**AWS Shield**

* AWS Shield Standard:
  + Free service that is activated for every AWS customer
  + Provides protection from attacks such as SYN/UDP Floods, Reflection attacks and other layer 3/layer 4 attacks
* AWS Shield Advanced:
  + Optional DDoS mitigation service ($3,000 per month per organization)
  + Protect against more sophisticated attack on Amazon EC2, Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, and Route 53
  + 24/7 access to AWS DDoS response team (DRP)
  + Protect against higher fees during usage spikes due to DDoS

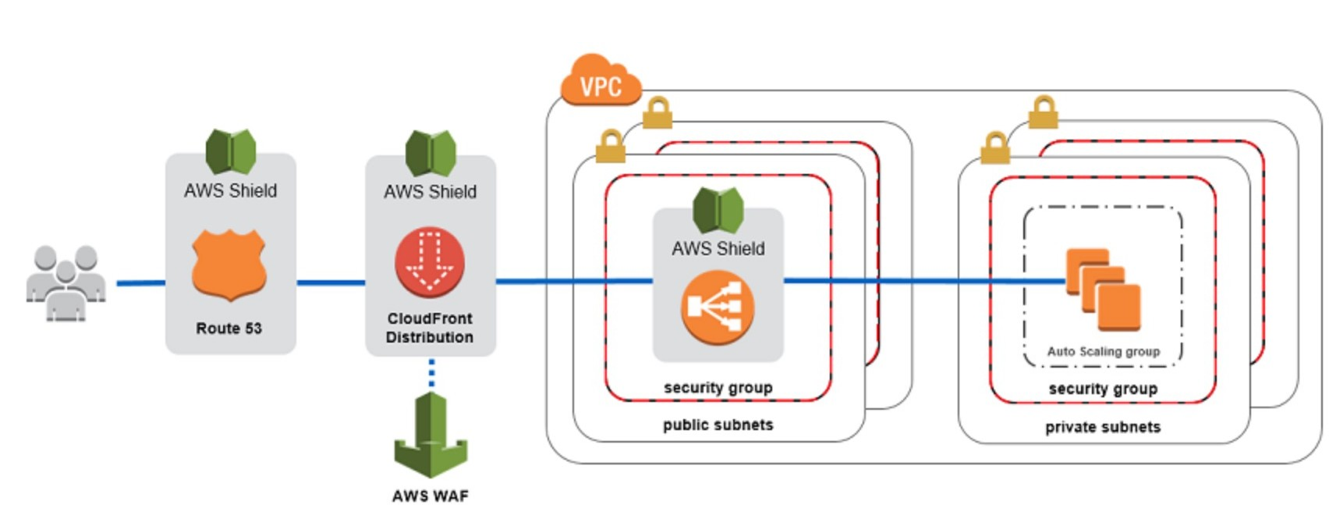
**AWS WAF – Web Application Firewall**

* Protects your web applications from common web exploits (Layer 7)
* Layer 7 is HTTP (vs Layer 4 is TCP)
* Deploy on Application Load Balancer, API Gateway, CloudFront
* Define Web ACL (Web Access Control List):
  + Rules can include: IP addresses, HTTP headers, HTTP body, or URI strings
  + Protects from common attack - SQL injection and Cross-Site Scripting (XSS)
  + Size constraints, geo-match (block countries)
  + Rate-based rules (to count occurrences of events) – for DDoS protection

