International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 16, No.1 (Sep-24)

http://dx.doi.org/10.12785/ijcds/1601111

Build a Secure Network Using Segmentation and Micro-segmentation Techniques

Hussein A. Al-Ofeishat[1] **and Rafat Alshorman**[2]

[1]*Department of Computer Engineering , Al-Balqa Applied University, Salt, Jordan*
[2]*Department of Computer Science,Yarmouk University, Irbid, Jordan*

Received 21 Sep. 2023, Revised 26 Jun. 2024 , Accepted 28 Jun. 2024 , Published 26 Sep. 2024

Abstract: Due to the increasing number of threats and attacks that have threatened the network in recent years, novel methods and techniques have been improved to secure the infrastructure of the network and the data transmitted within it. Micro-segmentation and segmentation techniques are popularly used over computer networks to reduce defensive versus cyberattack. These techniques aim to minimise the damage obtained from attackers by segmenting the network into many clusters or sections and limiting the communications among them. Thus, each cluster or segment within the network becomes isolated from the others, which increases the security of highly sensitive data networks and prevent unauthorised people and attackers from accessing these sensitive data. In this paper, an enhanced environment has been suggested using NSX-T VMware to overcome the limitations of conventional micro-segmentation and segmentation environments. the suggested environment NSX-T with Sky ATP and policy enforcer to enhance the performance and security of the network. The suggested environment is presented to deal with large environments that involve multi-hypervisors and multiple clouds. The performance of this environment has been combined with the other two scenarios. The results of the comparison proved that the performance of this suggested scenario is better than those of the other two scenarios. In addition, the results illustrated that security, workload mobility, and flexibility are higher within this scenario, whereas consumed time, cost, and complexity are lower than those in other scenarios.

Keywords: Micro-segmentation, Segmentation, cyberattack, Clusters, Security, Attackers, NSX-T, Sky API, policy enforcer

1. INTRODUCTION

Historically, the security of the network is considered a complex subject that only experienced and well-trained experts can treat. Nevertheless, more people have recently become interested in understanding the fundamentals of security within the networked world [1] and [2]. The design of most conventional networks has been concentrated only on the outer perimeter security. Thus, the segmentation of networks within recent networks has become a critical method to enhance the management of the network, cyber security, and inner perimeter security. Network violation becomes very difficult by network segmentation, which also retards attackers. In addition, the isolation of applications and sensitive data from curious users and industrial spying through network segmentation represents a restriction for insiders [3].

Further, the defence of computer network is known by the actions that are obtained by the network use to respond to, detect, analyse, monitor and protect unauthorised activity in the network and enterprise systems of information. Further, the defence of network uses an inclusive set of software and hardware tools to prevent nefarious actions obtained from malicious entities, Many recent enterprises construct their defenses based on the fortress approach. The defense tools of the network are used to defend this approach, where a strong boundary between the trusted inner side and the untrusted outer side is constructed by these tools. Network segmentation uses the concept of the fortress to construct a layered model of the fortress, presenting smaller fortresses with specific protections and boundaries within each fortress. Thus,more defense layers will be provided by this model, which will reduce the damage throughout intrusions and exploits as well as restrict the mobility of the threat [4], [5] and [6].

Conversely, recent organizations are largely based on their own systems of information, where large numbers of investments are made annually. In recent years, these systems have been computerised, while networking has become the most popular trend. Further, computer resources and information available in an organisation and among collaborative organizations are often sensitive to services and goods production. The availability, integrity, and con-

E-mail address: ofeishat@bau.edu.jo, r.alshorman@yu.edu.jo

fidentiality attributes are conventionally used to define the security of a computer. Availability means the avoiding of unauthorised resources or information withholding, while integrity means the avoiding of unauthorised information alternation. Furthermore, confidentiality means the avoiding of unauthorised information disclosure [7].

Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more and more people become "wired", an increasing number of people need to understand basics of security in a networked world.

Two scenarios for the implementation of micro-segmentation and segmentation within networks have been studied. An enhanced scenario has been suggested to overcome the limitations of conventional micro-segmentation and segmentation scenarios. The suggested scenario integrates NSX-T micro-segmentation with Sky API and policy enforcer to enhance the security and performance of the network.

The paper consists of four other sections, where many Previous works have been reviewed within the second section, while micro-segmentation and segmentation techniques have been studied within the third section. The methodology of the study has been illustrated in the fourth section. The results of the study have been discussed in the fifth section. A conclusion of the study has been provided in the last section.

