Project:
Securing the Perimeter

Benjámin Rácskai

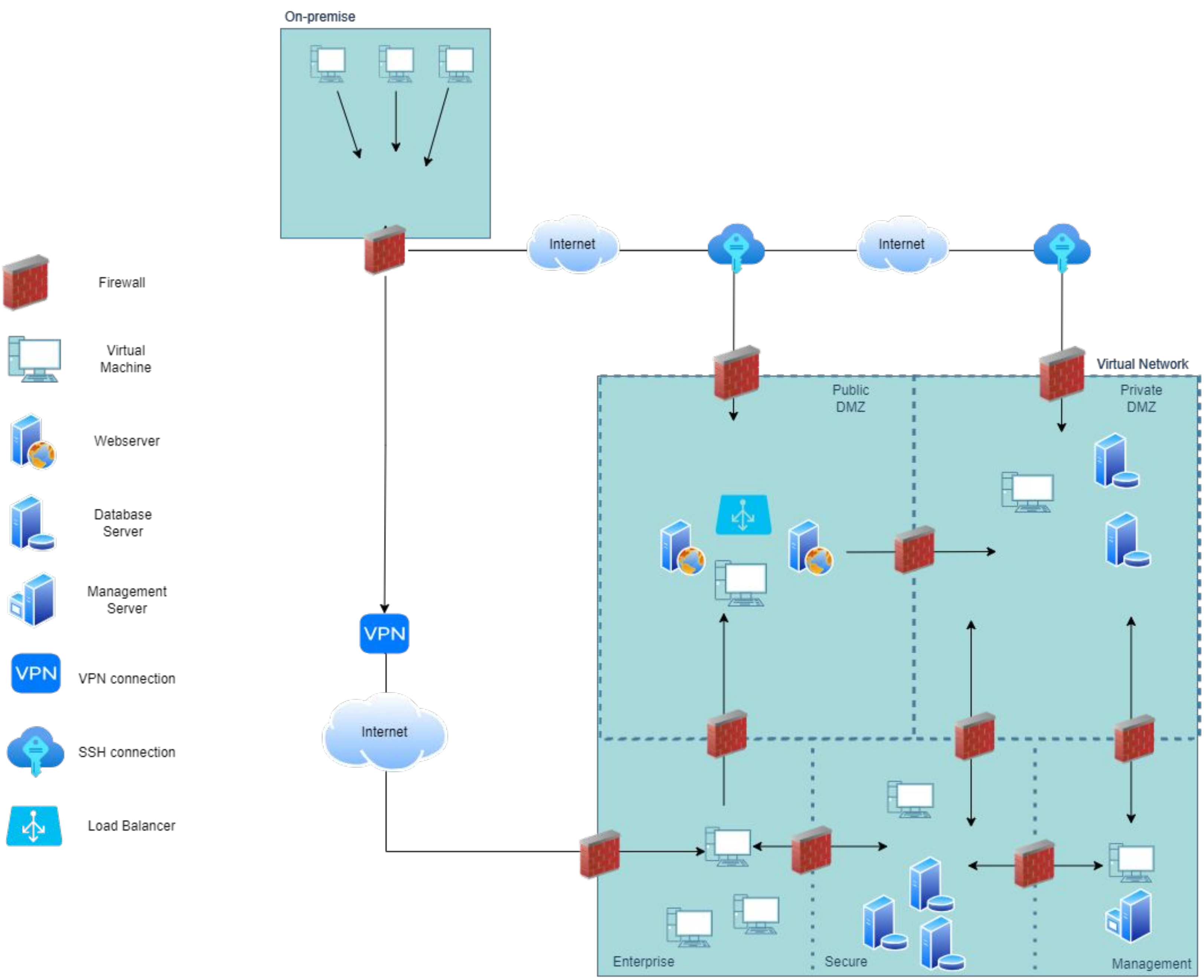
07.04.2024

Section 1

Designing a Secure Network Architecture

1.1 Designing the Network

Paste your Network Diagram here:

