International Journal of Advance Research in Science and Engineering
Vol. No.9, Issue No. 10, October 2020
www.ijarse.com
IJARSE
ISSN 2319 - 8354

SOFTWARE-DEFINED PERIMETER (SDP): THE NEXT-GENERATION SECURE VPN SOLUTION BUILT FOR FUTURE NETWORKS

A. SHAJI GEORGE[1], BASHIRU AREMU [2]

1, Post-Doctoral Researcher,Department of Information and Communication Technology,Crown University, Int'l. Chartered Inc. (CUICI) Argentina Campus, South America.

2, Vice Chancellor,Crown University, Int'l. Chartered Inc. (CUICI) Argentina Campus, South America.

E-mail: [1]drashajigeorge@gmail.com

ABSTRACT

In a world in which traditional network limits have ceased to exist, Virtual Private Network is demonstrating their era. Conventional Virtual Private Network was invented for more than two decades, in a period when every enterprise apps have been hosted in local data centers and nearly all people have been working on-premises.VPN provides secure, encrypted tunnels for communications and data. The new solution, or what is commonly called the next-generation Virtual Private Network is necessary to allow remote access to modern-day spread across enterprise networks. In enterprise access, requirements are becoming ever more complex because of applications dynamics, cloud adoption as well as mergers. To understand the intricacy, technical professionals must explore Software Defined Perimeter a brand-new technology whose power lies in enabling access to enterprise applications. The growth in the development and adoption of innovative technologies, architectures, as well as ideas such as cloud computing, Software Defined Network, during recent years, has resulted in a new array of security and privacy challenges as well as concerns. These challenges or concerns consist of proper authentication, data privacy, access control, as well as data integrity, among other things. Software-Defined Perimeter has been suggested as a security paradigm structure to protect modern-day networks in a dynamic way. This research paper analyzes Software Defined Perimeter as a convincing alternative to conventional Virtual Private Networks (VPN) which enables the organization to regulate remote access to all users, scale them more efficiently, and decrease the possible risk of attacks.

Keywords:Software Defined Perimeter(SDP),Virtual Private Network(VPN), Firewall,Zero Trust Network (ZTN),Cloud Solutions,

INTRODUCTION

This research paper describes the software defined perimeter (SDP) security structure and how it could be usedfor secured VPN and to safeguard infrastructure from network-based attacks. The principle of the traditional enterprise network design is to build an internal network split from the external world by a fixed perimeter which consists of a set of firewall functions which prevent external users from coming in although allow internal users to go outside. Traditional fixed perimeters permitted internal services to stay secure from outside threats for a few years because of the strong yet simple qualities of blocking visibility and accessibility from the external perimeter to internal infrastructure. However, the traditional permanent perimeter pattern is quickly becoming outdated due to Bring Your Own Device as well as phishing attacks providing unreliable admittance inside the perimeter as well as the SaaS and IaaS altering the location of the perimeter. In cloud computing, constructing such a perimeter is a challenge because of a broader and likely unknown boundary of various overlay networks of cloud-based services, resources, and appliances communicating with one another. To resolve this challenge, the SDP suggested by the Cloud Security Alliance can be used to create an easily managed secure perimeter used for cloud-connected services, resources as well as devices. Thus far, a Software-defined perimeter has been proven to be a powerful protection against network attacks in accordance with simulated trials and security challenges, hackathons performed by Cloud Security Alliance.

SDP deals with these problems by providing application holders the power to deploy perimeters that maintain the value of invisibility of the traditional model and unavailability to outsiders, however, they can be installed wherever on the internet, into the cloud, at the hosting center, at the private enterprise network, or through any or all of these locations. Standard security tools are brought together by the software defined perimeter including PKI, SAML, IPsec, TLS, , and standards, and ideas like federation, device attestation, as well as geo-location to facilitate the ability to connect from any device to any possible infrastructure. Connectivity in a software defined perimeter will be based upon a want to know model, wherever device stance and identity will be authenticated prior to access to application infrastructure has been granted. Application

infrastructure is essentially black, a DoD term which means that the infrastructure will not be able to be detected, with no visible DNS info or else IP addresses. Software Defined Perimeter mitigates the most frequent network-based attacks, comprising denial of service, server scanning, man-in-the-middle, OS and application vulnerability exploits, SQL injection, password cracking, XSS, pass-the-ticket, CSRF, pass-the-hash, etc., From an end-point perspective, the application for Software defined perimeter utilizes the lightweight access protocol to provide support for deployment on the mobile applications, networked sensors, as well as application servers. In this paper, we will introduce the Software defined perimeter and also talk about its security functions and components, comprising zero visibility, mutual transport layer security, single packet authorization, dynamic firewalls and application binding, device validation, etc., which are behind the successful protection of Software Defined Perimeter and a possible solution for securing information contained in the cloud.

