aws SUMMIT

Another Day, Another Billion Flows

Steve Seymour
Principal Specialist Solutions Architect, AWS

@sseymour

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

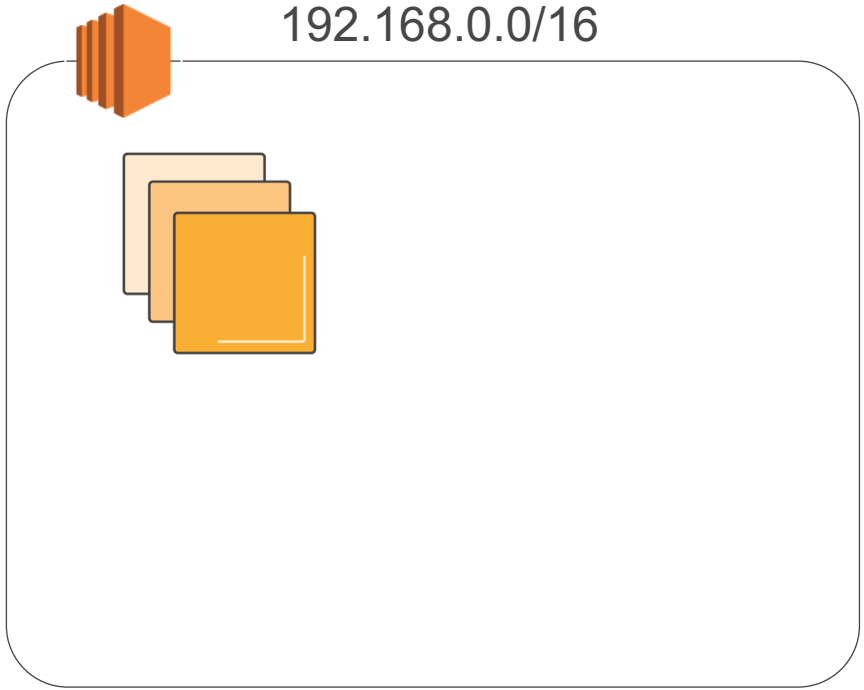
What is VPC?

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

What is VPC?

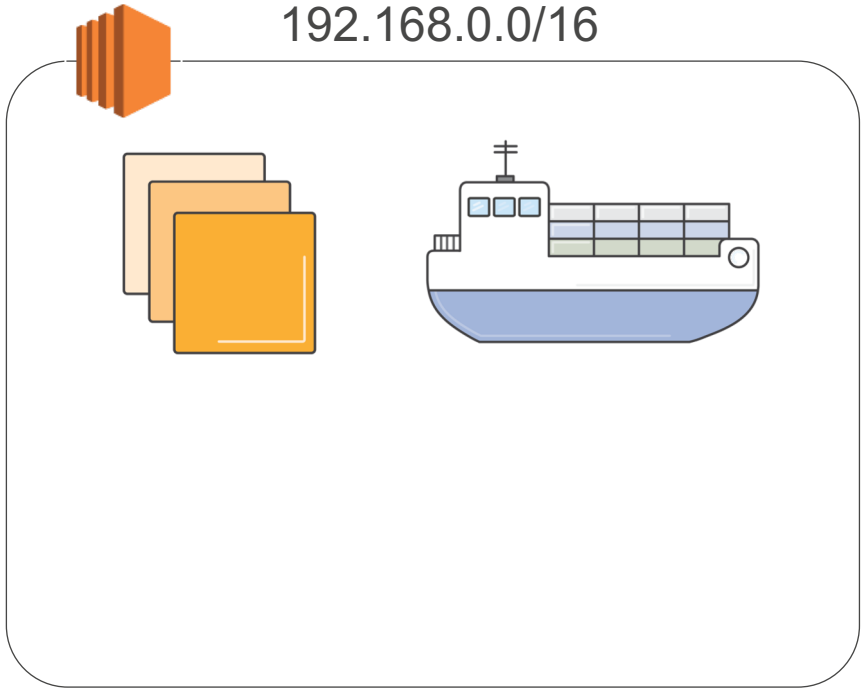
© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is VPC?



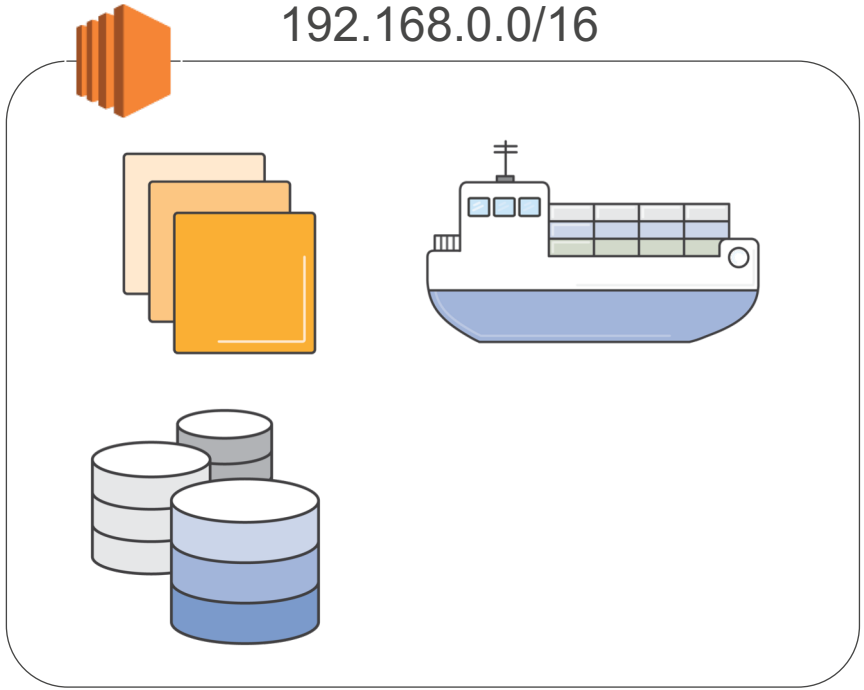
© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is VPC?



