

# **Project: Securing the Perimeter**

## **Directions and Submission Template**

*Roylan Pais*

*17-04-2024*



## **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:**

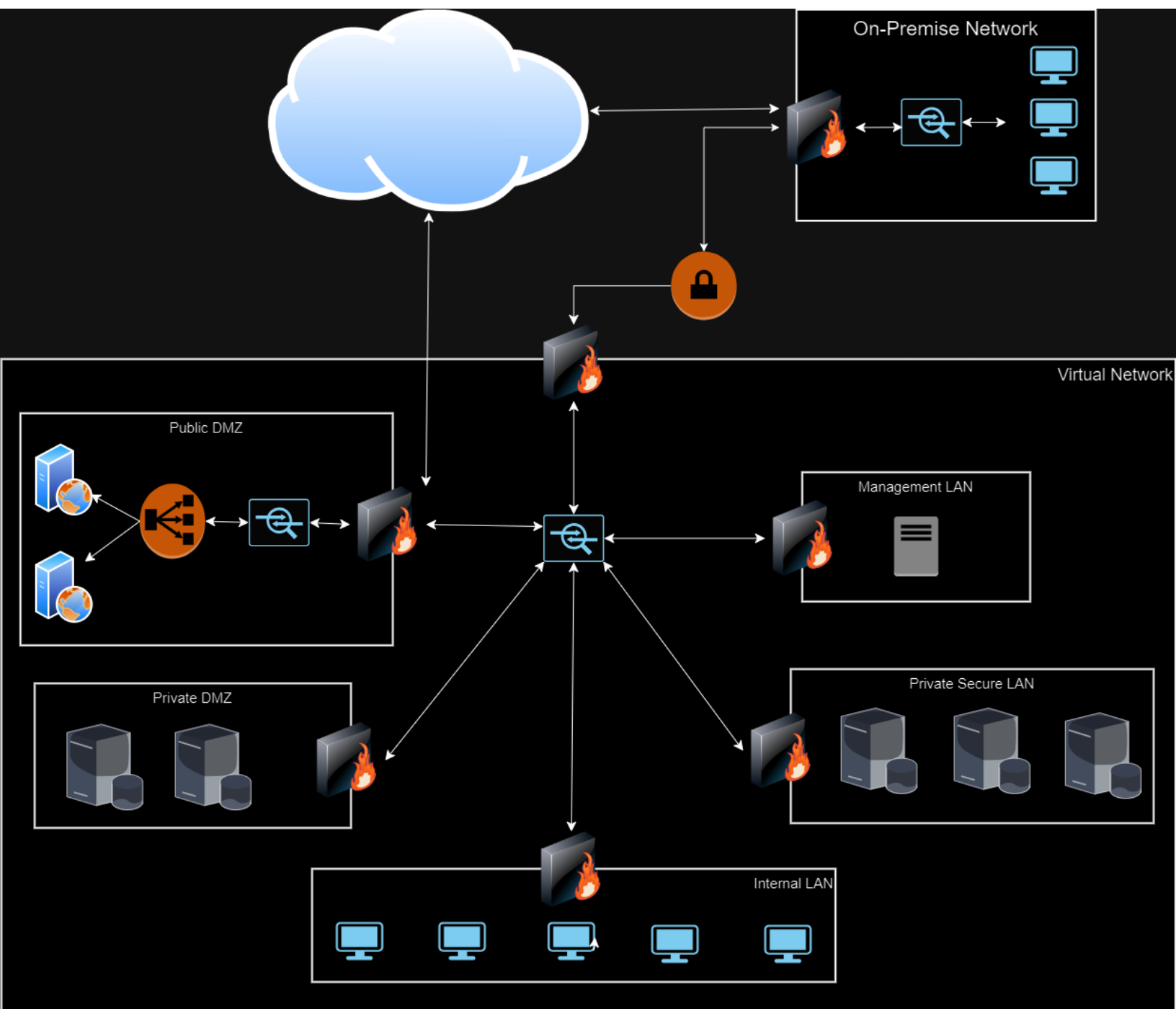
- 1) An on-premise network that has 3 workstations in it.
- 2) A Virtual Network with the following segments:
  - Public DMZ with two web servers and a load balancer in it.
  - Private DMZ with two database servers.
  - Management LAN with one management server in it.
  - Internal LAN with 5 workstations 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 to 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.

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.

