Project EmailNG

Next Generation Email System

Project EmailNG is an upgrade project of our mail systems which were installed in 2004 in their current form. Along with upgrading the existing systems new functionality and options are implemented to reflect the technological advances of the last years. EmailNG depends entirely on FOSS and makes use of the CS Dept. virtualization and consolidated storage systems.

Apart from the infrastructure being used and the time spent on implementing the project there are no other costs. The system is custom built using entirely internal technological knowledge and dependent entirely on the CS support personnel for support and maintenance (and the FOSS community of course).

The "Email administrator manual" should be read along with this document to understand the installation details. Here we describe the project steps. Description of the system and installation details are provides in the Administrator manual.

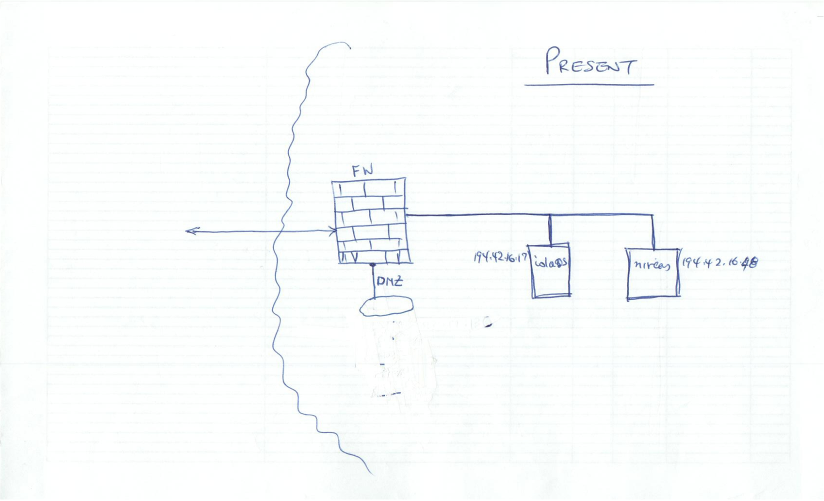
Features

- Advanced capabilities fit for a diverse community
- Expandability at all levels (Storage, IMAP, SMTP, SPAM and VIRUS control)
- Multilevel security (system, email, DMZ)
- E-Mail client independence supporting almost all IMAP, POP and Webmail clients
- Robustness, availability, fault tolerance built into the original design
- User control – users can customize their message delivery experience (filters, SPAM control etc)
- Support for advanced and entry level users
- Support for mobile devices and clients
- No down time maintenance operations
- Minimal cost with FOSS and off the shelf hardware. Uses widely available and tested FOSS software.
- Based on widely accepted protocol standards (RFC) for all the software
- Vendor independence. No vendor lock in. Built with local technology knowledge and experience.

