Responding to the de-perimeterisation of corporate networks

A practical guide

Paul Simmonds

Board of Management, Jericho Forum®
&
Global IS Integrated Assurance Director, AstraZeneca Plc.

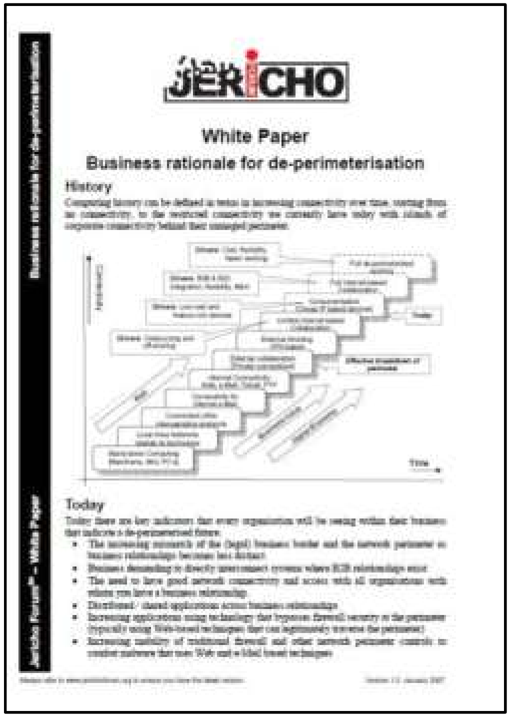
Introduction

- This presentation is combined best practice solutions from Jericho Forum members
  - Everything here is implemented somewhere
  - Any exceptions, caveats or issues are noted
  - Aim was to be totally product agnostic (but we failed for reasons of ease of clarity & understanding)
- **Aim**: No big bang required, but some “quick wins”
- **Acceptance**: No rip & replace – rather a 3-5 year "replacement / upgrade" timeline
- Jericho Forum Commandments used as product / design sanity check

Caveat – Warning

1. These are not the only solutions
2. These are possible solutions for migrating a (large) perimeterised corporate
3. Your mileage will vary.....

Pre-reading



Business rationale for de-perimeterisation

Jericho Forum™ – White Paper

White Paper

Business rationale for de-perimeterisation

History

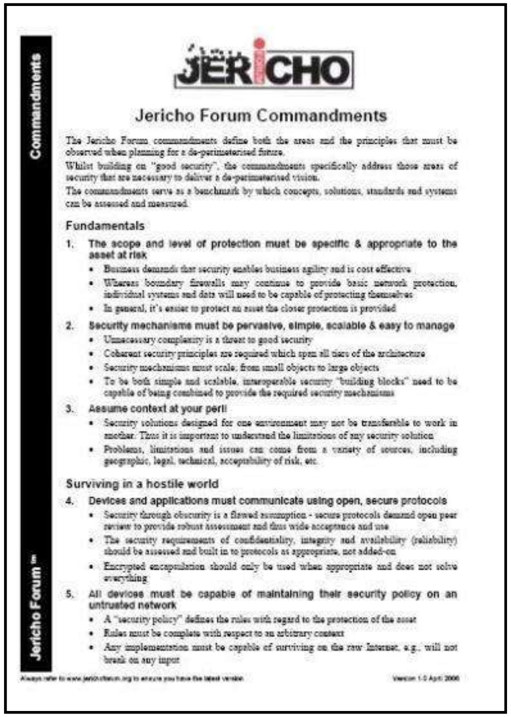
Computing history can be defined in terms in increasing connectivity over time, starting from no connectivity, to the restricted connectivity we currently have today with islands of corporate connectivity behind their managed perimeter.

Today

Today there are key indicators that every organisation will be seeing within their business that indicate a de-perimeterised future

- The increasing mismatch of the (legal) business border and the network perimeter as business relationships becomes less distinct
- Business demanding to directly interconnect systems where B2B relationships exist
- The need to have good network connectivity and access with all organisations with whom you have a business relationship
- Distributed / shared applications across business relationships
- Increasing applications using technology that bypasses firewall security at the perimeter (typically using Web-based techniques that can legitimately traverse the perimeter)
- Increasing inability of traditional firewall and other network perimeter controls to combat malware that uses Web and e-Mail based techniques

Always refer to www.jerichoforum.org to ensure you have the latest version. Version 1.0, January 2007



Commandments

Jericho Forum ™

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.

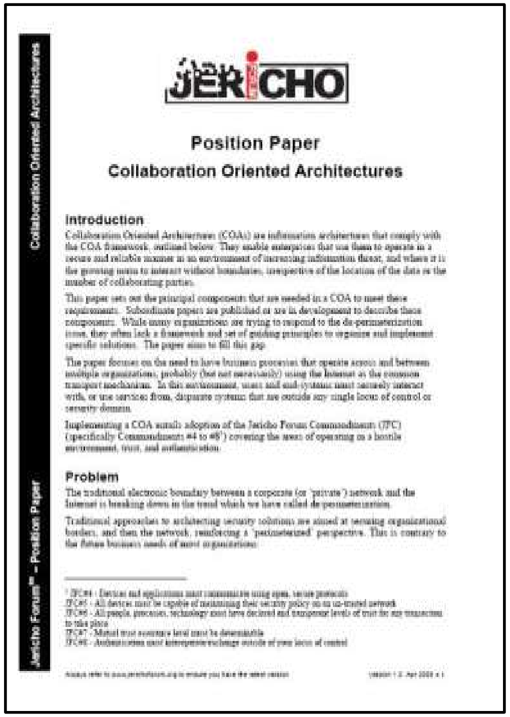
Fundamentals

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

Always refer to www.jerichoforum.org to ensure you have the latest version. Version 1.0 April 2006



Collaboration Oriented Architectures

Jericho Forum™ – Position Paper

Position Paper

Collaboration Oriented Architectures

Introduction

Collaboration Oriented Architectures (COAs) are information architectures that comply with the COA framework, outlined below. They enable enterprises that use them to operate in a secure and reliable manner in an environment of increasing information threat, and where it is the growing norm to interact without boundaries, irrespective of the location of the data or the number of collaborating parties.

This paper sets out the principal components that are needed in a COA to meet these requirements. Subordinate papers are published or are in development to describe these components. While many organizations are trying to respond to the de-perimeterization issue, they often lack a framework and set of guiding principles to organize and implement specific solutions. The paper aims to fill this gap.

The paper focuses on the need to have business processes that operate across and between multiple organizations, probably (but not necessarily) using the Internet as the common transport mechanism. In this environment, users and end-systems must securely interact with, or use services from, disparate systems that are outside any single locus of control or security domain.

Implementing a COA entails adoption of the Jericho Forum Commandments (JFC) (specifically Commandments #4 to #8[1]) covering the areas of operating in a hostile environment, trust, and authentication.

Problem

The traditional electronic boundary between a corporate (or 'private') network and the Internet is breaking down in the trend which we have called de-perimeterization.

Traditional approaches to architecting security solutions are aimed at securing organizational borders, and then the network, reinforcing a 'perimeterized' perspective. This is contrary to the future business needs of most organizations.

[1] JFC#4 - Devices and applications must communicate using open, secure protocols
JFC#5 - All devices must be capable of maintaining their security policy on an un-trusted network
JFC#6 - All people, processes, technology must have declared and transparent levels of trust for any transaction to take place
JFC#7 - Mutual trust assurance level must be determinable
JFC#8 - Authentication must interoperate/exchange outside of your locus of control

Always refer to www.jerichoforum.org to ensure you have the latest version. Version 1.2: Apr 2008

Business rationale for de-perimeterisation

Jericho Forum Commandments

Collaboration Oriented Architectures

Agenda

- Design principles, assumptions & caveats
- Requirements
- Solutions
  - Corporate e-mail
  - Secure Web access
  - Authenticated web solutions
  - End-point anti-malware & management
  - NAC & NAP
  - Integrating legacy systems
- Spin-off benefits & related solutions
  - Network reduction and resiliency
  - Wireless network infrastructure
  - Layered defence model
- Q&A

