IMPLEMENTATION OF MICRO-SEGMENTATION OF A COMPUTER NETWORK TO IMPROVE NETWORK SECURITY

BY

ODEY, OYALOWO TOLUWANISE

17010301020

A PROJECT SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE AND MATHEMATICS, COLLEGE OF BASIC AND APPLIED SCIENCES, IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD DEGREE OF BACHELOR OF SCIENCE (B.SC.) IN COMPUTER SCIENCE

AUGUST, 2021

DECLARATION

I hereby declare that this project written by me and is a record of my own research work. It has not been presented in any previous application for a higher degree of this or sny other University. All citations and information derived from various sources has been duly acknowledged by a means of references provided.

____

ODEY, OYALOWO TOLUWANISE

____

Date

CERTIFICATION

This is to certify that the content of this project titled **'IMPLEMENTATION OF MICRO-SEGMENTATION OF A COMPUTER NETWORK TO IMPROVE NETWORK SECURITY'**, was carried out and submitted by **ODEY, OYALOWO TOLUWANISE** in partial fulfillment of the requirements for the degree of **BACHELOR OF SCIENCE IN COMPUTER SCIENCE**.

The original research work was carried out by her under my supervision and is hereby accepted.

______________________________ Signature/Date

Prof. I.O. Akinyemi

Supervisor

______________________________ Signature/Date

Dr. M.O. Adewole

Coordinator, Department of Computer Science and Mathematics

DEDICATION

This project is dedicated to The Almighty God, the giver of life and wisdom and to my lovely parents.

ACKNOWLEDGEMENTS

I am eternally grateful to Almighty God for providing me with the strength, knowledge, and bravery, as well as divine aid and provision, from the beginning to the end of this project. I specially appreciate my supervisor, Prof. I.O Akinyemi, for his guidance and support in ensuring the successful completion of this project work.

I express my gratitude to Mr Jeremiah Balogun, for his help and guidance. My heart-felt gratitude goes to the Head of Department, Computer Science and Mathematics – Dr. Adewole and all other members of staff of the department of Computer Science: Late Dr. Oyetunji M.O., Dr. (Mrs.) Kasali F.A., Dr (Mrs.) Oladejo Bola, Dr. (Mrs.) Oladeji F.A., Dr. (Mrs.) Igiri and Mr. Ebo I.O.

I am grateful for my lecturers' unwavering support, which has considerably aided my academic performance. I hope that God would continue to make them forces to be reckoned with in their fields of specialization, as well as that God will enhance their knowledge.

I will forever be grateful to my parents Mr. and Mrs. Ogri, for their moral, emotional, financial support, time and other resources for the sake of my success; and my siblings for their love and support. I also want to appreciate Mr. Michael from Dell for his insights and knowledge and to my fellow course mates Ololade Adesgaba, Oyedemi KingDavid and Ogundare Oluwatoyosi. Also, a big thank you to all my Mountain Top University colleagues and friends for their prayers and support, and help in one way or the other. God bless them all greatly.

ABSTRACT

The rise of hybrid-cloud data centers, as well as Virtualization has created an IT environment that is time-consuming and difficult to manage due to its ever changing state meaning breaches are more likely to occur and mitigating their impact is crucial. To address these shortcomings, this project discusses how Micro-segmentation based on the Zero Trust Model works by segmenting a network and identifying its components in order to protect it from attacks.

Micro-segmentation functions by securing environments, inter and intra application traffic within a data center to greatly protect it while preventing network intrusion and isolating threats if they should occur. The implementation was done using VMware HOL Labs to simulate the micro-segmentation process.

The study results in determining how to migrate and protect network resources using hypervisors with each of its virtual machines and individual components by involving the use of stateful firewalls while making analysis of traffic that moves in the cloud environment.

Then coming to a conclusion that using hypervisors is a great option at micro-segmentation which supports containerization and mobile workloads.

Keywords – *Data Centers, Hybrid-Cloud, Virtualization, Micro-segmentation, Hypervisor, Zero Trust, Stateful firewall, Containerization.*

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

1.0 Background of Study

Virtual Local Area Networks (VLANs) in the 90s were used to address the issue of broadcast storms. Broadcast storms are the result of a network's broadcast and multicast traffic accumulating. Network segmentation was made possible through the use of Firewalls and Access Control Lists (ACLs). Network segmentation is a data center protection technique that splits the network into subnetworks (subnets) in order to reduce the attack surface so network traffic can be more organized and contained (Ashe, 2016). Optimal firewalls and network security policies can be maintained across all data servers for many companies and businesses. However, this can be time-consuming and difficult to manage, and breaches are more likely to occur, therefore, minimizing their impact is very critical. Although, various network segmentation concepts have existed over the years, it is commonly referred to as a north-south network traffic management. This means that software and users are trusted as long as they are within a given network region. Such trust models may result in breaches, which is one of the main reasons that segmentation has grown with micro-segmentation within data centers and cloud environments.

Micro-segmentation is a method used to logically divide data centers and cloud environments into segments in order to isolate workloads from one another and secure them individually. The main advantage of micro-segmentation is that attackers who get access to one segment cannot migrate to other sections of the network.

Network administrators can use micro-segmentation to build policies that separate and protect each individual element while also minimizing network traffic between workloads based on a *Zero Trust approach*. The Zero Trust Approach is a security concept (Kindervag, 2010) which is based on strict identity verification process. According to this rule, only authenticated and authorized users and devices can access applications and data on a network. Basically, organizations should not automatically trust anything inside or outside its network/cloud assets and instead must verify anything and everything trying to connect to its systems before granting access. The Zero Trust approach simply comes down to not trusting anyone.

The growth of hybrid-cloud data centers and virtualization has resulted in a dynamic and difficult-to-secure IT infrastructure. As a result, micro-segmentation is quickly becoming a security best practice for companies operating in such volatile environments. This technology has a wide range of applications such as zone segmentation, application isolation and service restriction. Individual workload levels can be rendered safer against future attacks from risky cyber-criminals and hackers by developing and applying a micro-segmentation or security segmentation plan. Micro-segmentation will reduce the likelihood of data exportation and malicious attacks with the correct architecture and deployment (Chickowski, 2019).

1.1 Statement of the problem

The rise in technology has resulted in innovative cybercriminals who can hack their way into nearly any server or data center. The latest security breach that occurred in July, 2020 on Twitter, where hackers broke into a number of verified accounts of popular users like Bill Gates, Jeff Bezos and Elon Musk.

To bring it close to home, in a recent survey by Sophos Group plc, a British security software and hardware company, reported that 86 percent of Nigerian businesses were victims of cyberattacks in the year 2019. The second highest proportion recorded internationally after India, and far higher than the 64 percent reported in South Africa (Paul, 2020). This indicates that most Nigerian businesses have been victims of different types of cyberattacks such as malware, ransomware, and data breaches in the last year.

Traditional network segmentation has a growing issue such that it is better at managing North-South traffic flows (client-server interactions) in and out of the data center, which is troublesome in the hybrid-cloud environment, where 75 to 80 percent of network traffic flows East-West (server-to-server) between applications (Chickowski, 2019).

Therefore, there is a need for network micro-segmentation in order to reduce and restrict unauthorized access to data centers or cloud assets as cyber threats are continuously adapting and hackers are discovering ways to do damages to enterprises of all kinds.

1.2 Aim and Objectives

The aim of this project work is to segment networks into micro-networks to prevent potential attacks by cyber criminals and also to determine if hypervisor micro-segmentation supports container and mobile workloads.

This aim will be achieved through the following objectives:

i. Identify the component of the existing network.

ii. Specify the design of the proposed micro-segmentation

iii. Deploy the micro-segmentation.

1.3 Methodology

In order to fulfill the goal of this project research, the micro-segmentation will fall into different phases:

Design and Project plan: The design document and project plan will address classification of end users, business applications and IT resources, a complete initial security policy, automation required for bulk installation, workflows and internal processes that may need to be tweaked to accommodate the new security model, Pre-production preparation, sequence in which applications will be protected.

Creating and application of security policies: Based on the analysis of the traffic flow patterns and relationships, security policies will be defined that incrementally open up specific communication channels between workloads, as needed. Define which users should have access to which information.

Micro-Segmentation Solution Installation and Configuration: The implementation can begin by logically grouping assets such as applications, servers, datasets, or people after establishing boundaries, important assets, authorized communications, and access levels and then installing and configuring the micro-segmentation tools and related infrastructure.

1.4 Scope and Limitation

This project work will be focused on the hypervisor micro-segmentation deployment instead of a complex host based micro-segmentation of a data center due to time constraints and limited resources. This work will investigate different techniques, various solution software that can be used for deployment and the issues and limitations relating to a successful Micro-segmentation implementation.

1.5 Significance of Study

This project work is done mainly due to the need for companies, organizations and businesses in Nigeria to secure their data centers and hybrid cloud assets in order to reduce the impact of data breaches in their network. The benefits of micro-segmentation entails:

- Increased Overall Data Security: Through segmenting networks, you can help secure the most sensitive data you have on your network infrastructure and track network activity at the same time.

- Stronger regulatory compliance: Regulatory officers can create polices that isolate systems that are subject to regulations from the rest of the infrastructure.

- Hybrid Cloud Environment Management: Through simple workflows, risk evaluation, and security policy management, micro-segmentation dynamically migrates device access and creates a single security policy.

1.6 Definition of terms

ACL – Access Control Lists (ACL) are permission-based systems that assign people in an organization different levels of access to files and information.

VLAN – Virtual Local Area Network (VLAN) separates an existing physical network into multiple logical networks. As a result, each VLAN sets up its own broadcast domain. The only way for two VLANs to communicate is through a router that is linked to both.

Firewall - A firewall is a network security system that filters traffic and prevents outsiders from obtaining unauthorized access by monitoring and controlling incoming and outgoing network traffic based on preset security rules.

Cyber-attacks- A cyberattack is any attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage or steal data within the systems or network.

Data Center- This is a physical location where businesses store important applications and crucial components such as routers, switches, firewalls, storage systems, servers, application-delivery controllers, and data. A data center's architecture is based on a network of computer and storage resources that allows for the distribution of shared applications and data.

Subnet (Subnetwork) - This is a logical subdivision of a network.

VMware NSX - VMware NSX is a network virtualization platform that lets you create virtual networks on your real network and within your virtual server environment. It provides the network with the operating model of a virtual machine.

CHAPTER TWO

LITERATURE REVIEW

2.0 INTRODUCTION

The concept of a modern data center is changing and evolving at a rapid pace. The shift from physical to virtual workloads, transition to software-defined data centers, the emergence of a multi-cloud environments etc., are all causing a constant evolution in technology. There is an underlying issue of typically organized security remaining inadequate even in traditional, static data centers.

According to Check Point Nigeria (2016) which is the largest global pure-play cybersecurity vendor, Nigeria is one of the world's most vulnerable countries to cyber-attacks, placing 16th in the world in 2016. In 2018 alone, about 60% of Nigerian firms suffered an attack and about $270 million was spent on cybersecurity. Most Nigerian companies hardly report data breaches and they rarely share information with each other when they happen.

Without a versatile approach to security and risk management that changes to the rise of emerging technological ideologies, security and risk management will remain stagnant. Realized threats raises an organization's attack surface as innovative compute technology is implemented, making it more vulnerable to innovative cyber criminals.

Therefore, the need for micro-segmentation arises to reduce and restrict unauthorized access to data centers or cloud assets as cyber threats are continuously adapting and hackers are discovering ways to do damages to enterprises of all kinds.

2.1 NETWORKING

In an information system, computer networking, is the process of transmitting and exchanging data between nodes across a common channel. The design, building, and usage of a network are all part of networking, as is the administration, maintenance, and operation of the network infrastructure, software, and policies (Scarpati, 2018). Devices and endpoints can be linked to each other on a local area network (LAN) or to a larger network, such as the internet or a private wide area network (WAN). This is a necessary feature for service providers, enterprises, and consumers all across the world to share resources, utilize or give services, and communicate. Everything from phone conversations to text messaging to streaming video to the internet of things (IoT) is made easier by networking (Scarpati, 2018).

2.1.1 Network Security

Your network and data are protected by network security from breaches, invasions, and other dangers. This is a broad and all-encompassing word that refers to hardware and software solutions, as well as procedures, policies, and settings pertaining to network use, accessibility, and overall threat prevention and protection. A sophisticated combination of physical devices, such as routers, firewalls, and anti-malware software programs, is required to secure a network (LaBounty, 2021).

Network security is critical for both personal and commercial networks. Most houses with high-speed internet have one or more wireless routers, which may be hacked if not adequately protected. Data loss, theft, and sabotage may all be reduced with a good network security solution (LaBounty, 2021).

2.2 INTRODUCTION TO DISTRIBUTED FIREWALLS

Traditional firewalls are becoming obsolete due to increased Internet connectivity. End-to-end encryption, as well as other protocols, pose a threat to this type of firewall. The notion of a "distributed firewall" has been proposed to remedy these flaws.

2.2.1 Traditional Firewalls and Their Issues

To implement traffic filtering, traditional firewalls rely on constrained topology and regulated network access points. Traditional firewalls are unable to filter internal traffic and hence cannot defend networks from assaults from within (Bellovin, 2000). Conventional firewalls normally function on a single computer and monitor traffic on the same network as the computer, however as network connection expands, such as extranets, high-speed lines, numerous entry points, and telecommuting, traditional firewalls face a few of the following challenges:

i. Internal assaults are not protected by firewalls; the only solution is to build numerous firewalls within internal networks, dividing the network into smaller networks and protecting them from each other. Because separate policies must be implemented to various firewalls, the administrative burden and complexity rise (Wan, 2002).

ii. Because of the substantially increased Internet connectivity, this approach has become outdated. Extranets and outside telecommuters are permitted to access all or parts of internal networks. Meanwhile, when encrypted tunnels are not in place, the machines of telecommuters who utilize the Internet for connectivity require security. Currently, the majority of such telecommuters connect to their companies' internal networks over a VPN tunnel. If the VPN tunnel is being used for general Internet browsing, it is not only wasteful, but it may also be against the organization's policies They either expose a security vulnerability or add to the strain of running several personal firewalls in different places if they do not use the VPN channel (Chowdhary, 2018).

iii. Unauthorized entry points are able to get over the firewall's protection. Anyone may now easily create a new, illegal network entry point without the knowledge or agreement of the network administrator. Individuals can build backdoor access that bypasses all of the security features offered by typical firewalls using various types of tunnels, wireless, and dial-up access techniques.

