Network Design

Team Gen ChimpanZ's

Novebmer 9, 2022

Team Leader

Mark Fastner

Team Members

Liam Joseph Abalos

Anh Huynh

Aster Lee

Github: https://github.com/markfastner/Nuclei

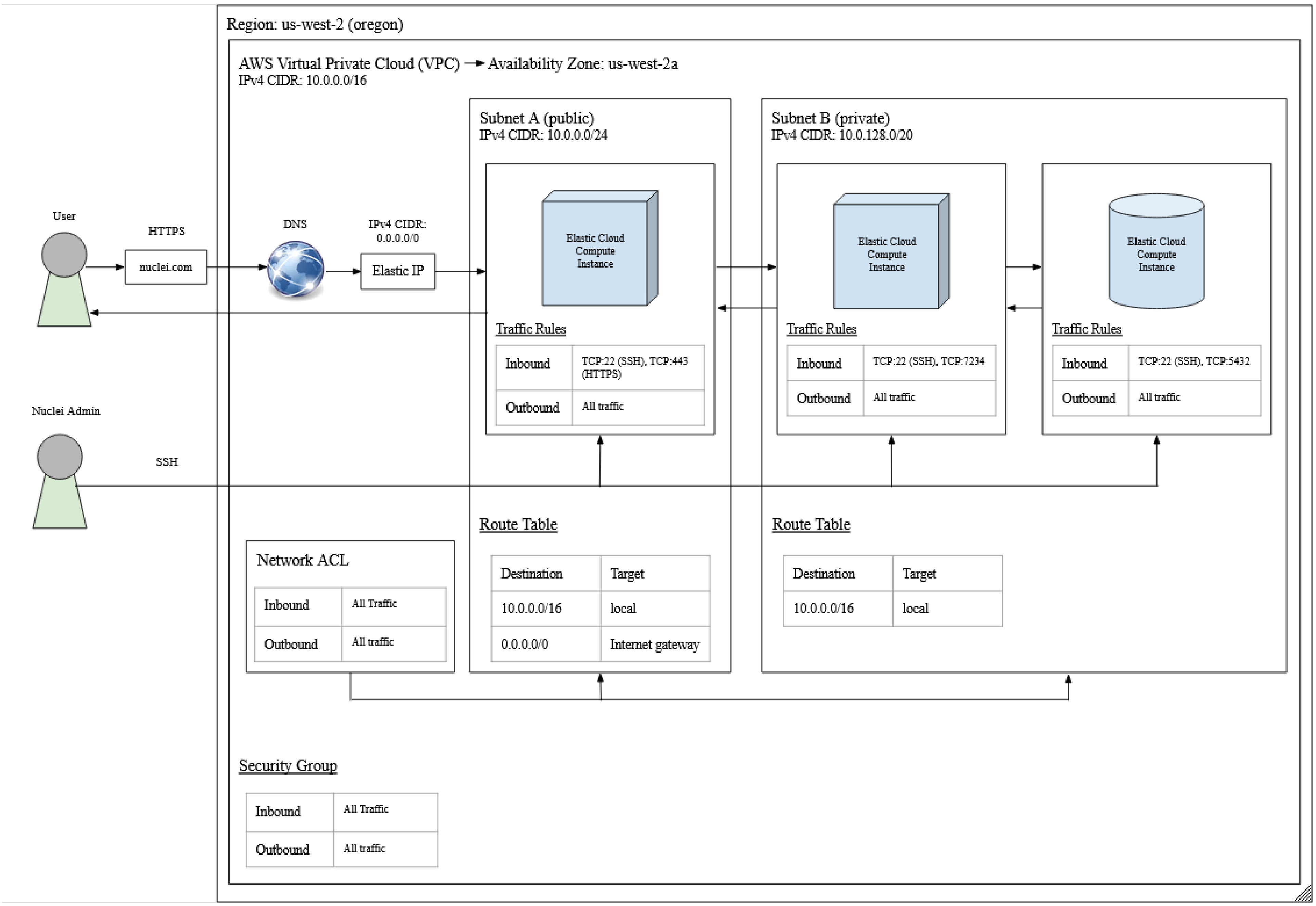
Table of Contents

Introduction

The network diagram will outline Nuclei’s network infrastructure and administration. This structure is responsible for connecting virtual cloud computing instances and delegating security rules between each of them. The network system also incorporates the Domain Name System (DNS) which is how clients will interface with Nuclei via the browser.

