ZTNA WITH SPARKVIEW

Why Switching to ZTNA is the Future of VPN Deployments

In today's fast-paced digital world, remote work has become the norm for many businesses, offering numerous benefits such as flexibility and increased productivity. However, this shift towards remote work has also highlighted the importance of securing remote access to company networks. As a result, companies are increasingly turning to Virtual Private Network (VPN) technology to provide secure remote access to their networks. Despite being a popular choice, traditional VPN deployments have limitations that make them increasingly difficult to manage and secure. This is where Zero Trust Network Access (ZTNA) comes in. ZTNA provides a more secure, flexible, and efficient way of connecting remote workers to the company's network. In this article, we will explore why switching to ZTNA is the future of VPN deployments and how it can help businesses stay ahead in the game.

Limitations of traditional VPN

Traditional VPN deployments are often a liability for businesses. One of the primary limitations of traditional VPNs is the lack of scalability. VPNs were initially designed for connecting remote workers to a central network. However, as more employees continue to work remotely, the number of connections to the VPN increases, putting a strain on the network infrastructure. This can lead to slow network speeds, which can affect productivity.

Another limitation of traditional VPNs is the lack of security. VPNs were not designed to handle the sophisticated cyber threats that exist today. As a result, VPNs have become a popular target for cybercriminals. VPNs can be easily compromised, allowing attackers to gain access to the network and steal sensitive data. Additionally, traditional VPNs sometimes still rely on a single factor of authentication, such as a username and password, which can be easily hacked or stolen.

Lastly, traditional VPNs can be challenging to manage. As the number of remote workers continues to increase, the management of VPNs becomes more complex. IT teams are required to manage multiple VPN connections, which can be time-consuming and can lead to errors.

What is ZTNA and how does it differ from VPN?

Zero Trust Network Access (ZTNA) is a modern security architecture that provides a more secure, flexible, and efficient way of connecting remote workers to the company's network. ZTNA differs from traditional VPNs in several ways.

Firstly, ZTNA uses a different approach to security. Unlike traditional VPNs, which assume that everything within the network is trusted, ZTNA operates on the principle of zero trust. This means that no user or device is trusted by default, and all access requests are verified and authenticated before access is granted. This approach provides an additional layer of security, making it harder for cybercriminals to gain access to the network.

Secondly, ZTNA is more flexible than traditional VPNs. ZTNA can be deployed on-premise, in the cloud, or in a hybrid environment. This means that businesses have more options when it comes to deploying ZTNA, allowing them to choose a deployment model that best suits their needs. Additionally, certain Zero Trust Network Access (ZTNA) solutions no longer require client software, providing increased flexibility and cost-efficiency on the client-side.

Lastly, ZTNA is more efficient than traditional VPNs. ZTNA uses a micro-segmentation approach, which means that access is granted on a per-application basis. This reduces the amount of data that flows through the network, improving network performance and reducing the risk of data breaches. This goes so far that data no longer even flows from the network to user devices, but is kept and processed only within the corporate network. This also applies to remote access.

Benefits of ZTNA over VPN

ZTNA provides several benefits over traditional VPNs. Firstly, ZTNA provides enhanced security features. ZTNA uses a zero-trust approach, which means that all access requests are verified and authenticated before access is granted. This approach provides an additional layer of security, making it harder for cybercriminals to gain access to the network. Additionally, ZTNA uses multi-factor authentication.

Secondly, ZTNA is more scalable than traditional VPNs. ZTNA uses a micro-segmentation approach, which means that access is granted on a per-application basis. This reduces the amount of data that flows through the network, improving network performance and scalability. This makes it easier for businesses to manage and secure their networks as the number of remote workers continues to increase. In case of a client software-free solution, scaling becomes even easier, as it can be done independently of the user devices.

Thirdly, ZTNA is more efficient than traditional VPNs. As ZTNA uses the micro-segmentation approach, it reduces the amount of data that flows through the network, improving network performance and reducing the risk of data breaches.

Lastly, ZTNA is more cost-effective than traditional VPNs. ZTNA requires less hardware and software than traditional VPNs, reducing the cost of deployment and maintenance. Additionally, ZTNA can be deployed in all kinds of environments, allowing businesses to choose a deployment model that best suits their needs.

ZTNA deployment models

ZTNA can be deployed on-premise, in the cloud, or in a hybrid environment, depending on the needs of the business.

On-premises deployment is suitable for businesses that require complete control over their network infrastructure.

Cloud deployment is suitable for businesses that don’t have a suitable IT infrastructure.

A hybrid deployment is suitable for businesses that want the benefits of both on-premises and cloud deployment.

Understanding ZTNA architecture

ZTNA uses a micro-segmentation approach to access control. This approach grants access on a per-application basis, reducing the amount of data that flows through the network and preventing lateral movements in the network. The zero-trust approach means, that all access requests have to be verified and authenticated every single time before access is granted, no matter from where the candidate comes both, internally and externally.

ZTNA vendors and solutions

Several vendors offer ZTNA solutions, including beyond SSL SparkView, Fortinet, and Akamai. These solutions vary in their features and capabilities, allowing businesses to choose a solution that best suits their needs. Additionally, ZTNA solutions can be deployed on-premise or in the cloud, giving businesses more options when it comes to deployment.

Future of VPN and ZTNA

The future of VPN and ZTNA is closely tied to the future of remote work. As more businesses continue to adopt remote work, the demand for secure and scalable remote access solutions will continue to increase. ZTNA is expected to become the standard for remote access, providing businesses with a more secure, flexible, and efficient way of connecting remote workers to the company's network.

Conclusion

In conclusion, remote work has become the norm for many businesses, highlighting the importance of securing remote access to company networks. Traditional VPN deployments have limitations that make them increasingly difficult to manage and secure. This is where Zero Trust Network Access (ZTNA) comes in. ZTNA provides a more secure, flexible, and efficient way of connecting remote workers to the company's network. From enhanced security features to the ability to support hybrid environments, ZTNA provides numerous benefits over traditional VPNs. As remote work continues to become more prevalent, businesses should consider switching to ZTNA for a more secure and scalable remote access solution.