

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

A Guide to
Building and Securing an Intranet Mail Server/Hub with AIX 5L Version 5.1
On An
IBM RS/6000 Server

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

Table of Contents 2
Statement of Purpose 4
Local Network Overview 4
Assumptions 4
Prerequisites 5
Operating System Overview 5
Preinstall Preparation 5
AIX 5.1 Installation 6
Configuration 8
Installing Updates 10
Hints& Tips (Optional but Recommended) 11
Logical Volume Management 11
- Set Up Dump Space 11
- Creating /usr/local Logical Volume and File System 11
- Increase System Default System Sizes 12
- Setup RAID 5 or Logical Volumes (Mirroring) 12

Post OS Install Security Measures 13
- Changing the Root User Defaults. 13
- Changing User Account Defaults 13
- Setting up Accounting 13
- Setting Timeout Values 14
- Setting System Error Checking 14
- Number of Licensed Users 14
- Path Configuration 14
- Network Security Setting 14
- Setting Default Login Messages 14
- Trusted Computing Base Check 15

Locking Down the Operating System 15
Stopping Script and SRC Controlled Services 15
Stopping inetd Services 15
Configuring System Auxiliary Tools 16
- NTP 16
- Syslog 17
- Linking AIX Error Log and Syslog 17
- Performance Diagnostic Tool (PDT) 18
- Sar (System Activity Reporter) 18
- Installation & Configuration of Third Party Auxiliary Software 18

Configuring the Mail System 20
- Configuring the Sendmail Proxy: Smap and Smapd 20
- Smapd 21
- SMTP Configuration 21
- Sendmail Installation 22
- Sendmail Configuration 22

© SANS Institute 2000 - 2005, Author retains full rights.

Non TIS Configuration 24
Popd Configuration **25**
Removing Unneeded software **25**
Install/Configure/Run Tripwire **25**
Backup of System **26**
Open the Floodgates **26**
Final Thoughts **26**
APPENDIX A **27**
Third Party Software Used 27
Verifying and Authenticating Software 27
APPENDIX B **28**
Third Party Software Installation and Configuration 28
Tcp_wrappers V 7.6.1 28
Openssh (v2.9p2) 28
Swatch (The Simple WATCHer and Filter) 29
Portsentry 30
Identd 31
Tripwire 31
APPENDIX C **33**
Hardware Specifications of Enterprise Server Model 7046-B50 33
APPENDIX D **34**
Sample /etc/motd 34
APPENDIX E **35**
Client Setup Example 35
REFERENCES **37**

© SANS Institute 2000 - 2005, Author retains full rights.

Statement of Purpose

This documentation is intended to guide the user through all steps necessary to build and correctly configure a secure Intranet mail server/hub with AIX 5L version 5.1 operating system running on an IBM Enterprise RS/6000 Server Model B50.

Local Network Overview

Our network structure is a ”Screened Subnet Architecture”, as described in [1]. Our bastion host is configured to run a secured SMTP server and do only elementary filtering. It is responsible for routing all incoming mail to the mailhub and direct all outgoing mail onto its destination. Our mailhub, “*mailhub*” will sit on the internal network and perform two functions. The first being the processing and filtering of incoming mail, the second, acting as a POP server from which clients will collect their mail.
In the interest of security, POP connection will be restricted to internal machines using Weitse Venema’s TCP Wrappers [2] and connections will be tunneled through the ssh. Our DNS has already been configured to direct all incoming mail for our site to the bastion host and client machines will direct all outgoing mail to the bastion.

The names and IP addresses used for this document are fictitious. Please consult your networking department for valid values.

ROLE	Fully Qualified Name	Alias	IP Address
BASTION:	bastion.anansi.com		10.4.126.1
MAILHUB	mailhub.anansi.com	mailhub	10.4.5.140
INTERNAL NETWORK			10.4.5

Assumptions

We make the following assumptions:

1) The installer/user of this document has elementary knowledge of Unix and is familiar with the *vi* editor.
2) The installer has access to the Internet for retrieval of third party software.
3) The installer is familiar with the use of a browser and/or an ftp client to retrieve required third party software.
4) The installer is able to obtain fixes on CDROM or via ftp.

© SANS Institute 2000 - 2005, Author retains full rights.

Prerequisites

1) AIX 5.1 installation CD's
2) AIX 5.1 fixes on CD or downloaded tar file from IBM. [3]
3) Third party software listed in Appendix B.
4) IBM Enterpriser Server Model B50 with accompanying monitor.
5) Networking Data
    a. Hostname
    b. IP address and Network mask
    c. DNS Nameserver address(s)
    d. Gateway address

6) A second UNIX machine with gpg installed.

7) An mm ape rive or other compatible tape device.

> **NOTE**: This machine will be used as a collection point for all third party software to be used. Required software is to be downloaded and verified ahead of time, then made accessible via ftp, to the machine being installed. Ideally, after software is downloaded onto this auxiliary machine it should be isolated allowing access only from the new machine(s) being installed.

Operating System Overview

IBM has positioned AIX 5 L version 5.1 as the new standard in UNIX operating systems. 5L is UNIX 98 branded and supports both 32 and 64-bit hardware systems. It is built on AIX 4.3.3 and provides improvements in critical areas of reliability, availability performance and security. IBM has gone one step further and included development tools and a new version of Performance Toolbox for system profiling and tuning. This is a leaner more flexible and reliable OS that runs across a wide cross-section of POWER-based systems and the new Intel Itanium chip. Linux compatible APIs and necessary header files provide support for cross development and porting of Linux and Open source software. [4]

Preinstall Preparation

Verify the authenticity and integrity of all third party software collected on the auxiliary UNIX/Linux machine. See Appendix B

© SANS Institute 2000 - 2005 Author retains full rights.

AIX 5.1 Installation

1) Set your SCSI tape device ID to 5. Consult you device manual on how to do this.
2) Power on all attached device including monitor/terminal and tape drive unit.
3) Insert installation CD #1 in the CDROM
4) Power on machine
   Press the numeral "5" after seeing scrolling RS/6000 lines, hearing the machine beep and seeing the text string "keyboard" being displayed along the bottom of the display. (Timing is everything here)

NOTE: ID 5 is generally a safe bet as disks and CDROM usually user lower ID's. If you encounter problems see instructions that came with the device.

At this point, you should be seeing "AIX Version 5.1" at the bottom of the display.

The next two menus ask you to define the System Console and System Console Language.
We select (1) to use the local terminal as the preferred system console and (1) to select English as our installation language.

The following sequence of menus guides you through the initial Operating System (OS) installation. Bold type indicates the appropriate choice at that point.
In many cases, we only display an option when a change is needed.

```
                    Welcome to Base Operating System
                    Installation and Maintenance

Type the number of your choice and Press Enter. Choice is indicated by >>>.

>>>   1 Start Install Now with Default Setting
      2 Change/Show Installation Setting and Install
      3 Start Maintenance Mode for System Recovery


      88 Help ?
      99 Previous Menu
      >>> Choice [1]: 2 <Enter>
```

© SANS Institute 2000 - 2005, Author retains full rights.

Installation and Settings

Either type 0 and press Enter to install with the current settings, or type the number of the setting you want to change and press Enter.

1 System Settings:
Method of Installation …… Preservation
Disk Where You Want to Install……..… ….. hdisk0 …

2 Primary Language Environment Settings (AFTER Install)
…
3 Advanced Options

>>> 0 Install with the current setting listed above

88 Help ?
99 Previous Menu

>>> Choice [0]: **1 <Enter>**

Change Method of Installation

Type the number of the installation method and press Enter.

1 New and Complete Overwrite
Overwrites EVERYTHING on the disk(s) selected
….
…
>>> 2 Preservation Install

88 Help
99 Previous Menu

>>> Choice [2]: **1 <Enter>**

Change Disk(s) Where You Want to Install

….

