Markus Kallatsa

STRATEGIES FOR NETWORK SEGMENTATION: A SYSTEMATIC LITERATURE REVIEW

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

ABSTRACT

Kallatsa, Markus
Strategies for Network Segmentation: A Systematic Literature Review
Jyväskylä: University of Jyväskylä, 2024, 76 pp.
Cyber Security, Master's Thesis
Supervisor: Hämäläinen, Timo

Organizational information assets are increasingly being stored digitally over information networks. Therefore, organizations should pay equal attention to the design and security of their networks in addition to other security arrangements. There are several security mechanisms that contribute to the computer network security. One of which is network segmentation that involves breaking up the network into architecturally smaller subnetworks called segments, between which traffic is controlled. Another and more recent mechanism based on the same principle is micro-segmentation, which takes segmentation into fine-grained level where granular segments have their own segment-level security policies closer to the protectable resources. General objective of network segmentation is to minimize adversary's potential for lateral movement by isolating protectable resources into segments separated from each other. This study delves deeper into network segmentation by examining through systematic literature review how the topic has been dealt in the research literature. Overall 29 publications were reviewed and analyzed on a thematic-driven basis. Current segmentation approaches and technical solutions including their benefits and drawbacks are included in the review. As a result, relevant organizational attributes related to segmentation process were identified such as costs, performance, manageability, protectability, granularity, size and dynamism. Another observed trend was related to utilization of automation tools in network segmentation. Finally, based on the results of the systematic literature review, the study concludes with practical recommendations based on a three-phased network segmentation process.

Keywords: network segmentation, macro-segmentation, micro-segmentation, network security, information security

TIIVISTELMÄ

Kallatsa, Markus
Strategioita tietoverkon segmentointiin: Systemaattinen kirjallisuuskatsaus
Jyväskylä: Jyväskylän yliopisto, 2024, 76 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Hämäläinen, Timo

Organisaatioiden tietovarantoja säilötään yhä enenevissä määrin digitaalisesti ja tietoverkkovälitteisesti. Näin ollen organisaatioiden tulisi yhtä lailla kiinnittää huomiota tietoverkkojensa rakenteeseen ja turvallisuuteen muiden turvallisuusjärjestelyjen lisäksi. Tietoverkkojen tietoturvaa edistäviä turvallisuusmekanismeja on olemassa useita. Eräs mekanismeista on tietoverkon segmentointi, jolla tarkoitetaan tietoverkon jakamista arkkitehtuurillisesti pienempiin ja toisistaan eristettyihin aliverkkoihin eli segmentteihin, joiden välistä liikennettä kontrolloidaan. Samaan periaatteeseen pohjautuva ja hieman uudempi lähestymistapa on mikrosegmentointi, joka vie segmentoinnin hienojakoisemmalle tasolle. Mikrosegmentoinnissa segmenttikohtaisia turvallisuusperiaatteita sovelletaan segmenttitasolla lähempänä suojeltavaa resurssia. Segmentoinnin yleisenä tavoitteena on minimoida hyökkääjän lateraalisen liikkumisen mahdollisuuksia eristämällä suojeltavat kohteet toisistaan erillään oleviin segmentteihin. Tässä tutkimuksessa syvennytään systemaattisen kirjallisuuskatsauksen kautta tietoverkkojen segmentointiin tarkastelemalla, miten aihetta on käsitelty tutkimuskirjallisuudessa. Kaiken kaikkiaan tutkimuksen tarkasteluun päätyi 29 julkaisua, joita analysoitiin teemapainotteisesti. Tarkasteluun on sisällytetty tämänhetkisiä segmentoinnin lähestymistapoja, teknisiä ratkaisuja sekä turvallisuusnäkökohtia mukaan lukien segmentoinnin hyötyjä ja haittoja. Tutkimuksen tuloksena tunnistettiin tietoverkon segmentointiprosessiin liittyviä, asiaankuuluvia organisatorisia attribuutteja, kuten toteutuksen kustannukset, suorituskyky, ylläpidettävyys, suojattavuus, hienojakoisuus, koko ja dynaamisuus. Toinen havaittu trendi liittyy automaatiotyökalujen soveltamiseen segmentointiprosessissa. Lopuksi systemaattisen kirjallisuuskatsauksen tulosten pohjalta esitetään käytännön suosituksia, jotka pohjautuvat kolmivaiheiseen tietoverkon segmentointiprosessiin.

Asiasanat: tietoverkon segmentointi, makrosegmentointi, mikrosegmentointi, tietoverkkoturvallisuus, tietoturva

LIST OF FIGURES

LIST OF TABLES

TABLE OF CONTENTS

1 INTRODUCTION

There is little end in sight to the growing burden created by cyber threats. According to Cybersecurity Predictions for 2024 from Norton Labs, it is expected that the cyber threat landscape will be populated by dense and highly personalized attacks (Pechoucek, 2023). Breaches and vulnerabilities of information systems can be multidimensional in nature, making it difficult to work on accurate threat perceptions and risk assessment. This contributes to forcing the defenders to dynamically design their defense mechanisms against constantly evolving threats. The challenge may not be easy to solve, given the manageability of complex systems, the difficulty of predicting emerging threats and the requirement to be able to understand interdependencies between the above two in depth.

Compared to the primitive digital systems from a couple of decades ago, there is one significant factor that should be emphasized in modern information security: the evolution of computer networks. Where devices have evolved to process information in a more advanced and efficient way, networks make it possible to connect these devices to each other while enabling communication between them. Looking at the evolution of malware threats, there was a phase of widespread network worms, which were the most common threats as internet developed (Alenezi et al., 2020). Since then, the types of network-based threats have become even more diverse.

From email-borne worms and other malware, we have reached the point where advanced cyber threats are used as a tool for extortion, damage and even warfare. For instance, the concept of ransomware originated in the 1980s, but it emerged as a significant risk to enterprises following the growth of cryptocurrency in 2010, which has become criminals' preferred payment method (Leo et al., 2022). As another example from context of cyber warfare, offensive cyber operations present strategic opportunities to obtain contextual and tactical advantage by disrupting enemy systems and weaken their confidence in their equipment (Bronk & Watling, 2021).

Research focusing on cybersecurity is therefore of paramount importance to minimize the wider damage of cyber-attacks. However, cybersecurity as an interdisciplinary research area is not only limited to technological aspects, but

also falls between law, psychology and sociology (Fujs et al., 2019). When approaching the security concept, it is therefore necessary to consider several different perspectives.

As we live in an era when digital systems are being used to minimize paperwork, organizations have either partially or fully migrated to digital environments using computer networks in order to streamline work. When it comes to the organizational network security, digital platforms and services may allow an attacker to gain access to the target organization. In the worst-case scenario, the whole organization uses a flat large-scale network, having both user devices and services easily accessible from a single point. Once the attacker gets inside that network, there is a wide range of possibilities available for exploitation. However, various security mechanisms have been put in place to reduce the attack surface in the case described above.

In order to ensure that the design of the network does not pose a security risk, we should focus in particular on network design and architectural aspects. Instead of having a single flat network, the network entity should be broken down into smaller subnetworks called *segments* (also known as *enclaves*) that are separated to each other. At the concept level, such an approach is called *network segmentation*, the aim of which is to minimize the potential for lateral movement of an attacker and protect resources within each secured segment (Simpson & Foltz, 2021). In addition, network segmentation plays a huge role in modern network security as a principle of widely adapted *zero trust model*. In the zero trust model, no user or device is automatically trusted regardless of their position or where they are located (Syed et al., 2022).

On the whole, technology-driven research in cybersecurity needs to be initiative-taking, because as technology evolves, so do the various technical vulnerabilities. More broadly, the research value extends beyond the scientific community to support the security of organizations and individuals. An increasing number of actors are dependent on technology nowadays, so knowledge of its secure application is an advantage in improving the general level of cybersecurity. Cybersecurity research has a vital role to play in advancing this goal.

From an objective point of view, this study is firstly a contribution to the above-mentioned general-level cybersecurity research. When looking at the computer networks of organizations, network architecture is one critical area of consideration. This thesis focuses on the same theme by taking a closer look at network segmentation and its current situation in the research literature. Based on current knowledge, no past literature reviews around network segmentation exist. Hence implementation of such would also promote research on that subject by shedding light on the current situation and by naming research gaps and challenges.

Fundamental research goal of this study is to gain a deeper understanding of network segmentation and its implementation in an organization. It should be noted that there can be significant differences between organizations and therefore usefulness of implementation and its methods can be dependent on the

context. The research problem of this study therefore boils down to one main research question:

RQ1. How network segmentation implementation should be approached in an organization considering the necessary attributes of that organization?

The main research question is followed by the following supporting research questions:

RQ2. What strategies and technical solutions for network segmentation exist?

RQ3. What are the benefits and drawbacks associated with different approaches of network segmentation?

For clarification, RQ1 does not, by its very nature, seek to identify solutions for network segmentation in each and every organization type and their networks. Instead, perception of both organizational and network-related attributes helps to support decision-making in network segmentation planning. Since relevant attributes are known, the delimitation of options is more feasible. RQ2 covers both strategies and technical solutions since the strategies are to some extent dependent on the technical implementation. RQ3 relates to the impacts that network segmentation may cause. These effects include enhancement of organizational security posture in addition to other advantages and disadvantages that network segmentation could introduce.

Contribution of this study is formed from the set of results corresponding to all of these research questions. For applying network segmentation effectively, we need to know available options, their impact on the network and the organization that uses it. Thus, practical recommendations for network segmentation design are presented as a part of this thesis. Strategic recommendations involve implementation guidelines for network segmentation based on the current knowledge of research literature.

This thesis is structured into chapters. The first and current chapter introduces the reader to the topic, including a description of the motivation for the research and preliminary justification for the choice of research methodology. The second chapter presents theoretical background for the topic before the actual research. The third chapter contains a more detailed definition of research methodology and its intermediate steps applied in this study. The fourth chapter presents the results. The fifth chapter presents the contribution of this study in a form of implementation guidelines on how to apply network segmentation as a network security mechanism. The sixth and final chapter contains discussion and critical review based on the results in addition to conclusions and implications for future research.

2 THEORETICAL BACKGROUND

In this chapter a theoretical basis for the study is provided. In the beginning, a simplified example of network segmentation is presented. The definitions, concepts and technical solutions of what is most relevant to the study have been also presented, including a brief overview of how zero trust model is applicable in the case of micro-segmentation.

2.1 Network Segmentation

In the modern era computer networks interconnect many more clients than just traditional personal computers. Business is gradually moving to the cloud environments, extending the share of devices and virtual services within both internal and external networks. As a real-life example, major international IT corporations utilize cloud technologies to deploy numerous virtual machines running production software, enabling them to offer a diverse range of services to their clients across the globe (Mescheryakov et al., 2020). Where in the old days a single firewall protected one network for entire organization, today that same protection is no longer enough.

Consider an example network where network protection is built on a single firewall (FIGURE 1). In addition, let us assume that management of that single firewall is done manually. For instance, if human error causes some fundamental firewall rule to be configured incorrectly, the target group exposed to the error could be all the devices and services connected to that network. A single point of failure thus is a threat to the whole organization.

Before thinking any architectural changes, communication and security requirements should be acknowledged. For example, let us assume that servers are the most critical part of the example network in FIGURE 1. Therefore, servers could be placed into their own segment (enclave) and database into their own. Communication could be restricted in a way that only servers and admin can access the database. In addition, client and admin will be separated due to the

diverging access rights to the resources. In conclusion, divided network based on the specification above is depicted in FIGURE 2.

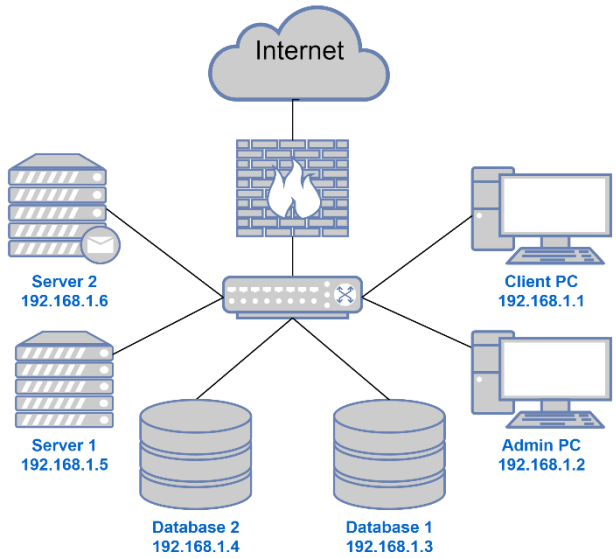

FIGURE 1 Flat network without segmentation

It should be noted that the divided network (FIGURE 2) is only partially implemented in terms of extensive network segmentation. Additionally, firewalls could be placed according to communication requirements in order to control and restrict the network traffic within each segment and between the segments. Even more, the implementation allows for a more targeted monitoring and logging since each segment is separated.

In summary, network segmentation necessitates architectural changes to the network to be segmented. More detailed execution depends on attributes of the target network, utilized technologies and requirements from different perspectives. Attention must also be paid to a number of other aspects and their interdependencies.

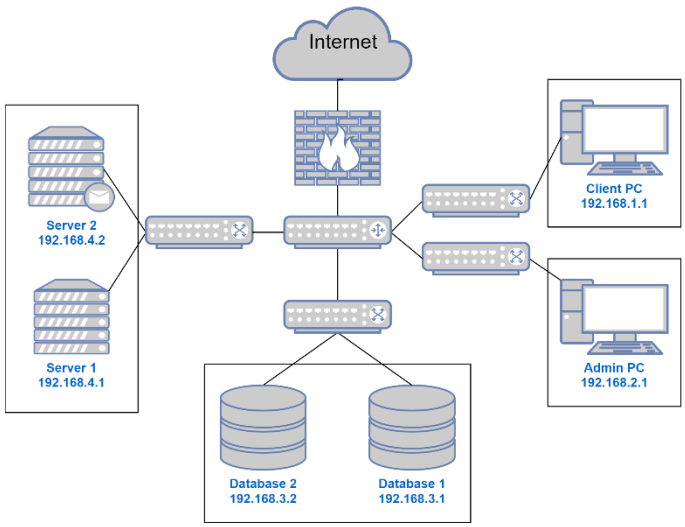

FIGURE 2 Segmented network without access control

The segmentation example shown above was to some extent simplified in order to support understanding of the original concept. The number of segmentation options increases significantly if the network is larger and more complex. This creates an interesting phenomenon that requires research and evidence of proven solutions to reach an optimal outcome.

2.2 Definition of Key Terms and Concepts

It is essential for this research to explicitly define a few abstract concepts that recur in the research. Previous definitions exist, but these will be used as a basis for a few refinements to make the definition of network segmentation more supportive to this study.

Network segmentation is often defined, as per Wagner et al. (2019), "into a practice of partitioning a computer network into multiple segments and restricting communications between segments to inhibit a cyber attacker's ability to move and spread infection". However, in this study the definition of complete process of network segmentation is further refined to meet the objectives of the study. Therefore network segmentation is thought as a process consisting of three phases. This definition could be expressed as follows:

> Network segmentation is a network security mechanism and a process that aims to divide one target network into separate segments allowing better restriction and control of traffic between each segment. The segmentation process involves three phases involving (1) grouping of resources to be placed within each segment, (2) network topology realization in which these segment groups within subnetworks are formed in practice and finally, (3) implementation of access control between these segments.

The definition does not only state why segmentation is implemented. In addition, differentiating between phases helps to fit inferences from data to the theory. Multiple phases of the process (e.g., second phase and third phase simultaneously) can of course be treated as one, but when done this way, it is not necessarily defined separately and precisely how the allocation of segments is done and what technologies are used for each phase. For example, grouping of segments could be done automatically with machine learning techniques and the implementation manually using physical segmentation approaches in which firewall and monitoring system of a third-party vendor is applied. Later in this study these defined network segmentation phases are referred to as follows: (1) network topology design phase, (2) network topology realization phase, and (3) access restriction phase.

When talking about sizes of the segments, in this study the segmentation approaches are divided in the traditional way based on the frequently used definitions of *macro-segmentation* and *micro-segmentation*. For instance, Simpson & Foltz (2021) presented a fortress approach example, where the number and size of fortresses (protectable segments) can vary depending on which school of thought (macro or micro) the segmentation approach belongs to. To the best of

the current knowledge, there is no precise universal definition of thresholds for the resources in the segment for both definitions. For example, micro-segmentation protects either a single resource or collection of resources (Katsis et al., 2021; Syed et al., 2022).

However, in this study tentative definitions of macro-segmentation and micro-segmentation are explicitly established, which in turn helps to better illustrate the differences between these two approaches. Declarative definitions can be expressed as follows:

> Macro-segmentation refers to a technique used for selection of resources to be placed within each segment in a way that there is more than one, but typically multiple protectable resources within a single segment.
>
> Micro-segmentation refers to a technique used for selection of resources to be placed within each segment in a way that there is typically one, but in some cases also a few more protectable resources within a single segment.

It should be noted that these definitions are not mutually exclusive, but when taken to extremes they are clearly distinguishable. Considering the whole segmentation process, this can be usually inferred from the context when looking at the overall picture.

Alongside network segmentation, in some contexts *network segregation* is mentioned. Definitions of segmentation and segregation may vary depending on the author. For instance, Arnaud & Wright (2016) define segmentation as a model in which LANs are separated from each other in a way that they are unable to communicate to each other, and segregation as an action where rules are added in order to control the network traffic. This can to some extent be seen as a separation between topology realization and access restriction phases per definition presented above. On the contrary, network segmentation and segregation are said to often refer to the same thing, just like network partition and isolation (Cisco, n.d.). However, in this study only one main term (network segmentation) is used to describe the issue as defined above, thus, including the access restriction phase in addition to the separation of segments.

When a network is compromised, network security controls can be crucial to improve visibility and stop malicious actors from moving laterally across the network (Sheikh et al., 2021). Often it is said that network segmentation and especially ZTA aim to minimize adversary's potential for *lateral movement*. For example, ZTA was created to deal with the lateral movement in target networks (Simpson, 2022). In order to locate the target, malware spreads through the target network onto new devices as a part of the lateral movement (King & Huang, 2023, p. 2). In its simplicity, therefore lateral movement is defined as an extension of the malicious activities of adversary on the target network.

