Relevance of Zero Trust Network Architecture amidts and it's rapid adoption amidts Work From Home enforced by COVID-19

Dr. Aniket Deshpande [1]

[1] Sales Engineering, Zscaler Inc, Singapore

ABSTRACT

As organizations evaluate different methods to improve data security, they have to shift to find the best alternative means to secure the servers. Zero Trust Network Architecture (ZTNA) has become the focus of many institutions to prevent data loss, especially from the employees working remotely due to the spread of Covid-19, requiring people to keep social distance minimize risks of an attack. Zero trust employs a multifactor authentication process that requires all users to verify their identity or the device they are using before using a network. This security procedure has been useful in eliminating the castle-and-moat concept's weaknesses that were initially used and could allow an individual to navigate freely through a network once they penetrated the firewall. The Zero trust does not allow the penetration and further segment of different materials; therefore, an individual cannot access all materials once in a network. This cybersecurity method will be advantageous post COVID-19 to deliver a simplified user experience enabling them to manage and find the contents with ease. For the customers, the architecture creates a uniform platform that can be used to amplify the security. The technology is a must for cost-benefit analysis for every organization considering its potential to help avoid potential security and financial losses.

Key words:

ZTNA, Network Security, Cloud Security, SASE, Cybersecurity, Securing Work-from-Home, Covid-19

Article Received: 10 August 2020, Revised: 25 October 2020, Accepted: 18 November 2020

Introduction

Cybersecurity is a meaningful discussion that should engage all organizations that handle critical information. Both private and government institutions are at risk of losing important data that either belongs to the institution or their respective clients. As a result, many companies are focused on implementing a network security structure that will provide the ultimate data security within their organization. Traditionally, the company's used built firewalls that allowed employees to operate their computer behind the firewall, preventing unauthorized intrusion. However, this network security method has proved to be very challenging in recent months due to the new guidelines that require the organization to shift to a remote workforce. During the onset of Covid-19, governments introduced protocols that aimed at reducing the spread of the virus. For this reason, the organization resolved to work from home (WFH) programs that do not support the use of firewalls, therefore leading to increased rates of attack. According to Mandal & Khan (2020), with growing Covid-19 cases and adherence to the procedures, several cloud mediums have been affected[1]. The attack of cyber threat will also tremendously increase if a similar trend of WFH is strictly followed. Mandal & Khan (2020) further say that network breaches are a major weakness in remote operation as an individual organization has no control over the internet sources used by their employees[1]. Therefore, logging in to unprotected servers enables hackers to access information stored in the computers or company systems easily. The security concern is a primary issue to all institutions; therefore, threats that arise due to the work from home scenario must be keenly taken into consideration. Verizon's survey says that 474 data breach cases were reported across the world, with 80% from March to June, and these intrusions were caused by hacking, stealing of data, and brute force attacks[2]. These statistics show the need for a new method of cyber protection. Therefore, a zero-trust network architecture is the most appropriate due to its ability to provide protection even for computer users logged into a private network.

What is the Trust Network Architecture ?

Zero trust security is an information technology (IT) data protection model that requires strict identification verification for every person or technological device that attempts to access any

resource on a private network[3]. Moreover, the verification procedure must be followed whether the access request is within or outside the network parameter. Cloudflare(R) (2020) further states that there are no specific technologies associated with Zero Trust Architecture[3]. It is a holistic approach to the network security system incorporating a wide range of principles and technologies. This modern IT network security dramatically differs from the traditional methods used to secure information in various servers. For instance, pre-modern technology is based on the castle-and-moat concept, which prevents unauthorized access from outside the network but enables access to people within the network. Still, devices found inside a particular network are trusted by default. With Zero Trust security, no user is trusted by default, whether from outside or inside a network. Every individual must have the right credentials to access the resources within it. Traditional network security systems had one primary vulnerability: once an attacker gains access to a network, they are free to reign over everything. According to DeCusatis et al. (2016), the fundamental principle of Zero Trust involves guaranteeing secure access to all resources regardless of the device's location with the assumption that the persons trying to access these materials are a threat until authorized, inspected, and secured[4]. Therefore, a company can easily partition the resources that need to be protected to prevent unauthorized personnel access.

