Knowledge Consortium of Gujarat
Department of Higher Education - Government of Gujarat
Journal of Multi-Disciplinary - ISSN : 2279-0268

Continuous Issue - 23 | March – April 2018

Safeguarding Educational Campus from Anonymous Users and Social Media Using MikroTik Operating System

Abstract:
Nowadays in educational campus especially in technical campuses use of Internet become obsolete. One cannot avoid internet during study time for the students. The problem with this scenario is that sometimes students can have distracted from the social media sites such as Facebook, WhatsApp and many more or there may be the case where administrator wants keep the watch on the students' activities as well as sometimes wants to block such sites. In addition, Administrator wants to keep the log of the activities performed on the specific workstation. Another issue discussed in the paper is that in the free wi-fi campus administrator wants to authenticate the anonymous users apart from the routine authentication like general password for all users. The paper describes the role of MikroTik Operating System to manage and authentic the issues discussed above.

1. Introduction

Nowadays, Internet becomes the prominent source of information gathering and knowledge sharing in the educational campus. Online communication becomes primary need for any educational campus for everyday communication between student-student and student-teacher and teacher-teacher as well. Social platform like WhatsApp, Facebook etc are unavoidable medium for communication. In the educational campus, especially in IT institute most of the study directly or indirectly deals with active Internet and its uses. Students as well as Instructors need Internet resources for their work. The free access of Internet resources sometimes leads students to use or misuse their social media platforms which are not advisable at study time. Distraction leads to harm their work and study. The paper focuses on issue related to track student's social media activities and somehow limits the usage of such medium. Using the Microtik Router Operating system architecture one can limit and track the student's access of social media.

MikroTik Limited known internationally as MikroTik is a Latvian manufacturer of computer networking equipment. The main product of MikroTik is a Linux-based operating system known as MikroTik Router OS. It allows users to turn a selected PC-based machine into a software router and allows features such as firewall rules, VPN Server and Client, bandwidth shaper Quality of Service, wireless access point and other commonly used features for routing and connecting networks together. The system is also able to serve as adaptive-portal based hotspot system [1].

MikroTik originally intended for Internet Service Provider (ISP) serving customers using wireless technology. Currently, MikroTikls provides services to many wireless ISPs for Internet access services in many countries in the world and is also very popular. MikroTik provides hardware and software devices for Internet connectivity in most countries around the world[6].

2. Proposed Model and Architecture

2.0 Introduction of the proposed architecture

To understand the scenario, we have taken the live case study of our University campus. Figure 1 shows the existing architecture as well as proposed architecture. As shown in the first part of the figure campus is fully Wi-Fi with fibre optics 1gbps internet line which is shared all over the university using ring topology for all four buildings. The existing line is open for all with common password and login. So, every known and unknown user can access the internet without any restriction, which is considered as severe security threat. In the existing architecture there is no monitoring as well as controlling mechanism.

Hence, there arise a need for securing the net as well to establish a monitoring mechanism for students, teachers and other users. As shown in the figure we have applied our model on existing shared internet line to make it super secure using two step authentication username passwords and to keep log to avoid unauthorised access as well.

