Welcome

2nd Jericho Forum
Annual Conference

25th April 2005

Grosvenor Hotel,
Park Lane, London

Hosted by SC Magazine

Welcome & Housekeeping

- **Richard Watts**
- *Publisher,*
  SC Magazine

SC
MAGAZINE
AWARDS
2006

Agenda

- 11.05 Opening Keynote – “Setting the scene” - Paul Fisher, Editor SC Magazine
- 11.15 The Jericho Forum “Commandments” - Nick Bleech, Rolls Royce
- 11.30 Case Study: What Hath Vint Wrought - Steve Whitlock, Boeing
- 12.00 Real world application: Protocols - Paul Simmonds, ICI
- 12.15 Real world application: Corporate Wireless Networking- Andrew Yeomans, DrKW
- 12.30 Real world application: VoIP - John Meakin, Standard Chartered Bank
- 12.45 Case Study: Migration to de-perimeterised environment - Paul Dorey, BP
- 13.15 Lunch
- 14.30 Prepare for the future: The de-perimeterised “road warrior” - Paul Simmonds
- 14.50 Prepare for the future: Roadmapping & next steps - Nick Bleech
- 15.15 Break (Coffee & Tea)
- 15.45 Face the audience: (Q&A) - Moderated by: Paul Fisher, Editor, SC Magazine
- 16.45 Summing up the day - Paul Fisher, Editor, SC Magazine
- 17.00 Close

Some of our members

ICI
BELARC
QANTAS
hp
invent
IBM
Deloitte.
MOTOROLA
Foreign &
Commonwealth Office
Nexus
P&G
Identum
Protecting Privacy
nCIPHER
ING
PHILIPS
symantec.
Royal Mail
bp
cybertrust
ROLLS
RR
ROYCE
CSIRO
OBVIOUS
A StopStone Company
Cabinet Office
KPMG
Standard Chartered
QUALYS
Security On Demand
HSBC
Lilly
Sun
microsystems
BOEING
Dresdner Kleinwort Wasserstein
C&C Technology Consulting
LOCKHEED MARTIN
We never forget who we're working for
EPFL
ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE
Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING
THE UNIVERSITY
OF AUCKLAND
NEW ZEALAND
KENT
UNIVERSITY OF KENT
40 YEARS 1965-2005
NOVARTIS
gsk
GlaxoSmithKline
NEC
M
MACQUARIE
UNIVERSITY~SYDNEY
BIND VIEW

Opening Keynote

- **“Setting the scene”**
- **Paul Fisher,**
  Editor SC Magazine

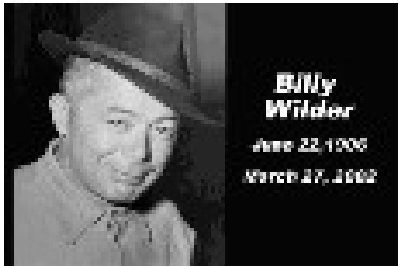
Setting the Foundations

- **The Jericho Forum "Commandments"**
- **Nick Bleech**
  Rolls Royce &
  Jericho Forum Board

SC MAGAZINE
AWARDS
2006

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

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

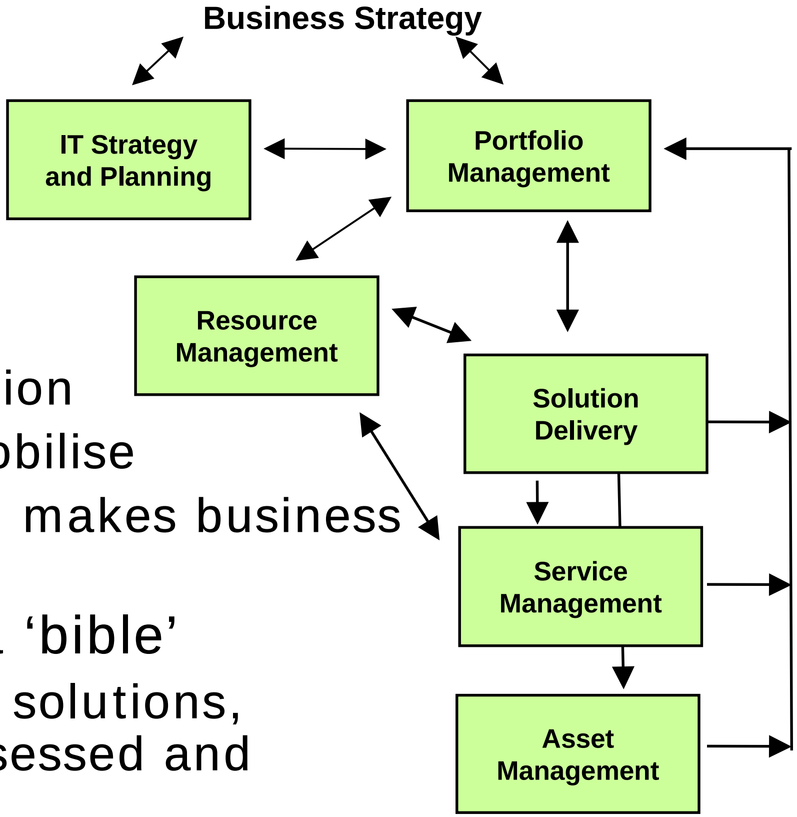


Rationale

- 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

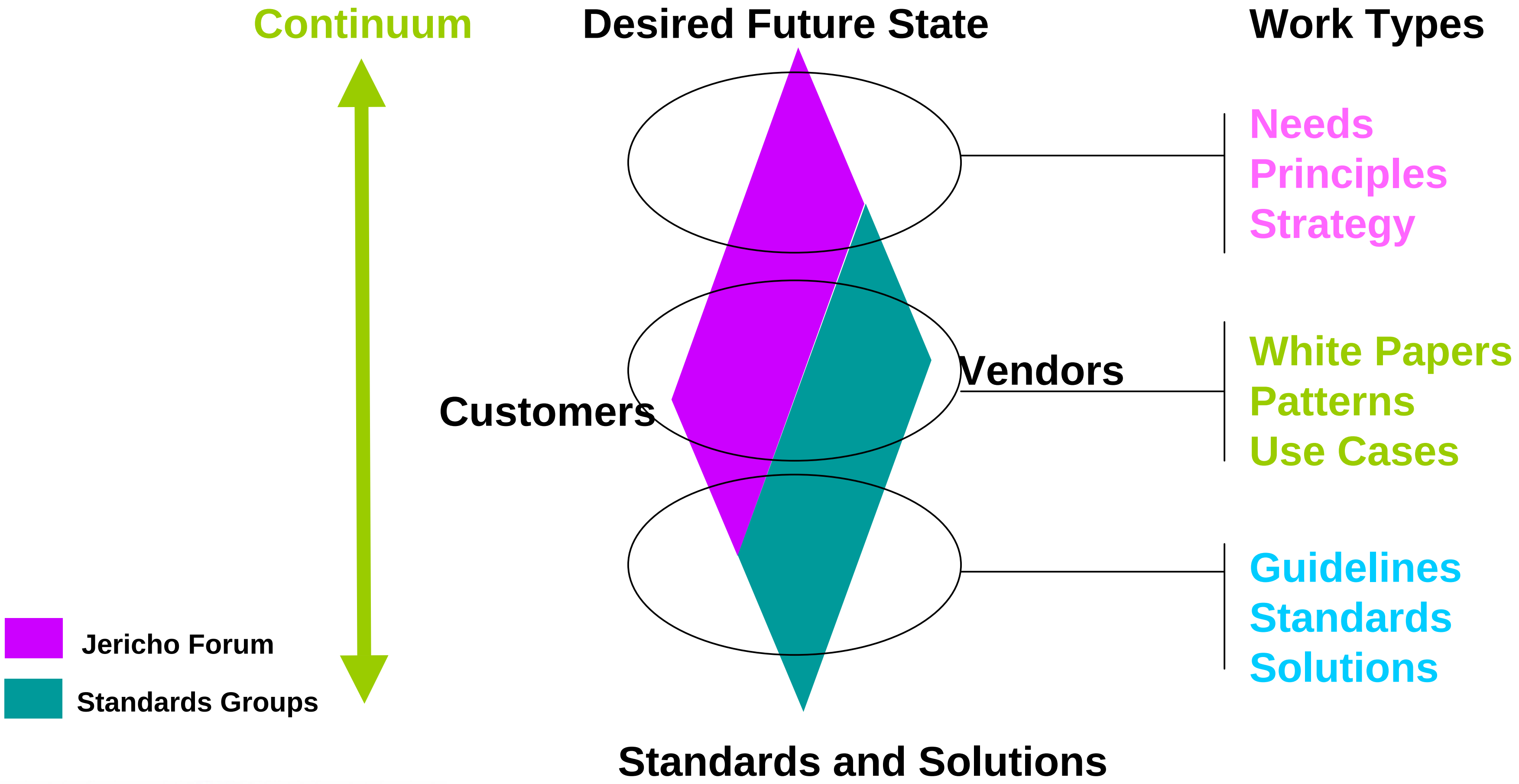
- Permissions, keys, privileges etc. must ultimately fall under independent control
  - or there will always be a weakest link at the top of the chain of trust.
- Administrator access must also be subject to these controls.

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?



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

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

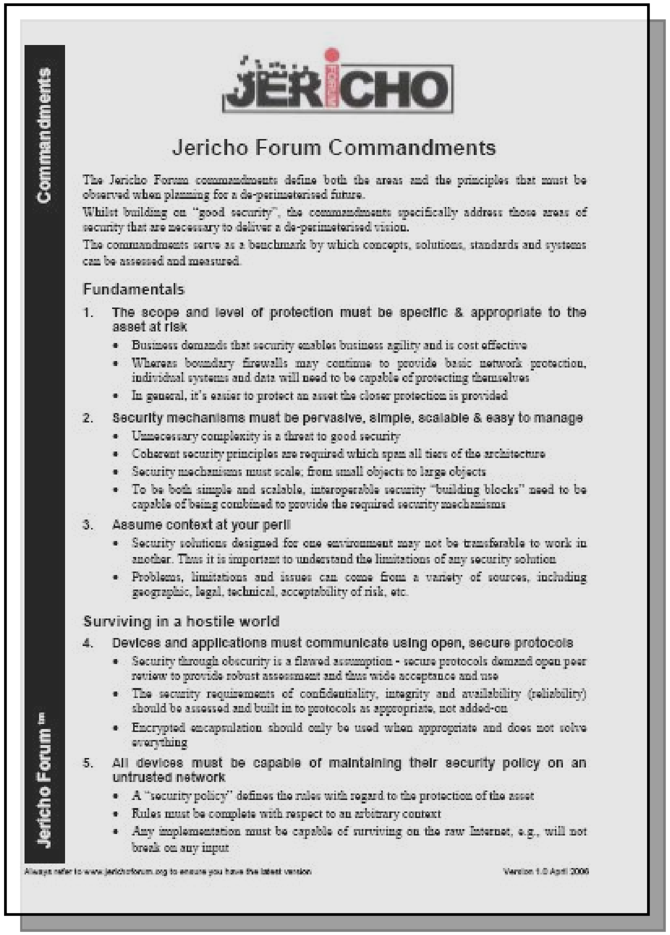
What I have crossed out I didn't like. What I haven't crossed out I'm dissatisfied with.

Cecil B. DeMille 1881-1959

Paper available from the Jericho Forum

- The Jericho Forum "Commandments" are freely available from the Jericho Forum Website

http://www.jerichoforum.org



Commandments

Jericho Forum Commandments

The Jericho Forum commandments define both the areas and the principles that must be observed when planning for a de-perimeterised future.

Whilst building on "good security", the commandments specifically address those areas of security that are necessary to deliver a de-perimeterised 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

Jericho Forum ™

Always refer to www.jerichoforum.org to ensure you have the latest version

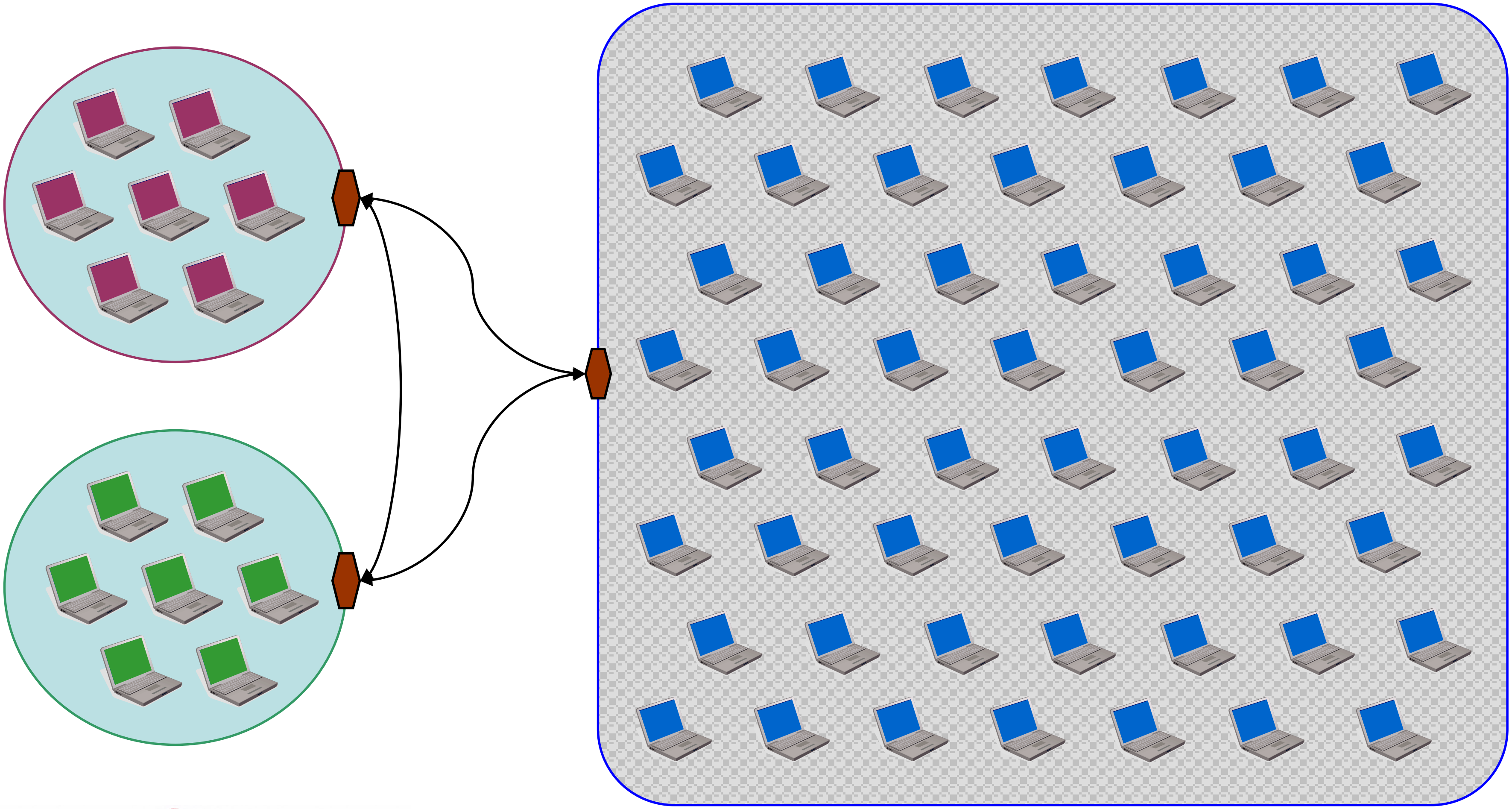
Version 1.0 April 2006

Case Study

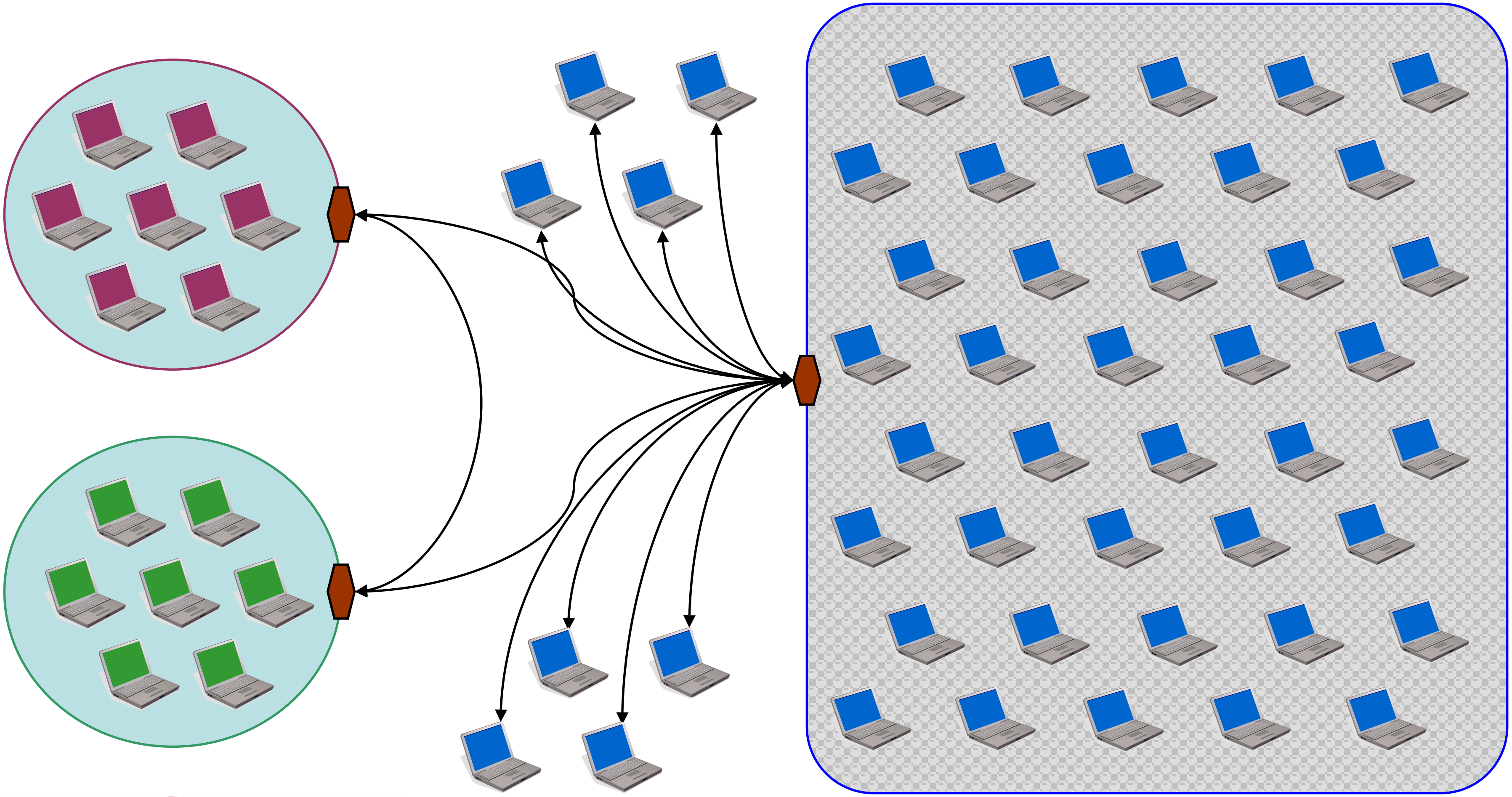
- **What Hath Vint Wrought**

- **Steve Whitlock**
  Boeing
  Chief Security Architect
  Information Protection &
  Assurance

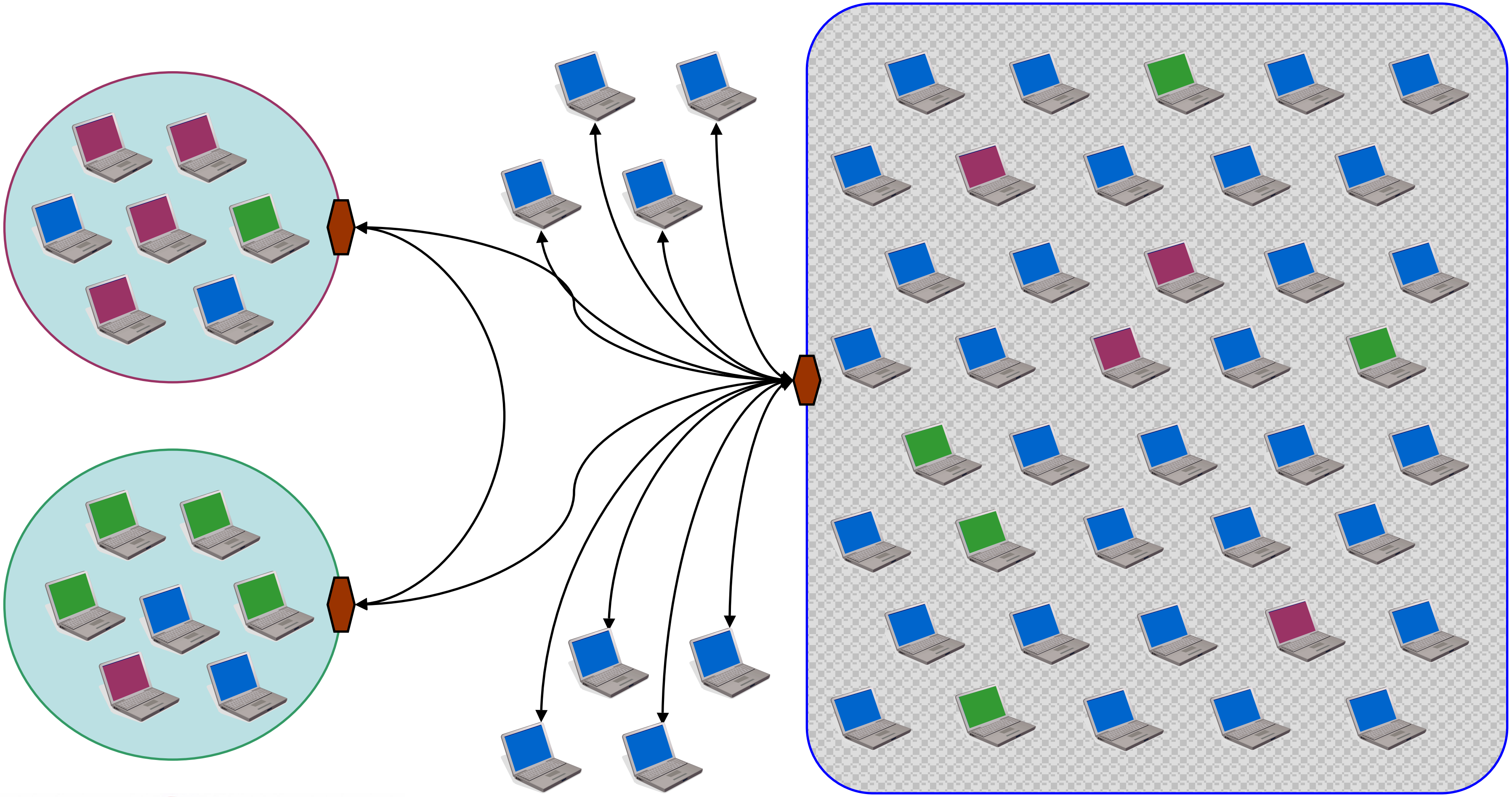
Prehistoric E-Business



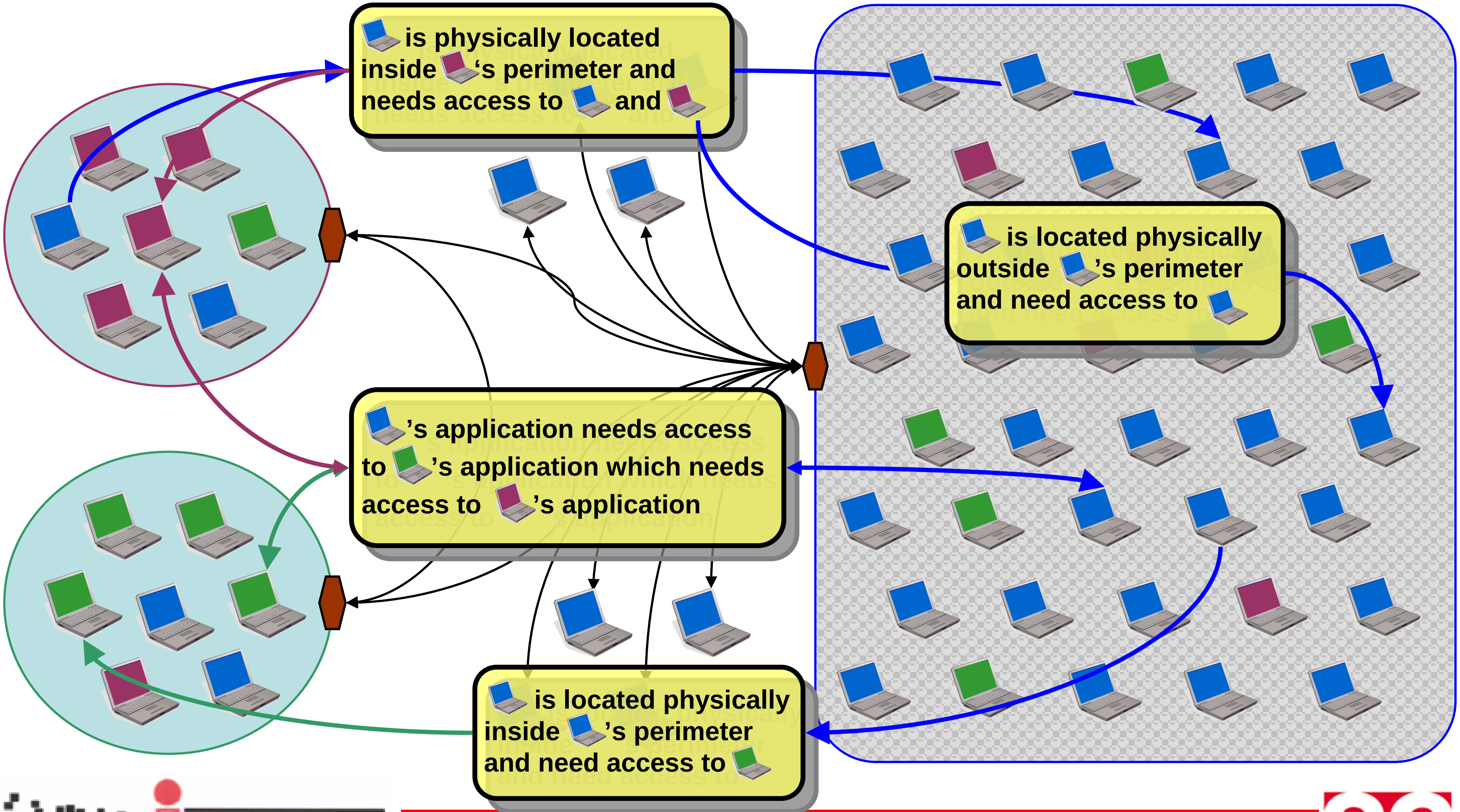
Employees moved out…



Associates moved in…



The Globalization Effect



🟦 is physically located inside 🟪 ‘s perimeter and needs access to 🟦 and 🟪

🟦 is located physically outside 🟦 ’s perimeter and need access to 🟦

🟦 ’s application needs access to 🟩 ’s application which needs access to 🟪 ’s application