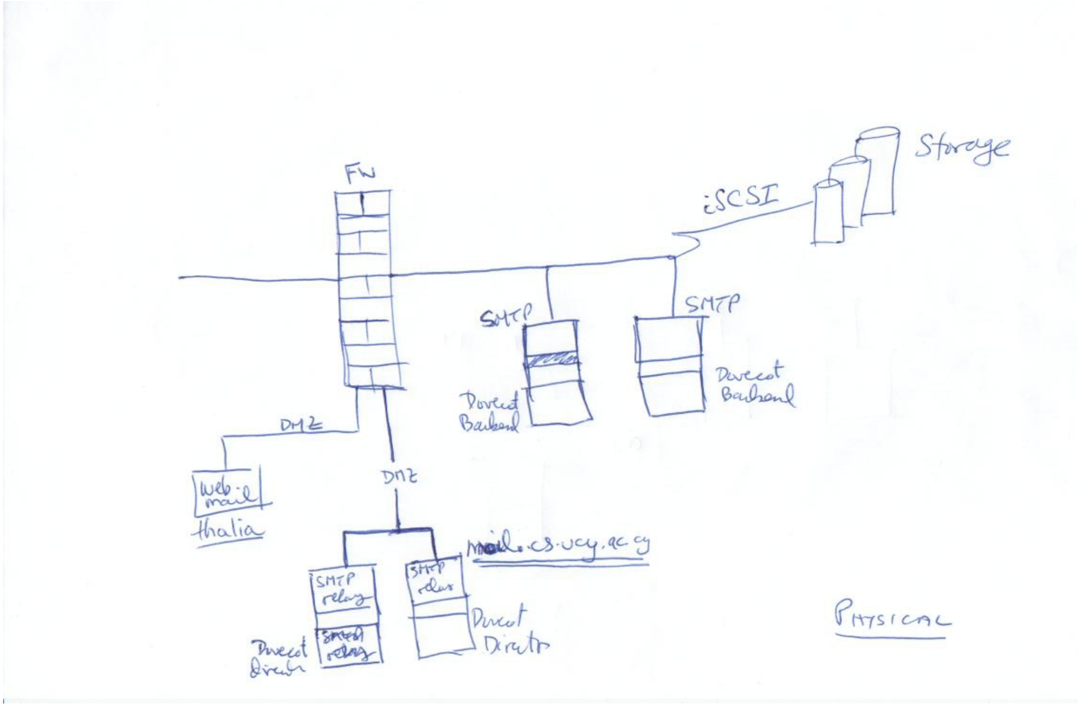
Why Change?

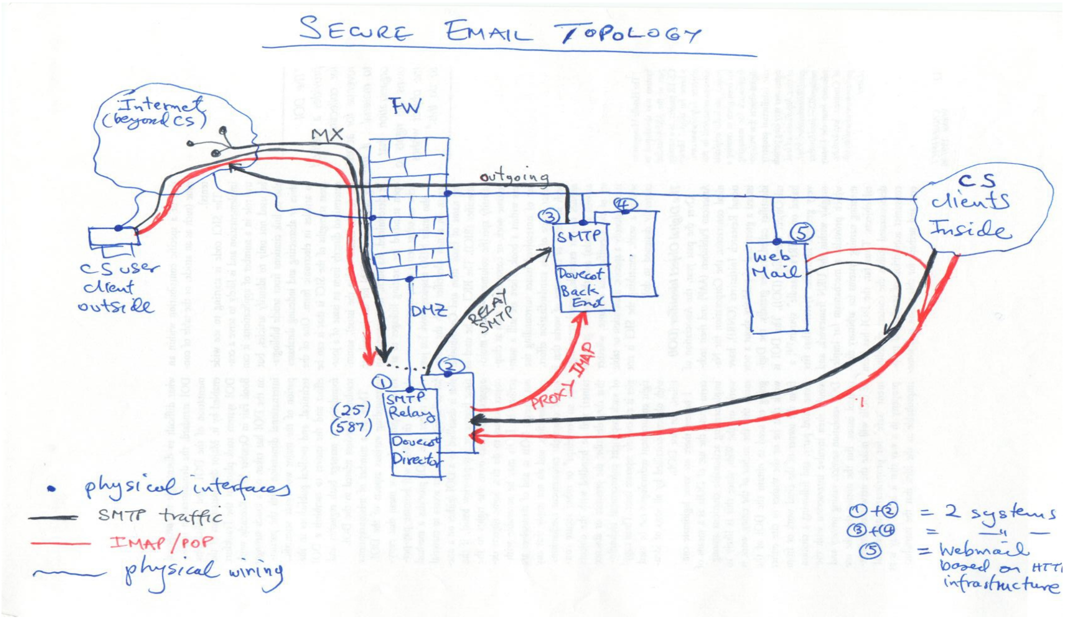
- There is a pressing need for a system upgrade of software and hardware
- security challenges have increased and the current status does not address even the basic threats that exist today
- provide better availability in line with dept. requirements both during normal operations but also during maintenance operations
- enhance the user functionality by allowing the user to better control his/her environment
- better mobile systems support

