Current State of IPv6 Support in aws

UK IPv6 Council
IPv6 Cloud Workshop
September 3, 2019

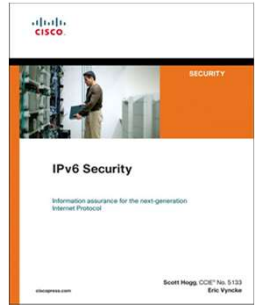
Scott Hogg
CTO & Co-founder, HexaBuild

Agenda

1	AWS IPv6 Features
2	Live Demonstration of AWS Dual-Protocol Environment
3	Summary, Resources, and Q&A

Co-Founder and Chief Technology Officer

Scott Hogg



- Reseller CTO & Executive Experience
- Federal Government Sales and Delivery Expertise
- Experienced Executive Engineering Leadership
- Training and Education Development
- Founder and Chair Emeritus of the RMv6TF
- Published Author on IPv6 Security
- Blogger for NetworkWorld and Infoblox
- Co-host of the IPv6 Buzz Podcast
- Rapidly Deploying IPv6 in AWS, A Cloud Guru

Motivation for IPv6 in the Cloud

If you are deploying cloud systems, you want those applications to be accessible by the broadest Internet population.

A large portion of those people already use IPv6-capable and IPv6-enabled devices on an IPv6 carrier network.

IPv6 can perform better, on average, than IPv4 on the Internet resulting in better end-user-experience.

Your cloud systems are modern, so you want to deploy IPv6 right from the start and not have IPv6 be an afterthought and added later.

If you are using scriptable cloud infrastructure you should deploy both IPv4 and IPv6 at the same time.

AWS IPv6 Features

IPv6 in ELB

IPv6 support for Elastic Load Balancer (ELB) since 2011

- You can create an IPv6 Virtual IP (VIP) listener but the real-servers EC2 instances are IPv4-only (EC2 Classic Only, no VPCs)
- This is a way to present an IPv6 public address to the Internet while keeping your application using IPv4-only

AWS Started to provide more IPv6 support in the Fall of 2016 and ahead-of and during their November 2016 re:Invent conference.

AWS re:Invent

IPv6 in ALB

Application Load Balancer (ALB) has native IPv6 support in a VPC

ALBs automatically receive IPv4 and IPv6 addresses when you select the IP address type = “dualstack”