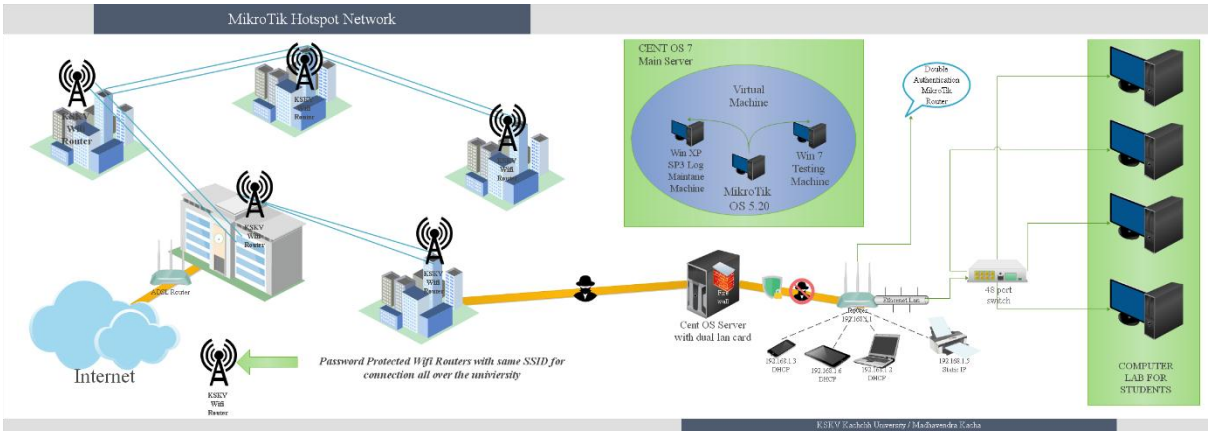

Figure 1. Existing and Proposed Architecture

Figure shows the MicroTik router for double authentication which will verify the user and it can monitor the activities of the user also. Using firewall, we can manage the user activities, filter the websites and manage the traffic also. In this model, we can assign each user a separate login and password. We can set the usage limit of data say 2 mbps per day. Students and faculties can be given separate access and identification. There is a facility to assign guest user access also. Administrator can keep the everyday log files of each user and block the unimportant and sensitive sites. For the pilot study, we have taken the case of computer science department and its laboratory scenario. Further section deals with technical aspects of the proposed architecture.

2.1 Installation of Microtik OS

The hardware and software used in the proposed architecture are as follows:

1. CentOS 7 server installed with 8GB RAM with two LAN cards
2. A Virtual Machine Installed in Cent OS Server with Win-XP for running Win-Box utility to connect with router OS.
3. A Virtual OS 512RAM, Virtual CDROM drive, Virtual Hard disk drive of 10Gigabytes, Virtual Motherboard with processor of 2.0 GHz speed.
4. MikroTik Routers CD for installation.
5. Microsoft FrontPage CD 2003 package for the web hotspot interface design in Win-XP SP3 OS
6. Kiwi Syslog Server Free Edition for log management [2].

During installation, press" a" key for select all and then press" i". Then, answer" n" to first question and" y" to second as shown in figure 2[3].

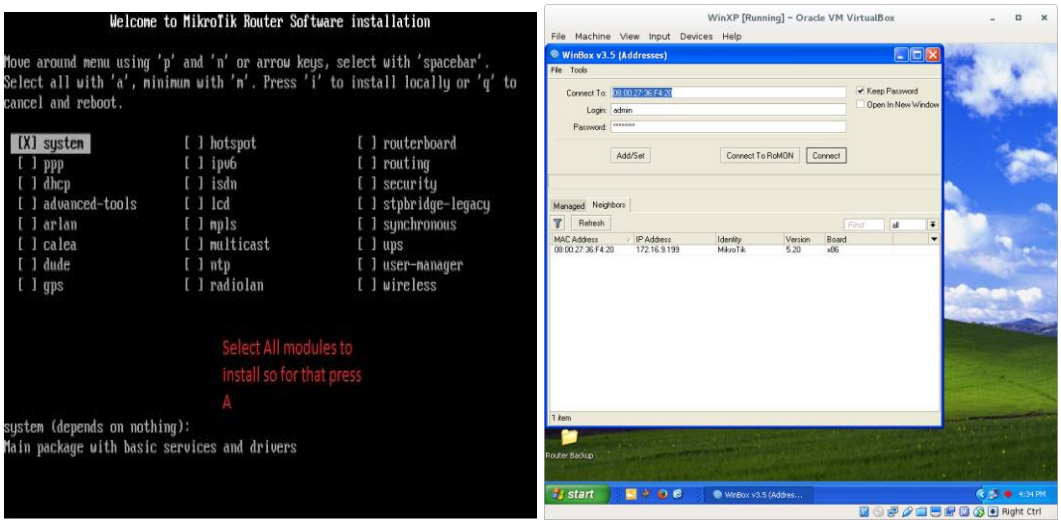

Figure 2. Installation steps and user access screen in Win-XP

Win-XP is required for installation as a virtual OS, it should be noted that linux based platform are not supported in this mechanism.

