
AWS
re:Invent

SEC311

Introducing AWS Network Firewall

Maritza Ramirez Mills

Senior Product Manager

AWS

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

The need for defense in depth: a history

Introducing AWS Network Firewall

Getting started

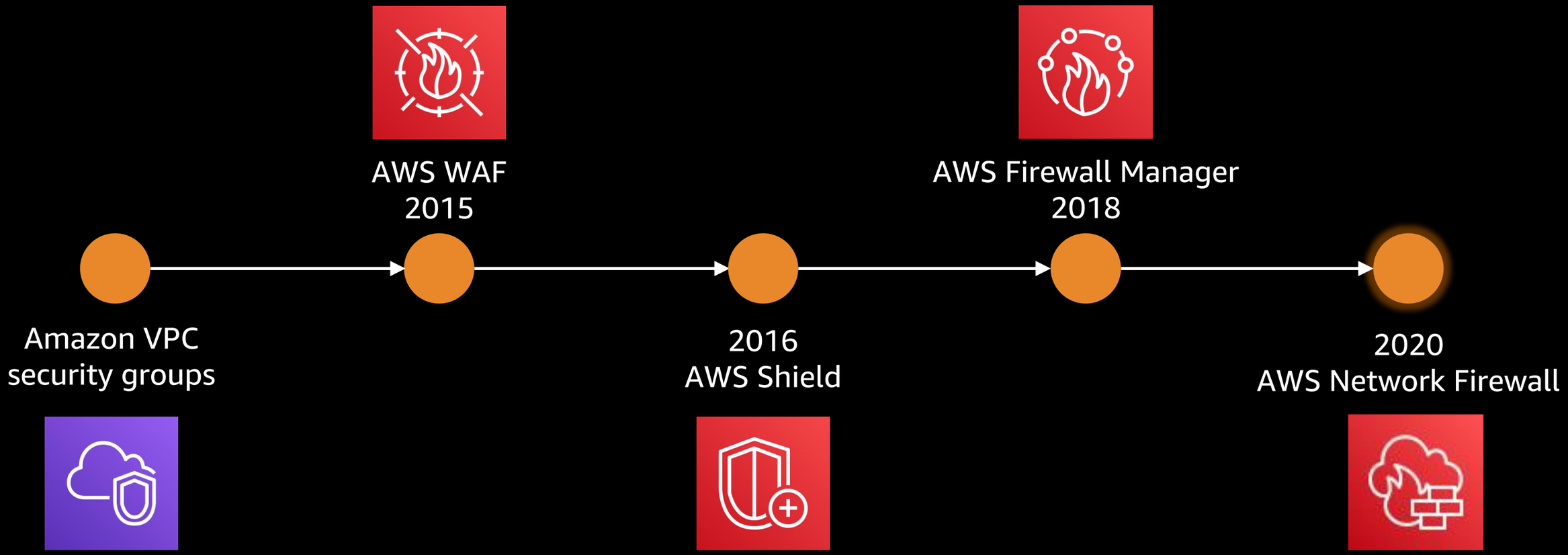
Regional availability and pricing



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

A brief history of protective services on AWS



Network Firewall



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

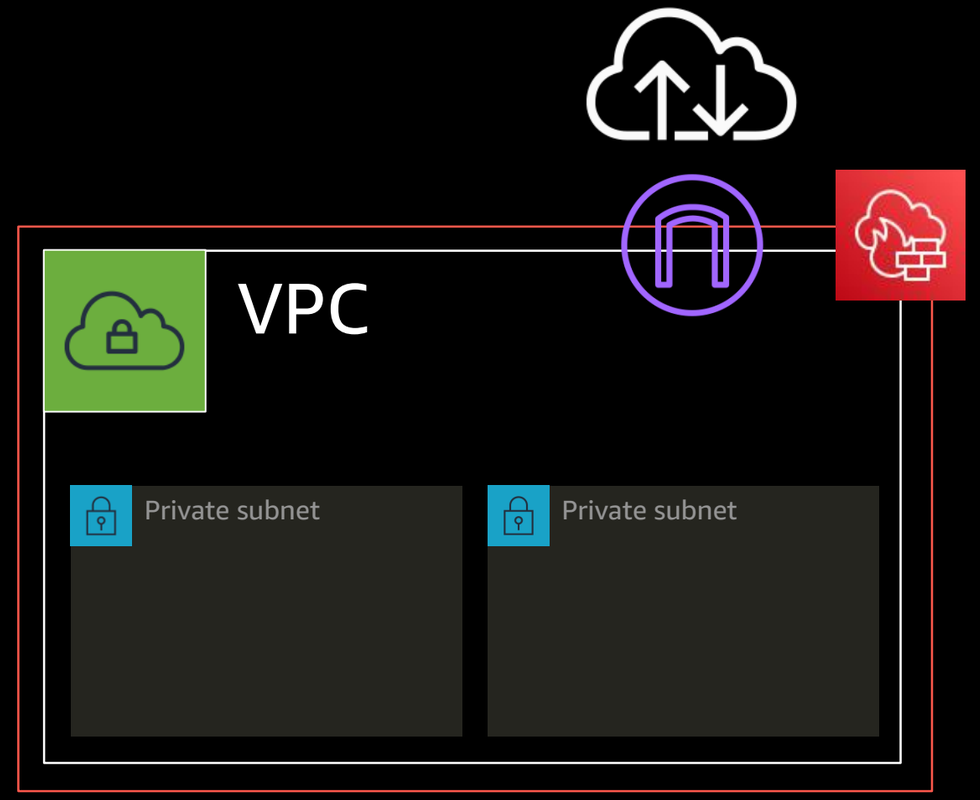
Network Firewall

Apply blanket protections for your entire Amazon VPC

Any application type or protocol (L3-L7 firewall)

