

Student Name:

Weight: 3%

Student ID:

Marks: /10

Lab: Azure Security Tools

Lab Objectives

In this lab, you'll explore how to use the Azure security tools. You will:

1. Create a bastion.
2. Review the DDoS Protection service.
3. Configure a firewall.
4. Create shared access signatures (SAS).
5. Create a key vault.

Lab Requirements

- Up to date web browser
- Azure account
- Virtual machine with Azure Storage explorer installed

Instructions

1. Working individually, follow the procedure below.
2. Take screenshots, as described in the *Marking Criteria* section.
3. Create a document that includes all screenshots appropriately titled and described, and then upload it to the Lab assignment drop box.
4. Be sure to include your name and student ID in the document.

Marking Criteria

Screenshots	Marks
Bastion configuration	/2
Firewall, route table and rules	/4
Storage Explorer SAS connection	/1
Linux SAS configuration and connection	/2
Key in Key Vault	/1
Total	/10

Note: This icon indicates when a screenshot is required.

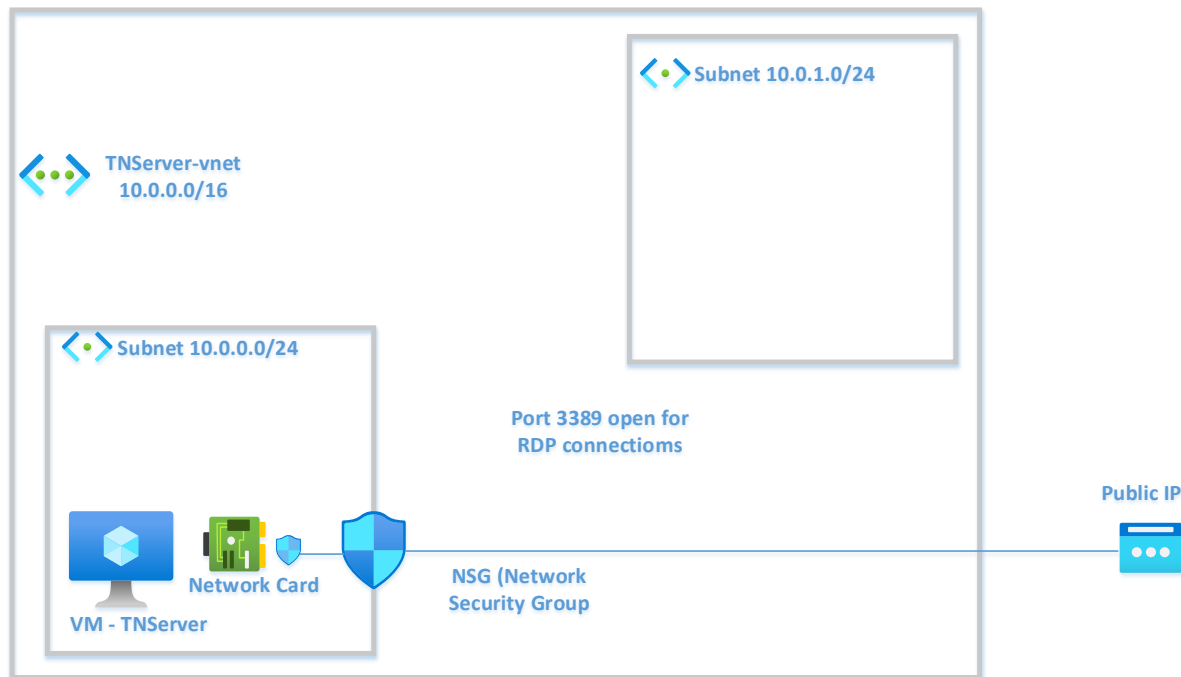


Source: Flatiron.com, Freepik, Image: [screenshot_983871](#)

Procedure

Part 1: Create a Bastion

In the network section of this course, you looked at NSGs and how they block or allow traffic on network interfaces and subnets. One of the things you created in that lab was a simple network with a virtual machine.



© 2023, Southern Alberta Institute of Technology.
This figure was designed with icons from Microsoft Azure.

When you created the virtual machine, the network interface and the NSG were created. You also configured the system to allow RDP connections on port 3389 so you could talk to the operating system on the virtual machine. A public IP address was required for the RDP connection. You could also use this with protocols like SSH or WinRM.

Inbound port rules
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

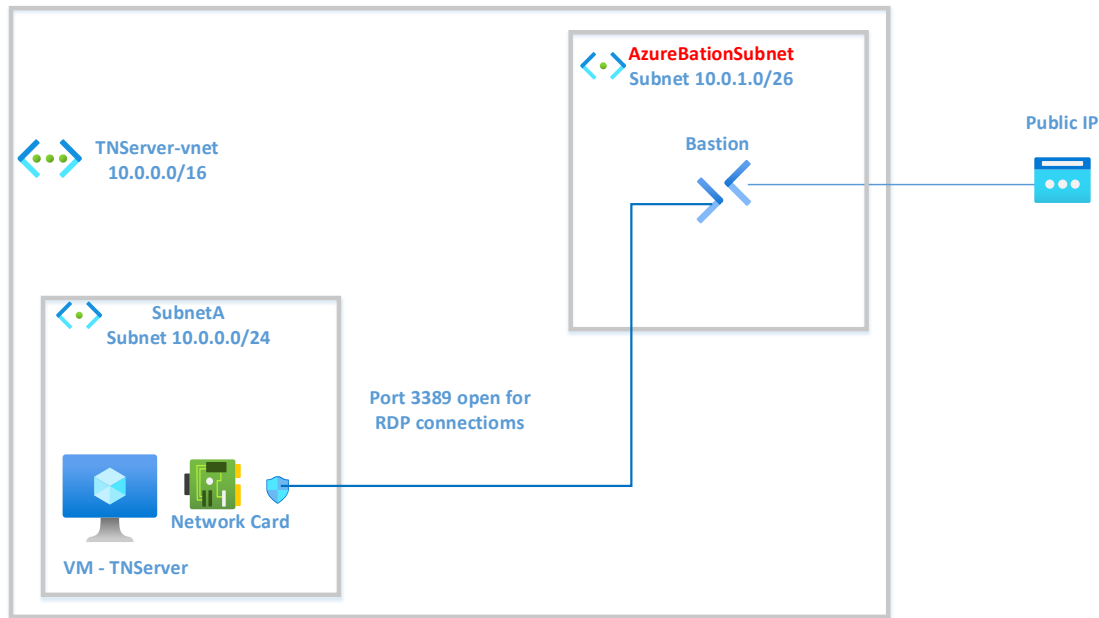
Public inbound ports * ☐ None ☒ Allow selected ports

