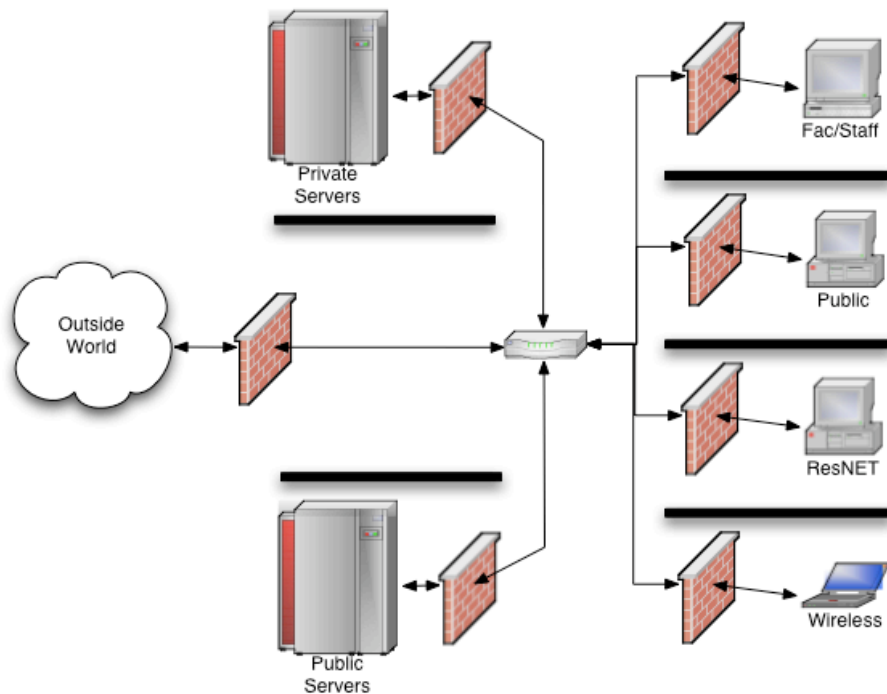


Secure Networks, Secure Computing Environments



First steps:

- Expand and update our old notions about “public” and “private.”
- Isolate groups; don’t let groups direct traffic to each other.
- Think carefully about what protocols should be allowed through the firewall, eliminate all others.

Take advantage of opportunities:

- Limit access to resources by network group; look for mechanism to control who joins what network.
- Consider using NAT to further secure clients from outside attack.
- Consider “clientless” authentication mechanisms such as NoCatAuth.

What is NoCatAuth?

- An open-source captive portal for network authentication and client management.
- Integrates DHCP, firewall, and authentication services.
- Uses web browser interface to take credentials, changes firewall behavior based on authentication. Looks for and reports ARP spoofing.
- Free for client and server; requires no additional client configuration.
- Links:
 - < <http://nocat.net/> >
 - < <http://www.oreillynet.com/pub/a/wireless/2001/11/09/nocatauth.html> >