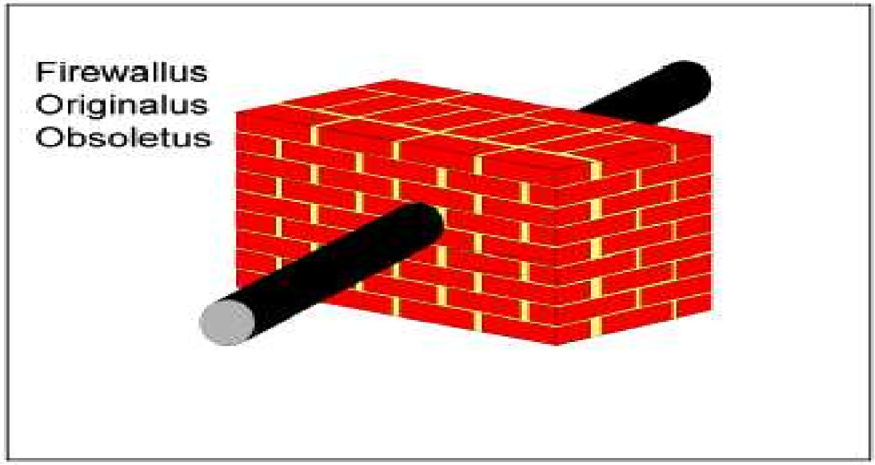
Design principles

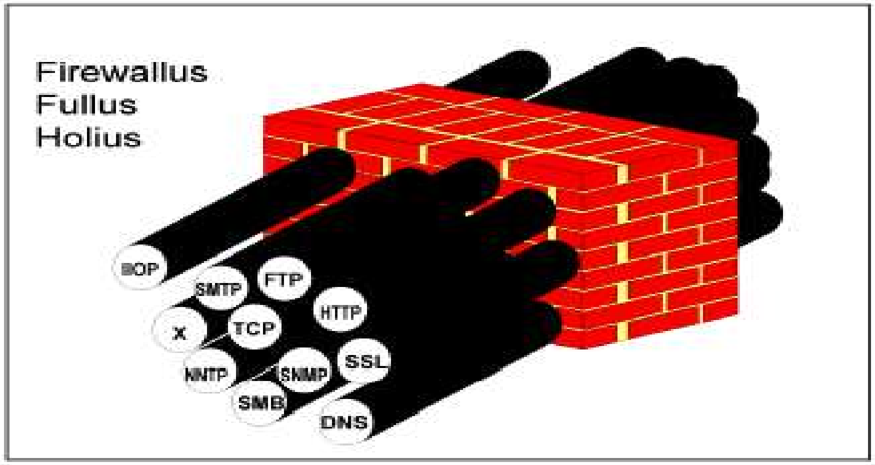
- Rule of thumb - the old engineering adage design for worst case
  - **Rule:** Design for Internet working
  - **Test:** could you (in theory) operate your entire corporation on the raw Internet
  - **Reminder:** Internal network provides QoS and cannot be guaranteed to provide any security
- Technology should be available today
- **Note:** This is the foundation for being able to utilise more collaboration technologies

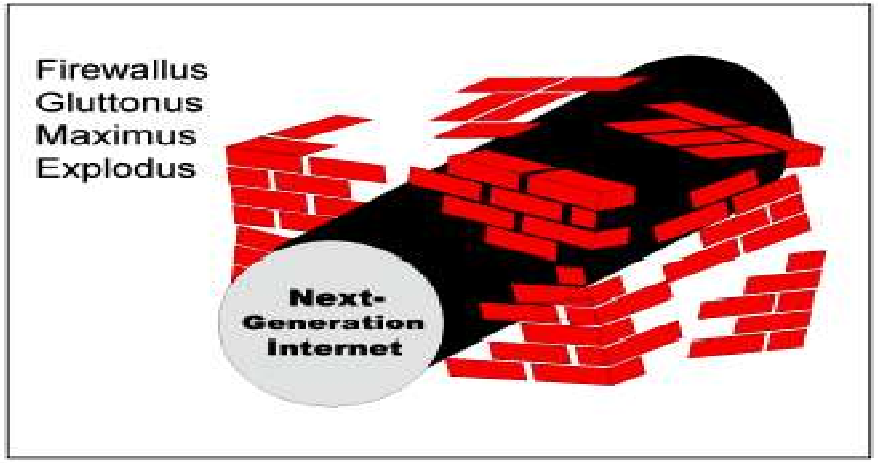
Design principles

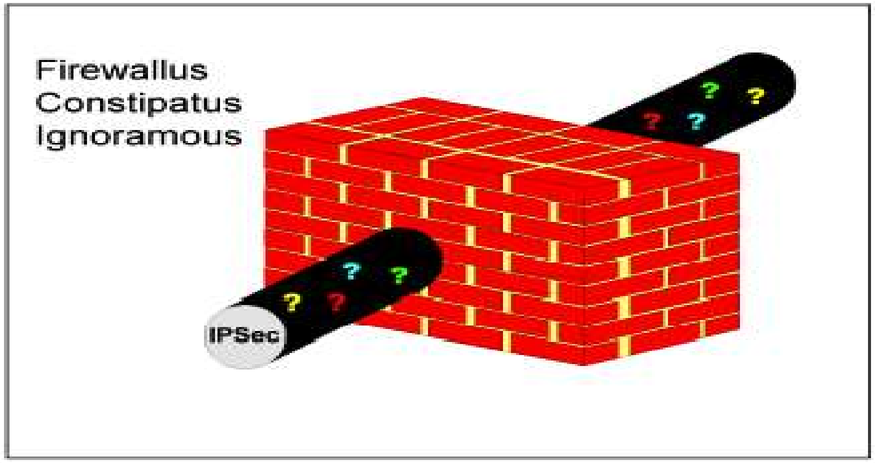
- Solution should operate **identically** in Intranet & Internet
  - Works as well within borders, just more secure (internally) due to better QoS
- Bake-in rather than bolt-on
  - Is generally more secure
  - Generally results in cheaper solutions
- Good (better) security practice & principles still need to observed
  - such as two-factor authentication

