

AWS Network Security Design

AWS Security Workshop



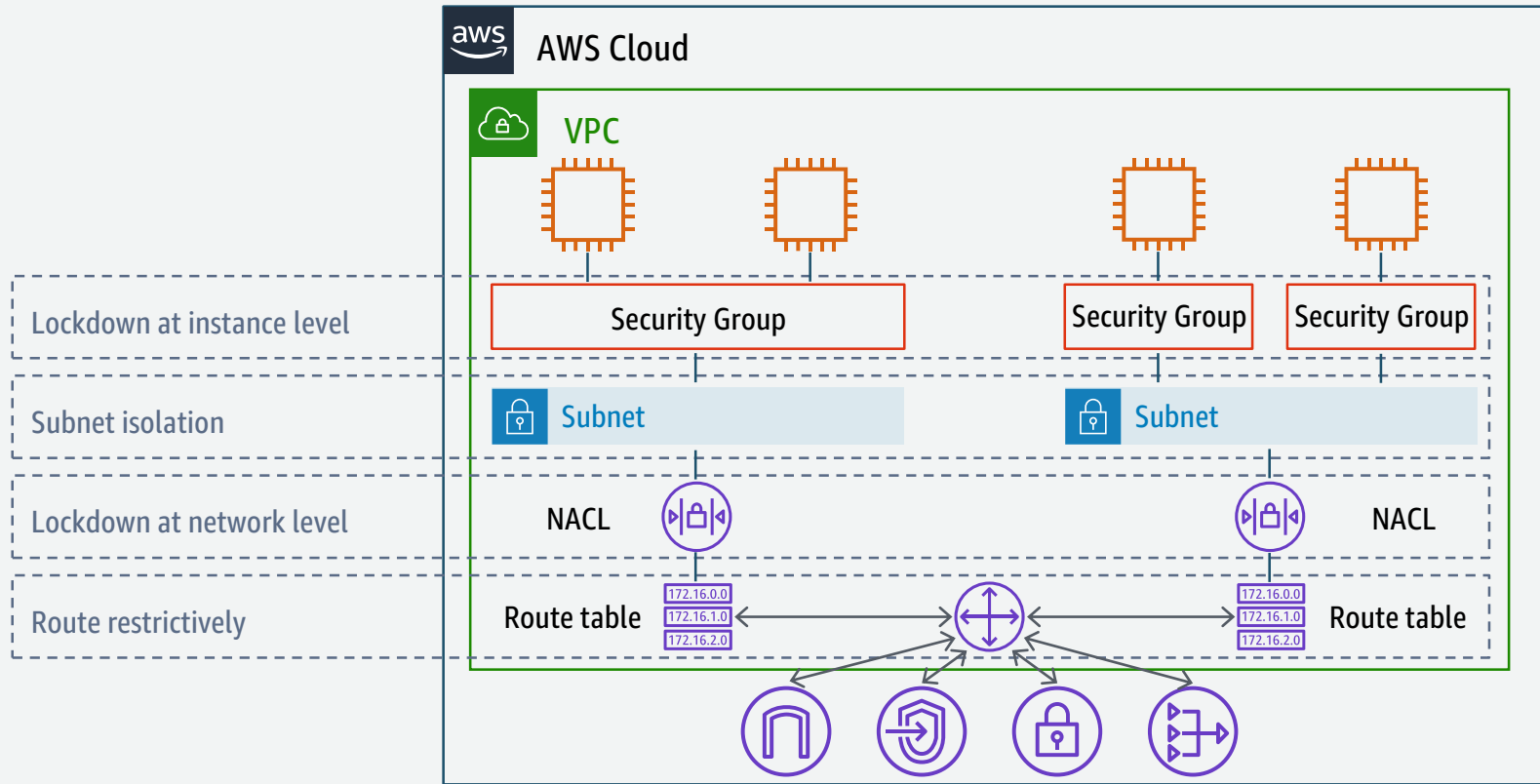
Agenda

- Denial of Service
- Defense in Depth
- Features of VPC network security
- Options for securing workloads

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

VPC Defense in Depth (review)