Inspect

- VPC-to-VPC traffic
- Outbound to internet
- Inbound from internet
- AWS Direct Connect and VPN



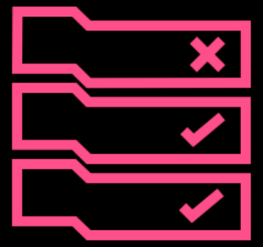
Key benefits



Fully managed



Flexible deployments



Fine-grained controls



Partner integrated

Managed availability

Scales automatically

Highly available

Removes friction



Flexible deployments



Selectively choose which flows you want to inspect

Scale out to thousands of accounts or centralize with AWS Transit Gateway

Learn more at NET306

Central management through Firewall Manager

Central management with Firewall Manager



One place to manage all protective controls on AWS

Continuously manage & audit

Enforce protections, even as new applications are created

View compliance posture centrally across AWS accounts

Learn more at SEC320

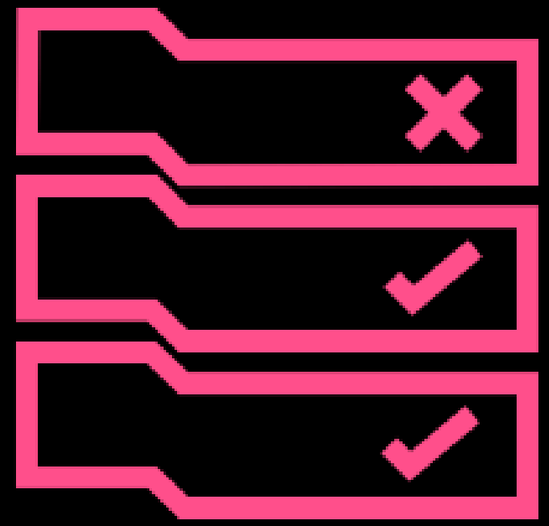
Fine-grained controls

IP/port/protocol

Fully qualified domain name

