



Implementing an Effective Network Architecture

Joe Reves
HP Services

© 2004 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice



Introduction

- Elements of an Effective Network Architecture
- HP's Adaptive Network Architecture experience
- Adaptive Network Architecture illustrated
- Governance and the Adaptive Network
- Accountability and the Security Culture
- The landscape of “Adaptive” solutions
- Return on investment in a virtualized infrastructure



“Fundamentally, the network as we once knew it is changing. It's no longer just your network, but also the network of your customers, your partners, your competitors, and of course, your adversaries. It's a network ecosystem where private and public boundaries collide, disappear, and relationship-driven boundaries emerge. It's a network ecosystem that's become life-critical to doing business. And while there are enormous efficiencies to be gained from sharing online resources - for example, in B2B commerce, trading communities, enterprise portals - we have to take the good with the bad. In an ecosystem with the kind of interconnectivity I just described, the role of security becomes very complex.”

Rich DeMillo

Former CTO, Hewlett-Packard
Company



The genesis of the Adaptive Network



- Architecture discussions began in spring of 1999
- Originally tagged, “The Bubble Architecture” by the “NAG”
- Internal IT operations very distributed, organizationally and culturally. Centralized “architecture” team providing standards/guidance
- Risk acceptance involved a time – consuming consensus process with many participants
- Both the balance of internet-bound traffic and the balance of partner connectivity was shifting rapidly
- HP was facing a major divestiture: Agilent Technologies, which would require restructuring of the network



Business Drivers

- HP could not move fast enough in the Internet economy
 - Adopting new business models
 - Integrate new partners, suppliers, customers
- Difficulty adopting new technologies
 - Publishing content
 - Managing public Internet access
- Difficulty adopting and managing outsource suppliers
 - NetAccess Internet (remote employee access)
 - Internet Service Providers
- Difficulty divesting & acquiring new businesses
- Difficult/impossible to measure success & impact of the security program (e.g. policy changes)
- **Exception process resulted in *greater risk and increased cost***
- Businesses lost opportunity by an inability to collaborate, share, and exchange information with partners securely
 - Either accept risk and drop security, or don't share
- Businesses could not manage their own risk without affecting risk to the rest of the company.
- Protection mechanisms were either absent, or were inconsistent and not leverageable across the infrastructure.
- Business were looking for a “magic bullet” solution that does not exist
 - Any solution required significant work by the businesses
- Infrastructure assumes an “HP Only” environment.
 - Company culture limited our ability to meet emerging business needs.

An Effective Architecture delivers:

Networks need to do 5 fundamental “new” things

- Create rapid infrastructure access for partners, customers, employees and suppliers without compromising security
- Integrate or split to support organizational changes (mergers, acquisitions, divestitures)
- Enable rapid implementation of new business models (transactional websites, supply chain mgt, outsourced functions, collaboration, customer relationship mgt)
- Provide geographic independence for common business functions (I.e. support global operations goals)
- Reduce the need for “one off” solutions by providing ubiquitous, simplified architecture applicable to the majority of demand

Cyclical Governance (pre-merger hp)



Corporate IT Centric

- Centralized Organization
- Central Billing / contracts
- Focus on common services (80%)
- Funded by “corporate tax”
- Strongly enforced standards

Business IT Centric

- Distributed Organization
- Regional Billing / contracts
- More focus on custom services
- Funded directly by the business
- Corporate “stewardship” model

~ 18 – 24 months

The Agility dynamic

Strategy:

The additional Dimension to improve agility, and positively Impact existing dimensions



Improve agility:

- Enable the IT environment to adapt to changing business needs (support 5 “new” goals of IT)

Manage costs:

- Lower operations and acquisition costs
- Manage fixed costs
- Optimize fixed vs. variable costs
- Manage cost of change

Increase quality:

- Improve levels of availability and response time
- Extend service levels across the enterprise

Mitigate risk:

- Ensure security and continuity of business operations
- Risk of innovation
- Impact of technology implementation

Agility Metrics and Principles

Measure and assess
business agility

Time

The length of time it takes to
make a change

+

Range

The breadth of change the
company is able to handle

+

Ease

The level of effort, cost, and
risk required to introduce
and support change

Implement through
critical people and
governance processes



Architect and integrate by applying
a consistent set of design principles

Simplification

- Reduce number of elements
- Eliminate customization
- Automate change

+

Standardization

- Use standard technologies
and interfaces
- Adopt common architectures
- Implement standard processes

+

Modularity

- Break down monolithic
structures
- Create reusable components
- Implement logical architectures

