



# *Enterprise IT Architectures*

## Security

## **Hints for Architecture Work (some more words)**

## IT Architect – There are Various Approaches

- **Architecture Document**
  - Like Proposal (as done for term paper)
  - Position paper
  
- **Workshop, e.g. “Assessment”**
  - Concentrating on AS-IS, TO-BE, and Roadmap
  - Interactive work with stakeholders
  - Final Presentation (or short document) as a result
  
- **Architecture Management, embedded in organization**
  - Committees
  - Policies, Processes

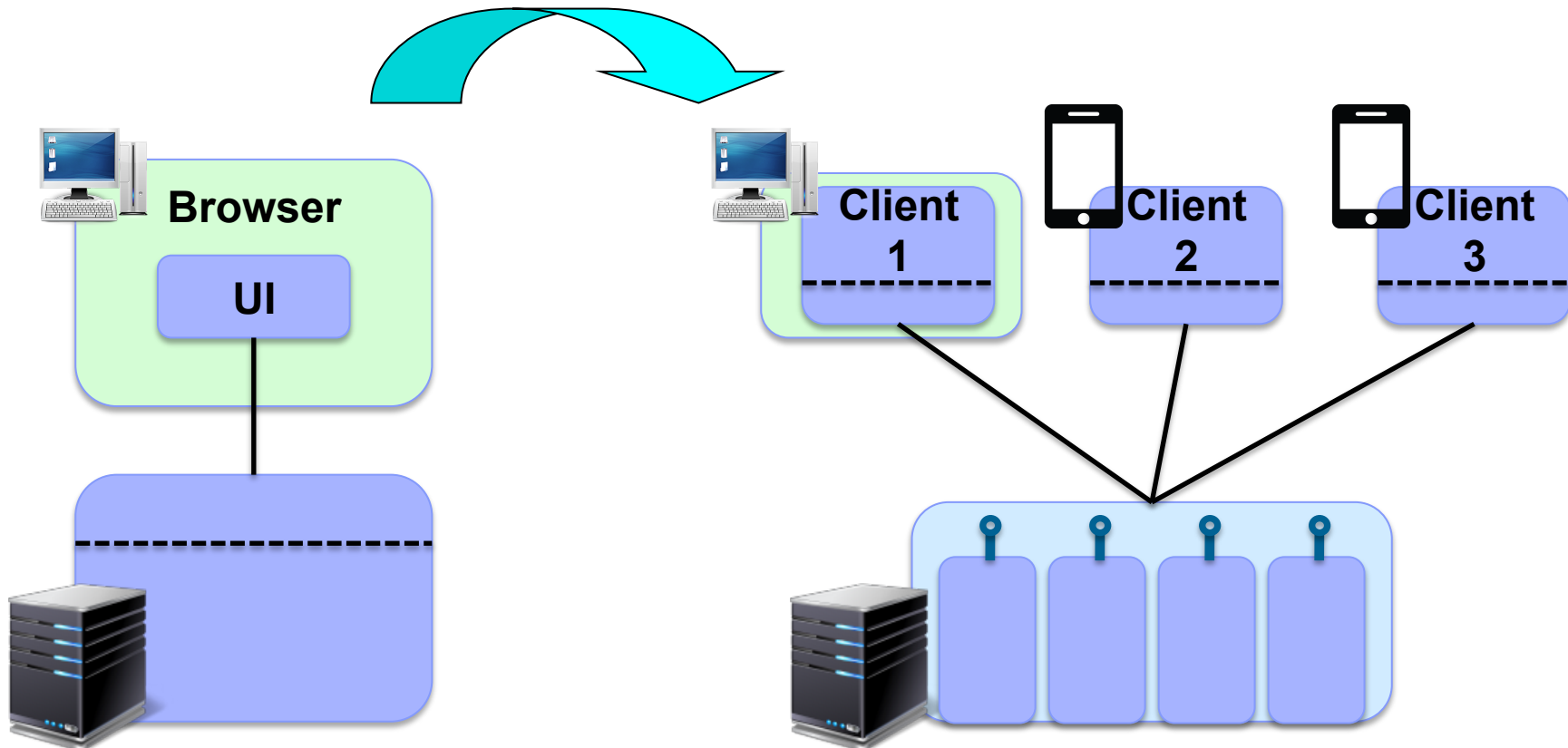
## IT Architect – “Assessment” in more Detail

- **Goals etc.**
  - **Provided by stakeholders**
  - **Driven by business**
  
- **AS-IS (or Baseline according to TOGAF)**
  - **Status of application landscape**
  
- **TO-BE (or Target according to TOGAF)**
  - **Coverage of business goals and requirements**
  
- **Roadmap**
  - **Closes the gaps**
  - **Timeline within months**

## Example for AS-IS and TO-BE

- **AS-IS: UI on Browser, all Business Logic in Server Application**

- **TO-BE: New Frontend on multiple Devices. Business Logic in Services**



# Questions



## **Security – Terminology and Architecture**

## Security is a critical concern in IT Architecture

- **Wherever systems are responsible for important data and processing, there is a risk that misuse of the system leads to a negative outcome for those associated in any way with that system**
  - **Typically in a commercial setting, IT Architects need to think about protecting our customers (e.g. a bank)**
  - **... and their customers (e.g. an account holder)**
  - **(... and both our reputations!)**
- **The scale of the risk depends on the nature of the organization(s) and the nature of the purpose of the system ...**



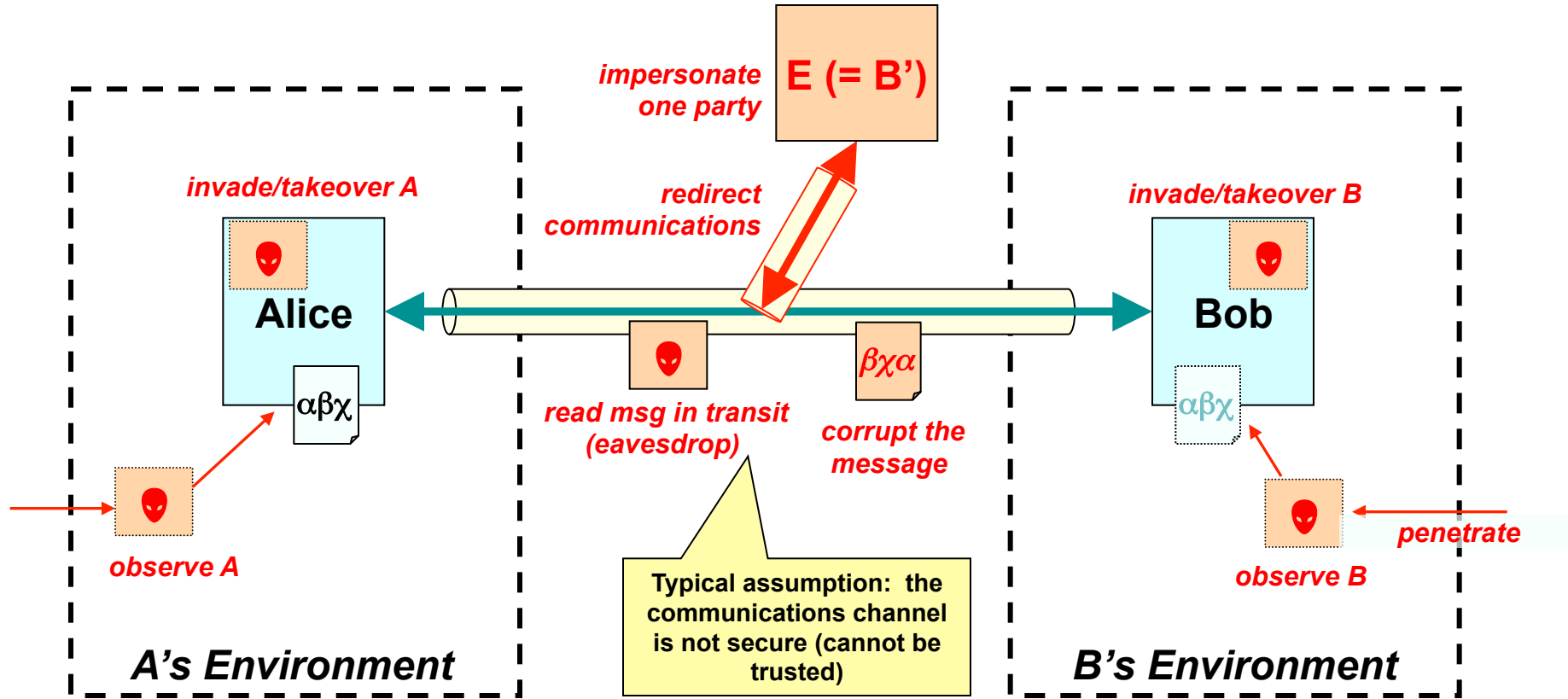
## Security & Safety

- **Security is a wide and fascinating topic encompassing a vast range of issues, arenas and disciplines**
  - from deep mathematics to international espionage
- **In IT systems, “security” can be associated with the following qualities:**
  - Not open to intentional misuse
  - Not open to accidental misuse
  - Protects the truth – maintains integrity
  - Protects service in the face of attack (overlap with Availability)
- **Secure means SAFE:**
  - Your data, your assets, your reputation

## Broad scope of a “Security Governance, Risk Management, and Compliance”

- **People and Identity (e.g. Authentication, Access Control)**
- **Data and Information (e.g. Cryptography, Data Loss Protection)**
- **Application and Processes (e.g. Security of Services)**
- **Network, Server, and Endpoints (e.g. Virtualization, Threat Protection, Malicious Traffic Detection, “Circle of Trust”)**
- **Physical Infrastructure (e.g. Operational Management)**

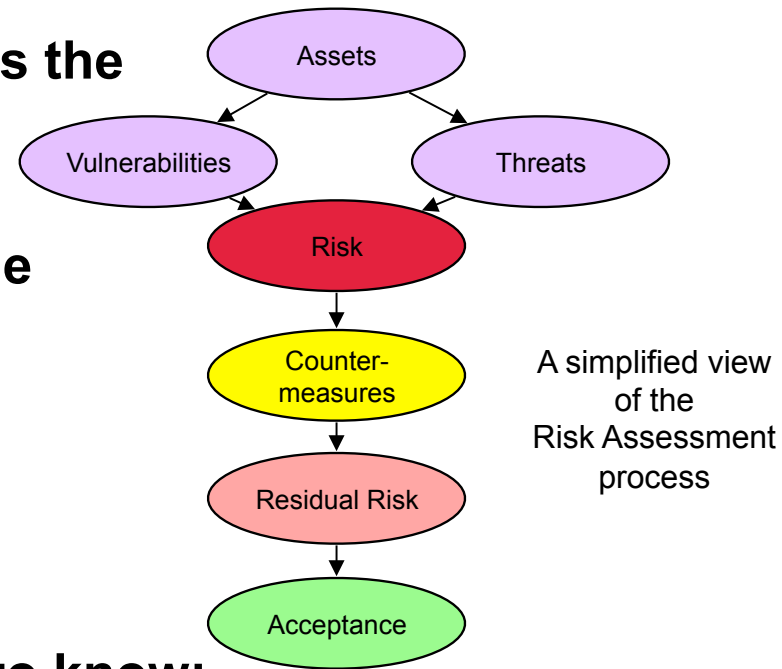
Consider: Alice wants to send a message to Bob (securely)



