STATISTICS DENMARK

Statistics Norway
Statistisk sentralbyrå

SCB Statistiska centralbyrån
Statistics Sweden

MOZ:2002:6

Establishing a Permanent Internet connection at INE

Report from a short-term mission

September 16th – October 11th 2002

Niels Jespersen

TA for the 'Bridging Support Program to Strengthen the Institutional Capacity of the National Statistics', Mozambique

Instituto Nacional de Estatística

This report contains
restricted information
and is for official use only.

Ref. no. 104.Mozambique.1-5

October, 2002

Niels Jespersen
Statistics Denmark
Sejrogade 11
DK-2100 Copenhagen O
Denmark

njn@dst.dk

Phone: +45 39173585, Mobile +45 405223

TABLE OF CONTENTS:

1 EXECUTIVE SUMMARY

INE has been interested in connecting to the Internet for an extended period of time. The interest is the result of a wish to be able to communicate in a timely manner with users, partners and customers.

During the mission Internet email and Internet browsing was established for INE staff. Additionally a number of other Internet related activities took place, including providing tools for analyzing Internet usage and for connecting external email clients to read INE mail.

Furthermore the system administration practices of INE were analyzed throughout the mission, and a number of specific recommendations for large and small improvements in this area have been provided to technical staff at INE. Initial work on implementing some recommendations has been initiated in cooperation with INE staff. An improved automated backup procedure is the main example of this activity.

An activity not planned ahead was the recovery work after a serious breakdown of the main server. The server broke down immediately after a consultant from a system vendor installed new disk capacity. All content of the server was lost and had to be restored from backup tape. The recovery work took one full day and caused problems needing immediate attention for several days afterwards.

A consequence of being connected to the Internet is that the INE network is now becoming a very critical resource of INE.

One obvious problem that can seriously impact the future success of the network is staffing. This problem is existing in terms of the amount of manpower needed and also in terms of skills of the available manpower.

The general recommendations in section 4.1 are given on background of INE's 5 year strategy. Important recommendations are to provide training for the system administration staff as well as obtaining external assistance in the interim period until staff is up to level on advanced system administration.

In addition to the general recommendations, specific Internet related and system administration related recommendations are given in section 4.2 and 4.3.

2 INTRODUCTION

INE has been interested in connecting to the Internet for an extended period of time. The interest is the result of a wish to be able to communicate in a timely manner with users, partners and customers worldwide.

There have been several attempts to establish a permanent connection in recent years. The attempts have been in the form of design suggestions combined with the intent of implementing these on a short time mission.

During the period when the long term Consultant Mogens Grosen Nielsen was preparing to travel to Mozambique, the issue of a permanent Internet connection was raised from INE. The matter was discussed within IT-Center of Statistics Denmark. The outline of a secure, viable, and sustainable design was developed and discussed with INE. The resulting design paper that formed the background for the Terms of Reference for the mission is attached as ANNEX 3.

The main deliverable of the mission is Internet mail to all staff at INE in Maputo, to separate mail to provincial offices of INE from INE Maputo, and web access to approximately 50 selected staff at INE, Maputo. The solution is secure and the installation is thoroughly documented for the purpose of future maintenance. A workshop was held during the final week of the mission where IT-staff was introduced to the detailed workings of the system.

Finally, the mission provided specific advice on selected areas of Network and System Administration. The areas selected have been chosen in cooperation with INE Network Administration staff.

3 ACTIVITIES DURING THE MISSION

According to the terms of reference for the mission, these activities were carried out as the main parts of establishing the full Internet connection:

1. Implementing Internet mail securely for all staff at INE.
2. Implementing capability for browsing the web securely for approximately 50 selected staff members.
3. Changing Regional mail-addresses to a new form: ine.regionname@delegacao.ine.gov.mz

Furthermore, these Internet related activities took place:

4. Implementing a system for analyzing the usage of web browsing on a daily basis.
5. Providing an internal technical workshop detailing the system for IT Staff.
6. Providing documentation of design, installation and operation of the Internet system.
7. Making it possible to access INEs mail system from outside the internal INE network.

The system administration practices of INE were analyzed throughout the mission, and a number of specific recommendations for large and small improvements in this area have been provided to technical staff at INE.

Initial work on implementing some recommendations has been initiated in cooperation with INE staff. An improved automated backup procedure is the main example of this activity.

