AWS

PUBLIC SECTOR SUMMIT

Using AWS Networking and Logging Features to Enhance Security

Nathan McGuirt, Senior Solutions Architect, AWS

Dave Rogers, Head of Architecture & Security, UK MOJ Digital & Technology

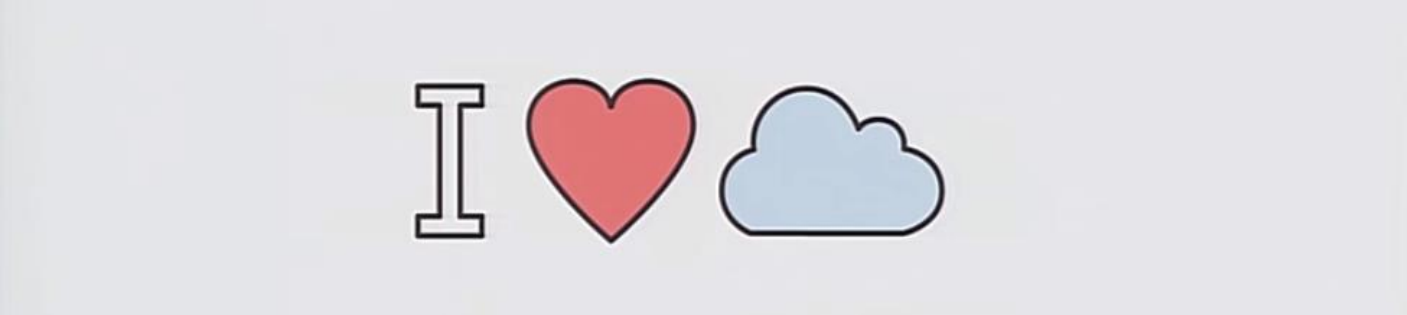
June 2016

Expectations

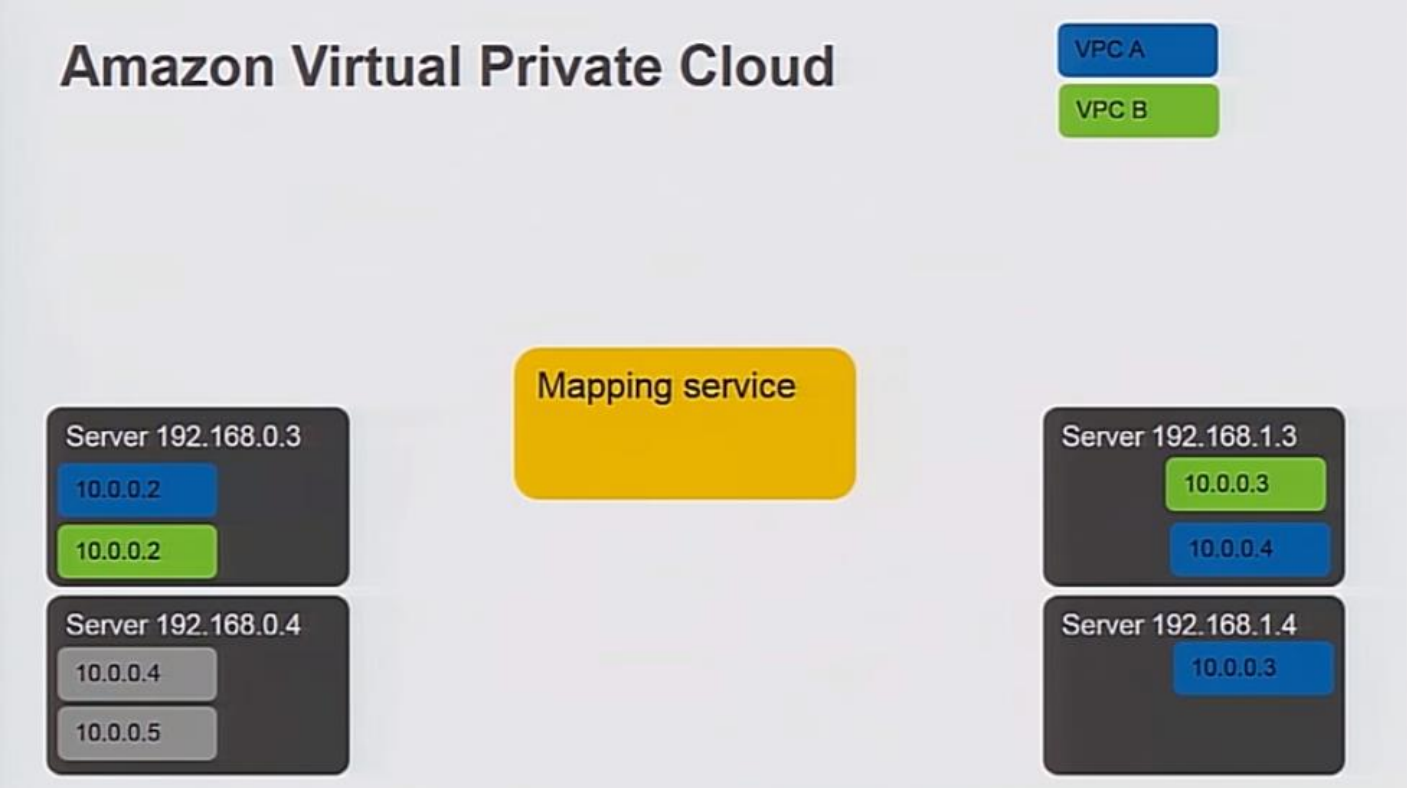
Managing traditional networks is hard

Lack of visibility

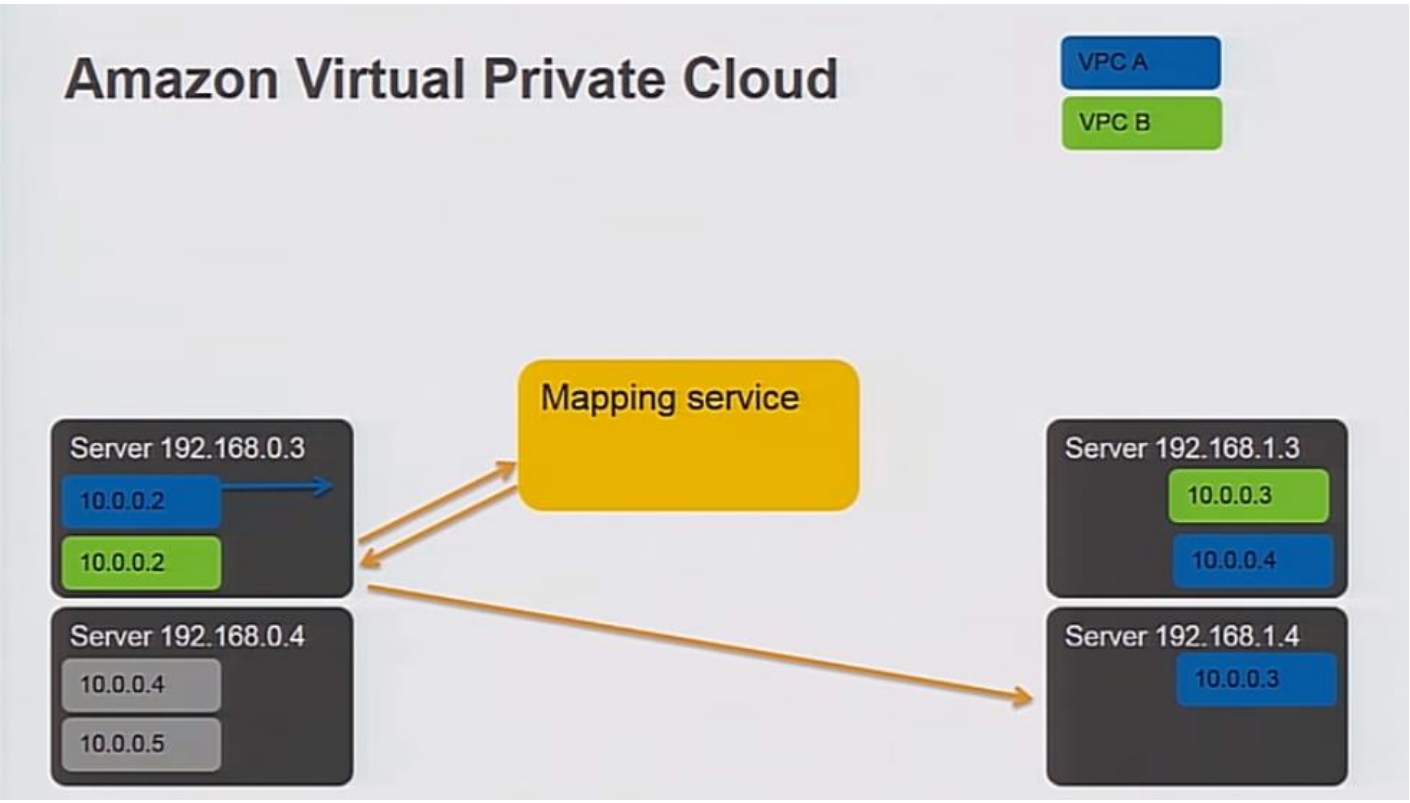
Heavy technical lift



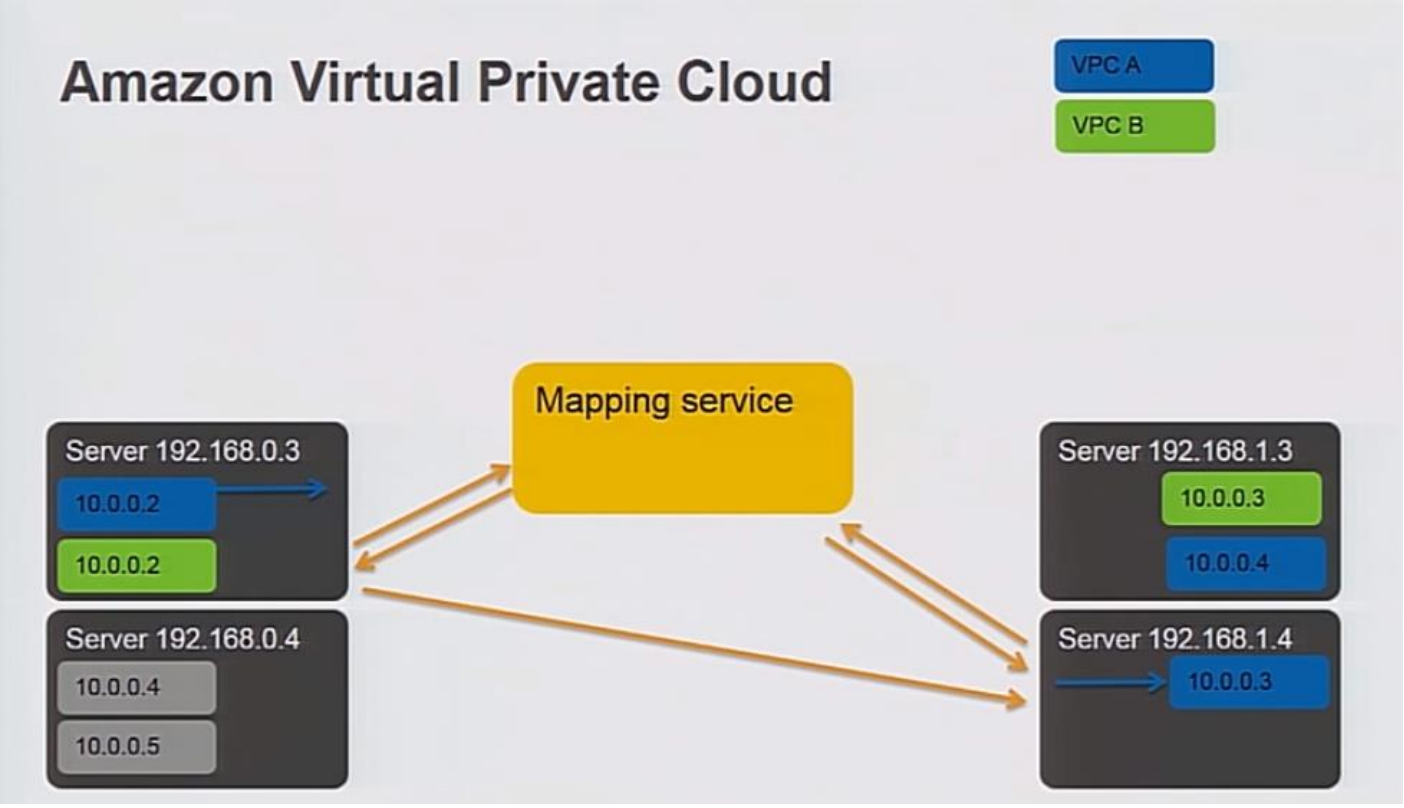
Network enforcement tools

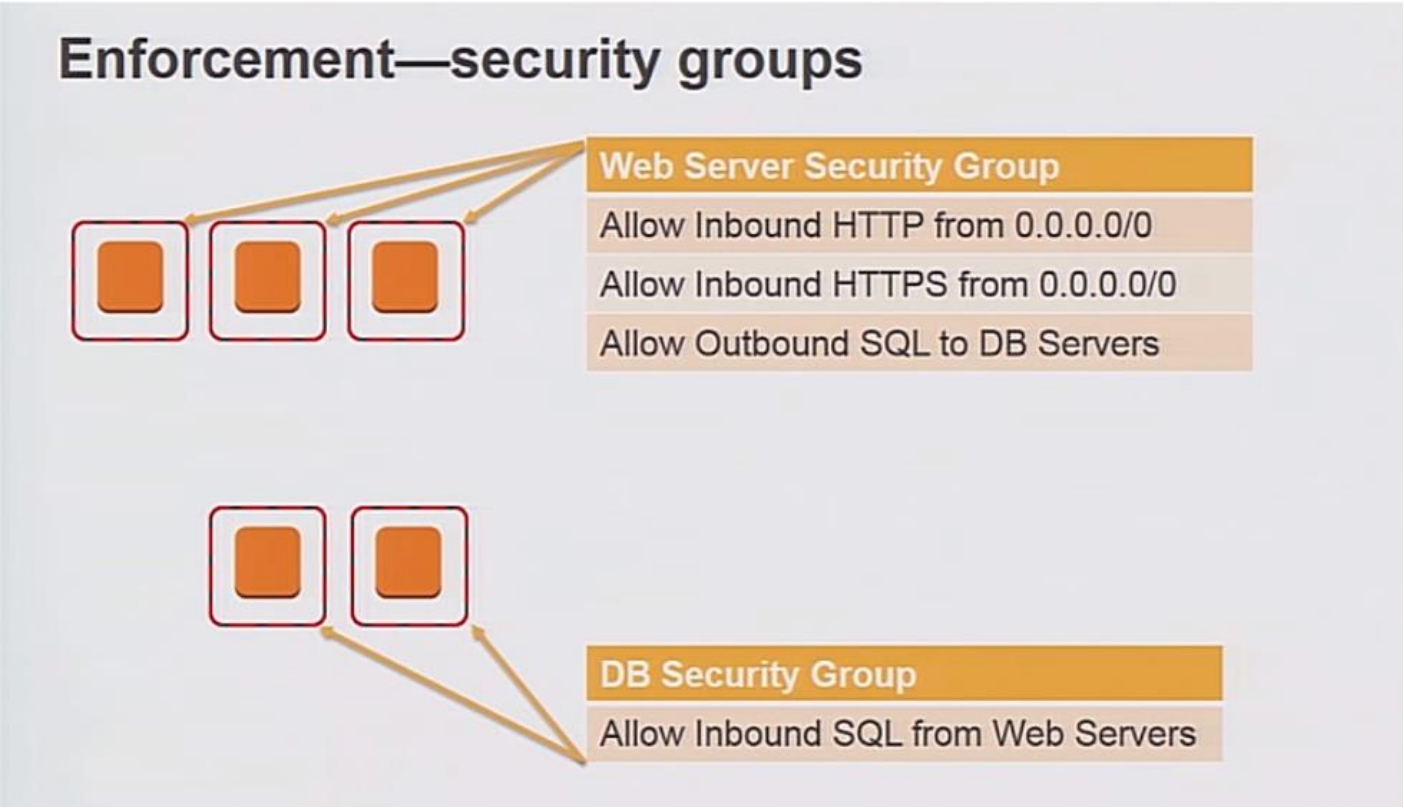


VPC gives you the ability to create isolated networks that you can put your resources into.

