

Welcome

# Jericho Forum Meeting

12<sup>th</sup> May 2006

Hosted by Motorola

Schaumburg, IL., USA



# Introduction

- **Ian Dobson**
- Director, Jericho Forum, The Open Group

# Agenda

- 09.30 Introduction – Ian Dobson, Director, Jericho Forum, The Open Group
- 09.40 Welcome & Logistics – Bill Boni, VP, Information & Protection, Motorola
- 09.50 Setting the Scene – evolution of the Jericho Forum - Paul Simmonds, ICI
- 10.10 The Jericho Forum Commandments - Nick Bleech, Rolls Royce
- 10.45 **Break**
- 11.00 Real world application: Protocols - Paul Simmonds, ICI
- 11.20 Real world application: VoIP – David McCaskill, Procter & Gamble
- 11.40 Real world application: Corporate Wireless Networking - Paul Simmonds, ICI
- 12.00 Case Study: What Hath Vint Wrought - Steve Whitlock, Boeing
- 12.30 Case Study: Migration to de-perimeterised environment - Mark Winzenburg, BP
- 13.00 **Lunch**
- 14.00 Prepare for the future: The de-perimeterised “road warrior” - Paul Simmonds
- 14.45 Prepare for the future: Roadmap for de-perimeterization - Nick Bleech
- 15.30 **Break**
- 15.45 Face the audience: (Q&A) - Moderated by Scott Shepard, Motorola
- 16.45 Summing up the day – Bill Boni
- 17.00 Close

# Some of our members



# Welcome & Logistics

- **Bill Boni**
- *VP, Information Protection & Security, Motorola*

# Setting the Scene

- **Paul Simmonds**
- *Global Information Security Director, ICI & Jericho Forum Board*

# What is the Jericho Forum?

- First, what actually is de-perimeterisation?
- Then, the Jericho Forum
  - How the two are related?
  - It's composition
  - It's relationship with the Open Group
  - It's charter
  - It's remit

# So what is de-perimeterisation?

## **It's fundamentally acceptance that:**

- Most exploits will easily transit perimeter security
  - We let through e-mail
  - We let through web
  - We will need to let through VoIP
  - We let through encrypted traffic (SSL, SMTP-TLS, VPN),
- Your border has effectively become a QoS Boundary
- Protection has little/no benefit at the perimeter,
- It's easier to protect data the closer we get to it,
- A hardened perimeter strategy is at odds with current and/or future business needs,
- A hardened perimeter strategy is un-sustainable.



# So what is it actually?

## **It's a concept:**

- It's how we solve the business needs for our businesses without a hardened perimeter,
- It's how businesses leverage new opportunities when there is no hardened perimeter,
- It's a set of solutions within a framework that we can pick and mix from,
- It's defence in depth,
- It's business-driven security solutions

It is not a single solution – it's a way of thinking . . .

## **Thus:**

- **There's a need to challenge conventional thinking**
- **There's the need to change existing mindsets**

# Why the Jericho Forum?

## Why now?

- No one else was discussing the problem
- Everyone was fixated on perimeter based designs
- Somebody needed to point out the “Kings new clothes” to the world
- Someone needed to start the discussion

## What's in it for us?

- We need Security Solutions that support de-perimeterisation – so we aim to stimulate a market for solutions to de-perimeterisation problems
- We want these solutions to use open standards, to improve interoperability and integration, both within our own IT systems and with our business partners

# The Jericho Forum Composition

## Initial Composition

- Initially only consumer (user) organisations
  - To define the problem space
  - To create and establish the initial vision
  - Free from perceptions of influence from vendors
  - With the promise of vendor involvement once the vision defined

## That point was passed at end-2004:

- User members own the Forum, vote on the deliverables, and run the Board of Managers (BoM)
- Vendors have no voting rights on deliverables or on the BoM
- We now have 12 vendor members, and want more, because we need to work with vendors

# The Open Group relationship

## ■ Why The Open Group?

- Experience with member-led “groups” of organisations and individuals
- Track record of delivery
- Regarded as open, vendor neutral, and impartial
- All published output is free or available under equal fair license terms
- Existing governance framework with a good fit for Jericho Forum requirements
- Existing legal framework – protects Forum members
- Global organisation
- Open Group vision for Boundaryless Information Flow is well aligned with Jericho Forum vision for de-perimeterisation

# The Jericho Forum Charter & Remit

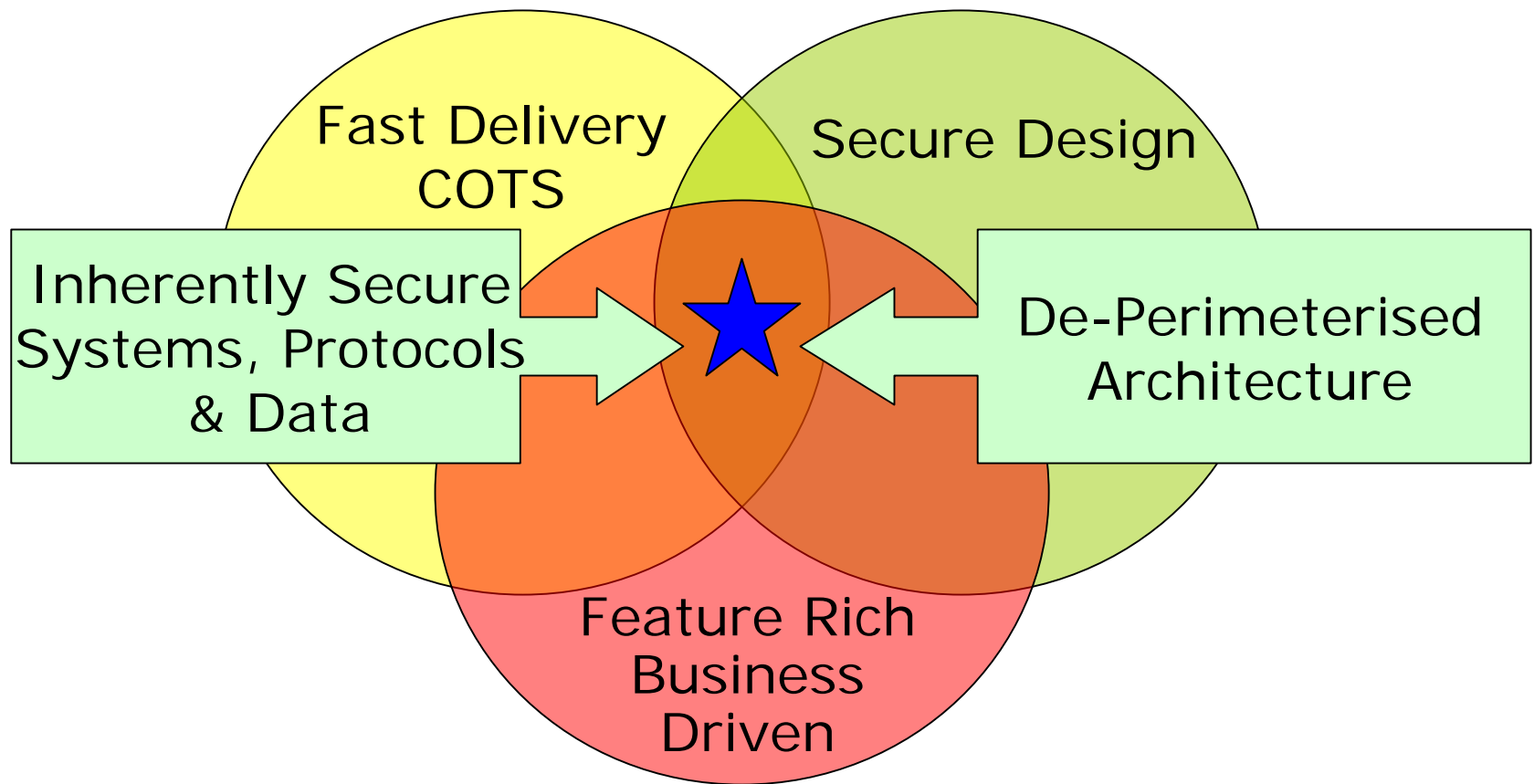
## **The Jericho Forum AIMS . . .**

- to drive and influence the discussion / change the mindset
- to help make de-perimeterised solutions work in the corporate space
- to refine and distinguish between what are Jericho Forum architectural principals vs. good secure design
- to build on the work in the published Visioning Document
- to define key items aligned with messages that make them specifically part of the Jericho Forum solutions space
- to clarify that there is not just one “Jericho Forum solution” (one size does not fit all)

## **The Jericho Forum IS NOT . . .**

- another standards body
- a cartel – this is not about buying a single solution
- here to compete with or dismantle existing “good security”.

# Jericho Forum Principles vs. Good Secure Design



# The Challenge

*We believe that in tomorrow's world  
the only successful e-transactions & businesses  
will utilise a de-perimeterised architecture*

## Thus the choice:

- sit back and hope the vendors will produce new solutions that keep the burgeoning IT security problems from overwhelming you?

## Or

- work with us to design the future to ensure you can buy the solutions YOUR business needs?

**We've made great progress since we started.**

**Work with us, to share the benefits of developing  
common requirements for tomorrow's IT solutions**

# Setting the Foundations

- **The Jericho Forum “Commandments”**
- **Nick Bleech**  
IT Security Director, Rolls Royce  
& Jericho Forum Board



I have ten commandments. The first nine are,  
thou shalt not bore.

The tenth is, thou shalt have right of final cut.

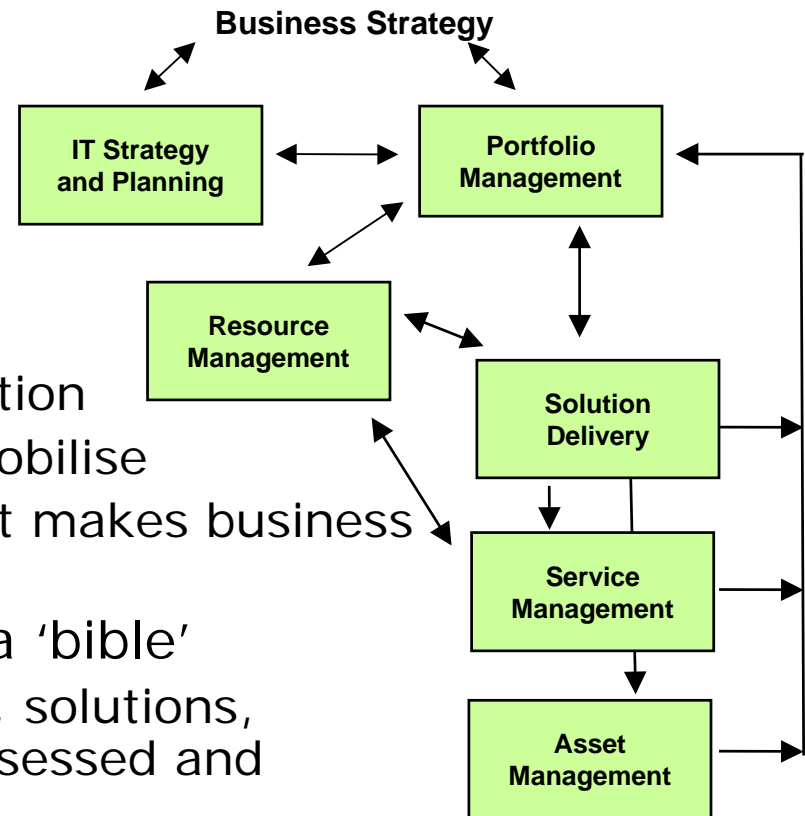


## Rationale

- Jericho Forum in a nutshell: “Your security perimeters are disappearing: what are you going to do about it?”
- Need to express what / why / how to do it in high level terms (but allowing for detail)
- Need to be able to draw distinctions between ‘good’ security (e.g. ‘principle of least privilege’) and ‘de-perimeterisation security’ (e.g. ‘end-to-end principle’)

# Why should I care?

- De-perimeterisation is a disruptive change
- There is a huge variety of:
  - Starting points / business imperatives
  - Technology dependencies / evolution
  - Appetite for change / ability to mobilise
  - Extent of de-perimeterisation that makes business sense / ability to influence
- So we need rules-of-thumb, not a 'bible'
  - "A benchmark by which concepts, solutions, standards and systems can be assessed and measured."



# Structure of the Commandments

- Fundamentals (3)
- Surviving in a hostile world (2)
- The need for trust (2)
- Identity, management and federation (1)
- Access to data (3)

# Fundamentals

1. The scope and level of protection must be specific and appropriate to the asset at risk.
  - Business demands that security enables business agility and is cost effective.
  - Whereas boundary firewalls may continue to provide basic network protection, individual systems and data will need to be capable of protecting themselves.
  - In general, it's easier to protect an asset the closer protection is provided.

# Fundamentals

2. Security mechanisms must be pervasive, simple, scalable and easy to manage.
  - Unnecessary complexity is a threat to good security.
  - Coherent security principles are required which span all tiers of the architecture.
  - Security mechanisms must scale:
    - from small objects to large objects.
  - To be both simple and scalable, interoperable security “building blocks” need to be capable of being combined to provide the required security mechanisms.

# Fundamentals

## 3. Assume context at your peril.

- Security solutions designed for one environment may not be transferable to work in another:
  - thus it is important to understand the limitations of any security solution.
- Problems, limitations and issues can come from a variety of sources, including:
  - Geographic
  - Legal
  - Technical
  - Acceptability of risk, etc.

# Surviving in a hostile world

4. Devices and applications must communicate using open, secure protocols.
  - Security through obscurity is a flawed assumption
    - secure protocols demand open peer review to provide robust assessment and thus wide acceptance and use.
  - The security requirements of confidentiality, integrity and availability (reliability) should be assessed and built in to protocols as appropriate, not added on.
  - Encrypted encapsulation should only be used when appropriate and does not solve everything.



# Surviving in a hostile world

5. All devices must be capable of maintaining their security policy on an untrusted network.
  - A “security policy” defines the rules with regard to the protection of the asset.
  - Rules must be complete with respect to an arbitrary context.
  - Any implementation must be capable of surviving on the raw Internet, e.g., will not break on any input.

# The need for trust

6. All people, processes, technology must have declared and transparent levels of trust for any transaction to take place.
  - There must be clarity of expectation with all parties understanding the levels of trust.
  - Trust models must encompass people/organisations and devices/infrastructure.
  - Trust level may vary by location, transaction type, user role and transactional risk.

# The need for trust

7. Mutual trust assurance levels must be determinable.

- Devices and users must be capable of appropriate levels of (mutual) authentication for accessing systems and data.
- Authentication and authorisation frameworks must support the trust model.

# Identity, Management and Federation

8. Authentication, authorisation and accountability must interoperate/ exchange outside of your locus/ area of control.
  - People/systems must be able to manage permissions of resources they don't control.
  - There must be capability of trusting an organisation, which can authenticate individuals or groups, thus eliminating the need to create separate identities.
  - In principle, only one instance of person / system / identity may exist, but privacy necessitates the support for multiple instances, or once instance with multiple facets.
  - Systems must be able to pass on security credentials/assertions.
  - Multiple loci (areas) of control must be supported.

## Finally, access to data

9. Access to data should be controlled by security attributes of the data itself.
  - Attributes can be held within the data (DRM/Metadata) or could be a separate system.
  - Access / security could be implemented by encryption.
  - Some data may have “public, non-confidential” attributes.
  - Access and access rights have a temporal component.

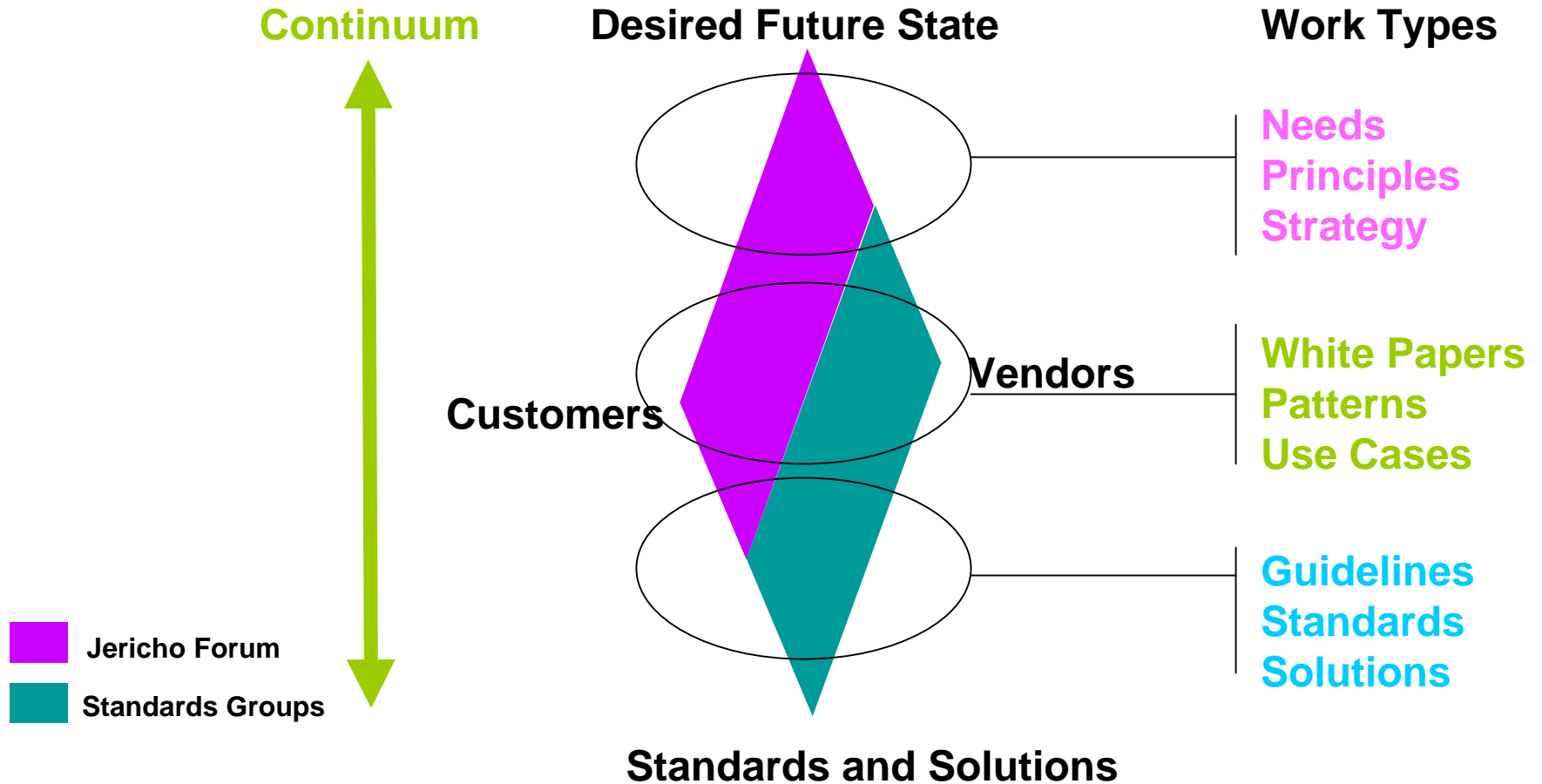
## Finally, access to data

10. Data privacy (and security of any asset of sufficiently high value) requires a segregation of duties/privileges
  - Permissions, keys, privileges etc. must ultimately fall under independent control
    - or there will always be a weakest link at the top of the chain of trust.
  - Administrator access must also be subject to these controls.

## Finally, access to data

11. By default, data must be appropriately secured both in storage and in transit.
  - Removing the default must be a conscious act.
  - High security should not be enforced for everything:
    - “appropriate” implies varying levels with potentially some data not secured at all.

# Consequences ... is that it?





# Consequences...is that it?

- We may formulate (a few) further Commandments ... and refine what we have ... based on
  - Your feedback (greatly encouraged)
  - Position papers (next level of detail)
  - Taxonomy work
  - Experience
- Today's roadmap session will discuss where we go from here

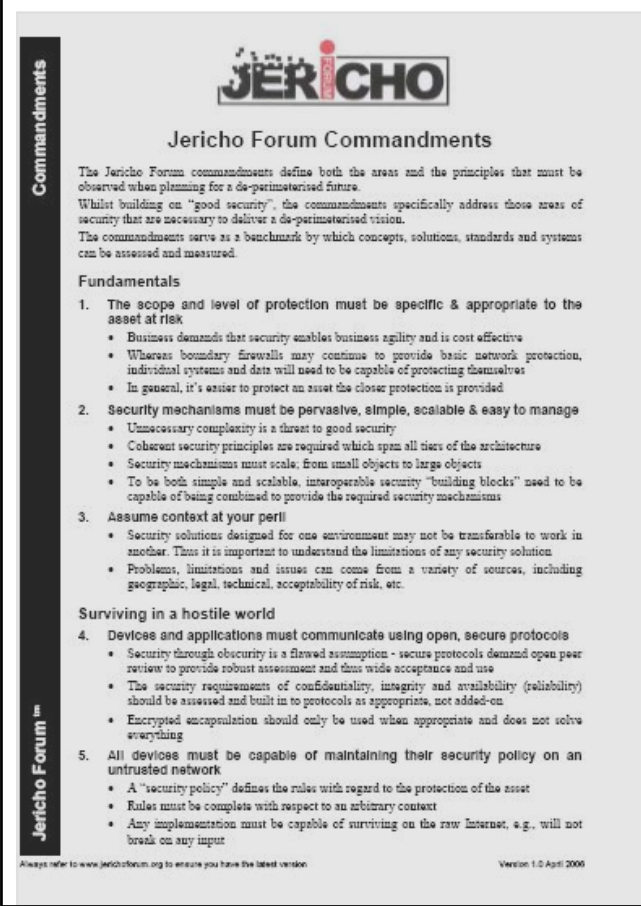
What I have crossed out I didn't like.  
What I haven't crossed out I'm  
dissatisfied with.



# Paper available from the Jericho Forum

- The Jericho Forum “Commandments” are freely available from the Jericho Forum Website

<http://www.jerichoforum.org>



**Jericho Forum Commandments**

The Jericho Forum commandments define both the areas and the principles that must be observed when planning for a de-petrimeterised future. Whilst building on “good security”, the commandments specifically address those areas of security that are necessary to deliver a de-petrimeterised vision. The commandments serve as a benchmark by which concepts, solutions, standards and systems can be assessed and measured.

**Fundamentals**

1. The scope and level of protection must be specific & appropriate to the asset at risk
  - Business demands that security enables business agility and is cost effective
  - Whereas boundary firewalls may continue to provide basic network protection, individual systems and data will need to be capable of protecting themselves
  - In general, it's easier to protect an asset the closer protection is provided
2. Security mechanisms must be pervasive, simple, scalable & easy to manage
  - Unnecessary complexity is a threat to good security
  - Coherent security principles are required which span all tiers of the architecture
  - Security mechanisms must scale, from small objects to large objects
  - To be both simple and scalable, interoperable security “building blocks” need to be capable of being combined to provide the required security mechanisms
3. Assume context at your peril
  - Security solutions designed for one environment may not be transferable to work in another. Thus it is important to understand the limitations of any security solution
  - Problems, limitations and issues can come from a variety of sources, including geographic, legal, technical, acceptability of risk, etc.

**Surviving in a hostile world**

4. Devices and applications must communicate using open, secure protocols
  - Security through obscurity is a flawed assumption - secure protocols demand open peer review to provide robust assessment and thus wide acceptance and use
  - The security requirements of confidentiality, integrity and availability (reliability) should be assessed and built in to protocols as appropriate, not added-on
  - Encrypted encapsulation should only be used when appropriate and does not solve everything
5. All devices must be capable of maintaining their security policy on an untrusted network
  - A “security policy” defines the rules with regard to the protection of the asset
  - Rules must be complete with respect to an arbitrary context
  - Any implementation must be capable of surviving on the raw Internet, e.g., will not break on any input

Always refer to [www.jerichoforum.org](http://www.jerichoforum.org) to ensure you have the latest version

Version 1.0 April 2000

Break

- Break
- Resume at 10.45pm

# Real world application

- **Protocols**
- **Paul Simmonds**  
*ICI plc.*  
*& Jericho Forum Board*

# Problem

- Image an enterprise where;
  - You have full control over its network
  - No external connections or communication
    - No Internet
    - No e-mail
    - No connections to third-parties
  - Any visitors to the enterprise have no ability to access the network
  - All users are properly managed and they abide by enterprise rules with regard to information management and security

# Problem

- In the real world nearly every enterprise;
  - Uses computers regularly connected to the Internet; Web connections, E-mail, IM etc.
  - Employing wireless communications internally
  - The majority of their users connecting to services outside the enterprise perimeter
- In this de-perimeterised world the use of inherently secure protocols is essential to provide protection from the insecure data transport environment.

