ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 7, July 2018

Enhancing Mikro Tik Router's Fundamental Security

Habibur Rahman Mukul[1], Saidur Rahman[2]

UG Student, Dept. of EEE, American International University-Bangladesh, Dhaka, Bangladesh[1]

UG Student, Dept. of EEE, American International University-Bangladesh, Dhaka, Bangladesh[2]

ABSTRACT: The evolution of networking and the Internet, the threats to information and networks has risen enormously. With the advent of the Internet, the need for a secure network has become vital for businesses with an Internet connection. Before a network can be secured for a business, a network security policy has to outline all the network resources (such as: router, switch, end devices) within that business and identify the required security level for those resources. The network security policy also defines the security threats and the actions taken for such threats [1]. In this paper, we offer some such elementary security policies for MikroTik router's to ensure proper security stability.

KEYWORDS: MikroTik Router, Router OS, WinBox, Security threats etc.

I. INTRODUCTION

Router security consists of three major elements: physical security of the router, operating system security, and security that can be affected through configuration. Physical security involves restricting access to the router. Exploits that can easily be prevented from remote locations are extremely difficult or impossible to prevent if an attacker can gain access to the router's management port or console [2], [3]. The inherent security of MikroTik OS also plays an important role in router security. MikroTik OS is quite stable and robust. MikroTik OS provides features to protect against attacks, allowing you to configure the router to minimize vulnerabilities.

II. REASONS FOR SECURITY

Any communication network is vulnerable with various security threats. Many of these threats have become cleverly exercised attacks causing damage or committing theft. Gaining the unauthorized access of the network is one of the great threats on the network. It is important to take preclusive steps for the unauthorized people to access the network. Besides this unauthorized access it also necessary to detect the intruders and prevent their intrusion within the network. Information is an asset that must be protected. Without adequate protection or network security, many individuals, businesses, and governments are at risk of losing that asset. Network security is the process by which digital information assets are protected, the goals of security is to protect confidentiality, maintain integrity, and assure availability [4]. But if any network faces security issues and attacks by multiple security threats then it is important to take necessary action for fixing the issues to ensure the obvious protection of information and infrastructure.

III. MITIGATION OF THE SECURITY THREATS

A. *Administrative users credentials:*

MikroTik router's default username is "admin". If it is kept to the default username, it can be assumed very easily. So it is recommended to change the username and set a strong password for the admin privileged user.

How to change credentials? :
Step 1: Log in WinBox
Step 2: Click on 'Systems' > 'Users'

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 7, July 2018

Step 3: Click on 'admin' and change the default username (we use 'titas' as username)
Step 4: Click on 'Password' and assign a password

