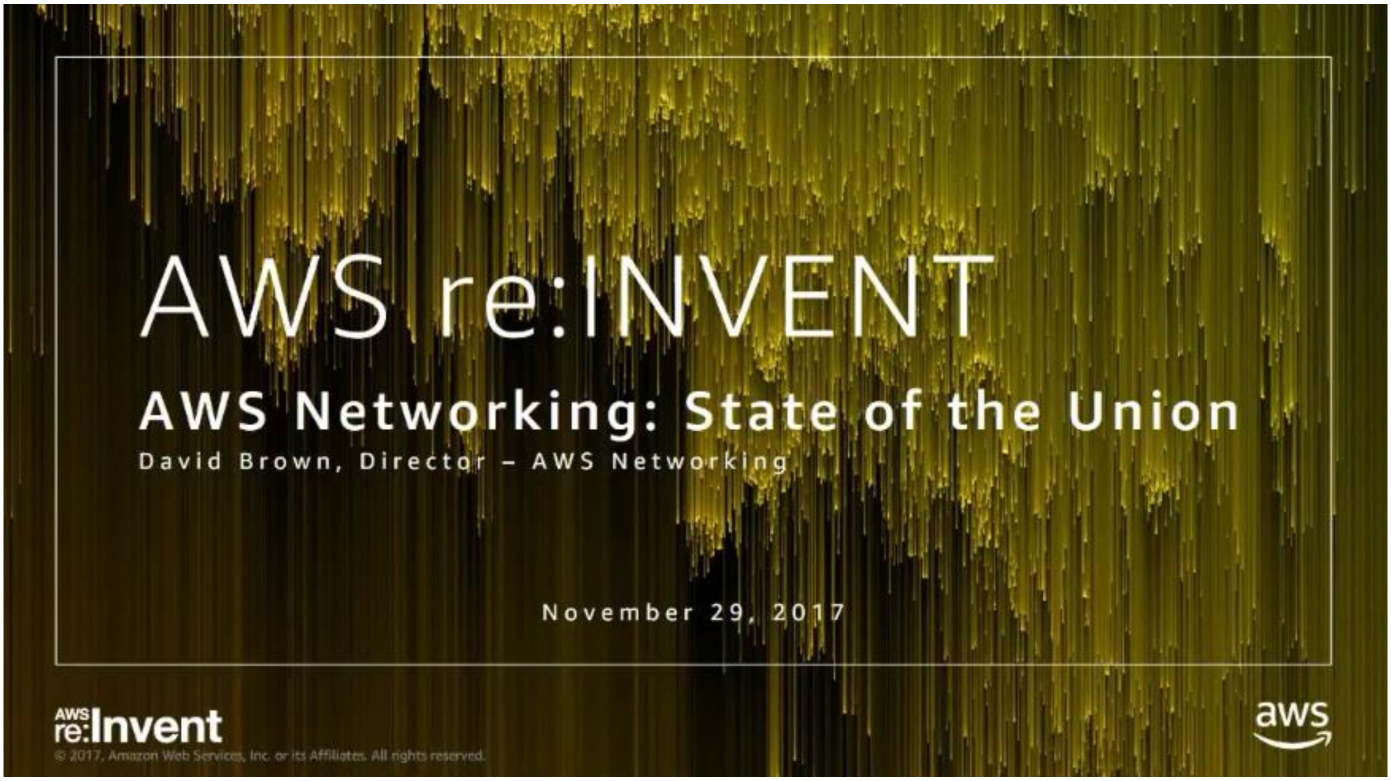


AWS re:INVENT

AWS Networking: State of the Union

David Brown, Director – AWS Networking

November 29, 2017

AWS re:Invent
aws

Learn about the new services and features we have and that we are launching across AWS Networking this year. Learn also about our vision for continued innovation in this space and the ongoing evolution of networking capabilities and performance. Gain insight into how these new capabilities help everyone—from developers to enterprises to startups—drive greater security and reliability, improved flexibility, and higher performance. Join Dave Brown, director of Amazon EC2 Networking, and learn more about Amazon Virtual Private Cloud (VPC), Elastic Load Balancing, AWS PrivateLink, VPN, AWS Direct Connect, and more. In addition, we cover new releases and show how easy it is to get started. You leave armed with details of how everything fits together in real-world customer scenarios.

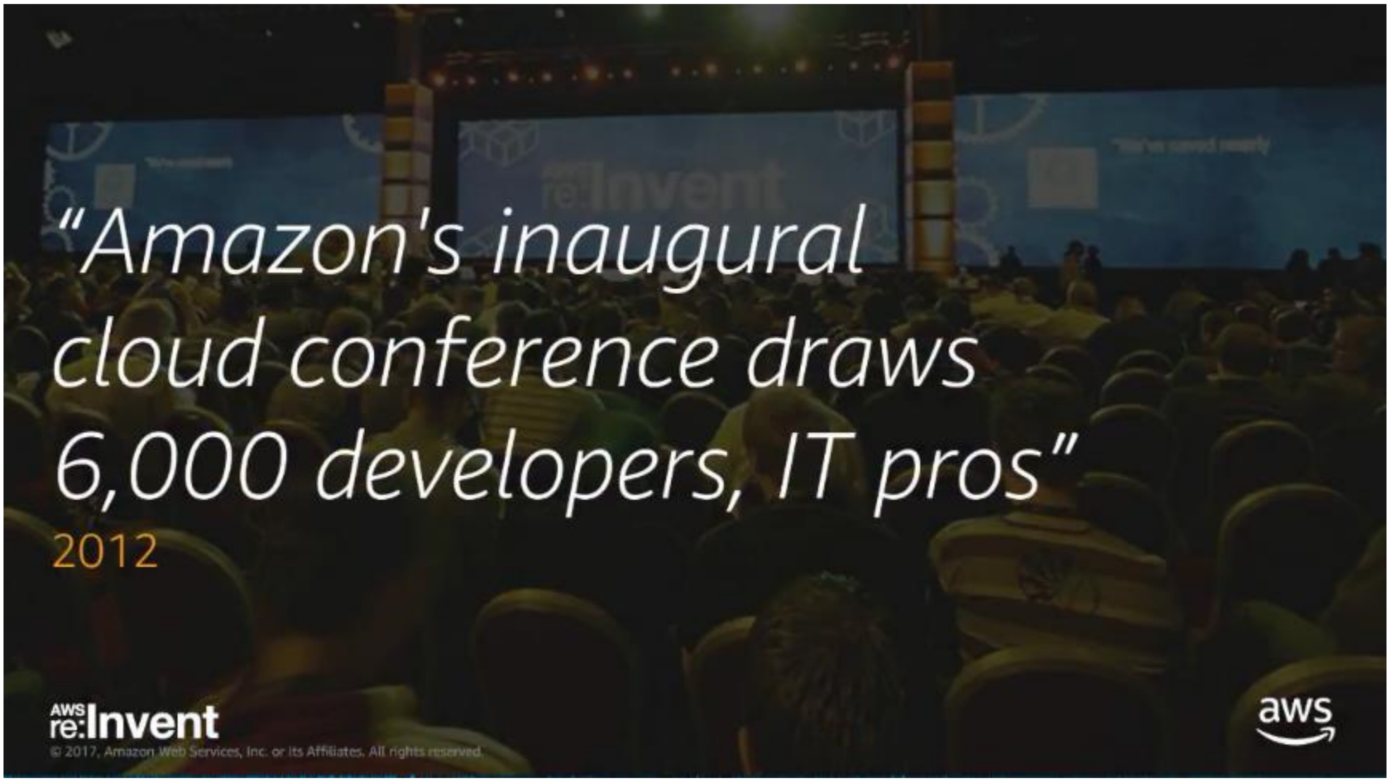
Thank you for your business!

Startup

Enterprise

Public Sector

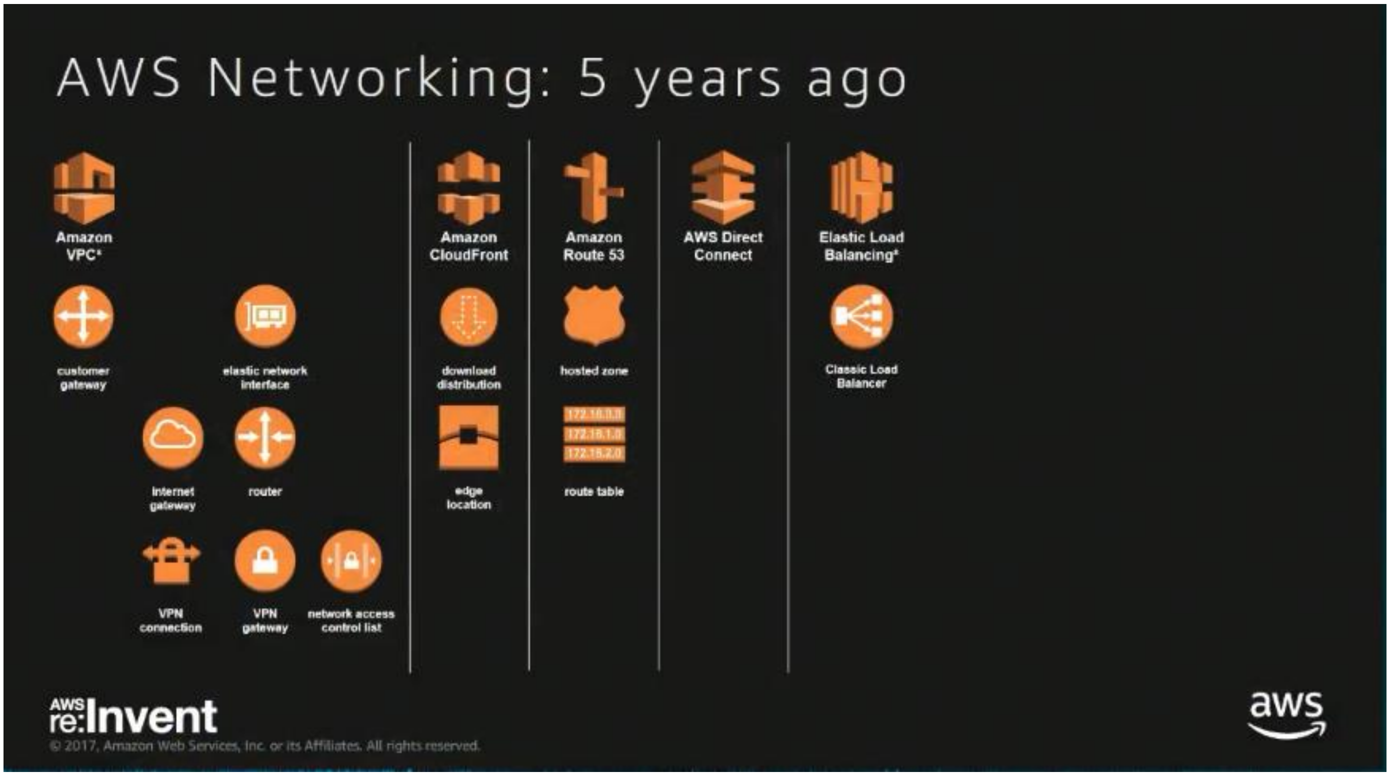
SI/ISV



"Amazon's inaugural cloud conference draws 6,000 developers, IT pros"

2012

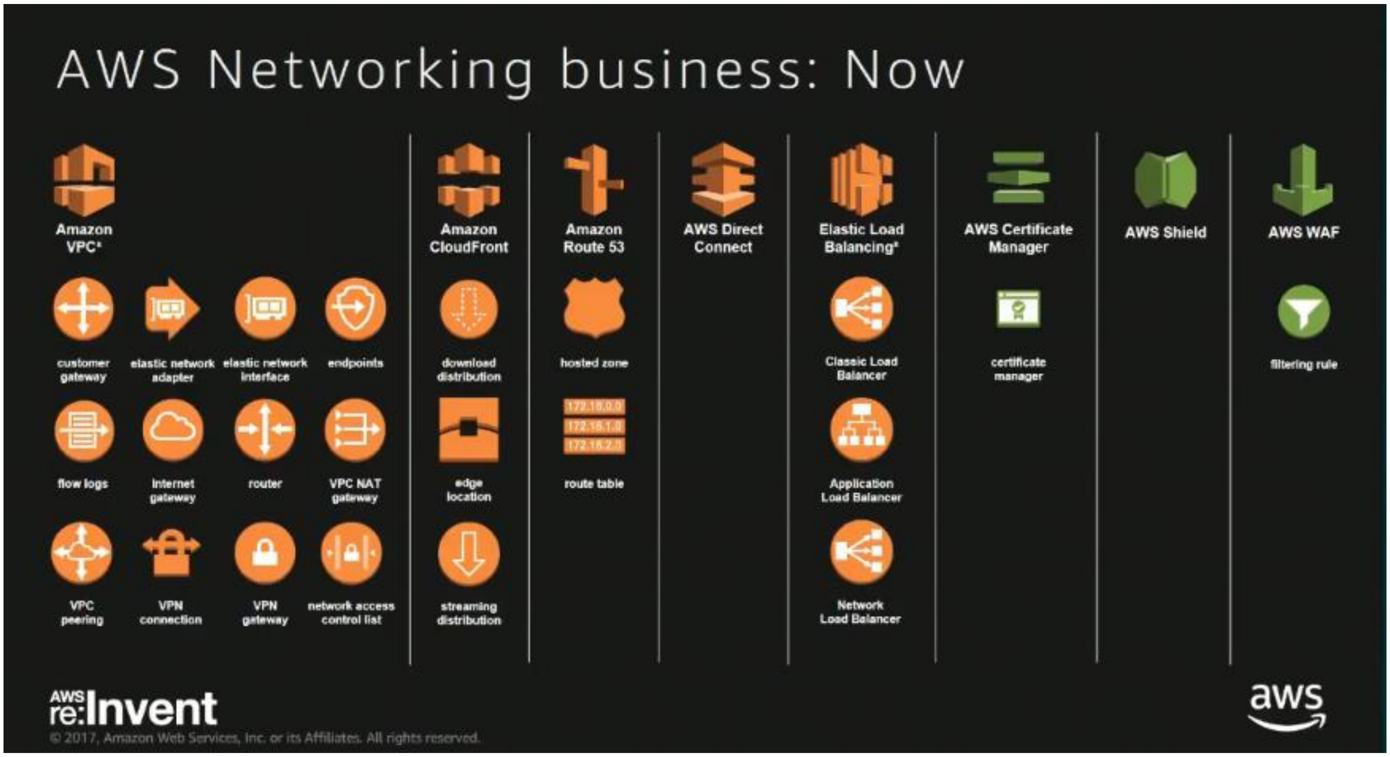
AWS re:Invent



AWS Networking: 5 years ago

- Amazon VPC*
  - customer gateway
  - elastic network interface
  - internet gateway
  - router
  - VPN connection
  - VPN gateway
  - network access control list
- Amazon CloudFront
  - download distribution
  - edge location
- Amazon Route 53
  - hosted zone
  - route table
- AWS Direct Connect
- Elastic Load Balancing*
  - Classic Load Balancer

AWS re:Invent



AWS Networking business: Now

Amazon VPC*

customer gateway

elastic network adapter

elastic network interface

endpoints

flow logs

Internet gateway

router

VPC NAT gateway

VPC peering

VPN connection

VPN gateway

network access control list

Amazon CloudFront

download distribution

edge location

streaming distribution

Amazon Route 53

hosted zone

172.16.0.0

172.16.1.0

172.16.2.0

route table

AWS Direct Connect

Elastic Load Balancing*

Classic Load Balancer

Application Load Balancer

Network Load Balancer

AWS Certificate Manager

certificate manager

AWS Shield

AWS WAF

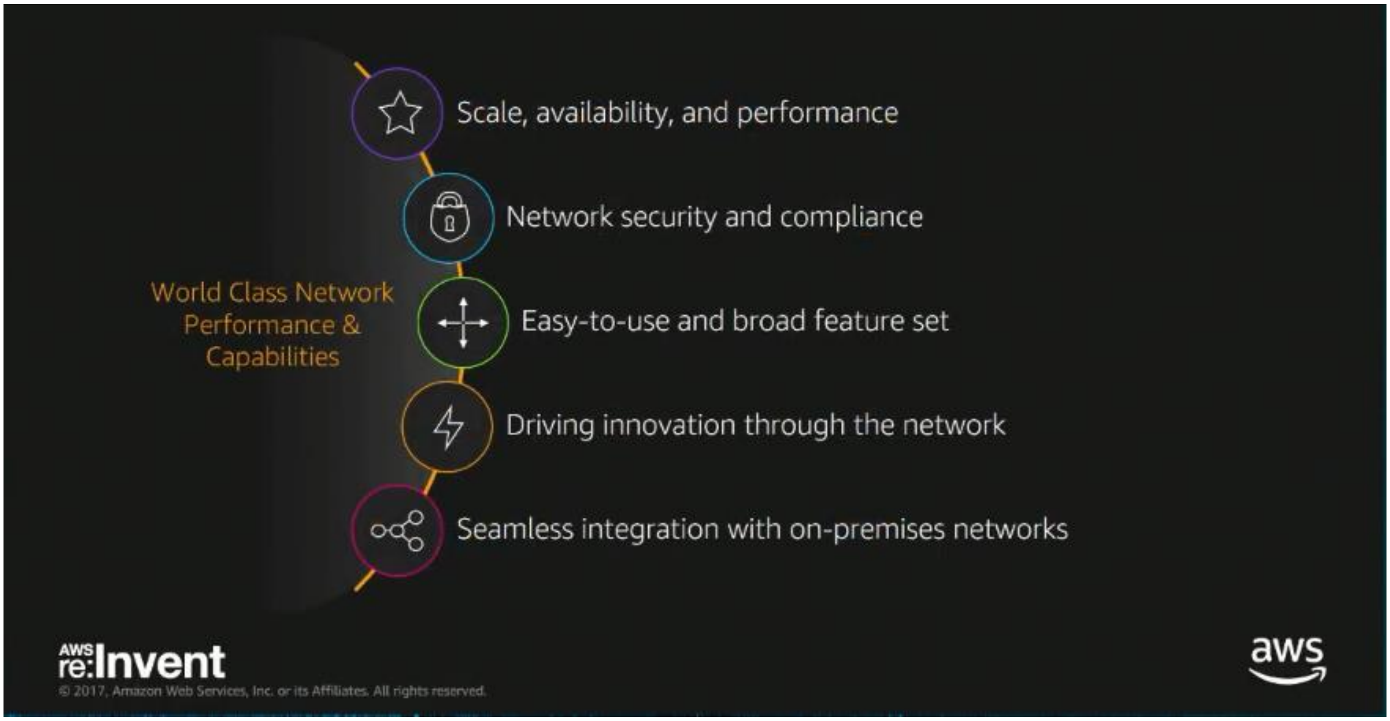
filtering rule

AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

For ELB, we have the ***Application Load Balancer*** for layer 7 HTTP type workloads, and the ***Network Load Balancer*** for TCP for layer 4 type workloads. The green services are new and for security.



World Class Network Performance & Capabilities

Scale, availability, and performance

Network security and compliance

Easy-to-use and broad feature set

Driving innovation through the network

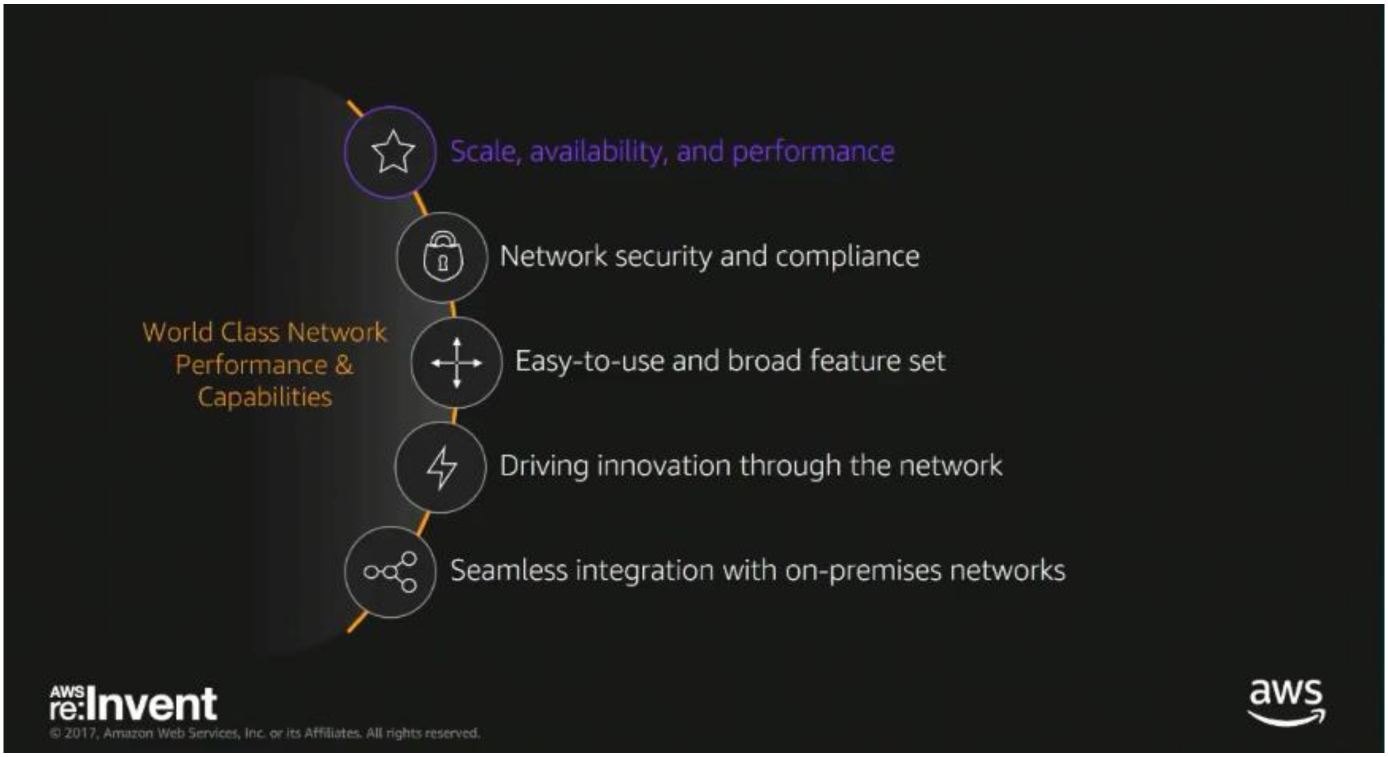
Seamless integration with on-premises networks

AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

We mostly want to design and run a VPC network that is optimized for running our workloads for scale, reliability and performance.



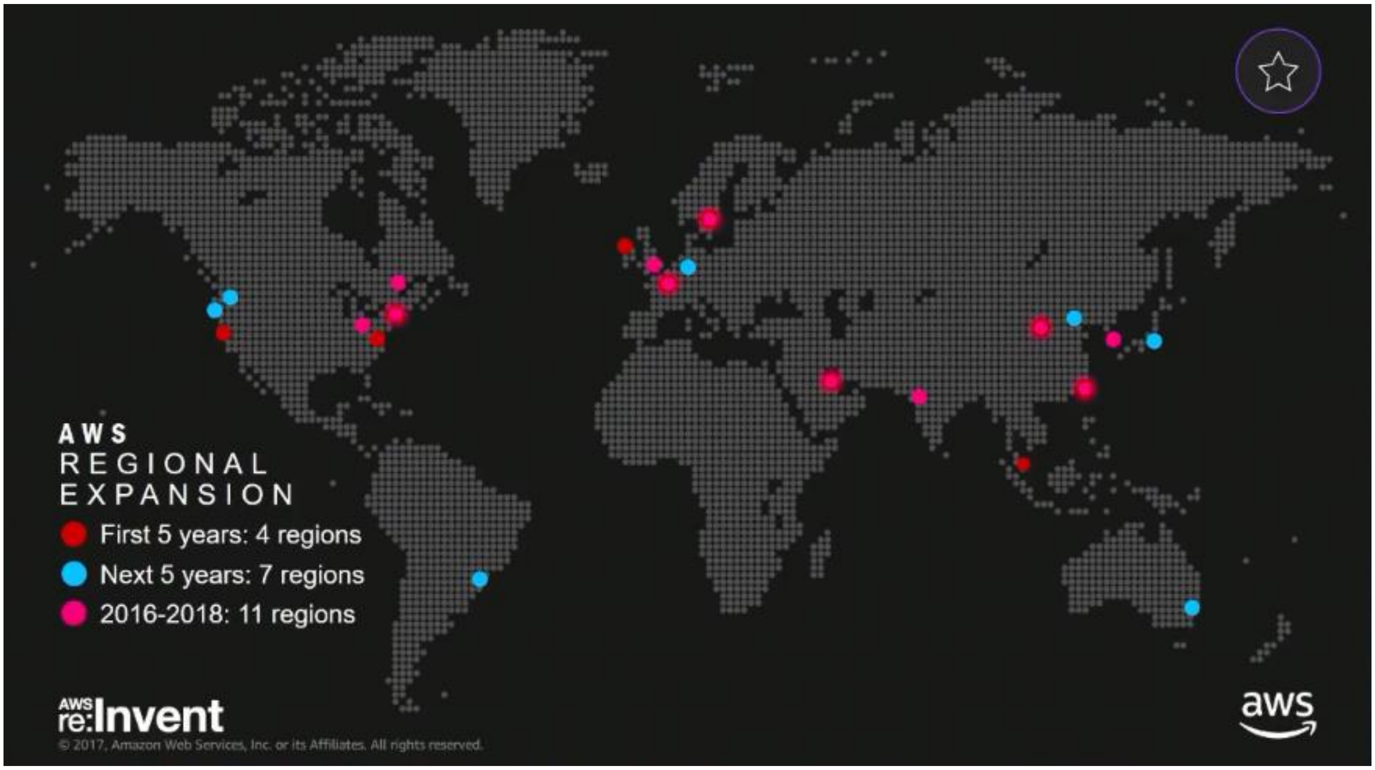
World Class Network Performance & Capabilities

- Scale, availability, and performance
- Network security and compliance
- Easy-to-use and broad feature set
- Driving innovation through the network
- Seamless integration with on-premises networks

AWS re:Invent

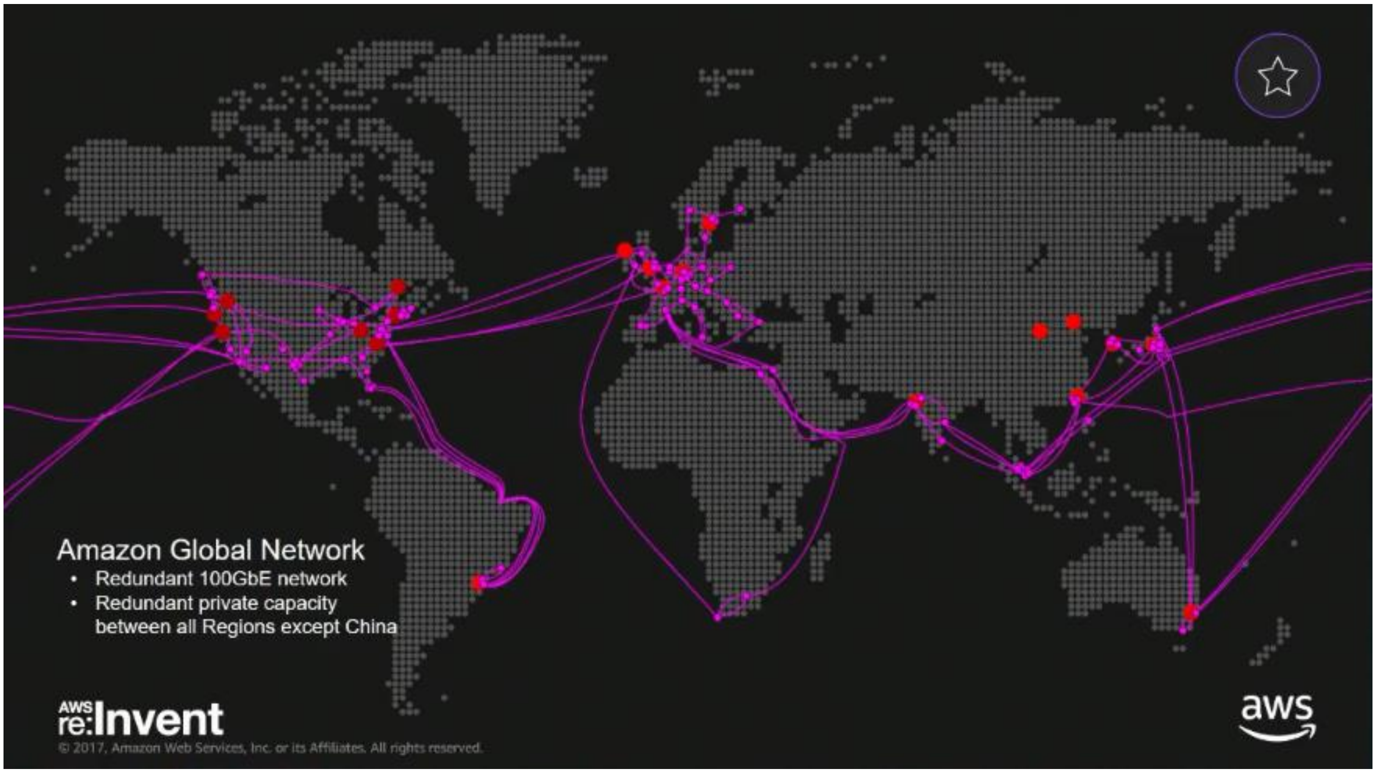
GLOBAL INFRASTRUCTURE

AWS re:Invent



AWS REGIONAL EXPANSION

- ● First 5 years: 4 regions
- ● Next 5 years: 7 regions
- ● 2016-2018: 11 regions



Amazon Global Network

- Redundant 100GbE network
- Redundant private capacity between all Regions except China

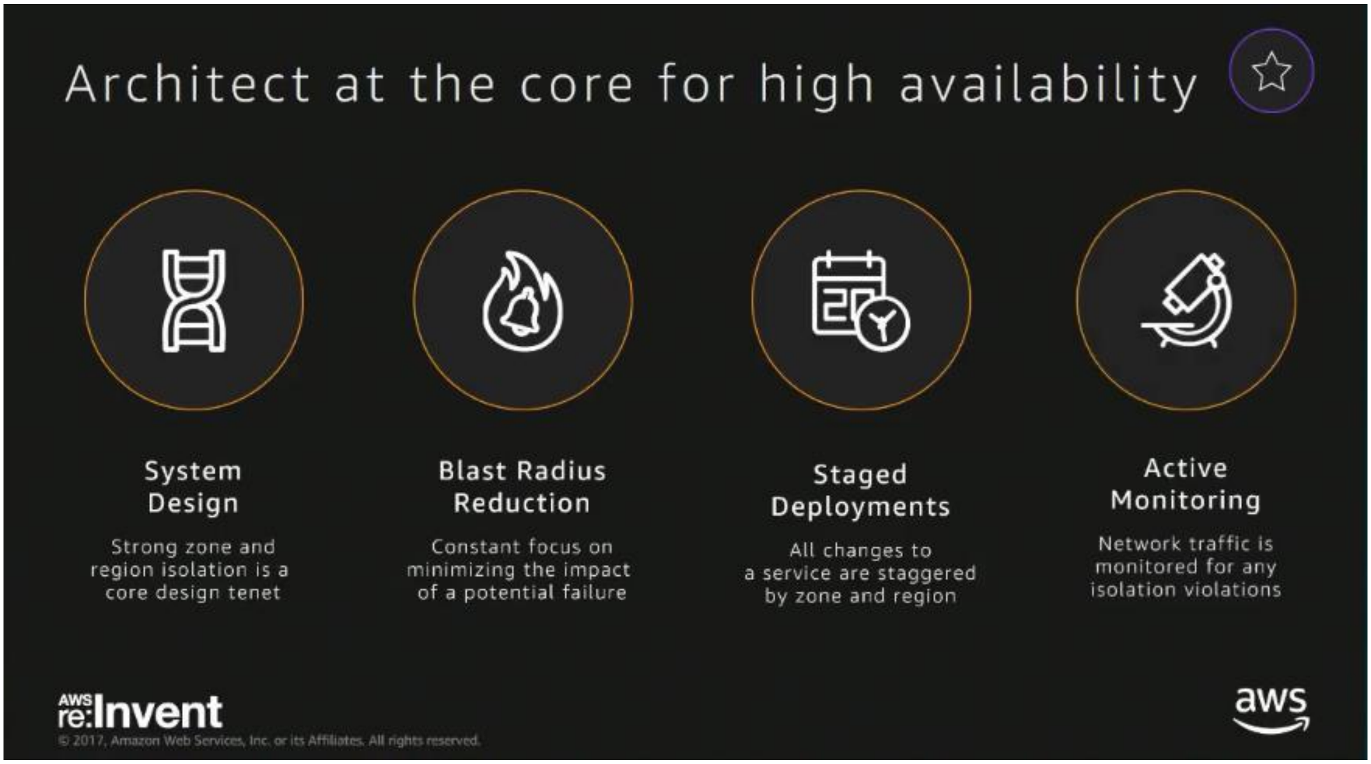
AWS as been building a ***global infrastructure backbone*** that literally spans the globe. All traffic between our regions from our ***CloudFront*** Points of Presence's ***POPs,*** over ***DirectConnect*** locations except the 2 regions in China all travel on fiber owned by AWS. These fibers are sometimes multiple strands all running 100GBps for handling extreme data packet loads for better packet transmission, lower packet loss, much better latency.

