Build a Secure Network using Segmentation and Micro-segmentation Techniques

Hussein A. Al-Ofeishat [1], Rafat Alshorman[2]
[1]Computer Engineering Department, Al-Balqa Applied University, Salt, Jordan.
[2]Computer science Department, Yarmouk University, Irbid, Jordan.

Abstract

Due to the increasing number of threats and attacks that threaten the network during the 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 the defensive versus cyberattack. These techniques aim to minimize 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 and this will increase the security of highly sensitive data networks and prevent unauthorized people and attackers from reaching to these sensitive data. In this paper, the micro-segmentation and segmentation techniques have been studied. Further, two scenarios of the implementation of micro-segmentation and segmentation within networks have been studied. Then, an enhanced scenario has been suggested to overcome the limitations of those two scenarios. The suggested scenario integrates NSX-T micro-segmentation with Sky API and policy enforcer to enhance the security and the performance of the network. After that, a comparison between all scenarios has been achieved to show which one is the best.

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

1. Introduction

Historically, the security of the network is considered as a complex subject that only the experienced and well-trained experts can treat it. Nevertheless, more people recently became interested in understanding the fundamentals of security within the networked world (Deshpande, 2015).

The design of most conventional networks has been only concentrated on the outer side perimeter security. Thus, the segmentation of network within the recent networks becomes a critical method to enhance the management of the network, the cyber security as well as the inner perimeter security. Network violation becomes very hard by network segmentation, which also retards the attackers. In addition, the isolation of applications and sensitive data from curious users and industrial spying through network segmentation represents a restriction for the insiders (Toivakka, 2017).

Further, the defense of computer network is known by the actions that obtained by the network use in order to respond to, detect, analyze, monitor and protect unauthorized activity in the network and enterprise systems of information. Further, the defense of network

uses an inclusive set of software and hardware tools in order to prevent nefarious actions obtained from malicious entities. A large number of recent enterprises constructs their defenses based on fortress approach. Defense tools of network are used to defend this approach, where a strong boundary among the trusted inner side and the untrusted outer side is constructed by these tools. The idea of the fortress is used by network segmentation to construct a layered model of the fortress, where smaller fortresses that supported by specific protections and boundaries are presented within each fortress. Thus, more defend layers will be provided by this model and this will reduce the damage throughout intrusions and exploits as well as restricts the mobility of threat (Simpson and Foltz, 2021).

On the other hand, recent organizations are largely based on their own systems of information, where large numbers of investments are yearly made. During the latest years, these systems have been computerized, while networking has become the most popular trend. Further, computer resources and information availabile in an organization and among collaborative organizations are oftentimes sensitive for services and goods production. The availability, integrity and confidentially attributes are conventionally used to define the security of computer. Availability means the avoiding of unauthorized resources or information withholding, while integrity means the avoiding of unauthorized information alternation. Further, confidentiality means the avoiding of unauthorized information disclosure (Zhang, 2020).

Therefore, this paper aims to study the micro-segmentation and segmentation techniques and to show how they can enhance the security of the network. In addition, two scenarios of the implementation of micro-segmentation and segmentation within networks have been studied. Finally, a comparison between the two scenarios has been achieved within this paper to show which one is the better.

2. Related Works

Layered protection and network segmentation strategies are considered as an essential step to construct more secure network. Thus, guarded commands and family algebra have been utilized by Mhaskar et al (2021) to form a formalism to define the segmentation of the network. A series of resources as well as their polices of access control has been used to suggest two algorithms that represent output and input strong network topology in addition to its firewall policies. The formalism of network segmentation has been used to compute the utilized firewall polices, which are then strategically inserted to the network for performing “Defense in Depth (DD)”. Moreover, a “Software Defined Network (SDN)” has been built using the suggested algorithms and the utilization of SDN within “Internet of Things (IoT)” and dynamic networks has been discussed.

The issue of cyber decision about how suitable segmentation architecture for the network can be selected has been studied within this literature. The selection of architecture is based on a mission and security behavior in a certain environment of networking. A new method has been suggested to support the selection decision using agent-based simulation and heuristic search approach. The suggested prototype system has been implemented within a simple case study to obtain better or ideal architectures supporting the environment of network exposed

to cyber-attack. Within the suggested prototype system version, several manual actions are demanded to begin the execution of components as well as the components of the system are not completely incorporated. Thus, the future version should completely incorporate the components of the system. Further, Wagner et al (2016) plan to explore techniques that based on population like grammatical evolution, particle swarm and genetic algorithms in order to enhance the behavior of systems that based on effective candidate structures.