General pattern matching – regular expression matching

Allow, drop, or alert



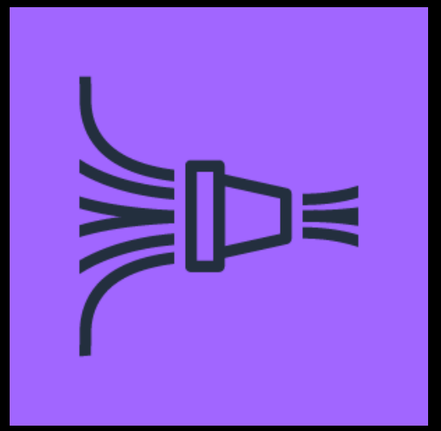
Configurable logging



Amazon S3



Amazon CloudWatch Logs



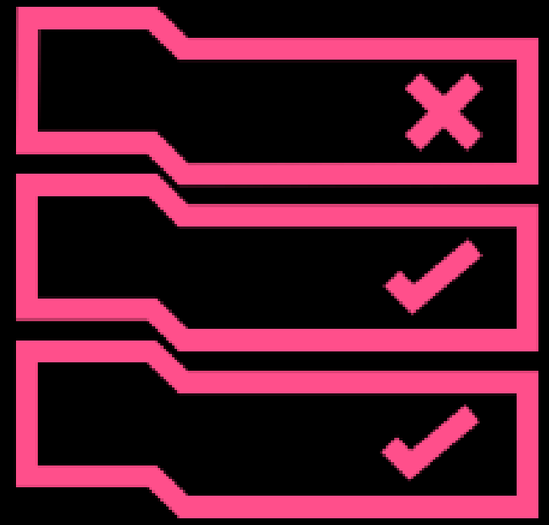
Amazon Kinesis Data Firehose

Defend against common network threats

Defend against common network threats with intrusion-prevention capabilities

Inspect traffic behavior in addition to source and destination

Detect protocol anomalies



Integrated with your existing ecosystem

Rule policy language that is compatible with familiar open source rule format

Integration with 14 security partners



Integrated Security Partners

AWS NETWORK FIREWALL

Security Monitoring

- sumo logic
- splunk>
- IBM Security
- DATADOG

Threat Intelligence

- FORTINET
- TREND MICRO
- CROWDSTRIKE

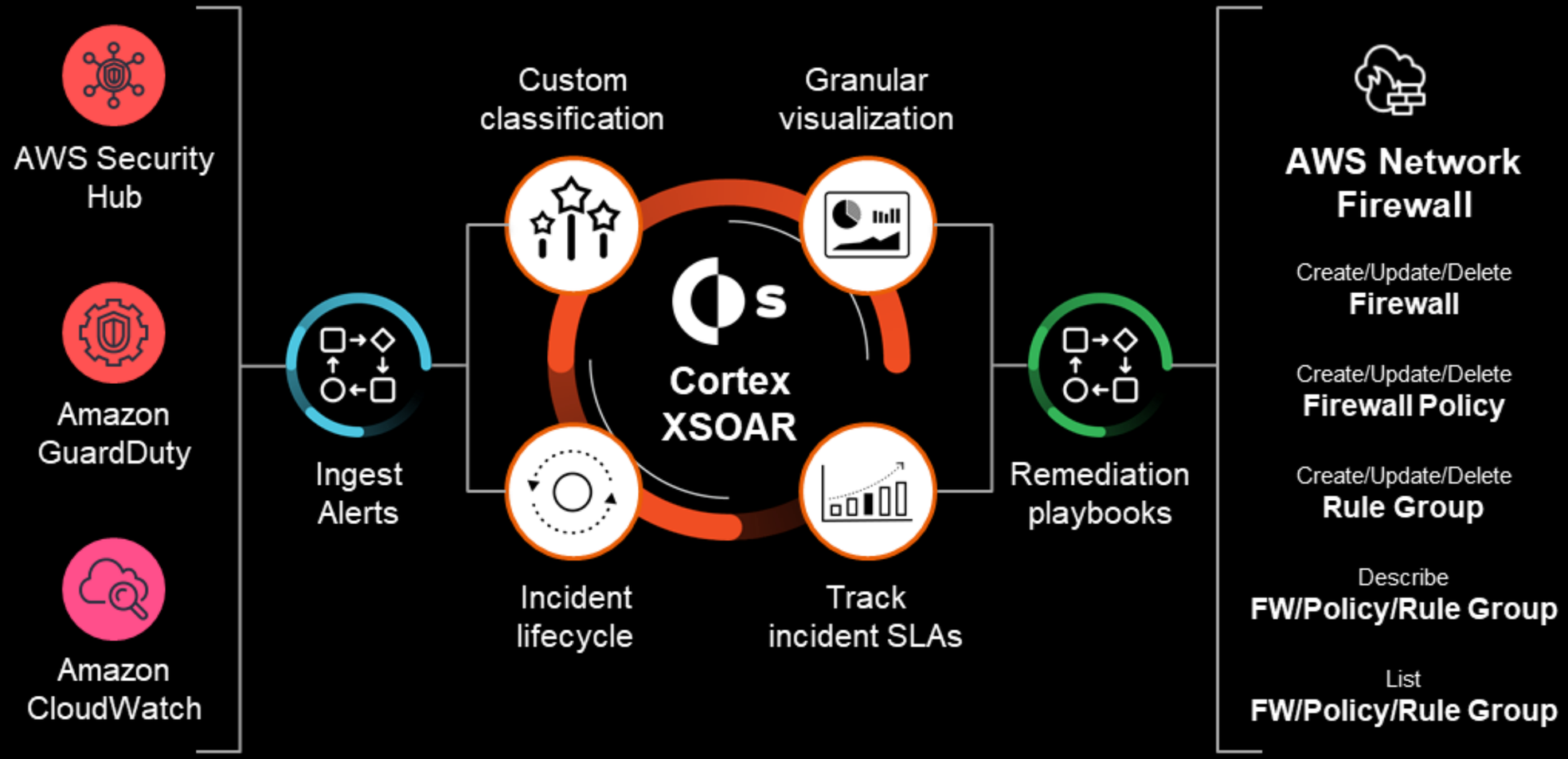
Policy Management

- Check Point SOFTWARE TECHNOLOGIES LTD
- HashiCorp Terraform
- CORTEX BY PALO ALTO NETWORKS
- tufin