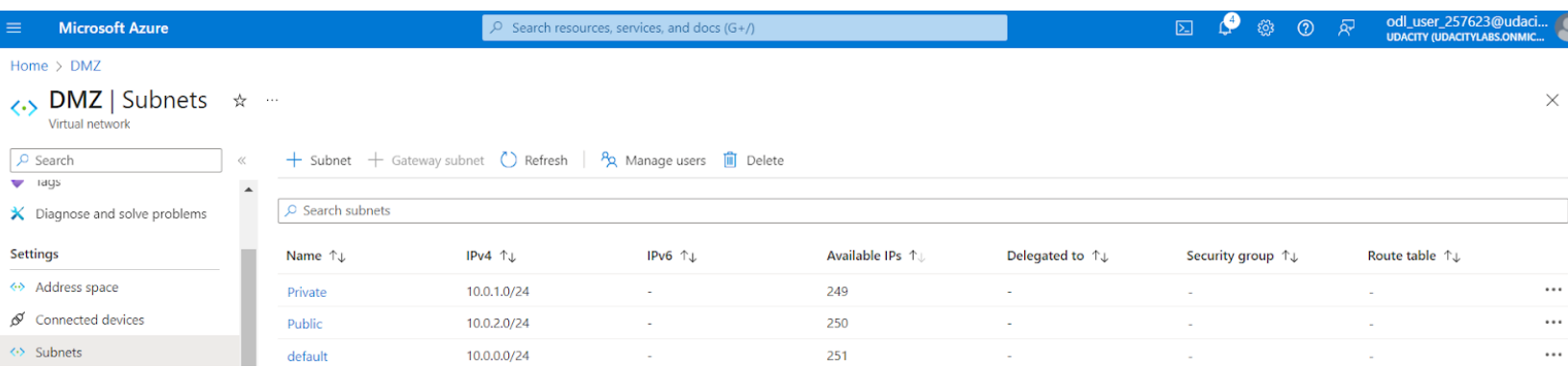
No grouping

List view

<input type="checkbox"/> Name ↑↓	Resource group ↑↓	Subscription ↑↓	Resource group ID ↑↓
<input type="checkbox"/> <=> DMZ	entp-project-257623	Udacity CloudLabs Sub - ...	/subscriptions/2698271c-... **
<input type="checkbox"/> <=> Internal	entp-project-257623	Udacity CloudLabs Sub - ...	/subscriptions/2698271c-... **

# 2.1.2 Screenshot

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





# 2.1.3 Screenshot

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

Microsoft Azure

Search resources, services, and docs (G+)

odl\_user\_257623@udaci...  
UDACITY (UDACITYLABS.ONMIC...

Home > Virtual networks > Internal

Virtual networks

Udacity (udacitylabs.onmicrosoft.com)

+ Create

Manage view

Filter for any field...

Name

DMZ

Internal

Internal | 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

Search subnets

Name	IPv4	IPv6	Available IPs	Delegated to	Security group	Route table
default	10.0.0.0/24	-	248	-	-	-
Management	10.0.1.0/24	-	251	-	-	-
Secure	10.0.2.0/24	-	251	-	-	-
Enterprise	10.0.3.0/24	-	251	-	-	-

<

Page 1 of 1

>

Give feedback

## 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.

The screenshot displays two Azure Virtual Machine (VM) instances side-by-side. Both VMs are named 'public-dmz-vm' and 'private-dmz-vm' respectively, and are running Linux (ubuntu 20.04) on Standard B1s hardware. The 'public-dmz-vm' is connected to the 'DMZ/public' virtual network, while the 'private-dmz-vm' is connected to the 'DMZ/private' virtual network. Both VMs have a public IP address of 172.206.210.164. The 'private-dmz-vm' has a DNS name of 'Not configured'. The 'public-dmz-vm' has a DNS name of 'Not configured'. The 'private-dmz-vm' has a DNS name of 'Not configured'. The 'public-dmz-vm' has a health state of 'Running', while the 'private-dmz-vm' has a health state of 'Not running'.

**public-dmz-vm** Virtual machine

Search

Connect Start Restart Stop Hibernate (preview) Capture Delete Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Connect

Bastion

Networking

Network settings

Essentials

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 [172.206.210.164](#)

Virtual network/subnet [DMZ/public](#)

DNS name [Not configured](#)

Health state -

JSON View

**private-dmz-vm** Virtual machine

Search

Connect Start Restart Stop Hibernate (preview) Capture Delete Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Connect

Bastion

Networking

Essentials

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 [DMZ/private](#)

DNS name -

Health state -

JSON View

## 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.

The screenshot shows the Azure portal interface for a virtual machine named 'secure-internal-vm'. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, and Networking. The main content area is divided into two columns. The left column, titled 'Essentials', displays key information: Resource group (entp-project-257837), Status (Running), Location (East US), Subscription (Udacity CloudLabs Sub - 45), and Subscription ID (56a26d77-4700-433d-90e1-e1ce4f1ff403). The right column displays additional details: Operating system (Linux (ubuntu 20.04)), Size (Standard B1s (1 vcpu, 1 GiB memory)), Public IP address (none), Virtual network/subnet (Internal/secure), DNS name (none), and Health state (OK). A 'JSON View' link is visible in the top right corner of the main content area.

The screenshot shows the Azure portal interface for a virtual machine named 'enterprise-internal-vm'. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, and Networking. The main content area is divided into two columns. The left column, titled 'Essentials', displays key information: Resource group (entp-project-257837), Status (Running), Location (East US), Subscription (Udacity CloudLabs Sub - 45), and Subscription ID (56a26d77-4700-433d-90e1-e1ce4f1ff403). The right column displays additional details: Operating system (Linux (ubuntu 20.04)), Size (Standard B1s (1 vcpu, 1 GiB memory)), Public IP address (none), Virtual network/subnet (Internal/enterprise), DNS name (none), and Health state (OK). A 'JSON View' link is visible in the top right corner of the main content area.

The screenshot shows the Azure portal interface for a virtual machine named 'management-internal-vm'. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, and Networking. The main content area is divided into two columns. The left column, titled 'Essentials', displays key information: Resource group (entp-project-257837), Status (Running), Location (East US), Subscription (Udacity CloudLabs Sub - 45), and Subscription ID (56a26d77-4700-433d-90e1-e1ce4f1ff403). The right column displays additional details: Operating system (Linux (ubuntu 20.04)), Size (Standard B1s (1 vcpu, 1 GiB memory)), Public IP address (none), Virtual network/subnet (Internal/management), DNS name (none), and Health state (OK). A 'JSON View' link is visible in the top right corner of the main content area.

## 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.

The screenshot displays the Azure portal interface for a Network Security Group (NSG) named 'PrivateDMZ-VM1-nsg'. The left sidebar shows the navigation menu with options like 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, and Automation. The main content area shows the 'Essentials' section with details about the resource group, location, subscription, and tags. Below this, there are filters for 'Filter by name' and buttons for 'Port == all', 'Protocol == all', 'Source == all', 'Destination == all', and 'Action == all'. The table below lists the security rules, categorized into Inbound Security Rules and Outbound Security Rules.

