PROJECT REPORT

Under Guidance of

Mr. Anupam Chanda
SENIOR ENGINEER ICT & SERVICES GROUP
C-DAC Kolkata
Plot - E-2/1, Block-GP, Sector-V
Salt Lake Electronics Complex
Bidhannagar, Kolkata - 700 091
Westbengal (India)

Project Title

Secure Network Architecture Planning

Submitted By

Saikat Adhikary(AU/2016/02/00782)

Name and Address of the Institution

Adamas University

(Barasat-Barrackpore Road,Barbaria,P.O.-Jagannathpur, District-24 Parganas(North),Kolkata-700126,Kolkata,India)

Date of Submission

27/07/ 2018

CERTIFICATE

Date: 27th July, 2018

Place: Salt Lake City, Kolkata

This is to certify that Saikat Adhikary of Adamas University (School of Engineering & Technology), Department of Computer Science and Engineering has successfully completed a project on "Secure Network Architecture Planning" as a record for Final Year 7th Semester Subject "Industrial Summer Training/Internship" at C-DAC Kolkata, under my guidance.

[Mr. Anupam Chanda]

Senior Engineer

C-DAC Kolkata

ACKNOWLEDGEMENT:-

I am thankful to Dr. Nabarun Bhattacharya(Center Head, CDAC Kolkata) for his kind permission to work in this project.

I am highly indebted to Dr. Amit Chaudhuri (Group Head, ICT & Services, CDAC Kolkata) for his valued guidance received during building of this project & for getting his generous help in every manner.

I pay my best regard to Mr.Anupam Chanda(Senior Engineer, CDAC Kolkata) and Mr. Aniruddha Datta(Project Engineer, CDAC kolkata) for their constant guidance & encouragement during the course of my project in Network Security Section. I am also thankful to Mr.Abhijit Chatterjee (Project Engineer, Language Technology Section, CDAC Kolkata) for his technical help and constant inspiration.

My sincere thanks to Mr. Jayanta Talapatra & Mr. Atanu Mitra(Career and Development Officer, Adamas University) for their strong recommendation that helped me to get into a prestigious institute like CDAC Kolkata.

……..……..

(Saikat Adhikary)

School of Engg. and Technology, B.Tech, CSE

TABLE OF CONTENTS:-

ABSTRACT: -

Our project of designing a secure network architecture basically deals with upgradation of various campus network policies in terms of security and management. So over here we have basically planned an network architecture of a ASUJS University Campus in terms of security by using open source user/captive portal authentication software and in terms of management by using open source log server management software along with network management software which includes genetic wireless controller software for managing all the Access Points. So various kinds of software solutions were provided in order to secure the network infrastructure of ASUJS Campus.

INTRODUCTION:-

Network architecture is the design of a communication_network as shown in Fig1. It is a framework for the specification of a network's physical components and their functional organization and configuration, its operational principles and procedures, as well as data formats use. In telecommunication, the specification of a network architecture may also include a detailed description of products and services delivered via a communications network, as well as detailed rate and billing structures under which services are compensated.

The network architecture of the Internet is predominantly expressed by its use of the Internet Protocol Suite, rather than a specific model for interconnecting networks or nodes in the network, or the usage of specific types of hardware links.

A computer network consists of computers and devices connected to one another. Information can be transferred from one device to the next. For example, an office filled with computers can share files together on each separate device. Computer networks can range from a local_area_network(LAN) to a wide_area_network (WAN). The difference between the types of networks is the size. These types of computer networks work at certain speeds, also known as broadband. The Internet network connects computers worldwide.

Internet network: access to the network allows users to use many resources. Over time the Internet network will replace books. This will enable users to discover information almost instantly and apply concepts to different situations. The Internet can be used for recreational, governmental, educational, and other purposes. Businesses in particular use the Internet network for research or to service customers and clients.

So over here in our project we are trying to design a upgraded network design of a university campus enabling various kinds of security and management policy.

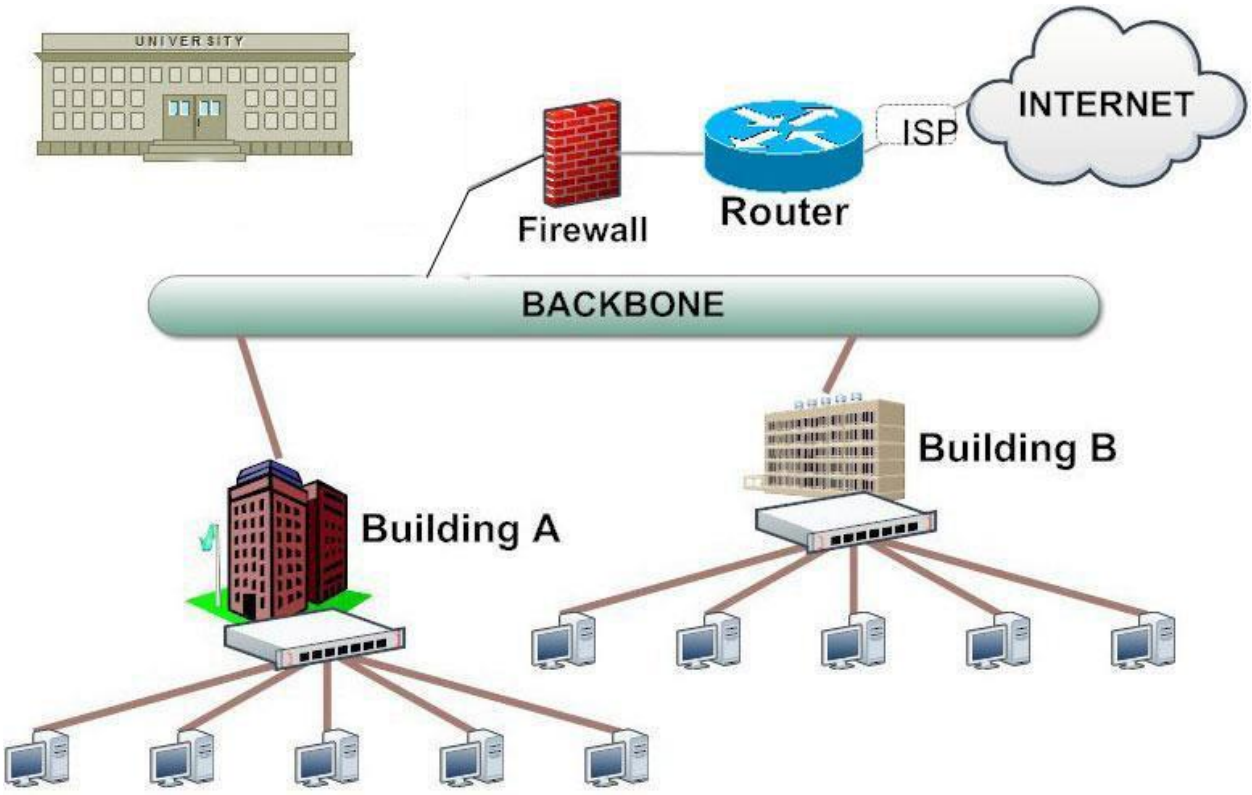


Fig 1: An example of a campus network architecture planning

ABOUT ASUJS: -

The Advancen State University of Juridical Sciences was established under the ASUJS Act, 1976 (Indian State Act IX of 1976) adopted by the West Bengal Legislature in July, 1976. The University was notified under Clause (f) of Section 2 of the UGC Act, 1956 in August 1977 and has been granted permanent affiliation by the Bar Council of India in July 1977.

The Advancen State University of Juridical Sciences (ASUJS) is one of the premiere national law schools of India. It has constantly been ranked as one of the top law schools of India. ASUJS, in its short existence, of about a decade or so has produced outstanding lawyers and legal scholarship. ASUJS has a very rich faculty, with diverse backgrounds, drawn from almost all corners of India. ASUJS faculty has been trained in top universities in India and abroad and has been constantly involved in delivering quality teaching and research. The faculty members of ASUJS have made a name for themselves, in their respective fields, by publishing research in reputed journals in India and abroad and with renowned publishing houses and are playing a key role in pushing the frontiers of legal knowledge and expertise. ASUJS has also attracted leading academicians, as visiting faculties, from top universities such as University of Sydney, University of London, National University of Singapore, Freiburg University and others. Students that have passed out from ASUJS are working in top law firms in India and abroad, some are practicing in courts and some have entered the field of legal academics and are teaching in India and abroad. Many of the ASUJS students have been awarded prestigious scholarships such as Rhodes, Felix and Chevening for higher studies in the United Kingdom and also in the United States and other leading universities. ASUJS under the inspiring leadership of its Vice Chancellor, Prof. K. Niranjan, one of the most respected and renowned legal scholars of India, is striving to become a centre of excellence. It is keen to attract talented faculties and students and further enrich its academic environment for cutting edge teaching and research.

The objectives of the University, inter alia, are to:

a. advance and disseminate learning and knowledge of law and legal processes and their role in national development.

b. promote legal knowledge and to make law and the legal process efficient instruments of social development.

c. develop in the student and research scholar a sense of responsibility to serve society in the field of law by developing skills with regard to advocacy, legal service, legislation, law reforms and the like.

d. promote inter-disciplinary study of law in relation to management, technology, international cooperation and development.

ABOUT CDAC's WORK & WHY CDAC IS ENTRUSTED TO REVIEW: -

Centre for Development of Advanced Computing (C-DAC) is the premier R&D organization of the Ministry of Electronics and Information Technology (MeitY) for carrying out R&D in IT, Electronics and associated areas. Different areas of C-DAC, had originated at different times, many of which came out as a result of identification of opportunities.

- The setting up of C-DAC in 1988 itself was to built Supercomputers in context of denial of import of Supercomputers by USA. Since then C-DAC has been undertaking building of multiple generations of Supercomputer starting from PARAM with 1 GF in 1988.
- Almost at the same time, C-DAC started building Indian Language Computing Solutions with setting up of GIST group (Graphics and Intelligence based Script Technology); National Centre for Software Technology (NCST) set up in 1985 had also initiated work in Indian Language Computing around the same period.
- Electronic Research and Development Centre of India (ER&DCI) with various constituents starting as adjunct entities of various State Electronic Corporations, had been brought under the hold of Department of Electronics and Telecommunications (now MeitY) in around 1988. They were focusing on various aspects of applied electronics, technology and applications.
- With the passage of time as a result of creative ecosystem that got set up in C-DAC, more areas such as Health Informatics, etc., got created; while right from the beginning the focus of NCST was on Software Technologies; similarly C-DAC started its education & training activities in 1994 as a spin-off with the passage of time, it grew to a large efforts to meet the growing needs of Indian Industry for finishing schools.

C-DAC has today emerged as a premier R&D organization in IT&E (Information Technologies and Electronics) in the country working on strengthening national technological capabilities

in the context of global developments in the field and responding to change in the market need in selected foundation areas. In that process, C-DAC represents a unique facet working in close junction with MeitY to realize nation's policy and pragmatic interventions and initiatives in Information Technology. As an institution for high-end Research and Development (R&D), C-DAC has been at the forefront of the Information Technology (IT) revolution, constantly building capacities in emerging/enabling technologies and innovating and leveraging its expertise, caliber, skill sets to develop and deploy IT products and solutions for different sectors of the economy, as per the mandate of its parent, the Ministry of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India and other stakeholders including funding agencies, collaborators, users and the market-place.

REVIEW DETAILS: -

CDAC Kolkata team visited ASUJS several times and interacted with network administrator Mr. Soumen Chaudhuri and visited the server room and available IT infrastructure. The available documentation on network infrastructure is also collected. Several meeting were also organized in presence of Registrar (Acting), Assistant Registrar, Assistant Professor Saurabh Bhattachryya, Network administrator Mr. Soumen Choudhury from ASUJS end and from CDAC Kolkata, Dr. Amit Chaudhuri (Group Head ICT & Services), Sri Anupam Chanda (Senior Engineer), and Sri Aniruddha Datta (Project Engineer) in this regard to review & objectives of the report that will be submitted as a output to ASUJS.

AVAILABLE INFRASTRUCTURE SUMMARY & INVENTORY LIST: -

The network is on three tier architecture of Core- Distribution-Access level with a star topology. All distribution levels are connected with core through OFC and all access levels are connected with distribution through 23/24 AWG UTP. UTP across the campus are tested OK for 250-500 MHz, with the Network analyzer. The Core switch and 4 nos. distribution switches are modular chassis based switch and 43 nos. Access switches are stand-alone 24 port managed switch with 2 additional gig ports. The L3 operation will be implemented on Core and Distribution level and L2 operation are on access level switches.

Regarding Server side implementation, there are implementation of NMS Server, AV Server, DNS server, Local Proxy Server and Cache server.

IT SERVICE MANAGEMENT:-

The IT services are managed through Central Server Room established in the University; the following IT services are managed:

- Network Security Firewall (Juniper NS5200)
- Juniper router by NKN
- CCTV Surveillance Server for Library.
- IBM and HP Servers for camps wide network.

INFORMATION SECURITY:-

For information security the University is using Juniper Firewall at its premises. To avoid outside threat all the necessary modules such as Anti Malware, Anti-Spam, Web and Application Filter and Intrusion Prevention System are installed at Gateway level.

All IT equipment's have power backup and the University has installed both online & offline UPS. The University has also installed Anti-Virus at server level and all the user (staff computers) update the anti-virus from the server. All the softwares are regularly updated to the latest version. All the servers installed in the university are secured with the password.

WIFI FACILITY:-

There are 42 nos. 802.11b/g wireless radio zone across Academic building, especially at Conference room, class room, auditorium, library, corridors, and at dining halls at hostels. These access points are centrally controlled by a controller.

The detailed summary inventory list of Hardware & Software is as follows:-

- **Hardware List:**

Sl No	Hardware Components	Quantity
1	Core Switch Chassis based with power supply & supervisory engine switch. Model:-Extreme Black Diamond BD8810	1
2	Distribution Switch gigabit layer 2 & layer 3 switch with non-locking architecture console. Model :- Extreme Black Diamond BD 8806	4
3	Access Switch 24 port 10/100 mbps Model :- Extreme 15101 Summit X 250 e-24t & Extreme Summit X 250e-24P	43
4	Wireless LAN controller supporting 802.11a/b/g Access points Model :- Extreme Summit WM3600 version 4.2.1.3-001R with 64 AP license	2
5	Access points supporting 802.11 a/b/g with dual antenna Model :- Extreme Altitude 3510-ROW	42
6	Network Management System(NMS) :-NMS with basic features for extreme switches - Extreme EPI Centre version 7.1	1
7	Firewall for Security :- Appliance based hardware firewall with minimum 8 auto sensing Gigabit Ethernet ports Model :-Juniper NS5200	1
8	Servers :-IBM System X 3650 M3	5
9	Servers :IBM System X 3650 M2	1
10	Servers :IBM System X 3200 M3	1
11	Server -HP server Proliant DL 380G7	1
12	HP Thin Client t5565	40
13	Laser Network Printer :-HP 3015	4
14	Library Laser Network Printer :-HP 3435MFP	1
15	Library Scanner HP Scanjet N9120	1
16	Desktops	81
17	Laptops	58
18	Tablets	7
19	HP Compaq MS6000 & Client	7

- **Software list:**

Sl No	Software Components	Quantity
1	Tally	1 Server , 5 Clients
2	Antivirus :- Trend Micro 11.0 Endpoint	750
	Antivirus :- Quick Heal Server Edition	1
	Antivirus : Quick heal Internet Security	15
3	VTLS Server	1
4	(EZ-Proxy Server) by Online Computer Library Center	1
5	AIR (All India Reporter Database)	5
6	Latest Red Hat Linux Server Edition Maintenance/ Renewal	3
7	Windows Server 2008 Operating System (Software Maintenance)	2

ISP INFORMATION AND INFRASTRUCTURE:-

The university is having 1 GBPS internet connectivity for entire campus through BSNL. ASUJS has become a part of National knowledge Network (NKN). The complete University area is equipped to offer Internet connectivity through a wireless network for students and staff, who bring their own portable computers with wireless capability. To reduce the paper work, the University is also providing Intranet Facilities for the students through which they can see the latest notices and read online e-books on their computer even when they are sitting in the hostels. 24x7 internet connectivity with 1GBPS (1:1) from NKN through BSNL is provided using optical fiber backbone covering departments, student hostels and residential areas. Wired & wireless internet connectivity is available in the campus.

CAMPUS SURVEY DETAILS:-

Based on the preliminary survey & visit several shortfalls are noticed in the Network Infrastructure. The shortfalls are as follows**:-**

Problem a) There is no user authentication mechanism in the university. As a result there is a chance of gross misuse of Internet.

