iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** I **Month of publication:** January 2024

DOI: https://doi.org/10.22214/ijraset.2024.58201

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue I Jan 2024- Available at www.ijraset.com

Enhanced Zero Trust Implementation - A Novel Approach for Effective Network Policy Management and Compliance Tracking

Arya Gokhale[1], Siddhivinayak Kulkarni[2]
Student of Computer Science and Engineering, MITWPU, Pune, India; #Faculty at School of Computer Engineering and Technology, MITWPU, Pune, India

Abstract: ***The Zero Trust network architecture is an embodiment of the Zero Trust security model, and is progressively being utilized for the improvement of security standards of the current security infrastructures. Fine-grained access control is one of the primary principles of developing zero trust solutions, in which it is expected to manage an overwhelming amount of security policies. Managing the compliance of policies at fine grain level is thus necessary for utmost security stature. This paper aims at developing a novel approach to improve the task of policy management workflow and compliance tracking.***
Keywords: Zero trust; zero trust network architecture; security policy; policy management; policy compliance; role based access control

I. INTRODUCTION

The traditional model of the network infrastructure i.e. the perimeter based network was built with the outside- in approach. Here the internal components of the network were considered trustworthy and security practices were applied on the network's edge. There has been an escalated migration of resources to the cloud with the increased use of service models which are hosted on cloud which include Infrastructure as Service (IaaS), Software as Service (SaaS) and Platform as Service (PaaS). Furthermore, with Covid-19 we witnessed that company ecosystems broadened and perimeters of institutions upscaled with the incorporation of work from home. As a result, public and private organisations need to rethink how to protect their IT infrastructure, assets and data better [1]. Today's businesses need to enhance their security via quick adaptation to the challenges of modern perimeterless network security [2]. As a result, the network topology has become more dynamic, making the perimeter based network security unsuitable. Additionally, when an attacker infiltrates through the network perimeter lateral movements can be performed in unrestrained fashion.

In order to cater to modern-day organisations' needs, an improvised solution is needed. A holistic approach for an advanced secure network model that has security at its core rather than an afterthought. One such proposed solution that has taken great notice is the Zero Trust security model.

The National Institute of Standards and Technology (NIST) further elucidates about the Zero Trust with its operational definition, explaining that it is a concept rather than fixed implementation practice. It is modeled to, "reduce uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised"[3].

It is a cybersecurity paradigm aiming at a holistic approach to securing a network, data and devices. Thus the network is considered to be perpetually compromised, this consideration is necessary for eliminating the trust factor from the network. It is thus expected that we must verify and secure all resources, limit and strictly enforce access control, and inspect and log all network traffic[4]. Rather than granting prejudged trust to the system components, fortification of the network is done by continuous verifying and diagnosis of the digital interactions. It adopts the concepts like least privilege access and role-based access control of the conventional security models, leveraging them by using a more fine-grained approach. This is executed by inculcating identity-centric (user and device identity) and context-specific policy implementation. By compartmentalising the system and giving least privilege access it tries to limit the infiltrators' attack surface.

II. TENETS OF ZERO TRUST

A. Considering All The Devices And Data Centers As A Valuable Resource

Enterprise resources and networks are availed by a varied pool of devices, from enterprise-authorised devices to personal machines, from on-premise data centres to cloud data centres.

The scope of cybersecurity controls is not limited to protecting perimeter networks, but the demand for fluid data requests forces Cyber practitioners to be everywhere. Hence safeguarding infrastructure and data is critical for successful operational business [5].Thus protecting access via all devices is a prerequisite for securing the enterprise.

B. The same security standard applies to all devices regardless of their location

Considering the trend of Bring Your Own Device (BYOD) and the use of VPNs, location is no longer a safe parameter to assess a device or user's security posture. Security policies are far less likely to be enforced on machines the company doesn't own [6]. With BYOD we expose ourselves to another attack surface, thus once data is transferred to a network entity that an organization doesn't control or monitor, it is at risk. Understanding this is important for developing a more integrated security system.

Thus be it an on premise enterprise asset or an off-premise asset all the users or devices should meet the same standard of security. Trust is not implied based on the location of the requestor or the resource being requested. Further by disregarding the inherent trust the security posture of the network can be improved.

C. Session-based grant for resource access

Granular access control is possible by granting access to particular resources per session. Previous resource access does not guarantee the expected security posture of network assets, validation and verification per session for the same is hence crucial. Some of the ways of limiting access privileges to resources are:

- Session-based-role-based (the role of the requestor acts in context to analyse the validity of the request)
- Session-based-attribute-based (the attributes of the subject and sometimes the systems environment are also considered)

D. Resource access control

Resources of an organisation are segregated and access to them is defined based on the identity of the device or individual, roles and attributes. Network environment and device specification dictates the resource access policies. The security posture of a network environment is transient thus the policies adapt to such changes to ensure the system's resilience. Device and user-specific analytics are necessary to further upgrade the policies.

