Sécurité dans les environnements infonuagiques

Module 3: Gestion des Configurations (Part 2)

Armstrong Foundjem

Polytechnique Montréal

Automne 2023

Plan

1. VPC & EC2 security
    1. Data Protection
    2. Infrastructure Security
    3. IAM
    4. Resilience
    5. Compliance Validation
    6. Vulnerability Analysis
    7. Threat Analysis

1 Data Protection

2 Infrastructure security

3 IAM

4 Resilience

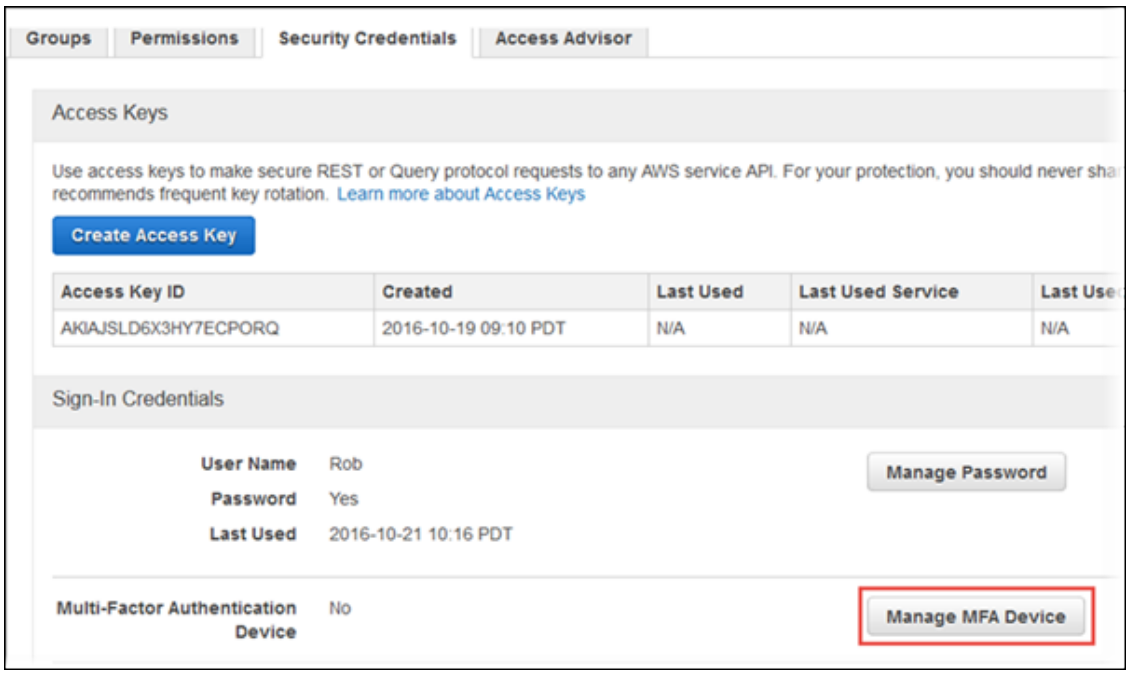
5 Compliance validation

6 Vulnerability Analysis

7 Threat Analysis

MFA

- Use Multi-factor Authentication (MFA) to check users access to the VPC infrastructure using a time-based one-time password (TOTP) algorithm.
  - Go to **Users** > **Security Credentials** to setup a virtual MFA device



  - Grant access to VPC for MFA-authenticated users using IAM policy

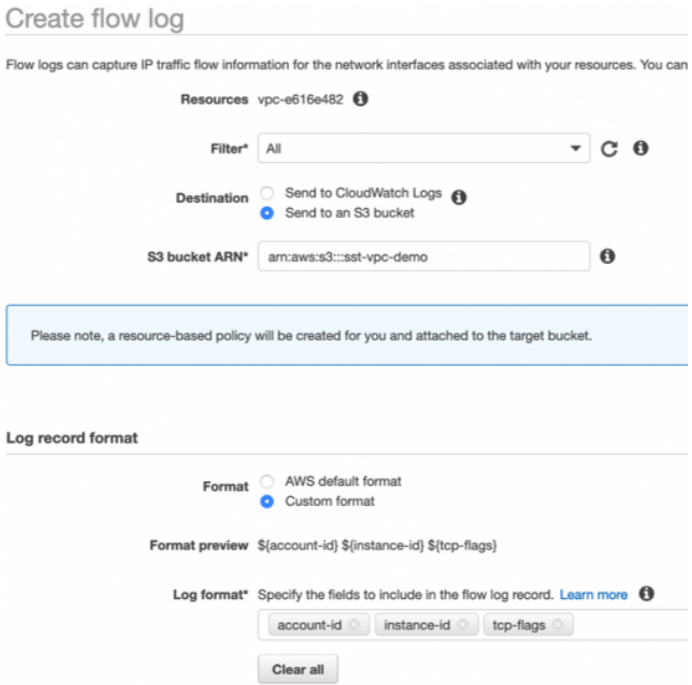
SSL/TLS encryption

```
"Statement":[
 {
        "Sid": "AllowActionsForEC2",
        "Effect": "Allow",
        "Action": ["ec2:RunInstances",
                   "ec2:DescribeInstances",
                   "ec2:StopInstances "],
        "Resource": "*"
 },
 {
    "Sid": "AllowActionsForEC2WhenMFAIsPresent",
    "Effect":"Allow",
    "Action":"ec2:TerminateInstances",
    "Resource":"*",
    "Condition":{
       "Bool":{"aws:MultiFactorAuthPresent":"true"}
    }
  }
]
```

- Enforce SSL/TLS (up to 1.2) for traffic encryption using AWS Certificate Manager. On AWS CLI,
  - Request a public certificate: *aws acm request-certificate –domain-name www.polystudent.com* (more options)
  - Check renewal status: *aws acm describe-certificate –certificate-arn arn:aws:acm:region:userID:certificate/cert_ID*
  - Import certificates: *aws acm import-certificate –certificate fileb://xx.pem –private-key fileb://xxxx.pem* (more options)

Logging

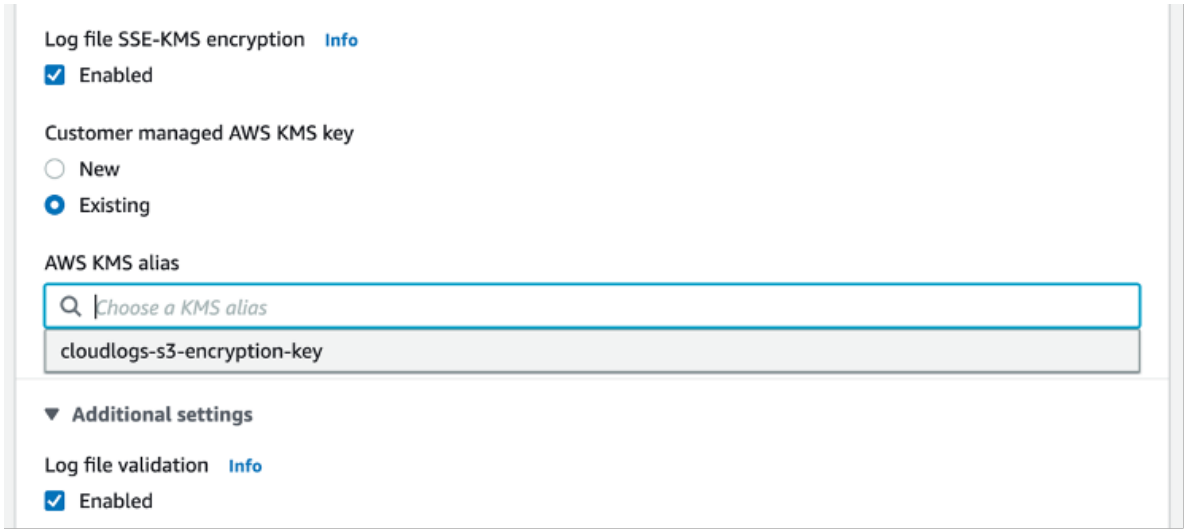
- Enable logging and monitoring using AWS Flow logs and AWS Cloud Trail
  - *Flow logs:* capture inbound/outbound IP flow information to/from network interfaces of the VPC and stores it on S3/CloudWatch



  - *Cloud Trail:* records and monitors logs across multiple regions or a single region