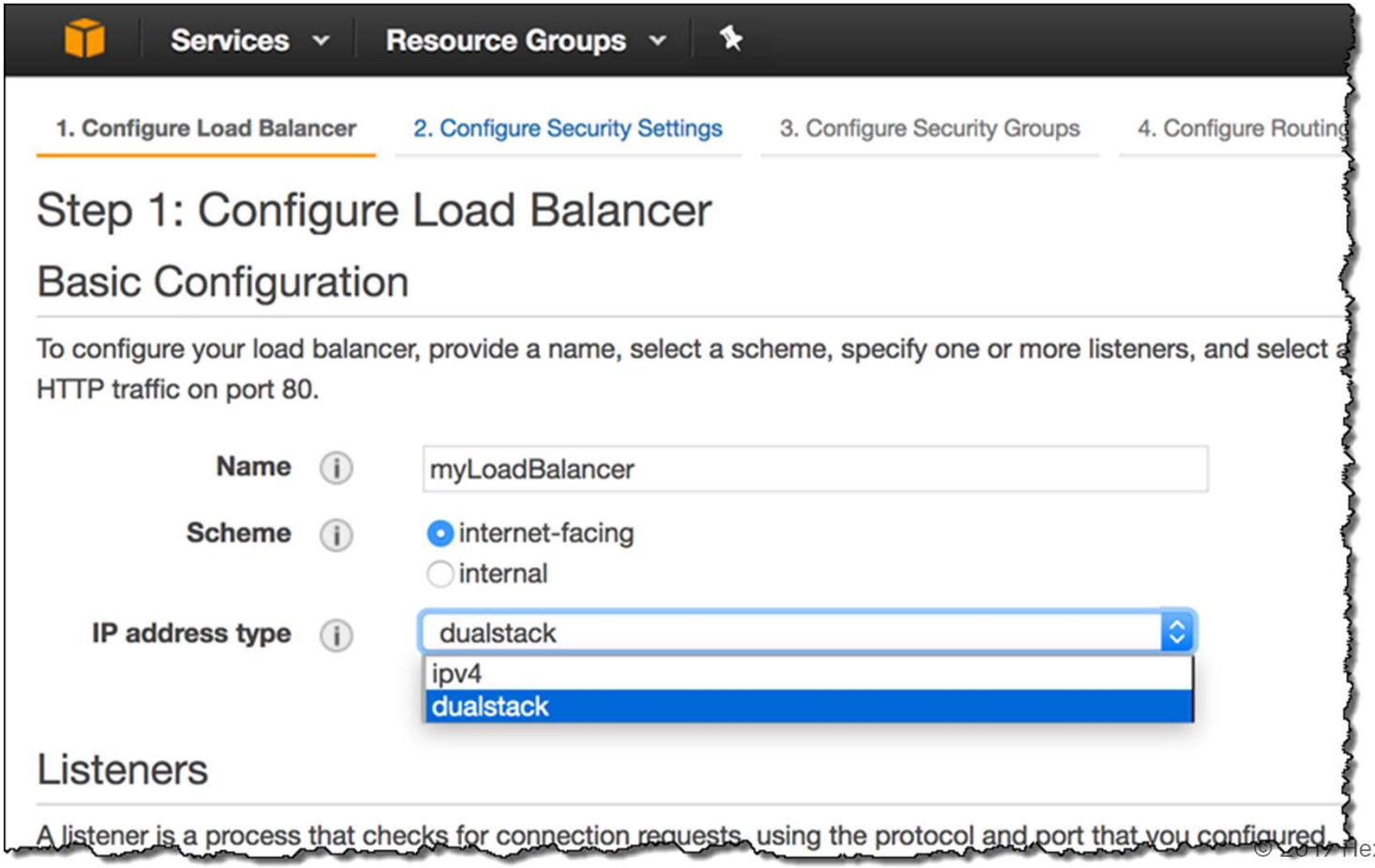
ALB then uses VPCs and subnets, but those subnets need IPv6 or you get the descriptive error

> “Selected subnets must have the CIDR block required by the IP address type.”

Then DNS resolutions for the ALB name will return A and AAAA records

Target Groups are IPv4-only on the back-end

IPv6 in ALB


Services
Resource Groups
1. Configure Load Balancer
2. Configure Security Settings
3. Configure Security Groups
4. Configure Routing
Step 1: Configure Load Balancer
Basic Configuration
To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a
HTTP traffic on port 80.
Name
myLoadBalancer
Scheme
internet-facing
internal
IP address type
dualstack
ipv4
dualstack
Listeners
A listener is a process that checks for connection requests, using the protocol and port that you configured.

IPv6 in S3

IPv6 Support for Amazon S3 (August 2016)

Bucket names use the “dualstack” moniker

- https://BUCKETNAME.s3.dualstack.AWSREGION.amazonaws.com
- https://s3.dualstack.AWSREGION.amazonaws.com/BUCKETNAME

IPv6 domain names for S3 buckets in CFTs

- AWS::S3::Bucket
- You can now specify IPv6 domain names for your Amazon S3 buckets.

