Project:
Securing the Perimeter

Directions and Submission Template

[Rohit Patil]:

[19th April, 2024]

Section 1

Designing a Secure Network Architecture

Section 1: Designing the Network

Time to tackle XYZ's perimeter challenges. You've identified that the first thing to do is design a secure network architecture for XYZ. XYZ has provided you a list of business requirements so you can get started on designing a secure layout. Your first task is to incorporate all the requirements securely in a network design.

Use https://app.diagrams.net/ to design a secure network architecture.

Include and label the following requirements in your design:

1) An on-premise network that has 3 workstations in it.

2) A Virtual Network with the following segments:

- Public DMZ with two web servers and a load balancer in it.
- Private DMZ with two database servers.
- Management LAN with one management server in it.
- Internal LAN with 5 workstations in it.
- Private Secure LAN with 3 database servers.

Additionally include the following:

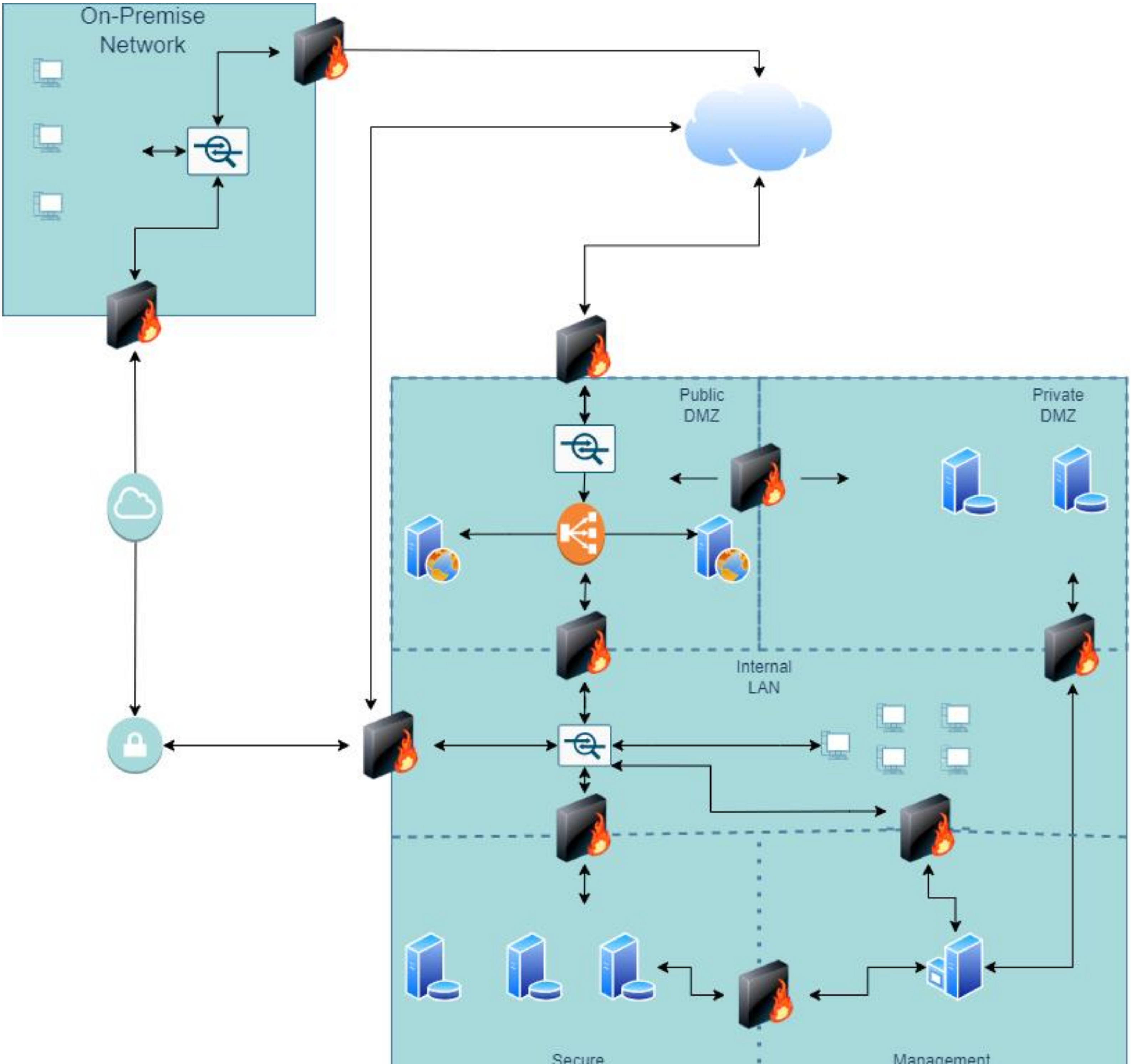
1) A VPN gateway connecting the on-premise network to your Virtual Network.

2) Show placement of security devices in the architecture, including load balancer(s), firewall(s), IDS/IPS device(s).

3) Show the flow of traffic, and remember to incorporate best security practices with the flow of traffic between the different subnets.

1.1 Designing the Network

Paste your Network Diagram here:



Section 2

Building a Secure Network Architecture in Azure

Section 2: Building the Network

After designing the network architecture, you now present your design to XYZ's stakeholders. They're all on board with your design, and have given you the green light to start building the architecture out in Azure.

So your next task is to go the Project Workspace in the classroom, and build out the enterprise network in Azure!

If you are accessing Azure with the Udacity classroom workspace, there will be a Resource Group in Azure called 'entp-project' that has already been created for you.

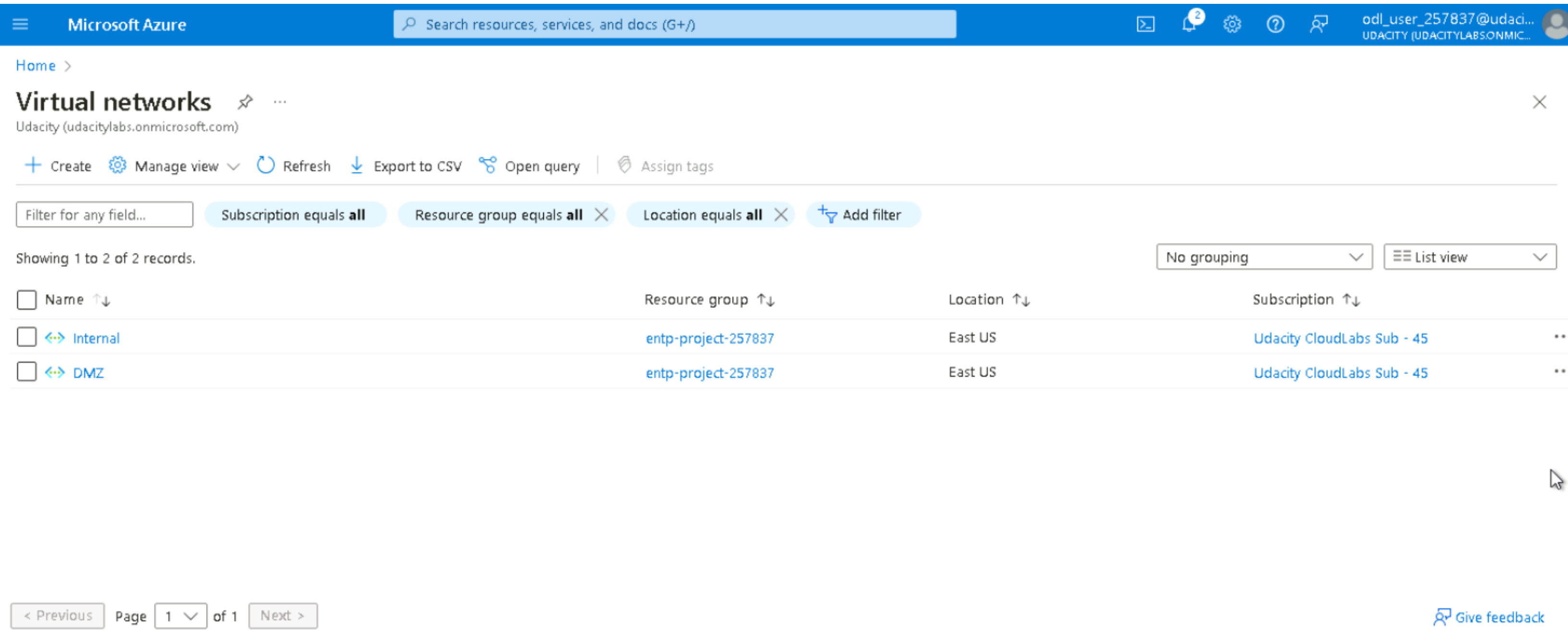
If you are accessing Azure using your own Azure account, first of all you should create a resource group called 'entp-project'.

This 'entp-project' resource group is where you will create all the components that make up this project. When creating VMs in this section, please only use Standard_B1s for your VM size and the Linux Ubuntu 18.04 image.

Insert screenshots of your network on the following pages, showing completion of each of the specified tasks.

2.1.1 Screenshot

Create two Azure Virtual Networks in the resource group ‘entp-project’. Label one for your DMZ and one as your Internal.

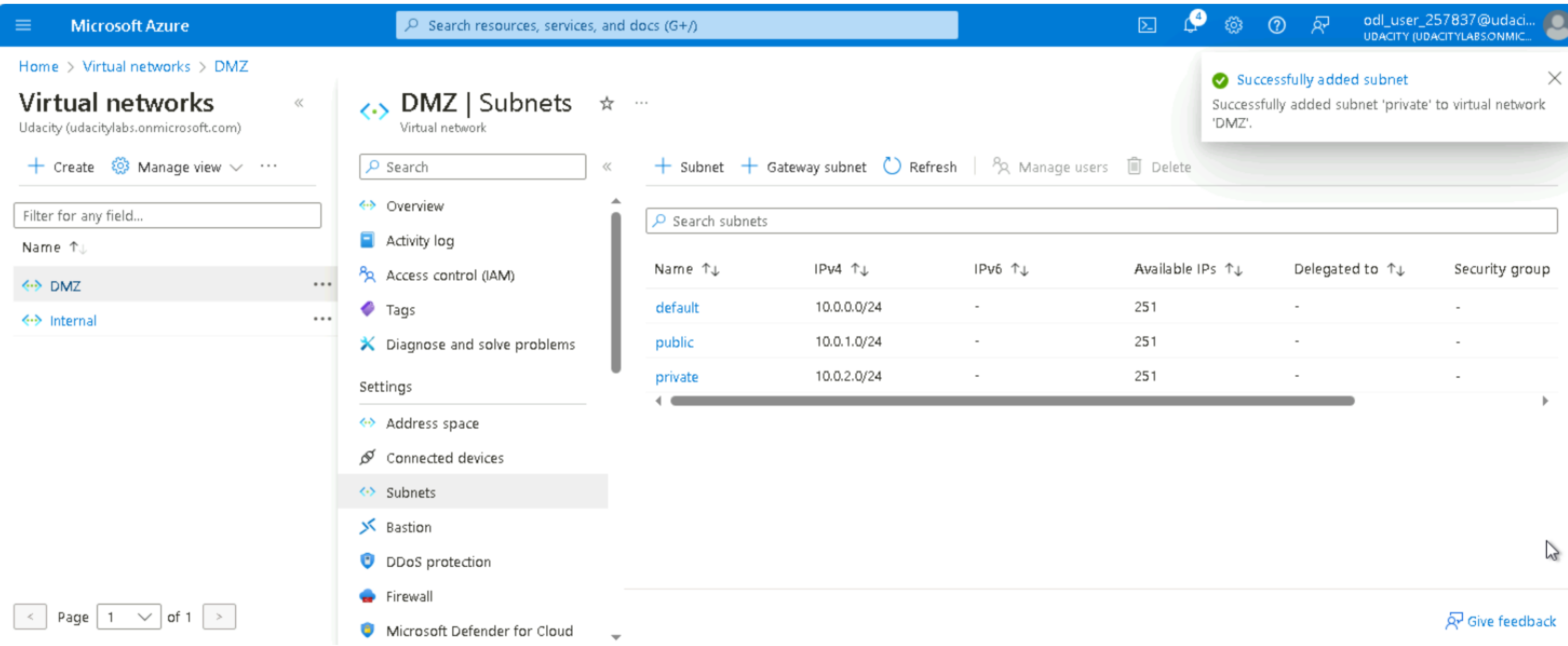


Showing 1 to 2 of 2 records.

Name	Resource group	Location	Subscription
Internal	entp-project-257837	East US	Udacity CloudLabs Sub - 45
DMZ	entp-project-257837	East US	Udacity CloudLabs Sub - 45

2.1.2 Screenshot

Create 2 subnets within your DMZ - subnets should be public and private.



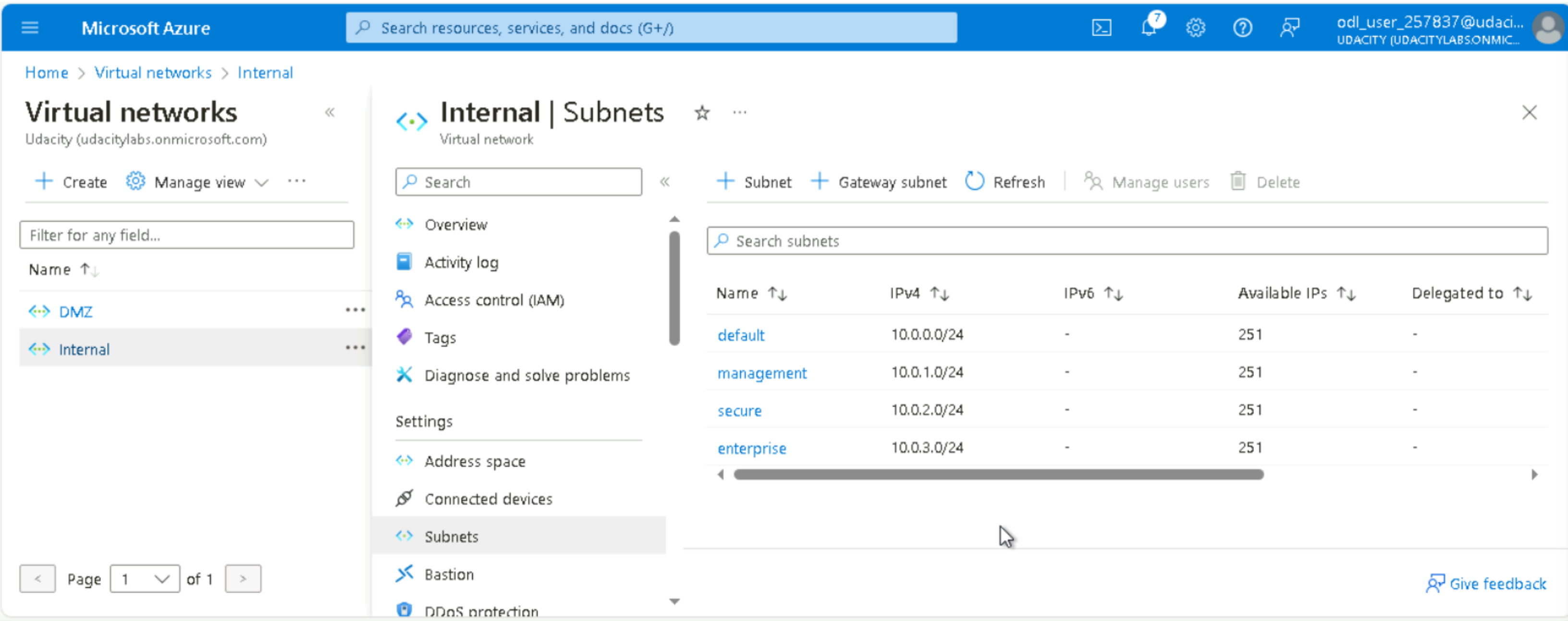
Successfully added subnet

Successfully added subnet 'private' to virtual network 'DMZ'.

Name	IPv4	IPv6	Available IPs	Delegated to	Security group
default	10.0.0.0/24	-	251	-	-
public	10.0.1.0/24	-	251	-	-
private	10.0.2.0/24	-	251	-	-

2.1.3 Screenshot

Create three subnets in your internal network and label them Management, Secure, and Enterprise.