2. Related Works

Layered protection and network segmentation strategies are considered essential to construct a more secure network. Thus, guarded commands and family algebra have been utilised by [8] to form a formalism and define the segmentation of the network. A series of resources and their polices of access control have been used to suggest two algorithms that represent output and input strong network topology in addition to firewall policies. The formalism of network segmentation has been used to compute the utilised firewall policies, which are then strategically inserted into the network for performing "Defence in Depth (DD)". Moreover, a "Software Defined Network (SDN)" has been built using the suggested algorithms and the use of SDN within "Internet of Things (IoT)" and dynamic networks has been discussed. The issue of cyber decision about how a suitable segmentation architecture for the network can be selected has been studied within this literature. The selection of architecture is based on the mission and security behaviour in a certain environment of networking. A new method has been suggested to support the selection decision using agent-based simulation and a heuristic search approach. The suggested prototype system has been implemented within a simple case study to obtain better or ideal architectures that support the environment of a network exposed to cyber-attacks. Within the suggested prototype system version, several manual actions are demanded to begin the execution of components, and the components of the system are not completely incorporated. Thus, future versions should completely incorporate the components of the system. Furthermore, [9] plan to explore techniques based on population like grammatical evolution, particle swarm, and genetic algorithms to enhance the behaviour of systems based on effective candidate structures. Architectures of network segmentation have been suggested by [10] as use case forms that are appropriate for information loss and security. The suggested system combined between simulation modelling and computational intelligence to estimate and construct the architectures as well as acclimate to the variation in threat to. The outcomes of the study show that the suggested system can acclimate to the variation in threat levels and segment architectures at acceptable risk threshold within a certain threat environment. Furthermore, recent work has addressed the requirement of systems that based on the architectures to minimise the loss of information within actual time and to obtain ideal decisions for cyber security. On the other hand, this system can be enhanced in the future to handle segmentation policy composition, automation, and synthesis. In addition, controls of network segmentation, which involve components and productive potentials of cyber security, can be used to achieve network security. Another segmentation technique is micro-segmentation, which is a novel security technique that divides physical networks into separated logical workloads or micro-segments. Thus, an analytical framework has been developed by [11] to quantify and characterise the micro-segmentation effectiveness in improving the security of networks. A framework based on attack graphs and network connectivity was used to estimate the robustness and exposure network. The results show that the use of micro-segmentation enhances the network robustness and exposure reduction in a range extending between 60% and 90%. According to [12], the secure design of a network based on micro-segmentation can reduce the movement rate of attackers within the network. It also offers more chances to discover this movement. However, organizations that use a secure design of the network will discover that micro-segmentation adds more complexity and cost to the network as compared with the percentage of incidents severity and number reduction. On the other hand, the effort prolonged in segmenting, classifying, and learning network strengthens and value for the whole controls of the organisation. Due to the absence of pure guidance on how segmentation can be suitably implemented within recent architectures, a Markov continuous-time chain has been suggested as a low-cost method to estimate architecture performance. In addition, the chain allows security practitioners to observe more than one candidate architecture of segmentation to determine the most optimal model that fits with their network environment[13]. According to [14], the impact of a conventional perimeter that is based on security becomes less effective due to the movement of data centres towards the visualisation of storage resources, networking, and computing. Thus, novel models of secure data centres should be based on software, involve the model of zero trust, and adopt micro-segmentation. [15] focused

on security of network within IT systems. It also presented security remedies and modern network threats. the key aim of the study was to supply consumers with a secure device for communication and to restrict hackers from reaching secured data. The review illustrated that system security can be enhanced using sophisticated security systems. Furthermore, sophisticated monitoring systems can minimise data breaches. Novel guidelines and protocols are also required to secure data of organizations.

3. Segmentation Technique

Segmentation of the network is considered a defensive technique to reduce and prevent the ability of cyber attackers to move throughout the network. Further, this technique is interested in separating the network into multiple segments and monitoring communication among the internet and segments and among segments. The aim of segmentation is to protect the resources of the network through communication restriction, which enhances the security of the network by [13]:

- Minimising entry point number that is demanded for the network.
- Restricting attackers from infiltrating the network.
- Obstructing the attacker's ability to pivot other devices of the network and their lateral entry.
- Enhancing the ability of defenders to remediate and detect cyber intrusions and simplify the observation of communication.

Segmentation is usually performed by the integration of "Software Defined Networking (SDN)", "Virtual Local Area Networks (VLANs)," and firewalls [16]. The main types of segmentation are as follows:

A. *VLANs Segmentation*

A set of separated networks is created inside the centre of the data by segmenting the network through VLANs. Every network represents an individual broadcast domain. VLAN segmentation strictly limits access to the surfaces of a system attack. Furthermore, it enhances threat of effort and minimises the packet-sniffing abilities. Furthermore, the network devices and servers can only be seen by authorised users who should access the network to perform daily tasks. Protocol segmentation is an additional benefit of segmentation, where the architects of the network can set particular protocols to particular enterprise segments [17].

Although VLAN segmentation provides users with elastic movement and enhances security within the network, it comes with two main restrictions [18]:

- Protocol limitations: there are a limited number of segments that can be provided by VLANs, which restricts the implementation of segmentation within huge data centres.

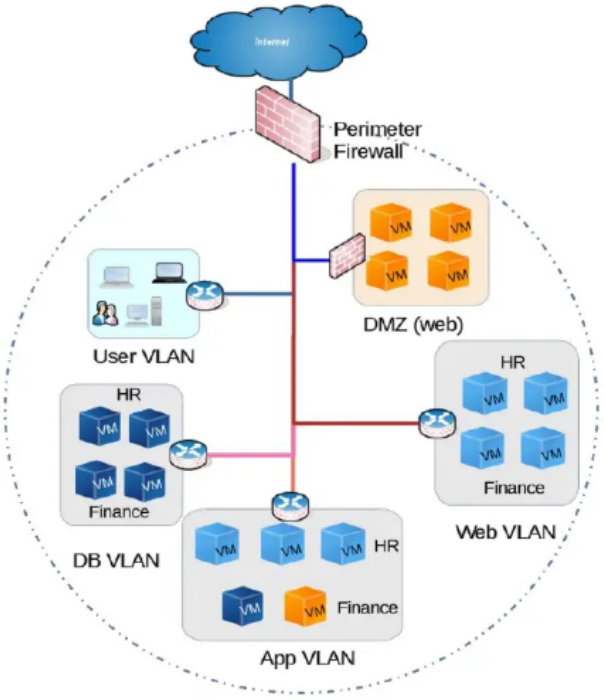

Figure 1. the structure of basic network segmentation based firewall [20].