2.3 Key Technical Solutions

Network segmentation is a technical network security mechanism in nature. The most common related technical solutions are *Virtual LAN*s (VLANs), *Private Virtual LAN*s (PVLANs), *Software-defined Networking* (SDNs) and *Access Control Lists* (ACLs). In this subchapter, these technical solutions are briefly examined.

2.3.1 Virtual LAN (VLAN) and Private VLAN (PVLAN)

To begin with the definition of Local Area Network (LAN), as a broadcast domain, LAN typically enables communication of all connected physical LAN devices in a way that router is not required (Ali Abdullah, 2019). A group of devices on multiple physical LAN segments that can communicate as they share a common network segment is what is commonly referred to as Virtual LANs (VLANs) (Makeri et al., 2021). In VLAN, a management switch can divide interfaces (ports) into groups based on the desired network requirements (Gatra et al., 2019).

VLAN is a one technical solution for network segmentation. Using VLAN it is possible to form different broadcast domains in order to restrict access at all network levels (Makeri et al., 2021). Often on relying on incoming physical port numbers or MAC addresses, VLANs offer machine-based security (Simpson & Foltz, 2021).

In addition to VLANs, Private VLANs (PVLANs) are also an opinion for network segmentation in the second layer. In PVLAN, endpoints are isolated, which means that endpoint connection on the same IP network could be restricted. Three roles (promiscuous, community or isolated) can be used to restrict communication and allow ports with certain roles to communicate with each other. (Álvarez et al., 2023)

As a concrete example, manageable network devices such as switches and routers made by Cisco and Brocade support VLAN management. Setup and configuration vary between devices, so there is no unambiguous way to implement VLANs in a network. However, after the setup, switch creates separate broadcast domains that are called the VLANs. (Gatra et al., 2019)

2.3.2 Software-defined Networking (SDN)

Software-defined networking (SDN) enables to innovatively design, implement and maintain networks with separate control through control plane and forwarding process though data plane (Benzekki et al., 2016). SDN has emerged a highly desirable platform for network virtualization due to its ability to enable tenant-specific control logic to operate on a centralized controller, rather than relying on physical switches (Drutskoy et al., 2013, p. 21). Three-layered architecture of SDN consist of data forwarding layer (switches), control layer (controller), and application layer (Shu et al., 2016).

The responsibilities of SDN controller include configuration, management, monitoring, and diagnostics of the virtual network infrastructure (Zahwa et al., 2023). Furthermore, SDN allows for flexible and dynamic network control, making work more efficient in environments where manual workload could otherwise increase due to the ever-changing network environment (Ramprasath & Seethalakshmi, 2021).

Network segmentation activities represent to some extent resource management since resources are grouped within segments. SDN paradigm serves this purpose well as it allows obvious separation between data plane and control plane services (Qin et al., 2014). Per Goransson & Black (2014, pp. 25–26), network activities are attempted to be segregated by SDN in a following way:

- Prioritization, access filtering and forwarding remain locally on the device.
- Centralized controller takes control of the network, taking the complex management burden off the device.
- Higher-level functionalities and involvement in decision-making are done above the controller in which network applications are run.

OpenFlow is considered as the de facto standard of SDN as well as it is widely adapted in research community and industry. Concrete examples of SDN-based products are SDN-enabled network virtualization software such as VMware NSX and VSP of Nuage Networks. In addition, SDN solutions have been adopted in data centers owned by Google and Microsoft. (Shu et al., 2016)

2.3.3 Technical Tools for Access Restriction

Many networking and security tools, such as firewalls and routers that perform i.e. packet filtering and monitoring, are built on Access Control Lists (ACLs) (Daly et al., 2016). To keep track of all incoming and outcoming packets, access control lists are set up at each point of entry between concealed network and the outside internet (Chate & Chirchi, 2015). Since network segmentation introduces multiple entry points due to separated segments, these entry points are subject to control in relation to access management in network segmentation.

Network administrations typically create ACLs to specify how each data packet should be handled when entering or leaving a network switch (Zahwa et al., 2023). For instance, firewalls classify the access based on rules that are defined in ACLs. Therefore ACLs policies are used for both dynamic and static traffic filtering by either allowing or disallowing the traffic to and from the network based on certain values, such as IP and port addresses (Ramprasath & Seethalakshmi, 2021).

ACL can be seen to some extent as a high-level access restriction tool in technical network security controls. In addition to firewalls, ACL could be utilized in SDN as well. For example, Ramprasath & Seethalakshmi (2021) presented an application where ACL policies are used for filtering out malicious network traffic in SDN environment established with OpenFlow switches. As another concrete example of ACL usage is a router that is capable of implement ACL-

based filtering where source addresses, destination addresses and other features of network protocols (Palugyai, 2005).

Firewalls can be divided into three different generations, where 1st generation firewalls operate on the transport layer as packet filters, 2nd generation firewalls operate on the same level with stateful packet inspection, and 3rd generation firewalls operate on the application-level where different proxies are required for each service (Haar & Buchmann, 2019). Traditional firewalls support packet filtering, network address translation (NAT), stateful review (up to layer 3), stability, low latency and safe operation, while next-generation firewalls (NGFWs) have some advanced features such as application control, identity check, anti-malware, capability for SSL inspection and intrusion detection and prevention systems (IDS/IPS) (Uçtu et al., 2021).

2.4 Zero Trust Model and Network Segmentation

Traditional perimeter-based security architectures have found it difficult to efficiently protect both enterprise assets and critical infrastructures due to continuous growth of Internet of Things (IoT) and edge-computing platforms (Syed et al., 2022). In response to this, zero trust model has increased its popularity. According to zero trust proponents, cybersecurity engineers should implement a different architecture that does not rely on trusting anything (Michael et al., 2022). For the actual zero trust architecture (ZTA) implementation, micro-segmentation is suggested by NIST as one of the core strategies (Syed et al., 2022).

ZTA includes several components, some of which are also relevant for the purposes of this study as access control mechanisms including these are presented in the results. Following three components are considered as core logical components in the zero trust model: policy enforcement point (PEP), policy administrator (PA) and policy engine (PE) (Rose et al., 2020; Syed et al., 2022). These components and their interdependencies to each other are illustrated in FIGURE 3.

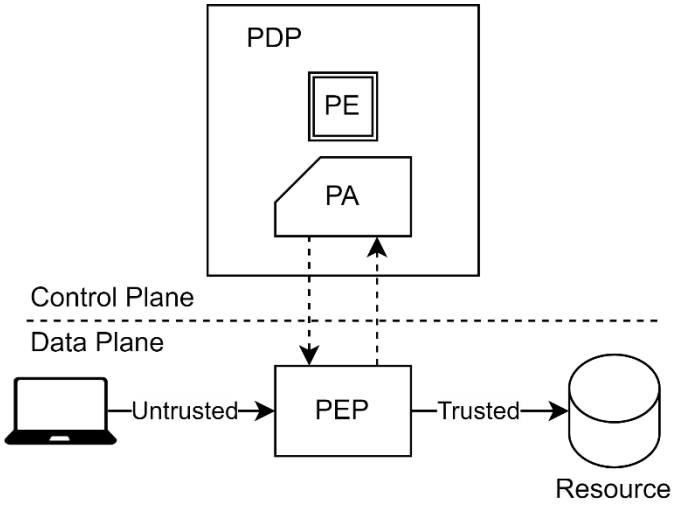

FIGURE 3 Core logical ZTA components (Rose et al., 2020; Syed et al., 2022)

When client is accessing some resource, PEP monitors the connection and talks to PA for policy enforcement. PA in turn relies on the access decision that is made by PE. Decision is made in accordance with business policies in a way that external inputs are given to a trust algorithm which can be considered as a "brain" for the entire system. After positive decision, the access is granted to trust-zone, which is the term used for the area beyond PEP. (Rose et al., 2020; Syed et al., 2022)

As a very concise description of the ZTA core logical components, this approach will emerge when micro-segmentation is discussed in more detail, in particular when access restriction phase is addressed. However, this study will not go into ZTA in depth, but a basic understanding of the operational logic of ZTA core logical components is essential when looking at the implementation of micro-segmentation, which is one of the principles of zero trust model.

2.5 Conceptual Model of Network Segmentation Process

A definition of network segmentation process for the study was presented earlier. The definition only considers the process, but it does not cover an organization as the initiator of the process. For this purpose, a conceptual model is also presented to complement the theoretical basis of the study, describing the process from a higher-level, which also includes the role of the organization in the process.

Conceptual model of network segmentation process involving target organization is presented in FIGURE 4. Organization is considered as a starting point for network segmentation and organization's network without applied network segmentation is presented as initial network that is converted to segmented network during the segmentation process.

Organization has its requirements and available resources for implementing them. Implementation and maintenance of segmentation architectures can demand significant resources, potentially leading to a decline in mission performance (Wagner et al., 2019). Since each organization has to some extent unique requirements that call for customized solutions for each situation, delivering effective cybersecurity is a challenging problem (Tselios et al., 2022). Therefore requirements could be set by a number of different parties such as organizational policies and general regulations.

It should be noted that network segmentation is not considered here as a one-off operation but more of a continuous process where segmented network needs maintenance done by the organization. After network modifications and change in the number of instances connected to the segmented network, the segmentation and policy specification might need to be adjusted and that is again dependent on the organization. For example, IoT devices introduce requirements for operational and scalability (Paillisse et al., 2020). This is reflected in the need for the network to constantly adapt to changing situations.

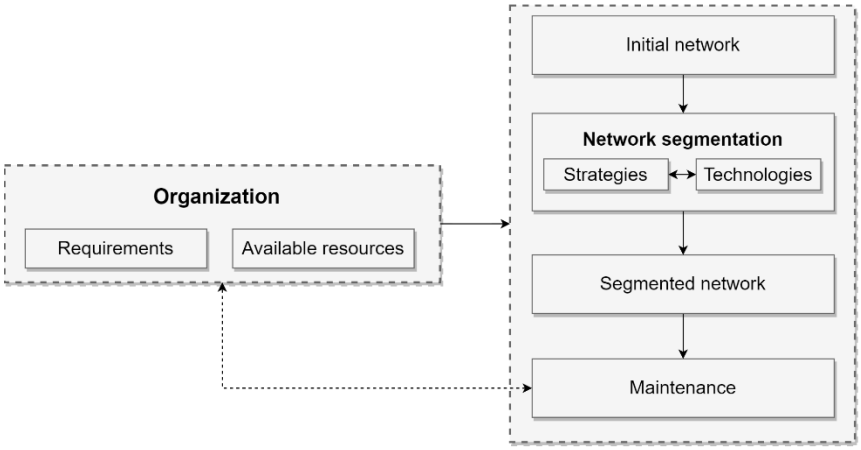

FIGURE 4 Conceptual model of organizational network segmentation

Segmentation process involves both strategies and technologies. Strategies are dependent on the technologies and vice versa since technologies are put in place in the application of the strategies. In brief, in this study network segmentation is seen as process in which initial network is the input and segmented network is the output which in ultimately requires the organization to act in terms of maintenance.

3 RESEARCH METHODOLOGY

In this chapter a brief background on the choice of the research method, its general purpose and application in this study is presented.

3.1 Research Design

Many sources of research literature claim the fact that no clear guidelines exist on how to implement network segmentation in practice. For instance, Wagner et al. (2016) confirm that network segmentation is a crucial defence mechanism, but they also highlight the fact that it is not known how to implement it decently. This encourages approaching the research problem applying both qualitative and quantitative methods. Of particular interest is the extent to which network segmentation has been addressed in research literature in the past and in what way. Quantitative analysis methods could be used to identify the quantities and characteristics of the target literature. For an extensive understanding of the topic, applying qualitative methods is appropriate. This includes, for instance, finding out the choices behind decisions regarding network segmentation arrangements. Therefore both research method types are convenient for the study.

Okoli (2015) presents an eight-step guide to conducting a systematic literature review in which it is shown that both qualitative and quantitative approaches can be utilized in multiple phases, as in data extraction and execution phases. According to Levy & Ellis (2006), an efficient literature review achieves understanding of the present state of the body of knowledge by establishing a solid theoretical basis for the proposed research. Together, these features pursue the objective of promoting research on network segmentation.

Grant & Booth (2009) have characterized overall fourteen different literature review types by methods used, one of the methods being *systematic search and review*. In addition to traditional systematic review, authors mention that systematic search and review method has features of critical review as well as having comprehensive search process for addressing broad questions. The main

objective of critical review is to identify strengths and weaknesses among other things related to a particular topic of interest (Paré & Kitsiou, 2017). Critical evaluation fits the nature of the research objectives of this study in such a way that it would potentially provide guidelines for future research and challenge existing strategies.

When it comes to perceived weaknesses of systematic search and review, part of critical review may be limited due to explicit inclusion and exclusion criteria of search (Grant & Booth, 2009). On the other hand, omission of a well-defined search and analysis processes could expose the issues noticed in other type of literature reviews. For instance, narrative reviews may have tendency to selectively ignore certain studies in order to support arguments (Paré & Kitsiou, 2017). Overall, the aim of this study is not, first of all, to prove validity of certain claims nor to focus on a critical analysis. Instead, the aim is to produce, with an investigate attitude, a specific analysis of the current situation through a clearly defined study and furthermore to present recommendations based on the synthesized knowledge. Consequently, a suitable combination of an analytical assessment and efficiently formulated research methodology supports the initial purpose of this study.

After examining the properties of different literature review methods, research was decided to base on *systematic review* that also utilizes critical evaluation presented in systematic search and review approach. The reasons for the choice are focused on synthesis and analysis approaches. Systematic review synthesis usually involves a narrative approach accompanied by tabular data, aiming to identify recommendations for practice as well as unresolved issues in the research literature (Grant & Booth, 2009). In addition to systematic review synthesis, a critical review will be presented separately at the end.

Since implementation guidelines and best practices are to be presented as a part of this thesis, attention should be paid on the selected research in the review. Therefore validity of the referenced articles should be ensured in order to use quality literature as a foundation of research (Barnes, 2005; Levy & Ellis, 2006). Quality assurance of the source literature is partly ensured by inclusion and exclusion criteria and quality assessment form defined in the research methodology, but these also offer the possibility of replicating the research which in turn increases the research value in a certain way.

3.2 Overview of Systematic Literature Review

Literature review can be conceived as a generic research concept from which multiple sub-types can be derived. When it comes to a rough classification of literature reviews, the concept of *systematic literature review* and its differences from other literature review types should be understood before proceeding to design phase of the study. When comparing between systemic reviews and traditional narrative reviews, a clear distinction can be made. Systematic reviews are different from traditional narrative reviews in that systematic reviews have a

transparent, repeatable and scientific process that reduce bias and provide an audit trail of reviewer's choices, actions and conclusions (Cook et al., 1997; Tranfield et al., 2003).

Since academic knowledge expands significantly with the appearance of new scientific publications, it is important to structure and critically assess the existing and available information based on these releases. At that point, literature reviews serve as one of the options. According to Linnenluecke et al. (2020), a literature review can help the research process by:

- finding theoretical support
- determining a context and delimiting a research problem
- rationalizing a problem and new lines of enquiry
- avoiding pointless study
- identifying the primary results and the methodologies employed in early studies
- separating what has already been done from what still needs to be done

Therefore literature review can be used in a number of separate ways to address the research problem. In addition to this, literature review also provides information for further research by finding out what is currently known about the topic and what aspects have not yet been researched. Such information will be useful, in particular when designing other related studies.

3.3 Research Protocol Development

As is typical of a systematic literature review, the research process should be defined and documented. When conducting a systematic literature review, research protocol development is an essential step during documentation of research design. In the context of literature reviews, review protocol is by definition a predetermined plan that outlines the methods used in conducting the review (Xiao & Watson, 2019). In addition to detailing the procedures involved in the review and serving as a recording of activities, defined protocol plays a role in ensuring the replicability of the review (Carrera-Rivera et al., 2022).

Research process of this study is based on the systematic literature review process presented originally by Xiao & Watson (2019) as it provides clear basis and template for setting up the research process. Research begins with planning phase, where the research questions are formulated and precisely defined. Research question formulation of this study is presented in the introduction chapter. Detailed explanation of research protocol development outcome is presented in sub-chapters of the current main chapter (3. Research Methodology).

Research continues with conducting phase, which involves searching, delimiting and analyzing the literature under review. This study focuses on searching for traditional research literature (peer-reviewed articles, journals etc.).

Research literature will be searched from popular databases that offer scientific publications.

Whole systematic literature review research process is presented on FIGURE 5. Interaction between the above two phases is indicated by a dotted line between planning and conducting phases. During the research phase, there may be a need to modify either the research problem or research protocol. Provision for this is also considered in the research process and its graph.

Lastly, the findings are reported during reporting phase. The written content has been incorporated in the results chapter (4. Results). In addition to the literature review, the analyzed results will be used for practical recommendation concerning network segmentation design and initial application in an organization. The related output will be presented in a separate chapter (5. Implementation Guidelines).

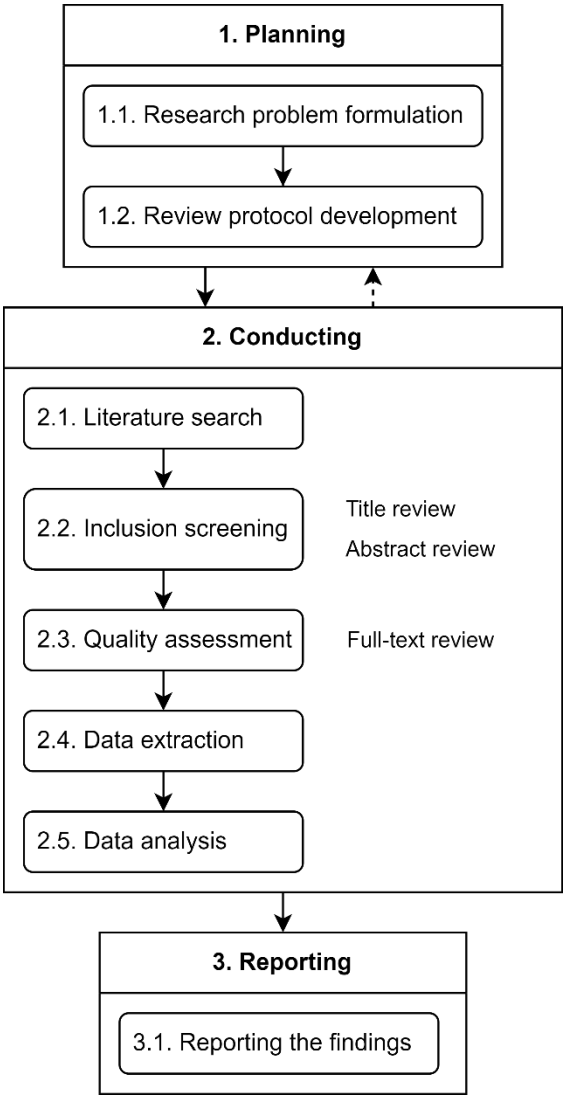

FIGURE 5 Systematic literature review research process

3.3.1 Search Strategy

When searching for the research literature, multiple popular databases will be utilized to collect literature material from a wide range of sources. Both discipline-specific (computer science and engineering) and interdisciplinary databases are included to ensure that results are diverse. The selected databases are listed in the TABLE 1. Inclusion and exclusion criteria will be partially applied in the search phase by filtering out the search results using time range filter that corresponds the publication year limit presented later in the inclusion and exclusion criteria.