Name	Location Code	Size(MB)	VG Status	Bootable	
>>> hdisk0	10-80-00-2,0	17357	rootvg	yes	
>>> hdisk1	10-80-00-4,0	17357	rootvg	yes	

…

>>> 0 Continue with choices indicated above
…
>>> Choice **[2]<Enter><Enter>**

© SANS Institute 2000 - 2005, Author retains full rights.

// Only the first disk should be selected. The second will be used later as mirror.

You should now be back at the *Installation and Settings* Menu.
Select option (3) Advanced Options

```
                                Advanced Options

Either type 0 ……

        1 Desktop                                          CDE

        2 Enable Trusted Computing Base                    yes
        …

        >>> Choice [0]: 1 <Enter>                        # desktop none
        >>> Choice [0]: 2 <Enter>                        # install TCB
        >>> Choice [0]: <Enter>
        …
```

Back at the *Installation and Settings* Menu.
>>> Choice [0]: **<Enter>**

The operating system installation now starts with the message,
"Installing Base Operating System"…… "please wait" …

At the bottom of the display will be a task completion percentage indicator.
Now is the time to get a glass of anything cold, and allow the installation to proceed.
On this system, this takes approximately 30 minutes.

Configuration

After the system reboots, the first menu presented is the *Installation Assistant* menu and you are prompted for the correct terminal type. If the terminal type is not set correctly this menu will be redisplayed until a valid type is entered. If in doubt try using *"ibm5131",* as a default value.

The *Software License Agreements* menu is next.

Select

Show Installed License Agreements // If you need to first read the agreement
Or
Accept License Agreement
→ Accept Installed License Agreements **<Enter><Tab><Enter>** // to change no to yes

© SANS Institute 2000 - 2005, Author retains full rights.

<F3><F3><F3> // Back to configuration Menu

We are now presented with the Systems Management Interface Tool (SMIT), *Installation Assist* menu. This leads us through an initial configuration. We will be doing our customized configuration later on.

The configuration menu is shown below.

```
                                Installation Assistant

Move cursor to desired item and press Enter.

        Set Date and Time
        Set root Password
        Set Installation Devices
        Configure Network Communications
        Manage System storage and Paging Space (rootvg)
        Manage language Environment
        Create Users
        Define Printers
        Import Existing Volume Groups
        Install Software Applications
        Backup the System
        Using SMIT (information only)
        Tasks Completed – Exit to Login

F1=Help          F2=Refresh       F3=Cancel          F8=Image
F9=Shell         F10=Exit         Enter=Do
```

SMIT usage:
Options with an "=" -- can be changed by selecting the TAB key.
Options with an "*" -- use the <TAB> key to scroll through list or F4 to generate a list
Options with [ ] -- accept user keyboard input

Set Time and Date
→ Change/Show Date & Time

YEAR	(00-99)	[ ]
MONTH	(1-12)	[ ]
DAY	(1-31)	[ ]
HOUR	(00-23)	[ ]
MINUTE	(00-59)	[ ]
SECONDS	(00-59)	[ ]

<Enter><F3><F3>

NOTE: At any time if you accidentally exit to the command line run the command "install_assist" to take you back to the Installation Assistant menu.

Change Time Zone Using Defined Values
→ DAYLIGHT SAVINGS TIME ? **1 Yes**
→ CUT Time Zone
Select correct time zone using arrow key(s)
<Enter><Enter><F3><F3> # back to main menu

Set root password
root's new password: ******** **<Enter>**
Enter the new password again: ******* **<Enter>**

© SANS Institute 2000 - 2005, Author retains full rights.

back to main menu

© SANS Institute 2000 - 2005, Author retains full rights.

// Fill in the network communication section with appropriate values for your network

```
Configure Network Communications
        → TCP/IP Startup
            → Available Network Interface  <Enter>        #en0 is the default
            HOSTNAME                       [ ]
            Internet ADDRESS               [ ]
            NAMESERVER
                → Internet ADDRESS         [ ]
                → DOMAIN name              [ ]
            Default Gateway
                → Address                  [ ]
                → Cost                     [ ]
                → Do Active Dead Gateway Detection          [Yes]
                …
                …
                <Enter> <F3><F3>                            #back to main menu

Manage System Storage and paging Space (rootvg)
        → Add/Show paging Space
                → New Paging Space         [512]

        <Enter> <F3><F3><F3>                                #back to main menu
```

Tasks Completed – Exit to login
<Enter> # to login prompt

Login as the root user, using the previously assigned password.

Login : root
passwd: ******

Installing Updates

Place updates CD in CDROM drive then invoke the SMIT update screen with the following command.
mailhub% smitty update_all

Enter "/dev/cd0" as your INPUT device. Hitting <Enter><Enter> will perform the install with the default settings.

// This process takes 15 minutes on this system.

On completion reboot the machine then log in as the root user.
mailhub% shutdown -r
login: root
passwd: ******

© SANS Institute 2000 - 2005, Author retains full rights.

Hints& Tips (Optional but Recommended)

1) Before editing any file, make a backup copy of the original using the following format.

   mailhub% cp original_file original_file-orig

2) Edit the root user's *.profile* and add the following lines:-

   export TERM=ibm3151
   set –o vi # this enables the use of command line editing

Logical Volume Management

Set Up Dump Space

```
mailhub%  extendvg rootvg hdisk1
mailhub%  sysdumpdev –e                    //shows estimated dump size needed in Bytes
mailhub%  lsvg  rootvg | grep 'PP SIZE'    // shows Physical Partition (PP) size
```

// Convert estimated dump size to MB then round up to determine the number of PP needed for dump space
// For our configuration, we need 1 PP

HINT: use the following to calculate space requirements.
mailhub % bc <size_given_by_sysdumpdev> / (1024 * 1024) > / <PP size>

```
mailhub%  mklv –y 'hd7' –t 'sysdump'  rootvg 1 hdiks0    //create primary dump device
mailhub%  sysdumpdev –C –P –p /dev/hd7

mailhub%  mklv –y 'hd71' –t 'sysdump' roovg 1 hdisk1     // create secondary dump device
mailhub%  sysdumpdev –C –P –s /dev/hd71

mailhub%  bootlist –m normal hdisk0 hdisk1 cd0           // set up boot list
mailhub%  bosboot –a                                     // create a boot image
```

Creating /usr/local Logical Volume and File System

Traditionally the */usr/local* subtree has been used for installing third party software. We won't break that tradition, but will use the following commands to isolate */usr/local* to its own logical volume.

© SANS Institute 2000 - 2005 Author retains full rights.

```
mailhub%    mklv –w n –y locallv rootvg 30  hdisk0                  // 30 PP's
mailhub%    crfs –v jfs –d 'locallv' –m '/usr/local'  –A yes
mailhub%    mv /usr/local/ /usr/local2                              // don't overwrite old /usr/local
mailhub%    mount  /usr/local
mailhub%    chown  root:system /usr/local
mailhub%    mv /usr/local2/* /usr/local
```

Increase System Default System Sizes

By default, AIX creates very small logical volumes. The following commands increase these defaults to more reasonable settings.

```
mailhub%   chfs –a size=262144    /
mailhub%   chfs –a size=262144    /home                  // 128 MB
mailhub%   chfs  -s size=262144   /tmp
mailhub%   chfs –s size=262144    /var
mailhub%   chfs –s size=614400    /opt                   // 300MB
mailhub%   chfs –s size=1024000   /usr                   // 500 MB
```

Setup RAID 5 or Logical Volumes (Mirroring)

AIX permits us to mirror logical volumes. In our installation, thus far we have only used one disk. Our intension is to use the second disk as a mirror of the first. This gives us the advantage of higher availability. If one disk fails then we can keep functioning. A secondary benefit is that in the unlikely event of a system compromise we now have a duplicate copy of everything.
The following procedure will mirror what we have done to the second disk.

```
mailhub%   mklvcopy  hd1 2 hdisk1
mailhub%   mklvcopy hd3  2 hdisk1
mailhub%   mklvcopy hd2 2 hdisk1
mailhub%   mklvcopy hd10opt 2 hdisk1
mailhub%   mklvcopy hd9var 2 hdisk1
mailhub%   mklvcopy hd4 2 hdisk1
mailhub%   mklvcopy locallv  2 hdisk1
mailhub%   syncvg –v rootvg                  // Synchronize the root volume group
```

AIX activates volume groups based on quorums. A volume group will not be varied on (brought online) unless more that 51% of it is available. We need the ability to restart the system even if one of our two disks is unavailable. Thus, we turn the quorum requirement off. The following command does this.

```
mailhub%   chvg –Qn  rootvg                  // Turn quorum off. We can boot from 1 disk.
mailhub%   shutdown –Fr                      // Reboot the system.
```

© SANS Institute 2000 - 2005, Author retains full rights.