- Cloud Technology: Clouds cannot be involved within VLAN segmentation and many other conventional networks.

B. *Firewall Segmentation*

Firewalls are considered as devices of network security that observe outgoing and incoming traffic of the network as well as determine if certain traffic will be blocked or allowed depending on certain security rules. In addition, firewalls represent a key part of a security system that implements security policies that only allow legal users from entering resources. Firewall segmentation is used to place each resource set under a certain firewall [19]. Figure 1 illustrates the structure of a basic network segmentation based on the firewall.

Furthermore, an edge or external firewall is used within segmentation where this firewall is not directly connected to the network segments of end users. Logical and physical separation is usually required between core infrastructure and user communities. This separation reduces the visibility of the inside network actions. Therefore, an internal firewall can be used to solve this challenge and enhance the performance of segmentation. The interior firewall connects multiple segments within the network, enabling traffic mitigation, control, and visibility among those segments [21]. Firewall VLAN segmentation is considered an application of firewall segmentation. As mentioned before, the security and performance of a system can be enhanced by

the segmentation technique. Thus, this is more significant for "Internet of Thing (IoT)" devices, where the network prevents communication between those devices and enables communication only between them and the controller or management platform. Furthermore, the data within IoT devices should be separated to enhance the traffic control among selected zones. Group areas are constructed by firewall VLANs, where network layers or geographic locations are used to divide those areas. In addition, access to devices and the control of traffic flow can be simply understood by properly segmenting resources. On the other hand, firewall VLANs represent the construction of Layer 2(Data Link), which makes the management of enterprise networks difficult and complex, particularly when flexible and agile networks are demanded[22] and [23].

C. SDN Segmentation

SDN represents a networking model that removes the restrictive limitations that are added to the network through networking hardware, which used within conventional non-SDN networks. Furthermore, SDN enhances the programmability, scalability, and agility of traffic switching and control. On the other hand, the algorithm of "Robust Network and Segmentation (RNS)" should be used within this type to implement segmentation strategies and layered defence in order to attain secure access control to the network and to properly divide the network. This algorithm segments the resources of the network into different clusters using a certain systematic approach. It also provides the topology of the network that determines the desired cluster placement within the network [19]. SDN technology has recently been used to simplify the segmentation of network traffic. Traffic tags are also used by this technology to remove the complexity of conventional approaches and to implement a policy of network segmentation on the components of the network. While customers use the identical fundamental physical infrastructure, various virtual networks are provided by SDN. Further, centralised controllers are used by SDN to enhance network programmability and automation. Complexity is the key weakness of segmentation with the SDN, where it concentrates on the policy of the network instead of application flows and security visibility directed through other approaches [24].

D. Zero-Trust segmentation

This type of segmentation is considered a developmental model of security that is constructed to reduce threats and attack risk in internal and external networks. Therefore, three topics should be considered when constructing a zero-trust network [25] :

- Guarantee secure access to the entire data depending on location and user.
- Access control implementation.
- • Examine traffic assets records.

Furthermore, the model of a zero-trust network is considered to be a segmentation gateway. All resources within recent networks involving package forwarding, cryptographic engines, firewalls, access control, and content filtering are concentrated by the zero-trust concept ([25]). In addition, the architecture of zero-trust utilises the protection principle of individual enterprise resources, involving computing and data rather than protecting the borders of the network. Thus, the access credentials and identities of the request advent of the interior network should be verified at every resource. The architecture of zero-trust has been constructed to reduce interior lateral movement and avoid data breaches within enterprises [26], [27]. The zero-trust model has several weaknesses and strengths, as shown in the table I [28]:

TABLE I. vulenerabilities and strengths of Zero-trust [28].

Strengths	Vulnerabilities
Fewer weakness	additional time of setup
Improved data protection	Extra complex administration of application
Smart segmentation of data	Extra appliances to treat with
Robust identity polices of user	Additional management for diverse users

4. Micro-segmentation Technique

Micro-segmentation is considered a technique to construct secure areas within cloud deployments and data centres to secure and separate all workloads to create a granulated secure network. Furthermore, polices within micro-segmentation are implemented on each workload to generate stronger attack resistance. Two key security problems are addressed by micro-segmentation: controlling and distinguishing traffic of the network above layer four [29].