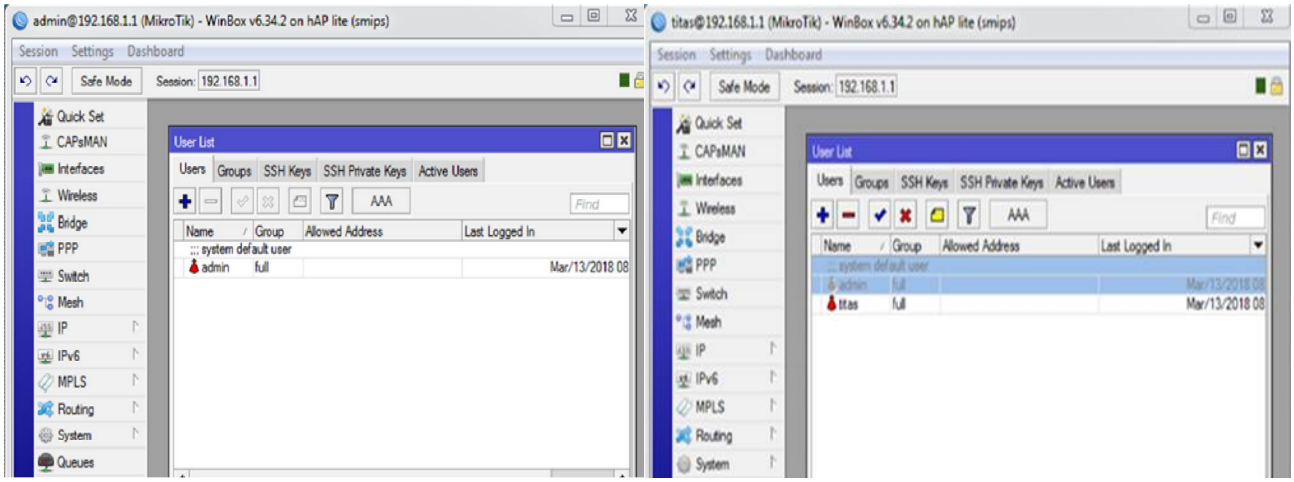

Fig.1. Changing user credentials

B. *WinBox default port:*

Usually we use WinBox application to log in to MikroTik router's admin panel. WinBox runs on default port 8291 [5]. If the default port is changed to a custom port it would require the exact port number to browse the admin panel. It will be a secured way when logging in using IP, username and password.

How to change WinBox default port number? :
Step 1: Log in WinBox
Step 2: Click on 'IP' > 'Services'
Step 3: Click on Name: 'winbox' Port: '8291' and change the port number (we use '8310' as our WinBox port number)

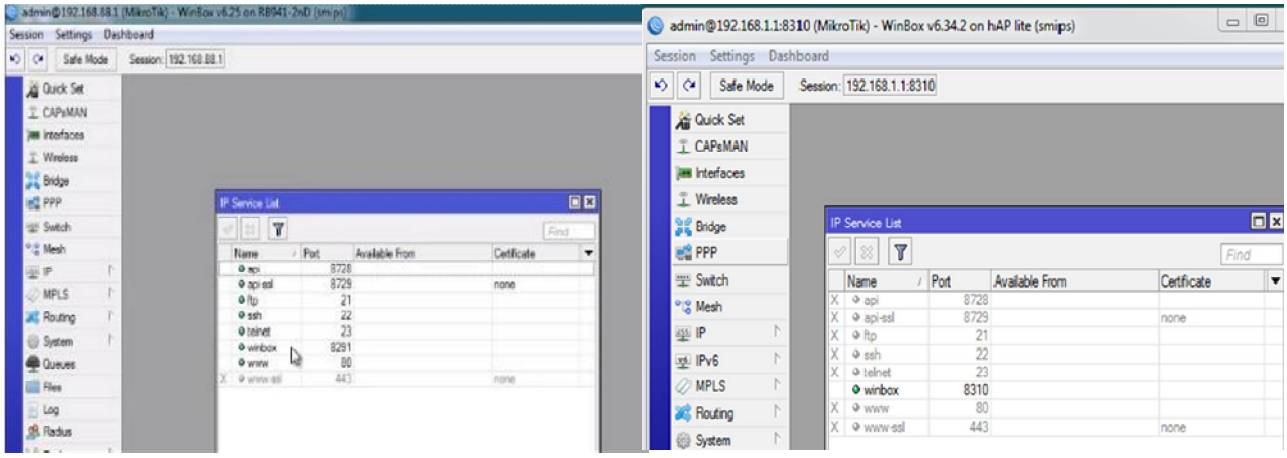

Fig.2. Changing WinBox default port number

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 7, July 2018

C. *MAC-access restriction:*

MikroTikRouter OS has a built-in options for easy management access to network devices through MAC address. But the particular services should be shut down on production networks for security purposes. So we should disable the feature of showing MAC address in order to restrict accessing using MAC.