Current Status



Future Status





Objectives:

1. Create a robust, fault tolerant upgrade of the existing system
2. Upgrade of software and take advantage of new features in software
3. Change from the MailScanner software to the Amavisd-new system
4. Make use of our extensive virtual server platforms and our consolidated storage
5. Take advantage of our LDAP installation to centralize and streamline the email system authentication and user profiles
6. Improvements on
   a) Security
   b) Efficiency (storage, processing speed)
   c) User capabilities and UI
7. The following areas will be affected:

Area	Short description
User Quota	• implement Dovecot based quota with the ability to enforce from LDAP settings rather than fs quota • over quota management • user monitoring
Message Storage	• Integration with consolidated storage systems at CS • Multiple location message storage • synchronization with dsync • migration to the more efficient mdbox message storage format
Message format	• Change from maildir to Dovecot mdbox
Better filtering	• Use a standards based filter engine (sieve) ○ clients will be affected
Better user experience	• Message filter setup from withing the clients • individual quota monitoring • over quota management
Fault tolerance, resilience	• Multiple message servers (virtual machines) • ability for the system to survive server failures • automatic redirection of mail traffic and users to surviving

	servers • automatic storage synchronization on two servers
Performance	• Separation of user activity from back end server activity
Better SPAM control	• Use of amavisd • Multilevel filtering • Server side filters and options (before queue-after queue filtering)
User filters (spam and message mgmt)	• Server side user filters with Sieve
User management	• Integration with LDAP services
Security/SMTPS	• Greatly enhance security by designing the whole system around using the DMZ with inside and outside facing servers • Login with encrypted channel to SMTP when submitting messages for delivery (SASL authentication)
Shared Mailboxes	• Internal Lists or Announcements

Project Overall Flow

This is an overview and plan. Not a complete action list. See the section “Project Time Flow” below for a detailed action list and the Appendix for a detailed action account and notes.

How to install, configure the systems, enable and protect services is described in the “Email Administrator Manual”.

The project takes a phased approach where the general flow is:

1. PHASE I: Primary IMAP network (theano, gorgo)
    1. priority is give to the primary IMAP network setup (since this will provide substantial improvement in user experience right from the start)
    2. Experiment with new features (mail alt locations, dsync to mdbox format)
2. PHASE II: Primary SMTP services network (theano, gorgo)
3. PHASE III: Secondary IMAP network
4. PHASE IV: Aecondary SMTP services network
5. PHASE V: Message storage format, security, tuning, final checks
    1. Message storage format change to mdbox
    2. Security enhancements
    3. tuning
6. PHASE VI: External systems integration
    1. Mailing list manager
    2. Pine on ADA
    3. caching DNS

- Primary and secondary IMAP/SMTP networks function simultaneously and do not have priority over each other. Here the terms are used for reference only.
- **It should be noted that where ever we mention IMAP we really mean both IMAP and POP3 since we support both protocols.**
- ***NO EMAIL SERVICE DISRUPTION IS EXPECTED***

Project Time Flow

PRE-REQUISITES:

1. Check and verify that at least one storage device to be used is ready to accept load
    1. hermes (nfs) -> argo -> /Mail (is already available)
    2. orpheas (nfs) –> argo -> /Mail (will be available soon as a final location)
    3. orpheas (nfs) -> NetApp -> /MailAlt (will be available soon)

PHASE I: PRIMARY IMAP SET-UP (Expected Duration: 20 days)

2. THEANO – IMAP proxy #1
    1. Install and secure OS - CentOS
        A) iptables, fail2ban, secure at the firewall, set up monitoring
    2. Compile and/or Install basic IMAP software
        A) Dovecot
        B) Configure IMAP proxy (director #1) to proxy to either NIREAS/IMAP or IOLAOS/IMAP based on user and or user-group. This is an initial state to test the director service.
3. GORGO – IMAP back end #1
    1. Install and secure OS - CentOS
        A) iptables, fail2ban, secure at the firewall, set up monitoring
    2. Compile and/or Install basic IMAP software – Dovecot (Ref.: Setting up Dovecot)
    3. Configure to become a back end IMAP server
    4. enable LDAP authentication.
    5. LDAP schema for users directly accessed by IMAP.
        A) Why not through PAM for password authentication
        B) MUST be direct for extra fields (is this true? Must be verified)
    6. Install the Sieve extension - filtering
    7. Enable IMAP Quota