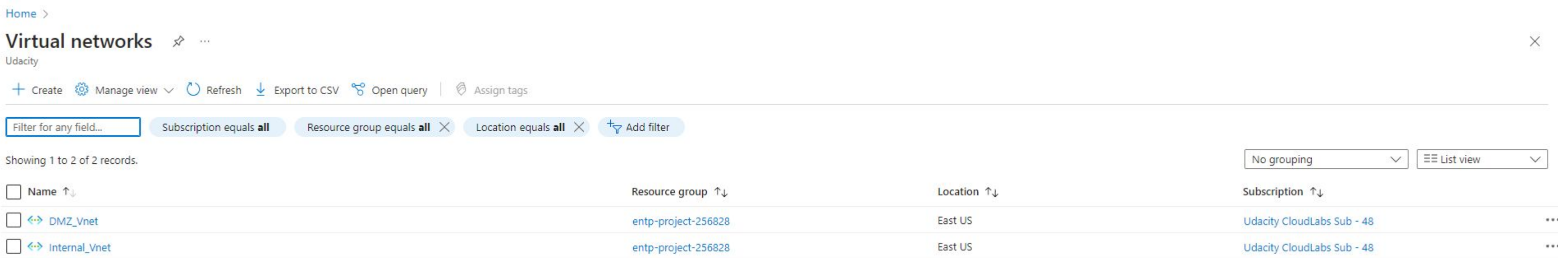


Section 2

Building a Secure Network Architecture in Azure

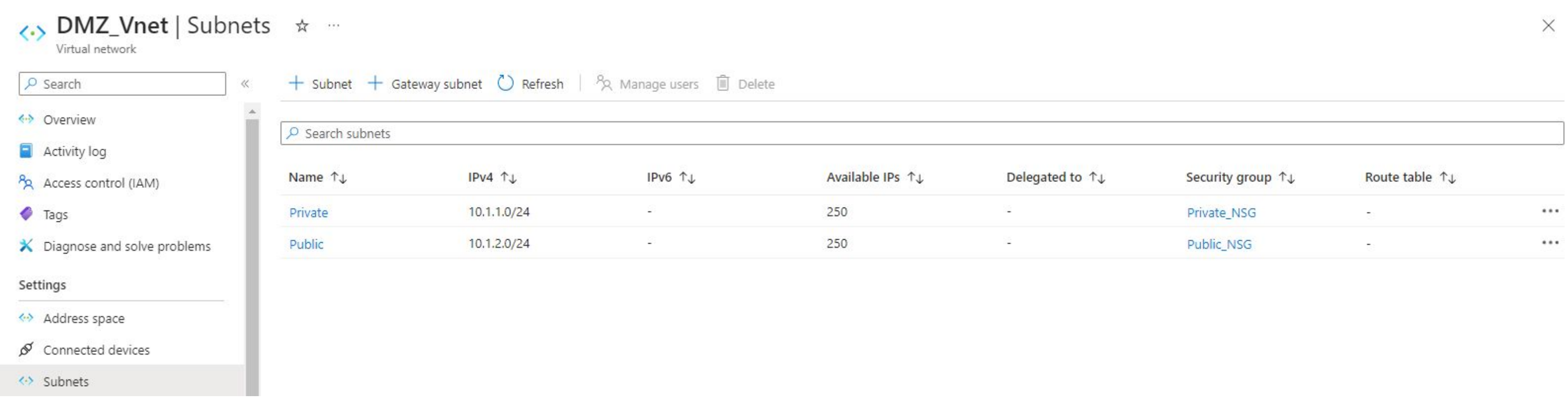
2.1.1 Screenshot

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



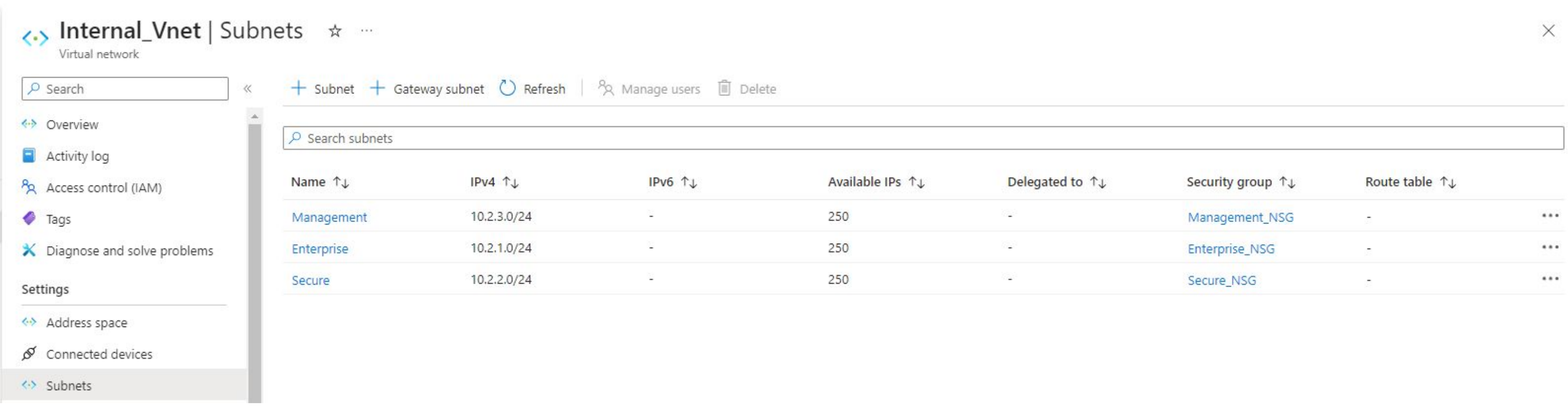
2.1.2 Screenshot

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



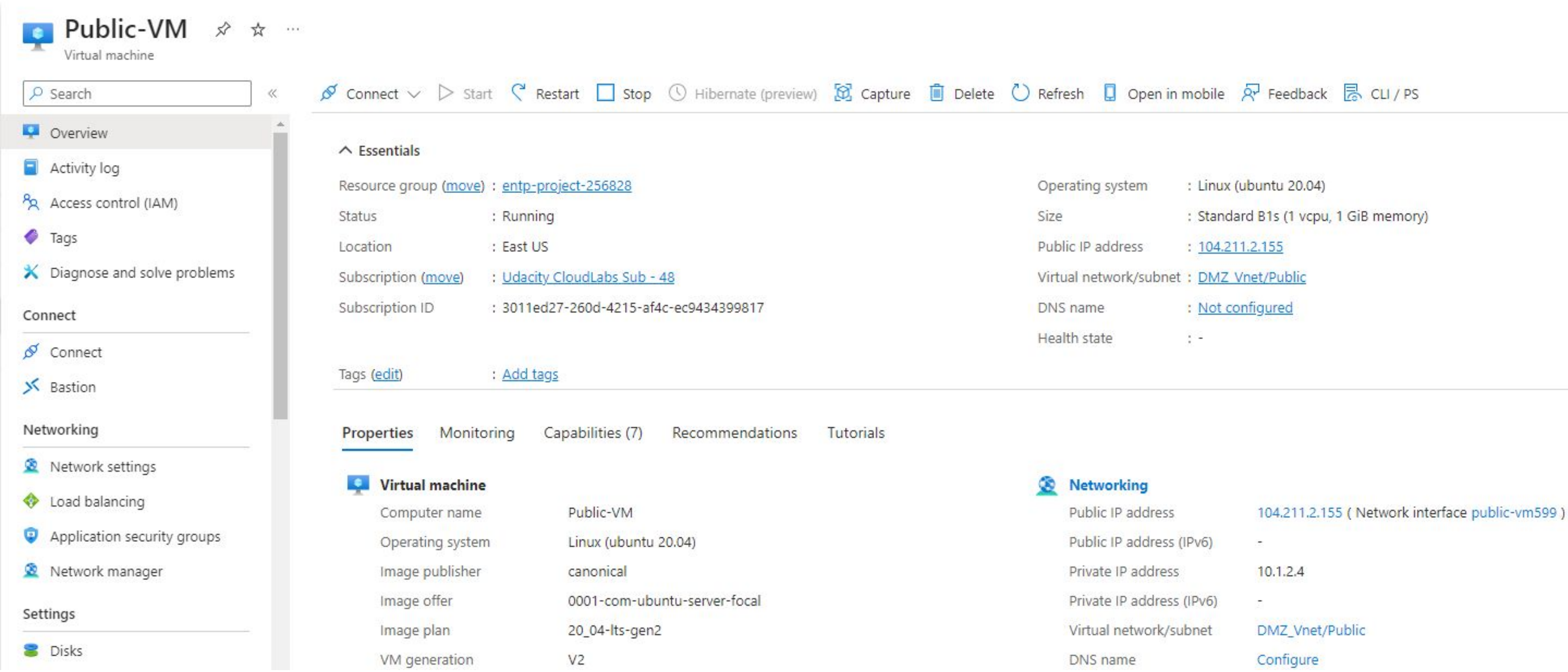
2.1.3 Screenshot

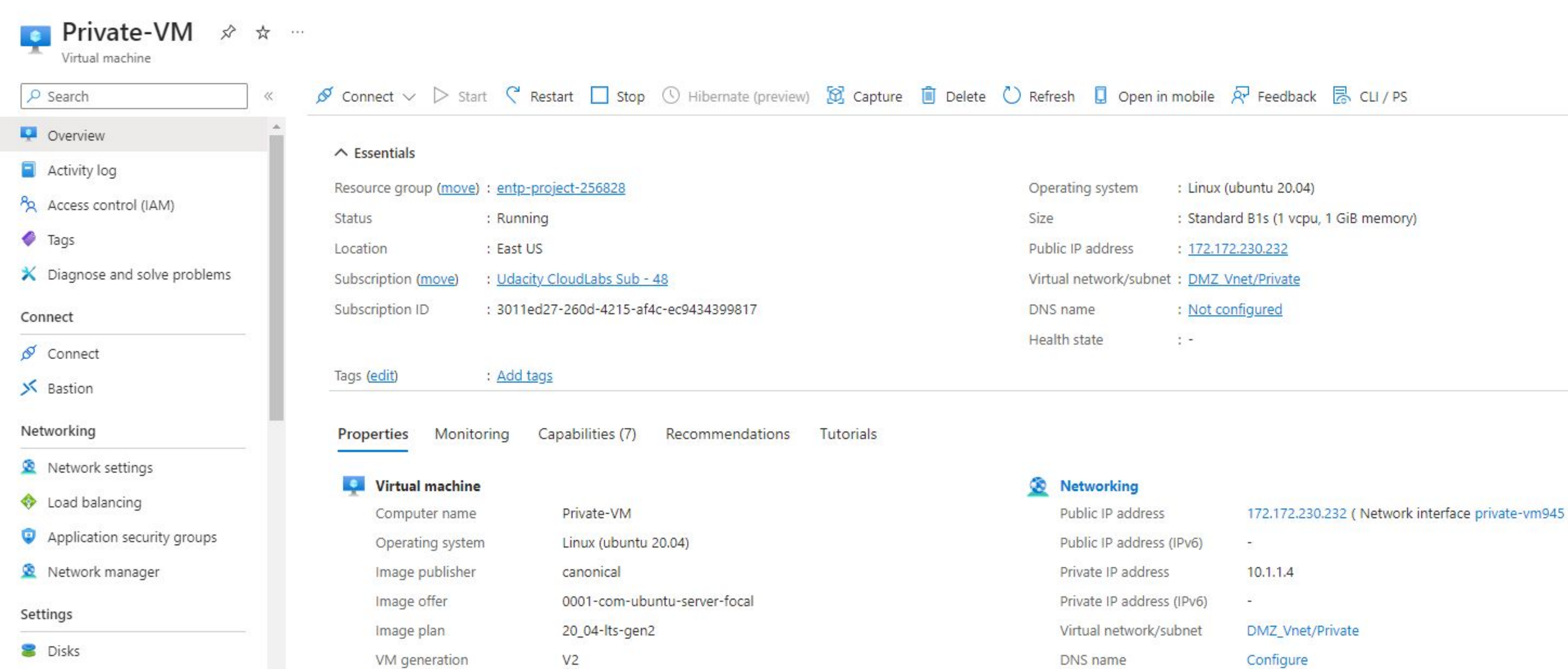
Create three subnets in your internal network and label them Management, Secure, and Enterprise.



2.2.1 Screenshot

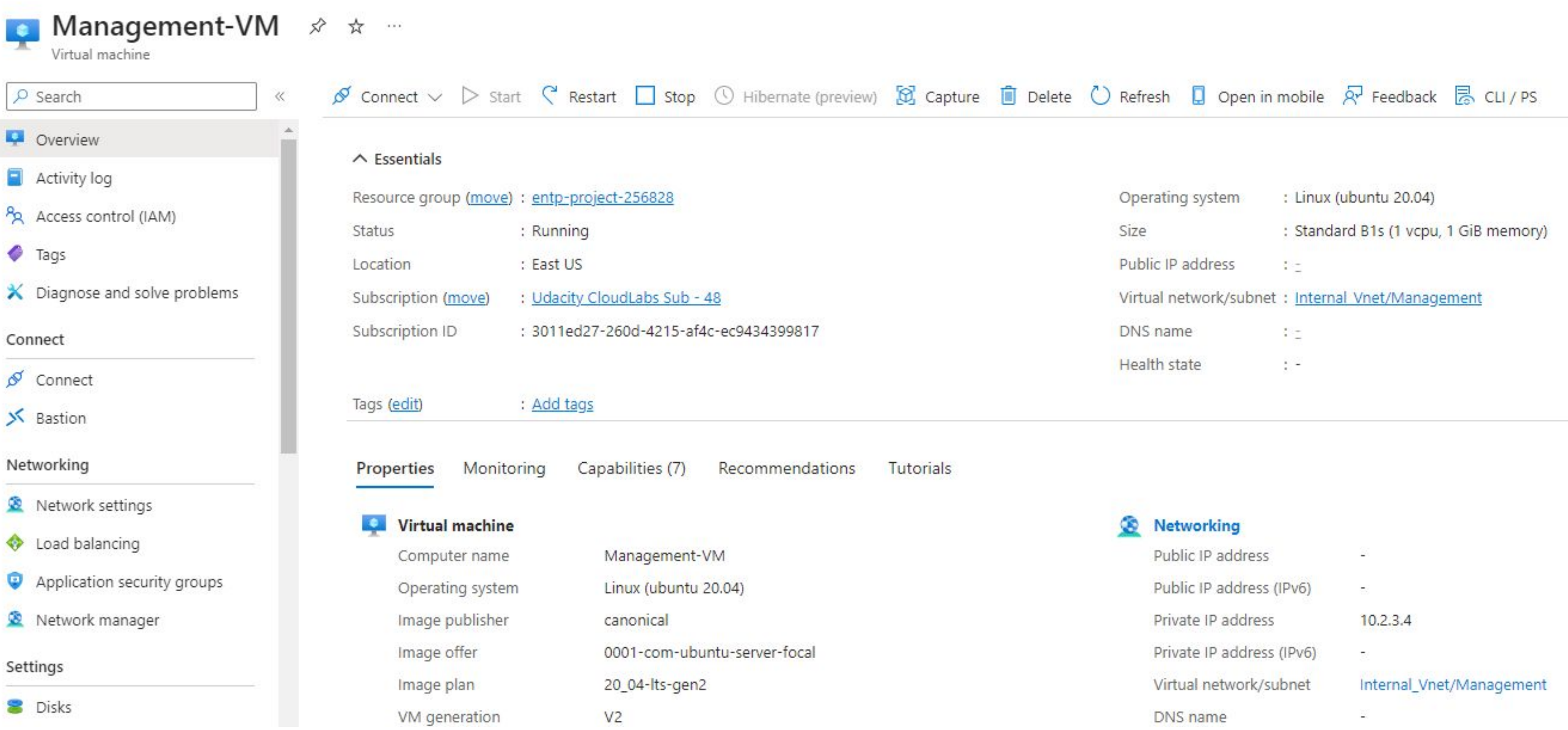
Create one VM in each of your public and private DMZ subnets. Please only use Standard_B1s for your VM size and select the Linux Ubuntu 18.04 image, otherwise you will encounter an error.

