

SECTION 11. SECURITY

The following access and security controls have been implemented in SARSS.

11.1 TCP Wrapper.

a. *Purpose.* TCP Wrapper will allow authorized FTP or TELNET access to this system based on the IP addresses contained in the /etc/hosts.allow file. In addition to filtering and monitoring FTP and TELNET, TCP Wrapper will also filter and monitor the following services, SYSTAT, FINGER, RLOGIN, RSH, TFTP and TALK. TCP Wrapper will log all attempted inbound network connections to a standard system log file, the /var/adm/tcpwrap.log.

b. *Adding and Deleting a User.* All valid FTP and TELNET users must be added to the TCP Wrapper hosts.allow file or the connection will be refused.

(1) SARSS1 - The **FTPUSER** and **FTPPASS** commands (F2) Add Login option will add a user IP automatically to the hosts.allow file in addition to establishing the user identification (RIC/DODAAC) and a password. The privilege for any user added with these commands is FTP access only. The (F4) Delete Login option will automatically remove the user's IP from the file. The UPDRT command will also automatically add records to the allow file.

(2) SARSS2A - The standard **FTPADD** command will add a user IP automatically to the hosts.allow file in addition to establishing the user identification (RIC) and a password. The privilege for any user added with this command is FTP access only. The **FTPDEL** command will automatically remove the user IP from the file.

c. *Maintaining the TCP Wrapper hosts.allow File.* The **ACCESS** command in SARSS1 and **TCPUTIL** command in SARSS2A are used to maintain the TCP Wrapper /etc/hosts.allow file. These are the only commands that can change the TCP IP privileges assigned to a user IP. Selecting one of three options from the TYPE OF ENTRY field for an IP performs this function. The options are: (1) FTP and TCP (TELNET), (2) FTP Only (Default if a user is added by the other commands discuss above), and (3) TCP Only (TELNET capability only).

NOTE: If the SARSS site is processing through an installation security firewall, the IP address of the firewall **may** need to be loaded in the hosts.allow file based on the installation-unique configuration of the firewall to allow FTP access.

AIS Manual 25-L1Y-AJT-ZZZ-EM (T)
AIS Manual 25-L14-AJQ-ZZZ-EM (T)
8 JAN 02

See figure 11-1. The following function keys provide navigation and update capability of the hosts.allow file.

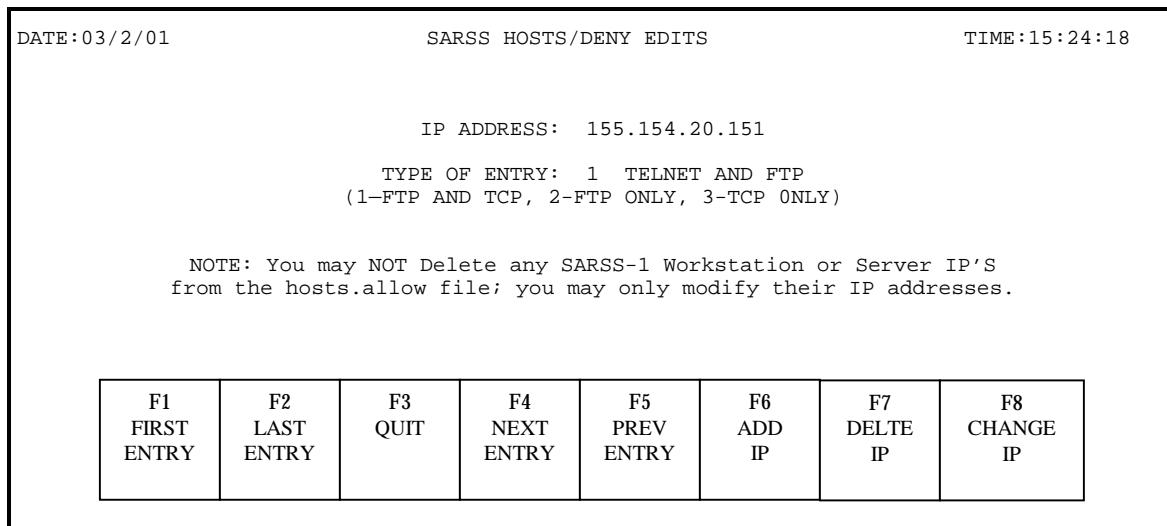


Figure 11-1. SARSS1 Access Submenu/SARSS2A TCPUTIL Submenu

NOTE: The SARSS2A **TCPUTIL Submenu** is the same as depicted above except the note reads “You may NOT Delete any SARSS2AD Workstations or Server IPs from the hosts.allow file; you may only modify their IP address.