E. Continuous evaluation of the security status of all the system assets

All the assets and users of the system are monitored persistently. Prior analysis of the security posture is evaluated before addressing the resource request. Continuous Diagnostics and Mitigation (CDM) is used to automate real-time monitoring, vulnerability detection and risk analysis, thus enhancing Network Security Management.

F. Continuous authentication and authorisation of assets based on dynamic policies

Continual authentication of assets and users to identify and alleviate potential threats. In addition to that, the authorisation of resources is based on relevant dynamic policies. Reauthentication and reauthorisation are carried out after the identity session expires. Multifactor authorisation can be applied for enhanced security. Identity provider (IdP) is a trusted third-party system component that chiefly provides authentication services. It also creates, maintains, manages and logs identity information for network entities. To eliminate the limitations of the legacy systems and VPN's identity management systems can incorporate Identity Providers (IdP) along with context based access policies. The threat response mechanism is implemented as contextual policy rules, which are then applied to the information system when contexts become active [7].

G. Comprehensive network asset data collection:

For maximum control of the network transparency and accessibility of all the assets of the network system is necessary. Continuous collection of events and the state of assets helps in User and Entity Behavior Analytics (UEBA).Currently, preventive measures like Firewalls are not 100% fool proof. Hackers & attackers enter the system at any point, hence the need for the detection is very important for minimal damage [8]. Furthermore, this ensures early detection and appropriate response to potential threats and attacks.

III. ZERO TRUST AS AN EVOLVING SOLUTION

In 2010, John Kindervag popularized the term "Zero Trust" by proposing that organizations should not inherently trust their network systems.

He highlighted the flaw in traditional network architecture where security is treated as a mere "blanket" rather than a core component. As a result, security is often neglected and considered an afterthought. To address this, the Zero Trust architecture emphasizes network segmentation, parallelization, and centralized management.

The key highlights of the proposed Zero Trust architecture comprise the following components:

1) *Network Segmentation Gateway:* This gateway combines essential security features and functionalities of the network, such as firewalls, VPN gateways, intrusion detection systems (IDS), and network access control (NAC). By consolidating these functions into a single enforcement point, it enables centralized management of security solutions, ensuring compatibility and reduced complexity.
2) *Multicore and Microperimeter:* The components of the network segmentation gateway are further grouped based on shared resource similarities, which helps in adopting a resource-centric security approach. These groups form microperimeters governed by tailored local policies. This effectively isolates the different parts of the network, thus reducing the attack surface.
3) *Centralized management:* Traditional hierarchical networks use inflexible switch infrastructure, making it difficult to modify and adapt to new security controls. Zero Trust (ZT) networks incorporate unified management of Microsegmentation and Continuous Adaptive Risk and Trust Assessment (MCAP) components.
4) *Data acquisition network (DAN):* Unlike traditional LAN and WAN architectures, DAN is a specialized network designed to capture and analyze real-time network data. It pools all network packets, syslog, and SNMP messages to a single location for inspection. The segmentation gateway plays an important role in data acquisition as it bridges all the MCAPs, making it a perfect point for collecting network traffic.

A. Zero Trust Network Architecture

The network infrastructure designed based on the principles of the ZT security model is Zero Trust Network Architecture (ZTNA).

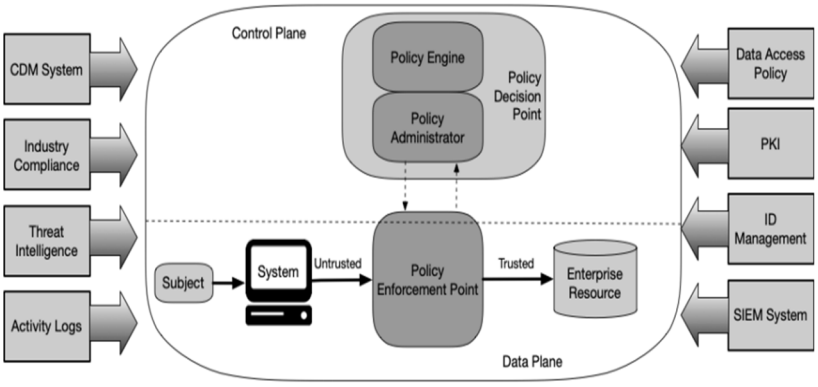


Fig. 1 Diagrammatic representation of the logical components proposed by NIST

A new paradigm in networking, software defined networking (SDN), advocates separating the data plane and the control plane [9], thus the network architecture is divided into two logical planes. Data plane manages all the application data traffic and the control plane shells the components that handle the process of continuously monitoring the network assets and their requests.

