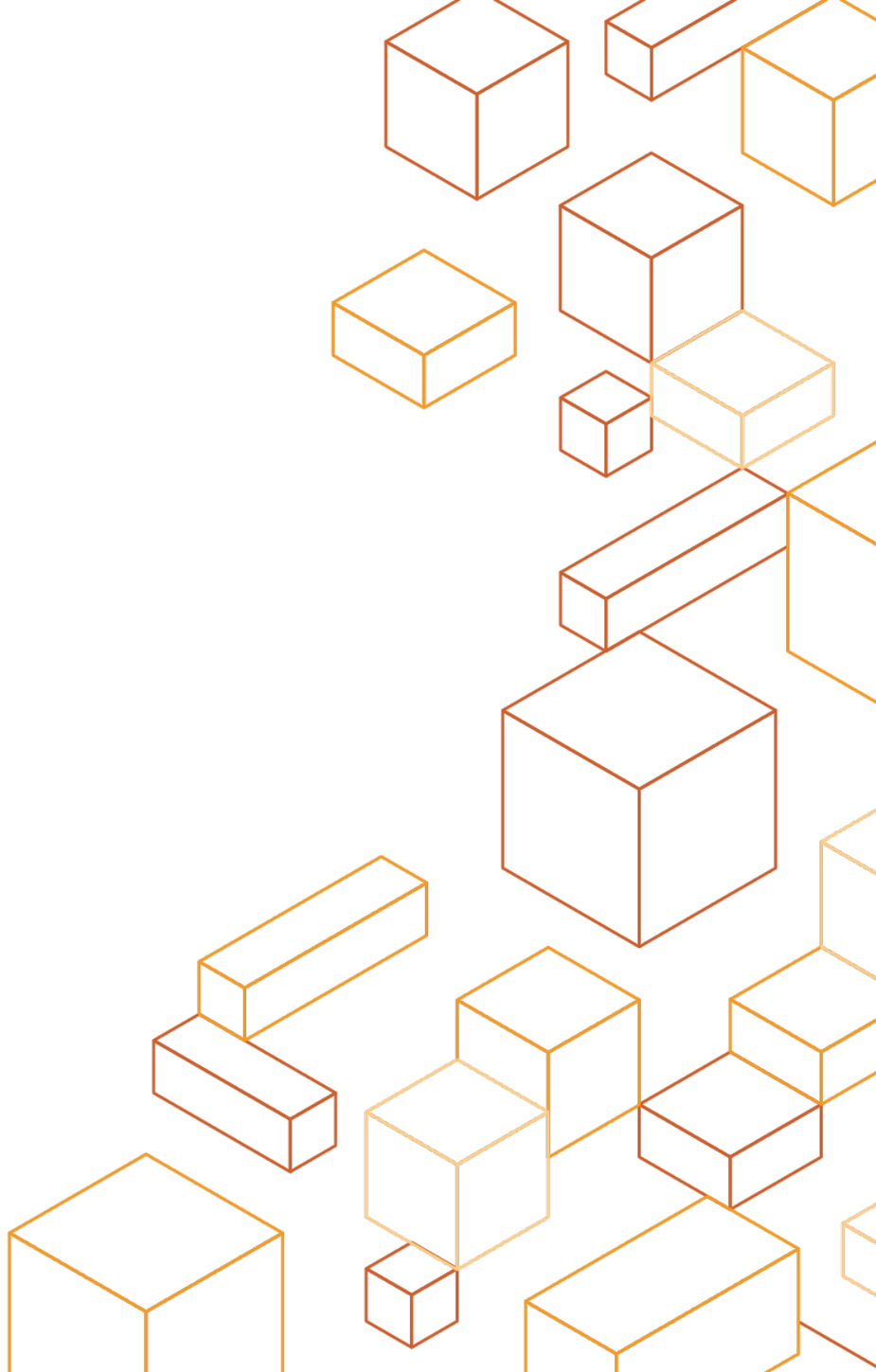
aws professional services

Infrastructure Security



Agenda

- Denial of Service
- AWS WAF
- AWS Firewall Manager
- AWS Network Firewall
- Features of VPC network security
- Systems Management in AWS

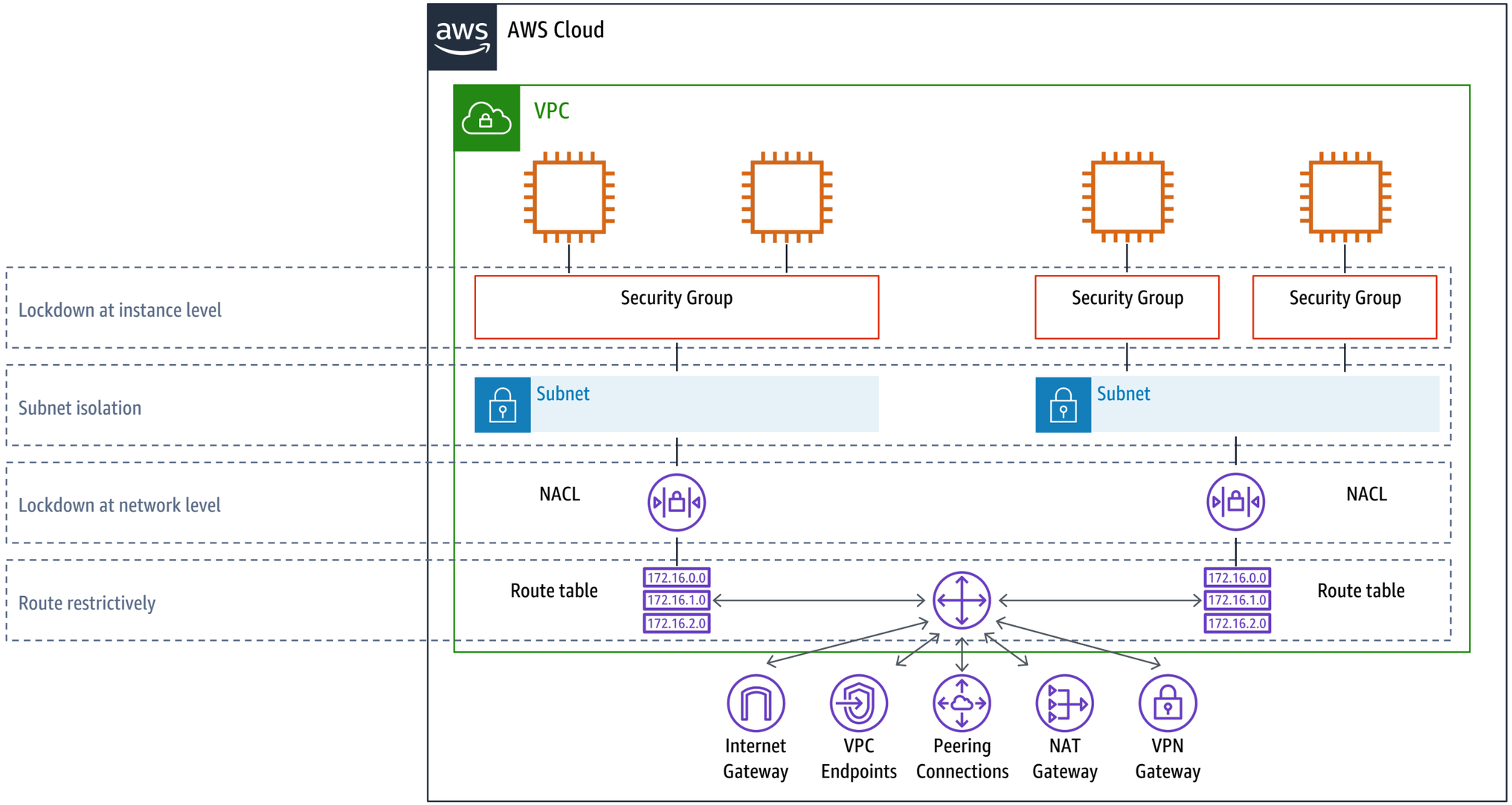
Goals

- Understand how AWS protects the network
- Consider the threat and risk profile of potential cloud workloads
- Choose network and workload security controls
- Gain awareness of the network security ecosystem
- Understand how to automate systems management in AWS

Outcomes

- One or more directive controls that apply to Security Groups and NACL's
- Decision on AWS Shield Advanced
- Decision on using AWS Network Firewall Manager to manage security rules
- Decision on whether to enable VPC Flow Logs and where to store them
- Decision on whether to use AWS WAF/3rd party WAF
- Decision on how to implement systems management/patch management

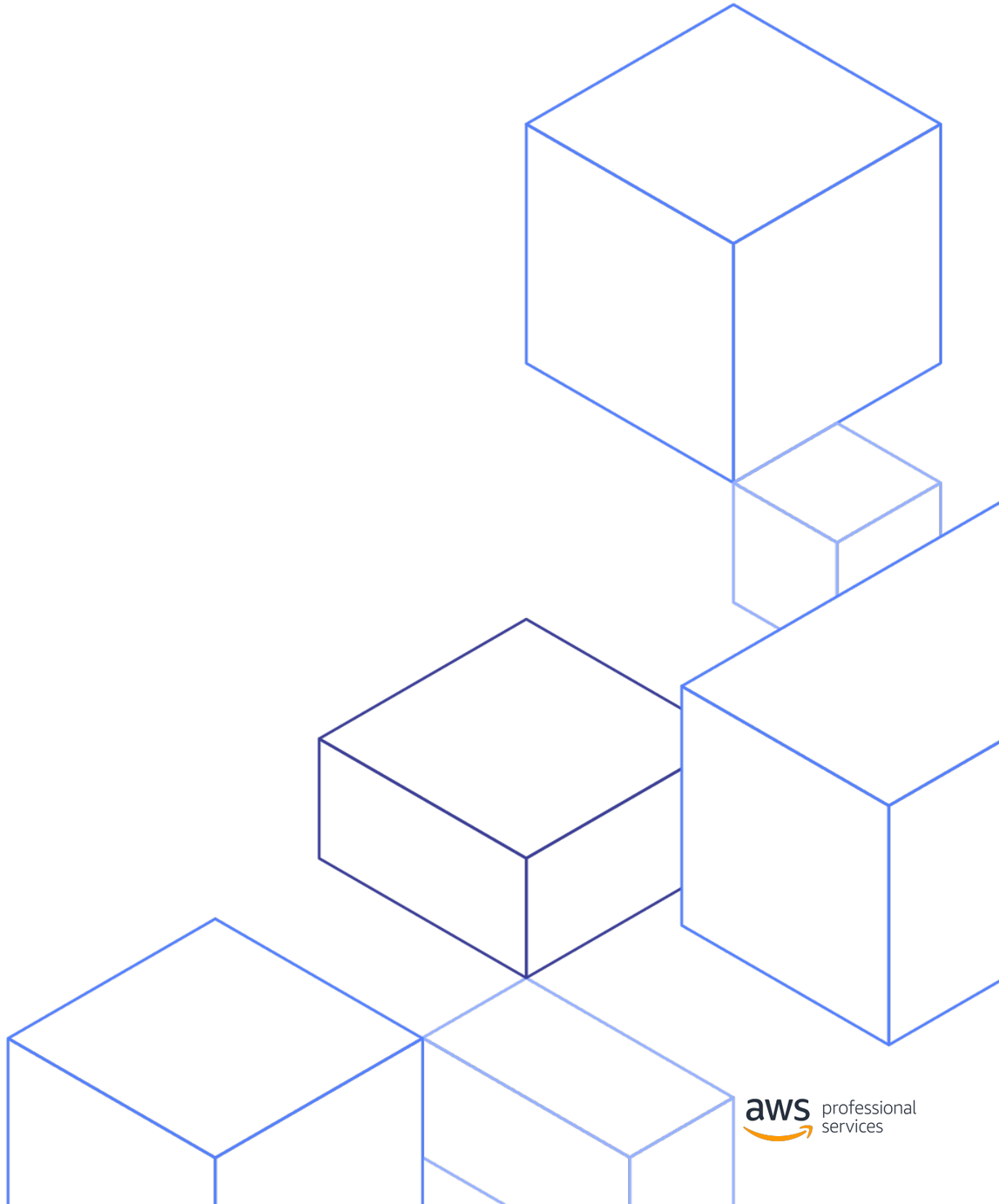
VPC Defense in Depth (review)



aws professional services

Denial of Service

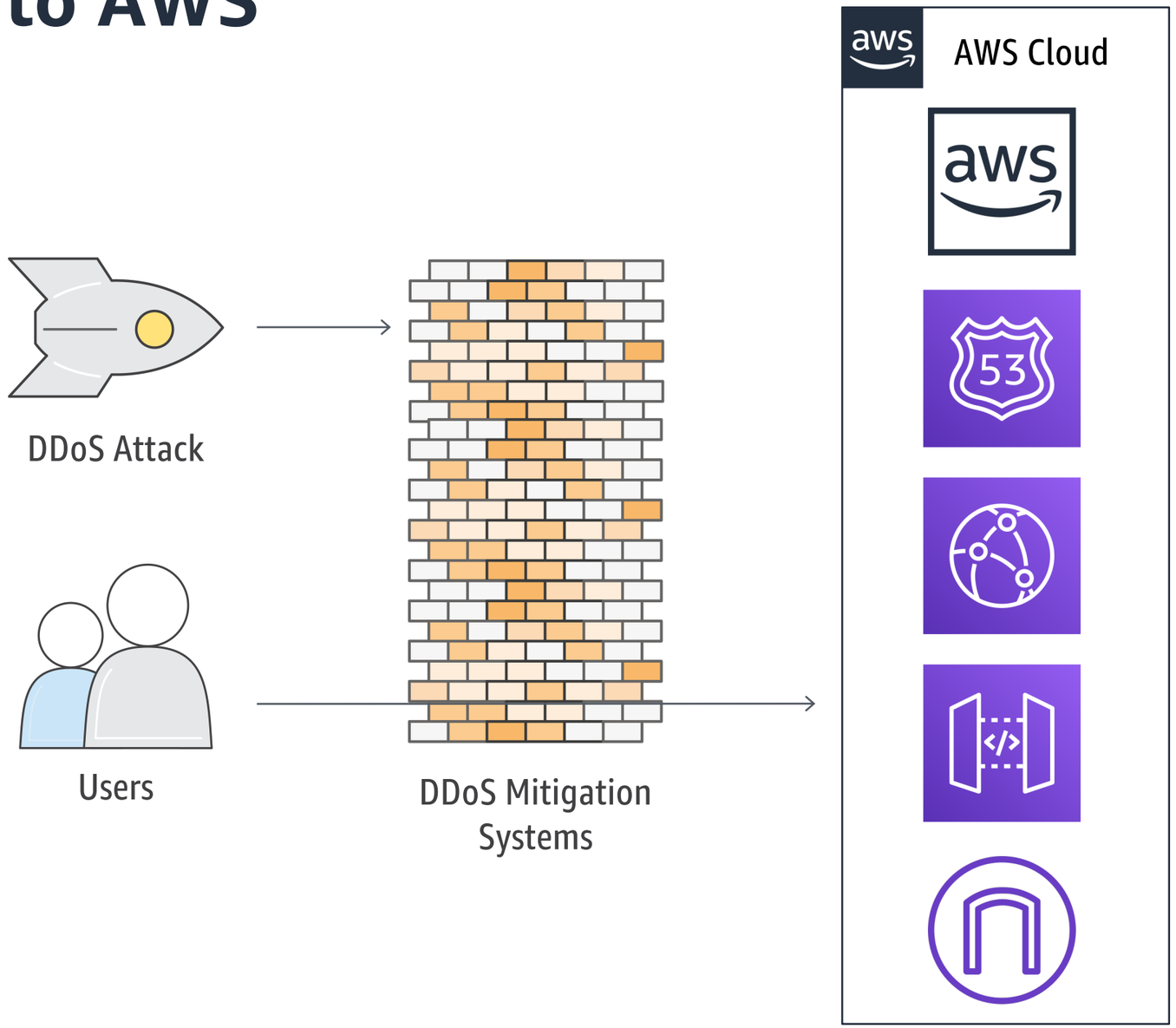
Infrastructure Security



aws professional services

DDoS protections built into AWS

- ✓ Protection against most common infrastructure attacks
- ✓ SYN/ACK Floods, UDP Floods, Reflection attacks, etc.
- ✓ No additional cost



AWS Shield

Standard Protection

Available to all AWS Customers at **no additional cost**

Advanced Protection

Paid service that provides additional protection, features, and benefits.

