

### I.3: Developments in networking and communication at RRCAT

#### A) Email service related developments and enhancements:

##### 1) Design, Development and Deployment of an automated bulk email sender detection and monitoring software:

Email server at RRCAT, receives large number of SPAM emails, which are delivered to users with a [SPAM] tag in the header, for identification. Processing of such email overloads the mail server and degrades its performance. To block such users from sending bulk emails in future, software has been developed.

The developed software, continuously monitors the logs of the email server for the size (including attachment) of emails received from each sender email id, on an hourly and daily basis and generates a list of all email ids which cross a defined threshold (e.g X MB per hour and Y MB per day) limit. The list is then merged with the list of blocked email ids of the mail server.

The software has provision to change both the threshold values – hourly and daily - conveniently. Currently, both the thresholds have been set to 300MB (X=Y=300), i.e a sender email id exceeding 300MB of total email data transfer to RRCAT domain, in an hour or in a day, will be blocked from sending further emails to RRCAT users. This improves the performance of email server by reserving resources for legitimate usage.

#### B) Internet Proxy service related enhancements and developments for network security:

The Internet proxy server farm setup, has been reconfigured and enhanced to block requests for anonymous surfing (using the popular anonymous 'Tor browser' and other anonymous web sites). This has been done to ensure that all Internet accesses by RRCAT users are logged properly.

The popular free desktop sharing application using the 'Team Viewer' software has been blocked on Internet proxy servers, to comply with the latest network security policy. This has been done to ensure that the security of the network is not compromised by unknowingly routing the traffic to some third party servers. Users are requested to note that the only secured way to access RRCATNet resources is by using the VPN tunnel software, as developed and recommended by RRCAT.

#### C) Commissioning of a new enhanced Network Security Monitoring Setup:

A new network security monitoring and analysis setup is commissioned with latest intrusion detection and traffic monitoring software. New OSSIM (64 bit version 4.1), which is an open-source SIEM (Security Incident Event Manager), Nfsen which an open source traffic profiler, NetDisco which is an open source network management software and network traffic sensor servers are configured for the setup.

Network Intrusion Detection System (SNORT) and Network asset health monitoring system (Nagios) plugins have been configured on OSSIM Currently 1030 assets, including servers, network switches and client PCs, are being monitored using this setup. Figure I.3.1, depicts the network asset health monitoring panel.

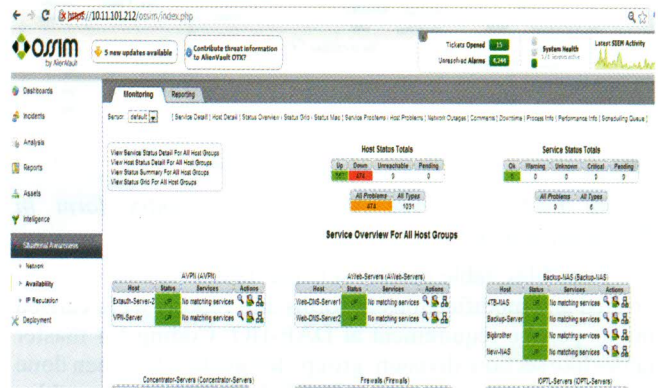


Figure I.3.1: Network asset health monitoring panel

Security incident alarms and security events can be monitored using this setup, as depicted in Figure I.3.2 and Figure I.3.3.