After installation you will be asked by Win-Box for user-name and password which you have set during installation process but by-default user-name will be ***admin*** and password will be blank but here we have set for security purpose.

2.2 License the software

The software allows you to use all its features for 24 hours only from the booting time. If the license key will not be entered during this period of time, the router will become unusable and will need a complete re-installation. Router OS licensing scheme is based on software IDs. To license the software, you must know the software ID. It is shown during installation procedures, and also you can get it from system console or Win-box. To get the software ID from system console, type: /system license print [4].

2.2.1 Network Planning

The IP address for the LAN1 is 172.16.9.199 for main internet line and for Secured Mikrotik double authentication LAN2 has this practical implementation DHCP Server with class C address concerned with 192.168.2. One is for router and from192.168.2.2–254 addresses are used for testing, while the subnet address is 255.255.255.0 and gateway is 192.168.2.1. We applied 192.168.2.1 as the gateway for the wireless interface also while the subnet address remains 255.255.255.0.
The DNS still remains 192.168.2.1 and our DNS name is kskvcc.com. so all the users will be diverted to this address which is our authentication system where user will authenticate itself by entering given user-name and password rather guest can get registered by self and they will get email their user-name and password and once administrator enable guest's account then only unknown guest can take grants to access internet other hackers will not get permission to access internet without contacting with administrator.

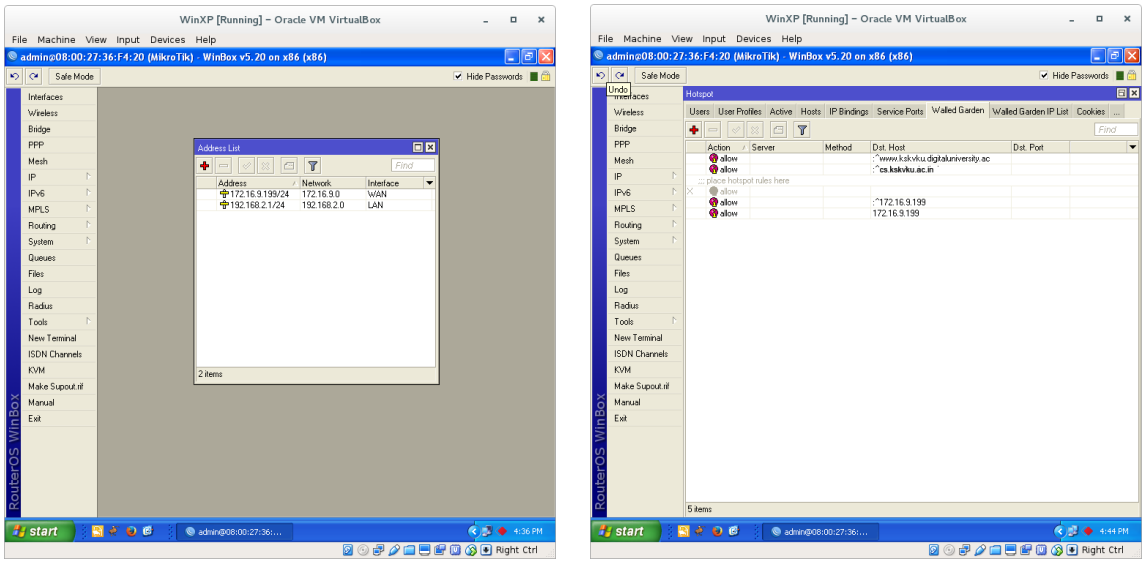

Figure 4. Interfaces WAN/LAN Configuration

2.2.2 Walled Garden

Walled garden is the place where anyone can be roaming as roam in the garden, here we have implemented two websites which are free to access without login to the Mikrotik system so any guests can surf our site to get news notice and updates. For example in our case, there are two sites namely http://kskvku.digitaluniversity.ac/ and http://cs.kskvku.ac.in/.

