# Securing the Cloud

## Identity Management and Network Security in the Cloud


Mark Ryland
Chief Solutions Architect
AWS Public Sector team

Khawaja Shams
Cloud Architect
Jet Propulsion Labs / NASA


QCon – New York 2012

# Agenda

- Identity & Access Management
  - Core concepts: user, groups, roles, policies
  - Demos: multi-factor authentication; S3 access control policies; introducing roles for Instances
- EC2 networking
  - EC2 classic networking
  - Introducing Virtual Private Cloud
  - Demos: network control via security groups; public and private connectivity to VPC; forensics in the cloud



# Identity & Access Management

- Identities & access control for AWS management plane
  - AWS APIs and console
  - Not for operating system or application level
  - Partners like Xceedium provide integrations across levels
- Principals: users, groups, and roles
- Actions: service-specific verbs
- Resources: very rich set of AWS objects
  - Addressable via Amazon Resource Names (ARNs)
- Single policy language applies everywhere

# Example Policy

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:ListAllMyBuckets",
      "Resource": "arn:aws:s3:::*“,
      "Condition": {}  //e.g., time, transport, source ARN, source IP, UserAgent, Referrer
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::qcon-nyc",
      "Resource": "arn:aws:s3:::qcon-nyc/*"
    }
  ]
}
```



# Model: Principals and Resources

- Single policy language used to express permissions on both principals and resources (actions on either/both)
- Some services support only actions/verbs; others provide resource-level permissioning
  - More resource-level will be added over time
- Policies are AND'd together; first "deny" ends processing

# Model

**User-Based Permissions**

**Larry**

Can Read, Write, List

On Resource X

**Sam**

Can Read

On Resources Y, Z

**Managers**

Can List

On Resources X, Y, Z

**Admins**

Can do All Actions

On All Resources

**Resource-Based Permissions**

**Resource X**

| | |
|---|---|
| Bob: | Can Read, Write, List |
| Jim: | Can Read, List |
| Sara: | Can List |
| Doug: | Can Read, Write, List |
| etc... | |

**Resource Y**

| | |
|---|---|
| Bob: | Can Read, Write, List |
| Larry: | Can Read |
| Sam: | Can Write, List |
| etc... | |

- For summary of service-level support, see http://docs.amazonwebservices.com/IAM/latest/UserGuide/Using_SpecificProducts.html

# IAM Demos

- Create user, assign to group
- Add virtual MFA for interactive sessions (and some APIs)
