Network microsegmentation design methodology in zero-trust architecture

Roman Syrotynskyi[1,*,†], Ivan Tyshyk[1,†] and Andrii Partyka[1,†]

[1]Lviv Polytechnic National University, Stepan Bandera Str.,12, Lviv, 79000, Ukraine

Abstract

The paper describes approache to implementing network microsegmentation in an organization's corporate network to ensure robust access control over infrastructure elements and improve their management. Deploying network microsegmentation to restrict lateral movement between components is a key step in migrating to a Zero Trust Architecture. Microsegmentation maintains optimal network performance while enabling effective access control both at the perimeter and within the network. It also isolates the organization's critical assets from untrusted connections, reducing the risk of unauthorized access. Introducing modern security models calls for careful planning and design of network microsegmentation. This process changes the network architecture and brings not only security benefits but also certain drawbacks, such as increased topology complexity, higher implementation costs, and greater spending on maintenance and operations. The study analyzes the advantages and disadvantages of microsegmentation at different levels of granularity. Dense microsegmentation raises the overall security of the corporate infrastructure if individual elements are compromised, whereas coarse segmentation demands fewer resources, is easier to operate, and generally does not degrade network performance. The paper proposes an analytical design method that uses risk matrices to assess corporate systems, determine the required security level, and choose an appropriate network microsegment size. It presents an example of microsegmentation applied to a typical infrastructure, highlighting the topology before and after the change. Finally, the work examines the reasons for and approaches to optimizing the initial microsegmentation design.

Keywords

microsegmentation, zero trust, network, firewall, infrastructure, granularity

1. Introduction

Microsegmentation is a method of network security that involves dividing a network into smaller, isolated segments (microsegments) to apply specific security controls to each segment. This method is commonly used to limit the horizontal movement of attackers by applying granular security policies to individual workloads or groups of devices. Thus, even if an attacker gains access to one part of the network, his ability to access other parts will be limited.

In modern implementations, especially in cloud environments, microsegmentation policies are often automatically created using dynamic and static analysis algorithms to control access between services based on legitimate access models [1].

Microsegmentation is considered an important part of the Zero Trust (ZTA) architecture, where it enhances security by ensuring that all internal communications are subject to the same stringent checks as external communications, reducing the attack surface and limiting potential harm from security breaches [2].

2. Literature review and problem formulation

The introduction and design of microsegmentation is mentioned by the authors of modern scientific papers quite often. The authors reflect on the impact of microsegmentation on corporate infrastruc-

CH&CMiGIN'25: Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, June 20–22, 2025, Kyiv, Ukraine

*Corresponding author.

†These authors contributed equally.

roman.m.syrotynskyi@lpnu.ua (R. Syrotynskyi); ivan.y.tyshyk@lpnu.ua (I. Tyshyk); andrijp14@gmail.com (A. Partyka)

0009-0002-6280-3290 (R. Syrotynskyi); 0000-0003-1465-5342 (I. Tyshyk); 0000-0003-3037-8373 (A. Partyka)

ture, offer implementation options, and work on algorithms for analyzing, designing, and applying microsegmentation using various technological solutions.

Noel et al. (2021) discuss trade-offs between security and performance when designing segmentation policies. Their study shows that fine-grained microsegmentation, although more complex, significantly increases resilience to cyberattacks, reducing the possibilities of lateral movement within the network [3].

Other studies claim that in practice, microsegmentation increases the overall level of security without significantly affecting network performance, making it effective for secure data center networks [4].

Authors Yinqiu Liu and others in their study propose a graph-based hierarchical microsegmentation model to optimize network security and efficiency. To improve the accuracy of segmentation, the use of an algorithm based on large language models is proposed [5].

Among the published modern works, a study has been conducted on the impact of microsegmentation on network performance. Authors: Muhammad Mujib and R. F. Sari evaluate the performance of microsegmentation in data centers using Cisco Application Centric Infrastructure and measure latency, jitter, and packet loss, showing that microsegmentation improves security without compromising network performance [4]. In their view, software-defined networking (SDN) is a key vehicle for implementing Zero Trust microsegmentation.

Modern papers also reflect on the specifics of implementing microsegmentation in cloud environments and propose a policy-based approach to inspecting network traffic at the port and protocol levels to limit unauthorized communication [6, 7, 8].

These publications provide an in-depth understanding of the design, implementation, and performance of microsegmentation in a zero-trust architecture. The study highlights key methodologies, from graph-based hierarchical segmentation to software-defined networking (SDN)-based implementations. Together, they strengthen microsegmentation as a fundamental security measure that reduces lateral movements, improves access control, and increases security in the cloud, data center, and enterprise environment.

In modern corporate environments, the task of designing microsegmentation arises taking into account individual characteristics, such as the specifics of the corporate infrastructure, requirements for increasing network security, a certain permissible level of productivity and manageability decline, and also last but not least, compliance with costs within the budget allocated for implementation.