On the other hand, this technique is distinguished by implementing rules on every VM instead of using a firewall to conserve the physical network environment. Many operations of the data centre have a dynamic nature that was not previously probable. Therefore, Micro-segmentation was created to support and reflect this nature [30]. Four key advantages can be added to the network by Micro-segmentation (See [30]):

1) Minimise surface of attack: visibility of the entire network environment is provided by micro-segmentation without reducing innovation and development.
2) Enhanced breach containment: security teams use micro-segmentation to observe network traffic versus predefined polices, remediate breaches, and reduce response time.
3) Robust regulatory compliance: a group of polices can be constructed by micro-segmentation to separate regulated systems from the remaining infrastructure. Therefore, applying granulated control over the communications of regulated systems, minimising the

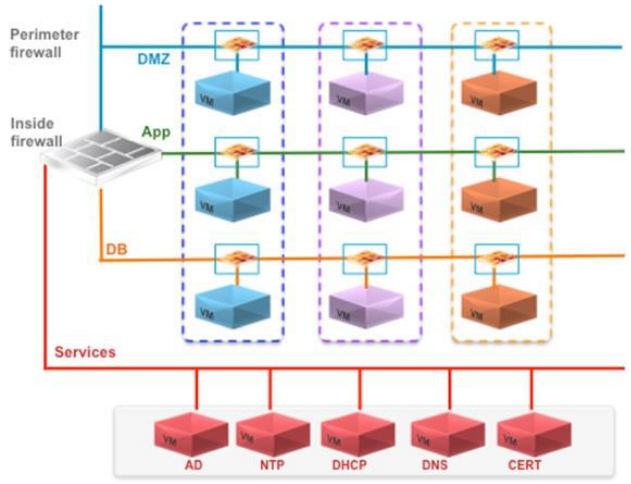

Figure 2. VMware NSX with micro-segmentation example [33].

incompatible usage risk.

4) 4. Management of streamlined policy: firewall polices can be managed simply through the particular architecture of micro-segmentation. A particular consolidated policy is used by this arising best practise to reduce and detect threats and to control subnet access within one network section. Hence, the security posture of organizations can be reinforced and the surface of attack can be also minimised using this approach.

Due to the increasing number of advanced permanent threats that spread through application vulnerabilities and targeted users, multiple network-layer segmentation is required to maintain an appropriate posture of protection and security. Therefore, security controls at the application level, like developed aware protection and application-level intervention protection, are required for these developed threats to conserve selected workloads [31]. Micro-segmentation with NSX represents a suitable platform to deal with these threats. Thus, VMware NSX enhances micro-segmentation to be more cost-effective, operationally feasible, and scalable. Furthermore, NSX supports micro-segmentation with service sequence for partner services, overlay-based separation, distributed firewalking, and central policy controls to address the security requirements for the rapidly developing landscape of information technology [32]. An example of implementing VMware NSX within micro-segmentation is illustrated in Figure 2.

The distributed firewall is the key module used within the micro segmentation. Furthermore, the implementation of NSX deployed the distributed firewall into every hypervisor as a core module. Thus, the policy rules for distributed enforcement can be centrally configured. Traffic can be filtered by distributing the firewall over the level extended between the 2nd layer and the 4th layer. Therefore, the rules of security can be implemented only when a connection between the VMs and the identical virtual or logical switch is presented [20].

TABLE II. components of the suggested environment .

Component name	Number of components	Location within the environment
External Firewall devices	2	external firewall cluster
Core switches	2	switching fabric cluster
Access switches	2	switching fabric cluster
VMware	2	Hypervisor cluster
VM-APP	1	Virtual layer cluster
VM-DB	1	Virtual layer cluster
APP VLANs	1	Virtual layer cluster
DB VLANs	1	Virtual layer cluster
Internal un-routed VXLAN switch	2	Virtual layer cluster (Inside hypervisor hosts)

5. Methodology

The methodology of this paper is based on reviewing three different scenarios to show how the performance and security of the network can be enhanced by segmentation. The first scenario represents the conventional segmentation environment, while the second represents the micro-segmentation environment. The third scenario represents the suggested environment that integrates NSX-T with Sky ATP and policy enforcer to overcome the limitations of the other two scenarios and to enhance the performance and security of the network. The structure, components, and topology of these scenarios are shown below:

A. The Structure of the Environment

The studied environment was segmented into four main clusters: external firewall, switching fabric, hypervisor, and virtual layer clusters. “Virtual Extensible LAN (VXLAN)” has also been introduced to perform logical segmentation for “Virtual Machines (VMs)”. Because VXLAN has various types of behaviour and overhead, it has been selected within this structure instead of VLANs to enhance the results. Furthermore, two databases and application roles VM have been used to represent the participants of the test environment. The key components involved within the constructed environment are shown in the table II:

Two simple scenarios were selected to investigate and

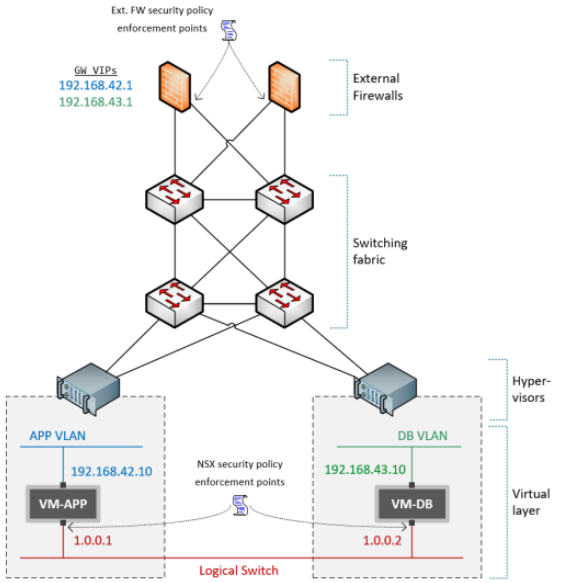

Figure 3. The entire structure of the suggested network environment [34].