- (1) (F1) FIRST ENTRY --- Brings up the first entry in the TCP Wrapper hosts.allow file (Sever IP).
- (2) (F2) LAST ENTRY --- Brings up the last entry in the TCP Wrapper hosts.allow file.
- (3) (F3) Quit --- Exits the menu and saves any changes.
- (4) (F4) NEXT ENTRY --- Brings up the next entry in the TCP Wrapper hosts.allow file.
- (5) (F5) PREV ENTRY --- Brings up the previous entry in the TCP Wrapper hosts.allow file.
- (6) (F6) ADD IP --- Add an IP to the TCP Wrapper hosts.allow file.

NOTE: This command should NOT normally be used to add new FTP users to the allow file, as the RIC (User Id) or password will not be added. This command is used after the initial load of the TCP Wrapper package to add currently established FTP users to ensure they are included in the hosts.allow file. New FTP users should be added with one of the commands discussed above.

(7) (F7) DELETE IP --- Removes an IP from the TCP Wrapper hosts.allow file.

(8) (F8) CHANGE IP --- Changes the selected IP in the TCP Wrapper host file to one you enter. It can also be used to change the Type of Entry.

d. *Reviewing the TCP Wrapper Log.* The TCP Wrapper Log, /var/adm/tcpwrap.log, should be reviewed at a minimum of at least once a week by the System Administrator for connectivity or unauthorized connection attempts. To review the log, log in as root and bring the file into vi or the Solaris text editor. The system automatically purges log data older than 30 days from the TCP Wrapper Log. An example of a TCPWRAPPER log is shown in figure 11-2.

AIS Manual 25-L1Y-AJT-ZZZ-EM (T)

AIS Manual 25-L14-AJQ-ZZZ-EM (T)

8 JAN 02

Example of a TCPWRAPPER Log

Successful Connections from TELNET

```
Jan 31 08:26:25 ajt01 in.telnetd[14708]: connect from ajt02
Jan 31 08:36:13 ajt01 in.telnetd[14969]: connect from ajt05
Jan 31 08:42:26 ajt01 in.telnetd[15177]: connect from ajt06
Jan 31 09:49:22 ajt01 in.telnetd[16854]: connect from ajt08
Jan 31 09:49:43 ajt01 in.telnetd[16861]: connect from ajt09
Jan 31 09:50:31 ajt01 in.telnetd[16925]: connect from ajt10
```

Successful Connections from FTP

```
Jan 31 09:52:04 ajt01 ajp8dp10[17011]: connect from MGT
Jan 31 16:46:03 ajt01 ajp8dp10[26602]: connect from WWF
Feb 14 15:33:04 ajt01 ajp8dp10[7859]: connect from ajt07
Mar 7 09:11:00 ajt01 ajp8dp10[27168]: connect from ajt04
```

Connections Refused from TELNET. Ensure that the LOGIN IDs or IP Addresses are not Authorized on the System

```
Jan 31 16:45:46 ajt01 in.telnetd[26569]: refused connect from S1028
Jan 31 16:45:46 ajt01 sendmail[26577]: QAA26577: from=root, size=192, class=0, pri=120192,
nrcpts=4, msgid=<200101312145.QAA26577@ ajt01.army.mil>, relay=root@localhost
Feb 4 23:28:42 ajt01 in.telnetd[18453]: refused connect from HHH
Feb 4 23:28:42 ajt01 sendmail[18461]: XAA18461: from=root, size=188, class=0, pri=120188,
nrcpts=4, msgid=<200102050428.XAA18461@ ajt01.army.mil>, relay=root@localhost
Feb 27 19:34:26 ajt01 in.telnetd[4968]: refused connect from h-64-105-46-175.bltmmdsn.covad.net
Feb 27 19:34:26 ajt01 sendmail[4976]: TAA04976: from=root, size=250, class=0, pri=120250,
nrcpts=4, msgid=<200102280034.TAA04976@ ajt01.army.mil>, relay=root@localhost
```

