IBM Software Group

Tivoli Access Manager for RACF Administrators

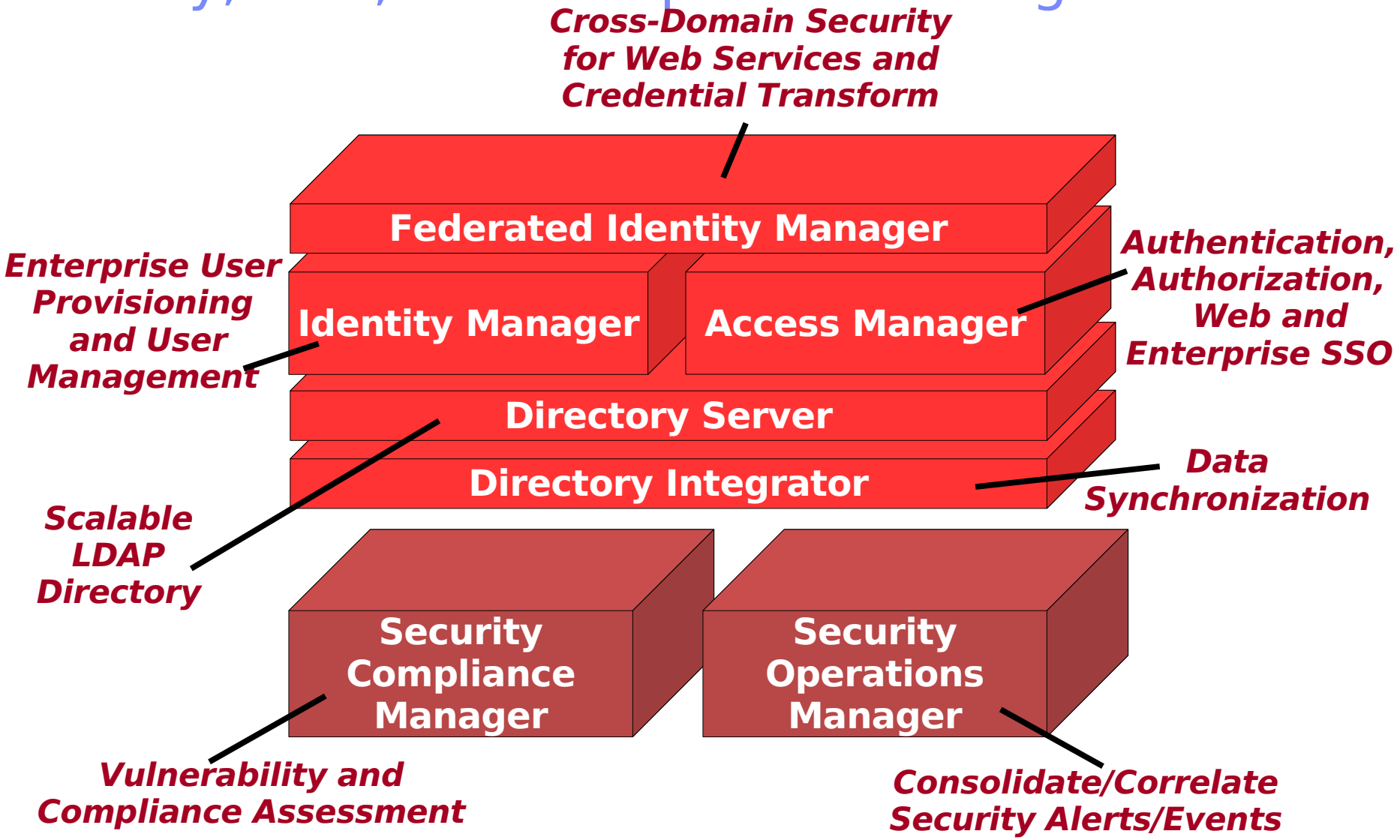
Session RTB14

Tim Hahn – IBM Tivoli Security

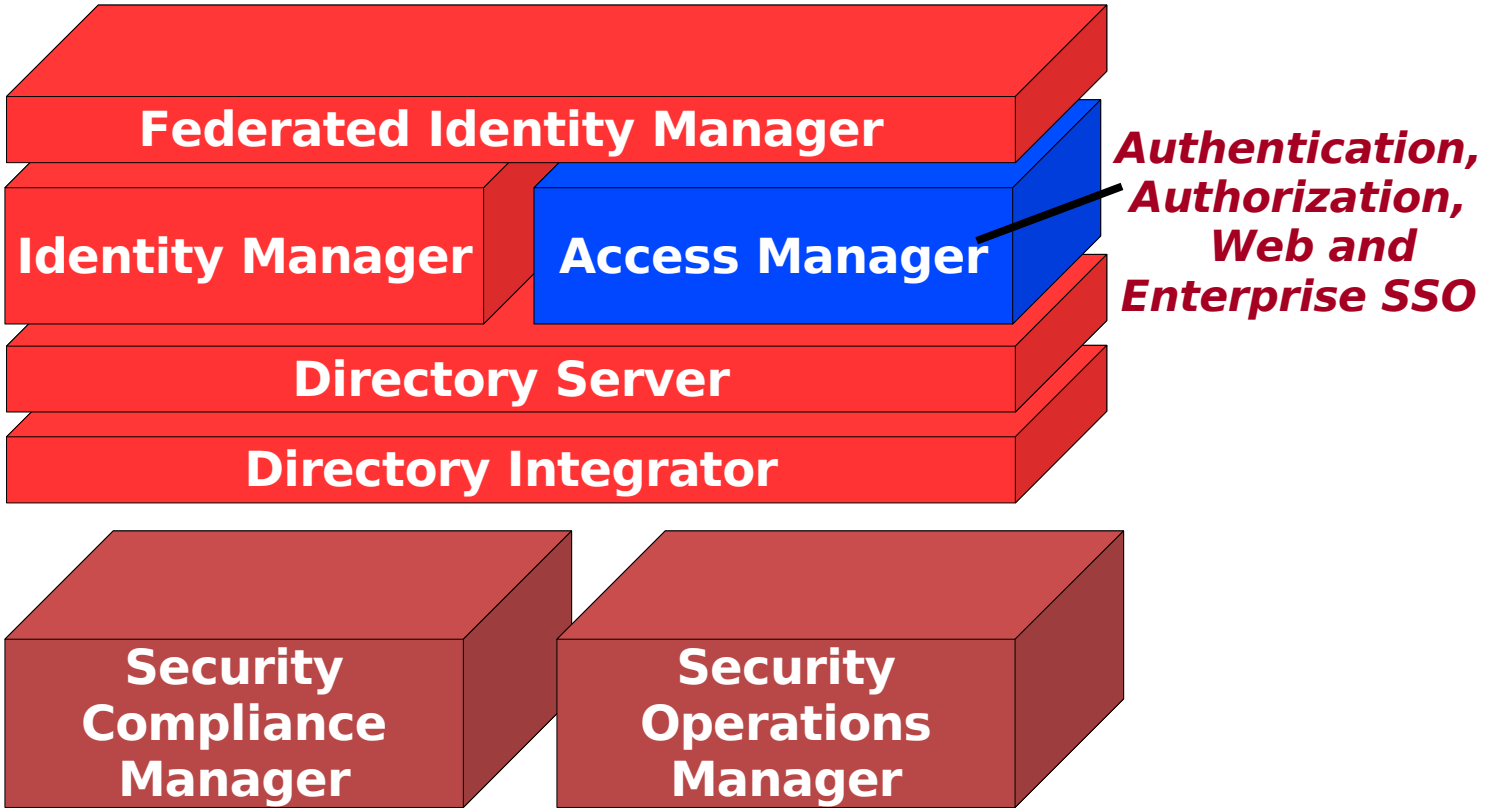
Tivoli. software

e business software

Identity, Risk, and Compliance Management



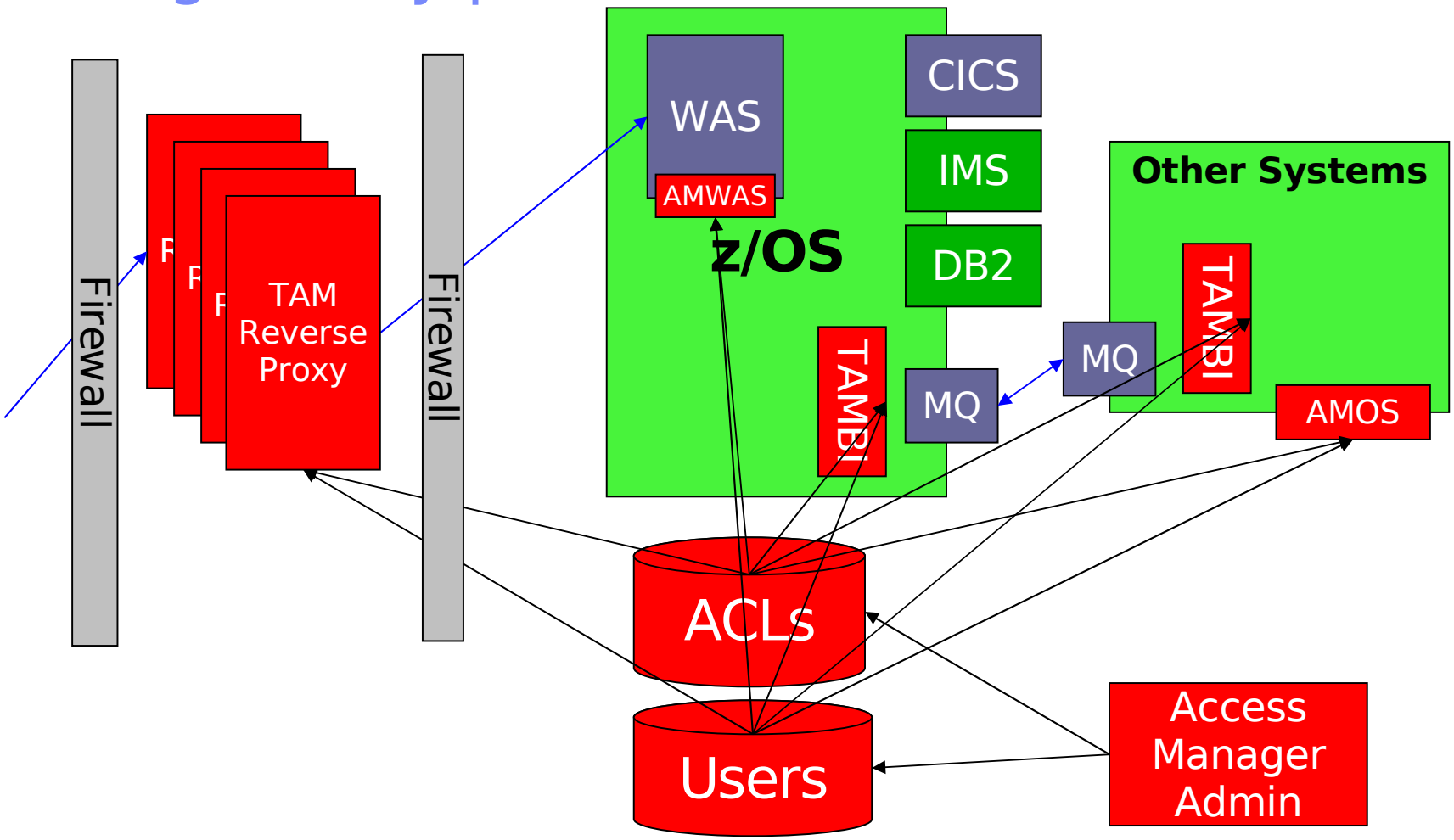
Tivoli Access Manager – Authentication and Access Control



TAM Family

- TAM for Business Integration
  - Protects access to read/write to MQSeries queues
  - Protects messages sent over MQSeries queues
- TAM for Operating Systems
  - Enhances the access control checks performed by a Linux or AIX operating system
- TAM for e-business
  - Authenticates users accessing information via HTTP (web).
  - Protects access to information based on URL
  - Supports single sign on to multiple web-accessible applications