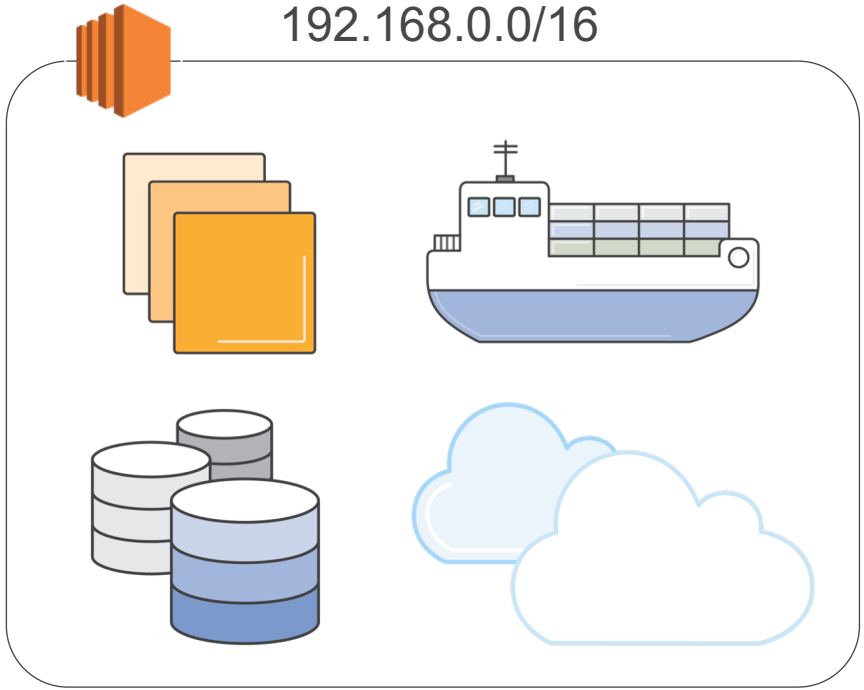
© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is VPC?



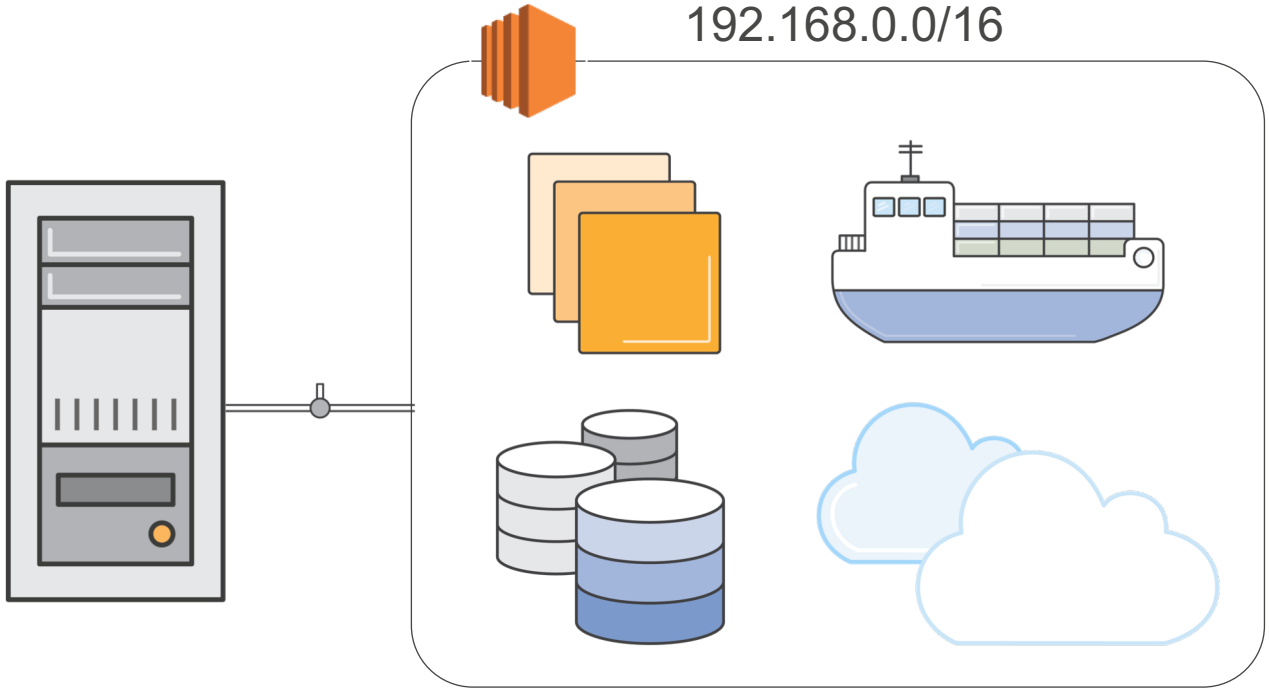
© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is VPC?



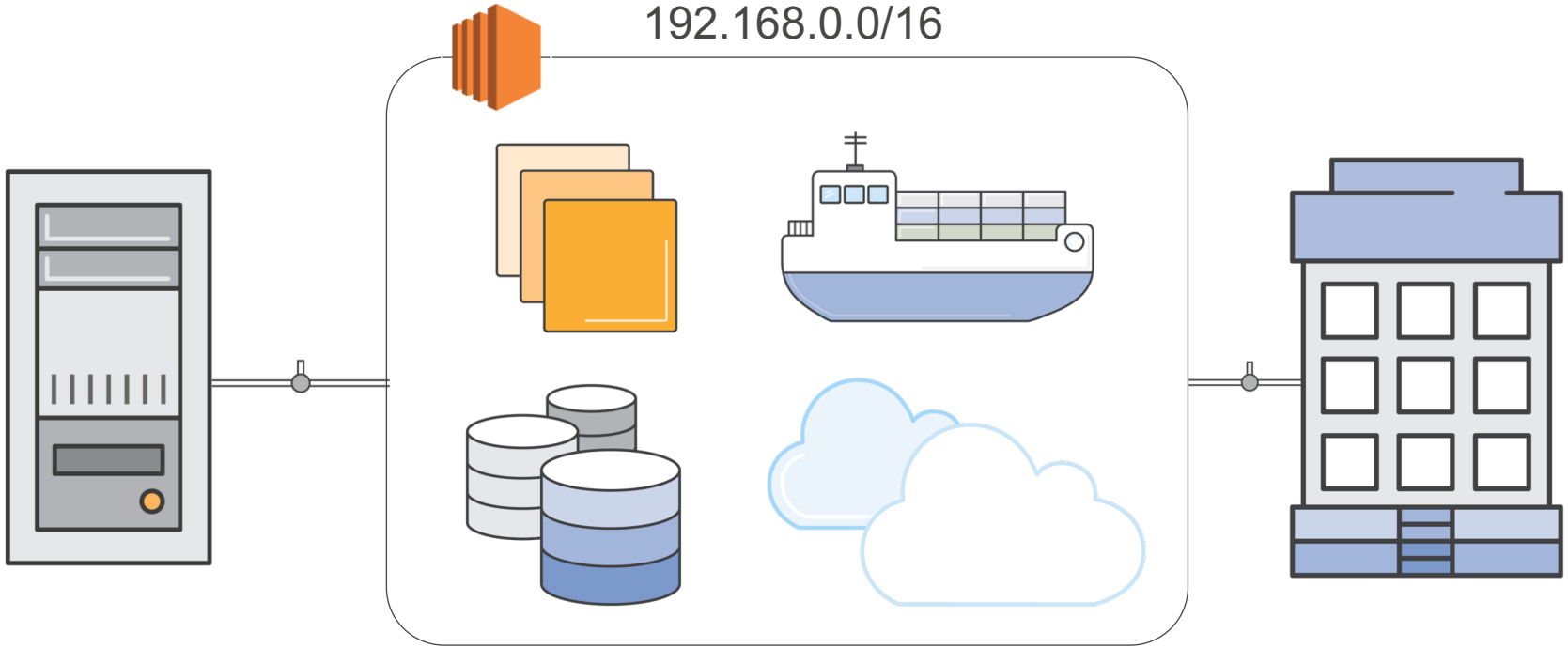
© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is VPC?