Managed Security

- accenture
- ALERT LOGIC
- rackspace technology
- IBM Security

paloalto NETWORKS Cortex XSOAR integration with Network Firewall



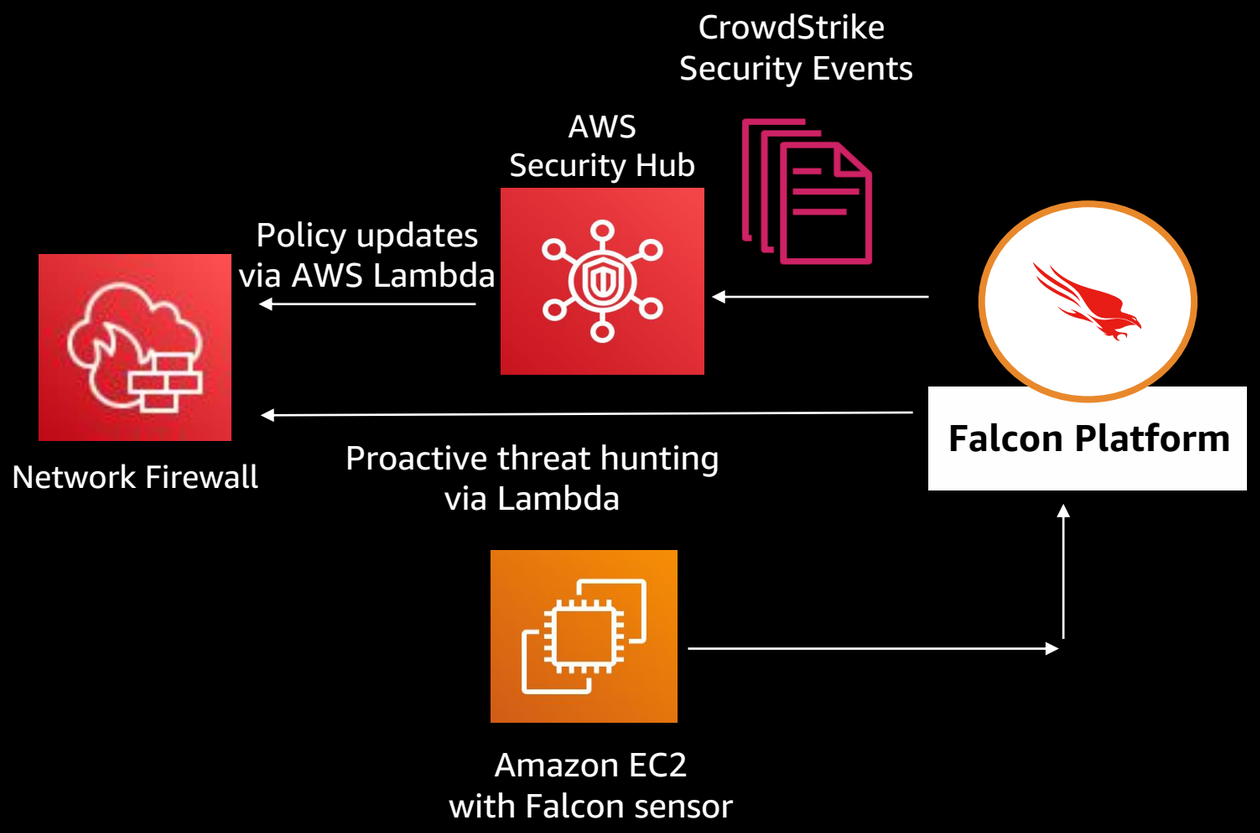
CrowdStrike integration

Leverage CrowdStrike threat detection

Proactive threat hunting

Dynamic policy creation

Streamlined incident response



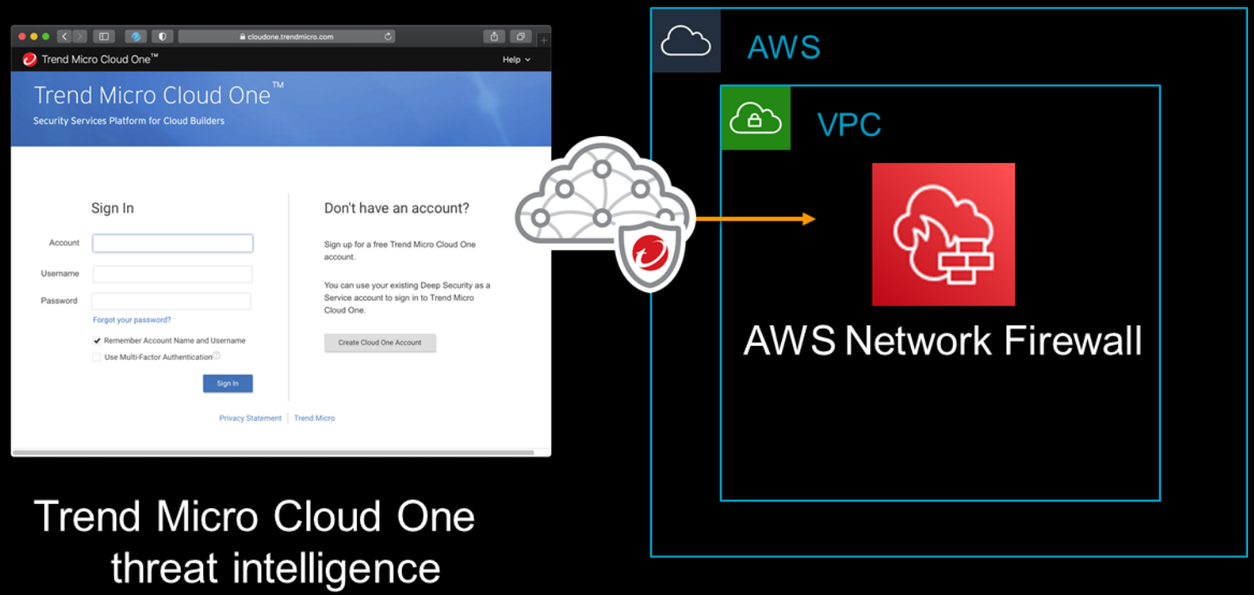
TREND MICRO | Cloud One™ integration

Detect and block unwanted traffic at scale with no management overhead

Easy rule deployment via Trend Micro Cloud One console

Automatic rule updates as new threat intelligence is available

Select Trend Micro Cloud One threat intelligence rules available at no additional cost