Various Interpretations of Zero Trust Network Architectures

Zero Trusts rely on several preventive techniques to provide the needed network security within the enterprises. Firstly, the model uses multifactor authentication (MFA) to confirm the user's identity and improve a network's safety[5]. MFA uses a complex security protocol, including posing certain security questions, automatically sending email or text confirmation messages to users trying to enter a network, or the logic-based exercises to assist in assessing user's credibility. Different companies use divers' authentication factors depending on the level of security that is required. Besides, the inclusion of more authentication points is critical for the strong overall security of a company. Secondly, least privilege access is another interpretation that is used to reinforce cybersecurity using Zero Trust. This method implies that the organization gives each user or device the lowest possible access to the network. This procedure will prevent lateral movement and the network in case of a breach, therefore minimizing the surface for attack. Thirdly, this model uses a micro-segmentation technique that entails dividing the parameters into small parts to maintain access to every network zone. This technique ensures that in case of insecurity, the hacker may not go beyond the microsegment. Even though the three techniques provide security, they are applied differently, and every organization can choose the preferable method to ensure the safety of their data. However, the application of all methods is essential for a reliable security system.

NIST Framework for ZTNA

The NIST security framework guides organizations on critical infrastructures. This guideline is categorized into five essential functions, such as identification, detection, protection, response, and recovery[6]. The framework is flexible and easy to integrate into security systems that are used in any organization. Therefore, before implementing any information security such as ZTNA, the NIST framework provide the recommended baseline that should be followed by organizations. Based on the NIST framework, before executing the ZTNA, an organization needs first to identify its most valuable asset and resources. The organization should then apply relevant safeguards and methods of protecting the critical infrastructure, such as data security and protective technology. The procedures selected should have the ability to alert the organization in case of a cyberattack, and the systems should respond appropriately to avoid any forms of attack. Lastly, recovery activities assist in maintaining resilience and ensuring business continuity in the event of an attack.

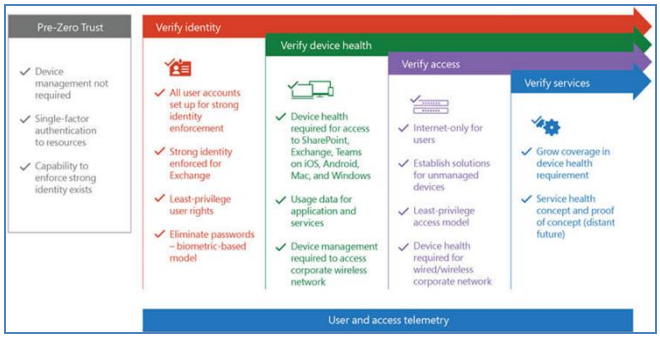
In adherence to the NIST framework, Zero trust is designed to specifically focus on resource and data protection in cases where this material requires any form of identity[6]. With the implementation of Zero trust, resources are only available to people in need, and privileges are very limited. Once employees need any material, they are granted access through a policy decision point and policy enforcement point. Zero trusts have particular logical components that can be operated within the enterprise premises and as cloud-based services (Rose et al., 2019). Every

component plays a specific role in maintaining a stringent security network. For instance, a policy engine is useful for permitting users to resources; policy administrates limits communication between a user, and the resource and policy enforcement point can enable, monitor, and further terminate the access of any resources belonging to a company. The policy engine uses the trust algorithm not only to permit users but also to lock them out of using the materials. The policy engine use has a wide range of inputs to assist in the adequate performance of the trust algorithm. For instance, access request input determines whether the security system approves the application, device, or user requesting the source. Five inputs perform a different function to uphold the best security standards. These are asset requests, subject database and history, asset database, resource policy requirements, and threat intelligence and logs.

