

# **Project: Securing the Perimeter**

## **Directions and Submission Template**

**Mohamad Abdelnaby**

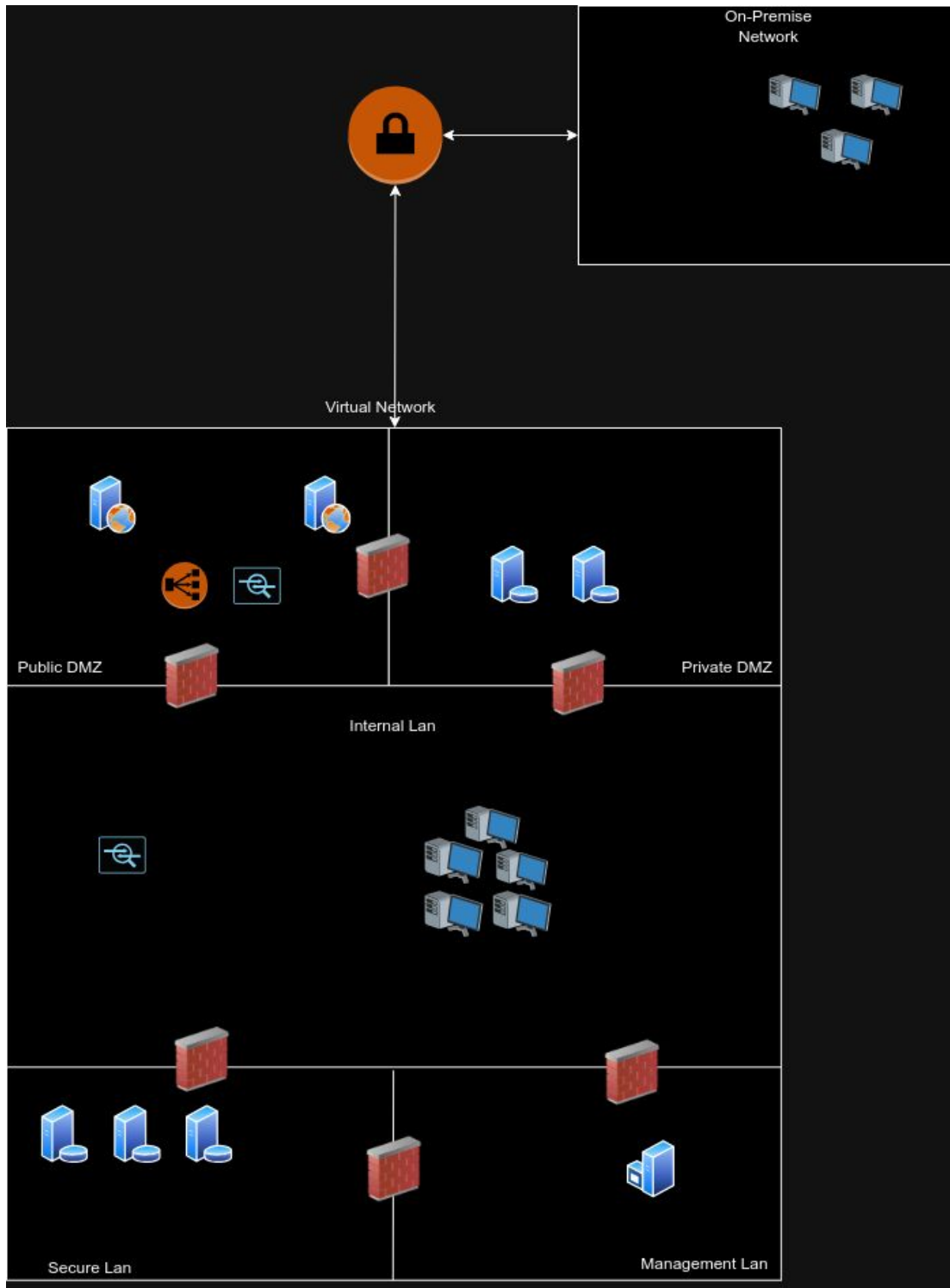
**2024/04/18**



## **Section 1**

# **Designing a Secure Network Architecture**

# 1.1 Designing the Network



---

## **Section 2**

# **Building a Secure Network Architecture in Azure**

# 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.

Microsoft Azure

Search resources, services, and docs (G+I)

odl\_user\_257555@udaci...

UDACITY (UDACITYLABS.ONMIC...

Home >

Virtual networks

Udacity (udacitylabs.onmicrosoft.com)

Create

Manage view

Refresh

Export to CSV

Open query

Assign tags

Filter for any field...

Subscription equals all

Resource group equals all

Location equals all

Add filter

Showing 1 to 2 of 2 records.

No grouping

List view

<input type="checkbox"/> Name ↑↓	Resource group ↑↓	Location ↑↓	Subscription ↑↓	
<input type="checkbox"/> DMZ	entp-project-257555	West US	Udacity CloudLabs Sub - 47	...
<input type="checkbox"/> Internal	entp-project-257555	West US	Udacity CloudLabs Sub - 47	...

< Previous

Page 1 of 1

Next >

Give feedback

# 2.1.2 Screenshot

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

Microsoft Azure

Search resources, services, and docs (G+)

odl\_user\_257555@udaci...  
UDACITY (UDACITYLABS.ONMIC...

Home > Virtual networks > DMZ

Virtual networks

Udacity (udacitylabs.onmicrosoft.com)

+ Create Manage view

Filter for any field...