Architectures of network segmentation have been suggested by Ramesh (2018), as use cases forms that are appropriate for information loss and security. The suggested system combined between simulation modeling and computational intelligence in order to estimate and construct the architectures as well as acclimating with the variation in threat levels. The outcomes of the study show that the suggested system is able to acclimate with the variation in threat levels and segment architectures at the acceptable risk threshold within a certain threat environment. Further, the recent work treats the requirement of systems that based on the architectures to minimize 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 with segmentation policies composition, automation, and synthesis. In addition, controls of network segmentation, which involve component and productive potentials of cyber-security, can be used to achieve network security.

Another technique of segmentation is micro-segmentation, which is a novel technique of security that divides physical networks to separated logical workloads or micro-segments. Thus, analytical framework has been developed by Basta et al (2022) to quantify and characterize the micro-segmentation effectiveness in improving the security of networks. A framework that based on attack graphs and network connectivity has been used to estimate the robustness and exposure network. The results show that the utilization of micro-segmentation enhances the network robustness and the exposure reduction in a range extended between 60% and 90%.

According to Peterson (2021), the secure design of network that based on micro-segmentation is able to reduce the movement rate of attacker within the network. It also can offer more chances to discover this movement. However, organizations that use a secure design of the network will discover that micro-segmentation added 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 improves strengthens and value for the whole controls of the organization.

Due to the absence of a pure guidance about how the segmentation can be suitably implemented within the recent architectures, a Markov continuous-time chain has been suggested as a method with low-cost to estimate the architecture performance. In addition, the chain allows security practitioners from observing more than one candidate architectures of segmentation in order to determine the most optimal model that fits with their environment of the network (Wagner et al, 2017).

According to Soto and Miller (2015), the impact of conventional perimeter that based on security

becomes less effective due to the movement of data centers towards the virtualization of storage resources, networking and computing. Thus, the novel models of secure data center should be based on software, involve the model of zero trust and adopt micro-segmentation.

3. Segmentation Technique

The segmentation of the network is considered as a defensive technique to reduce and prevent the ability of cyber attacker movement throughout the network. Further, this technique 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 network through communication restriction, which enhances the security of the network by (Wagner et al, 2017):

- Minimizing entry points number that demanded for the network.
- Restricting attackers from infiltrating the network.
- Obstructing the attacker's ability from pivoting other devices of the network and their lateral entry
- Enhancing the ability of defenders from remediating and detecting cyber intrusions and simplifying the observing of communication.

Segmentation is usually performed by integration of “Software Defined Networking (SDN)”, “Virtual Local Area Networks (VLANs) and firewalls (Turner, 2023). The main types of segmentations are:

1. VLANs Segmentation

A set of separated networks is created inside the center of the data by the segmentation of the network through VLANs. Every network represents an individual broadcast domain. VLAN segmentation strictly limits the access into the surfaces of system attack. Further, it enhances threat representative effort and minimizes the packet-sniffing abilities. Further, the network devices and servers can be only seen by authorized users who should access to the network to do the daily tasks. Protocol segmentation is an additional benefit of segmentation, where the architects of the network can set particular protocols to particular enterprise segments (Olzak, 2021).

Although VLANs segmentation provides users with elastic movement and enhances the security within the network, it comes with two main restrictions (Guardicore, 2019):

- Protocol limitations: there are a limit number of segments that can be provided by VLANs and this restricts the implementation of segmentation within huge data centers.
- Cloud Technology: Clouds cannot be involved within VLANs segmentation and many other conventional polices of network segmentation.

2. Firewall Segmentation

Firewalls are considered as the devices of network security that observe outgoing and incoming traffic of the network as well as determining if a certain traffic will be blocked or allowed depending on certain security rules. In addition, firewalls represent a key part of a security system which implementing policies of security that only allowing legal users from entering resources. Firewall segmentation is

referred to put each resource set under their certain firewall (Alabbade and Khedri, 2011). The figure below illustrates the structure of a basic network segmentation based on the firewall.