How we can configure it? :

Step 1: Log in WinBox

Step 2: Click on 'Tools' > 'MAC Server'

Step 3: Select 'WinBox Interfaces' and finally disable 'all'

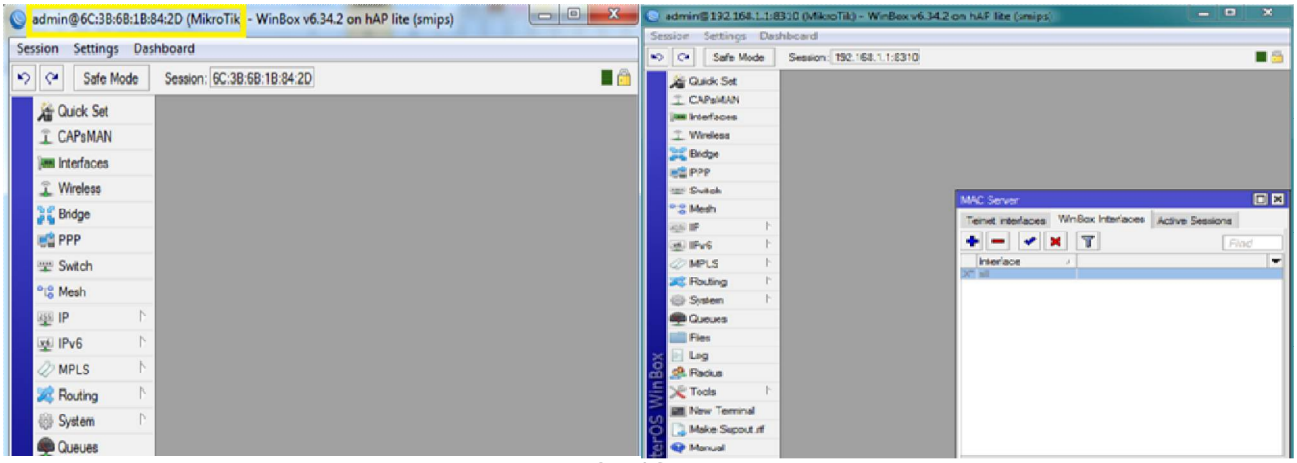

Fig.3. MAC-access restriction

D. *Site restriction:*

MikroTik router can be used to prevent access to select websites if required (i.e. adult sites, social media, entertainment websites etc.).

How to configure it? :

Step 1: Log in WinBox

Step 2: Click on 'IP' > 'Firewall'

Step 3: Select 'Layer7 Protocols', then click '+' to add the necessary sites to restrict, add site name and add the URL address of that desire site in the 'Regexp' box. Here we can add multiple site addresses by using comma (,) (here, we use URL of 'facebook' to restrict)

Step 4: Select 'Filter Rules' and then '+' to add new firewall rule

Step 5: In 'New Firewall Rule' select 'General', add 'Src. Address' (we use '192.168.1.222' as our Src. Address). Then select 'Advanced' to add site name in 'Layer7 Protocol' field (we use 'facebook')