- Create S3-related policy
- Login as new user, try S3 operations
- Start instance in role, view identity metadata



# Roles for Instances

- Example of using new STS model of auth in a REST call:

  https://sdb.amazonaws.com/
  ?Action=GetAttributes
  &AWSAccessKeyId=*Access Key ID provided by AWS Security Token Service*
  &DomainName=MyDomain
  &ItemName=MyItem
  &SignatureVersion=2
  &SignatureMethod=HmacSHA256
  &Timestamp=2010-01-25T15%3A03%3A07-07%3A00 &Version=2009-04-15
  &Signature=*Signature calculated using the SecretKeyId provided by AWS STS*
  &SecurityToken=*Security Token Value*

- AWS SDKs to the work for you

# Agenda

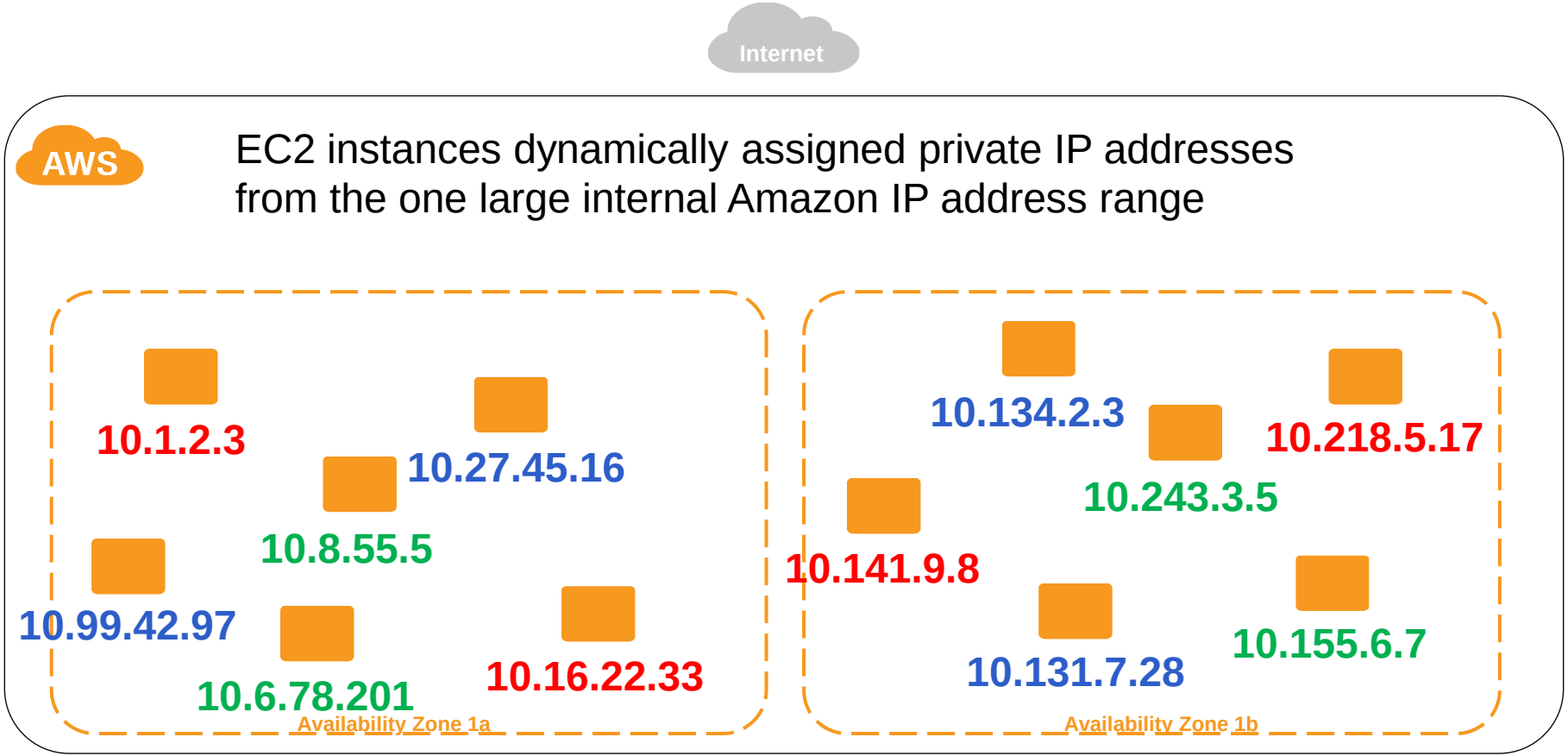
- Identity & Access Management
  - Core concepts: user, groups, roles, policies
  - Multi-factor authentication
  - Roles for Instances

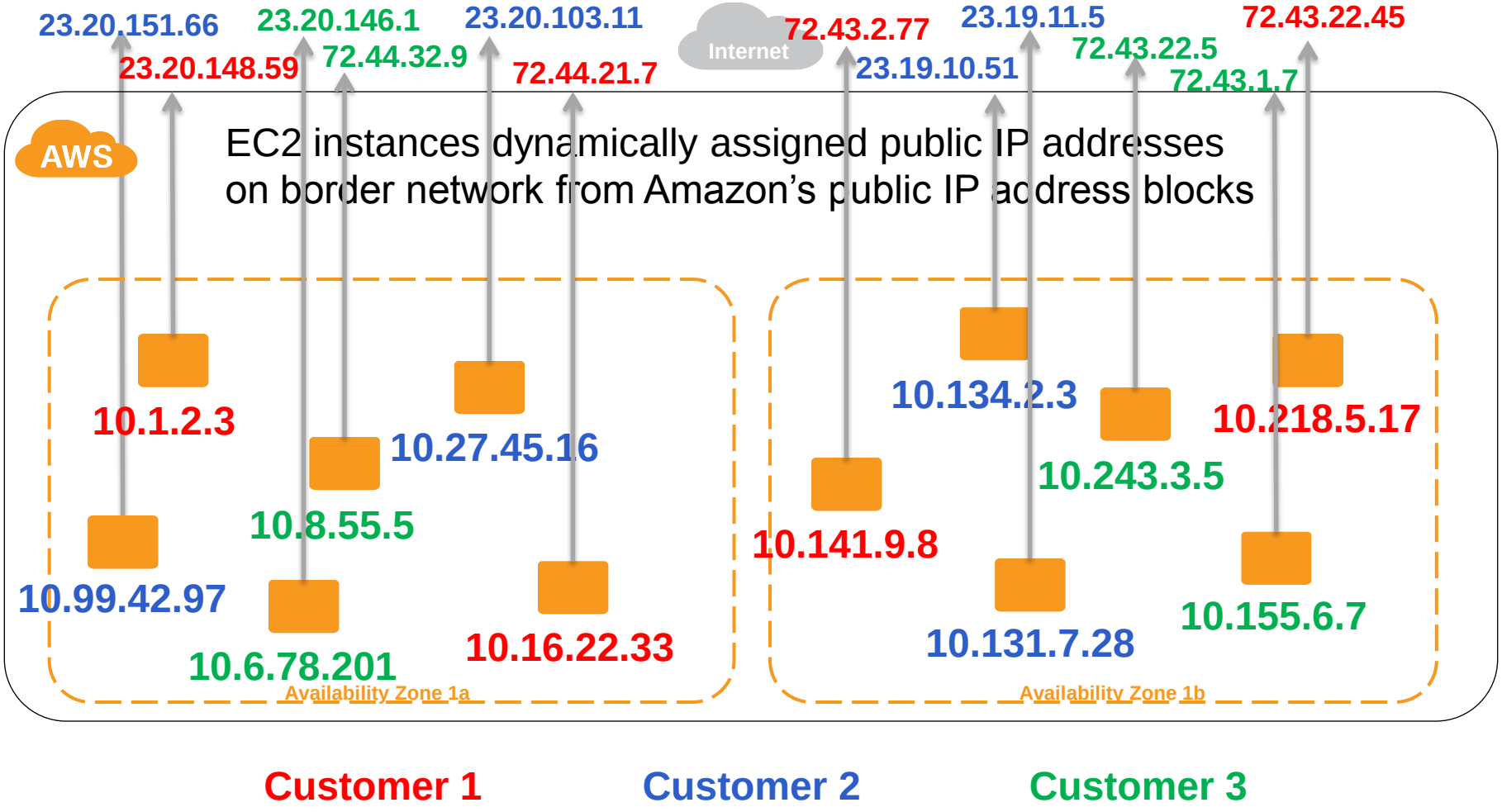
- EC2 networking
  - EC2 classic networking
  - The power of security groups
  - Additional capabilities of Virtual Private Cloud



# EC2 Standard Networking

- Distinct private/internal and public/external IPs
  - True 1:1 NAT (no port translation)
  - “Split-brained” DNS
  - Addresses change upon reboot
- Security groups control ingress
