INCIDENT REPORT

INFORMATION TECHNOLOGY SERVICES

Incident Report – August 15, 2016

Incident #2016-157/158

DCP Firewall Outage

Summary

Scheduled maintenance work was being performed on Sunday, August 7, 2016 to replace a failed firewall from a previous power outage. The new firewall was installed and at approximately 10 am the failover process began. The active firewall pushed the configuration to the new standby unit and the standby unit joined the failover cluster. At 10:10 am problems were identified on the new firewall and a decision was made immediately because of the number of services down and impact to applications to shut down the offending firewall and restore services to the previously active firewall until the problem could be fully understood. It was later found that the failover firewall configuration caused the disruptive failure causing the outages on many production applications across campus.

As a result of this incident, we were left with one firewall and before we could schedule in another maintenance window to fix it on Wednesday, August 10, at 2:30 am, the remaining firewall locked up and again several services became unavailable. The firewall was rebooted at 6 am after the first alert was received and the new fail over firewall was also put back in service at this time with an updated configuration file installed.

Impact

All outside access into the DCP firewall was halted between 10:16 am - 10:45 am. Services included:

- PeopleSoft
- Mail
- WebPublish (and associated web sites)
- Moodle
- Streaming
- Library QCat Search
- Wiki
- SSO
- Careers

Root Cause

At the time of this Incident Report, faulty failover configuration is to blame. Current suspicions are ARP cache issues or physical interface issues on the failover firewall or physical cable. Final root cause is yet to be determined.

Resolution

Sunday, August 7, 2016: Power off failover firewall, allowing the primary firewall to handle the load. When the second outage occurred on Wednesday, August 10, 2016 it was a good opportunity to get the failover appliance into service, thus not causing another outage in a separate maintenance window later.

Communications (Internal)

Call to Curtis Ireland (Systems). Email to Gail Ferland, Andy Hooper, Kevin Lackie, Terry Black, Curtis Ireland, Networks Level 3.

ITSPP Communications (External)

Notices were posted in both cases through the ITS Notification Tool. They were put up as soon as the website was functional. The Notification Tool alerted campus of the outage of services, updates to the issue, and notification of restoration of service.

Lessons Learned

Production firewalls should be treated as disruptive in future and change control tickets should reflect this. Procedures should be well laid out and testing completed where possible to confirm steps. Verify that failover works before making changes on any one firewall.