Methodology of network infrastructure analysis as part of migration to zero-trust architecture

Roman Syrotynskyi[1,†], Ivan Tyshyk[1,†], Orest Kochan[1,†], Volodymyr Sokolov[2,†] and Pavlo Skladannyi[2,*,†]

[1] Lviv Polytechnic National University, 12 Stepana Bandery str., 79000 Lviv, Ukraine
[2] Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine

Abstract

The limitations of traditional security models are becoming increasingly apparent in the face of new cyber threats and the growing complexity of the network environment. Traditional security approaches, often based on perimeter defense, heavily rely on the assumption that threats originate outside the network and that internal entities can be trusted. This assumption is no longer valid, as modern threats frequently bypass perimeter defenses and exploit internal vulnerabilities. Moreover, the rise of remote work, cloud computing, and the proliferation of mobile devices have expanded the attack surface, making it difficult to ensure comprehensive protection with traditional models. To further enhance the security level of an enterprise's network infrastructure, there is a need for a transition to a zero-trust (ZT) architecture, which requires a thorough methodological analysis of the existing network infrastructure and its information assets. There is a noticeable dependence on the implementation of the fundamental principles of ZT and the effective iterative implementation of the new security model on the transparency of the network structure, the assets involved, and the overall implemented information security policy. This paper presents a comprehensive methodology for analyzing an enterprise's network infrastructure, which is a critically important component in the process of implementing a ZT architecture. The structure of the stages for assessing the security model of the network infrastructure and the enterprise security model has been formed. Approaches and practices for implementing measures aimed at obtaining the necessary information are described, and key data for forming reports and documenting results are proposed. The proposed methodology includes detailed asset identification, mapping data flows, and application inventory, as well as a rigorous assessment of user access and behavior. By systematically evaluating each aspect of the network, organizations can identify vulnerabilities, develop a micro-segmentation strategy, enhance access controls, and align their security policies with ZT principles.

Keywords

zero-trust architecture, network assessment, NIST, access evaluation, network inventory, least access, data flow, user access, network host

1. Introduction

In the landscape of modern cybersecurity, the transition to a ZT architecture marks a significant turning point in moving away from traditional network security models. Based on the fundamental principle of "never trust, always verify", ZT architecture inherently trusts no entity inside or outside its perimeter, requiring verification at every access point in the network. This approach has gained significant popularity because it systematically makes it harder to implement potential breaches by treating every user, device, and network flow as a potential threat, regardless of their location on or off the network [1].

A fundamental step in the transition to a ZT architecture is to conduct a thorough assessment of the corporate network. This initial assessment is crucial because it provides a detailed overview of the current state of the network, identifies all assets, and maps data flows. Such a comprehensive assessment helps to pinpoint vulnerabilities and develop a customized ZT strategy that meets the specific needs of the organization.

The purpose of this study is to create and describe a methodology for conducting a comprehensive assessment of the enterprise's network infrastructure as an integral part of the migration to the ZT security model.

The implementation of ZT requires not only technological changes but also cultural changes within the organization, as security becomes an integral part of all network operations [2]. By thoroughly assessing the network, organizations can lay a solid foundation for a

CSDP-2024: Cyber Security and Data Protection, June 30, 2024, Lviv, Ukraine
*Corresponding author.
†These authors contributed equally.
roman.m.syrotynskyi@lpnu.ua (R. Syrotynskyi); ivan.y.tyshyk@lpnu.ua (I. Tyshyk); orest.v.kochan@lpnu.ua (O. Kochan); v.sokolov@kubg.edu.ua (V. Sokolov); p.skladannyi@kubg.edu.ua (P. Skladannyi)

0009-0002-6280-3290 (R. Syrotynskyi); 0000-0003-1465-5342 (I. Tyshyk); 0000-0002-3164-3821(O. Kochan); 0000-0002-9349-7946 (V. Sokolov); 0000-0002-7775-6039 (P. Skladannyi)

© 2024 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

CEUR-WS.org/Vol-3800/short3.pdf

successful transition to a ZT structure, thereby enhancing their ability to defend against sophisticated cyber threats.

2. Literature review

The concept of ZT in network security is gaining increasing importance as organizations seek to adapt to complex threats in modern network environments. Traditional perimeter-based network security models are no longer sufficient, leading to the emergence of ZT, which ensures strict identity verification for both internal and external access to computer network resources [2, 3].