Data Protection At Rest & In Transit

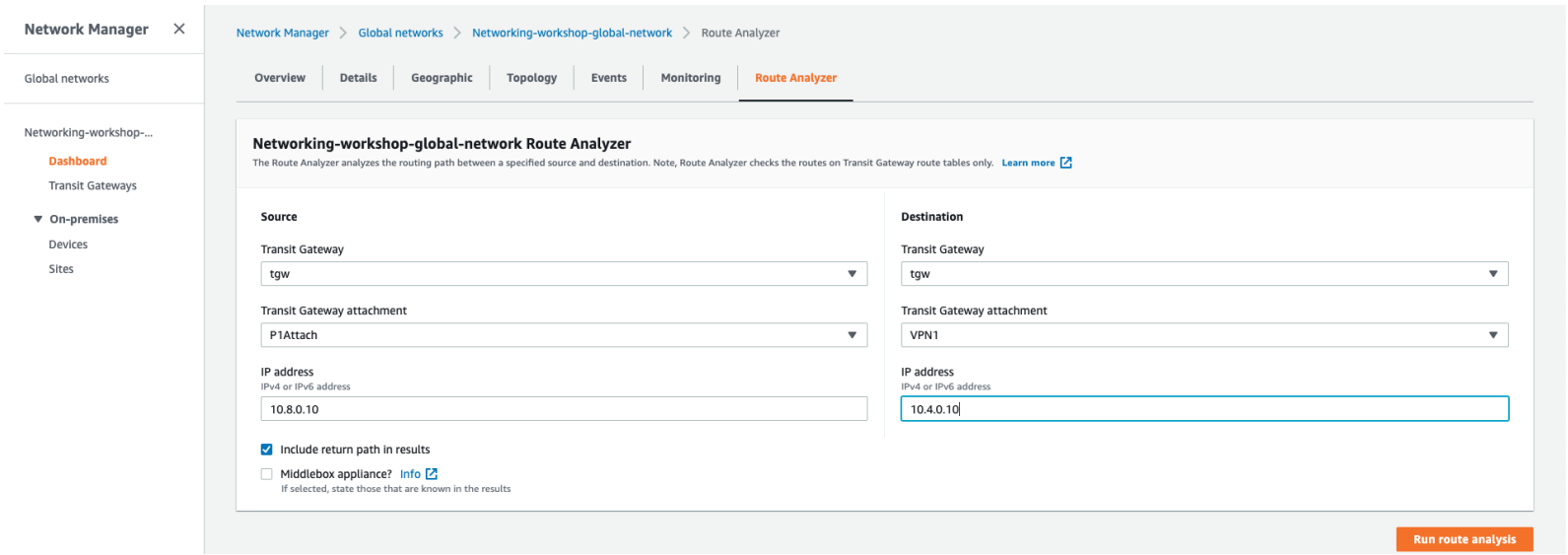
- Encrypt AWS Flow and Cloudtrail logs using AWS KMS
- Encrypt network traffic and S3 using AWS KMS and Macie



- Use AWS KMS and Cloud HSM to generate FIPS 140-2 compliant cryptographic keys
- Enable ingress/egress traffic control using AWS NACL, Security Groups, and Network Access Analyzer

Traffic Mirroring

- Enable traffic mirroring to copy the network traffic for monitoring (e.g., level of workloads, intrusion detection system, packet analysis)
- Enable network routing control using AWS route analyzer

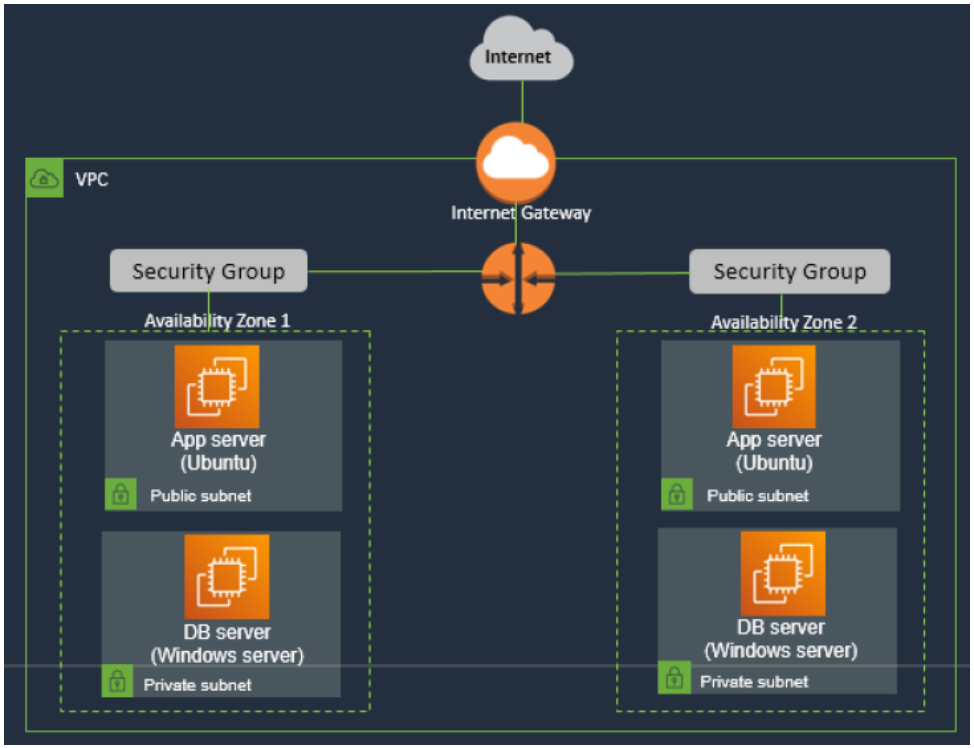


Sondage ☺: `https://app.wooclap.com/ZSDLFI`.

wooclap

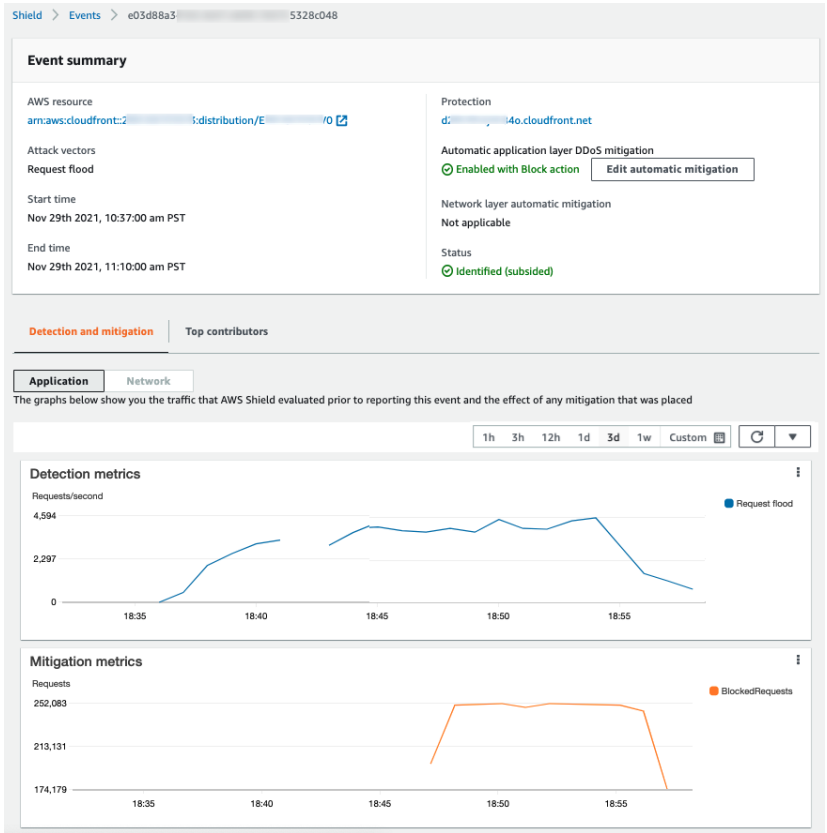
Network Isolation

- Isolate network in the VPC
  - subnets to isolate the tiers (e.g., app server, database server) in the VPC
  - private subnets for your instances that must not be accessed directly from the internet



