Cloud Computing

Assignment 3

Harshpreet singh (43501)

Sukhwinder singh (44300)

Table of Contents

Task 1: Connecting two VMS

Executive summary

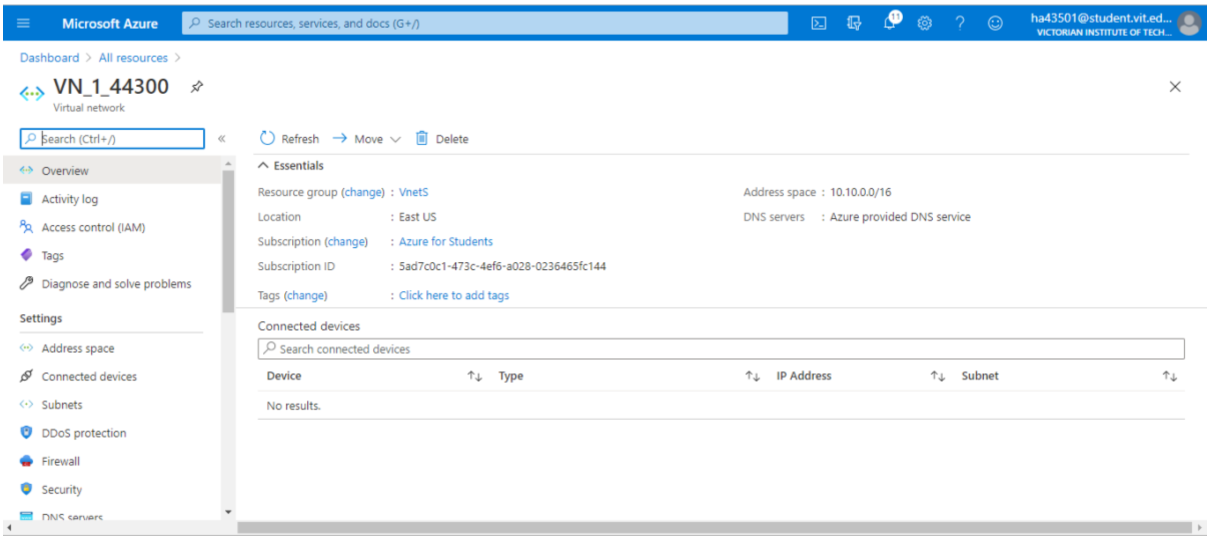
The report has designed and implement a cloud solution for an IT infrastructure. The main objective of this paper is the deployment of two virtual networks and secure communication within two virtual machines in the Microsoft Azure platform. Microsoft Azure is a public cloud computing infrastructure utilized for networking, storage, virtual computing, analytics, and much more. The Microsoft Azure cloud platform contains more than 200 cloud services and helps its clients to manage, run, and build applications across multiple clouds. The Virtual network provides secure communication within multiple virtual servers, virtual machines, computers, or other devices across different regions. While the virtual machine is one type of computer resource that utilizes software instead of utilizing physical networking devices to deploy applications and run programs. The virtual machine provides a safe environment and protects the network from various kinds of security issues.

In this project, two virtual networks have been created within the Microsoft Azure platform with specific address space and specific subnet range. After the development of two Virtual Networks Gateway subnets are added under each subnet. Therefore, two public IP address has been created for two virtual networks and both the public address are dynamic. Further, two Virtual gateway network has been created and both are connected with each other. Finally, the VM has been created and connected with two virtual machines. By deploying two virtual machines into the virtual network both the user can securely communicate with each other. The virtual network of the Microsoft azure is the basic building block of the private network that permits the utilization of any type of Azure resources like virtual machines in order to securely communicate with each other on the internet. In this project, both the VMs are connected with Connected through the putty application. Further, the 'ifconfig' command has been utilized to check the IP address configuration of both the virtual machines. Finally, both the connected virtual machines are tested by pinging from one machine to another.

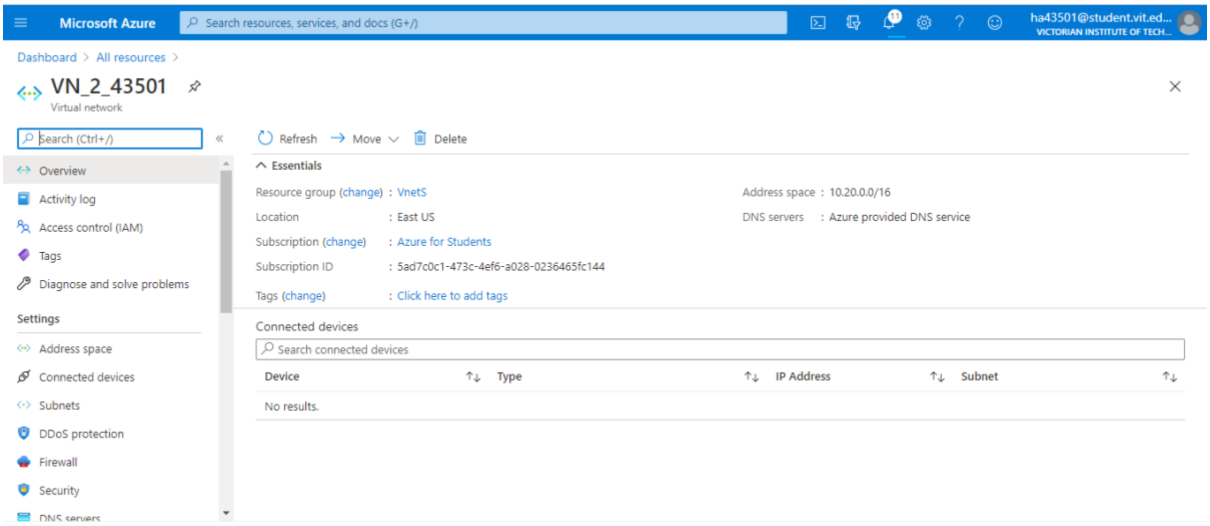
Therefore, once the virtual network has peered then both the virtual networks can communicate and share resources securely within each other with the same bandwidth and latency. In this project, both the virtual machines have been created in the same virtual network and both of the VMs utilizes a private IP address to communicate securely. Both the virtual machines are allocated with a dynamic IP address during deployment. Virtual network and virtual machine limit the cost of the network by reducing the requirements of the physical hardware network. Moreover, in this project, both the virtual networks are connected in such a way that they can securely communicate with each other and protect the network from various kinds of security issues.

Configuring VNet-to-VNet gateway connection

Step 1

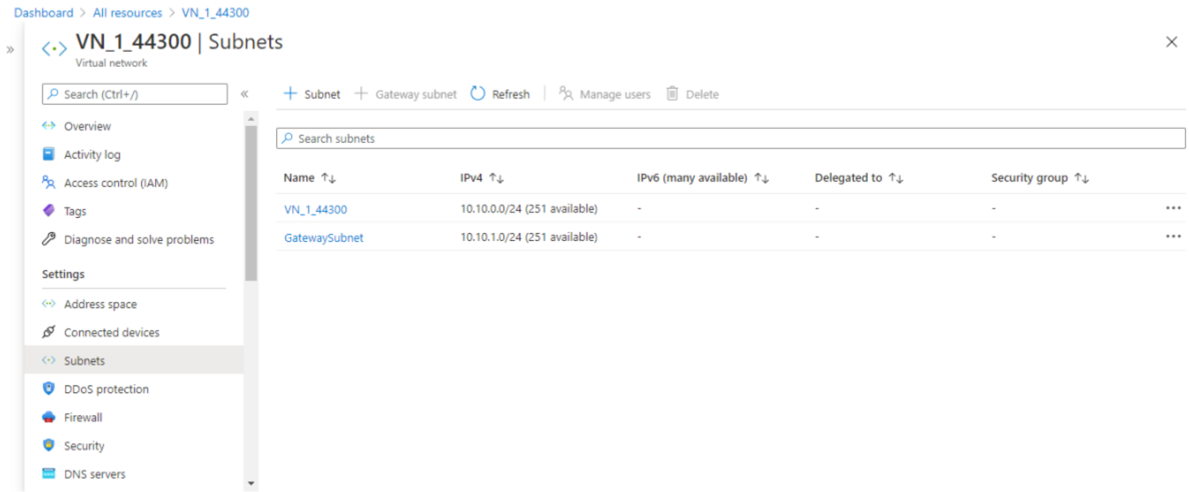


Screenshot 1: Virtual network 1 (VN_1_44300)

