E) Enhancement and revamping of RRCAT website for complying to GoI(Government of India) guidelines:

RRCAT website was enhanced and modified as per compliance matrix specified in GoI guidelines. The website was re-designed and revamped with new look and feel and also fine tuned by making changes under the headings (of GoI guidelines compliance matrix) like Government of India Identifiers (link to Home page of National Portal etc.), Building confidence (disclaimer, copy right, hyper linking policy etc.), Scope of contents (News, Contact Us, Secondary Content as per archiving policy etc.), Quality of contents (Documents with Timestamps etc.), Design (Alternate text provision etc.), Development (Meta Data for keywords etc.) and website hosting (security of website, regular backup of the website for disaster recovery purpose etc.).

Reported by:
Alpana Rajan (alpana@rrcat.gov.in) and Anil Rawat

I.3: Development in Networking and Communication at RRCAT

A) Commissioning of VPN connectivity setup for XRD beam line (BL12) at Indus-2

VPN connectivity setup was designed, developed and implemented for remote access of RRCATNet resources over internet. Software tools used for VPN setup implementation are OpenVPN v2.1 (GUI application for OpenVPN on Windows), fwbuilder V4.0 (Firewall Management Software), CreateInstall free Software V4.14.5 (VPN Client Installation file builder), Fedora Directory Server V1.2 (for VPN User database) and phpLDAPadmin V0.9.3 (for Access to VPN user database). Strong password and digital certificate based authentication technique has been used to allow only pre-registered users the access to the pre-identified resource, for a pre defined duration.

As a proof of concept, the VPN setup is being used to provide access to an instrumentation setup named "SPEC", procured from M/S. Certified Scientific Software, Cambridge. This setup is being used on XRD beam line (BL12) at Indus-2. To enable the vendor, to securely install some new features of the software and test its working with new x-ray detector, over Internet, the VPN connectivity is being provided using the recently commissioned setup.

B) Commissioning of Open Source Security Information Management (OSSIM) based Security Analysis and Management setup

OSSIM based security analysis and management setup is commissioned to monitor and log complete network traffic, related to Internet, Intranet, Anunet, DAEGrid and National

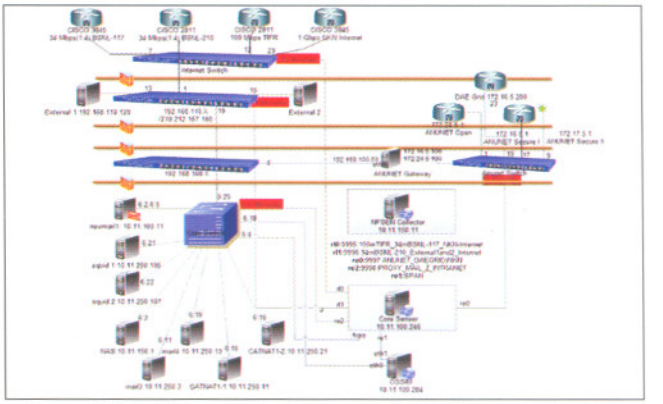

Figure I.3.1: Schematic diagram of OSSIM based Security Analysis and Management setup

#	Alarm	Risk	Sensor	Since
				Friday 21-Jan-2011
351	P2P BitTorrent: torrent download by 210.212.157.170	1	ossim.rrcat.gov.in	2011-01-21 16:35:02
352	AVT-FEED Spyware Fun Web Products Agent detected on 10.29.2.159	2	ossim.rrcat.gov.in	2011-01-21 16:44:28
353	AVT-FEED BitTorrent usage on 210.212.157.170	6	ossim.rrcat.gov.in	2011-01-21 16:36:49
354	AVT-FEED Spyware Fun Web Products Agent detected on 10.125.2.248	2	ossim.rrcat.gov.in	2011-01-21 16:35:50
355	AVT-FEED Spyware Fun Web Products Agent detected on 10.29.2.149	2	ossim.rrcat.gov.in	2011-01-21 16:19:58
356	AVT-FEED Spyware Fun Web Products Agent detected on 10.28.2.79	2	ossim.rrcat.gov.in	2011-01-21 16:08:31
357	AVT-FEED Spyware Fun Web Products Agent detected on 10.28.2.176	2	ossim.rrcat.gov.in	2011-01-21 15:32:38
358	AVT-FEED Spyware Fun Web Products Agent detected on 10.26.2.242	2	ossim.rrcat.gov.in	2011-01-21 15:24:24
359	AVT-FEED Spyware Fun Web Products Agent detected on 10.125.2.26	2	ossim.rrcat.gov.in	2011-01-21 15:22:42

