JAVA DAYS ´98

CORBA on the Internet

Barry O´Reilly

IONA Technologies

Sun microsystems

IIOP - Open for Business

- **The Internet e-commerce infrastructure must provide:**
  - **Integration with existing WWW technology,**
  - **Scalability,**
  - **Firewall Navigation and Access Control,**
  - **Security (Authentication, Privacy, Integrity),**
  - **Transactional Capability,**
  - **A standards-based approach.**

IONA Technologies

IIOP Plumbing for the Net

- **A first class protocol - critical factors:**
  - **Firewalls and Proxy technology,**
  - **Browser/Java security,**
  - **Maintaining CORBA/IIOP interoperability.**
- **Not just the server-side firewall**
  - **client-side and multiple-enclave scenarios must also be taken into consideration.**

IONA Technologies

Firewall Navigation

- **Navigating the firewall**
  - **a fixed well-known port,**
  - **proxy must understand and control IIOP traffic (fine-grained access control),**
  - **to serve and protect - requests routed on to back-end server,**
- **Basic access control for IIOP traffic.**

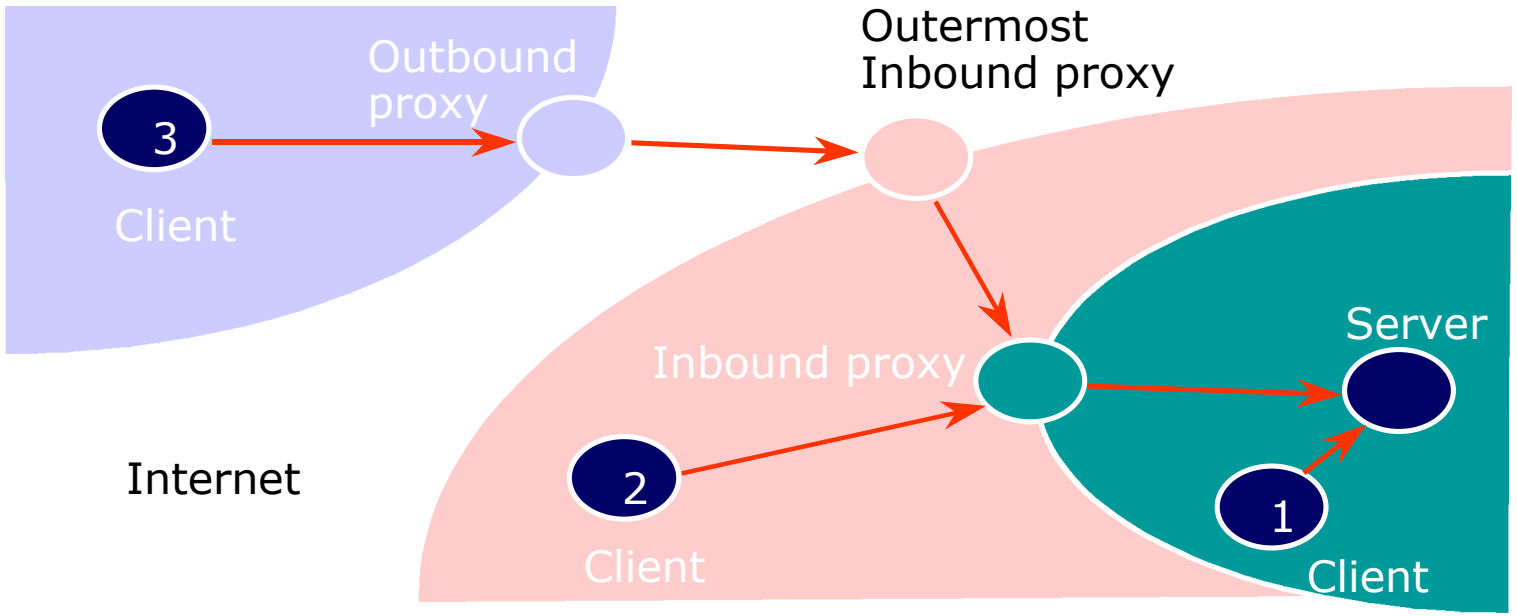
IONA Technologies

Architecture

- Firewall vs. Application-level Proxy.
- WWW-browser sandbox must be taken into account.
- Impact on firewall configuration
  - analogous to HTTP model,
  - dedicated IIOP port must be opened and proxy must be accessible to external IIOP traffic.