The problems with firewalls



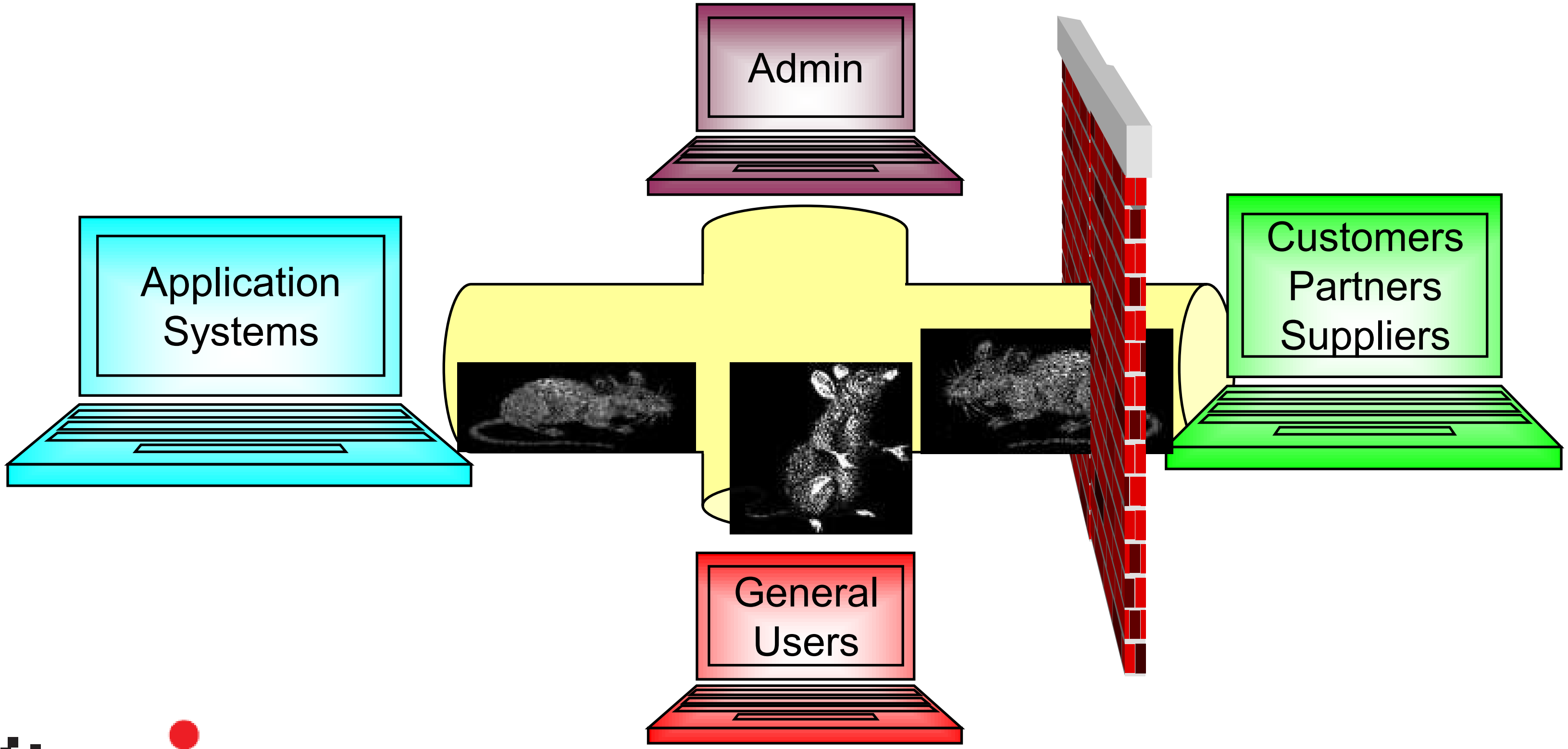




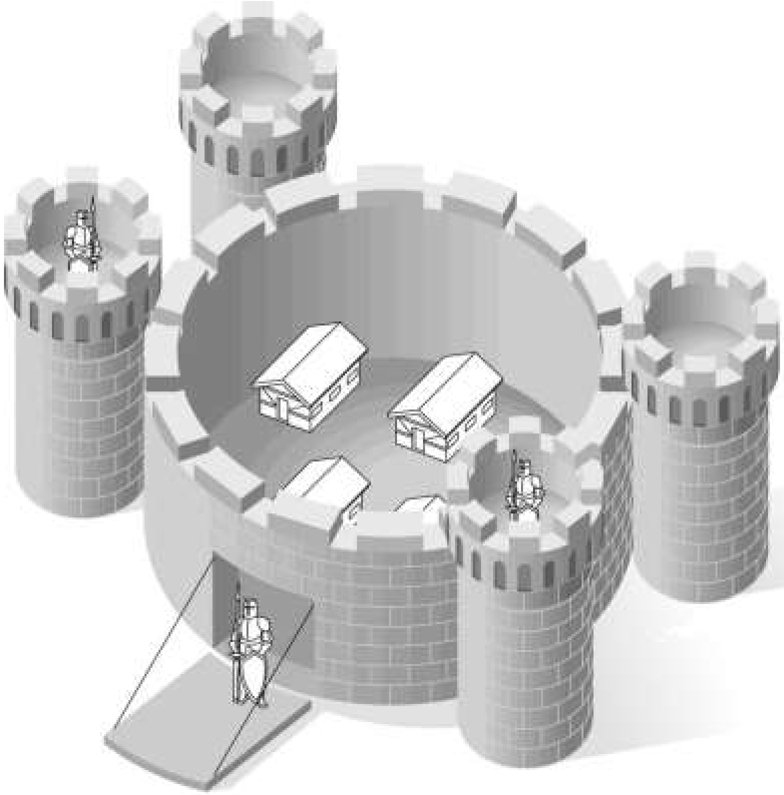


The problems with VPN

- General purpose IP Sec / SSL VPN is the Swiss-army knife of the security world



The problems with a fortress mentality

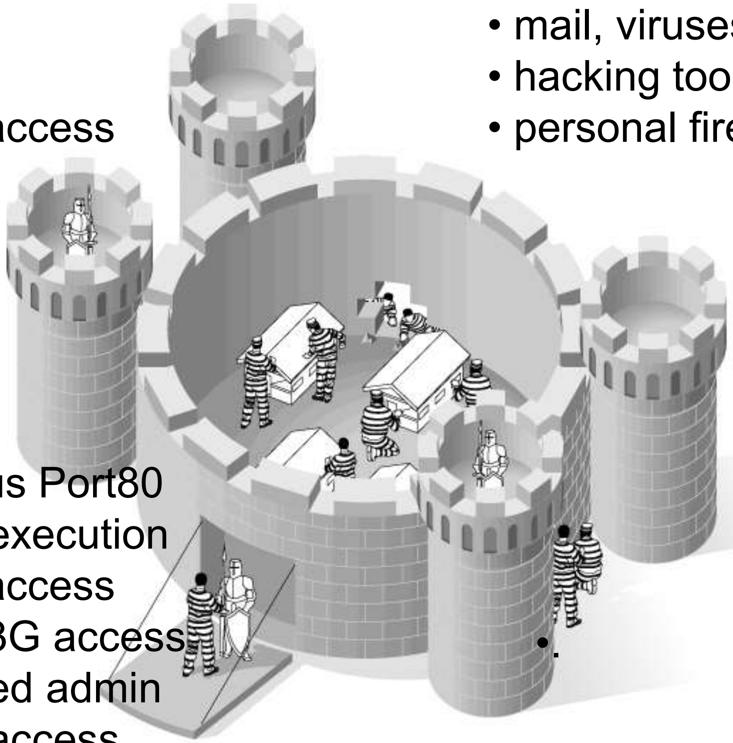


It used to be just a modem…

Now we have:

- Mobile computers
- USB memories
- PDA:s
- Software
- Internet access

- p2p
- VoIP
- mail, viruses
- hacking tools
- personal firewalls



- Ubiquitous Port80
- Remote execution
- Internet access
- WLAN, 3G access
- Outsourced admin
- Remote access
- etc

Use security solutions effectively

- Use firewalls to keep out “internet lumps”
  - “Home” firewall rules, no complex rule-set
- Use firewalls to front end systems
  - Simple, easy to maintain, IP and port rules
- Use VPN’s to front end legacy applications / systems, but not for general access
  - Restrict to specific IP’s and ports
- Protect systems and devices not networks

Old Thinking vs. Jericho Thinking

Old Mindset		New Mindset
▪ Connections to the secure network	→	▪ Connections to secure resources
▪ Connection-level authentication	→	▪ Protocol-level authentication
▪ Authentication to access the secure network	→	▪ Authentication to access individual secure resources
▪ Secure tunnel from device to network connection point	→	▪ Secure protocol from device directly to secure resources

Risks and benefits

Risks

- Get it wrong and expose the business
- Keep adding more layers of security
- Cost and/or inability to manage
- Saddled with yesterday's technology
- Inflexible to respond to market demands

Benefits

- Increased levels of security
- Simpler, less complex, more secure
- Cheaper to run, easier to manage
- Tomorrows technology with ability to gain business advantage
- Flexible and adaptable solutions

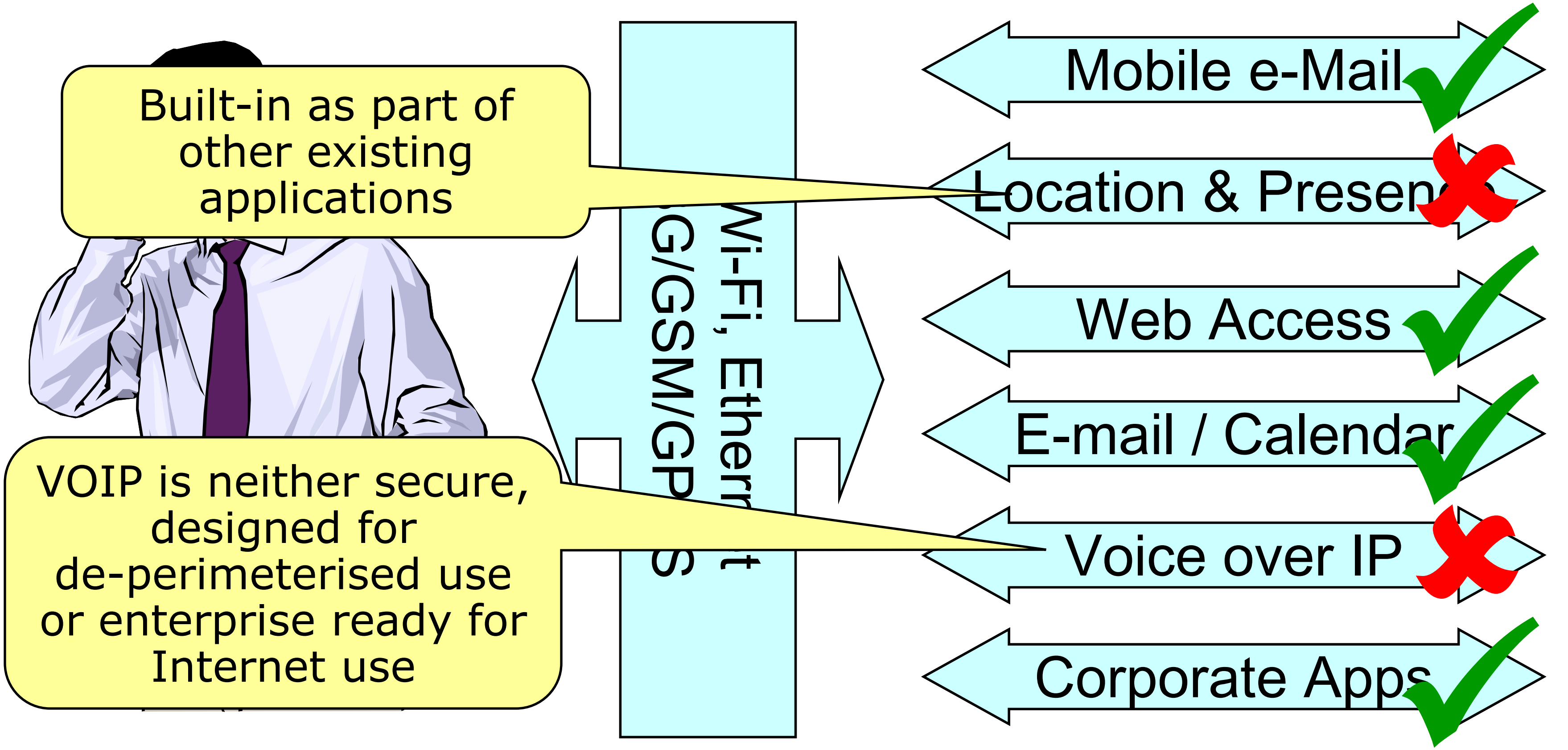
Definitions . . .