2.2.2 Distributed Firewalls

Firewalls have become congestion spots as internet access speeds have increased and the number of compute-intensive protocols that firewalls must evaluate has increased. Steven Bellovin, an AT&T researcher, suggested a "distributed firewall" to overcome the difficulties of traditional firewalls while preserving their benefits. *A Distributed Firewall* is a type of host-resident security software that protects the corporate network’s servers and end-user computers against malicious software by inspecting not just north-south traffic but east-west traffic and enforcing security at a granular level. It is made up of a number of host-resident firewalls that are centrally configured and maintained (Wan, 2002). In this architecture, the security policy is still defined centrally, but it is implemented at each endpoint (hosts, routers, etc.). The centralized policy specifies the types of connections that are authorized (Barracuda, 2021). Then this policy is distributed to all endpoints, where it is enforced. Each individual host in a distributed firewall is responsible for enforcing policy. Because we are no longer restricted by topology, the security administrator—who is no longer necessarily the "local" administrator—defines the security policy in terms of host IDs (Bellovin, 1999).

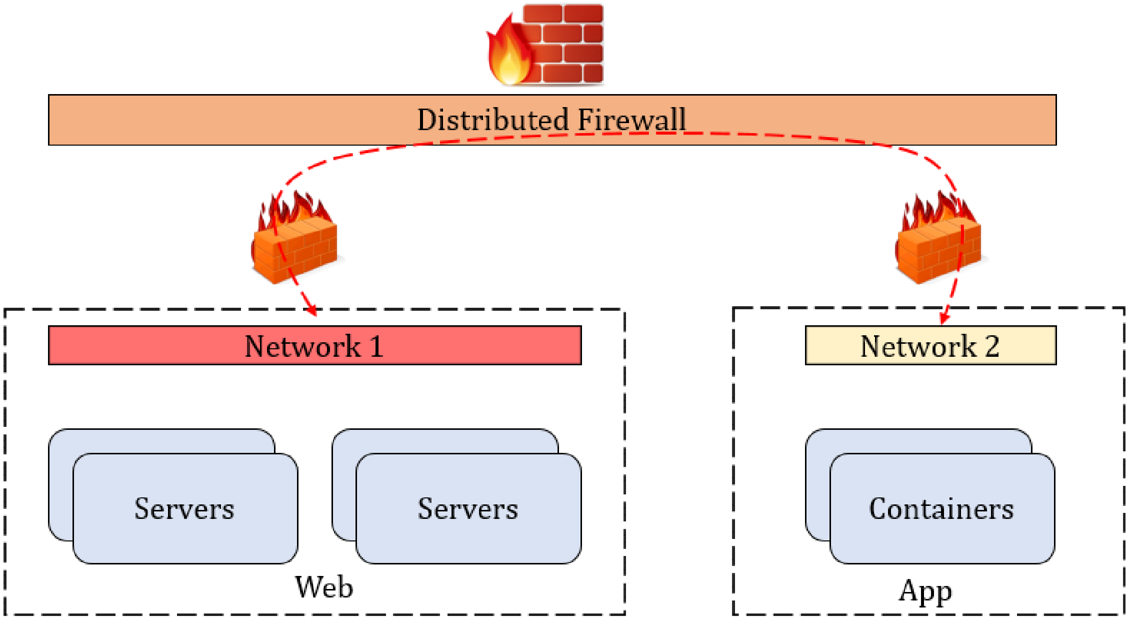


Figure 2.1 Distributed Firewall

According to Daniel Wan, Distributed Firewalls consists of the following necessary components:

1. A security policy language
2. A policy distribution scheme
3. An authentication and encryption mechanism such as IPsec.

The *security policy* language specifies which connections are authorized and which are not. It should support credentials as well as many sorts of apps. After the policy has been compiled, it is distributed to endpoints. The *policy distribution scheme* should ensure the policy's integrity throughout transfer. Before processing incoming or outgoing communications, this policy is considered. The distribution of the policy might vary depending on the execution. It can be immediately delivered to end systems, pulled as necessary, or even supplied to users in the form of credentials that they use when attempting to interact with the hosts.

Topology is used by traditional firewalls. Hosts are recognized by their IP addresses and network interfaces on the firewalls to which they are connected, such as "inside," "outside," and "DMZ." This type of construction is extremely frail. It is feasible that distributed firewalls will utilize IP addresses to identify hosts. However, a secure method is preferable. To identify hosts, it is preferable to use a certificate. Cryptographic certifications are provided by *IPsec*. These certificates have the potential to be highly trustworthy and unique identifiers. Unlike IP addresses, which are easily faked, digital certificates are far more secure, because certificate ownership cannot be easily falsified. Furthermore, they are not affected by topology.

2.2.3 Importance of Distributed Firewalls

The Distributed firewall does not completely eradicate the use of traditional firewalls but serves as an extra solution for certain new difficulties that occur when dealing with the complexities of maintaining a secure network in a corporate context. The capacity for Distributed Firewalls to maintain internal and external security, coupled with the theoretically infinite growth properties, make them a helpful tool for IT security (Betts, 2018).

2.2.4 Advantages of Distributed Firewall

Outlined below are a few of the advantages of Distributed Firewall:

i. Topology Independence

Telecommuters who use the Internet for general purposes as well as to tunnel into a business network are now better secured. Previously, they had to utilize “triangle routing” to tunnel into the business's network for generic Internet traffic, or they were not protected if they were not tunneled, which was a security breach for both the computer and the organization (Chowdhary, 2018).

ii. Prevention from Internal Attacks

Since distributed firewalls no longer enforce topology restrictions, hosts are no longer vulnerable to internal attacks. To the host, there is no distinction between "internal" and "external" networks. When a computer powers up, the policy is applied to all inbound and outgoing traffic. The hosts may also be recognized by their encrypted certificates, which removes the possibility of identity faking (Bellovin, 1999)

iii. Hosts Make Better Decisions

Conventional firewalls frequently lack sufficient understanding of what a host desires. Furthermore, many firewalls are set up to pass TCP packets from the outside world with the “ACK” flag set. Because they believe these packets are responses to the internal hosts that initiated the discussion. Unfortunately, this is not always the case, and faked ACK packets can be exploited as part of "stealth scanning." Similarly, traditional firewalls are incapable of properly handling UDP packets because they cannot distinguish between packets that are replies to outbound queries (and thus legal) and packets that are incoming attacks (Wan, 2002).

iv. Elimination of Single Point of Failure

To enforce rules, a conventional firewall requires a single access point. It not only creates a single point of failure, but it also restricts the entire network's performance to the firewall's speed. These issues are completely eliminated with the deployment of distributed firewalls. Performance, reliability, and availability are no longer dependent on a single computer, or in certain circumstances a collection of machines (s). In contrast, the host that initiates the conversation or sends out the queries knows exactly what packets it is expecting and what is not, because it has enough knowledge to determine whether an incoming TCP or UDP packet is legitimate and, in the case of end-to-end encryption, it has the necessary key. The same is true for protocols such as FTP (Stepanek, 2001).

2.3 NETWORK VIRTUALIZATION

The shift to virtualized data centers with the adoption of technologies such as Software Defined Networking (SDN) and Software Defined Data Center (SDDC) enables the intelligence of the data center infrastructure to move from hardware to software (Jaworski, 2017). Because SDN abstracts the control plane from the data forwarding plan in separate networking devices, a network becomes more flexible and easier to administer (Jaworski, 2017). SDN's agility enables more comprehensive granular zoning, allowing networks to be separated into microsegments.

The second technology being Software Defined Data Center (SDDC) also called a virtual data center effectively offers infrastructure services provided in the data center in a software-driven environment rather than traditional hardware making it easier to deploy micro-segmentation. The SDDC approach has been established by many of the largest, most active and efficient data centers in the world, including Google, Facebook and Amazon (VMware, 2014).

Network Virtualization makes it possible to create, provision and manage networks all in a software container and managed independently of the hardware serving as a simple packet-forwarding backplane (virtu, 2016). The software produces a network overlay that can run separate virtual network layers on top of the same physical network layer. Network Virtualization can combine or divide multiple physical networks or one physical network into one virtual, software-based network or separate, independent virtual networks.

2.3.1 How Network Virtualization works

Network virtualization separates network services from the underlying hardware, allowing for the virtualization of a complete network. Physical network resources, such as switching, routing, firewalling, load balancing, virtual private networks and more are combined together and delivered in software and require only Internet Protocol (IP) packet forwarding from underlying physical network. Network virtualization is designed to enhance administrator productivity, efficiency, and job satisfaction by automating many of these activities, masking the real complexity of the network. (Gillis, 2019).

2.3.2 Network Virtualization Forms

There are two types of virtual networks: internal and external. Both words apply to the inside and outside of the server. External virtualization can combine one or more networks into virtual units using technologies such as switches, routers, or a network. Internal virtualization refers to device containers on a single network host that provide network-like capabilities. Internal software enables virtual machines (VMs) to exchange data on a host without the use of an external network. A virtual LAN is an example of network virtualization (VLAN). A VLAN allows a group of devices from different networks to be merged into a single logical network (Gillis, 2019).

2.4 ZERO TRUST APPROACH

The Zero Trust Approach is a strategic cybersecurity model that was created in 2010 by John Kindervag at Forrester Research Inc. The main objective is to drastically diminish the risk of cyber-attacks in an enterprise by not trusting anything that tries to connect to an organizations' systems.

A secure perimeter is the foundation of traditional network security. Anything inside the perimeter can be trusted, but anything outside can't, however, since networks are fluid the cloud era, perimeter security is no longer appropriate. When you use your device to connect to a business network, the data passes through a mobile tower of Wi-Fi network, as well as several servers before reaching the network. If one of those servers is down your device is infected with a virus or a malicious program, or a hacker has gained access to your Wi-Fi, the perimeter defense could let them in the network (Virtu, 2020).

As today's technology has become and is becoming more complex by digital transformation and advancements, it is very necessary to reduce the risk and mitigate the damage of breaches, a Zero Trust network regards all traffic as untrusted, limiting access to important company data and resources to the greatest extent feasible.

2.4.1 Technologies behind Zero Trust

This framework's implementation incorporated advanced technologies such as multifactor authentication, Identity and Access Management (IAM), Identity Protection and Next-generation Endpoint Security to confirm a user's identity and retain system security.

i. Multifactor Authentication is an encryption technology that requires users to prove their identity in two or more methods of authentication before given access to accounts, applications or information. Examples of authentication factors include hardware tokens which are commonly small thumb drives or keycards, one-time passcodes (OTPs) for SMS, software tokens, biometric factors etc.

ii. Identity and Access Management (IAM) is a framework used in enterprises to track and manage the actions and roles of users without having to log into each application as an administrator while controlling user access to critical information.

iii. Next-generation Endpoint Security is a modern method of detecting threats by integrating real-time analysis such as Artificial Intelligence and Deep Learning of user and system behavior to analyze executables and file-less threats. Traditional signature-based antivirus is incapable of keeping up with current threats, and by the moment they do, it is too late. That's where Next-Generation Endpoint Security comes in, flawlessly detecting when a program or a user infiltrates the database, changes its name, or opens an unauthorized connection outside the firewall. (Goldstein, 2021).

Next-generation endpoint Security solutions push out instant updates to users' endpoints, allowing agency IT security administrators to swiftly ban IP addresses, update malware signatures, and spot new adversary techniques, allowing for rapid detection of emerging threats. (Goldstein, 2021).

2.5 IMPLEMENTATION APPROACHES TO MICRO-SEGMENTATION

Because it lets security teams see and control east-west traffic, micro-segmentation has emerged as a useful technique for combating lateral risks. Micro-segmentation reduces the attack surface to a minimum and introduces access controls to isolated segments, enabling organizations to monitor and control traffic to each segment. There are three primary approaches to micro-segmentation. These vary depending on which network layer is used for implementation.

i. Network-Based Micro-Segmentation:

Network based micro-segmentation makes use of network devices like switches, routers and load balancer as enforcement points. It relies on VLANs, subnets, firewalls or some other tagging technology to divide the network into segments. This approach is primarily used for North/South network traffic. Micro-segmentation solutions are constrained by the scope the vendor's network device, i.e., they cannot be applied to cloud platforms or data centers that use devices from another network equipment vendor (Cohen, 2017). A few problems with this approach being that it creates macro-segmentation which is the breaking up of a network into multiple discrete chunks to support business needs instead of micro-segmentation and is also very expensive to implement (Friedman, 2017).

ii. Hypervisor-based Micro-Segmentation

A hypervisor is a piece of hardware, software, or firmware that can create virtual computers, manage them, and assign resources to them. Software-defined data centers with virtual workloads are increasingly becoming the norm in modern data centers. As all the workload traffic must travel via the hypervisor, network isolation and micro-segmentation may be performed there and this solution takes advantage of the hypervisor firewall’s ability to offer visibility and micro-segment workloads (Cohen, 2017).

iii. Host-based Micro-Segmentation

Micro-segmentation rules may be put into hosts when they are deployed and then remain with the workloads independent of location or duration. This is especially helpful for mobile and temporal workloads. Managing policy and enforcement rules for hundreds or thousands of workloads rather than a few centralized networks or hypervisors can be difficult with host-based technology (Oltsik, 2018).

2.5.1 How is Security Configured with Micro-segmentation?

Security is configured via micro-segmentation depending on apps and their workloads, where these workloads are utilized, and the data these workloads require access to. Security policies can be configured such that if a task attempts to operate in violation of the policy's rules, its network access is terminated. This feature can be extended all the way down to the process level, providing for even more granular network security. Micro-segmentation is most effective for traffic moving between servers and the apps that access them. As a result, it is excellent for data centers and cloud platforms (Carklin, 2020).

