International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 06 | June - 2021 ISSN: 2582-3930

Virtual Private Networking Using IKEV2 and WIREGUARD: A Solution for Personalized VPN on the Go

Chinmay Santosh Kumbhare[1], Jay Gopal Agrawal[2], Omkar Vilas Bhujbal[3]

[1, 2, 3]Zeal College of Engineering and Research – Pune, Maharashtra, India

---

Abstract -These days, we're often told that security is a myth. With millions of cases of information stealing and identity theft, targeted advertisements are harassing people too. So, it is more than fair to have a VPN installed in our device. It not only disguises our location, but also provides us with protection from web trackers all over the internet. When you switch it on, a VPN creates an encrypted tunnel between you and a remote server operated by a VPN service. All your internet traffic is routed through this tunnel, so your data is secure from prying eyes along the way. Because your traffic is exiting the VPN server, your true IP address is hidden, masking your identity and location. Normally, the well known VPN service providers charge you a hefty amount for their premium service only to sell your data to external companies in exchange for money. This paper presents a model for self-hosting a VPN that supports connecting via SSH along with DNS Ad-blocking. This extra layer of security ensures that the user's data is not being stolen.

Key Words:cyber security, virtual private network, vpn, internet key exchange protocol, IKEv2, Wireguard

1.INTRODUCTION

Data in the 21st century has become an epitome of controversy due to the countless occurrences of crimes associated with data breaches and data loss. A VPN tunnel is an encrypted link between your computer or mobile device and an outside network. A VPN tunnel short for virtual private network tunnel can provide a way to cloak some of your online activity. How? A VPN tunnel connects your smartphone, laptop, computer, or tablet to another network in which your IP address is hidden and all the data you generate while surfing the web is encrypted.

VPN is not an alien thing for today's internet users. The number of VPN users are increasing every day but a few years back, there were hardly any users of VPN.

Even today, there are many people who aren't familiar with this term. The rising popularity of VPN raises the questions of what is a VPN and whether you should use one.

Apart from security, it has numerous other benefits that are making this service worth using. Here are some of the top reasons people turn to VPNs in their home or business lives. Major requirements are as follows:

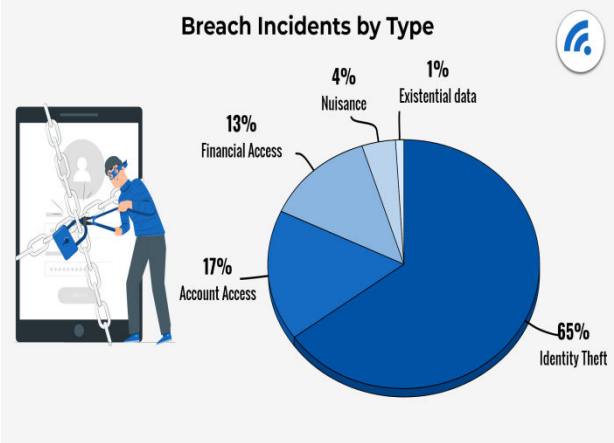

Fig -1: Figure1. Breach Incidents carried out online

1. Safety and Security

The first and the most important reason people use VPN is its safety feature. It provides an encrypted tunnel for transferring data to and from your device and the host site.

2. Anonymity

Another crucial reason that people choose to use a VPN is because it respects and preserves your anonymity. VPN allows its users to explore the internet from different location servers.

3. Breaking Geo-Restrictions

The Internet provides endless sources of entertainment and infotainment but unfortunately, these sources are not accessible for all.

4. Subsidized shopping and travelling

Many online shopping sites have different price lists for customers from different countries. The same is the case with airfares.

5. Using Public Wi-Fi

Public Wi-Fi is mostly free and is easily available but there are several security threats associated with it like data breaches and attacking malware.

2. Motivation

At the first occurrence of an acronym, spell it out followed by the acronym in parentheses, e.g., charge-coupled diode (CCD).

With the surge in data related crimes, orga-nizations and individuals are investing heav-ily in keeping data safe and secure from unwanted parties.

In today's modern and dangerous world, we need to protect our information from theft and from targeted advertising. The main culprits are the big organizations, businesses and government bodies that are prying on your data.