IONA Technologies

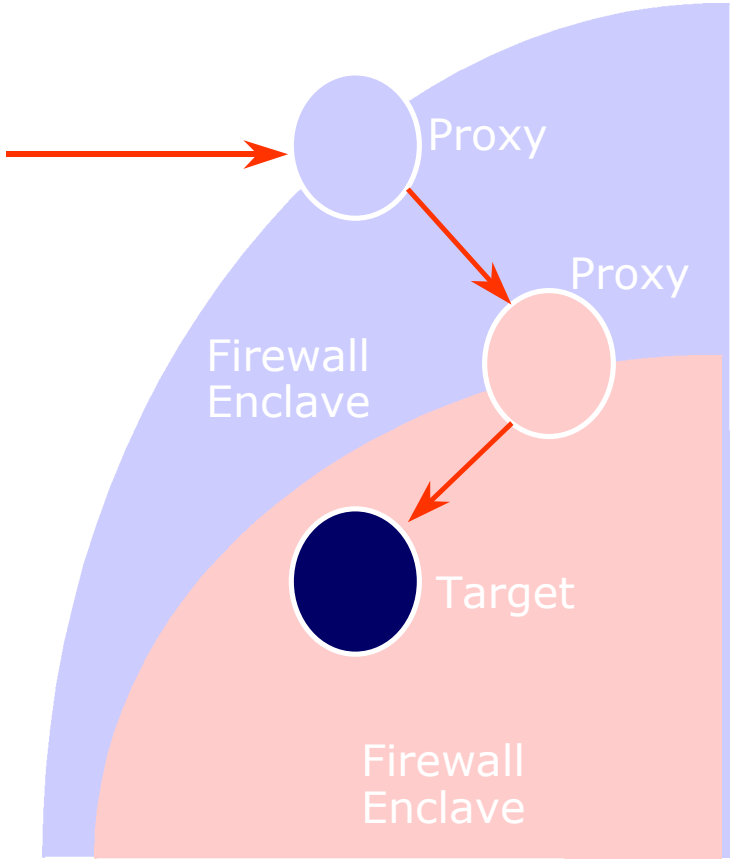
Some terminology ...



- **IIOP (GIOP) Proxy**
- **Outbound & Inbound**
- Enclaves
- Proxified IORs

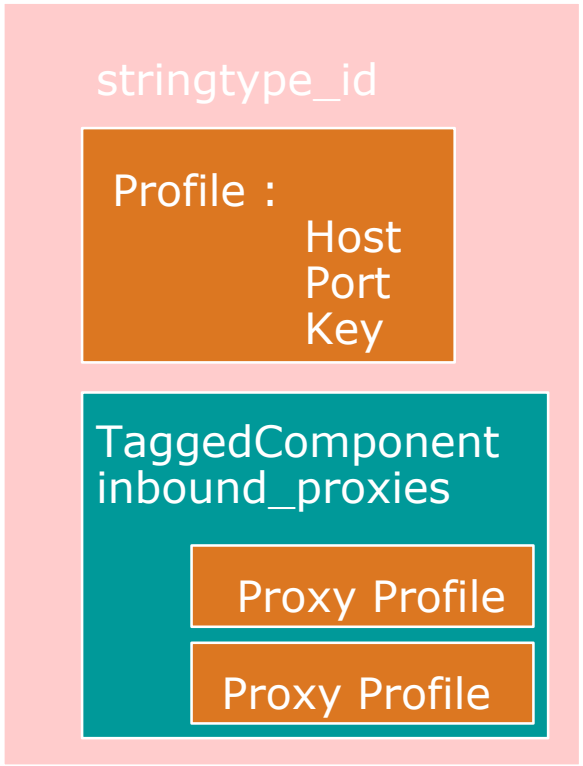
The IIOP Proxy

- Client and Proxies now require additional routing information.
- This routing information is stored in IOR profiles
  - no need for separate extranet and intranet object references.