AWS Shield Standard

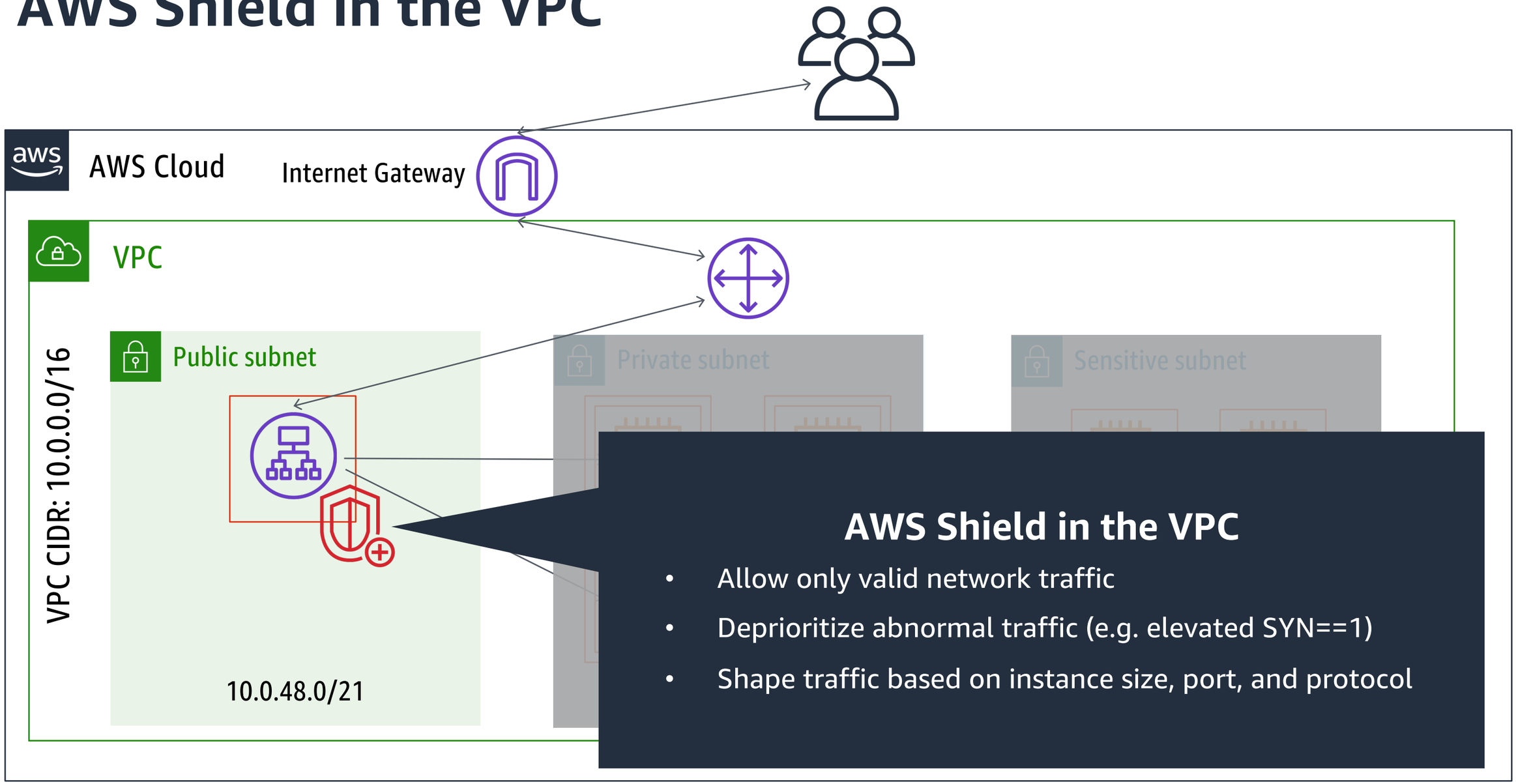
Layer 3/4 protection

- Automatic detection & mitigation
- Protection from most common DDoS attacks (SYN/UDP Floods, Reflection Attacks, etc.)
- Built into AWS API’s and Services

Layer 7 protection

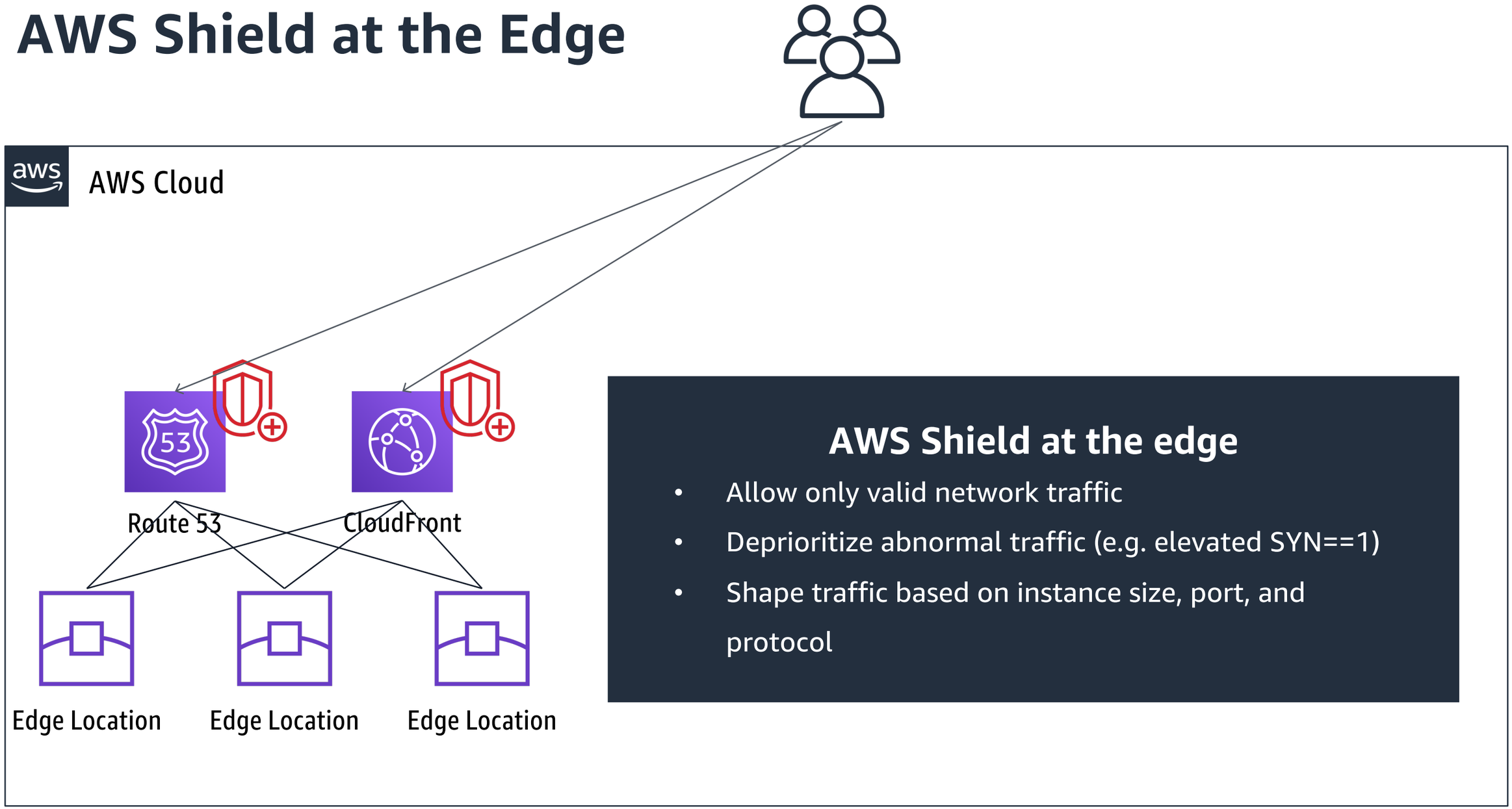
- Not included; use AWS WAF for layer 7 DDoS attack mitigation
- Self-service & pay-per-use

AWS Shield in the VPC



aws professional services

AWS Shield at the Edge



AWS Shield at the edge

- Allow only valid network traffic
- Deprioritize abnormal traffic (e.g. elevated SYN==1)
- Shape traffic based on instance size, port, and protocol

AWS Web Application Firewall (WAF)

Infrastructure Security

aws professional services

AWS Web Application Firewall (WAF)