Proposed Solution: Network authentication is a security process required when a computer on a network tries to connect to the server in order to use its resources. If the user's identity has been stored by the server, entering a valid username and password completes the connection. However, if there is a mismatch, you are required to establish your network identification.

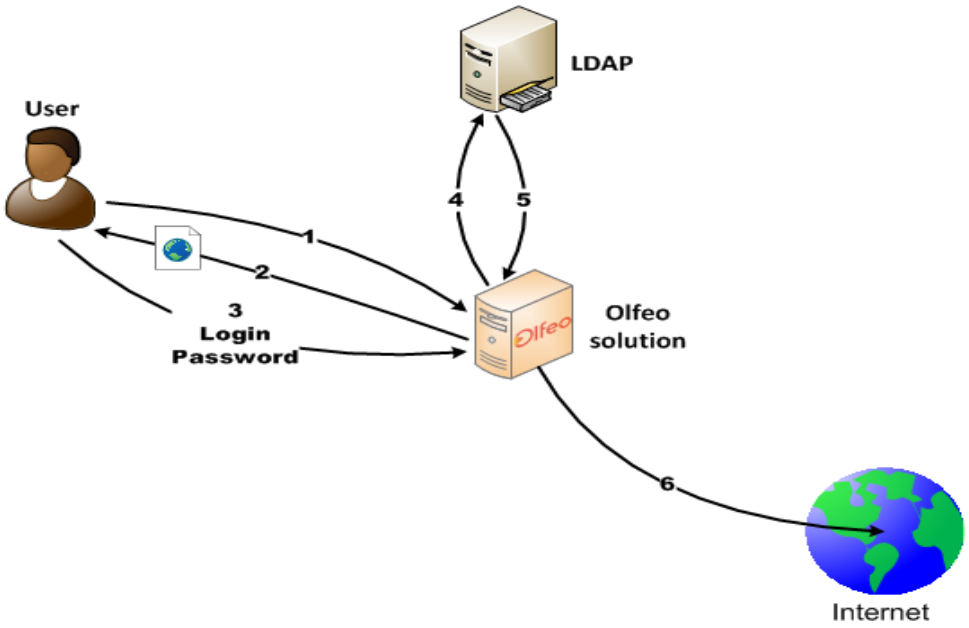


Fig 2: An Example of a user authentication mechanism

So, the above diagram describes how the network authentication security process works when any unknown user tries to access internet in a organisational network.So for executing this procedure of NAC (Network Authentication Control) we will be using a open source Captive Portal Authentication software like **Packet Fence.**

PacketFence is a network access control (NAC) system featuring a captive-portal for registration and remediation, wired and wireless management, 802.1x support, isolation of This tool can be used in the following areas:

- banks
- colleges and universities
- engineering companies
- convention and exhibition centers
- hospitals and medical centers
- hotels
- manufacturing businesses
- school boards (K-12)
- telcos
- plus many more…

Facilities Provided by Packet Fence Captive Portal Authentication Software:-

Enforcement:-

Out-of-band Deployment: PacketFence's operation is completely out-of-band which allows the solution to scale geographically and to be more resilient to failures. When using the right technology (like port security), a single PacketFence server can be used to secure hundreds of switches and many thousands nodes connected to them.

Inline Deployment: While out-of-band is the preferred way of deploying PacketFence, an inline mode is also supported for unmanageable wired or wireless equipment. Deploying PacketFence using the inline mode can also be accomplished in minutes! Note also that the inline mode can coexist very well together with an out-of-band deployment.

Aunthentication & Registration:-

802.1X Support: Wireless and wired 802.1X is supported through a FreeRADIUS module which is included in PacketFence. PEAP-TLS, EAP-PEAP and many more EAP mechanisms can be used.

Wireless Integration: PacketFence integrates perfectly with wireless networks through a FreeRADIUS module. This allows you to secure your wired and wireless networks the same way using the same user database and using the same captive portal, providing a consistent user experience. Mixing access points (AP) vendors and wireless controllers is supported.

Registration of Devices: PacketFence supports an optional registration mechanism similar to "captive portal" solutions. Contrary to most captive portal solutions, PacketFence remembers users who previously registered and will automatically give them access without another authentication. Of course, this is configurable. An Acceptable Use Policy can be specified such that users cannot enable network access without first accepting it.

Voice over IP (VoIP) Support: Also called IP Telephony (IPT), VoIP is fully supported (even in heterogeneous environments) for multiple switch vendors (Cisco, Edge-Core, HP, LinkSys, Nortel Networks and many more).

Compliance:-

Detection of Abnormal Network Activities: Abnormal network activities (computer virus, worms, spyware, traffic denied by establishment policy, etc.) can be detected using local and remote Snort, Suricata or commercial sensors. Content inspection is also possible with Suricata, and can be combined with malware hash databases such as OPSWAT Metadefender. Beyond simple detection, PacketFence layers its own alerting and suppression mechanism on each alert type. A set of configurable actions for each violation is available to administrators.

Proactive Vulnerability Scans: Nessus or OpenVAS vulnerability scans can be performed upon registration, scheduled or on an ad-hoc basis. PacketFence correlates the Nessus/OpenVAS vulnerability ID's of each scan to the violation configuration, returning content specific web pages about which vulnerability the host may have.

Windows Management Instrumentation(WMI): WMI support in PacketFence allows an administrator to perform audits, execute commands and even more on any domain-joined

Windows computers. For example, PacketFence can verify if some unauthorized software are installed and/or running before granting network access.

Security Agents: PacketFence integrates with security agent solutions such as OPSWAT Metadefender Endpoint Management, Symantec SEPM and others. PacketFence can make sure the agent is always installed before granting network access. It can also check the endpoint's posture and isolate it from any other endpoints if non-compliant.

Statement of Health: While doing a 802.1X user authentication, PacketFence can perform a complete posture assessment of the connecting device using the TNC Statement of Health protocol. For example, PacketFence can verify if an antivirus is installed and up-to-date, if operating system patches are all applied and much more - all without any agent installed on the endpoint device.

Remediation Through a Captive Portal: Once trapped, all network traffic is terminated by the PacketFence system. Based on the nodes current status (unregistered, open violation, etc), the user is redirected to the appropriate URL. In the case of a violation, the user will be presented with instructions for the particular situation he/she is in, reducing costly help desk intervention.

Isolation of Problematic Devices: PacketFence supports several isolation techniques, including VLAN isolation with VoIP support (even in heterogeneous environments) for multiple switch vendors.

Administration:-

Command-line and Web-based Management: Web-based and command-line interfaces for all management tasks. Web-based administration supports different permission-levels for users and authentication of users against LDAP or Microsoft Active Directory.

Advance Features:-

- Flexible VLAN Management and Role-Based Access Control

- Guest Access - Bring Your Own Device (BYOD)
- Portal Profiles
- More Built-in Violation Types
- Automatic Registration
- PKI and EAP-TLS Support
- Expiration
- Device Management
- Firewall Integration
- Bandwidth Accounting
- Floating Network Devices
- Flexible Authentication
- Microsoft Active Directory Integration
- Routed Networks
- Gradual Deployment
- Pass-Through
- High-Availability
- Supported Hardware

Component Architecture of Packet-Fence:-

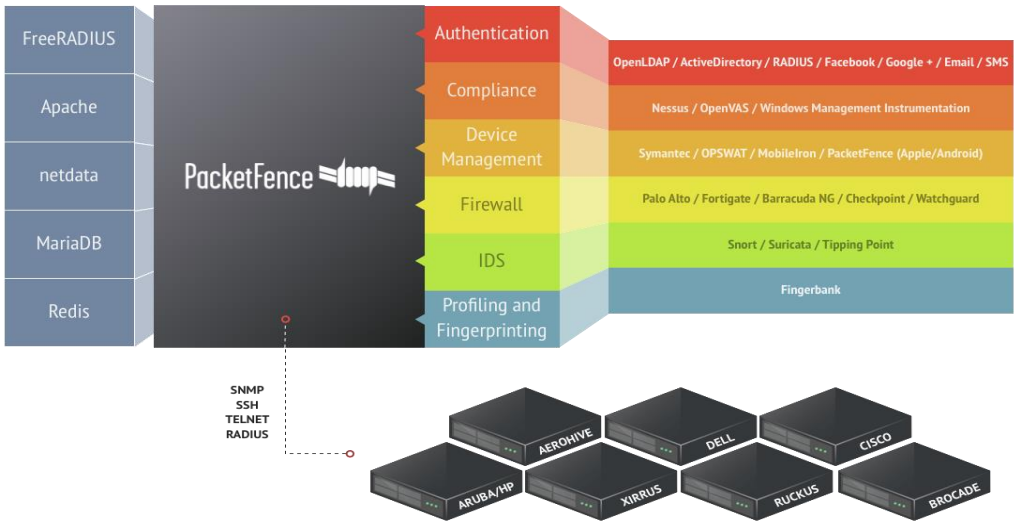


Fig 3: Open Source thats why it can mix various switch and AP(Access Point) Vendors

Network Architecture of Packet-Fence:-

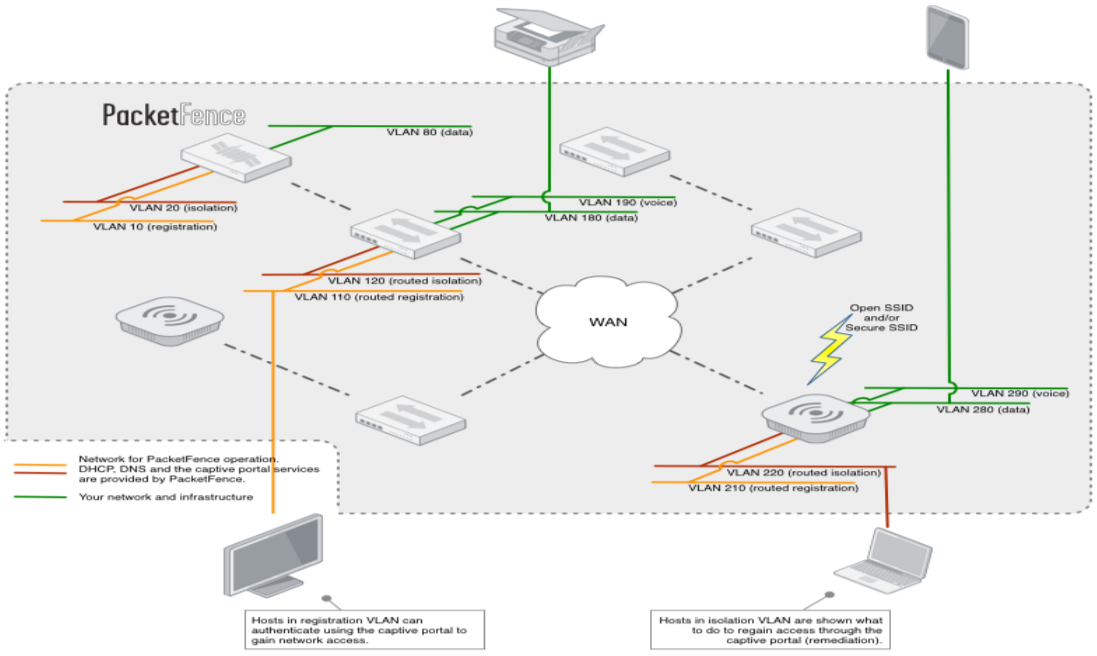


Fig 4: How Packet-Fence works in a network architecture

So there are many such open source captive Portal authentication software like Wifi Dog, pfSense, Utangle etc. but as per our recommendation as,

Recommendation 1: Packet Fence we suggest this for Network Access Control/ Captive portal Authentication Software which has been shown in Fig4 which is much more effective over the existing system for checking out the users who all are not recognised for accesing the campus internet service so it is very much helpful for the Network Admin in recognising a new/guest user trying to access campus internet service.

Problem b) There is a lack in maintaining proper log backup mechanism in campus. Basically the Logs that contain proper information regarding internal internet usage for at leat a duration of 3 month. Lack of content logging system needed. Lack of user specific logs.

Proposed Solution: Maintaining internet information log is a feature of backup applications that records the events that occur during a backup process. So as per the IT Act of India in it is mandatory for any organisation to keep a record of internet information logs for at least 3

month period for various security and analysis purpose. A record of the backup process can be a useful troubleshooting tool in case there is a problem with the backup. If and when a problem occurs during the backup process, the log will record the error messages created by the backup application when the error occurred. These error messages (also called error codes) are typically unique to the backup application that generated them, although some applications may share generic messages or codes to signal an error. Backup logs can be set to store essentially summary data, such as notification that a file failed to open, but logs can also be set to retain more details of the backup process, such as details about the files that were backed up.

So over here same kind of application will be implemented in a network infrastructure of a campus area in order to keep tracks of the browsing history, internet access for the purpose of analysis as well as to prevent internal and external attacks. So over here we will be using a centralized open source software for server log management for e.g. Nagios Log Server. **Log Server** is a powerful centralized enterprise-class log monitoring and management application that allows organizations to quickly and easily view, sort, and configure logs from any source on any given network. Log Server is designed to analyze, collect, and store log data based on custom specifications and provide users with extended insight into the data on their network's infrastructure.
Nagios Log Server is a Centralized Log Management, Monitoring and Analysis Software.

Benefits of Nagios Log Server :-

Ease of Use: Nagios Log Server greatly simplifies the process of searching your log data. Set up alerts to notify you when potential threats arise, or simply query your log data to quickly audit any system. With Nagios Log Server, you get all of your log data in one location, with high availability and fail-over built right in. Quickly configure your servers to send all log data with easy source setup wizards and start monitoring your logs in minutes.

Infinite Scalability: Nagios Log Server can scale to meet the needs of your entire IT infrastructure, so as your organization grows you can easily add additional Nagios Log Server instances to your monitoring cluster. This allows you to quickly add more power,

speed, storage, and reliability to your overall log analysis platform. Nagios Log Server is designed for organizations of any size and can adapt with the click of a button.

Your Data in Real Time: Easily correlate log events across all servers in a few clicks. Nagios Log Server allows you to view log data in real-time, providing the ability to quickly analyze and solve problems as they occur. This keeps your organization safe, secure, and running smoothly.

Adaptability: Nagios Log Server has a fully accessible API allowing for complete integration to fit the needs of your external applications. Nagios Log Server easily integrates with third-party solutions or your current infrastructure.

Network Security: Nagios Log Server is a premier solution that's perfectly designed for security and network auditing. Easily create alerts from the web-interface based on queries and thresholds most important to you. Notify users via Nagios XI / Nagios Core, email, SNMP traps, or execute a script to ensure quick problem resolution. Nagios Log Server lets you dive into the issue to help you find a solution. Additionally, Nagios Log Server can keep historical archives of all events should a security audit be needed, keeping your organization in compliance with security requirements.

Advance User Management: Multi-user capabilities allow IT teams to work together efficiently. Admins can add, modify, and remove users, as well as set access permissions. Admins can also grant specified users access to the external API via an access key.

Customized Dashboards: A powerful GUI provides for customization of layout, design, and preferences on a per-user basis, giving your customers and team members the flexibility they want. Users can create custom dashboards in the web-interface to see quick views of data most important to them. Users can also easily share dashboards with a custom URL to enhance team collaboration.

Network Insights: Nagios Log Server provides users with advanced awareness of their infrastructure. Dive deep into network events, logs, and security events. Use Log Server to provide the evidence necessary to track down security threats, and quickly resolve vulnerabilities with built-in alerts and notifications.

Features of Nagios Log Server :-

Comprehensive Dashboards: A powerful dashboard system provides users with the ability to query, filter, and analyze incoming log events as in Fig5.

