Common Vulnerabilities Exposed in VPN – A Survey

Rama Bansode¹, Anup Girdhar²
¹Research Scholar in TMV, Pune and Faculty in Modern College of Engg., Pune
²Tilak Maharashtra Vidyapeeth, Pune.
rama.bansode@yahoo.com¹, anupgirdhar@gmail.com²

Abstract. In COVID-19 Pandemic, Internet traffic has been increased by up to 90%. Work-from-home culture is initiated by almost every organization. The technology adapted to access the Enterprises Intranet is VPN (Virtual Private Network). Infrastructure administrators implemented/ updated VPN with the latest versions along with the security scripts to access Intranet. However, the contingencies faced by the organizations are out of their scope. Now VPN security is a big challenge for almost every organization. The Veracity is that no one claims the full prove security system in their Infrastructures. The latest Vulnerabilities have been exposed and indexed in context to VPN Hardware’s/ Software’s/ Configurations and Implementations. In this paper, it has been decided to analyze the exposed VPN vulnerabilities, along with the ongoing issues which have not been listed to date through the survey. The mitigation policies have been proposed based on observations.

Keywords: VPN, CVE, Network Attacks, NVD.

I. Introduction
A virtual private network (VPN) has been used variously. Security experts use VPN for sharing the Intranet services on a public network with authentication and Authorization. However, Cyber Criminals use it for Anonymity and spoofed identity. Now it’s the right time to revamp the Infrastructure Security Policies and prepare all the security checks on every stage of the data filtration, data Preservation, Authentication, and Authorization with the Notifications and preventions using Intrusion detection and prevention systems. However, the VPN is playing a vital role in the updated security systems.

The Availability of VPN.
Depending upon usage, the organizations select various types of Hardware and Software which is dedicated to configuring/ access VPN settings. The mentioned VPN hardware is mostly used for middle and large scale Networks like Cisco RV260, pfsense Firewall VPN device, TP-Link R600VPN.
Router, etc. However, these devices are the hybrid type of devices that carries the support of the next-gen Firewall, etc. Software-based VPN’s are also available for almost all the operating systems as an application (Server and Client Side), where further it has been categorized into two different behaviors of VPN sharing, i.e. First to configure the VPN as an Intranet resource sharing and the other one is to create anonymity on Internet, where the VPN server has been configured somewhere globally on cloud servers and VPN ID’s has been shared via services so that using Vendors preferred client-side App(s) need to be deployed on the clients PC/ any digital gadgets to access provided services etc.

**Process to configure VPN**

According to the usage, there are many different ways to configure the VPN on different operating systems/ Platforms which are as follows:

1. **Configure the VPN as a server**: To share the Intranet services on public networks, the configuration of the server is required. Most of the Organizations use hardware-level VPN for high performance and centralized troubleshooting. However Server-based VPNs are also available like OpenVPN server for Linux OS etc. which is under GPL (General Public License) and almost freely available, Moreover, it is easy to configure and manage as well.

2. **Configure the VPN as a Client**: To connect any client machine with any VPN services, some in build Apps are available in the Operating Systems or available in the OS repositories. These apps are used to access VPN servers for Corporate Infrastructure or any Cloud VPN service Provider to create anonymity to access blocked services at the Enterprises level or even ISP level. Recently Ubuntu releases its latest Desktop edition i.e. “Ubuntu 20.04 LTS” which comes with a pre-deployed VPN named as “WiredGuard VPN” [10].

**Exposed Vulnerabilities in VPN**

The more organizations are dependent on VPN, Similarly, the new vulnerabilities have been exposed. To date in total 479 vulnerabilities have been identified and exposed on the public domain where Top 28 vulnerabilities identified and exposed only in the year 2020 [6]. While surveying the listed vulnerabilities it has been identified that most of the vulnerabilities exist due to the old versions of the VPN, deployed in the Hardware. The Firmware has never been updated due to which many hacking attempts occurred and many organizations become the victim of VPN hacking. Where the impact was like Data Theft, Identity Theft, Cyber Attacks on internal/external Websites/ Networks, Hacking, Introducing Malwares, etc.