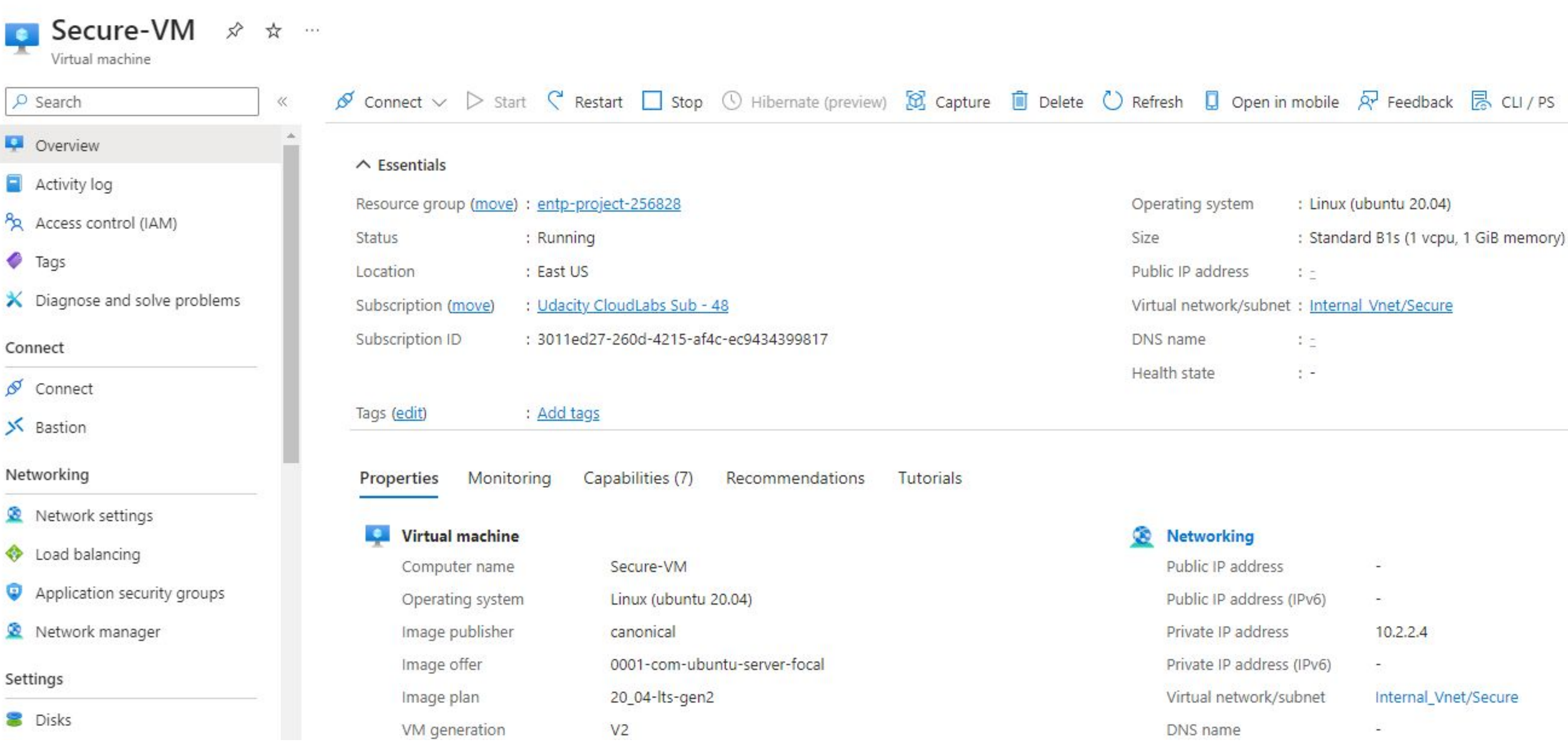


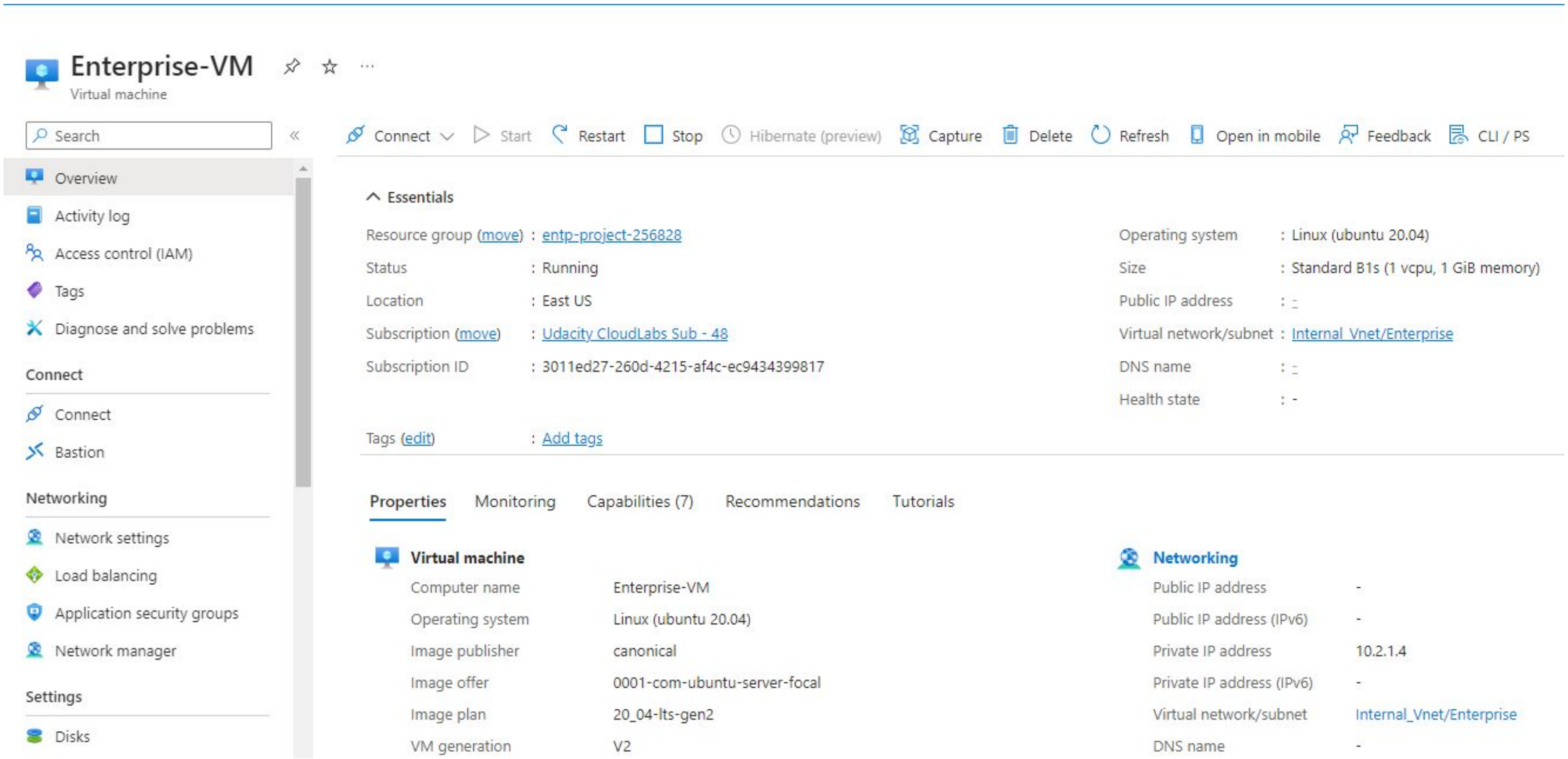


2.2.2 Screenshot

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.

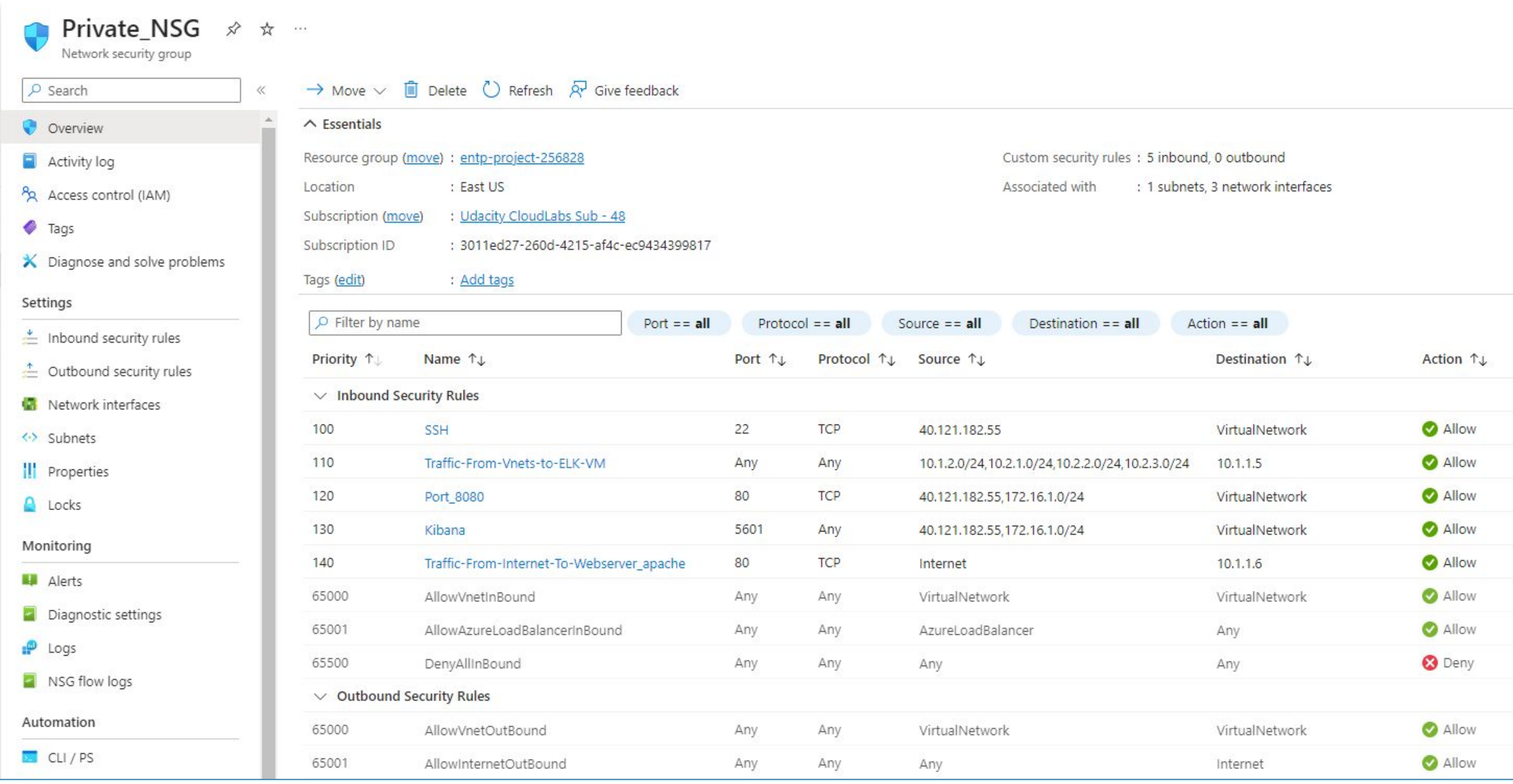




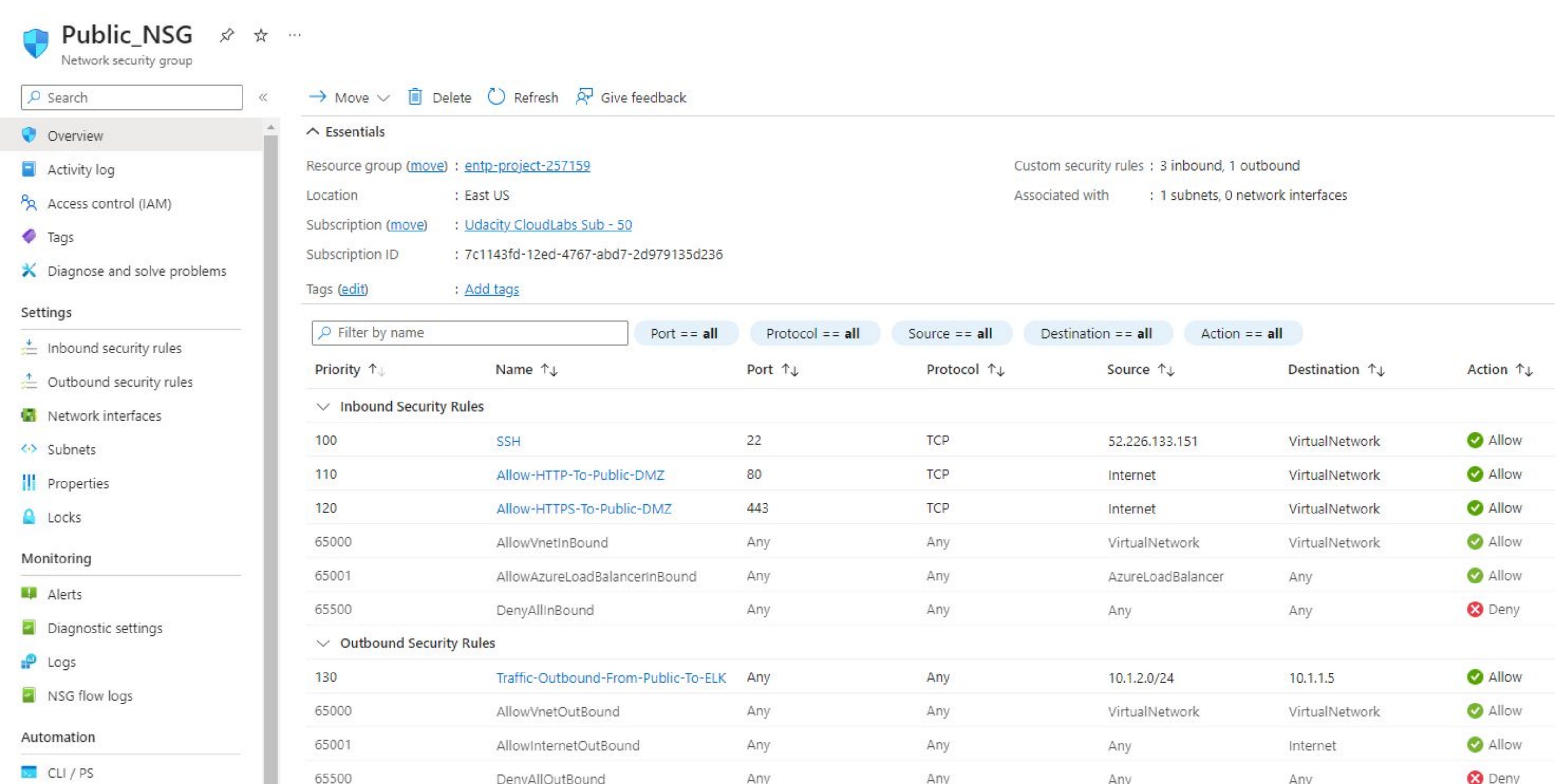

Enterprise-VM
Virtual machine
Search
Connect
Start
Restart
Stop
Hibernate (preview)
Capture
Delete
Refresh
Open in mobile
Feedback
CLI / PS
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Connect
Connect
Bastion
Networking
Network settings
Load balancing
Application security 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 B1s (1 vcpu, 1 GiB memory)
Public IP address : -
Virtual network/subnet : Internal_Vnet/Enterprise
DNS name : -
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.