Amazon Web Services will provide the majority of infrastructure and services necessary for this network design.

Network Diagram


Region: us-west-2 (oregon)
AWS Virtual Private Cloud (VPC) → Availability Zone: us-west-2a
IPv4 CIDR: 10.0.0.0/16
User
HTTPS
nuclei.com
DNS
IPv4 CIDR: 0.0.0.0/0
Elastic IP
Nuclei Admin
SSH
Subnet A (public)
IPv4 CIDR: 10.0.0.0/24
Elastic Cloud Compute Instance
Subnet B (private)
IPv4 CIDR: 10.0.128.0/20
Elastic Cloud Compute Instance
Elastic Cloud Compute Instance

Traffic Rules

Inbound	TCP:22 (SSH), TCP:443 (HTTPS)
Outbound	All traffic

Traffic Rules

Inbound	TCP:22 (SSH), TCP:7234
Outbound	All traffic

Traffic Rules

Inbound	TCP:22 (SSH), TCP:5432
Outbound	All traffic

Network ACL

Inbound	All Traffic
Outbound	All traffic

Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	Internet gateway

Route Table

Destination	Target
10.0.0.0/16	local

Security Group

Inbound	All Traffic
Outbound	All traffic

Network Outline

An overview and description of the above figure.

VPC

The main working infrastructure in our network is the Virtual Private Cloud (VPC) service. This is a service offered by AWS and it allows for the organization of virtual compute instances into sub-networks–or subnets–across an official Amazon server region. The purpose of a VPC is to encapsulate certain instances into the aforementioned subnets and impose traffic and routing rules into them. By doing so, certain subnets can be accessed by the public internet and some cannot; some can route out to the internet and some can only route to other subnets in the VPC. This method of controlling access allows for parts of our system such as the database or the backend API to be private and secure from public access.

Because Nuclei will only cater to users in the Southern California region, we feel it is appropriate to have chosen AWS's us-west-2 server region which is located in Oregon because it is near Southern California and is cheaper in cost compared to AWS's us-west-1 server region–albeit us-west-1 is closer, we feel it is worthwhile sacrificing latency for cost.

An Availability Zone, as defined by Amazon, are the physical locations where a serverbase is located, and according to Amazon, us-west-2 has four Availability Zones; our system uses the A Availability Zone. One very important notation to consider is the CIDR notation which denotes a range of private IPv4 addresses used in the private network. Note that these IPs are not public and are exclusive to the instances within the VPC. Our VPC defines a IPv4 CIDR of 10.0.0.0/16 covering a range of IPs from 10.0.0.0 to 10.0.255.255 (256^2 = 65,536 IPs in total which the system can allocate from).

Furthermore, each subnet will have a designated route table which defines the output of traffic from the subnet and where it will be routed to. Whatever the IP value is or its Destination, the VPC will automate traffic to the defined Target.

Lastly, in creating the VPC, AWS will automatically generate a Network ACL and a Security Group to attach to the VPC. Like each instance has its defined inbound and outbound rules, the Network ACL also defines inbound and outbound rules but for each subnet in the VPC. Currently, it allows all inbound and outbound traffic; there are no specified rules at the moment since they are individually defined by the instances, but the Network ACL exists as an overhead firewall for each subnet. Likewise, the Security Group defines inbound and outbound rules for the entire VPC, and like the Network ACL, no new rules are defined, either.

Elastic IP

AWS assigns private IPs to its compute instances dynamically, meaning the IP is bound to change if the instance were ever stopped then rebooted. An Elastic IP is a public IP that never changes and is assigned to a singular instance, specifically the frontend server instance in Subnet A. Additionally, because it is a public IP address and outside the VPC's IPv4 CIDR scope, it is accessible via the internet, therefore accessible to users of Nuclei.

Subnet A (Public)

This subnet will house a singular instance: the frontend web application. It is made public because it should be accessible to users via the internet. It has an IPv4 CIDR of 10.0.0.0/24, allotting 256 possible IPs from the pool of 65,536. The instance in this subnet will be assigned an address in this range.

Users will need a permanent IP address to access this subnet, thus an Elastic IP is assigned here.

