IONA Security Platform

February 22, 2002

Igor Balabine, PhD

IONA Security Architect

Agenda

- IONA Security Platform (iSP) architecture
- Integrating with Enterprise security services and administration
- iSP adapter internals
- Protecting Web Services
- Q&A

iSP Architecture

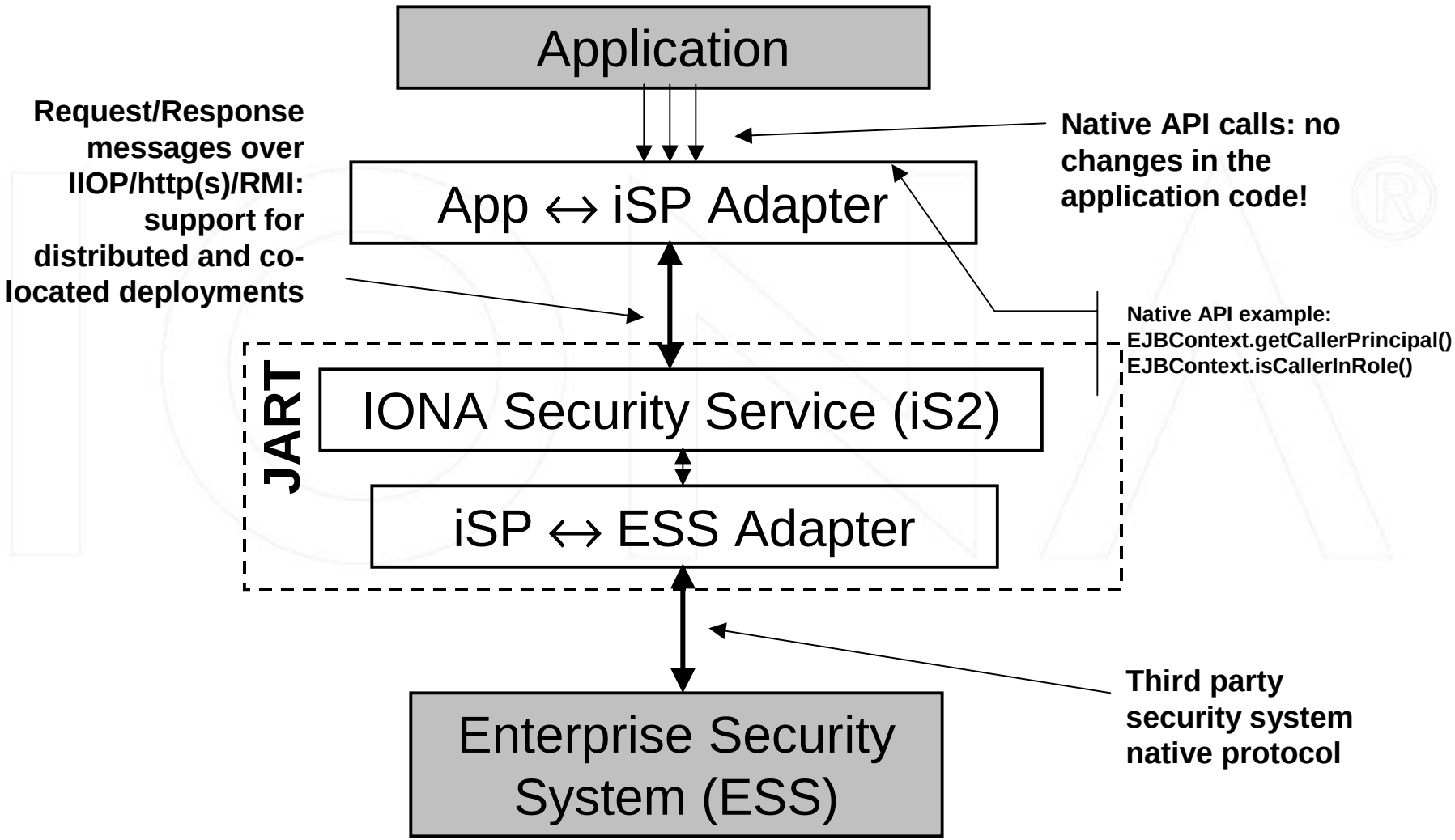
Why A Security Platform?