Priority	Name	Port	Protocol	Source	Destination	Action
1000	default-allow-ssh	22	TCP	172.16.1.0/24	VirtualNetwork	Allow
1500	DenyAnyCustomAn...	Any	Any	Any	VirtualNetwork	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancer...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

The screenshot displays the Azure portal interface for a Network Security Group (NSG) named 'public-dmz-nsg | Inbound security rules'. The left sidebar shows the navigation menu with options like 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, and Automation. The main content area shows the 'Inbound security rules' section with a description of how security rules are evaluated. Below this, there are filters for 'Filter by name' and buttons for 'Port == all', 'Protocol == all', 'Source == all', 'Destination == all', and 'Action == all'. The table below lists the security rules.

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	VirtualNetwork
1020	AllowAnyHTTPSInbound	443	TCP	Any	VirtualNetwork
1500	DenyAnyCustomA...	Any	Any	Any	VirtualNetwork
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancer...	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

# 2.3.2 Screenshot

## Traffic rules in your Internal network.

Home > Network security groups >

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

Create

Manage view

Filter for any field...

Name ↑

ELK-VM-nsg

EnterpriseInternal-VM1-nsg

ManagementInternal-VM1-nsg

PrivateDMZ-VM1-nsg

PublicDMZ-VM1-nsg

SecureInternal-VM1-nsg

Page 1 of 1

EnterpriseInternal-VM1-nsg

Network security group

Search

Move Delete Refresh 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

Essentials

Resource group (move) : entp-project-257623

Location : East US 2

Subscription (move) : Udacity CloudLabs Sub - 28

Subscription ID : 2698271c-1c0f-4e7e-ac71-2e53bd3348ea

Tags (edit) : Add tags

Custom security rules : 2 inbound, 0 outbound

Associated with : 0 subnets, 1 network interfaces

Filter by name

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

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
Inbound Security Rules						
1000	default-allow-ssh	22	TCP	172.16.1.0/24	Any	Allow
1500	DenyAnyInbound	Any	Any	Any	VirtualNetwork	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancer...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

ManagementInternal-VM1-nsg

Network security group

Search

Move Delete Refresh 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

Essentials

Resource group (move) : entp-project-257623

Location : East US 2

Subscription (move) : Udacity CloudLabs Sub - 28

Subscription ID : 2698271c-1c0f-4e7e-ac71-2e53bd3348ea

Tags (edit) : Add tags

Custom security rules : 2 inbound, 0 outbound

Associated with : 0 subnets, 1 network interfaces

Filter by name

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

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
Inbound Security Rules						
1000	AllowSSHInbound	22	TCP	172.16.1.0/24	VirtualNetwork	Allow
1500	DenyAnyCustomAn...	Any	Any	Any	VirtualNetwork	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancer...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

SecureInternal-VM1-nsg

Network security group

Search

Move Delete Refresh 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

Essentials

Resource group (move) : entp-project-257623

Location : East US 2

Subscription (move) : Udacity CloudLabs Sub - 28

Subscription ID : 2698271c-1c0f-4e7e-ac71-2e53bd3348ea

Tags (edit) : Add tags

Custom security rules : 2 inbound, 0 outbound

Associated with : 0 subnets, 1 network interfaces

Filter by name

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

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
Inbound Security Rules						
1000	default-allow-ssh	22	TCP	172.16.1.0/24	Any	Allow
1500	DenyAnyInbound	Any	Any	Any	VirtualNetwork	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancer...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	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.

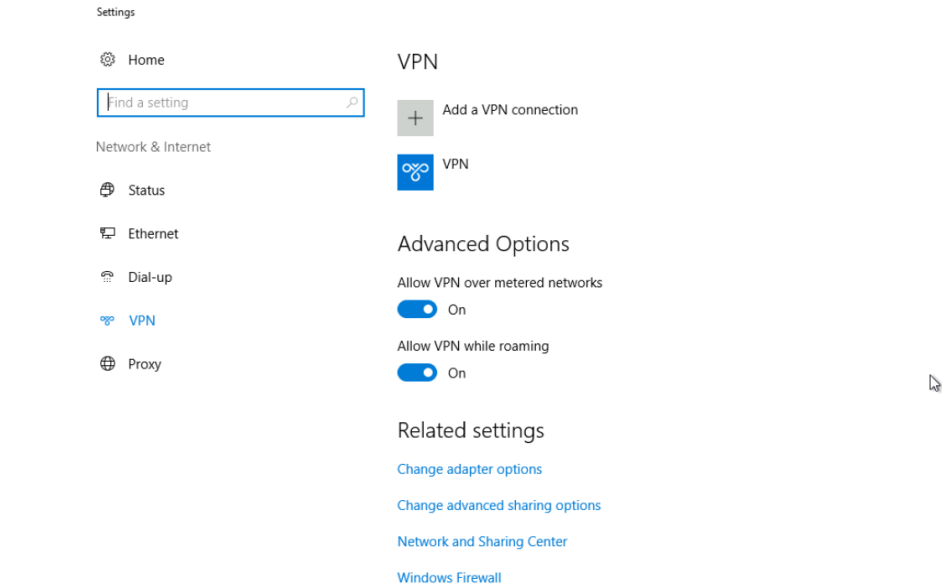
```
PS C:\Windows\system32> $cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature
-Subject "CN=AzureRootCert" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" `
-KeyUsageProperty Sign -KeyUsage CertSign

PS C:\Windows\system32> New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `
-Subject "CN=AzureClientCert" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" `
-Signer $cert -TextExtension @"(2.5.29.37={text}1.3.6.1.5.5.7.3.2)"

PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

Thumbprint                               Subject
-----
704C796A43061CE1DF6B57E479C2269D58178BBD CN=AzureClientCert

PS C:\Windows\system32>
```



## Virtual network ga...

Udacity (udacitylabs.onmicrosoft.com)

+ Create Manage view ...