Select inbound ports *

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

© 2023, Microsoft Azure. Used with permission from Microsoft.

Having an RDP connection on the internet, or open from other unknown networks, isn't secure and wouldn't be done in enterprise systems. Common practise is to create a bastion host or jump-box in a separate subnet to protect the traffic. Azure Bastion serves this purpose. This is a fully managed service, meaning that you don't need to harden it, protect against port scanning or manage it yourself.



© 2023, Southern Alberta Institute of Technology.
This figure was designed with icons from Microsoft Azure.

- ☐ Using PowerShell, create the network, server and two subnets shown in the figure above.

Notes:

- The bastion subnet must be named AzureBastionSubnet and have a CIDR prefix of at least /26.
- For a reminder of PowerShell commands, see: [Create a Windows Server VM by using PowerShell in Azure Stack Hub](https://learn.microsoft.com/en-us/azure-stack/user/azure-stack-quick-create-vm-windows-powershell) (<https://learn.microsoft.com/en-us/azure-stack/user/azure-stack-quick-create-vm-windows-powershell>).

- ☐ In the Azure portal, search for and navigate to the Bastion service.
- ☐ Click the **Create** button and fill in the resource group, name and region.
- ☐ The Tier selection is equivalent to the SKU and the tier you select determines the features available and the cost. Select the **Standard** tier.

Note: See tier details at: [SKUs](https://learn.microsoft.com/en-us/azure/bastion/configuration-settings#skus) (<https://learn.microsoft.com/en-us/azure/bastion/configuration-settings#skus>) [link](#).

- ☐ Leave the **Instance Count** (like the scaling you learned about in the Virtual Machines lab) at the default of **two**.

- ☐ Select your virtual network and the **AzureBastionSubnet**, and then review and create the bastion.

It may take several minutes to create the resource.

Create a Bastion ...

[Basics](#)
[Tags](#)
[Advanced](#)
[Review + create](#)

Bastion allows web based RDP access to your vnet VM. [Learn more](#)

Project details

Subscription *

Tootechi

Resource group *

TestNetwork

Create new

Instance details

Name *

BastionTest

Region *

Canada Central

Tier * ⓘ

Standard

Instance count * ⓘ

2

Configure virtual networks

Virtual network * ⓘ

TNServerr-vnet

Create new

Subnet *

AzureBastionSubnet (10.0.1.0/26)

Manage subnet configuration

Public IP address

Public IP address * ⓘ

☒ Create new
☐ Use existing

Public IP address name *

TNServerr-vnet-ip

Public IP address SKU

Standard

Assignment

☐ Dynamic
☒ Static

© 2023, Microsoft Azure. Used with permission from Microsoft.

- ☐ Go to the main page for the virtual machine and select **Connect** from the top menu.
- ☐ Select **Bastion** and click the **Use Bastion** button.
- ☐ If you click the drop-down arrow beside *connection settings* you can select **RDP** or **SSH** for your connection.

- ☐ Enter the username and password for the virtual machine. The authentication type can be a password or a key from a key vault. You'll explore key vaults later in this unit.
- ☐ Click the **Connect** button.

Note: If you have a pop-up blocker enabled in your browser, you need to allow connections from this site or disable it.

Another tab opens in your browser as your remote link to the server. You are now working with the server but through the Bastion service.



Part 2: Review the DDoS Protection Service

Azure Bastion won't protect you from DDoS attacks, but you can apply the Azure DDoS service to networks and IP addresses to address this issue. DDoS is quite expensive, so in this section you'll examine the service options but not actually engage the service.

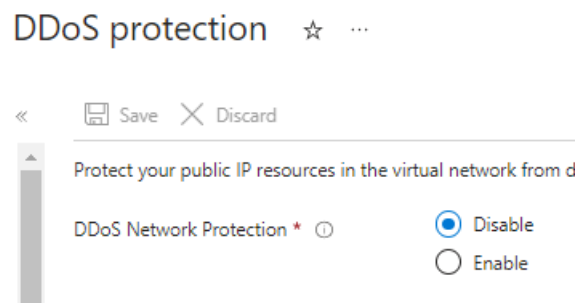
Note: See DDoS pricing information at: [Azure DDoS Protection pricing](https://azure.microsoft.com/en-us/pricing/details/ddos-protection/) (https://azure.microsoft.com/en-us/pricing/details/ddos-protection/).

Azure creates three mitigation policies that are auto-tuned for each public IP on the resource it is attached to.

