CareGroup

Network Administration

Angel Contreas, Christian Najera,
Daniel Thach

2/26/25

CIS - 4900

Contents

1. **Company History**

CareGroup was founded in early October 1996 in eastern Massachusetts because of a merger between Beth Israel Hospital, Deaconess Hospital, and Mount Auburn Hospital (McFarlan & Austin, 2005). This merger was because of the pressure of creating a more assertive regional healthcare network that each hospital could not fulfill independently. At the cost of 1.6 billion dollars, the merger was hoped to provide financial stability while enhancing their powers over HMOs for negotiations. CareGroup is a team of healthcare professionals that provides specialized treatments to patients in their health service facilities.

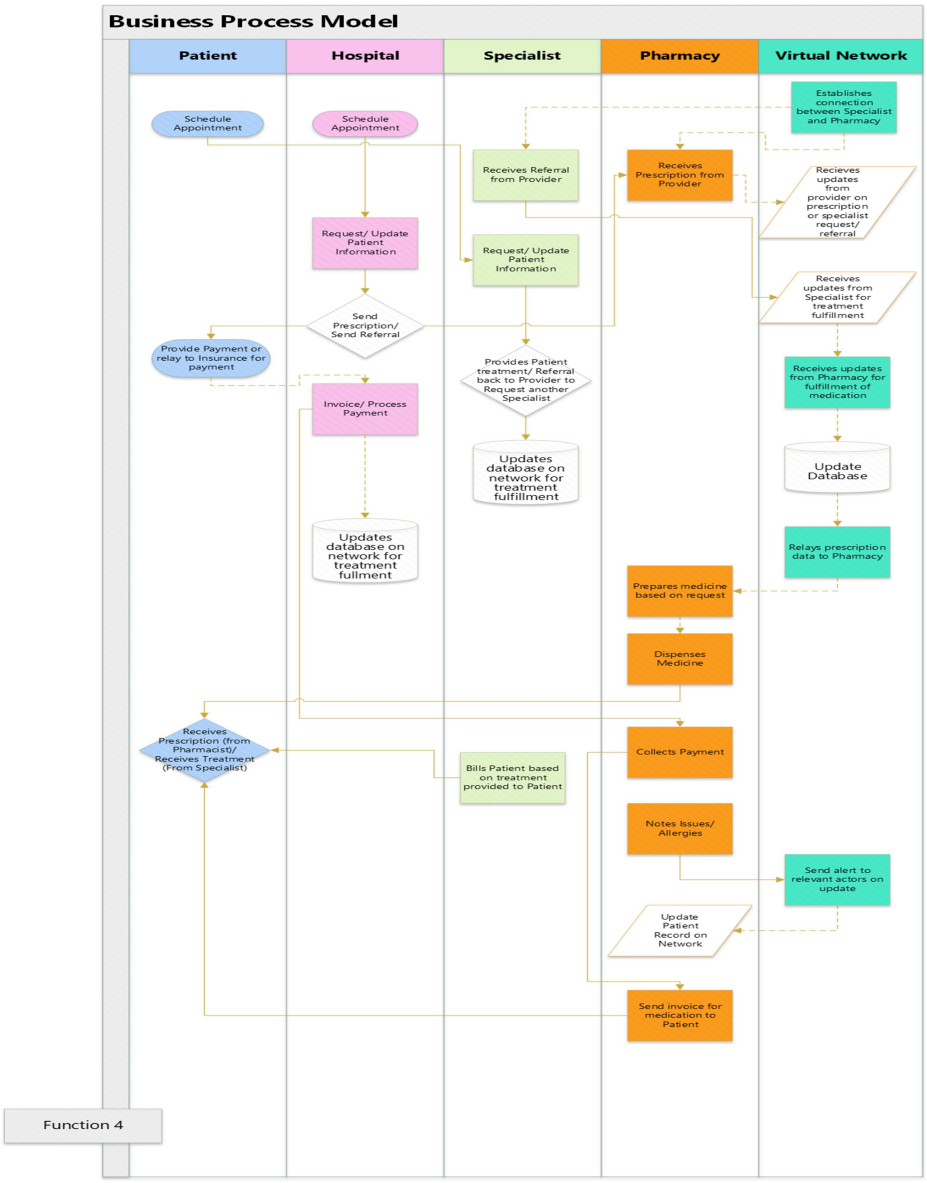
Despite the successful merger, the business suffered financial losses due to the costs of integrating the hospitals into a single network. However, over time, they found success further down the line.

They succeeded in keeping costs low during the restructuring, creating one of the best technological integrations to the point in which it was recognized by the healthcare IT industry in America. CareGroup was successful, thanks to John Halamka's contributions, and he overhauled the entire IT system using the Meditech software package to establish communication lines within the hospitals (McFarlan & Austin, 2005). Even then, it did not prevent the network outage in November 2002 that took down communication systems for 3 days. The issue was resolved with intervention from CISCO and became a lesson learned for the company to stay vigilant in their hardware and software configurations.

In 2018, there was a merger acquisition between CareGroup and Beth Israel Lahey Health, and because of that, CareGroup ceased to exist. Massachusetts Attorney General's Office initially contested their merger due to the impact on competition, but in the end, they approved the merger and dropped the case.

There have been changes in operation through the new merger, but the business goal is very similar, if not identical, to CareGroup. Beth Israel Lahey Health operates and manages 14

hospitals that handle a spectrum of health services, from common ones to more sophisticated specialized treatments (Massachusetts Health Policy Commission, 2018). They also have a research division and hospital sites where they teach the next generation of health professionals, but their pride is in satisfaction to the patient. Beth Israel Lahey Health operates in Massachusetts. They are now regarded as the most significant health system in Massachusetts because the hospitals they oversee have been reported to employ over 39,000 people.



2. **Proposed Network Project**

Virtualization is a technology that is very flexible and can be implemented in many ways, typically in the forms that support networking and machine operation. Two outstanding implementations of virtualization that Beth Israel Lahey Health could benefit from are those of virtual machines (VM) running on a virtualized network (VN). These virtualization technologies present the company with a cost-effective, robust, and powerful solution to its computational needs. For the enterprise, we will be implementing a virtualized IT infrastructure to fulfill BILH's business strategy and purpose.

BILH's **purpose statement is to "create healthier communities - one person at a time - through seamless care and groundbreaking science, driven by excellence, innovation, and equity."** They further state that "By working collaboratively to address top health concerns, we create a healthy future for everyone in the communities we serve. Our hospitals have a longstanding commitment to supporting community programs that serve those who face barriers to getting and staying healthy. This includes addressing issues such as access to care, chronic disease management, health disparities and social determinants of health such as food and housing insecurity and more."

From these excerpts, we can isolate some fundamental values and cornerstone requirements that BILH needs to fulfill its values and comply with its business strategy. BILH wants to effectively serve its community and foster a great work environment at the same time. BILH believes that to do these things, it needs to stand as a quality-built healthcare company that innovates in its space. First and foremost, in BILH's healthcare activities lies the absolute requirement to collaborate. Teams collaborate most effectively when everyone has access to the same resources so that they can understand what their peers are doing, and what they are thinking. When resources are shared, it can lead to a more productive work environment and therefore delivers the **high-quality care that BILH seeks to provide**. So that these teams have the **highest access and availability to resources**, a virtualized network is the leading contender for its IT infrastructure solution. Furthermore, BILH places a strong emphasis on innovation in its strategic outlook. To innovate, BILH seeks to develop improved methods and products compared to existing solutions to stand above the competition and to serve the community better. Development is a process that

requires lots of research; therefore, access to that research and research methods would be best fulfilled by a virtual network. Innovation in the modern age within the healthcare industry needs virtualization to happen. Competitors in the industry leverage virtualization to fulfill the same or similar purposes and without it, BILH's contributions to the community would surely suffer. Speaking of advantages, although top leading healthcare organizations may use virtualization, it's very common that healthcare systems are so very often outdated and run legacy technologies. It has proven time and time again that outdated systems eventually cause many different problems ranging from malfunction in operation or bigger catastrophes like data breaches. BILH would be disserving the community by allowing anything other up-to-date virtualized technology to be implemented where needed.

3. **Create a virtual network**

A virtual network is a technology usually hosted on a cloud that connects remotely located servers or computers over the internet. Off-site physical computers can also be virtual machines hosted on the cloud. However, they can represent an emulator that mimics the function of a computer or be an actual computer accessed through a virtual private network (VPN) on the network. The principles of a virtual network are based on traditional principles, but it is software-driven, so many components are hypotheticals that apply to a digital environment (GeeksforGeeks, 2022).

The virtual network provides all the benefits of a traditional physical network while taking advantage of working remotely; it also provides the benefit of standardizing the performance of machines on the network and reducing the cost of operations and maintenance. The offering of a virtual network varies by the vendor and the platform on which it is hosted. For example, Azure, provided by Microsoft, offers the ability to create a subnet with machines connected remotely to the area using the virtual network; the integration allows more effortless scalability, availability, and segregation (Microsoft, 2024a).

Azure’s cloud platform offers reliability backed by Microsoft. Building a network allows businesses or users to access Azure resources and functions in most virtual networks, such as filtering traffic, monitoring traffic, and routing outbound and inbound communications. A typical

virtual network includes a switch software that allows the connection between the physical and virtual parts of the network. It also contains a network adapter that allows LANs to interact with the broader web and servers and firewalls that would be useful for configuring safety (GeeksforGeeks, 2022). Any other features are dependent on the service provides like how Azure offers outbound communication encryption and encryption at rest.

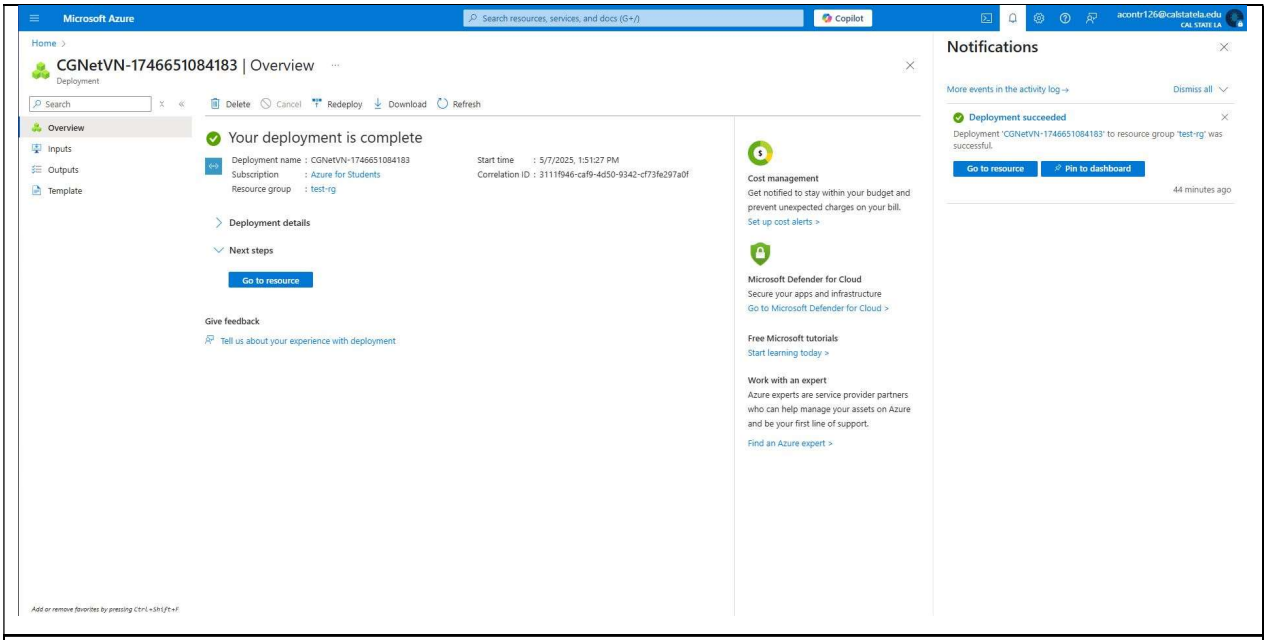


Figure 1: The Creation of "CGNetVN" a Virtual Network - A. Contreras

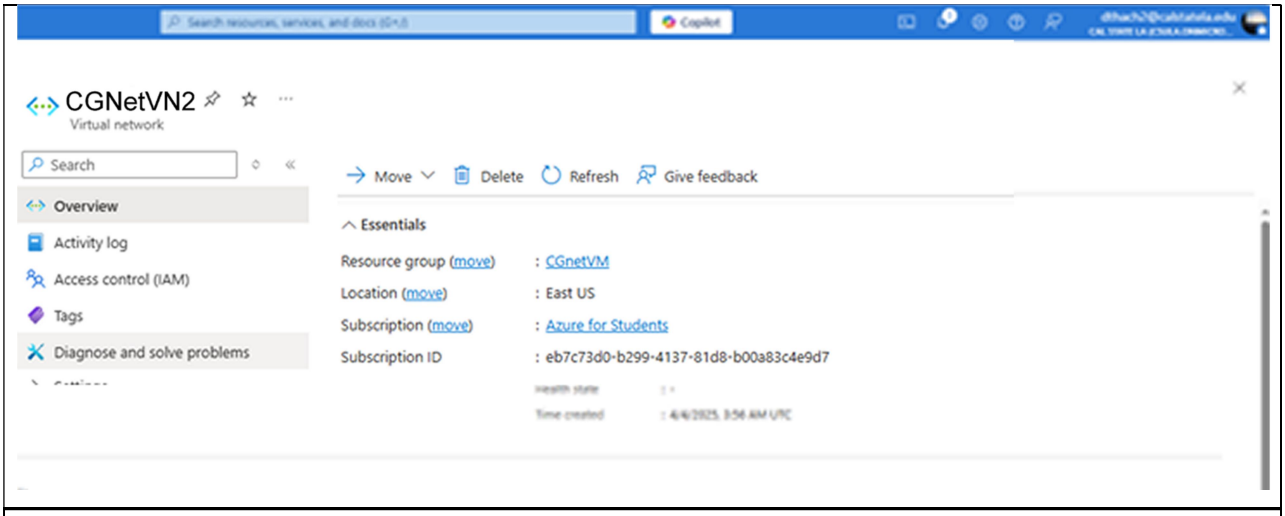


Figure 2: The Creation of "CGNetVN2" a Virtual Network on standby - D. Thach

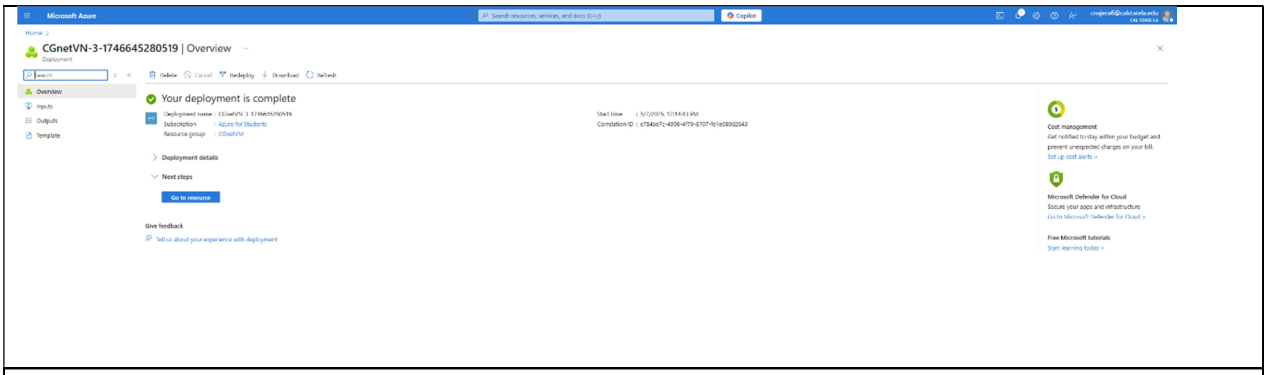


Figure 3: The Creation of "CGnetVN3" a Virtual Network being deployed - C. Najera

3.1. **Create virtual machines**

Virtual machines are emulations of a standard computer created within a physical computer with all the similar functions of a real computer. However, it allocates the host machine's resources because it is digital. A pre-requisite to making a virtual machine is a host machine to house the software and allocate the components to run the virtual machines. Since it mimics the functions of a computer, the machines require an operating system to run, and typically, anything that happens in the virtual machine is partitioned from the rest of the host (Microsoft, 2025a).

One of the reasons and benefits of using a virtual machine is that it helps users deploy applications in development in a controlled environment or as a safety precaution to tamper with files that would compromise real machines and cost money (Microsoft, 2025a). Businesses can save money because a single host can assign multiple virtual machines to unique users, increasing the workforce potential. It also offers scalability since a traditional computer would require the allocation of space and cost money to assemble when an expert can set up a machine to expand the capabilities and number of people working on a single network with proper set-ups. There is also the availability and reliability aspect, as virtual machines have low downtimes if hosted on the cloud and can be delegated to hosting backups in case of a network failure. The system is also secure because if a virtual machine is infected by malware or malicious code, it is isolated and will not affect other virtual machines or the host system itself (Susnjara & Smalley, 2024). The downside is that their performance relies on the machine's specifications and how well it was configured; it is also an issue that the single point of failure is that all virtual machines on one host can be disabled should something happen to the host machine itself.