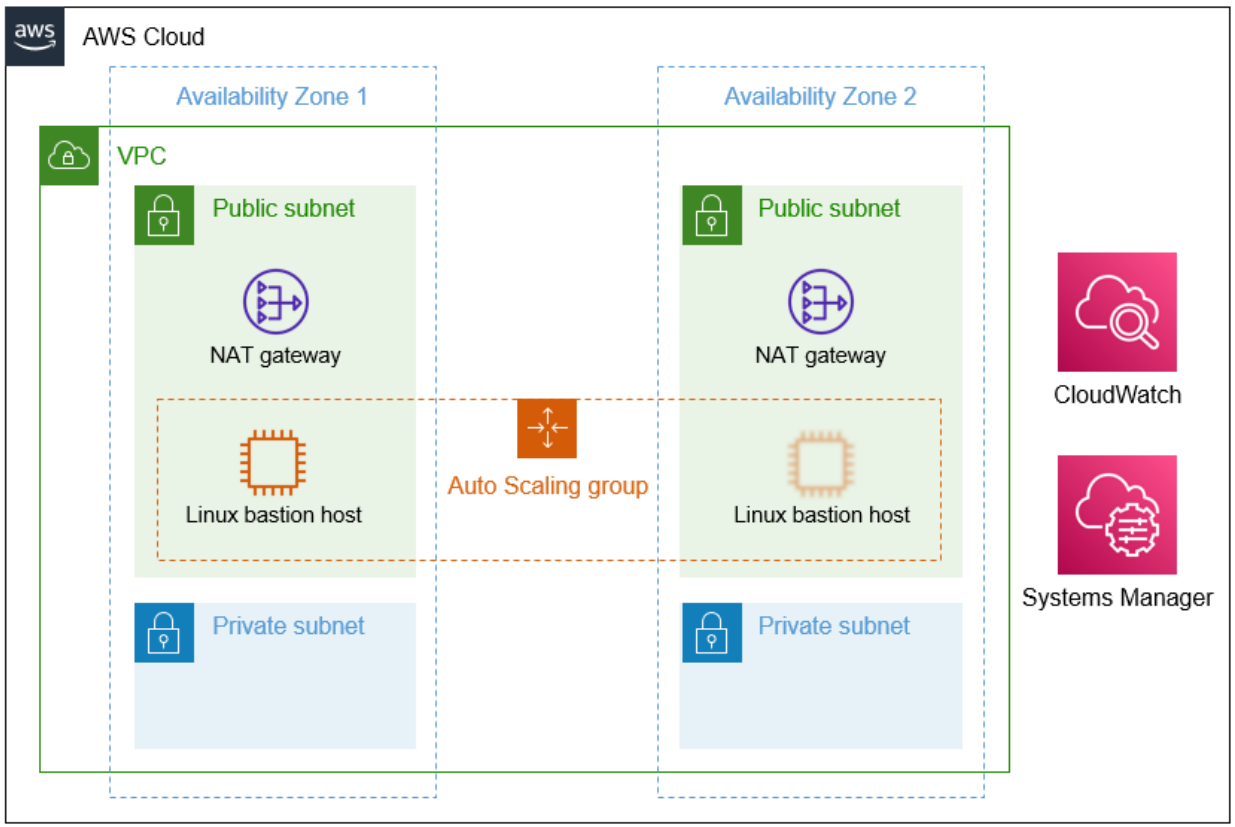
DDoS prevention

- Mitigate DDoS attacks
  - Use AWS Shield to automatically respond to and mitigate DDoS attacks
  - Use AWS WAF as first line to monitor HTTP and HTTPS requests forwarded to protected web apps
  - Use AWS CloudFront for protection at the edge by content caching



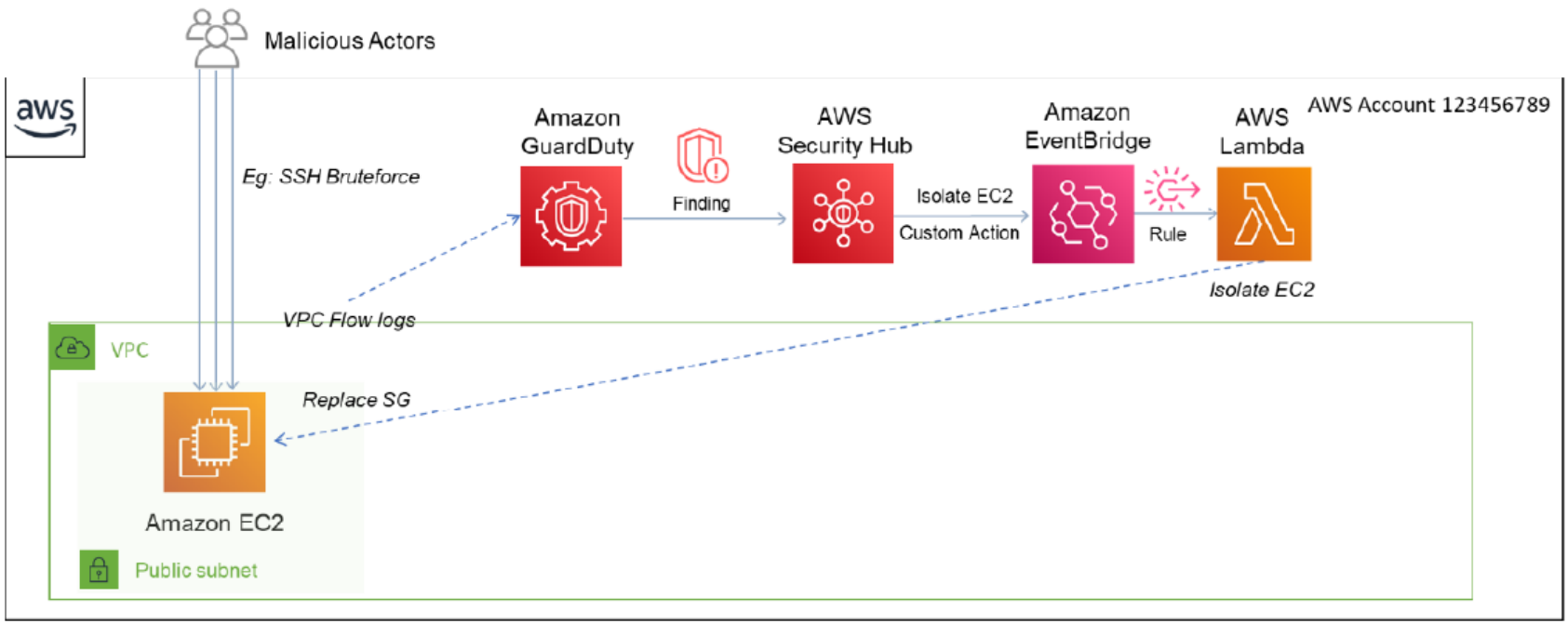
Inbound/Outbound network protection

- Use bastion host / NAT gateway for internet access from an instance in a private subnet.
- Use security groups to protect private and public subnets from potential threats from the ingress/egress traffic



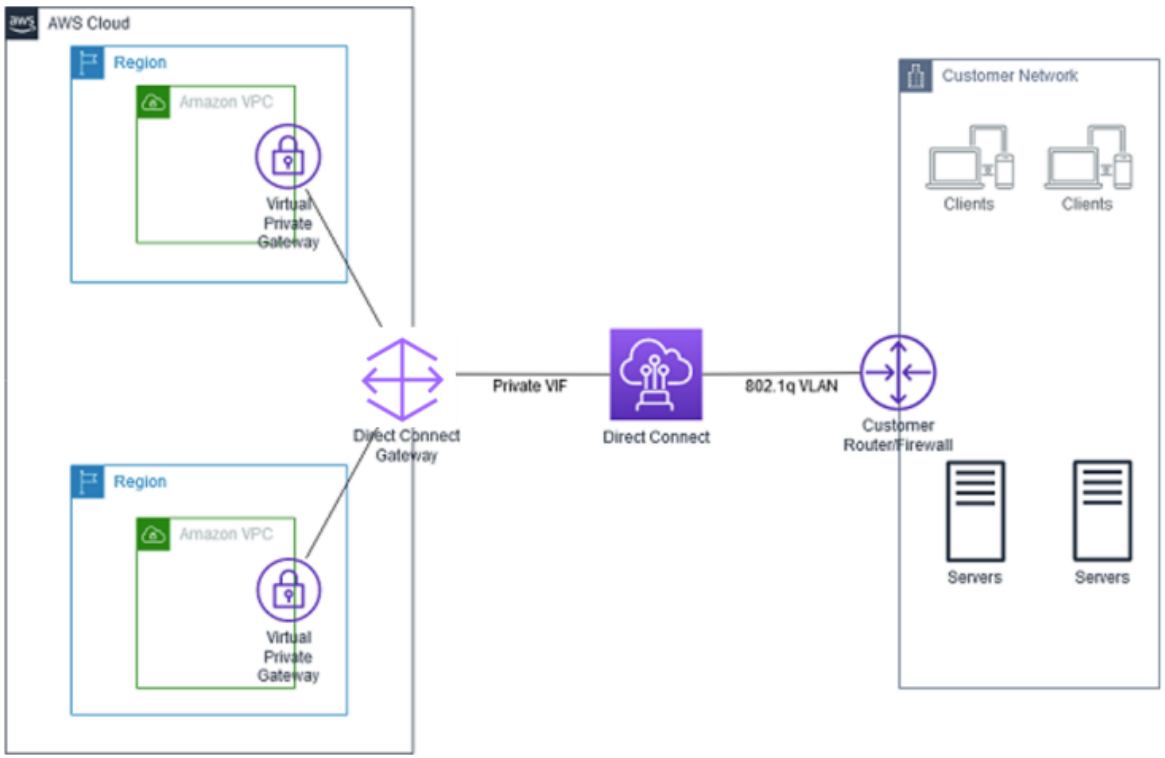
Logging and Monitoring

- Use VPC Flow Logs to monitor the ingress/egress traffic that reaches your VPC instances
- Use AWS Security Hub and AWS GuardDuty to check for malicious network accessibility from your VPC instances
- Use AWS Lambda to take immediate actions (e.g, isolate/delete instance).