Network assessment for ZT involves evaluating all network aspects to eliminate implicit trust, requiring verification at every level and segment. This paradigm shift concerns not only the technology stack but also changes in policies and management to ensure no organization is trusted by default [4, 5].

Implementing ZT models often focuses on network micro-segmentation, dynamic trust policies, and robust identity and access management frameworks to protect both data and applications. These models rely on meticulous real-time threat monitoring and assessment to dynamically adjust access controls based on perceived risk levels [6, 7].

Despite the theoretical robustness of ZT, implementation challenges include the complexity of integrating this model into legacy systems, the need for continuous improvement of security policies, and the resource intensity required to maintain and monitor a ZT environment. Future research and technological developments will likely focus on making ZT more accessible and manageable, improving the automation of trust decisions, and integrating artificial intelligence to support continuous adaptation to emerging threats [8, 9].

Phiayura and Teerakanok (2023) propose a detailed framework for transitioning to ZTA, emphasizing the need for a strategic approach to strengthening enterprise security. The study identifies crucial steps for initial assessment, including understanding the current security landscape, identifying critical assets, and evaluating existing security measures [10].

Teerakanok, Uehara, and Inomata (2021) discuss the concept of ZT and outline the challenges and considerations when transitioning from legacy architectures. The paper highlights the importance of initial assessments to identify potential risks and prepare for the transition [11]. Key steps include assessing the current network infrastructure, understanding user behavior, and defining security policies based on the principle of least privilege.

An extensive description of enterprise infrastructure components and their application in ZT architecture is provided in the book "ZT Security: An Enterprise Guide" by Jason Garbis and Jerry W. Chapman [12]; however, the issues of methodology and effective approaches for initial analysis and assessment are not addressed.

The authors of "ZT Networks" recommend using network traffic analysis through network flow generation when planning a migration to ZT architecture. After recording all network flows, the next goal is to classify the flows based on higher-level system connections. These connections should be defined at the logical system level rather than at the individual IP/port level [13]. The result will be a map of corporate system connections that will allow for the analysis and identification of necessary connections and the planning of appropriate security policies and network micro-segmentation.

Recommendations for conducting an initial analysis of corporate assets are widely discussed in contemporary scientific works describing ZT architecture and migration, confirming the importance of this stage. The granularity and detail of these approaches are either not disclosed or disclosed superficially, without recommended models for asset classification and data analysis approaches, confirming the relevance of research that would highlight the process of preliminary assessment and infrastructure analysis with recommendations for their implementation.

3. Problem statement

Taking into account the NIST 800-207 recommendations for the effective implementation of ZT architecture and the need to minimize operational costs associated with incorrect security policy development or insufficiently detailed risk assessments, there arises a necessity to develop approaches that help conduct a qualitative analysis of corporate network infrastructure, assets, and their access, as well as an inventory of information resources, applications, and data flows between them. This information is crucial for creating a list of connections that should be implemented considering the principle of "least privileged access".

Given the above, the relevant task of this work is to define the list of necessary stages for conducting a comprehensive analysis of the enterprise's network infrastructure, investigate methods for their implementation, and develop a methodology. The application of this methodology will allow for the acquisition of necessary information, which will subsequently be used for planning stages of network micro-segmentation and the overall development of security policies. This will ensure the correct migration of the existing enterprise security model to a ZT architecture.

4. Presentation of the main research material

Migrating an enterprise security system to a ZT model means moving from a traditional security model that trusts users and devices in the middle of the network perimeter to one that continuously verifies and authenticates all users and devices, regardless of their location. This involves implementing strict access controls, micro-segmentation, and constant monitoring to ensure that only authorized users can access certain resources. This approach minimizes the risk of unauthorized access and lateral movement in the network. The goal is to improve security by recognizing that threats can exist both inside and outside the network. This transition requires updating policies, deploying new technologies, and educating users on new security practices.

The ZT concept involves the application of its main principles, namely:

- Never trust, always verify.
- The principle of least sufficient privileges.
- The assumption is that the intervention has already taken place.

Despite the significant efforts that organizations are making to prevent compromise, the reality is that if cybercriminals attack a particular organization, they will find a way to infiltrate the internal infrastructure [14].

Planning network segmentation and granular access control according to the principles of ZT requires detailed accounting and transparency of the existing infrastructure and all traffic exchange points. To ensure the principle of minimum privileges and cut off any excessive access rights, it is necessary to have a clear understanding of data transfer needs and the level of access required for each application that uses the corporate network for its work.

