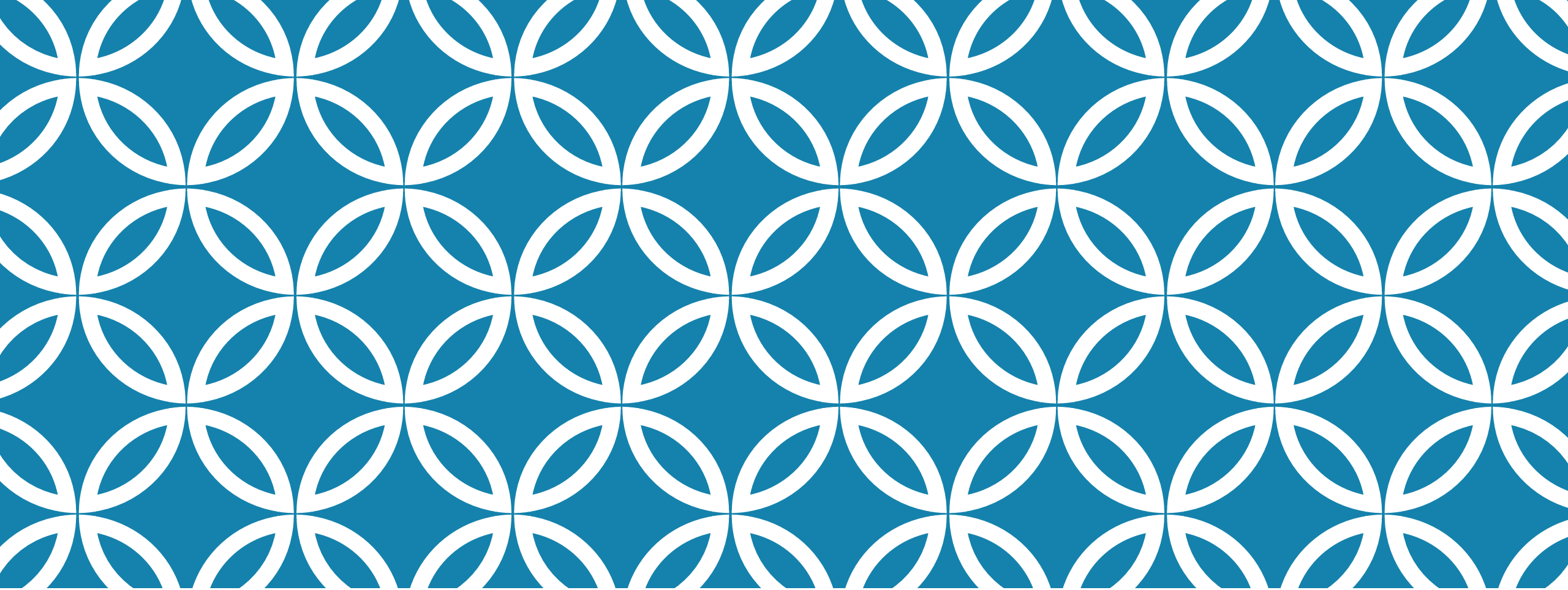


PROJECT 1

Automation| Sandbox Worms|

Aubrey Nigoza, Nick Yoon, Yerden Zhursinbek, Mark Siegmund, John Vinuya

PROJECT GOALS

Automation of Infrastructure Setup and Modification

Automation of Configuration of Service Infrastructure

