Zero-Trust & Network Security

Todd M. Hammond

Pace University

Introduction to Cybersecurity Fall 2024 72308 - CYB 611- 72308 - 202470

Jeytha Sahana Venkatesh Babu

October 2, 2024

Zero-Trust & Network Security

Introduction

In today's rapidly advancing world of technology, where technology has created a strong holding onto mankind's daily existence and helps us navigate through life by making it easier and easier. With this advantage, we have found ourselves understanding, analysing and finding ways to protect its existence while at same time while working on an expansion to reach newer milestones. Cybersecurity is the foundational key that is maintaining trust in this digital age(Qazi, 2022). As said earlier, due to the increase and advancement of technology there also has been an increase in the attacks carried out by malicious intruders that comes from a variety of opponents such as hackers who work independently to cyber-based gangs. Their intentions may most likely include trying to compromise the work inside internal networks and trying to hamper the integrity of the work established as well as the functionality of the systems.(Dhiman et al., 2024). In this paper, we will discuss the need for security and compare the traditional methods of safeguarding digital space and the new concept of zero-trust network security. Both the models follow different methods and protocols, however their end motive remains the same - Safety and Protection. This paper explores the in-depth difference between traditional network security in depth and zero-trust network security. In a traditional network security setting it is assumed that the threat is usually from outside, which would mean, that once an attacker breaches the perimeter access they will be able to access free movement and complete uninterrupted access within the digital zone(Qazi, 2022).

Nowadays the perimeter network security is getting outdated and since the domain has grown larger than before with the development of other cloud services and the introduction to Internet of Things and the concept of remote working, it is even harder to stick to what has previously been implemented. Hence organisations are forced to stick to more flexible and

adaptable ways of network security prevent the risks and challenges of data and revenue losses (TEERAKANOK, 2023). On the other hand zero trust's foundation lies on, i.e. potential threats could lie within the organisation not just externally. Zero Trust assumes that there is no trusted perimeter. Users and devices only receive the least privileged access. In the Zero Trust environment, continuous verification and authorization are required for users when accessing enterprise resources(TEERAKANOK, 2023).

Traditional Network Security

Traditional network security is based on the concept of perimeter/ boundary security - which refers to the boundary that separates the digital space externally and internally. It consists of a firewall, intrusion detection system and access control mechanisms. Setting up security systems that stand guard to protect the perimeter of an organisation will ensure the safety of the internal assets. Traditional security models function based on believing their internal resources and assure that the users and devices, mainly considered assets are extremely trustworthy and faithful however this often may not be the case in today's advancing world of technology.

Intrusion Detection

IDS analyses network traffic and generates alerts when malicious activity is discovered. They are generally able to reset TCP connections by issuing specially crafted packets after an attack begins and some are even able to interface with firewall systems to re-write firewall rulesets on the fly(Abbas et al., 2023).

We can classify IDS into three types based on their detection properties:

1. Misuse Detection: Attack patterns or unauthorized and suspicious behaviours are learned based on past activities and these patterns are used to make predictions and detect similar patterns
2. Anomaly Detection: Monitors network traffic for deviations from normal behaviour patterns
3. Hybrid detection: Combines anomaly-based and misuse detection methods to improve the effectiveness of intrusion detection

   (Patel, n.d.)

Firewall

A Firewall usually behaves as a separating feature as well as a limiting device and an analysis component that has inbuilt features to become an anti-attack feature. It is manufactured in such a way that is as a first line of defence, It is assigned the duty of monitoring any traffic both incoming and outgoing (Wang, 2022). A firewall is an inline structure that is installed within a network and any traffic that needs to pass will only pass through this this allows the firewall to start its analysis and thereafter filter any data according to the predetermined criteria for the safety of the organisation.(DeCarlo & Ferrell, 2021).

A firewall comprises of a collection of components or a system that is placed between two networks and possesses the following properties:

1. All traffic from inside to outside, and vice-versa, must pass through it.
2. Only authorised traffic, as defined by the local security policy, is allowed to pass
3. through it.
4. The firewall itself is immune to penetration(Habtamu Abie, 2000).

