**COMPLEXITIES OF THE CLOUD**

Term Definition : The cloud introduces different security concerns from on-premises setups:

Complex architecture Systems must be built to ensure basic security and allow infrastructure personnel to securely monitor, reconfigure, and redeploy machines as needed.

Extensive management The cloud offers more flexibility than organizations are used to, giving them freedom to create many more machines. This flexibility makes operations management more complex, requiring additional skills and techniques.

Different threats The cloud is exposed to public networks. Providers handle certain aspects of security,

which means security professionals have new and different considerations. Malicious actors will execute new escalation and lateral movement tactics.

Ensuring availability High availability of machines is a large part of security on the cloud. Ensuring availability and redundancy on the cloud is different than with on-premises environments.

**MODELS OF CLOUD SERVICES**

IaaS (Infrastructure as a Service)A service provider offerspay-as-you-go access to storage,networking, servers, and othercomputing resources in the cloud.

EXAMPLE : AWS, Azure, Google Cloud

PaaS (Platform as a Service) A service provider offers access to a cloud-based environment in which users can build and deliver applications. The provider supplies the underlying infrastructure.

EXAMPLE : Azure Classroom Labs

SaaS (Software as a Service) A service provider delivers software and applications through the internet. Users subscribe to the software and access it through the web or vendor APIs.

EXAMPLE : Office 365 Cloud Office Suite, Apple Cloud iWork

DaaS/DBaaS (Data as a Service/ Database as a Service) A service that provides a company's data product to the user on demand, regardless of geographic or organizational distance between provider and consumer.

EXAMPLE : Marketing company that keep databases of consumers categorized for many different industries.

CaaS (Communications as a Service) A service that provides an outsourced communications solution. such communications an include Voice over IP (VoIP or Internet telephony), instant messaging (IM), and collaboration and video conference applications.

EXAMPLE : Zoom, Facetime, Skype, GoToMeeting

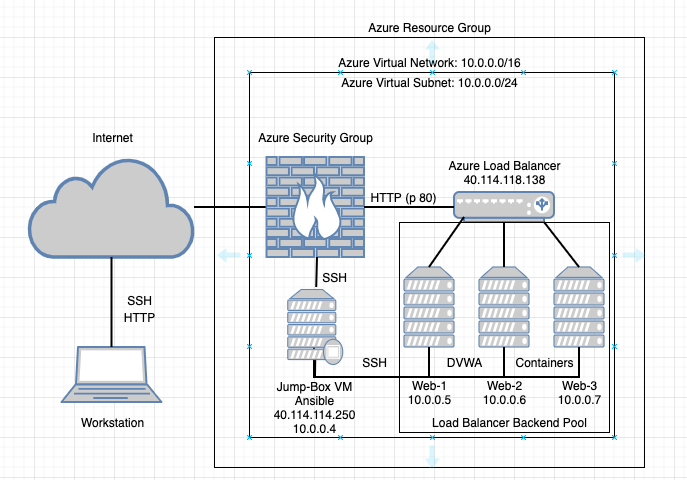
XaaS (Anything as a Service) Services providing all the offerings via cloud computing as opposed to locally, or on-premises.

EXAMPLE : Include Disaster Recovery as a Service (DRaaS), Communications as a Service (CaaS) and Network as a Service (NaaS).

Azure DDoS basic protection is integrated into the Azure platform by default and at no additional cost. Azure DDoS standard protection is a premium paid service that offers enhanced DDoS mitigation capabilities via adaptive tuning, attack notification, and telemetry to protect against the impacts of a DDoS attack for all protected resources within this virtual network.

Azure Bastion service is a new fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly in the Azure portal over SSL. When you connect via Azure Bastion, your virtual machines do not need a public IP address.

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources.



Base from this figure, below are the steps on how to create them .