Maintain consistent, secured and highly-available state files

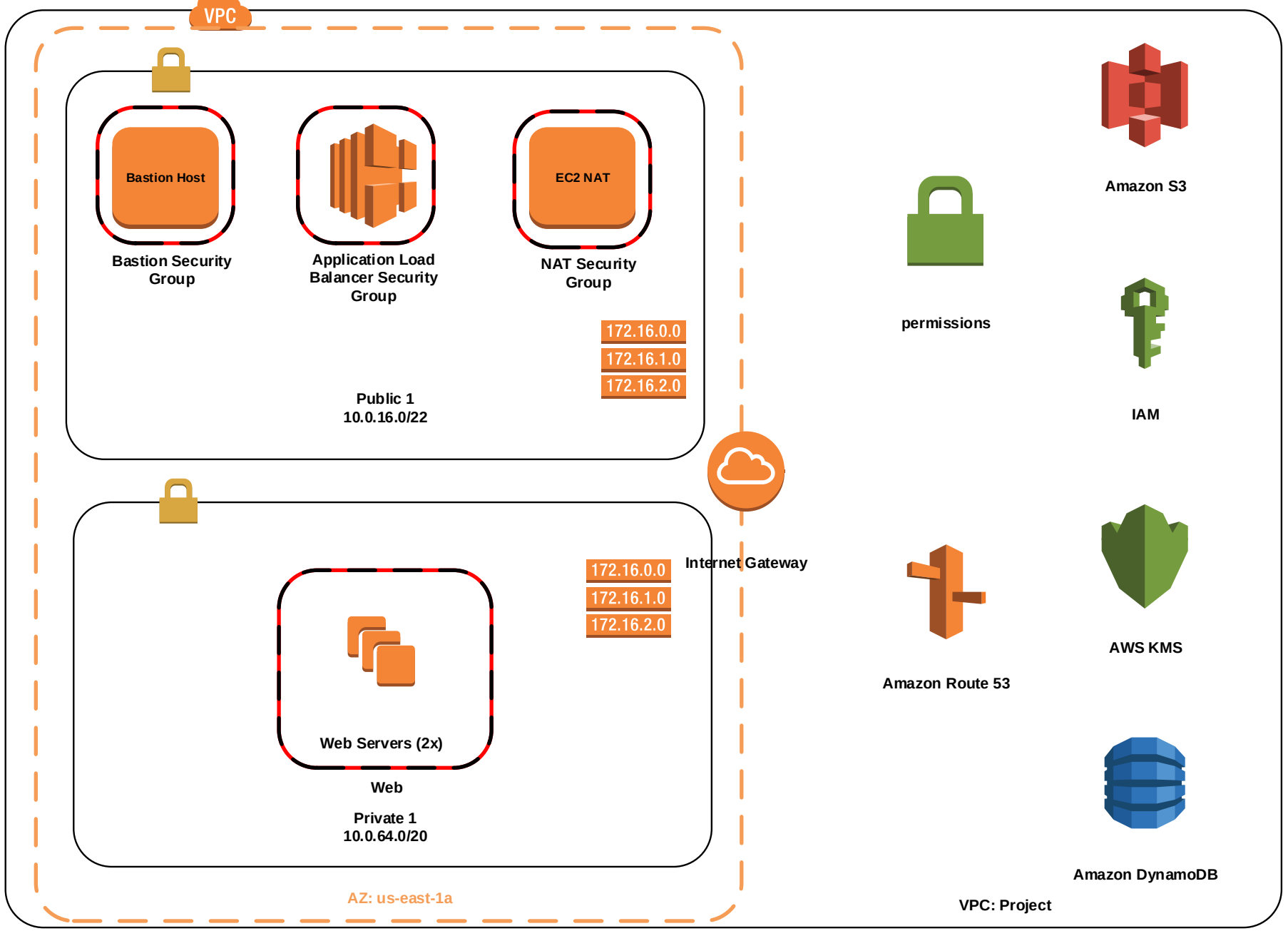
WORKFLOW FOR COLLABORATION

GitHub Repositories and SSH Keys

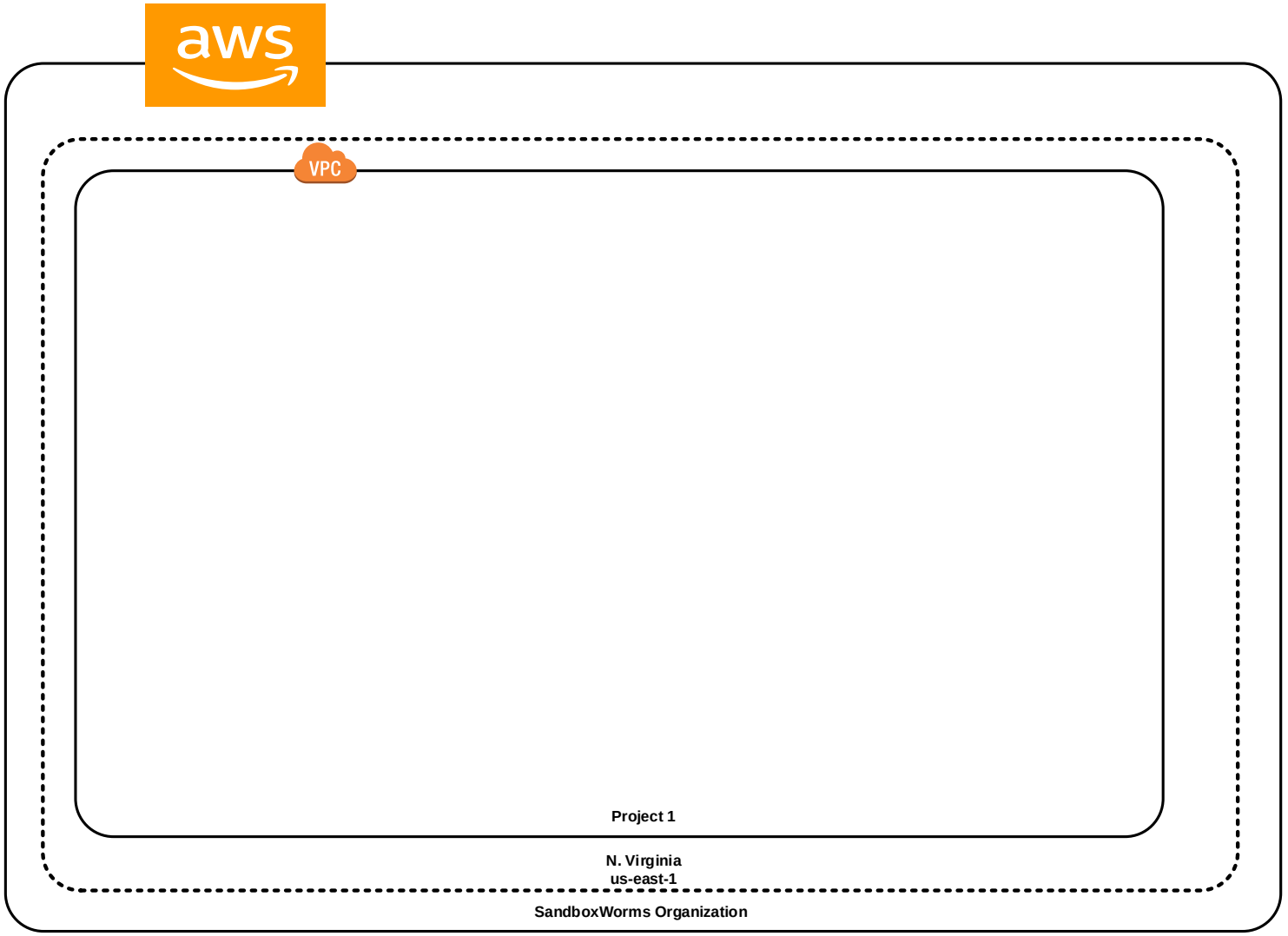
AWS Access Keys and Secret Keys on profiles (Ubuntu Controller) and files (Windows Machine)