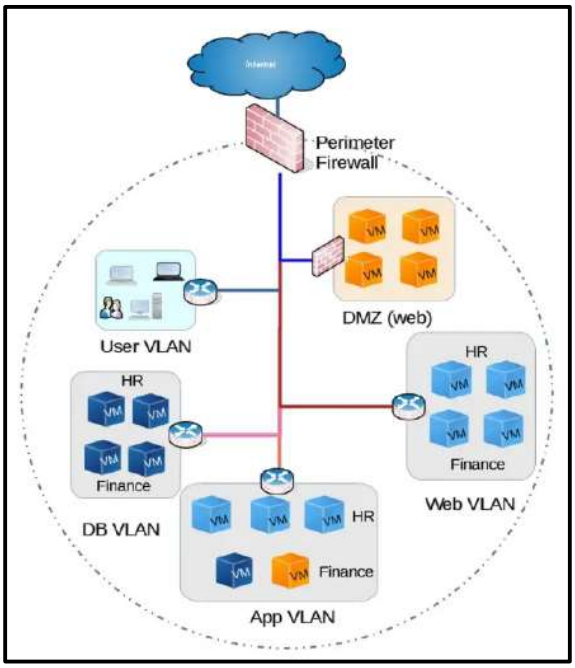

Figure 1: the structure of basic network segmentation based firewall (Bala, 2023).

Further, an edge or external firewall is used within segmentation where this firewall is not straightly connected to the network segments of end users. Logical and physical separation is usually demanded between core infrastructure and user communities. This separation reduces the visibility of the inside network actions. Therefore, internal firewall can be used to solve this challenge and to enhance the performance of segmentation. The interior firewall connects multiple segments with each other within the network and this enables traffic mitigation, controlling and visibility among those segments (FORTINET, 2016).

Firewall VLANs segmentation is considered as an application of firewall segmentation. As mentioned before the security and the performance of a system can be enhanced by segmentation technique. Thus, this is more significant for "Internet of Thing (IoT)" devices, where the network requires preventing the communication between those devices and enables the communication only between them and controller or management platform. Further, the data within IoT devices should be separated to enhance the traffic controlling among selected zones. Group areas are constructed by firewall VLANs, where network layers or geographic location are used to divide those areas. In addition, the access to devices and the controlling of traffic flow can be simply understood by segmenting resources properly. On the other hand, firewall VLANs represents the construction of Layer 2(Data Link) and this make the management of enterprise network difficult and complex, particularly when flexible and agile networks are demanded (JUNIPER Network, 2022).

3. SDN Segmentation

SDN represents a networking model removes the restrictive limitations that added to the network through networking hardware, which utilized within conventional non-SDN networks. Further, SDN enhances the programmability, scalability and agility of traffic switching and controlling. On the other hand, the algorithm of "Robust Network and Segmentation (RNS)" should be used within this type to implement segmentation strategies and layered defense in order to attain a secure access-control to the network and to properly divide the network. This algorithm segments the resources of network into different clusters using certain systematic approach. It also gives the topology of the network that determines the desired clusters placement within the network (Alabbade and Khedri, 2011).

The technology of SDN has recently been used to simplify the segmentation of network traffic. Traffic tags are also used by this technology to remove conventional approaches complexity and to implement a policy of network segmentation on components of the network. While customers used the identical fundamental physical infrastructure, various virtual networks are provided by SDN. Further, centralized 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 policy of the network instead of application flows and security visibility that directed through other approaches (Zenarmor, 2023).

4. Zero-Trust segmentation

This type of segmentation is considered as a developmental model of security that is constructed to reduce threats and attack risk internal and external network. Therefore, three topics should be attained when constructing Zero-trust network (Assunção, 2019):

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

Further, the model of a zero-trust network is considered as a segmentation gateway. All resources within recent networks involving, package forwarding, cryptographic engines, firewall, access control and content filtering are concentrated by zero-trust concept (Assunção, 2019).

In addition, the architecture of zero-trust utilizes the protection principle of individual enterprise resources, involving computing and data rather than protecting the borders of the network. Thus, access credentials and identities of the request advent of 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 (Eidle et al, 2017; DeCusatis et al, 2016).

The model of Zero-trust has several weaknesses and strengths as shown in the table below (Nyamasvisva and Mahmoud-Arabi, 2022):

Table 1: vulenerabilities and strengths of Zero-trust (Nyamasvisva and Mahmoud-Arabi, 2022).

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 as a technique to construct secure areas within cloud deployments and data centers to secure and separate all workloads in order to create granulated secure network. Further, polices within micro-segmentation are implemented on each workload in order to generate stronger attack resistance. Two key security problems are addressed by micro-segmentation: controlling and distinguishing traffic of the network that above layer four (Huang et al, 2018).