Step 5: After that select 'Action' and choose 'drop' as action

Step 6: Finally click on 'Apply' to apply the configuration

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 7, July 2018

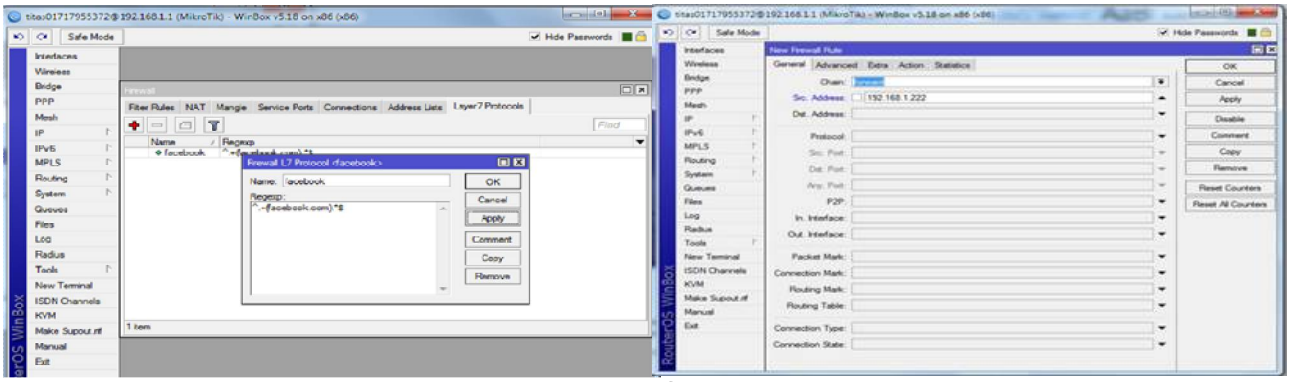

Fig.4.1. Site restriction

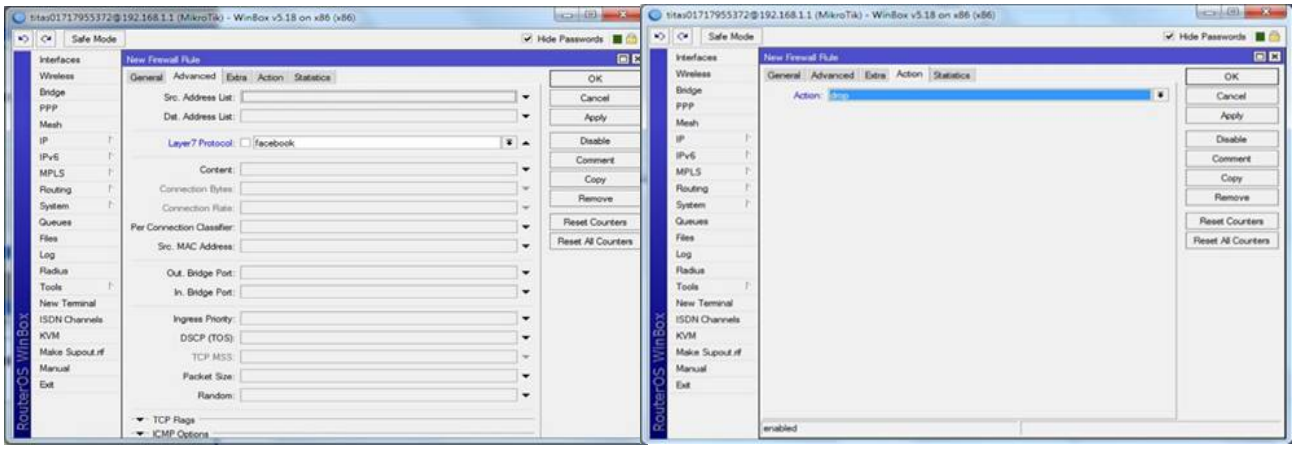

Fig.4.2. Site restriction

Site restriction result:

So that if he/she try to visit Facebook now, he/she can't able to access Facebook.