2.2.3 Network Rules

Traffic is getting higher and higher as there are unlimited data to be traverse from source to destination and as the nature of human not all the end users have same manner to obey rules strictly some of them will surely break the rules to collide our network so to keep sharp watch on them we must have some strict rules to be establish in the network to maintain the discipline.

Mikrotik have this functionality to reroute the traffic on the right path with firewall rules applied by the network administrator and keep log for each user with login till logout time. Students will get four hrs to surf internet per day with the speed of 1mbps and faculty members have with unlimited speed.

There are two types of registration scheme:

1. Self Registration 2. Registration by Administrator

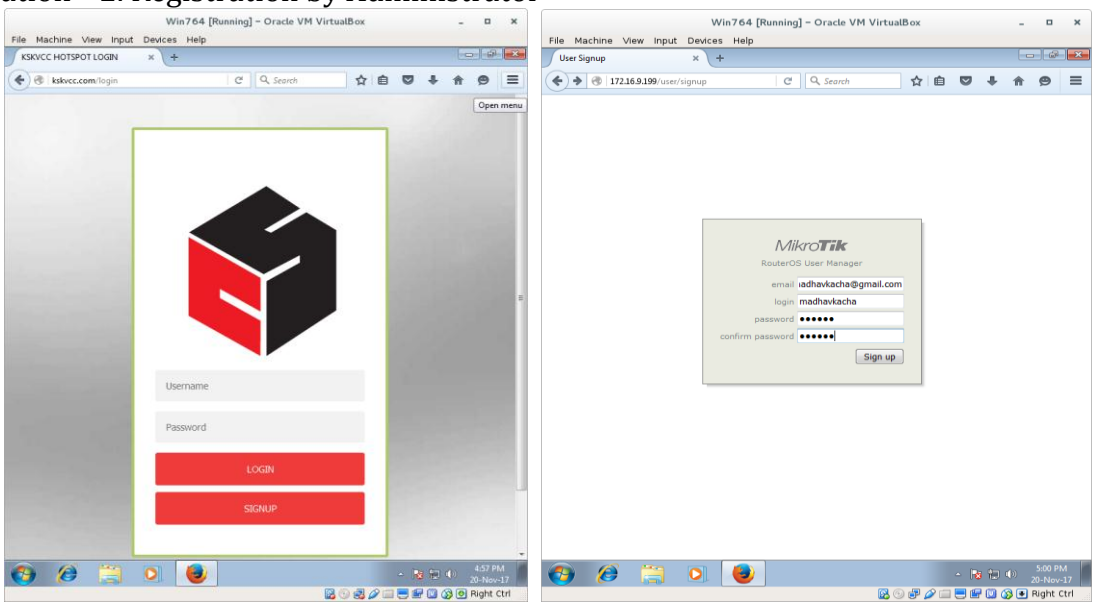

Figure 5. Login and sign up Screen and Self-Registration

2.2.4 Network Inspector

The job of network inspector is to keep sharp eyes on the entire route which are going from the source to the main ISP internet connection. The university Internet authentication system is not available at the time so for testing purpose we have tested on computer science department to apply successfully on whole university to wirelessly transmit internet services across the whole campus as university have fully

wifi connection all over the campus, especially within the classrooms, lecture halls and staff offices. It also offers free surfing of the department's website to the students and any outsiders. It also serves as a virtual e-notice board to students and lecturers for disseminating vital information across the campus using wireless Wi-Fi technology. In additional we have implemented to keep the entire student's URL visits logs to avoid any conflicts not to violate cybercrime rules. Each user with its allocated IP and MAC address will be note down in the log with time-stamp with URL link.