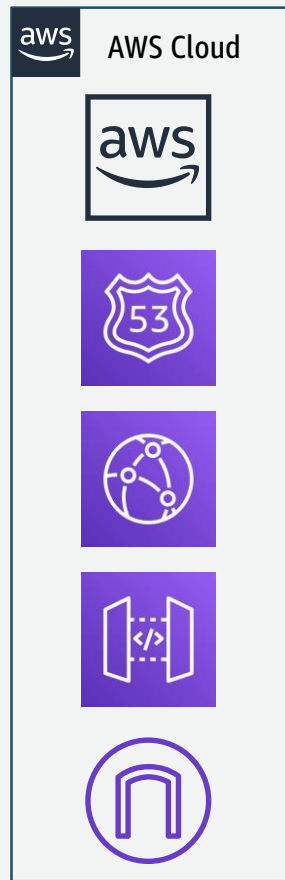
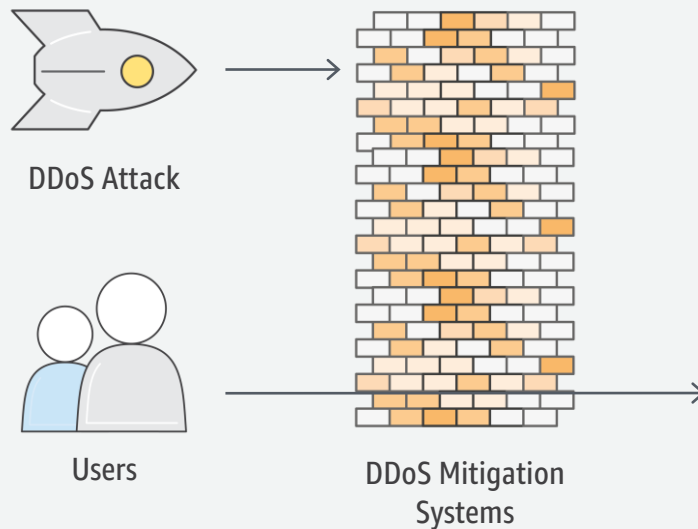


Denial of Service



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

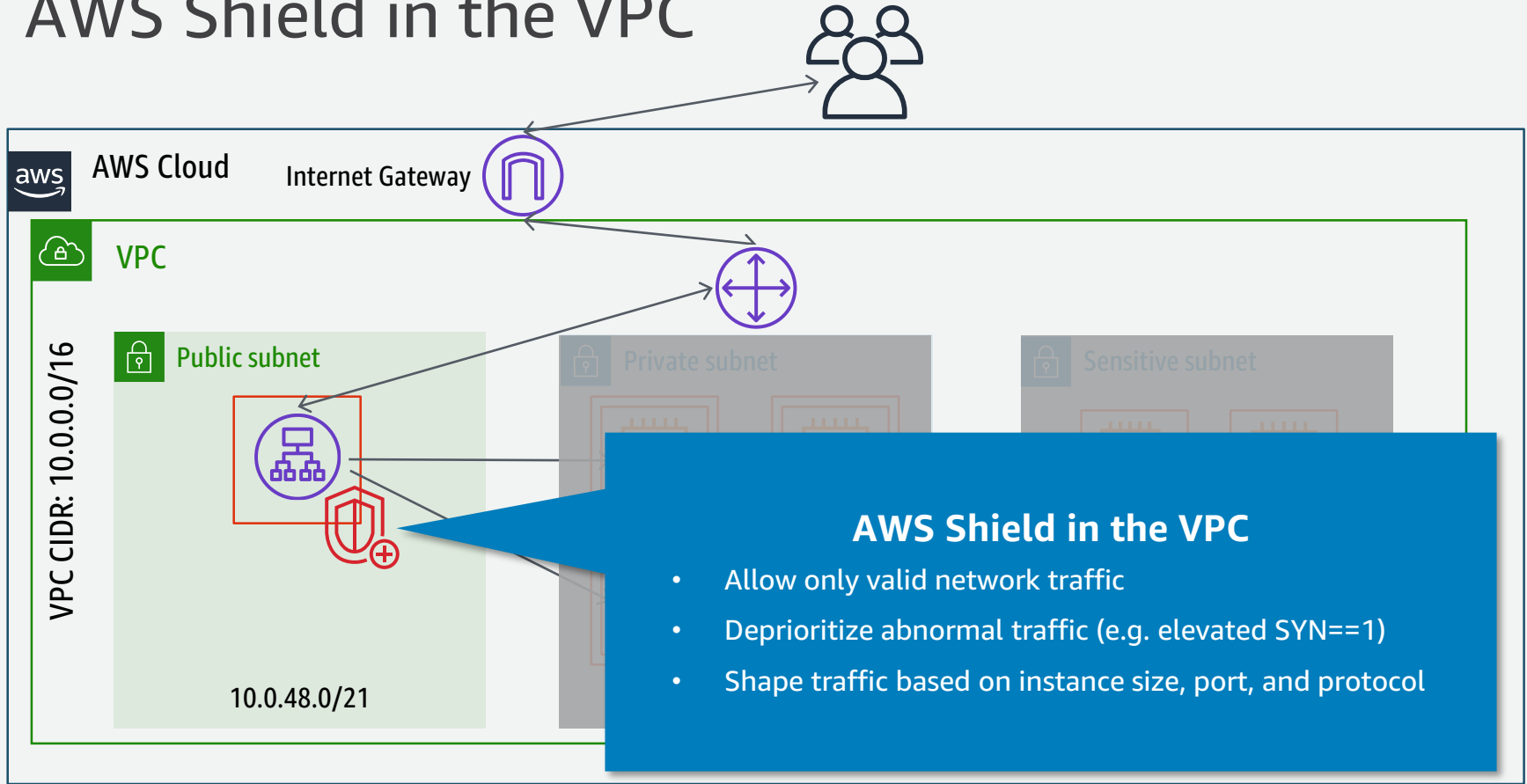
- Automatic detection & mitigation
- Protection from most common DDoS attacks (SYN/UDP Floods, Reflection Attacks, etc.)
- Built into AWS API's and Services