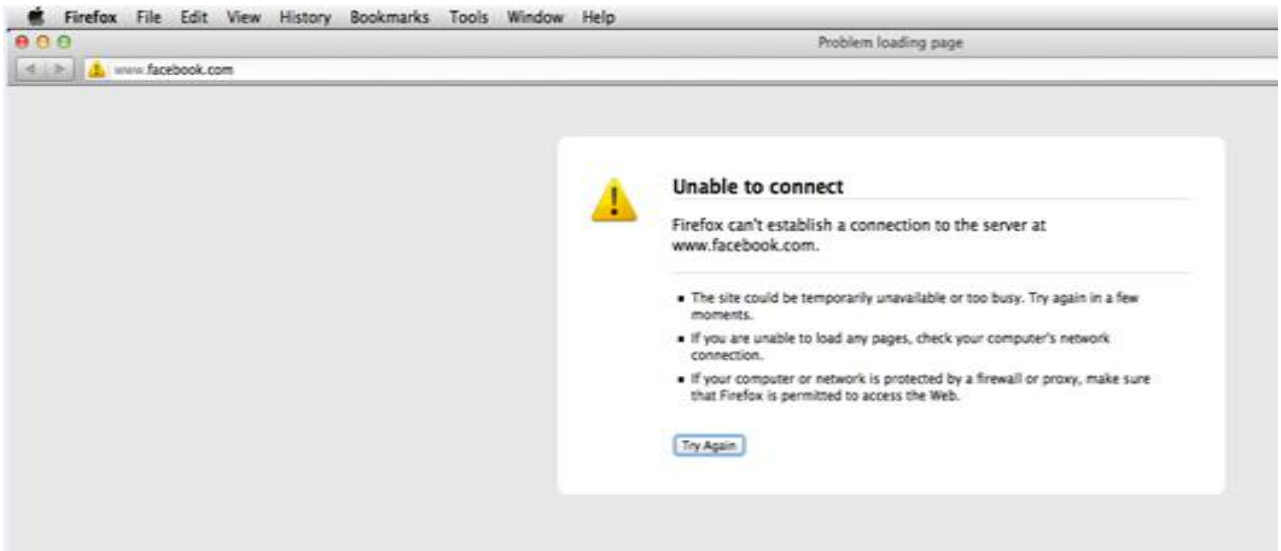

Fig.4.3. Site restriction result

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 7, July 2018

E. *Virus port filtering:*

Firewall filter keep outside threats away from sensitive data available inside the network. Whenever different networks are joined together, there is always a threat that someone from outside of your network will break into your LAN. MikroTik router's firewall easily filter virus ports and can able to drop it.

How to block all the virus ports in MikroTik? :

Step 1: Log in WinBox

Step 2: Click on 'IP' > 'Firewall'

Step 3: Click on 'Filter Rules' and add virus port numbers to drop

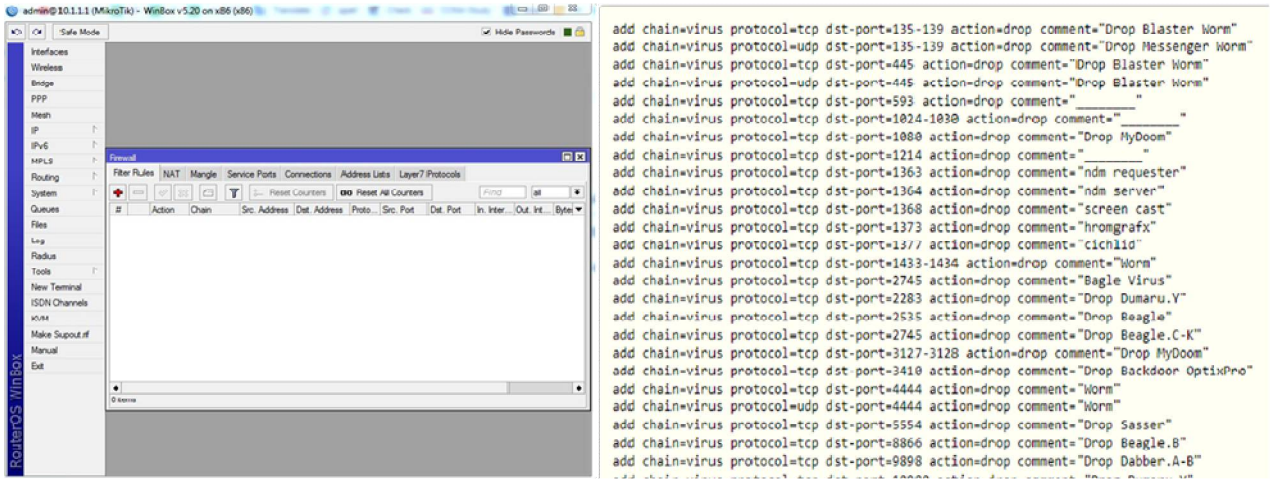

Fig.5. Virus port filtering

F. *Log server:*

MikroTik Router OS is capable of logging various system events and status information. As well, MikroTik router's logging is configured for view who is visiting which website. If anyone tries to visit any unauthorized site then we can easily track it.