The Policy Engine (PE) is the brain of the control panel which makes ultimate decisions regarding enterprise resource access. It does the job of creating, modifying, monitoring and enforcing dynamic policies. Access is consequently granted, denied, or revoked based on the security parameters defined by the policies. The final decision is then passed onto the policy administrator to execute the decision [10].

The Policy Administrator (PA) in conjunction with the PE and is responsible for managing session specific authentication. The devices and assets are not trusted and can access the resources via the Policy Enforcement Points (PEP).

PEP acts as a portal for communication of all the requests between the data plan clients with the control plane. PEP monitors, enables and disables the connection between network assets and the enterprise resource pool. The session's authorization is examined for its validity by the PE. Based on the decision made by the PE, PA guides the actions of PEP.

These policies are modified based on input from components such as Continuous Diagnostic and Mitigation (CDM) and Threat Intelligence systems. The inputs from these sources help in calculating the confidence level and risk score for each asset.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue I Jan 2024- Available at www.ijraset.com

B. Forrester Zero Trust eXtended (ZTX) Model

Today more than ever enterprises deal with a colossal volume of data, thus in today's business world, data is the number one commodity. Enterprise Data Management (EDM) has become increasingly complex considering the multifariousness options used for data storage, processing and accessing. Thus securing these data centres has become a priority.

On August 11 2020, Forrester released the Zero Trust eXtended model. A model that is a cornerstone for the data-centric approach of Zero Trust.

Fig. 2 Zero Trust eXtended model

It is an overarching approach to considering the entire digital ecosystem of an enterprise. A network comprises various components that act as extensive data producing channels, thus securing them becomes requisite. These components are not implicitly trusted, but are subjected to Zero Trust policies and principles.

1) *Data:* Classifying and tagging data is a crucial step for identifying low, moderate and high value data. Further tagging the data helps to couple the appropriate identity based and context specific access policies. Data can be available in structured or unstructured format. Unstructured data does not fit a particular schema as opposed to structured data. Thus the security specifications are not apparent, making it relatively challenging to apply security policies to unstructured data.
   Data can be found in motion when transferred, at rest when unaccessed, or actively used. It can have varying vulnerability levels in these stages, to ensure the utmost security Data Loss Prevention (DLP) is incorporated. DLP helps with, monitoring, detecting and blocking sensitive data while in use (endpoint actions), in motion (network traffic), and at rest (data storage).” 12
   When in motion it is prone to man-in-the-middle attacks that are mitigated through ZTX as continuous authentication makes it harder for the attacker to masquerade as a legitimate user.
2) *Workload:* It comprises all the computing resources and processes that an application requires to function. All the resources including the client-facing, i.e. the front end or the backend business-driven systems. Workloads include a range of system components from virtual machines, and containers to multi and hybrid cloud based data centres.
   In perimeter-based technologies, interactions between data centers and the rest of the network, such as client-server traffic, are generally monitored by firewalls. However, the components inside the perimeter and the implicitly trusted traffic within these workloads remain unattended. To address this inconsistency in inspecting traffic security, workloads are considered potential threats, and granular access policies are applied to them.
3) *Network:* Segmentation of the network isolates different workloads from one another. It gives granular control over the access control policies employed on each segment giving more control over the administration of traffic between subnets. Network performance is enhanced by keeping unwanted access at bay, allowing only the authorised flow of traffic and localising the technical problems in a segment.
   Microsegmentation is a security method to logically divide the network further isolating and managing the interactions between workloads. It limits the lateral movement of a malicious attacker and reduces the attack and impact surface. It helps in managing the inter-workload communication by mitigating implicit trust between them.

4) *Devices:* Network infrastructure devices are the components of a network that transport communications needed for data, applications, services, and multimedia [13]. With the advent of IoT devices the nexus of network devices have proliferated. These devices have expanded the attack surface and thus have become a common target for attackers.
Controlling access to the network via monitoring the credentials and configurations of IoT devices is simplified using a zero trust management model. With the aim of achieving Zero Trust, these devices need to be isolated, identified, monitored and controlled continuously [14].
5) *People:* In the line of defence against compromised enterprise resources, Monitoring and controlling the actions of the network users becomes crucial. Identity and access management (IAM) framework incorporates role based and attribute based access control systems. Along with Single Sign On (SSO), MFA and biometrics, it forms a rigorous security landscape.
6) *Visibility and analytics:* In order to alleviate threats, visualisation and analysis is important. Conventional security analysis platforms like Security Information and Event Management (SIEM) supplemented with advanced solutions like UEBA and Security orchestration, automation and response (SOAR). Systems are made resistant to attacks by continuously fathering log and event data from endpoints. Followed by anomalous behaviour detection for accurately detecting compromised users and entities. Real time reporting and incident handling, thus instrumenting a zero time response to threats.
7) *Automation and orchestration:* ZTX is a dynamic and decentralised ecosystem, to support this architecture automation of manual processes is necessary. This would lead to a more consistent security infrastructure. Moreover, automation reduces the complexity of orchestrating streamlined updates. Thus, zero time response to threats is obtained.

