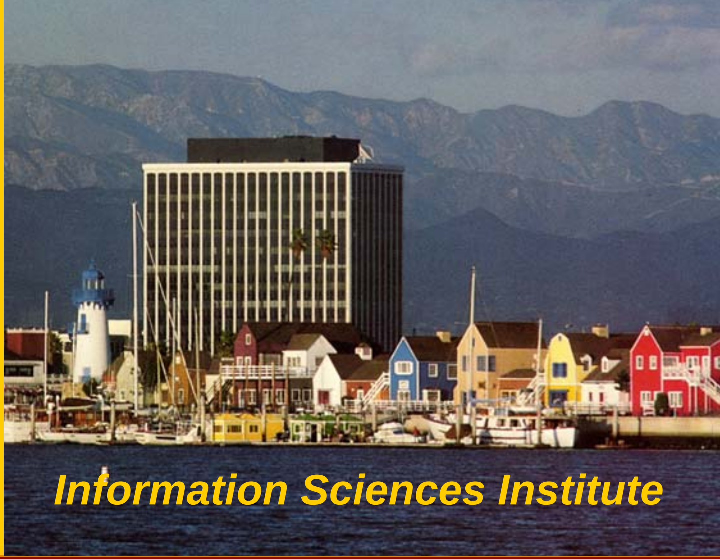
USC Viterbi
School of Engineering


Information Sciences Institute

Running Live Self-Propagating Malware on the DETER Testbed

Clifford Neuman, Chinmay Shah, Kevin Lahey

USC Information Sciences Institute
DETER Project

USC

June 16, 2006 Deter Community Workshop
Arlington, Virginia www.isi.edu/deter

DETER Testbed Goals

- **Facilitate scientific experimentation**
- **Establish baseline for validation of new approaches**
- **To protect the public internet from the side effects of security experiments**
  - Saturated Links
  - Broken routing
  - **Exfiltration of malicious code**
- **Provide access to wide community of users**

Outline

- Goals of Experiment
- Testbed Procedures
- Running the experiment
- Results and lessons learned
- Future experimentation
- Future of Malware on DETER

Goals of Malware Experiment

- **Exercise procedures for containment**
  - While using malicious code that would be relatively innocuous if our procedures failed.
  - We will exercise the procedures as if the code is more dangerous than it actually is.
- **Generate useful results**
  - Traces that can be used by other experimenters.
- **Improve procedures to improve future experiments by others.**