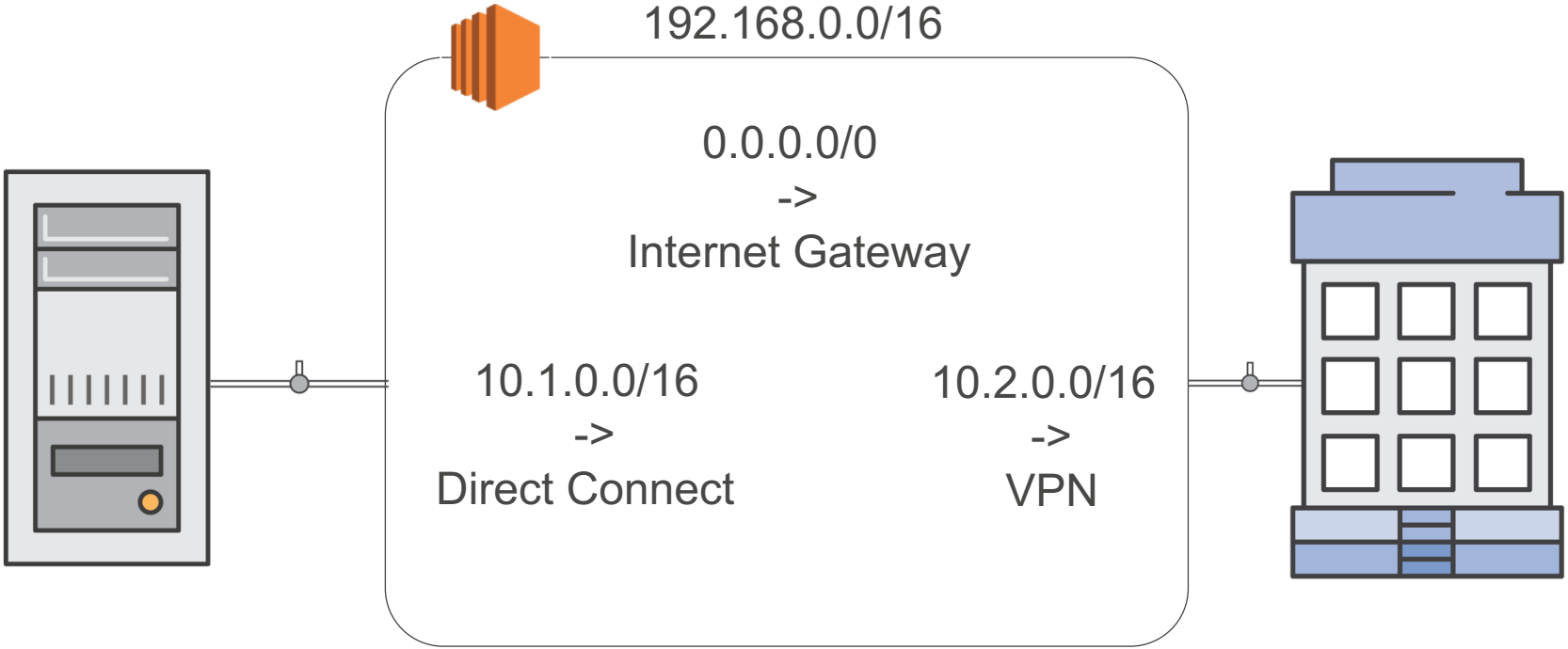
© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is VPC?



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

What is VPC?



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

What is VPC?

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

Every VPC comes with …

- Full programmatic control via APIs, templates, change history and audit capabilities, flow log support
- Built-in DHCP and DNS service, including private DNS
- Built-in firewall
- 9001 byte MTU

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

VPC is designed for many VPCs

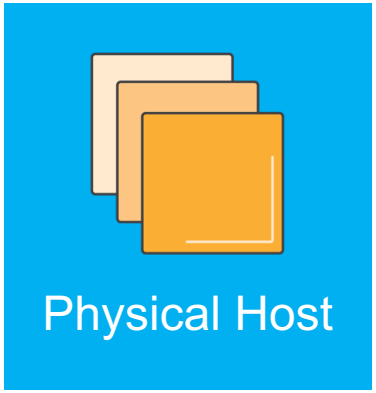
- Every VPC is free
- Useful for dev, beta, pre-prod, test and repro networks
- Multi-VPC architectures
- Immutable infrastructure patterns

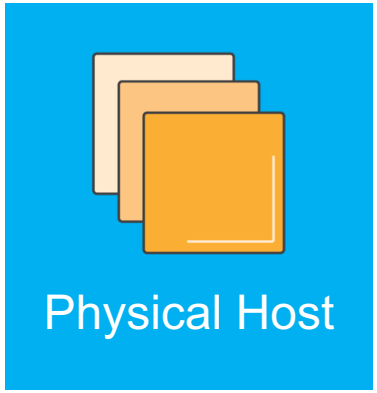
© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How does all of this work?

