

Why *Networking* still matters in Cloud



William Collins
Principal Cloud Architect



william-collins



wcollins502



Slides

<https://wcollins.io/talks/2023/ctnug/>

Presented By:



dead adjective

 Save Word

\ 'ded  \

Definition of *dead* (Entry 1 of 3)

1 : deprived of life : no longer alive

// a *dead* tree

// *dead* soldiers

// missing and presumed *dead*

2 a (1) : having the appearance of death : DEATHLY

// in a *dead* faint

(2) : lacking power to move, feel, or respond : NUMB

// my arm feels *dead*

What does it mean to be DEAD?



<https://www.networkworld.com> › article › are-firewalls-... ⋮

Are Firewalls Dead? - Network World.com

Jul 18, 2012 — No, really. With so many of today's attacks coming over port 80, is your **firewall** providing any defense anymore? Has the **firewall** outgrown its ...

<https://oxfordcomputergroup.com> › resources › traditio... ⋮

The Traditional Perimeter is Dead, Now What?

Jan 12, 2017 — Instead of '**perimeter** thinking', we need to implement policies that protect data and information regardless of the device being used or its ...

<https://www.infosecurity-magazine.com> › infosec › zer... ⋮

The Wall Has Fallen, but Zero-Trust Architectures Can Save You

Oct 19, 2020 — A collection of CISOs operating as the Jericho Forum heralded the **death** of the **network perimeter** in 2004, announcing it as 'deperimeterization.' ...

What does it mean to be DEAD?



<https://www.networkworld.com/article/are-firewalls-...>

Are Firewalls Dead? - Network World.com

Jul 18, 2012 — No, really. With so many of today's attacks coming over port 80, is your **firewall** providing any defense anymore? Has the **firewall** outgrown its ...

<https://oxfordcomputergroup.com/resources/traditio...>

The Traditional Perimeter is Dead, Now What?

Jan 12, 2017 — Instead of '**perimeter** thinking', we need to implement policies that protect data and information regardless of the device being used or its ...

<https://www.infosecurity-magazine.com/infosec/zer...>

The Wall Has Fallen, but Zero-Trust Architectures Can Save You

Oct 19, 2020 — A collection of CISOs operating as the Jericho Forum heralded the **death** of the **network perimeter** in 2004, announcing it as 'deperimeterization.' ...



<https://...the-ip-address-is-dead>

The IP address is dead

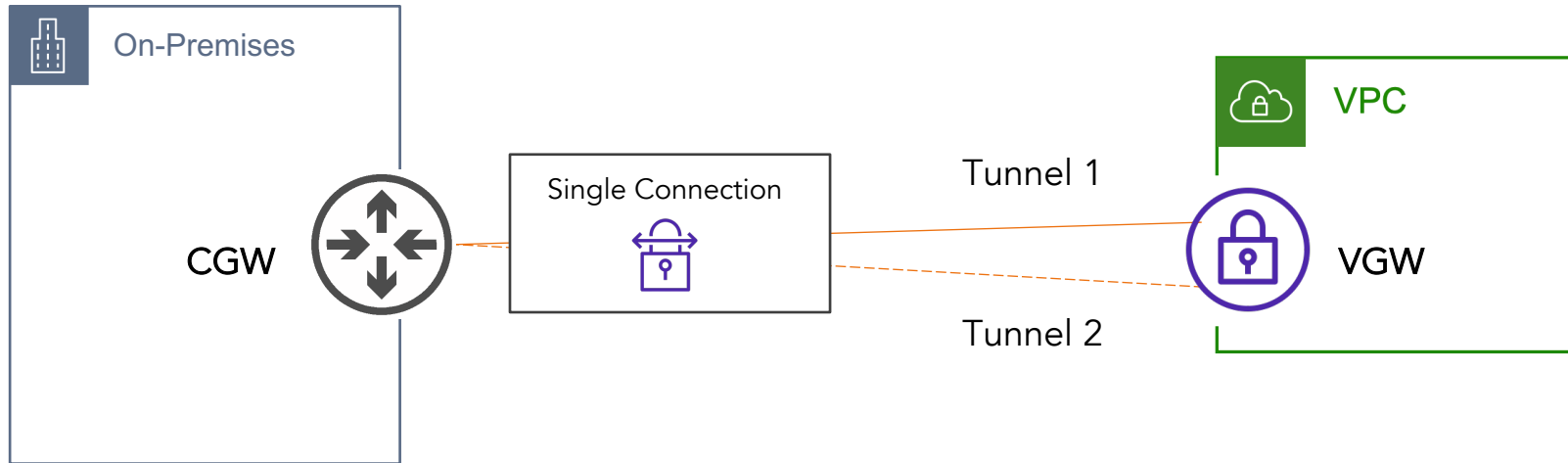
Jun 15, 2022 — Regardless of what you may have heard, **the IP address is in fact, dead.** Brought down by several public clouds that replicate the same ...