SUMMARY OF VIRTUAL PRIVATE NETWORK

Through the development of the network economy, companies are becoming more widely distributed, business partners continue to increase, and staff members are becoming more mobile. A company, thus, must connect its corporate headquarters and branches with the assistance of carrier's networks in order to form an enterprise network. Consequently, mobile employees can easily access the enterprise network outside the company. A VPN is set up over public networks through Internet Service Providers (ISPs) as well as Network Service Providers (NSPs) to encounter enterprises' necessary conditions for network flexibility, economy, security, and scalability. The virtual private network uses different tunneling technologies in order to encapsulate virtual private network packets in tunnels as well as to transparently transmit the packets via dedicated channels established on virtual private network backbone networks. The packets, thus, are transparently transmitted through the tunnel. The tunneling technology utilizes a protocol to encapsulate packets of a different protocol. Packets of an encapsulation protocol may also be encapsulated or transmitted by a different protocol.

ADVANTAGES AND DISADVANTAGES OF PRESENT GENERATION OF VPN

Present generation virtual private network (VPNs) has been working for two decades to make the ability to access resources remotely simpler and more secure. People can now access resources

from outside their existing networks. Virtual private network (VPNs) work to transmit your entire network traffic to a separate network. This enables you to access resources that are not available locally. They also offer characteristics such as enhanced security via encryption, restricted profiled based access, as well as visibility and monitoring. At the same moment, the emphasis of the present generation of virtual private networks continues upon safeguarding resources behind, whatever has been proven to be, an ineffectual network perimeter. That's why the time has come for a more cloud friendly alternative that accounts meant for the necessity for internal security within equally a network as well as the cloud instead of relying upon a firewall to protect a network perimeter because it can lead to vulnerabilities.

ABOUT NEXT GENERATION VPN

A Next-Generation Virtual Private Network (VPN) represents an evolution of both network architecture as well as virtual private network technology that offers a better degree of control, and therefore enhanced security, in access both to the cloud as well as centralized network resources or else a hybrid of both. In much the same way as with Zero Trust, those things which will put Next Generation virtual private network (VPNs) aside from present or traditional virtual private network technology are the following: i)They are going to default deny access or grant zero trust for all users. ii)They shall pursue a least-privilege access model, just granting users and devices the ability to access the applications, services, as well as data that are absolutely essential to their function within the organization instead of complete access to the network as a whole, similar to current virtual private network technology.

Few of the needs of the technology itself will also include: i)Data in transit: Encryption of the data shall be necessary because it is transmitted from the remote user device to either a centralized network or to the cloud environment. ii)Device compliance: The device itself will be necessary to comply with an array of standards for the protection of any data that is stored or accessed by them. iii)Verification and authorization: Specific authentication of the user, the device, as well as access privileges will be necessary to obtain access to each individual application as well as service. Iv)Auditing: A complete audit trail of not just virtual private

network logins, but what applications or services they were being used to access will be needed also.

THE BENEFITS OF SOFTWARE DEFINED PERIMETER – NEXT GENERATION VPN

Software Defined Perimeter (SDP) is a method of cybersecurity based upon the Zero Trust Model. Software defined perimeter operates to give the same customer experience to people who are on-premises or outside a network's perimeter whilst providing access to just the resources customers need. This capability to deliver a similar experience indicates that users don't have to remember to connect the way they normally would with a present generation VPN.

THE BENEFITS OF SDP – NEXT GENERATION VPN INCLUDE THE FOLLOWING
Offers a Zero Trust/least privilege model—authorize then connect
Mutual TLS utilizing a provided PKI
Integrates with your existing Identity Access Mechanism (SAML/AD/LDAP)
Micro-segmentation, a tunnel of one
Ensures that users can only access specific resources through Policy-based configuration
Ports are not open for public snooping or hacking
Consistent user experience on-premise or off
Additional hardware or network integration is not required
Lightweight client needs no end-user configuration
Additional security without significantly more experience
Control access whether applications are in the cloud or on-premise
Provides additional protection without additional throughput degradation

THE NECESSITY OF MOVING TO NEXT GENERATION VPNs

Let us take a step back for a time and find out why the industry is shifting in this direction, as well as what is increasing the necessity for the Next Generation VPNs. Several of the common issues or questions which come up now, which cannot be resolved by VPN technology the way it is, involve: i)How can you safely share data with third parties as well as contractors and also avoid losing data or compromises. ii)How can you secure remote and mobile employees. iii) How can you provide truly customer-friendly remote-access. iv)How can you give secure,

scalable communications to the thousands of remote IoT devices. v)How can you safely connect data centers as well as public and private cloud-based resources. vi) How can you provide a secure connection to a hybrid cloud infrastructure. For now, we might have a workaround a solution to the above use instances, but then there is not a solution which really examines all the boxes to produce a great solution. Traditional virtual private network technology makes it easier to provide secure communications from a remote site to the central server, but then it does not provide the granular level of access control as well as support for the substantial usage of cloud applications organizations have relied on.