2.5.2 Levels of Micro-Segmentation

There are several cases where it makes sense to go from coarse-grained to fine-grained segmentation over time. Here, different levels of micro-segmentation is discussed.

•**Application Micro-Segmentation:** Categorizing application modules simplifies some management tasks but creates target-rich zones for attackers so restriction of east-west connections protects high-value programs that deliver critical services, contain sensitive data running on bare metal servers, virtual machines, or containers (Imperva, 2021).

•Environmental Segmentation

Separates development, testing, and production environments. This prohibits communication across environments, which is usually unnecessary in regular operations but might be abused by an attacker. Traditional measures cannot achieve this level of segmentation because environments are dispersed across multiple data centers, both on-premises and in the cloud (Friedman, 2017).

• Tier-level and Server Segmentation

When an application has numerous tiers, such as a web server, application server, and database, segmenting each tier and isolating it from the others is beneficial especially when each tiers need to interact in places with adjacent tiers. This stops attackers from migrating across application levels, particularly between external-facing tiers such as the web server and back-end systems such as the database (Illumio, 2021).

• Process based Segmentation

Also called a Nano-segmentation, this is a very fine-grained segmentation that works at the process or service level. A single software service, for example, can be isolated and only interact across network pathways, protocols, and ports that have been expressly approved giving the administrators the ability to implement policies without compromising security or application functionality (Givati, 2018).

2.6 ISOLATION

Whether for compliance, containment, or the separation of development/test/production environments, isolation is the backbone of network security. Traditionally, isolation and multi-tenancy were established and enforced using ACLs, firewall rules, and routing policies. Support for such features comes standard with micro-segmentation.

Using VXLAN technology, virtual networks (i.e., Logical Switches) are L2 segments that are by default separated from other virtual networks as well as the underlying physical infrastructure, offering the security concept of least privilege. Virtual networks are formed in isolation and stay such unless they are deliberately linked. There is no need for physical subnets, VLANs, ACLs, or firewall rules to achieve this isolation.

2.6.1 Containment

It is not enough to merely identify the threat; it must also be controlled to the greatest extent feasible while the analysis is carried out. This is where using an allowlisting / least privilege paradigm to achieve micro-segmentation becomes a vital part of the architecture. Only the authorized communications between known systems are allowed when allowlisting / least privilege is enabled, while other combinations are banned. By default, lateral movement between unrelated computers is forbidden, making the attack's spread throughout the data center considerably more difficult (Holmes, 2017).

When something goes wrong, threat analysis tools send out an alarm. Once the type of an attack has been determined, some technologies go one step further and update security devices with new rules in order to counteract the danger. In the meanwhile, numerous systems will most certainly be infiltrated, with the possibility of data exfiltration in an environment that is not micro-segmented (Kumar, 2017).

Allowlisting / least privilege models begin by fingerprinting the application in order to determine how and where it interacts. This list is used to create a ruleset that allows only communication between certain parts while prohibiting all other communication. This method allows you to know exactly what should be permitted and monitored, so a simple "deny" statement becomes a catch-all for all other options (Holmes, 2017).

Once the data has been collected, a security group may be formed to offer the precise context required to construct an allowlisted / least privilege policy model. This eliminates the need to monitor all traffic and separate specific flows for each application, ensuring that only permitted traffic flows or is monitored.

2.7 HYPERVISORS

Server virtualization enables several operating systems to execute independent applications on the same server while sharing the same physical resources. These virtual machines enable system and network managers to have a dedicated computer for each service that must be operated (Bisht, 2021).

A host machine is the one on which a hypervisor is installed, as opposed to *guest virtual machines* that operate on top of it. The hypervisor is a hardware virtualization technique that allows several guest operating systems (OS) to operate on a single host computer at the same time. A virtual machine manager is another name for a hypervisor. (Simic, 2019).

2.7.1 Types of Hypervisor

• Type-1 Hypervisor

A “bare-metal or native hypervisor” is a Type 1 hypervisor that operates directly on the physical hardware of the host computer. The Type 1 hypervisor isn't required to load an operating system. Virtualization is easier with direct access to the underlying hardware and no extra software to worry with.

Direct-on-physical-hardware hypervisors are also extremely secure. Because each guest has its own OS, virtualization reduces the danger of attacks that target OS security weaknesses and vulnerabilities. This guarantees that an attack on a guest VM is logically isolated and cannot propagate to other VMs on the same hardware (Bigelow, 2021).

A typical Type 1 hypervisor may virtualize workloads over hundreds of CPU cores and many terabytes of RAM. In addition, Type 1 hypervisors frequently offer software-defined storage and networking, which gives virtualized workloads more security and mobility (Kirsch, 2021).

•Type-2 Hypervisor

Typically, a Type 2 hypervisor is placed on top of an existing operating system. Because it relies on the host machine's pre-existing OS to manage calls to CPU, memory, storage, and network resources, it's also referred to as a *hosted hypervisor*. As a result, Type 2 hypervisors are often not utilized in data centers and are instead reserved for client or end-user systems (also known as client hypervisors) where speed and security are less of a concern. They're most common in setups with a limited number of servers, and they're also less expensive than Type 1 hypervisors, making them an excellent test platform when compared to production virtualized systems or the cloud (Simic, 2019).

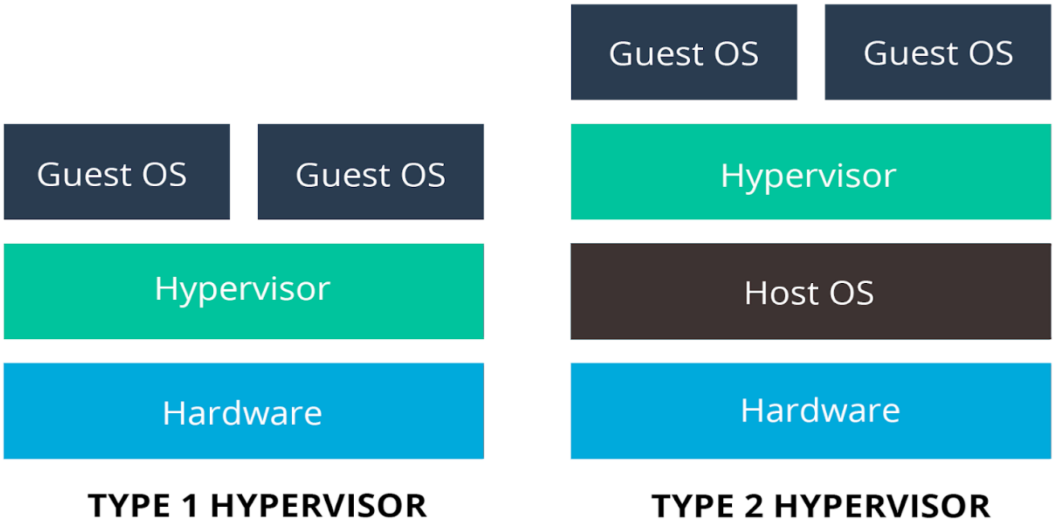


Figure 2.2 Hypervisor Types

2.8 Review of Related Works

This section discusses the numerous works on Micro-Segmentation, which covers network virtualization and data segmentation and allows direct east–west connectivity between server workloads through a virtual switch, minimizing east–west traffic hops and improving application efficiency.

Jaworski (2017), proposed that Micro-segmentation provides extra protection but is not a substitute for conventional security measures, suggesting that Micro-segmentation is an additional layer of security that allows to continue reducing the attack surface for east west network traffic. To meet the requirements of the Forester Research's "Zero Trust Approach," network micro-segmentation is required for all systems regardless of location.

Oltsik (2018), discussed how Micro-segmentation is becoming more mainstream, and many businesses are turning to micro-segmentation technologies. However, deciding which micro-segmentation technology to use can be difficult. Infrastructure, hypervisor, and host-based micro-segmentation architectures are three options that security professionals often consider based on micro-segmentation technologies.

Cohen (2018), explained that without knowing how systems interact, an organization cannot implement micro-segmentation. With the increasing number of attacks within the data center and cloud—malware, insider threats, or even malicious users exploiting technology or communications vulnerabilities—strong micro-segmentation techniques can't be applied until the operations and protection provide good visibility on how they want to see their systems interact so they can find out what could be interacting easily.

VMware (2014), highlighted how businesses and government IT organizations are adopting SDDC to virtualize computing, network, and storage, automate provisioning, and reduce time-to-market for IT applications and services. They also simplify and de-risk infrastructure transfers, additions, and modifications. This new business model offers several extra advantages. Micro-segmentation has been recognized as a best practice method in terms of security, but it has proven challenging to implement in traditional systems. For the first time, the NSX platform's inherent security and automation features make micro-segmentation operationally possible in the enterprise data center.

Chowdhary (2018), Illustrated that the transition from traditional firewall to modern micro-segmentation approaches using software-defined and virtual networking approaches. The enabling technique of micro-segmentation is due to the significantly improved capacity of networking devices and servers’ hardware supporting both virtualized networks and software security appliances.

CHAPTER THREE

METHODOLOGY

3.0 Introduction

In order to fulfill the goal of this project, the installation of NSX Public Cloud Gateway (PCG) will be deployed and validated in the public cloud environments, Microsoft Azure and Amazon AWS. Security polices will also be defined on the on-premises data center for the workloads that will be managed by VMware NSX. NSX is a distributed firewall that uses logical grouping to ease configuration and ensure consistency. The Central Management Plane which consists of the NSX Manager and NSX Cloud Services Manager would have been deployed on the on-premises data center.

3.1 Define and Secure Environments.

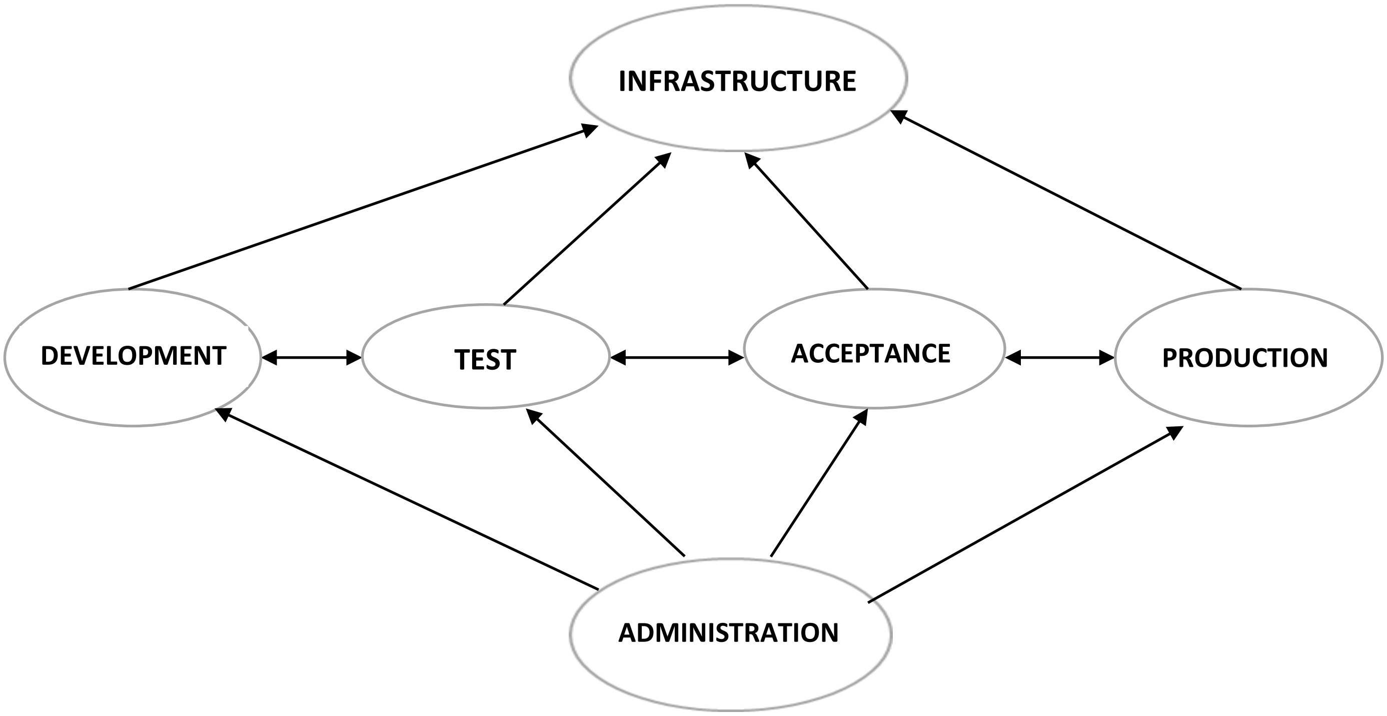


Figure 3.1 Defining Environments

This contains regulations for emergency situations, systems management, and infrastructure traffic. To do this, the environment can be defined in a simple way like Test, Development, Acceptance, and Production. Infrastructure group which is used within almost all organizations, usually consists of only one set of machines that service DNS, NTP and other infrastructure functions to all environments alike. Virtual machines are separated into environments and designed such that no traffic moves between them until it is absolutely essential.