Figure I.3.2: Snapshot of Report regarding network traffic related to threat Incidents and events

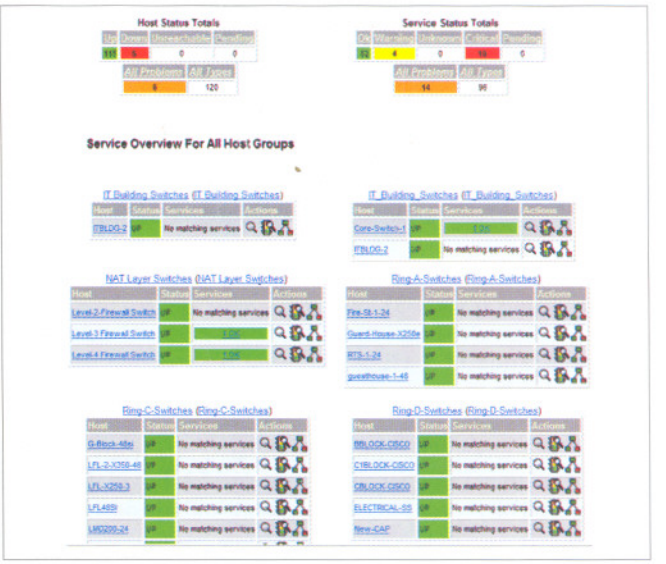

Figure I.3.3: Snapshot of Network fabric status view, both host and service wise

```
** nfdump -M /usr/local/nfsen/profiles-data/live/34mBSNL-210_External-1and2_
nfdump filter:
dst ip 210.212.157.164
Top 10     IP Addr ordered by flows:
Date first seen          Duration Proto          IP Addr    Flows  Packets
2010-11-11 14:32:43.848   296.843 any     210.212.157.164      215      728
2010-11-11 14:33:15.034   244.318 any      122.200.19.24       22      264
2010-11-11 14:33:13.631     0.584 any      192.25.218.38        6        6
2010-11-11 14:34:43.942     0.061 any       202.56.230.5        5        5
2010-11-11 14:34:41.017    44.099 any       202.56.240.5        5        5
2010-11-11 14:37:40.354     0.337 any      196.43.38.189        5        5
2010-11-11 14:35:37.667     1.324 any      125.160.4.82         4        4
2010-11-11 14:34:44.003    43.449 any       202.56.230.6        4        4
2010-11-11 14:37:37.288     0.076 any      203.115.71.66        4        4
2010-11-11 14:33:15.638    92.463 any     88.179.196.197        4       34

Summary: total flows: 215, total bytes: 104881, total packets: 728, avg bps:
Time window: 2010-11-11 14:31:58 - 2010-11-11 14:37:58
Total flows processed: 36884, Records skipped: 0, Bytes read: 1918004
Sys: 0.002s flows/second: 12302868.6 Wall: 0.002s flows/second: 13881821.6
```

Figure I.3.4: Snapshot of Network flow report for 34Mbps BSNL Link

Knowledge Network (NKN), networks. The setup is being used for both real time and forensic analysis, by generating online alarms and reports. These alarms and reports provide comprehensive information about the network security threats relevant to our organizational network. Port mirroring technique - available in the managed switches - has been used to collect the traffic flowing on the network. Open source freeware software tool named OSSIM, has been used in the implementation. Figure I.3.1, depicts the logical layout of the setup and figures I.3.2, I.3.3 and I.3.4 are snapshots of the various reports generated using the setup.