IV. METHOD

ZTNA is the manifestation of the policies designed to implement fine grained control and access to resources. As policy enforcement is essential for meticulous security control, managing the enforcement of security policy across the board is crucial.
Current software tools for network security policy management provide ways for assessing compliance with policies being implemented. Most businesses are incorporating these tools to automate policy compliance, thus there is a need for deriving security policies based on business policies and rules. While presently embodied software tools are effective in meeting multiple use cases across the hybrid plane of networks, an additional utility for reshaping business rules into security policies would be beneficial.
Often silos tend to form within organisations, where different teams manage various products. Each team has their own management consoles and ways of keeping track of applications, and compliance with policies on the same. The proposed solution aims to displace this obfuscation between different teams working in an organisation, thus a security solution must incorporate a more inclusive approach that caters to all of the needs of various teams working in an organisation.
The following proposal attempts to resolve the complexity of policy management, application and compliance:

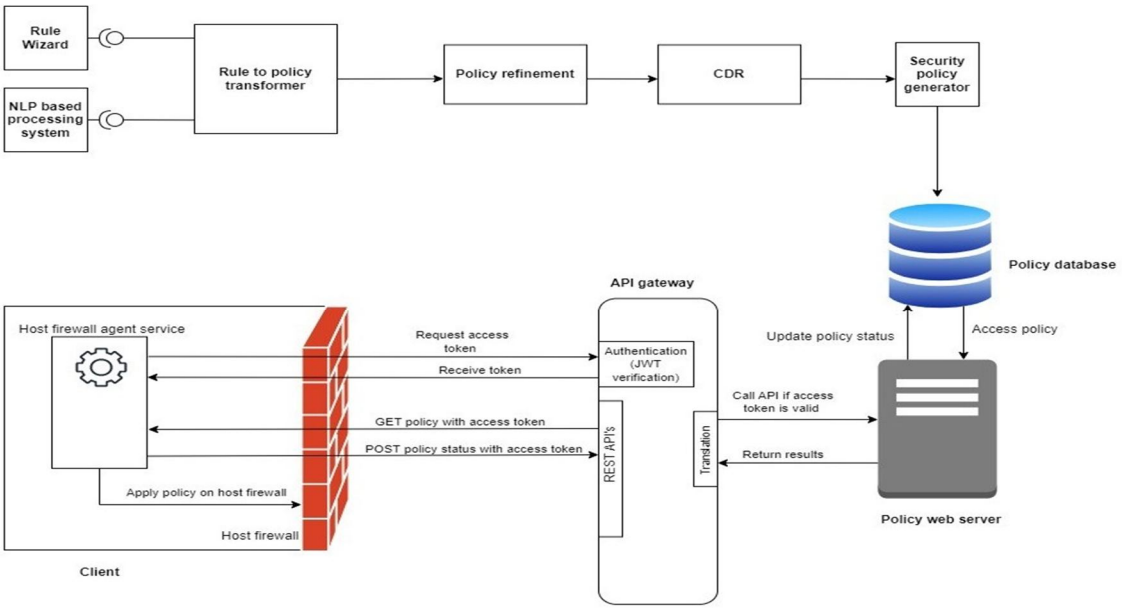


Fig. 3 Zero Trust dynamic automated policy generation, management and compliance tracking solution

Policy-based network management (PBNM) bridges together business functionalities and their requirements with how the network security needs to model accordingly. PBNM solutions require information models that contain business and system entities that can be easily implemented [15].