- TCP SYN
- TCP
- UDP

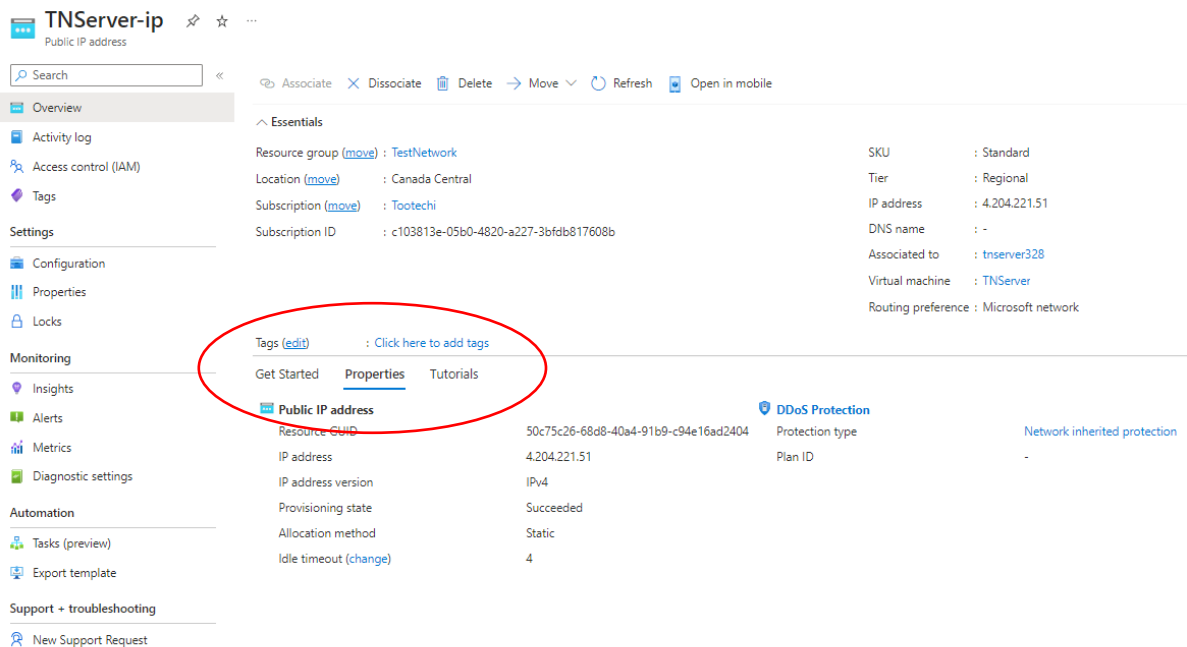
- ☐ Before you can use the DDoS service you have to have a DDoS Protection Plan. Search for and navigate to the **DDoS Protection Service**.
- ☐ Click the **Create** button and review the options. Note that this is a very simple setup, requiring only the resource group, name and region.
- ☐ Back out of the page without creating a DDoS protection plan.
- ☐ Navigate to the main page for your network and select **DDoS Protection** from the blade menu.

To use DDoS on this network, you would click the Enable button. **Don't enable it.**



© 2023, Microsoft Azure. Used with permission from Microsoft.

- ☐ Navigate to the main page for your public IP address and select the **Properties** tab in the middle menu.



TNServer-ip
Public IP address

Search << Associate X Dissociate Delete → Move Refresh Open in mobile

Overview

Activity log
Access control (IAM)
Tags
Settings
Configuration
Properties
Locks
Monitoring
Insights
Alerts
Metrics
Diagnostic settings
Automation
Tasks (preview)
Export template
Support + troubleshooting
New Support Request

Essentials

Resource group (move) : TestNetwork
Location (move) : Canada Central
Subscription (move) : Tootechi
Subscription ID : c103813e-05b0-4820-a227-3bfd817608b

SKU : Standard
Tier : Regional
IP address : 4.204.221.51
DNS name : -
Associated to : tnserver328
Virtual machine : TNServer
Routing preference : Microsoft network

Tags (edit) : Click here to add tags

Get Started Properties Tutorials

Public IP address

Resource GUID	50c75c26-68d8-40a4-91b9-c94e16ad2404
IP address	4.204.221.51
IP address version	IPv4
Provisioning state	Succeeded
Allocation method	Static
Idle timeout (change)	4

DDoS Protection

Protection type : Network inherited protection
Plan ID : -

© 2023, Microsoft Azure. Used with permission from Microsoft.

- ☐ Select **DDoS** from the middle menu. You see the option to apply it to either your network or just this IP address.
- ☐ Do not complete the configuration.

Configure DDoS Protection

Azure DDoS protection can help defend against DDoS (distributed denial of service) attacks directed at your resources. Select a DDoS protection setting for your IP address. [Learn more](#)

Protection type

☒ Network
Inherits DDoS protection from virtual network

☐ IP
Specific to this IP address

☐ Disable

© 2023, Microsoft Azure. Used with permission from Microsoft.

- ☐ Delete your resources to stop accruing costs.

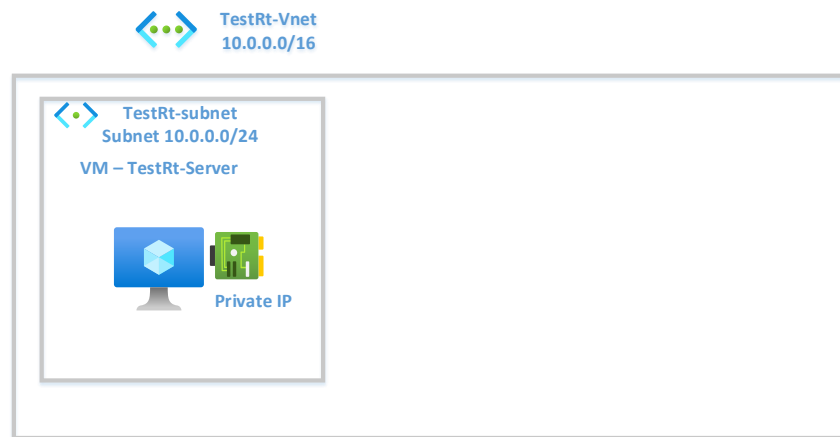
Part 3: Configure a Firewall

Azure has two firewall services:

- Firewalls – protects VNets and virtual WANs
- WAF (Web Application Firewall) – protects your web applications