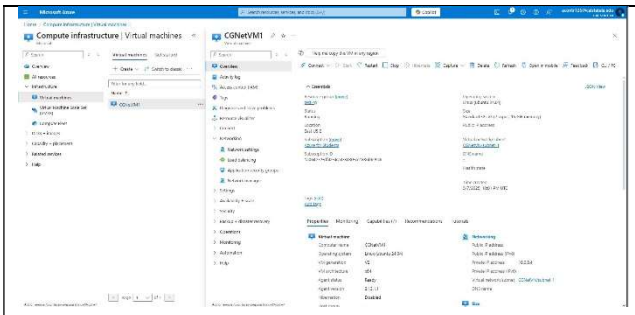


Figure 4: CareGroup Virtual Machine 1

- A. Contreras

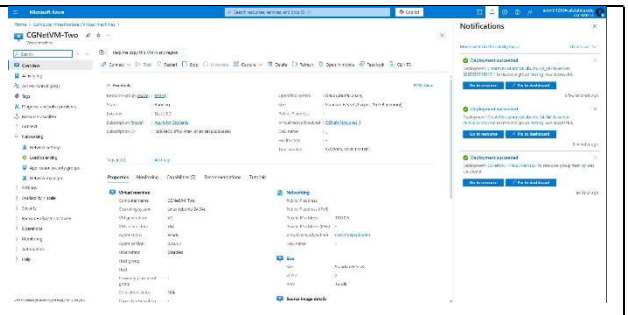


Figure 5: CareGroup Virtual Machine 2

- A. Contreras

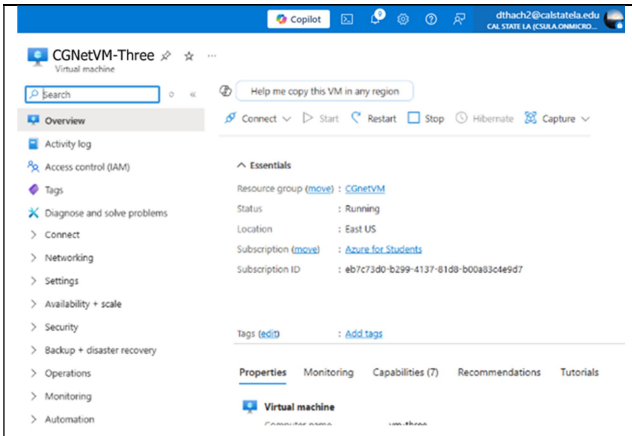


Figure 6: CareGroup Virtual Machine 3 named CGNetVM-Three

- D. Thach

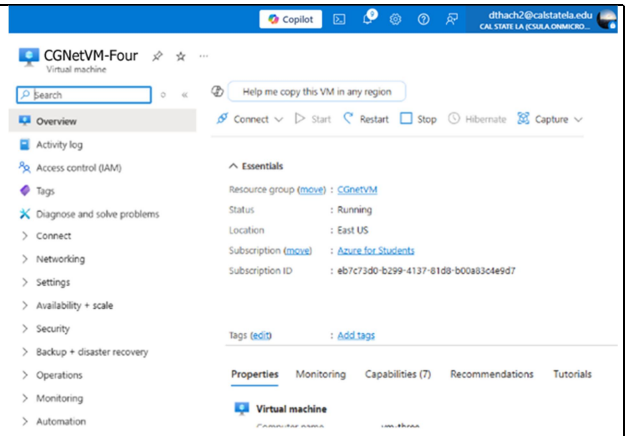


Figure 7: CareGroup Virtual Machine 4 named CGNetVM-Four

- D. Thach

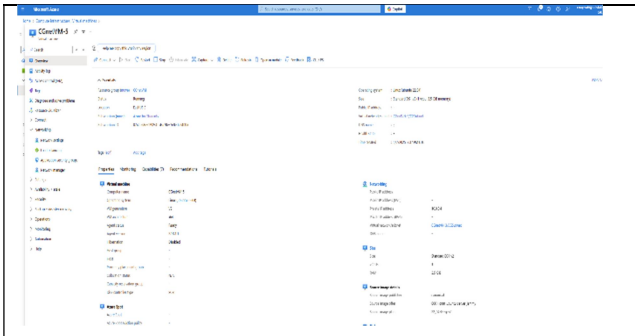


Figure 8: CareGroup Virtual Machine 5

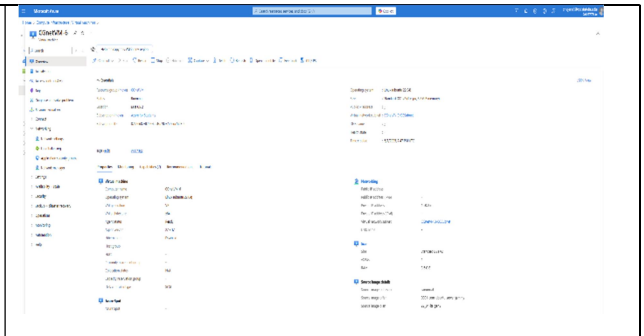


Figure 9: CareGroup Virtual Machine 6

- C. Najera	- C. Najera

3.2. Connect to a VM from the internet

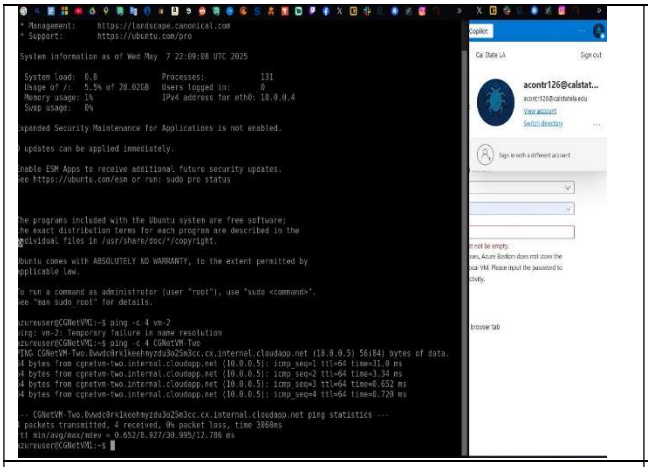


Figure 10: CareGroup Virtual Machine 1 connected to internet

- A. Contreras

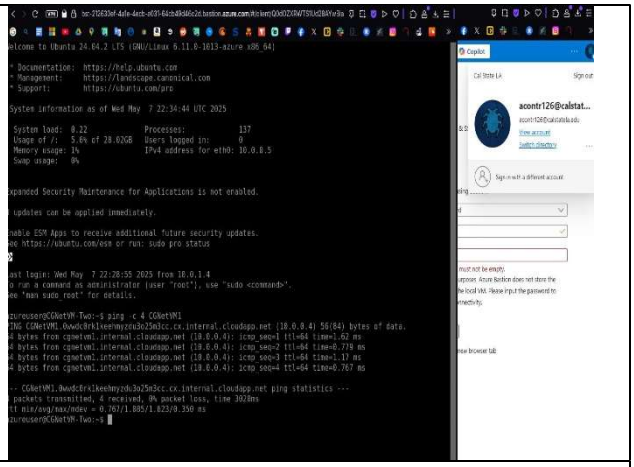


Figure 11: CareGroup Virtual Machine 2 connected to internet

- A. Contreras

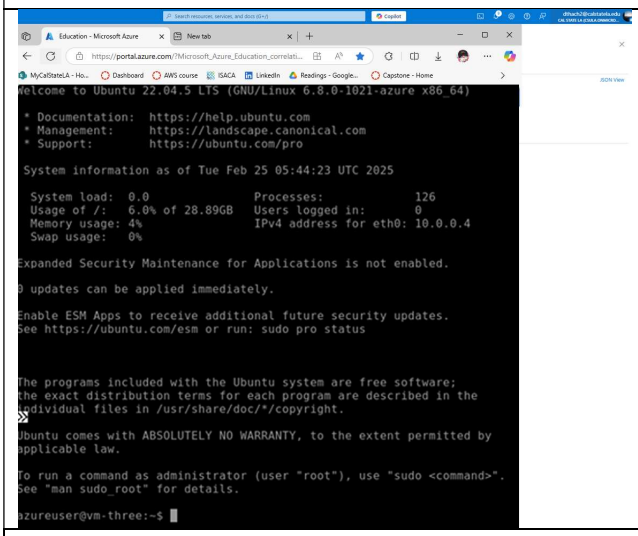


Figure 12: CareGroup Virtual Machine 3 connected to internet

- D. Thach

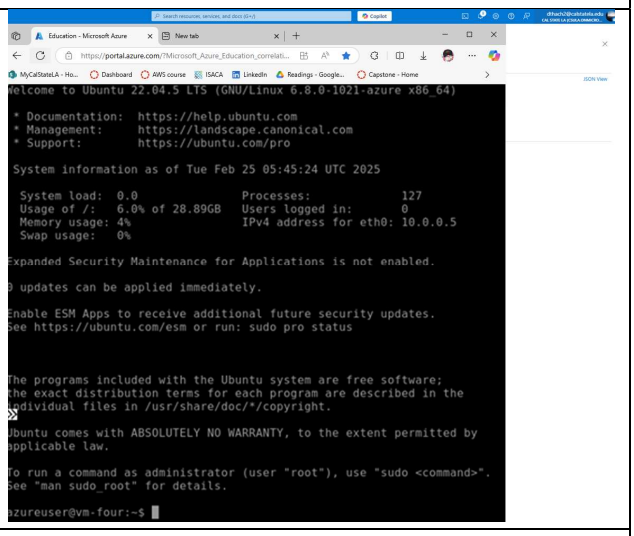


Figure 13: CareGroup Virtual Machine 3 connected to internet

- D. Thach

Figure 14: CareGroup Virtual Machine 5 connected to internet

- C. Najera

Figure 15: CareGroup Virtual Machine 6 connected to internet

- C. Najera

3.3. **Communicate between VMs**

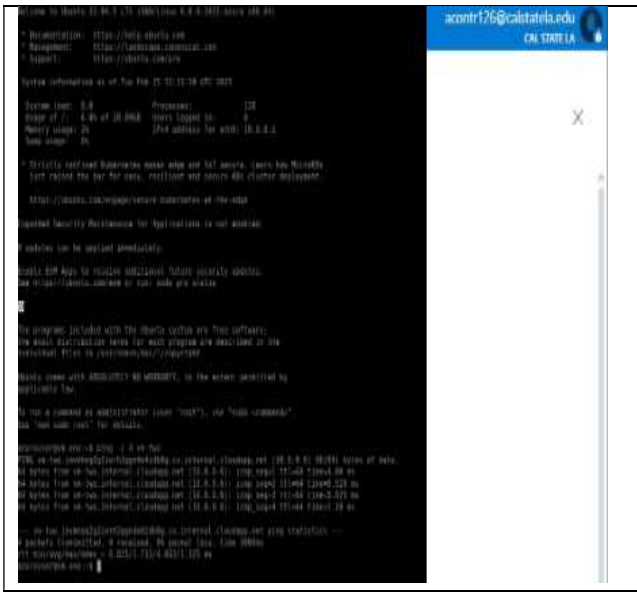


Figure 16: CareGroup Virtual Machine 1 communicating with Virtual Machine 2

- A. Contreras

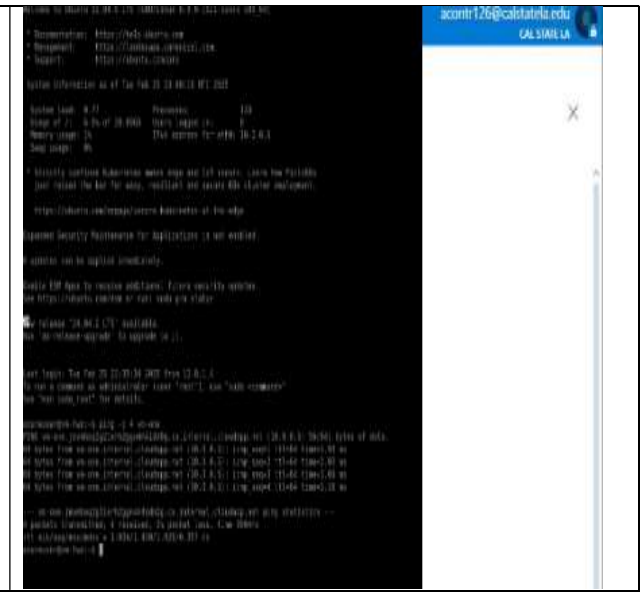


Figure 17: CareGroup Virtual Machine 2 communicating with Virtual Machine 1

- A. Contreras

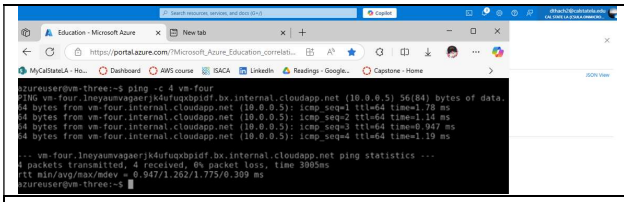


Figure 18: CareGroup Virtual Machine 3 communicating with Virtual Machine 4

- D. Thach

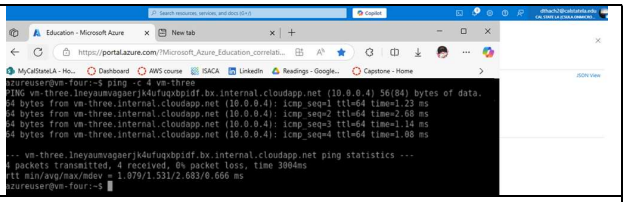


Figure 19: CareGroup Virtual Machine 4 communicating with Virtual Machine 3

- D. Thach

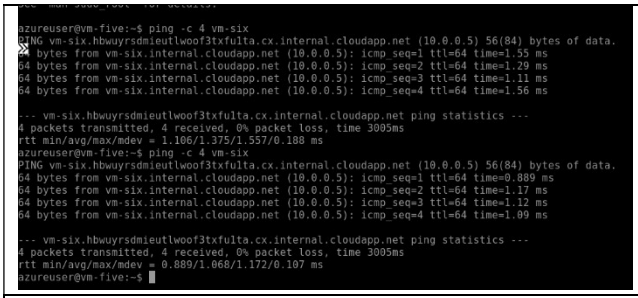


Figure 20: CareGroup Virtual Machine 5 communicating with Virtual Machine 6

- C. Najera

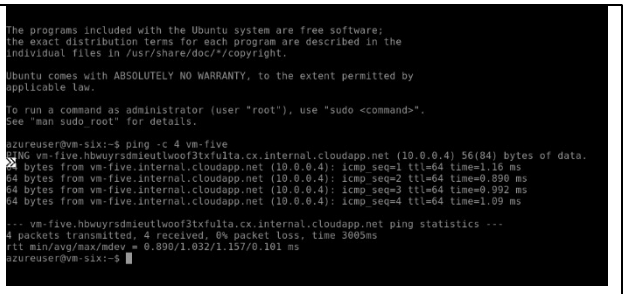


Figure 21: CareGroup Virtual Machine 6 communicating with Virtual Machine 5

- C. Najera

4. Filter network traffic with a network security group using the Azure portal

Brief Overview

A network security group filters network traffic by defining security rules that allow or deny inbound and outbound traffic based on source, destination, port, and protocol, essentially acting as a virtual firewall that controls access to Azure resources with a virtual network. Key points when creating a network security group with Azure would be to maintain security rules, associating the group to a subnet or network interface, and of course monitoring / troubleshooting.

Inbound Traffic

If there is a network security group hooked up to a subnet, Azure processes its rules as primary.

Conversely, if there is a network security group hooked up to a network interface, Azure will then process its rules second.

VM1: Network Security Group 1, processes rules since it's accounted w/ subnet 1 whereas vm1 resides. If there's no rule for port 80 inbound, traffic is denied by default. Network Security Group 2 won't evaluate the blocked traffic. Both network security groups must allow port 80 to permit traffic to the virtual machine.

VM2: Network Security Group 1, rules apply as VM2 is in a subnet 1. Without a network security group on the network interface, VM2 accepts allowed traffic through network security group 1 or gets denied accordingly.

VM3: Traffic enters Subnet2 freely and is then processed by NSG2, which is linked to VM3's network interface.

VM4: Traffic is blocked to VM4 as neither Subnet3 nor its network interface has an associated network security group.

Outbound Traffic

For traffic going outbound, Azure processes the rules in a network security group (nsg) associated to a network interface as it primary objective, if there is one, and then the rules in a network security group associated to the subnet, again if there is one. This process includes intra-subnet traffic.

VM1: NSG2 processes rules. Both NSG1 and NSG2 allow outbound traffic by default. To deny port 80, either NSG must have a rule that does it.

VM2: All traffic goes through the network interface to the subnet. NSG1 processes the rules.

VM3: NSG2 denies traffic if there's a rule for port 80; otherwise, traffic is allowed by default.

VM4: All traffic is allowed as there's no NSG associated with VM4's network interface or Subnet3.

Intra-Subnet Traffic

1. Security rules in a network security group hooked-up to a subnet can impact VM connectivity. By default, VMs in the same subnet commutate via an NSG rule allowing intra-subnet traffic. Adding a rule to NSG1 that denies all traffic stops VM1 and VM2 from communicating
2. Observing the effective security rules for a network interface is possible in order to see aggregate rules. Use Azure Network Watcher's IP flow verify to determine if communication is allowed or denied and to identify the responsible network security rule.

4.1. Create application security groups

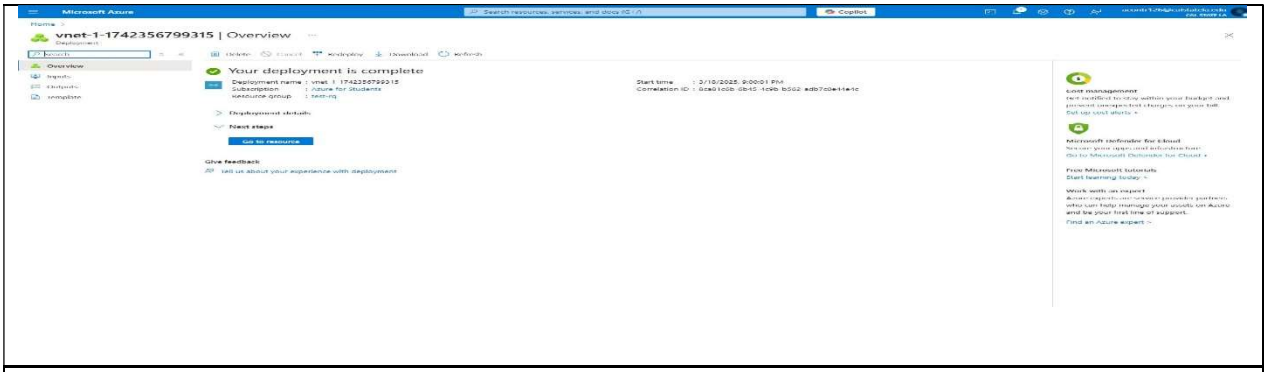


Figure 22: test-rg, vnet-1, subnet-1- A. Contreras

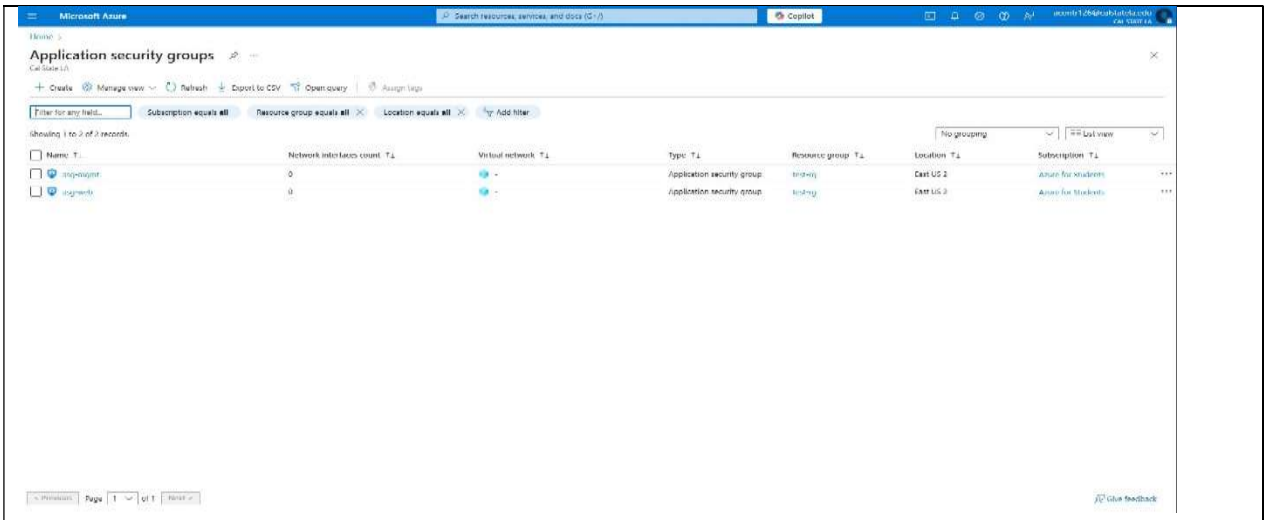


Figure 23: Application Security Groups - A. Contreras

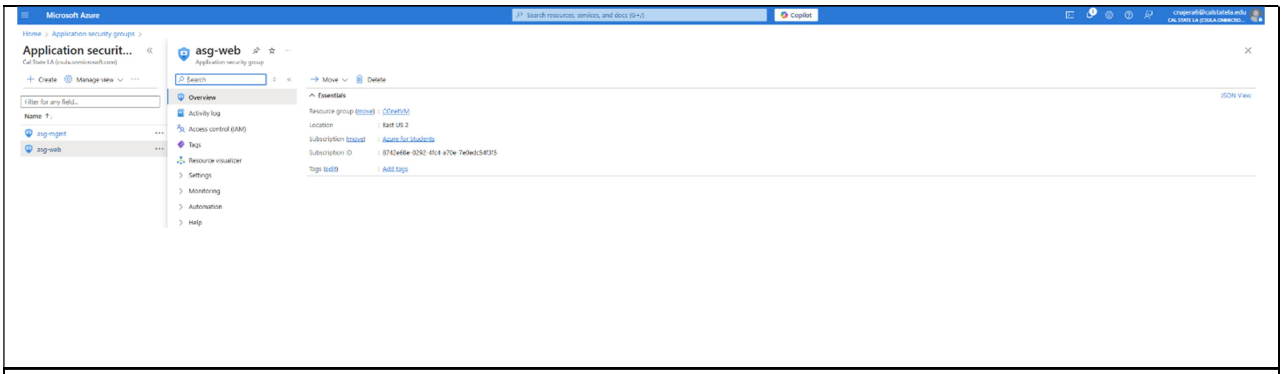


Figure 24: ASG Web- Application Security Group for Web - C. Najera

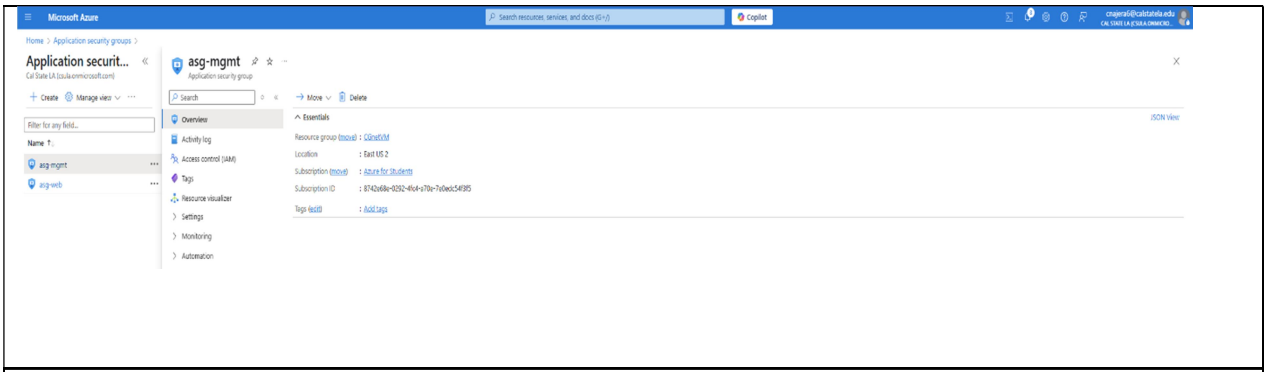


Figure 25: ASG MGMT- C. Najera

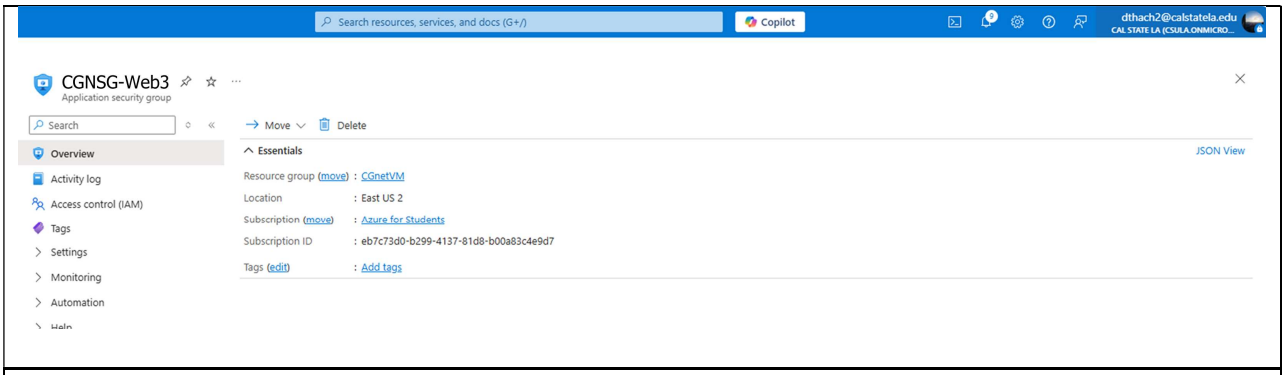


Figure 26: Application Security Group Web Group at BILH – An Application Security Group for Web group used to be filter inbound and outbound traffic using protocols that were configured during the creation. **-** D. Thach

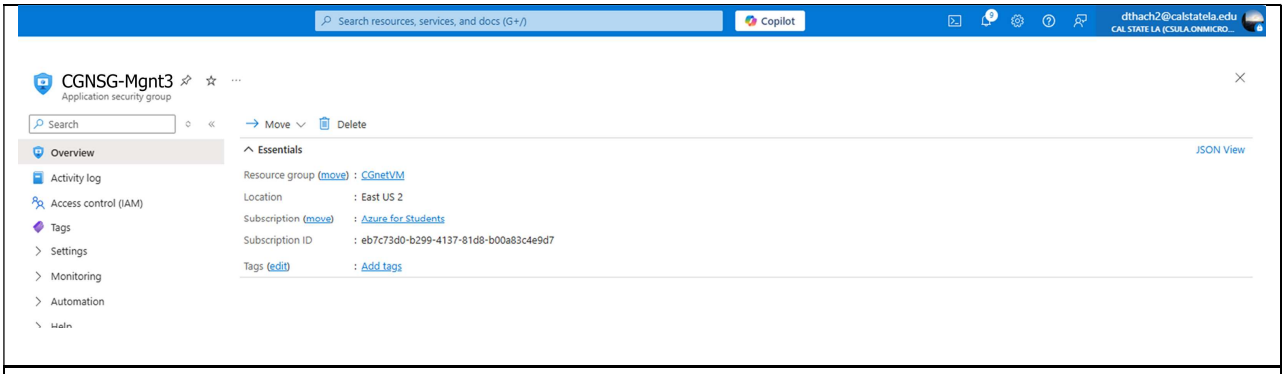


Figure 27: Application Security Group MGMT Group at BILH – An Application Security Group for Management group used to be filter inbound and outbound traffic using protocols that were configured during the creation. - D. Thach

4.2. **Create a network security group**

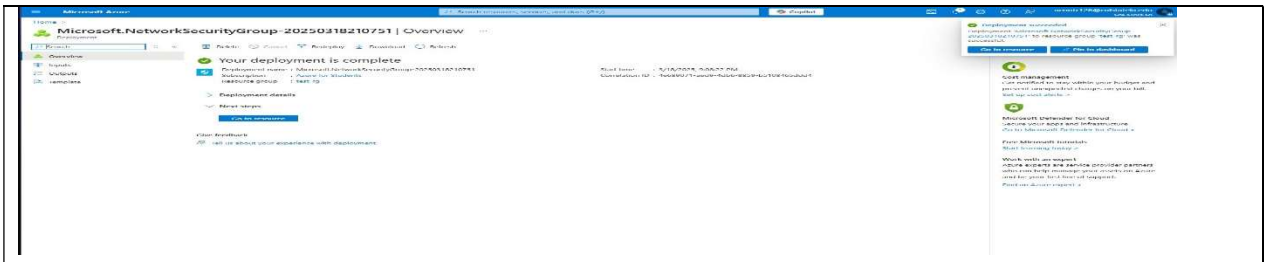


Figure 28: Network Security Group - A. Contreras

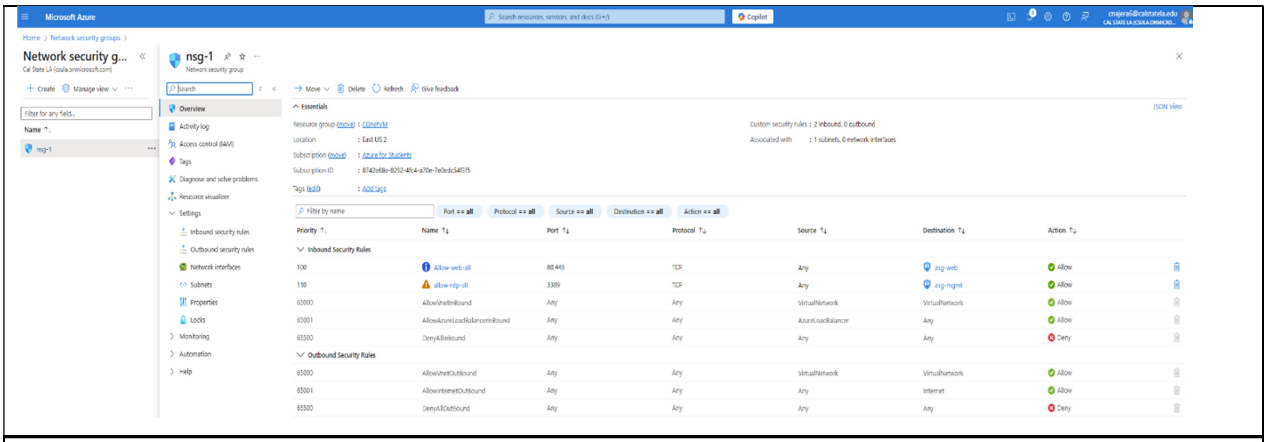


Figure 29: Network Security Group Created- C. Najera

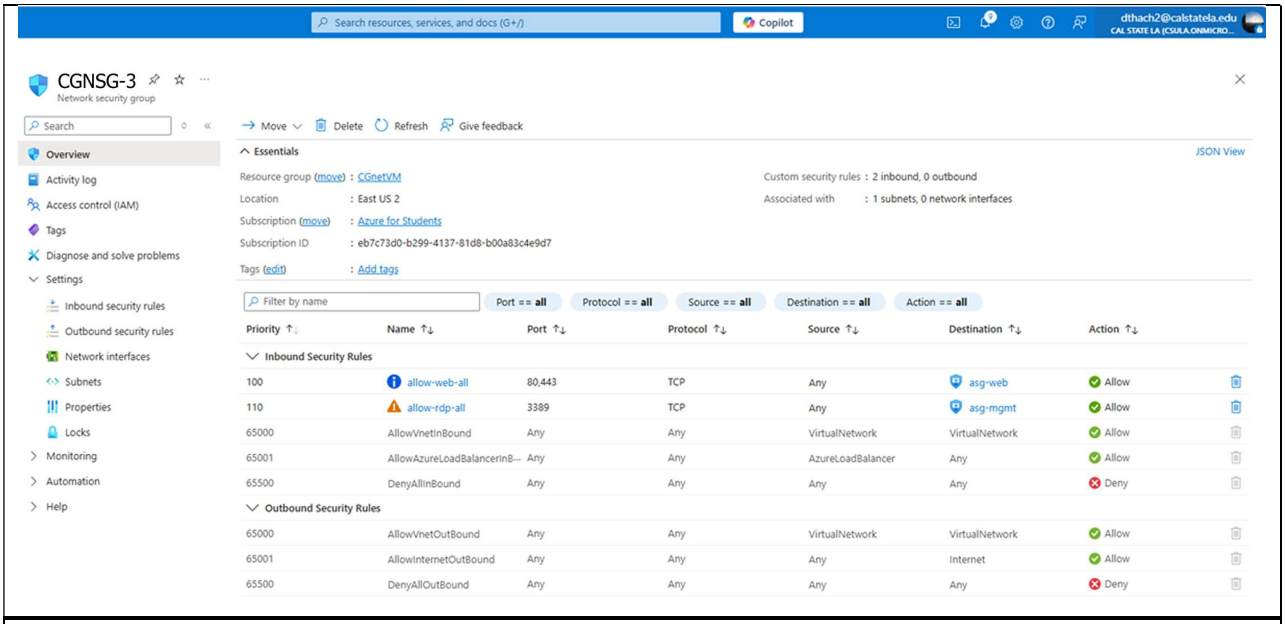


Figure 30: BILH Network Security Group 3 – The third security group created for testing in the BILH virtual network. This is where you can delegate rules that governs the traffic with network protocols. - D. Thach

4.3. Associate network security group to subnet

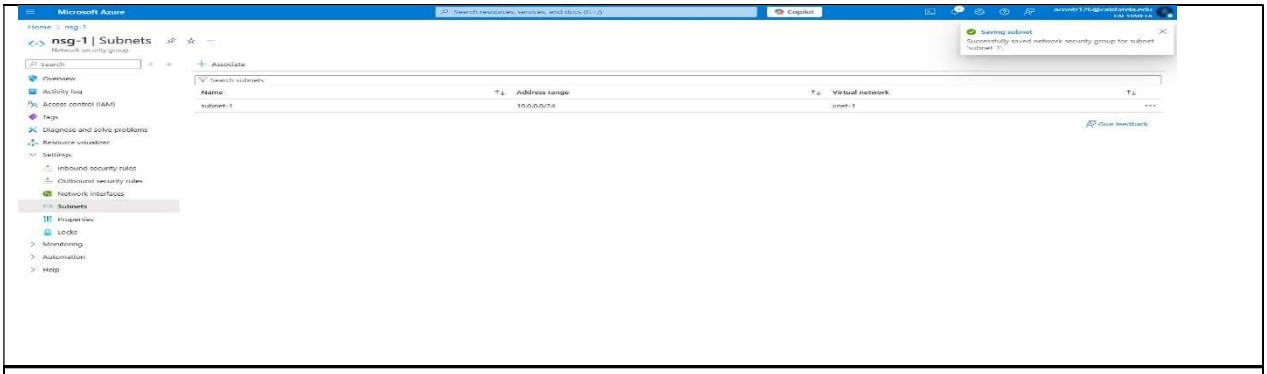


Figure 31: Associate NSG to Subnet - A. Contreras

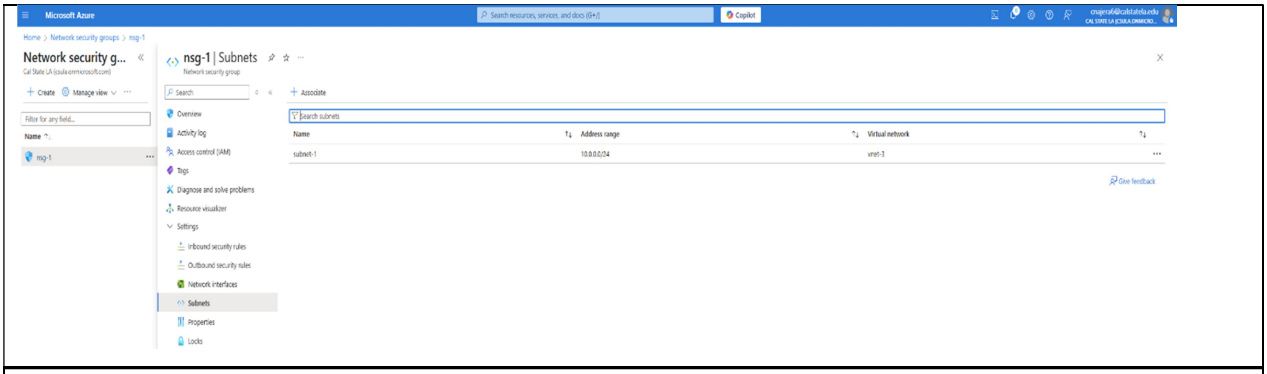


Figure 32: NSG Subnet Association - C. Najera

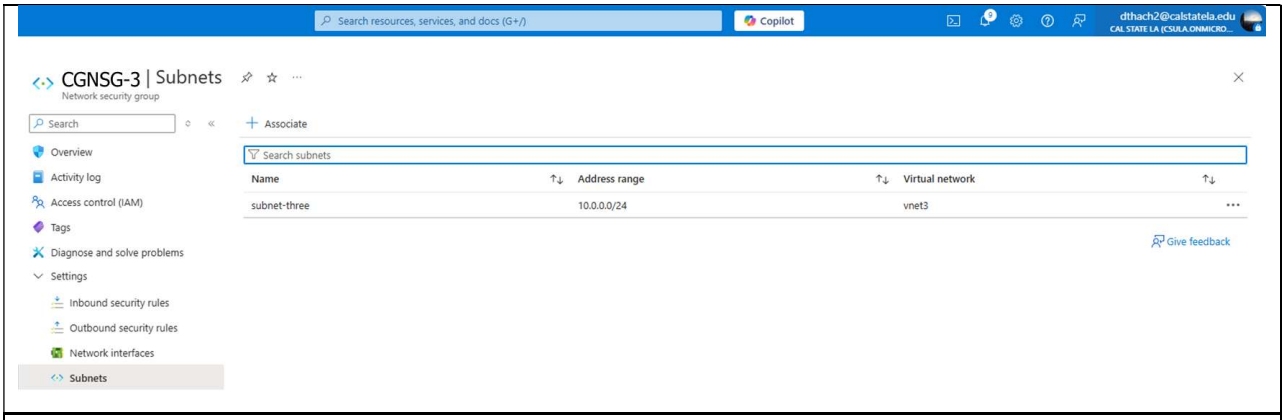


Figure 33: BILH can have virtual networks added to existing Network Security Groups. This subnet known as “GCNSG-3” is delegated to the “vent3” sub-network. - D. Thach