Name ↑

DMZ

Internal

DMZ | Subnets

Virtual network

Search

+ Subnet + Gateway subnet Refresh Manage users Delete

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

Bastion

DDoS protection

Firewall

Microsoft Defender for Cloud

Network manager

DNS servers

Peerings

Service endpoints

Private endpoints

Properties

Locks

Monitoring

Alerts

Metrics

Dagnostic settings

Search subnets

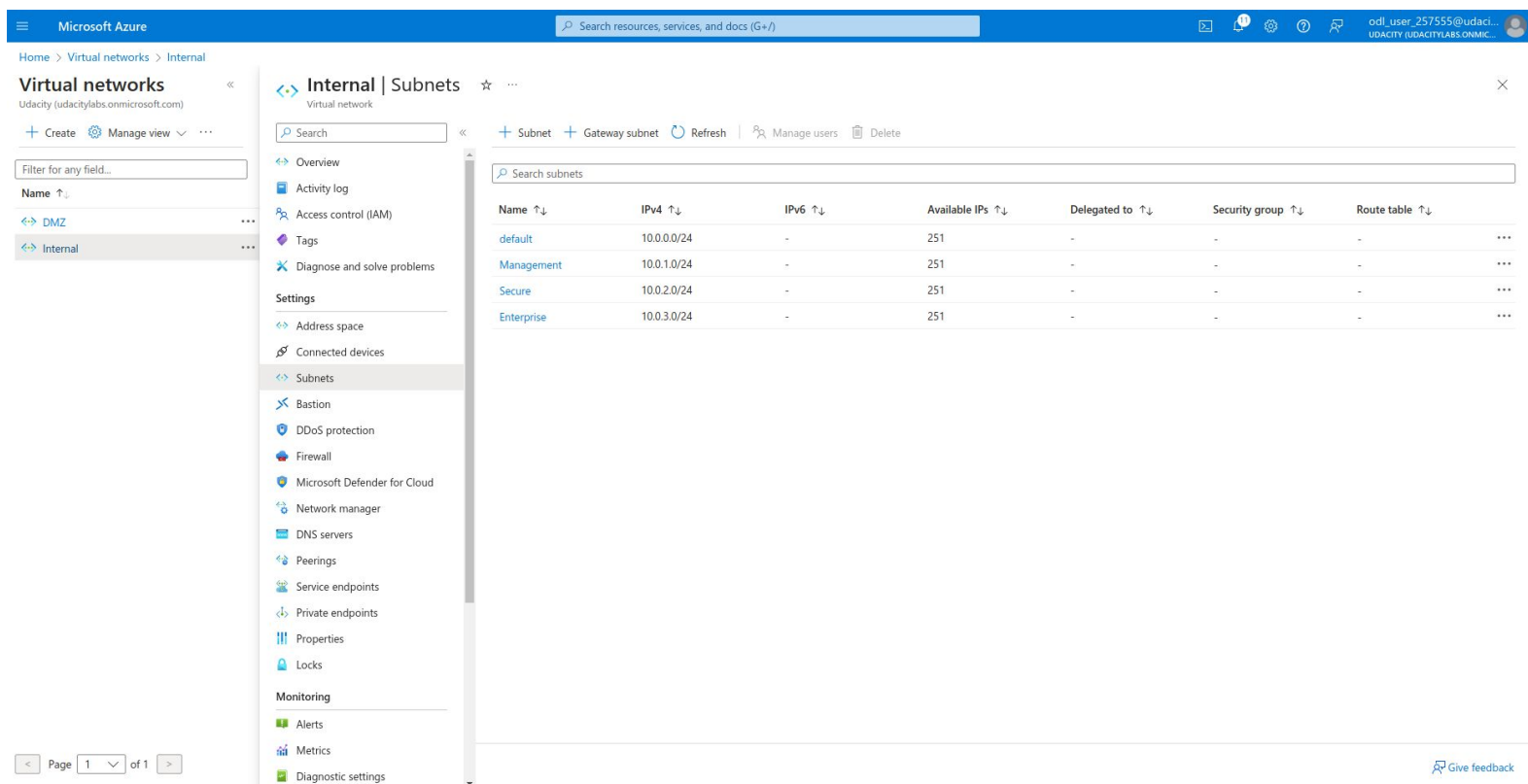
Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓	Delegated to ↑↓	Security group ↑↓	Route table ↑↓	
default	10.0.0.0/24	-	251	-	-	-	...
public	10.0.1.0/24	-	251	-	-	-	...
private	10.0.2.0/24	-	251	-	-	-	...

Page 1 of 1

Give feedback

## 2.1.3 Screenshot

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



The screenshot shows the Microsoft Azure portal interface. The top navigation bar is blue with the Microsoft Azure logo on the left, a search bar in the center, and user information on the right. The left sidebar contains a navigation menu with various options, including 'Subnets' which is currently selected. The main content area displays the 'Internal | Subnets' page. At the top of this page, there are buttons for '+ Subnet', '+ Gateway subnet', 'Refresh', 'Manage users', and 'Delete'. Below this is a search bar for subnets. A table lists the subnets with columns for Name, IPv4, IPv6, Available IPs, Delegated to, Security group, and Route table. The table contains four rows: 'default', 'Management', 'Secure', and 'Enterprise'. Each row has a three-dot menu icon on the right. At the bottom of the page, there is a 'Give feedback' link.

Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓	Delegated to ↑↓	Security group ↑↓	Route table ↑↓	
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	-	-	-	...

# 2.2.1 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.

The screenshot displays the Microsoft Azure portal interface for a virtual machine named 'publicDMZ-VM'. The left sidebar shows the 'Virtual machines' section with a filter for 'Name' and a list of VMs. The main content area is divided into two panels: 'Overview' and 'Essentials'. The 'Overview' panel shows the VM's status as 'Running' and its location as 'West US'. The 'Essentials' panel provides a detailed overview of the VM's configuration, including its operating system (Linux ubuntu 20.04), size (Standard B1s), and network settings (Public IP address: 13.93.164.123, Virtual network/subnet: DMZ/public). The 'Properties' tab is selected, showing the VM's configuration details, including the image (0001-com-ubuntu-server-focal), architecture (x64), and agent status (Ready). The 'Networking' tab shows the VM's network configuration, including the public IP address and the virtual network/subnet. The 'Size' tab shows the VM's size (Standard B1s) and its vCPUs (1) and RAM (1 GiB). The 'Disk' tab shows the VM's disk configuration, including the OS disk (publicDMZ-VM\_disk1\_c4c137e1dc3f4dabb7d3e47d6c963728) and its encryption status (Disabled).

Category	Property	Value
Essentials	Resource group	entp-project-257555
Essentials	Status	Running
Essentials	Location	West US
Essentials	Subscription	Udacity CloudLabs Sub - 47
Essentials	Subscription ID	4b3772c6-b172-4365-af69-d7c8dd719197
Essentials	Operating system	Linux (ubuntu 20.04)
Essentials	Size	Standard B1s (1 vcpu, 1 GiB memory)
Essentials	Public IP address	13.93.164.123
Essentials	Virtual network/subnet	DMZ/public
Essentials	DNS name	Not configured
Essentials	Health state	-
Properties	Computer name	publicDMZ-VM
Properties	Operating system	Linux (ubuntu 20.04)
Properties	Image publisher	canonical
Properties	Image offer	0001-com-ubuntu-server-focal
Properties	Image plan	20_04-its-gen2
Properties	VM generation	V2
Properties	VM architecture	x64
Properties	Agent status	Ready
Properties	Agent version	2.10.0.8
Properties	Hibernation	Disabled
Properties	Host group	-
Properties	Host	-
Properties	Proximity placement group	-
Properties	Colocation status	N/A
Properties	Capacity reservation group	-
Properties	Disk controller type	SCSI
Networking	Public IP address	13.93.164.123 ( Network interface publicdmz-vm323 )
Networking	Public IP address (IPv6)	-
Networking	Private IP address	10.0.1.4
Networking	Private IP address (IPv6)	-
Networking	Virtual network/subnet	DMZ/public
Networking	DNS name	Configure
Size	Size	Standard B1s
Size	vCPUs	1
Size	RAM	1 GiB
Disk	OS disk	publicDMZ-VM_disk1_c4c137e1dc3f4dabb7d3e47d6c963728
Disk	Encryption at host	Disabled
Disk	Azure disk encryption	Not enabled
Disk	Ephemeral OS disk	N/A

The screenshot displays the Microsoft Azure portal interface for a virtual machine named 'privateDMZ-VM'. The left sidebar shows the 'Virtual machines' section with a filter for 'Name' and a list of VMs. The main content area is divided into two panels: 'Overview' and 'Essentials'. The 'Overview' panel shows the VM's status as 'Running' and its location as 'West US'. The 'Essentials' panel provides a detailed overview of the VM's configuration, including its operating system (Linux ubuntu 20.04), size (Standard B1s), and network settings (Public IP address: 13.93.160.178, Virtual network/subnet: DMZ/private). The 'Properties' tab is selected, showing the VM's configuration details, including the image (0001-com-ubuntu-server-focal), architecture (x64), and agent status (Ready). The 'Networking' tab shows the VM's network configuration, including the public IP address and the virtual network/subnet. The 'Size' tab shows the VM's size (Standard B1s) and its vCPUs (1) and RAM (1 GiB). The 'Disk' tab shows the VM's disk configuration, including the OS disk (privateDMZ-VM\_disk1\_efdd265c9bd940d089c68b8dc6a5a806) and its encryption status (Disabled).