In the Beginning

Active Tunnel

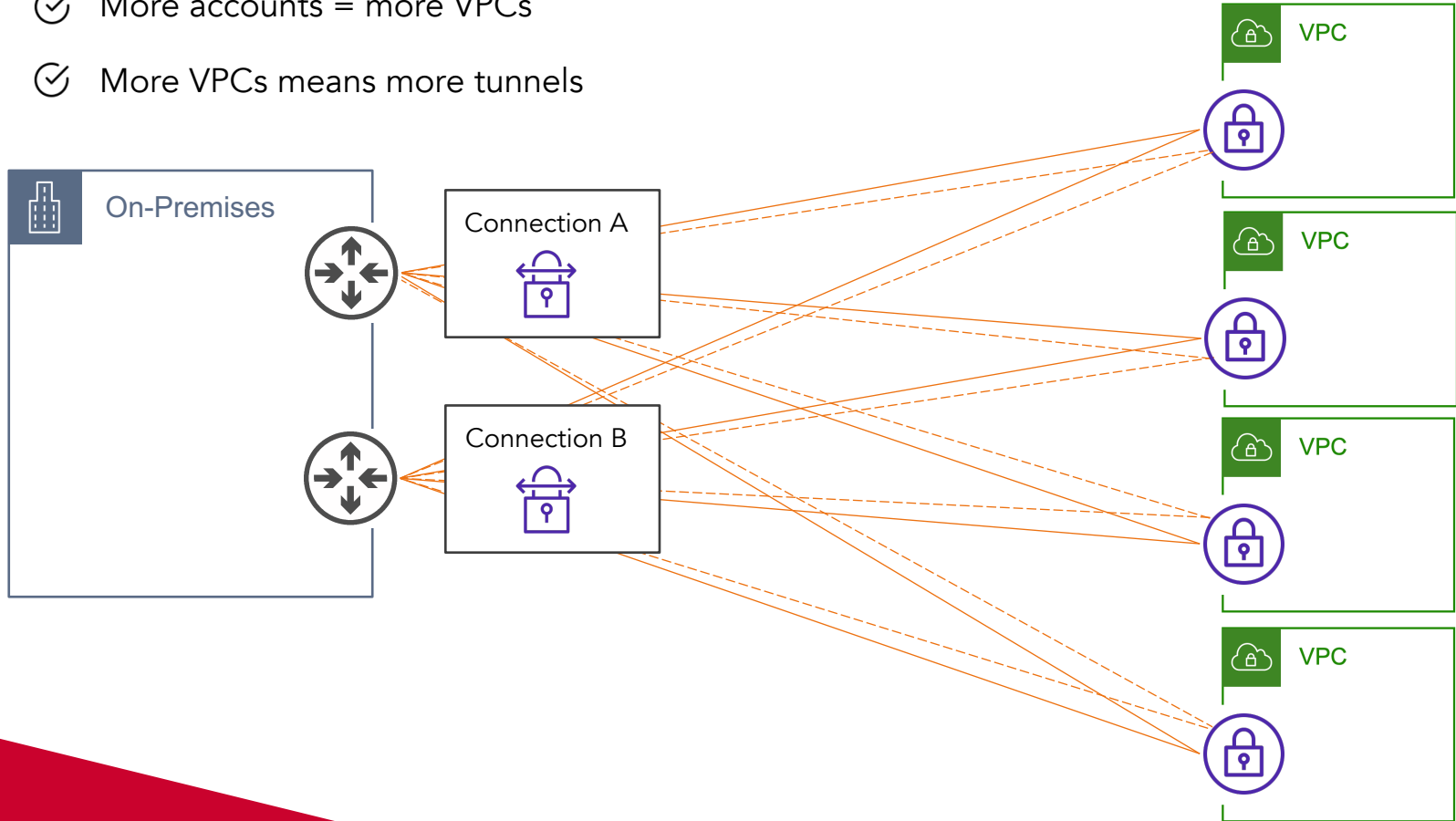
Standby Tunnel

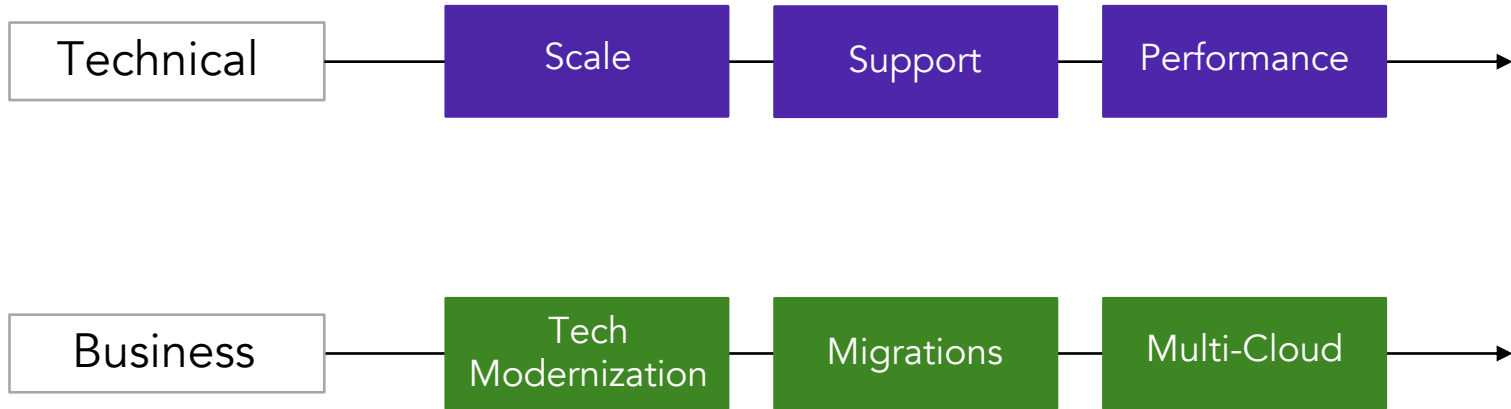
- ✓ 1x VPN connection = 2x VPN tunnels
- ✓ 1x VPN tunnel = 1.25 Gbps
- ✓ One tunnel is actively used