4.4. Create security rules

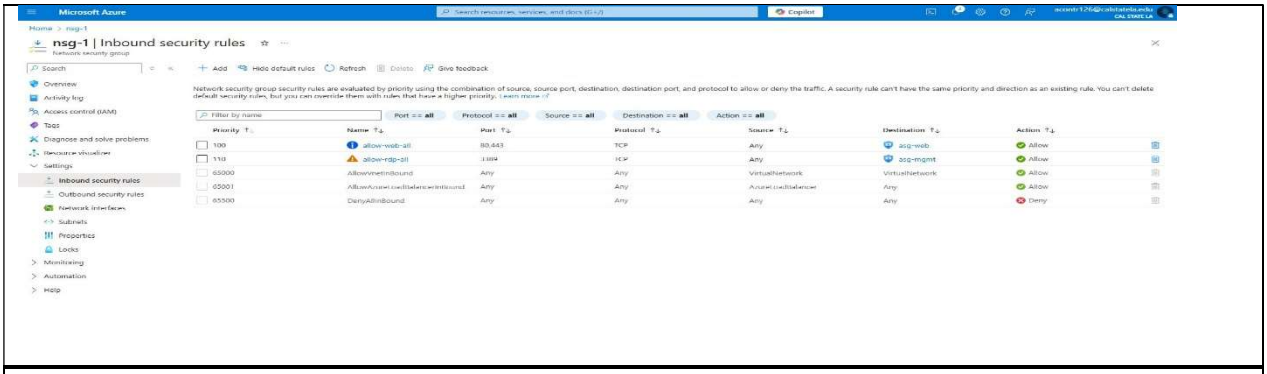


Figure 34: Here we are creating security rules that filter access to our network with protocols - A. Contreras

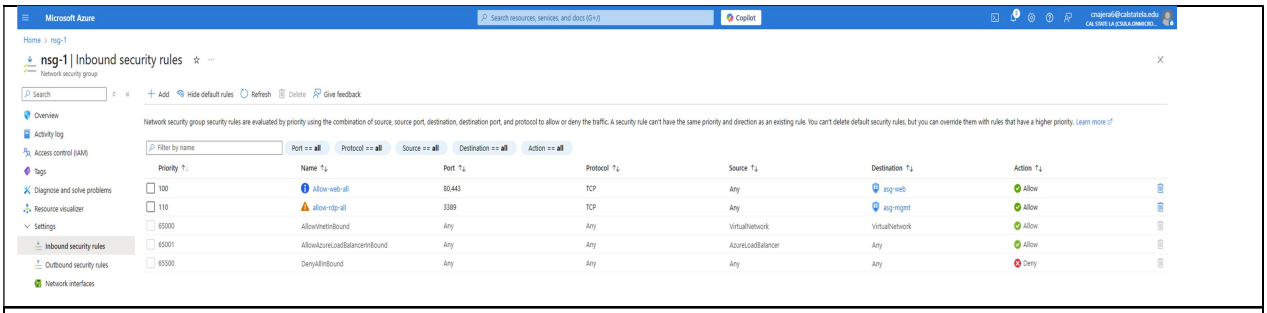


Figure 35: NSG Inbound Security Rules- C. Najera

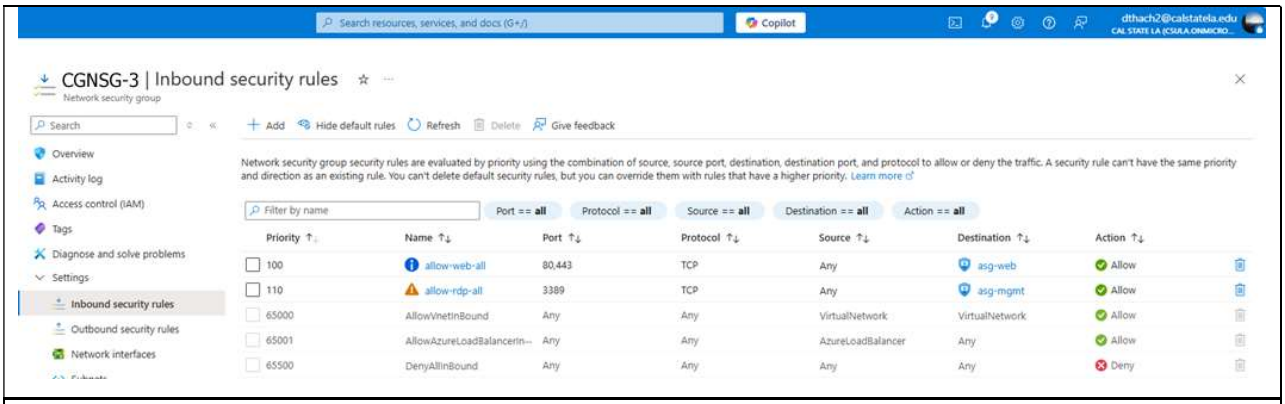


Figure 36: Here we are creating security rules that can filter access to our network with protocols. - D. Thach

4.5. Associate network interfaces to an ASG

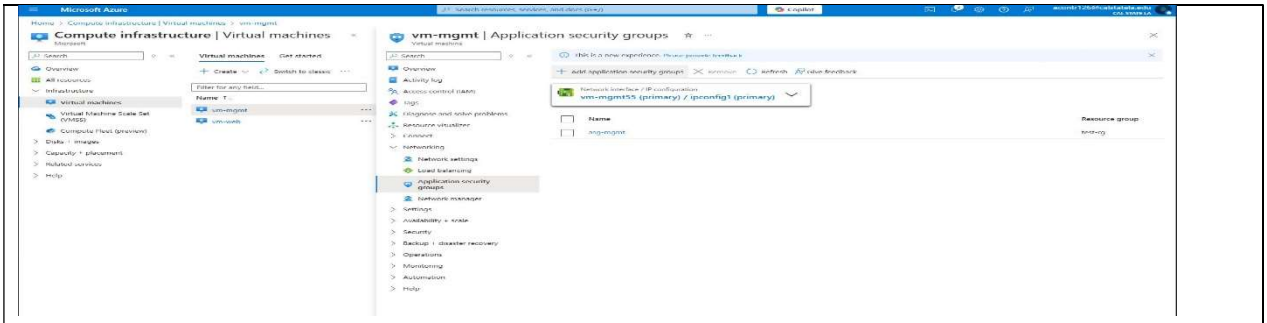


Figure 37: MGNT - A. Contreras

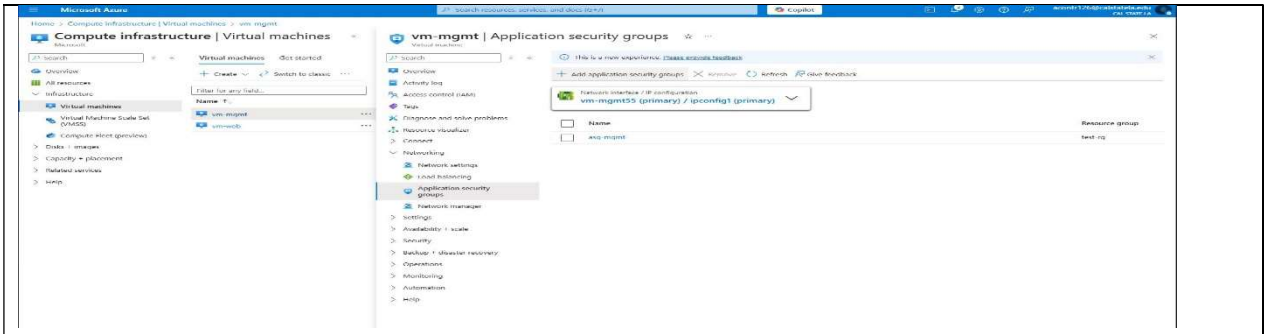


Figure 38: WEB - A. Contreras

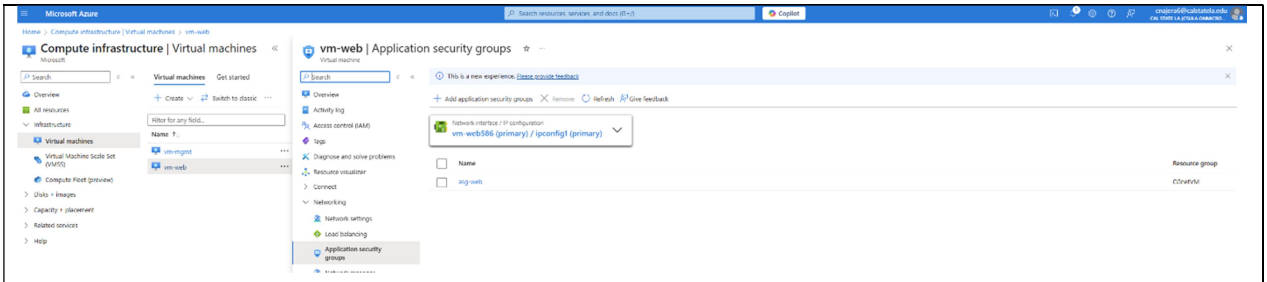


Figure 39: ASG Applied to VM-Web- C. Najera

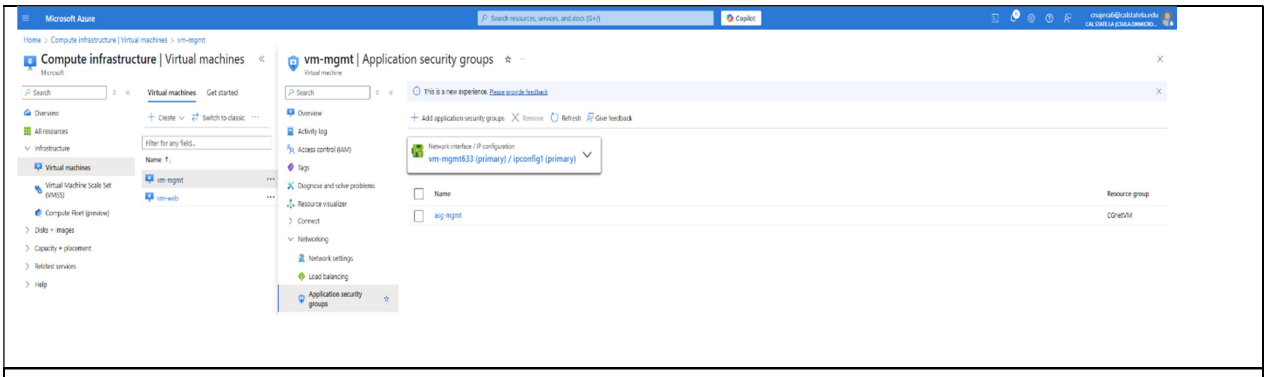


Figure 40: ASG Applied to VM-MGMT - C. Najera

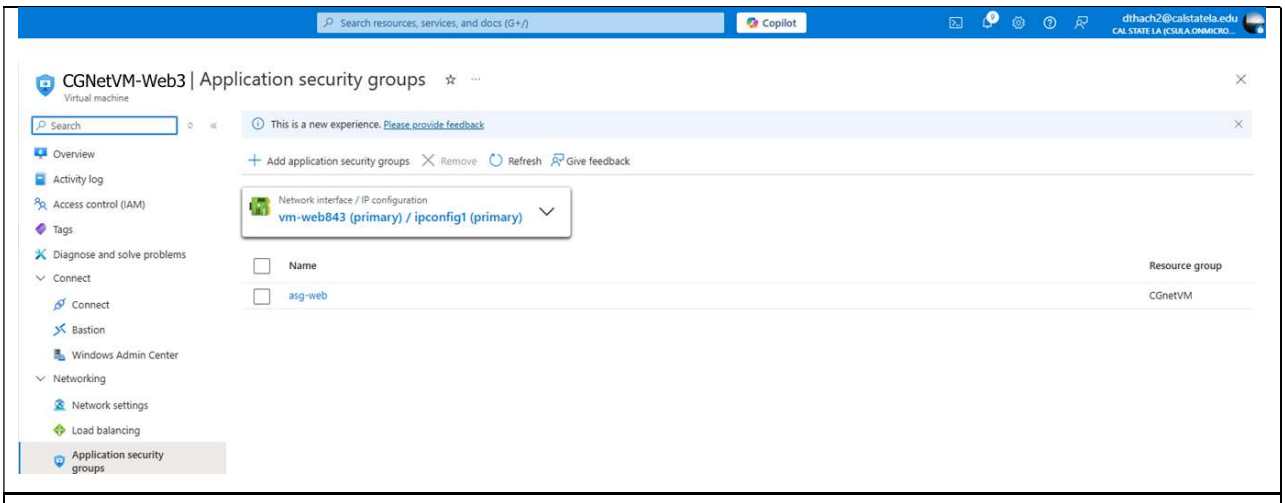


Figure 41: Security Group has been applied to the Web Server VM for third subnet. - D. Thach

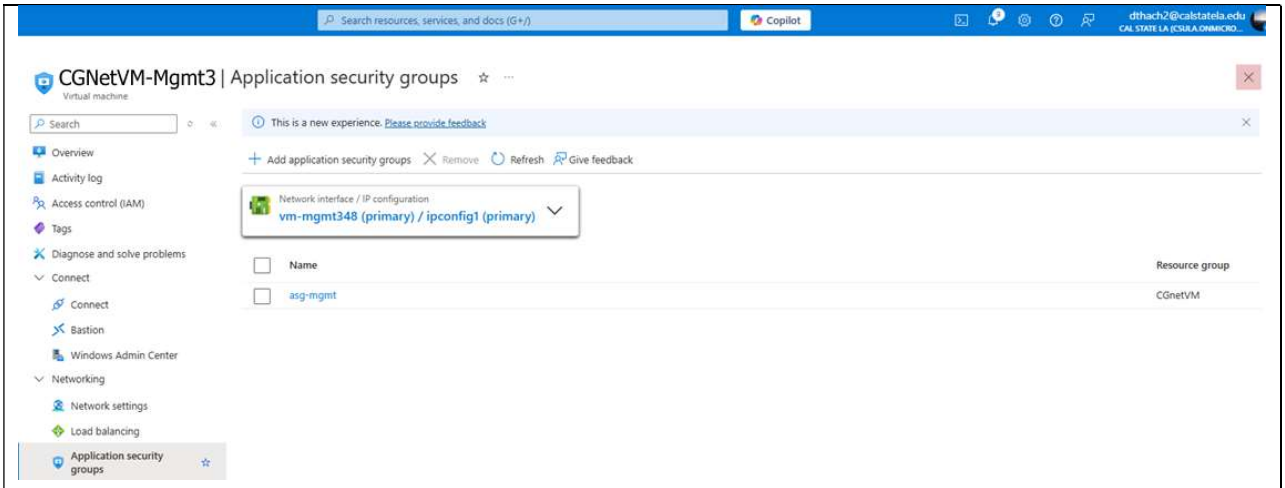


Figure 42: Security Group has been applied to the Management Server VM for third subnet. - D. Thach

4.6. Test traffic filters

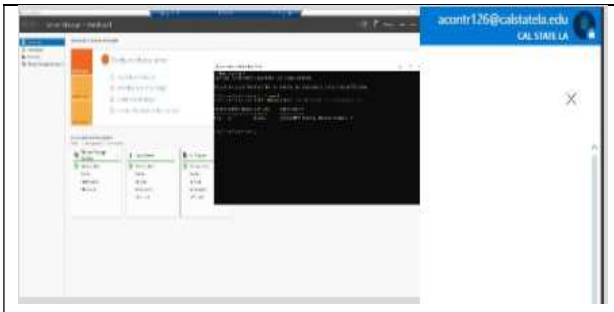
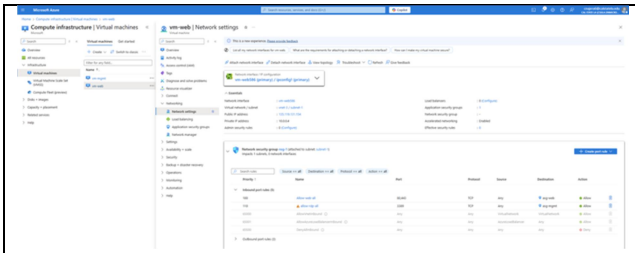


Figure 43: Using PowerShell to initiate connection commands proved successful

- A. Contreras

Figure 44: Successful webpage resulting in Default Microsoft webpage

- A. Contreras



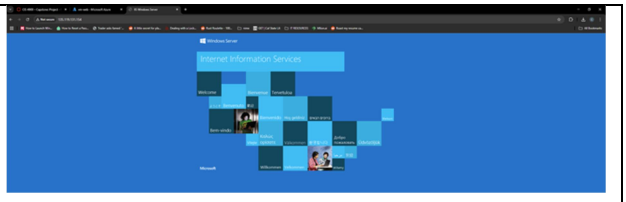


Figure 45: Web is allowed on VM-web **-** C. Najera	**Figure 46:** Successful connection to public IP of VM-WEB from browser **-** C. Najera

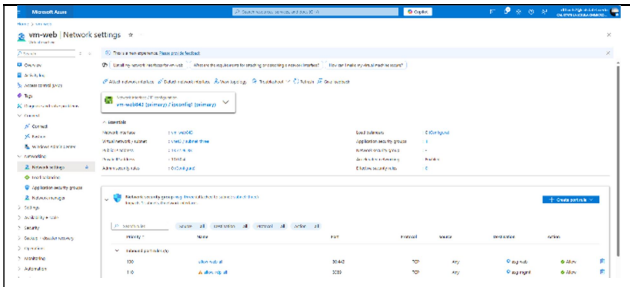
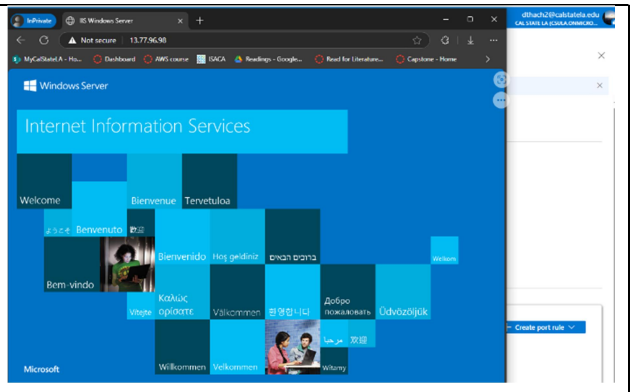
	

Figure 47: Inbound traffic of "Allow-Web-All" has been applied to the NSG for BILH test - D. Thach	**Figure 48:** Default Microsoft webpage for Information services, this means the test was successful based on the configurations **-** D. Thach

5. Route network traffic with a route table using the Azure portal

Routing network traffic is very important in cloud environments like Microsoft Azure because it ensures data reaches the right destination across large networks, securely, efficiently, and reliably. By default, especially in more complicated networks, the system does not initially know where to send traffic without specification from the network architect, this is where routing tables and associating subnet comes into play.

Azure uses two main types of routes:

System Routes – Created automatically by Azure to handle default traffic within a virtual network (VNet), between peered VNets, and to the internet.

User-Defined Routes (UDRs) – Custom routes that you create to control traffic paths, such as forcing traffic through firewalls or network virtual appliances (NVAs).

This customization makes sure that authorized traffic is allowed as specified and lets the system know where to send it.

Each route specifies:

Destination (IP range),

Next hop type (e.g., virtual appliance, internet, virtual network gateway),

Next hop IP (if applicable).

Routing tables are then associated with subnets to enforce the defined traffic flow.

5.1. **Create an NVA**

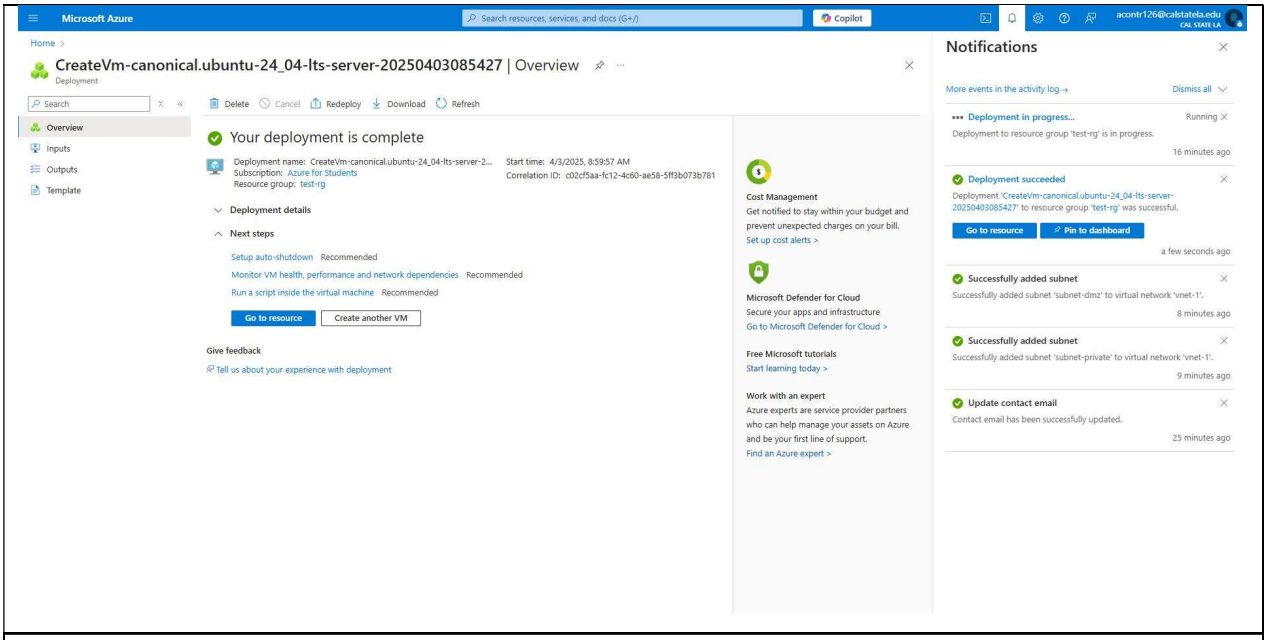


Figure 49: - A. Contreras

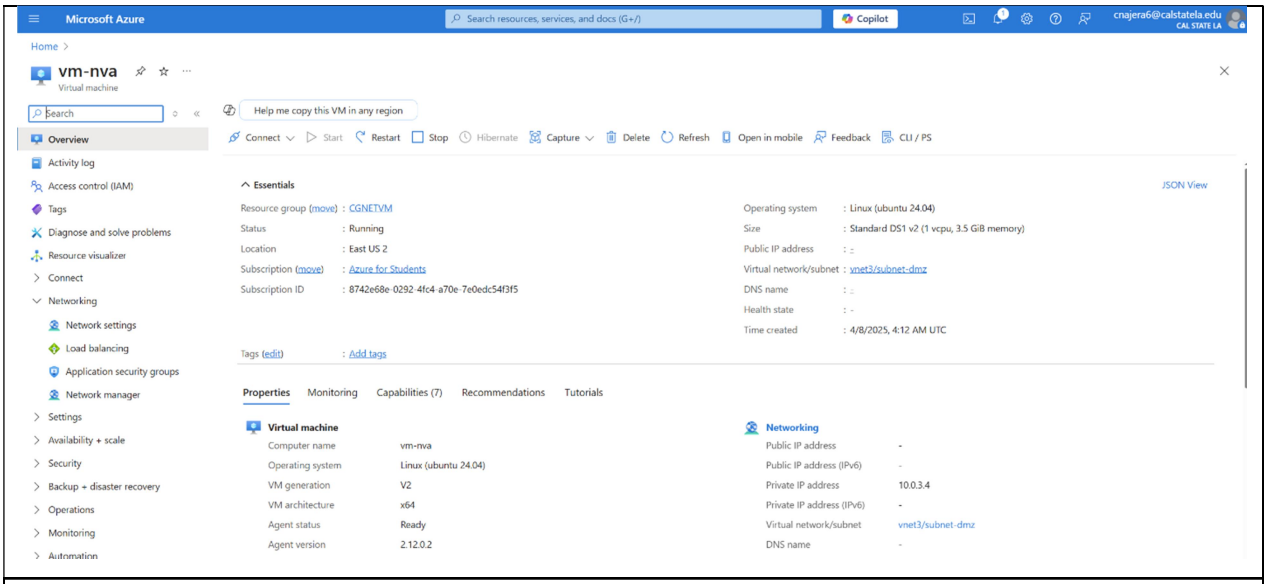


Figure 50: - C. Najera

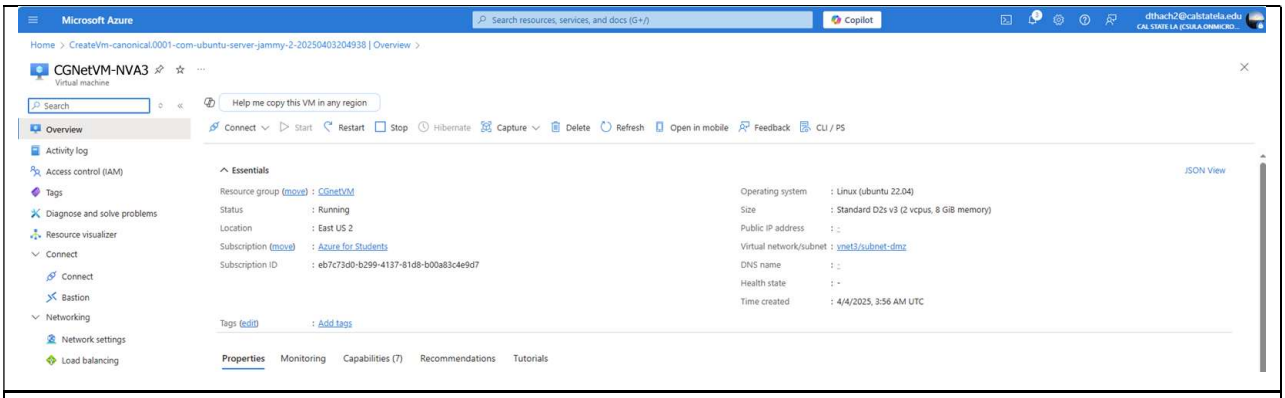


Figure 51: Creation of NVA machine for virtual network to provide function and services to the cloud platform **-** D. Thach