IONA Security Platform (iSP):

- allows to insulate applications from the diverse and changing enterprise security infrastructures.
- provides a uniform standards based approach to communicating security related requests across the enterprise.
- provides applications a single access point to multiple security services such as authentication, authorization and PKI.

iSP binds IONA products with any enterprise security infrastructure via development of a custom adapter!

iSP Architecture



IONA Security Service (iS2)

IONA Security Service (iS2):

- Is a servlet running in JART or in any standard application server.
- Uses a very simple flow:
  - receives a request message
  - determines the request type from the message content
  - loads an appropriate protocol specific module (if the module is not loaded yet)
  - dispatches message content to protocol specific module.
- In short: iS2 is a scaleable (intelligent) dispatcher!

iS2 is iSP's focal point but not a bottleneck!

Integration With Enterprise Security Services And Administration

AuthN and AuthZ Services

- Authentication and authorization services are supported via iS2 adapters.
- Internal protocol: SAML – satisfies purposes and allows extensibility. Could be easily replaced if necessary: internal interface is generic.
- Supported authorization models: coarse grain – RBAC (J2EE, Web Services), fine grain – DAC (CORBASEC, B2Bi).

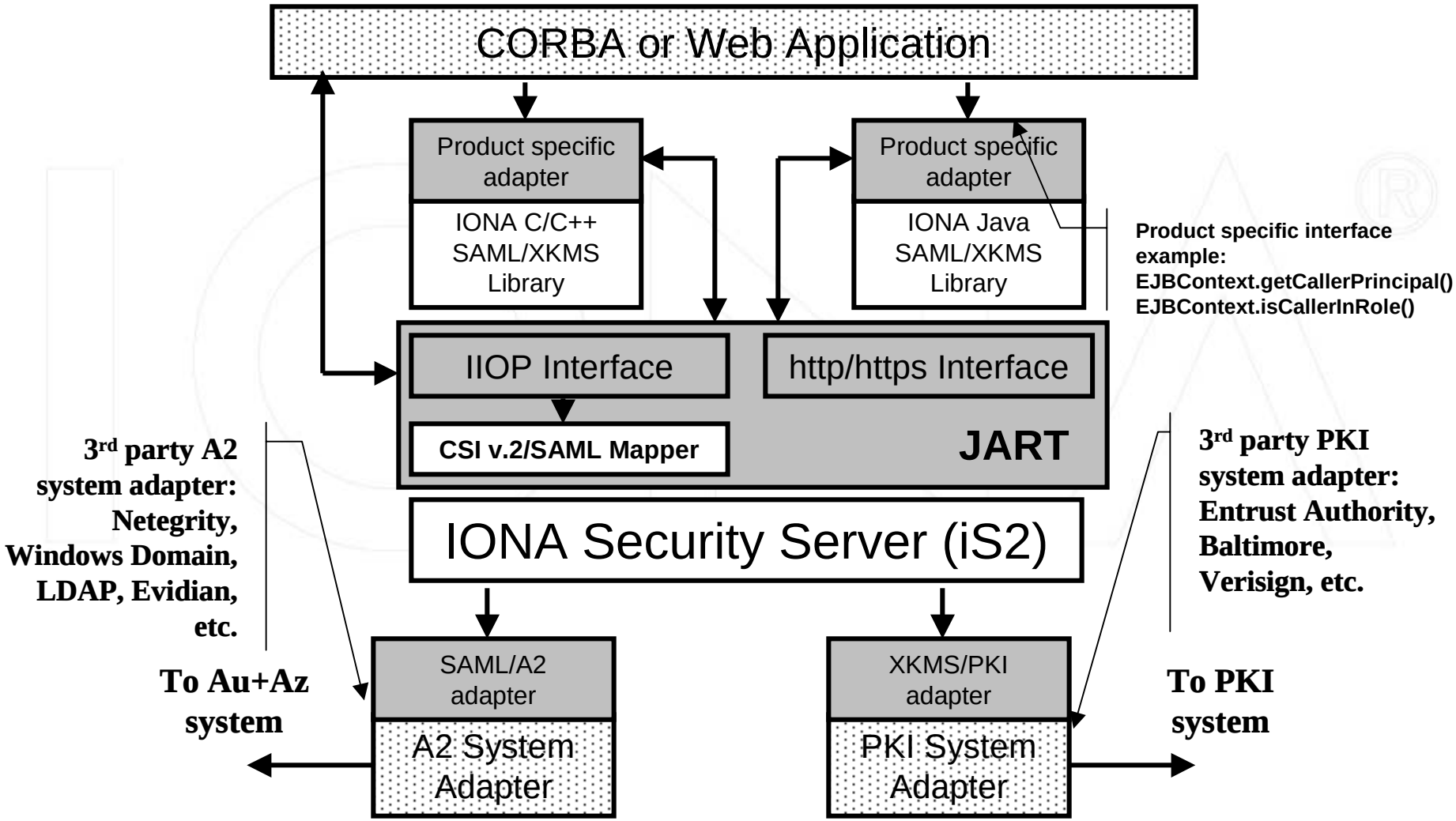
SAML protocol allows communicating arbitrary security assertions between applications and iS2!

