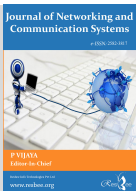
Vol.6 No.3 July 2023

Journal of Networking and Communication Systems

Received 26 April, Revised 29 May, Accepted 07 June



New Approach to Study the Possibilities of VPN Blocking in ISPs

Jouma Ali AlMohamad

Department of Communication Engineering
Faculty of Electrical and Electronic Engineering
Aleppo University, Syria

Abstract: The adoption of VPNs provides steady growth in the past decade because of its increased public awareness of privacy and threads. VPN analysis and blocking are critical in network security due to the urgent need by many companies and government organizations. This helps to secure the user's privacy or Government censorship. Several VPN providers perform streaming unblocking services. VPNs are used for online protection, however, many VPNs do not guarantee privacy and may even compromise user privacy through leakage of traffic flows, data collection and sharing, and so forth. In this paper, we have discussed the mechanism of VPN providers to facilitate access to geo-restrict content, copyrights, and school and work content. We proposed MikroTik Firewall for blocking and the mechanisms to achieve the desired goals, as well as the possibilities of bypassing this ban imposed on VPN networks. A step-by-step guide was provided to block websites such as Facebook. Finally, a practical approach to VPN blocking using MikroTik helped to completely block the network. To conclude, both objectives of this project were fully achieved and the scope of the study was followed thoroughly. Finally, a practical approach to VPN blocking using MikroTik helped to completely block the network.

Keywords: VPN, MikroTik Router, IPsec, WIFI Networks, DPI, Firewall.

Nomenclature

Acronym	Description
ISP	Internet Service Providers
DPI	Deep Packet Inspection
VPN	Virtual Private Networks
RTT	Round Trip Time

1. Introduction

VPN blocking is a technique used to block encrypted protocol communication methods used by VPN systems [17]. It is often used by large organizations such as governments or national corporations, as a tool for computer security or Internet censorship by preventing VPNs from being used to bypass firewall systems [12] Network protection.

VPN access can be blocked in many different ways [18]. Ports used by popular VPN protocols such as PPTP or L2TP, to establish their connections and transmit data are blocked by system administrators to prevent their use on certain networks [19]. Similarly, a website can block access to its content by blocking access from IP addresses known to belong to VPN providers [20]. Some governments are known to block all access to external IP addresses since VPN use can involve connecting to remote hosts that are not operating within the jurisdiction of that government. [1]

As organizations step up their efforts to block VPN access that bypasses their firewalls, VPN providers are using more sophisticated techniques to make their connections less visible [14]. For example, when the Chinese government began using deep packet inspection to identify VPN protocols, Golden Frog began collecting OpenVPN packet metadata for the popular VyprVPN service to avoid detection [2]. For example, Chinese internet users began reporting unstable connections in May 2011 while using VPNs to connect to external websites and services such as the Apple App Store. Universities and companies have begun issuing warnings to stop using tools to circumvent the firewall [15].

In late 2012, companies that provide VPN services claimed that the Great Firewall of China was able to "learn, detect and block" encrypted communication methods used by several different VPN systems [16].In 2017, the government instructed telecom companies in China to ban individuals from using VPNs

https://doi.org/10.46253/jnacs.v6i3.a1

by February 2018. [3]. In Russia in July 2017, the State Duma passed a bill requiring ISPs to block websites that offer VPNs, to prevent the spread of "extremist material" on the Internet. [4] It is unclear exactly how Russia plans to implement its new regulations. Although it appears that both the Federal Security Service (FSB) and ISPs will be tasked with identifying VPNs and cracking down on them.

The issue of banning VPN networks that hide the identity of the real user is a very important issue at various levels, especially for institutions and companies, depending on their respective policies, privacy,and property rights. This research aims to develop

- An in-depth study of the causes of VPN.
- Scenarios and types of blocking methods that are used for various VPNs.
- Implementation of a practical application to block the networks usingthe theMikroTik Router environment.

The proposed method used MikroTik Firewall to block websites such as Facebook and other websites to deny access. The experimental result showed the complete block of the network in the router environment. The organization of this paper is in this order: Section 2 presents the literature review, and Section 3 portrays the research method. The suggested method is explained in section 4. Section 5 covers the Mikrotik firewall rule to block VPN servers section 6 provides the advantages and disadvantages, Section 7 showed the result and finally, Section 7 concludes the paper with future work.

2. Literature Review

In 2022, Tejas Ravi Ghatikar and VemuriAnvesh Sai., [6] have implemented an automatic system to detect the VPN address and deny access cost-effectively. This method was designed to support small-scale websites in achieving high-level security from fraudulent activities. It grants or denies access to users based on IP address and VPN-enabled IP address. Users with VPN were denied access to the website.

In 2021, Fuzi*et al.,* [7] have used an open VPN protocol called Raspberry Pi 3 (RPi3) Model B+. This method includes several phases, such as analysis requirements, design and implementation, testing, and result analysis.SafeSearch was a viable solution for users who want to create a secure connection to another network over the public Internet without paying a premium price for a good VPN service or exposing themselves to targeted advertising when utilizing a free browser-based VPN.