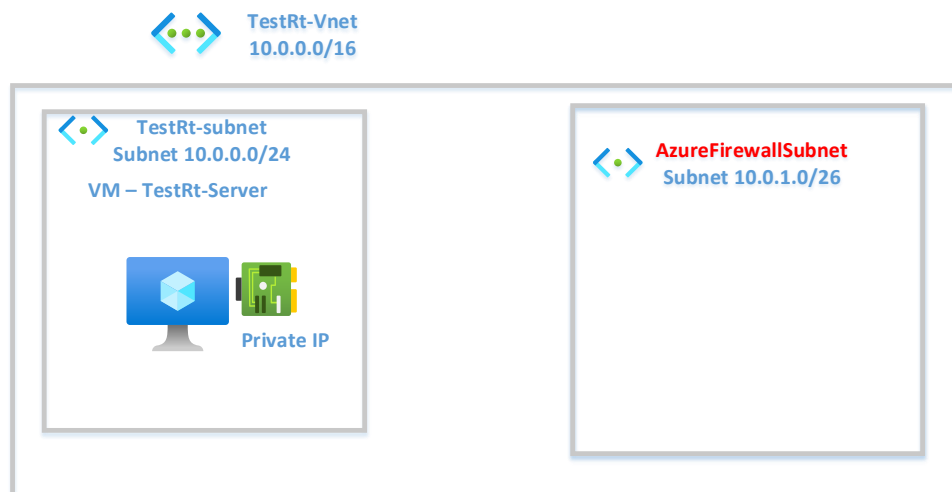
- ☐ Create the virtual machine and subnets shown in the figure below.

Note: The Server does not have a public IP address or any public inbound ports.



© 2023, Southern Alberta Institute of Technology.
This figure was designed with icons from Microsoft Azure.

- ☐ Just like the Bastion service, the Firewall service requires a subnet of its own and it must have the name **AzureFirewallSubnet**. Add the firewall subnet shown in the drawing below.

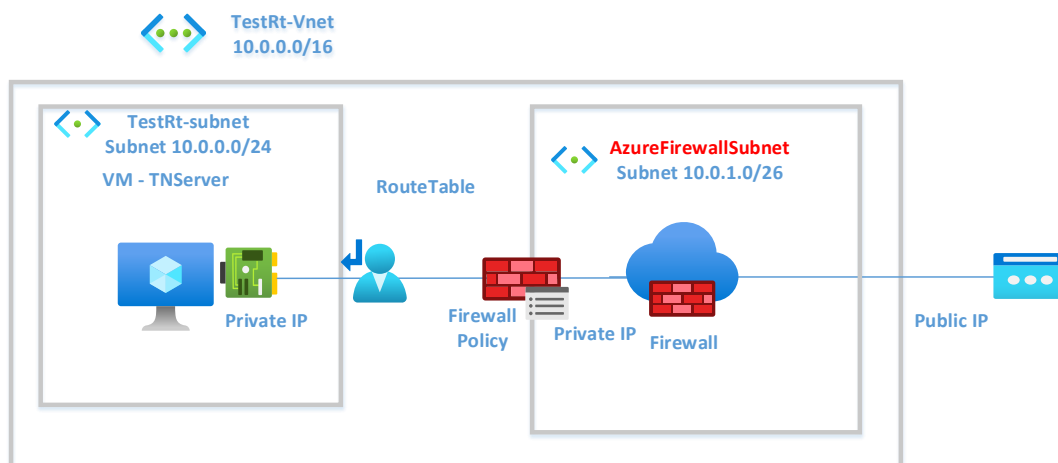


© 2023, Southern Alberta Institute of Technology.
This figure was designed with icons from Microsoft Azure.

In the steps that follow, you'll complete these tasks:

- Create a firewall in the firewall subnet.
- Create a route table.
- Create a route between the subnets in the route table.
- Create an application rule in the firewall that allows outbound access to Google.
- Create a network rule in the firewall that allows outbound DNS access.
- Create a DNAT rule in the firewall to allow RDP to your virtual machine.

By the end of this part of the lab, you'll be able to connect to the virtual machine through the firewall using RDP, open the browser on the virtual machine, perform a DNS request for Google, and then connect to Google, all completed securely through the firewall.



© 2023, Southern Alberta Institute of Technology.
This figure was designed with icons from Microsoft Azure.

To create a firewall in the firewall subnet

- ☐ Search for and navigate to the **Firewalls** service.
- ☐ Click **Create a Firewall** from the top menu.
- ☐ Enter the resource group, name and region.

Notes:

- Azure has three SKUs for a firewall and the SKU determines the features and pricing.
 - Read: [Choosing the right Azure Firewall SKU to meet your needs](https://learn.microsoft.com/en-us/azure/firewall/choose-firewall-sku) (<https://learn.microsoft.com/en-us/azure/firewall/choose-firewall-sku>).
- ☐ Select **Standard** for the SKU and make sure that **Use a Firewall Policy to manage this firewall** is selected.

Azure firewall policies are used to manage sets of rules about filtering traffic.

- ☐ Create a new policy in the same region as your network and virtual machine.

Create a new Firewall Policy

This will create a new firewall policy with default settings. You can customize your policy after creation.

Policy name *

Region

Policy tier ☐ Basic ☒ Standard ☐ Premium

© 2023, Microsoft Azure. Used with permission from Microsoft.

- ☐ Select your firewall network and create a new public IP.

Add a public IP

Name * ✓

SKU ☐ Basic ☒ Standard

Assignment ☐ Dynamic ☒ Static

© 2023, Microsoft Azure. Used with permission from Microsoft.

- ☐ Review and create the firewall.

Create a firewall ...