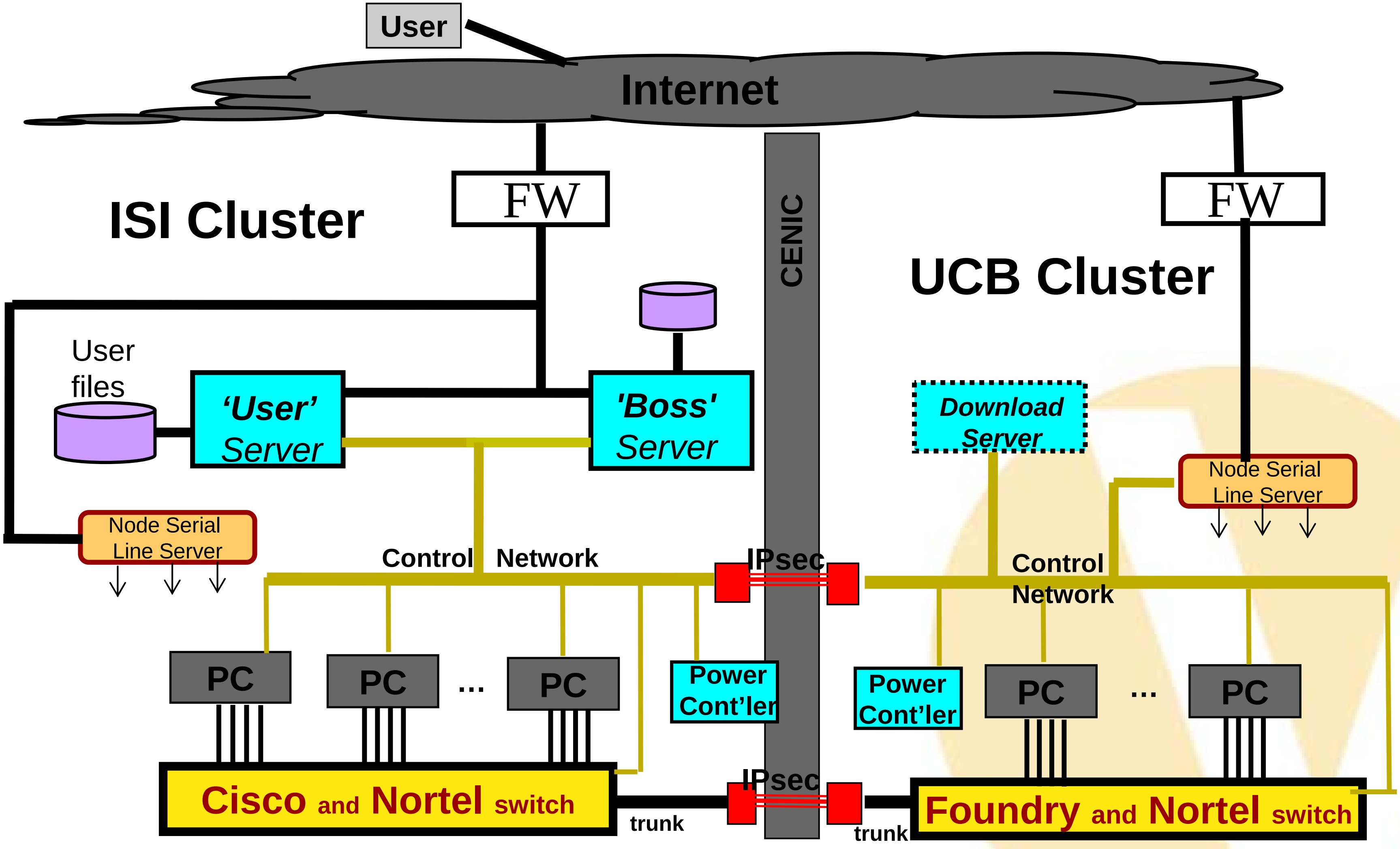
Not all Malware is the Same

- **Full containment is very restrictive**
  - Requires physical access to manage and run.
  - Can not run other experiments simultaneously.
- **Longer term goal is to allow some malware experiments to run while connected.**
  - Procedures developed and tested requiring strongest containment.
  - For particular pieces of known malware, individual procedures may be eliminated or modified.