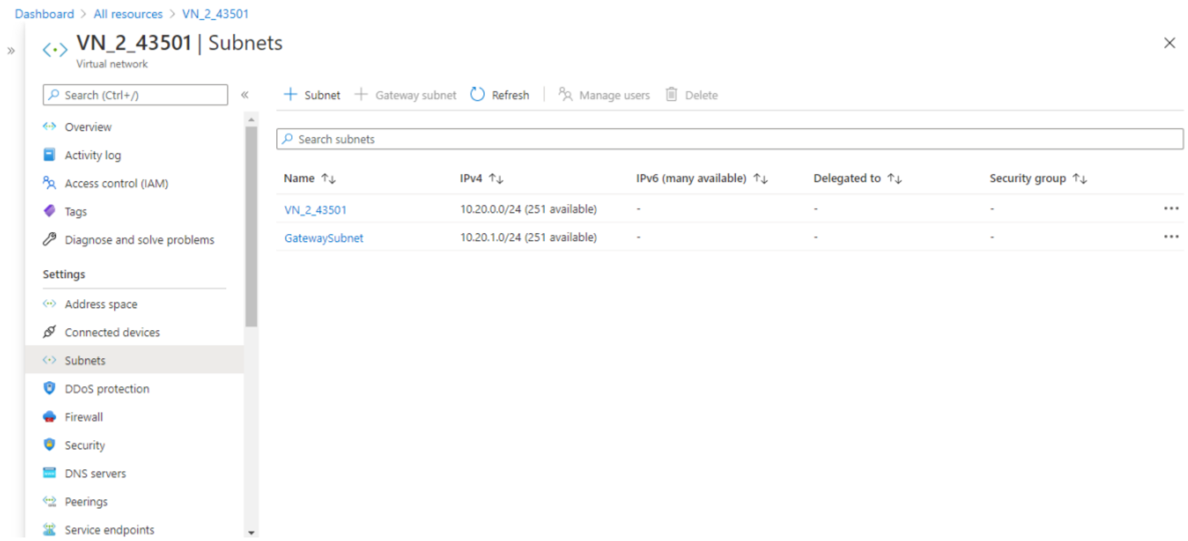


Screenshot 2: Virtual Network 2 (VN_2_43501)