  - Protects access to EJB methods
- TAM for Enterprise Single Sign On
  - Relieves the user from answering userid/password prompts for every application
  - Can be used to set up random passwords that user does not even see or need to remember

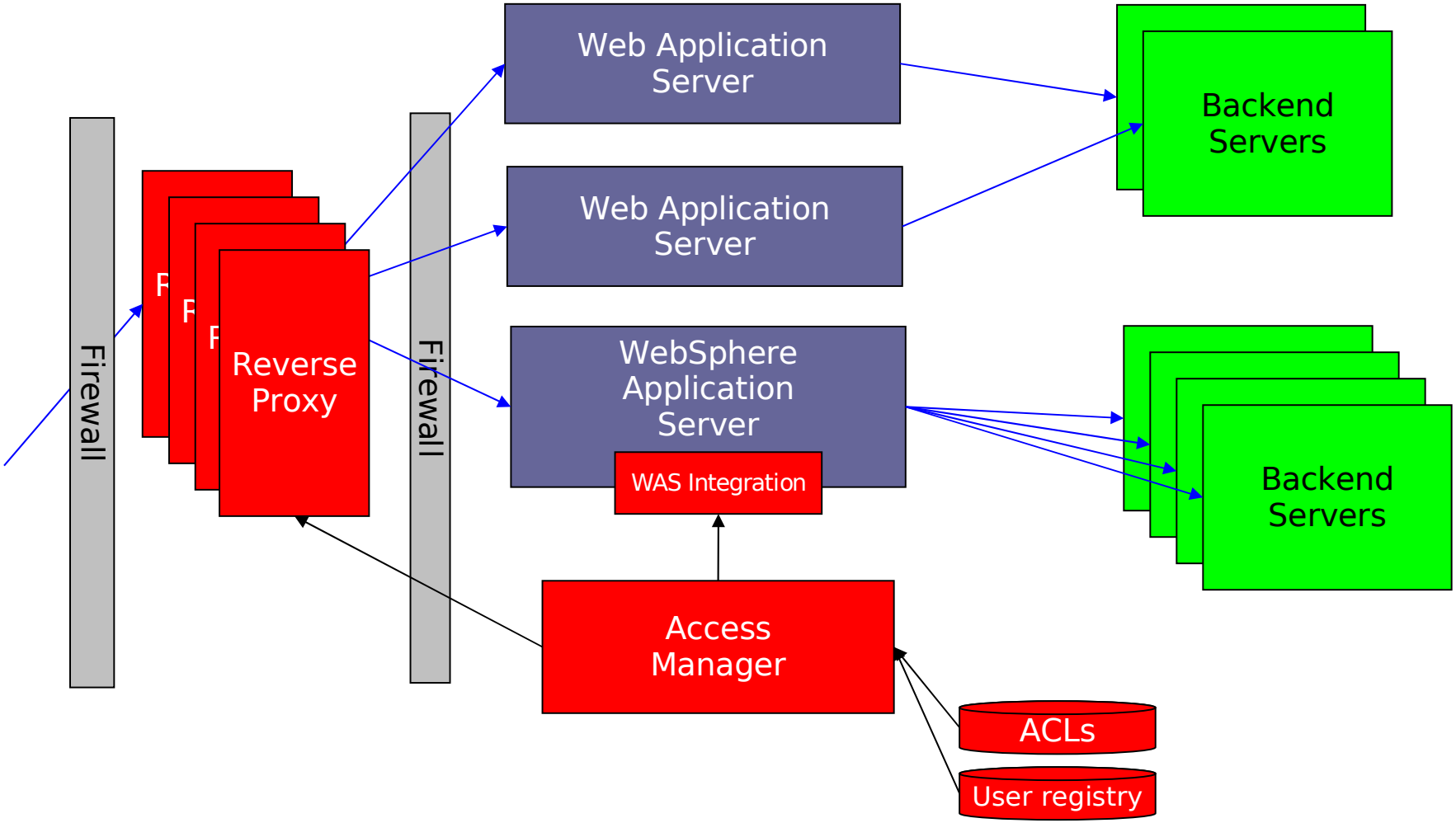
Tivoli Access Manager – Protects Access through many paths



TAM for e-business

- WebSEAL
  - Reverse proxy server that supports authentication, access control based on URL, and single sign on to multiple web-based applications
- WAS integration
  - Credential transfer to WAS, credential transform to WAS credential, EJB method protection
- TAM GSO lockbox
  - Used for web-based single sign on to multiple web-based applications
  - Used during credential translation when contacting legacy applications