Whichever strategy for building microsegmentation is chosen as a basis, microsegmentation design is a balancing between security on the one hand and ease of use/performance/cost of implementation on the other. For example, the most secure option - each individual network host in a separate segment protected by access control is an unrealistic scenario given the complexity of implementation and high resource consumption in modern corporate infrastructures. On the other hand, the formal implementation of microsegmentation with the division of a peer-to-peer network into 2 or 4 segments will not provide tangible protection and will not comply with the principles of zero trust. Thus, when implementing or migrating to a zero-trust architecture, the question arises of the optimal approach to microsegmentation design, which would primarily provide security value for the infrastructure and, on the other hand, would not burden it with excessive implementation cost, complexity of operational support, and also would not have a tangible impact on the quality of network services provided.

3. Purpose of the work and objectives of the study

The purpose of the work is to study the possibility of implementing network microsegmentation with different granularity in the corporate infrastructure of the organization in terms of improving its security characteristics and manageability. The objectives of the study are to solve the problem of developing approaches and practices for effective design of microsegmentation of the corporate network and its subsequent implementation into the network infrastructure of the organization, taking into account the increasing complexity of the network infrastructure within the framework of building a zero-trust architecture.

4. Methodology

Microsegmentation within the Zero Trust architecture (ZTA) can be implemented through a variety of strategies and approaches that provide robust protection by isolating network traffic and implementing strict access control measures. Here are the main types and strategies for implementing microsegmentation in Zero Trust environments:

1. Identity-based segmentation. This strategy involves implementing security measures based on the identity of users, devices, or applications, rather than based on IP addresses. Each segment is defined by identity attributes, allowing access only to verified and authenticated actors. This approach restricts lateral movement in the network by implementing strict access policies tied to identity data [9].

2. Dynamic policy support. Dynamic Policy Enforcement adjusts real-time security measures based on user behavior, device status, and other contextual data. This allows policymakers to change as the network environment changes, making the system adaptive and sensitive to threats [10].

3. Microsegmentation based on workloads. This strategy isolates workloads by assigning specific policies to each load, allowing for granular control of network traffic. Workload segmentation is especially useful in cloud environments where workloads are dynamic and can move between different servers or cloud environments [6].

4. Whitelist policy and ban by default. In this strategy, all traffic is blocked unless explicitly allowed (whitelisted). This ensures that only approved communications can occur in each microsegment. This positive security model ensures that unrecognized traffic is denied, which significantly reduces the attack surface [9].

5. Integration with software-defined networks (SDN). SDN allows you to programmatically define policies that control traffic between segments. This integration provides flexibility and scalability, especially in cloud and virtualized environments. Policies can dynamically adapt according to changes in network topology [11].

6. Segmentation at the periphery level. For industrial cyber-physical systems (ICPS) and distributed environments, edge-level segmentation isolates microservices and devices at the network edge, providing additional protection for systems operating outside of traditional data centers [12].

One of the key aspects when designing microsegmentation in a Zero Trust architecture is to determine the optimal level of granularity. Fine-grained segmentation, where every workload, user, or device is isolated, provides a higher level of security by minimizing the attack surface. However, fine-grained segmentation increases complexity and can affect network performance.

To design a microsegmentation of the network in the corporate infrastructure, it is necessary to acquire an understanding and vision of what components and elements it consists of. Everything that was within the security perimeter of a peer-to-peer network and somehow coexisted and communicated with each other must be identified and classified. At this stage, it will be advisable to use the documentation and knowledge collected during the analysis of the corporate infrastructure at the stage of network assessment as part of the migration to the Zero Trust architecture [13].

A critical component of microsegmentation within the Zero Trust architecture is the use of cryptographic mechanisms - such as encryption, authentication, and one-time token generation - which rely heavily on pseudorandom number generators [14, 15].

Microsegmentation design foresees the further application of security policies and the organization of access control between segments [16, 17, 18]. The goals of such an action are to prevent unauthorized access to sensitive data, as well as to localize and isolate the compromised segment and minimize the horizontal movement of attackers to other components of the corporate infrastructure and their potential compromise. Despite the obvious safety value, the implementation of dense microsegmentation has the following disadvantages:

- The cost of implementation directly depends on the number of firewall zones and points of application of security policies, which, with dense microsegmentation, can lead to exceeding the allocated budget for implementation;
- The complexity of management and operational support increases significantly;

- Increasing access control points in the path of traffic affects the bandwidth of the network infrastructure and increases latency, which can reduce its performance indicators below the acceptable level;
- A large number of security policies increases the operational burden on their maintenance and implementation;
- Highly dynamic environments can be poorly compatible with the operating conditions of corporate infrastructure with dense microsegmentation.