**Common Threats and Attacks on VPN**

Due to COVID-19, pandemic Enterprises are now more dependent on the VPN for Work-from-Home Model, where employees can connect as a VPN client to the corporate infrastructure and access internal network services. However, the major threats and attacks have been massively introduced in this pandemic period only. The real fact is that VPN clients can’t always be “trusted,” due to which organization is affected by a large number of data breaches around the globe. As the VPN ports are always open for Clients, it has been exploited by hackers and attackers easily with various attacks.

The few of the common threats and attacks are as follows:

1. **MITM Attacks**: It is known as “Man-in-the-middle” Attack, where hackers take the privilege to exploit from the network connections and try to penetrate between Server and Client communications. They try to exploit variously like from the Coding point of view, Protocols exploits, session hijacking, fuzzing, brute force attacks, Dictionary attacks, decryption of common algorithms, introducing Spywares on the Client machines, etc.

2. **DNS Hijacking**: Most of the organizations are now interested to redirect the end-user traffic via their DNS servers. It helps to filter the real-time content and to identify the behavior of the users.
Mostly Web access Firewall service providers sell their product which is technically based on DNS services. Hackers also try to penetrate the user’s router to reroute the entire network traffic via phished servers/ hackers controlled servers. Were they can easily redirect the legitimate client request to anonymous servers or they may introduce some adware’s or other spyware to hijack clients’ machines so that they can further penetrate the entire internal network using VPN or other proxy servers.

3. **Trojans and Worms**: Trojans are the Client-server architecture based program designed to open the backdoors on the end-user systems connected on the same network and able to prevail, users, their identities, resources, and credentials for hacker’s personal use. Worms are the self-replicated programs designed to infect the shareable resources like multiple drives, network drives, removable drives, and other network resources. It would be more dangerous at the time if the client is also connected to any VPN. Because it is quite easy to infect the entire corporate network by introducing Trojans and worms from the infected VPN client accessing internal network services.

4. **Repeated Login attempts**: This attack is a very common attack on the VPN servers/ routers because of the common software-defined parameters and configurations applied for authentication purposes. Such attacks are also known as Brute force attacks. Hackers try to find out the login behavior based on pre-define parameters and the identified URLs/ Links/ Pre-opened ports and they try to apply fuzzing tools to generate the adaptive authentication credentials.

5. **Legacy Apps**: These apps are such commonly used apps to connect various servers/ network services without any auditing or any version updates like Putty etc. Almost every windows user working on server configurations are much familiar with these apps. However the IT heads are least bother about its security concerns, the version used, downloaded from legitimate sites, or is that opening any backdoors and given privileges to their parent organizations or hackers or so. This is one of the most common routes to hijack VPNs and able to misuse any resource accessed by the end-user of an organization.

Further, this paper has been classified into various sections. In the next section, there is a brief detail about the literature review, which is very helpful to identify the previous research work done by other researchers, and also helps to identify the research Gap. The further section uses to mention the observations identified while proceeding with the survey and express the identified common issues in the form of stats and other relevant information. The next section explains the updation and the ramifications of the security policies to mitigate risk to access VPNs from the latest threats and vulnerabilities.

### II. Literature Review

This section introduces the literature review in the area of the opted domain of VPN security which is as follows:

(Singh et al.) [8], proposed an approach of VPN security. The proposed solution was applicable to the security of the user's data traveled in the form of a VPN Header. Moreover, it extends the encryption algorithm complexity to enhance the VPN security of the client’s privacy while working on the Internet.

(Baek et al.;) [1], identify the limitations in the IP-VPN standard of IETF for global policy management. They proposed a new policy-based hybrid management architecture implemented on a centralized global management server for IP-VPN services. A global policy has been classified into various levels of the administrator's authority. Finally, to demonstrate the functionality they propose a prototype of a VPN service management system.

(Gokulakrishnan et al.,) [4], explains the various VPN security protocols for tunneling. The list of the explained protocols are as follows:
• Internet Protocol Security (IPSec)
• Layer 2 Tunneling Protocol (L2TP)
• Point-to-Point Tunneling Protocol (PPTP)

The mentioned VPN tunneling protocol is used to protect the data transmission from MITM attacks however various new attacks have already been introduced and also need to revamp the security protocols accordingly.

(Mrs. Bansode et al.,) [2], explains the IPv6 security considerations, for VPN communications. It has been explained that the IPv6 carries inbuilt IPsec security tunneling which is comparatively better than IPv4 Implementation.