In 2018, Afroz*et al.,* [8] have used a combination of automated page loads, manual checking, TCP traceroute, and stateful HTTP traceroute to explore the phenomenon of websites blocking users from certain regions. The heuristics used for TCP are also applied to compare the HTTP traceroute to the ICMP traceroute. It also reports qualitative evidence that fears of abuse and the costs of serving requests to some regions may play a role in the server-side blocking of regions.

In 2018, Chen, Y. and Yang, D.Y., [9] have presented empirical evidence in providing access to an uncensored Internet leads citizens to acquire politically sensitive information, and the acquisition of politically sensitive information change citizens' beliefs, attitudes, and behaviors.

In 2021, Praveen *et al.,* [10] have executed using Feature Tree and K-means.The traffic flow was first identified by mapping DNS with the TCP/IP computer network stack and considering it as a non-standard traffic flow if domain name information is not available. Once the traffic flow is identified, it is classified and studied by machine learning techniques. The method does not require the network to decrypt or decode any network communication.

In 2019, Farnan, *et al.,* [11] have applied DNS cache snooping to determine the domains people were accessing through VPNs. They explore 3 methods of DNS cache snooping and briefly discuss their strengths and limitations. Using the most reliable of the methods, they performed a DNS cache snooping scan against the DNS servers of several major VPN providers. With this, they discover which domains were actually accessed through VPNs. The first stage of their experiment was run against 1000 popular domains.

In 2016, Fujikawa *et al.,* [12] have implemented network virtualization involves recognizing step-wise increases in RTT caused by intentionally blocking international communication links. This method predicts and avoids intentional blocks or restrictions by using differential calculus of RTT to predict or recognize the onset of the restriction in the early stage, automatically switching to VPN bypass before the serious increase in network latency is experienced by users, and using non-differential threshold value and elapsed time to determine the end of restriction and switch back to the open (ordinary or public) Internet. The method had been validated by quantitative analysis of latency data corresponding to real GS blocks.

In 2014, Wang, *et al.,* [13] have introduced a traffic obfuscation protocol called GoHop, which is an open-source VPN tool with innate traffic obfuscation features. This method involved the collection of two types of traffic, HTTP and SSH, from the client. When collecting data, one piece was collected from the

virtual interface, which was the traffic from and to user applications, and another piece at the physical interface, which was the traffic that can be inspected by the adversary. The collected data was then obfuscated using the pre-shared master key, traffic shaping, and random port communication. Finally, the obfuscated data was then sent to the server, which decrypts the data and sends it to the intended destination.

2.1 Review

Author	Methodology	Advantage	Disadvantage
Tejas Ravi Ghatikar and VemuriAnvesh Sai., [6]	Automated system to detect a VPN address	• Cost-effective • High-level security from unethical activities. • Easy to use and implement	• In-effective for IP spoofing. • Problems in the accuracy and collection of data from IP address tracking.
Fuzi*et al.*, [7]	Raspberry Pi 3 (RPi3) Model B+	• Secure and cost-effective solution. • Shield their browsing activity and encrypt data transmitted over the network.	• Slight latency and bandwidth decline.
Afroz*et al.*, [8]	TCP	• Reduced the number of websites that time-out. • Provided a comprehensive view.	• Lack of information makes it difficult to develop effective counter measures against such blocking.
Chen, Y. and Yang, D.Y., [9]	Empirical evidence	• Provided a systematic and evidence-based approach to studying the impact of Internet censorship on citizens' political attitudes.	• Relied on self-reported data from survey respondents. • Focused only on the short-term effects of exposure to uncensored information.
Praveen *et al.*, [10]	Feature Tree and K-means	• Did not require the network to decrypt or decode any network communication, ensuring privacy and security. • Can detect or block VPN clients in wireless sensor networks. • Classify the traffic flows as normal or VPN traffic flows based on time-related features.	• focused only on detecting or blocking VPN clients and did not address other types of network security threats.
Farnan, *et al.*, [11]	DNS cache snooping	• Provided a technique for discovering the frequency with which domain records were accessed on a DNS server. • Understand the properties of privacy, anonymity, and free communication over the internet that VPNs offer.	• Difficult to determine the queries that were made by users of the VPN.
Fujikawa *et al.*, [12]	Network virtualization	• Suddenly block international communication links. • Restriction in the early stage. • Reasonable cost.	• Effectiveness of the method may depend on the accuracy of the prediction of the onset of the restriction and the timely switching to VPN bypass. • Required some technical expertise to implement and maintain.
Wang, *et al.*, [13]	GoHop	• High level of security against internet censorship and surveillance. • High-bandwidth network throughput. • Easy to use	• Slow down the network due to the additional overhead of obfuscation.

2.2 Challenges

Some of the issues faced by the traditional routing approaches are discussed as follows:

- The Network virtualization was not effective, because of technical expertise to implement and maintain [12].
- The GoHop mechanism showed High level of security, but they slow down the process [13].

The researches face many challenges in methodology, implementation, process time and has to provide long-term solution. So, a reliable, implement friendly, easy to access method was required to block the VPN access.

3. Research Method

3.1 How to make VPN undetectable

VPNs work hard to maintain anonymity every time you go online. Most ISPs, websites, online services, and even governments are actively looking for VPNs and how to block their connections. This can prevent accessing content around the world or even using your VPN for fast and anonymous browsing on public WIFI. But with the right VPN service like NordVPN and by knowing the procedures. It is easy to bypass these barriers without compromising privacy or security[5].