Layer 7 protection

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



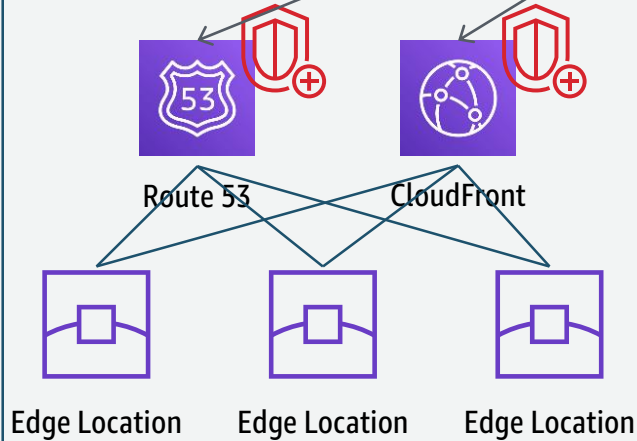
AWS Shield in the VPC



AWS Shield at the edge



AWS Cloud



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)



AWS Web Application Firewall (WAF)

Popular deployment modes



1. Custom Rules



2. Managed Rules



3. Security Automation

Or use any combination of the above ...

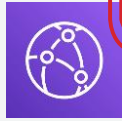
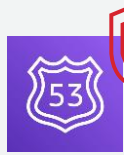
AWS WAF



AWS Cloud



AWS WAF



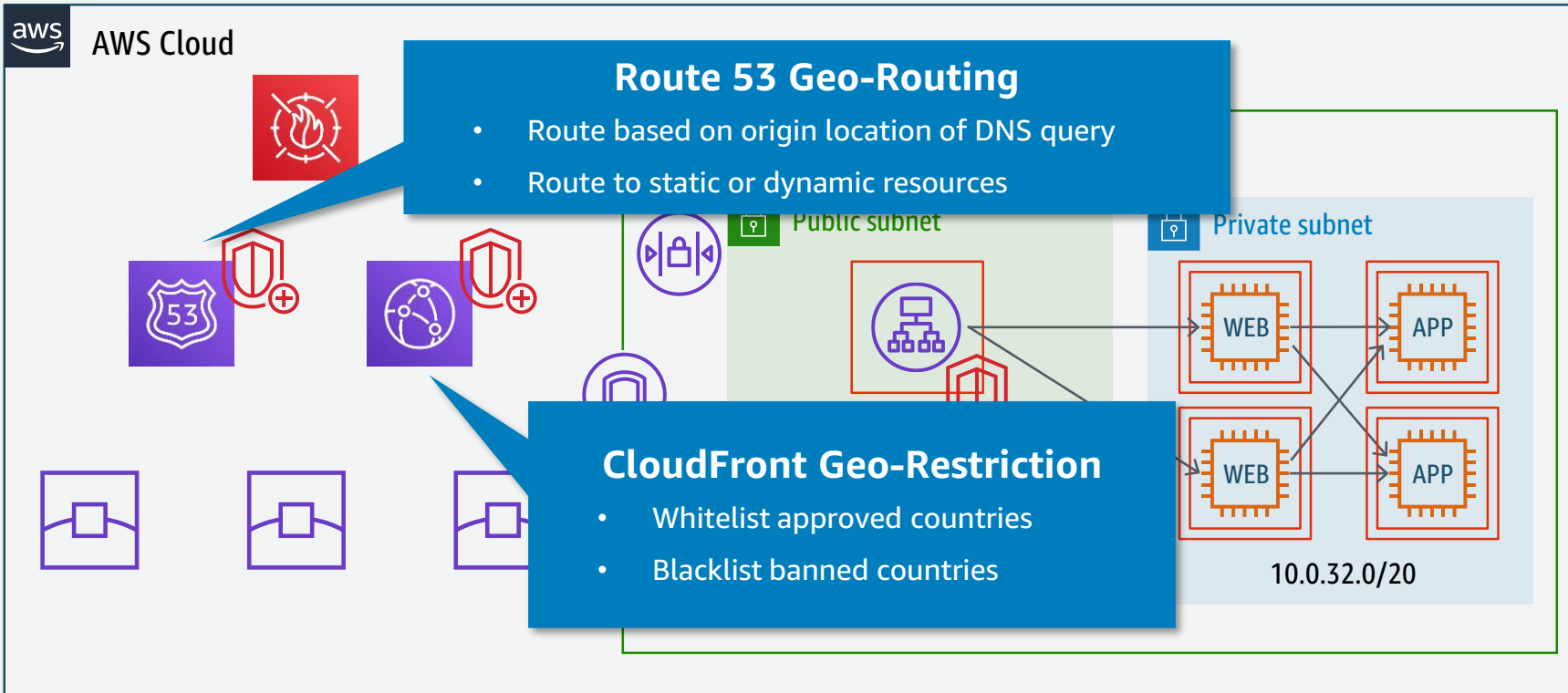
AWS WAF

- Web traffic filtering with custom rules
- Malicious request blocking
- Active monitoring and tuning
- Integrates with your applications & cloud infrastructure
- Enhanced security with managed rules