4. *Expire NIREAS/IMAP only – keep NIREAS/SMTP for now*
    A) Reconfigure THEANO to proxy to the new IMAP back end (GORGO)
    B) Disable IMAP on NIREAS
    C) mail.cs.ucy.ac.cy should point to theano.cs.ucy.ac.cy
    D) MX records should remain as is (iolaos, nireas)

5. **GORGO – NewFiler/MailAlt – Optional Activity**
    1. Convert message store from maildir to mdbox by using dsync
        - This is sort of a backup process
        - TO actually make use of the /MailAlt requires the ability to individually set the location of message repositories

MILESTONE #1:

Successful operation of Dovecot as an IMAP server, proxy/director on theano and back end on gorgo means that PHASE I is finished and we have a complete usable IMAP mail environment based on the new objectives.

PHASE II: PRIMARY SMTP SET-UP (Expected Duration: 20 days)

6. THEANO – SMTP External Relay #1
    1. Enable SMTP services
        - A) (Compile), install and configure Postfix as a relay
        - B) Relay SMTP traffic to IOLAOS, NIREAS
        - *C) SPAM/VIRUS control – AMAVISD*
            - *I. AMAVISD*
            - *II. CLAMAV set up*
            - *III. SPAMASSASSIN set up*
7. GORGO - SMTP Internal Back End #1
    1. (Compile), install and configure Postfix as a back-end
    2. *Dovecot needs to be configured here to enable its LDA/LMTP to enable the LDA delivery and Postfix to make use of it*
    3. *Configure Sieve global filters to replace procmail*
    4. *Add new MX record with higher priority on GORGO*
    5. *Demote NIREAS MX record to a very low priority (MX priorities are now GORGO, IOLAOS, NIREAS)*
    6. *mail-out.cs.ucy.ac.cy (???)*
8. *THEANO – Reconfigure to Relay to: IOLAOS, GORGO now*

MILESTONE #2:

<u>Proper</u> operation of both SMTP relay #1 and SMTP back end #1 allows bringing the new systems on-line (with an additional MX record). It also allows, as second step, transfer of existing system (nireas, iolaos SMTP) functionality to the new systems. At this point NIREAS is free of mail services but kept as backup in case we discover problems.

PHASE III: SECONDARY GROUP IMAP SET-UP (Expected Duration: 15 days)

9. ELYSSO – IMAP proxy #2
    1. Install and secure the OS - CentOS
        - A) Iptables, fail2ban, secure at the firewall, set up monitoring
    2. Compile, install, configure basic IMAP software - Dovecot
    3. Enable IMAP proxy/director #2
        - A) Proxy to GORGO and IOLAOS for now
10. MIRTO – IMAP back end #2
    1. Install and secure OS - CentOS
        - A) iptables, fail2ban, secure at the firewall, set up monitoring
    2. Compile and/or Install basic IMAP software - Dovecot

    3. Configure to become a back end IMAP server #2
    4. Install the Sieve extension – user filtering
    5. enable LDAP authentication

11. *Expire IOLAOS/IMAP only – keep IOLAOS/SMTP for now*
    - *A) Reconfigure THENO, ELYSSO to proxy to the new IMAP back ends #1, #2 (GORGO, MIRTO)*
    - *B) Disable IMAP on IOLAOS*
    - *C) mail.cs.ucy.ac.cy should now point to theano.cs.ucy.ac.cy and elysso.cs.ucy.ac.cy*
    - *D) MX records should remain as is (gorgo, iolaos, nireas)*