On the other hand, this technique is distinguished by implementing rules on every VM instead of using a firewall to conserve physical network environment. Many operations of the data center have a dynamic nature that was not probable before. Therefore, Micro-segmentation has been created to support and reflect this nature (Ekambaram and Varun, 2021).

Four key advantages can be added to the network by Micro-segmentation (Ekambaram and Varun, 2021)

1. Minimize surface of attack: a visibility for the whole network environment is provided by micro-segmentation without reducing innovation and development.
2. Enhanced breach containment: security teams use micro-segmentation to observe traffic of network 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, minimizing the incompatible usage risk.
4. Management of streamlined policy: firewall polices can be managed in a simple way through the particular architecture of micro-segmentation. A particular consolidated policy is used by this arising best practice to reduce and detect threats as well as controlling the subnet access within one network section. Hence, the security posture of organizations can be reinforced and the surface of attack can be also minimized by this approach.

Due to the increasing number of advanced permanent threats that spread through application vulnerabilities and targeted users, multiple network-layer segmentation is demanded to maintain appropriate posture of protection and security. Therefore, security controls of application-level, like developed malware protection and application-level intervention protection are demanded for these developed threats in order to conserve selected workloads (Holmes, 2016). 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 supported micro-segmentation with service sequence for partner services, overlay-based separation, distributed firewalling and central policy controls to treat the requirements of security for the fast developing landscape of information technology (VMware, 2014). An example of implementing VMware NSX within micro-segmentation is illustrated in the below figure.

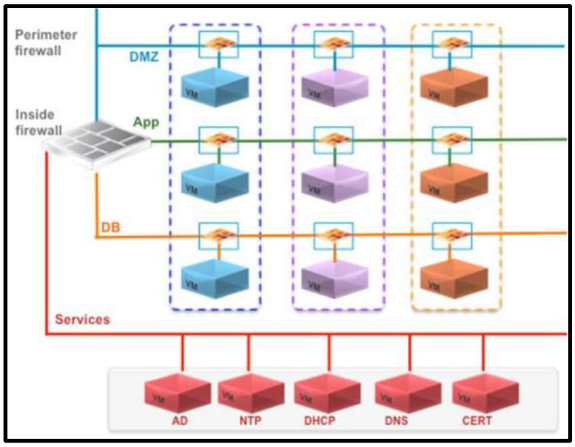

Figure 2: VMware NSX with micro-segmentation example (Myers, 2015).

Distributed firewall is the key module that used within the micro - segmentation. Further, the implementation of NSX deployed the distributed firewall into every hypervisor as a core module. Thus, the policy rules distributed enforcement can be centrally configured. Traffic can be filtered by distributing firewall over the level extended between the 2nd layer and the 4th layer. Therefore, the rules of security can be only implemented when a connection between the VMs and the identical virtual or logical switch is presented (Bala, 2023).

5. The studied Scenarios

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

Table 2: 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)

Two simple scenarios were selected to investigate and highlight the distinctions between the implementation of conventional segmentation and the implementation of 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 the figure below, where the two scenarios will be implemented in this structure.

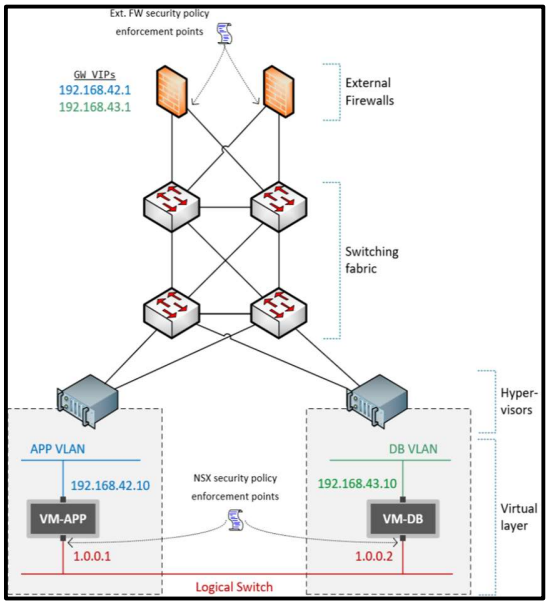

Figure 3: the entire structure of the suggested network environment ((Koskinen, 2020)

6. Scenario One: Secure network with conventional segmentation

A conventional implementation by segmenting the hosts into individual VLANs has been represented within Scenario 1, depending on security control and roles that allowed through the outer firewall device by routing of internal-VLANs. A policy of security has been applied where it is executed when traffic reached to the interfaces of the firewall (Koskinen, 2020).