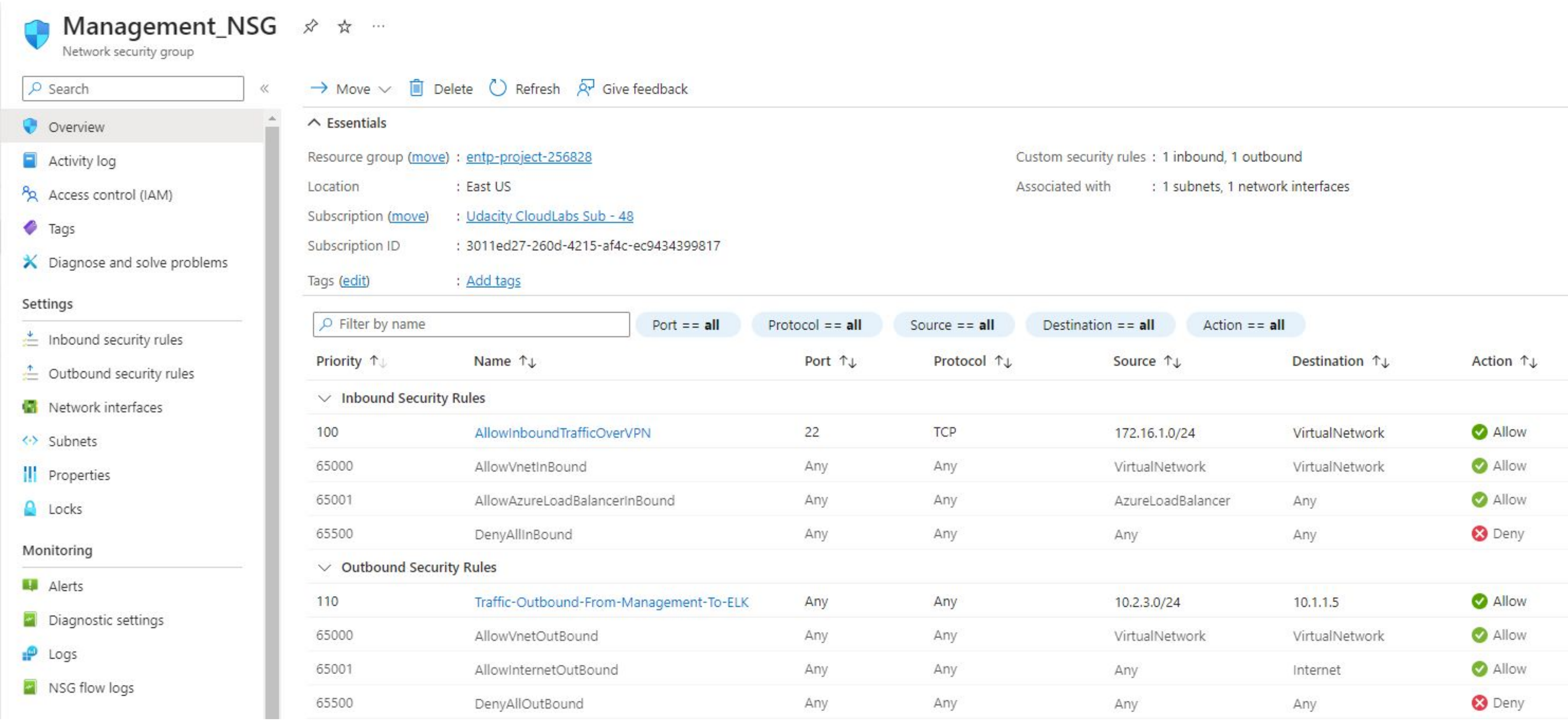
Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
100	SSH	22	TCP	40.121.182.55	VirtualNetwork	Allow
110	Traffic-From-Vnets-to-ELK-VM	Any	Any	10.1.2.0/24,10.2.1.0/24,10.2.2.0/24,10.2.3.0/24	10.1.1.5	Allow
120	Port_8080	80	TCP	40.121.182.55,172.16.1.0/24	VirtualNetwork	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



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
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks

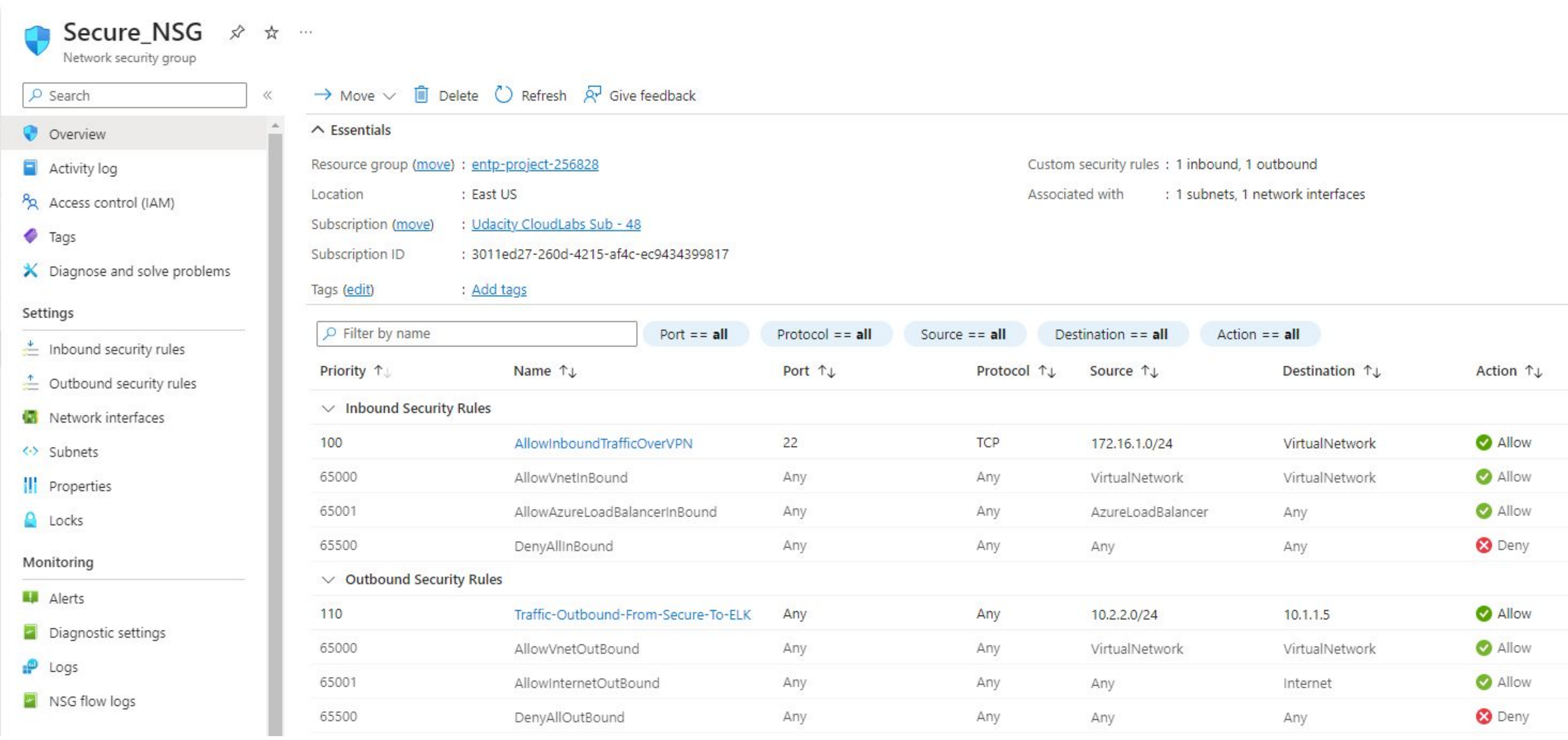
Monitoring
Alerts
Diagnostic settings
Logs
NSG flow logs

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 == 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
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks

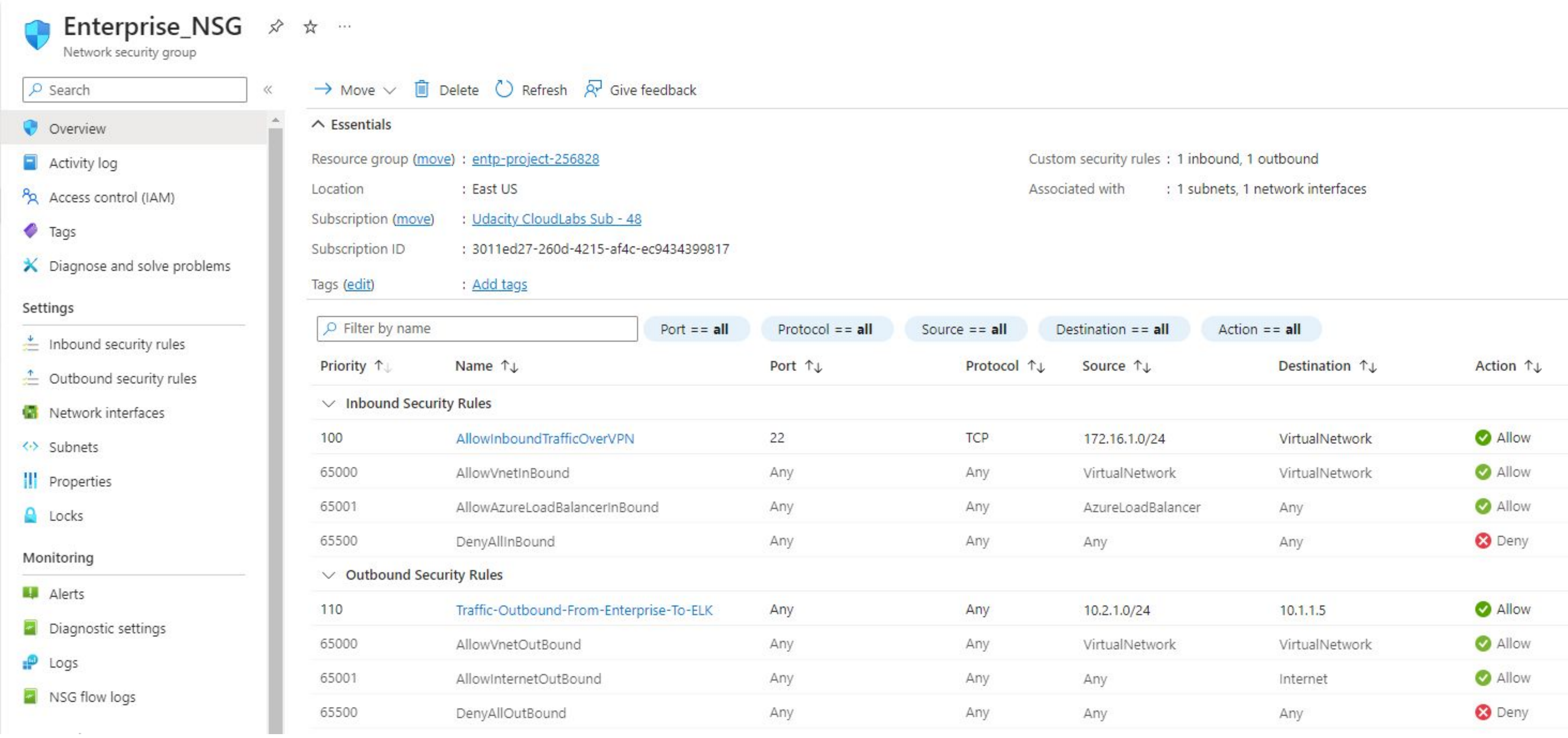
Monitoring
Alerts
Diagnostic settings
Logs
NSG flow logs

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 == all | Protocol == all | Source == all | Destination == all | Action == all