An activity not planned ahead was the recovery work after a serious breakdown of the main server. The server broke down immediately after a consultant from a system vendor installed new disk capacity. All content of the server was lost and had to be restored from backup tape. The recovery work took one full day and caused problems needing immediate attention for several days afterwards. Because of the time consumed for disaster recovery, it was agreed with INE to prolong the mission with one week.

4 CONCLUSIONS AND RECOMMENDATIONS

4.1 GENERAL RECOMMENDATIONS

The network at INE has been in operation for approximately three years and a lot of useful statistical work has been accomplished using the resources that the network provides. INE is now connected to the Internet as this will enhance the speed of communication between INE and its users and customers. A consequence of this improvement in service is that the INE network is now fast becoming a very critical resource of INE. The network is becoming the backbone of INE operations. The breakdown on October 2nd showed this very clearly as highly important email was unavailable during the breakdown.

One obvious problem that can seriously impact the future success of the network is staffing. The quarterly reporta of the twinning projects already have described this problem of staffing at the DISI. As the installation is growing more complex with the Internet connection and with future developments, this problem is very much intensified in terms of the amount of manpower needed and indeed also in terms of skills of the available manpower.

The overall objective on IT according to the 5 year strategy is to make the production of statistics more efficient, to reduce the costs and to improve the quality of the service and the quality of the working processes[1]. The goal is to establish a system architecture via establishing a well-functioning Local Area Network, including well established security measures, standardization on hardware and software, and on system development. Further the strategy emphasizes development of Internet and Intranet. Finally training is emphasized as an important aspect in order to ensure, among other things, a sustainable and smooth human resource situation at INE.

This shows that the network must remain a smooth and efficient IT-base in the future, and that the operation and development must be given high priority.

The recommendations in this report only focus on establishing the network and the related security and training measures. Recommendations for initiatives that can be decided and initiated immediately are given below:

General recommendation 1: A conservative installation and upgrade strategy should be decided.

Installation of new software and upgrading existing software is a resource demanding activity both in terms of manpower and money. It should therefore be decided to carefully consider each new software product introduced and each upgrade contemplated in terms of value added and resources spent. Specifically, the basis of NT on workstations and servers should not be upgraded during 2003, as the upgrade to Windows 2000/XP is very manpower and planning intensive compared to the value gained.

General recommendation 2: System administration staff should consist of at least two persons.

The day to day tasks of operation of the network add up to more work than one person can accomplish. Furthermore, system administration is very vulnerable in being dependent on only one person. Consequently, at least two persons should be assigned to the work area. Of these, at least one should be an experienced system administrator.

[1] Plano Estrategico do Sistema Estatistico Nacional 2003-2007, section 4.6

General recommendation 3: Training should be provided to system administration staff

The skill set of system administrators need to be widened and deepened as the installation gets more complex. The methods of choice for bringing the proper training to the staff is the set of training courses in Microsoft Technologies that lead to the acknowledged MCSE certification. MCSE is short for Microsoft Certified System Engineer. The training should be given to the two persons assigned to system administration. MCSE comprises x courses which are offered in Maputo??. The training will take up to a year to complete in the staff's free time, but value will be apparent shortly after the training is initiated.

General recommendation 4: External support should be secured until internal staff is up to speed.

The training will provide more and more value as the courses progress, but until the time when the staff is up to speed with all day to day tasks of operating the network, external support should be secured. Tasks that should be included in the support agreement include: Exchange configuration and administration, General network troubleshooting, Advanced NT system administration, Advice on automating common tasks.

General recommendation 5: Prepare disaster recovery plan

As the network at INE gets to be a critical resource for producing statistics, the consequences of losing this resource get more serious. Outages and breakdowns can be minimized but not avoided altogether. To minimize consequences and duration of smaller and larger breakdowns, INE should have a disaster recovery plan. Such a plan should cover disasters ranging from broken hardware such as the firewall connecting INE to the Internet to big disasters such as fires in the server room. Questions like "Did you store all backups in the server room during the fire? Sorry, INE is out of business!" are better asked **before** the fire. This plan should be revised regularly and also tested regularly for viability.

General recommendation 6: Problem solving guidelines.
In order not to solve the same problem twice and to facilitate structured accumulation of knowledge, it is suggested to introduce "problem solving guidelines". An example of a problem solving guideline could be "How to connect my Outlook-Express client at home to read INE mail?".

The outline of a guideline could comprise the following parts: short problem description (how, when and by whom was the problem encountered). Problem resolution (description of steps that solves the problem). Possible workaround (description of how to continue with an alternative solution of the problem).