- **De-perimeterisation** is what is happening to you
- **Collaboration Oriented Architecture (COA)** – the architecture you adopt as a response
- **Re-perimeterisation**
  Right-sizing to where it does some good, while still enabling the business
- **Micro-perimeterisation**
  Moving the perimeter closer to the data (ultimately to the data itself)
- **Macro-perimeterisation**
  Moving the perimeter into the cloud
- **Definition**
  A single (protected) device has no border / perimeter

Assumptions

- Corporate device (assume a PC)
- Aim for identity based access
  - Two-factor authentication (something you have – the PC, and something you know – username)
  - Leverage the I&AM system you have today (assume for most people it's Active Directory)
- Assumption: Federated I&AM in the future, not now
  - But be positioned to leverage Federated I&AM when available
- Solutions based on currently available solutions
  - Base solution implementable today
  - Under 10% bespoke or near-future product roadmap

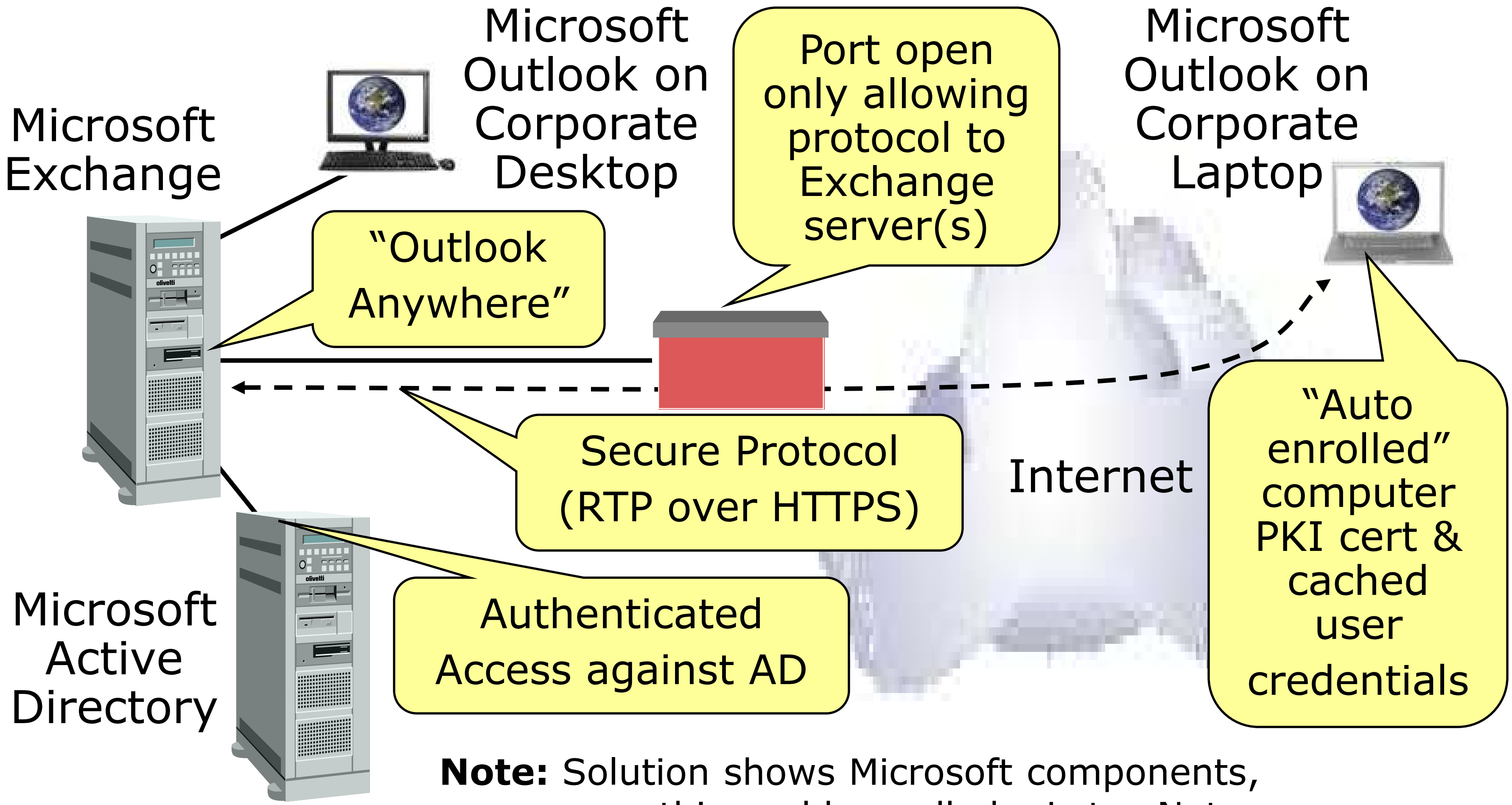
Requirements



Built-in as part of other existing applications

VOIP is neither secure, designed for de-perimeterised use or enterprise ready for Internet use

End-point solution – E-mail



Microsoft Exchange
Microsoft Outlook on Corporate Desktop
Port open only allowing protocol to Exchange server(s)
Microsoft Outlook on Corporate Laptop
"Outlook Anywhere"
Secure Protocol (RTP over HTTPS)
Internet
"Auto enrolled" computer PKI cert & cached user credentials
Microsoft Active Directory
Authenticated Access against AD

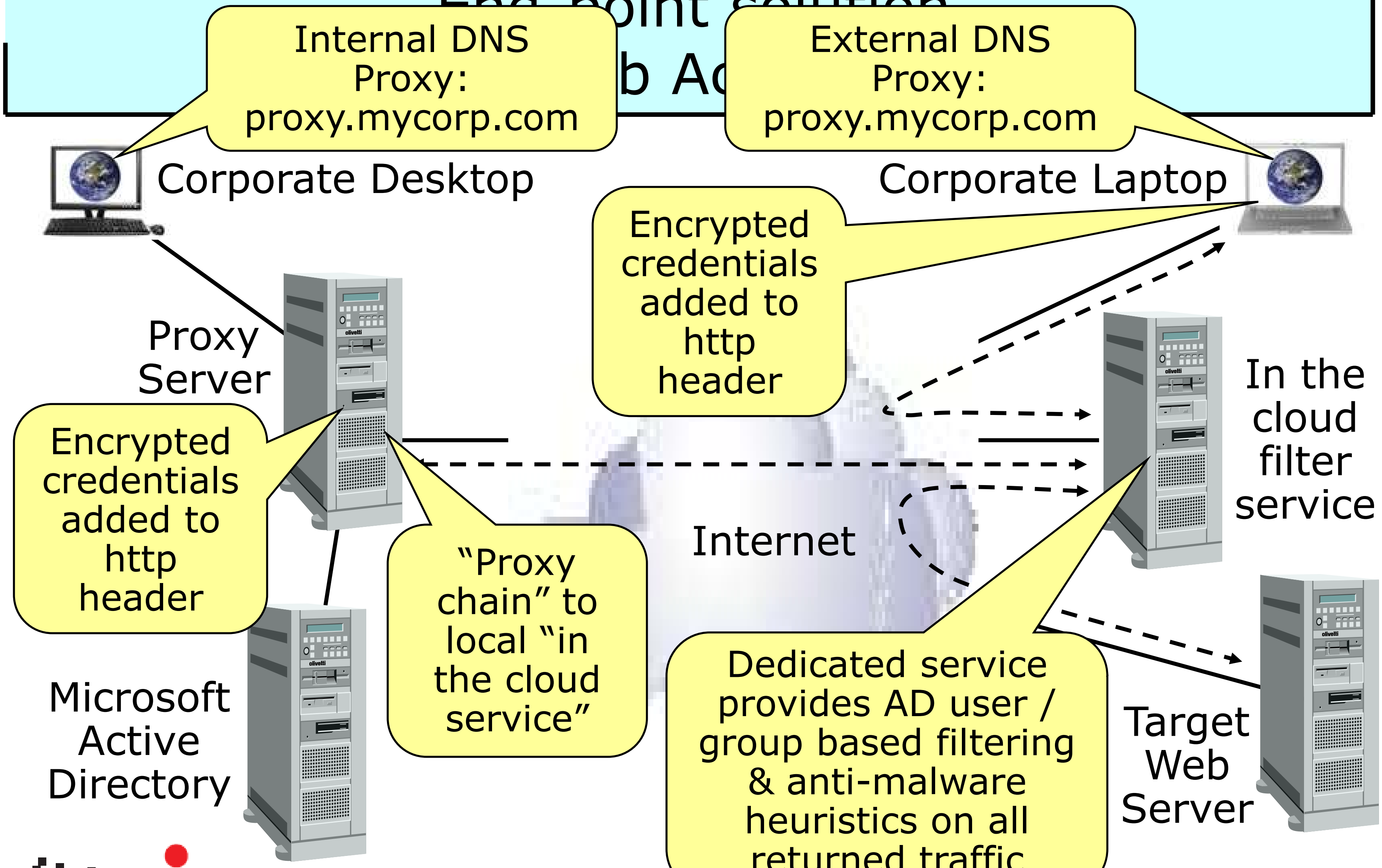
Note: Solution shows Microsoft components, this could equally be Lotus Notes