Category	Property	Value
Essentials	Resource group	entp-project-257555
Essentials	Status	Running
Essentials	Location	West US
Essentials	Subscription	Udacity CloudLabs Sub - 47
Essentials	Subscription ID	4b3772c6-b172-4365-af69-d7c8dd719197
Essentials	Operating system	Linux (ubuntu 20.04)
Essentials	Size	Standard B1s (1 vcpu, 1 GiB memory)
Essentials	Public IP address	13.93.160.178
Essentials	Virtual network/subnet	DMZ/private
Essentials	DNS name	Not configured
Essentials	Health state	-
Properties	Computer name	privateDMZ-VM
Properties	Operating system	Linux (ubuntu 20.04)
Properties	Image publisher	canonical
Properties	Image offer	0001-com-ubuntu-server-focal
Properties	Image plan	20_04-its-gen2
Properties	VM generation	V2
Properties	VM architecture	x64
Properties	Agent status	Ready
Properties	Agent version	2.10.0.8
Properties	Hibernation	Disabled
Properties	Host group	-
Properties	Host	-
Properties	Proximity placement group	-
Properties	Colocation status	N/A
Properties	Capacity reservation group	-
Properties	Disk controller type	SCSI
Networking	Public IP address	13.93.160.178 ( Network interface privatedmz-vm435 )
Networking	Public IP address (IPv6)	-
Networking	Private IP address	10.0.2.5
Networking	Private IP address (IPv6)	-
Networking	Virtual network/subnet	DMZ/private
Networking	DNS name	Configure
Size	Size	Standard B1s
Size	vCPUs	1
Size	RAM	1 GiB
Disk	OS disk	privateDMZ-VM_disk1_efdd265c9bd940d089c68b8dc6a5a806
Disk	Encryption at host	Disabled
Disk	Azure disk encryption	Not enabled
Disk	Ephemeral OS disk	N/A



# 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.

Home > Virtual machines >

Virtual machines

Udacity (udacitylabs.onmicrosoft.com)

+ Create

Switch to classic

Filter for any field...

Name

InternalManagement-VM

InternalSecure-VM

privateDMZ-VM

publicDMZ-VM

InternalManagement-VM

Virtual machine

Search

Connect

Start

Restart

Stop

Hibernate (preview)

Capture

Delete

Refresh

Open in mobile

Feedback

CLI / PS

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Connect

Bastion

Networking

Network settings

Load balancing

Application security groups

Network manager

Settings

Disks

Extensions + applications

Configuration

Advisor recommendations

Properties

Locks

Availability + scale

Size

Availability + scaling

Essentials

Resource group (new)

Status

Location

Subscription (new)

Subscription ID

Operating system

Size

Public IP address

Virtual network/subnet

DNS name

Health state

Tags (edit)

JSON View

Properties

Monitoring

Capabilities (7)

Recommendations

Tutorials

Virtual machine

Computer name

Operating system

Image publisher

Image offer

Image plan

VM generation

VM architecture

Agent status

Agent version

Hibernation

Host group

Host

Proximity placement group

Colocation status

Capacity reservation group

Disk controller type

InternalManagement-VM

Linux (ubuntu 20.04)

canonical

0001-com-ubuntu-server-focal

20\_04-its-gen2

V2

x64

Ready

2.10.0.8

Disabled

-

-

N/A

-

SCSI

Networking

Public IP address

Public IP address (IPv6)

Private IP address

Private IP address (IPv6)

Virtual network/subnet

DNS name

13.88.177.130 ( Network interface internalmanagement-vm758 )

-

10.0.1.4

-

Internal/Management

Configure

Size

Size

vCPUs

RAM

Standard B1s

1

1 GiB

Disk

OS disk

InternalManagement-VM\_disk1\_0d05449698a44e14b73d866b17b23347

Encryption at host

Azure disk encryption

Disabled

Not enabled

Virtual machines

Udacity (udacitylabs.onmicrosoft.com)

+ Create

Switch to classic

Filter for any field...

Name

InternalManagement-VM

InternalSecure-VM

privateDMZ-VM

publicDMZ-VM

InternalSecure-VM

Virtual machine

Search

Connect

Start

Restart

Stop

Hibernate (preview)

Capture

Delete

Refresh

Open in mobile

Feedback

CLI / PS

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Connect

Bastion

Networking

Network settings

Load balancing

Application security groups

Network manager

Settings

Disks

Extensions + applications

Configuration

Advisor recommendations

Properties

Locks

Availability + scale

Size

Availability + scaling

Essentials

Resource group (new)

Status

Location

Subscription (new)

Subscription ID

Operating system

Size

Public IP address

Virtual network/subnet

DNS name

Health state

Tags (edit)

JSON View

Properties

Monitoring

Capabilities (7)

Recommendations

Tutorials

Virtual machine

Computer name

Operating system

Image publisher

Image offer

Image plan

VM generation

VM architecture

Agent status

Agent version

Hibernation

Host group

Host

Proximity placement group

Colocation status

Capacity reservation group

Disk controller type

InternalSecure-VM

Linux (ubuntu 20.04)

canonical

0001-com-ubuntu-server-focal

20\_04-its-gen2

V2

x64

Ready

2.10.0.8

Disabled

-

-

N/A

-

SCSI

Networking

Public IP address

Public IP address (IPv6)

Private IP address

Private IP address (IPv6)

Virtual network/subnet

DNS name

13.88.179.150 ( Network interface internalsecure-vm90 )

-

10.0.2.4

-

Internal/Secure

Configure

Size

Size

vCPUs

RAM

Standard B1s

1

1 GiB

Disk

OS disk

InternalSecure-VM\_OsDisk\_1\_8a1130ba9109480ba16c5060ca21bb

Encryption at host

Azure disk encryption

Disabled

Not enabled

Virtual machines

Udacity (udacitylabs.onmicrosoft.com)

+ Create

Switch to classic

Filter for any field...