Name	IPv4	IPv6	Available IPs	Delegated to
default	10.0.0.0/24	-	251	-
management	10.0.1.0/24	-	251	-
secure	10.0.2.0/24	-	251	-
enterprise	10.0.3.0/24	-	251	-

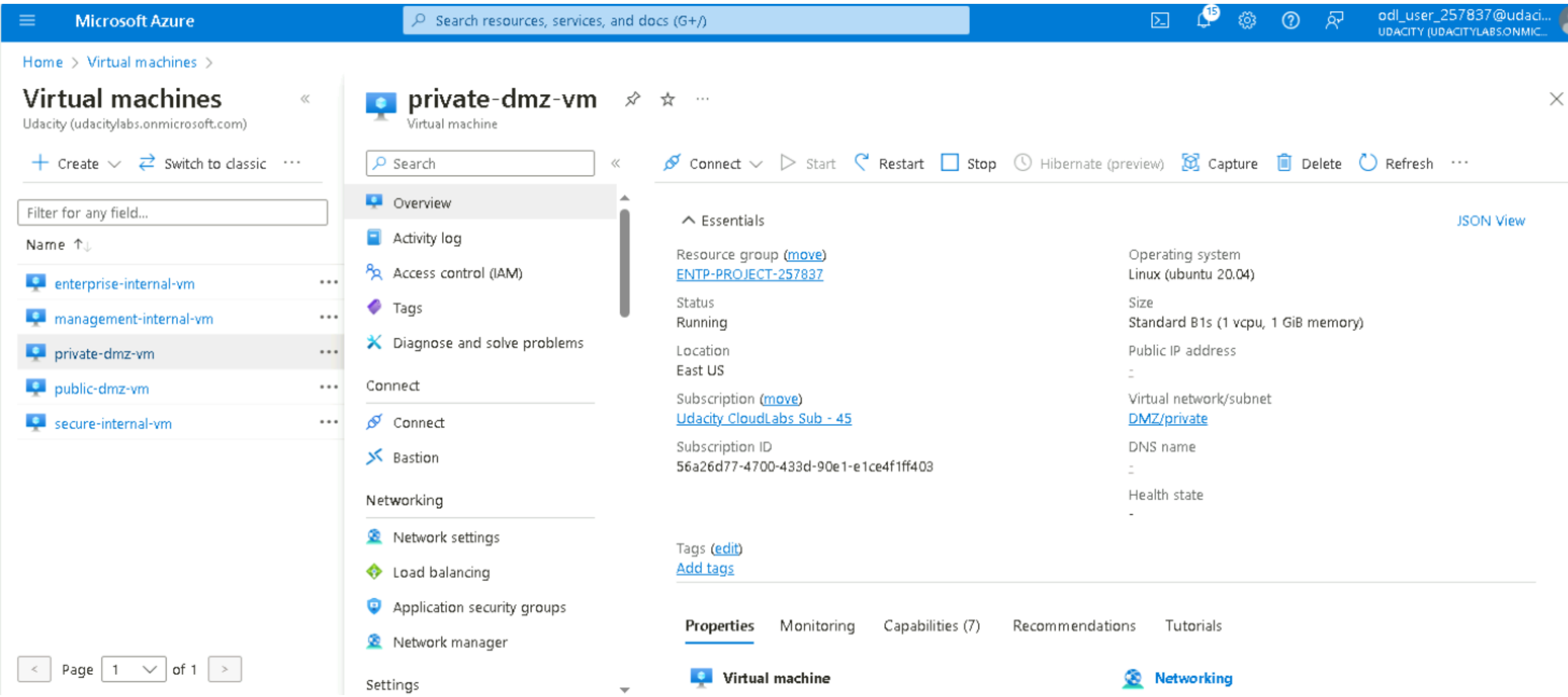
2.2 Creating Virtual Machines

In this next section you will create Virtual Machines in your subnets. You will create 2 VMs in your DMZ and 3 VMs in your internal network. Please only use the Standard_B1s VM size and the Linux Ubuntu 18.04 image.

Insert screenshots on the following pages, showing completion of each of the specified tasks.

2.2.1 Screenshot

Create one VM in each of your public and private DMZ subnets. Please only use Standard_B1s for your VM size and select the Linux Ubuntu 18.04 image, otherwise you will encounter an error.



Resource group (move)
ENTP-PROJECT-257837

Status
Running

Location
East US

Subscription (move)
Udacity CloudLabs Sub - 45

Subscription ID
56a26d77-4700-433d-90e1-e1ce4f1ff403

Tags (edit)
Add tags

Operating system
Linux (ubuntu 20.04)

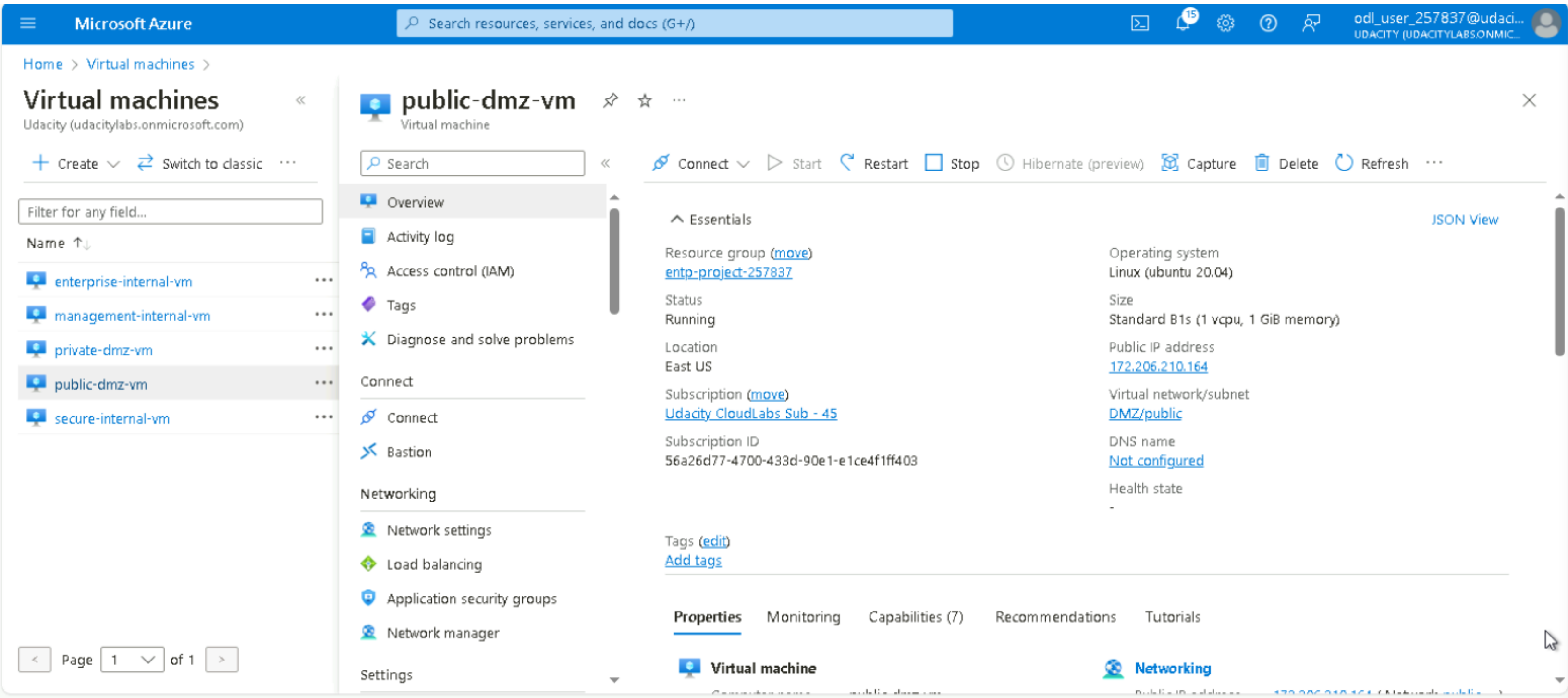
Size
Standard B1s (1 vcpu, 1 GiB memory)

Public IP address
-

Virtual network/subnet
DMZ/private

DNS name
-

Health state
-



Resource group (move)
entp-project-257837

Status
Running

Location
East US

Subscription (move)
Udacity CloudLabs Sub - 45

Subscription ID
56a26d77-4700-433d-90e1-e1ce4f1ff403

Tags (edit)
Add tags

Operating system
Linux (ubuntu 20.04)

Size
Standard B1s (1 vcpu, 1 GiB memory)

Public IP address
172.206.210.164

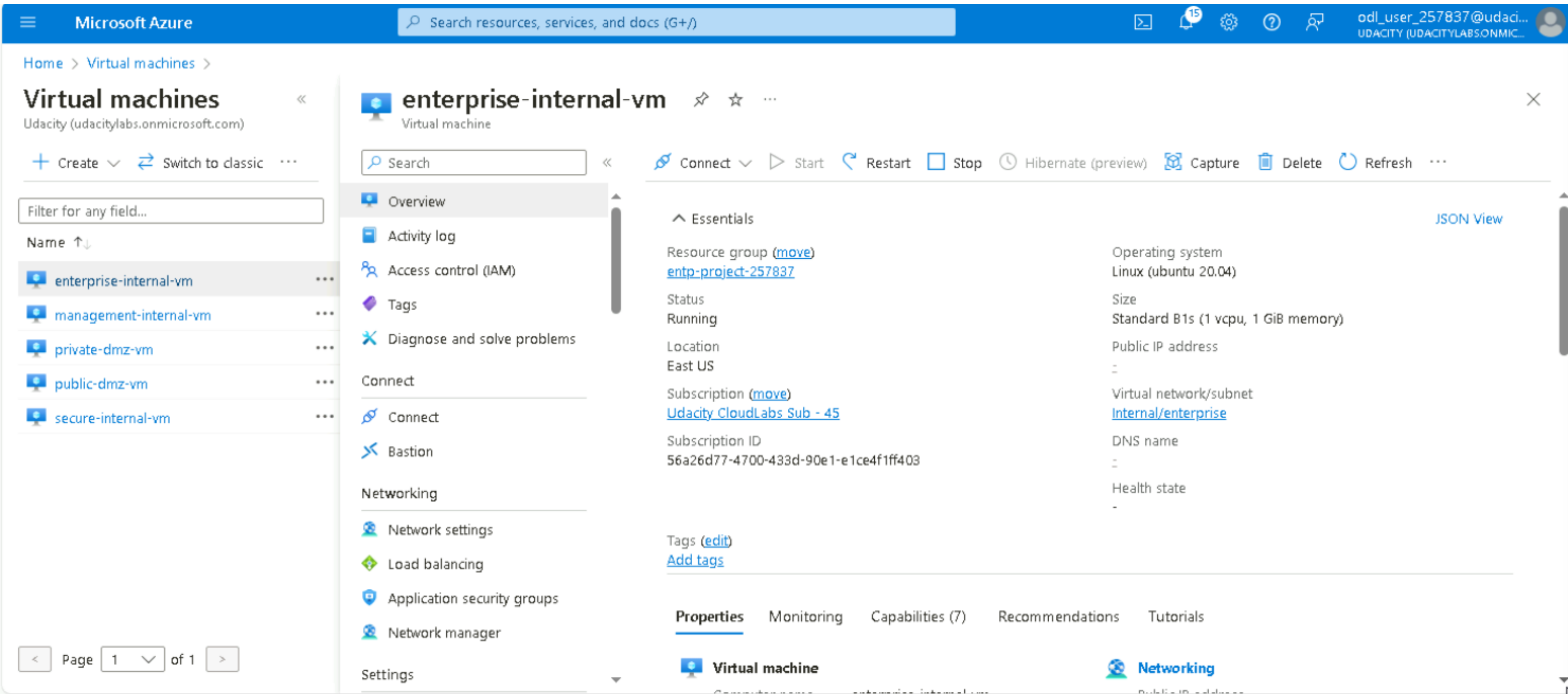
Virtual network/subnet
DMZ/public

DNS name
Not configured

Health state
-

2.2.2 Screenshot

Create one VM in each of your Management, Secure, and Enterprise internal subnets. Please only use Standard_B1s for your VM size and select the Linux Ubuntu 18.04 image, otherwise you will encounter an error.



Virtual machines:
- enterprise-internal-vm
- management-internal-vm
- private-dmz-vm
- public-dmz-vm
- secure-internal-vm

enterprise-internal-vm

Resource group (move): entp-project-257837

Status: Running

Location: East US

Subscription (move): Udacity CloudLabs Sub - 45

Subscription ID: 56a26d77-4700-433d-90e1-e1ce4f1ff403

Operating system: Linux (ubuntu 20.04)

Size: Standard B1s (1 vcpu, 1 GiB memory)

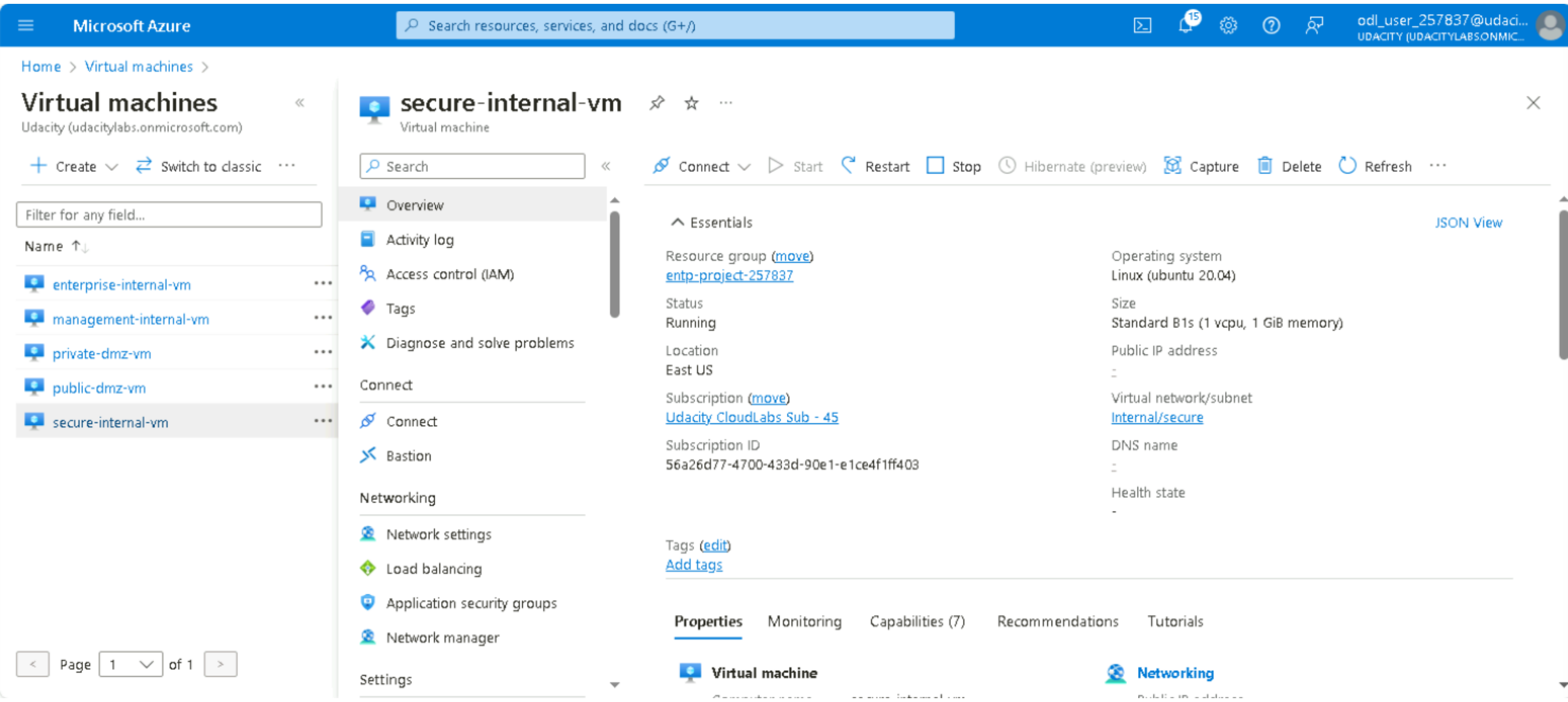
Public IP address: -

Virtual network/subnet: Internal/enterprise

DNS name: -

Health state: -

Tags (edit): Add tags



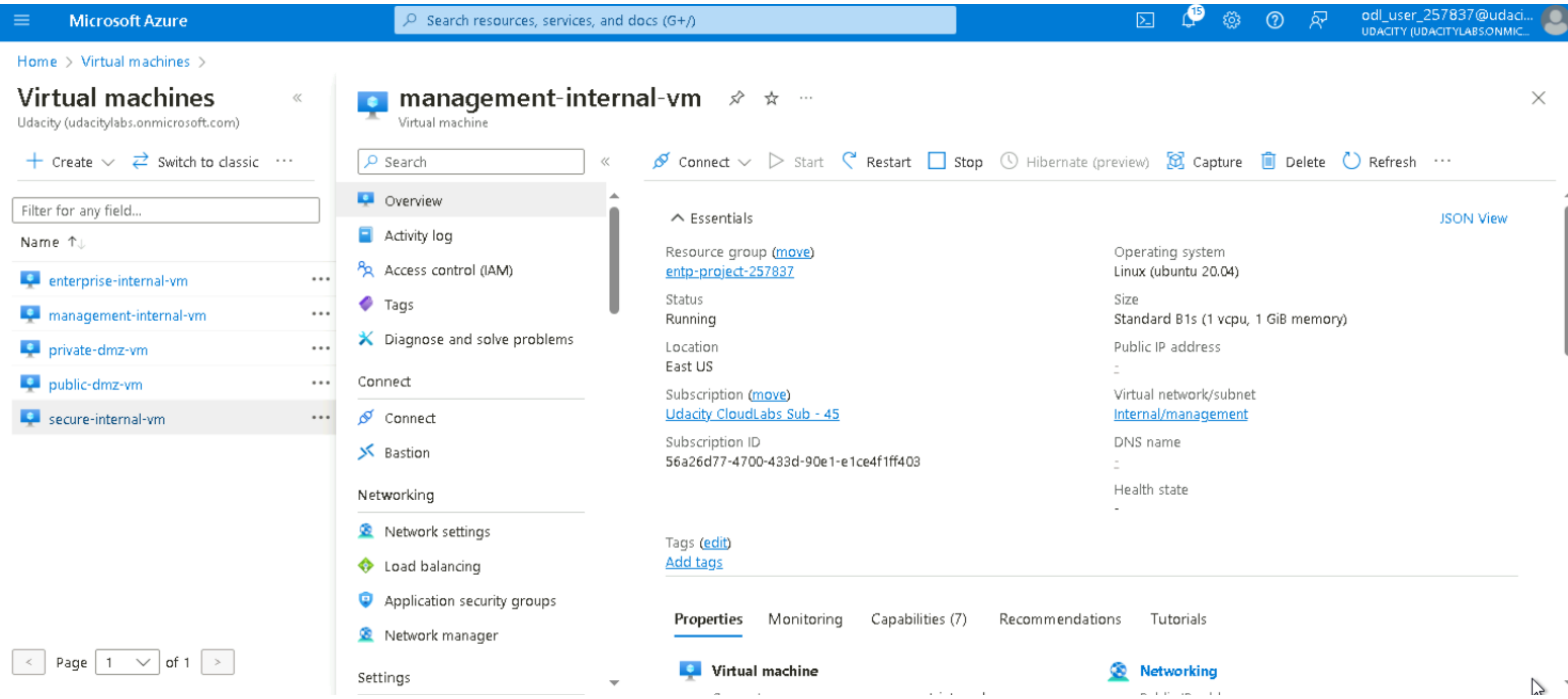
Virtual machines
Udacity (udacitylabs.onmicrosoft.com)