Post OS Install Security Measures

Changing the Root User Defaults.

Edit the file */etc/security/user*
Find the *root* users stanza // <esc>/root:
Add the following line

```
rlogin = false          // this prevents root access via tn, rsh .etc
minage =  1
maxage = 12
minlen = 6
```

Changing User Account Defaults

NOTE: User account defaults must be set in conjunction with your organizational security policy. Please consult with the necessary personnel in your organization to be on the safe side. The options we choose below are in accordance with our security polices and guidelines suggested by IBM. [5]

A brief description tells the function of each option below.
Edit */etc/security/user* file and change the options under the default section to those suggested in the table below.

Option	Advised Values	#Description
Login	False	Deny by default
Umask	027	Sets default file creation attributes
loginretires	5	Number of tries before account is locked
histexpire	26	Old passwords cannot be used for this many weeks
Histsize	0	Number of previous passwords that cannot be reused
Minage	0	Minimum time in weeks before change is allowed
maxage	8	Maximum weeks before having to change password
minlen	6	Minimum length allowed
mindiff	3	Minimum that must be different from old password
maxrepeats	1	Max number of times a character can be used
maxexpired	4	Weeks after expiration when change is allowed

Setting up Accounting

Use the following commands to create system accounting files.

```
mailhub%   /usr/sbin/acct/nulladm /var/adm/wtmp
mailhub%   /usr/sbin/acct/nulladm /var/adm/pacct
```

© SANS Institute 2000 - 2005 Author retains full rights.

Setting Timeout Values

Define the values TMOUT and TIMEOUT in the */etc/profile* file by adding the following lines.

```
TIMEOUT=300             # 5 minutes
TMOUT=300
```

// Be sure to update the export line to include both variables.

Setting System Error Checking

Use the *errpt* command to see if any system error messages are there.

```
mailhub%  errpt
```

Use the *errorclear* command to clear non-critical errors

```
mailhub%  errclear 0
```

Number of Licensed Users

Change the default setting of 2 to 80 (unlimited). There are no legal implications here. Licenses are free. ☺

```
mailhub%  chlicense  -u 80 off
```

Path Configuration

Edit the */etc/environment* file and add /usr/local/bin to the PATH environment variable. You line should look something like: -

```
PATH=/usr/bin:/usr/local/bin: …
```

Network Security Setting

Edit the */etc/rc.net* and add the following code to protect against SYN attacks

```
if [ -f /usr/sbin/no ] ; then
        /usr/sbin/no –o clean_partial_conns=1 >> /dev/null 2>&1
fi
```

Setting Default Login Messages

Edit the */etc/security/login.cfg* file. To the end of the default stanza, add the following line.

```
herald = “Unauthorized access to this <Insert_Company_name_here> machine is prohibited\nlogin: “ ”
```

Create an */etc/motd* file. It should include a warning and/or actions that will be taken by

© SANS Institute 2000 - 2005, Author retains full rights.

the company in the event of system abuse or misuse.
See Appendix D as a suggested document.
Trusted Computing Base Check

Run the tcbck command to establish a baseline of all the trusted programs on the system.
mailhub% tcbck –n ALL

Locking Down the Operating System

This essentially consists of turning off and stopping all un-needed services.

Services are started in one of three ways: -
1) rc startup scripts in /etc
2) Through the System Resource Controller SRC (may utilize a startup script also)
3) Through /etc/inetd.conf

Stopping Script and SRC Controlled Services

For this endeavor, we will stop several services with the commands below.

```
mailhub%  stopsrc –g nfs          #stops all nfs services
mailhub%  stopsrc –s sendmail
mailhub%  stopsrc –s portmap
mailhub%  stopsrc  -g spooler
mailhub%  stopsrc –s snmpd
mailhub%  stopsrc –s hostmibd
mailhub%  stopsrc –s dpid2
```

NOTE: "*lssrc –a* shows you the services under the control of the SRC.

To prevent these services from starting again after reboots, edit the */etc/rc.tcpip* file and comment the lines that start /usr/bin/snmpd, /usr/bin/dpid2, /usr/bin/sendmail , /usr/bin/hostmib and portmap.
Edit the */etc/inittab* file and comment the line starting with rcnfs.

Stopping inetd Services

Edit */etc/inetd.conf* and comment all services **except** pop3, then refresh the inetd process.
mailhub% refresh –s inetd // have changes take effect

© SANS Institute 2000 - 2005, Author retains full rights.

Configuring System Auxiliary Tools

NTP

Time stamping is critical in any computer system. In the event of a system compromise, accurate timelines are essential to establish the sequence and timing of events. Accurate time is also important for audit trails and mail thread tracking.

Following are instructions for configuring our machine as a Network Time Protocol (NTP) client.

1) Edit the */etc/hosts* file and add the following entry

```
x.x.x.x         timeserv1
y.y.y.y         timeserv2
z.z.z.z         timeserv3
```

NOTE: in place of x.x.x.x, etc use the real IP addresses of your network NTP servers. Three are ideal though not required ☺

2) Edit the */etc/ntp.conf* file.
Comment the broadcast line and add the following lines:

```
server timeserv1
server timeserv2
server timeserv3
driftfile /etc/ntp.drift
tracefile /etc/ntp.trace
restrict default nomodify
```

3) Create the file */etc/rc.local* and add the following stanza to it.

```
if [ -s /etc/ntp.conf ]  ; then
        Print "synchronizing time"
        ntpdate –b –s \                 // jump the time at startup
        `sed –e '/^server/!d'\
        -e 's/^server[  ]*//'\
        -e 's/[  ].*//' /etc/ntp.conf `

        sleep 5
        startsrc –s xntpd               //start under the control of the SRC
fi
```

4) Add an entry to your */etc/inittab* file for starting rc.local at boot time.

```
mailhub%   mkitab –i cons "rclocal:2:once:/etc/rc.local > /dev/console 2.&1 "
```

5) Change ownerships and permissions of files/scripts involved.

```
mailhub%   chown bin:bin /etc/rc.local ;chmod 700 /etc/rc.local;
mailhub%   touch  /etc/ntp.drift /etc/ntp.trace
mailhub%   chown  bin:bin /etc/ntp.conf
mailhub%   chmod 644  /etc/ntp.conf
```

© SANS Institute 2000 - 2005, Author retains full rights.

Syslog

We will use the syslog facility to control logging. This however is not your fathers syslog. AIX 5.1's new Syslog has capabilities allowing for log rotation based on file size and/or time. When using time-based rotation, date info is appended to the aged log files. Even compression is an option here.
To configure syslog take the following 3 steps: -

1) Edit the */etc/syslog.conf* file and include the following lines:

```
#Log all warnings
*.warning                          /var/log/warnings       rotate time 1d    # rotate daily
*.warning                          @loghost
#log mail debug messages
mail.debug                         /var/log/maillog        rotate time 1d
mail.none                          /var/log/maillog
# Log security related message
auth.debug                         /var/log/security       rotate time 1d
auth.notice                        @loghost
# System Problems
*.alert;*.crit                     *
*.emerge;*.alert;*.crit;*.err      @loghost
# all other messages except mail
*.debug; mail.none                 /var/log/debug          rotate time 1d
```

NOTE: Spaces in the /etc/syslog.conf are tabs, not spaces. Additional details on the *new* syslog can be found at [6].