=> Threats arise at both ends and everywhere in between

# Threat assessment needs to be combined with assessment of vulnerabilities to determine risk

- Information security **risk** can be viewed as the **cost** to an organization of **compromise or damage** to an information asset
- There are many ways to assess risk, some formal and **quantitative**, some informal and **qualitative**.
- In all cases, the purpose is to identify significant **threats** and address them through appropriate **countermeasures**
- In general, to assess risk it is necessary to know:
  - **Threats** – the bad things that might happen to an information asset
  - **Vulnerabilities** – the ways those bad things might come to pass
  - **Likelihood** – the probability of a vulnerability being exploited to make a bad thing happen
  - The “**value**” or “**sensitivity**” of the asset – the impact on the organization if a bad thing happened



## A good general approach to tackling IT security is to take a “threat-based” approach

- ***Document assets:***  
Identify and decide what you need to protect. This could be data, intellectual capital, processes, physical resources, or any other thing of value in the organization
- ***Understand threats:***  
Know your enemy. Determine from whom or what are you protecting your system and/or network
- ***Define policy:***  
Create a comprehensive security policy and implementation plan which is appropriate to the level of threat
- ***Implement policies:***  
Apply the security policies to your organization and systems. Update or include security elements and configurations in IT solutions
- ***Monitor policy:***  
Continually monitor to detect any deviation from your policies and take actions if needed

## Security is an example of run-time quality and covers these topics

### ▪ Safety

- To reduce or eliminate danger
- To reduce or eliminate anxiety
- To reduce or eliminate risk or liability

### ▪ Protection

- To defend against attacks (insider and outsider)
- To defend against fraud (misuse of assets or identity)
- To defend tangible assets (IT systems and applications or stored information or information in transit)
- To defend intangible assets (reputation)

### ▪ Assurance

- To ensure correct and reliable operation
- To enforce identity and ownership
- To promote trust

## Key Objectives of Security Engineering (1)

- **Authentication** – knowing who
  - The process of determining who users (human or otherwise) are and that they are who they claim to be. The most common technique for authenticating is by user ID and password. Others include certificate-based methods or biometrics
- **Authorization** – knowing what can they do
  - The process of establishing the ‘rights’ that a user has to access and to perform actions on resources. (Simple example – the permissions to read and/or write a file)
- **Confidentiality** – protecting confidential data
  - Ensuring that data classed as confidential is only seen by appropriately authorized parties. Often achieved through cryptography – i.e. encrypting data

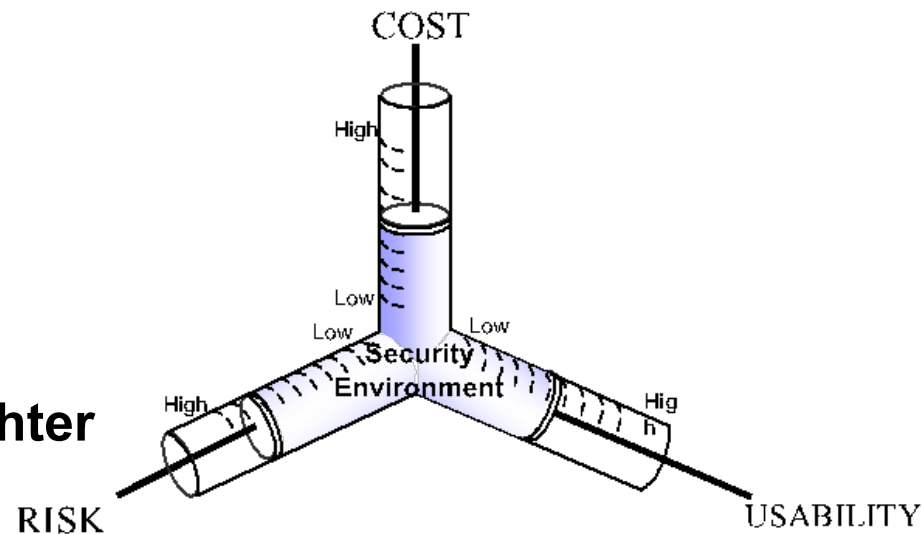
## Key Objectives of Security Engineering (2)

- ***Integrity*** – protecting the “truth”
  - The quality of a system whereby data and processing always conforms to the specified rules and constraints within the system
- ***Auditable*** – what did they do?
  - The trail of evidence proving the activities that have been performed on an internal asset – and attributing this to a known identity. This must be stored in a non-repudiable (tamper proof) format.
- ***Non-Repudiation*** – proving what happened happened
  - The ability to prove without contradiction that a transaction or event which is recorded as having taking place did take place May need to be able to prove events in a court of law



# Security Architecture is about answering the question “how much security is enough security”

- From a security perspective, all IT solutions must balance three conflicting factors:
  - **The *risk*** – to the organization of operating the IT solution
  - **The *cost*** – of implementing and operating the security controls in general, the tighter the controls the lower the risk
  - **The *usability*** – of the solution in general, the tighter the controls, the greater the impact on the users of the system



The resulting set of controls must be, as far as possible “**necessary** and **sufficient**”.

# Security Services – Standards

Service	Relevant Standards
Identity Services	IdAS, SPML, SAML, WS-Federation
Authentication Service	WS-Trust, Kerberos, SAML, PKI
Authorization and Privacy Services	XACML, JACC, WS-Authorization, WS-Privacy, WS-Policy, IDEMIX
Audit Service	CBE extensions, Audit web service (in progress), WS-BaseNotification
Message Protection	WS-Security, WS-SecureConversation, PKI, XKMS, WS-SecurityPolicy, SSL/TLS, JSSE/JCE

# Questions



## **Security – Basic Infrastructure**

## Security – Basic Infrastructure

- **Providing Functionality**
  - **Authentication & Authorization**
  - **Encryption**
  - **Identity Management**
- **Integration with Applications and other Functions**
  - **Integration with various Access Management Functions**
  - **Diverse Authentication Mechanisms (in the Backend)**

## People and Identity: Today's *Identity and Access* Challenges

### Trusting Identities



Customers  
or criminals?

Partners or  
competitors?

Employees  
or hackers?

### Managing Access



### Securing Services

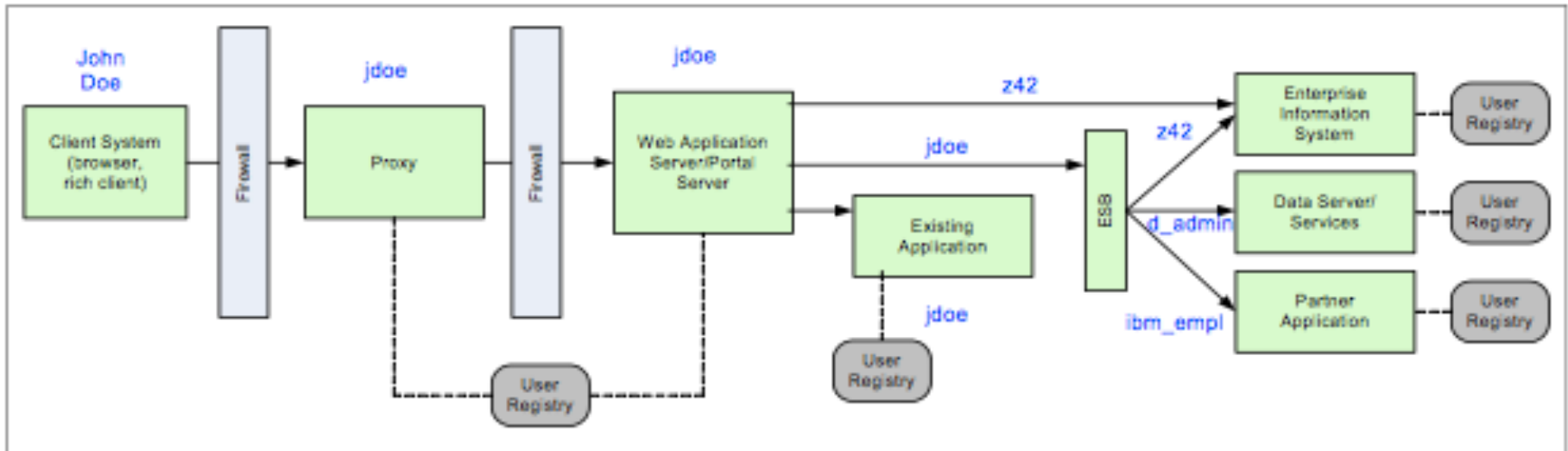
Payroll  
Online banking  
Loan applications  
Retail sales  
Inventory