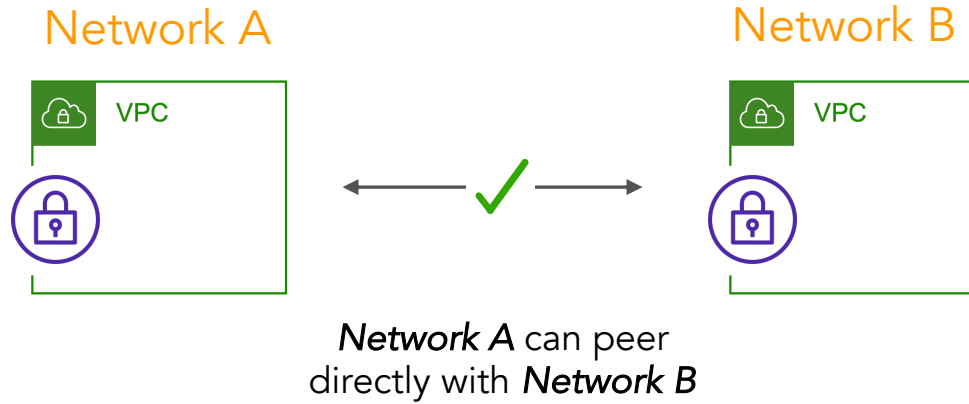


In the Beginning

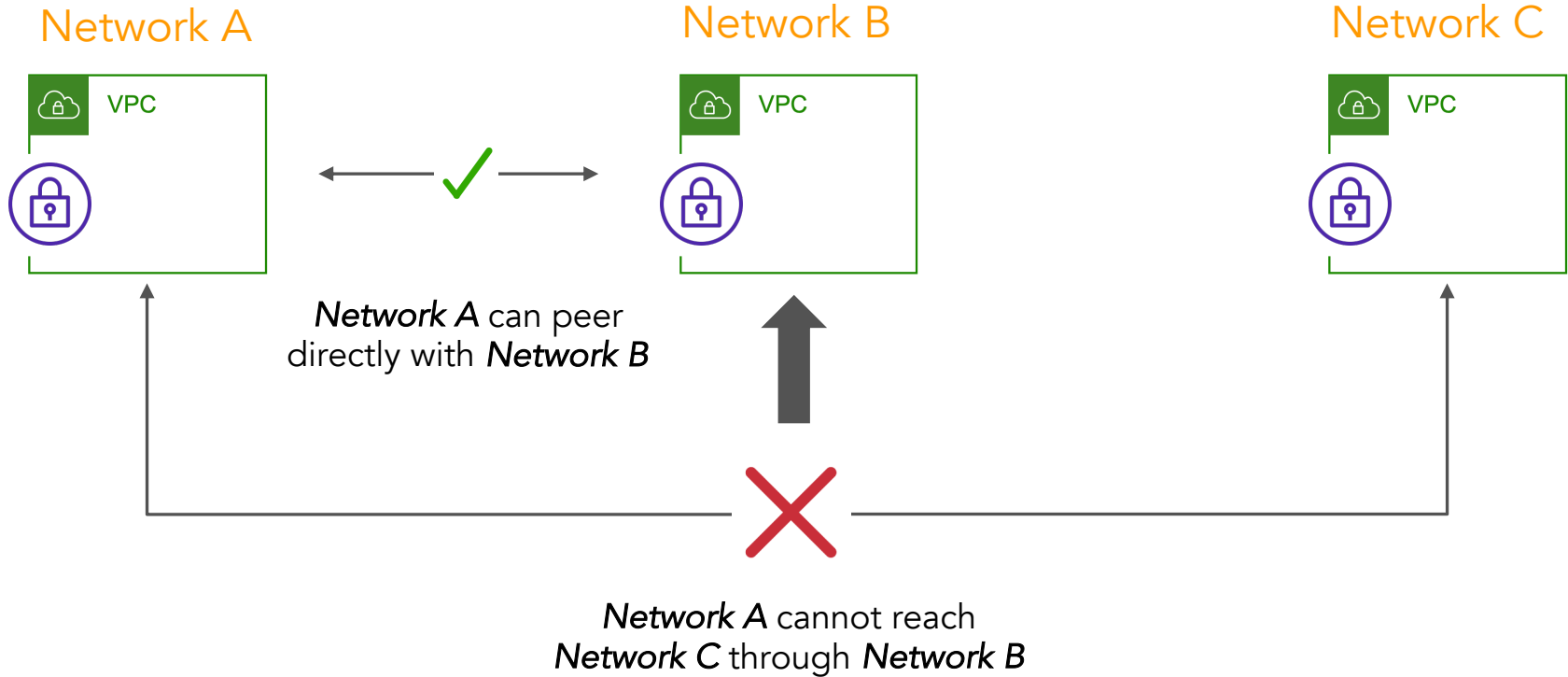
- ✓ Separate billing with accounts
- ✓ More accounts = more VPCs
- ✓ More VPCs means more tunnels