1) *Rule to policy transformer:* At the highest level, policy management must be considered from a business perspective[16]. Business rules are at the core of formulating security policies. This understanding is fundamental to a managed policy framework for the enterprise network [16]. A rule-to-policy transformer would encompass a method to transform business rules into security policies. A user interface in the form of a wizard can be designed to gather detailed information about business rules. NLP based systems can also be implemented in which rules in human textual language are processed.
2) *Policy refinement:* A process used to extract information from the business rules, which includes details regarding the attributes, constraints and resource requirements. This would help in transforming high level rules into more concrete low level policies.
3) *Conflict detection and resolution:* One aspect of policy-based networking that does not seem to be receiving much attention is the verification of policies that are going to be applied to the network. [17]. With hybrid networks with complex topologies, policy suits get augmented over time. In an organisation different teams have various goals to satisfy with their development and their security constraints can differ. Thus many underlying policies developed in this process offset each other making them redundant. Managing the correctness of the policies across the board is necessary so that they comply to satisfy their overall intended goal.
4) *Security policy generator:* Restructuring rules as policies which are structured following a template. Modelling policies based on template makes managing a wide range of policies easier.
5) *Policy database:* Stores policies and related data along with the policy status attribute which is associated with each policy which stores information regarding implementation status. A web server serves as a medium to access applicable policies for various clients. The input from the user is evaluated by the server with respect to the policy definitions and its corresponding supporting data. Decisions based on these evaluations are passed down as a response.
6) *API gateway:* Data required by different clients may vary and handling client interactions for specific services from servers can get complex, API gateway acts as a single entry point for all clients. Authentication of clients through the gateway via JWT tokens for verifying incoming requests from clients before calling and passing requests to corresponding APIs at the backend. Clients can communicate via REST APIs which use a request-response model. Translation of these requests can be done to backend-specific protocols.
7) *Client:* The client is a representative component of any network endpoint, it can be a network firewall, Security and Information Management (SIEM) tools, Domain Name System (DNS), proxies or personal devices.
8) *Host firewall agent service:* It is a background service/daemon that runs on client-side devices. It manages client-side authentication and request dispatch. Based on the response received from the server side it manages the adjustments of host firewall configurations.
9) *Host firewall:* It is a software-based firewall residing inside a device rather than a network. To improve security posture the host firewall agent service can exercise programmatic changes in the configurations of the host firewall. This device level changes give granular control over controlling the device level and network traffic.

Additionally, a centralised dashboard can be generated that collects feedback in a single pane of glass. It would be an aggregated view to evaluate the overall state of policies applied by various teams. This would resolve the issues created by the silos in an organisation, even with limited communication between teams, policies applied across the board would remain correct and consistent.

Frequent changes in business rules change the conditional policies built on them. Capturing the essence of business rules by modelling security policies on them is essential for abiding by organisational goals. The key is to consider these rules and construct consistent logic models that precisely represent the rules. Because meta-data reflects business information requirements, any system designed to process the meta-data will consequently meet those requirements [18].

- Business rules should be maintained in an ordered and well-structured rule base for efficient access. Business rules should elucidate all the business requirements, entities involved and their relationship along with their attributes.
- Effective extraction of qualitative and quantitative metadata can thus be done out of simple business statements.
- With this extracted metadata changing business rules into logical components can be done. These logical components can be further refined to transform them into security policies.

By taking an example of an organisation's business rule, we can further understand the implementation flow. Business rules are formulated to regulate access to an organisation's resources. Here is one such example:

"Interns cannot access the source control system after 5 pm."
This is an operational business rule which can be adapted as a security policy by drawing out the logical model from the statement. The business rules are processed to find the metadata using policy refinement techniques as stated before:

- We analyse the entities or actors in this rule, they are the interns and the source control system.
- We explore the attributes of these actors. These attributes can also be hierarchically structured values or instances. Here the actor should be an intern for this rule to be applied.
- We then explore the restraining parameters. Post 5 pm none of the interns can access the source control systems, thus our restrain parameter becomes time and the value it cannot exceed is 5 pm.
- Entity association is drawn out further, here the intern is related to the source control system based on the project designated to him or her.
- This metadata collected is used for formulating rule expressions which encapsulate the logical component of business rule. Here role-based access rules can be applied where time becomes our restraining parameter that governs the access right for the project database to the interns.

With the profuse amount of policies generated exception handling and conflict detection and resolution are performed over suites of policies to maintain their compatibility. The logical components generated before are utilised to generate a template for standardising policies that comply with the organisational standard of security and data protection standards.
Even with any modification in business standards and rules, the underlying metadata entities remain the same, the parameters for which may get altered. Thus, we can get a systemized and persistent approach to developing and security policies that are commensurate with the overarching business rules.