- enterprise-internal-vm
- management-internal-vm
- private-dmz-vm
- public-dmz-vm
- secure-internal-vm

secure-internal-vm
Virtual machine

Resource group (move) entp-project-257837	Operating system Linux (ubuntu 20.04)
Status Running	Size Standard B1s (1 vcpu, 1 GiB memory)
Location East US	Public IP address -
Subscription (move) Udacity CloudLabs Sub - 45	Virtual network/subnet Internal/secure
Subscription ID 56a26d77-4700-433d-90e1-e1ce4f1ff403	DNS name -
	Health state -

Tags (edit)
Add tags



Virtual machines
Udacity (udacitylabs.onmicrosoft.com)

- enterprise-internal-vm
- management-internal-vm
- private-dmz-vm
- public-dmz-vm
- secure-internal-vm

management-internal-vm
Virtual machine

Resource group (move) entp-project-257837	Operating system Linux (ubuntu 20.04)
Status Running	Size Standard B1s (1 vcpu, 1 GiB memory)
Location East US	Public IP address -
Subscription (move) Udacity CloudLabs Sub - 45	Virtual network/subnet Internal/management
Subscription ID 56a26d77-4700-433d-90e1-e1ce4f1ff403	DNS name -
	Health state -

Tags (edit)
Add tags

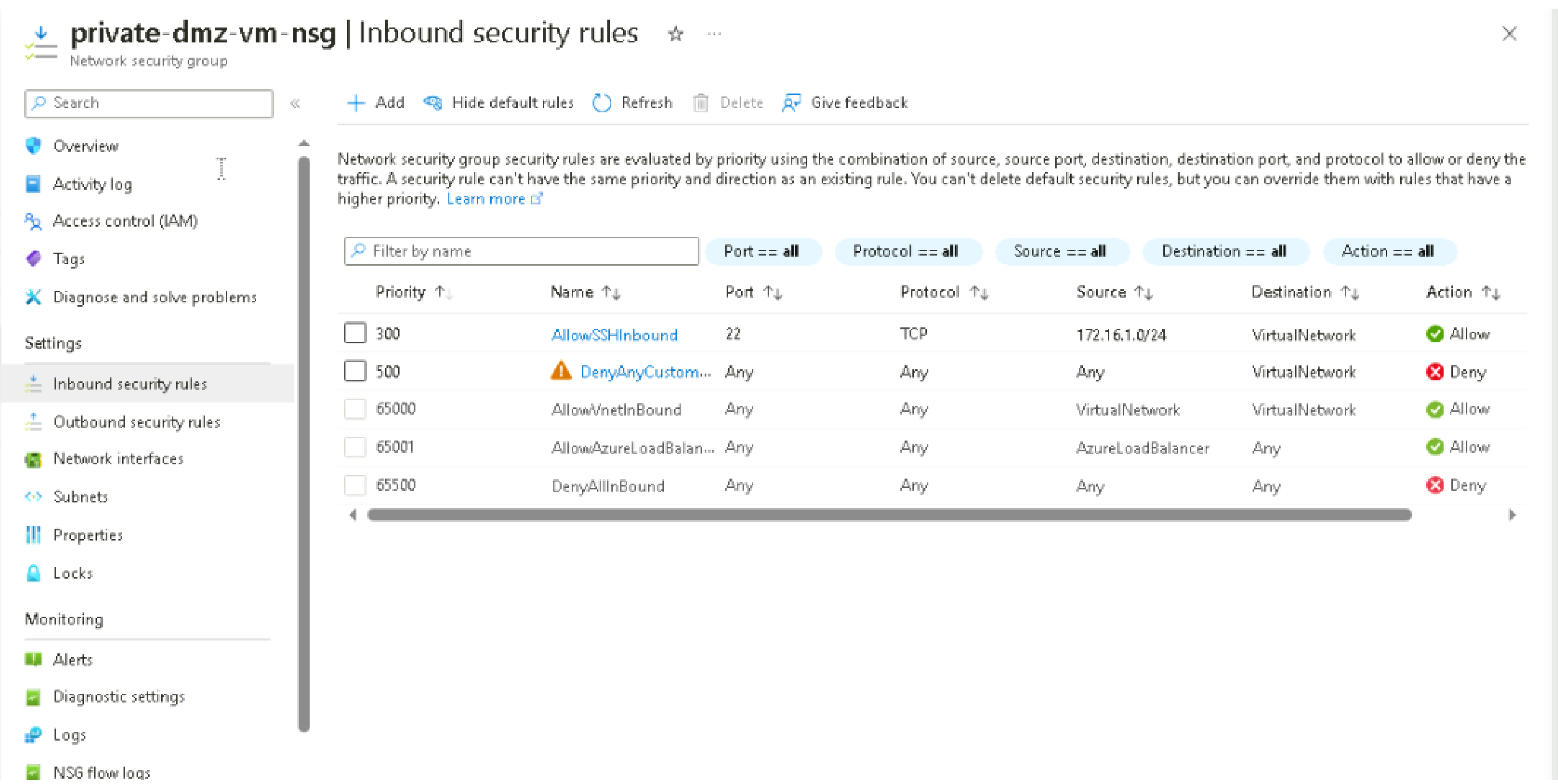
2.3 Secure Routing

In this next section you will configure secure routing within your Virtual Network and subnets. Follow secure best practices when creating network traffic rules.

Insert screenshots on the following pages, showing completion of each of the specified tasks.

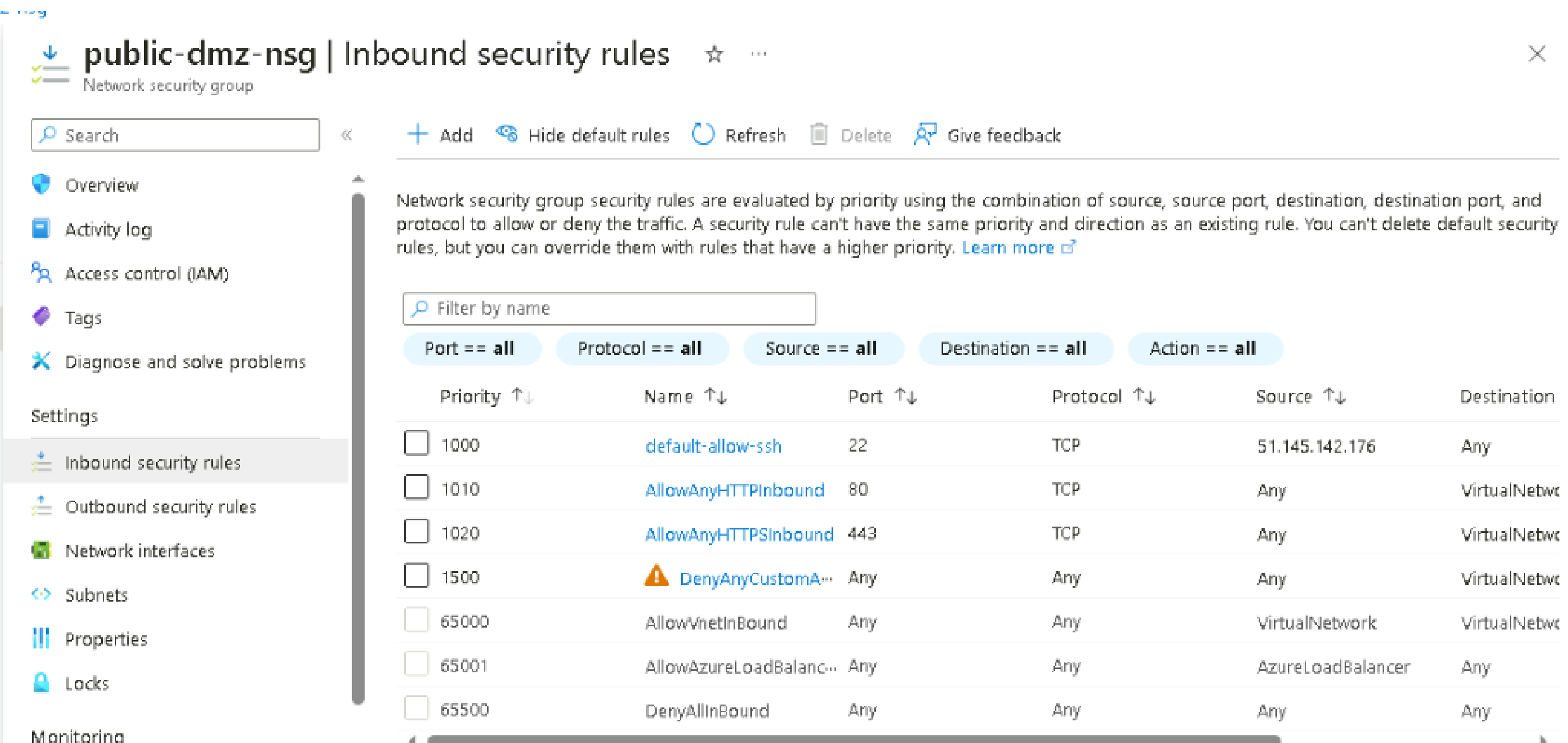
2.3.1 Screenshot

Traffic rules in your DMZ.



Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. Learn more

Priority	Name	Port	Protocol	Source	Destination	Action
300	AllowSSHInbound	22	TCP	172.16.1.0/24	VirtualNetwork	✓ Allow
500	⚠ DenyAnyCustom...	Any	Any	Any	VirtualNetwork	✗ Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny

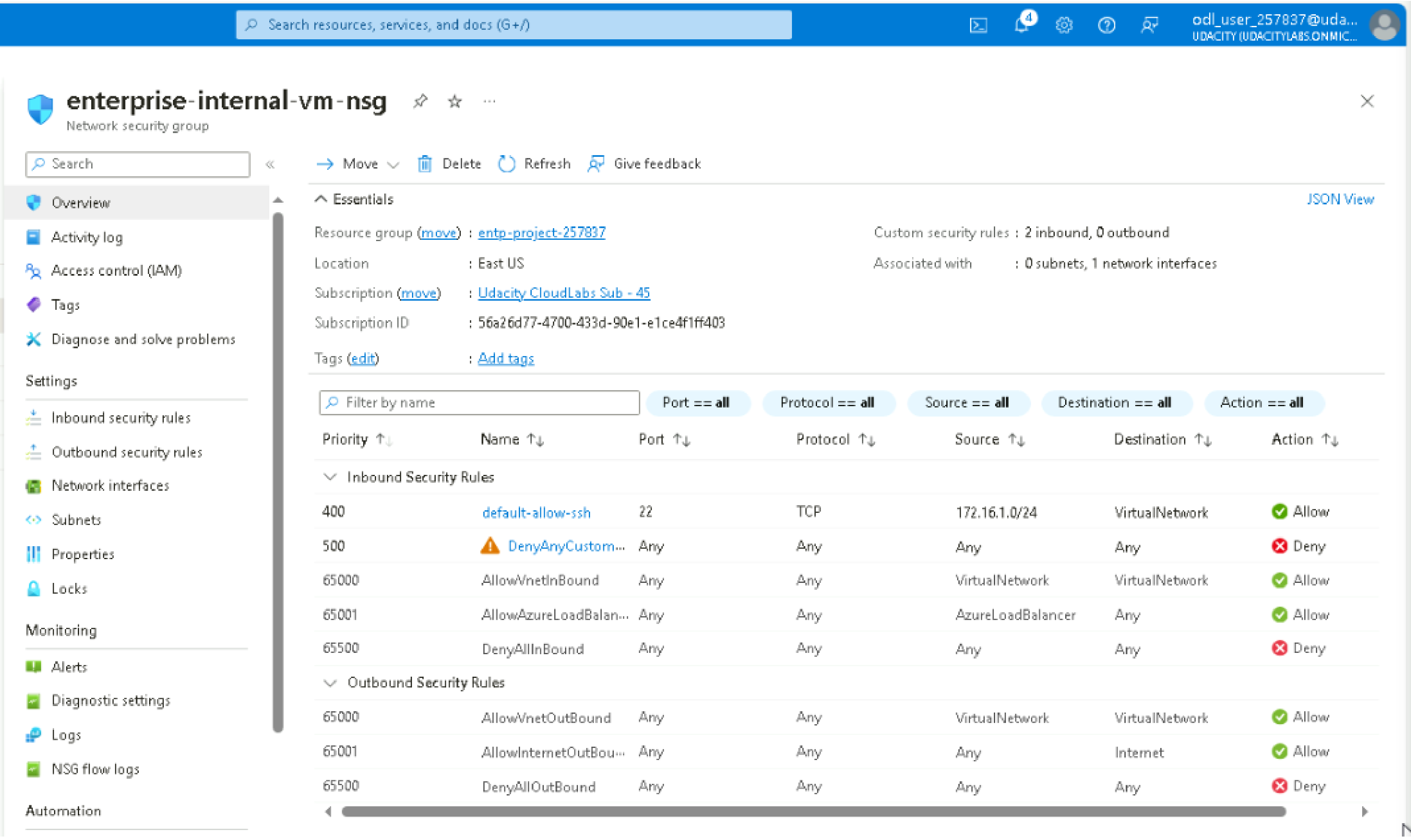


Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. Learn more

Priority	Name	Port	Protocol	Source	Destination
1000	default-allow-ssh	22	TCP	51.145.142.176	Any
1010	AllowAnyHTTPInbound	80	TCP	Any	VirtualNetw
1020	AllowAnyHTTPSInbound	443	TCP	Any	VirtualNetw
1500	⚠ DenyAnyCustomA...	Any	Any	Any	VirtualNetw
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetw
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

2.3.2 Screenshot

Traffic rules in your Internal network.