3.2 Reasons to Block VPNs

From copyright to censorship, there are many reasons for websites to block VPNs. VPN bans are even more intense in an area with tough digital surveillance.

Government Censorship: In some regions, governments impose strict censorship on the Internet. They may block websites that do not support the culture and values of their country.So that, the population cannot absorb information that goes against certain values. Even worse, these countries often regulate the use of VPNs, blocking vendor websites and app stores.So,the download of these services is denied.

The clearest example of strict government censorship is in China. Its Great Firewall restricts all kinds of sites including Google, Social media apps, YouTube, and some news websites. China also blocks most VPNs. Other countries with digital restrictions include Turkey, the UAE, and Iran. Many social media and live-streaming websites are blocked in these countries through the use of VPNs.

Finding a VPN is difficultfrom government censorship. However, there are three reliable options:

1. Restrictions by geographical location

Certain websites block their content to certain regions. Many streaming sites only allow access in certain regions. Netflix, BBC iPlayer, Hulu, HBO GO, and ITV Hub are just a few examples of platforms that use these geo-restrictions.

While some sites are exclusive to one region, like Hulu in the US, others like Netflix offer different libraries depending on the location. This is mostly due to broadcast and broadcast licenses. Therefore, the countrythat don't allow will prevented the user from continuing. The websites don't make it easy to get around these geographic barriers, the Netflix proxy error is one of the hardest to defeat.

2. Copyright

Some ISPs limit the use of a VPN to stop copyright infringement. While many VPN users engage in P2P sharing to send and receive files like photos or videos.Others use torrents for illegal hacking as they download copyrighted movies and songs.

Restricting VPN blocks all VPN users, whatever they do online. But if VPN can prevent ISP from knowing that the user is using a VPN, then ISP can't interfere with online activities.

3. School and work restrictions

Most schools and workplaces have restrictions so that the user cannot access certain websites. This may include YouTube and social media sites. To prevent access these sites , the schools and work places can block VPNs from organization's WIFI [5].

3.3 Types of VPN bans

There are many reasons for a VPN to get banned. Fortunately, the most common methods are explained below.

1. IP ban

When the user is connected to VPN, it hides the real IP address and displays the server IP address instead. This means that when the user usesNetflix USthey are connected to a US server, Netflix will see aUSIPaddress. In theory, any geographic restrictions can be easilyovercome. But it isn't simple.

Many sites keep a record of the selected VPN IP addresses. If the user connects to a server that the IP address in not in the list then it will be banned immediately. This makes the VPNs cannot access sites with hard geo-blocks, such as Netflix and BBC iPlayer.

2. Blocking the Gate

Most VPNs use specific ports when they connect to the Internet. These ports are identified by numbers and act as channels through which internet traffic is routed. For example, when using the OpenVPN AMA protocol, your traffic is usually sent to port 1194.

It's easy to block certain types of traffic when that traffic is always using the same port. All the website needs to monitor that port and block the traffic it doesn't need. When it happened, the user cannot access their favorite websites. Port blocking isn't as common as IP blocking, but it's still easy to bypass just by switching ports.

3. DPI

This is a very advanced way to block VPN traffic. Instead of checking the incoming traffic, sites look at the type of traffic instead.

When the user use a VPN, the traffic is anonymous. But some security protocols, such as OpenVPN, use unique cryptographic signatures that can be detected and blocked. OpenVPN is usually blocked because most VPNs use this default protocol, which means that sites are blocking traffic because of the use of VPN. Although no one can actually see your traffic, however they can see that it has been encrypted.

This type of VPN block is particularly difficult to bypass. It's a technique used by the Great Firewall of China to restrict VPN. It is so hard to find a VPN to use in China. But if the VPN allows to change security protocols then it is possible.

4. Suggested Method

This proposed method explain the steps to block VPN access using MikroTik Firewall.

System administrators sometimes create a firewall rule to block unwanted websites. But VPN apps break these firewall rules and allow access to unwanted websites. For example, if Facebook is blocked with MikroTik Firewall and any expert user has installed and enabled VPN apps (such as OpenVPN, Hotspot Shield, ProtonVPN, NordVPN, PureVPN, etc.,)then they can easily access Facebook.

Therefore, system administrators should also block Popular VPN applications so that user cannot use these VPN servers. Blocking VPN apps is not that easy. An expert is needed to block a VPN app.

When any user installs and enables a VPN application, it creates a channel between the user's computer and the VPN server. This server is located somewhere in the world.

The user's computer is now treated as a VPN computer. Therefore, any firewall rule applied to the user's IP no longer works. In VPN enabled computer, if user found the network public IP address with any online tools like whatismyipaddress.com, we will find VPN server IP address instead of our MikroTik public IP address.

Now if the user block this VPN server IP address [Install & Enable VPN Apps & Find VPN Server IP Address Using Online Tools] then no user can connect to VPN server nor user can break the MikroTik Firewall rule.

5. Mikrotik Firewall Rule To Block Vpn Servers

Initially, a firewall rule was created to block the VPN servers that will be present in the group of blacklisted servers. The following steps will show how to block a group of destination servers using MikroTik Firewall Rule.

5.1 How to block a specific site

First, we open the Micro Tik program and select connect, as shown in the following Figure 1.