3.1.1 Define and Secure Inter-application traffic

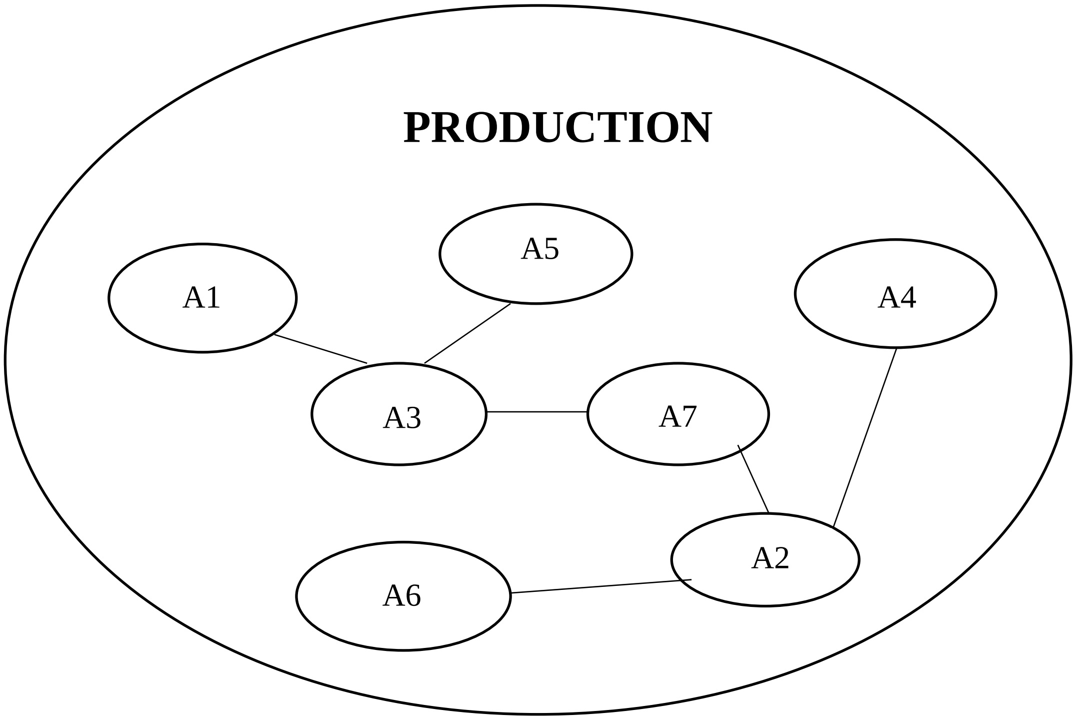


Figure 3.2 Defining Inter-application traffic

This has to do with specifying an application as a whole as well as which virtual machines are included. The next step is to specify that all traffic inside the application is permitted, but traffic from one application to another is permitted only if it is required for the application's proper operation.

3.1.2 Define and Secure Intra-application traffic

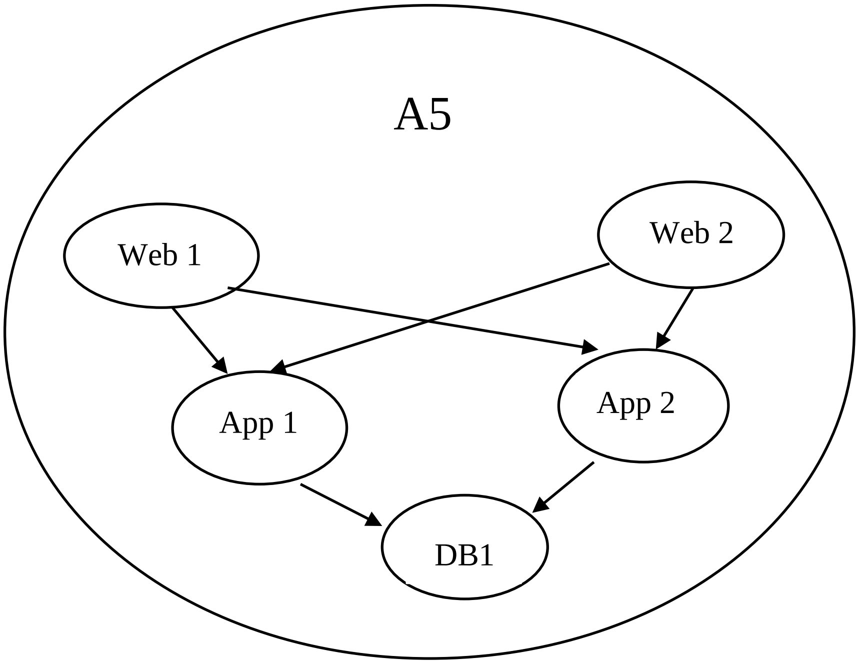


Figure 3.3 Defining Intra-application traffic

Traffic from one component inside the application to other components is defined once inter-application traffic has been established in rules. Here we are defining which traffic is permitted from each application component to other components.

3.2 Public Cloud Gateway

This is a public cloud local control plane that is in charge of gathering public cloud inventory. Public cloud service providers can be used as off-site extensions of on-premises data centers, allowing for the archiving of cold data from local storage to the cloud for longterm storage and backup data to the cloud. The storing of dormant data that is rarely utilized or accessed is referred to as cold data storage. Cold data is often kept for a long time, if not permanently, for business or regulatory considerations (Zeeshan, 2019). The NSX Public Cloud Gateway is installed in both public clouds (AWS and Azure) to demonstrate NSX Cloud's multi-cloud management capabilities.

3.3 Firewall Rules

Distributed stateful firewalling reduces the attack surface within the data center perimeter. A distributed system provides for a data plane that scales with the computational infrastructure, providing for per-application security and visibility. Application Level Gateways (ALGs) may be implemented with per-workload granularity and providing security enforcement in the public cloud because of statefulness. This implements access control at the VM level, avoiding the need for traffic to pass through the logical switch/router.

3.4 Security Group

Inbound and outbound traffic are controlled by a security group, which acts as a virtual firewall for your instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC can be allocated to a separate set of security groups.

3.5 Virtual Machines

Workload virtual computers can be configured with up to two (2) communication flows between them, each of which can be allowed or stopped separately.

CHAPTER FOUR

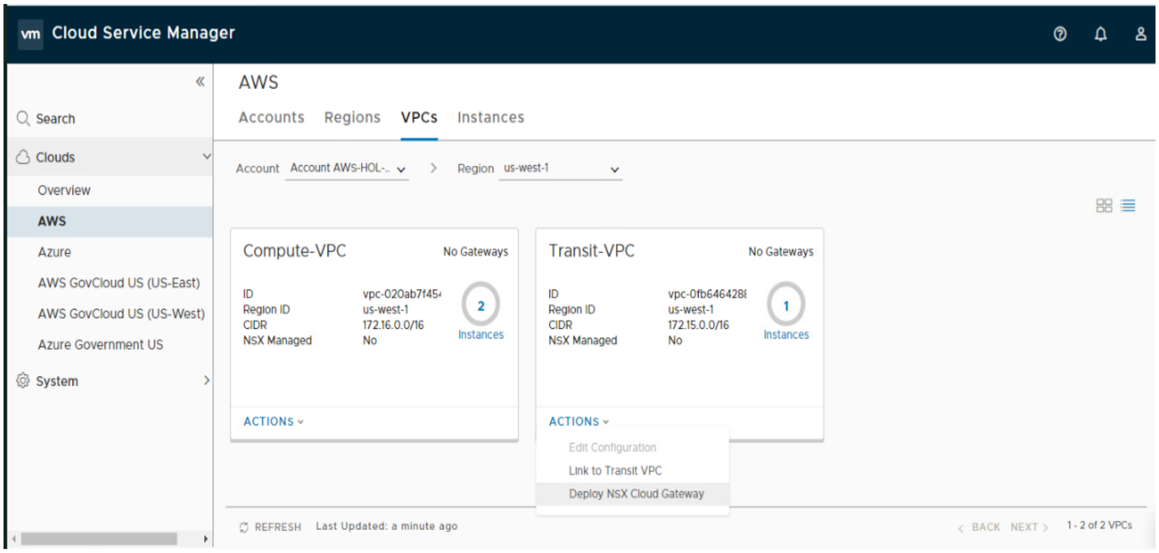
IMPLEMENTATION DETAILS

4.1 Implementation Environment

This research project uses the VMware Hands-on Lab as a testing and simulation environment. VMware Network Insight which is a VMware product is used to build an optimized, highly available, and secure network infrastructure across multi-cloud environments. Customers may use VMware NSX Cloud to design and administer Networking and Security rules that are consistent across native and hybrid cloud environments, from on-premises data centers to native AWS and Azure workloads or information technology applications and services

4.2 NSX Cloud Service Manager Setup in AWS

After opening the Cloud Service Manager (CSM) web interface, necessary Amazon Web Services (AWS) accounts were added and AWS EC2 was verified.



Account Account AWS-HOL-.. Region us-west-1

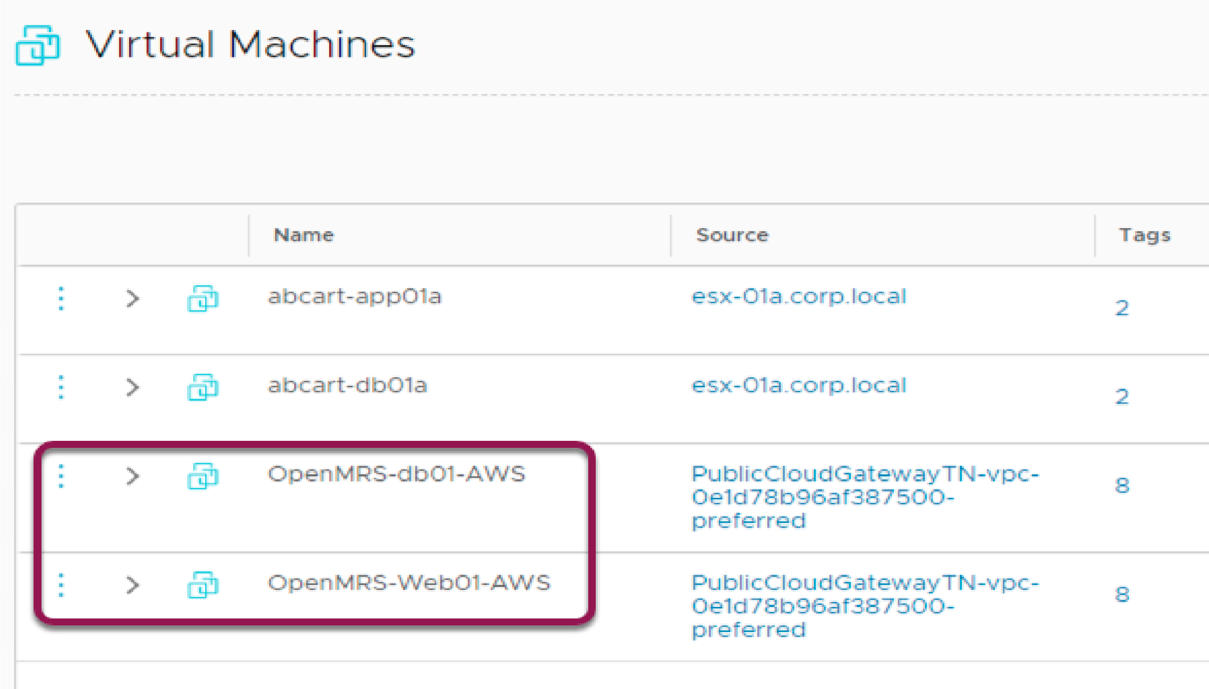
Compute-VPC No Gateways
ID vpc-020ab7f45
Region ID us-west-1
CIDR 172.16.0.0/16
NSX Managed No
2 Instances

Transit-VPC No Gateways
ID vpc-0fb646428
Region ID us-west-1
CIDR 172.15.0.0/16
NSX Managed No
1 Instances

Last Updated: a minute ago

1 - 2 of 2 VPCs

Figure 4.1 AWS VPC



Virtual Machines

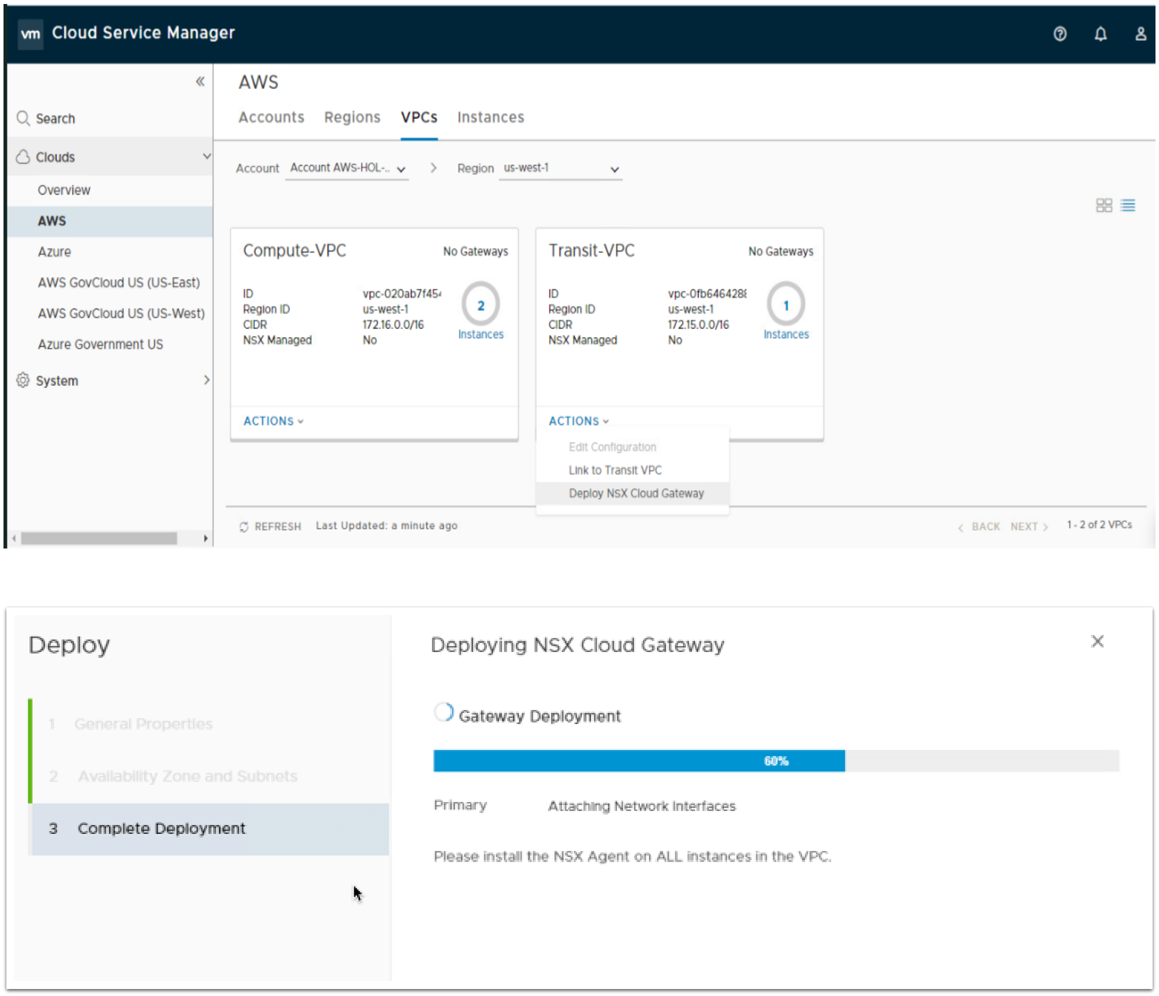
	Name	Source	Tags
	abcart-app01a	esx-01a.corp.local	2
	abcart-db01a	esx-01a.corp.local	2
	OpenMRS-db01-AWS	PublicCloudGatewayTN-vpc-0e1d78b96af387500-preferred	8
	OpenMRS-Web01-AWS	PublicCloudGatewayTN-vpc-0e1d78b96af387500-preferred	8

Figure 4.2 AWS EC2 Instances

An EC2 instance is a virtual server in Amazon's Elastic Compute Cloud (EC2) that is used to execute applications on the Amazon Web Services (AWS) architecture. It enables corporate subscribers to run application programs in a computing environment. The EC2 may function as an almost limitless number of virtual computers.