The description of problem solving guidelines should start immediately. One person should be responsible for adding and updating descriptions. The guidelines should be published on the Intranet in two categories: One for guidelines that describe problems affecting end-users and one for guidelines that are relevant to administrators only.

General recommendation 7: Modernize INEs Antivirus solution.

The network border between the INE network and the Internet has been secured against virus attacks in the Internet part of the mission. Antivirus software is employed on workstations and servers today in order to guard against viruses entering from the inside via diskettes and cdroms. But the software is old and does not support a centralized administration. It should be seriously considered to implement new antivirus software on workstations and servers in order to guard properly against viruses and other malignant software..

4.2 RECOMMENDATIONS RELATED TO FULL INTERNET

ANNEX 4 details the conclusions and recommendations in the area of the Internet connection. The recommendations are summarized below:

Internet Recommendation 1: It is recommended that outages are logged in a manual log file with information about time, duration and possibly reason for the outage. This log will form the necessary material for evaluating the service provided over a period.

Internet Recommendation 2: It is recommended that adding an external mail backup service is seriously considered. This requires the cooperation of a service provider, who will agree to accept incoming mail to ine.gov.mz, whenever the service at INE is unavailable to the public Internet. When mail service at INE is restored, mail will be forwarded automatically from the service provider to INE.

Internet Recommendation 3: Modems formerly used to facilitate dialup access to external mail should be retired from service after the users of the modems have had time to empty their external mailboxes.

Internet Recommendation 4: The web-site should for the time being stay hosted at Teledata. When and if the site develops into a dynamic database driven site, this decision should be reconsidered. It should be considered already today to contact Teledata in order to get log files of incoming traffic to www.ine.gov.mz in order to analyze usage patterns.

Internet Recommendation 5: The future need to access Exchange from the outside should be considered and evaluated with regard to the added complexity and operational cost of a fully configured Outlook Web Access solution.

Internet Recommendation 6: Add memory to the Proxy machine to at least 256 MB in order to improve the performance of web access.

Internet Recommendation 7: Create a list of recurring operational tasks, and add to that list a monthly task of checking the current version of operating systems and server applications against the current list of fixes from the vendor.

Internet Recommendation 8: It should be considered whether the user-friendly “Out-of-Office” messages should be delivered to the outside.

Internet Recommendation 9: After a period of a few months, the size limitation of one megabyte on mails should be reconsidered based on experience.

4.3 RECOMMENDATIONS RELATED TO SYSTEM ADMINISTRATION

ANNEX 5 details the conclusions and recommendations in the area of specific system administration issues. The recommendations are summarized below:

Administration recommendation 1: Backup procedures should be fully automated and documented. A backup policy should be formulated.

Administration recommendation 2: Monthly reporting of operational incidents should be introduced.

Administration recommendation 3: For administrative reasons the printing model should be systematically changed to Windows printing with central print queues.

Administration recommendation 4: The use of drive letters and access permissions for network files should be standardized.

5 References and the "INE Internet Connection CD"

The following links point to web sites of the vendors whose products are used in the Internet Connection.

- Caching web-proxy software: www.squid-cache.org
- Virus checking web-proxy software and mail relay software: www.antivirus.com
- Technical support for antivirus: solutionbank.antivirus.com
- Firewall support: www.multitech.com
- Exchange Server: www.microsoft.com/exchange
- Webalizer: www.webalizer.org

The following software, documentation and configuration files have been provided on two copies of the CD labeled "INE Internet Connection CD":

- The documentation for the installed connection at INE:
  - Design-of-internet-connection.doc (9 pages)
  - Installation-and-configuration-of-internet-connection.doc (49 pages)
  - Operation-of-internet-connection.doc (10 pages)
  - End-user-considerations-with-internet-connection.doc (10 pages)
- This draft report.
- Relevant patches for Microsoft Exchange 5.5
- All current documentation for the Multitech Firewall.
- The eicar.com virus for testing antivirus with a harmless virus.
- The InterScan Viruswall software, documentation and configuration file.
- The squid software, documentation and configuration files.
- Script files used in operational procedures.
- The Webalizer software and configuration files.