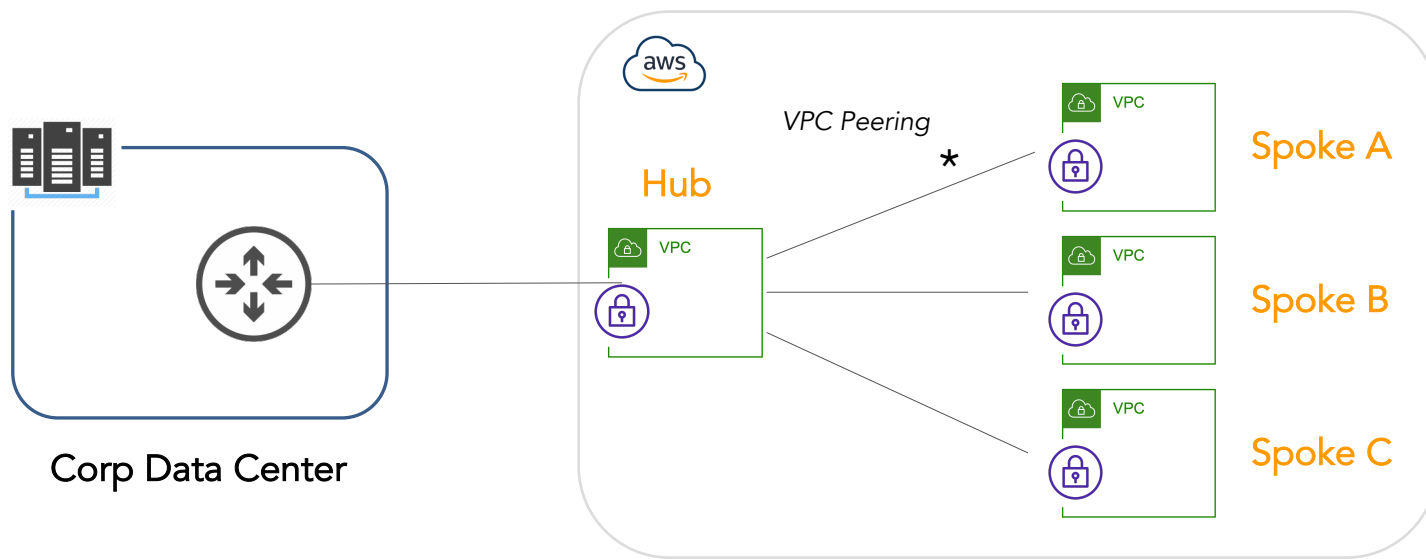
Things to Know





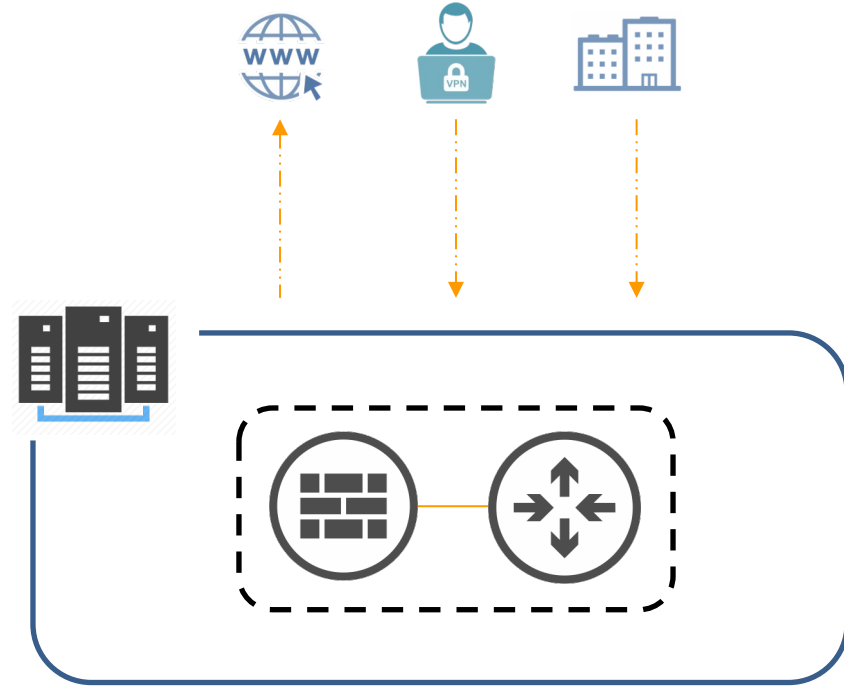
Important Patterns

- ✓ Spoke to Spoke
- ✓ Spoke internet egress
- ✓ Spoke to on-premises
- ✓ Spoke internet ingress