PKI Services

- PKI services are supported via iS2 adapters.
- Internal language: XKMS – powerful and extensible. Endorsed by industry leaders (Verisign, Entrust, MSFT).
- Initial use: integration with certificate stores.
- Advanced use: validation services.

Many PKI vendors are expected to adopt XKMS: iS2 PKI adapter becomes a pass through!

iSP At Work



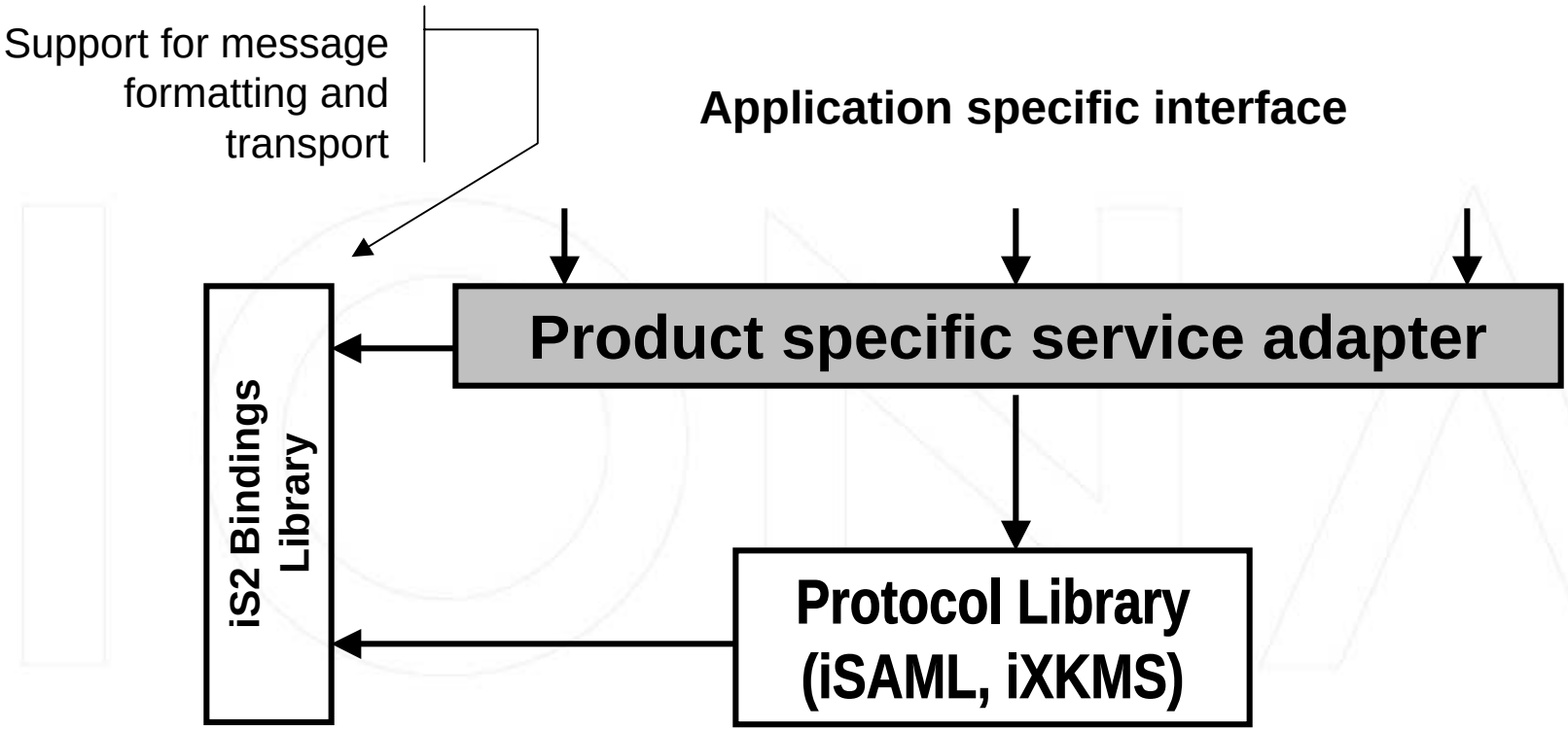
iSP Administration

- Solutions integrated with 3rd party systems are managed using native administrative