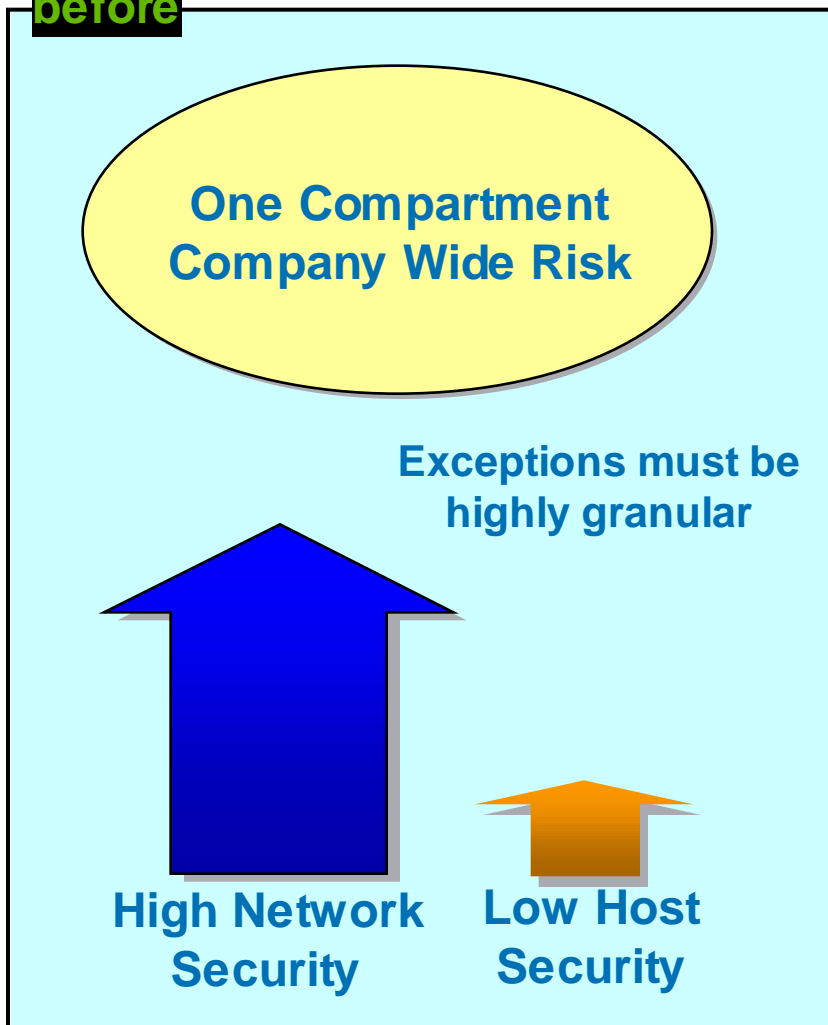
+

Integration

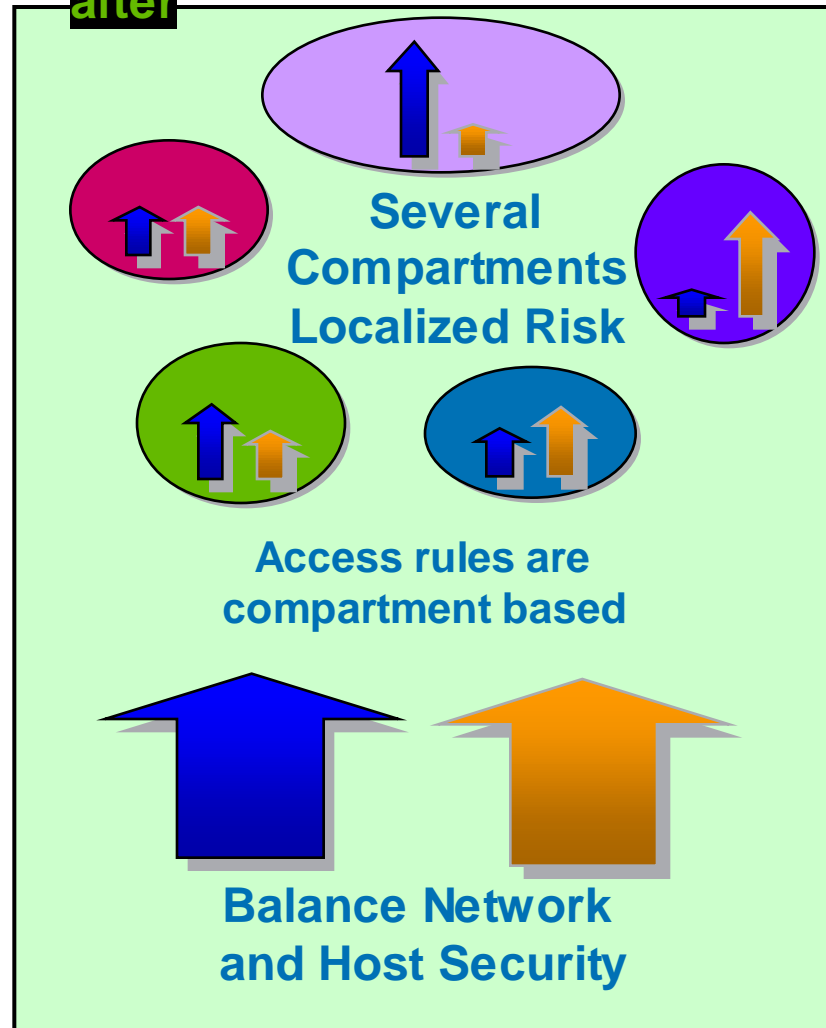
- Link business and IT
- Connect applications and
business processes within
and outside the enterprise

Balance and Granularity

before



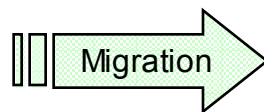
after



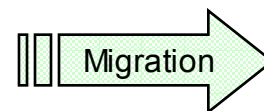
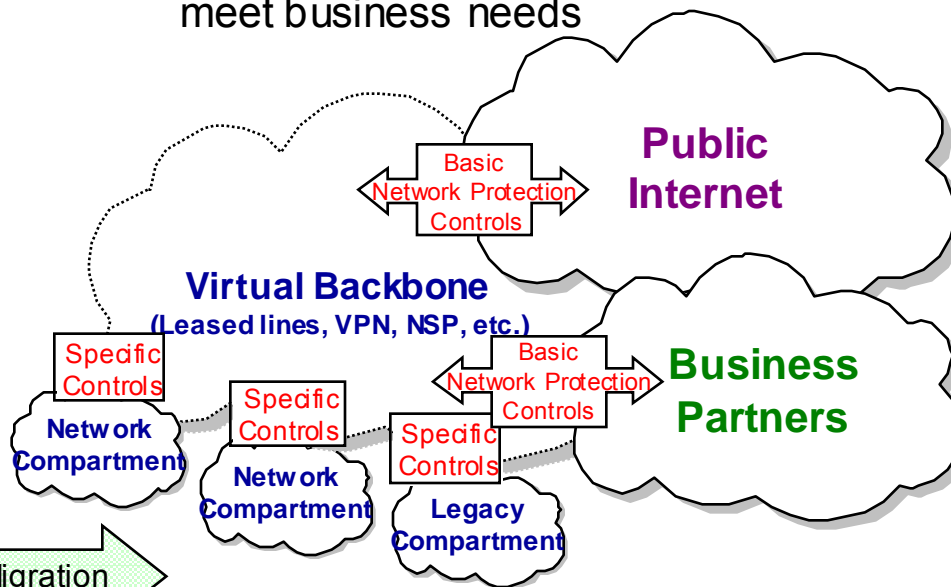
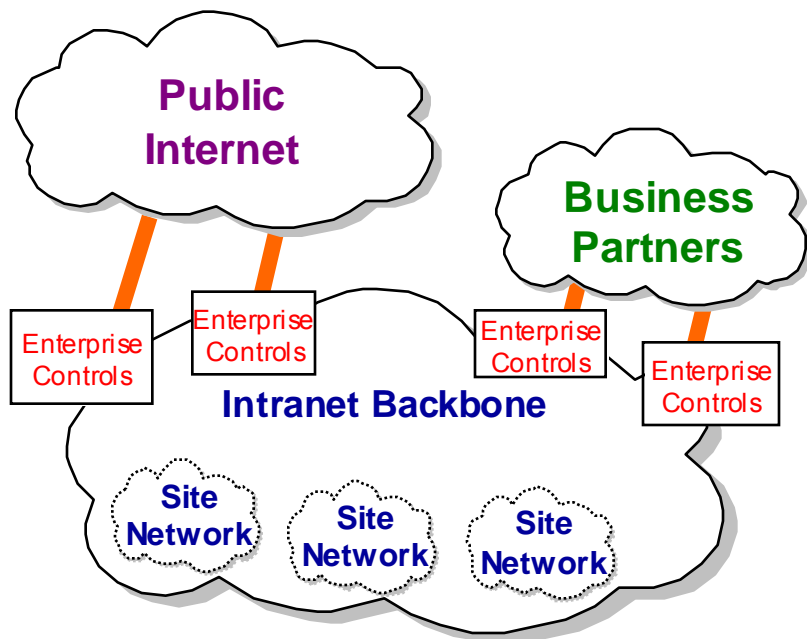
Compartmentalize for Agility

Traditional Network: Enterprise-wide controls protect Intranet network resources ...