Keys on Encrypted Drives

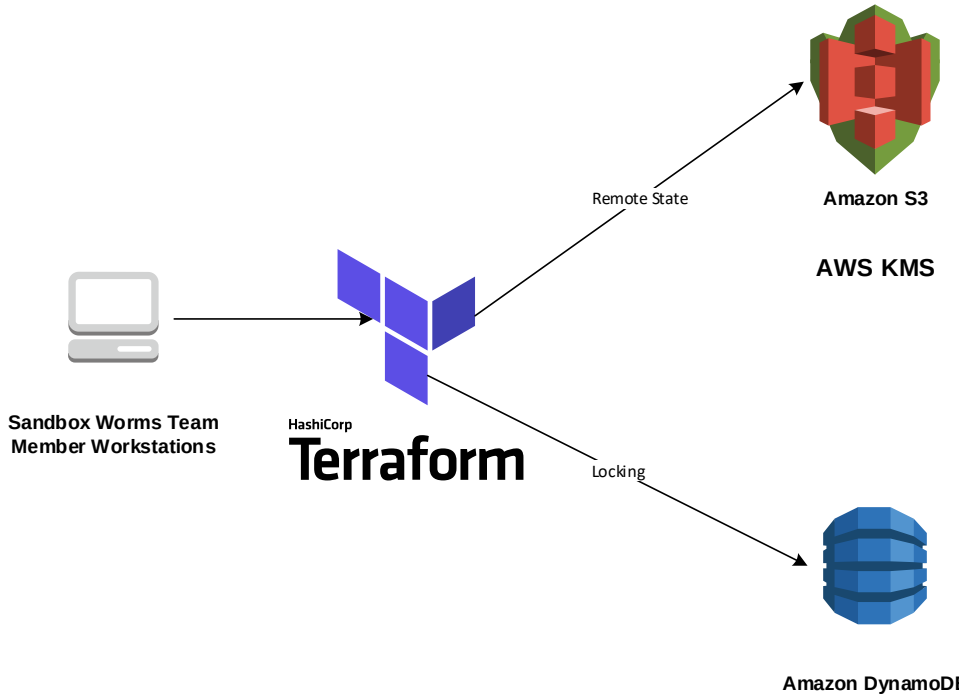
Folder Structures


VPC
Bastion Host
Bastion Security Group
Application Load Balancer Security Group
EC2 NAT
NAT Security Group
172.16.0.0
172.16.1.0
172.16.2.0
Public 1
10.0.16.0/22
Internet Gateway
Web Servers (2x)
Web
172.16.0.0
172.16.1.0
172.16.2.0
Private 1
10.0.64.0/20
AZ: us-east-1a
permissions
Amazon S3
IAM
Amazon Route 53
AWS KMS
Amazon DynamoDB
VPC: Project

AWS INITIAL STATE



REMOTE TFSTATE




```
bucket = "sandboxworms-tf-state-09112018"
key="tf-prod/terraform.tfstate"
region="us-east-1"
encrypt = true
versioning enabled = true
kms_master_key_id =
"${aws_kms_key.tf_enc_key.arn}"
```

```
resource "aws_dynamodb_table" "sandboxworms-tf-
lock-0911" {
 name = "sandboxworms-tf-lock-0911"
 hash_key = "LockID"
 read_capacity = 20
 write_capacity = 20

 attribute {
  name = "LockID"
  type = "S"
 }

 tags {
  Name = "DynamoDB Terraform State Lock Table"
 }
}
```

IAM, POLICIES AND KEYPAIRS


```
#Create Group
resource "aws_iam_group" "GroupMembers"{
    name = "${var.sandboxworms_group}"
}
#CREATE POLICY


resource "aws_iam_policy_attachment" "AdminAccess" {
  name       = "Grant-Admin-Access"
  groups     = ["${aws_iam_group.GroupMembers.id}"]
  policy_arn = "arn:aws:iam::aws:policy/AdministratorAccess"
}


resource "aws_iam_group_membership" "GroupMembers"{
    name = "GroupMembers"
    users = ["${aws_iam_user.yerden_p1.name}",
                "${aws_iam_user.mark_p1.name}",
                "${aws_iam_user.nick_p1.name}",
                "${aws_iam_user.john_p1.name}",
                "${aws_iam_user.aubrey_p1.name}"]
    group = "${aws_iam_group.GroupMembers.id}"

}
```

John

IAM

```
resource "aws_iam_user" “john_p1" {

    name = “john_p1"

}


resource "aws_iam_policy_attachment"
"AdminAccess" {

name = "Grant-Admin-Access"

groups     =
["${aws_iam_group.GroupMembers.id}"]

policy_arn =
"arn:aws:iam::aws:policy/AdministratorAccess"

}
```

```
resource "aws_iam_group_membership"
"GroupMembers"{

    name = "GroupMembers"

    users = ["${aws_iam_user.yerden_p1.name}",
                "${aws_iam_user.mark_p1.name}",
                "${aws_iam_user.nick_p1.name}",
                "${aws_iam_user.john_p1.name}",
                "${aws_iam_user.aubrey_p1.name}"]

    group =
"${aws_iam_group.GroupMembers.id}"


}
```

John

KEYPAIRS

resource "aws_key_pair" "key_john" {

key_name = "john"

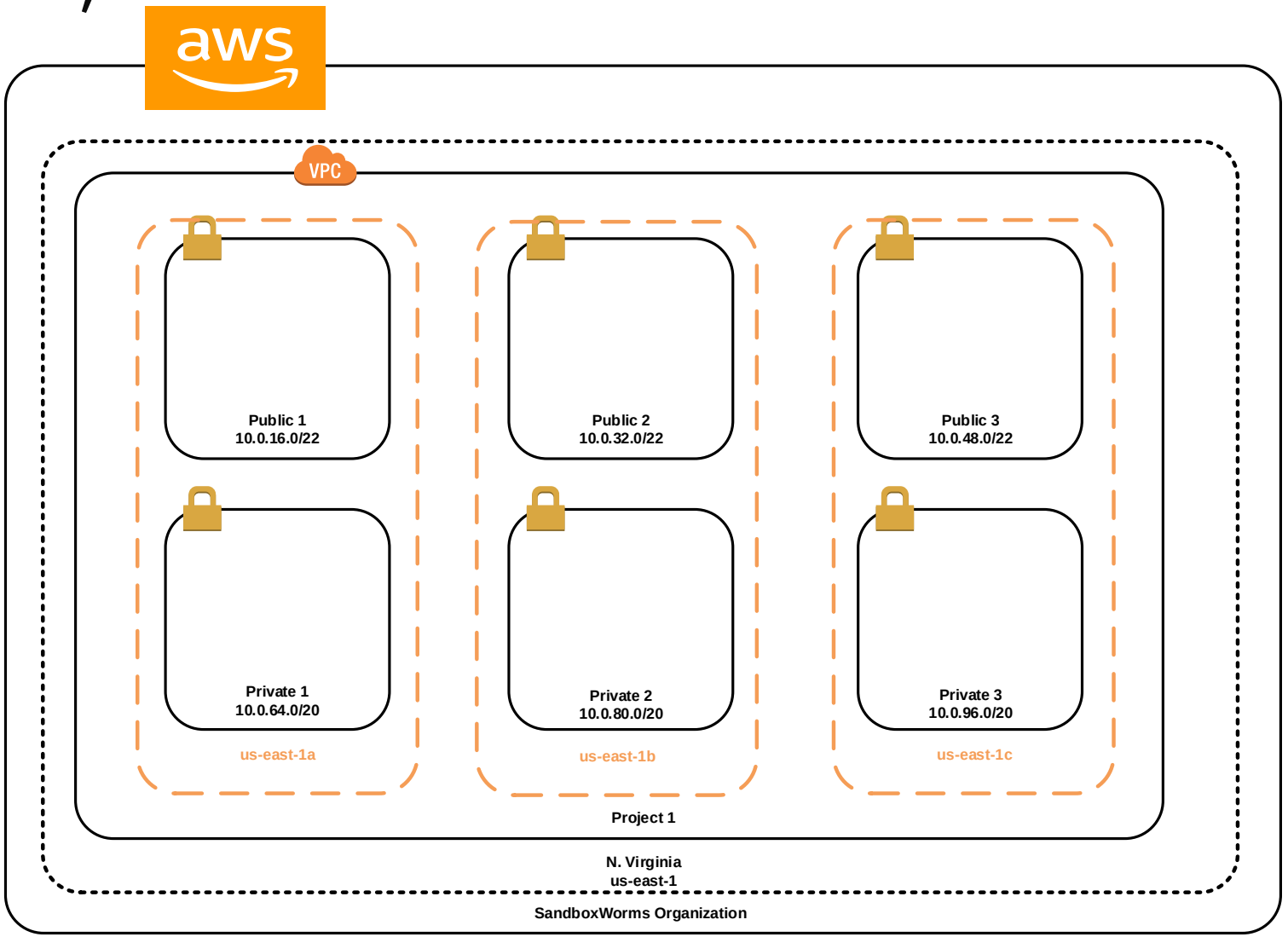
public_key = "ssh-rsa AAAAAADAQABAAABAQCRqEw0Ge/+lnkY1cpeIT7..."