.

2) Edit */etc/hosts* and add an entry for loghost . // Use the real IP in place of x.x.x.x

```
10.4.5.126          loghost          // machine where messages will be sent
```

3) Create empty log files and restart syslog daemon.

```
mailhub%  cd /var/log;
mailhub%  touch warnings mail.debug security debug
mailhub%  refresh –s  syslogd                    // restart the Syslog daemon
```

Linking AIX Error Log and Syslog

Create a file called */tmp/link_log* and add the following lines

```
erronotify:
        en_pid = 0
        en_name = "syslog"
        en_persistenceflg = 1
        en_label = ""
        en_crcid = 0
        en_class = ""
        en_type = ""
        en_alertflg = ""
        en_resource = ""
        en_rtype = ""
        en_rclass = ""
```

NOTE: AIX makes use of Syslog for traditional purposes. However, it also uses its proprietary error logging facility for generating system level error logs. The link_log script was written by Andreas Siegert[7] and can be used for linking both error-logging mechanisms, permitting entries generated by the errorlog to be also sent to Syslog.

© SANS Institute 2000 - 2005, Author retains full rights.

en_method = "/usr/bin/errpt –l $1| /usr/bin/tail –1| /usr/bin/logger –t errpt –p daemon.notice" [4]

Activate error notification and test linkage.

```
mailhub%  odmadd /tmp/link_log
mailhub%  errlogger testing                 // Test linkage
mailhub%  tail  /var/log/debug              // should see a line starting with the word "errpt"
```

Performance Diagnostic Tool (PDT)

First, install the necessary software.

```
mailhub%  installp –acd /dev/cd0 bos.perf      // with boot cd in CDROM
```

NOTE: PDT sends daily reports to the user specified. Reports include workload tracking, processes consuming CPU and or memory resources, I/O imbalances, journaling file system problems and a myriad of problems. It even does some elementary forecasting. PDT is highly customizable. More details on PDT can be found at [8].

http://as400bks.rochester.ibm.com/cgi-bin/ds_form?lang=en_US&viewset=AIX

Next, change the PDT report recipient and severity level

```
mailhub%  /usr/sbin/perf/diag_tool/pdt_config
```

```
_____________________PDT customization menu_____________________

    1)   show current          PDT report recipient and severity level
    2)   modify/enable         PDT reporting
    3)   disable               PDT reporting
    4)   modify/enable         PDT collection
    5)   disable               PDT collection
    6)   de-install  PDT
    7)   exit pdt_config
    Please enter a number: 2 <Enter>

    enter id@host for recipient of report : root@loghost <Enter>
    enter severity level for report  (1-3): 3 <Enter>

   report recipient and severity level
   root@loghost 3
```

On the redisplay of the menu, select option **4** to enable PDT collection and then option **7** to exit pdt_config.

Sar (System Activity Reporter)

NOTE: Sar shows CPU utilization and should be one of the tools an administrator uses to investigate system anomalies.

Set up Sar by taking the following steps

1) mailhub% su –adm
2) mailhub% crontab –e /* this throws you into the vi editor */
3) Uncomment the 4 crontab entries following the "SYSTEM ACTIVITY REPORTS" summary section.
4) Save and exit the file.

Installation & Configuration of Third Party Auxiliary Software

```
mailhub%  cd  /usr/local                    // local storage for already verified software
```

© SANS Institute 2000 - 2005, Author retains full rights.

```
mailhub%   mkdir src bin sbin include etc lib man;
mailhub%   chmod –R 755 /usr/local
```

AIX 5.1 is quite Linux/GNU friendly and indeed comes with several packages installed. These include zcat, gzip, patch and more.
Some critical software can also be found on the IBM Toolbox for Linux Applications CD or via the IBM web site at [9]. The software to be installed can be classified into three categories listed below.
1) Development tools: autoconf, automake, bison, db, flex, gcc, make
2) Utility tools: gdbm, m4, gawk
3) Informational/analysis tools: lsof

To install these from the CD insert the CD into CDROM drive and follow the instructions below: -

1) At the prompt
   ```
   mailhub%   smitty install_latest
   ```
2) Select <F4> to choose installation device, then <enter> to select /dev/cd0.
3) Select <F4> to get a listing of software on the CDROM.
4) Use <F7> to select the packages listed above.
   <Enter> when done selecting.
5) Back at the Install Software menu install the software by pressing
   <Enter><Enter> .
6) At the OK result select <F10>.

Install and configure the following security related packages. Please consult Appendix B for instructions if needed.

Tcp Wrappers:	used to restrict access to services
Statch:	realtime log analyzer written by E. Todd Atkins
Portsentry:	port scan detector and blocker
Openssh:	used for secure connections

© SANS Institute 2000 - 2005, Author retains full rights.

Configuring the Mail System

NOTE: TIS has had its share of bugs nevertheless it is still relatively useful. While it is probably most useful on a bastion host, having another layer of defense here can't be a bad thing. If you choose not to utilize the TIS Firewall Toolkit, you may skip its installation/configuration and refer to the "Non TIS Configuration " section below.

Installation and Configuration of the TIS Firewall Mail Proxy. (OPTIONAL)

The TIS Firewall toolkit license and README files can be found at ftp://ftp.tis.com/pub/firewalls/toolkit/. After reading and accepting the license, follow the instructions in the README (also shown in the note below) to obtain access to the toolkit.

NOTE: You will need to perform the actions below to obtain the firewall toolkit.

After you have read the FWTK software license, if you agree to abide by its restrictions, you are required to send a one word -- the word "accepted" -- e-mail message to fwtk-request@tislabs.com. The single word "accepted" (with no quotes) should be the entire *body* of the message (not the subject). Based on your acknowledgment of the terms and conditions of TIS FWTK software license, a responding e-mail will be sent to you and will contain the location of the FWTK source code and documentation.

// After downloading the software

```
mailhub%   uncompress fwtk.tar.Z
mailhub%   tar xvf fwtk.tar
mailhub%   cd fwtk
//download the smap anti-spam patch from
http://www.fwtk.org/fwtk/patches/yao-smap.pch
// apply patch
mailhub%   cp yao-smap.pch  /usr/local/src/fwtk/smap
mailhub%   cd /usr/local/src/fwtk/smap
mailhub%   patch –I  yao-smap.pch smap.c; cd ..
mailhub%   cp Makefile.config  makefile.Config-orig
mailhub%   cp Makefile.conf.aix3 Makefile.config
 Edit Makefile.config. Change the CC variable to point to gcc   (CC = gcc)
```

Edit the *Makefile*. We only need to compile the relevant mail sections. To do this change the *DIRS* setting to read, "DIRS= smap smapd".

```
mailhub%   make
mailhub%   make install                // Default files are put in /usr/local/fwtk  subtree
```

Configuring the Sendmail Proxy: Smap and Smapd

```
mailhub%   mkdir /var/spool/smap;
mailhub%   cd /var/spool/smap
mailhub%   mkdir baddir dev
mailhub%   cd dev
mailhub%   mknod  null c 2 2
mailhub%   chmod 700 /var/spool/smap
mailhub%   chown –R mail:mail /var/spool/smap
```

NOTE: Ensure that the userid used in */usr/local/etc/netperm-table* matches the user that will be running smapd and has write permissions to the directory just created. I created a *mail* user and a *mail* group.

© SANS Institute 2000 - 2005, Author retains full rights.

Edit the */usr/local/fwtk/netperm-table*, removing every section with the exception of the "example smap rules".