- Elastic IPs: fixed public IPs


Internet
AWS
EC2 instances dynamically assigned private IP addresses
from the one large internal Amazon IP address range
10.1.2.3
10.27.45.16
10.8.55.5
10.99.42.97
10.6.78.201
10.16.22.33
Availability Zone 1a
10.134.2.3
10.218.5.17
10.243.3.5
10.141.9.8
10.131.7.28
10.155.6.7
Availability Zone 1b
Customer 1
Customer 2
Customer 3


23.20.151.66
23.20.148.59
23.20.146.1
72.44.32.9
23.20.103.11
72.44.21.7
Internet
72.43.2.77
23.19.10.51
23.19.11.5
72.43.22.5
72.43.1.7
72.43.22.45
AWS
EC2 instances dynamically assigned public IP addresses
on border network from Amazon's public IP address blocks
10.1.2.3
10.27.45.16
10.8.55.5
10.99.42.97
10.6.78.201
10.16.22.33
Availability Zone 1a
10.134.2.3
10.218.5.17
10.243.3.5
10.141.9.8
10.131.7.28
10.155.6.7
Availability Zone 1b
Customer 1
Customer 2
Customer 3

# Introducing AWS Virtual Private Cloud

- User-defined virtual IP networking for EC2
- Private or mixed private/public addressing and ingress/egress
- Re-use of proven and well-understood networking concepts and technologies

# VPC Capabilities in a Nutshell

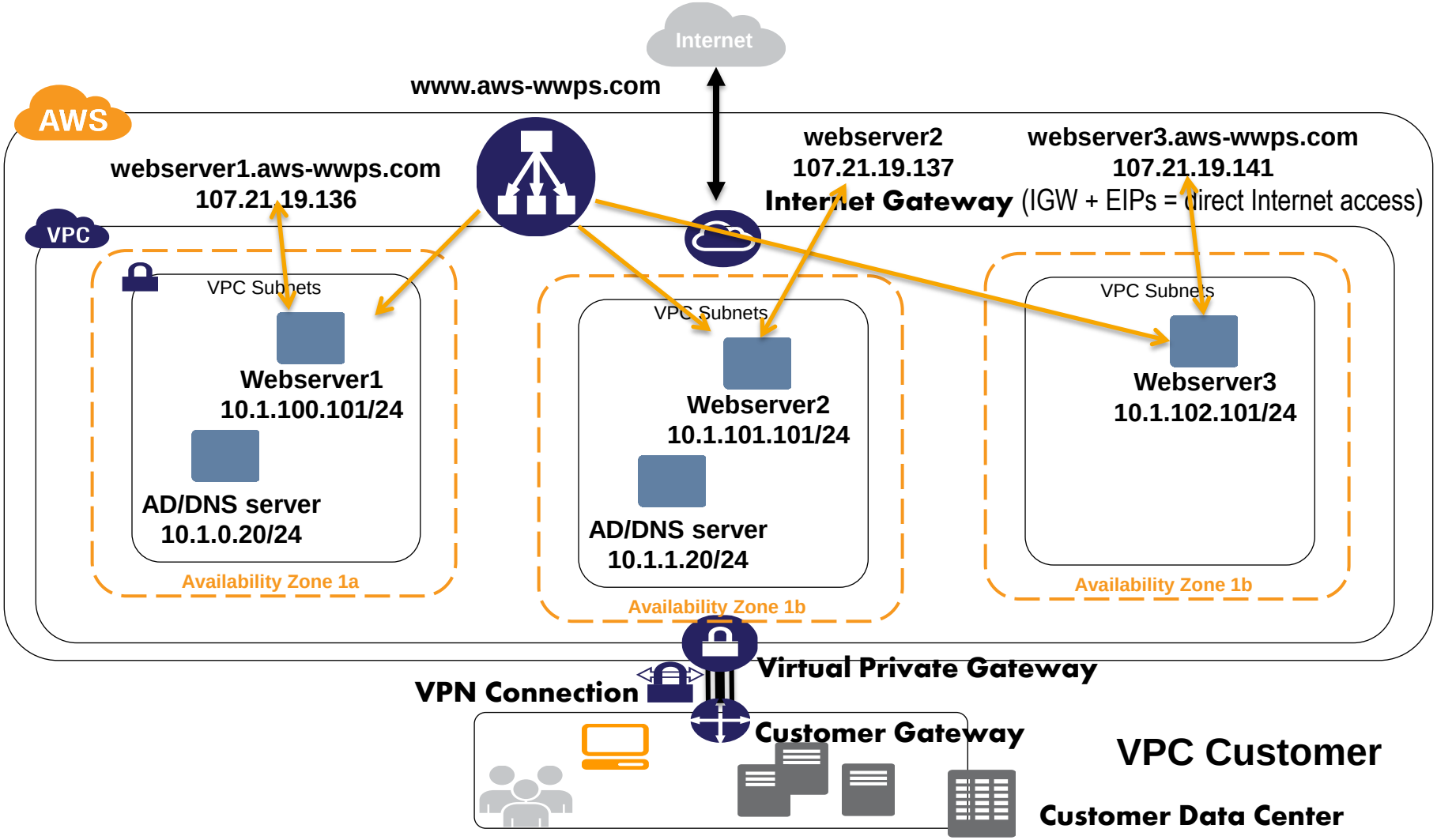
- User-defined address space up to /16
  - *Completely* disjoint from all other tenant networks