# Why should I care?

- The Internet is insecure, and always will be
- It doesn't matter what infrastructure you have, it is inherently insecure
- However, enterprises now wish;
  - Direct application to application integration
  - To support just-in-time delivery
  - To continue to use the Internet as the basic transport medium.
- Secure protocols should act as fundamental building blocks for secure distributed systems
  - Adaptable to the needs of applications
  - While adhering to requirements for security, trust and performance.

# Secure Protocols

- New protocols are enabling secure application to application communication over the Internet
- Business-to-business protocols; more specifically ERP system-to-ERP system protocols that include the required end-entity authentication and security to provide the desired trust level for the transactions
- They take into account the context, trust level and risk.



## Recommendation/Solution

- While there may be some situations where open and insecure protocols are appropriate (public facing “information” web sites for example)
- All non-public information should be transmitted using appropriately secure protocols that integrate closely with each application.

# Protocol Security & Attributes

- Protocols used should have the appropriate level of data security, and authentication
- The use of a protective security wrapper (or shell) around an application protocol may be applicable;
- However the use of an encrypted tunnel negates most inspection and protection and should be avoided in the long term.

# The need for open standards

- The Internet uses insecure protocols
  - They are de-facto lowest common denominator standards
  - But are open and free for use
- If all systems are to interoperate – regardless of Operating System or manufacturer and be adopted in a timely manner then it is essential that protocols must be open and remain royalty free.

## Secure “out of the box”

- An inherently secure protocol is;
  - Authenticated
  - Protected against unauthorised reading/writing
  - Has guaranteed integrity
- For inherently secure protocols to be adopted then it is essential that;
  - Systems start being delivered preferably only supporting inherently secure protocols; or
  - With the inherently secure protocols as the default option

# Proprietary Solutions

- Vendors are starting to offer hybrid protocol solutions that support
  - multiple security policies
  - system/application integration
  - degrees of trust between organisations and communicating parties (their own personnel, customers, suppliers etc.)
- Resulting in proprietary solutions that are unlikely to interoperate, and whose security may be difficult to verify
- Important to classify the various solutions an organisation uses or is contemplating.

# Challenges to the industry

1. If inherently secure protocols are to become adopted as standards then they must be open and interoperable (JFC#3)
2. The Jericho Forum believes that companies should pledge support for making their proprietary protocols fully open, royalty free, and documented
3. The Jericho Forum favours the release of protocol reference implementations under a suitable open source or GPL arrangement
4. The Jericho Forum hopes that all companies will review its products and the protocols and move swiftly to replacing the use of appropriate protocols
5. End users should demand full disclosure of protocols in use as part of any purchase
6. End users should demand that all protocols should be inherently secure
7. End users should demand that all protocols used should be fully open

# Good & Bad Protocols

Secure	<p><b>Point Solution (use with care)</b></p> <ul style="list-style-type: none"> <li>AD Authentication</li> <li>COM</li> </ul>	<p><b>Use &amp; Recommend</b></p> <ul style="list-style-type: none"> <li>SMTP</li> <li>TELNET</li> <li>SSH</li> <li>Kerberos</li> </ul>
	<p><b>Never Use (Retire)</b></p> <ul style="list-style-type: none"> <li>NTLM Authentication</li> </ul>	<p><b>Use only with additional security</b></p> <ul style="list-style-type: none"> <li>SMTP</li> <li>FTP</li> <li>TFTP</li> <li>Telnet</li> <li>VoIP</li> <li>IMAP</li> <li>POP</li> <li>SMB</li> <li>SNMP</li> <li>NFS</li> </ul>
	<b>Closed</b>	<b>Open</b>

# Implementing new systems

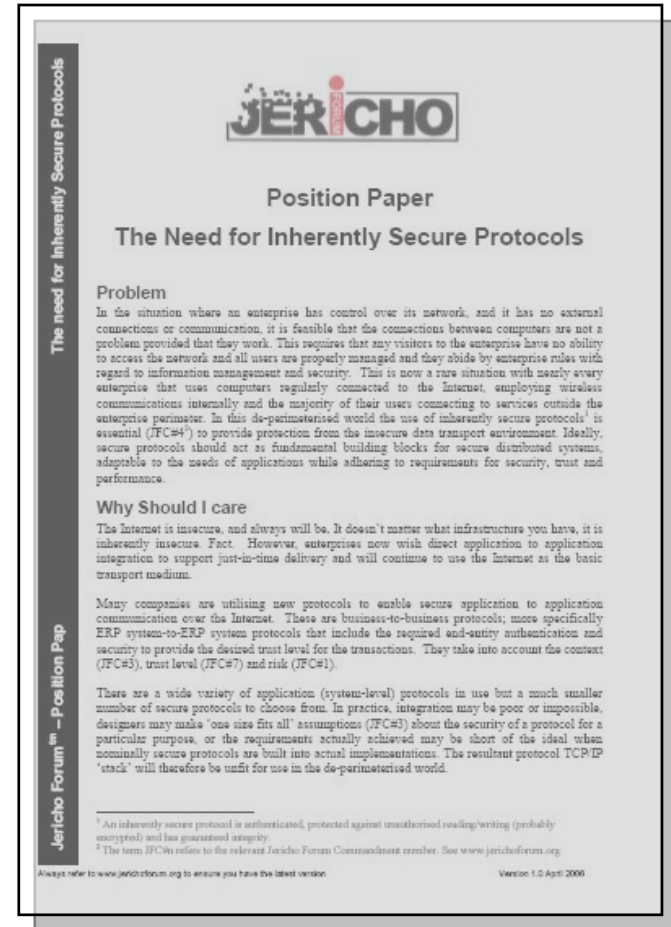
- New systems should only be introduced that either have
  - All protocols that operate in the Open/Secure quadrant; or
  - Operate in the Open/Insecure on the basis that anonymous unauthenticated access is the desired mode of operation.



# Paper available from the Jericho Forum

- The Jericho Forum Position Paper “The need for Inherently Secure Protocols” is freely available from the Jericho Forum website

<http://www.jerichoforum.org>



# Real world application

- **Voice over IP**
- **David McCaskill**  
*Procter & Gamble*  
*& Jericho Forum Board*

# The Business View of VoIP

- It's cheap?
  - Cost of phones
  - Cost of "support"
  - Impact on internal network bandwidth
- It's easy?
  - Can you rely on it?
  - Can you guarantee toll-bypass?
- It's sexy?
  - Desktop video

# The IT View of VoIP

- How do I manage bandwidth?
  - QoS, CoS
- How can I support it?
  - More stretch on a shrinking resource
- What happens if I lose the network?
  - I used to be able to trade on the phone
- How can I manage expectations?
  - Lots of hype; lots of “sexy”, unused/unusable tricks
- Can I make it secure??

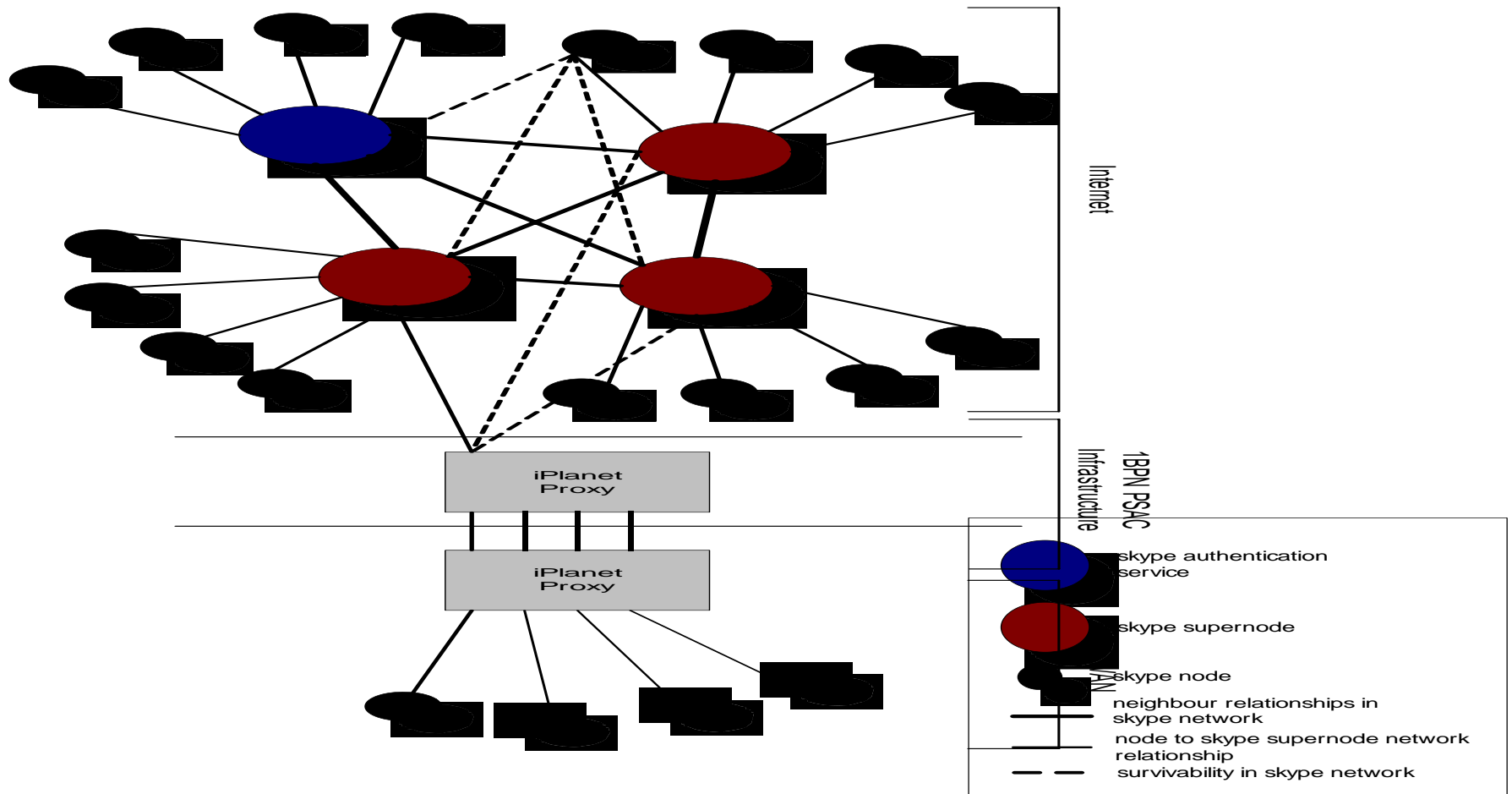
# The Reality of VoIP

- Not all VoIPs are equal!
- Internal VoIP
  - Restricted to your private address space
  - Equivalent to bandwidth diversion
- External VoIP
  - Expensive, integrated into PBX systems
- “Free” (external) VoIP (eg Skype)
  - Spreads (voice) data anywhere
  - Ignores network boundary
  - Uses proprietary protocols – at least for security

# The Security Problem

- Flawed assumption that voice & data sharing same infrastructure is acceptable
  - because internal network is secure (isn't it?)
- Therefore little or no security built-in
- Internal VoIP
  - Security entirely dependent on internal network
  - Very poor authentication
- External VoIP
  - Some proprietary security, even Skype
  - Still poor authentication
  - BUT, new insecurities

# VoIP Insecurity: An Example



## To Make Matters Worse.....

- Why would you just want internal VoIP?
- Think of flexibility?
  - Remote working; mobile working; customer calls
- Think of where the bulk of voice costs are?
- Think de-perimeterised
- Think Jericho!



# Recommended Solution/Response

- **STANDARDISATION!**
  - Allow diversity of phones (software, hardware), infrastructure components, infrastructure management, etc
- **MATURITY of security!**
  - All necessary functionality
  - Open secure protocol
    - Eg crypto
    - Eg IP stack protection

## Secure “Out of the Box”

- Challenge is secure VoIP without boundaries
- Therefore...
  - All components must be secure out of box
  - Must be capable of withstanding attack
  - “Phones” must be remotely & securely maintained
  - Must have strong (flexible) mutual authentication
  - “Phones” must filter/ignore extraneous protocols
  - Protocol must allow for “phone” security mgt
  - Must allow for (flexible) data encryption
  - Must allow for IP stack identification & protection

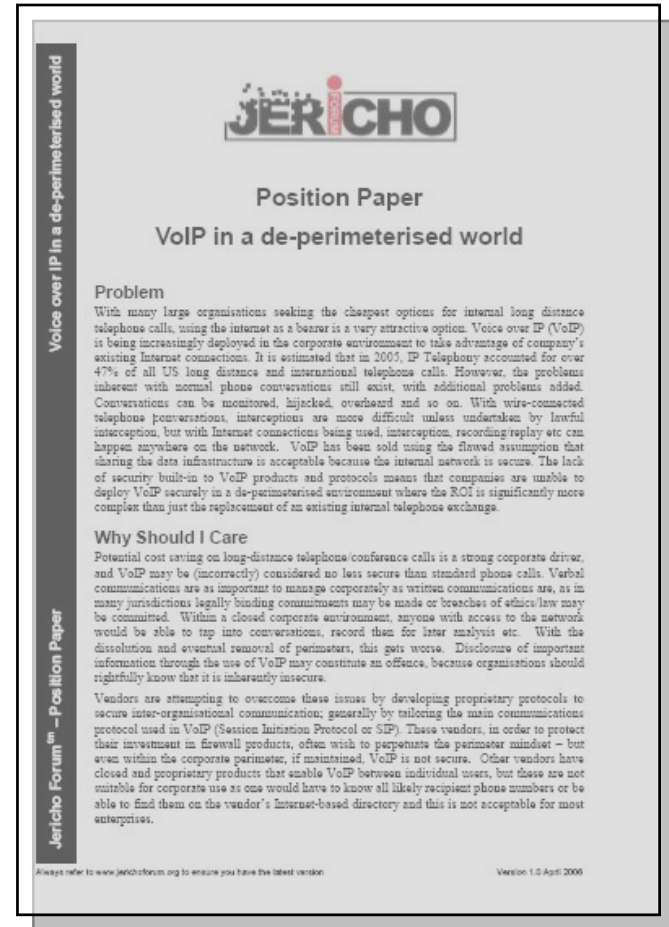
# Challenges to the industry

1. If inherently secure VoIP protocols are to become adopted as standards then they must be open and interoperable
2. The Jericho Forum believes that companies should pledge support for moving from proprietary VoIP protocols to fully open, royalty free, and documented standards
3. The secure VoIP protocol reference implementation should be released under a suitable open source license.
4. The Jericho Forum hopes that all companies will review its products and the protocols and move swiftly to include the use of inherently secure VoIP protocols.
5. End users should demand that VoIP protocols should be inherently secure
6. End users should demand that VoIP protocols used should be fully open

# Paper available from the Jericho Forum

- The Jericho Forum Position Paper “VoIP in a de-perimeterised world” is freely available from the Jericho Forum website

<http://www.jerichoforum.org>

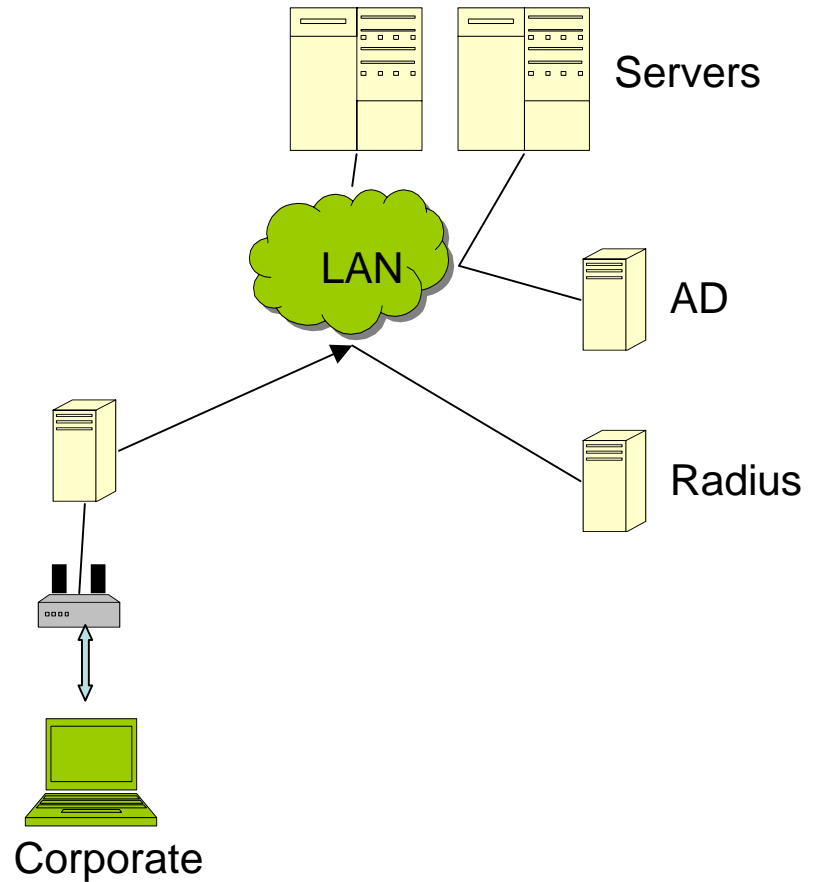


# Real world application

- **Corporate Wireless Networking**
- **Paul Simmonds**  
*ICI plc.*  
*& Jericho Forum Board*

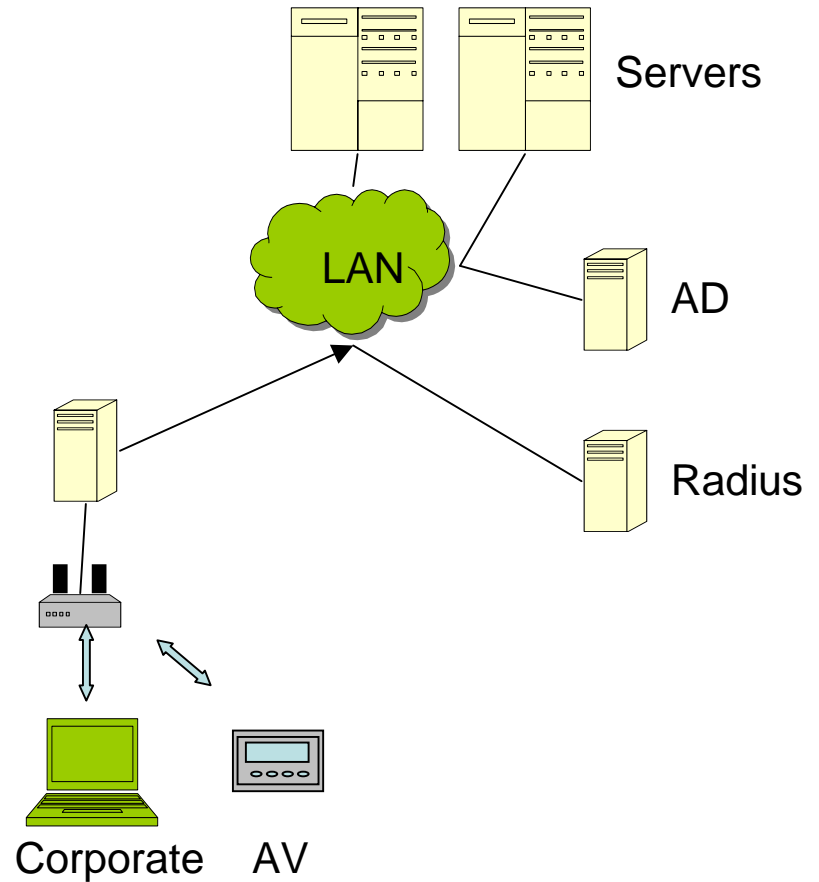
# Secure wireless connection to LAN

- Corporate laptops
- Use 802.11i (WPA2)
- Secure authenticated connection to LAN
- Device + user credentials
- Simple?



# Not just laptops

- But also...
- Audio-visual controllers
- Wi-Fi phones



# Blinkenlights?

- Play <Pong> with mobile phone!



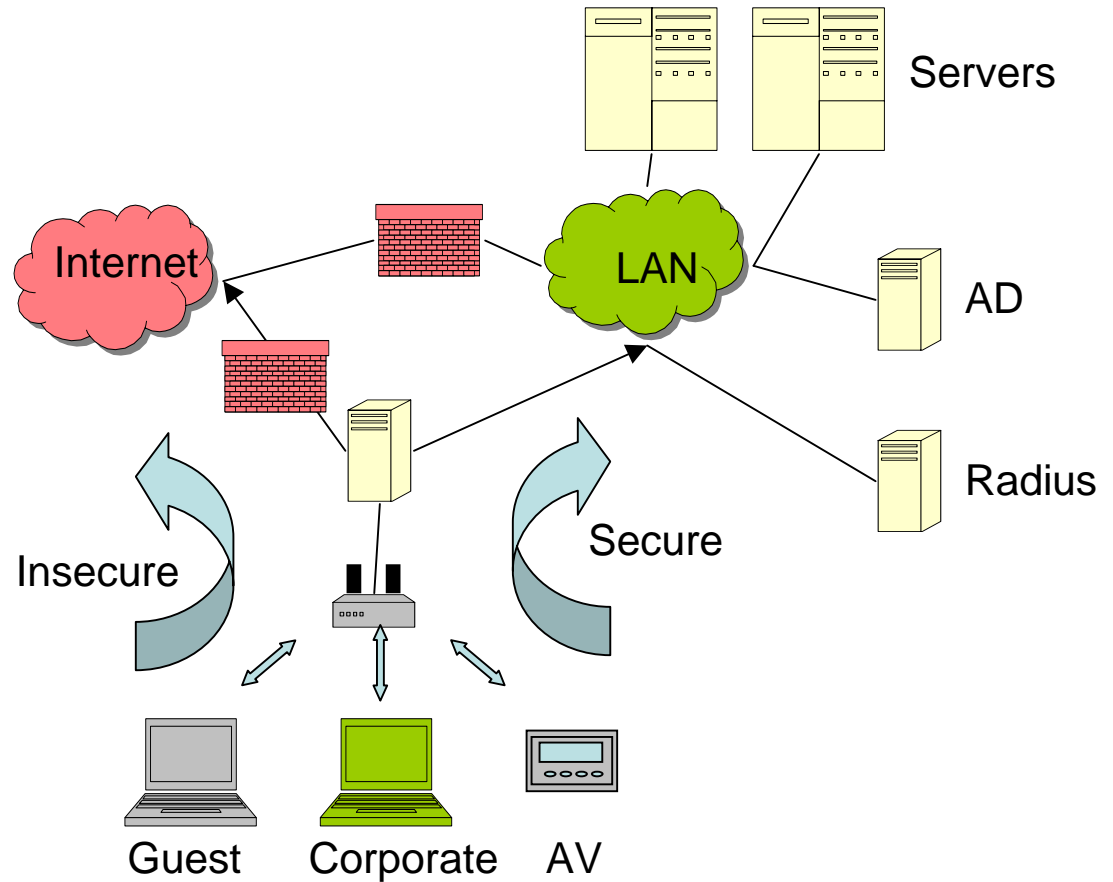
Photo: Dorit Günter, Nadja Hannaske



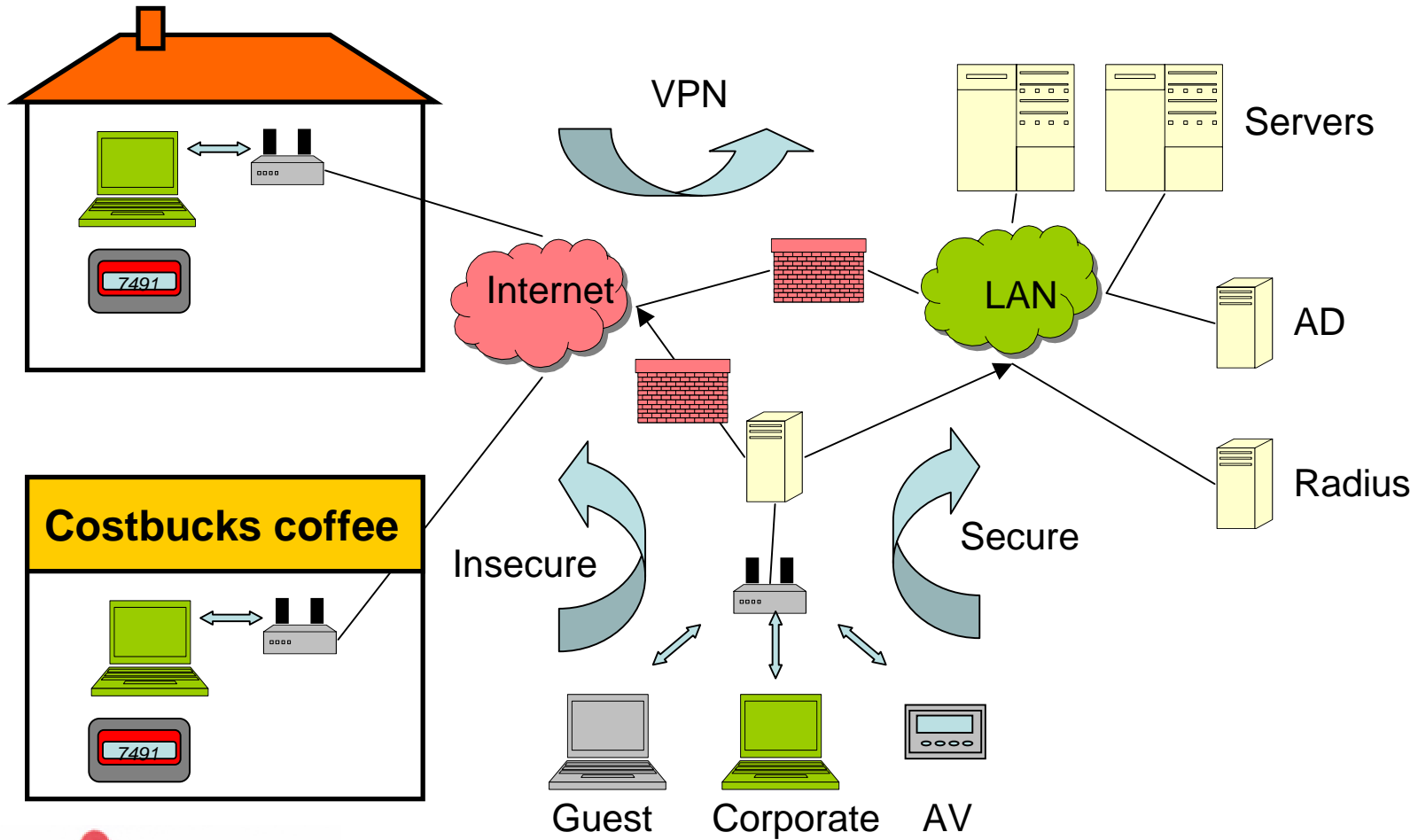


# Guest internet access too

- Mixed traffic
- Trusted or untrusted?
- How segregated?