4.2.1 NSX Cloud Gateway Setup in AWS

Before deploying the gateway, the AWS Subnets settings are reviewed to note their availability zones. The Transit VPC Cloud Gateway is then deployed after modifying the Configuration settings which takes about 7- 10 minutes.



Account: Account AWS-HOL-.. Region: us-west-1

Compute-VPC — No Gateways
ID: vpc-020ab7f45
Region ID: us-west-1
CIDR: 172.16.0.0/16
NSX Managed: No
2 Instances

Transit-VPC — No Gateways
ID: vpc-0fb646428
Region ID: us-west-1
CIDR: 172.15.0.0/16
NSX Managed: No
1 Instances

Last Updated: a minute ago
1 - 2 of 2 VPCs

Deploying NSX Cloud Gateway

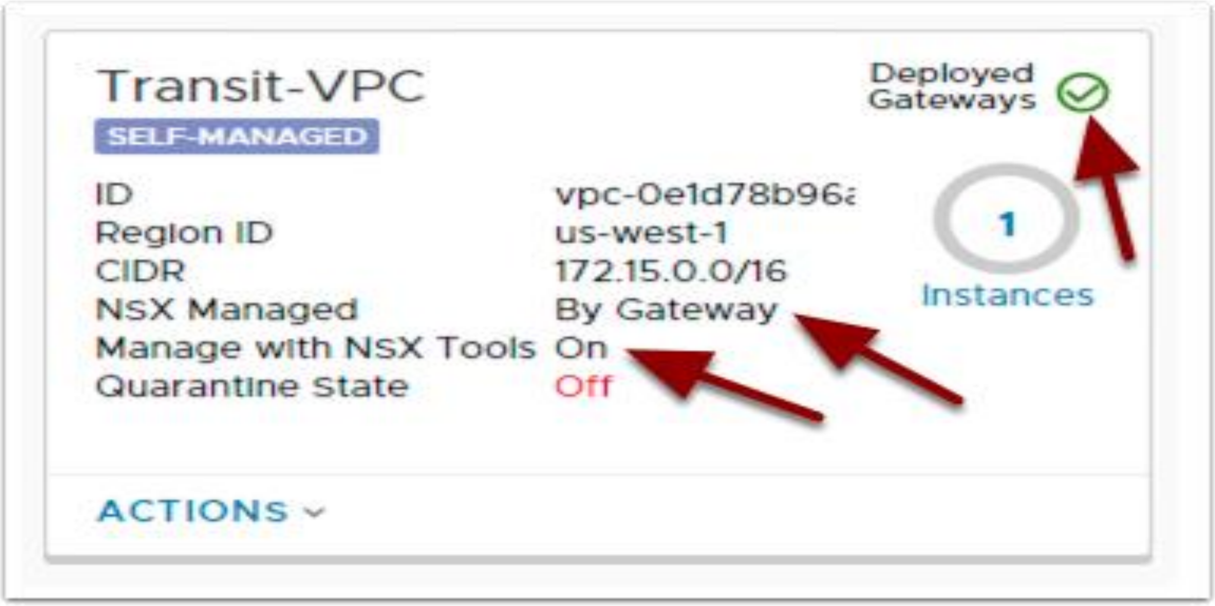
Gateway Deployment 60%

Primary: Attaching Network Interfaces

Please install the NSX Agent on ALL instances in the VPC.

Figure 4.3 Deployment in progress

Deployment of the NSX Cloud Gateway provides the local control plane for NSX policies in this VPC.


Transit-VPC

SELF-MANAGED

ID	vpc-0e1d78b96a
Region ID	us-west-1
CIDR	172.15.0.0/16
NSX Managed	By Gateway
Manage with NSX Tools	On
Quarantine State	Off

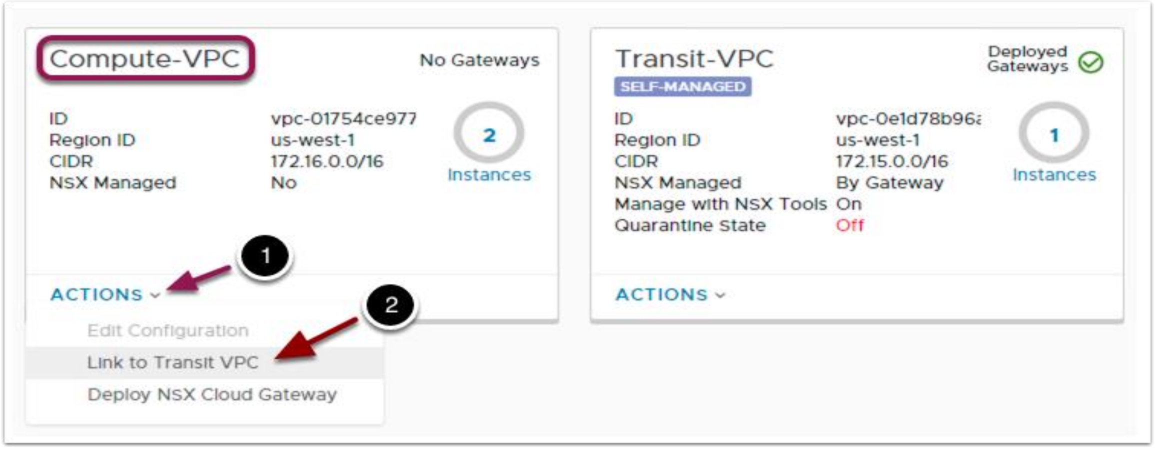
Figure 4.4 Deployment Successful

VPC is now marked as "green", "Self-managed" and displays "Deployed Gateways".

4.2.2 Linking VPC's

By linking VPCs, a user can route traffic between them using private IPv4 or IPv6 addresses.

Instances on each PC can communicate as though they are on the same network.


Compute-VPC

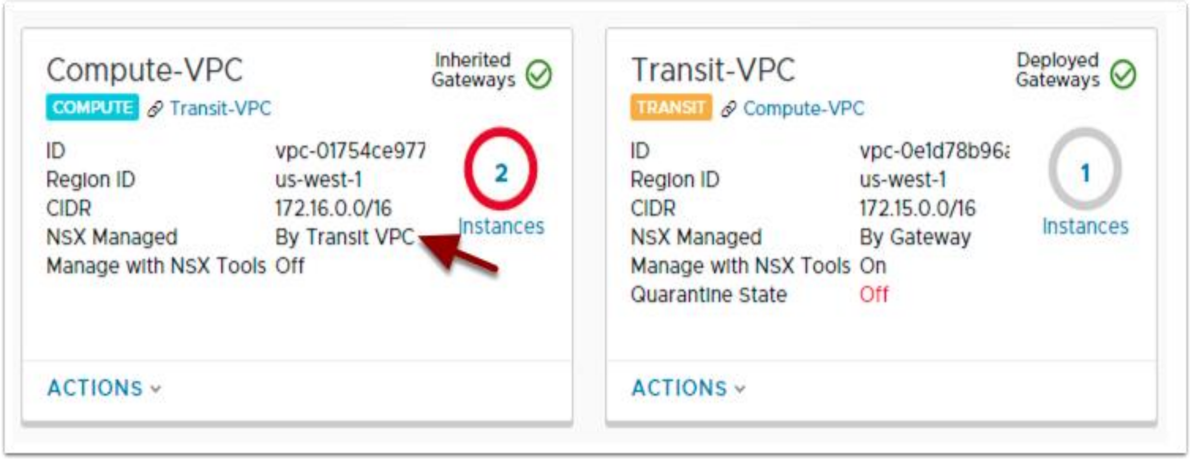
ID	vpc-01754ce977
Region ID	us-west-1
CIDR	172.16.0.0/16
NSX Managed	No

Transit-VPC

SELF-MANAGED

ID	vpc-0e1d78b96a
Region ID	us-west-1
CIDR	172.15.0.0/16
NSX Managed	By Gateway
Manage with NSX Tools	On
Quarantine State	Off

Figure 4.5 Link VPC



Compute-VPC — Inherited Gateways ✓

COMPUTE · Transit-VPC

ID	vpc-01754ce977
Region ID	us-west-1
CIDR	172.16.0.0/16
NSX Managed	By Transit VPC
Manage with NSX Tools	Off

Transit-VPC — Deployed Gateways ✓

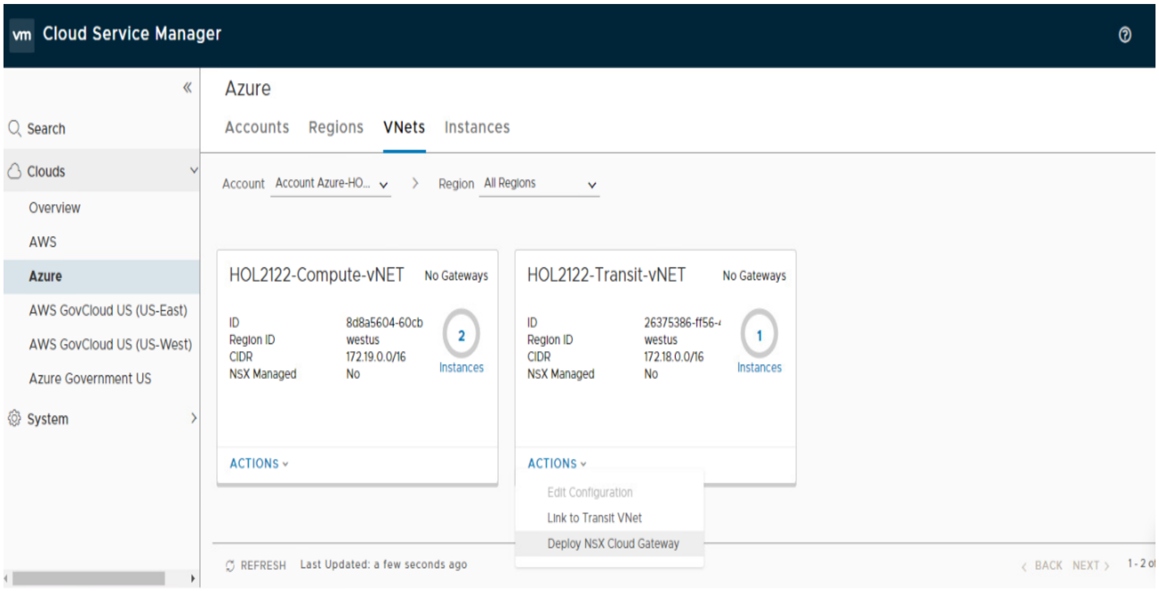
TRANSIT · Compute-VPC

ID	vpc-0e1d78b96
Region ID	us-west-1
CIDR	172.15.0.0/16
NSX Managed	By Gateway
Manage with NSX Tools	On
Quarantine State	Off

Figure 4.6 VPCs have been linked

4.2.3 NSX Cloud Gateway Setup in Azure

The same process implemented in AWS is also used in deploying the cloud gateway in Azure.