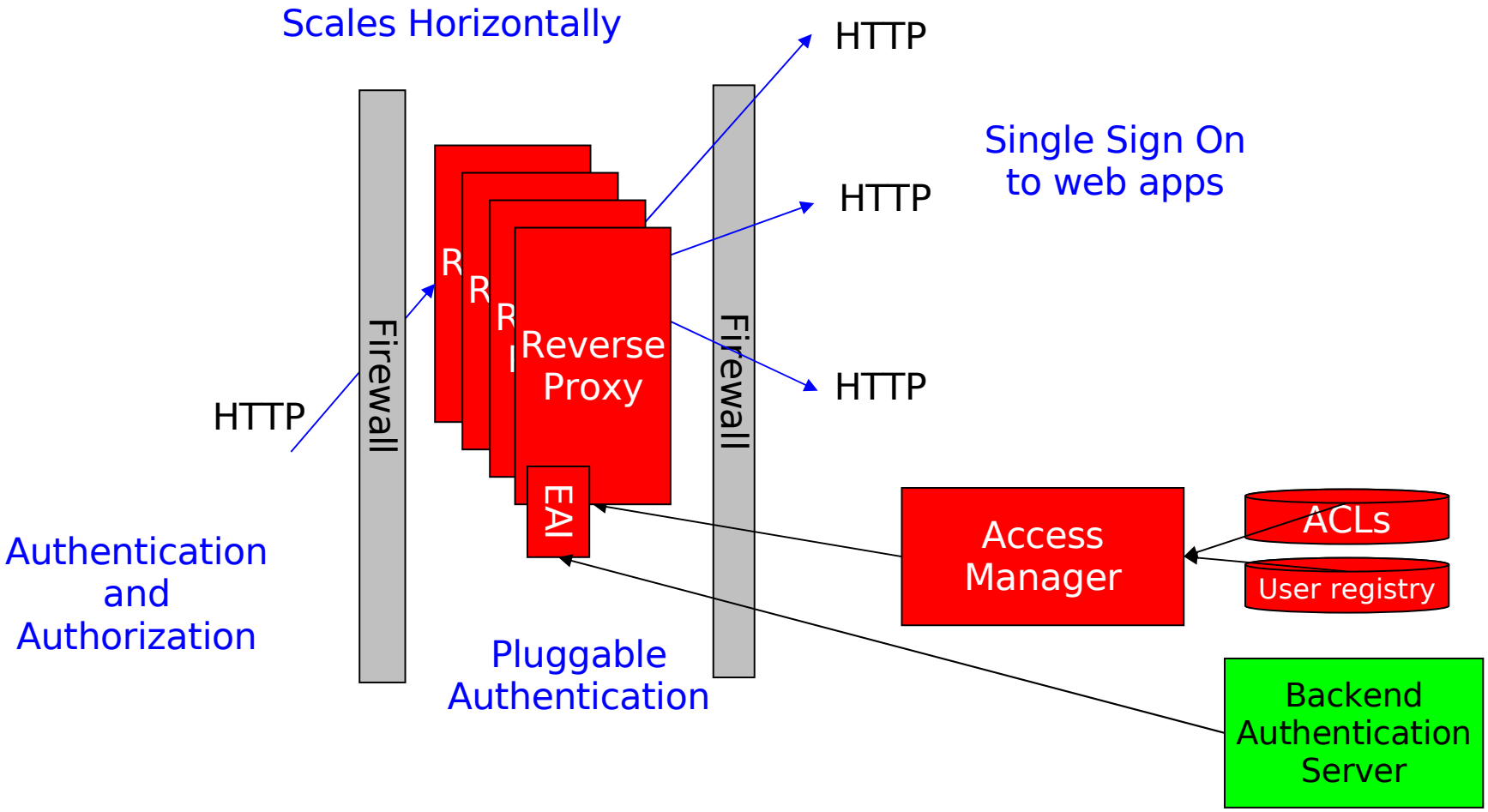
TAM for e-business



TAM for e-business Reverse Proxy

- HTTP Reverse proxy – a “point of contact”
- Handles authentication and authorization
- Scale horizontally
- Allows for different login mechanisms using External Authentication Interface (EAI)
- Supports “step up” authentication through Protected object Policies (PoPs)
- Available as a plug-in to several Web servers including WebSphere
- Single Sign On to multiple web applications

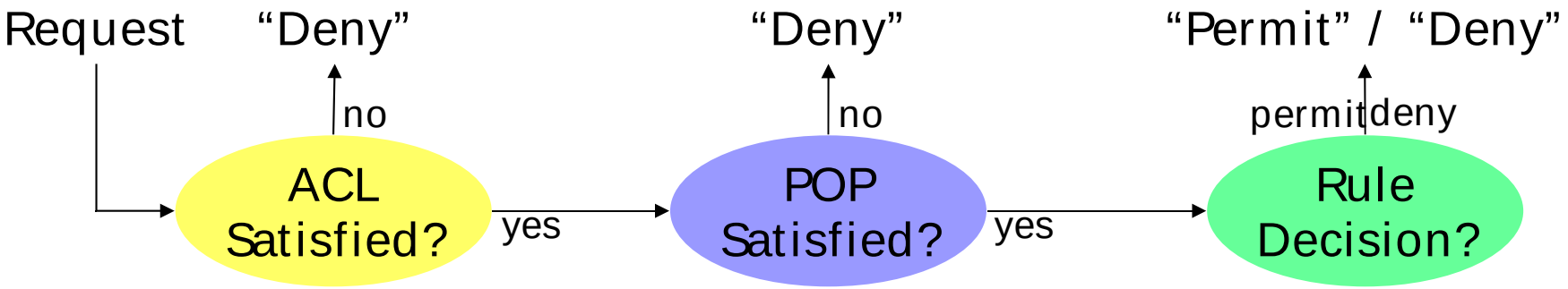
TAM for e-business Reverse Proxy

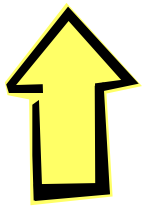


TAM Access Checking

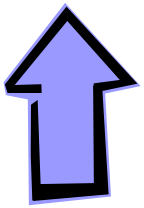
- Three pieces of information are used to perform the access check:
  - Access Control List (ACL)
  - Protected Object Policy (POP)
  - Rules Engine – additional rules created by the installation to further enhance the permission check

TAM ACL checking

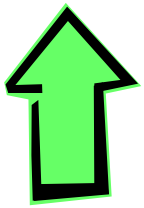




Access determined by user/ group permissions



Object access characteristics (e.g. audit, time- of- day or day- of- week)