5. A firewall monitors and restricts access by controlling protocols and services, it is responsible for the protection of the internal network and caters to logging and editing as well as VPN function.

We can broadly classify firewalls based on their primary functionalities

1. Packet filtering firewall.
2. Circuit-level gateway.
3. Application-level gateway, aka proxy firewall.
4. Stateful inspection firewall.
5. Next-generation firewall (NGFW)(DeCarlo & Ferrell, 2021).

Antivirus Tools

Computer viruses are executable code programs that have a unique ability to replicate themselves in computer systems and spread rapidly from one computer to another affecting files, documents and programs to alter their normal running. Viruses are represented as patterns of computer instructional codes that exist over time in computer systems. Antiviruses on the other hand are programs specially developed to counter challenges brought about by viruses as they protect the computer systems from virus attacks by heavily relying on the controls enhanced in their databases(Yusuf et al., 2017). It primarily functions by scanning identifying, and deleting suspected malware from the system and it improves its efficiency. Specially developed to counter challenges brought about by viruses, they protect computer systems from virus attacks by heavily relying on the controls enhanced in their databases(Yusuf et al., 2017). Typically, anti-virus could use a range of plausible solutions

such as scanning files and matching files to existing virus dictionaries/databases to find matches and identify unusual computer activity(Rohith Cheerala & Kaur, 2021).

Anti Malware tools

Malware is typically software that is utilised to monitor machine activities and in order to obtain access to a system. Malware is differentiated by its harmful expectation, which works in contradiction to the features of a computer client and does not include computer software whose deficiency produces unintentional harm(Azeem et al., 2024). Malware is generally divided into classes namely -

- Trojans: A vicious code that attaches itself to another code like a parasite and multiplies. Worms are self-replicating programs that wipe out or debase a computer's database.
- Spyware: It implants itself into the user’s database and starts monitoring activities without the knowledge of the user.
- Rootkit: introduce themselves as drivers or part modules, contingent upon the inside subtleties of a working framework's systems (Azeem et al., 2024).
- Botnet: A botnet is a collection of loosely connected programs. For any system structure, it is often a zombie program (worms, Trojans) running under ordinary resistors.
- Adware: Portrays itself as advertisements to users and appears seldom, like a spring, or once in a while in an enclosable window

Utilising anti-malware software ensures a variety of techniques to detect, quarantine, and remove malicious software (malware) from the system.

Defense-in-Depth

Defense-in-depth follows a layered approach to security that builds on traditional network security services. It enhances security through a variety of multiple defensive techniques rather than following a single line of defence(Defense in Depth: Stopping Advanced Attacks in Their Tracks, n.d.). Network segmentation plays a huge role in defence-in-depth. This technique involves the method of isolation of multiple segments of the network therefore preventing attackers from gaining access and freely wandering around the network from one part to another part of the network(Cisco, 2019). The defence in depth addresses security vulnerabilities in personnel, technology and operations, and this tactic was initially conceived by the National Security Agency (NSA) as a comprehensive approach to information and electronic security. Usually, a defence-in-depth approach may contain more than one of the following layers as mentioned below:

1. Physical security
2. Authentication and password security
3. Antivirus software
4. Demilitarized zones
5. Packet filters
6. Routers
7. Proxy servers
8. Virtual private networks
9. Logging and auditing
10. Biometrics
11. Timed access control

Zero Trust Security

The method helps read any exposure of internal data that could have been led to because of the presence of compromised accounts and network monitoring by malicious intended people or organisations and any other form of threats. Authentication is a positive approach towards security and is built into every step of access theatre internal or external(Qazi, 2022). Zero-Trust mandates strict authentication and authorization processes. Users and devices must be continuously verified through multifactor authentication (MFA), with access granted on a need-to-know basis. This limits the potential damage caused by compromised credentials or insider threats. (Gargan, 2024)