### Protecting Data and Privacy



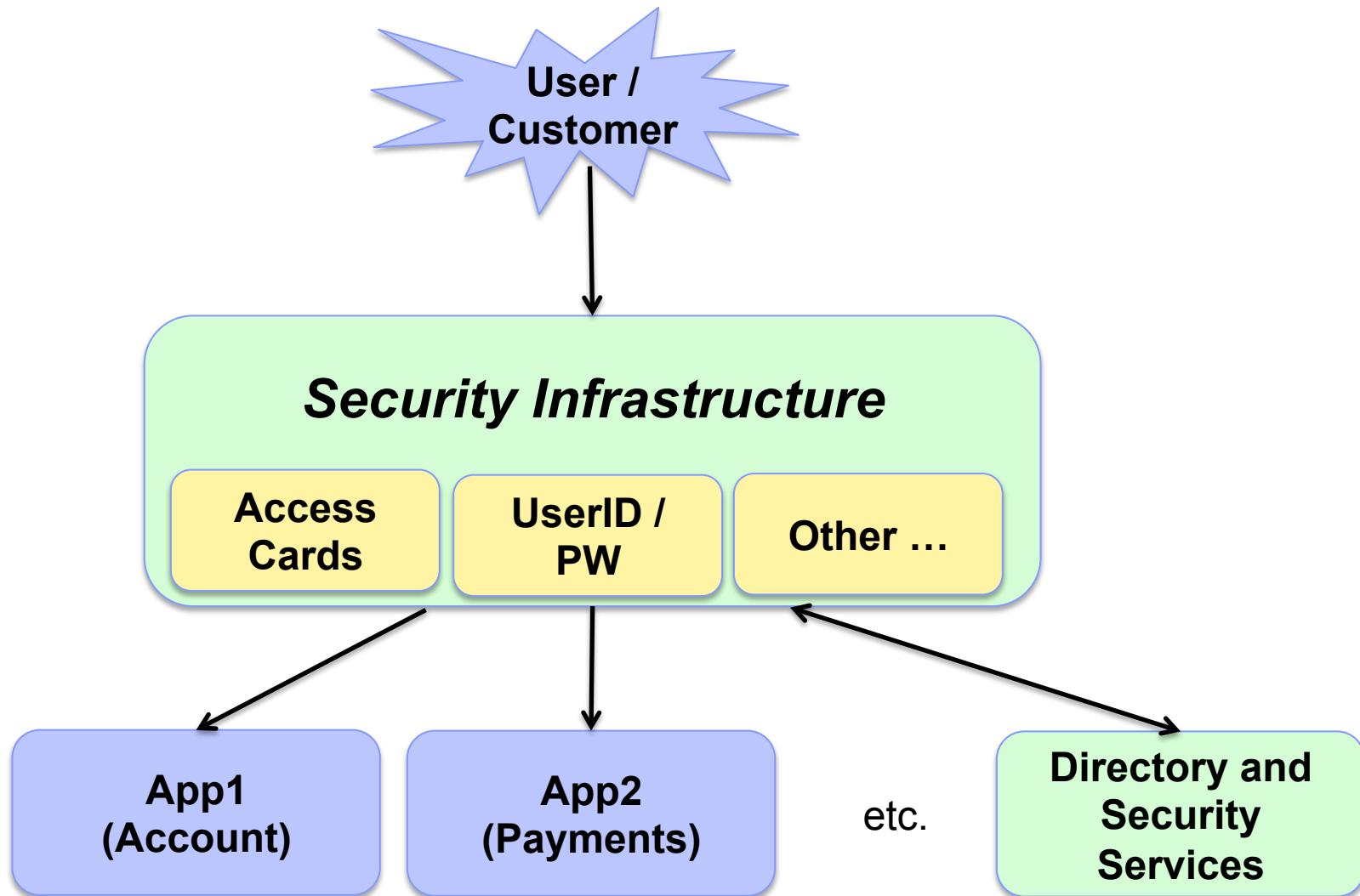
**Security has to be applied within a Business context and fused into the fabric of business and not as a widget to solve the next security threat**

## Identity and Access: Various “Identities” for one person



- John Doe with multiple “identities” and roles
- Applications with multiple user registries
- Challenges: Transferring identities, aligning registries, areas of trust
- Reference:  
<http://www.redbooks.ibm.com/abstracts/sg247310.html?Open>

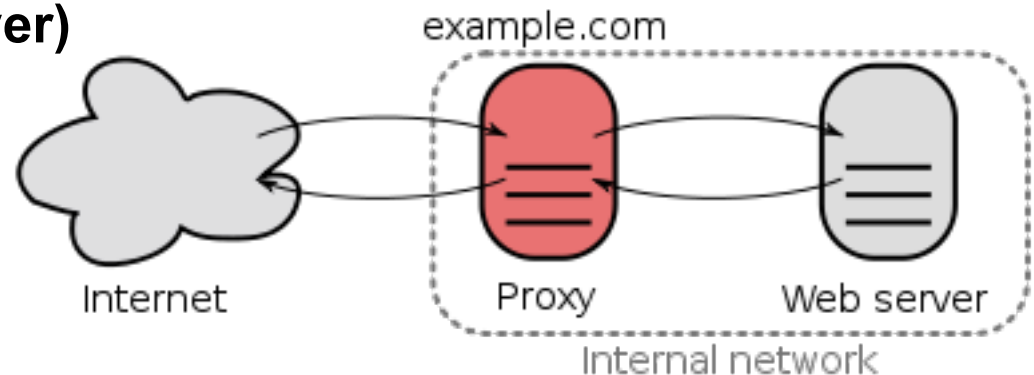
## General Structure of Security-Infrastructure





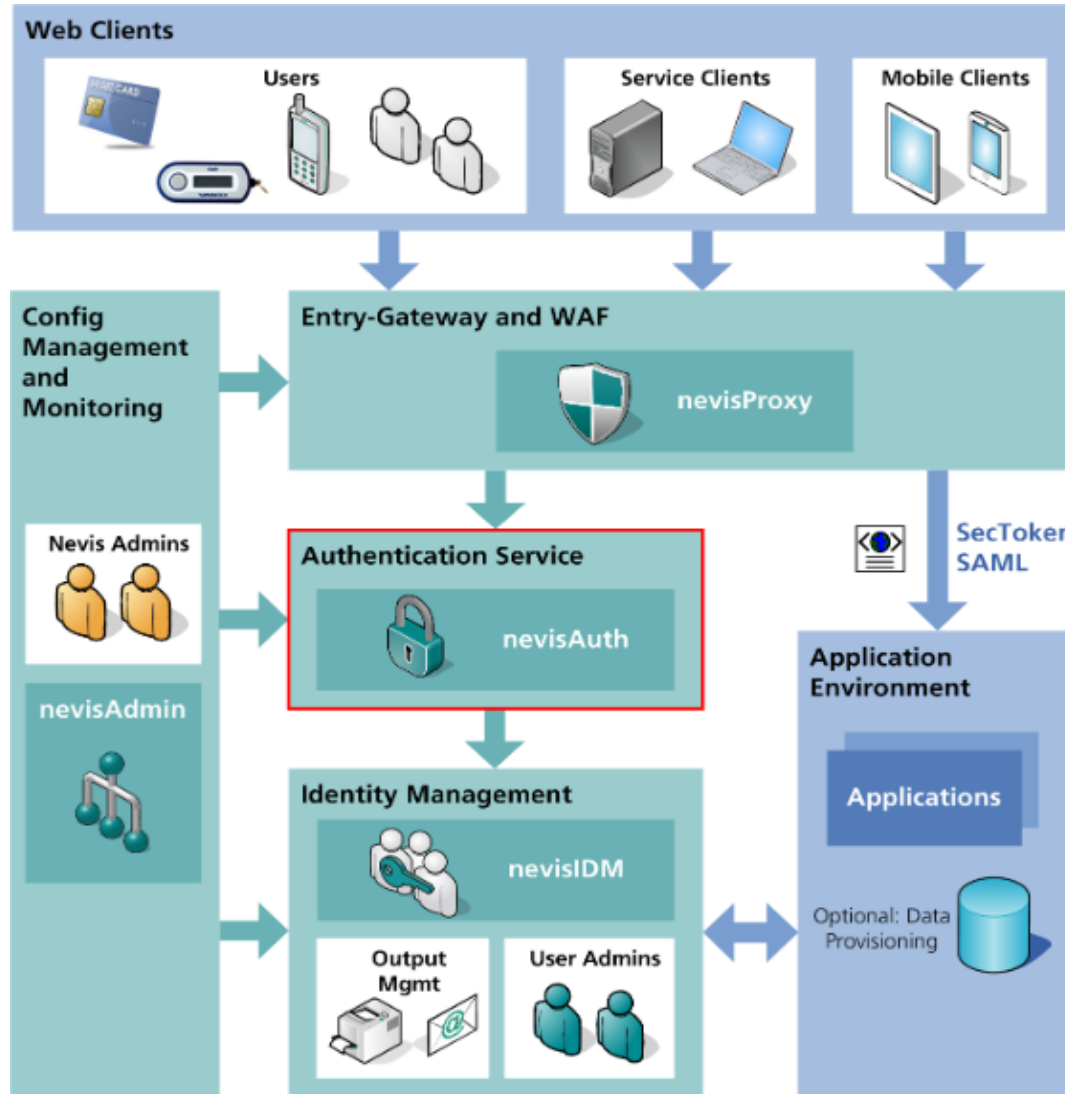
## Key Elements: Proxy & Firewall

- (Secure) Reverse Proxy *protects* and provides:
  - Session Handling (supporting SSO – Single Sign-on)
  - Authentication (using Security Services and Identity Management)
  - SSL (Secure Sockets Layer)



- Firewall (WAF – Web Application Firewall) provides:
  - Validation of Input and Protocol
  - Content Inspection
  - Filtering of Requests und Responses
  - Encryption

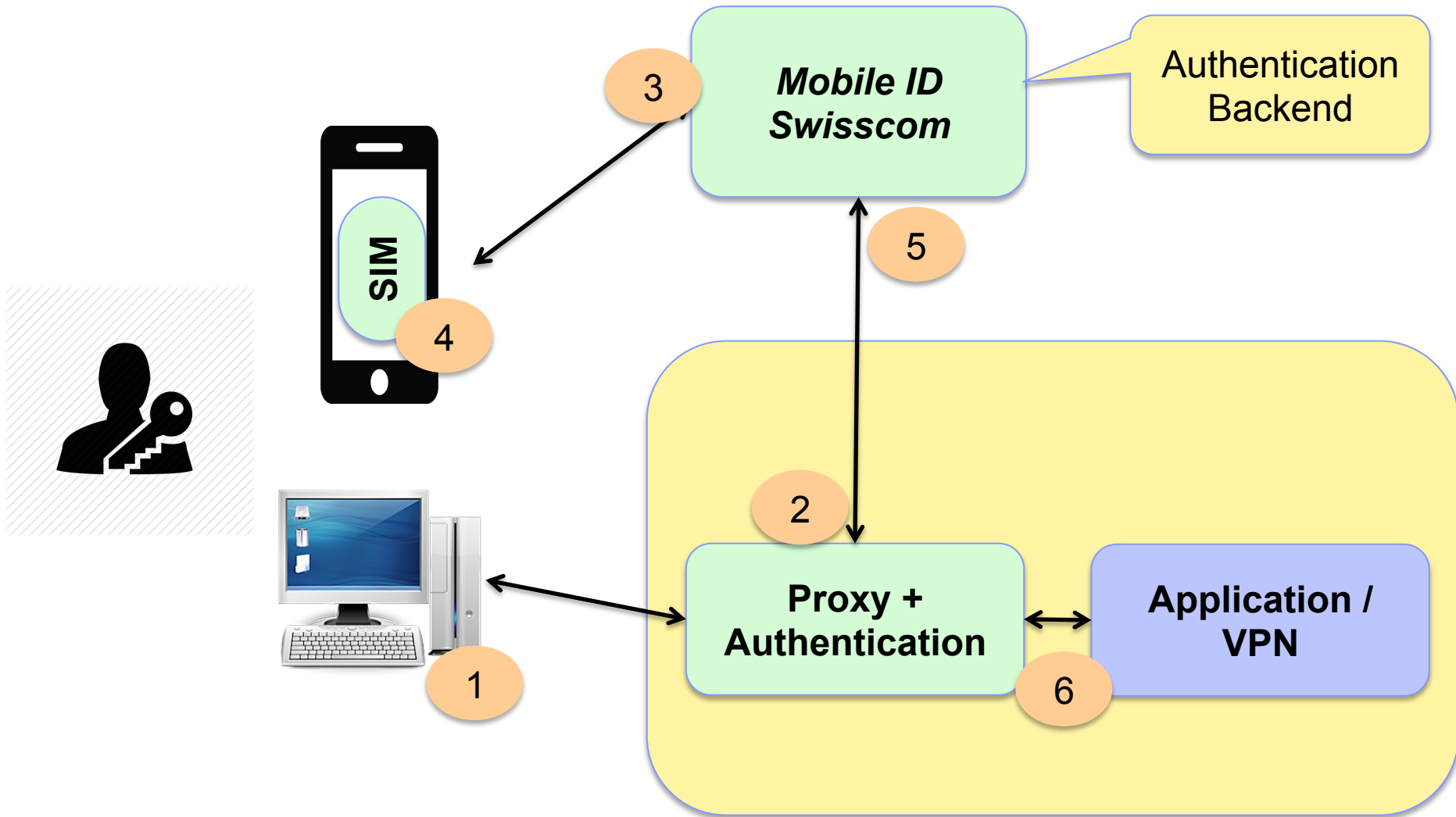
## Example of a Security-Infrastructure (AdNovum Nevis)