ANNEX 1 Terms of Reference for the mission

A.1.1 Background

The overall reason for establishing an Internet Connection is to facilitate communication between INE, users and producers of statistics[2]. The National Institute of Statistics has twenty-four dial-up accounts for internet connection. 13 at INE HQ and 11 in the provincial delegations. At HQ, INE has about 130 computers situated on four different floors, connected in a network. The network operating system is NT Server 4.0 with the majority of clients running NT Workstation 4.0 and a few workstations running Windows 98 based on the TCP/IP protocol. An upgrade from Office 97 to Office 2000 is currently taking place. The internal e-mail is handled by Microsoft Exchange 5.5. Part of the environment is also two databases, Live Data Base that is based on SQL 2000 and Childinfo that is based on Microsoft Access.

INE has an Intranet in place since August 2000. The software used for the web server is Microsoft Internet Information Server 4.0. The INE Web site is currently hosted at Teledata. It is about 20 MB and has about 2,000 visitors a month.

The idea is that INE should have a permanent connection to the internet which would provide all users in the network with internet e-mail and internet browsing. Later on INE would also host its own web site. The technology used will be cable connection from the company NetCabo.

A.1.2 Main reasons for the mission

The main reason for the mission is to get knowledge from outside INE on establishing and configuration the Internet Connection, since INE does not have the technical capacity to do that including the security implications that follows.

A.1.3 Benefactors of the mission

Having external e-mail will benefit all INE HQ staff with external relations. The possibility of browsing the Internet will benefit statisticians and IT support staff.

Also the external users and producers will benefit from better communication facilities.

A.1.4 Objectives of the mission

The main objective of the mission is for INE Headquarters to have a computing environment permitting INE sending Internet e-mail and Internet browsing by means of a permanent internet connection.

A secondary objective is to train the technical staff sufficiently in order to maintain this environment.

A third objective is to give advice on specific network administration issues (configuration, performance, operation, security etc) in order to ensure a smooth and efficient IT-base for production of statistics and administration tasks at INE.

A.1.5 Expected results

[2] Section ”4.6 Sistemas e Tecnologias de Informacão” in “Plano Estrategico de Sistema Estatistico Nacional 2003-2007” contains general ideas on the strategic of use of information technologies. Section 4.6.5 stresses Internet as an important technology in improving communication.

1. A system that enables INE users to send and receive internet e-mail and browse the World Wide Web.
2. Workshop, including written material on the implemented solution
3. Documentation of the system established for permanent Internet Connection
4. Report on specific network administration issues and implementation of selected recommendations
5. Final report (draft version)

A.1.6 Work to be carried out by the consultant during the mission

The work during the mission consists of a major part (A) and a minor part (B). The major part consists in establishing a permanent Internet-connection and the minor part consist in giving advice on specific network administration issues (performance, configuration, security etc.).

A. Establishing a permanent Internet-connection

1. 1. Configuration, testing and connecting firewall securely to INE network and Internet provided by NetCabo.
2. Test new delegacao.ine.gov.mz mail domain with Teledata.
3. Installation and testing of proxy/mail relay machine.
4. Configure Exchange for accepting and sending Internet mail.
5. Move main ine.gov.mz mail domain from Teledata to INE.
6. Provide onsite training/workshop for INE technical staff.
7. Plan operations including backup/restore and log handling with INE.
8. Provide documentation of all other activities.

Appendix A gives a detailed description of the activities.

B. Advice on specific network administration issues

This activity includes security strategy: how to best configure for at good security including back-up models. Configuration: what system policies to use in order to get a more or less equal environment for all. Performance issues.

This activity includes Security Strategy: how to best configure for at good security including back-up models. Configuration: what system policies to use in order to get a more or less equal environment for all. Performance issues e.g. advice on measurement of internal usage of the Internet.

The final list of issues to be included should be agreed upon as part of the mission.

The use of Internet as a communication tool aims at improved data quality – especially timeliness and accessibility. The use of Internet (including improvements in network administration) also aims at improving TQM values. Especially “focus on clients” and “orientation towards processes”. E.g. e-mail can be used to facilitate the communication with respondents and users of statistics.

A.1.7 Agenda for the mission

Introductory meetings with INE staff

1. Implementation of activities listed above
2. On the job training
3. Workshop. The workshop includes a theoretical and practical part. The theoretical part covers areas such internet mail, internet web, anti virus programs, techniques for troubleshooting

network applications etc. The practical part covers training in how to configure and operate the firewall, discussions of settings etc.
4. Informing users on how to use internet mail and internet web

A.1.8 Tasks to be done by INE to facilitate the mission

Before mission:
1. Acquisition of all needed hardware and software.
2. Sign contract with NetCabo that assures physical installation of cables and cable modems
3. Inform Teledata and NetCabo about eventual changes of the primary DNS-server for ine.gov.mz
4. Inform Teledata about the need to change the e-mail addresses of the provincial delegations
5. Identify which users that will have access to internet e-mail and web surfing.
6. Have a clear policy on the use of the Internet.
7.