Compartmentalized Network: Network compartment-specific controls protect business network resources ...



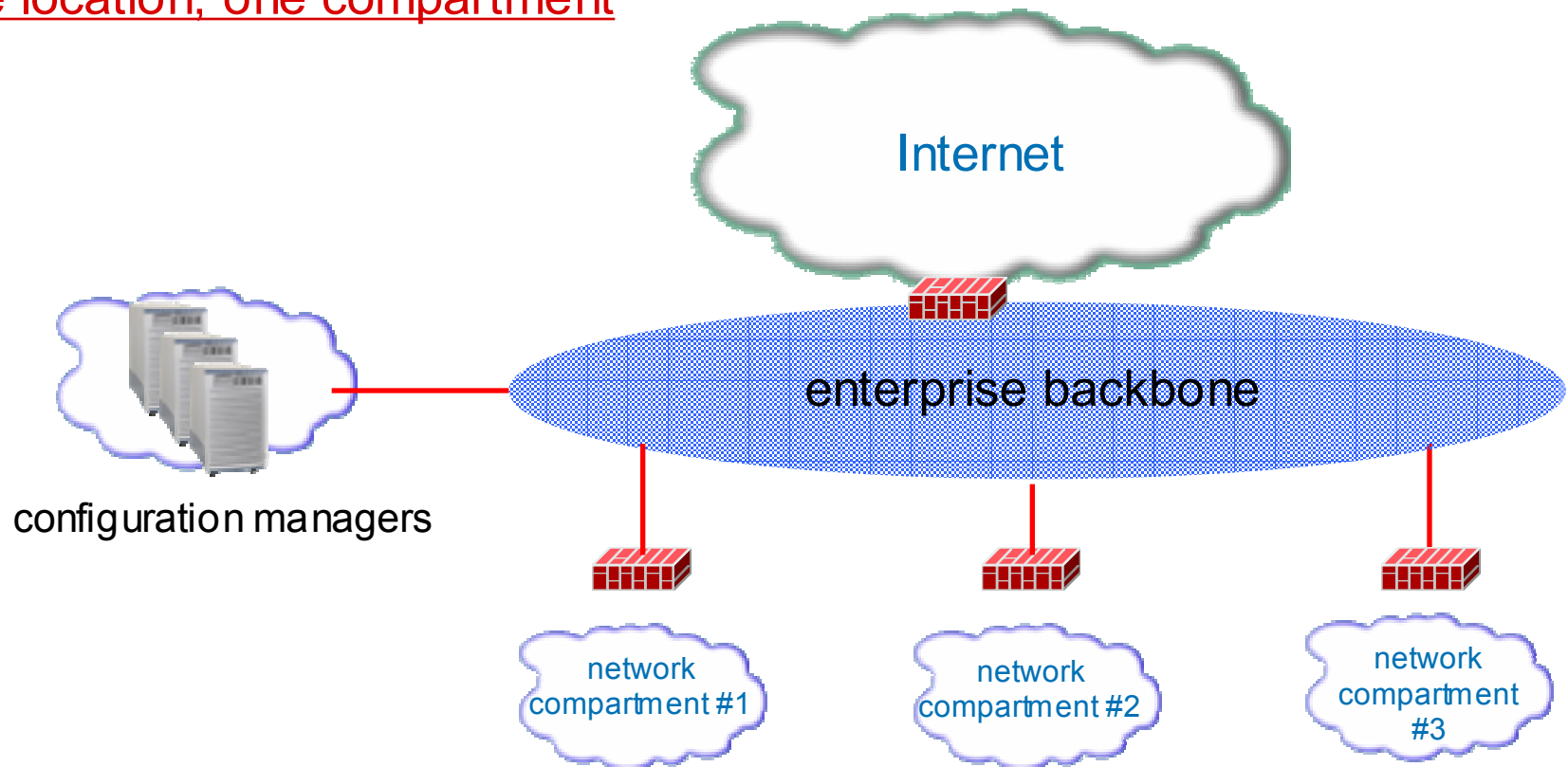
- Basic network protection security controls needed to mitigate nuisance attacks and provide a basic level of security for the backbone
- New network compartments created to meet business needs