Scope and Boundaries. The initial stage of analyzing the network infrastructure as the foundation of all corporate services will be to define its scope and boundaries, as well as zones of responsibility and control. Due to recent trends, the answer to this question may not be straightforward. Remote workforce, cloud computing, and VPN connections with partner networks blur the lines of responsibility and protection.

At this stage, it is advisable to create or review the existing network diagram. Use tools and methods to map out the entire network infrastructure, including all devices, endpoints, and connections. This includes defining the geographical and administrative boundaries of the network, as well as its logical segments [15].

The primary data sources for creating the network diagram will be existing documentation and corporate systems such as the Configuration Management Database (CMDB). Due to the static nature of the data and the widespread issue of "Shadow IT", it is not advisable to rely solely on documented data from these sources. Instead, validate and supplement them with real data obtained using tools from the "Network Inventory" category. A mandatory step should be manual reconnaissance using tactics such as reviewing network device configurations, identifying neighboring connections using appropriate protocols and network device management commands, analyzing monitoring systems, and enabling logging and analysis of all network flows. The outcome of this stage will be network diagrams showing all segments and nodes, as well as a comprehensive list of network devices.

Subnet inventory. Since network nodes can aggregate different logical networks on the same physical links, it is important to identify all corporate network prefixes. Taking into account the already-known network topology and its segments, all corporate networks (prefixes) should be documented. Sources of this information can include the corporate CMDB system, corporate monitoring, as well as an analysis of network device configurations. The information should include both private and public address blocks, and it is also necessary to document client networks with connectivity that may be established through Site-to-Site VPN.

Network host inventory. To ensure visibility of everything interacting with the corporate network and potentially accessing corporate resources, or being the resource accessed, it is necessary to identify assets and document all equipment, software, and devices that are part of the network. This includes servers, routers, switches, firewalls, endpoints, and any IoT devices. It is important that this inventory is updated and includes all assets connected to the network [16].

The primary data source can be the analysis of information in the corporate CMDB system, if available, as well as service documentation describing all elements of a particular corporate service. As with network nodes, the found information should be verified and supplemented using precise system verification tools, including virtualization tools, network scanning, monitoring system analysis, and network traffic analysis.

To effectively manage the collected data, it is recommended to define mandatory fields for each identified asset. Examples of important fields might include asset type, asset name, host IP addresses, home network name, service affiliation, geographical location, and host purpose. When creating a list of network assets, it is advisable to use the list of corporate prefixes to clearly distinguish: "internal," "external," and internet addresses.

During the identification of hosts, there may be cases where certain hosts are temporarily turned off or have very low activity, making them absent from logs, and the ARP table may not show a corresponding entry. In such cases, there is a risk of missing them. Under the traditional security model, these would be categorized as Shadow IT, but under the ZT security model, their network activity will either be blocked or significantly limited, leading to an incident and requiring additional configurations to restore their proper functionality.

To find such low-activity assets, the "exclusion" method can be applied. The idea is to exclude all already identified assets and analyze what remains. One implementation option is manipulating corporate firewall rules with enabled traffic logging. For example, to filter all identified hosts, create an additional rule similar to the existing one, but instead of specifying a broad network prefix in the Source section, specifically list all known hosts and place it above the existing rule.

Thus, the general (lower) rule will pass the traffic of missed and not listed in the filtering rule known hosts.

Such configurations can be left for a certain period and then the logs can be reviewed to see the traffic that appeared in the general rule, below the "filter" rule. This way, all potential assets that were not previously identified for various reasons can be "caught".

The figures show an example of implementing this approach using a Palo Alto firewall, where the existing general rule is "Default-Rule-Permit-From-Network", and the temporary filter rule is "Filter-Rule-For-Known-Hosts."

Analysis of network host access. Another fundamental principle of ZT is the "principle of least privilege". In the context of its application to network assets, this principle is based on defining the minimal access rights to other resources necessary for the correct operation of the asset or the applications installed on it, while restricting all other access. The assessment and audit of the network at this stage involve analyzing the existing network accesses of its assets, inventorying them, and then determining the least allowable privileges.