Protection of user's data is the very reason VPN is used but it is also known that many large companies that provide VPN services sell the data of customer to third party for various reasons, so they are protecting users from web trackers, government restrictions and then selling user's information to third party, which makes no sense. So there should be a new approach towards designing the VPN services which holds only one goal and that is of user's safety.

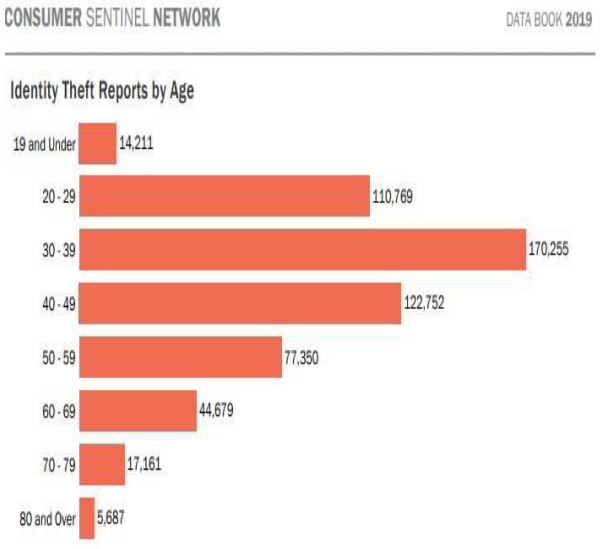

Fig -2: Age-group targeted for maximum financial theft.

3. LTERATURE REVIEW

With the increasing demand for internal network access, virtual private networks built by VPN technology between individuals and enterprises has been very large-scale due to its low deployment cost, flexible management strategy and high security characteristics. Virtual private network is a communication environment. The characteristic of this environment is private. This kind of privacy is virtual, that is to achieve this kind of privatization through the virtual way instead of the physical way. Although the VPN as a data security service by public network is widely used, but the encryption characteristics of traditional network audit equipment related to the lack of support for the commonly used VPN recognition and VPN itself by tunnel transmission caused by the traditional way of network protocol identification to filter illegal VPN traffic, network security will be more difficult to take care of.

Protocol identification system can be divided into the traditional port protocol identification system based on recognition system based on the load and recognition system based on host behavior, the current widely used DPI (Deep packet inspection) technology, using the matching search algorithm of data packet protocol payload in keywords, and then determining the protocol, this method in the application when it is relatively complex, in accordance with the data transmission characteristics are divided into independent data streams, and the matching features can be found in the data stream in series so as to identify the protocol type, and its main process includes traffic sampling, information processing, data analysis. The traditional method is only applicable to follow and be used by the IANA (Internet Assigned Numbers Authority), matching feature provides a specific port and protocol of application layer which is fixed, but some applications are in order to pass through the firewall or bypass the restrictions operating system using nonstandard ports, and DPI technology such as SSH (Secure Shell cannot be detected Vo IP (Skype), Voice over Internet Protocol) encryption technology flow after treatment. With the safety of the VPN tunnel enhanced through the traditional way of screening protocol identification, audit VPN traffic has become more difficult, there is a low accuracy such as protocol identification, DPI scheme is easy to construct malicious packet spoofing, and information complexity and recognition results are often too high, feedback computing system using machine learning algorithms to achieve the small defects. In terms of recognition rate, with the increase of network data transmission speed, the real-time data traffic on the network has increased dramatically. Therefore, it is hard for traditional passive protocol identification to deal with such massive network data on hardware and software.

Nowadays, the Internet connects millions of people around the world and allows for immediate communication and access to a seemingly limitless amount of information. The language of the Internet is Internet Protocol (IP). The IP has proven to be highly efficient, cost-effective, and a flexible communication protocol for local and global communication. However, IP is vulnerable to security risks that are preventing its serious use for business and other purposes involving secure applications. IP Security (IPSec) [l] is a suite of protocols that integrate security into 1P and provide services like data source authentication; data integrity; confidentiality; protection against replay attack; data privacy; access control; and, end-to-end security for IP packets. Security services provided by IPSec, like other cryptographic security services, need to establish shared keys between the source and destination. Since IPSec provides security services in the 1P layer, and these services are transparent from the viewpoint of applications and processes, automatically using the key exchange protocol is vital. Internet Key Exchange (IKE) [Z] is provided as a suitable solution for this requirement. To continue, at first, the original version of IKE and its successors are introduced. Then a proposed protocol is presented that is based on the Diffie-Hellman key exchange.