Account: Account Azure-HO... Region: All Regions

HOL2122-Compute-vNET — No Gateways

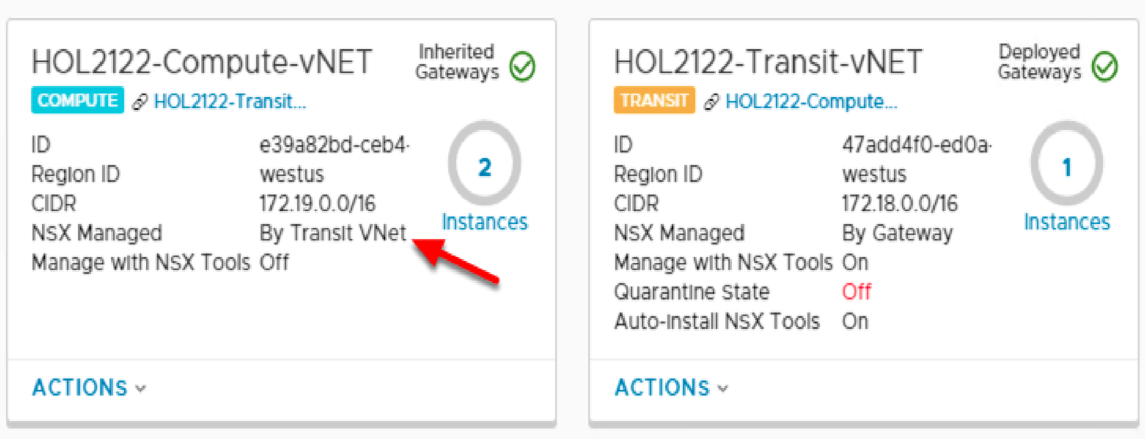
ID	8d8a5604-60cb
Region ID	westus
CIDR	172.19.0.0/16
NSX Managed	No

HOL2122-Transit-vNET — No Gateways

ID	26375386-ff56-
Region ID	westus
CIDR	172.18.0.0/16
NSX Managed	No

Last Updated: a few seconds ago

Figure 4.7 AZURE vNET

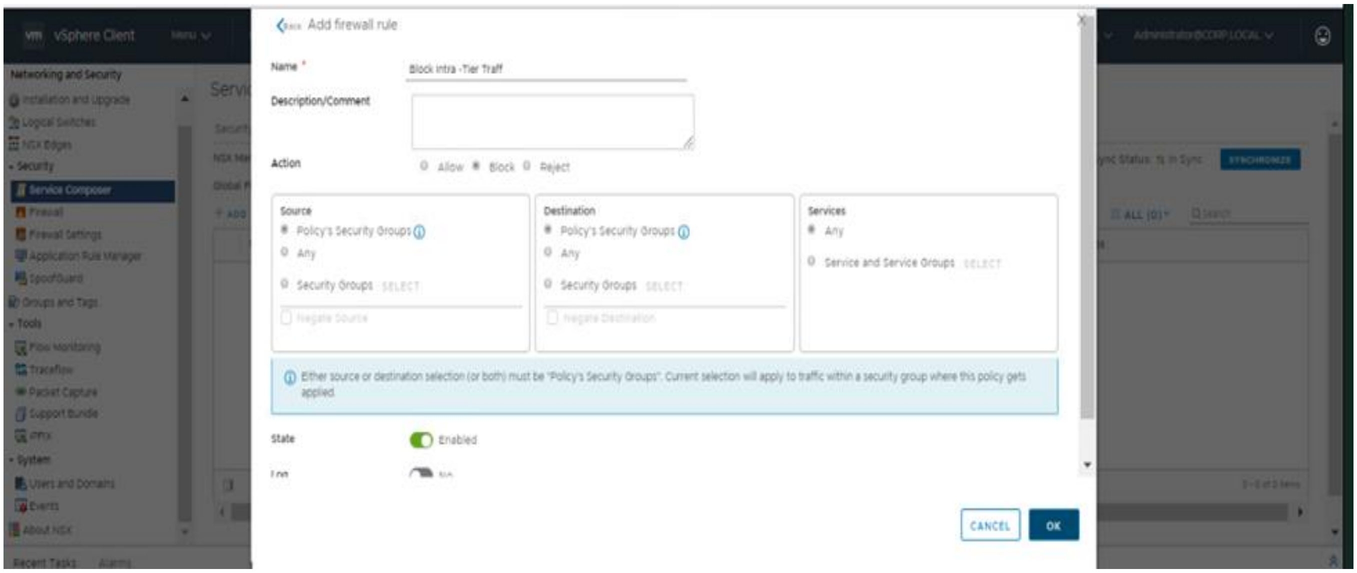

HOL2122-Compute-vNET
Inherited Gateways ✓
COMPUTE HOL2122-Transit...
ID e39a82bd-ceb4-
Region ID westus
CIDR 172.19.0.0/16
NSX Managed By Transit VNet
Manage with NSX Tools Off
2 Instances
ACTIONS

HOL2122-Transit-vNET
Deployed Gateways ✓
TRANSIT HOL2122-Compute...
ID 47add4f0-ed0a-
Region ID westus
CIDR 172.18.0.0/16
NSX Managed By Gateway
Manage with NSX Tools On
Quarantine State Off
Auto-Install NSX Tools On
1 Instances
ACTIONS

Figure 4.8 The Transit vNET has been deployed and linked together.

4.3 NSX Distributed Firewall

NSX Distributed firewall (DFW) is a stateful firewall that enforces security for workloads in the public cloud, resulting in micro-segmentation.



Add firewall rule

Name * Block intra -Tier Traff

Description/Comment

Action ○ Allow ● Block ○ Reject

Source
● Policy's Security Groups
○ Any
○ Security Groups SELECT
□ Negate Source

Destination
● Policy's Security Groups
○ Any
○ Security Groups SELECT
□ Negate Destination

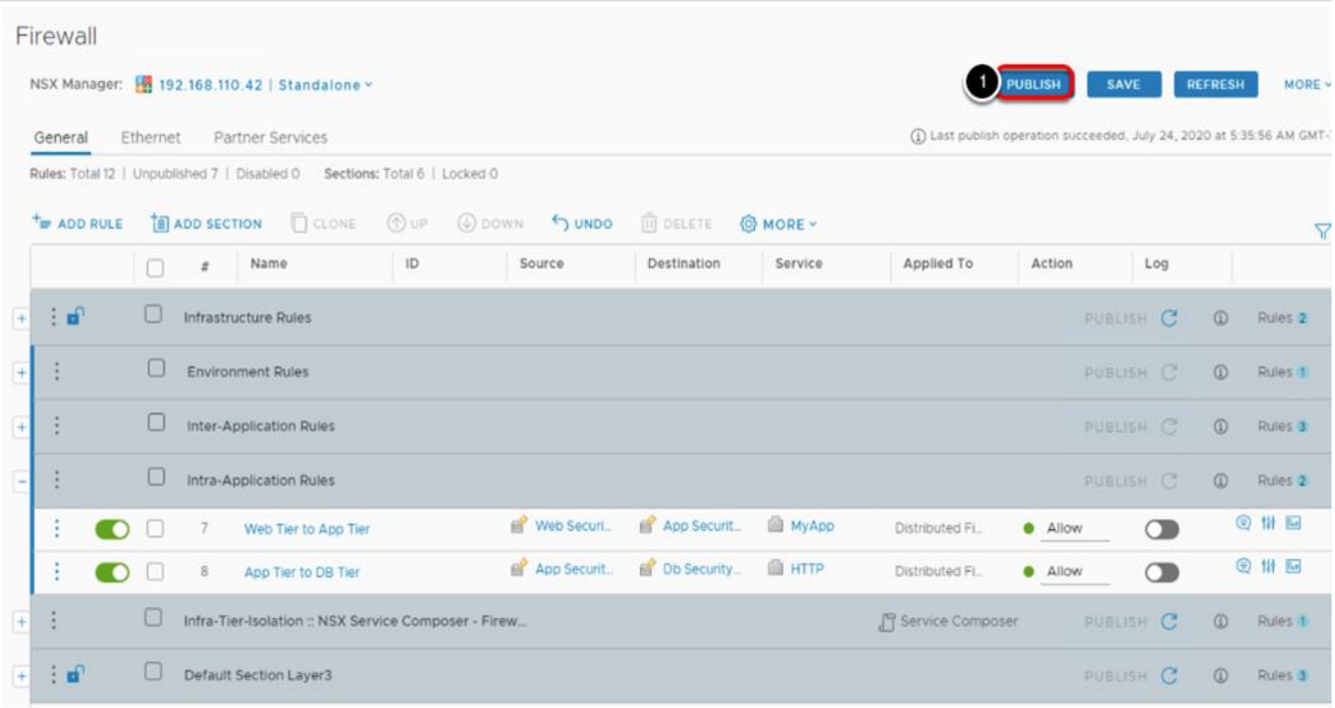
Services
● Any
○ Service and Service Groups SELECT

Either source or destination selection (or both) must be "Policy's Security Groups". Current selection will apply to traffic within a security group where this policy gets applied.

State Enabled

Log No

Figure 4.9 Adding DFW Rules



Firewall

NSX Manager: 192.168.110.42 | Standalone

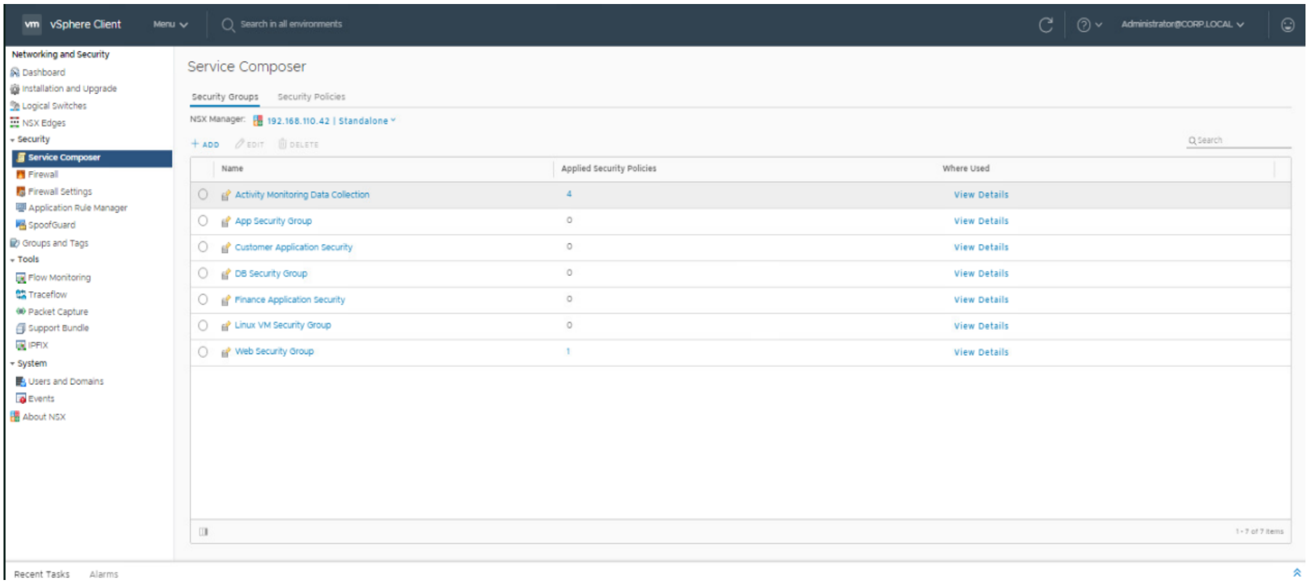
Last publish operation succeeded, July 24, 2020 at 5:35:56 AM GMT-

Rules: Total 12 | Unpublished 7 | Disabled 0   Sections: Total 6 | Locked 0

#	Name	ID	Source	Destination	Service	Applied To	Action	Log	
	Infrastructure Rules							PUBLISH	Rules 2
	Environment Rules							PUBLISH	Rules 1
	Inter-Application Rules							PUBLISH	Rules 3
	Intra-Application Rules							PUBLISH	Rules 2
7	Web Tier to App Tier		Web Securi...	App Securit...	MyApp	Distributed Fi...	Allow		
8	App Tier to DB Tier		App Securit...	Db Security...	HTTP	Distributed Fi...	Allow		
	Infra-Tier-Isolation :: NSX Service Composer - Firew...					Service Composer		PUBLISH	Rules 1
	Default Section Layer3							PUBLISH	Rules 3

Figure 4.10 Published Firewall Rules

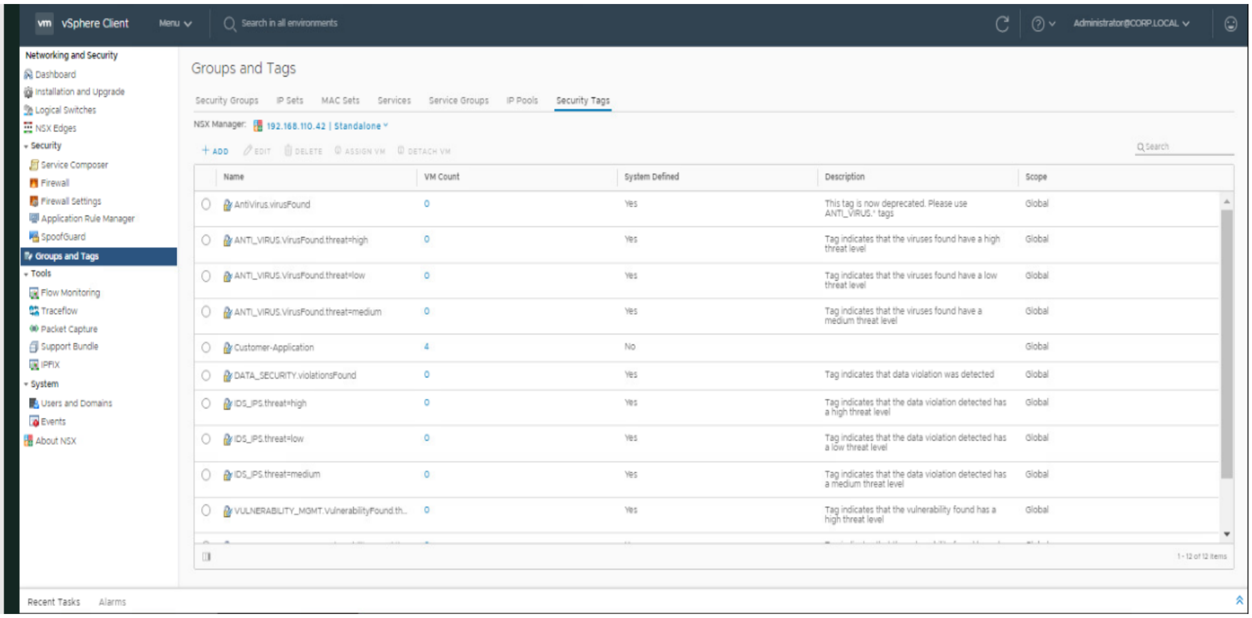
Now that all Firewall Rules have been established, they may be published and confirmed. All traffic between the environments is prohibited with the exception of pinging it.