Name

InternalEnterprise-VM

InternalManagement-VM

InternalSecure-VM

privateDMZ-VM

publicDMZ-VM

InternalEnterprise-VM

Virtual machine

Search

Connect

Start

Restart

Stop

Hibernate (preview)

Capture

Delete

Refresh

Open in mobile

Feedback

CLI / PS

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Connect

Bastion

Networking

Network settings

Load balancing

Application security groups

Network manager

Settings

Disks

Extensions + applications

Configuration

Advisor recommendations

Properties

Locks

Availability + scale

Size

Availability + scaling

Essentials

Resource group (new)

Status

Location

Subscription (new)

Subscription ID

Operating system

Size

Public IP address

Virtual network/subnet

DNS name

Health state

Tags (edit)

JSON View

Properties

Monitoring

Capabilities (7)

Recommendations

Tutorials

Virtual machine

Computer name

Operating system

Image publisher

Image offer

Image plan

VM generation

VM architecture

Agent status

Agent version

Hibernation

Host group

Host

Proximity placement group

Colocation status

Capacity reservation group

Disk controller type

InternalEnterprise-VM

Linux (ubuntu 20.04)

canonical

0001-com-ubuntu-server-focal

20\_04-its-gen2

V2

x64

Ready

2.10.0.8

Disabled

-

-

N/A

-

SCSI

Networking

Public IP address

Public IP address (IPv6)

Private IP address

Private IP address (IPv6)

Virtual network/subnet

DNS name

13.88.180.141 ( Network interface internalenterprise-vm805 )

-

10.0.3.4

-

Internal/Enterprise

Configure

Size

Size

vCPUs

RAM

Standard B1s

1

1 GiB

Disk

OS disk

InternalEnterprise-VM\_OsDisk\_1\_8981af07976a69b3b123866a6d802b

Encryption at host

Azure disk encryption

Disabled

Not enabled

# 2.3.1 Screenshot

## Traffic rules in your DMZ.

Home > DMZ

DMZ | Inbound security rules

Network security group

Search

+ Add Hide default rules Refresh Delete Give feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Alerts

Diagnostic settings

Logs

NSG flow logs

Automation

CLI / PS

Tasks (preview)

Export template

Help

Effective security rules

Filter by name

Port == all Protocol == all Source == all Destination == all Action == all

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
<input type="checkbox"/> 300	port8080	80	TCP	Any	VirtualNetwork	Allow
<input type="checkbox"/> 320	port443	443	TCP	Any	VirtualNetwork	Allow
<input type="checkbox"/> 330	kibanaa	5601	Any	172.16.1.0/24	VirtualNetwork	Allow
<input type="checkbox"/> 400	YamoVPN	22	TCP	172.16.1.0/24	VirtualNetwork	Allow
<input type="checkbox"/> 500	DenyAllInboundTraffic	Any	Any	Any	Any	Deny
<input type="checkbox"/> 65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
<input type="checkbox"/> 65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
<input type="checkbox"/> 65500	DenyAllInBound	Any	Any	Any	Any	Deny

# 2.3.2 Screenshot

## Traffic rules in your Internal network.

Microsoft Azure

Search resources, services, and docs (G+)

odl\_user\_257555@udaci...  
UDACITY (UDACITYLABS.ONMIC...

Home > Network security groups > Internal

Network security g...  
Udacity (udacitylabs.onmicrosoft.com)

Create

Manage view

Filter for any field...

DMZ

Internal

Internal | Inbound security rules

Network security group

Search

Add

Hide default rules

Refresh

Delete

Give feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Alerts

Diagnostic settings

Logs

NSG flow logs

Automation

CLI / PS

Tasks (preview)

Export template

Help

Effective security rules

Filter by name

Port == all

Protocol == all

Source == all

Destination == all

Action == all

Priority	Name	Port	Protocol	Source	Destination	Action
400	YamoVPN	22	TCP	172.16.1.0/24	VirtualNetwork	Allow
500	DenyAllInboundTraffic	Any	Any	Any	VirtualNetwork	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn...	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](#)

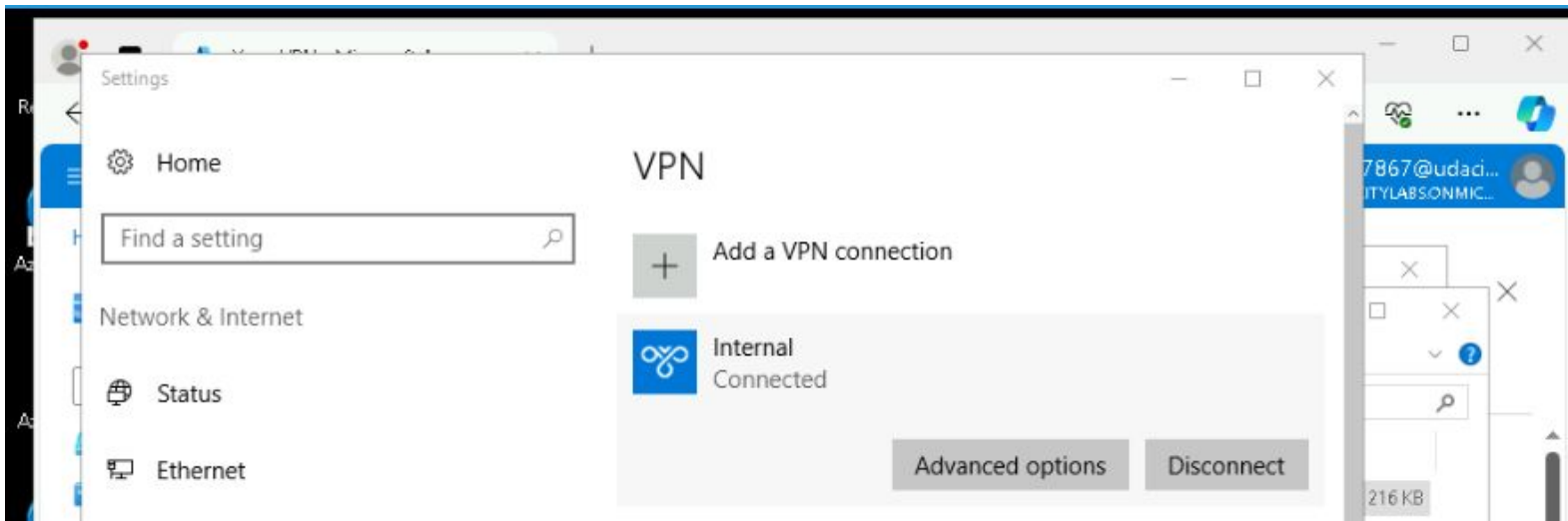
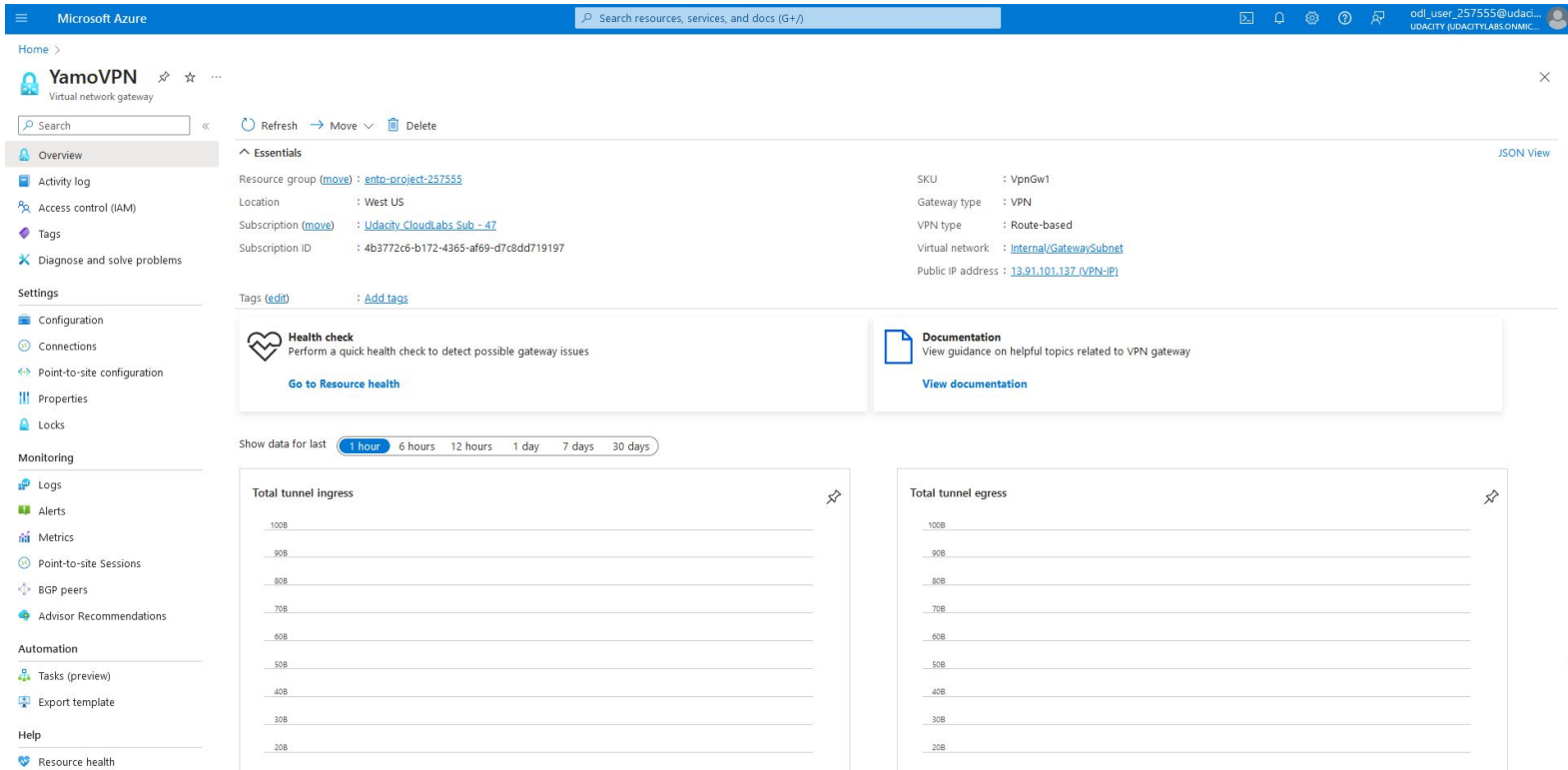
Page 1 of 1