Figure 4. Path of network traffic in Scenario 1 [34].

highlight the distinctions between the implementation of conventional segmentation and the implementation of a novel micro-segmentation approach. The major tests that will be studied by these scenarios are: network security, performance, complexity, flexibility, cost, and workload mobility. The entire structure of the suggested network environment is shown in Figure 3, where the two scenarios will be implemented.

B. Scenario 1: Secure network with conventional segmentation

A conventional implementation by segmenting the hosts into individual VLANs has been represented within Scenario 1, depending on the security control and roles allowed through the outer firewall device by routeing of internal VLANs. A policy of security has been applied where it is executed when traffic reaches the interfaces of the firewall [34]. Thus, the packets of the network are required to pass over more than one physical and virtual component, as illustrated in the Figure 4. In addition, the firewall within this scenario represents a bottleneck for traffic transmitted from one network to another and passing over it [34] and [20].

The security within the conventional network is established at the border or the edge to involve the south-north communication. Sub-sections and sections are created

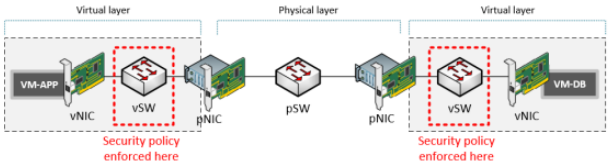

Figure 5. Path of network traffic in Scenario 2 [34].

beside the firewall to extend the security. Therefore, any communication with the outer section entities should go over the firewall. Furthermore, any outer or intersection communication that comes from every host within the section should be accessed over a departmental firewall, and this will increase the delay and traffic within the network [20].

C. Scenario 2: Secure network with NSX micro-segmentation

Segmentation within this scenario has been applied within "Virtual Network Layer (VNL)", where there is no need to pass via layer-3 or firewall devices. Thus, an individual unrouted segment of the logical network is used to connect all VMs within the network. In addition, the real policy of security has been enforced within the ports of virtual switches and implemented only on hypervisor hosts. Therefore, micro-segmentation of the VM level and the use of the basic flat structure of the network are enabled. By this scenario, logical segments can be separated from the security area thinking type and designed in a more effective way. Moreover, when a shift within protection requirements is needed, the security policy can be simply modified compared with the re-structuring architecture of a logical network [34].

In addition, as the traffic needs hair-pinning through any physical appliance, its path is as direct as possible, and it only traverses through the necessary switching fabric from one hypervisor to another, as shown in Figure 5. This data path topology was verified using the NSX network trace tool, [34].

D. The Suggested Scenario

VMware NSX can be considered as a security and networking platform that is able to provide micro-segmentation through the developed components involved within the recent centre of data. In addition, micro-segmentation with NSX enhances the efficiency and agility of the centre of data and allows it to maintain an agreeable posture of security at the same time [31].

Furthermore, NSX-T segmentation provides IT security with a zero-trust structure, which means to verify everything and trust nothing. Therefore, this type of micro-segmentation constructs a container workload or security perimeter across every VM with a vitally identified policy [35].

As shown in the previous sections, the second scenario with NSX micro-segmentation achieved enhanced performance compared with conventional segmentation in scenario 1. However, this scenario is not adequate for dealing with large environments that involve multiple hypervisors and multiple clouds. Therefore, it cannot provide a high level of security for large, sensitive, and variant workloads. An enhanced environment has been suggested in this paper to overcome these limitations. The suggested environment inserted NSX-T VMware product for micro-segmentation where it integrates innermost in the infrastructure of the network and not only in visualisation layer. This product also simplifies operations within security and networking. In addition, the suggested environment integrated NSX-T with Sky ATP and policy enforcer to enhance the performance and security of the network. The integration between policy enforcement and threat to secures the virtual and physical network environments. This integration is considered by the solution of "Juniper Connected Security (JCS)" which is composed of the following:

- An engine of threat to: this is represented by a cloud relay on SKY "Advanced Threats Prevention (ATP)" to detect recognised and unrecognised threats. Feed information is used from different sources to detect recognised threats while unrecognised threats are determined through different methods like threat to, machine learning, and sandbox.
- Central management of policies: This component is based on a policy enforcer that communicates with third-party appliances through the network and the appliances of Juniper Networks. By this policy, inter- and intra-communications of the network are visible.

Furthermore, the cloud relays on SKY ATP can be considered as a security framework that protects the hosts within the network from advanced security threats. A system of next-generation firewall like (SRX firewall) is integrated with the cloud that relies on software for threat detection to represent this framework, as shown in the Figure 6.

A series of API connectors are also provided by the utilised policy enforcer for third-party switches or adaptors. These connectors are then used to integrate the policy enforcer with the NSX connector to allow the policy of the infected host to be implemented at the secure fabric. Furthermore, the connectors of NSX-T comprise an edge firewall that represents the desired Secure Fabric and NSX-T Manager, which represents vCenter. Two Tyre gateways are used to connect segments of the network with the physical infrastructure. Each tyretire gateway comprises two main components; Services router and a distributed router. In addition, the series device (vSRX) has been used as an edge firewall to transmit any suspected data traffic into Sky ATP. The logical topology of the suggested environment is shown in Figure 7.