}

```
18  variable "aws_secret_key" {}
19  variable "sandboxworms_group" {
20    default = "Group_Members"
21  }
22  variable "aws_key_name" {
23    default = "proj0_aubrey"
24  }
```

John

SUBNETS, AVAILABILITY ZONE DESIGN CHANGES



Mark

VPC RESOURCES

Security Groups

Application Load Balancer Security Group

NAT Instance Security Group

Private Instances Security Group

Bastion Host Security Group

Route Tables

Private Subnets

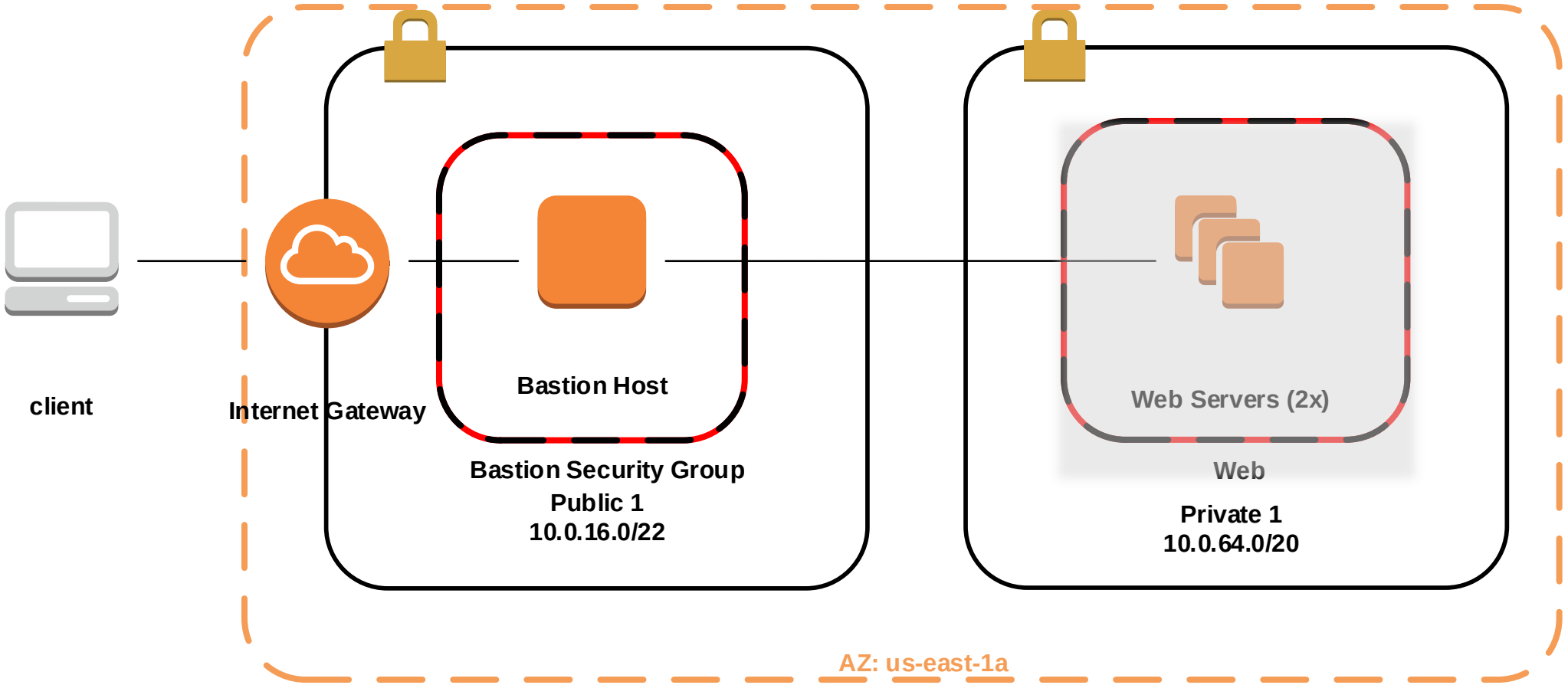
- Internet access thru the NAT Instance
- AWS Resources: WebServers

Public Subnets

- Internet access thru the Internet Gateway
- AWS Resources: NAT Instance, Application Load Balancers, Bastion Host