Conventional Compartmentalization



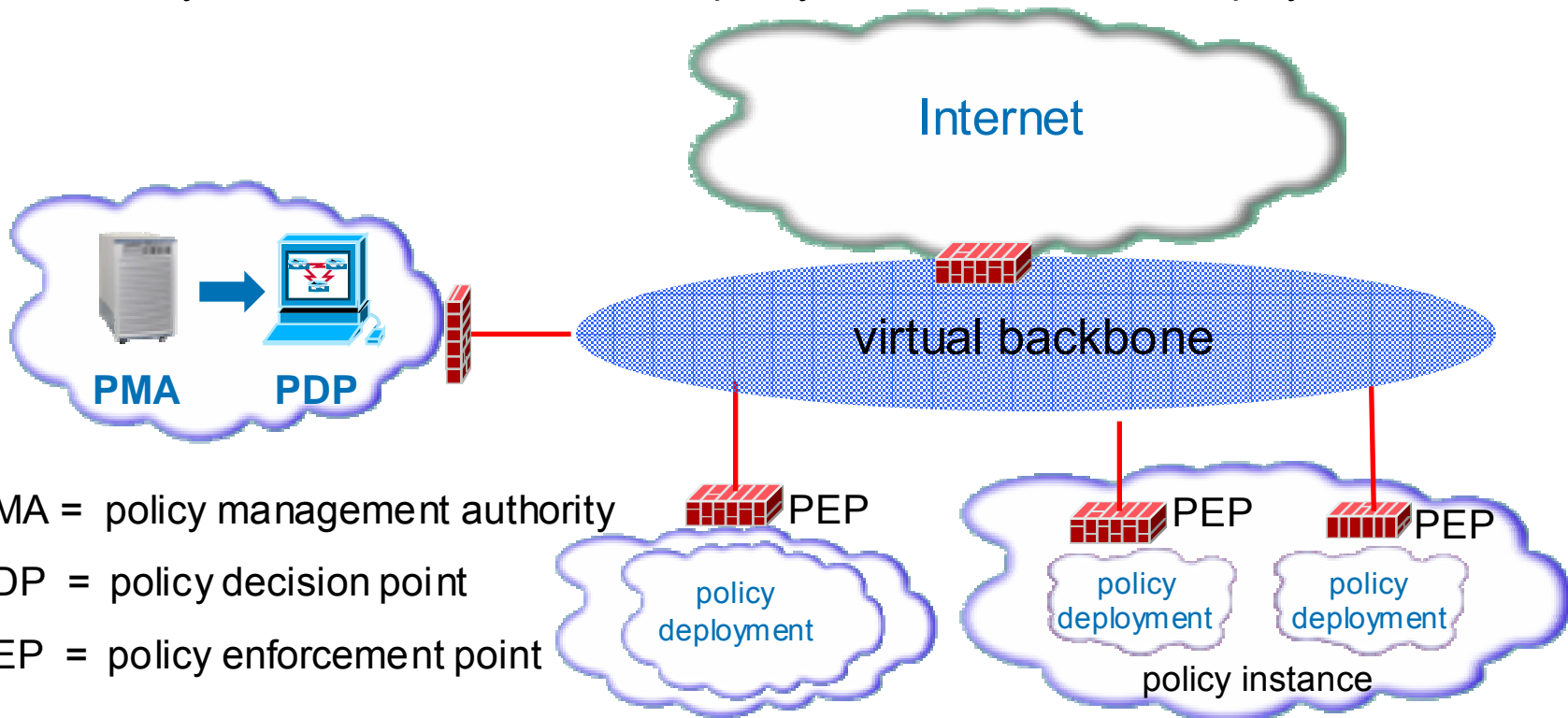
- Core enterprise backbone provides connectivity
 - Configuration manager(s) for both perimeter and internal access controls
 - Configuration manager deploys ACLs
 - Internal Firewall controls configured on each compartment boundary
- One location, one compartment



Adaptive Network Architecture



- Virtual backbone enforces address integrity
- Central policy registry generates access policies
- Device configuration manager provisions policies onto devices
- Policy enforcement takes place at the deployment boundary
- Common policy is extended for all deployments in the policy instance
- Granularity of control is extended to the policy instance level for all deployments