Trend Micro Cloud One threat intelligence

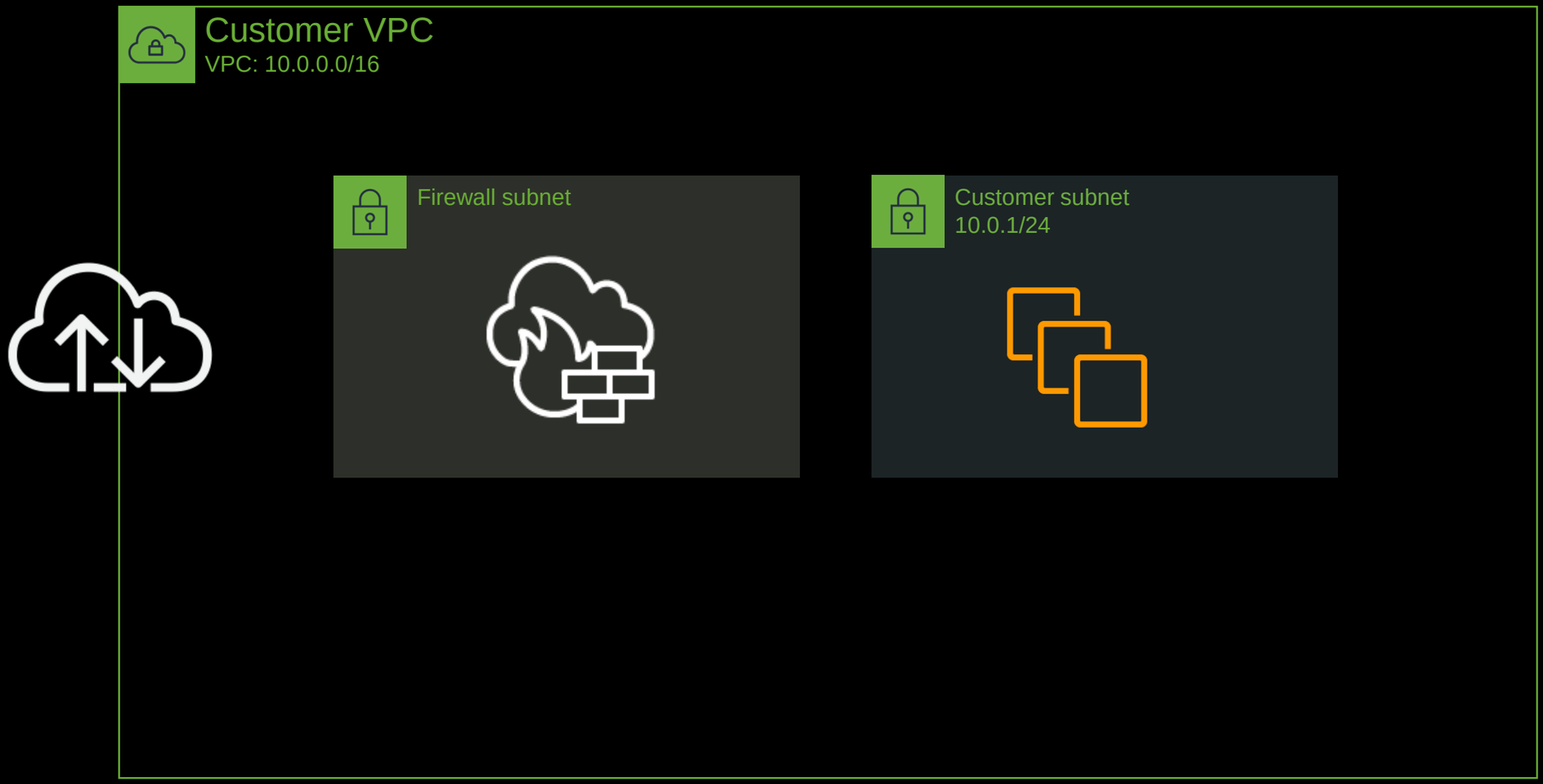
How do I get started with Network Firewall?



