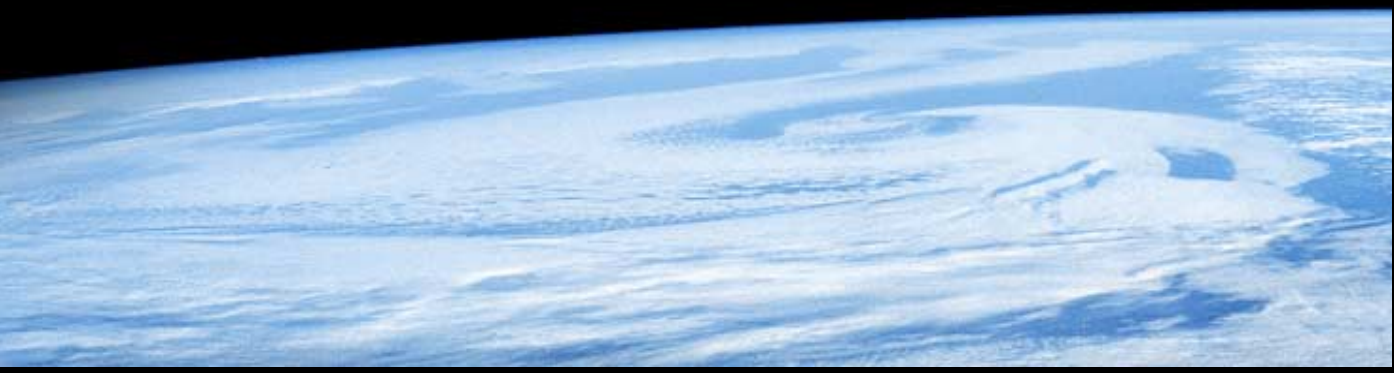
Sun microsystems

CMG DOCsec2002
March, 2002
Baltimore



Agenda

Overview (J2EE environment & Security)
J2EE and application level security techniques
J2EE and application infrastructure security techniques
Q & A

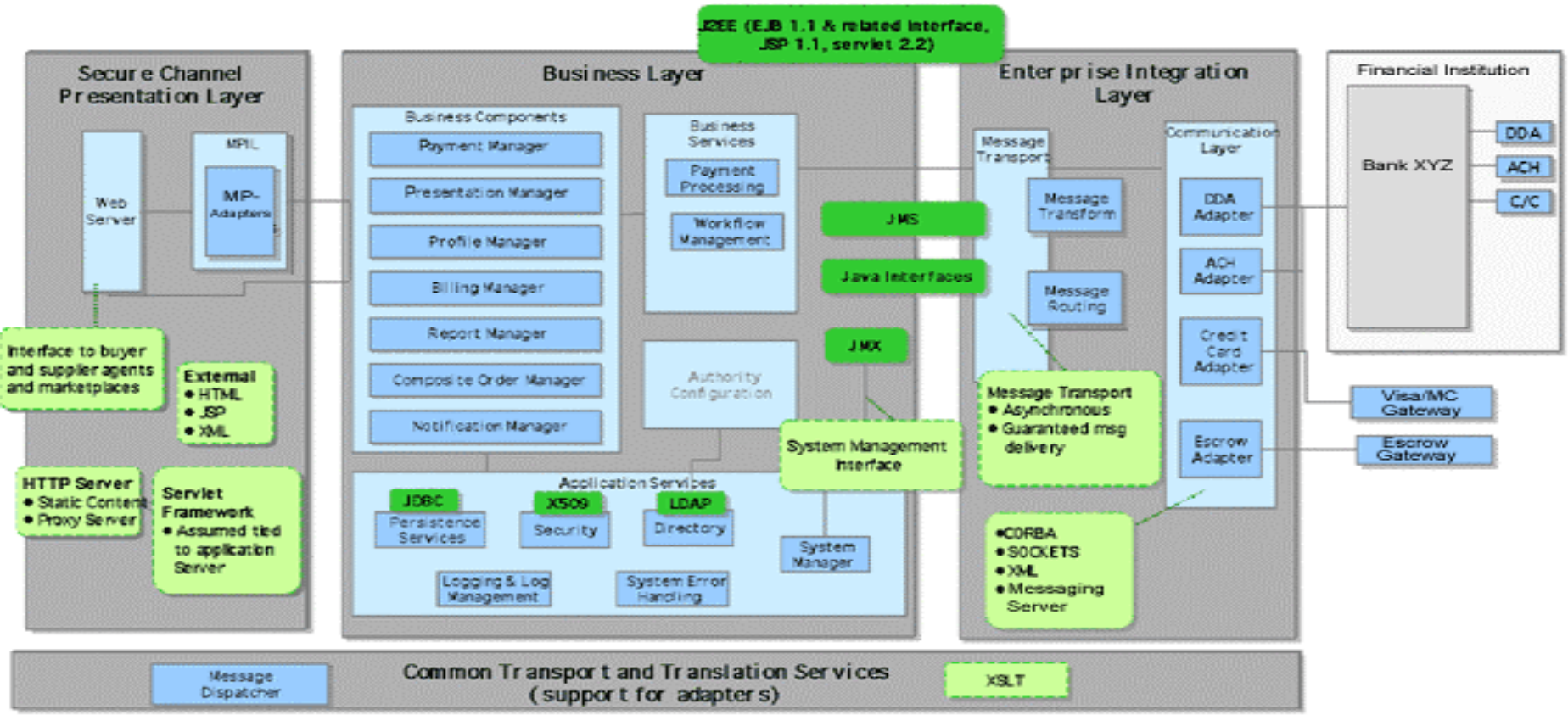
Overview (Common Techniques)

- J2EE as a Technology Platform (going beyond a simple OO programming language)
- Mostly Container Enforced Security Techniques
- JCE – Java Cryptography Extensions
- JSSE – Java Secure Socket Extensions
- JAAS – Java Authentication and Authorization Services
- JBCV – Java Byte Code Verifier
- JSM – Java Security Manager
- JAD – Java Application Descriptor (a.k.a Deployment Descriptor)

Overview (Common Issues)

- Disclosure of confidential information
- Modification or destruction of information
- Misappropriation of protected resources
- Compromise of accountability
- Misappropriation that compromises availability

Overview (Sample Architecture)



- Message Security
- Security Administration Authentication Server
- Certificate X509
- Meta-directory
- Firewall
- Intrusion Detection
- VPN
- Link Encryption
- Application Security Delegation
- Messaging Security

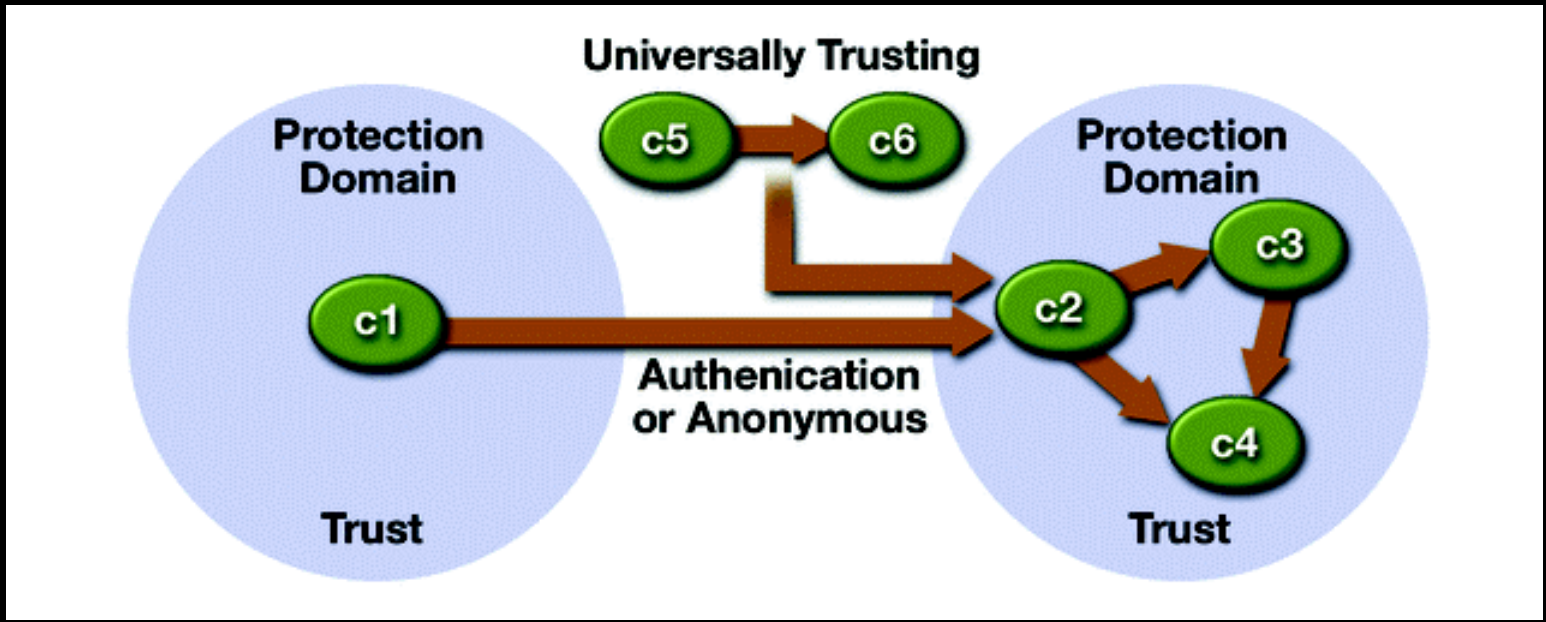
Sun microsystems

J2EE Security Patterns (by Ron Monzillo and Mark Roth)

- Class Scoped Authorization Pattern where all instances share common policy
- Instance Scoped Authorization Patterns where the policy is modified by either the state of the target instance or by the arguments of the invocation
- Distinguished Caller Pattern – Embedded in instance at instance creation or obtained from call arguments
- Distinguished Caller – Front Control Pattern – where only identity corresponding to front controller may operate on target class
- Distinguished Role Pattern – Instance determines if caller is in select role using isCallerinRole
- Lazy Authentication Gateway Pattern –where protected "EJB" component tier is accessed through protected "web" tier components
- Proactive Authentication Pattern – Presentation of unprotected web resources that provides links to protected web resources that can be visited to force authentication

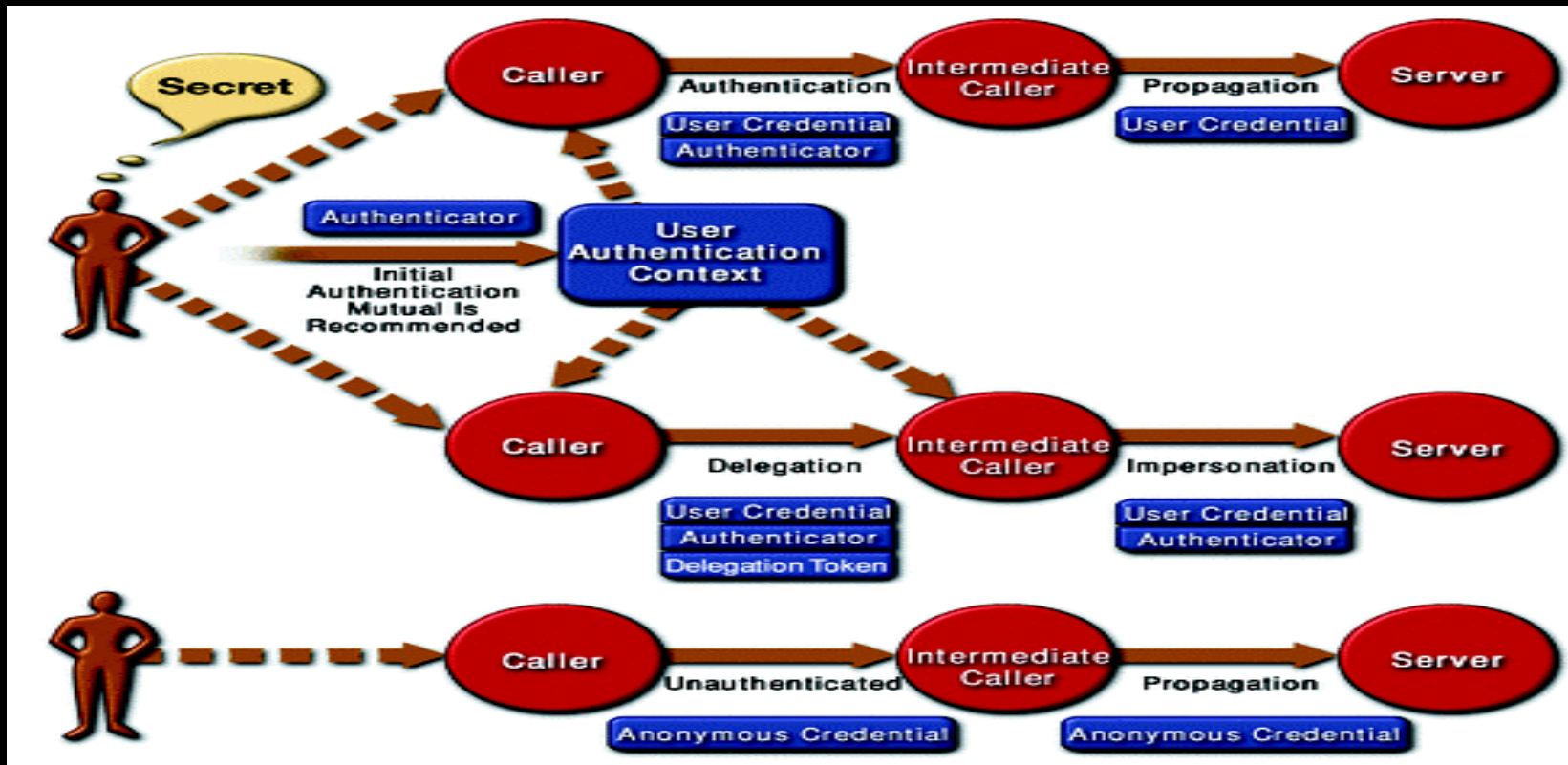
J2EE & Application Level Security

- Authentication is only required for interactions that cross the boundaries of a protection domain