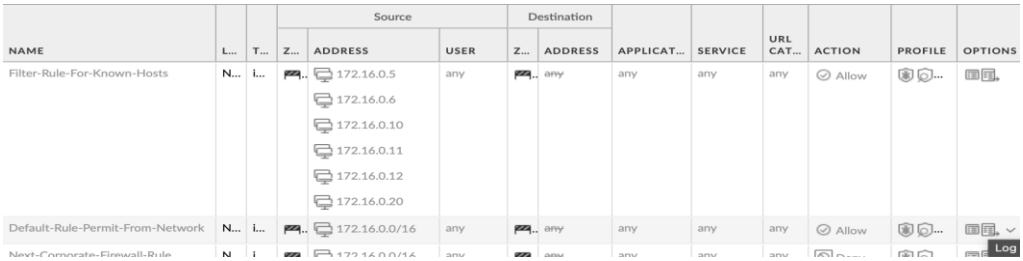

Figure 1: Example of rule application—a filter to exclude known assets

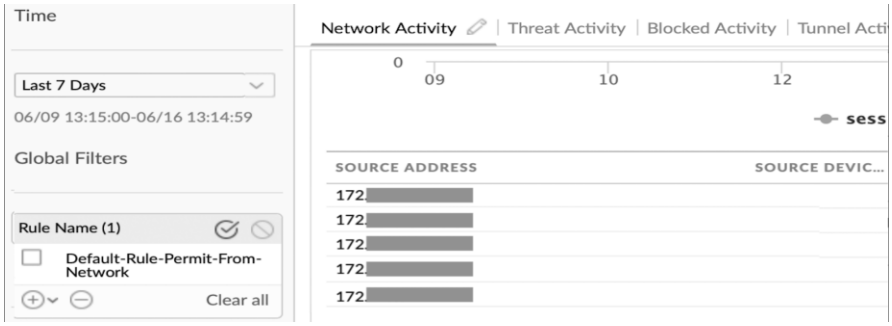

Figure 2: Visualization of assets by per rule name logs filtering

Due to the perimeter-based security model ideology, identifying the existing connections of certain hosts is not always an easy task. This refers to horizontal connections that are not recorded anywhere or hosts that do not support the installation of appropriate applications for local traffic analysis [17].

Several approaches can be applied to analyze existing accesses and determine the minimally required accesses. For example:

- Analysis of necessary connections using expert evaluation.
- Analysis of necessary connections using the technical documentation of the network node or its applications.
- Analysis of the technical documentation of the service to which the node belongs.
- Analysis of the existing connections of the node in the network by capturing and reviewing traffic or analyzing NetFlow-type flows.
- Analysis of traffic logging when passing through the firewall.

Using just one of the listed approaches will not be sufficient to obtain objective and comprehensive results. For the highest quality determination of the minimally required privileges, it is advisable to start with researching the documentation of the host or the software product installed on the host. Such documentation will give us a typical description of the ports and protocols used by this solution.

The next step should be to analyze the configuration and determine which resources this host communicates with. The information obtained from researching the manufacturer's documentation and analyzing the configuration will provide an understanding of the access needs to ensure the main functions of this host or application. However, traditionally, in addition to accesses to ensure the main function, most hosts require certain accesses to ensure the administrative and operational needs of the system. These may include:

- Administrative access.
- Access for monitoring.
- Access for backup.
- Access to name resolution services.
- Access to repositories for installing and updating system packages.
- Access to licensing servers.

After completing the theoretical analysis, to confirm the collected information, it is recommended to analyze the existing traffic to and from this system over a certain period and compare it with the results obtained previously. Common network traffic analysis algorithms include:

- Using network traffic analyzer programs.
- Using tools based on connection logging on corporate firewalls.
- Using solutions based on network traffic accounting protocols.

Mapping data flows. Understanding data transmission paths and dependencies is crucial for defining security policies that align with the ZT model. To map how data moves through the network and determine which applications and services access and process the data, a thorough investigation should be conducted. The key steps in this process include:

- Identifying Sources and Destinations of Data Flows: Catalog all databases, file servers, cloud storage services, endpoints, and any other repositories or sources of data.
- Inventorying Applications and Services Interacting with Data: Document all applications and services that interact with the data.

- Mapping Data Interactions: Track how data moves from one point to another. This includes data at rest (stored data) and data in transit (data moving through the network).
- Determining Data Access Patterns: Recognize how, when, and by whom data access occurs.
- Analyzing Network Segments: Evaluate how data moves through various network segments, including isolated or restricted zones, to confirm that segmentation complies with security policies.
- Identifying External Data Flows: Record data flows that cross network boundaries.

Mapping data flows in a ZT environment provides a clear vision of how data moves through the network, which is essential for identifying potential vulnerabilities and ensuring the effective application of security policies.

Application inventory. The inventory and analysis of corporate applications, including proprietary and third-party programs, is the next crucial step in network assessment as part of the migration to a ZT architecture. The goal is to assess the security status of each application, understand their data handling practices, and ensure they are configured to operate securely within a ZT framework.