2.2.5 Social App Ban

End users now a day are engaging with WhatsApp and face book and all other social apps, as well as torrents which is time wasting for most of the time so to keep ban on such activities there are certain port blocks and traffic rules to be accepted and to be rejected is assigned by the network administrator.

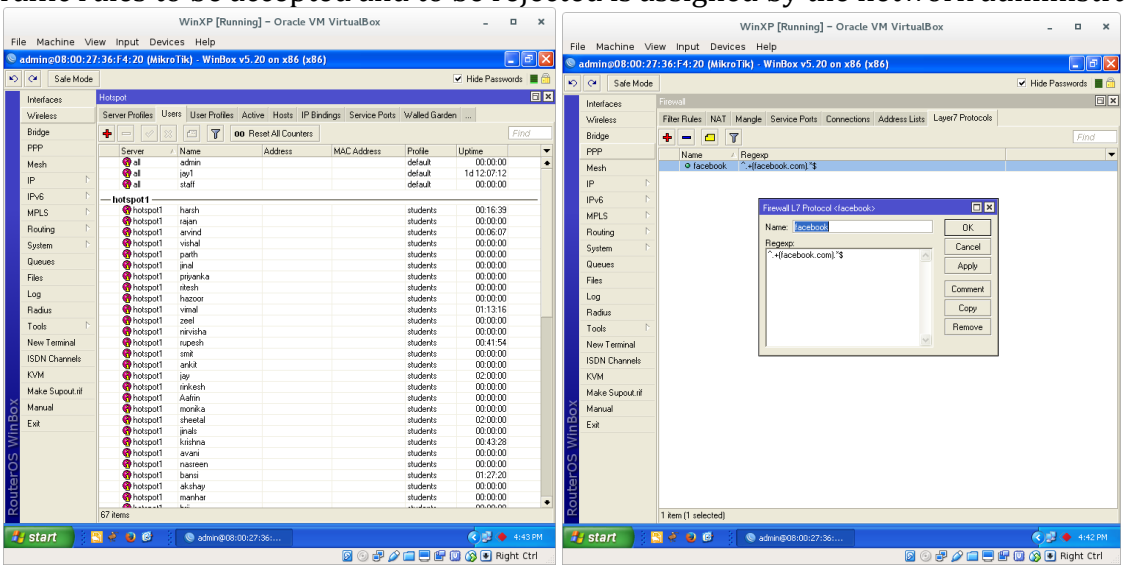

Figure 6. List of students are being inspect and Face book Banned

2.2.6 Log Management

As shown in figure 6 Kiwi log manager is free to use and keep URL records for every user with date time and login logout time with URL visited, URL requested with time stamp except https traffic sites secured so only http traffic and porn sites and torrents are ban for the institute.

Figure 7 shows the banned user of WhatsApp and screen shots of Kiwi log manager. Figure 8 shows the day to day log management and detailed log files.