enterprise-internal-vm-nsg

Network security group

Essentials

Resource group (move) : entp-project-257837

Location : East US

Subscription (move) : Udacity CloudLabs Sub - 45

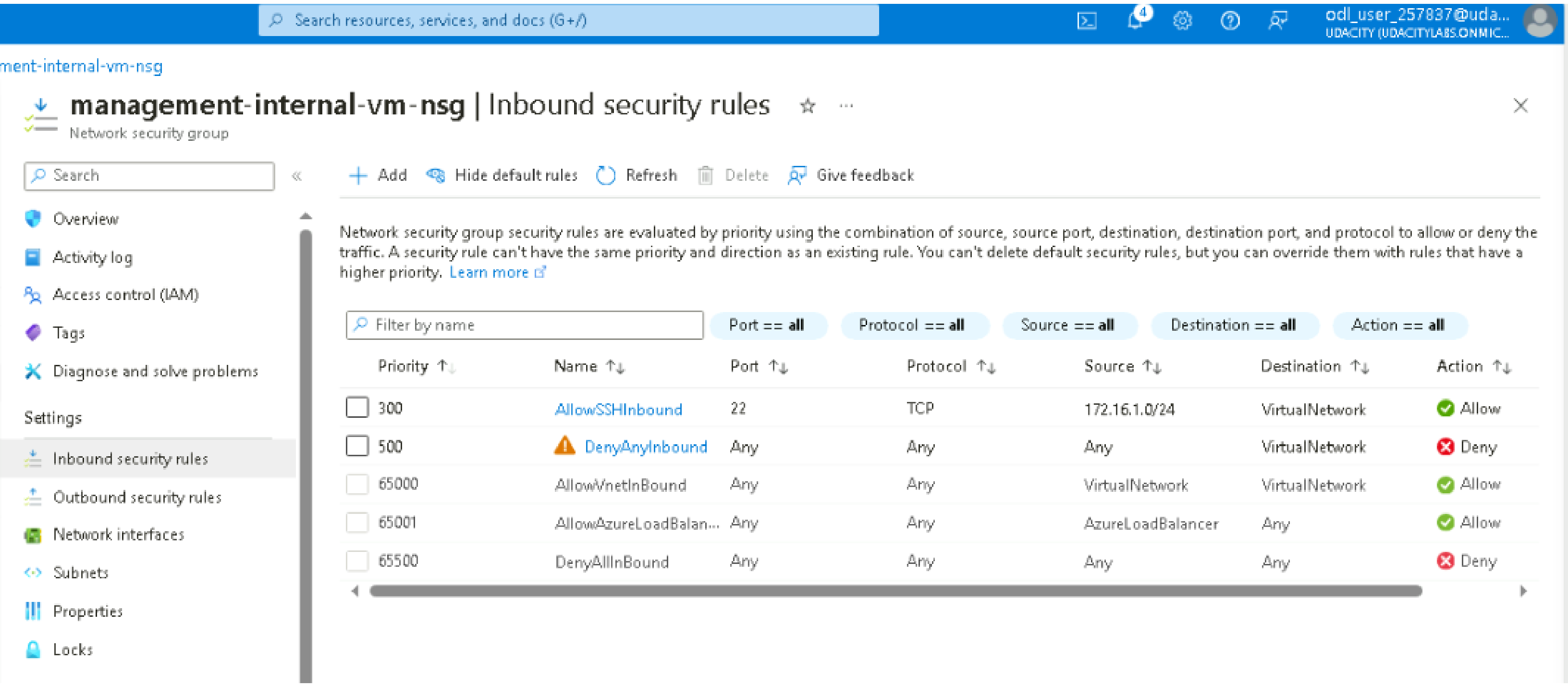
Subscription ID : 56a26d77-4700-433d-90e1-e1ce4f1ff403

Tags (edit) : Add tags

Custom security rules : 2 inbound, 0 outbound

Associated with : 0 subnets, 1 network interfaces

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
Inbound Security Rules						
400	default-allow-ssh	22	TCP	172.16.1.0/24	VirtualNetwork	✓ Allow
500	⚠ DenyAnyCustom...	Any	Any	Any	Any	✗ Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowInternetOutBou...	Any	Any	Any	Internet	✓ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✗ Deny

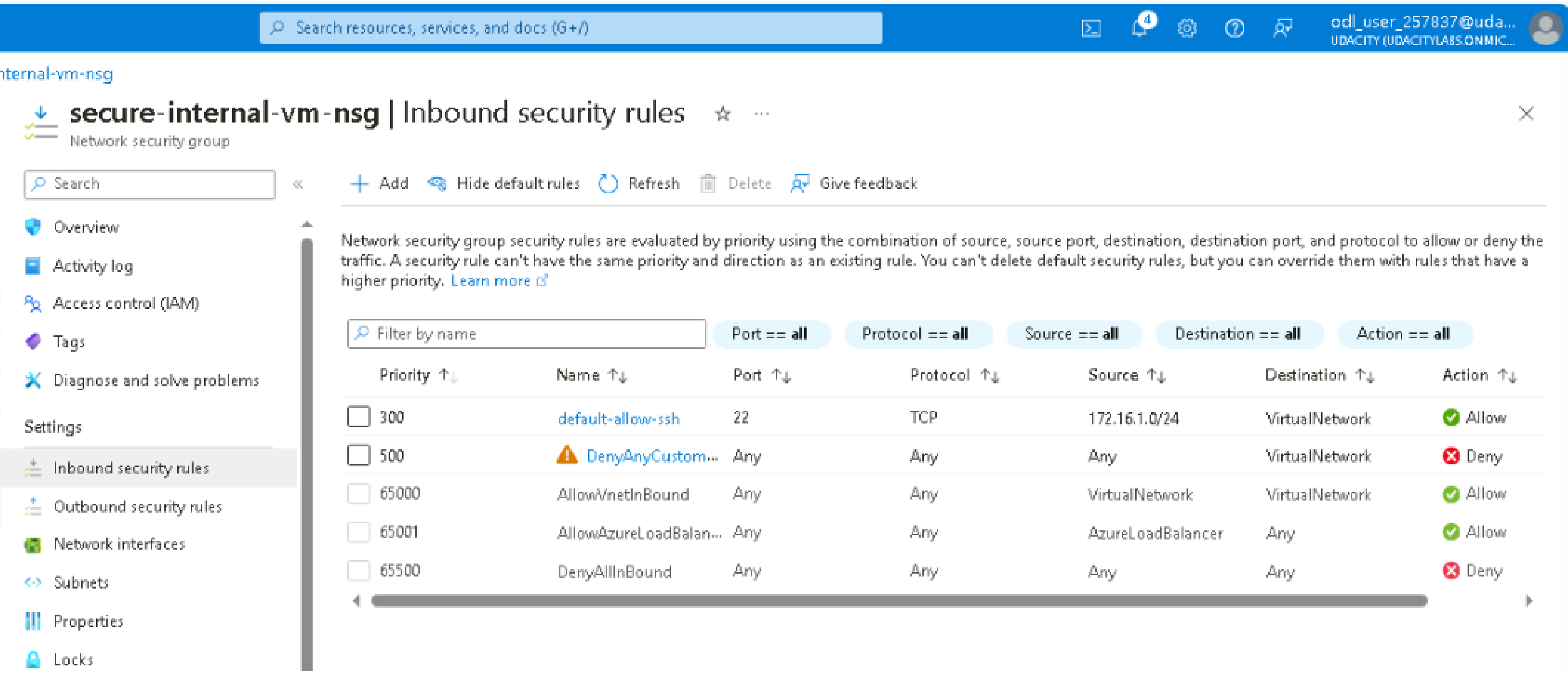


management-internal-vm-nsg | Inbound security rules

Network security group

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. Learn more

	Priority	Name	Port	Protocol	Source	Destination	Action
☐	300	AllowSSHInbound	22	TCP	172.16.1.0/24	VirtualNetwork	✓ Allow
☐	500	⚠ DenyAnyInbound	Any	Any	Any	VirtualNetwork	✗ Deny
☐	65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
☐	65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	✓ Allow
☐	65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny



secure-internal-vm-nsg | Inbound security rules

Network security group

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. Learn more

	Priority	Name	Port	Protocol	Source	Destination	Action
☐	300	default-allow-ssh	22	TCP	172.16.1.0/24	VirtualNetwork	✓ Allow
☐	500	⚠ DenyAnyCustom...	Any	Any	Any	VirtualNetwork	✗ Deny
☐	65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
☐	65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	✓ Allow
☐	65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny

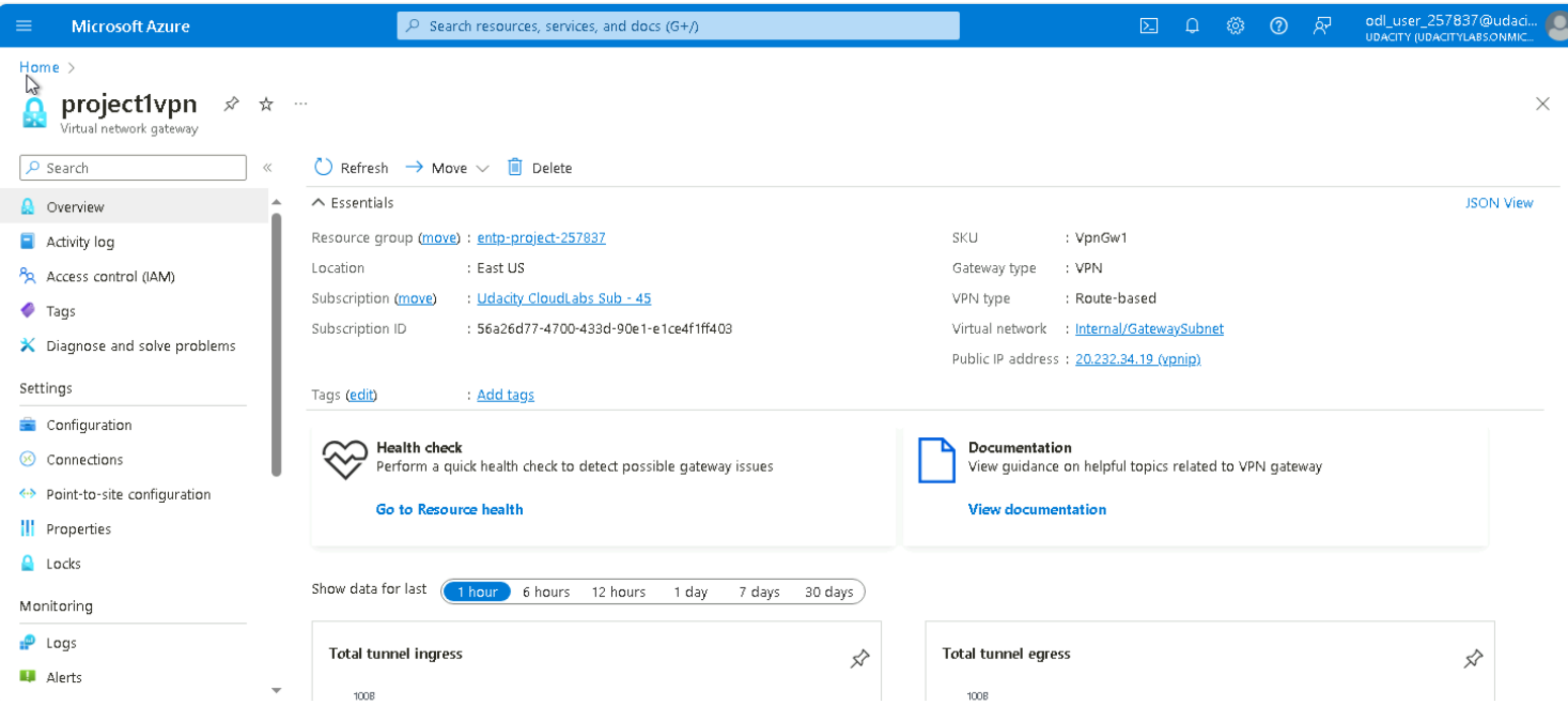
2.4 VPN Access

In this next section you will create a VPN to secure access to your internal network. After creating your VPN, test your VPN connection and attempt connecting to one of your VMs in your internal network.

Insert screenshots on the following pages, showing completion of each of the specified tasks.

2.4.1 Screenshot

Create a VPN to connect to your internal network.



project1vpn
Virtual network gateway

Essentials

Resource group (move) : entp-project-257837
Location : East US
Subscription (move) : Udacity CloudLabs Sub - 45
Subscription ID : 56a26d77-4700-433d-90e1-e1ce4f1ff403
Tags (edit) : Add tags

SKU : VpnGw1
Gateway type : VPN
VPN type : Route-based
Virtual network : Internal/GatewaySubnet
Public IP address : 20.232.34.19 (vpnip)

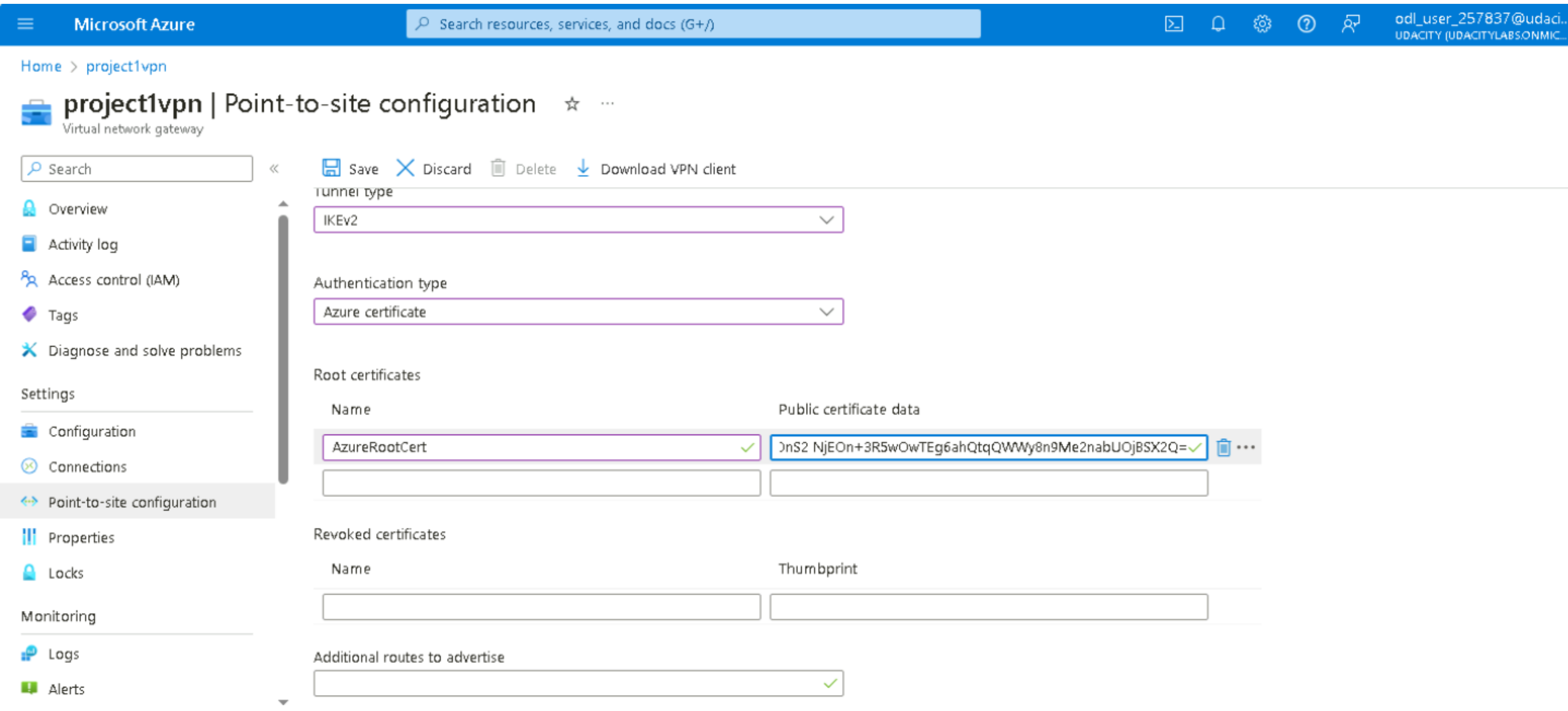
Health check
Perform a quick health check to detect possible gateway issues
Go to Resource health

Documentation
View guidance on helpful topics related to VPN gateway
View documentation

Show data for last: 1 hour | 6 hours | 12 hours | 1 day | 7 days | 30 days

Total tunnel ingress
100B

Total tunnel egress
100B



project1vpn | Point-to-site configuration
Virtual network gateway

Tunnel type: IKEv2

Authentication type: Azure certificate

Root certificates

Name	Public certificate data
AzureRootCert	)nS2 NjEOn+3R5wOwTEg6ahQtqQWWy8n9Me2nabUOjBSX2Q=