Thus, the number and structure of segments in the network should be optimal so that, on the one hand, it fulfills the set security tasks, and on the other hand, does not impair the performance and manageability of the network and remains within the allocated budget for implementation.

You can take a different approach to network segmentation. An integrated approach is proposed based on the categorization of assets according to certain key characteristics. Since the number of features per particular asset will vary, it will be advisable to use tags or tags for further analysis and segmentation planning.

The following set of characteristics of network assets can be basic:

- Functional role;
- Belonging to a specific corporate service;
- The level of sensitivity of the host's data or the criticality of the host itself;
- Likelihood of compromise;
- Location on the network.

After network assets tagging, it will be advisable to classify and group them by levels.

Clarification of corporate systems by levels involves the organization of system components or structures into separate hierarchical levels, each of which has certain roles and responsibilities. This layered approach is typically applied in areas such as management, information systems, and management structures to simplify complexity and increase efficiency. Levels are hierarchical levels in a system, each designed to perform specific tasks or functions. In corporate systems, they can include operational, managerial, and strategic levels to effectively distribute responsibilities [19].

Leveling simplifies complex systems by dividing them into manageable levels, improves decision-making by clarifying roles, and improves adaptability by isolating changes at certain levels [20].

Based on the function and criticality of the host, all assets are divided into levels as follows:

- Level 1 - Critical Systems;
- Level 2 - Important Systems;
- Level 3 - General Systems.

Understanding the level of all corporate hosts, and taking into account their signs, the next step is to develop a network segmentation strategy and plan access control points. In this case, the final decision may be influenced by restrictions on the creation of network zones at firewalls on the basis of which segregation will take place, but they should not be taken into account during the initial design, it is recommended leaving it to the optimization stage if necessary.

Depending on the level of the systems and their type and location, it is proposed to use the following zones of the corporate firewall:

- Restricted Area for Level 1 Systems;
- Secure area for Level 2 systems;
- Public area for Layer 3 systems that must be accessible from the Internet;
- Custom Area for Enterprise Workstations;
- Service area for transit segments of the network.

From the point of view of the configuration of the zone on the firewall, there is no difference between them, however, this lays down an understanding of the level of security of a particular zone in the future by firewall access control tools and makes it possible to more clearly understand the purpose of the zone, which will be useful when distributing all corporate hosts to the corresponding network segments. Depending on the level of the system, belonging to the service and placement in the network, the host can be placed in an individual segment or a group one. In turn, group network segments served by one zone can contain a certain number of hosts grouped according to a certain characteristic and taking into account their level.

Thereby a traditional network topology consisting of 2-3 firewall zones and 2-3 network segments should be transformed into a multi-segment topology using the appropriate number of firewall zones to provide network microsegmentation - which is the goal when building a zero-trust architecture.

However, the number of network segments usually cannot correspond to the number of hosts in the corporate network due to limiting factors. These include limitations on the number of firewall zones, reduced bandwidth and increased latency when multiple firewalls are traversed sequentially, as well as the operational complexity of the initial implementation of access control policies and their effective operational support. Therefore, having a certain finite resource to ensure network segmentation, it is necessary to develop an optimal approach to dividing the entire fleet of corporate hosts into appropriate segments, followed by the development of security policies between them.

Several key factors will influence the design of microsegmentation that will form requirements and constraints for the development topology, for example:

- Increasing the resilience of the microsegmented network to cyber threats and lateral movement;
- Minimum allowable level of network performance;
- Segmentation does not interfere with existing business operations;
- The cost of implementing microsegmentation does not exceed a certain budget.

Since microsegmentation is part of zero-trust architecture - and this is primarily about increasing the level of security of the corporate infrastructure - the key factor will be to ensure resilience to cyber threats and minimize horizontal movement. The implementation of this factor should be carried out first of all, and the rest of the requirements should be achieved later.

Since the number of microsegments of the network will almost certainly not correspond to the number of hosts in the network, it is obvious that 1 microsegment will account for a certain number of hosts that will be placed in it. Whether to make all microsegments of the same capacity in terms of the hosts placed in them - this approach will not have any obvious advantage, but the disadvantages will be present. Therefore, the granularity of the microsegments will be heterogeneous, and this makes sense given the previous division of corporate hosts into levels and their different placement on the network. Some hosts will be placed in individual segments, some will be grouped according to a certain characteristic and placed in a common segment, with different densities.

The proper granularity of microsegmentation ensures that each segment is protected, maintaining low latency and minimal operational load. Overly detailed segmentation can lead to reduced performance, while too general granularity can ineffectively limit threats [4]. Effective granularity ensures that security measures do not require excessive resources that could increase operational complexity and costs. A well-balanced approach ensures an adequate level of security while maintaining the efficiency of the system [21].