(Rahimi et al.,) [7], introduce the probabilistic model for the purpose to evaluate and quantify the security of VPN configurations. Depending upon the various VPN configurations the simulated model is used to investigate parameters and trade-offs. Recommendations are provided in industrial control environments based on experimental results on secured VPN deployments.

In this section, most of the Authors explained the requirement of VPN in the organizations where it has also been defined as the existing technologies of VPN security using secure tunnels, etc. However, the research gap identified in the reviewed papers is as mentioned. (Singh et al.,)[8] Explains the VPN security implementation by changing the packet header, however, the spoofed packet header can be sniffed and tampered easily. (Baek et al.,)[1] Proposed the centralized global management server which authenticates users based on the policy framework, however, the MITM DOD/DDOS and session hijacking types of attacks are possible on Centralize servers. It’s good that the traffic is now centralized but at the same time, it is difficult to handle authentic traffic. On real-time bases.

Gokulakrishnan et al., [4] listed the VPN security tunneling protocols and the various methods introduced to mitigate the MITM and other attacks. However due to rapid changes in the technologies the attackers also have versatile methods to bypass the security systems. Mrs. Bansode et al., [2] explains another adaptive method of VPN security by using IPv6 instead of IPv4. The concept is good however the limitations of acceptance are still there due to compliance issues of the old hardware, Software, and Firmwares. Rahimi et at., [7], introduce the probabilistic model to quantify the configuration of the VPN security. However, the model was based on customizing requirements related to the Industrial control environment only which is not the standardized adaptive system.

III. Methodology
Based on the identified research gap, it has been noticed that to date the VPN security is in the grey area. The Implementations are based on the common steps with a basic level of security configurations available on related websites. Admins follow those instructions only and still they are not confident about the Security contingencies. The major gap identified that very rare research papers discuss the exposed vulnerabilities and its mitigations policies in the existing configured infrastructures. Based on the qualitative research methodology [3], initially, the process begins with a survey to collect the relevant data of exposed vulnerabilities connected to VPN securities. In the next step, it has been categorized year wise and generates informative graphs for upcoming analysis purposes. Further, it has been categorized into the common issues based on the Attacks compliant to the configured systems. The reports are based in the form of tables and charts. Further, it extends to propose the mitigation policies in general for benefit of the society. At the end of this paper, it concluded with the outcome of the entire process along with its future scope.

IV. Observations
Based on the survey, initially collected all the details about commonly exposed vulnerabilities – CVE [6] and categorized annually. It represents the present scenario of the impact generated by the attacks on VPN securities.

| Year wise details | CVE’s in Total | Top 5 CVE |
|-------------------|----------------|-----------|
| 2020 – till (24th Aug. 2020) | 28 | CVE-2020-6760, CVE-2020-5893, CVE-2020- |
Another analytical result is based on the common issues exposed to the existing Infrastructures in the year 2020 to date.

Identified Artifacts are as follows:

| Issue Id. | Identified Common Issues in | Impact | Total Exposed Vulnerabilities as per Issues identified in- 2020 |
|-----------|-----------------------------|--------|---------------------------------------------------------------|
| ID1       | Software Versions           | Allow remote attackers to cause a denial of service/reset Devices | 1 |
| ID2       | Software Versions           | Client responds to authentication requests over HTTP/ Unauthorized Access/ arbitrary File Deletion/ Effects to Client OS/ Remote execution | 5 |
| ID3       | Hardware Firmware           | Authenticated to remote command execution/ code execution/ Web based code execution/ arbitrary Code execution/ Authentication Bypass/ Failure | 10 |
| ID4       | Hardware Models/ Services    | Allow remote attackers to cause a denial of service/reset Devices/ Restart Devices/ Unstable/ Reload/ Memory overflow / System Crashes/ | 6 |
| ID5       | Hardware based Services     | Allow an authenticated, local attacker to overwrite VPN profiles/ disconnect legitimate IPsec VPN sessions/ Digital Signature bypass/ Access protected Resources/ Session Hijacking/ LFI | 6 |