PHASE IV: SECONDARY GROUP SMTP SET-UP (Expected Duration: 15 days)

12. ELYSSO – SMTP External Relay #2
    1. Enable SMTP services
        - A) (Compile), install and configure Postfix as a relay
        - B) Relay SMTP traffic to GORGO, IOLAOS
        - *C) SPAM/VIRUS control – AMAVISD*
            - *I. AMAVISD*
            - *II. CLAMAV set up*
            - *III. SPAMASSASSIN set up*
13. MIRTO - SMTP Internal Back End #2
    1. (Compile), install and configure Postfix as a back-end
    2. *Dovecot needs to be configured here to enable its LDA/LMTP to enable the LDA delivery and Postfix to make use of it*
    3. *Configure Sieve global filters to replace procmail*
    4. *SPAM/VIRUS control – AMAVISD*
        - *A) CLAMAV set up*
        - *B) SPAMASSASSIN set up*
    5. *Add new MX record for MIRTO*
        - *A) MX records priority now GORGO, MIRTO, IOLAOS*
        - B) *Remove NIREAS MX record (NIREAS is now dead for email. Thank you – more than 10 years of service!!)*
    6. *mail-out.cs.ucy.ac.cy (???)*
14. *THEANO – Reconfigure to SMTP relay to: GORGO and MIRTO now*

PHASE V:

MDBOX MESSAGE STORE CONVERSION, TUNING, SECURITY ENHANCEMENTS, FINAL CHECKS (Expected Duration: 20 days)

15. *Convert message store to mdbox message format*
    1. DSYNC – Replicate message storage to a secondary storage area
    2. *Enable “alternative” location for Dovecot*
16. Tuning of systems – Final Configurations – SMTP

1. *Remove IOLAOS MX record (IOLAOS is now dead for email)*

MILESTONE #3:

PHASE VI: The Further Work Phase

(Some of these actions are not in the Project Plan. Some are also noted for further investigation as a wish list))

17. *FURTHER ENHANCEMENTS*
    1. *Mailing lists management*
        - *A) csall etc*
        - *B) project mailing lists*
        - *C) ad-hoc mailing lists – user defined – announce*

          Current setup: mailing lists are directed to <list>@listserver.cs.ucy.ac.cy directly. This also works with theano for the time being since it uses the same virtual-users set up. (13/01/2014)
        - *D) Aliases – investigate how aliases can be used in cases where no real users are needed – ex. conferences where the email eventually goes to a real account or accounts (16/01/2014)*
18. *SPF record checking for incoming traffic on the SMTP relays.*
    1. *SPF DNS RR for cs.ucy.ac.cy*
    2. *SPF breaks .forward (!!) -- see how to fix with SRS or ditch SPF (!!)*
19. *Unresolved Issues on which no decision has been made*
    1. *pine on ADA*
    2. *caching DNS (on outgoing SMTP)*
20. Investigate *POLICYD for POSTFIX to battle the most nasty of SPAM and attack vectors. (16/01/2014)*
21. *Should there be internal MX records on in.cs.ucy.ac.cy (in which the internal mail servers are) such that forwarding from the relays but also transmission from internal systems like listserver can direct to local servers in a fault tolerant manner?*
22. how to solve the problem of external relays access to internal users so that we reject messages destined to non-existent users on the border NOT inside. (16/01/2014)
    1. *see postfix verify(8)*
23. *Full Text indexing support from Dovecot (27/01/2014)*
24. *Limit the number of messages a user can send*
    1. *smtpd_recipient_limit = 20 (;;)*
    2. *smtpd_recipient_overshoot = 10 (;;)*

Appendix: Activity Schedule

d – working day (estimate)

- Notes may need to be transferred to the user or admin manual
- **Where ever IMAP is mentioned we really mean both IMAP/POP3.**
- Yellow highlights contain issues that need to be revisited.