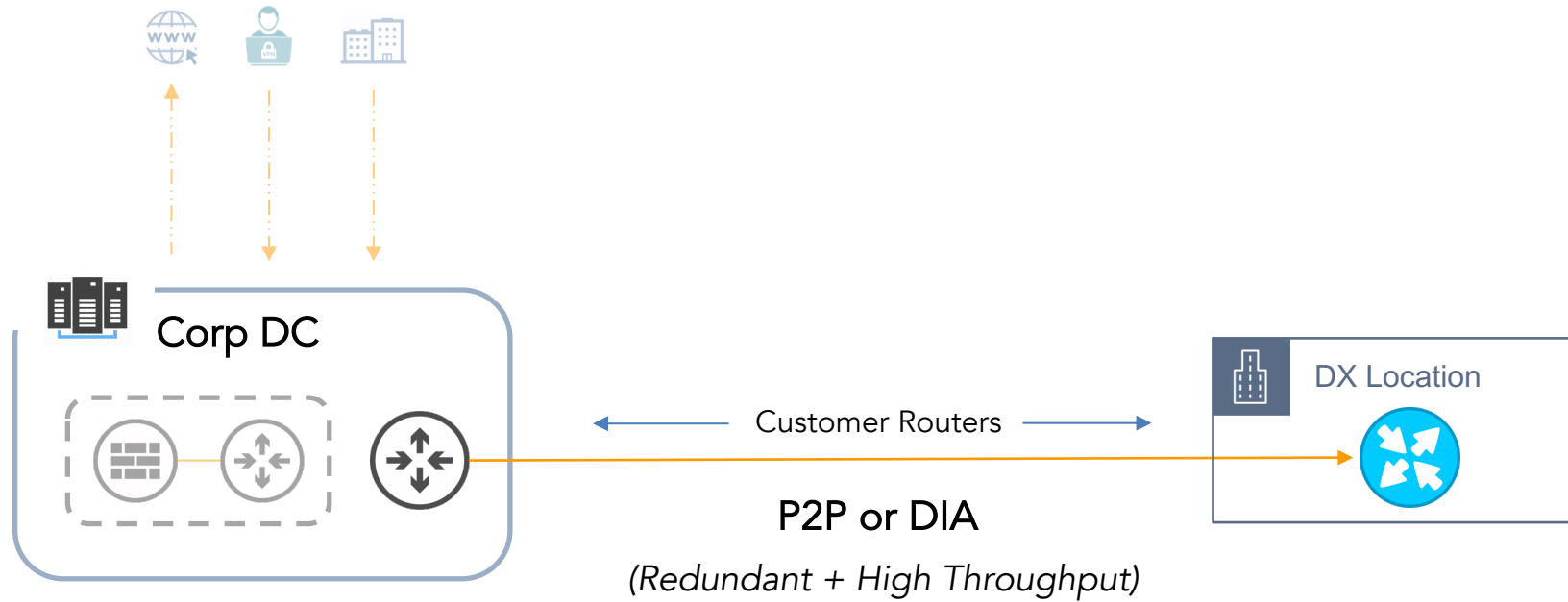


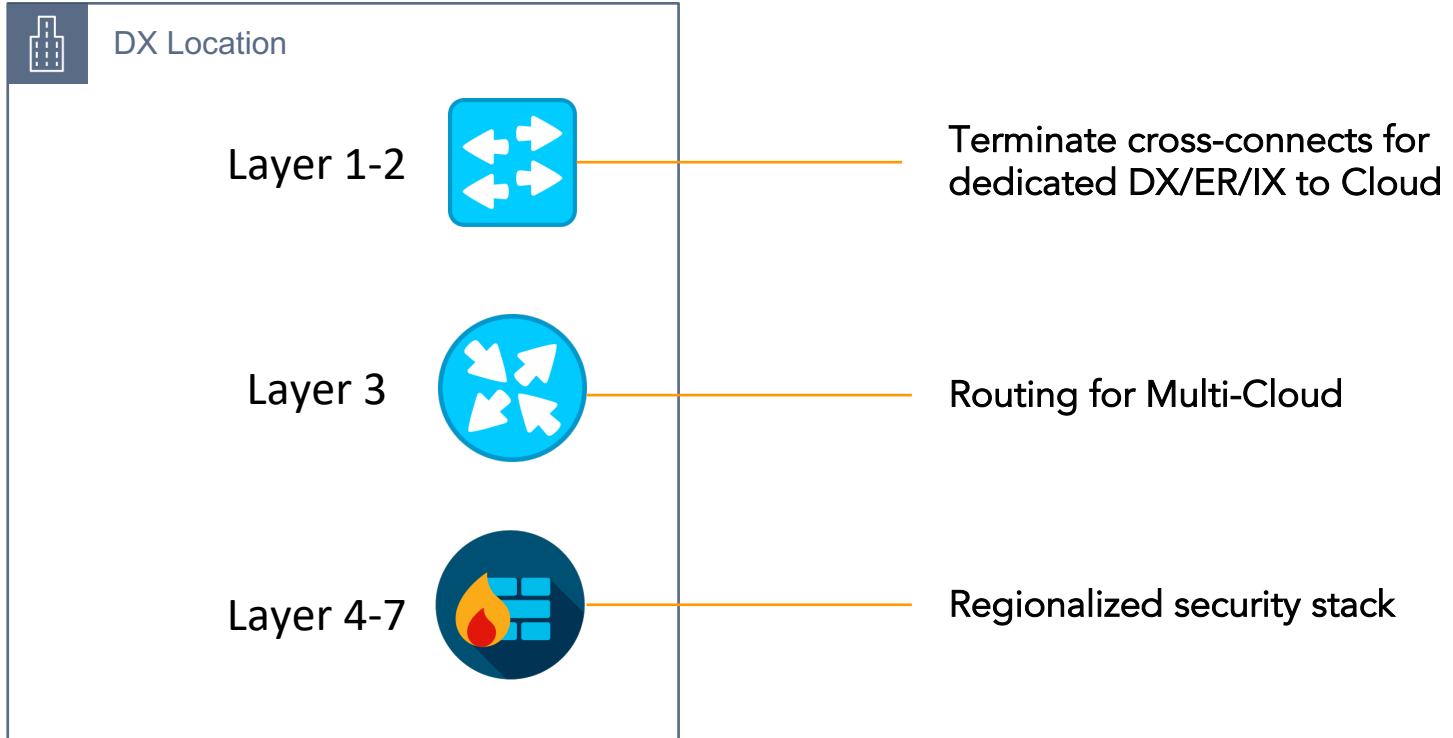


Don't disrupt existing
network infrastructure



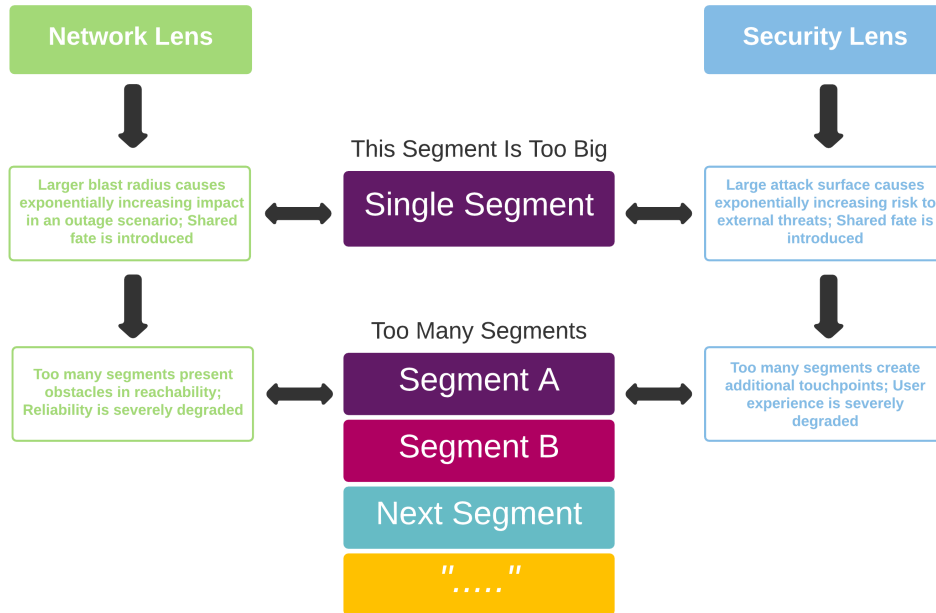
Corp Data Center







Same problem, different lens

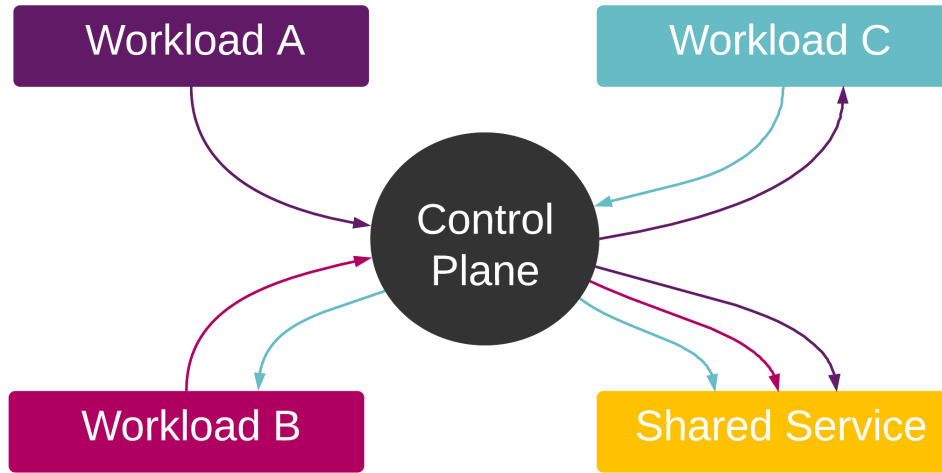


* Macro Segments

- ✓ North-South communication
- ✓ Higher-Level categories
- ✓ Paves the way for 'micro' segments