5.2. Create a route table

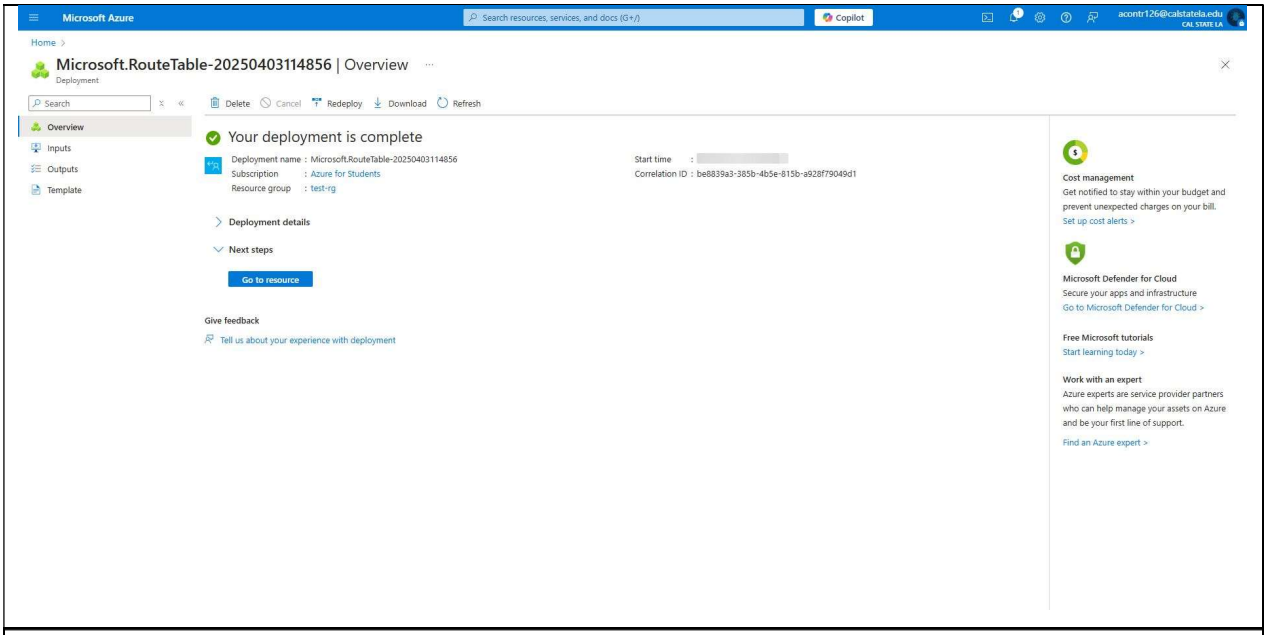


Figure 52: - A. Contreras

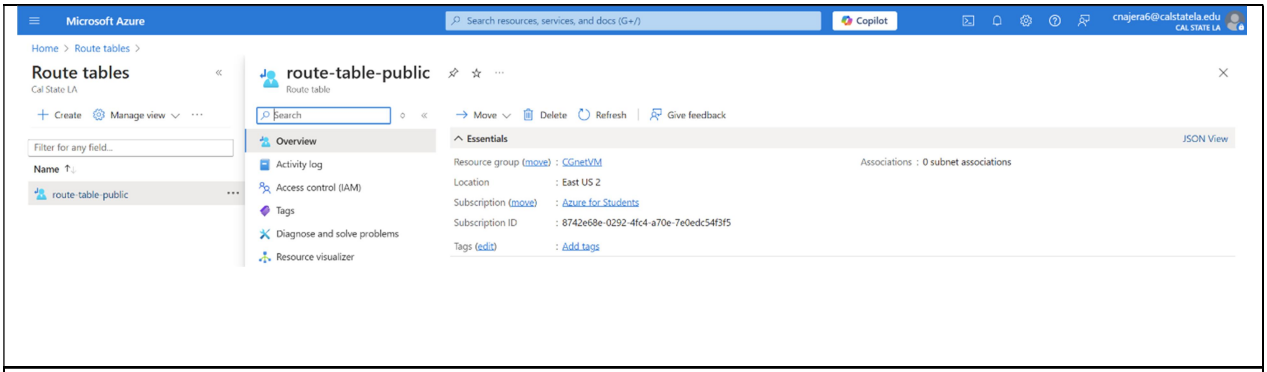


Figure 53: - C. Najera

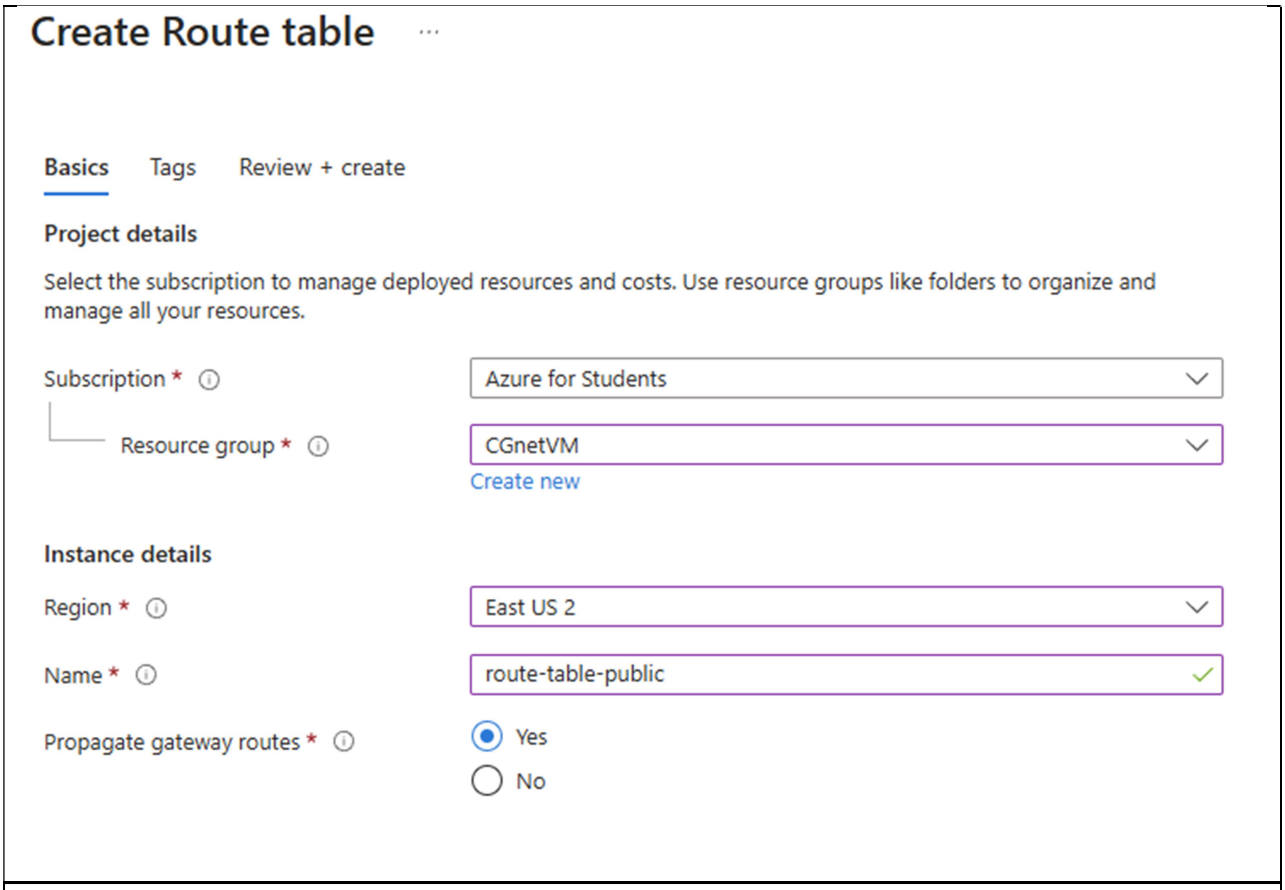


Figure 54: Route table create to add routes to forward IP on the virtual network - D. Thach

5.3. Create a route

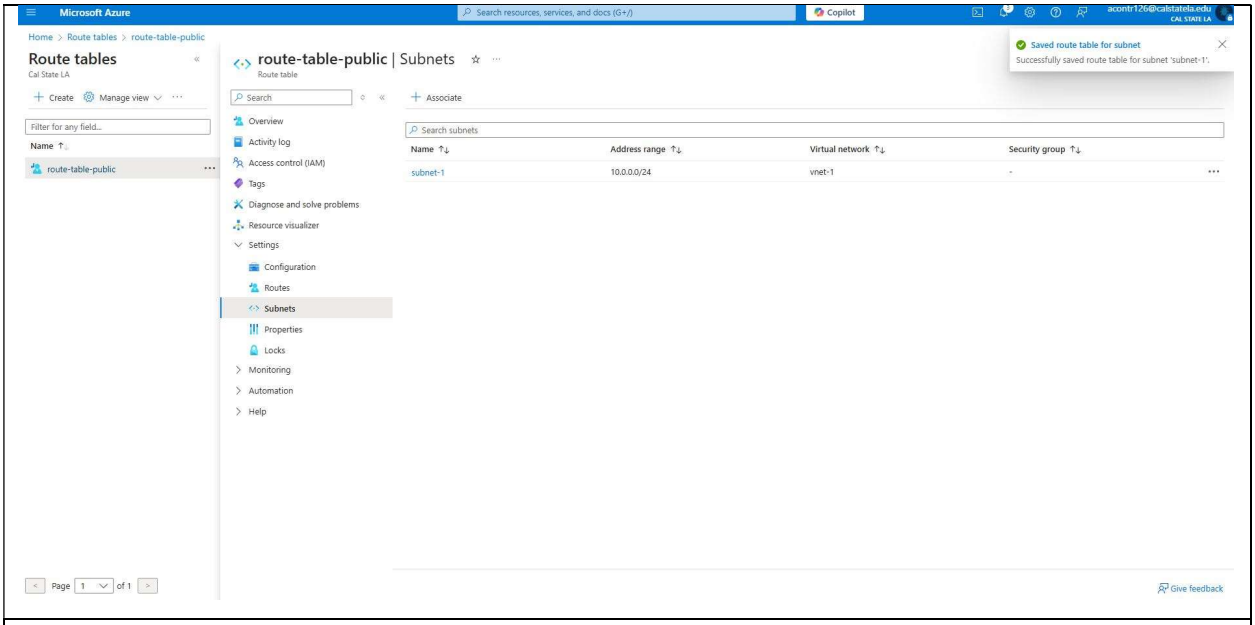


Figure 56:

- A. Contreras

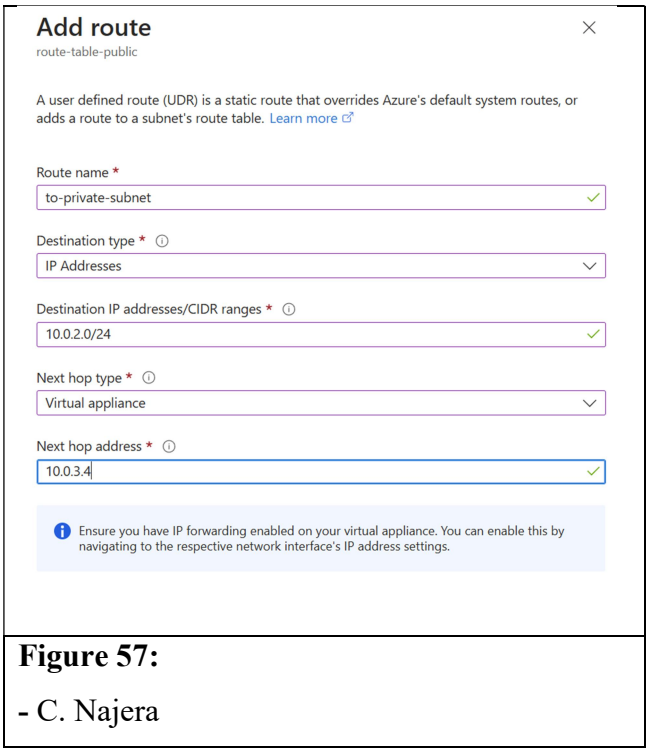
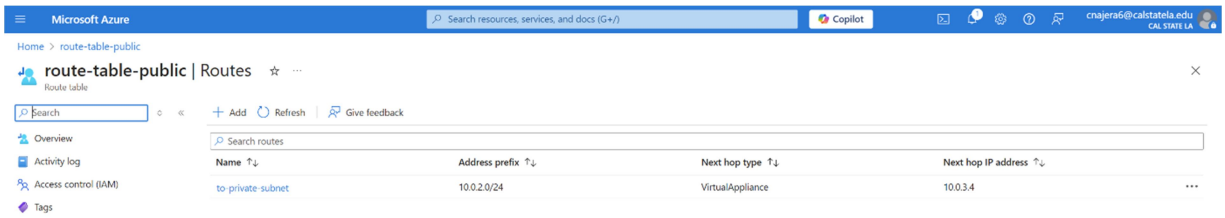


Figure 57:

- C. Najera

Figure 58:



- C. Najera

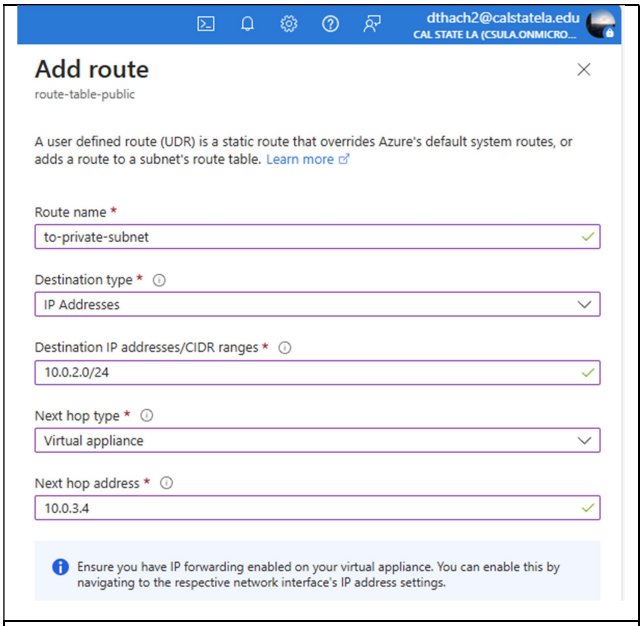


Figure 59: Added route to the routing table that shows path from private network to the DMZ

- D. Thach

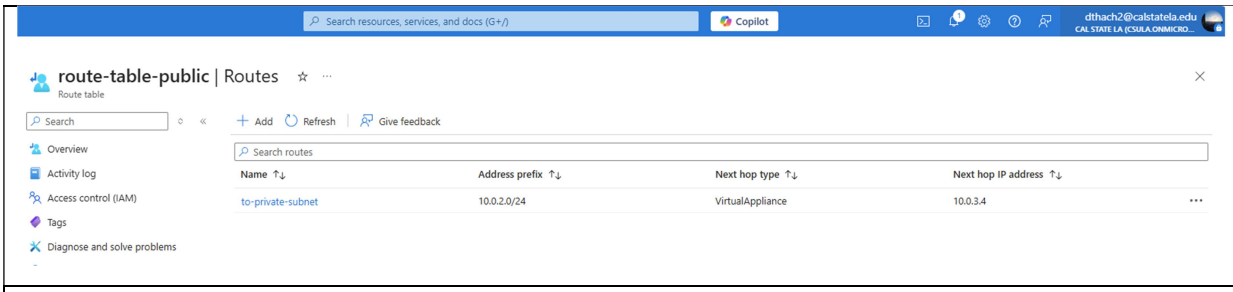


Figure 60: Added a route to the routing table, this is a picture to verify the system has accepted the routing configurations.

- D. Thach

5.4. **Associate a route table to a subnet**

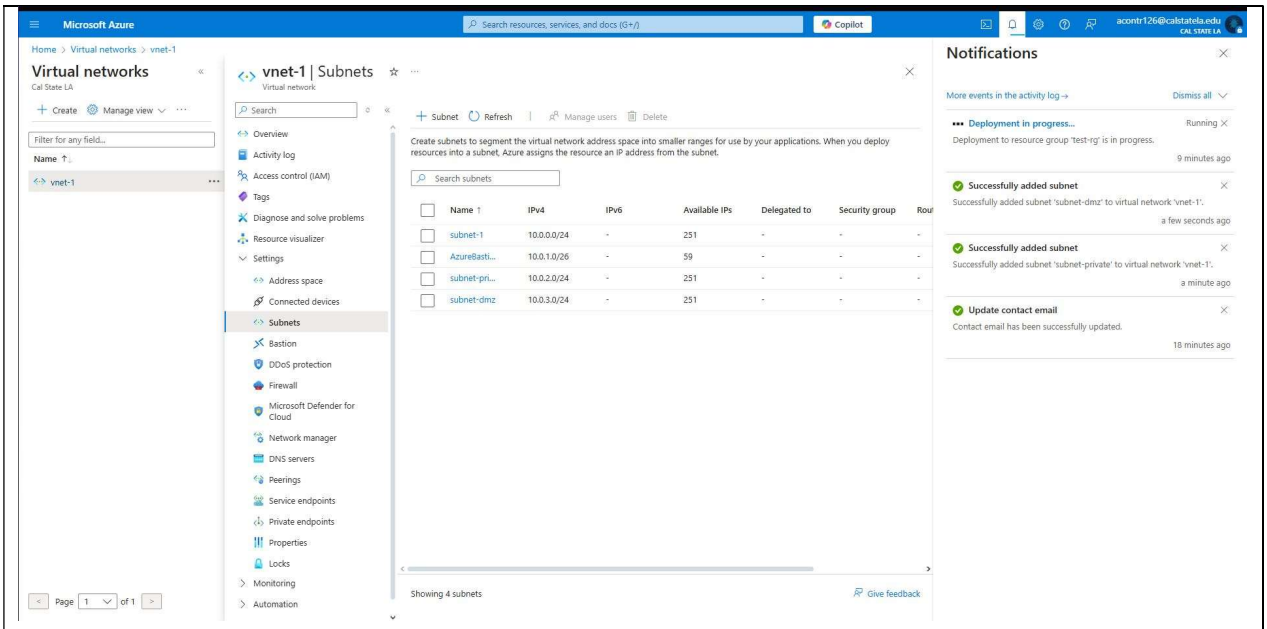


Figure 61: - A. Contreras

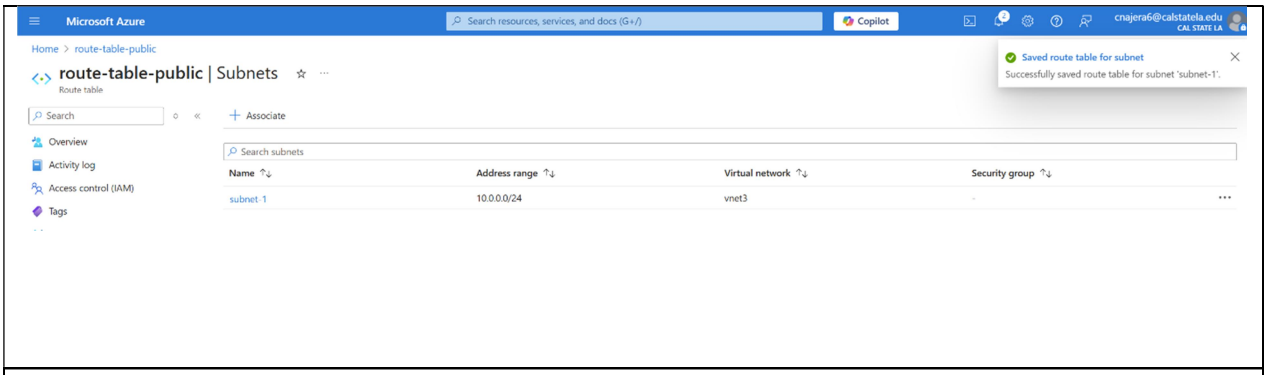


Figure 62: - C. Najera

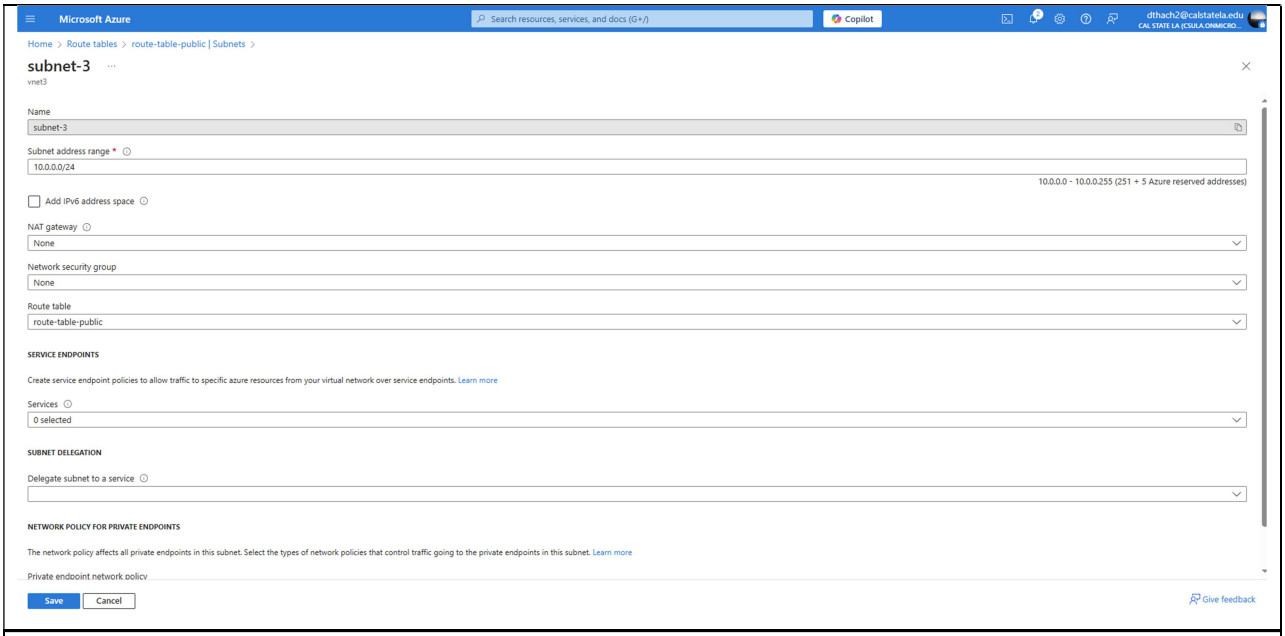


Figure 63: Creation of subnet 3, theses are the configurations for the process. **-** D. Thach

5.5. Turn on IP forwarding

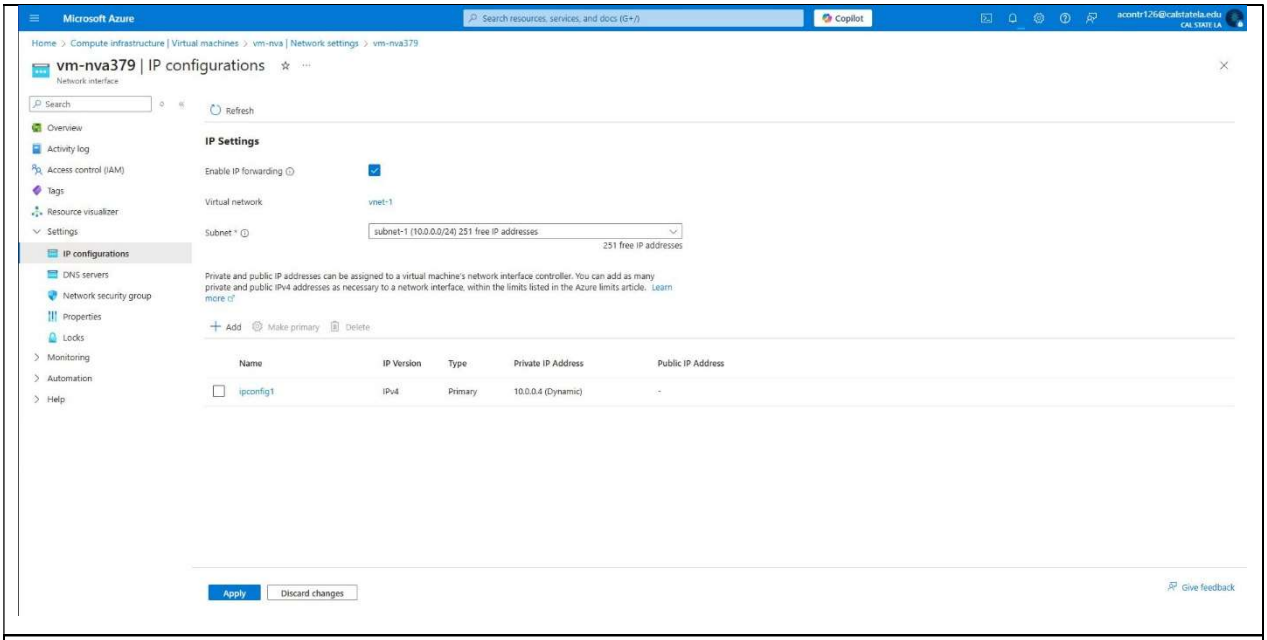


Figure 64: - A. Contreras

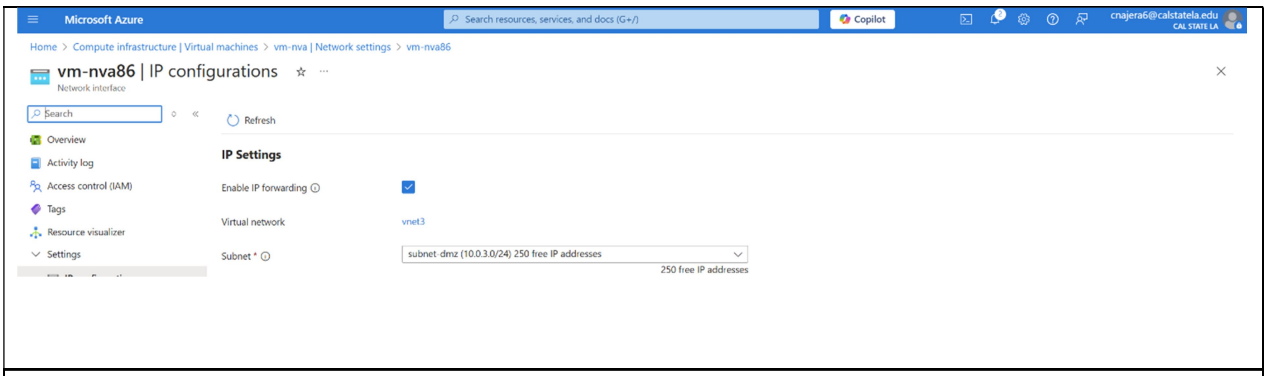


Figure 65: - C. Najera

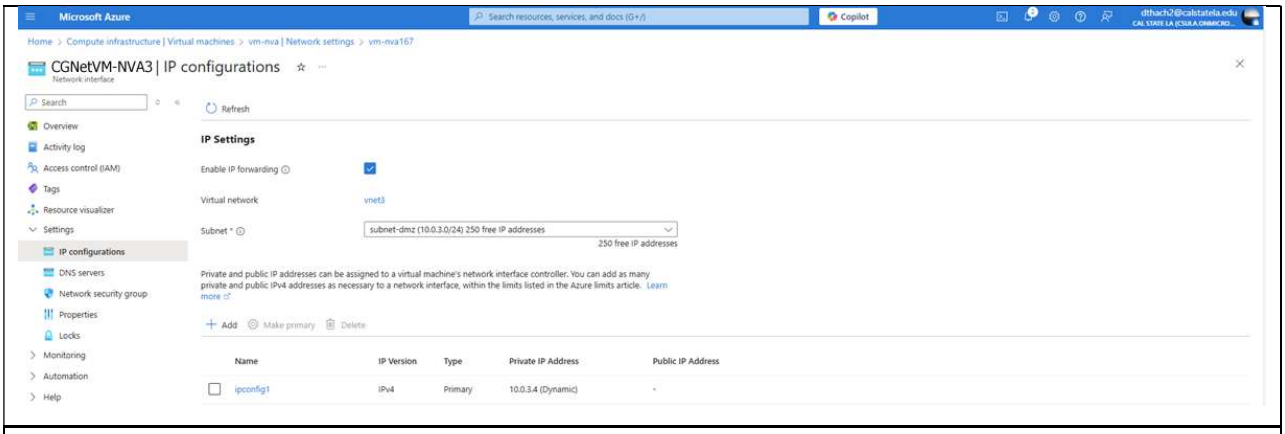


Figure 66: IP forwarding has been enabled to route the traffic configured from the routing table **-** D. Thach

5.6. Create a public and private virtual machines

Various advantages and disadvantages between the use of public and private virtual machines are present in this project regarding creating a virtual network. In this section, we will weigh both the advantages and disadvantages of having either and give input on why they are still valuable.