Connections Refused from FTP. Ensure that the LOGIN IDs or IP Addresses are not Authorized on the System

```
Feb 27 19:36:21 ajt01 ajp8dp10[5022]: refused connect from h-64-105-46-195.bltmmdsn.covad.net
Feb 27 19:36:21 ajt01 sendmail[5030]: TAA05030: from=root, size=250, class=0, pri=120250,
nrcpts=4, msgid=<200102280036.TAA05030@ ajt01.army.mil>, relay=root@localhost
Jan 31 16:46:32 ajt01 ajp8dp10[26612]: refused connect from WCW
Jan 31 16:46:32 ajt01 sendmail[26620]: QAA26620: from=root, size=190, class=0, pri=120190,
nrcpts=4, msgid=<200101312146.QAA26620@ ajt01.army.mil>, relay=root@localhost
```

Figure 11-2. Example of a TCPWRAPPER Log

NOTE: The bold heading titles do not appear in the log and are provided for clarification purposes.

11.2 SOLARIS Auditing and Accounting Report.

- a. The System Administrator should review this report on a weekly basis.
- b. To access Account Report menu:
 - (1) Logon to root.

- (2) From the terminal or console enter “darpt” and press <Enter>.
- (3) The Accounting Report Menu screen will appear with four options: (1) Print Report -- prints the report, (**Note that report may be very lengthy.**), (2) Display To The Screen -- lets you view the report on line, (3) Send Report to Diskette – writing the report to a diskette, (Note, if your system is suspected of comprise you may be requested to provide copies of your audit reports on diskette.), and (4) Exit the Report Menu – Returns you to root.
- (4) The system automatically purges report data greater than 30 days old from the audit report. An example of a DARPT log is shown in figure 11-3.

AIS Manual 25-L1Y-AJT-ZZZ-EM (T)
 AIS Manual 25-L14-AJQ-ZZZ-EM (T)
 8 JAN 02

| <u>FileSystem Space and Use</u> | | | | | | |
|---------------------------------|---------|--------|---------|----------|--------------|--|
| Filesystem | Kbytes | used | avail | capacity | Mounted on | |
| /dev/dsk/c1t0d0s0 | 1986078 | 972864 | 9536332 | 51% | / | |
| /dev/dsk/c1t0d0s6 | 966319 | 225006 | 683334 | 25% | /usr | |
| /proc | 0 | 0 | 0 | 0% | /proc | |
| fd | 0 | 0 | 0 | 0% | /dev/fd | |
| /dev/dsk/c1t0d0s3 | 483151 | 107840 | 326996 | 25% | /var | |
| /dev/dsk/c1t0d0s7 | 966319 | 19658 | 888682 | 3% | /ajp | |
| /dev/dsk/c1t0d0s5 | 1986078 | 192254 | 1734242 | 10% | /ajt | |
| /dev/dsk/c1t0d0s1 | 966319 | 192267 | 716073 | 22% | /usr/openwin | |
| swap | 166032 | 224 | 165808 | 1% | /tmp | |

| <u>System Commands Executed</u> | | | | | | |
|---|--|--|--|--|--|--|
| Feb 21 13:25 2001 DAILY REPORT FOR tripleh Page 1 | | | | | | |
| from Tue Feb 20 05:00:01 2001 | | | | | | |
| to Wed Feb 21 05:00:01 2001 | | | | | | |
| 1 runacct | | | | | | |
| 1 acctcon | | | | | | |

| <u>Devices Used and Length of Use</u> | | | | | | |
|---------------------------------------|---------|---------|--------|------|-------|--|
| TOTAL DURATION IS 1440 MINUTES | | | | | | |
| LINE | MINUTES | PERCENT | # SESS | # ON | # OFF | |
| /dev/pts/3 | 0 | 0 | 0 | 0 | 0 | |
| console | 1440 | 100 | 1 | 1 | 1 | |
| pts/4 | 1440 | 100 | 1 | 1 | 1 | |
| pts/3 | 2 | 0 | 1 | 1 | 1 | |
| TOTALS | 2882 | -- | 3 | 3 | 3 | |