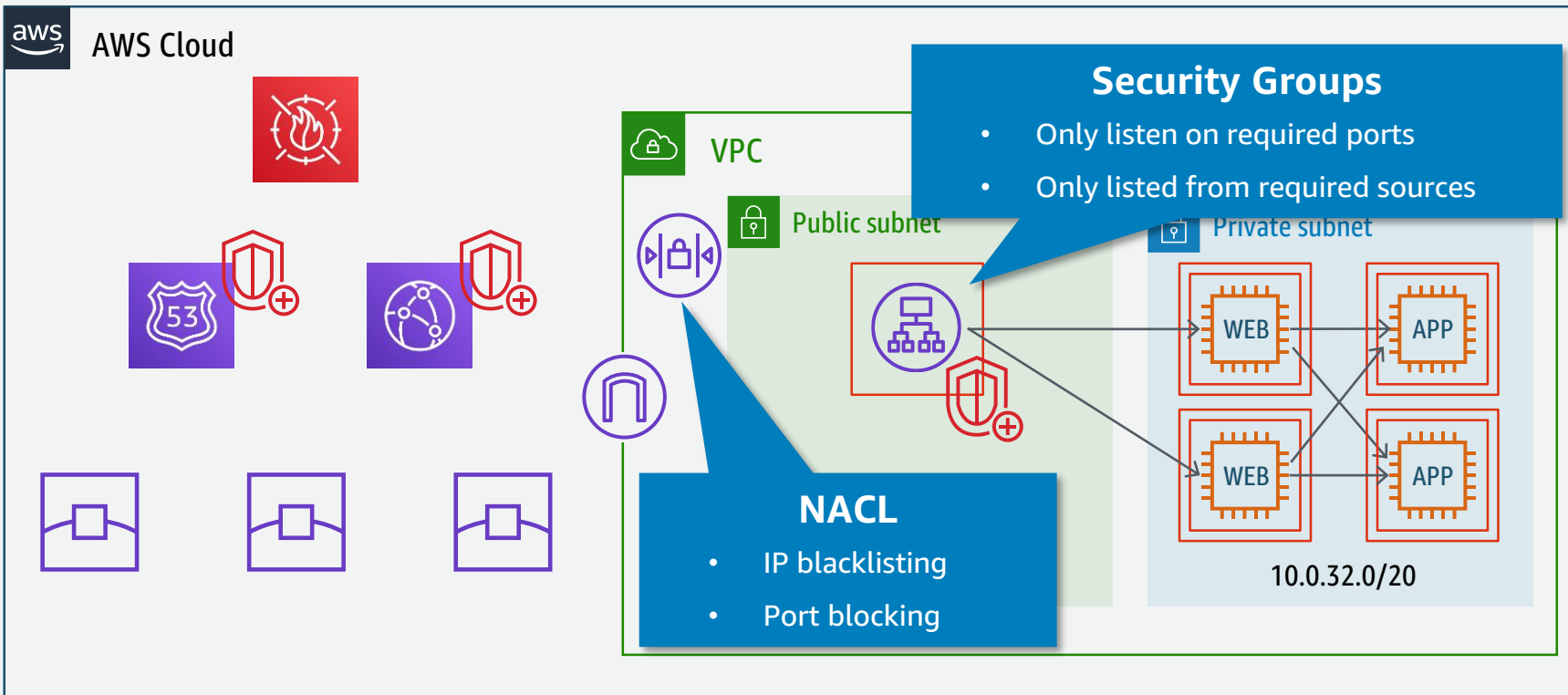
10.0.48.0/21

10.0.32.0/20

Stopping bad actors



Stopping bad actors



Stopping bad actors



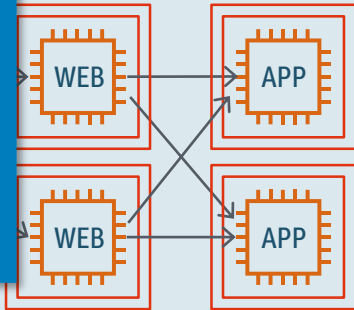
AWS Cloud



AWS WAF Rules

- IP blacklisting
- SQL injection prevention
- Cross site scripting prevention
- User-agent blocking
- Bad bot blocking
- Content scraper blocking