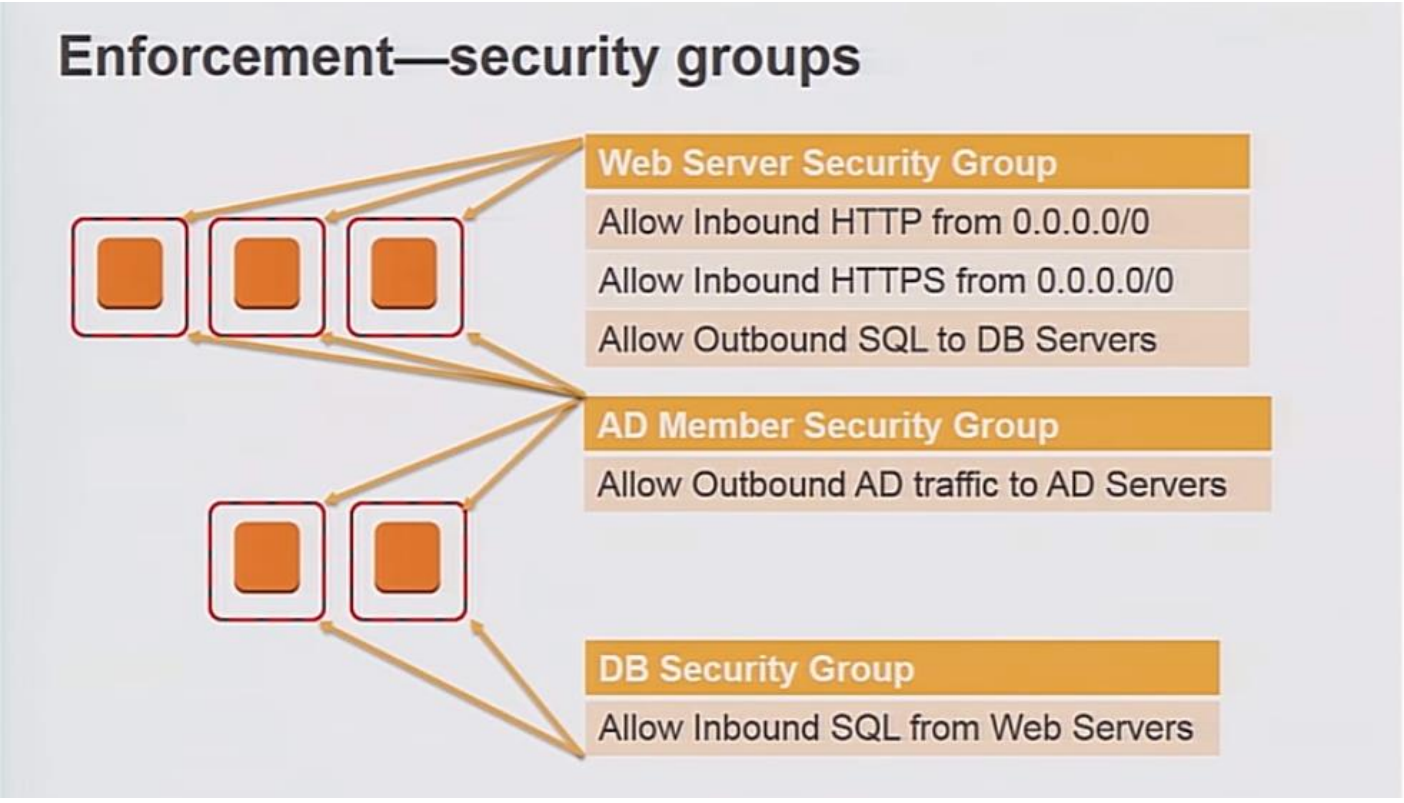


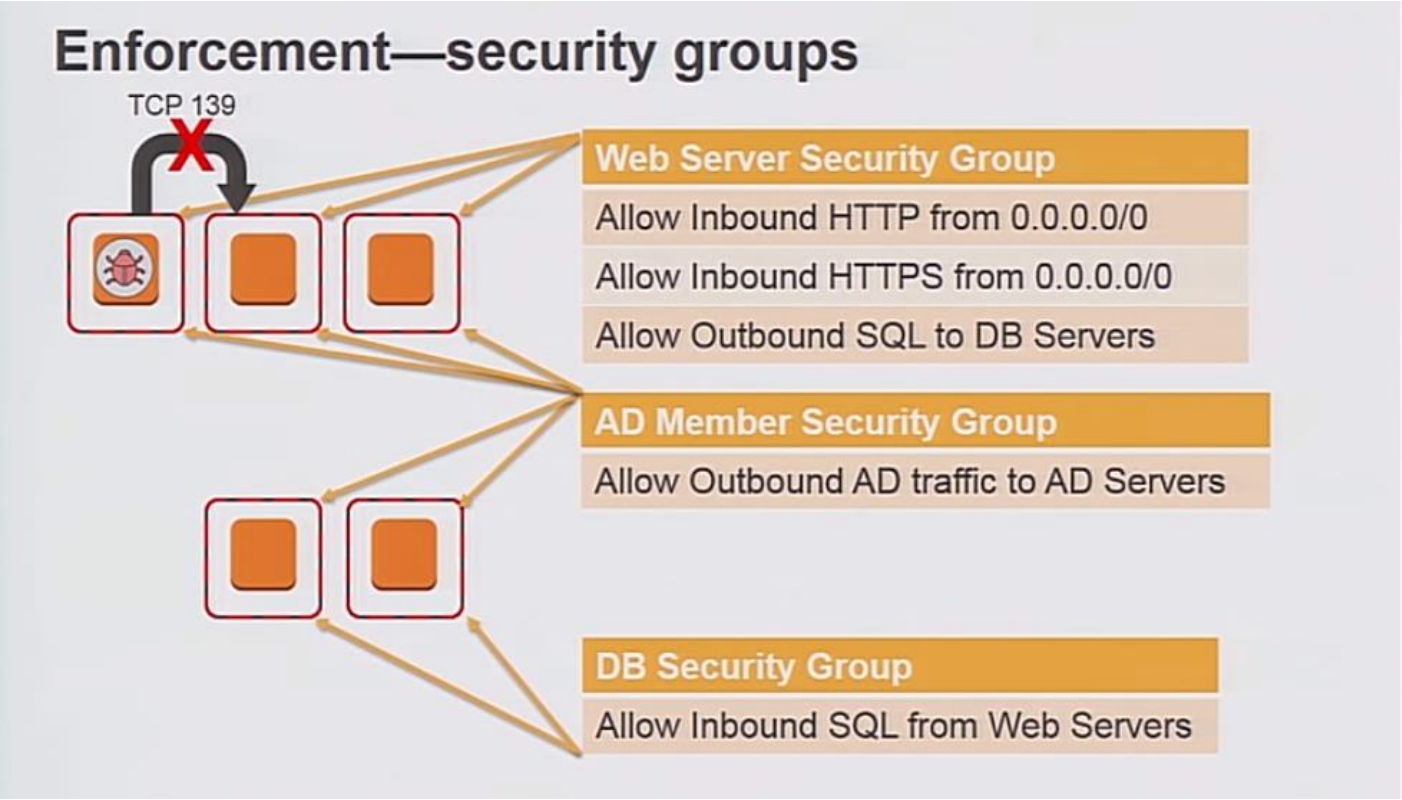
The instances are green and blue are guest OSes from different VPCs that are sitting on some host and need to communicate with other instances on other hosts via packets getting transferred over the simulated ethernet interfaces on the hosts, it needs to talk to the mapping service to know the address of the destination instances.

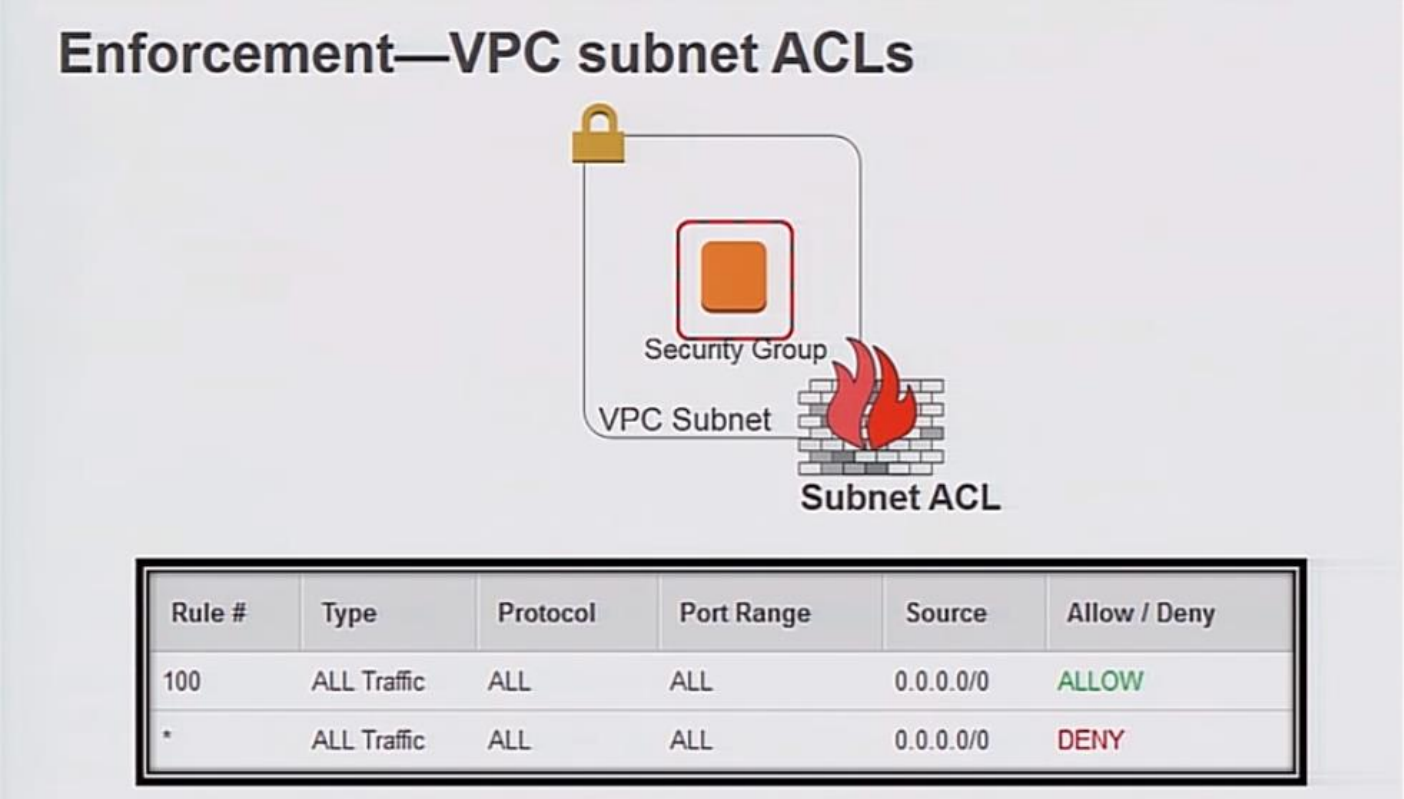




Security groups are stateful firewalls and are mandatory for every instance, SGs can also reference one another. We are only allowing in-bound web traffic only on the DB servers and allow only Outbound traffic for the web servers to the DB servers only.