Instance details

Name *	TestRt-Firewall ✓
Region *	Canada Central ▼
Availability zone ⓘ	None ▼

i Premium firewalls support additional capabilities, such as SSL termination and IDPS. Additional costs may apply. [Learn more](#)

Firewall SKU	<input type="radio"/> Basic <input checked="" type="radio"/> Standard <input type="radio"/> Premium
Firewall management	<input checked="" type="radio"/> Use a Firewall Policy to manage this firewall <input type="radio"/> Use Firewall rules (classic) to manage this firewall
Firewall policy *	(New) TestRt-FirewallPolicy ▼ Add new
Choose a virtual network	<input type="radio"/> Create new <input checked="" type="radio"/> Use existing
Virtual network	TestRt-vnet (TestRt-RG) ▼
Public IP address *	(New) TestRt-FirewallPubIP ▼ Add new
Forced tunneling ⓘ	<input checked="" type="checkbox"/> Disabled ⓘ

© 2023, Microsoft Azure. Used with permission from Microsoft.

- ☐ Go to the main page for the firewall and make a note of the private and public IP addresses.

Next, you'll create a routing table to route traffic from **TestRt-Subnet** to the firewall subnet.

To create a route table

- ☐ Open the **Route Tables** tool and create a new route table.

Create Route table ...

Basics Tags Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Resource group * ⓘ

Tootechi

TestRt-RG

[Create new](#)

Instance details

Region * ⓘ

Name * ⓘ

Propagate gateway routes * ⓘ

Canada Central

TestRt-RouteTable

☒ Yes

☐ No

© 2023, Microsoft Azure. Used with permission from Microsoft.

To create a route between the subnets in the route table

- ☐ When the resource is created, go to the main page for the route table.
- ☐ Select **Subnets** from the blade menu and associate the **TestRt-Subnet** with the route table.

Associate subnet ×

TestRt-RouteTable

Virtual network * ⓘ

Subnet * ⓘ

TestRt-vnet (TestRt-RG)

TestRt-subnet

© 2023, Microsoft Azure. Used with permission from Microsoft.

- ☐ Select **Routes** from the blade menu and add a new route to the table. The route should send all destination addresses (0.0.0.0/0) to the private IP of the firewall virtual appliance, so the **Next Hop address** is the private IP of the firewall.

TestRt-RouteToFirewall ...

TestRt-RouteTable

Destination address prefix * ⓘ

IP Addresses

Destination IP addresses/CIDR ranges * ⓘ

0.0.0.0/0

Next hop type * ⓘ

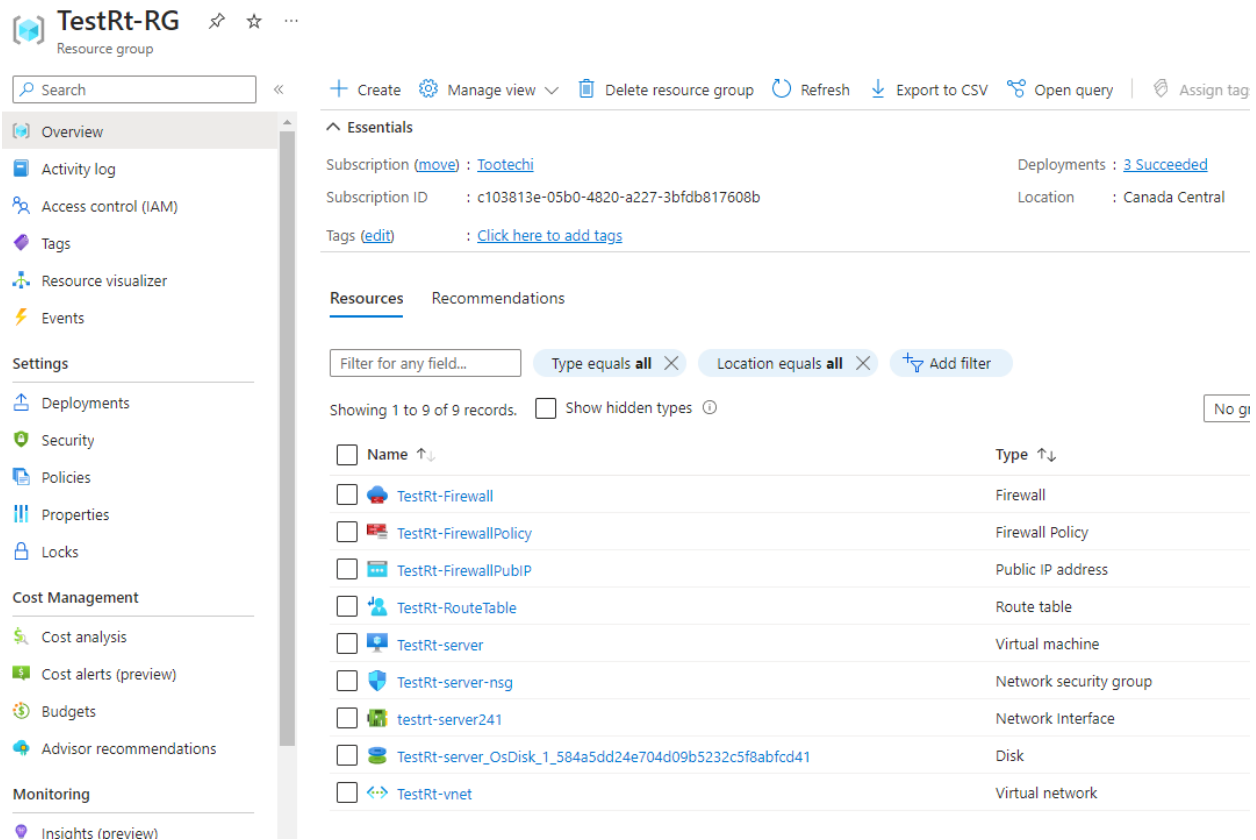
Virtual appliance

Next hop address * ⓘ

10.0.1.4

© 2023, Microsoft Azure. Used with permission from Microsoft.

- ☐ Go to the main page for the resource group and examine the individual components that have been created.