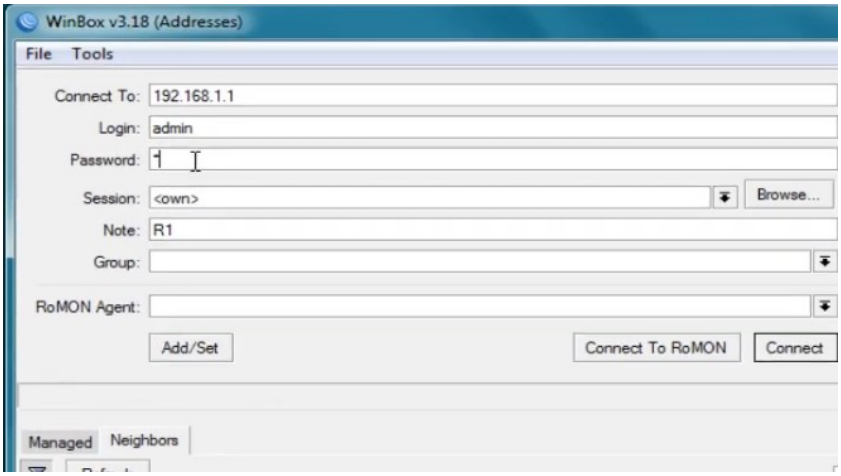


Figure 1.*Mikrotik interface*

Then from the list on the left, Choose IP, then firewall, as shown in the following Figure 2.

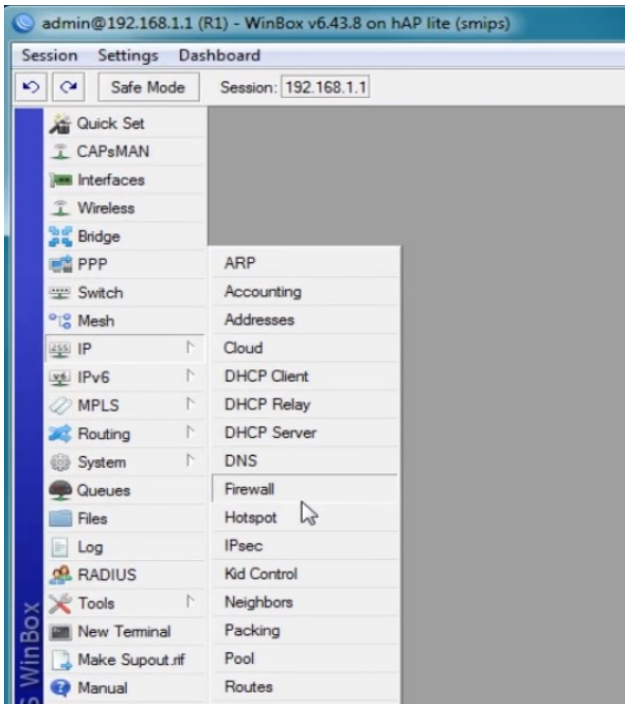


Figure 2. *Selecting a firewall*

Then an interface appears, from which choose Layer7Protocols, then press the + (plus) button to add a site to the ban list, for example, Facebook, as shown in the following Figure 3.

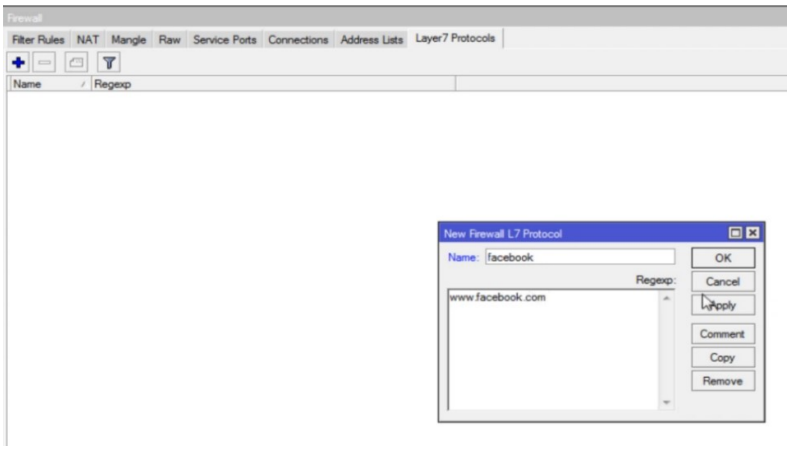


Figure 3. *Adding a site to the ban list*

Then, Press Apply and then OK, then choose Filter Rules from the interface and press the plus button, so an interface appears, from which choose General, and add the Ip of the network that are connected to, as in the following Figure 4.

