

Project: Securing the Perimeter

Benjámín Rácskai

07.04.2024

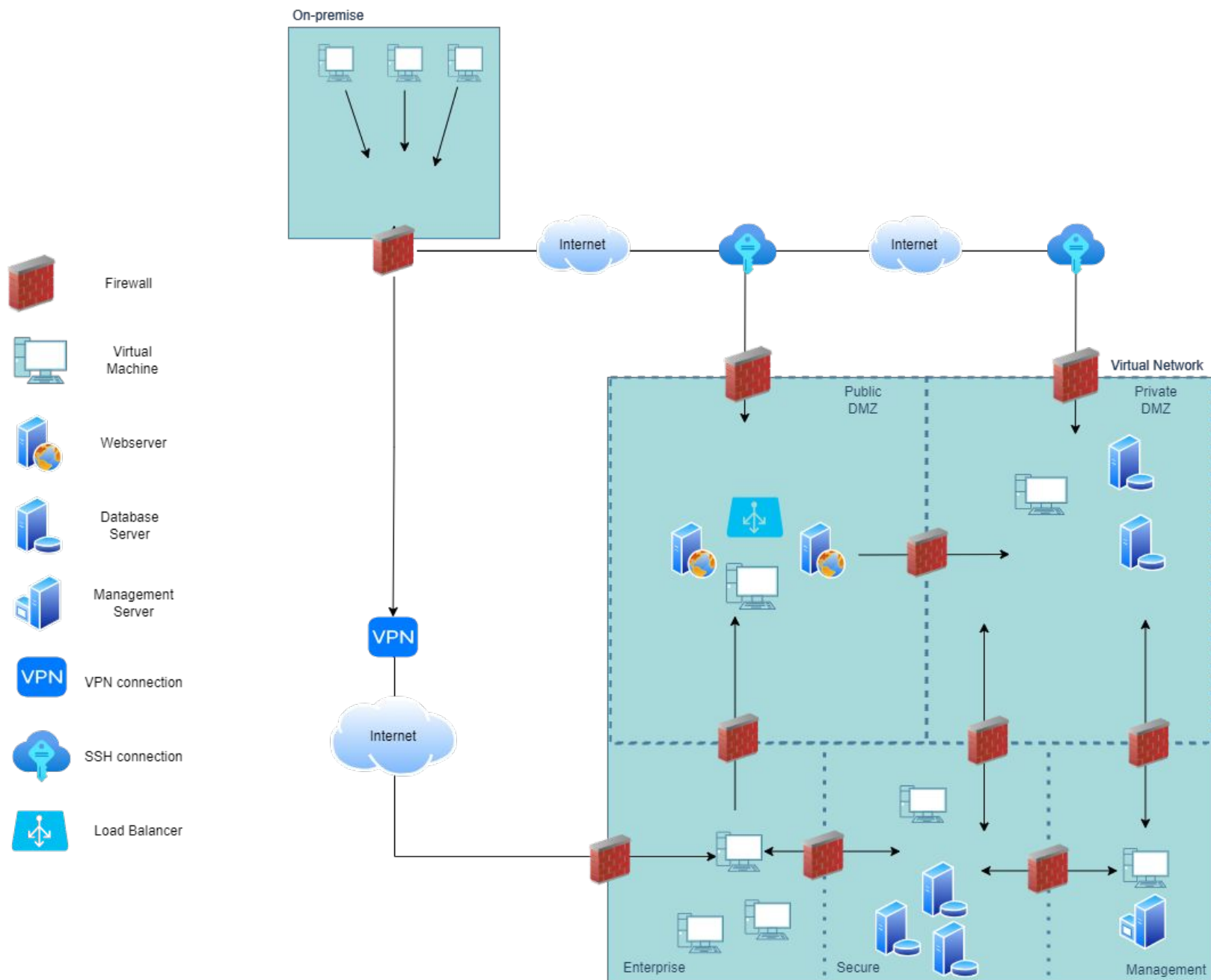


Section 1

Designing a Secure Network Architecture

1.1 Designing the Network

Paste your Network Diagram here:



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.

[Home](#) >

Virtual networks

Udacity

+ 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.

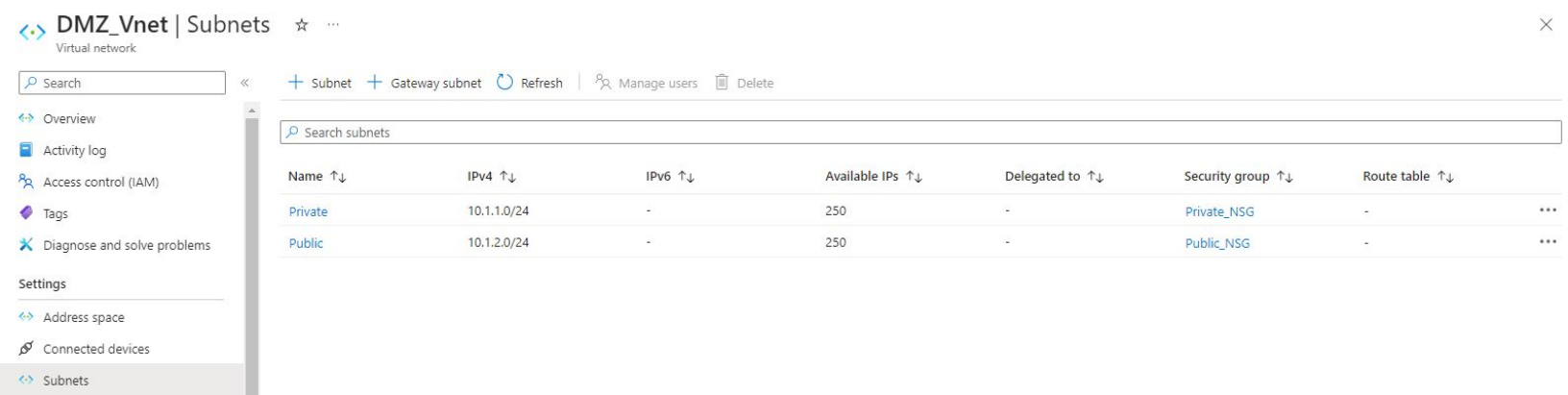
No grouping

List view

<input type="checkbox"/> Name ↑↓	Resource group ↑↓	Location ↑↓	Subscription ↑↓	
<input type="checkbox"/> DMZ_Vnet	entp-project-256828	East US	Udacity CloudLabs Sub - 48	...
<input type="checkbox"/> Internal_Vnet	entp-project-256828	East US	Udacity CloudLabs Sub - 48	...