tools, e.g. SiteMinder console for an enterprise which uses Netegrity SiteMinder
- IONA applications use iSP authorization models (RBAC, DAC) class libraries to manage native authorization policies via IONA Administrator
- iSP Auditing Component provides logs in a standard format (syslog) easily consumable by event monitoring systems.

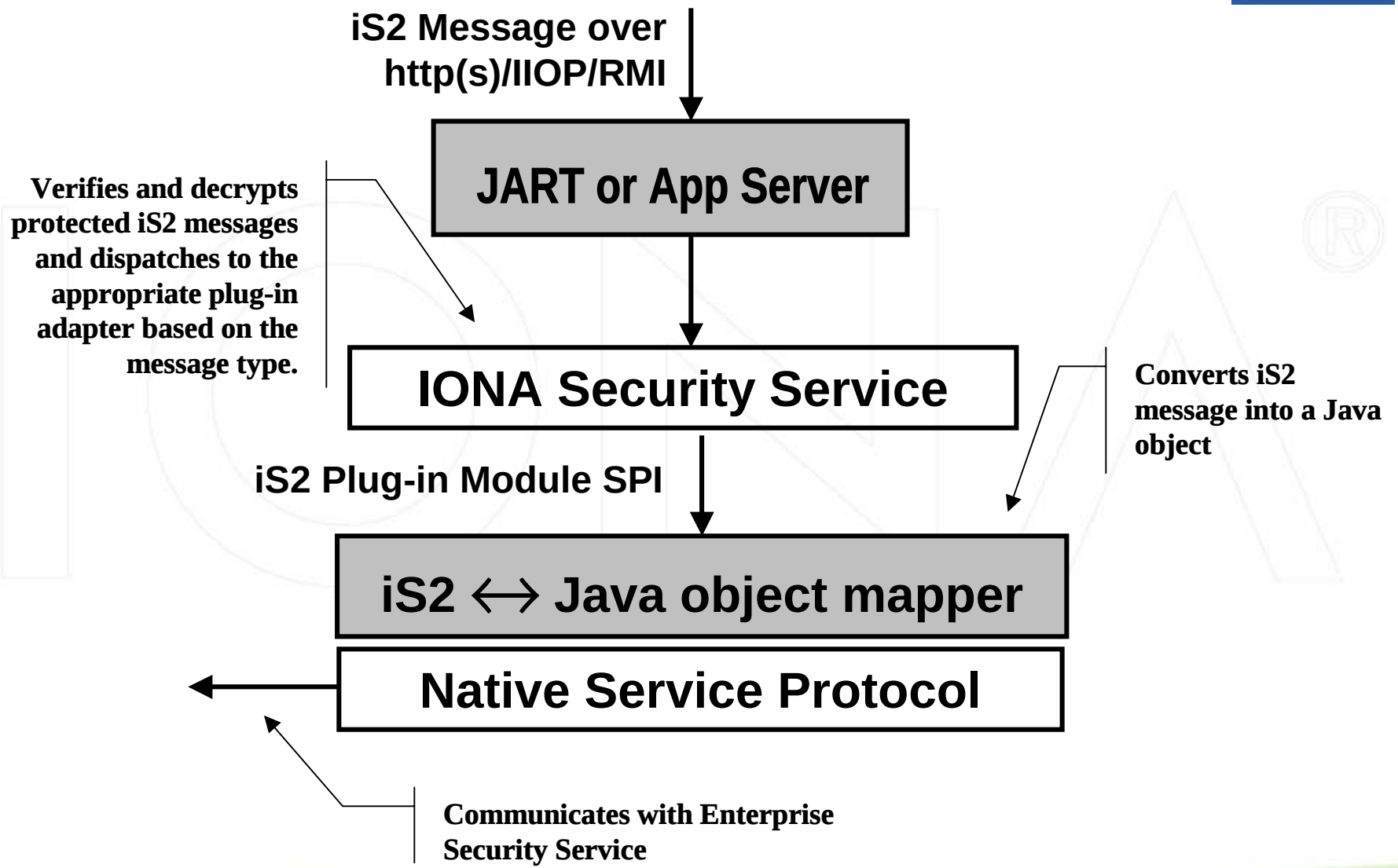
iSP offloads administrative tasks to 3rd party tools where possible and provides components to manage custom security information!