Popular deployment modes

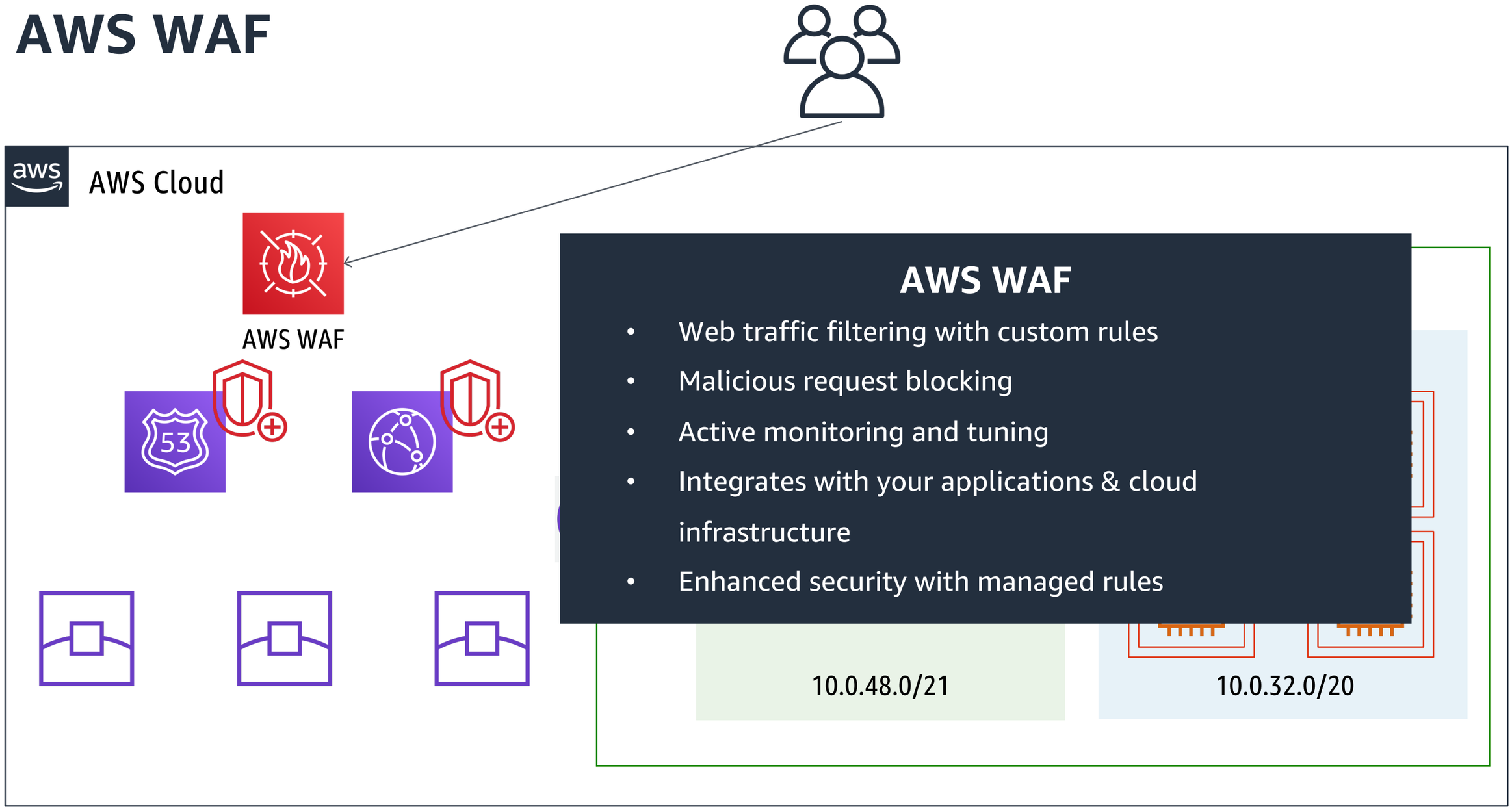
1. Custom Rules

2. Managed Rules

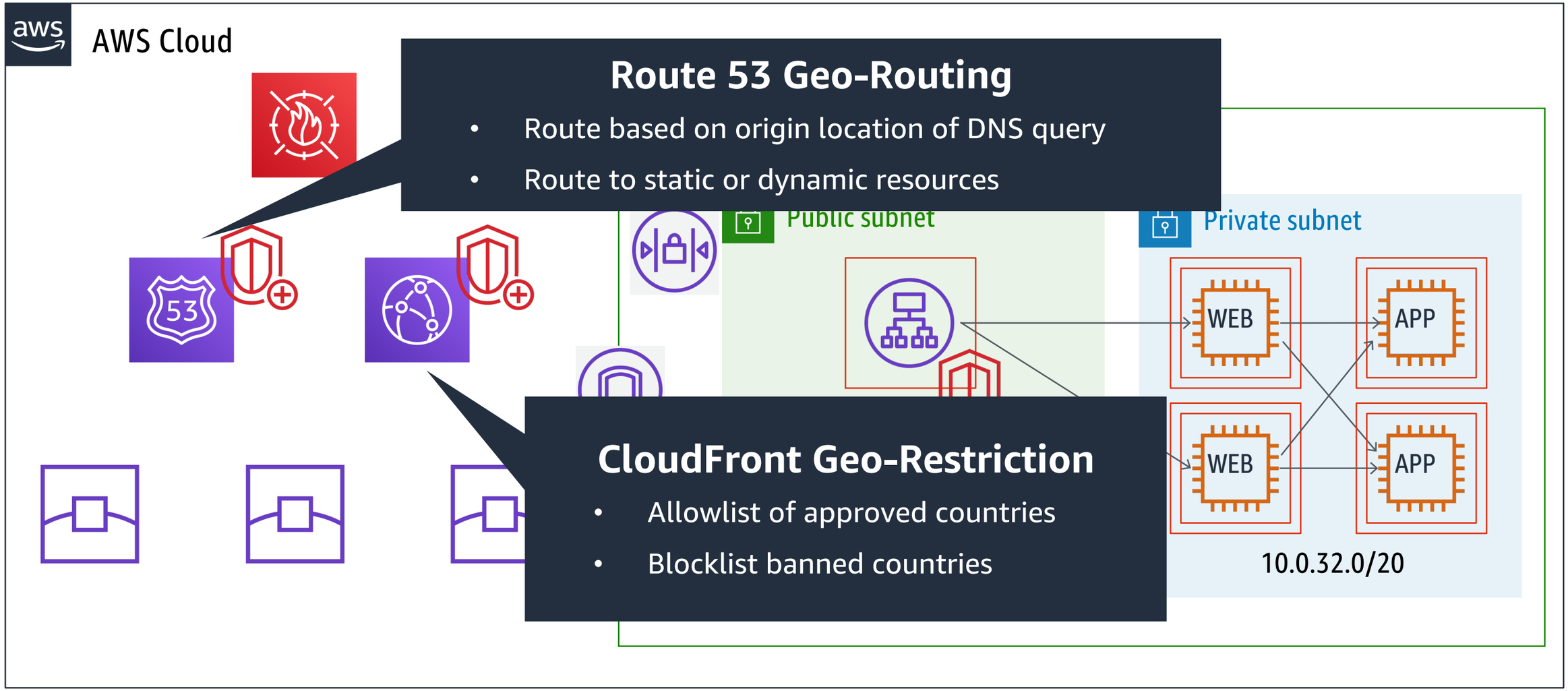
3. Security Automation

Or use any combination of the above …

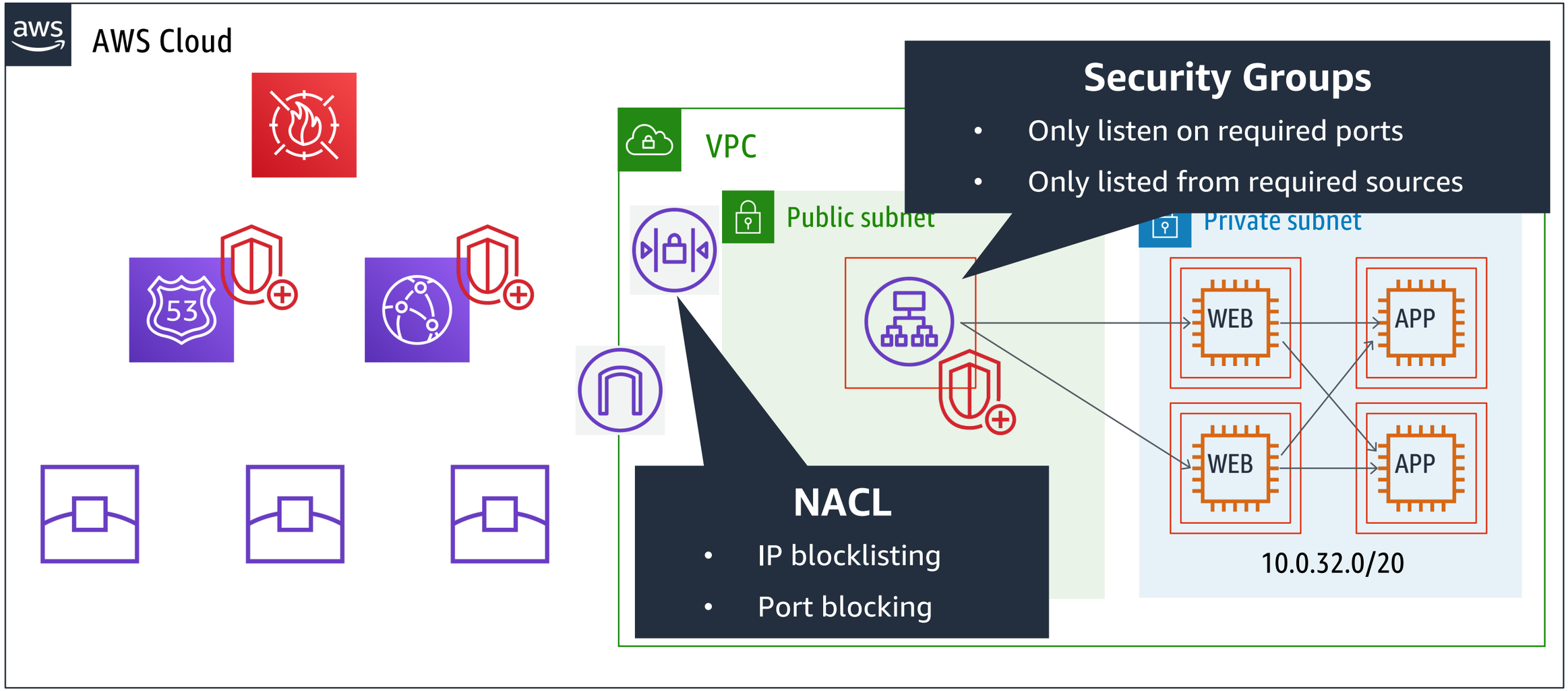
AWS WAF



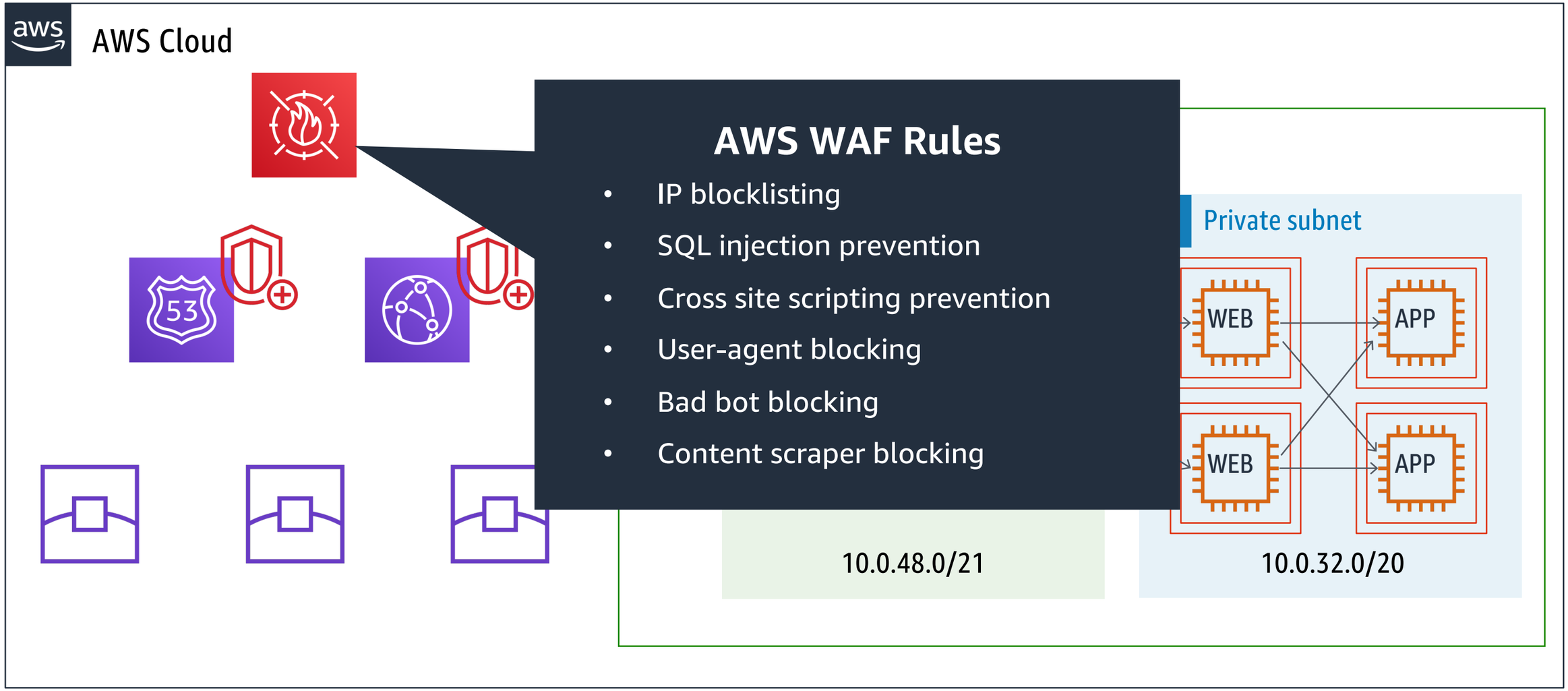
Stopping bad actors



Stopping bad actors

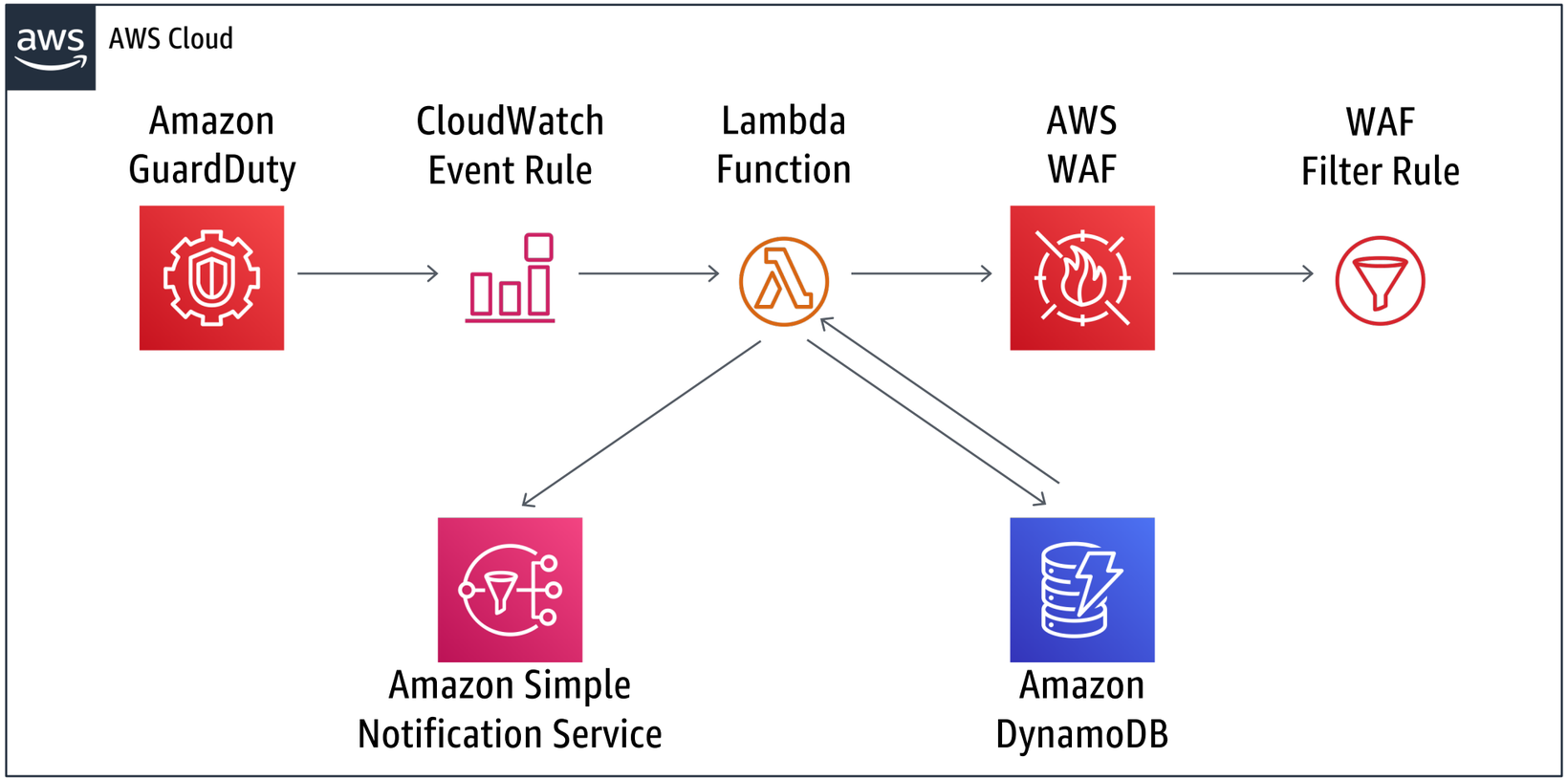


Stopping bad actors



AWS Web Application Firewall (WAF)

Automatic block of suspicious hosts using **Amazon GuardDuty** and **AWS WAF.**



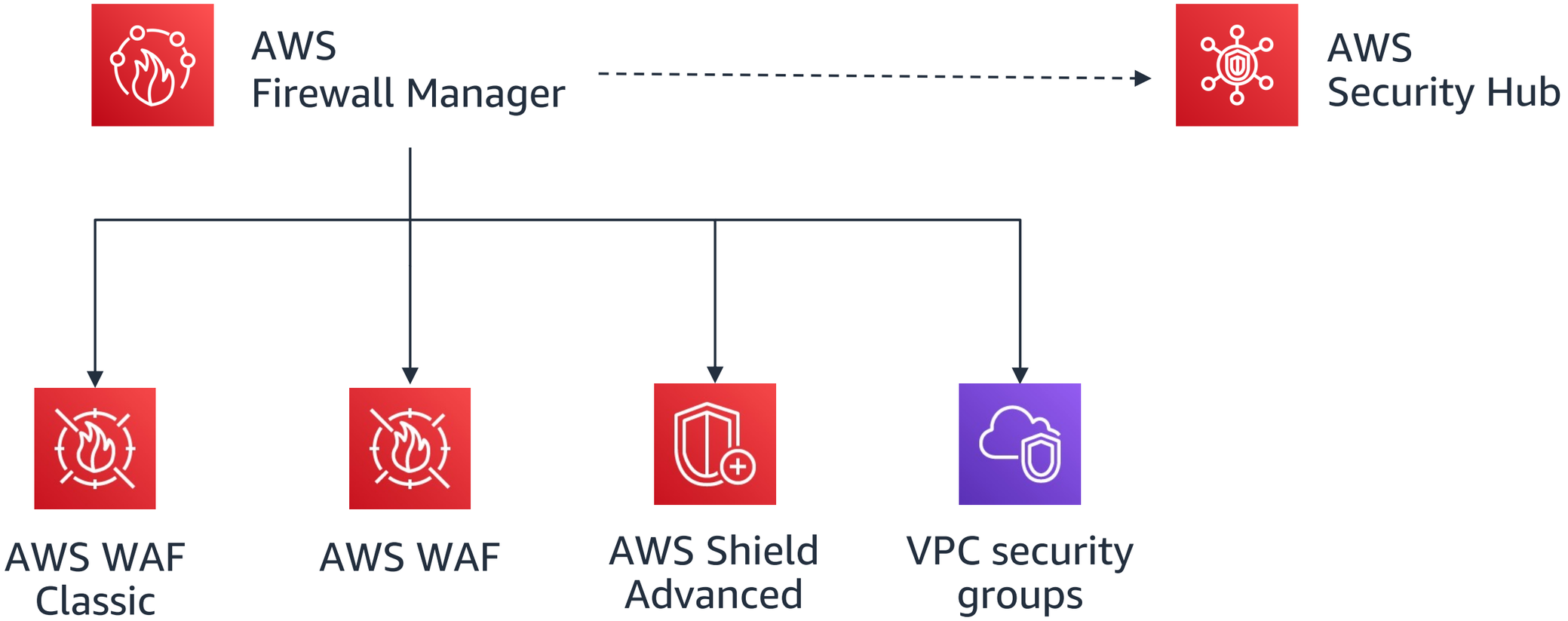
AWS Firewall Manager

Infrastructure Security

aws professional services

AWS Firewall Manager - Overview

AWS Firewall Manager is a security management service to centrally configure and manage your firewall policies across your accounts and applications in your organization



aws professional services

AWS Firewall Manager - Typical Use Case

Monitoring for overly-permissive VPC security groups

- Centrally monitor VPC security groups
- Define managed policies to remediate overly-permissive rules
- Continuous audit and remediation of existing and new security group rules
- Cross-account and cross-VPC