Step 2

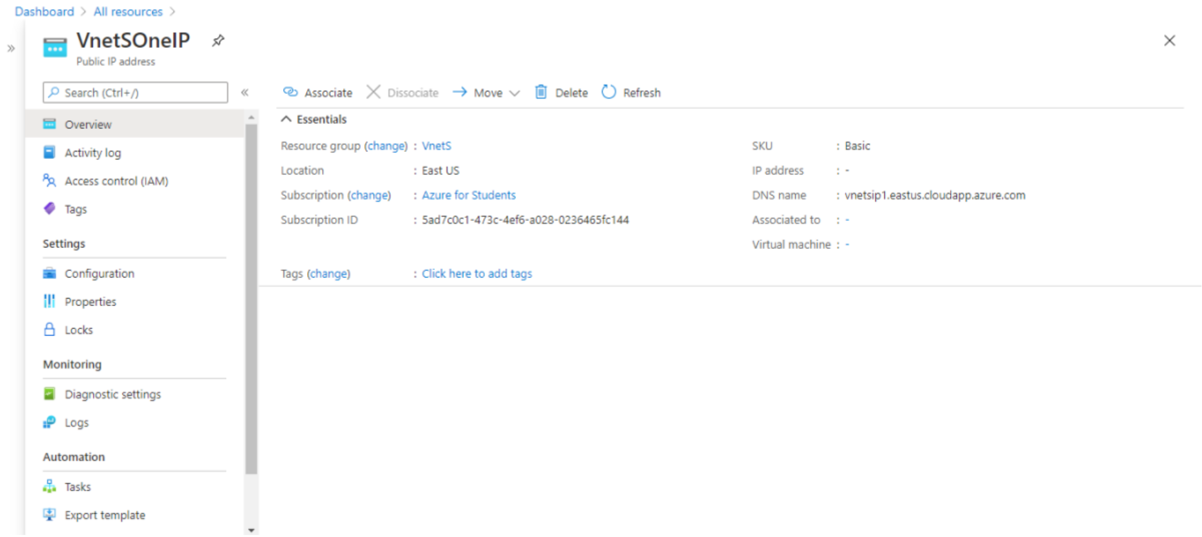


Screenshot 3: Gateway Subnet for VN_1_44300

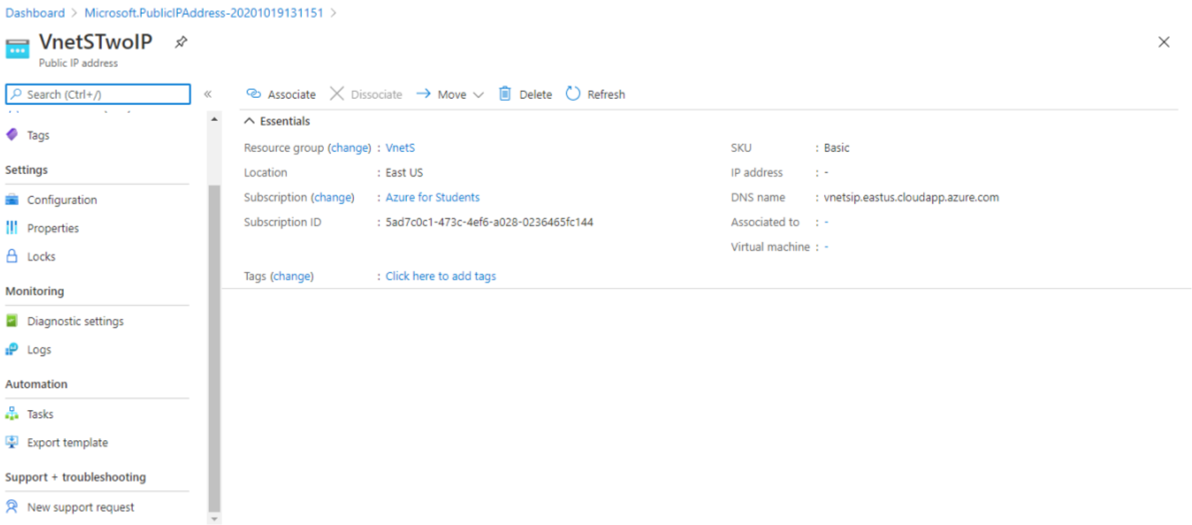


Screenshot 4: Gateway subnet for VN_2_43501

Step 3

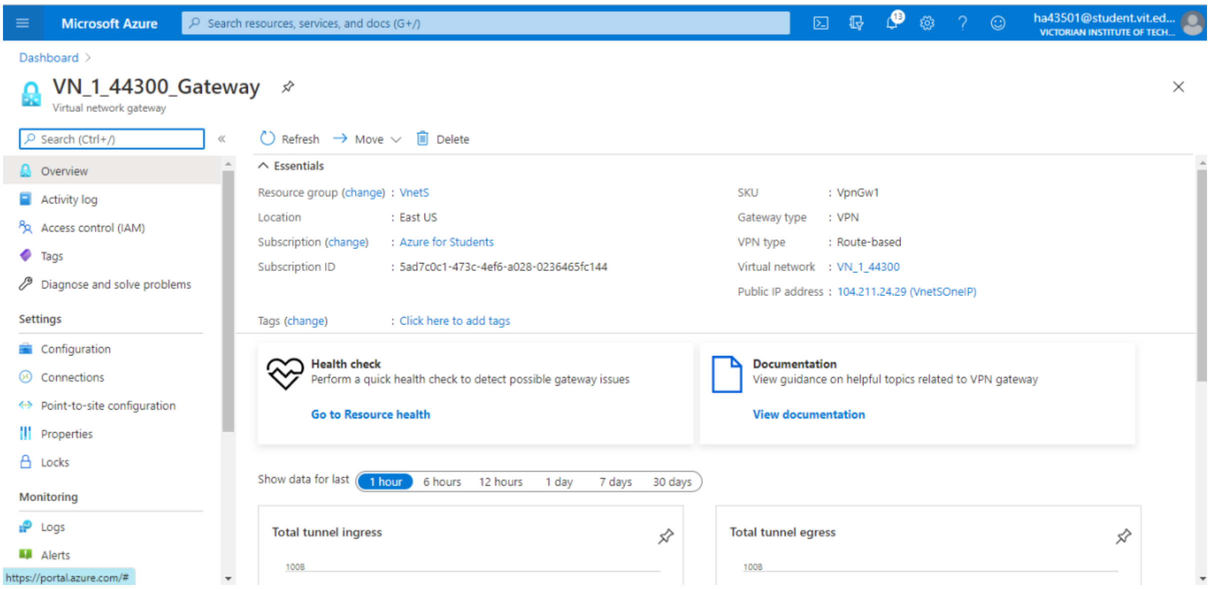


Screenshot 5: Public IP address for VN_1_44300