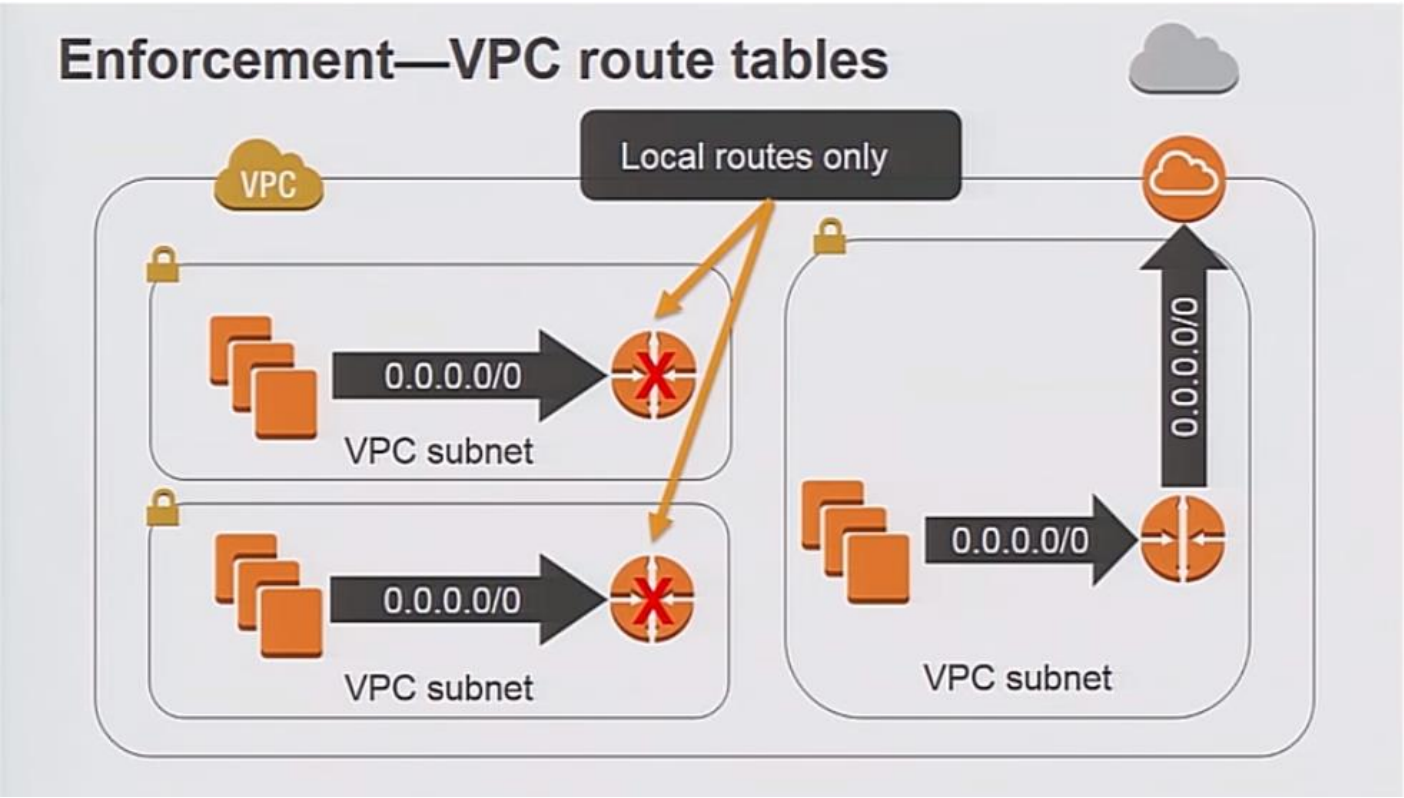




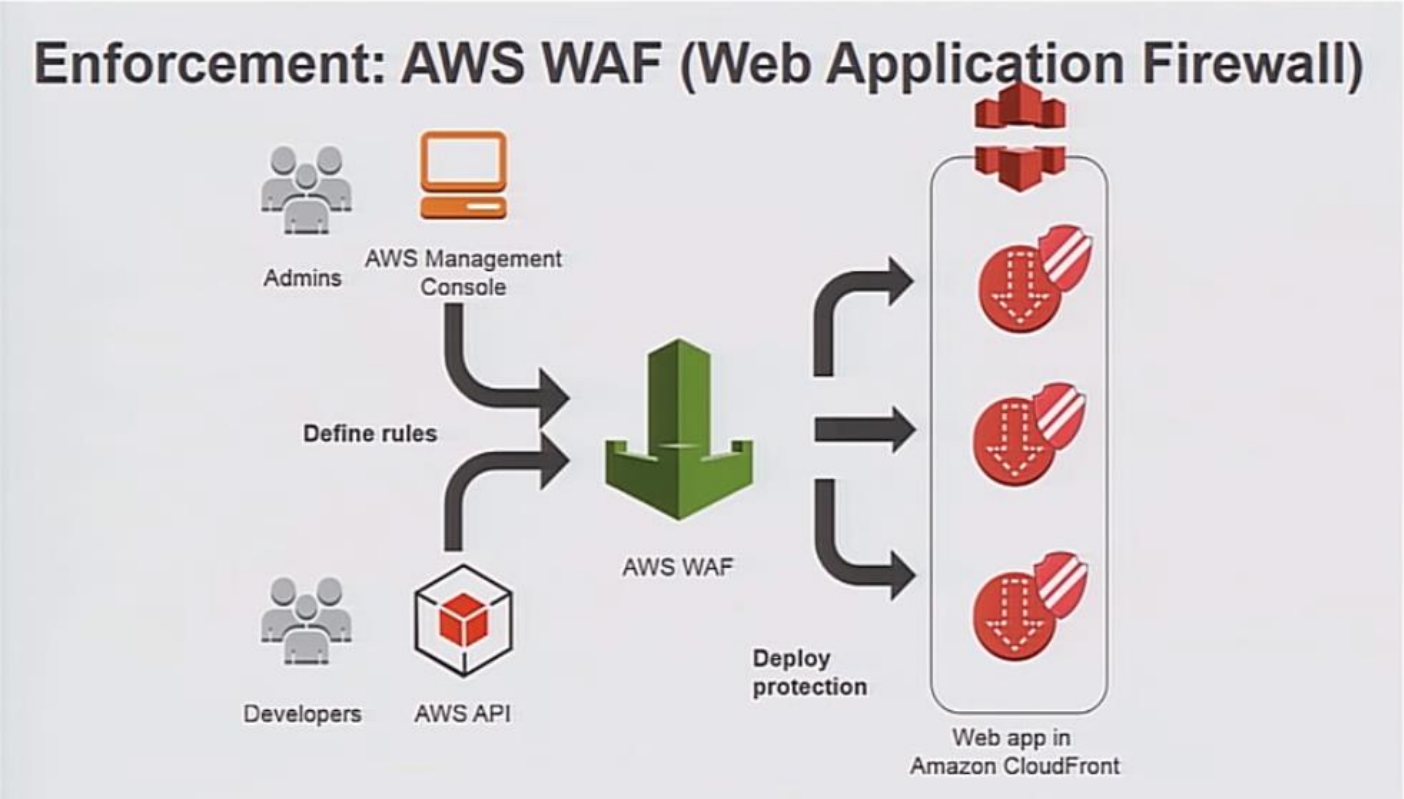


Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

VPC subnet ACLs are explicit ALLOW and DENY rules that are stateless and they apply at the edges of VPC subnets, they can be used as a second level layer for your VPC security.

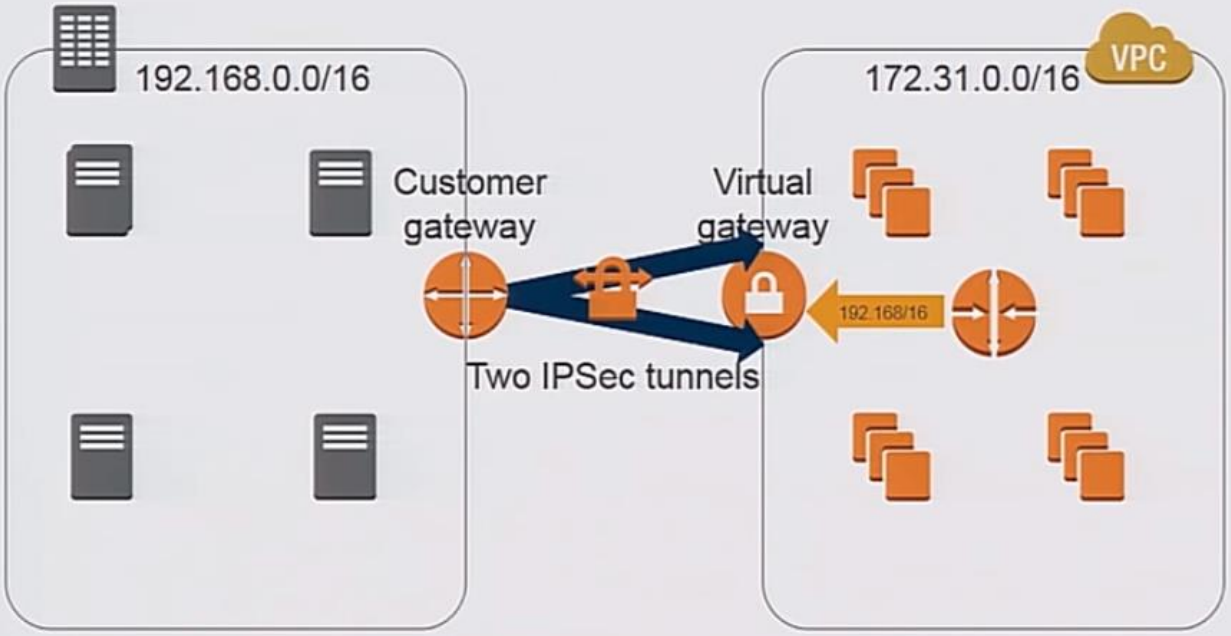


Route tables are another way to enforce VPC security.

