플렉스팀 AWS 보안 아키텍쳐

이 3rd-party는 왜 필요할까?

flex

flex가 대체 뭐죠? 뭐하는 곳이죠?

“팀 성장을 만드는 단 하나의 HR”

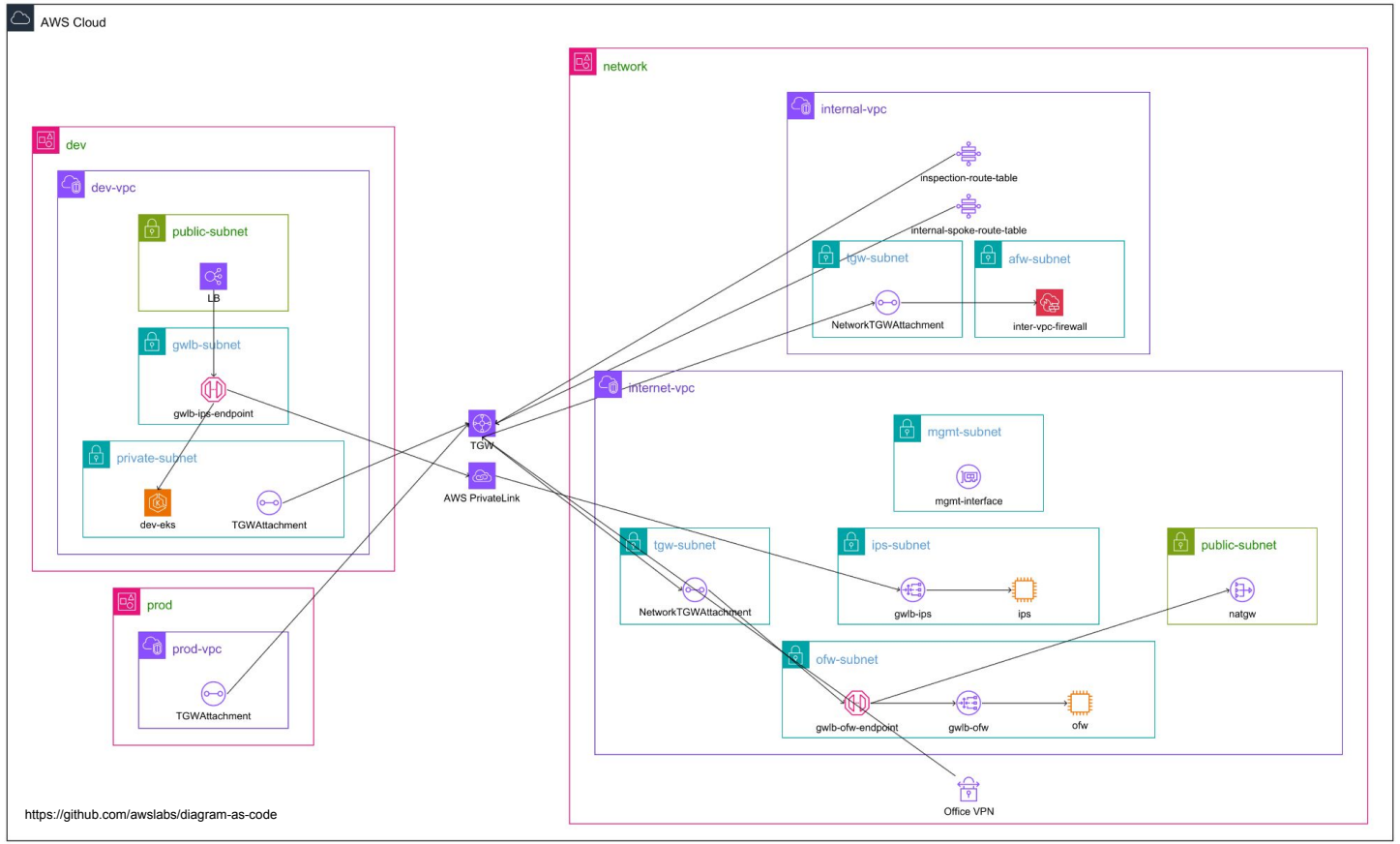
- HR Platform (https://flex.team/)
  - SaaS
  - B2B
- MSA X AWS
  - Multi-Account / Multi-VPC
  - EKS + Istio 기반

Cloud Native Security?!

