CALIFORNIA STATE UNIVERSITY
SAN BERNARDINO

CSUSB Network Architecture
CSUSB, Information Security Office

Last Revised: **01/10/2013**

Final

REVISION CONTROL

Document Title: CSUSB Campus Network Architecture

Author: James Macdonell

File Reference:

Date	By	Action	Pages
06/02/2009	J Macdonell	Created Campus Network Guidelines	All
06/01/2010	J Macdonell	Added additional screen shots	5,6 and 7

Review/Approval History

Date	By	Action	Pages

1.0 Server Farm Firewall Architecture 4
2.0 External “Untrusted” Zones 4
3.0 Campus-only Zones 4
4.0 Internet Exposed Zones 5
5.0 Campus-only, Restricted Access 6

1.0 Server Farm Firewall Architecture

The farm firewall architecture is intended to allow the campus to better manage its access controls to a broad range of services. It encourages use of highly segmented networks in order to accommodate the diversity of campus services and the consolidation initiative. It facilitates maintaining strict access control for high-risk, sensitive services while at the same time allowing flexibility for lower-risk service.

There are eight zones defined in the current architecture. Each zone will contain multiple networks with intrazone blocking. That is, all traffic between networks is implicitly denied.

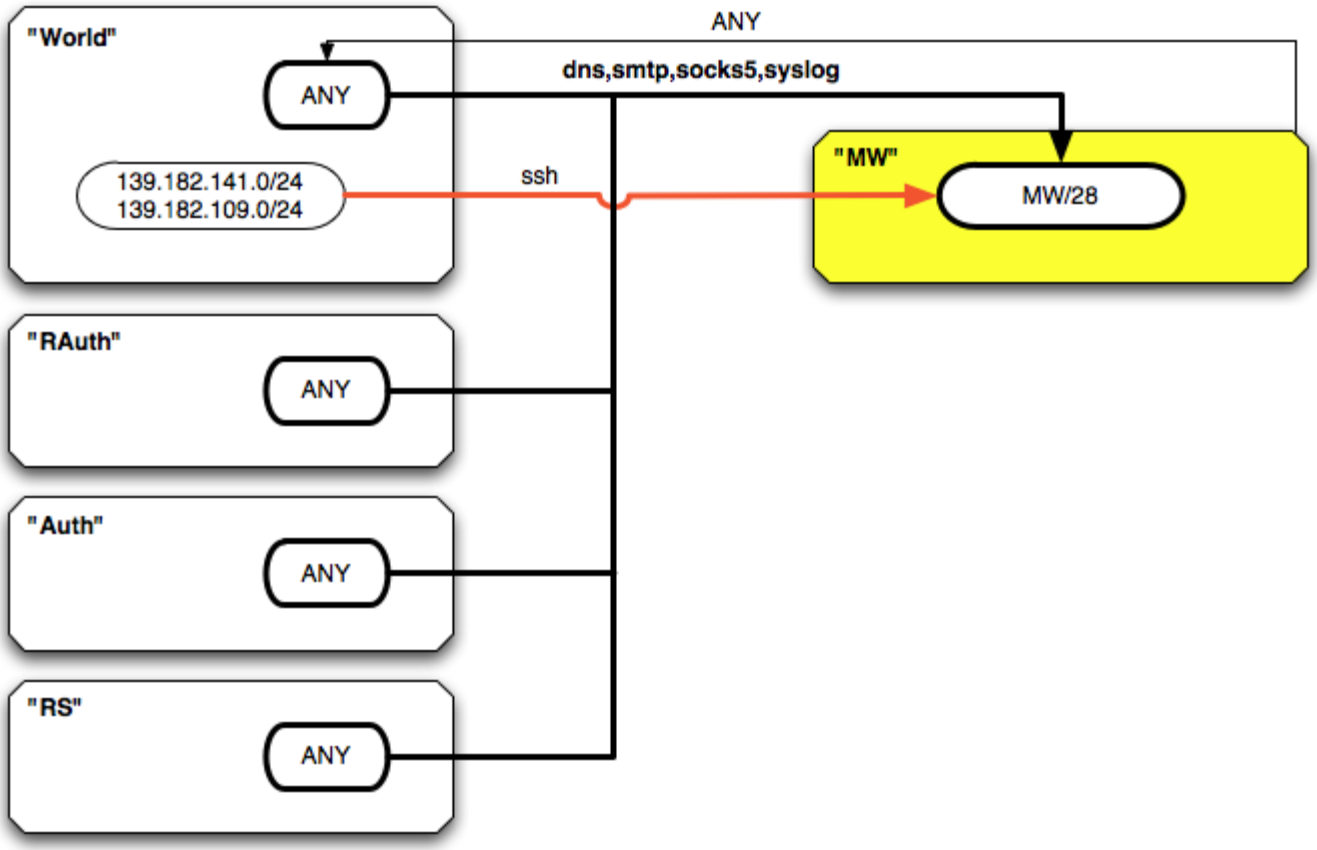
2.0 External "Untrusted" Zones

World **-**These networks outside the server farm, including the Internet, Wireless network, and other on-campus networks.

3.0 Campus-only Zones

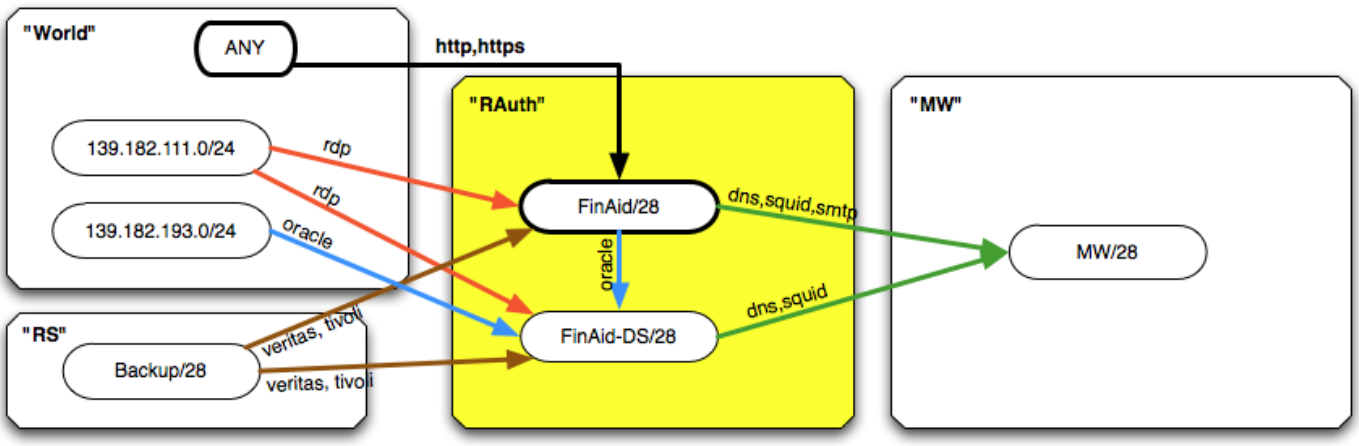
MW **–** Middleware contains internal services that are dependencies for other services: DNS, DHCP, NTP, Licensing, LDAP, AD, SOCKS5, Monitoring

- Example, middleware administrated by ISO/TNS:

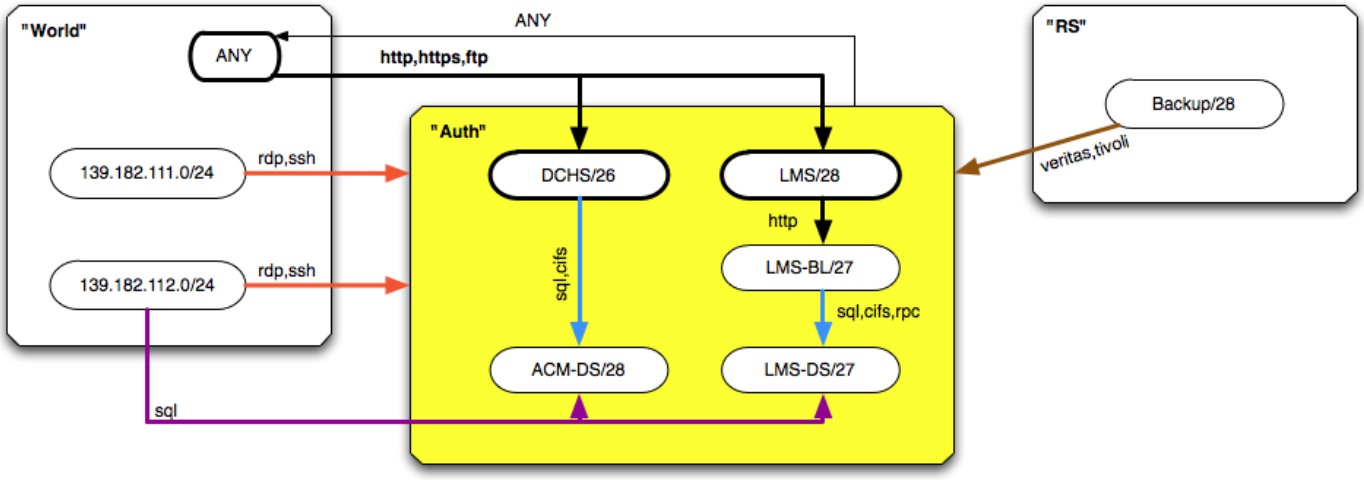


4.0 Internet Exposed Zones

- **RAuth** - Restricted Authenticated Services
  - Public services that process or store Level 1 Information.
  - Highly segmented intra-zone networks. Restrictive outbound traffic. Support for multi-tier applications
  - Example, fictitious financial aid application:



- **Auth** - Authenticated Services
  - Public services that process or store Level 2 Information and/or require authentication.
  - Support for multi-tier applications.
  - Example two- and three-tier applications:



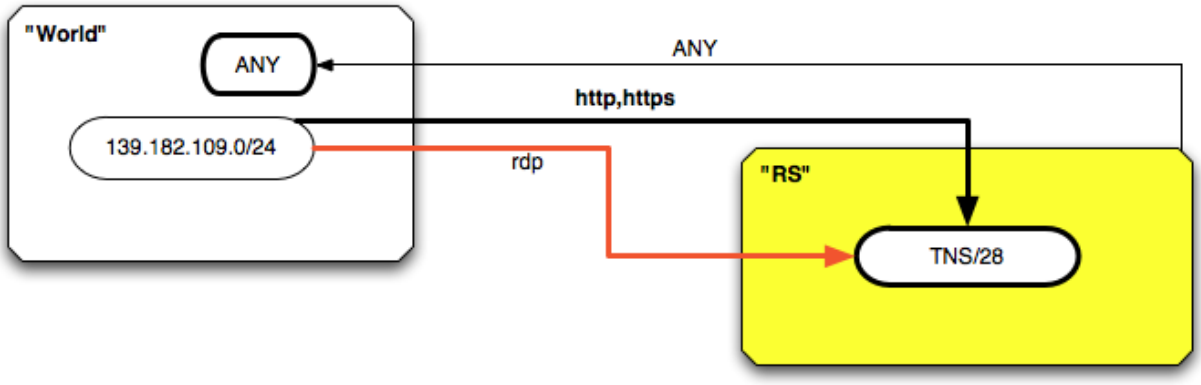
- **Acad** - Academic Services
  - Services related to grants, research, or student projects. Typically web sites.
  - Developed and maintained by faculty and students.

- **Anon** - Anonymous Services
  - Public services (Level 3). Typically web sites.
  - Developed and maintained by administrative staff.

5.0 Campus-only, Restricted Access

- **RS** - Restricted Support Services
  - Back-office services used by an exclusive group of on-campus clients across many user networks: OneCard DB, FinAid DB, "M: drive", Veritas

- Example, an intranet for TNS:



Voice

- VoIP infrastructure, including phones