V. IMPLEMENTATION

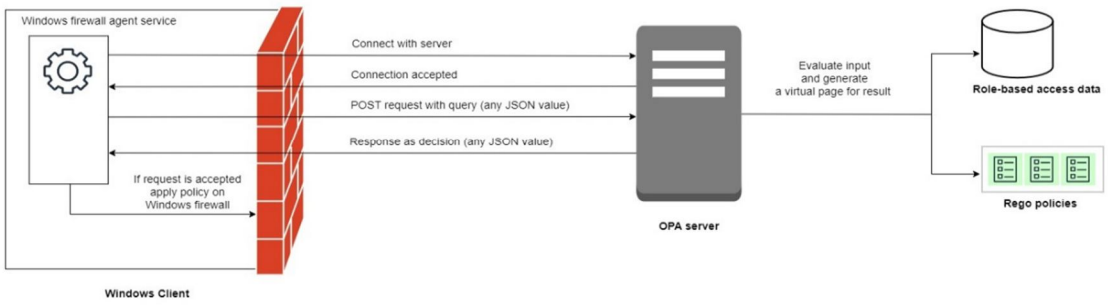


Fig. 4 Proof of concept for Zero Trust policy management and compliance tracking on local machine

We have implemented the proposed solution with whitelisting applications as our use case. We have developed a role based access control system where each user has a role assigned and each role has corresponding permission for approving certain applications to be active on their device. The policies are developed to evaluate input and grant or deny the requests. This implementation is done locally in a Windows environment.
Windows client is a Windows device, which has a Windows firewall agent service running in the background. This is the host firewall agent service as proposed in the solution. It is configured with the Windows Firewall with Advanced Security using its APIs. As, host-based microsegmentation can be implemented using software agents on the endpoint artifacts (e.g. servers). It leverages native firewall functionality built into the host [19].
For generating and maintaining policy and its related data, Open Policy Agent (OPA) has been used. OPA separates the policy from the service code thus making the task of policy creation and implementation independent of each other. In OPA policies are written as code using high level language Rego.

We can upload policies and required data on OPA's server running on port 8181. The data contains information about different roles and permitted applications to be active and whitelisted for each role.

The Windows firewall agent service can query OPA locally via the CRUD endpoints exposed by OPA REST API. The service sends a POST request with some JSON input which contains details about the application to be whitelisted. The OPA server evaluates the request made based on the policies and data provided and sends back the result of the evaluation. If the evaluation results in allowing the whitelisting of an application then the configurations in Windows Firewall are altered to whitelist the application.

VI. ADVANTAGES AND DISADVANTAGES

A. *Advantages*

1) *Strictly monitored user authentication and access control*: Usernames and passwords are vulnerable to attacks, for preventing bad actors from infiltrating the system ZTNA incorporates two factor or multifactor authentication. This ensures the utmost security posture while relaying authentication not just on user credentials but multiple other security factors.
With the least privilege access at the core of implementing ZTNA, resources are secured from unwarranted access. Further, this also prevents the spread of malware as allocation and access to resources is restricted.
2) *Segmented approach:* Microsegmentation helps in better compliance with applied security policies in a particular sub-network region. Furthermore, it improves the performance of each sub-network as performance as monitoring and control of subsystems get optimised.
3) *Security at application and user level:* Instead of applying security measures just at the perimeter, we move it to the core of network assets. This helps in gaining more access to the network and thus improving the visibility of the network components, logging network traffic and troubleshooting. While implementations vary, the concept zero-trust imposes controls to lie close to applications and users rather than in the network infrastructure[20]. Thus constraints embody the fundamental essence of the security notion at device level rather than network level. Assuming controls lied on in the organization's network framework, the extra intricacy would burden the network layers.
4) *Data-centric security:* Total data control by protecting all the data points in a network, which includes enterprise resources, personal devices and private apps.
5) *Continual security posture analysis:* The security posture of the networks is continuously monitored. As trust is not implicit real time incessant trust assessment of network components is performed. Additionally, continual threat assessment is done to monitor the security stance while detecting and preventing any possible threats.

B. *Disadvantages*

1) *Time and resource extensive:* Making the shift ZTNA from a traditional parameter based network security structure requires fundamentally restructuring an organisation's network system. This shift requires analysis of pre-existing systems and compatible finding ZTNA deployment solutions. Additionally, to handle such mature security models and their computational power, the resource requirements assuredly increase. To simplify this process CISA provides Zero Trust Maturity Model, which further elaborates on the different stages of maturity of ZT solutions.
2) *Complex system management:* ZTNA solutions modelled perform complex functionalities. With a broadened implementation surface for these solutions controlling and managing these systems gets intricate.
3) *Data security issues:* With deep packet analysis and detailed examination of user generated data, privacy and legal issues are raised. Users are reluctant to safeguard data, but there is ambiguity when it comes to predicting the level to which user data is accessed and assessed. Thus, when it comes to potential end user related concerns, practitioners acknowledge that zero-trust leads to new challenges concerning data security and regulation, since all traffic is examined [21].

VII. DISCUSSION

Investing in next generation cybersecurity solutions is essential for maintaining the business and security standards of an organisation. In 2021 in the "Executive Order on Improving the Nation's Cybersecurity", President Joe Biden addressed the need for incorporating zero trust as the key element for developing a resilient system to face ever increasing sophisticated cyber threats.