TestRt-RG
Resource group

Search

+ Create Manage view Delete resource group Refresh Export to CSV Open query Assign tag

Essentials

Subscription (move) : [Tootechi](#) Deployments : [3 Succeeded](#)

Subscription ID : c103813e-05b0-4820-a227-3bfdb817608b Location : Canada Central

Tags (edit) : [Click here to add tags](#)

Resources Recommendations

Filter for any field... Type equals all Location equals all Add filter

Showing 1 to 9 of 9 records. Show hidden types No g

Name	Type
TestRt-Firewall	Firewall
TestRt-FirewallPolicy	Firewall Policy
TestRt-FirewallPubIP	Public IP address
TestRt-RouteTable	Route table
TestRt-server	Virtual machine
TestRt-server-nsg	Network security group
testrt-server241	Network Interface
TestRt-server_OsDisk_1_584a5dd24e704d09b5232c5f8abfcd41	Disk
TestRt-vnet	Virtual network

© 2023, Microsoft Azure. Used with permission from Microsoft.

Next, you'll set the firewall policy.

To create an application rule in the firewall that allows outbound access to Google

- ☐ Navigate to the main page of the new firewall policy and notice the options for rules.

The rule types are:

- Application rules – allow you to set the FQDNs that can be accessed from a VNet.
- Network rules – allow you to set the rules that contain source addresses, protocols, destination ports and destination addresses.
- DNAT rules – allow NAT translation

As an example, you'll create an application rule collection that contains a rule, and that rule allows outbound access to Google.

- ☐ Select **Application Rules** from the blade menu and click **+ Select a Rule Collection** on the top menu.
- ☐ Create the rule collection and rule as shown below.

Add a rule collection



Name *	TestRt-GoogleRuleCollect						✓
Rule collection type *	Application						✓
Priority *	201						✓
Rule collection action	Allow						✓
Rule collection group *	DefaultApplicationRuleCollectionGroup						✓
Rules							
Name *	Source type	Source	Protocol *	TLS inspection	Destination Type *	Destination *	
TestRt-GoogleRule ✓	IP Address	10.0.0.0/24 ✓	http, https ✓	<input type="checkbox"/> TLS inspection	FQDN	www.google.ca ✓	⋮

© 2023, Microsoft Azure. Used with permission from Microsoft.

To create a network rule in the firewall that allows outbound DNS access

- ☐ Select **Network Rules** from the blade menu and click **+ Select a Rule Collection** on the top menu.
- ☐ Create the collection and rule to allow Google's DNS server at 8.8.8.8 on port 53.

Add a rule collection



Name *	TestRt-DNSRuleCollection						✓
Rule collection type *	Network						✓
Priority *	200						✓
Rule collection action	Allow						✓
Rule collection group *	DefaultNetworkRuleCollectionGroup						✓
Rules							
Name *	Source type	Source	Protocol *	Destination Ports *	Destination Type *	Destination *	
TestRt-DNSRule ✓	IP Address	10.0.0.0/24 ✓	UDP	53 ✓	IP Address	8.8.8.8 ✓	⋮
	IP Address	*, 192.168.10.1, 192...	0 selected	80,8000-9000	IP Address	*, 10.0.0.1, 10.1.0.0/1...	

© 2023, Microsoft Azure. Used with permission from Microsoft.

Lastly, you'll create a DNAT rule to allow network translation for the RDP connections.

When you create a virtual machine, it receives its IP address and other information from the default DHCP service on the Azure network. Since the VM doesn't have a public IP address, it won't have information for a DNS server on the internet. When you set up the network rule, you choose to use Google's DNS service at 8.8.8.8, so you need to tell the virtual machine to use that address, otherwise it won't be allowed through the firewall.

Edit DNAT rules ×

Any changes you make here will be applied to all selected rules.

Name *

TestRt-DNATRule

Source Type

IP Address

Source IP Addresses *

*

Destination IP Addresses

20.104.51.79

Protocol *

TCP

Destination Ports *

3389

Translated Type

IP address

Translated Address *

10.0.0.4

Translated Port *

3389

© 2023, Microsoft Azure. Used with permission from Microsoft.

To create a DNAT rule in the firewall to allow RDP to your virtual machine

- ☐ Go to the main page for your VNet and select **DNS Servers** from the blade menu.
- ☐ Select **Custom**, and then add the DNS server's IP address.

DNS servers ⓘ

☐ Default (Azure-provided)

☒ Custom

IP Address

8.8.8.8 ✓

Add DNS server

© 2023, Microsoft Azure. Used with permission from Microsoft.

- ☐ To get the new DNS information into the VM, restart it.

To test the connection

- ☐ Open the RDP connection on your laptop and connect to the public IP address of the firewall.

Your request is allowed through the firewall because of the network rule, and then it is translated by the DNAT rule.

- ☐ Open the web browser and go to google.com and then google.ca.

Neither of these will be allowed because the FQDN you used is www.google.ca.

- ☐ Try it and you should be successful.

