An Introduction To The SASE

Introduction

With the reality that the Remote Workforce is going to be around with us for quite some time to come in the foreseeable future, there are still many Cybersecurity issues that need to be resolved, still. For example, there is still the co-mingling of home networks with business networks, thus causing the flow of network communications to become at grave risk for malicious, third party intervention.

Then there is the Virtual Private Network (VPN). This has been a warrior when it comes to the safe transmission of Personal Identifiable Information (PII) datasets across the Internet, but it too is showing its signs of wear and tear.

In other words, there too many pieces to be put together when trying to resolve these issues. All of the networking tools and technologies need to come under one umbrella for ease of management, and this is where the SASE could come into play.

What Is The SASE?

It is an acronym that stands for the "Secure Access Service Edge" and is pronounced as "sasssyyyy". It was actually conceived by Gartner back in 2019, when they published a report back in 2019, entitled the "The Future Of Network Security In The Cloud". Essentially, this is a specific methodology which allows any type of business, large or small, to have a unified network system that will allow them to bring both networking and security functionalities under one common platform.

For example, it can also incorporate both the functionalities of the WAN as well the SD-WAN with some of the latest frameworks that soon Corporate America will be embracing, and these are as follows:

- The Next Generation Firewall (NGFW);
- The Secure Web Gateway (SWG);
- The Zero Trust Model;
- The use of Cloud Security Brokers (CASBs).

The ultimate of goal of SASE is to bring end to end protection from the wireless device all the way to the servers that are being accessed, and vice versa.

Examples Of How SASE Would Be Used

It is primarily targeted towards those individuals and teams that work from a remote location, and don't usually often have to come into their traditional brick and mortar offices. With the rapid explosion of the Remote Workforce, it is highly anticipated that SASE will be adopted by over 40% of businesses and organizations by 2024.

(SOURCE: 1).

But it will also prove highly beneficial as well to those employees that are constantly on the go, and to external third parties.:

1) <u>The Road Warrior</u>:

Take the example of Tracey. She is always on traveling somewhere, on an almost weekly basis. In order to further expedite her workflows so that she can get them done quickly and efficiently, Tracey decides to use the Public Wi-Fi system at her hotel room. Of course, accessing, sharing, and the transmission of confidential information would present to be a grave security threat here. After all, there is no level of encryption that is involved here, and any of this could be quite easily hijacked by a Cyberattacker. The use of SASE could potentially solve all of these issues, by enforcing rules that would make sure that all of the data packets that are transmitted back and forth are actually encrypted. But not only that, it would also help to ensure that the data packets that are delivered to Tracey's wireless do not have any traces of malware in them, as she could be communicating with other clients and prospects that are external to her network connection.

2) The Third Party:

Suppose that Jane is an outside contractor, trying to access sensitive documents from the corporate server. Under normal circumstances, she would have to probably use what is known as Two Factor Authentication (2FA), in order to have her identity completely confirmed. But even under these circumstances, trusting an external, third party in this regard can still pose to be a very serious threat. But if were SASE were to be used, it would implement the Zero Trust Framework (as stated earlier in this article). With this, absolutely nobody is trusted, and any individual would have to pass through many layers of authentication (at least 3 of them or more) in order to have their identity confirmed beyond a reasonable doubt. By doing it this way, there is almost a 100% guarantee that Jane is who she claims to be.

The Benefits Of Using SASE

The following are some of the strategic of it:

- It is highly scalable:

  SASE is primarily meant to be used when accessing shared resources from a Cloud based platform, such as that of AWS or Microsoft Azure. Because of this, you quickly and easily ramp or down your security needs. For example, apart from the characteristics described earlier, you can also implement the following:

  *Threat prevention tools;

  *Web filtering;

  *Sandboxes;

  *Multiple layers of DNS security;

  *ID Theft prevention techniques;

  *Controls to help mitigate the chances of data loss, whether it is intentional or non-intentional in nature.

- Substantial cost savings:

Since it is compatible with the major Cloud based providers, businesses will realize substantial savings when it comes to procurement and deployment. For example, rather than having to pay a sizeable down payment, SASE can offer fixed and monthly pricing schedules that will make it affordable to any organization.

- A reduction in complexity:

Up to this point, many businesses have deployed many types of security tools and technologies, from all sorts of vendors. CIO's and CISO's are now starting to understand the ramifications of this from two different perspectives:

*It greatly increases the target surface for the Cyberattacker to penetrate into;

*Many alerts and warning messages are created, which creates many false positives.

The SASE can alleviate most of this because everything is consolidated into one primary platform, and this provides two key benefits:

*There is a sharp reduction in the complexity with regards to the lines of defense that have been implemented. For example, the security tools will now be deployed into a much more strategic fashion. For instance, instead of having 10 firewalls in a haphazard fashion, perhaps using just 3 of them will make much more sense if they are installed where they are needed the most;

*Fewer tools means that there will be less false positives filtering through, which means that the IT Security team will be able to triage and react to the real threats in a prompt manner.

- A coupling of security functionalities:

Many of the Cloud providers offer they own suite security tools, and these can also be connected with the security features of SASE seamlessly. The end result is that the business will probably have one of the most secure environments imaginable.

Conclusions

Overall, this article has examined what SASE is, and its major benefits. But keep in mind that this is just an overview, and in-depth knowledge of the tools and frameworks that is uses is also needed, in order to fully grasp what your business will need in this regard. A future article will examine these in greater detail.

Sources

1) https://www.paloaltonetworks.com/cyberpedia/what-is-sase#:~:text=SASE%20is%20the%20convergence%20of,%2C%20cloud%2Ddelivered%20service%20model.&text=This%20approach%20allows%20organizations%20to,applications%20or%20devices%20are%20located.
2) https://www.sd-wan-experts.com/sase/
3) https://www.sdxcentral.com/security/definitions/what-is-sase-secure-access-service-edge/
4) https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/what-is-sase.html
5) https://www.fortinet.com/resources/cyberglossary/sase