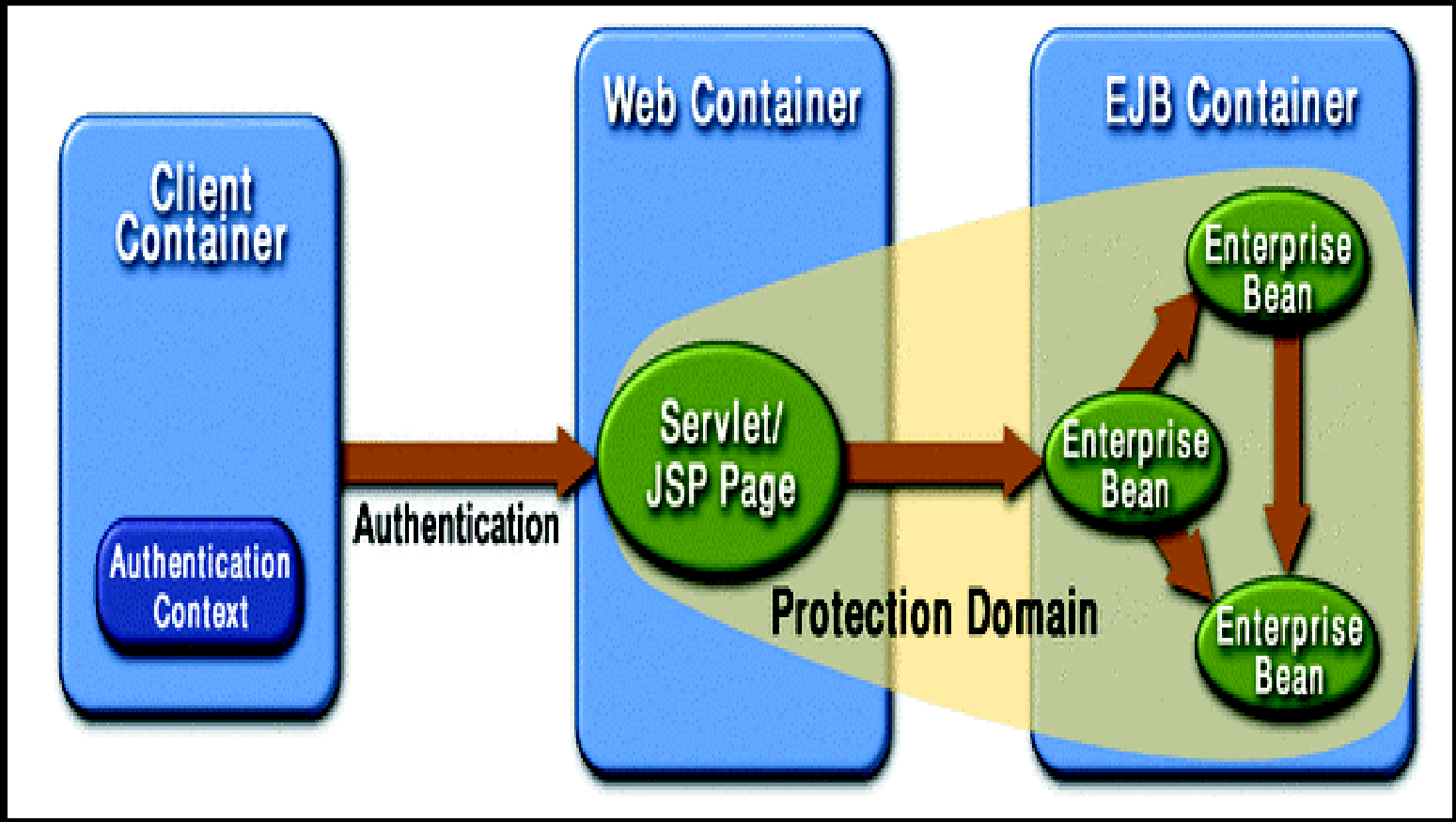
J2EE & Application Level Security

- For inbound calls, it is the container's responsibility to make an authentic representation of the caller identity available to the component in the form of a credential. An X.509 certificate and a Kerberos service ticket are examples of credentials.
- For outbound calls, the container is responsible for establishing the identity of the calling component. In general, it is the job of the container to provide bi-directional authentication functionality to enforce the protection domain boundaries of the deployed applications.



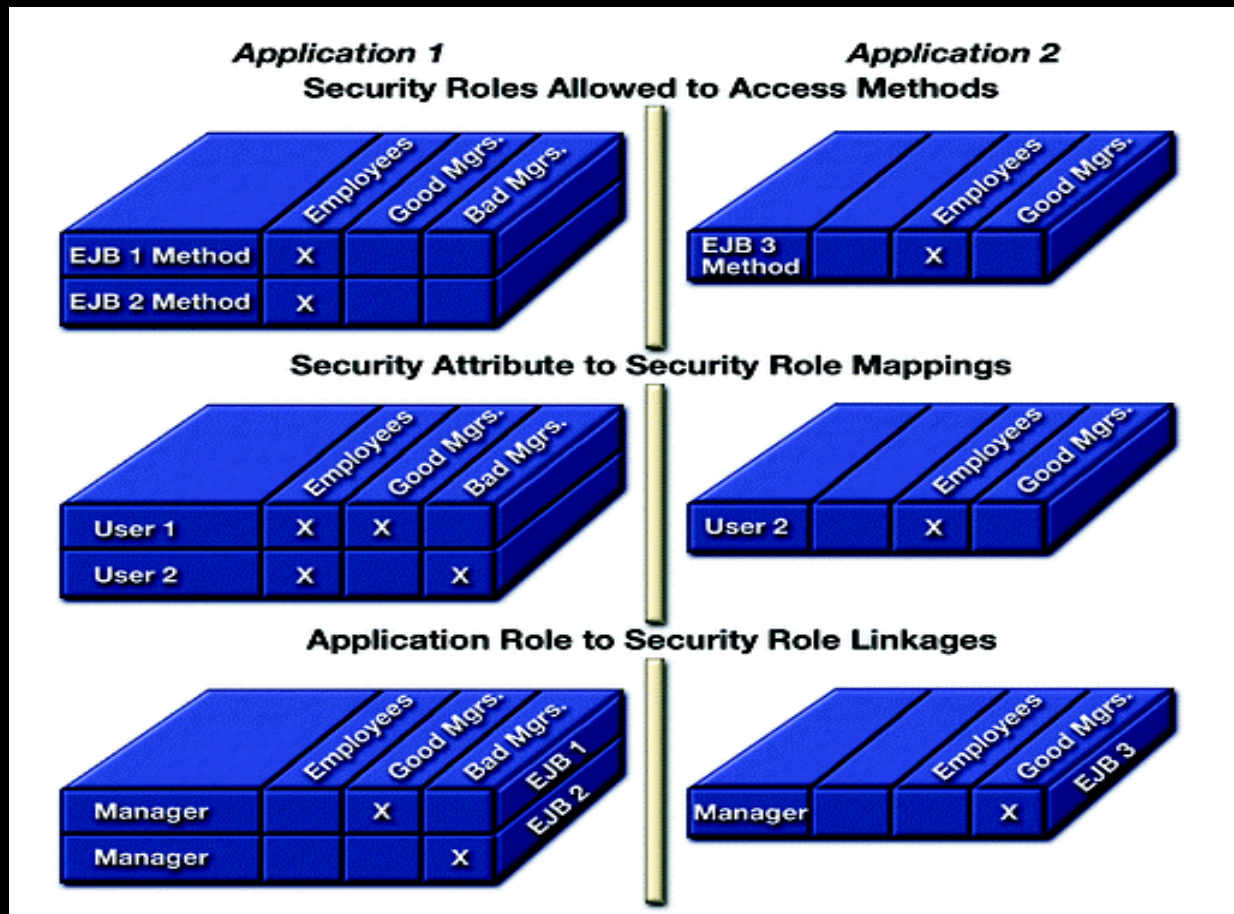
J2EE & Application Level Security

- A Web container is leveraged to enforce protection domain boundaries for Web components and the enterprise beans that they call.



J2EE & Application Level Security

- configuration of method permissions as a relationship between roles and methods is used for mapping of caller security attributes to roles, and the link between privilege names embedded in the application and roles.



J2EE Security Compatibility Tests

- J2EE secure interoperability Tests -emphasize that all j2EE compatible containers must pass the conformance test suites CTS, to confirm that they are interoperable
- Servlet Container - HTTP and HTTPS, with Basic Auth, Digest Auth (is optional), and Form-Based Login, which can be run over an SSL secured transport. Also require SSL mutual auth
- All EJB 1.3 containers, are required to support CSIv2 level 0
- For EJB containers, Sun has developed a logging interceptor, that run as either the client or the server side to validate the behaviour of a peer. Logging state SAS protocol messages, and security tokens received and compare them with expected values.

J2EE Security -Integration of EE Container with J2SE Security Model

- This is a new feature being developed in JCP for EE 1.4 Containers – the idea is will be required to use the interfaces of the SE policy objects to perform their access decisions.
- This will allow replace-ability and bridging to external policy via SE's Policy replace-ability interface.
- This SPI/Contract defines a policy configuration subcontract for translating the declarative authorization rules in deployment descriptors into Policy statements within a Policy module.
- It also defines a Policy decision subcontract that defines how containers shall use the SE policy decision interface to perform their access decisions.
- It also will integrate the container defined access control context associated with a call thread with the SE notion of an access control context, such that the caller's access control context will be applied in permission checks made from components.
- It also provides the option, for containers to supply the parameters to a call, or a reference to the target instance for use in the Policy decision.
- JCP is working to make sure that an XACML Policy Provider may plug in under EE

Sun microsystems

J2EE Security –for Web Services

- JCP (led by IBM) is working on JSR 109 Implementing Enterprise (Java) Web Services to implement and deploy web services on the EE platform.
- Integrated with the WSDL (web services description language), UDDI, and SOAP web services computing paradigm.
- JAX-RPC (i.e. JSR 101 Java API for XML-based RPC. - to define Java API's for invoking remote procedures using an XML based protocol (i.e SOAP 1.1evolution to 1.2). Both the client and the server sides of the remote procedure are defined.
- API's are being added to the Java Platform to support XML digital signature JSR 105 and XLM Encryption JSR 106.
- JSR 104 Trust Services, will integrate XKMS into the platform such that the barrier to PKI reliance can be reduced WRT relying parties.
- JCP is also working to define profiles for the use of XML signatures to protect data content above the network transport, to support end-to-end integrity of messages.
- JSR 155 will provide API's to interact with SAML authorities, to get things like attribute assertions (i.e read attribute certificates) while treating the SAML authority a an other JAX-RPC accessible web service.

J2EE Security –Project LIBERTY

- Project Liberty, which intends to rely on SAML as its form for exchanging representations of identity.
- SAML an XML based Framework for exchanging Security Information is leveraged for SSO, Distributed Transaction and Authorization Services.
- The liberty authentication service providers will act as SAML authorities to their relying parties.
- Network Identity Project announced by SMI – a Platform that includes software, hardware and services to establish and validate identities associated with users (consumers/employees) and servers – to support Liberty when the specifications are finalized.
- Go to JAXR (JSR 93) – http://jcp.org/jsr/detail/93.jsp
- Go to Enterprise Web Services JSR 109 at http://jcp.org/jsr/detail/109.jsp

J2EE Security – Security Management

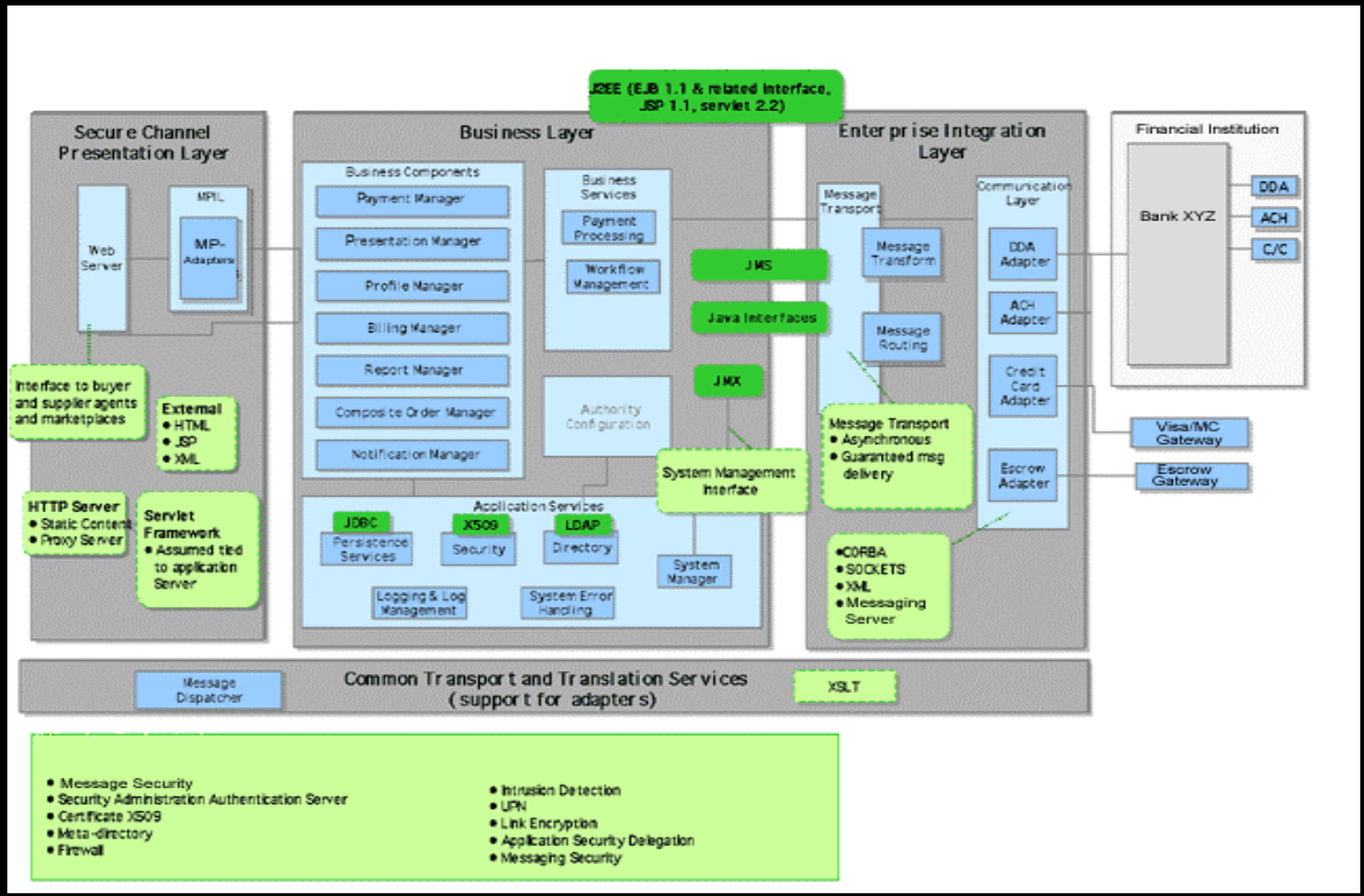
- JSR 77 defines a paradigm (based on JMX) for wrapping objects with mbeans.
- Container vendors, (e.g. BEA), have already begun the process of using this paradigm to manage EE security providers.
- JSR 77 intends to evolve to model and standardize the management of EE systems.