10 YEARS

OF THE AVAILABILITY ZONE

The concept of AZs and Regions being completely isolated from each other are core ideas.

There is no compression algorithm for experience



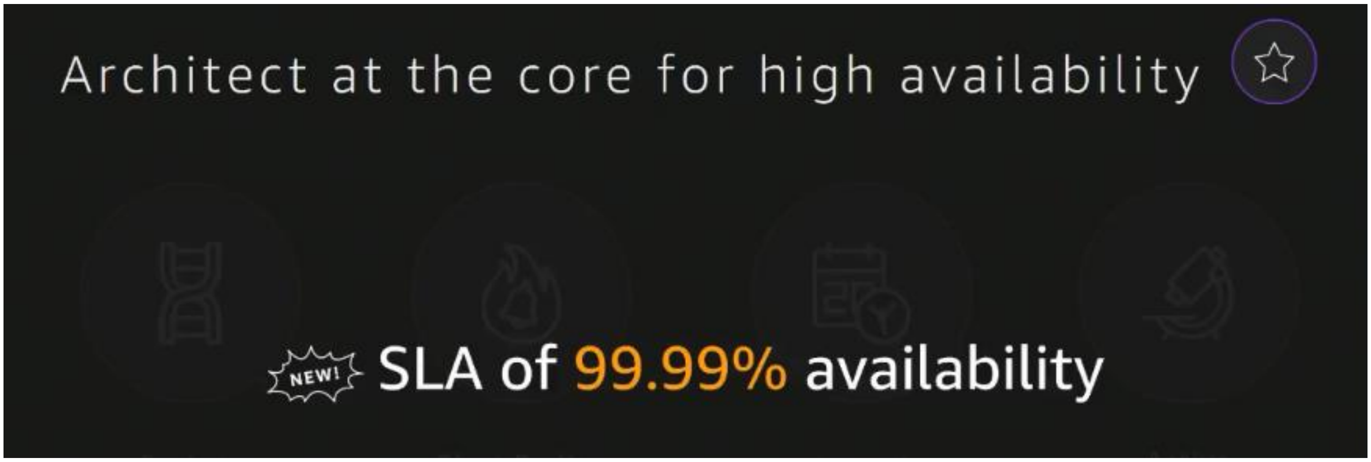
Architect at the core for high availability

System Design
Strong zone and region isolation is a core design tenet

Blast Radius Reduction
Constant focus on minimizing the impact of a potential failure

Staged Deployments
All changes to a service are staggered by zone and region

Active Monitoring
Network traffic is monitored for any isolation violations



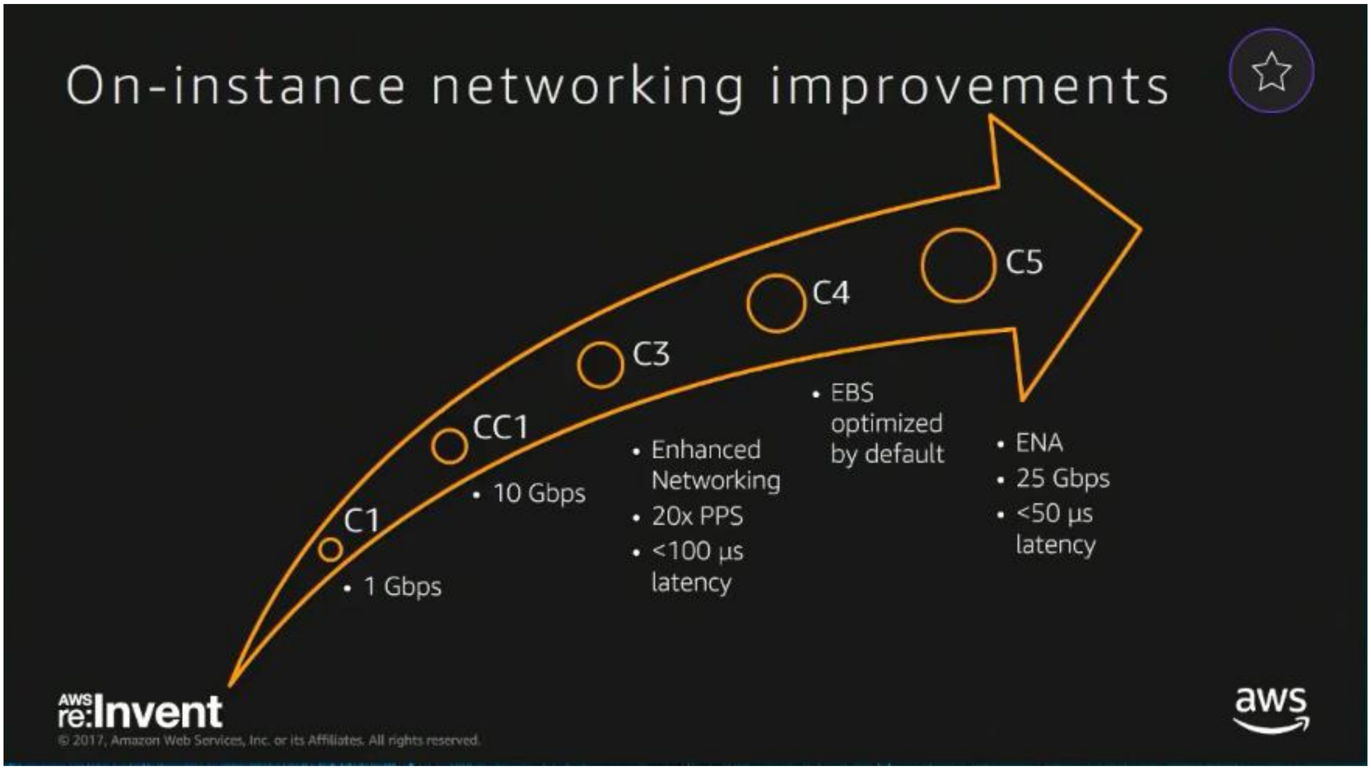
Architect at the core for high availability

NEW! SLA of 99.99% availability

EC2 now has a ***SLA of 99.99%*** availability

INSTANCE

NETWORK PERFORMANCE



On-instance networking improvements

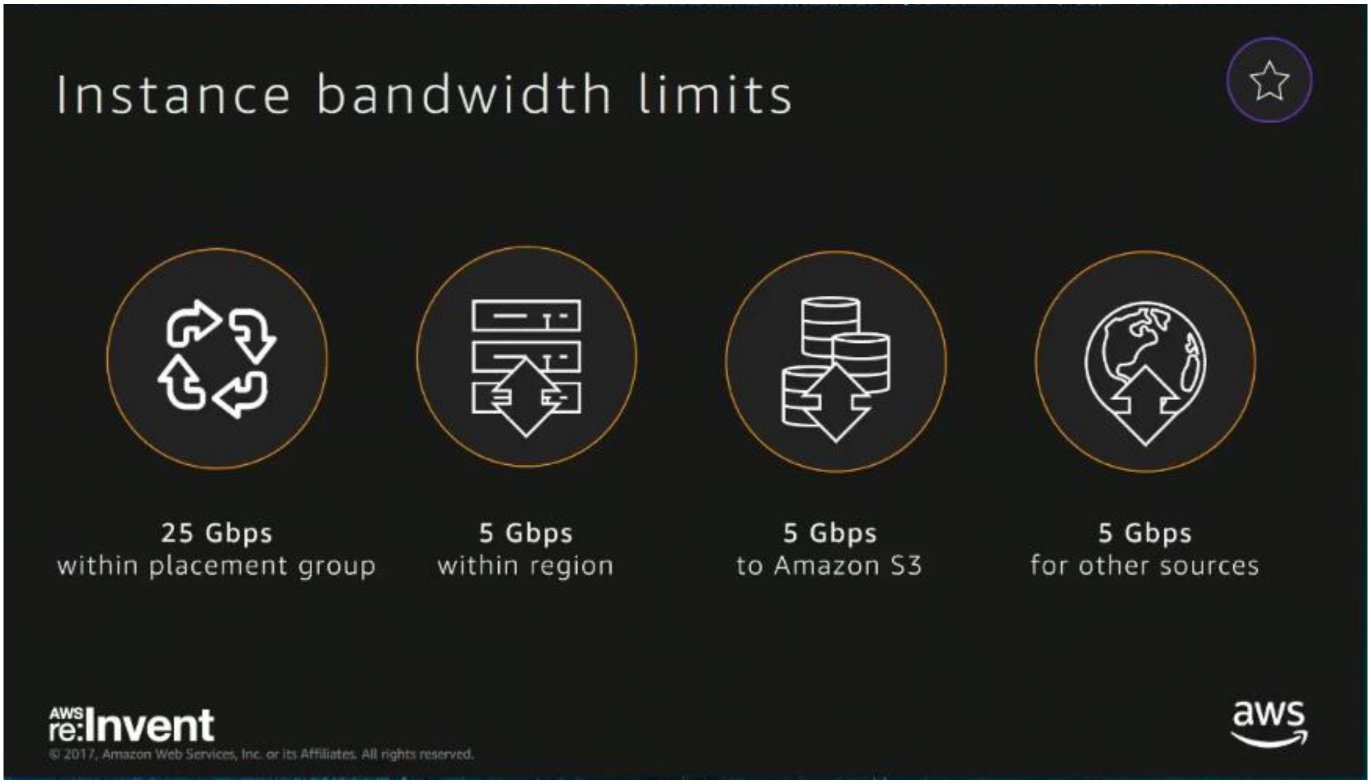
C1
- 1 Gbps

CC1
- 10 Gbps

C3
- Enhanced Networking
- 20x PPS
- <100 µs latency

C4
- EBS optimized by default

C5
- ENA
- 25 Gbps
- <50 µs latency



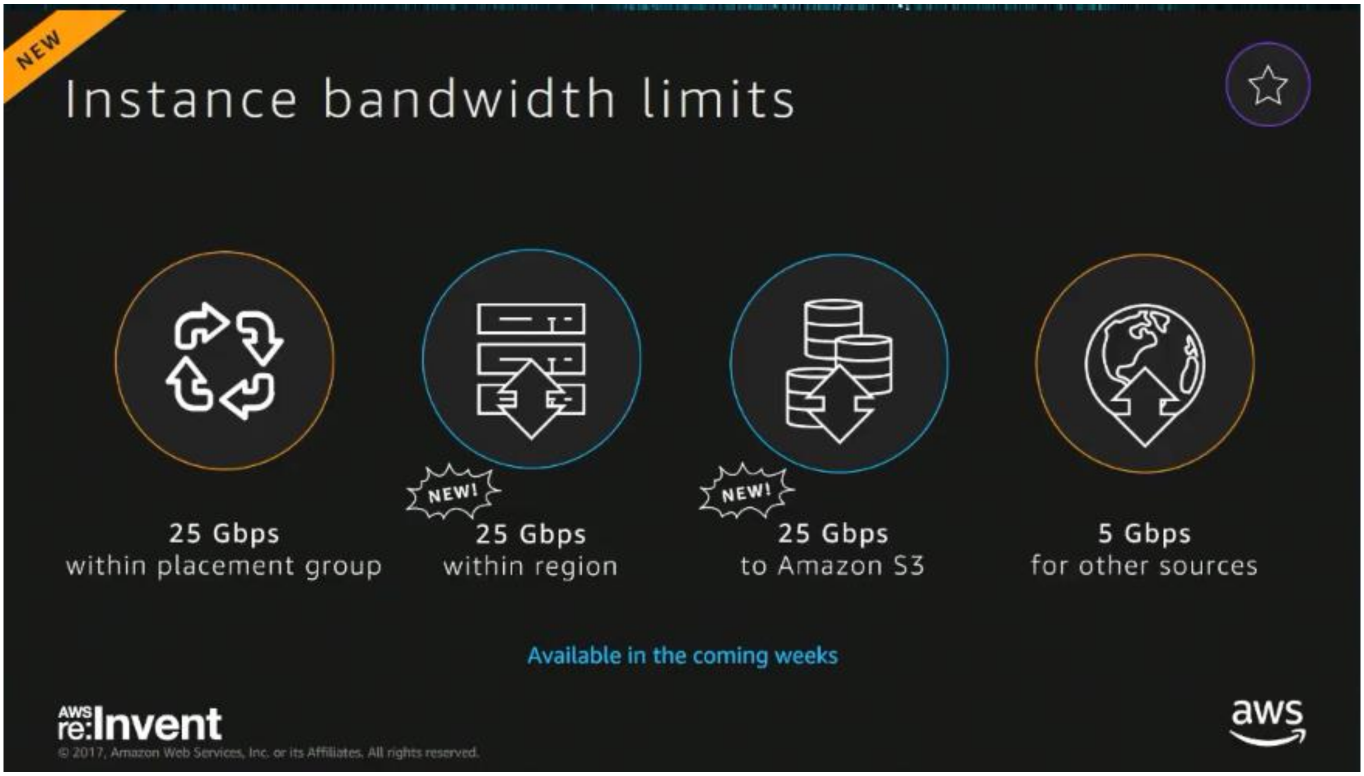
Instance bandwidth limits

25 Gbps
within placement group

5 Gbps
within region

5 Gbps
to Amazon S3

5 Gbps
for other sources



NEW

Instance bandwidth limits

25 Gbps
within placement group

NEW!
25 Gbps
within region

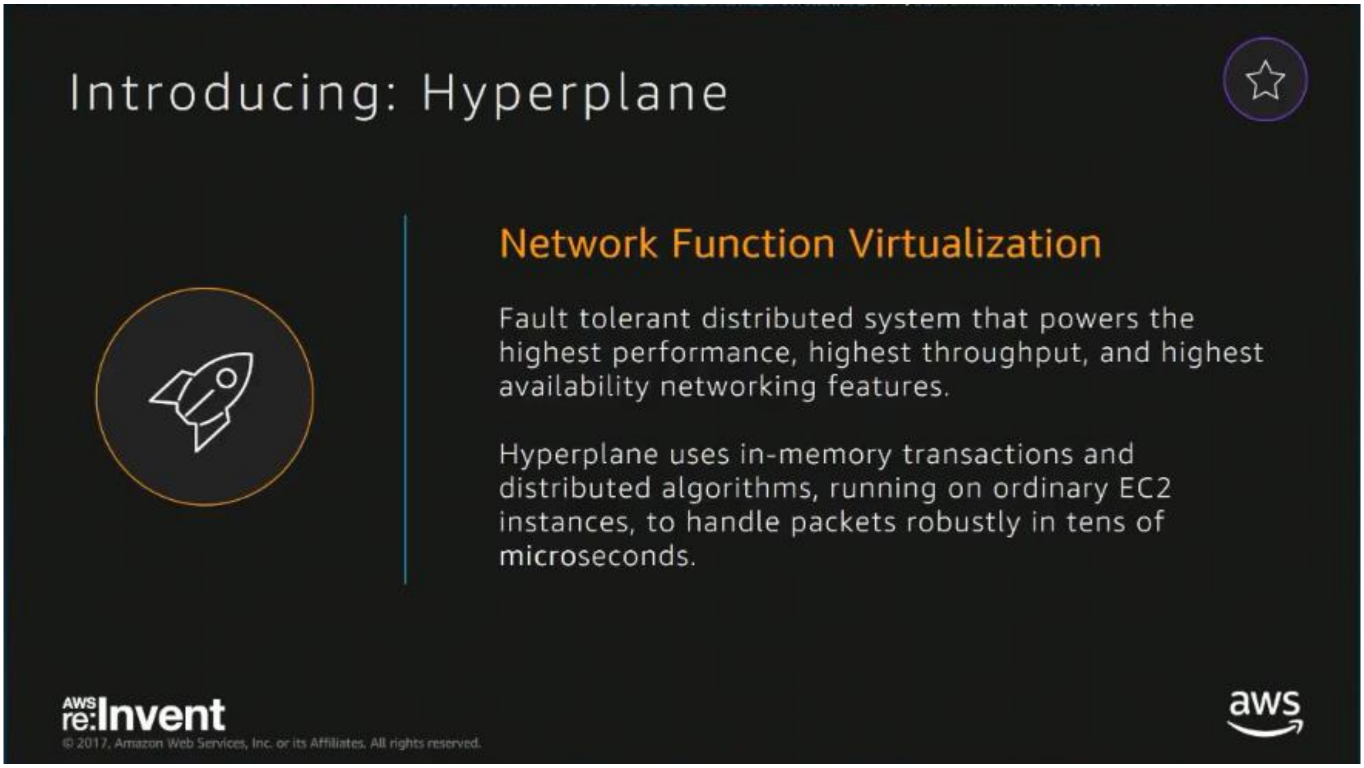
NEW!
25 Gbps
to Amazon S3

5 Gbps
for other sources

Available in the coming weeks

HYPERPLANE

NETWORK FUNCTION VIRTUALIZATION



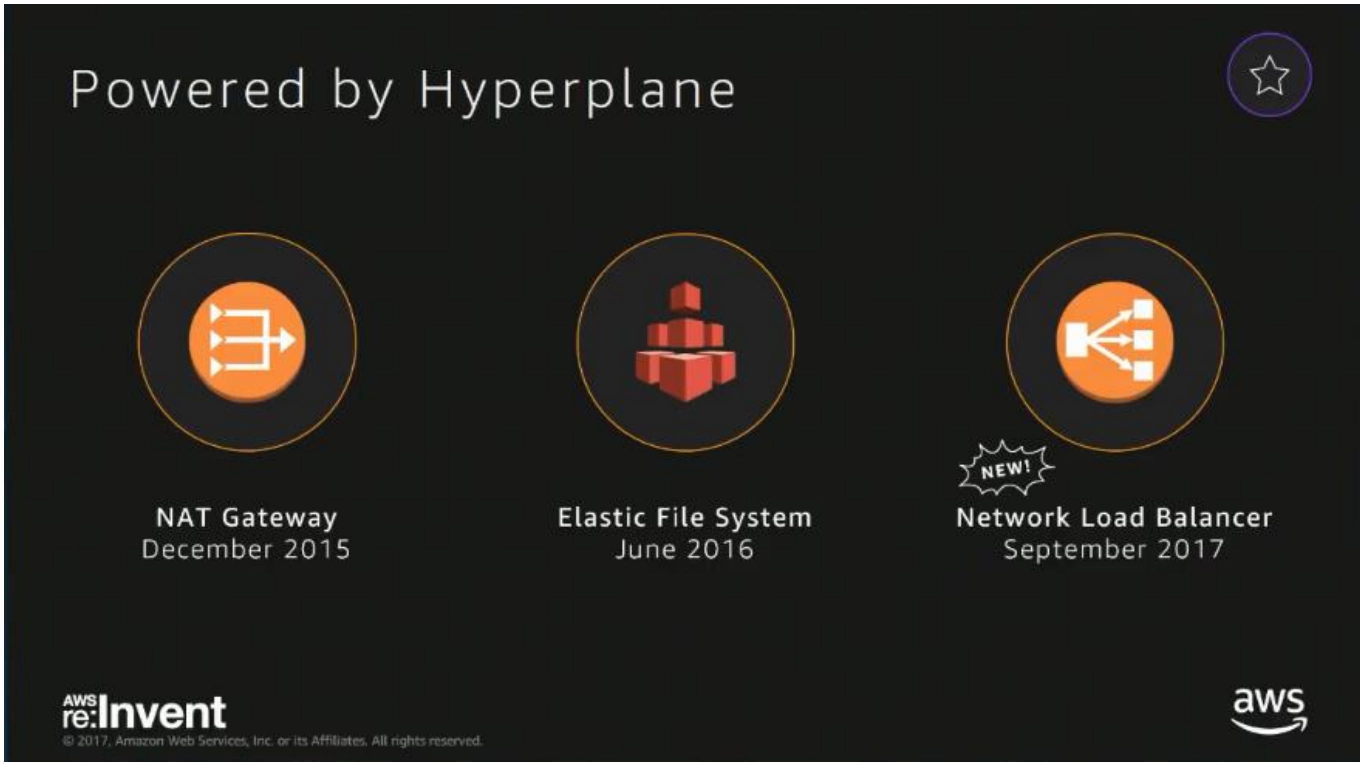
Introducing: Hyperplane

Network Function Virtualization

Fault tolerant distributed system that powers the highest performance, highest throughput, and highest availability networking features.

Hyperplane uses in-memory transactions and distributed algorithms, running on ordinary EC2 instances, to handle packets robustly in tens of microseconds.

AWS re:Invent
aws



Powered by Hyperplane

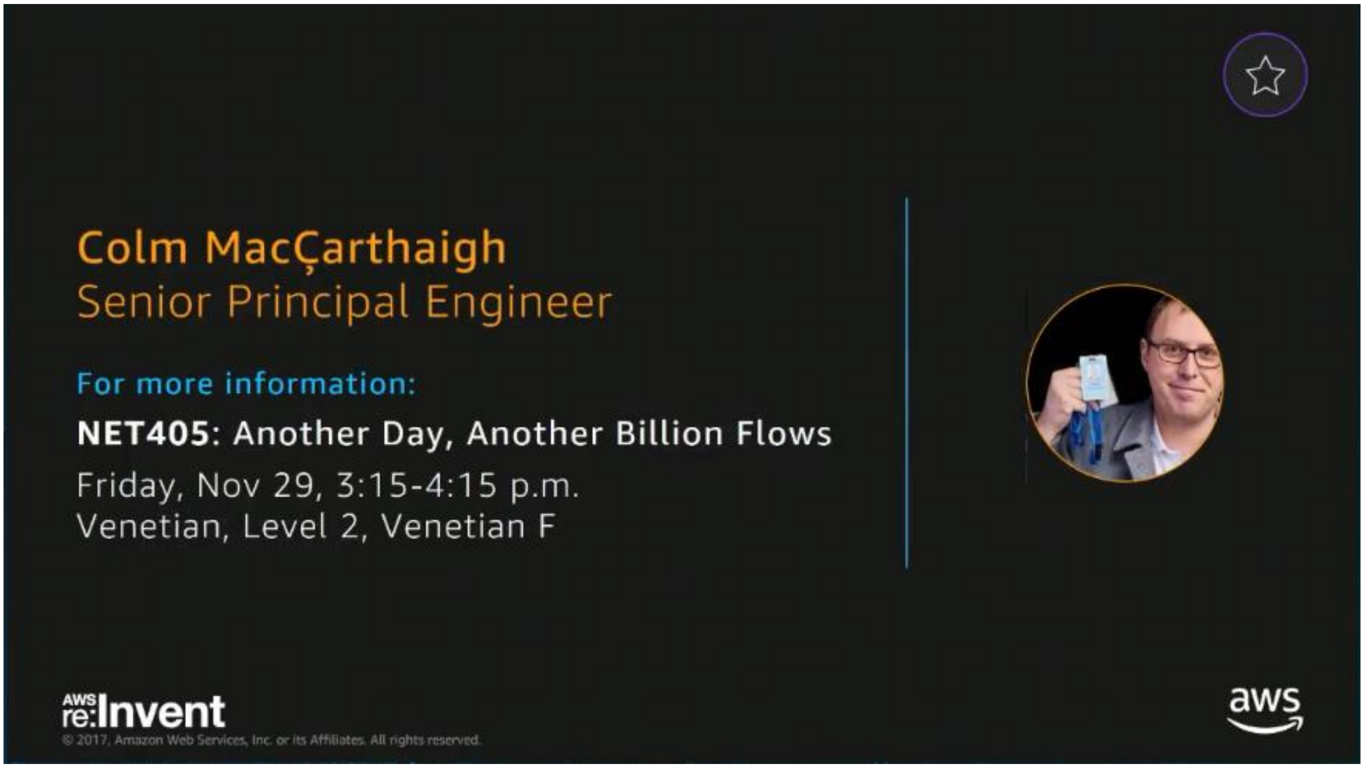
NAT Gateway
December 2015

Elastic File System
June 2016

NEW!
Network Load Balancer
September 2017

AWS re:Invent
aws

Hyperplane powers these 3 services, it is built on EC2 instances in a clustered formation to provide the service.