Enterprise nodes, which are considered the most critical in the infrastructure due to their role or the level of data they operate, will need the most careful access control, and in order to ensure this, uncontrolled connections from other, potentially compromised nodes should be restricted. To achieve this, such hosts must be placed in isolated network segments which are secured by an individual firewall zone. The cost of 1 to 1 microsegmentation (individual network segment per single host) is the highest, this approach makes sense only with the most important nodes, provided that there is sufficient firewall resource.

The systems that should be protected in the most effective way will be all most critical hosts, identified as tier 1, these might be the following corporate infrastructure nodes:

- Domain Controllers and Authentication Servers;
- Database servers with confidential data;
- Servers that provide a key function of the business;
- Administrative and management servers.

Since the high granularity of microsegmentation, despite the high level of security, has obvious inevitable drawbacks - it is impractical to place all network hosts in this way, which means that all other nodes must be grouped and placed in enclaves into microsegments.

Microsegmentation with medium granularity of microsegments is used when there is a need to place network hosts in them that have certain common characteristics. These can be servers that are part of the same service or have hosts that perform the same role in the infrastructure. It makes sence for such hosts to be combined and placed in a common network segment under the control of a single firewall zone per group. With this design, it should be clear that compromise of one of the hosts of the enclave should be taken as a compromise of the entire segment, because horizontal movement there is no longer regulated by the network firewall. The likelihood of compromise also increases, since more hosts, more open accesses per segment - correspondingly a larger area of potential attack.

This approach of enclave host placement in a microsegment can also be justified for highly integrated services that require either dynamic access control between nodes or have a high intensity of data exchange between nodes, which can carry an additional load on network or application firewalls. Redundancy in such systems can be implemented by dividing the service into several equivalent working groups with the expectation that in case of compromise, one group (one microsegment) will be disabled, and the neighboring one will work independently. Medium granularity microsegmentation, which involves multiple hosts per network segment, is a popular and efficient approach. With a weighted microsegment design, the level of security is still at a high level, and the number of firewall zones required to provide microsegmentation is significantly reduced compared to the 1-to-1 approach. And this significantly affects the cost of the solution, which is reduced to realistic amounts for implementation and operational support, and also significantly increases the number of companies that can afford high-quality microsegmentation.

For example, according to a study by N. Sytnik, M. Kravchenko 2021, the average infrastructure of a medium-sized business can consist of 50-250 servers [22], even if the average value is 150. The average cost of a corporate new generation firewall zone, on the example of the most affordable model PaloAlto PA-1410 with a Threat Prevention license for 3 years, starting from $ 100. Therefore, the minimum cost of providing firewall zones only for microsegmentation starts from $ 15,000 in use case of PaloAlto products. Such an investment in security can be unaffordable in certain cases and jeopardize the entire process of building a zero-trust architecture.

The strategy of corporate network segmentation and the placement of hosts that did not fall into individual segments may consist in the following approaches. Since the compromise of the host of a certain corporate service threatens to fail the entire service - one can consider the granularity of microsegmentation up to the service level or up to level 2 segments per service. The following approaches to dividing the service into separate segments will be meaningful (Figure 1):

- Division of the service into frontend parts and backend parts;
- Separation of servers with databases from the service for reasons of additional protection of corporate data;
- Separation of test, development and production environments into separate segments.

Thus, the full list of hosts that support corporate services or applications will be divided into microsegments, which will significantly strengthen the resilience of the entire network to destabilizing events by localizing and preventing the horizontal movement of attackers. Nevertheless, there will still be a significant number of hosts in the corporate infrastructure that are present and do not need the classic small or medium microsegmentation, it will be enough for them to separate them by type and apply other approaches to traffic restriction. For example, devices that require the same level of