Traffic Rules

The frontend instance in this subnet will establish its firewall only to allow inbound traffic of HTTPS and SSH. HTTPS is considered because users will be making HTTP Secure API requests to the instance in this subnet, and SSH is necessary for remoting into the instance and controlling it. All types of outbound traffic are allowed.

Route Table

Any traffic output from this subnet within the IPv4 CIDR 10.0.0.0/16 will target local addresses within the VPC, this includes the instances in the private subnet. Also, traffic output within IPv4 CIDR 0.0.0.0/0, which denotes all public IPs across the internet will target the respective internet gateway to be relayed to the internet. This particular routing rule is what makes this subnet public.

Subnet B (Private)

Moreover, the remaining subnet will contain two compute instances which should remain private from public internet access: the backend API and the database. The only way data can enter this subnet is through the public subnet. This subnet has a IPv4 CIDR of 10.0.128.0/20, allocating 4,096 possible IPs from the pool of 65,536. Both the instances in this subnet will be assigned an address within this range.

Traffic Rules

Either instance in this subnet will have its own firewall for connection traffic. For the instance hosting the backend server, it will allow incoming TCP connections of port 7234 and SSH, while the instance hosting the database server will allow TCP connections of port 5432 and SSH. The TCP type with ports 7234 and 5432 define the host address of the backend API service and the database, respectively. Outbound rules are similar in both and will allow all types of traffic.

Route Table

Any traffic output from this subnet within the IPv4 CIDR 10.0.0.0/16 will target all local addresses in the VPC including the public subnet. Because this subnet does not have a target for the internet gateway, ensures that data will not leak into the public internet, and the only way to gain access to this subnet is via the public subnet. This creates an encapsulation effect for instances that we want to keep private.

Network Flow

The network flow describes the flow, direction, or traffic of data. The flow of data mainly starts at the user, where he or she performs actions on the User Interface which executes commands with data that subsequently propagates throughout the network.

User

A user will start by interacting with the Nuclei web application, which is done in the browser by pasting the domain in the address bar. By using our domain, the DNS which is considered the phonebook of the internet, will route that request to a public unique IP address established by the Elastic IP. That public IP is an alias for the frontend web server virtually hosted on an Amazon virtual machine instance.

Nuclei Admin

The developing team will have access to the instances across the VPC via the UNIX command line. This type of connection is known as Secure Shell Protocol (SSH) and is used to gain control over the virtual compute instance's operating system. System administrators of Nuclei are granted access to SHH into the network instances to perform work or maintenance.

Glossary

Term	Definition
VPC	Virtual Private Cloud. Secure, isolated private network within a public cloud
Subnet	Logical partition of the IP network into multiple, smaller network segments
CIDR	Classless Inter-Domain Routing. Method of IP address scheme to improve allocation of IP address by combining several address ranges into single network or route
TCP	Transmission Control Protocol. One of Internet protocol which takes part in communications, enabling applications and devices to exchange messages over a network
DNS	Domain Name System. Machine-readable IP address translated so humans can read as a domain name.
Internet Gateway	VPC component that allows instances with public IP address to access the resources in the VPC from Internet

References

1. https://cutewallpaper.org/24/sports-png/view-page-24.html
2. https://www.youtube.com/watch?v=bGDMeD6kOz0
3. https://www.ipaddressguide.com/cidr
4. https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html
5. https://freesvg.org/connected-globe-vector-icon
6. https://www.cloudflare.com/learning/cloud/what-is-a-virtual-private-cloud/
7. https://www.techtarget.com/searchnetworking/definition/subnet
8. https://www.ibm.com/docs/en/wip-mg/5.0.0?topic=reference-classless-inter-domain-routing
9. https://www.keycdn.com/support/what-is-cidr
10. https://www.fortinet.com/resources/cyberglossary/tcp-ip
11. https://aws.amazon.com/route53/what-is-dns/
12. https://medium.com/awesome-cloud/aws-vpc-difference-between-internet-gateway-and-nat-gateway-c9177e710af6

Version Changelog

Version	Submission Date	Changelog
1	10/23/22	Initial Draft Version
2	10/27/22	Changed Network Diagram Information
3	11/01/22	Added Descriptions to Diagrams, Added Same Info to Network Outline
4	11/08/22	Finalized Document. Finish Table of Contents. Better Definitions.