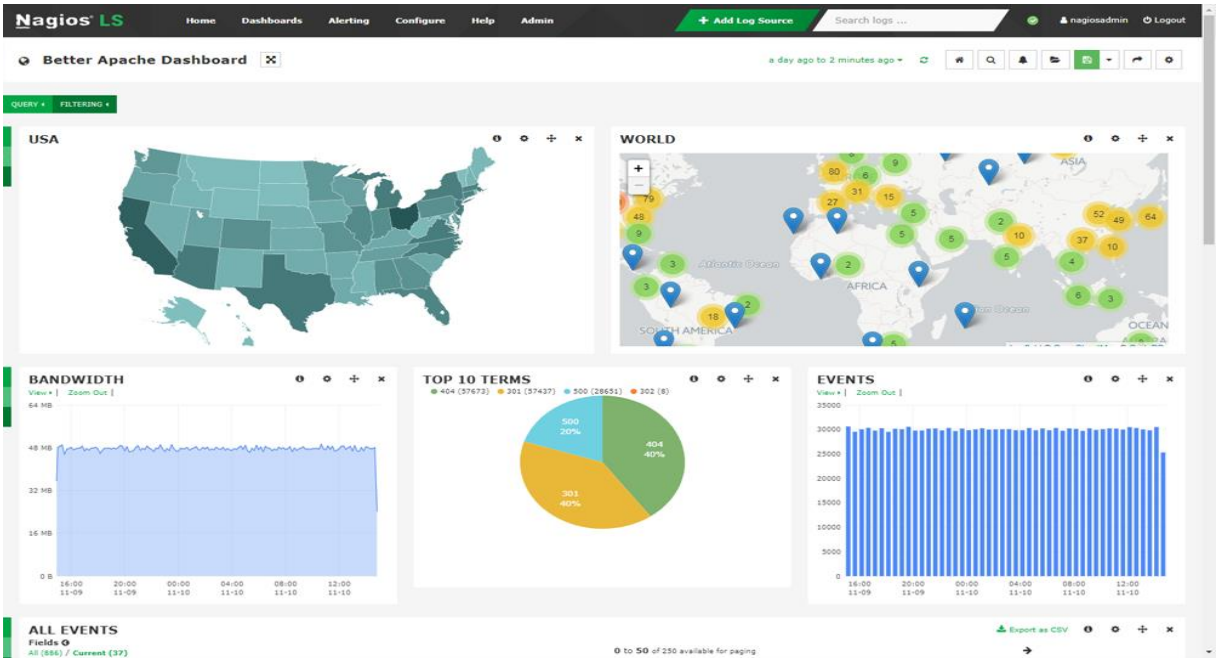


Fig 5: Nagios Log Server High Power GUI Dashboard

High Availability & Failover: Log Server uses a cluster of servers to store log data to prevent data loss and ensure the availability of your log information in Fig6.

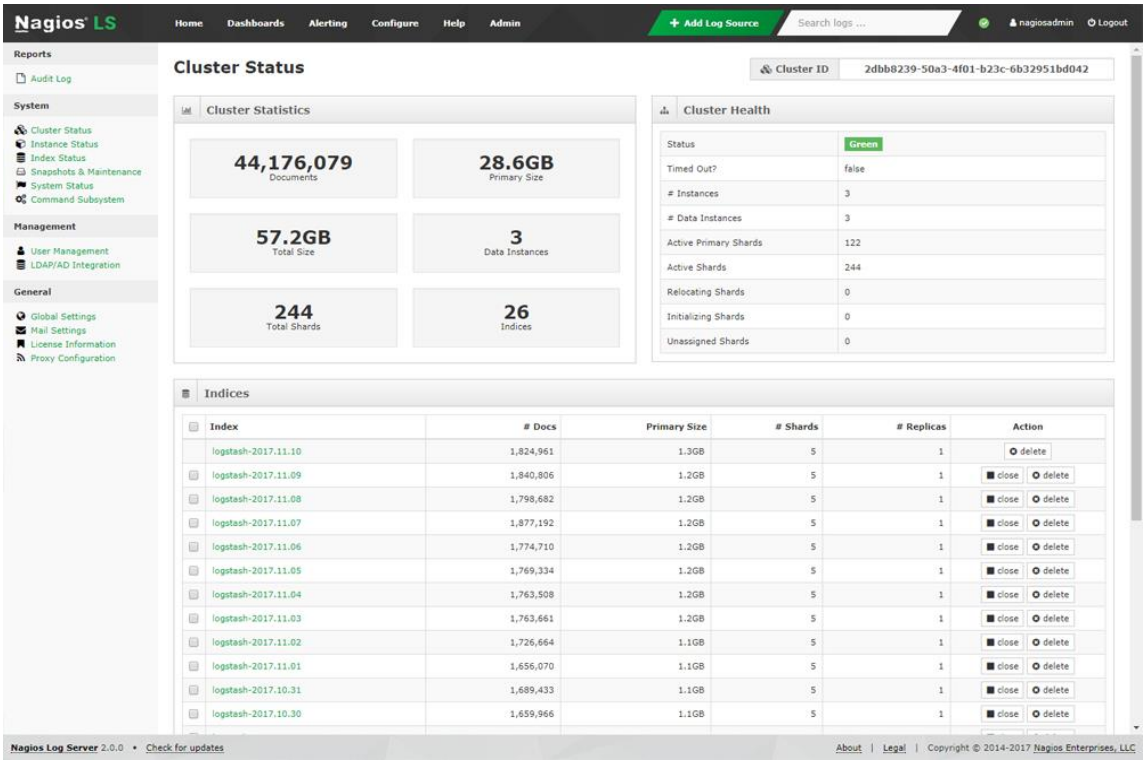


Fig 6: Nagios Log Server cluster status information

Alerting: Create alerts based on queries with specific thresholds and send them to proper team members as shown in Fig7.

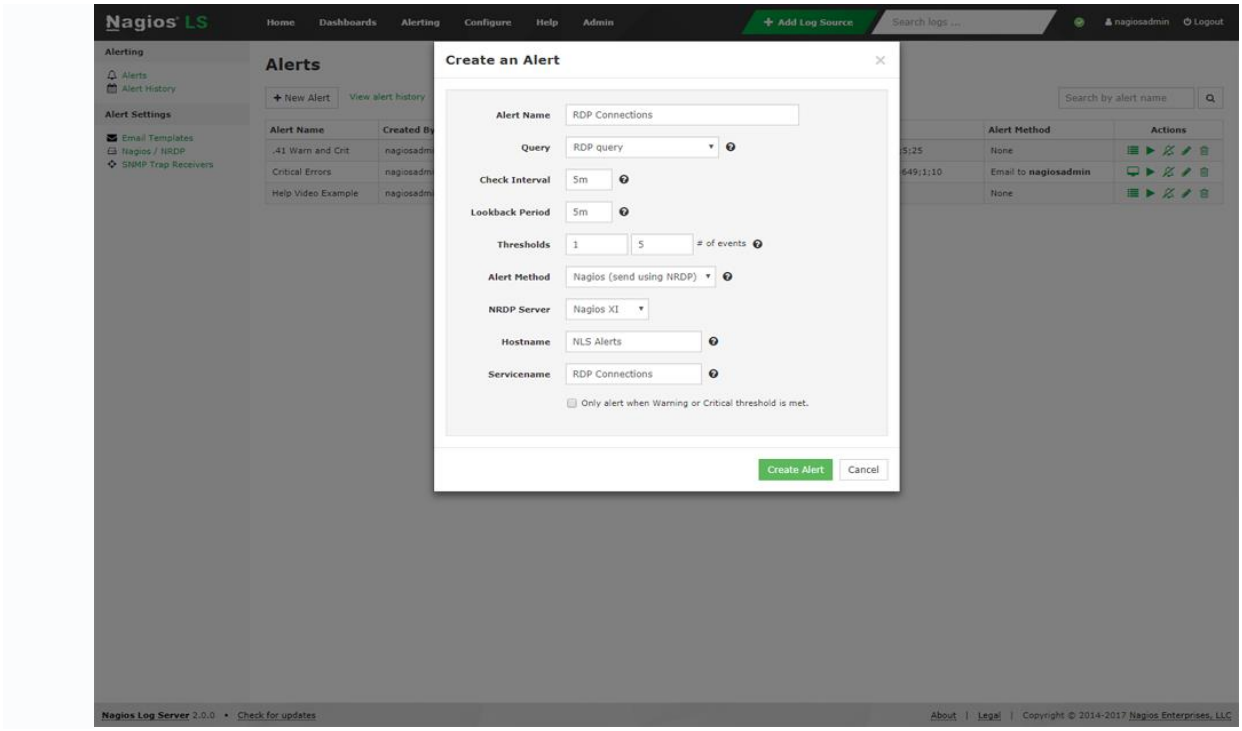


Fig 7: Nagios Log Server alerting portal

Setup Wizards: Receive log data from a designated source with just a few clicks using easy to follow instructions in Fig8.

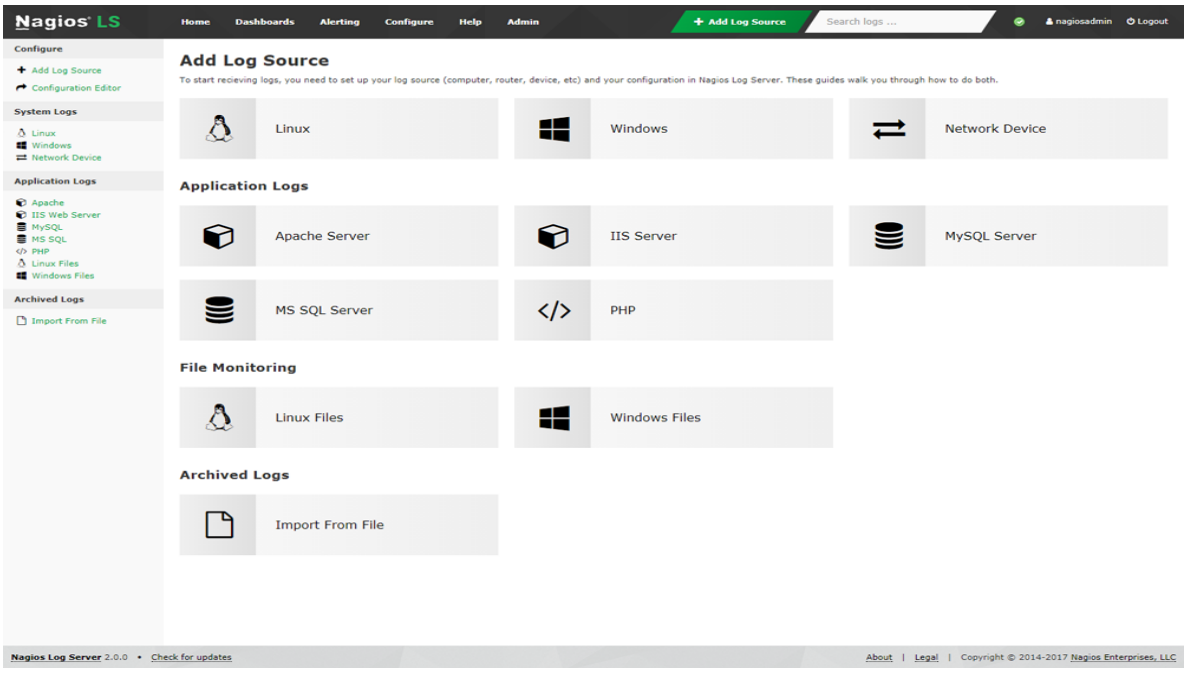


Fig 8: Nagios Log Server adding log source portal.

Quick Search & Query: Search with multiple queries and filters allowing you to quickly drill down to the exact problem you are searching for as shown in Fig9.

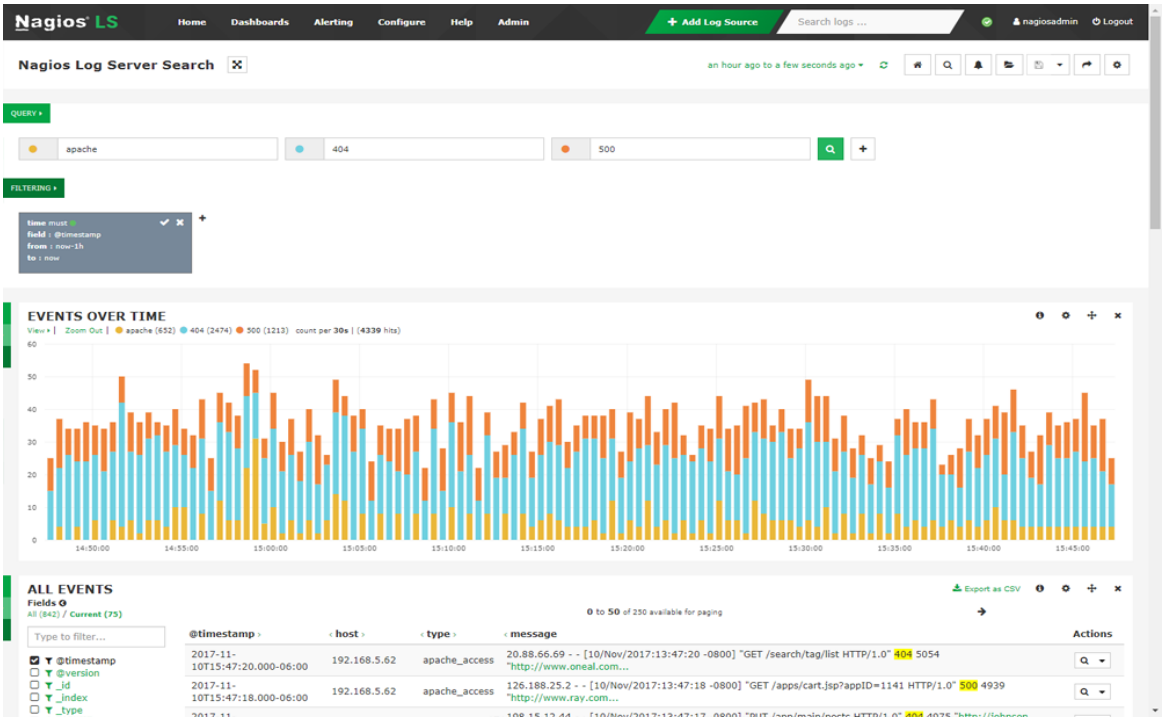


Fig 9: Nagios Log Server quick search & query portal

Extendable Architecture: Admins have full access to the back end API allowing for limitless customization with in-house and third-party apps as shown in Fig10.

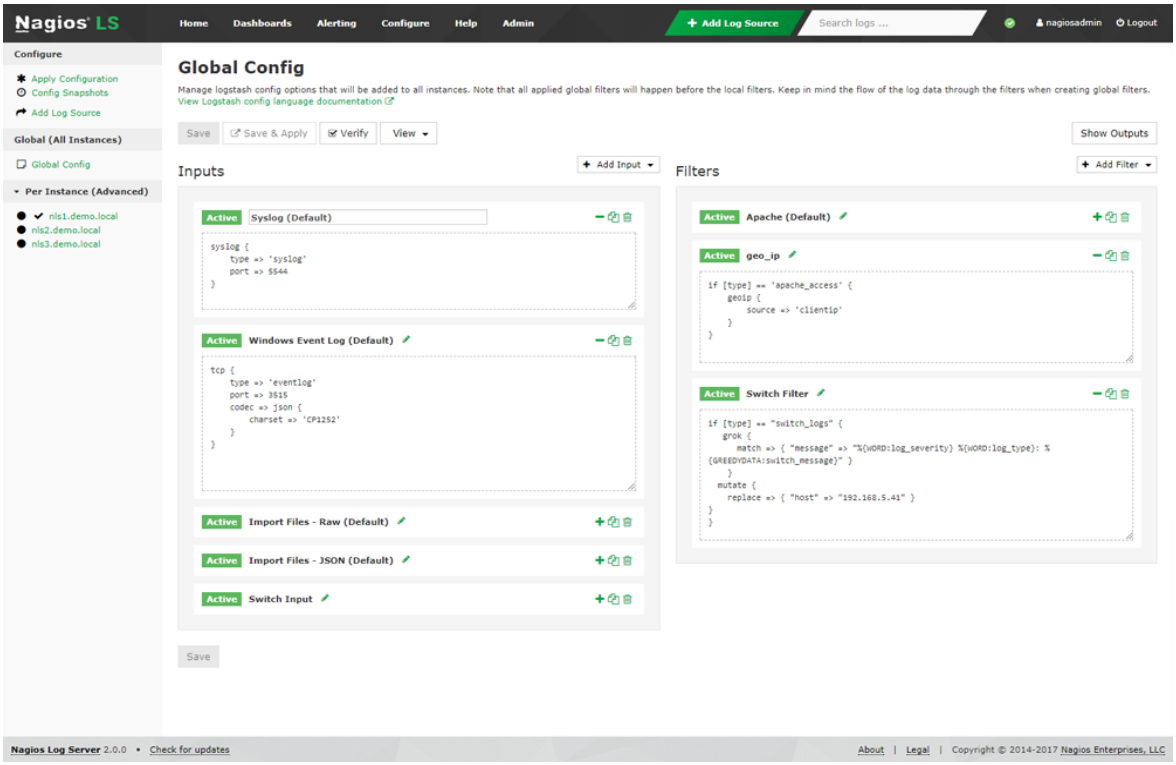


Fig 10: Nagios Log Server extendable architecture portal

Real-Time Data: See log data from all of your servers in real time, allowing you to analyze and solve problems as they occur as shown in Fig11.