End-point solution – E-mail

- Very user friendly and intuitive
  - Just connect as you would internally
- Still a need for "clean-pipe" to e-mail server
  - Using MessageLabs, Postini etc.
- Still a need for a holistic e-mail solution
  - Web Access for occasional users
  - Blackberry (or other "push" email solutions)

  Note: *Web Access and Blackberry obey the principle of working identically inside and outside the perimeter*
- Issues with embedded (internal) links
  - Unless those servers externalised (see later)
  - Potential same issue with blackberry solutions

End point solution
b Ac



Internal DNS Proxy: proxy.mycorp.com

External DNS Proxy: proxy.mycorp.com

Encrypted credentials added to http header

Encrypted credentials added to http header

"Proxy chain" to local "in the cloud service"

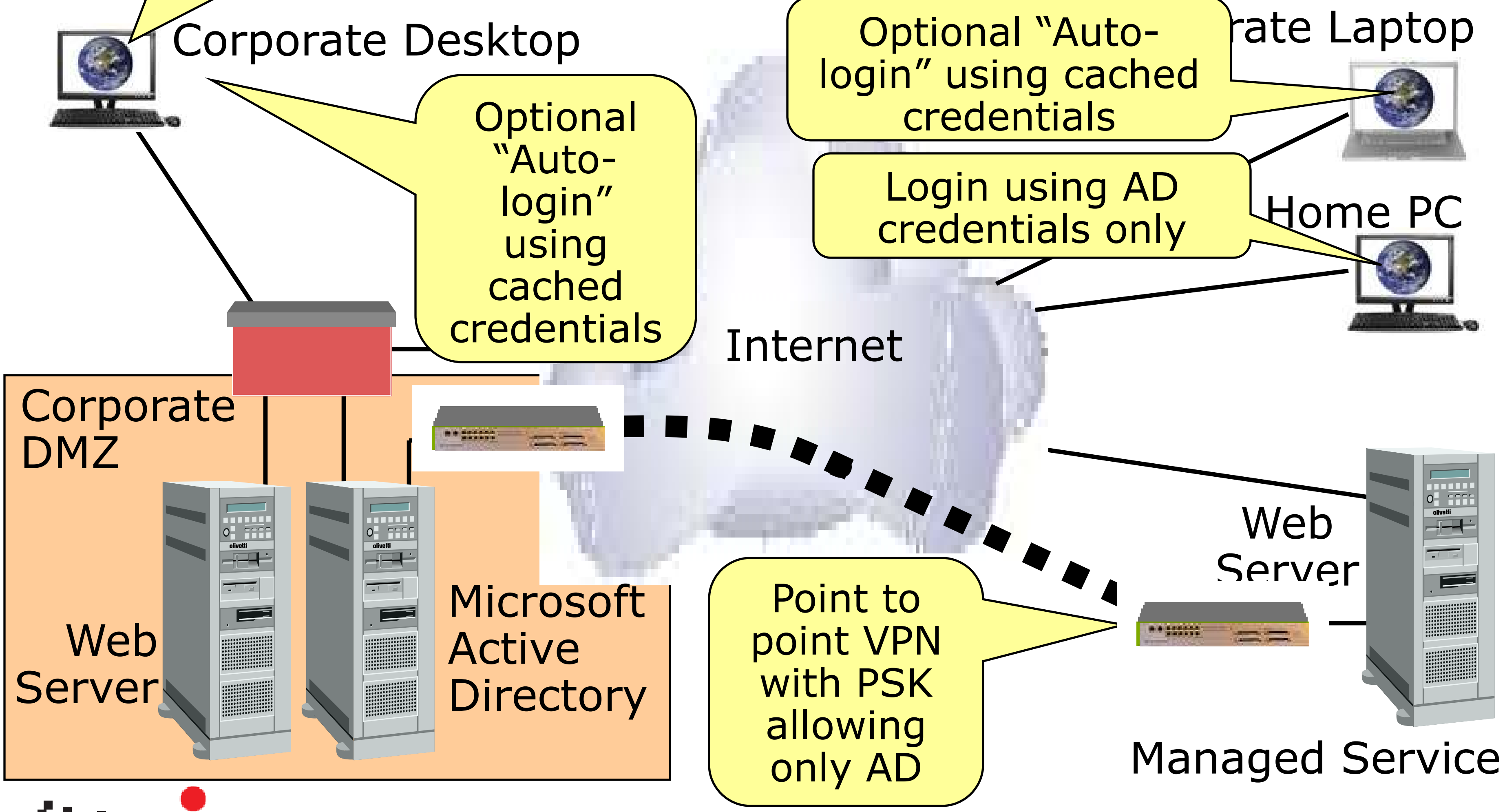
Dedicated service provides AD user / group based filtering & anti-malware heuristics on all returned traffic

End-point solution
Web Access

- Better security
  - Provides global consistent URL access rules based on AD
  - Browsing via a “clean-pipe” using heuristics
  - **Example**: 15k user organisation, blocking 9k incoming web-sites / month for malware / spyware etc.
- Always protected, even when on Internet
  - Uses cached AD credentials to provide identical application of URL access rules
- Fixes “China” browsing issues
  - Just buy a service with tower infrastructure inside “Great Firewall of China”
- TCO very similar to “in-house” / DMZ model
  - Huge benefits for usability and security