Many businesses came up with advanced security solutions which align with the framework developed by NIST for the implementation of Zero Trust Architecture (ZTA). Google developed BeyondCorp which targeted securing remote working. Furthermore, ZTNA is incorporated in the Secure Access Service Edge (SASE) solutions which is an integrated security service.

This pairing is crucial for managing policy enforcement across the entire network infrastructure, access control management and preventing data breaches.

"However, deploying ZTA is complex from both the technical and organizational points of view as ZTA makes security management much more complex than already is."[22]

The complexity of policy management increases with the fine tooth approach of network analysis, having a systematic approach to handle this complexity is crucial for optimal ZTA implementation.

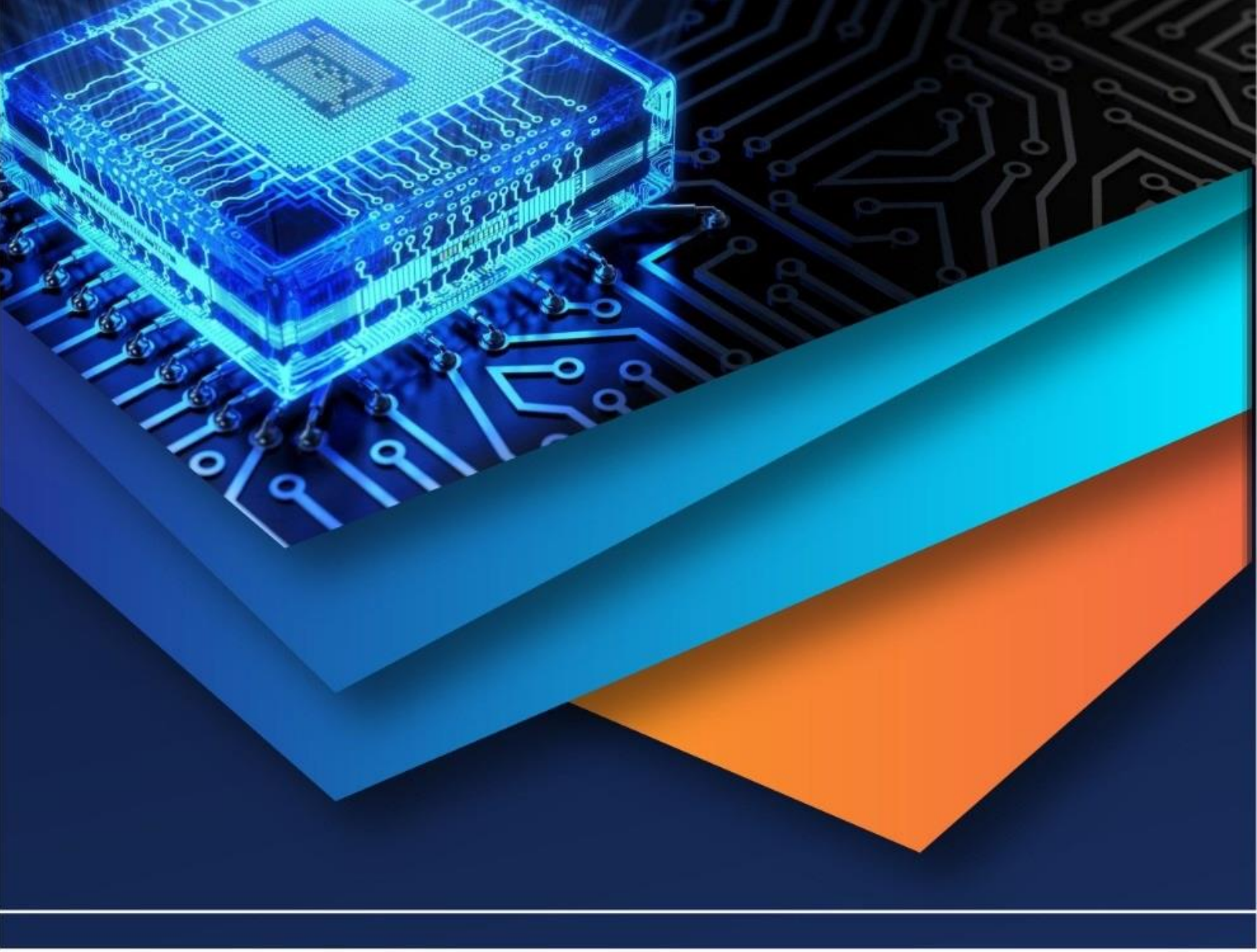
For organisations aiming for incorporating ZTNA, CISA provides maturity models for a smooth transition from current network design towards zero trust. CISA bases its maturity on five pillars which includes identity, device, network, application workload, and data. As the model maturity increases, we move towards a more automated approach of handling system controls along with managing dynamic security policies.