AWS Firewall Manager

VPC security groups

AWS Firewall Manager - Typical Use Case

Deploy OWASP rules for PCI compliance

- PCI DSS 3.0 Requirement 6 suggests customers deploy a WAF, with rules like OWASP top 10
- Use the AWS managed WAF rules
- Subscribe to Managed Rules from AWS Marketplace
- Ensure the OWASP rule is applied across all PCI-tagged resources

AWS Firewall Manager

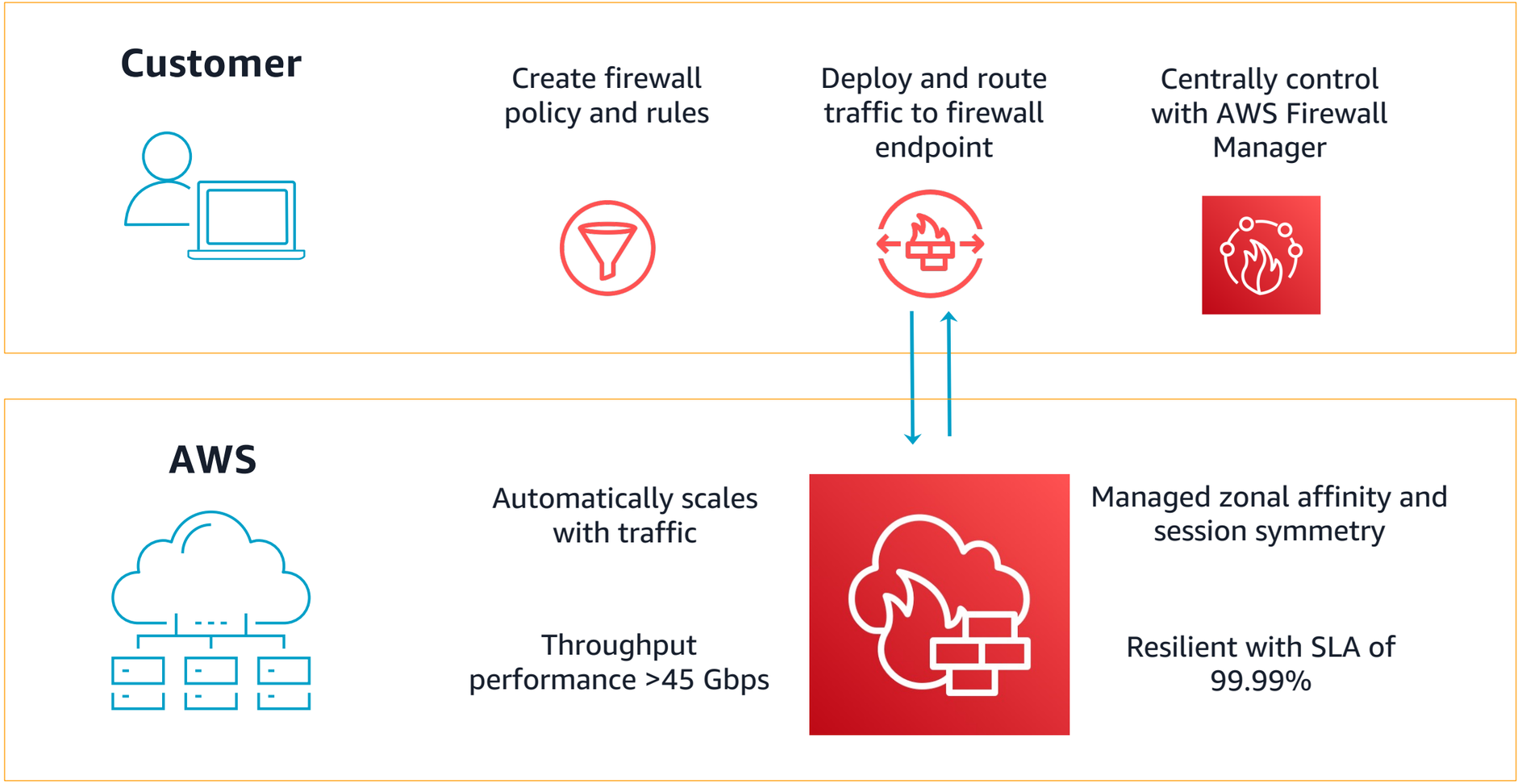
AWS WAF

AWS Network Firewall

Infrastructure Security

aws professional services

AWS Network Firewall overview



aws professional services

AWS Network Firewall Features

Packet Filtering

Large IP block/allow lists

Stateless & Stateful rules: IP/Port/Protocol

FQDN filtering on HTTP/HTTPS

Protocol detection, enforcement

Application rules: IPS/IDS (common open source rule format)

Visibility & Reporting

CloudWatch rule metrics

Full network flow logs

Event, rule-based logs

Log collection to S3, CloudWatch Logs, or Kinesis Firehose

Central Management

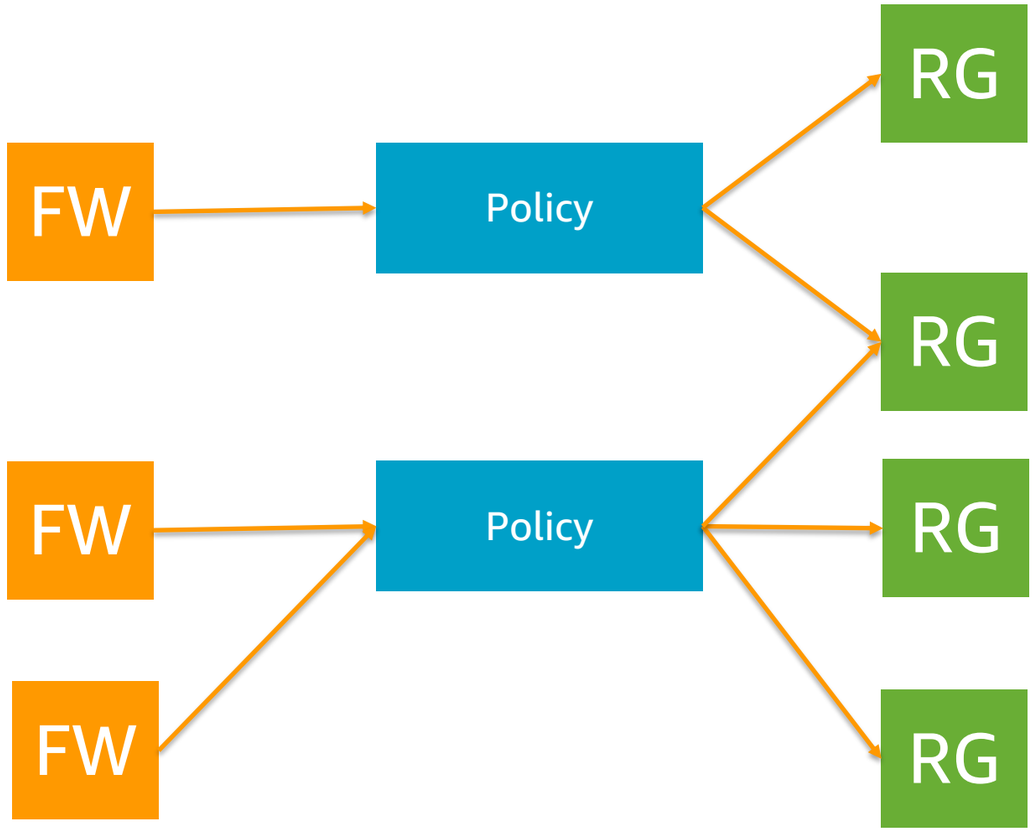
Cross-account management and rule visibility using AWS Firewall Manager

CloudFormation and Terraform templates

AWS Resource Access Manager

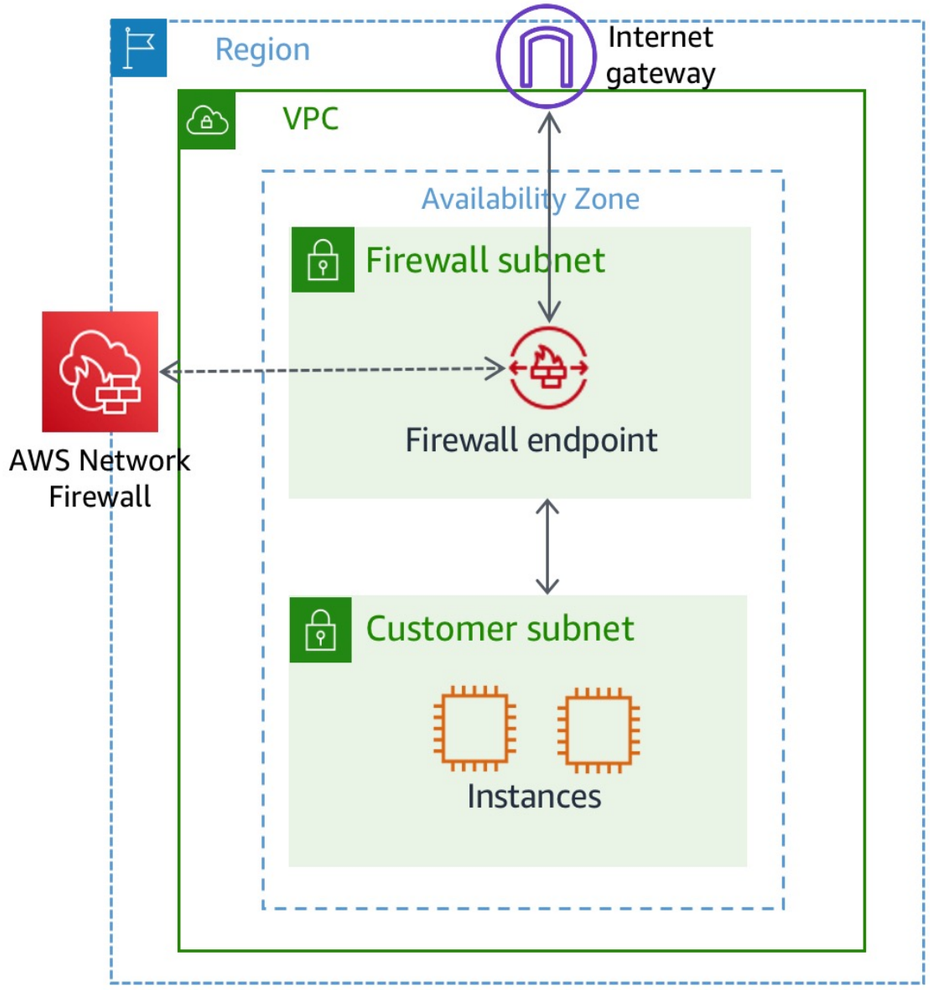
AWS Network Firewall resources

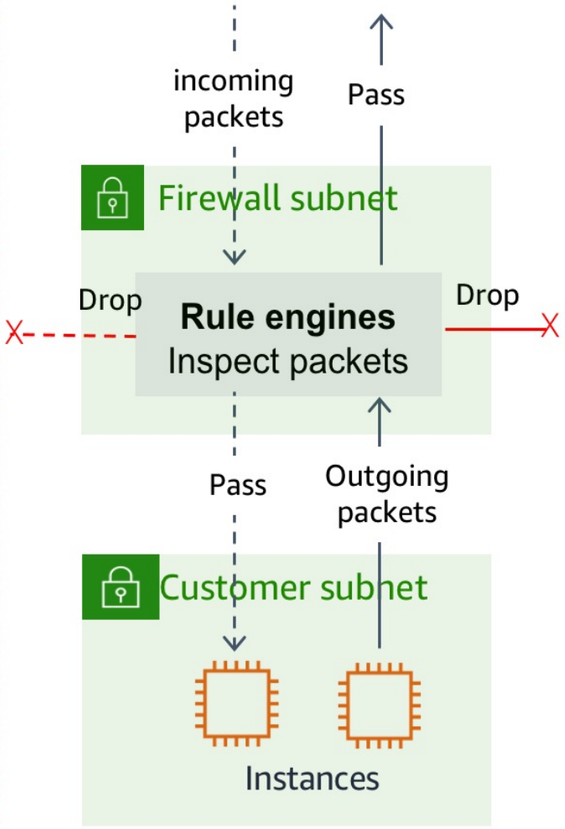
- Firewall
- Firewall policy
- Network Firewall rule groups
    - Stateless rulegroup - priority
    - Stateful rulegroup – by action