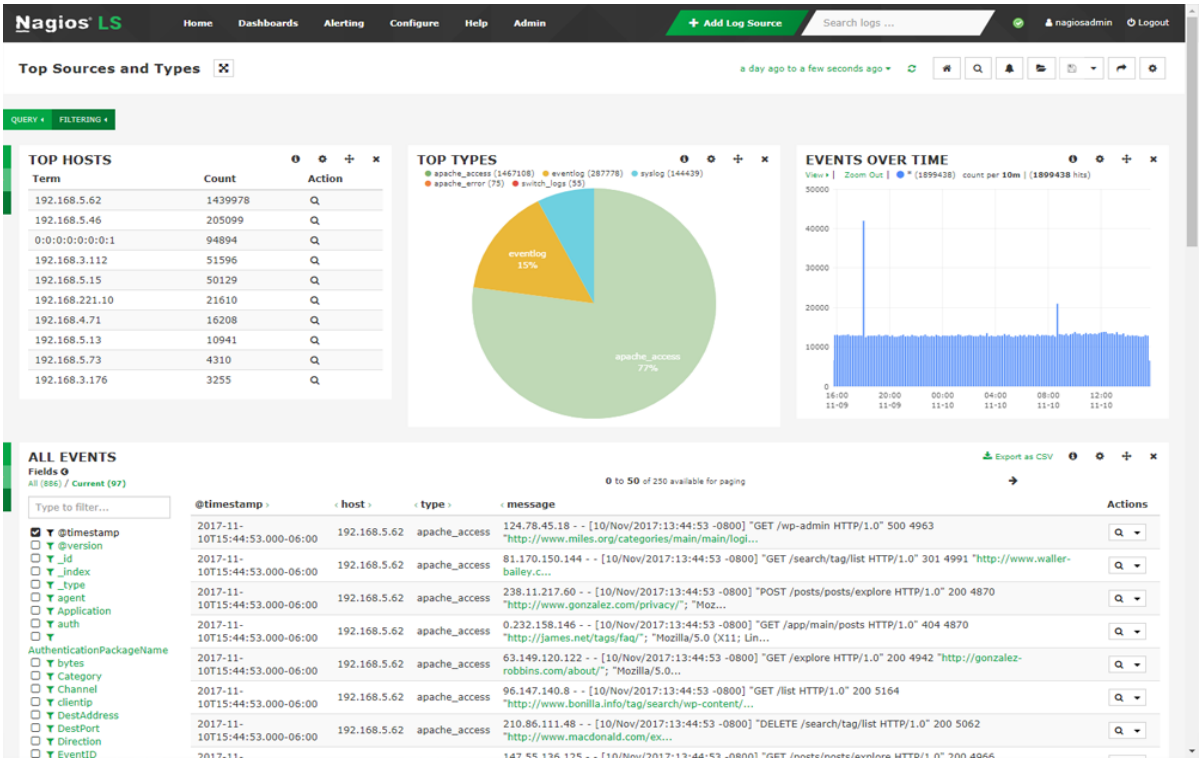


Fig 11: Nagios Log Server Real Time Data Analysis portal

Highly Scalable: You can easily add additional cluster instances to give you more power, speed, storage, and reliability as shown in Fig 12.

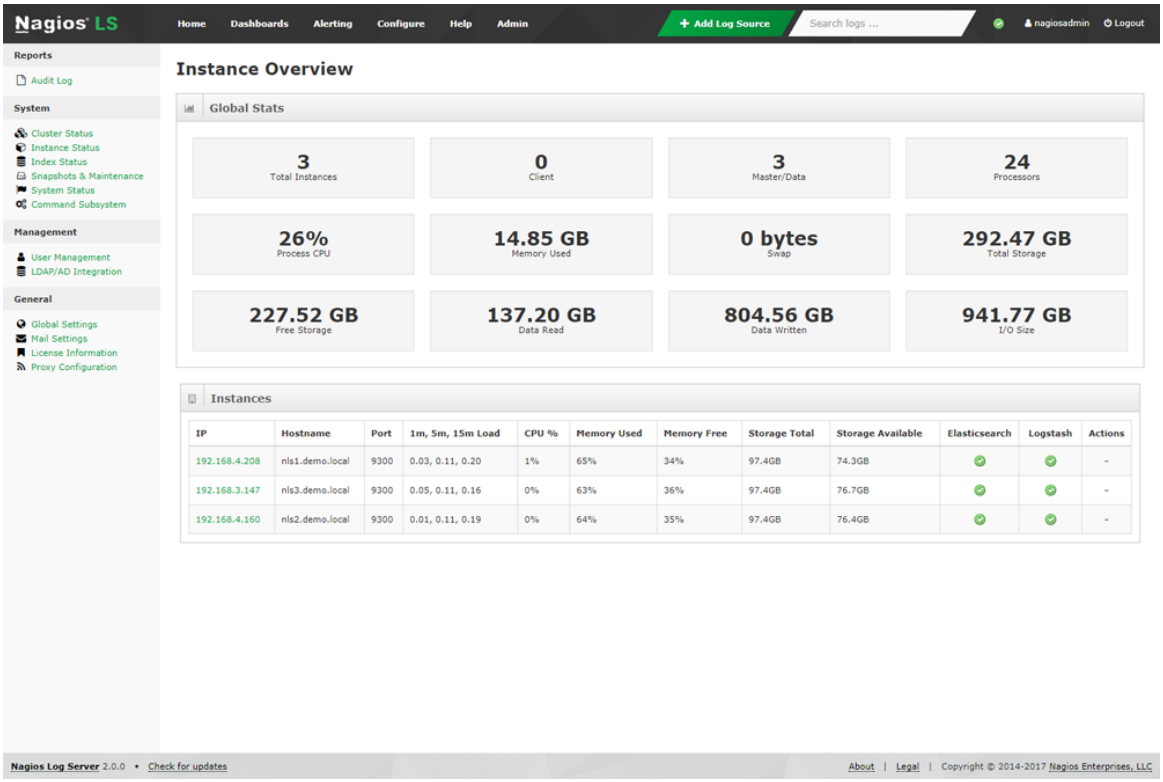


Fig 12: Nagios Log Server Instance Overview portal

So in the market of networking there are many such open source log management software like logentry, logscape, loggly etc. but as per suggestion we recommend.

Recommendation 2: **Nagios Log Server** for it's flexibility and real time event analysis and cluster status information as it provides better performance then the existing system in the campus network setup keeping track and maintaining logs for the various internal internet access related information following the IT Law of India for a duration of 3 Months surely.

Problem c) The Network Management Software (Extreme Epicenter 7.1) which is essential for monitoring all the nodes across the campus is outdated. Unable to support newer version of Extreme product/ other vendor products.

Proposed Solution: A **Network Management Software** is used to monitor, maintain and provision computer networks. It helps you to keep track of the network's bandwidth, availability, performance and hardware. So over here we will be using an open source network management software for the feasibility of managing and configuring switches and various other network devices and nodes. So we will be using NagiosXI. **NagiosXI** is an Enterprise Server and Network Monitoring Software**.**

Benefits of NagioXI:-

Comprehensive IT Infrastructure Monitoring: Provides monitoring of all mission-critical infrastructure components including applications, services, operating systems, network protocols, systems metrics, and network infrastructure. Hundreds of third-party addons provide for monitoring of virtually all in-house applications, services, and systems.

Performance: The powerful Nagios Core 4 monitoring engine provides users with the highest degree of monitoring server performance. High-efficiency worker processes allow for nearly limitless scalability and monitoring effectiveness.

Visibility: Provides a central view of your entire IT operations network and business processes. Powerful dashboards provide at-a-glance access to powerful monitoring information and third-party data. Views provide users with quick access to the information they find most useful.

Proactive Planning & Awareness: Automated, integrated trending and capacity planning graphs allow organizations to plan for infrastructure upgrades before outdated systems catch them by surprise. Alerts are sent to IT staff, business stakeholders, and end-users via email or mobile text messages, providing them with outage details so they can start resolving issues immediately**.**

Customizability: A powerful GUI provides for customization of layout, design, and preferences on a per-user basis, giving your customers and team members the flexibility they want.

Ease of Use: Integrated web-based configuration interface lets admins hand out control of managing monitoring configuration, system settings, and more to end-users and team

members easily. Configuration wizards guide users through the process of monitoring new devices, services, and applications – all without having to understand complex monitoring concepts.

Multi-Tenant Capabilities: Multi-user access to web interface allows stakeholders to view relevant infrastructure status. User-specific views ensure clients only see the infrastructure components they're authorized for. Advanced user management simplifies administration by allowing you to manage user accounts easily. Provision new user accounts with a few clicks and users automatically receive an email with their login credentials**.**

Extendable Architecture: Multiple APIs provide for simple integration with in-house and third-party applications. Thousands of community-developed addons extend monitoring and native alerting functionality. Custom interface and addon developments are available to tailor Nagios XI to meet your organization's exact needs.

Features of NagiosXI:-

Powerful Monitoring Engine: Nagios XI uses the powerful Nagios Core 4 monitoring engine to provide users with efficient, scalable monitoring as shown in Fig 13.

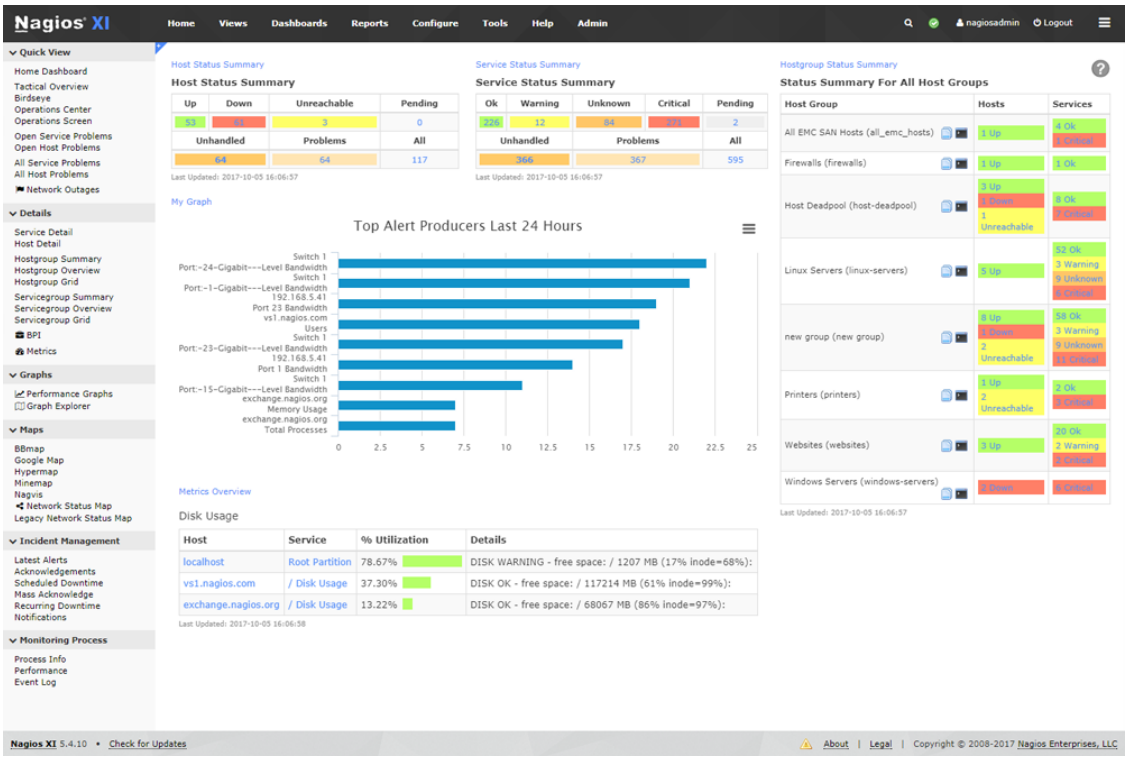


Fig 13: NagiosXI powerful monitoring Portal

Updated Web Interface: Your new dashboard provides a customizable high-level overview of hosts, services, and network devices as shown in Fig14.

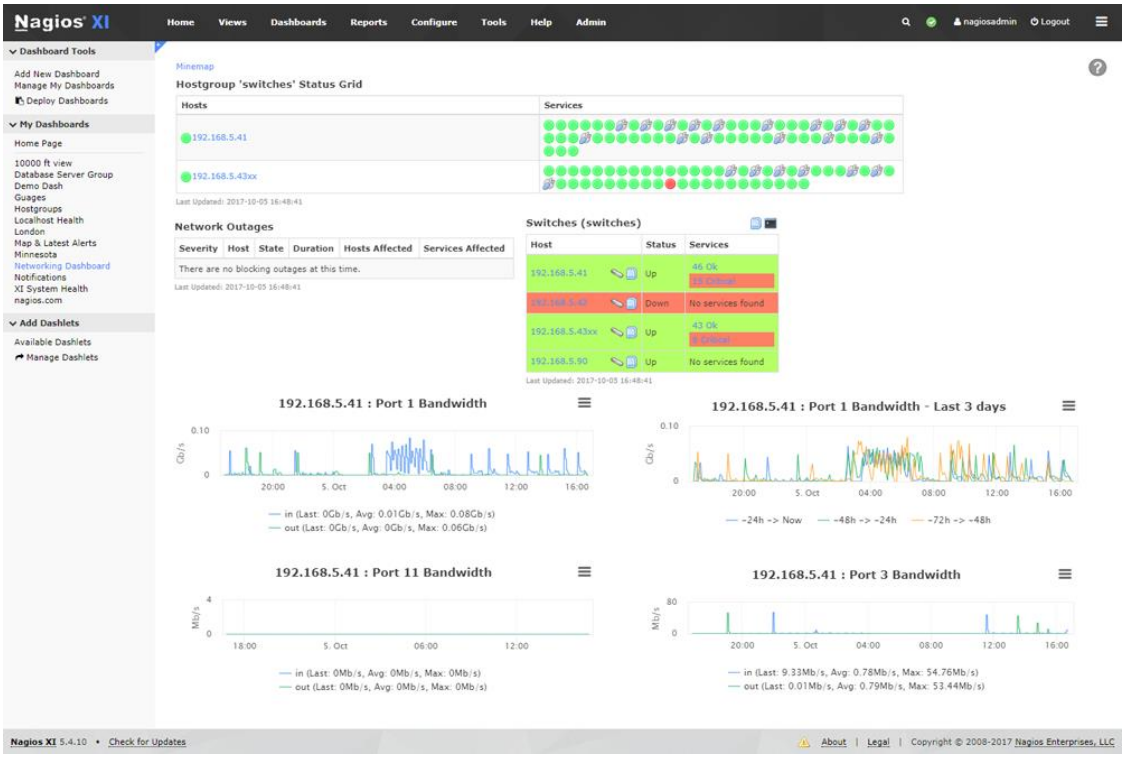


Fig 14: NagiosXI updated web Interface

Advanced Graphs: Administrators can easily view network incidents and resolve them before they become major catastrophes as shown in Fig15.

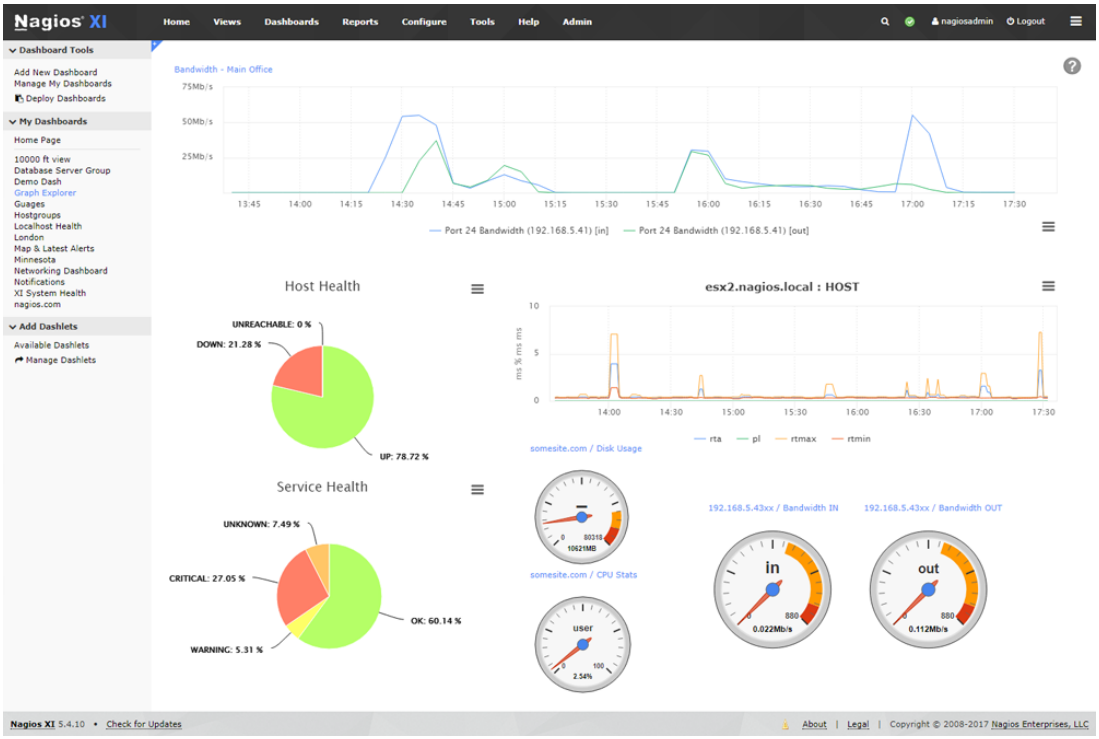


Fig 15: NagiosXI Graph Interface

Capacity Planning: Automated, integrated trending and capacity planning graphs allow organizations to plan for upgrades as shown in Fig 16.