Various Interpretence of Zero Trust Architectures

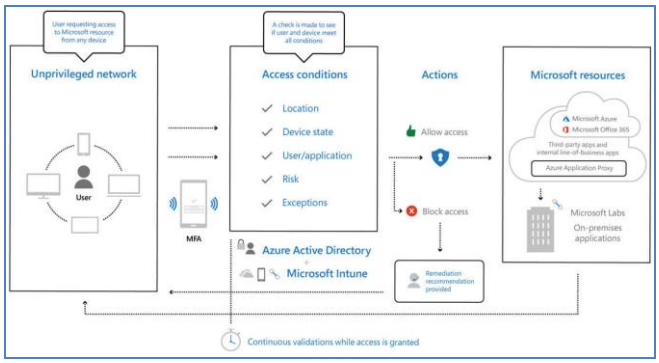
Different companies have instantiated for varied domains when implementing Zero Trust Network Architecture. For instance, Microsoft uses ZTNA to ensure strict adherence to corporate and customer data[7]. Moreover, this model is used to deliver a simplified user experience enabling them to manage and find the contents with ease. For the customers, the architecture creates a uniform platform that can be used to amplify the security.

The picture below (Figure 1) shows the Zero Trust scope and phases created by Microsoft to guide the new security model's implementation. Figure1 clearly indicates the roadmap organized based on phases, which includes goals and the current security status. Before the outbreak of Covid-19, many organizations used parameter security systems, characterized by a lack of proper device management, a single-factor authentication process, and the capability to enforce a strong identity. Figure1 further shows how Microsoft has emphasized identity-driven security solutions and centres through the robust MFA process. This is a simple scope that can be adopted by small and large enterprises effectively to ensure excellent data security using the Zero Trust model.



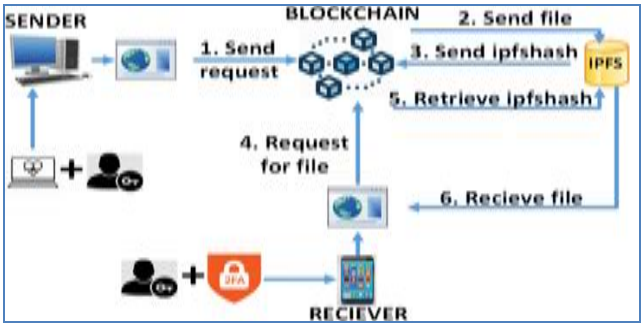
Zero Trust scope and phases created by Microsoft[7]

Figure 2 shows a simplified reference architecture that was used by Microsoft to implement a Zero Trust. The critical components of this procedure are device management and device configuration requirements. The company Azure Active Directory (Azure AD) performs device health validation and is also used for user and device inventory. Microsoft employs this security system to ensure the configuration requirement of the devices. The screened devices then generate statements of health, which are stored in the Azure AD. Upon the user's request to access specific sources, the health of the devices is verified to enable authentication.



Simplified Microsoft Proposed Zero Trust Reference Architecture[7]

Figure 3 shows how Zero Trust can be implemented in combination with the block-chain model. Block-chain is usually used to maintain decentralization and immutability of data, while Zero Trust principles are used for access control and authorization. Therefore, a company that uses a block-chain can easily incorporate Zero Trust for effective data protection[8]. An interpretation of this diagram shows that most institutions will implement ZTNA regardless of the type of services they offer and the working framework. Therefore, it is essential to find the best way to incorporate the ZTNA into the existing business model.



ZTNA with Blockchain (courtsey Sultana et al. 2020)

Potential Cost-Benefit Analysis to Adopt ZTNA

According to Froehlich (2020), ZTNA is an excellent investment against stolen data, and institutions should regard this as investment capital if the information of a company is stolen[9]. Froehlich (2020) further states that the cost of a single data breach is approaching $4 million; therefore, implementing a Zero Trust cybersecurity framework to prevent information loss and further avoid loss of capital should be considered a good investment by an organization[9]. Generally, depending on the type of company, an organization can incur massive losses due to hacking. For instance, financial and insurance companies will directly lose capital through hacking if there is a data breach.