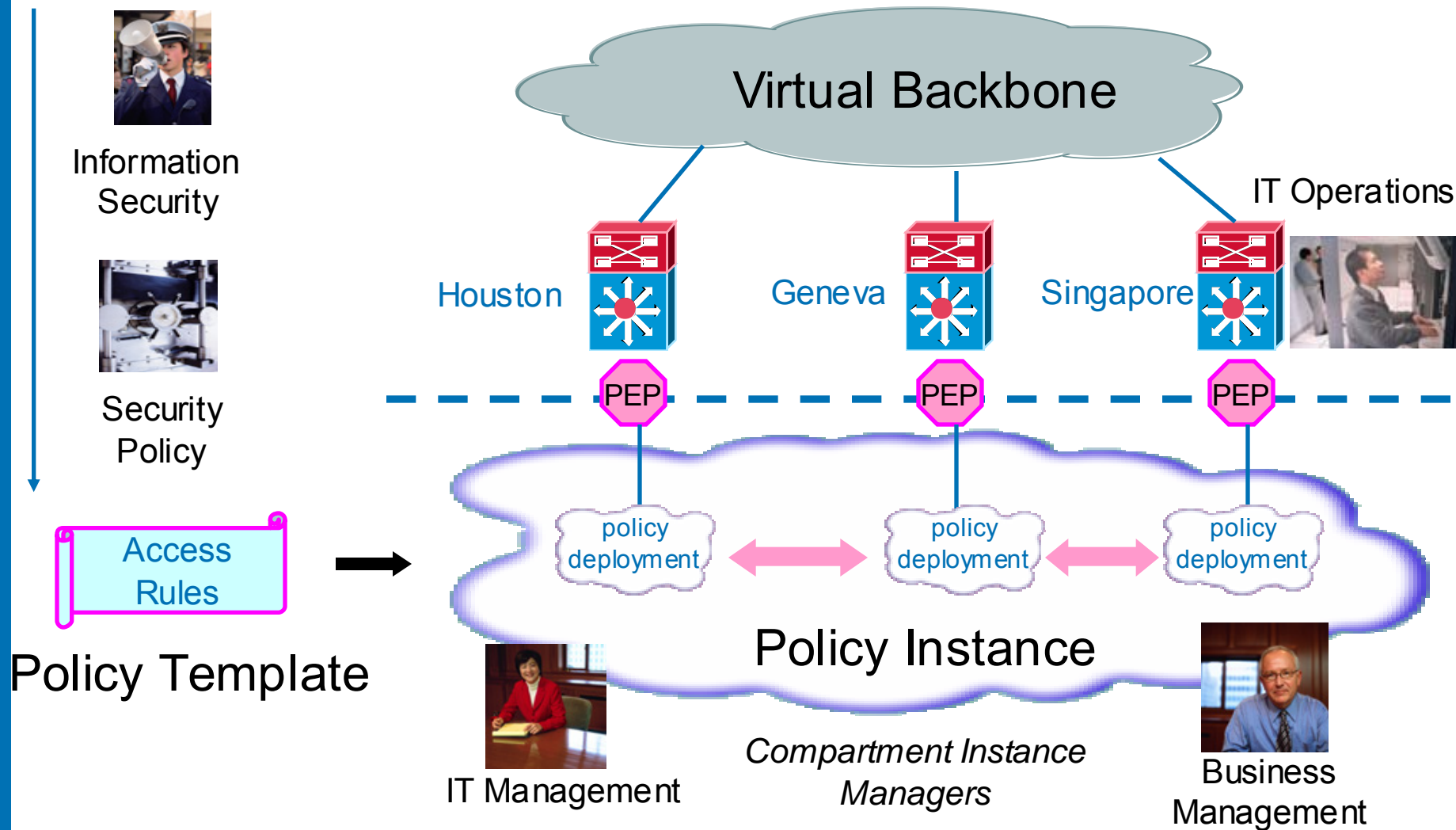


PMA = policy management authority

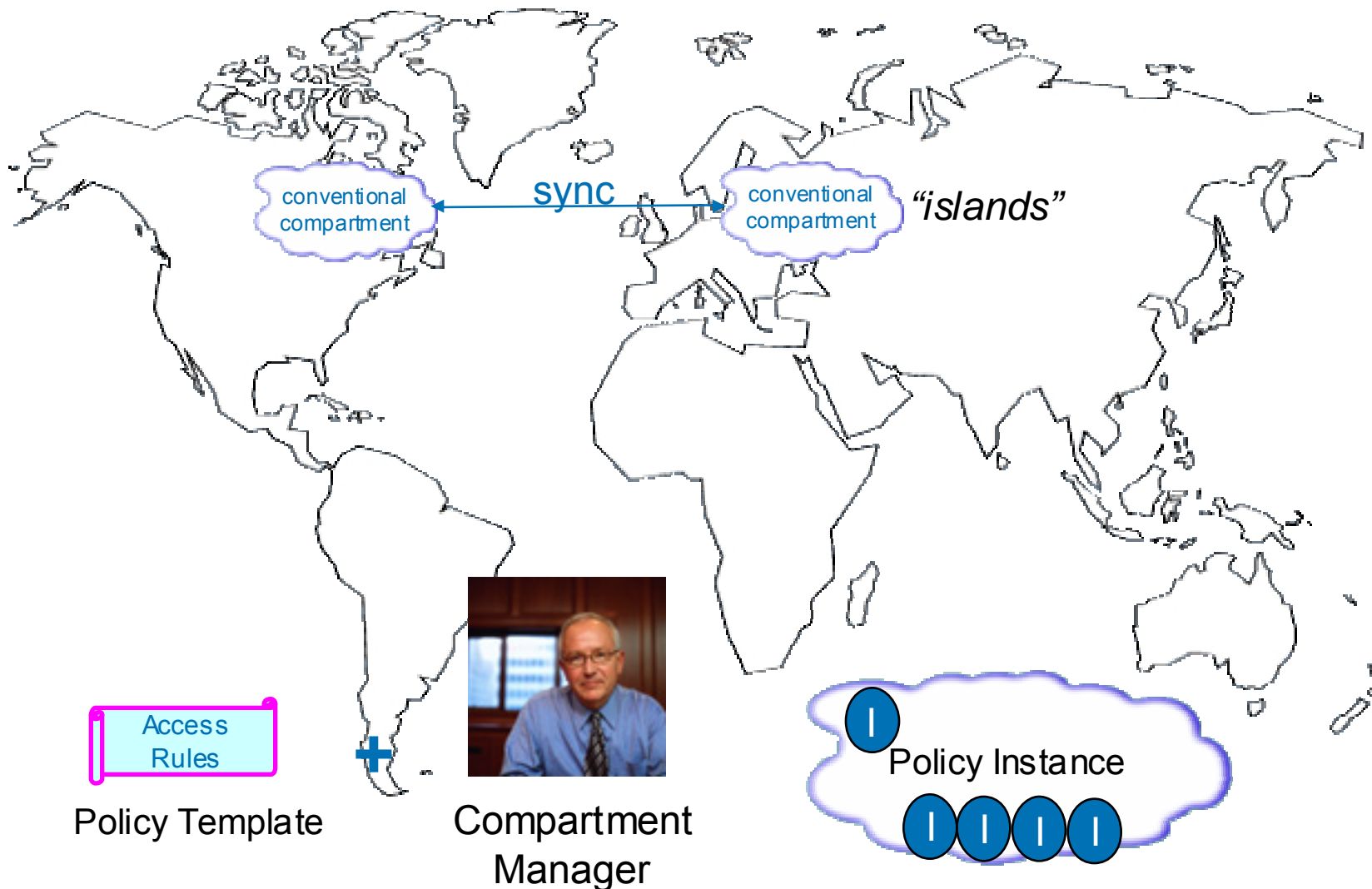
PDP = policy decision point

PEP = policy enforcement point

Policy Hierarchy



Global versus Regional Governance

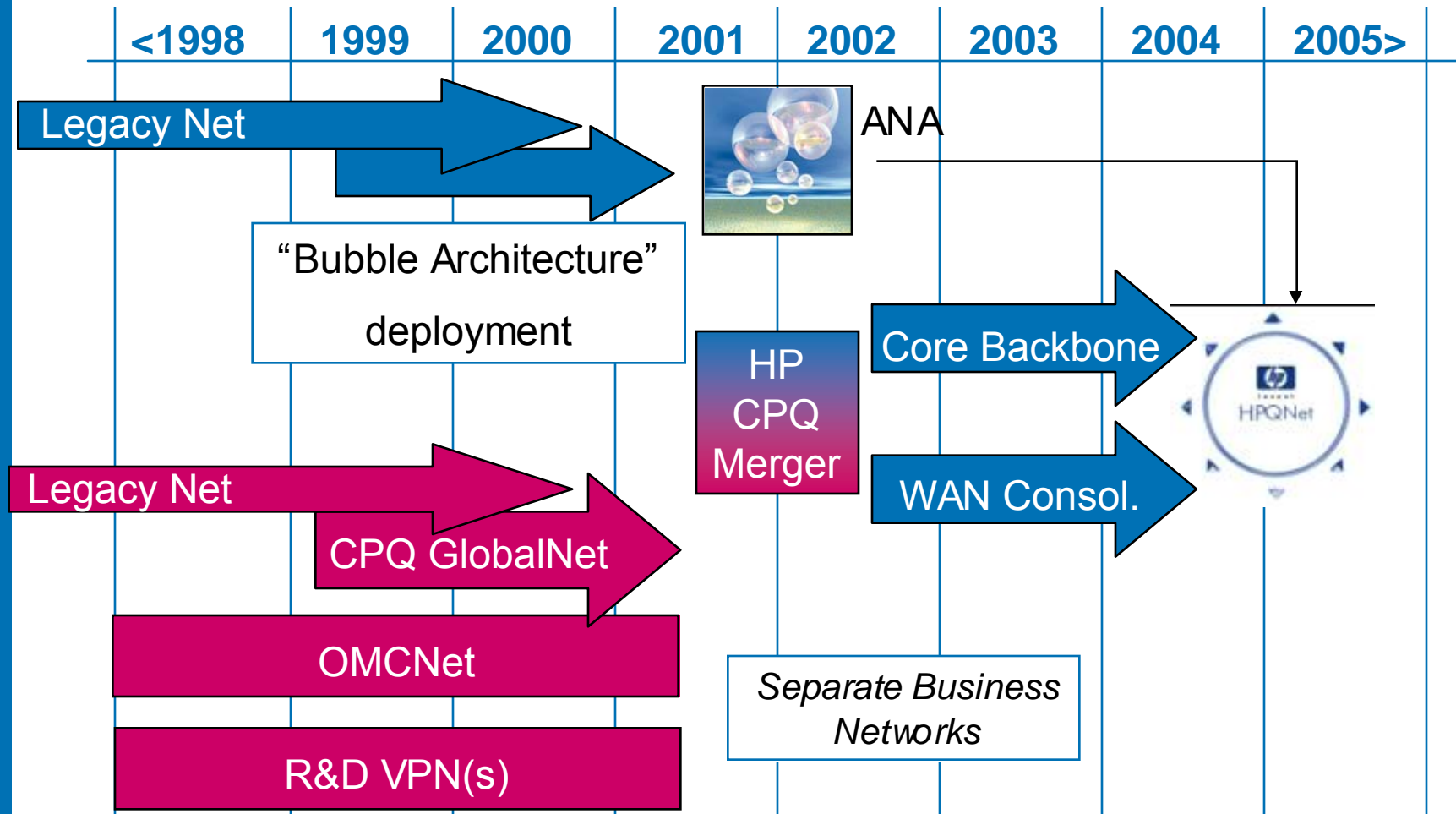


Accountability and Governance

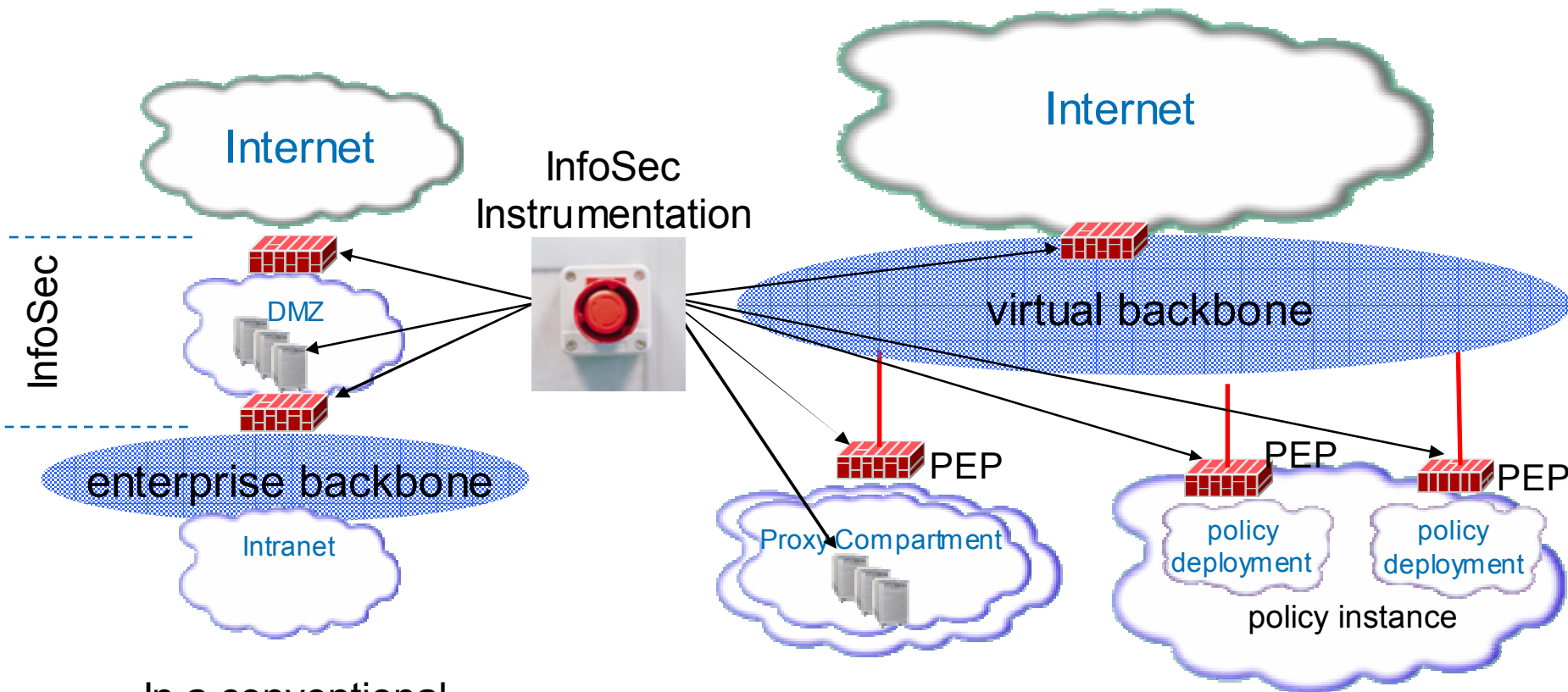
- Giving businesses the freedom to accept structured risk improves agility
- A delegated security model shares accountability between Information Security, and the business's Compartment Instance Manager.
- Compartment instance managers assume more accountability than in the traditional model of compromise with InfoSec