Database	URL	Disciplines
ACM Digital Library	https://dl.acm.org/	Computer science
IEEE Xplore Digital Library	https://ieeexplore.ieee.org/	Computer science, electrical engineering and electronics
Scopus (Elsevier)	https://www.scopus.com/	Interdisciplinary
Web of Science	https://webofscience.com/	Interdisciplinary

TABLE 1 List of selected digital libraries

Test searches were conducted prior to the official literature review search. A need for alternative terms was identified to expand and specify the search results. For instance, modern network security includes micro-segmentation which covers the same concept as traditional network segmentation, but at a more detailed level as a part of ZTA. Thus, it was decided to include micro-segmentation explicitly in the keywords linked to the original network segmentation concept to obtain results on the same topic.

Final search terms were formulated using Boolean operators. Concepts and their alternative terms including whole initial formulation of search statements are presented in TABLE 2. The use of quotation marks ensures that sub-strings are managed correctly.

Concept	Alternative terms
Segmentation	(“*network segmentation*” OR “*network partitioning*” OR “*network compartmentalization*” OR “*micro-segmentation*”) AND
Security	((“*network*” OR “*cyber*” OR “*information*” OR “*computer*”) AND “*security*”) AND
Strategy	(“*strateg**” OR “*approach**” OR “*technolog**” OR “*best practice**“ OR “*guideline**”)

TABLE 2 Formulation of search statements

Formulation above (TABLE 2) serves as the basis for actual search string. The final search string used in each database search was:

> (("network segmentation" OR "network partitioning" OR "network compartmentalization" OR "micro-segmentation") AND (("network" OR "cyber" OR "information" OR "computer") AND "security") AND ("strateg*" OR "approach*" OR "technolog*" OR "best practice*" OR "guideline*"))

3.3.2 Inclusion and Exclusion Criteria

After the results are obtained from the executed search, results are evaluated for relevance using defined inclusion and exclusion criteria. Per following **inclusion criteria**, found publications are included for further inspection if they meet the following requirements:

- Published after 2013
- Written in English language
- Publication addresses network segmentation as more than a single mention in broader context
- Peer-reviewed journals, conference proceedings, or other scientific materials that are considered as higher priority

Justification for the 10-year time range limit (at the time of writing) is, in its simplicity, the rapid evolution of technology and related threats. To ensure that the information is up-to-date, material must also meet today's technical requirements. Excluding the time range limitation above, the inclusion criteria were chosen to be kept broad in order to get a better understanding of the current state-of-the-art instead of limiting the results unnecessarily.

Resulting publications that do not meet certain conditions are excluded from further processing of the results. These **exclusion criteria** are:

- Published before 2013
- Written in language other than English
- Publications that are not related to network segmentation, which for the purposes of this study, is defined as
- Publications that do not give enough information to address the defined research questions
- Publications that are duplicate and already included in the results

3.3.3 Study Selection

Database searches were executed on 6th September 2023. 10-year-time-range filter was applied in the searches to ease study selection process. In all, searches from all databases produced 465 publications in total. All search results were extracted into a single spreadsheet document in which duplicates and incomplete entries

(missing title or author information) were removed. After initial removal, there were 358 papers left for further processing.

Result qualification was organized in three stages: title review, abstract review and full-text review. In each of these stages inclusion and exclusion criteria were adhered. During full-text review extensive quality assessment was performed after inclusion screening.

Quality assessment utilized defined quality assessment form containing questions of four different quality aspects and a scoring measurement system (APPENDIX 1). These four quality aspect categories (reporting, rigor, credibility and relevance) are based on four main aspects presented originally by Zhou et al. (2015) in the domain of software engineering. As mentioned by Carrera-Rivera et al. (2022), numerical scale with a checklist containing multiple factors to evaluate can be used to quantify the quality assessment phase of systematic literature review process. Quality assessment is focused on general-level research aspects since relevancy in relation to network segmentation was considered in the inclusion and exclusion criteria. Score of 19 points was used as a threshold score value in qualification. Each publication had to score equal or more than 19 points in order to be included in the results.

After title review 139 papers remained for abstract review. 69 papers ended up in full-text review stage. In the end, 29 publications qualified for the study after quality assessment stage. In summary, the whole study selection process is presented in FIGURE 6.

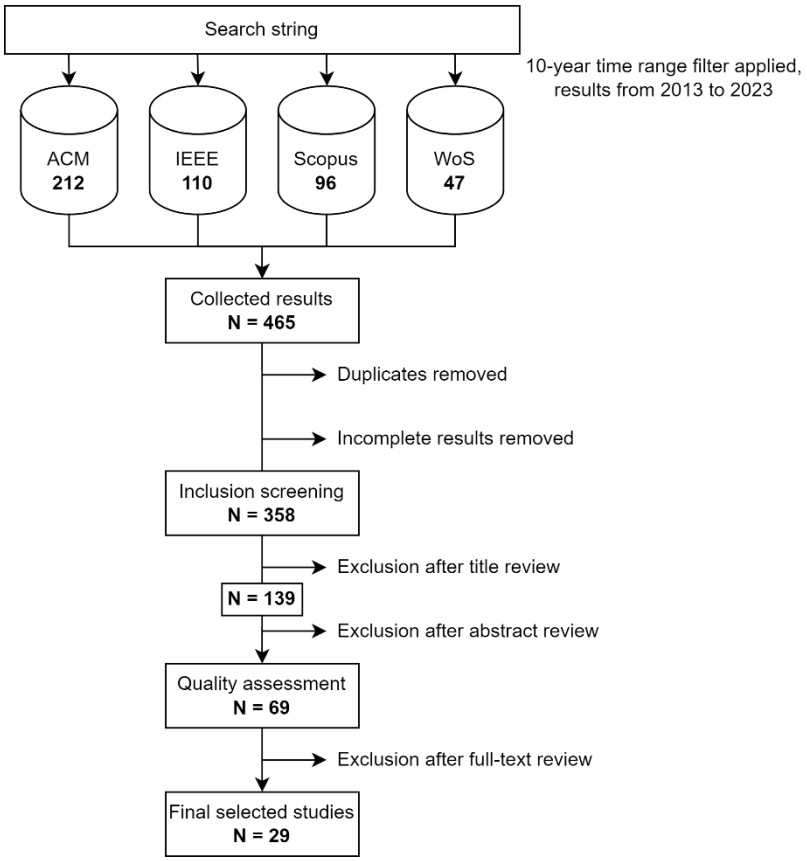

FIGURE 6 Study selection process

3.3.4 Data Extraction and Analysis

In the data extraction phase information is systemically taken from each validated paper before synthesizing the information (Okoli, 2015). For systematic literature review research documentation purposes, also key information of selected primary studies will be collected, such as paper title, name of the author(s) and publication year. Considering the research questions of this study, the data extraction should be based on these questions in order to produce corresponding data.

On the whole, all extracted fields are shown in TABLE 3. Title, author(s) and publication year are treated as metadata used for identifying papers and therefore they are not exclusively linked to any particular research question. Any references to information security guidelines and standards are collected in the extraction phase. References are reviewed for relevance to find out general guidelines for implementing network segmentation in practice. Also type of findings, identified research gaps and challenges are included to support forming the overall picture of network segmentation research. Rest of the extracted fields are formed based on themes extracted from research questions.

Field	Description	Related research question(s)
Title	Paper title	-
Author(s)	Name of the author(s)	-
Year	Publication year	-
Findings	General summary of findings, such as framework, methodology or development approach	-
Gaps and challenges	Identified research gaps and challenges in network segmentation and its research domain	-
Referenced guidelines	References to general information security guidelines and standards that provide information on network segmentation	RQ1, RQ2, RQ3
Strategies	All strategies and techniques mentioned for implementing network segmentation including technologies	RQ1, RQ2, RQ3
Organization attributes	Attributes of an organization and its network that are relevant for network segmentation	RQ1
Effects	Effects of network segmentation on organizational security posture and on the network to be segmented	RQ2, RQ3

TABLE 3 Data extraction form for research literature

Information according to data extraction form was collected into a spreadsheet document in which each column represents a single field of data extraction form. The matrix table itself allowed the compilation of quantitative data related to characteristics of target literature, such as publication year distribution and top-level categories of the publications.

After the data was filled into the table, thematic analysis method was applied as follows: each column was gone through row by row, coded and finally reviewed for identified themes and trends. For the coding, "structural coding", as mentioned by Belotto (2018, p. 2624), was used. In structural coding sections were labeled with terms related to the research questions. Based on the terms, themes and trends were identified and used as a basis for structuring and presenting the results in the reporting phase.

Furthermore, SWOT (strengths, weaknesses, opportunities and threats) analysis was conducted in order to perceive the themes and trends in a contextualized overview regarding mostly benefits and drawbacks related to organization-centered network segmentation (RQ1 and RQ3). The SWOT analysis method can be used, for example, to analyze the competitiveness and opportunistic goods of an organization at large, and as a fourfold method it is used for assessment, identification of learning, and development for business strategies (Pöyhönen & Lehto, 2017). In this context the "opportunities" are seen as possibilities that network segmentation could offer, whereas "threats" are seen as long-term risks that may arise from the implementation.

4 RESULTS

In this chapter, the results of the study are presented starting from a general level moving towards research question-specific analysis.

4.1 Overview

29 publications from four popular databases were included in the review. The resulting publications contained a wide variety of areas around network architecture and defence, some specialized in particular domain where in network architectural application is related to.

Distribution by publication year is shown in FIGURE 7. Having a 10-year time range filter between 2013 and 2023, annually most of the publications are published in 2021. The fewest annual releases are at beginning (around 2016) and the end (in 2023) of applied time range.

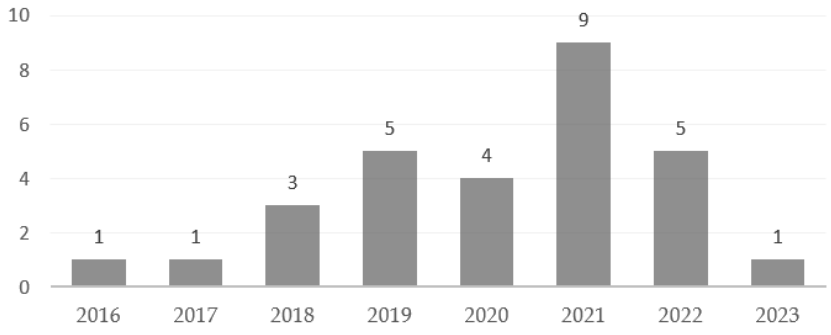

FIGURE 7 Publications per year

All resulting publications with references and short summarized descriptions are listed in TABLE 4. Recurring research areas include SDN, micro-segmentation as a part of ZTA and industry-specific implementation containing, for example, different models, architectures and cybersecurity automation through

algorithms and other additional supporting solutions. Most active researchers within the results are William Simpson by having two publications and Neal Wagner by having three publications in the results.

Authors	Summarized description of the study
Alabbad & Khédri (2021)	Authors assess three different SDN architectures for network segmentation that utilized RSN algorithm in order to generate network topology and segments based on policy specification.
Álvarez et al. (2023)	Authors conducted performance analysis of software-defined networks to mitigate attacks targeted at PVLAN technology.
Arief et al. (2020)	Authors develop a risk-based decision-making methodology based on Bayesian network and graph theory to investigate and evaluate the robustness of network segmentation alternatives.
Basta et al. (2022)	Authors develop an analytical framework to characterize and quantify the efficiency of micro-segmentation on enhancing security of networks.
Bondareva & Shilov (2021)	Authors develop appropriate methods for grouping users and services when performing network segmentation according to information security requirements.
da Rocha et al. (2021)	Authors present a security model based on zero trust model for preventing APT attacks that can exploit vulnerabilities of IoT devices connected in LAN network.
DeCusatis et al. (2017)	Authors develop an approach to implement authentication with packet-level granularity compatible with networks based on zero trust architecture.
Haar & Buchmann (2019)	Authors present a firewall appliance concept for smart home installation.
Hemberg et al., (2018)	Authors identify the most effective defender parameters against serial propagating malware attacks.
Johansson et al. (2020)	Authors investigate personnel's perception in relation to segmentation of medical devices and IT infrastructure in the healthcare sector.
Johnson et al. (2020)	Authors analyzed three additional network defense techniques while producing power system performance and cybersecurity metrics to advise the power system industry.
Katsis et al. (2021)	Authors introduce graph-based policy specification framework to capture communication requirements of networks.
Kurniawan & Yazid (2020)	Authors conduct a systemic literature review of SDN regarding research trends, threats, attacks, detection, mitigation and countermeasures.

Mhaskar et al. (2021)	Authors formally define network segmentation and demonstrated two algorithms that turn a set of requirements into a robust network topology and the policies of its firewalls.
Paillisse et al. (2020)	Authors present implementation, evaluation, experience and rationale matured in deploying software-defined access.
Paul & Rao (2022)	Authors examine zero trust approach and document its principles, architecture and implementation procedure.
Sheikh et al. (2021)	Authors present novel network security architecture that supports zero trust approach.
Simpson (2022)	Authors move toward a generic metric of trust in the context of zero trust model.
Simpson & Foltz (2021)	Authors review concepts of network segmentation and zero trust model and illustrate their combination.
Smeriga & Jirsik (2019)	Authors explore the possibilities of using behavior-aware network segmentation that utilizes IP flows and machine learning techniques.
Syed et al. (2022)	Authors conduct a state-of-the-art review of ZTA for effective implementation in context of critical infrastructure.
Tselios et al. (2022)	Authors provide overview on common network-related cybersecurity attacks and guidelines for mitigating these kinds of attacks.
Tsuchiya et al. (2018)	Authors present manufacturing system network architecture based on SDN firewalls with temporal filtering.
Venugopal et al. (2019)	Authors evaluate the use of SDN switches to implement least privilege networking.
Wagner et al. (2019)	Authors propose an automated method for generating network segmentation architectures that are optimized for security, cost and mission performance.
Wagner et al. (2016)	Authors present a novel method for supporting network segmentation that utilize an approach based on heuristic search and agent-based simulation.
Wüsteney et al. (2021)	Authors analyze the problems that arise when time-sensitive networks are segmented using modern firewalls and packet filters.
Xie et al. (2021)	Authors present a protection scheme based on zero trust architecture.
Zvabva et al. (2018)	Authors evaluate network packet latency, jitters and packet loss caused by open-source Linux firewalls in Modbus TCP/IP industrial networks following IEC 62443 standard.

TABLE 4 List of all included studies in the literature review

High-level categorization of the results is presented in FIGURE 8. Publications under each category are listed in TABLE 5. Top-three popular thematic

areas are zero trust architecture (ZTA), industry-specific implementations and software-defined networking (SDN). The categorization may not be trivial as they are not necessarily mutually exclusive. In any case, it is indicative, and some trends emerge from it, such as SDN and ZTA.

Although most of the papers are technology-centric, exceptionally distinct perspective is presented by Johansson et al. (2020). In the study authors explored perceptions of personnel regarding network segmentation in an IT environment of a medical organization. The study was conducted with qualitative approach in a form of focus group study that is related to human awareness, which is presented under category "Awareness and Training" in the FIGURE 8.

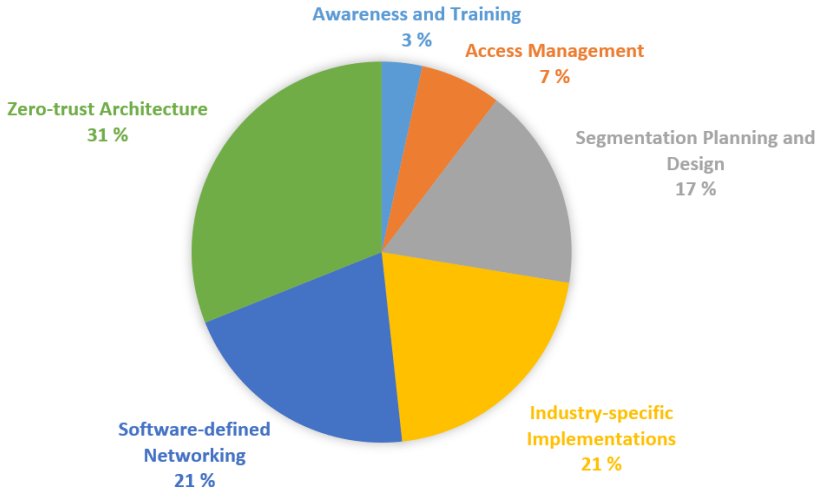

FIGURE 8 High-level categorized concepts extracted from the results

Theme	Related papers
Zero-trust architecture	(Basta et al., 2022), (da Rocha et al., 2021), (DeCusatis et al., 2017), (Paul & Rao, 2022), (Sheikh et al., 2021), (Simpson, 2022), (Simpson & Foltz, 2021), (Syed et al., 2022), (Xie et al., 2021)
Industry-specific implementation	(Arief et al., 2020), (Haar & Buchmann, 2019), (Johnson et al., 2020), (Tselios et al., 2022), (Wüsteney et al., 2021), (Zvabva et al., 2018)
Software-defined networking	(Alabbad & Khédri, 2021), (Álvarez et al., 2023), (Kurniawan & Yazid, 2020), (Paillisse et al., 2020), (Tsuchiya et al., 2018), (Venugopal et al., 2019)
Segmentation planning and design	(Bondareva & Shilov, 2021), (Hemberg et al., 2018), (Mhaskar et al., 2021), (Wagner et al., 2016) , (Wagner et al., 2019)
Access management	(Katsis et al., 2021), (Smeriga & Jirsik, 2019)
Awareness and training	(Johansson et al., 2020)

TABLE 5 Categorized publications

4.2 Strategies and Technologies

Descriptive objective of network segmentation is clear: break down the network into smaller segments and ensure that each segment is secured well. However, this leaves a few questions unanswered:

- How the resources should be grouped in network segmentation? In other words, what resources should be placed within same segment?
- What techniques or technologies should be used to secure and manage the segments?
- How the arrangements should be altered in the event that the network's size varies?