- Up to 20* user-defined subnets up to /16
- User-defined:
  - Virtual routing, DHCP servers, and NAT instances
  - Internet gateways, private, customer gateways, and VPN tunnels
- Private IPs are stable once assigned
- *Internet access is not automatic*
- Elastic Network Interfaces (virtual NICs)

# Enhanced Security Capabilities

- Network topology, routing, and subnet ACLs
- Security group enhancements
  - Egress control; dynamic (re)assignment; multiple SGs; richer protocol support
- Multiple network interfaces per instance
- Completely private networking via VPN
- Support for dedicated instances

# Common Use Cases

- Mixing public and private resources
  - *E.g.*, web-facing hosts with DMZ subnets, control plane subnets
- Workloads that expect fixed IPs and/or multiple NICs
- AWS cloud as private extension of on-premises network
  - Accessible from on-premises hosts
  - No change to addressing
  - No change to Internet threat/risk posture

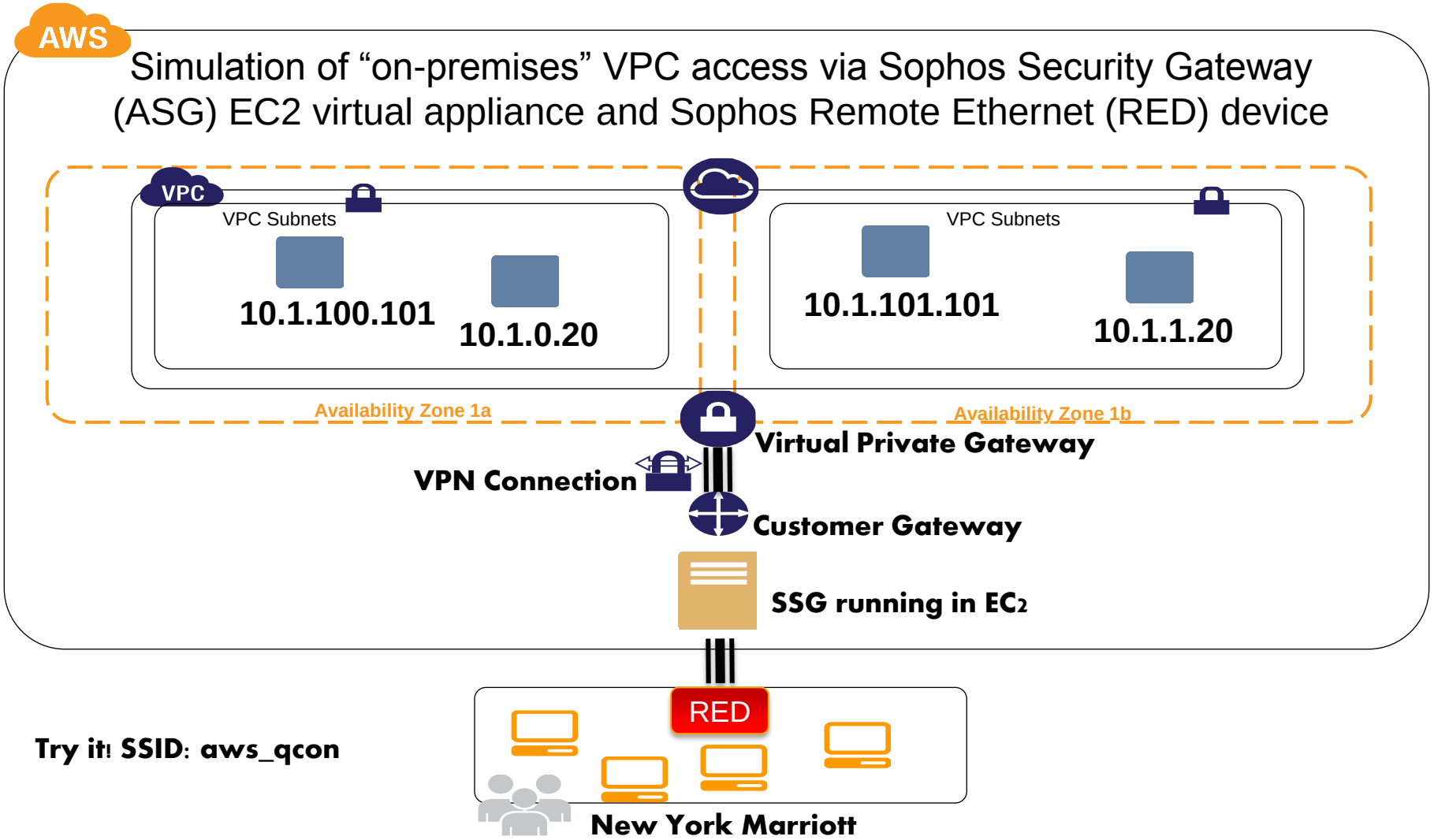

Internet
www.aws-wwps.com
AWS
webserver1.aws-wwps.com
107.21.19.136
webserver2
107.21.19.137
webserver3.aws-wwps.com
107.21.19.141
Internet Gateway (IGW + EIPs = direct Internet access)
VPC
VPC Subnets
Webserver1
10.1.100.101/24
AD/DNS server