Official Start: 09/12/2013

Time	System	What	Notes	Done
PHASE I: PRIMARY IMAP SET-UP (+20d total)				
+3d	THEANO	- Install and secure OS with all already standard methods (see Linux install and security in wiki	Checked	11/12/2013
		- iptables, fail2ban, secure, firewall - check further the VLAN security	This should be revisited on the final check-out and in line with future DMZ mods.	11/12/2013
+7d	THEANO		Due to a problem with IOLAOS hanging at random:	
		- compile and install dovecot - Dovecot configuration as a front-end proxy #1 - configure IMAP proxy to NIREAS/IOLAOS based on user/group (50/50).	* this was slightly modified to go directly to gorgo which was already a live IMAP server also (see below) removing load from nireas and bypassing the unstable iolaos. Proxying is currently static and should be modified when the secondary IMAP is available.	12/12/2013 12/12/2013
			* also decided to redirect RC to theano to bypass the unstable iolaos as soon as the theano/gorgo IMAP couple are ready and as a testing ground.	12/12/2013
+10d	GORGO	- Install and secure OS with all already standard methods (see Linux install and security in wiki	Checked	12/12/2013
		- iptables, fail2ban, secure, firewall - check further the VLAN security	This should be revisited on the final check-out and in line with future DMZ mods.	12/12/2013
+15d	GORGO	- compile and install Dovecot 2.2.x	Checked	12/12/2013
		- Dovecot configuration as a back end #1	Checked	12/12/2013
		- enable LDAP authentication	* authentication is via SSSD/PAM to LDAP	12/12/2013
		- install the Sieve extension	* managesieve installed BUT cannot be used since proxying of this protocol MUSt be enabled on	12/12/2013 Proxying functional

		- install/enable IMAP quota - Test for stand alone operation -Test proper proxying from THEANO	THEANO-proxy – postponed until after installation of GORGO Checked Checked ** static proxying ** This should be changed when the whole system is in operation	on 16/01/2014 12/12/2013 12/12/2013 12/12/2013
Due to problems with IOLAOS being unstable decided to jump to PHASE II and postpone actions here until IOLAOS/SMTP is replaced. (12/12/2013)				
+18d	LDAP	- set up of LDAP mail schema (kekkos) - enable IMAP to receive user info from LDAP	** See temporary arrangement #1 below	16/01/2014
+20d	NIREAS	- reconfigure THEANO to proxy to the new GORGO/IMAP back end - expire NIREAS IMAP – keep NIREAS/SMTP - mail.cs.ucy.ac.cy should point to THEANO - MX remain as (iolaos, nireas)	Checked postponed postponed MX (see also below)	12/12/2013 06/02/2014
+22d	GORGO/ NewFiler	- convert message store from maildir to mdbox by using dsync manually - this is actually a backup process on the message store level - NOTE: using the mail alt feature of Dovecot requires the ability to individually set the message location - This is experimental at this stage and meant to test the concept		
MAILSTONE #1: TEST all above functionality for • dovecot proxying • dovecot operation • quota • sieve • LDAP schema • conversion from maildir to mdbox Completed at 27/01/2014 except 1. LDAP schema 2. conversion from maildir to mdbox which is postponed for later due to urgency with IOLAOS.				
PHASE II: PRIMARY SMTP SET-UP (+20d total)				
+27d	THEANO	- Enable SMTP services	Checked	13/01/2014