Firewall profiles in the IOR

- **Notion of proxified IOR.**
- **A Tagged Component contains the profiles of the *inbound* proxies to the target object**
  - **A sequence of profiles with at least the outermost inbound proxy.**



IONA Technologies

Using the proxified IOR

When a client receives an object reference there are three possible client scenarios:

1. **in the same enclave as the target object,**
2. **within the outermost inbound proxy,**
3. **outside the outermost inbound proxy**

IONA Technologies

Talking to Proxies

- **Communication uses std IDL interface on the GIOP Proxy (`connect_to_object`)**
- **This is invoked on the proxy which navigates through any other proxies to establish a connection to the target server.**
  - **At any point an exception can be thrown e.g. `NO_PERMISSION` if access is to be denied.**

IONA Technologies

OrbixWeb Configuration

- **Server-Side BOA requires**
  - **Inbound GIOP proxy information.**
- **OrbixWeb 3.1/Wonderwall 1.2**
  - **Single inbound proxy currently supported,**
  - **Transparent to developer,**
  - **Simple configuration (at deployment) via owconfig: `IT_IIOP_PROXY_HOST` and `_PORT`.**

IONA Technologies

Bi-directional GIOP

- **Bi-directional GIOP is proposed as an addition to the current callback model.**
  - **Pragmatic for handling today s client-side firewalls,**
  - **Lower overhead for callbacks,**
- **Applies primarily to Internet traffic where there are plenty of firewalls and short lived CORBA applications e.g. Java applets.**

IONA Technologies

OrbixWeb Bi-directional IIOP

- **Request for bi-directional IIOP based on ServiceContext exported in IOR for callback object.**
- **Configured simply by switching on `IT_USE_BIDIR_IIOP` (at deployment) using owconfig.**
- **Bi-directional IIOP also supported by Wonderwall 1.2**