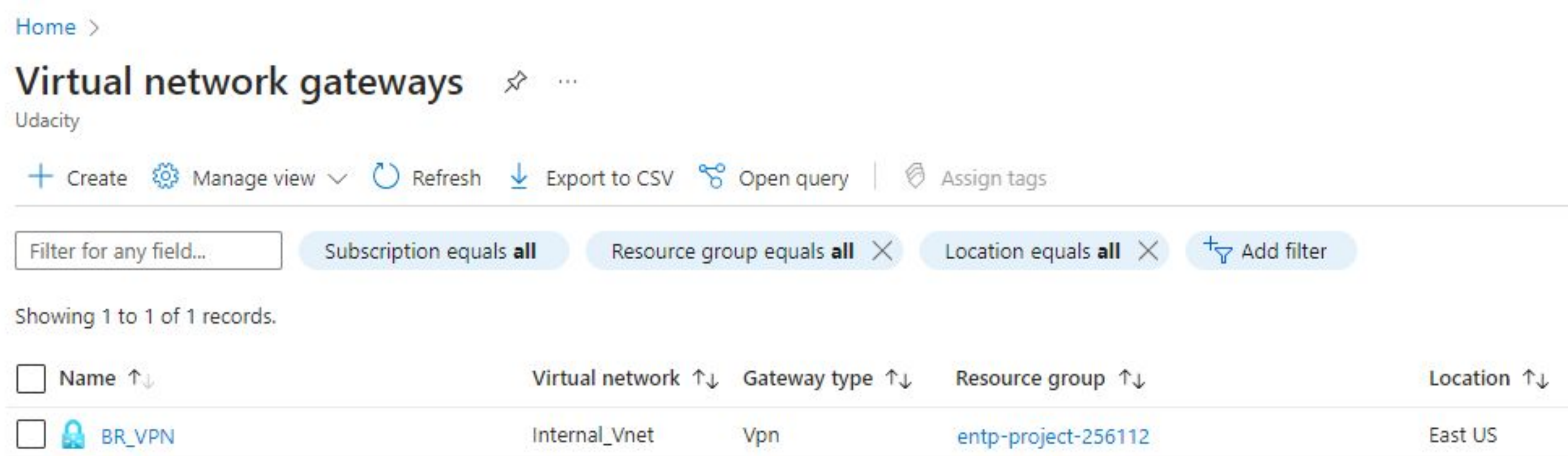
Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
100	AllowInboundTrafficOverVPN	22	TCP	172.16.1.0/24	VirtualNetwork	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	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

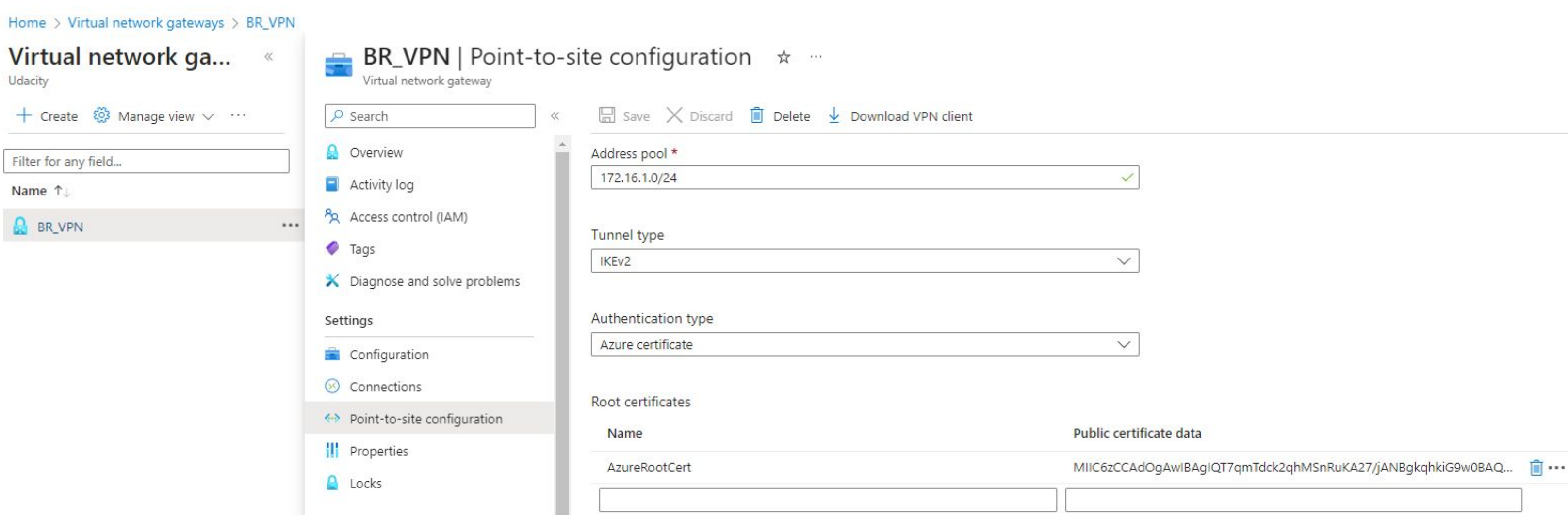


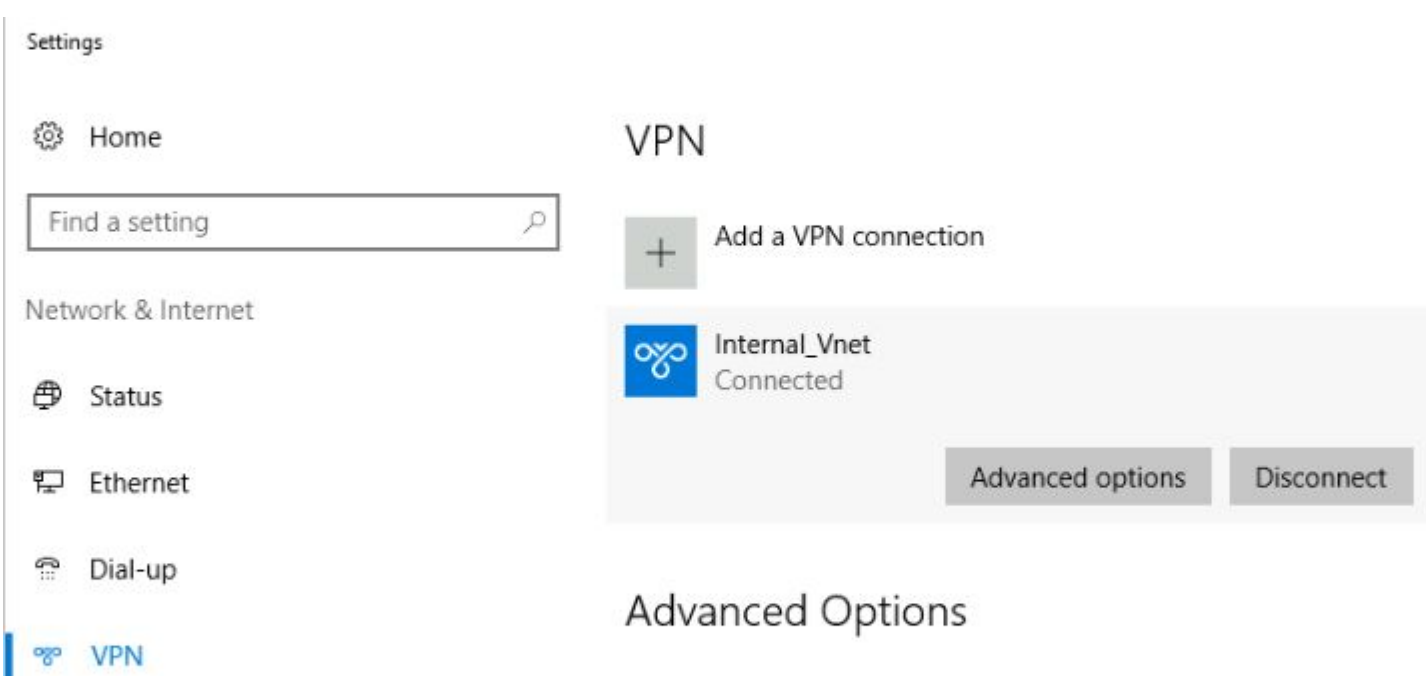
Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
100	AllowInboundTrafficOverVPN	22	TCP	172.16.1.0/24	VirtualNetwork	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	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.