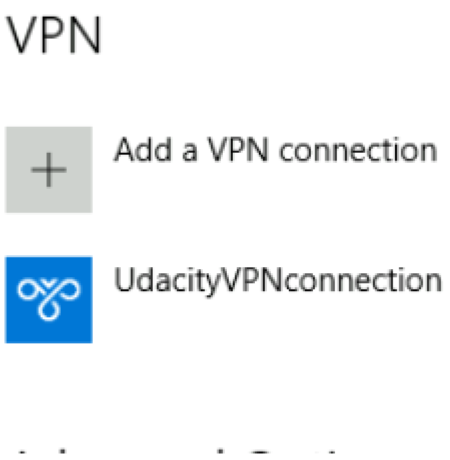
Revoked certificates

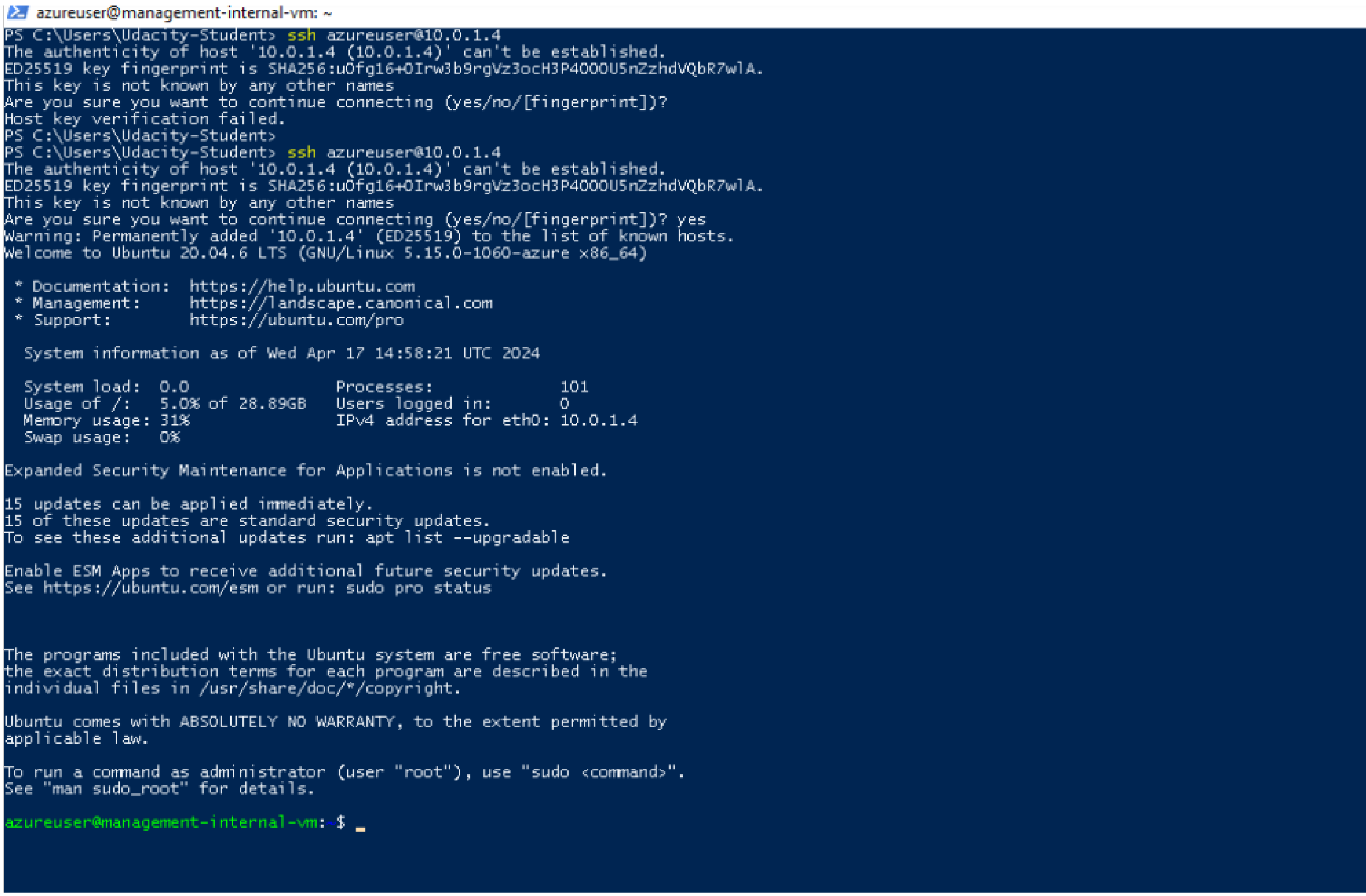
Name	Thumbprint

Additional routes to advertise

2.4.2 Screenshot

Test VPN connection by connecting to one of the VMs in your internal network.





```
PS C:\Users\Udacity-Student> ssh azureuser@10.0.1.4
The authenticity of host '10.0.1.4 (10.0.1.4)' can't be established.
ED25519 key fingerprint is SHA256:uOfg16+OIrw3b9rgVz3ocH3P4OOOU5nZzhdVQbR7wlA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Host key verification failed.
PS C:\Users\Udacity-Student>
PS C:\Users\Udacity-Student> ssh azureuser@10.0.1.4
The authenticity of host '10.0.1.4 (10.0.1.4)' can't be established.
ED25519 key fingerprint is SHA256:uOfg16+OIrw3b9rgVz3ocH3P4OOOU5nZzhdVQbR7wlA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.1.4' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1060-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

  System information as of Wed Apr 17 14:58:21 UTC 2024

  System load:  0.0               Processes:             101
  Usage of /:   5.0% of 28.89GB   Users logged in:       0
  Memory usage: 31%               IPv4 address for eth0: 10.0.1.4
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

15 updates can be applied immediately.
15 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

azureuser@management-internal-vm:~$ _
```

Section 3

Continuous Monitoring with a SIEM

Section 3: Build the SIEM

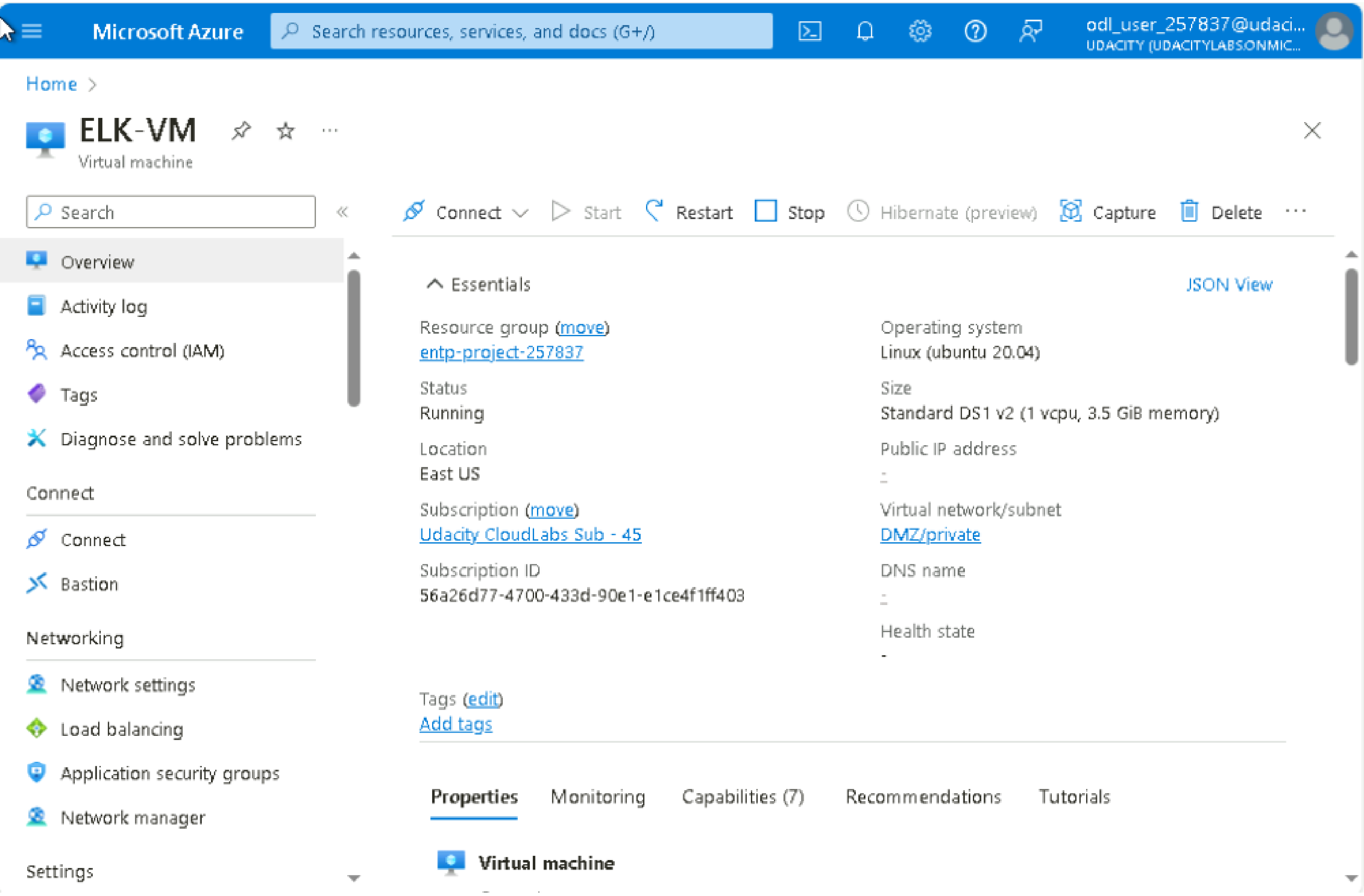
Now that you've built a secure network architecture and a Zero Trust model, you're ready to wrap up your contract and finish the last piece of work. Your last task is to set up a solution to monitor the enterprise network and alert you about potential attacks.

For this section, you will continue working in the Project Workspace in the classroom, then provide screenshots of your work here in this document.

Insert screenshots on the following pages, showing completion of each of the specified tasks.

3.1.1 Screenshot

Create a VM in your private DMZ. On that VM, go through the process to create an ELK Server. For your Elk Server use the VM size DS1_v2 and Linux Ubuntu 18.04 image.



Resource group (move)
entp-project-257837

Status
Running

Location
East US

Subscription (move)
Udacity CloudLabs Sub - 45

Subscription ID
56a26d77-4700-433d-90e1-e1ce4f1ff403

Operating system
Linux (ubuntu 20.04)

Size
Standard DS1 v2 (1 vcpu, 3.5 GiB memory)

Public IP address
-

Virtual network/subnet
DMZ/private

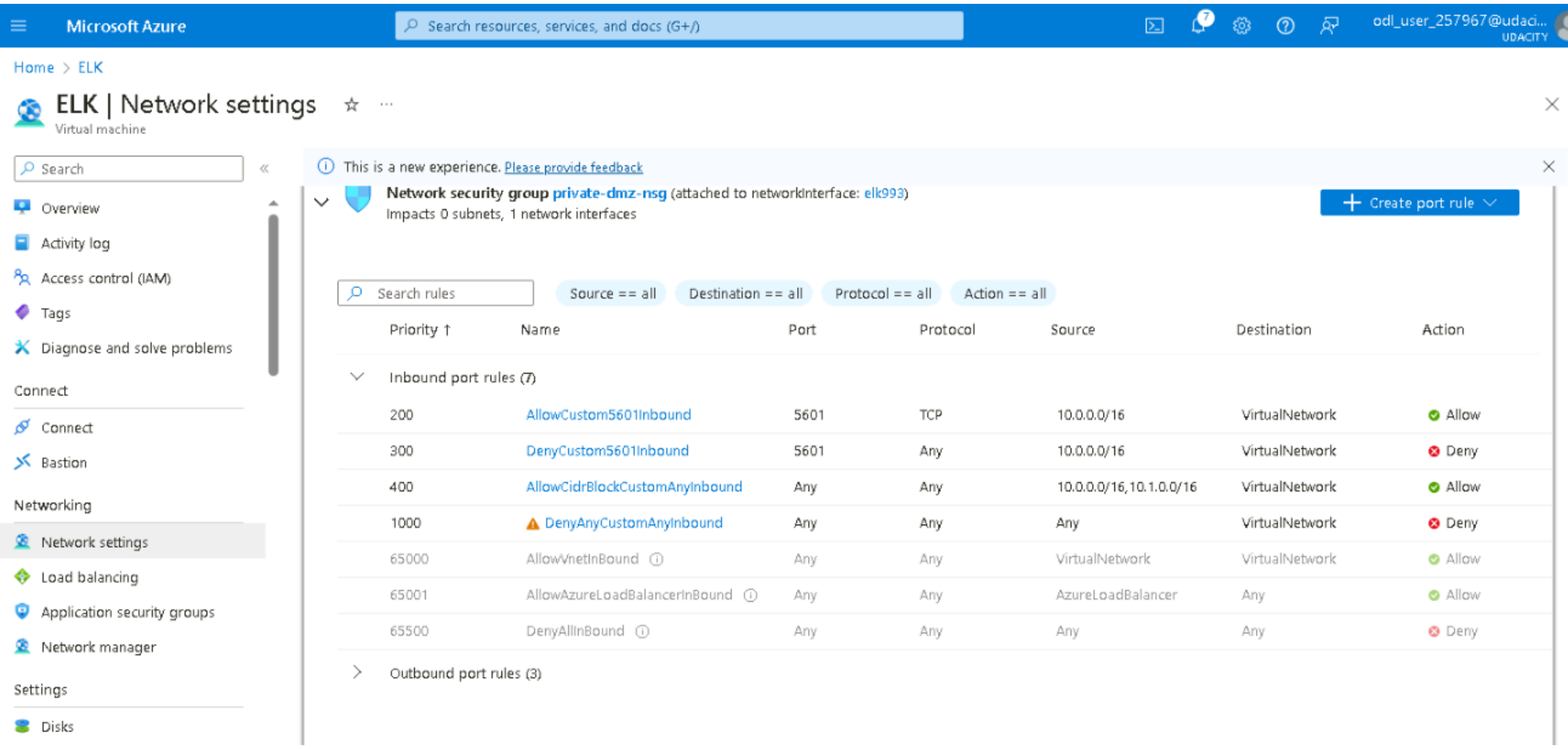
DNS name
-

Health state
-

Tags (edit)
Add tags

3.1.2 Screenshot

Set up routing to only allow traffic inbound to the server from both your virtual networks, and make sure Kibana is only accessible when you're on the network.



Network security group private-dmz-nsg (attached to networkinterface: elk993)
Impacts 0 subnets, 1 network interfaces

Inbound port rules (7)

Priority ↑	Name	Port	Protocol	Source	Destination	Action
200	AllowCustom5601Inbound	5601	TCP	10.0.0.0/16	VirtualNetwork	✓ Allow
300	DenyCustom5601Inbound	5601	Any	10.0.0.0/16	VirtualNetwork	✕ Deny
400	AllowCidrBlockCustomAnyInbound	Any	Any	10.0.0.0/16,10.1.0.0/16	VirtualNetwork	✓ Allow
1000	⚠ DenyAnyCustomAnyInbound	Any	Any	Any	VirtualNetwork	✕ Deny
65000	AllowVnetInBound ⓘ	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInBound ⓘ	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound ⓘ	Any	Any	Any	Any	✕ Deny

Outbound port rules (3)

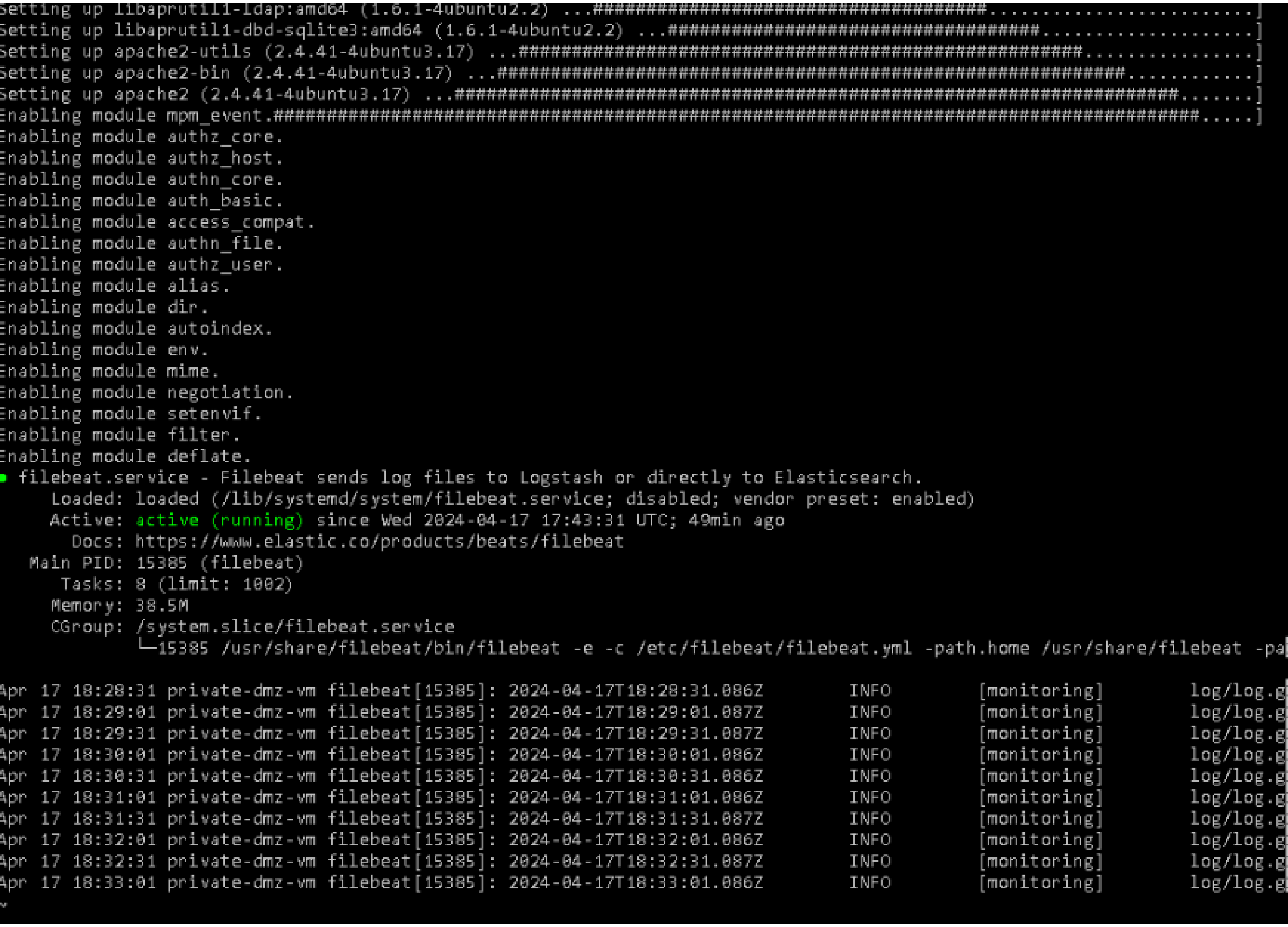
3.2 Ingest Logs

In this next section, you will start setting up ingest sources for your ELK server.