Filter for any field...

Name ↑

VPN

## VPN | Point-to-site configuration

Virtual network gateway

Search Save Discard Delete Download VPN client

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

### Settings

- Configuration
- Connections
- Point-to-site configuration
- Properties
- Locks

Address pool \*  
172.16.1.0/24

Tunnel type  
IKEv2

Authentication type  
Azure certificate

### Root certificates

Name	Public certificate data
AzureRootCertificate	MIIC6zCCAdOgAwIBAgIQQC5BZXrl+69KBqVbmUW...

## 2.4.2 Screenshot

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

```
azureuser@enterprise-internal-vm: ~
C:\Users\Udacity-Student>ssh azureuser@10.0.3.4
The authenticity of host '10.0.3.4 (10.0.3.4)' can't be established.
ED25519 key fingerprint is SHA256:gNKgiJXHen0VwOvalnFlzL2IlhBrHWyEletGuD8L94.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.3.4' (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 15:05:16 UTC 2024

System load:  0.08               Processes:            101
Usage of /:   5.0% of 28.89GB    Users logged in:     0
Memory usage: 31%               IPv4 address for eth0: 10.0.3.4
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@enterprise-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.

Home > Virtual machines >

## Virtual machines

Udacity (udacitylabs.onmicrosoft.com)

+ Create ▾ ↺ Switch to classic ...

Filter for any field...

Name ↑↓

- ELK-VM ...
- enterprise-internal-vm ...
- management-internal-vm ...
- private-dmz-vm ...
- public-dmz-vm ...
- secure-internal-vm ...

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Connect

- Connect
- Bastion

Networking

- Network settings
- Load balancing
- Application security groups
- Network manager

ELK-VM Virtual machine

Search

Connect ▾ ▶ Start ↺ Restart □ Stop ⌚ Hibernate (preview) 📷 Capture 🗑 Delete ↻ Refresh ...

### Essentials

[JSON View](#)

Resource group <a href="#">(move)</a> <a href="#">entp-project-257837</a>	Operating system Linux (ubuntu 20.04)
Status Running	Size Standard DS1 v2 (1 vcpu, 3.5 GiB memory)
Location East US	Public IP address -
Subscription <a href="#">(move)</a> <a href="#">Udacity Cloudlabs Sub - 45</a>	Virtual network/subnet <a href="#">DMZ/private</a>
Subscription ID 56a26d77-4700-433d-90e1-e1ce4f1ff403	DNS name -
	Health state -

Tags [\(edit\)](#)  
[Add tags](#)

Properties Monitoring Capabilities (7) Recommendations Tutorials

Virtual machine Networking

# 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+/I)

odl\_user\_257967@udac...  
UDACITY

Home > ELK

ELK | Network settings

Virtual machine

Search

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

This is a new experience. [Please provide feedback](#)

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

Create port rule

Search rules

Source == all

Destination == all

Protocol == all

Action == all

Priority ↑	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (7)						
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.

```
azureuser@private-dmz-vm:/etc/filebeat$ sudo systemctl status filebeat
● 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; 54min 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.hor

Apr 17 18:34:01 private-dmz-vm filebeat[15385]: 2024-04-17T18:34:01.087Z          INFO          [mon
Apr 17 18:34:31 private-dmz-vm filebeat[15385]: 2024-04-17T18:34:31.086Z          INFO          [mon
Apr 17 18:35:01 private-dmz-vm filebeat[15385]: 2024-04-17T18:35:01.086Z          INFO          [mon
Apr 17 18:35:31 private-dmz-vm filebeat[15385]: 2024-04-17T18:35:31.087Z          INFO          [mon
Apr 17 18:35:44 private-dmz-vm filebeat[15385]: 2024-04-17T18:35:44.416Z          INFO          log.
Apr 17 18:36:01 private-dmz-vm filebeat[15385]: 2024-04-17T18:36:01.087Z          INFO          [mon
Apr 17 18:36:31 private-dmz-vm filebeat[15385]: 2024-04-17T18:36:31.086Z          INFO          [mon
Apr 17 18:37:01 private-dmz-vm filebeat[15385]: 2024-04-17T18:37:01.086Z          INFO          [mon
Apr 17 18:37:31 private-dmz-vm filebeat[15385]: 2024-04-17T18:37:31.086Z          INFO          [mon
Apr 17 18:38:01 private-dmz-vm filebeat[15385]: 2024-04-17T18:38:01.087Z          INFO          [mon
lines 1-20/20 (END)
```



## 3.2.2 Screenshot

Configure Filebeat to route web server logs to Elasticsearch.