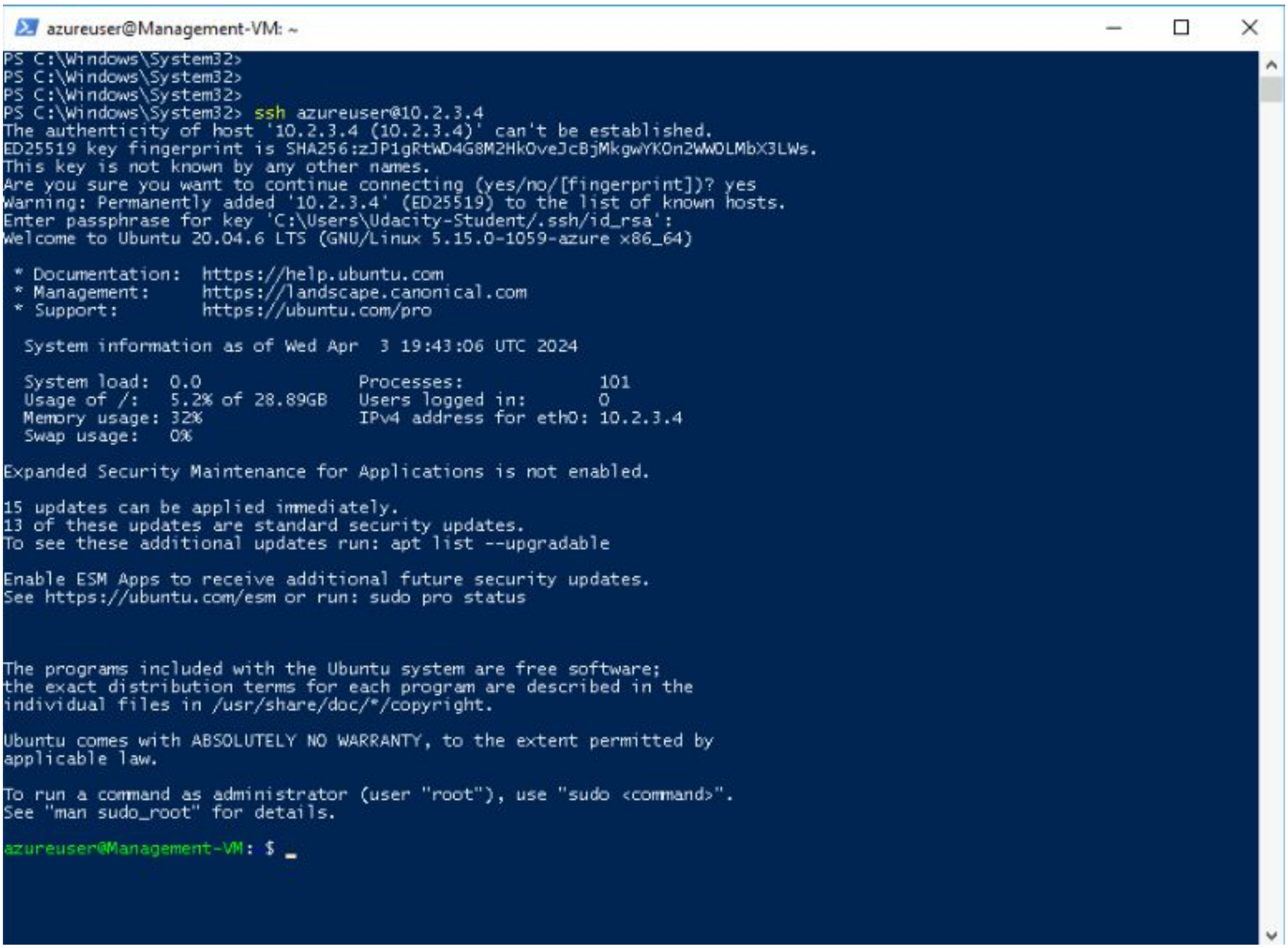






2.4.2 Screenshot

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

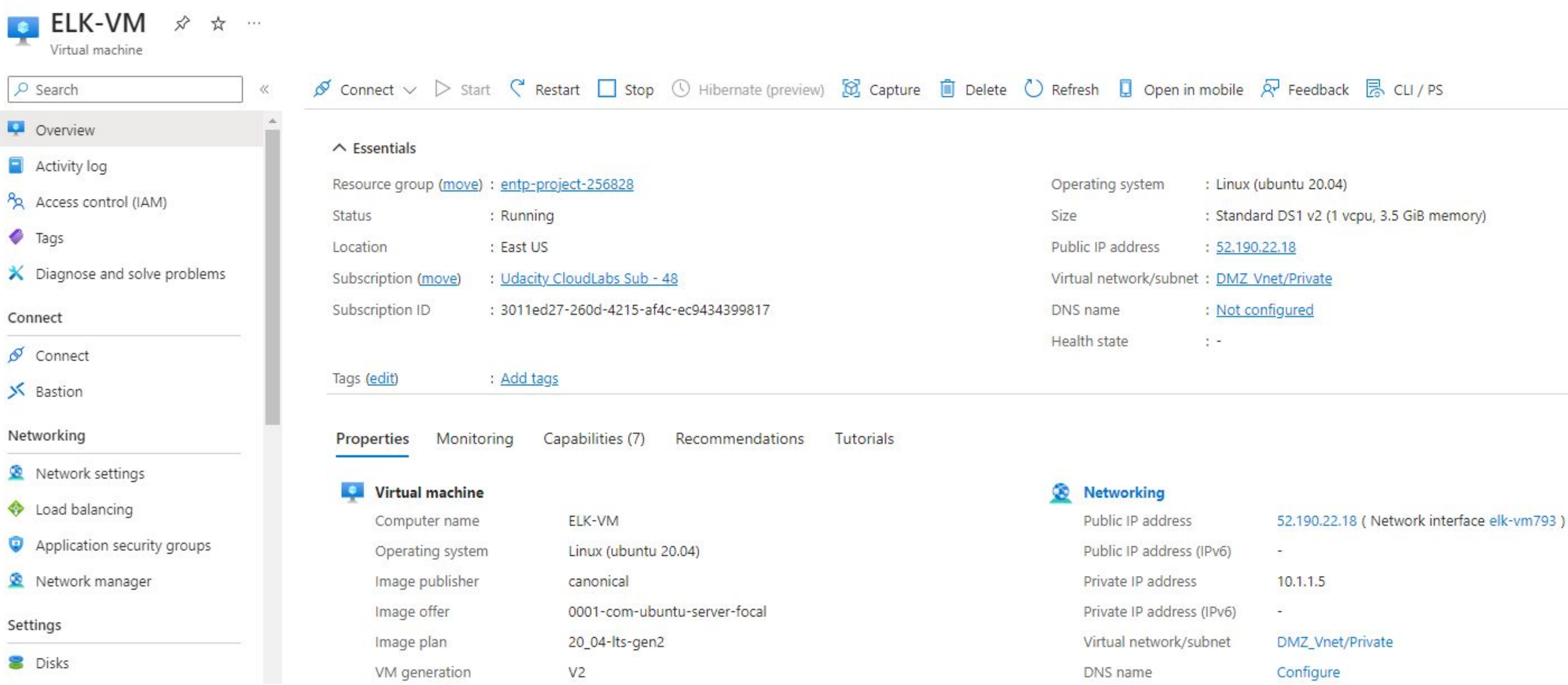


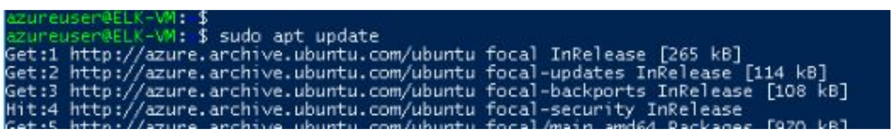
Section 3

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.





```
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 dp
  libasan5 libatomic1 libbinutils libc-dev-bin libc6-dev libcc1-0 libcrypt-dev li
  liblsan0 libmpc3 libpython3-dev libpython3.8-dev libquadmath0 libstdc++-9-dev l
Suggested packages:
  binutils-doc cpp-doc gcc-9-locales debian-keyring g++-multilib g++-9-multilib g
The following NEW packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu build-essential cpp cpp-9 dp
  libasan5 libatomic1 libbinutils libc-dev-bin libc6-dev libcc1-0 libcrypt-dev li
  liblsan0 libmpc3 libpython3-dev libpython3.8-dev libquadmath0 libstdc++-9-dev l
  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
```

```
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->docke
Requirement already satisfied: certifi>=2017.4.17 in /usr/lib/python3/dist-packages (from requests>=2.26.0-
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
```

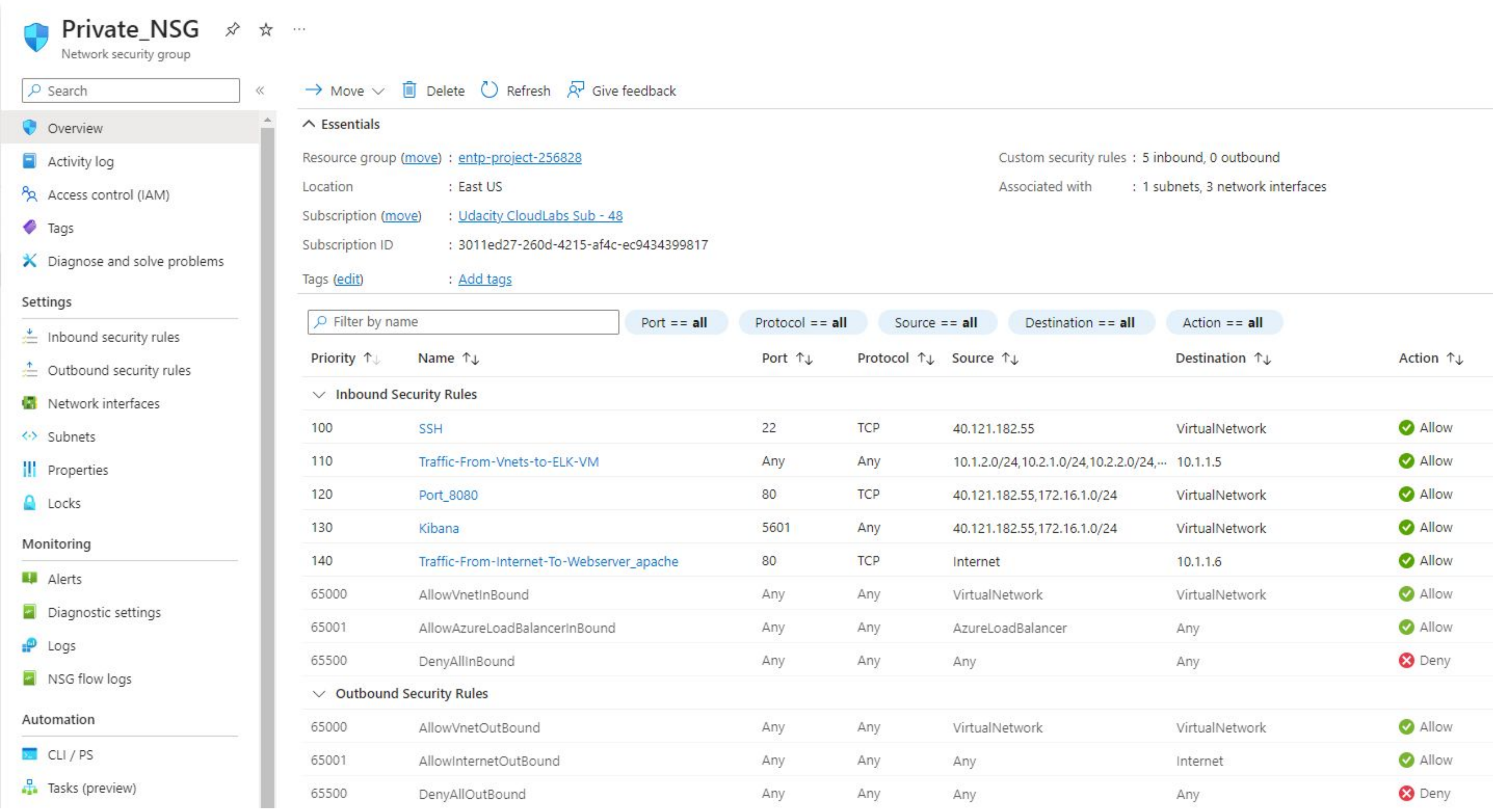
```
azureuser@ELK-VM:~$ sudo docker pull sebp/elk:761
761: Pulling from sebp/elk
c64513b74145: Pull complete
01b8b12bad90: Pull complete
c5d85cf7a05f: Pull complete
b6b268720157: Pull complete
e12192999ff1: Pull complete
d39ece66b667: Pull complete
65599be66378: Pull complete
e691df9ee752: Extracting [==========>                                        ]  26.74MB/131MB
1caea7f89afb: Download complete
c19457083ca7: Download complete
ab24e084844b: 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)
```

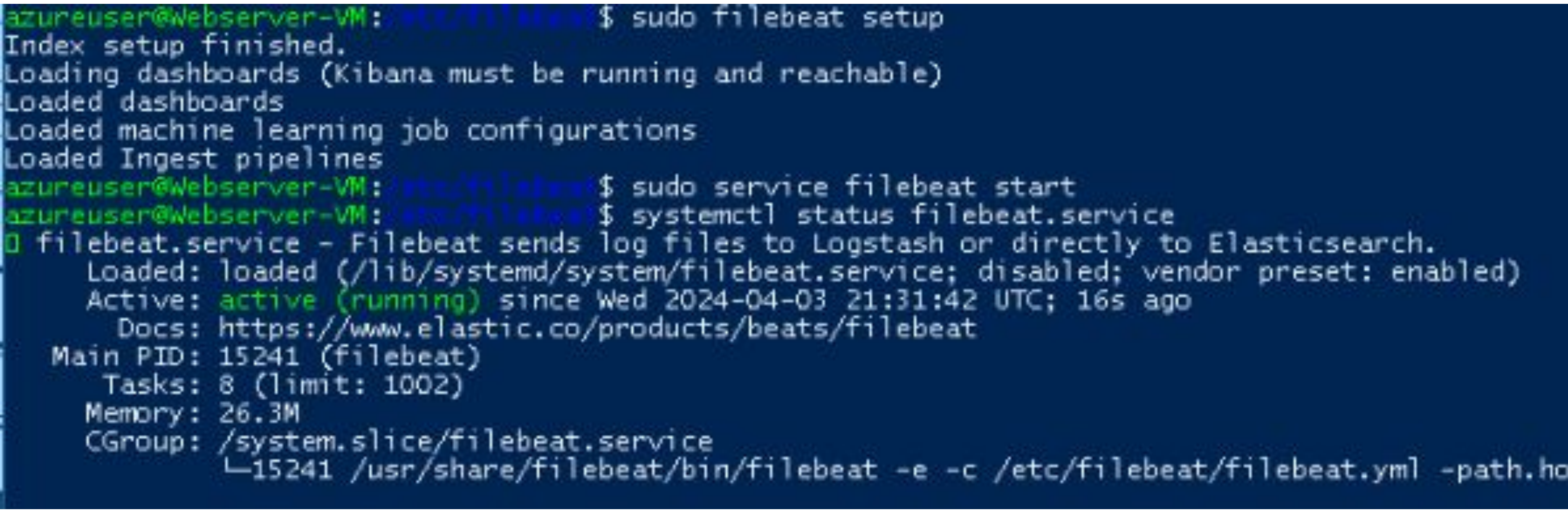
3.1.2 Screenshot

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.