Same problem, different lens



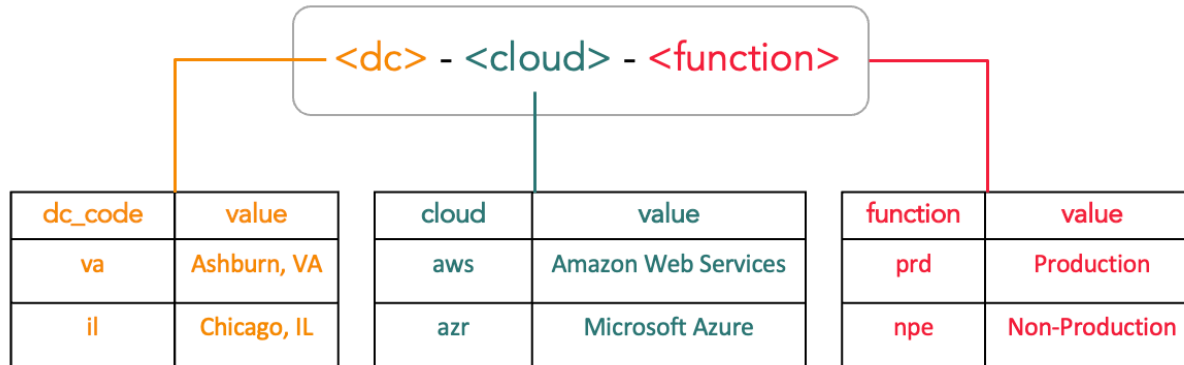
* Micro Segments

- ✓ East-West communication
- ✓ Granular / workload focused
- ✓ Dependent on well-architected macro-segmentation

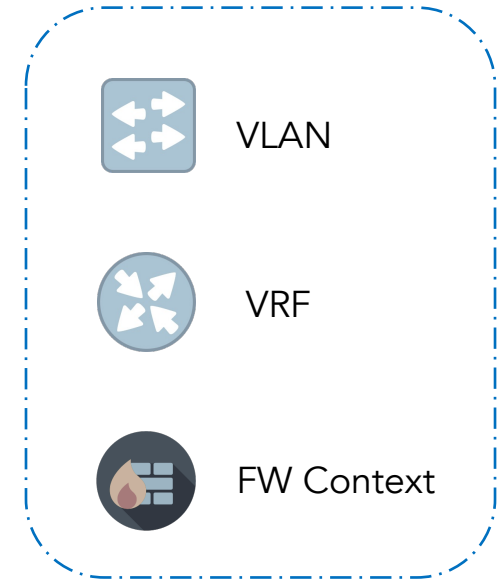


Meaningful Names = Power

- ✓ Self-Descriptive: Relevant to NetEng, SecEng, and Ops
- ✓ Self-Organizing: Accommodate additional CNFs, Clouds, and functions
- ✓ Operationally-Sound: Short, lowercase, and hyphen-separated



va-aws-npe





BGP Communities

- ✓ Link Function: Learned via Primary or Secondary peer
- ✓ DC Origin: Data Center the prefix originated from
- ✓ Cloud Provider: Cloud provider the prefix originated from

<type> : <value>

type	meaning
1	link function
2	dc origin
3	cloud provider

type	meaning
1 2	primary peer secondary peer
1 2 3	dc-01 dc-02 dc-03
1 2 3	aws azure gcp

<type> : <value>

type	meaning
1	link function
2	dc origin
3	cloud provider

type	meaning
1 2	primary peer secondary peer
1 2 3	dc-01 dc-02 dc-03
1 2 3	aws azure gcp



```
route-map aws-in permit 10  
match ip address prefix-list aws  
set community 1:1 2:1 3:1
```

1:1

2:1

3:1

AWS route

Originated from DC-01

Learned via primary



```
route-map azr-in permit 10  
match ip address prefix-list azr  
set community 1:2 2:2 3:2
```