ADNOVUM

NEVIS

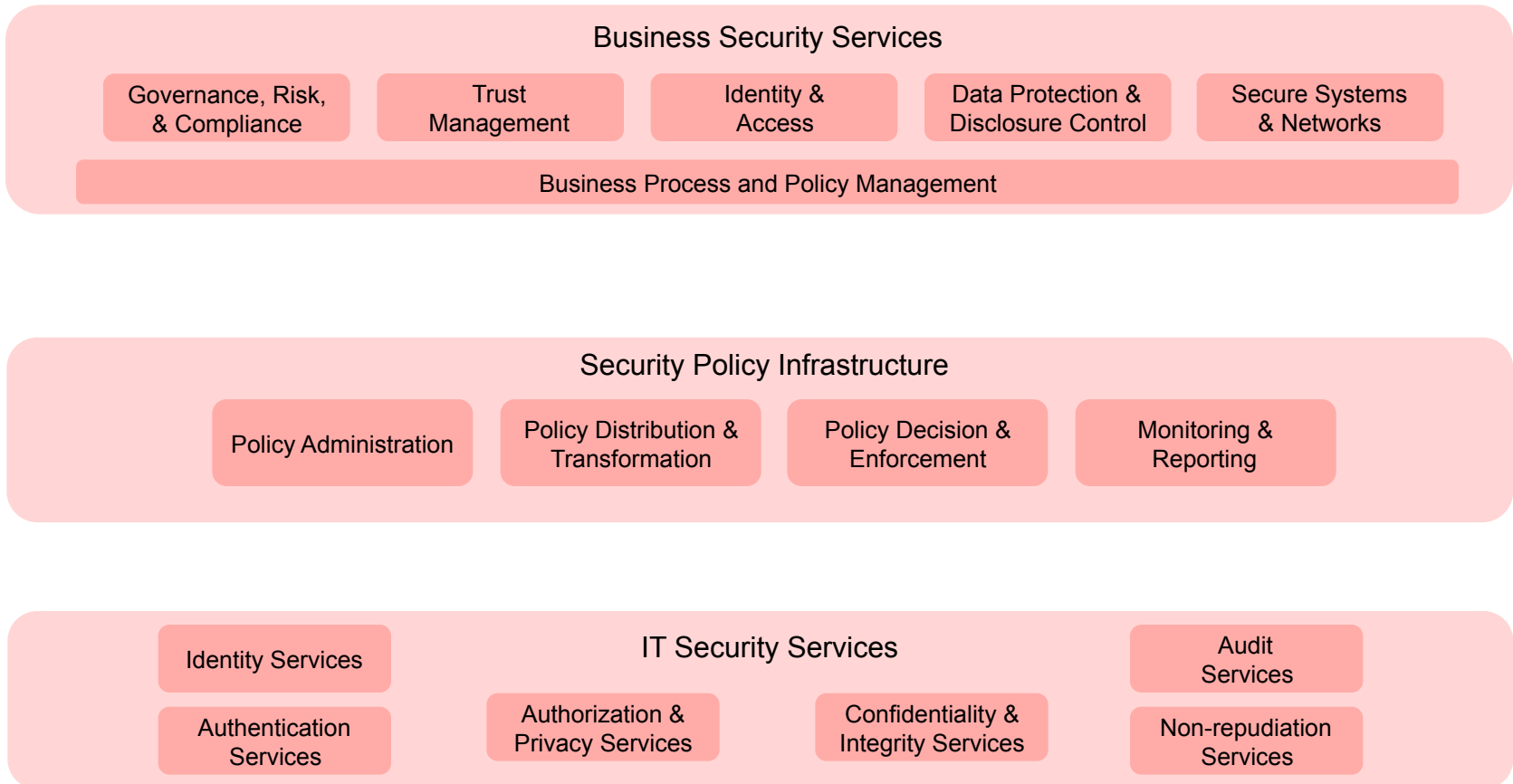
# Example: Mobile ID from Swisscom (with Security Application on SIM-Card)



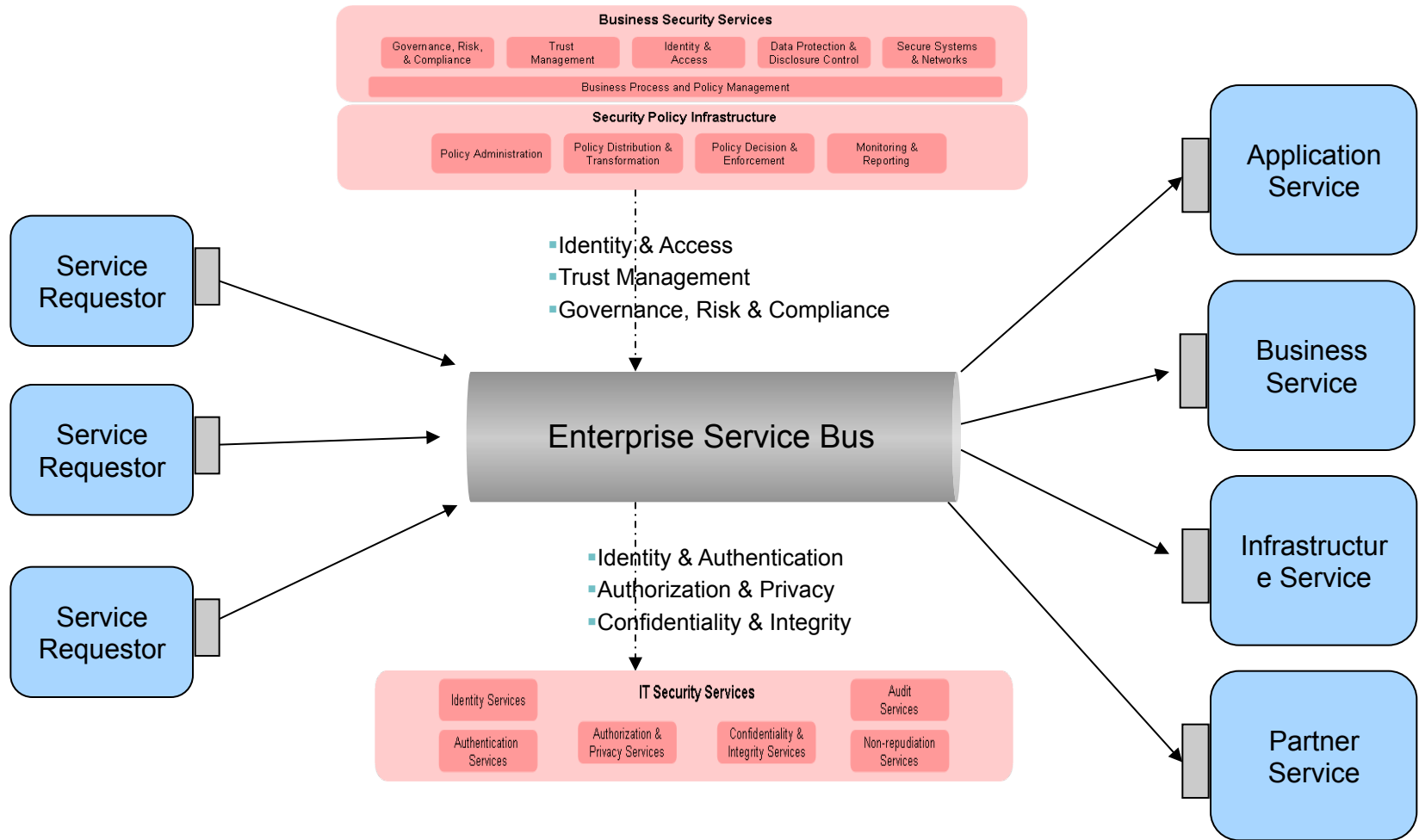
## Key Security Challenges of an SOA Environment

- **The need for user and service identities and propagation of these identities across the organization.**
- **The need to seamlessly connect to other organizations on a real-time, transactional basis.**
- **The need to ensure for composite applications that proper security controls are enacted for each service and when used in combination.**
- **The need to manage identity and security across a range of systems and services that are implemented in a diverse mix of new and old technologies.**
- **Protection of data in transit and at rest.**
- **The need for demonstrable compliance with a growing set of corporate, industry, and regulatory standards.**