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

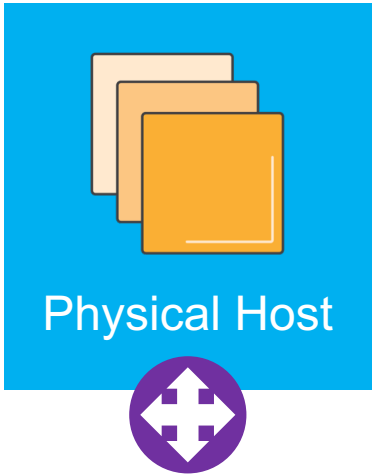
VPC on the wire

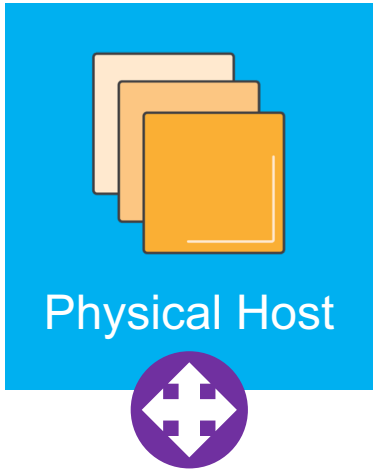




© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

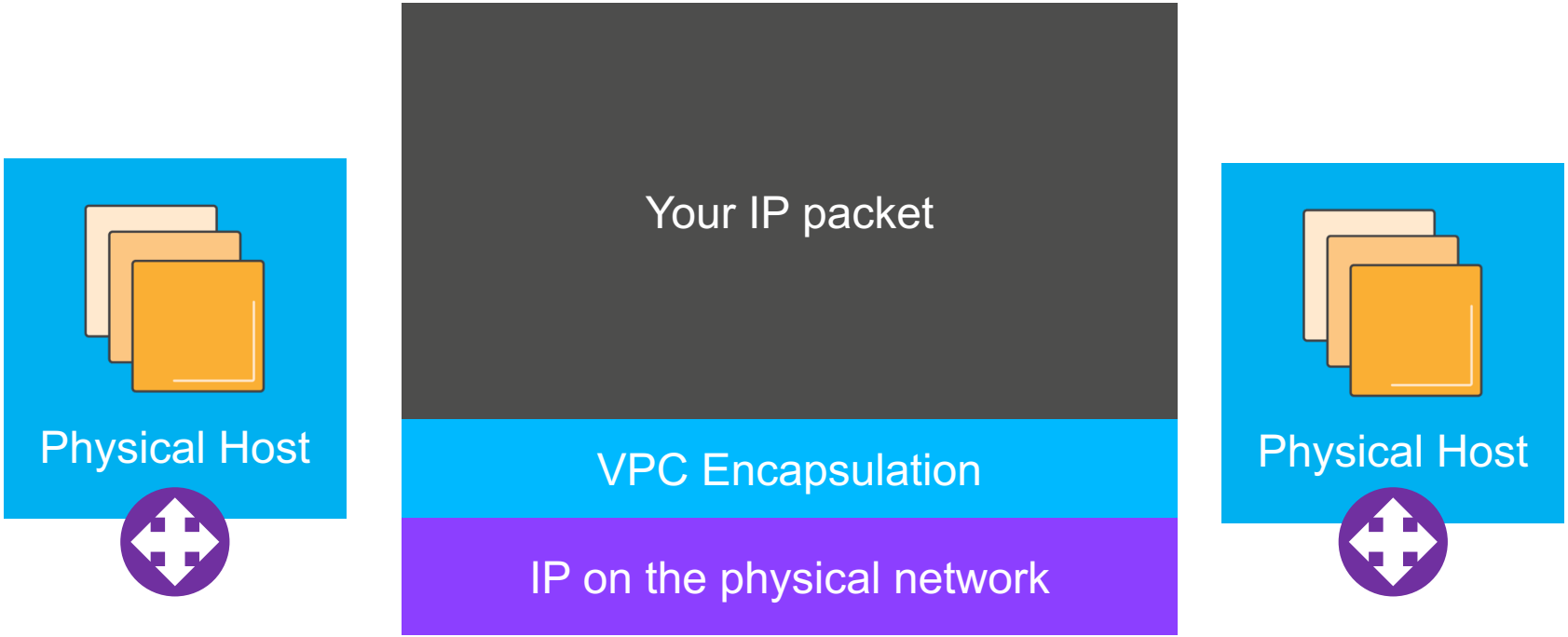
VPC on the wire





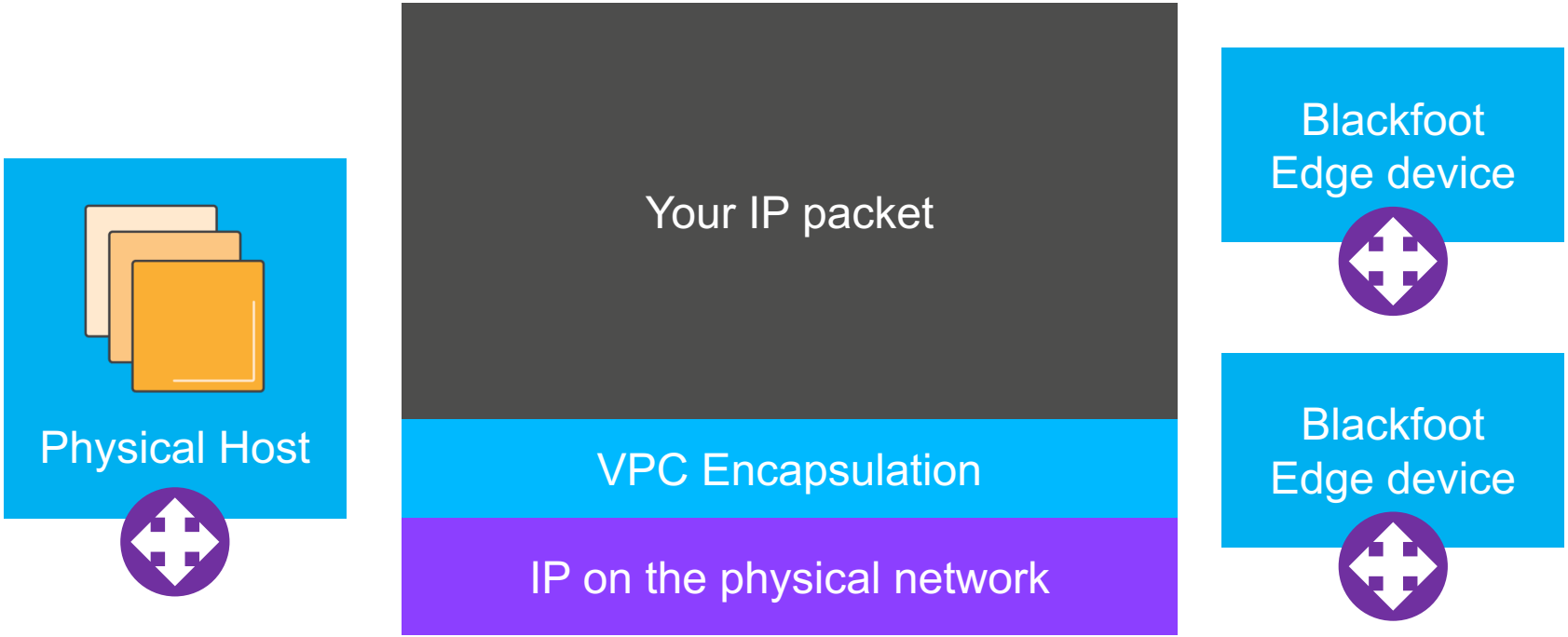
© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC on the wire