Insert screenshots on the following pages, showing completion of each of the specified tasks.

3.2.1 Screenshot

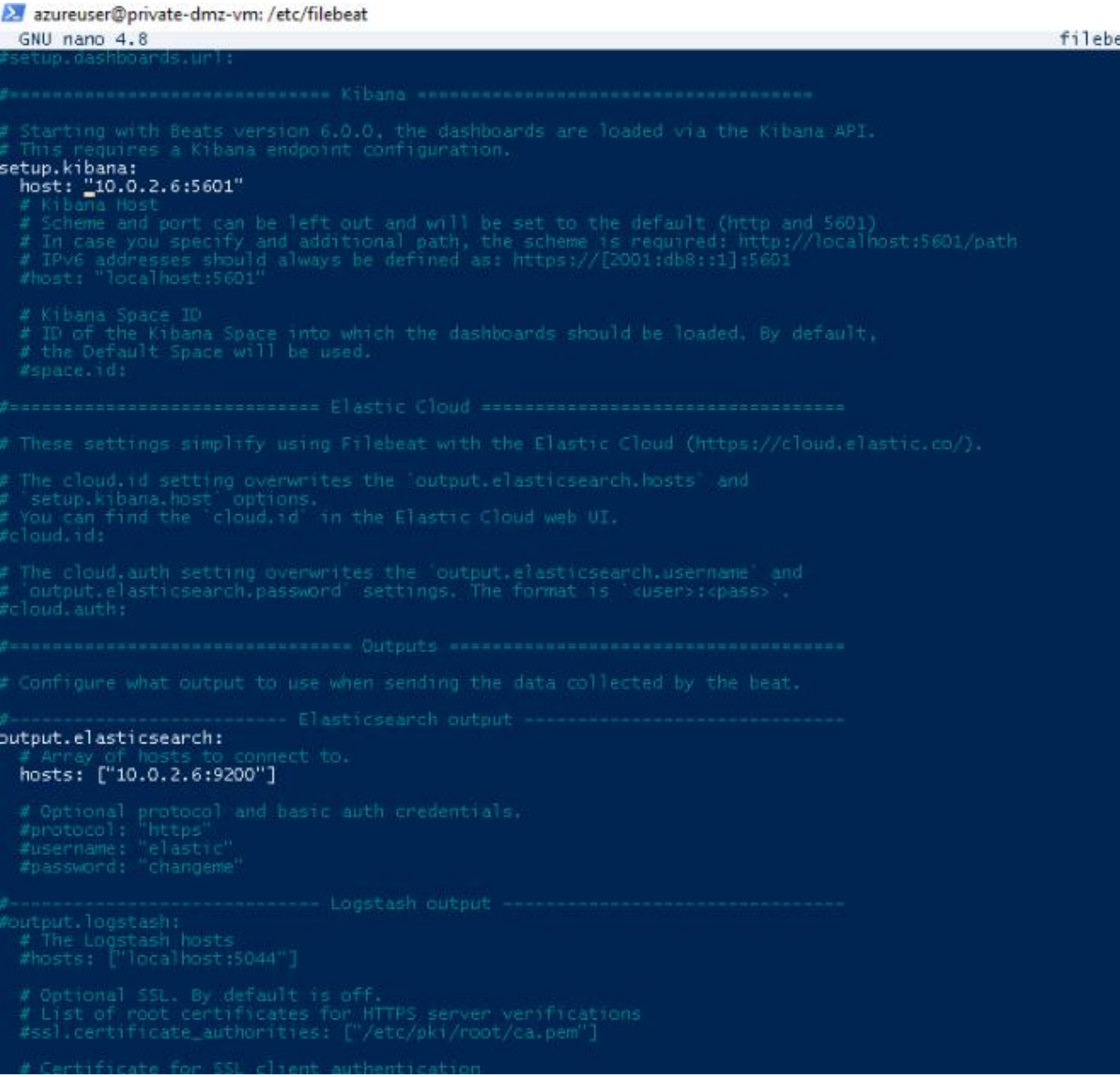
Install Filebeat on your web servers and show the Filebeat service as active.



```
Setting up libaprutil1-ldap:amd64 (1.6.1-4ubuntu2.2) ...#####################################.........................]
Setting up libaprutil1-dbd-sqlite3:amd64 (1.6.1-4ubuntu2.2) ...###################################.....................]
Setting up apache2-utils (2.4.41-4ubuntu3.17) ...#####################################################.................]
Setting up apache2-bin (2.4.41-4ubuntu3.17) ...###########################################################............]
Setting up apache2 (2.4.41-4ubuntu3.17) ...####################################################################.......]
Enabling module mpm_event.#######################################################################################.....]
Enabling module authz_core.
Enabling module authz_host.
Enabling module authn_core.
Enabling module auth_basic.
Enabling module access_compat.
Enabling module authn_file.
Enabling module authz_user.
Enabling module alias.
Enabling module dir.
Enabling module autoindex.
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module filter.
Enabling module deflate.
● filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.
     Loaded: loaded (/lib/systemd/system/filebeat.service; disabled; vendor preset: enabled)
     Active: active (running) since Wed 2024-04-17 17:43:31 UTC; 49min ago
       Docs: https://www.elastic.co/products/beats/filebeat
   Main PID: 15385 (filebeat)
      Tasks: 8 (limit: 1002)
     Memory: 38.5M
     CGroup: /system.slice/filebeat.service
             └─15385 /usr/share/filebeat/bin/filebeat -e -c /etc/filebeat/filebeat.yml -path.home /usr/share/filebeat -pa

Apr 17 18:28:31 private-dmz-vm filebeat[15385]: 2024-04-17T18:28:31.086Z        INFO        [monitoring]        log/log.g
Apr 17 18:29:01 private-dmz-vm filebeat[15385]: 2024-04-17T18:29:01.087Z        INFO        [monitoring]        log/log.g
Apr 17 18:29:31 private-dmz-vm filebeat[15385]: 2024-04-17T18:29:31.087Z        INFO        [monitoring]        log/log.g
Apr 17 18:30:01 private-dmz-vm filebeat[15385]: 2024-04-17T18:30:01.086Z        INFO        [monitoring]        log/log.g
Apr 17 18:30:31 private-dmz-vm filebeat[15385]: 2024-04-17T18:30:31.086Z        INFO        [monitoring]        log/log.g
Apr 17 18:31:01 private-dmz-vm filebeat[15385]: 2024-04-17T18:31:01.086Z        INFO        [monitoring]        log/log.g
Apr 17 18:31:31 private-dmz-vm filebeat[15385]: 2024-04-17T18:31:31.087Z        INFO        [monitoring]        log/log.g
Apr 17 18:32:01 private-dmz-vm filebeat[15385]: 2024-04-17T18:32:01.086Z        INFO        [monitoring]        log/log.g
Apr 17 18:32:31 private-dmz-vm filebeat[15385]: 2024-04-17T18:32:31.087Z        INFO        [monitoring]        log/log.g
Apr 17 18:33:01 private-dmz-vm filebeat[15385]: 2024-04-17T18:33:01.086Z        INFO        [monitoring]        log/log.g
~
```

3.2.2 Screenshot

Configure Filebeat to route web server logs to Elasticsearch.

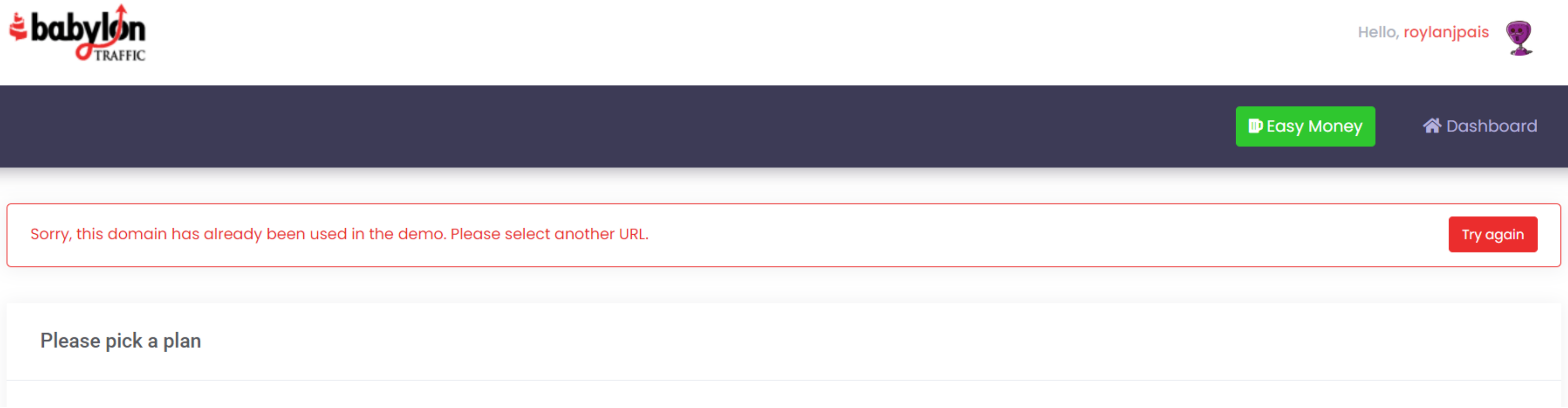


azureuser@private-dmz-vm: /etc/filebeat

```
  GNU nano 4.8                                                                                          filebe
#setup.dashboards.url:

#============================== Kibana =====================================

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:
  host: "10.0.2.6:5601"
  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify and additional path, the scheme is required: http://localhost:5601/path
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  #host: "localhost:5601"

  # Kibana Space ID
  # ID of the Kibana Space into which the dashboards should be loaded. By default,
  # the Default Space will be used.
  #space.id:

#============================= Elastic Cloud ==================================

# These settings simplify using Filebeat with the Elastic Cloud (https://cloud.elastic.co/).

# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.
#cloud.id:

# The cloud.auth setting overwrites the `output.elasticsearch.username` and
# `output.elasticsearch.password` settings. The format is `<user>:<pass>`.
#cloud.auth:

#================================ Outputs =====================================

# Configure what output to use when sending the data collected by the beat.

#-------------------------- Elasticsearch output ------------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["10.0.2.6:9200"]

  # Optional protocol and basic auth credentials.
  #protocol: "https"
  #username: "elastic"
  #password: "changeme"

#----------------------------- Logstash output --------------------------------
#output.logstash:
  # The Logstash hosts
  #hosts: ["localhost:5044"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
```

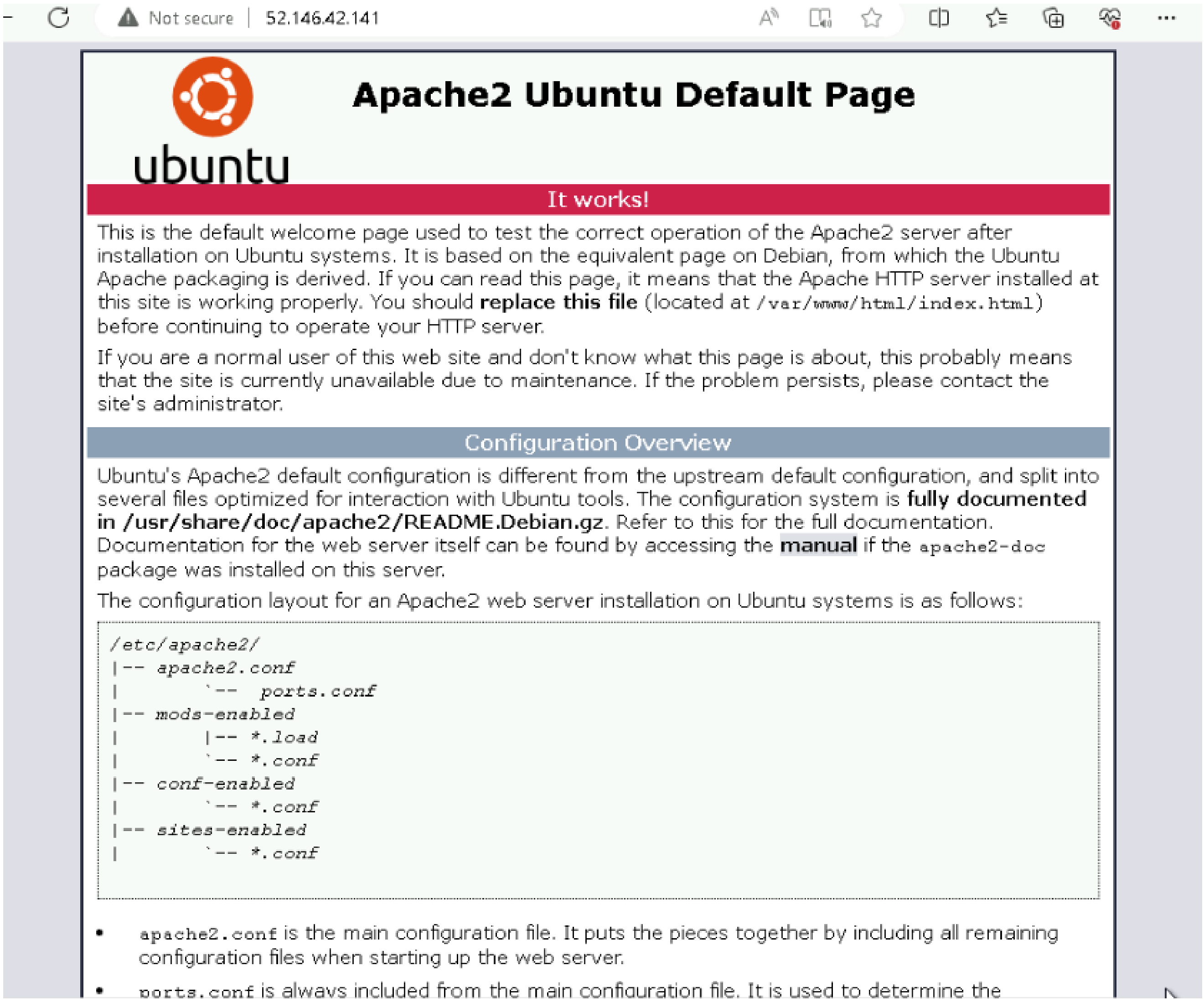
3.2.3 Screenshot

Simulate web traffic to your web servers using https://www.babylontraffic.com.



Sorry, this domain has already been used in the demo. Please select another URL.