The factors influencing the necessity for next-generation VPN in the case of specific to enterprise organizations:

i)Applications as well as workloads have already been moving progressively more to the cloud (e.g. PaaS, IaaS, SaaS).

ii)Enhanced risk exposure owing to the use of cloud-based services.

iii)Unlimited access to cloud storage and workloads poses a serious threat.

iv)A mobile staff requires remote access service is a requirement instead of a "good to have."

v)Public, Private, and hybrid clouds are all distributing enterprise data.

vi)Internal security threats are on the increase and securing inner critical resources from on-premises users and remote employees become more and more important.

vii)IP connected devices are currently being installed in astonishing numbers.

viii)Legacy or insecure infrastructures are becoming more and more connected to the internet, particularly IoT devices.

ix)Companies must also deal with the dangerous proposition of offering access to a diverse list of contractors, partners, customers, suppliers, and developers. Therefore, partner identity management, as well as more granular access control for the third-party is necessary.

x)A shortage of IT, security talent, and experience, particularly in the areas of automation as well as managed services, is pushing a necessity for simpler technology.

xi)Cyber-attacks, foreign exploitation, malware, and IP Theft are on the rise, significantly influencing the security of remote access.

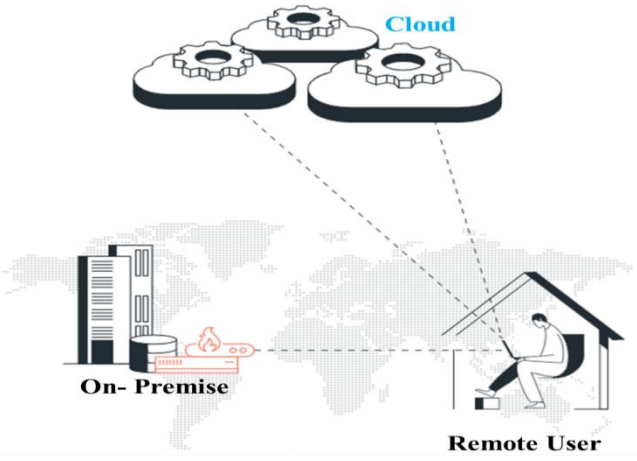
International Journal of Advance Research in Science and Engineering
Vol. No.9, Issue No. 10, October 2020
www.ijarse.com
IJARSE
ISSN 2319 - 8354

ABOUT SOFTWARE DEFINED PERIMETER (SDP)

An SDP is a method to hide Internet-connected infrastructures such as routers, servers, etc. So as to ensure that external parties and attackers will not be able to see it, whether or not it is hosted on-premises or else in the cloud. The objective of the Software-Defined Perimeter method is to base the network perimeter on top of software rather than hardware. A company which uses a Software-Defined Perimeter is basically covering a veil of invisibility over its servers and other infrastructure so as to ensure that no one will be able to view it from the outside though, legitimate users will still be able to access the infrastructure.An SDP shapes the virtual environment boundary around the company's assets on the network layer, but not the application layer. This distinguishes it from other access-based controls that restrict user rights although enable wide network access. Another important difference lies in the fact that Software-Defined Perimeter authenticates devices and user identity. Cloud Security Alliance originally developed the Software-Defined Perimeter concept.

Software-defined perimeter (SDP) is also known as Zero Trust Network Access (ZTNA), represents a new method for securing remote access to corporate applications together on-premises as well as in the cloud. Software defined perimeter is an integral part of Gartner's Secure Access Service Edge (SASE) framework. Companies have for a long time depended on VPNs to connect mobile or else, remote users, to the applications as well as other network resources. However, traditional virtual private networks are badly suited for the transition to the cloud as well as to the rise in work from home customers. Virtual Private Networks depend on appliances, like firewalls or Virtual Private Network concentrators, pushing remote users' traffic to particular physical sites. Architecture enhances latency and generates capacity constraints. When the connection is established through a virtual private network, users will be trusted along with access to all resources on a network, raising the risk of malware spread and data breach. Furthermore, to get to the VPN gateways, users will have to depend on the unpredictable. In summary, legacy virtual private network architectures reveal the enterprise to attacks as well as has an adverse effect on the user experience, particularly when gaining access to cloud applications.