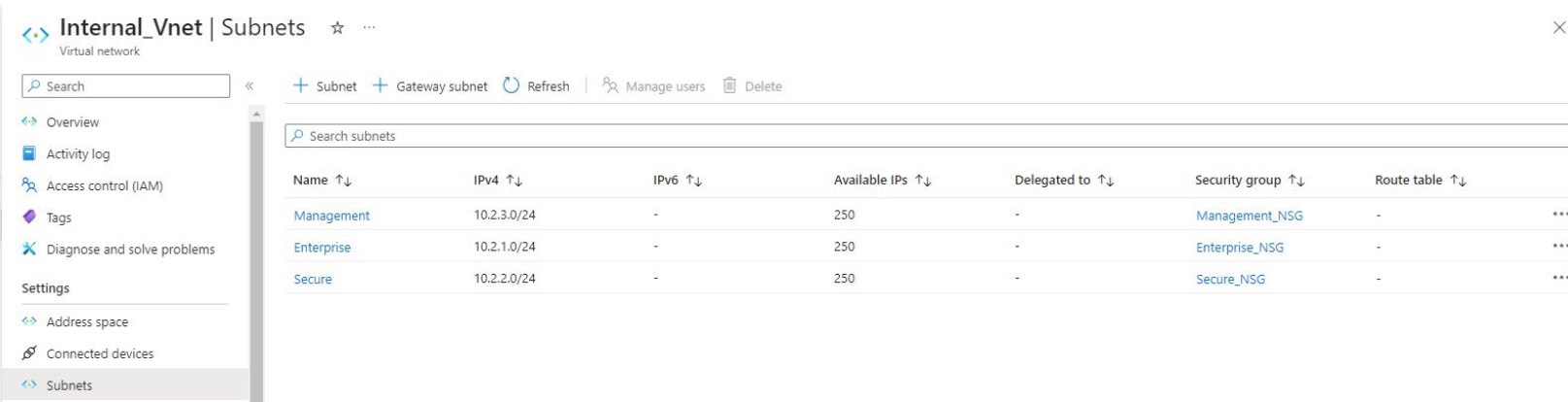
2.1.2 Screenshot

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.



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.

Public-VM

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

Connect

Start

Restart

Stop

Hibernate (preview)

Capture

Delete

Refresh

Open in mobile

Feedback

CLI / PS

Essentials

Resource group (move) : [entp-project-256828](#)

Status : Running

Location : East US

Subscription (move) : [Udacity CloudLabs Sub - 48](#)

Subscription ID : 3011ed27-260d-4215-af4c-ec9434399817

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

Operating system : Linux (ubuntu 20.04)

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

Public IP address : [104.211.2.155](#)

Virtual network/subnet : [DMZ_Vnet/Public](#)

DNS name : [Not configured](#)

Health state : -

Properties

Monitoring

Capabilities (7)

Recommendations

Tutorials

Virtual machine

Computer name : Public-VM

Operating system : Linux (ubuntu 20.04)

Image publisher : canonical

Image offer : 0001-com-ubuntu-server-focal

Image plan : 20_04-lts-gen2

VM generation : V2

Networking

Public IP address : [104.211.2.155](#) (Network interface [public-vm599](#))

Public IP address (IPv6) : -

Private IP address : 10.1.2.4

Private IP address (IPv6) : -

Virtual network/subnet : [DMZ_Vnet/Public](#)

DNS name : [Configure](#)

Private-VM

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

Connect

Start

Restart

Stop

Hibernate (preview)

Capture

Delete

Refresh

Open in mobile

Feedback

CLI / PS

Essentials

Resource group (move) : [entp-project-256828](#)

Status : Running

Location : East US

Subscription (move) : [Udacity CloudLabs Sub - 48](#)

Subscription ID : 3011ed27-260d-4215-af4c-ec9434399817

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

Operating system : Linux (ubuntu 20.04)

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

Public IP address : [172.172.230.232](#)

Virtual network/subnet : [DMZ_Vnet/Private](#)

DNS name : [Not configured](#)

Health state : -

Properties

Monitoring

Capabilities (7)

Recommendations

Tutorials

Virtual machine

Computer name : Private-VM

Operating system : Linux (ubuntu 20.04)

Image publisher : canonical

Image offer : 0001-com-ubuntu-server-focal

Image plan : 20_04-lts-gen2

VM generation : V2

Networking

Public IP address : [172.172.230.232](#) (Network interface [private-vm945](#))

Public IP address (IPv6) : -

Private IP address : 10.1.1.4

Private IP address (IPv6) : -

Virtual network/subnet : [DMZ_Vnet/Private](#)

DNS name : [Configure](#)

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.

Management-VM

Virtual machine

Search

ConnectStartRestartStopHibernate (preview)CaptureDeleteRefreshOpen in mobileFeedbackCLI / 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

Essentials

Resource group (move) : entp-project-256828

Status : Running

Location : East US

Subscription (move) : Udacity CloudLabs Sub - 48

Subscription ID : 3011ed27-260d-4215-af4c-ec9434399817

Operating system : Linux (ubuntu 20.04)

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

Public IP address : -

Virtual network/subnet : Internal_Vnet/Management

DNS name : -

Health state : -

Tags (edit) : Add tags

PropertiesMonitoringCapabilities (7)RecommendationsTutorials

Virtual machine

Computer name : Management-VM

Operating system : Linux (ubuntu 20.04)

Image publisher : canonical

Image offer : 0001-com-ubuntu-server-focal

Image plan : 20_04-lts-gen2

VM generation : V2

Networking

Public IP address : -

Public IP address (IPv6) : -

Private IP address : 10.2.3.4

Private IP address (IPv6) : -

Virtual network/subnet : Internal_Vnet/Management

DNS name : -

Secure-VM

Virtual machine

Search

ConnectStartRestartStopHibernate (preview)CaptureDeleteRefreshOpen in mobileFeedbackCLI / 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

Essentials

Resource group (move) : entp-project-256828

Status : Running

Location : East US

Subscription (move) : Udacity CloudLabs Sub - 48

Subscription ID : 3011ed27-260d-4215-af4c-ec9434399817

Operating system : Linux (ubuntu 20.04)

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

Public IP address : -

Virtual network/subnet : Internal_Vnet/Secure

DNS name : -

Health state : -

Tags (edit) : Add tags

PropertiesMonitoringCapabilities (7)RecommendationsTutorials

Virtual machine

Computer name : Secure-VM

Operating system : Linux (ubuntu 20.04)

Image publisher : canonical

Image offer : 0001-com-ubuntu-server-focal

Image plan : 20_04-lts-gen2

VM generation : V2

Networking

Public IP address : -

Public IP address (IPv6) : -

Private IP address : 10.2.2.4

Private IP address (IPv6) : -

Virtual network/subnet : Internal_Vnet/Secure

DNS name : -

 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

Essentials

Resource group (move)	: entp-project-256828	Operating system	: Linux (ubuntu 20.04)
Status	: Running	Size	: Standard B1s (1 vcpu, 1 GiB memory)
Location	: East US	Public IP address	: -
Subscription (move)	: Udacity CloudLabs Sub - 48	Virtual network/subnet	: Internal_Vnet/Enterprise
Subscription ID	: 3011ed27-260d-4215-af4c-ec9434399817	DNS name	: -
Tags (edit)	: Add tags	Health state	: -

- Properties
- Monitoring
- Capabilities (7)
- Recommendations
- Tutorials



Virtual machine

Computer name	Enterprise-VM
Operating system	Linux (ubuntu 20.04)
Image publisher	canonical
Image offer	0001-com-ubuntu-server-focal
Image plan	20_04-lts-gen2
VM generation	V2



Networking

Public IP address	-
Public IP address (IPv6)	-
Private IP address	10.2.1.4
Private IP address (IPv6)	-
Virtual network/subnet	Internal_Vnet/Enterprise
DNS name	-

2.3.1 Screenshot

Traffic rules in your DMZ.

