happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

Azure Bastion

Remote desktop RDP/SSH in Azure using Bastion Service as (PaaS)

Aure Bastion is a PaaS solution for your remote desktop which is more secure than the jump server. It comes with web-based login, and never expose VM public IP to the internet. This service will work seamlessly on your environment using VM's private IP address within your Vnet. Highly secure and trustable.

TABLE OF CONTENTS

ABSTRACT

This document guides you on Azure Bastion service, which is helpful for a remote solution on Azure cloud. Azure Bastion service is Platform As Service (PaaS) in Azure. The recent world health crisis and the economic crisis has massively accelerated the adoption of Cloud Technology. While public clouds provide more flexibility and scalability to set up the data centers on cloud, it also comes with a lot of security risks if the serves are not guarded properly, irrespective of whether it is Windows, Linux, or others. To accomplish day to day work, we need to login different remote servers using SSH/RDP, if we expose the server's public IP and Ports to the internet, this will leads high risk. So, we need to adopt a solution which is more secure than just exposing servers to the internet or using a Jump Server. In Azure, we can use Azure Bastion Service.

The audience of this document are those who move applications from on-premises to Azure or who build applications on the Azure. Such as cloud solution architect, remote desktop administrator, developers and operation team members, and those who involved in taking servers on remote to accomplish their day to day work.

INTRODUCTION

The rush to facilitate work from home for employees due to the pandemic has resulted in 1.5 million new RDP servers which are exposed to the internet. Thus, increasing the number of attacks in the month of March and April. (Lucian Constantin, CSO)

Not many companies have a full stock of unused laptops for their employees to take home on short notice. But, most of the companies still managed with the work from home scenario, which resulted in an increasing number of attacks. The RDP/SSH are frequently targeted for credential stuffing, password guessing and brute-force attacks which is on the list of common usernames and passwords combinations or credentials gained from different sources because all these ports open to the internet to access the machines.

Azure Bastion is a PaaS service published by the Microsoft Azure which is secure and seamless to access RDP and SSH to a virtual machine on your favorite web browser directly from the Azure portal. Azure Bastion must be provisioned on your virtual network (Vnet), and it will use the VM's Private IP to access the RDP/SSH. It doesn't need public IP address assigned to VM for access RDP/SSH. the connection establishes from your system to Azure VM using Secure Sockets Layer (SSL) protocol which is very secure.

CONCEPT OF BASTION

Before understanding the concept of Bastion service, let's talk about pre-authentication vulnerabilities that have been found in remote desktops. The vulnerability found on Remote Desktop Service (RDP) is called as Remote Code Execution. When an unauthenticated user connects to the system using RDP protocol, they send some specially crafted requests, and this vulnerability is pre-authenticated, which doesn't require any user interaction. An attacker who successfully exploits this can execute arbitrary code on the target system. Then the attacker will have access to view, change, create, or delete the data or can create a new admin account on target machines, and they can even install/uninstall any software in the target machine.

Let's understand the concept of Bastion and how it helps to overcome the above challenges.

The word "Bastions" means a projecting part of a fortification built at an angle to the line of a wall in layman language. You might have heard the term "Bastion" in cloud recently; however the term "Bastion" is not new, It is a very old concept to isolate your valuable machines or services behind the firewall and yet you have a way to access those resources. Here in Azure, valuable virtual machines are placed behind the firewall, Network Security Group, and more. Using Azure Bastion service if you need to connect to your Azure VM then first you must remote into the Bastion host through https connection, and then from Bastion, you will remote into your machine which is placed into your same Vnet which is also isolated using any network appliance or Network Security Group (NSG).

You can take any Azure machine right from the Azure portal, navigate to your VM and then click on connect using Bastion, which will open a new tab in your browser and connects.

WHAT'S AZURE BASTION

01

MANAGED RDP/SSH TO VMS OVER SSL

Azure Bastion is fully managed PaaS service, which provides you seamless remoting solution directly from the Azure portal over SSL connection. Azure Bastion can provision directly to your Vnet (Virtual Network), and all the VMs can be accessed from same Vnet (Virtual Network) over SSL without exposing your Public IP address.

02

ONE CLICK EXPERIENCE

Connect your RDP / SSH sessions directly from Azure Portal using a single click. Its support all latest browsers like Firefox, edge, chrome, and more.

03

RDP WITH PRIVATE IP

Login into your Azure virtual machines and avoid exposing your public IP address to the internet using SSH and RDP with private IP address only.