During mission:

1. Keying in e-mail addresses for users.
2. Configuration of selected PC's to use the internet connection
3. Support – information and documentation of the infrastructure etc.

After the mission

1. Follow up of the recommendations of the mission. Maintain and administer of the new hardware and software. Give internal training to the INE users.

A.1.9 Name(s) of Consultant(s) and Counterpart(s)

Consultant: Sr. Niels Jespersen, Statistics Denmark
Counterpart is the Network Manager, Sr. Salomão Muianga.

A.1.10 Timing of the mission

Three weeks (September 16, 2002 – October 3, 2002)

A.1.11 Finalization of the report

The consultant will prepare a draft report to be discussed with INE before leaving Maputo. He/she will submit a final draft to INE for final comments within one week of the end of the mission. Statistics Denmark as Lead Party will print the final version within 3 weeks of the end of the mission.

These Terms of Reference were prepared by (date and name)
18 /09 /20002 Anastásia Judas Honwana

Approved by/in the name of the President of INE (date and name)
18/09 /20002 Luis Mungamba

ANNEX 2 Persons met during the mission

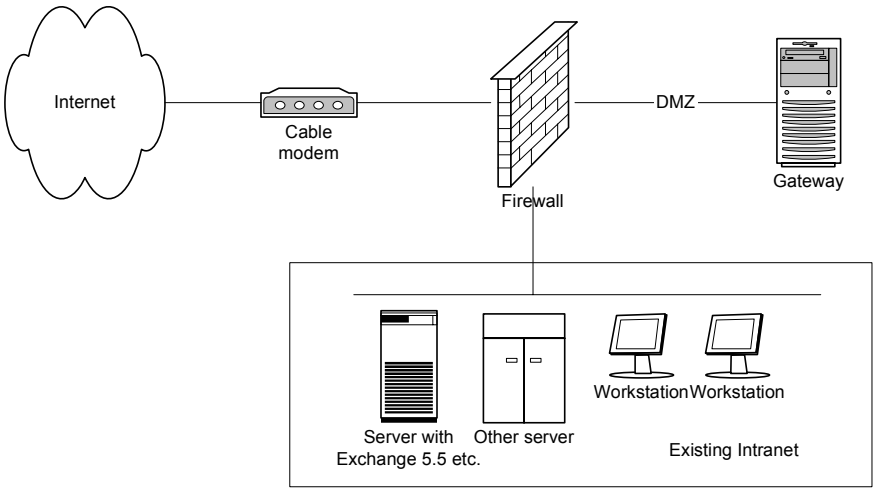
- Dr. João Dias Loureiro, Presidente do INE.
- Mr. Luis Mungamba, Director Adjunto DICRE.
- Ms. Anastásia Judas Honwana, Head of IT.
- Mr. Salomão Muianga, Network Manager.
- Mr. Milagre Mula, Programmer
- Mr. Eugenio Matavel, Programmer
- Mr. Calado Fijamo, Programmer
- Mr. Hans Erik Altvall, Consultant, Coordinator.
- Mr. Bo Yttergren, Consultant.
- Mr. Mogens Grosen Nielsen, Consultant

ANNEX 3 Design of Permanent Internet connection at INE

A.3.1 Specification of architecture and functionality

A.3.1.1 Hardware- and network-architecture

The architecture is based on best practices in network security design:
- No Internet traffic goes directly to the Intranet.
- Firewall placed to separate network in security zones.
- All allowed traffic will be scanned for virus.



