AWS Networking Fundamentals

Tom Adamski
Specialist Solutions Architect, AWS
Traditional Network

![Diagram of Traditional Network with VPNs and WAN connections to applications.]
AWS Network

- **VPN**
- **WAN**
- **Fiber** (AWS Direct Connect)
- **Applications**
  - (VPC Peering)

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
What is an Amazon Virtual Private Cloud (VPC)?

“A virtual network that closely resembles a traditional network that you'd operate in your own data center”
Creating an Internet-connected VPC: Steps

Choosing an address range

Create subnets in Availability Zones

Creating a route to the Internet

Authorizing traffic to/from the VPC
Choosing an IP address range
CIDR notation review

CIDR range example:

172.31.0.0/16

1010 1100 0001 1111 0000 0000 0000 0000
Choosing an IP address range for your VPC

Avoid ranges that overlap with other networks to which you might connect.

172.31.0.0/16

Recommended: RFC1918 range

Recommended: /16 (65,536 addresses)
IPv6 in Amazon VPC – Dual-stack

172.31.0.0/16
2001:db8:1234:1a00::/56

Amazon Global Unicast Addresses (GUA) – Internet Routable
Associate an /56 IPv6 CIDR (Automatically allocated)
Subnets
VPC subnets and Availability Zones

172.31.0.0/16

- eu-west-1a
  - 172.31.0.0/24
  - VPC subnet
  - Availability Zone

- eu-west-1b
  - 172.31.1.0/24
  - VPC subnet
  - Availability Zone

- eu-west-1c
  - 172.31.2.0/24
  - VPC subnet
  - Availability Zone
Expand your existing Amazon VPC
Initial VPC CIDR: 172.31.0.0/16

VPC CIDR 172.31.0.0/16

- Availability Zone A
  - Instance A 172.31.1.11/24
  - Subnet

- Availability Zone B
  - Instance B 172.31.2.22/24
  - Subnet
  - Instance C 172.31.3.33/24
  - Subnet
  - Instance D 172.31.4.44/24
  - Subnet
Initial VPC CIDR: 172.31.0.0/16
Initial VPC CIDR: 172.31.0.0/16

Additional VPC CIDR: 172.21.0.0/16
VPC subnet recommendations

- /16 VPC (65,536 addresses)
- Expand your VPC when necessary
- At least /24 subnets (251 addresses)
- Use multiple Availability Zones per VPC through multiple subnets
Route to the Internet
Routing in your VPC

• **Route tables** contain rules for which packets go where
• Your VPC has a *default* (main) route table
• But, you can assign **different route tables** to different subnets
rtb-04304e61

**Routes**

<table>
<thead>
<tr>
<th>Destination</th>
<th>Target</th>
<th>Status</th>
<th>Propagated</th>
<th>Remove</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.31.0.0/16</td>
<td>local</td>
<td>Active</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
Traffic destined for my VPC stays in my VPC.
Internet gateway

Send packets here if you want them to reach the Internet
Everything that isn’t destined for the VPC: send to the Internet

<table>
<thead>
<tr>
<th>Destination</th>
<th>Local</th>
<th>IGW</th>
<th>Route Status</th>
<th>Egress Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.31.0.0/16</td>
<td>local</td>
<td></td>
<td>Active</td>
<td>No</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td></td>
<td>igw-3376c756</td>
<td>Active</td>
<td>No</td>
</tr>
<tr>
<td>172.31.0.0/16</td>
<td>local</td>
<td></td>
<td>Active</td>
<td>No</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td></td>
<td>igw-3376c756</td>
<td>Active</td>
<td>No</td>
</tr>
</tbody>
</table>
Network security in your VPC:
Security groups
Security groups follow application structure

Allow web traffic on 0.0.0.0/0

“MyWebServers” Security Group

Allow only “MyWebServers”

“MyBackends” Security Group
Security groups example: Web servers

- **Allow all HTTP traffic**

  - Rule descriptions:
    - **HTTP**
      - **Protocol**: TCP
      - **Port Range**: 80
      - **Source**: 0.0.0.0/0
      - **Description**: Allow all HTTP traffic
    - **HTTP**
      - **Protocol**: TCP
      - **Port Range**: 80
      - **Source**: ::/0
      - **Description**: Allow all HTTP traffic
Security groups example: Backends

Allow application traffic from web servers only
AWS Network - Progress

- VPC Peering
- AWS Direct Connect
- Applications
Beyond Internet connectivity

- VPC Subnet
  - Restricting Internet access

- Connecting to other VPCs

- Connecting to your corporate network
Restricting Internet access:
Routing by subnet
Routing by subnet

- **Public subnet**
  - Has route to Internet

- **Private subnet**
  - Has **no** route to Internet
Outbound-only internet access: NAT gateway

<table>
<thead>
<tr>
<th>Destination</th>
<th>Target</th>
<th>Status</th>
<th>Propagated</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.31.0.0/16</td>
<td>local</td>
<td>Active</td>
<td>No</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>nat-0ad85536b976c2ad2</td>
<td>Active</td>
<td>No</td>
</tr>
</tbody>
</table>