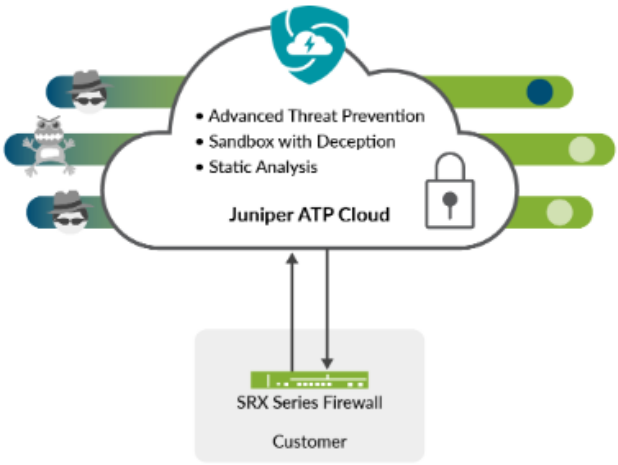

Figure 6. Path of network traffic in Scenario 2 [**?**].

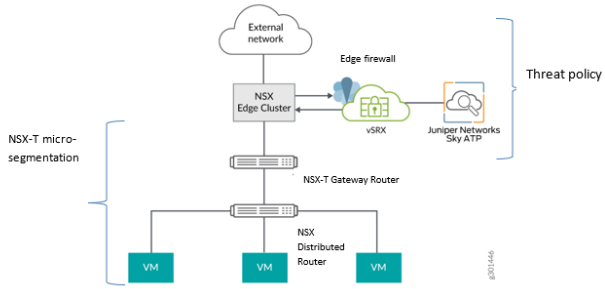

Figure 7. Logical topology of the suggested environment [22]

.

Then, the workflow manner of the applied policy can be summarised by the following steps:

- Step one: If any infection is discovered, the Policy enforcer will be informed by the infected addresses through Sky ATP.
- Step two: If the infected address pertains to the NSX secure fabric, the infected address list will be sent to the NSX connector through the NSX API.
- Step three: the VM matching to the sent IP addresses will be retrieved by the NSX service.
- Step four: The $SDSN\_BLOCK$ security tag will be then created by the NSX API to be tagged into a suitable VM.

The above steps show the high level of security provided by implementing NSX into the segmented network and by the integration between the policy enforcer and Sky ATP. Inner threats (inside the network) and outer threats (surrounding the network) can also be detected by this environment.

6. Results and Discussion

Segmentation techniques and micro-segmentation techniques have been developed to secure and protect the network from various threats and attacks. However, conventional segmentation cannot solve all network security problems. Therefore, micro-segmentation has been developed to solve these problems and to enhance the behaviour of the network. Within this section, the performance of the studied scenarios is discussed and compared to show which one is the best. The results of network measurements have been provided at the end of this section based on the performance evaluation. Within the conventional network segmentation scenario, the network is broken or segmented into several segments (VLANS). In addition, the network has been segmented depending on the North-South transferred traffic, which crosses the border of security and runs among servers and clients. On the other hand, micro-segmentation within the second scenario places every application or device within its particular logically separated segment, and this enhances the control and visibility within the network. Furthermore, the network within scenario 2 has been segmented depending on east-west transmitted traffic, which moves horizontally inside and across the network. Based on the above, the performance and security of the network were enhanced by the implementation of segmentation through the external firewall cluster and the segmented VLANs. However, this scenario only focuses on the North-South traffic security without concern for the internal security of traffic. Therefore, Scenario 2 provides the suggested environment with greater security than Scenario 1. Further, the architecture of the network may require re-architecture from time to time, and this will be expensive, time-consuming, and difficult through segmentation because it is based on physical infrastructure breaking. However, this issue does not exist within micro-segmentation, and this will reduce time-consuming, complexity, and cost. The insertion of micro-segmentation enhances the performance of the network by minimising the amount of hair pinning. Furthermore, there is no need for an external hardware device (external firewall) within Scenario 2, and this makes the path of traffic more suitable and shorter as well as enhances the security of traffic and the environment. Thus, the performance of the network in Scenario 2 is better than in Scenario 1. Furthermore, the implementation of micro-segmentation with kernel-based firewall and hypervisor level provides a security workload over virtualization clouds and platforms. Furthermore, this implementation provides flexibility to deal with changes, additional policy options to be integrated with the platform, workload mobility, and dynamic firewalling load distribution. However, the suggested environment within the two scenarios (Scenario 1 and 2) is not adequate to deal with large environments that involve multiple hypervisors and multiple clouds. Therefore, it cannot provide a high level of security for large and variant workloads. In addition, the inner and outer threats cannot be detected by one scenario, where the outer threats can be detected by scenario 1 and the inner threats can be detected by scenario 2. Therefore, the suggested scenario overcomes these limitations. The suggested scenario provides a high level of security by implementing NSX into the segmented network and by integrating the policy enforcer and Sky ATP. Inner threats (inside the network) and outer threats (surrounding the network) can be detected by this environment. In addition, the physical site of information is not important to be protected where it can be preserved anywhere it exists. On the other hand, security within this environment depends on policies; therefore, it is simpler than security within hardware architectures. Furthermore, the structure of this environment is more cost-effective because it is considered as a software model where security can be easily and rapidly scaled without the need to subtract or add hardware devices.