Answers to these questions is sought through RQ2 considering the strategies and technologies used for network segmentation. The concept of "strategy" in this context includes both segmented network formation and its maintenance as presented in the conceptual model (FIGURE 4). As commonly used tools and techniques are identified, scope for their comprehensive application (considered in RQ1) is to some extent clearer.

Following subchapters are divided based on the definition presented in the theoretical background: how segmented network topology can be designed, what techniques are used when the design is put into practice and lastly, what are the options for access control implementation. As a common objective is to outline available methods used for network segmentation.

4.2.1 Network Topology Design Phase

To begin with segment grouping question, the definition between macro-segmentation and micro-segmentation provides subtle guidelines concerning size of the segments. Macro-segmentation could in its ultimate form contain the whole enterprise network within a single segment while on the other hand micro-segmentation could extract each individual resource into its own separate segment (Simpson & Foltz, 2021).

In micro-segmentation the division is done by dividing the various segments of each workload level logically (Xie et al., 2021). Workload level typically contains a single workload to which restrictions policies are applied. Commonly identified three tiers of workloads are both web and application servers, and databases (Basta et al., 2022).

Since in micro-segmentation a single segment includes a small number of protectable resources, the choice for resources to be placed within segments is to some extent easier compared to macro-segmentation. Therefore number of options for grouping in macro-segmentation is much broader. In order to format the macro-segment groups, multiple approaches can be used. Segment groups can be, for example, created based on:

- Requirements, such as
  - "similar security requirements" (Alabbad & Khédri, 2021)
  - "requirements for information security" (Bondareva & Shilov, 2021)
  - "requirements for functions and risks to attendee security" (Hemberg et al., 2018)
  - "requirements for special protection based on standards, policies or other rules" (Kurniawan & Yazid, 2020)
- Resource-specific attributes, such as
  - "resource's various levels of sensitivity such as degree of vulnerability and confidentiality" (Kurniawan & Yazid, 2020)
  - "group of policies that concern each resource within a single segment" (Mhaskar et al., 2021)
  - "common risk profiles" (Smeriga & Jirsik, 2019)
  - "logically isolated parts, each accessible by specific individuals and key personnel only" (Tselios et al., 2022)

Instead of mere grouping, the "depth" of the segments has also been addressed in the research literature. This refers to how far away certain segment is located from the entry point (from demilitarized zone (DMZ), for example), dependent on the need for protection (Alabbad & Khédri, 2021; Mhaskar et al., 2021). Regarding the optimal number of segments, optimal depth for resource could be concluded by a certain measure, such as similarity or above-mentioned distance (Smeriga & Jirsik, 2019).

Irrespective of which of the above grouping principles is chosen, prior security analysis work must be conducted before completing decision as mentioned by Kurniawan & Yazid (2020). Regarding the rigor of the above criteria, ambiguity of grouping criterion has been raised in the research literature, as Mhaskar et al. (2021) assessed as obscure the definition of "different sensitivity levels (i.e., different risk tolerance values and threat susceptibility)" claimed by Stawowski (2007).

In order to facilitate and clarify network topology design work, machine-assisted solution have been developed. Bondareva & Shilov (2021) presented an application of machine learning techniques which are utilized in the topology design phase. Authors collected features of protectable resources (both subjects and objects), turned them into groups by cluster formation and suggested that output could be utilized as a basis for network segment division. Another proven example of using machine learning to cluster segments is demonstrated by Smeriga & Jirsik (2019). In the work, IP flows were utilized alongside machine learning in order to formulate either behavior-consistent or administrative-based segments.

In addition to machine learning, solutions based on algorithmic definitions in parallel with SDN implementation exist in the research literature. Authors refer to RNS which stands for *robust network and segmentation* algorithm. RNS is defined as a PFA-based (product family algebra) algorithm that uses

segmentation and layered defence strategies to systematically divide resources for the creation of secure networks (Alabbad & Khédri, 2021). First presentation of the RNS algorithm was done by Mhaskar et al. (2021) in addition to formally defining network segmentation. Authors initially discussed its usage in SDN environment. As a follow-up, Alabbad & Khédri (2021) defined an additional plane to SDN for configuring and governing purposes, but also for executing RNS in SDN environments which implements automated network segmentation in practice.

The above methods partly overlap with the next phase (network topology realization). Wagner et al. (2019) proposed a novel cyber decision support based on heuristic search and agent-based simulation. In the implementation, automatic cyber decision support is used for generating network architecture suggestions. Per authors, the actual execution would require manual actions since the generated components are not fully integrated. The method is therefore appropriate for exclusive use in the topology design phase.

Either only at the topology design phase or in several network segmentation phases, automated implementations based on machine learning and formal algorithms appear as a kind of emerging trend. In addition to the topology design phase, the network topology realization phase itself can already be partially implemented using SDN environments. However, for manual segmented topology design there appears to be lack of rigorous guidelines that have been validated and proven to work. In contrast, superficial recommendations based on various requirements and resource-specific attributes give some indication, but not complete support for a full end-to-end manual network topology design.

4.2.2 Network Topology Realization Phase

Concerning general components of network segmentation, Wagner et al. (2019) list following components related to network segmentation architecture: collection of network segments as well as software services for allowing communications between segments and between Internet. In addition, authors mention two more components that are in particular related to their own research: software service patching rate and segment cleansing rate.

Related to associated technologies in practical implementation of network segmentation, VLANs or PVLANs are mentioned as common technologies (Álvarez et al., 2023; Paillisse et al., 2020; Simpson & Foltz, 2021; Wüsteney et al., 2021). The segmentation is usually implemented in the second layer in which the above two technologies are utilized (Álvarez et al., 2023). However, also VRF (virtual routing and forwarding) could be utilized in enterprise network environments with combination of associated technologies (Paillisse et al., 2020).

Another of the much discussed and also previously mentioned technology is SDN. Network segmentation and segregation guidance that advises using technologies at more than just the network layer, includes SDN switch as a crucial component (Venugopal et al., 2019). Based on data gathered from sources other than the network itself (i.e. honey pots, security analytical engines, and other sources), programmable SDN controllers can implement dynamic network

segmentation (DeCusatis et al., 2017). Especially when talking about IoT networks, SDN in addition to network function virtualization (NFV), and software-defined perimeter (SDP) can be used for micro-segmentation (Syed et al., 2022). In summary, SDN appears as a flexible tool for network segmentation for versatile use. Furthermore, SDN has the potential to be used at combining network topology design and realization phases.

Support and guidance for micro-segmentation is to some extent more readily available compared to macro-segmentation. Speaking of available guidance, the references are usually based on the general guidelines, such as NIST SP 800-207 and other similar (discussed later in a separate chapter below). ZTA recognizes some common main components in the implementation. For instance, gateways, routers, switches and firewalls could act out as PEPs in micro-segmentation arrangement (da Rocha et al., 2021; Katsis et al., 2021). Syed et al. (2022) presented a comprehensive survey on ZTA in which several micro-segmentation approaches are highlighted. These deployment models include, according to Syed et al., (2022):

- Native micro-segmentation
    - Using "natively" hypervisor or operating system for deploying the application servers
- Third-party model
    - Using third-party firewall vendors' firewalls in deploying
- Overlay model
    - Using central controller or orchestration, and agent software to
        - gain visibility into workflow communications
        - enforce dynamic access policies
- Hybrid model
    - Using a combination of above-mentioned models in deployment

These deployment models are primarily to effectively protect "a single resource (or logical group of them)" (Syed et al., 2022). Consequently, these deployment models are more ore less linked to the access control phase, as it is quite clear that in micro-segmentation each segment typically contains only one or few resources to be protected.

References to concrete commercial products were found from one publication in the results. Sheikh et al. (2021) mentioned *Illumio* as a micro-segmentation tool and Microsoft's *Azure* cloud environment as a platform that offers a diverse range of tools for micro-segmentation. Isolated network environment could be based on three common segmentation patterns: single virtual network, multiple virtual networks with peering or multiple virtual networks in a hub-and-spoke-model (Sheikh et al., 2021). However, there was no comprehensive demonstration or analysis of these patterns.

In conclusion, as identified trends in network segmentation technologies, VLAN and SDN have been well covered in the research literature. Some

additional technologies, such as cloud-integrated tools, have also been identified, to some extent as an aside without going into further details. In addition, the availability of guidance also varies between macro-segmentation and micro-segmentation. This is reflected in how well the components of different models are defined, and how many and what kind of solutions have been created for these components. For example, macro-segmentation has vaguely identifiable components recognized while on the other hand guidance concerning micro-segmentation specifies commonly used ZTA components, such as PEP and PDP.

4.2.3 Access Restriction Phase

In general, access control plays a relevant role in network segmentation. Segmentation is usually implemented by the use of access control mechanisms, such as firewalls, application-level filters, and physical hardware infrastructure (Wagner et al., 2019). Although there are several methods for network traffic control, usage of firewalls stood out the most in the resulting literature. Firewalls, which manage network traffic in and out of every segment, are the primary security system suggested by all standards for implementing the segmentation security strategy (Tsuchiya et al., 2018).

Network segmentation aims to extend the rule of least privilege by decently implementing security zones that include all network infrastructure and interconnected hosts (Tselios et al., 2022). As a part of the segmentation implementation, firewall and routing rules are used for dividing network into segments (Smeriga & Jirsik, 2019). In the way they limit connectivity, firewalls also improve cyber resilience of network topologies by applying strict firewall rules (Johnson et al., 2020). In relation to essential guidelines of network segmentation, Tselios et al. (2022) collected considerations that all firewalls and gateways must support in implementation of network segmentation:

- Authentication and proxy of client connections
    - to prevent malicious requests and malformed packets in a physical or logical subnetwork known as the demilitarized zone (DMZ) that contains and exposes organization's external-facing services
- Optimization, multiplexing and rate limiting of connections to backend servers
    - to protect resources located there
- A software-defined architecture
    - that makes use of virtualization to securely partition the hardware platform into distinct instances with separate SLAs, SSL, CPU, assigned memory, and virtual NICs that can be shared or dedicated

On a larger scale, firewall-based access control is not just about creating and updating firewall rules, but rather a process consisting of various stages and factors, which as whole requires an active contribution from the implementer. This

is strongly linked to the workload that the maintenance phase in the conceptual model of network segmentation (FIGURE 4) requires. Haar & Buchmann (2019) addressed access control powered by firewalls in a context of smart home installation and network segmentation. Authors also mentioned how firewall fits for the IT-Security process (FIGURE 9) presented originally by Lodin & Schuba (1998). In the figure solid arrowed lines indicate direction of control and dashed arrowed lines indicate direction of information flow.

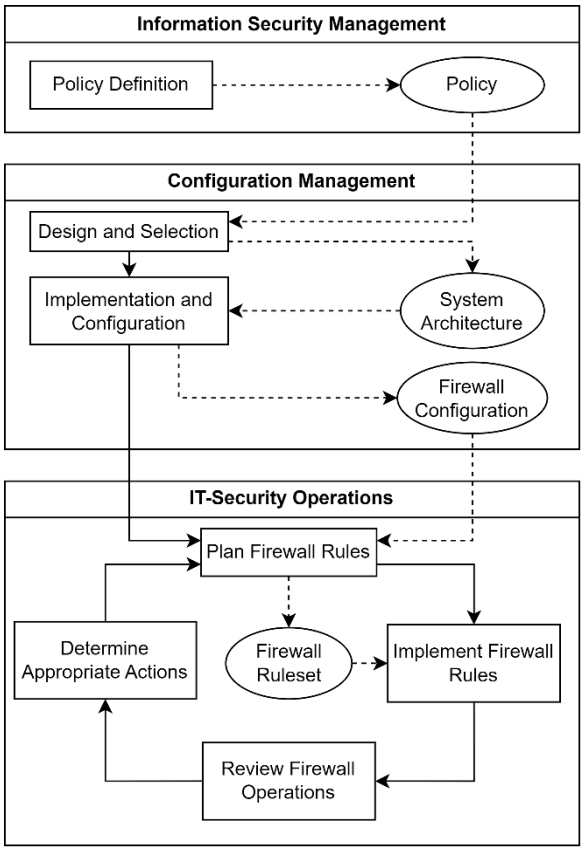

FIGURE 9 Firewall management process (Haar & Buchmann, 2019)

In the context of micro-segmentation, some specified mechanisms related to access restriction are also presented. These are based on the perspective from which access control is approached. The concept of a single protectable resource to some extent simplifies and guides thinking.

In a *network-dependent approach*, using the network identities of the applications requiring access, the identified network flows associated with a particular workflow must be converted into network-based access rules. Conversely, in a *network-independent approach*, fine-grained policies are created by using workload identities. (Syed et al., 2022)

Concerning the latter opinion, Syed et al. (2022) have summarized four modern access management approaches for network-independent approach. These approaches are presented in TABLE 6.

Access control technique	Description
Transport-level	After confirming the identity using packet authentication in TCP/IP communication, the TCP handshake procedure continues only if the access is granted for the requesting identity.
Label-based	Grouping and applying access policies based on labels that are assigned to various workflows.
DPI-based	Packet contents are examined at various levels using deep pack inspection (DPI) engines in order to either allow or reject connections.
API-aware	Workflow is divided into smaller container-based services that use application programming interfaces (APIs) to communicate with one another (such as Docker and Kubernetes).

TABLE 6 Network-independent access control (Syed et al., 2022)

In addition to traditional firewalls, also advanced access control mechanisms are mentioned in the context of network segmentation access control. Multilayered deep inspection firewalls could be placed in order to enforce zone-boundary security (Zvabva et al., 2018). In the implementation, in addition to smart switches or routers, next-generation firewalls (NGFWs) could be utilized as well (da Rocha et al., 2021).

4.2.4 Summary

On the conventional distinction between distinct types of network segmentation, scattered and shallow references to these can be found in the literature. For example, Arief et al. (2020) mentioned physical segmentation, logical segmentation and network traffic filtering. Nevertheless, detailed comparisons of these segmentation implementation types and contexts in which these approaches are best suited were not found from the results.

When talking about segmentation techniques, two kinds of segmentation techniques (considering all three stages of network segmentation) were identified from the analyzed results: automatic and manual. Manual network segmentation is the most traditional approach to which a larger part of the results can be assimilated, although automated network segmentation solutions seem to have gained a foothold in the research literature.

Crux of the issue in network segmentation process automation is that how requirements are turned into network topology specification and security policies: by a human or by machine-assisted solutions. Brief comparison between these two recognized techniques and associated technologies are presented in TABLE 7.

	Fully automated	Fully manual
Segment partition	Using automation to find out the most optimized network topology that is segmented.	Manually grouping protectable resources into segments per desired specification or requirements.
Communication restriction	Using automation for generating and/or deploying access control lists (firewall rules) that restrict communication between segments.	Manually configuring firewalls and other associated security controls that restrict the network traffic.
Characteristic techniques	SDN, NFV, NGFW, DPI and utilization of machine learning algorithms	NFV, VLAN, VRF, PVLAN, iptables and manually configurable firewalls

TABLE 7 Comparison between automated and manual segmentation

In response to the question about segmentation rearrangements when the network structure changes, usually repeating the segmentation process produces an updated network structure depending on the chosen segmentation method. This was discussed when dynamic network governance was addressed in the literature. For instance, Mhaskar et al. (2021) considered runtime of RNS algorithm and proposed as a potential solution an optimization-oriented execution in which the algorithm is run and targeted at only the part of the network in which the structure is being changed.

However, the analyzed results revealed the extent of the firewall-based access management, and the fact how it ties into maintenance work as a part of firewall management process. Together, these are worth considering when planning the segmentation arrangements before the actual implementation as they are strongly linked to the costs and requirements of the network segmentation.

4.3 Implementation Benefits and Drawbacks

At a general level, the results revealed observations related both to general segmentation practices and to particular technologies in more detail. In order to structure the discussion, the results are first reviewed at a higher level, moving down to a lower level of details. Extracts from SWOT analyses have also been included to summarize the outcomes in a broader picture of organizational context.

Starting with general benefits and drawbacks associated with network segmentation, a few key elements can be identified on both sides. Network segmentation brings an advantage by preventing unauthorized access to protected resources (da Rocha et al., 2021; Mhaskar et al., 2021; Smeriga & Jirsik, 2019; Tsuchiya et al., 2018; Wagner et al., 2016; Zvabva et al., 2018). Furthermore, network segmentation helps to minimize the chances of an attacker's lateral

movement (Bondareva & Shilov, 2021; Simpson, 2022; Syed et al., 2022; Tselios et al., 2022; Wagner et al., 2019; Zvabva et al., 2018). Other additional benefits are related to better control of the network (Basta et al., 2022; Johansson et al., 2020).

When talking about general disadvantages associated with the network segmentation, implementation can lead to complexity, which is reflected both in access management and in the overall network design (da Rocha et al., 2021; Johansson et al., 2020; Paul & Rao, 2022; Simpson & Foltz, 2021; Zvabva et al., 2018). A network architecture shaped by segmentation can also introduce performance issues though increased intersegment latency (Hemberg et al., 2018; Johnson et al., 2020; Paul & Rao, 2022). Another downside from an organizational point of view is the costs of implementation (Álvarez et al., 2023; Paul & Rao, 2022; Wagner et al., 2016).

Concerning the high-level implementation, dichotomies between automated and manual network segmentation as well as micro-segmentation and macro-segmentation approaches will also be used in later discussion of the results concerning implementation benefits and drawbacks. This will help later to identify the contexts in which each approach will be most beneficial.