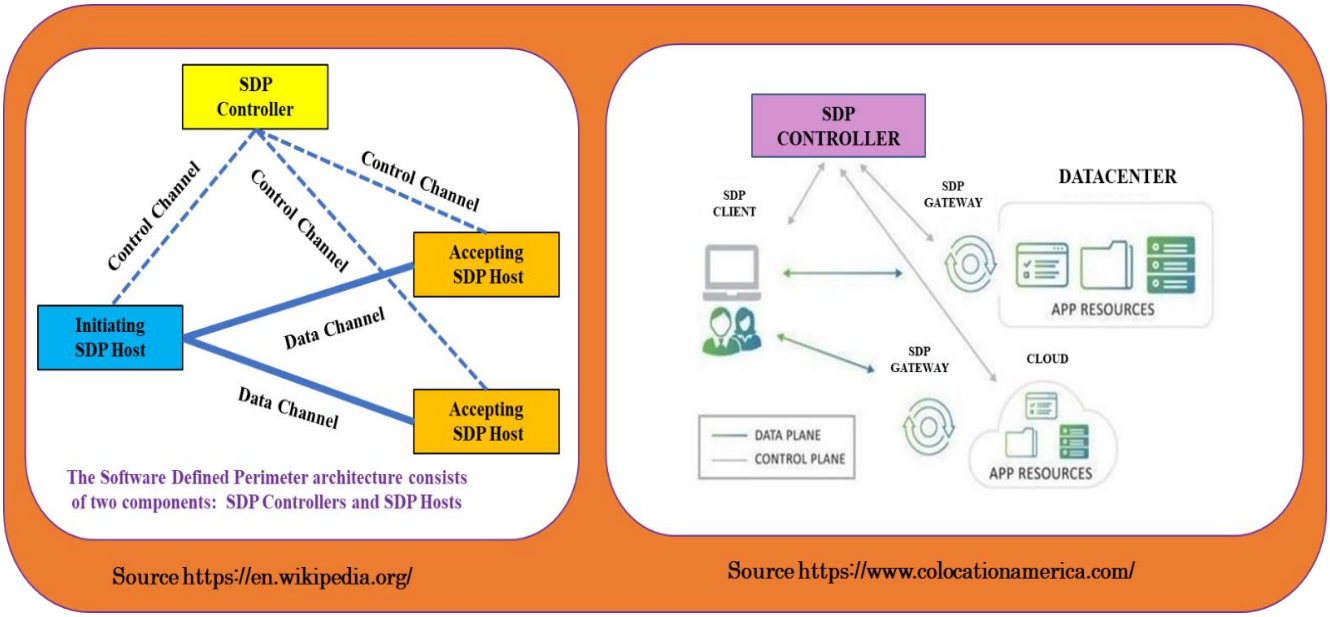
International Journal of Advance Research in Science and Engineering
Vol. No.9, Issue No. 10, October 2020
www.ijarse.com
IJARSE
ISSN 2319 - 8354



Source www.catonetworks.com/sdp/

SOFTWARE DEFINED PERIMETER ARCHITECTURE

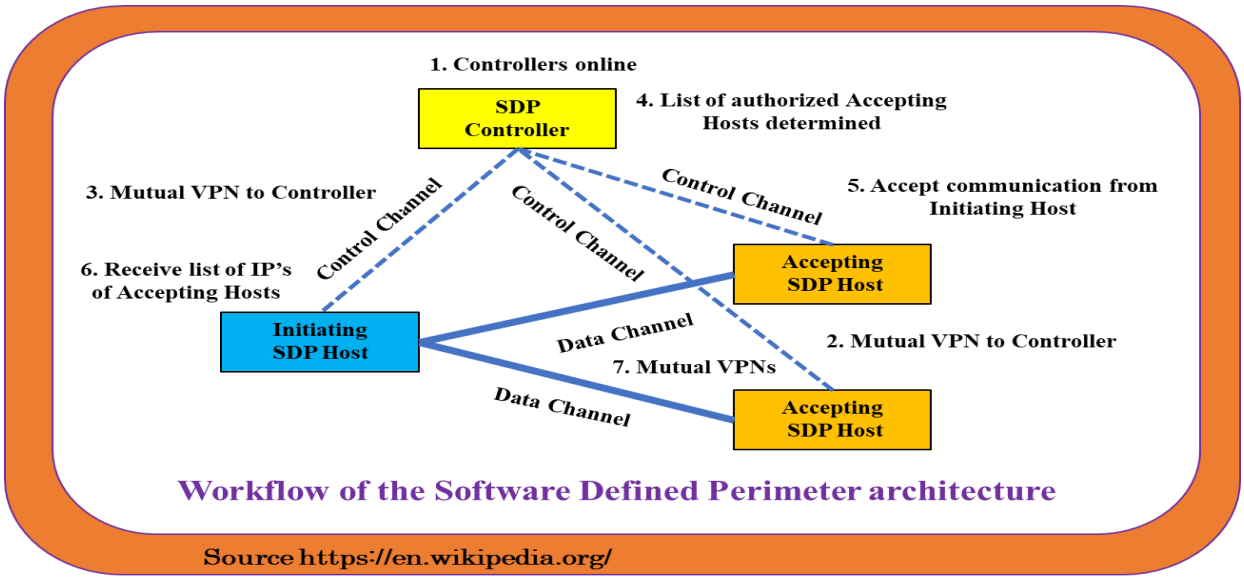
In the simplest form, the SDP architecture comprises of two parts: SDP Controllers and SDP Hosts. SDP Hosts will be able to either trigger the connections or acknowledge connections. Such actions are run by interactions by the SDP Controllers through a control channel. Therefore, in an SDP, the control plane is split from the data plane to allow more scalability. Additionally, all the individual components can be redundant for increased availability.