4. SYSTEM ARCHITECTURE

4.1 IKEv2 Protocol

For VPN encryption, IKE protocol involves the following steps:

1. Initiate connection between client and its kernel.
2. Initial exchange and secure channel establishment.
3. Authenticate the client-side connection and request server.
4. Exchange of pre-shared keys in between client and server.
5. Contact with a server, establish a tunnel.

There are 3 major constraints for the project. They are as follows:

1. IKE_SA_INIT Exchange: It is the initial exchange in which the peers establish a secure channel. After it completes the initial exchange, all further exchanges are encrypted.
2. IKE_AUTH Exchange: After the IKE_SA_INIT exchange is complete, the IKEv2 SA is encrypted; however, the remote peer has not been authenticated. The IKE_AUTH exchange is used to authenticate the remote peer and create the first IPsec SA.
3. CREATE_CHILD_SA Exchange: It serves the same function that the Quick mode exchange does in IKEv1. There are only two packets in this exchange; however, the exchange repeats for every rekey or new SA.

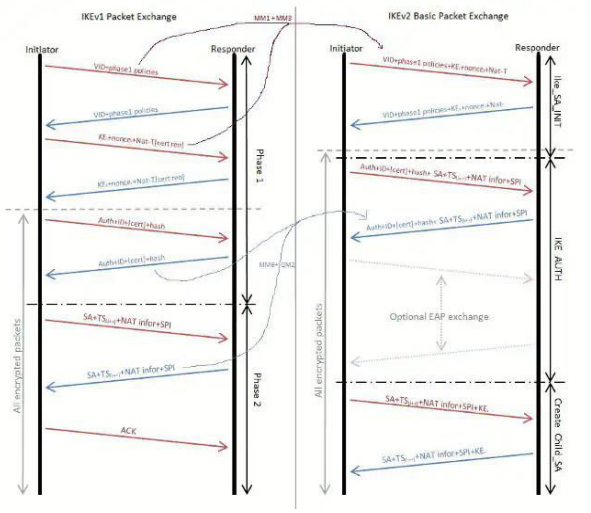

Figure 3: IKE Packet Exchange Diagram

4.2 Wireguard: VPN Tunnel

WireGuard is one of a few VPN protocols in common use today. A VPN protocol defines the rules and specifications of the communication between your local network and the remote network, such as the type of encryption that will be used and how user authentication works.

VPN protocols often have different priorities. For example, the aged PPTP VPN protocol is very fast, but at the cost of being highly insecure. OpenVPN is very secure but can be relatively slow. IKEv2 is designed to work particularly well on mobile devices, where the internet connections may frequently switch and can often drop.

What makes WireGuard different from other protocols?

WireGuard is a simplified VPN protocol. While protocols like OpenVPN have over 400,000 lines of code, WireGuard has only around 4,000 lines. This makes it easier to audit and harder to find flaws to exploit.WireGuard uses the latest encryption protocols (ChaCha20, Curve25519, BLAKE2s, SipHash24, HKDF, etc.), making it arguably more secure than older, more established VPN protocols.

From a user's point of view, the clearest benefit of WireGuard is a faster connection time. WireGuard delivers extremely fast VPN connections that are virtually instantaneous to connect, whereas OpenVPN can take 10 seconds or more to do the same. You should also get a more reliable connection and better battery life when using a WireGuard VPN on a mobile device.