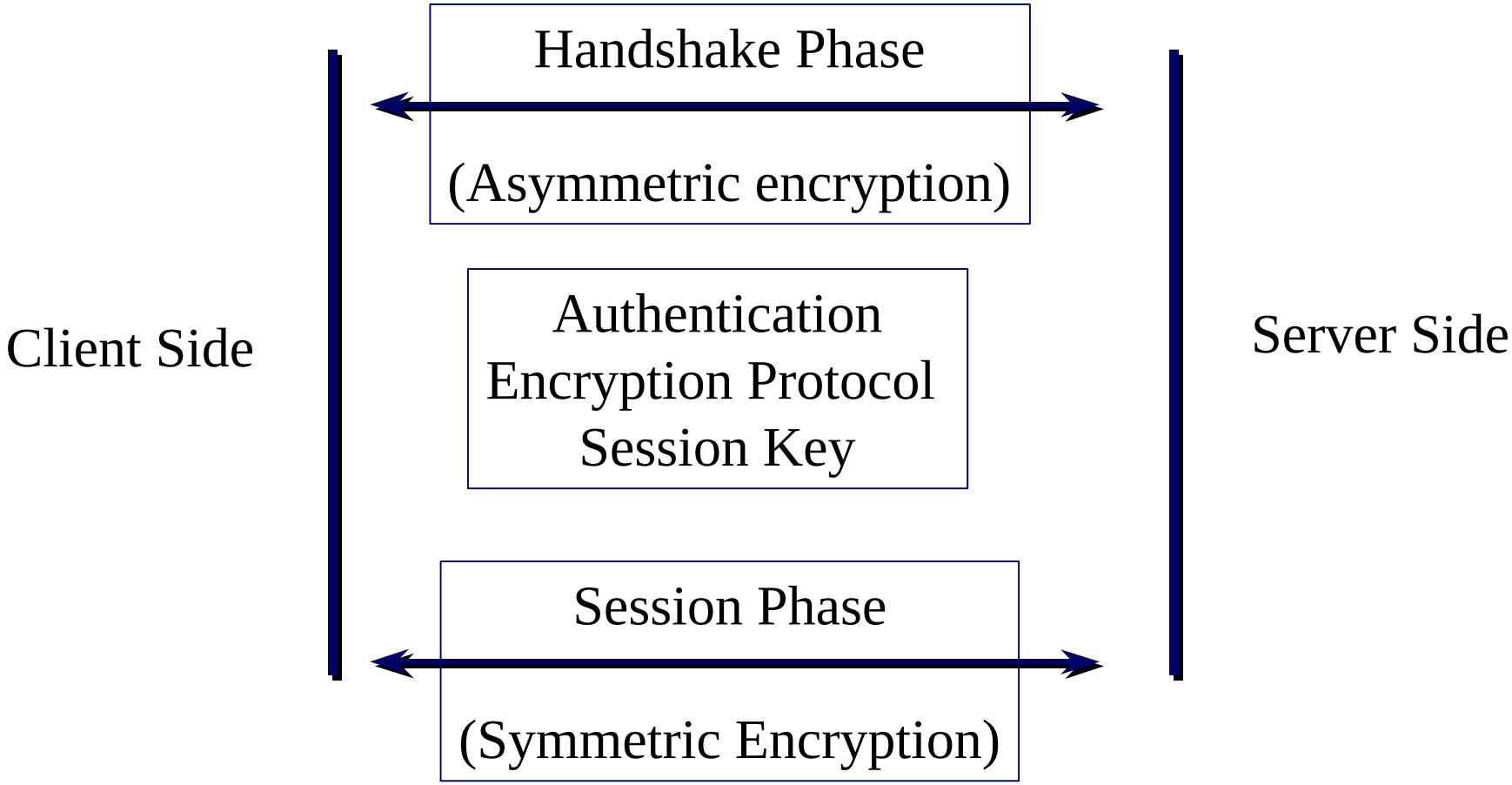
IONA Technologies

SSL Security

- IIOP across SSL V3.0 - de facto security solution for Internet CORBA.
- SSL - open Internet security protocol. Designed to provide connection security between applications
  - client/server authentication (X.509),
  - Message encryption (DES, 3DES, IDEA).
- Lightweight & tough security option.

IONA Technologies

An SSL Session



OrbixWeb + SSL

- **Minimal code changes required**
  - **can be added at the end of the development cycle,**
  - **simple to configure at deployment via OrbixWeb configuration utility (owconfig).**
- **SSL capability available as set of downloadable Java classes**
  - **sandbox implications for browser hosted clients.**

IONA Technologies

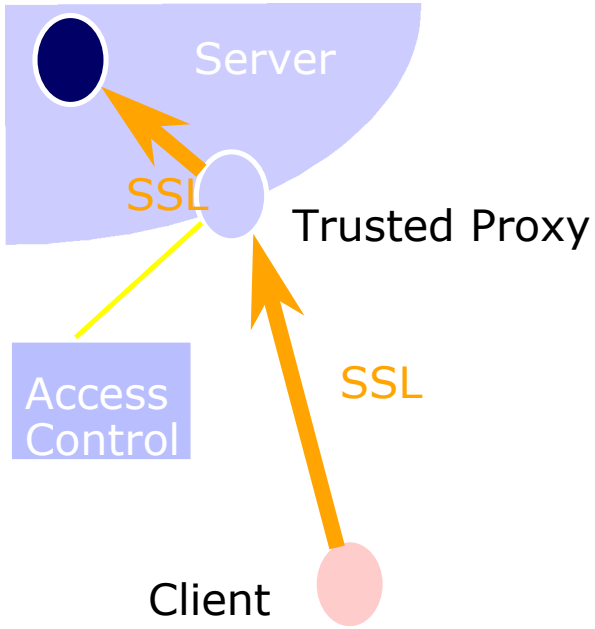
Best of both worlds

- Simple SSL approach based on opening dedicated firewall port.
- However ideal scenario would be same level of IIOP access control available even though using SSL transport.
- Therefore need to introduce notion of trusted and untrusted SSL-aware IIOP proxies.