| <u>Where and How Long Have Users Been Logged on</u> | | | | | | |
|---|------------|-------------------------|-------------------------|----------------------|-------------|--|
| Feb 21 13:25 2001 DAILY USAGE REPORT FOR tripleh Page 1 | | | | | | |
| | | | | | | |
| UID | LOGIN NAME | CPU (MINS) PRIME NPRIME | KCORE-MINS PRIME NPRIME | CONNECT (MINS) PRIME | DISK NPRIME | # OF BLOCKS # OF PROCS # DISK SESS FEE SAMPLES |
| 0 | TOTAL 0 | 3 0 | 3 0 | 3394 2946 | 1560 1322 | 0 19040 3 0 |
| 0 | cao 0 | 0 0 | 0 0 | 0 0 | 1560 1322 | 0 0 3 |
| 0 | root 0 | 3 0 | 3 0 | 3375 2941 | 0 0 | 0 18901 0 |
| 3 | ajt01 0 | 0 0 | 0 0 | 19 6 | 0 0 | 0 139 0 |

Figure 11-3. Example of a DARPT Log

AIS Manual 25-L1Y-AJT-ZZZ-EM (T)

AIS Manual 25-L14-AJQ-ZZZ-EM (T)

8 JAN 02

| <u>Which Commands Have been Executed and How Many Times for the Current Day</u> | | | | | | | | | | |
|---|----------------|-----------------------|------------------|-------------------|----------------|-----------------|---------------|-----------------|----------------|--|
| COMMAND NAME | NUMBER CMDS | TOTAL COMMAND SUMMARY | | | | | | | | |
| | | TOTAL KCOREMIN | TOTAL CPU-MIN | TOTAL REAL-MIN | MEAN SIZE-K | MEAN CPU-MIN | HOG FACTOR | CHARS TRNSFD | BLOCKS READ | |
| TOTALS | 19040 | 6702.31 | 5.54 | 3019.42 | 1210.35 | 0.00 | 0.00 | 149399040 | 2545 | |
| dtSCREEN | 435 | 2701.03 | 1.40 | 1294.84 | 1933.22 | 0.00 | 0.00 | 8993830400 | 2 | |
| dtTERM | 3 | 180.9 | 0.05 | 3.75 | 3457.63 | 0.02 | 0.01 | 5747712 | 0 | |
| uname | 1450 | 152.45 | 0.17 | 0.19 | 873.65 | 0.00 | 0.92 | 8718 | 0 | |
| find | 8 | 59.40 | 0.10 | 1.38 | 583.27 | 0.01 | 0.07 | 401 | 2213 | |
| who | 1442 | 51.23 | 0.23 | 0.24 | 218.62 | 0.00 | 0.98 | 10766656 | 0 | |
| vi | 21 | 23.94 | 0.02 | 25.83 | 1177.28 | 0.00 | 0.00 | 658943 | 73 | |
| more | 21 | 21.47 | 0.03 | 3.72 | 700.02 | 0.00 | 0.01 | 4200937 | 0 | |
| date | 129 | 12.36 | 0.02 | 0.02 | 741.40 | 0.00 | 0.70 | 163648 | 13 | |
| cp | 66 | 8.24 | 0.01 | 0.05 | 951.15 | 0.00 | 0.18 | 5552291 | 38 | |
| telnet | 3 | 7.11 | 0.01 | 332.05 | 1066.40 | 0.00 | 0.00 | 150808 | 0 | |
| sendmail | 3 | 1.49 | 0.00 | 0.02 | 1488.67 | 0.00 | 0.06 | 41178 | 15 | |
| darpt | 12 | 1.39 | 0.00 | 6.74 | 1385.33 | 0.00 | 0.00 | 7363 | 0 | |