Add the following line to the */etc/local/etc/netperm-table*

```
smapd:          baddir    /var/spool/smap/baddir
smapd:          executable /usr/local/etc/smapd

mailhub%   chmod 600  /etc/local/etc/netperm-table
```

Smapd

Add the following stanza to your */etc/rc.local:*

```
## Start of addition

echo "Starting Firewall Mail Proxy …"
(cd /var/spool/mqueue; rm –f nf* lf* )

#start queuer
if [ -f /usr/local/etc/smapd ] then
        echo "Starting  smtp querer "
        /usr/local/etc/smapd &
fi

#process undelivered mail queue
if [ -f  /usr/local/etc/mqueue ] ; then
        echo "Processing mail queue"
        /usr/local/etc/mqueue &
fi

# start listener
if [ -f /usr/local/etc/smap] then
        echo " starting smtp listener …"
        /usr/local/etc/smap -daemon &
fi

## End of rc.local addition
```

SMTP Configuration

Edit */etc/host* file and add all aliases and a fully qualified domain name for you host. For example: -

```
10.4.5.104          mailhub.anansi.com mailhub
```

Create a new mail group and mail user and add the *mail* user to the group.

```
mailhub%   mkgroup mail
mailhub%   mkuser id=6 groups=mail mail
```

© SANS Institute 2000 - 2005, Author retains full rights.

Edit */etc/resolv.conf*.
Add the names of your DNS Nameservers.

```
domain          anansi.com
nameserver      10.1.1.200
nameserver      10.1.1.201
nameserver      10.4.1.200
```

Create */etc/netsvc.conf* adding the line below.
hosts=local,bind

Sendmail Installation

```
mailhub%   gzip –dc  sendmail-8.11.6.tar.gz | tar xvf -
mailhub%   cd sendmail-8.11.6/devtools/OS
mailhub%   mkdir save; mv * save; mv save/AIX .
```

Edit the AIX file.
Listed below are the contents of this file with changes highlighted.

```
# $Id: AIX,v 8.11 2001/05/29 23:57:19 ca Exp $
define(`confMAPDEF', `-DNDBM -DNIS -DNEWDB')
define(`confENVDEF', `-D_AIX3')
define(`confCC', `/usr/bin/gcc')
define(`confOPTIMIZE', `-g')
define(`confLIBS', `-ldbm')
define(`confEBINDIR', `/usr/lib')
define(`confSBINGRP', `system')
define(`confINSTALL', `/usr/ucb/install')
define(`confDEPEND_TYPE', `AIX')
define(`confSM_OS_HEADER', `sm_os_aix')
```

//Compile problems forced me to make the following change.
mailhub%   cd ../../mail.local

Edit the mail.local/mail.local.c file and comment out the line that defines the vsnprintf function.

```
/*
extern int vsnprintf ……
*/
```

```
mailhub%   cd ..
mailhub%   ./Build
mailhub%   ./Build install
```

Sendmail Configuration

This is a two-step process. We generate an appropriate sendmail.cf file, and then create local access files that limit and restrict the use of the server.

© SANS Institute 2000 - 2005, Author retains full rights.

1) Generating the */etc/mail/sendmail.cf*

```
mailhub%   cd  /usr/local/src/sendmail-8.11.6/cf/cf
mailhub%   cp generic-bsd4.4mc aix5.mc
```

Change the contents of *aix5.mc* to match below.

```
divert(0)dnl
VERSIONID(`west.com, V1.0')          //domain and Version
OSTYPE(aix5)dnl                      // domain
DOMAIN(west)dnl
MAILER(local)dnl
MAILER(smtp)dnl

// End of file
```

NOTE: The bastion host has to be configured to define the mail hub as pointing to this machine. This would be done with a statement such as, "define (`MAIL_HUB', 'mailhub.anansi.org'). For a more detailed discussion see [10][11].

```
mailhub%   cd /usr/local/src/sendmaill-8.12.0/cf/domain/
mailhub%   cp generic.m4 west.m4
```

Change the contents of *west.m4*

```
divert(0)
VERSIONID(`$Id: generic.m4,v 8.15 1999/04/04 00:51:09 ca Exp $')
define(`confFORWARD_PATH',
`$z/.forward.$w+$h:$z/.forward+$h:$z/.forward.$w:$z/.forward')dnl
define(`confMAX_HEADERS_LENGTH', `32768')dnl
define(`confSMTP_LOGIN_MSG',$j mailer ready at $b')dnl
define(`confTRUSTED_USERS',`mail')dnl
define(`confMIME_FORMAT_ERRORS',`False')
FEATURE(`redirect')dnl
FEATURE(`use_cw_file')dnl
EXPOSED_USER(`root')
MASQUERADE_AS(west.com)dnl
FEATURE(masquerade_envelope)dnl
FEATURE(`access_db')dnl
FEATURE(`blacklist_recipients')dnl                  // Allow hub to do inbound filtering
                                                    // taking load off of bastion
```

// End of File

```
mailhub%   cd /usr/local/src/sendmaill-8.12.0/cf/ostype
```

Edit *aix5.m4* to match the following.

```
divert(0)
VERSIONID(`$Id: aix5.m4,v 1.1 2000/12/08 21:53:36 ca Exp $')
ifdef(`LOCAL_MAILER_PATH',, `define(`LOCAL_MAILER_PATH', /bin/bellmail)')dnl
ifdef(`LOCAL_MAILER_ARGS',, `define(`LOCAL_MAILER_ARGS', mail -F $g $u)')dnl
_DEFIFNOT(`LOCAL_MAILER_FLAGS', `mn9')dnl
define(`confEBINDIR', `/usr/lib')dnl
define(`confTIME_ZONE', `USE_TZ')dnl
FEATURE(smrsh)dnl


// End of File
```

All the steps taken above were made so that we could to this: -

© SANS Institute 2000 - 2005, Author retains full rights.

```
mailhub%   mv /etc/mail/sendmail.cf /etc/mail/sendmail.cf-orig
mailhub%   cd ../cf
mailhub%   mailhub%   m4 ../m4/cf.m4 aix5.mc > /etc/mail/sendmail.cf
```

2) Restricting Access

Edit the files *local-host-names* and *access* making necessary changes to satisfy your local networking settings. Add all aliases for you machine to the *local-host-names* file. The *access* is your primary filter file. Add entries for sites you want rejected as well as local machines that need to be able to relay mail. See the samples below.

```
// /etc/mail/local-host-names                    // do not include this line
mailhub.anansi.com
mailhub
[10.4.5.140]
localhost
[127.0.0.1]
// End of file
```

```
// /etc/mail/access                              //do not include this line
mailhub.anansi.com          RELAY
10.4.5.140                  RELAY
anansi.com                  RELAY
10.4.5                      RELAY          //local network
10.4.126.1                  RELAY
user@spammer.com            REJECT                 // add you favorite spammers here
193.132                     REJECT
bigisp.com                  REJECT
// End of file
```

Set proper permissions

```
mailhub%   chmod 644 /etc/mail/relay-domains /etc/mail/local-host-names /etc/mail/access
```

Make database file(s)

```
mailhub%   makemap hash access < access
mailhub%   newaliases      // build aliases file
```

Non TIS Configuration

If you elect not to run TIS's smap/smapd daemons, you then need to run sendmail as a daemon. To do this, take the following two steps.

1) Edit the */etc/rc.tcpip* file. Uncomment the line that starts the sendmail daemon.
   "start /usr/lib/sendmail "$src_running" –bd –q${qpi}"
   This ensures that it will be started on a reboot.
2) Start the sendmail daemon.
   mailhub%   startsrc –s sendmail

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.

Popd Configuration

The pop server we will use is IBM's native pop server. The only modification we need to make is to restrict access to internal machines by using Tcp Wrappers. (See Appendix B)

Edit the */etc/ined.conf* file.
Uncomment the line that begins with "pop3", and change it to say
pop3 stream tcp nowait root /usr/sbin/tcpd pop3d

All done!