Governance and Architecture in HP

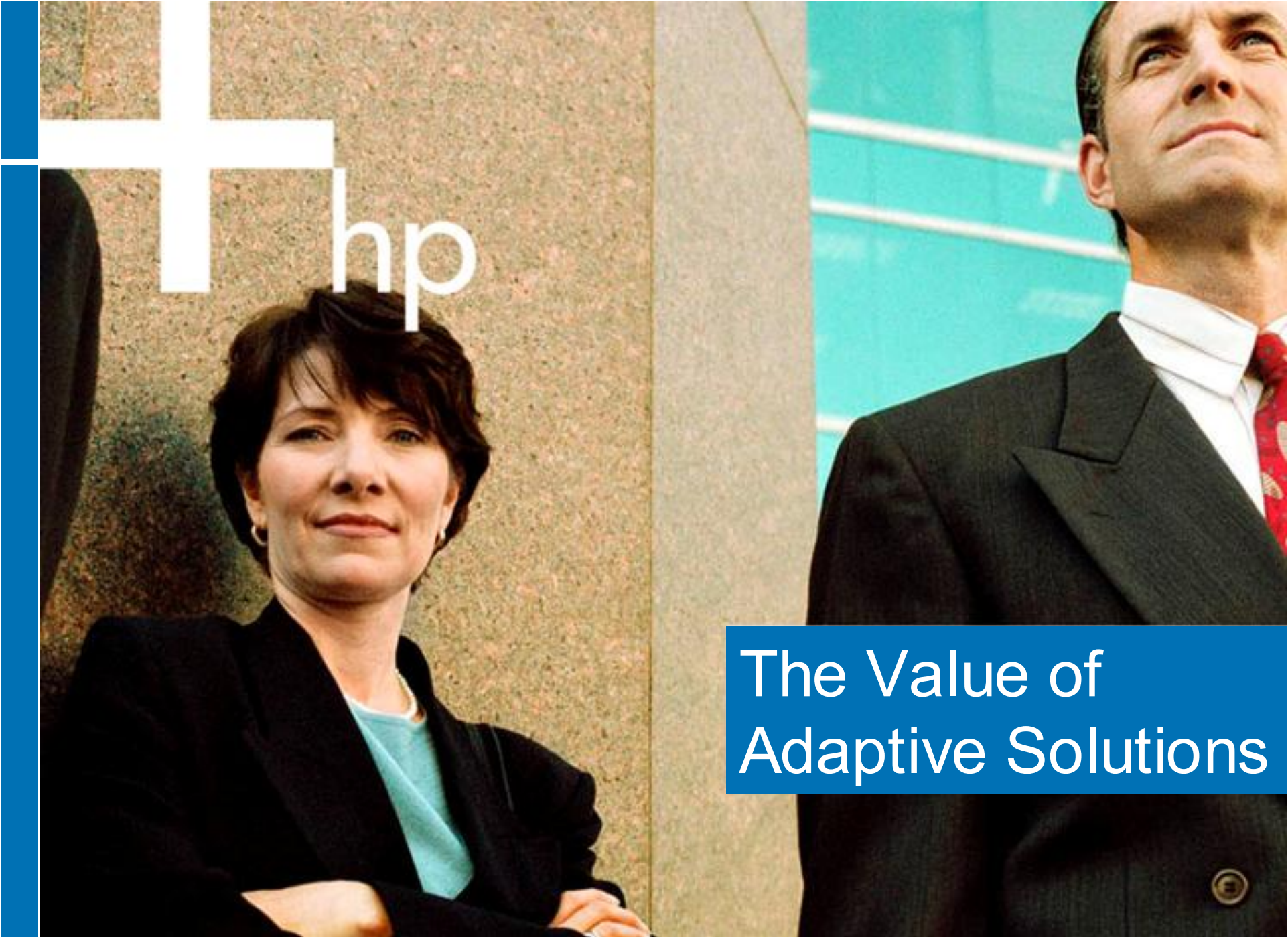


Working with Information Security



In a conventional network architecture, it's clear where the "knobs" are located

In a compartment network architecture, it's a more complex, but richer set of instrumentation