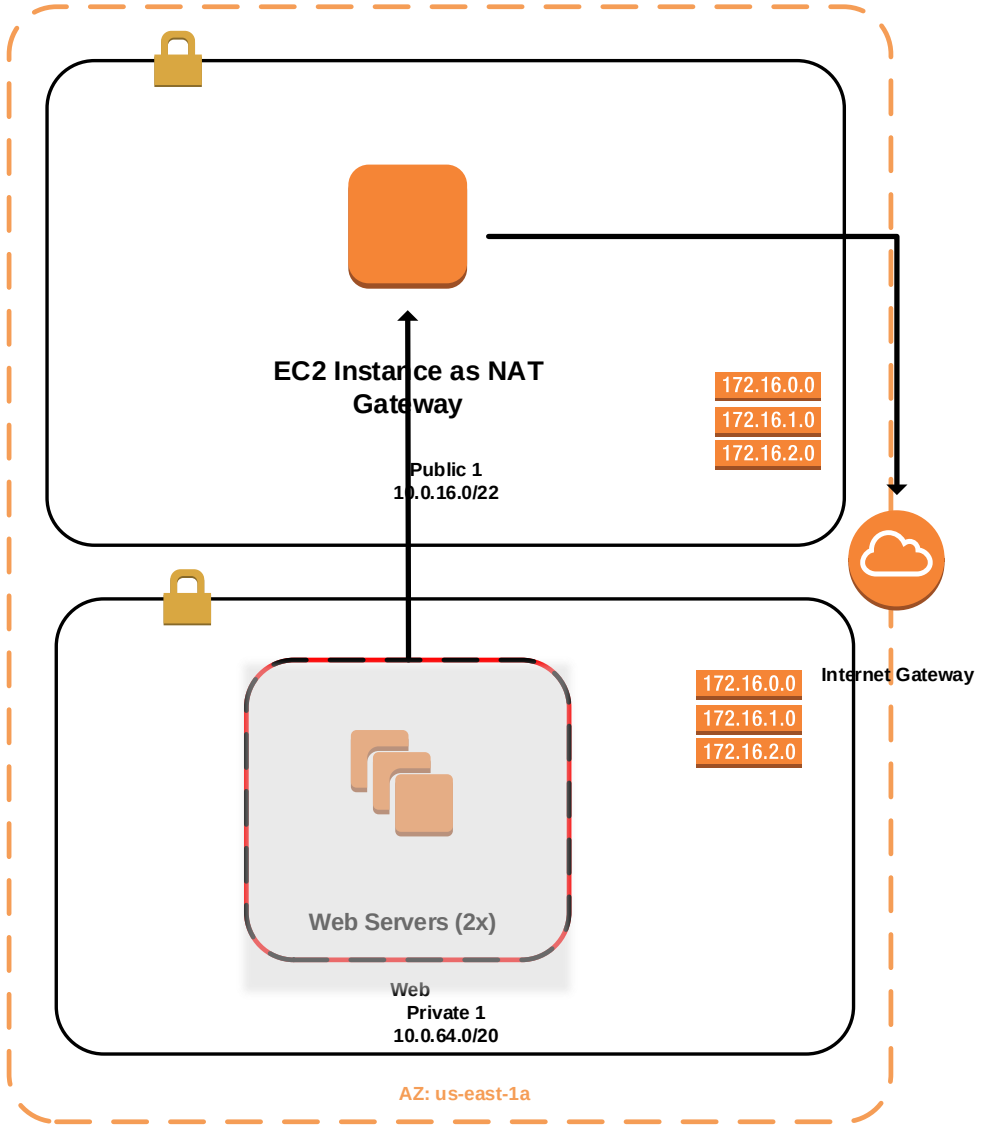
Mark

BASTION HOST



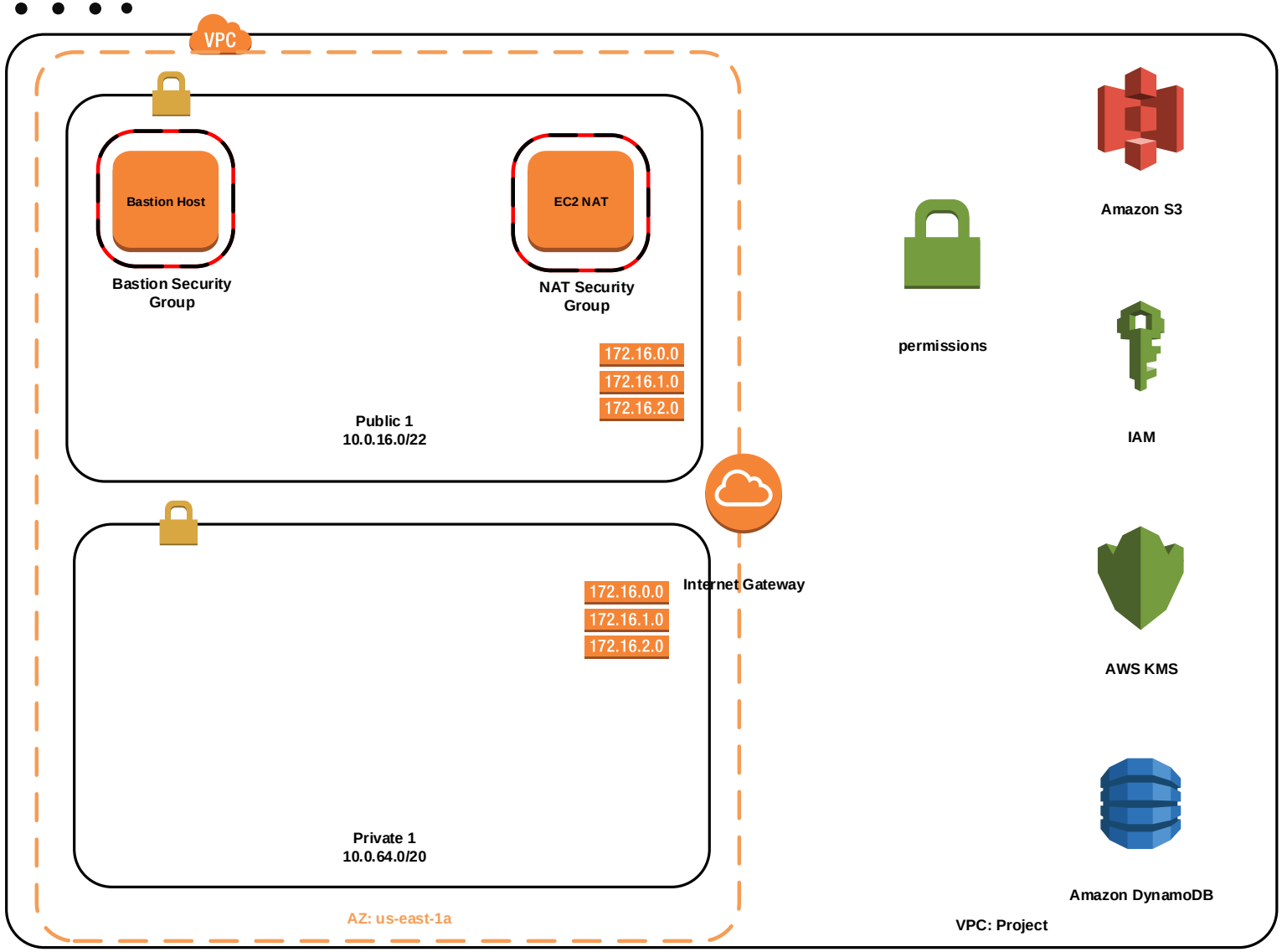
Mark

OUTBOUND INTERNET TRAFFIC FOR PRIVATE SUBNET



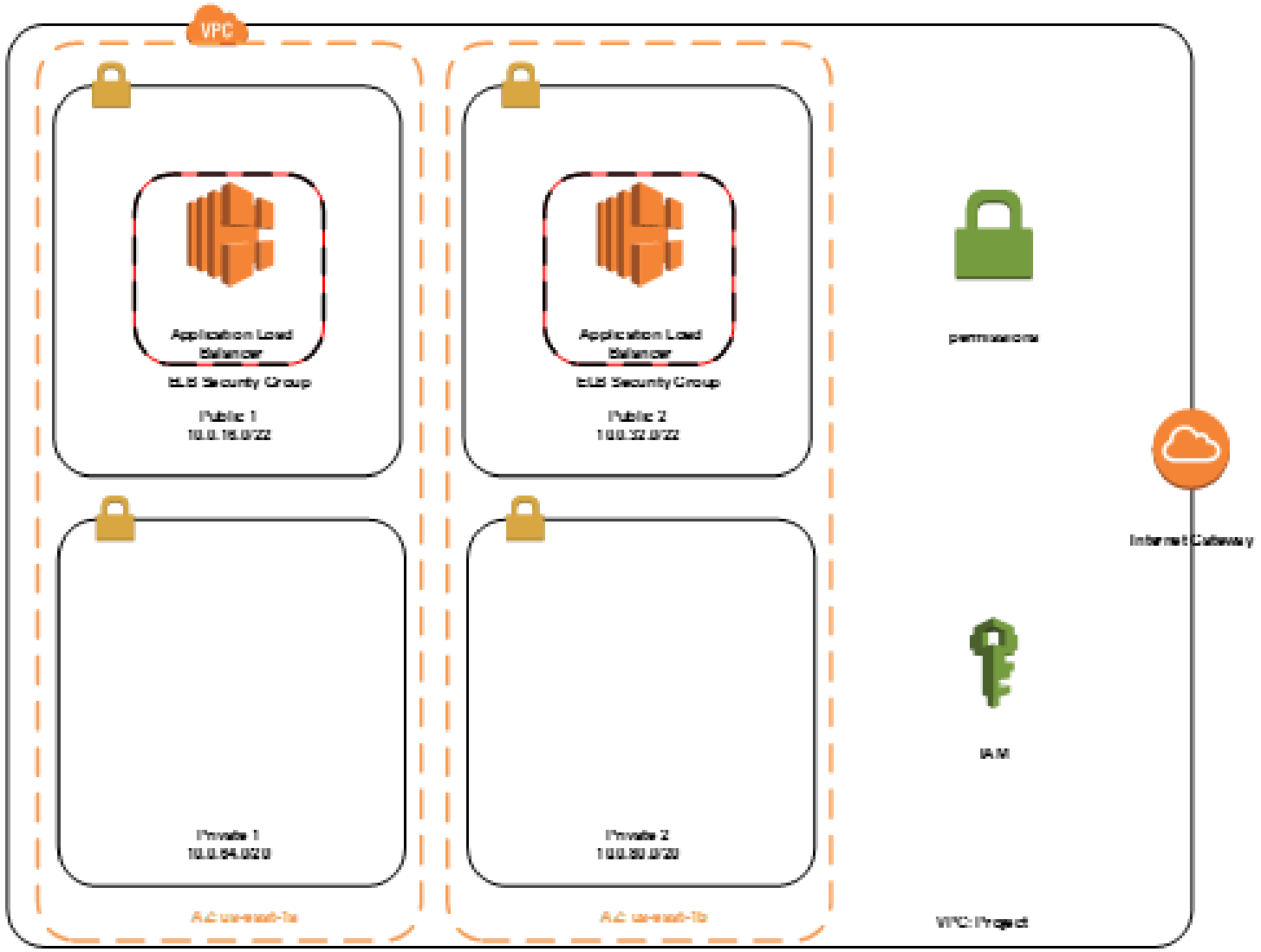
Nick

SO FAR....


VPC
Bastion Host
Bastion Security Group
EC2 NAT
NAT Security Group
172.16.0.0
172.16.1.0
172.16.2.0
Public 1
