Present network security on whoi ships.

1) firewall on the ship between the router and the ship's network (highly restrictive)
2) Firewall on shore router (somewhat open)
3) Access control lists on ship and shore routers (for incoming connections)

Shipboard access to internet:

1) Only 4 "browsers" per ship, 1 linux and 1 osX machine, 2 science machines, but no windows.
2) All browsers are located in public spaces
3) Browsers are allowed to use only 80, 443 and 3128 (proxy server)
4) No wireless access to ship's network or internet.
5) No change even when connected to dock or swap, except for windows updates.
6) Dhcp is currently supported

All oncoming windows machines are checked.

1) up to date virus definitions
2) reasonable service pack level
3) scan for suspicious open ports

New network security model (starting next month)

1) 4 networks
   a) sssg but with no dhcp and tight access control (all data collecting stuff, web server and email)
   b) science jungle , including wireless access(all machines supplied by science)
   c) ship's business (all machines operated by the port office)
   d) staterooms
2) Rules 1, 2 and 3 from the present model are unchanged.
3) Science, ship and stateroom networks are not checked or monitored
4) All networks have access to email and web from sssg network, and have access to ntp, dns and dhcp
5) When a hi speed network connection is available, networks 2, 3 and 4 have full internet access.

Jim Akens, whoi