Please pick a plan



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

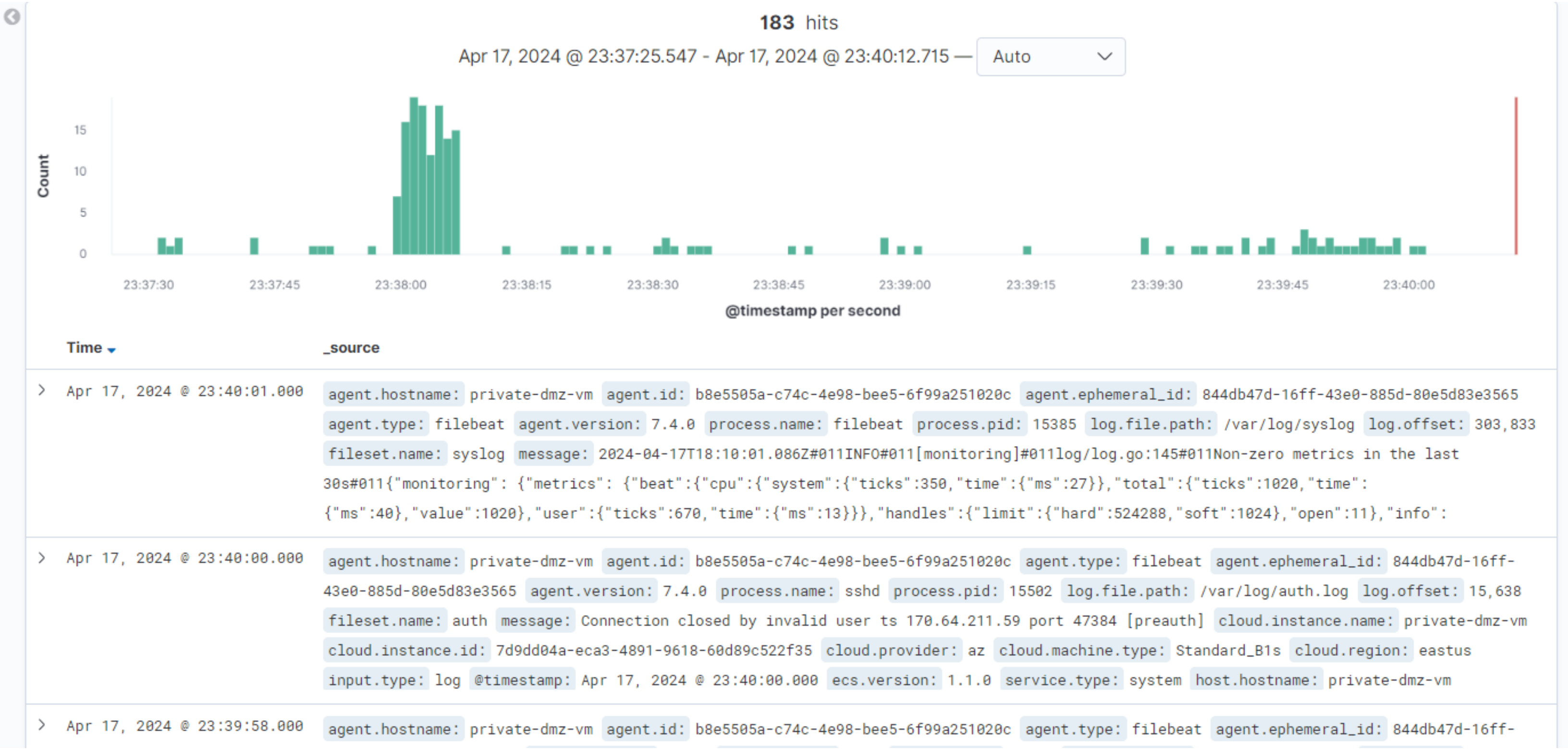
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the

3.2.4 Screenshot

Web server logs appear in Kibana.



```
> Apr 17, 2024 @ 23:40:01.000   agent.hostname: private-dmz-vm agent.id: b8e5505a-c74c-4e98-bee5-6f99a251020c agent.ephemeral_id: 844db47d-16ff-43e0-885d-80e5d83e3565
                                agent.type: filebeat agent.version: 7.4.0 process.name: filebeat process.pid: 15385 log.file.path: /var/log/syslog log.offset: 303,833
                                fileset.name: syslog message: 2024-04-17T18:10:01.086Z#011INFO#011[monitoring]#011log/log.go:145#011Non-zero metrics in the last
                                30s#011{"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":350,"time":{"ms":27}},"total":{"ticks":1020,"time":
                                {"ms":40},"value":1020},"user":{"ticks":670,"time":{"ms":13}}},"handles":{"limit":{"hard":524288,"soft":1024},"open":11},"info":

> Apr 17, 2024 @ 23:40:00.000   agent.hostname: private-dmz-vm agent.id: b8e5505a-c74c-4e98-bee5-6f99a251020c agent.type: filebeat agent.ephemeral_id: 844db47d-16ff-
                                43e0-885d-80e5d83e3565 agent.version: 7.4.0 process.name: sshd process.pid: 15502 log.file.path: /var/log/auth.log log.offset: 15,638
                                fileset.name: auth message: Connection closed by invalid user ts 170.64.211.59 port 47384 [preauth] cloud.instance.name: private-dmz-vm
                                cloud.instance.id: 7d9dd04a-eca3-4891-9618-60d89c522f35 cloud.provider: az cloud.machine.type: Standard_B1s cloud.region: eastus
                                input.type: log @timestamp: Apr 17, 2024 @ 23:40:00.000 ecs.version: 1.1.0 service.type: system host.hostname: private-dmz-vm

> Apr 17, 2024 @ 23:39:58.000   agent.hostname: private-dmz-vm agent.id: b8e5505a-c74c-4e98-bee5-6f99a251020c agent.type: filebeat agent.ephemeral_id: 844db47d-16ff-
```

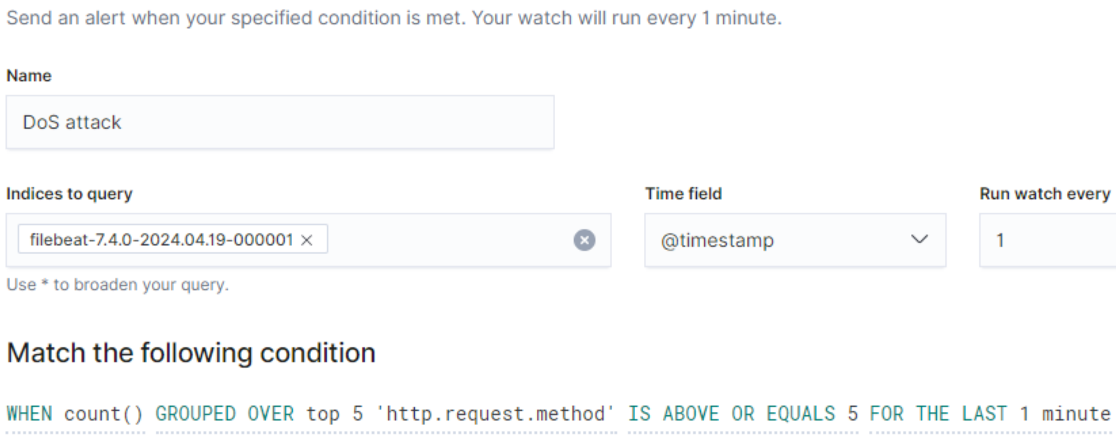
3.3 Build Alerts

In this next section, you will create alerts on the simulated web traffic you see. Build alerts to alert you of possible DoS, brute force, and probing attacks.

Insert screenshots on the following pages, showing completion of each of the specified tasks.

3.3.1 Screenshot

Create an alert for DoS attack.



Send an alert when your specified condition is met. Your watch will run every 1 minute.

Name

DoS attack

Indices to query

filebeat-7.4.0-2024.04.19-000001 ×

Use * to broaden your query.

Time field

@timestamp

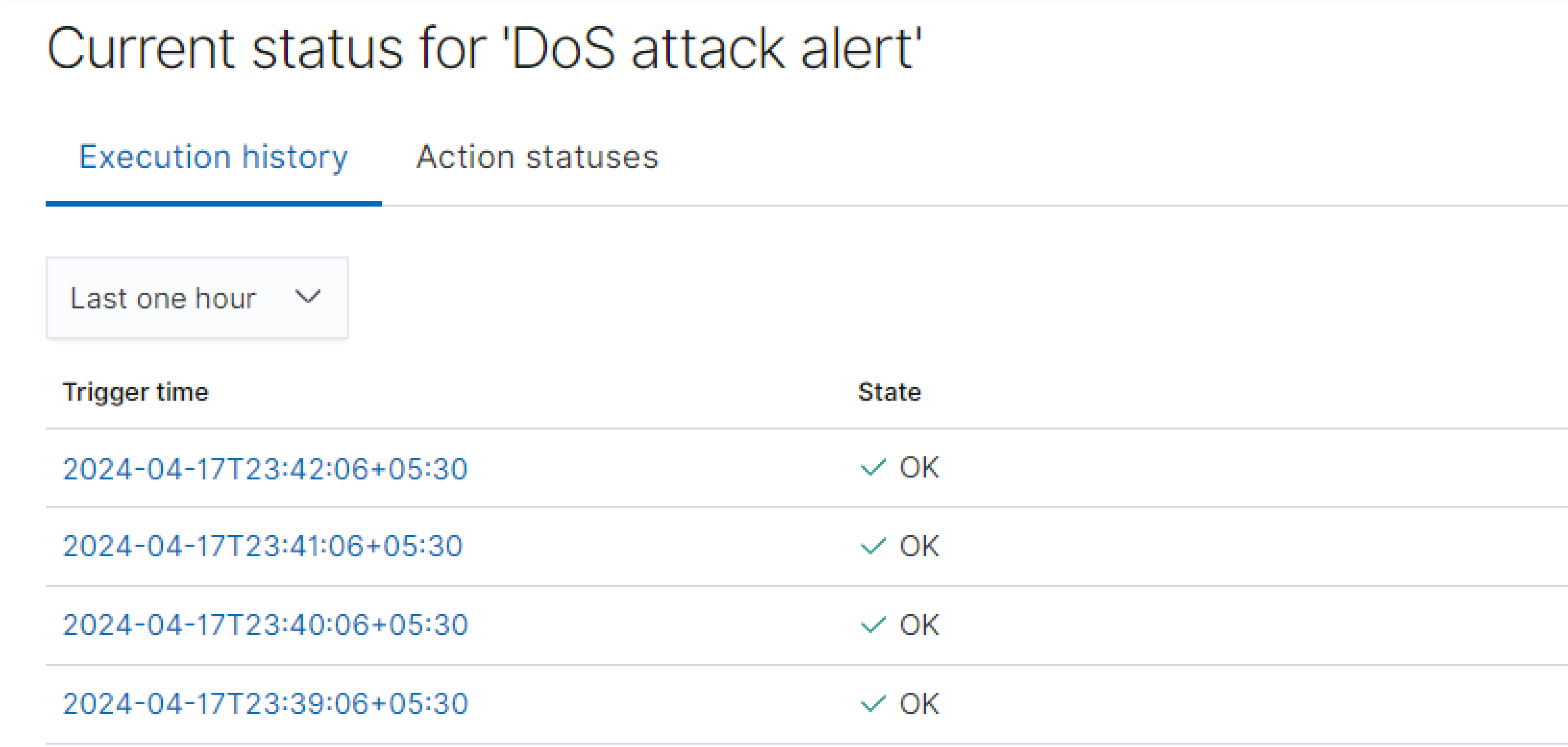
Run watch every

1

minute

Match the following condition

```
WHEN count() GROUPED OVER top 5 'http.request.method' IS ABOVE OR EQUALS 5 FOR THE LAST 1 minute
```

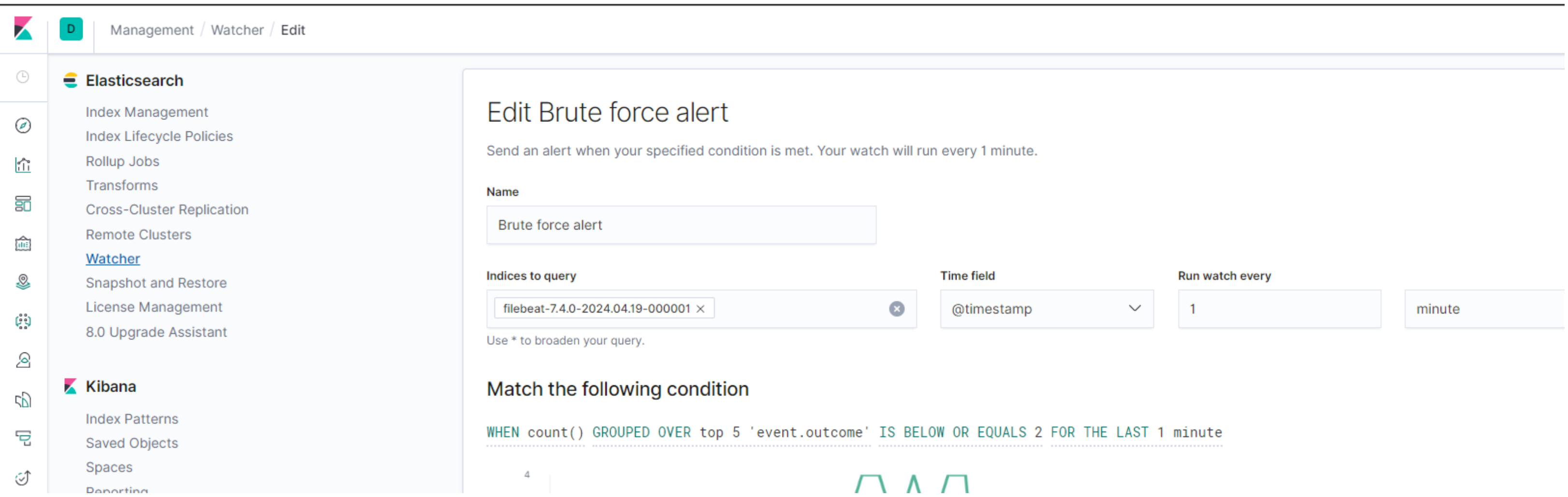


Current status for 'DoS attack alert'

Trigger time	State
2024-04-17T23:42:06+05:30	✓ OK
2024-04-17T23:41:06+05:30	✓ OK
2024-04-17T23:40:06+05:30	✓ OK
2024-04-17T23:39:06+05:30	✓ OK

3.3.2 Screenshot

Create an alert for Brute Force attack.



Edit Brute force alert

Send an alert when your specified condition is met. Your watch will run every 1 minute.

Name: Brute force alert

Indices to query: filebeat-7.4.0-2024.04.19-000001

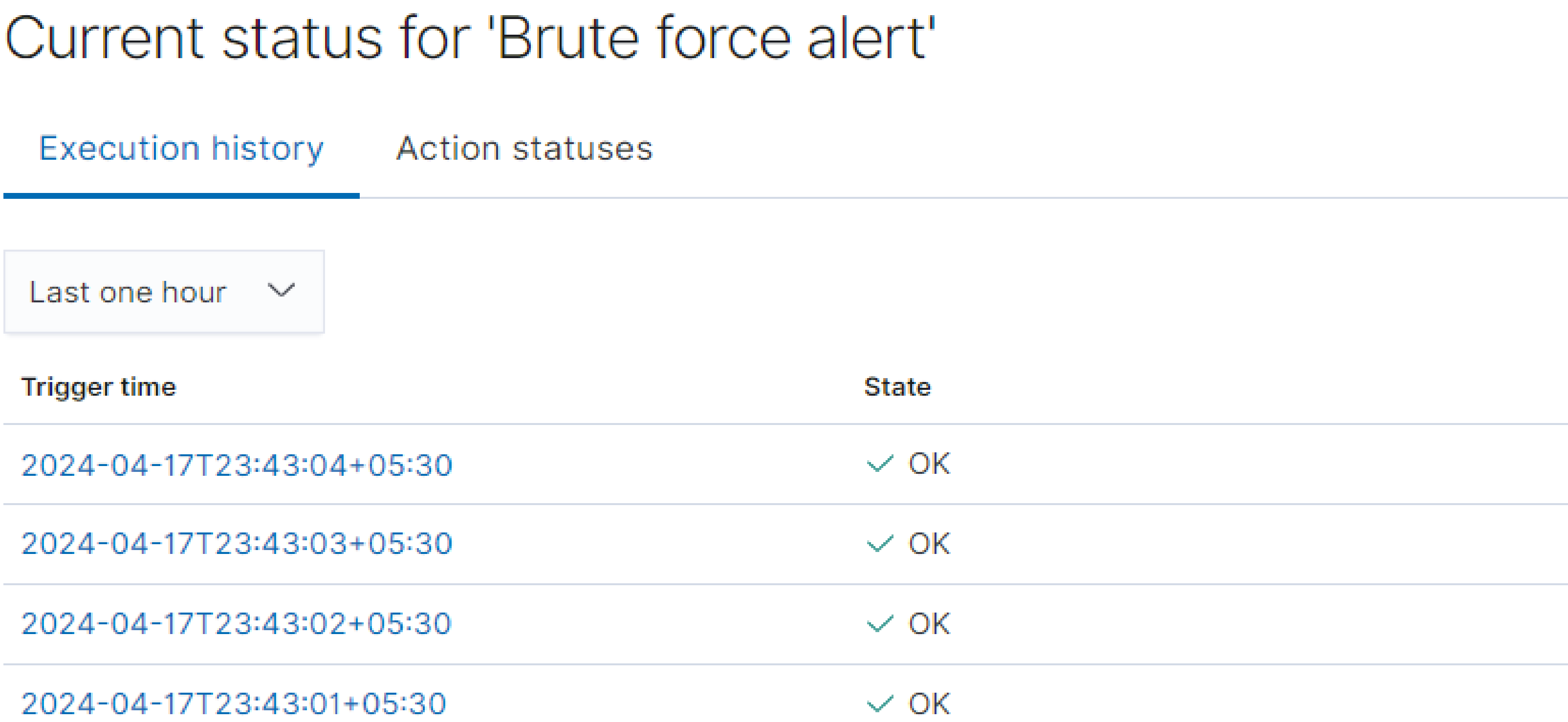
Use * to broaden your query.