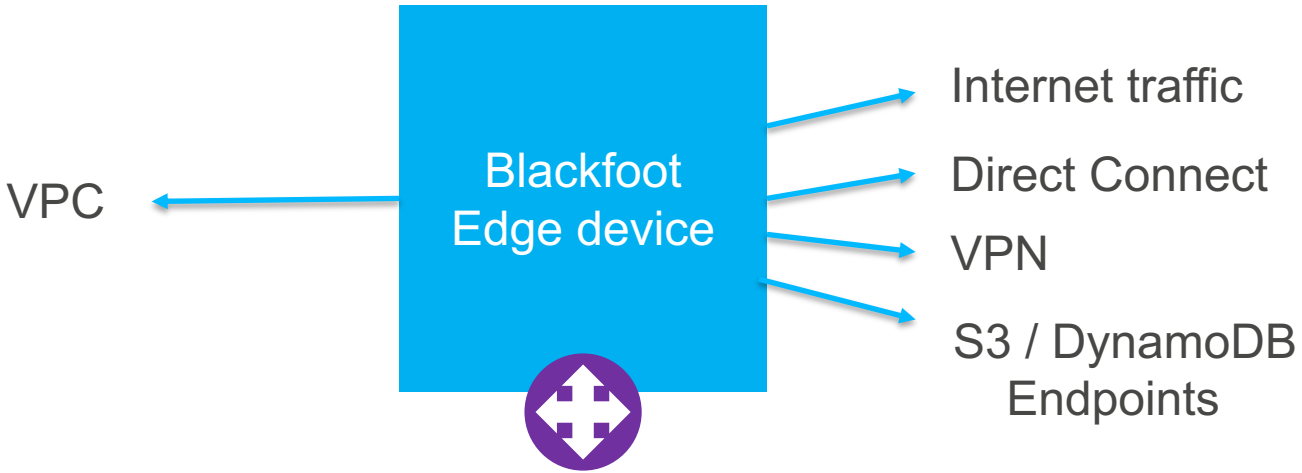
© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC on the wire



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

VPC on the wire



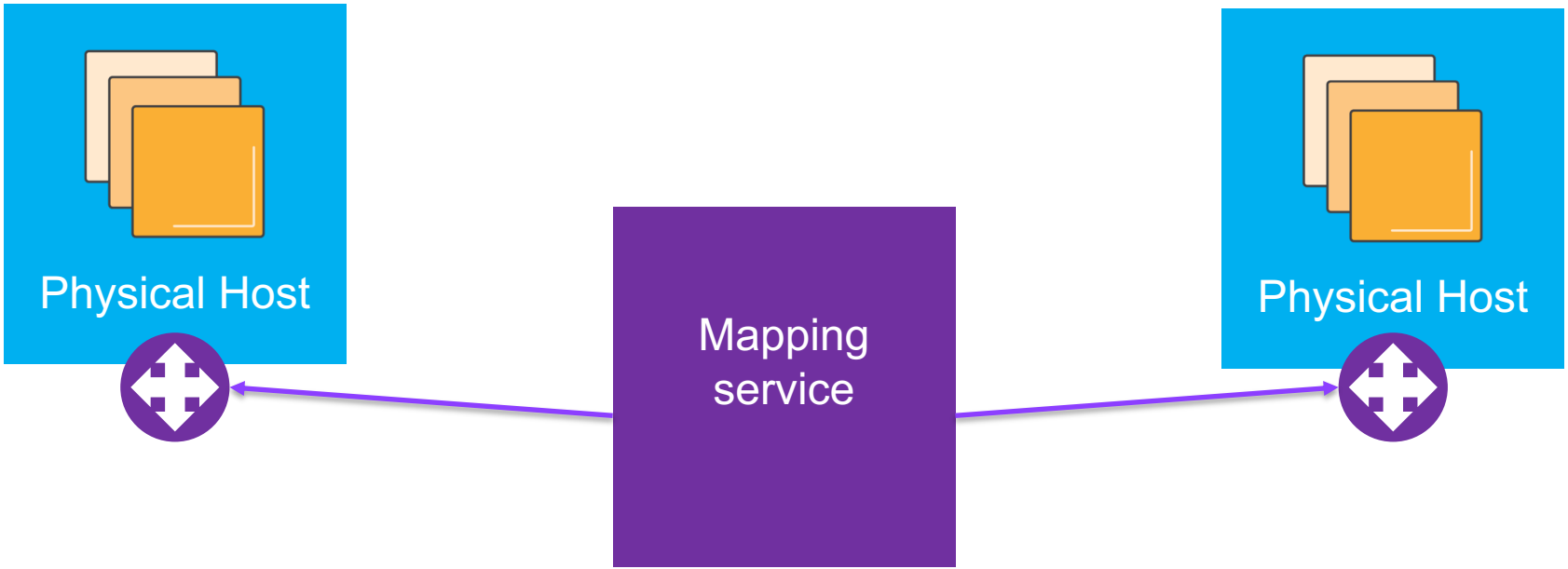
© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Encapsulating the packet

- Outer-most IP destination identifies the target physical host
- Encapsulation marks each packet with the VPC and the Elastic Network Interface
- How does the sender know these? The mapping service …

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

The mapping service



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

The mapping service

- A distributed web service that handles mappings between customers VPC routes and IPs and physical destinations on the wire.

- To support microsecond-scale latencies, mappings are cached where they are used, and pro-actively invalidated when they change.

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

But what about flows?