First, we must define a public and private virtual machine. A public virtual machine is a VM with a public IP address that can be accessed and communicate with other endpoint users online. These kinds of virtual machines are used to host public-facing databases or servers. It usually hosts content meant to be accessed by others on the internet, whether a service or application such as an API or web server. A private virtual machine is more secure, and while it is connected to the internet, it is not truly exposed to it and requires special tools or configurations to access it, such as VPNs or bastion hosts. These machines often relay more sensitive information for internal operations and sensitive data processing (Microsoft, 2024a; Susnjara & Smalley, 2024).

5.6.1. Advantages and Disadvantages of Public Virtual Machines

Advantages	Disadvantages
1. **Convenient Accessibility:** Public virtual machines are accessible from any eligible device on the internet to connect because they have a public IP (internet protocol address). Suppose Lahey Health wants users to utilize their machines to conduct operations such as scheduling appointments and sending requests when deploying their services to fit those needs on a public machine(Microsoft, 2024a).	1. **Security Risk:** Typically, you would not have any risk towards the data being kept on public VMs, but since they are public on the internet, it exposes the machines to other threats. DDoS attacks, unauthorized access, and malware are threats that can harm people's access to the machine and thus reduce accessibility to the service many may rely on. Another threat is the human error of bad configuration or a patch that does not have a rollback option in case there are bad configurations (Susnjara & Smalley, 2024).
2. **Cost Efficiency:** Without hardening the security, these machines are more budget-friendly and would only have costs tied to overhead and cloud hosting rates. Lahey could benefit from the money these machines saved and reinvest it in other network sectors or their business(Microsoft, 2024a).	2. **Compliance:** The industry standards and laws are constantly changing, so it is advised to have any sensitive data be volatile on the public machine and stored away on a private network. Though there will be exploits to the machine, and maybe new laws will challenge and complicate how these front-facing machines will operate, it may become more trouble than it is worth to keep them operational.
3. **Compatibility:** Public VMs are compatible with external services like APIs or online SaaS platforms. This means that deploying these machines is fast and functional, which is	3. **Limited Scalability:** Even with the correct configurations, public VMs only have the bare minimum to operate at a specific capacity, so performance will decline if there is a massive usage of data from end users.

important for Lahey(Microsoft, 2024a).	This can be circumvented with load balancing or auto-scaling configurations.

5.6.2. Advantages and Disadvantages of Public Virtual Machines

Advantages	Disadvantages
1. **Hardened Security:** Private VMs operate in a closed environment, minimizing their exposure to the open internet. This reduces the risk of them being attacked by threats.	1. **Limited Accessibility:** Private VMs require authentication and external tools to access because they are tucked away in a closed/limited network. It may not work in favor of Lahey Health if the organization struggles to acquire frequently used data, and it harms its business efficiency.
2. **Regulated:** By nature of their operations and needs, often sensitive data are processed on private machines, and with the only way to access them held by VPNs and other configured tools, typically only those with access to the layered authentication use see the activities. It would comply with HIPPA standards in Lahey Health's case.	2. **Complex Management:** Private VMs must be maintained frequently and monitored more often than public VMs. This means that more time is spent on audits and may require scaling depending on the purpose of the machine that was deployed. It also takes more time to deploy a VM for private use because of the configurations that will be used to ensure that it aligns with the laws and business objectives.
3. **Monitored Networking:** Private VMs often have more importance than public VMs, and they will often have configurations set, such as subnet routing, firewalls, and rules. It also makes it easier to monitor the machine's activities.	3. **Higher Cost:** Private VMs have high upkeep because of the load they are tasked with processing, which requires host machines/services to be high-end. It also eats up more cost because they will use higher tier configurations that would cost more to host on a PaaS or Host machine's overhead (Susnjara & Smalley, 2024).

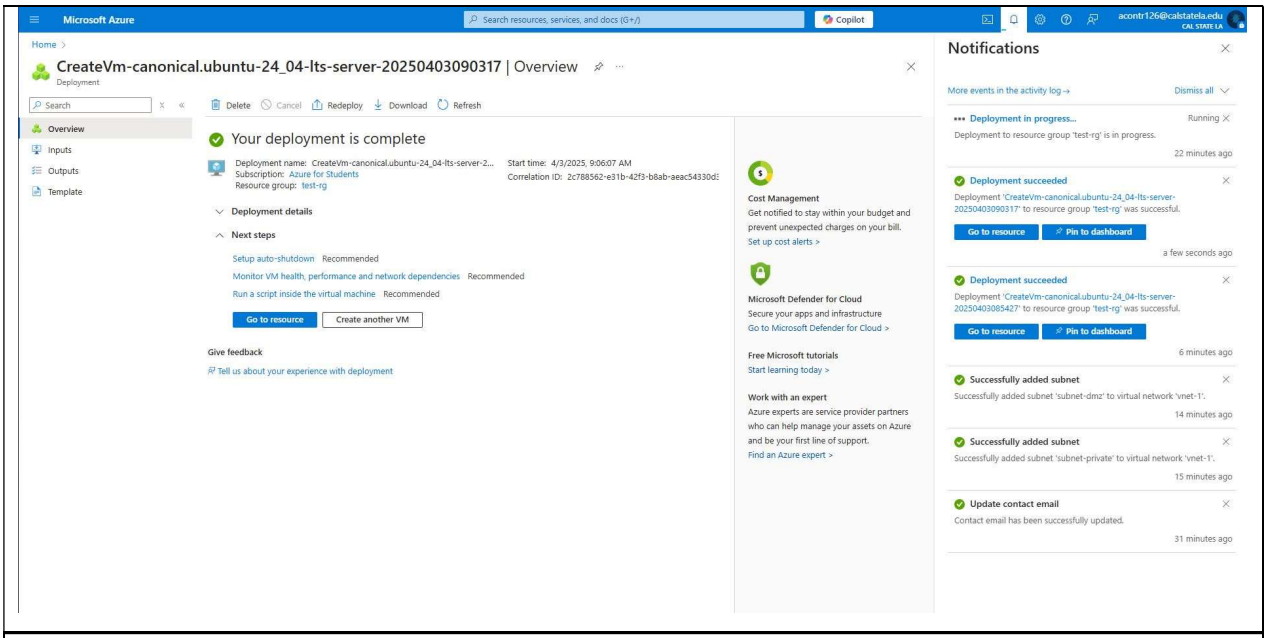


Figure 67: - A. Contreras

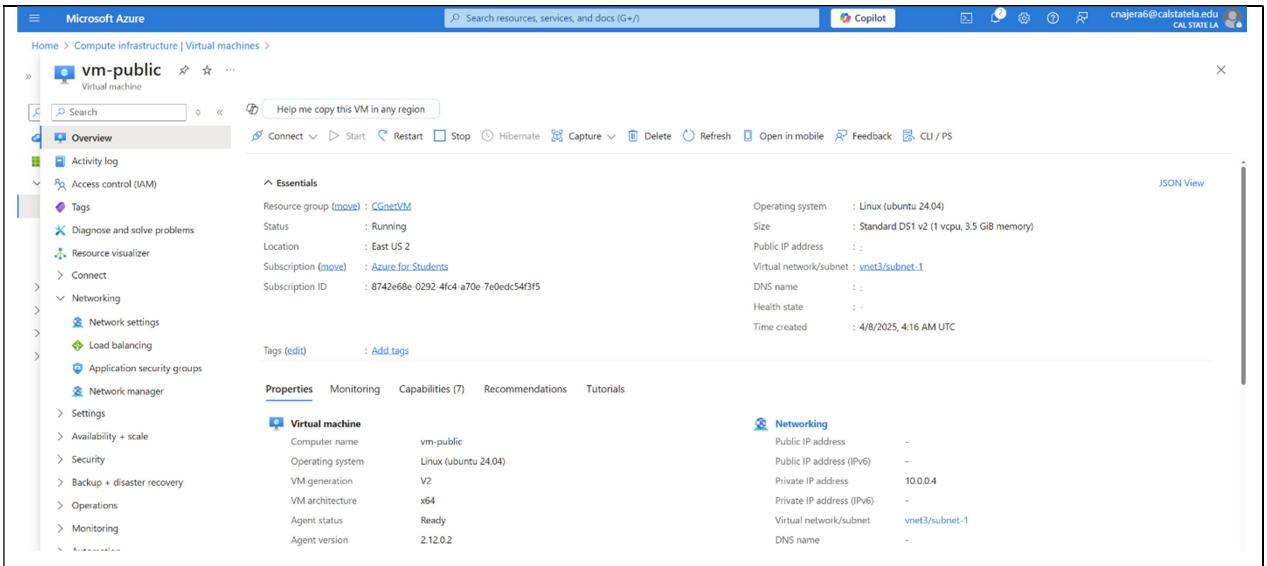


Figure 68: - C. Najera

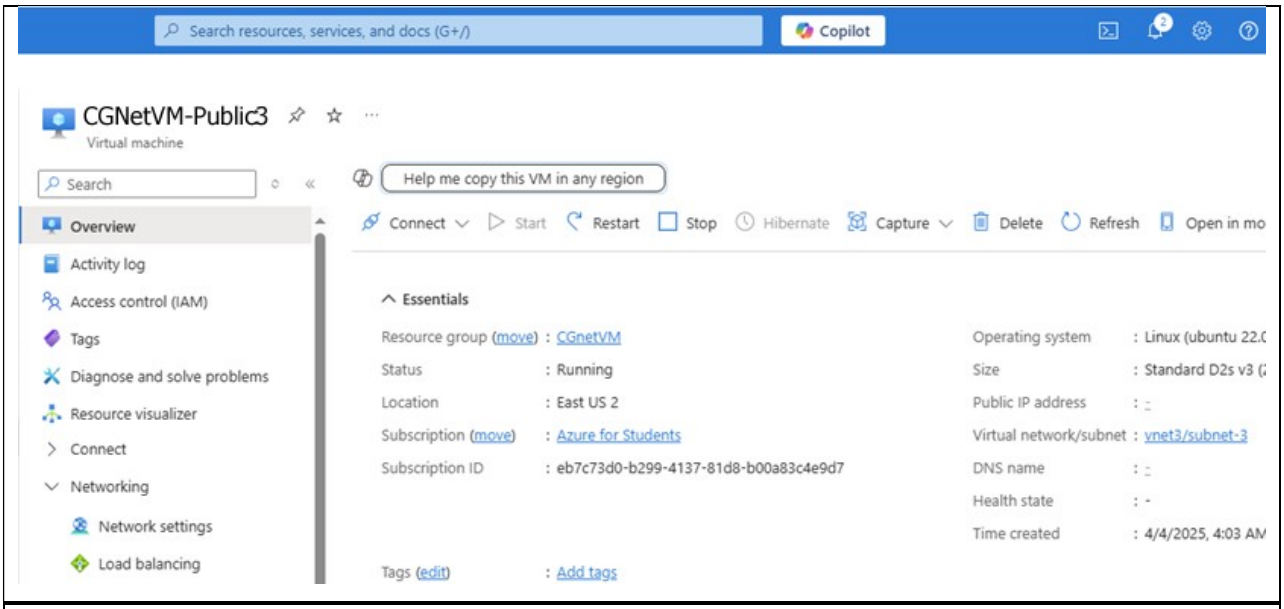


Figure 69: Public Virtual machine has been create within the resource group to be a part of the network to test routing **-** D. Thach

5.6.3. Private VM

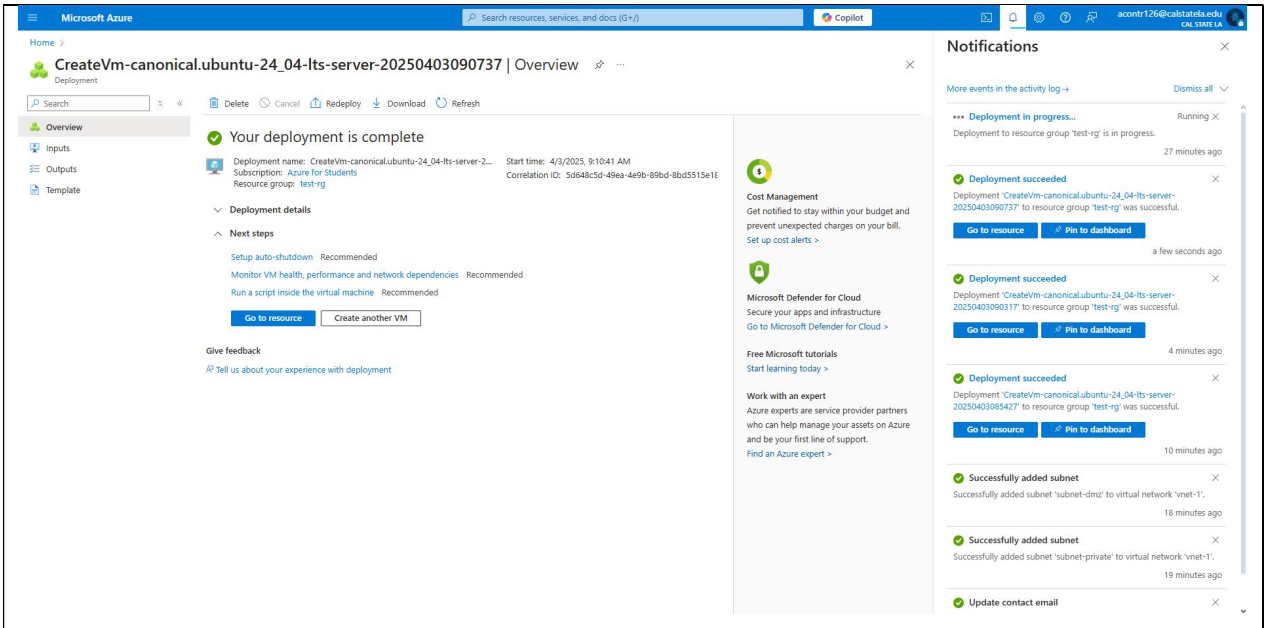


Figure 70: - A. Contreras

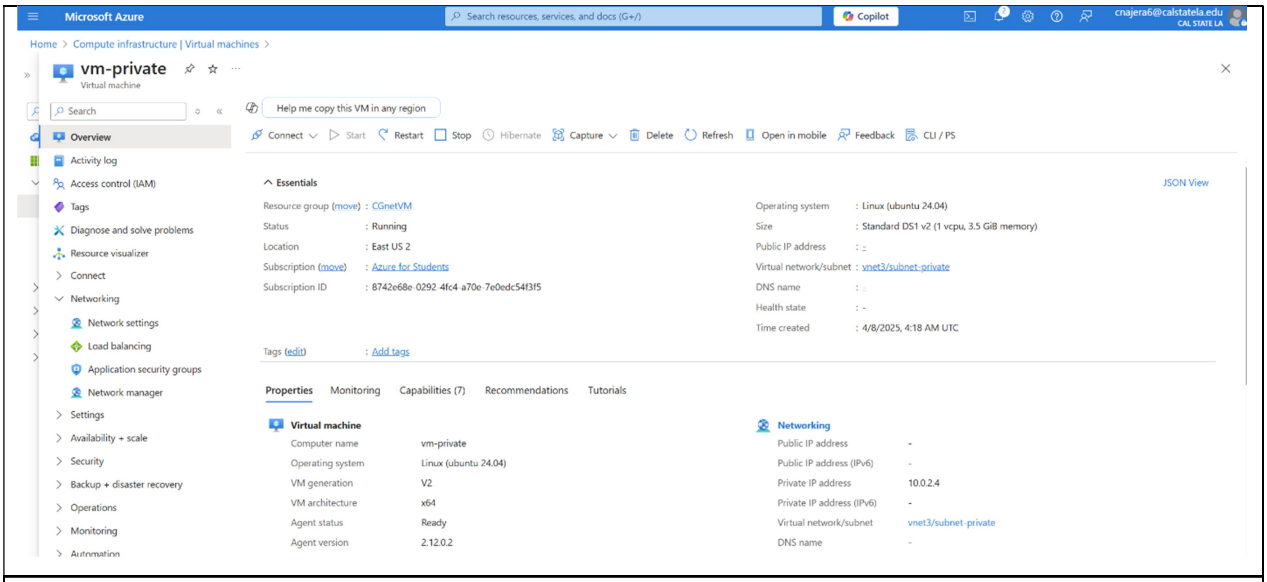


Figure 71: - C. Najera

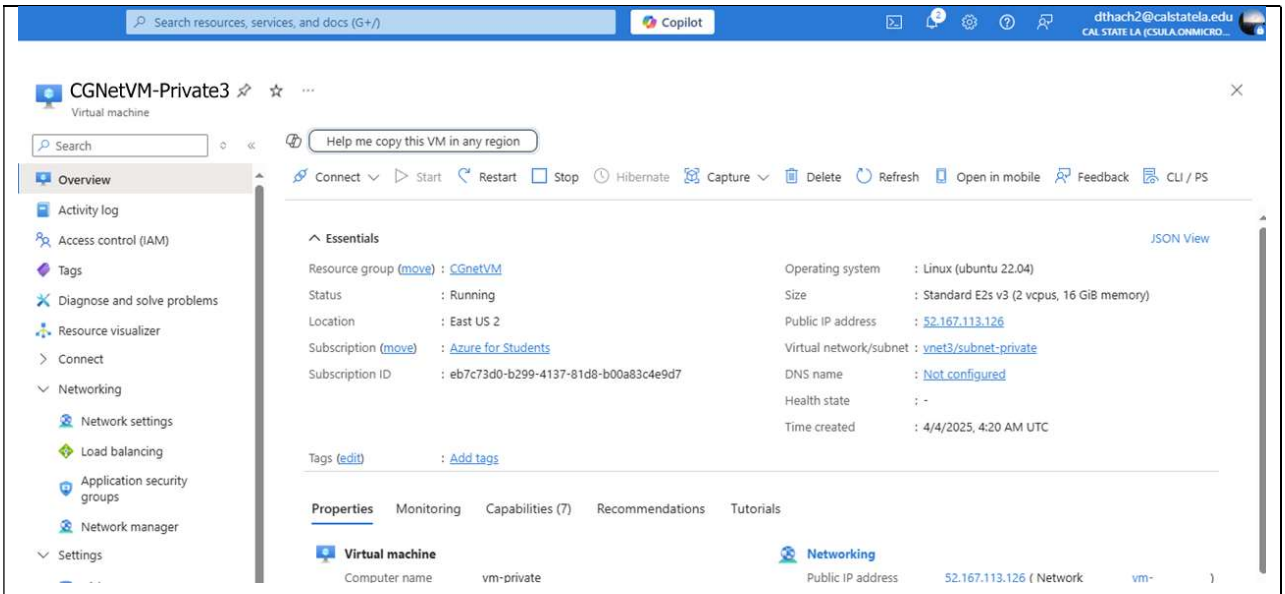


Figure 72: Private virtual machine create to test the routing configurations of the network in the Azure Resource Group- D. Thach

5.7. **Route traffic through an NVA**

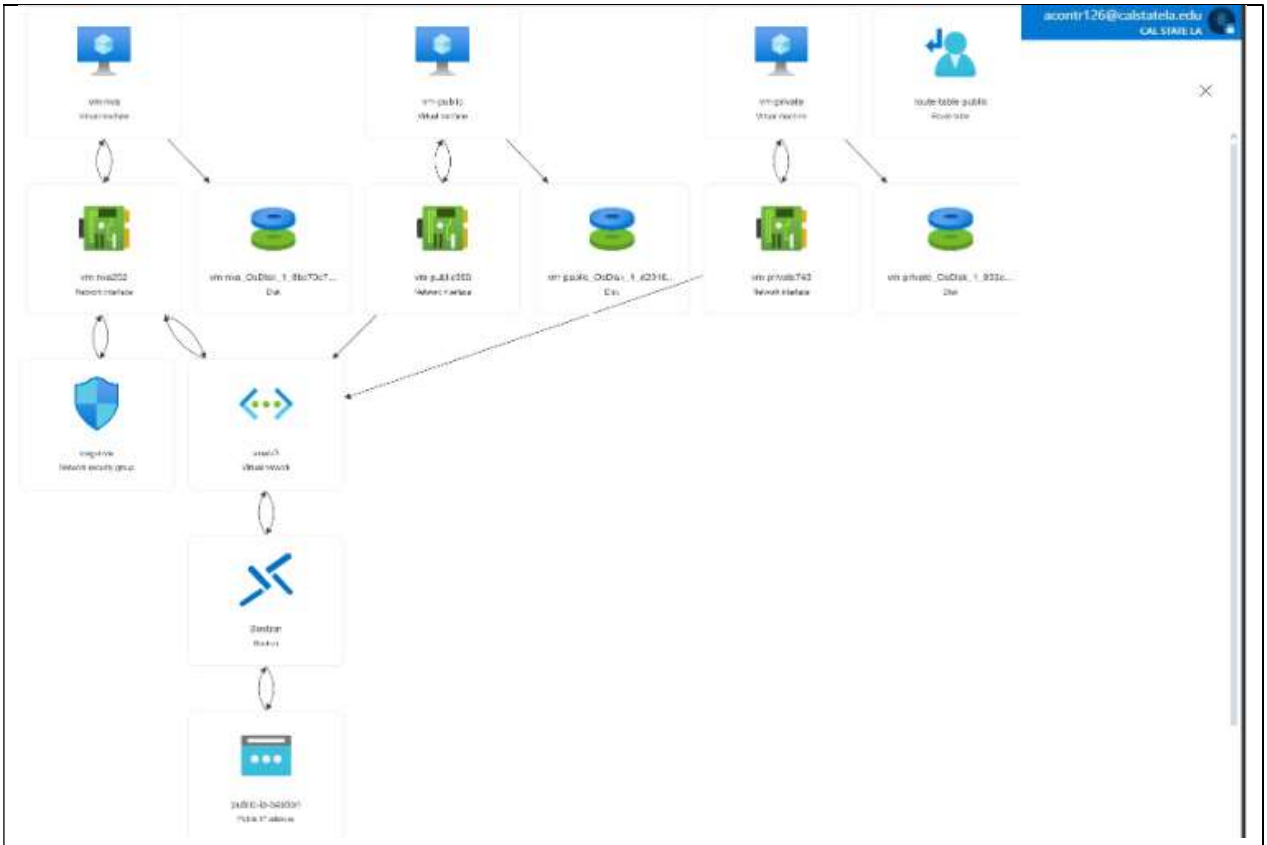


Figure 73: - A. Contreras

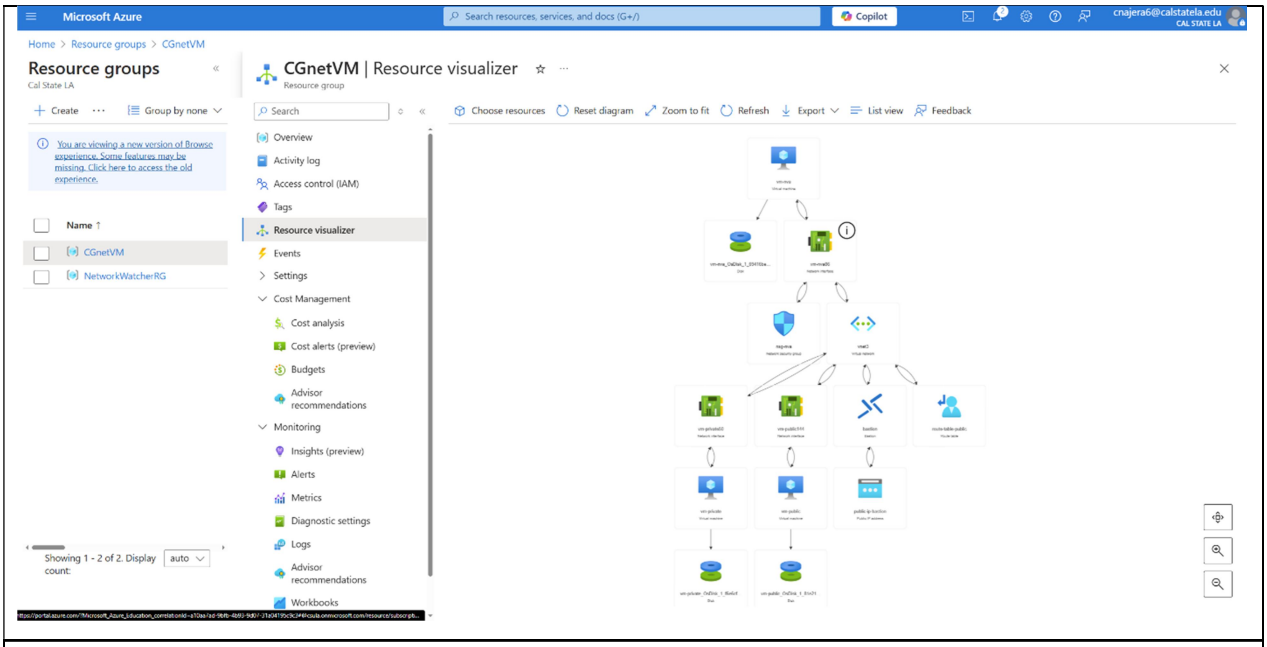


Figure 74: - C. Najera

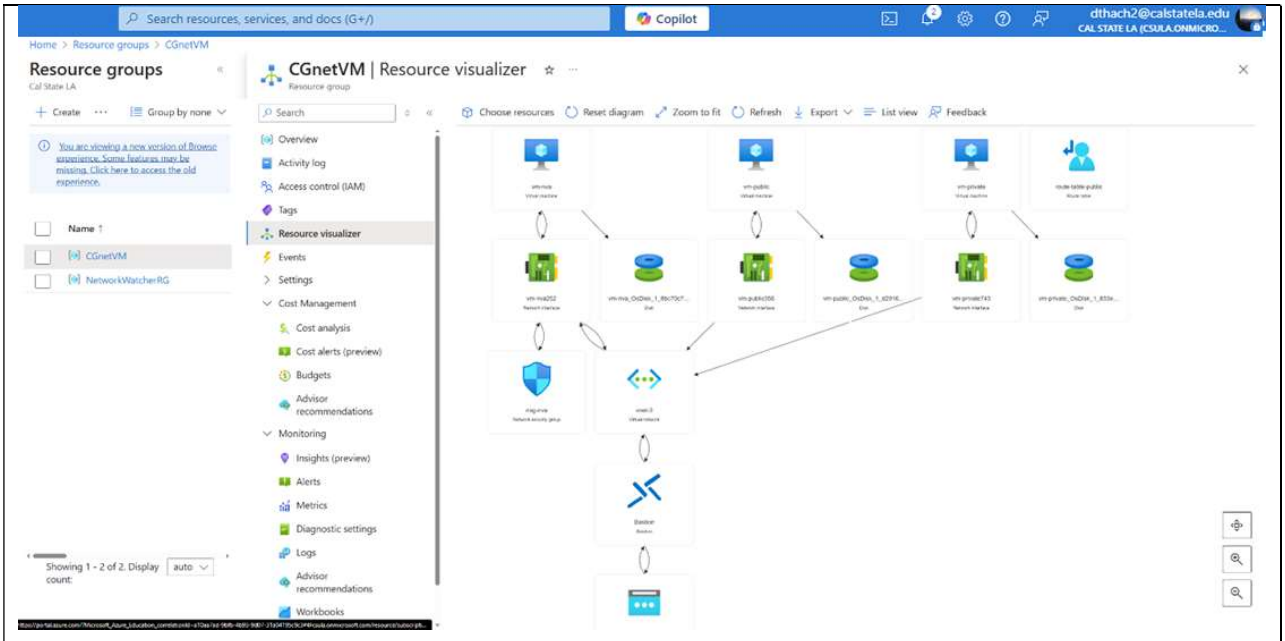


Figure 75: Depiction of the topology using the resource overview mapping tool found in the Azure Resource Group views; depicts how this network will function with the resources created **-** D. Thach