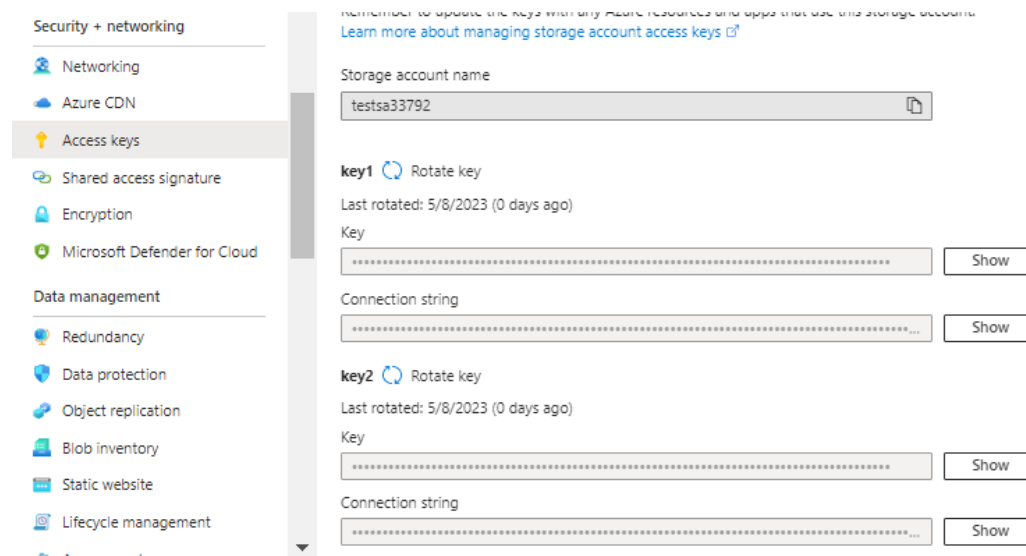


Part 4: Create a Shared Access Signatures

In Azure, storage at rest in the cloud is automatically encrypted for security. As is common in IT systems, keys are used for access security in Azure. When you create a storage account, two keys are created to access it.

- ☐ Navigate to the **Storage Accounts** page and select **Create Storage Account**.
- ☐ Fill in the resource group and name, and then select **Standard** with **LRS**.
- ☐ Click **Next** to go to the **Advanced** page and review the security options.
- ☐ Click **Next** to go to the **Network** page, where you can set the access to public or private.
- ☐ Review and create the storage account.
- ☐ Go to the main page and select **Access Keys** from the blade menu.

You should have two keys that can be rotated. Each key has a connection string that can be used to access the account.

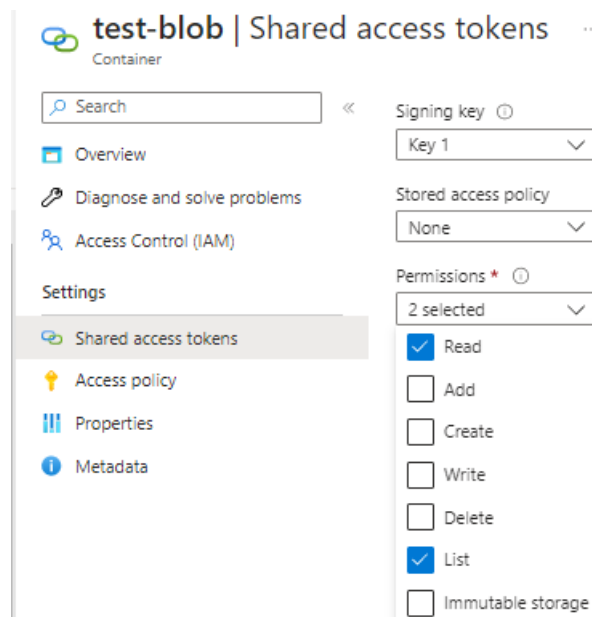


© 2023, Microsoft Azure. Used with permission from Microsoft.

The access keys and connection string allow you to access the storage account but they don't give you detailed control over that access. SAS gives you more granular control over the accounts, such as:

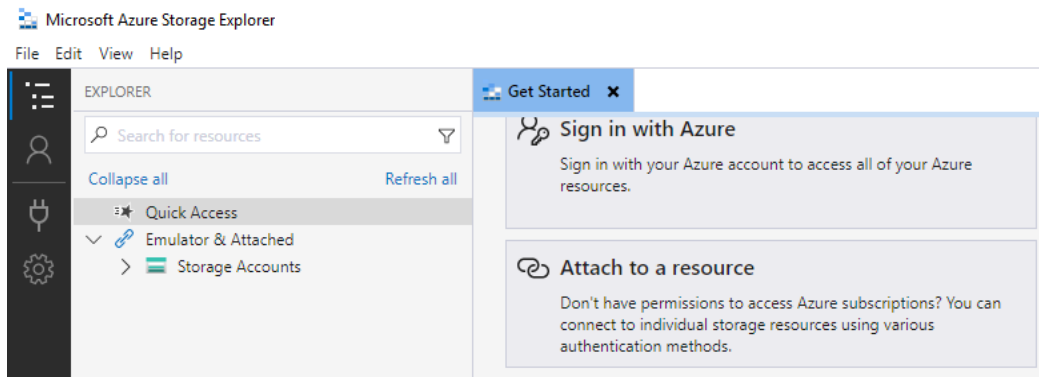
- What, specifically, the user/resource needs to access in the storage account (e.g., the account, the container, or a single blob)
- How long access to storage permission lasts (start and expiry times)
- From which IPs the storage can be accessed
- Which protocol (HTTP or HTTPS)

- ☐ Select **Containers** from the blade menu and select **+ Container** from the top menu.
- ☐ Give the container a name and note the *Public Access Level* settings.
- ☐ Choose **Private** and create the container.
- ☐ Upload a few pictures or files to the container.
- ☐ Select the container. Verify that you don't have an access key option for the container but there is a Shared Access Tokens option.
- ☐ Select the **Shared Access Tokens** from the blade menu.
This is where you can configure two keys and what access they have to the container.
- ☐ For **Key 1**, select the **Read** and **List** permissions.