go.microsoft.com/fwlink/?linkid=2174617

Reset 100% Apr 13 05:51

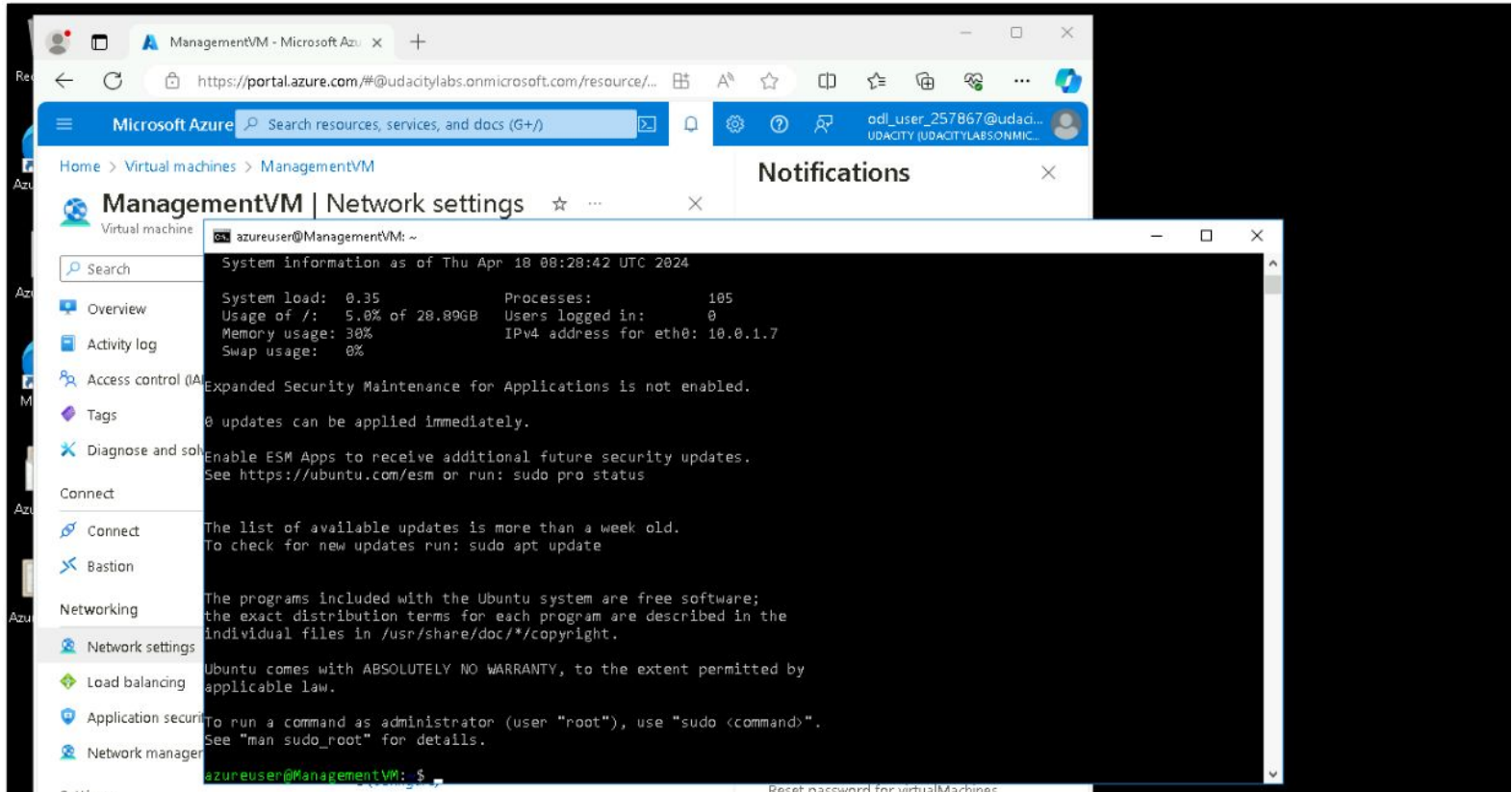
# 2.4.1 Screenshot

Create a VPN to connect to your internal network.