- 3rd-party 솔루션을 도입하면 Cloud Native 아니지 않아?!
  - 꼭 그렇지만은 않다!

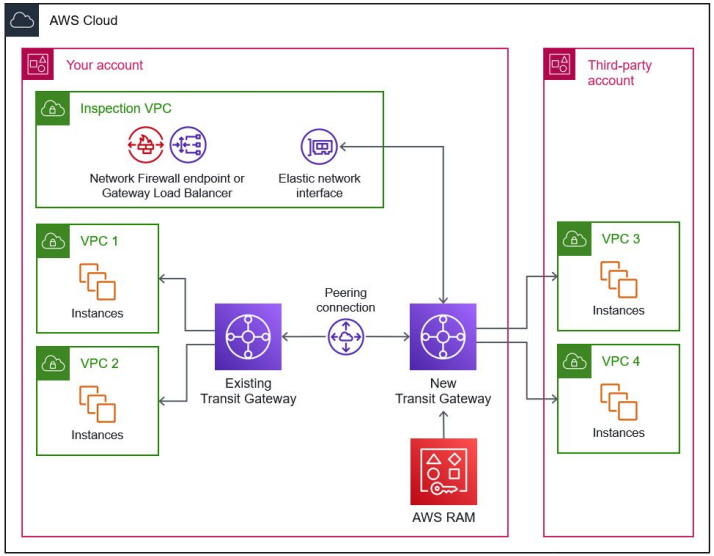
- 3rd-party 솔루션을 도입할때 중요하게 생각한 포인트
  - 확장 가능성
    - GWLB 형태로 구성이 가능할까?
  - IaC
    - Code로 정의 가능한가?
  - Dynamic Security
    - MSA 형태의 서비스를 커버할 수 있는가?
    - EKS 환경에 적합한가?

네트워크 구성도


AWS Cloud
network
internal-vpc
inspection-route-table
internal-spoke-route-table
tgw-subnet
afw-subnet
NetworkTGWAttachment
inter-vpc-firewall
dev
dev-vpc
public-subnet
LB
gwlb-subnet
gwlb-ips-endpoint
private-subnet
dev-eks
TGWAttachment
TGW
AWS PrivateLink
internet-vpc
mgmt-subnet
mgmt-interface
tgw-subnet
NetworkTGWAttachment
ips-subnet
gwlb-ips
ips
public-subnet
natgw
ofw-subnet
gwlb-ofw-endpoint
gwlb-ofw
ofw
prod
prod-vpc
TGWAttachment
Office VPN
https://github.com/awslabs/diagram-as-code

네트워크 중앙화

- (TGW + RAM) X Terraform
  - multi-account 환경에서 TGW는 RAM으로 단순화!
  - Terraform을 통해 신규 Account/VPC 추가 단순화!



https://docs.aws.amazon.com/prescriptive-guidance/latest/integrate-third-party-services/architecture-3-1.html

```
locals {
  attachment_list = [
    [redacted]
  ]
}

data "aws_ec2_transit_gateway_attachment" "spoke-vpc-attachment" {
  for_each = { for a in local.attachment_list : a => { "name" = a} }
  filter {
    name   = "transit-gateway-id"
    values = [aws_ec2_transit_gateway.tgw.id]
  }

  filter {
    name = "tag:Name"
    values = ["[redacted]/${each.key}-attachment"]
  }
}

locals {
  route_destnation = [
    {
      name = "[redacted]"
      cidr = "[redacted]"
      target = data.aws_ec2_transit_gateway_attachment.[redacted].id
      rt_association = true
      internal_inspection = true
    },
```