A few elements of the zero trust include:

1. Implicit trust region: Assuming threat lies within the organisation.
2. Bring your own device policies: The organization employs BYOD policies to accommodate guests, contracted services, and enterprise subjects who use personal devices
3. Security Policies: Security policy must be in compliance at all times even during the migration of assets.
4. Assumption of Untrusted Local Network: Remote enterprise topics and assets must assume that their local network connections are untrustworthy
5. Context-Responsive Access Controls: Certain access controls can leveraged based on device status, user roles, position, and potential risk factors.
6. User and Entity Behaviour Analytics: Use advanced analytics to analyse user and object behaviour, discovering patterns and detecting abnormalities (Dhiman et al., 2024).

Despite all the advantages and increase in the efficiency of security, it is often found transitioning to zero trust architecture is challenging and can be a long journey, some challenges include,

1. Vendor Lock-in: Traditional network protection providers may prevent users from leaving by imposing legal restrictions, technical barriers, or additional fees which can become overbearing to the user who wants to switch for better protection(*Vendor Lock-In*, 2020).
2. Industry Standards- Since the concept has not found a strong foothold in the security industry it is challenging to have a complete picture of whether the ZTA has successfully implemented it in their enterprises
3. Service Disruptions: Migration can lead to disruptions in the services offered by the organisations to the users or clients.
4. Integration Issues: Migrating to zero trust architecture is a complex adjustment and configuration.
5. Zta service controls: The zero trust platform consists of several intelligently supported systems to make an appropriate decision to grant users access.
6. Regulatory Compliance: Industrial or supervisory authorities regulate many enterprises, however, they may lack behind innovative technology solutions
7. Analysis Paralysis: An enterprise should thoroughly understand its technology and architecture requirements before implementing the zero trust architecture. (TEERAKANOK, 2023)

Based on the analysis of Traditional Network Security and Zero Trust, below is a table drawing comparisons between the two.

Classification	Traditional/InDepth	Zero Trust
Security Motivation	Permimeter-based security assumes threat lies only externally.	The threat lies both internally and externally
Access Control	Role Based	Constant Verification Protocol/Least Privilege
Authentication	One-time authentication to gain full access	Every step requires authentication.
Segmenting	Large segmentation - full access inside the perimeter	Granular segmentation. Access based segmentation
Threat Detection	Relies on Firewall, IDS, Antivirus and Anti-malware software	Real-time monitoring and analysis behaviour of individuals with access internally
Recovery Strategy	Depends on detecting when a breach occurs and recovering from it	Constantly assuming that breaches happen
Principle	Trusts within the perimeter are all safe and threat-free	Verification is mandatory for every access and activity. No Trust

Use Case	Legacy organisations and traditional IT industries.	Latest cloud-based/hybrid/remote organisations.

Conclusion

Traditional networks and Defense in Depth have always proven to be effective in their domain of protecting internal networks. However, with time adaptability is an essential feature considering the changing scenario in the domain of science and technology, and hence there is also a change in the way safety needs to be perceived, unlike earlier, with the fast-progressing world even risk of safety is fast changing and increasing and it is imperative to maintain a strong foothold in protecting our assets. This could be achieved by adopting the zero-trust feature whose foundation lies on real-time monitoring and analysis of behaviour and the basic notion for its motivation, i.e. breaches are prevalent at all times. In conclusion, it is advisable for organisations to adapt and incorporate zero-trust network security practises besides the traditional network security strategies, by doing so they will have a strong unshakable structure of security that better prepares the organisation to protect its assets and data from both external and internal threats.