**AWS Firewall Manager**

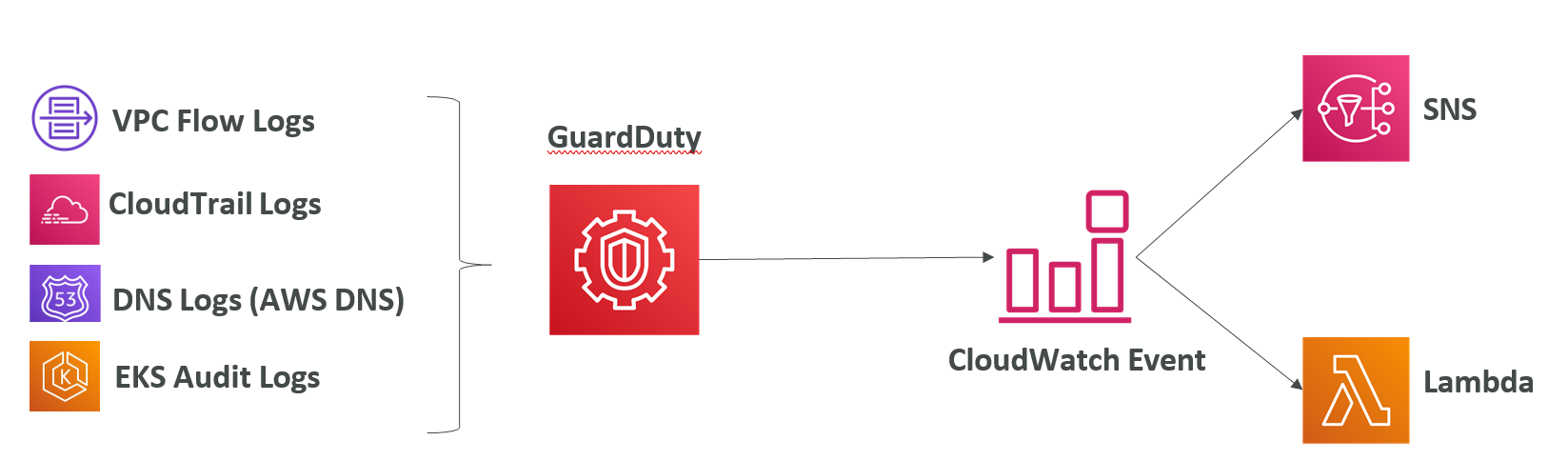
* Manage rules in all accounts of an AWS Organization
* Common set of security rules
* WAF rules (Application Load Balancer, API Gateways, CloudFront)
* AWS Shield Advanced (ALB, CLB, Elastic IP, CloudFront)
* Security Groups for EC2 and ENI resources in VPC

**Sample Reference Architecture for DDoS Protection**



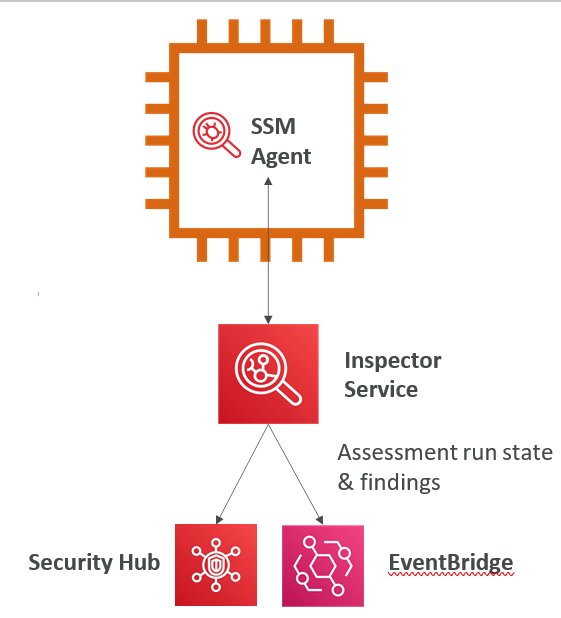
**Amazon GuardDuty**

* Intelligent Threat discovery to Protect AWS Account
* Uses Machine Learning algorithms, anomaly detection, 3rd party data
* One click to enable (30 days trial), no need to install software
* Input data includes:
  + CloudTrail Events Logs – unusual API calls, unauthorized deployments
    - CloudTrail Management Events – create VPC subnet, create trail, …
    - CloudTrail S3 Data Events – get object, list objects, delete object, …
  + VPC Flow Logs – unusual internal traffic, unusual IP address
  + DNS Logs – compromised EC2 instances sending encoded data within DNS queries
  + Kubernetes Audit Logs – suspicious activities and potential EKS cluster compromises
* Can setup CloudWatch Event rules to be notified in case of findings
* CloudWatch Events rules can target AWS Lambda or SNS
* Can protect against CryptoCurrency attacks (has a dedicated “finding” for it)



**Amazon Inspector**

* Automated Security Assessments
* For EC2 instances
  + Leveraging the AWS System Manager (SSM) agent
  + Analyze against unintended network accessibility
  + Analyze the running OS against known vulnerabilities
* For Containers push to Amazon ECR
  + Assessment of containers as they are pushed
* Reporting & integration with AWS Security Hub
* Send findings to Amazon Event Bridge



**Amazon Macie**

Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS.

Macie helps identify and alert you to sensitive data, such as personally identifiable information (PII)