Colm MacÇarthaigh
Senior Principal Engineer

For more information:

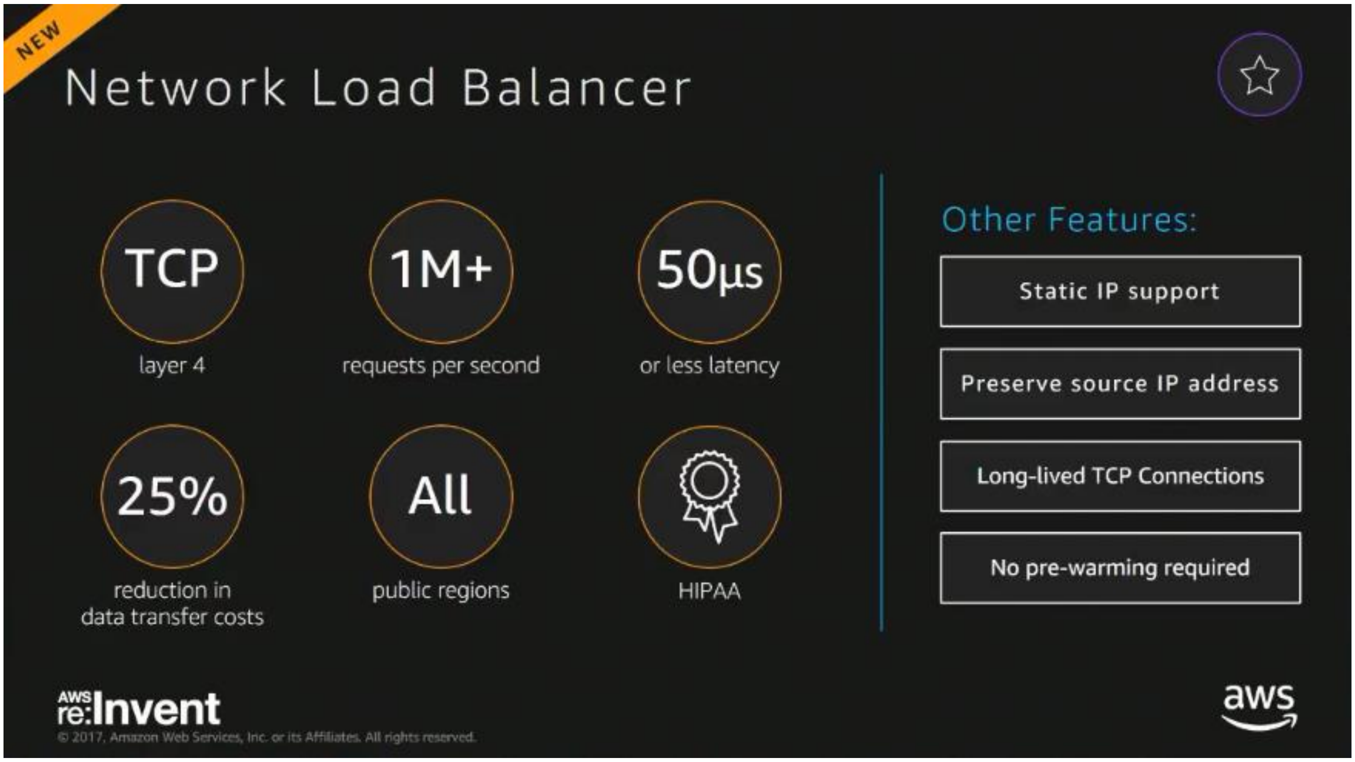
NET405: Another Day, Another Billion Flows

Friday, Nov 29, 3:15-4:15 p.m.
Venetian, Level 2, Venetian F

AWS re:Invent

aws

NETWORK
LOAD BALANCER



NEW

Network Load Balancer

TCP
layer 4

1M+
requests per second

50µs
or less latency

25%
reduction in data transfer costs

All
public regions

HIPAA

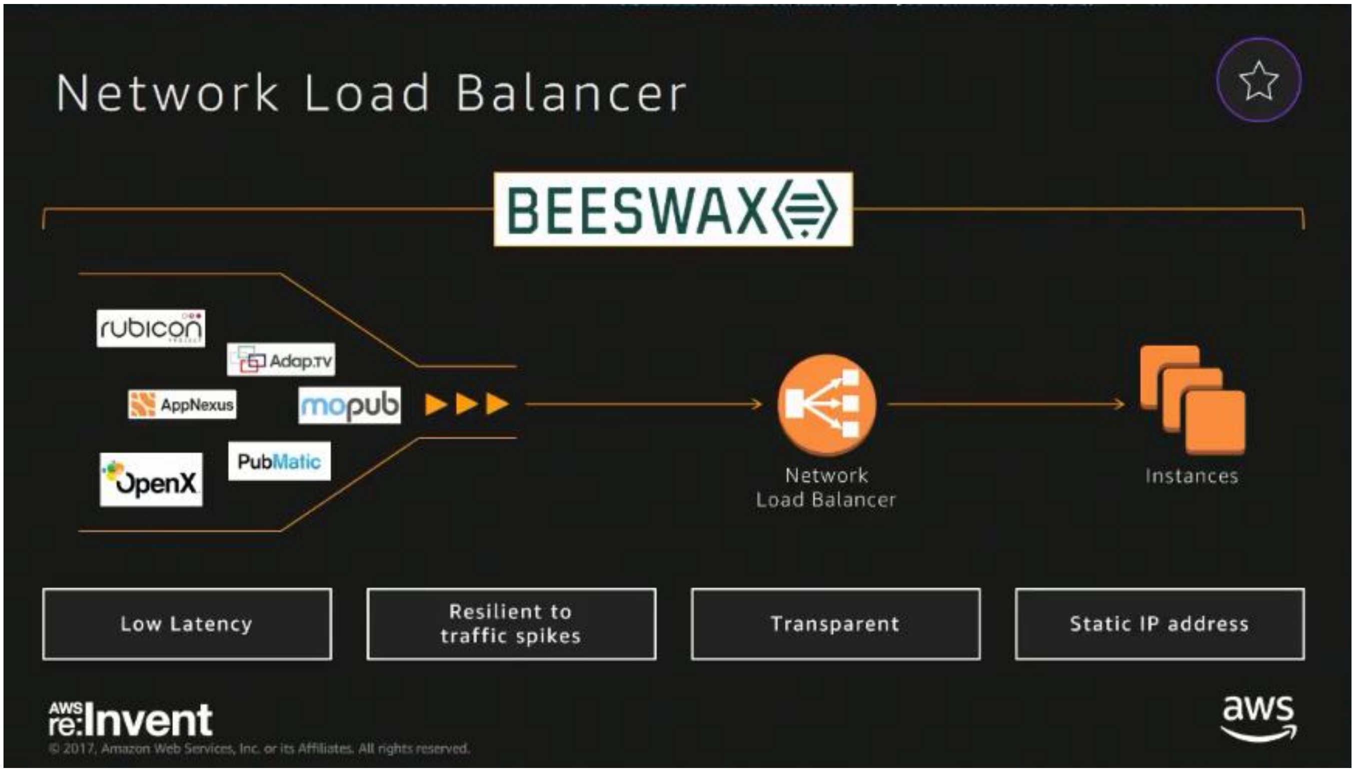
Other Features:

- Static IP support
- Preserve source IP address
- Long-lived TCP Connections
- No pre-warming required

AWS re:Invent

aws

The ***Network Load Balancer*** NLB is TCP-based and is powered by Hyperplane for high throughput data transfers. You can attach an Elastic IP address to the NLB to give it a static IP address. ***Preserve source IP address*** means that your backend instance is actually going to see the IP address of the client sending the request into your front facing NLB, there is no need for proxy protocols at all.



Network Load Balancer

- Low Latency
- Resilient to traffic spikes
- Transparent
- Static IP address

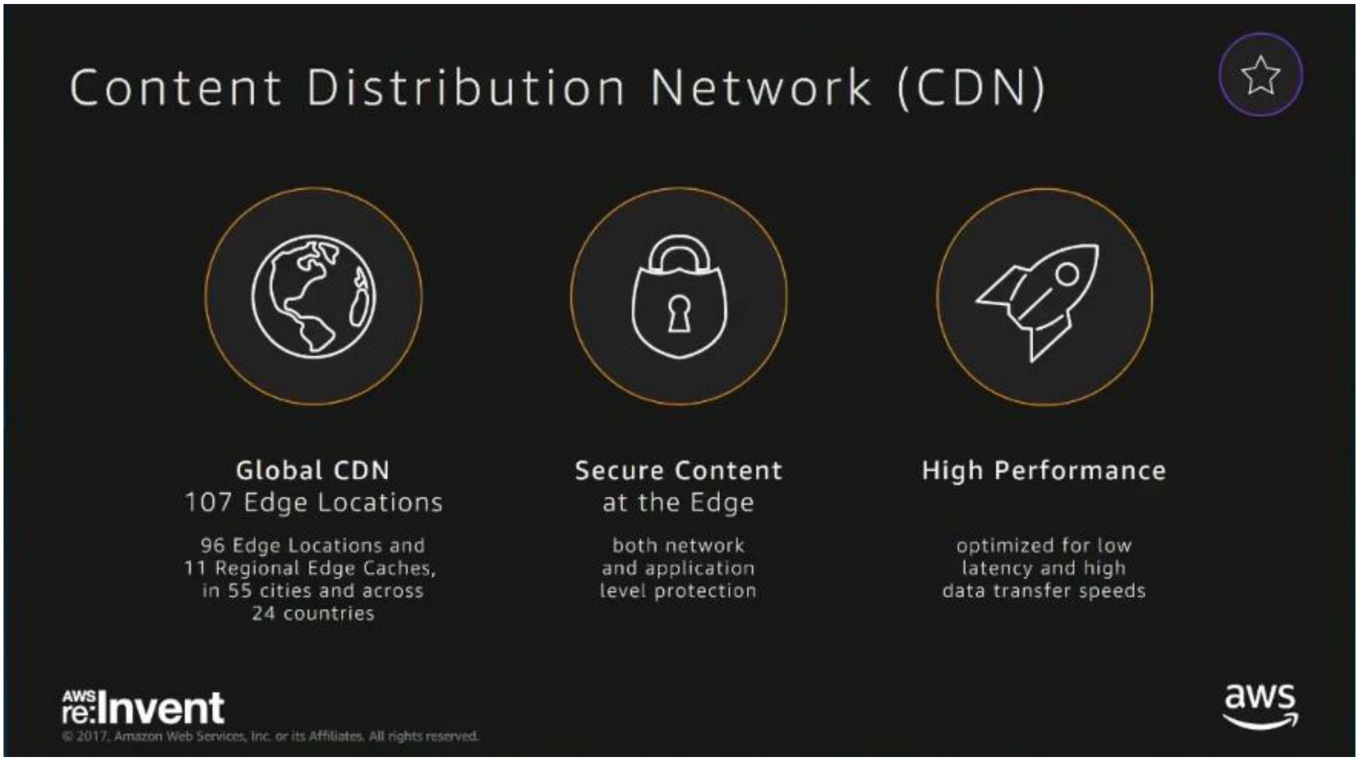
AWS re:Invent

aws

Let us see a custom use case for the NLB. Beeswax is an AdTech company that is building a platform that other AdTech companies are building on top of. They have a whole lot of ad exchanges that asks ads provider if they would like to show an ad to a web page? You only have about 10-30ms to make a yes or no decision to spend money on that ad.

CLOUDFRONT

CONTENT DISTRIBUTION NETWORK



Content Distribution Network (CDN)

Global CDN
107 Edge Locations

96 Edge Locations and
11 Regional Edge Caches,
in 55 cities and across
24 countries

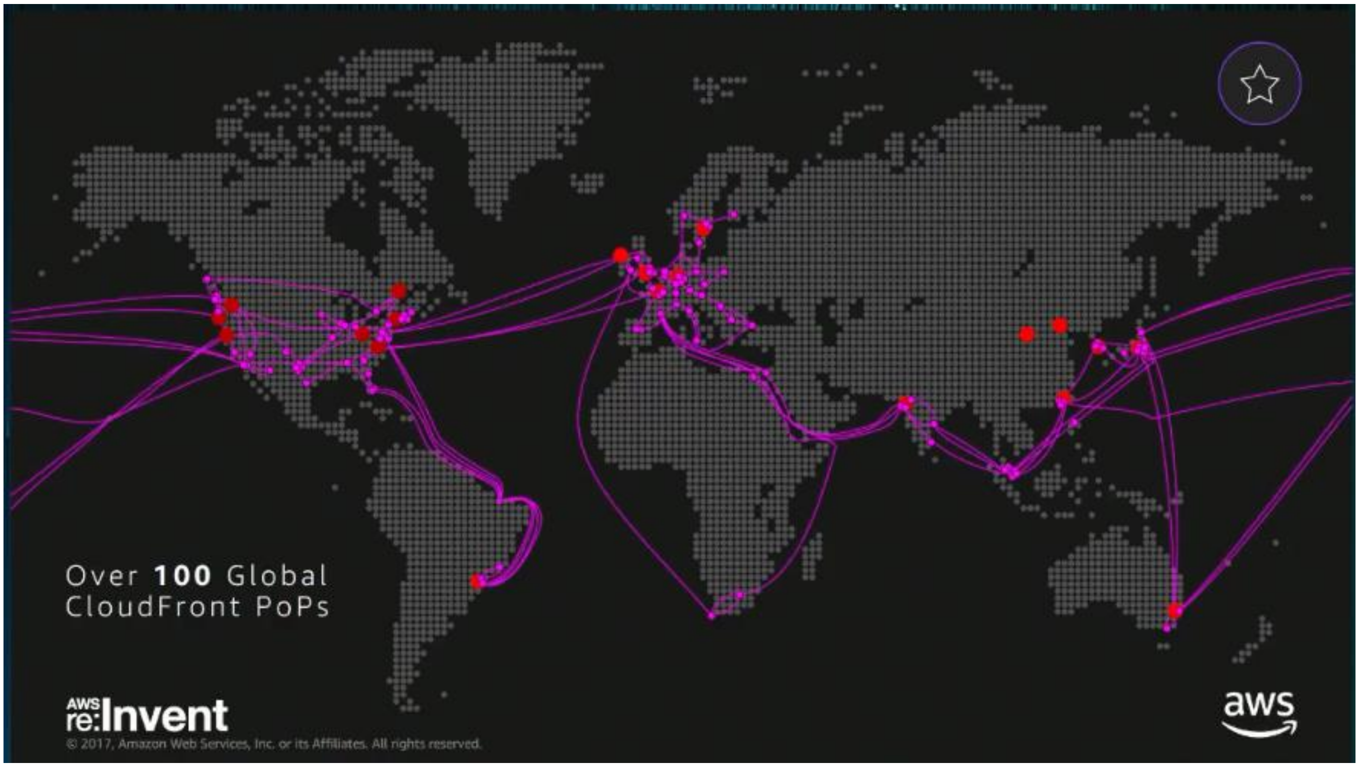
Secure Content
at the Edge

both network
and application
level protection

High Performance

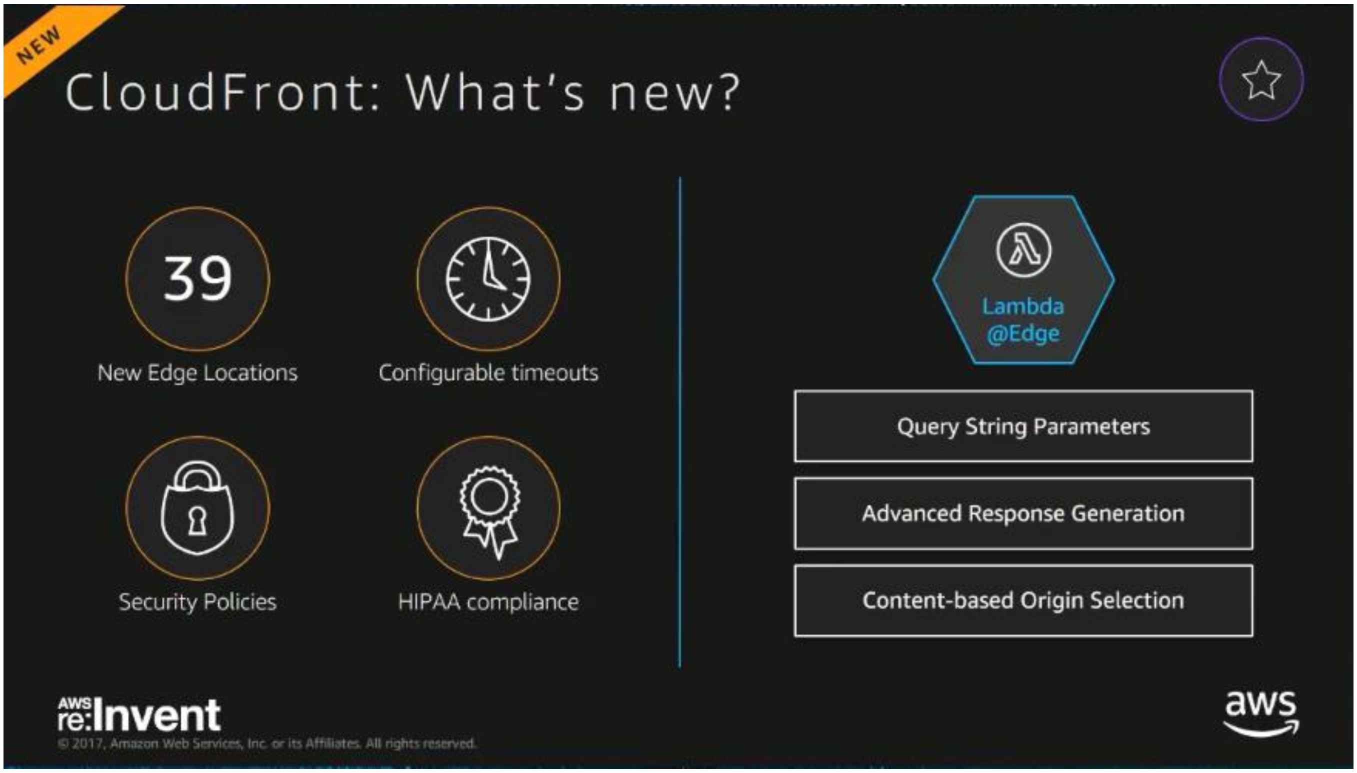
optimized for low
latency and high
data transfer speeds

CloudFront allows you to do security at the edge using SNI or SSL termination right at the edge closer to your customer to improve latency.



Over **100** Global CloudFront PoPs

***Every CloudFront POP is connected to the Amazon backbone*.**



NEW

CloudFront: What's new?

39 New Edge Locations

Configurable timeouts

Security Policies

HIPAA compliance

Lambda @Edge

Query String Parameters

Advanced Response Generation

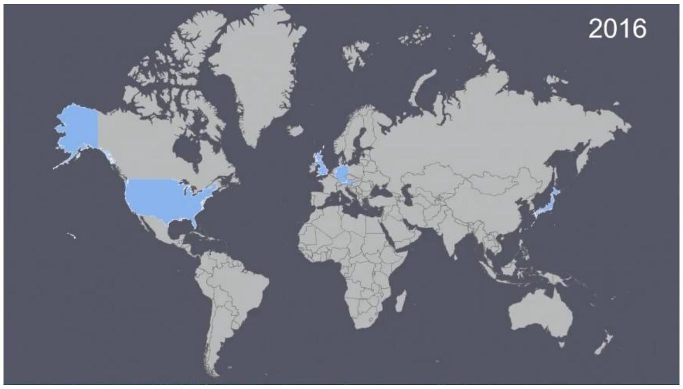
Content-based Origin Selection

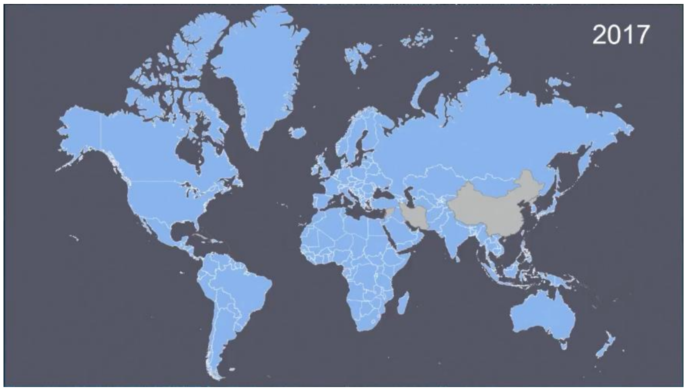
Olga Hall
Senior Manager, Technical Programs,
Amazon Instant Video

SUBSCRIPTION

TRANSACTIONAL

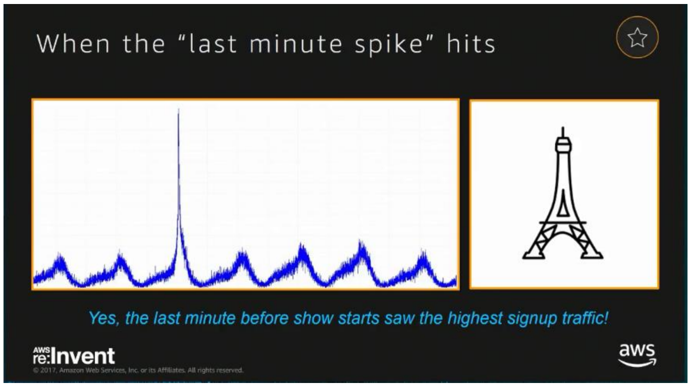
CHANNELS





WINTER IN JULY

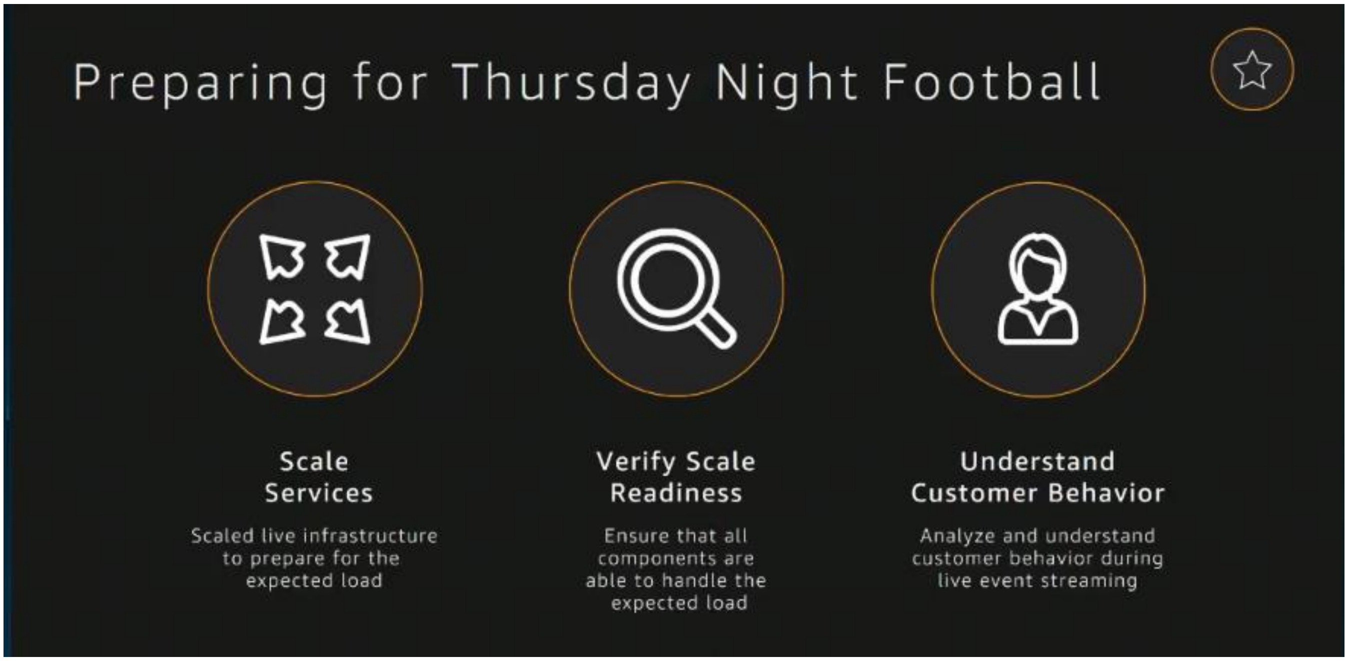
"Game of Thrones is the most popular series of all time … by a long way. It's probably at least **three times** the audience in terms of any other single show"



When the "last minute spike" hits

Yes, the last minute before show starts saw the highest signup traffic!

You need to think through how you architect your system to handle spikes. There is no 2nd chances for live events



Preparing for Thursday Night Football

Scale Services

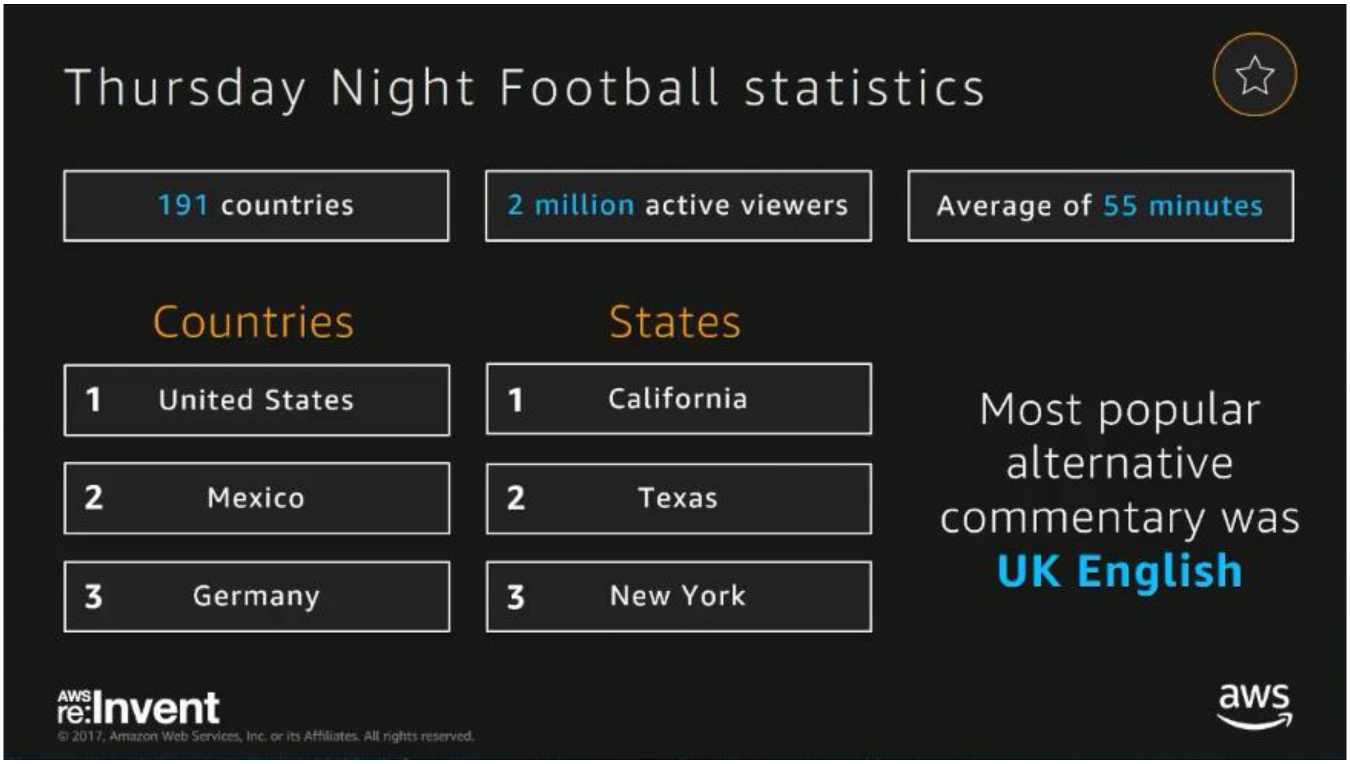
Scaled live infrastructure to prepare for the expected load

Verify Scale Readiness

Ensure that all components are able to handle the expected load

Understand Customer Behavior

Analyze and understand customer behavior during live event streaming



Thursday Night Football statistics

191 countries

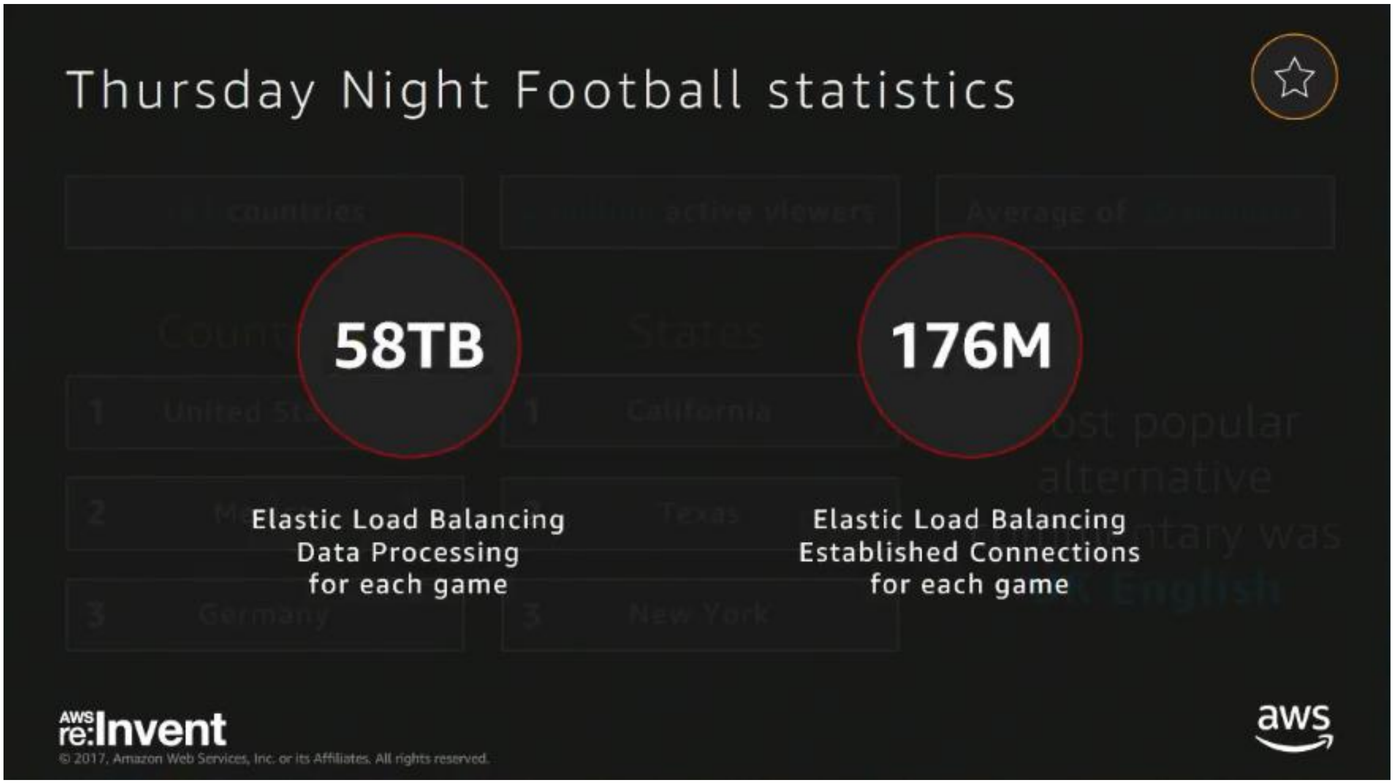
2 million active viewers

Average of 55 minutes

Countries	
1	United States
2	Mexico
3	Germany

States	
1	California
2	Texas
3	New York

Most popular alternative commentary was **UK English**



Thursday Night Football statistics

58TB

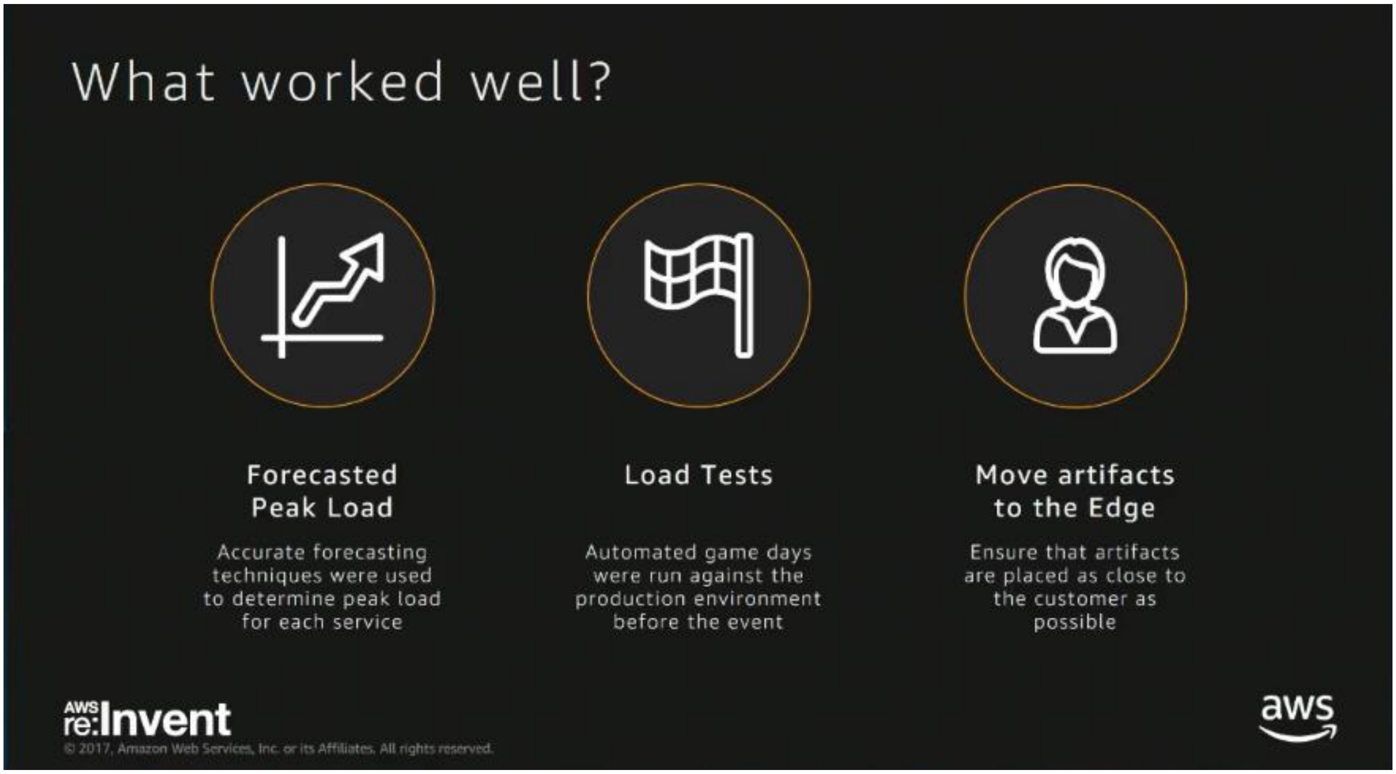
Elastic Load Balancing
Data Processing
for each game

176M

Elastic Load Balancing
Established Connections
for each game

AWS re:Invent
aws

Caching strategies mostly do not work for personalized services, you need to think the whole architecture carefully for speed and resilience



What worked well?