References

Abbas, S., Khuder, A., & Abbas, A. (2023, February 28). *Subject review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)*. ResearchGate; unknown. https://www.researchgate.net/publication/368928254_Subject_review_Intrusion_Detection_System_IDS_and_Intrusion_Prevention_System_IPS

Azeem, M., Khan, D., Iftikhar, S., Shaikhan Bawazeer, & Alzahrani, M. (2024). Analyzing and comparing the effectiveness of malware detection: A study of machine learning approaches. *Heliyon*, *10*(1), e23574–e23574. https://doi.org/10.1016/j.heliyon.2023.e23574

Cisco. (2019). *What Is Network Segmentation?* Cisco. https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html

cyber_pix. (2024, September 26). *Connecting the Dots: Zero Trust and Traditional Network Security*. Medium. https://medium.com/@use.abhiram/connecting-the-dots-zero-trust-and-traditional-network-security-c8395ea7391b

DeCarlo, A. L., & Ferrell, R. G. (2021a, January). *The 5 Different Types of Firewalls Explained*. TechTarget. https://www.techtarget.com/searchsecurity/feature/The-five-different-types-of-firewalls

DeCarlo, A. L., & Ferrell, R. G. (2021b, January). *The 5 Different Types of Firewalls Explained*. TechTarget. https://www.techtarget.com/searchsecurity/feature/The-five-different-types-of-firewalls

Defence In Depth: Stopping Advanced Attacks in their Tracks. (n.d.). Exabeam. https://www.exabeam.com/explainers/information-security/defense-in-depth-stopping-advanced-attacks-in-their-tracks/

Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U., & Hamid, Y. (2024). A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. *Sensors*, *24*(4), 1328. https://doi.org/10.3390/s24041328

Gargan, R. (2024). *How the Zero-Trust Principle Applies to Data Security*. Netmaker.io. https://www.netmaker.io/resources/zero-trust-data-security

Habtamu Abie. (2000, December 23). *An Overview of Firewall Technologies*. ResearchGate; unknown. https://www.researchgate.net/publication/2371491_An_Overview_of_Firewall_Technologies/link/02e7e5240fd612164d000000/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19

Patel, A. (n.d.). *Detecting Intrusion - an overview | ScienceDirect Topics*. Www.sciencedirect.com. https://www.sciencedirect.com/topics/computer-science/detecting-intrusion

Qazi, F. A. (2022). Study of Zero Trust Architecture for Applications and Network Security. *2022 IEEE 19th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET)*. https://doi.org/10.1109/honet56683.2022.10019186

Rohith Cheerala, & Kaur, G. (2021, April 28). *A Comprehensive Study on Malware Detection and Prevention Techniques Used by Anti-Virus*. ResearchGate; unknown. https://www.researchgate.net/publication/352137349_A_Comprehensive_Study_on_Malware_Detection_and_Prevention_Techniques_used_by_Anti-Virus

TEERAKANOK, S. (2023, April 31). *IEEE Xplore Full-Text PDF:* Ieeexplore.ieee.org. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10052642

The Perimeter Problem: Why Traditional Network Security Fails. (2023). Pomerium. https://www.pomerium.com/blog/the-perimeter-problem

Vendor lock-in. (2020, July 23). Wikipedia. https://en.wikipedia.org/wiki/Vendor_lock-in

Verma, S., & Student. (2023). Redefining Network Security: A Comparative Study Of Traditional And AI-Driven Approaches. *Redefining Network Security: A Comparative Study of Traditional and AI-Driven Approaches*, *11*(Issue 12 December 2023), 2320–2882. https://ijcrt.org/papers/IJCRT2312852.pdf

Wang, P. (2022, December 26). *Research on firewall technology and its application in computer network security strategy*. ResearchGate; Darcy & Roy Press Co. Ltd. https://www.researchgate.net/publication/367103503_Research_on_firewall_technology_and_its_application_in_computer_network_security_strategy/link/63c15cf8d7e5841e0bc63d54/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19

Yusuf, M., Neyole, W., Jacob, M., & Neyole Misiko. (2017). *Review of Viruses and Antivirus Patterns*. ResearchGate; Springer Nature. https://www.researchgate.net/publication/322552067_Review_of_Viruses_and_Antivirus_Patterns/link/5a5f6456458515b4377966be/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uRG93bmxvYWQiLCJwYWdlIjoicHVibGljYXRpb24ifX0