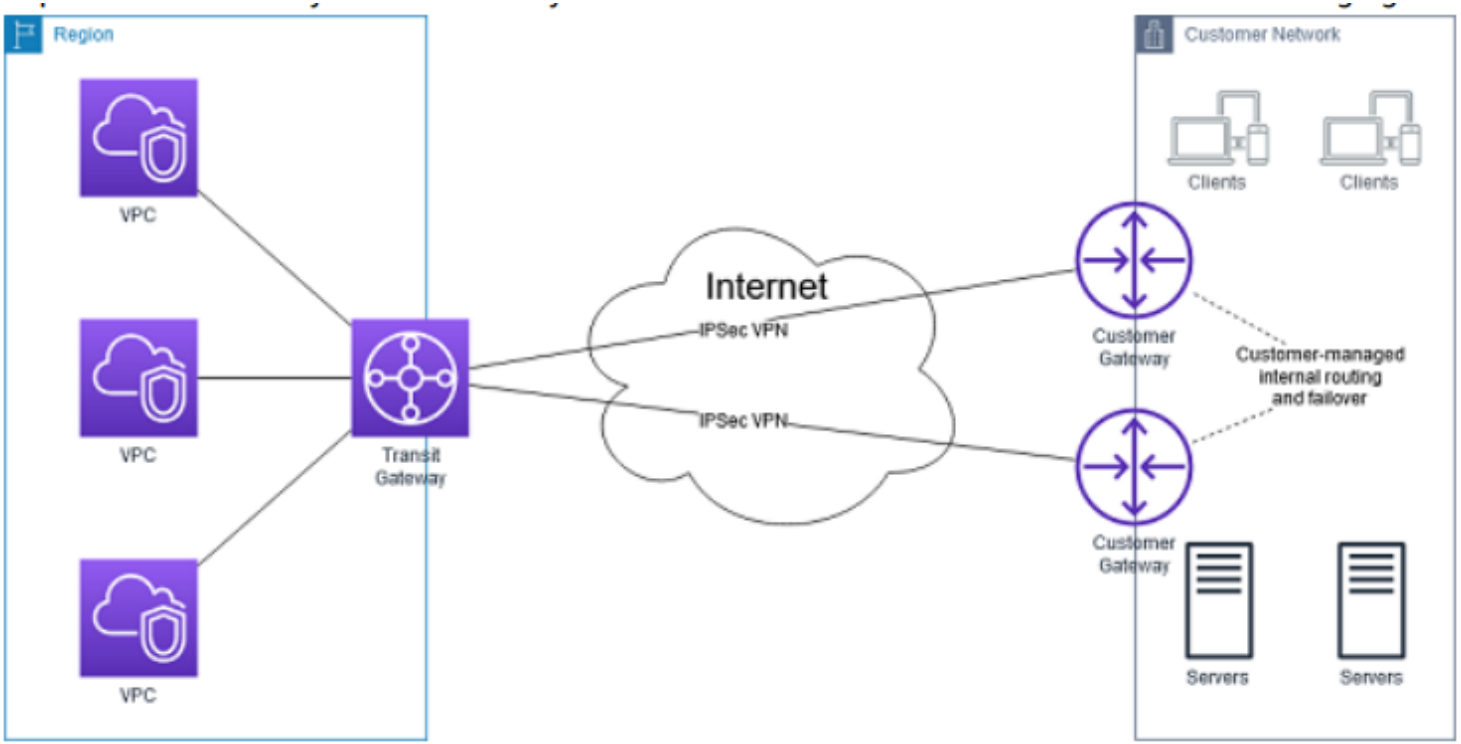
Remote Access Security

- Use Virtual Private Network or AWS Direct Connect to establish private connections from remote networks to VPCs
  - *AWS Direct Connect* helps to etablish a dedicated connection between on-premises network to one or many VPCs in a single region (without/through a gateway)



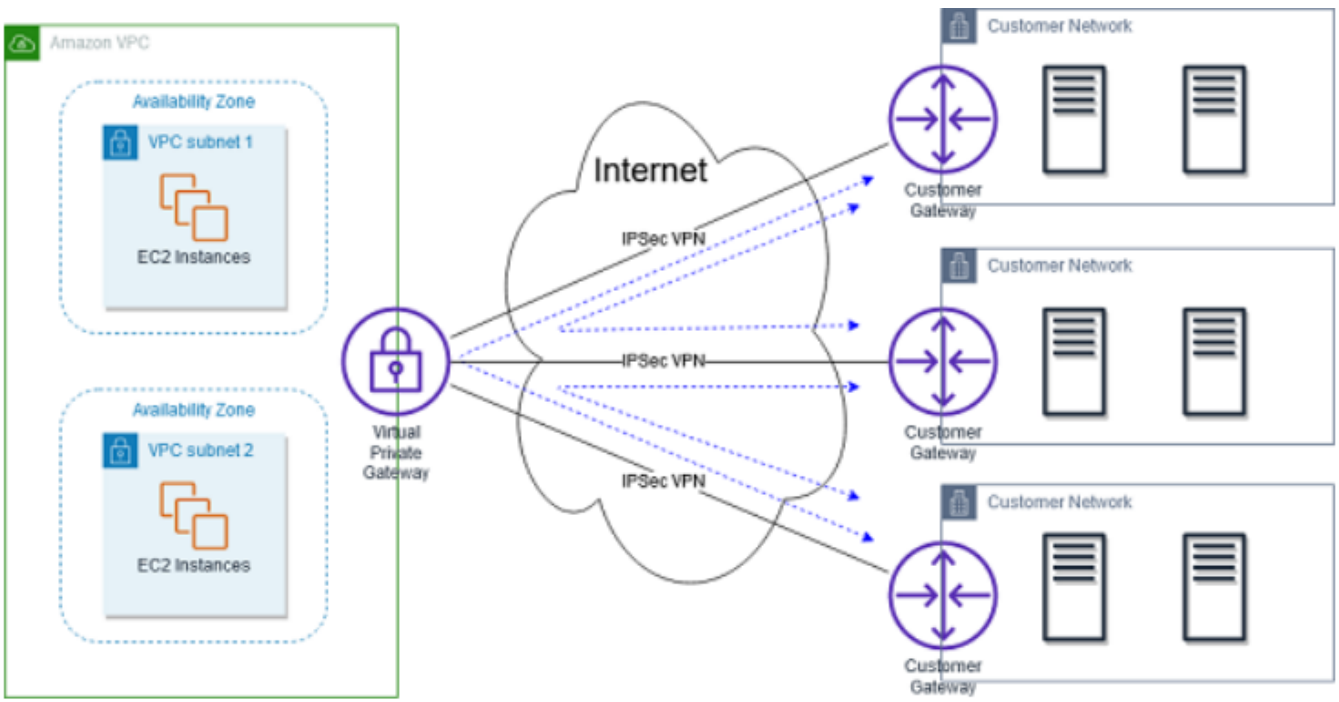
Remote Access Security

- Use Virtual Private Network or...(Next)
  - *AWS Transit Gateway* helps to interconnect VPCs and customer networks, allowing IPsec VPN connections or Direct Connect VPN connections.