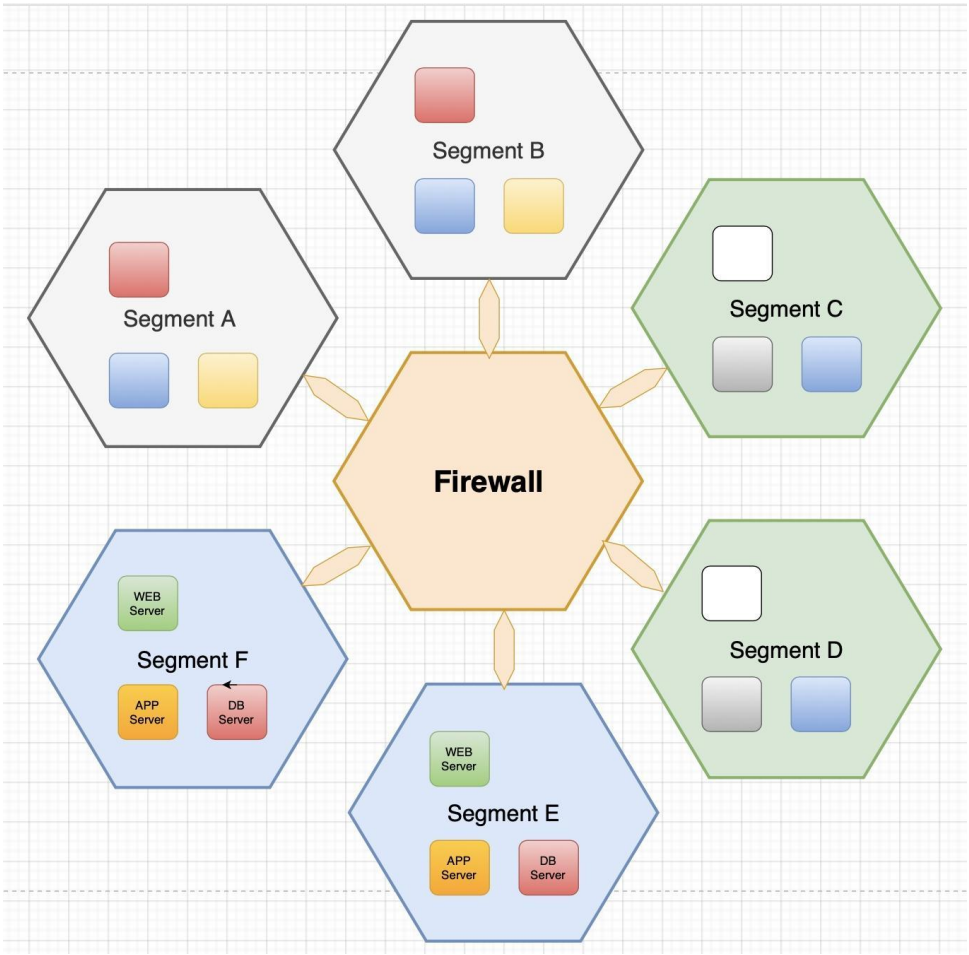

Figure 1: Redundancy of corporate services in microsegments.

authentication and authorization, such as workstations of employees of the same department, can be grouped. This makes it easier to comply with the policy and simplifies the implementation of zero trust principles [9]. Also, IoT devices with limited functionality and similar vulnerabilities can be grouped into a single segment protected by firewalls or modern security solutions [23].

Therefore, such devices may include the following groups of network hosts:

- Corporate Workstations;
- Enterprise IoT devices;
- Guest Devices;
- VPN client connection segment.

Peer-to-peer traffic restriction by wireless network management tools or access lists on switch ports could be implemented as additional microsegmentation means, in case if it is supported by platform vendor. These are alternative measures that allow partial microsegmentation in user dynamic environments, since they limit only horizontal movement.

A separate category of network nodes that will require special attention includes hosts that are located in the demilitarized zone and (or) publicly published on the Internet. Such assets have a significantly higher risk of compromise because they are exposed to external threats, not fully protected by a corporate firewall and might have allowed incoming access due to the architecture of the service they belong to. Such hosts are available for scanning by attackers 24x7 and cannot always be protected by WAF tools. Regardless of the criticality of these hosts, or belonging to some service, it is important to place them in individual segments and especially meticulously adhere to the principle of least privilege

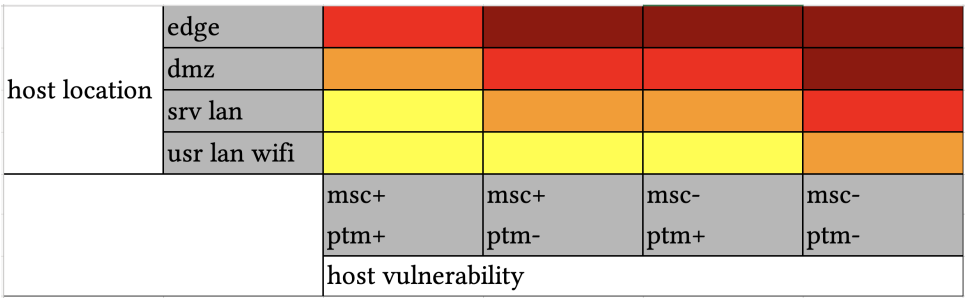

Figure 2: Host risk factor matrix.

in all possible directions, including access control not only to neighboring DMZ hosts or within the network, but also to the Internet. It is important to allow access in both directions by clearly specified source IP addresses, destinations, ports and applications.

There is also the idea that granularity should dynamically adapt to specific conditions, such as time, user behavior and threat levels, providing maximum flexibility while maintaining security [12]. This is an interesting and promising approach, but no such experiments and studies have been conducted in this study.