| in.telne | 1 | 0.59 | 0.00 | 2.45 | 890.00 | 0.00 | 0.00 | 20216 | 0 | |
| cpio | 2 | 0.55 | 0.00 | 0.17 | 819.00 | 0.00 | 0.00 | 61240 | 0 | |
| <u>Which Commands Have been Executed and How Many Times for the Current Month</u> | | | | | | | | | | |
| Feb 21 05:00 2001 MONTHLY TOTAL COMMAND SUMMARY Page 1 | | | | | | | | | | |
| COMMAND NAME | NUMBER CMDS | TOTAL COMMAND SUMMARY | | | | | | | | |
| | | TOTAL KCOREMIN | TOTAL CPU-MIN | TOTAL REAL-MIN | MEAN SIZE-K | MEAN CPU-MIN | HOG FACTOR | CHARS TRNSFD | BLOCKS READ | |
| TOTALS | 555783 | 1230115.56 | 244.85 | 385174.48 | 5023.96 | 0.00 | 0.00 | 180322861056 | 185312 | |
| java | 35 | 646864.69 | 31.55 | 321.67 | 20501.65 | 0.90 | 0.10 | 236268272 | 42022 | |
| Xsun | 3 | 255724.54 | 39.12 | 1218.28 | 6536.84 | 13.04 | 0.03 | 215975424 | 74 | |
| dtSCREEN | 8201 | 107243.14 | 54.22 | 24580.79 | 1978.00 | 0.01 | 0.00 | 170853744640 | 10 | |
| soffice. | 2 | 42159.61 | 0.75 | 10.45 | 56564.78 | 0.37 | 0.07 | 135626752 | 299 | |
| setup.bi | 4 | 39987.97 | 2.07 | 12.47 | 19342.78 | 0.52 | 0.17 | 469585920 | 7548 | |
| jre | 7 | 22841.11 | 1.06 | 84.71 | 21511.01 | 0.15 | 0.01 | 28817792 | 29 | |
| ps | 61646 | 20808.85 | 31.73 | 36.50 | 655.89 | 0.00 | 0.87 | 1751396544 | 27 | |
| sh | 92039 | 17091.37 | 12.13 | 7822.22 | 1408.82 | 0.00 | 0.00 | 175705584 | 259 | |
| dtexec | 8320 | 11651.33 | 4.75 | 25004.43 | 2452.66 | 0.00 | 0.00 | 76439842 | 32 | |
| wc | 57695 | 6243.61 | 6.82 | 55.83 | 915.66 | 0.00 | 0.12 | 3655563 | 0 | |
| awk | 28959 | 4689.37 | 5.18 | 10.98 | 905.13 | 0.00 | 0.47 | 2713835 | 0 | |
| dtTERM | 155 | 4349.04 | 1.17 | 10421.79 | 3719.25 | 0.01 | 0.00 | 91406120 | 30 | |
| ajsmqp.r | 11824 | 4280.31 | 4.17 | 32.30 | 1027.19 | 0.00 | 0.13 | 14803733 | 20 | |
| uname | 29338 | 3069.45 | 2.85 | 3.16 | 1078.89 | 0.00 | 0.90 | 176760 | 1 | |
| grep | 65896 | 2931.77 | 4.71 | 7.42 | 622.96 | 0.00 | 0.63 | 254724976 | 11 | |
| acctcom | 36 | 2877.16 | 3.33 | 3.39 | 863.49 | 0.09 | 0.98 | 42679616 | 34 | |
| stty | 28920 | 2810.45 | 2.10 | 2.29 | 1337.57 | 0.00 | 0.92 | 980581 | 0 | |
| dtsessio | 11 | 2464.52 | 0.54 | 17139.73 | 4535.93 | 0.05 | 0.00 | 16732332 | 10 | |
| SolarisN | 16 | 2284.38 | 3.18 | 405.58 | 719.11 | 0.20 | 0.01 | 578278464 | 1246 | |

