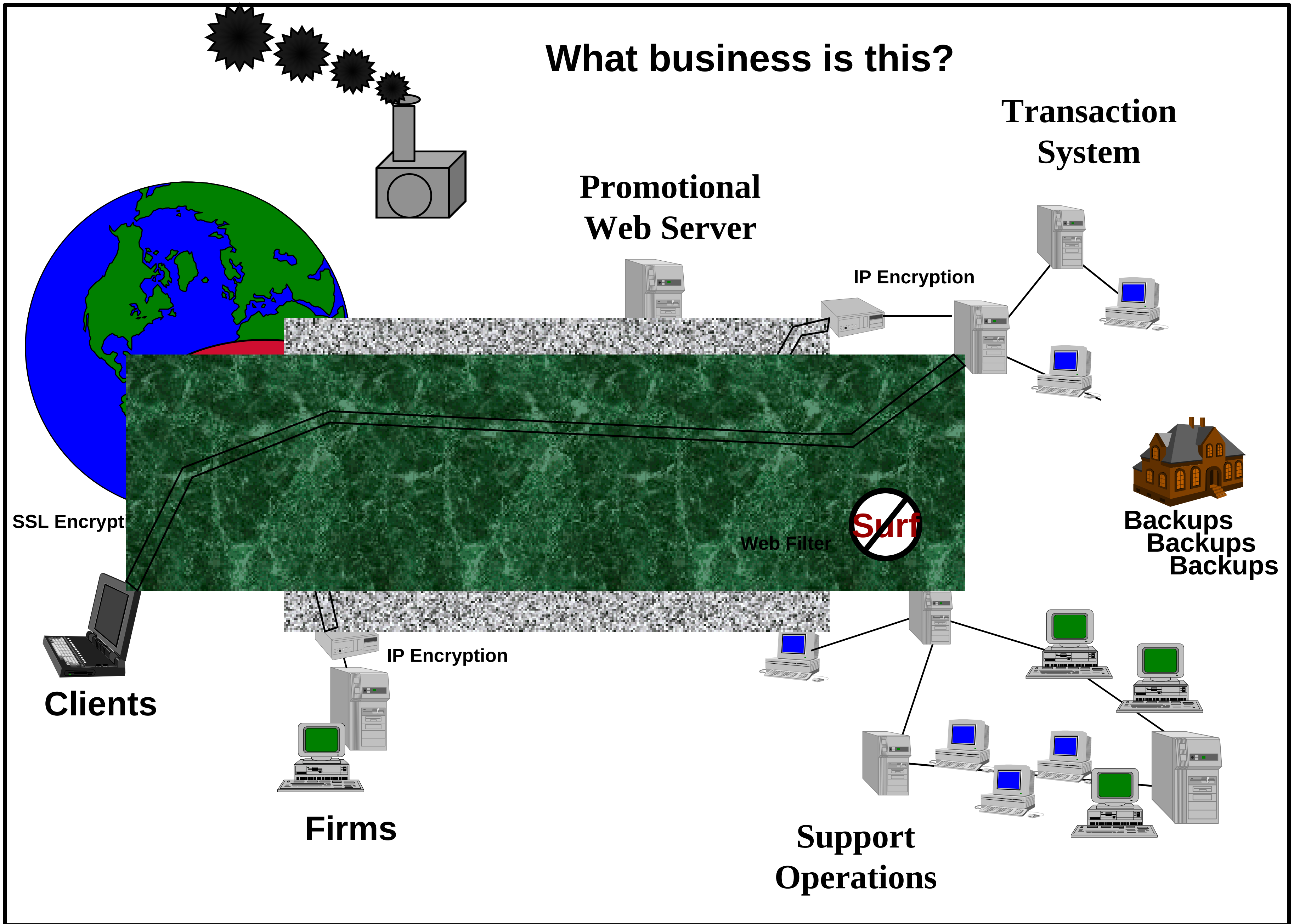
IP Encryption

Clients

Firms

Support Operations

What business is this?



