VIRTUAL PRIVATE NETWORKS (VPN)

Group members:

Mohammed Hadad 2240328

Abdullah Alansari 2240003

basm alahmadi 2240107

Abstract

OpenVPN is an open-source VPN solution that tunnels traffic through the transport layer using TCP or UDP protocols. It employs a virtual network interface to capture and encrypt/decrypt traffic, utilizing the OpenSSL library for robust encryption like AES and Blowfish. The VPN technology provides portability and security for transmitting data over public networks, consolidating multiple communications services onto a common high-capacity platform. Firewalling is essential for securing the individual network "bubbles" interconnected by the VPN, acting as the primary line of defense. However, potential issues like insecure tunneling protocols, developer misconfigurations, and DNS/IPv6 leaks can undermine user privacy and security when using VPN apps.

Introduction

VPN innovation permits the creation of virtual private systems over open foundation just like the web. This gives movability, security, and security compared to physical private systems. The key drivers for VPNs are the financial matters of organizing - VPNs permit numerous administrations to share a high-capacity arrange, amortizing the settled costs.

Firewalling is fundamental for VPN security, as each taking part organize must be separated and secured. Firewalls frame the essential line of defense, controlling which ports and activity can stream between the "bubbles" made by the VPN.

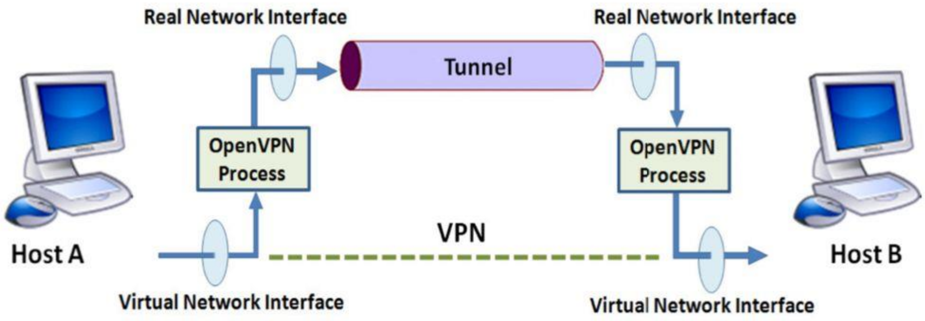
Be that as it may, VPN conventions and usage points of interest can make vulnerabilities. Uncertain tunneling conventions, designer botches, and ignored highlights like IPv6 and DNS can weaken the protection and security that VPNs are implied to supply. Cautious investigation of VPN app behavior is required to distinguish and relieve such dangers.

Concept of VPN

Concept of VPN Technology VPN technology is the condensation for Virtual Private Network fashion, which isn't the factual network generally used by people, it only has certain functions of the private network. Through the data processing of packaging and encryption, VPN technology can realize the complete of data transmission in public network, at the same time enjoying the stability and security of private network system(2). The practical operation of VPN technology should have the following characteristics 1) the specific of portability and profitable operation during the use of public network; characteristics of privacy and security.

OpenVPN

OpenVPN is a free and open source user space VPN solution that tunnels traffic through the transport layer, encapsulating and transferring data using the TCP or UDP protocols.It employs a virtual network interface (VNI) to capture incoming traffic before encryption and send outgoing traffic after decryption.The OpenSSL cryptographic library handles security in Open VPN, providing robust encryption over Secure Socket Layer (SSL) using popular algorithms such as Advanced Encryption (AES), Blowfish, or Triple DES. The OpenVPN employs a mode known as Cipher Block Chaining (CBC), which makes the cipher text of the current block dependent on the cipher text of the preceding block.This prevents an attacker from identifying patterns between blocks containing identical plaintext messages and changing one or more of them.



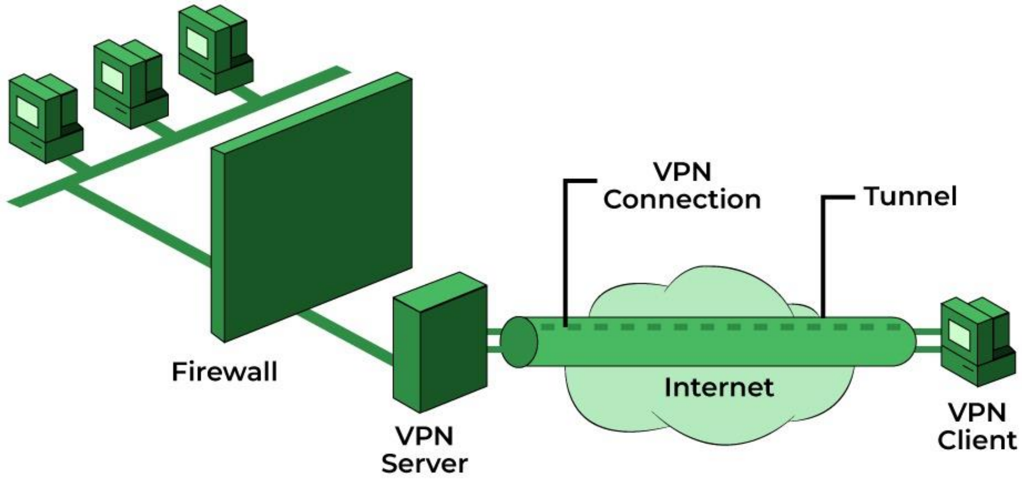
Use of Firewalling in a VPN

Since a VPN interconnects multiple disconnected networks over public infrastructure like the internet, it is essential to protect these individual networks using firewalls. Imagine each .network participating in the VPN as a separate bubble, with its own connections and users