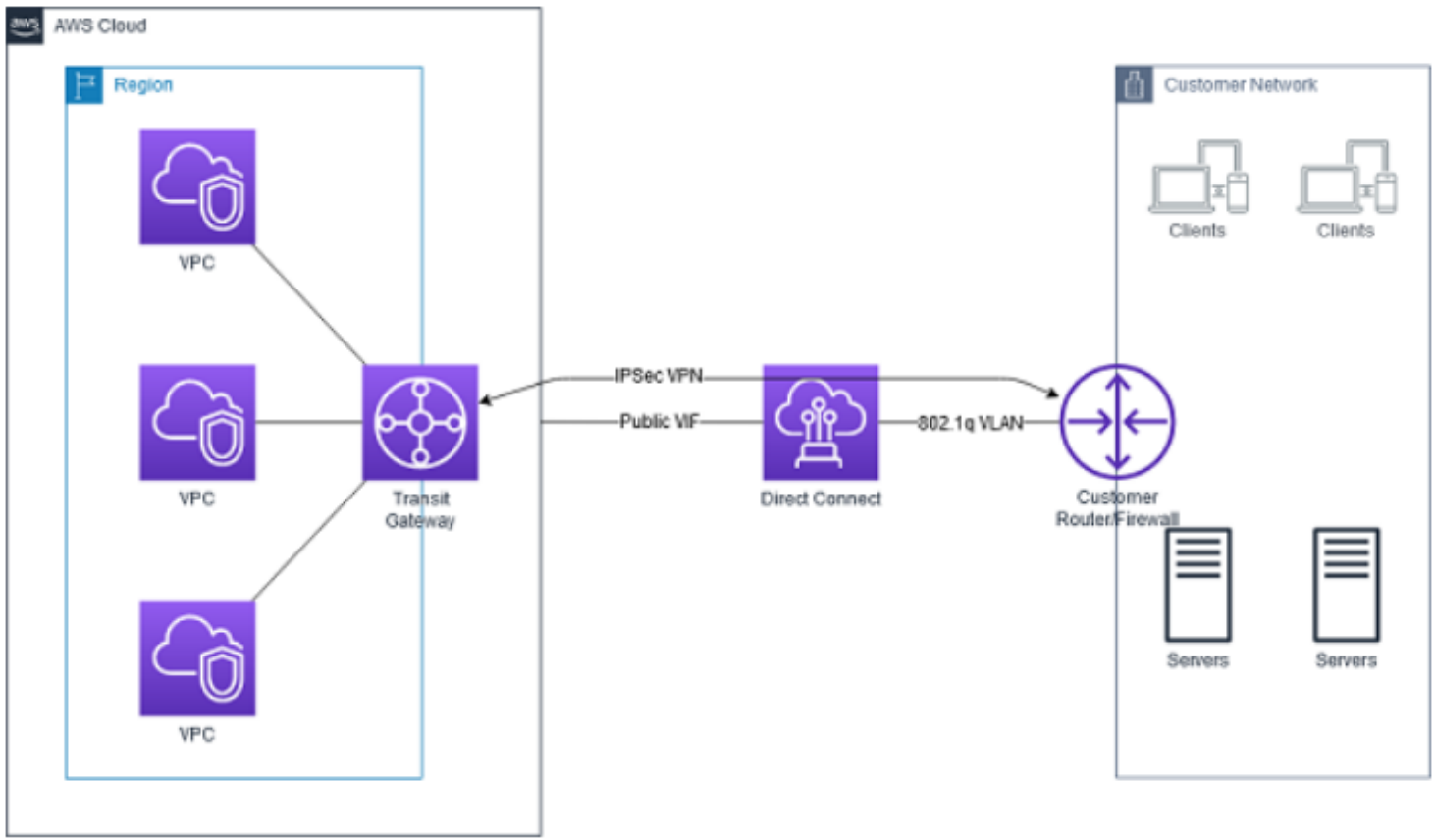
Remote Access Security

- Use Virtual Private Network or...(Next)
  - *AWS VPN CloudHub* is a low-cost hub-spoke model allowing secure primary/backup connectivity between multiple branch offices using a virtual private gateway with multiple customer gateways



Remote Access Security

- Use Virtual Private Network or...(Next)
  - *AWS Direct Connect + Transit Gateway + VPN* can be combined to minimize the cost and latency of IPsec VPN connections to multiple VPCs in the same region



Sondage ☺: `https://app.wooclap.com/XYLCCG`.

wooclap

VPC Management policies

- Help to define security policies to be applied on VPC and subnets
- Recall that an IAM policy specifies the effect (e.g., Allow, Deny), actions (e.g., ec2:CreateVPC) and resources (e.g., arn:aws:ec2:*:*:route-table/*).
- For example, the following policy allows one to create VPC and its associated subnets, routing tables, and internet gateways

```
"Statement": [{
   "Effect": "Allow",
   "Action": [
     "ec2:CreateVpc",
     "ec2:CreateSubnet",
     "ec2:DescribeAvailabilityZones",
     "ec2:CreateRouteTable",
     "ec2:CreateRoute",
     "ec2:CreateInternetGateway",
     "ec2:AttachInternetGateway",
     "ec2:AssociateRouteTable",
     "ec2:ModifyVpcAttribute"
   ],
   "Resource": "*"
 }
]
```

VPC Management Policies

- Enforce an IAM policy to manage VPC resources (e.g., modification routing table, deleting internet gateway) given a purpose tag (e.g., test, dev, production)

```
{
    "Effect": "Allow",
    "Action": "ec2:DeleteInternetGateway",
    "Resource": "arn:aws:ec2:*:*:internet-gateway/*",
    "Condition": {
        "StringEquals": {
            "ec2:ResourceTag/Purpose": "Test"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:DeleteRouteTable",
        "ec2:CreateRoute",
        "ec2:ReplaceRoute",
        "ec2:DeleteRoute"
    ],
    "Resource": "arn:aws:ec2:*:*:route-table/*",
    "Condition": {
        "StringEquals": {
            "ec2:ResourceTag/Purpose": "Test"
        }
    }
}
```

Security Group policies

- Enforce an IAM policy to manage egress/ingress security groups attached to a VPC (create, update, modify, revoke)

```
"Statement":[{
  "Effect":"Allow",
  "Action": [
     "ec2:AuthorizeSecurityGroupIngress",
     "ec2:RevokeSecurityGroupIngress",
     "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
     "ec2:AuthorizeSecurityGroupEgress",
     "ec2:RevokeSecurityGroupEgress",
     "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
     "ec2:ModifySecurityGroupRules"
  ],
   "Resource": "arn:aws:ec2:region:account-id:security-group/*",
    "Condition": {
      "ArnEquals": {
        "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/vpc-id"
      }
    }
  },
```

Remote Access Policies

- Enable an IAM policy to use AWS Direct Connect for secure Network to VPC communication

```
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "directconnect:*",
            "ec2:DescribeVpnGateways"
        ],
        "Resource": "*"
    }
]
```

- When the policy is enabled, we can now create a direct connect
  aws directconnect create-connection –location us-east-1 –bandwidth 5Gbps –connection-name "PolyStudent Connection"

Remote Access Policies

- Enable IAM policy to use AWS VPC Peering for secure VPC to VPC communication

```
"Statement": [
  {
    "Effect":"Allow",
    "Action": "ec2:CreateVpcPeeringConnection",
    "Resource": "arn:aws:ec2:region:account-id-1:vpc/*"
  },
  {
    "Effect": "Allow",
    "Action": "ec2:CreateVpcPeeringConnection",
    "Resource": "arn:aws:ec2:region:account-id-1:vpc-peering-connection/*",
    "Condition": {
      "ArnEquals": {
        "ec2:AccepterVpc": "arn:aws:ec2:region:account-id-2:vpc/vpc-id"
      }
    }
  }
]
```

- When the policy is enabled, we can now create a VPC peering connection
  aws ec2 create-vpc-peering-connection –vpc-id vpc1 –peer-vpc-id vpc2

Logging policies

- Enable VPC flow logging on S3 buckets. Two actions are needed: *s3:PutObject* for write access and *s3:GetBucketAcl* for read access.

```
{
    "Sid": "AWSLogDeliveryWrite",
    "Effect": "Allow",
    "Principal": {
        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "my-s3-arn",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": account_id,
            "s3:x-amz-acl": "bucket-owner-full-control"
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:logs:region:account_id:*"
        }
    }
},
{
    "Sid": "AWSLogDeliveryAclCheck",
    "Effect": "Allow",
    "Principal": {
        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": "s3:GetBucketAcl",
    "Resource": "arn:aws:s3:::bucket_name",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": account_id
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:logs:region:account_id:*"
        }
    }
}
```

Traffic Mirroring policies

- Enforce IAM policy to allow the creation of a traffic mirror session for backup/redundancy and monitoring purposes

```
"Statement": [
    {
        "Effect": "Allow",
        "Action": "ec2:CreateTrafficMirrorSession",
        "Resource": [
            "arn:aws:ec2:*:*:traffic-mirror-target/tmt-12345645678",
            "arn:aws:ec2:*:*:traffic-mirror-filter/*",
            "arn:aws:ec2:*:*:network-interface/*"
        ]
    }
]
```