Transaction System

Promotional Web Server

IP Encryption

SSL Encrypt

Surf

Web Filter

Backups
Backups
Backups

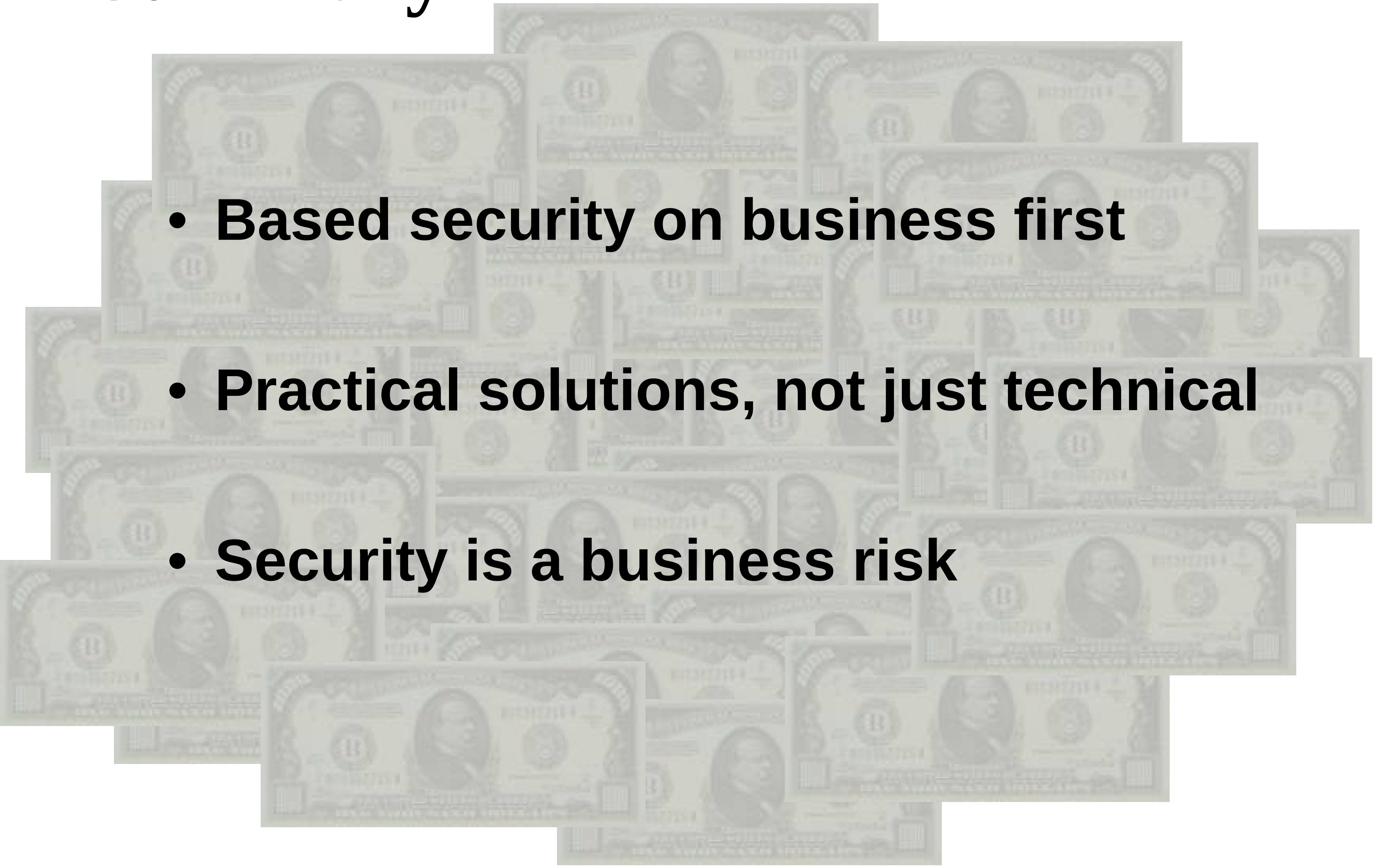
Clients

IP Encryption

Firms

Support Operations

Summary



- Based security on business first
- Practical solutions, not just technical
- Security is a business risk

“Holistic” Security: Circles, Pies, or Crystals?

Securing a system is not like plugging a hole in a dam. Throwing a firewall and/or cryptography at the problem is not enough. Using his over twenty years of experience conducting system security reviews, he will identify the most common security misperceptions that he has seen, i.e., “Black Box Solutions”, “MS Evaluation”, “Trust”, “Circle-based Security”, and “KISS Principle”. Jim will illustrate how these misperceptions with real-world examples and the resulting impact to the companies they supported. After this presentation, the audience will understand what is meant by “Holistic” security and the “PIES Concept”, and how they are applied to securing any information system.