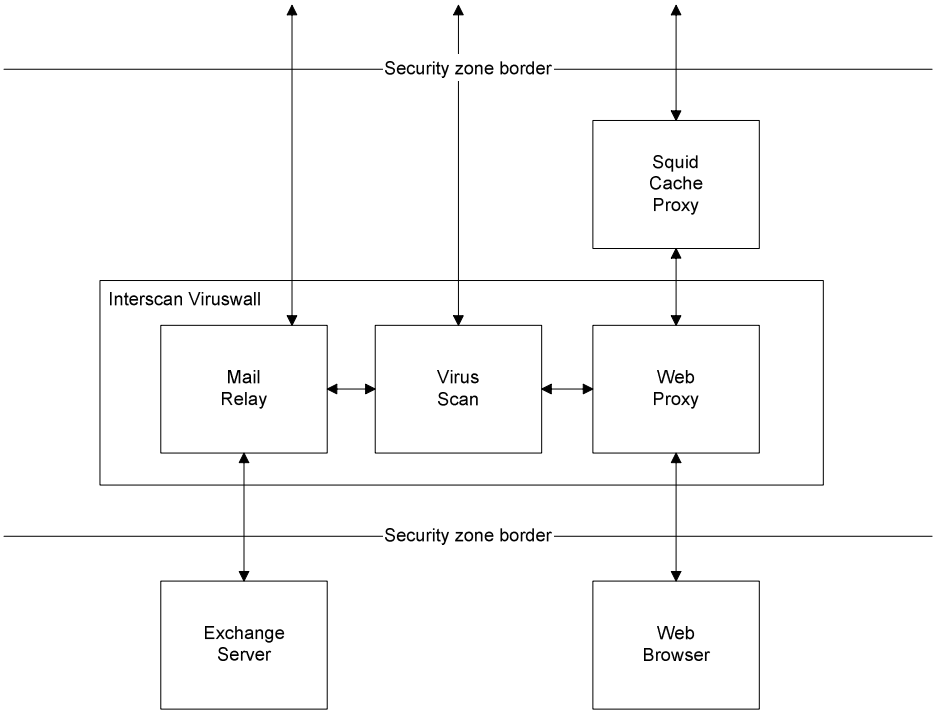
The architecture is centered on a firewall in the form of a hardware appliance to separate the net in three different security zones: Internet, DMZ and Intranet. Traffic only flows between zones according to specific rules set up in the firewall. See for detailed description.

The machine providing external mail relay (with built in virus scanning) and proxy access for web access (with built in virus scanning) is placed in the DMZ. All INE servers and workstations are placed on the Intranet segment.

The IP-addresses on the Intranet and DMZ are private (RFC1918-compliant). Only the external interface on the firewall and the cable modem need public IP-addresses. The firewall will perform the necessary Network Address Translation (NAT) to make access from Internet to DMZ and from Internet to DMZ possible.

A.3.1.2 Software-architecture

The software architecture of the solution is based on a gateway solution, where mail traffic and web traffic can be scanned for virus and other malignant files. The different components in the solution communicate with each other and the security zones according to this diagram:



– The web browser, who wants a file from the Internet zone, connects to the web proxy component who in turn delivers the request to yet another proxy who forwards the request to the final destination.
– When the reply comes along through the outermost proxy, the first web proxy sends it to virus scanning. After virus scanning, the reply goes to the browser.
– Incoming mail goes through the mail relay, which performs some mail related content checking, after which the mail is virus scanned. After virus scanning the mail is delivered to the Exchange server for final delivery.
– Outgoing mail goes from the Exchange server to the mail relay. After virus scanning and other checks, the mail is delivered to the outside world.
– The virus scanner periodically collects updates to its virus definitions.

Security Issues

The firewall shall be managed by one pc on the Intranet by using a browser. The configuration of the firewall must be such that only this one pc can do management functions.

The gateway must accept mail relaying for only ine.gov.mz. Relaying for any other domains must be turned off.

DNS and other issues

MX Record for ine.gov.mz must point to external IP of firewall. NetCabo should perhaps be consulted for the possibility for them to provide mail-backup. DNS Resolver for gateway and firewall must be set to addresses of two NetCabo provided DNS-servers.

A.3.1.3 Hardware components

Id	Description	Comment
HW.1	MultiTech RF650VPN Firewall	Delivered by INE. Already procured.
HW.2	PC Hardware for Gateway	
HW.4	UPSes for Firewall, Gateway	

A.3.1.4 Software components

Id	Description	Comment
SW.1	Interscan VirusWall 3.52 for Windows NT/2000	Amount of licenses to be decided. Software can be bought from SecureData in South Africa (reseller). Can be brought by DSt from Danish reseller.
SW.2	Squid 2.3 STABLE 5	Delivered by DSt
SW.3	Windows NT/2000	Delivered by INE
SW.4	Microsoft Exchange 5.5	Delivered by INE. Software already installed and running. Installation CD (plus appropriate Service Packs) is needed to install Internet Mail Connector

ANNEX 4 RECOMMENDATIONS RELATED TO FULL INTERNET

The necessary changes to the Microsoft Exchange mail system did cause some unplanned difficulty, which required some additional time to resolve. The mail system was fully operational internally during the period of change dating from Wednesday September 18th through the weekend to Monday September 23rd. Specifically the new Internet Mail Service in Microsoft Exchange needed updating from the initially installed version 5.5SP4 to hotfix Q289258. This upgrade fixed stability problems within the Internet Mail Service of Exchange.