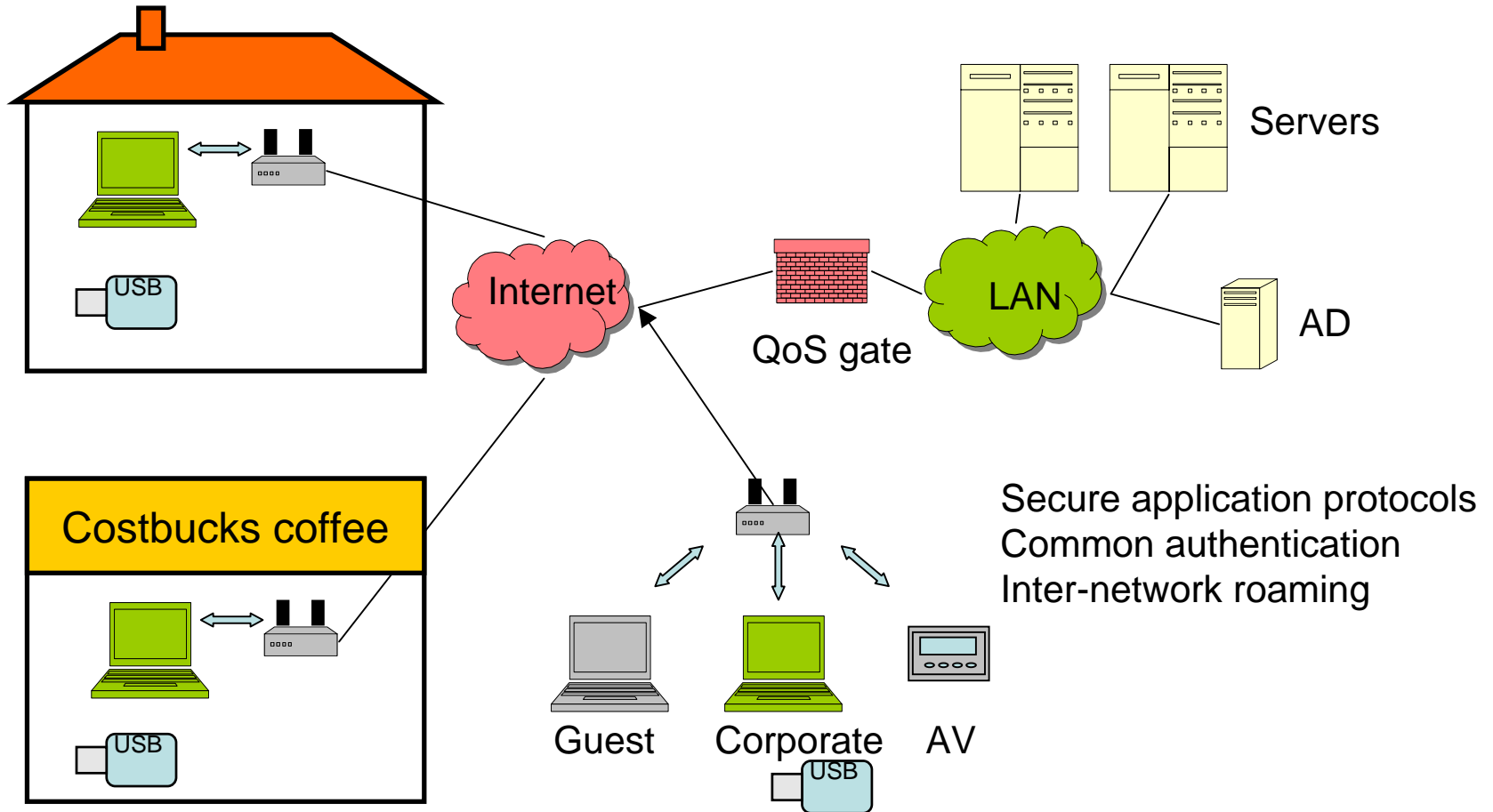
# Laptops also used at home or in café



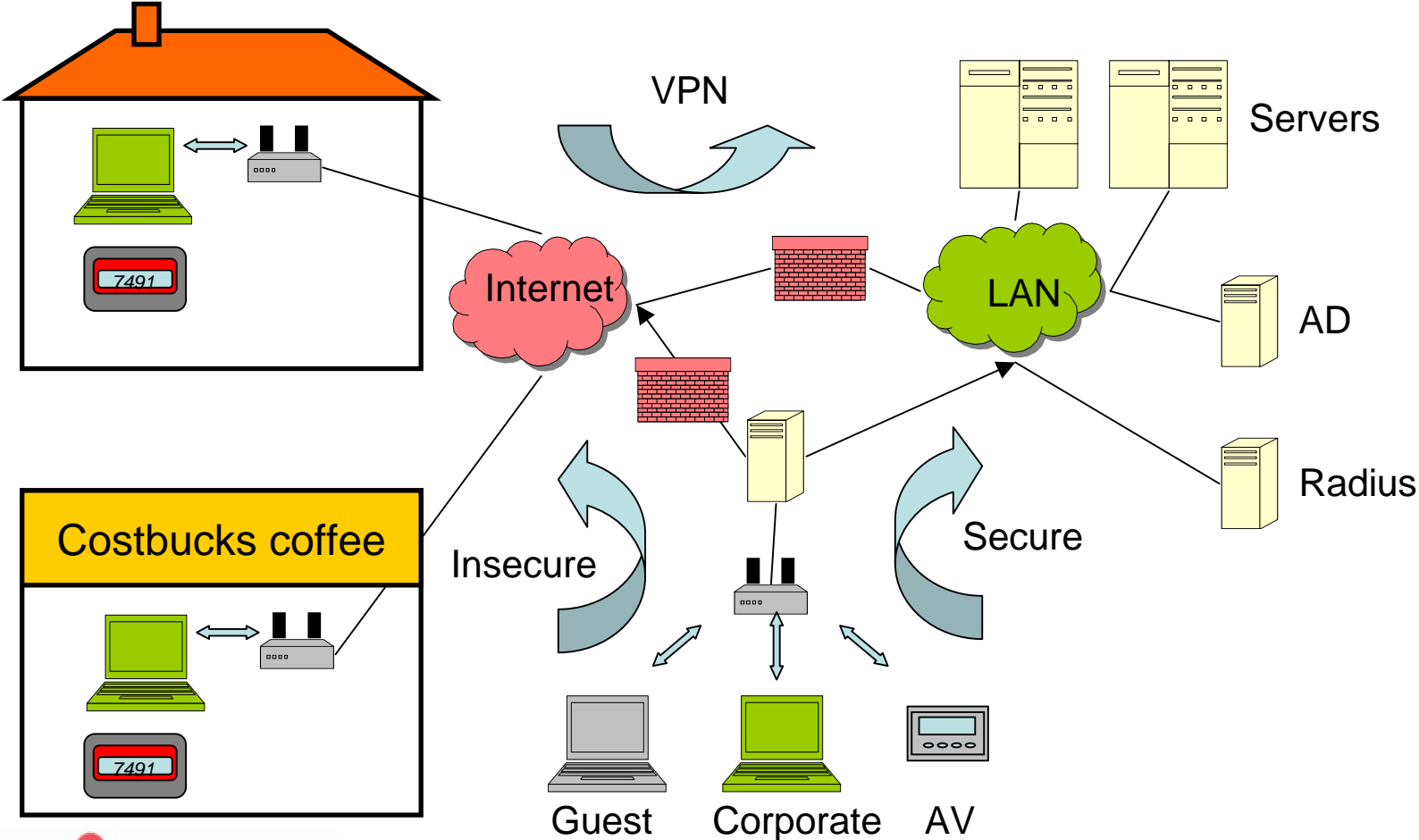
# Security complexity

- Need location awareness
- 802.11i if corporate wireless link
- VPN if not corporate
- Still not perfect security, insecure connections needed to set up café/home connections
- Security on direct connections too

# Jericho visions



# Today's complexity



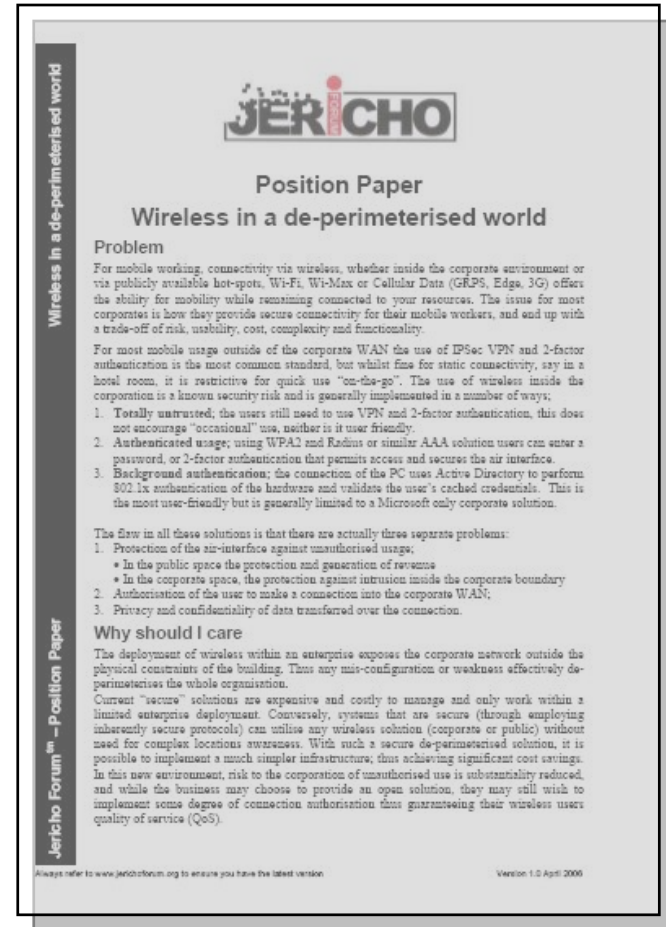
# Challenges to the industry

1. Companies should regard wireless security on the air-interface as a stop-gap measure until inherently secure protocols are widely available
2. The use of 802.1x integration to corporate authentication mechanisms should be the out-of-the-box default for all Wi-Fi infrastructure
3. Companies should adopt an “any-IP address, anytime, anywhere” (what Europeans refer to as a “Martini-model”) approach to remote and wireless connectivity.
4. Provision of full roaming mobility solutions that allow seamless transition between connection providers

# Paper available from the Jericho Forum

- The Jericho Forum Position Paper “Wireless in a de-perimeterised world” is freely available from the Jericho Forum website