Example of Building Resource Group and VNET/Virtual Networking

A. Setup Resource Group (Organizational Unit)

1. Search for Resource Group > Select > Add

2. Basics > Subscription: Free Trial, Resource Group: Red-Team, Region: (Canada) Canada East

3. Tags > Name: Blank > Value: Blank > Next and Leave Blank > Create

B. Setup VNet or Virtual Network (Networking)

1. Search Virtual Network > Select > Add

2. Subscription> Free Trial, Resource Group: Red-Team (Select Existing), Name: RedTeamNet, Region: Canada East

3. IP Address> Just use Default for IPV4 10.0.0.0/16 and Subnet 10.0.0.0/24

4. Security> BastionHost:Disabled , DDos protection: Basic, Firewall: Disabled

5. Tag: No Value > Create

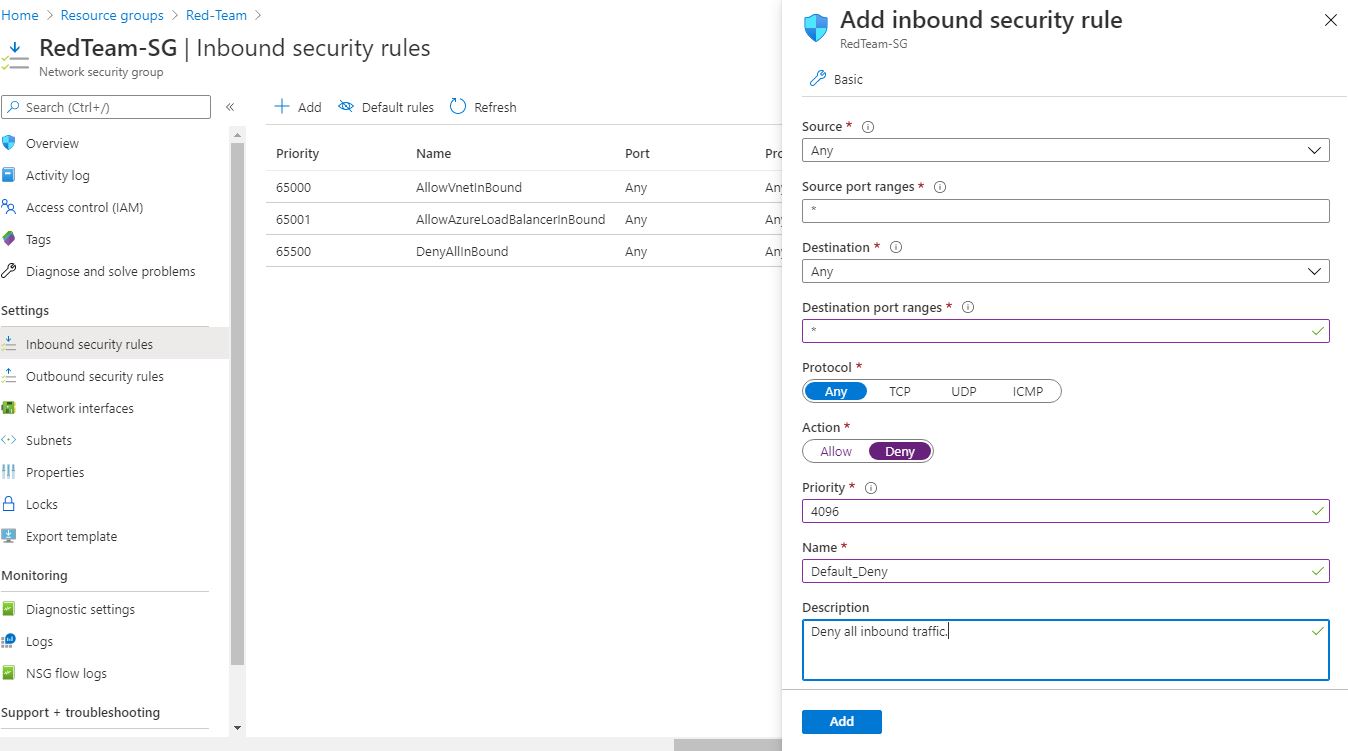
C. Setup Security Group (or A.K.A Cloud Based Firewall)

1. Search Network Security Group > Select > Add

2. Select Existing Resource Group > Name: RedTeam-SG

3. Tag: Blank > Create

4. Add Inbound Security Rules > Add >

* It is always best practice to Deny all Inbound from other Resource Group

D. Create an SSH Key

1. Open Git Bash Terminal, Linux Terminal or MAC Terminal – this case we are using Git Bash in Admin Privilege

Run $ ssh-keygen > Paraphrase: Enter (Blank) > Re Enter Paraphrase: Enter (Blank)