The modifications needed to facilitate the changes for the mail provided for the regional offices of INE was delayed due to problems getting changes done within Teledata, the service provider that will provide mail to the regional offices in the future. After several telephone calls and several visits at Teledata headquarters, a competent technician was located. He quickly performed the changes during a telephone conference.

The design of the proxy solution was modified as a result of the added activity 10 mentioned in section 3. The modified architecture consists of one squid proxy performing caching and detailed logging for analysis purposes. This proxy forwards requests to the virus scanning proxy which in turn forwards requests to a second squid proxy. This proxy does not provide logging or caching at all, but collects content directly from the internet.
After the installation of the permanent Internet connection, a number of issues requiring consideration have been identified. Some of these have come up as a result of the experiences of the operation of the solution, while others are issues that need to be considered as a consequence of the changed network environment.

A.4.1 Stability of the cable connection:

The experience with the NetCabo Cable connection during the first week is that short disruptions of service do occur a few times during the week. Some times, the service is down for no apparent reason, other times it can be explained by power failures in the city. When Internet service is down, it will immediately affect staff browsing. Mail is more resilient toward outages, as outgoing mail is queued at INE and incoming mail is queued at the sender. The queuing will usually take care of outages of up to at least one hour's duration.

Recommendation 1: It is recommended that outages are logged in a manual log file with information about time, duration and possibly reason for the outage. This log will form the necessary material for evaluating the service provided over a period.

A.4.2 Adding mail backup at a Internet Service Provider

Internet mail will with almost certainty quickly become critical to the communication from staff at INE to/from communication partners around the world. The need for smooth mail delivery will increase as a result of this. The solution established during this mission requires the permanent connection of the Exchange Server to the Internet. As mentioned above, short outages of Internet service will not influence operations of mail, but outages of several hours will cause mail to bounce and not be delivered.

Recommendation 2: It is recommended that adding a mail backup is seriously considered. This requires the cooperation of a service provider, who will agree to accepting mail to ine.gov.mz, whenever the service at INE is unavailable to the public Internet. When service is restored, mail will be forwarded automatically from the service provider to INE.

A.4.3 Remove dialup capability from workstations connected to the INE network.

Formerly, several staff has had Internet access by using a modem connected to their workstation on the INE network. As these members of the staff now have direct Internet access, there is no continued need for dialup access. The new Internet connection implements a security separation of the internal network from the Internet, and consequently continued dialup access will breach this separation.

Recommendation 3: Modems formerly used to facilitate dialup access to external mail should be retired from service after the users of the modems have had time to empty their external mailboxes.

A.4.4 Moving INEs web-presence in-house

The new Internet solution makes it very easy to in-source the web-site of INE (www.ine.gov.mz). This would require only a modest machine as a web server and a very few adjustments to the firewall. However the benefits of a possible move should be considered carefully before making any decision in this matter. The stability of the cable connection is an important aspect to consider, as is the burden of administrating the web server and keeping it updated with security patches. On the other hand, if the website at some time in the future will be connected to a live database, then it will make a lot of sense to have the site in-house.

Recommendation 4: The web-site should for the time being stay hosted at Teledata. When and if the site develops into a dynamic database driven site, this decision should be reconsidered. It should be considered already today to contact Teledata in order to get log files of incoming traffic to www.ine.gov.mz in order to analyze usage patterns.

A.4.5 Access to mail at INE from outside INE

During the mission, the requirement for staff to be able to access their Exchange mailbox from the Internet outside INEs internal network was added to the Terms of Reference. There are several possibilities for allowing external access to mailboxes within INE. For security reasons, full access via Outlook should not be given. Full access to Exchange can be given via web by installing Outlook Web Access at INE. This gives a smooth web interface to Exchange, but requires substantial reconfiguration of the Exchange system. A more basic access can be given by allowing clients to connect Outlook Express to INE mail via the IMAP and/or POP3 protocol. IMAP provides full access to mail folders where POP3 only gives access to the Inbox. Outgoing mail will be delivered through the Internet provider, which the staff member is connected to.