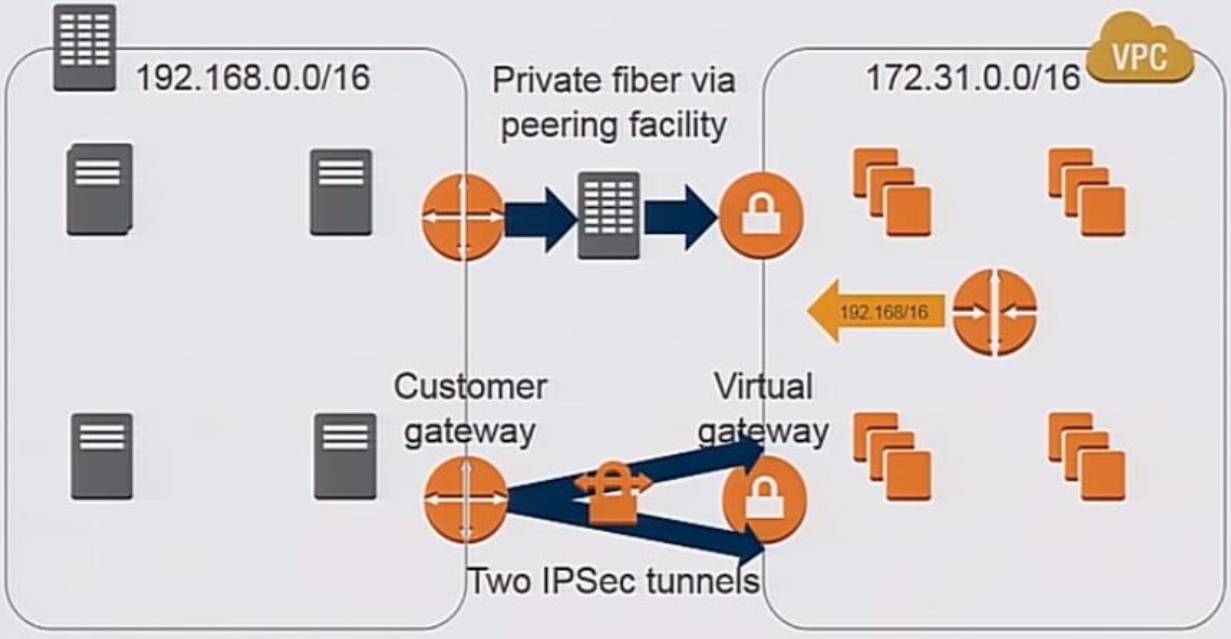


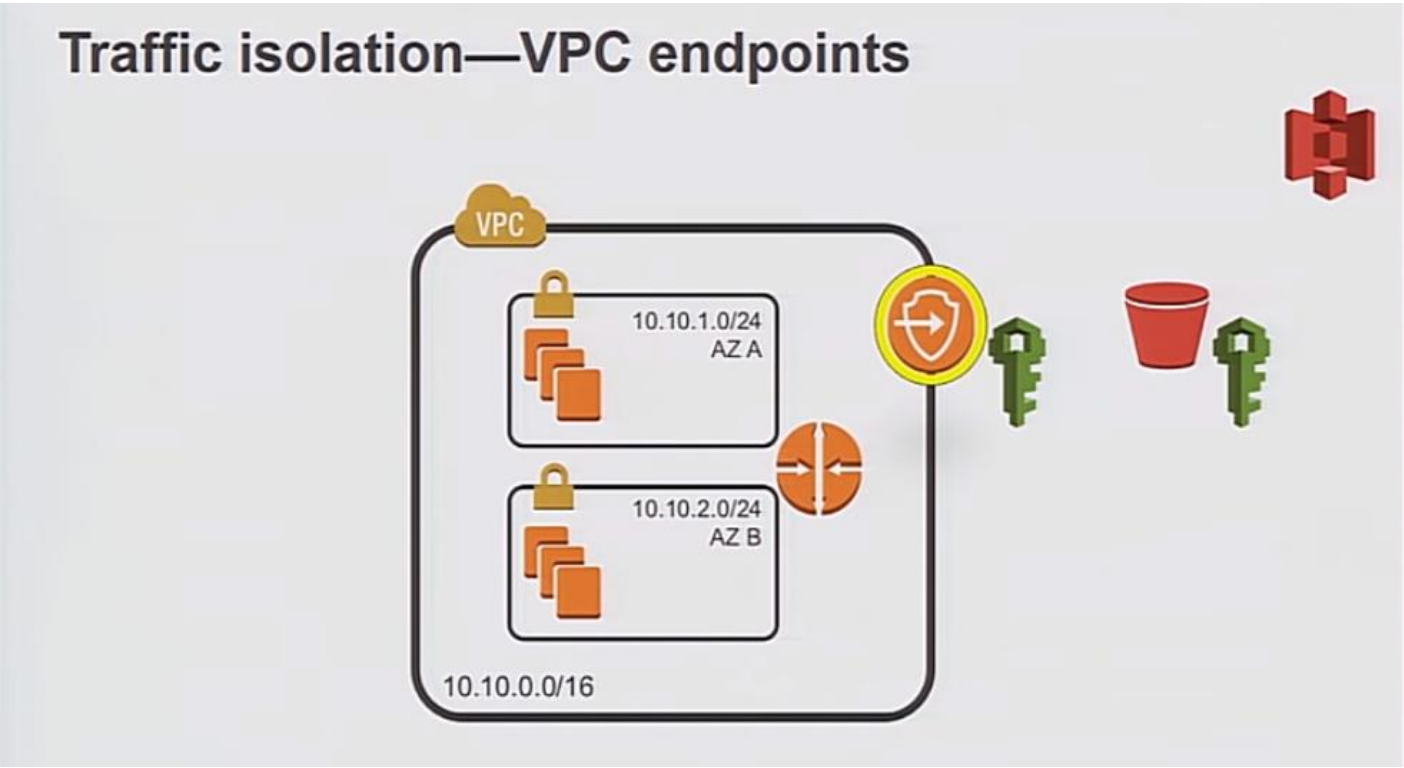
Your can define WAF rules that get enforced at the edge automatically without you having to manage anything

Traffic isolation—VPN and AWS Direct Connect

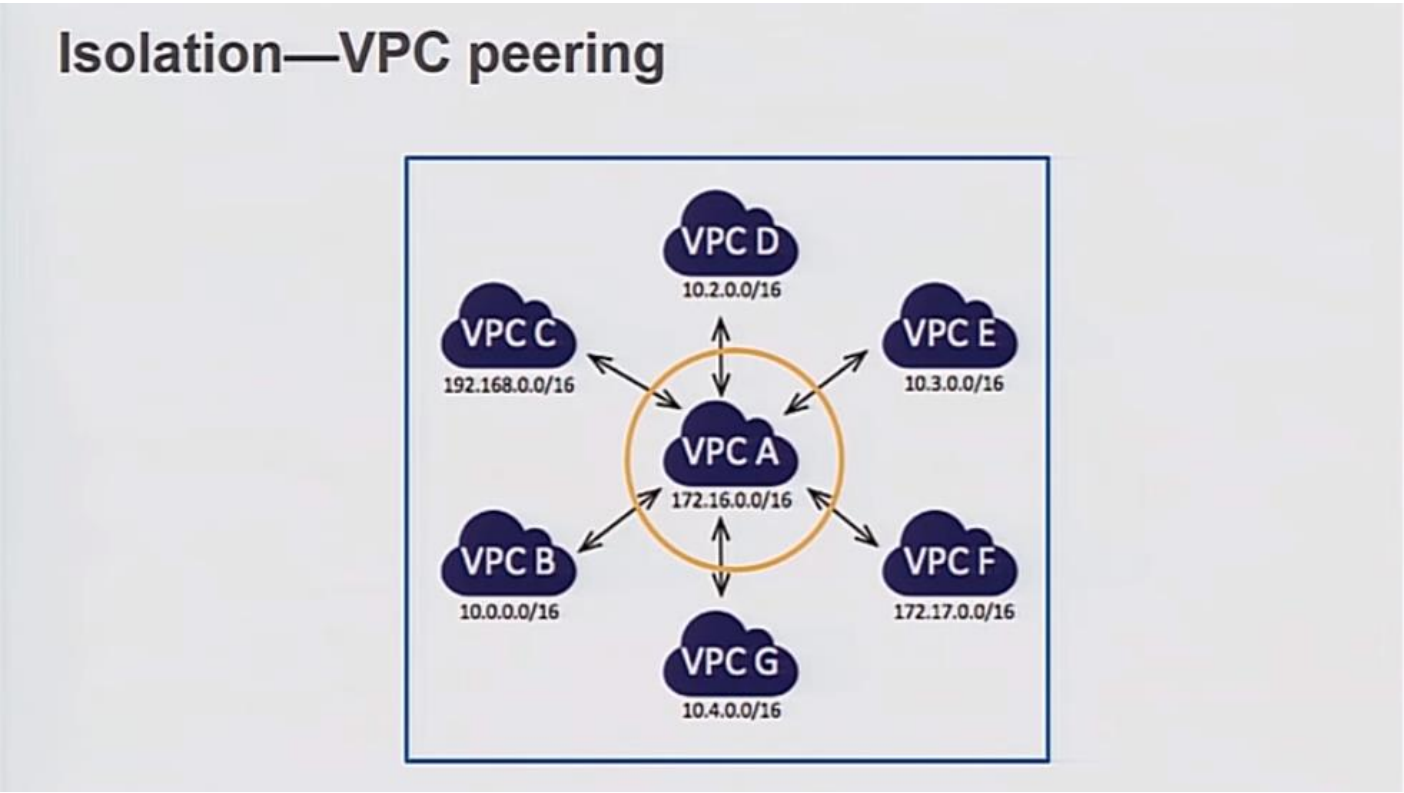


Traffic isolation—VPN and AWS Direct Connect





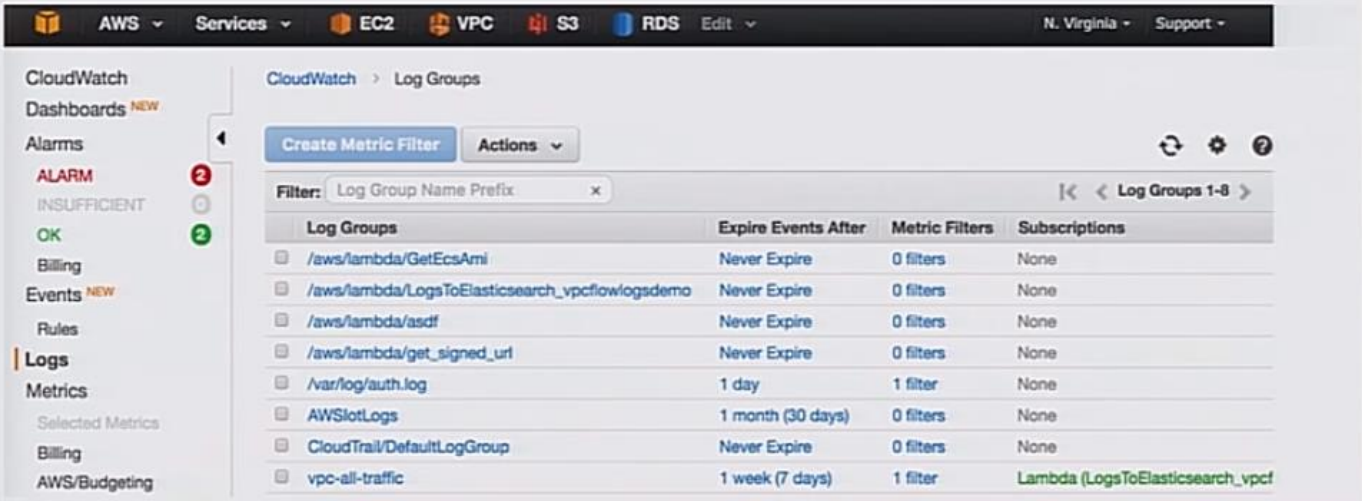
This provides a routing target that makes S3 look like it is attached to the VPC, it supports IAM policy for controlling what buckets to talk to.



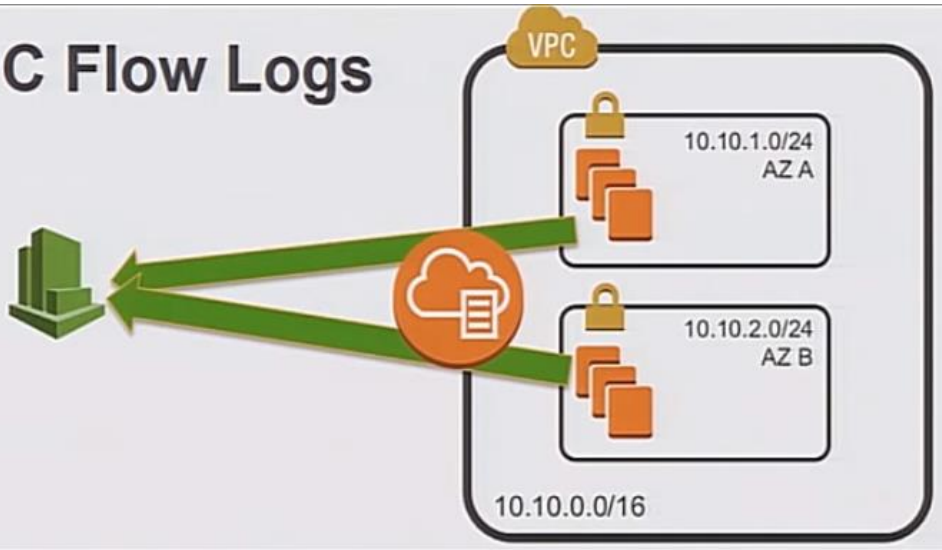
The shared services like logging, config data and others can be put into the central VPC that other VPCs can talk to and get needs met.