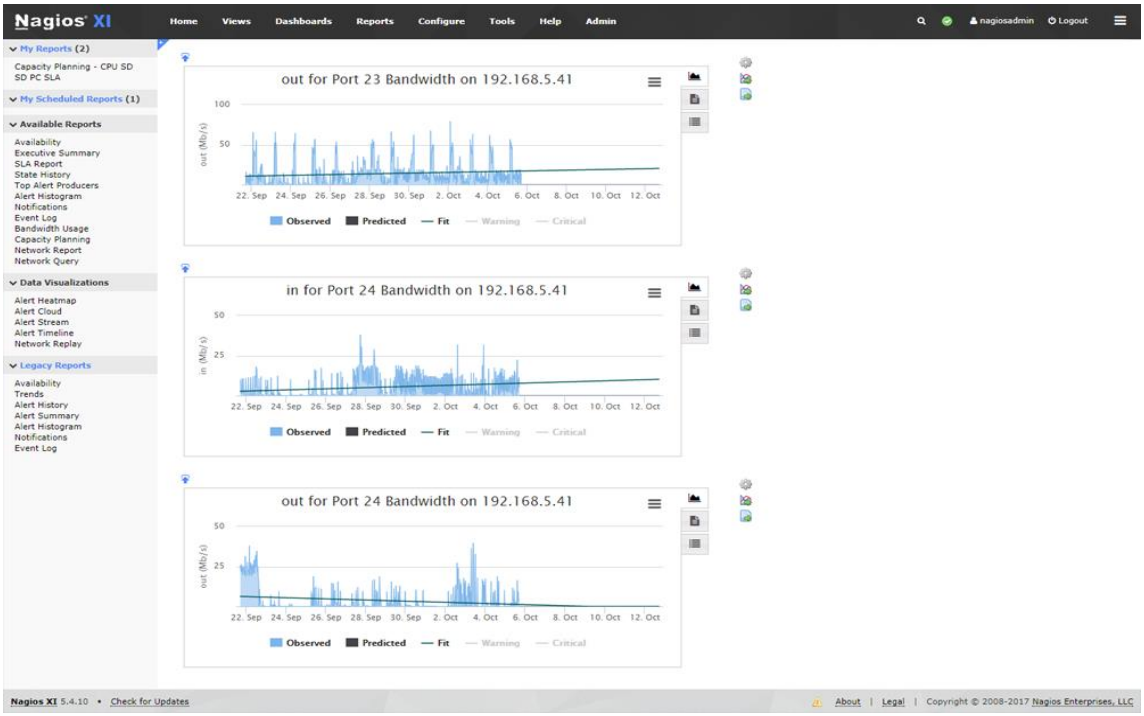


Fig 16: NagiosXI Capacity Planning Interface

Configuration Wizards: Fast Wizards! Simply enter the required information, and you're up and monitoring with a few simple clicks as shown in Fig17.

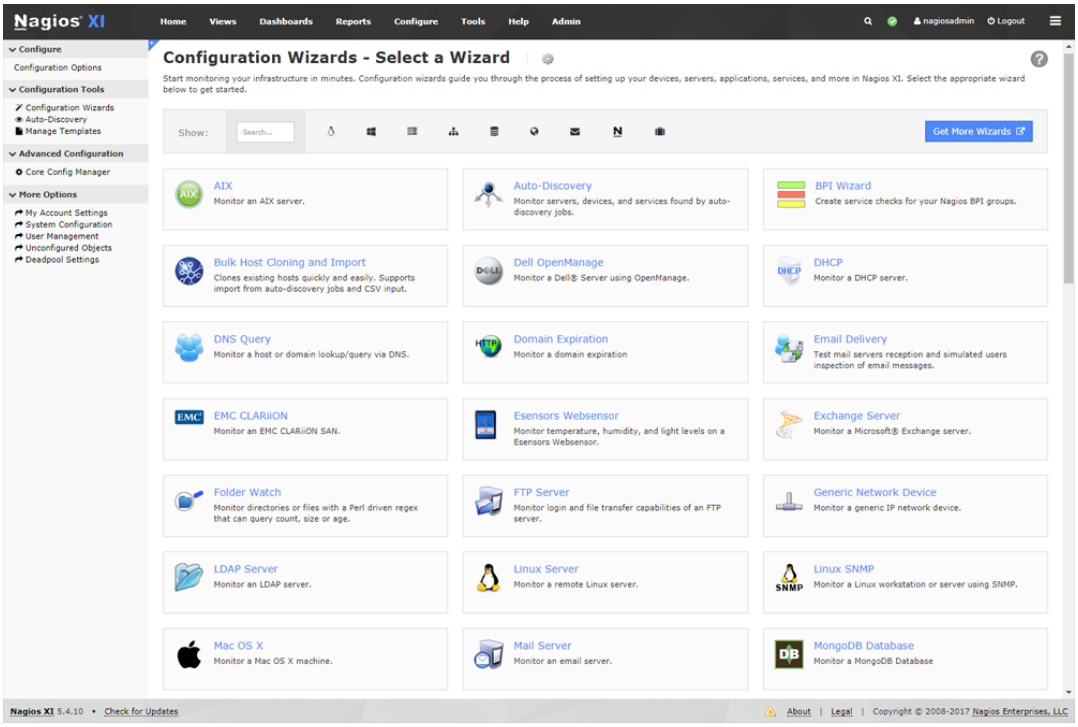


Fig 17: NagiosXI Configuring Wizard Interface

Infrastructure Management: Improved Bulk Host Import, Autodiscovery, Auto Decommissioning, Mass Acknowledgment as shown in Fig 18.

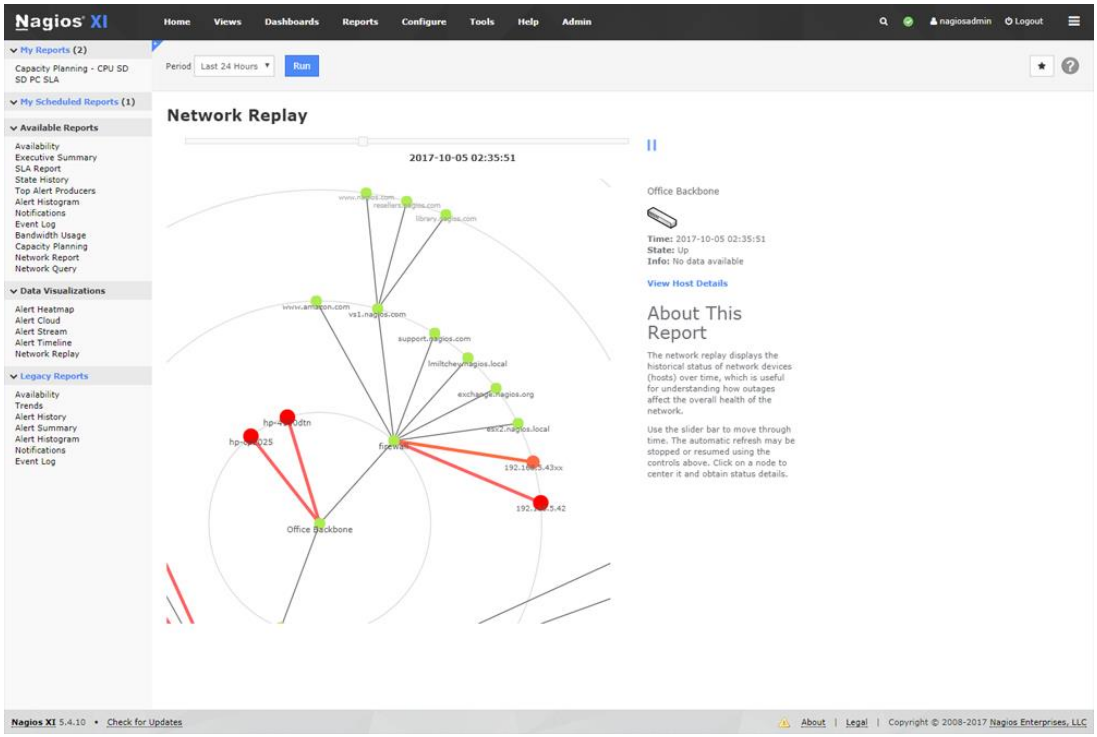


Fig 18: NagiosXI Infrastructure Management Interface

Configuration Snapshot: Save your most recent configurations. Archive it. Revert back whenever you like. Never lose it again. Relax as shown in Fig19.

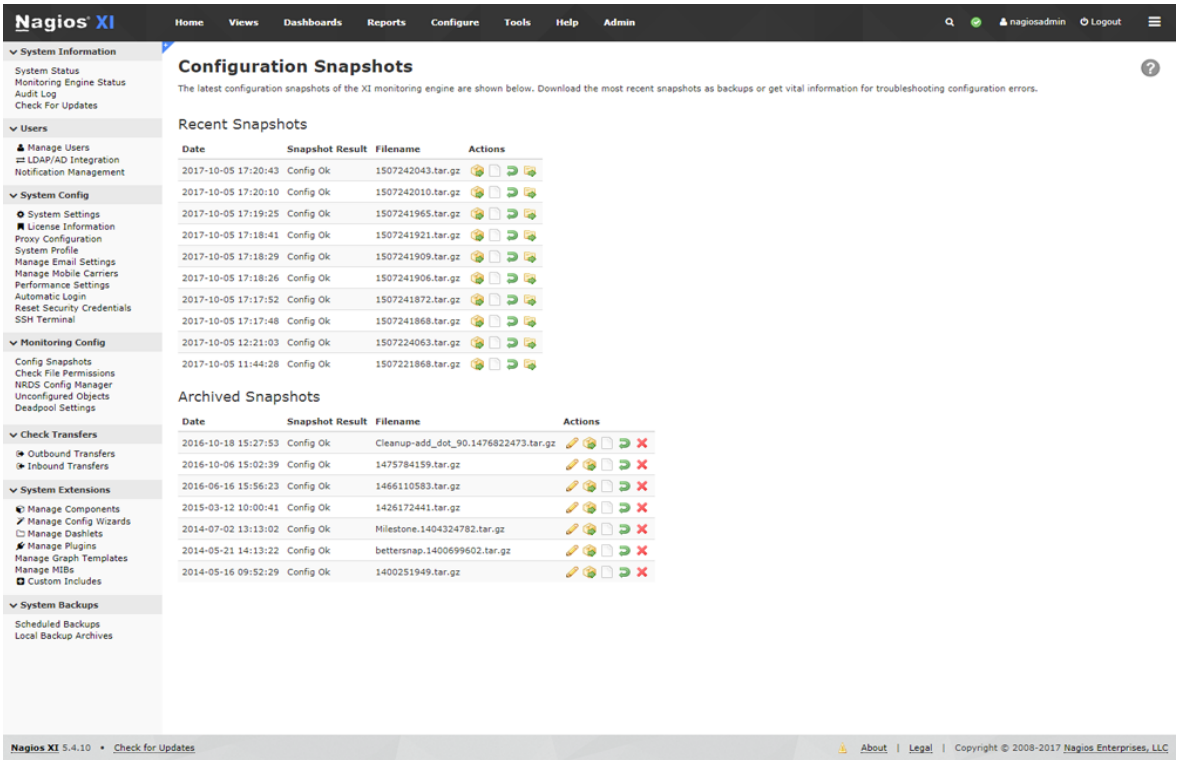


Fig 19: NagiosXI Configuration Snapshot Interface

Advanced User Management: Easily setup and manage user accounts with only a few clicks then assign custom roles to ensure a secure environment as shown in Fig20.

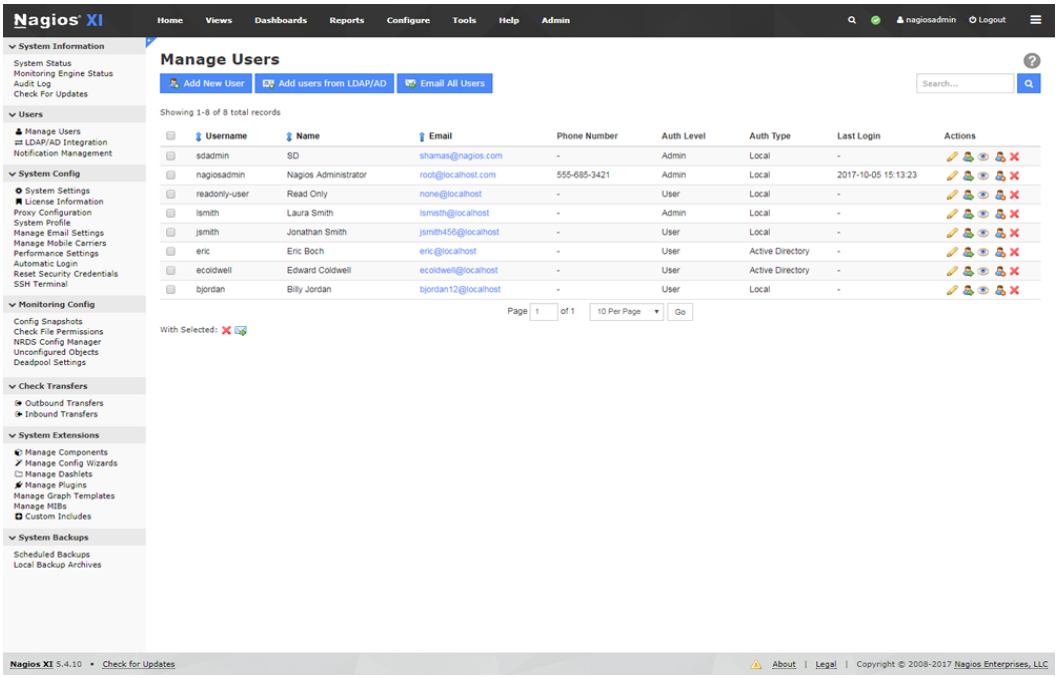


Fig 20: NagiosXI User Management Interface

So there are many such Network Management Systems in the field of networking like OpenNMS, Zabbix, Incigna etc. but as per suggestion as we recommend,

Recommendation 3: **NagiosXI** as a open source Network Management Software because it is very much user friendly and real time which helps network admin to manage any network device in a network cluster and performs in a better way than the existing systems for which we needed the same company based software but this is quite open to manage any device on a network infrastructure.

Problem d) Wireless controller (Extreme Summit WM3600 version 4.2.1.3) manages all the access-points (Extreme Altitude 3510-ROW) in the campus. The controller has 64 AP license out of which only 42 AP are active. The particular AP model is not available in market. Newer version AP / Other vendor AP not supported by Wireless controller.

Proposed Solution: A wireless LAN (WLAN) controller is used in combination with the Lightweight Access Point Protocol (LWAPP) to manage light-weight access points in large quantities by the network administrator or network operations center. So for managing all the Access Points we need to have a open source software which can configure Access Point of any model.So over here we will be using **OpenWisp** WLAN Controller Software to control any Access Point device.

OpenWisp is a software platform that can be used to implement a complete Wi-Fi service.The OpenWISP software suite includes five main applications, derived from tools used to offer public wifi service in Italy and other European countries.