<http://www.jerichoforum.org>



# Case Study

- **What Hath Vint Wrought**

- **Steve Whitlock**

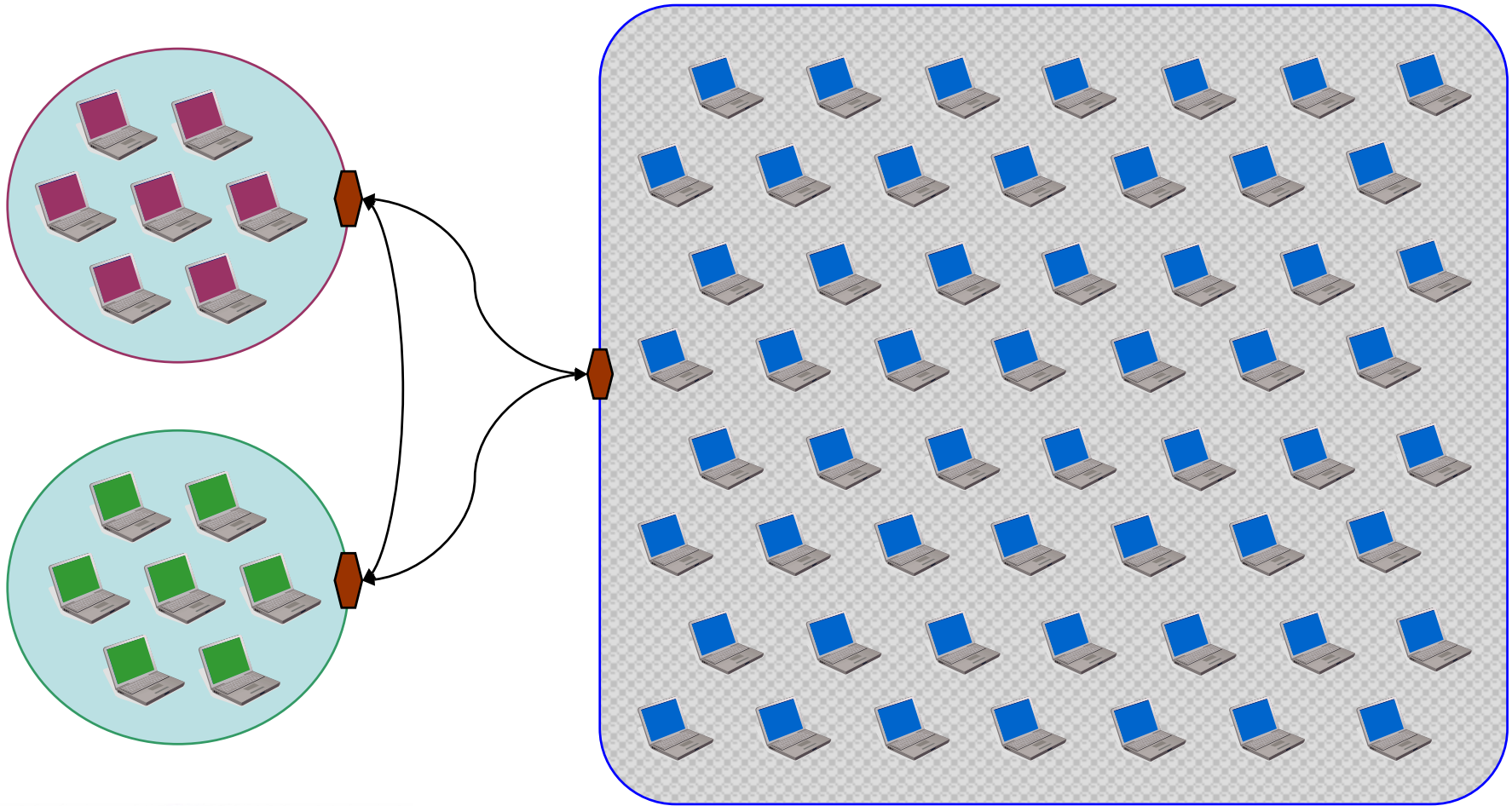
*Boeing*

*Chief Security Architect*

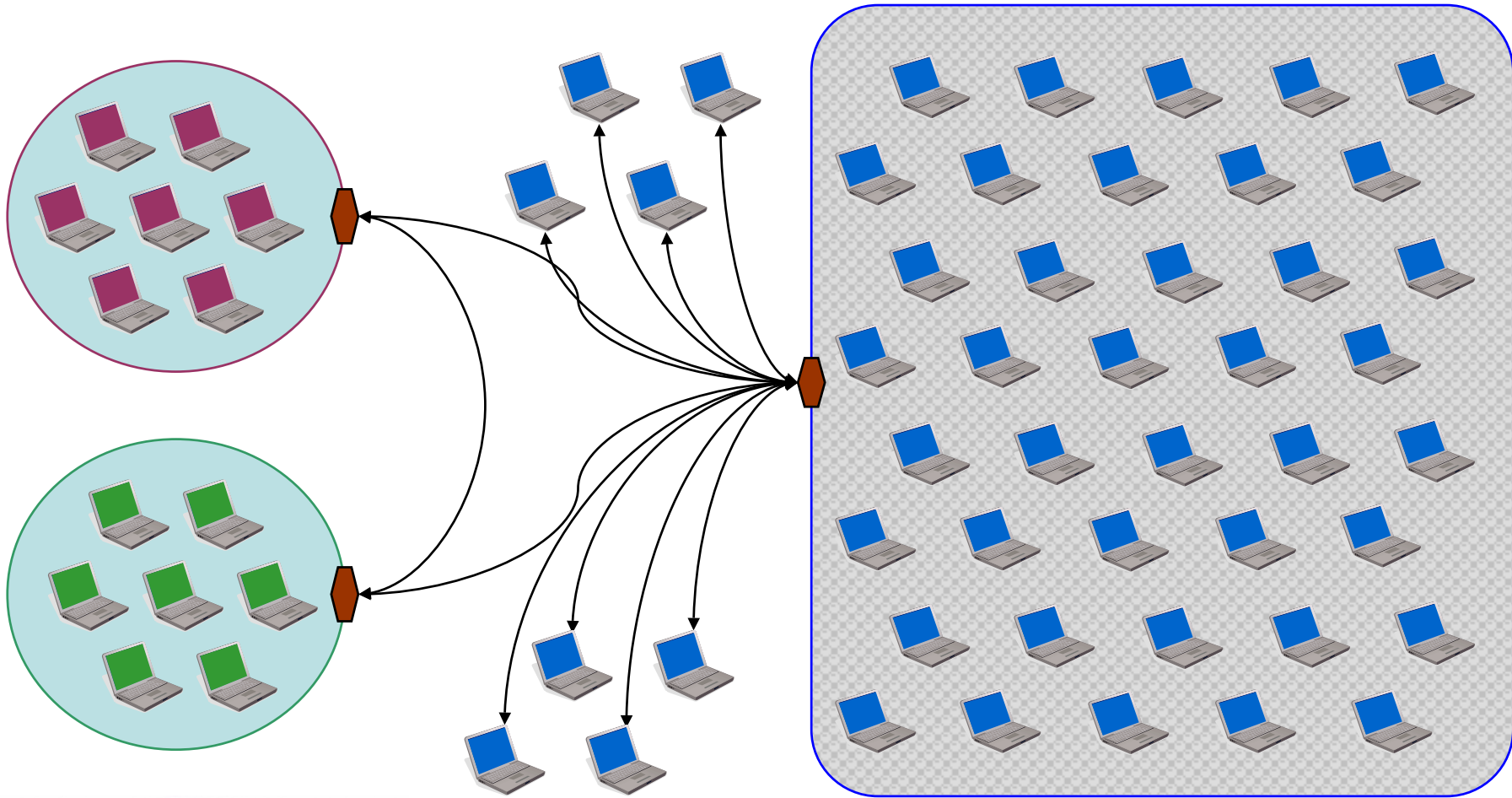
*Information Protection & Assurance*



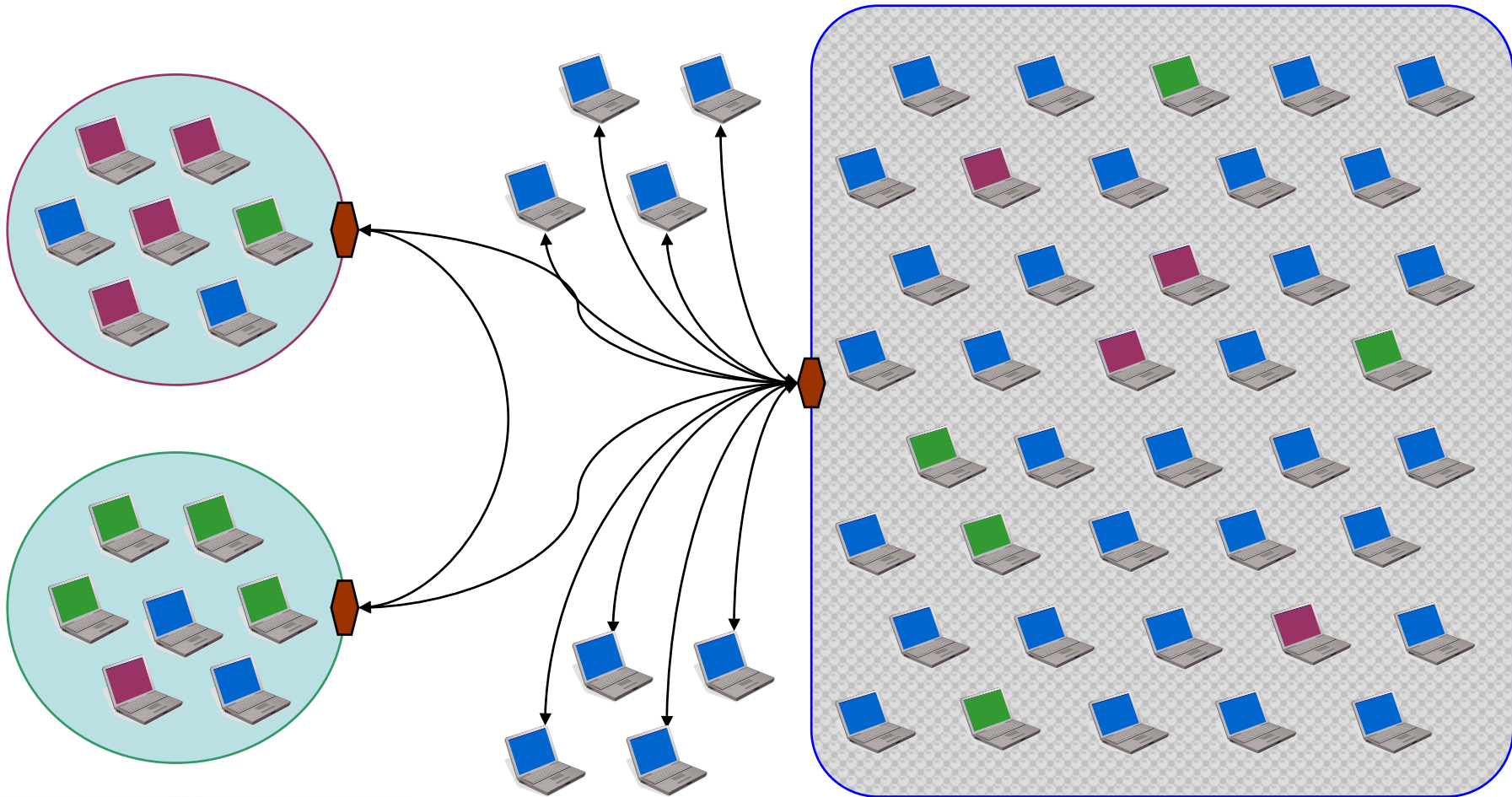
# Prehistoric E-Business



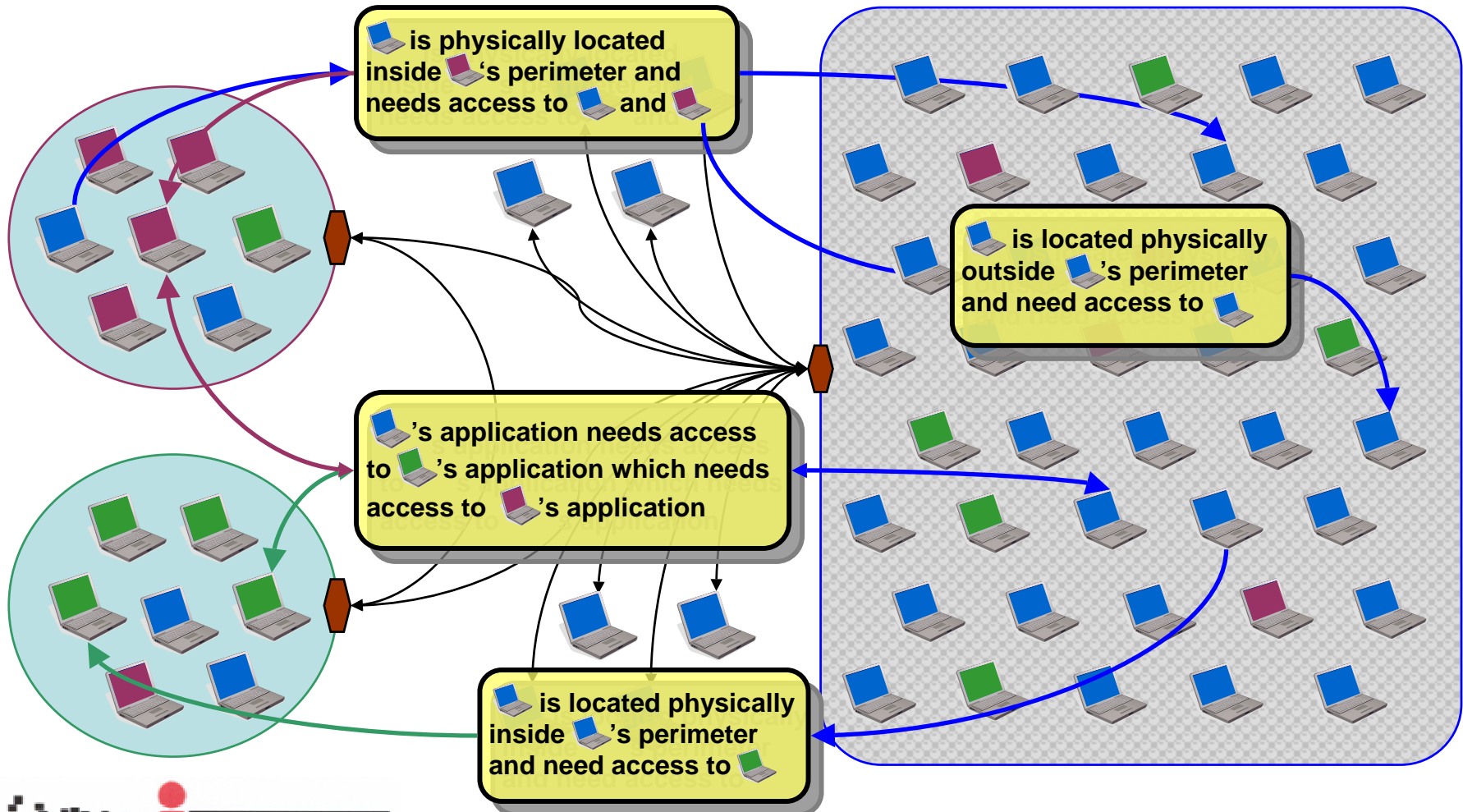
# Employees moved out...



# Associates moved in...



# The Globalization Effect



# De-perimeterisation

- **De-perimeterisation...**

- ... is not a security strategy

- ... is a consequence of globalisation by cooperating enterprises

- **Specifically**

- Inter-enterprise access to complex applications

- Virtualisation of employee location

- On site access for non employees

- Direct access from external applications to internal application and data resources

- Enterprise to enterprise web services

- **The current security approach will change:**

- Reinforce the Defence-In-Depth and Least Privilege security principles

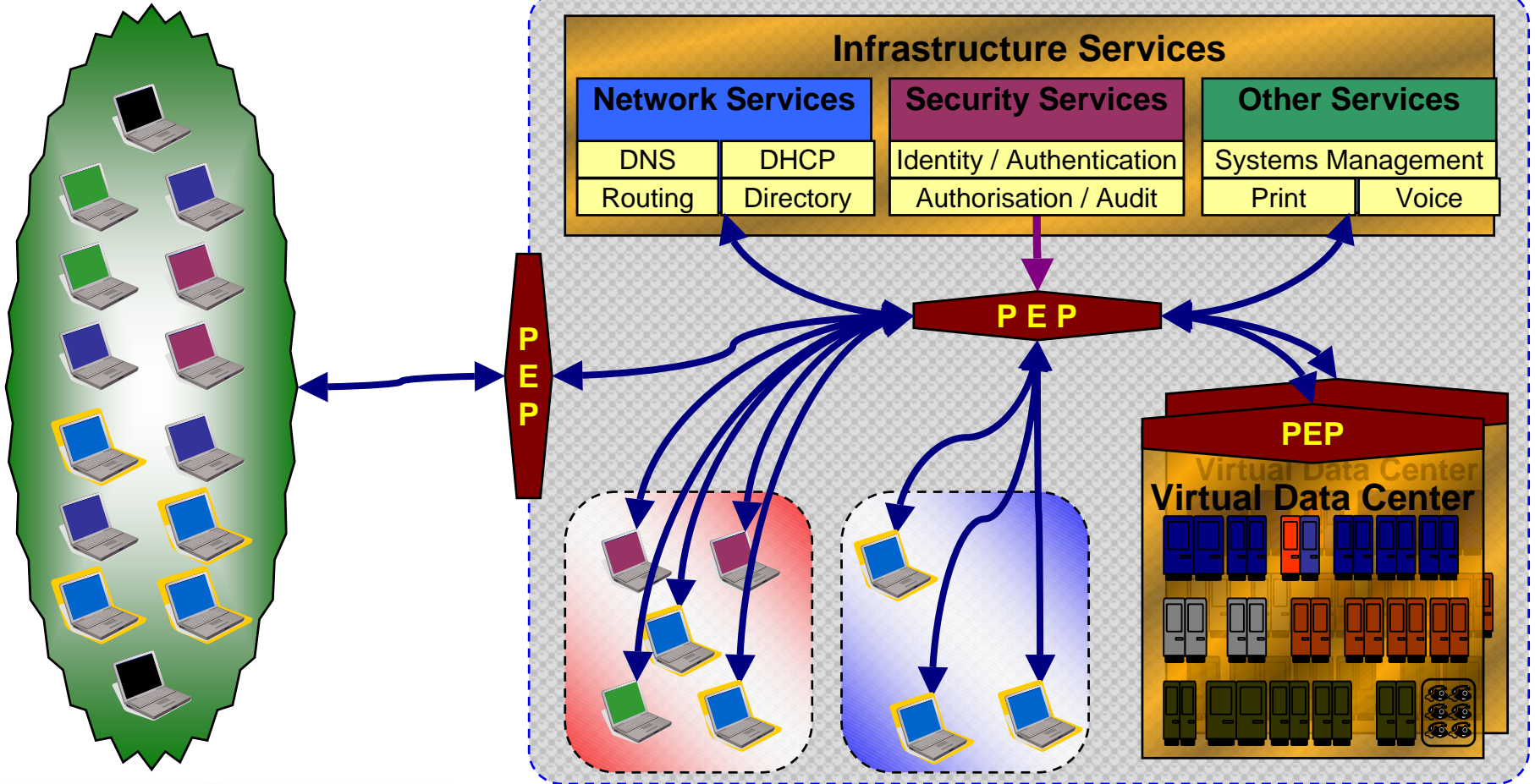
- Perimeter security emphasis will shift towards supporting resource availability

- Access controls will move towards resources

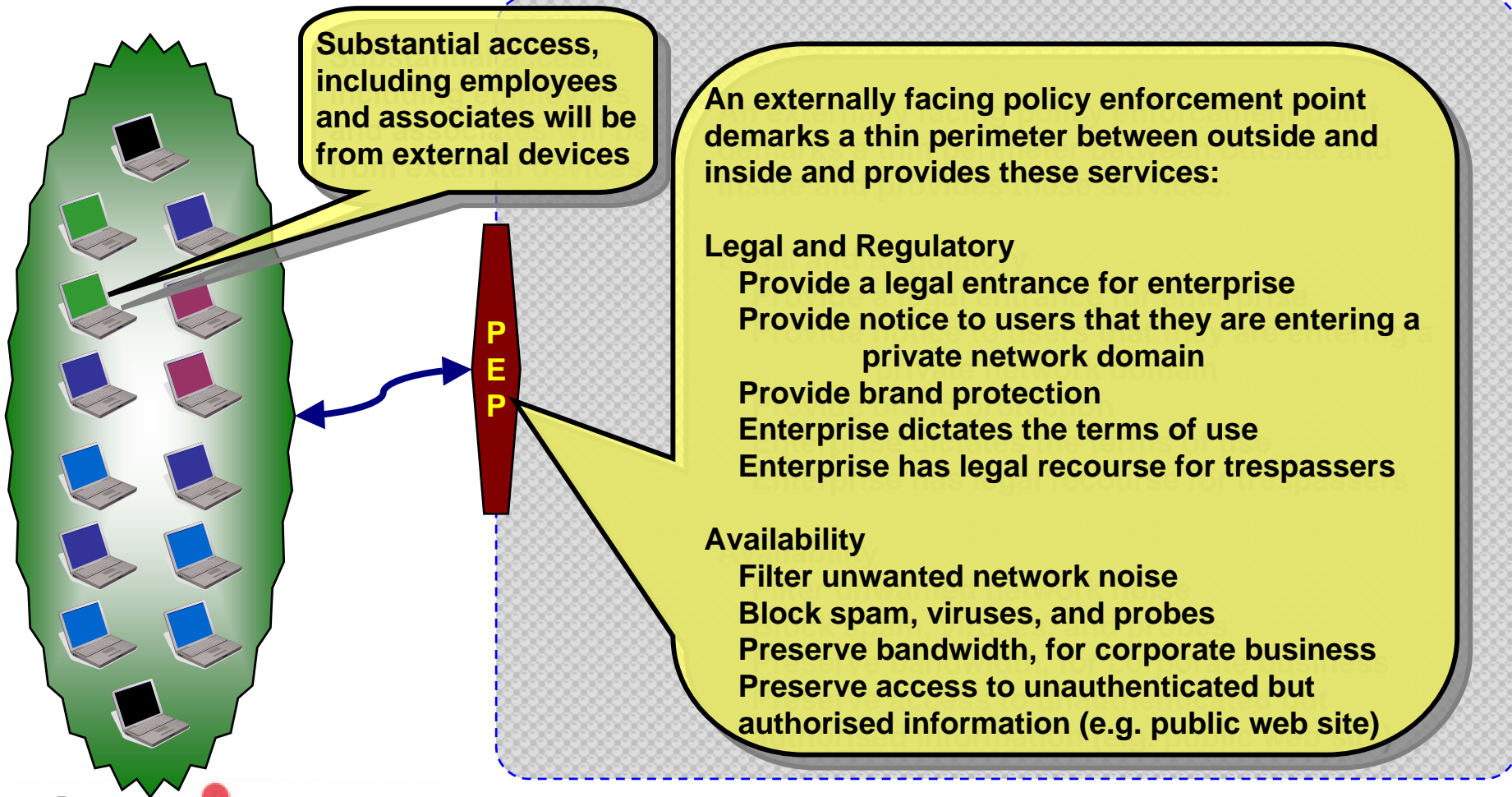
- Data will be protected independent of location