Access
https://myapp.mycorp.com

t solution
Authenticated Web Access



Corporate Desktop

Optional "Auto-login" using cached credentials

rate Laptop

Optional "Auto-login" using cached credentials

Login using AD credentials only

Home PC

Internet

Corporate DMZ

Web Server

Microsoft Active Directory

Point to point VPN with PSK allowing only AD

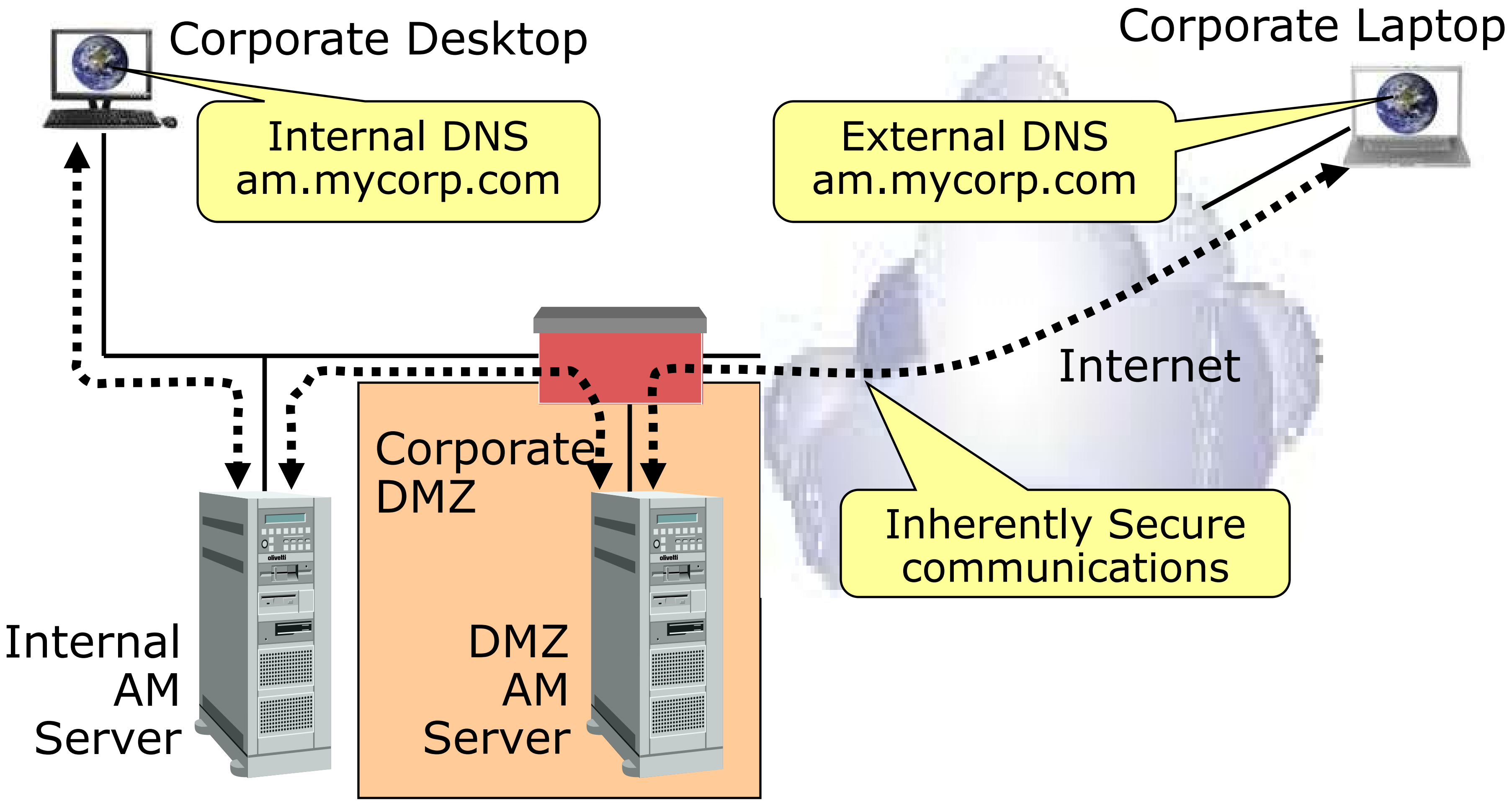
Web Server

Managed Service

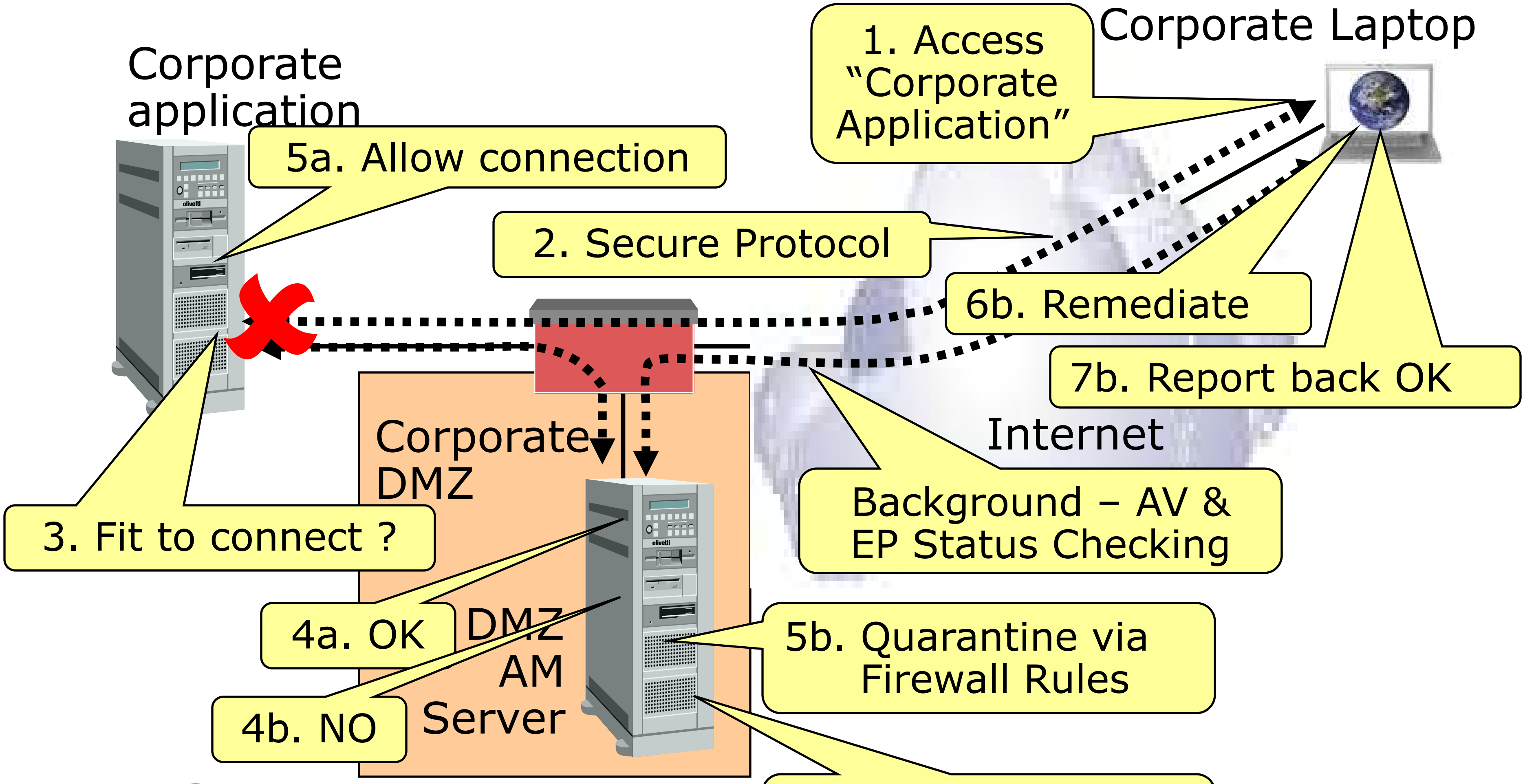
End-point solution
Authenticated Web Access

- Consistent user experience whether internally or externally
- Fixes the "e-mailed embedded links" issue when receiving e-mail remotely
- Allows access from other than corporate PCs
- Use DMZ solution when back-end connection required to corporate systems
- In future use a federated I&AM solution or secure protocol to link systems instead of VPN

End-point solution
Anti-Malware / End-Point Management



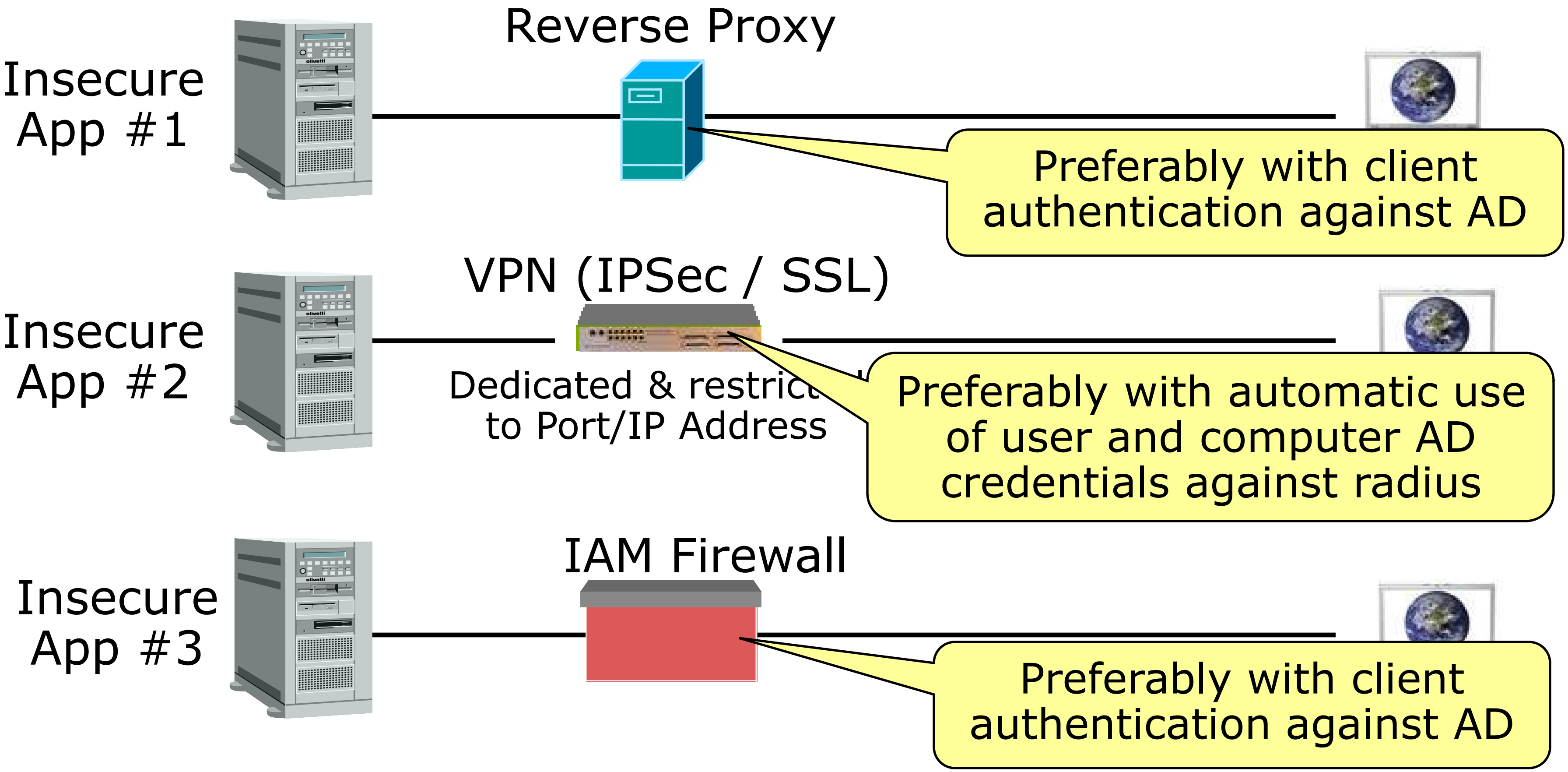
End-point solution - Future (Custom)
NAC / NAP



End-point solution
Anti-Malware / End-Point Management

- **Caveat:** may be multiple management servers for;
  - anti-malware
  - configuration management
  - software & patch roll-out
- Improved security
  - Always able to talk / update / log / manager end devices
- Always protected, even when on Internet
- Ability to manage security posture even if remote
  - Consistent management of ALL devices irrespective of location
  - Change firewall rules (automatically) based on security / configuration / risk / location of end-point device