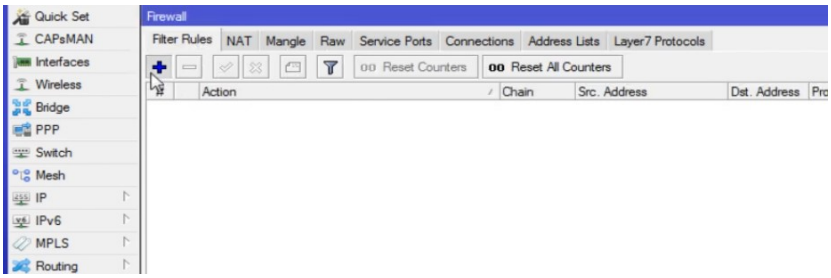


Figure 4.*Adding a network IP*

As the following Figure 5 shows, to find the Ip of the network to which it is connected, Choose from the list on the left IP, then Addresses

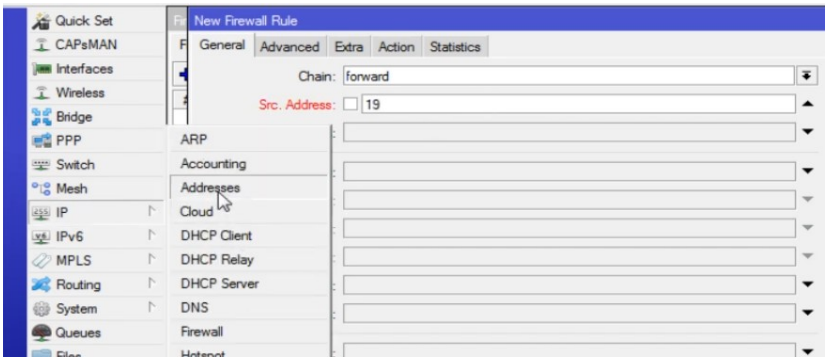


Figure 5.*Selecting a title*

In Figure 6, window contain the network IP.

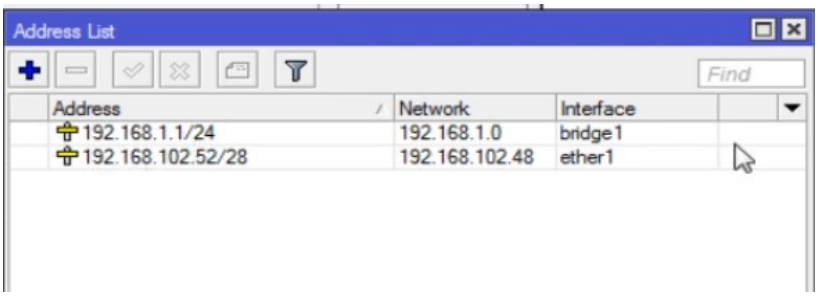


Figure 6.*The appearance of the network IP*

Then enter the IP in the Src.Address field, as shown in the following Figure 7.

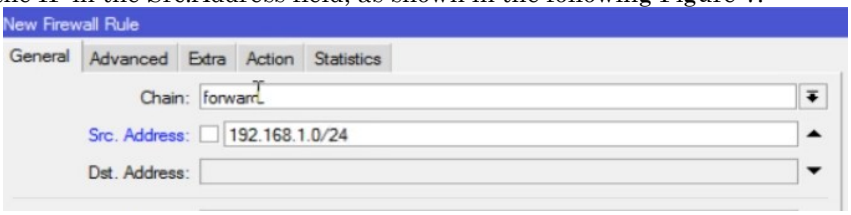


Figure 7.*IP installation*

Then,Choose Advance, and click Layer7Protocol, and choose Facebook, which was saved earlier, as shown in the following Figure.8

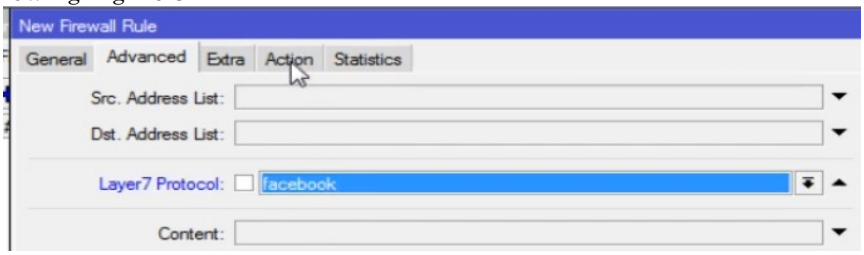


Figure 8.*Choosing a site to block*

Then, Choose Action to choose the event ,when trying to connect to the Facebook server from the browser, and choose the drop event, meaning blocking the site, as in the following Figure 9.

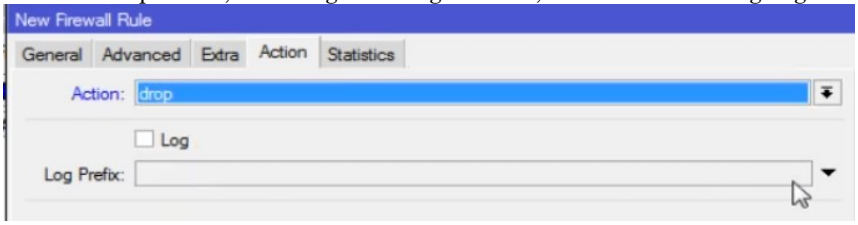


Figure 9.*Blocking a site*

Then click on Apply, then OK, and go to the browser and access the Facebook site, where noticed, it was denied as shown in the following Figure 10.