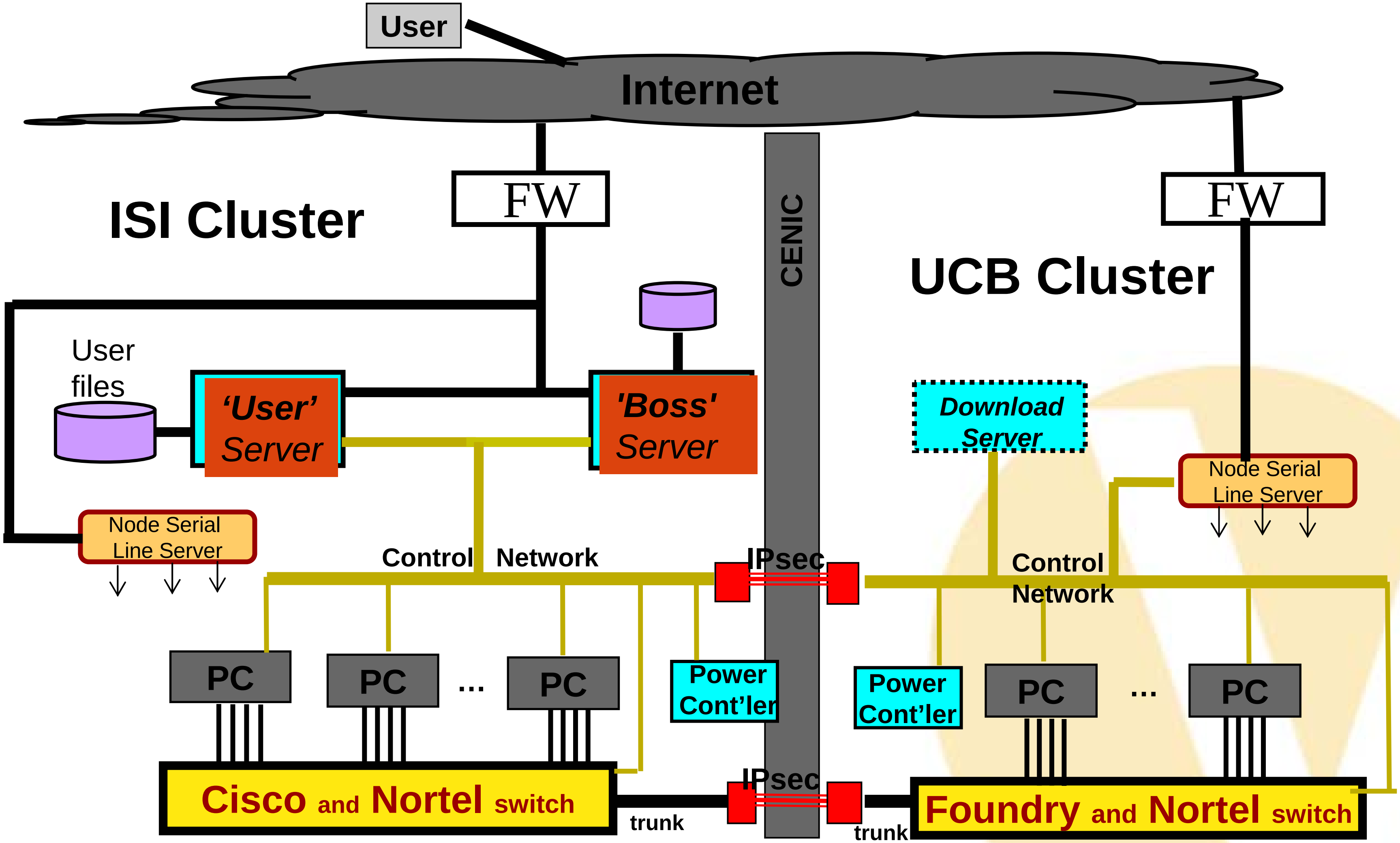
Securing the Testbed

- **Up front one time steps to secure the testbed**
  - Collect BIOS and OS checksums
  - Disable writing of BIOS
  - Intrusion detection running on control network and inside severed connection to the outside.
- **Per experiment steps**
  - Backup user and boss and power down backup
  - Power down unused assets
  - Disconnect from outside and power down connection
  - Regression test that no packets escape