The objective is to compile a comprehensive list of applications used and supported by the corporate infrastructure. An effective approach combines automated discovery tools and manual checks. This includes identifying the names of programs, their versions, and their purposes. The next step is to assess the security status of specific applications. The authors of the publication "Performance Analysis of ZT Multi-Cloud" recommend the following practices: conduct security assessments such as vulnerability scans, penetration tests, and code reviews. Look for known vulnerabilities, outdated software versions, and incorrect configurations [18].

It is important to understand how each application processes and stores data. Analyzing data flows within applications will help assess how data is encrypted, transmitted, and stored. This assessment is necessary to ensure compliance with data protection regulations and adherence to internal security policies.

Mapping and documenting integration points and dependencies between applications will provide an understanding of integration points with other applications. "Document APIs, data exchange protocols, and network communications to identify potential security gaps" [3].

The evaluation of access control mechanisms for corporate applications includes reviewing and analyzing access control lists, role-based access control configurations, and other security settings required to enforce the principle of least privilege. It is important to ensure that Multi-Factor Authentication (MFA) and continuous monitoring are in place [19].

User identification and access. In addition to system inventory, user inventory, and access identification are essential when conducting a network assessment. This process ensures a comprehensive understanding of all users in the network, their roles, and access levels.

First, it is necessary to identify the existing types of user accounts and their access options to network resources. Common types of user accounts include guest, employee, administrative, and service accounts. These can be local on the systems or global accounts registered in corporate directory services. Regarding user access methods to the network, the following are distinguished:

- Local wired access
- Local wireless access
- Remote access from outside the organization's perimeter.

Typically, each of these access methods has its security policies that regulate access to corporate resources for specific roles or groups of accounts. Analyzing authentication and authorization parameters will help determine which user groups have certain access [20]. Understanding who is allowed to connect is essential to determine the target resources they can access. This information should also be described in connection policies. The traffic path from the user to the target resource may pass through more than one access control point, so to assess the access level of a specific user or group of users, it is necessary to carefully analyze all access control points, compare the data, and describe a clear list of addresses and ports to which such access is granted.

To further process the obtained results and determine the minimally acceptable level of access, the existing user access list should be additionally analyzed to identify the following:

- Access Verification: Review access levels and permissions for each user. Pay attention to any discrepancies or excessive permissions that do not match their job roles.
- Privilege Identification: At this stage, it is necessary to identify users with elevated privileges and ensure that such access is necessary and documented.

All useful information should be reflected in the user inventory report. This should be a comprehensive report documenting all user accounts, their types, roles, current access levels, and any identified issues. Using the obtained information, it is important to conduct a risk assessment: and identify potential security risks, such as lost accounts, excessive permissions, and discrepancies in user roles and access levels.

Summary of accesses and common policies. Given the modern virtualization capabilities and the complexity of infrastructures, the number of hosts in the network and, consequently, the number of potentially required rules that will describe all possible connections will be significant. The development and maintenance of numerous security policies is a labor-intensive and costly task not only from the perspective of human resources for maintenance but also from the standpoint of hardware requirements for firewalls that will ensure their operation and enforcement.

To optimize and reduce the number of rules, a good approach is to use common security policies for similar access types. In a typical organization, similar access types might include the following categories:

- Shared patch management.
- Shared administrative access.
- Shared backup and monitoring access.
- Similar access to certain resources.

In such cases, a common rule is used that allows traffic to pass in one direction using the same services or applications for a certain number of different network nodes listed in the "source" or "destination" field. Conducting the procedure of categorizing accesses at the stages of evaluating user and network host access allows for more effective and optimized planning and development of security policies.

Reducing the overall number of security policies that describe access to corporate nodes and applications is worthwhile and necessary, but only if this optimization does not reduce the level of security and does not grant additional unnecessary accesses. This categorization approach should also be used when analyzing accesses for similar hosts, such as remote users or identical computing units.

Endpoint security. Users access corporate resources using their endpoint devices. Analyzing the security status of endpoint devices that participate in data exchange with corporate resources is also part of the comprehensive network assessment needed for a successful transition to ZT architecture.

To create a complete list of all endpoint devices connected to the network, it is advisable to use automated tools for network scanning and device identification, including desktop PCs, laptops, mobile devices, and IoT devices. Document the details of each device, such as type, operating system, and installed software [21].

To help classify and supplement the list, analyze corporate monitoring systems, and mobile device management tools, and review information registered in the CMDB.