Sun microsystems

J2EE and Application Infrastructure Security Techniques

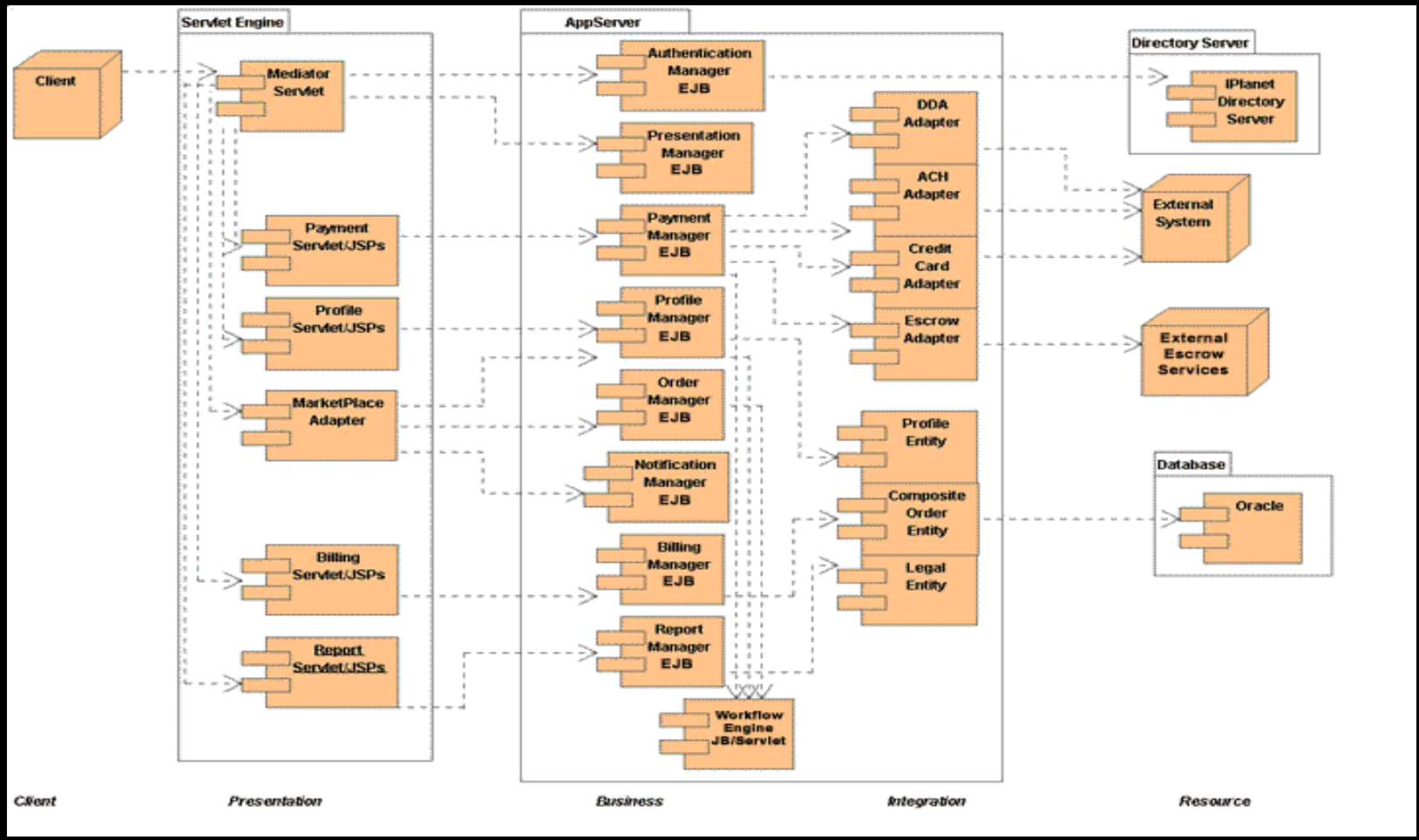
- Location of Application Infrastructure Solutions
- Communication Flow
- EDMZ/IDMZ/DMZ rules
- Impact on HA and Scalability
- Impact on Storage Architecture

Application's Functional Architecture

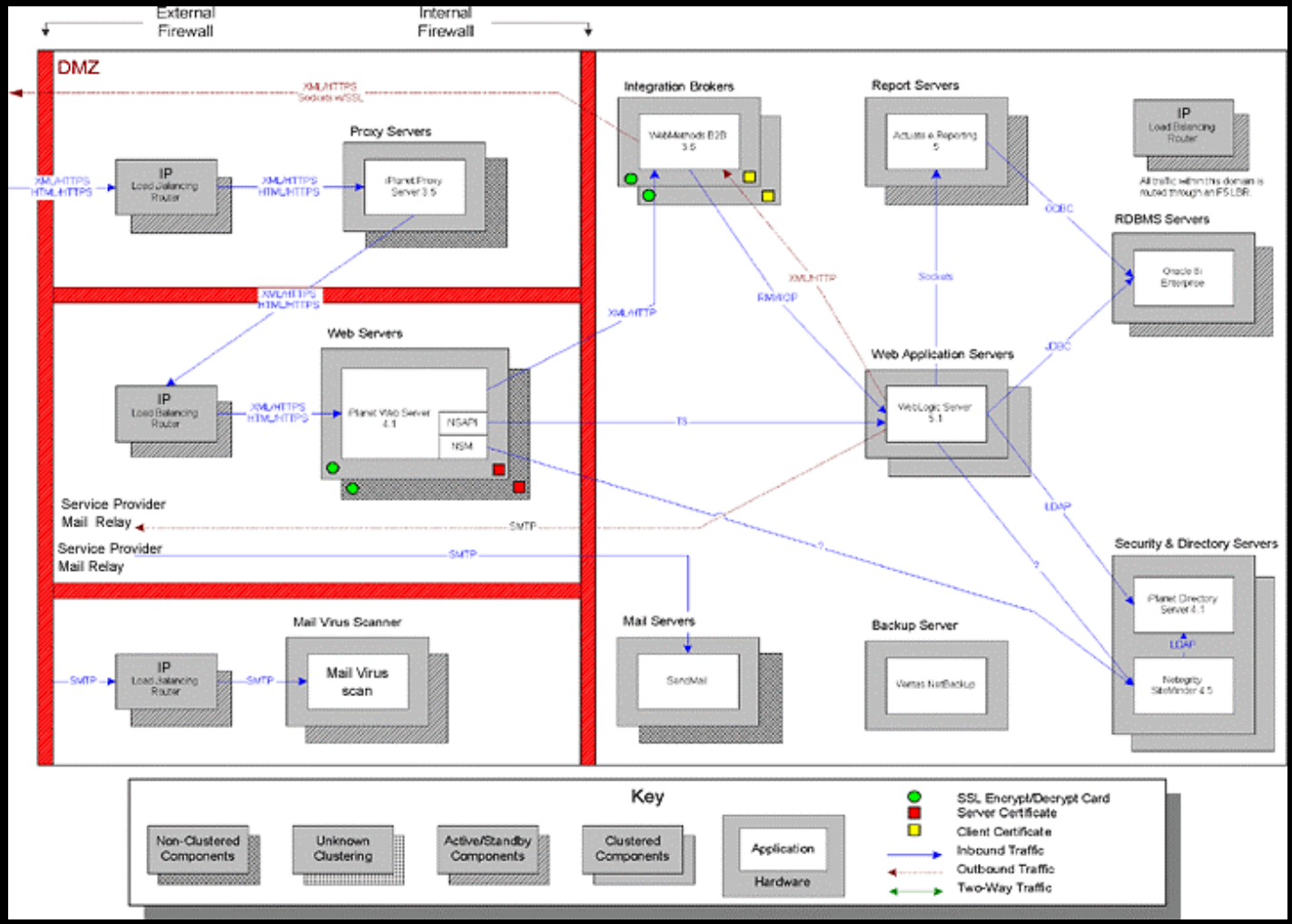


Sun microsystems

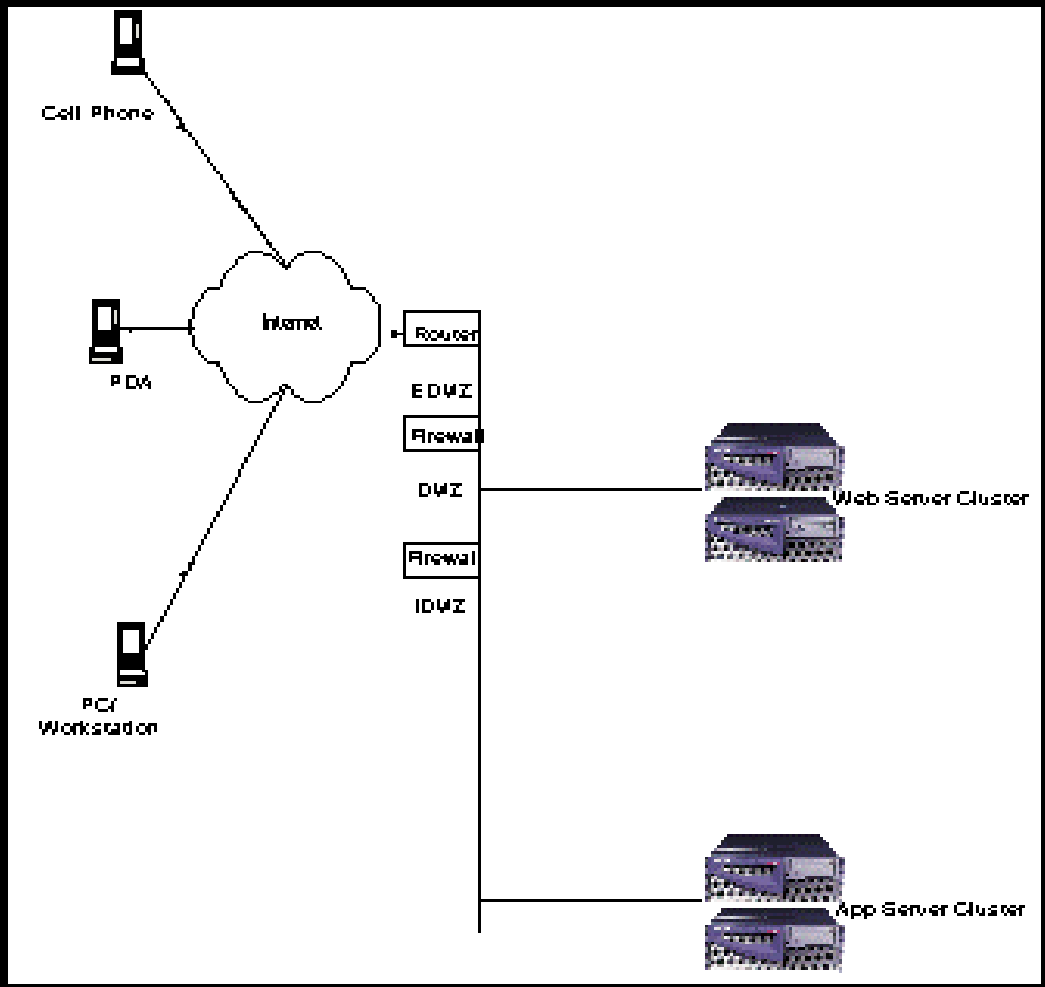
Application's Application Infrastructure Architecture