Forecasted Peak Load

Accurate forecasting techniques were used to determine peak load for each service

Load Tests

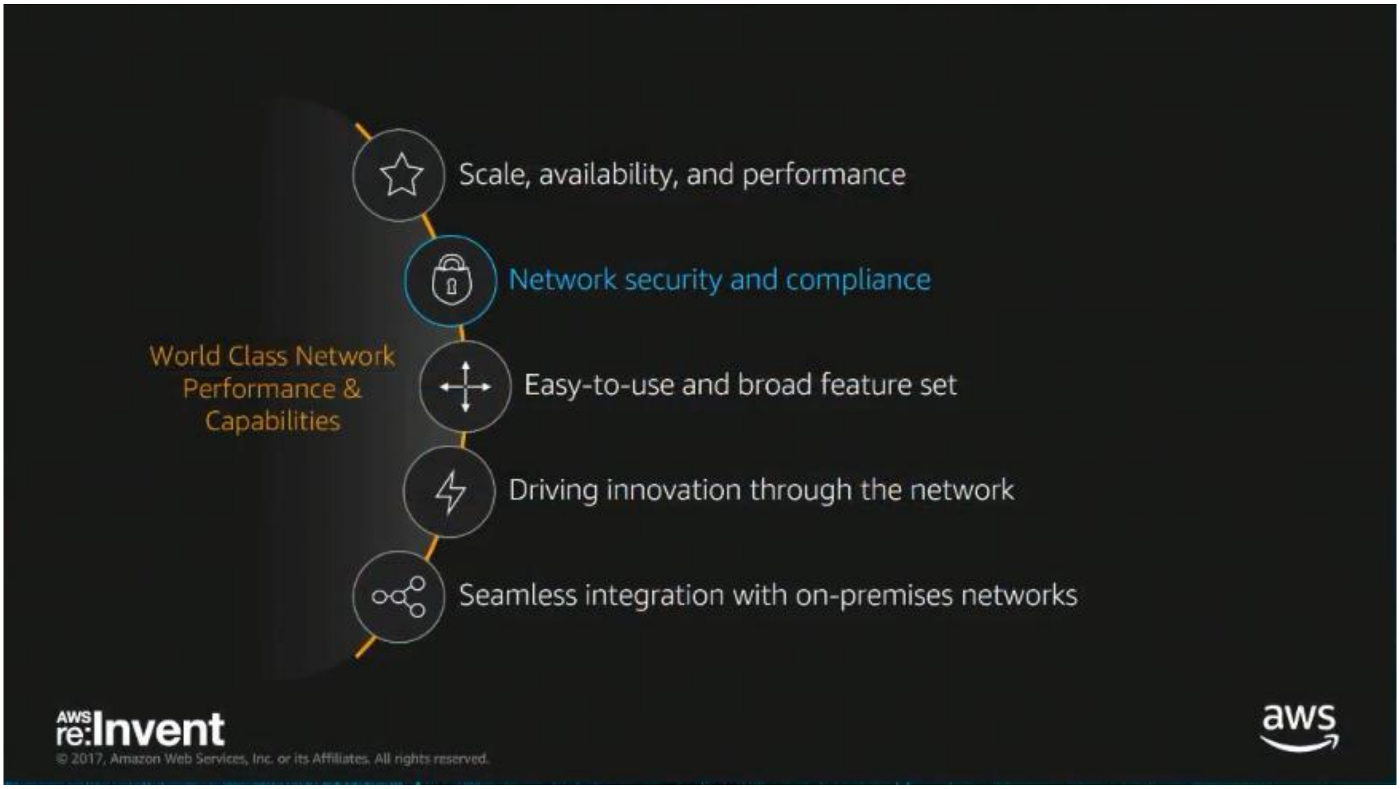
Automated game days were run against the production environment before the event

Move artifacts to the Edge

Ensure that artifacts are placed as close to the customer as possible

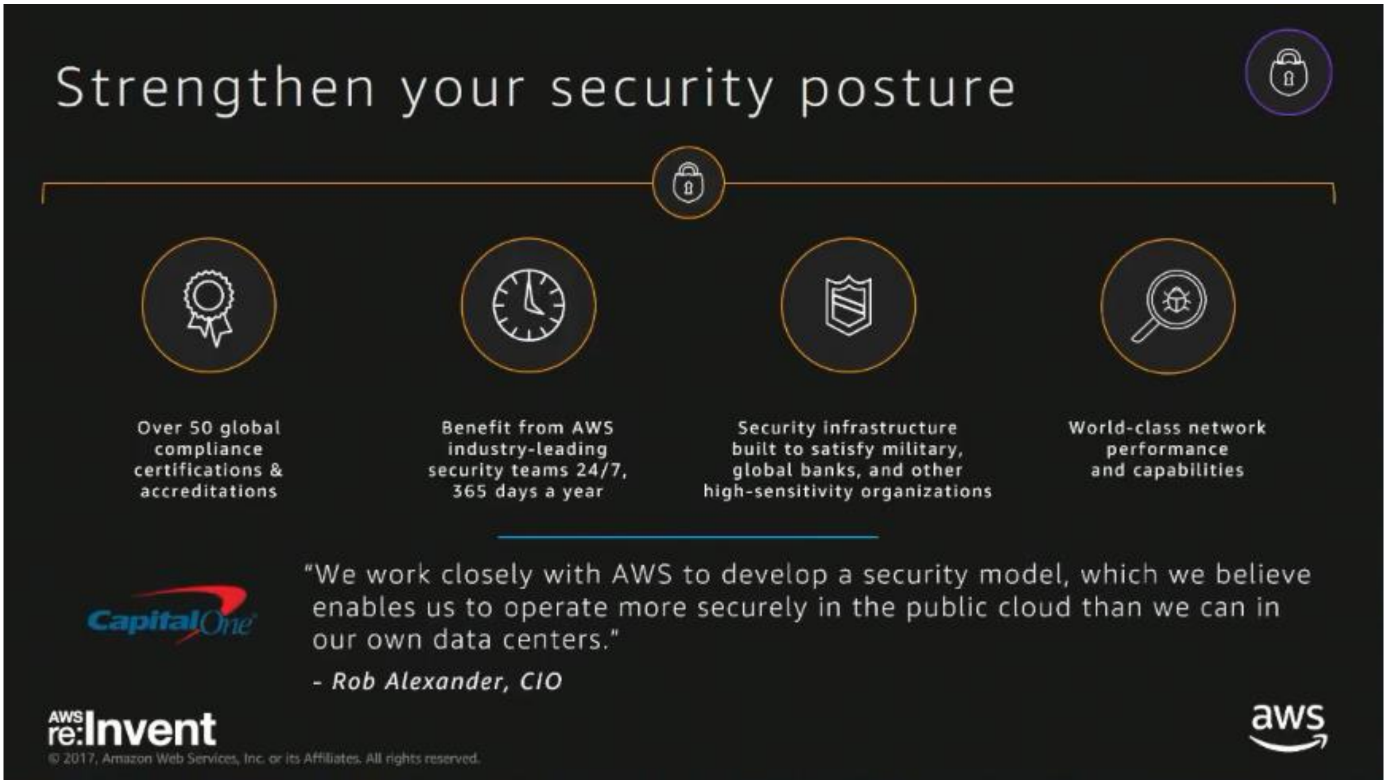
AWS re:Invent
aws

THE NEW NORMAL



World Class Network Performance & Capabilities

- Scale, availability, and performance
- Network security and compliance
- Easy-to-use and broad feature set
- Driving innovation through the network
- Seamless integration with on-premises networks



Strengthen your security posture

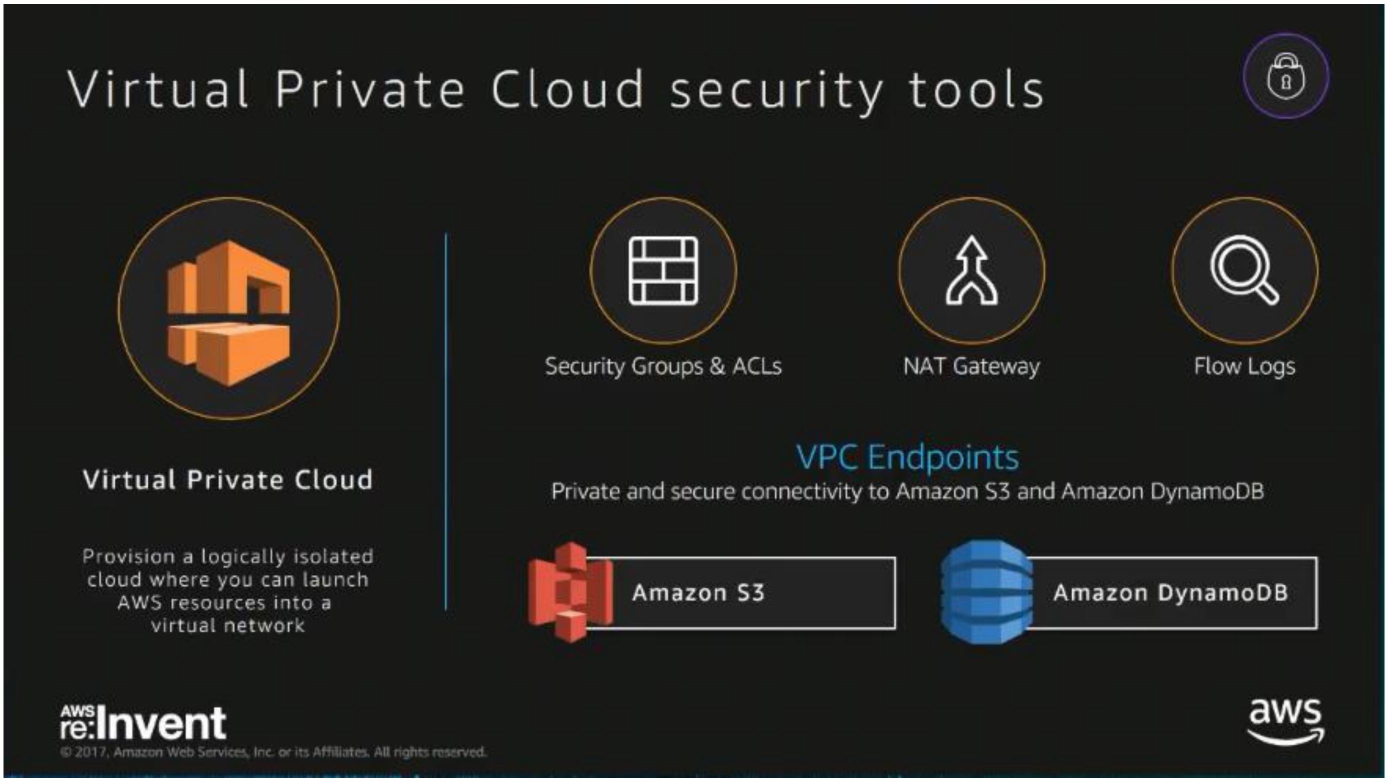
Over 50 global compliance certifications & accreditations

Benefit from AWS industry-leading security teams 24/7, 365 days a year

Security infrastructure built to satisfy military, global banks, and other high-sensitivity organizations

World-class network performance and capabilities

> "We work closely with AWS to develop a security model, which we believe enables us to operate more securely in the public cloud than we can in our own data centers."
>
> *- Rob Alexander, CIO*



Virtual Private Cloud security tools

Virtual Private Cloud

Provision a logically isolated cloud where you can launch AWS resources into a virtual network

Security Groups & ACLs

NAT Gateway

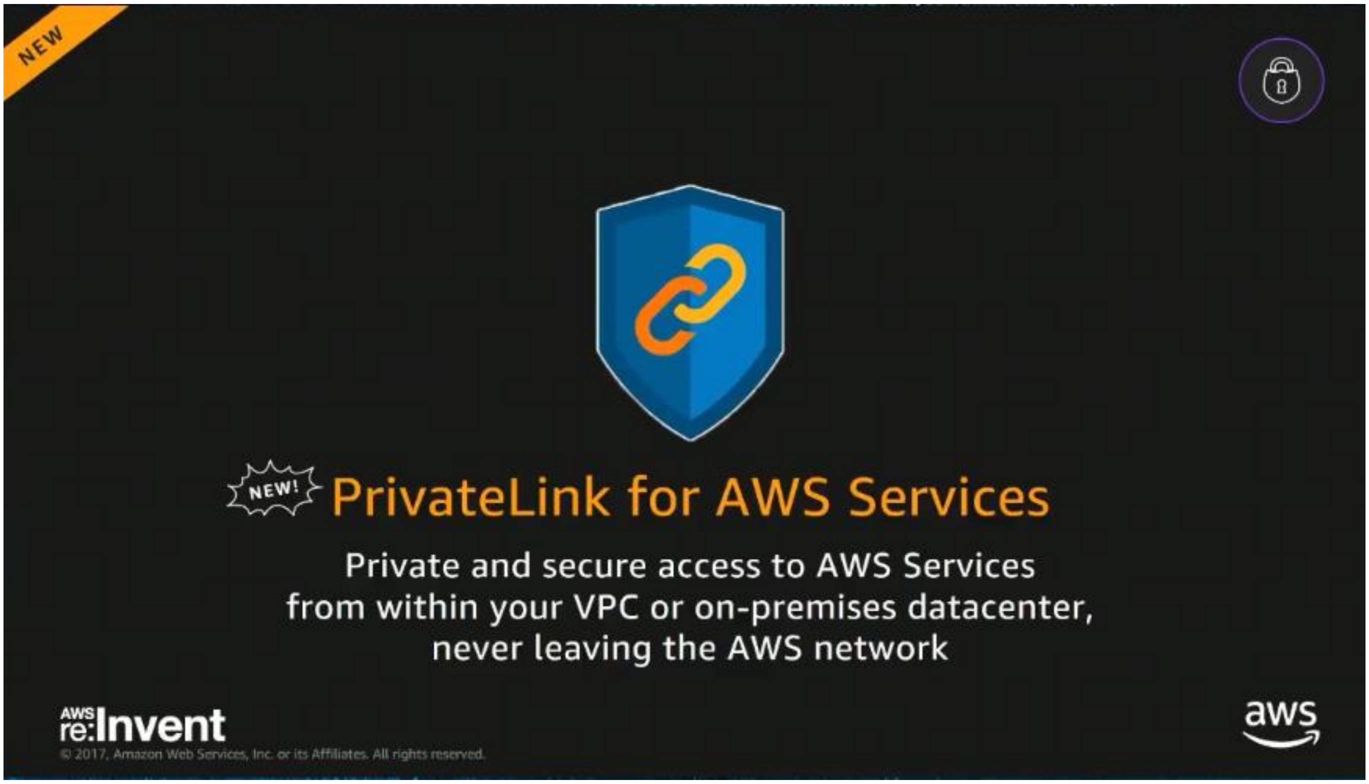
Flow Logs

VPC Endpoints

Private and secure connectivity to Amazon S3 and Amazon DynamoDB

Amazon S3

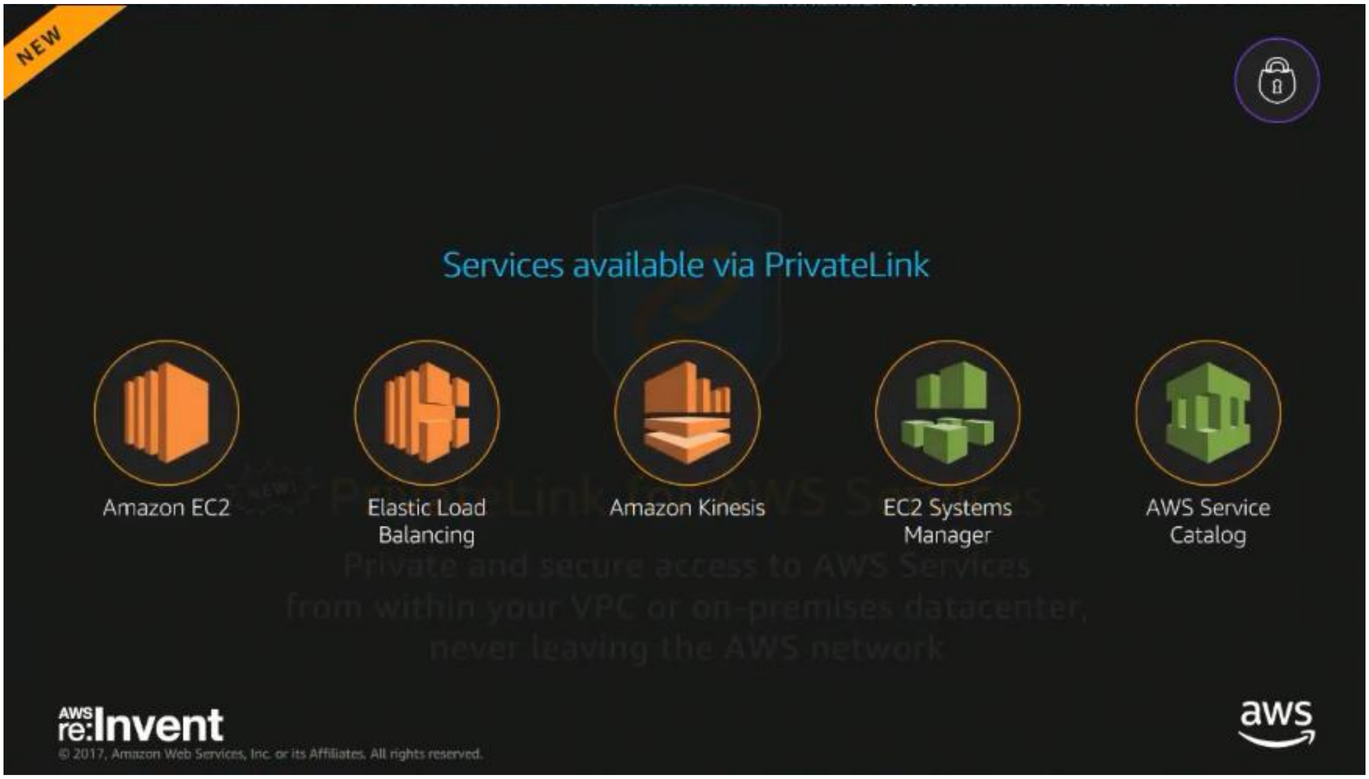
Amazon DynamoDB



NEW

NEW! PrivateLink for AWS Services

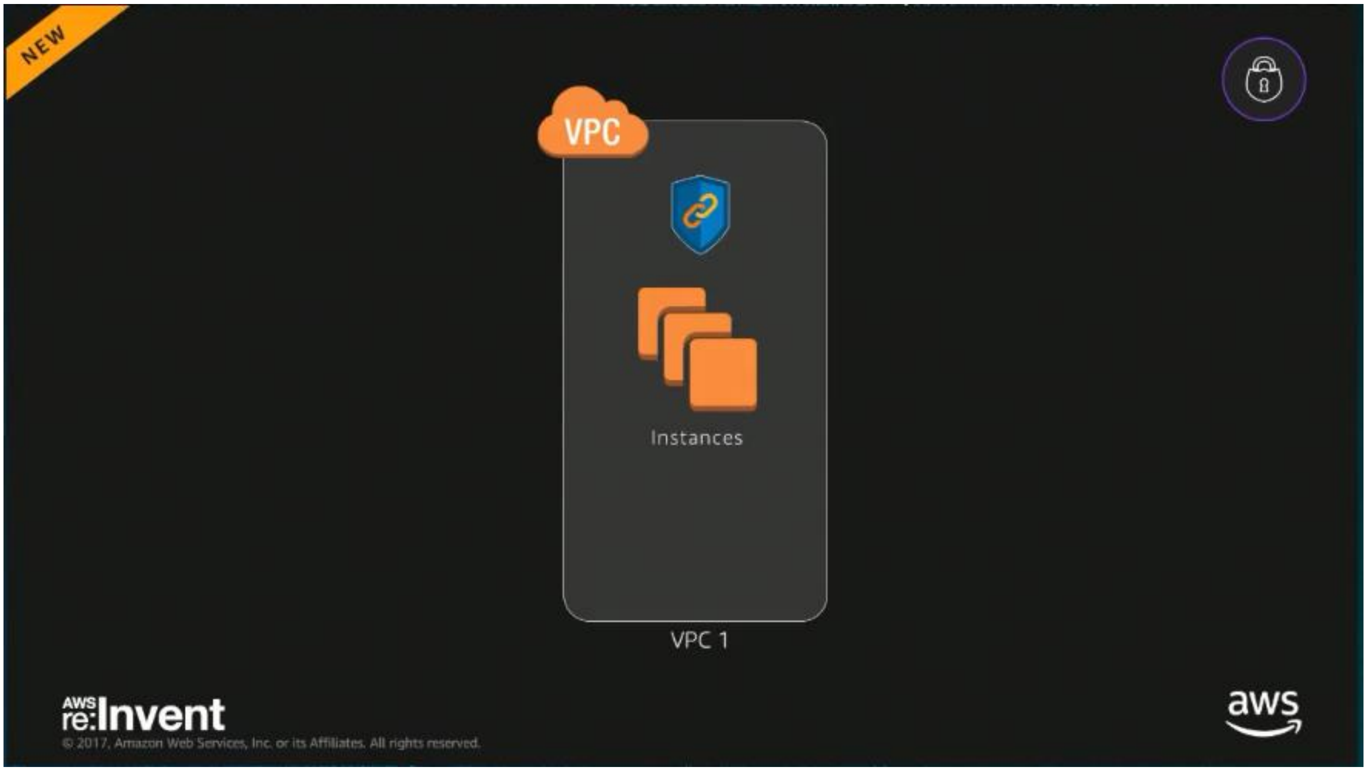
Private and secure access to AWS Services
from within your VPC or on-premises datacenter,
never leaving the AWS network



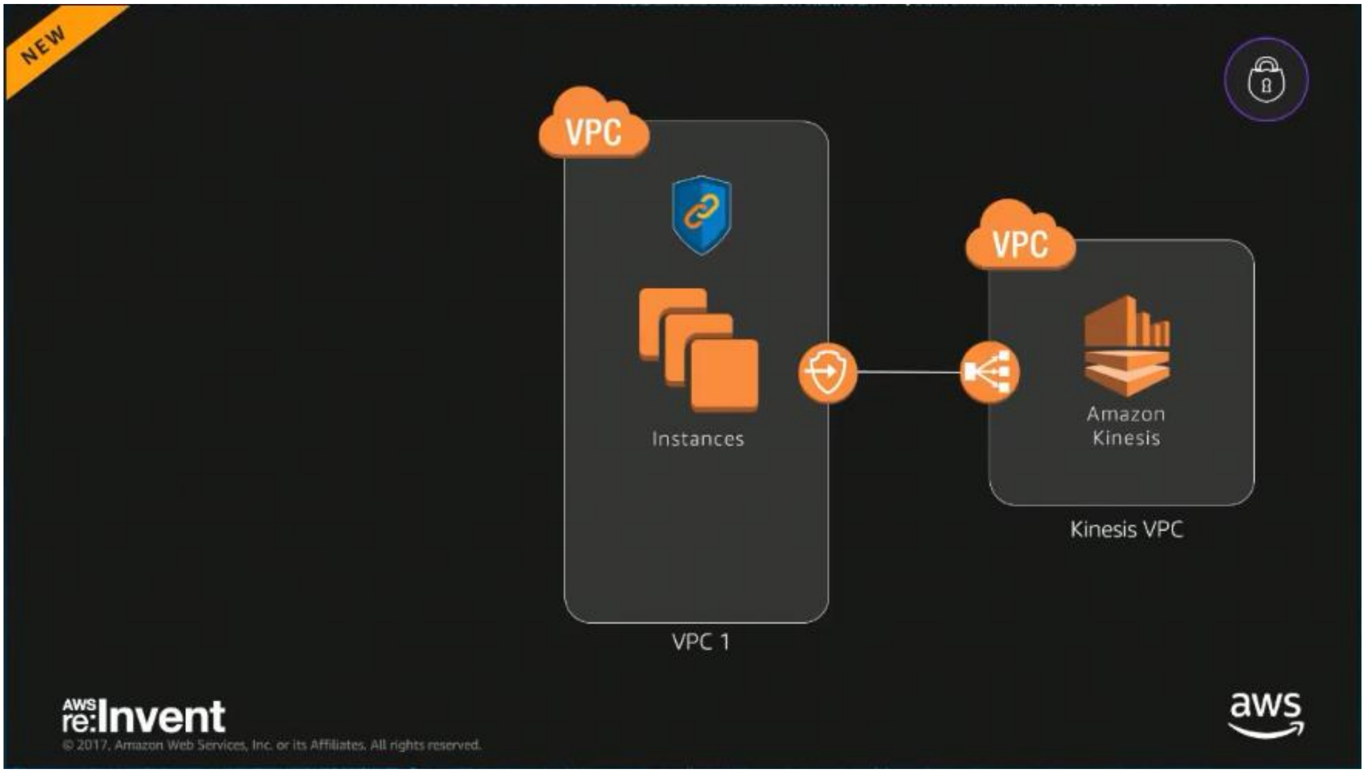
NEW

Services available via PrivateLink

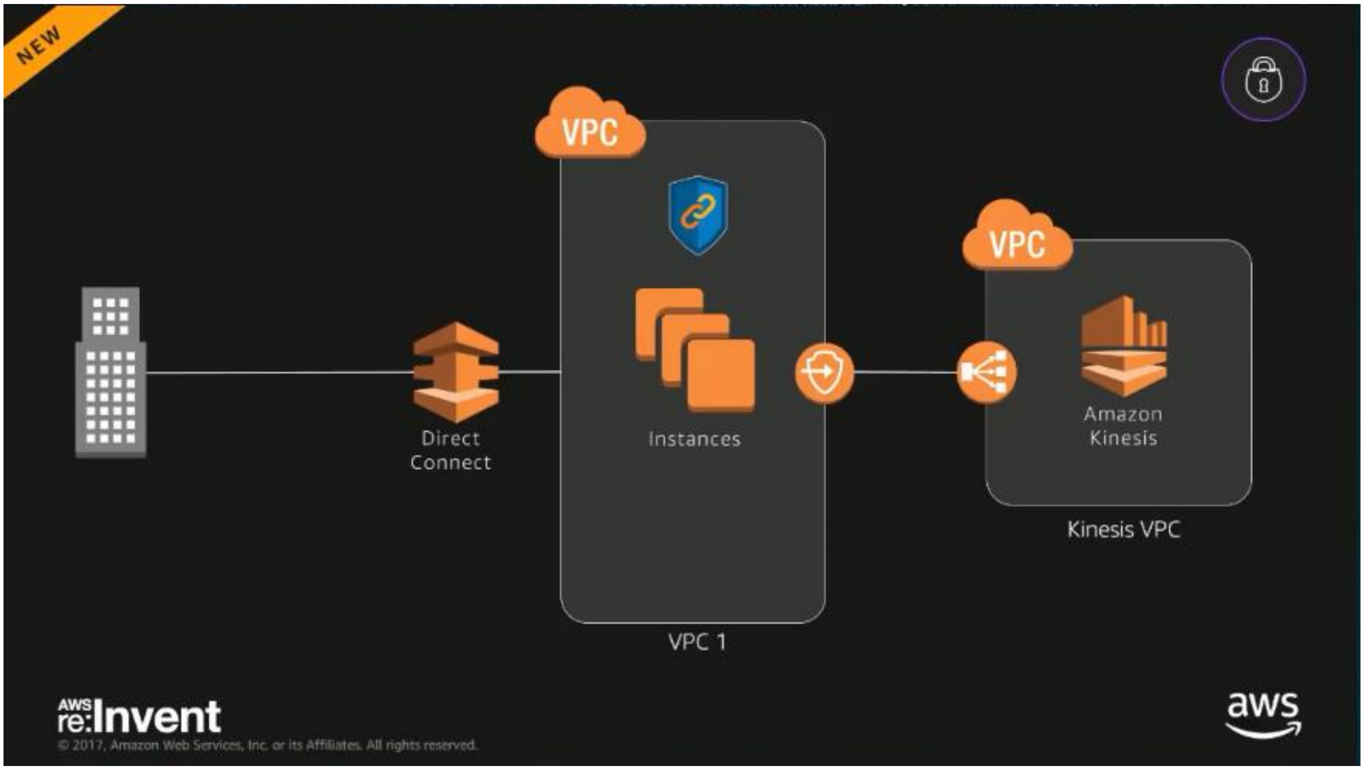
NEW! PrivateLink for AWS Services
Private and secure access to AWS Services
from within your VPC or on-premises datacenter,
never leaving the AWS network


NEW
VPC
Instances
VPC 1
AWS re:Invent
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
aws

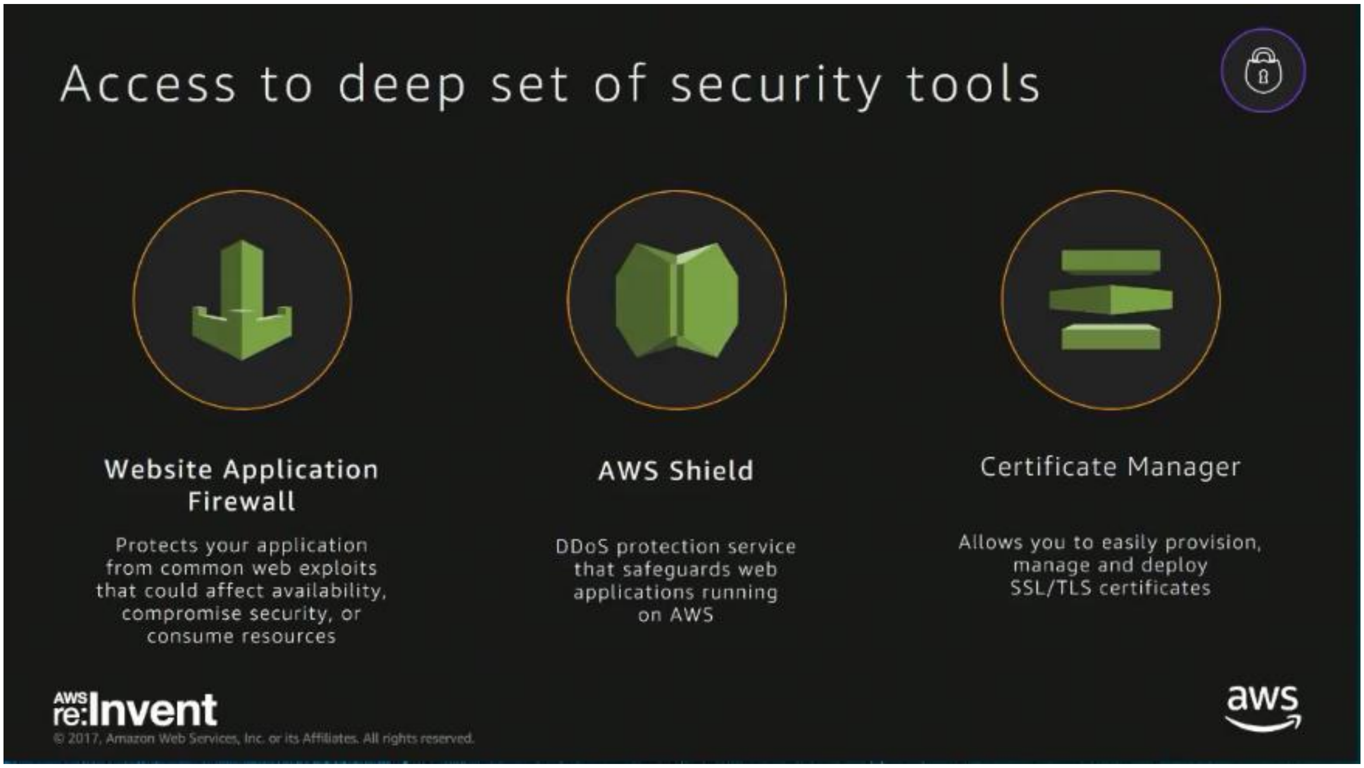
With ***PrivateLink***, you get a private IP address inside your VPC that you can talk to. You simply talk to that private IP address to get the service at the end of that PrivateLink.