Thus, the packets of the network required to pass over more than one physical and virtual component as illustrated in the following figure. In addition, the firewall within this scenario represents a bottleneck for traffic transmitted from one network to another and passing over it (Koskinen, 2020; Bala, 2023).

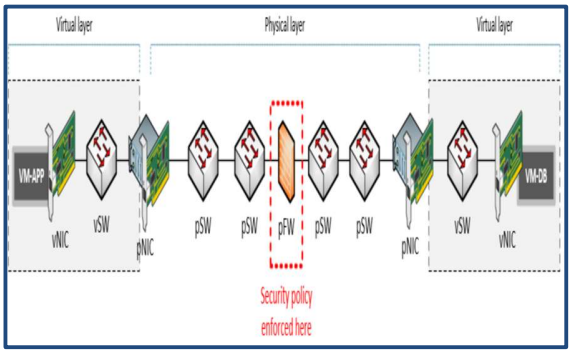

Figure 4: Path of network traffic in Scenario 1 (Koskinen, 2020).

The security within conventional network is established at the border or the edge to involve the south-north communication. Sub-sections and sections are created beside to firewall to extend the security. Therefore, any communication with the outer section entities should go over the firewall. Further, any outer or intersection communication that comes from every host within the section should access over departmental firewall and this will increase the delay and the traffic within the network (Bala 2023).

7. Scenario Two: Secure network with NSX micro-segmentation

The 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 un-routed segment of logical network has been used to connect all VMs within the network. In addition, the real policy of security has been enforced within the ports of virtual switch and only implemented on hypervisor hosts. Therefore, the micro-segmentation of VM level and the utilization of the basic flat structure of the network becomes enabled.

By this scenario, logical segments can be separated from security area thinking type and designed within more effective way. Moreover, when a shift within protection requirements is needed, the security policy can be simply modified in comparison with the re-structuring architecture of logical network (Koskinen, 2020).

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 the following figure. This data path topology was verified by NSX network trace tool. (Koskinen, 2020)

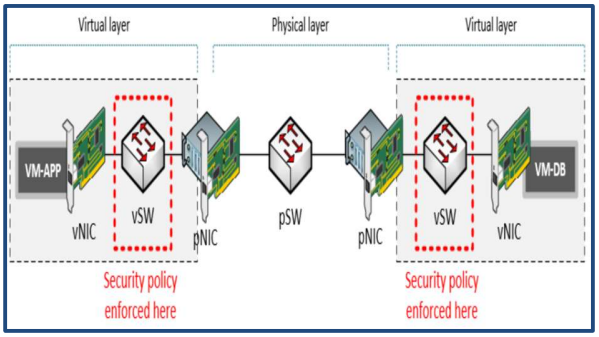

Figure 5: Path of network traffic in Scenario 2 (Koskinen, 2020)

8. The Suggested Scenario

VMware NSX can be considered as a security and networking platform that able to provide micro-segmentation through all the developed components involved within the recent center of data. In addition, micro-segmentation with NSX enhances the efficiency and the agility of the center of data as well as it is able to keep an agreeable posture of security at the same time (Holmes, 2016). Furthermore, NSX-T segmentation provides IT security with 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 (The Network DNA, 2021).

As shown in the previous sections, the second scenario with NSX micro-segmentation achieved enhanced performance than conventional segmentation in scenario 1. However, this scenario is not adequate to deal with large environments that involve multi-hypervisors and multiple clouds. Therefore, it cannot provide high level of security for large, sensitive and variant workloads. An enhanced environment has been suggested within 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 not only in virtualization layer. This product also makes operations within security and networking simpler. In addition, the suggested environment integrated NSX-T with Sky ATP and policy enforcer to enhance the performance and the security of the network. The integration between policy enforcement and threat detection secures the virtual and physical network environments. This integration is considered by the solution of “Juniper Connected Security (JCS)” which is composed of:

- An engine of threat detection: this is represented by a cloud relays on SKY ”Advanced Threats Prevention (ATP)” to detect recognized and unrecognized threats. Feed information is used from different sources to detect recognized threats while unrecognized threats are determined through different methods

like threat deception, machine learning and sandboxing.