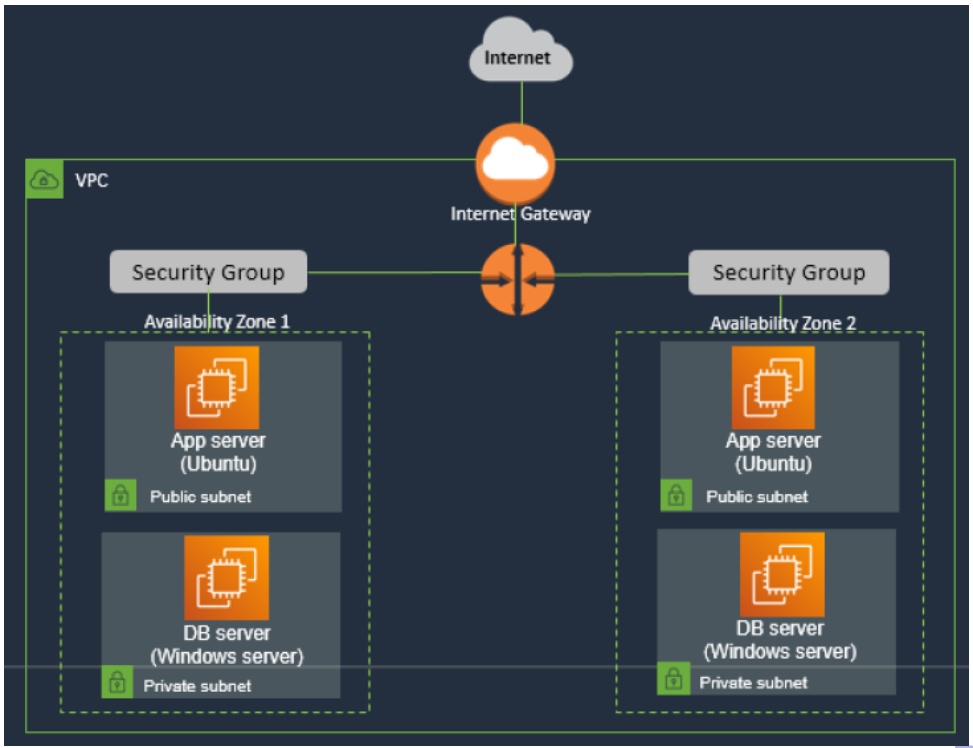
- When the policy is enforced, we can now create a traffic mirroring session
  aws ec2 create-traffic-mirror-session –description "test backup" –traffic-mirror-target-id tmt-07feffffTest –network-interface-id eni-0702ffffffTest –session-number 1 –packet-length 25 –traffic-mirror-filter-id tmf-0436fffffTest

Sondage ☺: `https://app.wooclap.com/XHDMKA`.

wooclap

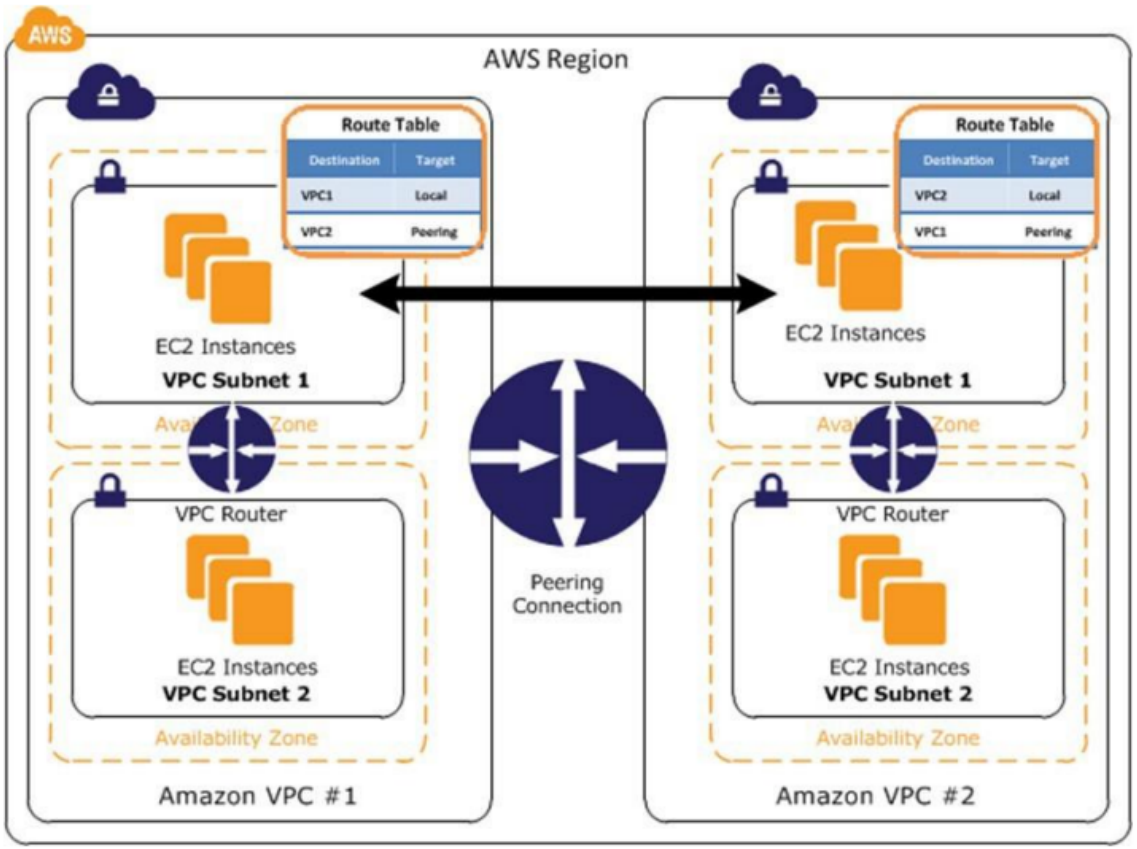
Availability Zones & Regions

- Use AWS Regions and Availability Zones (AZ) in the VPC infrastructure
- to allow multiple physically separated and isolated AZs connected with low-latency, high-throughput, and highly redundant networking



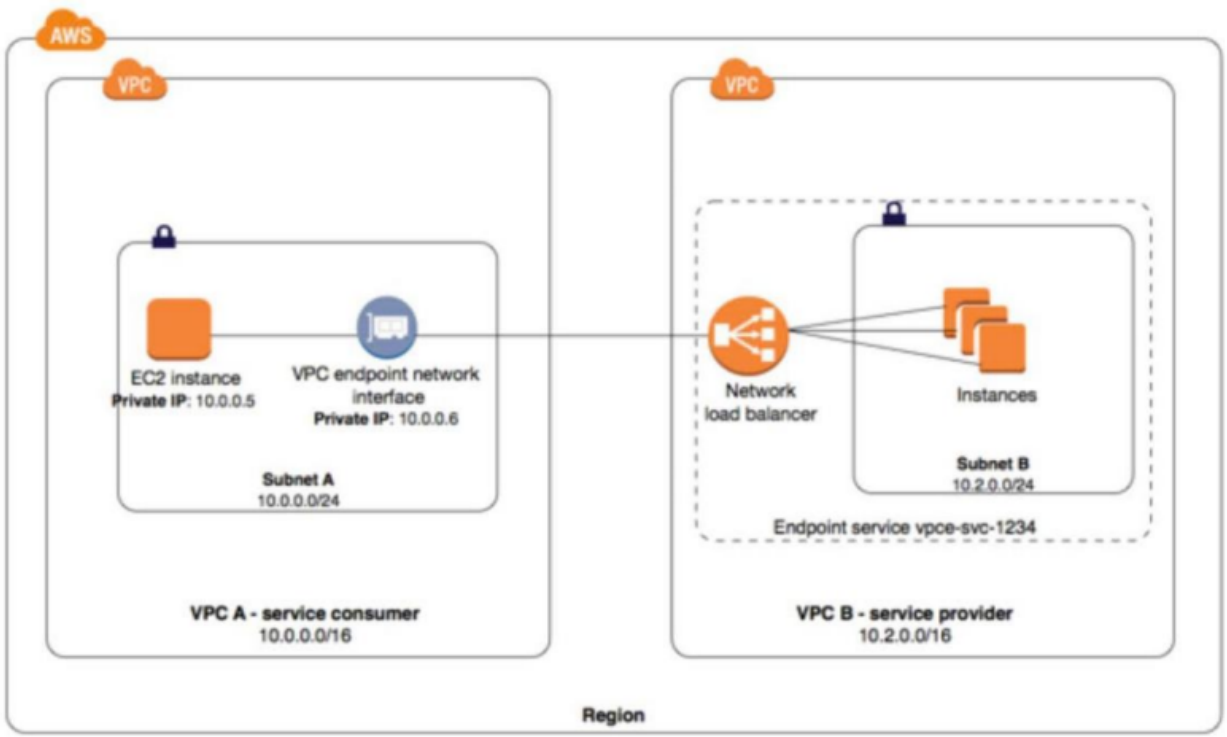
Data Replication

- Enforce replication/redundancy in one or multiple regions using VPC-to-VPC connectivity
  - *AWS VPC Peering* enables networking connection between two VPCs using their private IP addresses: no single point of failure, no network bandwidth bottleneck