Logging

Amazon CloudWatch Logs



Logging: VPC Flow Logs




```
eni-2fc40d00 122.9.35.119 172.16.0.244 6000 5901 6 1 40 1464280539 1464280598 REJECT OK
eni-2fc40d00 172.16.0.244 64.125.239.242 22 46905 6 6 264 1464280618 1464280718 ACCEPT OK
eni-2fc40d00 209.126.127.134 172.16.0.244 5425 5060 17 1 443 1464280618 1464280658 REJECT OK
eni-2fc40d00 64.125.239.242 172.16.0.244 46905 22 6 1 40 1464280618 1464280658 ACCEPT OK
eni-2fc40d00 122.9.35.119 172.16.0.244 6000 2222 6 1 40 1464280618 1464280658 REJECT OK
eni-2fc40d00 172.16.0.244 172.16.1.229 123 123 17 2 152 1464280749 1464280838 ACCEPT OK
eni-2fc40d00 132.163.4.101 172.16.0.244 123 123 17 1 76 1464280749 1464280778 ACCEPT OK
eni-2fc40d00 172.16.1.229 172.16.0.244 123 123 17 2 152 1464280749 1464280838 ACCEPT OK
```

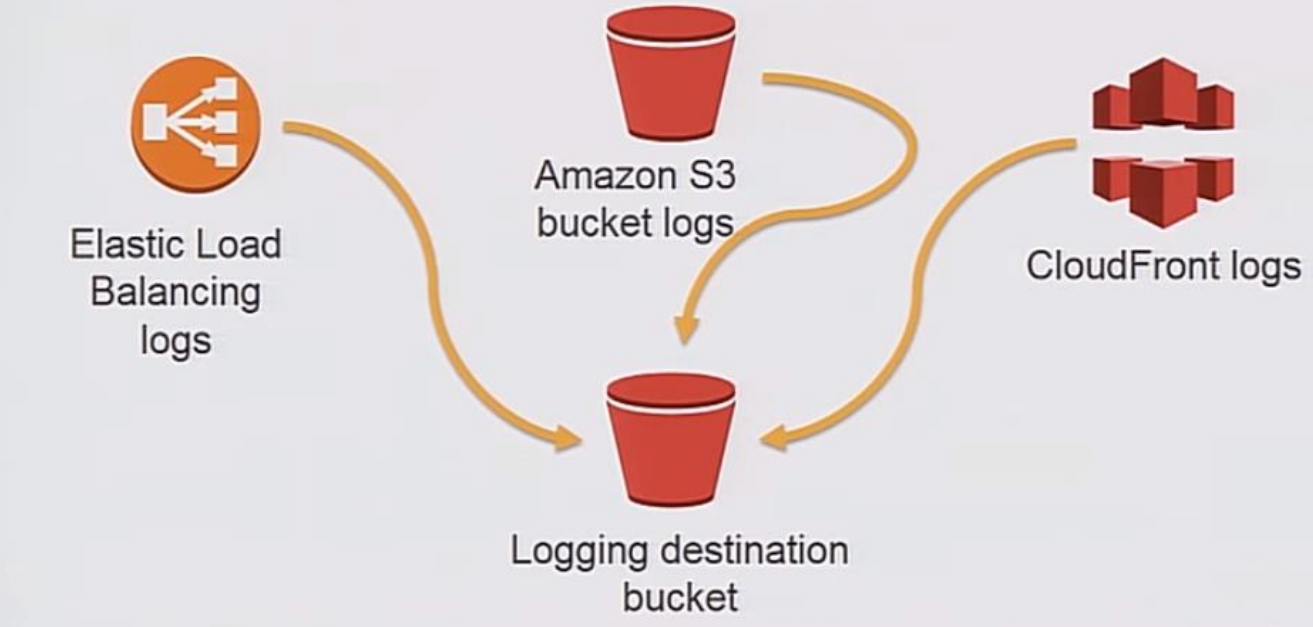
This is a way to get network logging information from all your environments, it also goes to your CloudWatch logs

Logging—AWS CloudTrail

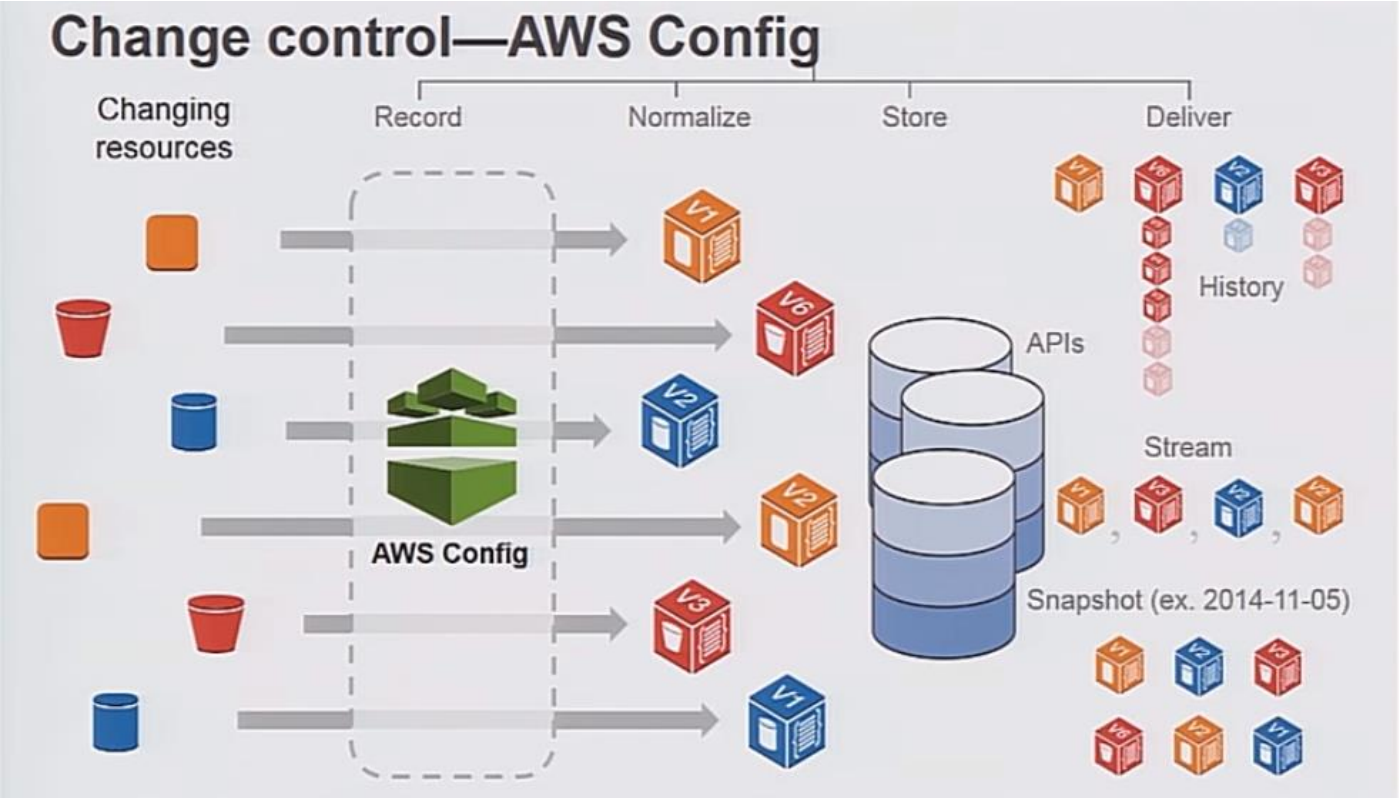
```
"Records": [{
        "eventVersion": "1.0",
        "userIdentity": {
...
            "arn": "arn:aws:iam::123456789012:user/Alice",
...
        },
        "eventTime": "2015-03-24T21:11:59Z",
        "eventSource": "iam.amazonaws.com",
        "eventName": "CreateUser",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "55.55.55.55",
...
```

AWS CloudTrail is a way to do auditing of your environment in AWS, you can use tools to monitor the CloudTrail logs

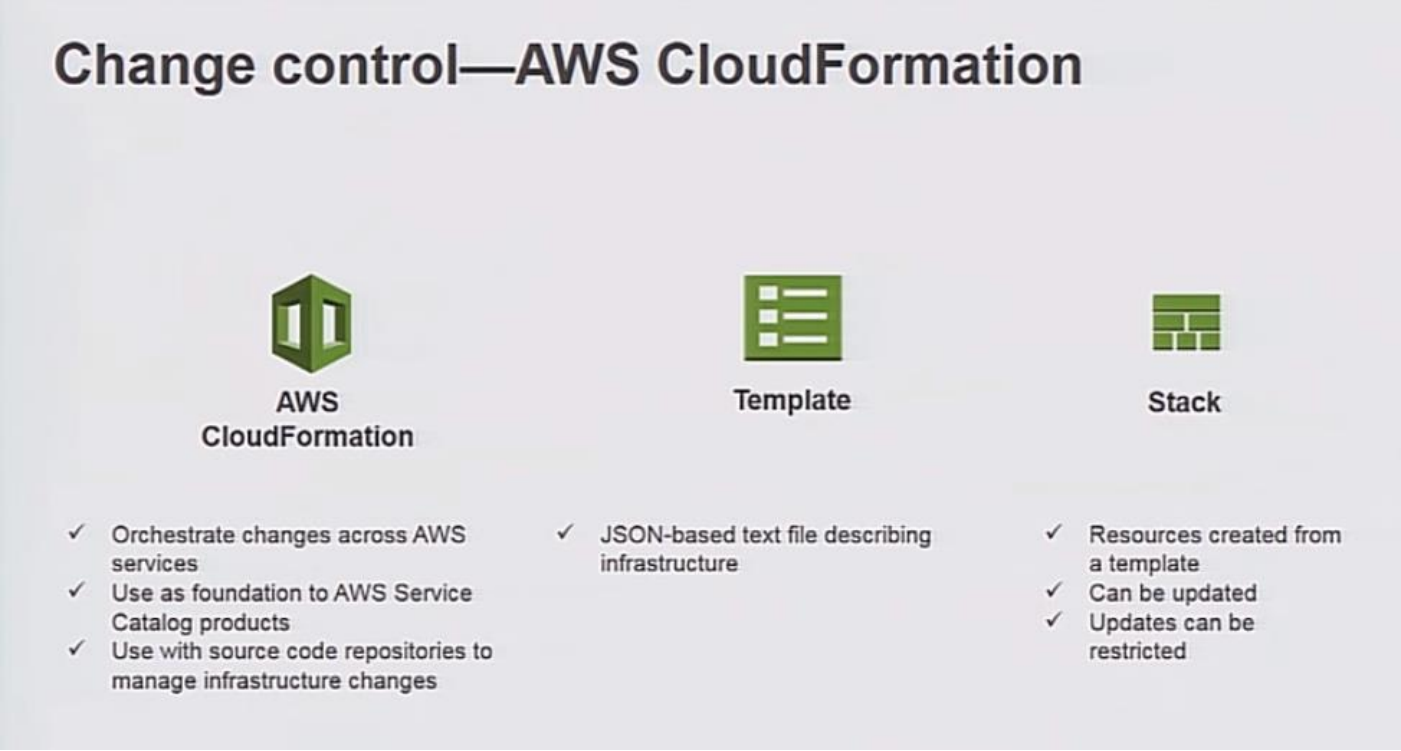
Logging—Elastic Load Balancing, CloudFront, Amazon S3 access logs