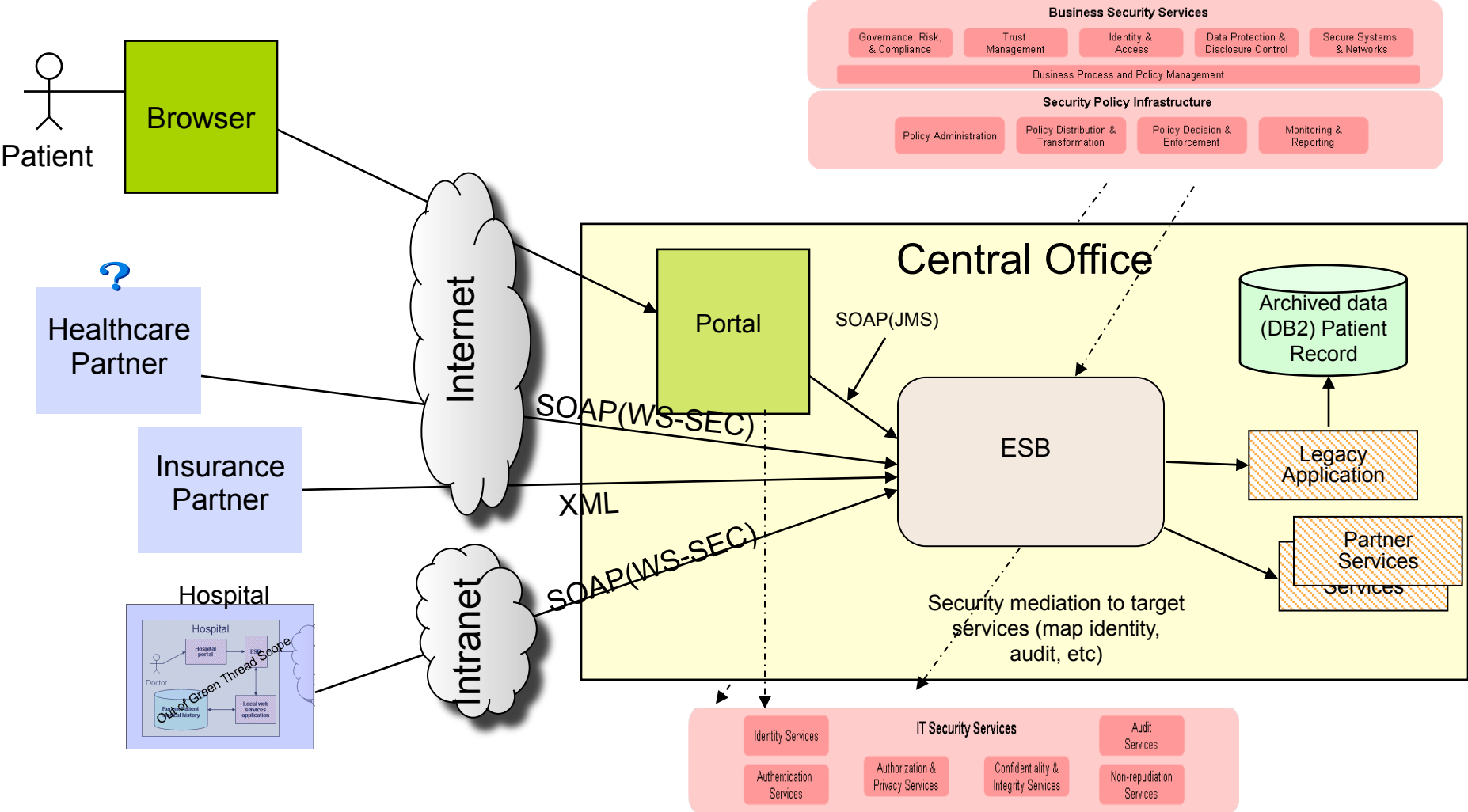
## Security Reference Model (for SOA by IBM)