Source https://en.wikipedia.org/

Source https://www.colocationamerica.com/

The Software Defined Perimeter structure includes the following workflow
1.One or several Software Defined Perimeter Controllers will be brought online and linked to the relevant optional verification and authorization services (e.g., PKI, device geolocation, fingerprinting, SAML, multifactor authentication, OAuth, LDAP, OpenID, Kerberos, as well as other such essential services).
2.One or several Accepting Software Defined Perimeter Hosts will be brought online. These hosts establish a connection and authenticate with the Controllers. Though, they do not accept communication from some other Host and will not reply to any non-provisioned request.
3.Every Initiating Software Defined Perimeter Host which is taken online connects with, as well as authenticates to, the Software Defined Perimeter Controllers.
4.When authenticating the Initiating Software Defined Perimeter Host, the Software Defined Perimeter Controllers define a list of Accepting Hosts to whom the Initiating Host is allowed to communicate.
5.The Software Defined Perimeter Controller directs the Accepting Software Defined Perimeter Hosts to acknowledge communication from the Initiating Host and any mandatory policies necessary for encrypted communications.
6.The Software Defined Perimeter Controller provides the Initiating Software Defined Perimeter Host the list of Accepting Hosts and any optional policies necessary for encrypted communications.
7.The Initiating Software Defined Perimeter Host initiates a mutual Virtual Private Network (VPN) link to all authorized Accepting Hosts.



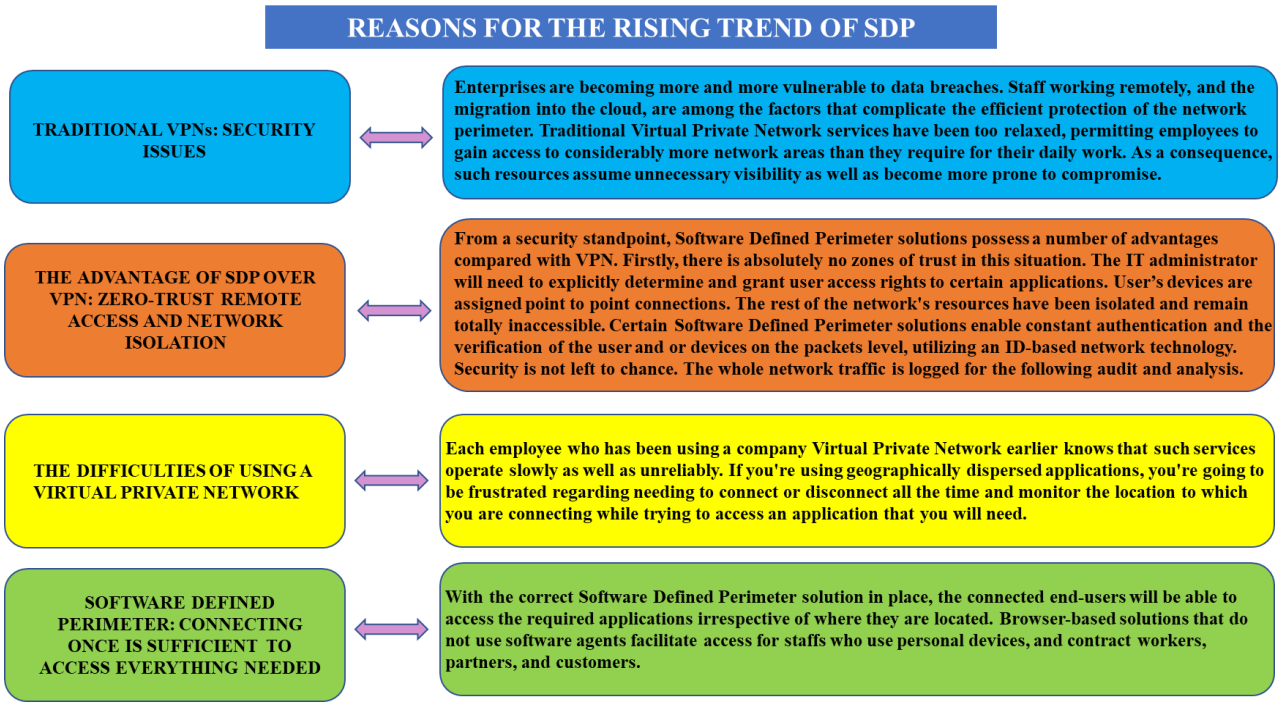
Workflow of the Software Defined Perimeter architecture