Total CVE: In the year 2020 – till 24/ Aug./ 2020 28

Table 2: Categorize Identified Issues with Impact on exposed CV in the year 2020

In Total VPN – CVE’s according to the NVD[5]: 479.
Table 3: List of CVE, categorized with Issue ID in the Year 2020

| S.no | CVE            | Issues Identified in                                                                 | Issue ID |
|------|----------------|--------------------------------------------------------------------------------------|----------|
| 1    | CVE-2020-6760  | Schmid ZI 620 V400 VPN 090 routers                                                  | ID3      |
| 2    | CVE-2020-5893  | BIG-IP Edge Client, versions 7.1.5-7.1.8                                              | ID2      |
| 3    | CVE-2020-5739  | Grandstream GXP1600 series firmware 1.0.4.152                                       | ID3      |
| 4    | CVE-2020-5548  | Yamaha LTE VoIP Router                                                                | ID4      |
| 5    | CVE-2020-5180  | Viscosity 1.8.2 on Windows and macOS                                                  | ID2      |
| 6    | CVE-2020-3435  | (IPC) channel of Cisco AnyConnect Secure Mobility Client for Windows                 | ID5      |
| 7    | CVE-2020-3398  | (BGP) Multicast VPN (MVPN) implementation of Cisco NX-OS Software                    | ID4      |
| 8    | CVE-2020-3397  | (BGP) Multicast VPN (MVPN) implementation of Cisco NX-OS Software                    | ID1      |
| 9    | CVE-2020-3358  | (SSL) VPN feature for Cisco Small Business RV VPN Routers                            | ID4      |
| 10   | CVE-2020-3357  | (SSL) VPN feature of Cisco Small Business Routers                                    | ID3      |
| 11   | CVE-2020-3331  | Web-based management interface of Cisco Wireless VPN Routers                          | ID3      |
| 12   | CVE-2020-3330  | Cisco Small Business, VPN Firewall Routers                                           | ID3      |
| 13   | CVE-2020-3310  | XML parser code of Cisco Firepower Device Manager                                     | ID4      |
| 14   | CVE-2020-3220  | Hardware crypto driver of Cisco IOS XE Software                                       | ID5      |
| 15   | CVE-2020-3189  | VPN System Logging functionality for Cisco Firepower Threat Defense (FTD) Software    | ID4      |
| 16   | CVE-2020-3146  | Web-based management interface of the Cisco VPN Firewall                              | ID3      |
| 17   | CVE-2020-3145  | Web-based management interface of the Cisco VPN Firewall                              | ID3      |
| 18   | CVE-2020-3144  | Web-based management interface of the Cisco VPN Firewall                              | ID3      |
| 19   | CVE-2020-3125  | Kerberos authentication feature of Cisco Adaptive Security Appliance (ASA) Software    | ID4      |
| 20   | CVE-2020-25043 | Kaspersky VPN Secure Connection prior to 5.0                                          | ID2      |
| 21   | CVE-2020-2021  | improper verification of signatures in PAN-OS SAML                                     | ID5      |
| 22   | CVE-2020-2005  | (XSS) vulnerability exists when visiting malicious websites with the Palo Alto - VPN  | ID5      |
| 23   | CVE-2020-1987  | Vulnerability in the logging component of Palo Alto                                  | ID5      |
| 24   | CVE-2020-1631  | Vulnerability in the HTTP/HTTPS service used by J-Web                                | ID5      |
| 25   | CVE-2020-15467 | Cohesive Networks vns3:vpn appliances before version 4.11.1                           | ID3      |
| 26   | CVE-2020-13417 | Privilege issue was discovered in Aviatrix VPN Client before 2.10.7                   | ID2      |
| 27   | CVE-2020-12828 | AnchorFree VPN SDK before 1.3.3.218                                                   | ID2      |
| 28   | CVE-2020-12812 | Authentication vulnerability in SSL VPN in FortiOS 6.4.0, 6.2.0 to 6.2.3, 6.0.9        | ID3      |

Based on the Analysis, It has been identified that the Firmware of mostly used VPN Hardware is vulnerable at a high scale.

Other listed Vulnerabilities also placed more impact on the VPN Routers/ Firewall/ other Hardware’s.