Private_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

CLI / PS

Essentials

Resource group (move) : entp-project-256828

Location : East US

Subscription (move) : Udacity CloudLabs Sub - 48

Subscription ID : 3011ed27-260d-4215-af4c-ec9434399817

Tags (edit) : Add tags

Custom security rules : 5 inbound, 0 outbound

Associated with : 1 subnets, 3 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						
100	SSH	22	TCP	40.121.182.55	VirtualNetwork	Allow
110	Traffic-From-Vnets-to-ELK-VM	Any	Any	10.1.2.0/24,10.2.1.0/24,10.2.2.0/24,10.2.3.0/24	10.1.1.5	Allow
120	Port_8080	80	TCP	40.121.182.55,172.16.1.0/24	VirtualNetwork	Allow
130	Kibana	5601	Any	40.121.182.55,172.16.1.0/24	VirtualNetwork	Allow
140	Traffic-From-Internet-To-Webserver_apache	80	TCP	Internet	10.1.1.6	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	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

Public_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

CLI / PS

Essentials

Resource group (move) : entp-project-257159

Location : East US

Subscription (move) : Udacity CloudLabs Sub - 50

Subscription ID : 7c1143fd-12ed-4767-abd7-2d979135d236

Tags (edit) : Add tags

Custom security rules : 3 inbound, 1 outbound

Associated with : 1 subnets, 0 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						
100	SSH	22	TCP	52.226.133.151	VirtualNetwork	Allow
110	Allow-HTTP-To-Public-DMZ	80	TCP	Internet	VirtualNetwork	Allow
120	Allow-HTTPS-To-Public-DMZ	443	TCP	Internet	VirtualNetwork	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
130	Traffic-Outbound-From-Public-To-ELK	Any	Any	10.1.2.0/24	10.1.1.5	Allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

2.3.2 Screenshot

Traffic rules in your Internal network.

Management_NSG

Network security group

Search

Move Delete Refresh Give feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Network interfaces

Subnets

Properties

Locks

Monitoring

Alerts

Diagnostic settings

Logs

NSG flow logs

Essentials

Resource group (move) : entp-project-256828

Location : East US

Subscription (move) : Udacity CloudLabs Sub - 48

Subscription ID : 3011ed27-260d-4215-af4c-ec9434399817

Tags (edit) : Add tags

Custom security rules : 1 inbound, 1 outbound

Associated with : 1 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						
100	AllowInboundTrafficOverVPN	22	TCP	172.16.1.0/24	VirtualNetwork	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
110	Traffic-Outbound-From-Management-To-ELK	Any	Any	10.2.3.0/24	10.1.1.5	Allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Secure_NSG

Network security group

Search

Move Delete Refresh Give feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Network interfaces

Subnets

Properties

Locks

Monitoring

Alerts

Diagnostic settings

Logs

NSG flow logs

Essentials

Resource group (move) : entp-project-256828

Location : East US

Subscription (move) : Udacity CloudLabs Sub - 48

Subscription ID : 3011ed27-260d-4215-af4c-ec9434399817

Tags (edit) : Add tags

Custom security rules : 1 inbound, 1 outbound

Associated with : 1 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						
100	AllowInboundTrafficOverVPN	22	TCP	172.16.1.0/24	VirtualNetwork	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
110	Traffic-Outbound-From-Secure-To-ELK	Any	Any	10.2.2.0/24	10.1.1.5	Allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

- 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

Essentials

Resource group (move) : entp-project-256828

Location : East US

Subscription (move) : Udacity CloudLabs Sub - 48

Subscription ID : 3011ed27-260d-4215-af4c-ec9434399817

Tags (edit) : Add tags

Custom security rules : 1 inbound, 1 outbound

Associated with : 1 subnets, 1 network interfaces

Filter by name

Port == allProtocol == allSource == allDestination == allAction == all

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
100	AllowInboundTrafficOverVPN	22	TCP	172.16.1.0/24	VirtualNetwork	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
110	Traffic-Outbound-From-Enterprise-To-ELK	Any	Any	10.2.1.0/24	10.1.1.5	Allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

2.4.1 Screenshot

Create a VPN to connect to your internal network.

Home >

Virtual network gateways

Udacity

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 1 of 1 records.

Name	Virtual network	Gateway type	Resource group	Location
BR_VPN	Internal_Vnet	Vpn	entp-project-256112	East US

Home > Virtual network gateways > BR_VPN

Virtual network ga...

Udacity

Create

Manage view

Filter for any field...

Name

BR_VPN

BR_VPN | Point-to-site configuration

Virtual network gateway

Save

Discard

Delete

Download VPN client

Search

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
AzureRootCert	MIIC6zCCAdOgAwIBAgIQT7qmTdck2qhMSnRuKA27/jANBgkqhkiG9w0BAQ...