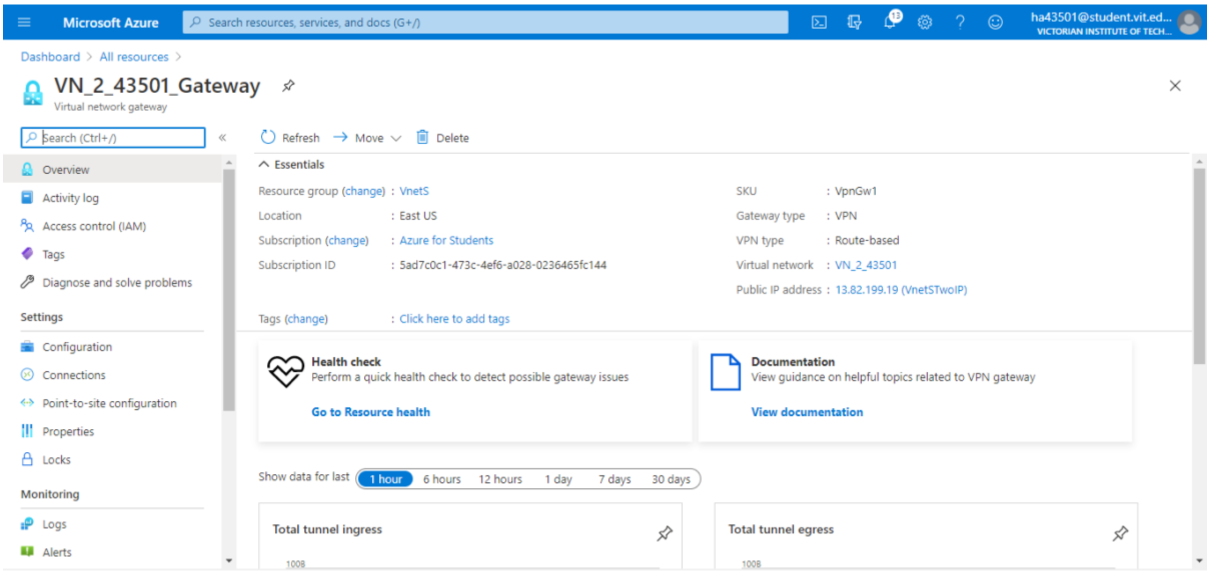


Screenshot 6: Public IP address for VN_2_43501

Step 4

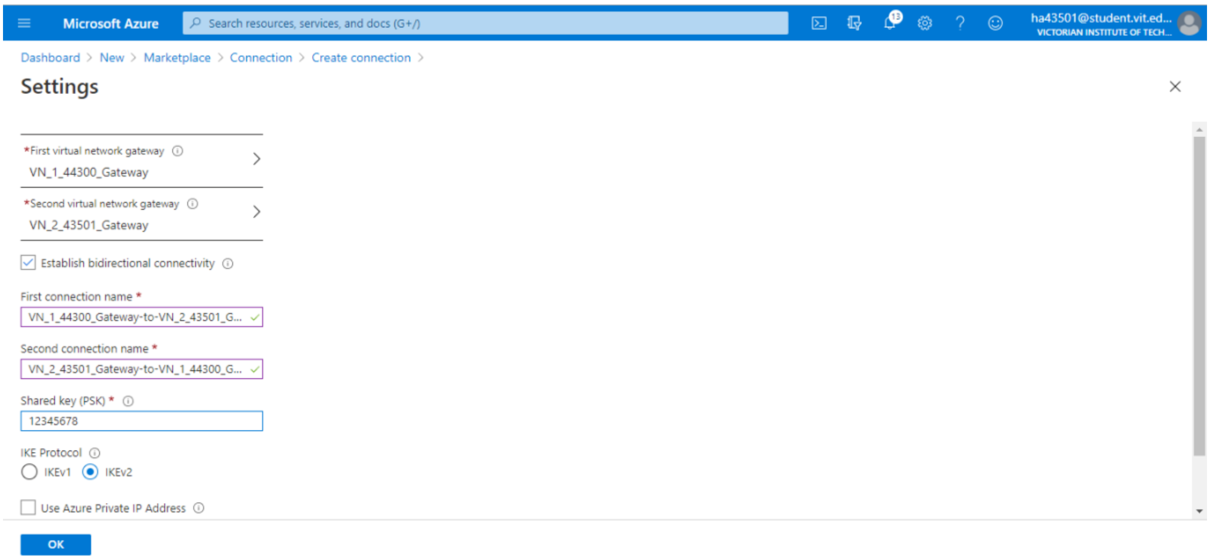


Screenshot 7: Virtual Network gateway for student 1

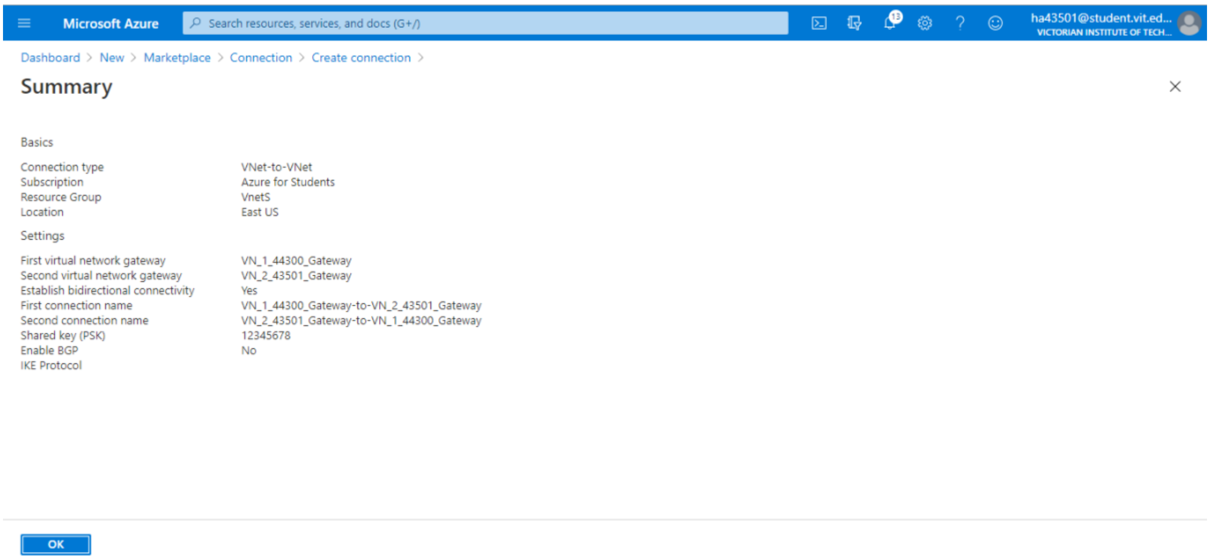


Screenshot 8: Virtual Network Gateway for student 2

Step 5:

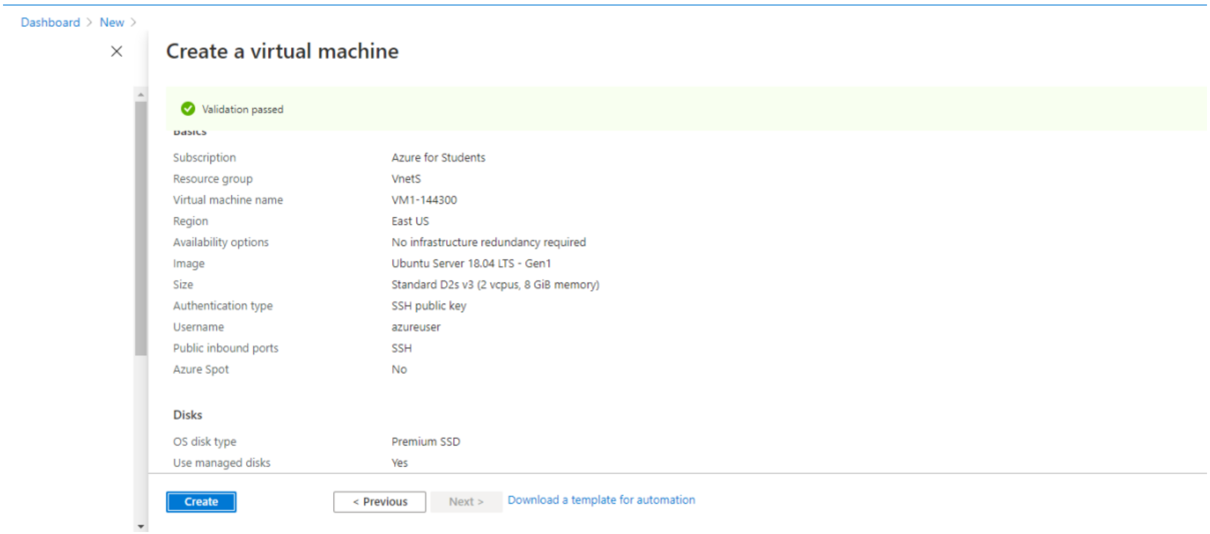


Screenshot 9: Gateway Connection

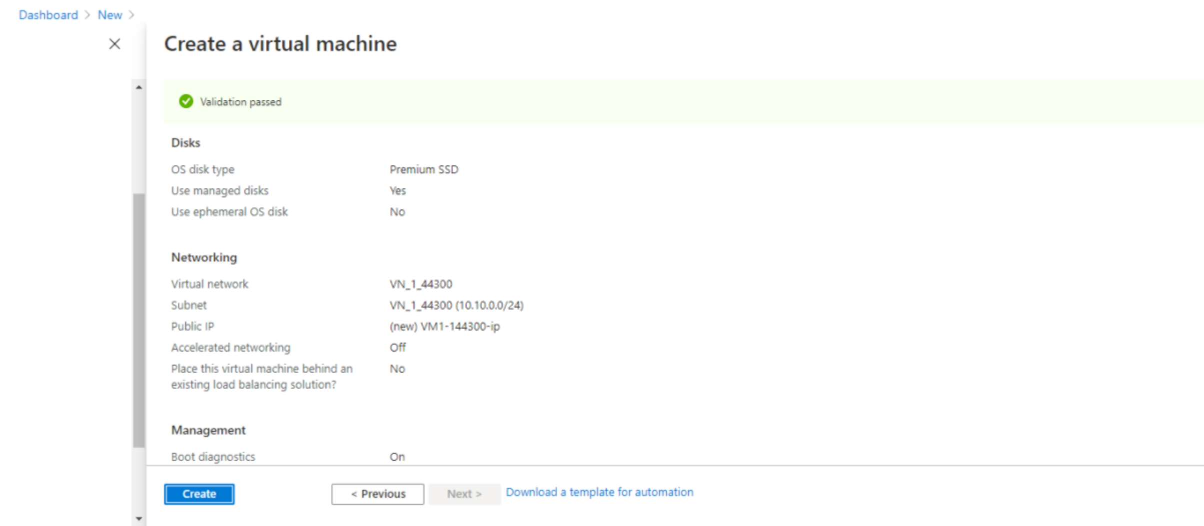


Screenshot 10: Connection between two Vnets

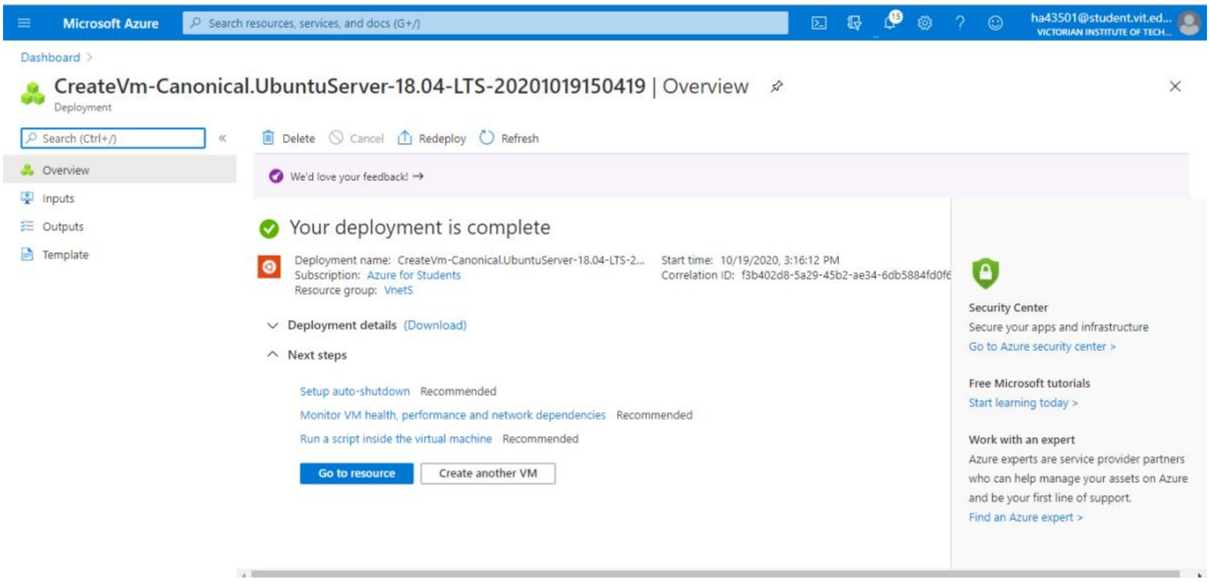
Step 6



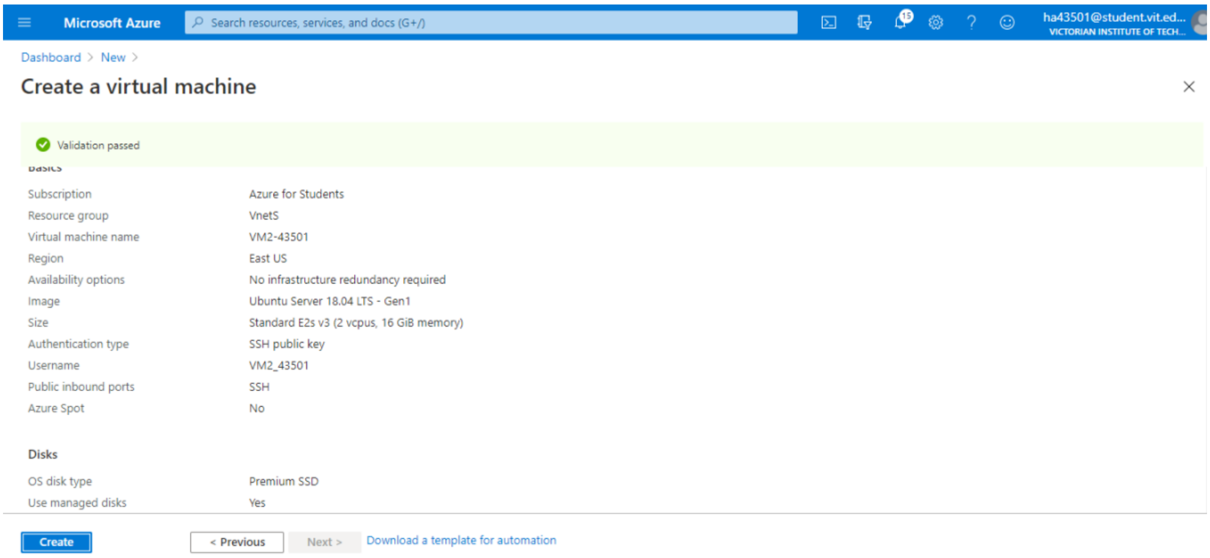