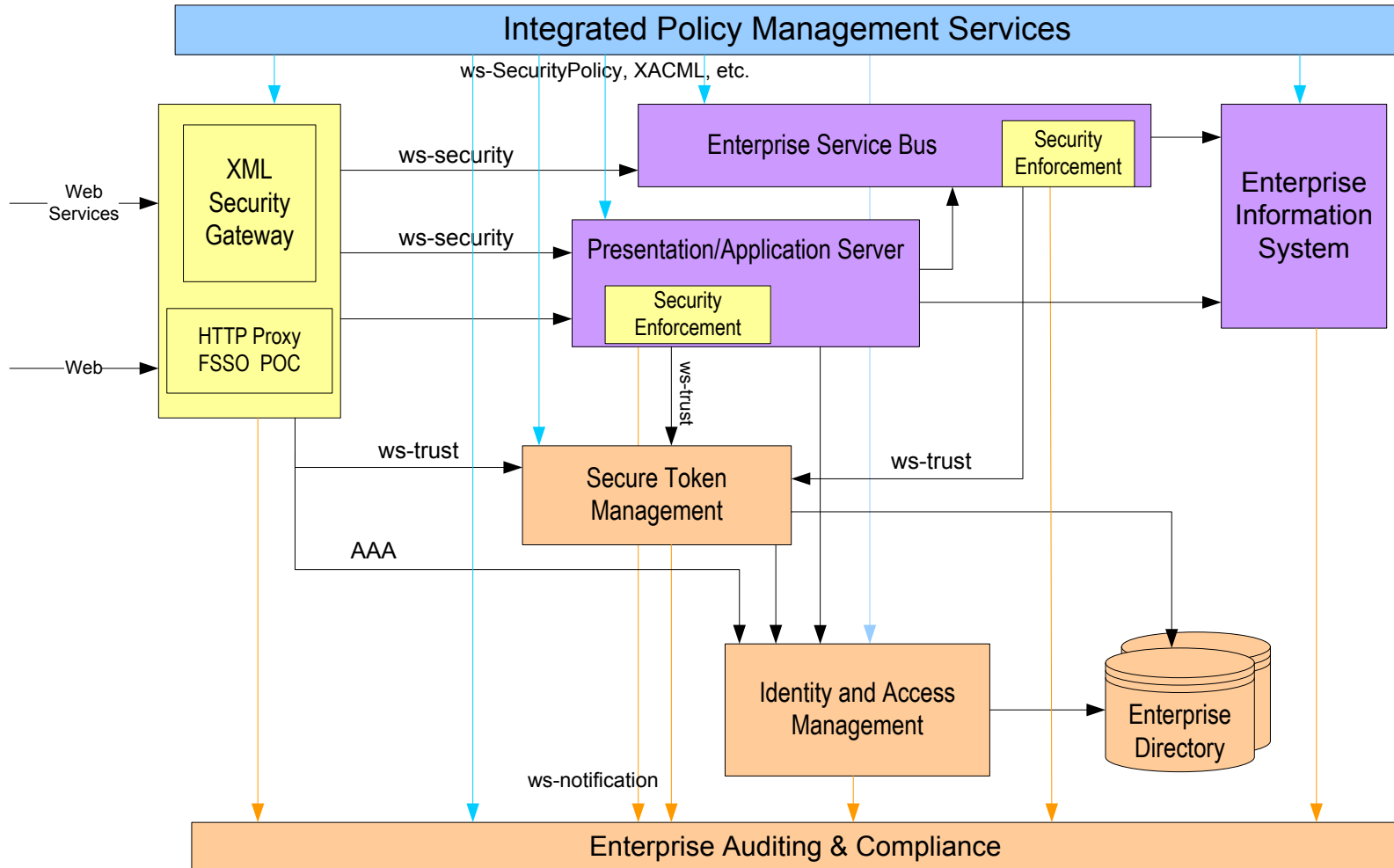
## Services Integration Scenario



# Service Integration Scenario with Security



## Logical Architecture for Service Integration Scenario



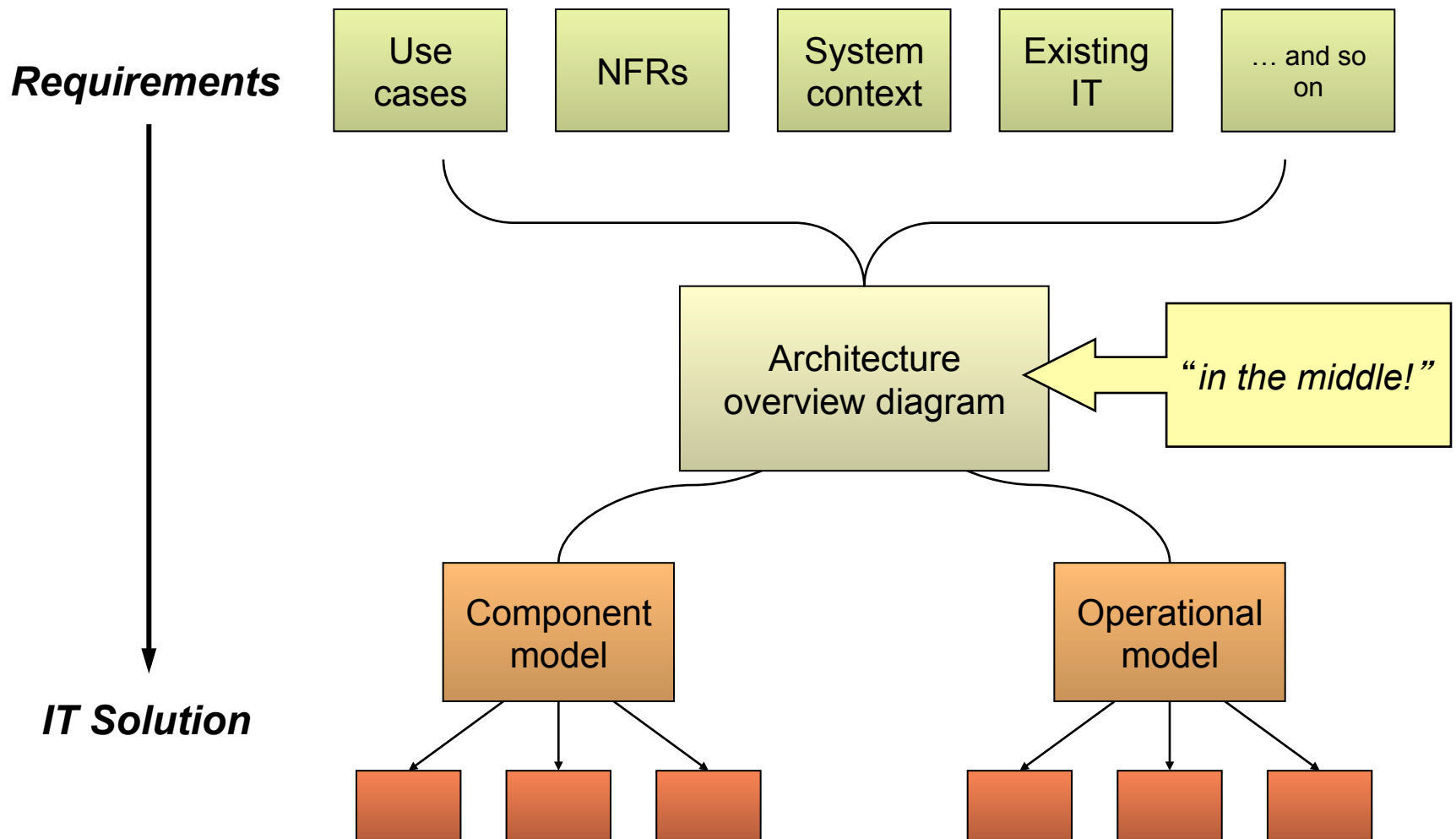


## **Security in Architecture Overview and Operational Model**

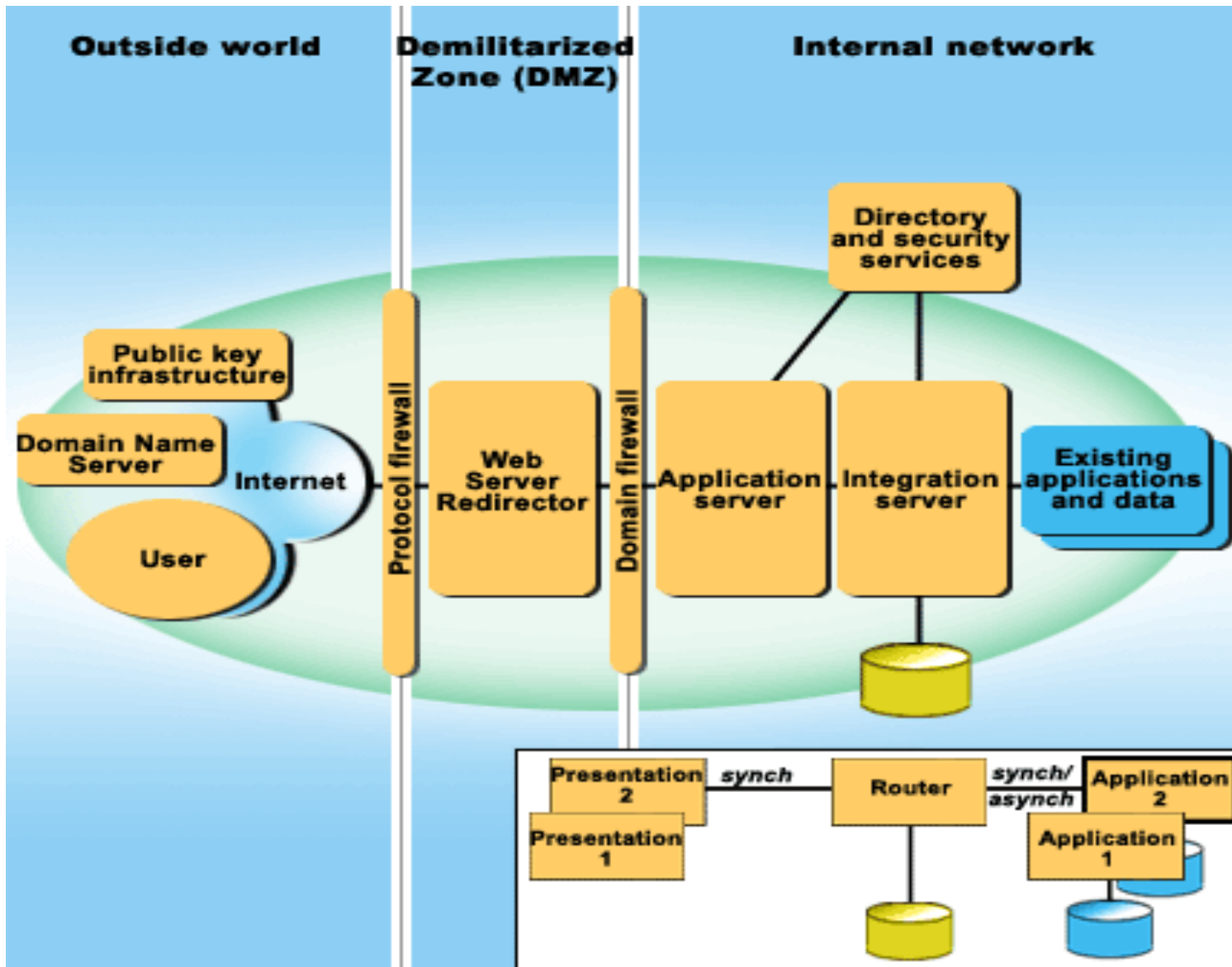
## Recap – Architecture Overview Diagram

- An Architecture Overview Diagram contains schematic diagrams that represent the governing ideas and building blocks of an IT system.
- An AOD can include both functional and operational concepts.
  - To **communicate** to the sponsor and external stakeholders a conceptual understanding of the intended IT system
  - To provide a **high-level shared vision** of the architecture and scope of the proposed IT system for the development teams
  - To explore and **evaluate alternative architectural options**
  - To enable early recognition and validation of the **implications of the architectural approach**
  - To facilitate **effective communication** between different communities of stakeholders and developers

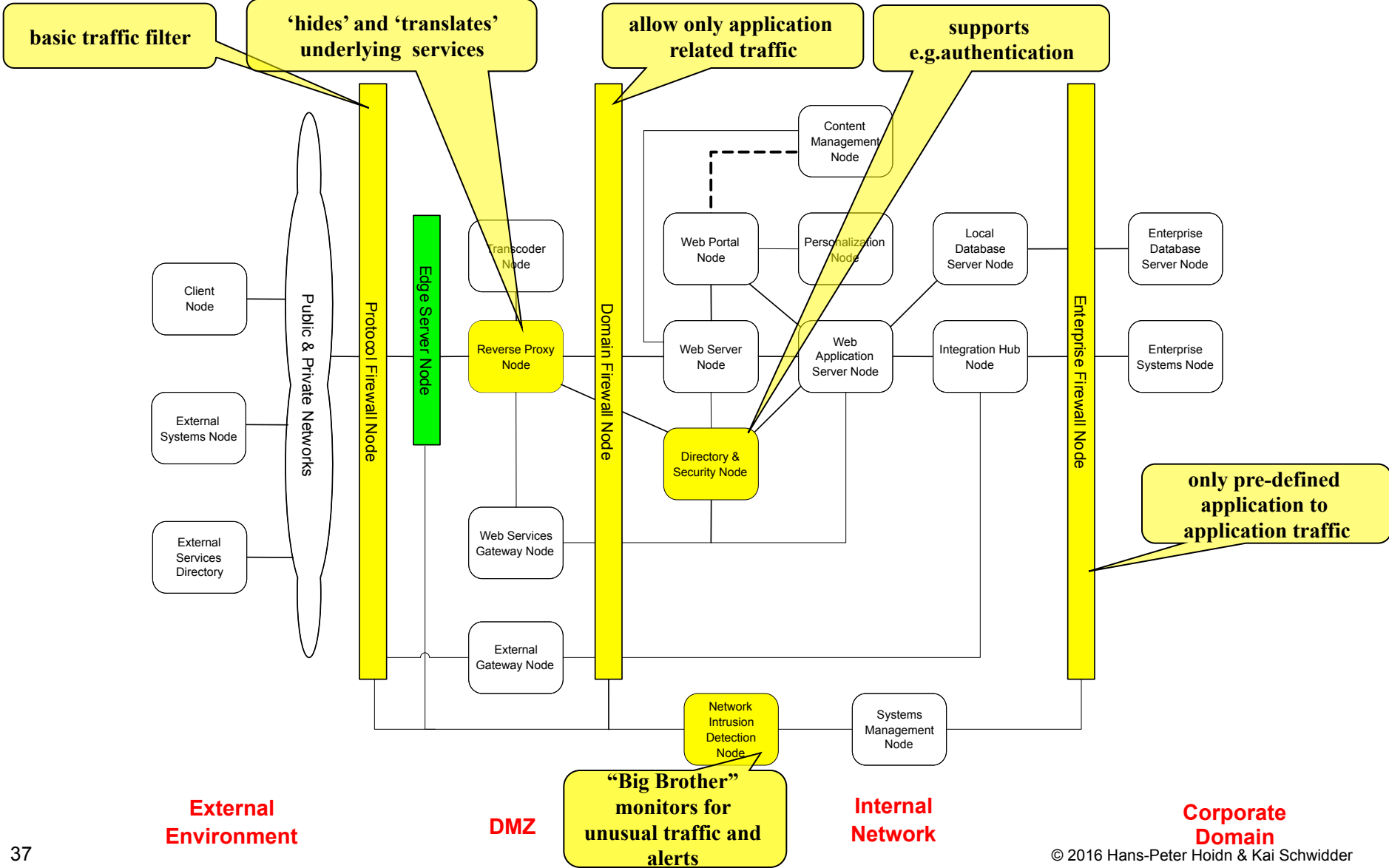
## Where does the Architecture Overview Diagram fit?