5.8. Sign in to myVmPrivate over remote desktop

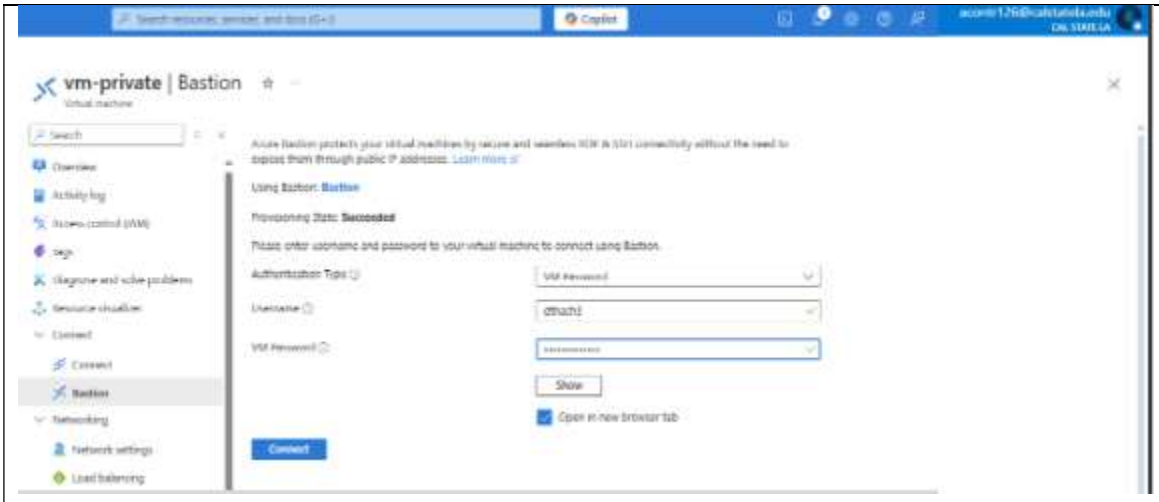


Figure 76: - A. Contreras

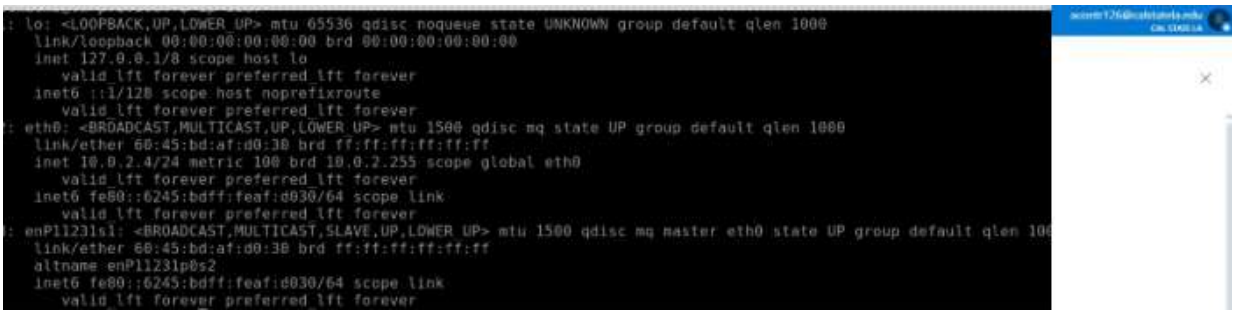


Figure 77: - A. Contreras

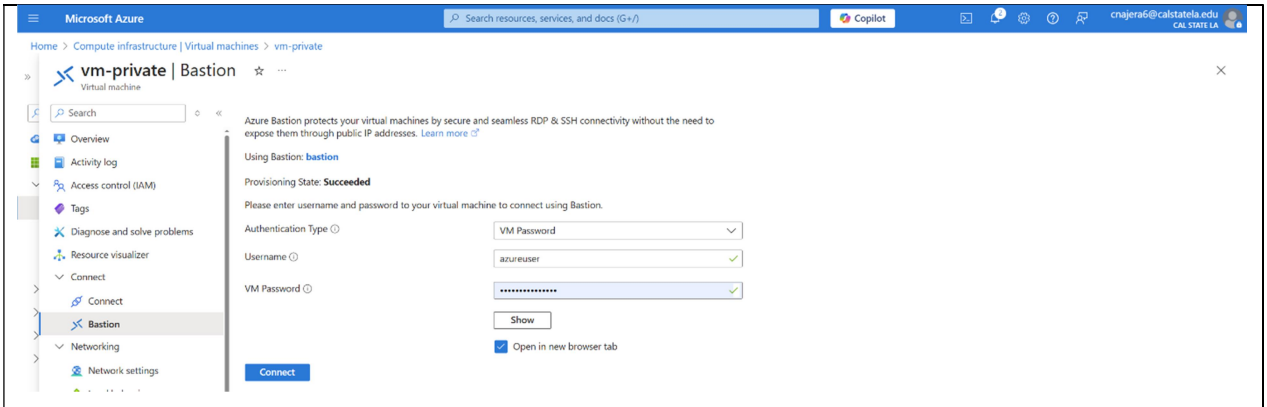


Figure 78: - C. Najera

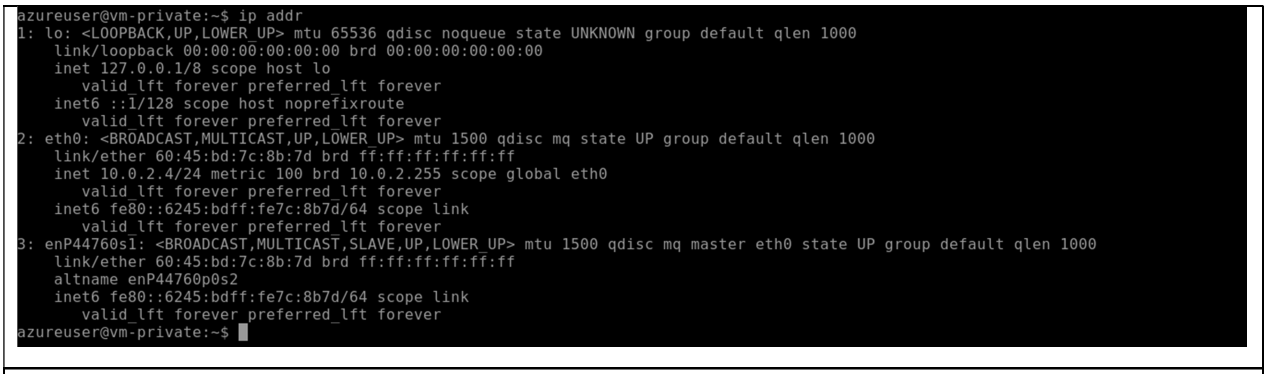


Figure 79: - C. Najera

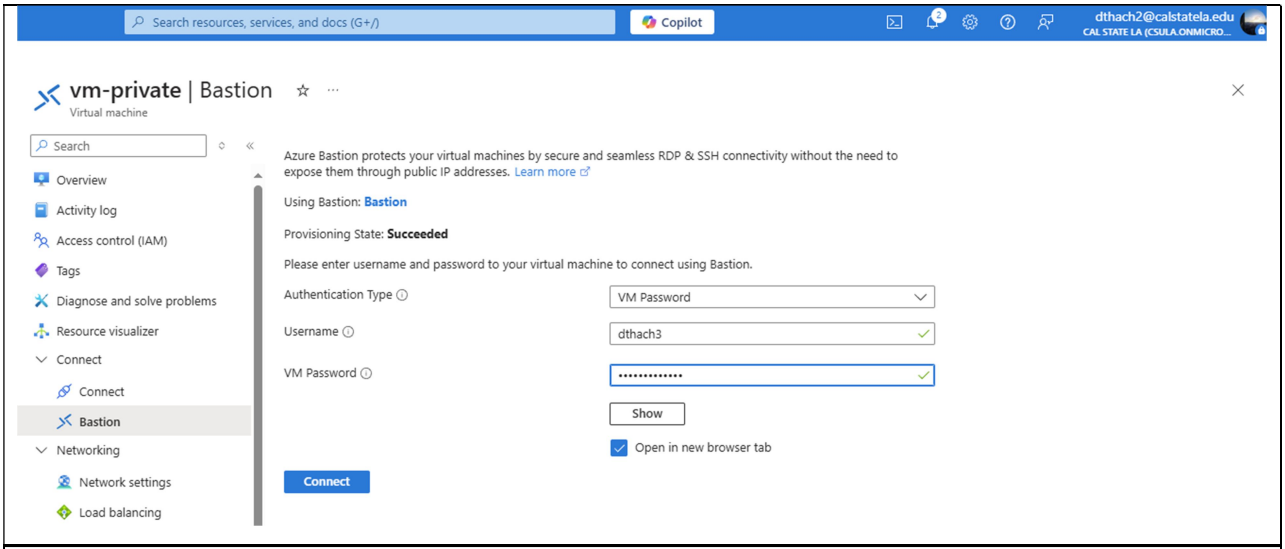


Figure 80: Using Bastion Host to access the private VM **-** D. Thach

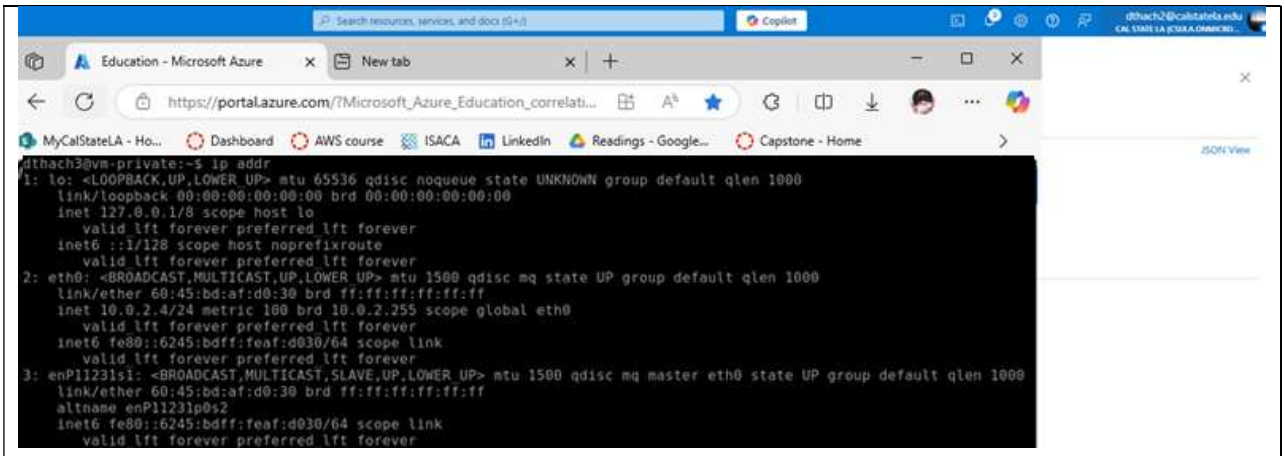


Figure 81: IP config or Linux machine, the lines display the status of IPv4 in the test and their

relevant address- D. Thach

5.9. Enable ICMP through the Windows firewall

Figure 82: - A. Contreras

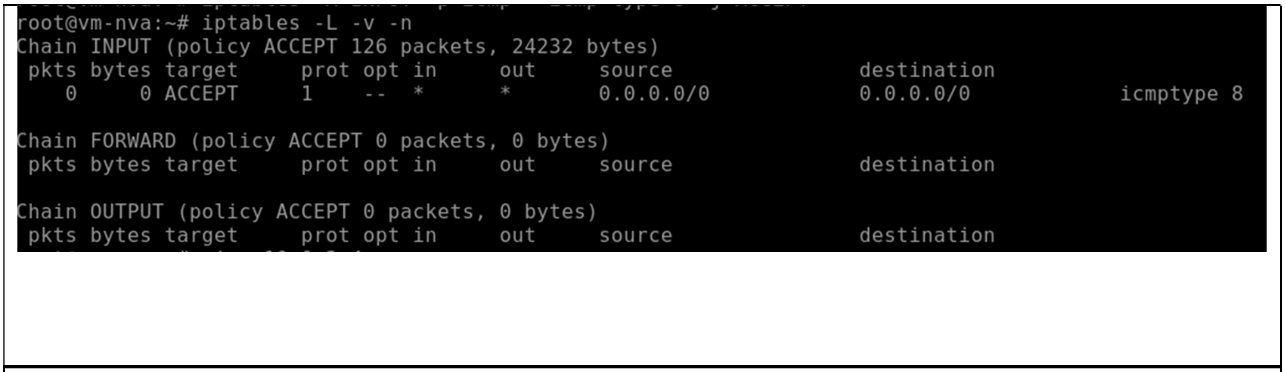


Figure 83: - C. Najera

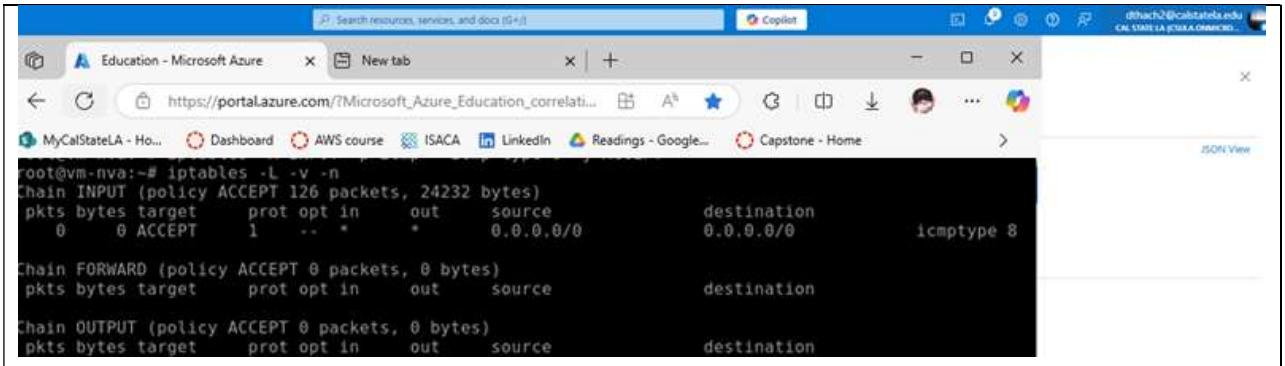


Figure 84: Allowed the TCP/IP protocol ICMPv4 through Linux commands **-** D. Thach

5.10. **Turn on IP forwarding withing myVmNva**

Figure 85: - A. Contreras

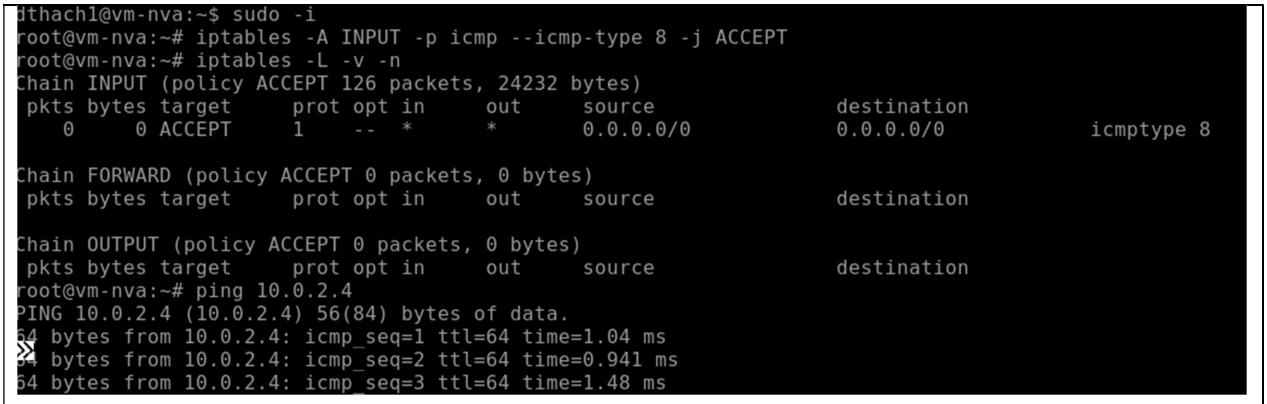


Figure 86: - C. Najera

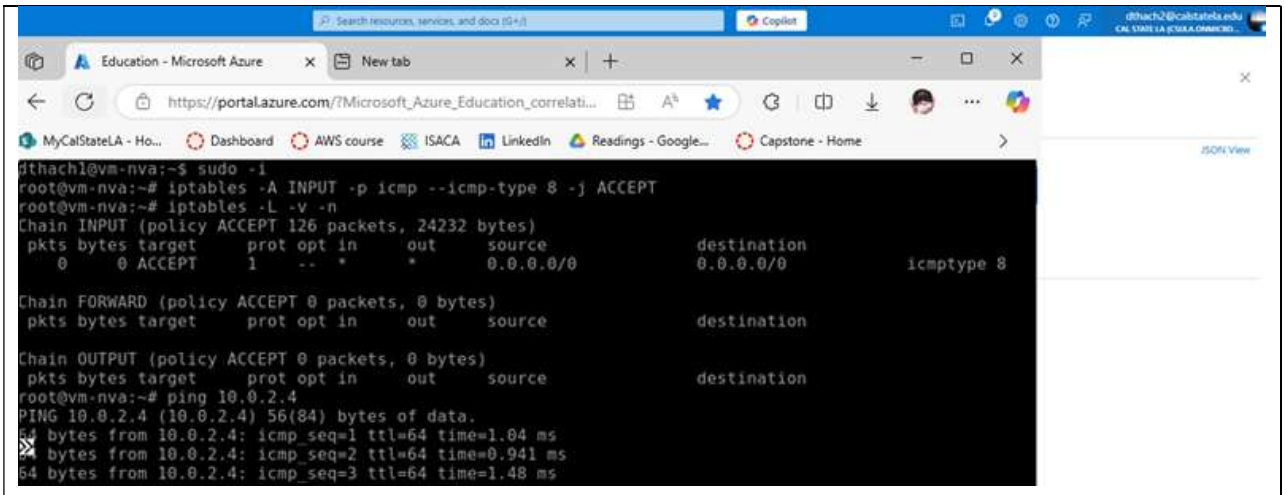


Figure 87: Showcasing the script used to generate rule and allow traffic for Nva machine and testing out the function by pinging the public virtual machine **-** D. Thach