Figure 11-3. Example of a DARPT Log

AIS Manual 25-L1Y-AJT-ZZZ-EM (T)
 AIS Manual 25-L14-AJQ-ZZZ-EM (T)
 8 JAN 02

| <u>The Last Time a User Logged In</u> | | | | | | |
|--|-------|----------|----------|----------|----------|--------|
| Feb 21 05:00 2001 LAST LOGIN Page 1 | | | | | | |
| 00-00-00 | adm | 00-00-00 | ajt09 | 00-00-00 | nobody4 | |
| 00-00-00 | ajt | 00-00-00 | ajt10 | 00-00-00 | nuucp | |
| 00-00-00 | ajt01 | 00-00-00 | bin | 00-00-00 | shutdown | |
| 00-00-00 | ajt02 | 00-00-00 | daemon | 00-00-00 | smtp | |
| 00-00-00 | ajt03 | 00-00-00 | listen | 00-00-00 | sys | |
| 00-00-00 | ajt04 | 00-00-00 | lp | 00-00-00 | uucp | |
| 00-00-00 | ajt05 | 00-00-00 | mgt | 01-01-27 | ajt07 | |
| 00-00-00 | ajt06 | 00-00-00 | noaccess | 01-02-20 | root | |
| 00-00-00 | ajt08 | 00-00-00 | nobody | 01-02-21 | cao | |
| <u>Commands Executed by the System and all Users</u> | | | | | | |
| NAME | USER | TTYNAME | TIME | TIME | (SECS) | FACTOR |
| #accton | root | ? | 05:00:00 | 05:00:00 | 0.01 | 0.01 |
| turnacct | root | ? | 05:00:00 | 05:00:00 | 0.05 | 0.01 |
| who | root | ? | 05:01:00 | 05:01:00 | 0.01 | 0.01 |
| awk | root | ? | 05:01:00 | 05:01:00 | 0.02 | 0.01 |
| stty | root | ? | 08:11:00 | 08:11:00 | 0.01 | 0.01 |
| uname | root | ? | 08:11:00 | 08:11:00 | 0.01 | 0.01 |
| sh | root | ? | 08:11:00 | 08:11:00 | 0.13 | 0.01 |
| #sh | root | ? | 08:11:00 | 08:11:00 | 0.14 | 0.01 |
| ls | root | pts/4 | 08:11:23 | 08:11:23 | 0.03 | 0.02 |
| more | root | pts/4 | 08:11:23 | 08:11:23 | 0.05 | 0.02 |
| ls | root | pts/4 | 08:12:03 | 08:12:03 | 0.01 | 0.01 |
| more | root | pts/4 | 08:12:03 | 08:12:03 | 0.02 | 0.01 |
| expr | root | pts/4 | 08:12:17 | 08:12:17 | 0.01 | 0.01 |
| tput | root | pts/4 | 08:12:17 | 08:12:17 | 0.01 | 0.01 |
| tput | root | pts/4 | 08:12:17 | 08:12:17 | 0.01 | 0.01 |
| pt_chmod | root | ? | 08:12:17 | 08:12:17 | 0.01 | 0.01 |
| mi | root | pts/4 | 08:12:17 | 08:12:17 | 0.16 | 0.01 |
| #vi | root | ? | 08:12:17 | 08:12:34 | 17.96 | 0.03 |
| xterm | root | pts/4 | 08:12:17 | 08:12:35 | 18.04 | 0.08 |
| expr | root | pts/4 | 08:12:58 | 08:12:58 | 0.01 | 0.01 |
| tput | root | pts/4 | 08:12:58 | 08:12:58 | 0.01 | 0.01 |
| tput | root | pts/4 | 08:12:58 | 08:12:58 | 0.01 | 0.01 |
| grep | root | ? | 08:28:00 | 08:28:00 | 0.01 | 0.01 |
| wc | root | ? | 08:28:00 | 08:28:00 | 0.05 | 0.01 |
| grep | root | pts/3 | 12:44:19 | 12:44:19 | 0.01 | 0.01 |
| sed | root | pts/3 | 12:44:19 | 12:44:19 | 0.02 | 0.01 |
| who | root | pts/3 | 12:44:19 | 12:44:19 | 0.01 | 0.01 |
| sh | root | pts/3 | 12:44:19 | 12:44:19 | 0.02 | 0.01 |
| ajsd5p.r | root | pts/3 | 12:44:19 | 12:44:19 | 0.17 | 0.03 |

Figure 11-3. Example of a DARPT Log

NOTE: The bold heading titles do not appear in the report and are provided to clarify these report entries.