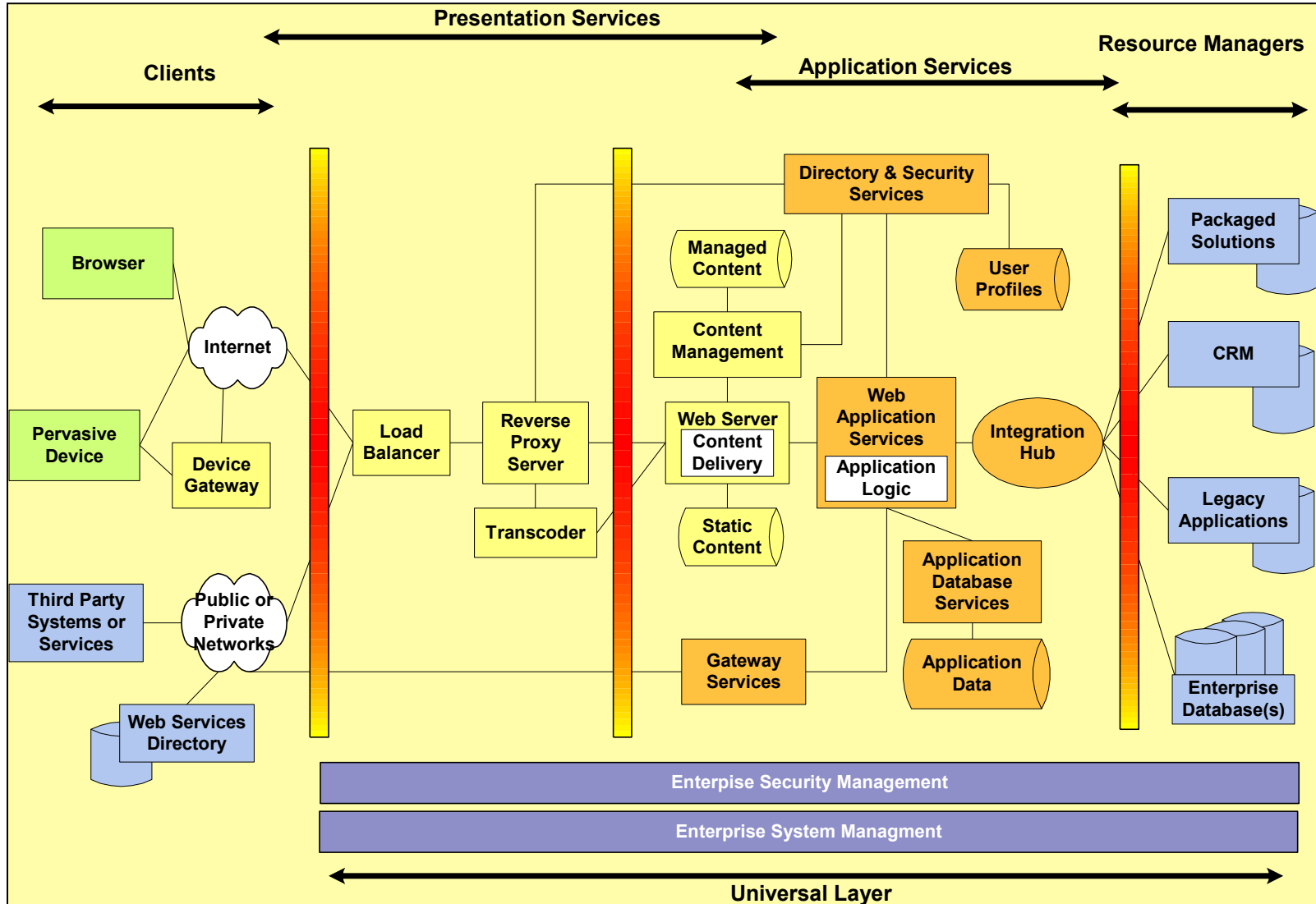
# Using Patterns – Example e-Business



# Security and access related Nodes in AOD



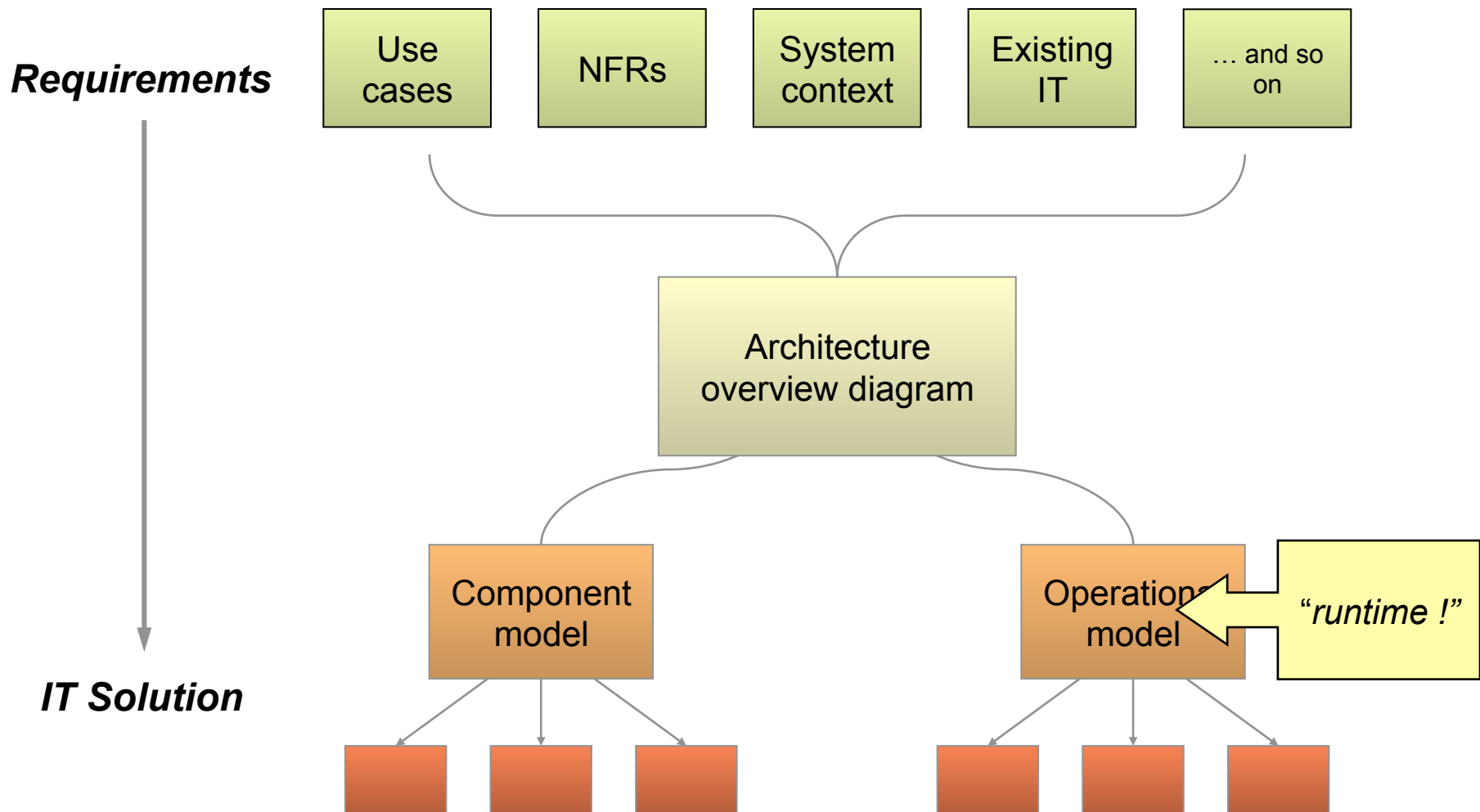
## Major Components in the AOD – Example e-Business



### Recap – Operational Model

- The ***Operational Model*** is the key work product created in analyzing the operational aspect of the architecture of an IT System.
- Represents how components (described in the component model) are ***deployed*** across the (geographical) structure of the IT System
- Describes how the Service Level Requirements (***SLRs***) are satisfied and how the system will be managed and operated
- Is usually documented as ***deployment units*** (DUs) placed on nodes in locations (static relationships), and their interactions across connections (dynamic behavior)

## Where does the Operational Model fit?





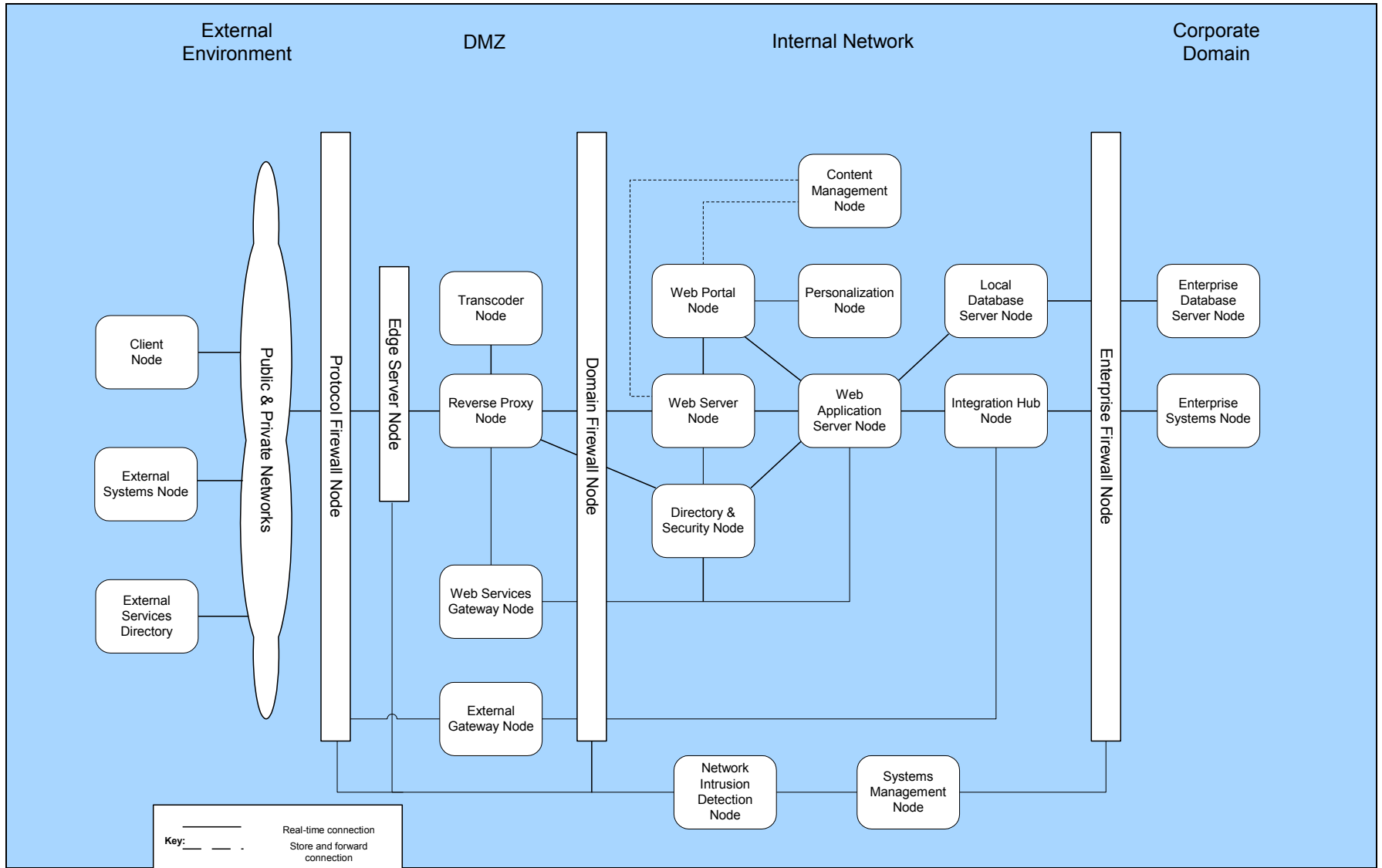
### Operational Model Purpose

- **The Operational Model can be thought of as the “infrastructure architecture”, documenting the design for:**
  - The overall geographic structure of the **locations** and **zones** over which the IT system will operate
  - The logical and physical **nodes** which represent the computers, network components and other devices which comprise the system’s infrastructure
  - The **placement** of both application and technical components across the system’s locations and nodes
  - The **connections** between nodes which are required to support the interactions of the components
- **At the lowest level (Physical level), the OM ultimately documents:**
  - The overall configuration of the technologies and products necessary to deliver the functional and non-functional requirements of the IT system
  - The hardware and software technologies and products which have been selected
  - Sizings and hardware specifications for all the computers, storage devices and networks
- **One of the primary concerns of the Operational Model is to ensure the solution **meets all the Non-functional Requirements!****