Change control

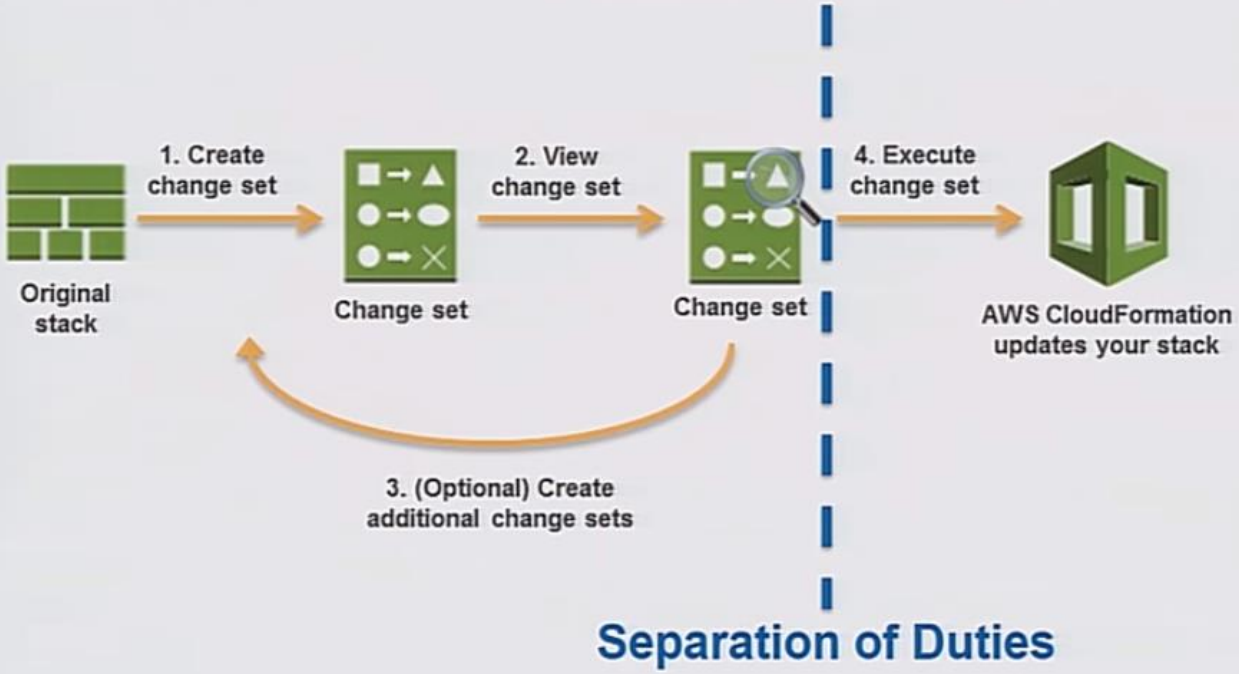


As resources change, AWS Config helps to monitor the configuration of those resources and stores the changes as logs



CloudFormation lets you write templates that deploy AWS resources. We can treat the templates as code and check them into a repo location