04

CONNECT SECURELY

Integrate and traverse existing firewalls and security perimeter using a modern HTML5 based web client and standard SSL ports and use your SSH keys for authentication when logging into your VM.

AZURE BASTION VS JUMP SERVER

Microsoft Azure is one of the biggest cloud solution providers, understands the threat of exposing RDP/SSH ports to the public internet. And if you use a jump server instead, even that exposing the RDP/SSH ports to the public internet will have several security risks. Here we need to understand Bastion host or jump servers both functions similarly, they segregate a private network or group of servers and external traffic. Usually, if you connect them using either RDP or SSH each create a single point of entry to a cluster, but their intended purpose and architecture are totally different in practice.

JUMP SERVER:	AZURE BASTION:
Azure IaaS Server is managed by us	Azure PaaS Service is managed by Microsoft.
Jump Server VM Deployed in Vnet but support all peer Vnets	Deployed in Vnet but doesn’t support all other Peer Vnets
Need to have RDP / SSH client to access VMs	No need any clients to access VMs works on all latest Browsers
Need to assign public IP Address to Jump Server	No need to have public IP to any of VMs
Need to Expose the RDP port to the internet	Works on port 443
Max concurrent users limit to RDP is 2	Max concurrent users limit to RDP is 25
Pricing would depend on VM size, and additional data transfer will cost	Pricing $0.19 per hour, first 5GB Data transfer is free per month.
Doesn’t gives users logging information	Gives users logging information to diagnose further which users had logged in which time.
Don’t have a live monitoring system in place	Has live remote monitoring system in place, you can view which users has connected on which VM and more.

BASTION KEY FEATURES

RDP AND SSH DIRECTLY FROM AZURE PORTAL:

You can get your VM remote directly from the Azure portal with single click irrespective of its Operating System.

REMOTE SESSION OVER TLS:

Azure Bastion service works on HTML5 based web browser, the connection establishes over TLS on port 443, enabling secure port 443. and it doesn't require any public IP address to be associated on your virtual machine. Azure Bastion opens the RDP/SSH connection to your VM through the machine's private IP address only. You don't need to expose public IP just for remoting, and you can save cost on public IP as well.

NO PUBLIC IP ADVERTISEMENT ON THE AZURE VM:

Azure Bastion always connects the RDP/SSH to your Azure VM using their private IP address. You don’t need any public IP address to connect remotely on your virtual machines.

NO HASSLE OF MANAGING NSGS:

Azure Bastion is a fully managed PaaS service which is provided by Microsoft from Azure, and it is hardened internally to provide you with Secure RDP/SSH connectivity, Azure Bastion service is hosted in its own subnet where you don't need to add any NSG because it connects your virtual machines over the private IP address, you can configure your NSG to allow RDP/SSH from Azure Bastion only. This is called the hassle of managing NSGs, every time you need to connect securely to your virtual machines.

PROTECTION AGAINST PORT SCANNING:

As you use Azure Bastion to remote your VMs, you don't need to expose ports to the public internet. VMs are protected against ports scanning by a rogue, and malicious users or hackers who reside on the public internet.