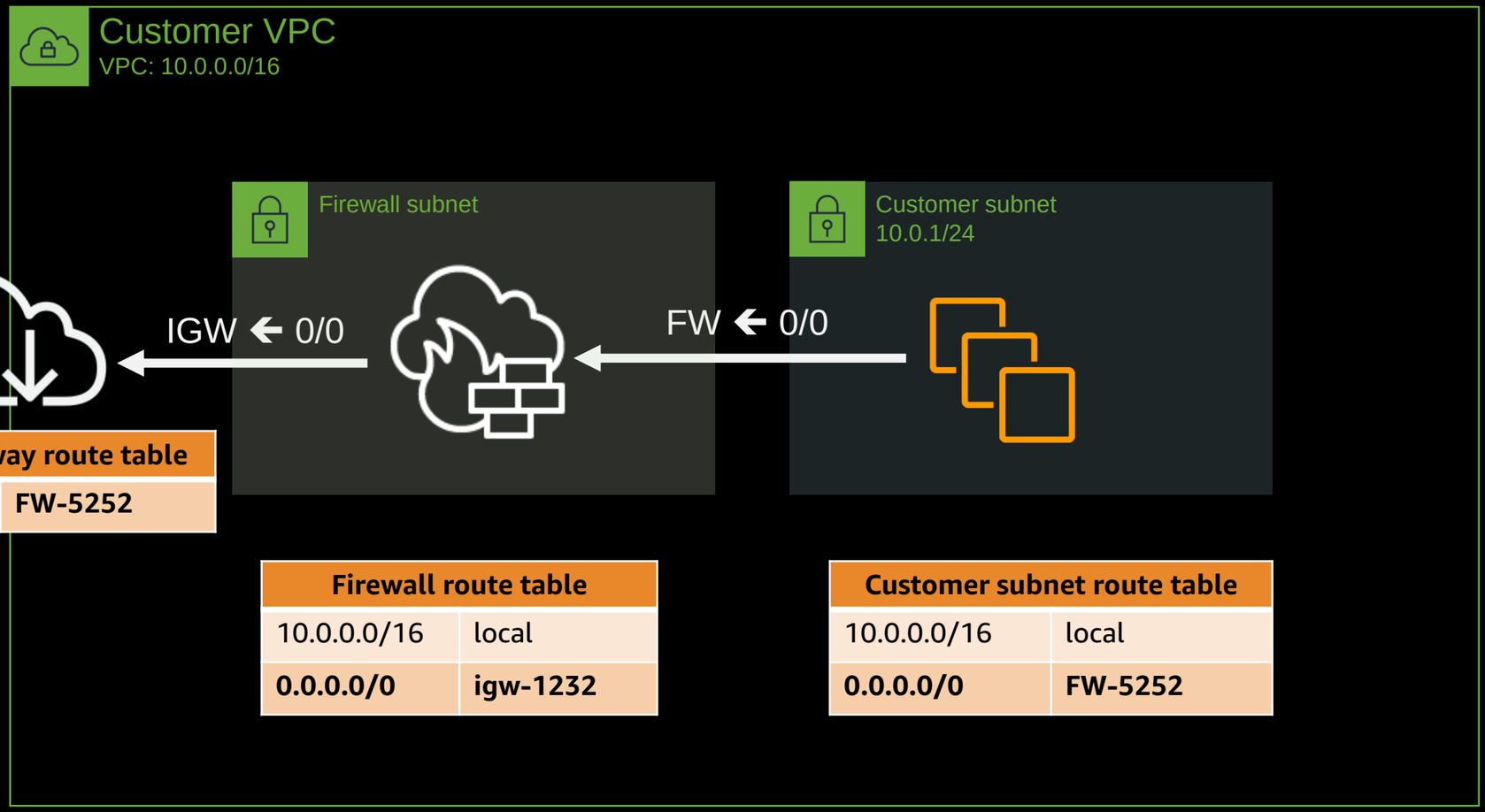
AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step 1: Set up your firewall subnet



Step 2: Configure Amazon VPC route tables



Internet gateway route table	
10.0.0.0/16	**FW-5252**

Firewall route table	
10.0.0.0/16	local
0.0.0.0/0	**igw-1232**

Customer subnet route table	
10.0.0.0/16	local
0.0.0.0/0	**FW-5252**

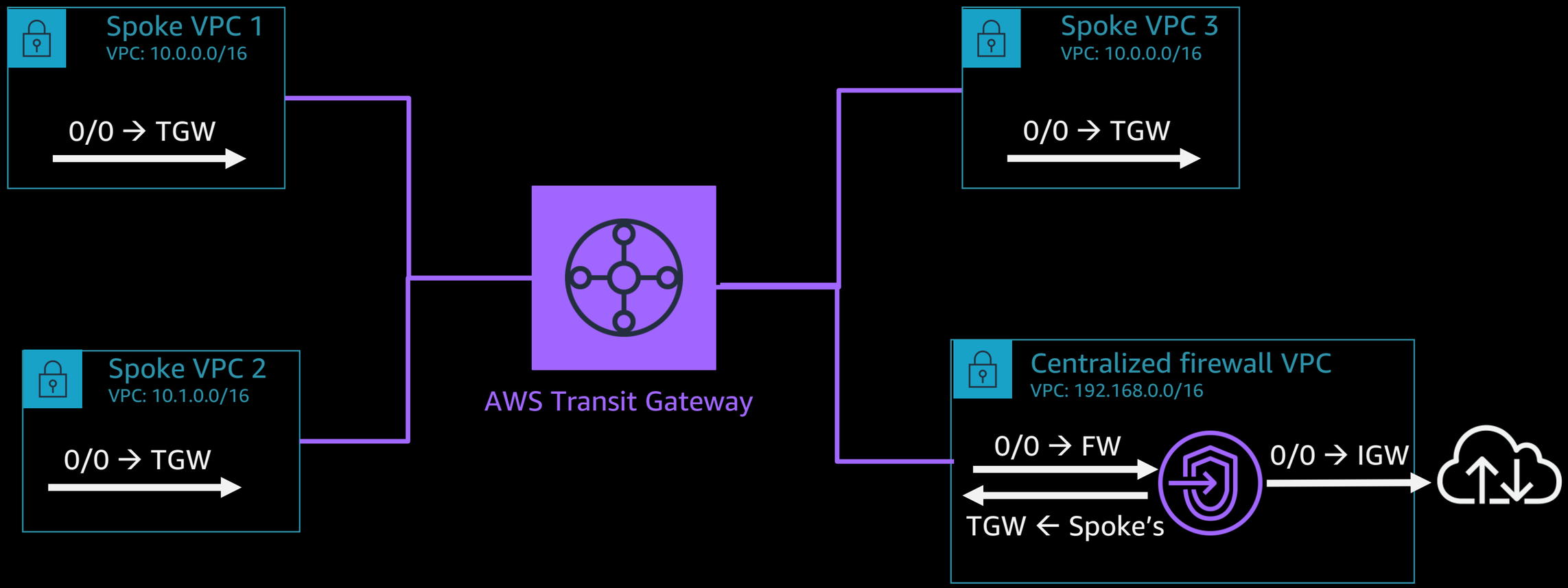
For central deployments with AWS Transit Gateway