Inter-VPC 제어

- ANF X Terraform
  - Inter-VPC간 트래픽을 최소 비용으로 Security zoning!
  - ANF 손으로 하고 계신가요? Terraform은요?
  - Alert과 Pass를 한번에 설정할 수 있도록 해서 3rd-party 방화벽과 최대한 유사하게 설정

```
{
  protocol = "TLS"
  source = "$DEV"
  source_port = "ANY"
  destination = "[                                                    ]"
  destination_port = "ANY"
  direction = "ANY"
  sid = 402
  msg = "allow tls dev-vpc to dev environ"
},
{
  protocol = "HTTP"
  source = "$DEV"
  source_port = "ANY"
  destination = "[                                                    ]"
  destination_port = "ANY"
  direction = "ANY"
  sid = 404
  msg = "allow http dev-vpc to dev environ"
},
```

```
locals {
  apply_allow_rule =  flatten([
    for rule in var.allow_rule : [
      for action in ["ALERT","PASS"] : {
        action = action
        header = rule
        options = {
          sid = [( action == "ALERT" ? "${rule.sid}" : "${rule.sid+1}" )]
          msg = ["\"${rule.msg}\""]
        }
      }
    ]
  ])
}

check "sid_number" {
  assert {
    condition = alltrue([
      for v in var.allow_rule : (v.sid % 2 == 0)
    ])
    error_message = "sid is must be even number!"
  }
}
```

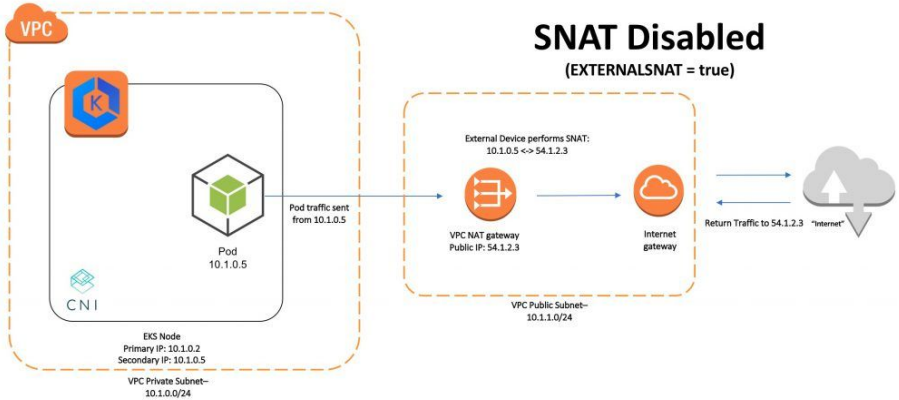
침해대응/탐지

- Private Link + GWLB
  - TGW를 경유하지 않고 직접 Attach 가능
  - 비교적 덜 복잡한 라우팅 / 부분 적용 가능
  - Scale-out이 용이함
  - 이 또한 Terraform으로!

- 왜 ANF의 Suricata를 사용하지 않나요?
  - 풍부한 Vendor Rule
  - Rule관리까지 Terraform으로 어려움
  - 탐지된 공격의 Payload 확인 어려움
- 극세사팁
  - PrivateLink를 경유하면 SG Chain이 되지 않아요!
  - 라우팅 전환 시 Terraform으로 하면 순단이 발생할 수 있어요!
    - AWS CLI를 사용해보세요! (replace-route-table-association)