Time field: @timestamp

Run watch every: 1 minute

Match the following condition

```
WHEN count() GROUPED OVER top 5 'event.outcome' IS BELOW OR EQUALS 2 FOR THE LAST 1 minute
```

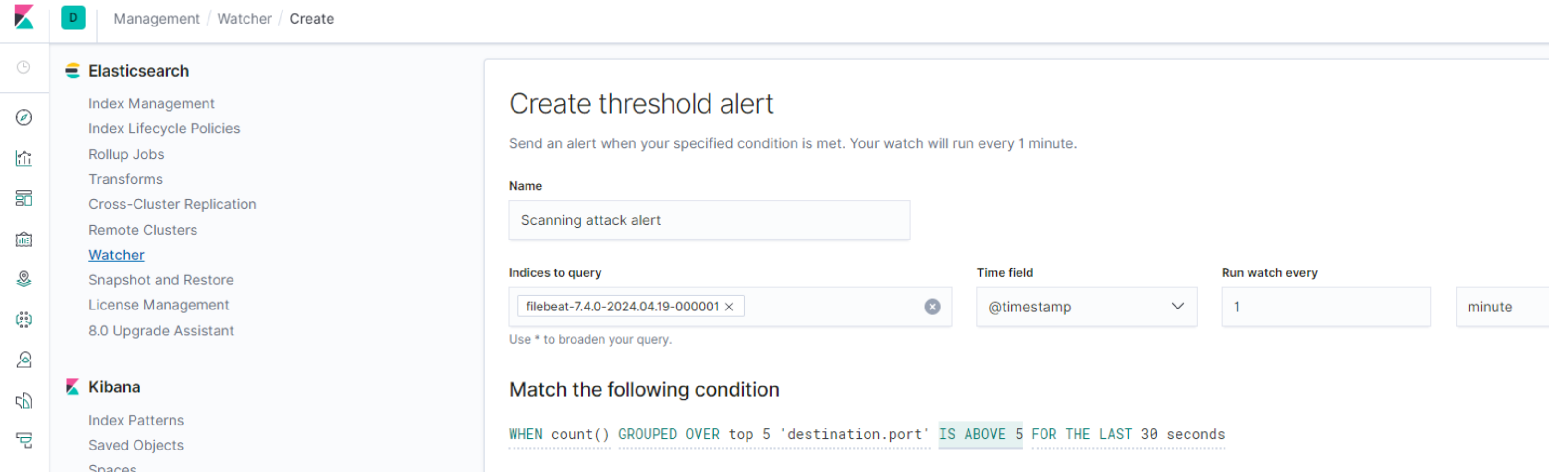


Current status for 'Brute force alert'

Trigger time	State
2024-04-17T23:43:04+05:30	✓ OK
2024-04-17T23:43:03+05:30	✓ OK
2024-04-17T23:43:02+05:30	✓ OK
2024-04-17T23:43:01+05:30	✓ OK

3.3.3 Screenshot

Create an alert for a scanning attack. During the scan, an attacker is looking to identify what ports are open.



Create threshold alert

Send an alert when your specified condition is met. Your watch will run every 1 minute.

Name: Scanning attack alert

Indices to query: filebeat-7.4.0-2024.04.19-000001

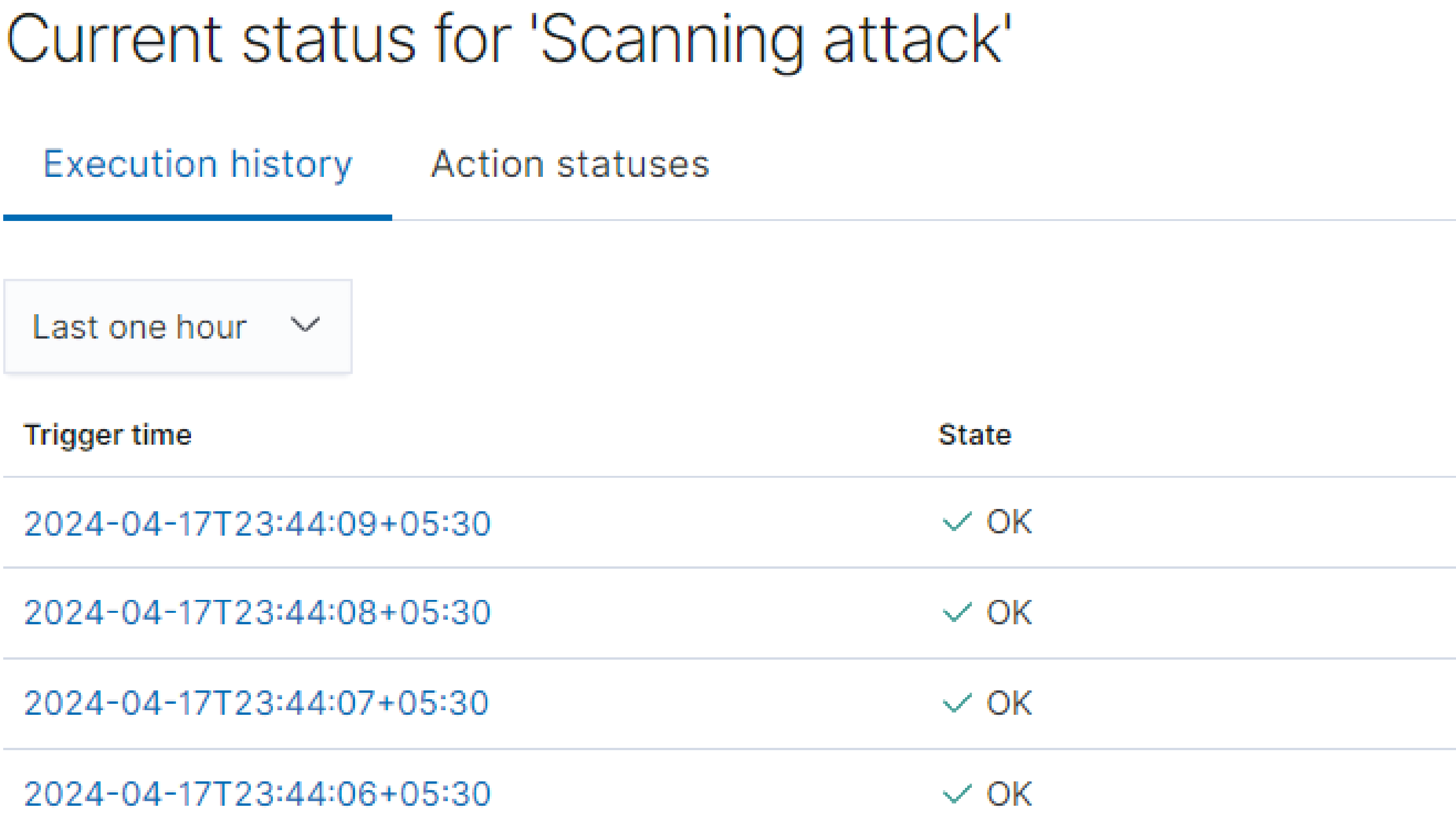
Use * to broaden your query.

Time field: @timestamp

Run watch every: 1 minute

Match the following condition

```
WHEN count() GROUPED OVER top 5 'destination.port' IS ABOVE 5 FOR THE LAST 30 seconds
```



Current status for 'Scanning attack'

Last one hour

Trigger time	State
2024-04-17T23:44:09+05:30	✓ OK
2024-04-17T23:44:08+05:30	✓ OK
2024-04-17T23:44:07+05:30	✓ OK
2024-04-17T23:44:06+05:30	✓ OK

3.4 Incident Response Playbook

Write a playbook below, detailing what the set of steps would be in response to each of the alerts you created in the last section 4.3. Add more pages if you need.

DoS Attack Playbook

1. Preparation:

Establish a response team and define their roles and responsibilities.

Develop a communication plan and ensure that all stakeholders are aware of it.

Create and maintain a DoS attack response plan that includes procedures for detecting, analyzing, containing, eradicating, and recovering from an attack.

2. Detection & Analysis:

Monitor network traffic and set up alerts for unusual patterns.

Analyze network logs to determine the source and type of the attack.

Determine the impact of the attack on your network and applications.

3. Containment, Eradication, and Recovery:

Implement access controls to limit the spread of the attack.

Block traffic from the source of the attack.

Work with your service provider to filter traffic and mitigate the attack's impact.

4. Post-Incident Activity:

Conduct a post-incident review to identify the root cause and assess the effectiveness of the response.

Update your incident response plan and procedures based on the lessons learned.

Provide training and awareness programs to prevent similar incidents in the future.

Brute Force Attack Playbook

1. Preparation:

Establish a response team and define their roles and responsibilities.

Implement strong access controls and authentication mechanisms.

Develop a brute force attack response plan that includes procedures for detecting, analyzing, containing, eradicating, and recovering from an attack.

2. Detection & Analysis:

Monitor login attempts and set up alerts for unusual patterns.

Analyze logs to determine the source and frequency of the attacks.

Determine the impact of the attack on your network and applications.

3. Containment, Eradication, and Recovery:

Implement account lockout policies and CAPTCHA mechanisms.

Block traffic from the source of the attack.

Reset user passwords and review access controls.

4. Post-Incident Activity:

Conduct a post-incident review to identify the root cause and assess the effectiveness of the response.

Update your incident response plan and procedures based on the lessons learned.

Provide training and awareness programs to prevent similar incidents in the future.

Scanning Attack Playbook

Preparation

1. Develop a comprehensive inventory of all systems and assets to understand the baseline of your network.
2. Implement intrusion detection systems and network monitoring tools to detect scanning activities.
3. Establish communication protocols and escalation procedures to respond swiftly to any detected scanning attacks.

Detection & Analysis

1. Monitor network traffic for unusual patterns or spikes in scanning activity.
2. Analyze logs and alerts from intrusion detection systems to identify the source and nature of the scanning attack.
3. Utilize threat intelligence feeds to understand the tactics, techniques, and procedures commonly associated with scanning attacks.

Containment, Eradication, and Recovery

1. Isolate affected systems to prevent further spread of the scanning attack.
2. Remove malicious code or malware associated with the scanning attack.
3. Restore systems from clean backups and implement security patches to prevent future scanning attacks.

Post-Incident Activity

1. Conduct a thorough post-incident analysis to identify gaps in security controls that allowed the scanning attack to occur.
2. Update incident response procedures based on lessons learned from the scanning attack.
3. Provide training and awareness programs to educate employees on how to recognize and report scanning activities in the future.

Section 4

Designing a Zero Trust Model

Section 4: Zero Trust Model

XYZ is elated with the work you've done so far! But they've been hearing about this new buzzword "Zero Trust" and are curious as to what it is and what the architecture would look like in a Zero Trust model. So your next task below is to design a Zero Trust model, then explain the differences between your network architecture and your Zero Trust model.

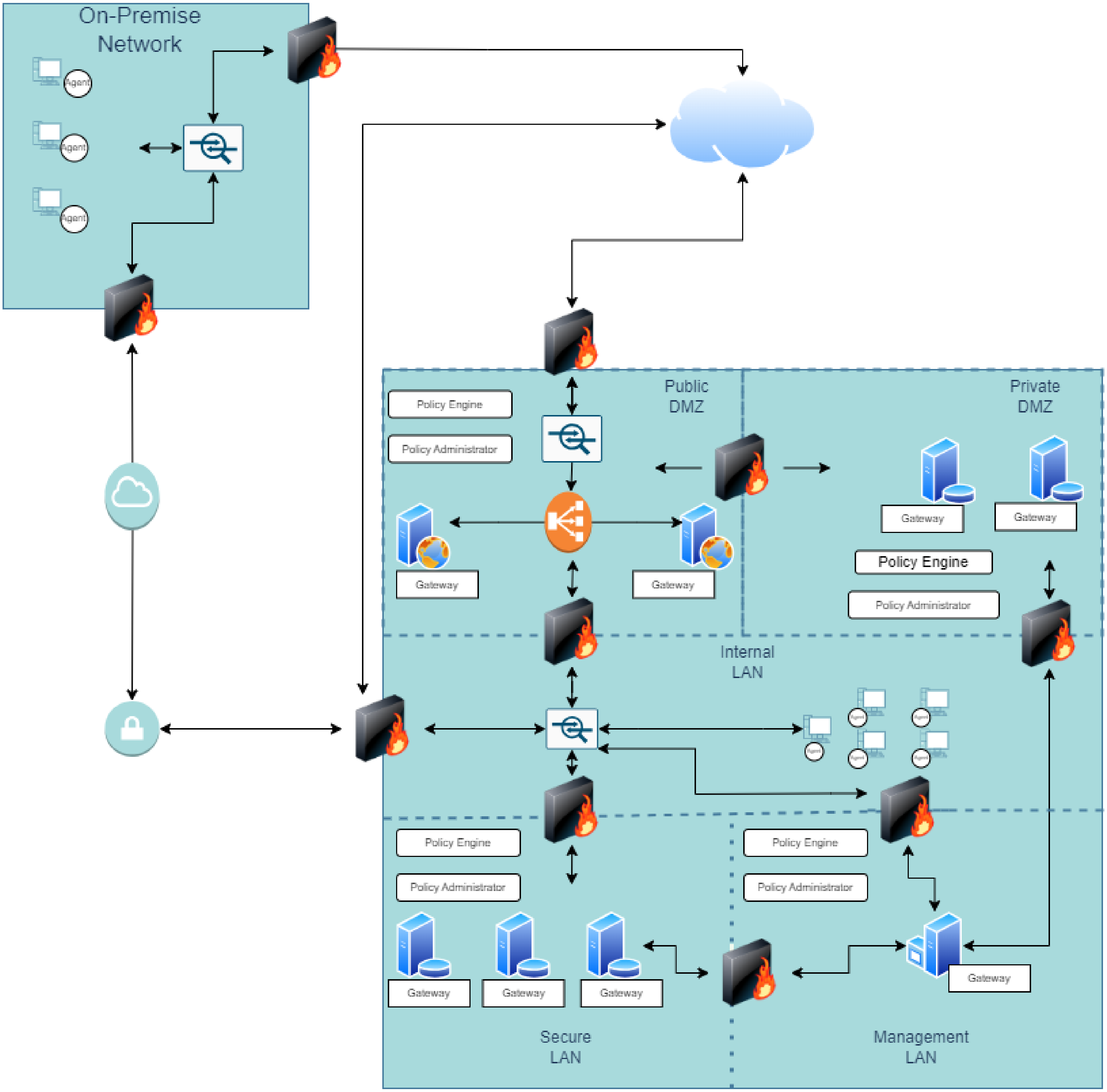
Design a Zero Trust model of your network architecture using https://app.diagrams.net/.

Make sure to incorporate the following into your design:

- Identity
- Devices
- Apps
- Network
- Data
- Infrastructure
- Trusted and Untrusted Devices
- Controls

4.1 Zero Trust Model

Paste your Zero Trust model diagram here:



4.2 Modern Architecture vs. Zero Trust

Write a detailed comparative analysis of the differences between your Zero Trust model and your secure network architecture design.

Trust Model:

1.Traditional: Implicit trust for users within the network perimeter.
2.Zero Trust: Continuous verification of users, devices, and access requests.

Perimeter Security:

1. Traditional: Relies heavily on a strong network perimeter firewall.
2. Zero Trust: De-emphasizes perimeter, focusing on access control for all.

Access Control:

1. Traditional: Static access based on pre-defined user groups.
2. Zero Trust: Dynamic access control based on real-time factors (identity, device health, application).

Data Security:

1. Traditional: Data security as an afterthought, often perimeter-dependent.
2. Zero Trust: Integrates data security throughout (encryption, access controls).

Visibility:

1. Traditional: Limited visibility into user activity within the network.
2. Zero Trust: Continuous monitoring of user and device behavior for anomalies.

Least Privilege:

1. Traditional: Risk of granting excessive access privileges.
2. Zero Trust: Focus on granting only the minimum access needed (least privilege).

Microsegmentation:

1. Traditional: Large network segments with broad access.
2. Zero Trust: Network segmentation into smaller, more secure zones.

Device Security:

1. Traditional: Limited device security checks before granting access.
2. Zero Trust: Rigorous device security checks (posture, compliance) before access.

Remote Access:

1. Traditional: Remote access often relies on VPNs, creating a new perimeter.
2. Zero Trust: Secure remote access through dedicated access points.