Change control—CloudFormation change sets

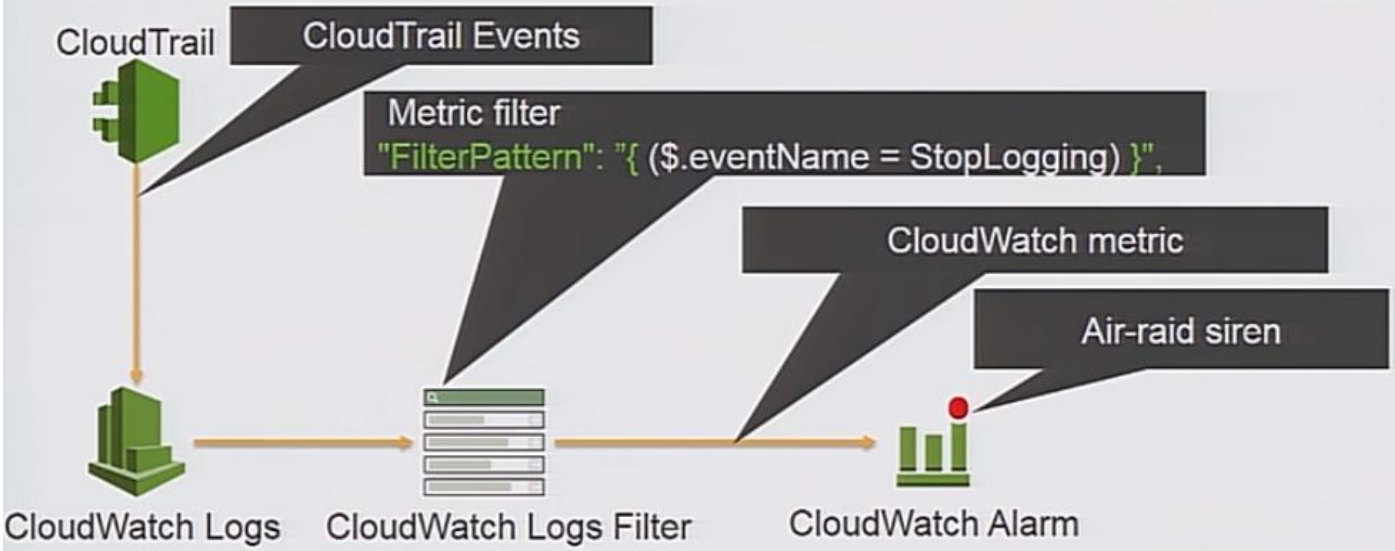


Making use of logs

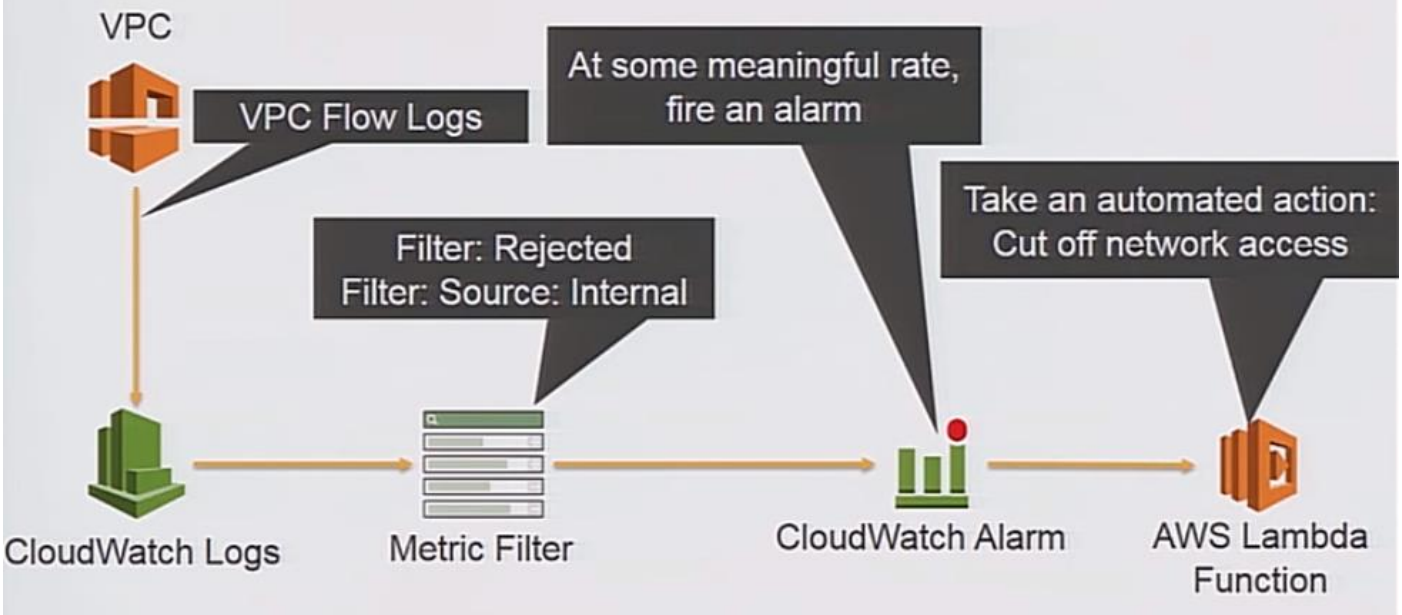
Example events of concern

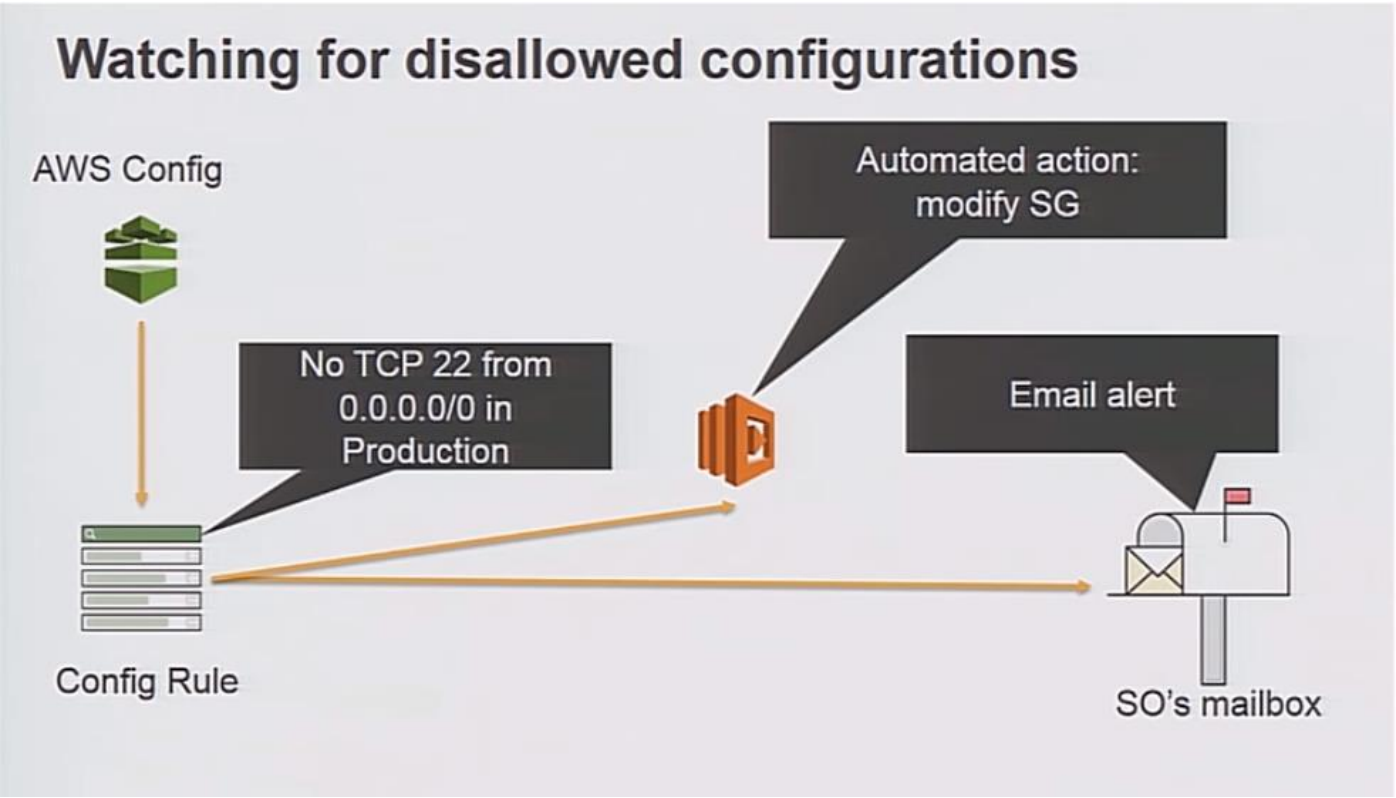
- Configuration changes that impact ability to detect or understand events
- Activities that are inconsistent with expectations
- Activities that violate policy

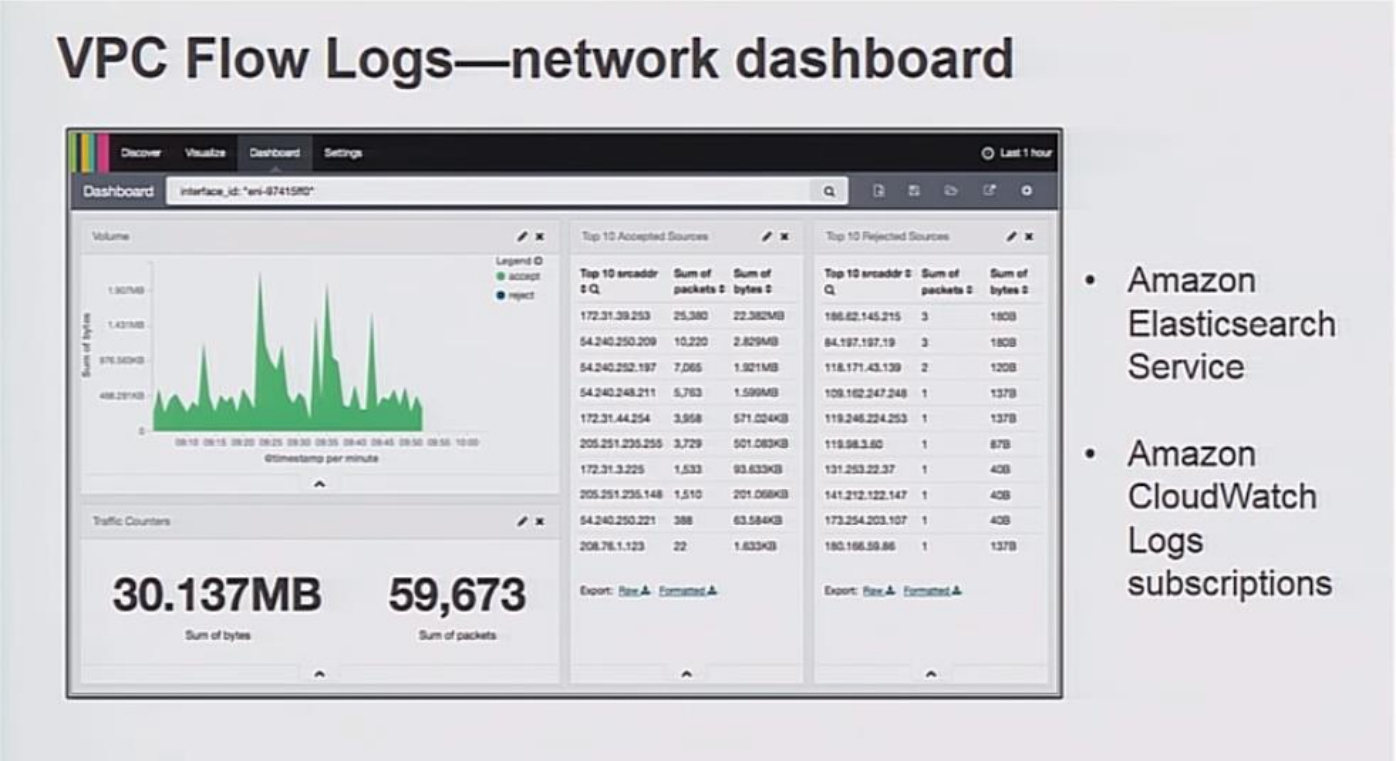
Monitoring logging status—CloudTrail



Monitoring for unexpected (network) behavior







You can push all your logs into ES and put Kibana in front of it to see your network traffic dashboard

All of this can be automated

So what does that do for practices in the cloud?

Automation, enabled by public cloud, leads to continuous practice

continuous delivery is the foundation

continuous security

prevention & response

continuous delivery
continuous security testing
continuous hacking