Screenshot 11: Virtual machine 1 creation



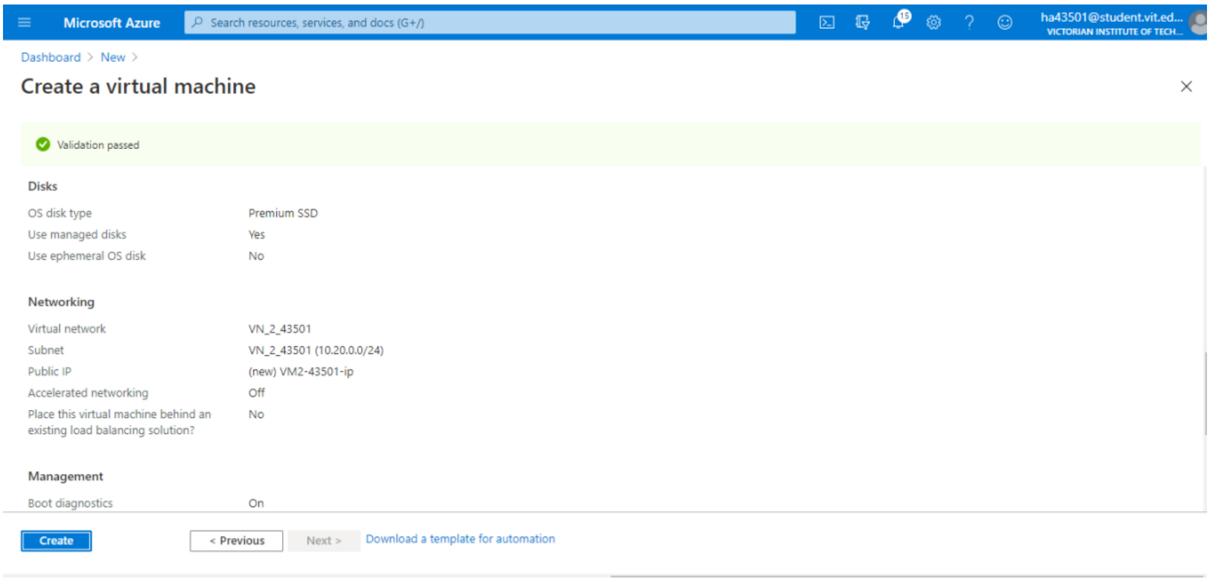
Screenshot 12: Virtual machine 1 creation



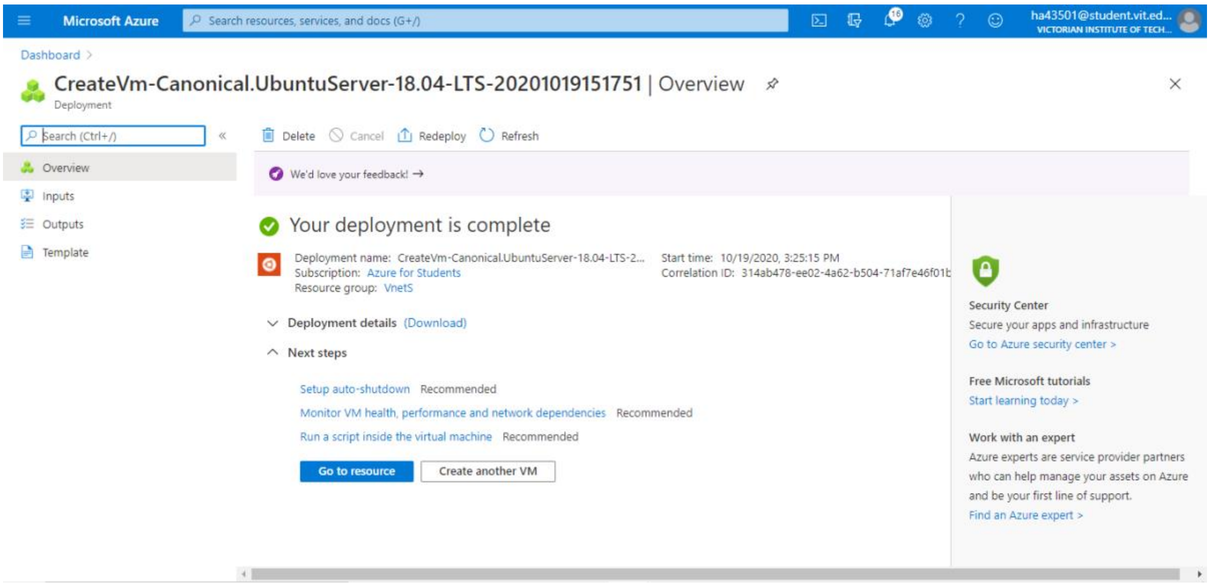
Screenshot 13: Virtual machine 1 creation