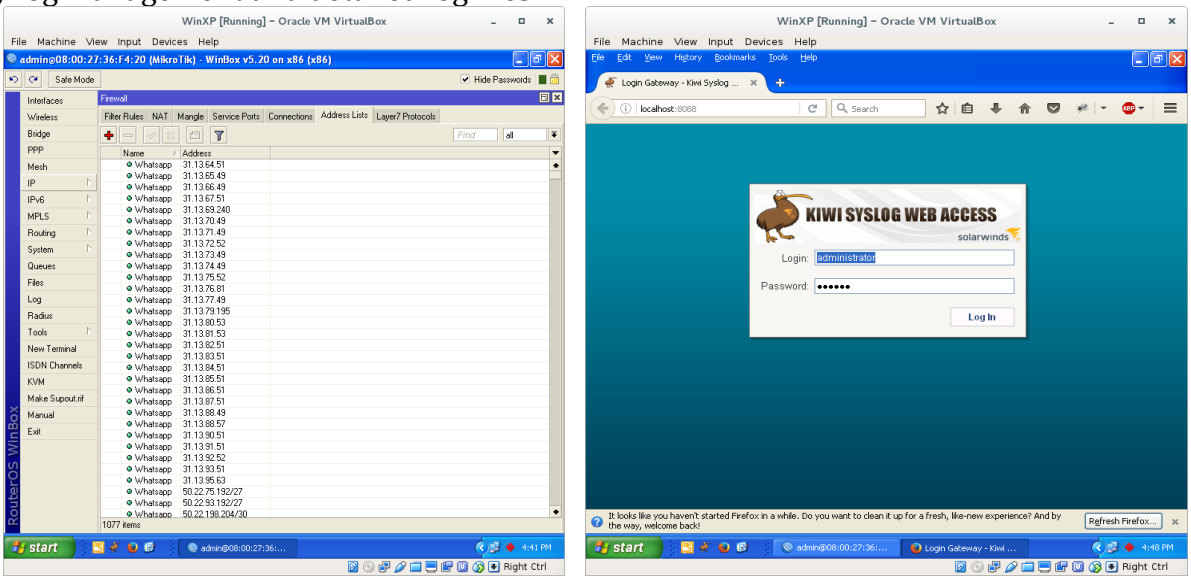

Figure 7. Whatsapp Block with list of all the 1077 IPs and Kiwi Log Manager

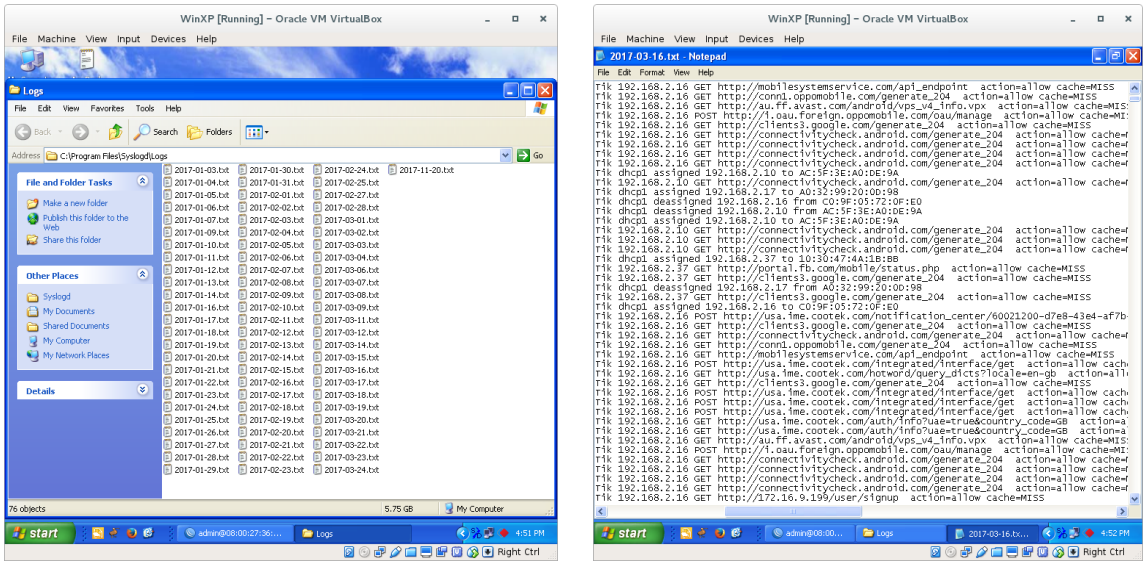

Figure 8. Day by Day Logs with Automatic Timestamps and Detailed log

2.2.7 Self-User Management

Self-registered users can manage and modify their profile from the emailed information like password change usage details and bandwidth usage information with session wise day by day report. Figure 9 shows the screen for self user management.

2.2.8 Guest Users

Mikrotik has a great facility to generate a batch of voucher generation system in which we can generate one or more vouchers for our guest who wants to surf the internet with unlimited speed and hours. Figure 10 shows the screen for guest user management.