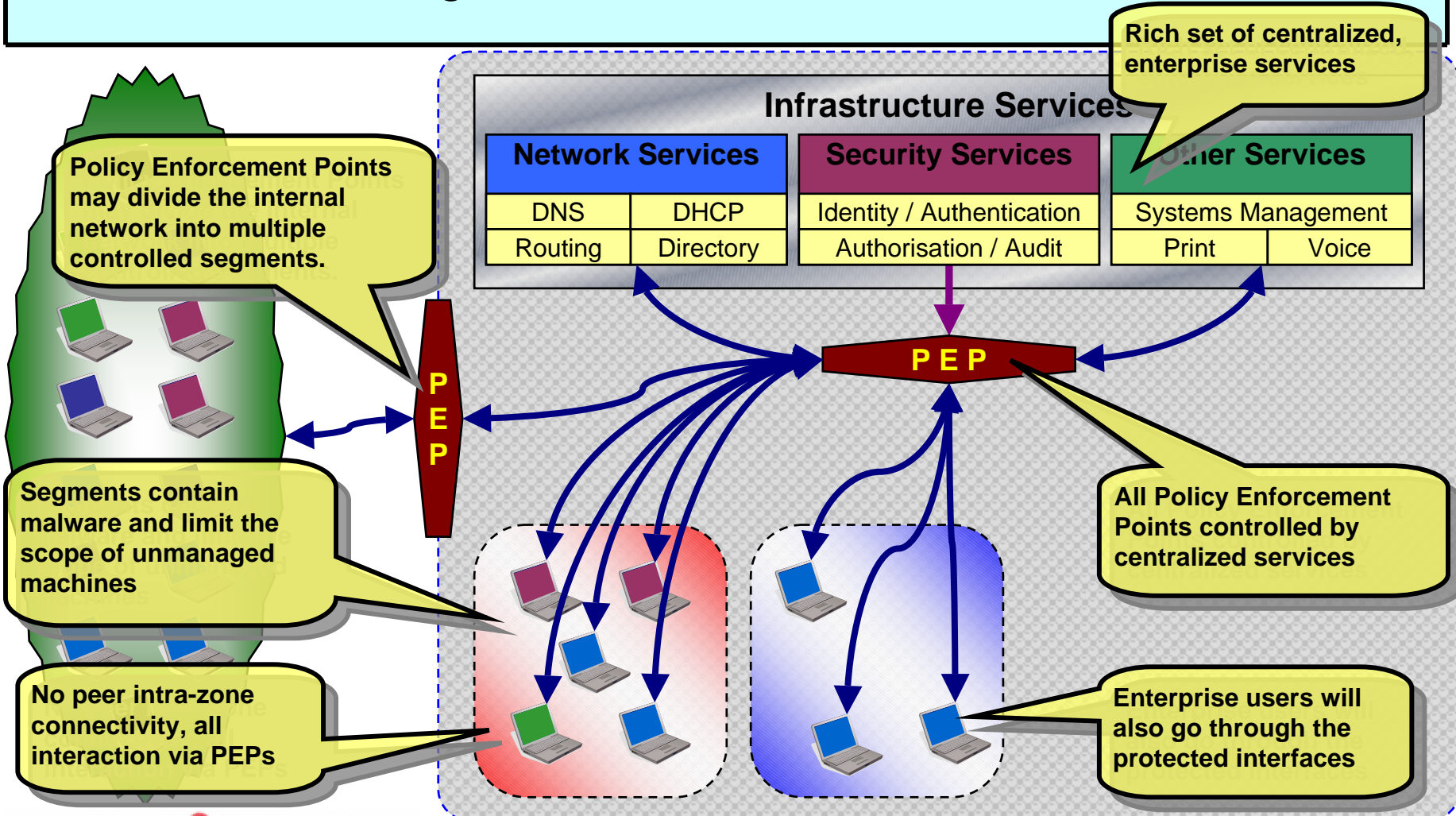
# Restoring Layered Services



# Defense Layer 1: Network Boundary

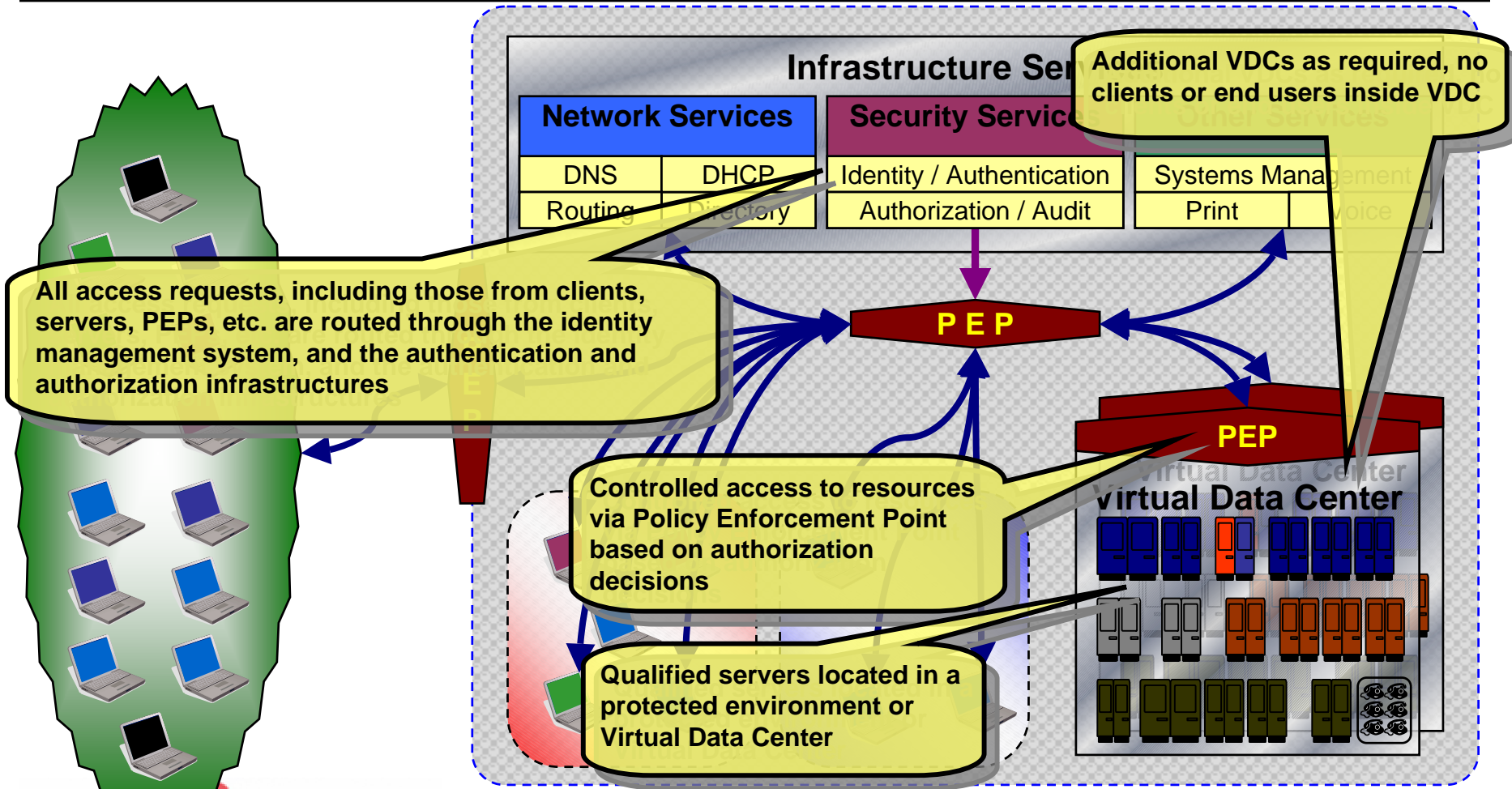


# Defense Layer 2: Network Access Control

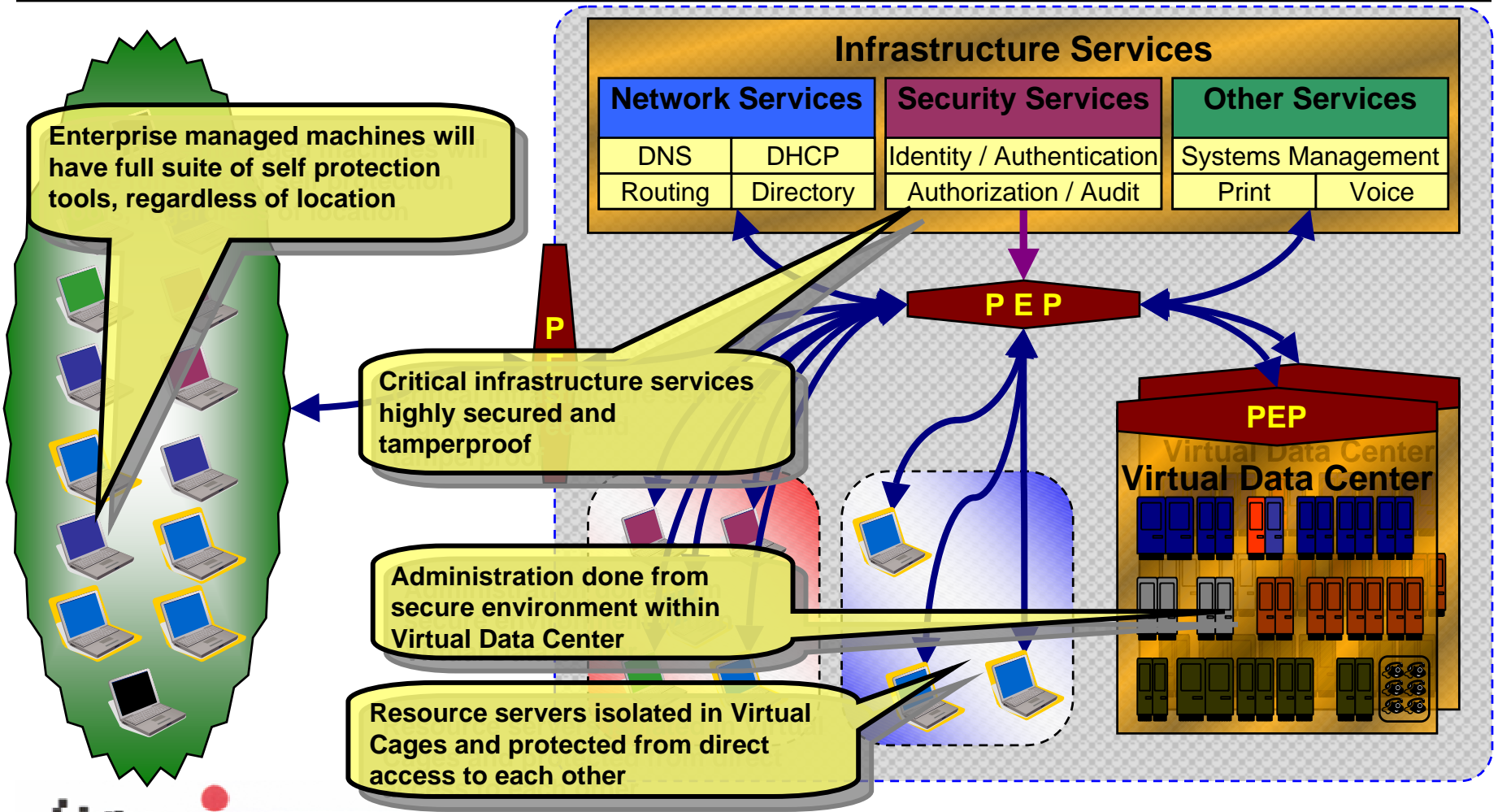




# Defense Layer 3: Resource Access Control

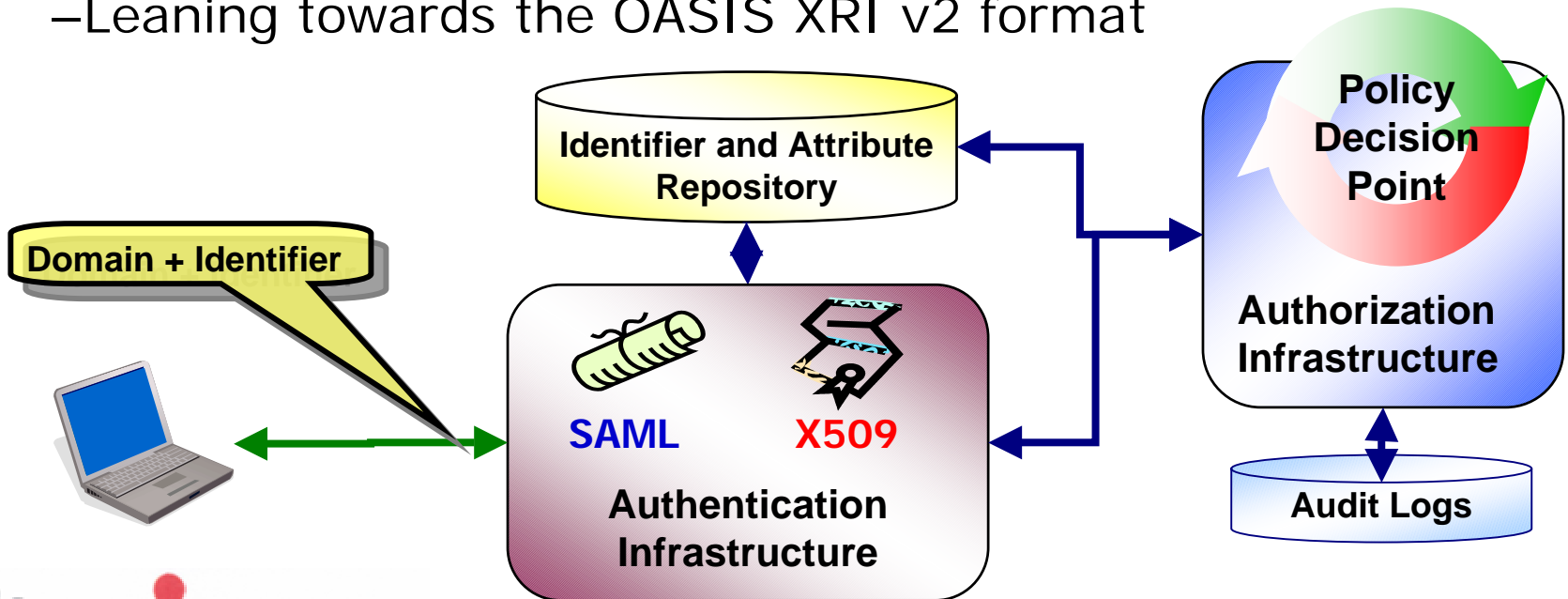


# Defense Layer 4: Resource Availability



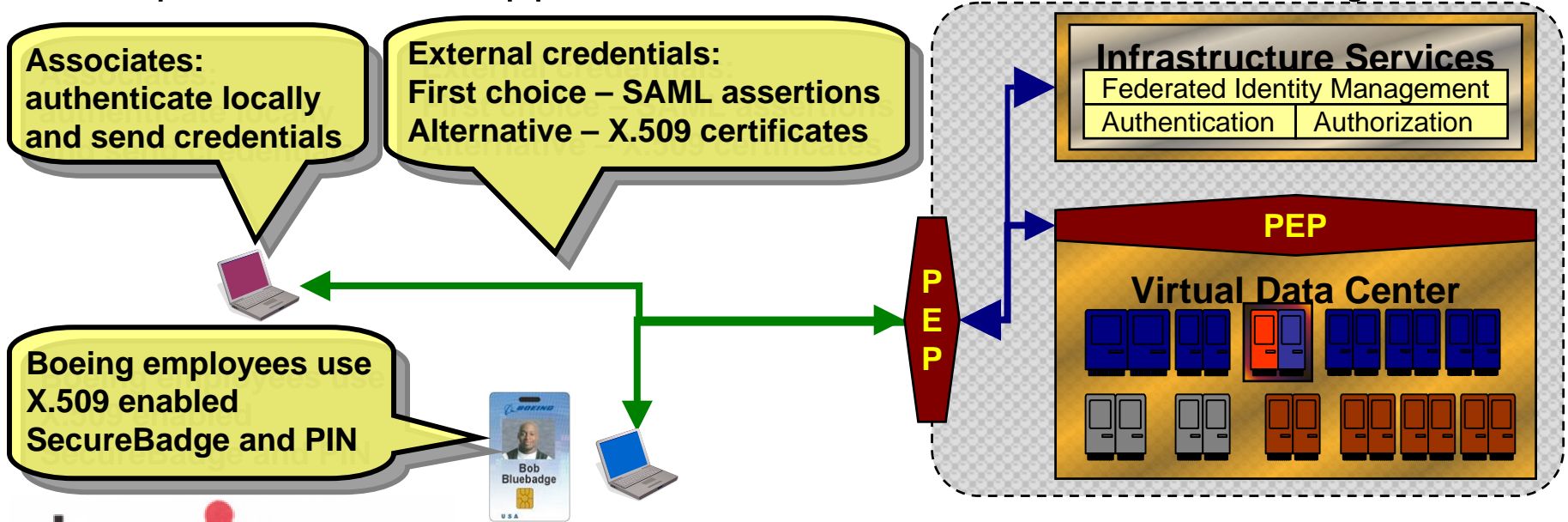
# Identity Management Infrastructure

- Migration to federated identities
- Support for more principal types – applications, machines and resources in addition to people.
- Working with DMTF, NAC, Open Group, TSCP, etc. to adopt a standard
  - Leaning towards the OASIS XRI v2 format



# Authentication Infrastructure

- Offer a suite of certificate based authentication services
- Cross certification efforts:
  - Cross-certify with the CertiPath Bridge CA
  - Cross-certify with the US Federal Bridge CA
  - Operate a DoD approved External Certificate Authority

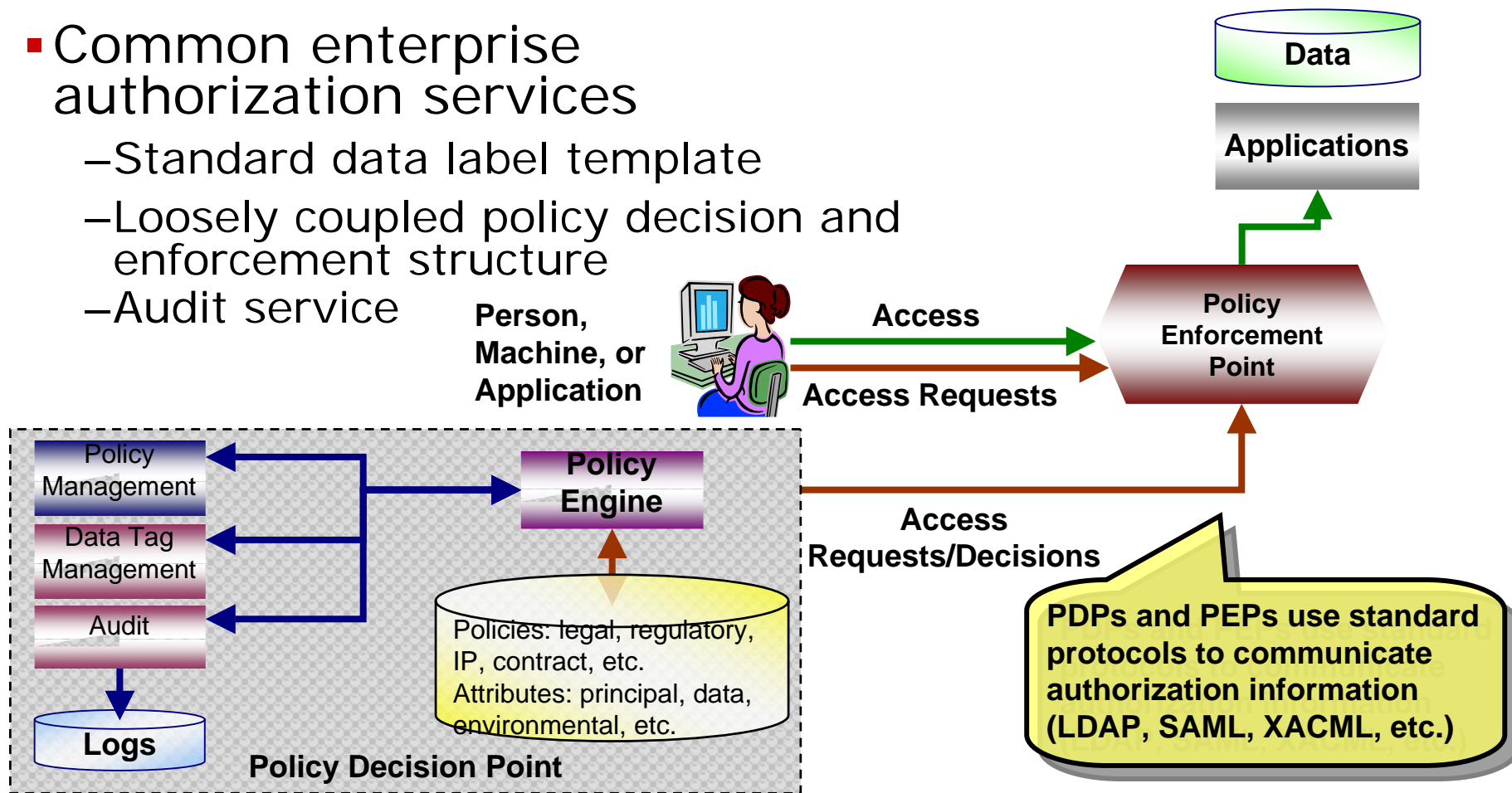




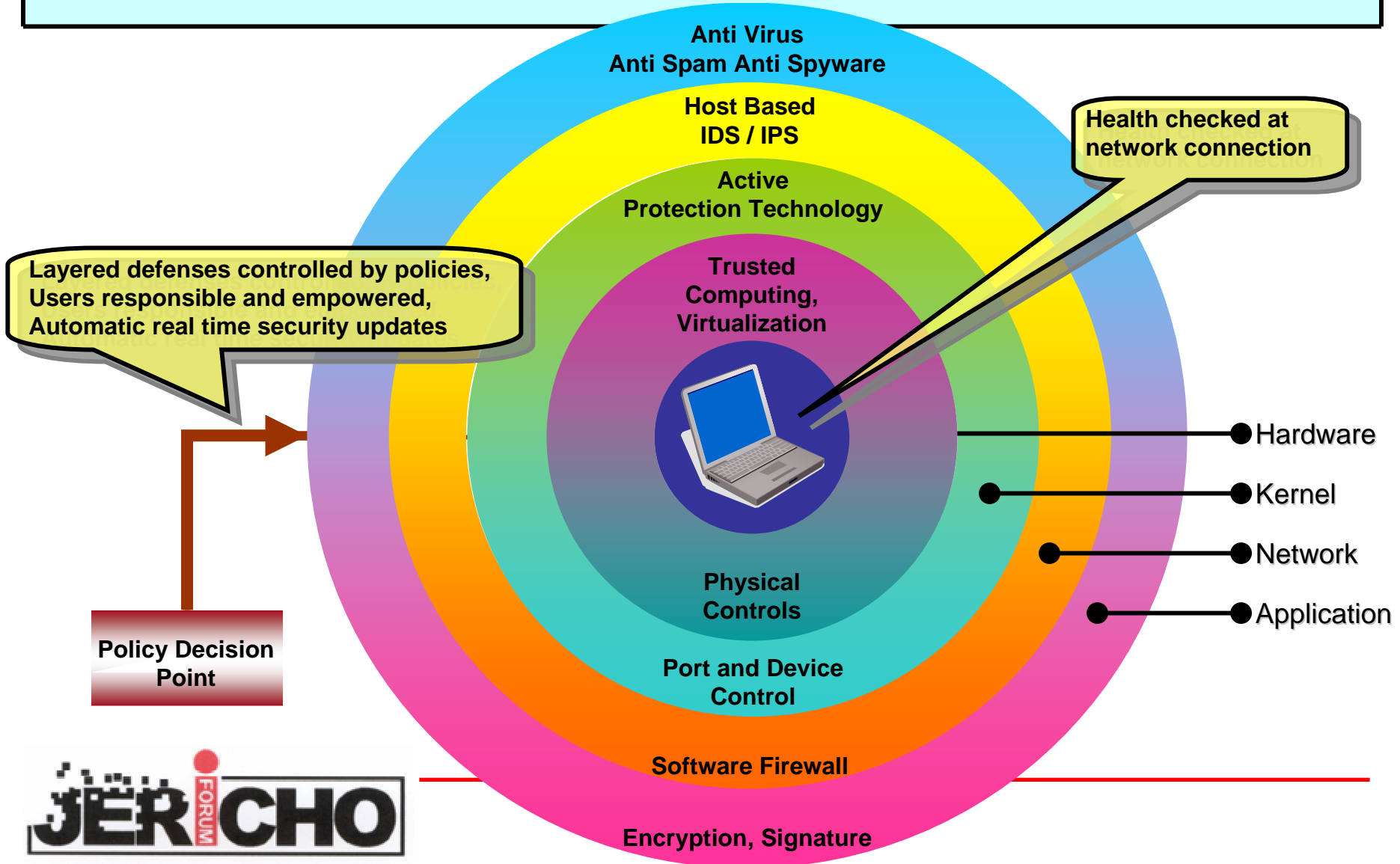
# Authorization Infrastructure

- Common enterprise authorization services

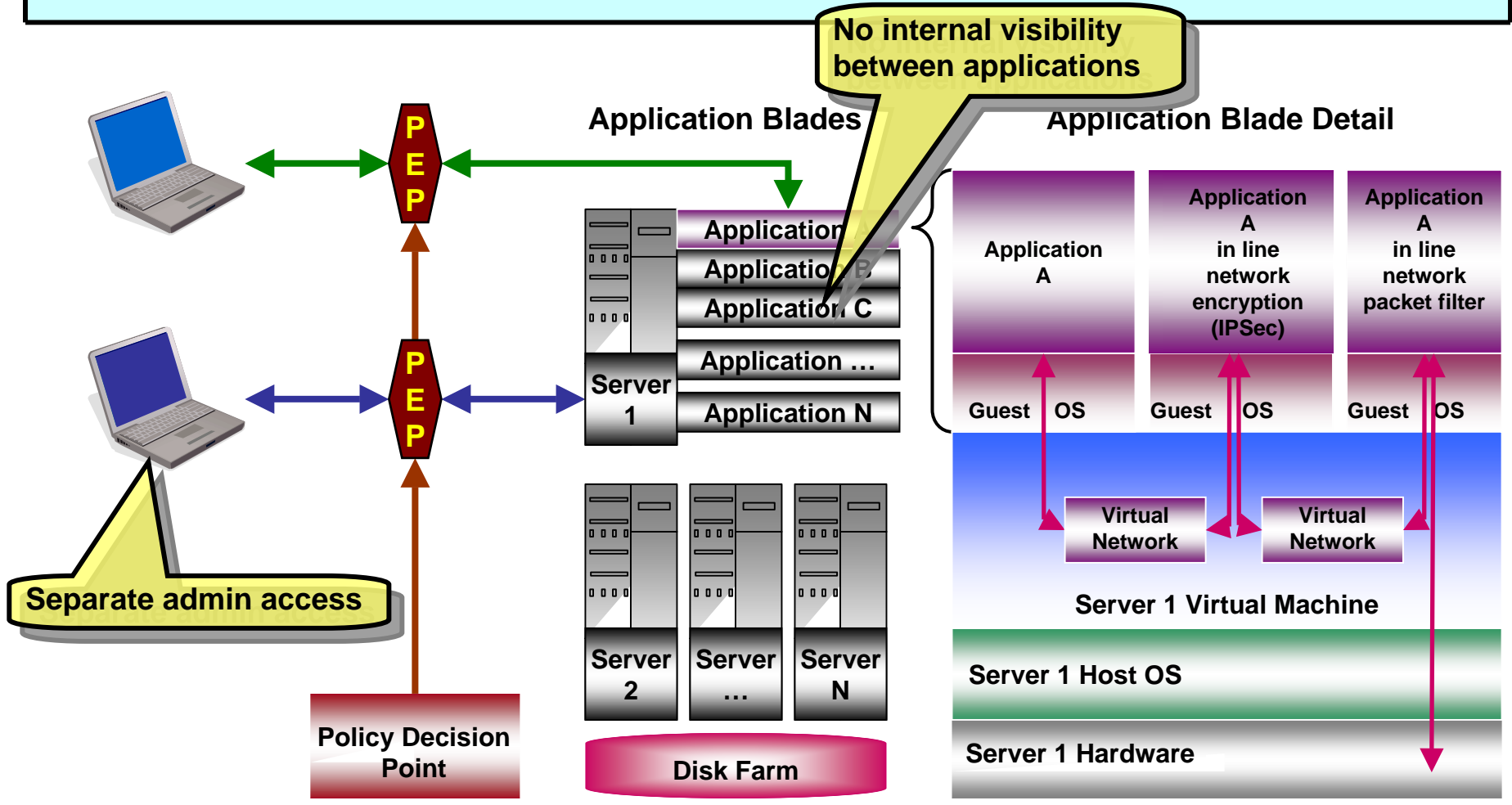
- Standard data label template
- Loosely coupled policy decision and enforcement structure
- Audit service