End-point solutions – Legacy Systems



Insecure App #1

Reverse Proxy

Preferably with client authentication against AD

Insecure App #2

VPN (IPSec / SSL)

Dedicated & restrict
to Port/IP Address

Preferably with automatic use of user and computer AD credentials against radius

Insecure App #3

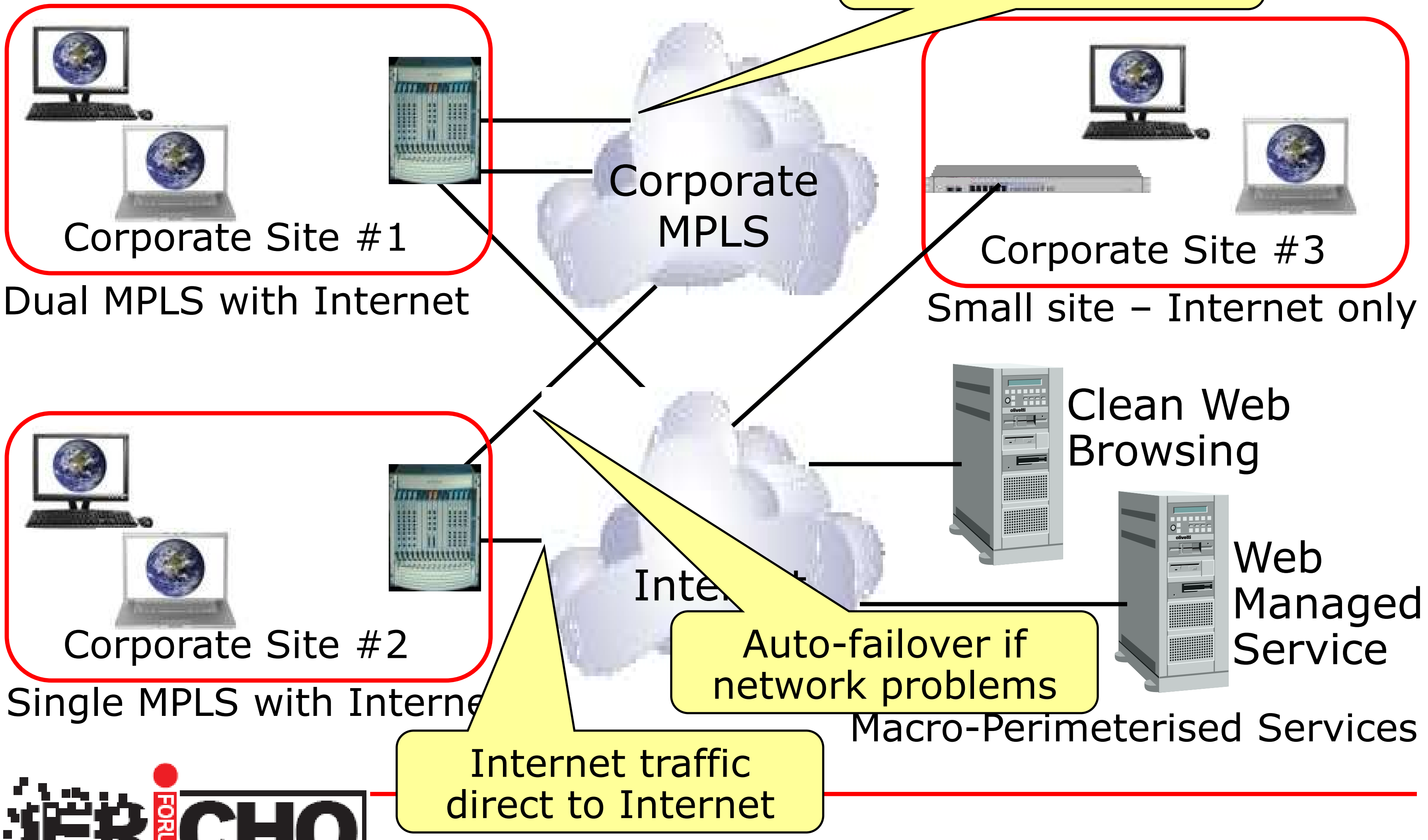
IAM Firewall

Preferably with client authentication against AD

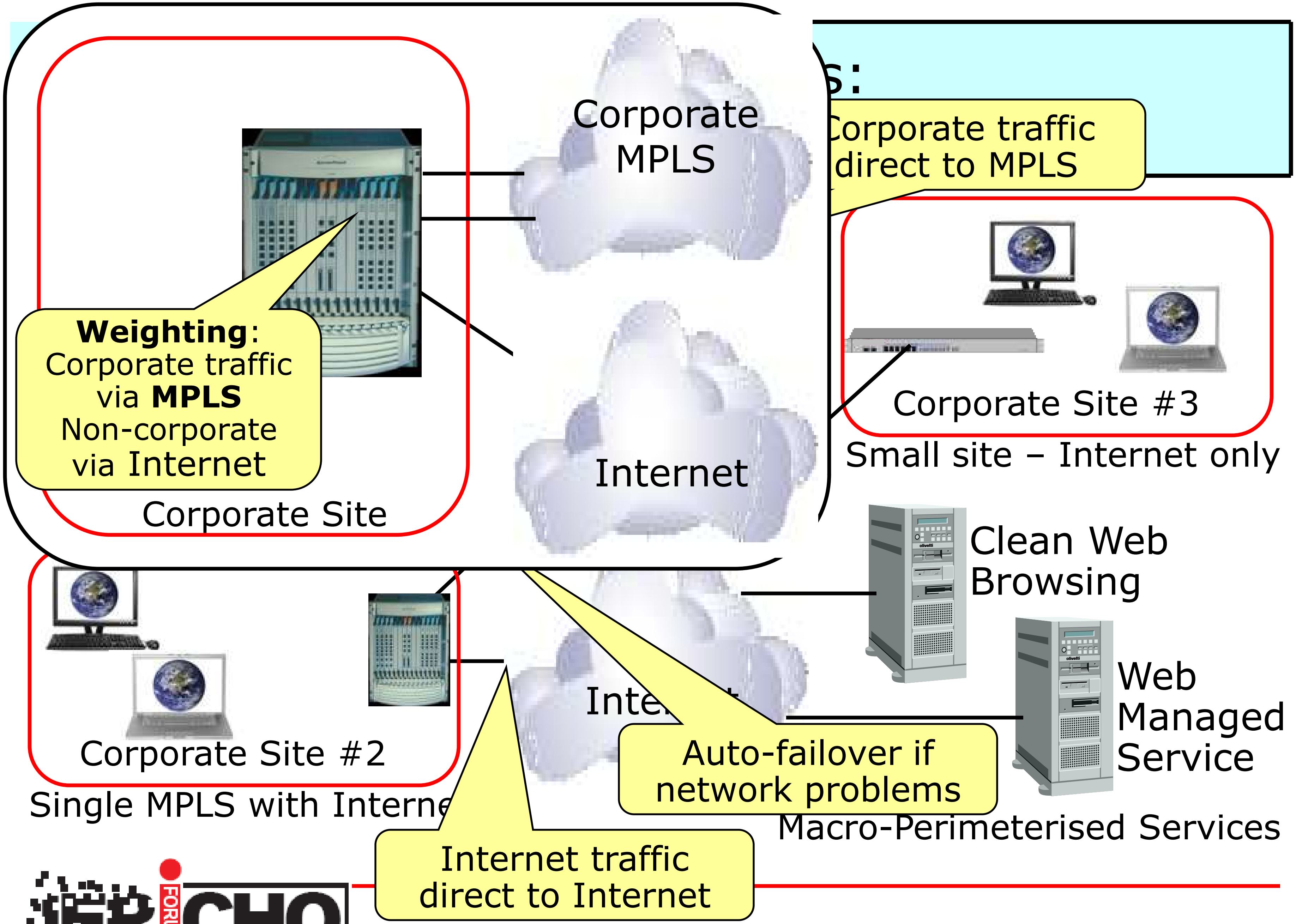
End-point solutions – Legacy Systems

- Leverage existing credentials to give a good / transparent user experience
- Use SSO or direct authentication against AD at the legacy application
- Your design should take into account the QoS implications of the total end-to-end connection path
  - But this is just good system design

Other solutions:
Network Reduction &



Corporate traffic direct to MPLS
Corporate MPLS
Corporate Site #1
Dual MPLS with Internet
Corporate Site #3
Small site – Internet only
Clean Web Browsing
Corporate Site #2
Internet
Web Managed Service
Auto-failover if network problems
Single MPLS with Internet
Macro-Perimeterised Services
Internet traffic direct to Internet



s:

Corporate MPLS

Corporate traffic direct to MPLS

Weighting: Corporate traffic via **MPLS** Non-corporate via Internet

Corporate Site

Internet

Corporate Site #3

Small site – Internet only

Clean Web Browsing

Web Managed Service

Corporate Site #2

Single MPLS with Interne

Inte

Auto-failover if network problems

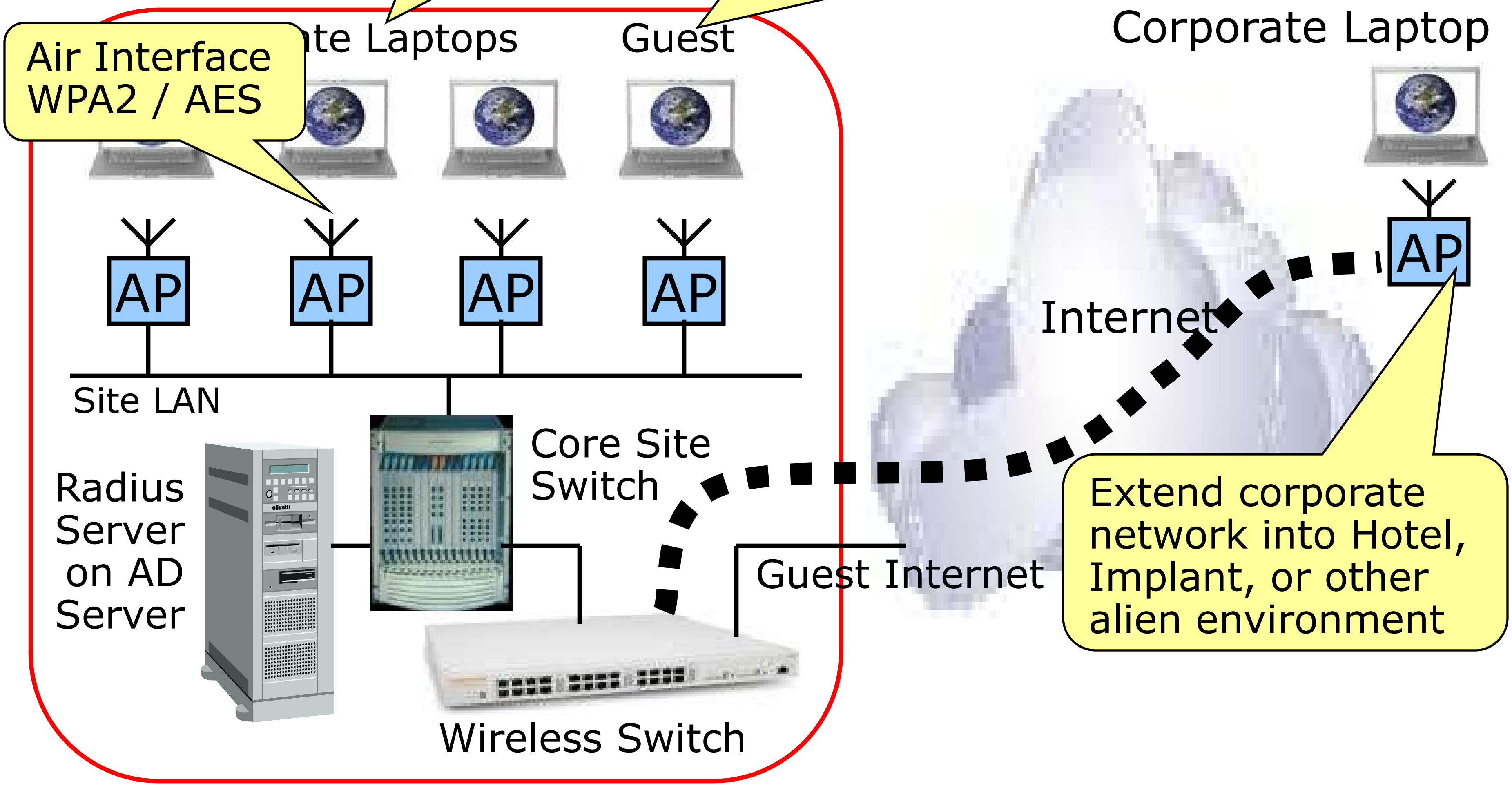
Macro-Perimeterised Services

Internet traffic direct to Internet

Other solutions: Network Reduction & Resiliency

- Enterprise more resilient to problems
  - Full automatic failover
  - Traffic flow optimised
  - Increased PoPs means harder to DoS
  - Simple rule-set means easy to manage
  - Use TCP/IP and IP protocols that way they were originally meant!
- Will need legal addressing to implement
  - For most this probably implies IPv6
- Reduced cost
  - Only sites that warrant QoS now need MPLS
  - Potential to save up to half the cost of current corporate MPLS network (your mileage will vary)

O solutions: Wireless



SSID (Hidden) mycorp-private

SSID mycorp-guest

Air Interface
WPA2 / AES

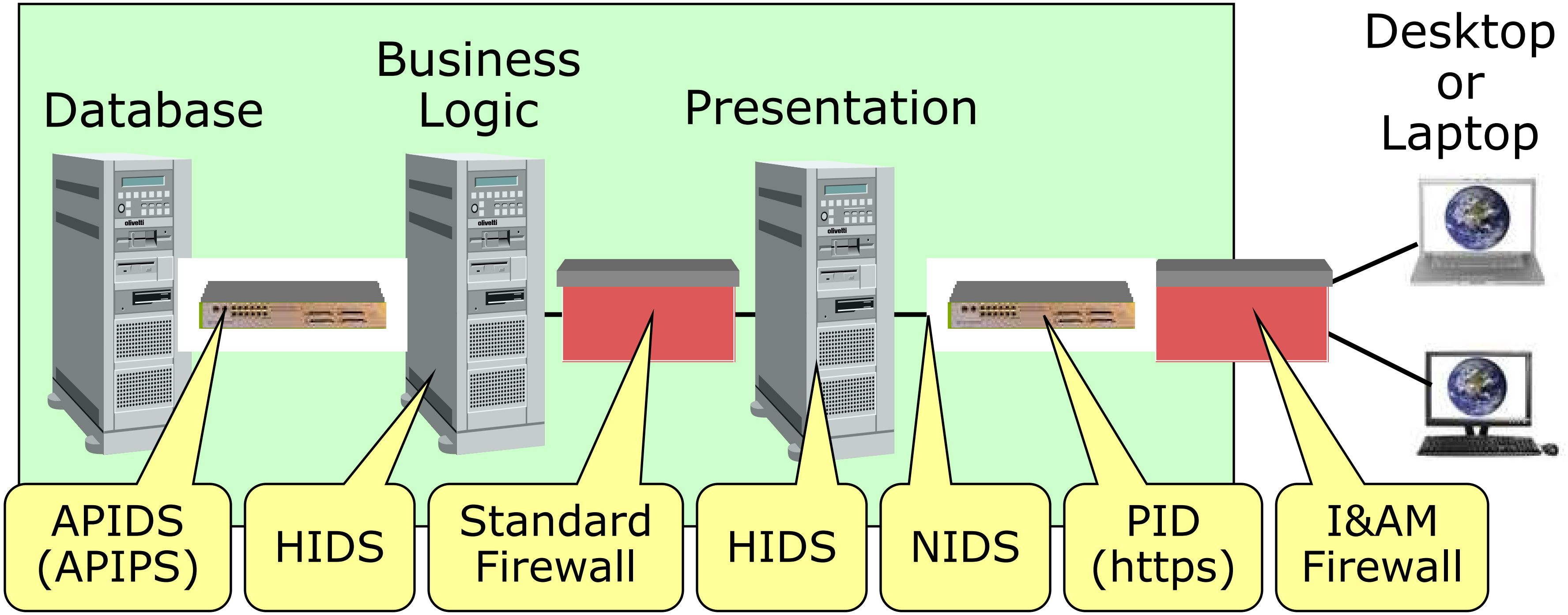
Extend corporate network into Hotel, Implant, or other alien environment

Other solutions: Wireless

- Transparent wireless access for authenticated users
  - Lift lid, screensaver password and just connect
  - More secure than most office / wired networks
- Dual-use Access Point to give guest users Internet access (optional)
- Extend a perimeterised network into a remote environment
- Still a need for connection control in a de-perimeterised world
  - Risk is NOT to insecure devices on the network (as we don’t trust the Network anymore); but
  - Risk to to rogue devices affecting QoS on Intranet
  - Risk to reputation of hackers accessing Internet via corporate gateways

Other solutions
Layered defence in a de-perimeterised world

- Moving your layered defence model to where it does some good!



Othe
Layered defence in

Jericho Commandment #1:
"It's easier to protect an asset the closer protection is provided"
-
APIDS is the first intrusion detection technology where it should be feasible to enable "protection" (APIPs) without undue risk of business disruption

- Glossary:
  - I&AM = Identity a
  - PID = Protocol usion
  - HID = Host Intrusion Detection
  - APID = Application Protocols Intrusion Detection (eg: SQL)
  - APIP = Application Protocols Intrusion Prevention
- Good security design is still layered!
- Depending on model you will use all or some of the security solutions
- In web applications PIDs will need to be between SSL and web front-end
- Localised firewalls should mean;
  - simpler rules (easier to define, write and understand)
  - less change (and can understand two years for now)

Conclusions

- You are being de-perimeterised whether you like it or not
- Designing for a de-perimeterised world gives;
  - Increased security
  - Increased business capability
  - Happier users
- The technology to start implementing this exists today