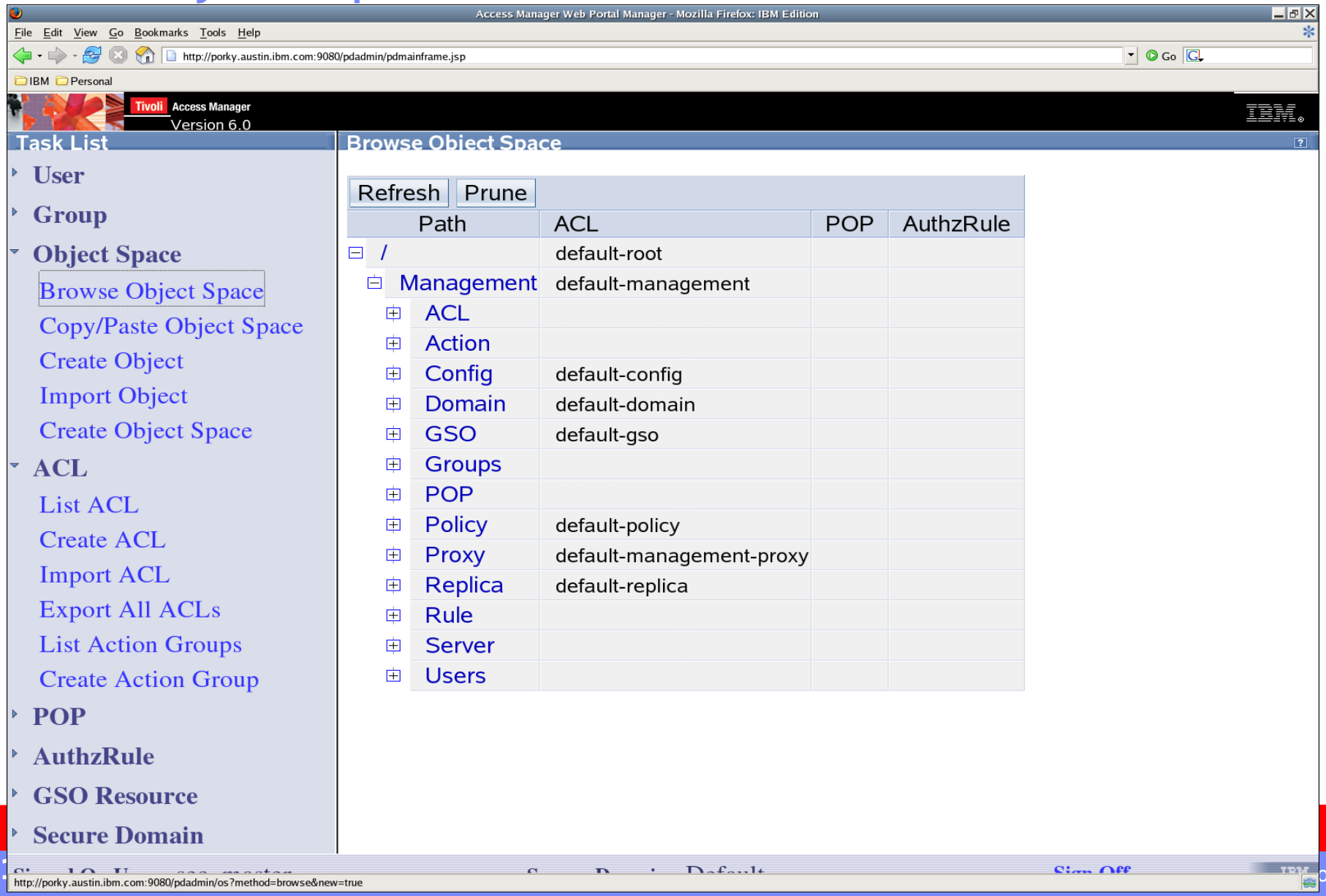


Access determined dynamically, based on current conditions

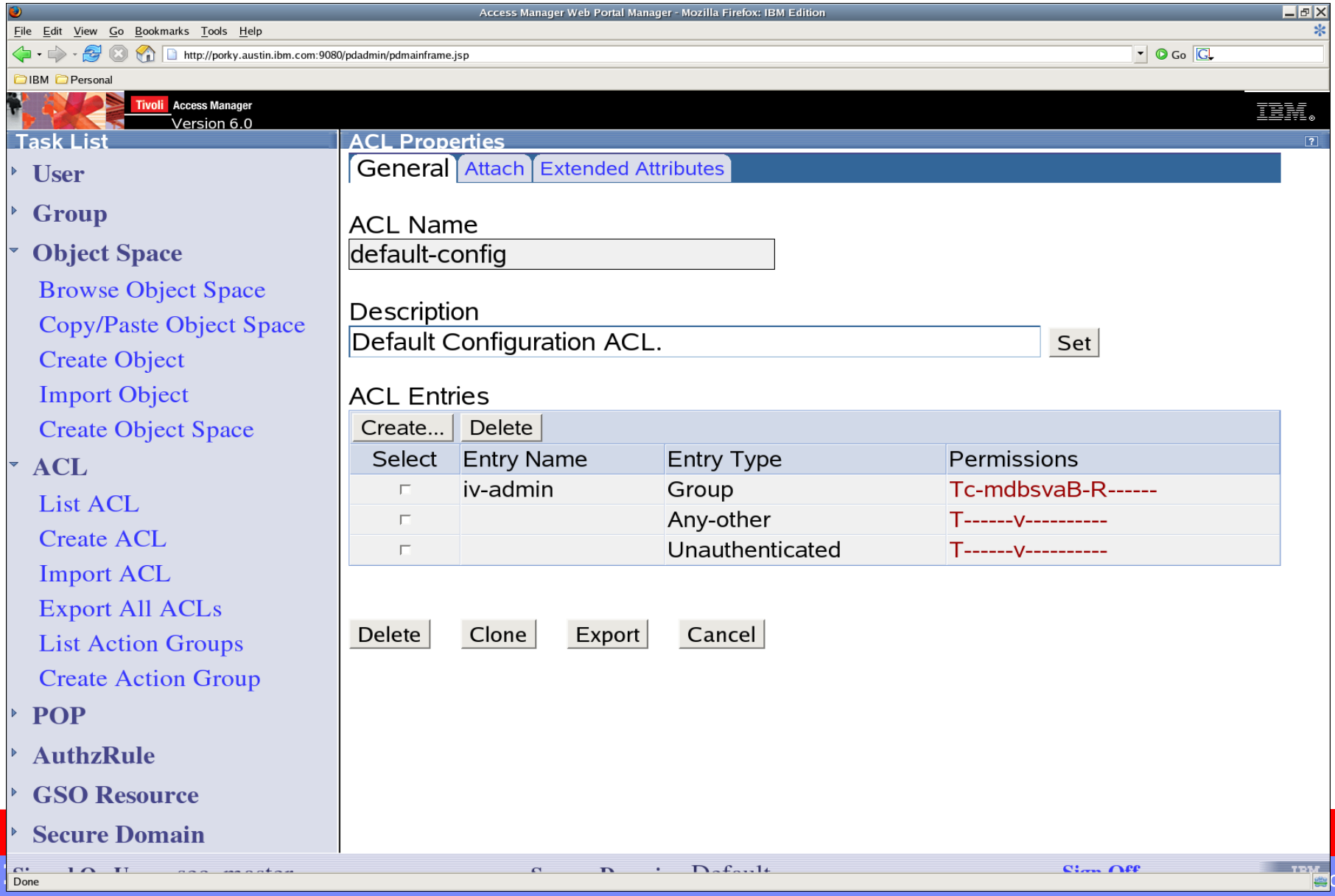
TAM ACLs

- Hierarchical namespace
- Many permissions can be used
- Associated with users or groups (preferred)
- URLs for WebSEAL
- EJB Role names for WebSphere EJBs
- Extensible namespace allows for general usage in application-level access control checking