외부 정보유출 최소화

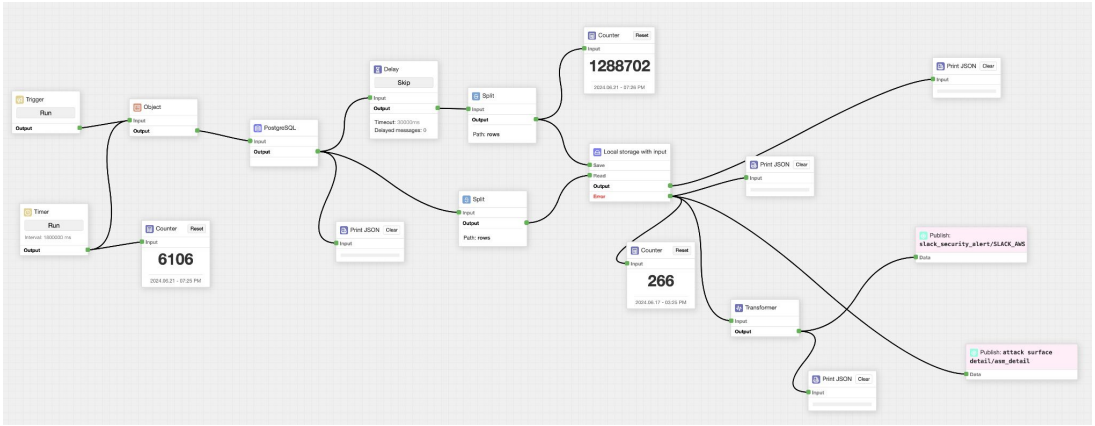
- TGW + GWLB
  - Outbound Traffic을 한곳으로 집중!
  - 이또한 Terraform으로!
- 3rd-party FW
  - AWS_VPC_K8S_CNI_EXTERNALSNAT
  - Pod 별 Outbound 트래픽을 제어합니다.
- 극세사팁
  - GWLB에서 Cross-AZ는 켜주세요.
  - 기본적으로 같은 AZ를 먼저 사용합니다!
  - Object를 미리 다 등록해줘야 트래픽 식별이 가능합니다.



https://aws.amazon.com/ko/blogs/opensource/vpc-cni-plugin-v1-1-available/

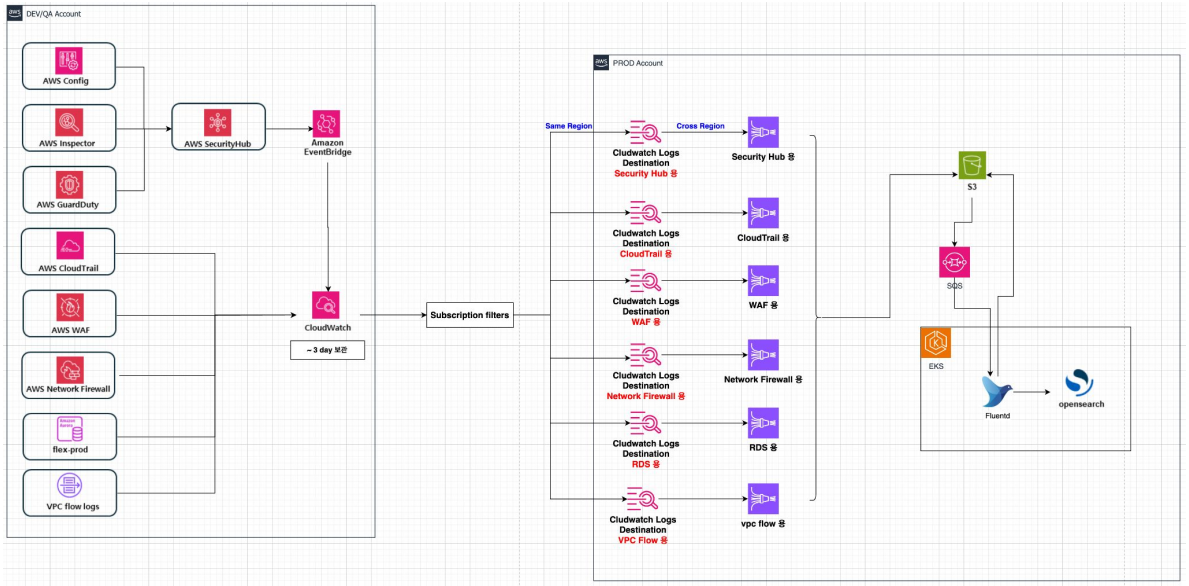
CSPM (Cloud Security Posture Management)

- Low-Code Platforms
  - n8n or total.js/flow + steampipe



Log Pipeline

- Cloudwatch->Firehose->S3 -> SQS -> Fluentd
  - 모든 보안 로그를 한곳으로 집중!
  - 로그양에 따라 Sacle-out!
- 극세사팁
  - Firehose에서 new line 옵션, uncompressed 을 선택하시면 파싱하기 편합니다.



https://dev.to/aws-builders/cross-account-log-data-sharing-using-kinesis-data-firehose-4e9b

Q&A

We are hiring!

https://flex.careers.team/job-descriptions