NEW
VPC
Instances
VPC 1
VPC
Amazon Kinesis
Kinesis VPC
AWS re:Invent
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
aws

The Kinesis VPC is owned by the Kinesis service team and that is where they are running their Kinesis service on EC2, they simply put a Network Load Balancer in their VPC and then share a private IP address into the VPC of any customer that wants to use Kinesis inside their VPC. This provides a private, secure connectivity from a private address inside your private network to whatever AWS service you need.



PrivateLink is also available over ***DirectConnect***, we can now use Kinesis from within our data centers within our CIDR range without having to go over the internet.



Access to deep set of security tools

Website Application Firewall

Protects your application from common web exploits that could affect availability, compromise security, or consume resources

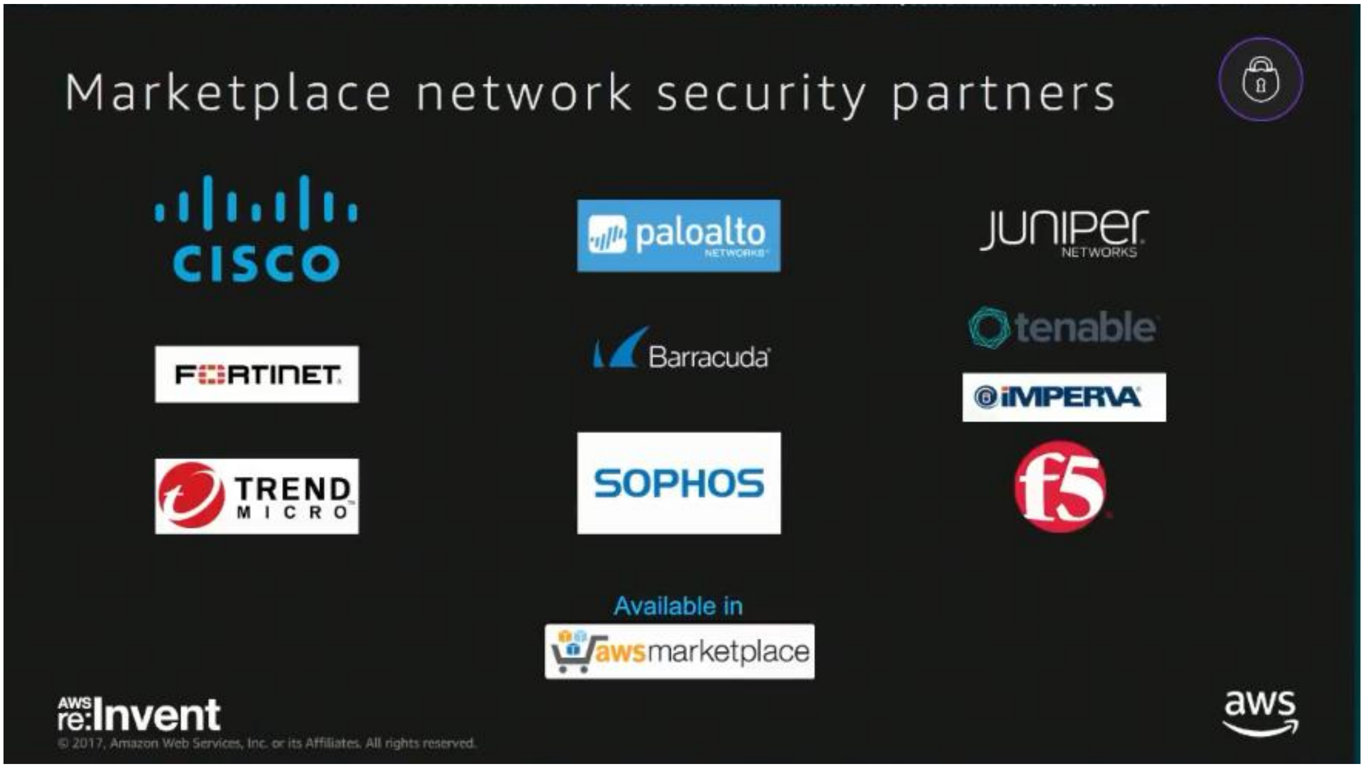
AWS Shield

DDoS protection service that safeguards web applications running on AWS

Certificate Manager

Allows you to easily provision, manage and deploy SSL/TLS certificates

Everybody gets AWS Shield for DDOS protection



Marketplace network security partners

CISCO

paloalto NETWORKS

JUNIPER NETWORKS

FORTINET

Barracuda

tenable

IMPERVA

TREND MICRO

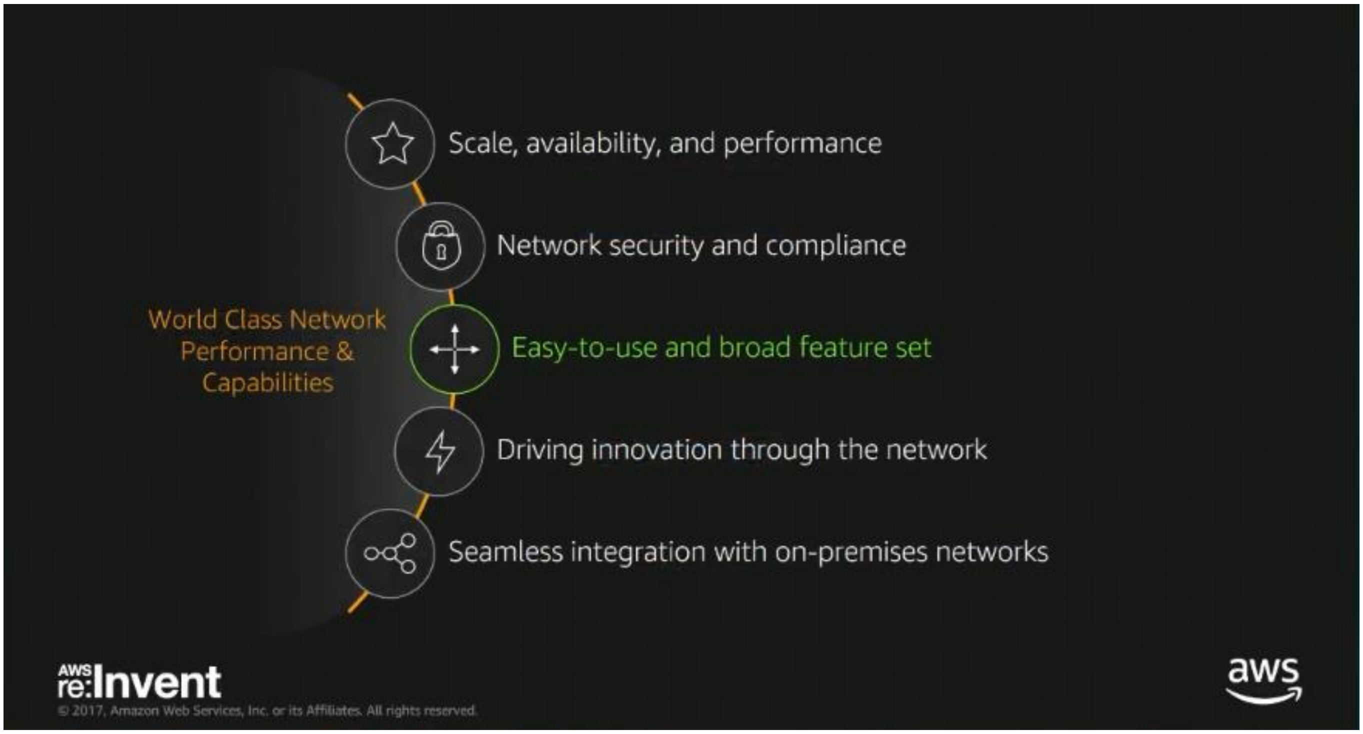
SOPHOS

f5

Available in awsmarketplace

AWS re:Invent

aws

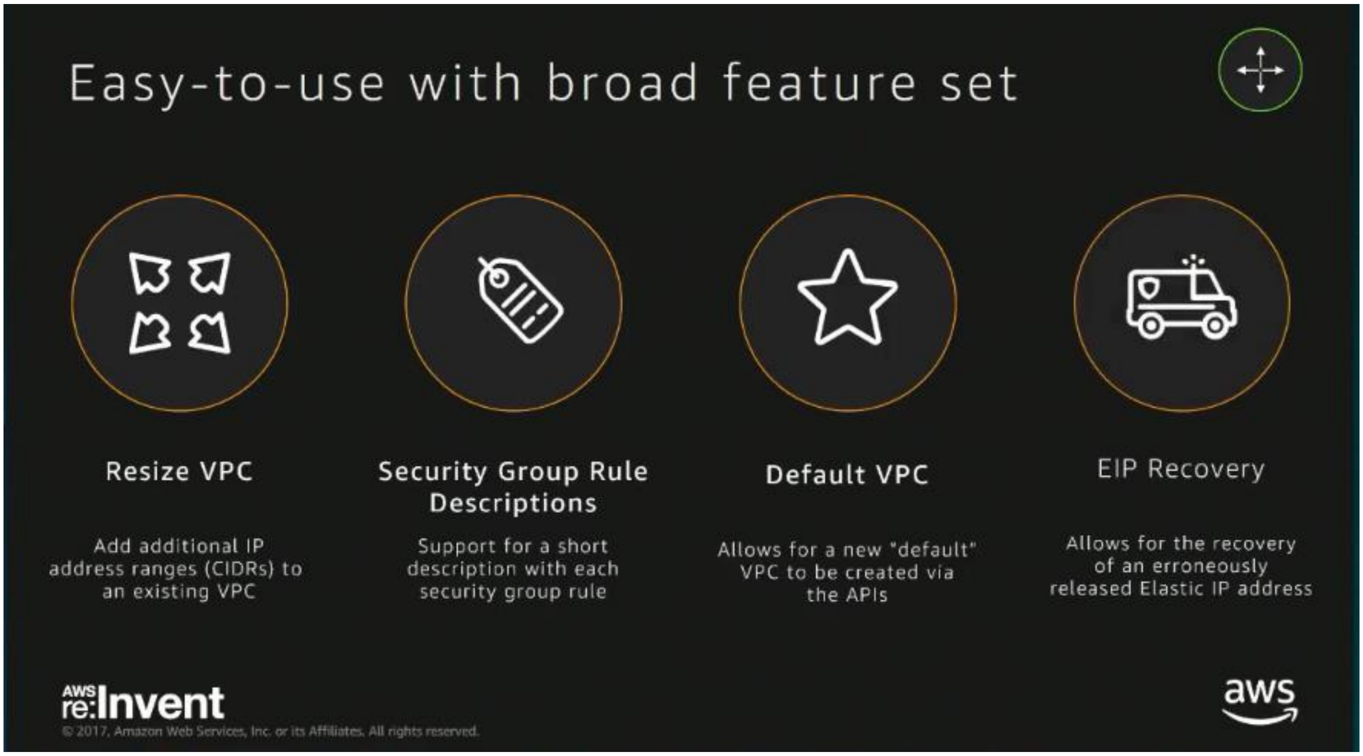


World Class Network Performance & Capabilities

- Scale, availability, and performance
- Network security and compliance
- Easy-to-use and broad feature set
- Driving innovation through the network
- Seamless integration with on-premises networks

AWS re:Invent

aws



Easy-to-use with broad feature set

Resize VPC

Add additional IP address ranges (CIDRs) to an existing VPC

Security Group Rule Descriptions

Support for a short description with each security group rule

Default VPC

Allows for a new "default" VPC to be created via the APIs

EIP Recovery

Allows for the recovery of an erroneously released Elastic IP address

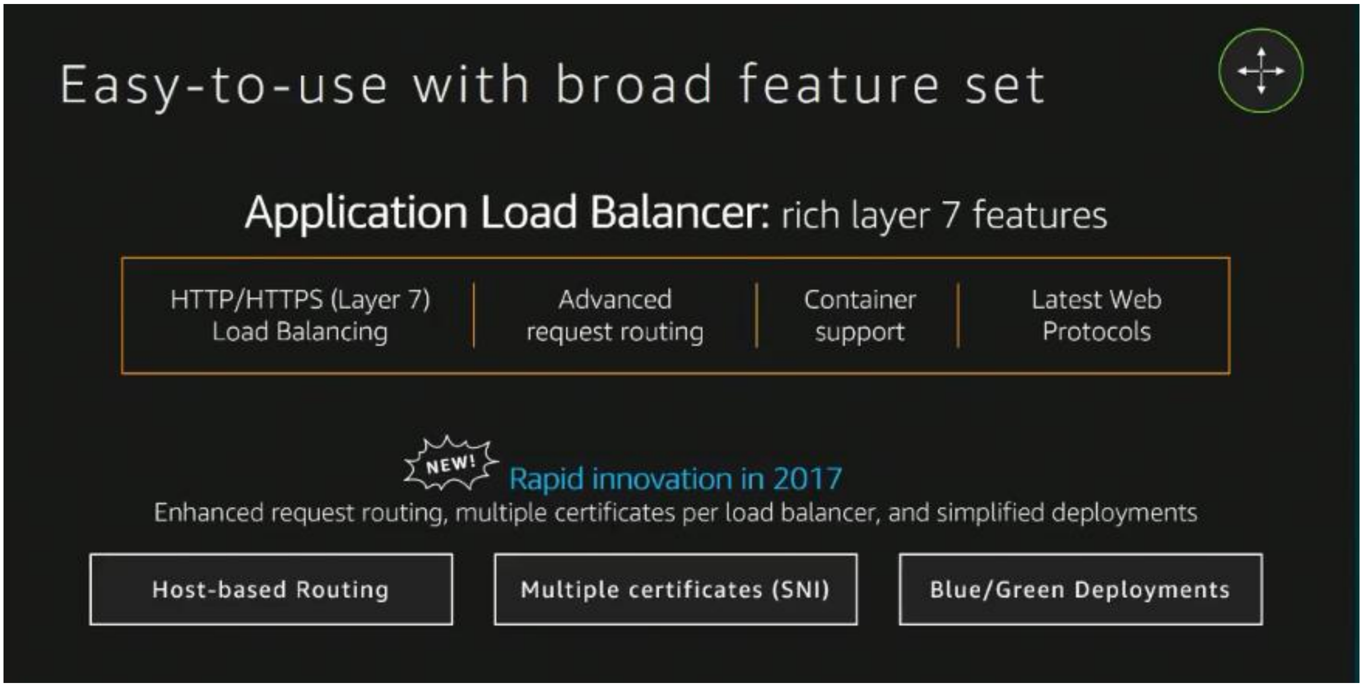
AWS re:Invent

aws

Resize VPC allows you to launch, resize and configure your VPC CIDR blocks.

APPLICATION LOAD BALANCER

Network Load balancers NLB are all about performance and low latency, ***Application Load Balancers*** ALB are all about ***features*** and ***Layer 7***.



Easy-to-use with broad feature set

Application Load Balancer: rich layer 7 features

HTTP/HTTPS (Layer 7) Load Balancing | Advanced request routing | Container support | Latest Web Protocols

NEW! Rapid innovation in 2017

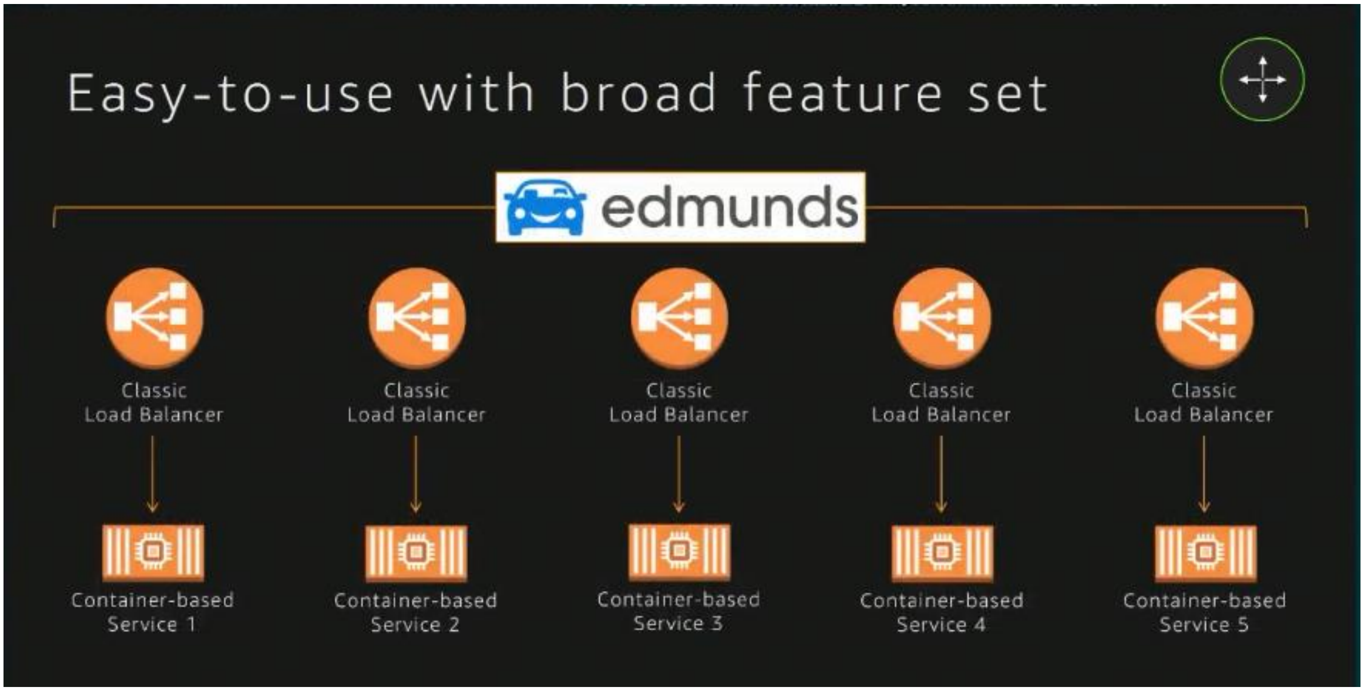
Enhanced request routing, multiple certificates per load balancer, and simplified deployments

Host-based Routing

Multiple certificates (SNI)

Blue/Green Deployments

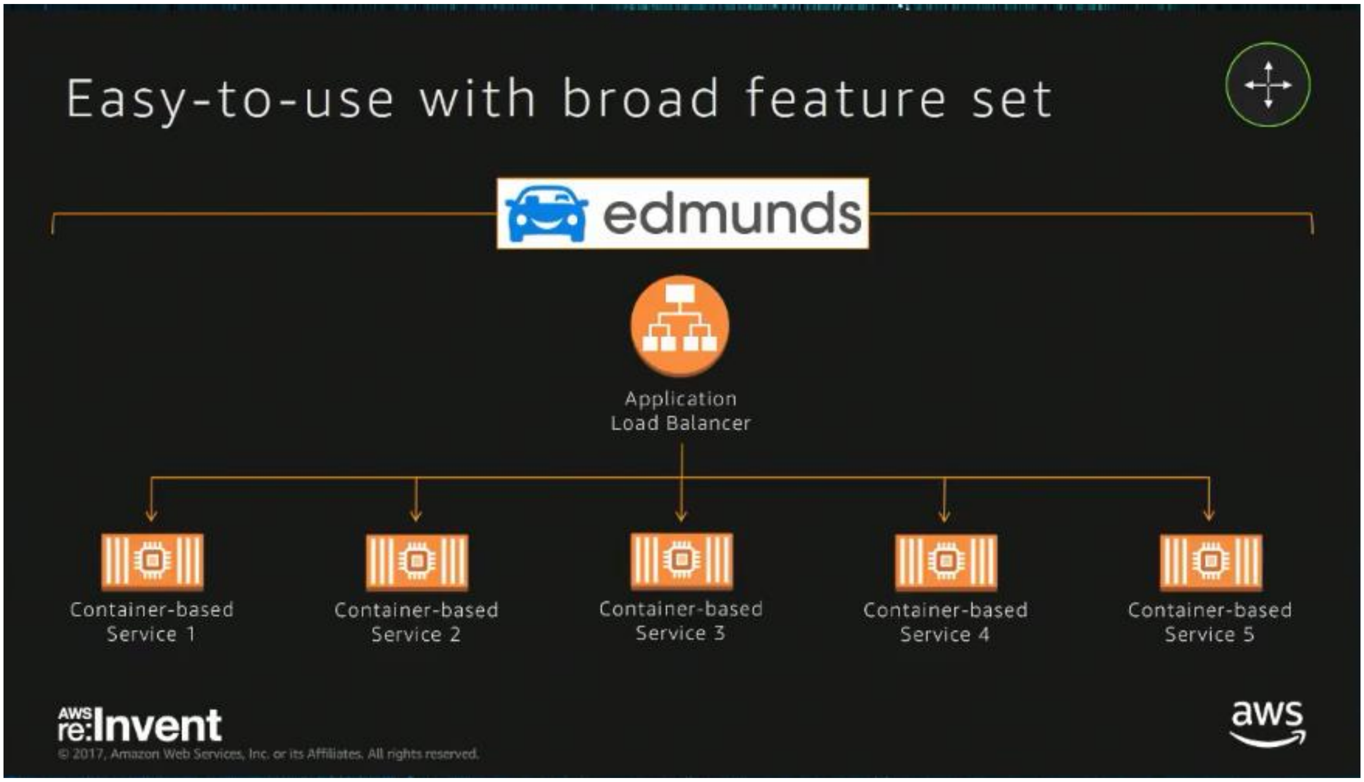
Host-based Routing allows you to host multiple websites with hostnames as part of the DNS name on a single load balancer. ***Multiple Certificates*** (with SNI browser support). ***Blue/Green deployment*** using CodeDeploy to safely deploy to a load balancer.



Easy-to-use with broad feature set

edmunds
Classic Load Balancer
Classic Load Balancer
Classic Load Balancer
Classic Load Balancer
Classic Load Balancer
Container-based Service 1
Container-based Service 2
Container-based Service 3
Container-based Service 4
Container-based Service 5

Edmunds runs an architecture having a container stack with a lot of classic LBs. with Host-based routing and ability to use SNI in an application load balancer, Edmunds have since migrated this architecture to below



Easy-to-use with broad feature set

edmunds

Application Load Balancer

Container-based Service 1

Container-based Service 2

Container-based Service 3

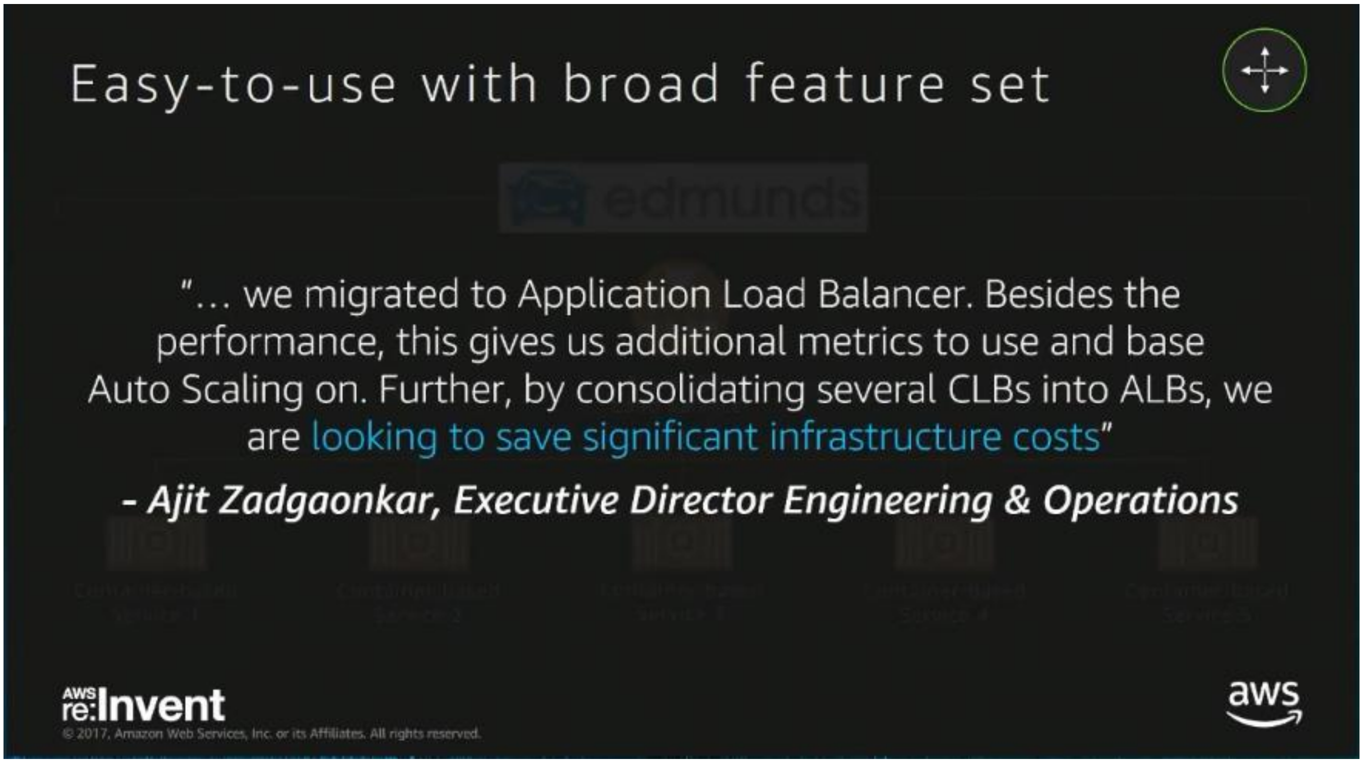
Container-based Service 4

Container-based Service 5

AWS re:Invent

aws

They can now host hundreds of websites on a single ALB, saving a lot of money.