5. Research results

The methodology of adaptive microsegmentation design of the corporate network is proposed to be improved by the analytical method on the basis of a modified double risk matrix: Figure 2 and Figure 3. This approach allows determining the optimal size of a microsegment for placing a host or network hosts in it, depending on the criticality of the host in terms of business impact or data confidentiality level on the Y axis (1 – most critical, 4 -least critical) and the host risk factor on the X axis. The risk factor is a metric, which in turn will be determined by another risk matrix based on the host's location in the corporate network on the Y axis and the level of susceptibility to compromise depending on security factors on the X axis. Such factors can nominally be exposure, patch management process (ptm) coverage and the ability to configure security settings and support for the installation of security applications (msc). Thus, by analyzing the security factors and comparing the results with the degree of criticality of the host, we can calculate the granularity requirement of the microsegmentation for each of the network hosts in the following color-segment ratios:

- Dark red color - individual microsegment, full isolation;
- Red color is a microsegment with hosts that belong to the same service, without business-critical applications or storages with a high level of sensitivity data. Such hosts are located in a separate microsegment, dividing the enterprise service environment into several divided environments. Strict intra-group access will be organized and dense monitoring to be implemented;
- Orange color is a microsegment with any hosts that belong to the same corporate service, monitoring will be applied;
- Yellow color - a microsegment with hosts belonging to different services or a network segment in which control of horizontal movement is provided by access control lists or functions for blocking peer-to-peer connections. It may not needed classical network segmentation, monitoring only.

This approach deserves attention as a corporate network microsegmentation design tool and does not claim to be a universal and uncontested approach. The specifics of each individual infrastructure must be taken into account and adjusted in the development process. Additional to generated results some exceptions logic should be integrated into that decision-making process based on specific requirements each enterprise may have. They could include:

Criticality for business	1	2	1	1	1
	2	3	2	2	1
	3	4	3	3	2
	4	4	4	4	3
		green	orange	red	dark red
		risk factor			

Figure 3: Host microsegment size matrix.

- Existence of horizontal traffic communication patterns. If hosts don't communicate with each other (or shouldn't), they should not share a segment;
- Identity and access control capabilities. If hosts support strong identity-based policies (e.g., via mTLS, device identity, or EDR integration), then grouping is safer even across teams;
- Operational scalability. Too many individual segments can create policy sprawl. It makes sense to group similar low-risk, non-critical assets to keep management overhead reasonable;
- Compliance or regulatory requirements. Some standards (e.g., PCI-DSS, HIPAA) may mandate segmentation of specific systems. Hosts processing regulated data must often be in dedicated microsegments to prevent data leakage from lateral movement;
- Blast Radius Limitation. Use attack path modeling (e.g., with MITRE ATT&CK simulation) to determine if compromising one host in the group could compromise others. If yes, split the segment or harden inter-host communication;
- High-traffic, latency-sensitive applications degradation under complex segmentation. In such cases, usage of logical segmentation (e.g., host-based firewalls, identity policies) instead of physical or virtual isolation makes sence;
- Dynamic Re-Evaluation. Periodically re-evaluate groupings based on new vulnerabilities (e.g., CVEs affecting grouped systems), changes in business use, and user behavior analytics.

After the analysis and design of microsegmentation, the corporate network infrastructure takes the form of a certain set of microsegments of different capacities, which are interconnected, but access is regulated by firewall security policies. To ensure the primary value of microsegmentation, each microsegment must be provided with a separate corporate firewall zone, which in the future will make it possible to carry out access control in all directions and exclude or significantly minimize horizontal movement. Separately, it is worth mentioning various kinds of service zones, such as zones responsible for the connectivity of firewalls with each other, as well as interface zones that act as connection points to other network devices, such as routers or VPN hubs. For effective and granular access control, the zones for such segments shouldn't be shared.

As an example, let's consider designing microsegmentation for a small corporate network, which consists of 6-7 servers and a fleet of user devices, 3 different patterns. The implementation of this model will require an increase in firewalls from 1 to 2-3 devices and an increase in firewall zones from 3 to 10 at least.

This example of microsegmentation development reflects a change in the network architecture to provide flexible access control between its components and demonstrates an increase in the cost of implementation compared to a peer-to-peer network from one firewall with 3 zones to 2-3 firewalls with up to 16 zones in total (10 in fact, 6 for expansion).

The implementation of microsegmentation at the network level is always an increase in the complexity of the network topology, an increase in the number of security policies in the future, and the requirement of additional firewalls or network firewall resources. The size of the corporate infrastructure greatly affects the number of firewall zones required to deploy network microsegmentation and to a lesser extent affects the number of firewalls required to ensure traffic control in different locations. However, in any case, this leads to an increase in the cost of implementing microsegmentation and an increase in the cost of operational support compared to the costs of low-segmented networks.