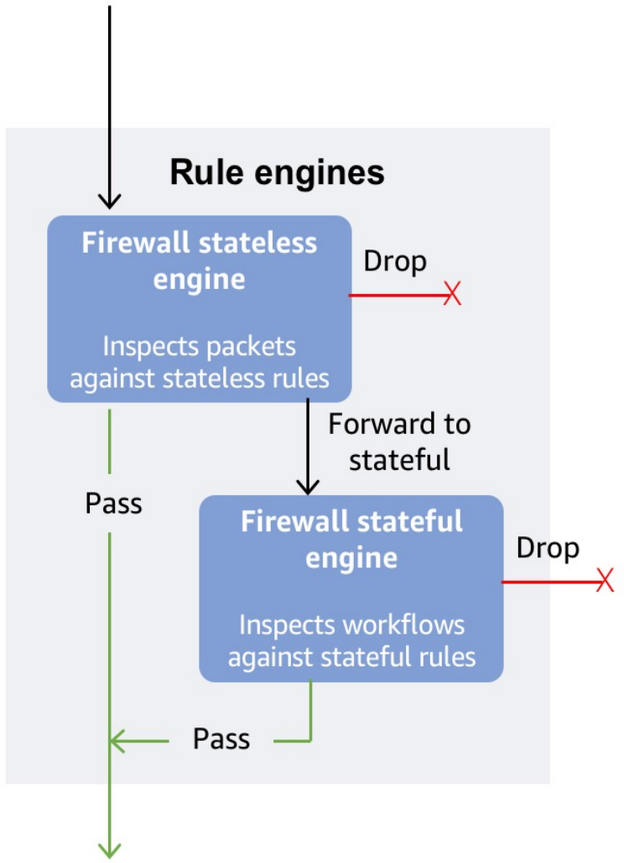


aws professional services

AWS Network Firewall

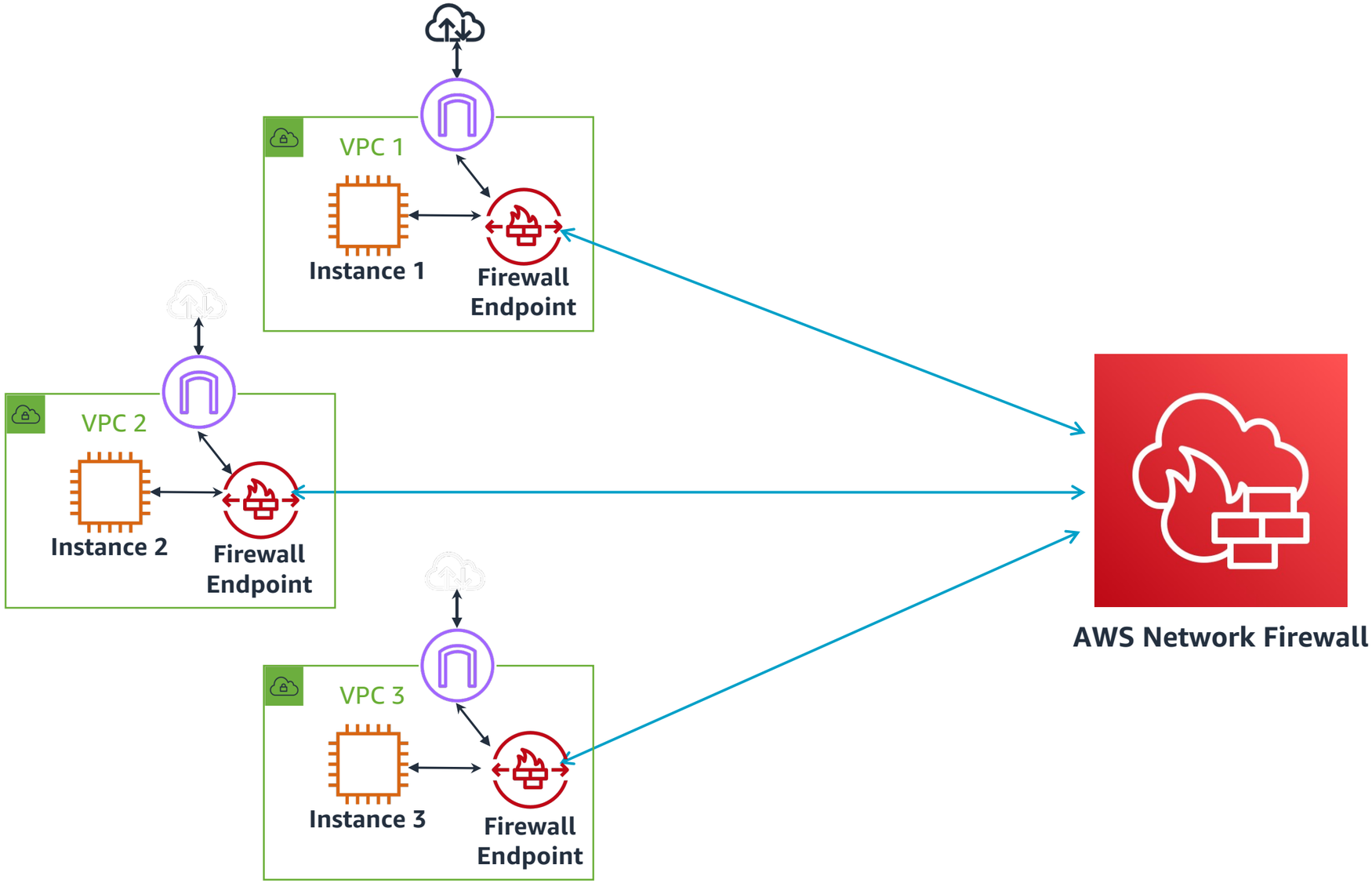






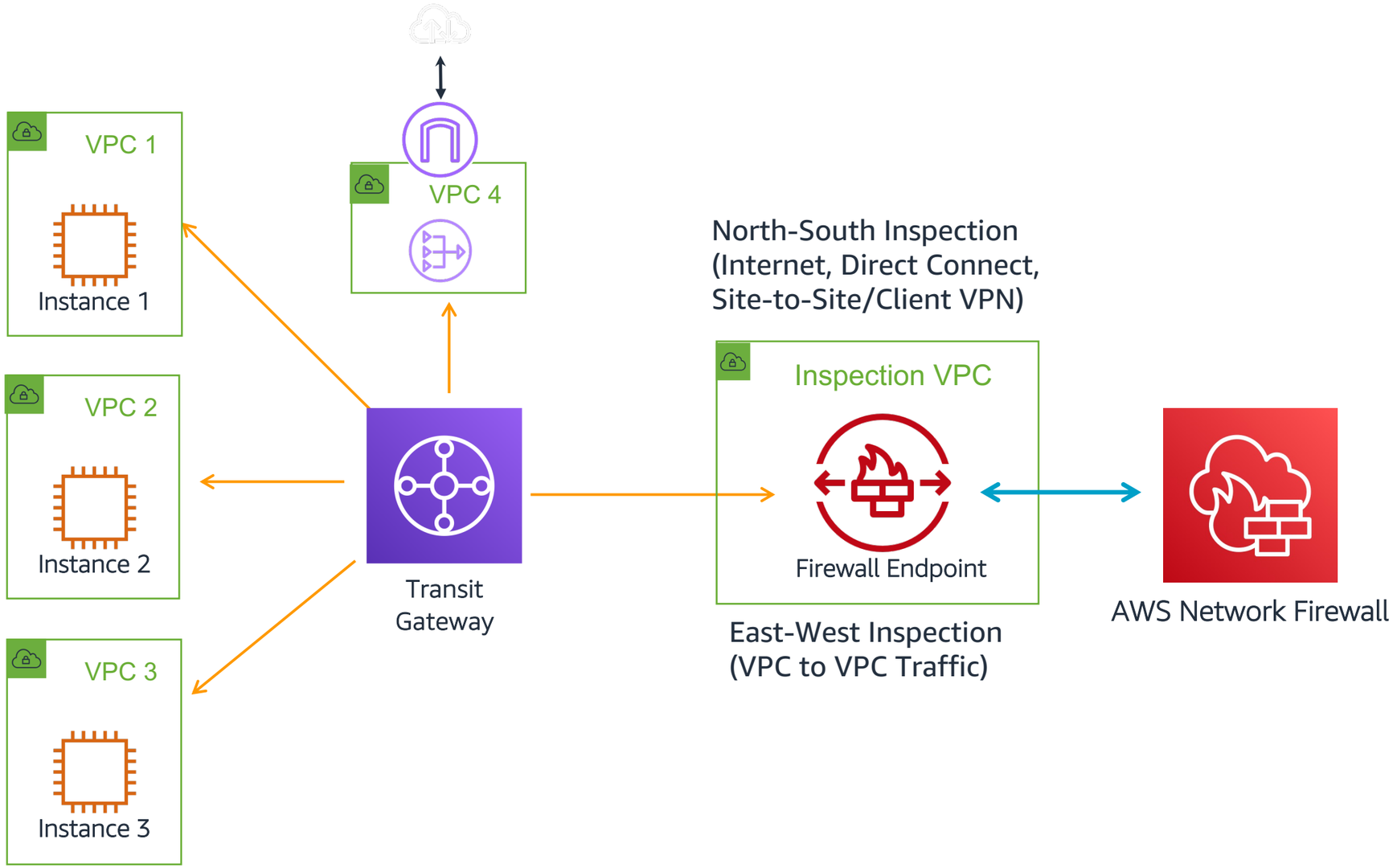
aws professional services

AWS Network Firewall deployment model: distributed



aws professional services

AWS Network Firewall deployment model: centralized



aws professional services

Additional VPC Security Features

Infrastructure Security

aws professional services

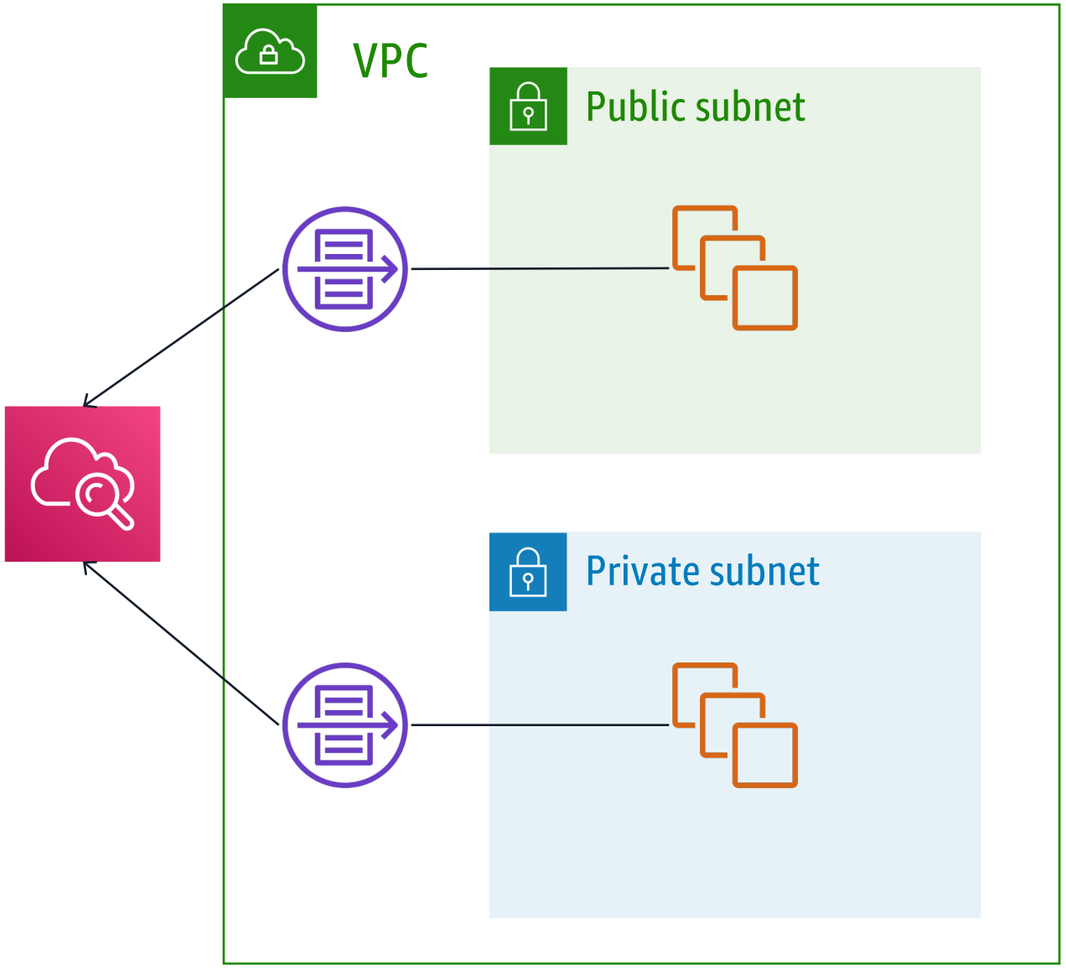
Native AWS Network Security Features

Examples from “Overview of Security Processes” whitepaper

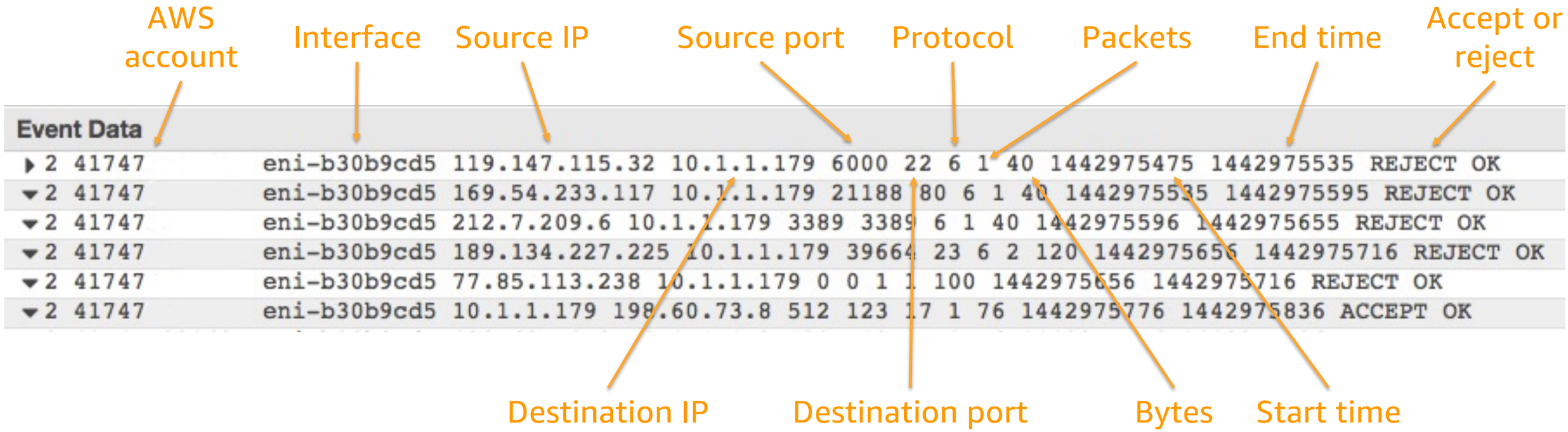
- **IP Spoofing**: Traditional Layer 2 security attacks, including MAC spoofing and ARP spoofing, are blocked.
- **Packet sniffing by other tenants**: It is not possible for a virtual instance running in promiscuous mode to receive or “sniff” traffic that is intended for a different virtual instance.
- **Man in the Middle (MITM) Attacks**: All AWS APIs are available via TLS-protected endpoints, which provides server authentication.

VPC Flow Logs

- Visibility into effects of Security Group rules
- Troubleshooting network connectivity
- Ability to analyze traffic
- Logged per ENI
- Agentless
- Create CloudWatch metrics from log data
- Alarm on CloudWatch metrics



Anatomy of a VPC Flow Log entry



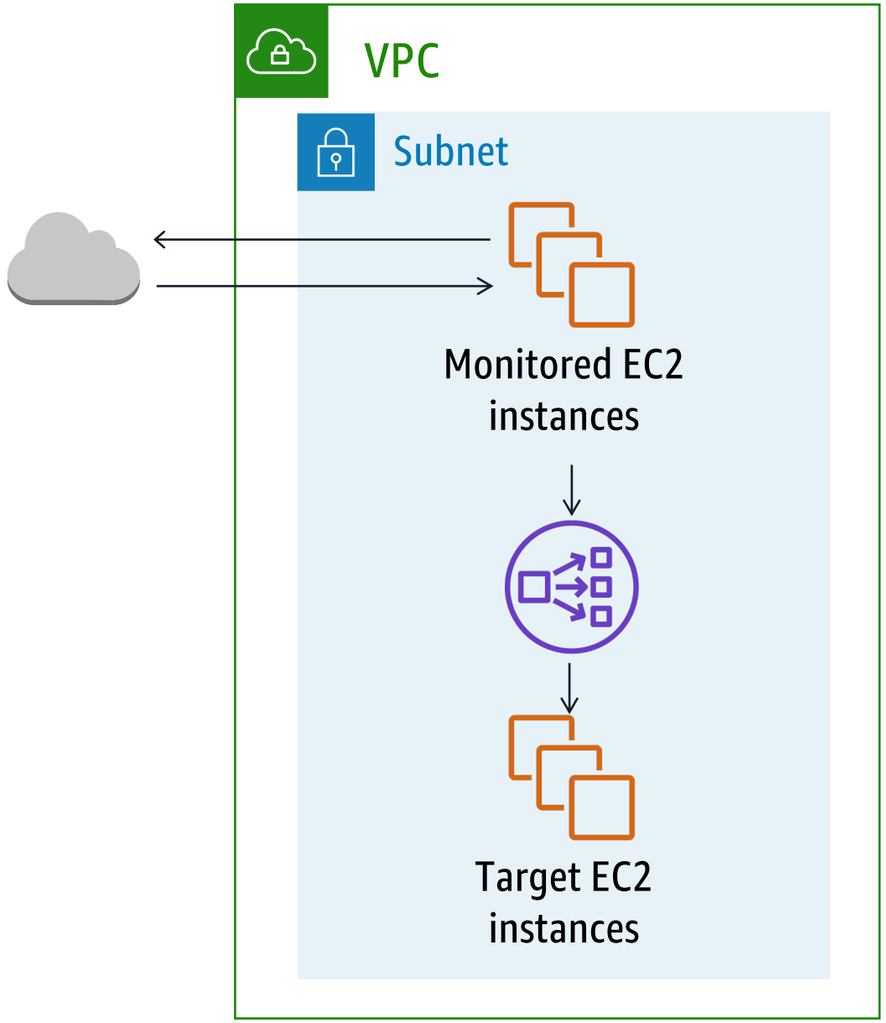
aws professional services

VPC Traffic Mirroring

- Capture and inspect network traffic at scale from EC2 instances
- Detect Network & Security Anomalies
- Implement Compliance & Security Controls
- Target instances can be in the same, or other VPC.