A crucial aspect is the classification of devices into those under corporate control and those not controlled by corporate security policies. When transitioning to ZT architecture, different levels of access will be applied to corporate and non-corporate endpoint devices.

For corporate devices, it is necessary to analyze and verify the status of security solutions applied to them. The purpose of this assessment is to ensure that endpoint devices comply with security policies and are adequately protected from threats. The following should be checked and documented:

- All devices comply with corporate security policies, including encryption, password, and software update policies.
- Antivirus software and malware protection programs are installed and updated.
- Firewall and intrusion prevention system settings.
- Evaluation of the encryption status of sensitive data both at rest and in transit.
- The status of patches and updates for operating systems, applications, and security software, and ensure that automated patch management tools effectively deploy updates.
- Secure connection methods such as VPN or ZT Network Access (ZTNA) solutions are used, and device authentication mechanisms such as MFA are implemented.

Review of security policies. Reviewing security policies and procedures is necessary to align with the principles of ZT during the network assessment. The goal is to gather all existing security policies and procedures, such as documentation on access control policies, incident response plans, data protection protocols, and other relevant security measures, and ensure that all documents are up to date and reflect current practices [22].

To assess the effectiveness of current security policies, qualitative and quantitative methods will be effective in evaluating how well the policies protect against threats. This includes reviewing compliance reports, conducting interviews with key stakeholders, and analyzing incident response records to identify any gaps or weaknesses [23].

Existing security policies should mandate the use of MFA and strong password requirements for all users and devices. User onboarding and off-boarding procedures should support timely updates to access controls. Evaluating the effectiveness of device security policies should highlight mandatory encryption and regular software updates. Data protection policies should ensure the encryption of sensitive information both at rest and in transit.

It is also important to review incident response procedures to ensure they support the rapid detection, reporting, and mitigation of security incidents [24-25]. Assessing the governance structure is necessary to ensure clear accountability and regular review of security practices. Finally, it is essential to document the results of the review and relevant observations of all corporate security policies and their effectiveness, considering the current state of their communication and enforcement throughout the organization.

5. Research results

The migration of an enterprise's security model to a ZT architecture is a complex and costly process that requires thorough preparation, an understanding of the security model architecture, a well-developed migration plan, an understanding and agreement on costs, risk management, and acceptance of the changes that will occur within the organization during and after the migration.

One of the initial stages of migration is conducting an analysis and assessment of the corporate network infrastructure. Depending on the thoroughness of this assessment, the duration, cost, and risks of the migration will vary.

The result of this research is a proposed methodology and recommendations for conducting activities to describe and inventory the structure of the corporate network, its segments and assets, describe and classify accesses and data flows, document corporate applications, and more. The described approach is based on the recommendations for a phased and cyclical approach to implementing ZT architecture as outlined in the special publication NIST SP 800-207 [2].

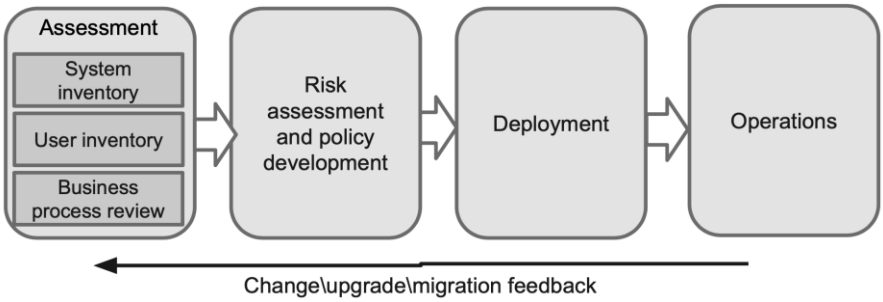

Figure 3: Zero-trust architecture deployment cycle according to NIST SP 800-207

The methodology involves conducting successive stages of a comprehensive assessment using recommended measures and techniques for identifying, searching, analyzing, and classifying information for documentation and subsequent use in building the ZT security model.