10.0.16.0/22
Internet Gateway
172.16.0.0
172.16.1.0
172.16.2.0
Private 1
10.0.64.0/20
AZ: us-east-1a
permissions
Amazon S3
IAM
AWS KMS
Amazon DynamoDB
VPC: Project

Nick

APPLICATION LOAD BALANCER



John

EC2 WEB SERVERS

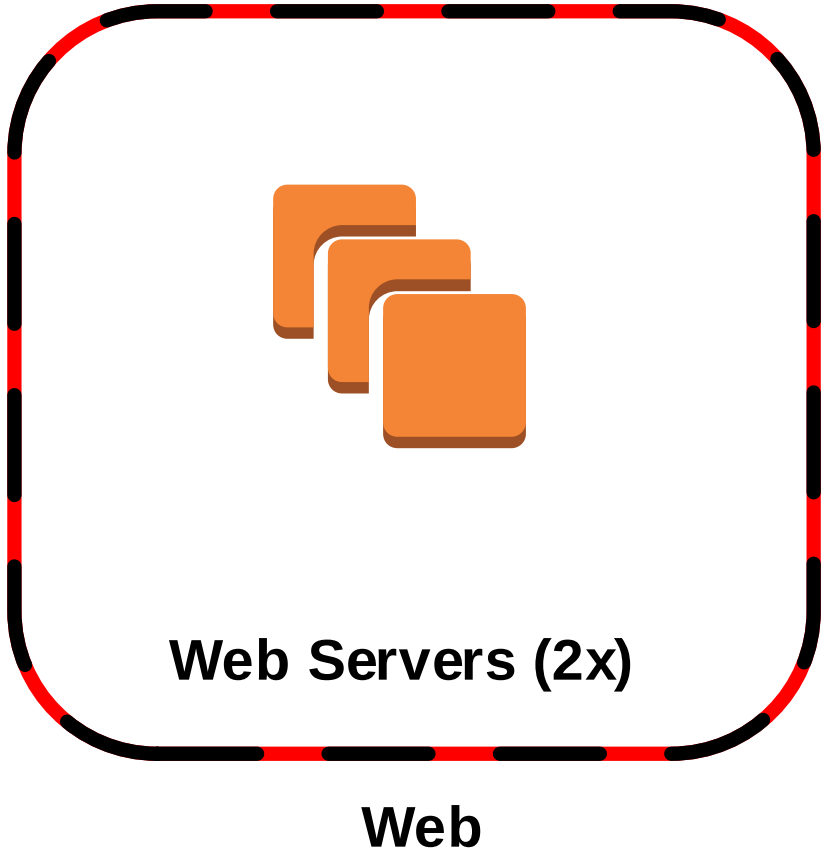
Red Hat Enterprise Linux Servers

Private Subnet

Dynamic Private IP

Tag:

- Key: Type
- Value: WebServer

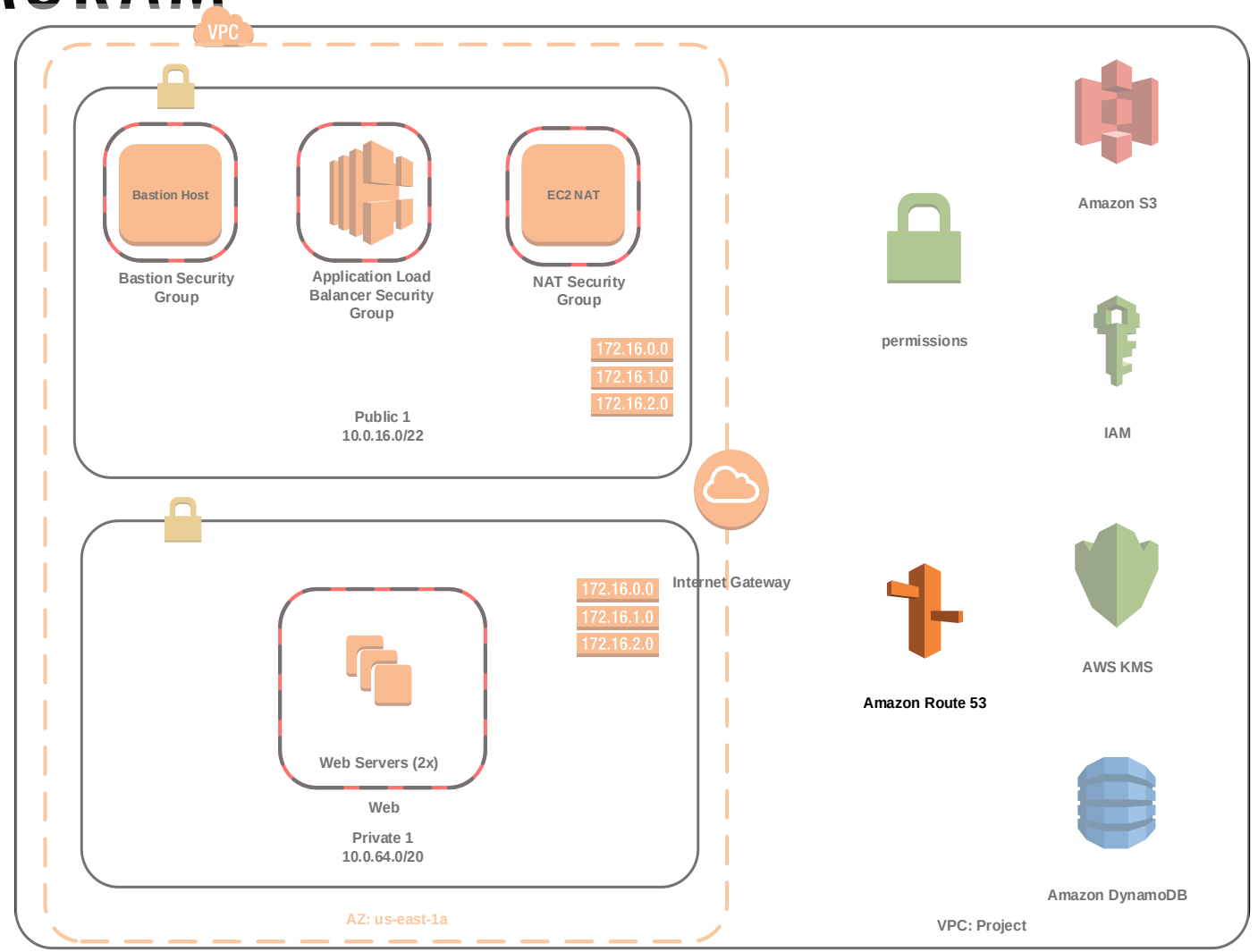


```
34  resource "aws_instance" "web01" {
35      ami = "ami-6871a115" #redhat linux
36      #availability_zone = "${data.aws_availability_zones.available.names[0]}"  #subnet id should set it.
37      instance_type = "t2.micro"
38      key_name = "${var.aws_key_name}"
39      vpc_security_group_ids = ["${data.aws_security_group.privateInstanceSG.id}"]
40      subnet_id = "${data.aws_subnet.private_sub1.id}"
41      tags {
42          Type = "WebServer"
43      }
44  }
```

COMPLETING THE DIAGRAM

```
data "aws_route53_zone" "sandboxworms_zone"{
name = "sandboxworms.me."
}
resource "aws_route53_record" "www" {
zone_id = "${data.aws_route53_zone.sandboxworms_zone.id}"
name = "www"
type = "A"
alias {
name = "${aws_alb.sandboxworms-alb.dns_name}"
zone_id = "${aws_alb.sandboxworms-alb.zone_id}"
evaluate_target_health = true
}
}

resource "aws_route53_record" "apex" {
zone_id = "${data.aws_route53_zone.sandboxworms_zone.id}"
name = ""
type = "A"
#ttl = "300"
alias {
name = "${aws_alb.sandboxworms-alb.dns_name}"
zone_id = "${aws_alb.sandboxworms-alb.zone_id}"
evaluate_target_health = true
}
}
```