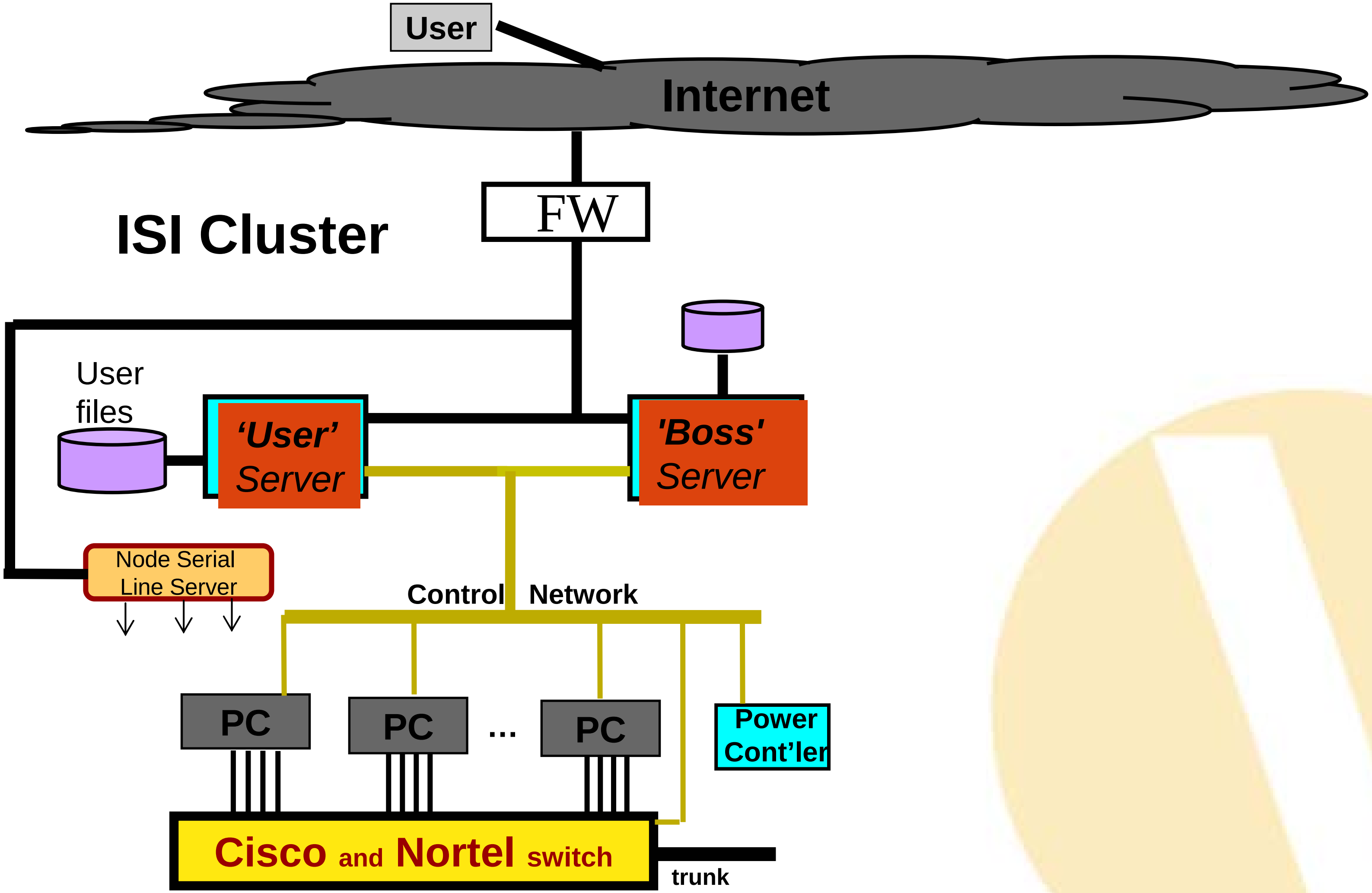
DETER Architecture



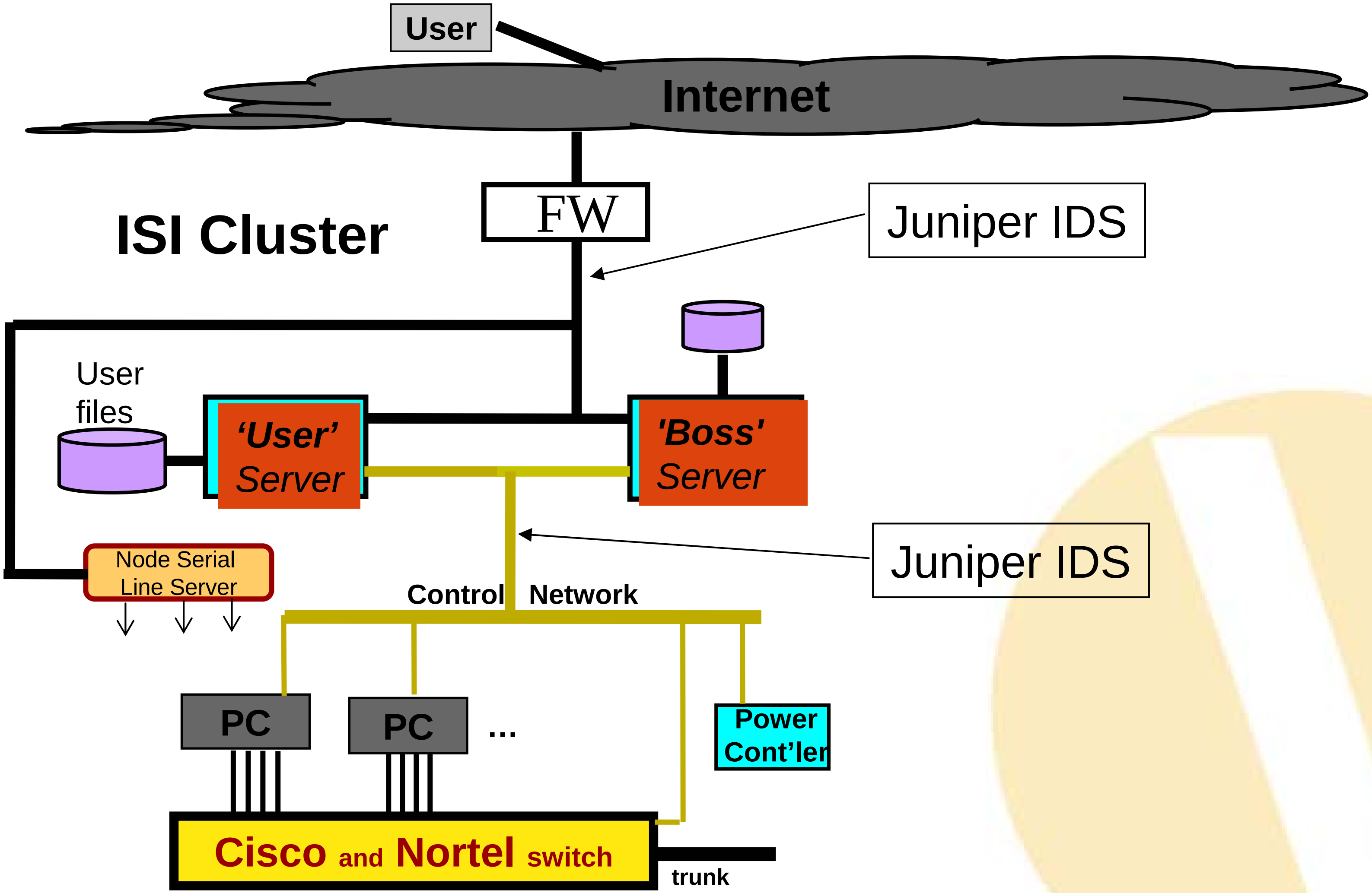
Backup User/Boss



Disconnect Intercluster

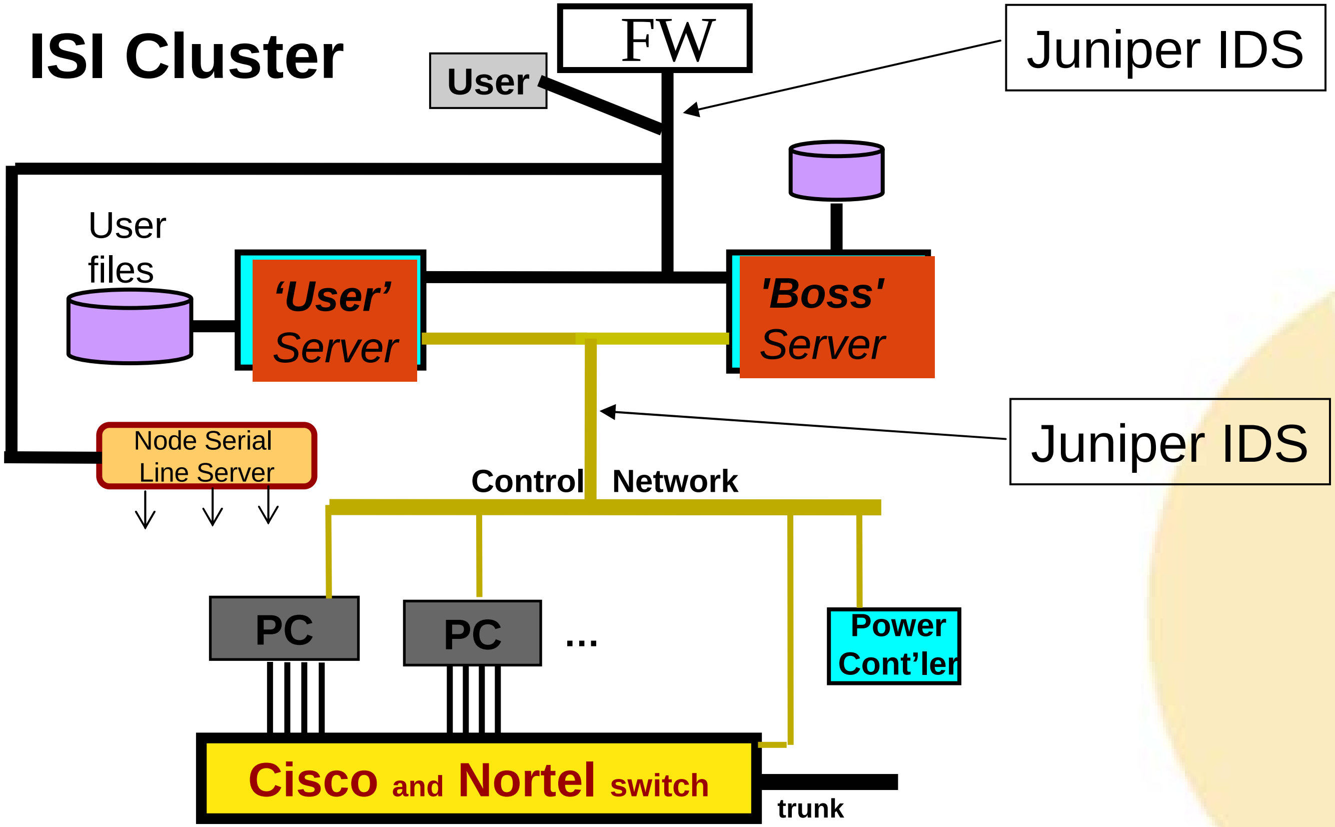


Placement of ID devices



Sever Outside Connection

Move user inside, Run Regression



Running the Experiment

- **Experiment staged sans malware before disconnecting**
  - Nodes swapped in
  - Data collection tested
- **Testbed disconnected and worm introduced**
  - TCPdump and Tethereal used to collect traces
  - Traces transferred to a single experiment node and written to a USB disk which is then disconnected

Scalper Experiment

- **The Scalper experiment**
  - Current configuration was only 4 nodes
    - Started with 52, but because testbed was needed by others we scaled it down to get it working.
    - Now that meeting is complete we can schedule downtime again to collect larger traces.
    - Post processing in progress off-line, removing worm code from traces.
    - Traces from larger experiment will be available to DETER researchers.