Table 1
Assessment structure

Stage	Evaluation algorithm	Key data
Scope and Boundaries.	1. analysis of existing documentation 2. analysis of information in the CMDB 3. viewing the configuration of network devices	– network diagram – network segments – segment type – segment location – network hosts – hostname – host location – host platform
Subnet inventory.	1. analysis of information in the CMDB 2. viewing the configuration of network devices	– prefix – network name (if available) – network type (assignment: user network, server network, client network, external subnet, etc.) – the device on which this subnet is terminated
Network host inventory.	1. analysis of information in the CMDB 2. analysis of documentation of corporate services 3. review of information in monitoring systems 4. viewing information in virtualization tools 5. analysis of network traffic logging 6. analysis of ARP tables of network devices 7. generating reports and creating “tenet”–type policies based on network traffic logging 8. use of network scanning tools	– hostname – host type – IP address is internal – IP address is external – the name of the home network – belonging to a certain service – host assignment (Production\Development\Test\Stage) – host status – host owner – host location
Analysis of network host access.	1. study of the technical documentation of the software or hardware product developer 2. analysis of accesses of hosts and applications using expert evaluation 3. host configuration analysis 4. Analysis of corporate service documentation 5. network traffic analysis by various means: – traffic logging on the firewall – analysis of mirrored traffic – analysis of “NetFlow” type streams	– access name – access category (management, operational, working) – access source – assignment of access – port and protocol – application – access context – description of access
User identification and access.	1. analysis of user registration and their access to the CMDB	– Account – account type – identity provider name

	2. analysis of entry points and user traffic paths on the network diagram 3. analysis of authentication and authorization parameters at network access points 4. analysis of the configuration of network devices and determination of address pools 5. analysis of user roles and their access levels 6. analysis of sources of identity	– list of authentication and connection points – the list of access privileges in detail (IP, port, application, context) – description of access contexts and their access levels
Mapping data flows.	1. network diagram analysis 2. analysis of network segments and hosts 3. analysis of the location of data stores 4. analysis of documentation of corporate services that interact with data 5. analysis of data flows using peer review	– data flow diagrams – sources and destinations of data streams – applications and services that interact with data – data at rest – data in transit – data access model – data movement within the network – moving data outside the network
Application inventory.	1. analysis of documentation of corporate services 2. analysis of the results of the inventory of networks and network assets 3. analysis of application security settings 4. scanning of application vulnerabilities 5. application penetration testing	– the name of the application – application version – purpose of the application – integration points and dependencies between programs – internal\external publication – access control
Endpoint security.	1. analysis of means of inventory of corporate equipment 2. analysis of corporate mobile device management tools 3. analysis of corporate remote access services 4. analysis of the corporate security policy	– inventory of corporate devices – classification of corporate devices – antivirus software – firewall settings – data encryption – update of patches of the operating system and applications – secure remote access tools
Review of security policies.	1. assessment of current security policies	– creating and deleting users – device security – data protection on the device – requirements for using MFA and strong passwords – incident response procedures – network segmentation policy – standards for safe configuration of environments

By conducting a thorough audit covering these areas, an organization can lay a solid foundation for implementing a ZT architecture that protects data flows, applications, and the overall network environment. This comprehensive approach is essential to protecting against sophisticated cyber threats in today's complex and dynamic IT landscape.

6. Conclusions

Summarizing the above, it has been established that the implementation of a ZT architecture is currently essential for enterprises and organizations seeking to enhance the protection of their information systems from both existing and anticipated cyber threats. It has been determined that integral attributes of the process of migrating an enterprise's security model to a ZT architecture (security model) include a clear understanding of the architecture of the existing model, knowledge of the corporate network structure, conducting an inventory of its assets and the distribution of data flows necessary for the functioning of corporate applications and the operation of business processes built on them.

The network infrastructure analysis methodology outlined in this paper provides a structured approach to conducting comprehensive network infrastructure assessments, describes approaches and practices for finding useful information when conducting them, and emphasizes the key data needed to document the results.

It has been established that conducting a detailed assessment and documentation of the corporate network infrastructure, inventorying its assets, access, and data flows, as well as classifying the received information from the perspective of information security, will allow the enterprise to effectively plan an iterative migration of the existing

security model to a ZT architecture, with a lower probability of abnormal situations, reduced downtime of business processes, and lower costs for operational support.

Prospects for further research may be aimed at developing approaches and practices for the iterative migration of corporate infrastructure elements to a ZT architecture.

References

[1] S. Rose, Planning for a Zero-Trust Architecture: A Planning Guide for Federal Administrators (NIST CSWP 20), National Institute of Standards and Technology (2022) 1–16. doi: 10.6028/NIST.CSWP.20.

[2] S. Rose, Zero-Trust Architecture. NIST Special Publication 800-207, National Institute of Standards and Technology (2020) 1–50. doi: 10.6028/NIST.SP.800-207.