## 2.4.2 Screenshot

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



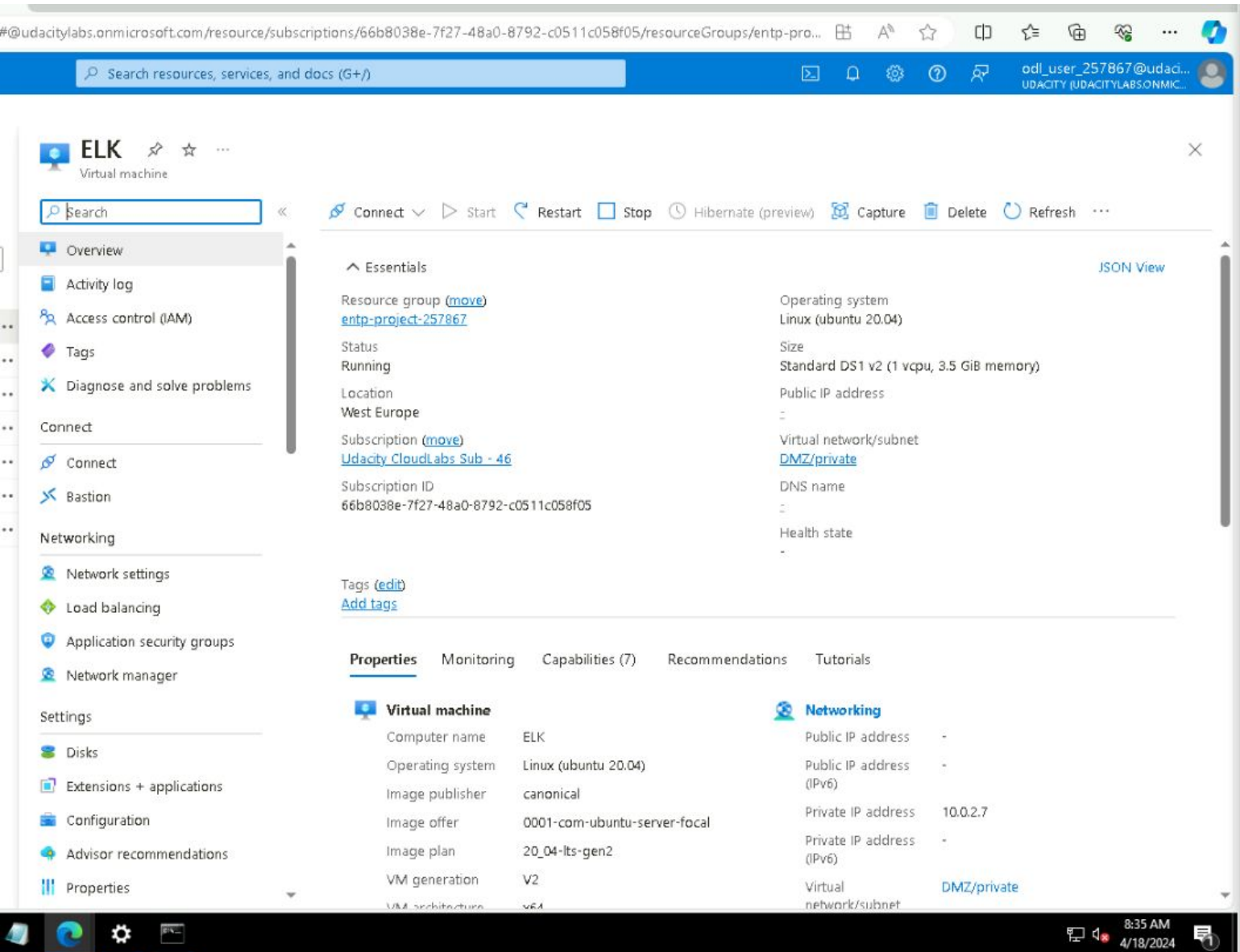


## **Section 3**

# **Continuous Monitoring with a SIEM**

# 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.



LABVM - 257867

Expand

# 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.

Microsoft Azure

Search resources, services, and docs (G+)

odl\_user\_257867@udaci...  
UDACITY

Home > Network security groups > DMZ

Network security g...  
Udacity

Create

Manage view

Filter for any field...

Name ↑

DMZ

Internal

DMZ | Inbound security rules

Network security group

Search

Add

Hide default rules

Refresh

Delete

Give feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Alerts

Diagnostic settings

Logs

NSG flow logs

Automation

CLI / PS

Tasks (preview)

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](#)

Filter by name

Port == all

Protocol == all

Source == all

Destination == all

Action == all

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
<input type="checkbox"/> 190	VPN	22	TCP	172.16.1.0/24	VirtualNetwork	✓ Allow
<input type="checkbox"/> 200	SSH	22	TCP	172.16.1.0/24	Any	✓ Allow
<input type="checkbox"/> 300	port8080	80	TCP	172.16.1.0/24	VirtualNetwork	✓ Allow
<input type="checkbox"/> 310	kibanaa	5601	Any	172.16.1.0/24	VirtualNetwork	✓ Allow
<input type="checkbox"/> 500	DenyAllInboundTraffic	Any	Any	Any	VirtualNetwork	✗ Deny
<input type="checkbox"/> 65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
<input type="checkbox"/> 65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	✓ Allow
<input type="checkbox"/> 65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny



# 3.2.1 Screenshot

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

```
azureuser@WebServerVM:/etc/filebeat$ sudo filebeat modules enable system
Enabled system
azureuser@WebServerVM:/etc/filebeat$ sudo filebeat modules enable apache
Enabled apache
azureuser@WebServerVM:/etc/filebeat$ sudo filebeat setup
Exiting: Couldn't connect to any of the configured Elasticsearch hosts. Errors: [Error connection to Elasticsearch http://10.0.2.9:9200: Get http://10.0.2.9:9200: dial tcp 10.0.2.9:9200: i/o timeout]
azureuser@WebServerVM:/etc/filebeat$ sudo filebeat setup
Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
Loaded machine learning job configurations
Loaded Ingest pipelines
azureuser@WebServerVM:/etc/filebeat$ sudo service filebeat start
azureuser@WebServerVM:/etc/filebeat$
```

## Step 1 of 2: Define index pattern

Index pattern

filebeat-7.4.0-2024.04.18-000001

You can use a \* as a wildcard in your index pattern.  
You can't use spaces or the characters \, /, ?, ", <, >, |.

> Next step

✓ **Success!** Your index pattern matches **1 index**.

filebeat-7.4.0-2024.04.18-000001

Rows per page: 10 ▾

## 3.2.2 Screenshot

Configure Filebeat to route web server logs to Elasticsearch.

```
GNU nano 4.8 filebeat.yml

# The URL from where to download the dashboards archive. By default this URL
# has a value which is computed based on the Beat name and version. For released
# versions, this URL points to the dashboard archive on the artifacts.elastic.co
# website.
#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:

  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify an additional path, the scheme is required: http://localhost:5601/path
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  host: "10.0.2.9:5601"

  # 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: ["10.0.2.9:9200"]

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

#----- Logstash output -----

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

[ Wrote 216 lines ]
^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos      M-U Undo
^X Exit          ^R Read File    ^_ Replace      ^U Paste Text  ^T To Spell    ^_ Go To Line   M-E Redo
```