— Central management of policies: this component based on policy enforcer which communicates with third-party appliances through the network and the appliances of Juniper Networks. By this policy inter- and intra-communications of network are visible.

Furthermore, the cloud relays on SKY ATP can be considered as a framework of security that aims to protect 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 below.

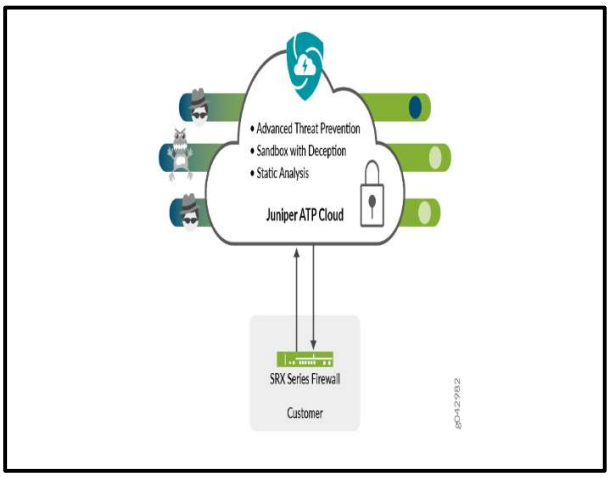

Figure 6: framework of cloud relays on SKY ATP.

A series of API connectors are also provided by the utilized policy enforcer for third-party switches or adaptors. These connectors are then used to integrate policy enforcer with NSX connector to allow the policy of infected host to be implemented at secure fabric. Further, the connectors of the NSX-T are composed of edge firewall that represents desired Secure Fabric and NSX-T Manager, which represents vCenter.

Two Tire gateways are used to connect segments of the network with the physical infrastructure. Each tire gateway is composed of two main components; Services router and distributed router. In addition, the series device (vSRX) has been used as edge firewall in order to transmit any suspected data traffic into Sky ATP. The logical topology of the suggested environment is shown in the figure below.

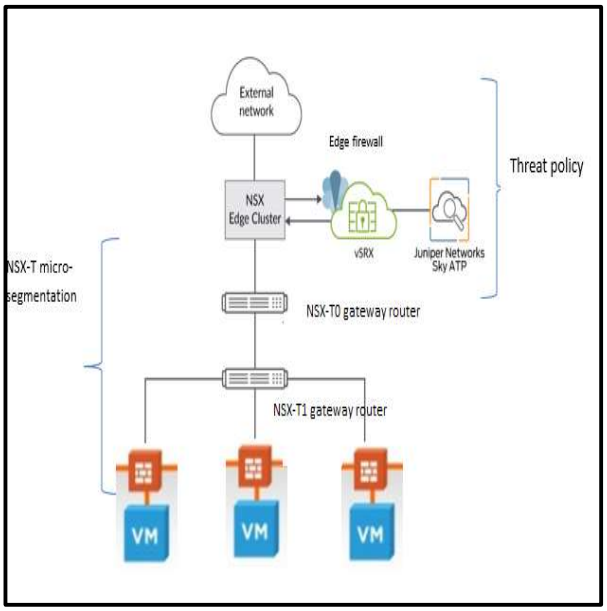

Figure 7: The logical topology of the suggested environment.

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

— Step one: If there is any infection discovered, then Policy enforcer will be informed by the infected addresses through Sky ATP.

— Step two: If Infected address pertains to NSX secure fabric, then Infected address list will be sent to the NSX connector through NSX API.

- Step three: the VM matching to the sent IP addresses will be retrieved by NSX service.
- Step four: SDSN_BLOCK security tag will be then created by NSX API to be tagged into a suitable VM.

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

9. Comparison

Segmentation technique and micro-segmentation have been both developed to secure and protect the network from various threats and attacks. However, conventional segmentation cannot solve all problems of network security. Therefore, micro-segmentation has been developed to solve these problems and to enhance the behavior of the network. Within this section, a comparison between the both techniques has been achieved based on the two scenarios that studied within the previous section.