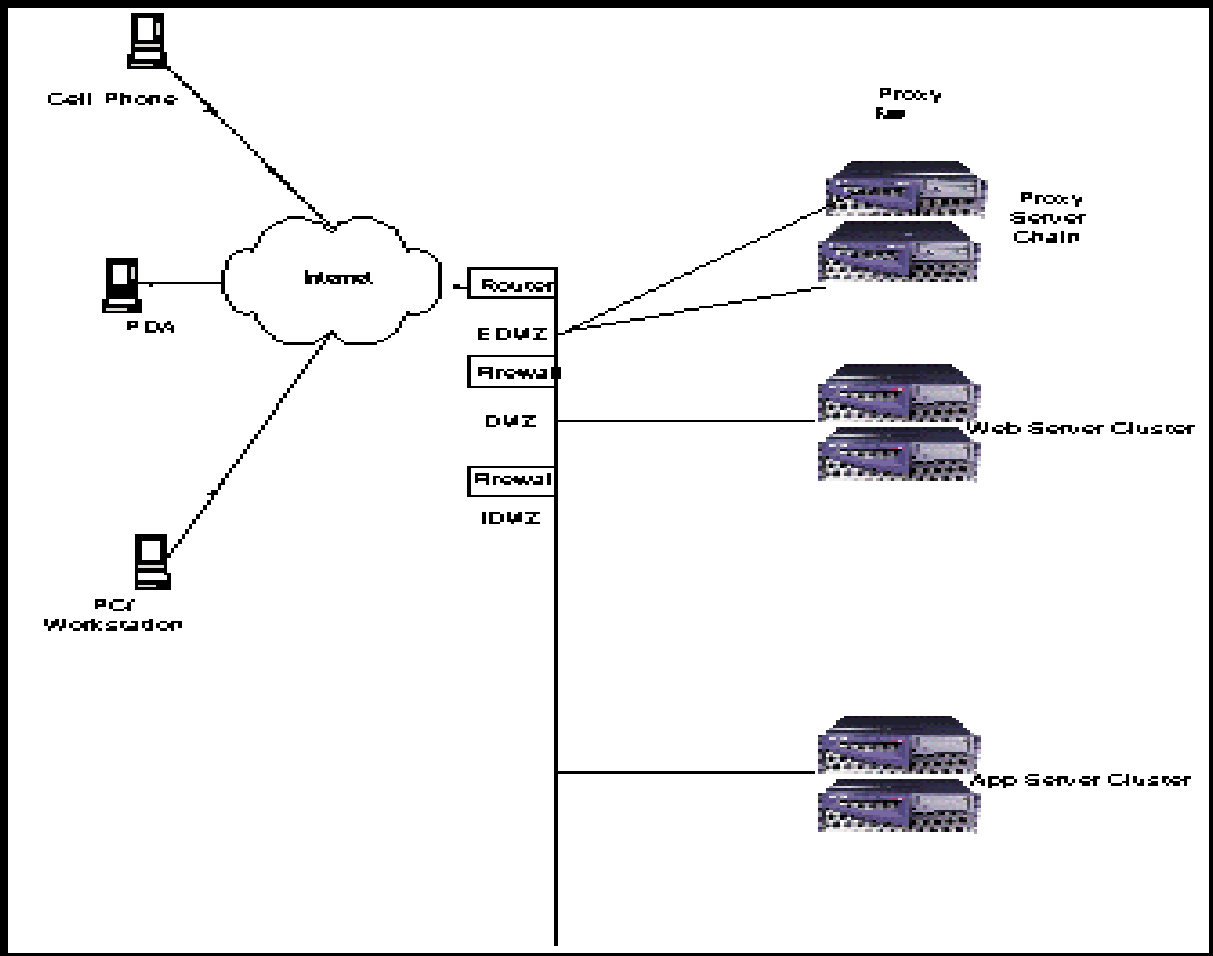
Application Infrastructure Communication Flow



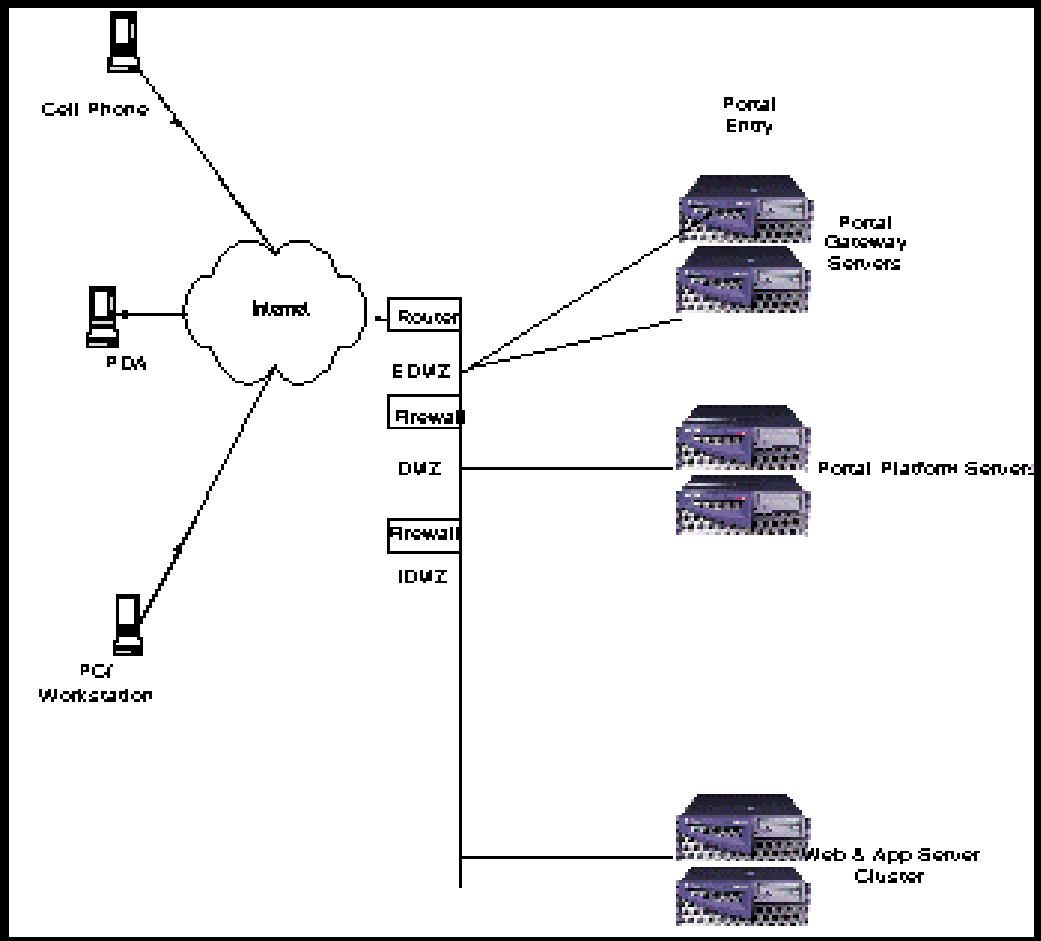
Application Infrastructure – Web Server & Web proxies (JSSE™ and JCE™ components)



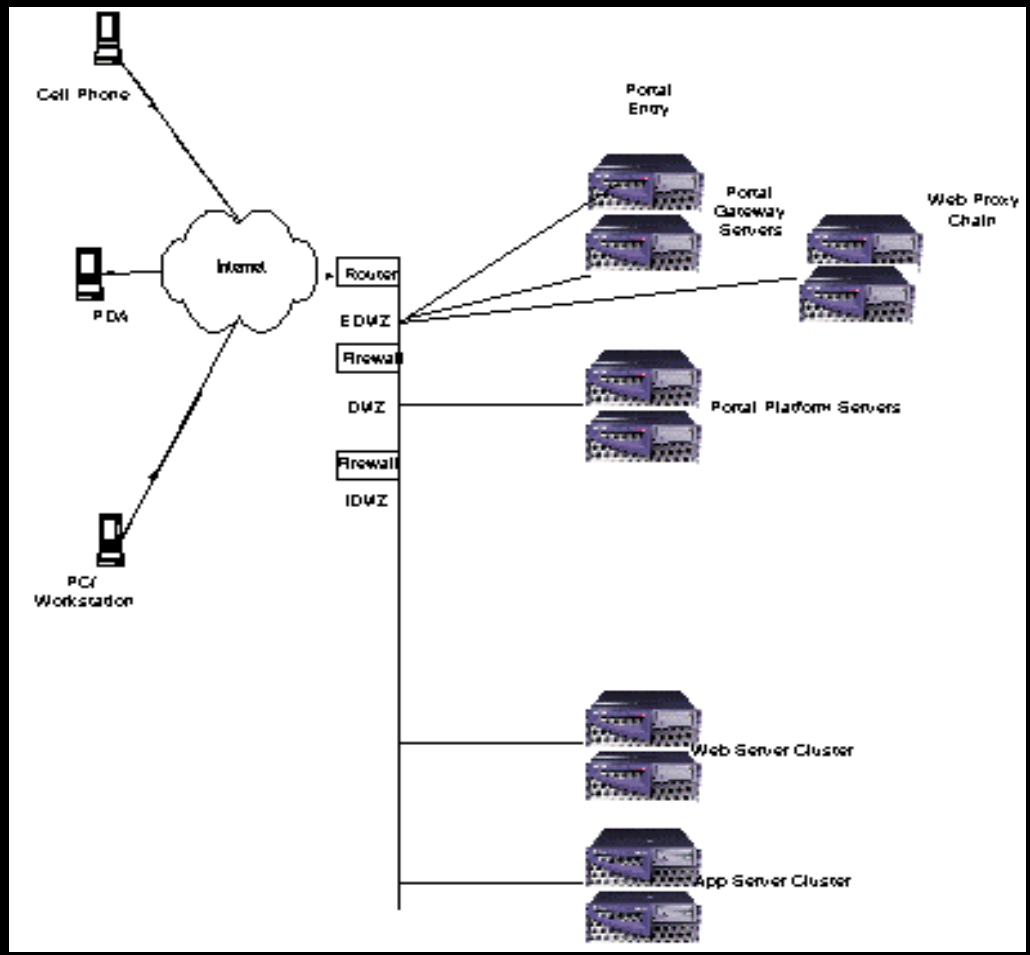
Application Infrastructure – Web Server & Web proxies (JSSE™ and JCE™ components)



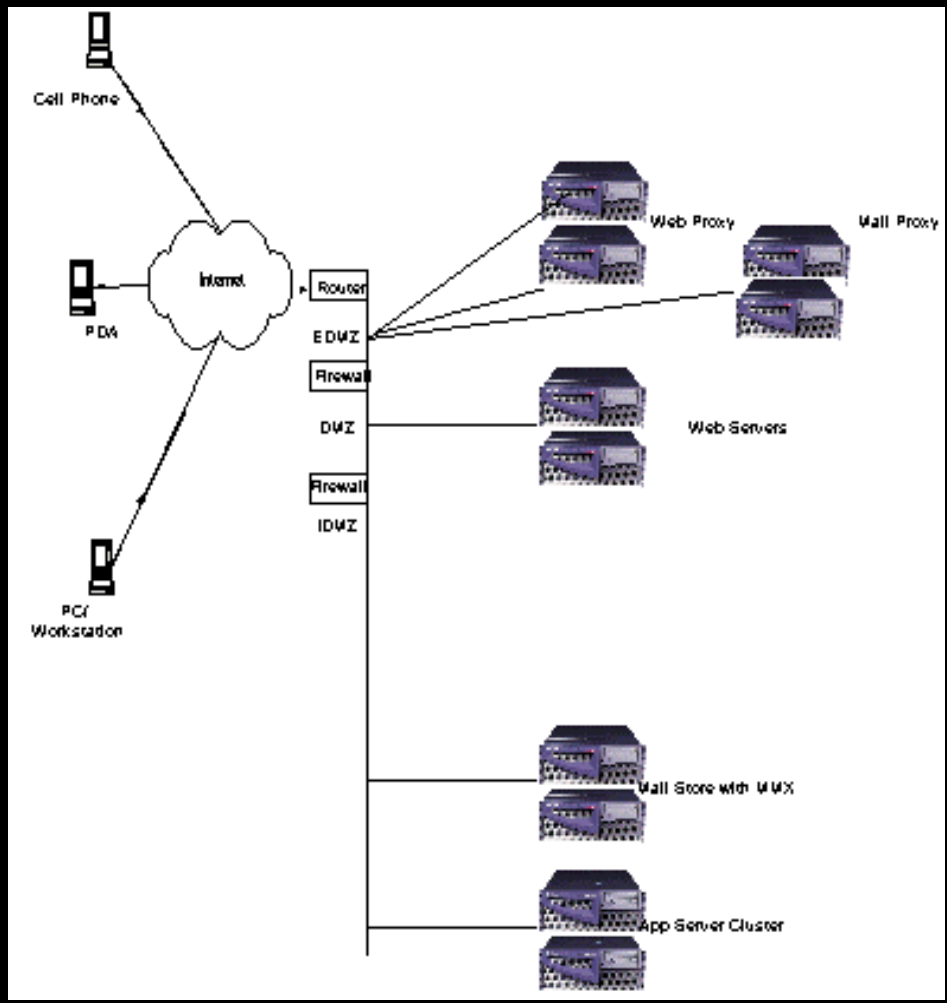
Application Infrastructure – Portal Gateways and Portal Servers (JSSE™, JAAS™ and JCE™ components)