Settings

Home

Find a setting

Network & Internet

Status

Ethernet

Dial-up

VPN

VPN

Add a VPN connection

Internal_Vnet

Connected

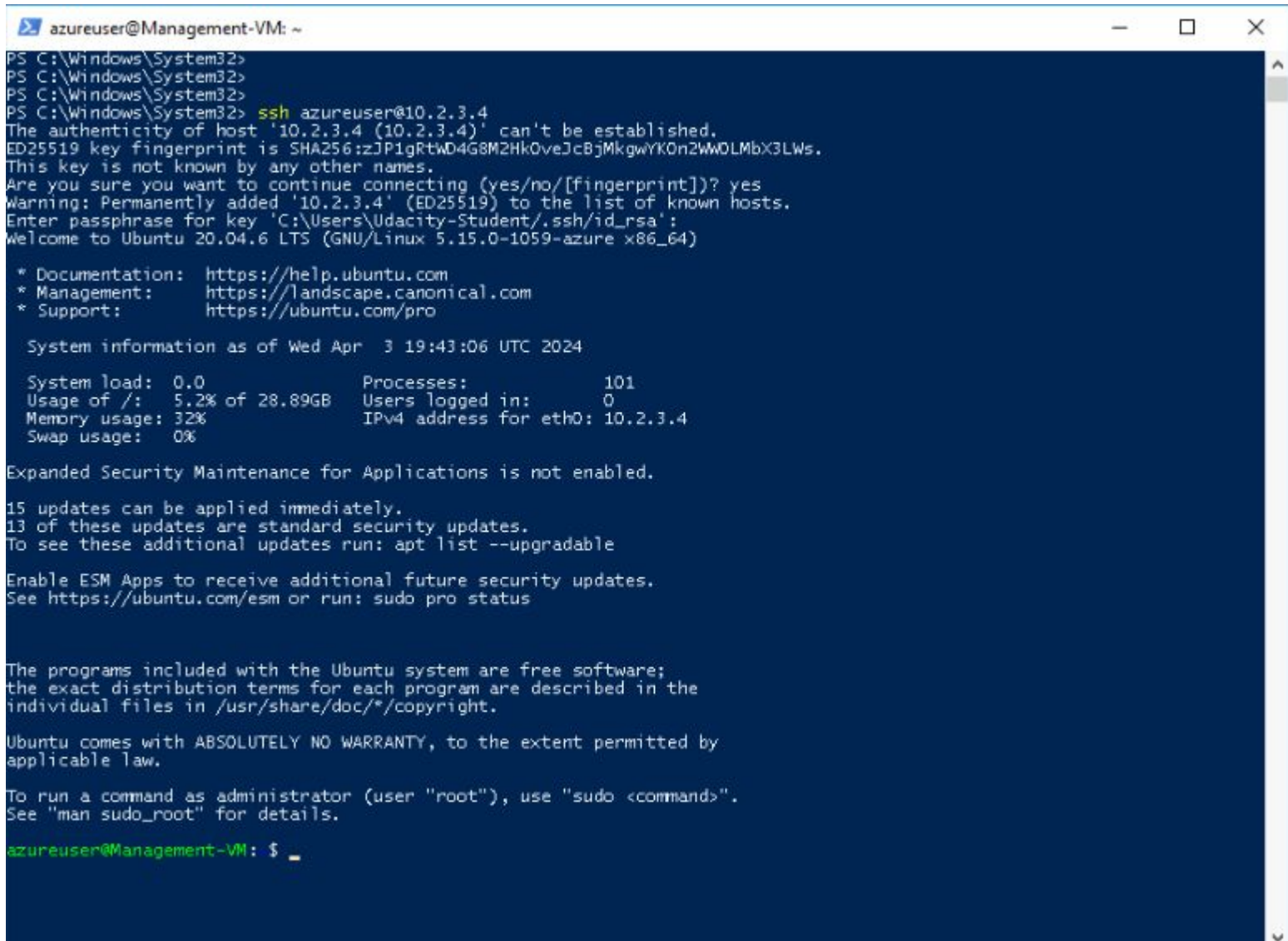
Advanced options

Disconnect

Advanced Options

2.4.2 Screenshot

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



```
azureuser@Management-VM: ~
PS C:\Windows\System32>
PS C:\Windows\System32>
PS C:\Windows\System32>
PS C:\Windows\System32> ssh azureuser@10.2.3.4
The authenticity of host '10.2.3.4 (10.2.3.4)' can't be established.
ED25519 key fingerprint is SHA256:zJPigRtWD4G8M2HkOveJcBjMkgwYKOn2WwOLMbX3LWs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.2.3.4' (ED25519) to the list of known hosts.
Enter passphrase for key 'C:\Users\Udacity-Student/.ssh/id_rsa':
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1059-azure x86_64)

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

System information as of Wed Apr  3 19:43:06 UTC 2024

System load:  0.0          Processes:            101
Usage of /:   5.2% of 28.89GB Users logged in:        0
Memory usage: 32%          IPv4 address for eth0: 10.2.3.4
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

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

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

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

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

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

azureuser@Management-VM: $
```



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 displays the Azure portal interface for a virtual machine named 'ELK-VM'. The left sidebar shows navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, Networking, and Settings. The main area is divided into 'Essentials' and 'Properties' tabs. The 'Essentials' tab shows the VM's status as 'Running' and its location as 'East US'. The 'Properties' tab shows the VM's configuration, including the operating system 'Linux (ubuntu 20.04)' and the image publisher 'canonical'. The 'Networking' tab shows the public IP address '52.190.22.18' and the private IP address '10.1.1.5'. Below the portal, two terminal windows show the command to update the package list and install Docker on the VM.

ELK-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

Essentials

Resource group (move) : [entp-project-256828](#)

Status : Running

Location : East US

Subscription (move) : [Udacity CloudLabs Sub - 48](#)

Subscription ID : 3011ed27-260d-4215-af4c-ec9434399817

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

Operating system : Linux (ubuntu 20.04)

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

Public IP address : [52.190.22.18](#)

Virtual network/subnet : [DMZ_Vnet/Private](#)

DNS name : [Not configured](#)

Health state : -

Properties Monitoring Capabilities (7) Recommendations Tutorials

Virtual machine

Computer name	ELK-VM
Operating system	Linux (ubuntu 20.04)
Image publisher	canonical
Image offer	0001-com-ubuntu-server-focal
Image plan	20_04-lts-gen2
VM generation	V2

Networking

Public IP address	52.190.22.18 (Network interface elk-vm793)
Public IP address (IPv6)	-
Private IP address	10.1.1.5
Private IP address (IPv6)	-
Virtual network/subnet	DMZ_Vnet/Private
DNS name	Configure

```
azureuser@ELK-VM: $  
azureuser@ELK-VM: $ sudo apt update  
Get:1 http://azure.archive.ubuntu.com/ubuntu focal InRelease [265 kB]  
Get:2 http://azure.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]  
Get:3 http://azure.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]  
Hit:4 http://azure.archive.ubuntu.com/ubuntu focal-security InRelease  
Get:5 http://azure.archive.ubuntu.com/ubuntu focal/main amd64 Packages [920 kB]  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following additional packages will be installed:  
  bridge-utils containerd dns-root-data dnsmasq-base libidn11 pigz runc ubuntu-fan  
Suggested packages:  
  ifupdown aufs-tools cgroupfs-mount | cgroup-lite debootstrap docker-doc rinse zfs-fuse | zfsutils  
The following NEW packages will be installed:  
  bridge-utils containerd dns-root-data dnsmasq-base docker.io libidn11 pigz runc ubuntu-fan  
0 upgraded, 9 newly installed, 0 to remove and 15 not upgraded.  
Need to get 63.3 MB of archives.  
After this operation, 267 MB of additional disk space will be used.  
Do you want to continue? [Y/n] yes  
Get:1 http://azure.archive.ubuntu.com/ubuntu focal/universe amd64 pigz amd64 2.4-1 [57.4 kB]  
Get:2 http://azure.archive.ubuntu.com/ubuntu focal/main amd64 bridge-utils amd64 1.6-2ubuntu1 [30.5
```

```

azureuser@ELK-VM: $ sudo apt install python3-pip
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu build-essential cpp cpp-9 dpkg-dev
  libasan5 libatomic1 libbinutils libc-dev-bin libc6-dev libcc1-0 libcrypt-dev libctf-nobfd
  libctf0 liblsan0 libmpc3 libpython3-dev libpython3.8-dev libquadmath0 libstdc++-9-dev libstdc++6
Suggested packages:
  binutils-doc cpp-doc gcc-9-locales debian-keyring g++-multilib g++-9-multilib gcc-9-doc
  libstdc++-9-doc
The following NEW packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu build-essential cpp cpp-9 dpkg-dev
  libasan5 libatomic1 libbinutils libc-dev-bin libc6-dev libcc1-0 libcrypt-dev libctf-nobfd
  libctf0 liblsan0 libmpc3 libpython3-dev libpython3.8-dev libquadmath0 libstdc++-9-dev libstdc++6
  zlib1g-dev
0 upgraded, 50 newly installed, 0 to remove and 15 not upgraded.
Need to get 52.3 MB of archives.
After this operation, 228 MB of additional disk space will be used.
Do you want to continue? [Y/n] yes
Get:1 http://deb.debian.org/debian bullseye/main amd64 binutils-x86-64-linux-gnu 2.35.1-1 [14.7 MB]