Gartner SASE Framework as an Overlapping Concept to ZTNA

Secure access service edge (SASE) is a security framework that allows safe and fast cloud adoption. Moreover, this security framework ensures that users and devices have secure cloud access to applications, data services at any place, and any time. SASE effectively combines network security functions such as SWG, CASB, FWaaS, and ZTNA with WAN to support an organization's dynamic security needs. SASE provides real-time context and security and compliance policies upon assessing the entity's identity when delivering security services using ZTNA, SWG, CASB, and other capabilities. Generally, SASE is a technological package that includes ZTNA as its core capabilities. For this reason, SASE can easily provide network security by determining the identity of the user, device, and application. Moreover, ZTNA also follows NIST SP 800-63-3 digital identity guidelines and integrates the agency's ICAM policy making it one of the best security protocols not only for remote workers but also for employees working within specific organizations[10]. Implementing ZTNA in line with the NIST framework ensures that data privacy risks and mitigation factors are considered before its implementation process, therefore making it more suitable for any organization.

Covid-19 Pandemic and Impact on Adoption of Zero Trust Network Architectures

Fast-tracked emphasise on adoption due to COVID-19

Zero Trust Network Architecture has gained popularity among diverse companies since the first case of Covid-19 was reported. According to Hope (2020), as many small and medium organizations moved towards remote working, many firms were looking for alternative ways to solve their legacy security practices, which did not support the WFH[11]. As a result, Zero Trust was highly embraced by the IT experts to be one of the best methods to secure valuable company resources and prevent hackers from obtaining important information that belongs to the company or their clients. Hope (2020) acknowledges that many firms were not adequately preparing for cloud transformation during the virus attack. For this reason, cybersecurity departments scrambled to configure their network parameter for remote access by their employees[11]. Despite a lack of proper security preparedness, maintaining the right network protection proved difficult, especially for those using other methods such as firewall security system forcing most employers to undergo cloud transformation. As a result, the firms accelerated their shift to the Zero network framework. Hope (2020) says that 76% of the polled companies, to determine their preparedness to adopt new systems that could offer stringent security measures, were using outdated methods to protect their data[11]. The organizations using the old fashioned processes needed to adapt the Zero Trust Architecture quickly. The research further indicates that 82% of the organization surveyed during the pandemic was more committed to implementing ZTNA to enable employees to operate remotely with cybersecurity challenges. One of the major difficulties reported among the organization adopting this new criterion was Identity and Access Management (IAM). IAM is essential for informing all network users of some

of the things they are allowed to do and something they cannot do in a network.

Research by McGillicuddy (2020) states that 61% of the firms that shifted to ZTNA lead to improved security issues[12]. Many organizations have experienced a surge in the number of devices penetrating their networks; therefore, adopting the Zero Trust system has been critical for improved data security for the affected firms. Moreover, ZTNA provides companies with an opportunity to allow employees to use their devices without the risk of hacking. ZTNA has a wide range of benefits to users and specific companies that have employed it. For instance, network security architecture allows employees to access the web despite their remote location directly. Users can easily connect with the applications, and the traffic flows along the shortest secure path. This security system also improves context-awareness by enabling users only to see what they should see. Context-awareness can be more beneficial in scenarios other than just working from home security. Mergers and acquisitions, cloud migration, and third-party access are some of the essential advantages that enterprises stand to enjoy even when this system is implemented post-Covid-19. Challenges that might be experienced in this situation can easily be addressed through user-centric policies. Moreover, ZTNA enhances greater visibility by allowing companies to know who is accessing what, and where, anywhere in the network, which is very beneficial for remote working and even in a situation where employees need to work from one central location.