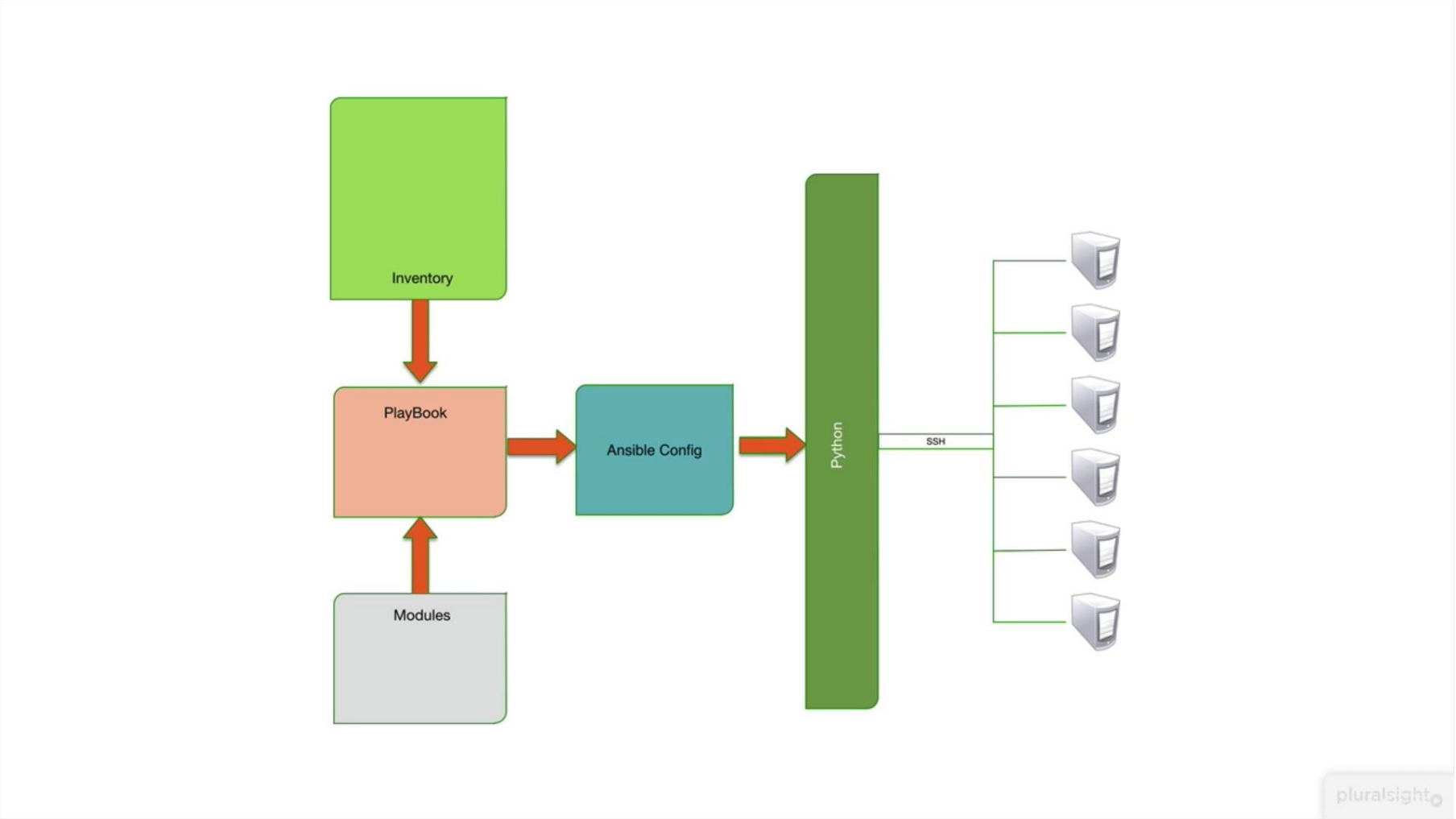


Aubrey

TERRAFORM DEMO

AWS

ANSIBLE



Credit: Plurasight

ANSIBLE SETUP

Authentication Mechanisms:

- Private Public Key Pairing: Ubuntu controller, GitHub, AWS EC2 Instances (Bastion, Webs, NAT)
- SSH Agent (Forwarder)
- AWS Profile (awscli)

Connectivity:

- ssh proxy command in ~/.ssh/config

Inventory:

- Dynamic Inventory via ec2.py and AWS tags
- ec2.ini : configured to use private ip's of ec2 instances

Playbooks:

- ec2config.yml
- blogbuild.yml (extra: buildsite bash script)

ANSIBLE PLAYBOOKS

ec2config.yml

All:

- Add Keypairs

Webservers:

- Apache Configuration

Bastion Host

- epel-release
- fail2ban

blogbuild.yml

- Unarchive the blog.tar.gz (generated and packaged by buildsite script) to all the Webservers

ISSUES AND IMPROVEMENTS

Issues

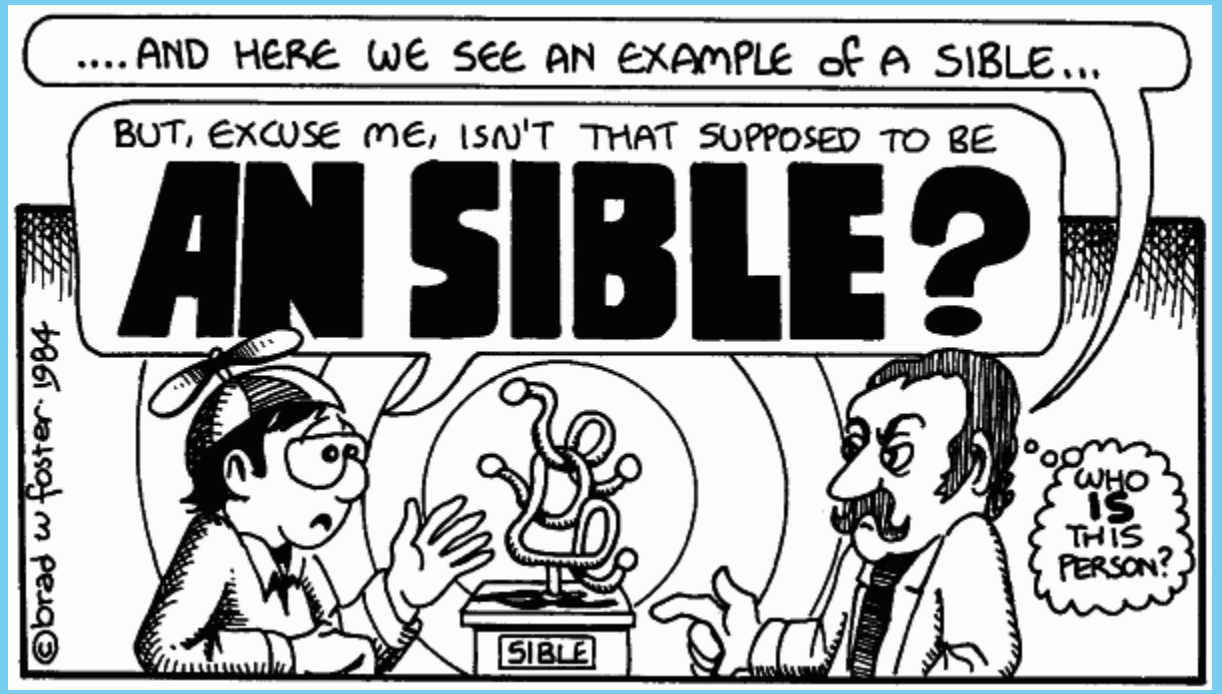
Hacked

Terraform learning curve

Delay due to dependency of tasks

Features

High Availability of Web Servers



QUESTIONS

Terraform and Ansible