OpenWISP2 is a set of software modules that aims to replace some of the previous generation projects of OpenWISP, which we now refer to as OpenWISP1. The OpenWISP1 modules that are being replaced are:

- OpenWISP Manager
- OpenWISP Geographic Monitoring
- OpenWISP Firmware

The goal of this new development is to overcome the high limitations of these softwares, that were designed and developed between 2008 and 2011 to solve specific problems, but are hardly reusable in different contexts. The controller is composed of several modules:

netjsonconfig: configuration generator based on the NetJSON specification, currently ships backends for OpenWRT/LEDE and OpenWISP Firmware.

OpenWRT- The OpenWrt Project is a Linux operating system targeting embedded devices. Instead of trying to create a single, static firmware, OpenWrt provides a fully writable filesystem with package management. This frees you from the application selection and configuration provided by the vendor and allows you to customize the device through the use of packages to suit any application. For developers, OpenWrt is the framework to build an application without having to build a complete firmware around it; for users this means the ability for full customization, to use the device in ways never envisioned.

LEDE- is a Linux operating system for people who want to install high-performance, easily-configured, reliable and robust firmware on a home router or embed the Linux-based software in other equipment.

As we enter 2018, both OpenWrt and the former LEDE project are happy to announce their unification under the OpenWrt name as per the Fig21.

Fig 21: OpenWisp2 and LEDE Dependency

django-netjsonconfig: django reusable web app that provides a web interface to manage OpenWRT and OpenWISP configurations using netjsonconfig behind the scenes.

django-x509: django app that implements PKI management in django, used to generate VPN certificates.

django-owm-legacy: provides backward compatibility with OpenWISP1 Firmware.

OpenWisp2 Firmware:

The new firmware composed of the following modules:-

- **openwisp-config**: OpenWRT agent that takes care of downloading and updating the configuration from the new controller
- **luci-openwisp**: an optional simplified/limited web interface for operators

OpenWisp2 Monitoring:

The new monitoring features that are going to replace *OpenWISP Geographic Monitoring* have not been integrated with the new controller yet, but some work has already been done in the following projects:

- **django-netjsongraph, Network Topology Visualizer**: monitors the network topology (for more information read Network Topology Visualizer: django-netjsongraph).
- **netjsongraph.js**: a javascript library based on d3.js that allows visualization of a NetJSON NetworkGraph object, which is an object that respects a specific json graph format.

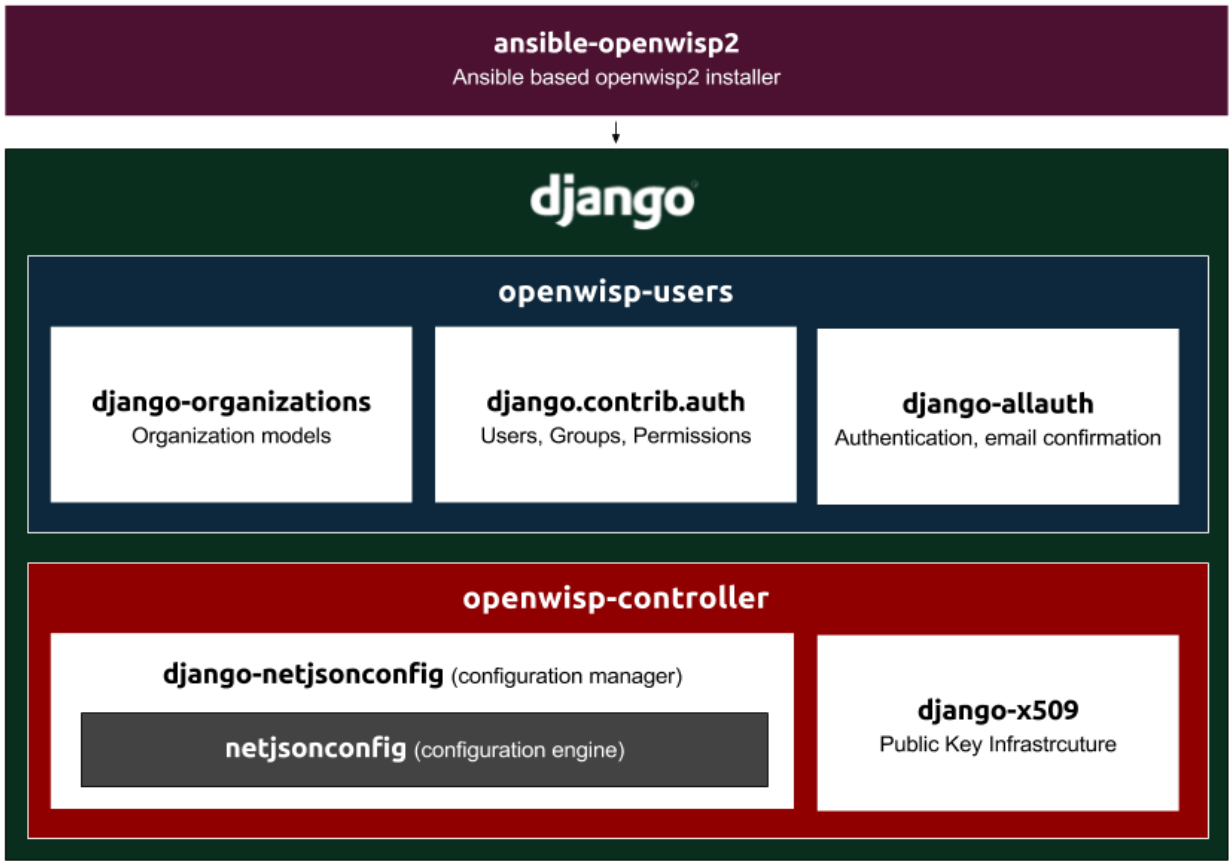


Fig 22: OpenWisp2 Architecture

The **OpenWISP Manager** makes centralized management of a large number of access points easier. With this tool it is possible to manage devices with a customized version of the OpenWRT firmware (i.e.the OpenWISP Firmware) that is also released with an open-source license. For this reason **OpenWM** and **OpenWF** can be used with any access point containing an Atheros Wi-Fi card supported by OpenWRT.

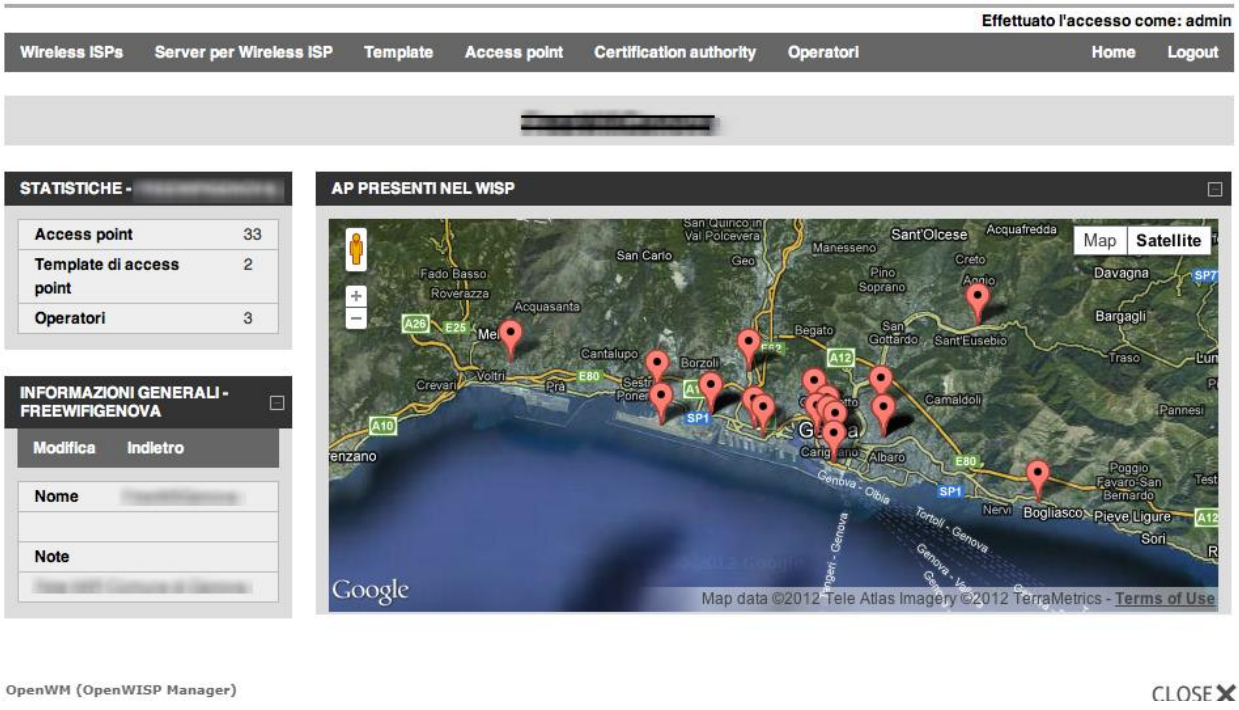


Fig 23: OpenWisp Access Point Management Interface

So there are many such genetic software for managing any kind of Access Point but as per our suggestion we recommend,

Recommendation 4: **OpenWisp** because it has got a open source license and it can configure any Access Point so it is much more feasible and flesxible to use in order control and configure any access points of any brand replacing the previous systems in more effective and efficient way.

Problem e) For remote access at ASUJS.ac.in no SSL certificate is found.

Proposed Solution: SSL Certificates are small data files that digitally bind a cryptographic key to an organization's details. When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to a browser. Typically,

SSL is used to secure credit card transactions, data transfer and logins, and more recently is becoming the norm when securing browsing of social media sites.

SSL Certificates bind together:

- A domain name, server name or hostname.
- An organizational identity (i.e. company name) and location.

An organization needs to install the SSL Certificate onto its web server to initiate a secure session with browsers. Once a secure connection is established, all web traffic between the web server and the web browser will be secure.

When a certificate is successfully installed on your server, the application protocol (also known as HTTP) will change to HTTPs, where the 'S' stands for 'secure'. Depending on the type of certificate you purchase and what browser you are surfing the internet on, a browser will show a padlock or green bar in the browser when you visit a website that has an SSL Certificate installed.

Fig 24:Working of SSL

So over here we will be using SSL Certification from **GlobalSign** an SSL Certification provider.

GlobalSign helps reduce the time, effort and cost associated with managing multiple enterprise level SSL Certificates. We provide centralized certificate management and all the tools, services and SSL products to reduce risk, respond to threats and control SSL cost.

Benefits:

Robust Range of SSL Assurance Levels & Configuration Options:

GlobalSign offers a range of SSL options ensuring your public servers and sites are in line with industry best practices but also offers cost effective-options for internal servers and special use cases.

Simplified Certificate and User Management:

GlobalSign's cloud-based certificate management platform offers unique features and functionality that give you complete control of your certificate needs from one centralized account.

Lower Total Cost of Ownership for SSL:

GlobalSign's Managed SSL platform significantly lowers the Total Cost of Ownership for SSL by reducing the man hours needed to manage certificates and offering volume discounts and flexible business terms.

Discover and Track All SSL:

GlobalSign's Certificate Inventory Tool (CIT) locates all of your SSL Certificates, and saves valuable time and resources over manual monitoring.

Define and Enforce SSL Policies:

Using outdated cryptography or weak key sizes can leave your company vulnerable. Ensure all your SSL Certificates comply with enterprise policy and that only appropriate individuals have access to certificate resources.

Fig 25: Facilities of getting SSL Certification through GlobalSign

So there many such SSL Certification provider but as per our suggestion we recommend,

Recommendation 5: **GlobalSign** SSL Certification provider which is quite effective and efficient for setting up a secure protocol in order prevent the malicious attack at the time of any transaction or sharing of confidential information.

Problem f) Antivirus license is expired.

Proposed Solution: Open Source Anti-Virus Policy

Purpose and Scope:

- To provide a university network environment that is virus-free and secure.
- To establish base requirements that must be met by computers connected to the University network to ensure effective virus detection and prevention.

- This policy applies to all computers that are connected to the University network via a university network connection, a wireless connection, a connection through the modem pool, or a VPN connection.
- This policy covers computers that are university-owned and computers that owned by individuals that are attached to the network. This policy covers all types of computers including, but not limited to, desktop computers, laptop computers, server class computers.
- This policy covers home computers that are owned and/or used by students, faculty, and staff, and/or their families that connect to the University network via the modem pool.

But in case of this university as per the survey the antivirus licenses are getting getting expired so we will be recommending a open source antivirus like Armadito. **Armadito Antivirus** is an open source antivirus tool for your servers and PCs. It protects your systems from any viruses and malware and provides solutions available for Windows machines. It is created with a web-based central administration console that can be remotely used from any location via an intuitive interface that will provide access to lots of features. Its dashboard offers access to on-demand scanning, real-time protection, threat detection journal, technical support and more.

Features:-

User-Friendly Interface:

Armadito Antivirus has been built in a way that it is quick, effective and simple to use. An easy-to-manage interface has been developed using AngularJs, HTML5, CSS3 technology, and aims to be multi-platform (Windows, Linux, Mac OS X).Indeed, the security software interface offers an easy setup and run functions that allow you to check your computers and servers status in an instant !The dashboard also gives access to all Armadito's features: on-demand scanning, real-time protection, quarantine zone, threat detection journal, technical support, and more.

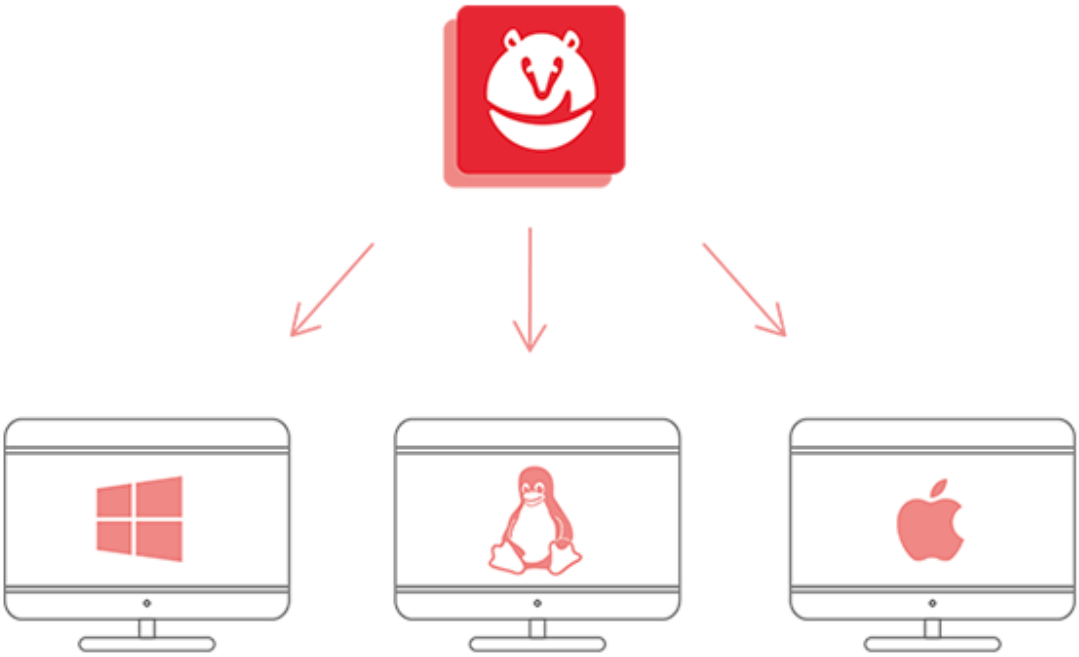


Fig 26: Open Source Feature of Armadito AntiVirus

IT IS A SECURE OPEN SOURCE ANTIVIRUS THAT INCLUDES:

- Classical signature-based malware detection.
- Both ClamAV signatures and YARA rules support.
- Innovative heuristic detection modules for binaries (MS-Windows and GNU/Linux) and for PDF documents.
- Real-time protection on MS-Windows and GNU/Linux.
- Quarantine zone, alerts transmission, events journal.
- Open-source codes (LGPL v3, GPL v3, MS-PL).

Antivirus auto renewal policy need to be implemented for the systems in ASUJS Campus for that we will be recommending a software license renewal solution like **Delphi License Renewal Tool.**

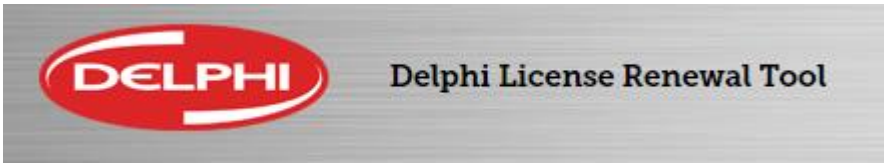
The License Renewal Tool makes your orders easy,

Designed for Delphi Distributors and dedicated to the Aftermarket software packages, this portal standardizes the license ordering process and offers a wealth of additional functionalities. Improve your business and increase your license renewal rate by taking full advantage of the LRT and its features.