Data Replication

- Enforce replication/redundancy in ... (Next)
  - *AWS PrivateLink* enables private connections between VPCs using interface VPC endpoints whose access can be made using AWS Direct Connect or managed using security groups

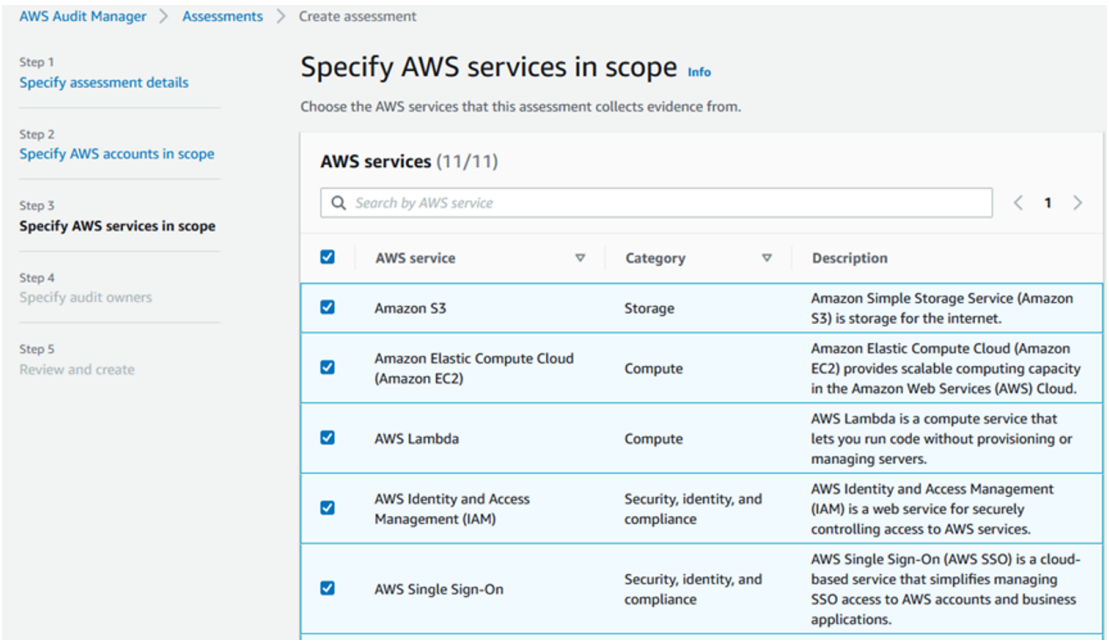


Sondage ☺: `https://app.wooclap.com/ASKIAD`.

wooclap

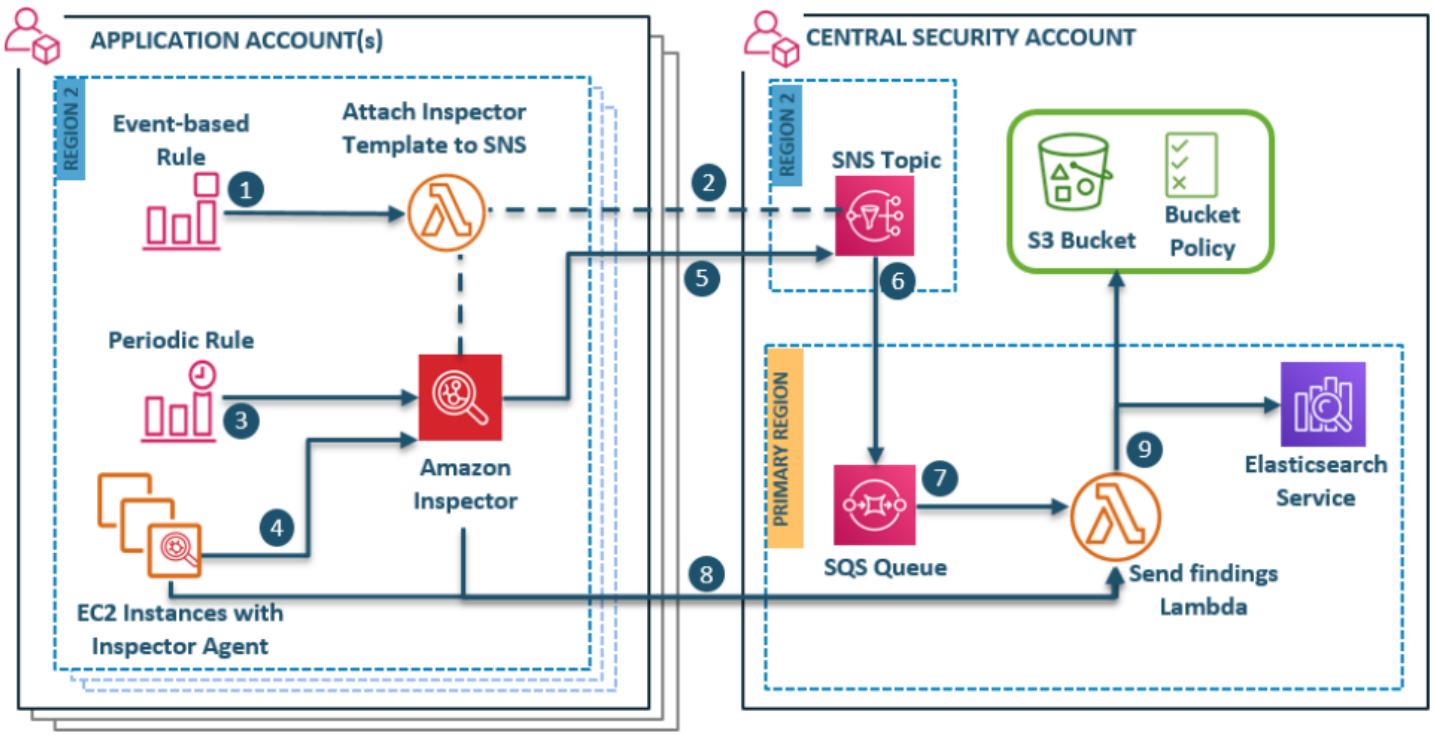
Audit Reports & Evidence

- Access audit reports using AWS Artifact such as Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, or ISO/IEC 27001:2013 reports
- Continuously collect evidence from AWS usage (VPC, S3, EC2, etc.) to simplify compliance with regulation/standards using AWS Audit Manager



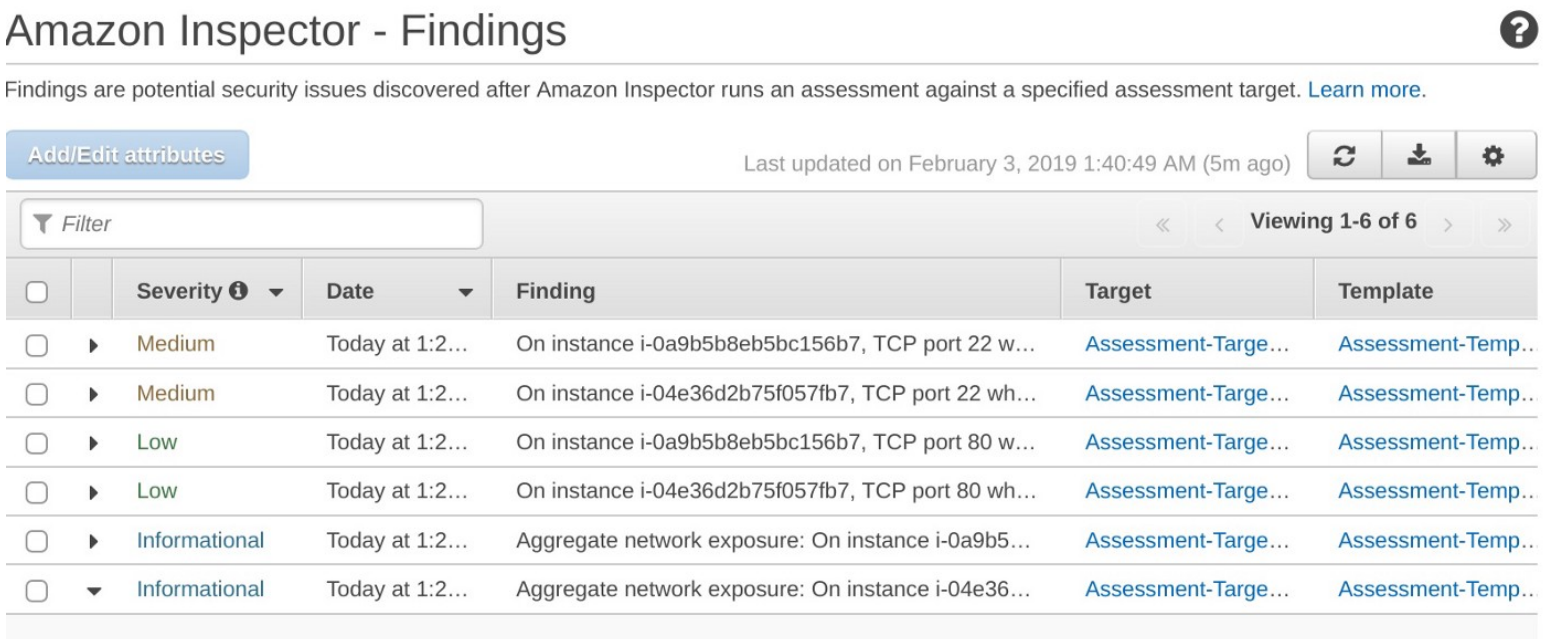
Vulnerability Assessment

- Assess VPC, EC2 instances, and application configurations for exposure, vulnerabilities, and deviations from best practices using AWS Inspector