1:2

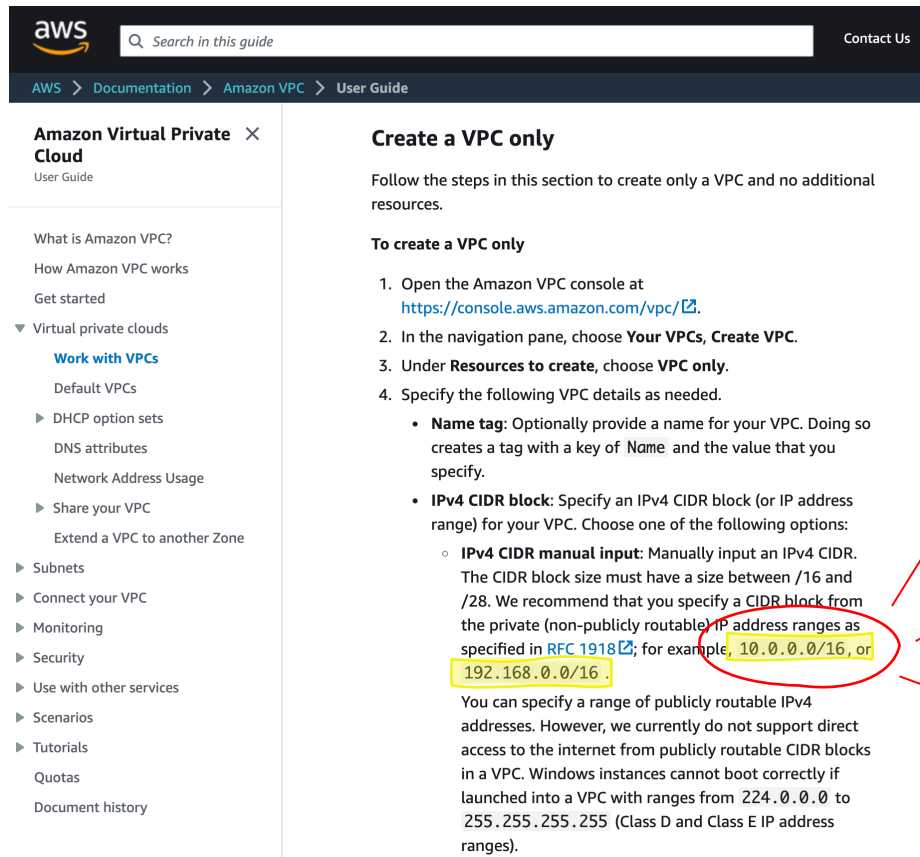
2:2

3:2

Azure route

Originated from DC-02

Learned via secondary



The screenshot shows the AWS documentation page for 'Create a VPC only'. The left sidebar contains a navigation menu with options like 'What is Amazon VPC?', 'How Amazon VPC works', 'Get started', 'Virtual private clouds', 'Work with VPCs', 'Default VPCs', 'DHCP option sets', 'DNS attributes', 'Network Address Usage', 'Share your VPC', 'Extend a VPC to another Zone', 'Subnets', 'Connect your VPC', 'Monitoring', 'Security', 'Use with other services', 'Scenarios', 'Tutorials', 'Quotas', and 'Document history'. The main content area is titled 'Create a VPC only' and includes instructions on how to create a VPC. A red circle highlights the text '10.0.0.0/16' in the 'IPv4 CIDR block' section, with red arrows pointing from this circle to three VPC diagrams on the right.

aws Search in this guide Contact Us

AWS > Documentation > Amazon VPC > User Guide

Amazon Virtual Private Cloud User Guide

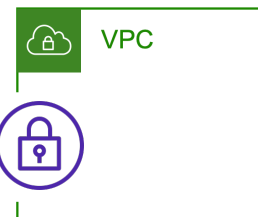
Create a VPC only

Follow the steps in this section to create only a VPC and no additional resources.

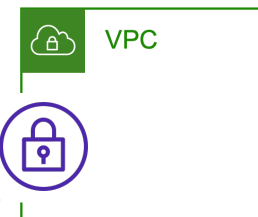
To create a VPC only

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the navigation pane, choose **Your VPCs**, **Create VPC**.
3. Under **Resources to create**, choose **VPC only**.
4. Specify the following VPC details as needed.
 - **Name tag**: Optionally provide a name for your VPC. Doing so creates a tag with a key of `Name` and the value that you specify.
 - **IPv4 CIDR block**: Specify an IPv4 CIDR block (or IP address range) for your VPC. Choose one of the following options:
 - **IPv4 CIDR manual input**: Manually input an IPv4 CIDR. The CIDR block size must have a size between /16 and /28. We recommend that you specify a CIDR block from the private (non-publicly routable) IP address ranges as specified in [RFC 1918](#); for example, `10.0.0.0/16`, or `192.168.0.0/16`.

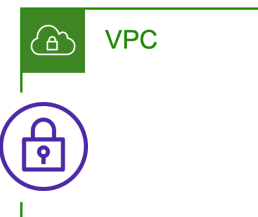
You can specify a range of publicly routable IPv4 addresses. However, we currently do not support direct access to the internet from publicly routable CIDR blocks in a VPC. Windows instances cannot boot correctly if launched into a VPC with ranges from `224.0.0.0` to `255.255.255.255` (Class D and Class E IP address ranges).



Network A
10.0.0.0/16



Network B
10.0.0.0/16

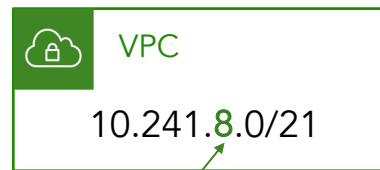
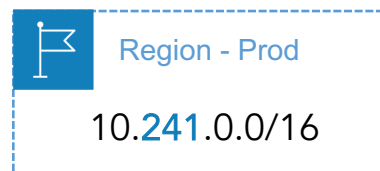
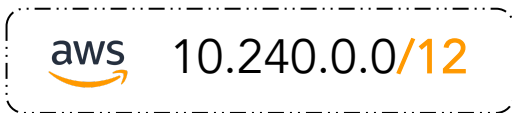
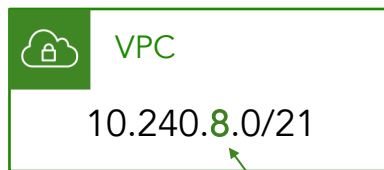
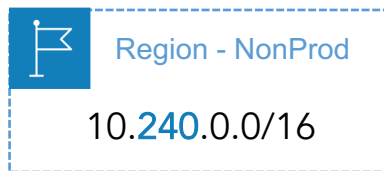


Network C
10.0.0.0/16



IP Addressing
still matters...

Even numbered
/16 allocated to all
non-production



```
> ipcalc 10.240.0.0/12
Address: 10.240.0.0
Netmask: 255.240.0.0 = 12
Wildcard: 0.15.255.255
=>
Network: 10.240.0.0/12
HostMin: 10.240.0.1
HostMax: 10.255.255.254
Broadcast: 10.255.255.255
Hosts/Net: 1048574
```

```
00001010.1111 0000.00000000.00000000
11111111.1111 0000.00000000.00000000
00000000.0000 1111.11111111.11111111
=>
00001010.1111 0000.00000000.00000000
00001010.1111 0000.00000000.00000001
00001010.1111 1111.11111111.11111110
00001010.1111 1111.11111111.11111111
Class A, Private Internet
```

Odd numbered
/16 allocated to
all production

3rd octet matches between
NonProd and Prod VPCs.