Components:

- Target
- Filter
- Session



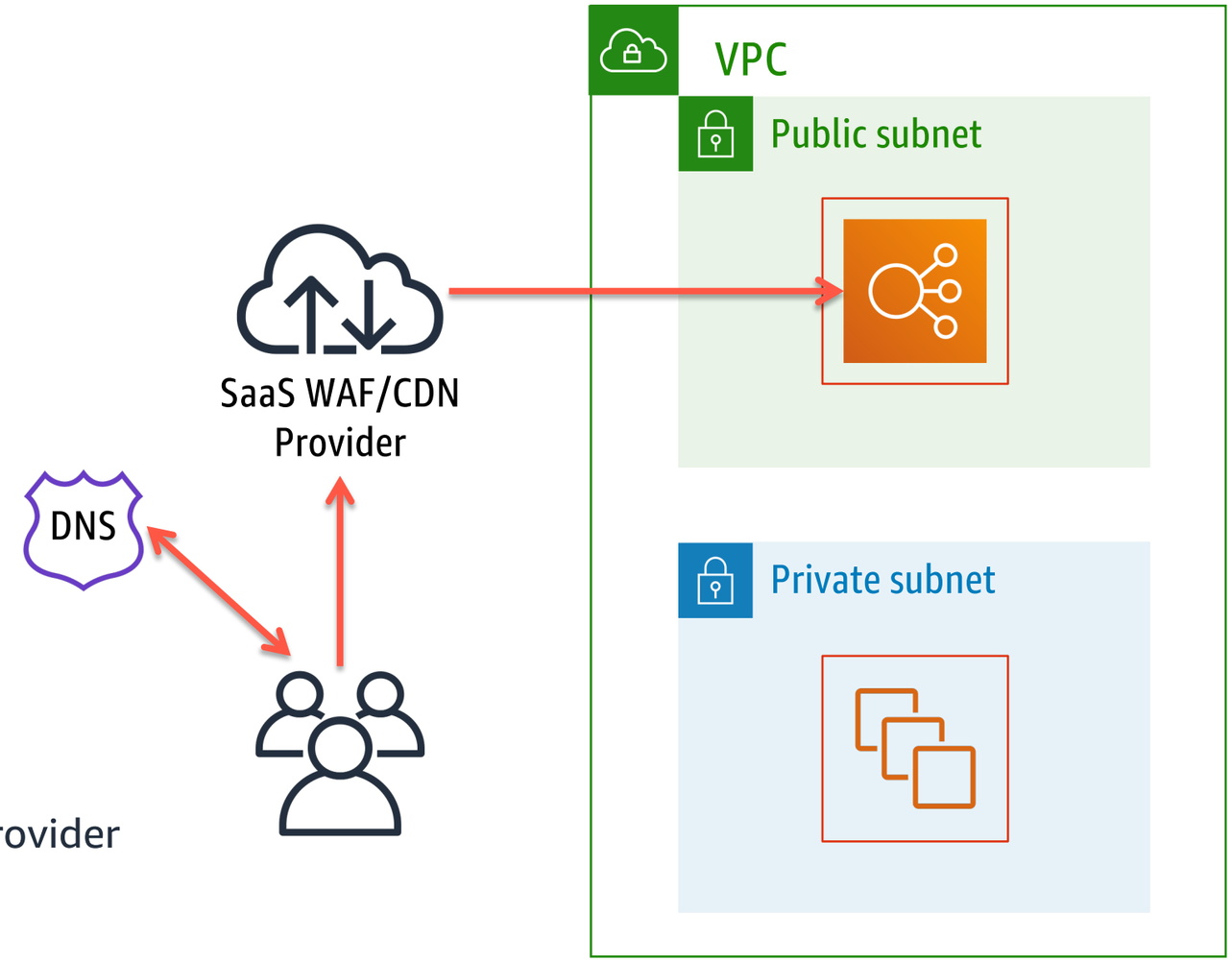
Non-Native Network Security

Infrastructure Security

aws professional services

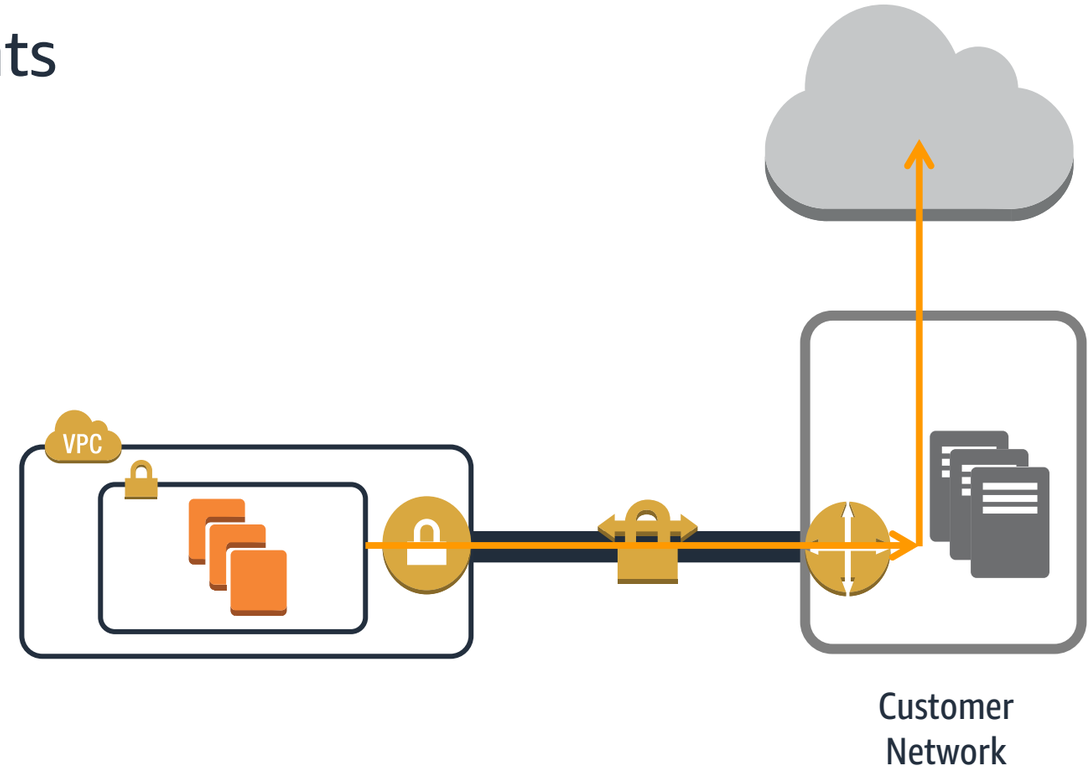
SaaS WAF/CDN Providers

- Various offerings
  - Intrusion prevention
  - Vulnerability assessment
  - Botnet detection/protection
  - Content proxy/caching
  - OWASP Top 10 protection
- Optional Managed Services
  - Analysis & incident response
  - Reporting
- Challenges
  - May be limited to inbound traffic
  - Scalability depends on vendor
  - Visibility into your traffic varies by provider
  - Adds latency, sometimes significant



Option: Use your current perimeter security stack

- “Lollipop”, “tromboning”, “router-on-a-stick”
- Benefits
    - Leverage your existing investments
    - Quick to implement
- Challenges
    - Extra latency
    - Bandwidth intensive
    - Low/no elasticity support
    - Amazon Linux Repos
    - Same old approval process



AWS Partner Network (APN) Security Solutions

Infrastructure Security

aws professional services

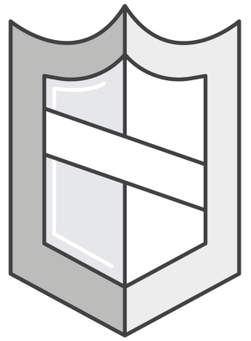
AWS Professional Services Security Workshop v6.0
Infrastructure Security

What is the AWS Partner Network (APN)?

- APN Partner products complement the existing AWS services to enable you to deploy a comprehensive security architecture and a more seamless experience across your cloud and on-premises environments.
- Collection of SaaS, AMI, Open-Source, and Marketplace product offerings.

What is the APN Security Competency Program?

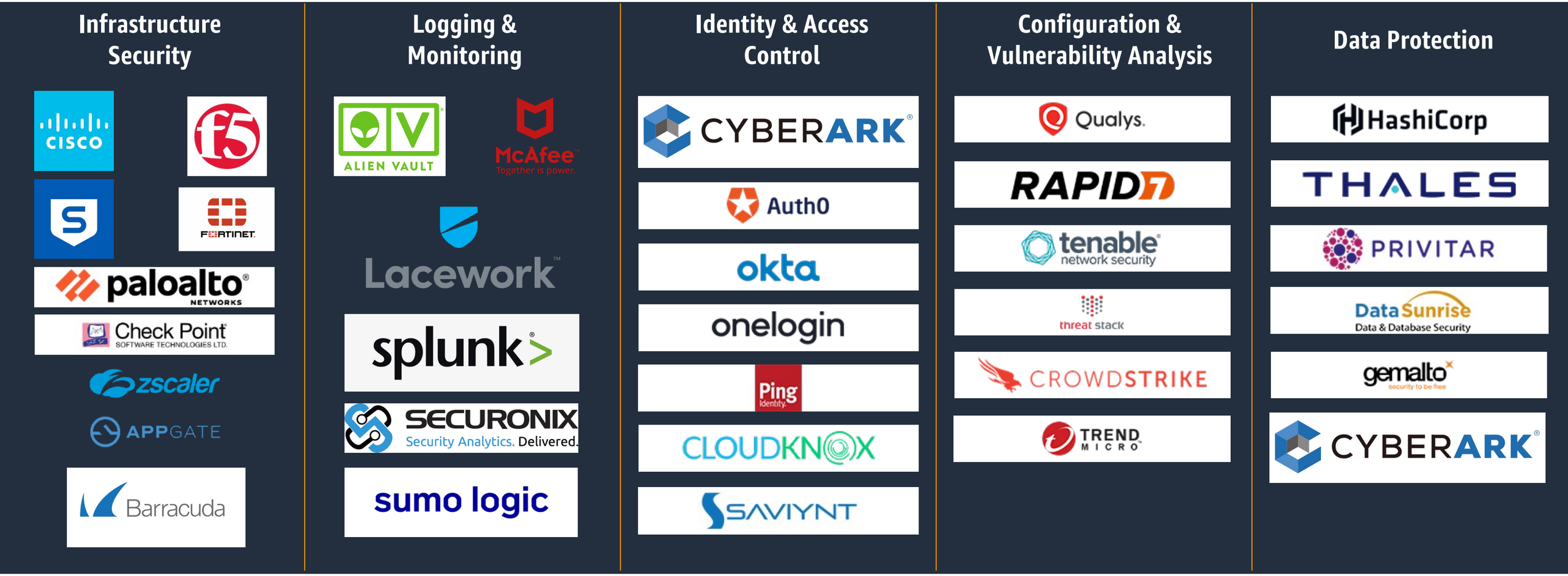
- APN Security Competency Partners have demonstrated success in building products and solutions on AWS to support customers.
- They provide deep technical and consulting expertise helping enterprises adopt, develop, and deploy complex Security projects.
- Infrastructure must support:
    - ELB above and below
    - Multi-AZ support
    - Bootstrapping
    - Auto-scaling support



APN Security Competency

aws professional services

APN Partner Overview



aws professional services

AWS Marketplace Enterprise Solutions

- Network firewalls
- Protection solutions from SaaS/CDN providers
- Web application firewalls (WAF)
- Network IDS solutions
- Host-based IPS

Factors for Choosing Security Solutions

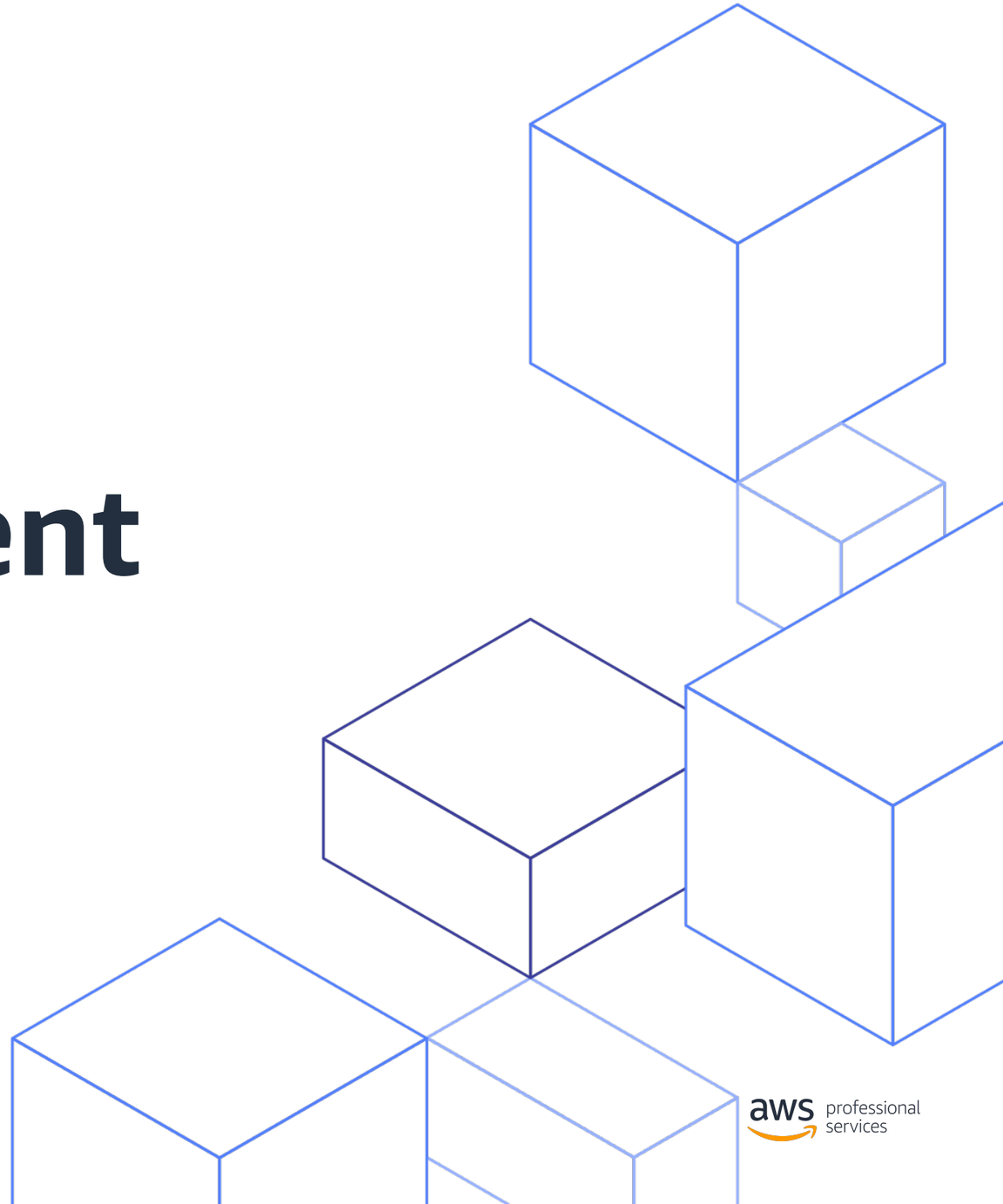
- Consider threat & risks to individual workloads
- APN Security Competency will shorten your list
- Any existing relationship or operational experience may affect preference
- Remember that a bake-off can be very rapid using AWS Marketplace