Public IP: 54.161.0.39

Private subnet

NAT gateway

Public subnet
Inter-VPC connectivity: VPC peering
Example VPC peering use:
Shared services VPC

- Common/core services
  - Authentication/directory
  - Monitoring
  - Logging
  - Remote administration
  - Scanning
Establish a VPC peering: Initiate request

Step 1
Initiate peering request

172.31.0.0/16

10.55.0.0/16
Establish a VPC peering: Accept request

Step 1: Initiate peering request

Step 2: Accept peering request

172.31.0.0/16

10.55.0.0/16
Establish a VPC peering: Create a route

Step 1: Initiate peering request

Step 2: Accept peering request

Traffic destined for the peered VPC should go to the peering

<table>
<thead>
<tr>
<th>Destination</th>
<th>Target</th>
<th>Status</th>
<th>Propagated</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.31.0.0/16</td>
<td>local</td>
<td>Active</td>
<td>No</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>igw-3376c756</td>
<td>Active</td>
<td>No</td>
</tr>
<tr>
<td>10.55.0.0/16</td>
<td>pcx-63ea270a</td>
<td>Active</td>
<td>No</td>
</tr>
</tbody>
</table>
Security groups across peered VPCs

VPC Peering

ALLOW

Orange Security Group

Blue Security Group

172.31.0.0/16

10.55.0.0/16
Inter-Region VPC Peering

VPC A

VPC B

eu-west-1 (Ireland)

us-east-1 (N.Virginia)
Some notes…

Inter-Region VPC Peering encrypts with no single point of failure or bandwidth bottleneck

Traffic using Inter-Region VPC Peering always stays on the global AWS backbone
AWS Network - Progress

Applications

(VPC Peering)

Applications
Connecting to on-premises networks: AWS Virtual Private Network and AWS Direct Connect
Extend an on-premises network into your VPC

VPC

VPN

AWS Direct Connect
AWS VPN basics

Traffic destined for the VPN/Direct Connect via the VGW
AWS Direct Connect Gateway

EU-WEST-1

VPC 172.31.0.0/16

Private Virtual Interface

“Attachment”

VGW

“Association”

Direct Connect Gateway

Direct Connect Location (London)

192.168.0.0/16
AWS Direct Connect Gateway

EU-WEST-1

VPC
172.31.0.0/16

VGW

192.168.0.0/16

Direct Connect Location (London)

Direct Connect Gateway

VGW
"Association"

Private Virtual Interface
"Attachment"
AWS Direct Connect Gateway

### EU-WEST-1
- **VPC**: 172.31.0.0/16
- **VGW**: "Association"

### EU-CENTRAL-1
- **VPC**: 172.16.0.0/16
- **VGW**: "Association"

### Direct Connect Gateway
- **Virtual Interface "Attachment"**
- **Direct Connect Location**
  - (London)
  - (Frankfurt)
Direct Connect Gateway—traffic flows

VGW "Association"

Virtual Interface "Attachment"

Direct Connect Location
AWS VPN and AWS Direct Connect

• Both allow **secure connections** between your network and your VPC

• **VPN** is a pair of IPSec tunnels over the Internet

• **AWS Direct Connect** is a dedicated line with lower per-GB data transfer rates

• For **highest availability**: Use both
AWS Network - Progress

- VPN (VPC Peering)
- WAN (AWS Direct Connect)
- Applications

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
AWS Services in your VPC
Example: Amazon RDS Database in your VPC
Example: Application Load Balancer in your VPC
AWS Services outside your VPC
Endpoints for AWS Services
Amazon S3 and your VPC

Your applications

172.31.1.0/24
AZ A

172.31.2.0/24
AZ B

172.31.0.0/16

Your data

S3 bucket

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Gateway VPC Endpoints

A VPC endpoint allows you to securely connect your VPC to another service. An interface endpoint is powered by PrivateLink, and uses an elastic network interface (ENI) as an entry point for traffic destined to the service. A gateway endpoint serves as a target for a route in your route table for traffic destined for the service.

Service Name

- **com.amazonaws.eu-west-1.dynamodb**
- **com.amazonaws.eu-west-1.ec2**
- **com.amazonaws.eu-west-1.ec2messages**
- **com.amazonaws.eu-west-1.elasticloadbalancing**
- **com.amazonaws.eu-west-1.kinesis-streams**
- **com.amazonaws.eu-west-1.s3**
- **com.amazonaws.eu-west-1.servicecatalog**
- **com.amazonaws.eu-west-1.ssm**

Select "com.amazonaws.eu-west-1.s3" as a Gateway service.
VPC Endpoints: Amazon S3 and DynamoDB