How to configure it? :

Step 1: Log in WinBox

Step 2: Click on 'Systems' > 'Logging'

Step 3: Select 'Actions' and add a remote address. Then select 'Rules' and from there choose 'remote' as action

Step 4: Finally select 'Apply' to apply the configuration

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 7, July 2018

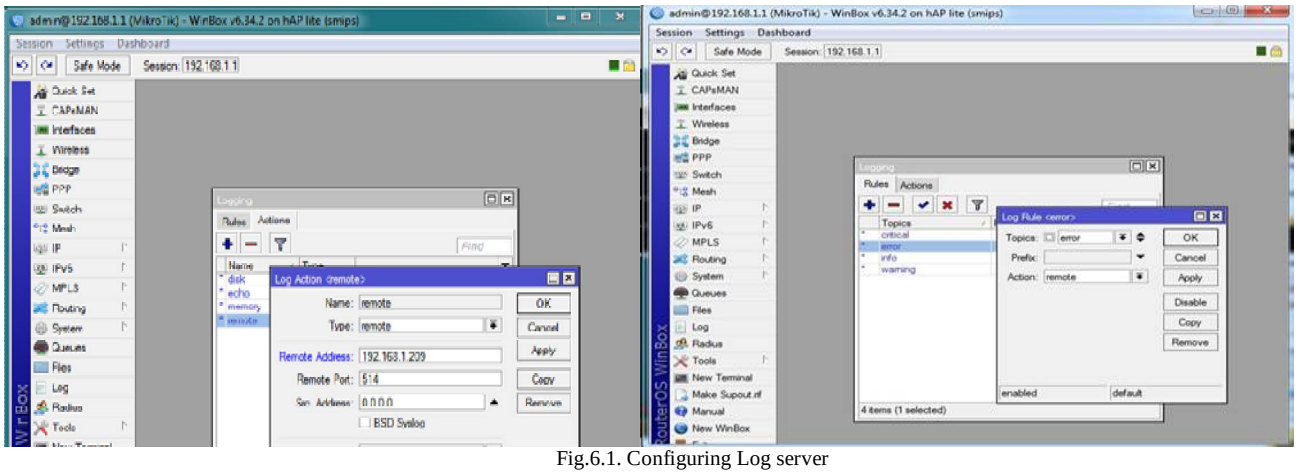

Fig.6.1. Configuring Log server

Log server's output:
Here we use Kiwi Syslog for view purpose.

Fig.6.2. Log server's output

IV. CONCLUSION AND FUTURE WORK

In this paper, we have presented an overview of the existing all basic security scenario of MikroTik router. In a future study we plan to identify advanced security threats and will try to mitigate that threats by analyzing proper actions in order to ensure a total security policy whoever will use this router.

REFERENCES

1. Kim J., Lee K., Lee C.," Design and Implementation of Integrated Security Engine for Secure Networking," In Proceedings International Conference on Advanced Communication Technology, 2004.[Accessed 28th April 2018].
2. Router security supported features. [ONLINE] Available at: https://www.juniper.net/documentation/en_US/junos/topics/concept/junos-software-router-security-supported-features.html [Accessed 4th May 2018].

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 7, July 2018

3. Protecting the network from Web-based service attacks with defense in depth. [ONLINE] Available at: https://searchsecurity.techtarget.com/tip/Protecting-the-network-from-Web-based-service-attacks-with-defense-in-depth [Accessed 11th May 2018].
4. Network Security Concepts and Policies. [ONLINE] Available at: http://www.ciscopress.com/articles/article.asp?p=1998559 [Accessed 12th May 2018].
5. Services, Protocols and Ports. [ONLINE] Available at: https://mikrotik.com/testdocs/ros/2.9/ip/service.php [Accessed 2nd June 2018].