4.3.1 Micro-segmentation vs. Macro-segmentation

Size of the segments is the differentiating factor between macro-segmentation and micro-segmentation. A group within a macro-segment also constitutes a group with similar access requirements. The requirement that segment policies are based on the common access policies for the resources within the segment is one issue with segment access controls (Simpson & Foltz, 2021). It can be also though that segment containing multiple resources corresponds a single sign-on service. (Simpson, 2022). In other words, this means that the link between instances within same segments is interpreted as reliable by default.

If reliability is to be increased, this means more fine-grained access control, which is typical of micro-segmentation. In turn, this may lead to more complex access management arrangements. Micro-segmentation potentially necessitates little automation and significant operational complexity (da Rocha et al., 2021). In addition, thorough understanding of the traffic that should be permitted in each micro-segment is necessary to create well-tailored policies for the network (Katsis et al., 2021).

Comparing micro-segmentation and macro-segmentation together, the different types of benefits offered by each approaches have been identified. Simpson & Foltz (2021) raise a point about security and overall benefits: where ZTA implementation through micro-segmentation provides network security, macro-segmentation promotes other benefits, such as performance improvements and cost savings. A more segmented network offers less mission efficiency due to increased overhead in intersegment communication, which is a trade-off in network segmentation design (Hemberg et al., 2018).

Segmented objects can be used to find resources that can benefit from the same set of protection measures (Bondareva & Shilov, 2021). In macro-segmentation, this means common access policies. Shared policies may contribute to

reducing the number of access restriction rules that may be duplicated in micro-segmentation setting. SWOT analysis on moving towards granular micro-segmentation from macro-segments is presented in TABLE 8. The strengths and weaknesses highlight the opposing both benefits and drawbacks when macro-segmentation is contrasted against micro-segmentation.

Strengths	**Weaknesses**
• Achieving fine-grained protection, which supports the ZTA as well as solid access control. • Segment's internal access is usually limited to one or few resources.	• Granular access policy management may increase the number of access policies, some of which may be very similar to each other. • More access restriction and security measures may indicate more costs.
Opportunities	**Threats**
• As the network grows, granular control is better maintained. • Popularity and evolution of ZTA in the long term support the implementation.	• Increased number of security policies enhance maintenance burden and risk of misconfiguration. • Implementation is difficult to maintain if there is lack of understanding of the network requirements.

TABLE 8 SWOT analysis on moving towards granular segmentation

4.3.2 Automated vs. Manual Approaches

Automated approaches can be used in each of the three defined segmentation phases (topology design, topology realization and access restriction). Example for topology design phase is presented by Bondareva & Shilov (2021). For topology realization and access restriction, example works are presented by Mhaskar et al. (2021) and Alabbad & Khédri (2021). In the latter two examples, automatic decision-making is used in deciding on the placement of switches and their access policies as a part of access restriction phase. In the first phase (topology design), the ambiguity of the grouping logic can cause complications. In general, it is challenging to format networking requirements from business needs (Sheikh et al., 2021).

In both topology realization and access restriction phases, configuration is needed. SDN enables algorithm-driven and dynamic segmentation in addition to configuring access policies, as presented by Alabbad & Khédri (2021). In general, when it comes to the manual configuration, publications of the results argued in favor of a risk that manual misconfiguration may introduce. For instance, complicated segmentation architecture necessitates careful configuration and furthermore, a new vulnerability is created by any configuration error (Simpson & Foltz, 2021). As another example in industry-specific context, DER (distributed energy resources) devices could be controlled in the study due to system configuration and networking implementation flaws (Johnson et al., 2020).

In summary, three main themes related to automatic and manual approaches were identified from the results: greater efficiency as a result of less ambiguity, costs of implementation and guaranteeing error-free configuration. The ambiguity relates to the freedom of implementation and how to choose optimal solution for the organization that uses it. Costs include both the time and other additional resources required for the implementation. Error-free in this context of network security means configuration of network devices and services which, when in use, does not constitute a particular security threat.

Strengths	**Weaknesses**
• Well-performing algorithm manages to find the most optimal segmented network topology. • Automation reduces human error that most often occur during manual configuration.	• Automated setup requires additional expertise on its integration and troubleshooting. • Automation leaves less room for autonomy in deciding on structure of the network.
Opportunities	**Threats**
• Automation contributes to scalability of the target network. • Automation streamlines segmentation of complex and large networks, even with frequent structural changes.	• Automation may result in cost issues if required capacity is used in excess of the budgeted amount. • Potential failure in an automated process could lead to further failures.

TABLE 9 SWOT analysis on moving towards automated segmentation

4.3.3 Technical Solutions

When it comes to technologies, issues in particular of VLAN have been raised in the research literature. Firstly, workflows lack of granular security when using conventional network segmentation methods like VLANs, routers and firewalls (Syed et al., 2022). Secondly, due to complicated network address design of VLAN and the potential presence of VLAN-related protocols that are vulnerable (such as DTP, VTP, GVRP), VLAN has some disadvantages (Álvarez et al., 2023). Thirdly, despite simplicity of VLANs and VRFs, VLANs do not scale well because their scope must be kept small to avoid broadcast traffic flooding or L2 forwarding loops (Paillisse et al., 2020). However, strong isolation at macro-level is offered by virtual networks (Paillisse et al., 2020).

Another key technology, SDN, was also highlighted in the results. Although SDN switch adds more complexity, it also adds more control (Venugopal et al., 2019). Related to complexity in general, SDNs may aid in lowering the management complexity of defence-in-depth in sizable corporate networks (Álvarez et al., 2023). Network configuration rules must be flexibly defined in order to achieve secured vertical integration, where SDN is likely a crucial technology when minimizing security threats (Tsuchiya et al., 2018).

In summary, SDN can be seen as a trend that seeks to address some of the problems related to general attributes, such as manageability and scalability. In conclusion, the optimal choice of used technology depends on the application and its needs. For instance, the needs could include continuous adaptation, which is reflected in dynamism in the target network. On the contrary, small and stable networks do not require constant changes, but can equally well be adapted to other technologies that support the original protection objectives.

4.4 Relevant Attributes in Network Segmentation

In order to take account of organizational differences in the implementation of network segmentation, it is first necessary to identify the attributes that are relevant to the network segmentation. The analysis of the results led to identifying relevant attributes by their interdependencies. Attribute identification started with network-related attributes and ended with recognition of organizational attributes that are derived from groups of network-related attributes.

Identified network-related attributes were size, granularity, visibility, dynamism, manageability, costs, protectability, resiliency, functionality and performance. Identified organizational attributes were control, protection and operationality. As a summary, all of the identified attributes are described in TABLE 10. The descriptions do not necessarily accurately describe the metrics in a quantitative manner but seek to outline explanations in broad terms.

First of the organizational attributes is *control*. The network-related attributes are linked by the fact that they are related to the network governance. One of the most determining network-related attributes that also has an impact on other attributes is the *size* of the network. *Granularity* specifies what are the sizes of the segments in the segmented network. *Dynamism* refers to density, according to which the architectural structure of the network changes. The capability for monitoring is treated as *visibility*. Networks need maintenance, so *manageability* refers to the amount of action that is required from the organization managing the target network. *Costs* include all direct and indirect costs incurred as a result of the maintenance that the target network requires.

Second identified organizational attribute is *protection* which covers both the need for the protection (*protectability*) and the effect of protection (*resiliency*). As mentioned earlier in the context of segment grouping, system resources of different sensitivity levels must be stored in multiple network segments and protected by various measures (Kurniawan & Yazid, 2020). Therefore, the need for protection may vary between the protectable resources. In addition, it is worth considering resiliency as the impact of applied security controls, which are realized when the attack against the target network occurs.

Lastly, *operationality* was identified as an organizational attribute that is related to the functionality and performance of the managed network. Since protection measures and other arrangements are applied, it may have an effect on the network and its functionality as well. For instance, performance issues could

be caused by ACLs that are placed in a non-optimal manner when the network is in oversubscribed state (Álvarez et al., 2023).

Organizational attribute	Network-related attribute	Description
Control	Size	How large and complex the network is in general
	Granularity	How large are the segments in the segmented network
	Dynamism	How frequently the network structure is expected to change
	Visibility	How well the network could be monitored
	Manageability	How much action the network requires from the organization
	Costs	How much it costs to run and maintain the network
Protection	Protectability	How much protection is needed for the resources inside the network
	Resiliency	How well the network resists the attack
Operationality	Functionality	Are the resources within the network performing as expected in general
	Performance	How well the network is capable of carrying a normal load within a reasonable time

TABLE 10 Identified organizational network attributes

One of the most determining network-related attributes that also has an impact on other attributes is the *size* of the network. The general conclusion is that the larger the network, the more it increases the complexity especially if security measures are implemented on the network. Network segmentation increases the complexity of the network and requires careful configuration in order to avoid breaches caused by misconfigurations (Simpson & Foltz, 2021).

As a follow-up, micro-segmentation encourages the adoption of fine-grained access control, which is considered here as *granularity*. Granularity at the packet-level promotes visibility, scalability, portability of applications, and use of vendor-independent architectures (DeCusatis et al., 2017). In micro-segmentation, enforcing strict security policies requires granular security controls (Syed et al., 2022). On the contrary, fine-grained segmentation may increase costs and risk of errors (Wagner et al., 2016). In addition, more granular segmentation can be read as part of the defence-in-depth strategy. Thus, as an example from industrial automation and control systems, implementing these defence-in-depth strategies may be associated with packet delays and loss as well as jitters (Zvabva et al.,

2018). Hence a certain link between performance challenges and granularity can be observed.

Network environment where growing technologies are deployed, embodies *dynamism* (Alabbad & Khédri, 2021). Network segmentation suffers a lack of visibility into processes in dynamic, complex, and multilayered networks, which leads to looser network security and less precise segment definition (Smeriga & Jirsik, 2019). Every change in the network environment has an effect on the efficiency of the network (Katsis et al., 2021). Thus, visibility into the network, its performance and protectability could vary according to the dynamic nature. It is nearly impossible to manually establish rules for network segmentation due to the complexity of network environments, the number of connected hosts and the network dynamics such as automated instance deployment (Smeriga & Jirsik, 2019). In general, automated solutions are therefore designed with dynamic networks in mind, requiring dense segmentation and organizing of access policies. Automation or maintenance in general is not free but may require costs for the organization. All but the most resource-rich organizations may not be able to afford the cost of immediately establishing, monitoring, maintaining and supporting such an infrastructure (Wagner et al., 2016).

Regarding *protectability*, *resiliency* was appointed by a few authors in the results. For instance, in order to reduce the risk of cyberattack-related domino effects in ICS networks in chemical and process plants, network segmentation can be applied (Arief et al., 2020). This is considered as resilience since network segmentation as a security mechanism prevents from further damage after attack. As an example in the zero trust concept, it offers the highest level of security, but it also has some drawbacks, such as complexity, increased labor requirements, slower application performance, higher costs, and reduced productivity (Paul & Rao, 2022).

In conclusion, dependencies between attributes were found as a result of the analysis. Majority of these dependencies are justified by the theoretical basis of the research literature and few are derived around the theoretical knowledge. The list may not necessarily include all theoretically possible dependencies but it provides an overview of the resulting analysis. In the big picture, these can be described in dependency graph (FIGURE 10). In addition to the graph, the dependencies of network-related attributes are explained explicitly for clarity in TABLE 11.

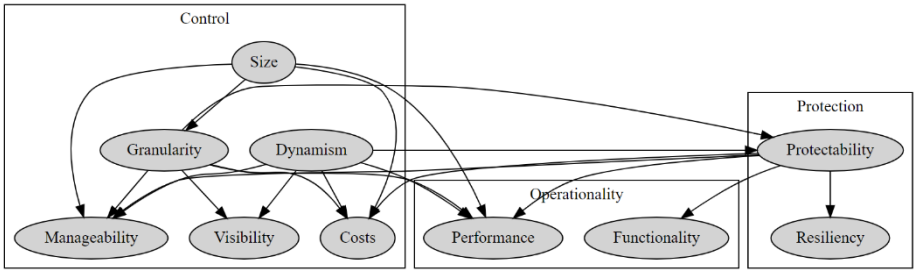

FIGURE 10 Dependency graph for identified attributes

Effective attribute	Target attribute	Explanation of the effect
Size	Manageability	Larger network contains more resources that need to be managed
	Costs	Larger network increases costs due to increased total traffic and maintenance
	Performance	Increased network traffic due to large network may affect overall performance
	Granularity	Larger network affects the options on how granularity could be implemented
Granularity	Visibility	Smaller segments allow for more detailed network traffic monitoring
	Protectability	Smaller segments allow for detailed access policies for each protectable resource
	Performance	Segments that share common access policies reduce total number of them
	Manageability	Increased number of segments may require more maintenance
	Costs	Increased number of segments implies more costs related to access control
Dynamism	Manageability	The more dynamic network, the more it needs monitoring and maintenance
	Costs	The more dynamic network, the more it creates costs related to network changes
	Performance	The more dynamic network, the more it requires changes that may affect to network performance
	Protectability	The more dynamic network, the more it makes its protection challenging
	Visibility	The more dynamic network, the more it is challenging to monitor it
Protectability	Resiliency	Increased protection is assumed to create network that is more resistant to attack
	Performance	Increased protection mechanisms can cause performance delays in the network
	Functionality	Increased access restriction may in some cases cause prevention of essential use
	Costs	Increased protection mechanisms may increase costs
	Manageability	Increased number of security policies require more maintenance work

TABLE 11 Network-related attribute dependency mapping

To some extent, it can be though that the above dependencies repeat themselves through different attributes. For instance, size and granularity both have an effect on the manageability. However, granularity can be often implemented in several ways even if the size of the network remains constant, since only the size of the segments matter in the case above. As another example, all four impacting attributes affect the costs. Therefore an explicit definition is necessary, as dependencies are thought to be linked: protectability adds protection costs, granularity add total costs of granular-specific maintenance, size includes costs as a result of all collective traffic generated by the network, and dynamism relates to the costs arising from the ongoing regeneration of segments or related manual work.

Overall, the dependency mapping helps to identify among all the available attributes that should be given higher priority when designing the network segmentation. Looking at the arrows in the dependency graph, several lead to the following attributes: *costs*, *performance*, and *manageability*. Secondly, looking at the network-related attribute mapping, attributes that most influence others are *protectability*, *granularity*, *size* and *dynamism*. The result of this analysis will help in the implementation of the network segmentation design, allowing conclusion to be drawn when presenting practical recommendations later.

4.5 Network Segmentation in Information Security Guidelines

At the data extraction phase, references to general information security guidelines including information security managements standards were collected. Due to the scope of the study, detailed analysis of each of these references will not be conducted. There were individual references to other external guidelines as well, but only those referred more than once and by more than one author were included in the list.

In total six publications had referenced guidelines from NIST. These reference are by da Rocha et al. (2021), Simpson (2022), Simpson & Foltz (2021), Syed et al. (2022), Tsuchiya et al. (2018) and Venugopal et al. (2019). IEC 62443 series of standard was referred three times in total by Tsuchiya et al. (2018), Wüsteney et al. (2021) and Zvabva et al. (2018). NSA Technical Report Top 10 Information Assurance Mitigation Strategies was referred two times by Hemberg et al. (2018) and Wagner et al. (2016). Google's Approach to IT security was referred two times by Alabbad & Khédri (2021) and Mhaskar et al. (2021). In conclusion, a list of most referenced guidelines is presented in TABLE 12.

Half of the references are to information security guidelines provided by NIST (National Institute of Standards and Technology). To begin with the most reference guideline, NIST SP 800-207, in addition to providing general deployment models and use cases, the document provides an abstract definition of ZTA, which has the potential to enhance an organization's overall information technology security posture (Rose et al., 2020).

Guideline or standard	Description	Reference frequency
NIST SP 800-207	Describes how zero trust architecture could be applied using micro-segmentation	4
IEC 62443	Cybersecurity standard for OT, of which parts contain requirements for network segmentation	3
NIST SP 800-82	Focused on network segmentation in OT context	2
NSA: Technical Report. Top 10 Information Assurance Mitigation Strategies	States network segmentation and application-aware network defence as an eighth mitigation strategy.	2
Google's Approach to IT Security	States enforcement of network segregation using industry standard firewalls and ACL technologies.	2

TABLE 12 Referenced guidelines and standards per authors

Another guideline from NIST is NIST SP 800-82 that offers instructions on how to secure operational technology (OT) in order to meet operational technology's particular performance, reliability, and requirements related to safety (Stouffer, 2023).

One standard that was pointed out in the results was related to OT as well. Electronically secure industrial automation and control systems (IACS) must be implemented and maintained in accordance with the ISA/IEC 64443 series of standards (International Society of Automation, n.d.). Standards also contains network segmentation instructions in addition to other security guidance in the context of OT environments.

NSA (National Security Agency) published technical report containing top 10 information assurance and mitigation strategies. Network segmentation is suggested in addition to application-aware defenses as required by law and policy to obstruct improperly formed traffic and limit content. Common protocols are used to conceal malicious data and remove data, necessitating the development of sophisticated and application-aware defensive mechanisms that are essential for contemporary network defense. (NSA, 2013)

Google's Approach to IT Security is a security strategy that also promotes network segmentation. Although it is a strategy, it is also intended here as a guidance. Google's network security strategy has multiple elements, one of which being control over the network perimeter's size and composition. In addition, network segregation is enforced using ACL technologies and industry-standard firewalls. (Google, 2012)

5 IMPLEMENTATION GUIDELINES

In this chapter, high-level implementation guidelines on how to approach network segmentation in organizational context is presented as a contribution of the thesis.

5.1 Key Steps for Implementing Network Segmentation

As a conclusion of the study, three main phases for network segmentation are presented: network topology design, network topology realization and access restriction. The phasing allows the choice of different approaches, so that the approach in question fits a particular phase.

As a whole, the network segmentation and its phases are presented in FIGURE 11. Different implementation options have been put together for each phase. These options include the choice between macro-segmentation and micro-segmentation in addition to level of automation and selection of technical solutions. In general, micro-segmentation advocates use of more manual approaches while automation increases the efficiency of macro-segmentation.