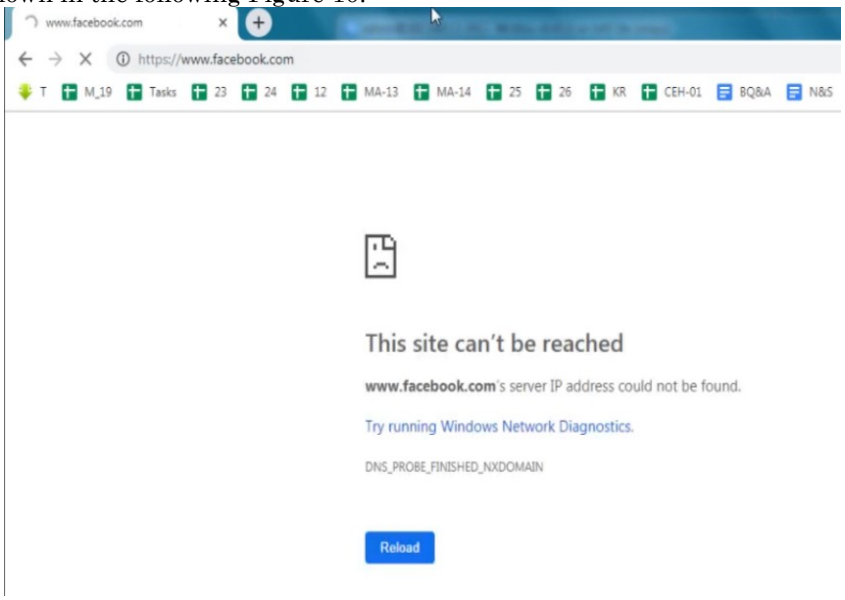


Figure 10.*Confirmation of blocking*

5.2 Block VPN servers

In the search engine, write "what is my Ip" to find the current IP, as in the following Figure 11.

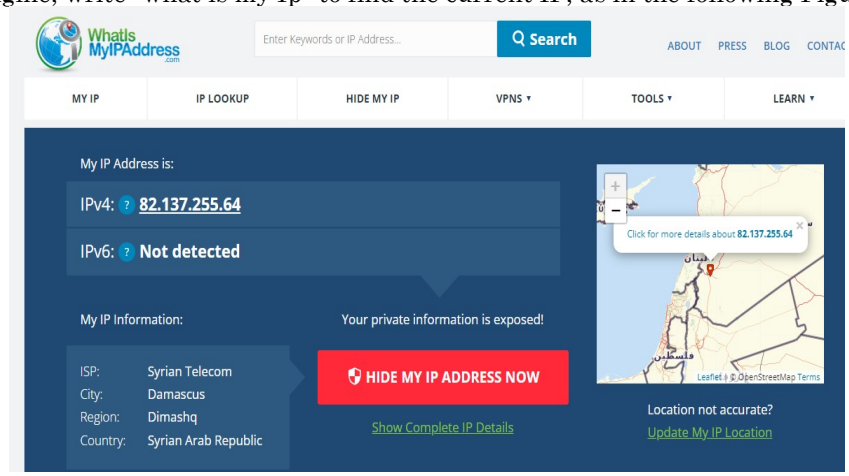


Figure 11.*Knowing the IP*

Then add the VPN to the browser and run it as shown in the following Figure 12.

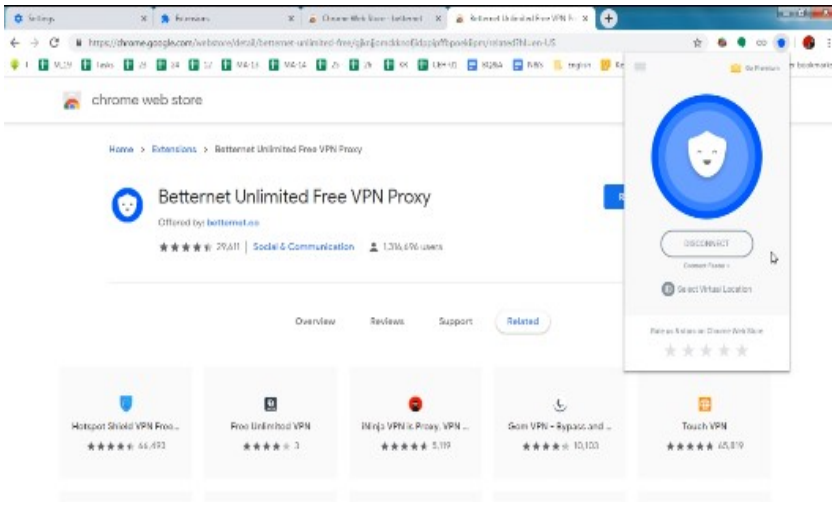


Figure 12.*Adding a VPN*

After turning on theVPN, the Facebook server can be accessed.

Whenre-entering"what is my Ip" to find out the IP of the VPN server, as shown in the following Figure 13.