🟦 is located physically inside 🟦 ’s perimeter and need access to 🟩

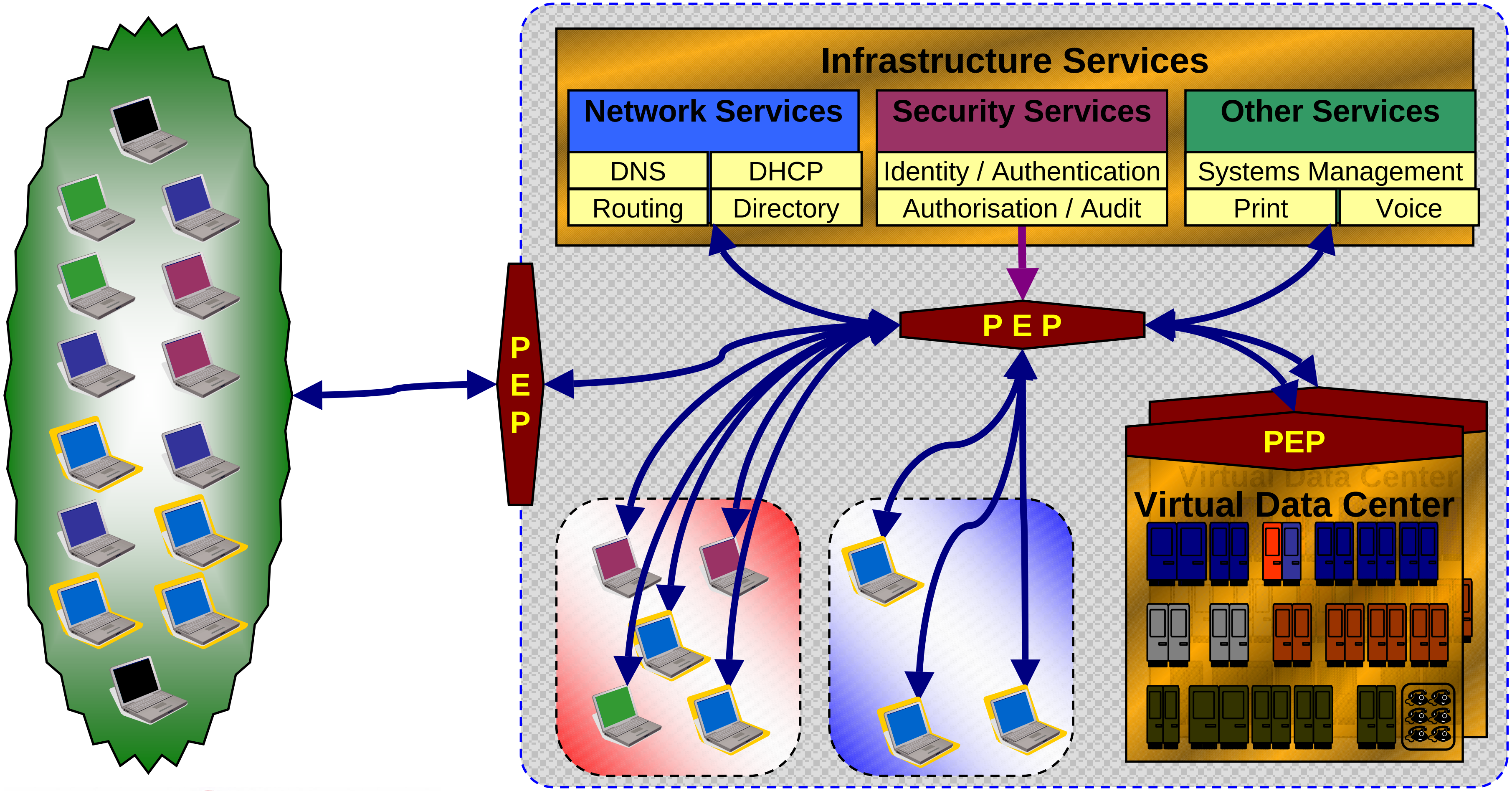
De-perimeterisation

- **De-perimeterisation…**

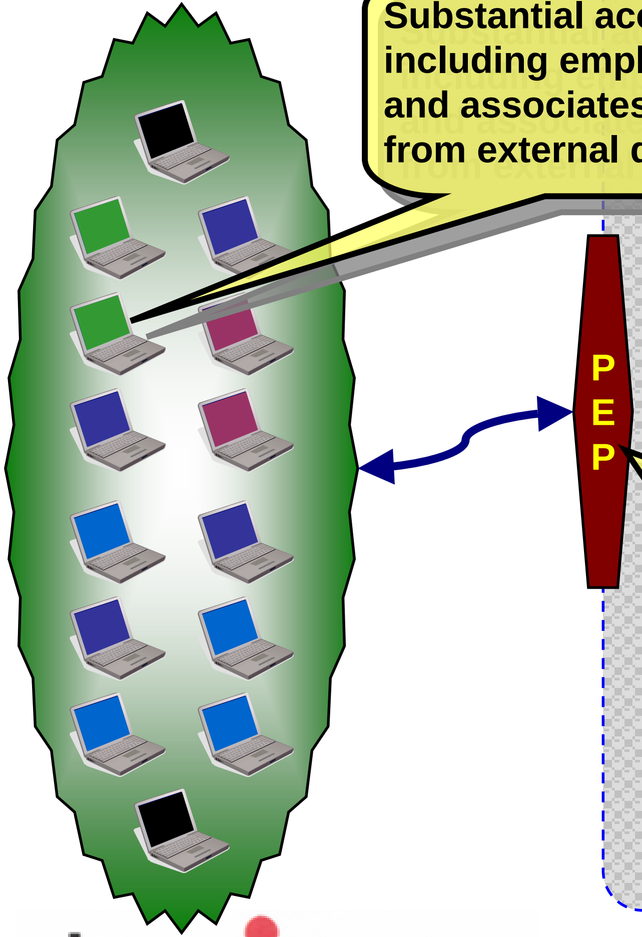
  … is not a security strategy

  … 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



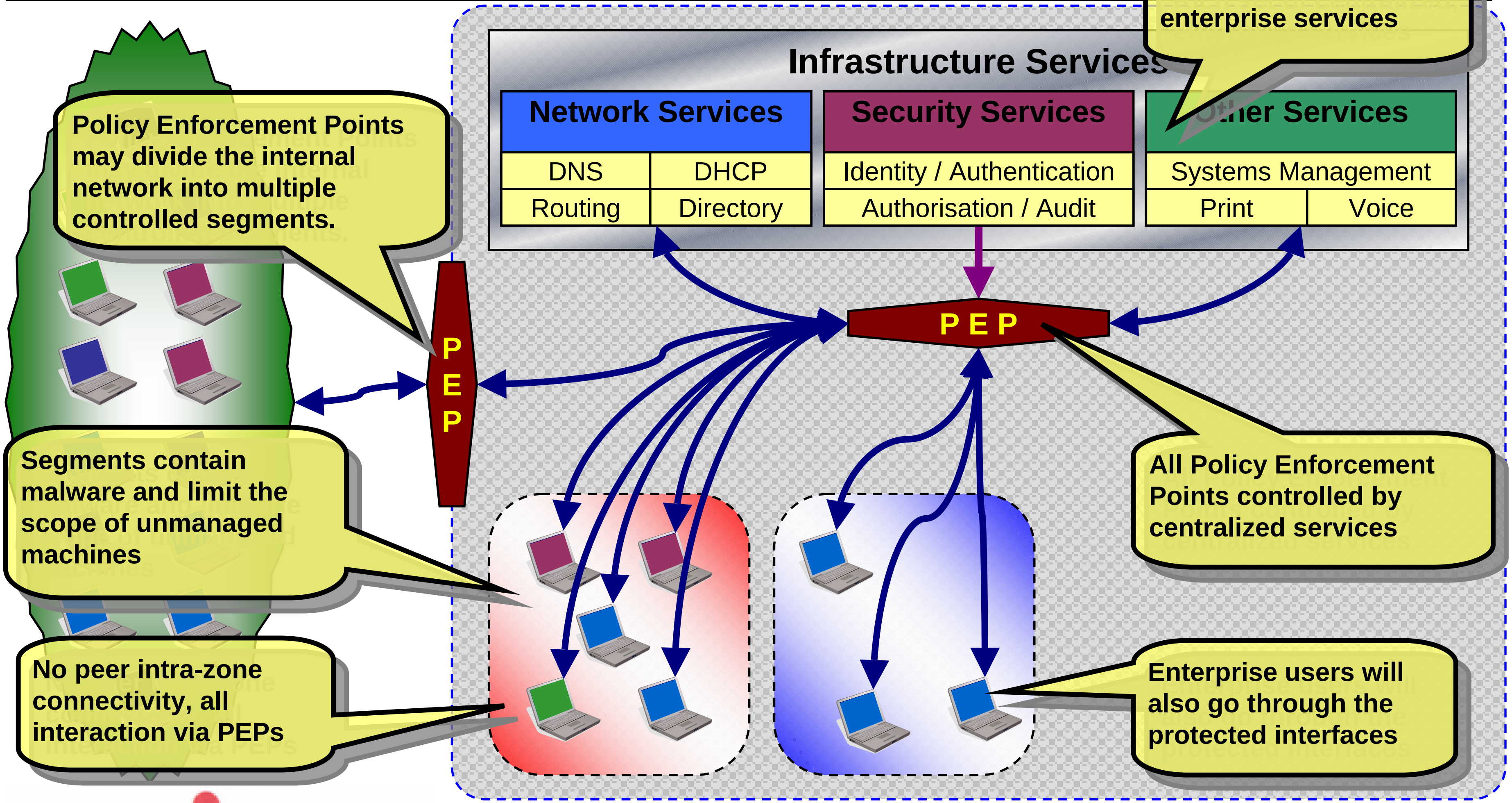
Substantial access, including employees and associates will be from external devices

An externally facing policy enforcement point demarks a thin perimeter between outside and inside and provides these services:

Legal and Regulatory
- Provide a legal entrance for enterprise
- Provide notice to users that they are entering a private network domain
- Provide brand protection
- Enterprise dictates the terms of use
- Enterprise has legal recourse for trespassers

Availability
- Filter unwanted network noise
- Block spam, viruses, and probes
- Preserve bandwidth, for corporate business
- Preserve access to unauthenticated but authorised information (e.g. public web site)

Defense Layer 2: Network Access Control



Rich set of centralized, enterprise services

Policy Enforcement Points may divide the internal network into multiple controlled segments.

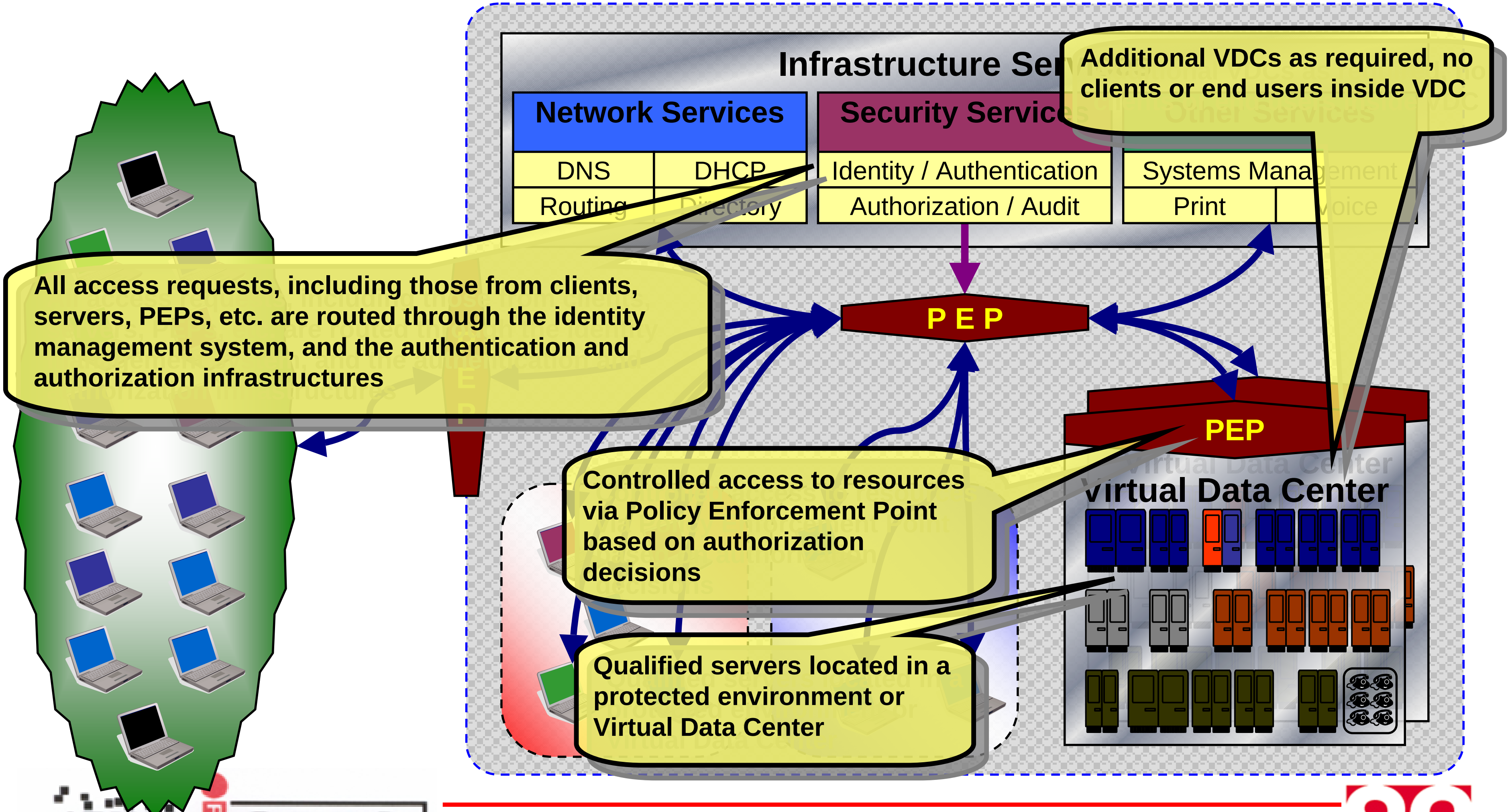
Segments contain malware and limit the scope of unmanaged machines

No peer intra-zone connectivity, all interaction via PEPs

All Policy Enforcement Points controlled by centralized services

Enterprise users will also go through the protected interfaces

Defense Layer 3: Resource Access Control



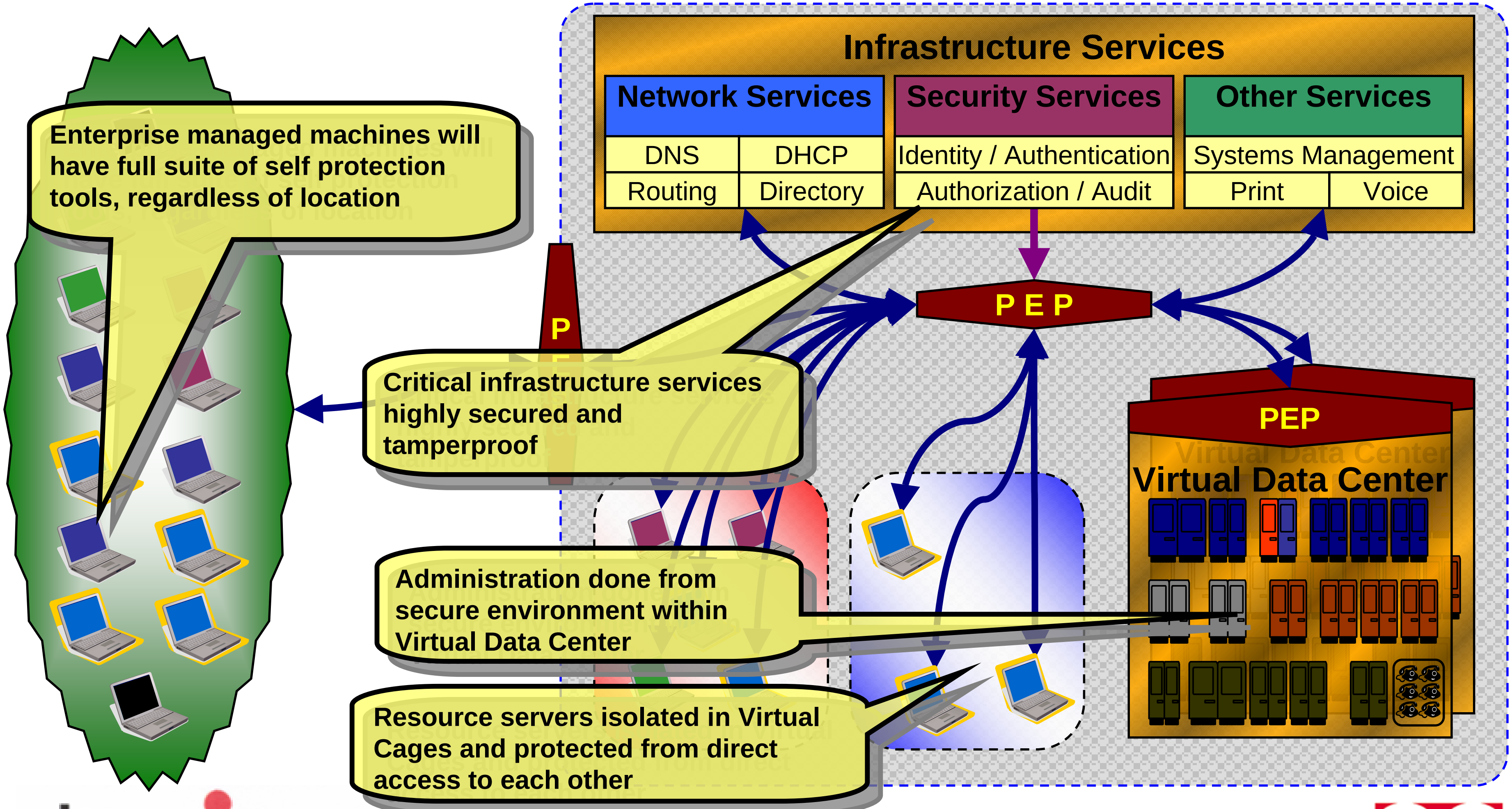
Additional VDCs as required, no clients or end users inside VDC

All access requests, including those from clients, servers, PEPs, etc. are routed through the identity management system, and the authentication and authorization infrastructures

Controlled access to resources via Policy Enforcement Point based on authorization decisions

Qualified servers located in a protected environment or Virtual Data Center

Defense Layer 4: Resource Availability



Enterprise managed machines will have full suite of self protection tools, regardless of location

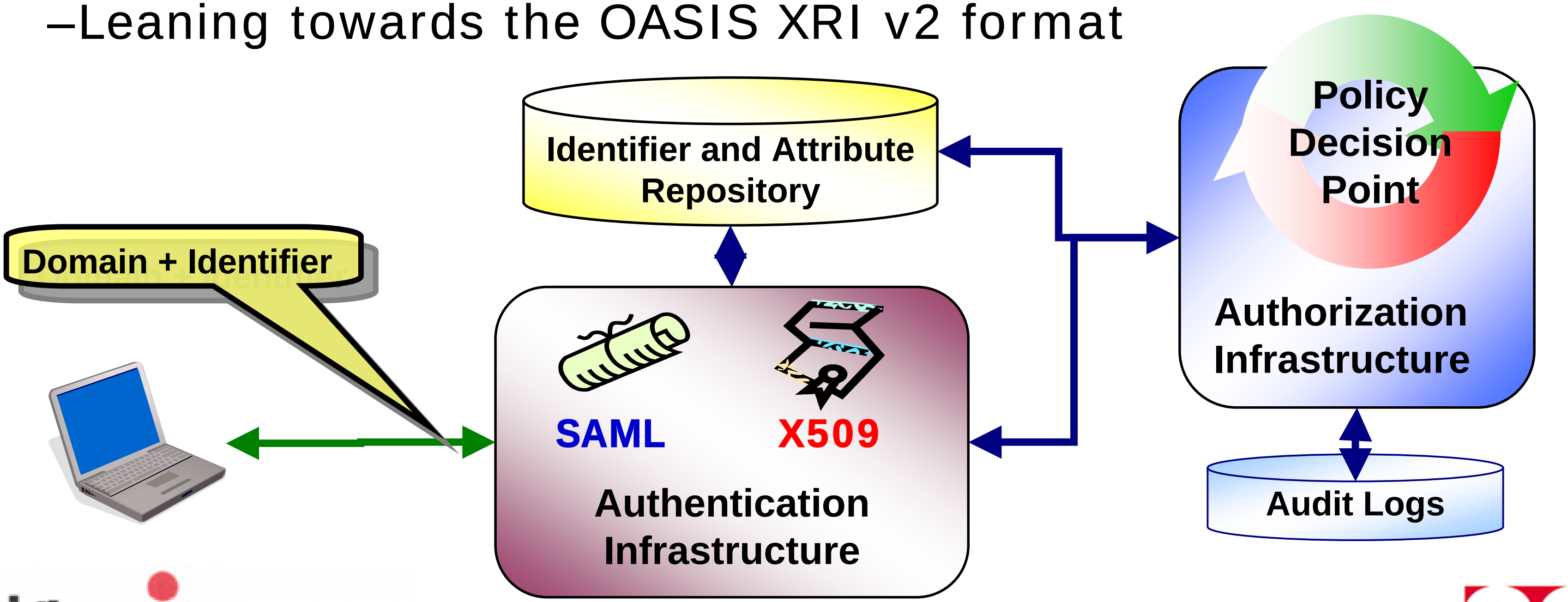
Critical infrastructure services highly secured and tamperproof