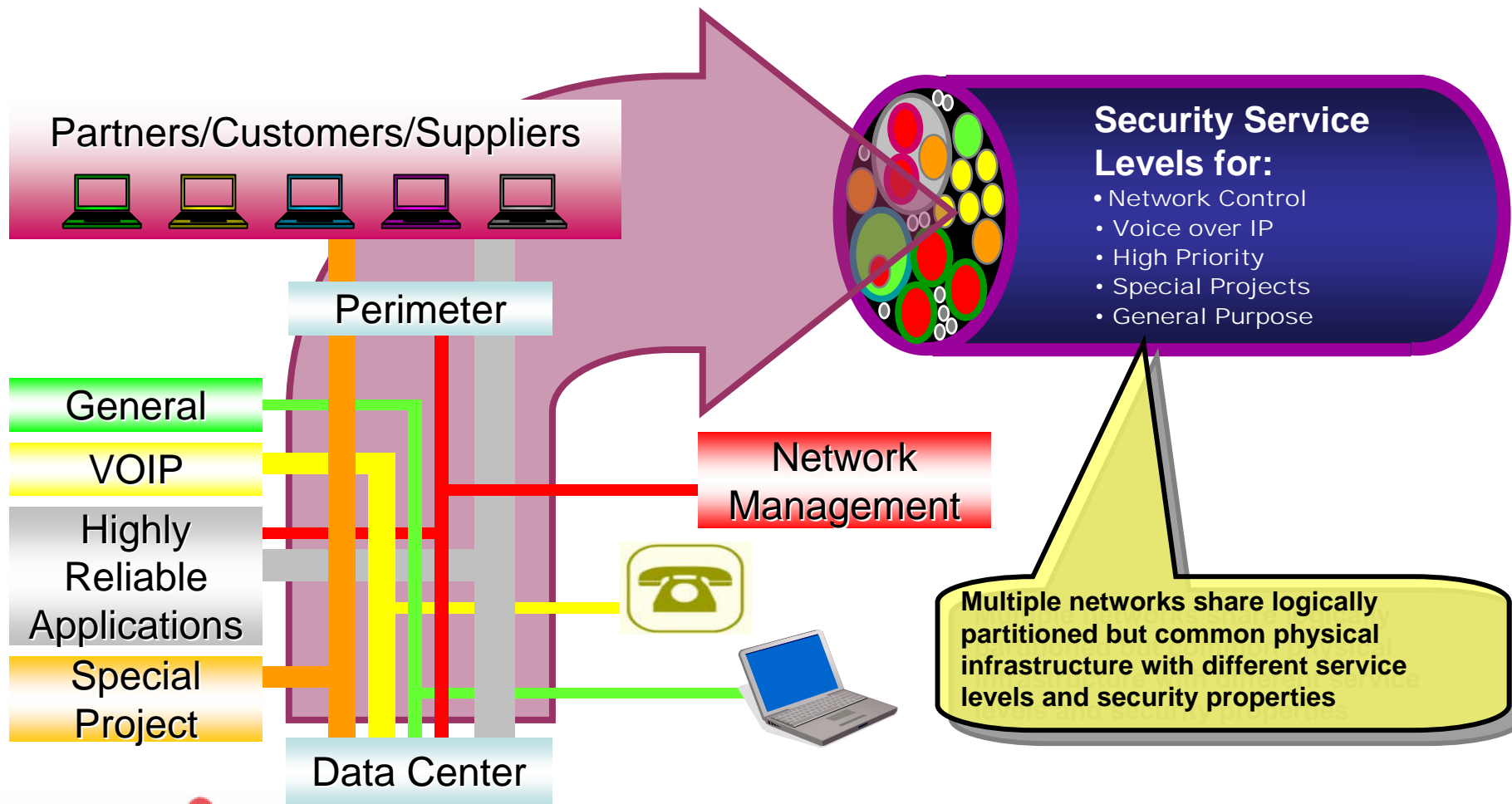
# Resource Availability: Desktop



# Resource Availability: Server / Application

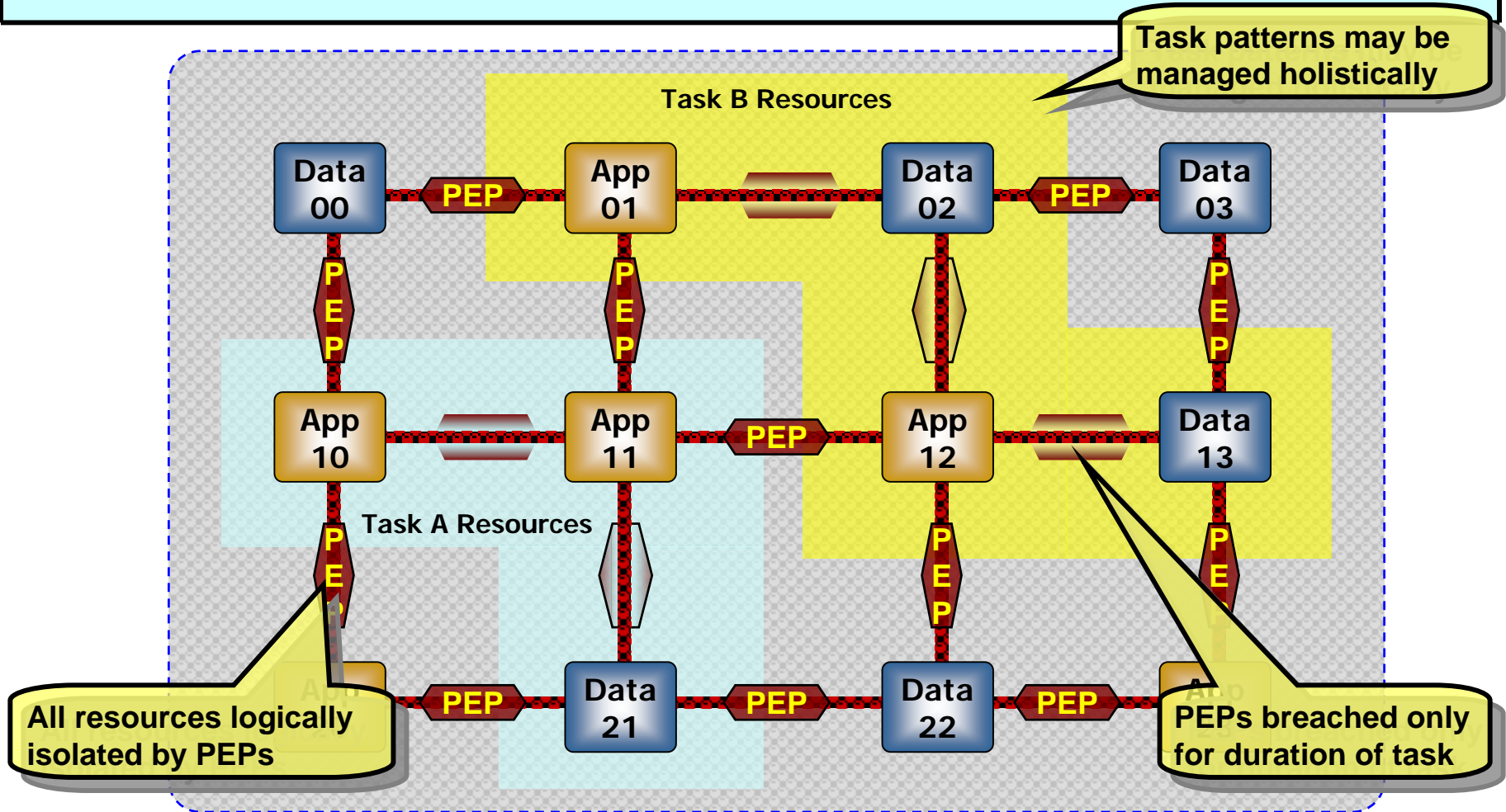


# Resource Availability: Network

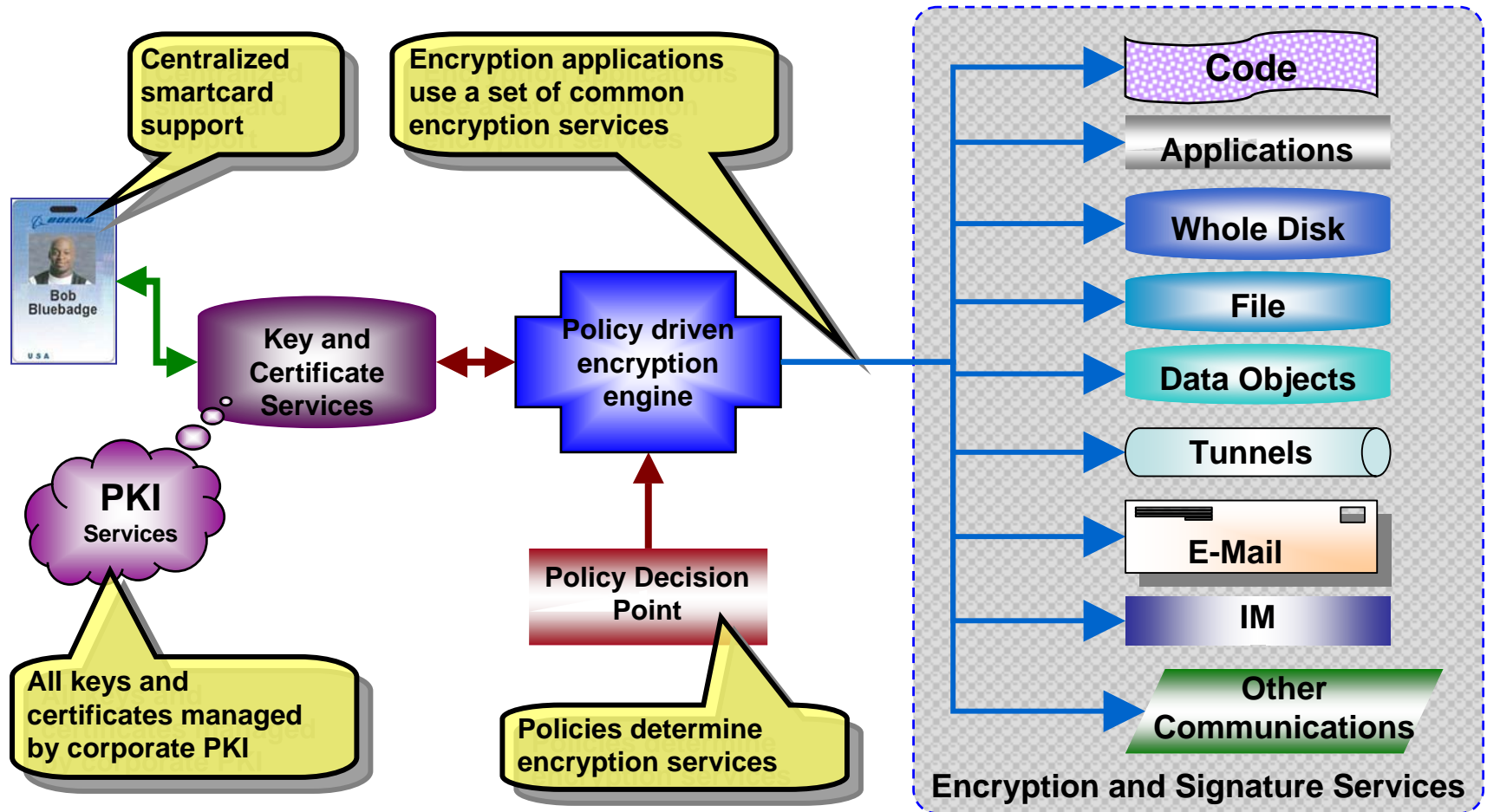




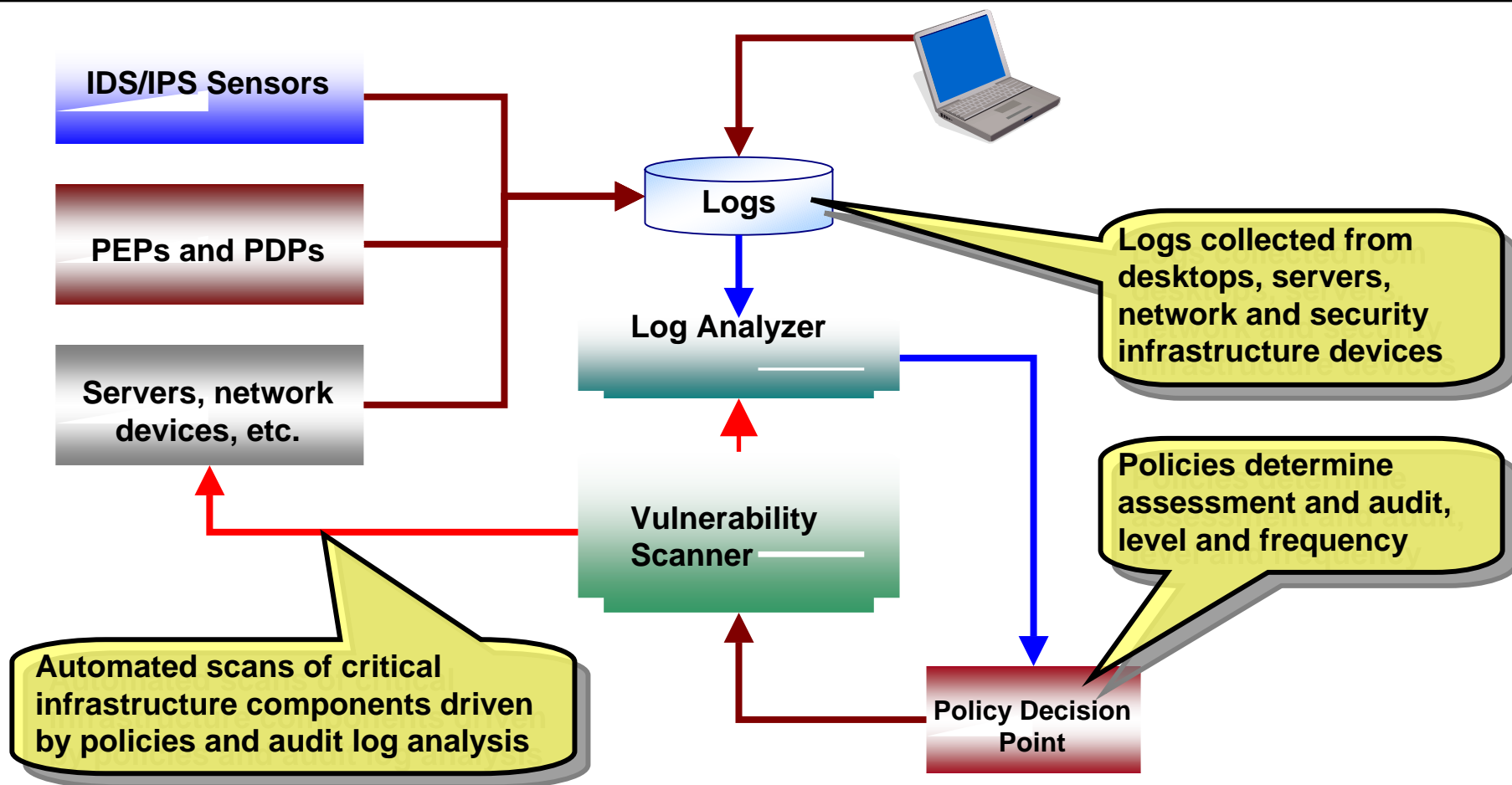
# Availability: Logical View



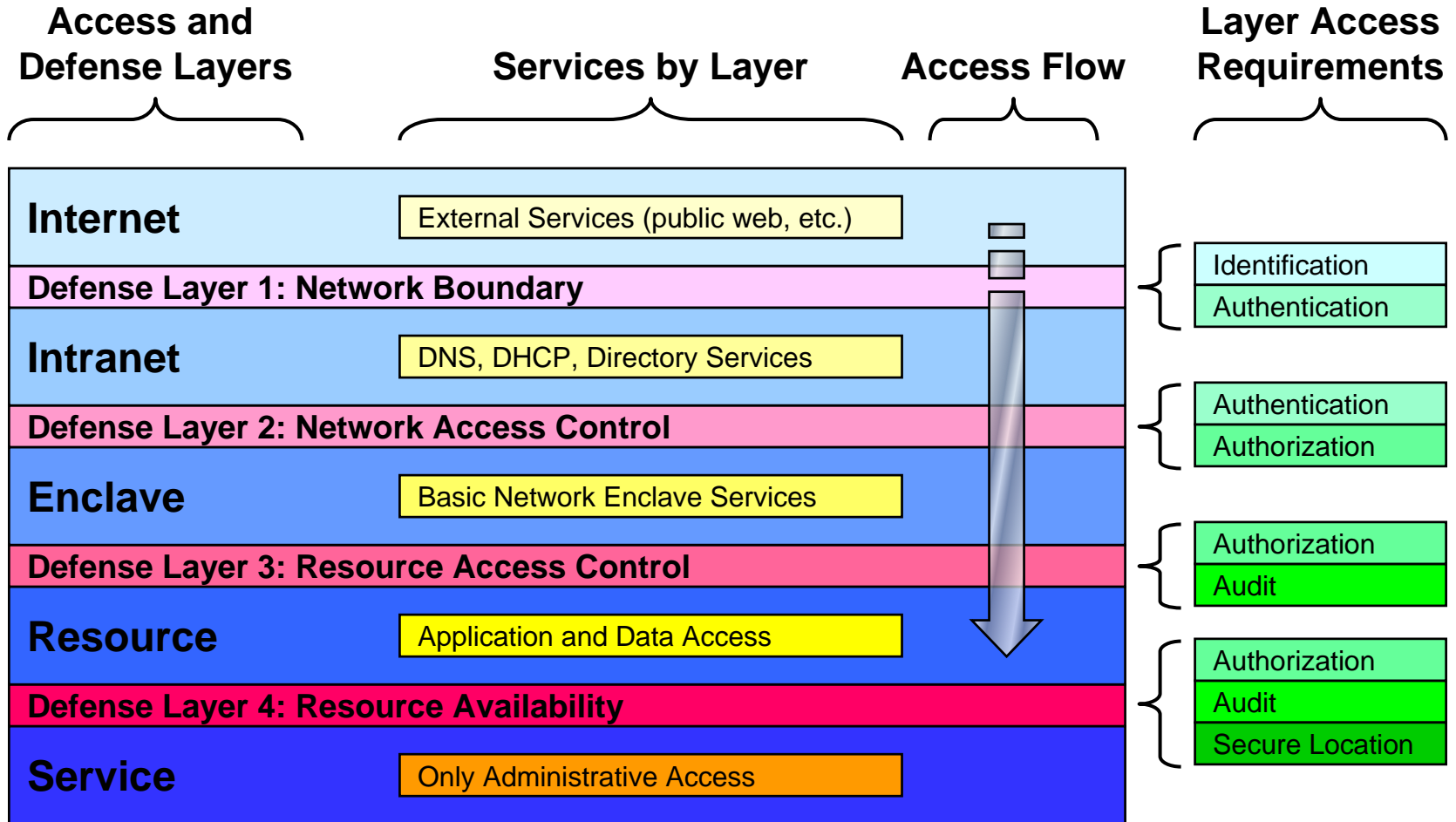
# Supporting Services: Cryptographic Services



# Supporting Services: Assessment and Audit Services



# Protection Layer Summary



# Case Study

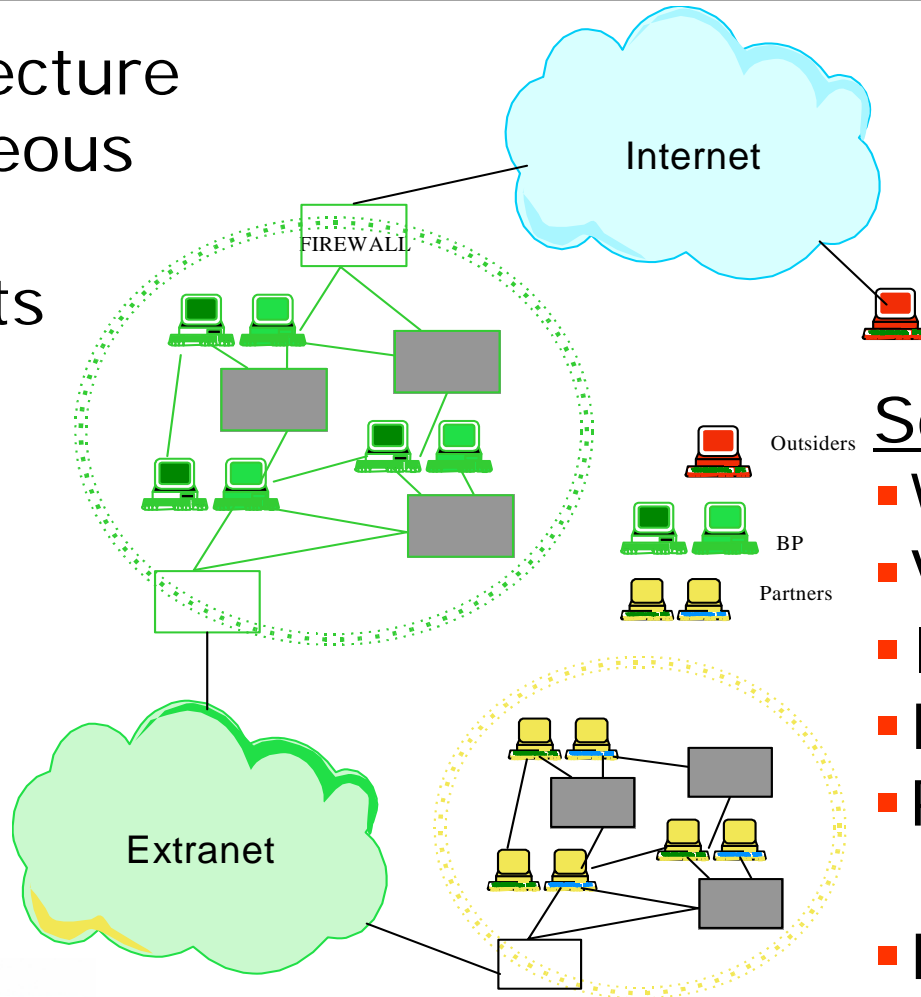
- **Migration to a de-perimeterised environment**
- **Mark Winzenburg**  
*BP Digital Security*

# Desktop Migration Strategy

- Previous Environment
- Drivers for Change
  - Business
  - Technology
  - Security
- Migration strategy

# Current Architecture

- Flat Architecture
- Heterogeneous
- Barriers & Chokepoints
- "Us" and "Them"



## Solutions?

- Wireless
- VPNs
- IDS/IPS
- Discovery
- Push Patch/Cfg.
- NAC/NAP

# Business Drivers (BP)

- Significant operations in 135+ countries
- Many users 'on the road', globally
- Large and increasing home-working
- Much use of outsourcers & contractors
- Many JVs, often with competitors
- Opening up to customers

## The archetypical 'virtual enterprise'.

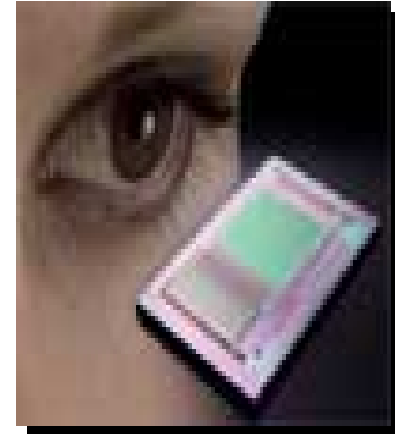
- Wasting money on private networks
- Create barriers to legitimate 3<sup>rd</sup> parties
- Hard to define what is inside vs. outside?





# Technology Drivers ...

- Pervasive computing - networks of small, inexpensive devices
- Ubiquitous wireless, sensory networks, mesh
- Mass digitisation in the industrial workplace
- Peer to peer, grid, high-performance computing
- Exploding connectivity and complexity (embedded Internet, IP convergence)
- Machine-understandable information (Semantic Web), predictive data analytics
- Social networking & collaboration



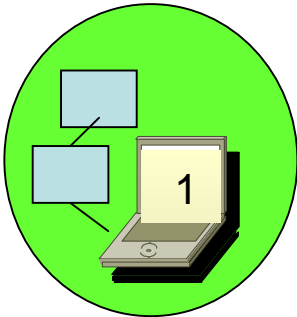
# Security Drivers

- Insiders
- Outsiders inside
- Port 80 and Mail traffic get in anyway
- Hibernating or 'rogue' devices
- Firewall rule chaos
- VOIP & P2P
- Stealth attackers
- Black list vs. white list
- False sense of security

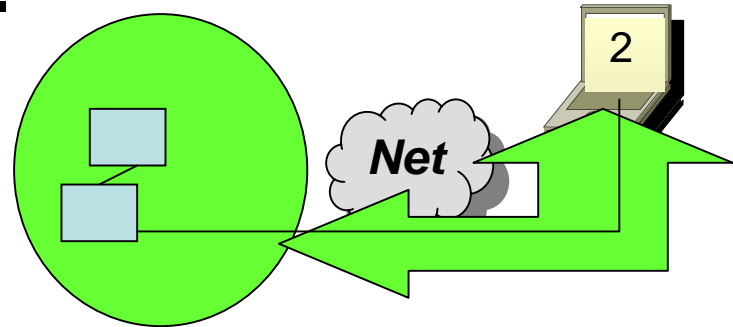


# Migration to the new model

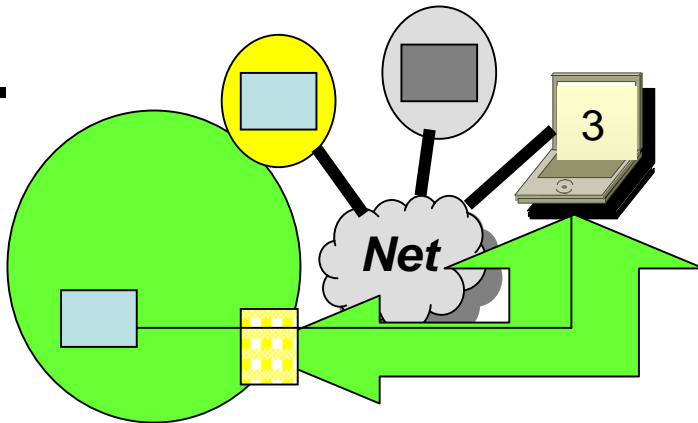
1.



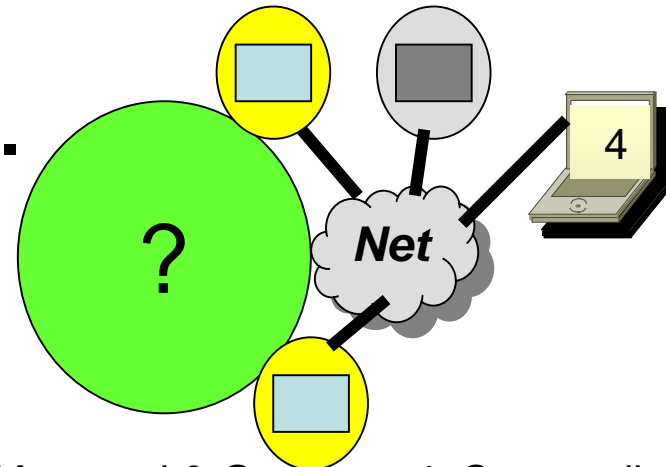
2.



3.

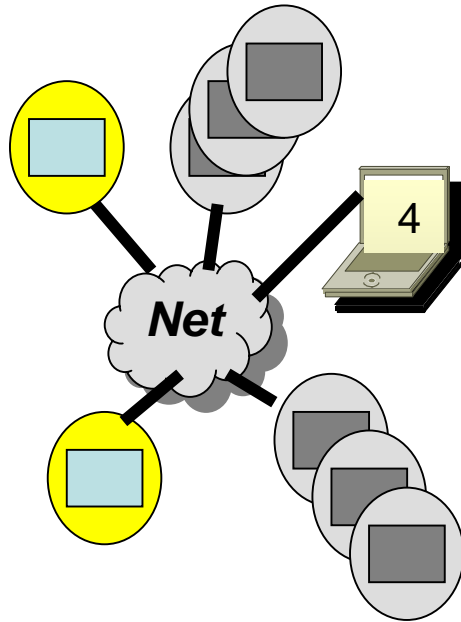


4.