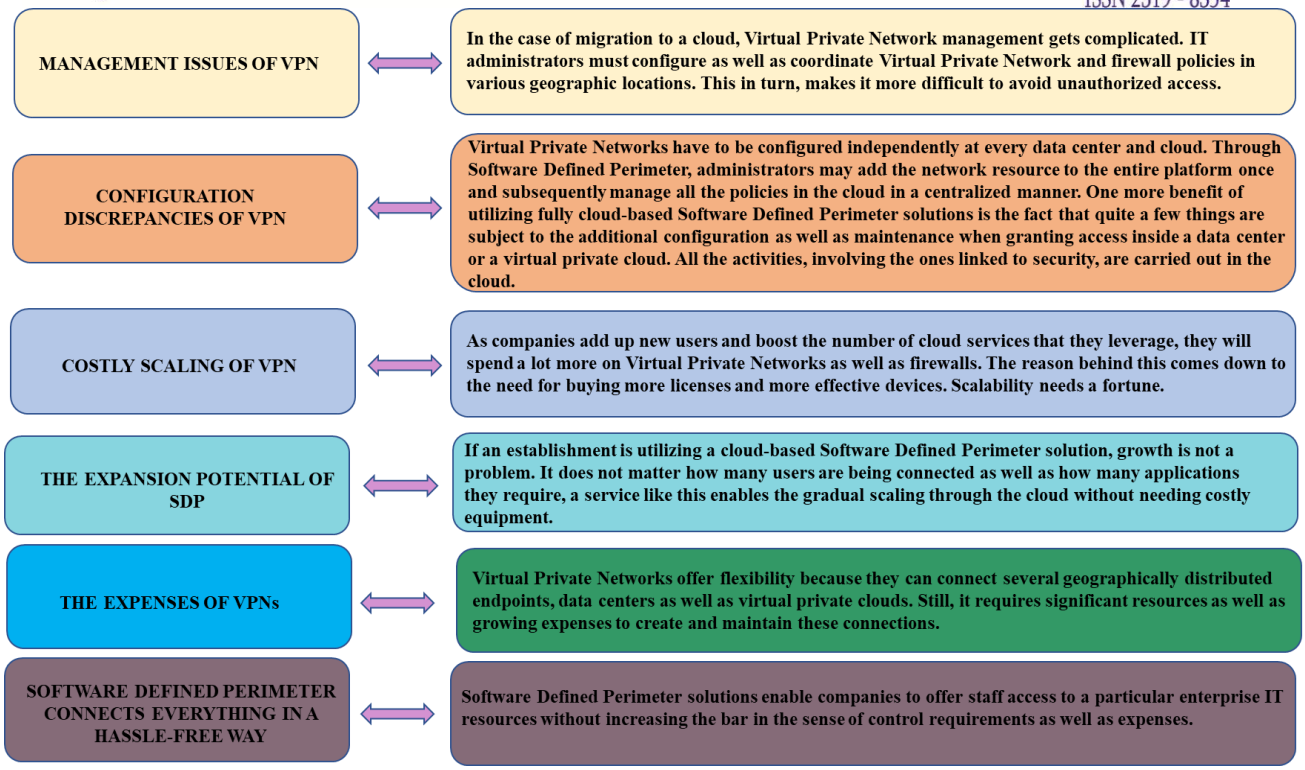
Source https://en.wikipedia.org/

International Journal of Advance Research in Science and Engineering
Vol. No.9, Issue No. 10, October 2020
www.ijarse.com
IJARSE
ISSN 2319 - 8354

THE ADVANTAGES OF SDP OVER VPN

The most important underlying reasons why companies rethink the protection of their remote-access services provided the security, reliability, scalability, and flexible approach advancements in the presence of Software Defined Perimeter services. Perimeter oriented VPN have been deployed to give staffs and contract workers, access to corporate networks. Until very recently, this has been one of the most suitable methods to preserve secure remote access. Though, having logged in, VPN users receive broad access to corporate network resources. This approach revolves around the all or nothing principle which puts confidential information at potential risk. This caution has provoked an increasing interest in the software defined perimeter. Such solutions carry out user authorization and authentication based upon pre-established policies before granting access to certain network areas and applications instead of the entire network. On the other hand, the total number of staffs working at home, or perhaps even cafes, airports, etc., is growing now. Moreover, the damage resulting from network intrusions is so large that the disadvantages of perimeter based VPN services are getting more and more noticeable than ever before. Under these circumstances, companies are beginning to regard alternatives such as Software Defined Perimeter solutions, that control the zero-trust model.





In conclusion, a thorough understanding of safe remote-access mechanisms encourages companies who are migrating in the cloud to deploy Software Defined Perimeter solutions. These services fulfill a custom network access policy for the users and resources at an individual level. Such resources stay hidden by unauthorized users, thus reducing the potential attack surface. The customer focus of Software Defined Perimeter solutions is making them simpler to control, relevant across the board, adequately protected, and adaptable. These qualities beat the advantages of traditional Virtual Private Network services.

THE WORKING PROCESS OF SOFTWARE DEFINED PERIMETER

With a software defined perimeter, it must not be technically feasible to make a connection with a server if not permitted to do so. Software Defined Perimeter enables access to users only after checking the user identity and evaluating the state of the device. When the user and device have been authenticated, the software defined perimeter sets up a specific network connection between that device as well as the server it is attempting to access. An authorized user has not logged into a larger network, however, is given its own network connection which nobody else can access and which contains only the services which the user will have approved permission to

access. Envision a web server that is connected to the Internet but will not open connections with anything. It will not accept requests or transmit responses it does not have open ports and there is no access to the network even if it is plugged into the Internet. This is the state which is the default for servers within an SDP. An alternative way to imagine software defined perimeter is to envision a front door which is always locked. Nobody can go through the door, or else even peek inside, till the person on the opposite side of the door confirms who the guest is and what they're doing. When the visitor is permitted inside, the individual in the house locks up the door again.

HOW CAN A USER ACCESS AN SOFTWARE DEFINED PERIMETER

User identification: The user's identity is usually authenticated through a third-party identity provider (IDP). Software Defined Perimeters can also be integrated with an SSO solution. User verification can include a straightforward username and password combination, although it is safer to utilize multi-factor authentication with some kind of hardware token.