Private subnet

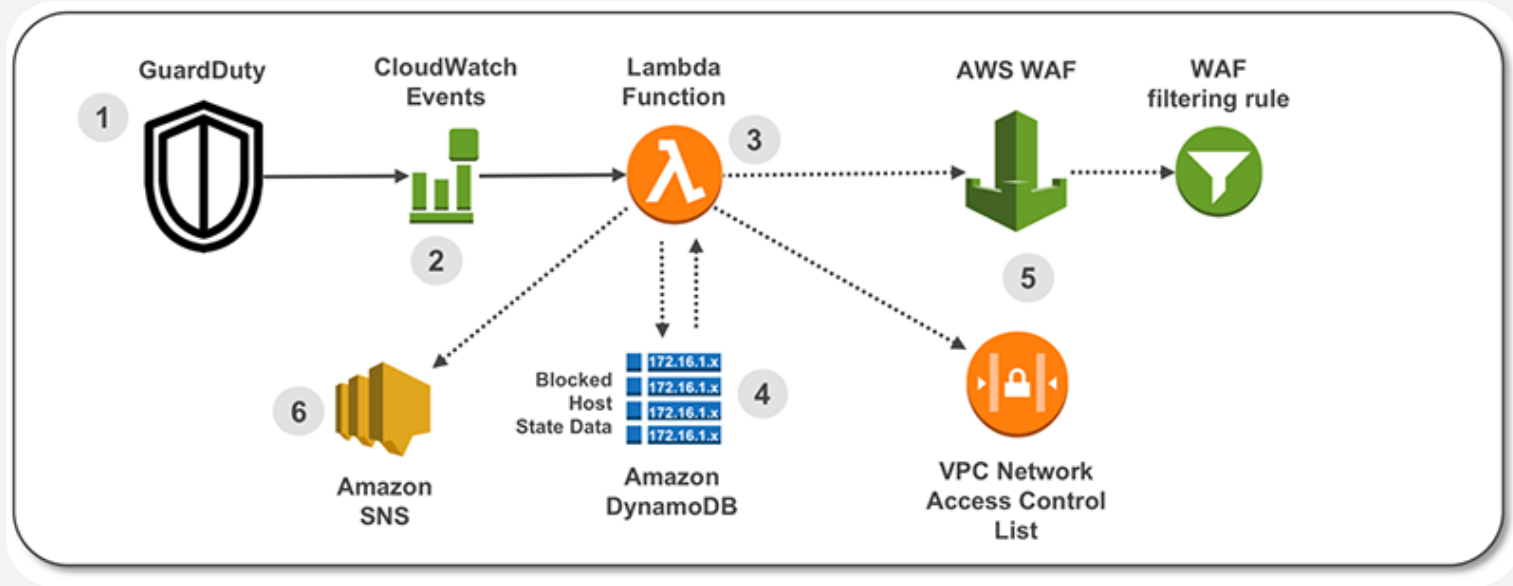


10.0.48.0/21

10.0.32.0/20

AWS Web Application Firewall (WAF)

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



AWS Firewall Manager



AWS Firewall Manager - Key Benefits

Simplified Management of WAF Rules

Integrated with
AWS Organizations

Centrally managed global
rules, and Account-specific
rules



Ensure Compliance to WAF Rules

Ensure entire Organization
adheres to mandatory set
of rules

Apply protection even when
new Accounts or resources
are created



Central Visibility Across Organization

Central visibility of WAF threats
across Organization

Compliance Dashboard for audit
firewall status

An organization's InfoSec team
learns and operates WAF
instead of each Account owner



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
- Subscribe to Managed Rules from AWS Marketplace
- Ensure the OWASP rule is applied across all PCI-tagged resources



AWS
Firewall
Manager



AWS
WAF

Additional VPC Security Features



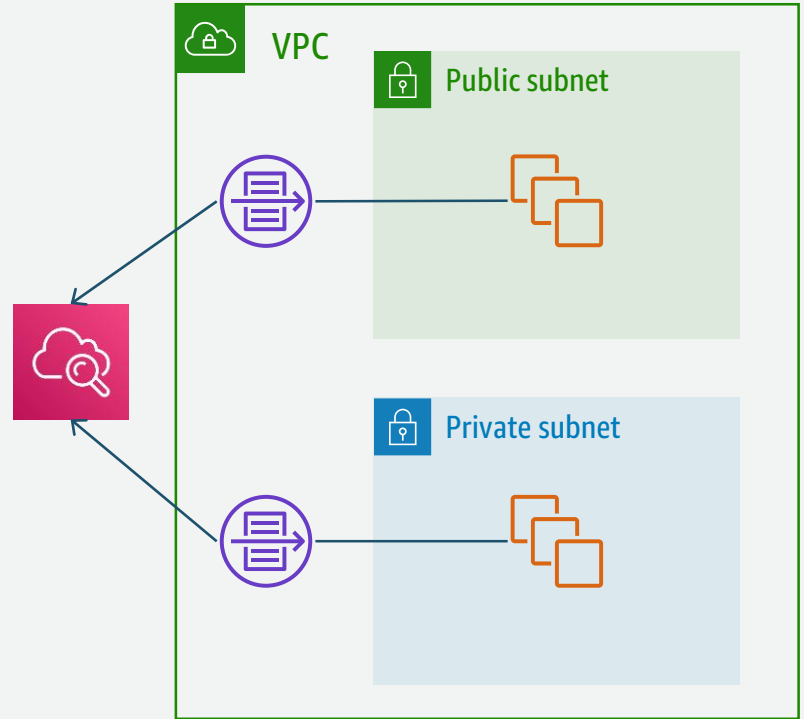
Native AWS Network Security Features

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

The diagram illustrates the structure of a VPC Flow Log entry. Orange arrows point from labels to specific fields in the table:

- AWS account** points to the first field (2).
- Interface** points to the second field (eni-b30b9cd5).
- Source IP** points to the third field (119.147.115.32).
- Source port** points to the fourth field (10.1.1.179).
- Protocol** points to the fifth field (6000).
- Packets** points to the sixth field (22).
- End time** points to the seventh field (6).
- Accept or reject** points to the eighth field (1).
- Destination IP** points to the ninth field (40).
- Destination port** points to the tenth field (1442975475).
- Bytes** points to the eleventh field (1442975535).
- Start time** points to the twelfth field (REJECT).