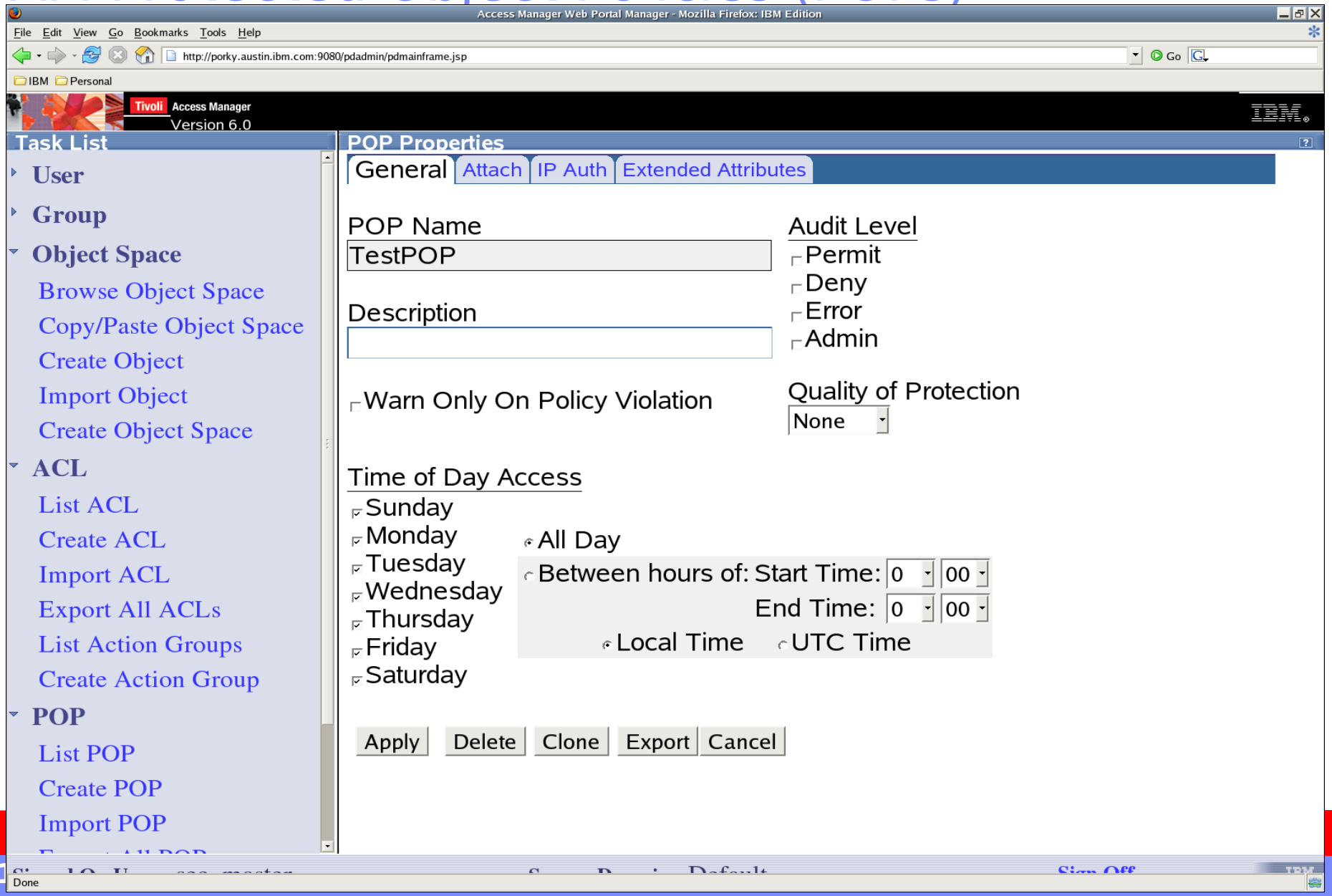
TAM Object Space



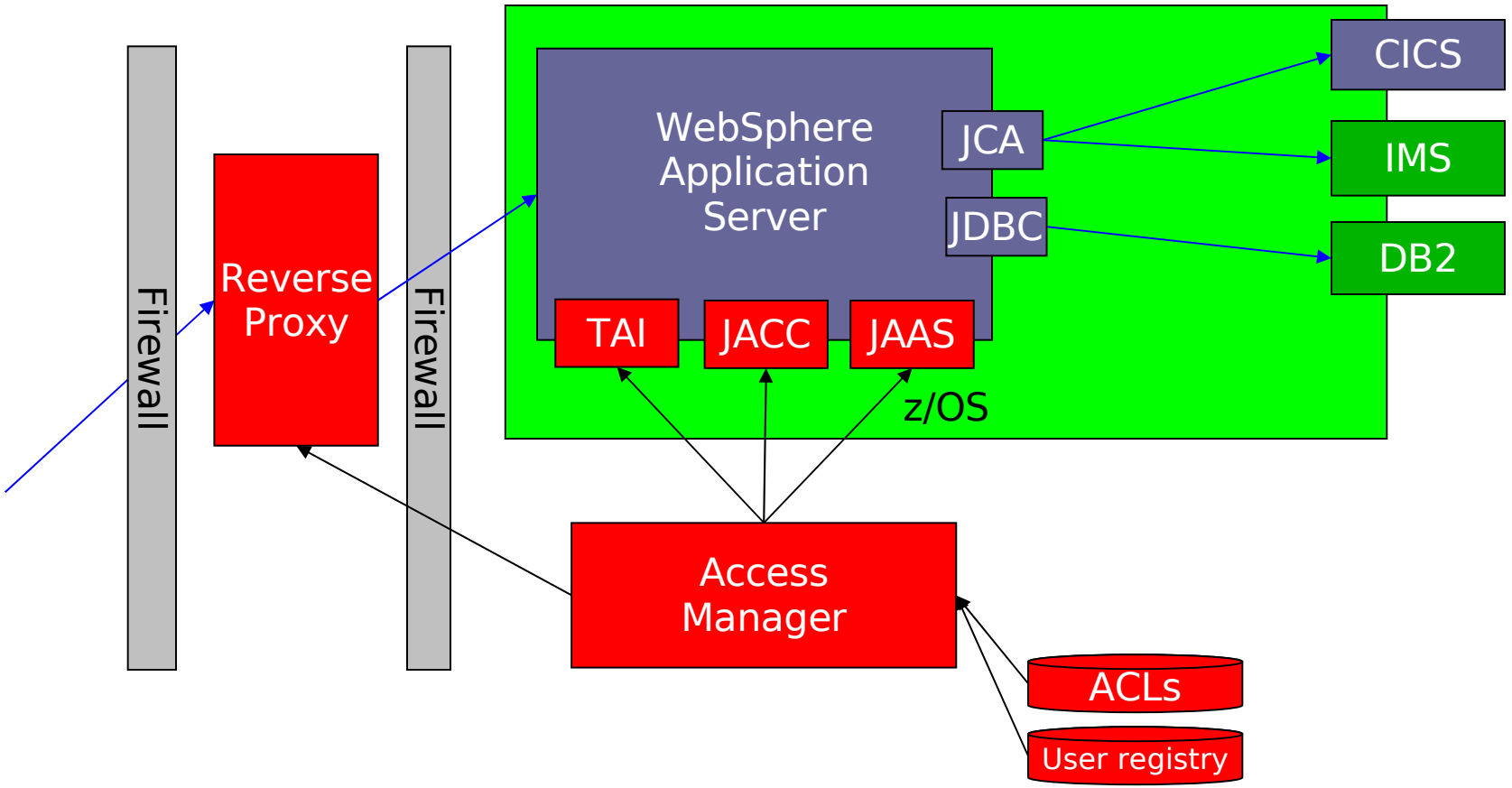
TAM ACLs


Access Manager Web Portal Manager - Mozilla Firefox: IBM Edition
File Edit View Go Bookmarks Tools Help
http://porky.austin.ibm.com:9080/pdadmin/pdmainframe.jsp
IBM Personal
Tivoli Access Manager
Version 6.0
Task List
User
Group
Object Space
Browse Object Space
Copy/Paste Object Space
Create Object
Import Object
Create Object Space
ACL
List ACL
Create ACL
Import ACL
Export All ACLs
List Action Groups
Create Action Group
POP
AuthzRule
GSO Resource
Secure Domain
ACL Properties
General
Attach
Extended Attributes
ACL Name
default-config
Description
Default Configuration ACL.
Set
ACL Entries
Create...
Delete
Select
Entry Name
Entry Type
Permissions
iv-admin
Group
Tc-mdbsvaB-R------
Any-other
T------v----------
Unauthenticated
T------v----------
Delete
Clone
Export
Cancel
Sign Off
Done

TAM Protected Object Policies (POPs)



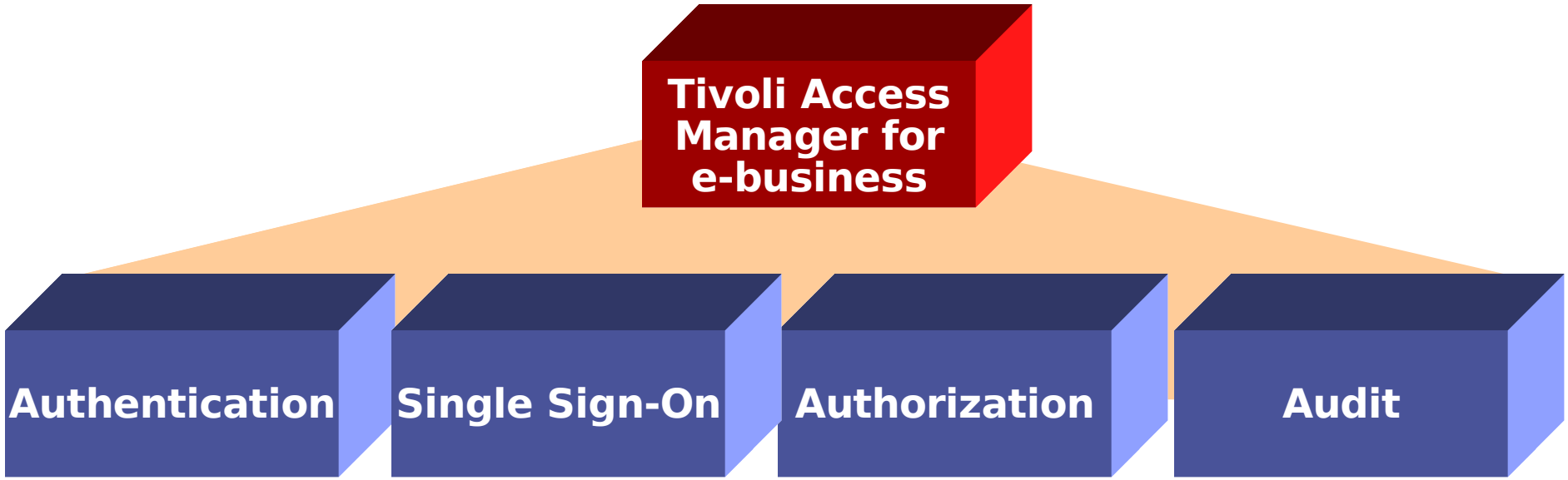
TAM and WebSphere Integration



TAM for e-business ACL Checking

- WebSEAL
  - Authenticate user
  - Verify user is allowed to access requested URL
  - If authorized, contact appropriate web server and re-drive HTTP request
- EJB Roles Support
  - Method permissions
    - Methods are mapped to EJB Roles in EJB deployment descriptor
    - Access is granted to EJB Role in TAM protected object space
    - If user has access to the role, the user is “in the role” and thus granted access to invoke the EJB method
  - isCallerInRole()

Tivoli Access Manager v6 – New Capabilities



- ✔ Flexible choice among diverse authentication mechanisms
- ✔ Step-up
- ✔ Forced re-authentication

- ✔ Native—Desktop and Web SSO
- ✔ Integrate w/TFIM for federated SSO
- ✔ Integrate w/partner products for client/server SSO

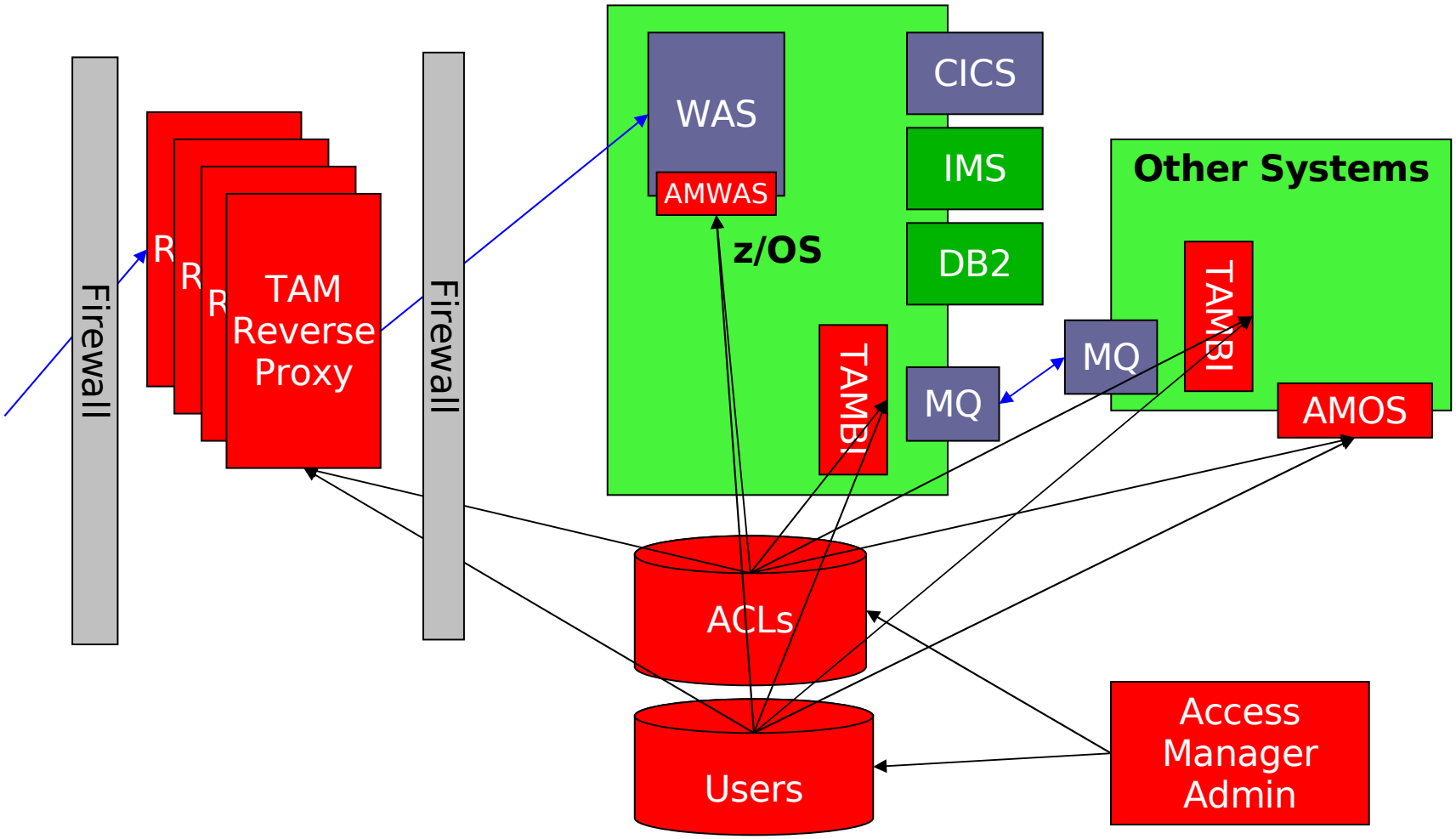
- ✔ Policy-driven
- ✔ Resource "agnostic"
- ✔ Standards-based (Java, .NET, C/C++)