Criteria for Choosing Security Solutions

- Use cloud-aware or host-based solutions when possible
  - Security infrastructure should be cloud-aware
  - Host-based solutions are preferred for scalable applications
  - Test the solution for application stack issues, consider any performance impact, and determine operations & support
- If using in-line vendor solutions, determine where & why
  - Work with vendor to determine performance and high availability impact
  - May need to use solution in an isolated part of the network (e.g. separate VPC)

Systems Management

Infrastructure Security

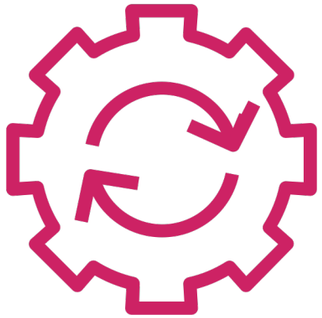


aws professional services

AWS Systems Manager

- Enable automated configuration
- Support ongoing management of systems at scale
- Work across all of your Windows and Linux workloads
- Run in Amazon EC2 or on-premises
- Carry no additional charge to use

AWS Systems Manager - Capabilities

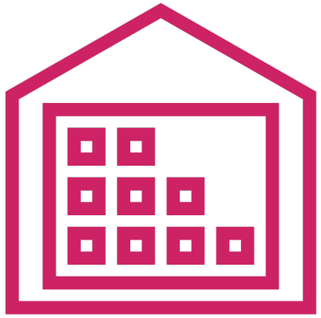


Automation

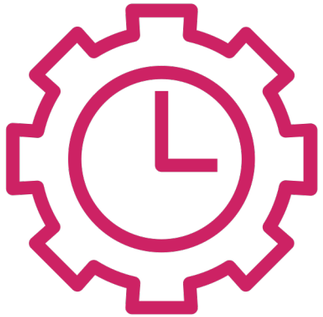
Documents

Patch Manager

Parameter Store



Inventory



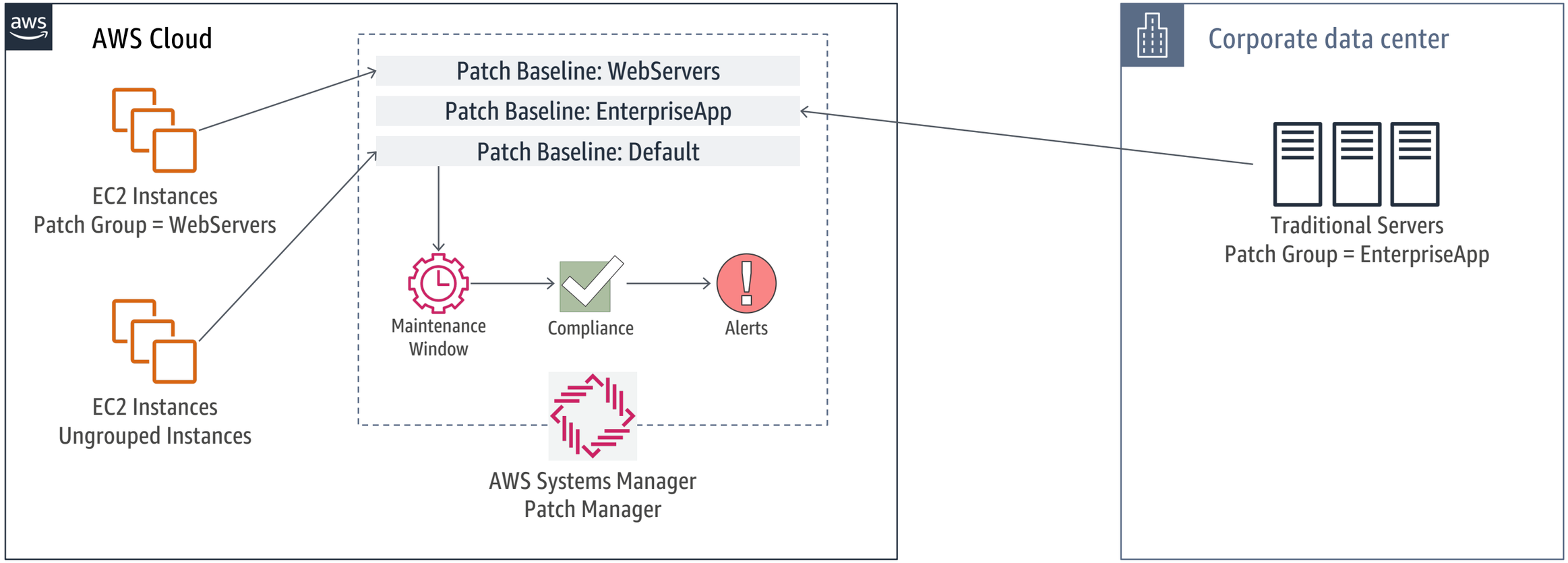
Maintenance Windows

State Manager

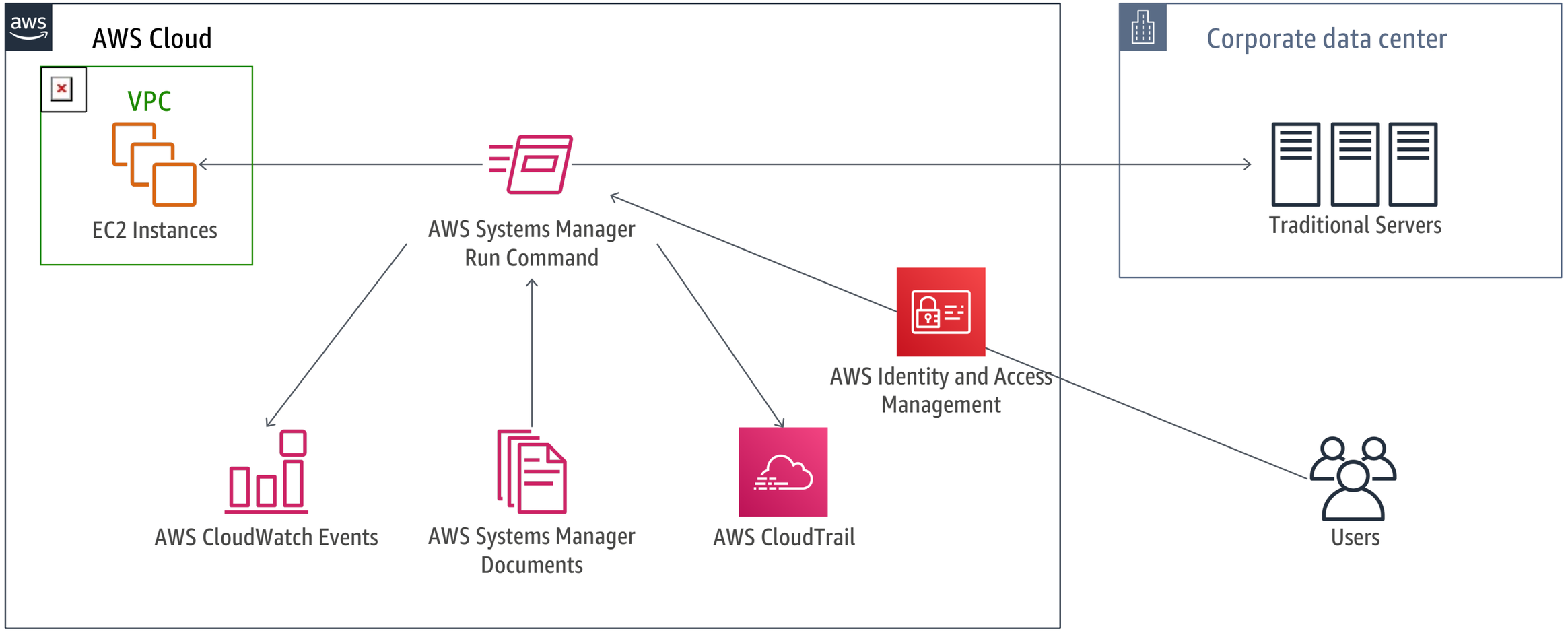
Run Command

aws professional services

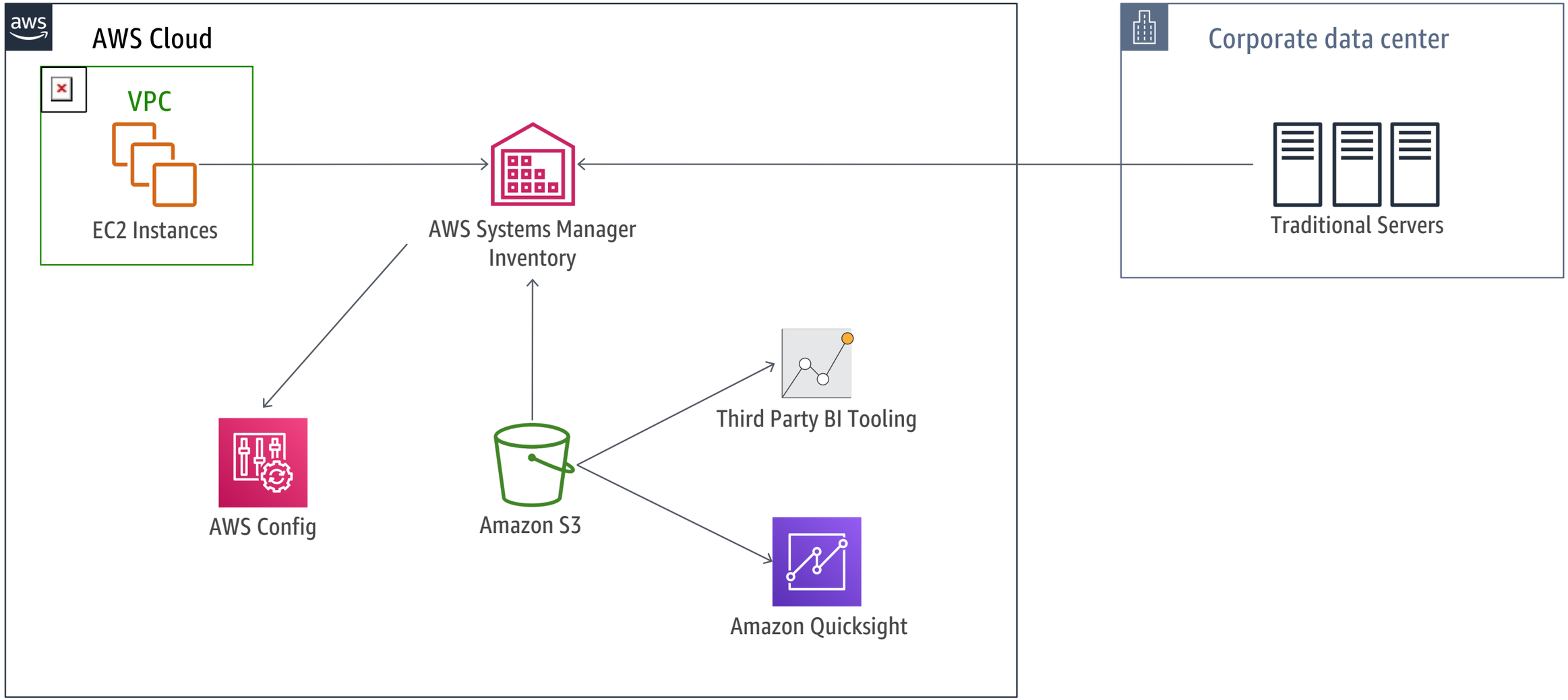
AWS Systems Manager – Compliance with Patch Manager