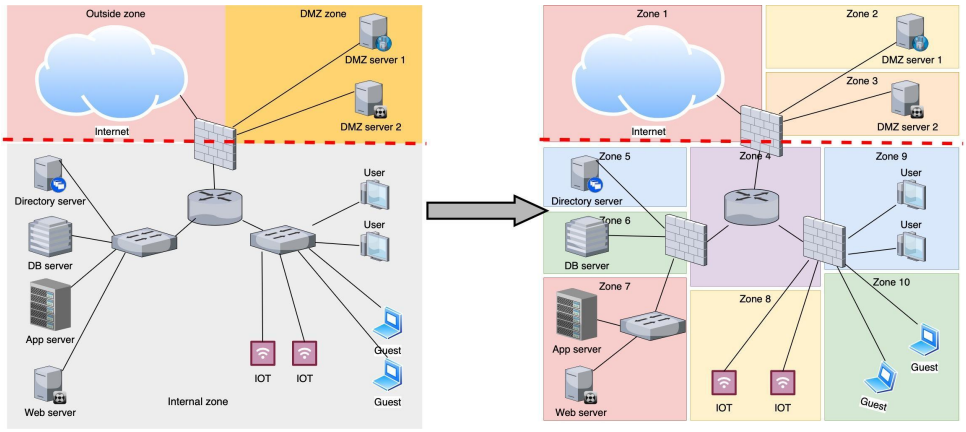

Figure 4: Illustrative example of network microsegmentation in corporate infrastructure.

If microsegmentation design requires the number of firewalls and their zones, which exceeds the allocated budget for implementation, the developed topology can be revised for optimization and reduction of the necessary resources for controlling network traffic or finding other means of implementing microsegmentation. Optimization measures may include reviewing the criticality of corporate hosts using risk matrices to determine the level of impact on the business and infrastructure in the event of their compromise. Hosts that have less impact on the company's business processes or have less potential for compromise can be combined into common microsegments and thus reduce the total number of firewalls required, their zones, and the number of policies that need to be created and then maintained.

Modern microsegmentation optimization techniques include implementing dynamic rules that adapt to user behavior and traffic, reducing the need for static, resource-intensive configurations. This allows for a reduction in the number of active zones while maintaining flexibility[3].

As for other microsegmentation implementation approaches, these include techniques for limiting horizontal traffic for user connections in dynamic segments of corporate networks. Access control to other network resources is partial and mostly static. Horizontal traffic can be blocked by means of organizing wireless networks, and in the case of wired connections, by using port access lists on the switch. Vertical access may or may not be allowed, in the latter case, it is assumed to connect a VPN with authentication and authorization to obtain vertical access to corporate resources or the Internet. In this way, each user, as a client of the network, is separated from other peers horizontally and his vertical access is regulated. This practice is justified due to the dynamism of the environment, the unification of access control and the reduction in the cost of implementation.

6. Conclusions

Microsegmentation is found to be an important element of the zero-trust architecture, as it divides the network into isolated segments, preventing lateral movement of attackers within the organization's corporate network. It creates the prerequisites for increasing the level of security and improving visibility in the network. The process of implementing microsegmentation involves a preliminary analysis of the organization's corporate infrastructure network topology, hosts and features, taking into account which allows you to develop its optimal design. Dense microsegmentation significantly increases the security of the infrastructure, but it is difficult in implementation and expensive. Individual design of microsegmentation based on the analysis of the existing infrastructure, the location of its nodes and assessment of the level of criticality for the business makes it possible to reduce the cost of its implementation and further maintenance, while ensuring compliance with the principles of zero trust.

The paper characterizes the features of microsegmentation design, analyzes its impact on the level of security, functioning and controllability of corporate infrastructure elements, studies the impact

on the infrastructure of microsegmentation implementation with different granularity. An analytical method for adaptive design of a corporate network microsegmentation using a double risk matrix for host analysis and determination of the optimal level of granularity of microsegments depending on certain factors is proposed. It has been established that despite the high level of protection in microsegmentation with individual segments for all network hosts, the optimal solution is to use a microsegmentation design with a variable size of microsegments depending on the criticality of the host, its security status and location.

Further areas of research may be the combination of effective implementation with operational support of security policies in a microsegmented network as an element of building a zero-trust architecture.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] M. Ma, Z. Yu, B. Liu, Automatic generation of network micro-segmentation policies for cloud environments, in: 2023 4th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), 2023, pp. 1–5. doi:10.1109/AINIT59027.2023.10212857.

[2] N. Basta, M. Ikram, M. Kâafar, A. Walker, Towards a zero-trust micro-segmentation network security strategy: An evaluation framework, in: NOMS 2022 - IEEE/IFIP Network Operations and Management Symposium, 2021, pp. 1–7. doi:10.1109/NOMS54207.2022.9789888.

[3] S. Noel, V. Swarup, K. Johnsgard, Optimizing network microsegmentation policy for cyber resilience, The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology 20 (2021) 57–79. doi:10.1177/15485129211051386.

[4] M. Mujib, R. Sari, Performance evaluation of data center network with network microsegmentation, in: 2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE), 2020, pp. 27–32. doi:10.1109/ICITEE49829.2020.9271749.