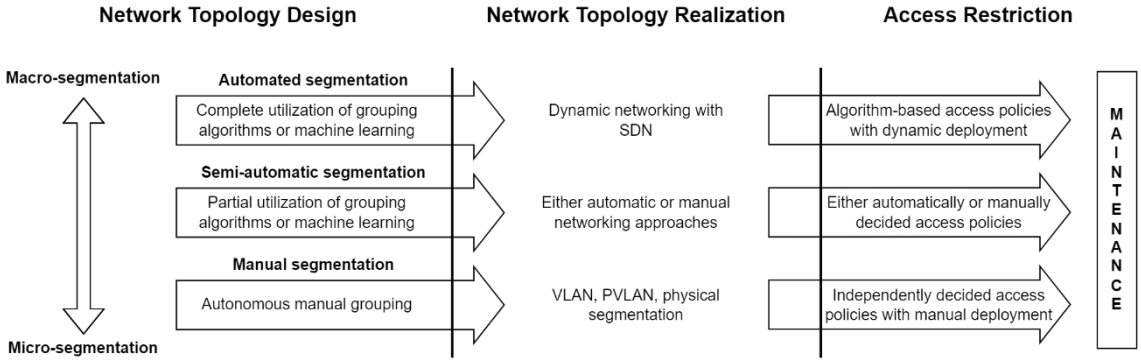

FIGURE 11 Key steps for implementing network segmentation

A phased transition from a budgeting perspective may be disadvantageous if additional costs are incurred as a result of realized implementation. Therefore at the beginning of the phases the organization should pay attention not only to the immediate costs but also to the costs that maintenance work may entail in the longer term. In the term of network segmentation phases, this also means that the transition does not need to be set in stone, but the guidelines present from a high level the essential steps to get from the initial network to the point where this network is segmented.

Detailed descriptions of each phase are divided into their own subchapters. Based on the result of the study, the options for implementation that are relevant for the organization are discussed. The appropriateness of the choices will be justified on the basis of the evidence based on the research literature. As a whole the subchapters aim to respond to the main research question (RQ1).

5.2 Network Topology Design

Network segmentation begins with a network topology design phase that will result in a plan for what kind of network topology will be implemented and what are the communication requirements between protectable resources. At the beginning of the design phase, the organization shall define estimated budget and identify existing requirements that are relevant to the whole segmentation implementation.

Requirements include, for example, security requirements for the network and communication requirements for the resources inside the target network. Once the requirements have been identified, the implementation must be related to them from the very beginning and in every phase, so that the resulting network arrangement complies the requirements. Estimated budget should be respected thorough the process in both design and implementation phases and evaluated at the end of the complete process.

To begin with the grouping question, it should be decided how granular segments will be formed. This means the choice between macro-segmentation and micro-segmentation. Macro-segmentation results in a traditional choice where segments share common access policies. Typical deployment environments include, for example, data centers, and stable enterprise networks created using physical devices. Reciprocally, micro-segmentation contributes to the adoption of broader security arrangements aligned with ZTA. In this case, suitable environments include modern cloud platforms and dynamic SDN networks, for example.

In network topology design phase another issue to be decided is the level of automation in segment grouping. Automation includes utilization of machine-learning or algorithm-based solutions in grouping of the segments. Automated topology arrangement is more typical for macro-segmentation since size of the segments are larger compared to micro-segmentation, which in itself to some extent creates a formally solvable optimization problem. Automation can be either

partially or fully benefited, meaning that the output of the algorithm can be used directly or just to support decision-making. Exploring the available automation solutions requires the organization initiative and ability to choose the most appropriate solution.

Considering the organization, attention should be paid on the target network. Firstly, size of the network affects a number of things. Larger network may introduce complexity, meaning that automation can save time resources. Secondly, dynamism of the network may indicate more intensive grouping in the case of macro-segmentation. Again, automation can save time and resources in continuous network structural management.

From an organizational perspective of view, automation may introduce additional costs, such as maintenance costs. In conclusion, benefits introduced by automated grouping must be considered and weighted on a case-by-case basis, knowing the total costs of each option. However, manual grouping may be the easiest option for small and stable networks since automation does not in itself give the full benefit in that case. In addition, manual grouping enables full autonomy to decide the network topology at cost that the manual work requires.

After the organization has decided the segmentation level (macro or micro) and level of automation, the network topology plan should be made. The topology plan should consider all previous decisions and must be feasible, before continuing to network topology realization phase.

5.3 Network Topology Realization

After the network topology design phase, the implementation itself is approachable, as the realistic objective exists in a form of network topology plan. The organization has a key role to play at this phase in the technical solution selection.

If a complex and dynamic network led to an automated grouping solution, its integration to network topology realization phase can be considered. This means that if it is chosen that network topology will be implemented using SDN solution, then it might be possible to integrate automated grouping into the topology realization phase as if by merging the first two phases. This supports the organizational objective, especially if a requirement for dynamism was identified at the network topology design phase.

However, if the organization requires more autonomy, network topology could be realized manually based on the grouping decision implemented either fully manually or semi-automatically. Here the options for technical solution can to some extent increase, as centralized network management is not prerequisite. Depending on the case, segmentation could be technically implemented using SDN, VLANs, PVLANs, cloud platform segmentation tools, or even physical segmentation approaches.

At the technological solution selection stage, attention must be paid to following aspects: manageability, protectability, performance, and costs. Manageability was dealt with in the topology design phase as the size of the network was

considered. Topology plan, however, inevitably also has an impact on the realization phase since different segmentation tools require different amounts of input for the topology realization.

In addition to manageability, rest of the considerable attributes (protectability, performance and costs) may vary from one to another. For example, VLANs are said to be weakly scalable and physical segmentation approaches may not even suitable for cloud platforms due to their intended use and the model of shared responsibility. In conclusion, network topology realization requires a kind of competitive tendering process for the organization, and discretion in general to achieve the most advantageous outcome, which appears as a relative whole between protectability, performance and overall costs.

At the end of the topology realization phase the network should be functional, albeit without full access control. Detailed topology formulation is left to the implementer since there is no one universal way to realize a network topology. Furthermore, technological solutions are evolving and so are the implementation options.

5.4 Access Restriction

As the formed segments exist, the traffic should be controlled to be ensured that network protection has been applied. Prerequisite for this phase are the communication requirements established in the first phase (network topology design). In its simplicity, this can be seen as a continuation for the topology realization phase since access controls are realized in this phase on top of the realized topology implementation.

The most common type of access control techniques is ACLs which may appear differently in various applications. Again, dependent on the choice of technological solution in the previous phase, the access control solution must be aligned with choices from network realization phase. For instance, firewalls in many different forms (traditional, NGFWs, switch-integrated etc.) may be the feasible solution for network environments that support firewalls. However, modern cloud platforms may require second type of access control solutions such as traffic filtering based on API-awareness or DPI engines. Sometimes advanced solutions can help to minimize the manual access restriction work in case centralized access policy management is possible.

Since access restriction is a critical securing part of network segmentation, the access policies need careful maintenance and consideration for extensive network protection. Here again, automated solutions can reduce the risk of misconfigurations, but integrating automated access policy formation into dynamic operations requires successful coordination of previously selected technologies. Not all technical solutions are compatible with each other, and therefore implementation requires overall consideration.

ACL in itself constitutes to some extent documentation of the communication requirements. However, it may not fundamentally background why certain

communication is established. Hence matching the external and supporting documentation behind the operational access control rules in practice is of paramount importance. This aims to avoid allowing unnecessary rules that could compromise network security. Network segmentation should be based on the principle of least privilege, and redundant access rights do not pursue this objective. When only necessary access rights exist, the attack surface is also smaller.

5.5 Use Case Demonstration

Practical application of network segmentation guidelines takes place in organizational context. Therefore for a better grasp of concrete, a couple of use case examples are presented. Two fictitious examples include both smaller and growing enterprise environments where guidelines are used to support planning and decision-making. The main objective is firstly to demonstrate from a high-level how network segmentation works in practice and secondly how the guidelines support the network segmentation implementation process.

5.5.1 Example Organization 1: Small-scale Micro-segmentation

First example organization is a small-sized company, which physical internal network consists of several departments, including users' devices, HR, finance, sales, and R&D (research and development). They have planned to adopt principles of the zero trust model, and as a part of it, micro-segmentation arrangements have been started. The organization uses the network only for internal purposes, thus neither organization hosts external services nor have a DMZ setup in their network.

Organization starts the process with a mapping to find out the original unsegmented network topology, its properties and all requirements that are crucial to the implementation. Budget limit was also set to the entire process including estimation of maintenance costs. Let us assume that there are no external regulatory requirements for the implementation but only the vital communication requirements between users and resources:

- R&D department has its one database administrator (user 1) which should have access to the database and another server administrator (user 2) that maintains two servers, and thus the administrator should access these servers. The server should be able to communicate with the database.
- Finance and sales services should be accessible by only two persons (user 3 and user 4), both should have access to all services in finance and sales departments.
- HR resources contain sensitive information, so only two persons (user 5 and user 6) should have access to the resources, each has exclusive

access to their "own" database and servers. HR remote controller computer should also have access to the virtual server.

The outcome of the network-nature evaluation concluded that the target network is small-scaled and fairly stable. Therefore organization decides to engage in manual work in both micro-segmentation process and its maintenance. In addition to the segmentation, organization could consider cloud migration alongside the network architectural changes enabling micro-segmentation with tools of cloud platform. However, due to the budget, expertise and other currently available resources, organization ended up using physical VLAN techniques (using VLAN-supported router-switch and switches, as well as firewall systems) for the micro-segmentation. The segmentation realization phase is depicted in FIGURE 12. (unsegmented network on the left and realized segmented in the rights, as an output).

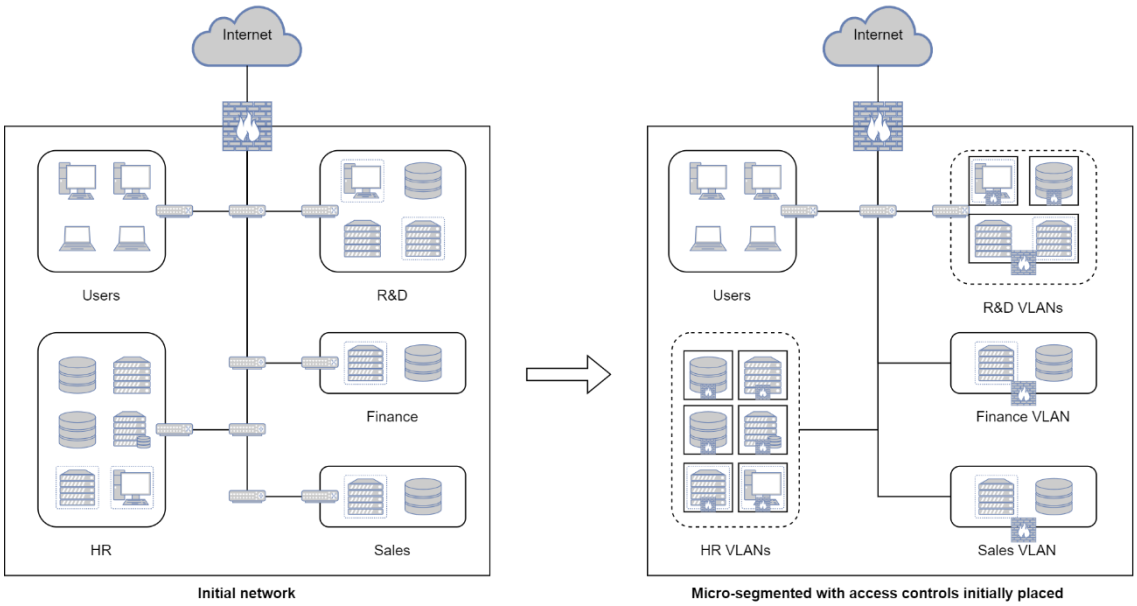

FIGURE 12 Example of network micro-segmentation

Access controls are based on firewalls. VLAN-supporting routers (one of which has also is a support for switch options) offer ACL-type of firewalls that can be used to configure permitted traffic to and from R&D, finance and sales VLANs. Every of HR resources has its own firewall of a third-party vendor. These access controls are configured per communication requirements in a way that only necessary traffic between segments is allowed. VLAN arrangements could be done by following

- R&D department: remote controller computer in VLAN 10, database in VLAN 20, and both servers in VLAN 30.
- Finance department: VLAN 40
- Sales department: VLAN 50

- HR department: database 1 in VLAN 60, database 2 in VLAN 70, server 1 in VLAN 80, server 2 in VLAN 90, virtual server in VLAN 100, and remote controller computer in VLAN 110.

Access control is based on the principle of extending the least privilege. Configuration of the network router and switches is required, and as a result, access controls between users and VLAN segments are managed as following:

- Permit traffic between
  - R&D department
    - user 1 and VLAN 20
    - user 2 and VLAN 30
    - VLAN 20 and VLAN 30
  - Finance and sales
    - user 3 and VLAN 40, VLAN 50
    - user 4 and VLAN 40, VLAN 50
  - HR
    - user 5 and VLAN 60, VLAN 80
    - user 6 and VLAN 70, VLAN 90
    - VLAN 100 and VLAN 110

When it comes to optimization on a long-term, organization plans to monitor traffic after the first pilot implementation and potentially improves the implementation iteratively after feedback considering and scrutinizing the costs of implementation in the light of the budget that was set in the beginning. Their segmentation strategy includes systematic management of access control policies since granular segments result in increased number of security perimeters and more requirements for access restriction is coming later.

It should be noted that ZTA strategy is only partly implemented since access controls are not yet centralized according to core logical ZTA components. As another long-term objective, organization aims to improve the implementation and its security through experience and development. This may appear in the adoption of new technical solutions in network security and improvement of previous foundations, including further utilization of ZTA principles.

5.5.2 Example Organization 2: Scalable Network Segmentation

Second example organization is growing company that hosts a data center. Therefore the target network, due to its need for scalability requires a flexible solution for network segmentation. In addition, company is subject to a number of external requirements concerning physical security, customer privacy, network security and personnel's cybersecurity awareness. The requirements necessary for the implementation of the network segmentation must consider physical aspects of the networking equipment where relevant but also network security requirements including usage of firewalls and capabilities of network traffic monitoring.

The initial network was implemented in a traditional three-layer tree-based data center architecture with a physical switches and routers. The most common three-tier data center architecture contains three layers: core, aggregation and access layers (Pries et al., 2012). However, network architectural changes encouraged the organization to consider change from management perspective by introducing reorganization of the architecture with SDN controller and switches, which also enables centralized management. Furthermore, SDN enables flexible network segmentation that reduces the manual work related to physical device configuration. In summary, this integration of network topology design and realization phases is depicted in FIGURE 13, where upper topology is the initial architecture. The lower topology represents the renewed architecture. The renewed SDN architectural solution is inspired by the data center SDN architecture presented by Montazerolghaem (2021).

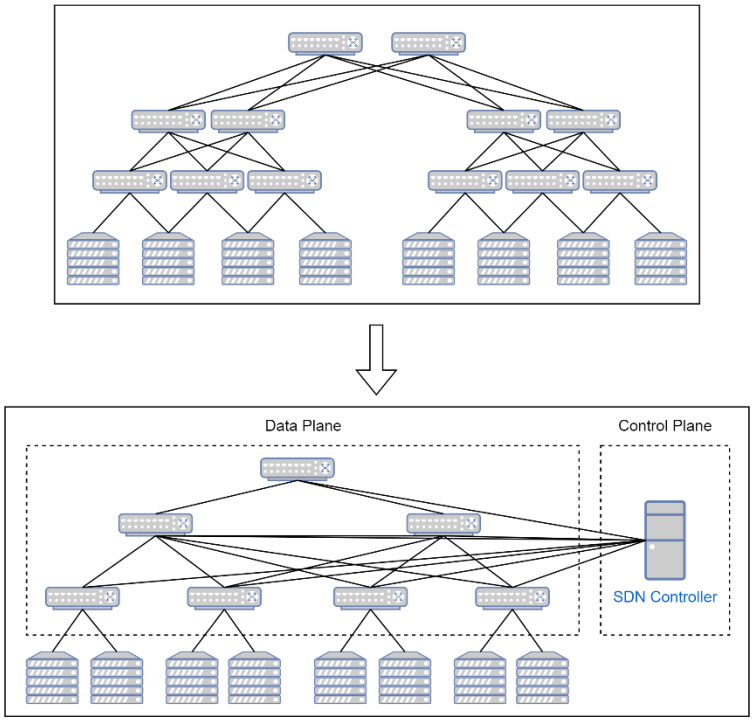

FIGURE 13 Example of data center SDN network architecture migration

To begin with the access restriction phase, SDN architecture allows multiple options for firewall setup. However, due to the high-level traffic and network stability, organization decided to use multiple distributed firewalls located in the switches at the data plane (see Alabbad & Khédri (2021) for similar implementation). Switch-integrated firewalls are applied in the edge switches in order to allow only necessary incoming and outcoming traffic to the isolated segment (FIGURE 14). These firewalls can thus be centrally controlled via the SDN controller, which promotes the flexibility.

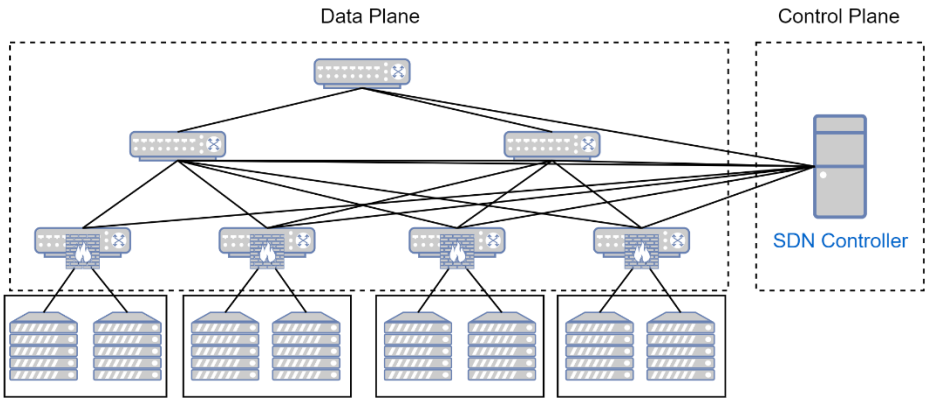

FIGURE 14 Example access restriction implementation in SDN architecture

Regarding requirement for monitoring, the SDN controller by its logging capabilities allows for runtime logging in order to obtain information on how both the software and hardware are acting (Siniarski et al., 2016). In this case, SDN controller also complies with the requirement for logging. Otherwise logging is an implementation of its own in terms of i.e. its management.