C) Commissioning of 34 Mbps (1:4) leased line from BSNL

A new 34 Mbps (1:4) shared bandwidth, Internet link from M/s. BSNL, was commissioned in addition to the already existing 34 Mbps (1:4) shared bandwidth Internet link from same ISP for Internet browsing and file downloading facilities on RRCATNet. Both the links are configured in load balancing and failover mode. The load balancing configurations have allowed us to use both the links seamlessly for outgoing traffic, thus aggregating available outgoing bandwidths of both the links. The failover configuration allows automated shifting of outgoing traffic to the active link in case of single link failures. Network address translation configurations have been carried out on link concentrators, to seamlessly allow incoming traffic to access the domain, web and email services in load balanced and failover mode, Figures I.3.5 and I.3.6 depict typical utilization of the two links on a working day.

D) Integration of 1 Gbps National Knowledge Network (NKN) link in the common pool of internet links.

The 1 Gbps NKN link is integrated in already existing pool of Internet links consisting of two 34 Mbps (1:4) shared links from BSNL, for Internet browsing and file downloading facilities on RRCATNet. The link is configured in load balancing and failover mode. Network address translation configurations have been carried out on link concentrators, to seamlessly allow incoming traffic to access the domain, web

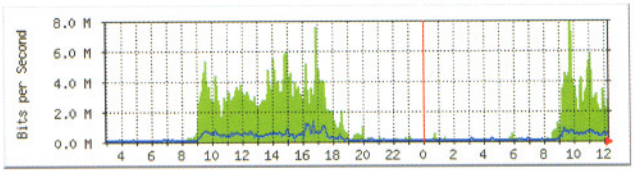

Figure I.3.5: New 34 Mbps (1:4) link usage graph

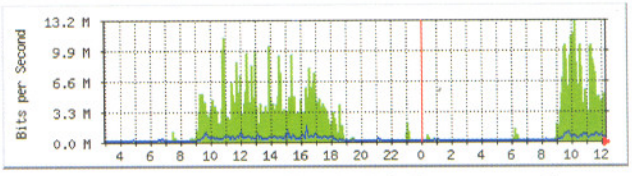

Figure I.3.6: Old 34 Mbps (1:4) link usage graph

and email services in load balanced and failover mode, Figures I.3.7 depicts the typical utilization of the links on a working day.

E) Expansion of communication Network

Nine numbers of new phone connections were provided at various locations in RRCAT campus. Twenty five number of telephone connections, were shifted to other locations. Mobile facility has been enabled for twenty users. Ten number of digital reflex phones were installed with voice mail facility for SO/G officers, as per norms.

F) RRCATNet Planning, Expansion and Upgradation

Five number of newly configured, refurbished switches were replaced in MIA, Fabrication building, Library, G-Block, ADL and LFL buildings. Three number of new points were added to the purchase network. Coordination work for

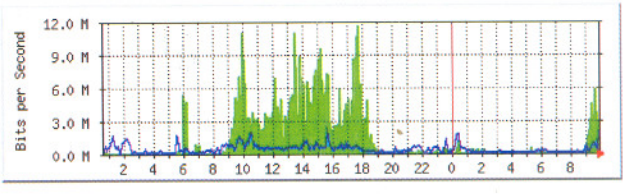

Figure I.3.7: 1 Gbps NKN link usage graph

shifting of 16 points in purchase building for new office cubicles was carried out. A network consisting of sixty ports was completed in IT Extension building. OFC laying between IT building and IT extension for 8(single mode) + 8(multi mode) cores was completed. OFC laying for 14 nos. of segments of phase-V was started. UPS/PAC installation / commissioning work in IT Extension was completed. Core switch installation in IT Extension building was initiated.

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