5.11. **Test the routing of network traffic**

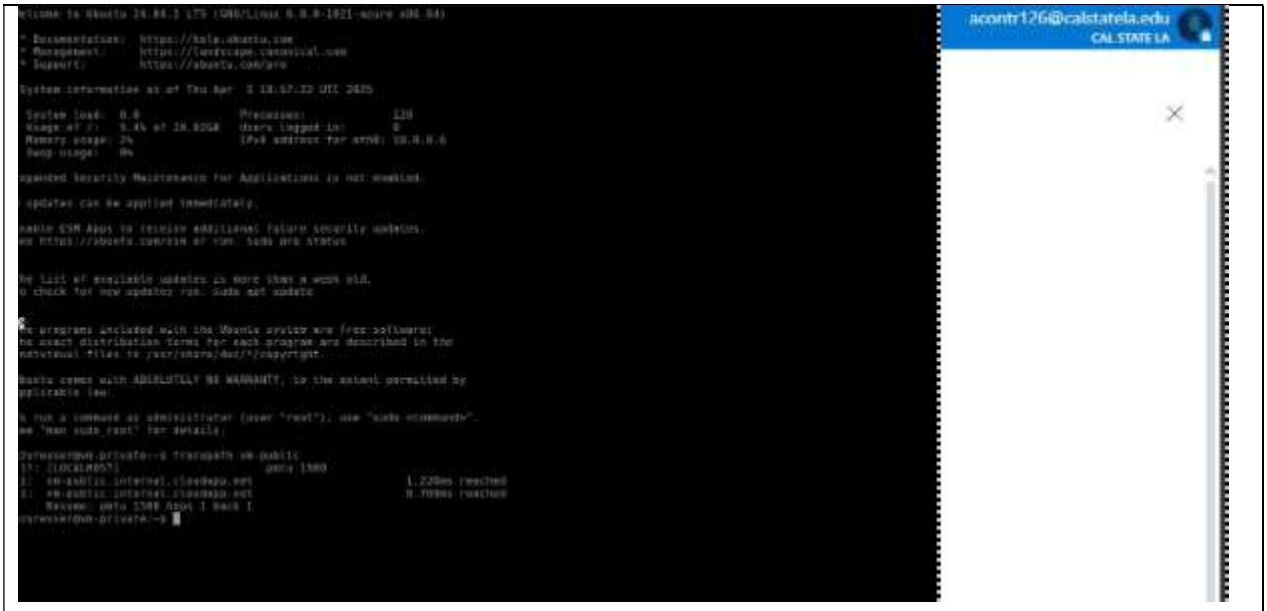


Figure 88: - A. Contreras

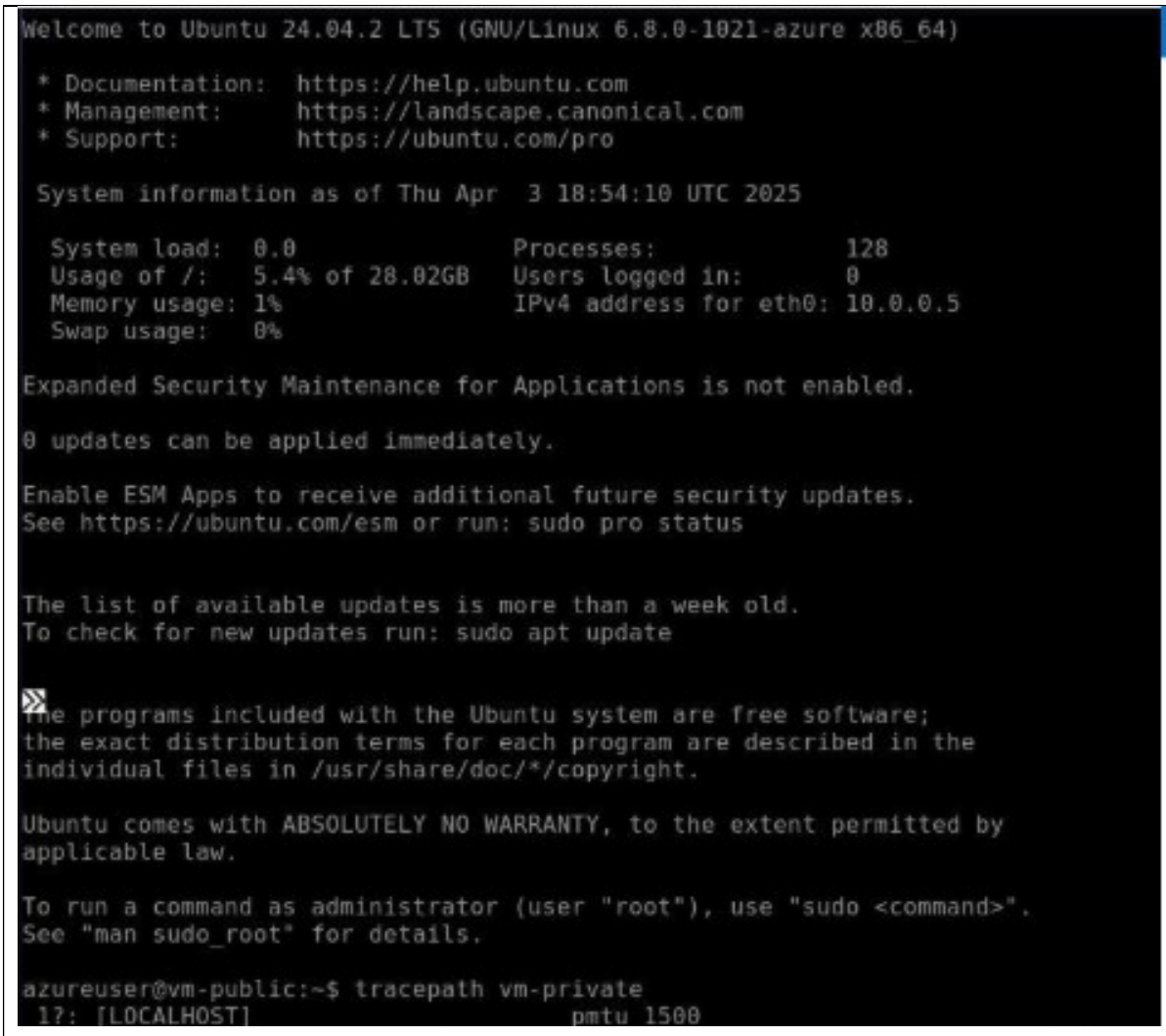


Figure 89: - A. Contreras

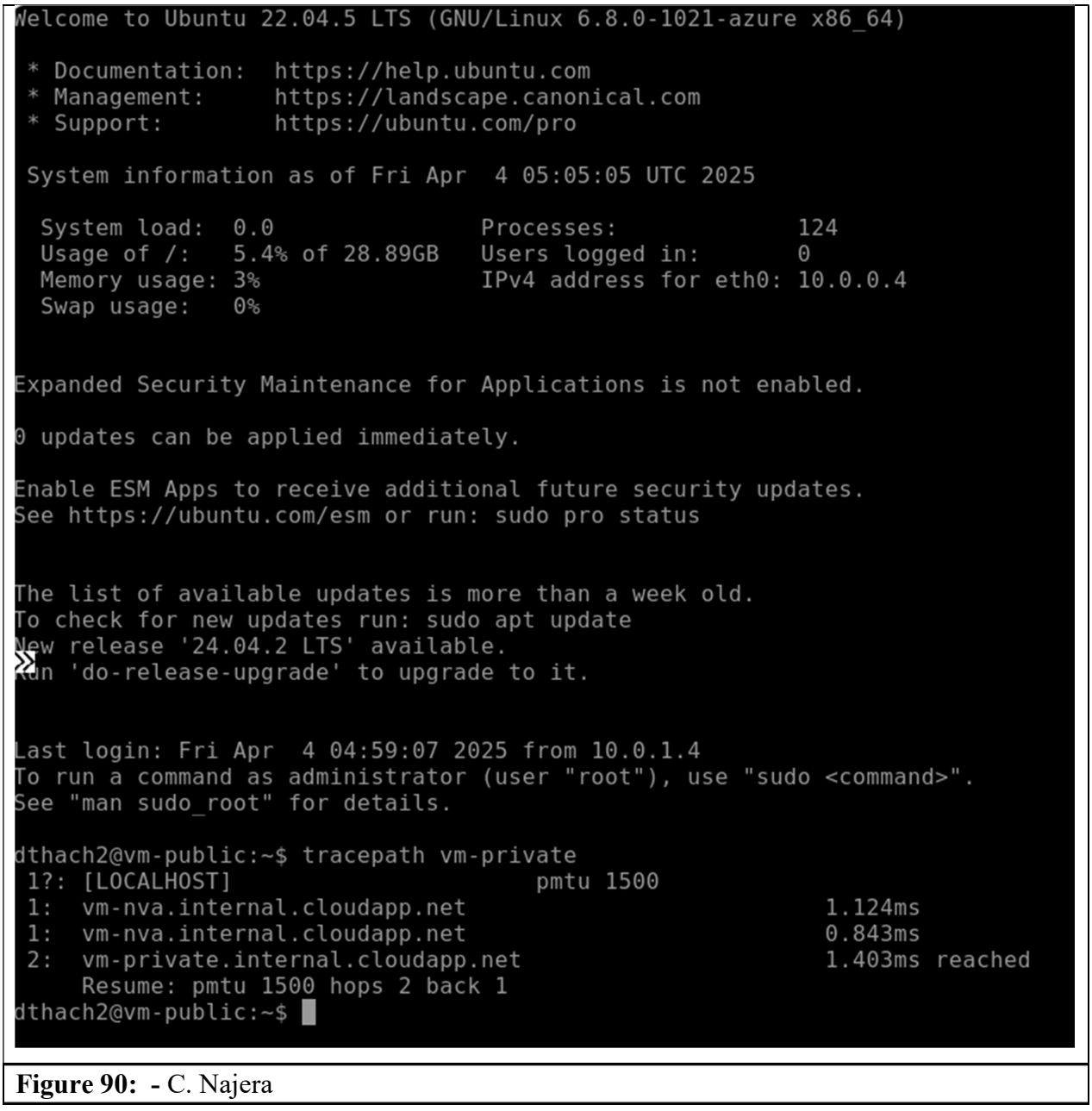


Figure 90: - C. Najera

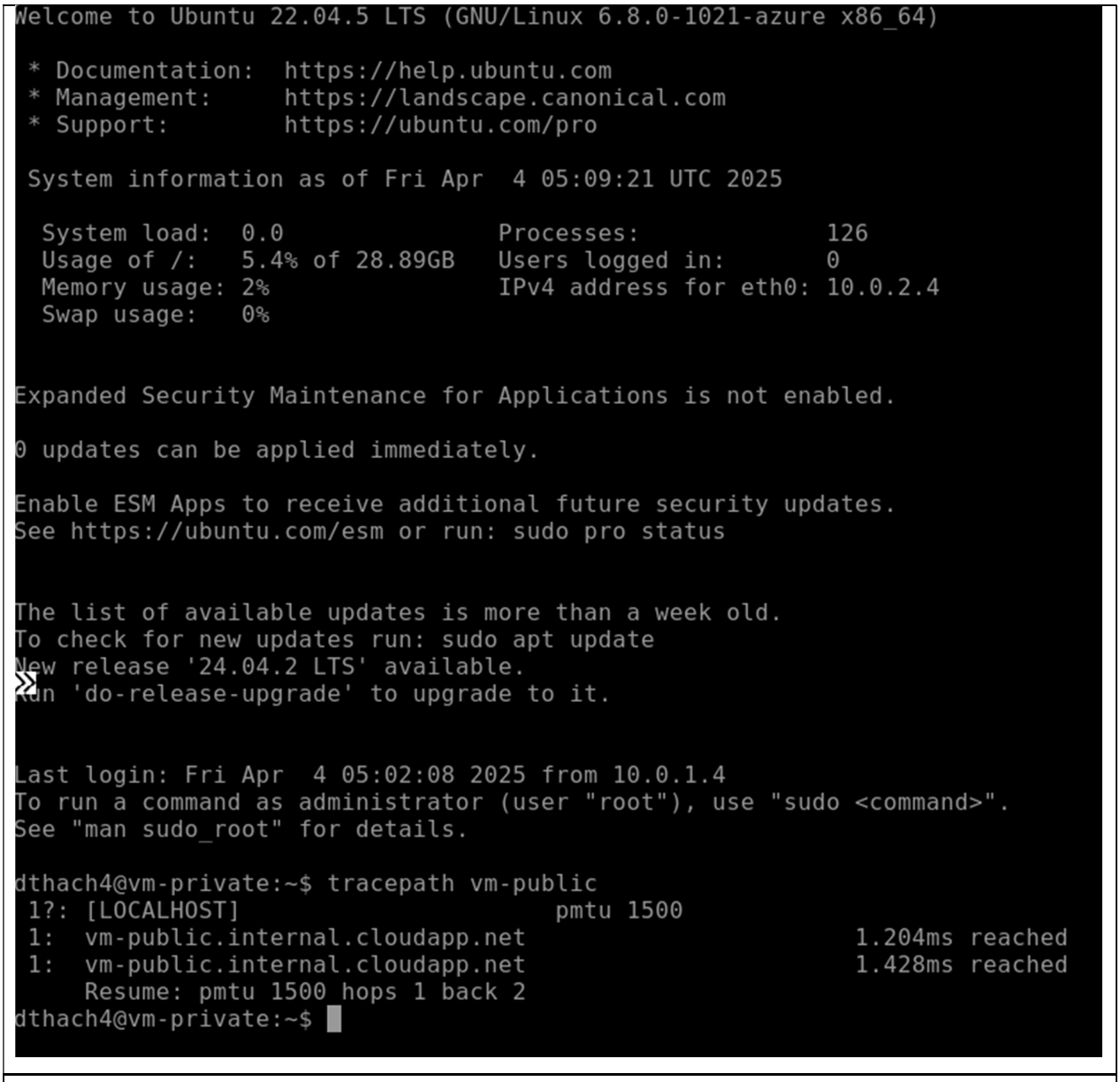


Figure 91: - C. Najera

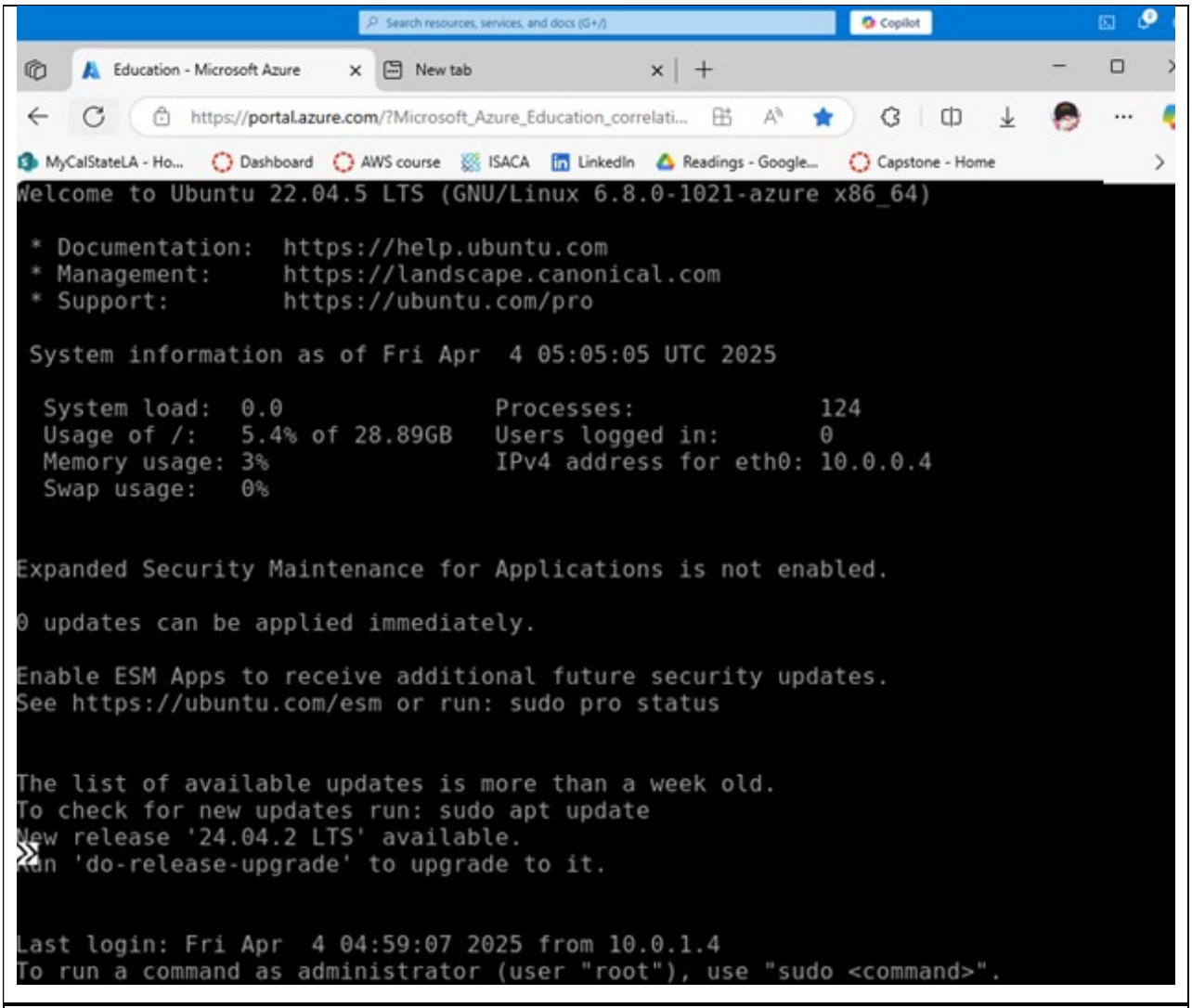


Figure 92: Traced network path from public machine to private machine to ensure configurations are correct and functional - D. Thach

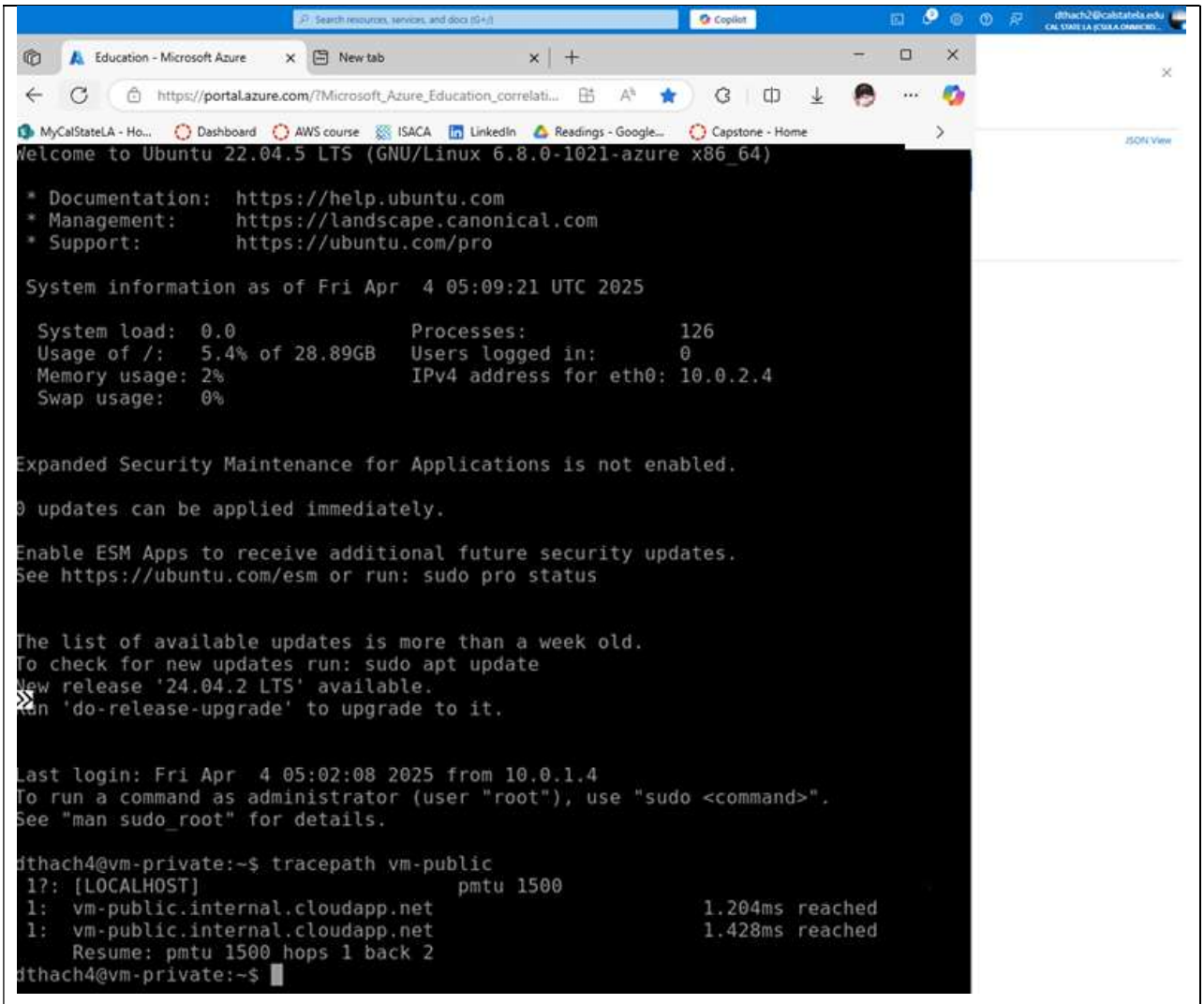


Figure 93: Traced network path from private machine to public machine to ensure configurations are correct and functional **-** D. Thach

6. Connect virtual networks with virtual network peering using the Azure portal

The ability to connect virtual networks (VNets) is a game-changer for modern infrastructure. By bridging these networks, organizations can unlock new possibilities for resource sharing and

microservices communication (Microsoft, 2023). This kind of connectivity is especially valuable in hybrid cloud environments, where seamless integration between on-premises networks and cloud-based VNets is crucial. It also enables global collaboration, allowing teams to work together more effectively across different regions (Turnbull, 2020).

When virtual networks are connected thoughtfully, they can enhance both security and scalability. Techniques like VNet peering and VPN gateways provide a secure pathway for data exchange, while other services offer a high-bandwidth solution for demanding applications (Microsoft, 2023). By leveraging these tools, businesses can build robust infrastructures that support their growth and innovation. The result is a more agile, responsive, and efficient system that meets the needs of today's fast-paced digital landscape.

6.1. Using the network of your team mates

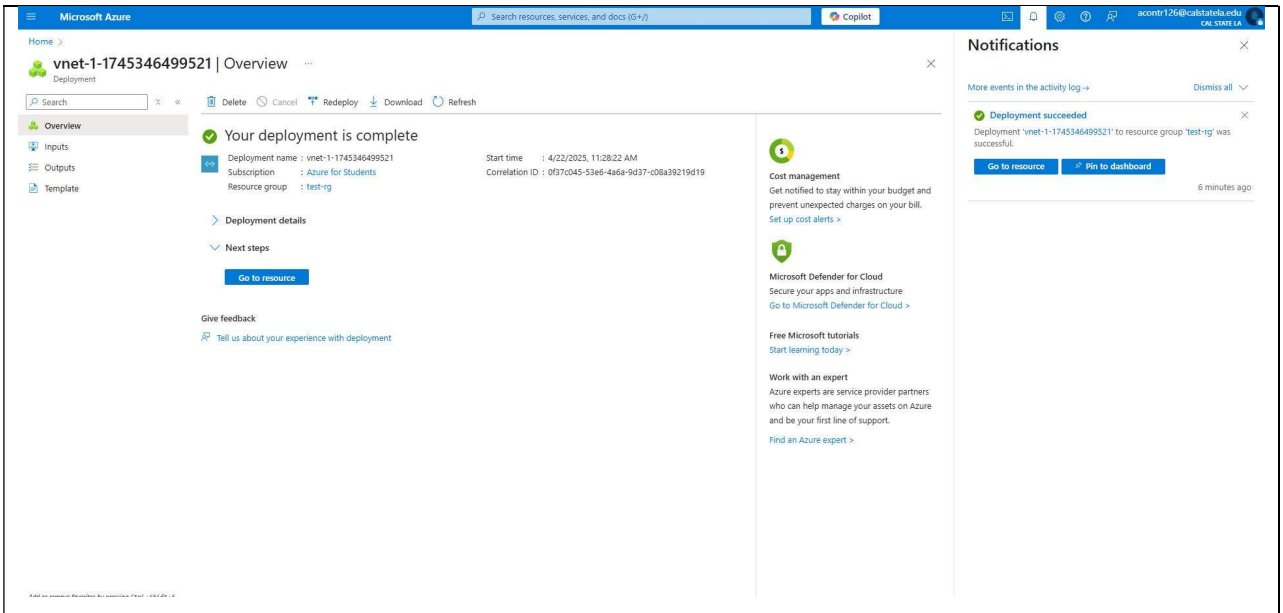


Figure 94: - A. Contreras

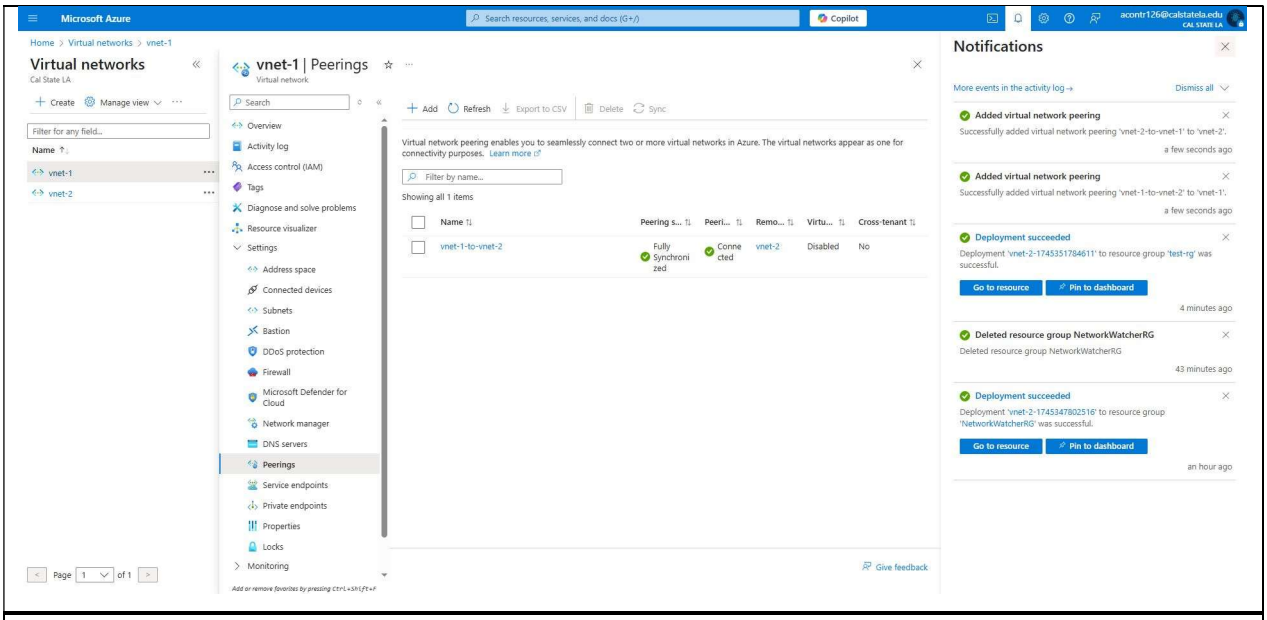


Figure 95: Virtual Network created with the peer connection established between vm1 and vm2 - A. Contreras

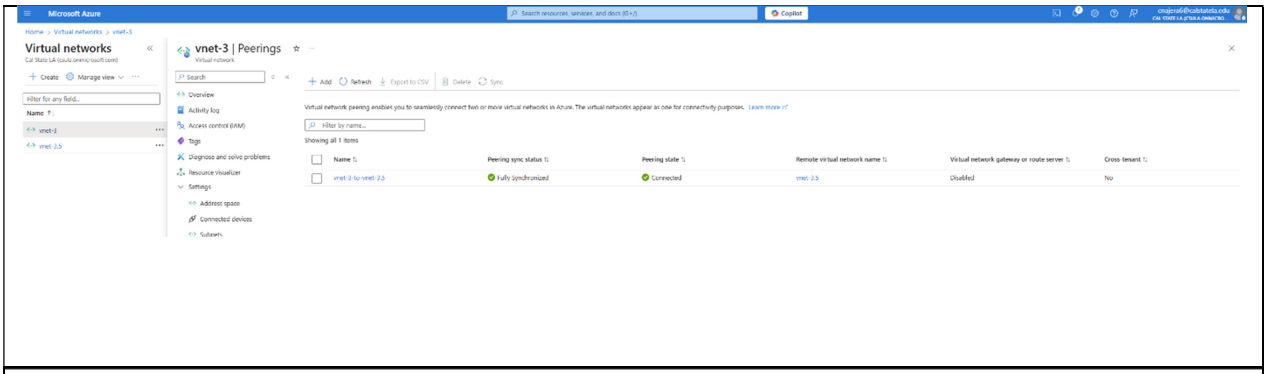


Figure 96: vnet3 to vnet3.5 peering - C. Najera

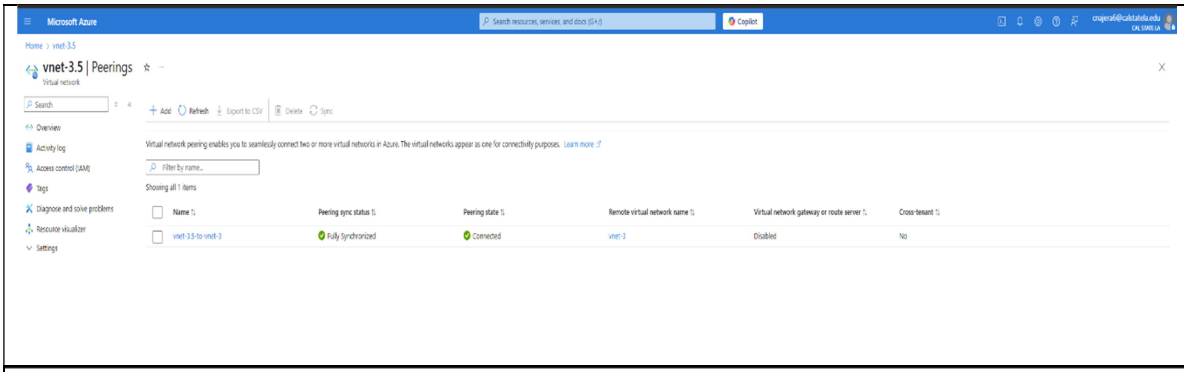


Figure 97: vnet3.5 to vnet3 peering - C. Najera

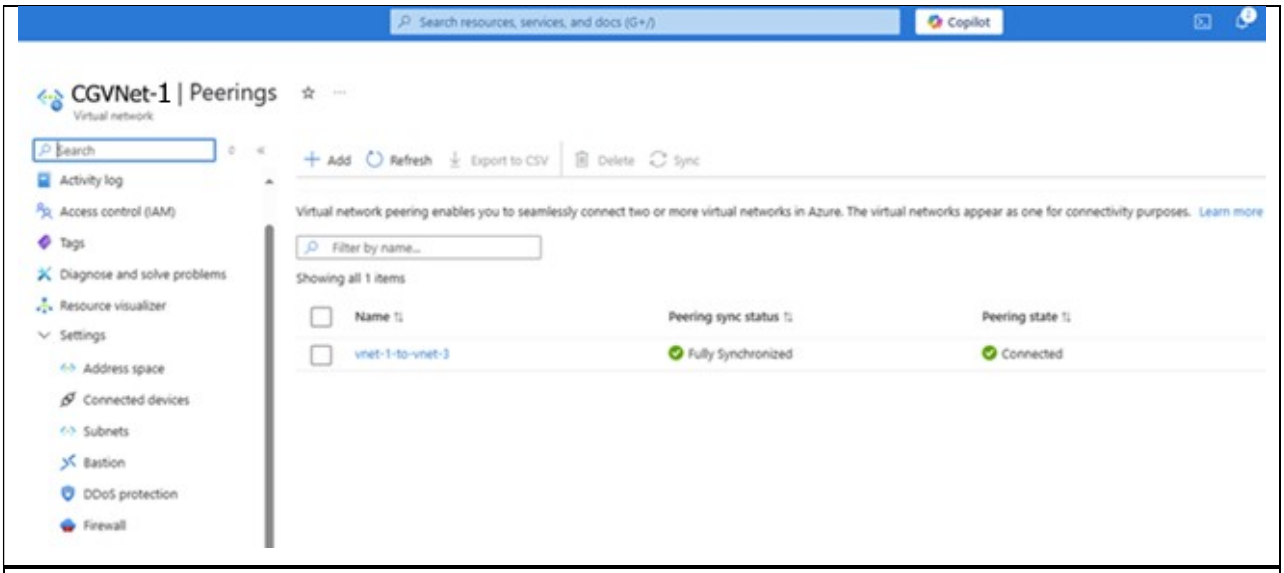


Figure 98: This picture shows that the network has been linked to its peer in the first virtual network. **-** D. Thach