Administration done from secure environment within Virtual Data Center

Resource servers isolated in Virtual Cages and protected from direct access to each other

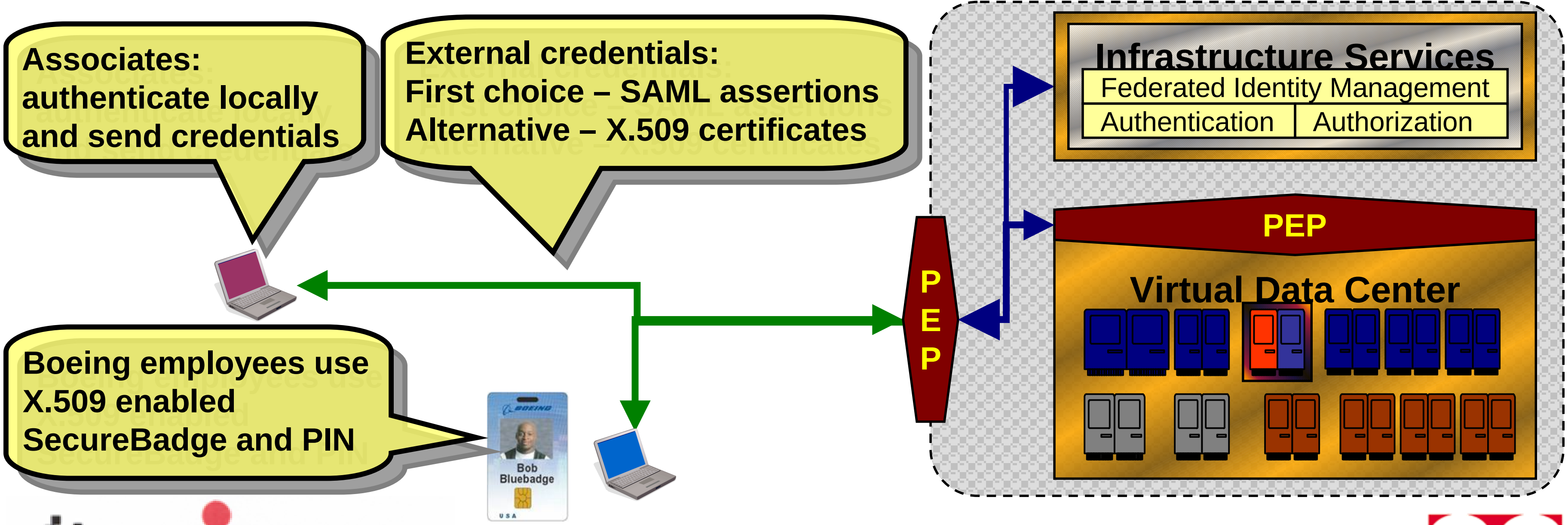
Identity Management Infrastructure

- 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


Identifier and Attribute Repository
Policy Decision Point
Domain + Identifier
Authorization Infrastructure
SAML
X509
Authentication Infrastructure
Audit Logs

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



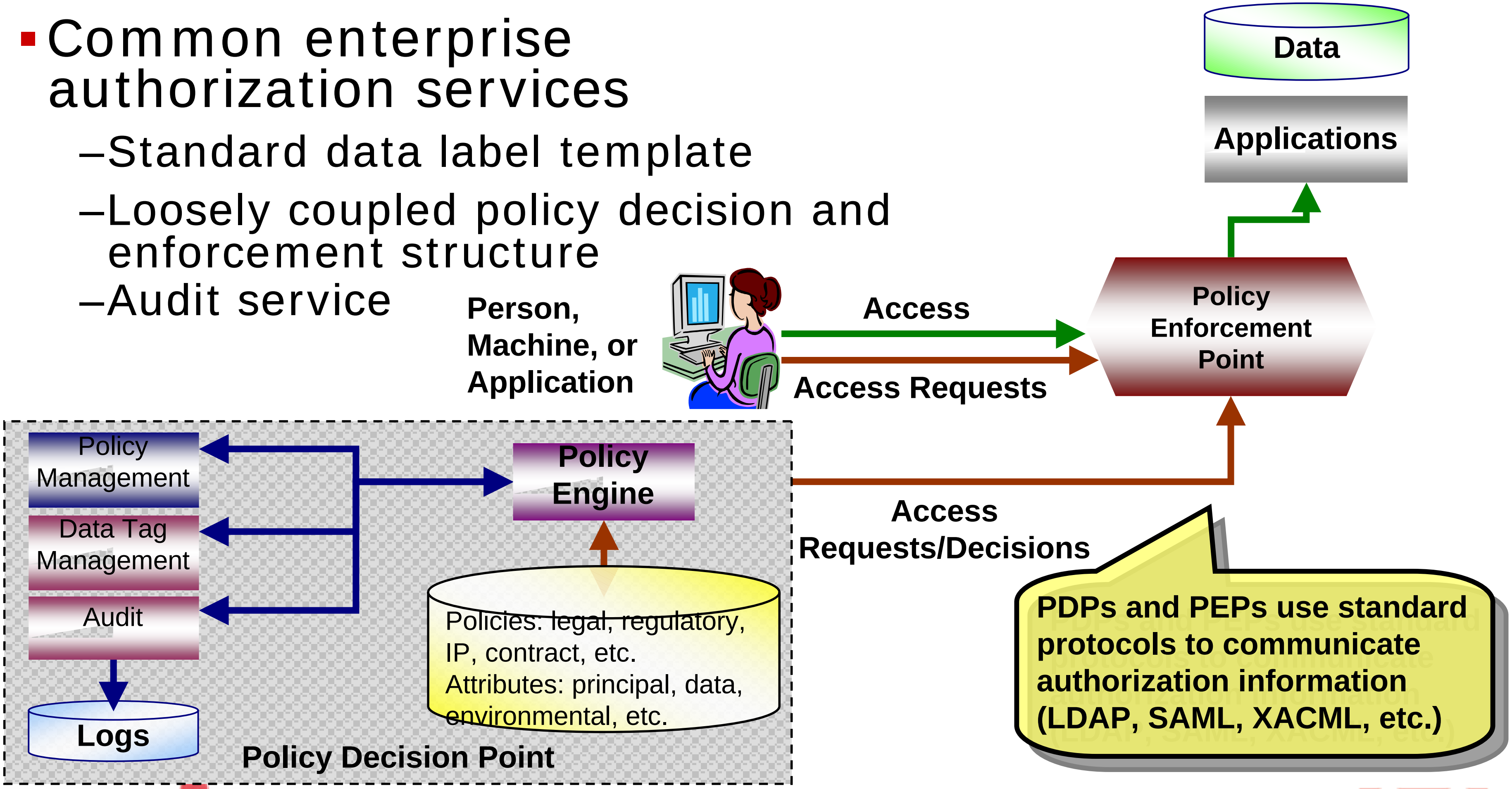
Associates: authenticate locally and send credentials

External credentials:
First choice – SAML assertions
Alternative – X.509 certificates

Boeing employees use X.509 enabled SecureBadge and PIN

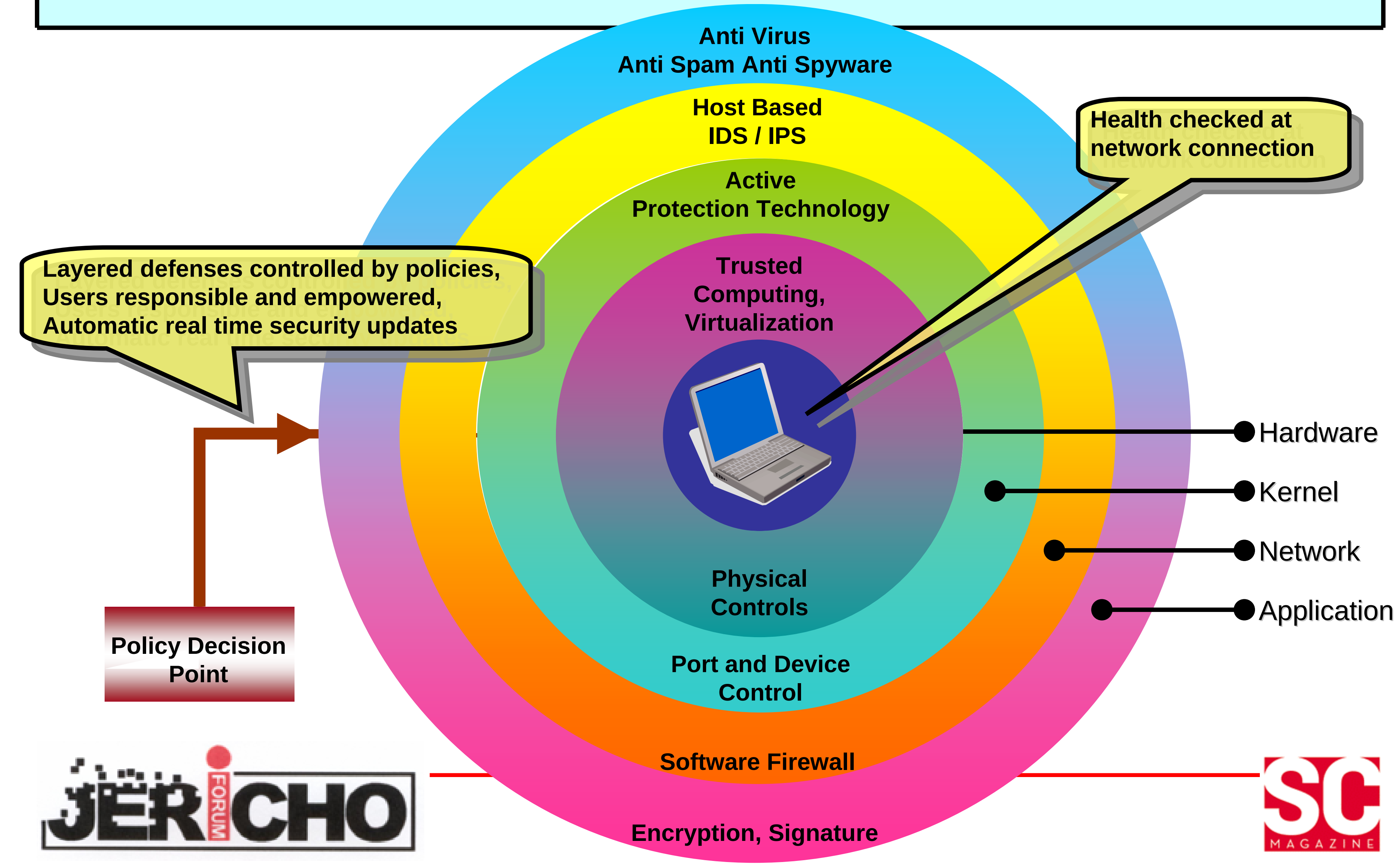
Authorization Infrastructure

- Common enterprise authorization services
  - Standard data label template
  - Loosely coupled policy decision and enforcement structure
  - Audit service

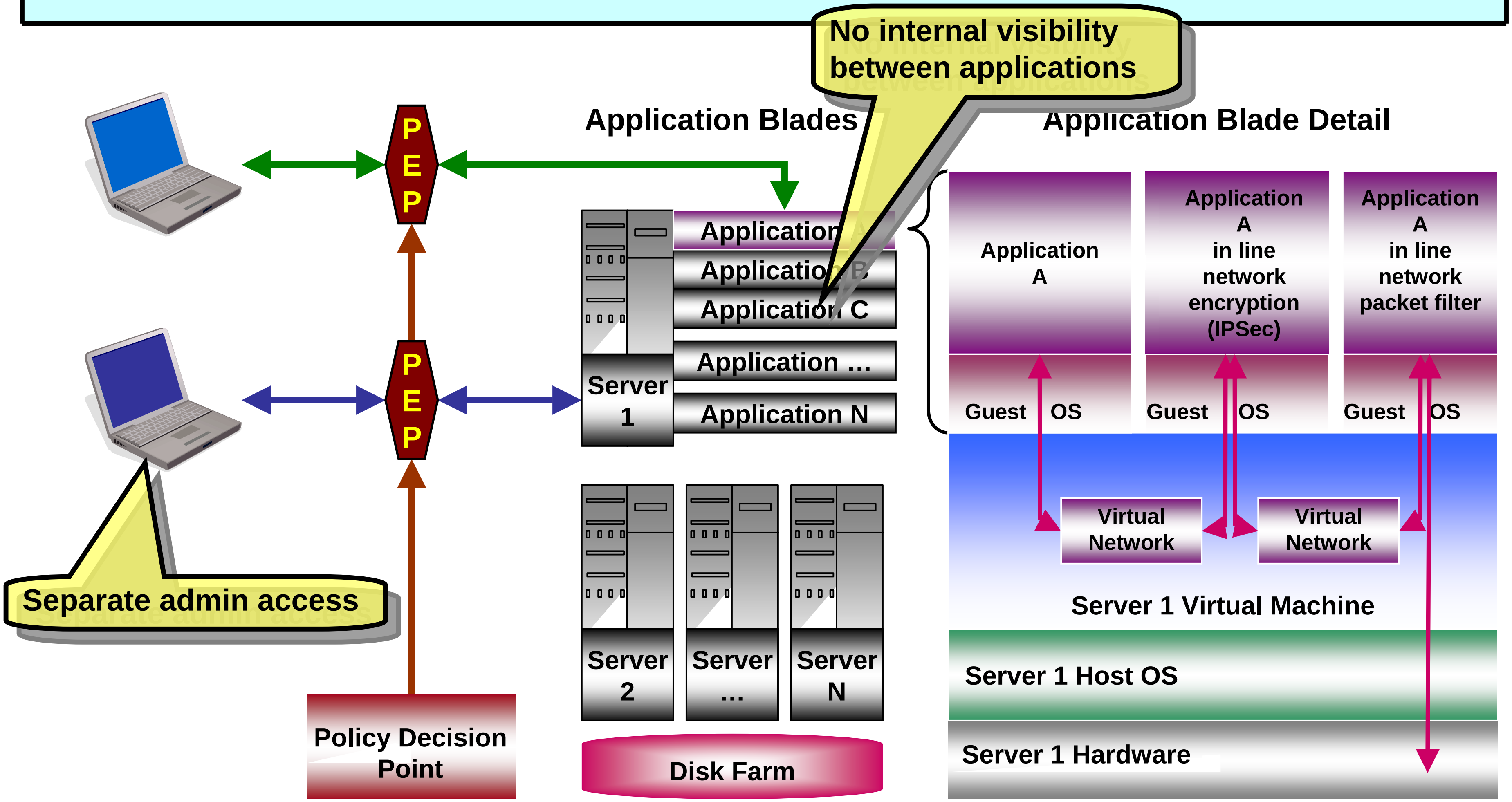

Data
Applications
Person, Machine, or Application
Access
Access Requests
Policy Enforcement Point
Access Requests/Decisions
Policy Management
Data Tag Management
Audit
Logs
Policy Engine
Policies: legal, regulatory, IP, contract, etc.
Attributes: principal, data, environmental, etc.
Policy Decision Point

PDPs and PEPs use standard protocols to communicate authorization information (LDAP, SAML, XACML, etc.)

Resource Availability: Desktop



Resource Availability: Server / Application



No internal visibility between applications

Application Blades

Application Blade Detail

P E P

P E P

Server 1

Application A

Application B

Application C

Application …

Application N

Application A

Application A in line network encryption (IPSec)

Application A in line network packet filter

Guest OS

Guest OS

Guest OS

Virtual Network

Virtual Network

Server 1 Virtual Machine

Server 1 Host OS

Server 1 Hardware

Server 2

Server …

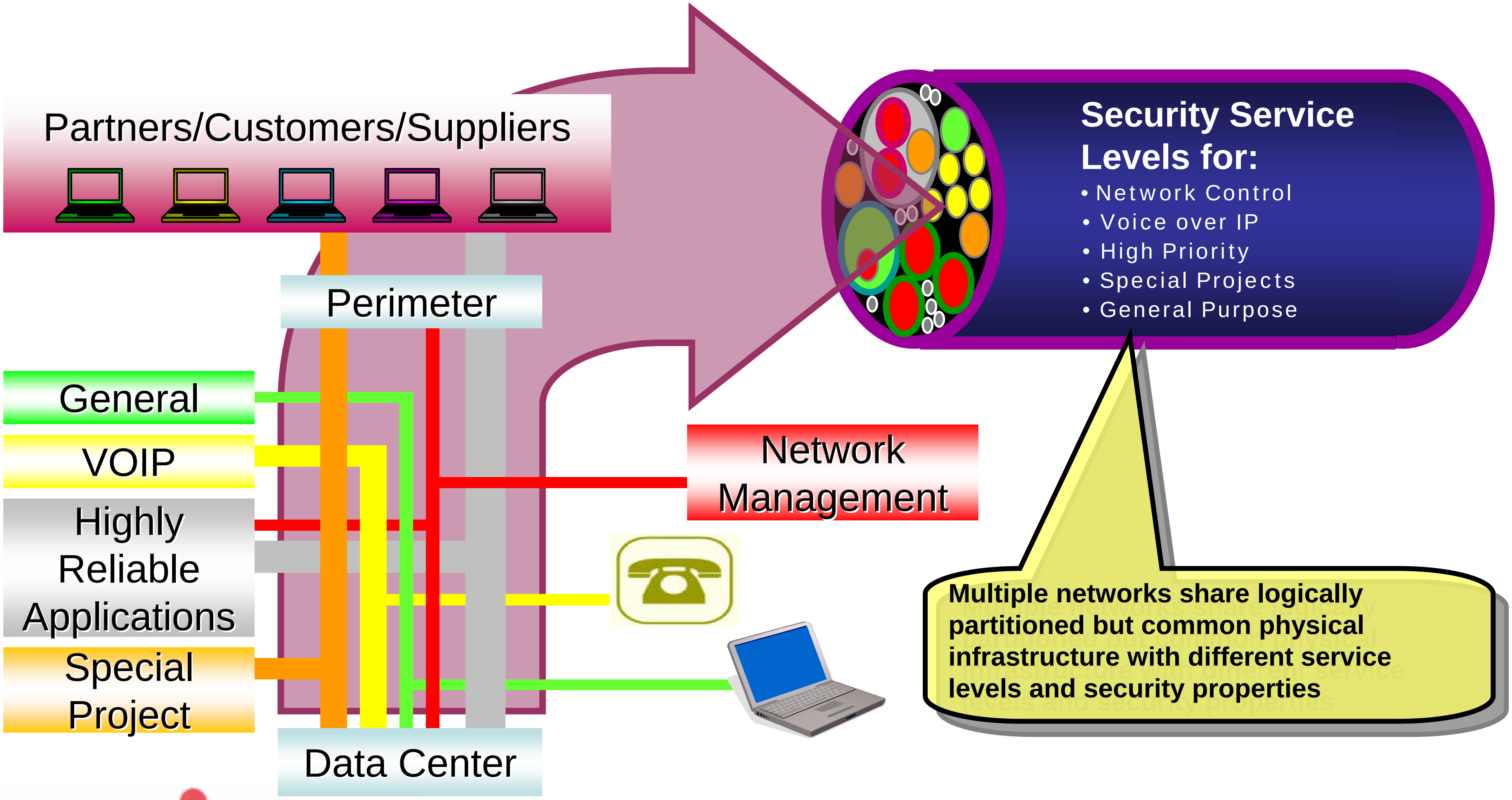
Server N

Disk Farm

Policy Decision Point

Separate admin access

Resource Availability: Network



Partners/Customers/Suppliers

Perimeter

General

VOIP

Highly Reliable Applications

Special Project

Data Center

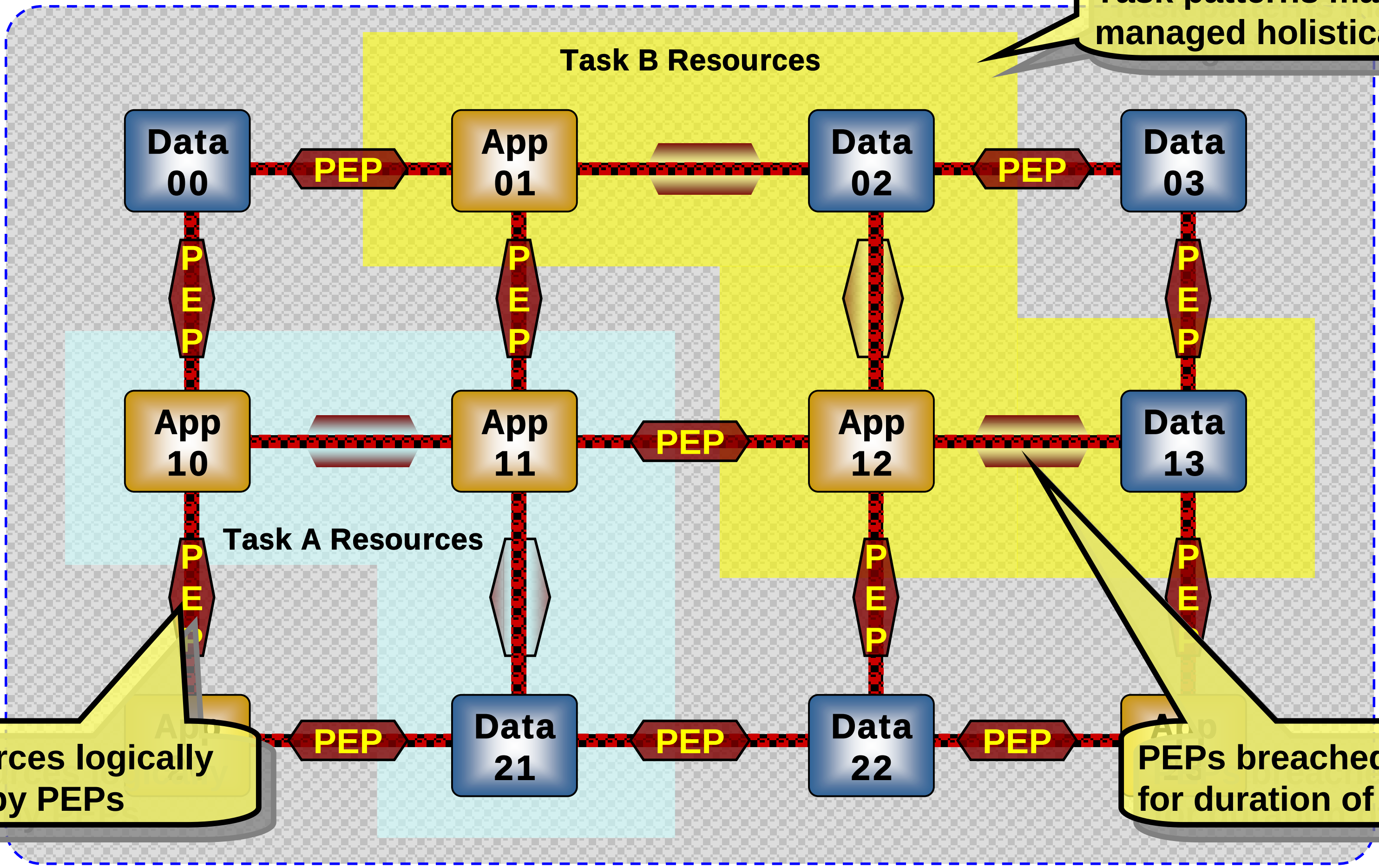
Network Management

Security Service Levels for:

- Network Control
- Voice over IP
- High Priority
- Special Projects
- General Purpose

Multiple networks share logically partitioned but common physical infrastructure with different service levels and security properties

Availability: Logical View

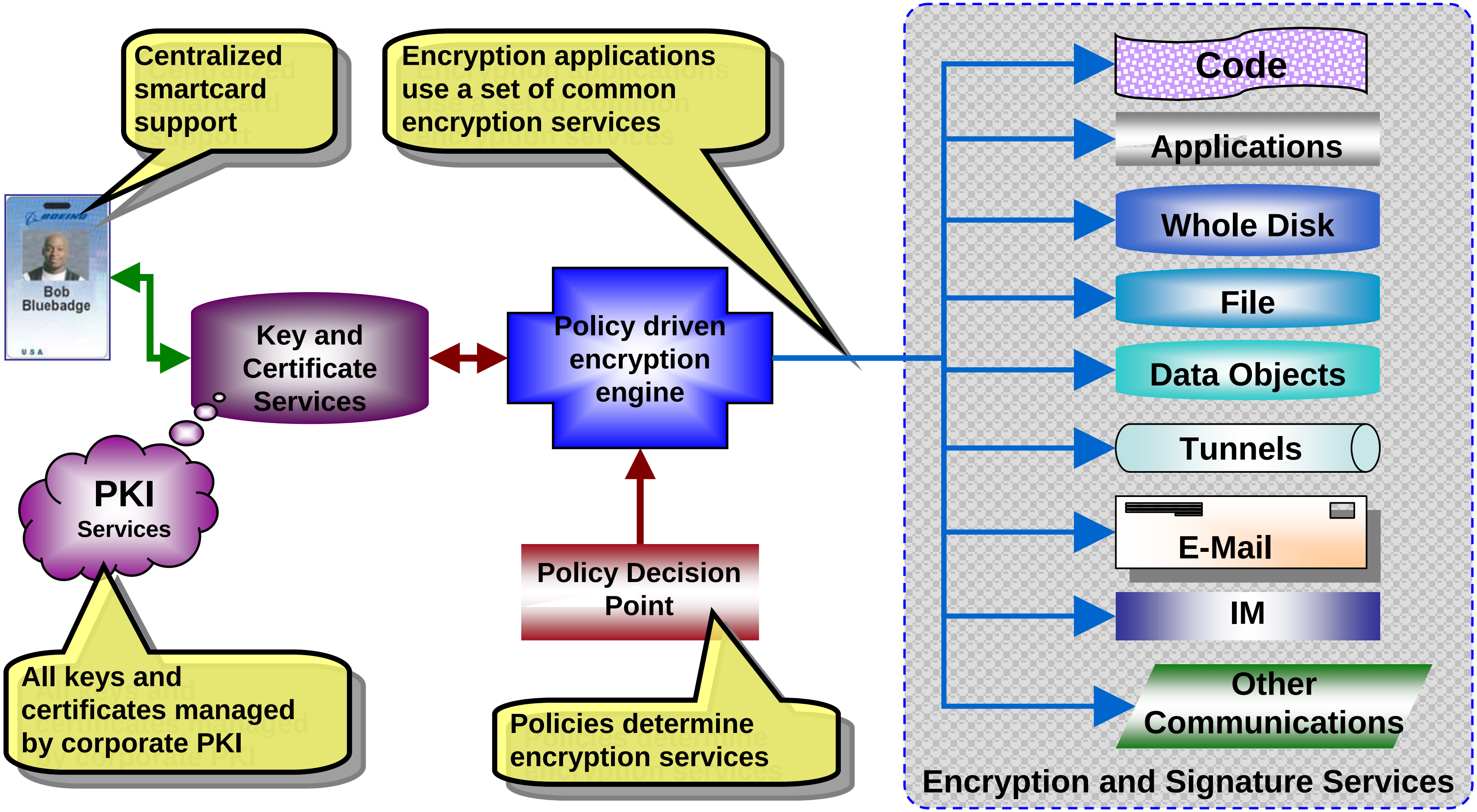


Task patterns may be managed holistically

All resources logically isolated by PEPs

PEPs breached only for duration of task

Supporting Services: Cryptographic Services



Centralized smartcard support

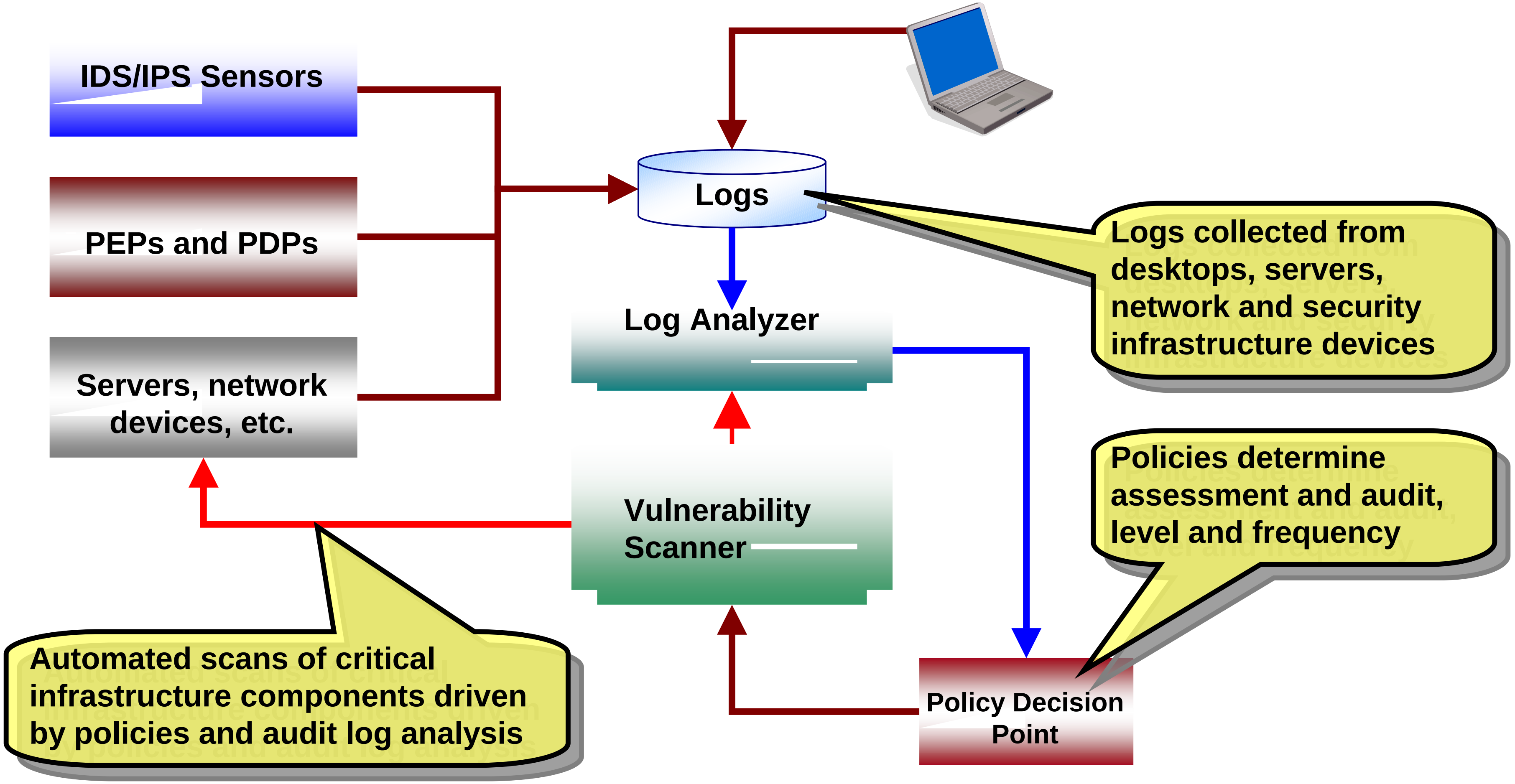
Encryption applications use a set of common encryption services

All keys and certificates managed by corporate PKI

Policies determine encryption services

Encryption and Signature Services

Supporting Services: Assessment and Audit Services

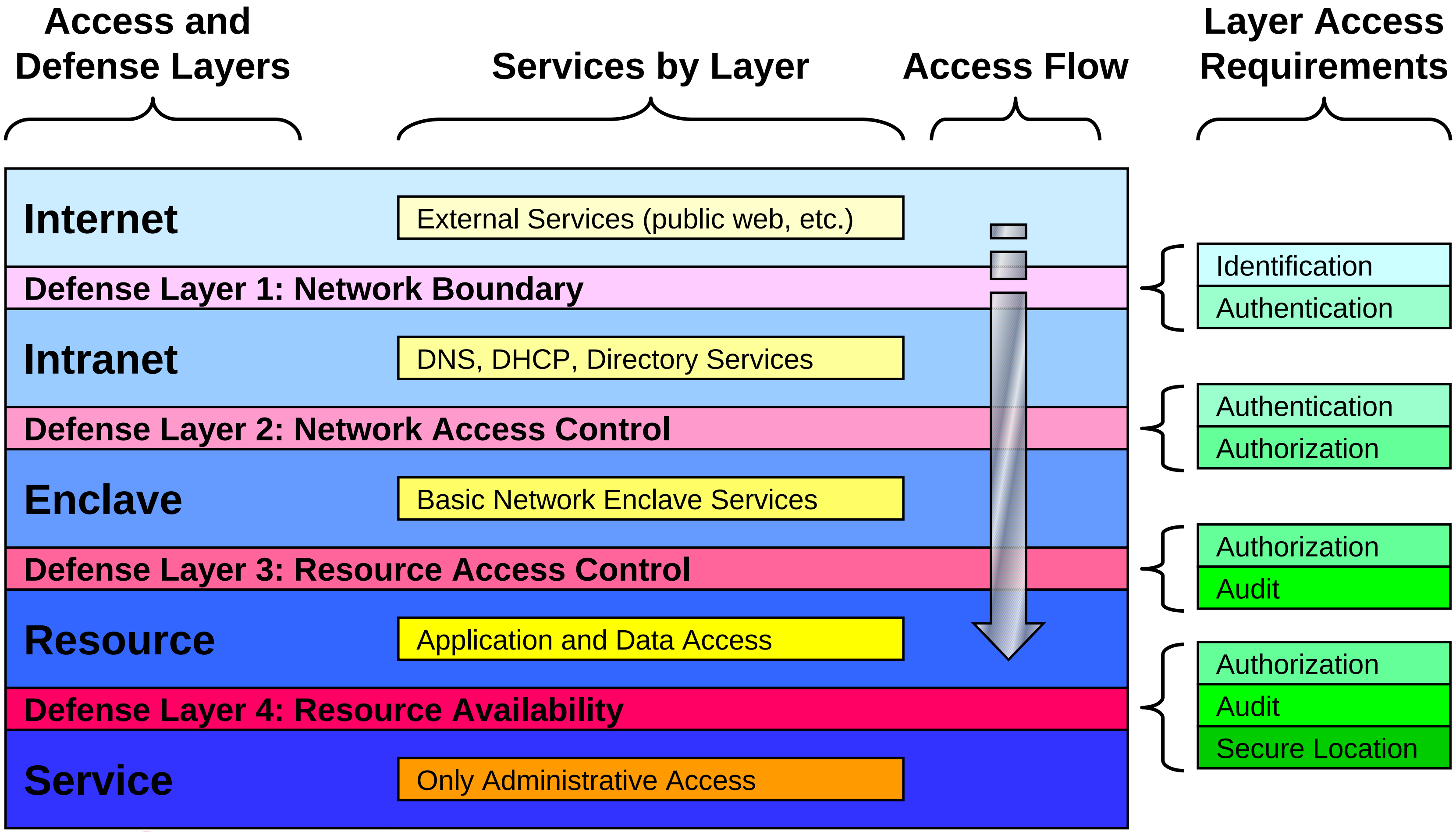


Logs collected from desktops, servers, network and security infrastructure devices

Policies determine assessment and audit, level and frequency

Automated scans of critical infrastructure components driven by policies and audit log analysis

Protection Layer Summary



Access and Defense Layers

Services by Layer

Access Flow

Layer Access Requirements

Internet

External Services (public web, etc.)

Defense Layer 1: Network Boundary

Identification

Authentication

Intranet

DNS, DHCP, Directory Services

Defense Layer 2: Network Access Control

Authentication

Authorization

Enclave

Basic Network Enclave Services

Defense Layer 3: Resource Access Control

Authorization

Audit

Resource

Application and Data Access

Defense Layer 4: Resource Availability

Authorization

Audit

Secure Location

Service

Only Administrative Access

Real world application

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

SC MAGAZINE
AWARDS
2006

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

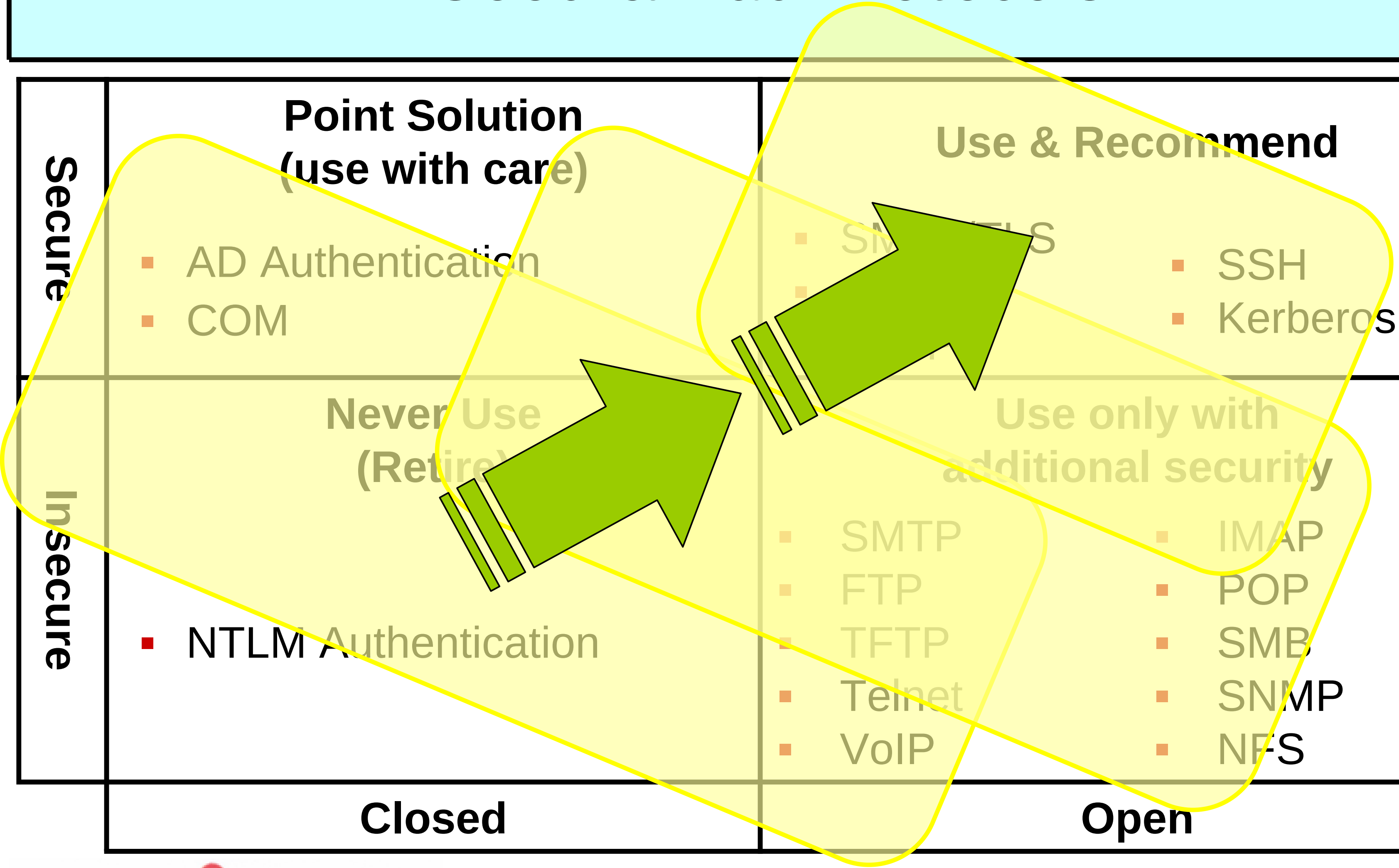
Proprietary Solutions

- 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



	Closed	Open
Secure	**Point Solution (use with care)** AD Authentication COM	**Use & Recommend** SMTP/TLS [illegible] SSH Kerberos
Insecure	**Never Use (Retire)** NTLM Authentication	**Use only with additional security** SMTP FTP TFTP Telnet VoIP IMAP POP SMB SNMP NFS

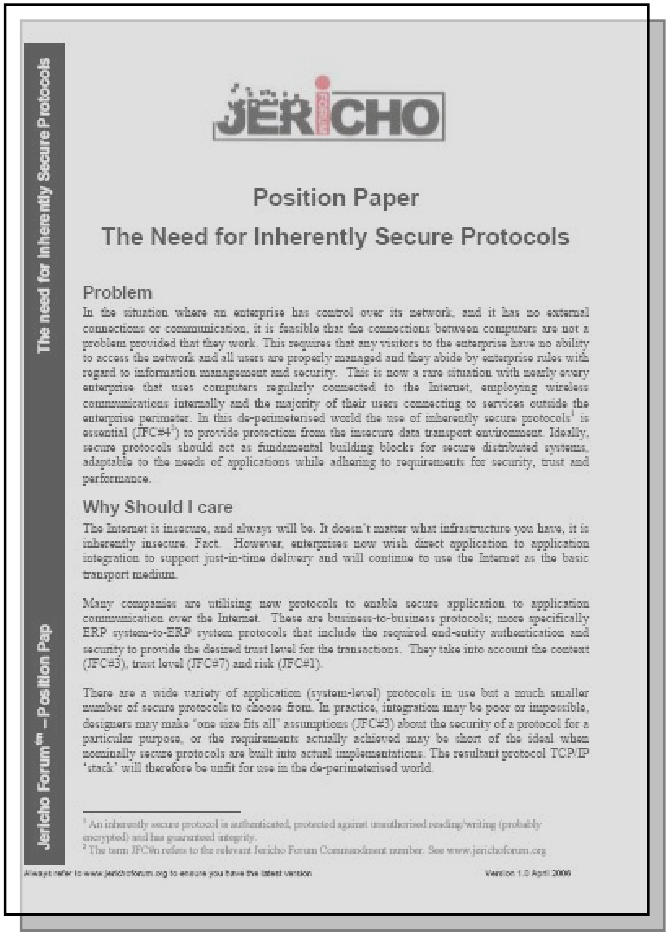
Implementing new systems

- 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



The need for Inherently Secure Protocols

Jericho Forum™ – Position Pap

Position Paper

The Need for Inherently Secure Protocols

Problem

In the situation where an enterprise has control over its network, and it has no external connections or communication, it is feasible that the connections between computers are not a problem provided that they work. This requires that any visitors to the enterprise have no ability to access the network and all users are properly managed and they abide by enterprise rules with regard to information management and security. This is now a rare situation with nearly every enterprise that uses computers regularly connected to the Internet, employing wireless communications internally and the majority of their users connecting to services outside the enterprise perimeter. In this de-perimeterised world the use of inherently secure protocols[1] is essential (JFC#4[2]) to provide protection from the insecure data transport environment. Ideally, 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.

Why Should I care

The Internet is insecure, and always will be. It doesn`t matter what infrastructure you have, it is inherently insecure. Fact. However, enterprises now wish direct application to application integration to support just-in-time delivery and will continue to use the Internet as the basic transport medium.

Many companies are utilising new protocols to enable secure application to application communication over the Internet. These are 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 (JFC#3), trust level (JFC#7) and risk (JFC#1).

There are a wide variety of application (system-level) protocols in use but a much smaller number of secure protocols to choose from. In practice, integration may be poor or impossible, designers may make "one size fits all" assumptions (JFC#3) about the security of a protocol for a particular purpose, or the requirements actually achieved may be short of the ideal when nominally secure protocols are built into actual implementations. The resultant protocol TCP/IP 'stack' will therefore be unfit for use in the de-perimeterised world.

[1] An inherently secure protocol is authenticated, protected against unauthorised reading/writing (probably encrypted) and has guaranteed integrity.
[2] The term JFC#n refers to the relevant Jericho Forum Commandment number. See www.jerichoforum.org

Always refer to www.jerichoforum.org to ensure you have the latest version

Version 1.0 April 2006

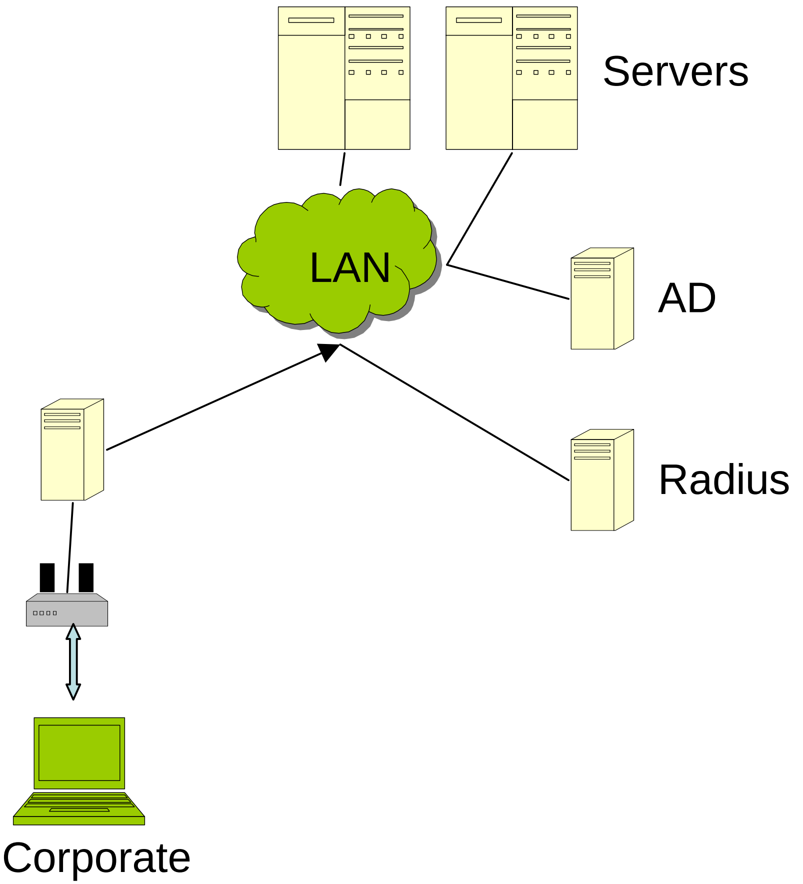
Real world application

- **Corporate Wireless Networking**
- **Andrew Yeomans**
  DrKW &
  Jericho Forum Board

SC MAGAZINE
AWARDS
2006

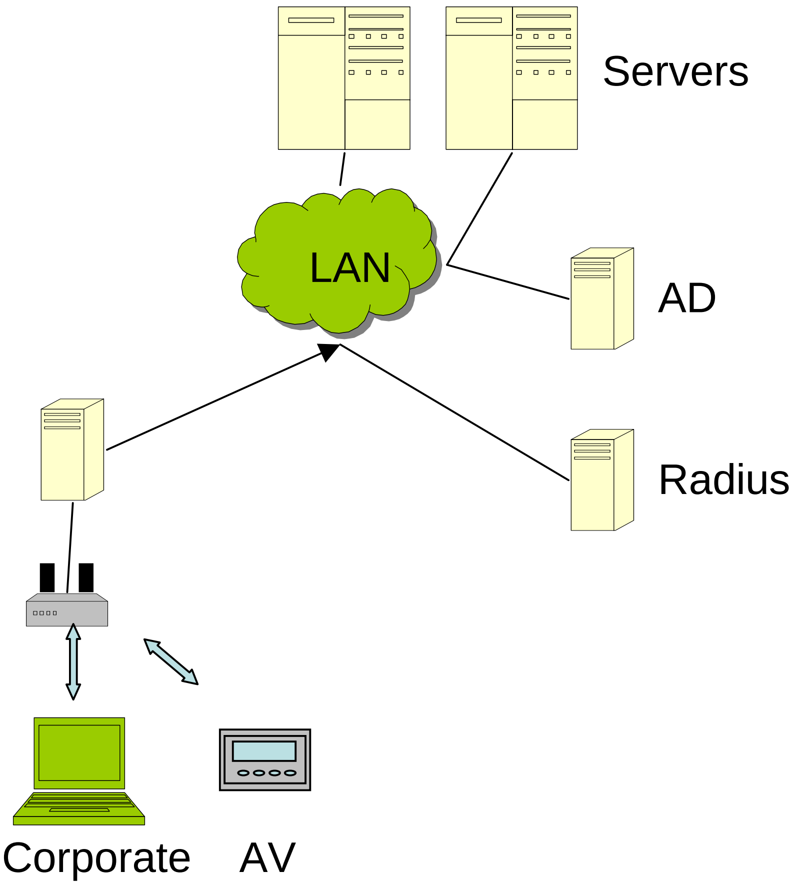
Secure wireless connection to LAN

- 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?