iSP Adapter internals

Application Adapter Architecture

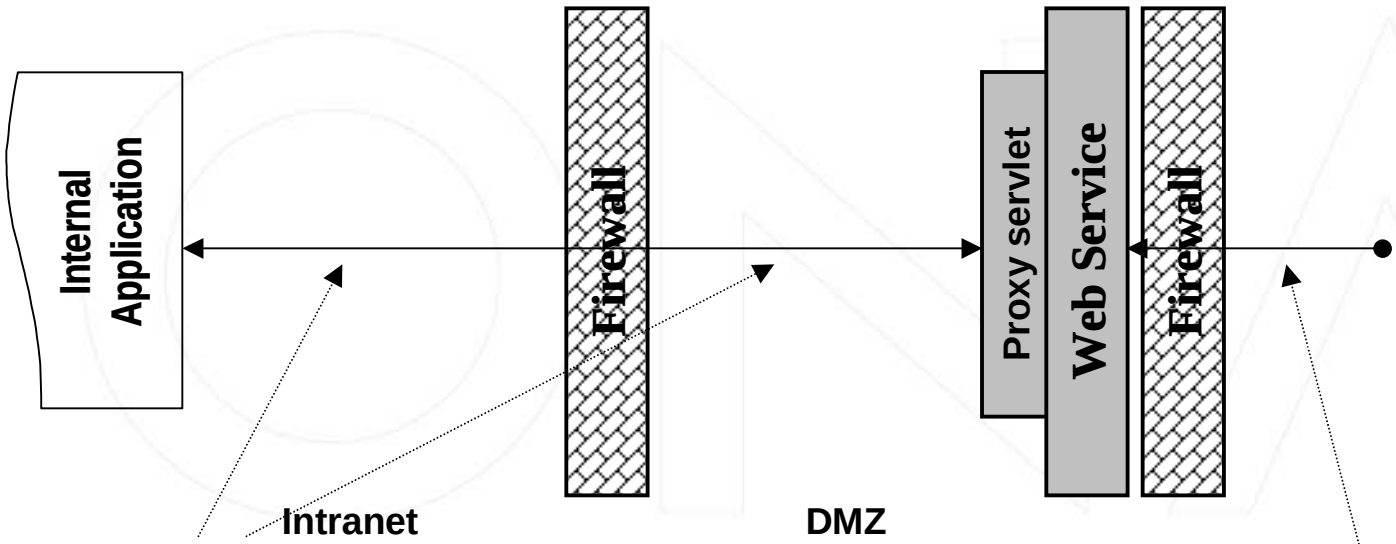


iS2 Plug-In Modules



Protecting Web Services

Typical “Secure” Deployment

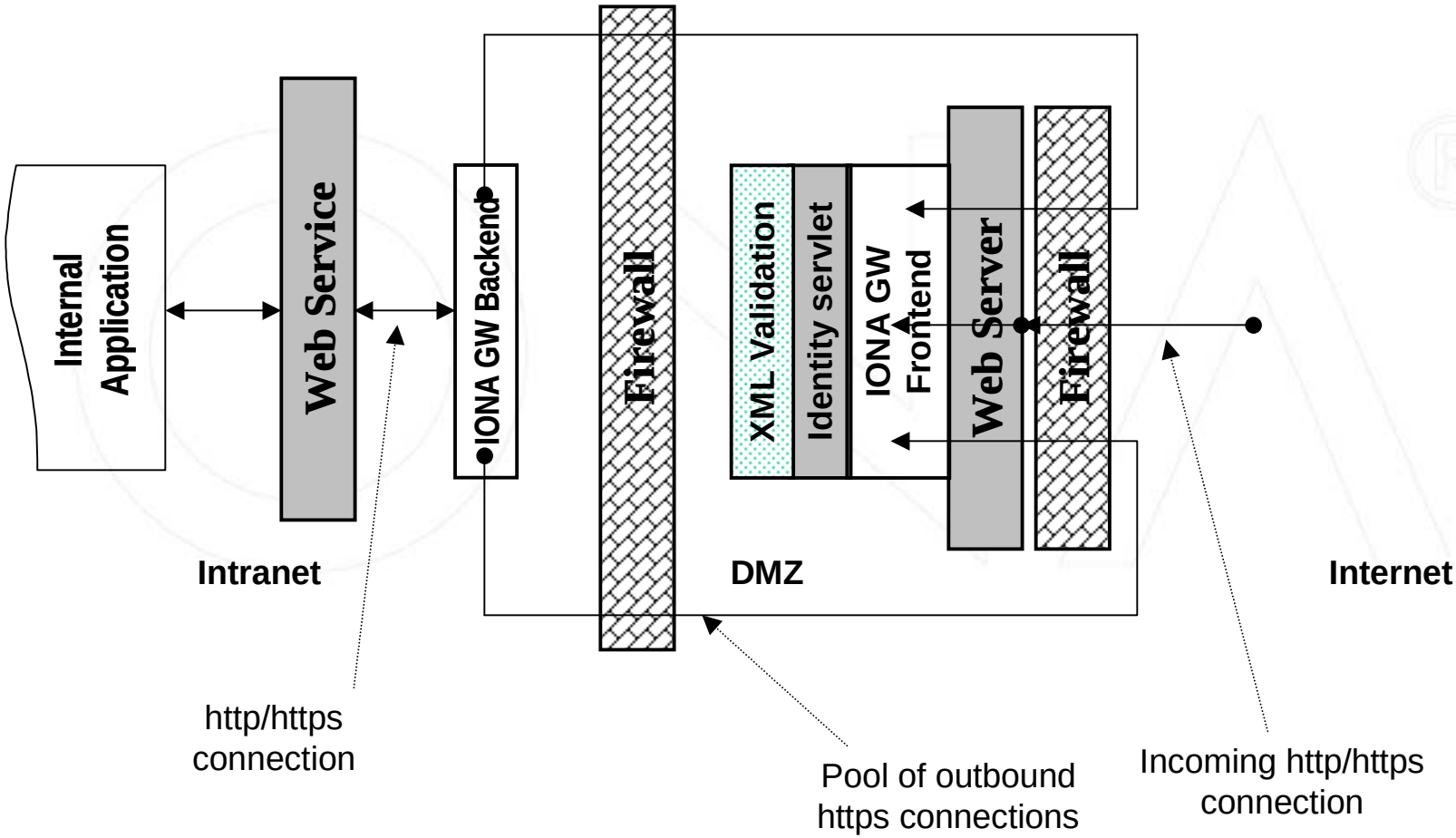


Problems With Traditional Deployment

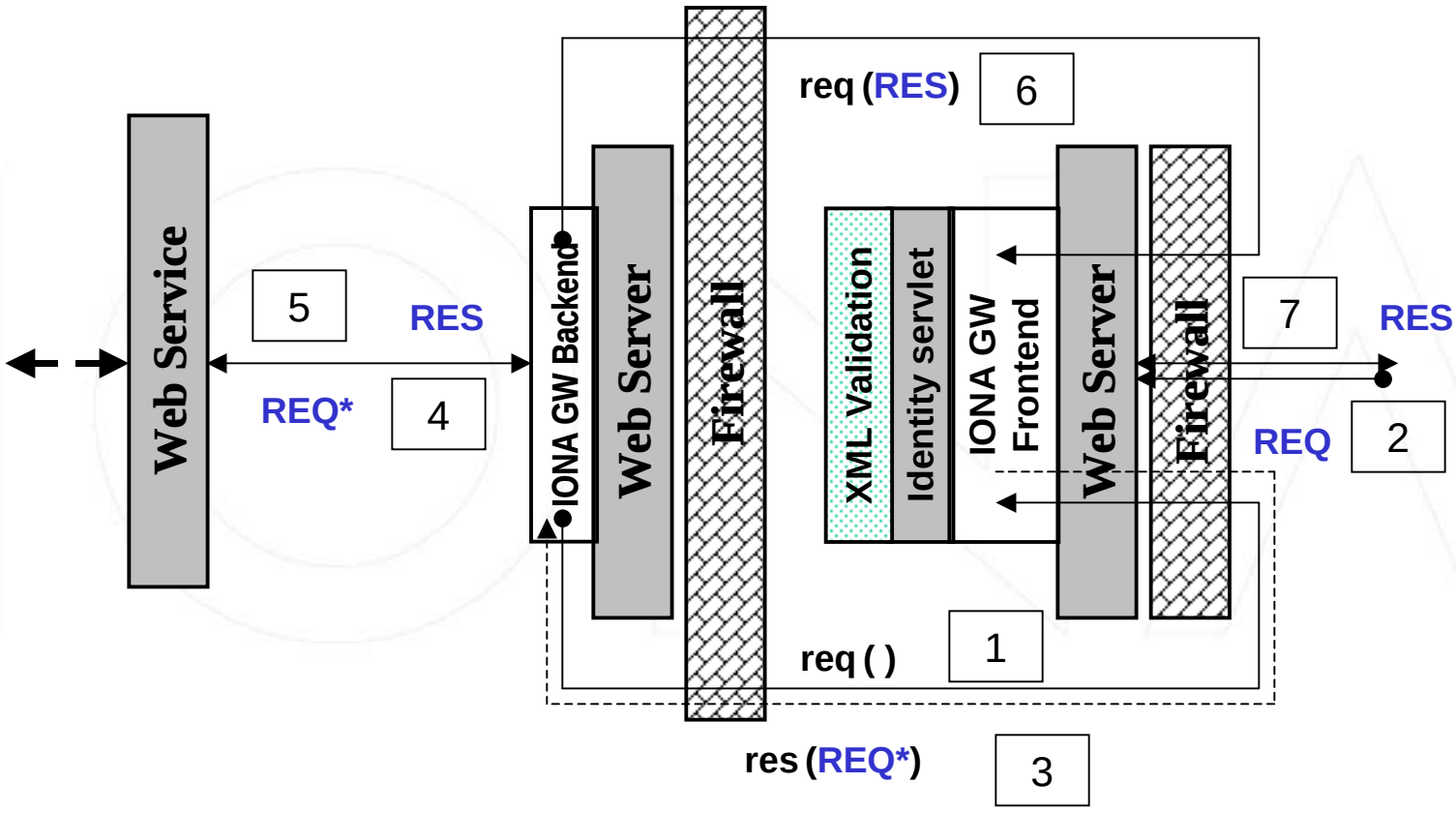
- Internal firewall has to be opened for secondary IIOP connections: nothing prevents the attacker from penetrating internal firewall using the secondary protocol!
- Same problem with SSH especially after discovery of a weakness in the SSH protocol (short byte sequences – e.g. key strokes - allow to recover session key).
- FTP client and server in the active mode open listening ports and require a hole in the firewall.