4.3 Sequence Diagram

To get a better insight at what actually is going on, here are the important parameters used:

1. Generate Keys: Since the IKE communication occurs between Kernels, this is a very important prerequisite. All the further communications are terminated if the key generation fails.
    a. Sharing of keys through wireguard: Once step 1 is successfully completed, all our communication occurs through Wireguard.
    b. Private Tunnelling: All the traffic from our device to the cloud server is routed through the wire guard's own private tunnel

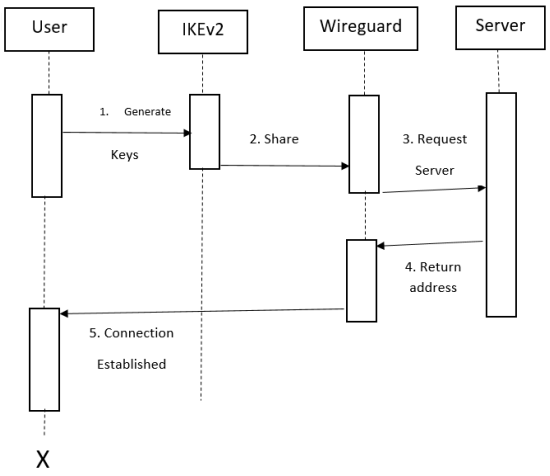

Figure 4: Sequence Diagram

5. CONCLUSIONS

In this project, we are able to use VPN which gives you online privacy and anonymity by creating a private network from the public internet. VPN services establish secure and encrypted connections to provide greater privacy than even a secured Wi-Fi hotspot. In future work, the proposed system can be developed and implemented on a large scale for many users. In the future, we would also increase the bandwidth and the tunnels. This system can be further extended to building a real-time DNS resolver. It can thus keep your searches private and masked from your local ISP.

4.1 Recommendations

Based on the results of the experiments conducted, it can be recommended that one must take the following steps:

1. Always ensure that your VPN is in active state before accessing sensitive data.
2. Cloud hosting always comes with terms and conditions attached. Always keep an eye on the billing cycle.
3. Beware of the red flags that your ISP gives you.
4. Ensure that you use your self-hosted DNS too.

4.2 Future Work

Since a VPN redirects the traffic from ISP's servers into its own, we can enforce some additional encryptions and techniques so that the data cannot be readable by the web crawlers.

Another important aspect that is left uncovered includes the dynamic addition of an IP into the VPN's whitelist(i.e allowed list). Since a VPN is supposed to be a very handy device, all the future implements would include a user-friendly experience.

REFERENCES

[1] Yi Xiaoqing, Wang Ming, (2012), Design of lKEv2 Protocol Based on the PKI/OCSP, 2012 International Conference on Computer Science and Information Processing (CSIP)

[2] IrfaanCoonjah, Pierre Clarel Catherine, K. M. S. Soyjaudah (2018), Design and Implementation of UDP Tunneling-based on OpenSSH VPN.2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)

[3] JINHAI ZHANG, (2018), RESEARCH ON KEY TECHNOLOGY OF VPN PROTOCOL RECOGNITION, 2018 IEEE INTERNATIONAL CONFERENCE OF SAFETY PRODUCE INFORMATIZATION (IICSPI)

[4] Hossein Haddad, Mehdi Berenjkoub, Saeed Gazor, (2004), A PROPOSED PROTOCOL FOR INTERNET KEY EXCHANGE (IKE), Canadian Conference on Electrical and Computer Engineering 2004 (IEEE Cat. No.04CH37513)

[5] M.Lavanya, V.Natarajan, (2017), Certificate-free Collaborative Key Agreement based on IKEv2 for IoT, 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bioinformatics (AEEICB)

[6] Abdullah Alshalan, Sandeep Pisharody, Dijiang Huang, (2015), A Survey Of Mobile VPN Technologies, IEEE Communications Surveys & Tutorials

[7] Chen Fei, Wu Kehe, Chen Wei, Zhang Qianyuan, (2013), The research and implementation of the VPN gateway based on SSL 2013 International Conference on Computational and Information Sciences

[8] Zhu Xiaowei, ZHOU Haigang, Liu lun, (2010), Analysis and Improvement of IKEv2 against Denial of Service Attack,2010 International Conference on Information, Networking and Automation (ICINA)

[9] Ana Kukec, StjepanGroš, Vlado Glavinic´, (2007), Implementation of Certificate Based Authentication in IKEv2 Protocol, 2007 29th International Conference on Information Technology Interfaces

Does a VPN work?https://www.tomsguide.com/features/how-does-a-vpn-work