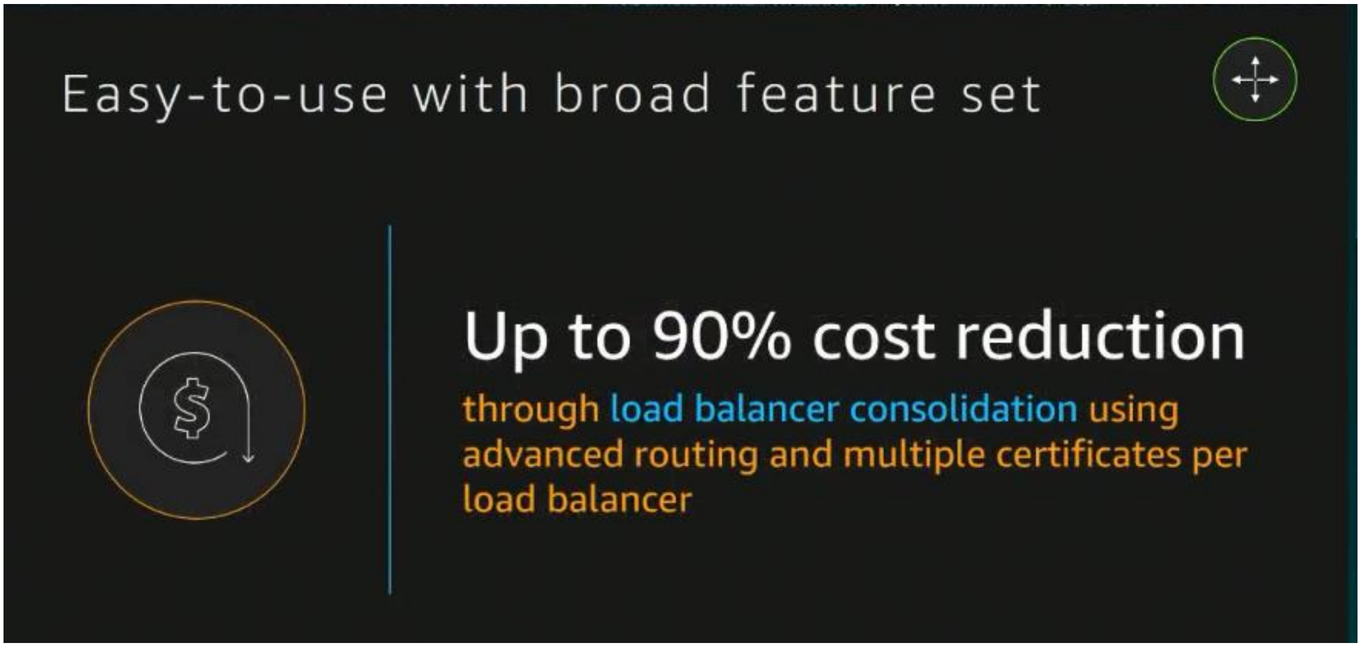
Easy-to-use with broad feature set

"… we migrated to Application Load Balancer. Besides the performance, this gives us additional metrics to use and base Auto Scaling on. Further, by consolidating several CLBs into ALBs, we are looking to save significant infrastructure costs"

- Ajit Zadgaonkar, Executive Director Engineering & Operations

AWS re:Invent

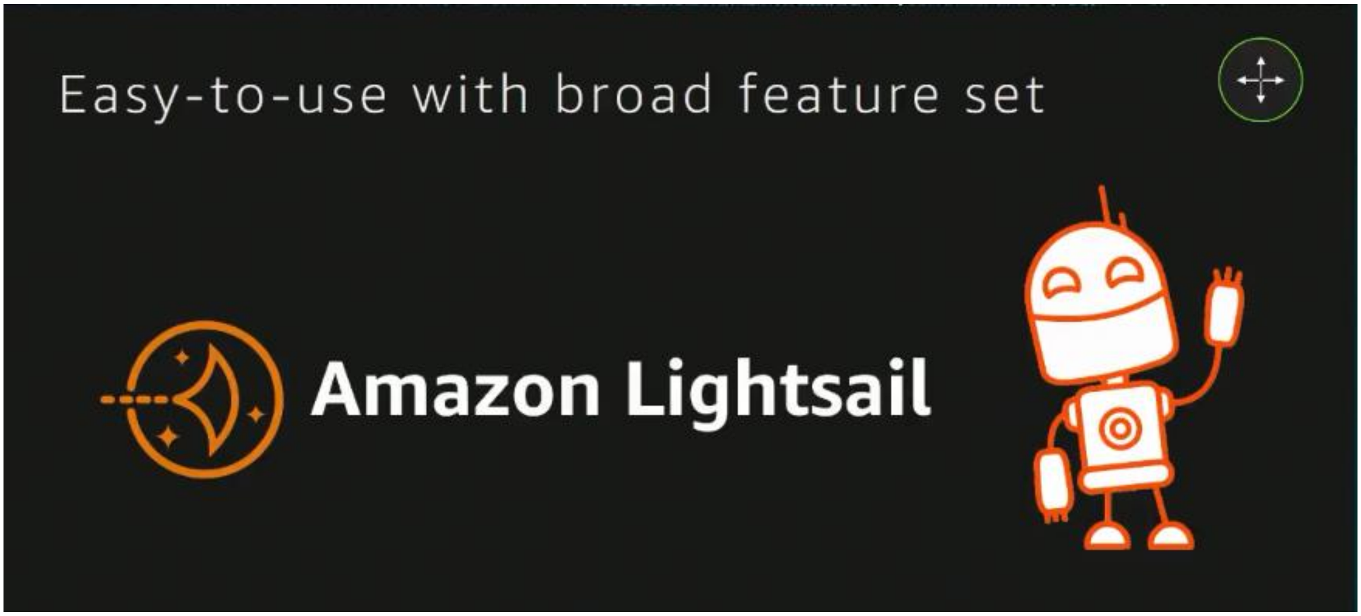
aws



Easy-to-use with broad feature set

Up to 90% cost reduction

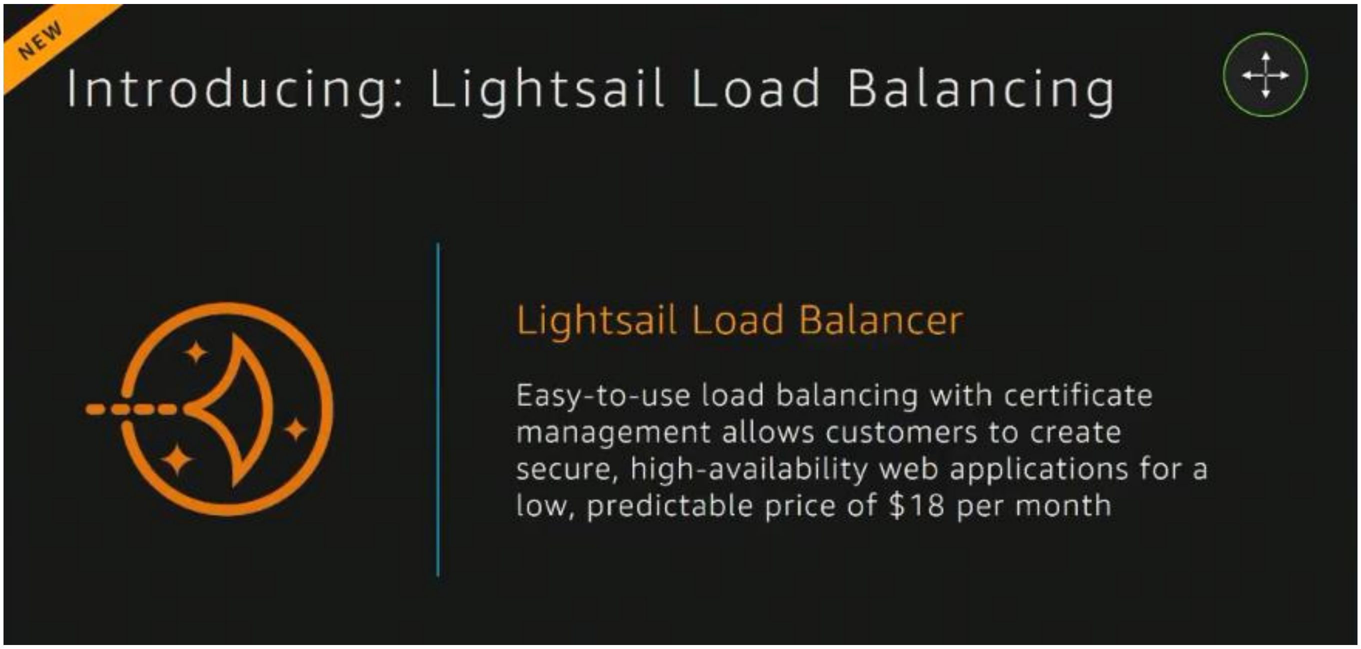
through load balancer consolidation using advanced routing and multiple certificates per load balancer



Easy-to-use with broad feature set

Amazon Lightsail

Amazon Lightsail is a sort of entry level offering for EC2, this is a host based experience that abstracts all the EC2 stuff away from the user



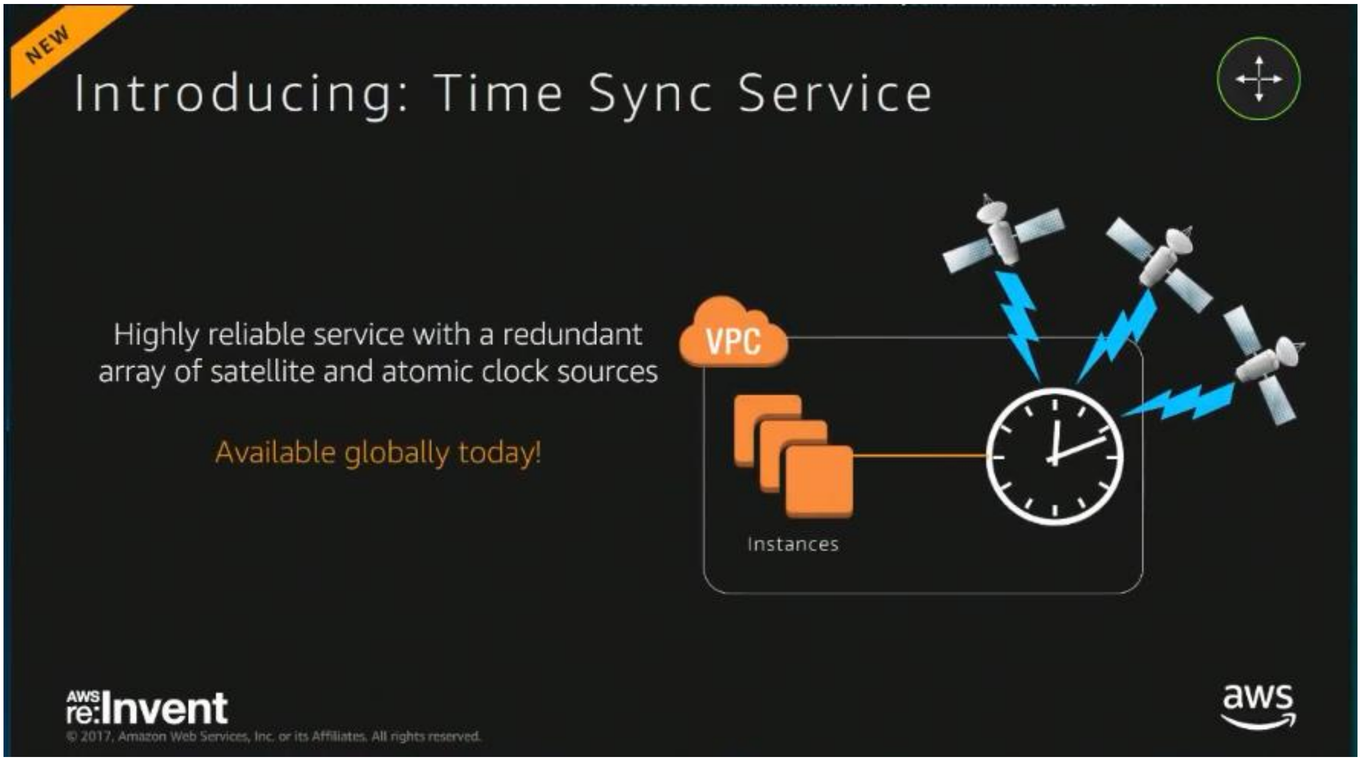
NEW

Introducing: Lightsail Load Balancing

Lightsail Load Balancer

Easy-to-use load balancing with certificate management allows customers to create secure, high-availability web applications for a low, predictable price of $18 per month

You can now get an ***Amazon Lightsail Load Balancer*** for $18/month



NEW

Introducing: Time Sync Service

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

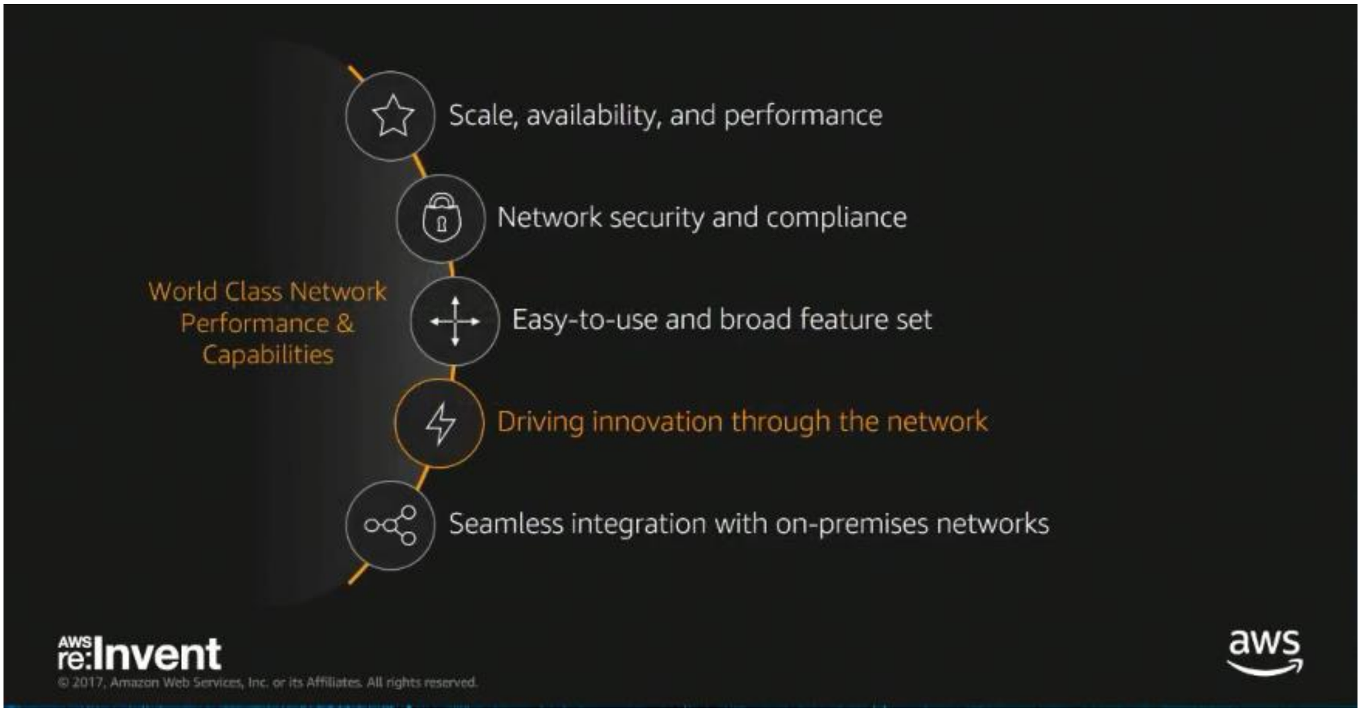
Available globally today!

AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

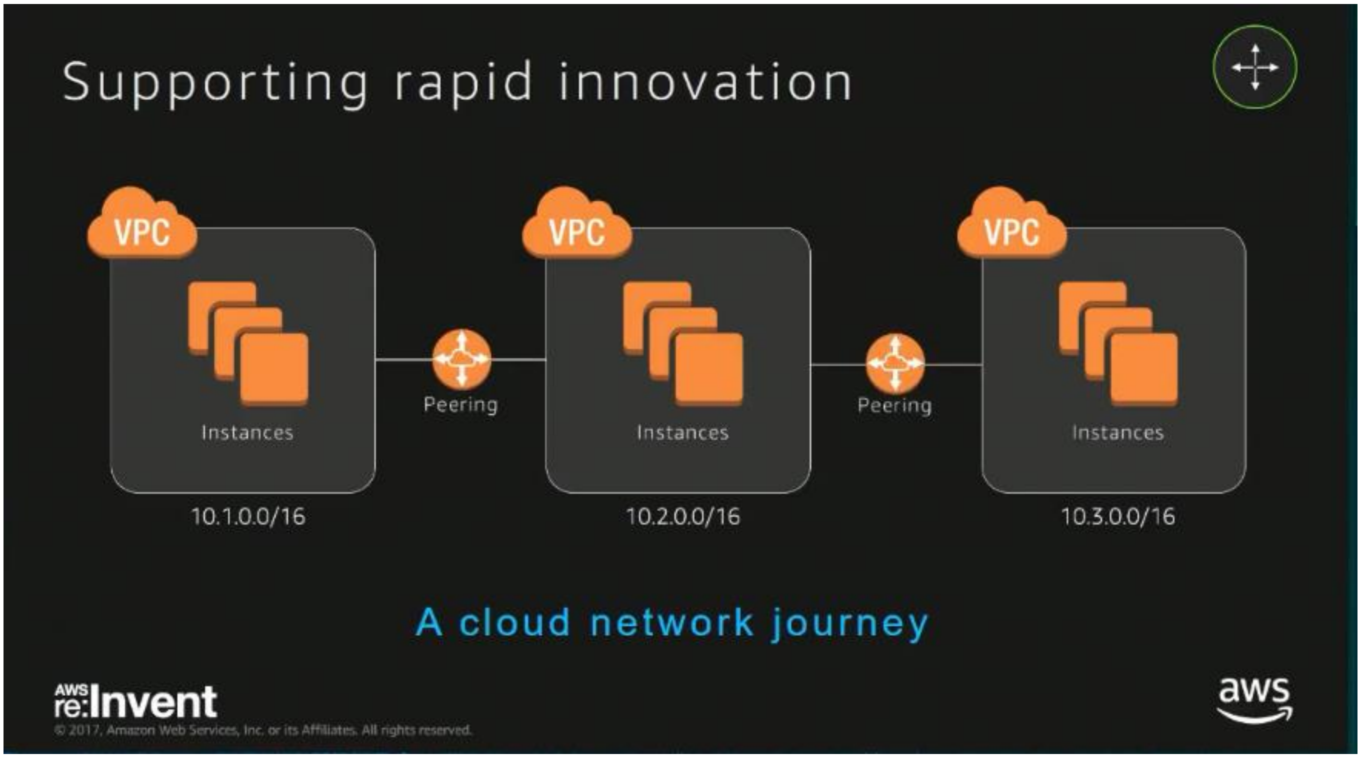
The ***Time Sync Service*** gives you a synchronized, atomic clock inside your VPC that you can use for all your VPC instance down to about 1ms of accuracy.



World Class Network Performance & Capabilities

- Scale, availability, and performance
- Network security and compliance
- Easy-to-use and broad feature set
- Driving innovation through the network
- Seamless integration with on-premises networks

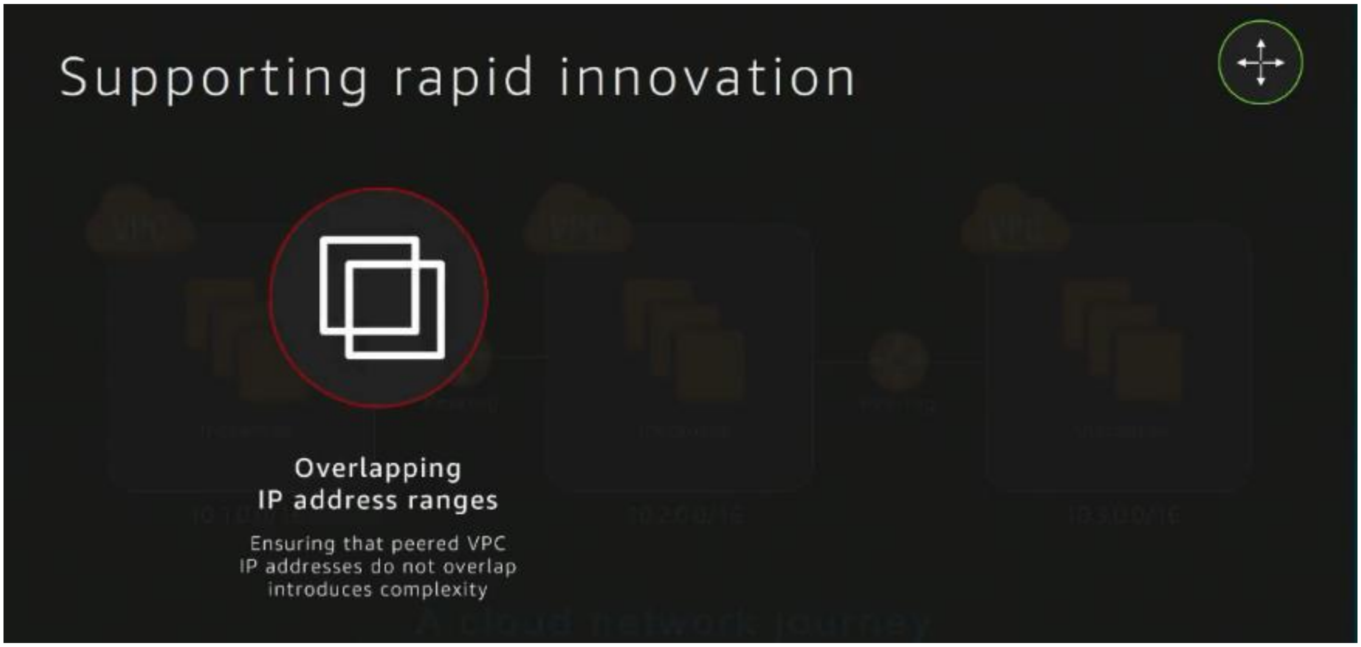
The network **MUST** support rapid innovation,
NOT slow things down



Supporting rapid innovation

A cloud network journey

A customer can now have many VPCs running at the same time, ***the system we have today for joining together VPCs is called Peering***. You can peer VPCs together using this peering approaches, but there are a few challenges with this.

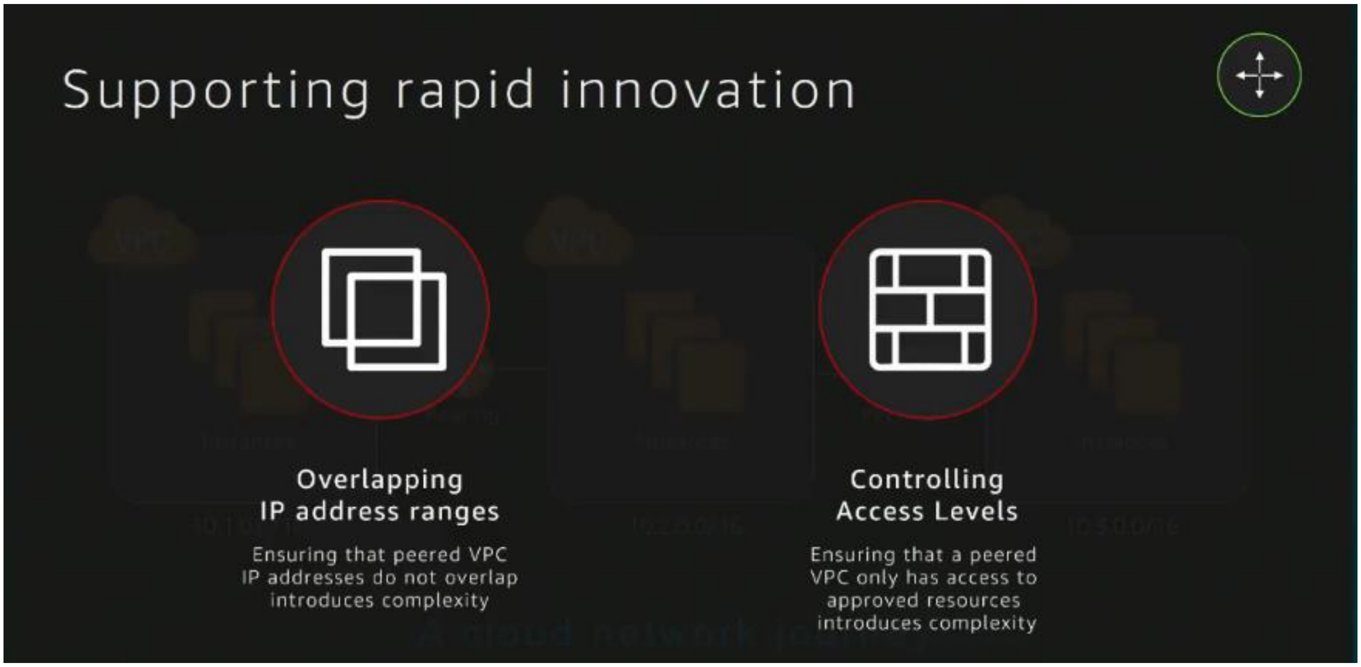


Supporting rapid innovation

Overlapping
IP address ranges

Ensuring that peered VPC
IP addresses do not overlap
introduces complexity

You can't peer 2 VPCs together if their IP address ranges overlap, managing the IPs and making sure they don't overlap becomes a lot of work for customers with multiple VPCs. You generally will need IP Management systems.



Supporting rapid innovation

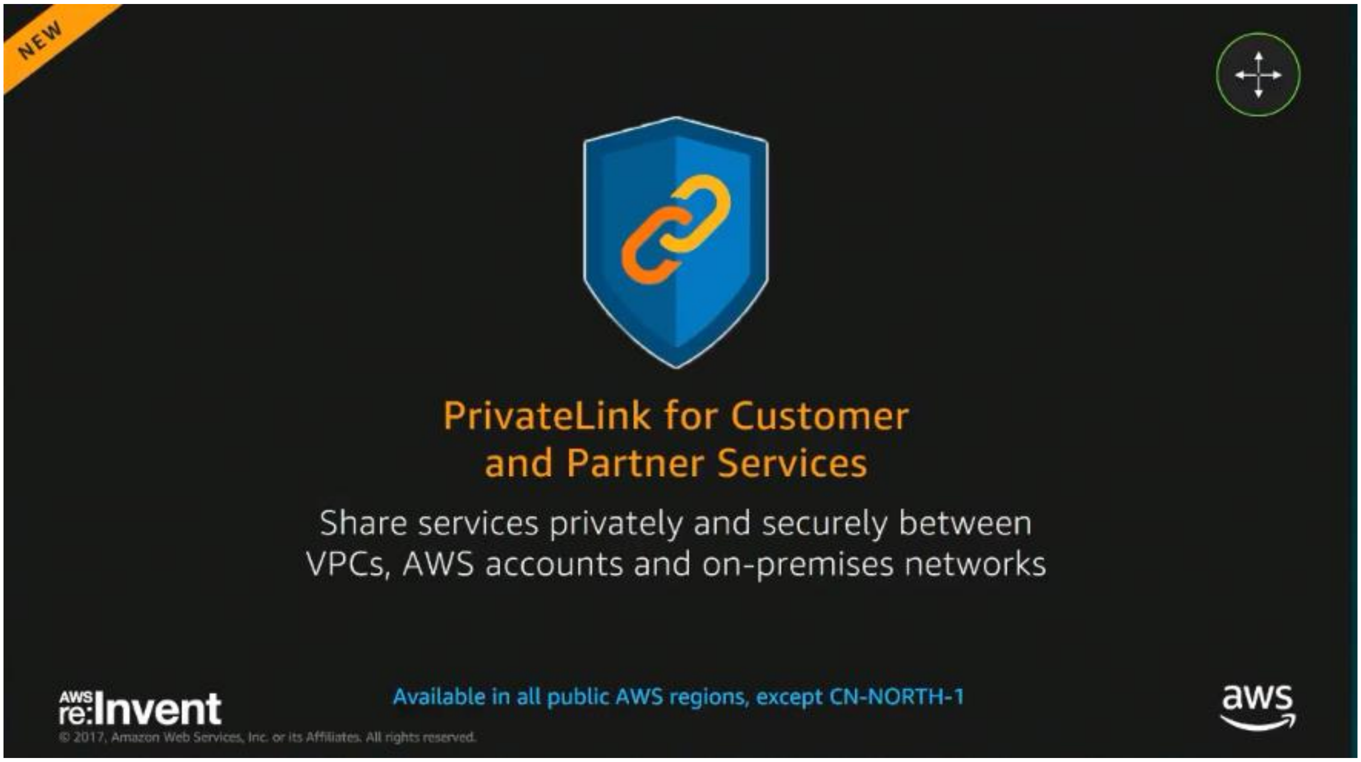
Overlapping IP address ranges

Ensuring that peered VPC IP addresses do not overlap introduces complexity

Controlling Access Levels

Ensuring that a peered VPC only has access to approved resources introduces complexity

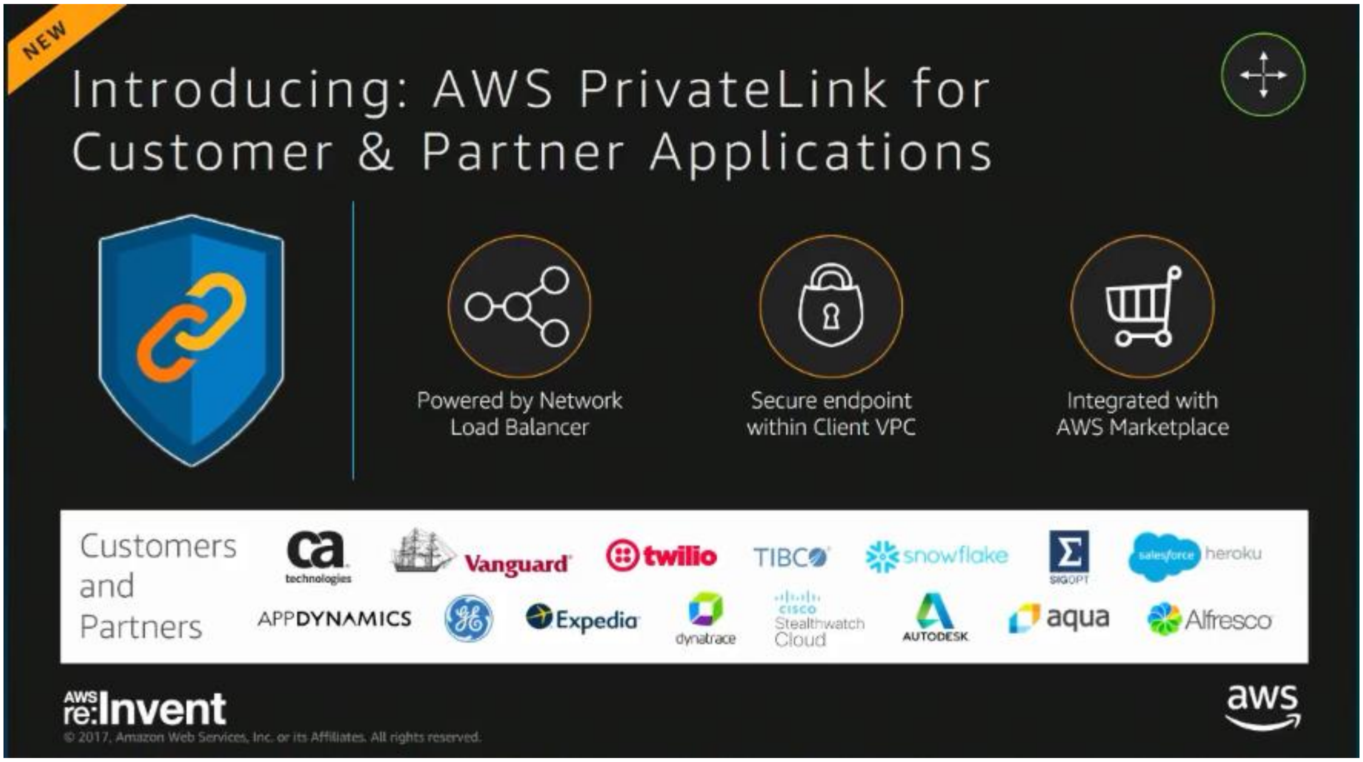
Sometimes you don’t want a peered VPC access to all the resources in the other VPC’s network, you need a way to constrain peer VPC access.