1. Internal Managed. 2. Managed VPN 3. Self Managed & Gateway 4. Commodity/Allowance

# "In the Cloud" Security Services

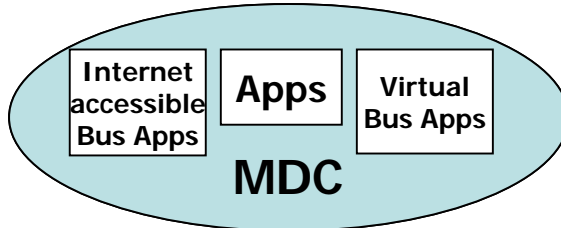


Can be 'in the cloud' or provided internally to 'cloud resident' devices

- Automated Patching
- Anti-malware - heuristic
- Trusted Device Certification
- "Clean" mail, IM, Web
- Federated Identity/Access
- Provisioning
- Alert ("Shields Up")
- Protection of 'atomic' data
- Trusted agent introduction
  - (White Listing)

# Desktop Strategy – Vision

Internet hosted services



• *consolidated Data Centres*

## Beyond PassPort

- seamless, secure access
- expose app not network



## "BP PassPort"

- good apps access
- full network access
- wired & wireless access



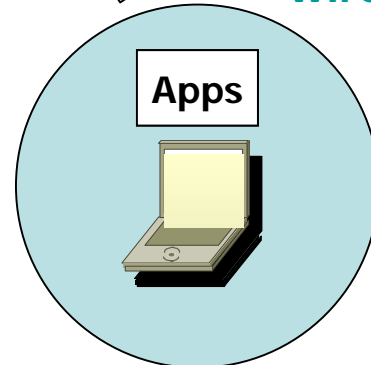
• choice of *Device Connectivity Support*

**Applications & Access Strategy**

- Simplify client, apps and access

## "Explorer"

- *internet based*
- *simplify client*
- *wireless access*



BP maintained  
BP provided  
BP supported

Auto-maintaining  
User provided  
Support choice

<< \$

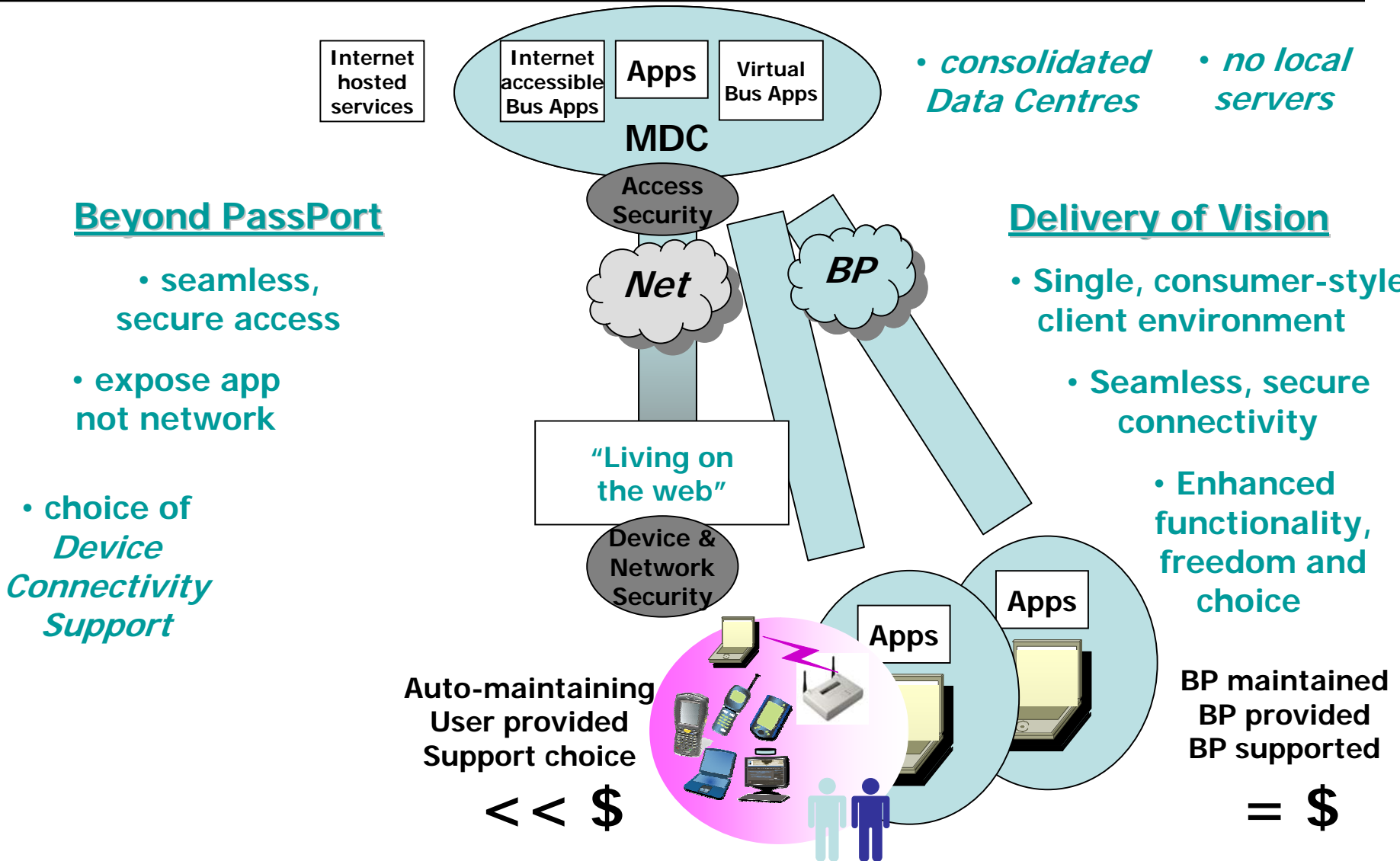


User maintained  
BP provided  
Self supported

< \$

= \$

# Desktop Strategy – Delivery of Vision



# - Scenarios

Access to applications from the Internet

**Strategic**

**SSL**

no client software  
 device and location specific  
 firewall friendly  
 connects at the application layer  
 only  
 no direct contribution to single sign-on  
 Requires generic Infrastructure Access gateway or per app ISA)

- Outlook 2003 diagnostic (RPC/HTTP)
- SharePoint
- New business application

**Tactical**

**SSL VPN**

- ~2008 (SRA)
- ~Q207 (RDP/HTTP)
- per app
- BP Services - File
- BP Services - Intranet - WTS

client software and/or on-demand client software  
 device and location specific  
 in-built device and access security  
 direct contribution to single sign-on  
 Requires generic Infrastructure Access gateway or per app ISA)

- Legacy application (offline use)
- Shrink-wrap application (offline use)
- ~ Local Virtual App

**Current**

**IPSec VPN**

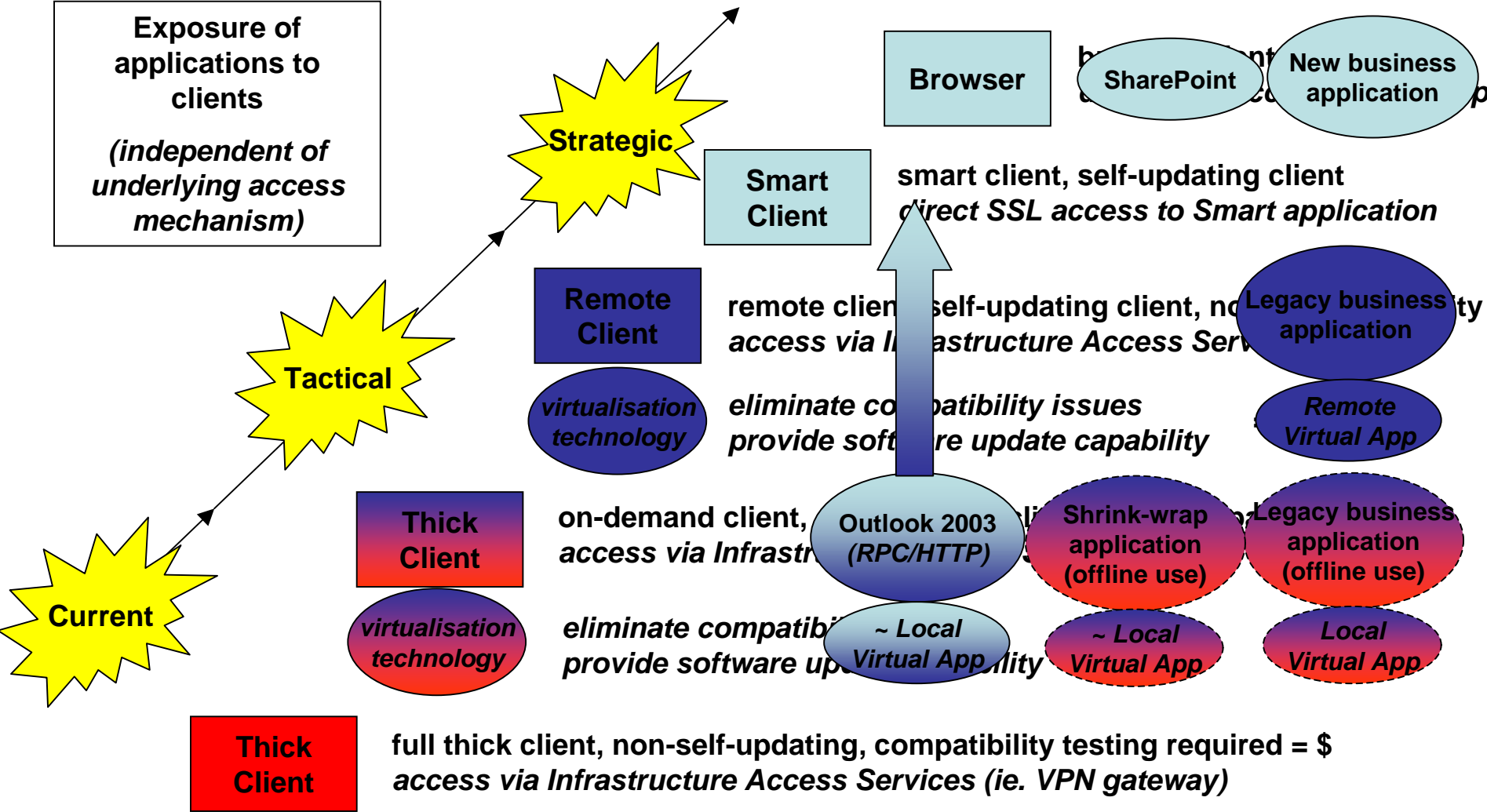
installed client software  
 device and location specific  
 non-firewall friendly  
 connects at the network layer  
 requires additional device and access security  
 no direct contribution to single sign-on  
 Requires proprietary Infrastructure Access Services (ie. VPN gateway)

Timeframe is now unless otherwise stated

Timeframe stated is Microsoft native feature

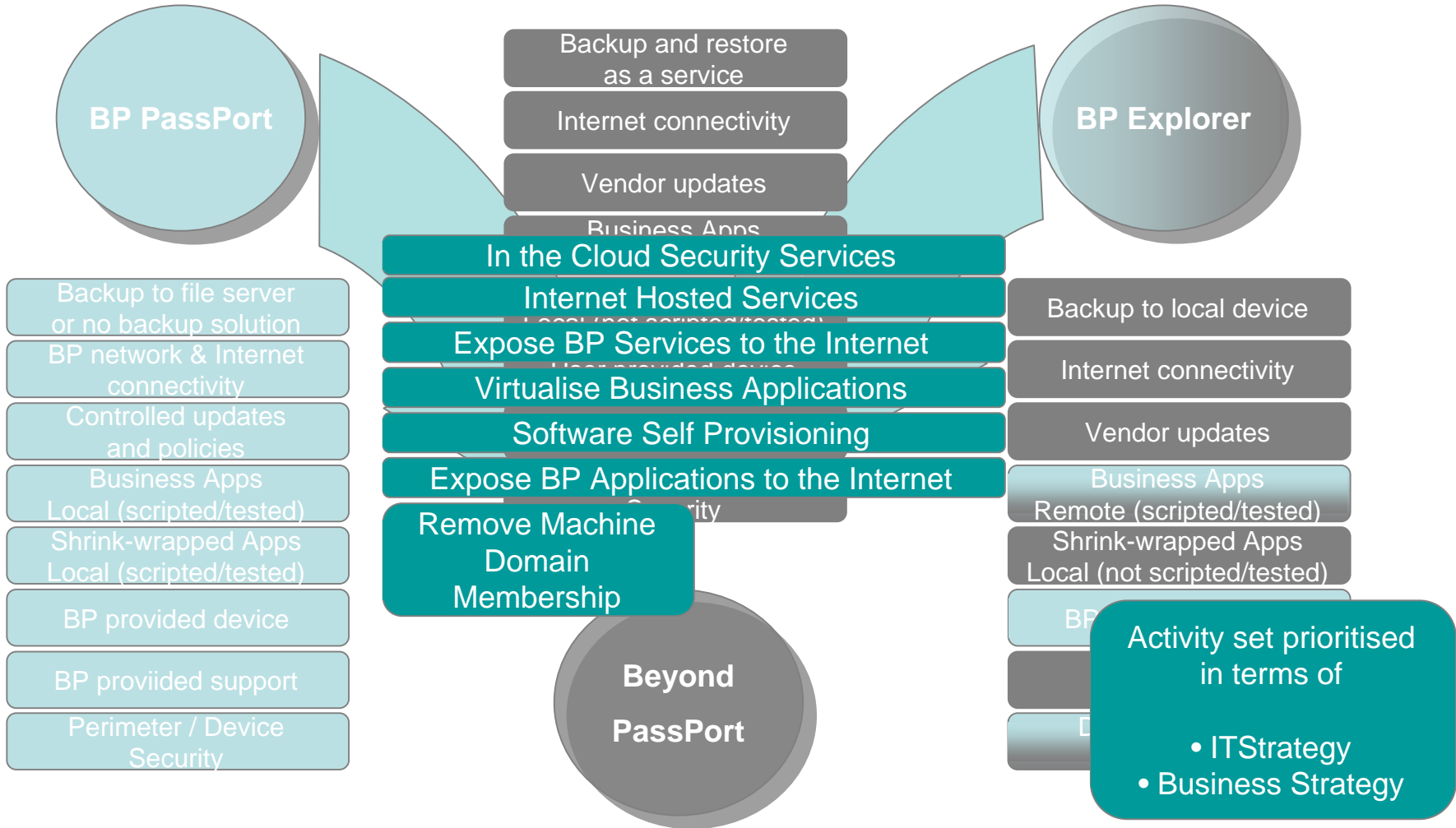
# Application Strategy - Scenarios

Exposure of applications to clients  
(independent of underlying access mechanism)





# 'Beyond Passport' - The Activities



# Global Adoption May Take Time



Gas Station in  
Cambodia

- 
- **Lunch**
  - **Resume at 2.00pm**

# The Jericho Forum – 3rd US Conference

**Thurs-Fri Sept 21-22, 2006**

**Hosted by Boeing**

Museum of Flight, Seattle, WA., USA

## Thursday

- 09.00 Reception
- 09.30 Welcome & Introductions
- 09.45 Opening Keynote
- 10.15 The Commandments
- 11.15 Position Papers overview
- 11.20 Selected Papers 1, 2, 3
- 12.20 Case Study: Migration to de-perimeterised environment
- 12.30 Lunch
- 13.30 Roadmap and next steps
- 15.00 Break
- 15.30 Q&A Panel
- 16.45 Summary
- 17.00 Close

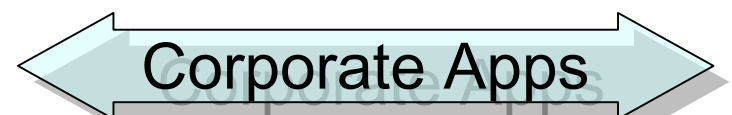
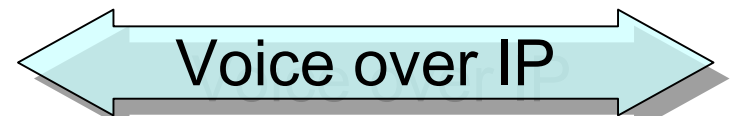
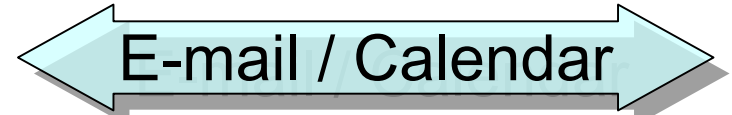
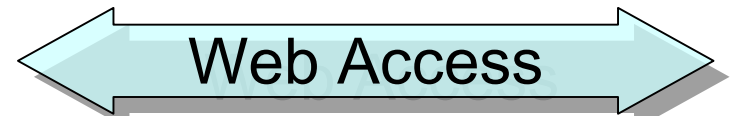
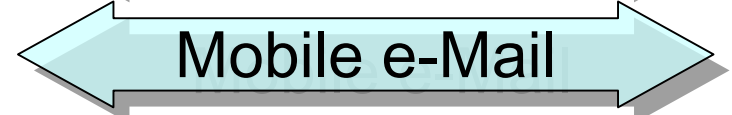
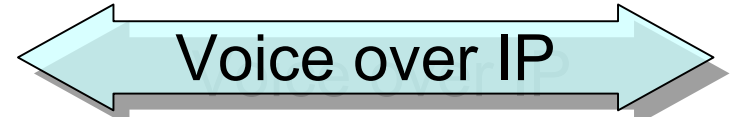
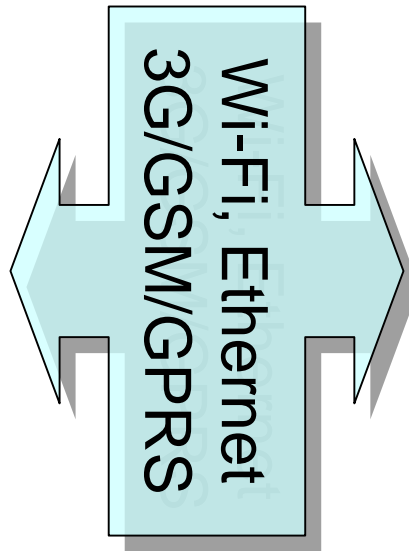
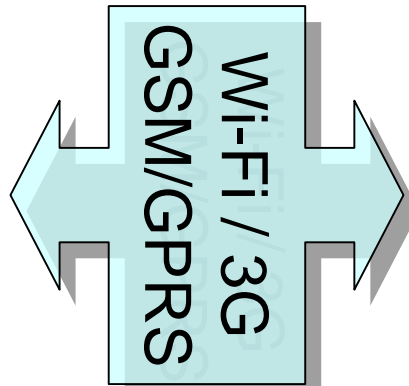
## Friday

- 09.00 Plenary on 2-3 selected security problems
- 09.45 Breakout into 2-3 WGs
- 10.30 Break
- 10.45 Move to 2<sup>nd</sup> WG
- 11.30 Move to 3<sup>rd</sup> WG
- 12.15 Summary reports & review
- 13.00 Lunch
- 14.00 Round table: open forum feedback session
- 15.15 Summary
- 15.30 Close

# Prepare for the future

- **The de-perimeterised road-warrior"**
- **Paul Simmonds**  
*ICI plc.*  
*& Jericho Forum Board*

# Requirements



# Requirements – Hand-held Device

- VoIP over Wireless
  - Integrated into Corporate phone box / exchange with calls routed to wherever in the world
- Mobile e-Mail & Calendar
  - Reduced functionality synchronised with laptop, phone and corporate server
- Presence & Location
  - Defines whether on-line and available, and the global location
- Usability
  - Functions & security corporately set based on risk and policy.

# Requirements – Laptop Device

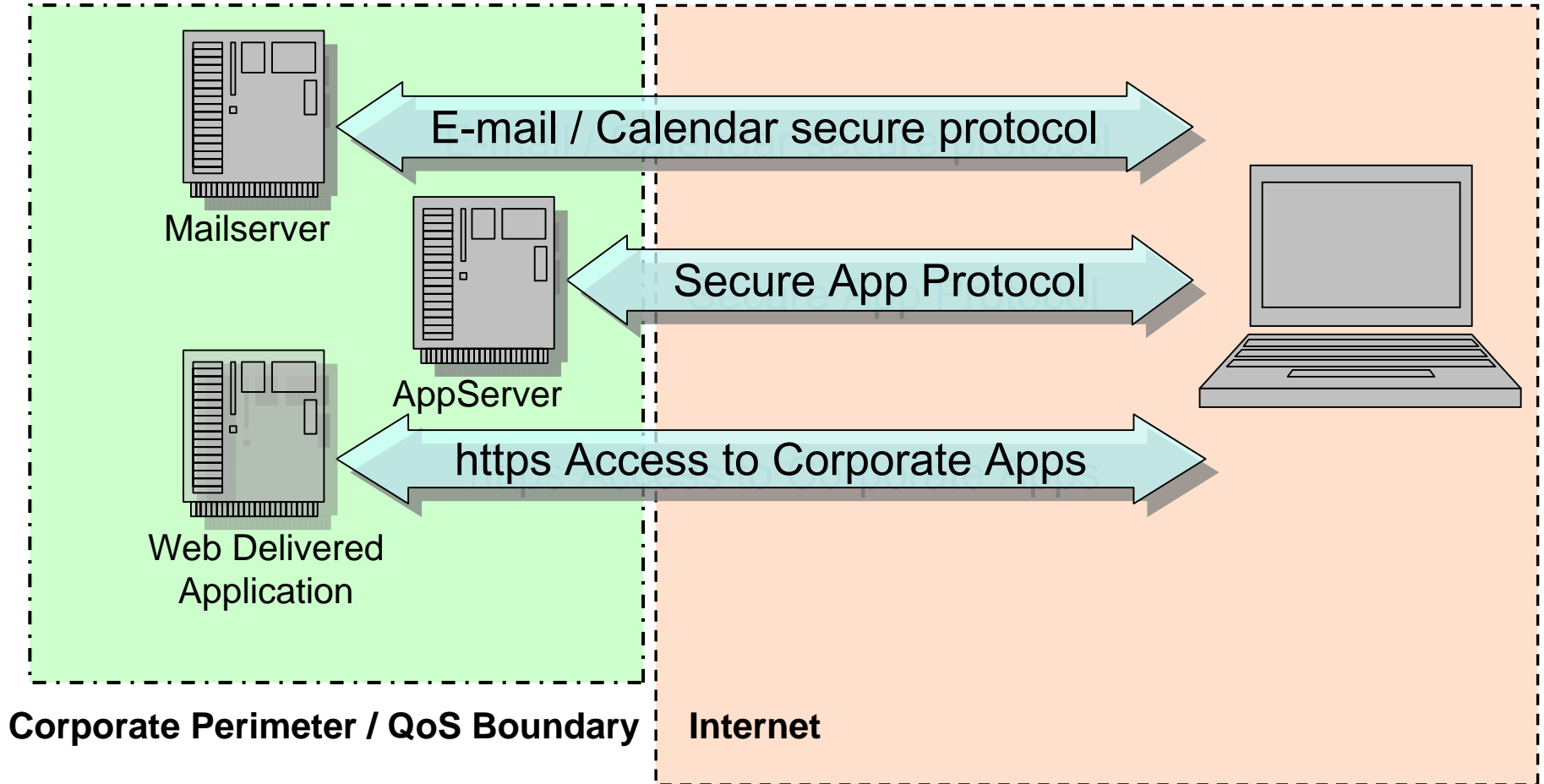
- Web Access
  - Secure, “clean”, filtered and logged web access irrespective of location
- e-Mail and Calendar
  - Full function device
- Voice over IP
  - Full feature set with “desk” type phone emulation
- Access to Corporate applications
  - Either via Web, or Clients on PC
- Usability
  - Functions & security corporately set based on risk and policy
  - Self defending and/or immune
  - Capable of security / trust level being interrogated



# Corporate Access – The Issues

- Corporate users accessing corporate resources typically need;
  - Access to corporate e-mail (pre-cleaned)
  - Access to calendaring
  - Access to corporate applications (client / server)
  - Access to corporate applications (web based)

# Putting it all together – Corporate Access

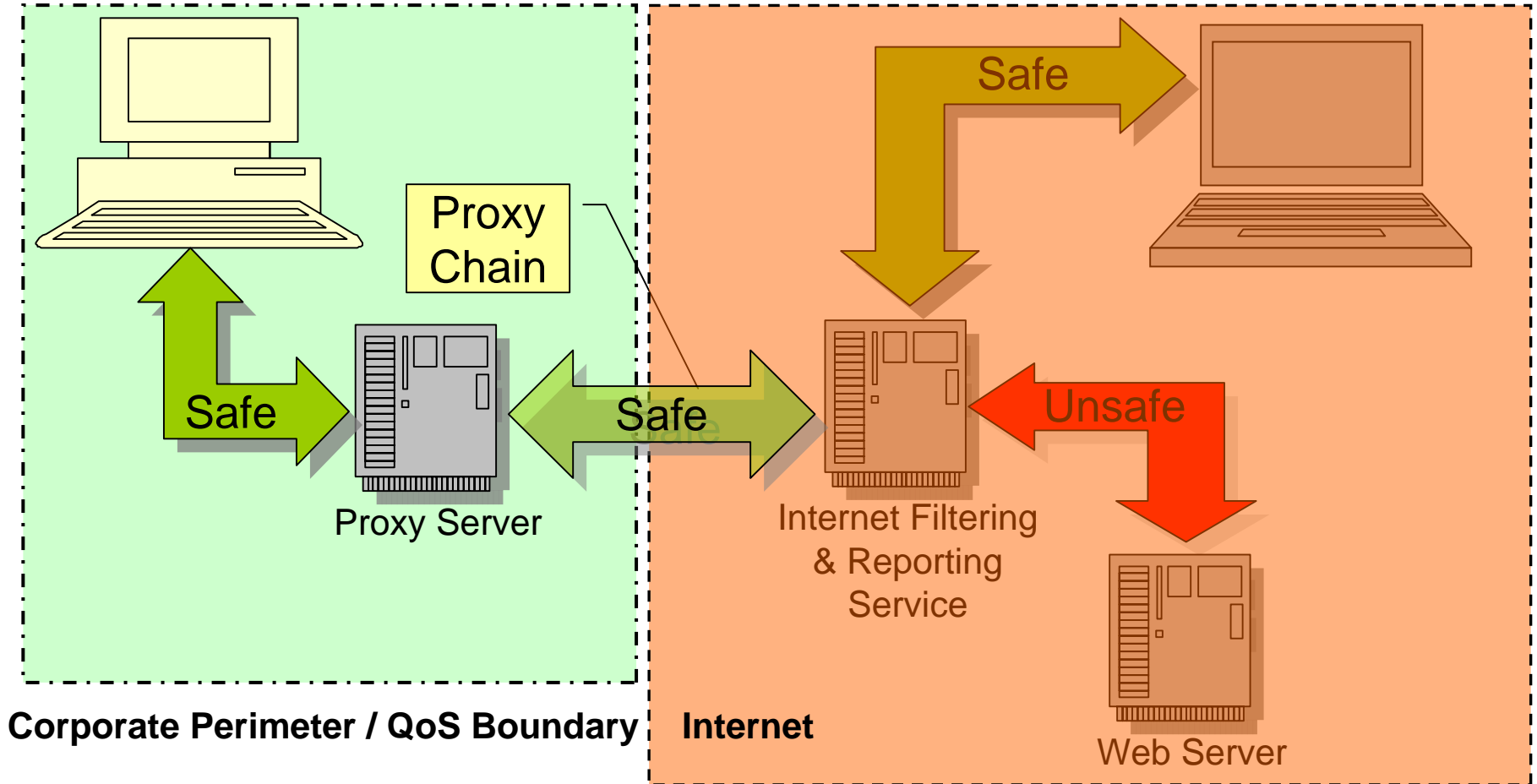


## Web Access – The Issues\*

- Single Corporate Access Policy
  - Regardless of location
  - Regardless of connectivity method
  - With multiple egress methods
- Need to protect all web access from malicious content
  - Mobile users especially at risk