[5] Y. Liu, G. Liu, H. Du, D. Niyato, J. Kang, Z. Xiong, D. Kim, X. Shen, Hierarchical microsegmentations for zero-trust services via large language model (LLM)-enhanced graph diffusion, arXiv preprint abs/2406.13964 (2024). doi:10.48550/arXiv.2406.13964.

[6] N. Sheikh, M. Pawar, V. Lawrence, Zero trust using network micro segmentation, in: IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2021, pp. 1–6. doi:10.1109/INFOCOMWKSHPS51825.2021.9484645.

[7] J. S. Al-Azzeh, M. A. Hadidi, R. S. Odarchenko, S. Gnatyuk, Z. Shevchuk, Z. Hu, Analysis of self-similar traffic models in computer networks, International Review on Modelling and Simulations 10 (2017) 328–336. doi:10.15866/iremos.v10i5.12009.

[8] Z. Hu, Y. Khokhlachova, V. Sydorenko, I. Opirskyy, Method for optimization of information security systems behavior under conditions of influences, International Journal of Intelligent Systems and Applications 9 (2017) 46–58. doi:10.5815/ijisa.2017.12.05.

[9] S. Keeriyattil, Microsegmentation and zero trust: Introduction, in: Zero Trust Networks with VMware NSX, Apress, 2019. doi:10.1007/978-1-4842-5431-8_2.

[10] P. Zhang, C. Tian, T. Shang, L. Liu, L. Li, W. Wang, Y. Zhao, Dynamic access control technology based on zero-trust light verification network model, in: 2021 International Conference on Communications, Information System and Computer Engineering (CISCE), 2021, pp. 712–715. doi:10.1109/CISCE52179.2021.9445896.

[11] B. Paul, M. Rao, Zero-trust model for smart manufacturing industry, Applied Sciences (2022). URL: https://doi.org/10.3390/app13010221. doi:10.3390/app13010221.

[12] W. Lei, Z. Pang, H. Wen, W. Hou, X. Zhang, Edge-enabled zero trust architecture for icps with

spatial and temporal granularity, in: 2023 IEEE 6th International Conference on Industrial Cyber-Physical Systems (ICPS), 2023, pp. 1–6. doi:10.1109/ICPS58381.2023.10127999.

[13] R. Syrotynskyi, I. Tyshyk, O. Kochan, V. Sokolov, P. Skladannyi, Methodology of network infrastructure analysis as part of migration to zero-trust architecture (short paper), in: CSDP-2024: Cyber Security and Data Protection, Lviv, Ukraine, 2024, pp. 97–105.

[14] V. M. Maksymovych, et al., Generator of pseudorandom bit sequence with increased cryptographic security, Metallurgical and Mining Industry: scientific and technical journal (2014) 25–29.

[15] I. Opirskyy, et al., Pseudorandom sequence generator based on the computation of ln 2, in: CEUR Workshop Proceedings, volume 3829, 2024, pp. 79–86.

[16] V. Susukailo, et al., Methodology of isms establishment against modern cybersecurity threats, in: Lecture Notes in Electrical Engineering, Springer International Publishing, Cham, 2021, pp. 257–271. doi:10.1007/978-3-030-92435-5_15.

[17] S. Vasylyshyn, et al., A model of decoy system based on dynamic attributes for cybercrime investigation, Eastern-European Journal of Enterprise Technologies 1 (2023) 6–20. doi:10.15587/1729-4061.2023.273363.

[18] O. Deineka, et al., Designing data classification and secure store policy according to soc 2 type ii, in: CEUR Workshop Proceedings, volume 3654, 2024, pp. 398–409.

[19] S. Douma, The two-tier system of corporate governance, Long Range Planning 30 (1997) 612–614. doi:10.1016/S0024-6301(97)00047-2.

[20] N. Dowling, A. Punt, L. Little, C. Dichmont, D. Smith, M. Haddon, M. Sporcic, E. Fulton, R. Gorton, Assessing a multilevel tier system: The role and implications of data quality and availability, Fisheries Research 183 (2016) 588–593. doi:10.1016/J.FISHRES.2016.05.001.

[21] M. Khan, Zero trust architecture: Redefining network security paradigms in the digital age, World Journal of Advanced Research and Reviews (2023). doi:10.30574/wjarr.2023.19.3.1785.

[22] N. Sytnik, M. Kravchenko, Application of knowledge management tools: Comparative analysis of small, medium, and large enterprises, Journal of Entrepreneurship, Management and Innovation (2021). doi:10.7341/20211745.

[23] B. Da Rocha, L. De Melo, R. De Sousa, Preventing apt attacks on lan networks with connected iot devices using a zero trust based security model, in: 2021 Workshop on Communication Networks and Power Systems (WCNPS), 2021, pp. 1–6. doi:10.1109/WCNPS53648.2021.9626270.