```

```

azureuser@ELK-VM: $ sudo pip3 install docker
Collecting docker
  Downloading docker-7.0.0-py3-none-any.whl (147 kB)
    | 147 kB 18.2 MB/s
Collecting urllib3<=1.26.0
  Downloading urllib3-2.2.1-py3-none-any.whl (121 kB)
    | 121 kB 43.2 MB/s
Collecting requests<=2.26.0
  Downloading requests-2.31.0-py3-none-any.whl (62 kB)
    | 62 kB 1.2 MB/s
Collecting packaging<=14.0
  Downloading packaging-24.0-py3-none-any.whl (53 kB)
    | 53 kB 2.4 MB/s
Requirement already satisfied: idna<4,>=2.5 in /usr/lib/python3/dist-packages (from requests<=2.26.0->docker)
Requirement already satisfied: certifi<2017.4.17 in /usr/lib/python3/dist-packages (from requests<=2.26.0->docker)
Collecting charset-normalizer<4,>=2
  Downloading charset-normalizer-3.3.2-cp38-cp38-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (141 kB)
    | 141 kB 45.7 MB/s
Installing collected packages: urllib3, charset-normalizer, requests, packaging, docker
  Attempting uninstall: urllib3
    Found existing installation: urllib3 1.25.8
    Not uninstalling urllib3 at /usr/lib/python3/dist-packages, outside environment /usr
    Can't uninstall 'urllib3'. No files were found to uninstall.
  Attempting uninstall: requests
    Found existing installation: requests 2.22.0
    Not uninstalling requests at /usr/lib/python3/dist-packages, outside environment /usr
    Can't uninstall 'requests'. No files were found to uninstall.
Successfully installed charset-normalizer-3.3.2 docker-7.0.0 packaging-24.0 requests-2.31.0 urllib3-2.2.1

```

```

azureuser@ELK-VM: $
azureuser@ELK-VM: $ sudo sysctl -w vm.max_map_count=262144
vm.max_map_count = 262144
azureuser@ELK-VM: $

```

```

azureuser@ELK-VM: $
azureuser@ELK-VM: $ sudo docker pull sebp/elk:761
761: Pulling from sebp/elk
c64513b74145: Pull complete
01b8b12bad90: Pull complete
c5d85cf7a05f: Pull complete
b6b268720157: Pull complete
e12192999ff1: Pull complete
d39ece66b667: Pull complete
65599be66378: Pull complete
e691df9ee752: Extracting [=====] 26.74MB/131MB
1caea7f89afb: Download complete
c19457083ca7: Download complete
ab24e08d84db: Download complete

```

```

azureuser@ELK-VM: $
azureuser@ELK-VM: $ sudo docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it --name elk sebp/elk:761
* Starting periodic command scheduler cron
* Starting Elasticsearch Server
/jvm/java-8-openjdk-amd64/jre] does not meet this requirement

waiting for Elasticsearch to be up (1/30)
waiting for Elasticsearch to be up (2/30)

```

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.

Private_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

CLI / PS

Tasks (preview)

Essentials

Resource group (move) : entp-project-256828

Location : East US

Subscription (move) : Udacity CloudLabs Sub - 48

Subscription ID : 3011ed27-260d-4215-af4c-ec9434399817

Tags (edit) : Add tags

Custom security rules : 5 inbound, 0 outbound

Associated with : 1 subnets, 3 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						
100	SSH	22	TCP	40.121.182.55	VirtualNetwork	Allow
110	Traffic-From-Vnets-to-ELK-VM	Any	Any	10.1.2.0/24,10.2.1.0/24,10.2.2.0/24,...	10.1.1.5	Allow
120	Port_8080	80	TCP	40.121.182.55,172.16.1.0/24	VirtualNetwork	Allow
130	Kibana	5601	Any	40.121.182.55,172.16.1.0/24	VirtualNetwork	Allow
140	Traffic-From-Internet-To-Webserver_apache	80	TCP	Internet	10.1.1.6	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	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