Removing Unneeded software

Remove source code from */usr/local/src*.

```
mailhub%  cd /usr/local/src
mailhub%  mv tripwire ..          // We don't want to get rid of Tripwire just yet ☺
mailhub%  rm –ri *
mailhub%  mv ../tripwire .
```

Remove the compiler. This was installed from an IBM backup file format (bff), file and can be easily removed.

```
mailhub%  smitty deinstall
```

Remove Installed Software

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]
* SOFTWARE name	[**freeware.gnu.gcc.rte]**
PREVIEW only? (remove operation will NOT occur)	yes
REMOVE dependent software?	no
EXTEND file systems if space needed	**no**
DETAILED output	**yes**

Install/Configure/Run Tripwire

Tripwire is a file integrity checker written by Gene Kim and Gene Stafford of Purdue University [12]. It is useful in ascertaining if a file has been changed. By running Tripwire at regular intervals, we can easily determine what has changed in our filesystem. Tripwire can be configured to report these changes, giving the administrator the opportunity to accept and integrate the changes into an existing database. See Appendix C for Tripwire

© SANS Institute 2000 - 2005, Author retains full rights.

installation.

Backup of System

Verify that the tape device is available. If it is not available, refer to tape device installation instructions.
```
mailhub%   lsdev –Cc tape                    // look for word “Available” from output
```

Place tape in drive unit before running the next command.
```
mailhub%   mksysb –i /dev/rmt0
```

Repeat the process for a second tape. Label, date and store one tape in a secured location. The second copy can be sent offsite for storage.

Reboot the system to have all configuration changes take effect.
```
mailhub% shutdown -Fr
```

Open the Floodgates

The following steps are an overview of the processes that have to take place to facilitate client use of the machine.

1) Add user accounts to the server and assign them temporary passwords.
   ```
   mailhub%   mkuser <username>
   mailhub%   passwd <username> *******
   ```
2) Install an Ssh client capable of port forwarding. One such Microsoft Windows application is SecureCrt. [13]. See Appendix E.
3) Set up port forwarding on client machine
4) Configure client pop3 server.
5) Configure the client SMTP server to be the bastion host.
6) Have users Ssh into machine and change their default passwords.
7) Fire up pop/mail clients and test.
8) Educate users on how to use Ssh and Pop clients.

Final Thoughts

Many of the decisions taken in our installation were made after consulting our site security policy guidelines. You need to use your security policies as a guide.
While we have not spoken about physical security this is also critical. Your system cannot be considered secure if it offers easy physical access to all. Finally, continual vigilance is

© SANS Institute 2000 - 2005, Author retains full rights.

important. One must pay attention to security alerts and software updates that are put out by vendors and/or security organizations.

© SANS Institute 2000 - 2005, Author retains full rights.

APPENDIX A

Third Party Software Used

In some cases the location of both source code and binaries are given. Our choice always appears first.

Software Title	Distribution type	Location	Version
Tcp Wrappers	Tar file(s)	ftp://ftp.porcupine.org/pub/security	7.6
	Binary	http://www.bull.de/pub/aix432	
lsof	Tar file(s)	ftp://vic.cc.purdue.edu/pub/tools/unix/lsof	4.51
	Binary	www-1.ibm.com/servers/aix/products/aixos/linux/download.html	
gcc	Binary	http://www.bull.de/pub/aix432	2.95.3
mke	Binary	Aix toolbox for Linux applications	3.79.1
identd	Tar file(s)	ftp://sunsite.unc.edu/pub/Linux/system/daemons/	
PortSentry	Tar file(s)	http://www.psionic.com/abacus/portsentry	1.1
Tripwire	Binary	Contact sales@tripwire.com	2.4.2
	Binary	http://www.bull.de/pub/out_frame.html	
Tis toolkit	Tar file(s)	www.tis.com	2.0+
swatch	Tar file	ftp://ftp.stanford.edu/general/security-tools/swatch	3.01
Openssh	Tar file(s)	http://www.openssh.org/portable.html	2.9p2
Openssl		http://www.openssl.org	0.9.6b
Zlib		http://www.gzip.org/zlib/	1.1.3
Sendmail	Tar file	http://www.sendmail.org8.11.html	8.11.6

Verifying and Authenticating Software

Use gpg software to verify every software package. To do this we first obtain the authors public key and install it in to our key ring.
% gpg –import <new key>

Verify software with the following command.
% gpg <software.packager.tar.asc>
Enter the name of the software package when prompted.

A good "*signature message"* indicates that the software is pristine.

© SANS Institute 2000 - 2005 Author retains full rights.

APPENDIX B

Third Party Software Installation and Configuration

After verification, on the auxiliary machine, ftp files to *mailhub*. Place source file in */usr/local/src*, rpm files in */opt/freeware/src/packages/RPMS/ppc* and AIX bff files in */usr/sys/inst.images*.

Source installation instructions for other packages:

Tcp_wrappers V 7.6.1

From source

```
mailhub%   gunzip tcp_wrappers_7.6.tar.gz
mailhub%   tar xvf tcp_wrappers_7.6.tar
mailhub%   cd  tcp_wrappers
```

Edit

Makefile and change the following Options

```
REAL_DAEMON_DIR=/usr/sbin
FACILITY=LOG_AUTH
IPV6=-DHAVE_IPV6 –DUSE_GETHOSTBYNAME2
STYLE=-DPROCESS_OPTIONS CC=gcc
```

Building

```
mailhub%   make aix
```

Installation

```
mailhub%   cp  tcpd safe-finger tcpdchk tcpdmatch try_from  /usr/sbin
mailhub%   cp  hosts_access.3 /usr/man/man3
mailhub%   cp  host_access.5  hosts_options.5 /usr/man/man5
mailhub%   cp tcpd.8 tcpdchk.8 tcpdmatch.8 /usr/man/man8
mailhub%   cp libwrap.a /usr/lib
mailhub%   cp tcpd.h /usr/lib
```

Configuration

Edit */etc/hosts.deny* and add the following line

```
ALL: ALL:  /usr/sbin/mail  \
        -s “%s: Attempted connection from %c” root                    //deny everyone
```

Edit */etc/hosts.allow* to include the following

```
ALL: 10.4.0.0/255.255.0.0                                    // Internal IP address
Range
sshd : x.x.x.x,                                  // IP address of bastion ☺
```

Openssh (v2.9p2)

Requires openssl and zlib

Zlib (ver 1.1.3 or latest)

© SANS Institute 2000 - 2005, Author retains full rights.

```
mailhub%   tar xvf zlib-1.1..3.tar
mailhub%   cd zlib-1-1-3
mailhub%    ./configure
mailhub%   make
mailhub%   make install                    // defaults to /usr/local/lib
```

openssl (0.9.6b)

```
mailhub%   tar xvf  openssl*
mailhub%   cd /openssl-0.9.6b
mailhub%   ./Configure aix43-gcc
mailhub%   make
mailhub%   make install                    // defaults to /usr/local/ssl
```

openssh (2.9p2)

```
mailhub%   tar xvf openssh-2.9p2.tar
mailhub%   cd openssh-2.9p2
mailhub%   ./configure  --with-ipv4-default  --with-tcp-wrappers
mailhub%   make
mailhub%   make install
```

Configuration

To the */usr/local/etc/sshd_config* make the following changes

```
DSAAuthentication yes
PermitRootlogin  no
PrintMotd          no
```

Add the following lines to */etc/rc.local* to start sshd at system startup.

```
if –[ -f /usr/local/sbin/sshd ] ; then
        Echo “Starting sshd daemon “
        /usr/local/sbin/sshd &
        sleep 5
if
```

Swatch (The Simple WATCHer and Filter)

Swatch is a Perl program that watches logs in real time. It can be used to alert an administrator when an event triggers.
Installation is simple.

```
mailhub%   gzip  -dc swatch-3.0.1.tar.gz | tar xvf -
mailhub%   cd swatch-3.0.1
mailhub%   perl Makefile.PL
        Say “y” when prompted to install any modules.
        Accept all other defaults. It may be necessary to give the path for specific programs.
mailhub%   make
mailhub%   make test
mailhub%   make install
```

© SANS Institute 2000 - 2005, Author retains full rights.