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

VPC Networking and Flows

- Security Groups include stateful connection tracking
- Flow logs give per-ENI aggregated audit data
- Network Load Balancer can load balance flows natively and transparently in the VPC network
- NAT Gateway brings per-flow stateful NAT to VPC

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

How flow tracking works

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

How flow tracking works

Protocol	Source IP	Destination IP	Source Port	Destination Port
TCP	192.0.2.1	52.84.25.90	33763	443
TCP	192.0.2.1	52.84.25.90	27441	443
UDP	192.0.2.10	205.251.197.26	15732	53
ICMP	192.0.2.1	52.84.25.90	-	-

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

How flow tracking works

Protocol	Source IP	Destination IP	Source Port	Destination Port	SEQ	ACK
TCP	192.0.2.1	52.84.25.90	33763	443	6532	34224
TCP	192.0.2.1	52.84.25.90	27441	443	18931	45312

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

How flow tracking works

Protocol	Source IP	Destination IP	Source Port	Destination Port	Datagram ID
UDP	192.0.2.10	205.251.197.26	15732	53	5178

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

How flow tracking works

Protocol	Source IP	Destination IP	Bonus embedded header
ICMP	192.0.2.10	205.251.197.26	[Same as previous slides]

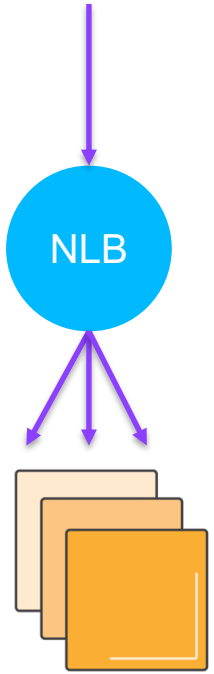
© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC Networking and Flows

- **Security Groups include stateful connection tracking**
- **Flow logs give per-ENI aggregated audit data**
- Network Load Balancer can load balance flows natively and transparently in the VPC network
- NAT Gateway brings per-flow stateful NAT to VPC

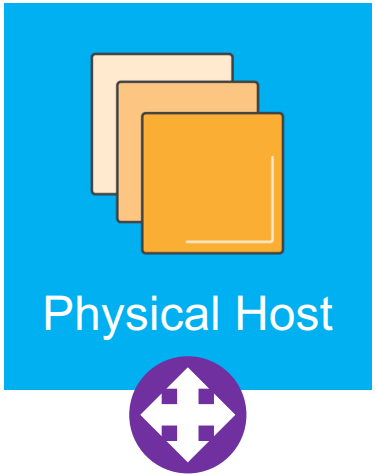
© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

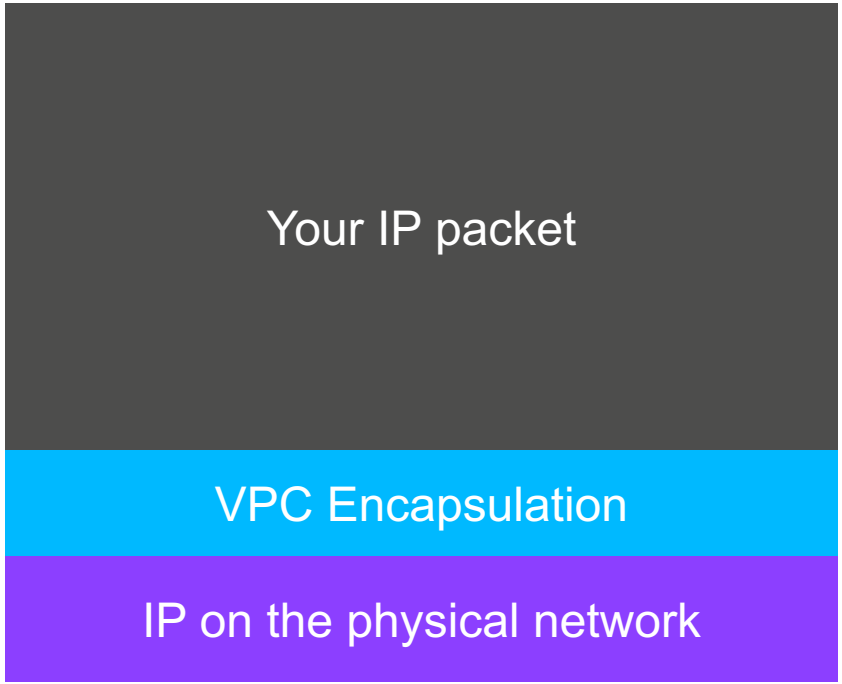
NAT Gateway and Network Load Balancer

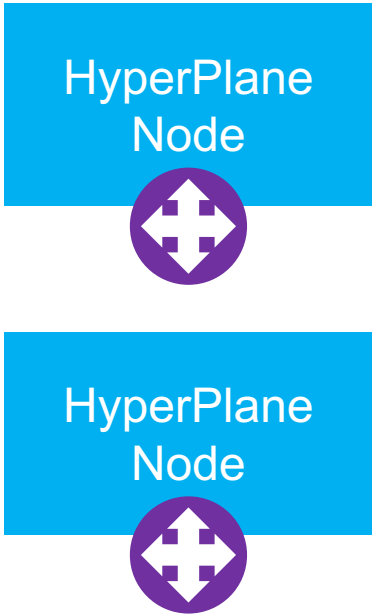


© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

HyperPlane







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

HyperPlane

HyperPlane nodes make transactional decisions and share state in tens of microseconds.

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

HyperPlane

For NAT: HyperPlane guarantees that connections to the same destination IP / destination port pair have a unique source port

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

HyperPlane

For NLB: HyperPlane selects the target instance or container that should handle a connection