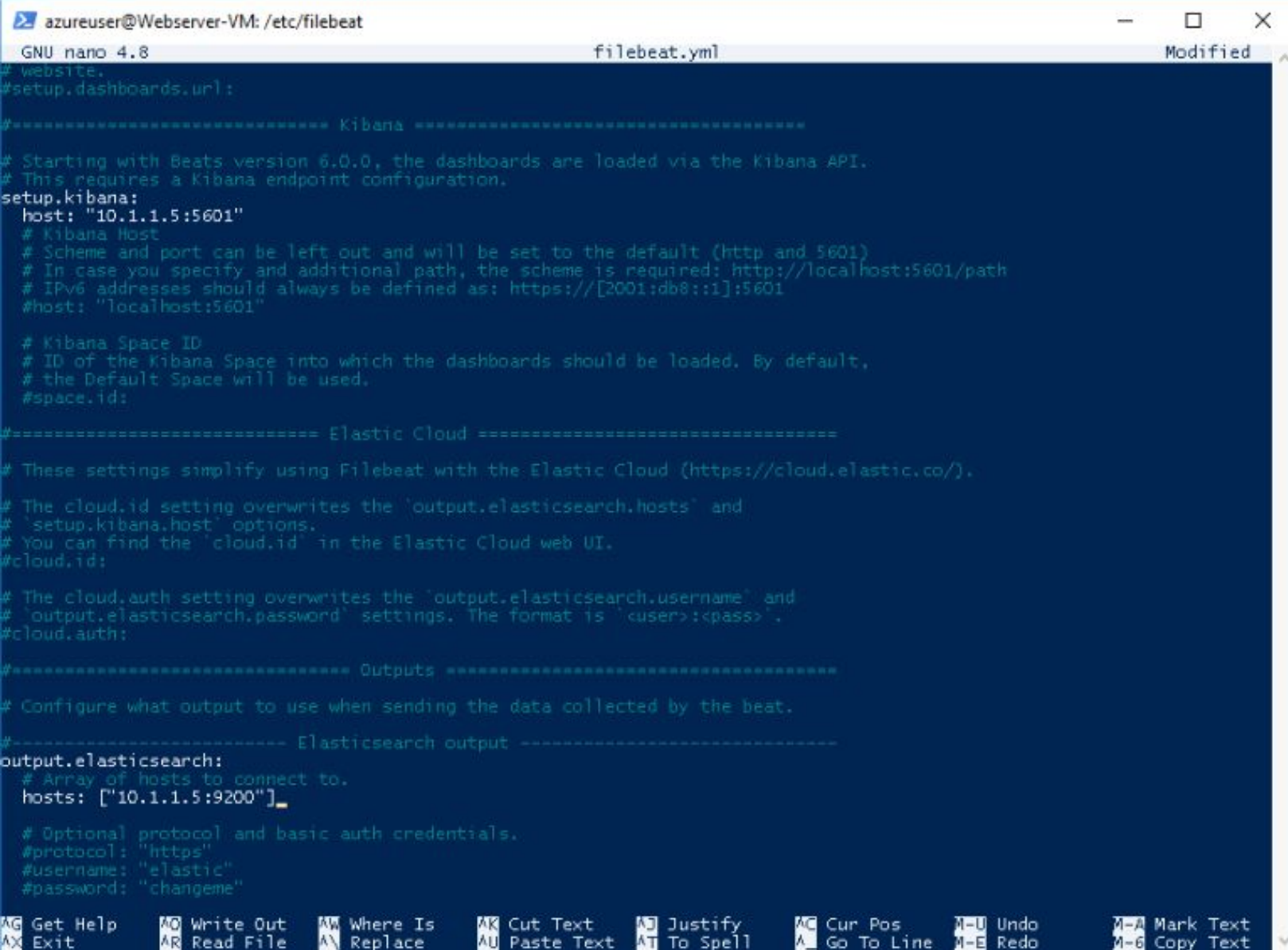
3.2.1 Screenshot

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

```
azureuser@Webserver-VM: /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@Webserver-VM: /etc/filebeat$ sudo service filebeat start
azureuser@Webserver-VM: /etc/filebeat$ systemctl status filebeat.service
● 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 2024-04-03 21:31:42 UTC; 16s ago
     Docs: https://www.elastic.co/products/beats/filebeat
   Main PID: 15241 (filebeat)
      Tasks: 8 (limit: 1002)
     Memory: 26.3M
    CGroup: /system.slice/filebeat.service
            └─15241 /usr/share/filebeat/bin/filebeat -e -c /etc/filebeat/filebeat.yml -path.ho
```

3.2.2 Screenshot

Configure Filebeat to route web server logs to Elasticsearch.



```
azureuser@Webserver-VM: /etc/filebeat
GNU nano 4.8 filebeat.yml Modified
# 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:
  host: "10.1.1.5:5601"
  # 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:

#===== 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: ["10.1.1.5:9200"]

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

AG Get Help  AO Write Out  AW Where Is  AK Cut Text  AJ Justify  AC Cur Pos  M-U Undo  M-A Mark Text
AX Exit      AR Read File  AN Replace AU Paste Text AT To Spell  A_ Go To Line M-E Redo  M-6 Copy Text
```

3.2.3 Screenshot

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

Your account has been activated! We unleashed the horde!



ubuntu

Apache2 Ubuntu Default Page

It works!

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

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

Configuration Overview

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

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

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

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the 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 particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available/` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf`. See their respective man pages for detailed information.
- The binary is called `apache2`. Due to the use of environment variables, in the default configuration, `apache2` needs to be started/shopped with `/etc/init.d/apache2` or `apache2ctl`. Calling `/var/lib/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 of 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 (such as in `/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

2024-04-03 22:52:52	Visit #50	SUCCESS! ✓
2024-04-03 22:52:49	Visit #49	SUCCESS! ✓
2024-04-03 22:52:48	Visit #48	SUCCESS! ✓
2024-04-03 22:52:32	Visit #47	SUCCESS! ✓

3.2.4 Screenshot

Web server logs appear in Kibana.

The screenshot displays the Kibana Discover interface in a web browser. The browser's address bar shows the URL `52.190.22.18:5601/app/kibana#/discover?_g=()&_a=(columns:!(source),index:'filebeat-*',interval:auto,query:(language:kuery,query:''),sort:!(@timestamp,...)`. The interface includes a left-hand sidebar with navigation icons and a main content area displaying a list of log entries. Each entry is timestamped and contains detailed log data, including agent information, file paths, and source details.

Timestamp	Log Data
Apr 3, 2024 @ 21:48:59.000	<p>source.geo.continent_name: South America source.geo.region_iso_code: BR-RJ source.geo.city_name: Belford Roxo source.geo.country_iso_code: BR source.geo.region_name: Rio de Janeiro source.geo.location: { "lon": -43.3817, "lat": -22.7856 } source.as.number: 263,033 source.as.organization.name: LINXBR TELECOMUNICACOES LTDA source.address: 177.12.183.140</p> <p>agent.hostname: Webserver-VM agent.id: ba57cc22-81b0-4037-bee8-4c5bbe25a036 agent.type: filebeat agent.ephemeral_id: f4b1e0c5-002d-4f16-934f-4481239ad0c5 agent.version: 7.4.0 log.file.path: /var/log/apache2/access.log log.offset: 44,362 source.geo.continent_name: North America source.geo.country_iso_code: US source.geo.location: { "lon": -97.822, "lat": 37.751 } source.address: 35.150.75.101 source.ip: 35.150.75.101 fileset.name: access url.original: /favicon.ico cloud.instance.name: Webserver-VM cloud.instance.id: 180434bd-f8cc-4757-8776-864065656147 cloud.provider: az</p>
Apr 3, 2024 @ 21:48:57.000	<p>agent.hostname: Webserver-VM agent.id: ba57cc22-81b0-4037-bee8-4c5bbe25a036 agent.type: filebeat agent.ephemeral_id: f4b1e0c5-002d-4f16-934f-4481239ad0c5 agent.version: 7.4.0 log.file.path: /var/log/apache2/access.log log.offset: 43,900 source.geo.continent_name: North America source.geo.country_iso_code: US source.geo.location: { "lon": -97.822, "lat": 37.751 } source.address: 35.150.75.101 source.ip: 35.150.75.101 fileset.name: access url.original: / cloud.instance.name: Webserver-VM cloud.instance.id: 180434bd-f8cc-4757-8776-864065656147 cloud.provider: az cloud.machine.type: Standard_B1s</p>
Apr 3, 2024 @ 21:48:57.000	<p>agent.hostname: Webserver-VM agent.id: ba57cc22-81b0-4037-bee8-4c5bbe25a036 agent.type: filebeat agent.ephemeral_id: f4b1e0c5-002d-4f16-934f-4481239ad0c5 agent.version: 7.4.0 log.file.path: /var/log/apache2/access.log log.offset: 44,129 source.geo.continent_name: North America source.geo.country_iso_code: US source.geo.location: { "lon": -97.822, "lat": 37.751 } source.address: 35.150.75.101 source.ip: 35.150.75.101 fileset.name: access url.original: /icons/ubuntu-logo.png cloud.instance.name: Webserver-VM cloud.instance.id: 180434bd-f8cc-4757-8776-864065656147 cloud.provider: az</p>
Apr 3, 2024 @ 21:48:44.000	<p>agent.hostname: Webserver-VM agent.id: ba57cc22-81b0-4037-bee8-4c5bbe25a036 agent.type: filebeat agent.ephemeral_id: f4b1e0c5-002d-4f16-934f-4481239ad0c5 agent.version: 7.4.0 log.file.path: /var/log/apache2/access.log log.offset: 43,417 source.geo.continent_name: Africa source.geo.country_iso_code: MU source.geo.location: { "lon": 57.55, "lat": -20.2833 } source.as.number: 23,889 source.as.organization.name: MauritiusTelecom source.address: 102.115.83.151 source.ip: 102.115.83.151 fileset.name: access url.original: /ip cloud.instance.name: Webserver-VM cloud.instance.id: 180434bd-f8cc-4757-8776-</p>
Apr 3, 2024 @ 21:48:44.000	<p>agent.hostname: Webserver-VM agent.id: ba57cc22-81b0-4037-bee8-4c5bbe25a036 agent.type: filebeat agent.ephemeral_id: f4b1e0c5-002d-4f16-934f-4481239ad0c5 agent.version: 7.4.0 log.file.path: /var/log/apache2/access.log log.offset: 43,630 source.geo.continent_name: Africa source.geo.country_iso_code: ET source.geo.location: { "lon": 38, "lat": 8 } source.as.number: 24,757 source.as.organization.name: Ethiopian Telecommunication Corporation source.address: 196.191.221.46 source.ip: 196.191.221.46 fileset.name: access url.original: http://20.172.210.142/favicon.ico cloud.instance.name: Webserver-</p>

3.3.1 Screenshot

Create an alert for DoS attack.