# 3.2.3 Screenshot

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



Hello, yamo406.x

Easy Money

Dashb

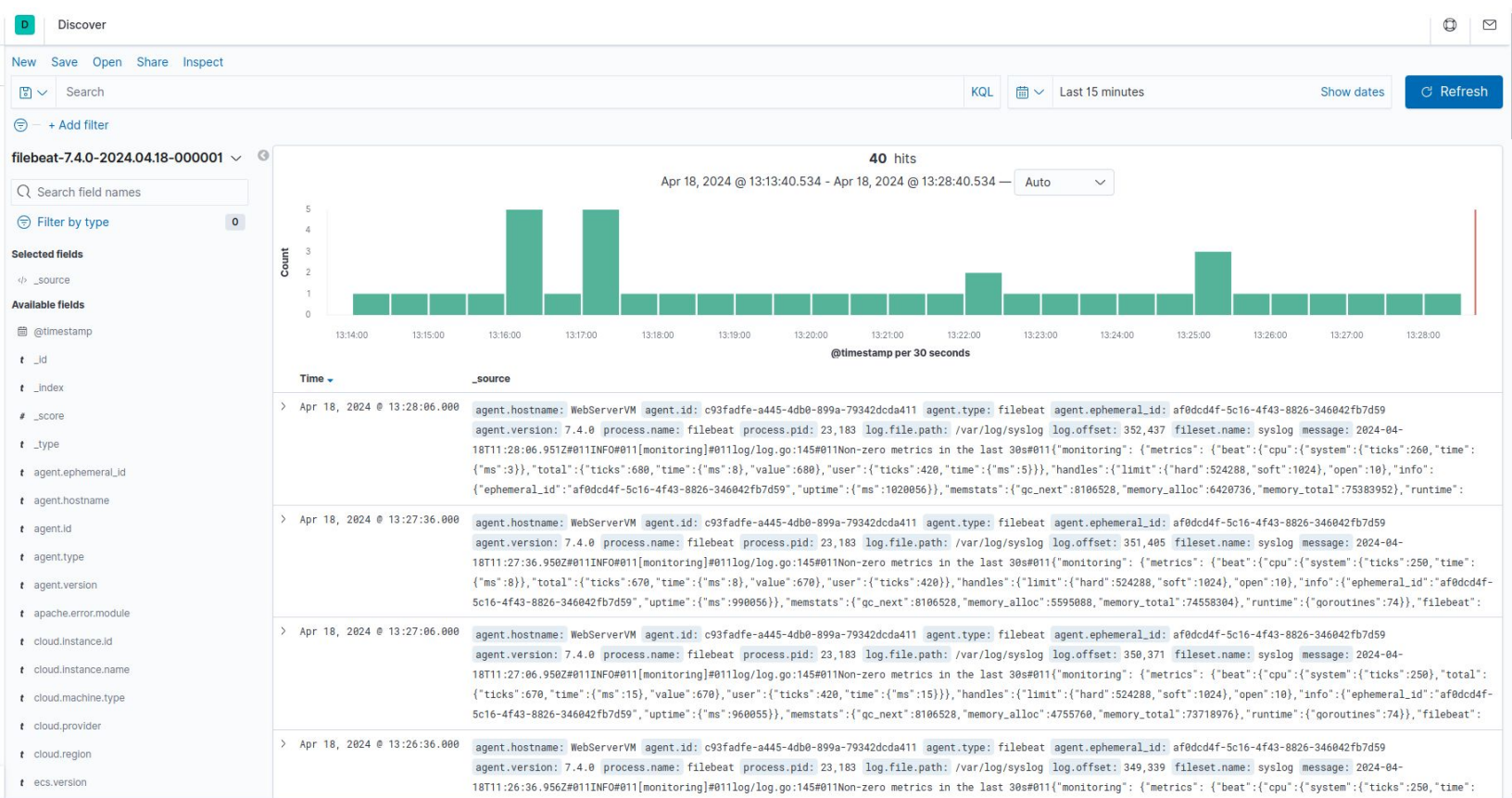
Connection to the target host failed mid communication

50 /50  
visits

2024-04-18 12:29:45	Visit #33	SUCCESS! ✓
2024-04-18 12:29:44	Visit #32	SUCCESS! ✓
2024-04-18 12:29:44	Visit #31	SUCCESS! ✓
2024-04-18 12:29:43	Visit #30	SUCCESS! ✓

# 3.2.4 Screenshot

Web server logs appear in Kibana.



# 3.3.1 Screenshot

## Create an alert for DoS attack.

Management / Watcher / Edit

Elasticsearch

Index Management

Index Lifecycle Policies

Rollup Jobs

Transforms

Cross-Cluster Replication

Remote Clusters

Watcher

Snapshot and Restore

License Management

8.0 Upgrade Assistant

Kibana

Index Patterns

Saved Objects

Spaces

Reporting

Advanced Settings

Beats

Central Management

Machine Learning

Jobs list

Edit 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-7.4.0-2024.04.18-000001 x

Time field

@timestamp

Run watch every

1

minute

Use \* to broaden your query.

Match the following condition

WHEN count() GROUPED OVER top 5 'http.request.method' IS ABOVE 100 FOR THE LAST 1 minute

No data

Your index and condition did not return any data.

Perform 1 action when condition is met

Add action

> Logging

Save alert

Cancel

Show request

# 3.3.2 Screenshot

Create an alert for Brute Force attack.

### Edit Brute Force Attack

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

**Name**

Brute Force Attack

**Indices to query**

filebeat-7.4.0-2024.04.18-000001

**Time field**

@timestamp

**Run watch every**

1

minute

Use \* to broaden your query.


**Match the following condition**

WHEN count() GROUPED OVER top 5 'source.address' IS ABOVE OR EQUALS 5 FOR THE LAST 5 minutes

No data

Your index and condition did not return any data.

**Perform 1 action when condition is met** [Add action](#)

☒  Logging

**Log text**

Watch for failed login attempts, indicator of Brute force attack

[Log a sample message](#)

✓ Save alert

Cancel

[Show request](#)



# 3.3.3 Screenshot

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

### Edit Scanning Attack

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

**Name**

Scanning Attack

**Indices to query**

filebeat-7.4.0-2024.04.18-000001

**Time field**

@timestamp

**Run watch every**

1

minute

Use \* to broaden your query.


**Match the following condition**

WHEN count() GROUPED OVER top 5 'source.port' IS ABOVE OR EQUALS 20 FOR THE LAST 5 minutes

No data

Your index and condition did not return any data.

**Perform 1 action when condition is met**

☒  Logging

**Log text**

Watch ports has exceeded the threshold

Log a sample message

Save alert

Cancel

Show request

# DOS Attack Playbook

## **Preparation:**

- Train the Security employees on identifying the true DOS attack alerts from false positives.
- All the employees have a direct contact to the security lead in case of DOS attack

## **Detection & Analysis:**

- Set up alerts for detecting DOS attacks, have them check if they get multiple requests that could threaten to flood the server and shutdown
- Document the logs including the DOS attack alert
- Prioritize business continuity if an attack will cause operations to stop immediately document the Source IP of the attack.

## **Containment, Eradication & Recovery:**

- Block the Source IP responsible for the attack
- Get all the threat actor details from the logs and document it
- If any service goes down restart and get it up and running, small patches for business continuity

## **Post-incident Activity:**

- Document the incident details, the threat actors information
- Can we do anything extra to mitigate future DOS attacks?
- Hold a meeting to discuss the incident.