To simplify your license management even more,

Sign-up to an Automatic License Renewal model and forget all about:

- Losing functionality for a period of time.
- Keeping track of expiry dates.
- That last minute rush when licenses are about to expire.



So there many such open source antivirus softwares in the market and licence renewal tools but as per our suggestion we recommend,

Recommmendation 6: **Armadito Anti-Virus** and **Delphi Software Renewal** Tool as it is effective and efficient over the previous system setups for automatic renewal warning and a open source antivirus in order to secure any systems in a network.

Problem g) Existing firewall Juniper NS5200 used as a gateway device. No proper access-control mechanism is in place.

Proposed Solution: The **NetScreen-5200** is a chassis-based, two-slot network security device with a 2U (rack unit) chassis. Slot 1 is for the management module and Slot 2 is for the Secure Port Module (SPM). The device has two hot-swappable power supplies for power redundancy and a removable fan module. The figure below shows a NetScreen-5200 with a management module in slot 1 (top) and an SPM in slot 2 (bottom).

Fig 27: Juniper NS5200 Gateway FireWall Device

Features:

- Purpose-built platform
- High performance
- Advanced network segmentation
- System and network resiliency
- High availability (HA)
- Interface flexibility
- Robust routing engine
- Virtual system support
- World-class professional services

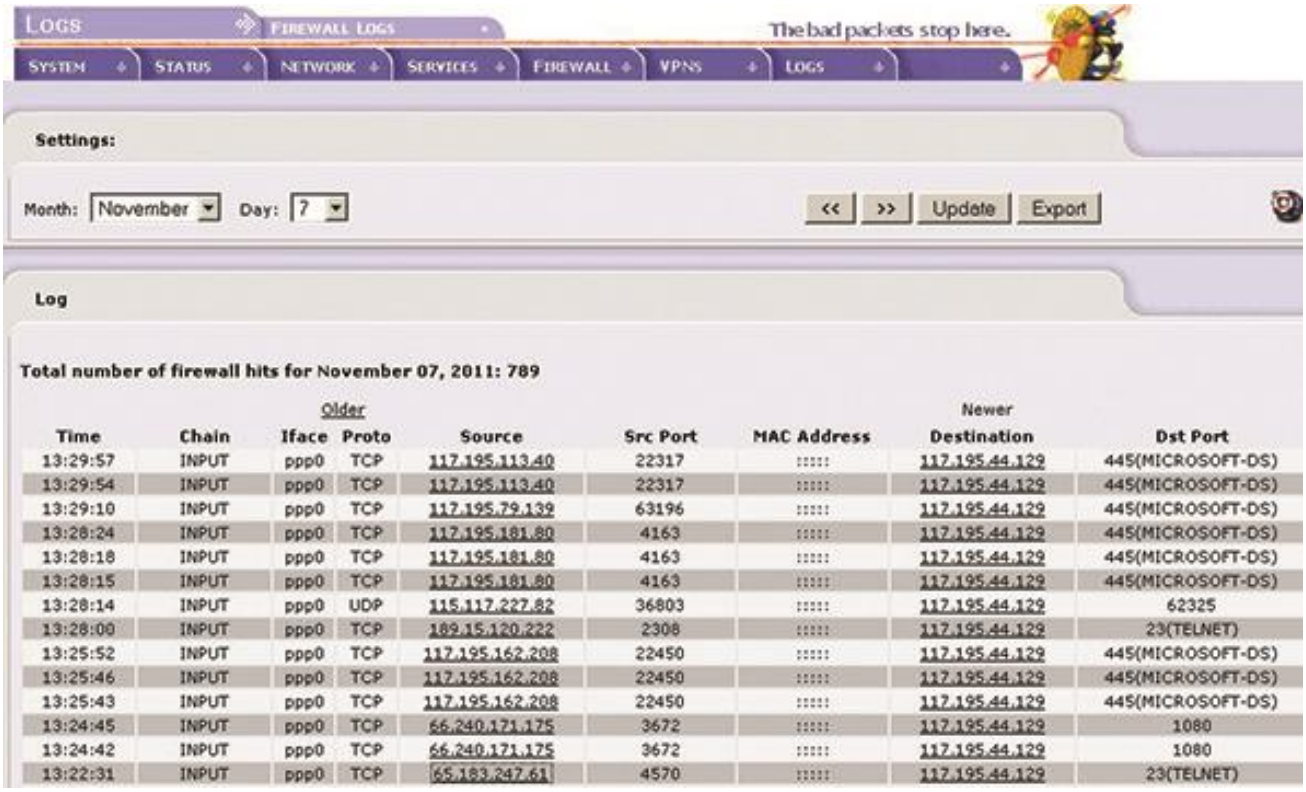
But the campus network firewall lacks the proper access control management software so for controlling the existing firewall device Juniper NS5200 we need a software solution like **IPCop.**

IPCop is an Open Source Linux firewall distribution, It is a stable, secure, user-friendly and highly configurable Firewall management system. IPCop provides a well-designed web interface to manage the firewall. It's very useful and good for Small businesses and Local PCs. It can turn your Old PC as a secure VPN to provide a secure environment over the internet**.**

Key Features:-

- Monitor and show the performance Graphics for CPU, Memory, and Disk as well as Network throughput.
- Provide logs.
- Multiple language support.

- Provides very secure stable and easily implementable upgrade and add on patches.



		Older					Newer	
Time	Chain	Iface	Proto	Source	Src Port	MAC Address	Destination	Dst Port
13:29:57	INPUT	ppp0	TCP	117.195.113.40	22317	::::::	117.195.44.129	445(MICROSOFT-DS)
13:29:54	INPUT	ppp0	TCP	117.195.113.40	22317	::::::	117.195.44.129	445(MICROSOFT-DS)
13:29:10	INPUT	ppp0	TCP	117.195.79.139	63196	::::::	117.195.44.129	445(MICROSOFT-DS)
13:28:24	INPUT	ppp0	TCP	117.195.181.80	4163	::::::	117.195.44.129	445(MICROSOFT-DS)
13:28:18	INPUT	ppp0	TCP	117.195.181.80	4163	::::::	117.195.44.129	445(MICROSOFT-DS)
13:28:15	INPUT	ppp0	TCP	117.195.181.80	4163	::::::	117.195.44.129	445(MICROSOFT-DS)
13:28:14	INPUT	ppp0	UDP	115.117.227.82	36803	::::::	117.195.44.129	62325
13:28:00	INPUT	ppp0	TCP	189.15.120.222	2308	::::::	117.195.44.129	23(TELNET)
13:25:52	INPUT	ppp0	TCP	117.195.162.208	22450	::::::	117.195.44.129	445(MICROSOFT-DS)
13:25:46	INPUT	ppp0	TCP	117.195.162.208	22450	::::::	117.195.44.129	445(MICROSOFT-DS)
13:25:43	INPUT	ppp0	TCP	117.195.162.208	22450	::::::	117.195.44.129	445(MICROSOFT-DS)
13:24:45	INPUT	ppp0	TCP	66.240.171.175	3672	::::::	117.195.44.129	1080
13:24:42	INPUT	ppp0	TCP	66.240.171.175	3672	::::::	117.195.44.129	1080
13:22:31	INPUT	ppp0	TCP	65.183.247.61	4570	::::::	117.195.44.129	23(TELNET)

Fig 28:: IPCop Firewall Hit list

So there many such Firewall management software but as per our suggestion we recommend,

Recommendation 7: **IPCop** Firewall management software as a open source which is quite effective and efficient for controlling any type of firewall device of any brand.

Problem h) Server Room maintained at ground floor with UPS Room. Problem in Air-conditioning unit occurs. Need for up gradation of Server Room with proper cooling and electrical safety mechanism.

Proposed Solution: A server room with a proper air-conditioning unit is an important part of a secure network infrastructure in order to keep the various network and end devices within a moderate temperature in a proper working condition but since it is a survey by the network team we would like to remain fix to our field by giving a suggestion of consulting

with the Air-Conditioning experts/electrical experts with a proper fire protection in case of emergency.

A server room is a room, usually air-conditioned, devoted to the continuous operation of computer servers. An entire building or station devoted to this purpose is a data center.

The computers in a server rooms are usually headless systems that can be operated remotely via KVM switch or remote administration software, such as Secure Shell (ssh), VNC, and remote desktops.

The fire protection system's main goal should be to detect and alert of fire in the early stages, then bring fire under control without disrupting the flow of business and without threatening the personnel in the facility. Server room fire suppression technology has been around for as long as there have been server rooms.

The following are the compotents of a server room:

Hardware: Primary hardware such as servers and data storage devices.

Racks: A system for stacking hardware such that space is used efficiently.

Cabling System:A system and set of conventions for cabling that keeps the complexity of cables manage.

Power: Server rooms typically consume significant power and may be designed to have redundant power sources such as grid and solar power.

UPS: uninterruptible power supply devices are used to protect equipment from unstable power such as a surge.

Infrastructure:Foundational services such as network equipment. A server room may be designed with no single points of failure for critical infrastructure. For example, multiple connections to the internet from different telecom companies.

Physical Security:Protecting the assets in a server room with access control, monitoring, emergency response, training and other internal controls.

Fire Protection:Fire protection equipment, procedures and structures such as a path for employees to escape a fire in the server room.

Environment Control:Control of humidity and air temperature. Computing equipment runs hot and cooling is a significant consideration in the design of a server room. For example, cool air can be directed at racks from the floor and warm air collected from the ceiling.

Operations:Processes and resources for supporting the server room including physical tasks such as swapping devices.

Backup:Backup of data and hot or cold sites for disaster recovery that are in a different physical location, preferably in another city or region.

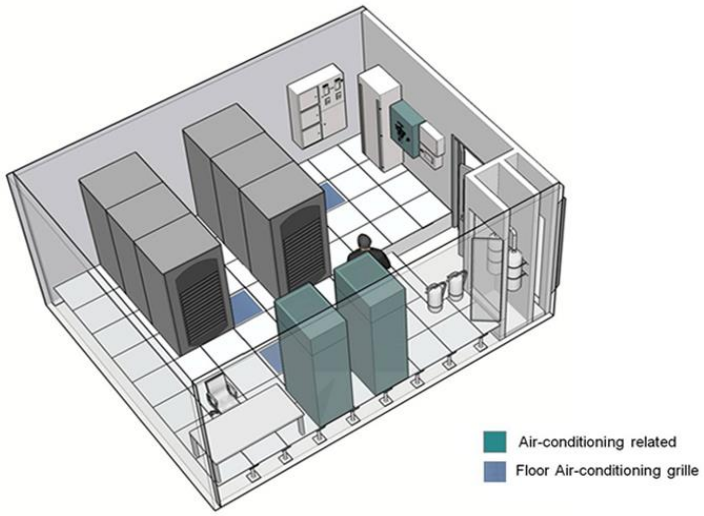


Fig 29: An example of a server room set-up

Benefits using HVAC in Server Rooms:

Heating, ventilation, and air conditioning (HVAC) is the technology of indoor and vehicular environmental comfort. Its goal is to provide thermal comfort and acceptable indoor air quality. HVAC system design is a subdiscipline of mechanical engineering, based on the principles of thermodynamics, fluid mechanics and heat transfer. "Refrigeration" is sometimes added to the field's abbreviation, as HVAC&R or HVACR or "ventilation" is dropped, as in HACR (as in the designation of HACR-rated circuit breakers).

HVAC is an important part of residential structures such as single family homes, apartment buildings, hotels and senior living facilities, medium to large industrial and office buildings

such as skyscrapers and hospitals, on ships and submarines, and in marine environments, where safe and healthy building conditions are regulated with respect to temperature and humidity, using fresh air from outdoors.

Ventilating or ventilation (the V in HVAC) is the process of exchanging or replacing air in any space to provide high indoor air quality which involves temperature control, oxygen replenishment, and removal of moisture, odors, smoke, heat, dust, airborne bacteria, carbon dioxide, and other gases. Ventilation removes unpleasant smells and excessive moisture, introduces outside air, keeps interior building air circulating, and prevents stagnation of the interior air.

Recommendation 8: Setting up a proper server room with a proper Air-Conditioning unit to keep the server systems and devices with in a moderate temperature.

Secure Network Infrastructure Design: -

The survey report around the ASUJS campus gives us the overview idea about the network Infrastructure/design. So, Wired Internet Access as well as Wireless Internet Access is distributed throughout the whole campus which includes ACDM Ground Floor portion, 1st Floor, 2nd Floor and 3rd Floor. It has also been distributed in the Library section as well as in the Staff Quarter, Boy's Hostel and Girl's Hostel. So, our team has planned out with the various h/w and s/w requirements as per the passive components like OFC/PVC Duct pipes and depending upon all this components our team has designed an optimized secure network infrastructure diagram to cope up the requirements as ASUJS is a part of National Knowledge Network (NKN). So the following diagram will describe the design in a detailed manner which includes 2 ISPs, a modem, a load balancer, a firewall, a router, a proxy server, a core switch, 4 distributed switch for ACDM, Boy's Hostel, Girl's Hostel, library and staff quarter along with a WLAN Controller device, Thin APs, wired APs for users carrying their own laptop or wireless devices, as well as for desktop and server machines. Beside N/w components and end user peripherals we have also upgraded networks infrastructure using an Open Source Network Management software Tools like Nagios, a Linux based captive portal authentication software to increase the security of the campus network infrastructure by restricting the new users/guest from accessing internet without filtration as well doing

the tasks like spam blocking, web filtering, antivirus, antispyware, intrusion prevention, VPN, Firewall etc. as well as latest antivirus software installed in every individual systems along with an automatic software updater and a O.S patch updater and a log table manager software on server system for the security and analysis purpose. So in the following network diagram we have also taken some other measures like renewing the antivirus policy of the system connected to the network.So we will be using latest version of antivirus software in the systems connected to the network infrastructure for the security purpose.

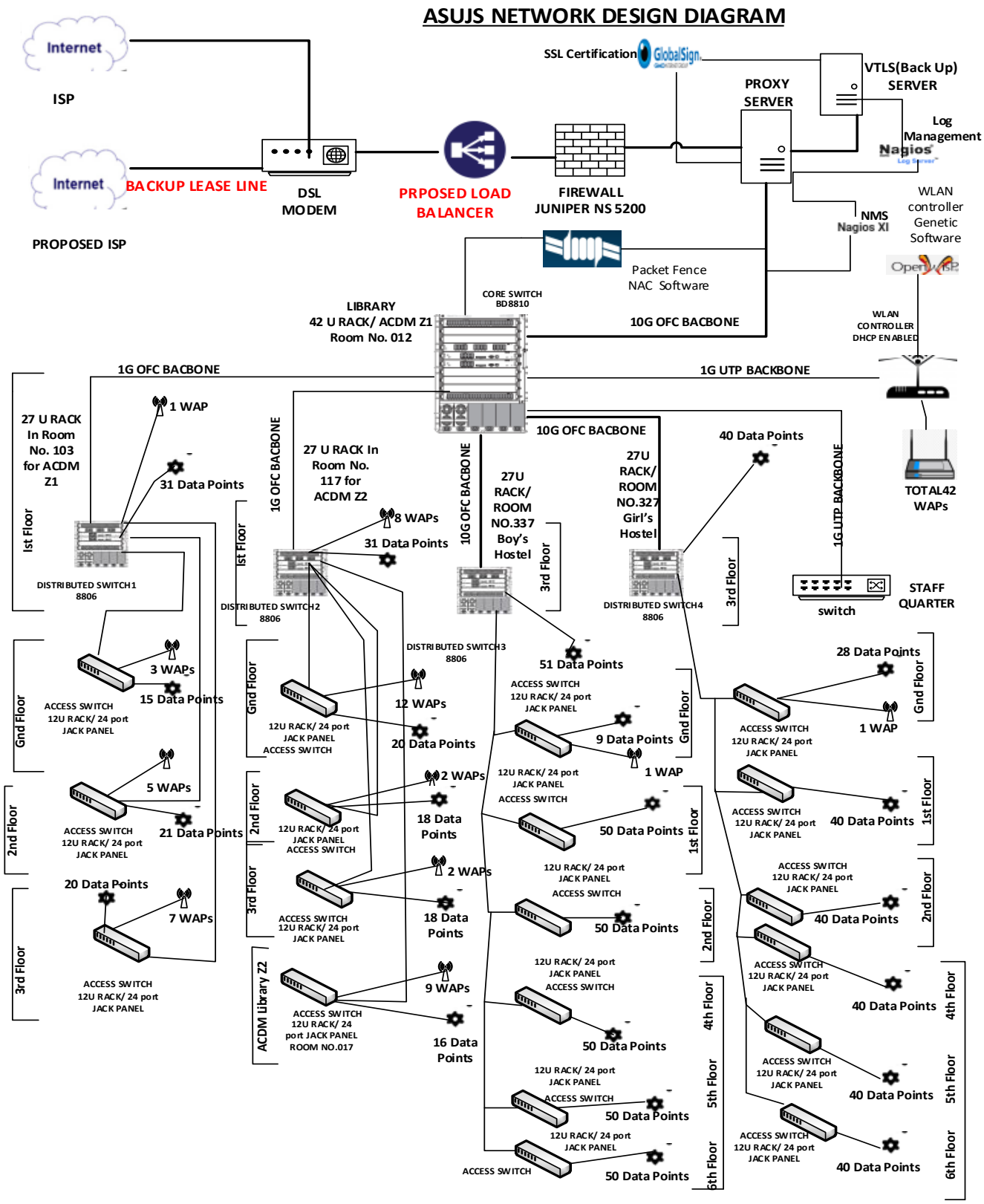


Fig 30:: Secure Network Architecture Diagram along with the security softwares

Conclusion: -

A secure network architecture planning has been executed so far along with various solution proposals for the afforementioned problems has also been recommended through the following recommendations focusing on the network security of an university campus through various ways namely:-

Recommendation 1: **Packet Fence** we suggest this for Network Access Control/ Captive portal Authentication Software which has been shown in Fig4 which is much more effective over the existing system for checking out the users who all are not recognised for accesing the campus internet service so it is very much helpful for the Network Admin in recognising a new/guest user trying to access campus internet service.