TABLE III. The results of Scenarios measurements.

Measurement name	Scenario 1	Scenario 2	Scenario 3
Security	Low level	Middle level	High level
Performance	Low	Middle	High
Cost	High	Middle	Low
Complexity	High	Middle	Low
Consumed-time	High	Middle	Low
Workload mobility	Low	Middle	High
Flexibility	Low	Middle	High
Inner threats	Not Detected	Detected	Detected
Outer threats	Detected	Not Detected	Detected
Multi-cloud environments	Cannot deal with them	Cannot deal with them	Deal with them

With the implementation of Micro-segmentation based on NSX, a dynamic policy of security can be created where it can be simply introduced into any novel requirements without the need to modify the existing infrastructure of the network. In addition, the implementation of micro-segmentation through NSX provides scalable software and distributes the processing of security control over the entire virtualisation platform rather than of a selected centralised network point.

The results of the Scenarios measurements can be summarized in Table III:

7. Conclusion

Micro-segmentation and segmentation techniques are popularly used over computer networks to reduce defensive versus cyber-attacks. These two techniques have been used to enhance the performance and security of the network. Thus, Two simple scenarios were selected to investigate and highlight the distinctions between the implementation of conventional segmentation and the implementation of

a novel micro-segmentation approach. However, these two scenarios are not adequate for dealing with large environments that involve multiple hypervisors and multiple clouds. Therefore, an enhanced environment has been suggested in this paper to overcome these limitations. The suggested environment inserted the NSX-T VMware product for micro-segmentation to enhance network security. The results of the comparison confirmed that the performance of the suggested environment network is better within Scenario 3. The comparison shows that Scenario 3 provides higher security, performance, flexibility, and workload mobility.

References

[1] A. Deshpande, "Introduction to network security," *International Journal of Computer Sciences and Engineering*, vol. 3, no. 9, pp. 124–134, 2015.

[2] A. Kulkarni, A. Shivananda, A. Kulkarni, A. Kulkarni, A. Shivananda, and A. Kulkarni, "Ted talks segmentation and topics extraction using machine learning," *Natural Language Processing Projects: Build Next-Generation NLP Applications Using AI Techniques*, pp. 65–88, 2022.

[3] J. Toivakka, "Network segmentation," 2018.

[4] K. F. WR.Simpson, "Network segmentation and zero trust architectures," in *Proceedings of the Fifth International C* Conference on Computer Science and Software Engineering*, ser. WCE, July 7-9, 2021.

[5] D. Annu and A. Dudy, "Review of the osi model and tcp/ip protocol suite on modern network communication," *International Journal of Current Science Research and Review*, pp. 1230—-1239, 2024.

[6] P. Konduru and N. Nethravathi, "Secure and energy-efficient routing protocol based on micro-segmentation and batch authentication," *Computer Networks*, vol. 248, p. 110293, 2024.

[7] N. Zhang, "An introduction to computer & network security threats," *International Journal of Advance Research in Computer Science and Management Studies*, pp. 5–10, 2020.

[8] N. Mhaskar, M. Alabbad, and R. Khedri, "A formal approach to network segmentation," *Computers & Security*, vol. 103, pp. 102–162, 2021.

[9] N. Wagner, C. Şahin, M. Winterrose, J. Riordan, J. Pena, D. Hanson, and W. W. Streilein, "Towards automated cyber decision support: A case study on network segmentation for security," in *2016 IEEE Symposium Series on Computational Intelligence (SSCI)*, 2016, pp. 1–10.

[10] K. Ramesh, "Network segmentation strategies to articulate a new method to address growing information security concerns," *CIOSR Journal of Engineering (IOSRJEN)*, vol. 8, no. 6, pp. 43–52, 2018.

[11] N. Basta, M. Ikram, M. A. Kaafar, and A. Walker, "Towards a zero-trust micro-segmentation network security strategy: an evaluation framework," in *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2022, pp. 1–7.

[12] B. Peterson, "Secure network design: Micro segmentation." *ISSA Journal*, vol. 14, no. 12, 2016. [Online]. Available: https://sansorg.egnyte.com/dl/6p0mC8GPeQ

[13] N. Wagner, C. Ş. Şahin, J. Pena, J. Riordan, and S. Neumayer, "Capturing the security effects of network segmentation via a continuous-time markov chain model," in *Proceedings of the 50th Annual Simulation Symposium*, 2017, pp. 1–12.

[14] . L. Muller and J. Soto, "Micro-segmentation for dummies," *Tech. Rep,Wiley and Sons*, 2015.

[15] A. K. Dwivedi, M. Dwivedi, and M. Kumar, "Advances in network security: A comprehensive analysis of measures, threats, and future research directions," 2023.

[16] J. Turner, "7 network segmentation best practices to level-up your security," *Strongdm*, 2024. [Online]. Available: https://www.strongdm.com/blog/network-segmentation

[17] T. Olzak, "Vlan network segmentation and security-chapter 5," *Retrieved on*, vol. 15, no. 02, p. 2015, 2021. [Online]. Available: http://web.archive.org/web/20080207010024/http://www.808multimedia.com/winnt/kernel.htm

[18] Guardicore, "Network segmentation and micro-segmentation in modern enterprise environments," *White paper*, 2019.