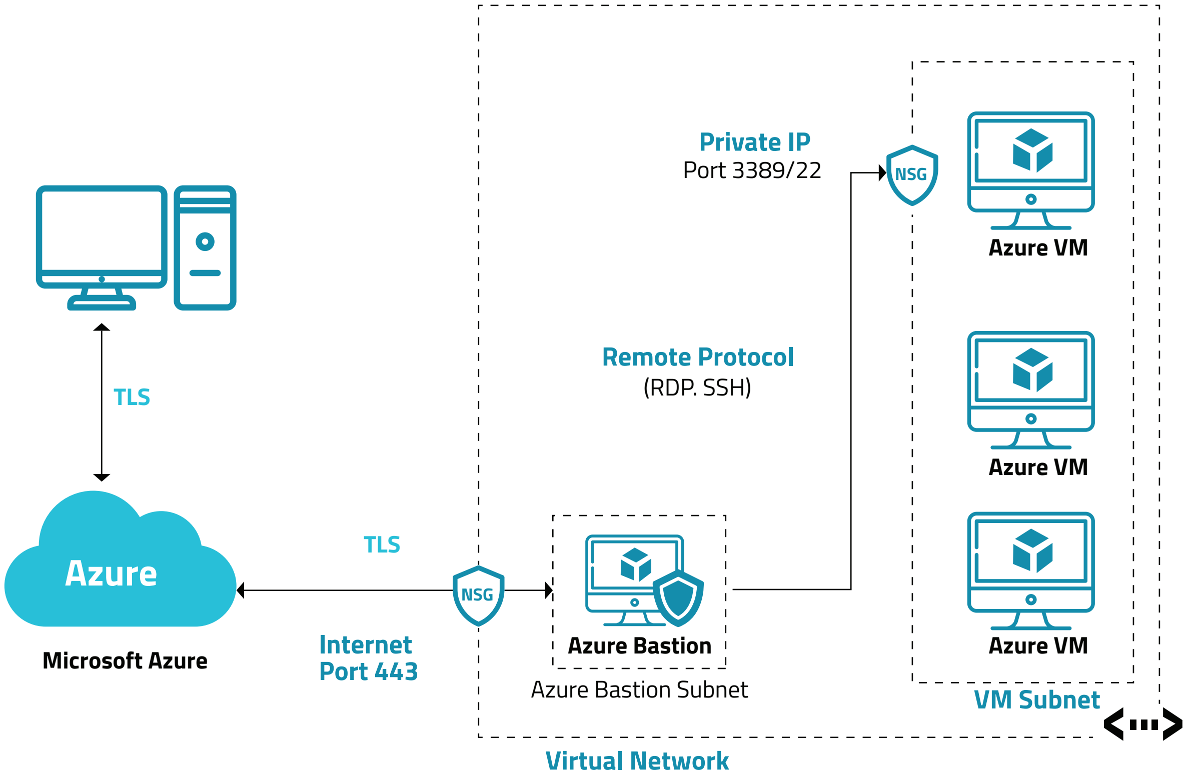
PROTECT AGAINST ZERO-DAY EXPLOITS:

As you know, Azure Bastion is completely managed service offered as PaaS by Azure. It lies at the perimeter of your virtual network, and you don't need to worry about the hardening of the virtual machine in your azure private network. Azure protects you against zero-day exploits by keeping the Bastion service hardened and always up to date for you.

BASTION ARCHITECTURE

Azure Bastion service deployment is per virtual Network (Vnet) but not per subscription/ account or virtual machine. Once you provision the Bastion service in your environment, then the RDP/SSH experience is available to all your virtual machines on the same network where you deployed your Bastion service.

To work with any of your virtual machines in cloud it's fundamental that you connect those machines using either RDP or SSH connection. But exposing the RDP/SSH ports to the public internet isn't a good idea, and it has seen significant threats surface in the past. This happens very often because of the protocol vulnerabilities. To avoid this kind of threats, Azure brought Bastion service to its users which is very secure and seamless service. Bastion host servers are designed in such a way that it can withstand the attacks. Bastion provides the RDP and SSH connectivity to the workload that resides behind the Bastion, as well as further inside the network.



The above figure shows the architecture of an Azure Bastion deployment. In this diagram:

The Bastion host is deployed in the virtual network	The user connects to the Azure portal using any HTML5 browser	The user selects the virtual machine to connect
With a single click, the RDP/SSH session opens in the browser	No public IP is required on the Azure VM	Copy / Paste only on text
Can connect anyone who has even read access on VM, NIC & Bastion	It works as RDS but doesn't require to have an RDS CAL license	

AUTHOR BIO

Zia has over 13 years of experience in windows servers, data center and Azure cloud. He has spent years on Azure operation services, Azure planning, designing, consulting, migrations, and trainings. He is currently a part of Azure infra structure at Happiest Minds Technologies working as senior tech lead. He is responsible for designing, migrating workloads to azure cloud.

happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

www.happiestminds.com

Business Contact **business@happiestminds.com**

About Happiest Minds Technologies

Happiest Minds Technologies Limited (NSE: HAPPSTMNDS), a Mindful IT Company, enables digital transformation for enterprises and technology providers by delivering seamless customer experiences, business efficiency and actionable insights. We do this by leveraging a spectrum of disruptive technologies such as: artificial intelligence, blockchain, cloud, digital process automation, internet of things, robotics/drones, security, virtual/augmented reality, etc. Positioned as 'Born Digital . Born Agile', our capabilities span digital solutions, infrastructure, product engineering and security. We deliver these services across industry sectors such as automotive, BFSI, consumer packaged goods, e-commerce, edutech, engineering R&D, hi-tech, manufacturing, retail and travel/transportation/hospitality.

A Great Place to Work-Certified™ company, Happiest Minds is headquartered in Bangalore, India with operations in the U.S., UK, Canada, Australia and Middle East.