		- Compile, install, configure Postfix as a relay #1 - relay SMTP traffic to IOLAOS, NIREAS - install, configure AMAVISD to do CLAMAV, SPAMASSASSIN scans	Checked Due to problems with IOLAOS, GORGO was set up to replace it (see below) and relaying is to GORGO. Note: 1) relaying is done on internally destined traffic, other traffic is sent to its destination 2) TLS v.1 (STARTTLS) has been enabled also for SMTP auth. 3) Relaying is done suign the LMTP protocol	13/01/2014 13/01/2014 OK
+32d	GORGO	- enable SMTP services - compile install, configure Postfix as SMTP Internal back end #1 ** enable Dovecot LDA/LMTP (required for delivery to message store by Postfix) – change from PROCMAIL - add new MX record with higher priority than NIREAS	Checked Checked Checked Note: 1) PROCMAIL is not enabled. Sieve installed but not verified. 2) aliases and virtual users (ex mailing lists need to be properly set up as per existing method) Sieve/Managesieve -Sieve installed - managesieve proxying from theano checked - clients enabled ** further configuration and tuning possible with sieve plug ins etc added MX weight 300 for theano which is the lowest priority. This should be changes eventually. MX for theano (mail3) now 150 (between IOLAOS and NIREAS).	13/01/2014 13/01/2014 13/01/2014 Checked 06/04/2014 16/01/2014 17/01/2014 06/02/2014
+34d	NIREAS	- Demote NIREAS MX record to least priority ** MX priorities are now ~~GORGO~~ THEANO, IOLAOS, NIREAS	Theano 100 iolaos 100 nireas 200	11/02/2014
+36d	DNS	Mail-out.cs.ucy.ac.cy this should be obsoleted eventually and just use mail.cs.ucy.ac.cy which should point to theano, elysso.		
+40d	THEANO	- reconfigure to relay to IOLAOS, GORGO	This was changed at +7d to bypass IOLAOS	27/01/2014
MILESTONE #2				

Test all above **- at this stage we have a complete system (IMAP/SMTP services) except the fault tolerant part** - complete functionality testing is done here. - SMTP delivery - IMAP proxying - IMAP and SMTP back ends - sieve/managesieve (including proxying) - LDAP schema working - auxiliary systems (quota, sieve) **- begin writing the user manual**				
PHASE III: SECONDARY IMAP SET-UP (+15d total)				
+43d	ELYSSO	- Install and secure OS with all already standard methods (Linux install and security in wiki - iptables, fail2ban, secure, firewall - check further the VLAN security		28/01/2014
+45d	ELYSSO	- compile and install dovecot - configure IMAP proxy #2 to GORGO/IOLAOS based on user/group (50/50).		
+50d	MIRTO	- Install and secure OS with all already standard methods (Linux install and security in wiki - iptables, fail2ban, secure, firewall - check further the VLAN security		
+52+	MIRTO	- compile and install Dovecot 2.2.x - Dovecot configuration as back end #2 - enable LDAP authentication - install the Sieve extension - install/enable IMAP quota		
+55d	IOLAOS	- expire IOLAOS/IMAP - reconfigure THEANO, ELYSSO to proxy to the new IMAP back ends #1 #2 (GORGO, MIRTO) - DISABLE IMAP on IOLAOS		
+55d	DNS	- mail.cs.ucy.ac.cy should now point to theano.cs.ucy.ac.cy and elysso.cs.ucy.ac.cy - MX records should remain as is (GORGO, IOLAOS, NIREAS)		
PHASE IV: SECONDARY SMTP SET-UP (+15d total)				
+57d	ELYSSO	- SMTP External Relay #2 - Enable SMTP services - Compile, install, configure Postfix as a relay #2 - relay SMTP traffic to GORGO, IOLAOS - install, configure AMAVISD to do CLAMAV, SPAMASSASSIN scans	Checked Checked. IOLAOS not used. Relaying to GORGO only. Checked.	11/02/2014
+60d	MIRTO	- Internal Back end #2 - enable SMTP services - compile install, configure Postfix as SMTP Internal back end #2 - ** enable Dovecot LDA/LMTP		