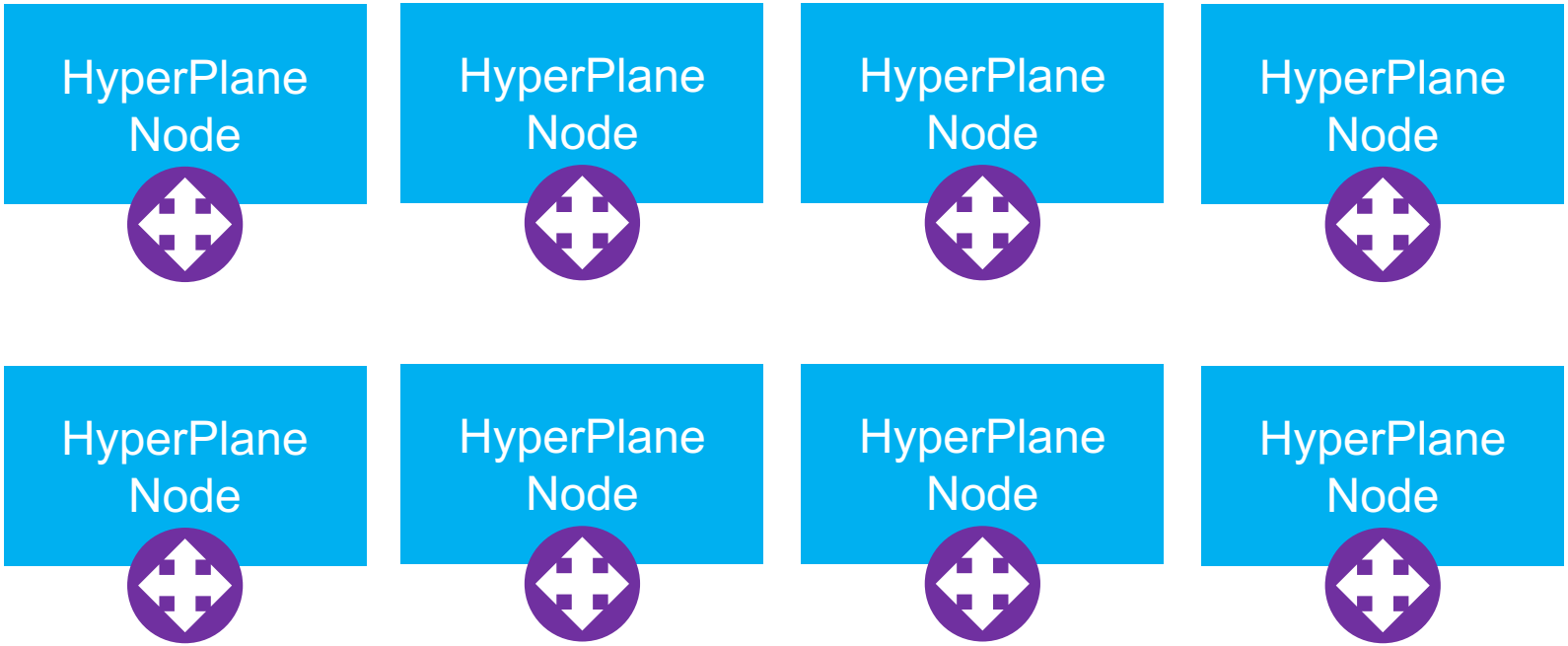
© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

HyperPlane

For security best practice, HyperPlane doesn't need to know about VPC mappings, only flows

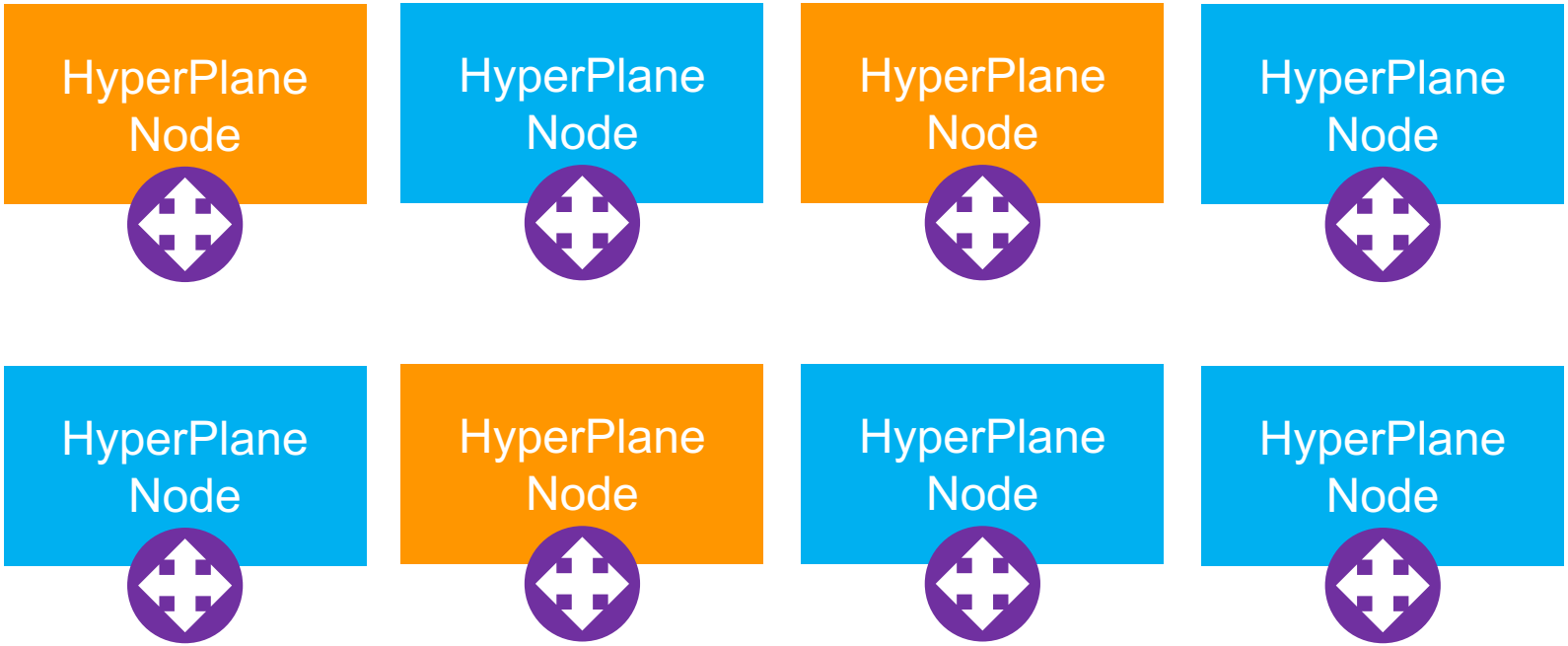
© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