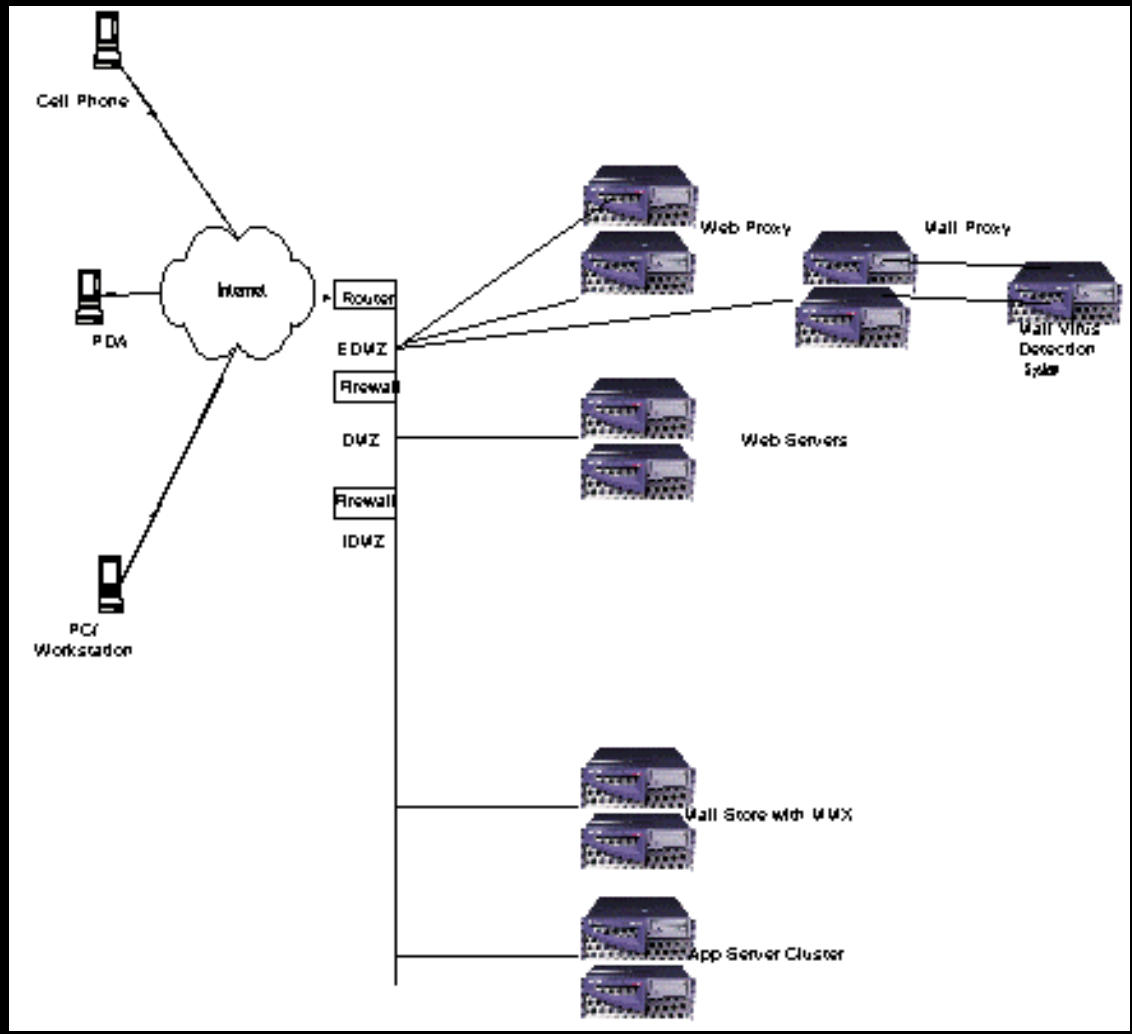
Application Infrastructure – Web proxies with Portal Gateways (JSSE™, JAAS™ and JCE™ components)



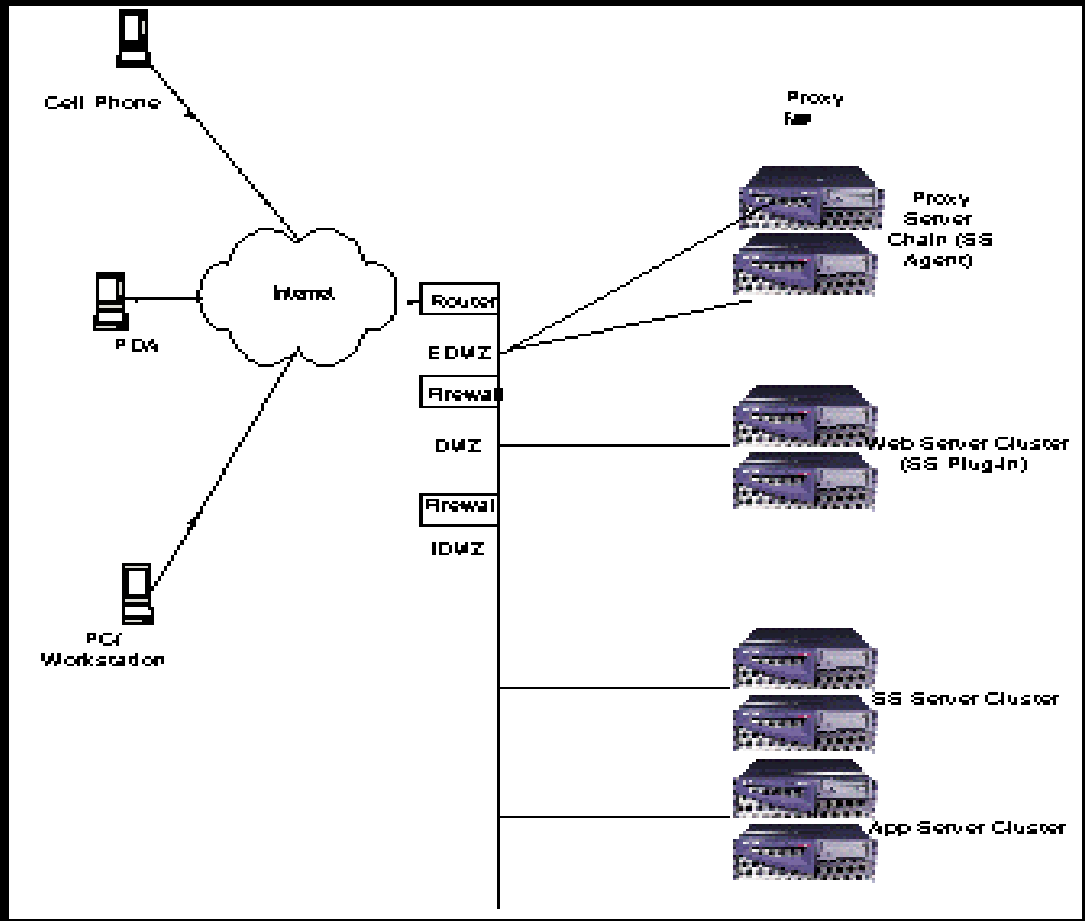
Application Infrastructure – Web Mail with Web Mail Proxy (Java Mail API's)



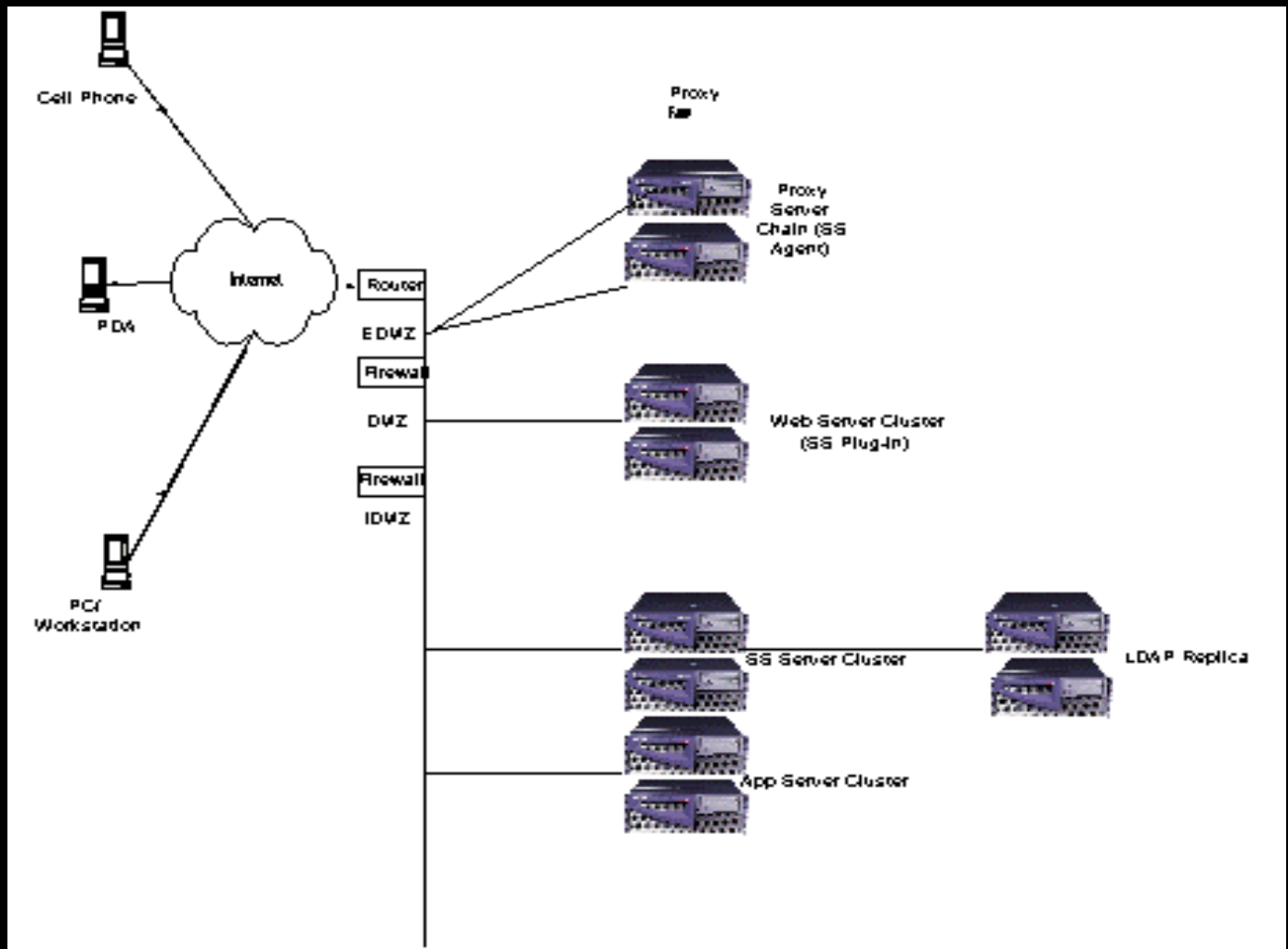
Application Infrastructure – Web Mail with Web Mail Proxy and MVD (Java Mail API's)



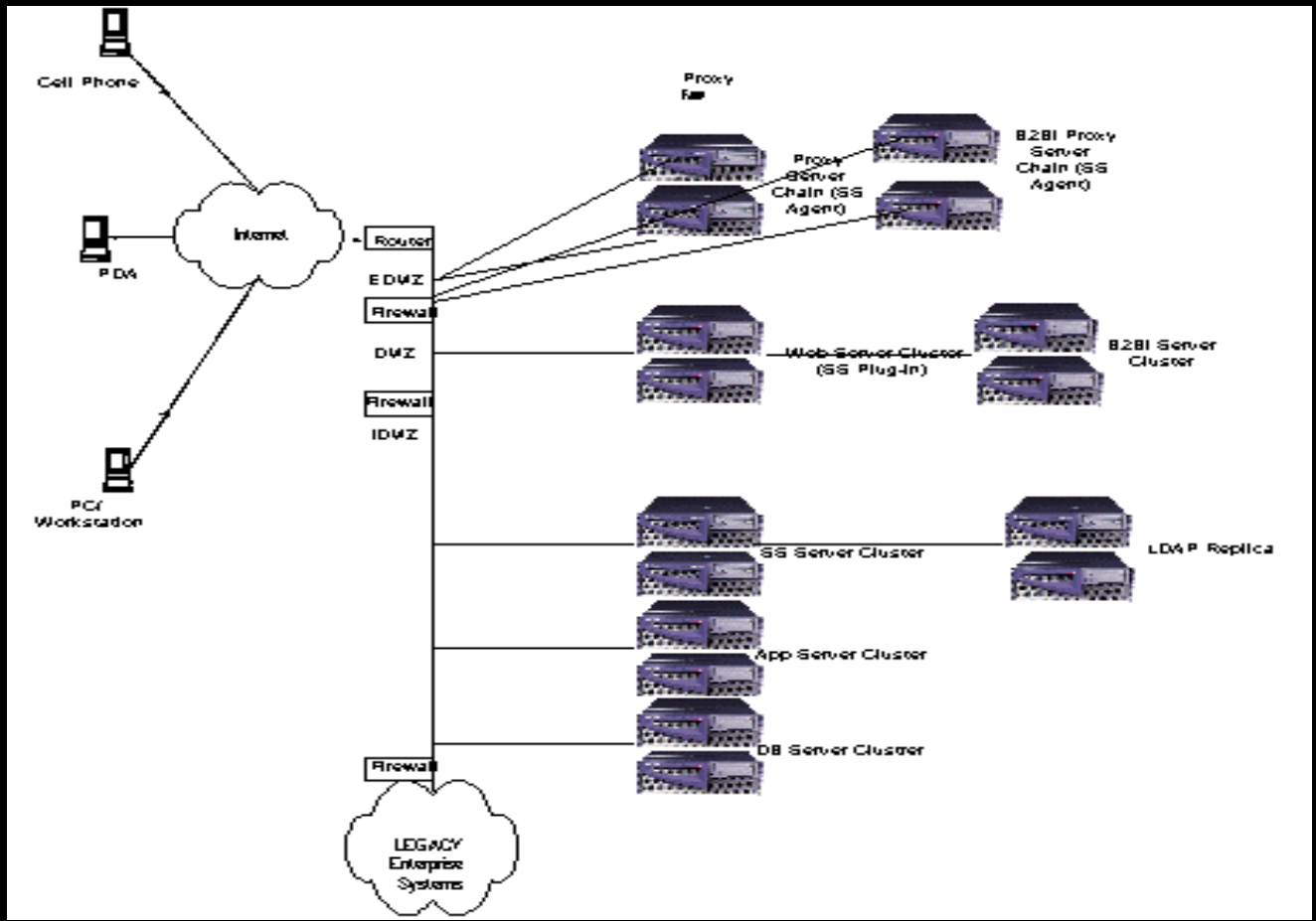
Application Infrastructure – Application Server with Security Server (EJB™, JSP™ and Servlet components)