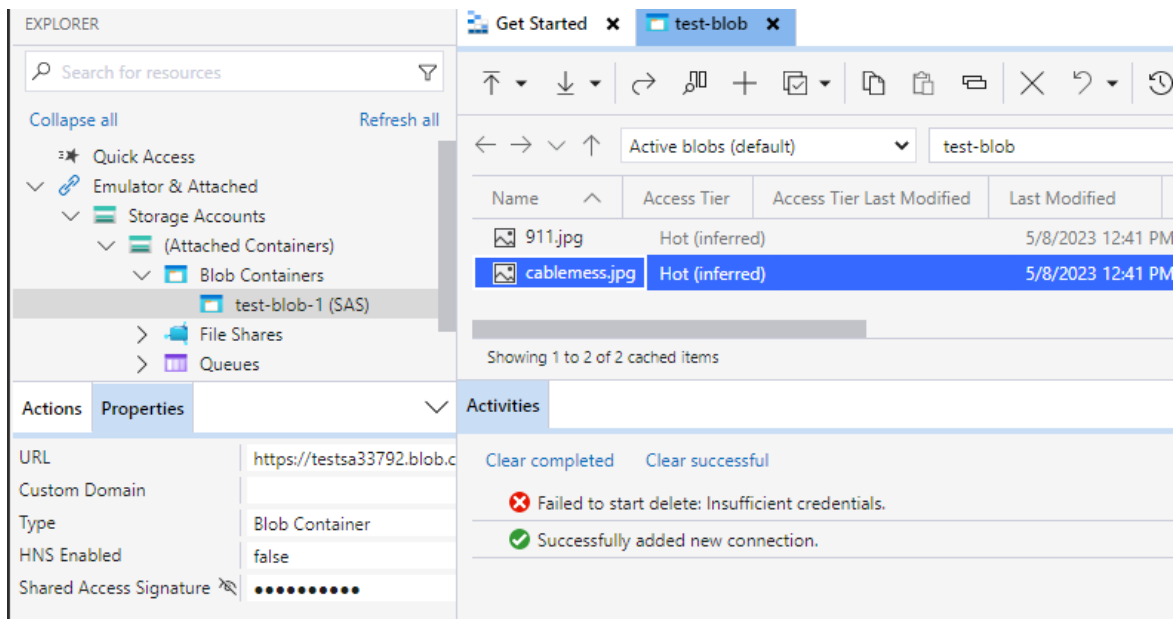
© 2023, Microsoft Azure. Used with permission from Microsoft.

- ☐ Review the interval, IP and protocol options, and then generate the tokens.
- ☐ Copy the Blob SAS URL.
- ☐ Go to your local VM and open the Azure Storage Explorer but do not log in.
- ☐ Select the **Attach to a Resource** option, and then select **Blob Container**.



© 2023, Microsoft Azure. Used with permission from Microsoft.

- ☐ Select **Shared Access URL (SAS)** and click **Next**.
- ☐ Paste the Blob SAS URL to the **Blob Container SAS URL** box.
The Display Name is automatically created.
- ☐ Click **Next**, review the information and click **Connect**.
- ☐ Test your access by attempting to delete one of your blobs, which should fail because you only have read and list permissions with that URL.



© 2023, Microsoft Azure. Used with permission from Microsoft.



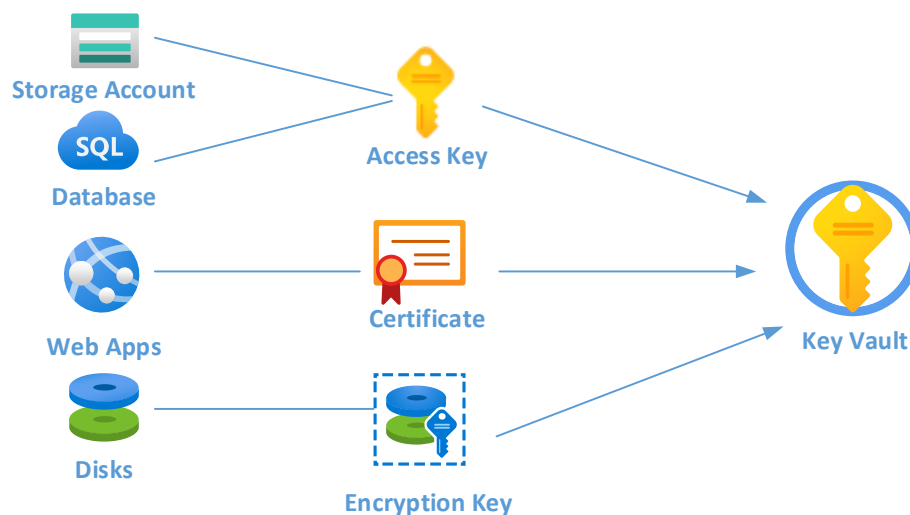
SAS can be used to give your clients, customers, applications limited connection to storage objects.

- ☐ Complete the tutorial: [Use a Linux VM system-assigned identity to access Azure Storage via a SAS credential](https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-linux-vm-access-storage-sas) (https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-linux-vm-access-storage-sas).



Part 5: Create a Key Vault

Different Azure resources require different security mechanisms, and as your number of resources grows, so will the number of security tokens. You may have access keys for your storage accounts or databases, your web applications may use certificates and your disks can use encryption keys. Azure Key Vault is a service that you can use to store and manage your security tokens.



© 2023, Southern Alberta Institute of Technology.
This figure was designed with icons from Microsoft Azure.

- ☐ Navigate to and select **Key Vaults** and click **Create Key Vault**.
- ☐ Enter your resource group, name and region.
- ☐ Select the **Standard** pricing tier and click **Next**.

Note: To learn more, read: [Key Vault pricing](https://azure.microsoft.com/en-us/pricing/details/key-vault/) (https://azure.microsoft.com/en-us/pricing/details/key-vault/).

- ☐ Review all the options, and then select the permission model for the vault and which resources can access secrets in the vault.

- ☐ Review and create the key vault.
- ☐ When the resource is created, select the resource and note that you have three options under **Objects** on the blade menu:
 - Keys
 - Secrets
 - Certificates
- ☐ Select **Keys** from the blade menu and then select **+ Generate/Import** from the top menu.
- ☐ Select **Generate**, give your key a name and review the other options.
- ☐ Create the key.
- ☐ Select the key, and then click the current version of the key.
- ☐ Download the public key.