5.6 Conclusion

In the first use case, the small size of the organization and its target network allowed more granular segment management in terms of available resources and requirements. The organization started the implementation with a small milestone towards extensive utilization of ZTA. This allows for the iterative development of segmentation implementation. While on the other hand, in the second use case organization opted for a scalable solution, which led to more extensive network architectural changes. The migration made it easier to implement network segmentation in the present case due to centralized management offered by SDN architecture.

In the first example communication requirements between resources were showed in a simplified way. In reality, however, both communication and security requirements may be more extensive and in some cases more complex. For instance, one resource must be accessible to certain people, and in addition, other services must be able to communicate with it. In the longer term outlining and realized access control implementation requires diligence in accordance with a continuous model where access control requirements live on as the personnel and requirements change over time.

Neither of the examples utilized fully automated network segmentation due to the nature of the target networks: they required autonomy in terms of network management and maintenance. In the first use case, automation would not have been of much benefit to a stable and small network. In the second case, data center requires active maintenance done by administrators in any case, so

manual administration also regarding segmentation arrangements ensures prudent solutions.

Both examples of use cases were implementation models described at a very rough level, meaning that the technical details such as configuration, load balancing, traffic monitoring and continuous access control management on a long-term were ignored. In the end, the ultimate purpose was to demonstrate how these network segmentation phases of implementation guidelines can be achieved in practice and how the relevant attributes guide the choices when planning implementation of network segmentation.

6 DISCUSSION AND CONCLUSION

In this chapter, the results of the study are summarized, critical review is carried out, research limitations are identified and suggestions for future research directions are presented.

6.1 Summary of Findings

Primary objective of this study was to identify existing options for network segmentation and distinguish between available options from a high level according to what is the most appropriate in each organizational context. Instead of detailed analysis and given the scope of the study, the objectives can be met by identifying the most common trends around network segmentation, albeit not at the precise technical level. Based on current knowledge this was one of the firsts comprehensive systematic literature reviews on network segmentation and thereby an overview of how network segmentation has been addressed in the research literature.

Considering the whole network segmentation process, results indicate that the automated solutions could be one area for development in the context of network segmentation. Although the majority of the results are based on manual network segmentation, automation can improve efficiency and security. In particular, this applies for routine operations in a highly dynamic network environment where misconfigurations due to human error can compromise network security.

Furthermore, macro-segmentation and micro-segmentation were treated in parallel in this study. While micro-segmentation is an essential element to complement the principles of ZTA, granular segmentation as a sub-concept differs from macro-segmentation where segments typically consist of multiple protectable resources. The main differences between these two approaches are related to the level of protection and costs as a result of, for example, the burden of maintenance, which may increase due to higher number of access policies between multiple granular segments.

When approaching the network segmentation in an organization (RQ1), the essential attributes for the implementation are costs, performance and manageability, protectability, granularity, size and dynamism as the key attributes of segmentation implementation. The identified attributes help in the selection of the available technical solution options while forming an optimization problem in which the interdependencies of the attributes must be reconciled in an optimal way. When it comes to the most common available technical solutions for the implementations (RQ2), VLAN (as well as PVLAN) and SDN are the popular choices for network segmentation. The benefits and drawbacks of these solutions (RQ3) are related to the possibility of centralized network management, the capability to adapt to dynamic and frequent structural changes in the target network, and readiness for granular protection especially in the case of micro-segmentation.

On the basis of results, implementation guidelines were presented as a contribution of this study. According to the theoretical background, three-phased segmentation through-flow guides planning and decision-making but does not give direct advice on every detailed aspect in every organizational context. These are left deliberately to the organization to figure out, as solution options evolve rapidly and the number of viable options varies from organization to organization. In any case, the most efficient security arrangements require judgement close to the applicable context.

6.2 Critical Review

One of the common pitfalls in network security related studies could be inadequate reasoning and lack of solid evidence. On the contrary, formal definitions and quantitative research results speak for themselves. However, arguments from the general level often fall by the wayside. For instance, if it is argued that "network segmentation enhances organizational security posture", it leaves the rest up to interpretation. We can get closer to the concrete by supplementing the claim with additional statements, such as "network segmentation allows for better control and restriction of the traffic". Nevertheless, the ambiguity may not be completely resolved. What is the "better control" and how the traffic is "restricted" in a way that organizational security benefits from it? This requires exact definitions and defined metrics to achieve a more robust evidence base.

One of the emerging trends was network segmentation using automation. Automated solutions may to some extent reduce human error most commonly in the cases of routine activities. However, no case studies were found on the errors caused by algorithm-based segmentation setting. These could, for example, be certain borderline cases that have not been considered in the algorithmic design. While their exactness reduces routine manual configuration errors to some extent, they may not be necessarily completely bulletproof.

Additionally, one can easily think of the fact that automation solves the problem of segmenting a network. However, it makes more sense to see

automation as a tool that, if used correctly, streamlines work alongside other inputs and therefore creates value. Similarities can also be observed in the field of software test automation: although test automation reduces the testing effort, it is not considered as the panacea for all software testing activities (Jose, 2021, p. 5). If we do not want to leave all the decision-making in the hands of an automated solution, humans must be involved in the process of making decisions.

Where a reduced number of access controls in macro-segmentation saves costs, automated calculation based on dynamic classification can at least partially reverse them. Although optimal segmentation arrangement can save on other expenses, the process itself may require some costs related to execution of the algorithm, for example. In any case, even if the grouping is done manually, it still requires deliberation and at least time resources. This can commit the organization during the maintenance phase, even later on if the network structure has to be changed manually due to structural changes in the segmented network. Therefore, when considering the costs, all direct and indirect costs should be addressed in the full scope of the segmentation process.

6.3 Limitations

While the study seeks to respond to the defined research questions, it has some limitations. Firstly, between the research methodology (systematic literature review) and main research question (RQ1), certain challenges can be identified. The knowledge base has been established from a limited set of research publications meaning that practical recommendations had to be derived by synthesis from earlier studies. Although another research method would have been well suited to the main research question, one of the aims of this study was to systemically review the current state-of-the-art.

At a later stage of the systematic literature review process, quality assessment was based on a well-defined assessment form. However, the assessment and scoring were based on an interpretation of the author, which can be seen to some extent as a tendency to bias and selective ignoring. In any case, considering the whole systematic literature review process and its transparency, the objective is to minimize biases and to ensure greater transparency.

Secondly, computer networking and its security domain is an extremely broad research field, and a thorough description of it is incomplete in this study. This is reflected in the high-level proposals and in the aim to identify emerging trends around network segmentation. For instance, the technical aspect is only given a superficial glimpse in the review. On the other hand, as such, the study cannot be used to identify detailed segmentation options without precise definition of the applicable organization. Thus, the presented practical recommendations aim to encourage and support discussion and planning of network segmentation instead of creating strict models for segmentation action.

Thirdly, concerning practical recommendations, the applications developed in the research literature may not have fully matured into the commercial

products that are used by the majority of practitioners. For example, machine learning solutions may require customized solutions to put their main idea into practice. This study did not take a position on what solutions are available for practitioners. Instead, presented implementation guidelines is more about outlining and even thinking about developing own solutions tailored to specific needs than directly suggesting exclusively for available named product. This, in particular, leads to a certain gap between theory and practice.

Fourth, practical recommendations were derived loosely from the results, meaning a lack of rigorous research process and complete transparency in the development of implementation guidelines. This is justified by the delimited overall scope of the study and the fact that the main research method was based on systematic literature review. However, the recommendations were treated as kind of DSR artifact as per Peffers et al. (2007), which was demonstrated with fictious example use cases. On the whole, this to some extent brings the recommendations closer to practice and eventual evaluation.

Fifth, network segmentation is applicable to different type of networks, such as traditional enterprise networks consisting of office devices or cloud platform networking environments where logically separated software components are run. Due to the loose definition of the target network type, thematic-driven analysis was about examining the general attributes, trends and phases for network segmentation as an organizational action. More detailed segmentation requires expertise in the available technologies and their integration, and the will to maintain the whole network and its security in order to minimize risks.

6.4 Future Research Directions

The range of network segmentation options has increased significantly. Computer networks are no longer limited to physical network setups and on-premises environments. On a larger scale, this means diversity of computer networks, from traditional physical data centers to cloud platforms where the model of shared responsibility between organization and cloud-platform provider applies. In terms of network security research, future research could conduct even lower-level review of the suitability of the network segmentation options for the diverse kinds of networks, such as networks of online software providers, classic traditional intranet, and the network formed jointly by the operational departments of an organization (as seen in the first example case above).

Since the modern computing environments offers an even better potential for use of automation, automated network segmentation may receive more attention. Consequently, future research could focus on exploring especially how automated network segmentation works in real enterprise environments since earlier studies have focused on simulated environments. Future research could include examination of automated segmentation benefits in addition to case studies where automated solutions have led to an undesirable outcome, such as

failure in predefined automation tool implementation. Ultimately, this would help drive design and deployment in a more efficient and secure direction.

Another potential area for further research is the maintenance of segmented network. Network segmentation is easily seen as a one-way and one-off process that secures the network. However, considering access policy management and integration of added tools and technologies in any of the network segmentation phases presented in this study, maintenance work cannot necessarily be avoided. Future research could find out what kind of maintenance work certain network segmentation arrangements actually produce. This would better support decision-making when solutions are seen as far-reaching.

REFERENCES

Alabbad, M., & Khédri, R. (2021). Configuration and Governance of Dynamic Secure SDN. *Procedia Computer Science*, *184*, 131–139. https://doi.org/10.1016/j.procs.2021.03.024

Alenezi, M. N., Alabdulrazzaq, H., Alshaher, A. A., & Alkharang, M. M. (2020). Evolution of Malware Threats and Techniques: A Review. *International Journal of Communication Networks and Information Security*, *12*(3), 326–337.

Ali Abdullah, S. (2019). *Simulation of Virtual LANs (VLANs) Using OPNET*. https://doi.org/10.9790/2834-1106026780

Álvarez, D., Nuño, P., González, C. T., Bulnes, F. G., Granda, J. C., & García-Carrillo, D. (2023). Performance Analysis of Software-Defined Networks to Mitigate Private VLAN Attacks. *Sensors*, *23*(4). https://doi.org/10.3390/s23041747

Arief, R., Khakzad, N., & Pieters, W. (2020). Mitigating cyberattack related domino effects in process plants via ICS segmentation. *Journal of Information Security and Applications*, *51*, 102450. https://doi.org/10.1016/j.jisa.2020.102450

Arnaud, J., & Wright, J. W. (2016). Network segregation in the digital substation. *13th International Conference on Development in Power System Protection 2016 (DPSP)*, 1–4. https://doi.org/10.1049/cp.2016.0056

Barnes, S. J. (2005). Assessing the Value of IS Journals. *Commun. ACM*, *48*(1), 110–112. https://doi.org/10.1145/1039539.1039573

Basta, N., Ikram, M., Kaafar, D., & Walker, A. (2022). *Towards a Zero-Trust Micro-segmentation Network Security Strategy: An Evaluation Framework*. 1–7. https://doi.org/10.1109/NOMS54207.2022.9789888

Belotto, M. J. (2018). Data Analysis Methods for Qualitative Research: Managing the Challenges of Coding, Interrater Reliability, and Thematic Analysis. *The Qualitative Report*, *23*(11), 2622–2633. ProQuest Central; Publicly Available Content Database; Social Science Premium Collection.

Benzekki, K., El Fergougui, A., & Elbelrhiti Elalaoui, A. (2016). Software-defined networking (SDN): A survey. *Security and Communication Networks*, *9*(18), 5803–5833. https://doi.org/10.1002/sec.1737

Bondareva, A., & Shilov, I. (2021). Method of Grouping Subjects and Objects in Information Systems. *2021 30th Conference of Open Innovations Association FRUCT*, 10–15. https://doi.org/10.23919/FRUCT53335.2021.9599989

Bronk, J., & Watling, J. (2021). I. The Slow and Imprecise Art of Cyber Warfare. *Whitehall Papers*, *99*(1), 11–23. https://doi.org/10.1080/02681307.2021.2005891

Carrera-Rivera, A., Ochoa, W., Larrinaga, F., & Lasa, G. (2022). How-to conduct a systematic literature review: A quick guide for computer science research. *MethodsX*, *9*, 101895–101895. https://doi.org/10.1016/j.mex.2022.101895

Chate, A. B., & Chirchi, V. R. (2015). Access Control List Provides Security in Network. *International Journal of Computer Applications*, *121*(22), 14–16. https://doi.org/10.5120/21831-5090

Cisco. (n.d.). *What Is Network Segmentation?* What Is Network Segmentation? - Cisco. Retrieved January 11, 2024, from https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html

Cook, D. J., Greengold, N. L., Ellrodt, A. G., & Weingarten, S. R. (1997). The Relation between Systematic Reviews and Practice Guidelines. *Annals of Internal Medicine*, *127*(3), 210–216. https://doi.org/10.7326/0003-4819-127-3-199708010-00006

da Rocha, B. C., de Melo, L. P., & de Sousa, R. T. (2021). Preventing APT attacks on LAN networks with connected IoT devices using a zero trust based security model. *2021 Workshop on Communication Networks and Power Systems (WCNPS)*, 1–6. https://doi.org/10.1109/WCNPS53648.2021.9626270

Daly, J., Liu, A. X., & Torng, E. (2016). A Difference Resolution Approach to Compressing Access Control Lists. *IEEE/ACM Transactions on Networking*, *24*(1), 610–623. https://doi.org/10.1109/TNET.2015.2397393

DeCusatis, C., Liengtiraphan, P., & Sager, A. (2017). Zero Trust Cloud Networks using Transport Access Control and High Availability Optical Bypass Switching. *Advances in Science, Technology and Engineering Systems Journal*, *2*, 30–35. https://doi.org/10.25046/aj020305

Drutskoy, D., Keller, E., & Rexford, J. (2013). Scalable Network Virtualization in Software-Defined Networks. *IEEE Internet Computing*, *17*(2), 20–27. https://doi.org/10.1109/MIC.2012.144

Fujs, D., Mihelič, A., & Vrhovec, S. L. R. (2019). The Power of Interpretation: Qualitative Methods in Cybersecurity Research. *Proceedings of the 14th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3339252.3341479

Gatra, R., Akbar, R., Sugiantoro, B., & Asyhab, N. (2019). VLAN-based LAN Network Management Comparison using Cisco and Brocade. *IJID (International Journal on Informatics for Development) (Online)*, *7*(2), 45–49.

Google. (2012). *Google's Approach to IT Security* [Technical Report].

Goransson, P., & Black, C. (2014). *Software Defined Networks: A Comprehensive Approach*. https://doi.org/10.1016/C2013-0-00167-3

Grant, M. J., & Booth, A. (2009). A typology of reviews: An analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal*, *26*(2), 91–108. https://doi.org/10.1111/j.1471-1842.2009.00848.x

Haar, C., & Buchmann, E. (2019). FANE: A Firewall Appliance for the Smart Home. *2019 Federated Conference on Computer Science and Information Systems (FedCSIS)*, 449–458. https://doi.org/10.15439/2019F177

Hemberg, E., Zipkin, J. R., Skowyra, R. W., Wagner, N., & O'Reilly, U.-M. (2018). Adversarial Co-Evolution of Attack and Defense in a Segmented Computer Network Environment. *Proceedings of the Genetic and Evolutionary Computation Conference Companion*, 1648–1655. https://doi.org/10.1145/3205651.3208287

International Society of Automation. (n.d.). *The World's Only Consensus-Based Automation and Control Systems Cybersecurity Standards*. Retrieved November 12, 2023, from https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Johansson, Jönsson, Ivarsson, & Christiansson. (2020). Information Technology and Medical Technology Personnel's Perception Regarding Segmentation of Medical Devices: A Focus Group Study. *Healthcare*, *8*, 23. https://doi.org/10.3390/healthcare8010023

Johnson, J., Onunkwo, I., Cordeiro, P., Wright, B. J., Jacobs, N., & Lai, C. (2020). Assessing DER network cybersecurity defences in a power-communication co-simulation environment. *IET Cyber-Physical Systems: Theory & Applications*, *5*(3), 274–282. https://doi.org/10.1049/iet-cps.2019.0084

Jose, B. (2021). *Test Automation: A manager's guide*.

Katsis, C., Cicala, F., Thomsen, D., Ringo, N., & Bertino, E. (2021). Can I Reach You? Do I Need To? New Semantics in Security Policy Specification and Testing. *Proceedings of the 26th ACM Symposium on Access Control Models and Technologies*, 165–174. https://doi.org/10.1145/3450569.3463558

King, I. J., & Huang, H. H. (2023). Euler: Detecting Network Lateral Movement via Scalable Temporal Link Prediction. *ACM Transactions on Privacy and Security*, *26*(3), 1–36. https://doi.org/10.1145/3588771

Kurniawan, M. T., & Yazid, S. (2020). A Systematic Literature Review of Security Software Defined Network: Research Trends, Threat, Attack, Detect, Mitigate, and Countermeasure. *Proceedings of the 3rd International Conference on Telecommunications and Communication Engineering*, 39–45. https://doi.org/10.1145/3369555.3369567

Leo, P., Isik, Ö., & Muhly, F. (2022). The Ransomware Dilemma. *MIT Sloan Management Review*, *63*(4), 13–15.

Levy, Y., & Ellis, T. J. (2006). A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. *Informing Science*, *9*, 181–212.