IPv6 is also supported for S3 Transfer Acceleration

S3 static web hosting is not yet available over IPv6

IPv6 in CloudFront



IPv6 Support for AWS CloudFront, AWS WAF & S3 Transfer Acceleration (Oct 2016)

CloudFront edge locations have IPv6 connectivity

CloudFront will resolve AAAA records for blahblah.cloudfront.net distributions

CloudFront distributions will have IPv6-enabled by default

- IPV6Enabled property added to the DistributionConfig property type

Connections to origin servers will remain IPv4-only

CloudFront access logs will contain the client's IPv6 address in the "c-ip" field

IPv6 addresses will be carried in the X-Forwarded-For header to the origins

IPv6 in AWS Web Application Firewall

IPv6 Support for AWS CloudFront, AWS WAF & S3 Transfer Acceleration (Oct 2016)

AWS WAF can be used with CloudFront or an ALB

WebACLs can contain IP rulesets (blacklists or whitelists) that contain IPv4 and/or IPv6 addresses

IP Match Conditions can use IPv4 and/or IPv6 addresses (using / notation)

WAF supports /16, /24, /32, /48, /56, /64, and /128 IPv6 address ranges

- Some problems with it recognizing the “CIDR” block prefix syntax

IPv6 in Route 53

Route 53 Public DNS service now supports IPv6 (Oct 2016)

Route 53 supports queries over IPv4 and IPv6 transport and can provide authoritative DNS for IPv4 and IPv6 resource records

Recursive DNS resolvers on IPv6 networks can now use either IPv4 or IPv6 transport to send DNS queries to Amazon Route 53

AAAA records and Reverse IPv6 PTR records are supported

Route 53 health checks can be performed over IPv6 transport for IPv6 addresses (but Route 53 will perform IPv4 health checks for domain names)

IPv6 in EC2 and VPCs

IPv6 Support for EC2 Instances in VPCs (Dec 2016)

AWS assigns /56 IPv6 prefix to VPCs (AWS PA-space)

You configure /64 IPv6 prefixes to your subnets within the VPC

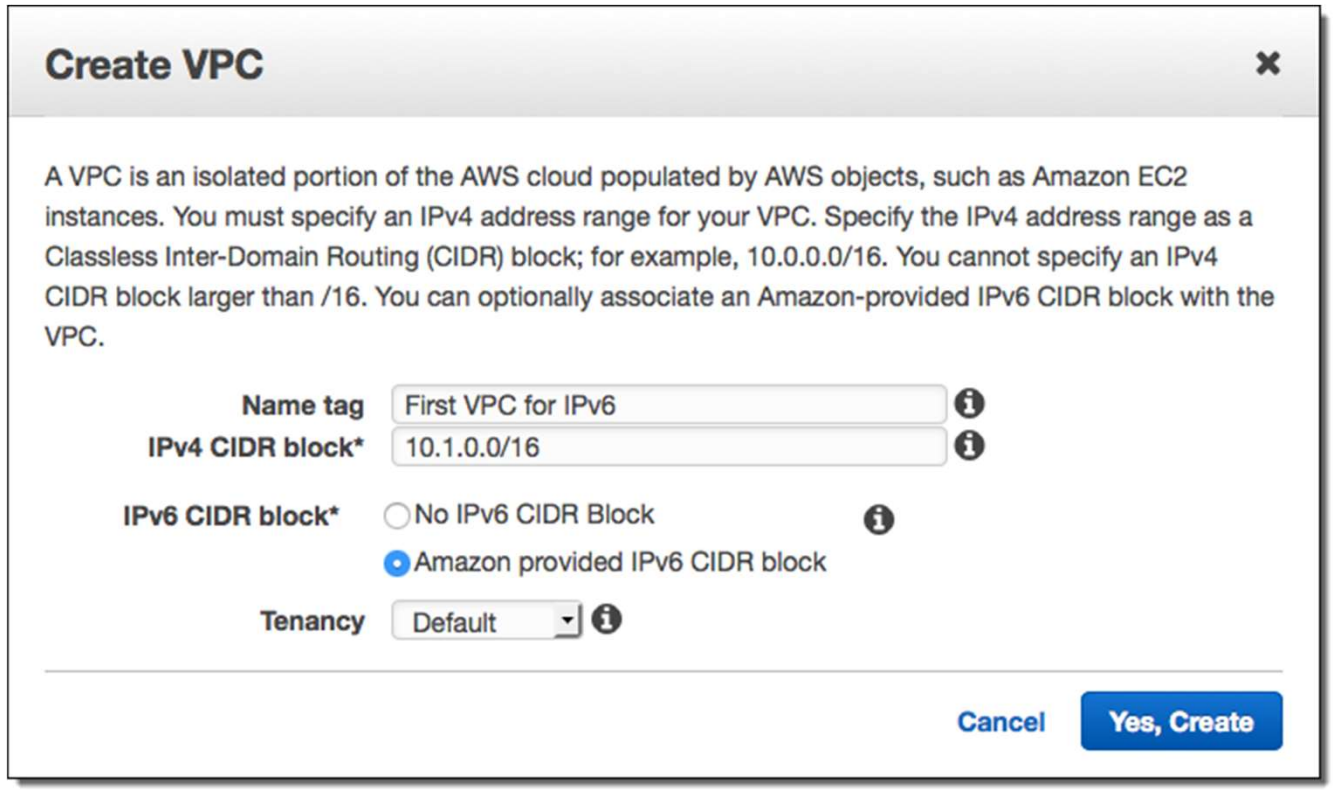
IPv4 and IPv6 addresses are configured in the NACLs associated to the subnets