IONA Technologies

Trusted proxies

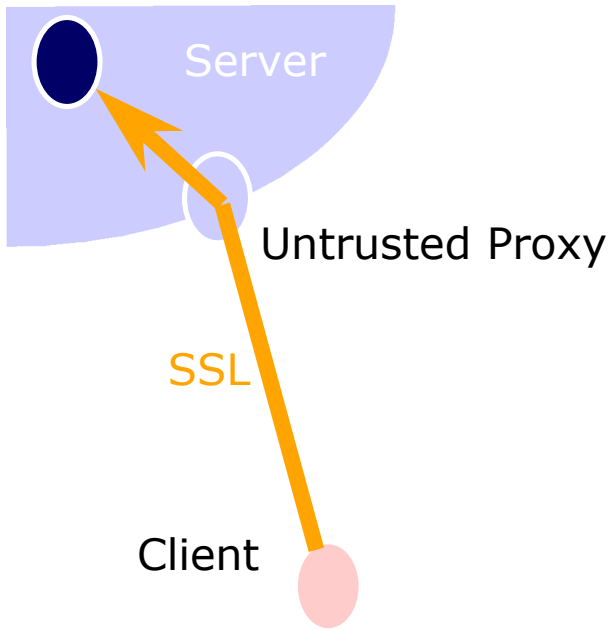
- Decrypts traffic and applies access control.
- Passes client identity to target on it s behalf.
- Can view data unencrypted.
- Maintains a separate connection with the target.



IONA Technologies

Untrusted proxies

- **Tunnels SSL connection.**
  - **Cannot view encrypted traffic.**
- **Access control can be applied at connection time only.**
- **Client and server authenticate directly.**



IONA Technologies

Trusted and Untrusted Proxies

- **Trusted proxies belong to a trust group specified by the server**
  - **Inbound proxies would normally be part of a trust group.**
- **Trusted proxies can also support the tunneled SSL method.**
- **Untrusted proxies are typically outbound proxies of which the server has no knowledge.**

IONA Technologies

OMG Standardisation

- **Revised submissions for CORBA/Firewall Security - orbos/98-07-03**
  - **IIOP Proxy mechanism,**
  - **SSL as an alternative transport,**
  - **Bi-directional GIOP.**
- **Joint submission based on Wonderwall**
  - **IONA, IBM, Oracle, Sun, Netscape, ...**
- **RFP Adopted - Sept. 25th., 1998**

IONA Technologies

Tunneling

- **Pragmatic interim solution for the client-side firewall - outbound TCP/IP capability may not be available.**
- **Auto-selected by OrbixWeb runtime - details can be configured (at deployment) using owconfig.**
- **Full IIOP access control retained by WWall**
- **No modifications to FW HTTP config.**