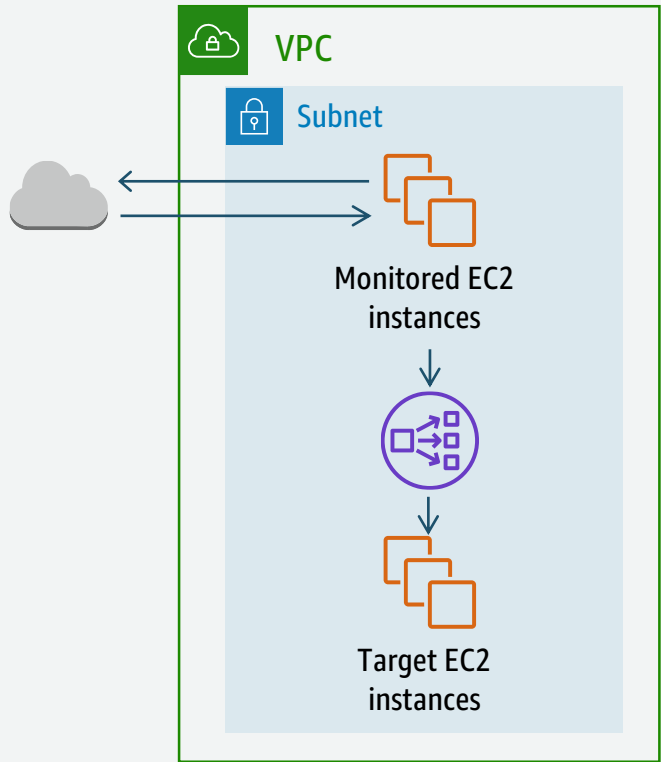
Event Data												
▶ 2	41747	eni-b30b9cd5	119.147.115.32	10.1.1.179	6000	22	6	1	40	1442975475	1442975535	REJECT OK
▼ 2	41747	eni-b30b9cd5	169.54.233.117	10.1.1.179	21188	80	6	1	40	1442975535	1442975595	REJECT OK
▼ 2	41747	eni-b30b9cd5	212.7.209.6	10.1.1.179	3389	3389	6	1	40	1442975596	1442975655	REJECT OK
▼ 2	41747	eni-b30b9cd5	189.134.227.225	10.1.1.179	39664	23	6	2	120	1442975656	1442975716	REJECT OK
▼ 2	41747	eni-b30b9cd5	77.85.113.238	10.1.1.179	0	0	1	1	100	1442975656	1442975716	REJECT OK
▼ 2	41747	eni-b30b9cd5	10.1.1.179	198.60.73.8	512	123	17	1	76	1442975776	1442975836	ACCEPT OK