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network Firewall & AWS Transit Gateway



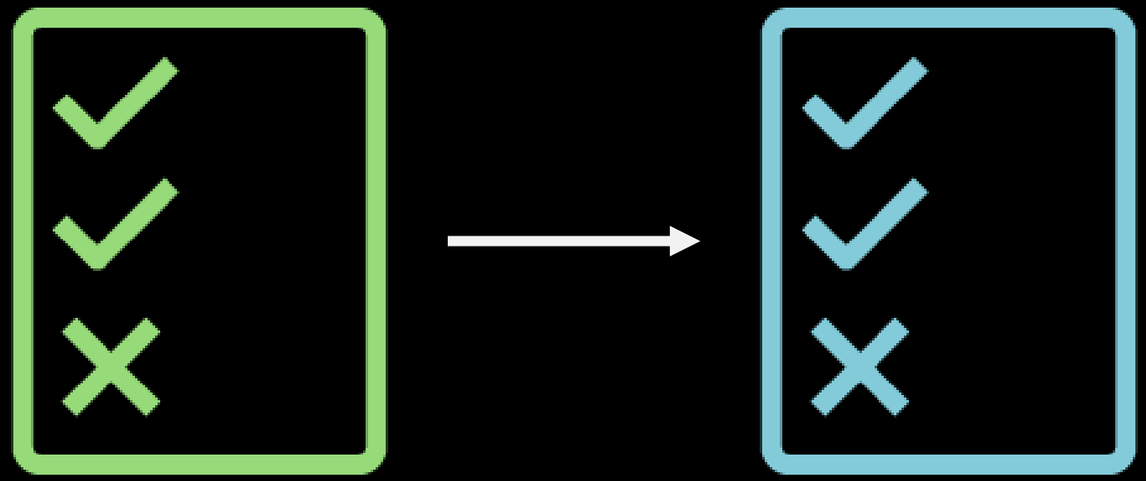
Step 3: Configure your policies

Each firewall has one policy with multiple rule groups

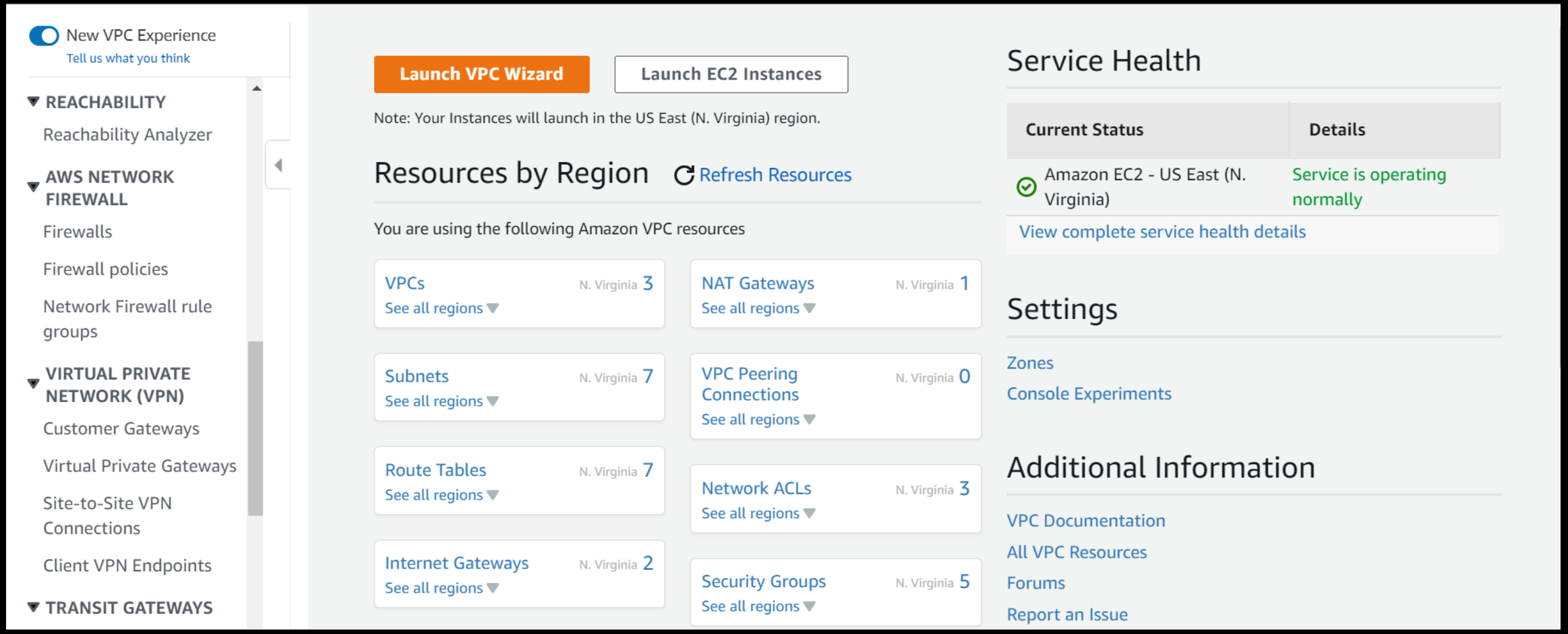
A rule group can be either stateless or stateful