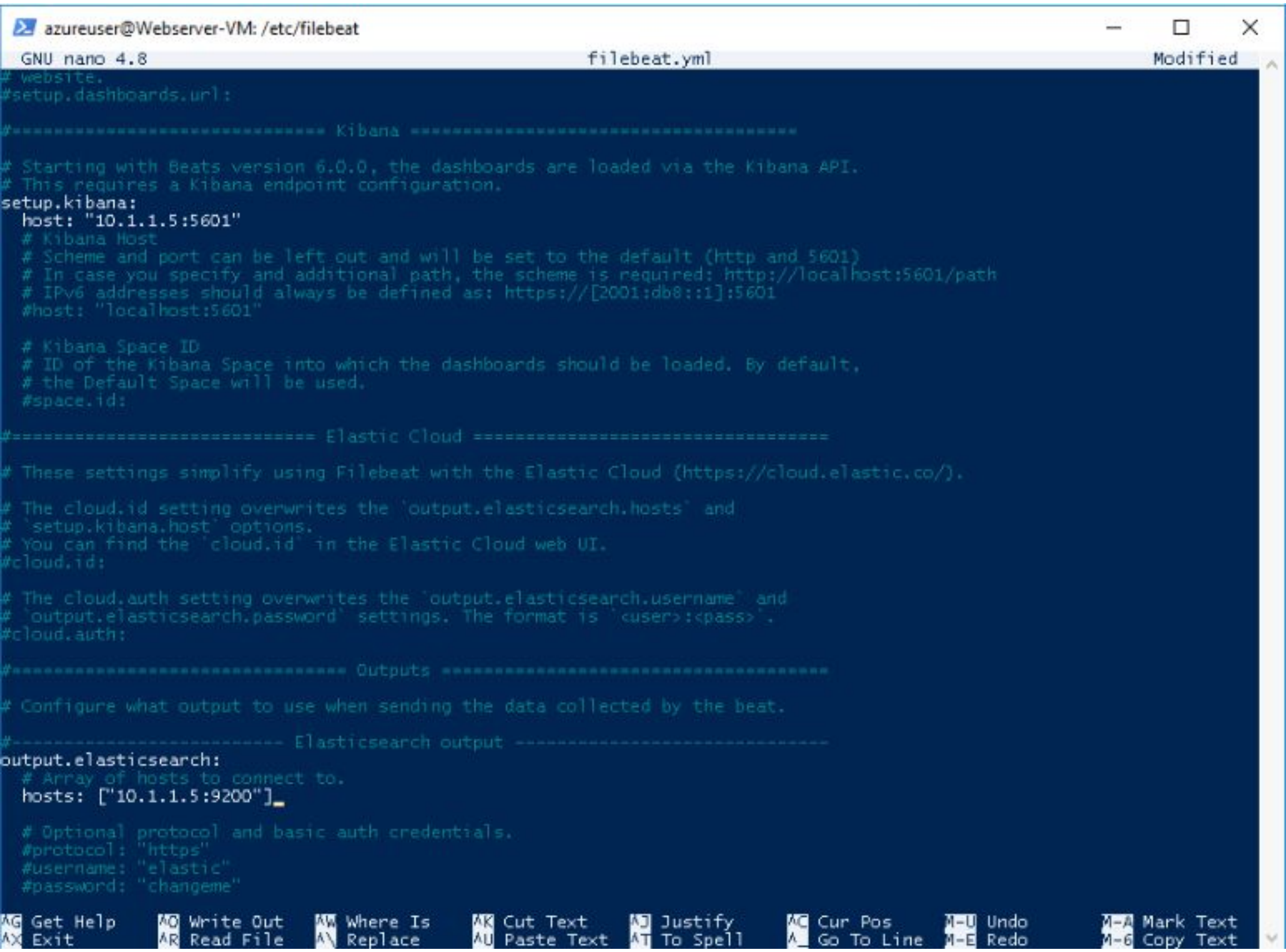
3.2.1 Screenshot

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



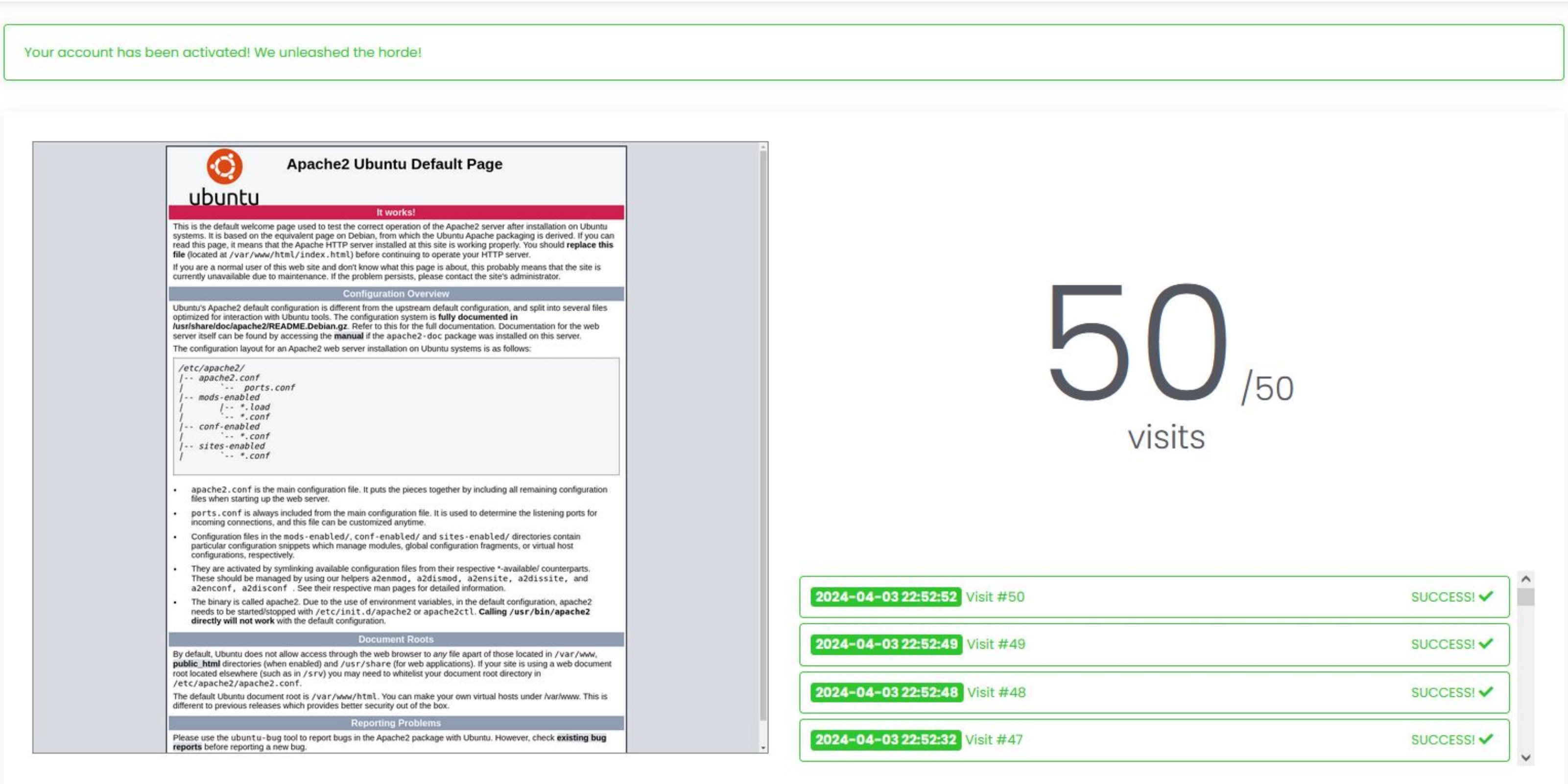
3.2.2 Screenshot

Configure Filebeat to route web server logs to Elasticsearch.