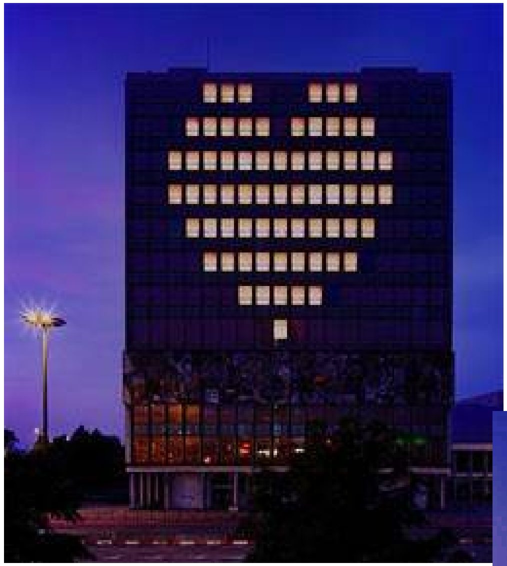
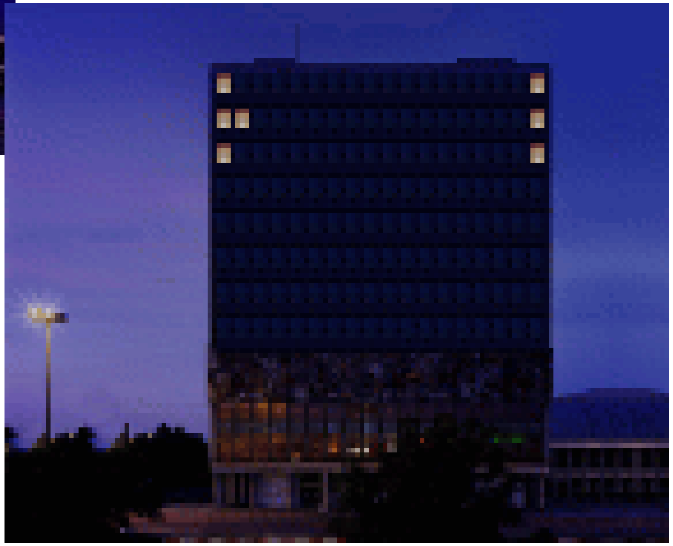


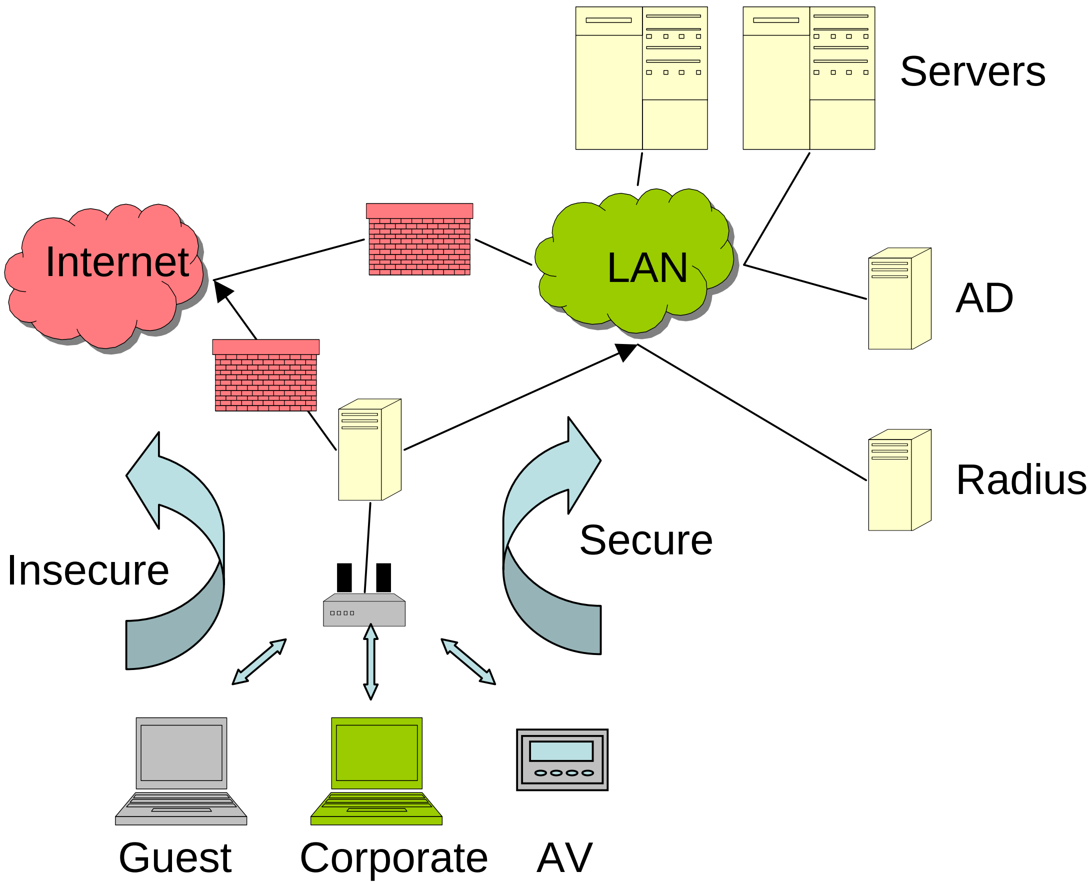
Photo: Dorit Günter, Nadja Hannaske



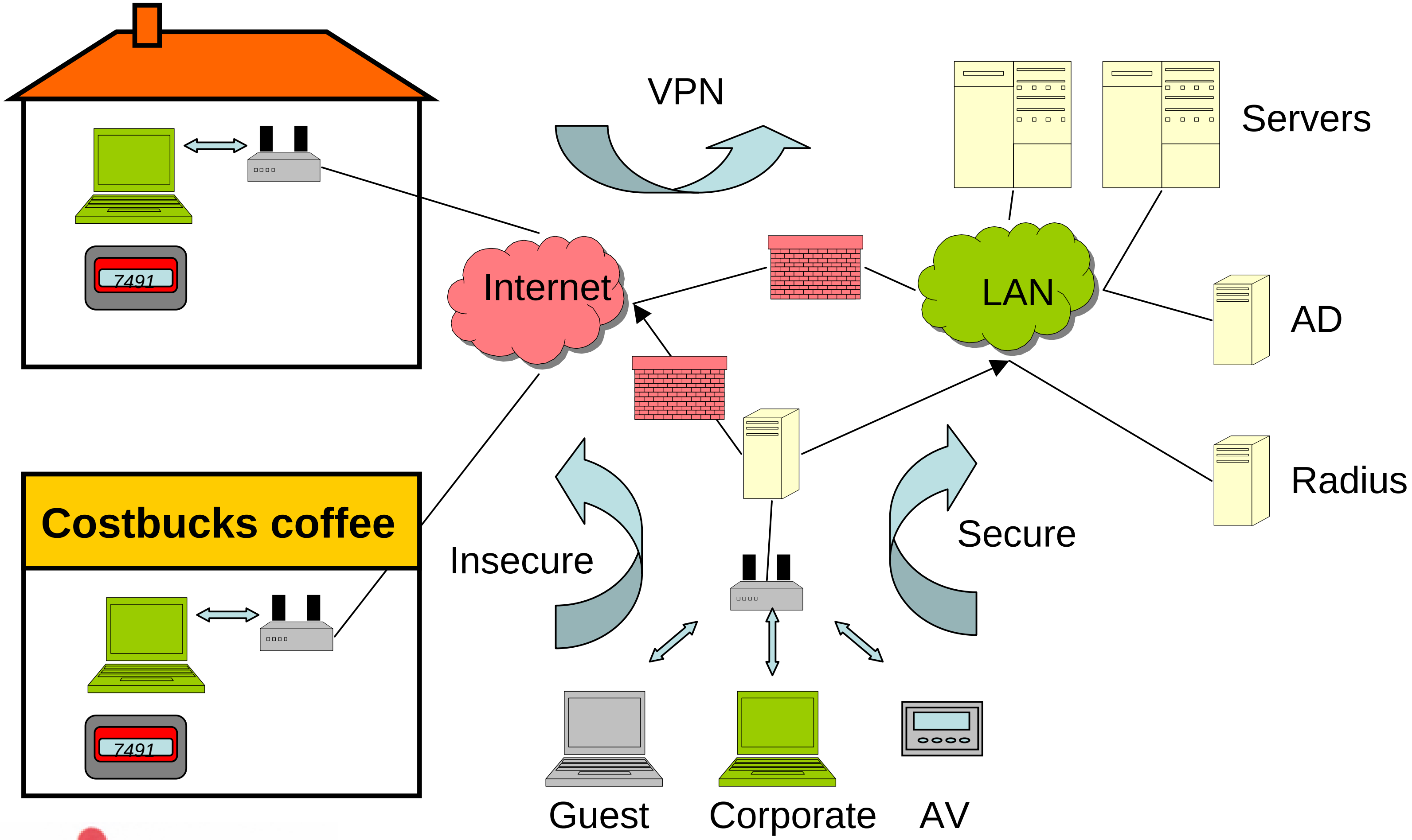
- Play <Pong> with mobile phone!

Guest internet access too

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



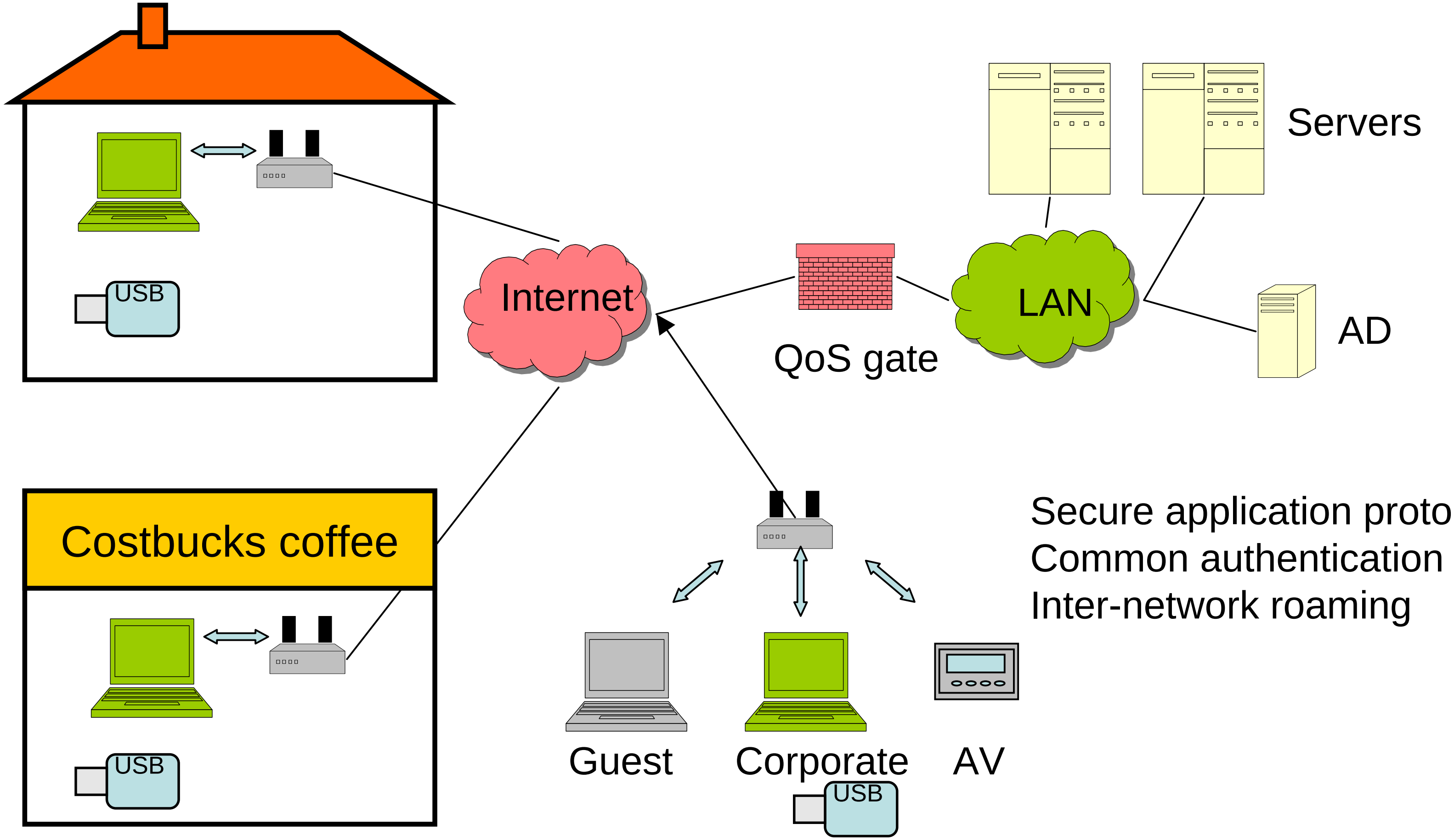
Laptops also used at home or in café



Security complexity

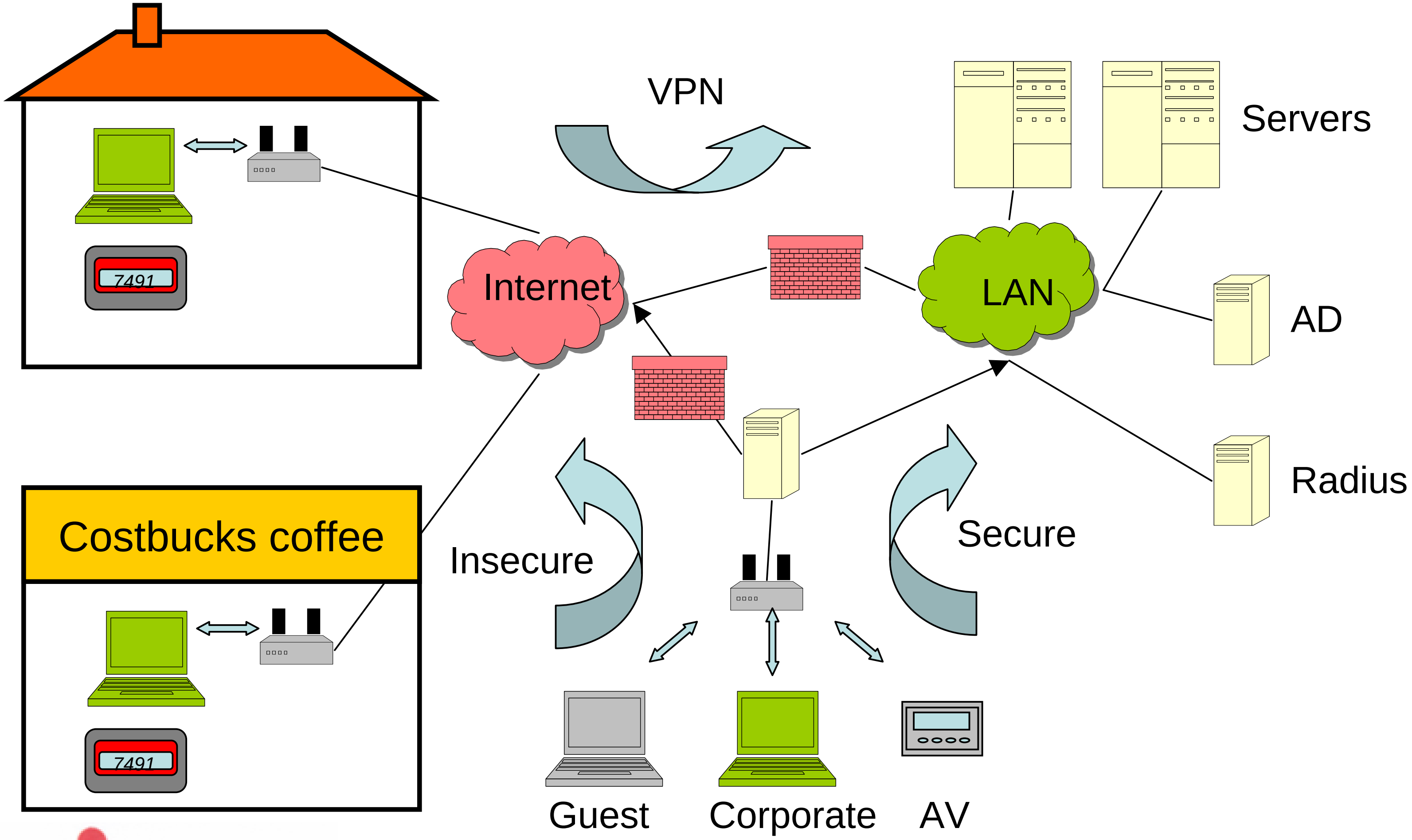
- Need location awareness
- 802.11i if corporate wireless link
- VPN if not corporate
- Still not perfect security, insecure connections needed to set up café/home connections
- Security on direct connections too

Jericho visions



Secure application protocols
Common authentication
Inter-network roaming

Today’s complexity



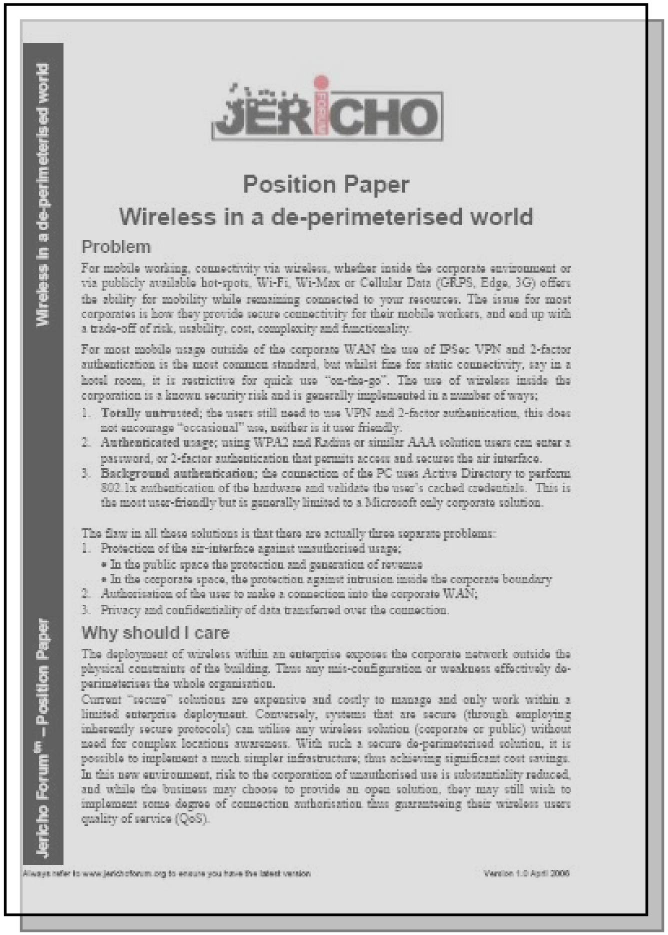
Challenges to the industry

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



Wireless in a de-perimeterised world

Position Paper

Wireless in a de-perimeterised world

Problem

For mobile working, connectivity via wireless, whether inside the corporate environment or via publicly available hot-spots, Wi-Fi, Wi-Max or Cellular Data (GRPS, Edge, 3G) offers the ability for mobility while remaining connected to your resources. The issue for most corporates is how they provide secure connectivity for their mobile workers, and end up with a trade-off of risk, usability, cost, complexity and functionality.

For most mobile usage outside of the corporate WAN the use of IPSec VPN and 2-factor authentication is the most common standard, but whilst fine for static connectivity, say in a hotel room, it is restrictive for quick use “on-the-go”. The use of wireless inside the corporation is a known security risk and is generally implemented in a number of ways;

1. **Totally untrusted**; the users still need to use VPN and 2-factor authentication, this does not encourage “occasional” use, neither is it user friendly.
2. **Authenticated usage**; using WPA2 and Radius or similar AAA solution users can enter a password, or 2-factor authentication that permits access and secures the air interface.
3. **Background authentication**; the connection of the PC uses Active Directory to perform 802.1x authentication of the hardware and validate the user's cached credentials. This is the most user-friendly but is generally limited to a Microsoft only corporate solution.

The flaw in all these solutions is that there are actually three separate problems:

1. Protection of the air-interface against unauthorised usage;
   - In the public space the protection and generation of revenue
   - In the corporate space, the protection against intrusion inside the corporate boundary
2. Authorisation of the user to make a connection into the corporate WAN;
3. Privacy and confidentiality of data transferred over the connection.

Why should I care

The deployment of wireless within an enterprise exposes the corporate network outside the physical constraints of the building. Thus any mis-configuration or weakness effectively de-perimeterises the whole organisation.

Current “secure” solutions are expensive and costly to manage and only work within a limited enterprise deployment. Conversely, systems that are secure (through employing inherently secure protocols) can utilise any wireless solution (corporate or public) without need for complex locations awareness. With such a secure de-perimeterised solution, it is possible to implement a much simpler infrastructure; thus achieving significant cost savings.

In this new environment, risk to the corporation of unauthorised use is substantiality reduced, and while the business may choose to provide an open solution, they may still wish to implement some degree of connection authorisation thus guaranteeing their wireless users quality of service (QoS).

Jericho Forum℠ – Position Paper

Always refer to www.jerichoforum.org to ensure you have the latest version

Version 1.0 April 2006

Real world application

- **Voice over IP**
- **John Meakin**
  Standard Chartered Bank
  & 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??