<table>
<thead>
<tr>
<th>Destination</th>
<th>Target</th>
<th>Status</th>
<th>Propagated</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.31.0.0/16</td>
<td>local</td>
<td>Active</td>
<td>No</td>
</tr>
<tr>
<td>pl-68a54001 (com.amazonaws.us-west-2.s3)</td>
<td>vpce-3a14fc53</td>
<td>Active</td>
<td>No</td>
</tr>
</tbody>
</table>

Route S3-bound traffic to the VPC endpoint

S3 bucket
IAM policy for VPC Endpoints

IAM policy at VPC endpoint:
restrict actions of VPC in Amazon S3 or Amazon DynamoDB

IAM policy at S3 bucket:
make accessible from VPC endpoint only
Interface VPC Endpoints

A VPC endpoint allows you to securely connect your VPC to another service. An interface endpoint is powered by PrivateLink, and uses an elastic network interface (ENI) as an entry point for traffic destined to the service. A gateway endpoint serves as a target for a route in your route table for traffic destined for the service.

**Service Name**

Select a service

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Owner</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.amazonaws.eu-west-1.dynamodb</td>
<td>amazon</td>
<td>Gateway</td>
</tr>
<tr>
<td>com.amazonaws.eu-west-1.ec2</td>
<td>amazon</td>
<td>Interface</td>
</tr>
<tr>
<td>com.amazonaws.eu-west-1.ec2messages</td>
<td>amazon</td>
<td>Interface</td>
</tr>
<tr>
<td>com.amazonaws.eu-west-1.elasticloadbalancing</td>
<td>amazon</td>
<td>Interface</td>
</tr>
<tr>
<td>com.amazonaws.eu-west-1.kinesis-streams</td>
<td>amazon</td>
<td>Interface</td>
</tr>
<tr>
<td>com.amazonaws.eu-west-1.s3</td>
<td>amazon</td>
<td>Gateway</td>
</tr>
<tr>
<td>com.amazonaws.eu-west-1.servicecatalog</td>
<td>amazon</td>
<td>Interface</td>
</tr>
<tr>
<td>com.amazonaws.eu-west-1.ssm</td>
<td>amazon</td>
<td>Interface</td>
</tr>
</tbody>
</table>

**VPC**

- vpc-28b7004c

* Required

Cancel  Create endpoint
AWS PrivateLink for AWS Services

VPC

172.31.1.0/24
AZ A

172.31.2.0/24
AZ B

Private IP: 172.31.1.6

Private IP: 172.31.2.10

EC2 APIs

ec2.eu-west-1.amazonaws.com
AWS PrivateLink for Customer & Partner Applications

Share services privately and securely between VPCs, AWS accounts, and on-premises networks

- Powered by Network Load Balancer
- Secure endpoint within Client VPC
- Integrated with AWS Marketplace

Available in all public AWS regions, except CN-NORTH-1

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
VPC Flow Logs: VPC traffic metadata in Amazon CloudWatch Logs
VPC Flow Logs

- Visibility into effects of security group rules
- Troubleshooting network connectivity
- Ability to analyze traffic
VPC Flow Logs: Setup

VPC traffic metadata captured in Amazon CloudWatch Logs
VPC Flow Logs data in CloudWatch Logs

<table>
<thead>
<tr>
<th>Time (UTC -04:00)</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>16:46</td>
<td></td>
</tr>
<tr>
<td>16:48</td>
<td></td>
</tr>
<tr>
<td>16:48</td>
<td></td>
</tr>
<tr>
<td>16:48</td>
<td></td>
</tr>
<tr>
<td>16:48</td>
<td></td>
</tr>
<tr>
<td>16:48</td>
<td></td>
</tr>
<tr>
<td>16:48</td>
<td></td>
</tr>
<tr>
<td>16:48</td>
<td></td>
</tr>
<tr>
<td>16:48</td>
<td></td>
</tr>
<tr>
<td>16:48</td>
<td></td>
</tr>
<tr>
<td>16:48:01</td>
<td>2 280328680831 eni-19116c47 109.236.86.32 10.0.0.117 60000 27015 17 1 53 1474750081 1474750133 REJECT OK</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Who’s this?

# dig +short -x 109.236.86.32
internetpolice.co.

REJECT

UDP Port 27015
The VPC Network
VPC Network Security
VPC Connectivity
On-Instance Networking Improvements

- **C1**
  - 1 Gbps

- **CC1**
  - 10 Gbps
  - Enhanced networking
  - 20x PPS
  - <100-µs latency

- **C3**
  - Enhanced networking
  - 20x PPS
  - <100-µs latency

- **C4**
  - EBS optimized by default
  - Elastic Network Adapter
  - 25 Gbps
  - <50-µs latency

- **C5**

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Instance Bandwidth Limits

- 25 Gbps within placement group
- 25 Gbps within region
- 25 Gbps to Amazon S3
- 5 Gbps for other sources
Amazon Time Sync Service

Highly reliable service with a redundant array of satellite and atomic clock sources

Available globally today!
Thank You!

Tom Adamski
Specialist Solutions Architect