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

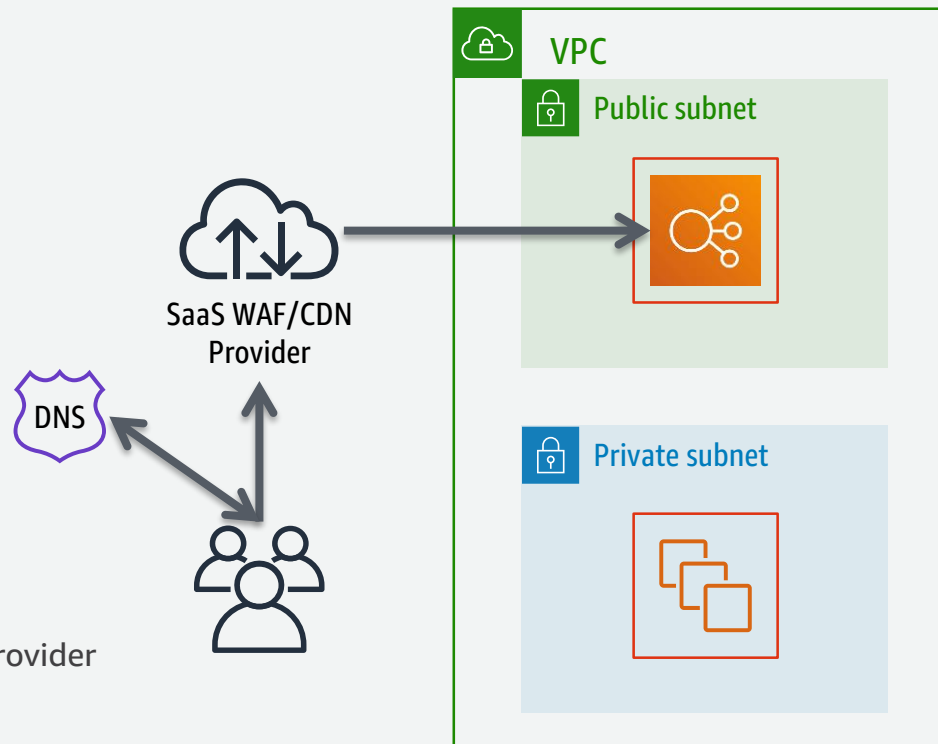


Non-Native Network Security



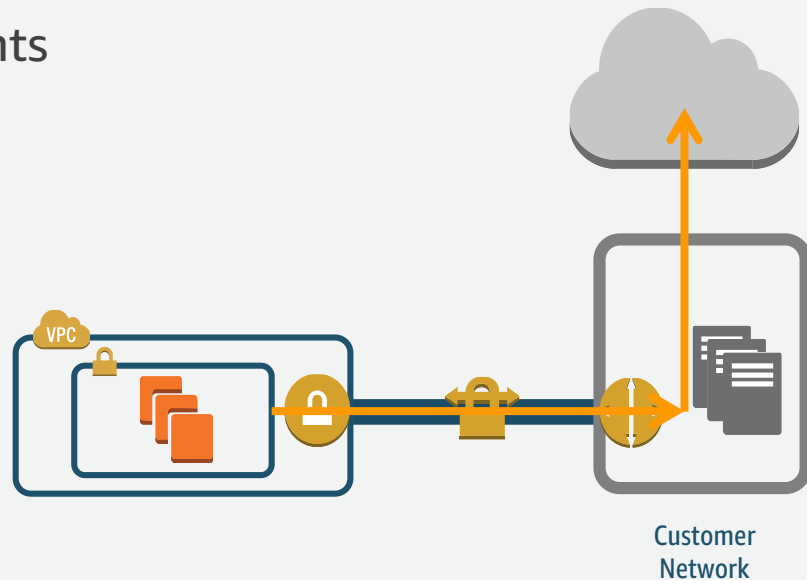
SaaS WAF/CDN Providers

- 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



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

APN Partner Overview

Infrastructure Security



Logging & Monitoring



Identity & Access Control



Configuration & Vulnerability Analysis



Data Protection



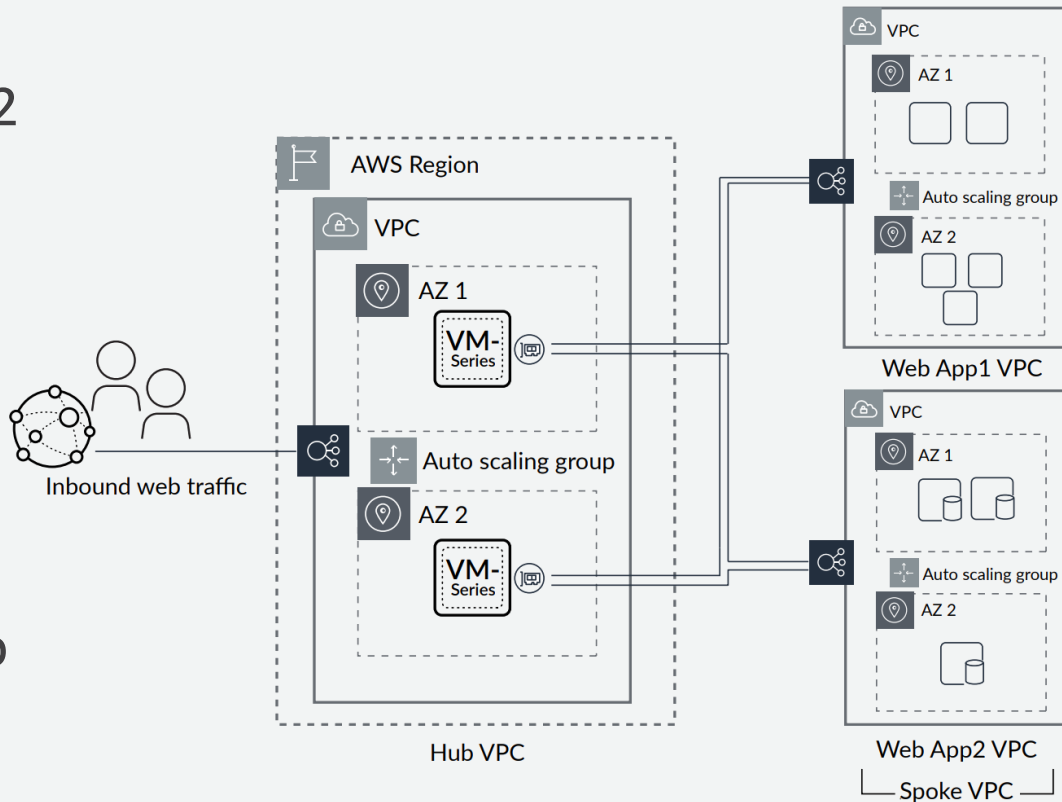
AWS Marketplace Enterprise Solutions

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



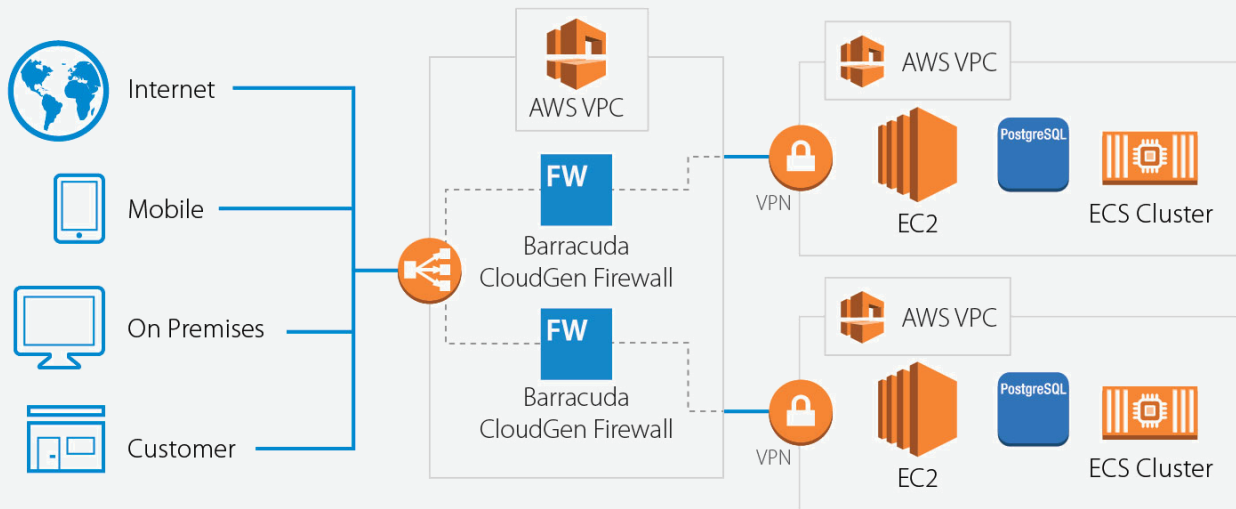
Firewall: Palo Alto VM-series on AWS

- Virtual appliance(s) on EC2
- Features:
 - Firewall
 - Network IDS/IPS
 - Application aware
 - User-based policies
- Can connect VPCs
- Integration with AWS GuardDuty & Security Hub
- BYOL or hourly billing



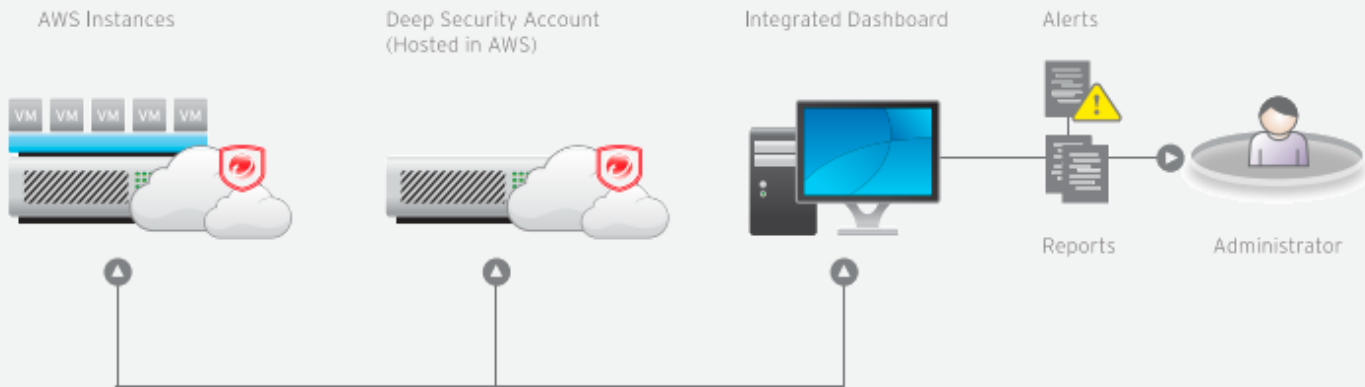
WAF: Barracuda CloudGen WAF

- Works together with AWS ELB
- Can help comply with PCI-DSS, HIPAA and NIST 800-52
- Built-in caching & compression
- OWASP Top 10
- Layer 7 DDoS protection
- Inbound & Outbound protection
- Auto-scaling
- Available as BYOL, Pay-as-you-go, or Metered



Host-based IDPS: Trend Micro Deep Security

- Long features list
 - IDS, IPS
 - Firewall
 - Anti-malware
 - Integrity monitoring
 - Log inspection
 - Web reputation
- Can help meet PCI DSS, HIPAA, NIST, SAS 70
- Compatible with cloud deployment tools OpsWorks, Chef, Puppet, Rightscale
- Available as SaaS or software solution



More security options in Appendix A:

Web Application
Firewalls

Security Incident
Event Management
(SIEM)

Security Group
Management

Security
Configuration
Management

Anti-virus

Web Proxies

Scanning &
Vulnerability
Assessment

Data Loss
Prevention

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)

Questions?

Appendix A: Additional Security Solutions



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