```
#===== 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: ["10.0.1.4:9200"]

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

#===== 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: "10.0.1.4:5601"
  # 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: "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:
```

## 3.2.3 Screenshot

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



Launch the demo

×

We will send you 50 visits for free! Just fill the following form:

Website

Session Duration

Bounce Rate

Referrers

Countries



Which country should the visits come from?

World

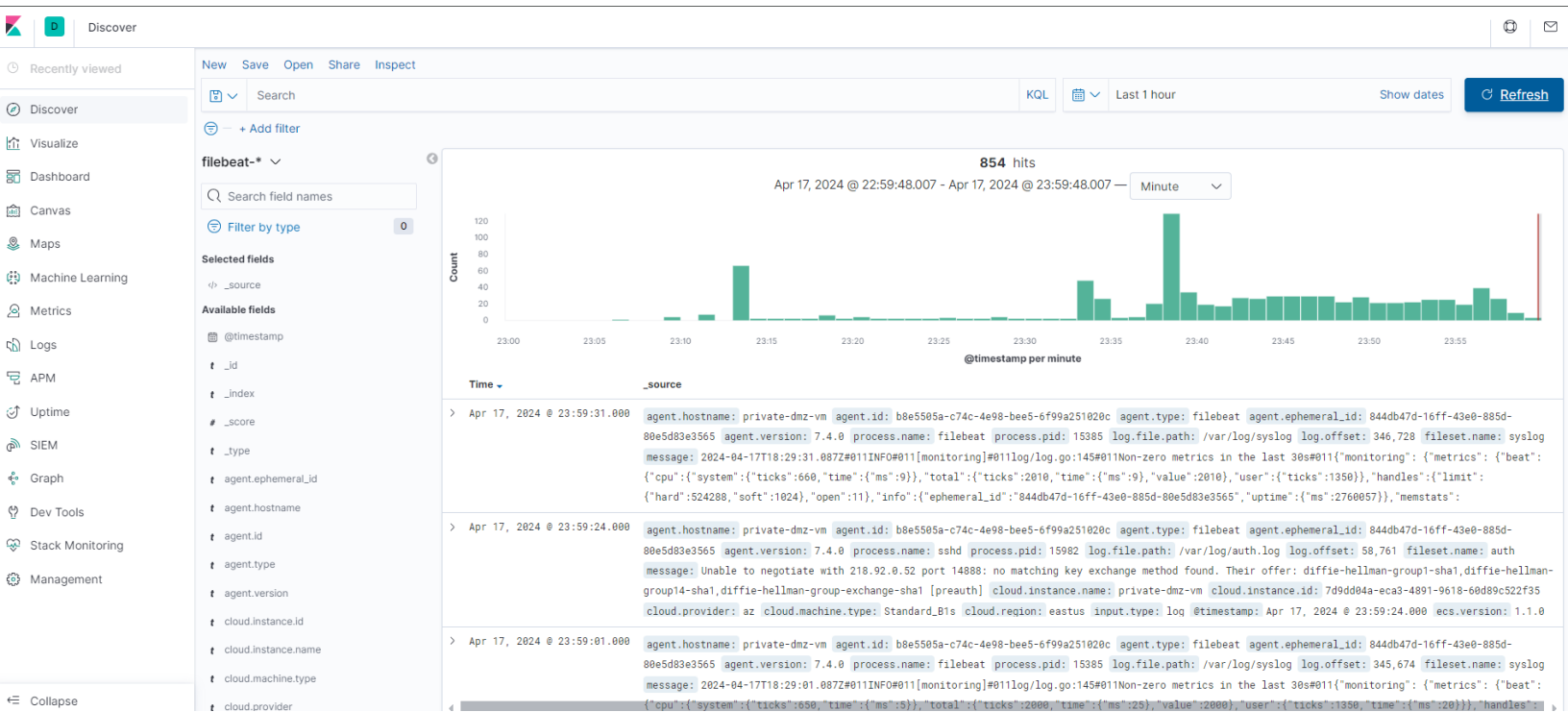
▼

Previous

Finish

# 3.2.4 Screenshot

Web server logs appear in Kibana.



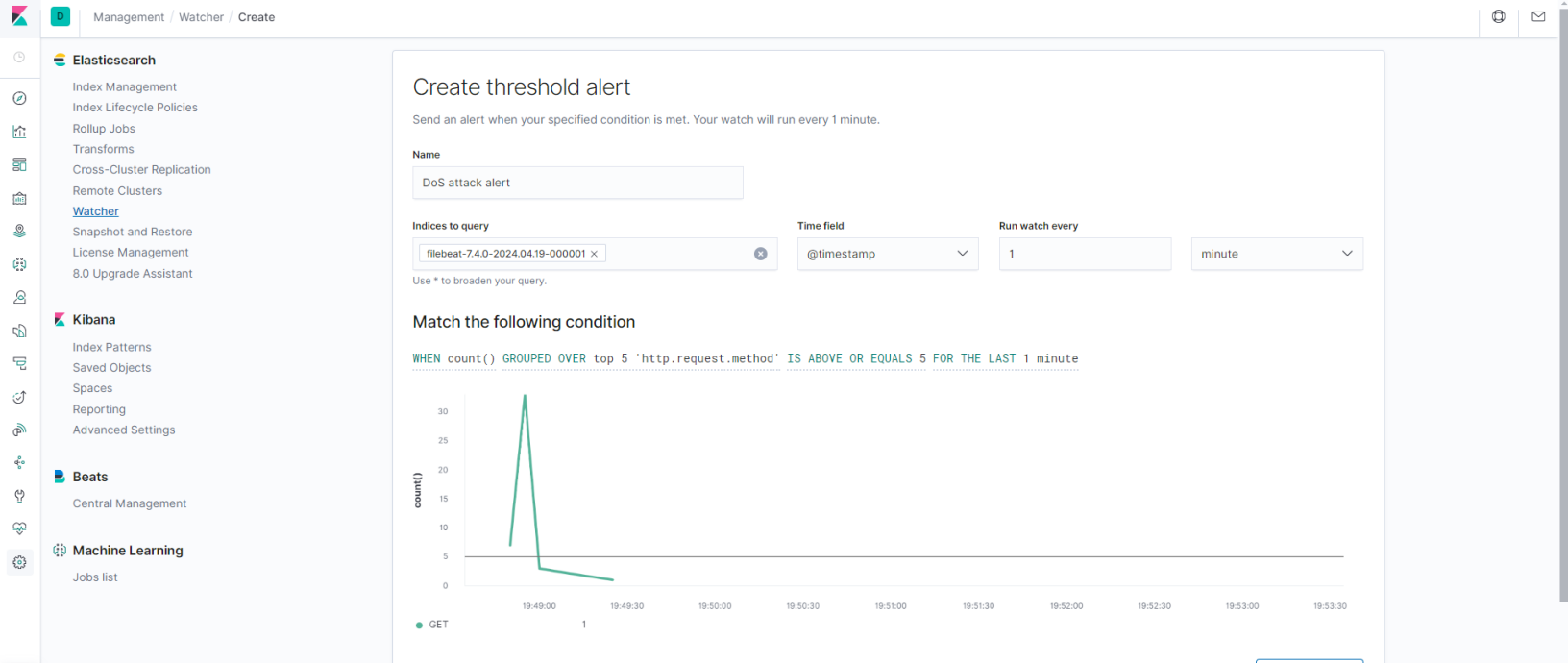
## 3.3 Build Alerts

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.



### Current status for 'DoS attack alert'

Deactiv

Execution history    Action statuses

Last one hour

Trigger time	State	Comment
2024-04-19T20:00:18+05:30	✓ OK	
2024-04-19T19:59:18+05:30	✓ OK	
2024-04-19T19:58:18+05:30	✓ OK	
2024-04-19T19:57:18+05:30	✓ OK	
2024-04-19T19:56:18+05:30	✓ OK	
2024-04-19T19:55:18+05:30	✓ OK	

Rows per page: 10

# 3.3.2 Screenshot

## Create an alert for Brute Force 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 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

Time field

@timestamp

Run watch every

1


minute

Use \* to broaden your query.

Match the following condition

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

count()



● failure

### Current status for 'Brute force alert'

Execution history    Action statuses

Last one hour

Trigger time	State	Comment
2024-04-19T20:01:11+05:30	✓ OK	
2024-04-19T20:00:11+05:30	✓ OK	
2024-04-19T19:59:11+05:30	✓ OK	
2024-04-19T19:58:11+05:30	✓ OK	
2024-04-19T19:57:11+05:30	✓ OK	
2024-04-19T19:56:11+05:30	✓ OK	
2024-04-19T19:55:11+05:30	✓ OK	
2024-04-19T19:54:11+05:30	✓ OK	
2024-04-19T19:53:11+05:30	✓ OK	
2024-04-19T19:52:11+05:30	✓ OK	
2024-04-19T19:51:11+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.

Management / Watcher / Create

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

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 x

Time field

@timestamp

Run watch every

1

minute

Use \* to broaden your query.

Match the following condition

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

No data

Your index and condition did not return any data.

Perform 0 actions when condition is met

Add action

Create alert

Cancel

Show request

## Current status for 'Scanning attack alert'

Execution history    Action statuses

Last one hour

Trigger time	State	Comment
2024-04-19T20:00:31+05:30	✓ OK	
2024-04-19T19:59:31+05:30	✓ OK	
2024-04-19T19:58:31+05:30	✓ OK	

Rows per page: 10

# 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.

## Brute Force Attack Playbook

### Preparation

- 1. Define Team and Roles:** Establish a team responsible for handling brute force attacks, including IT security, system administrators, and application owners. Assign clear roles for each phase (detection, analysis, containment, recovery).
- 2. SIEM systems:** Utilize security information and event management (SIEM) systems to correlate login attempts from various sources and identify potential brute force attacks.
- 3. Establish Communication Plan:** Define communication channels (email, chat) and escalation procedures for notifying stakeholders during an attack.
- 4. Identify Critical Accounts:** List accounts with high access privileges or access to sensitive data that are prime targets for brute force attacks.
- 5. Implement Strong Password Policies:** Enforce password complexity requirements (length, mix of characters) and enforce regular password changes for critical accounts.
- 6. Update security software:** Regularly update security software and firmware to address vulnerabilities that attackers might exploit to gain access through brute force attacks.
- 7. Account Lockout Thresholds:** Configure account lockout mechanisms after a predefined number of failed login attempts.
- 8. Monitor Login Attempts:** Implement tools to monitor login attempts, including origin IP addresses and timestamps. Establish baselines for regular login activity to identify anomalies.

### Detection & Analysis

- 1. Alert on Login Anomalies:** Set up alerts for unusual login activity, such as:
  1. High number of failed login attempts from a single IP address in a short period.
  2. Login attempts from unexpected geographical locations.
  3. Attempts to access privileged accounts outside of regular working hours.
- 2. Analyze Login Attempts:** Investigate suspicious login activities. Analyse IP addresses for malicious origin using threat intelligence feeds.

### Containment, Eradication & Recovery

- 1. Lock Out Accounts:** Automatically lock accounts after exceeding the predefined failed login threshold.
- 2. Implement IP Blocking:** Block IP addresses identified as sources of brute force attacks. Consider implementing temporary blocks with the option to unblock after a specific timeframe.
- 3. MFA for Critical Accounts:** Enable multi-factor authentication (MFA) for privileged accounts and accounts with access to sensitive data.
- 4. Investigate Compromised Credentials:** If a brute force attack is successful, assume the compromised account's credentials are leaked. Reset passwords for compromised accounts and potentially related accounts.
- 5. Identify Root Cause:** If a vulnerability is exploited to facilitate the brute force attack, patch the vulnerability to prevent future attacks.

### Post-Incident Activity

- 1. Document the Incident:** Document the details of the attack, including the timeline of events, attack source (if identified), containment actions taken, and lessons learned.
  - 2. Review and Improve:** Conduct a post-incident review to assess the response's effectiveness and identify areas for improvement. This may involve adjusting lockout thresholds, MFA implementation, or communication protocols.
- Security Awareness Training:** Train users on strong password practices and how to identify phishing attempts that could lead to credential theft used in brute force attacks.



# DoS Attack Playbook

## Preparation

- 1. Define team and roles:** Identify the team members responsible for DoS incident response, including IT security, network operations, and business continuity personnel. Assign clear roles and responsibilities for each phase. Train the team on DoS attack tactics, mitigation strategies, and the incident response playbook.
- 2. Establish a communication plan:** Determine how the team will communicate during a DoS attack. This includes defining communication channels, escalation procedures, and protocols for notifying stakeholders.
- 3. Identify critical assets:** List the essential systems and resources that must be protected from DoS attacks. This will help prioritize response efforts during an incident.
- 4. Update security software:** Regularly update security software and firmware to address vulnerabilities that attackers might exploit in DoS attacks.
- 5. Baseline network traffic:** Monitor and establish baseline metrics for network traffic patterns to identify anomalies that might indicate a DoS attack.
- 6. Implement DoS mitigation strategies:** Configure firewalls, intrusion detection/prevention systems (IDS/IPS), and web application firewalls (WAFs) to detect and block DoS attacks. Consider implementing DDoS mitigation services offered by cloud providers or security vendors.
- 7. Prepare for recovery:** Develop a plan for restoring affected systems and services after a DoS attack. This includes having backups readily available and practicing recovery procedures.
- 8. Automation:** Incorporating automation tools to streamline detection, analysis, and mitigation of DoS attacks.

## Detection & Analysis

- 1. Monitor for signs of DoS attacks:** Monitor network traffic, system resource utilization, and application logs for unusual activity that might indicate a DoS attack. Utilize the baselines established during preparation for anomaly detection.
- 2. Alert and escalate:** If a potential DoS attack is detected, trigger alerts and escalate the incident to the designated response team members according to the communication plan.
- 3. Analyze attack characteristics:** Identify the type of DoS attack (volumetric, protocol, application layer) and gather information about the attack source and target.

## Containment, Eradication, and Recovery

- 1. Isolate the attack:** Isolate the target system or network segment from the DoS attack traffic. This may involve implementing rate limiting, blackholing malicious IP addresses, or utilizing DDoS mitigation service features.
- 2. Protect critical resources:** Ensure essential systems and resources remain available during the attack. This may involve scaling resources or diverting traffic to alternate systems.
- 3. Eradicate the attack (if possible):** If the attack source can be identified and isolated, stop the attack at its origin. This may involve working with law enforcement or internet service providers.
- 4. Recover affected systems:** Restore affected systems and services using backups and recovery procedures established during the preparation phase.

## Post-Incident Activity

- 1. Document the incident:** Document all activities taken during the DoS incident response. This includes the timeline of events, attack details, mitigation strategies employed, and lessons learned.
- 2. Review and improve:** Conduct a post-incident review to assess the response plan's effectiveness and identify improvement areas. This may involve updating the playbook, strengthening DoS mitigation strategies, or improving communication protocols.
- 3. Test the playbook:** Regularly test the DoS incident response playbook through simulations or exercises to ensure team members are familiar with their roles and procedures.

# Scanning Attack Playbook

## Preparation

- 1. Define Team and Roles:** Establish a team responsible for handling brute force attacks, including IT security, system administrators, and application owners. Assign clear roles for each phase (detection, analysis, containment, recovery).
- 2. SIEM systems:** Utilize security information and event management (SIEM) systems to correlate login attempts from various sources and identify potential brute force attacks.
- 3. Establish a Communication Plan:** Define communication channels (email, chat) and escalation procedures for notifying stakeholders during an attack.
- 4. Identify Critical Accounts:** List accounts with high access privileges or access to sensitive data that are prime targets for brute force attacks.
- 5. Implement Strong Password Policies:** Enforce password complexity requirements (length, mix of characters) and enforce regular password changes for critical accounts.
- 6. Update security software:** Regularly update security software and firmware to address vulnerabilities that attackers might exploit to gain access through brute force attacks.
- 7. Account Lockout Thresholds:** Configure account lockout mechanisms after a predefined number of failed login attempts.
- 8. Monitor Login Attempts:** Implement tools to monitor login attempts, including origin IP addresses and timestamps. Establish baselines for regular login activity to identify anomalies.

## Detection & Analysis

- 1. Alert on Login Anomalies:** Set up alerts for unusual login activity, such as:
  1. High number of failed login attempts from a single IP address in a short period.
  2. Login attempts from unexpected geographical locations.
  3. Attempts to access privileged accounts outside of regular working hours.
- 2. Analyze Login Attempts:** Investigate suspicious login activities. Analyze IP addresses for malicious origin using threat intelligence feeds.

## Containment, Eradication & Recovery

- 1. Lock Out Accounts:** Automatically lock accounts after exceeding the predefined failed login threshold.
- 2. Implement IP Blocking:** Block IP addresses identified as sources of brute force attacks. Consider implementing temporary blocks with the option to unblock after a specific timeframe.
- 3. MFA for Critical Accounts:** Enable multi-factor authentication (MFA) for privileged accounts and accounts with access to sensitive data.
- 4. Investigate Compromised Credentials:** If a brute force attack is successful, assume the compromised account's credentials are leaked. Reset passwords for compromised accounts and potentially related accounts.
- 5. Identify Root Cause (if possible):** If a vulnerability is exploited to facilitate the brute force attack, patch the vulnerability to prevent future attacks.

## Post-Incident Activity

- 1. Document the Incident:** Document the details of the attack, including the timeline of events, attack source (if identified), containment actions taken, and lessons learned.
  - 2. Review and Improve:** Conduct a post-incident review to assess the response's effectiveness and identify areas for improvement. This may involve adjusting lockout thresholds, MFA implementation, or communication protocols.
- Security Awareness Training:** Train users on strong password practices and how to identify phishing attempts that could lead to credential theft used in brute force attacks.



# **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.**

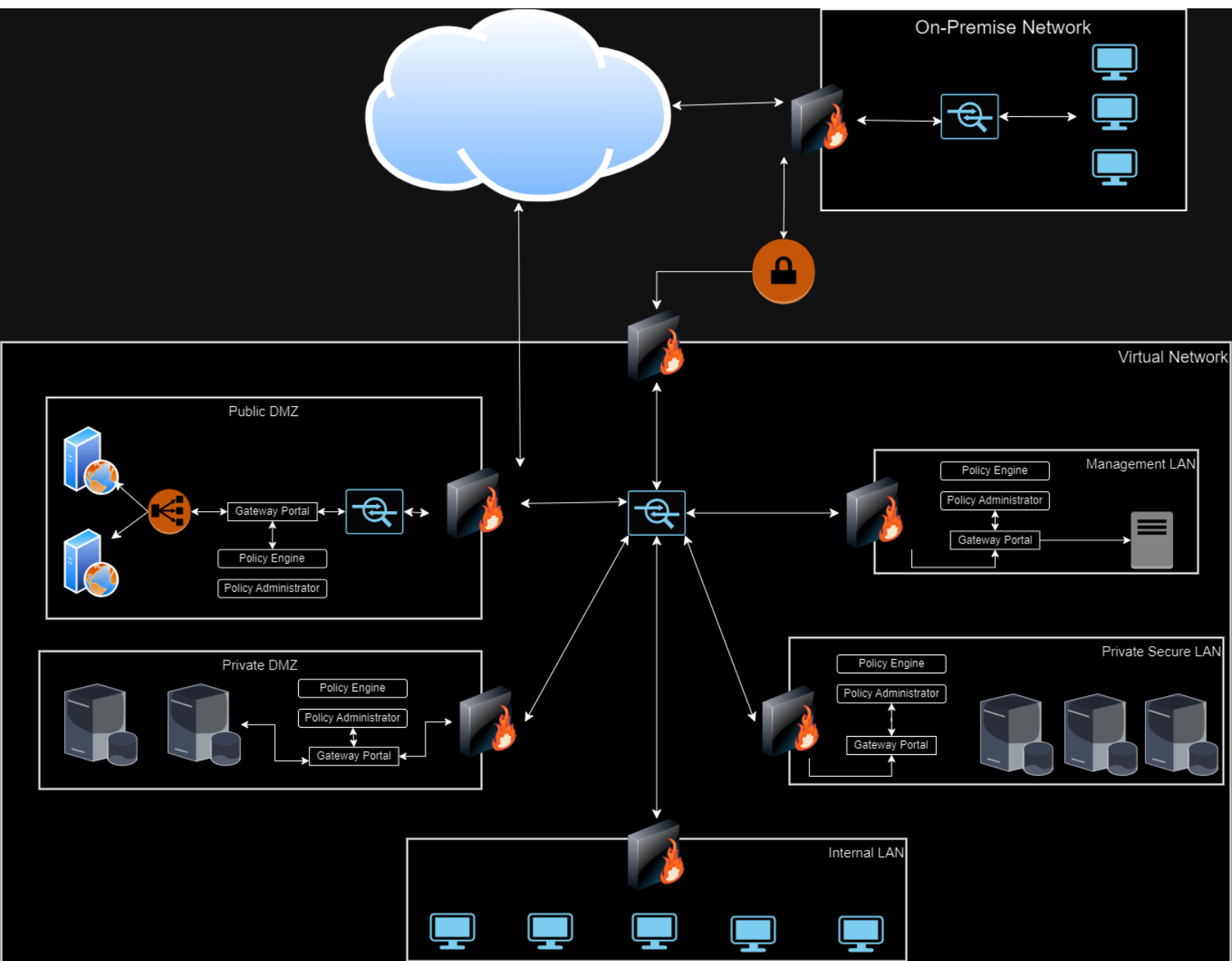
Design a Zero Trust model of your network architecture using <https://app.diagrams.net/>.

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.

## 1. Trust Assumption:

- Traditional: Trust is established once inside the network.
- Zero Trust: Trust is never assumed; verification is required for every access request.

## 2. Network Segmentation:

- Traditional: Basic segmentation with less strict access controls.
- Zero Trust: Extensive micro-segmentation with strict access controls throughout the network.

## 3. Device Trust:

- Traditional: Trust in company-managed devices.
- Zero Trust: All devices are treated as potentially hostile, with continuous security posture assessment.

## 4. Identity and Access Management:

- Traditional: Less stringent user identity verification.
- Zero Trust: Strong Identity and Access management controls.

## 5. Data Protection:

- Traditional: Data security focused on perimeter defence.
- Zero Trust: Data encryption throughout the network, tightly controlled access based on roles.

## 6. Application Security:

- Traditional: Implicit trust in internal applications.
- Zero Trust: Applications must authenticate, with continuous monitoring and access based on user identity.

## 7. Infrastructure Management:

- Traditional: Centralized management with limited micro-segmentation.
- Zero Trust: Infrastructure managed as code for consistent, secure deployments and enhanced visibility.

## 8. Continuous Authentication:

- Zero Trust emphasizes continuous authentication and authorization for all users and devices.

## 9. Granular Access Controls:

- Zero Trust enforces strict access controls at a granular level, not just at the perimeter.

## 10. Dynamic Access Controls:

- Zero Trust implements dynamic access controls that adjust permissions based on the access request context.