\* This will be the subject of a future Jericho Position Paper

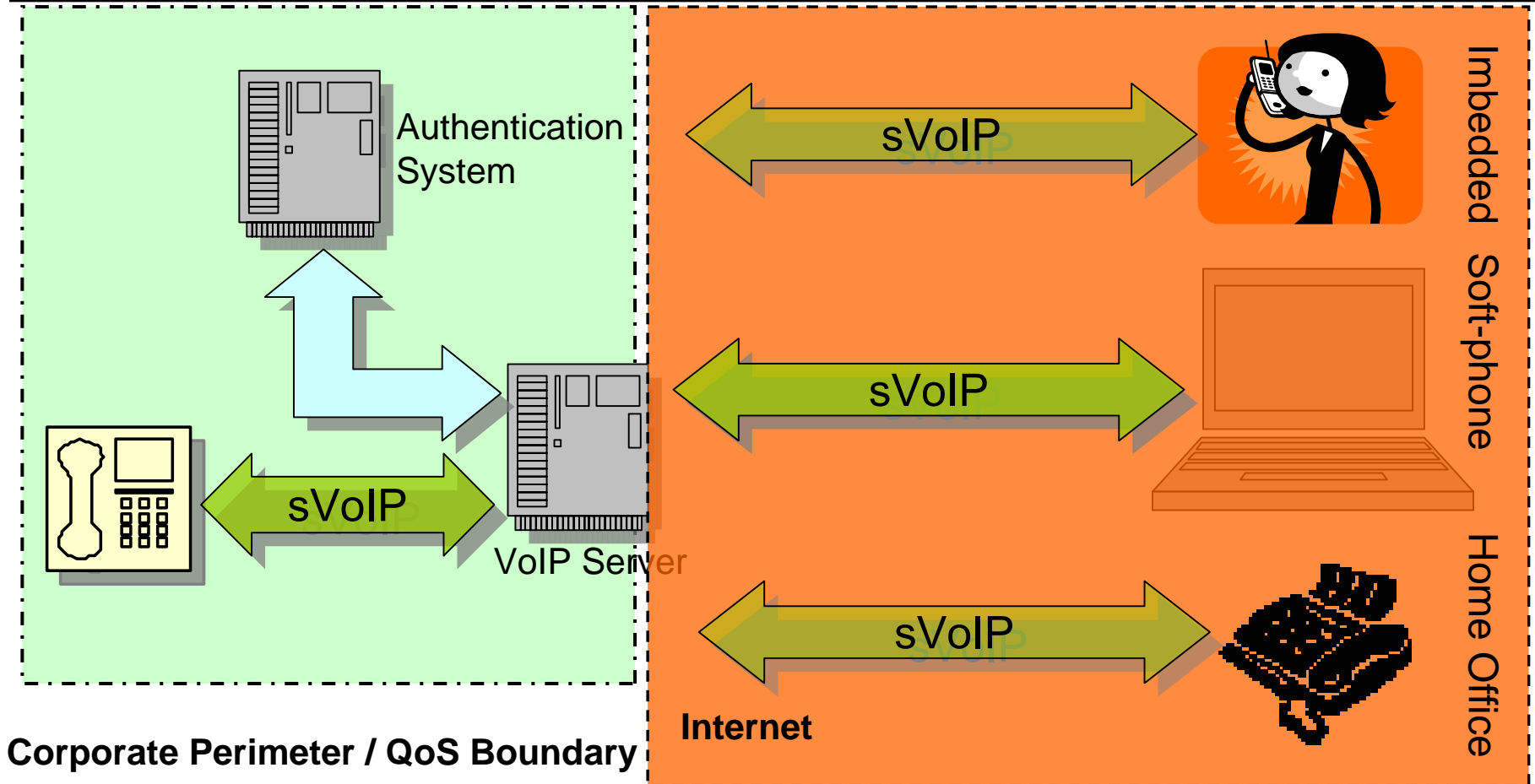
# Putting it all together – Web Access



# Voice /Mobile Access - The Issues

- Mobile / Voice devices require;
  - Connection of any VoIP device to the corporate exchange
  - Single phone number finds you on whichever device you have logged in on (potentially multiple devices)
  - No extra devices or appliances to manage
  - Device / supplier agnostic secure connectivity

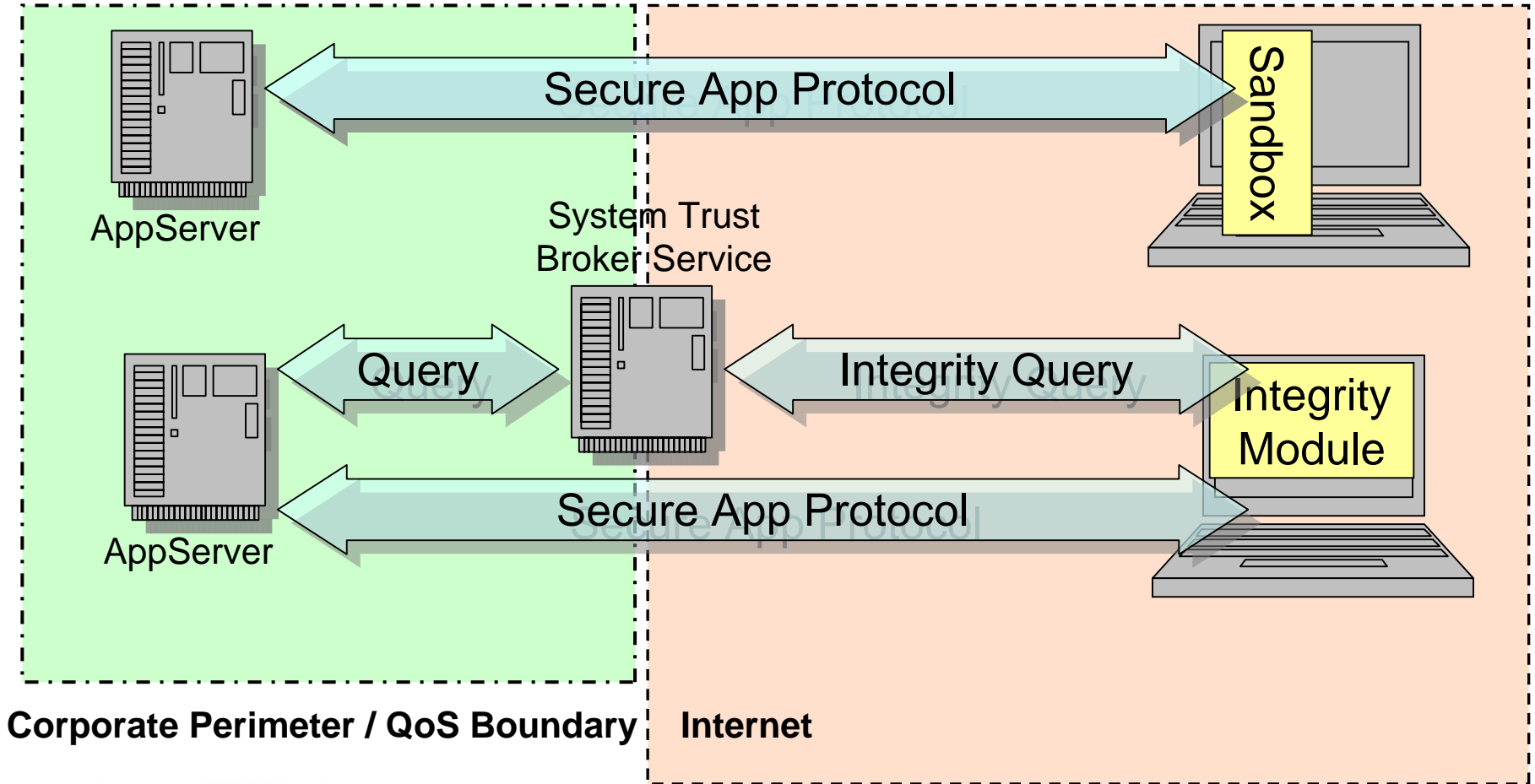
# Putting it all together – VoIP Access



## Issues - Trust

- NAC generally relies on a connection
  - Protocols do not make a connection in the same way as a device
- Trust is variable
  - Trust has a temporal component
  - Trust has a user integrity (integrity strength)
  - Trust has a system integrity
- Two approaches;
  - Truly secure sandbox (system mistrust)
  - System integrity checking

# Putting it all together – System Trust





# An inherently secure system

- When the only protocols that the system can communicate with are inherently secure;
  - The system can “black-hole” all other protocols
  - The system does not need a personal firewall
  - The system is less prone to malicious code
  - Operating system patches become less urgent

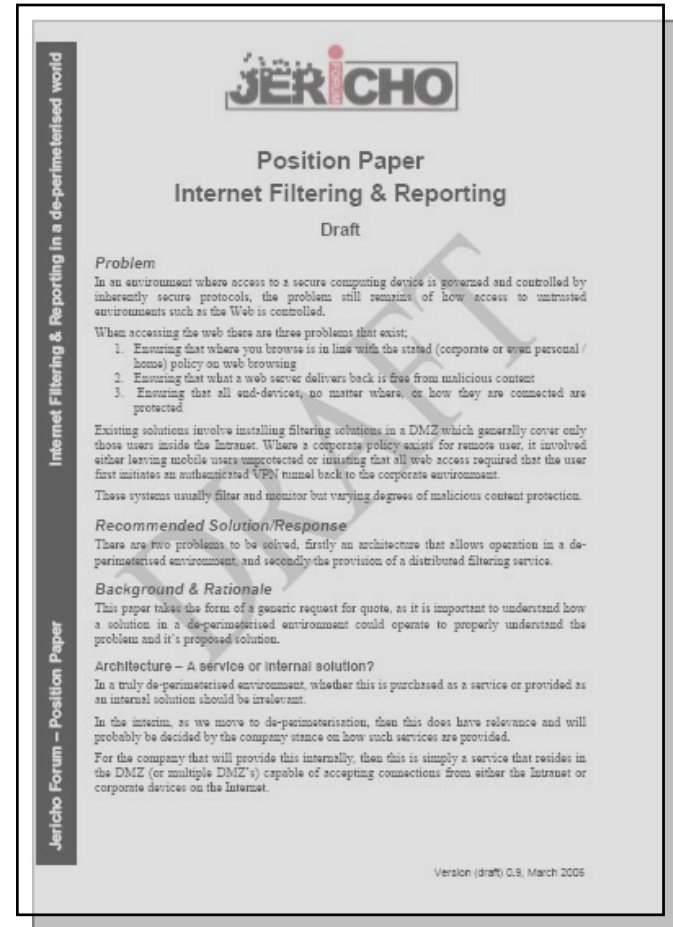
# An inherently secure corporation

- When a corporate retains a WAN for QoS purposes;
  - WAN routers only accept inherently secure protocols
  - The WAN automatically “black-holes” all other protocols
  - Every site can have an Internet connection as well as a WAN connection for backup
  - Non-WAN traffic automatically routes to the Internet
  - The corporate “touchpoints” now extend to every site thus reducing the possibility for DOS or DDOS attack.

# Paper available soon from the Jericho Forum

- The Jericho Forum Position Paper “Internet Filtering and reporting” is currently being completed by Jericho Forum members

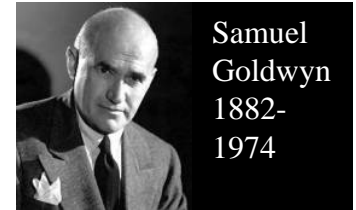
<http://www.jerichoforum.org>



# Prepare for the future

- **Road-mapping & next steps**
- **Nick Bleech**  
*Rolls Royce & Jericho Forum Board*

We want a story that starts out with an earthquake and works its way up to a climax.



# Two Ways to Look Ahead

- Solution/System Roadmaps (both vendor and customer)
- Security Themes from the Commandments
  - Hostile World
  - Trust and Identity
  - Architecture
  - Data protection

# Solution/System Roadmaps

Continuum



Desired Future State

Work Types


Needs  
Principles  
Strategy

Customers

Vendors

White Papers  
Patterns  
Use Cases

Guidelines  
Standards  
Solutions

 Jericho Forum  
 Standards groups

Standards and Solutions

# Potential Roadmap

Key Components New & evolving technologies ( <a href="#">partial</a> )	<ul style="list-style-type: none"> <li>Firewalls (Filter /DPI/Proxy)</li> <li>Anti-Virus Anti-Spam</li> <li>Cli&amp;Svr Patch Mgmt</li> <li>IPSec VPN</li> <li>SSL/Web SSO</li> <li>Proxies/IFR for -Trading Apps -Web/Msging</li> <li>DS point solutions</li> <li>IPS point solutions</li> <li>Dev config</li> </ul>	<ul style="list-style-type: none"> <li>Firewalls (Fltr/DPI)</li> <li>Anti-Virus/Spam</li> <li>Cli&amp;Svr Patch Mgmt</li> <li>Proxies/IFR for - Trading Apps - Web/Msging</li> <li>DS point solutions</li> <li><a href="#">TL/NL gateways</a></li> <li><a href="#">XML point solutions</a></li> <li><a href="#">Fed. Identity</a></li> <li><a href="#">Intrusion correlation &amp; response</a></li> <li><a href="#">Micro-perim mgmt &amp; device firewall/config</a></li> </ul>	<ul style="list-style-type: none"> <li>Firewalls (Fltr/DPI)</li> <li>Anti-Virus/Spam</li> <li>Svr Patch Mgmt</li> <li>Proxies/IFR for Trading Apps</li> <li>DS point solutions</li> <li><a href="#">TL/NL gateways</a></li> <li><a href="#">Fed. Identity</a></li> <li><a href="#">Intrusion correlation &amp; response</a></li> <li><a href="#">Micro-perim mgmt &amp; dev firewalls/config</a></li> <li><a href="#">Redc'd surface OS &amp; client patching</a></li> <li>Virtual Proxies/IFR</li> <li><a href="#">XML subsetting</a></li> <li>P2P point solutions</li> </ul>	<ul style="list-style-type: none"> <li>Firewalls (Fltr/DPI)</li> <li>Anti-Spam</li> <li>Svr Patch Mgmt</li> <li><a href="#">TL/NL gateways</a></li> <li><a href="#">Fed. Identity</a></li> <li><a href="#">Intrusion correlation &amp; response</a></li> <li>Micro-perim mgmt &amp; dev firewalls/ config</li> <li><a href="#">Redc'd surface OS &amp; client/svr patching</a></li> <li>Virtual Proxies/IFR</li> <li>XML subsetting</li> <li><a href="#">P2P trust models</a></li> </ul>	<ul style="list-style-type: none"> <li>Firewalls (DPI)</li> <li>Anti-Malware</li> <li><a href="#">TL/NL gateways</a></li> <li><a href="#">Intrusion correlation &amp; response</a></li> <li><a href="#">Micro-perim mgmt &amp; dev firewalls/config</a></li> <li><a href="#">Redc'd surface OS &amp; client/svr patching</a></li> <li><a href="#">Virtual Proxies/IFR</a></li> <li><a href="#">XML subsetting</a></li> <li><a href="#">P2P trust models and identity</a></li> <li><a href="#">Trust assurance mgmt</a></li> <li><a href="#">Interoperable DS</a></li> </ul>
	60% Adoption	Pre 2006	2006	2007	2008
Key Obsoleted Technology	<ul style="list-style-type: none"> <li>Dial-up security</li> <li>Simple IDS</li> </ul>	<ul style="list-style-type: none"> <li>IPsec VPN</li> <li>Firewall-based proxies</li> </ul>	<ul style="list-style-type: none"> <li>Proxies/IFR for Web/Msging</li> <li>XML point solutions</li> <li>CInt 'service releases'</li> </ul>	<ul style="list-style-type: none"> <li>Hybrid IPsec/TLS gateways</li> <li>Proxies/IFR</li> <li>Standalone AV</li> </ul>	<ul style="list-style-type: none"> <li>Fltr Firewalls</li> <li>Svr 'service releases'</li> <li>Fed. Identity</li> </ul>



# Hostile World Extrapolations

- Convergence of SSL/TLS and IPsec:
  - Need to balance client footprint, key management, interoperability and performance.
  - Server SSL = expensive way to do authenticated DNS.
  - Need a modular family of inherently secure protocols.
  - See Secure Protocols and Encryption & Encapsulation papers.
- Broad mass of XML security protocols condemned to be low assurance.
  - XML Dsig falls short w.r.t. several Commandments
- Platforms are getting more robust, but:
  - Least privilege, execute-protection, least footprint kernel, etc. ... WIP
  - Need better hardware enforcement for protected execution domains.
  - Papers in preparation.
- Inbound and outbound proxies, appliances and filters litter the data centre - time to move them 'into the cloud'.
  - See Internet Filtering paper.

# Trust and Identity Extrapolations

- 'Trust management' first identified in 1997; forgotten until PKI boom went to bust.
  - Last three years research explosion
- Decentralised, peer to peer (P2P) models are efficient
  - Many models: rich picture of human/machine and machine/machine trust is emerging.
  - Leverage PKC (not PKI) core concepts; mind the patents!
- 'Strong identity' and 'strong credentials' are business requirements.
- 'Identity management' is a set of technical requirements.
  - How we do this cross-domain in a scalable manner is WIP.
- At a technical level, need to clear a lot of wreckage.
  - ASN.1, X.509 = 'passport', LDAP = 'yellow pages' ... etc.
- Papers in preparation.

# Architecture Extrapolations

- Enterprise-scale systems architecture is inherently domain-oriented and perimeterised (despite web and extranet).
  - Client-server and multi-tier.
  - Service-oriented architecture -> web services.
  - Layer structure optimises for traditional applications
  - Portals are an attempt to hide legacy dependencies.
- Collaboration and trading increasingly peer-to-peer.
- Even fundamental applications no longer tied to the bounded 'enterprise':
  - Ubiquitous computing, agent-based algorithms, RFID and smart molecules point to a mobile, cross-domain future.
  - Grid computing exemplifies an unfulfilled P2P vision, encumbered by the perimeter.
  - See Architecture paper.

# Data Protection Extrapolations

- Digital Rights Management has historically focused exclusively on copy protection of entertainment content.
- 'Corporate' DRM as an extension of PKI technology now generally available as point solutions.
  - Microsoft, Adobe etc.
  - Copy 'protection', non-repudiation, strong authentication & authorisation.
  - 'Labelling' is a traditional computer security preoccupation.
- Business problems to solve need articulating.
  - The wider problem is enforcement of agreements, undertakings and contracts; implies data plus associated 'intelligence' should be bound together.
- Almost complete absence of standards.
- Paper in preparation.

# What about 'People and Process'?

Jericho Forum assumes a number of constants:

- Jurisdictional and geopolitical barriers will continue, and constrain (even reverse) progress
- Primary drivers for innovation and technology evolution are:
  - Perceived competitive advantage / absence of disadvantage.
  - Self-interest of governments and their agents as key arbiters of demand (a/k/a/ the Cobol syndrome).
- IT industry will continue to use standards and patents as proxies for proprietary enforcement.
- Closed source vs. open source is a zero sum.

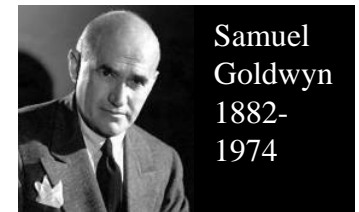
## How are we engaging?

- Stakeholders WG: chair - David Lacey
  - Corporate and government agendas
  - Our position in the Information Society
- Requirements WG: chair - Nick Bleech
  - Business Scenarios, planning and roadmapping
  - Assurance implications
- Solutions WG: chair - Andrew Yeomans
  - Patterns, solutions and standards
  - Jericho Forum Challenge

# Conclusions

- A year ago we set ourselves a vision to be realised in 3-5 years
- Today's roadmap shows plenty of WIP still going on in 2009!
- Want this stuff quicker? Join us!

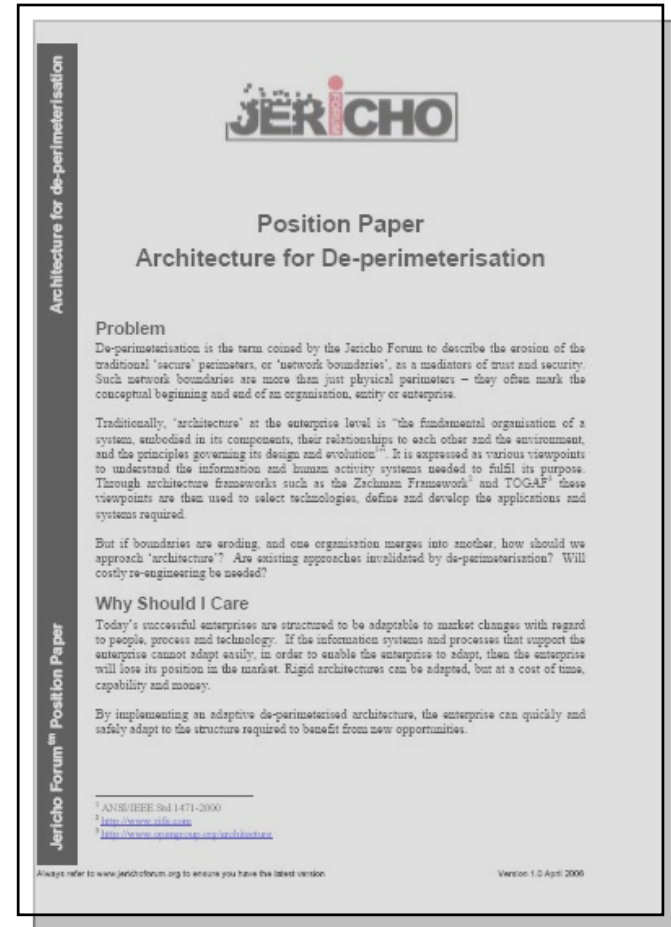
I never put on a pair of shoes until I've worn them at least five years.




# Paper available from the Jericho Forum

- The Jericho Forum Position Paper "Architecture for de-perimeterisation" is freely available from the Jericho Forum website

<http://www.jerichoforum.org>





- 
- **Break**  
*Tea & Coffee*
  - **Resume at 3.45pm**

# Question & Answers

- **Face the audience Q&A session**
- **Moderated by  
Scott Shepard, Motorola**



- **Summing up the day**

- **Bill Boni**  
*Motorola*

# The Jericho Forum – 2nd US Conference

**Fri, May 12, 2006**

**Hosted by Motorola**

Motorola Center, Schaumburg, Chicago, IL, USA

- 09:00 Arrival
- 09.30 Welcome & Housekeeping
- 09.35 Opening Keynote:  
Setting the scene
- 09.50 The Jericho Forum  
Commandments
- 10:45 Break
- 11.00 Real world application:  
Protocols
- 11.20 Real world application:  
VoIP
- 11.40 Real world application:  
Corp. Wireless Networking
- 12.00 Case Study: Boeing:  
What Hath Vint Wrought?
- 12.30 Case Study: BP:  
Migration to a de-  
perimeterised environment
- 13.00 Lunch
- 14.00 The future:  
The de-perimeterised  
road warrior
- 14.45 The future: Roadmap &  
next steps
- 15.30 Break (Coffee & Tea)
- 15.45 Face the audience: Q&A
- 16:45 Summing up the day  
Bill Boni, Motorola
- 17:00 Close

# Jericho Forum

## Shaping security for tomorrow's world



[www.jerichoforum.org](http://www.jerichoforum.org)