Recommendation 5: The future need to access Exchange from the outside should be considered and evaluated with regard to the added complexity and operational cost of a fully configured Outlook Web Access solution.

A.4.6 Performance of web browsing

The machine running the web proxy software and the virus scanning and the mail relay, currently has 128 MB of memory. The resources spent in the machine under operation heavily suggests that memory is the bottleneck in the machine. It does work with the current configuration, but it is very clear that adding more memory will improve particular the performance of the web access. Mail delivery will not improve significantly.

Recommendation 6: Add memory to the Proxy machine to at least 256 MB in order to improve the performance of web access.

A.4.7 Update software exposed to the Internet

The proxy machine is exposed to the Internet for mail delivery, and the Exchange server is exposed to the Internet for IMAP/POP3 mail access. The firewall is exposed to the Internet in general. Consequently these machines should for security reasons at all times be up to date with installation of service packs and hotfixes.

Recommendation 7: Create a list of recurring operational tasks, and add to that list a monthly task of checking the current version of operating systems and server applications against the current list of fixes from the vendor.

A.4.8 "Out-of-Office" messages on the Internet

Outlook/Exchange lets the staff members create Out-of-Office messages for the purpose of automatically inform senders of mail that you are out of the office for a period of time. Exchange can be configured so that these messages also get sent to persons outside the internal network. This is clearly a good service to those contacting you by mail during absence. There are, however, drawbacks as well. Incoming spam (junk mail, UCE (unsolicited commercial email)), will get the "Out-of-Office" messages and can hence conclude that this particular mailbox is indeed alive and also a viable target in future spamming.

Recommendation 8: It should be considered, whether the user-friendly "Out-of-Office" messages should be delivered to the outside.

A.4.9 Limits on the size of mail messages

The system is now configured to reject sending or receiving mail of a size of more than 1 (one) megabyte. Spreadsheets with embedded graphs and PowerPoint presentations tend to grow large, and will probably be rejected for size occasionally. Using compression tools can alleviate the problem somewhat, but not solve it entirely.

Recommendation 9: After a period of a few months, the size limitation of one megabyte should be reconsidered based on experience.

ANNEX 5 RECOMMENDATIONS RELATED TO SYSTEM ADMINISTRATION

The system administration practices at INE have been studied throughout the mission and specific advice has been given in a number of cases on diverse issues that have come up during discussion and daily administrative tasks. A number of topics have identified themselves as critical and as areas where the administration work can profit by a concentrated effort to effect changes.

A.5.1 Backup procedures

The data residing on the network at INE is important to the statistical production. Inevitably, data get lost for various reasons. It can be deleted or overwritten by mistake and disasters can destroy large amounts of data. Good and tested backup/restore procedures are the means to minimize data loss. Backup procedures should be fully automated and documented in order to secure uniform quality of backups. A backup policy should be formulated in order to formalize decisions on what is backed up and when it is backed up.

Administration recommendation 1: Backup procedures should be fully automated and documented. A backup policy should be formulated.

A.5.2 Monthly reporting and organization

In order to ensure knowledge sharing and to get at higher information level the network administrator should report every month: the report should include description of main activities and incidents of the passed month and main planned ativities in the coming month. The reporting should include statistics on downtime and usage of critical resources such as disk space and internet usage. Operations should be organized so that one person is always available during working hours and one person should be responsible for operations and the monthly reporting.

Administration recommendation 2: Monthly reporting of operational incidents should be introduced and operations should be organized so that one person is responsible for operations and that one person is always available during working hours.

A.5.3 Printing

The setup of printing from workstations to network printers is now done in several ways. In order to secure the same quality of print for all end-users and in order to minimize administration work in case of new printers, the printing should be standardized. The standard should be based on Windows printing from workstation to server queue and LPR/LPD from server queue to network printer.

Administration recommendation 3: For administrative reasons the printing model should be systematically changed to Windows printing with central print queues.

A.5.4 Network files

The use of drive letters for network files is almost standardized today. The standardization should be completed and documented for clarity, and the assignment of drive letters in login scripts should be consolidated to one logon script for enforcing the standard drive letter assignment. The access permissions of different areas of network files should be standardized and documented for clarity and security.

Administration recommendation 4: The use of drive letters and access permissions for network files should be standardized.