Vulnerability Logging & Monitoring

- Log and Monitor vulnerability findings from AWS Inspector agents to CloudTrail and CloudWatch



Amazon Inspector - Findings

Findings are potential security issues discovered after Amazon Inspector runs an assessment against a specified assessment target. Learn more.

Add/Edit attributes

Last updated on February 3, 2019 1:40:49 AM (5m ago)

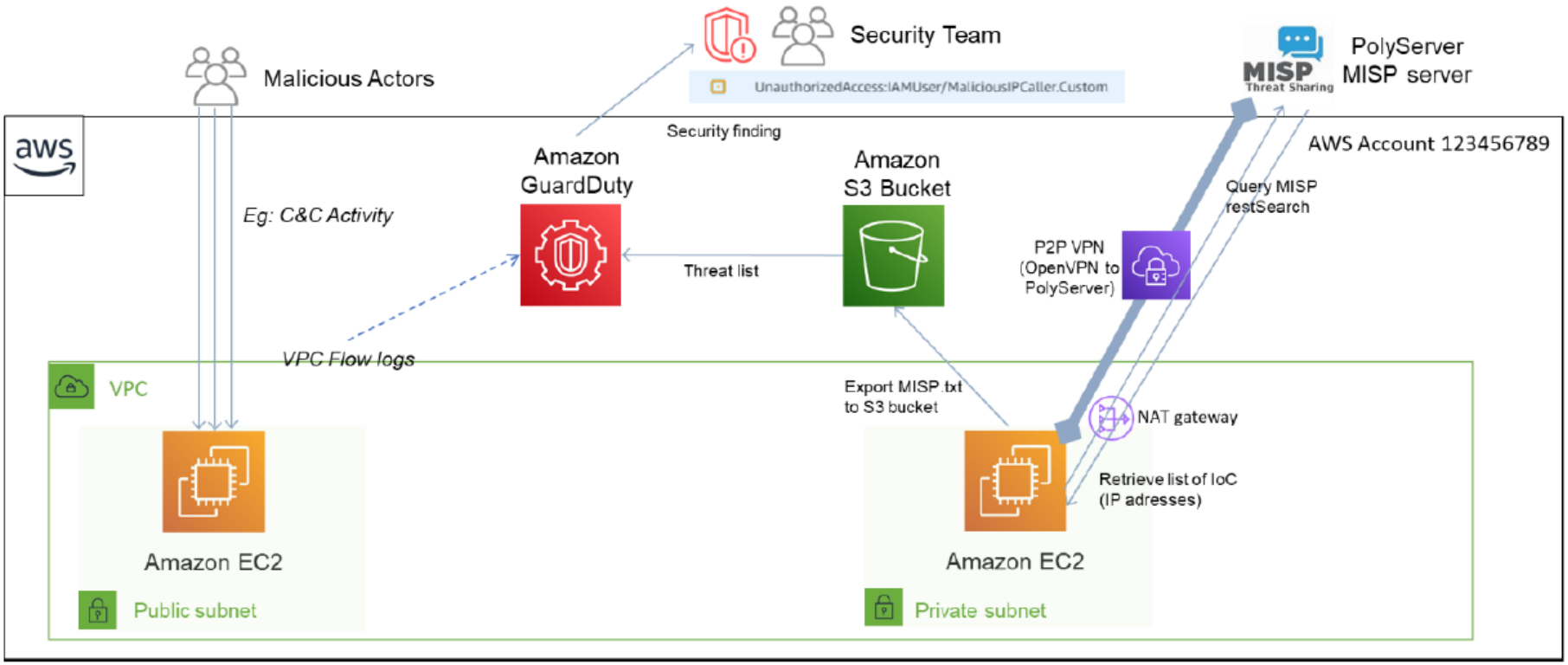
Filter

Viewing 1-6 of 6

Severity	Date	Finding	Target	Template
Medium	Today at 1:2…	On instance i-0a9b5b8eb5bc156b7, TCP port 22 w…	Assessment-Targe…	Assessment-Temp…
Medium	Today at 1:2…	On instance i-04e36d2b75f057fb7, TCP port 22 wh…	Assessment-Targe…	Assessment-Temp…
Low	Today at 1:2…	On instance i-0a9b5b8eb5bc156b7, TCP port 80 w…	Assessment-Targe…	Assessment-Temp…
Low	Today at 1:2…	On instance i-04e36d2b75f057fb7, TCP port 80 wh…	Assessment-Targe…	Assessment-Temp…
Informational	Today at 1:2…	Aggregate network exposure: On instance i-0a9b5…	Assessment-Targe…	Assessment-Temp…
Informational	Today at 1:2…	Aggregate network exposure: On instance i-04e36…	Assessment-Targe…	Assessment-Temp…

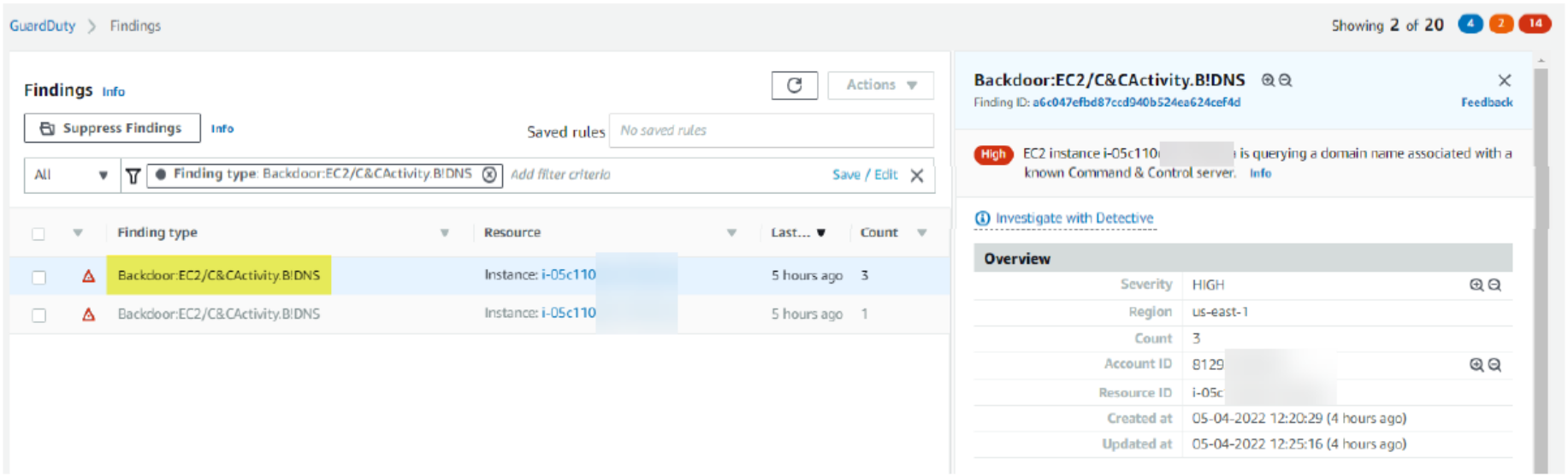
Threat monitoring

- Continuously monitor AWS accounts, running resources (VPC Flow logs, EC2, S3) and generates detailed findings (alerts) about security postures on VPCs



Threat Detection

- From VPC Flow logs, GuardDuty checks the reputation of IP addresses and identify malicious IP of an EC2 instance (e.g., Backdoor CC activity).



Sondage ☺: `https://app.wooclap.com/SFLUBI`.

wooclap