To secure these bubbles, a protective firewall is needed around each one to prevent unauthorized access. The concept is to treat the networks as isolated, with the system administrator opening specific ports on the packet filtering router to allow the encrypted VPN traffic to flow between the bubbles. This sets up a private and secure communication .channel between the sites, based on the cryptographic techniques used in the VPN

The VPN software provides the security and application-level routing, making the interconnected networks appear as a single logical network to users at both ends. Firewall techniques form the primary line of defense in a VPN implementation, and must be properly .developed and tested before the full benefits of the VPN can be realized

Even if the VPN software or hardware has built-in firewalling capabilities, it is still prudent to follow additional security guidelines for the network to stay on the safe side.



Network Virtualization Solution

There are several provocations for erecting VPN’s, but a common thread in each is that they all partake the demand to “ virtualize ” some portion of an association’s dispatches – in other words, make some portion(or maybe all) of the dispatches basically “ unnoticeable ” to external spectators, while taking advantage of the edge of a common dispatches structure. The base provocation for VPN's falsehoods in the economics of dispatches. Dispatches systems moment generally parade the characteristic of a high fixed- cost element, and lower variable cost factors which vary with the transport capacity, or bandwidth, of the system. Within this profitable terrain, it's generally financially seductive to rush a number of separate dispatches services onto a common high capacity dispatches platform, allowing the high fixed- cost factors associated with the platform to be amortized over a larger number of guests. Consequently, a collection of virtual networks enforced on a single common physical dispatches factory is cheaper to operate than the original collection of lower physically separate dispatches shops, each servicing a single network customer

VPN Protocols and Business Leaks

VPN Protocols and Business Leaks
immaculately, the business encouraged through the VPN lair
must be opaque to an in- path bystander(e.g., Internet service
.provider, marketable Wi-Fi APs and surveillance agencies)
still, there's a wide range of tunneling protocols, each with diverse security covenants, that can be exploited by app inventors to further business out of the device from secure IPSec
.coverts to introductory TCP coverts without any encryption
In addition to insecure tunneling protocols, developer induced misconfigurations and crimes may also
undermine stoner’s sequestration and security. VPN app inventors must explicitly forward IPv6 business and give the
.DNS settings at the time of creating the virtual interface programmatically
still, DNS and IPv6 business may not be encouraged through the virtual interface(95), If not
.done precisely

.In particular, DNS leakage can reveal stoner’s networking exertion and interests
The VPN API also allows app inventors to overwrite stoner’s
.DNS determinedness with one of their choice
All these vestiges can come a serious detriment for druggies trying to circumvent surveillance or seeking
online obscurity by using VPN apps. To probe those pivotal aspects of
VPN apps, we run a script that performs machined HTTP requests(both over IPv4 and IPv6) as well as DNS
,lookups to our binary- mound garçon under our control. In this section
we dissect the pcaps captured by our in- path WiFi AP
to probe the presence of coverts without encryption in
the wild(i.e., we consider a lair perpetration as unencrypted if the cargo of our custom HTTP requests is seen
in the clear by our WiFi AP) and to identify implicit IPv6
and DNS leaks. We work the reciprocal features
handed by a pcap parser(40) and Bro’s comprehensive
protocol analyzers(which give support to identify some
tunneling technologies)(94) to check in detail the business
collected for each app.

Conclusion

VPN technology provides a valuable solution for secure and private data transmission over public networks. But its effective implementation requires a holistic approach that addresses both the technical capabilities of the VPN solution and the security practices around its deployment and use. Ongoing vigilance is needed to mitigate emerging threats and vulnerabilities that can compromise the privacy and security promised by VPNs.

References

https://arxiv.org/pdf/1201.0428

https://ojs.s-p.sg/index.php/met/article/view/327

https://books.google.com.sa/books?hl=ar&lr=&id=OuFQ3t7eF4IC&oi=fnd&pg=PR9&dq=Virtual+Private+Networks%C2%A0(VPN)research&ots=hhjVzzCK5F&sig=isNLLqRzfWReL3VwnMjzAPaAOBE&redir_esc=y#v=onepage&q=Virtual%20Private%20Networks%C2%A0(VPN)research&f=false

http://sol.te.net.ua/www/nanog/vpn.pdf

https://dl.acm.org/doi/pdf/10.1145/2987443.2987471