Name	Applied Security Policies	Where Used
Activity Monitoring Data Collection	4	View Details
App Security Group	0	View Details
Customer Application Security	0	View Details
DB Security Group	0	View Details
Finance Application Security	0	View Details
Linux VM Security Group	0	View Details
Web Security Group	1	View Details

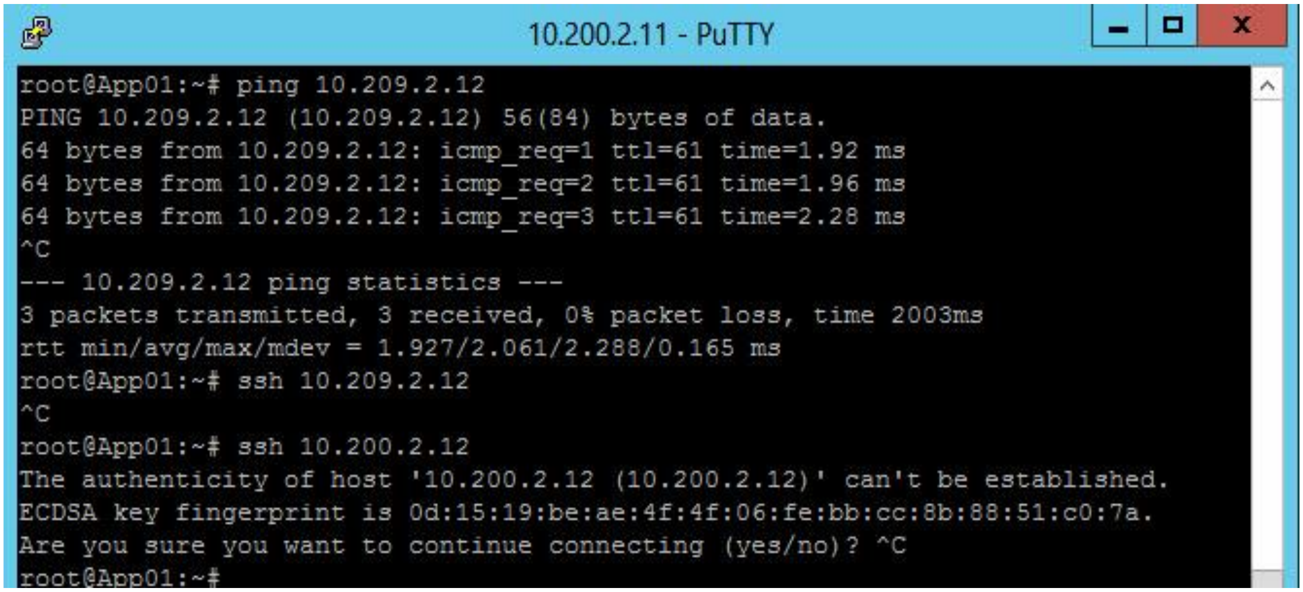
Figure 4.11 Security Groups on vSphere Client

This ensures all the rules applied takes effect in all virtual machines which are part of the selected group and tags.



Name	VM Count	System Defined	Description	Scope
AntiVirus.virusFound	0	Yes	This tag is now deprecated. Please use ANTI_VIRUS.* tags	Global
ANTI_VIRUS.VirusFound.threat=high	0	Yes	Tag indicates that the viruses found have a high threat level	Global
ANTI_VIRUS.VirusFound.threat=low	0	Yes	Tag indicates that the viruses found have a low threat level	Global
ANTI_VIRUS.VirusFound.threat=medium	0	Yes	Tag indicates that the viruses found have a medium threat level	Global
Customer-Application	4	No		Global
DATA_SECURITY.violationsFound	0	Yes	Tag indicates that data violation was detected	Global
IDS_IPS.threat=high	0	Yes	Tag indicates that the data violation detected has a high threat level	Global
IDS_IPS.threat=low	0	Yes	Tag indicates that the data violation detected has a low threat level	Global
IDS_IPS.threat=medium	0	Yes	Tag indicates that the data violation detected has a medium threat level	Global
VULNERABILITY_MGMT.VulnerabilityFound.th...	0	Yes	Tag indicates that the vulnerability found has a high threat level	Global

Figure 4.12 Verified Security Tags



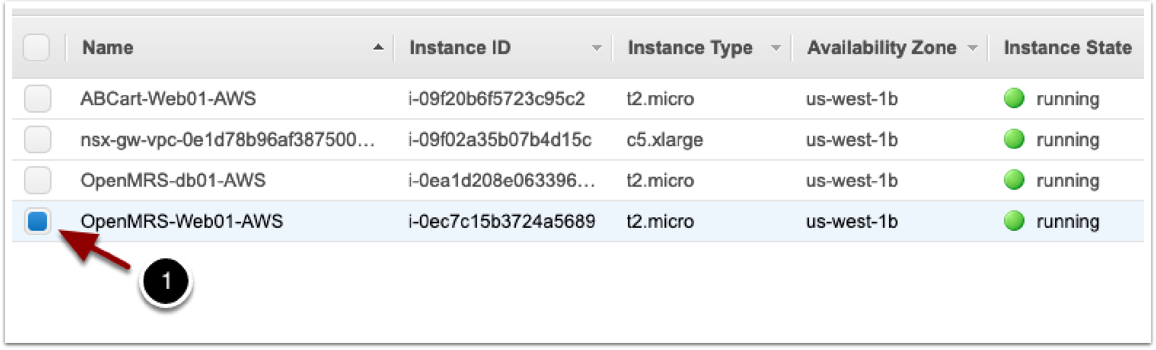
```
root@App01:~# ping 10.209.2.12
PING 10.209.2.12 (10.209.2.12) 56(84) bytes of data.
64 bytes from 10.209.2.12: icmp_req=1 ttl=61 time=1.92 ms
64 bytes from 10.209.2.12: icmp_req=2 ttl=61 time=1.96 ms
64 bytes from 10.209.2.12: icmp_req=3 ttl=61 time=2.28 ms
^C
--- 10.209.2.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.927/2.061/2.288/0.165 ms
root@App01:~# ssh 10.209.2.12
^C
root@App01:~# ssh 10.200.2.12
The authenticity of host '10.200.2.12 (10.200.2.12)' can't be established.
ECDSA key fingerprint is 0d:15:19:be:ae:4f:4f:06:fe:bb:cc:8b:88:51:c0:7a.
Are you sure you want to continue connecting (yes/no)? ^C
root@App01:~#
```

Figure 4.13 Network Ping

This is a ping from one of the Production environment's application servers to one of the Development environment's application servers. This is permissible. The virtual machines secured in one environment are blocked off from the virtual machines in another environment, regardless of how the network is connected.

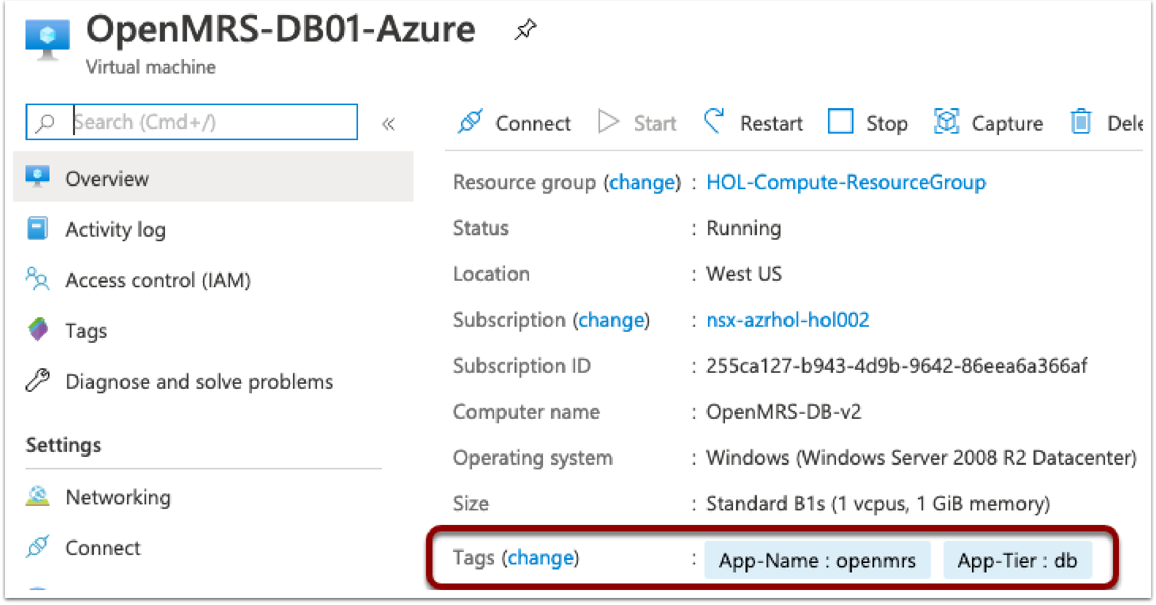
4.4 Verifying Tags in AWS and Azure

Customers can assign information to their AWS resources in the form of tags. Each tag is a basic label made up of a customer-defined key and an optional value that can help with resource management, searching, and filtering.



□	Name	Instance ID	Instance Type	Availability Zone	Instance State
□	ABCart-Web01-AWS	i-09f20b6f5723c95c2	t2.micro	us-west-1b	● running
□	nsx-gw-vpc-0e1d78b96af387500…	i-09f02a35b07b4d15c	c5.xlarge	us-west-1b	● running
□	OpenMRS-db01-AWS	i-0ea1d208e063396…	t2.micro	us-west-1b	● running
■	OpenMRS-Web01-AWS	i-0ec7c15b3724a5689	t2.micro	us-west-1b	● running

Figure 4.14 Verifying tags in AWS



Resource group (change) : HOL-Compute-ResourceGroup

Status : Running

Location : West US

Subscription (change) : nsx-azrhol-hol002

Subscription ID : 255ca127-b943-4d9b-9642-86eea6a366af

Computer name : OpenMRS-DB-v2

Operating system : Windows (Windows Server 2008 R2 Datacenter)

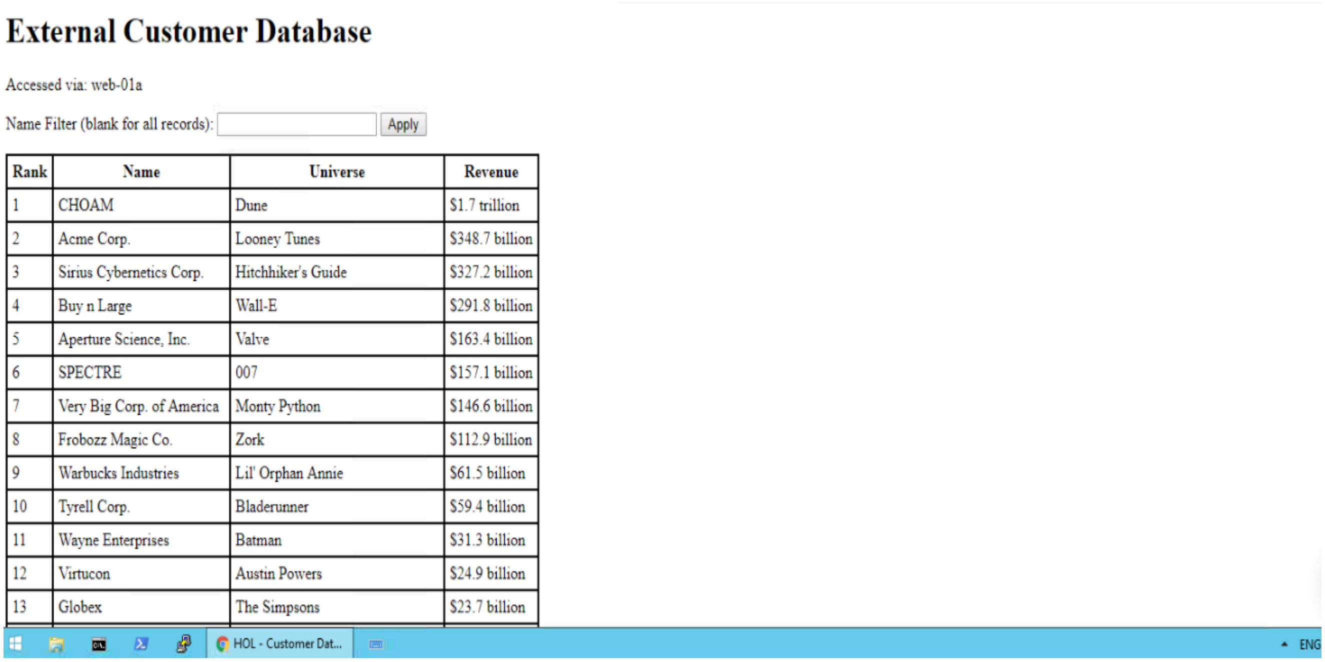
Size : Standard B1s (1 vcpus, 1 GiB memory)

Tags (change) : App-Name : openmrs App-Tier : db

Figure 4.15 Verifying tags in Azure

4.5 Testing the Native Application

The Application which was secured on cloud is accessed and tested to make sure it’s functioning properly.



External Customer Database

Accessed via: web-01a

Name Filter (blank for all records): Apply

Rank	Name	Universe	Revenue
1	CHOAM	Dune	$1.7 trillion
2	Acme Corp.	Looney Tunes	$348.7 billion
3	Sirius Cybernetics Corp.	Hitchhiker's Guide	$327.2 billion
4	Buy n Large	Wall-E	$291.8 billion
5	Aperture Science, Inc.	Valve	$163.4 billion
6	SPECTRE	007	$157.1 billion
7	Very Big Corp. of America	Monty Python	$146.6 billion
8	Frobozz Magic Co.	Zork	$112.9 billion
9	Warbucks Industries	Lil' Orphan Annie	$61.5 billion
10	Tyrell Corp.	Bladerunner	$59.4 billion
11	Wayne Enterprises	Batman	$31.3 billion
12	Virtucon	Austin Powers	$24.9 billion
13	Globex	The Simpsons	$23.7 billion

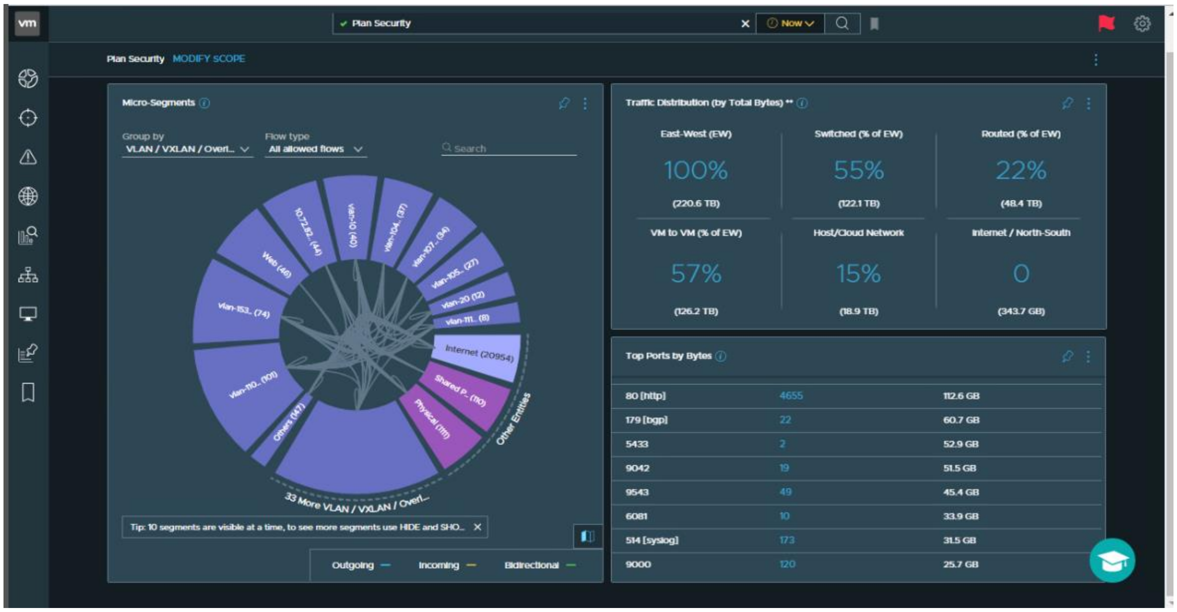
Figure 4.16 Functioning CustomerDB Application

4.5.1 Testing the Firewall Enforcement

This agentless technique enforces security utilizing the public cloud's natural security architecture. After testing the firewall rules, applications in an environment that has been secured was no longer able to communicate with other applications or virtual machines in another environment meaning the network has been micro-segmented and has been secured properly.