Watcher

Watcher docs

Watch for changes or anomalies in your data and take action if needed.

Search...

Create

ID	Name	State	Last fired	Last triggered	Comment	Actions
d7eec75f-6edc-4aff-aaa0-3e24e853e5f7	DoS Attack	OK		a minute ago		

Management / Watcher / Edit

Elasticsearch

Index Management

Index Lifecycle Policies

Rollup Jobs

Transforms

Cross-Cluster Replication

Remote Clusters

Watcher

Snapshot and Restore

License Management

B.D Upgrade Assistant

Kibana

Index Patterns

Saved Objects

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-7.4.0-2024.04.07-000001

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 5 FOR THE LAST 1 minute

3.3.2 Screenshot

Create an alert for Brute Force attack.

Watcher

Watcher docs

Watch for changes or anomalies in your data and take action if needed.

Search...

Create

ID	Name	State	Last fired	Last triggered	Comment	Actions
<input type="checkbox"/> 6b440ec4-6127-4de6-ba29-db2dc8086ed2	Brute Force Attack	✓ OK		a minute ago		

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

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-7.4.0-2024.04.07-000001 x

Time field

@timestamp

Run watch every

1

minute

Use * to broaden your query.

Match the following condition

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

3.3.3 Screenshot

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

Watcher

Watcher docs

Watch for changes or anomalies in your data and take action if needed.

Search...

Create

ID	Name	State	Last fired	Last triggered	Comment	Actions
7f51fb06-07b6-4f5c-8a4c-84c301b892cd	Port Scan Attack	OK		a few seconds ago		

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

Edit Port Scan Attack

Send an alert when your specified condition is met. Your watch will run every 30 seconds.

Name

Port Scan Attack

Indices to query

filebeat-7.4.0-2024.04.07-000001

Time field

@timestamp

Run watch every

30

seconds

Match the following condition

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

3.4 Incident Response Playbook

Alert: Denial of Service (DoS) Attack

Initial Identification and Verification:

Upon receiving an alert for a potential DoS attack, the first step is to verify the alert and confirm if it indeed indicates a DoS attack.

Utilize SIEM logs, network traffic analysis, and any other available sources to corroborate the alert.

Containment and Mitigation:

Implement network filtering or access control lists (ACLs) to block or limit traffic from the attacking source(s).

If possible, work with upstream service providers to filter out malicious traffic before it reaches your network.

Consider deploying anti-DDoS solutions or services to absorb or mitigate the attack traffic.

Communication and Notification:

Notify relevant stakeholders, including IT security teams, network administrators, and management, about the ongoing DoS attack.

Provide updates on the situation and any actions being taken to mitigate the impact.

Investigation and Root Cause Analysis:

Conduct a thorough investigation to determine the root cause of the DoS attack.

Analyze SIEM logs, network traffic data, and any other relevant sources to identify the attack vectors and potential vulnerabilities exploited.

Remediation and Recovery:

Apply necessary patches or configurations to address vulnerabilities exploited during the attack.

Consider implementing additional security controls, such as rate limiting or traffic shaping, to prevent future DoS attacks.

Restore affected services to normal operation and monitor for any residual effects.

Alert: Brute Force Attack

Initial Identification and Verification:

Upon receiving an alert for a potential brute force attack, verify the alert and determine if it indicates a genuine brute force attempt.

Containment and Mitigation:

Temporarily block the IP address(es) associated with the brute force attempt.
Strengthen authentication mechanisms by implementing account lockout policies or multi-factor authentication (MFA) where applicable.

Communication and Notification:

Notify relevant stakeholders, including system administrators and affected users, about the ongoing brute force attack. Emphasize the importance of strong passwords and encourage users to enable MFA for added security.

Investigation and Root Cause Analysis:

Analyze SIEM logs and authentication records to determine the scope and severity of the brute force attack. Identify any vulnerable accounts or services targeted by the attackers.

Remediation and Recovery:

Reset passwords for compromised accounts and perform a security review to ensure no unauthorized access. Consider implementing intrusion detection/prevention systems (IDS/IPS) to detect and block brute force attempts in real-time.
Conduct security awareness training for users to educate them about the risks of weak passwords and the importance of secure authentication practices.

Alert: Scanning and Reconnaissance Attempt

Initial Identification and Verification:

Upon receiving an alert for scanning and reconnaissance activity, verify the alert and confirm if it indicates malicious behavior.

Containment and Mitigation:

Monitor and analyze network traffic to identify the source of the scanning activity.
Implement firewall rules or network segmentation to limit the attacker's ability to scan and gather information.

Communication and Notification:

Notify relevant stakeholders, including network and system administrators, about the scanning and reconnaissance attempt.
Emphasize the need for heightened vigilance and monitoring to detect any further suspicious activity.

Investigation and Root Cause Analysis:

Analyze SIEM logs and network traffic data to identify the targets and methods used by the attackers during the scanning and reconnaissance phase.
Determine if any vulnerabilities were identified during the reconnaissance phase and prioritize patching or mitigation efforts accordingly.

Remediation and Recovery:

Patch or mitigate identified vulnerabilities to prevent exploitation by potential attackers.
Implement network security controls, such as intrusion detection systems (IDS) or endpoint detection and response (EDR) solutions, to detect and block future scanning attempts.
Review and update network configurations and access controls to minimize the risk of unauthorized access or exploitation.

Most important:

Continuously update and refine the incident response playbook based on lessons learned from past incidents and emerging threats.