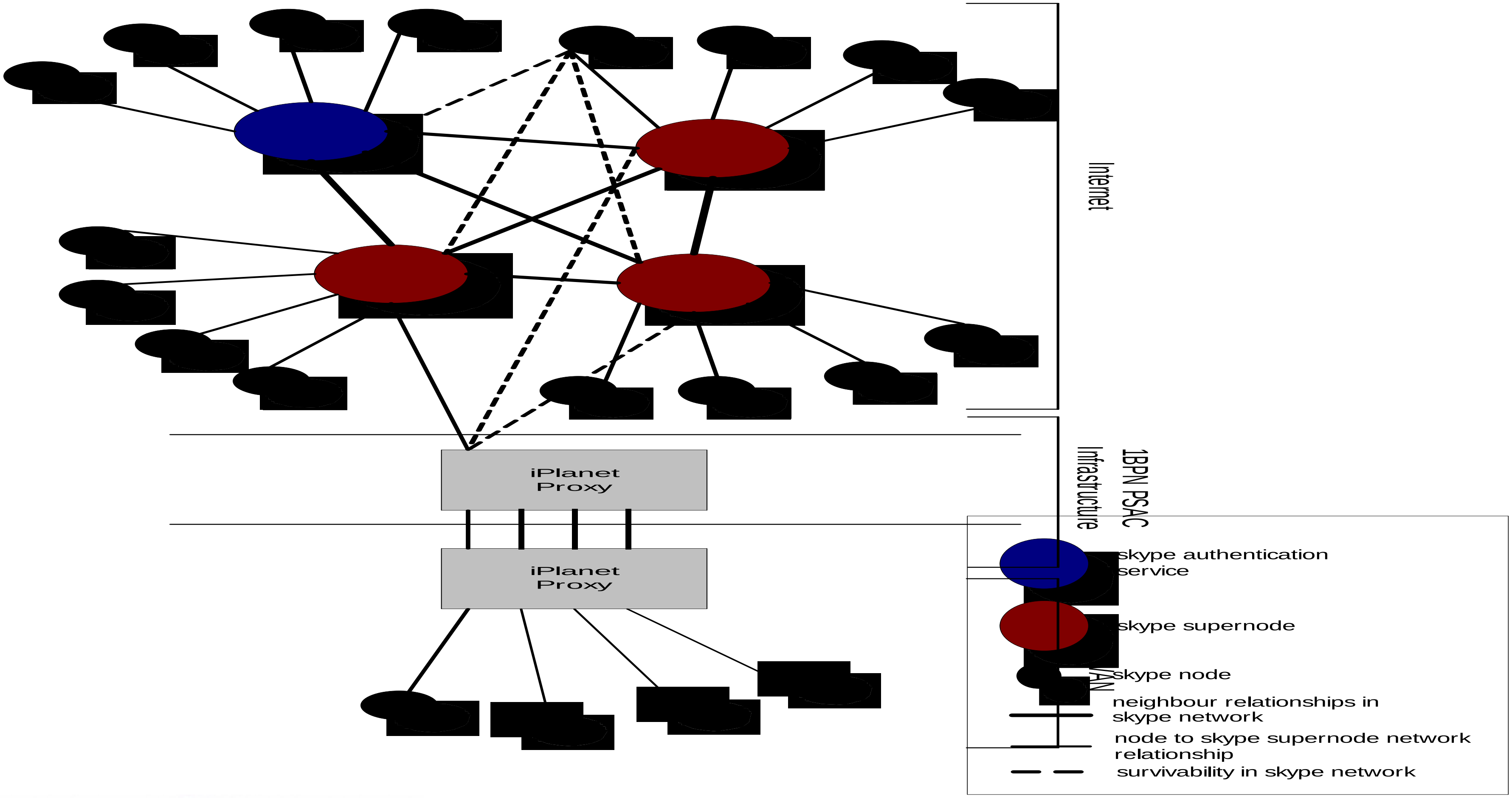
The Reality of VoIP

- 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


iPlanet Proxy
iPlanet Proxy
Internet
1BPN PSAC Infrastructure
skype authentication service
skype supernode
skype node
neighbour relationships in skype network
node to skype supernode network relationship
survivability in skype network

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

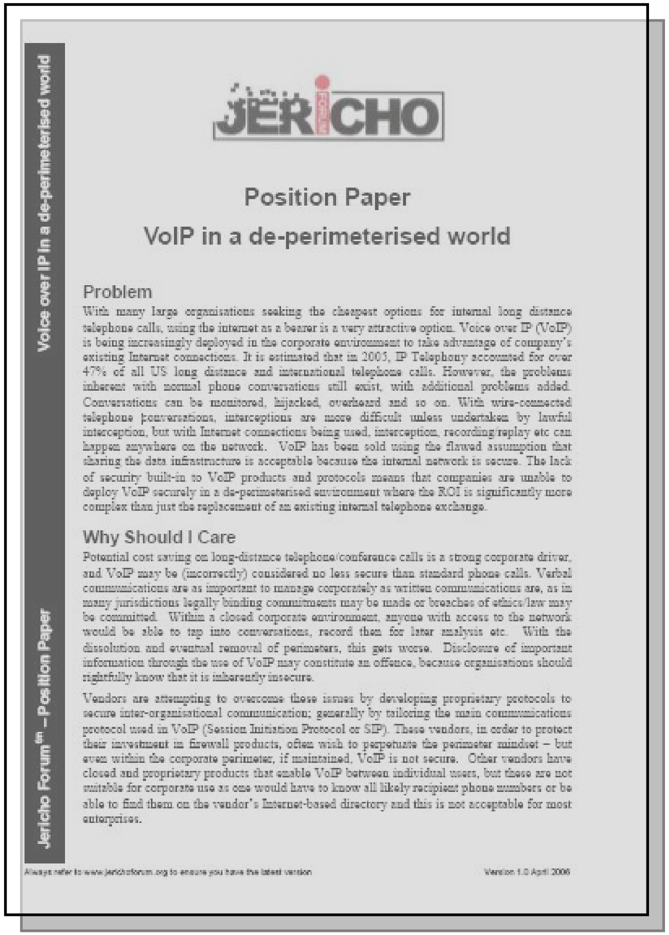
Challenges to the industry

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 should be released 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 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



Voice over IP in a de-perimeterised world

JERICHO FORUM

Position Paper

VoIP in a de-perimeterised world

Problem

With many large organisations seeking the cheapest options for internal long distance telephone calls, using the internet as a bearer is a very attractive option. Voice over IP (VoIP) is being increasingly deployed in the corporate environment to take advantage of company's existing Internet connections. It is estimated that in 2005, IP Telephony accounted for over 47% of all US long distance and international telephone calls. However, the problems inherent with normal phone conversations still exist, with additional problems added. Conversations can be monitored, hijacked, overheard and so on. With wire-connected telephone conversations, interceptions are more difficult unless undertaken by lawful interception, but with Internet connections being used, interception, recording/replay etc can happen anywhere on the network. VoIP has been sold using the flawed assumption that sharing the data infrastructure is acceptable because the internal network is secure. The lack of security built-in to VoIP products and protocols means that companies are unable to deploy VoIP securely in a de-perimeterised environment where the ROI is significantly more complex than just the replacement of an existing internal telephone exchange.

Why Should I Care

Potential cost saving on long-distance telephone/conference calls is a strong corporate driver, and VoIP may be (incorrectly) considered no less secure than standard phone calls. Verbal communications are as important to manage corporately as written communications are, as in many jurisdictions legally binding commitments may be made or breaches of ethics/law may be committed. Within a closed corporate environment, anyone with access to the network would be able to tap into conversations, record them for later analysis etc. With the dissolution and eventual removal of perimeters, this gets worse. Disclosure of important information through the use of VoIP may constitute an offence, because organisations should rightfully know that it is inherently insecure.

Vendors are attempting to overcome these issues by developing proprietary protocols to secure inter-organisational communication; generally by tailoring the main communications protocol used in VoIP (Session Initiation Protocol or SIP). These vendors, in order to protect their investment in firewall products, often wish to perpetuate the perimeter mindset – but even within the corporate perimeter, if maintained, VoIP is not secure. Other vendors have closed and proprietary products that enable VoIP between individual users, but these are not suitable for corporate use as one would have to know all likely recipient phone numbers or be able to find them on the vendor's Internet-based directory and this is not acceptable for most enterprises.

Jericho Forum™ – Position Paper

Always refer to www.jerichoforum.org to ensure you have the latest version

Version 1.0 April 2006

Case Study

- **Migration to a de-perimeterised environment**

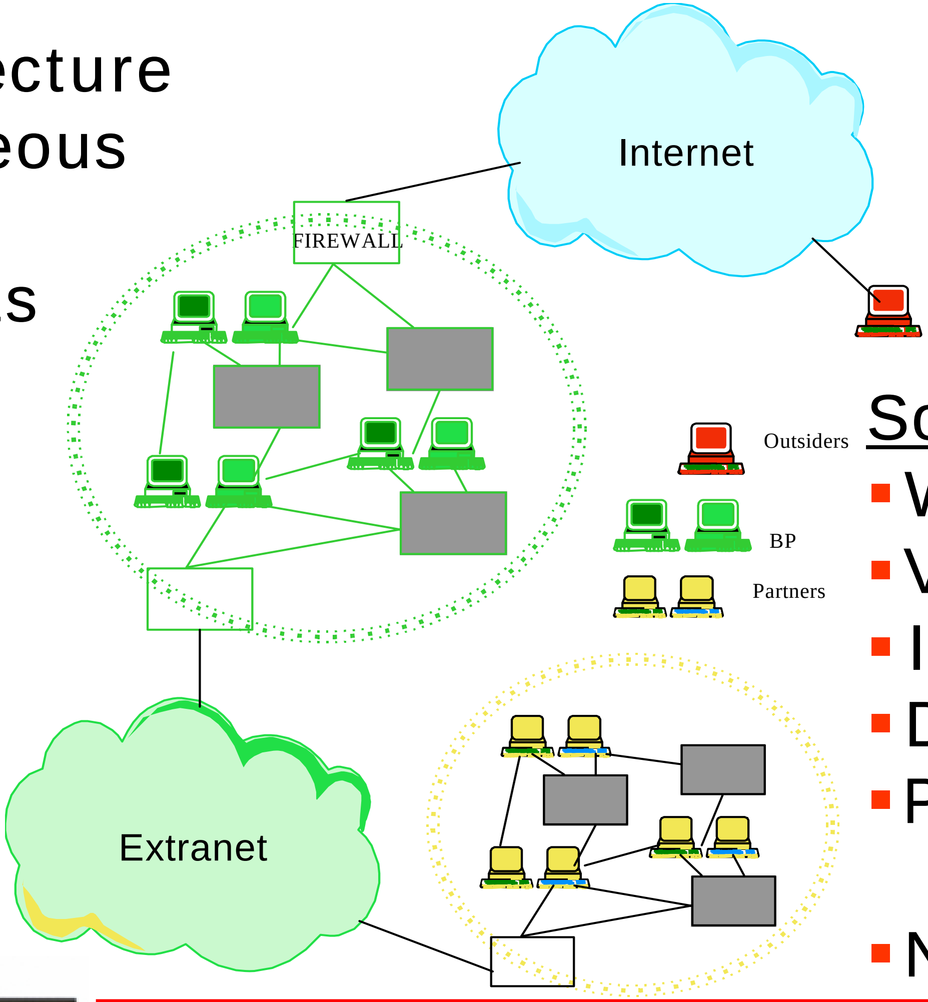
- **Paul Dorey**
  BP &
  Jericho Forum Board

Desktop Migration Strategy

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

Current Architecture

- Flat Architecture
- Heterogeneous
- Barriers & Chokepoints
- “Us” and “Them”



<u>Solutions?</u>

- 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 architypical ‘virtual enterprise’

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

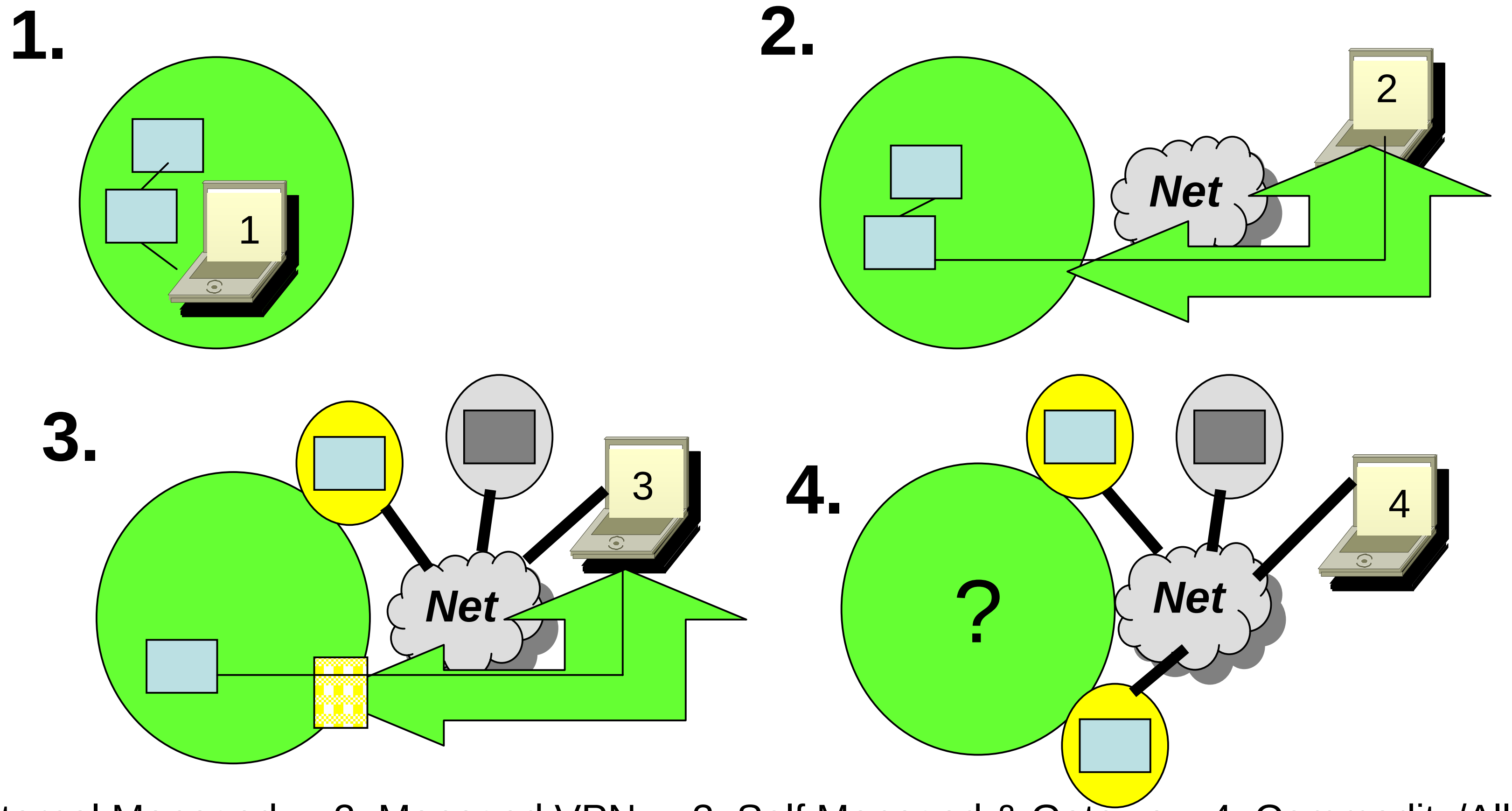
Technology Drivers ...

- Exploding connectivity and complexity (embedded Internet, IP convergence)
- Peer to peer,sensory networks, mesh, grid, mass digitisation
- Machine-understandable information (Semantic Web)
- De-fragmentation of computers into networks of smaller devices
- Wireless, wearable computing

Security Drivers

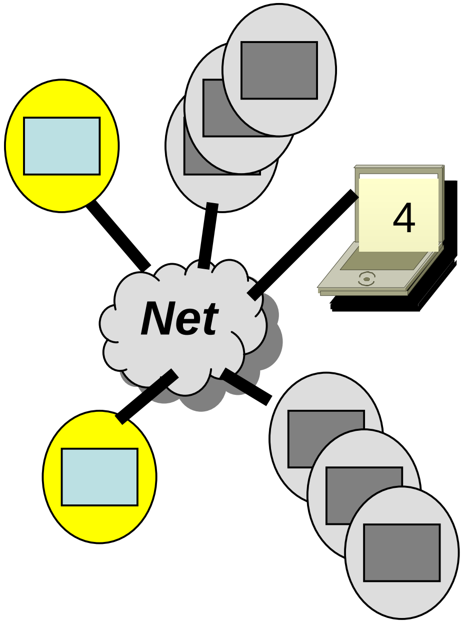
- Insiders
- Outsiders inside
- Port 80 and Mail traffic get in anyway
- Hibernating or ‘rogue’ devices
- Firewall rule chaos
- VOIP & P2P
- Stealth attackers
- Black list vs. white list
- False sense of security

Migration to the new model



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

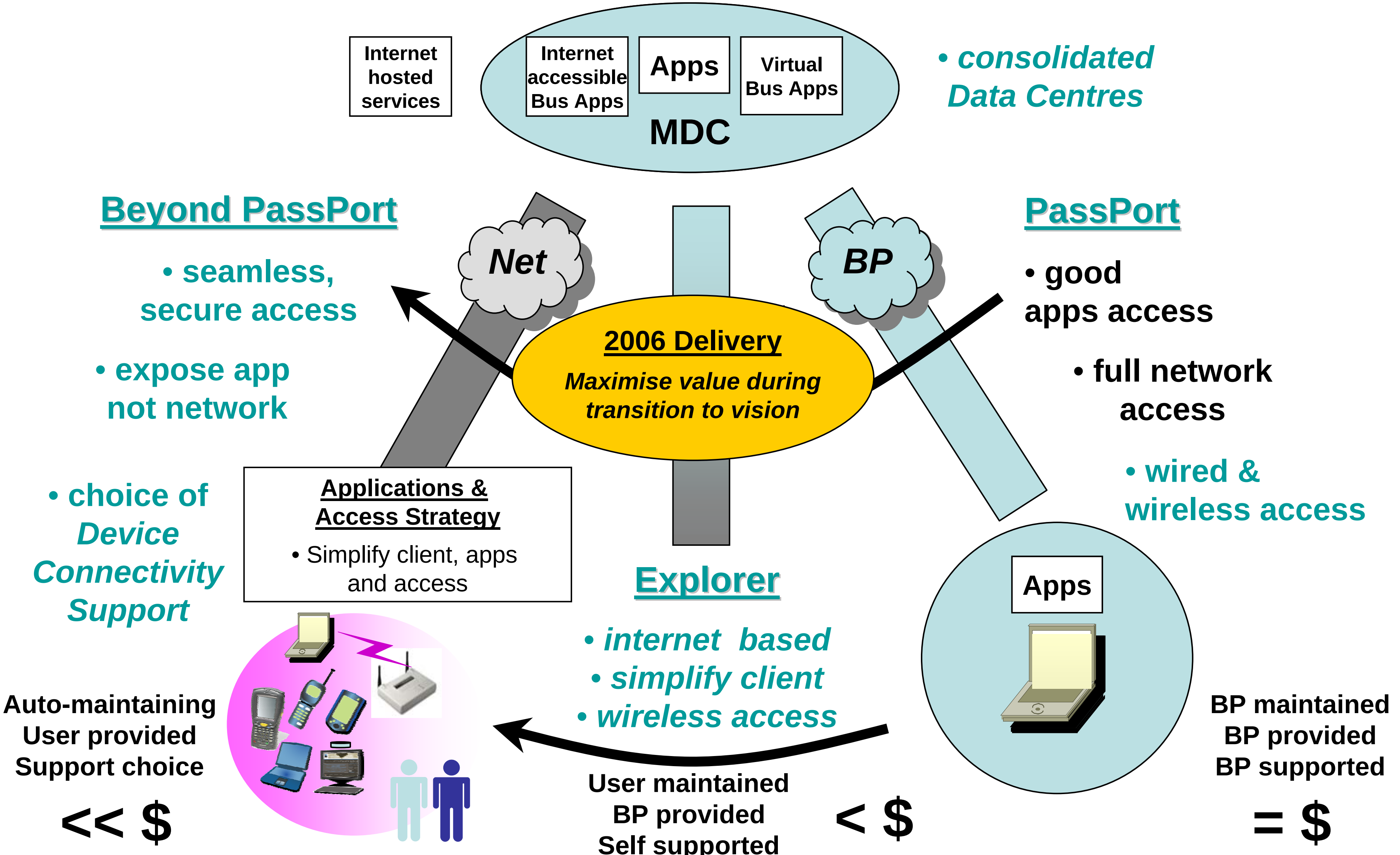
“In the Cloud” Security Services



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

Internet accessible Bus Apps

Apps

Virtual Bus Apps

MDC

- *consolidated Data Centres*

Beyond PassPort

- seamless, secure access
- expose app not network

Net

BP

PassPort

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

2006 Delivery

Maximise value during transition to vision

Applications & Access Strategy

- Simplify client, apps and access

- choice of *Device Connectivity Support*

Explorer

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

Apps

Auto-maintaining
User provided
Support choice

<< $

User maintained
BP provided
Self supported

< $

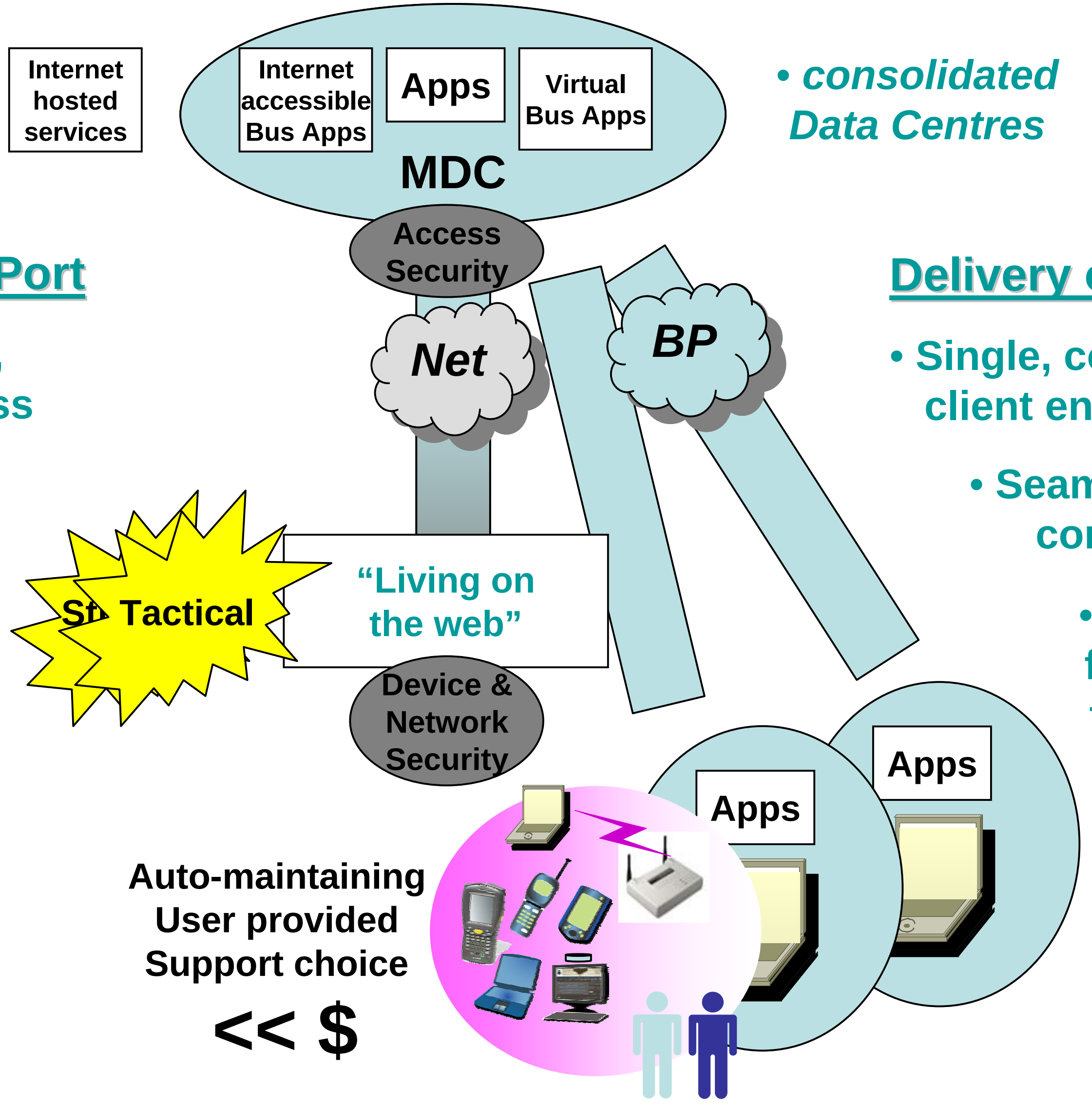
BP maintained
BP provided
BP supported

= $

Desktop Strategy – Delivery of Vision

Beyond PassPort

- seamless, secure access
- expose app not network
- choice of *Device Connectivity Support*