$ cd ~/.ssh

id\_rsa id\_rsa.pub

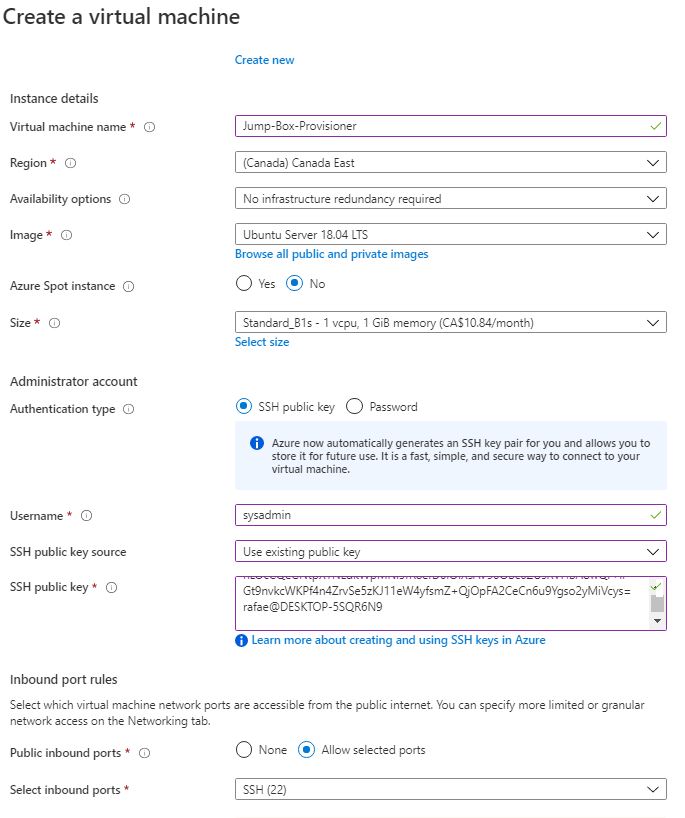
$ cat id\_rsa.pub

ssh-rsa  rafae@DESKTOP-5SQR6N9

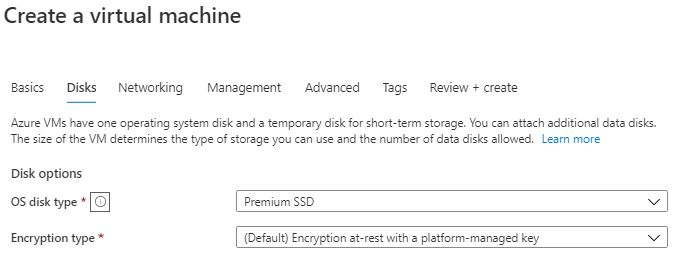
E. Create a Virtual Machine

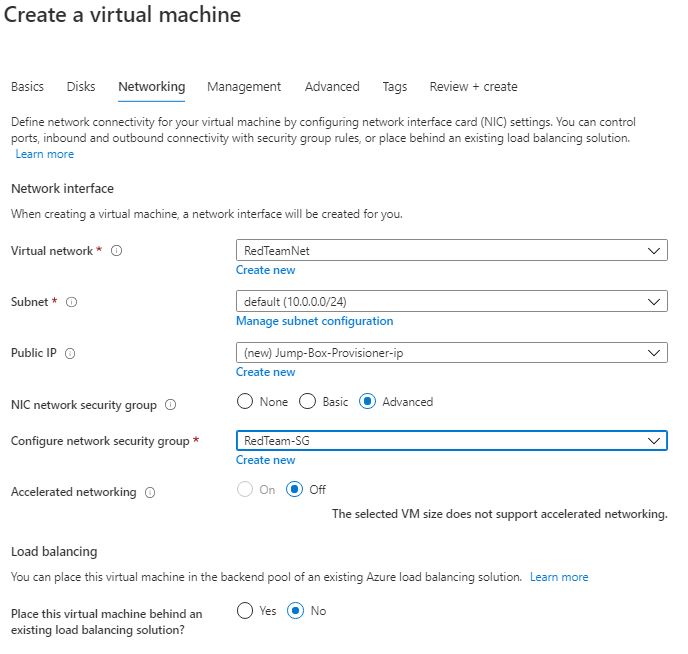
1. Select Resource Group : Red-Team , Name : Jump-Box-Provisioner, Region : Canada East