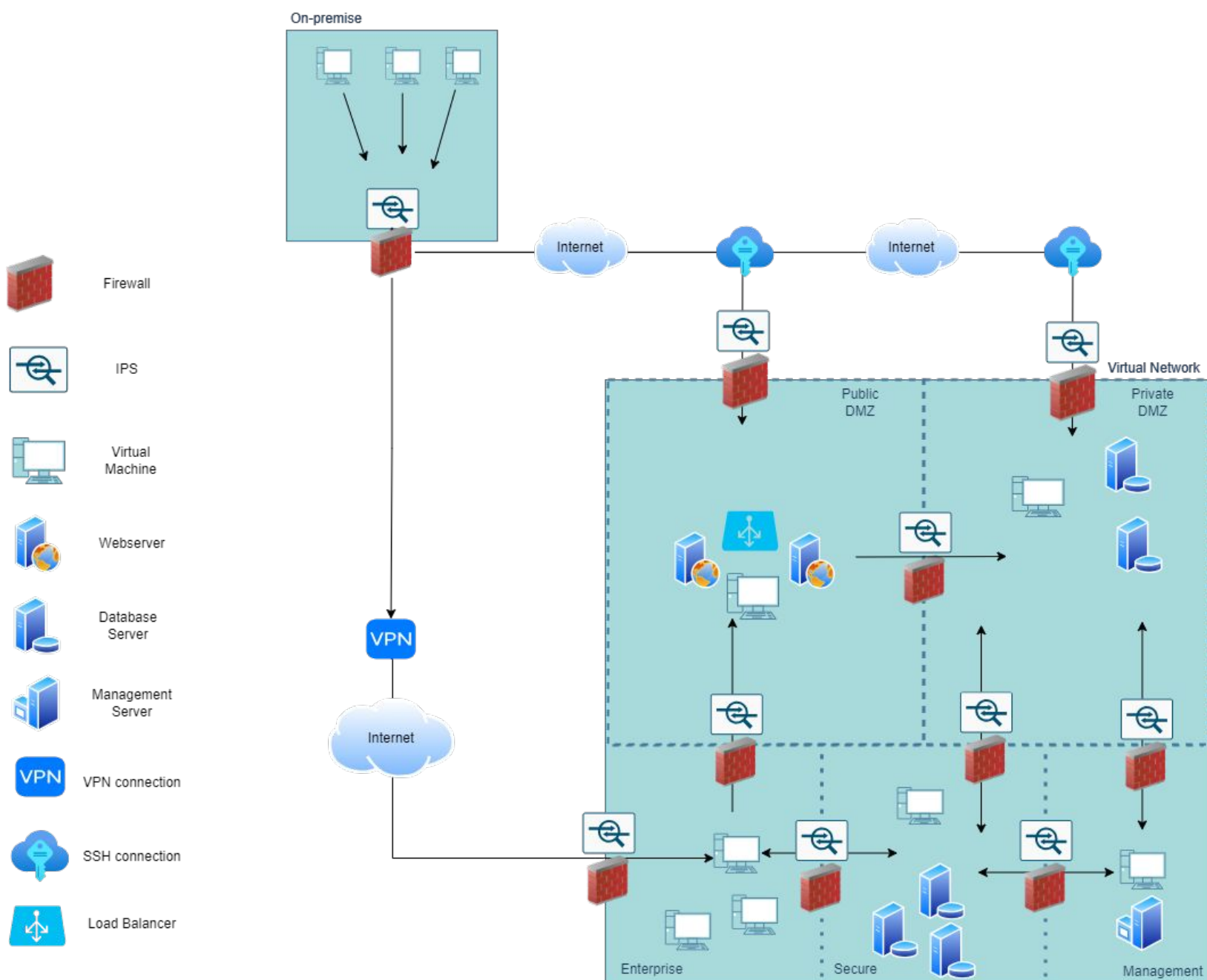


Section 4

Designing a Zero Trust Model

4.1 Zero Trust Model

Paste your Zero Trust model diagram here:



4.2 Modern Architecture vs. Zero Trust

Zero Trust Model vs. Modern Security Architecture

Zero Trust Model:

Core Principle:

Zero Trust: The fundamental principle of Zero Trust is to never trust, always verify. It assumes that threats can come from both inside and outside the network perimeter, thus requiring continuous verification of identity, device health, and other contextual factors before granting access to resources.

Key Emphasis: Identity-centric security, strict access controls, and continuous monitoring are the key elements of a Zero Trust model.

Access Control:

Zero Trust: Access control is based on the principle of least privilege, where users and devices are granted only the minimum level of access required to perform their tasks. Access decisions are made dynamically based on user identity, device health, location, and other contextual attributes.

Key Mechanisms: Role-based access control (RBAC), conditional access policies, and micro-segmentation are commonly used to enforce access control in Zero Trust environments.

Network Segmentation:

Zero Trust: Network segmentation is a critical component of Zero Trust architecture, where the network is divided into smaller segments or zones based on security requirements. Traffic between segments is strictly controlled and inspected, reducing the risk of lateral movement by attackers.

Key Focus: Granular control over network traffic flows, with policies enforced at the application and workload level rather than relying solely on perimeter defenses.

Trust Boundaries:

Zero Trust: Zero Trust does not rely on traditional network trust boundaries, such as perimeter firewalls, to protect assets. Instead, trust is established on a per-session basis, with authentication and authorization enforced at every interaction, regardless of the network location.

Boundaryless Security: Zero Trust extends security controls to every endpoint, workload, and data source, regardless of their location within or outside the corporate network.

Monitoring and Analytics:

Zero Trust: Continuous monitoring and behavioral analytics are essential for detecting and responding to threats in real-time within a Zero Trust model. Security telemetry from endpoints, networks, and applications is collected and analyzed to identify suspicious activities and anomalies.

Key Tools: Security Information and Event Management (SIEM) solutions, User and Entity Behavior Analytics (UEBA), and threat intelligence feeds are used to enhance detection and response capabilities.

Modern Security Architecture:

Incorporating Legacy Elements:

Modern Security Architecture: While modern security architecture may adopt Zero Trust principles, it often incorporates legacy security elements, such as perimeter-based defenses like firewalls and VPNs. These elements may still play a role in enforcing security policies and controlling traffic flows.

Hybrid Approach: Modern security architectures may blend traditional perimeter defenses with Zero Trust principles to create a hybrid approach that provides defense-in-depth while enabling more granular access controls and visibility.

Focus on Cloud and Mobility:

Modern Security Architecture: With the proliferation of cloud services and mobile devices, modern security architectures place a strong emphasis on securing data and applications regardless of their location. This includes implementing cloud-native security controls, such as cloud access security brokers (CASBs) and identity federation, to protect cloud-hosted resources.

Adaptability: Modern security architectures are designed to be agile and adaptable, capable of securing diverse environments spanning on-premises, cloud, and hybrid infrastructures.

Integration with DevOps Practices:

Modern Security Architecture: Modern security architectures align with DevOps practices to integrate security into the software development lifecycle (SDLC). This involves implementing security automation, continuous integration/continuous deployment (CI/CD) pipelines, and infrastructure-as-code (IaC) to embed security controls early in the development process.

Shift Left Approach: By shifting security left in the development process, modern architectures aim to identify and remediate vulnerabilities earlier, reducing the risk of security incidents in production environments.

User Experience and Productivity:

Modern Security Architecture: Balancing security with user experience and productivity is a key consideration in modern architectures. This involves implementing frictionless authentication mechanisms, such as single sign-on (SSO) and passwordless authentication, to enhance user convenience while maintaining security.

Contextual Access: Modern security architectures leverage contextual information, such as user behavior and device posture, to dynamically adjust security controls and provide seamless access to resources based on risk.

Conclusion:

While modern security architectures may incorporate elements of Zero Trust, they often retain traditional security components and adapt to the evolving landscape of cloud computing, mobility, and DevOps practices. Zero Trust models, on the other hand, represent a paradigm shift towards a more stringent and dynamic approach to security, focusing on identity, least privilege, and continuous monitoring to protect against modern threats. Both approaches aim to enhance security posture and mitigate risks, albeit with different emphases and strategies. Organizations must evaluate their unique requirements and risk profiles to determine the most suitable approach for securing their assets and data in today's dynamic threat landscape.