PrivateLink for Customer and Partner Services

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

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



NEW

Introducing: AWS PrivateLink for Customer & Partner Applications

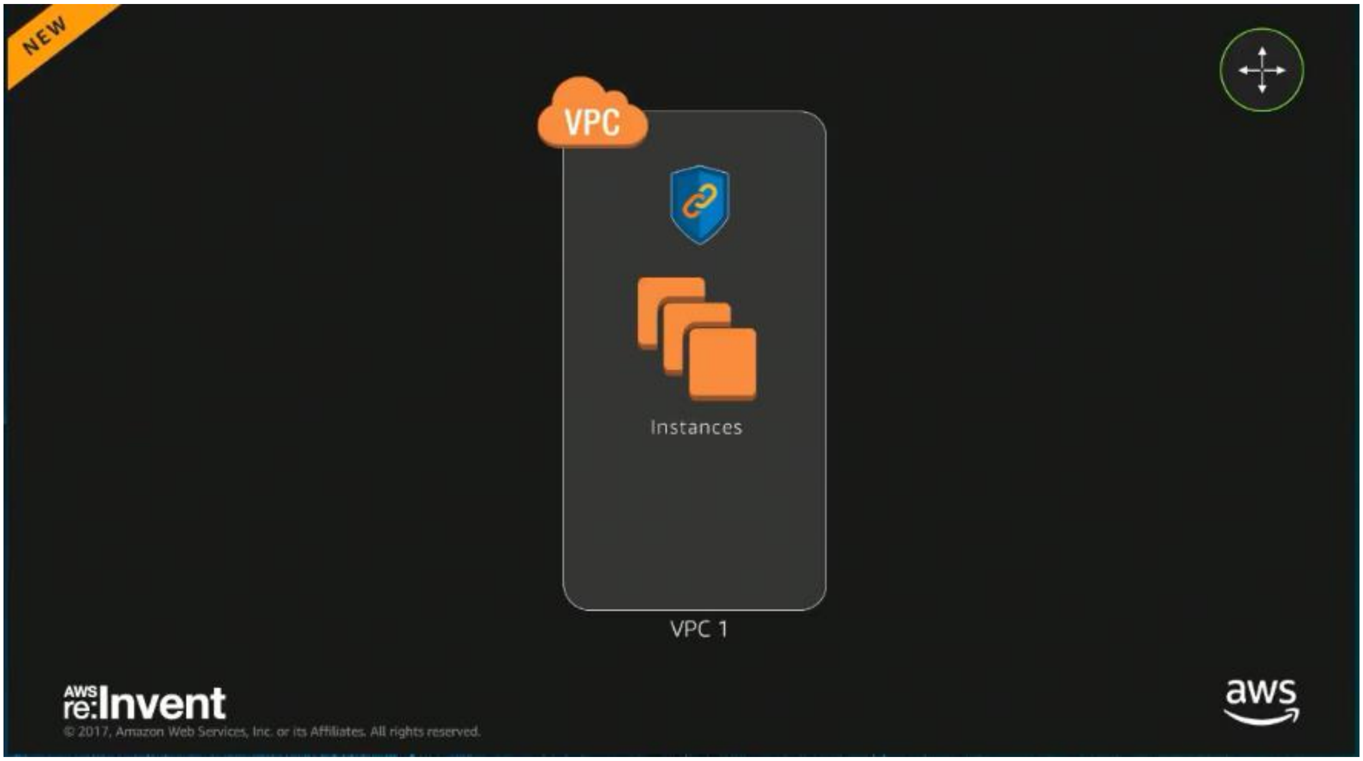
Powered by Network Load Balancer

Secure endpoint within Client VPC

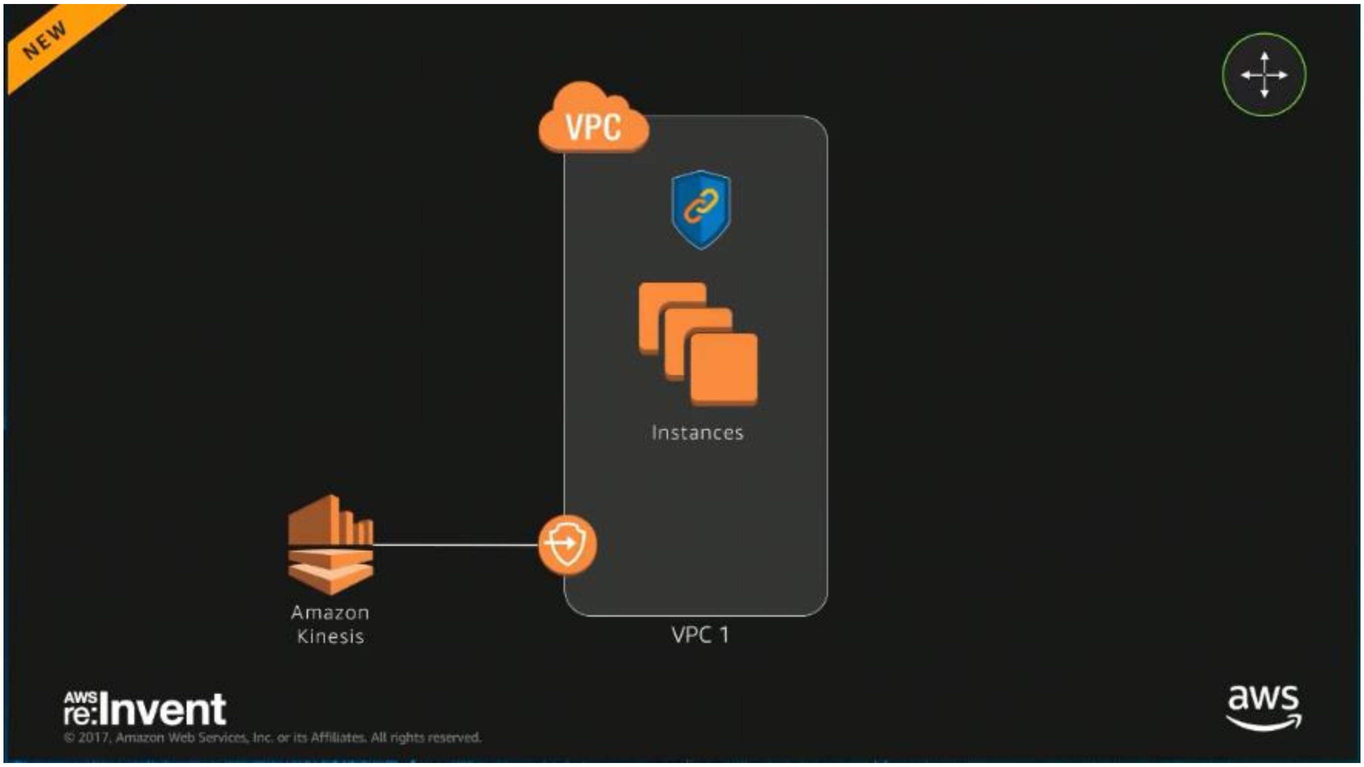
Integrated with AWS Marketplace

Customers and Partners

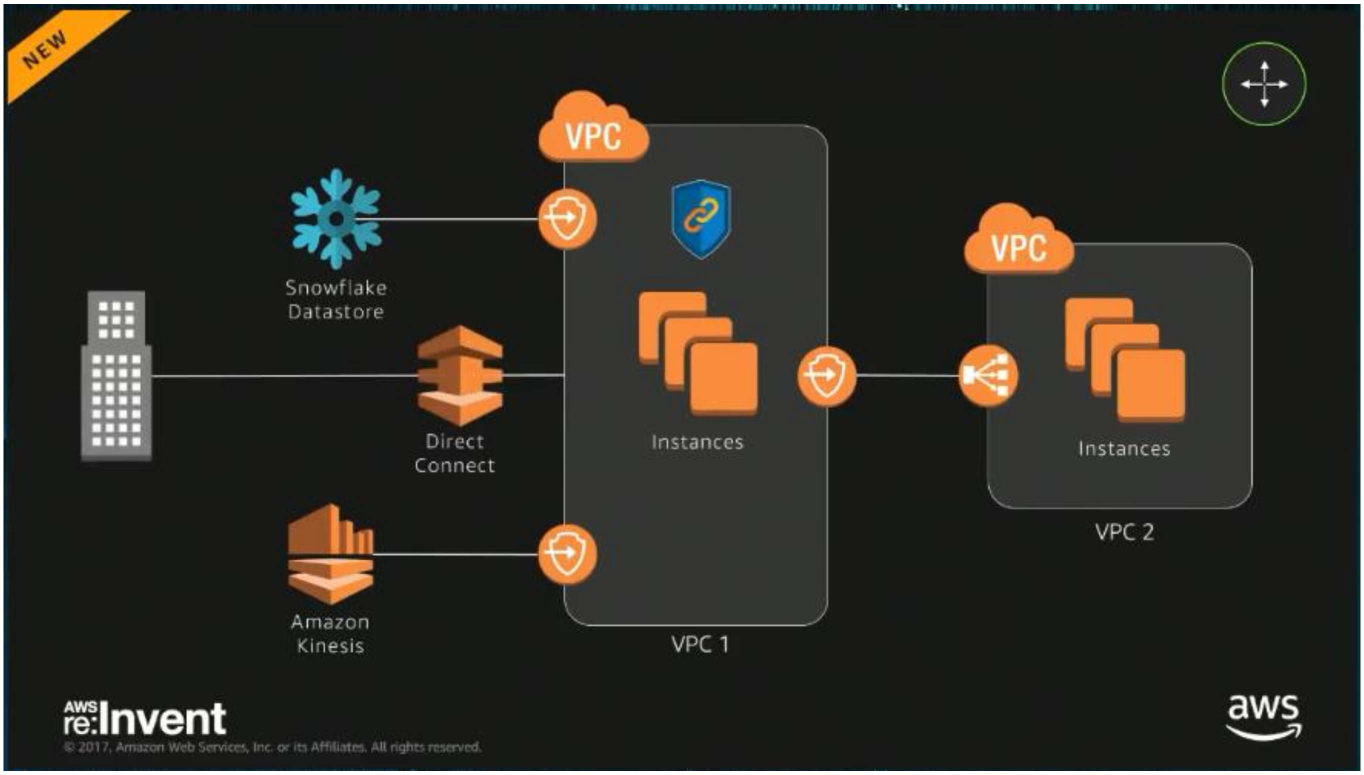
PrivateLink is powered by Network Load Balancers that you have to put in front of your applications to use privately. *It provides you with a secure endpoint within your VPC*. ***PrivateLink*** is also integrated with applications in the AWS Marketplace. If you want a snowflake database that is privately located within your VPC that you can connect to with a private IP or use via ***DirectConnect*** from your on-premises database, snowflake is integrated using ***PrivateLink*** to give you that possibility. ***Snowflake uses a NLB in front of a stack that they can now provision with an IP address in your VPC***, your network team is still happy with this because that IP address is still within the security perimeter of your VPC.



This is what using Privatelink like, we have a VPC that does not have a NAT gateway and only uses PrivateLink.


NEW
VPC
Instances
Amazon Kinesis
VPC 1
AWS re:Invent
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
aws

We might want to use Amazon Kinesis as above, we don't need a NAT gateway anymore.



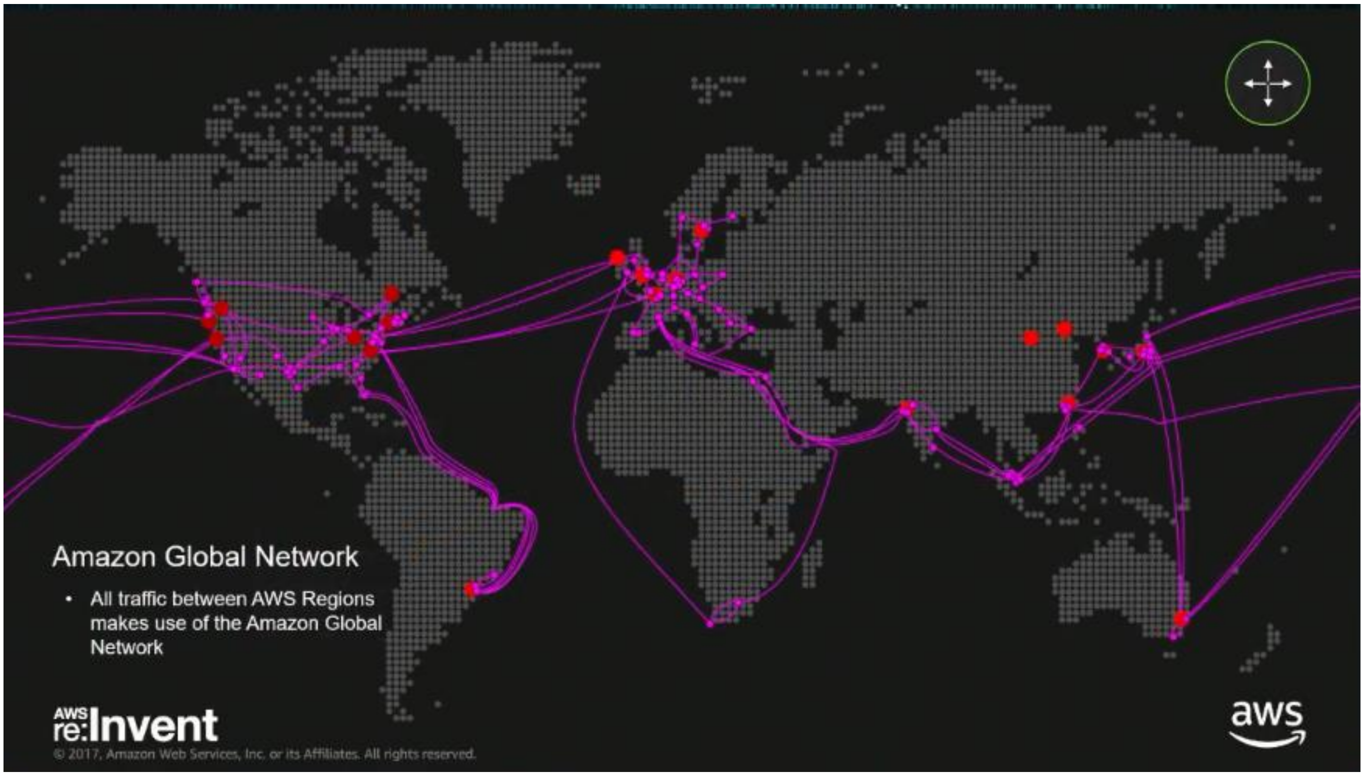
Maybe there is a team in our company that is also building a logging service, they can build that too and we don't have to worry about what CIDR they are given. We simply issue them a private endpoint within the VPC as above. We can also use snowflake or some other 3rd-party provided service within our VPC by simply issuing it a ***PrivateLink*** within the VPC too. We can also integrate with the on-premises network by using ***DirectConnect*** as above.

The network architectures today having multiple peered VPCs backing up a lot of your instances, PrivateLink is a very interesting to consider using. Schedule a Cloudfront template that creates a VPC network with PrivateLinks in it.

Jesper Joergensen
VP, Product Management,
Salesforce

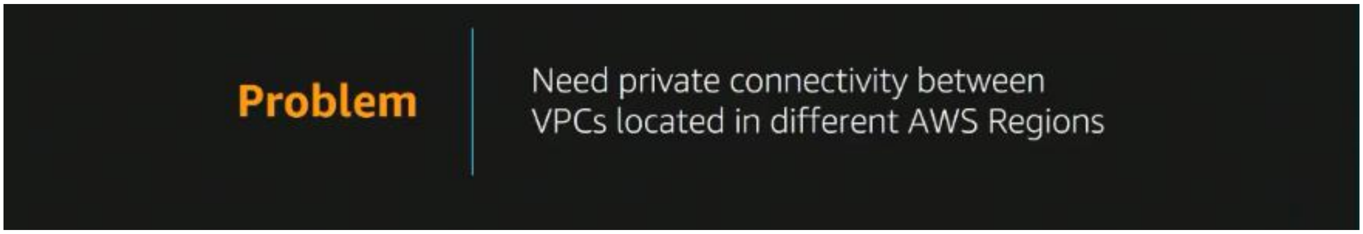
Salesforce & AWS Strategic Partnership

Running and extending Salesforce with AWS



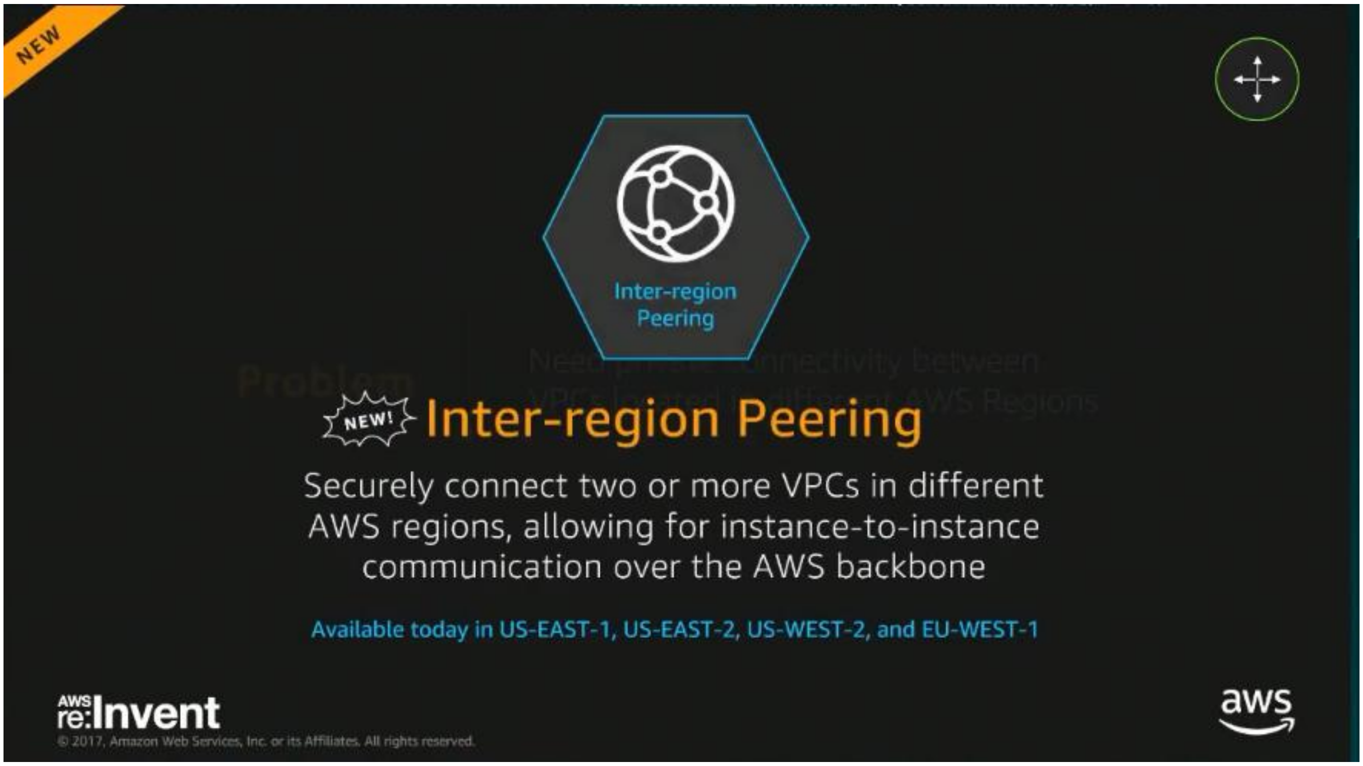
Amazon Global Network

- All traffic between AWS Regions makes use of the Amazon Global Network



Problem

Need private connectivity between VPCs located in different AWS Regions



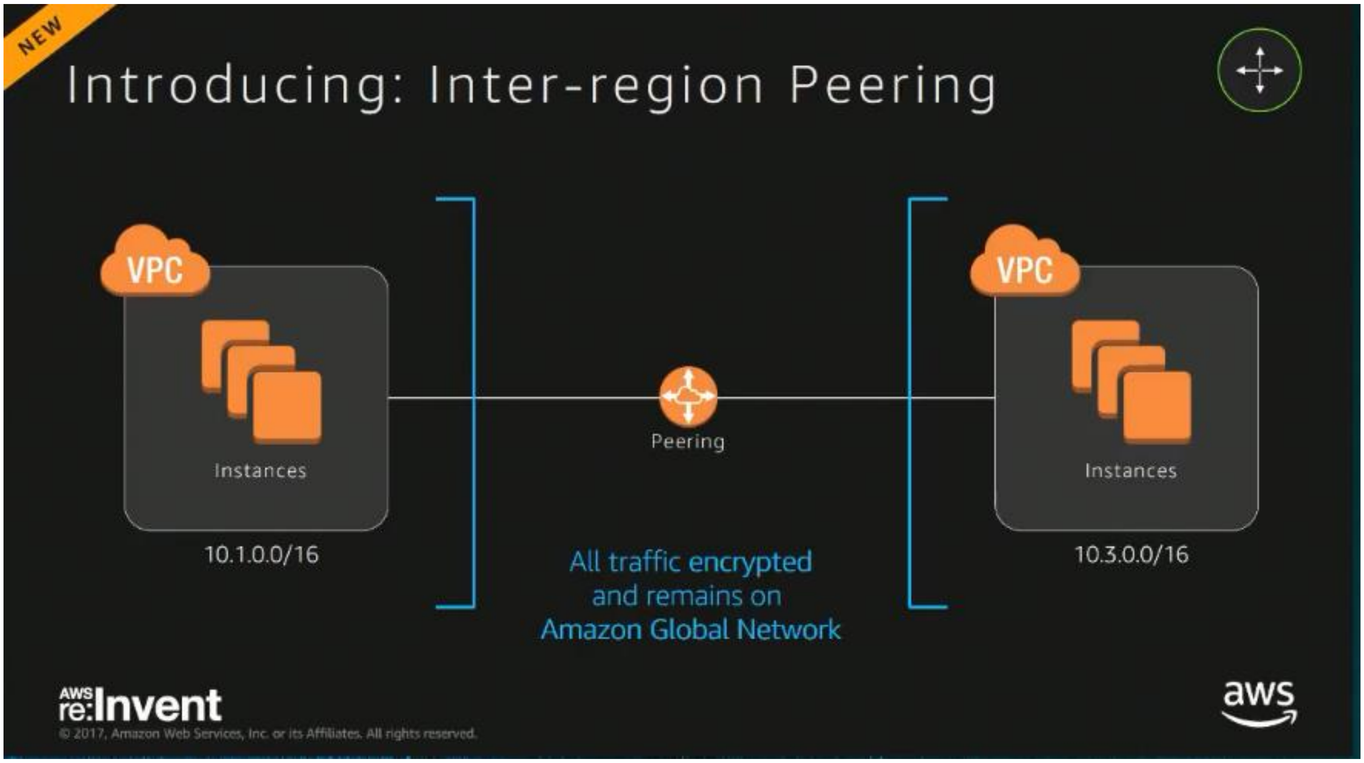
NEW
Inter-region Peering

Problem
Need private connectivity between VPCs located in different AWS Regions

NEW! Inter-region Peering

Securely connect two or more VPCs in different AWS regions, allowing for instance-to-instance communication over the AWS backbone

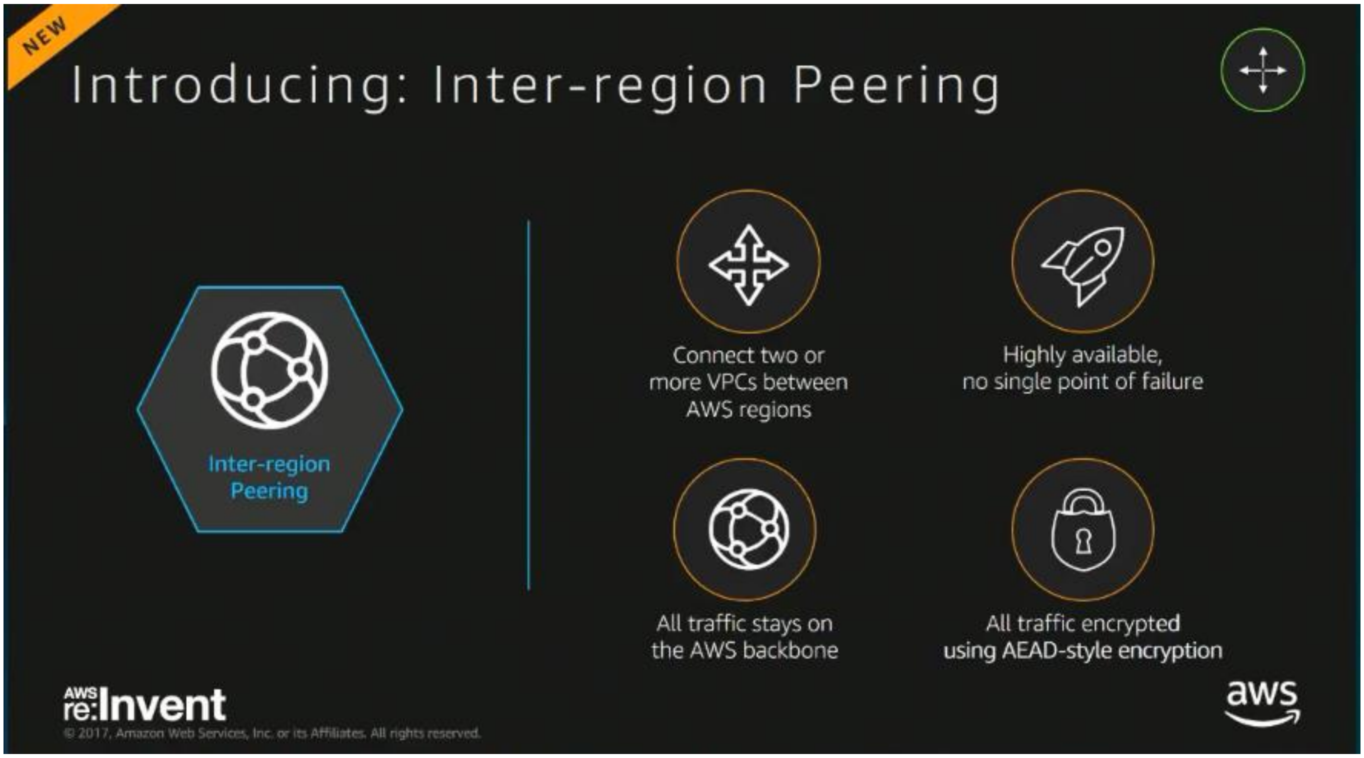
Available today in US-EAST-1, US-EAST-2, US-WEST-2, and EU-WEST-1



Introducing: Inter-region Peering

All traffic encrypted and remains on Amazon Global Network

A VPC in us-east-1 can now talk privately to a VPC in eu-west-1 across the Atlantic using the ***Amazon backbone*** and VPC Peering without the communication going through the public internet and all traffic also being encrypted.