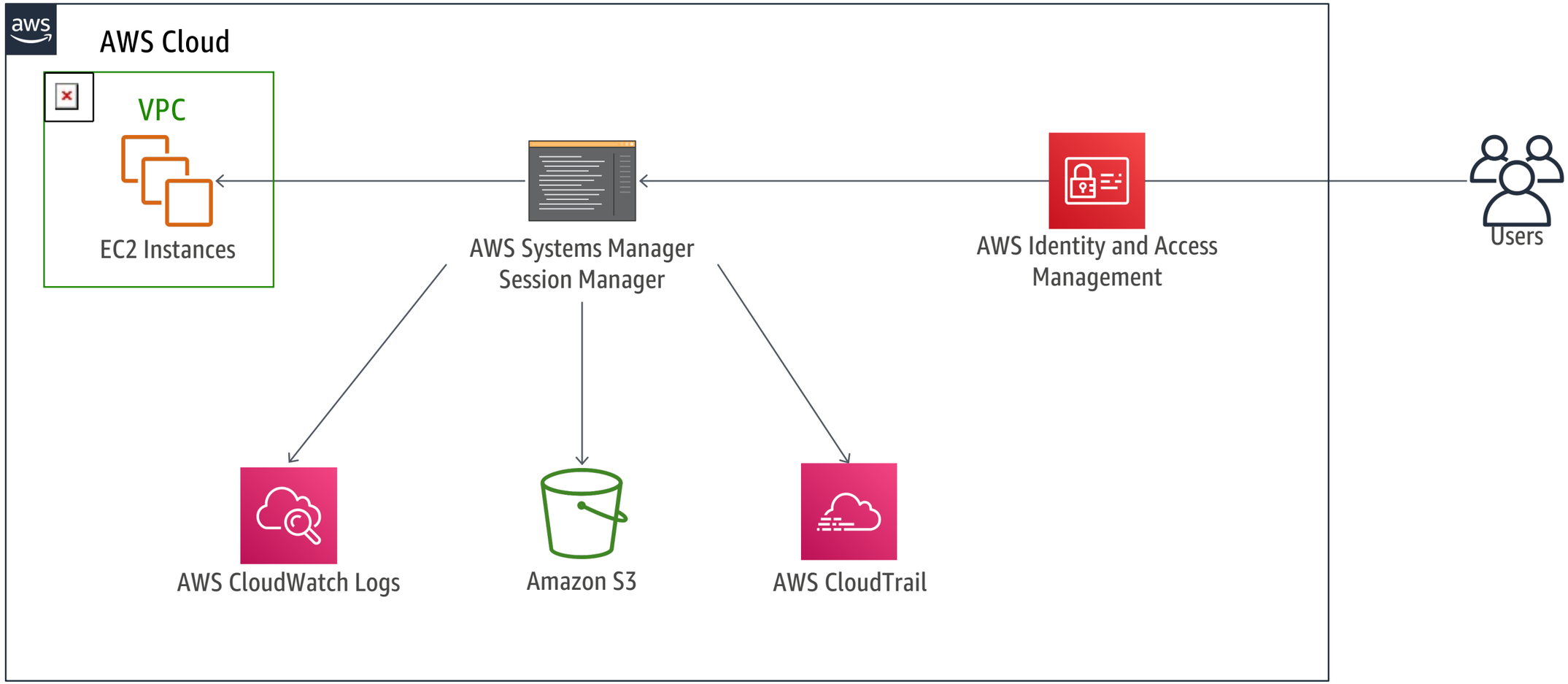
AWS Systems Manager – Run Command



AWS Systems Manager – Inventory

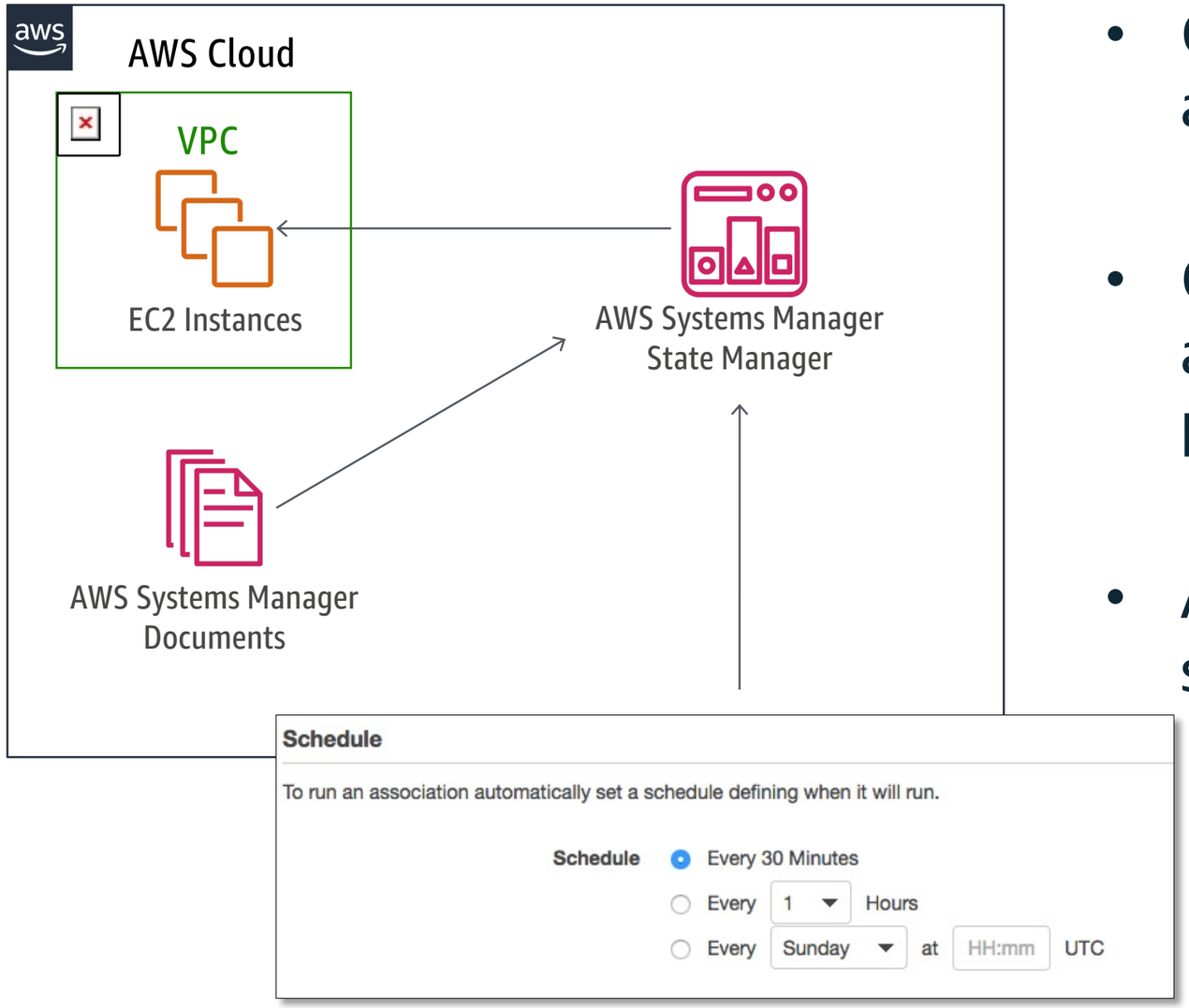


AWS Systems Manager – Session Manager



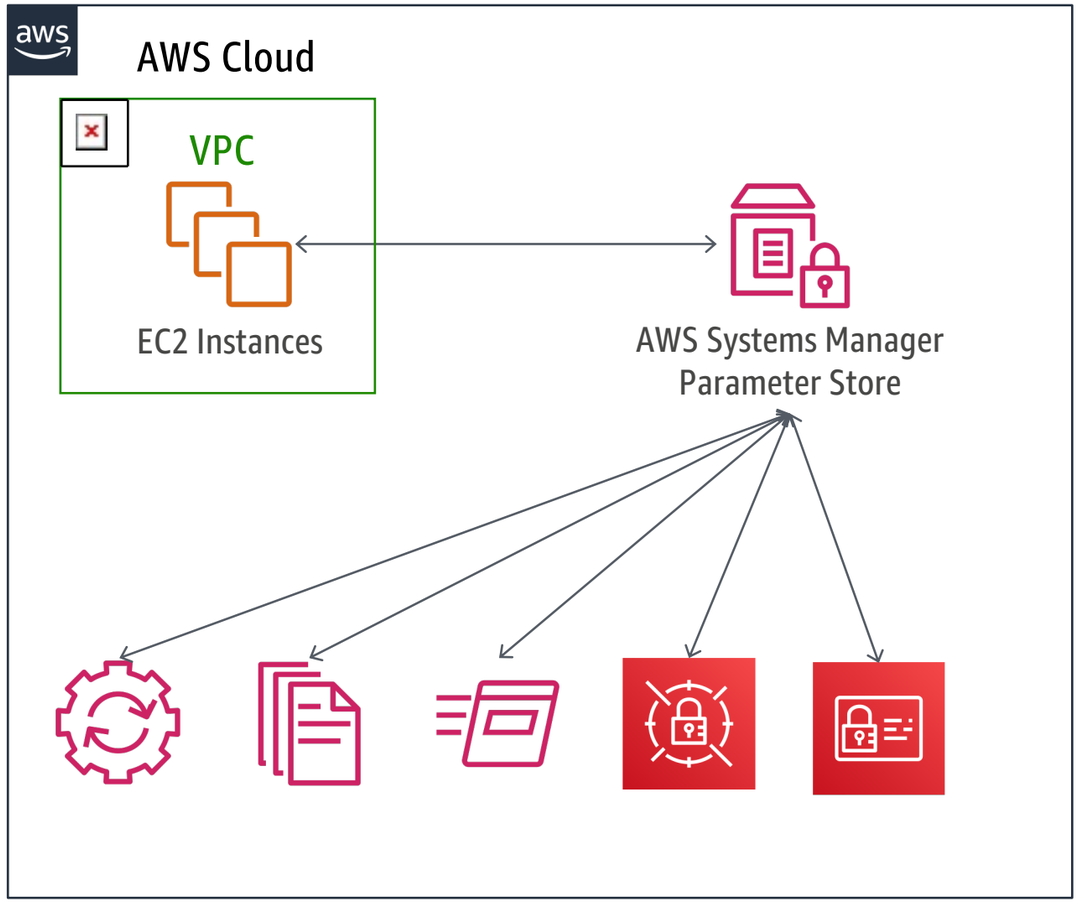
aws professional services

AWS Systems Manager – State Manager



- Control configuration details such as anti-virus settings, iptables, etc.
- Compare actual deployments against specified configuration policy
- Automatically re-apply policies if state drift is detected
  - OS changes
  - Local users and permissions

AWS Systems Manager – Parameter Store



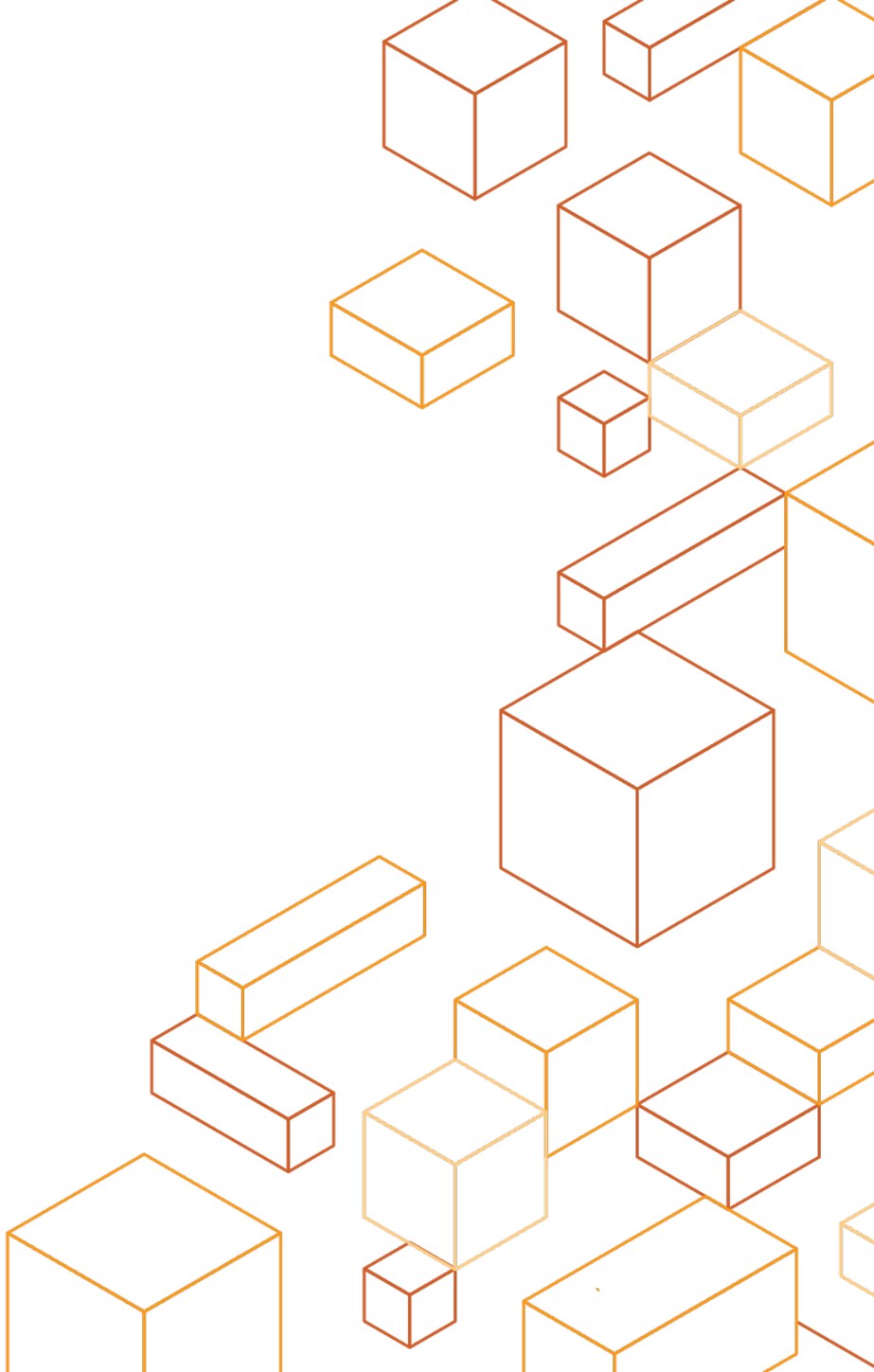
- Raise your security profile by managing configuration data separately from code
- Store parameters in hierarchies, track versions and dynamically reference to them from APIs
- Granularly control and audit access at parameter, tag, and path levels
- Integrates with AWS Secrets Manager and the other AWS Systems Manager components

AWS Systems Manager

Run Command	allows for a simple way of automating common administrative tasks like remotely executing shell scripts or PowerShell commands, installing software updates, or making changes to the configuration of OS, software.
Inventory	an extensible framework to collect and query configuration and inventory information about your instances and the software installed on them.
Patch Manager	helps select and deploy operating system and software patches automatically across large groups of instances.
State Manager	helps define and maintain consistent OS configurations such as firewall settings and anti-malware definitions to comply with your policies.
Maintenance Window	defines a recurring window of time to run administrative and maintenance tasks across your instances.
Session Manager	lets you manage your Amazon EC2 instances through an interactive one-click browser-based shell or through the AWS CLI. Session Manager provides secure and auditable instance management without the need to open inbound ports, maintain bastion hosts, or manage SSH keys.
Automation	simplifies common maintenance and deployment tasks, such as updating Amazon Machine Images (AMIs).
Parameter Store	a centralized location to store, provide access control, and easily reference your configuration data and secrets.
Documents	describe an instance configuration, which you can use to set up and run commands on your instances.

aws professional services

Questions



Appendix A: Additional Security Solutions

Infrastructure Security

aws professional services

Additional Firewall & VPN solutions

APN Partners

- Riverbed SteelConnect (formerly Ocedo)
- Cisco ASA
- Cisco CSR
- Juniper vMX
- Juniper vSRX

Open Source

- Iptables
- OpenVPN
- StrongSwan
- LibreSwan
- VyOS

Additional Intrusion Detection solutions

File and Instance Integrity

File Integrity Monitoring

- CloudPassage Halo
- OSSec
- TripWire

AWS Instances

- Symantec Cloud Workload Protection

Network Monitoring

Network traffic monitoring (similar to SPAN)

- Gigamon agent (ERSPAN)

Open Source

- Pfsense

Additional Web Application Firewall Solutions

AWS Native & APN Security Competency

AWS Web Application Firewall

APN Security Competency Partners

- AlertLogic Threat Manager
- Imperva SecureSphere
- Sophos
- Barracuda

Open Source

ModSecurity

NAXSI

Security Group Management solutions

APN Security Competency Partners

-  Dome9 SecOps
- AlgoSec
- Tufin
- Flowmon

Security Incident Event Management (SIEM) solutions

APN Security Competency Partners

- Splunk
- Sumo Logic

LogRhythm

AlienVault

ArcSight

Configuration Management Solutions

- Evident.io
- CloudCheckr
- Alert Logic Cloud Insight
- Tenable Network Security – Nessus
- ThreatStack

Additional Web Proxy solutions

APN Partners

- Barracuda
- Sophos
- Fortinet
- Palo Alto
- Check Point

Open Source

- Squid
- HA Proxy
- nginx

Anti-Virus Solutions

APN Partner Solutions


McAfee Public Cloud Server Security Suite (PCS)


Trend Micro Deep Security

Existing Solutions

Your current anti-virus solutions should continue to work with EC2 instances

Alternative Scanning & Vulnerability Assessment Solutions

Amazon Inspector

APN Security Competency Partners

- Qualys (pre-authorized)
- Nessus for Enterprise Cloud (pre-authorized)

Rapid7

Alien Vault

Data Loss Prevention (DLP) solutions

Symantec DLP

Data Protection Solutions

- Vormetric Transparent Encryption
- Gemalto’s SafeNet ProtectV
- SafeNet
- ProtectV and SafeNet Virtual KeySecure
- HyTrust DataControl for AWS 25VM
- Alliance Key Manager for Amazon Web Services