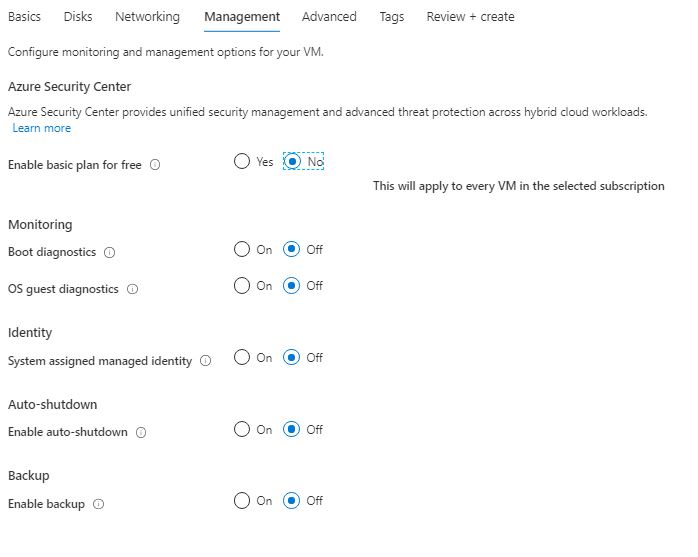
Copy the SSH key created: located in ~/.ssh/id\_rsa.pub



DISK

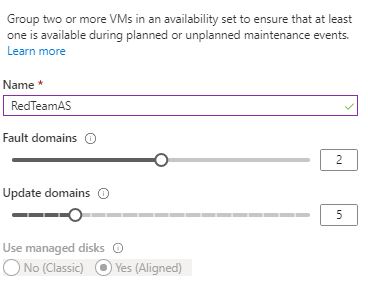


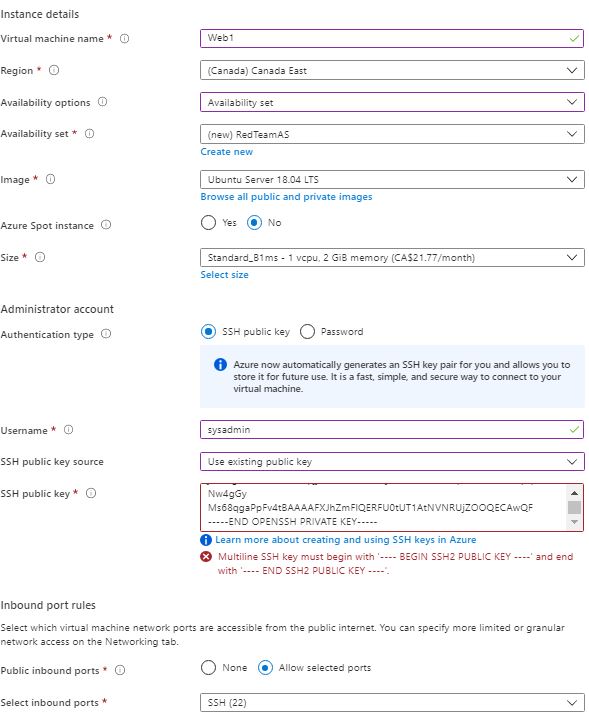
NETWORKING

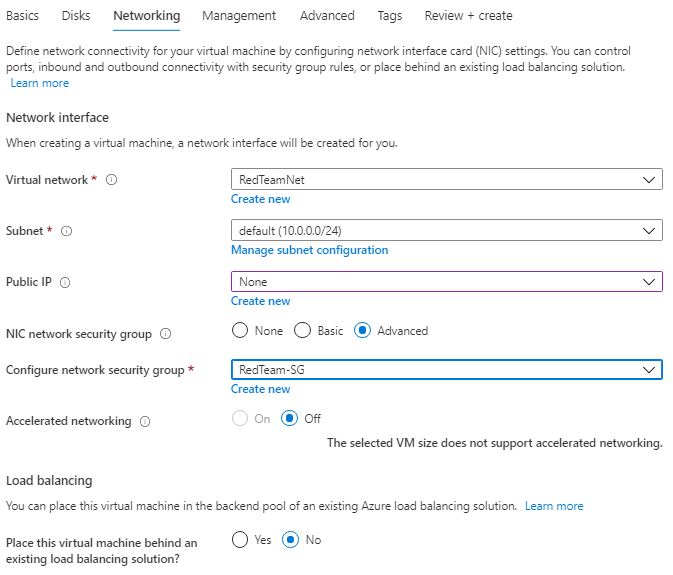
MANAGEMENT

NEXT > NEXT > NEXT > Create >> See below the setting of the first VM

F. Create a New VM named : Web1 and Web2 with Availability Set : Name RedTeamAS







Everything is Default on Disk, Management are all off, Advance is default, Tags is Default

Always search for the Resource Group and Select the Resource Group if creating an Environment otherwise it will not be assigned to the Resource Group