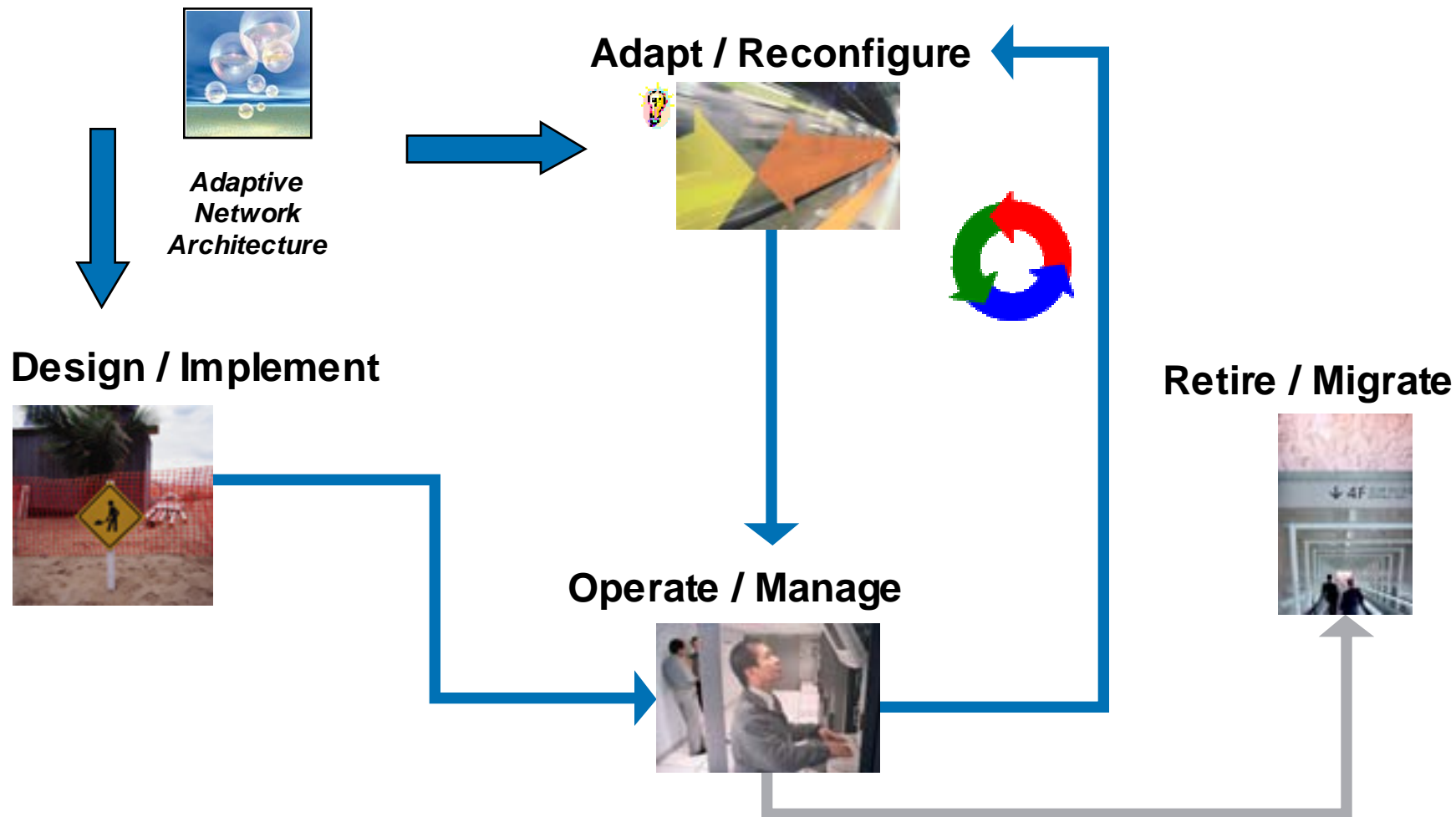
hp

The Value of Adaptive Solutions

The Adaptive Solutions Landscape

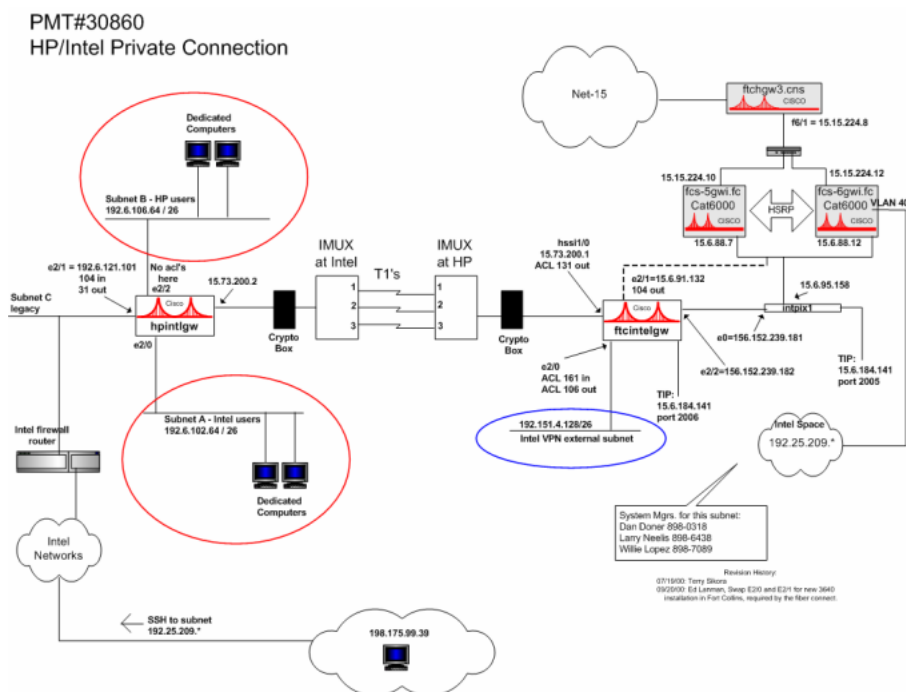
- Adaptive Capacity
 - Systems that are capable of providing flexible capacity based upon demand (either reactive, or predictive)
 - grid computing solutions, “on demand”, “pay-for-use”
- Adaptive Monitoring
 - Systems that can analyze and self-regulate based upon a stream of events or collected data
 - Moving beyond a static policy store, “learning” systems
 - “autonomic” solutions, “adaptive baselining”
- **Adaptive Functionality**
 - Systems that are deliberately architected to support functional change on demand, rather than designed against static requirements
 - HP Adaptive Network Architecture and Utility Data Center fit here

Infrastructure Lifecycle



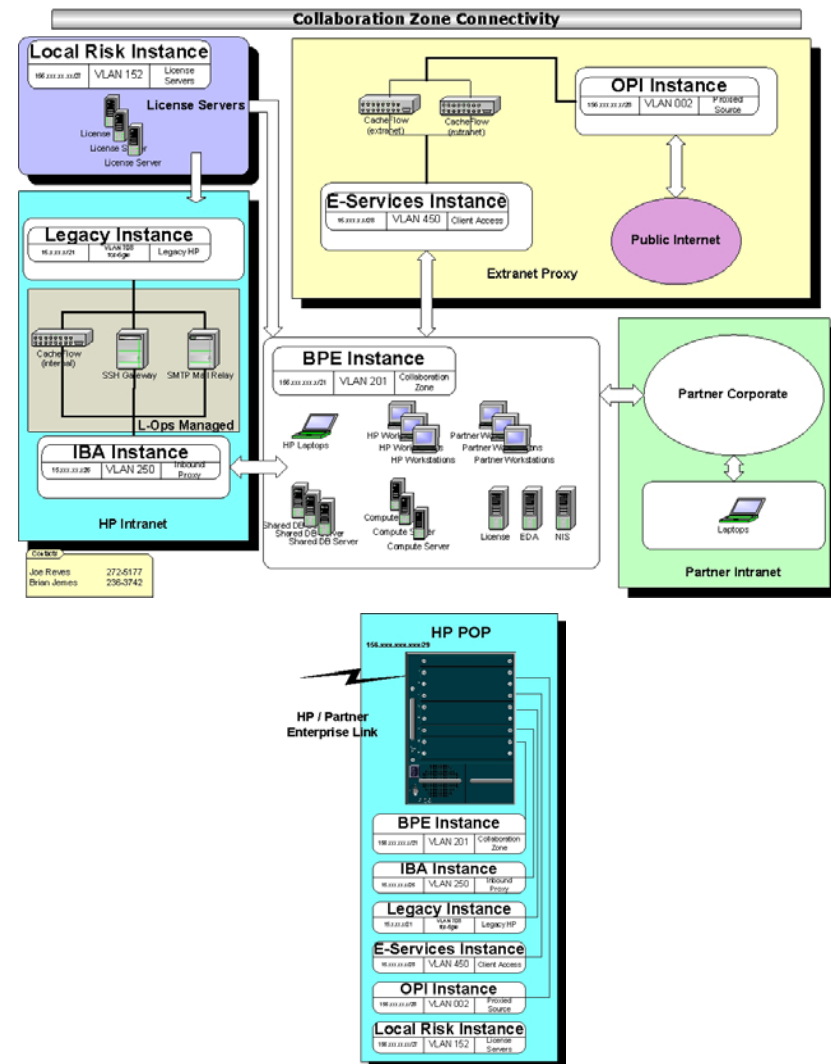
Conventional ROI calculations

- Conventional solutions are custom engineered, “pay-as-you-go”
- We’re accustomed to calculating ROI in the face of clear, static requirements
- Our businesses are accustomed to justifying additional IT infrastructure on an as-needed basis
- Financial approval cycles, purchasing, receiving, etc. often take longer than actual engineering efforts



ROI in a virtualized infrastructure

- From a pure equipment and resources perspective, it's easy to demonstrate that using a "slice" of a virtual infrastructure costs less to install and maintain
- More difficult to quantify – but nonetheless tangible benefits include time to implement, standardization to engineer and support, and lower risk of failure
- The real issue is not for any individual solution, but justifying the virtual infrastructure investment up front – without knowing precisely how it will be employed over it's service life



Measuring the value of Agility

“Every business decision triggers an IT event.”

Bob Napier(1946-2003)
HP Executive VP, CIO

- What is the rate of business-driven change you experience in your infrastructure?
- What are the magnitudes of changes you have experienced?
- What does a typical change project cost to execute, and what is the incremental cost to support the environment?
- For your businesses, what's the tangible value of executing an order of magnitude more rapidly?
- What's the value of planning for IT investment strategically, rather than tactically?
- What's the value of running on a standard, modular solution rather than a custom solution?
- What is reducing the risks in execution worth, for an IT infrastructure project?

Questions



i n v e n t