- ✔ Enterprise-class auditing
- ✔ Reporting
- ✔ Key element for compliance

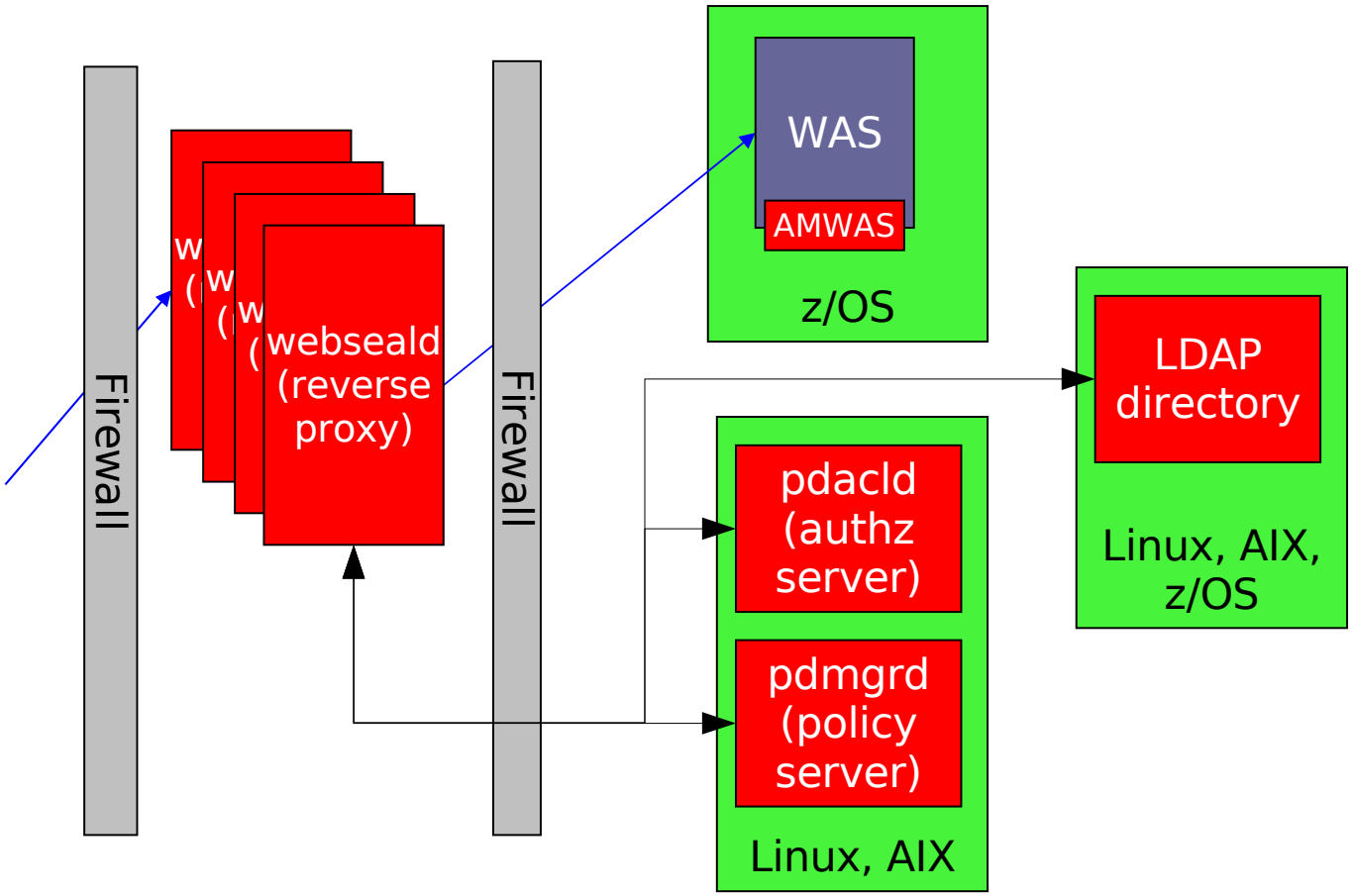
Tivoli Access Manager Integration Points

- Review of Tivoli Access Manager deployment model
- Integration points
  - Use of z/OS LDAP server for TAM registry
    - z/OS LDAP configuration
    - TAM runtime configuration
  - Use of ITDI to synch z/OS LDAP users and RACF users
  - Use of External Authentication Interface (EAI)
  - Use of Linux for zSeries for webseald, pdacld, and pdmgrd
- Where to go for more information

Tivoli Access Manager – Conceptual View



Tivoli Access Manager – Deployment View



Integration 1: Use z/OS LDAP Server for TAM Registry

- Allows user registry for TAM to reside on z/OS
- Backup/restore of LDAP directory based on DB2 for z/OS procedures
- Enables usage of RACF password for TAM authentication processing (if so configured)

Configuring z/OS LDAP Server

- Configure TDBM database backend (LDAP server config file)

```
database tdbm GLDBTDBM
suffix “secAuthority=default”
suffix “dc=company.com”
```

- Load schema: schema.user.ldif, schema.IBM.ldif – ldapmodify command, TAM ivrgy_tool command

```
ldapmodify -h <host:port> -D ... -w ... -f
schema.user.mod.ldif
ldapmodify -h <host:port> -D ... -w ... -f
schema.IBM.mod.ldif
ivrgy_tool -h <host> - p <port> -D ... -w ... -d schema
```

- Configure Native Authentication (LDAP server config file)

```
useNativeAuth selected
nativeUpdateAllowed on
nativeAuthSubtree “dc=company.com”
```

Configuring TAM runtime environment

- Be sure z/OS LDAP server is running and accessible when configuring TAM runtime
  - If z/OS LDAP has SDBM backend configured, disable it while configuring TAM runtime
  - SDBM can be re-enabled after runtime environment on systems running TAM is configured
- Run pdconfig

```
pdconfig
```

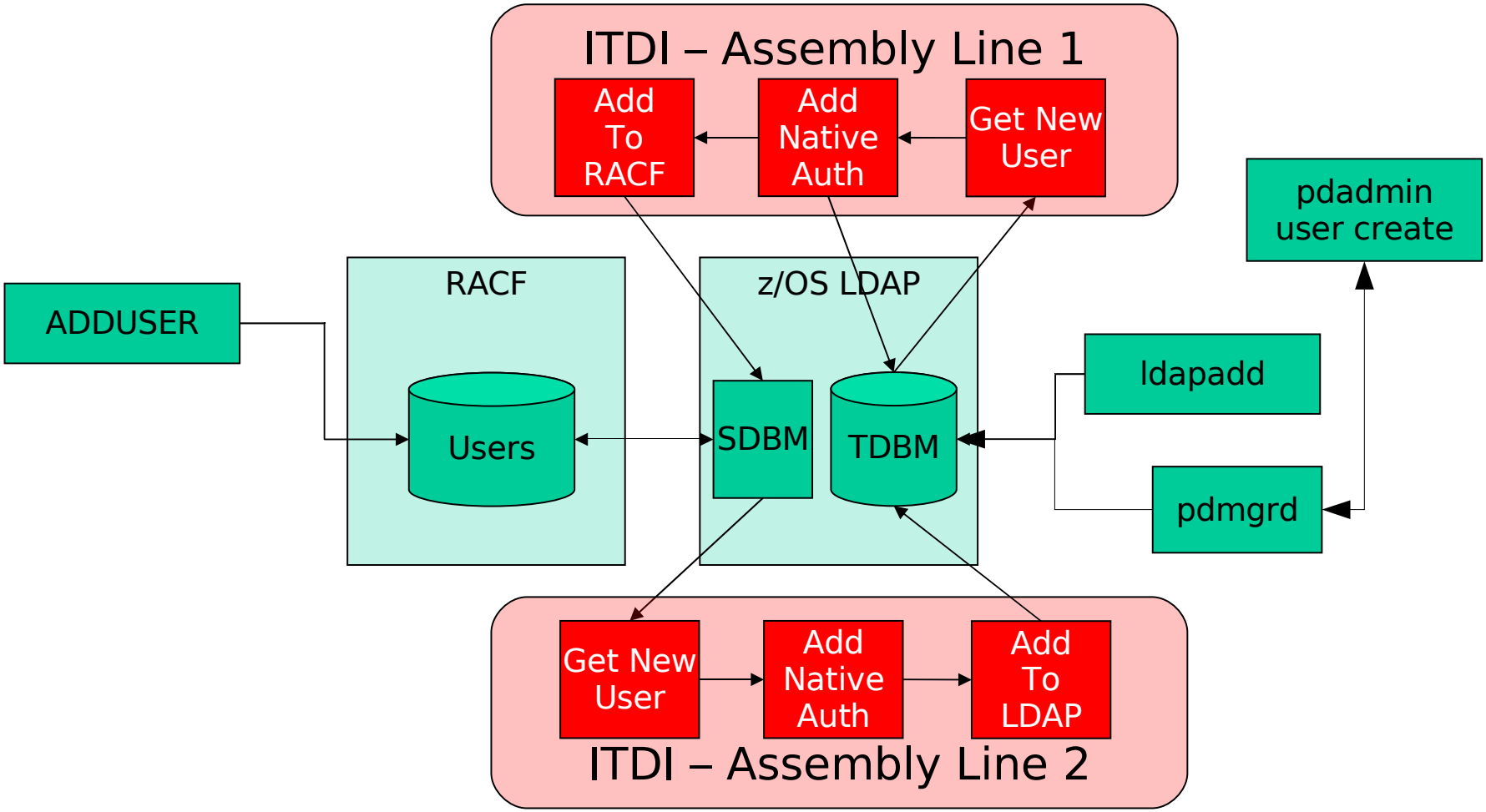
- Modify TAM runtime configuration properties (/<InstallDir>/etc/ldap.conf)

```
ignore-suffix = “cn=racf,dc=yourcompany.com”
auth-using-compare = no
```