10.1.0.20/24
Availability Zone 1a
VPC Subnets
Webserver2
10.1.101.101/24
AD/DNS server
10.1.1.20/24
Availability Zone 1b
VPC Subnets
Webserver3
10.1.102.101/24
Availability Zone 1b
Virtual Private Gateway
VPN Connection
Customer Gateway
VPC Customer
Customer Data Center

# Rich Capabilities in VPC

- ELB, AutoScaling, CloudWatch, alarms
- Relational Database Service (MySQL engine, for now)
- Elastic MapReduce
- CloudFormation
- And many others, with more to come…
- “Blackbox” services with public endpoints reachable via Internet gateway (or VPN)

# Networking Demos

- Ping instances from inside and outside VPC
- Change security group content and examine behavior
  - Ping
  - Egress control (web browser)
- Drop public IPs, switch to accessing VPC from (virtual) “on premises” network


AWS
Simulation of “on-premises” VPC access via Sophos Security Gateway (ASG) EC2 virtual appliance and Sophos Remote Ethernet (RED) device
VPC
VPC Subnets
10.1.100.101
10.1.0.20
VPC Subnets
10.1.101.101
10.1.1.20
Availability Zone 1a
Availability Zone 1b
Virtual Private Gateway
VPN Connection
Customer Gateway
SSG running in EC2
RED
Try it! SSID: aws_qcon
New York Marriott

# Securing the Cloud

Questions & Answers

QCon – New York 2012