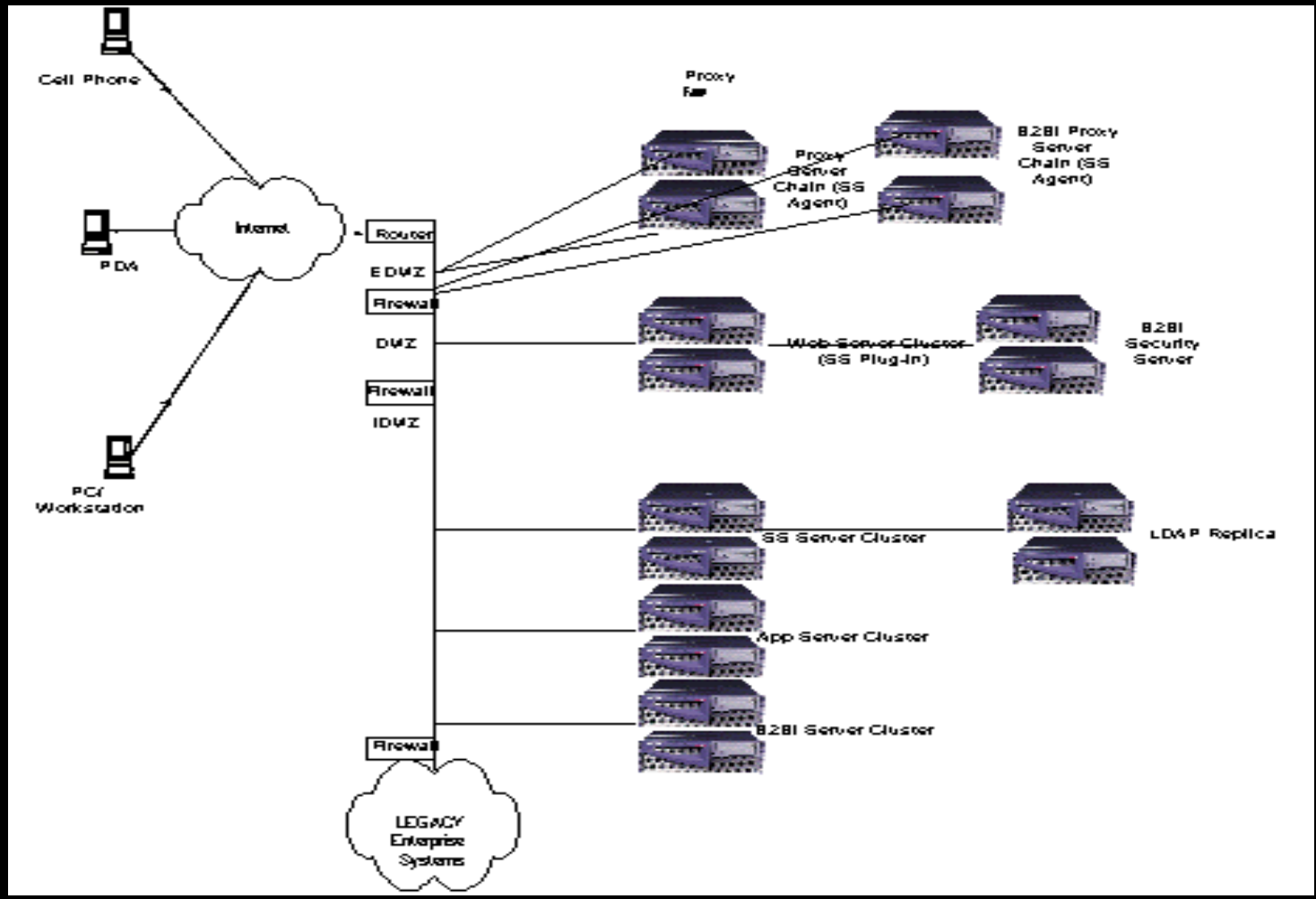
Application Infrastructure – Application Server with Security/LDAP (EJB™, JSP™ and Servlet components)



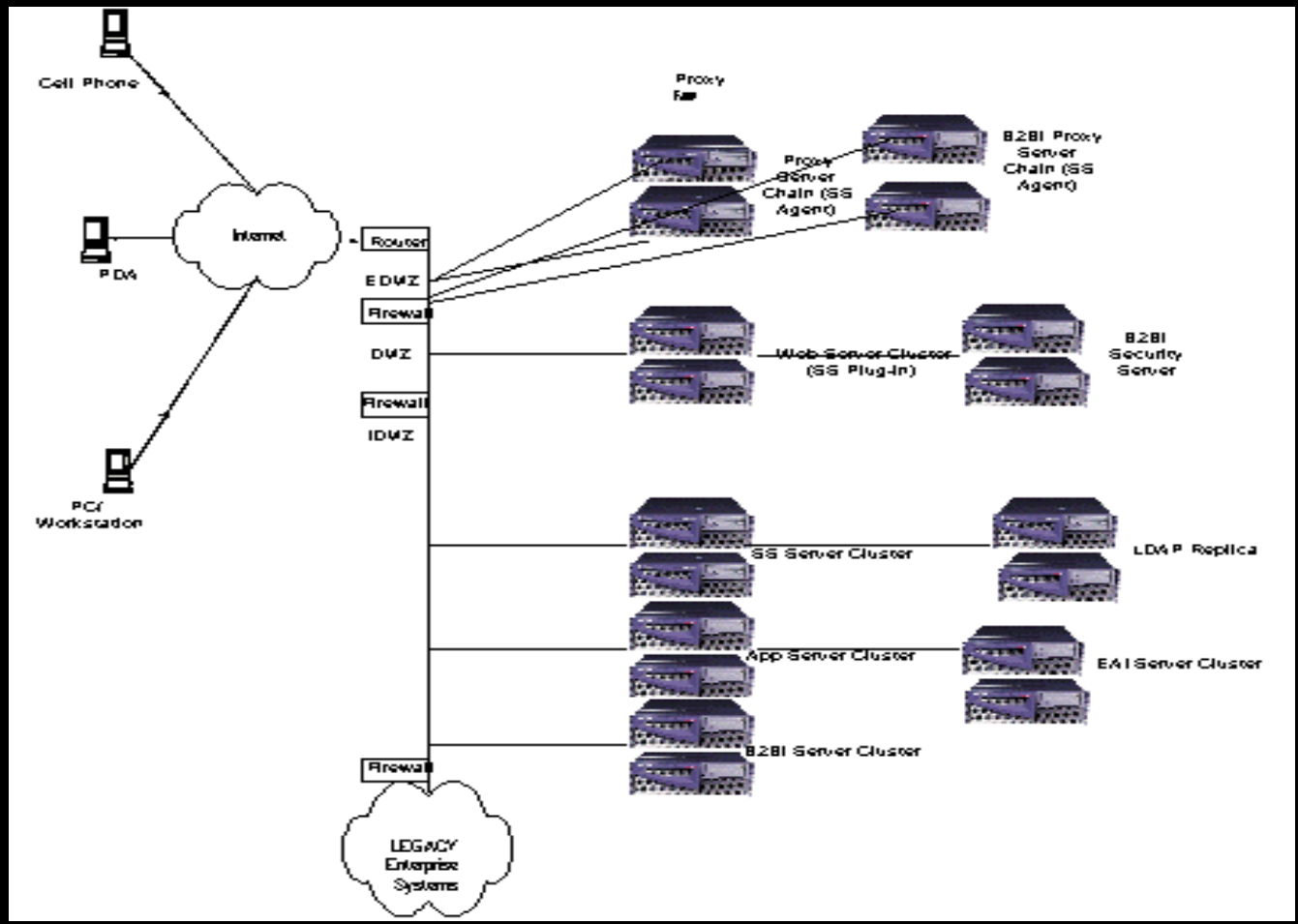
Application Infrastructure –Integration Server B2Bi (+Proxy) (JMS™, JTS™, XML™ and JCA™ components)



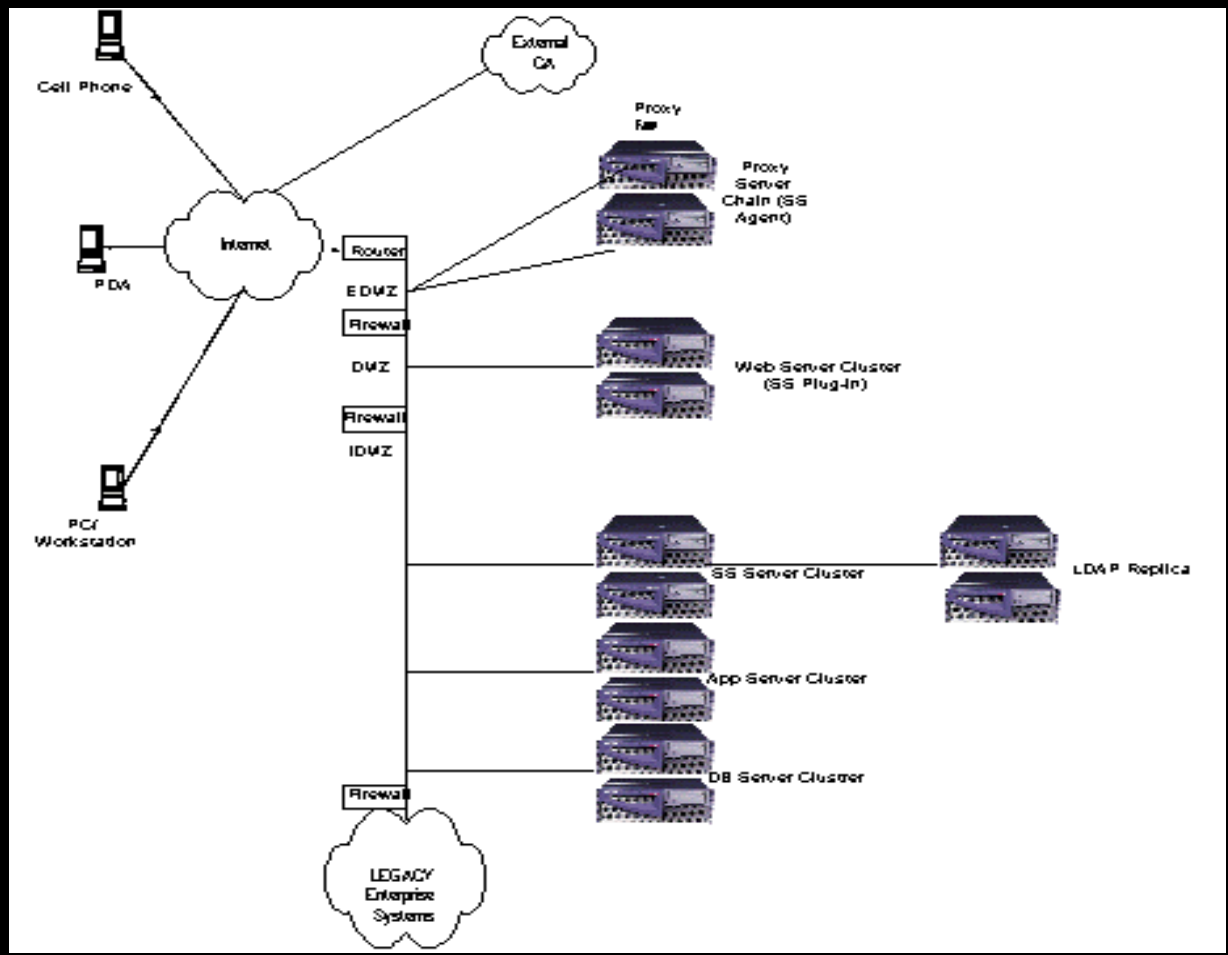
Application Infrastructure –Integration Server B2Bi (+Proxy+SS) (JMS™, JTS™, XML™, SOAP™ and JCA™ components)



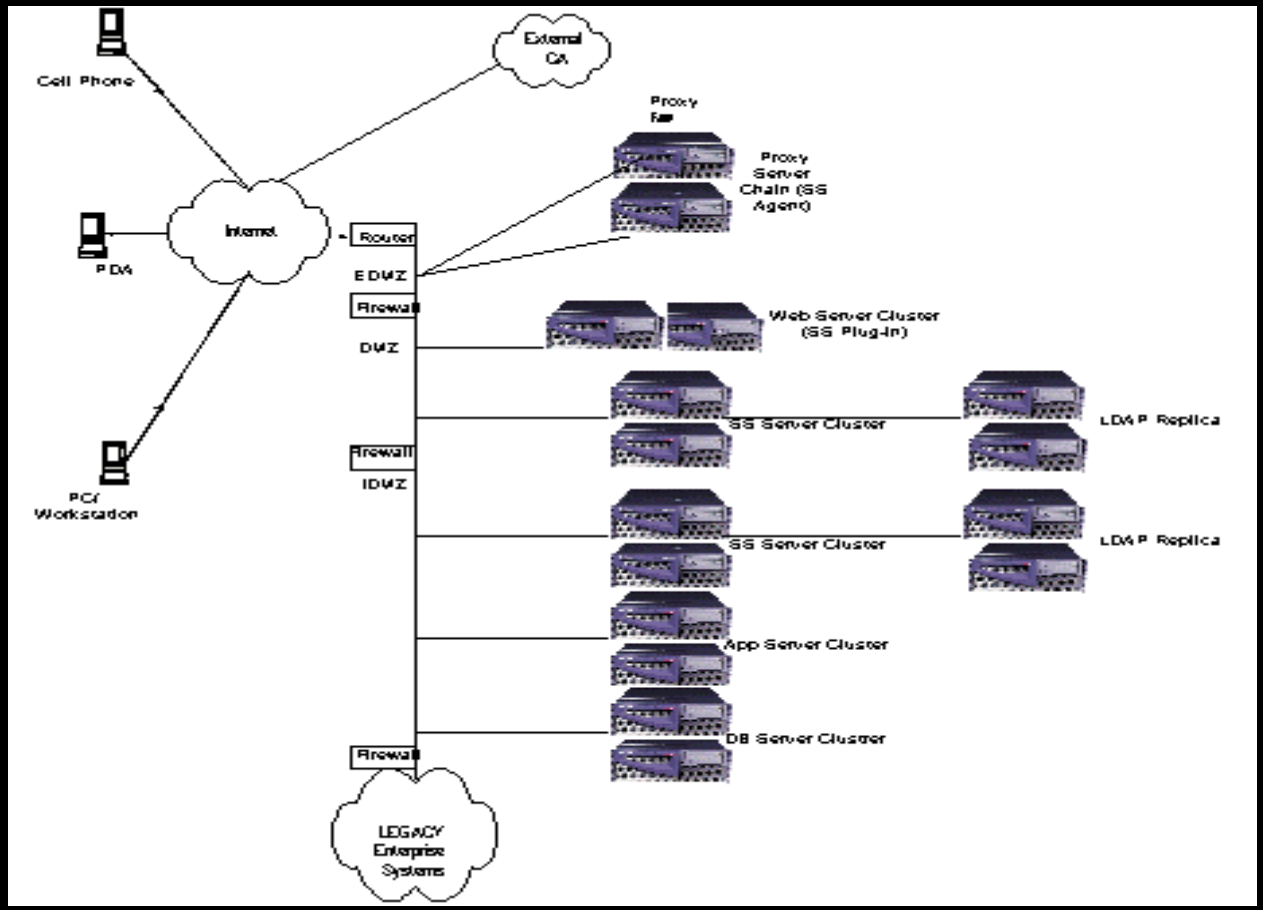
Application Infrastructure –Integration Server B2Bi & EAI (JMS™, JTS™, XML™, SOAP™ and JCA™ components)