NEW
Inter-region Peering
AWS re:Invent
aws

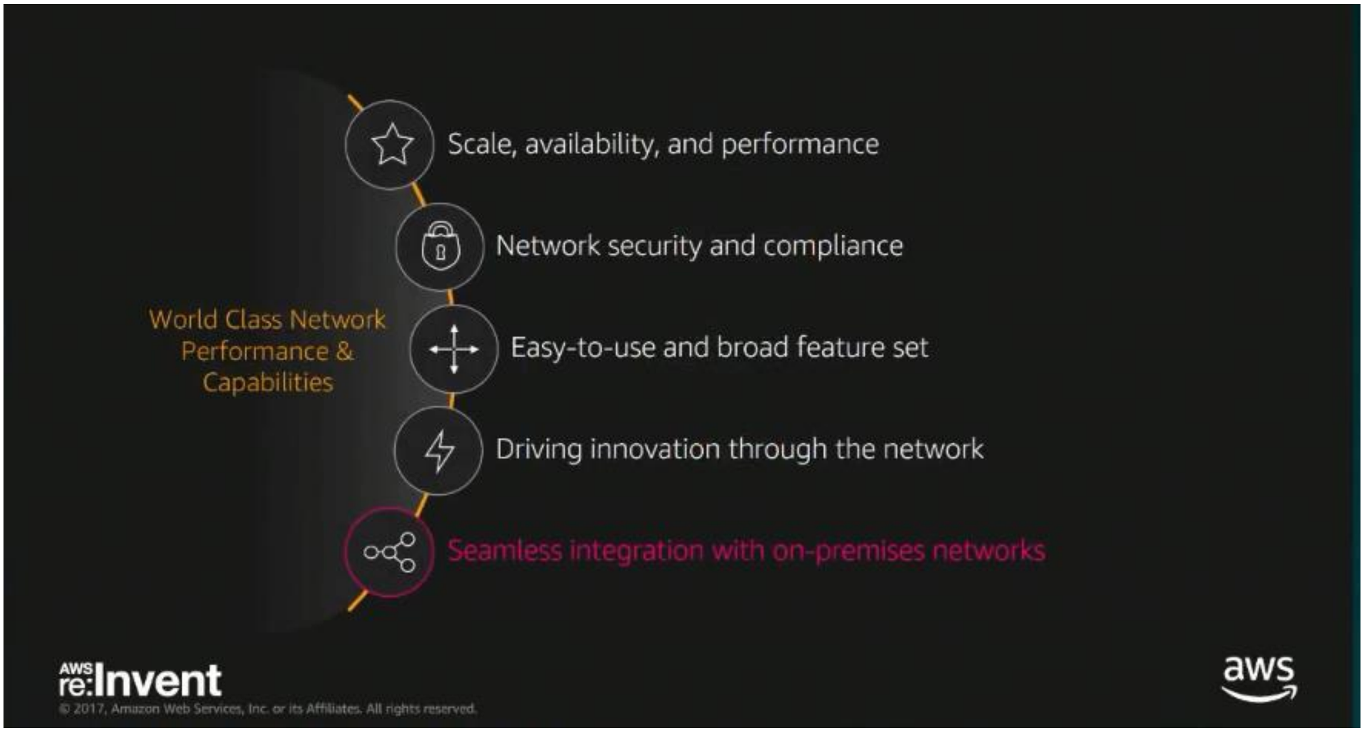
Introducing: Inter-region Peering

Connect two or more VPCs between AWS regions

Highly available, no single point of failure

All traffic stays on the AWS backbone

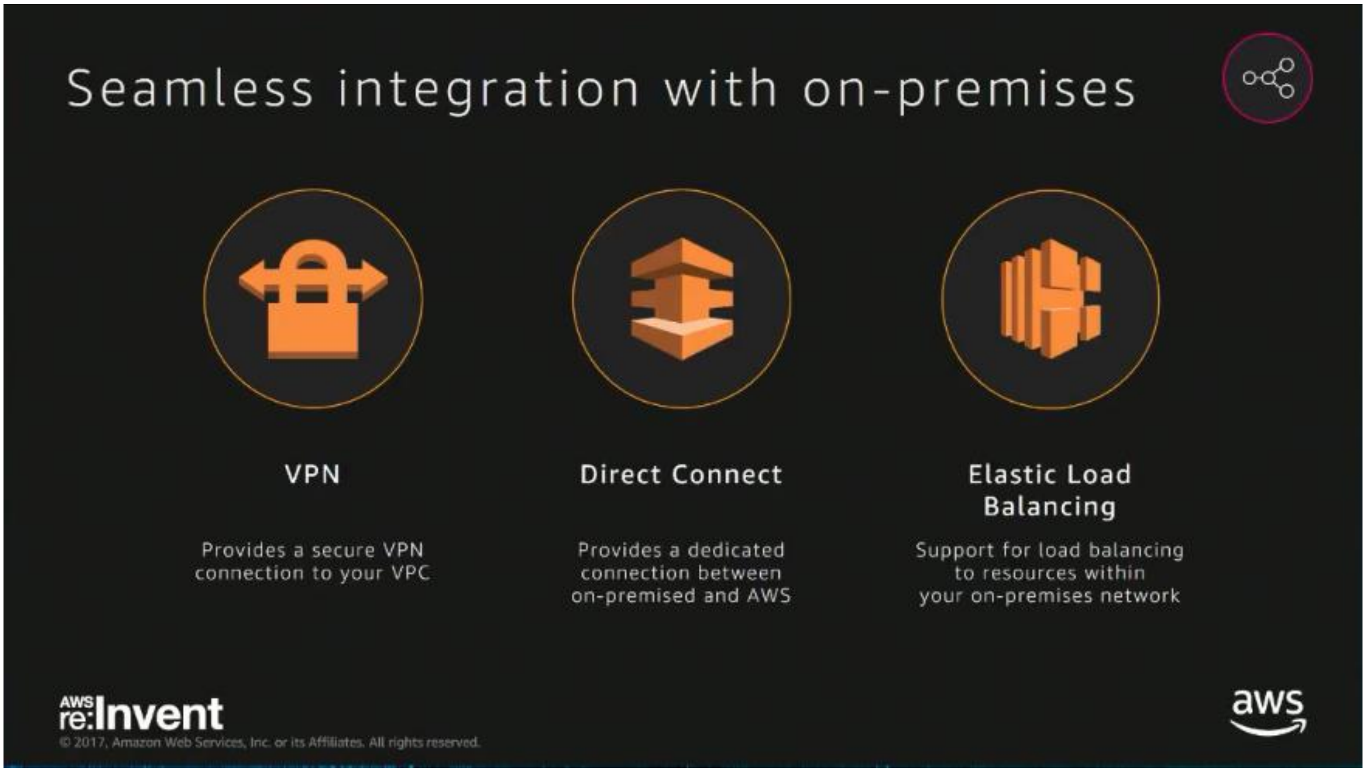
All traffic encrypted using AEAD-style encryption



World Class Network Performance & Capabilities

- Scale, availability, and performance
- Network security and compliance
- Easy-to-use and broad feature set
- Driving innovation through the network
- Seamless integration with on-premises networks

We still need a way to provide seamless connectivity between the applications you run in your branch offices and what you have developed or migrated to the cloud.



Seamless integration with on-premises

VPN

Provides a secure VPN connection to your VPC

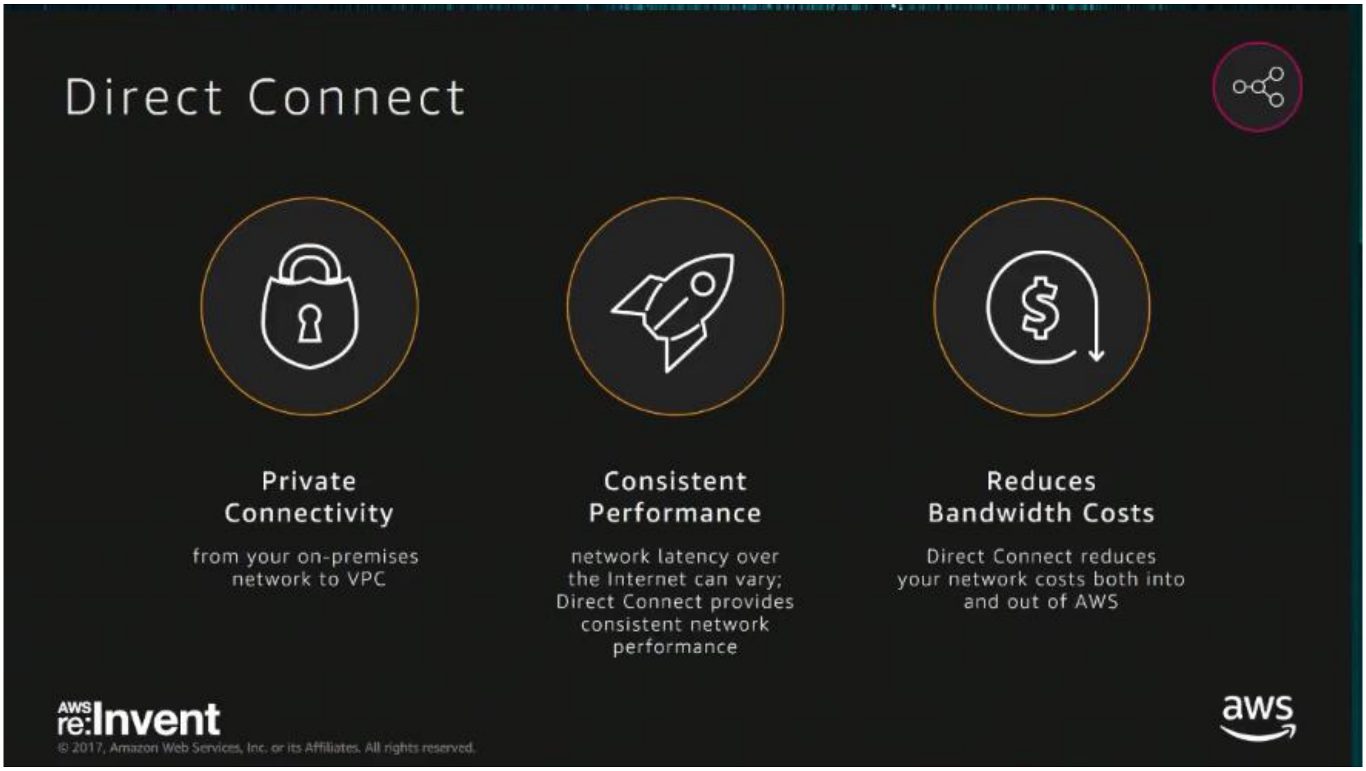
Direct Connect

Provides a dedicated connection between on-premised and AWS

Elastic Load Balancing

Support for load balancing to resources within your on-premises network

A NLB or ALB can now load balance to an IP address that it not an EC2 instance, you can set up an Elastic Load Balancer ELB by simply putting an IP address of a machine that might be in your data center.



Direct Connect

Private Connectivity

from your on-premises network to VPC

Consistent Performance

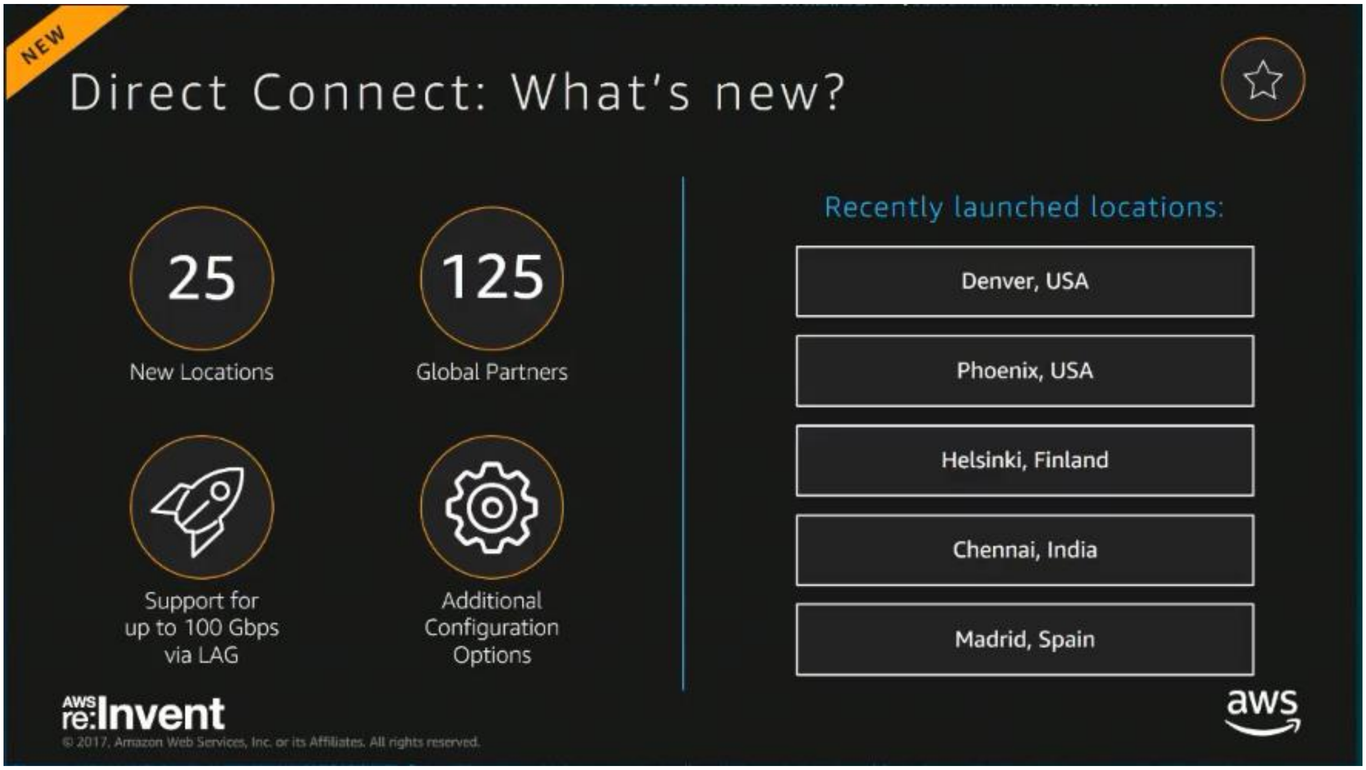
network latency over the Internet can vary; Direct Connect provides consistent network performance

Reduces Bandwidth Costs

Direct Connect reduces your network costs both into and out of AWS

AWS re:Invent
aws

DirectConnect gives you private connectivity DNS style, it is a dedicated fiber connection into AWS from the DirectConnect location.



NEW

Direct Connect: What's new?

25 New Locations

125 Global Partners

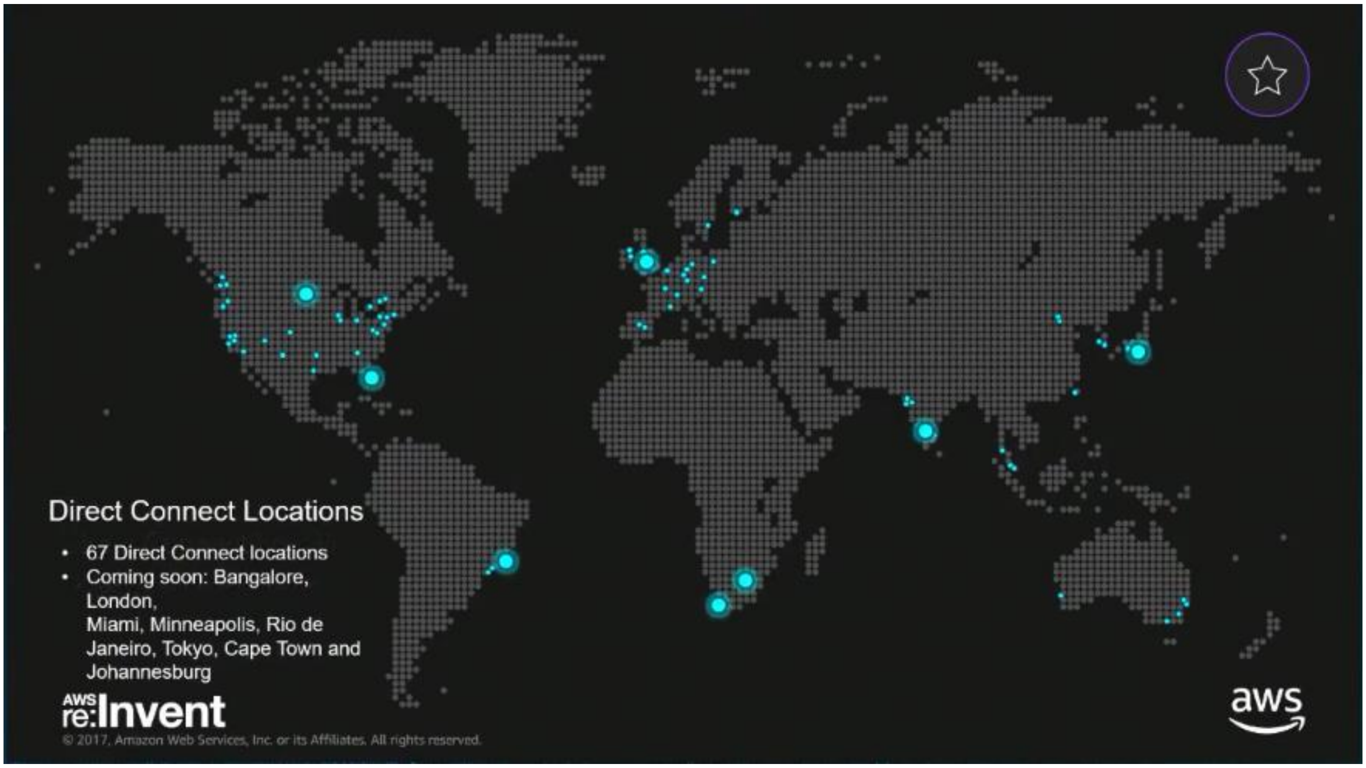
Support for up to 100 Gbps via LAG

Additional Configuration Options

Recently launched locations:

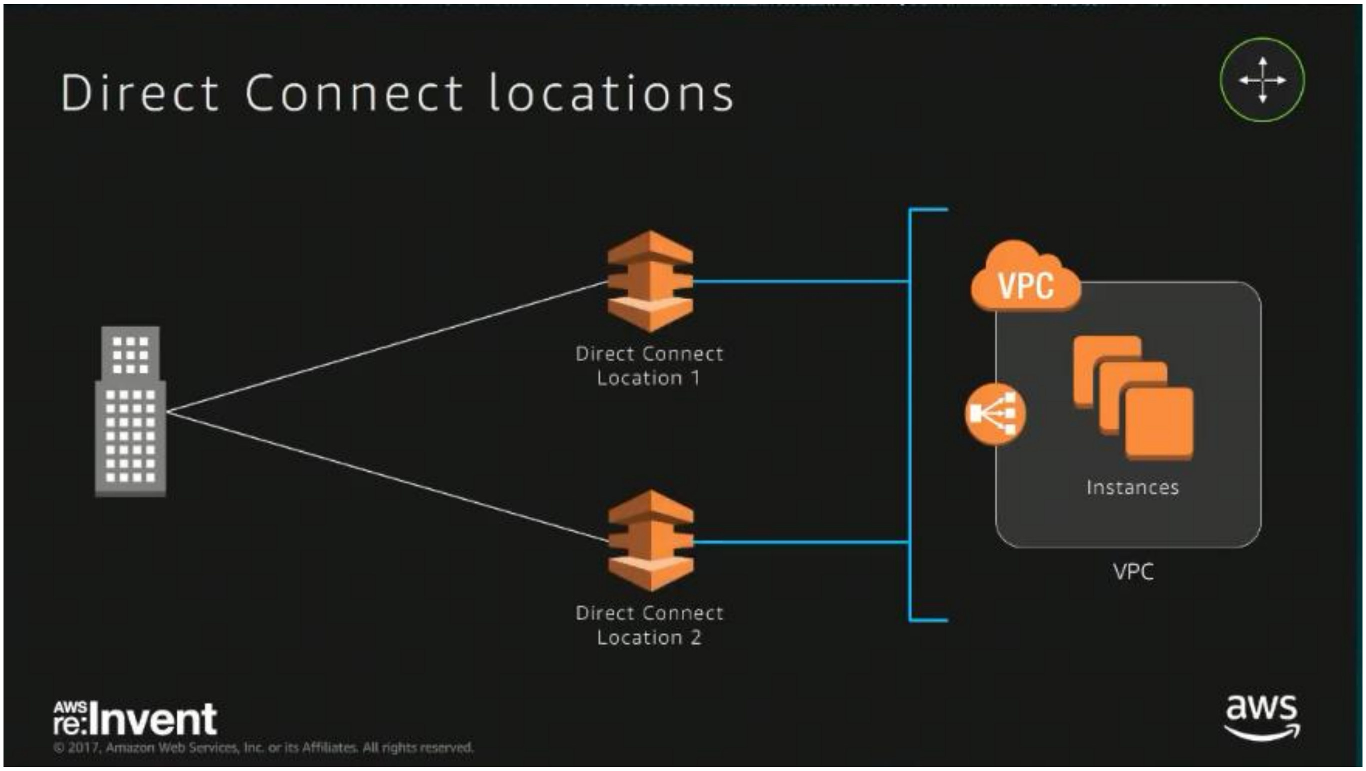
- Denver, USA
- Phoenix, USA
- Helsinki, Finland
- Chennai, India
- Madrid, Spain

AWS re:Invent
aws



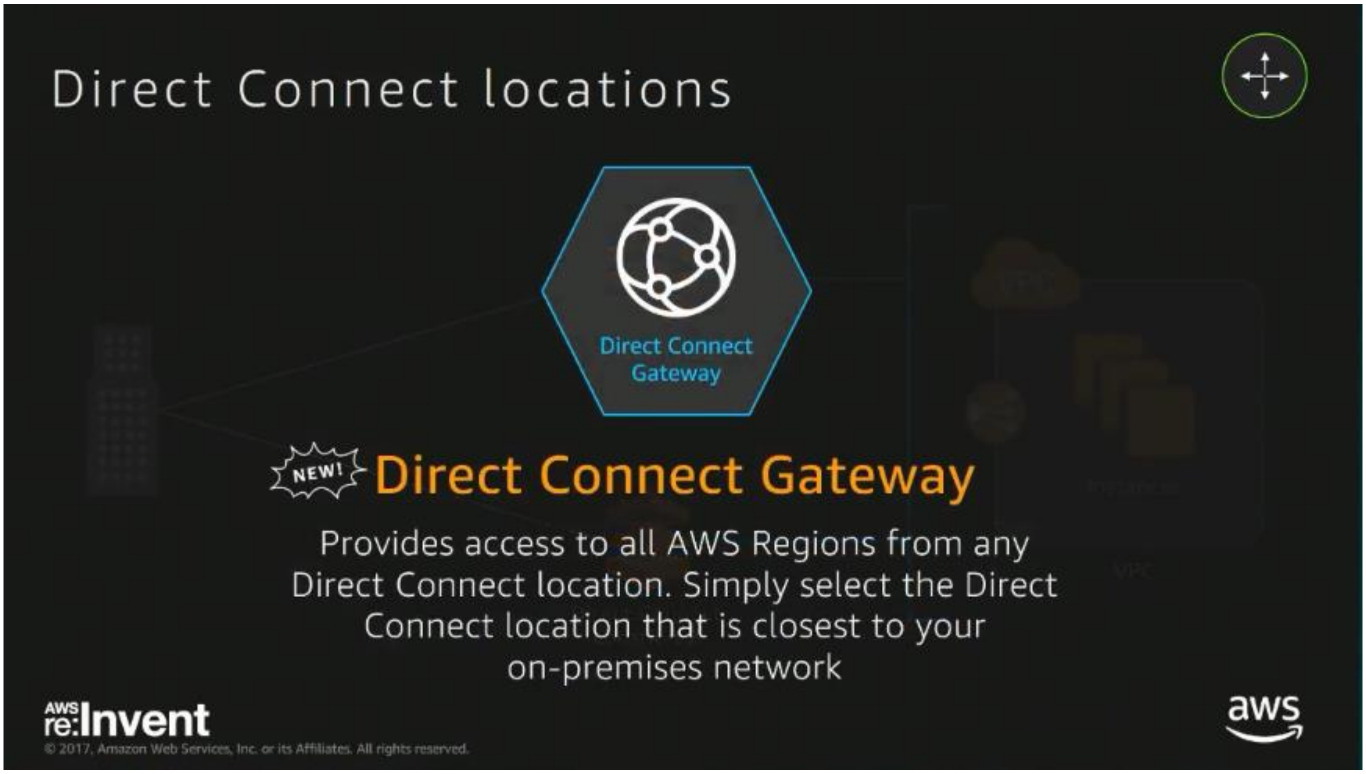
Direct Connect Locations

- 67 Direct Connect locations
- Coming soon: Bangalore, London, Miami, Minneapolis, Rio de Janeiro, Tokyo, Cape Town and Johannesburg



Direct Connect locations

To use a DirectConnect location, you need to find a location that is associated with a region that is closest to you. Then you run fiber to connect to the location.



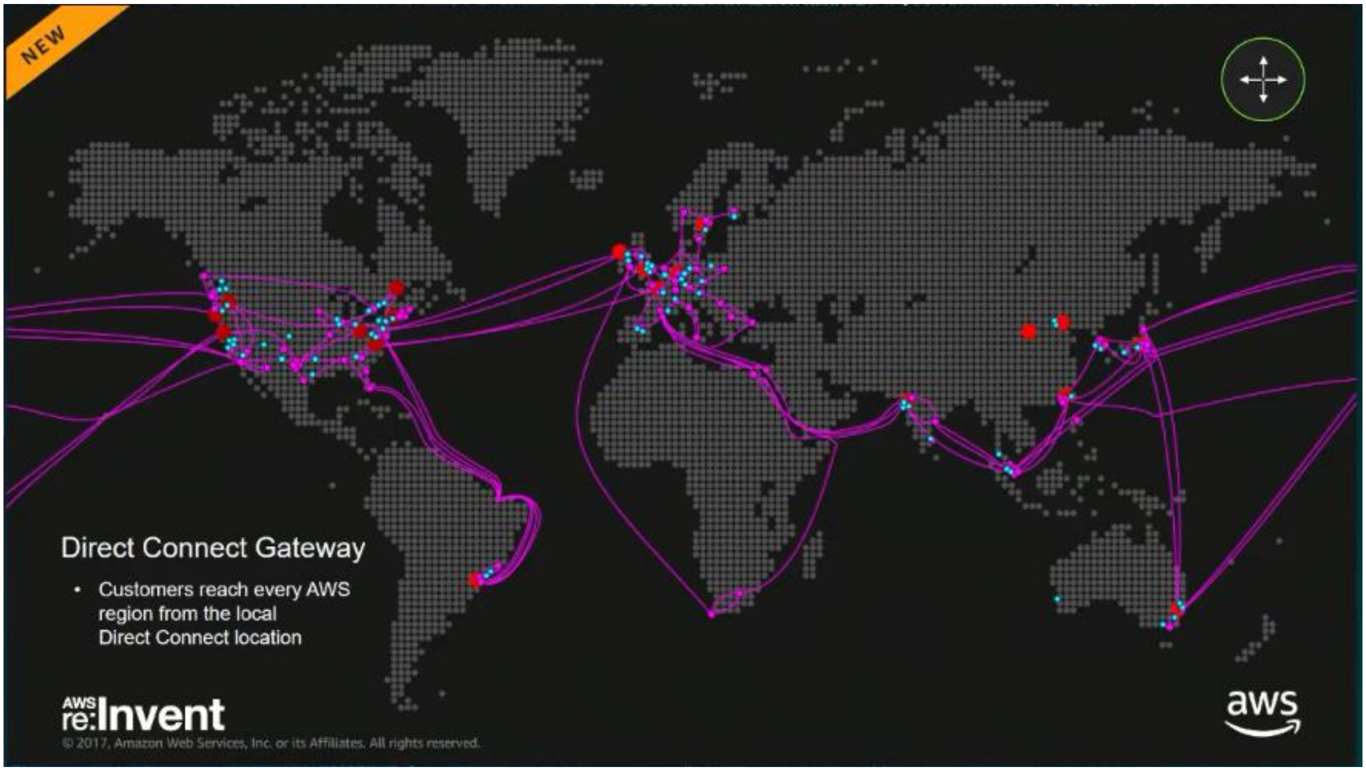
Direct Connect locations

NEW! **Direct Connect Gateway**

Provides access to all AWS Regions from any Direct Connect location. Simply select the Direct Connect location that is closest to your on-premises network

AWS re:Invent

aws

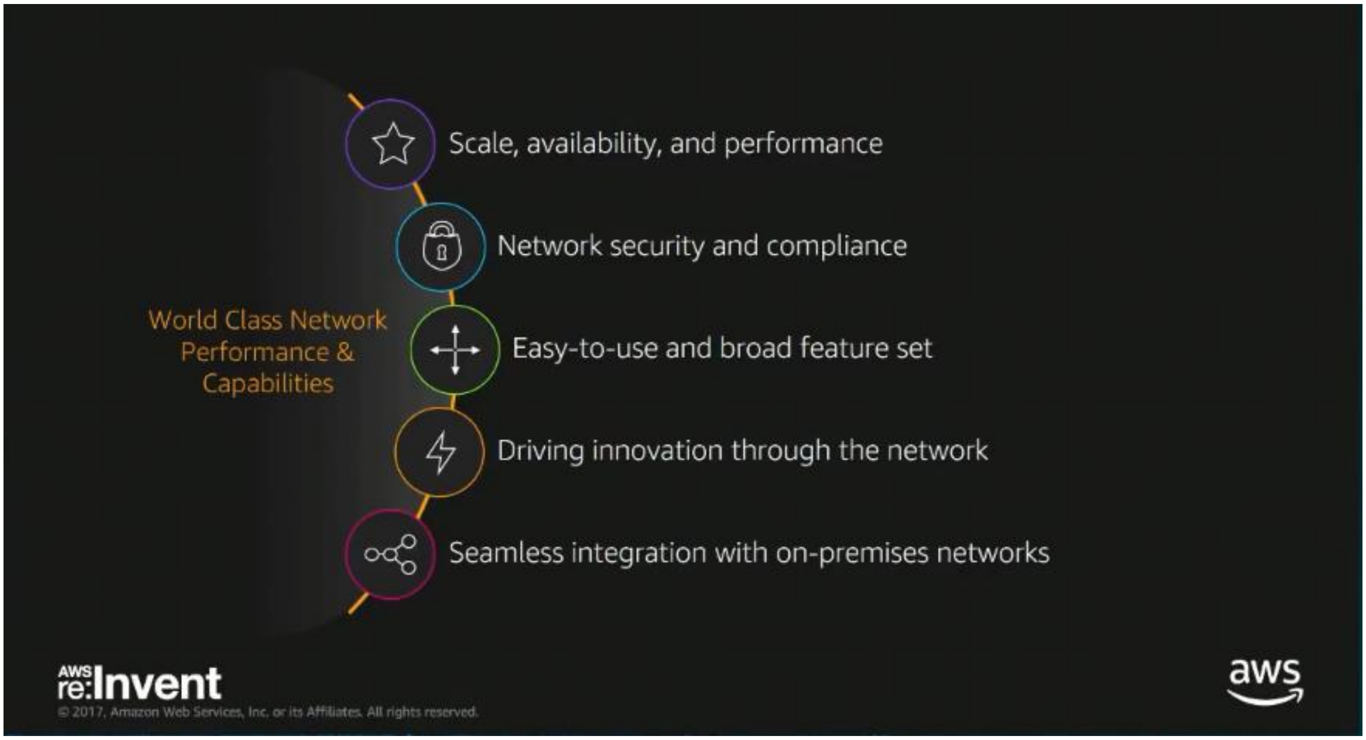


Direct Connect Gateway

- Customers reach every AWS region from the local Direct Connect location

AWS re:Invent

aws



World Class Network Performance & Capabilities

- Scale, availability, and performance
- Network security and compliance
- Easy-to-use and broad feature set
- Driving innovation through the network
- Seamless integration with on-premises networks

Customer-obsessed

90%

of the items on the roadmap originate with customer requests and are designed to meet specific needs and requirements

AND IT'S ALWAYS

DAY 1

AWS re:Invent

Thank you!