Screenshot 14: Virtual machine 2 creation

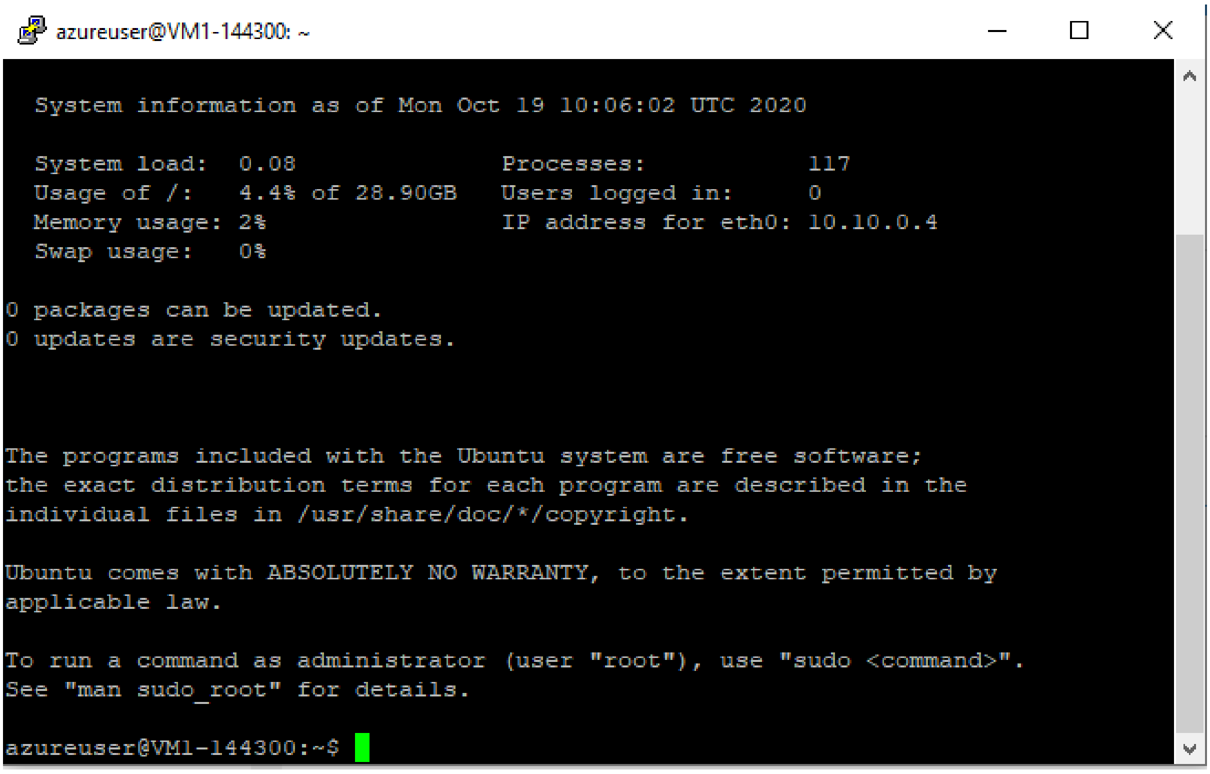


Screenshot 15: Virtual machine 2 creation

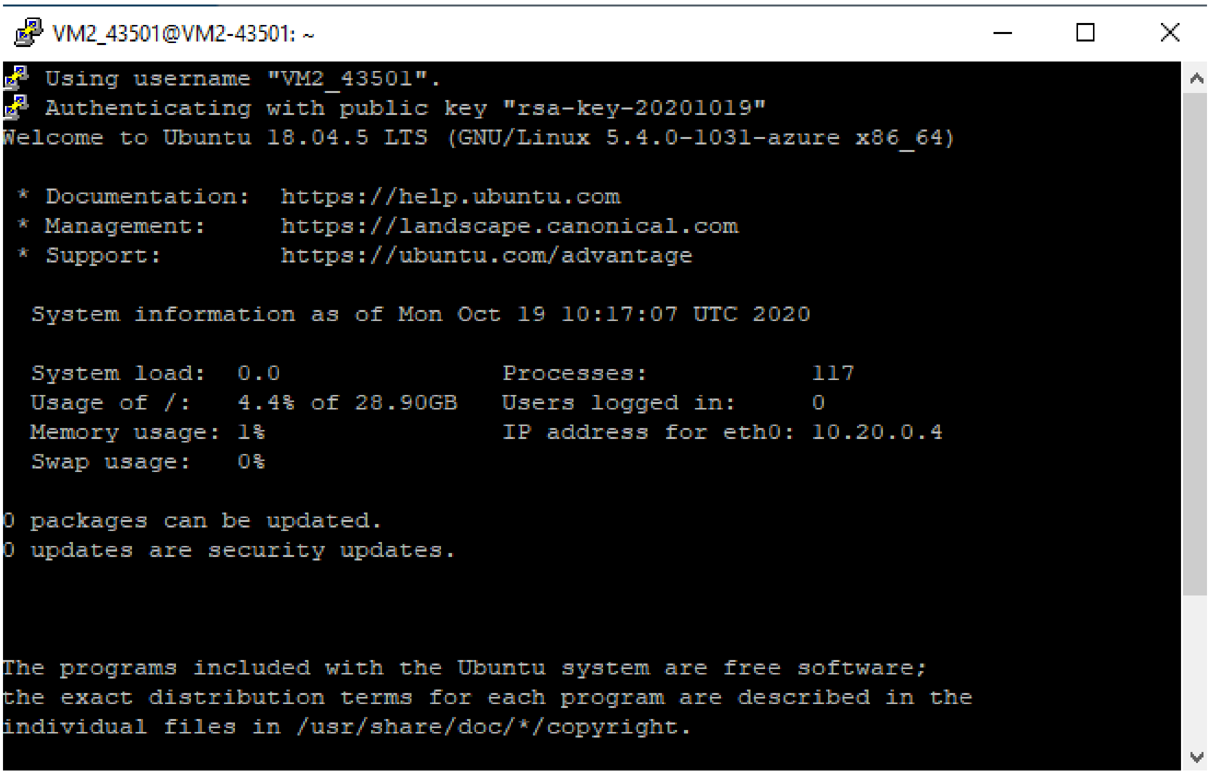


Screenshot 16: Virtual machine 2 creation

Step 7

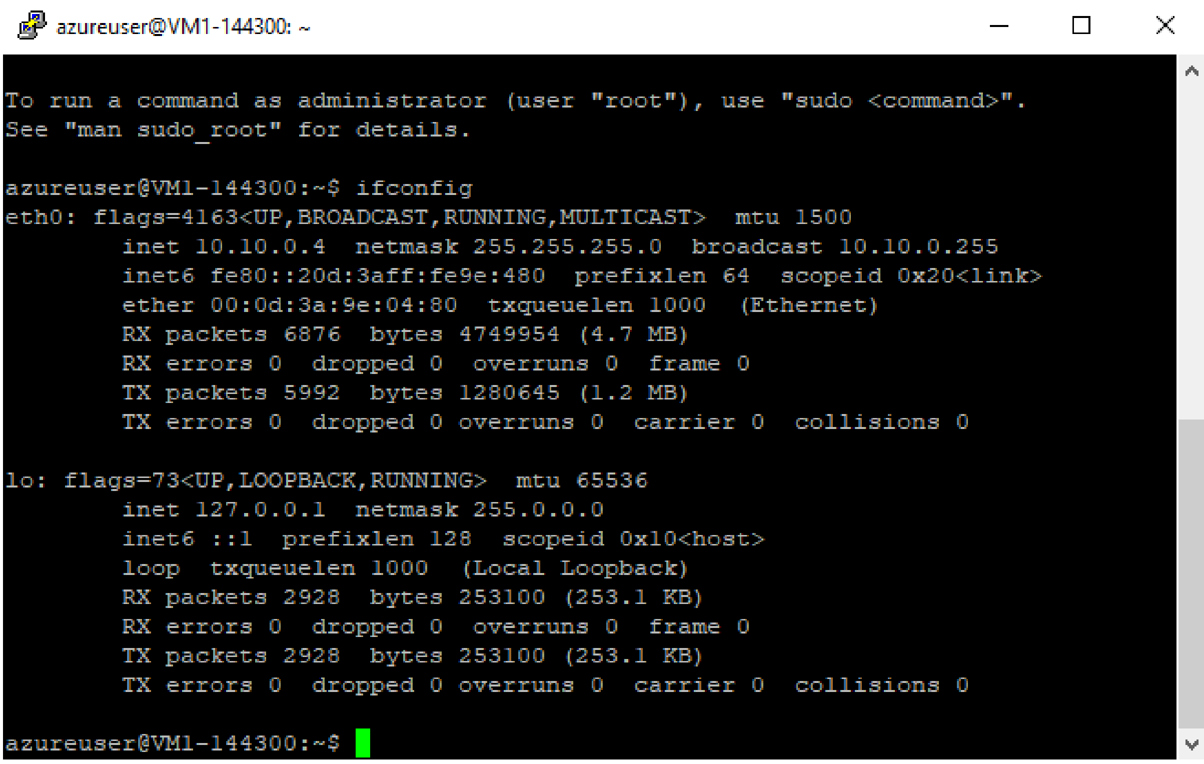


Screenshot 17: VM1 connection through putty

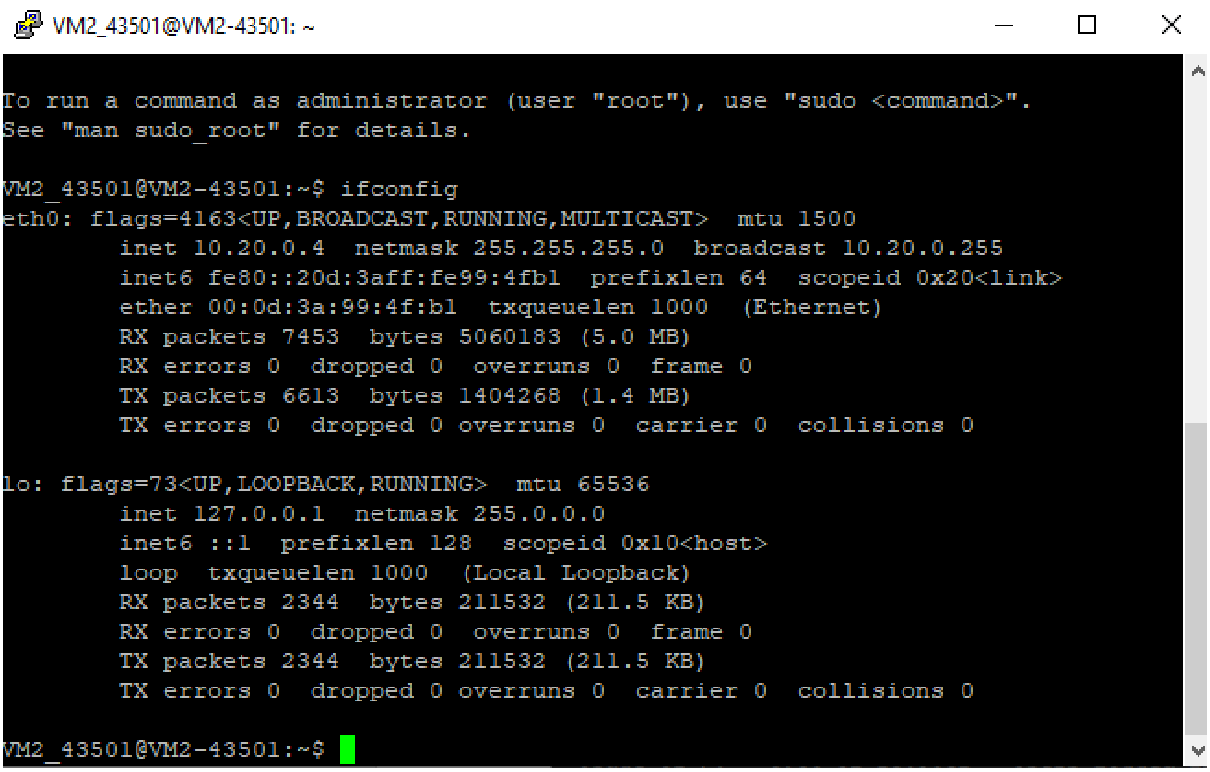


Screenshot 18: VM2 connection through putty

Step 8:

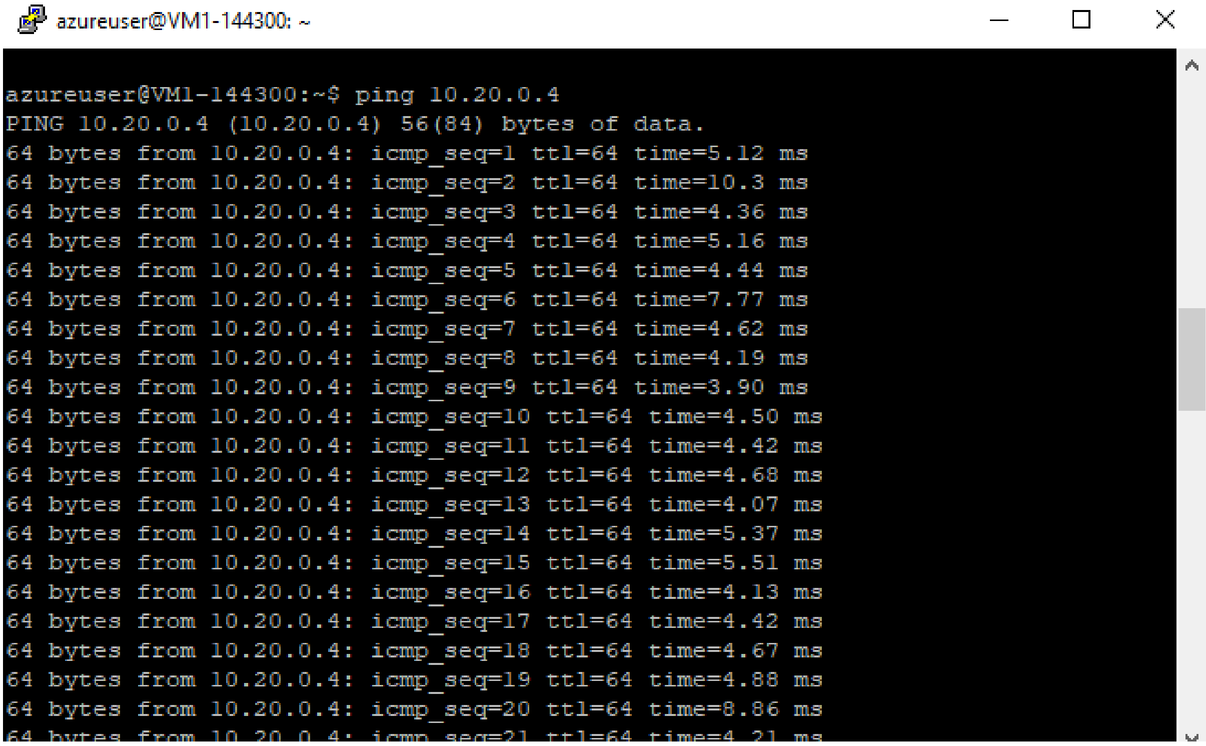


Screenshot 19: Ifconfig of VM1

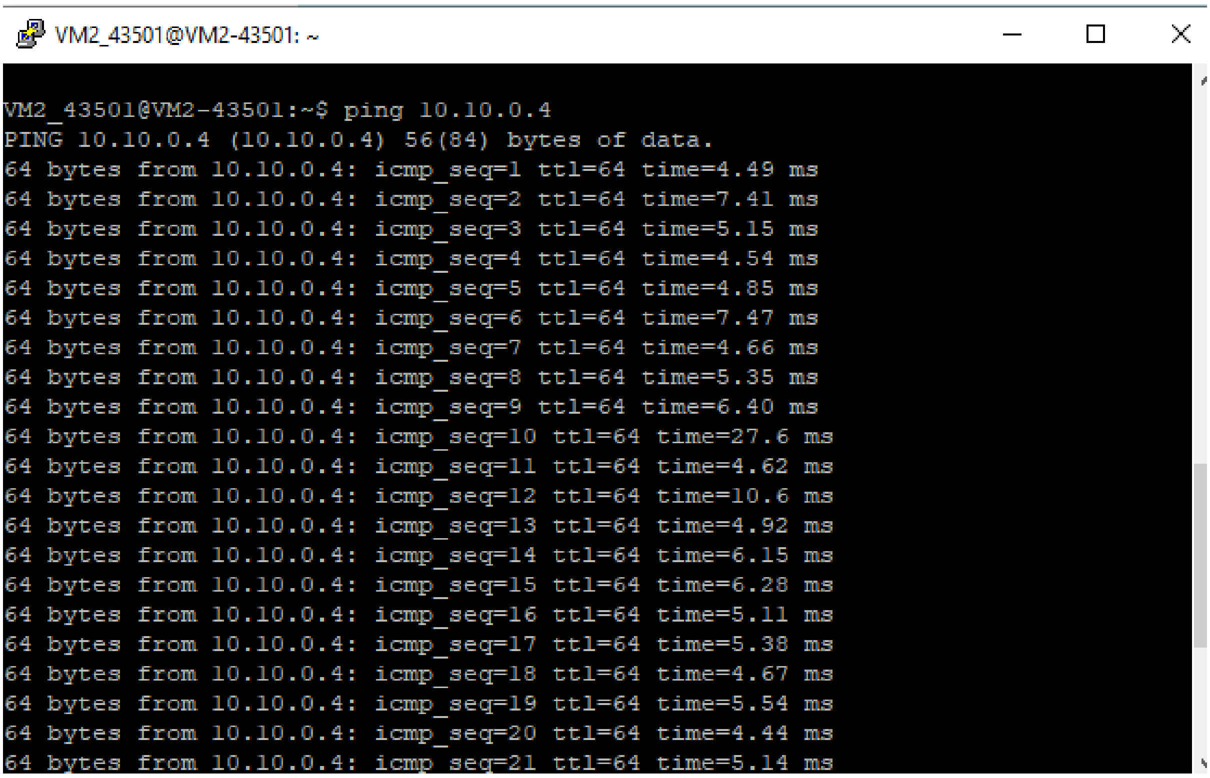


Screenshot 20: Ifconfig of VM2

Step 9:



Screenshot 21: Ping from VM 1 to VM 2



Screenshot 22: Ping from VM 2 to VM 1

Task 2: Risk management plan

Executive Summary

Risk treatment is the procedure of picking and implementing security measures to limit the risk. Risk treatment measures can contain retaining, transferring, optimizing, or avoiding risks and risks can be controlled internally by avoiding or by preventing the risks. Therefore, the report has been provided a risk assessment plan that will mitigate three identified security issues such as the distributed denial of service attacks, shared cloud computing services, and employee negligence. A distributed denial of service attack is a malevolent attempt by the attacker to interrupt the normal traffic of a targeted network, service, or server by flooding the target server. Shared cloud computing services is another security issues in cloud computing as it increases the chances of data theft or a breach in cloud computing. Finally, another security issue discussed in the report is employee negligence that will cause many data thefts or data breaches within the organization.

Distributed-Denial-of-Service Attacks

An attack of DDoS can be very much disruptive and they are being risen. It targets the IT services, cloud computing, and software. It is an attack that is intended to take offline a service or organization or otherwise render unusable resources that have an origin from hosts multiple in number (Bhushan & Gupta, 2019). The multiple host part of this attack is what makes it called distributed and this part makes the attack much more difficult to defend it.

- **Risk Mitigation Plan:** Protection of the network from the DDoS attack requires correct response planning. The mitigation plan's first step is to make the infrastructure DDoS resistant by having sufficient bandwidth in order to handle any kind of spikes that arise in the traffic which can be caused due to various malicious activities (Bawany, Shamsi & Salah, 2017). Having a secured DNS server is one of the ways of mitigating the attack from DDoS. The DNS server should have enough redundancy to make sure that such an attack does not happen. Another way is of installing anti-DDoS hardware and modules of the software.
- **Risk Monitoring Plan:** The steps that can be taken include performing frequent scans on the web services and fixing any type of vulnerable web applications in order to lessen the compromise risk, ensuring that the network used is protected with the help of prevention of intrusion and other threat management systems in order to help protect the assets of the network, ensuring that there is a presence of advance SIEM (Security Information and Event Management) solution in hands to

take care of security that is consolidated. There is also a need for a 24/7 monitoring and mitigation solution process.

Shared Cloud Computing Services

Cloud environments also experience threats at a very high level and the same ones as the traditional data center environments face. Actually, cloud computing run software, and software always face vulnerabilities (Abrar et al., 2018). There are problems like the consumers gets reduced visibility and control over the assets present there. There are also other problems faced like that of exposure to a set of application programming interfaces that are used by the customer in order to manage and interact with cloud services. The threat posing actors looks for various vulnerabilities that can be turned into successful attacks.

- **Risk Mitigation Plan**: There are several ways to mitigate it. They include, encryption of data at rest which means encrypting data at the situation where it protects the data that is used or in transit, then there is a two-factor authentication plan, elimination of the shared accounts, and insisting on a well-defined shared model of responsibility (Kar & Mishra, 2016). There are also other ways like usage of standardized cloud assessment questions and so on.
- **Risk Monitoring Plan:** In monitoring the risk, the ways include there should be two-factor authentication provided at the doorstep of this because that provides a high level of monitoring of the data at the primary position.

Employee Negligence

Cloud security is very much important for an organization as it protects the data stored on the internet from deletion, leakage, and theft. Employment negligence is an area of law that seriously affects the organization, other employees, and causes data breach. Therefore, employee negligence is the biggest cybersecurity risk for organizations all around the world. The laptops and computers used by the employee contain highly sensitive information and most of the organization's sensitive data breach or security incident happens due to a negligent or malicious activity.

- **Mitigation policy:** In order to mitigate the employee negligence risk, the organization needs to train out the employees about cybersecurity. Most of the riskiest offenses consider by the employees are potentially dangerous or negligent behavior such as leaves the computer unlocked while leaving the office. Therefore, organizations need to provide security training in their onboarding process to teach employees about cybersecurity and data protection best practices (Cunningham, Jones & Dreschler, 2018). When employees of an organization get frequent and proper training, they will become more sensitive and effectively protect the data of the organization. The organization also needs to develop security-focused culture by providing accessible training opportunities and by conducting regular information sessions for both old and new staff. Regular review procedure implementation helps to identify the negligence employees as well as the various security issues. Therefore, in order to manage the employee's negligence, the organization also needs to establish remote control over mobile security because the risks taken by employees are increase when they are working remotely such as in-home or coffee office. Therefore, an organization needs to implement all the above risk mitigation policies to mitigate employee negligence.

- **Risk monitoring and risk reviewing plan:** Risk monitoring and reviewing plan is a significant way to protect the organization's significant data from employee's negligence (Brown, 2020). The risk monitoring plan also helps to identify all the risks that harm the workplace of the organization. The organization needs to continuously monitor all the employees to protect the organization's sensitive data from breaches. The risk assessment plan will also contain good management practices that will train the employees about cyber security.

References

Abrar, H., Hussain, S. J., Chaudhry, J., Saleem, K., Orgun, M. A., Al-Muhtadi, J., & Valli, C. (2018). Risk analysis of cloud sourcing in healthcare and public health industry. *IEEE Access*, *6*, 19140-19150.

Bawany, N. Z., Shamsi, J. A., & Salah, K. (2017). DDoS attack detection and mitigation using SDN: methods, practices, and solutions. *Arabian Journal for Science and Engineering*, *42*(2), 425-441.

Bhushan, K., & Gupta, B. B. (2019). Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. *Journal of Ambient Intelligence and Humanized Computing*, *10*(5), 1985-1997.

Brown, A. (2020). *Why Are Non-Malicious Employees Non-Compliant: Guidance for Identifying Employee Negligence and Implementing Information Security Policies to Reduce Employees Inadvertently Becoming Insider Threats* (Doctoral dissertation, Utica College).

Cunningham, M. R., Jones, J. W., & Dreschler, B. W. (2018). Personnel risk management assessment for newly emerging forms of employee crimes. *International Journal of Selection and Assessment*, *26*(1), 5-16.

Kar, J., & Mishra, M. R. (2016). Mitigating Threats and Security Metrics in Cloud Computing. *JIPS*, *12*(2), 226-233.