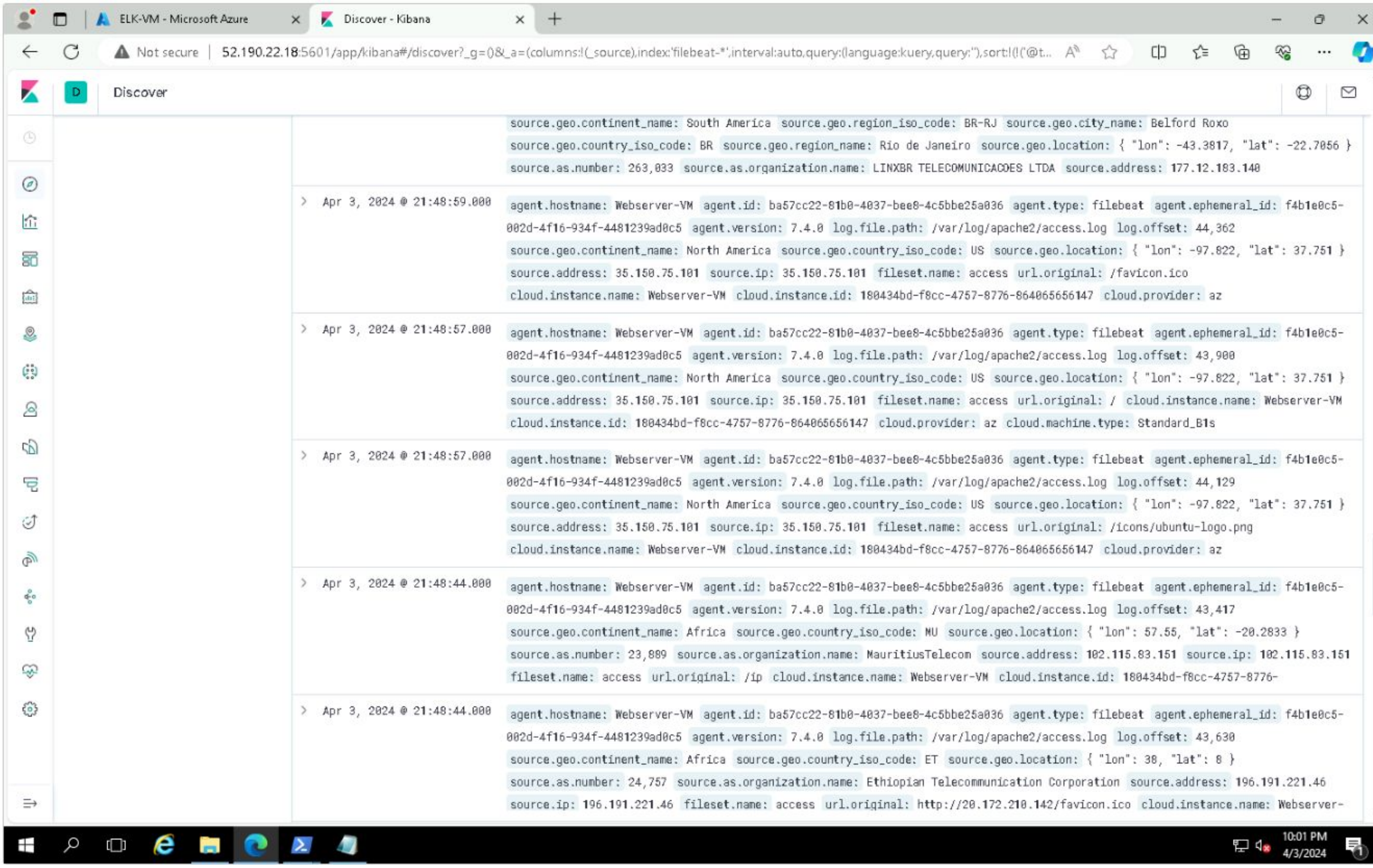
3.2.3 Screenshot

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



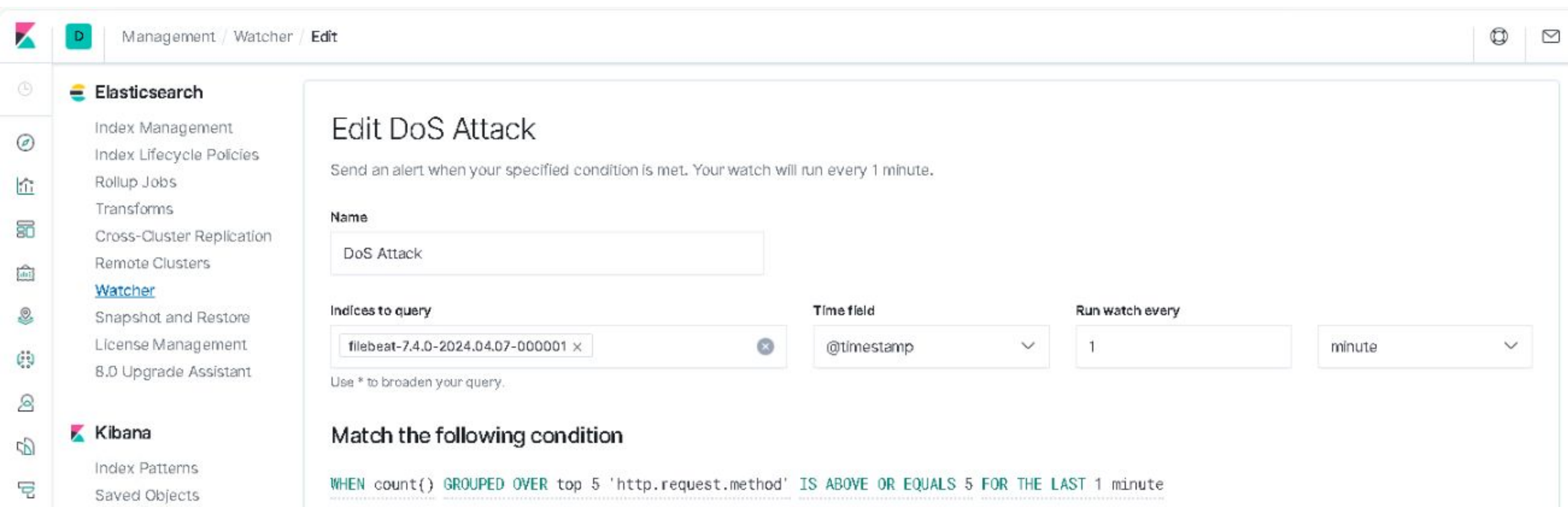
3.2.4 Screenshot

Web server logs appear in Kibana.



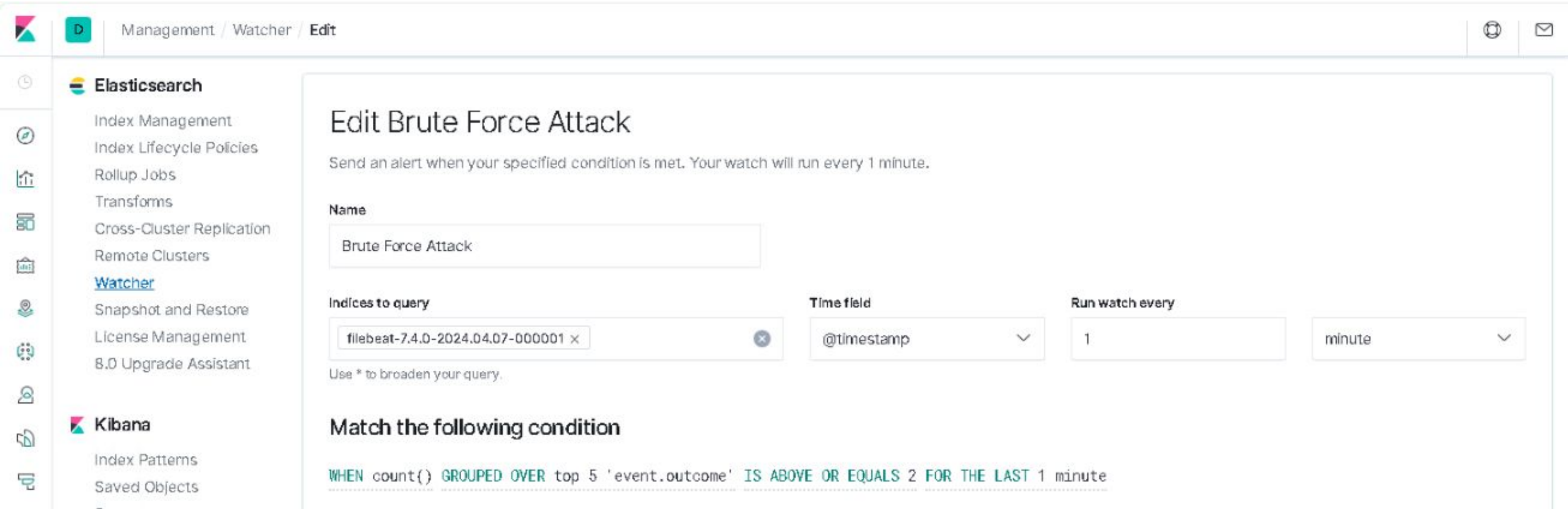
3.3.1 Screenshot

Create an alert for DoS attack.



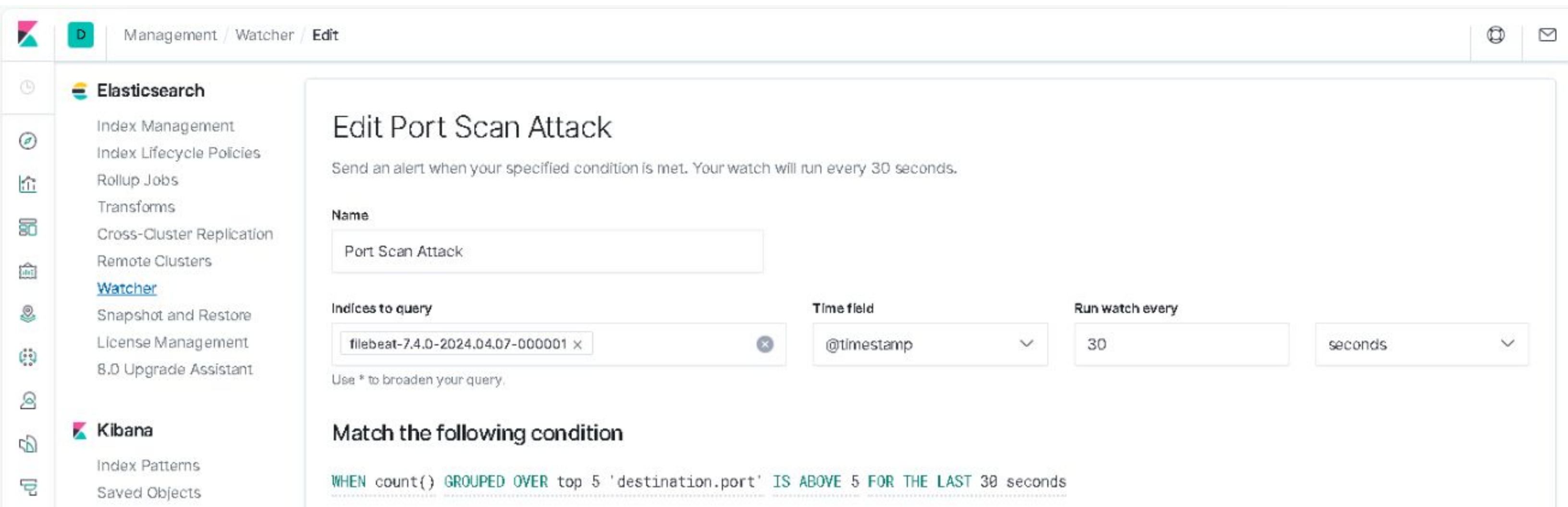
3.3.2 Screenshot

Create an alert for Brute Force attack.



3.3.3 Screenshot

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



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.

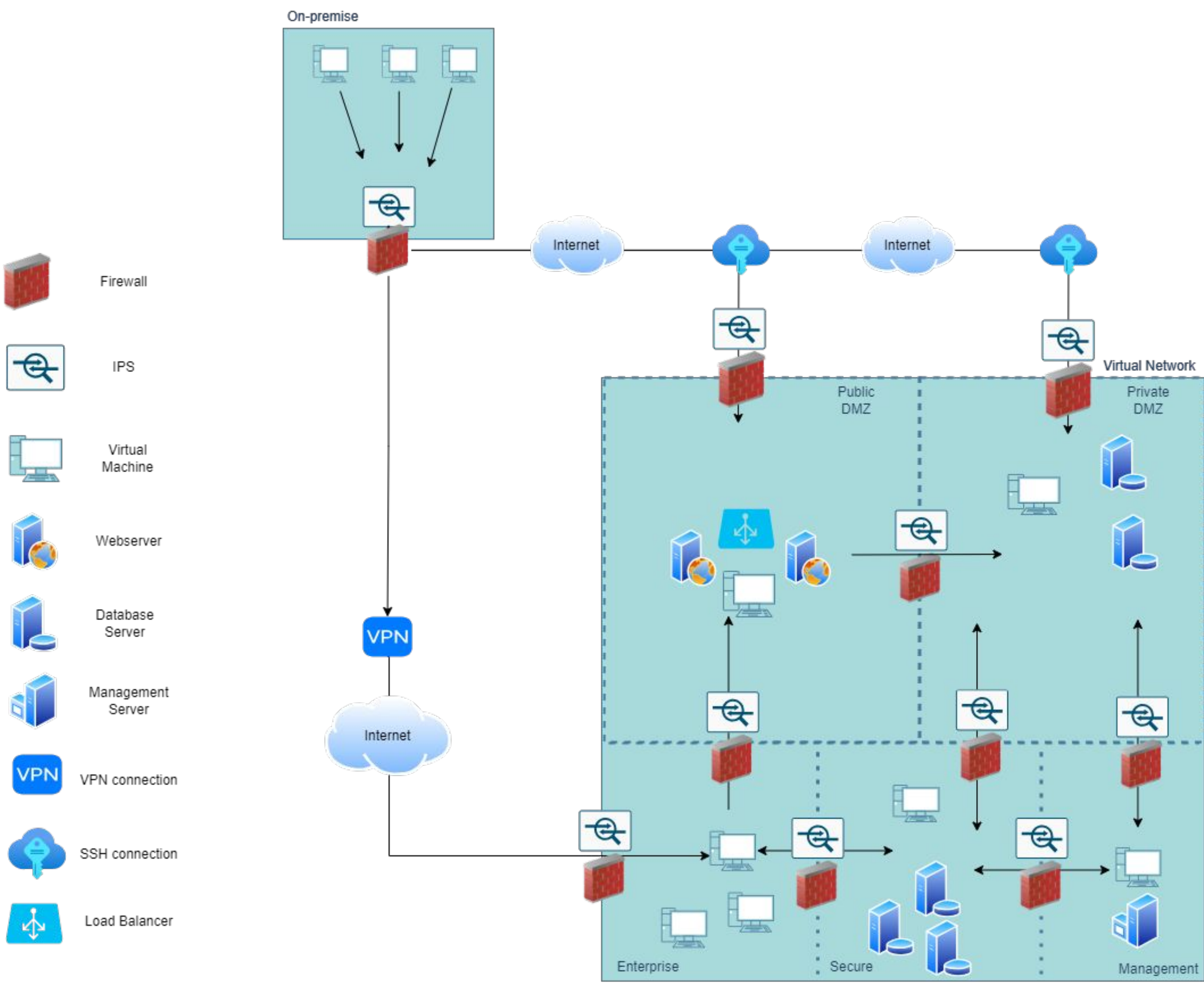
Most important:
Continuously update and refine the incident response playbook based on lessons learned from past incidents and emerging threats.

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.