Device authentication: This will involve an inspection to make certain that the user's device is working up to date software, inspecting for malware infections, as well as performing other security inspections. In Theory, an software defined perimeter might even create a block list of prohibited devices and then check to make sure that the device is not present on the blocklist.

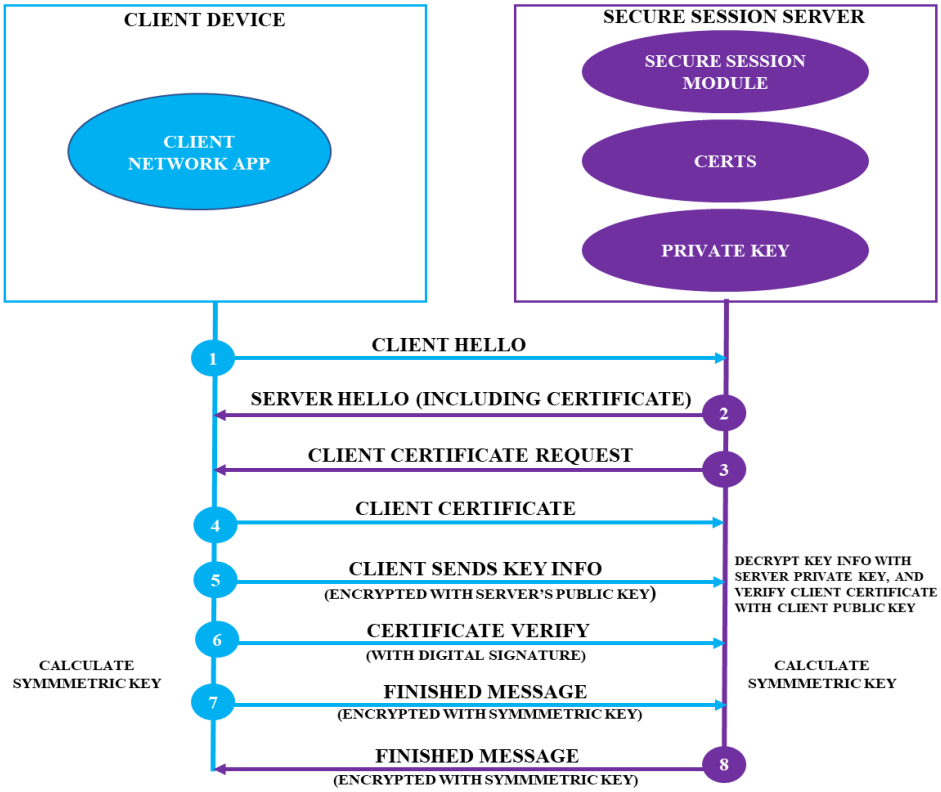
Software Defined Perimeter controller authorization: The software defined perimeter Controller is the most logical component of the software defined perimeter which is responsible for deciding which devices and servers should be permitted to connect. When the user and device have been authenticated, the controller passes along approval of the user as well as the device to the software defined perimeter gateway. The software defined perimeter gateway is a place where access is allowed or denied.

How an SDP establishes a Secure network connection: The software defined perimeter gateway will open the virtual gate to enable the user through. It establishes a secure network connection with the user’s device on the one side of the gateway, while on the other side it establishes a network connection with the services which the user will be able to access. No other users or servers will be sharing this connection. These safe network connections usually include the use of mutual TLS and might use a Virtual Private Network.

User access: The user will be able to access formerly hidden network resources and are able to continue utilizing their device normally. The user operates inside an encrypted network to which just them and the services that they access belong.

A DESCRIPTION OF MUTUAL TLS

Mutual TLS is a commonplace security practice which uses client TLS certificates to offer an extra layer of security, which makes it possible to verify the client information through cryptography. In most instances when you attempt to access a safe and secure HTTPS or TLS endpoint, you encounter just the client-side verify of a server certificate. The aim of this inspection is to guarantee that no fraud is engaged and the data transmission between the client and the server will be encrypted. Furthermore, the TLS standard enables you to specify the client certificate, so that the server can accept contacts only for clients with certificates registered by the server certificate authority, or provide additional security checks based on the information stored in the client certificate. Here is what we call mutual TLS once the two sides of the connection verify certificates.



SOFTWARE DEFINED PERIMETER AND ZERO TRUST NETWORKING (ZTN)

The security industry recognizes that the current security mechanisms are just partially effective. The implementation of a software-defined perimeter could be applied before TCP/IP as well as TLS, which reduces the probability of these and more susceptible protocols that are used as attack vectors by threat detectors. SDP implementations in compliance with the CSA software-defined perimeter ver 1 design establish zero-trust implementations that avoid the common approaches of an attack like DDoS, credential stealing, as well as the notorious. highest 10 threats issued by the Open Web Application Security Project. Software-defined perimeter makes assets hidden and avoids access till the related identity is effectively authenticated and permitted for access to such assets for a tried and tested zero trust implementation. In a practical sense, Zero Trust is the idea behind the software-defined perimeter architecture. Software-defined perimeter's fundamental principles are Assume nothing, Believe nobody, Check everything, Defeat threats (ABCD). While software-defined perimeter, zero trusts is meant to be implemented at the Network L3 of the International Standards Organization (ISO) OSI mode, from the perspective of the shared architecture patterns for example in applications accessing hybrid cloud services, care should be taken to apply zero-trust network as close as possible to a domain perimeter such as possible, to ensure optimum performance and prevent unnecessary service latency.