Integration 2: Use of ITDI to synchronize z/OS LDAP and RACF users

- When a user is added to RACF, an LDAP directory entry is not automatically created
- When a user is added to TAM or LDAP, a RACF user is not automatically created
- ITDI assembly lines can be used to enable such processing
  - See next page
- Or Tivoli Identity Manager (TIM) might be used to enable coordinated user management across these multiple registries

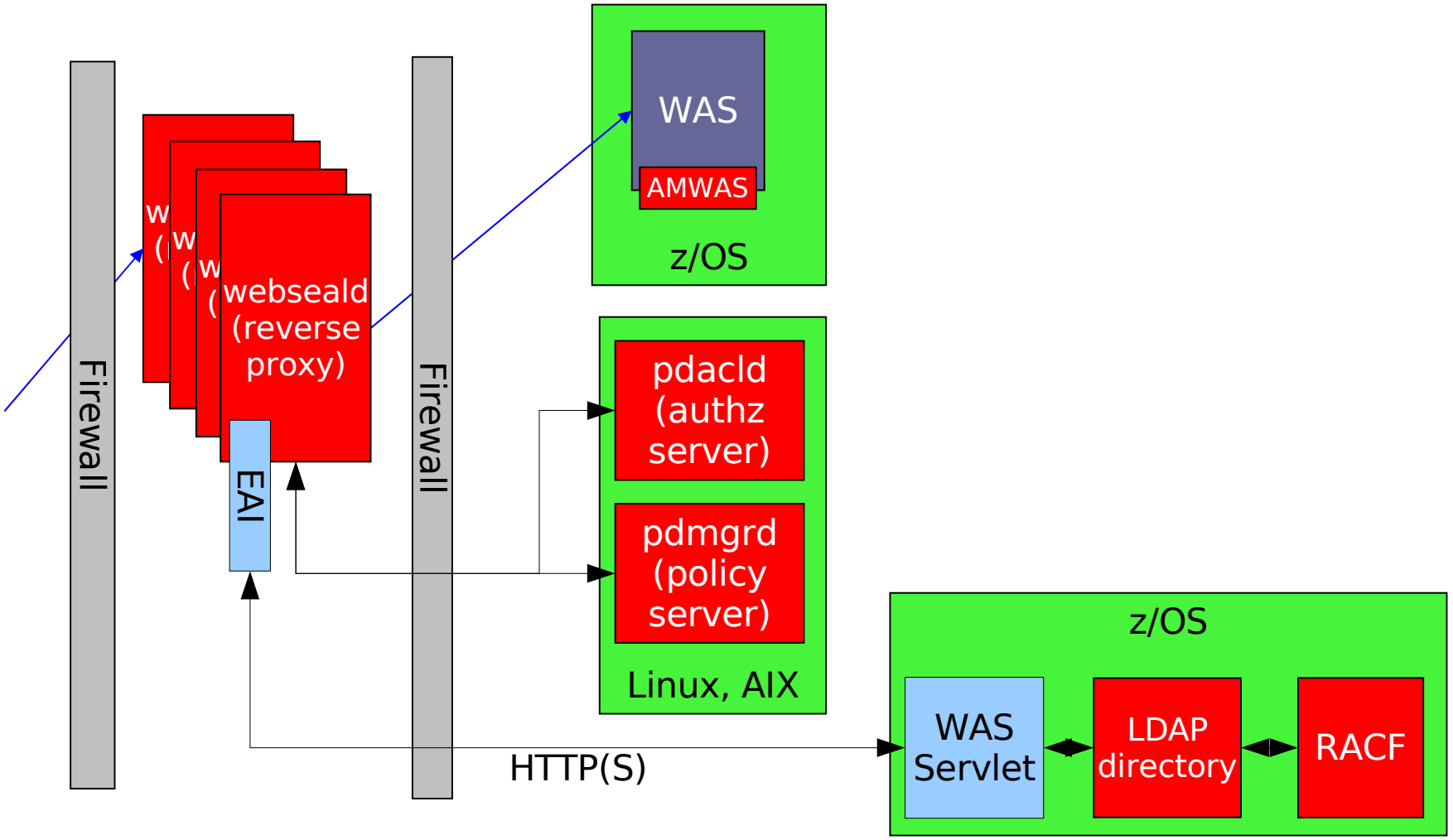
Two ITDI assembly lines to handle user synchronization



Integration 3: Use an External Authentication Interface

- Replaces the now obsolete CDAS plug-point
- A plug-point within webseald
- Allows extensibility for authentication processing in webseal
- Utilize z/OS LDAP SDBM backend for LDAP access to RACF user/group information, including authentication checks

Using an EAI plug-in to communicate with RACF



Configuring the EAI interface

- Configure the EAI in the webseal configuration file

```
<WebSealInstallDirectory>/etc/webseald-<instanceName>.conf
```

- Define an HTTP junction to webseal which will serve as the EAI implementation

```
pdadmin server task <instanceName>-webseald \
virtualhost create -t tcp -h vhost.mycompany.com eaiServer
```

- Enable EAI using [eai] stanza of configuration file.

```
[eai]
eai-auth = http
```

- Configure the HTTP header names used to convey information back to webseal in HTTP responses

```
eai-user-id-header = am-userid
eai-xattrs-header =am-name,am-address
```

- Configure external authentication

```
[authentication-mechanisms]
ext-auth-interface = libeaiauthn.so
```

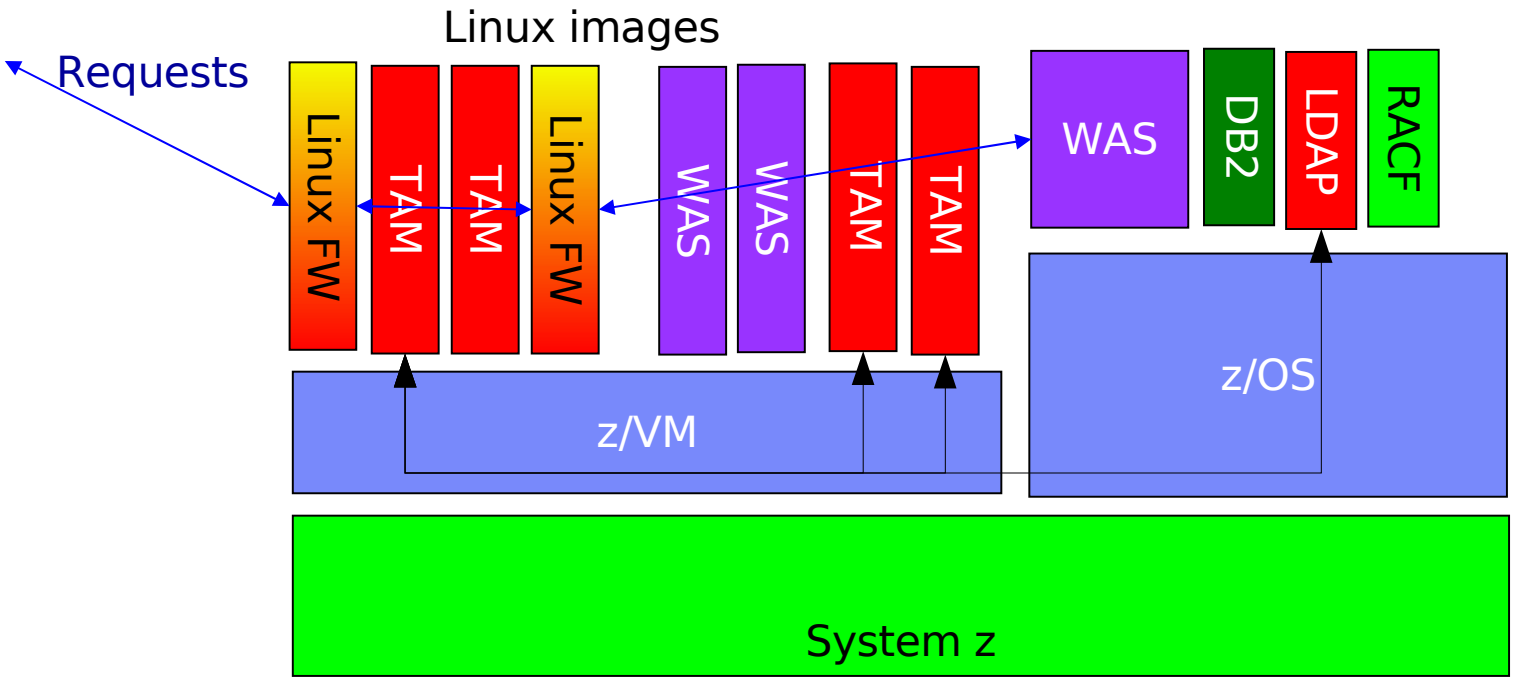
- Configure EAI Trigger URL(s)

```
[eai-trigger-urls]
HTTP://vhost.mycompany.com/servlets/*
```

Integration 4: Use of Linux for zSeries for webseald, pdacld, and pdmgrd

- This allows hosting of a TAM-protected environment entirely on System z systems
- Hipersockets support can be used between Linux for zSeries systems and z/OS
- z/VM virtual network connections enable precise routing between webseal-dedicated images and other system images