HyperPlane and Shuffle Sharding



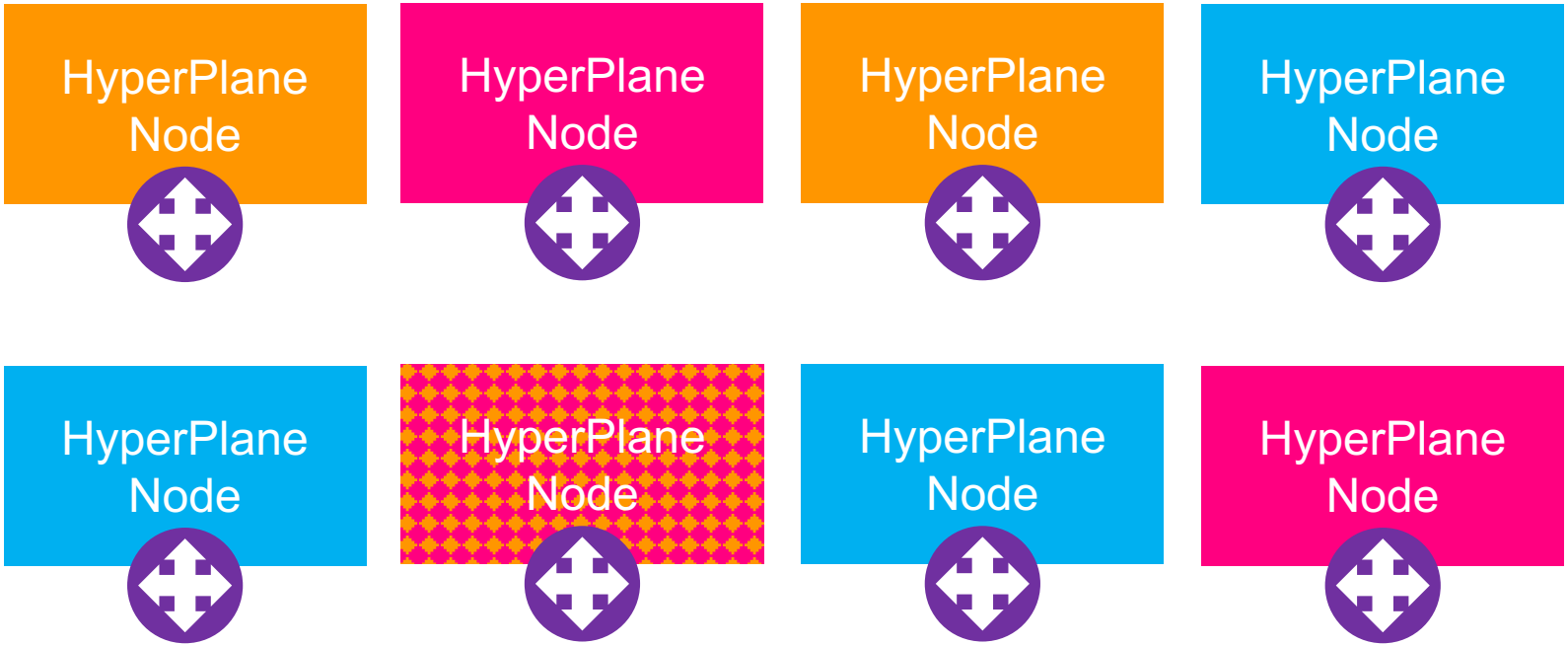
© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

HyperPlane and Shuffle Sharding



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

HyperPlane and Shuffle Sharding



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

HyperPlane and Shuffle Sharding

Potential Overlap	Percentage chance
0	18%
1	54%
2	26%
3	2%

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

HyperPlane and Shuffle Sharding

Potential Overlap	Percentage chance
0	77%
1	21%
2	1.8%
3	0.06%
4	0.0006
5	0.00000013

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

HyperPlane and Shuffle Sharding

Potential Overlap	Percentage chance
0	77%
1	21%
2	1.8%
3	**0%**
4	**0%**
5	**0%**

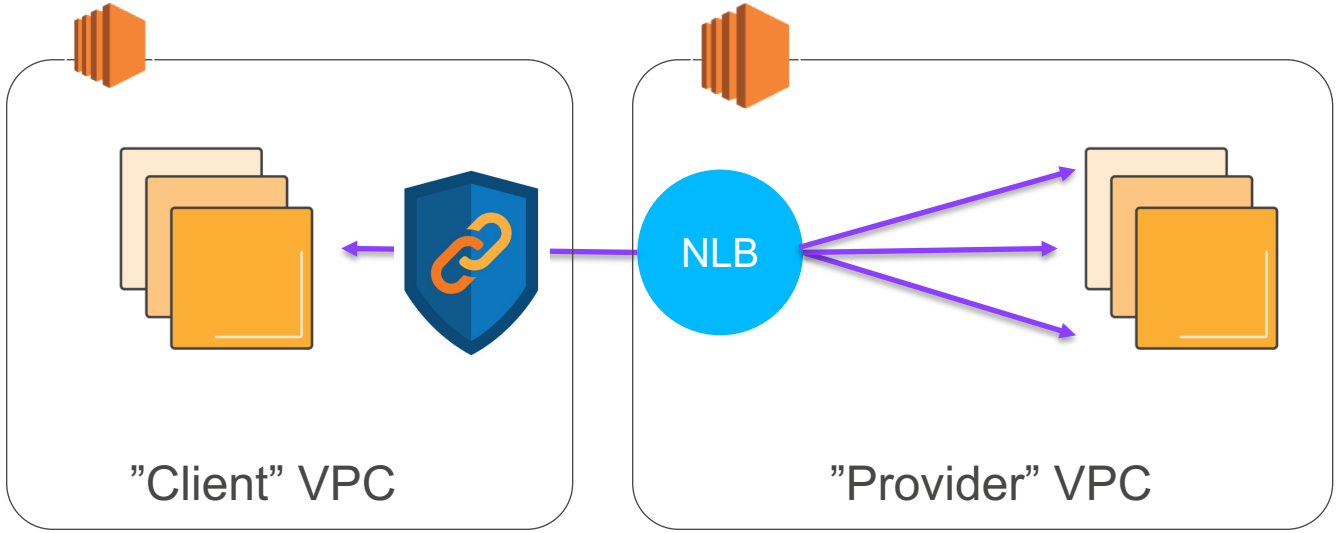
© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

More on HyperPlane

- Based on the S3 Load Balancer
- Used by Elastic Filesystem since launch
- Every HyperPlane resource has 5Gbit/sec of capacity by default, and scales in increments of 5Gbit/sec … to Terabits
- Sub-millisecond latency, hundreds of millions of connections, millions of connections per second

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

PrivateLink



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

PrivateLink

- Enables more compartmentalized VPCs; one per service, one per team
- Enables service providers and partners to offer private services into customer's private networks, including on-premises via Direct Connect
- Integration with the AWS Marketplace!

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

Key takeaways

- VPC is a software defined network that uses encapsulation to securely isolate customers
- VPCs can be controlled programmatically
- VPCs can be seamlessly integrated into existing networks via Direct Connect, VPN and Internet access

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

Key takeaways

- The VPC Network includes native support for tracking flows

- NATGW and NLB can be used to manage enormous connection loads, at scale, with high availability.

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

aws SUMMIT

Thank you!

Steve Seymour
Principal Specialist Solutions Architect, AWS
@sseymour

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