Auto-maintaining
User provided
Support choice

<< $

- *consolidated Data Centres*
- *no local servers*

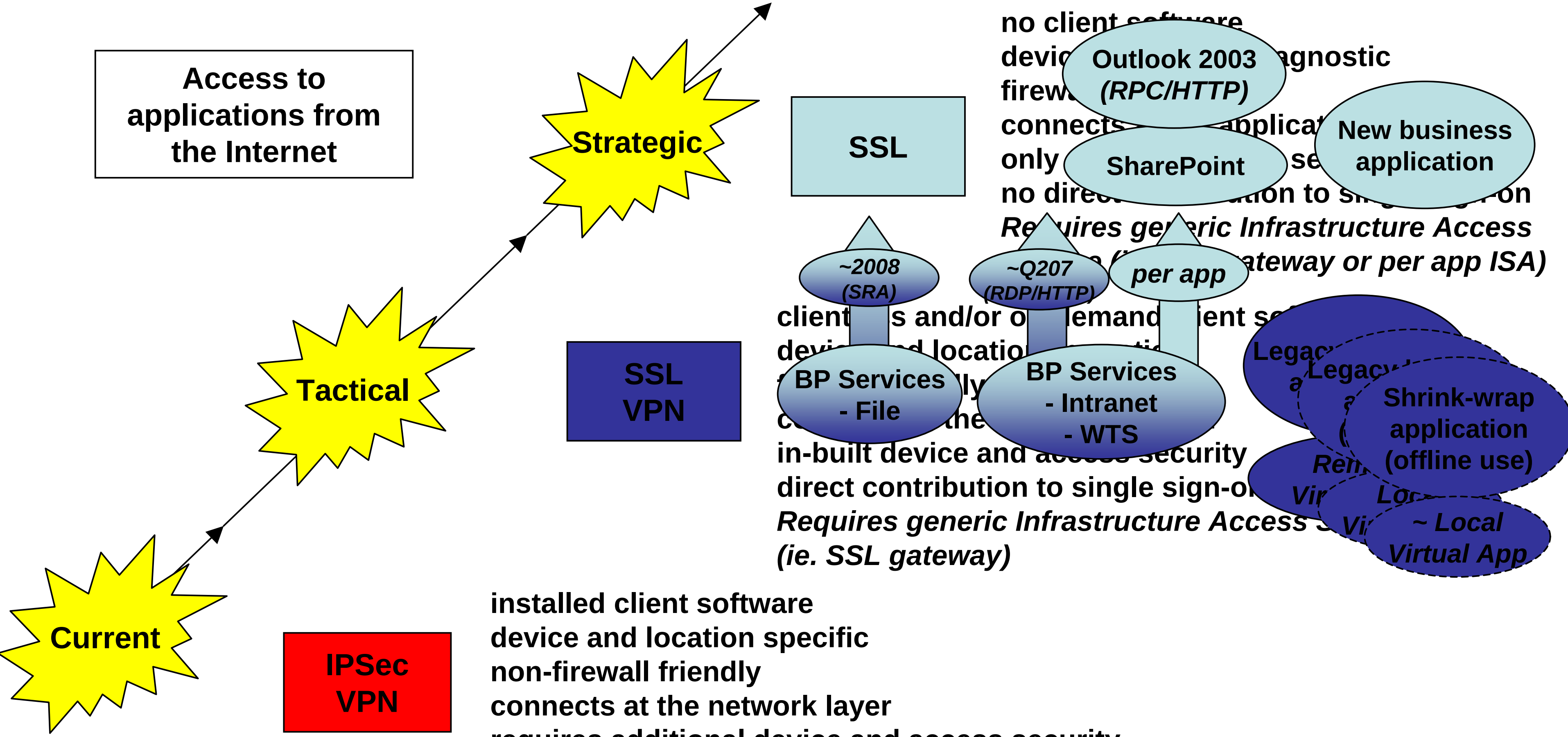
Delivery of Vision

- Single, consumer-style client environment
- Seamless, secure connectivity
- Enhanced functionality, freedom and choice

BP maintained
BP provided
BP supported

= $

Access Strategy - Scenarios



no client software
devic agnostic
firew
connects applicat
only se
no direc ution to si on
Re uires ge eric Infrastructure Access
e (i ateway or per app ISA)

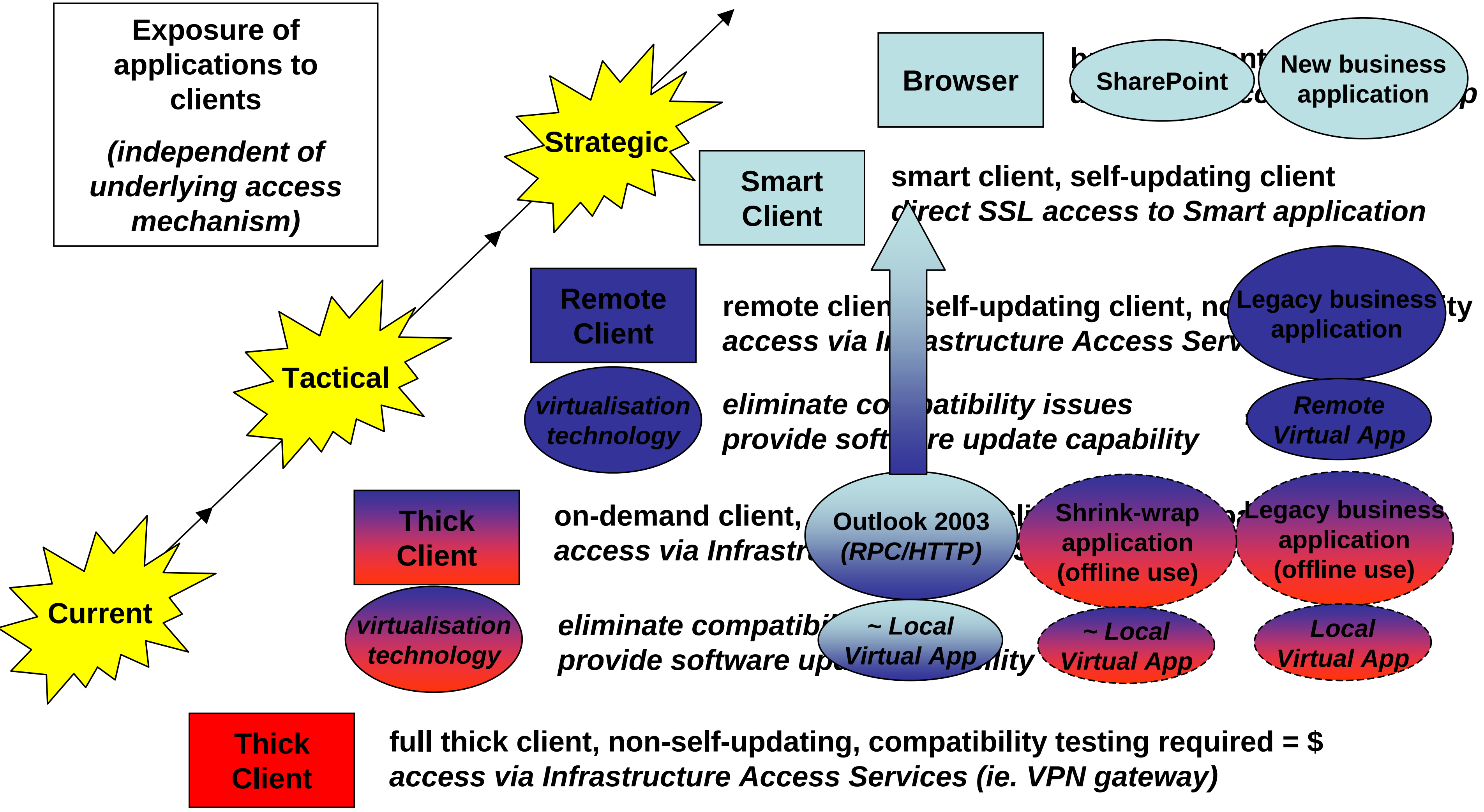
client s and/or o lemand ient s
devi d locatio
f ly
c the
in-built device and access security
direct contribution to single sign-o
Requires generic Infrastructure Access S
(ie. SSL gateway)

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)

b nt

smart client, self-updating client
direct SSL access to Smart application

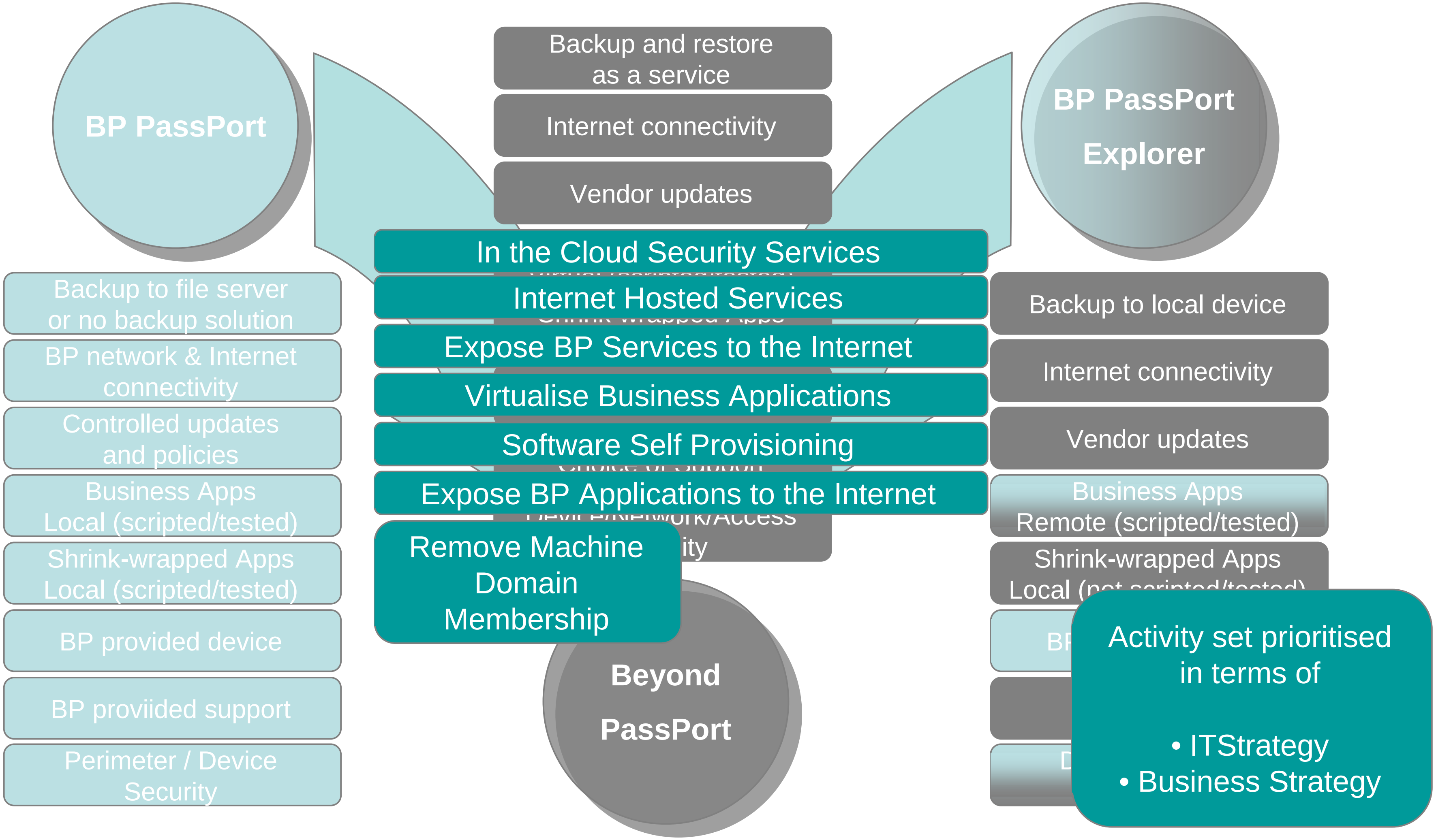
remote clien self-updating client, no ty
access via In astructure Access Serv

eliminate co patibility issues
provide soft re update capability

on-demand client,
access via Infrastr

eliminate compatibi
provide software up lity

full thick client, non-self-updating, compatibility testing required = $
access via Infrastructure Access Services (ie. VPN gateway)



BP PassPort

Backup to file server or no backup solution

BP network & Internet connectivity

Controlled updates and policies

Business Apps Local (scripted/tested)

Shrink-wrapped Apps Local (scripted/tested)

BP provided device

BP proviided support

Perimeter / Device Security

Backup and restore as a service

Internet connectivity

Vendor updates

In the Cloud Security Services

Internet Hosted Services

Expose BP Services to the Internet

Virtualise Business Applications

Software Self Provisioning

Expose BP Applications to the Internet

Remove Machine Domain Membership

Beyond PassPort

BP PassPort Explorer

Backup to local device

Internet connectivity

Vendor updates

Business Apps Remote (scripted/tested)

Shrink-wrapped Apps Local (not scripted/tested)

Activity set prioritised in terms of

- ITStrategy
- Business Strategy

- Lunch
- Resume at 2.30pm

The Jericho Forum – 2nd US Conference

Fri, May 12, 2006 **Hosted by Motorola**

Motorola Center, Schaumberg, Chicago, Il, USA

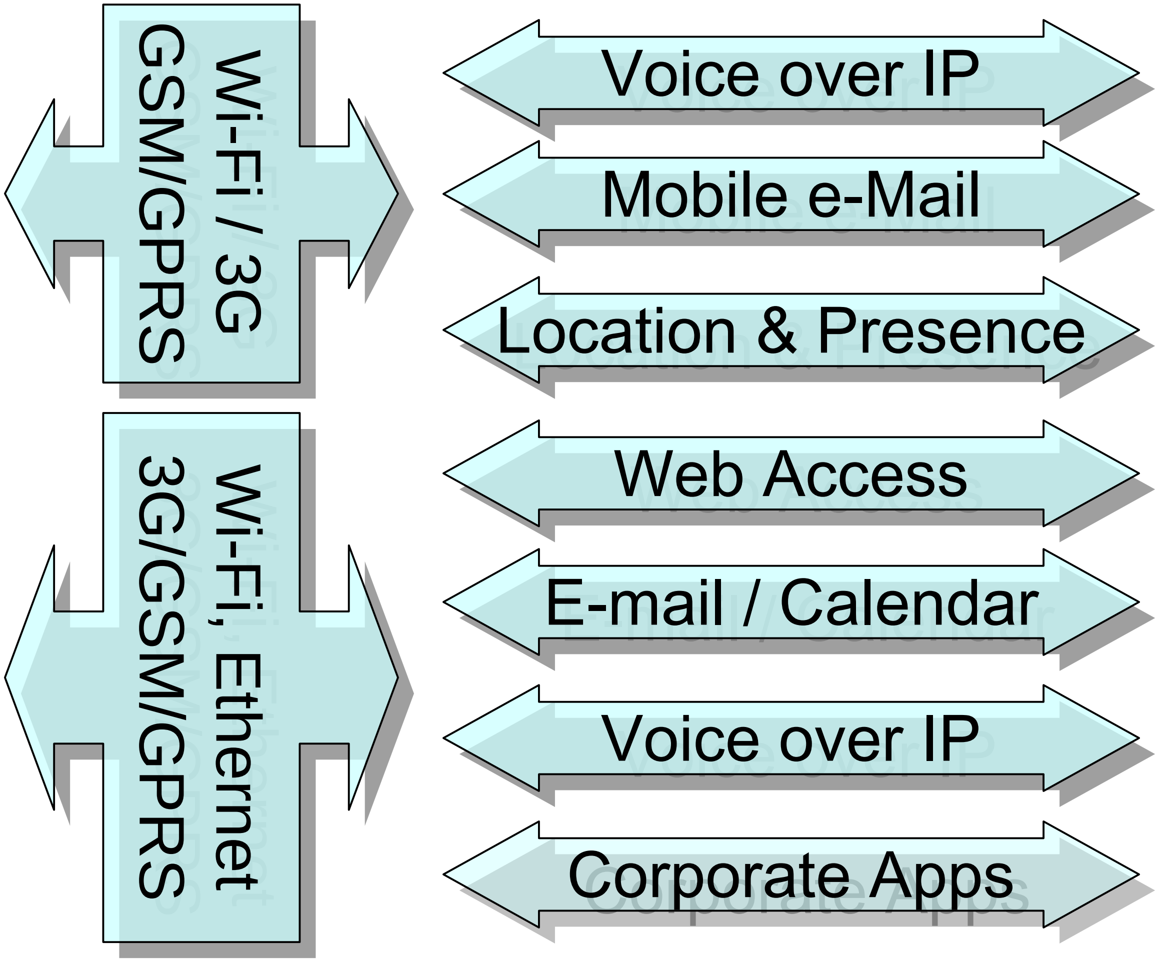
- 09.00 Arrival
- 09.30 Welcome & Housekeeping
- 09.35 Opening Keynote: Setting the scene
- 09.50 The Jericho Forum Commandments
- 10.45 Break
- 11.00 Real world application: Protocols
- 11.20 Real world application: VoIP
- 11.40 Real world application: Corp. Wireless Networking
- 12.00 Case Study: Boeing: 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

Prepare for the future

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

SC MAGAZINE
AWARDS
2006

Requirements



Wi-Fi / 3G
GSM/GPRS

Wi-Fi, Ethernet
3G/GSM/GPRS

Voice over IP

Mobile e-Mail

Location & Presence

Web Access

E-mail / Calendar

Voice over IP

Corporate Apps

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.