THE FUTURE POSSIBILITIES OF SOFTWARE DEFINED PERIMETER

The policies are a key component of the software-defined perimeter architecture which uses a centralized software-defined perimeter controller and distributed software-defined perimeter gateways to allow adaptable, quick, and secure connections. Standardized, normal language policies help decrease data loss as well as spillage by regulating access only to certain applications, information, and resources. Dynamic, connection centered models like software-defined perimeter based upon user, device, or else application security constitutes a natural extension from per application or Network access control-based connections. This additionally secures the network and lessens the possibility of malware intrusion. Furthermore, incorporating and augmenting the software-defined perimeter client with a policy that provides true zero-trust protection with extra, dynamic granular connection options. As well as allowing application

transparency through the software-defined perimeter gateway data path - Virtual Private Network, Network Access Control offers convincing value to contemporary enterprises guaranteeing applications that are up-and-running, as well as those workforces are equipped with secure, 24/7 access irrespective of location.

SOFTWARE DEFINED PERIMETER ARCHITECTURE MEETS TODAY'S BUSINESS REQUIREMENT

A actual software defined perimeter architecture which meets today's business needs and fits as well as grows as those requirements transformation should include centralized policy management and authorization and distributed micro segmented application and access resources manage both for the data center as well as cloud applications through micro segmentation develops on an SDN Network segment access model along with allocated policy implementation inside the software defined network. (which is based on a centralized depository) and application service centric policies, that are not based on IP address. A trust model in such an environment is built on SDN network segment access, implies assumes a zero-trust model, and offers distinct segments intended for privileged users. This software defined perimeter implementation and trust paradigm support and incorporates well with today's Secured solutions.

CONCLUSION:

This research paper describes the Next Generation Virtual Private Network and Software Defined Perimeter as a possible solution to the various security challenges and concerns confronting modern-day networks from the perspective of its architecture, concept, and potential applications. Software defined perimeter guarantees to find a solution to many security challenges. Architectural design influences existing technologies, for example, virtual private network tunnels, mixes it with modern ideas from software defined perimeter as well as micro segmentation to offer an architecture that displays promise for solving several security problems. SDP provides powerful security advantages making resources opaque to hackers, enabling always on connections, improving network strength as well as flexibility, as well as reducing malware infiltration. Adopting the cloud has many advantages but frequently requires numerous changes to take advantage of. This research paper helps to think about the cloud in a different way, and all this an opportunity to transform the way that users have access to such resources to

make it more secure, more resilient, and more effective. Software defined perimeter is an important step forward in security for the very first time allowing dynamic, identity centric security that will be applied at the network layer as well as excited about witnessing it more broadly adopted by enterprises to get to know the modern security and business needs. However, Software defined perimeter does not solve each security issue there are numerous parts of infosec that are just not within the scope for software defined perimeter, and residual dangers that might be associated with a specific product, or else powered by the particulars of an enterprise's implementation. Overall, SDP is a novel and convincing method for improving security with specific relevance to Infrastructure as a Service environment, Enterprises are exploring to strengthen security and compliance stance, facilitate true workforce agility, and enhance business responsiveness. Thus, Enterprises must discover how software defined perimeter can tackle their business needs.

REFERENCES:

[1] Innovation enterprise- Strategy- SDP or VPN: Which is better to secure remote access- David Balaban https://channels.theinnovationenterprise.com/

[2] Software Defined Perimeter - https://en.wikipedia.org/wiki/Software_Defined_Perimeter

[3] McClure, Stuart (July 11, 2012). Hacking Exposed 7 Network Security Secrets & Solutions. McGraw Hill. ISBN 0071780289.

[4]CLOUDFLARE- what is a software-defined perimeter -https://www.cloudflare.com/learning/access-management/software-defined-perimeter/

[5]Meta Networks-Whitepaper-SDP vs VPN – 5 Reasons to Make the Switch.https://www.proofpoint.com/

[6]Cloudflare Docs- Access- Mutual TLS authentication -https://developers.cloudflare.com/

[7]Software Defined Perimeter(SDP) and Zero Trust-https://cloudsecurityalliance.org/

[8]Pulse Securer's Software Defined Perimeter – Secure Access in a Zero Trust world - Whitepaper

[9]Attila security- Next gen VPNs: what are the coming changes to vpn Technology- by Vesh Bhatthttps://www.attilasec.com/blog/

[10]impulse acquired by OPSWAT- August 21,2019 -SDP Vs VPN —Why not the best of both- https://impulse.com/blog/sdp-vs-vpn-why-not-the-best-of-both

[11]https://support.huawei.com/enterprise/en/doc/EDOC1100086559