continuous risk management
continuous assurance
continuous compliance

continuous security testing

continuous hacking

continuous risk management

continuous compliance

the public cloud provides a platform

continuous security

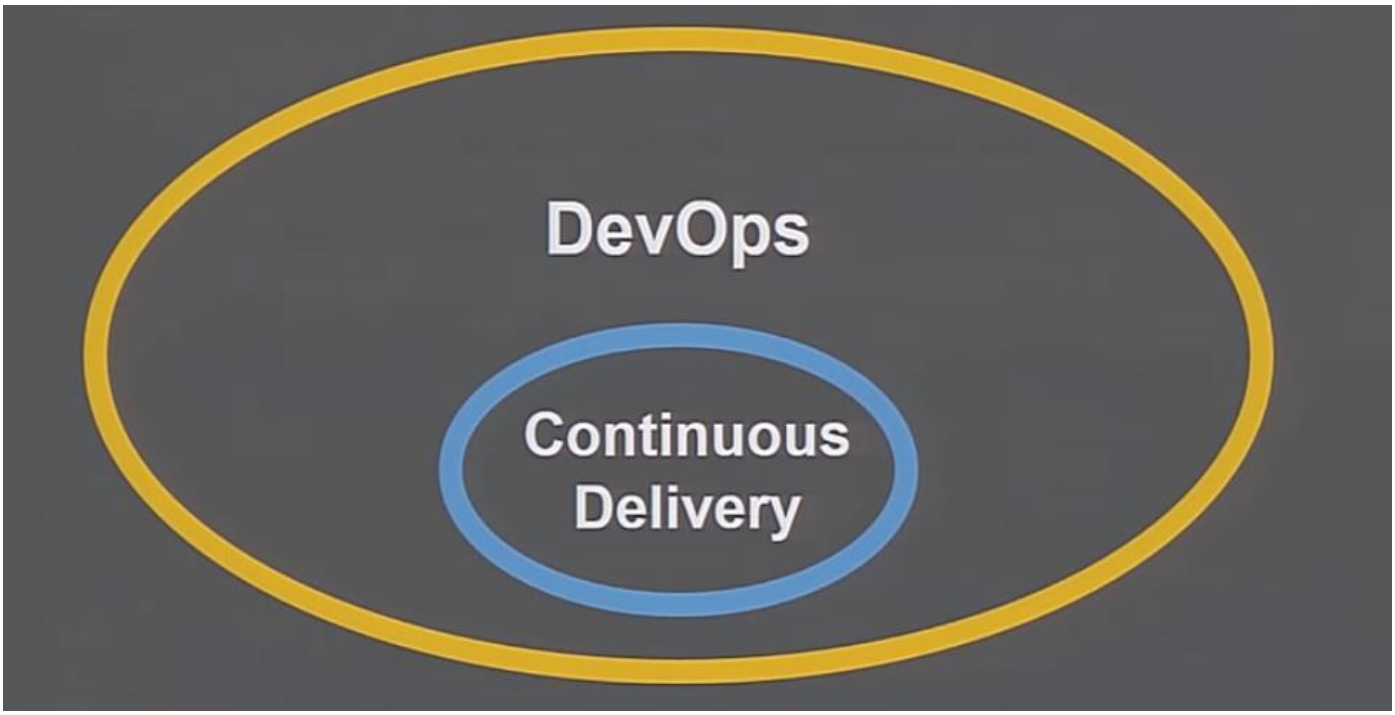
detection

continuous intrusion detection
continuous health checking
continuous anomaly detection
continuous capacity management
continuous scaling

continuous prevention & response

continuous detection

continuous delivery is hard



DevOps is **hard**

because change toward
DevOps is culture change

DevOps is culture change

New skills
New methodologies
New hours & working locations
New careers
New ways of thinking
New planning
New governance
Sometimes, new clothes

Rising cyber security threats require us to be adaptive.

Security conservatism, attempting to achieve stability through restricted change, increases risk.

We must embrace continuous practice.