Configuration

Swatch events are triggered when a match is made between the message generated in the log file and a regular expression in the configuration file. See [16] on how to configure your log file.

All we want to be notified of is illegal relaying attempts. Our */usr/local/etc/swatchrc* file contain the following:

```
watchfor        /Relaying denied|expn/
                echo=normal
                mail=root@loghost.anansi.com, subject="— llegal Sendmail Attempt" –
```

Start Swatch by adding the following stanza to */etc/rc.local.*

```
if   [ -f  /usr/opt/perl5/bin/swatch ] ; then
                /usr/opt/perl5/bin/swatch –c /usr/local/etc/swatchrc –t  /var/log/maillog
fi
```

Portsentry

```
mailhub%   tar xvf portsentry-1-1.tar
mailhub%   cd protsentry-1.1
```

Edit the Makefile making the following changes:
CFLAGS = -g –Wall
CC = gcc

```
mailhub%   make aix
mailhub%   make install
```

Edit the */usr/local/psionic/portsentry/portsentry.conf* file.
Set or change the following variables to match below.

```
KILL_ROUTE=/usr/sbin/route add $TARGET$  127.0.0.1  –reject
RESOLVE_HOST=0
```

Starting Portsentry

Although no startup scripts come bundled with PortSentry the following stanza may be placed in */etc/rc.local* to start Portsentry.

```
#Startup Portsentry

if [ -f /usr/local/psionic/portsentry/portsentry ]; then
          echo "Starting PortSentry  (non Stealth mode)"
         /usr/local/psionic/portsentry –tcp  2> /dev/console
```

NOTE: PortSentry does not run in stealth mode on this OS.

© SANS Institute 2000 - 2005, Author retains full rights.

```
        /usr/local/psionic/portsentry –udp 2> /dev/console
fi
```

Identd

```
mailhub%   unzip identd-masquerade.tar.gz
mailhub%   tar xvf identd-masquerade.tar
mailhub%   cd identd
```

Edit the Makefile and set the following variables: -
CFLAGS = -g
CC = gcc

```
mailhub%   make
mailhub%   chown root.bin identd
mailhub%   chmod 555 identd
mailhub%   cp identd /usr/local/etc
```

Edit */etc/identd.conf* and add the following line:

```
ident     stream   tcp      nowait   root     /usr/local/etc/identd        identd
```

Edit */etc/services* to contain the line "ident 113/tcp auth".
Comment out the line that starts with *auth*.

```
mailhub%   refresh –s inetd
```

Tripwire

```
mailhub % gzip –dc  tfs_242_aix_eval.tar.gz | tar xvf –
mailhub % cd tar_242_aix_eval
mailhub % ./install.sh
```

NOTE: To obtain a 30-day evaluation copy of tripwire, contact the sales team at sales@tripwire.com. You will be sent a password and the address of an ftp site from which you can then download the software.

Read the license agreement and type "accept" to accept the license agreement. Do not install the server agent.
Specify site passphrase when prompted.
Specify local passphrase when prompted.
Tripwire will now generate site and local keys, a configuration file, and a default policy file. The default installation path for tripwire is */usr/local/tripwire/tfs/*.

Configuration

Edit the configuration file and make the following changes:

1) GLOBALEMAIL=root@loghost.west.com
2) SMTPHOST=mailhub.west.com

© SANS Institute 2000 - 2005, Author retains full rights.

Digitally sign and encode the configuration file.
mailhub % cd */usr/local/tripwire/tfs/bin*
mailhub % twadmin –create-cfgfile –sitekey ../key/site.key twcfg.txt

Test E-mail notification.
mailhub % tripwire –test –email root@loghost.com

Customize our policy file.
This file has been already tuned for AIX. We will make a few minor customizations. See [12] for more details.
Edit */usr/local/tripwire/tfs/policy/twcfg.txt*
To the "System Configuration files" section add the following:

```
/etc/mail                                   -> $(SEC_CONFIG) ;
/usr/local/etc                              -> $(SEC_CONFIG) ;
```

Sign and install our policy file.
mailhub % twadmin --create-polfile twpol.txt

Initialize database
mailhub % tripwire --init

Automate regular runs.
mailhub % crontab –e
Add the line: *"0 * * * * /usr/local/tripwire/tfs/bin/tripwire --check --email-report*

Finally, make a backup of you tripwire database. This can be copied to a secure remote server or at the minimum to a floppy disk.
mailhub % dd if=mailhub.anansi.com of=/dev/fd0

© SANS Institute 2000 - 2005, Author retains full rights.

APPENDIX C

Hardware Specifications of Enterprise Server Model 7046-B50

Microprocessor	
Type	604e
Processors/system	1
Clock Rate	375
Memory	
System (min/max)	1GB
L2 Cache	1MB
Capacity	
Slots	2 PCI
Media Bays	2/2
Int. Disks(min/max)	72.8GB

© SANS Institute 2000 - 2005, Author retains full rights.

APPENDIX D

Sample /etc/motd

[14]

```
================================== FYI ================================== \
* This system is for the use of authorized users only.                    *
| Individuals using this computer system without authority, or in         |
* excess of their authority, are subject to having all of their           *
| activities on this system monitored and recorded by system              |
* personnel.                                                              *
|                                                                         |
* In the course of monitoring individuals improperly using this system,   *
| on in the course of systems maintenance, the activities of authorized   |
* users may also be monitored.                                            *
|                                                                         |
* Anyone using this system expressly consents to such monitoring and is   *
| advised that if such monitoring reveals possible evidence of criminal   |
* activity, systems personnel may provide the evidence of such            *
| activity to law enforcement officials.                                  |
\======================================================================== /
```

© SANS Institute 2000 - 2005, Author retains full rights.

APPENDIX E

Client Setup Example

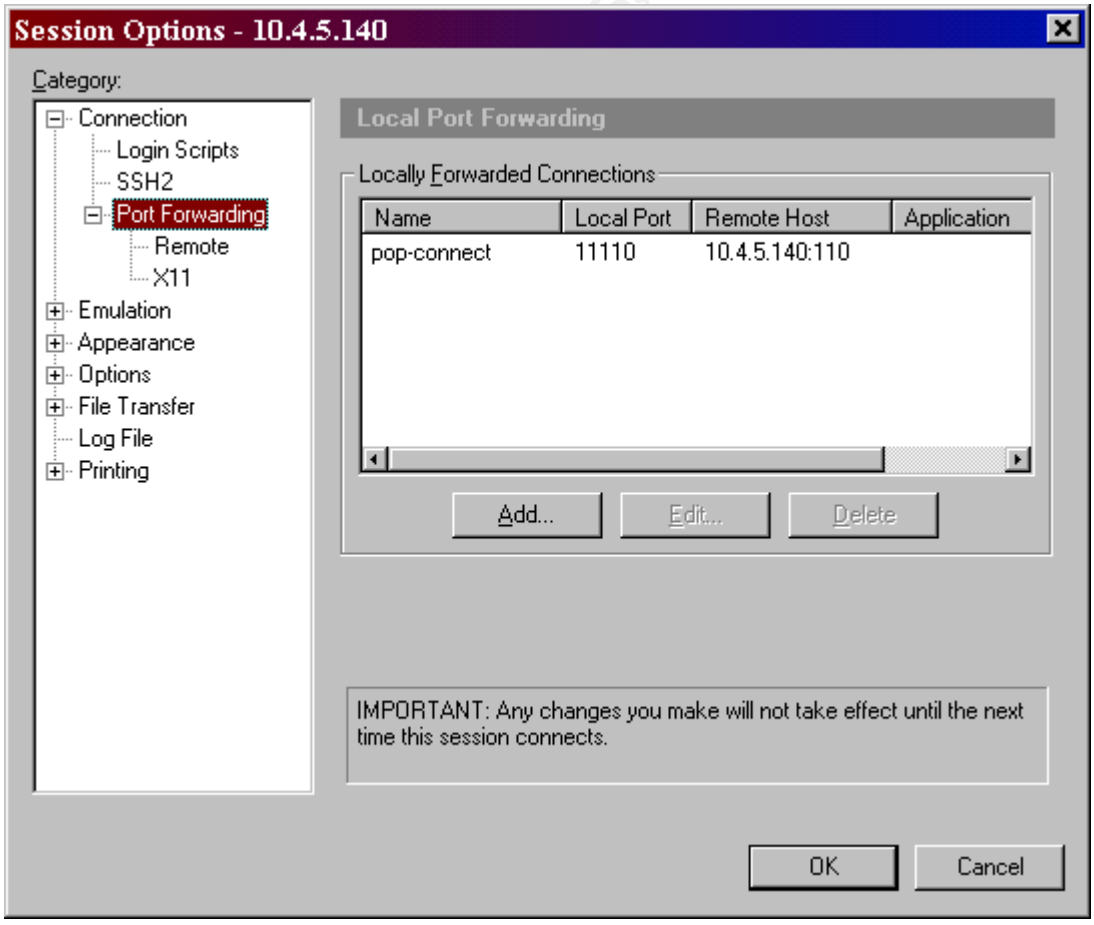
Pop traffic can be tunneled via Ssh to prevent passwords traveling though the network in clear text. Below is a typical example that may be customized for your environment. For UNIX/Linux systems see [15].