# Brute Force Attack Playbook

## **Preparation:**

- Train the Security analysts on identifying a Brute force attack
- Contact information of a security lead who can answer at the time of incident, multiple tech leads with separate shifts covering the full 24/7

## **Detection & Analysis:**

- Check for alerts of failed logins from the same IP for a username.
- Check for alerts of different login geolocation for a username.
- Analyze the logs in out of hours logins.

## **Containment, Eradication & Recovery:**

- Block the IP address if it's not a trusted IP of an employee, lock the account.
- Did the threat actor get into the network? (Y/N)
  - Y: Determine the damage done i.e. infiltrated machines and isolate the machine from the network and block the IP
  - N: Block the IP and monitor the next hour for other similar attacks from other IPs

## **Post-incident Activity:**

- Document incident details
- Document threat actor information from the logs and add him to the blocked list of unauthorized IPs
- Hold a meeting to discuss the incident.
- Can we improve something to prevent future similar incidents?

# Scanning Attack Playbook

## **Preparation:**

- Train employees on identifying a scan attack on the ports of the machine or server on the network.
- Available access to a security lead 24/7
- Close all unused ports, use firewalls, and use DMARK for email authentication.

## **Detection & Analysis:**

- Monitor for alert of a scan of ports on the network

## **Containment, Eradication & Recovery:**

- Block the IP scanning and monitor next hour for similar attacks
- Did the threat actor gain access to the network? (Y/N)
  - Y: isolate the infected machines, and block the IP
  - N: Block the IP and monitor for similar attacks

## **Post-incident Activity:**

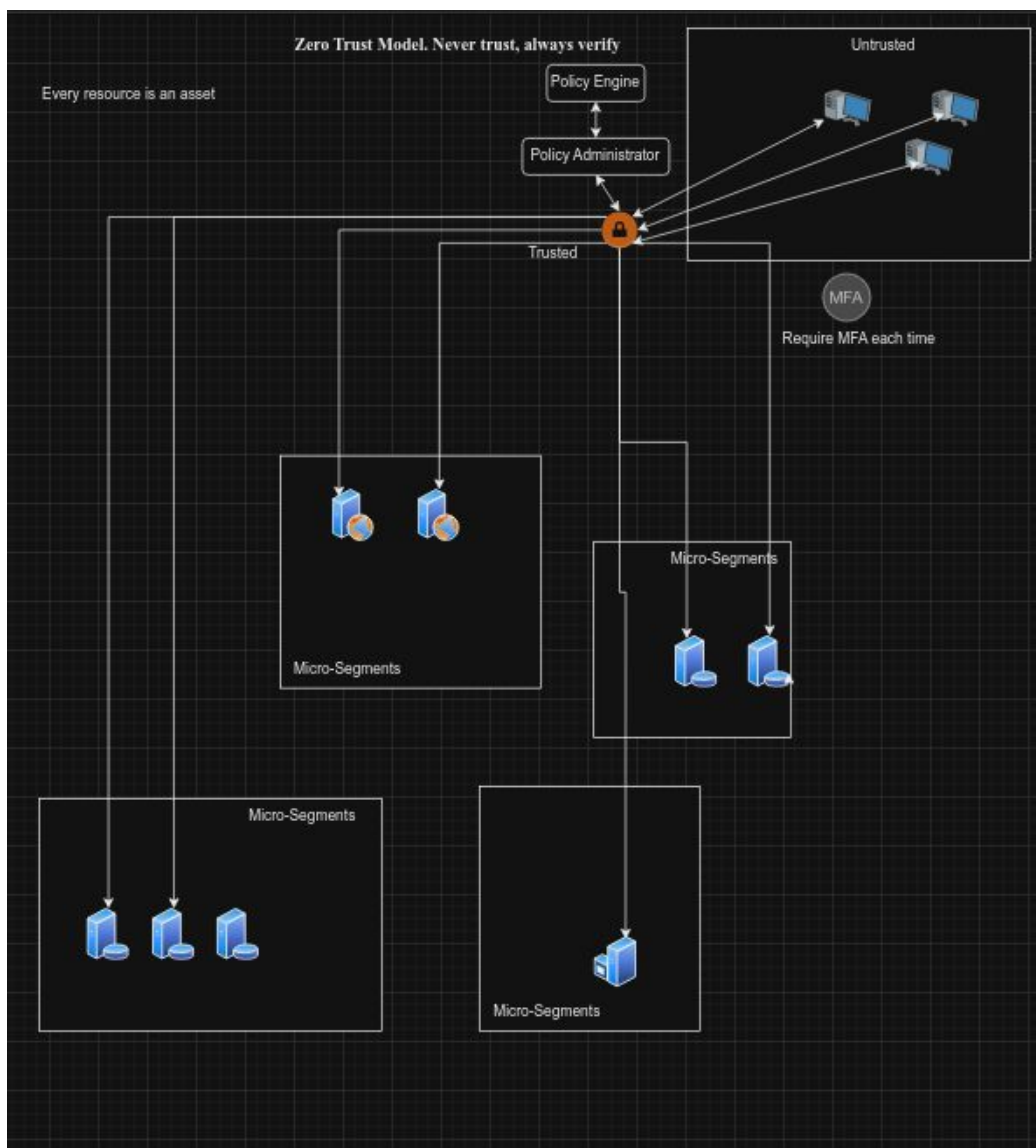
- Hold a meeting to discuss incident details
- Can we improve anything to prevent future attacks?
- Log incident details and threat actor information.



# **Section 4**

## **Designing a Zero Trust Model**

# 4.1 Zero Trust Model



## 4.2 Modern Architecture vs. Zero Trust

	Zero Trust	Secure Network
Core Philosophy	Assumes no trust within the network. Every user and device, regardless of origin (internal or external), must be continuously authenticated and authorized before granting access to resources.	Relies on a perimeter-based approach. It establishes strong security controls around the network's edge (firewalls, intrusion detection systems) to create a trusted internal zone. Once inside, users and devices generally have more relaxed access controls.
Access Control	Enforces granular access control. Users and devices are granted only the minimum privileges required to perform their specific tasks. Access is constantly monitored and can be revoked dynamically based on changing circumstances.	Relies on role-based access control (RBAC). Users are assigned roles with predefined permissions, granting access to specific resources within the trusted zone.
Network Segmentation	Leverages micro-segmentation to further isolate resources and limit lateral movement within the network. Even authorized users may only access specific segments relevant to their tasks.	Typically less granular and focuses on isolating specific network sections (e.g., DMZ) rather than individual resources.
Focus	Prioritizes continuous verification and least privilege access. It assumes breaches can occur and focuses on minimizing damage by limiting access to compromised resources.	Emphasizes preventing unauthorized access at the network perimeter. It aims to create a secure internal zone where traditional access controls can be relaxed.
Scalability	Scales well for dynamic and cloud-based environments. The focus on micro-permissions and least privilege simplifies access management for distributed resources.	Complex as the network grows or adopts cloud services. Managing access control lists for a large user base at the perimeter can be cumbersome.
Implementation	Complex to implement and requires a cultural shift within organizations accustomed to traditional perimeter security.	More established model with readily available security tools and technologies. Implementation is generally easier but may require upgrades to existing infrastructure.