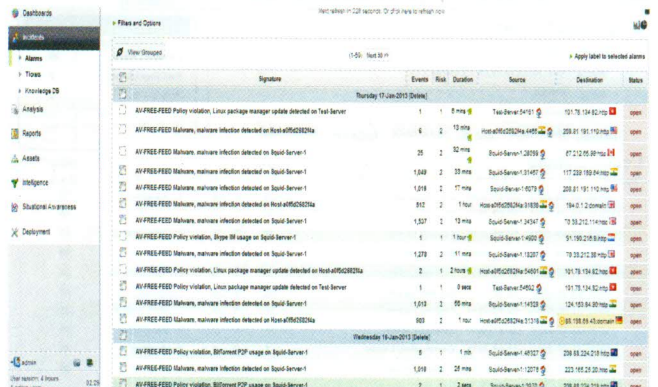


Figure I.3.2: Network security incident alarms window

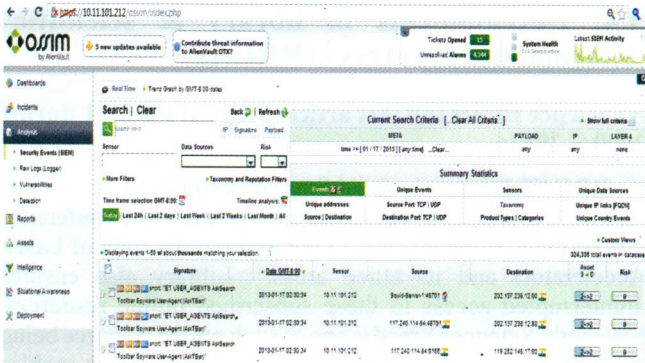


Figure I.3.3: Network Security events window

Email alerts are configured on the server for generating threat notifications for unauthorized attempts to access Internet DMZ (De Militarized Zone) resource accesses, as depicted in Figure I.3.4.

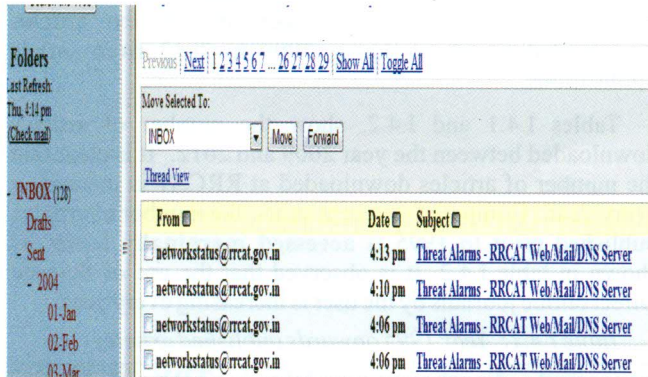


Figure I.3.4: Network Security events display window

D) Internet DMZ web server security enhancements:

Two web servers are located in Internet DMZ of RRCAT. One web server, hosts email access over Internet application and other hosts online recruitment and Ph.D registration application. In order to further strengthen the security of these web servers, SSL (Secure Socket Layer) certificate has been installed on the servers to enable secure data transmission on Internet. The data of these sites are encrypted with 256 bit key, before transfer over Internet. The servers are secured with Verisign class 3 certificates. Both the web servers are scanned every day for presence of malwares in them. Figure I.3.5, depicts the secured first page of the webmail facility, provided over Internet, with the Norton Security seal. Figure I.3.6, depicts the secured first page of the online recruitment and Ph.D registration application with the Norton Security seal.

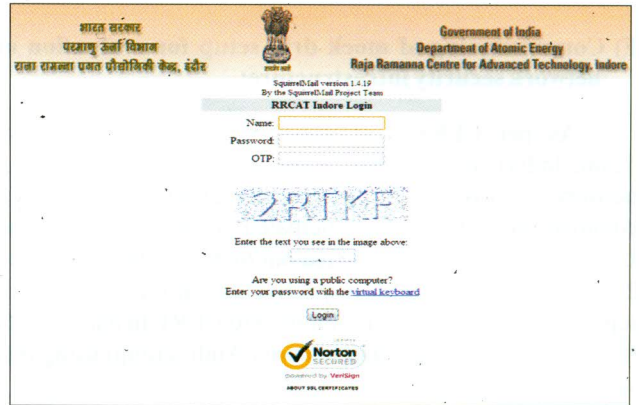


Figure I.3.5: First page of webmail over Internet website with Norton Security Seal

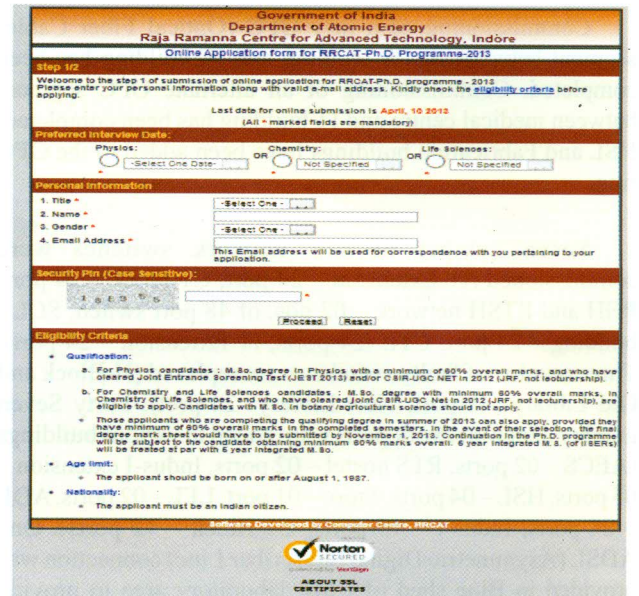


Figure I.3.6: First page of online Ph.D. registration website with Norton Security Seal

E) Design and Development of routine network servers and services status monitoring and consolidated reporting application:

Various routine tasks related to upkeep of important networking servers and critical services are performed on a daily basis. To automate the checking procedure and generate consolidated reports, various scripts have been developed. These scripts are placed on respective servers. By executing the scripts on each of the servers manually, on a daily basis, a consolidated checklist report is generated. A web based application is developed to view the consolidated status and upkeep related reports of all the servers. The reports are archived and can be searched datewise. This helps in proactive management of the numerous network components and thus increases the uptime of the network services.