Within the conventional network segmentation scenario, the network has been broken or segmented into several segments (VLANS). In addition, the network has been segmented depending on the north-south transferred traffic, which crossing the border of security and running among servers and clients. On the other hand, micro-segmentation within the second scenario placing every application or device within its particular logically separated segment and this enhances the control and the visibility within the network. Further, 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 the security of network have been 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 concerning on the internal security of traffic. Therefore, Scenario 2 provides the suggested environment with more enhanced security than Scenario 1. Further, the architecture of network may require re-architected from time to time, and this will be expensive, time-consuming and difficult through segmentation because it is based on the physical infrastructure breaking. However, this issue does not exist within the micro-segmentation and this will reduce time-consuming, complexity and the cost.

The insertion of micro-segmentation enhances the performance of the network by minimizing the amount of hair pinning. Further, there is no need for external hardware device (external firewall) within scenario 2 and this makes the path of traffic more suitable and shorter as well as enhancing the security of traffic and the environment. Thus, the performance of the network within scenario 2 is better than that within scenario one.

Furthermore, the implementation of micro-segmentation with kernel-based firewall and hyper-visor level provides security workload over virtualization clouds and platforms. Further, this implementation provides a 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&2) is not adequate to deal with large environments that involve multi-

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 outer threats can be detected by scenario 1 and inner threats can be detected by scenario 2. Therefore, the suggested scenario becomes to overcome those limitations.

The suggested scenario provides a high level of security by implementing NSX into segmented network and by the integration between the policy enforcer and Sky ATP. The inner threats (inside the network) and the 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, the security within this environment depends on policies, therefore it is simpler than security within hardware architectures. Further, 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 needed to subtract or add hardware devices.

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 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 virtualization platform rather than of a selected centralized network point.

The comparison between the Scenarios can be summarized by the following table:

Table 3: comparison between the Scenarios.

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

10. Conclusion

Due to the increasing number of threats and attacks that threatens the network during the recent years, novel methods and techniques have been improved to secure the infrastructure of the network and the data transmitted over its. Micro-segmentation and segmentation techniques are popularly used over computer networks to reduce the defensive versus cyber-attack. These two techniques have been used to enhance the performance and the security of the network. Two simple scenarios have been selected to investigate and highlight the distinctions between the implementation of conventional segmentation and the implementation of novel micro-segmentation approach. The environment has been segmented into four clusters: external firewall cluster, switching fabric cluster, hyper-visors

cluster and virtual layer cluster. VXLAN has been also introduced to perform a logical segmentation for VMs. Further, two databases and application roles VM have been used to represent the participants of test environment. However, these two scenarios are not adequate to deal with large environments that involve multi-hypervisors and multiple clouds. Therefore, it cannot provide a high level of security for large and variant workloads. An enhanced environment has been suggested within 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 not only in virtualization layer. This product also makes operations within security and networking simpler. The suggested scenario provides the highest level of security as compared with other two scenarios. The integration between the policy enforcer and Sky ATP within NSX-T micro-segmentation environment largely enhances the level of security. The inner threats and the outer threats 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, the security within this environment depends on policies, therefore it is simpler than security within hardware architectures. Further, 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 needed to subtract or add hardware devices.

Based on the achieved comparison, 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

- Simpson WR., and Foltz KE. Network Segmentation and Zero Trust Architectures. *Proceedings of the World Congress on Engineering, WCE 2021*, July 7-9, 2021, London, U.K.
- Deshpande AV. Introduction to Network Security. *International Journal of Computer Sciences and Engineering*, 2015, 3(9): 124-134
- Zhang N, An Introduction to Computer & Network Security Threats. *International Journal of Advance Research in Computer Science and Management Studies*, 2020: 5-10.
- Toivakka J. Network segmentation [Bachelor's thesis]. Degree Programme in Information and Communication Technology, 2017.
- Mhaskar N., Alabbad M., and Khedri R. A Formal Approach to Network Segmentation. Article in Computer & Security, 2021: 1-25.
- Wagner N., S¸ahin C S¸., Winterrose M., Riordan J., Pena J., Hanson D., and Streilein W W. Towards Automated Cyber Decision Support: A Case Study on Network Segmentation for Security. *IEEE Symposium Series on Computational Intelligence (SSCI)*. 2016.
- Ramesh K. Network Segmentation strategies to articulate a new method to Address Growing Information Security Concerns. IOSR Journal of Engineering (IOSRJEN). 2018, 8(6): 43-52
- Basta N., Ikram M., Kaafar M A., and Walker A.Towards a Zero-Trust Micro-segmentation Network Security

Strategy: An Evaluation Framework. *IEEE/IFIP Network Operations and Management Symposium*. 2022.