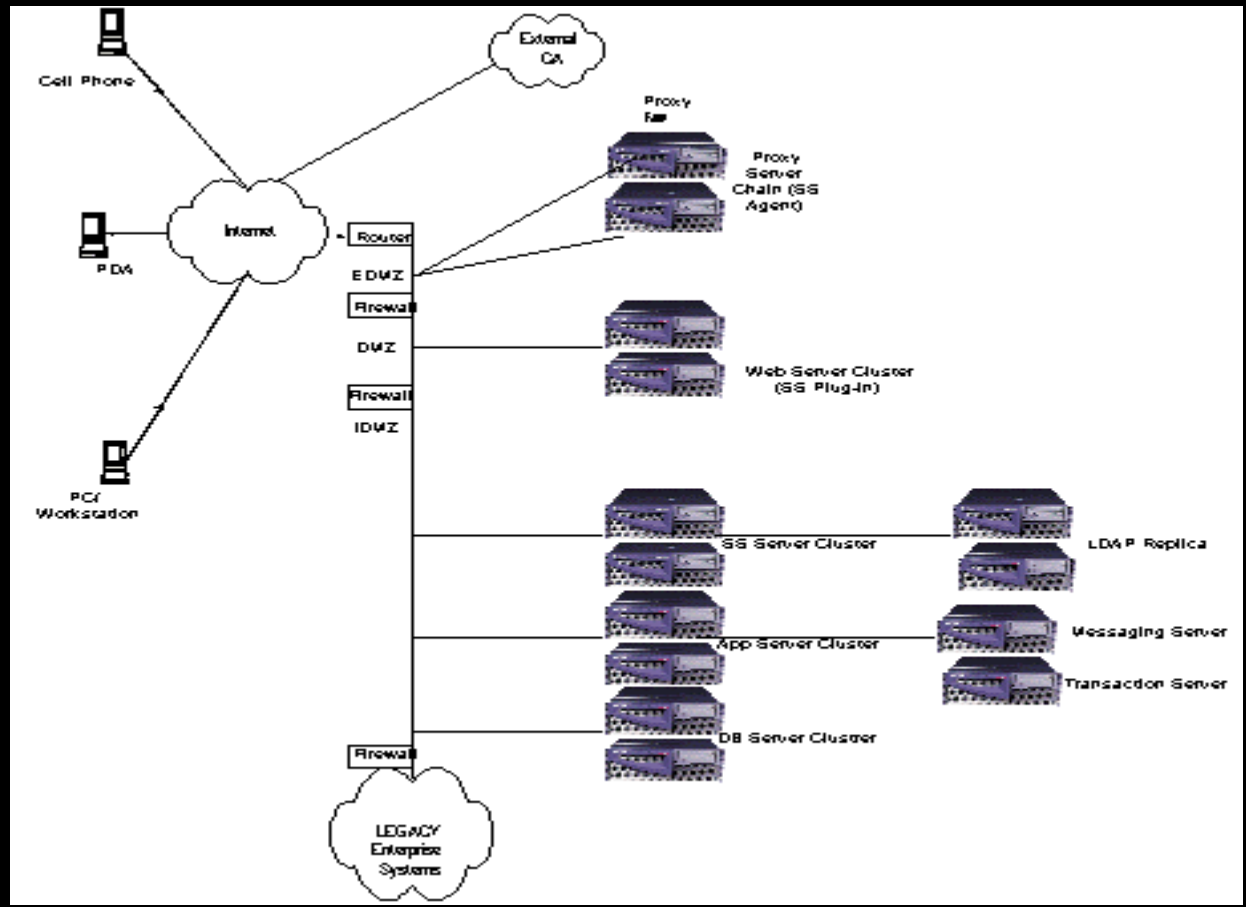
Application Infrastructure – Directory and AAA Server (JNDI™, JAAS™, and SSO™ components)



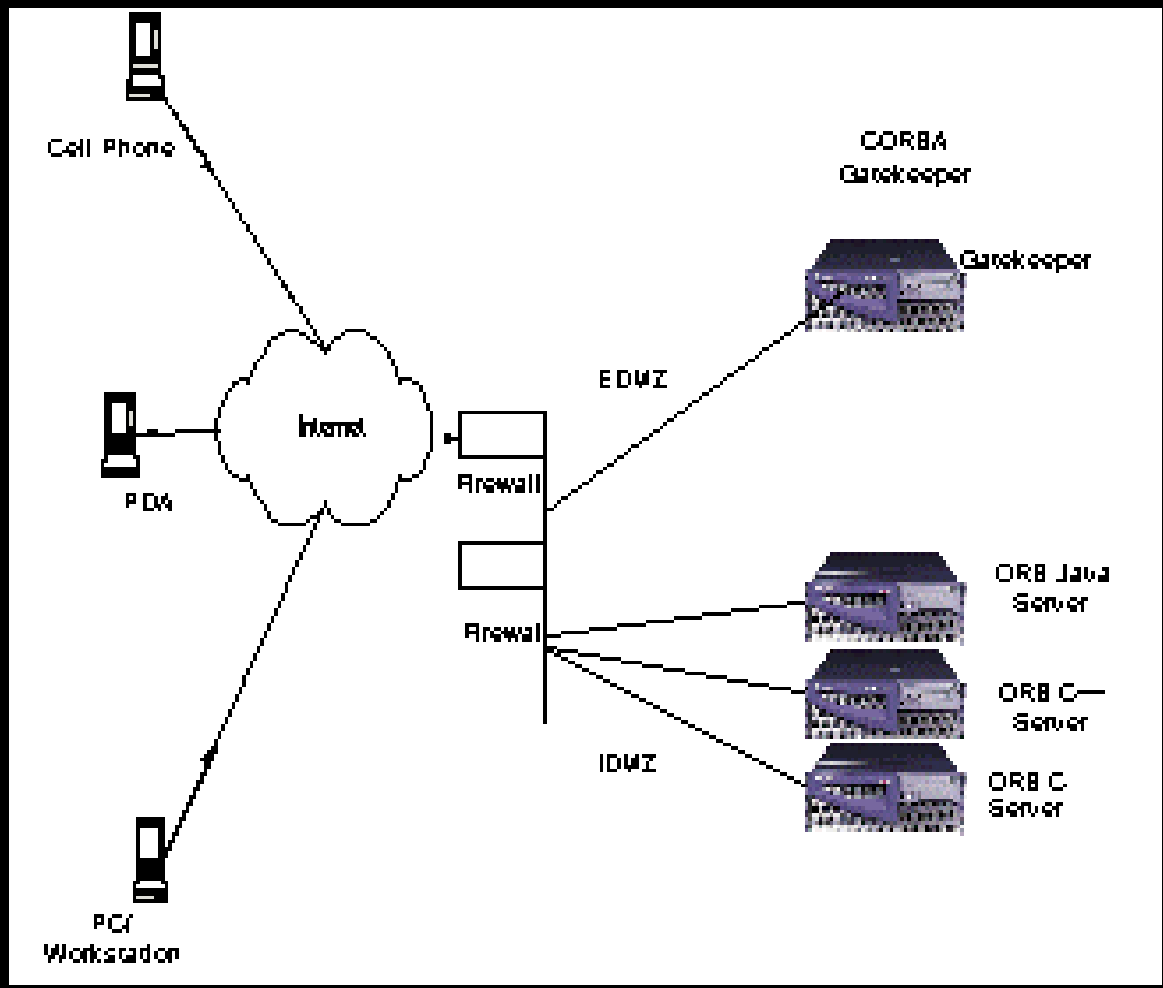
Application Infrastructure – Directory and AAA Server (JNDI™, JAAS™, and SSO™ components)



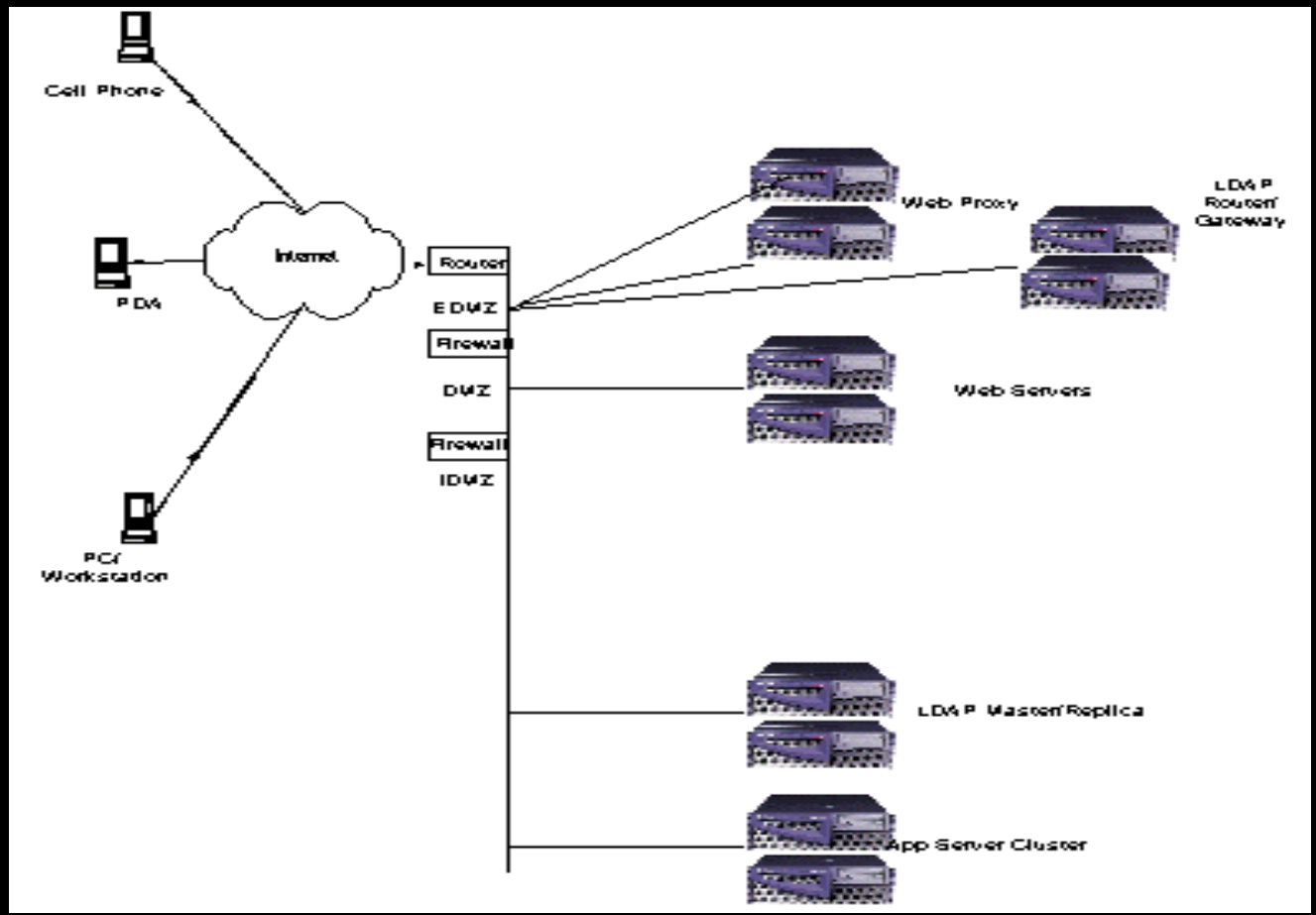
Application Infrastructure – Messaging & Transaction Server (JTS™ and JMS™ components)