V. Mitigation Policies
According to the analytical results, the proposed mitigation policies are as follows:
• Update VPN hardware’s with the latest Firmware’s.
• Update VPN hardware’s with the latest versions of required services and Security Patches.
• Block all those services which are not in use.
• Maintain the proper logs for analysis purposes.
• Update software versions for client access.
• In case the client has the older version of any software connecting to the VPN, then in such a scenario either block the client or notify them for contingencies.
• Implement VPN infrastructure on IPv6 if possible instead of IPv4
• Strongly recommendation to apply 2 step Verification model for User Authentication.
• Monitor Network Bandwidth, Network packet transmission, with the connection status.
• Analyze client’s behavior based on various parameters like Duration, Accessed Hosts, Flow of data transmissions, IP Geo Location, etc.
• Implement updated secured tunnels and their protocols only for data transmissions.
• Maintain sessions with TLS encryption.

VI. Conclusion:
VPN networks are at high risk. Hackers are continuously identifying CVE and apply Auxiliaries/payloads to exploit the entire network. Admin awareness and proper timely auditing of the entire infrastructure is highly recommended to mitigate risk factors from various contingencies. Based on the exposed common vulnerabilities, it has been focused to categorize identified common issues and its impacts. Moreover, the results have been analyzed on the latest vulnerabilities exposed in the year 2020 till 24th Aug. 2020. Further various Mitigation policies and recommended based on the analyzed facts.

VII. Future Scope:
This analytical survey can be extended to various other factors as well. However, I am sure it is helpful to all the IT admins who configured VPN and share their Intranet/ Internal Networks to remote users. The real-time challenges are high, and difficult to mitigate, however, based on identified problems the further incident handling and mitigation of Zero-day attacks are possible via Machine Learning/ AI algorithms.

References
[1] Baek, Seung-Jin and Jeong, Moon-sang and Park, Jong-Tae.(1999). ‘Policy-based Hybrid Management Architecture for IP-based VPN’, [online] KNOM Review, 2(2) pp. 22-30, Available at: <http://www.knom.or.kr/knom-review/v2n2/jtpark.pdf>, [Accessed 24, Aug. 2020]
[2] Bansode, Rama and Girdhar, Dr. Anup. (2017). ‘IPV6 Security Considerations’, Cyber Times International Journal of Technology and Management, [online] New Delhi, India. 10(1), pp. 22-26. Available at: <http://journal.cybertimes.in/?q=Vol10_A_P4> [Accessed 24, Aug. 2020]
[3] Bhandari, Pritha. (2020). ‘What is Qualitative Research?scribbr.com’, [online] Available at: <https://www.scribbr.com/methodology/qualitative-research/> [Accessed 25, Aug. 2020]
[4] Gokulakrishnan, Jayanthi and Bai, Dr. V. Thulas. (2014). ‘A Survey Report on VPN Security & its Technologies’. Indian Journal of Computer Science and Engineering (IJCSE). ISSN: 0976-5166, 5(4) - Aug-Sep 2014, pp. 135-139.
[5] NIST. (2020). ‘NVD – Home, nvd.nist.gov’. [online] National Institute of Standards and Technology, US. Available at: <https://nvd.nist.gov/> [Accessed 23, Aug. 2020]
[6] NVD. (2020). ‘CVE – Search results - VPN’, [online] Available at: <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=vpn> [Accessed 24, Aug. 2020]
[7] Rahimi, Sanaz and Zargham, Mehdi. (2011). ‘Security Analysis of VPN Configurations in Industrial Control Environments’, [online] Chapter6, pp. 73-88, Available at: <http://dl.ifip.org/db/conf/ifip11-10/iccip2011/RahimiZ11.pdf> [Accessed 24, Aug. 2020]
[8] Singh, Kuwar Kuldeep Veer Vikram and Gupta, Himanshu. (2016). ‘A NEW APPROACH FOR THE SECURITY OF VPN’. [online] ACM, ISBN 978-1-4503-3962, Udaipur India. Available at: <https://www.researchgate.net/publication/307090754_A_New_Approach_for_the_Security_of_VPN> [Accessed 24, Aug. 2020]
[9] Wikipedia. (2020). ‘Virtual Private Network’, [online] Available at:<https://en.wikipedia.org/wiki/Virtual_private_network> [Accessed 23, Aug. 2020],
[10] ZDnet. (2020). ‘Ubuntu 20.04 arrives with Linux 5.4 kernel and WireGaurdVPN’, [online] Available at: <https://www.zdnet.com/article/ubuntu-20-04-arrives-with-linux-5-4-kernel-and-wireguard-
WireGuard: The new, simplified wildly, statement 2C%20Wire
Guard%20creator%20Jason%20A.> [Accessed 23, Aug. 2020].