SecureCrt (v3.3) Settings on Windows machine:

Options
Session Options
PortForwarding
Add

Name	[pop-connection]
Local port	[11110]
Remote Hosname	[mailhub]
Port	[110]

See Screen shot below

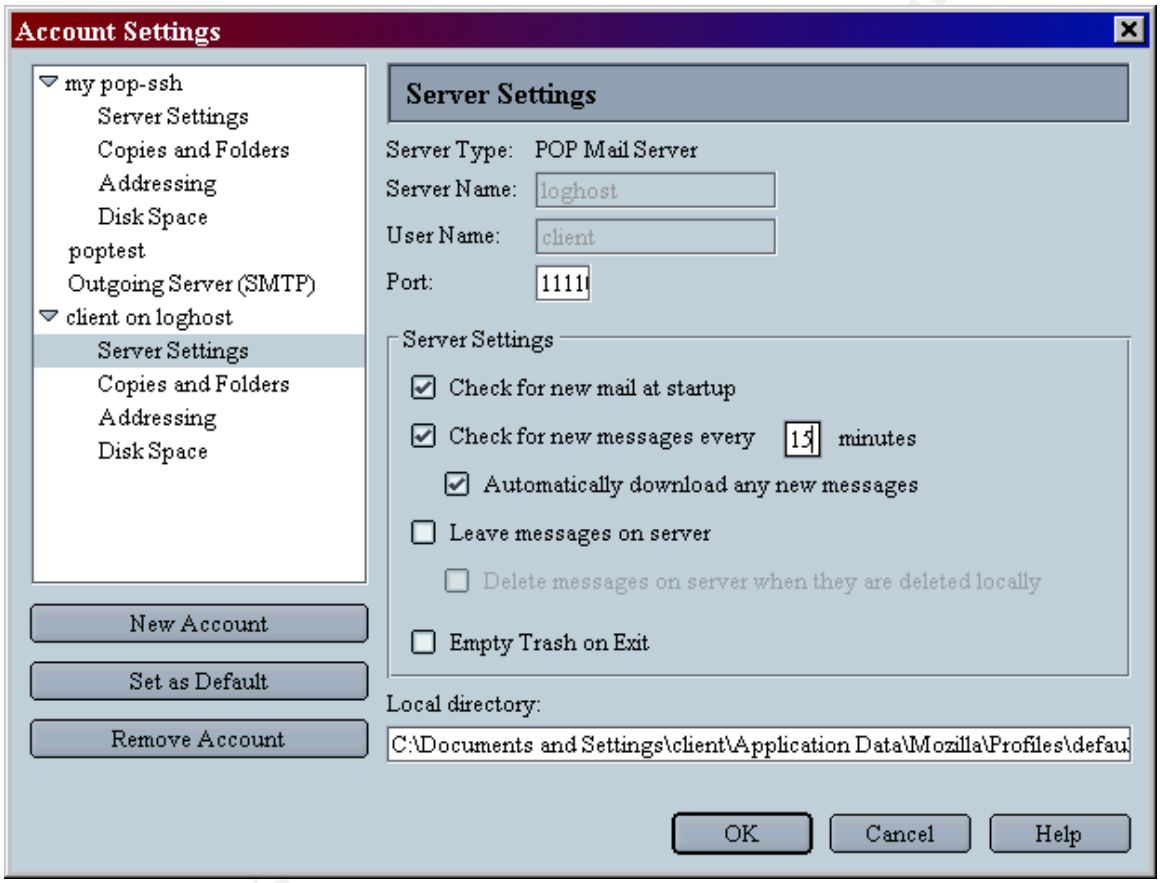


© SANS Institute 2000 - 2005 Author retains full rights.

Netscape (6.1) Mailer

Server Settings	
Server Name	[localhost]
User Name	[client]
Port	[11110]

See screen shot below



© SANS Institute 2000 - 2005 Author retains full rights.

REFERENCES

Cited References

[1] Chapman, D. Brent and Zwicky, Elizabeth D. "Building Internet Firewalls." Sebastopol, CA: O'Reilly & Associates, Inc. 1995.

[2] "Wietse's Tools and Papers ", ftp://ftp.porcupine.org/pub/security/index.html

[3] "IBM e-server Pseries Support", http://techsupport.services.ibm.com/rs6k/fixes/5L/ml/510001/510001.html

[4] "AIX 5L Version 5.1 Operating System", http://www-1.ibm.com/servers/aix/os

[5] "SecurityAdministration", http://www.unet.univie.ac.at/aix/aixbman/baseadmn/security_admin.htm

[6] "Command Reference, Volume 5. Syslog Daemon http://as400bks.rochester.ibm.com/doc_link/en_US/a_doc_lib/cmds/aixcmds5/syslogd.htm

[7] Seigert, Andreas. "The AIX Survival Guide." Addison-Wesley, 1996.

[8] "Performance Management Guide", http://as400bks.rochester.ibm.com/doc_link/en_US/a_doc_lib/aixbman/prftungd/prftungdtfrm.htm

[9] "AIX toolbox for Linux applications", http://www-1.ibm.com/servers/aix/products/aixos/linux

[10] Brotzman, Lee and Pomeranz, Hal. "Running Linux Applications Securely." The SANS Institute, 2001.

[11] Hunt, Craig. "Linux Sendmail Administration." Alameda, CA: Sybex, Inc., 2001.

[12] "documents/Servers_userguide.pdf", Tripwire for Servers Version 2.4.2 for UNIX Operating Systems, August 2001

[13] "SecureCrt Screen Shots", http://www.vandyke.com/products/securecrt/screenshots.html

[14] "Titan", http://www.fish.com/titan/lisa-paper.html

[15] "The Secure POP via SSH mini-HOWTO", http://yosh.gimp.org/Secure-POP-SSH-1.html

[16] "Watching Your Logs", http://www.enteract.com/~lspitz/swatch.html

Additional References

Garfinkel, Simson and Spafford, Gene. "Practical UNIX and Internet Security, 2nd edition." Sebastopol, CA: O'Reilly & Associates, Inc., 1996.

Barret, Daniel J. and Silverman, Richard E. "SSH the Secure Shell: The Definitive Guide." Sebastopol, CA: O'Reilly and Associates, Inc., 2001.

© SANS Institute 2000 - 2005 Author retains full rights.