		(required for delivery to message store by Postfix) – change from PROCMAIL		
+65d	DNS	- add new MX record for MIRTO - MX records now: GORGO, MIRTO, IOLAOS - remove NIREAS MX record **(NIREAS now dead!!)** - mail-out.cs.ucy.ac.cy (???)		
+70d	THEANO	- reconfigure to SMTP relay to GORGO, MIRTO		
PHASE V: NewFiler and MDBOX change (+10d)				
+75d	GORGO MIRTO	- Dovecot dynamic synchronization (DSYNC) - test manual synchronization for proper operation (from - set up DSYNC for on line synchronization (		
+78d	GORGO MIRTO	- make use of newfiler instead of hermes NFS		
+80d	DNS	- remove MX record for IOLAOS (ioloas now dead for email)		
PHASE VI: Additional Work – Tuning (+10d)				
+83d		Postfix Policyd		
+85d		Mailing list management		
+88d		Dovecot mail alt feature		
+90d		SPAM config with outside SPAM DBs		

RC – Roundcube

Temporary Arrangements

1. In order enable delivery to aliases/groups/lists the current set-up of /etc/mailalaises was transferred to theano/gorgo. This enables us to check other aspects of the system before setting up new systems like LDAP for this. This will be changed once a final decision is made on how to reconfigure this part. (rsync from iolaos) (16/01/2014).

Appendix B: Bugs and unresolved issues

This catalogs issues and bugs (of lesser importance than the actual project) that need to be resolved.

No.	Date	Issue	Notes	Resolved
001	13/01/2014	Theano - postfix (2.10) does not stop/start properly on reboot – not in chkconfig --list		31/01/2014
002	13/01/2014	Jan 13 16:32:07 theano postfix/tlsmgr[4179]: warning: request to update table btree:/var/spool/postfix/smtpd_tls_cache in non-postfix directory /var/spool/postfix Jan 13 16:32:07 theano postfix/tlsmgr[4179]: warning: redirecting the request to postfix-owned data_directory /usr/local/var/lib/postfix		
003	13/01/2014	11117561 3069 Mon Jan 13 17:35:26 andreas.kasenides@cs.ucy.ac.cy (host gorgo.in.cs.ucy.ac.cy[10.16.1.113] said: 550 5.1.1 <junkone@cs.ucy.ac.cy>: Recipient address rejected: User unknown in local recipient table (in reply to RCPT TO command)) junkone@cs.ucy.ac.cy	Fix relays (theano) so that they do not accept/forward mail for non existent users.	
004	16/01/2014	/usr/local/etc/postfix/bounce.cf should be fixed on internal servers to not advertise *.in.cs.ucy.ac.cy systems when bouncing non-deliverable messages ** should we also examine the bounce system also		
005	20/01/2014	Jan 20 03:38:35 theano postfix/smtpd[25502]: warning: dict_nis_init: NIS domain name not set - NIS lookups disabled	??	
006	24/01/2014	Should we create a separate filesystem (LV) for /var/spool/amavis? This is used as a quarantine space and potentially can be overflown with the result of the OS becoming unavailable (filling /var)		
007	28/01/2014	Fine tune iptables. Ssh should be allowed only from some hosts (/etc/hosts.allowed etc)		
008	30/01/2014	Jan 30 10:29:01 theano dovecot: imap-login: Debug: Ignoring unknown passdb extra field: nopassword Jan 30 10:29:01 theano dovecot: imap-login: Invalid certificate: self signed certificate: /OU=Computer Science Department/CN=mail.cs.ucy.ac.cy/emailAddress=postmaster@cs.ucy.ac.cy		
009	31/01/2014	Protection of internal mailing lists	/usr/local/etc/postfix/access needs to be checked again	

			and fine tuned	
010	31/01/2014	With Postfix >2.10 there is also smtpd_relay_restrictions in addition to smtpd_recipient_restrictions. Since theono/elysso are actually relays we need to look at this change more carefully		
011	09/02/2014	Currently over quota rejection happens at the back end systems (gorgo, mirto with overquota.users) which is not ideal. This can be improved by rejecting at the relay instead. Makes no sense to accept message for user just to find out at the back end that he/she is over quota. See http://sys4.de/en/blog/2013/04/08/postfix-dovecot-mailbox-quota/		
012	11/02/2014	Consider nullmailer to replace postfix set up on machines doing send only.		