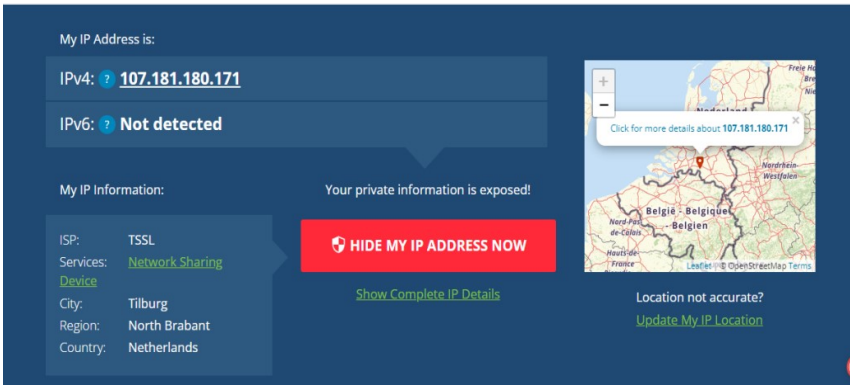


Figure 13.*VPN server identification*

Then the Micro Tik program, close all windows, re-select the IP from the list, then choose Firewall, window appears from that choose Filter Rules, then press the plus button, and a window appears, from that choose Advanced, then add the name needed in the Dst.Address List field, then choose Action, after that choose Drop, finally click on Apply and then OK, as shown in the following Figure 14.

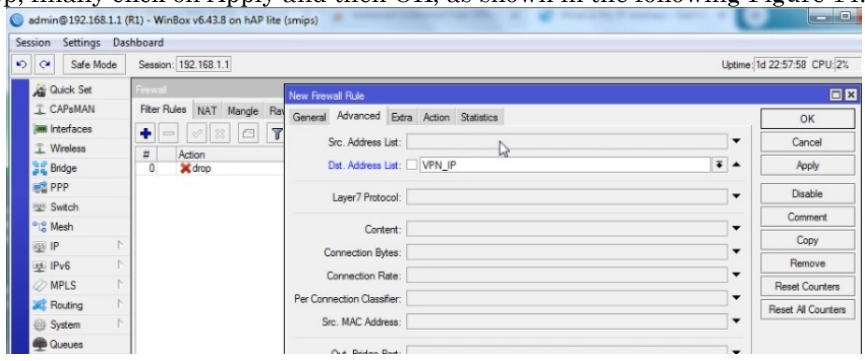


Figure 14.*VPN server blocking implementation*

In the main window, select Address Lists as shown in the following Figure 15.

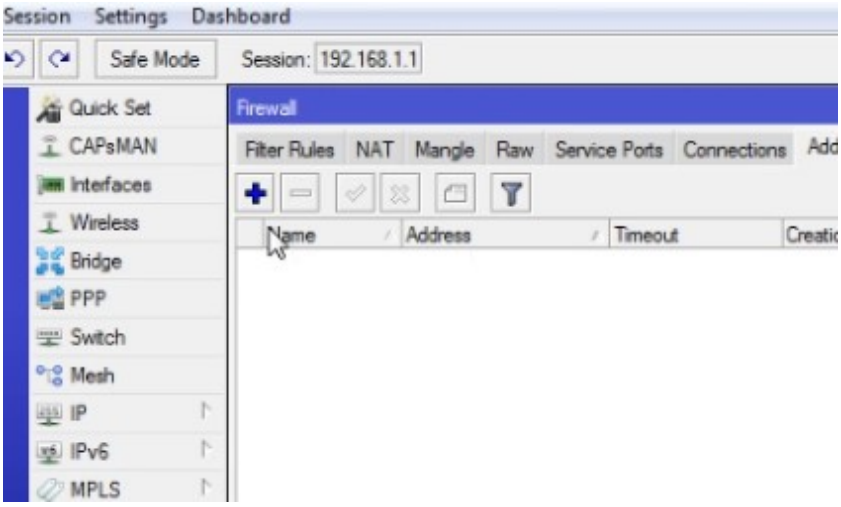


Figure 15.*Choosing a VPN server*

Then press the plus button, a window appears in that choose the Name field the name that was choosen. Add address in the Address field of the IP address of the VPN server that was got when accessing the site what is my Ip as in the following Figure 16.

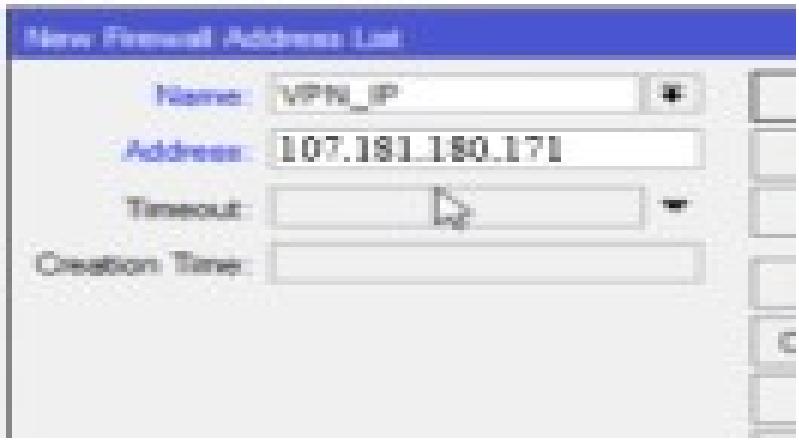


Figure 16.*Blocking the VPN server*

Then click on Apply and then OK, and notice that access to any site on the browser is no longer possible. Here, the address that appears in the previous figure can be changed, and add the new address to the ban list.

6. Advantages and Disadvantages

Advantages

- This method is easy to implement and manage.
- It supports filtering and security of functions using policy.
- It is affordable and can be operated with basic functions.

Disadvantages

- It does not contain a wide range of features.
- It is not efficient for high-traffic environments.