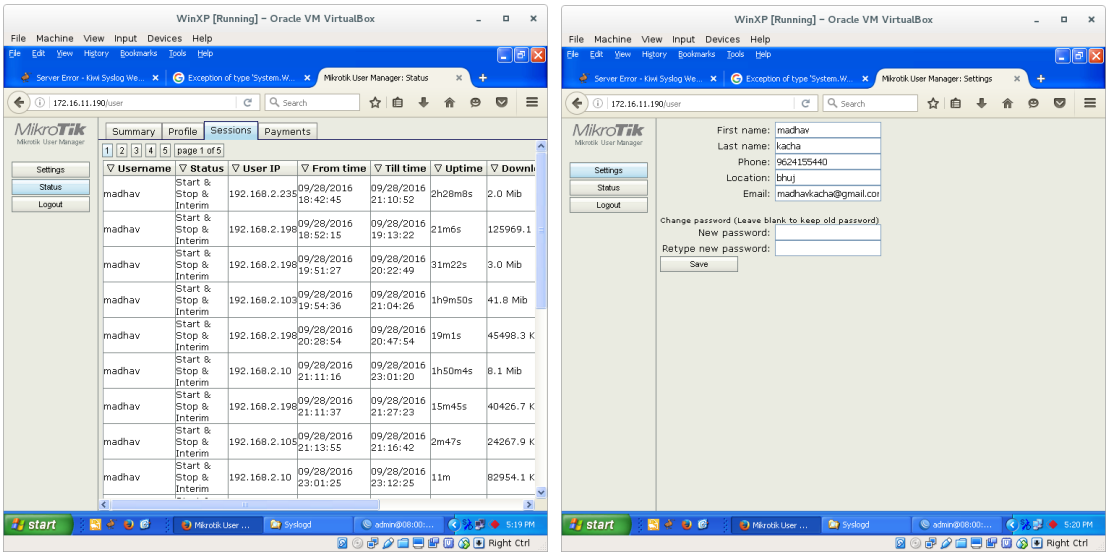

Figure 9. User log for their use and Self-Password change

Figure 10. System Generated User-name/password for guest

Conclusion

The paper discussed the issues related to the misuse of the social media which is publically accessible freely. Using MicroTik OS router administrator the double authenticates the security of the internet and intranet. One can monitor and track all the activities of the user on the workstation and instruct and

restrict whenever necessary. Initially as a pilot case it is demonstrated for the one particular campus only, in future we can cover it for the whole campus.

Acknowledgment

Our sincere gratitude to the authorities of KSKV Kachchh University and Department of Computer Science for facilitating the infrastructure and motivating for the project.

References

I. The MikroTik Documentation Manual (2018, April 17). Retrieved from https://wiki.mikrotik.com/wiki/Manuals

II. The Kiwi Syslog Free Edition (2018). Retrieved from https://www.kiwisyslog.com/free-tools/kiwi-free-syslog-server

III. Saliu, A.M. & Kolo, M.I & et.al. (2013). Internet authentication and billing (hotspot) system using MikroTik router operating system. 1(1): 51-57.

IV. Mollick, P. & Biswas, S. & et.al. (2016). Mikrotik Router Configuration using IPv6. International Journal of Innovative Research in Computer and Communication Engineering,4(2).

V. R. Berry & R. Gallager (2002). Communication over fading channels with delay constraints. IEEE Trans. Inf. Theory , 48(5), 1135-1149.

VI. Siahaan, M.D. & Panjaitan M.S & et.al. (2016). MikroTik Bandwidth Management to Gain the Users Prosperity Prevalent. International Journal of Engineering Trendsand Technology (IJETT), 42(5).

****

Madhavendra V. Kacha
Department of computer science
Krantiguru Shyamji Krishna Verma Kachchh University
Bhuj

Mahesh D. Mulani
Department of computer science
Krantiguru Shyamji Krishna Verma Kachchh University
Bhuj

Copyright © 2012 – 2018 KCG. All Rights Reserved. | Powered By: Knowledge Consortium of Gujarat