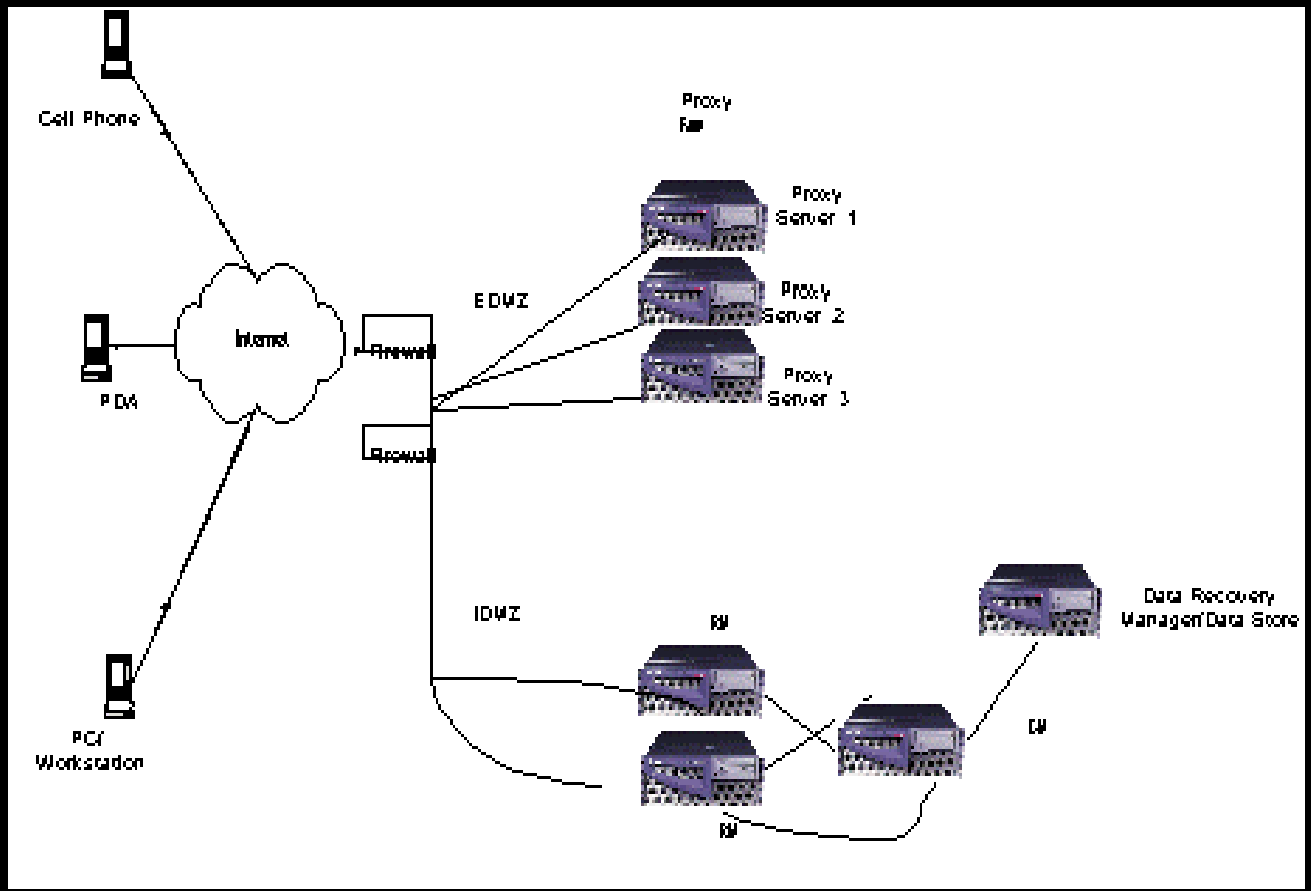
Application Infrastructure – CORBA & LDAP gateways (JavaIDL and JNDI components)



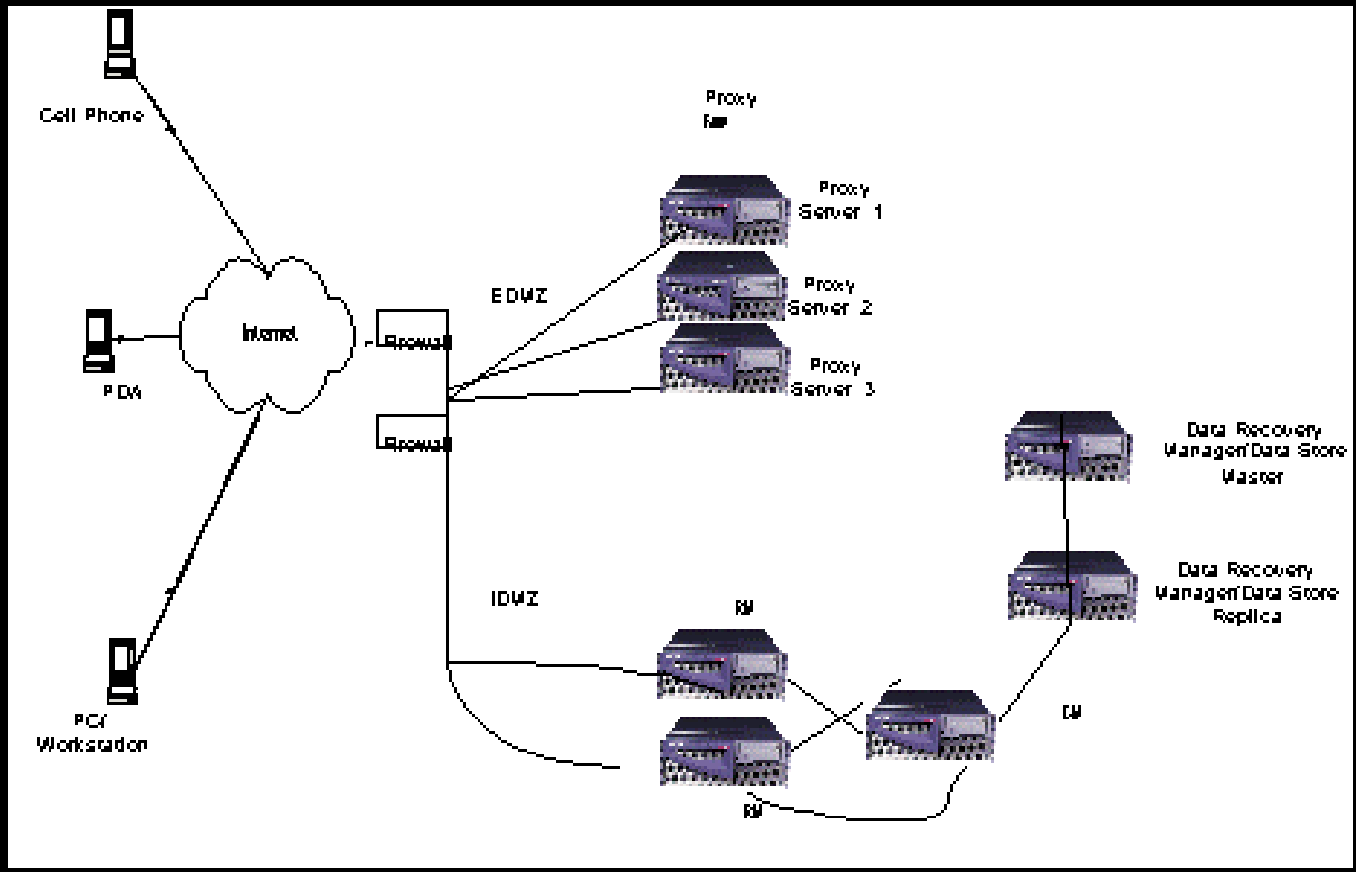
Application Infrastructure – CORBA & LDAP gateways (JavaIDL and JNDI components)



Application Infrastructure – Certificate Server (CMS components)



Application Infrastructure – Certificate Server (CMS components)



Sun microsystems

Application Infrastructure – Additional Solutions

- J2ME-MIDP/CLDC based mobile application servers
- Trans-coding Servers
- SOAP handlers (outside firewall)
- SAML/Web Services Security Servers

Pervasive Nature of Security Requirements

- Application Security (protection domains within and between applications, application level intrusion detection/deployment descriptors, JAD, etc.)
- Application Infrastructure Security (PKI, Certificates, SSL, Ldap, S-Http, etc.)
- Network Security (Firewalls, DMZ, VLAN, VPN, NID, etc.)
- Compute and Storage Security (OS hardening, zoning, etc.).

Systemic Qualities impact on Security

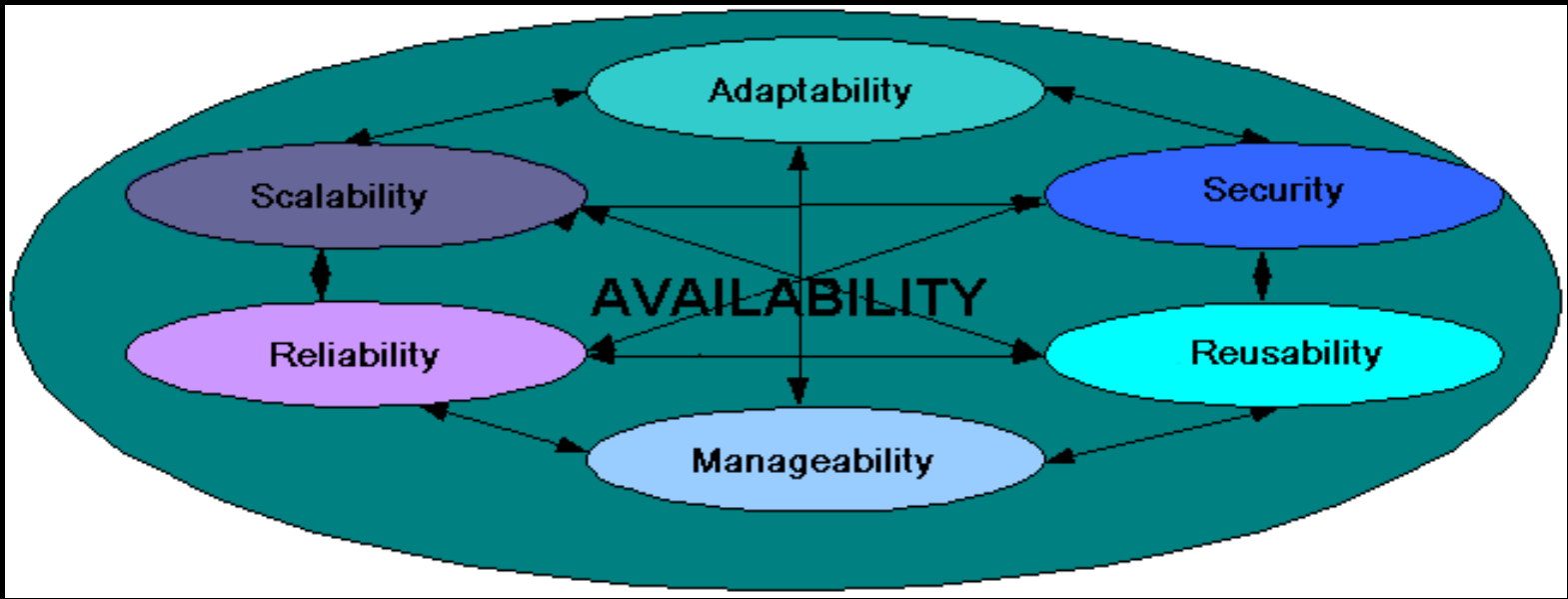
High Availability – WAP gateway as a SPOF

Scalability – Web Proxy Servers Scalability

Compatibility – Security Techniques hindering inter-operability

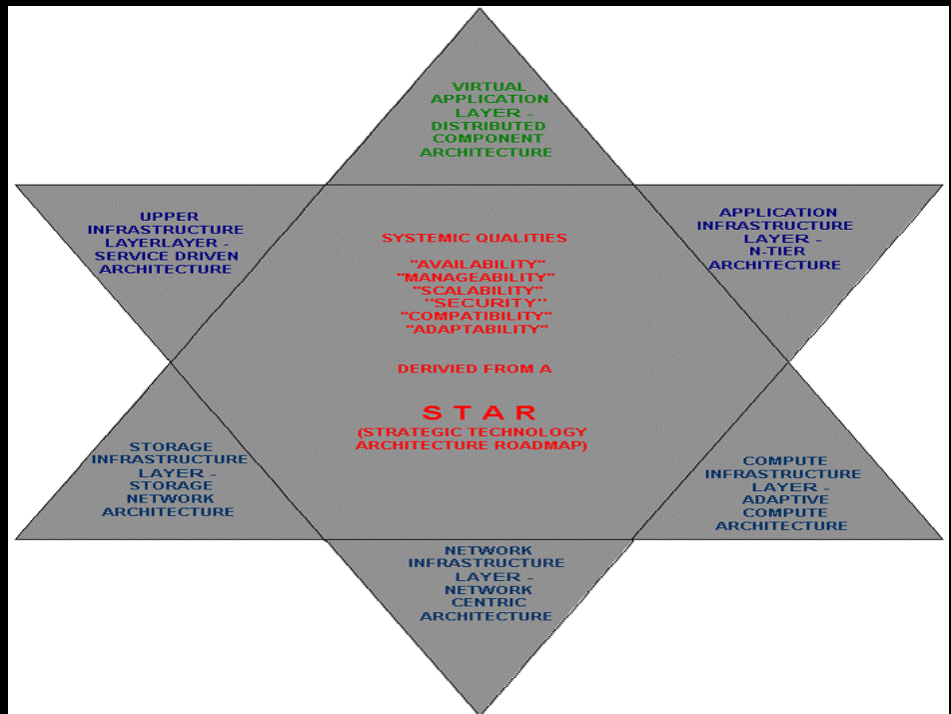
Adaptability – Changing Security Requirements

Manage-ability – Secure Management Environment



Layered Approach to Addressing Systemic Qualities

VAL –	Distributed Component Architecture –	J2EE™ + JAX pack
AIL –	N Tier Architecture -	SunONE
UIL –	Service Driven Architecture –	SunTONE and Managed Services
NIL –	Network Centric Architectures –	SDN
CIL –	Adaptive Compute Architecture –	N1
SIL –	Storage Network Architecture –	Storage ONE



Layers of Security Techniques

Application	Application Layer	J2EE™ Technology Platform (EJB™, JSP™, Servlet, Applet, JMS, JTS, JCE, JMX, JMF, etc.)
Infrastructure	Application Infrastructure Layer	Application Infrastructure Technologies (app server, integration server, database server, CORBA server, media server)
Infrastructure	Management Infrastructure Layer	Management Infrastructure Technologies (change management tools, system management tools, problem management tools)
Infrastructure	Network Infrastructure Layer	Networking Infrastructure (VLAN, DMZ, IDMZ, EDMZ, HSRP, VRRP, and switching/routing)
Infrastructure	Compute Server Infrastructure Layer	Compute Server Infrastructure (low-end systems [4-way], high-end systems [64- way], RSM, SSM, DSD, ADR, IDN)
Infrastructure	Data Storage Infrastructure Layer	Data Storage Technologies (NAS, DAS, SAN, Solid State, HSM, SNDR, II)

Sun microsystems

J2EE™ Vs .NET

Category	J2EE™ Vs .NET	Comments
Secure Communication	J2EE™	Java is the hands down winner here
Role based Access Control and user Authentication	J2EE™	JAAS is better that what's available in .NET
Code containment and execution	.NET	App domains are less permeable
Code based Access Control	.NET	.NET seems to have learned a lot from J2EE™ Security
Code and Data Protection	TIE	J2EE™ is more flexible - .NET offers Windows features
Auditing and Tracking	TIE	Both are weak

Questions??

Email: Rakesh.Radhakrishnan@sun.com

RAKESH
RADHAKRISHNAN
Sr. IT Architect

rakesh@east.sun.com