Linnenluecke, M. K., Marrone, M., & Singh, A. K. (2020). Conducting systematic literature reviews and bibliometric analyses. *Australian Journal of Management*, *45*(2), 175–194. https://doi.org/10.1177/0312896219877678

Lodin, S. W., & Schuba, C. L. (1998). Firewalls fend off invasions from the Net. *IEEE Spectrum*, *35*(2), 26–34. https://doi.org/10.1109/6.648669

Makeri, Y. A., Cirella, G. T., Galas, F. J., Jadah, H. M., & Adeniran, A. O. (2021). Network Performance Through Virtual Local Area Network (VLAN) Implementation & Enforcement On Network Security For Enterprise. *International Journal of Advanced Networking and Applications*, *12*(6), 4750–4762. https://doi.org/10.35444/IJANA.2021.12604

Mescheryakov, S., Shchemelinin, D., Izrailov, K., & Pokussov, V. (2020). Digital Cloud Environment: Present Challenges and Future Forecast. *Future Internet*, *12*(5). https://doi.org/10.3390/fi12050082

Mhaskar, N., Alabbad, M., & Khédri, R. (2021). A Formal Approach to Network Segmentation. *Computers & Security*, *103*, 102162. https://doi.org/10.1016/j.cose.2020.102162

Michael, J. B., Dinolt, G. C., Cohen, F. B., Wijesekera, D., & Michael, J. B. (2022). Can You Trust Zero Trust? *Computer (Long Beach, Calif.)*, *55*(8), 103–105. https://doi.org/10.1109/MC.2022.3178813

Montazerolghaem, A. (2021). Software-defined load-balanced data center: Design, implementation and performance analysis. *Cluster Computing*, *24*. https://doi.org/10.1007/s10586-020-03134-x

NSA. (2013). *Top 10 Information Assurance Mitigation Strategies*. Information Assurance Directorate.

Okoli, C. (2015). A Guide to Conducting a Standalone Systematic Literature Review. *Communications of the Association for Information Systems*, *37*, 43. ProQuest Central; SciTech Premium Collection. https://doi.org/10.17705/1CAIS.03743

Paillisse, J., Portoles, M., Lopez, A., Rodriguez-Natal, A., Iacobacci, D., Leong, J., Moreno, V., Cabellos, A., Maino, F., & Hooda, S. (2020). SD-Access: Practical Experiences in Designing and Deploying Software Defined Enterprise Networks. *Proceedings of the 16th International Conference on Emerging Networking EXperiments and Technologies*, 496–508. https://doi.org/10.1145/3386367.3431288

Palugyai, S. (2005). Measurement and optimization of access control lists. *Acta Cybernetica (Szeged)*, *17*(2), 185.

Paré, G., & Kitsiou, S. (2017). *Methods for Literature Reviews*. https://www.ncbi.nlm.nih.gov/books/NBK481583/

Paul, B., & Rao, M. (2022). Zero-Trust Model for Smart Manufacturing Industry. *Applied Sciences*, *13*, 221. https://doi.org/10.3390/app13010221

Pechoucek, M. (2023, December 7). *Cybersecurity predictions for 2024*. https://www.nortonlifelock.com/blogs/blog-post/cybersecurity-predictions-2024

Peffers, K., Tuunanen, T., Rothenberger, M., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*, 45–77.

Pöyhönen, J., & Lehto, M. (2017, June). *Cyber security creation as part of the management of an energy company*.

Pries, R., Jarschel, M., Schlosser, D., Klopf, M., & Tran-Gia, P. (2012). *Power Consumption Analysis of Data Center Architectures*. *51*. https://doi.org/10.1007/978-3-642-33368-2_10

Qin, Z., Denker, G., Giannelli, C., Bellavista, P., & Venkatasubramanian, N. (2014). *A Software Defined Networking architecture for the Internet-of-Things*. https://doi.org/10.1109/NOMS.2014.6838365

Ramprasath, J., & Seethalakshmi, V. (2021). Secure access of resources in software-defined networks using dynamic access control list. *International Journal of Communication Systems*, *34*(1), n/a. https://doi.org/10.1002/dac.4607

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-207

Sheikh, N., Pawar, M., & Lawrence, V. (2021). Zero trust using Network Micro Segmentation. *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 1–6. https://doi.org/10.1109/INFOCOMWKSHPS51825.2021.9484645

Shu, Z., Wan, J., Li, D., Lin, J., Vasilakos, A. V., & Imran, M. (2016). Security in Software-Defined Networking: Threats and Countermeasures. *Mobile Networks and Applications*, *21*(5), 764–776. https://doi.org/10.1007/s11036-016-0676-x

Simpson, W. R. (2022). Toward a zero trust metric. *Procedia Computer Science*, *204*, 123–130. https://doi.org/10.1016/j.procs.2022.08.015

Simpson, W. R., & Foltz, K. E. (2021). Network Segmentation and Zero Trust Architectures. *Proceedings of the World Congress on Engineering 2021*.

Siniarski, B., Perry, P., Olariu, C., & Murphy, J. (2016, September). *Real-time monitoring of SDN networks using non-invasive cloud-based logging platforms*. https://doi.org/10.1109/PIMRC.2016.7794973

Smeriga, J., & Jirsik, T. (2019). Behavior-Aware Network Segmentation Using IP Flows. *Proceedings of the 14th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3339252.3339265

Stouffer, K. (2023). *Guide to Operational Technology (OT) Security*. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-82r3

Syed, N., Shah, S., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access*, *10*, 1–1. https://doi.org/10.1109/ACCESS.2022.3174679

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. *British Journal of Management*, *14*(3), 207–222. https://doi.org/10.1111/1467-8551.00375

Tselios, C., Politis, I., & Xenakis, C. (2022). Improving Network, Data and Application Security for SMEs. *Proceedings of the 17th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3538969.3544426

Tsuchiya, A., Fraile, F., Koshijima, I., Bas, A., & Poler, R. (2018). Software defined networking firewall for industry 4.0 manufacturing systems. *Journal of Industrial Engineering and Management*, *11*, 318. https://doi.org/10.3926/jiem.2534

Uçtu, G., Alkan, M., Doğru, İ. A., & Dörterler, M. (2021). A suggested testbed to evaluate multicast network and threat prevention performance of Next Generation Firewalls. *Future Generation Computer Systems*, *124*, 56–67. https://doi.org/10.1016/j.future.2021.05.013

Venugopal, V., Alves-Foss, J., & Ravindrababu, S. G. (2019). Use of an SDN Switch in Support of NIST ICS Security Recommendations and Least Privilege Networking. *Proceedings of the Fifth Annual Industrial Control System Security (ICSS) Workshop*, 11–20. https://doi.org/10.1145/3372318.3372321

Wagner, N., Sahin, C. S., Peña, J., & Streilein, W. (2019). *Automatic Generation of Cyber Architectures Optimized for Security, Cost, and Mission Performance: A Nature-Inspired Approach* (pp. 1–25). https://doi.org/10.1007/978-3-319-96451-5_1

Wagner, N., Şahin, C. Ş., Winterrose, M., Riordan, J., Pena, J., Hanson, D., & Streilein, W. W. (2016). Towards automated cyber decision support: A case study on network segmentation for security. *2016 IEEE Symposium Series on Computational Intelligence (SSCI)*, 1–10. https://doi.org/10.1109/SSCI.2016.7849908

Wüsteney, L., Menth, M., Hummen, R., & Heer, T. (2021). Impact of Packet Filtering on Time-Sensitive Networking Traffic. *2021 17th IEEE International Conference on Factory Communication Systems (WFCS)*, 59–66. https://doi.org/10.1109/WFCS46889.2021.9483611

Xiao, Y., & Watson, M. (2019). Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research*, *39*(1), 93–112. https://doi.org/10.1177/0739456X17723971

Xie, L., Hang, F., Guo, W., Lv, Y., & Chen, H. (2021). A Micro-Segmentation Protection Scheme Based on Zero Trust Architecture. *ISCTT 2021; 6th International Conference on Information Science, Computer Technology and Transportation*, 1–4.

Zahwa, W., Lahmadi, A., Rusinowitch, M., & Ayadi, M. (2023). *Automated Placement of In-Network ACL Rules*. https://doi.org/10.1109/NetSoft57336.2023.10175436

Zvabva, D., Zavarsky, P., Butakov, S., & Luswata, J. (2018). Evaluation of Industrial Firewall Performance Issues in Automation and Control Networks. *2018 29th Biennial Symposium on Communications (BSC)*, 1–5. https://doi.org/10.1109/BSC.2018.8494696

APPENDIX 1 QUALITY ASSESSMENT FORM

Quality aspect	Questions	Measure (score)
Reporting	1. Are the research objectives clearly stated? 2. Are the research methods clearly defined?	1 - Disagree 2 - Neither agree nor disagree 3 - Agree
Rigor	3. Were data collection and analysis procedures systematic? 4. Were potential sources of bias or other limitations discussed and addressed?	1 - No 2 - Partially yes 3 - Yes
Credibility	5. Are data analysis techniques appropriate and transparent? 6. Is the research conducted by reputable author?	1 - Low credibility 2 - Medium credibility 3 - High credibility
Relevance	7. Is the research aligned with current trends or technologies in the field? 8. Does the study provide practical insights or implications for real-word applications?	1 - Not relevant 2 - Moderately relevant 3 - Highly relevant

APPENDIX 2 ARTICLE QUALITY ASSESSMENT

Article	Assessment (score) **Q** = question number per quality assessment form (Appendix 1) **S** = score value (max. total score is 24)
Alabbad, M., & Khédri, R. (2021). Configuration and Governance of Dynamic Secure SDN. Procedia Computer Science, 184, 131-139.	**Q** 1. 2. 3. 4. 5. 6. 7. 8. = **S** 3 3 3 1 3 3 3 2 **21**
Álvarez, D., Nuño, P., González, C. T., Bulnes, F. G., Granda, J. C., & García-Carrillo, D. (2023). Performance Analysis of Software-Defined Networks to Mitigate Private VLAN Attacks. Sensors (Basel, Switzerland), 23(4), 1747	**Q** 1. 2. 3. 4. 5. 6. 7. 8. = **S** 3 3 3 3 3 3 3 2 **23**
Arief, R., Khakzad, N., & Pieters, W. (2020). Mitigating cyberattack related domino effects in process plants via ICS segmentation. Journal of information security and applications, 51, 102450.	**Q** 1. 2. 3. 4. 5. 6. 7. 8. = **S** 3 3 3 2 3 3 1 2 **20**
Basta, N., Ikram, M., Kaafar, D., & Walker, A. (2022). Towards a Zero-Trust Micro-segmentation Network Security Strategy: An Evaluation Framework. 1-7. 10.	**Q** 1. 2. 3. 4. 5. 6. 7. 8. = **S** 3 3 3 3 3 3 3 3 **24**
Bondareva, A., & Shilov, I. (2021). Method of Grouping Subjects and Objects in Information Systems. In 2021 30th Conference of Open Innovations Association FRUCT (pp. 10-15).	**Q** 1. 2. 3. 4. 5. 6. 7. 8. = **S** 3 3 2 3 2 3 2 2 **20**
da Rocha, B. C., de Melo, L. P., & de Sousa, R. T. (2021). Preventing APT attacks on LAN networks with connected IoT devices using a zero trust based security model.	**Q** 1. 2. 3. 4. 5. 6. 7. 8. = **S** 2 3 2 2 2 2 3 3 **19**
DeCusatis, C., Liengtiraphan, P., & Sager, A. (2017). Zero Trust Cloud Networks using Transport Access Control and High Availability Optical Bypass Switching. Advances in Science, Technology and Engineering Systems Journal, 2(3), 30-35.	**Q** 1. 2. 3. 4. 5. 6. 7. 8. = **S** 3 3 3 2 3 3 3 3 **23**

Haar, C., & Buchmann, E. (2019). FANE: A Firewall Appliance for the Smart Home.

Q	1.	2.	3.	4.	5.	6.	7.	8.	=
S	3	3	3	3	3	3	2	3	23

Hemberg, E., Zipkin, J., Skowyra, R., Wagner, N. & O'Reilly, U. (2018). Adversarial co-evolution of attack and defense in a segmented computer network environment. 1648-1655.

Q	1.	2.	3.	4.	5.	6.	7.	8.	=
S	3	3	3	2	3	3	2	2	21

Johansson, D., Jönsson, P., Ivarsson, B., & Christiansson, M. (2020). Information Technology and Medical Technology Personnel´s Perception Regarding Segmentation of Medical Devices: A Focus Group Study. Healthcare (Basel), 8(1), 23.

Q	1.	2.	3.	4.	5.	6.	7.	8.	=
S	3	3	3	3	3	3	1	2	21

Johnson, J., Onunkwo, I., Cordeiro, P., Wright, B. J., Jacobs, N., & Lai, C. (2020). Assessing DER network cybersecurity defences in a power-communication co-simulation environment. IET Cyber-Physical Systems, 5(3), 274-282.

Q	1.	2.	3.	4.	5.	6.	7.	8.	=
S	3	3	3	3	3	3	2	2	22

Katsis, C., Cicala, F., Thomsen, D., Ringo, N., & Bertino, Elisa. (2021). Can I Reach You? Do I Need To? New Semantics in Security Policy Specification and Testing. 165-174.

Q	1.	2.	3.	4.	5.	6.	7.	8.	=
S	3	3	3	2	3	3	3	3	23

Kurniawan, M., & Yazid, S. (2019). A systematic literature review of security software defined network: research trends, threat, attack, detect, mitigate, and countermeasure. 39-45. 10.

Q	1.	2.	3.	4.	5.	6.	7.	8.	=
S	3	3	3	2	3	3	3	3	23

Mhaskar, N., Alabbad, M., & Khédri, R. (2021). A Formal Approach to Network Segmentation. Computers & Security.

Q	1.	2.	3.	4.	5.	6.	7.	8.	=
S	3	3	3	3	3	3	2	3	23

Paillisse, J., Portoles, M., Lopez, A.M Rodriguez-Natal, A., Iacobacci, D., Leong, J., Moreno, V., Cabellos, A., Maino, F., & Hooda, S. (2020). SD-Access: Practical Experiences in Designing and Deploying Software Defined Enterprise Networks.

Q	1.	2.	3.	4.	5.	6.	7.	8.	=
S	3	3	3	3	3	3	3	3	24

Paul, B., & Rao, M. (2022). Zero-Trust Model for Smart Manufacturing Industry. Applied Sciences. 13. 221.

Q	1.	2.	3.	4.	5.	6.	7.	8.	=
S	2	2	2	2	3	3	3	3	**20**

Sheikh, N., Pawar, M., & Lawrence, V. (2021). Zero trust using Network Micro Segmentation. In IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 1-6).

Q	1.	2.	3.	4.	5.	6.	7.	8.	=
S	3	3	2	3	3	3	3	2	**22**

Simpson, D. W. R. (2022). Toward a zero trust metric. Procedia computer science, 204, 123-130.

Q	1.	2.	3.	4.	5.	6.	7.	8.	=
S	3	2	3	3	3	3	3	3	**23**

Simpson, W.R., Foltz, K.E. Network Segmentation and Zero Trust Architectures (2021) Lecture Notes in Engineering and Computer Science, 2242, pp. 201-206.

Q	1.	2.	3.	4.	5.	6.	7.	8.	=
S	3	2	2	3	3	3	3	3	**22**

Smeriga, J., & Jirsik, T. (2019). Behavior-Aware Network Segmentation using IP Flows

Q	1.	2.	3.	4.	5.	6.	7.	8.	=
S	3	3	3	3	3	3	2	3	**23**

Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero Trust Architecture (ZTA): A Comprehensive Survey. IEEE access, 10, 57143-57179.

Q	1.	2.	3.	4.	5.	6.	7.	8.	=
S	3	3	3	3	3	3	3	3	**24**

Tselios, C., Politis, I., & Xenakis, C. (2022). Improving Network, Data and Application Security for SMEs. Association for Computing Machinery.

Q	1.	2.	3.	4.	5.	6.	7.	8.	=
S	3	2	2	2	3	3	3	3	**21**

Tsuchiya, A., Fraile, F., Koshijima, I., Bas, A., & Poler, R. (2018). Software defined networking firewall for industry 4.0 manufacturing systems. Journal of Industrial Engineering and Management. 11. 318.

Q	1.	2.	3.	4.	5.	6.	7.	8.	=
S	3	3	3	3	3	3	3	3	**24**

Venugopal, V., Alves-Foss, J., Gogineni Ravindrababu, S. (2019). Use of an SDN Switch in Support of NIST ICS Security Recommendations and Least Privilege Networking. ICSS: Proceedings of the Fifth Annual Industrial Control System Security (ICSS) Workshop. 11-20.

Q	1.	2.	3.	4.	5.	6.	7.	8.	=
S	3	3	3	2	3	3	3	3	**23**

Wagner, N., Şahin, C.Ş., Pena, J., Streilein, W.W. (2019). Automatic Generation of Cyber Architectures Optimized for Security, Cost, and Mission Performance: A Nature-Inspired Approach. In: Shandilya, S., Shandilya, S., Nagar, A. (eds) Advances in Nature-Inspired Computing and Applications. EAI/Springer Innovations in Communication and Computing. Springer, Cham.

Q	1.	2.	3.	4.	5.	6.	7.	8.	=
S	3	3	3	3	3	3	2	3	**23**

Wagner, N., Sahin, C.M., Winterrose, M., Riordan, J., Peña, J, Hanson, D., & Streilein, W. (2016). Towards automated cyber decision support: A case study on network segmentation for security. 1-10.

Q	1.	2.	3.	4.	5.	6.	7.	8.	=
S	3	3	3	3	3	3	2	2	**22**

Wüsteney, L., Menth, M., Hummen, R., & Heer, T. (2021). Impact of Packet Filtering on Time-Sensitive Networking Traffic. In 2021 17th IEEE International Conference on Factory Communication Systems (WFCS) (pp. 59-66).

Q	1.	2.	3.	4.	5.	6.	7.	8.	=
S	3	3	3	3	3	3	3	3	**24**

Xie, L., Hang, F., Guo, W., Lv, Y., & Chen, H. (2021). A Micro-Segmentation Protection Scheme Based on Zero Trust Architecture. In ISCTT 2021; 6th International Conference on Information Science, Computer Technology and Transportation (pp. 1-4).

Q	1.	2.	3.	4.	5.	6.	7.	8.	=
S	2	2	3	3	3	2	3	3	**21**

Zvabva, D., Zavarsky, P., Butakov, S., & Luswata, J. (2018). Evaluation of Industrial Firewall Performance Issues in Automation and Control Networks.

Q	1.	2.	3.	4.	5.	6.	7.	8.	=
S	3	3	3	3	3	3	2	3	**23**