A policy can contain up to 10 rule groups

You'll need to configure a default action



Visit the Amazon VPC console



Region availability and pricing



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Regional availability

- US-East-1 (N. Virginia)
- US-West-2 (Oregon)
- EU-West-1 (Dublin)



Pricing

- $0.395 per endpoint hour
- $0.065 per GB processed
- Use one hour and one GB of NAT Gateway at no additional cost for every hour and GB charged for Network Firewall endpoints



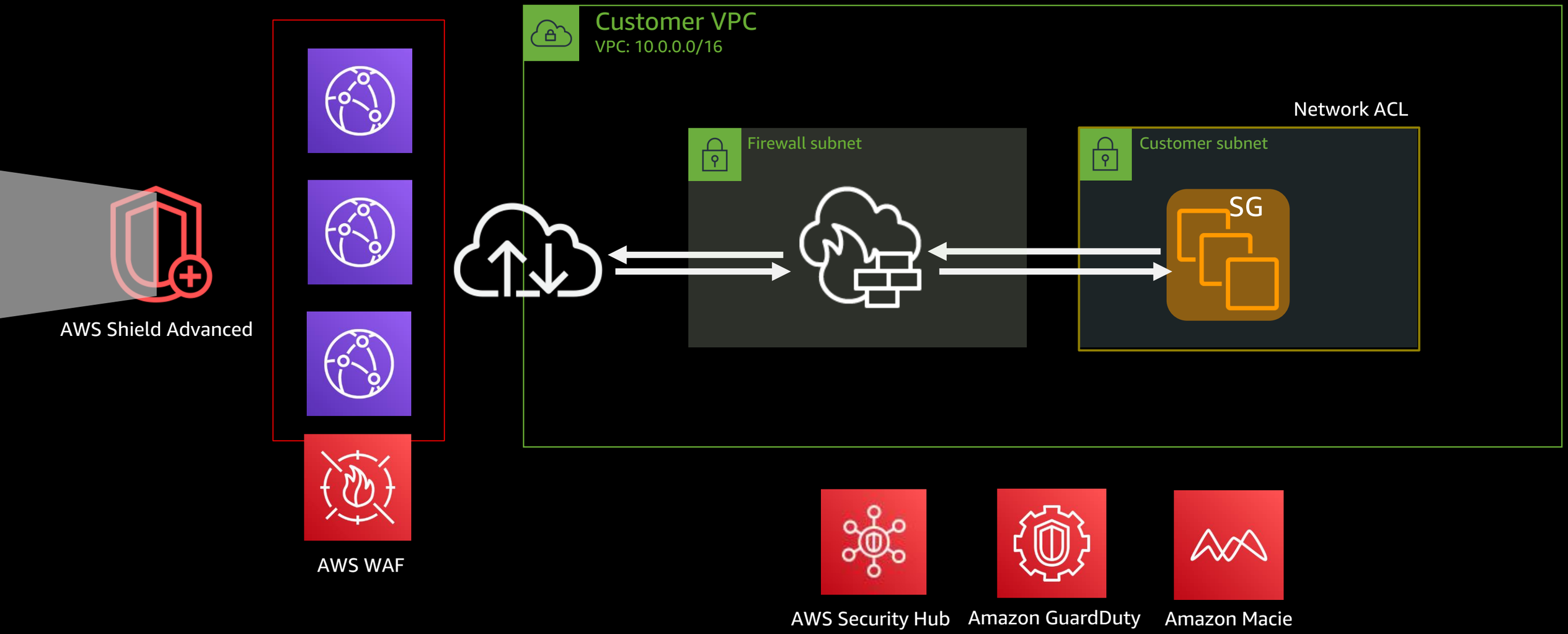
Defense in depth with Network Firewall



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Defense in depth



Recap

Highly available, scalable firewall service

Flexible deployment options

Customizable rules for network segmentation, event logging, and intrusion detection and prevention

Integrated with your existing security ecosystem

No upfront costs, only pay for what you use



Thank you!



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.