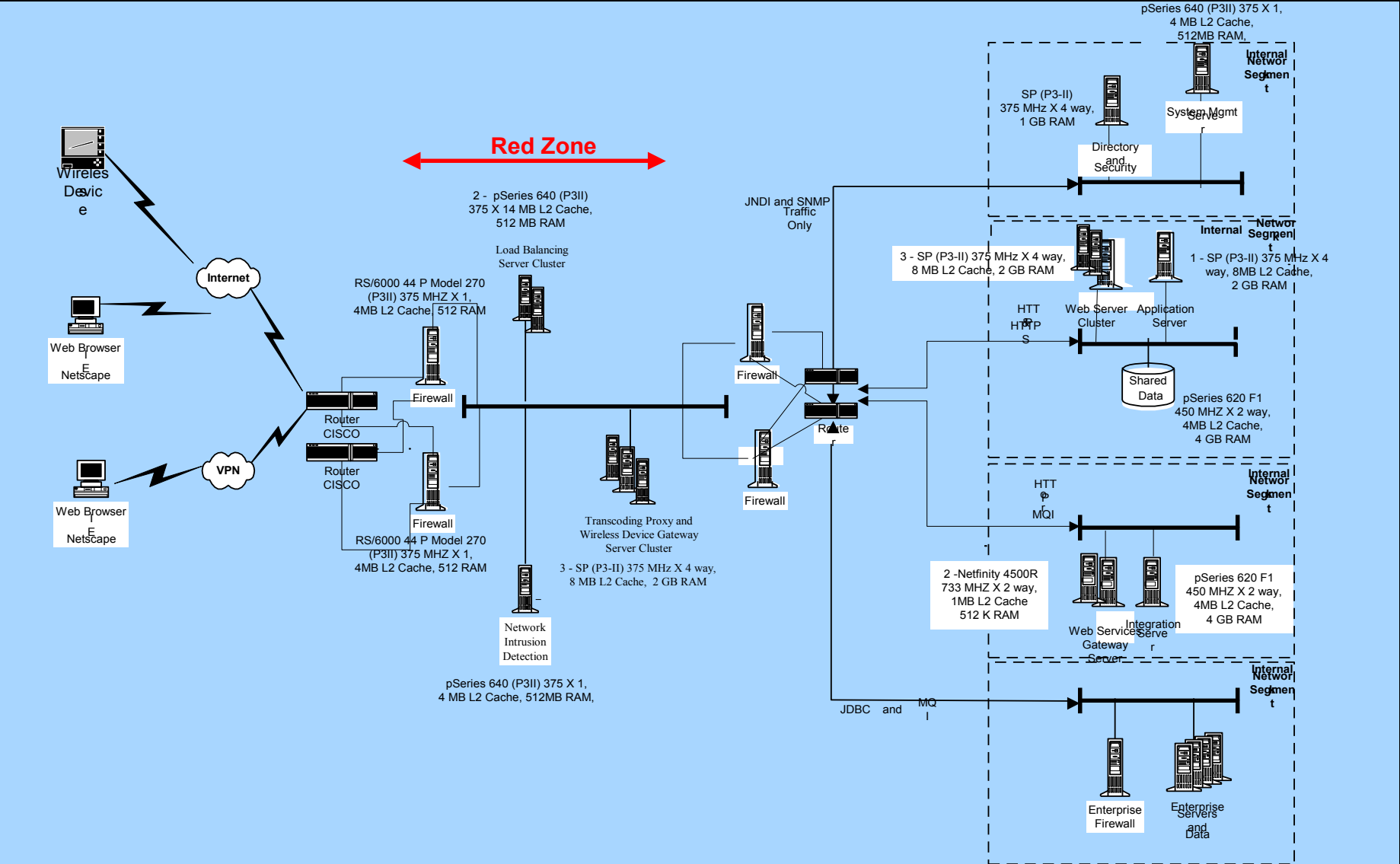
### Definitions

- **Node** - platform on which software executes
- **Location** - type of geographical area or position
- **Border** - separates adjacent locations
- **Zone** - an area for which a common set of non-functional requirements can be defined
- **Connection** - physical data path between nodes (LAN, WAN, dial-up etc)
- **Deployment Unit** - one or more components placed together on a node; execution, presentation, data and installation aspects may be separately placed.
- **Walkthrough** - description of the flow of a scenario starting from a user all the way through the system and back to the user

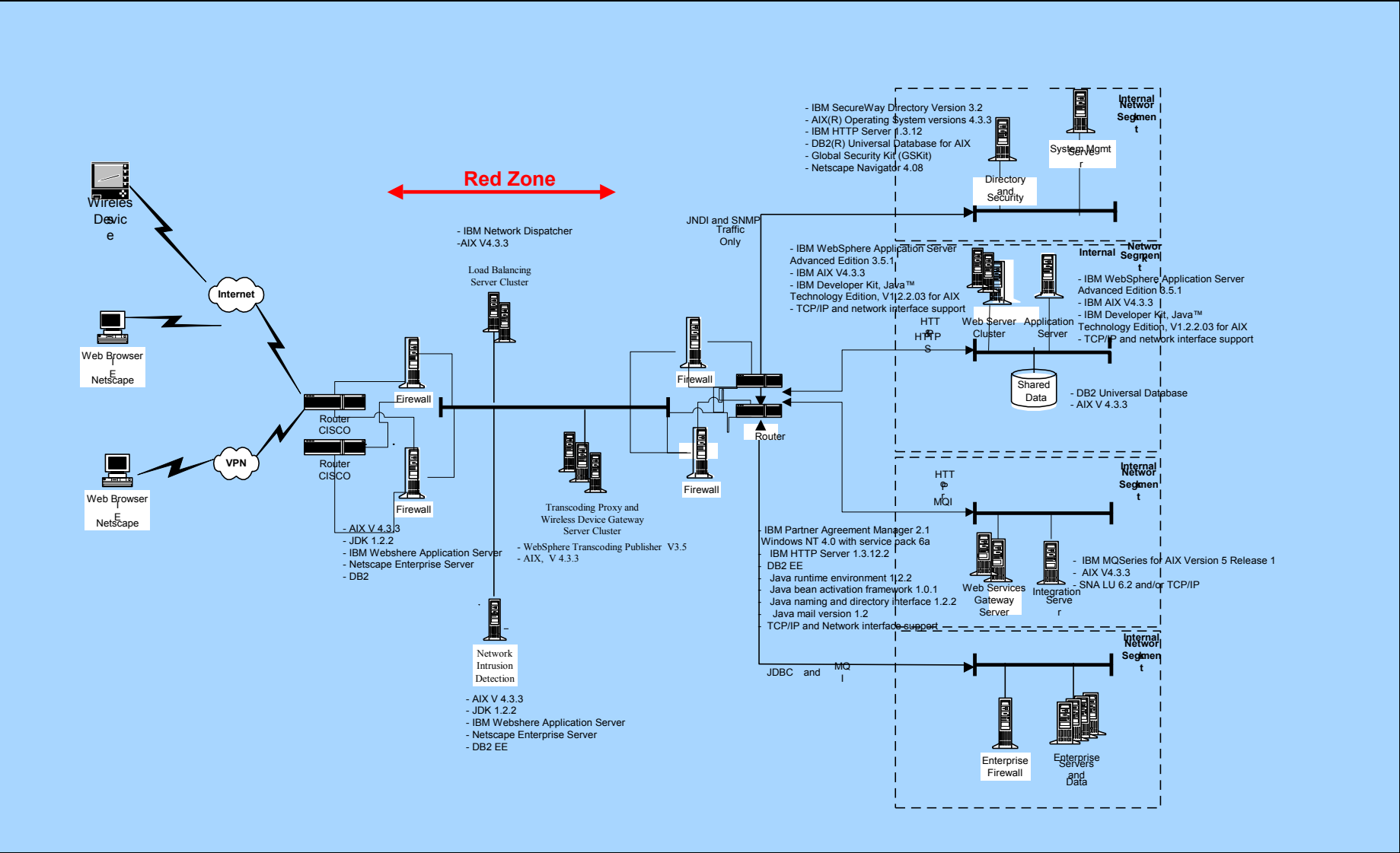
## Specification Level Operational Model



# Sample Physical Level Network View

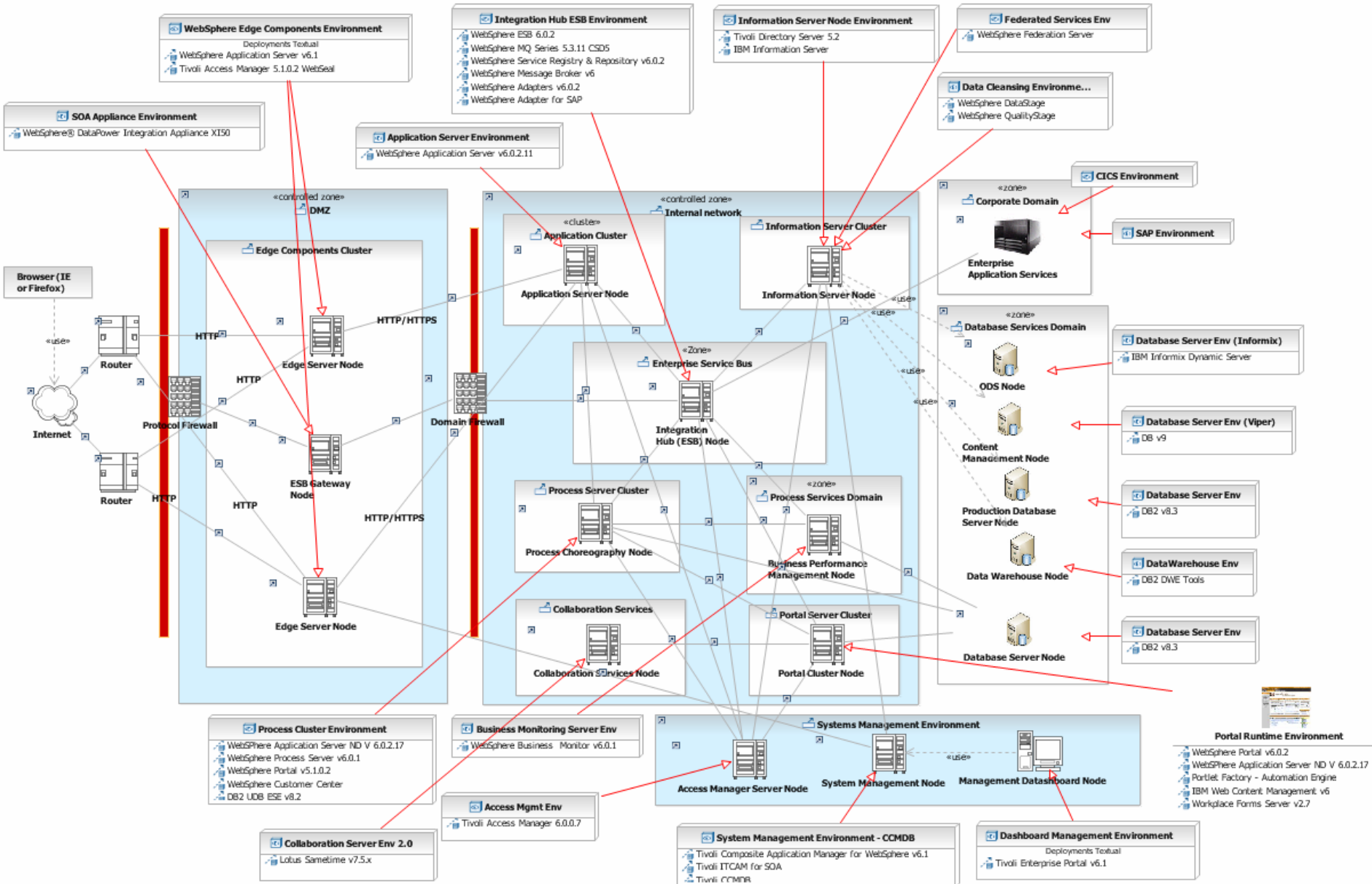


## Sample Physical Level Software View



# Enterprise IT Architectures

JKE - Operational Model - Software & Node View



# Questions