7. Result

The MikroTik Router provided accurate results through configuration and monitoring through the GUI tool -Winbox. The MikroTik firewall was used for its flexibility, cost, user friendly and provide an effective shield from malicious activities and the flow of data. We can monitor connections through

theaddress that are assigned to the router and allow access only to the required host, and TCP ports of the routers.

8. Conclusion and Future Work

The results drawn from this research, and after a practical application to block these networks in the MikroTik Firewall environment, indicate that we can block VPNs, which are one of the types of security attacks (Man in the Middle) and the harm it causes to the individual, society, or the country as a whole. By creating a blacklist, with the need to update this rule periodically, as mentioned above. If it is necessary to use a VPN for some applications, the service provider can subscribe to one of the trusted VPN servers and block the rest.

We recommend developing this research by using other types of firewalls and comparing them to find out the best of these types in terms of dealing with VPN bans.

Compliance with Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows the ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

References

[1] G.D.Gil, A.H.Lashkari,M.S.I.Mamun and A.A.Ghorbani, "Characterization of Encrypted and VPN Traffic using Time-related Features", University of New Brunswick, Canada, 2016.

[2] Al-Fayoumi, M., Al-Fawa'reh, M. and Nashwan, S., "VPN and Non-VPN Network Traffic Classification Using Time-Related".

[3] Kaur, D., "the vital role of VPN in making secure connection over internet world", International Journal of Recent Technology and Engineering (IJRTE) ISSN, pp.2277-3878, 2022.

[4] M. Z. ul Abideen, S. Saleem, and M. Ejaz, "VPN Traffic Detection in SSL-Protected Channel," In Security and Communication Networks, pp. 1–17, 2019.

[5] L. Alchaal, V. Roca, A. El-Sayed, and M. Habert,"A VPRN Solution for Fully Secure and Efficient Group Communications", INRIA, Rh^one Alpes, April 2003.

[6] Ghatikar, T.R. and Sai, V.A., "VPN Detection and Blocking".

[7] Fuzi, M.F.M., Alias, M.R.M., Kaur, N. and Abd Halim, I.H., "SafeSearch: obfuscated VPN server using raspberry Pi for secure network", Journal of Computing Research and Innovation, Vol. 6, no. 4, pp.90-101, 2021.

[8] Afroz, S., Tschantz, M.C., Sajid, S., Qazi, S.A., Javed, M. and Paxson, V., "Exploring server-side blocking of regions". arXiv preprint arXiv:1805.11606, 2018.

[9] Chen, Y. and Yang, D.Y., "The impact of media censorship: Evidence from a field experiment in China", Retrieved, Vol. 24, pp.2021, 2018.

[10] Praveen, S.P., Krishna, T.B.M., Chawla, S.K. and Anuradha, C., "Virtual Private Network Flow Detection in Wireless Sensor Networks Using Machine Learning Techniques", International Journal of Sensors Wireless Communications and Control, Vol. 11, no.7, pp.716-724, 2021.

[11] Farnan, O., Wright, J. and Darer, A., Analysing censorship circumvention with VPNs via DNS cache snooping", In 2019 IEEE Security and Privacy Workshops (SPW),pp. 205-211, 2019.

[12] Fujikawa, H., Damiani, E., Yamamoto, Y., Yamaki, H. and Tsuruta, S., "Network virtualization by differentially switched VPN for stable business communication with offshore computers. Journal of Reliable Intelligent Environments", Vol. 2, pp.119-130, 2016.

[13] Wang, Y., Ji, P., Ye, B., Wang, P., Luo, R. and Yang, H., "GoHop: Personal VPN to defend from censorship", In 16th International Conference on Advanced Communication Technology, pp. 27-33, 2014.

[14] Jingyao, S., Chandel, S., Yunnan, Y., Jingji, Z. and Zhipeng, Z., "Securing a network: how effective using firewalls and VPNs are?", In Advances in Information and Communication: Proceedings of the 2019 Future of Information and Communication Conference (FICC), Vol. 2, pp. 1050-1068,2020.

[15] Jang-Jaccard, J. and Nepal, S., "A survey of emerging threats in cybersecurity",Journal of Computer and System Sciences, Vol. 80, no.5, pp.973-993, 2014.

[16] Chandel, S., Jingji, Z., Yunnan, Y., Jingyao, S. and Zhipeng, Z., "The golden shield project of china: A decade later—an in-depth study of the great firewall", In 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 111-119, 2019.

[17] X. Zhong, I. Jayawardene, G. K. Venayagamoorthy and R. Brooks, "Denial of Service Attack on Tie-Line Bias Control in a Power System With PV Plant," in IEEE Transactions on Emerging Topics in Computational Intelligence, Vol. 1, no. 5, pp. 375-390, 2017.

[18] Song, Y. and Hengartner, U., “Privacyguard: A vpn-based platform to detect information leakage on android devices”, In Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices, pp. 15-26, 2015.

[19] Scott, C., Wolfe, P. and Erwin, M., “Virtual private networks”, O'Reilly Media, Inc.", 1999.

[20]Khan, M.T., DeBlasio, J., Voelker, G.M., Snoeren, A.C., Kanich, C. and Vallina-Rodriguez, N., “An empirical analysis of the commercial vpn ecosystem”, In Proceedings of the Internet Measurement Conference 2018, pp. 443-456, 2018.