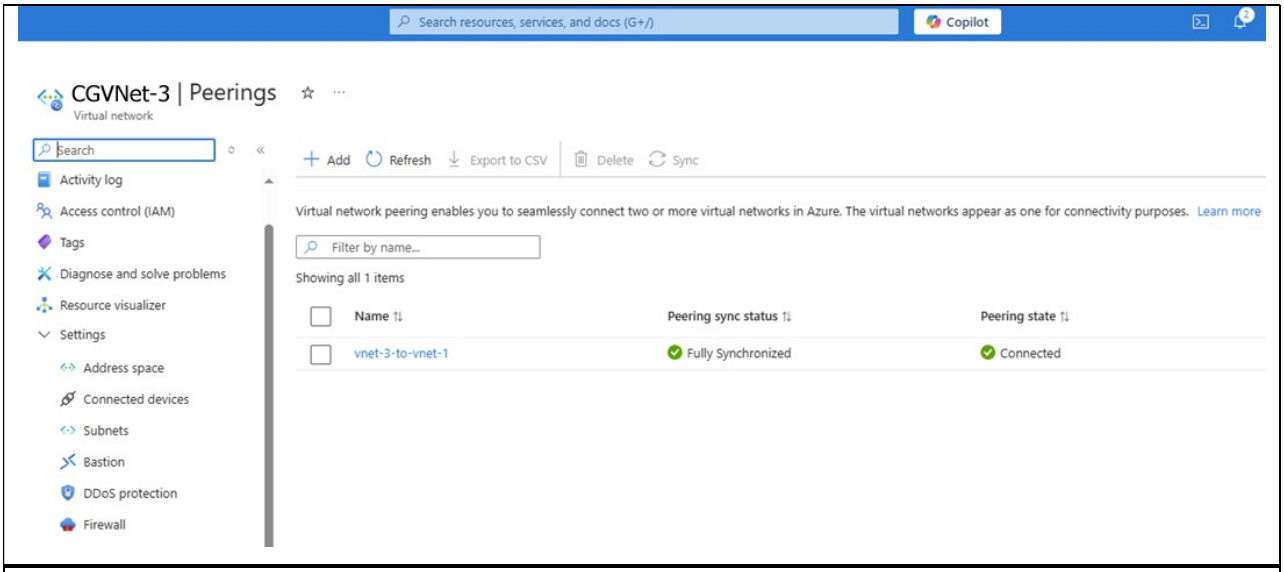


Figure 99: This picture shows that the network has been linked to its peer in the third virtual network in the resource group. **-** D. Thach

6.2. **Peer virtual networks**

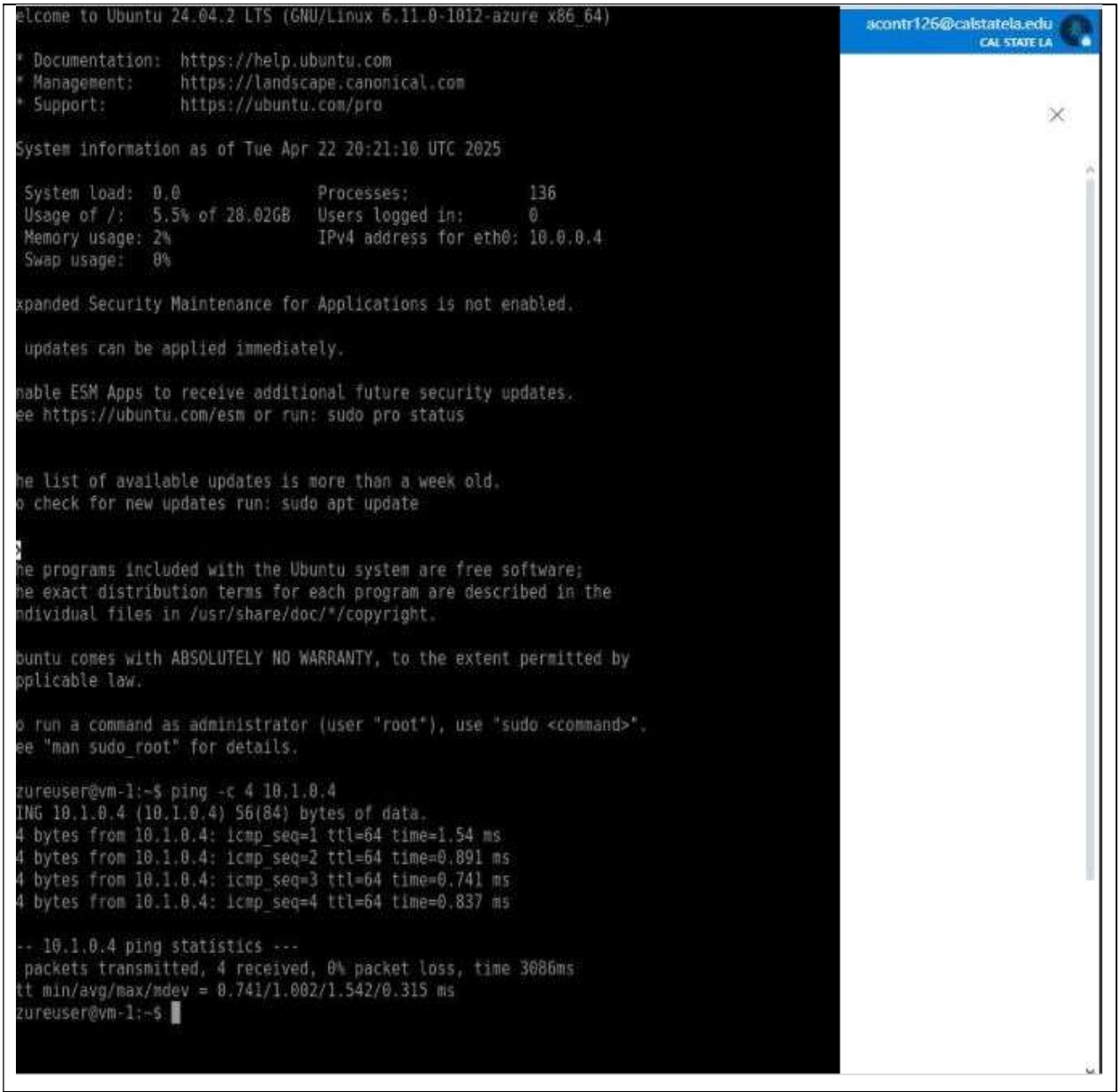


Figure 100: - A. Contreras

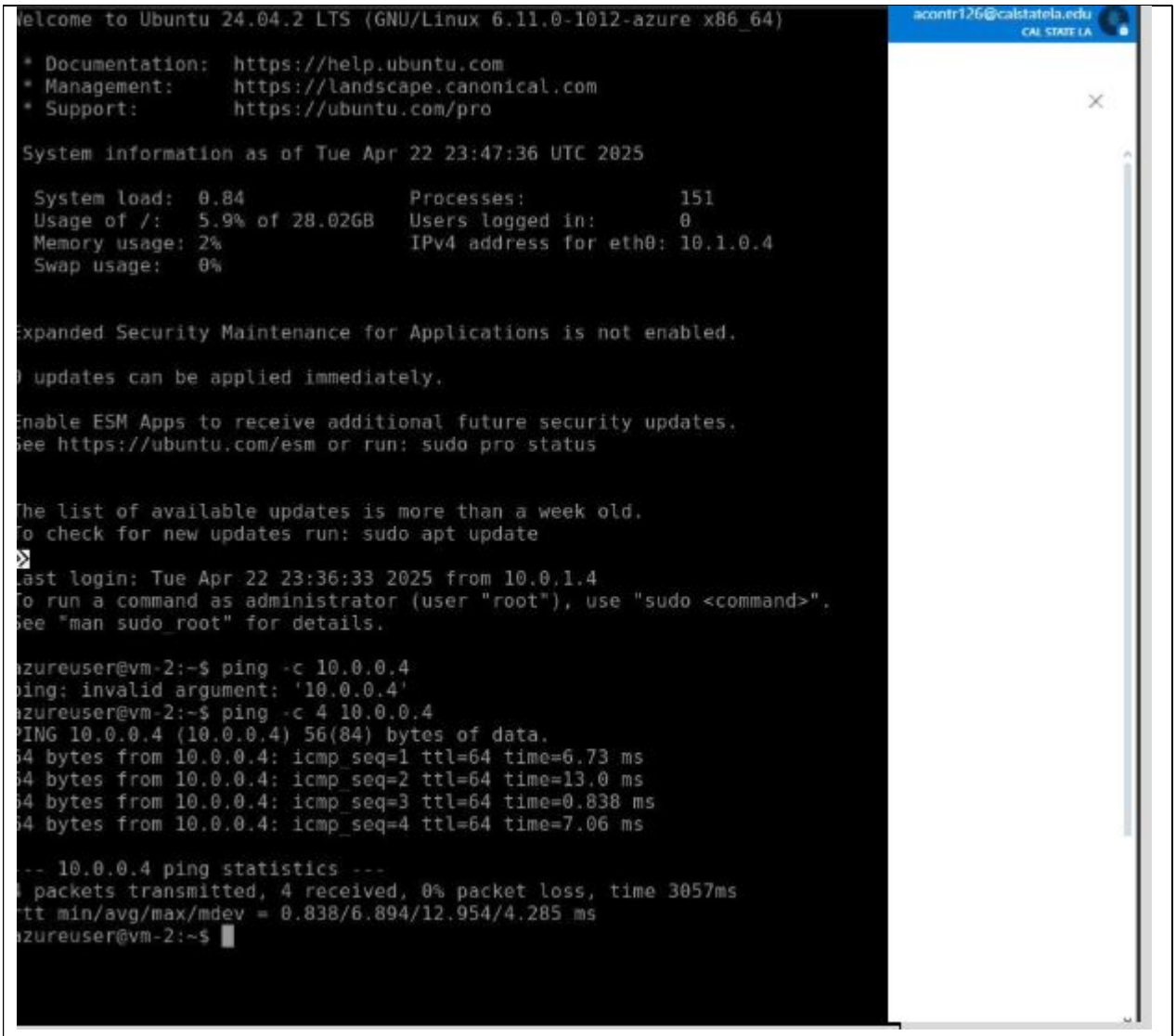


Figure 101: - A. Contreras

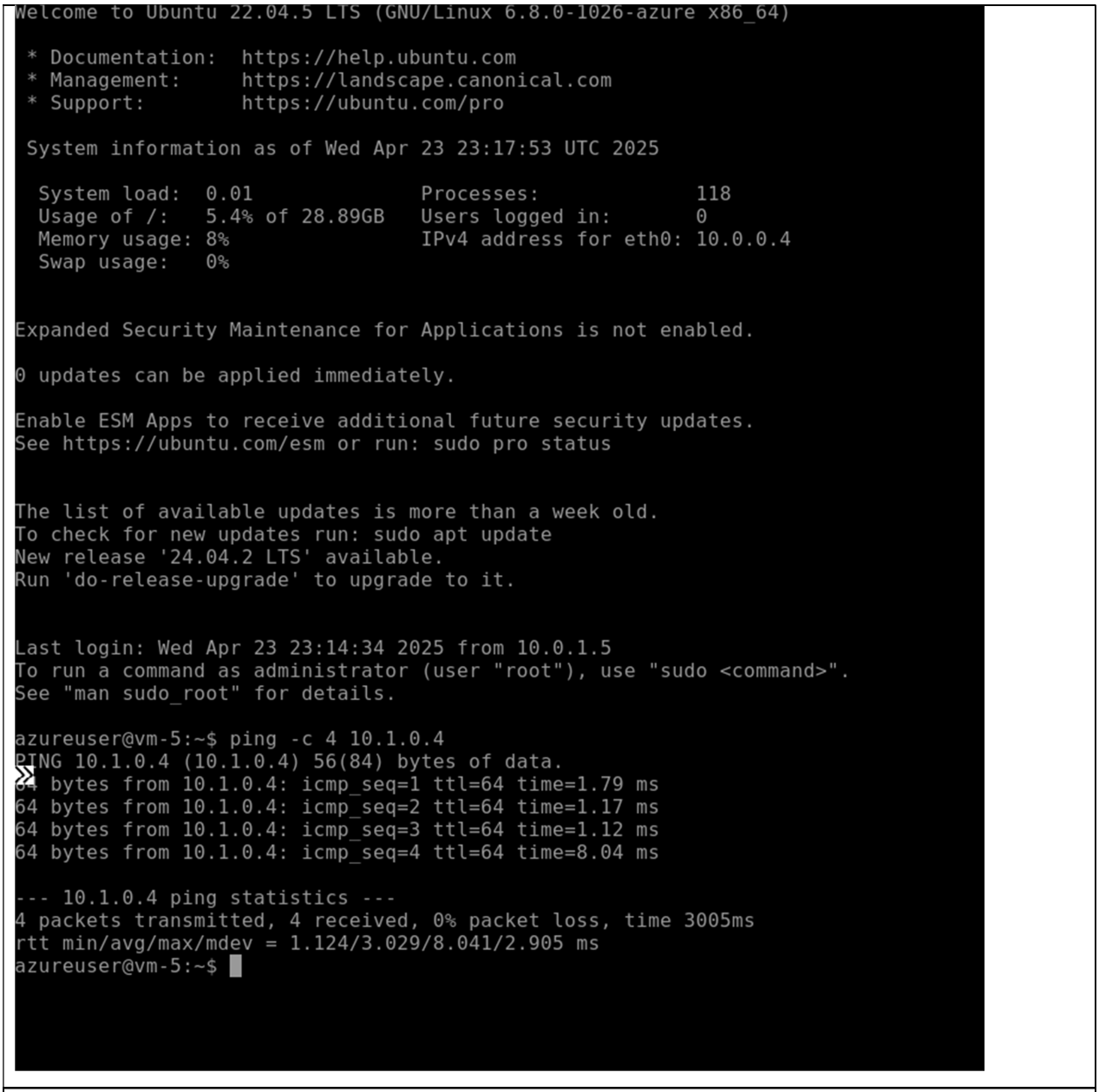


Figure 102: VM5 successful connection to VM6- C. Najera

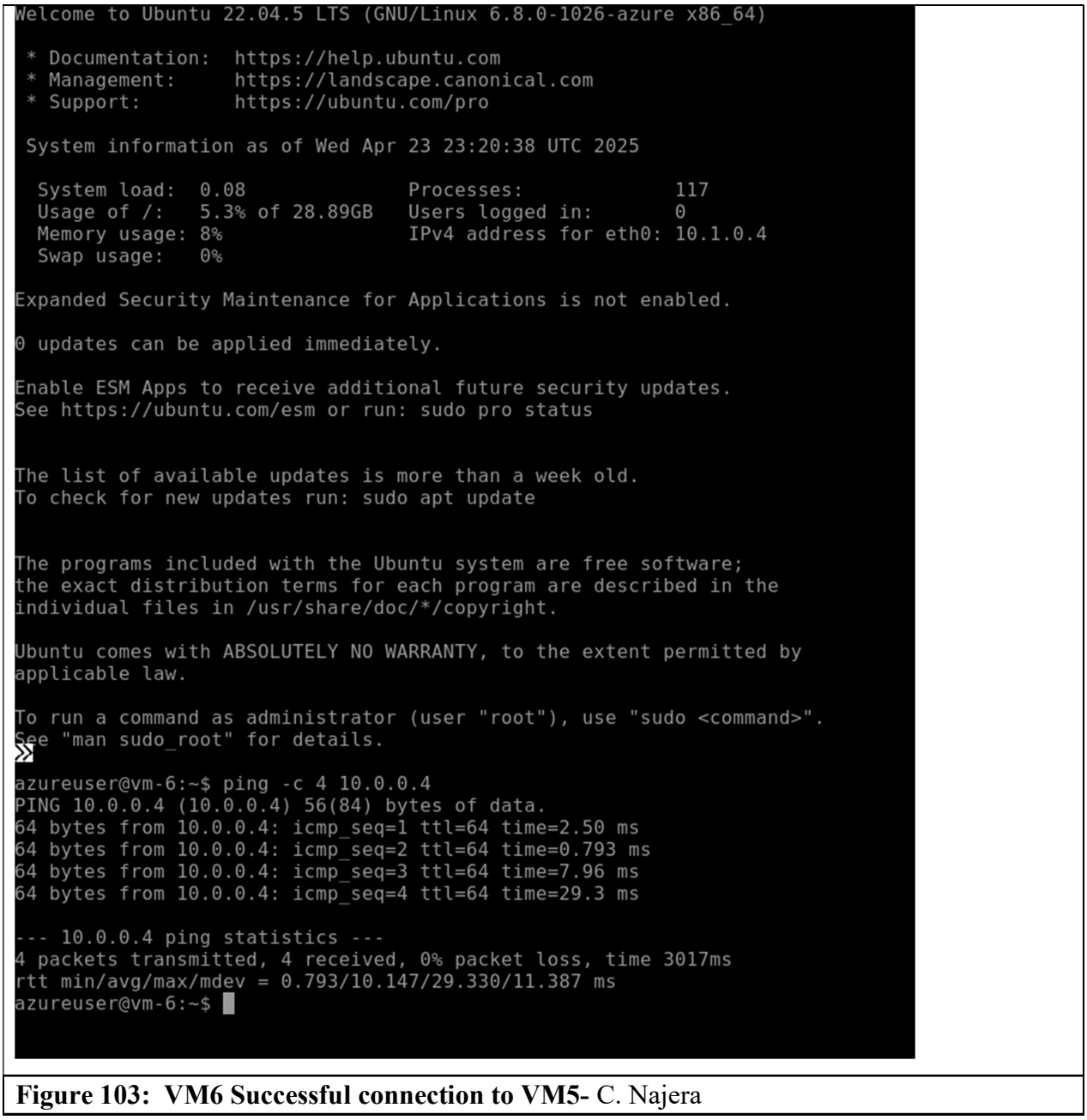


Figure 103: VM6 Successful connection to VM5- C. Najera

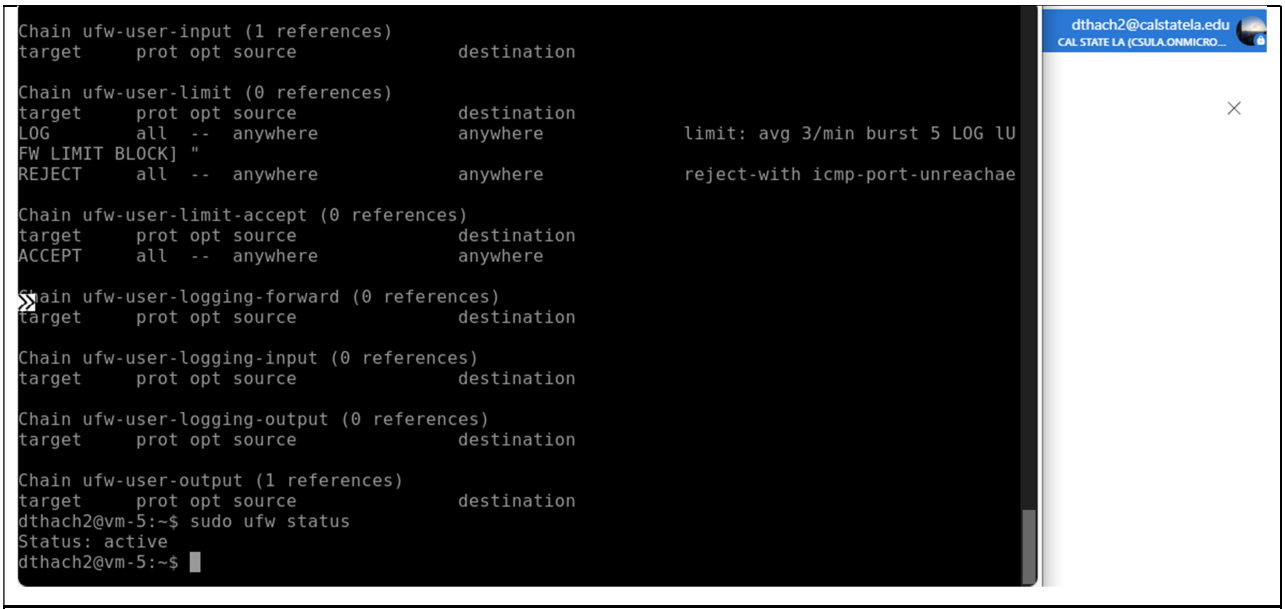


Figure 104: Executed command lines to allow ICMP echo request to permit ICMP traffic, this is a method to allow certain network protocols to be processed on the machines - D. Thach

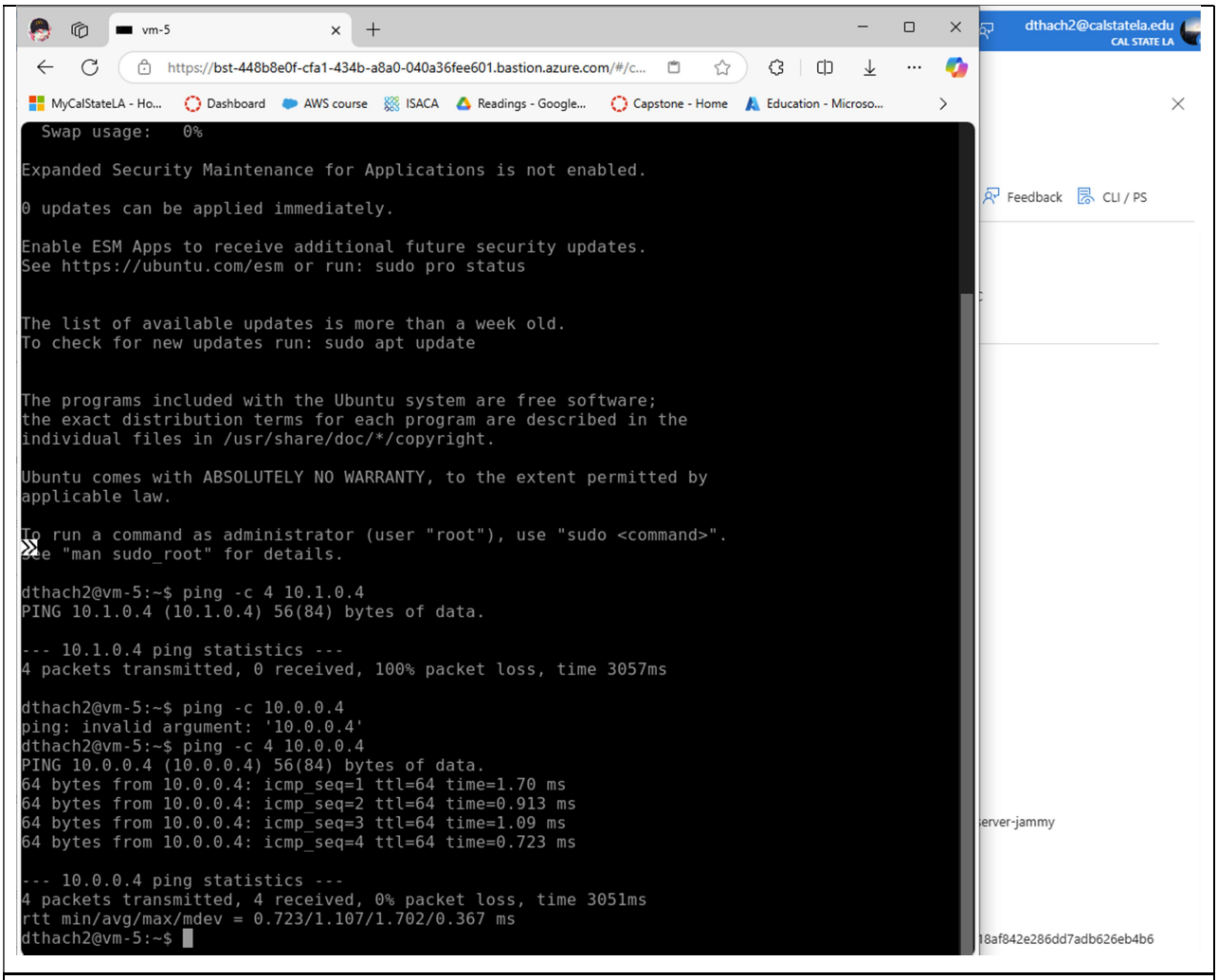


Figure 105: Virtual Machine on CGnetVM is communicating with another machine on another virtual network showing that the configuration was correct and that the machines can connect. - D. Thach

7. References

asudbring. (2023, May 4). *Network security group – how it works*. Learn.microsoft.com. https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works

asudbring. (2024, August 20). *Tutorial: Filter network traffic with a network security group (NSG)*. Microsoft.com. https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic?tabs=portal

GeeksforGeeks. (2022, July 22). *Fundamentals of virtual networking*. Retrieved February 24, 2025, from https://www.geeksforgeeks.org/fundamentals-of-virtual-networking/

Khan, A. (2023, March 6). *How network security groups filter network traffic*. Linkedin.com. https://www.linkedin.com/pulse/how-network-security-groups-filter-traffic-ali-khan-/

KumudD. (n.d.). *Route network traffic – tutorial – Azure Portal*. Retrieved from https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-create-route-table-portal

Massachusetts Health Policy Commission. (2018). *Final CMIR Report – Beth Israel Lahey Health – Executive Summary*. Massachusetts Health Policy Commission. https://www.mass.gov

McFarlan, F. W., & Austin, R. D. (2005). *CareGroup* (Case No. 9-303-097). Harvard Business School.

Microsoft. (2023). *Virtual network documentation*. Microsoft Azure. https://learn.microsoft.com/en-us/azure/virtual-network/

Microsoft. (2024a). *What is Azure Virtual Network?*. Retrieved February 25, 2025, from https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview

Microsoft. (2025a). *What is a virtual machine and how does it work | Microsoft Azure*. https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-virtual-machine/?msockid=1b50d6747d616ea30770c3467cf36f18

Samanro. (n.d.). *Microsoft cloud architecture models – Enterprise resource planning*. Retrieved from https://docs.microsoft.com/en-us/microsoft-365/solutions/cloud-architecture-models?view=o365-worldwide

Susnjara, S., & Smalley, I. (2024, March 3). *What is a virtual machine (VM)?* IBM. https://www.ibm.com/think/topics/virtual-machines

Turnbull, J. (2020). *The cloud infrastructure handbook: A guide to building and managing cloud infrastructure*. Turnbull Press.

8. Glossary

Azure

A cloud computing platform and service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centers.

Virtual Network (VNet)
A representation of a network in the cloud that enables communication between Azure resources and remote computers, often replacing traditional physical networks.

Virtual Machine (VM)
A software-based emulation of a computer that runs an operating system and applications like a physical machine but is hosted on a physical server.

Network Security Group (NSG)
A set of rules used to allow or deny network traffic to Azure resources based on source/destination IP addresses, ports, and protocols.

Application Security Group (ASG)
A feature in Azure that allows you to group servers with similar functions and apply security rules collectively for easier management.

Route Table
A configuration in Azure that defines how network traffic is directed in a virtual network, based on destination IP addresses and next hop types.

IP Forwarding
A network feature that allows a virtual machine to act as a router, forwarding traffic between networks or subnets.

Bastion Host
A special-purpose instance that acts as a gateway to securely access private network resources without exposing them directly to the internet.

DDoS Attack (Distributed Denial of Service)
A type of cyberattack where multiple systems flood the bandwidth or resources of a targeted system, often causing service outages.

Public vs Private Virtual Machine

Public VMs are accessible over the internet via public IPs, while private VMs are secured within a virtual network and require VPN or bastion access.

Subnet

A segmented portion of a virtual network that allows isolation and management of network traffic for better control and security.

NVA (Network Virtual Appliance)

A virtual appliance used to control the flow of network traffic, typically functioning as a firewall, router, or WAN optimizer.