4.6 vRealize Network Insight

This network monitoring tool lets you develop a network architecture that is efficient, highly available, and secure across your cloud environments.



Traffic Distribution (by Total Bytes) **

East-West (EW): 100% (220.6 TB)

Switched (% of EW): 55% (122.1 TB)

Routed (% of EW): 22% (48.4 TB)

VM to VM (% of EW): 57% (126.2 TB)

Host/Cloud Network: 15% (18.9 TB)

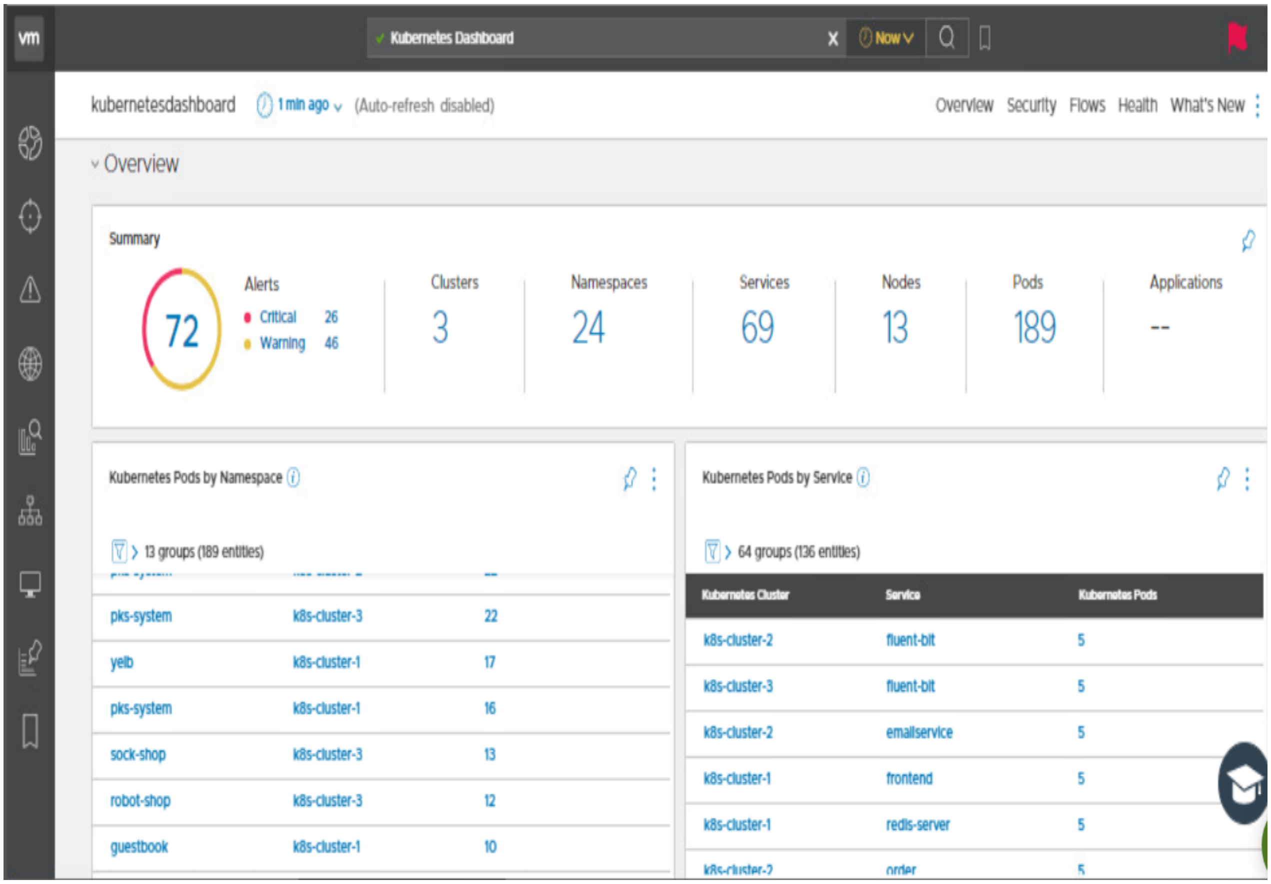
Internet / North-South: 0 (343.7 GB)

Top Ports by Bytes

80 [http]	4655	112.6 GB
179 [bgp]	22	60.7 GB
5433	2	52.9 GB
9042	19	51.5 GB
9543	49	45.4 GB
6081	10	33.9 GB
514 [syslog]	173	31.5 GB
9000	120	25.7 GB

Figure 4.17 vRealize Network Insight

This diagram of traffic that shows the logic link between each physical or virtual component in order to trace flows and sessions through a network. The applications, which are made up of tiers, allow for the construction of hierarchical groups of virtual machines (VMs) and the visualization of traffic/flows between the tiers of the same application.



kubernetesdashboard 1 min ago (Auto-refresh disabled)

Overview

Summary

Alerts	Clusters	Namespaces	Services	Nodes	Pods	Applications
72 Critical 26 Warning 46	3	24	69	13	189	--

Kubernetes Pods by Namespace

13 groups (189 entities)

pks-system	k8s-cluster-3	22
yelb	k8s-cluster-1	17
pks-system	k8s-cluster-1	16
sock-shop	k8s-cluster-3	13
robot-shop	k8s-cluster-3	12
guestbook	k8s-cluster-1	10

Kubernetes Pods by Service

64 groups (136 entities)

Kubernetes Cluster	Service	Kubernetes Pods
k8s-cluster-2	fluent-bit	5
k8s-cluster-3	fluent-bit	5
k8s-cluster-2	emailservice	5
k8s-cluster-1	frontend	5
k8s-cluster-1	redis-server	5
k8s-cluster-2	order	5

Figure 4.18 Container environment being managed by vRealize Network insight

This shows that Micro-segmentation provides support for container workloads and manages them.

4.7 Micro-segmented Application

After Micro-segmenting the application and testing to see if the application still works, the web-server is no longer allowed to connect to the Database Server even through ping. Environments and applications were defined, as well as tags, groups, policies, and rules to govern which traffic is permitted and which is not.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATION

5.0 Conclusion

There are a few methods to keep cybercriminals and hackers from freely wandering within data centers and a few good answers to the problem of making IT security more flexible and adaptable, such as firewalls, but they have been shown to be ineffective in today's ever expanding network. Both of these issues are addressed by micro-segmentation. It is one of the few technologies that can increase both security and agility.

This project effort contributes to a better understanding of the necessity for Micro-segmentation in Nigerian enterprises in order to secure the network and avoid network intrusion.

5.1 Limitations

The first of the limitations faced while undergoing this project work was time constraints. Due to the fact that Micro-segmentation is an expert level network segmentation and requires in-depth knowledge of the network and its connection.

Micro-segmentation solution software has an initial costly payment which made implementing it on an actual network not possible resulting in limited access to resources.

5.2 Recommendations for future works

For future studies, it is recommended that researchers should study the probability of applying support for physical workloads in a data center and improving process visibility which is the capacity to see processes, transactions, and other activity inside an organization correctly and fully.

5.3 References

Bellovin. S., Ioannidis. S., Keromytis, A., Smith, J. (2000). *Distributed Firewalls.* Conference: CCS 2000, Proceedings of the 7th ACM Conference on Computer and Communications Security, Athens, Greece.

Carklin, N. (2020). *Micro-segmentation: Guide on How to Build Secure Zones in Your Virtualized Environment.* Retrieved in July, 2021 from Parallels RAS VDI Blog https://www.parallels.com/blogs/ras/microsegmentation-improve-security-infrastructure/

Chickowski, E. (2019). *A Beginner's Guide to Micro-segmentation.* Retrieved in February, 2021 from Edge Articles. https://www.darkreading.com/edge/theedge/a-beginners-guide-to-microsegmentation/b/d-id/1335849?page_number=1

Chowdhary, A. (2018). *Micro-Segmentation: From Theory to Practice.* Retrieved in June, 2021 from Research Gate. https://www.researchgate.net/publication/330952978

Cohen, A. (2018). The Truth about Micro-segmentation. [White Paper]. Illumio. Inc. https://www.illumio.com/sites/default/files/Illumio_Article_SecurityWeek_The_Truth_About_Micro-Segmentation_2019_03.pdf

Cohen, A. (2018). The Truth about Micro-segmentation. [White Paper]. Illumio. Inc. https://www.illumio.com/sites/default/files/Illumio_Article_SecurityWeek_The_Truth_About_Micro-Segmentation_2019_03.pdf

Friedman, J. (2017). *The Definitive Guide to Micro-Segmentation.* Illumio. Inc. California, United States of America. Retrieved on March 11, 2021 from https://cdn2.hubspot.net/hubfs/407749/Downloads/Illumio_eBook_The_Definitive_Guide_to_Micro_Segmentation_2017_08.pdf

Fuller, R. (2016). *NSX Distributed Firewall Deep Dive.* Paper presented at the meeting of VMware World, United States of America. Retrieved on June, 2021 from https://static.carahsoft.com/concrete/files/5014/5711/5419/SDDC_Data_Center_Agility_and_Security_002.pdf

Gillis, A. (2019). *Network Virtualization.* Retrieved in July, 2021 from Tech target: https://searchservervirtualization.techtarget.com/definition/network-virtualization

Goldstein, P. (2021). *How Next-Generation Endpoint Security Is Different from Traditional Endpoint Security.* Retrieved in June, 2021 from BizTech: https://biztechmagazine.com/article/2021/03/how-next-generation-endpoint-security-different-traditional-endpoint-security-perfcon

Gozani, M. (2016). *Network Virtualization for Dummies, VMware Special Edition.* Hoboken: John Wiley & Sons, Inc. Retrieved on February 25, 2021 from MicroAge https://microage.com/wp-content/uploads/2016/12/Network-Virtualization-For-Dummies.pdf

Holmes, W., et.al. (2017). *VMware NSX Micro-Segmentation.* California, USA. VMware Press. Retrieved in June, 2021 from https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-microsegmentation.pdf

Jaworski, S. (2017), *Does Network Micro-segmentation Provide Additional Security?.* [White Paper]. Retrieved on February 15, 2021 from SANS Institute: https://www.sans.org/reading-room/whitepapers/networksecurity/network-micro-segmentation-provide-additional-security-38030

Kollimarla, S. (2018). *Micro-Segmentation for Data Centers: How it Works*. Retrieved July, 2021 from Color tokens*:* https://colortokens.com/blog/data-center-micro-segmentation/

LaBounty, C. (2021). *What is Network Security ad Why It is Important?.* Retrieved in July, 2021 From: https://www.herzing.edu/blog/what-network-security-and-why-it-important

McGee, J. (2018). *The best workloads for containers: All of them*. Retrieved from Info World.https://www.infoworld.com/article/3251712/the-best-workloads-for-containers-all-of-them-really.html

Miller, L., & Soto, J. (2015). *Micro-segmentation for Dummies, VMware Special Edition.* Hoboken: John Wiley & Sons, Inc. Retrieved on February 15, 2021 from https://static.cbsileads.com/direct/whitepapers/Micro-segmentationForDummies.pdf

Oltsik, J. (2018). *The Case for Host-based Micro-segmentation.* [ESG White Paper]. Illumio Inc.

Patel, B. (2011). *Approach of Data Security in Local Network using Distributed Firewalls.* International Journal of P2P Network Trends and Technology (IJPTT) - Volume 1 Issue 3. Motibhai Patel Institute of Computer Science.

Schonberg, Z (2020). *The State of Container Workloads* [White Paper]. Spot by NetApp. Retrieved on June, 2021 from https://snsltd.co.uk/downloads/vendors/NetApp/The_State_of_Container_Workloads_2020.pdf

Shackleford, D. (2020). *How to Create a Comprehensive Zero Trust Strategy.* Sans Institute. Retrieved from https://www.sans.org/white-papers/39790/

Stepanek, R. (2001). *Distributed Firewalls.* Article in T-110.501 Seminar on Network Security 2001 ISBN 951-22-5807-2. http://www.tml.hut.fi/Studies/T-110/501/2001/papers/index.html

VMware. (2014). *A Software Defined Data Center Approach for a "Zero Trust" Security Strategy*. [White Paper]. VMware. Inc.

V. Ramsurrun, and K. M. S. Soyjaudah. (2009).*A Stateful CSG-Based Distributed Firewall Architecture for Robust Distributed Security*. Paper presented at University of Mauritius (UoM). Réduit, Mauritius.

Wan, D. (2002). *Distributed Firewall*. GSEC Practical Assignment Version 1.2c. Sans Institute. Retrieved from https://www.giac.org/paper/gsec/766/distributed-firewall/101682