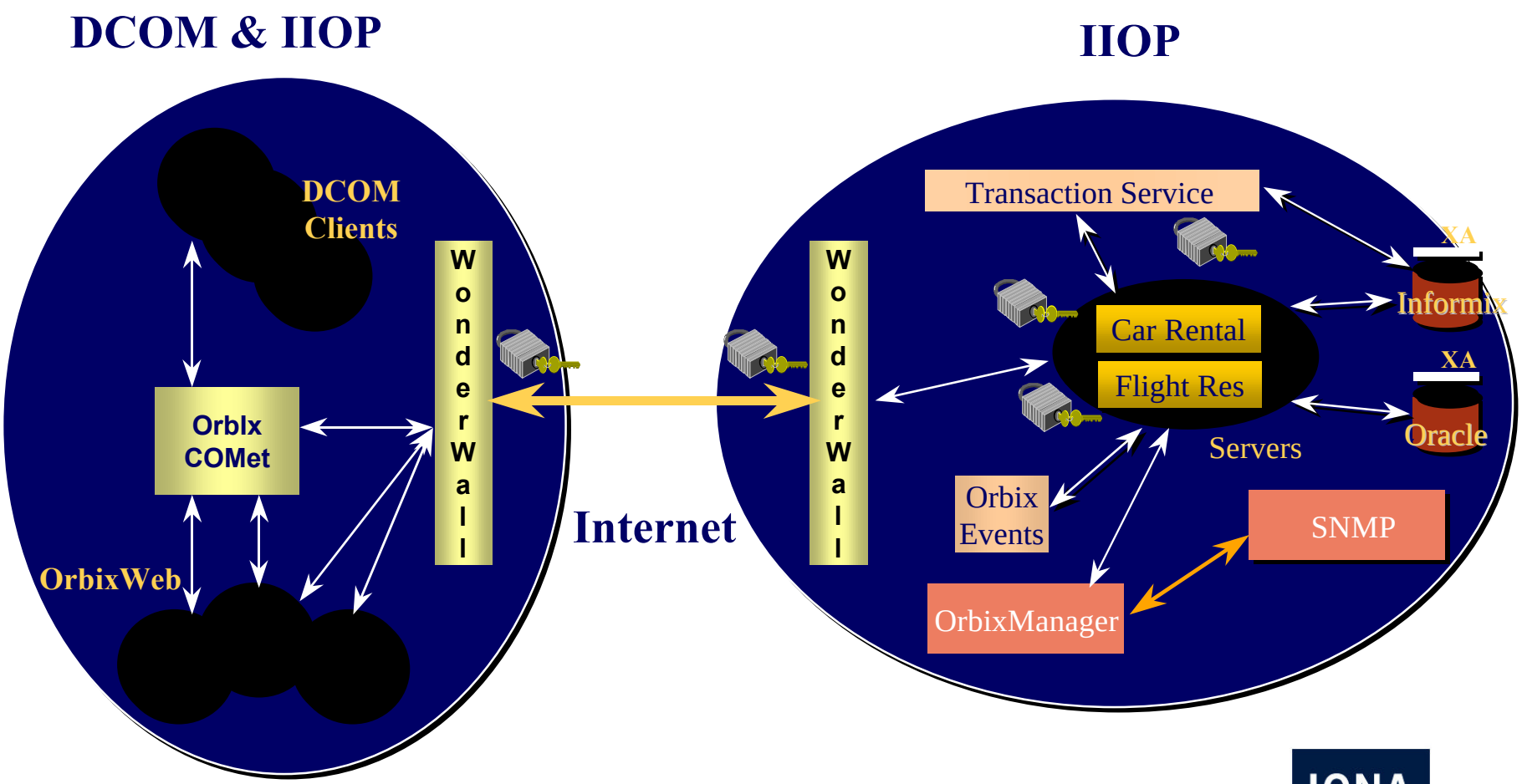
IONA Technologies

The infrastructure is there ...

- **OrbixWeb3**
  - **Internet-aware (Proxy navigation, bi-directional GIOP, Tunneling support).**
- **Wonderwall 1.2**
- **Full IIOP Access control, WWW-server capability to facilitate tunneling.**
- **OrbixSSL**
  - **Java SSL V3.0 capability.**

IONA Technologies

Making Software Work Together



OrbixWeb Futures

- **OrbixWeb is the Java front-end for the Internet Application Server - OrbixOTM**
  - **Java transactional client and server capability,**
  - **Java deployment support via OrbixMgr.**
- **Wonderwall**
  - **Reference implementation for the IIOP firewall proxy.**
  - **Upgraded to provide SSL transport capability.**

IONA Technologies

Questions ?

boreilly@iona.com

IONA Technologies