Tivoli Access Manager on System z



Useful documentation

- Tivoli Access Manager Infocenter

  http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itame.doc/welcome.htm

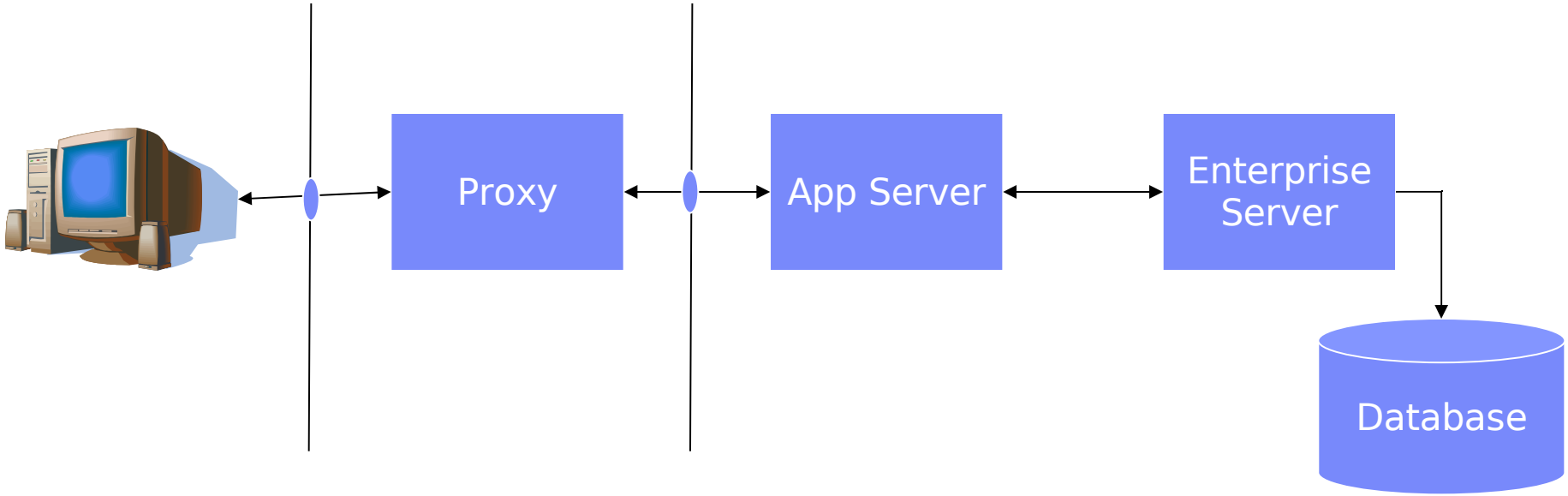
- z/OS LDAP server Administration and Use

  http://publibz.boulder.ibm.com/epubs/pdf/glda2a31.pdf

End-to-End integration

- Using TAM for e-Business and TFIM, end-to-end security integration is possible
- Authentication and Access Checking at point of contact
- Credential transfer and transform as requests flow through WAS
- Additional Access Checking at EJB and application level
- Credential transform for back-end system access using TFIM trust service

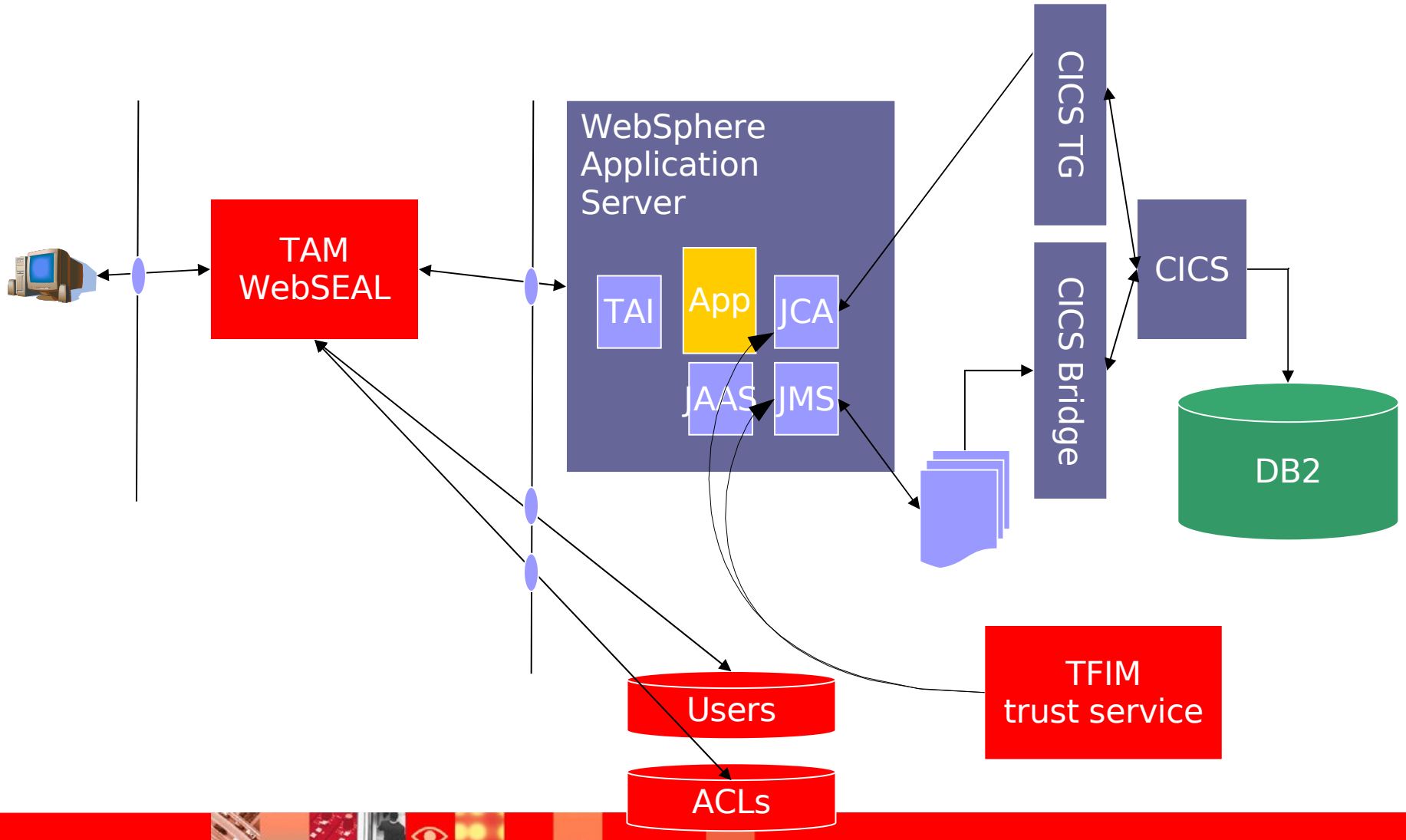
General Pattern for Enterprise Access



General Pattern

- User connects to Organization's web presence and authenticates
- "proxy" in DMZ authenticates user and protects Enterprise
- Requests are sent from user, through proxy, to Application Server
- JSPs, Servlets, and EJBs running in Application Server connect to Enterprise Server and database(s)
- Results are returned to user, through proxy

End-to-end Integration using TAM and TFIM



IMS or CICS – Some details

- WebSEAL authenticates the user
- WebSEAL authenticates to WAS on behalf of the user, passing TAM credentials and using TAM TAI.
- In WAS, a TAM Trust Association Interceptor (TAI) returns a userid for WebSphere to use for the request.
- JCA Connector obtains JAAS Principal, uses this to invoke JAAS LoginModule
- JAAS LoginModule used to invoke TFIM trust service to get the userid and password/passticket associated with the JAAS Principal
- Mainframe userid + password (or passticket) supplied in ConnectionSpec for Java Connector Architecture connection (through IMS Connect or CICS Transaction Gateway)
  or
- Mainframe userid + password (or passticket) supplied in MQMD/MQCIH header for CICS bridge connection

Summary

- There exist many integration points between Tivoli Access Manager and security of applications and subsystems running on z/OS
- Tivoli Access Manager can be deployed entirely on a System z platform
- There is deep integration between TAM, WAS, TFIM, and RACF to support application environments and end-to-end integration
- And there are more examples too:
  - Enterprise Single Sign On using TAM-ESSO
  - Usage of TAM, WebSphere, WebSphere Portal, and z/OS-based applications
  - Usage of TAM, HostOnDemand, and HATS along with z/OS-based applications

For More Information

- Tivoli Identity Manager
  - http://www.ibm.com/software/tivoli/products/identity-mgr/
- Tivoli Access Manager
  - http://www.ibm.com/software/tivoli/products/access-mgr-e-bus/
  - http://www.ibm.com/software/tivoli/products/access-mgr-operating-sys/
  - http://www.ibm.com/software/tivoli/products/access-mgr-bus-integration/
  - http://www.ibm.com/software/tivoli/products/access-mgr-esso/
- Tivoli Federated Identity Manager
  - http://www.ibm.com/software/tivoli/products/federated-identity-mgr
- IBM Tivoli Directory Server
  - http://www.ibm.com/software/tivoli/products/directory-server/
- IBM Tivoli Directory Integrator
  - http://www.ibm.com/software/tivoli/products/directory-integrator/
- Redbook on Patterns: Connecting Apps to the Enterprise
  - http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg247310.pdf
  - http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg246572.pdf
  - http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg246014.pdf
- Contact me
  - mailto:hahnt@us.ibm.com