[19] M. Alabbad and R. Khedri, "Dynamic segmentation, configuration, and governance of sdn," *Journal of Ubiquitous Systems and Pervasive Networks*, vol. 16, no. 1, pp. 7–22, 2022.

[20] P. Bala, "Network micro-segmentation," *SCRIBD*, 2023. [Online]. Available: https://www.scribd.com/document/564160802/Network-Micro-Segmentation

[21] "Internal segmentation firewall security where you need it, when you need it," *White paper*, 2016. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-isf-security-where-you-need-it-when-you-need-it.pdf

[22] JUNIPER Network, "Iot network segmentation," *Engineering Simplicity*, pp. 1–4, 2022. [Online]. Available: https://www.juniper.net/content/dam/www/assets/solution-briefs/us/en/iot-network-segmentation.pdf

[23] N. Basta, M. Ikram, M. A. Kaafar, and A. Walker, "Towards a zero-trust micro-segmentation network security strategy: an evaluation framework," in *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2022, pp. 1–7.

[24] Zenarmor, "What is network segmentation? introduction to network segmentation," *Sunny Valley Cyber Security Inc. (d/b/a Zenarmor).*, 2023. [Online]. Available: https://www.zenarmor.com/docs/network-basics/network-segmentation

[25] P. Assunção, "A zero trust approach to network security," in *Proceedings of the Digital Privacy and Security Conference*, vol. 2019. Porto Protugal, 2019.

[26] D. Eidle, S. Y. Ni, C. DeCusatis, and A. Sager, "Autonomic security for zero trust networks," in *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*. IEEE, 2017, pp. 288–293.

[27] C. DeCusatis, P. Liengtiraphan, A. Sager, and M. Pinelli, "Implementing zero trust cloud networks with transport access control and first packet authentication," in *2016 IEEE International Conference on Smart Cloud (SmartCloud)*. IEEE, 2016, pp. 5–10.

[28] T. E. Nyamasvisva and A. A. M. Arabi, "a comprehensive swot

analysis for zero trust network security model," *International Journal of Infrastructure Research and Management Vol. 10 (1), June 2022*, 2022.

[29] D. Huang, A. Chowdhary, and S. Pisharody, *Software-Defined networking and security: from theory to practice*. CRC Press, 2018.

[30] K.Ekambaram and M. Varun, "Microsegmentation: Defense in depth," *Dell Technologies Proven Professional Knowledge Sharing*, pp. 1–8, 2021. [Online]. Available: https://education.dell.com/content/dam/dell-emc/documents/en-us/2021KS_Ekambaram-Microsegmentation_Defense_in_Depth.pdf

[31] W. Holmes, "Mmicro-segmentation defined – nsx securing– part i," *VMware*, 2016. [Online]. Available: https://blogs.vmware.com/networkvirtualization/2016/06/micro-segmentation-defined-nsx-securing-anywhere.html/

[32] VMware NSX for vSphere, release 6.0x, "Microsegmentation using nsx distributed firewall: Getting started," *VMware*, 2014. [Online]. Available: https://docplayer.net/15756686-Microsegmentation-using-nsx-distributed-firewall-\protect\@normalcr\relaxgetting-started.html

[33] J. Myers, "Network security with micro segmentation from vmware," 2015. [Online]. Available: http://www.enpointe.com/blog/network-security-with-micro-seg-mentation-from-vmware

[34] J. Koskinen, "Microsegmentation as part of organization's network architecture: Investigating vmware nsx for vsphere[master's thesis]. jamk university of applied sciences," 2020.

[35] T. N. DNA, "Nintroduction to microsegmentation in vmware nsx-t," 2021. [Online]. Available: https://www.thenetworkdna.com/2021/03/introduction-to-micro-segmentation-in.html

Hussein Al-ofeishat is an associate Professor at Al Balqa Applied University, Department: Computer Engineering Department, College of Engineering E-mail: ofeishat@bau.edu.jo Field of Specialization: Computer Engineering Major: Computer Engineering. Research Interest: Computer Network and Network Security. Ph.D. 2005 at National Technical University of Ukraine, Faculty of Computer Engineering, MSc. 1992 at National Technical University of Ukraine Faculty of Electrical Engineering.

Scopus: https://www.scopus.com/authid/detail.uri?authorId=55539903200
google scholar: https://scholar.google.com/citations?user=O49fynUAAAAJ&hl=en
research gate: https://www.researchgate.net/scientific-contributions/2137895665_Amman-Jordan_Hussein
ORCID ID registered to your address ofeishat@bau.edu.jo is https://orcid.org/0000-0002-0113-6415

Rafat Alshorman is an associate professor in the department of computer science at Yarmouk University/Jordan. He completed his Ph.D. at Loughborough University/UK and his undergraduate studies at Yarmouk University
Jordan. His research interests lie in the area of algorithms and mathematical models, ranging from theory to implementation, with a focus on checking the correctness conditions of concurrent and reactive systems. In recent years, he has focused on theoretical computer science such as Graph theory and Numerical analysis. Dr. Alshorman research interests are: 1. Mathematical methods in computer science 2. Temporal logics 3. Concurrent systems 4.Machine learning 5. Network Security.