Restarting the Testbed

- **Experiment nodes zeroed**
- **BIOS checksums & tripwire checked**
  - Users and BOSS
- **ID device logs checked**
  - Looking for unexpected communication to users and Boss
  - Any unexpected communications to external firewall
    - Physically disconnected, but indicates failure of internal containment.
  - Power to disabled assets
  - Reconnect testbed to outside

Lessons Learned

- **Malware is more sensitive to environment than expected at first.**
  - Advanced testing sans malware not enough.
  - It still took us 4 attempts with associated testbed downtime to get the worm to propoagate.
  - Solution: Stage sans malware connected (as we did) plus test with malware on single node using vmware and on mini-bed, before running on full testbed.
- **Missing testbed features**
  - Honeynet module mapping nodes to dynamically detected target addresses.

Future Experiments

- **Two phase modeling**
  - Experimenter should be able to order traces from a catalog of malware, specifying topology details, and what trace details need preservation.
    - Traces generated, scrubbed, and made available for use by investigator.
- **Questions to be answered**
  - Can background traffic be mixed with traces, or must it be present when trace generated.
    - Will likely depend on the malware used
  - What kind of experiments is this useful for
    - Probably detection experiments, but less useful where there is two way interaction between studied protocol/device and the worm.

Future Of Malware on DETER

- **Development of mini-beds will allow small malware experiments concurrent with other use of testbed.**
  - Malware experiments also tested on smaller topologies to work out the bugs before introducing to larger testbed.
- **Federation of Testbed for Malware experiments**
  - For less dangerous malware
- **Addition of Honeynet features.**
  - This will support study of binary worms where scanning behavior can not be predicted.
- **Development of a catalog of Malware**
  - With a list of specific containment features needed for each.