Looking into the Future with (*NaaS*)

Sites



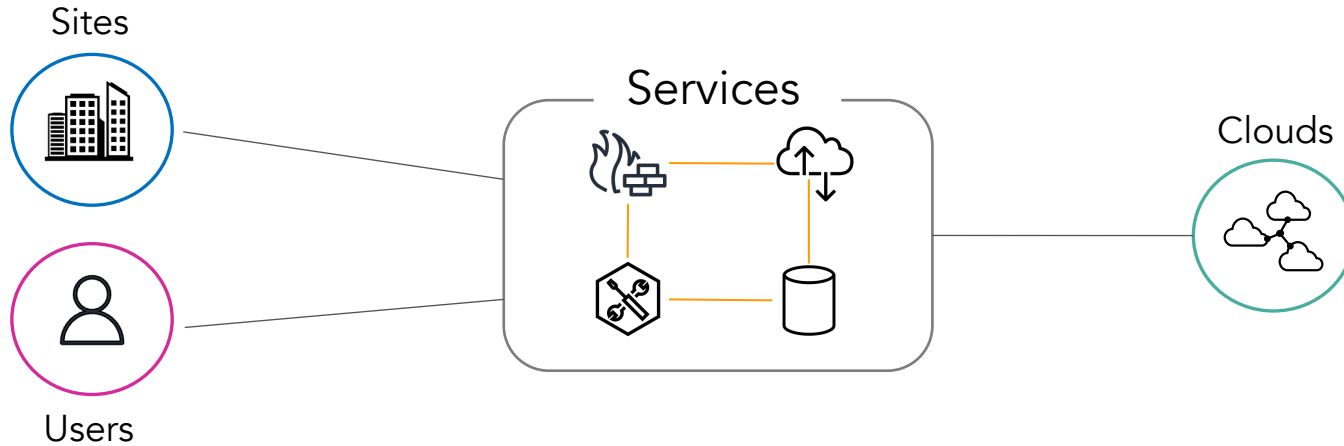
Users



Clouds



Looking into the Future with (NaaS)



Deploy, and operate
networking to, inside,
and across clouds

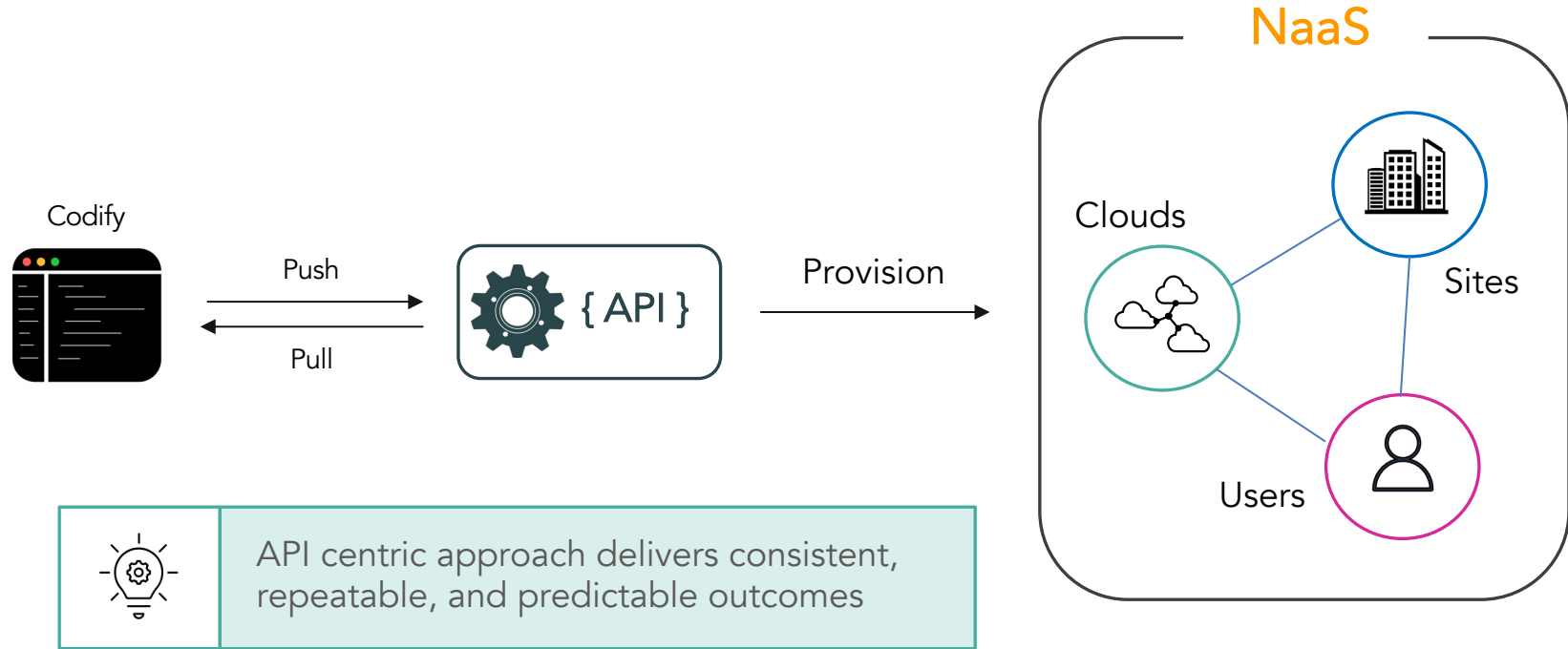


Common controls,
policy, security, and
governance



Integrate with
best-of-breed
services

Looking into the Future with (NaaS)



Thanks!

Presented By:

(US)NUA
US Networking User Association