- Wagner, N., Sahin, C. S., Pena, J., Riordan, J., and Neumayer, S. Capturing the Security Effects of Network Segmentation via a Continuous-time Markov Chain Model. *In Proceedings of the 50th Annual Simulation Symposium*, 2017: 1—12.
- Soto J., and Miller L. Micro-Segmentation for Dummies. *John Wiley and Sons*, 2015, 68 pages.
- AbuAlghanam O, Qatawneh M, Al Ofeishat HA, Adwan O, Huneiti A (2017) A new parallel matrix multiplication algorithm on tree-hypercube network using iman1 supercomputer. Int J Adv Comput Sci Appl 8(12):201–205
- Peterson B. Secure Network Design: Micro Segmentation. GIAC (GSEC) Gold Certification, 2021: 1-23. https://sansorg.egnyte.com/dl/6p0mC8GPeQ
- Olzak T. VLAN network segmentation and security- chapter five. Management, compliance & auditing. INFOSEC. 2021. https://resources.infosecinstitute.com/topic/vlan-network-chapter-5/
- JUNIPER Network. IOT Network Segmentation. Engineering Simplicity. 2022: 1-4
- Alabbade M., and Khedri R. Dynamic Segmentation, Configuration, and Governance of SDN. Journal of Ubiquitous Systems & Pervasive Networks. 2011, 3(1): 1-16.
- Huang D., Chowdhary A., and Pisharody S. Microsegmentation: From Theory to Practice. ResearchGate, In book: Software-Defined Networking and Security (pp.155-180), 2018.
- Ekambaram S K., and Varun M. Microsegmentation: Defense in Depth. Dell Technologies Proven Professional Knowledge Sharing, 2021: 1-8.
- Bala P. Network Micro-Segmentation. SCRIBD. 2023. https://www.scribd.com/document/564160802/Network-Micro-Segmentation#
- Koskinen J. Microsegmentation as Part of Organization's Network Architecture Investigating VMware NSX for VSphere [Master's Thesis]. JAMK University of Applied Sciences. 2020.
- VMware. Microsegmentation using NSX Distributed Firewall: Getting Started. NCH Software. 2014. https://docplayer.net/15756686-Microsegmentation-using-nsx-distributed-firewall-getting-started.html
- Holmes W. Micro-segmentation Defined – NSX Securing "Anywhere" – Part I. VMware, 2016. https://blogs.vmware.com/networkvirtualization/2016/06/micro-segmentation-defined-nsx-securing-anywhere.html/
- Assunção P. A Zero Trust Approach to Network Security. Proceedings of the Digital Privacy and Security Conference. 2019: 65-72
- Turner J. 7 Network Segmentation Best Practices to Level-up Your Security. Strongdm. 2023. https://www.strongdm.com/blog/network-segmentation

- Nyamasvisva T E., and Mahmoud-Arabi A A. A Comprehensive SWOT Analysis For Zero Trust Network Security Model. International Journal of Infrastructure Research and Management. 2022. 10 (1): 44 – 53.
- Zenarmor. What is Network Segmentation? Introduction to Network Segmentation. Sunny Valley Cyber Security Inc. (d/b/a Zenarmor). 2023. https://www.zenarmor.com/docs/network-basics/network-segmentation
- Eidle D., Ni S Y., DeCusatis C., and Sager A. Autonomic security for zero trust networks. *Ubiquitous Computing Electronics and Mobile Communication Conference (UEMCON) 2017 IEEE 8th Annual*, 2017: 288–293.
- Hussein, A. L., Trad, E., & Al Smadi, T. (2018). Proactive algorithm dynamic mobile structure of Routing protocols of ad hoc networks. IJCSNS, 18(10), 86.
- DeCusatis, C., Liengtiraphan P., Sager A., and Pinelli M,. Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication. *2016 IEEE International Conference on Smart Cloud (SmartCloud)*. 2016: 5–10.
- Myers J. Network Security with Micro Segmentation from VMware. 2015. Available at: http://www.enpointe.com/blog/network-security-with-micro-seg-mentation-from-vmware
- Guardicore. Network Segmentation and Micro-Segmentation in Modern Enterprise Environments. White paper. 2019.
- FORTINET. Internal Segmentation Firewall Security Where You Need It, When You Need It. White paper. 2016
- The Network DNA. Introduction to MicroSegmentation in VMware NSX-T. 2021.https://www.thenetworkdna.com/2021/03/introduction-to-micro-segmentation-in.html