VIII. CONCLUSION

In this paper, we discussed ZTNA and how implementation and efficient management of security policies are essential for developing a secure ZTNA model. We aimed at incorporating various research guidelines and analysing research gaps and business needs for modelling an optimal solution. We developed an architecture which aids in the transformation of business rules and developing dynamic security policies out of them. This helps in enhancing the policy management and compliance tracking process which is critical for maintaining fine gained control over the network.

REFERENCES

[1] http://resolver.tudelft.nl/uuid:fe96c8fb-2d9a-4c6e-8e5e-d526c6ec6733 (referred on: 14/02/2023)
[2] Natalia Miloslavskaya,Security Zone Infrastructure for Network Security Intelligence Centers, Procedia Computer Science, Volume 169, 2020, Pages 51-56, ISSN 1877- 0509, https://doi.org/10.1016/j.procs.2020.02.113.
[3] Rose, S. , Borchert, O. , Mitchell, S. and Connelly, S. (2020), Zero Trust Architecture, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800- 207, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=930420 (Accessed February 17, 2023)
[4] Kindervag, J., 2010. Build security into your network's dna: The zero trust network architecture. *Forrester Research Inc*, *27*.
[5] Kak, Sanjay. *Zero Trust Evolution & Transforming Enterprise Security*. Diss. California State University San Marcos, 2022.
[6] K. W. Miller, J. Voas and G. F. Hurlburt, "BYOD: Security and Privacy Considerations," in IT Professional, vol. 14, no. 5, pp. 53-55, Sept.- Oct. 2012, doi: 10.1109/MITP.2012.93.
[7] Debar, H., Thomas, Y., Cuppens, F. *et al.* Enabling automated threat response through the use of a dynamic security policy. *J Comput Virol* 3, 195–210 (2007). https://doi.org/10.1007/s11416-007-0039-z
[8] Babu, Shekar. "Detecting anomalies in Users-An UEBA approach." *Proceedings of the International Conference on Industrial Engineering and Operations Management*. 2020.
[9] Kim, Hyojoon, and Nick Feamster. "Improving network management with software defined networking." *IEEE Communications Magazine* 51.2 (2013): 114-119. doi:10.1109/MCOM.2013.6461195
[10] F. A. Qazi, "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), Marietta, GA, USA, 2022, pp. 111- 116, doi: 10.1109/HONET56683.2022.10019186.
[11] Cunningham, C., 2018. The Zero Trust eXtended (ZTX) Ecosystem: Extending Zero Trust Security Across Your Digital Business. *Cambridge, MA*.
[12] https://en.wikipedia.org/wiki/Data_loss_prevention_software (referred on: 10/02/2023)
[13] https://www.cisa.gov/uscert/ncas/tips/ST18-001 (referred on: 21/01/2023)
[14] Samaniego, Mayra, and Ralph Deters. "Zero-trust hierarchical management in IoT." *2018 IEEE international congress on Internet of Things (ICIOT)*. IEEE, 2018. doi:10.1109/ICIOT.2018.00019
[15] Strassner, John, and John S. Strassner. Policy-based network management: solutions for the next generation. Morgan Kaufmann, 2004.
[16] https://www.osti.gov/servlets/purl/920772 (referred on: 03/03/2023)
[17] Stone, Gary N., Bert Lundy, and Geoffrey G. Xie. "Network policy languages: a survey and a new approach." *IEEE network* 15.1 (2001): 10-21. doi:10.1109/65.898818
[18] https://www.researchgate.net/publication/3863706_Business_rulesmeta-data Perkins, Alan. (2000). Business rules=meta-data. 285-294. 10.1109/TOOLS.2000.868979.
[19] Chandramouli, Ramaswamy. *Guide to a Secure Enterprise Network Landscape*. No. NIST Special Publication (SP) 800-215 (Draft). National Institute of Standards and Technology, 2022. doi: https://doi.org/10.6028/NIST.SP.800-215
[20] Banyan. BeyondCorp for the Enterprise. Banyan; 2019. https://info.banyansecurity.io/beyondcorp-for-the-enterprise (referred on: 01.03.2023)
[21] Buck, Christoph, et al. "Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust." *Computers & Security* 110 (2021): 102436. doi: https://doi.org/10.1016/j.cose.2021.102436
[22] E. Bertino, "Zero Trust Architecture: Does It Help?" in IEEE Security & Privacy, vol. 19, no. 05, pp. 95-96, 2021. doi: 10.1109/MSEC.2021.3091195



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY