

Project: Securing the Perimeter

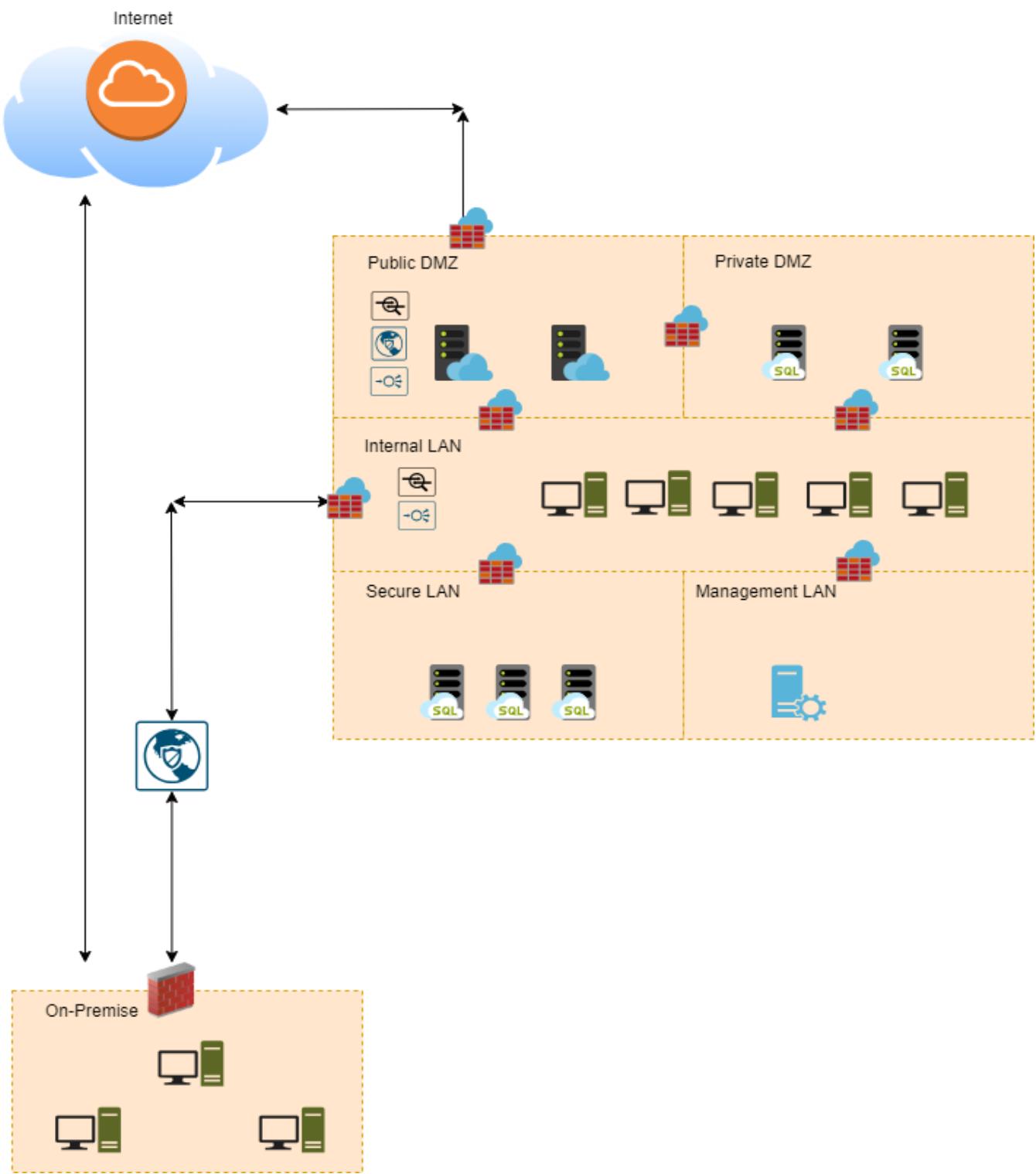
Yaser Issa Ahmed

04/21/2024

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.

The screenshot shows the Microsoft Azure portal interface for managing Virtual Networks. The browser address bar indicates the URL is <https://portal.azure.com/#view/HubsExtension>. The main content area displays a list of Virtual Networks under the heading "Virtual networks". There are two entries visible:

Name	Resource Group	Location	Subscription
DMZ	entp-project-258070	East US	Udacity CloudLabs Sub...
Internal	entp-project-258070	West Europe	Udacity CloudLabs Sub...

A blue callout box is overlaid on the "Create" button, containing the text: "Save the current columns, sorting, filtering and summary as a view and access your saved views here." Below this, there are buttons for "NEXT", "group ↑", "Location ↑", and "Subscription ↑". The bottom of the screen shows the Windows taskbar with various icons and the system tray indicating the date and time as 10:07 AM on 4/21/2024.

2.1.2 Screenshot

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

The screenshot shows the Microsoft Azure portal interface for managing a virtual network named 'DMZ'. The left sidebar navigation includes options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Address space, Connected devices, Subnets (which is currently selected), Bastion, DDoS protection, Firewall, Microsoft Defender for Cloud, and Network manager. The main content area displays a table of subnets with columns for Name, IPv4, IPv6, and Available. A success message box is visible, stating 'Successfully added subnet' and 'Successfully added subnet 'public' to virtual network 'DMZ''. The table data is as follows:

Name	IPv4	IPv6	Available
default	10.0.0.0/24	-	251
private	10.0.1.0/24	-	251
public	10.0.2.0/24	-	251

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 URL in the address bar is <https://portal.azure.com/#@udacitylabs.onmicrosoft.com>. The main content area is titled "Internal | Subnets" under "Virtual network". On the left, there is a sidebar with various navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Address space, Connected devices, Subnets (which is currently selected and highlighted in grey), Bastion, DDoS protection, Firewall, Microsoft Defender for Cloud, and Network manager. The main pane shows a table of subnets:

Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available
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

At the bottom right of the main pane, there is a "Give feedback" link. The system tray at the bottom of the screen shows the date and time as 10:14 AM, 4/21/2024.

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 shows the Microsoft Azure portal interface. The left sidebar navigation includes Home, private-VM (Virtual machine), Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect (with options for Connect and Bastion), Networking (with Network settings, Load balancing, Application security groups, and Network manager), and Settings (with Disks). The main content area displays the 'private-VM' details. It shows the VM is running in the 'East US (Zone 1)' location, part of the 'entp-project-258168' resource group, and is connected to the 'Udacity CloudLabs Sub - 29' subscription. The VM size is 'Standard B1s (1 vcpu, 1 GiB memory)', with a public IP address of '74.235.108.32'. It is associated with the 'DMZ/private' virtual network subnet and has a DNS name of 'Not configured'. The health state is listed as '-'. A note at the top states: 'private-VM virtual machine agent status is not ready. Troubleshoot the issue →'. The bottom navigation bar includes Properties, Monitoring, Capabilities (7), Recommendations, and Tutorials. The URL in the browser is https://portal.azure.com/#/resource/subscriptions/entp-project-258168/resourceGroups/entp-project-258168/providers/Microsoft.Compute/virtualMachines/private-VM.

The screenshot shows the Microsoft Azure portal interface, similar to the previous one but for a different VM. The left sidebar navigation includes Home, public-VM (Virtual machine), Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect (with options for Connect and Bastion), Networking (with Network settings, Load balancing, Application security groups, and Network manager), and Settings (with Disks). The main content area displays the 'public-VM' details. It shows the VM is running in the 'East US (Zone 1)' location, part of the 'entp-project-258168' resource group, and is connected to the 'Udacity CloudLabs Sub - 29' subscription. The VM size is 'Standard B1s (1 vcpu, 1 GiB memory)', with a public IP address of '74.235.109.179'. It is associated with the 'DMZ/public' virtual network subnet and has a DNS name of 'Not configured'. The health state is listed as '-'. A note at the top states: 'public-VM virtual machine agent status is not ready. Troubleshoot the issue →'. The bottom navigation bar includes Properties, Monitoring, Capabilities (7), Recommendations, and Tutorials. The URL in the browser is https://portal.azure.com/#/resource/subscriptions/entp-project-258168/resourceGroups/entp-project-258168/providers/Microsoft.Compute/virtualMachines/public-VM.

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 Microsoft Azure portal interface with two tabs open: "Secure-VM - Microsoft Azure" and "Enterprise-VM - Microsoft Azure". Both tabs are viewing the "Overview" page for their respective VMs.

Secure-VM Overview:

- Essentials:**
 - Resource group: entp-project-258168
 - Status: Running
 - Location: East US (Zone 1)
 - Subscription: Udacity CloudLabs Sub - 29
 - Subscription ID: c4f47e86-cf48-4611-8c4d-6f6124a34a60
 - Availability zone: 1
 - Tags: Not configured
- Properties:** Computer name: Secure-VM
- Networking:** Public IP address: 74.235.107.11, Virtual network/subnet: Internal/Secure

Enterprise-VM Overview:

- Essentials:**
 - Resource group: entp-project-258168
 - Status: Running
 - Location: East US (Zone 1)
 - Subscription: Udacity CloudLabs Sub - 29
 - Subscription ID: c4f47e86-cf48-4611-8c4d-6f6124a34a60
 - Availability zone: 1
 - Tags: Not configured
- Properties:** Computer name: Enterprise-VM
- Networking:** Public IP address: 172.210.17.88, Virtual network/subnet: Internal/Enterprise

Both VMs are listed under the "Compute" section of the Azure portal navigation bar.

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 Microsoft Azure portal interface for managing a virtual machine. The main title bar includes tabs for 'Management-VM - Microsoft Azure' and 'CreateVm-canonical.0001-com-'. The browser address bar shows the URL <https://portal.azure.com/#@udacitylabs.onmicrosoft.com/resource/subscript...>. The top navigation bar has a search bar and user information for 'odl_user_258168@udaci...' and 'UDACITY (UDACITYLABSONMIC...)'.

The main content area displays the 'Management-VM' details:

- Overview:** Resource group ([move](#)) [entp-project-258168](#), Status: Running, Location: East US (Zone 1), Subscription ([move](#)) [Udacity CloudLabs Sub - 29](#), Subscription ID: c4f47e86-cf48-4611-8c4d-6f6124a34a60, Availability zone: 1.
- Properties:** Computer name: Management-VM.
- Networking:** Public IP address: [74.235.107.44](#), Virtual network/subnet: [Internal/Management](#).
- Tags:** Tags ([edit](#)) [Add tags](#).

Below the main content, there are tabs for Properties, Monitoring, Capabilities (7), Recommendations, and Tutorials. The status bar at the bottom shows the date and time: 4/22/2024 4:55 PM.

2.3.1 Screenshot

Traffic rules in your DMZ.

Microsoft NetworkSecurityGroup | DMZ-NSG - Microsoft Azure

Microsoft Azure | Search resources, services, and docs (G+)

Home > Network security groups > DMZ-NSG

DMZ-NSG | Inbound security rules

Network security group

Search | Add | Hide default rules | Refresh | Delete | Give feedback

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 ↑
<input type="checkbox"/> 100	public-DMZ	80	TCP	Any
<input type="checkbox"/> 110	Public-DMZ-https	443	TCP	Any
<input type="checkbox"/> 65000	AllowVnetInBound	Any	Any	VirtualNetwork
<input type="checkbox"/> 65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBal...
<input type="checkbox"/> 65500	DenyAllInBound	Any	Any	Any

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Alerts

Diagnostic settings

5:10 PM 4/22/2024

2.3.2 Screenshot

Traffic rules in your Internal network.

The screenshot shows the Microsoft Azure portal interface for managing Network Security Groups (NSGs). The current view is for the "Internal-NSG" NSG, specifically focusing on its inbound security rules.

Left Sidebar: The sidebar contains several sections: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (with "Inbound security rules" selected), Outbound security rules, Network interfaces, Subnets, Properties, Locks, Monitoring, Alerts, and Diagnostic settings.

Header: The header includes the Microsoft NetworkSecurityGroup tab, the Internal-NSG - Microsoft Azure tab, and a search bar for "my ip - Search". The URL is https://portal.azure.com/#@udacitylabs.onmicrosoft.com/resource/subscripti... . The browser tabs also show "Microsoft Azure" and "Search resources, services, and docs (G+/)". The user is od1_user_258168@udaci... UDACTY (UDACITYLABS.ONMIC...).

Main Content: The main area displays the "Internal-NSG | Inbound security rules" page. It features a search bar, a toolbar with "Add", "Hide default rules", "Refresh", "Delete", and "Give feedback" buttons, and a detailed description of how security rules are evaluated by priority. A "Learn more" link is provided for further information.

Table: A table lists the current inbound security rules:

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑
100	mysshaccess	22	TCP	13.87.206.67
65000	AllowVnetInBound	Any	Any	VirtualNetwor...
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBal...
65500	DenyAllInBound	Any	Any	Any

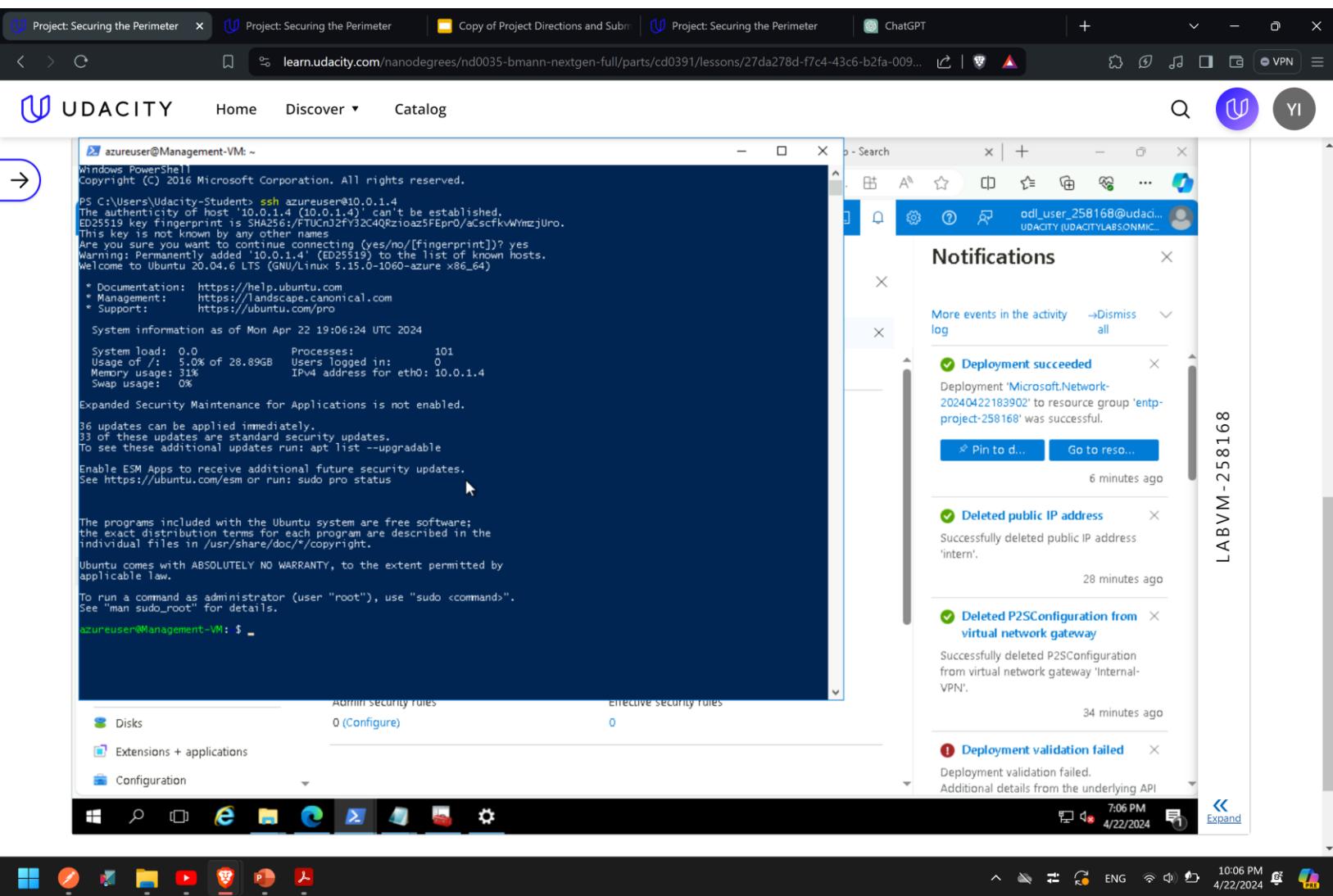
2.4.1 Screenshot

Create a VPN to connect to your internal network.

The screenshot displays two windows side-by-side. On the left is a Microsoft Edge browser window showing the Azure portal. The URL is <https://portal.azure.com/#@udacitylabs.onmicrosoft.com/resource/subscriptions/c4f47e86-cf48-4611-8c4d-6f6124a34a60/resourceGroups/entp-project-258168/providers/Microsoft.Network/virtualNetworkGateways/Internal-VPN>. The page shows details for a Virtual Network Gateway named 'Internal-VPN'. It includes sections for Overview, Essentials (SKU: VpnGw1, Gateway type: VPN, VPN type: Route-based), Health check, and Documentation. Notifications on the right show deployment successes and validation failures. On the right is a Windows Control Panel window titled 'Network & internet' under 'VPN'. It shows a connection to 'Internal' (Connected) with a 'Disconnect' button. Advanced settings for all VPN connections include 'Allow VPN over metered networks' (On) and 'Allow VPN while roaming' (On). A 'Related support' section links to 'Help with VPN' and 'Setting up a VPN'. At the bottom, there are links for 'Get help' and 'Give feedback'.

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.

The screenshot shows the Microsoft Azure portal interface. A virtual machine named "ELK1" is selected. The main pane displays the "Properties" tab of the VM's configuration, showing details like Resource group (entp-project-258168), Status (Running), Location (East US (Zone 1)), Subscription (Udacity CloudLabs Sub - 29), and Operating system (Linux (ubuntu 20.04)). The Notifications sidebar on the right shows three recent events: "Deployment succeeded" (21 minutes ago), "Successfully stopped virtual machine" (22 minutes ago), and "Successfully deleted virtual machine 'ELK'" (23 minutes ago). The URL in the browser bar is <https://portal.azure.com/#/udacitylabs.onmicrosoft.com/resource/subscriptions/c4f47e86-cf48-4611-8c4d-6f6124a34a60/resourceGroups/entp-project-258168/providers/Microsoft.Compute/virtualMachines/ELK1>.

3.1.2 Screenshot

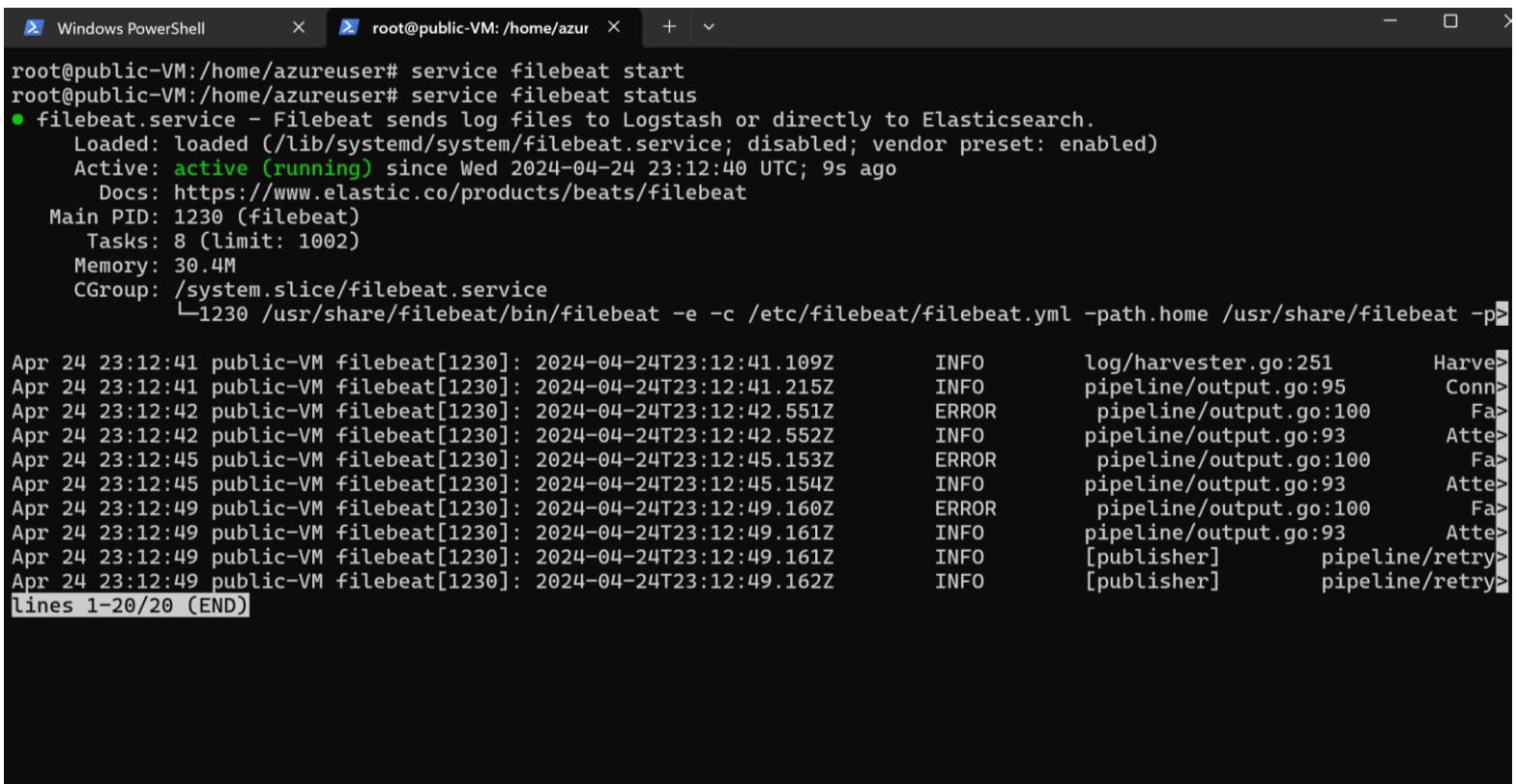
Set up routing to only allow traffic inbound to the server from both your virtual networks, and make sure Kibana is only accessible when you're on the network.

The screenshot shows a Microsoft Edge browser window with multiple tabs open. The active tab is 'DMZ-NSG - Microsoft Azure' displaying the 'Inbound security rules' for a Network Security Group (NSG). The page title is 'DMZ-NSG | Inbound security rules'. The table lists 18 rules, each with columns for Priority, Name, Port, Protocol, Source, Destination, and Action. Most rules have a priority of 100 and are set to Allow. One rule, 'allowThepublickibana', has a priority of 150 and is set to Allow. The 'Source' column for most rules is 'Any', while for the Kibana rule it is '13.87.206.67'. The 'Destination' column for the Kibana rule is '10.0.1.0/24'. The 'Action' column for all rules is 'Allow'. The browser's address bar shows the URL: https://portal.azure.com/#@udacitylabs.onmicrosoft.com/resource/subscriptions/c4f47e86-df48-4611-8c4d-6f... . The status bar at the bottom right shows the time as 8:30 PM and the date as 4/22/2024. A vertical watermark 'LABVM-258168' is visible on the right side of the screen.

Priority	Name	Port	Protocol	Source	Destination	Action
100	public-DMZ	80	TCP	Any	10.0.2.0/24	Allow
110	Public-DMZ-https	443	TCP	Any	10.0.2.0/24	Allow
120	mysshaccess	22	TCP	13.87.206.67	10.0.0.0/24	Allow
150	allowThepublickibana	5601	Any	10.0.0.0/24	Any	Allow
160	Management	5601	Any	74.235.107.44	Any	Allow
170	Secure	80	TCP	74.235.107.11	Any	Allow
180	Secure-HTTP-Access	80	TCP	74.235.107.11	Any	Allow
190	ManagementHttpAccess	80	TCP	74.235.107.44	Any	Allow
200	Enterprise	80	TCP	172.210.17.88	Any	Allow
210	Enterprisek	5601	Any	172.210.17.88	Any	Allow
220	myhttpaccess	80	Any	13.87.206.67	10.0.1.0/24	Allow
230	mykibanaaccess	5601	TCP	13.87.206.67	10.0.1.0/24	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

3.2.1 Screenshot

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



The screenshot shows a Windows PowerShell window with two tabs: "Windows PowerShell" and "root@public-VM: /home/azureuser". The "root@public-VM" tab is active and displays the following command and its output:

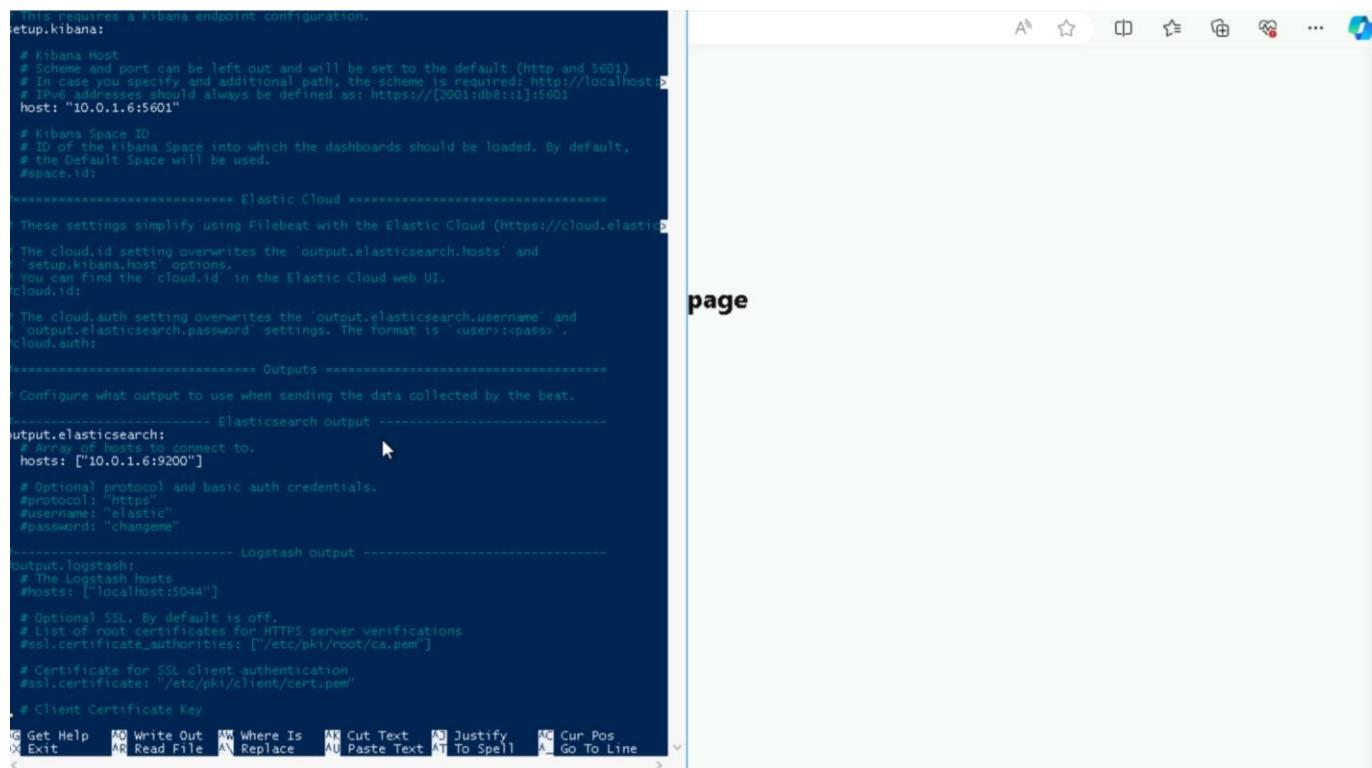
```
root@public-VM:/home/azureuser# service filebeat start
root@public-VM:/home/azureuser# service filebeat status
● filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.
  Loaded: loaded (/lib/systemd/system/filebeat.service; disabled; vendor preset: enabled)
  Active: active (running) since Wed 2024-04-24 23:12:40 UTC; 9s ago
    Docs: https://www.elastic.co/products/beats/filebeat
   Main PID: 1230 (filebeat)
     Tasks: 8 (limit: 1002)
    Memory: 30.4M
      CGroup: /system.slice/filebeat.service
              └─1230 /usr/share/filebeat/bin/filebeat -e -c /etc/filebeat/filebeat.yml -path.home /usr/share/filebeat -p

Apr 24 23:12:41 public-VM filebeat[1230]: 2024-04-24T23:12:41.109Z      INFO      log/harvester.go:251      Harve...
Apr 24 23:12:41 public-VM filebeat[1230]: 2024-04-24T23:12:41.215Z      INFO      pipeline/output.go:95      Conn...
Apr 24 23:12:42 public-VM filebeat[1230]: 2024-04-24T23:12:42.551Z      ERROR     pipeline/output.go:100      Fa...
Apr 24 23:12:42 public-VM filebeat[1230]: 2024-04-24T23:12:42.552Z      INFO      pipeline/output.go:93      Atte...
Apr 24 23:12:45 public-VM filebeat[1230]: 2024-04-24T23:12:45.153Z      ERROR     pipeline/output.go:100      Fa...
Apr 24 23:12:45 public-VM filebeat[1230]: 2024-04-24T23:12:45.154Z      INFO      pipeline/output.go:93      Atte...
Apr 24 23:12:49 public-VM filebeat[1230]: 2024-04-24T23:12:49.160Z      ERROR     pipeline/output.go:100      Fa...
Apr 24 23:12:49 public-VM filebeat[1230]: 2024-04-24T23:12:49.161Z      INFO      pipeline/output.go:93      Atte...
Apr 24 23:12:49 public-VM filebeat[1230]: 2024-04-24T23:12:49.161Z      INFO      [publisher]      pipeline/retry...
Apr 24 23:12:49 public-VM filebeat[1230]: 2024-04-24T23:12:49.162Z      INFO      [publisher]      pipeline/retry...
```

At the bottom of the log output, it says "Lines 1-20/20 (END)".

3.2.2 Screenshot

Configure Filebeat to route web server logs to Elasticsearch.



```
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:[port]
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  host: "10.0.1.6:5601"

  # 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: "1"

----- 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: "1"

The cloud.auth setting overwrites the 'output.elasticsearch.username' and
'output.elasticsearch.password' settings. The format is <user>:<pass> .
cloud.auth: "elastic:changeme"

----- 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: ["10.0.1.6:9200"]

  # 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.certificateAuthorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"

Get Help  Write Out  Where Is  Cut Text  Justify  Cur Pos  Go To Line
Exit  Read File  Replace  Paste Text  To Spell  Go To Line >
```

3.2.3 Screenshot

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



Hello, ahmedsahra517

Easy Money

Dashboard

Your account has been activated! We unleashed the horde!

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, then congratulations! Your system is working correctly. You should [replace this file](#) (located at `/var/www/html/index.html`) before continuing to operate your HTTP service.

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 under `/etc/apache2`. See [/usr/share/doc/apache2/README.Debian.gz](#) 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
|   |
|   +-- sites-available
|       |-- *.conf
|
+-- conf-available
    |-- *.conf
    +-- envvars
        +-- envvars
            +-- envvars
                +-- envvars
                    +-- envvars
                        +-- envvars
                            +-- envvars
                                +-- envvars
                                    +-- envvars
                                        +-- envvars
                                            +-- envvars
                                                +-- envvars
                                                    +-- envvars
                                                        +-- envvars
                                                            +-- envvars
                                                                +-- envvars
                                                                    +-- envvars
                                                                        +-- envvars
                                                                            +-- envvars
                                                                                +-- envvars
                                                                                    +-- envvars
                                                                                        +-- envvars
                                                                                            +-- envvars
                                                                                                +-- envvars
                                                                                                    +-- envvars
                                                                                                        +-- envvars
................................................................
```

• `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 listening ports for incoming connections, and this file can be customized anytime.

• Configuration files in the `mods-enabled`, `conf-enabled` and `sites-enabled` directories contain snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.

• They are activated by symbolinking available configuration files from their respective `*.available` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enrc`, `a2disrc` (see the [configuration overview](#) for details).

• The binary is called `apache2`. Due to the use of environment variables in the default configuration, `apache2` needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`. Calling `/usr/bin/apache2` directly will not work with the default configuration.

Document Roots

By default, Ubuntu does not allow access through the web browser to any file apart from those located in `/var/www`, `public_html` directories (when enabled) and `/usr/share` (for web applications). If your site is using a web document root located elsewhere (e.g. `/srv`) you may need to whitelist your document root directory in `/etc/apache2/apache2.conf`.

The default Ubuntu document root is `/var/www/html`. You can make your own virtual hosts under `/var/www`. This is different to previous releases which provides better security out of the box.

Reporting Problems

Please use the `ubuntu-bug` tool to report bugs in the Apache2 package with Ubuntu. However, check [existing bug reports](#) before reporting a new bug.

50 /50 visits

2024-04-24 21:35:31	Visit #50	RUNNING!
2024-04-24 21:35:30	Visit #49	RUNNING!
2024-04-24 21:35:29	Visit #48	RUNNING!
2024-04-24 21:35:28	Visit #47	RUNNING!

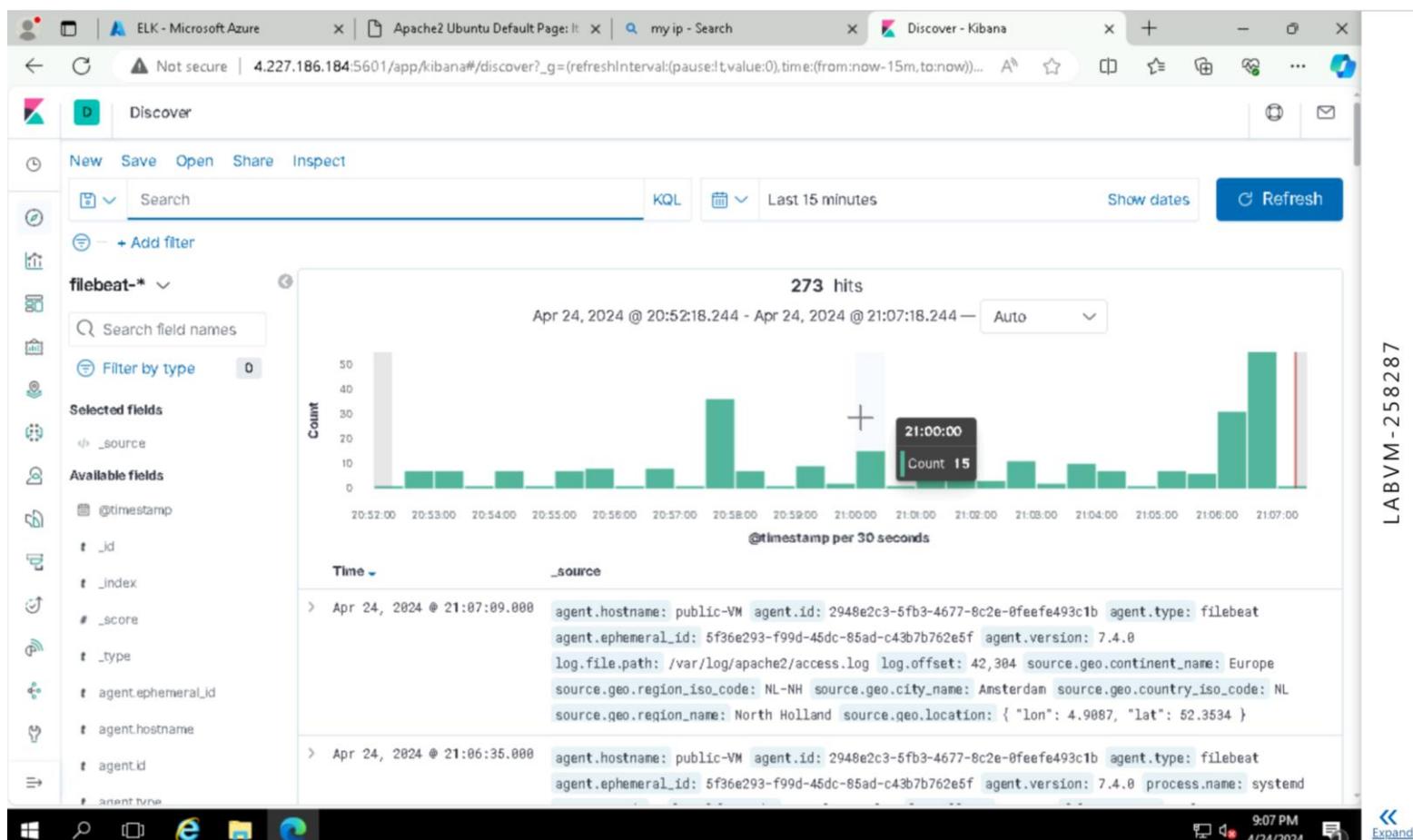


<https://www.babylontraffic.com/account/demo/screenshot?id=201676>

3.2.4 Screenshot

Web server logs appear in Kibana.

LABVM-258287



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.

The screenshot shows the Elasticsearch Management interface, specifically the Watcher section, where a new alert is being created. The left sidebar contains navigation links for various features like Transform, Cross-Cluster Replication, Remote Clusters, and Kibana. The main area is titled "Management / Watcher / Create".

Name: DoS ALert

Indices to query: filebeat-7.4.0-2024.04.24-000001

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 20 FOR THE LAST 1 minute
```

No data: Your index and condition did not return any data.

Perform 1 action when condition is met:

Logging:

Log text: there may be a Denial of Service Attack

Log a sample message:

Buttons: Create alert (highlighted), Cancel, Show request

3.3.2 Screenshot

Create an alert for Brute Force attack.

The screenshot shows the Elasticsearch Management interface, specifically the Watcher section, where a new alert is being created. The left sidebar contains navigation links for various features like Transform, Cross-Cluster Replication, Remote Clusters, and Kibana. The main form is titled 'Create' and includes the following fields:

- Name:** Brute Force Alert
- Indices to query:** filebeat-7.4.0-2024.04.24-000001
- Time field:** @timestamp
- Run watch every:** 1 minute

Below these settings, there's a section titled "Match the following condition" with the query: `WHEN count() GROUPED OVER top 5 'event.outcome' IS ABOVE OR EQUALS 2 FOR THE LAST 1 minute`. A note below it says "No data" and "Your index and condition did not return any data.".

Under the "Perform 1 action when condition is met" section, there is a "Logging" action selected. It includes a "Log text" field containing the placeholder `there may be a Brute Forcing Attempt`. A button labeled "Log a sample message" is also present.

At the bottom of the form, there are buttons for "Create alert" (which is highlighted in green), "Cancel", and "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.

The screenshot shows the Elasticsearch Management interface, specifically the Watcher section, where a new alert is being created. The left sidebar contains navigation links for Index Management, Index Lifecycle Policies, Rollup Jobs, Transforms, Cross-Cluster Replication, Remote Clusters, Watcher (selected), Snapshot and Restore, License Management, and 8.0 Upgrade Assistant. The Kibana section includes Index Patterns, Saved Objects, Spaces, Reporting, and Advanced Settings. The Beats section has Central Management. The Machine Learning section shows a 'Jobs list'. The main content area is titled 'Create threshold alert' and describes sending an alert when a specified condition is met, running every 1 minute. It shows the 'Name' field set to 'Scanning ALert', the 'Indices to query' set to 'filebeat-7.4.0-2024.04.24-000001', the 'Time field' set to '@timestamp', and the 'Run watch every' interval as '1 minute'. Below this, under 'Match the following condition', the query is defined as 'WHEN count() GROUPED OVER top 5 'destination.port' IS ABOVE 5 FOR THE LAST 30 seconds'. A note indicates 'No data' because the index and condition did not return any data. Under 'Perform 1 action when condition is met', there is a 'Logging' section with a 'Log text' field containing 'There may be a Someone Scanning the Site!' and a 'Log a sample message' button. An 'Add action' button is also present.

3.4 Incident Response Playbook

1) DoS Attack:

Rate Limiting: Implement rate limiting on the server to restrict the number of requests it can handle within a given timeframe. This helps prevent the server from being overwhelmed by too many requests.

Block List: Identify the IPs sourcing the attack by analyzing logs and network traffic. Once identified, block these IPs at the network level to stop the attack traffic from reaching the server.

Traffic Analysis: Analyze incoming traffic to identify patterns specific to the DoS attack. Look for common characteristics such as high request rates from particular IPs or unusual traffic spikes.

Resource Scaling: Temporarily scale up server resources such as CPU, memory, and bandwidth to handle the increased load caused by the attack. This can help mitigate the impact on service availability until the attack is resolved.

3.4 Incident Response Playbook

Remediation:

Review and update server configurations to optimize performance and mitigate future DoS attacks.

Implement DDoS protection services or appliances to detect and mitigate similar attacks in real-time.

2) Brute Force Attack:

Account Lockout Policies: Implement account lockout policies to automatically lock out user accounts after a certain number of failed login attempts. This helps prevent attackers from guessing passwords through brute force.

Change Passwords: Prompt affected users to change their passwords immediately to prevent unauthorized access to their accounts. Provide guidance on creating strong, unique passwords.

3.4 Incident Response Playbook

Monitor for Suspicious Activity: Continuously monitor system logs and authentication records for any unusual login attempts or access patterns. Investigate any suspicious activity promptly.

Remediation:

Enhance authentication mechanisms with multi-factor authentication (MFA) to add an extra layer of security. Educate users on password hygiene and security best practices to minimize the risk of successful brute force attacks.

3) Scanning and Reconnaissance:

Alter Firewall Rules: Analyze incoming traffic patterns and adjust firewall rules to block or restrict traffic from suspicious sources. This helps prevent attackers from conducting further reconnaissance or exploiting vulnerabilities.

3.4 Incident Response Playbook

Honeypots: Deploy honeypots strategically within the network to lure and trap attackers. Analyze the behavior of attackers targeting the honeypots to gather intelligence on their tactics and techniques.

Network Segmentation: Ensure critical assets are isolated within segmented network zones. This limits the potential impact of a successful attack and prevents lateral movement within the network.

Remediation:

Regularly review and update firewall rules to adapt to evolving threats and attack techniques.

Conduct periodic security assessments and penetration tests to identify and address vulnerabilities in the network infrastructure.

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.

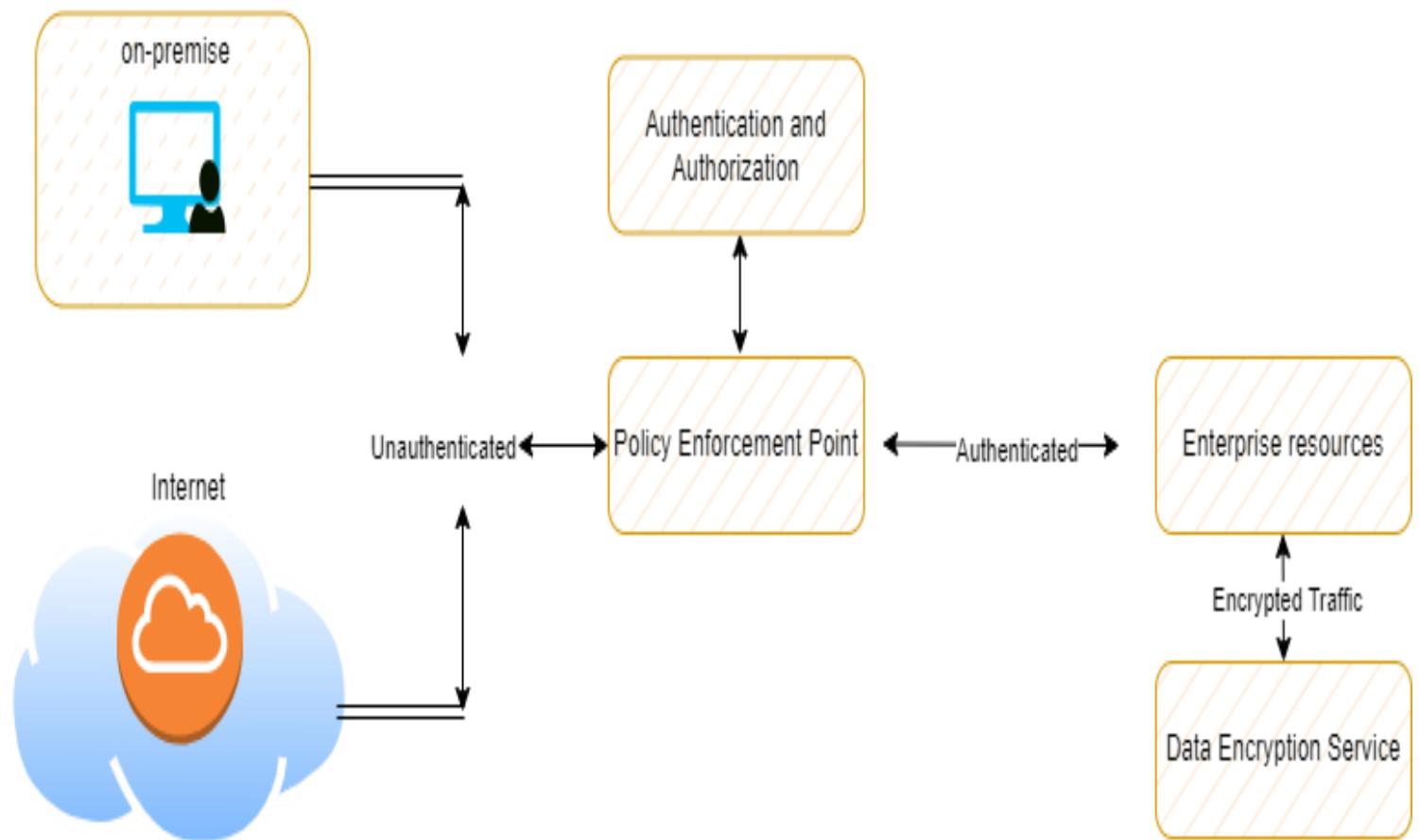
Design a Zero Trust model of your network architecture using <https://app.diagrams.net/>.

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

In my Zero Trust model, authentication serves as the cornerstone of network security, requiring rigorous verification of users, whether they originate from the on-premise network or connect directly from the internet. Before granting access to resources such as the VPN or the Public DMZ, users must undergo an authentication process, to ensure their identities are validated. This approach mitigates the risk of unauthorized access attempts and strengthens the overall security posture of the network.

Furthermore, encryption plays a pivotal role in safeguarding data integrity and confidentiality throughout the entire system. All traffic flowing within the network, whether between segments or from external sources, is encrypted to prevent any eavesdropping. This aligns with the Zero Trust principle of assuming breach and implementing robust data protection measures.

Additionally, the concept of trust is redefined within this model, moving away from implicit trust based on network location to continuous verification of identity and behavior. Trust is never assumed and must be earned through ongoing authentication and authorization processes. This contrasts with traditional network architectures that rely heavily on perimeter-based trust models.

4.2 Modern Architecture vs. Zero Trust

Moreover, the emergence of cloud services has rendered traditional perimeter defenses outdated, necessitating a shift towards a Zero Trust mindset. Modern network architectures must adapt to the dynamic nature of cloud environments by implementing granular access controls and encryption mechanisms that transcend traditional network boundaries.

Finally, the evolution of the threat landscape underscores the importance of adopting a Zero Trust approach. With increasingly sophisticated cyber threats, organizations can no longer rely solely on perimeter defenses but must instead adopt proactive security measures that continuously monitor and respond to threats in real-time.