Compare and Contrast b/w Firewall & VPN

Research By: XYZ

Abstract

The research evaluates technical aspects of differences between the security integrating technologies i.e. VPN and Firewall, All the contents embedded within this research are based on the updated advances of technology which rightly explains the job, methodology, and responsibility of the subjected technologies. The content is elaborated with graphical data which gives a pictorial representation of the working scenario of each technology.

Writings

Comparison between VPN & Firewall:

Structural & Functional Contrasts

VPN or virtual private network and firewall are the two forms of security against networking threat. Besides the infrastructure design and methodology of these two network securities The key point which identifies the basic difference between a VPN and firewall is, a virtual private network is a ***'service'***, whereas firewall is an ***'integrated system'***. When the term service comes in view then it means that it is related to a particular operation or set of operations which are specified to perform a certain task. On the other end, an integrated system is a facility or tool which comes in the embedded form within your computer system.

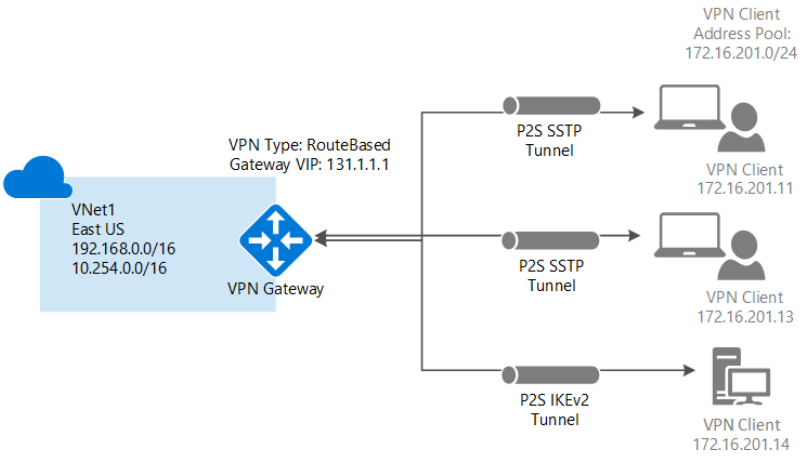
VPN (Virtual Private Network):

The virtual private network is a combination of three words which describes its purpose and functionality scope, i.e. virtual which means in the Internet world, private which means it is personally owned, and network which means it lets you keeping and maintaining connections within secure boundaries. Internet is an open-source platform which does not provide specific privacy at the global end. VPN is more related to making your network private or unknown to the world with a particular IP mapping strategy. The concept of VPN is more dominated with ***'personalizing***' rather providing security.

Functional Structure of VPN:

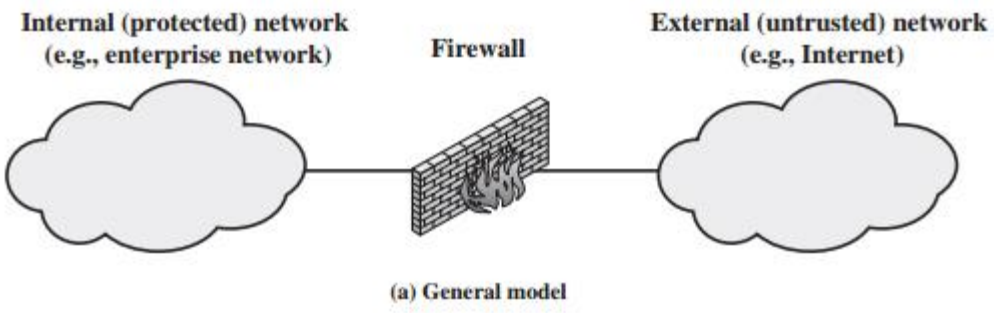
In the context of term personalizing, the virtual private network provides specific tunneling, which encapsulate a network from being identified with its original identity. This may lead to the discussion to legality of VPN, yet the usage of this service is rendered in particular for keeping an IP address veiled against making an open-source access platform. Data transmitting with VPN services are also taken via tunneling process. This means that the

data packets within a network are encapsulated, and packed in a new packet with placing a new header which gives them a new recognition with hiding the previous address. The new header contains routing data which helps in traversing a public network before it reaches its destination. It is all taken via a logical path which is named as ***'tunnel'***. As soon as the encapsulated packet is reached at the end point of the tunnel it is decapsulated, and moved to reach its final destination. The end-points of the tunnel require encapsulated protocols for the recognition of the data packet. This process is taken at any one of the OSI layers, data-link layer or the network layer. Protocols used for this specific purpose are L2TP, PPTP, IPsec, and SSL. (Region, 2008)



Firewall:

A firewall is an integrated system facility which works as a filter to allow or disallow certain IP packets on the basis of their recognition. Firewall processing is more like packet filtering process, which accepts authentic recognized packets while rejects the unauthentic and spam IP packets. However, there are different kinds of firewalls which work according to their methodologies with specifying every filtered packet for accessing the system. According to the particular type of firewall, it works by assessing protocol headers of data packets, the payload of these data packets, or the specific network pattern generated by the sequential arrangement of data packets.



(Mercury.Webster.Edu, 2019)

Functional Structure of Firewall:

The function of the firewall identifies point-to-point encryption, which works as an obstacle to filter out unauthorized accessibility. With this single point security integration, a system becomes completely secure from being damaged with vulnerable attacks, spams, security threats, and other potential dangers. Firewalls works according to its specified types. For a basic overview there are three commonly used types of firewalls:

- Packet Filtering Firewalls: This firewall function is carried with filtering the unknown or security threatened data packets. The filtering capability is based on individual packet assessment which means it allows or denies packets on the basis of individual packet headers.
- Stateful Firewalls: This firewall is deterministic about the state of connection which is established with data packets interactions. It collects data packets and decides after accomplishing a stateful connection. The acceptance or rejection is applied after the complete collection as the rules are applied.
- Application firewall: It is an advanced form of firewall, which considers proxy based, application or services, based filtering. It has a set of rules which specifies certain services or applications to be accepted or rejected. (Anicas, 2015)

References:

(n.d.). *http://mercury.webster.edu/aleshunas/COSC%205130/Chapter-22.pdf*.

Anicas, M. (2015, August). What is a firewall and how does it work.

Mercury.Webster.Edu. (2019). http://mercury.webster.edu/aleshunas/COSC%205130/Chapter-22.pdf.

Region, T. G. (2008, Febraury). VPN Security.

Writingsol.c