**F) Commissioning of mock drill setup for evaluation of network security infrastructure:**

As per CERT-In (Computer Emergency Response Team, India) requirements, a mock drill setup for testing network security related preparedness at RRCAT, has been commissioned. RRCAT participated in both Layer-II and Layer-III mock drills, as carried out by CERT-In, on 19<sup>th</sup> and 20<sup>th</sup> of December 2012 respectively. Various mock drill reports were prepared and submitted to CERT-In and CISAG (Computer Installations and Security Audit group) using this setup.

**G) RRCATNet Planning, Expansion and Upgradation:**

Commissioning of a new OFC (Optical Fiber Cable) segment between SCLS building and IT building has been completed. Commissioning of an alternate OFC segment between medical centre and IT building has been completed. HSL and Fabrication buildings have been added to the OFC ring.

Seven number of new network switches were commissioned (IT Extension – 24 port, C1-block – 24 port, PGH and RTSH network – 02 nos. of 48 port switch, SCLS building – 24 port, CTL -24-ports, IT Extension – 24 port). Three number of faulty switches were replaced (H-Block and Old Library- 48-port, New-Library- 24-port). Forty Seven number of new network ports were added in various buildings (AECS – 02 ports, RTS hostel – 02 ports, Indus-I extension – 05 ports, HSL – 04 ports, Store – 01 port, LFL – 02 ports, ADL – 04 ports, Indus-I – 15 ports, C1 Block – 12 ports). One ADSL (Asymmetric Digital Subscriber Line) connection was provided in Blue shed of CME laboratory area to provide network connectivity to three users. Rack installation has been completed in five buildings (CTL building, Indus user hall building, LBAID building, UHV and MFL building).

**H) Expansion of communication network:**

58 number of new telephone connections were provided at various locations in RRCAT campus, 27 telephone connections were shifted to other location as per user requirement, 7 additional telephone lines were commissioned in new SCRF building.

*Reported by:  
S. S. Tomar (tomar@rrcat.gov.in), Anil Rawat and  
colleagues*

**I.4: Developments in library & scientific information resources at RRCAT**

**A) Science Direct full text article usage at RRCAT during 2009 to 2012:**

RRCAT Library is providing subscription based online scientific information resources such as journals, conference proceedings, standards etc. to the users in the field of Laser, Accelerators and its allied areas. Library also ensures uninterrupted access to these subscribed online resources. Elsevier's 'Science Direct' is one of such online resource being subscribed through DAE libraries consortium, which enables campus wide full text access of scholarly literature to the users. The Science Direct in its platform offers full text content to over 3687 serial publications and 15662 non-serial publications of various publishers such as Elsevier, Pergamon Press, Academic Press, etc. However, RRCAT Library has access (subscription) to full text content of 2397 serials, 140 complimentary serials, and 322 non-serials collections. This article briefly reports the number of full text articles downloaded /accessed during 2009 to 2012 from serials publications.

Tables I.4.1 and I.4.2, show the number of articles downloaded between the year 2009 and 2012. It is clear that the number of articles downloaded at RRCAT is increasing every year. Compared to recent years, the number of articles published prior to 1995 is **accessed marginally** lesser, as shown in table I.4.2, It is observed that the use of Science Direct online journals by the user is increasing every year.

*Table I.4.1: Year 1995 onwards published articles*

Accessed Year	Number of Journals Used	TDY HTML	TDY PDF	TDY Total
2009	914	16272	27422	43694
2010	967	16482	30482	46964
2011	978	17859	30636	48495
2012*	880	14343	23365	37708
TDY = Total Downloads in a Year		* --> Till October 2012		

*Table I.4.2: Prior to 1995 published articles*

Accessed Year	Number of Journals Used	TDY HTML	TDY PDF	TDY Total
2009	132	6	3762	3768
2010	161	6	7346	7352
2011	168	28	6770	6798
2012*	147	1	5708	5709
TDY = Total Downloads in a Year		* --> Till October 2012		