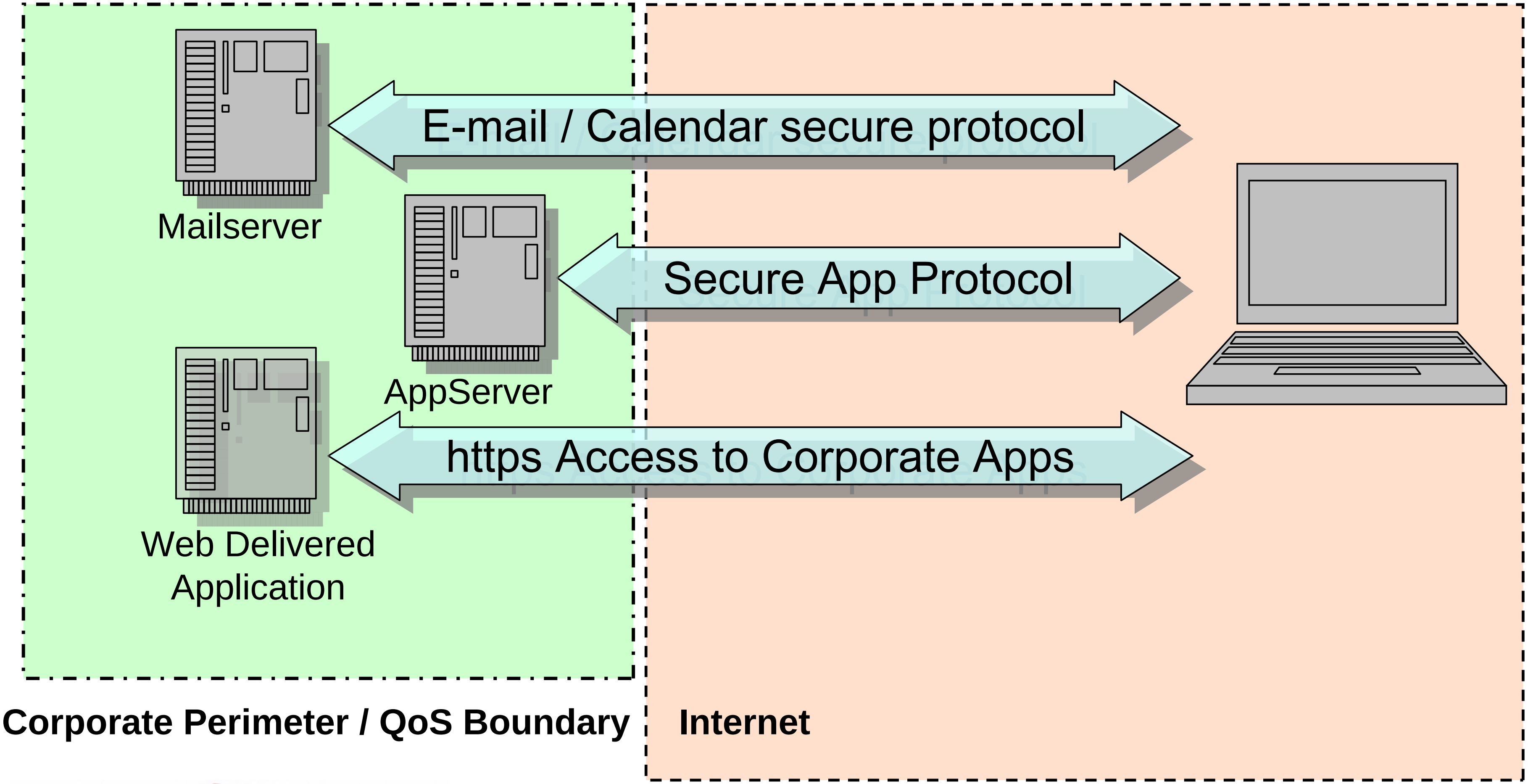
Requirements – Laptop Device

- 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



E-mail / Calendar secure protocol

Secure App Protocol

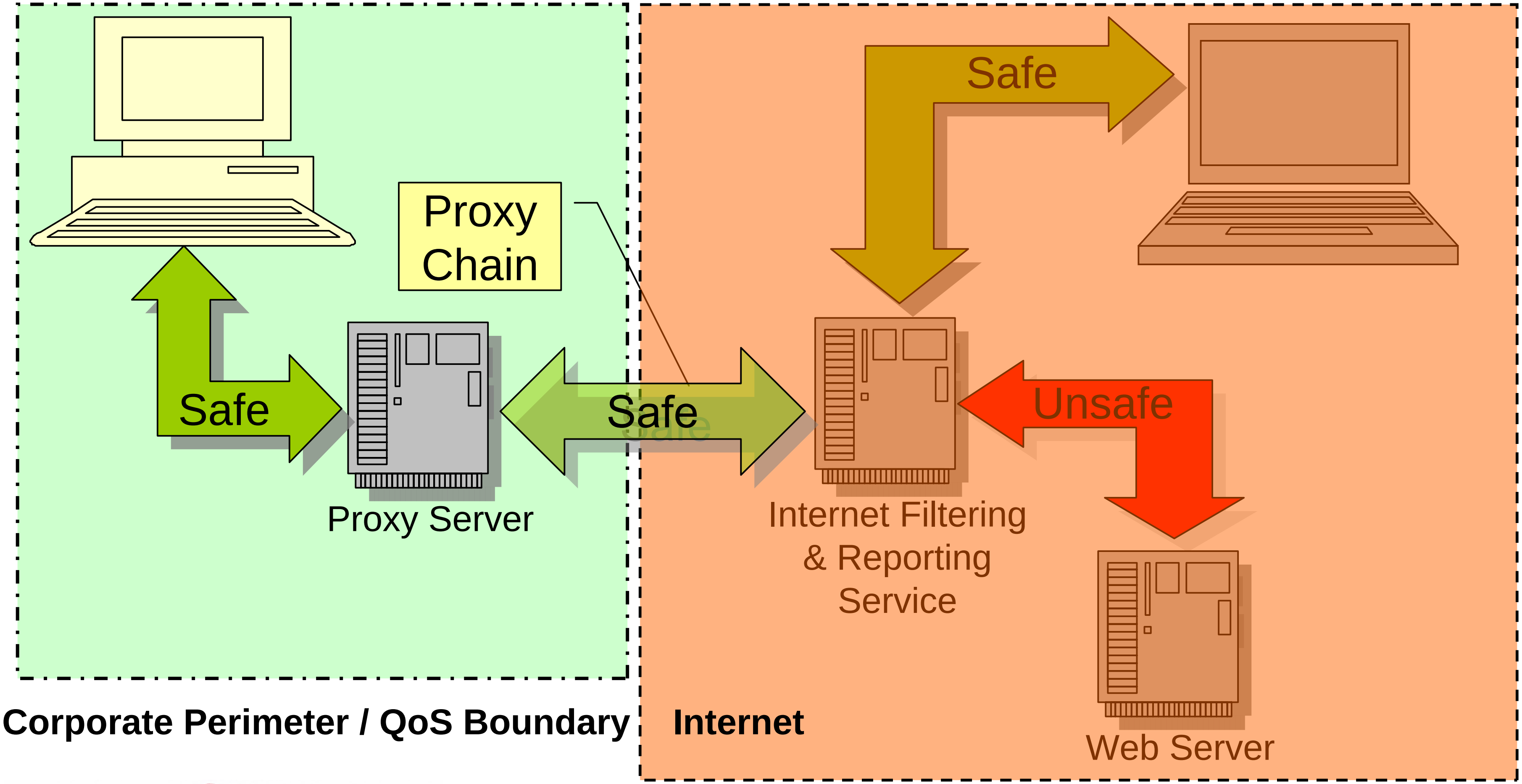
https Access to Corporate Apps

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**

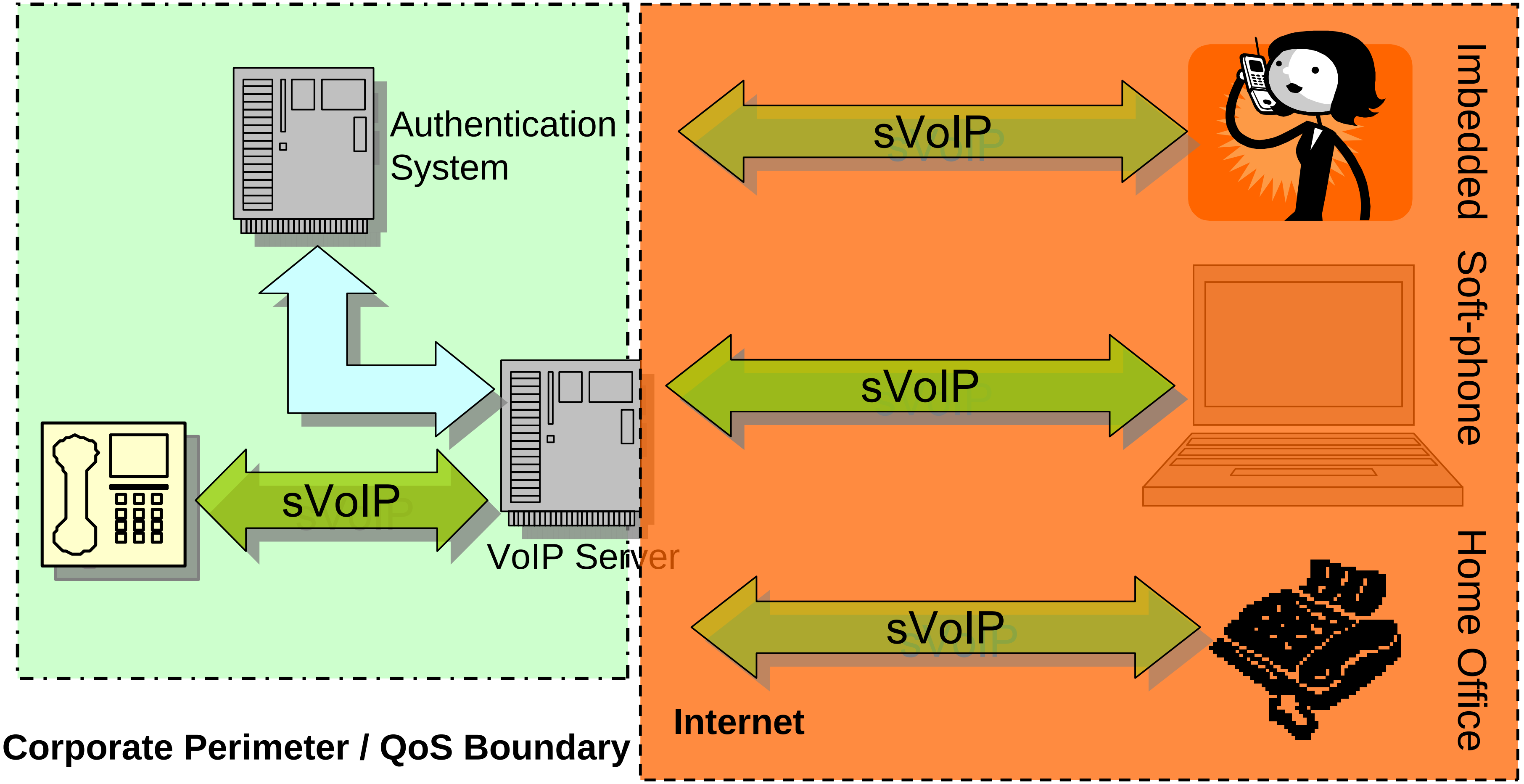
Putting it all together – Web Access



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



Authentication System

sVoIP

VoIP Server

sVoIP

sVoIP

sVoIP

Imbedded

Soft-phone

Home Office

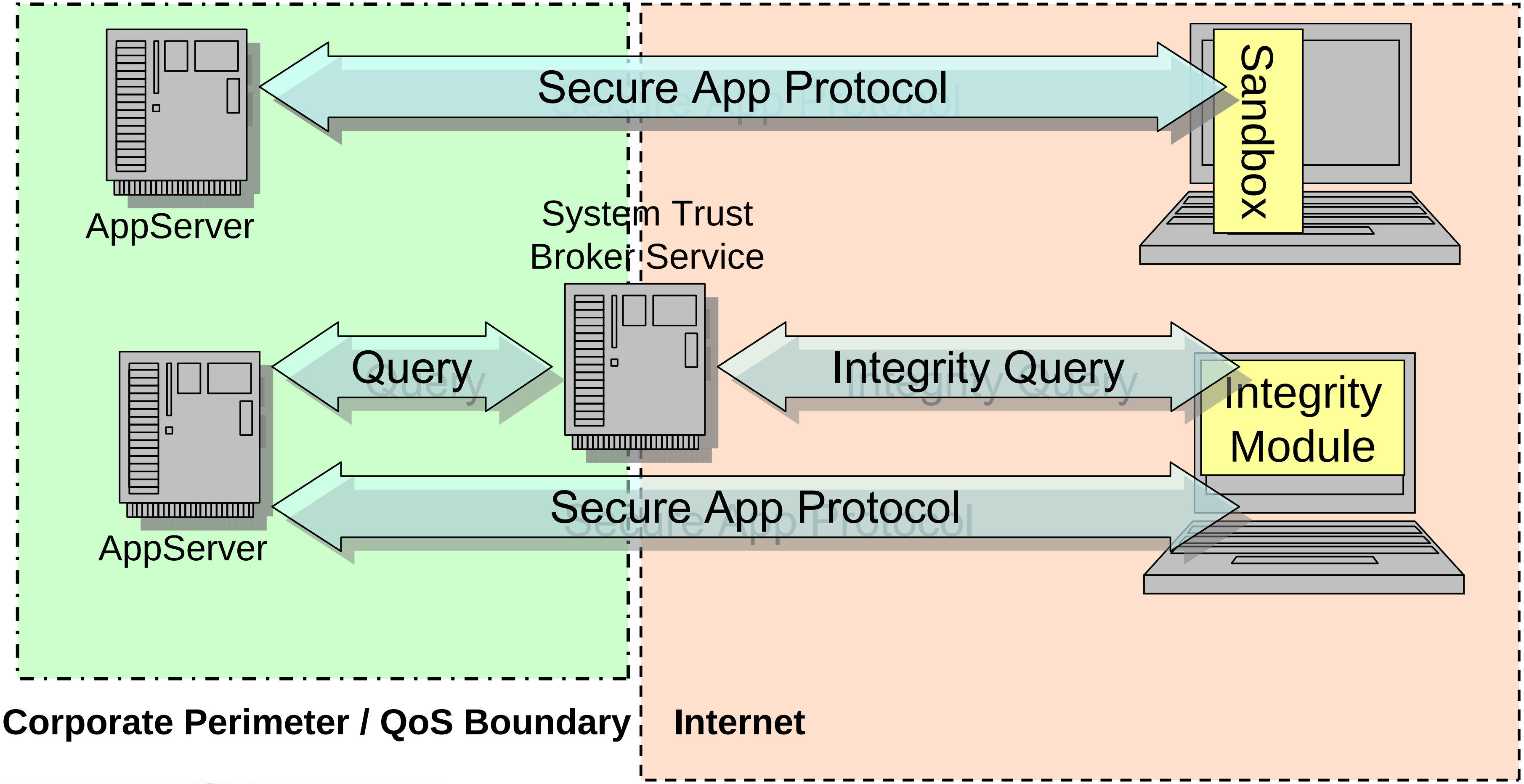
Internet

Corporate Perimeter / QoS Boundary

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

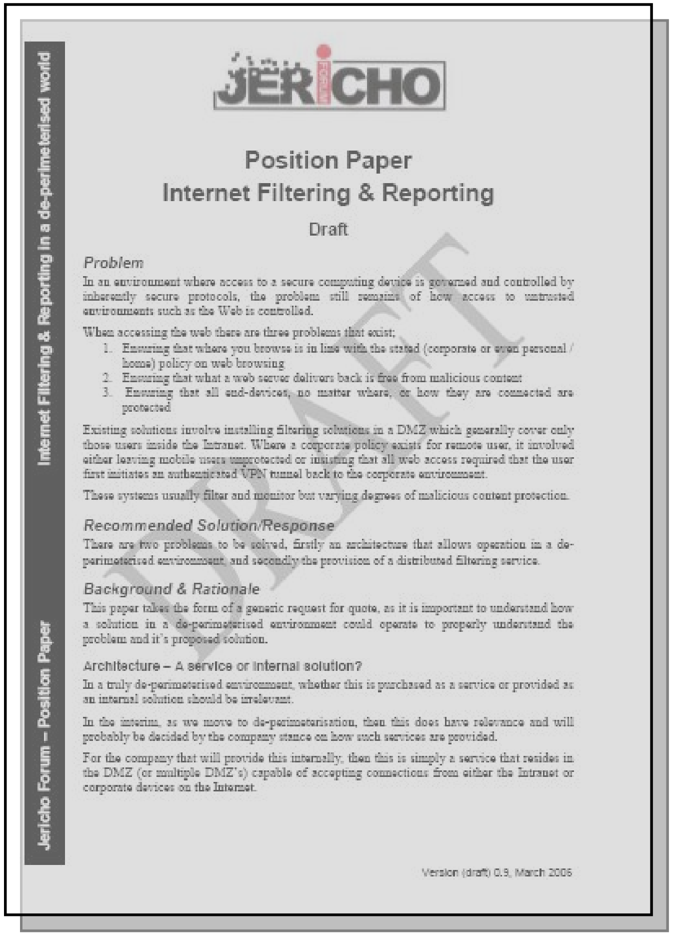
An inherently secure corporation

- 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



Internet Filtering & Reporting in a de-perimeterised world

Jericho Forum – Position Paper

Position Paper
Internet Filtering & Reporting

Draft

Problem

In an environment where access to a secure computing device is governed and controlled by inherently secure protocols, the problem still remains of how access to untrusted environments such as the Web is controlled.

When accessing the web there are three problems that exist;

1. Ensuring that where you browse is in line with the stated (corporate or even personal / home) policy on web browsing
2. Ensuring that what a web server delivers back is free from malicious content
3. Ensuring that all end-devices, no matter where, or how they are connected are protected

Existing solutions involve installing filtering solutions in a DMZ which generally cover only those users inside the Intranet. Where a corporate policy exists for remote user, it involved either leaving mobile users unprotected or insisting that all web access required that the user first initiates an authenticated VPN tunnel back to the corporate environment.

These systems usually filter and monitor but varying degrees of malicious content protection.

Recommended Solution/Response

There are two problems to be solved, firstly an architecture that allows operation in a de-perimeterised environment, and secondly the provision of a distributed filtering service.

Background & Rationale

This paper takes the form of a generic request for quote, as it is important to understand how a solution in a de-perimeterised environment could operate to properly understand the problem and it's proposed solution.

Architecture – A service or internal solution?

In a truly de-perimeterised environment, whether this is purchased as a service or provided as an internal solution should be irrelevant.

In the interim, as we move to de-perimeterisation, then this does have relevance and will probably be decided by the company stance on how such services are provided.

For the company that will provide this internally, then this is simply a service that resides in the DMZ (or multiple DMZ's) capable of accepting connections from either the Intranet or corporate devices on the Internet.

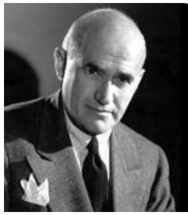
Version (draft) 0.9, March 2005

Prepare for the future

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

SC MAGAZINE AWARDS 2006

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

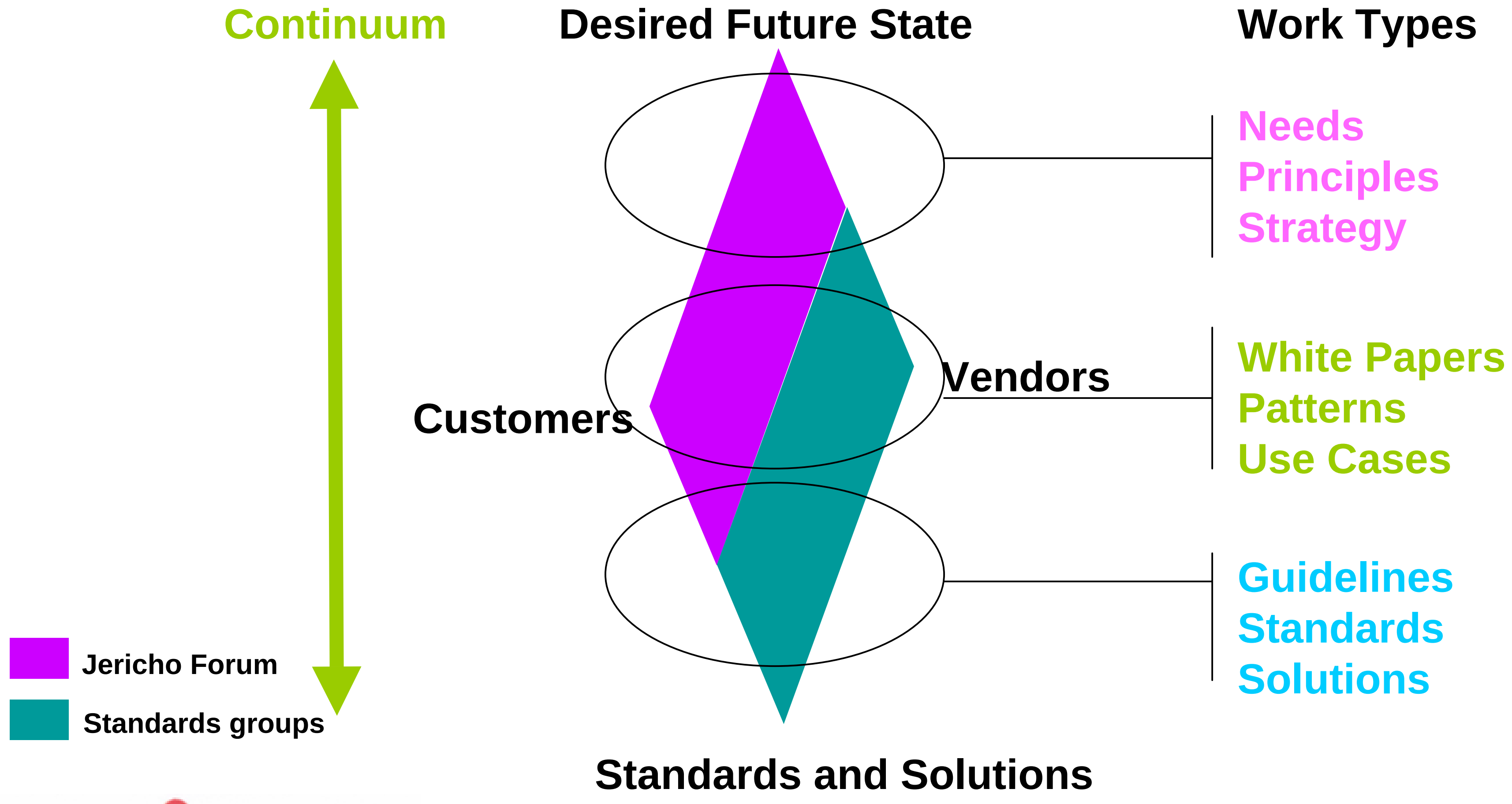


Samuel Goldwyn
1882-
1974

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



Potential Roadmap

Key Com-ponents New & evolving technologies (partial)	▪ Firewalls (Filter /DPI/Proxy) ▪ Anti-Virus Anti-Spam ▪ Cli&Svr Patch Mgmt ▪ IPSec VPN ▪ SSL/Web SSO ▪ Proxies/IFR for -Trading Apps -Web/Msging ▪ DS point solutions ▪ IPS point solutions ▪ Dev config	▪ Firewalls (Fltr/DPI) ▪ Anti-Virus/Spam ▪ Cli&Svr Patch Mgmt ▪ Proxies/IFR for - Trading Apps - Web/Msging ▪ DS point solutions ▪ TL/NL gateways ▪ XML point solutions ▪ Fed. Identity ▪ Intrusion correlation & response ▪ Micro-perim mgmt & device firewall/config	▪ Firewalls (Fltr/DPI) ▪ Anti-Virus/Spam ▪ Svr Patch Mgmt ▪ Proxies/IFR for Trading Apps ▪ DS point solutions ▪ TL/NL gateways ▪ Fed. Identity ▪ Intrusion correlation & response ▪ Micro-perim mgmt & dev firewalls/config ▪ Redc'd surface OS & client patching ▪ Virtual Proxies/IFR ▪ XML subsetting ▪ P2P point solutions	▪ Firewalls (Fltr/DPI) ▪ Anti-Spam ▪ Svr Patch Mgmt ▪ TL/NL gateways ▪ Fed. Identity ▪ Intrusion correlation & response ▪ Micro-perim mgmt & dev firewalls/ config ▪ Redc'd surface OS & client/svr patching ▪ Virtual Proxies/IFR ▪ XML subsetting ▪ P2P trust models	▪ Firewalls (DPI) ▪ Anti-Malware ▪ TL/NL gateways ▪ Intrusion correlation & response ▪ Micro-perim mgmt & dev firewalls/config ▪ Redc'd surface OS & client/svr patching ▪ Virtual Proxies/IFR ▪ XML subsetting ▪ P2P trust models and identity ▪ Trust assurance mgmt ▪ Interoperable DS
60% Adoption	Pre 2006	2006	2007	2008	2009
Key Obsoleted Technology	▪ Dial-up security ▪ Simple IDS	▪ IPsec VPN ▪ Firewall-based proxies	▪ Proxies/IFR for Web/Msging ▪ XML point solutions ▪ Clnt 'service releases'	▪ Hybrid IPsec/TLS gateways ▪ Proxies/IFR ▪ Standalone AV	▪ Fltr Firewalls ▪ Svr 'service releases' ▪ Fed. Identity

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.

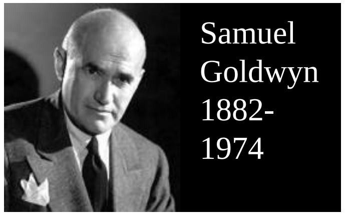
How are we engaging?

- 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!

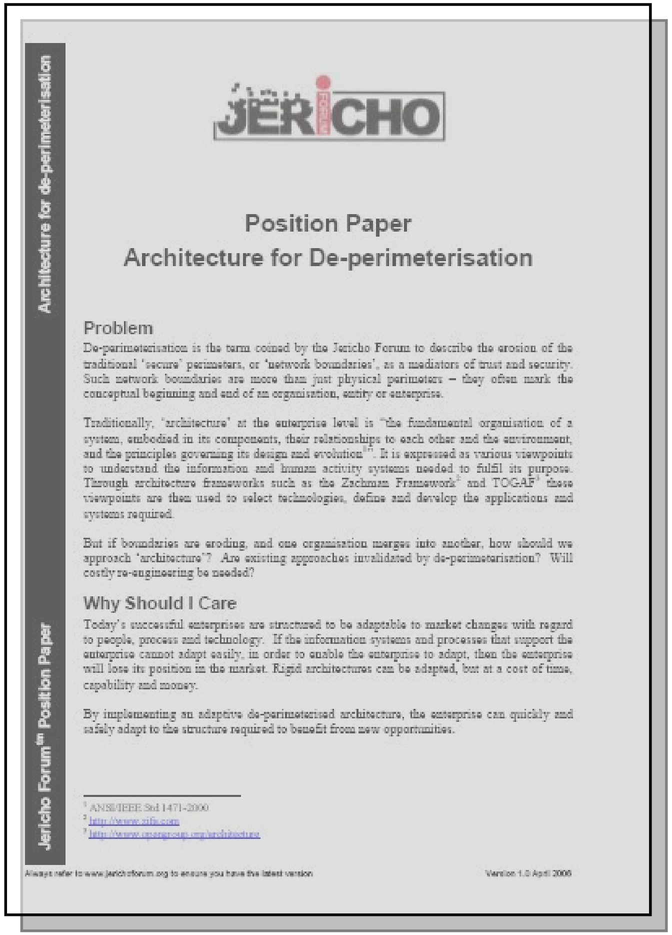
I never put on a pair of shoes until I've worn them at least five years.



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



Architecture for de-perimeterisation

Position Paper

Architecture for De-perimeterisation

Problem

De-perimeterisation is the term coined by the Jericho Forum to describe the erosion of the traditional ‘secure’ perimeters, or ‘network boundaries’, as a mediators of trust and security. Such network boundaries are more than just physical perimeters – they often mark the conceptual beginning and end of an organisation, entity or enterprise.

Traditionally, ‘architecture’ at the enterprise level is “the fundamental organisation of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution[1]”. It is expressed as various viewpoints to understand the information and human activity systems needed to fulfil its purpose. Through architecture frameworks such as the Zachman Framework[2] and TOGAF[3] these viewpoints are then used to select technologies, define and develop the applications and systems required.

But if boundaries are eroding, and one organisation merges into another, how should we approach ‘architecture’? Are existing approaches invalidated by de-perimeterisation? Will costly re-engineering be needed?

Why Should I Care

Today’s successful enterprises are structured to be adaptable to market changes with regard to people, process and technology. If the information systems and processes that support the enterprise cannot adapt easily, in order to enable the enterprise to adapt, then the enterprise will lose its position in the market. Rigid architectures can be adapted, but at a cost of time, capability and money.

By implementing an adaptive de-perimeterised architecture, the enterprise can quickly and safely adapt to the structure required to benefit from new opportunities.

[1] ANSI/IEEE Std 1471-2000
[2] http://www.zifa.com
[3] http://www.opengroup.org/architecture

Jericho Forum™ Position Paper

Always refer to www.jerichoforum.org to ensure you have the latest version

Version 1.0 April 2006

- **Break**
  Tea & Coffee served

- **Resume at 3.45pm**

SC MAGAZINE
AWARDS
2006

Question & Answers

- **Face the audience**
- **Moderated by;**
  Paul Fisher,
  Editor SC Magazine

- **Summing up the day**
- **Paul Fisher,**
  Editor SC Magazine

The Jericho Forum – 2nd US Conference

Fri, May 12, 2006 **Hosted by Motorola**

Motorola Center, Schaumberg, 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