Continued Adoption of ZTNA Post COVID-19

The Castle-and-moat approach used by different enterprises has proved to have a wide range of security vulnerabilities. Firstly, the Castle can allow any individual who has penetrated the firewall to freely operate within a network since there are no additional security measures. Several studies have revealed that the Castle no longer exists in isolation as it once did. Secondly, the information technology world is shifting towards cloud and mobile platforms; therefore, many users need quick access to different applications and data from various devices and multiple locations. Moreover, companies are dealing with distributed information infrastructure, which is very challenging to secure with a perimeter-based approach. Therefore, the Zero Trust model is essential for the identification of users, devices, and applications that are on a network. Besides, companies can easily employ policy rules using a role-based approached[13]. Institutions can also grant appropriate network access to specific users, devices, and applications and further segment the data based on its type, sensitivity, and use. This procedure ensures that Zero Trust is used to protect critical information within an organization, and the surfaces that are more prone to cyber-attacks are reduced drastically. Even though Zero Trust has been useful in improving security for employees working remotely, the model will be equally crucial for securing materials that are accessed within the institution. Moreover, it limits the chances of attack even when hackers have penetrated the firewall and other parameter security systems, making it more important to protect company data even post COVID-19. Implementation of the Zero Trust model guarantees an excellent security orchestration by ensuring no holes are left uncovered. The combined security elements complement one another, protecting the institution's valuable information.

Conclusion

A wide range of organizations has adopted ZTNA during this pandemic to ensure information security and reduce the increasing rate of data loss. Besides, it is essential to note that ZTNA has been crucial even in workers' remote locations, especially in areas where the parameter security system cannot be used. ZTNA eliminates cybersecurity weaknesses that are present when using the firewall method. For instance, segmentation of the network to prevent a hacker from navigating through the entire system once they penetrate the firewall. With the old system, any individual who has penetrated the firewall can easily access resources within a network. ZTNA will require authentication for any user or device, therefore preventing these risks.

References

[1] S. Mandal and D. A. Khan, “A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic,” in Proceedings - International Conference on Smart Electronics and Communication, ICOSEC 2020, 2020, pp. 837–842.

[2] "COVID-19 Data Breach Landscape | Verizon Enterprise Solutions," Verizon Inc., 2020. [Online]. Available: https://enterprise.verizon.com/en-sg/resources/articles/analyzing-covid-19-data-breach-landscape/. [Accessed: 20-Dec-2020].

[3] "Zero Trust Security | What's a Zero Trust Network? | Cloudflare UK," Cloudflare Inc., 2020. [Online]. Available: https://www.cloudflare.com/en-gb/learning/security/glossary/what-is-zero-trust/. [Accessed: 20-Dec-2020].

[4] C. DeCusatis, P. Liengtiraphan, A. Sager, and M. Pinelli, "Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication," in 2016 IEEE International Conference on Smart Cloud (SmartCloud), 2016, pp. 5–10.

[5] "Zero Trust Security Explained | Principles of the Zero Trust Model," Crowdstrike Inc., 30-Apr-2020. [Online]. Available: https://www.crowdstrike.com/epp-101/zero-trust-security/. [Accessed: 20-Dec-2020].

[6] [6]National Institute of Standards and Technology, "Zero Trust Architecture - Draft (2nd) NIST Special Publication 800-207," p. 49, 2020.

[7] [7]"Implementing a Zero Trust security model at Microsoft," Microsoft Corporation, 2020. [Online]. Available: https://www.microsoft.com/en-us/itshowcase/implementing-a-zero-trust-security-model-at-microsoft. [Accessed: 20-Dec-2020].

[8] [8]M. Sultana, A. Hossain, F. Laila, K. A. Taher, and M. N. Islam, "Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology," BMC Med. Inform. Decis. Mak., vol. 20, no. 1, p. 256, Oct. 2020.

[9] [9]A. Froehlinch, "The 6 benefits of zero-trust security for businesses," TechTarget, Oct-2020.

[10] [10] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," Gaithersburg, MD, Aug. 2020.

[11] [11] A. Hope, "COVID-19 Pushed Most Firms To Adopt Zero Trust Security Model, a New Study Found - CPO Magazine," CPO Magazine, 19-Oct-2020.

[12] S. McGillicuddy, "Survey: Zero Trust benefits remote work during pandemic | Network World," Network World, IDG Communications, Inc., 28-Oct-2020.

[13] J. Kindervarg, S. Balaouras, and K. Mak, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture," Forrester Inc., 2012. [Online]. Available: https://www.forrester.com/report/Build+Security+Into+Your+Networks+DNA+The+Zero+Trust+Network+Architecture/-/E-RES57047#. [Accessed: 20-Dec-2020].