- FTP client and server in the passive mode suffer from the server side PASV exploits (“Pizza Thief”: rogue client connects to a newly opened port) and from port number substitution exploits by rogue servers (see **http://www.securiteam.com/exploits/5YP0E000HG.html**).

Traditional deployment exposes internal hosts to potentially hostile DMZ environment!

Deployment With IONA Secure Gateway (iSG)



iSG At Work



iSG Benefits

- The internal firewall is closed to all inbound traffic.
- HTTP headers of the inbound messages are parsed and filtered in the DMZ preventing buffer overflow attacks (e.g. CodeRed Worm, Nimda) on the Intranet machine running Web Service.
- Message headers and content could be scanned for viruses and attack signatures by virus and IDS plug-ins.
- Incoming messages on the DMZ machine are never written to the disk.

There are no inbound connections through the Internal firewall!

More iSG Benefits

- iSG scales linearly and could be deployed in n:m configuration.
- Computationally intensive SSL handshake is offloaded to machines in the DMZ.
- SSL connections between the Internal Gateway machine and machine in the DMZ could be authenticated using certificates issued by a private CA.

iSG offloads computationally intensive cryptographic computations from internal application servers!

Conclusion

- IONA Security Platform (iSP) provides applications a robust integration layer with Enterprise wide security services.
- iSP architecture is flexible and allows integration with diverse security solutions.
- iSP covers such important aspects of security as network protection, authentication, authorization and PKI services.

Q&A