Recommendation 2: **Nagios Log Server** for it's flexibility and real time event analysis and cluster status information as it provides better performance then the existing system in the campus network setup keeping track and maintaining logs for the various internal internet access related information following the IT Law of India for a duration of 3 Months surely.

Recommendation 3: **NagiosXI** as a open source Network Management Software because it is very much user friendly and real time which helps network admin to manage any network device in a network cluster and performs in a better way than the existing systems for which we needed the same company based software but this is quite open to manage any device on a network infrastructure.

Recommendation 4: **OpenWisp** because it has got a open source license and it can configure any Access Point so it is much more feasible and flesxible to use in order control and configure any access points of any brand replacing the previous systems in more effective and efficient way.

Recommendation 5: **GlobalSign** SSL Certification provider which is quite effective and efficient for setting up a secure protocol in order prevent the malicious attack at the time of any transaction or sharing of confidential information.

Recommendation 6: **Armadito Anti-Virus** and **Delphi Software Renewal** Tool as it is effective and efficient over the previous system setups for automatic renewal warning and a open source antivirus in order to secure any systems in a network.

Recommendation 7: **IPCop** Firewall management software as a open source which is quite effective and efficient for controlling any type of firewall device of any brand

Recommendation 8: Setting up a proper server room with a proper Air-Conditioning unit to keep the server systems and devices with in a moderate temperature.

Short Term measures:-

- **Internet Access Rules**: - User based authentication must be implemented in the university to prevent misuse of Internet access. User may have to register them

with their user-id & machine mac address to get the access of the network. Unified threat management (UTM) or Radius server may be implemented for the purpose.

- **Internet Security Guidelines**: - A one page Internet security guideline providing do`s and don'ts may be distributed & signed during admission of Students. The guidelines also mention the penalties if found breaching the policy. This will prevent adding extra device to network and user related network issue.
- **Suggestion for Infrastructure upgrades**: - Based on the survey it is found that limitation of proprietary software. So more use of generic or open source software are encouraged. In case of Network Management software **Nagios** can be considered as an alternative. In case of Wireless controller issue the options are limited either upgrading the wireless controller or using the access-points as a separate entity without need of controller.

Long Term measure:-

- **Information Security Policy implementation**: - In long term perspective gradual implementation of Information Security Policy across the university may be implemented. Inputs from each stakeholder who are accessing network for their work should be taken into account.
- **Suggestion for Infrastructure Upgrades**: - In view of current server room infrastructure and future plan there is a need to upgrade the server room facilities and gradually move towards Data center.
- Moving towards for flexible and automatic network management and control.

Packet Fence Installation:-

Installing PacketFence from the ZEN:

The ZEN (Zero Effort NAC) edition of PacketFence allows you to rapidly get PacketFence running in your network environment. It consists of a fully installed and preconfigured version of PacketFence distributed as a virtual appliance. It can be deployed on VMware ESX/ESXi, Microsoft Hyper-V and other products. This section covers the deployment of the virtual appliance on VMware-based products. We are not supporting any Xen-based hypervisors yet.

Virtual Machine:

This setup has been tested using VMWare ESXi, Fusion and Workstation products with 8 GB of RAM dedicated to the virtual machine. It might work using other VMWare products. To properly run the PacketFence virtual appliance, you need a CPU that supports long mode. In other words, you need to have a 64-bit capable CPU on your host. PacketFence ZEN comes in a pre-built virtual disk (OVF). If you are using an ESX type hypervisor, you need to import the OVF using vSphere Client (or vCenter).

The virtual appliance passwords are:

- Management (SSH/Console) and MySQL
- Login: root
- Password: p@ck3tf3nc3
- Captive Portal / 802.1X Registration User
- Login: demouser
- Password: demouser

Import to ESX:

Make sure that there is only one virtual network card created, and also make sure that your vEthernet is connected to a virtual switch (vSwitch). That virtual network card will be used as the PacketFence management interface.

Import to VMWare Player/Workstation for Linux:

Newer version of VMWare Player handles the VLAN trunking a lot better. Having that said, we can use a single interface on the VM. So, you need to ensure that your VM host is plugged into a physical trunk port with VLAN 1,2,3,5,10 and 200 as the allowed VLAN. These VLANs will be used later in configuration examples.

Installing PacketFence on existing Linux

PacketFence provides packages repository for RHEL / CentOS as well as package repository fo Debian.

These repositories contain all required dependencies to install PacketFence. This provides numerous advantages. Among them, there are:

- easy installation
- everything is packaged as RPM and Debian packages
- easy upgrade
- Install your supported distribution with minimal installation and no additional packages. Then:
- On Red Hat-based systems
- Disable firewall
- Disable SELinux
- On Debian
- Disable AppArmor
- Disable resolvconf

Make sure your system is up to date and your yum or apt-get database is updated. On a RHEL-based system, do:

yum update
On a Debian system, do:
apt-get update
apt-get upgrade

Regarding SELinux or AppArmor, even if they may be wanted by some organizations, PacketFence will not work properly if SELinux or AppArmor are enabled. You will need to explicitly disable SELinux from the /etc/selinux/config file and reboot the machine. For AppArmor, you need to execute the following commands:

update-rc.d -f apparmor stop
update-rc.d -f apparmor teardown
update-rc.d -f apparmor remove

Regarding resolvconf, you can remove the symlink to that file and simply create the /etc/resolv.conf file with the content you want.

Extreme Networks Switch Configuration (Black Diamond BD8000 Series):

PacketFence supports Extreme Networks switches using:

- linkUp/linkDown
- MAC Address Lockdown (Port Security)
- Netlogin - MAC Authentication
- Netlogin - 802.1X
- RADIUS authentication for CLI access

All Extreme XOS based switches

In addition to the SNMP and VLANs settings, this switch needs the Web Services to be enabled and an administrative username and password provided in its PacketFence configuration for Web Services.

MAC Address Lockdown (Port-Security):

linkUp/linkDown traps are enabled by default so we disable them and enable MAC Address

Lockdown only.

Global config settings without Voice over IP (VoIP):

enable snmp access

configure snmp add trapreceiver 192.168.1.5 community public

enable web http

configure vlan "Default" delete ports <portlist>

configure vlan registration add ports <portlist> untagged

configure ports <portlist> vlan registration lock-learning

disable snmp traps port-up-down ports <portlist>

where <portlist> are ports you want to secure. It can be an individual port or a port-range with a dash.

Global config settings with Voice over IP (VoIP):

enable snmp access

configure snmp add trapreceiver 192.168.1.5 community public

enable web http

configure vlan "Default" delete ports <portlist>

configure vlan registration add ports <portlist> untagged

configure vlan voice add ports <portlist> tagged

configure ports <portlist> vlan registration lock-learning

configure ports <portlist> vlan voice limit-learning 1

disable snmp traps port-up-down ports <portlist>

where <portlist> are ports you want to secure. It can be an individual port or a port-range with a dash.

MAC Authentication:

AAA Configuration: configure radius netlogin primary server 192.168.1.5 1812 client-ip 10.0.0.8 vr.

VR-Default:

configure radius netlogin primary shared-secret 12345

enable radius netlogin

Netlogin (MAC Authentication):

configure netlogin vlan temp

enable netlogin mac

configure netlogin add mac-list default

configure netlogin dynamic-vlan enable

configure netlogin dynamic-vlan uplink-ports 50

configure netlogin mac authentication database-order radius

enable netlogin ports 1-48 mac

configure netlogin ports 1-48 mode port-based-vlans

configure netlogin ports 1-48 no-restart

802.1X

AAA Configuration:configure radius netlogin primary server 192.168.1.5 1812 client-ip 10.0.0.8 vr

VR-Default: configure radius netlogin primary shared-secret 12345

enable radius netlogin

Netlogin (802.1X):

configure netlogin vlan temp

enable netlogin dot1x

configure netlogin dynamic-vlan enable

configure netlogin dynamic-vlan uplink-ports 50

enable netlogin ports 1-48 dot1x

configure netlogin ports 1-48 mode port-based-vlans

configure netlogin ports 1-48 no-restart

RADIUS authentication for CLI access: Configure RADIUS server IP address as primary server and the switch IP address as the client-ip. Be sure to specify the correct virtual router

configure radius mgmt-access primary server <SERVER_IP> 1815 client-ip <CLIENT_IP>

vr <VR>

Configure the RADIUS shared-secret

configure radius mgmt-access primary shared-secret <SHARED_SECRET>

Enable RADIUS for management access

enable radius mgmt-access

Installing Nagios XI with VMware Workstation Player:

- Click “Download Now” under VMware.
- Add your information to the form and click “Continue”.
- Your download will begin in the lower left hand corner of your browser. This is the Nagios XI OVA file.
- Click “Download VMware Workstation Player.”
- A new tab will open up taking you to VMware.com. This is where you can
- Download the virtual machine VMware Workstation Player.
- Click “Download Now” under VMware Workstation 12.5 Player for Windows 64 bit. The download will begin in the lower left hand corner of your browser.
- Run setup wizard for VMware Workstation.
- Open VMware Workstation Player from your Desktop.
- Click on “Player” -> “File” -> “Open.”
- Click on the OVA file from your downloads folder.
- Name your virtual machine whatever you like Click “Import”.
- The OVA file will begin importing.
- Click “Play virtual machine.” This will boot up Nagios XI’s login prompt.
- You’ll see the player turn to black and begin loading at the bottom.
- The final step in VMware Workstation Player is to login. You’ll see the login credentials highlighted here.
- Click in the window and type “root” for the login. Press ENTER on your keyboard. Keep in mind, when in the VMware Workstation Player your mouse will not be visible. To release your mouse, hold down CTRL + ALT. Your mouse will then become available to you. To type back in VMware Workstation Player, you will first have to click the window.
- Type “nagiosxi” for the password. When typing you will not see the characters show up. When finished, press ENTER on your keyboard.
- The following screen will show up. It is important to note that your IP address will be different. Make sure you use the IP address shown in your VMware Workstation Player.
- Open up your preferred web browser. You’ll see Google Chrome here. This is where you would type in your specific IP address (found in VMware Workstation Player, just below the Nagios XI banner) and type it into the search bar. Hit ENTER on your keyboard when done.
- You’re now able to access Nagios XI. Click the button to configure General Program Settings.

- In the Nagios XI Installer you can configure your name, email address, password and choose your time zone. Once all of your changes have been made, click “Install.”
- Congratulations! You have successfully installed Nagios XI. Here you’ll see your login information. It will be different than you see here, depending on the configurations you made on the previous screen. It is important that you know your username and password intimately before clicking “Login to Nagios XI.”
- Here is the login page.
- Insert your login credentials from the previous page into the login box. The default language for Nagios XI is English. If you speak another language, it will benefit you to choose that language on this page as well. Click “Login.”
- In order to access the Nagios XI Dashboard, you’ll have to read the license agreement andclick “Submit.”
- That’s it! You have successfully installed Nagios XI and can being monitoring.

Installing Nagios Log Server with VMware Workstation Player:

- Click “Download Now” under Open Virtualization Format.
- Add your information to the form and click “Continue”.
- Your download will begin in your browser. This is the Nagios Log Server OVA file.
- Click “Download VMware Workstation Player.”
- A new tab will open up taking you to VMware .com. This is where you can download the virtual machine VMware Workstation Player.
- Click “Download Now” under VMware Workstation 12.5 Player for Windows 64-bit. The download will begin in your browser.
- Run setup wizard for VMware Workstation.
- Open VMware Workstation Player from your desktop.
- Click on “Open a Virtual Machine.”
- Click on the OVA file from your hard drive.
- Name your virtual machine whatever you like Click “Import.”
- The OVA file will begin importing.
- Click “Play virtual machine.” This will boot up Nagios Log Server’s login prompt.
- You’ll see the player turn to black and begin loading.
- The final step in VMware Workstation Player is to login. You’ll see the login credentials highlighted here.
- Click in the window and type “root” for the login. Press ENTER on your keyboard. Keep in mind, when in the VMware Workstation Player your mouse will not be visible. To release your mouse, hold down CTRL + ALT. Your mouse will then become available to you. To type back in VMware Workstation Player, you will first have to click the window.
- Type “nagiosls” for the password. When typing you will not see the characters show up. When finished, press ENTER on your keyboard.
- The following screen will show up. It is important to note that your IP address will be different. Make sure you use the IP address shown in your VMware Workstation Player.
- Open up your preferred web browser. You’ll see Google Chrome here. This is where you would type in your specific IP address (found in VMware Workstation Player, just below the Nagios LS banner) and type it into the search bar.Hit ENTER on your keyboard when done.
- Fill in the important information for the username, password, email address, language and timezone. When done, click on “Finish Installation.”

- With the username and password you created on the previous page, input that information and log in.

How to add Inputs to Nagios Log Server :

The inputs are a structured format like this:

<plugin> {

<config_option> => <config_value>

<config_option> => <config_value>

}

Logstash allows a large amount of possible plugin types, here are

two examples:

syslog {

type => 'syslog'

port => 5544

}

file {

type => 'syslog'

path => ['/log/file/location/*.log']

start_position => 'beginning'

add_field => { 'program' => 'your_program' }}

Another example is the tcp plugin configured for receiving Windows Event Logs. This isconfigured by default in Nagios Log Server:

tcp {

type => 'eventlog'

port => 3515

codec => json

{

charset => 'CP1252'

} }

Click the Add Input drop down list and select Custom. A new block will appear at the bottom of the list of Inputs. Type a unique name for the input. In the text field you will need to define the input configuration. Here is a basic example for a local file on the Nagios Log Server machine itself:

file {

type => "testing"

path => "/tmp/test.log"

}

Once you have finished click the Save button.

Click the Apply button and then on the modal that appears click the Yes, Apply Now button.

Test Input :

Establish a terminal session to your Nagios Log Server instance and then execute thefollowing command:

echo "This is a test log entry" >> /tmp/test.log

Now in Nagios Log Server open the Dashboards page and perform the query type: testing.

The query should return one result in the ALL EVENTS panel. Clicking on the log entry will show you the full details about the entry.

Here you can see that the type is testing and the text has been stored in the message field.

Obviously this test input we created isn't that useful however the purpose was to demonstrate how you can easily create an input and start receiving log data.

Verify :

The Verify button ensures that the current saved configuration is valid. It can be useful when updating your configurations before attempting to Apply Configuration. Wait while the configuration is verified.

If you do not receive a Configuration is OK message then you will need to fix the problem before applying the configuration.

Reference: -

https://www.google.co.in/

https://www.nagios.com/products/nagios-xi/

https://www.nagios.com/products/nagios-log-server/

https://packetfence.org/

http://openwisp.org/

http://learn.extremenetworks.com/

https://products.office.com/en-in/visio/flowchart-software

https://www.vmware.com/in/products/workstation-pro.html