EC2 ENIs can have IPv6 addresses (Set “Auto-assign IPv6 IP” = Enable)

Security Groups can have IPv4 or IPv6 addresses

Subnets have route tables and those route tables can have IPv4 and IPv6 routes

IPv6 in EC2 and VPCs



AWS DHCPv6

AWS operates DHCPv6 relay on VPC subnet router ".1", AWS DNS on ".2"

IPv6 is automatically enabled on Amazon Linux 2016.09.0 or later, or Windows Server 2008 R2 or later, otherwise, you need to verify/enable DHCPv6

Example for configuration dhclient on Ubuntu OSs

/etc/network/interfaces.d/50-cloud-init.cfg

```
auto eth0
iface eth0 inet dhcp
```

/etc/network/interfaces.d/60-default-with-ipv6.cfg

```
iface eth0 inet6 dhcp
```

Reboot the instance or restart the network interface (sudo ifdown eth0 ; sudo ifup eth0)

IPv6 Routing in VPCs



- Internet Gateway (IGW) used for IPv4 egress from VPC
  - IGW performs a NAT function for Public IPs and EIPs
  - NAT Instance or NAT Gateway is required for IPv4 private subnets
- Egress Only Internet Gateway (EOIGW) used for IPv6
  - EOIGW doesn't perform any NAT functionality
  - No need for NAT with IPv6 – the addresses are already global/public
  - IPv6 default route ::/0 needs to go to IGW for public subnets
  - IPv6 default route ::/0 needs to point to the EOIGW for private subnets
- IPv6 routing works for static or dynamic routing (e.g. route propagation)
- IPv6 routing works over intra-region VPC peering connections
- Transit Gateway (TGW) supports IPv6 static, dynamic, and RAM policies
- No IPv6 on VGW or CGW

IPv6 and Direct Connect

IPv6 is supported for Direct Connect links to your VPCs

AWS allocates /125 for interconnection

AWS accepts /64 or shorter prefixes from CGW

CGW will receive ~2000 prefixes from AWS

BFD support for BGP peerings

- AWS has set the BFD liveness detection minimum interval to 300, and the BFD liveness detection multiplier to 3.

BGP over IPv4 and IPv6 transport using two eBGP peering sessions

Direct Connect Public VIFs & Private VIFs both support IPv6

Direct Connect Gateway (recently launched) - also supports IPv6

IPv6 and VPC Flow Logs

VPC Flow Logs capture IP traffic on VPC interfaces for deeper analysis

Inspection of IP traffic going to/from network interfaces in your VPC - metadata about traffic (Like NetFlow)

- Traffic to/from ENIs, Subnets, or VPCs
- Not traffic to/from AWS DNS/DHCP or VPC router ".1" or metadata 169.254.169.254

Flow Logs show connection data for IPv4 and IPv6 packets:

- 2, AWS Acct#, ENI, Src IPv4/IPv6, Dest IPv4/IPv6, Src Port, Dest Port, Protocol, # of packets, # of bytes, Capture Start/End, Accept/Reject, OK

```
2 123456789010 eni-f41c42bf
2001:db8:1234:a100:8d6e:3477:df66:f105
2001:db8:1234:a102:3304:8879:34cf:4071 34892 22 6 54 8855
1477913708 1477913820 ACCEPT OK
```


Other IPv6-Capable AWS Services

- AWS WorkSpaces can use native IPv6 Internet connectivity
  - AWS WorkSpaces (Value, Standard, Power work with IPv6, but not Performance and Graphics bundles) can use IPv6 to access the Internet from your VPC

- API Gateway is now IPv6 enabled (Nov 2017)
  - CloudFront can front-end your API gateway

- AWS IoT has supported IPv6 for a few years now (Dec 2015)
  - IPv6 application interactions with IoT services can use IPv6
  - IoT Device Gateway now supports IPv4 and IPv6 using the same endpoint, and AWS IoT service can use MQ Telemetry Transport (MQTT) client interactions

Migrating to IPv6

Migrating to IPv6

Step	Notes
Step 1: Associate an IPv6 CIDR Block with Your VPC and Subnets	Associate an Amazon-provided IPv6 CIDR block with your VPC and with your subnets.
Step 2: Update Your Route Tables	Update your route tables to route your IPv6 traffic. For a public subnet, create a route that routes all IPv6 traffic from the subnet to the internet gateway. For a private subnet, create a route that routes all internet-bound IPv6 traffic from the subnet to an egress-only internet gateway.
Step 3: Update Your Security Group Rules	Update your security group rules to include rules for IPv6 addresses. This enables IPv6 traffic to flow to and from your instances. If you've created custom network ACL rules to control the flow of traffic to and from your subnet, you must include rules for IPv6 traffic.
Step 4: Change Your Instance Type	If your instance type does not support IPv6, change the instance type.
Step 5: Assign IPv6 Addresses to Your Instances	Assign IPv6 addresses to your instances from the IPv6 address range of your subnet.
Step 6: (Optional) Configure IPv6 on Your Instances	If your instance was launched from an AMI that is not configured to use DHCPv6, you must manually configure your instance to recognize an IPv6 address assigned to the instance.

Scriptable Infrastructure for IPv6

If you're using the "AWS Management Console", you're doing it wrong!

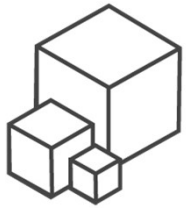
- Take a page from the DevOps handbook and AUTOMATE!

AWS Quick Starts CloudFormation Templates (CFTs)

- https://aws.amazon.com/quickstart/

Ansible playbooks with Boto3 (1.9.X) and Python

AWS CLI Commands, Newer (1.16.X) == Better



Summary, Resources, and Q&A

Valuable (but FREE) AWS IPv6 Resources

AWS re:Invent 2017: IPv6 in the Cloud: Protocol and AWS Service Overview (NET202), by Alan Halachmi

https://www.youtube.com/watch?v=GE_FqZ-XLR0

Delivering IPv6 on Amazon Virtual Private Cloud, by Alan Halachmi, Senior manager, solutions architecture, Amazon

https://atscaleconference.com/videos/delivering-ipv6-on-amazon-virtual-private-cloud%E2%80%A8/

Migrating to IPv6

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-migrate-ipv6.html

Other AWS & IPv6 Classes

"Rapidly Deploying IPv6 on AWS", A Cloud Guru Course

- 6 hours of online video teaching and showing how to enable IPv6 on AWS infrastructure
- https://acloud.guru/learn/aws-ipv6

HexaBuild 1-day hands-on virtual class (HBT330)

- Contact me if you might be interested in attending

Questions and Answers

Are there any questions?

Thank you very much for your time.

Please contact me if ever I can ever be of service to you.

Scott@HexaBuild.io +1-303-949-4865 @ScottHogg

Thank You