[3] Y. He, A Survey on Zero-Trust Architecture: Challenges and Future Trends, Wireless Communications and Mobile Computing (2022). doi: 10.1155/2022/6476274.

[4] Y. Ge, Q. Zhu, Zero-Trust for Cyber Resilience, ArXiv (2023). doi: 10.48550/arXiv.2312.02882.

[5] R. Habash, M. Khalel, Zero-trust Security Model for Enterprise Networks, Iraqi J. Inf. Commun. Technol. (2023). doi: 10.31987/ijict.6.2.223.

[6] S. Hong, et al., Research on Zero-Trust Evaluation Method for Network Security, in: 3rd International Conference on Frontiers of Electronics, Information and Computation Technologies (ICFEICT), (2023) 449–454. doi: 10.1109/icfeict59 519.2023.00080.

[7] M. Xu, et al., Zero-Trust Security Authentication Based on SPA and Endogenous Security Architecture, Electronics (2023). doi: 10.3390/electro nics12040782.

[8] Y. Ge, Q. Zhu, Trust Threshold Policy for Explainable and Adaptive Zero-Trust Defense in Enterprise Networks, IEEE Conference on Communications and Network Security (2022) 359–364. doi: 10.1109/CNS56114.2022.9947263.

[9] S. Sarkar, et al., Security of Zero-Trust Networks in Cloud Computing: A Comparative Review, Sustainability (2022). doi: 10.3390/su141811213.

[10] P. Phiayura, S. Teerakanok, A Comprehensive Framework for Migrating to Zero-Trust Architecture, IEEE Access 11 (2023) 19487–19511. doi: 10.1109/ACCESS.2023.3248622.

[11] S. Teerakanok, T. Uehara, A. Inomata, Migrating to Zero-Trust Architecture: Reviews and Challenges, Secur. Commun. Netw. (2021) 1–10. doi: 10.1155/2021/9947347.

[12] J. Boston, J. Chapman, Zero-Trust Security: An Enterprise Guide, Apress (2021). doi: 10.1007/978-1-4842-6702-8.

[13] E. Gilman, D. Barth, Zero-Trust Networks, O'Reilly Media, Incorporated (2017).

[14] S. Vasylyshyn, et al., A Model of Decoy System Based on Dynamic Attributes for Cybercrime Investigation, Eastern-European J. Enterp. Technol. 1(9(121) (2023). 6–20. doi: 10.15587/1729-4061.2023.273363.

[15] M. Luckie, et al., bdrmap: Inference of Borders Between IP Networks, Proceedings of the 2016 Internet Measurement Conference (2016). doi: 10.1145/2987443.2987467.

[16] J. Myerson, Identifying Enterprise Network Vulnerabilities, Int. J. Netw. Manag. 12 (2002). doi: 10.1002/nem.433.

[17] S. Yevseiev, Models of Socio-Cyber-Physical Systems Security: monograph, PC TECHNOLOGY CENTER (2023).

[18] S. Rodigari, et al., Performance Analysis of Zero-Trust multi-cloud, IEEE 14th International Conference on Cloud Computing (CLOUD) (2021) 730–732. doi: 10.1109/CLOUD53861.2021.00097.

[19] S. Ghasemshirazi, G. Shirvani, M. Alipour, Zero-Trust: Applications, Challenges, and Opportunities, ArXiv, (2023). doi: 10.48550/arXiv.2309.03582.

[20] D. Shevchuk, Designing Secured Services for Authentication, Authorization, and Accounting of Users, in: Cybersecurity providing in information and telecommunication systems II, vol. 3550 (2023) 217–225.

[21] C. Mu, et al., ETA: A Method of Dynamic Network Device Security Assessment, Journal of Physics: Conference Series 1229 (2019). doi: 10.1088/1742-6596/1229/1/012060.

[22] Y. Shunzheng, Assessment of Network Security Policy Based on Security Capability, Journal of Wuhan University (2009).

[23] M. Abedin, et al., Vulnerability Analysis for Evaluating Quality of Protection of Security Policies, QoP '06: Proceedings of the 2nd ACM Workshop on Quality of Protection (2006) 49–52. doi: 10.1145/1179494.1179505.

[24] J.S. Al-Azzeh, et al., Analysis of self-similar traffic models in computer networks, International Review on Modelling and Simulations 10(5) (2017) 328–336.

[25] M. Zaliskyi, et al., Method of traffic monitoring for DDoS attacks detection in e-health systems and networks, in: Informatics & Data-Driven Medicine, vol. 2255 (2018) 193–204.