(CT)NUG
Connecticut Networking User Group

Why *Networking* still matters in Cloud

William Collins
Principal Cloud Architect

in william-collins

wcollins502

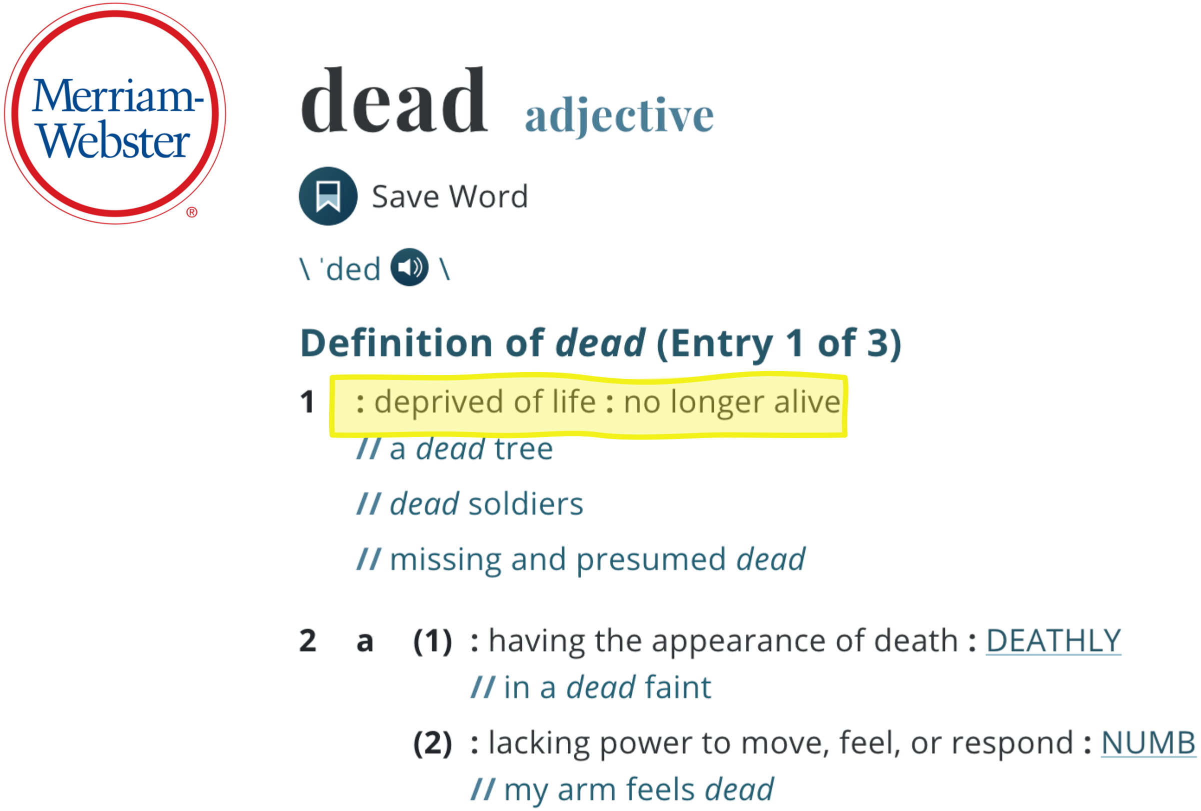
Slides

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

Presented By:

(US)NUA
US Networking User Association

What does it mean to be **DEAD?**



Merriam-Webster

dead adjective

Save Word

\ ˈded \

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

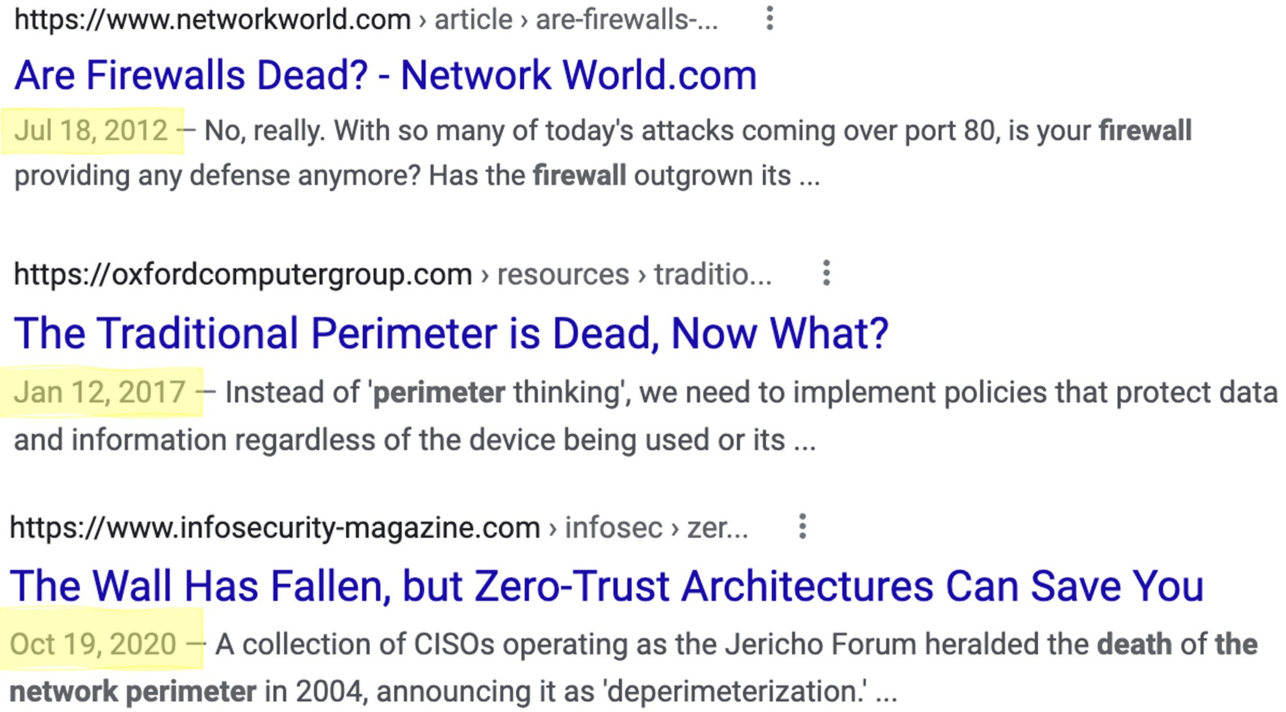
// in a *dead* faint

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

// my arm feels *dead*

(CT)NUG
Connecticut Networking User Group

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...

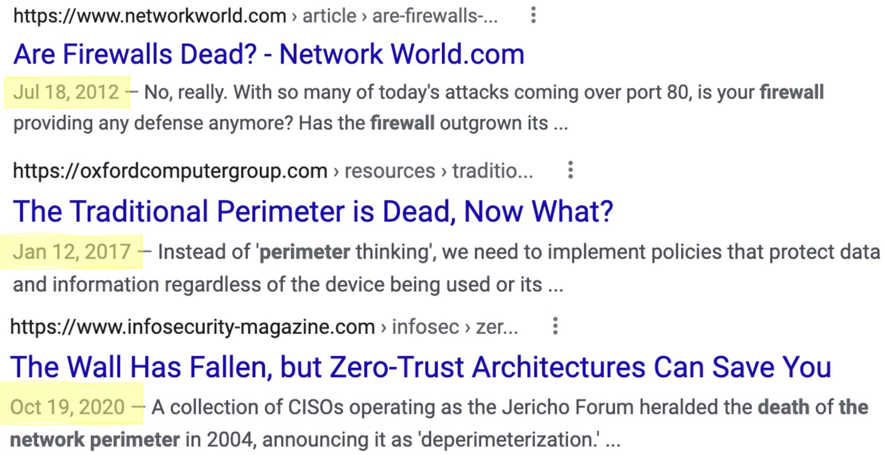
The Wall Has Fallen, but Zero-Trust Architectures Can Save You

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.' ...

Presented By:
(US)NUA
US Networking User Association

(CT)NUG
Connecticut Networking User Group

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...

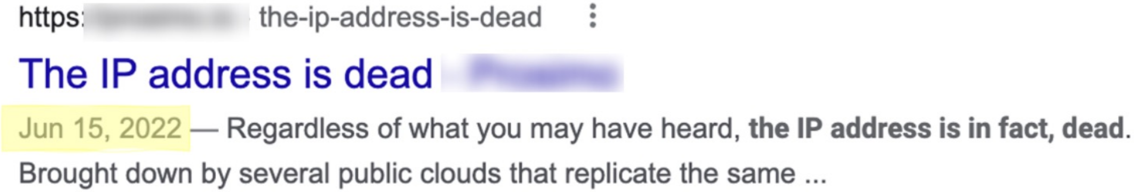
The Traditional Perimeter is Dead, Now What?

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:[redacted] the-ip-address-is-dead

The IP address is dead [redacted]

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 ...

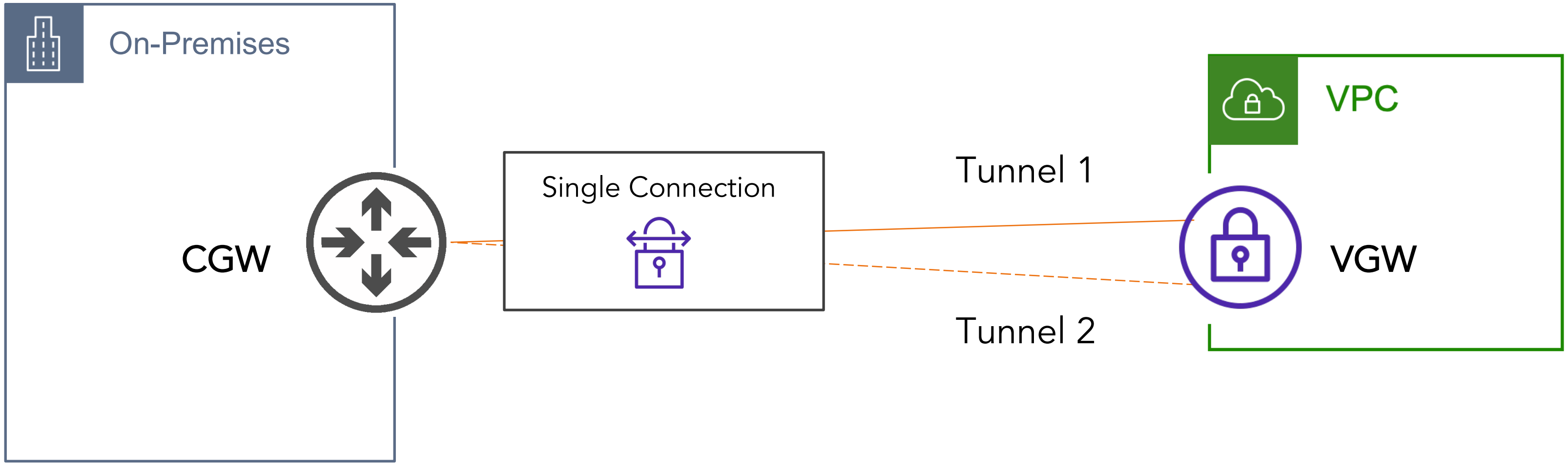
Presented By:
(US)NUA
US Networking User Association

In the Beginning

Active Tunnel ———

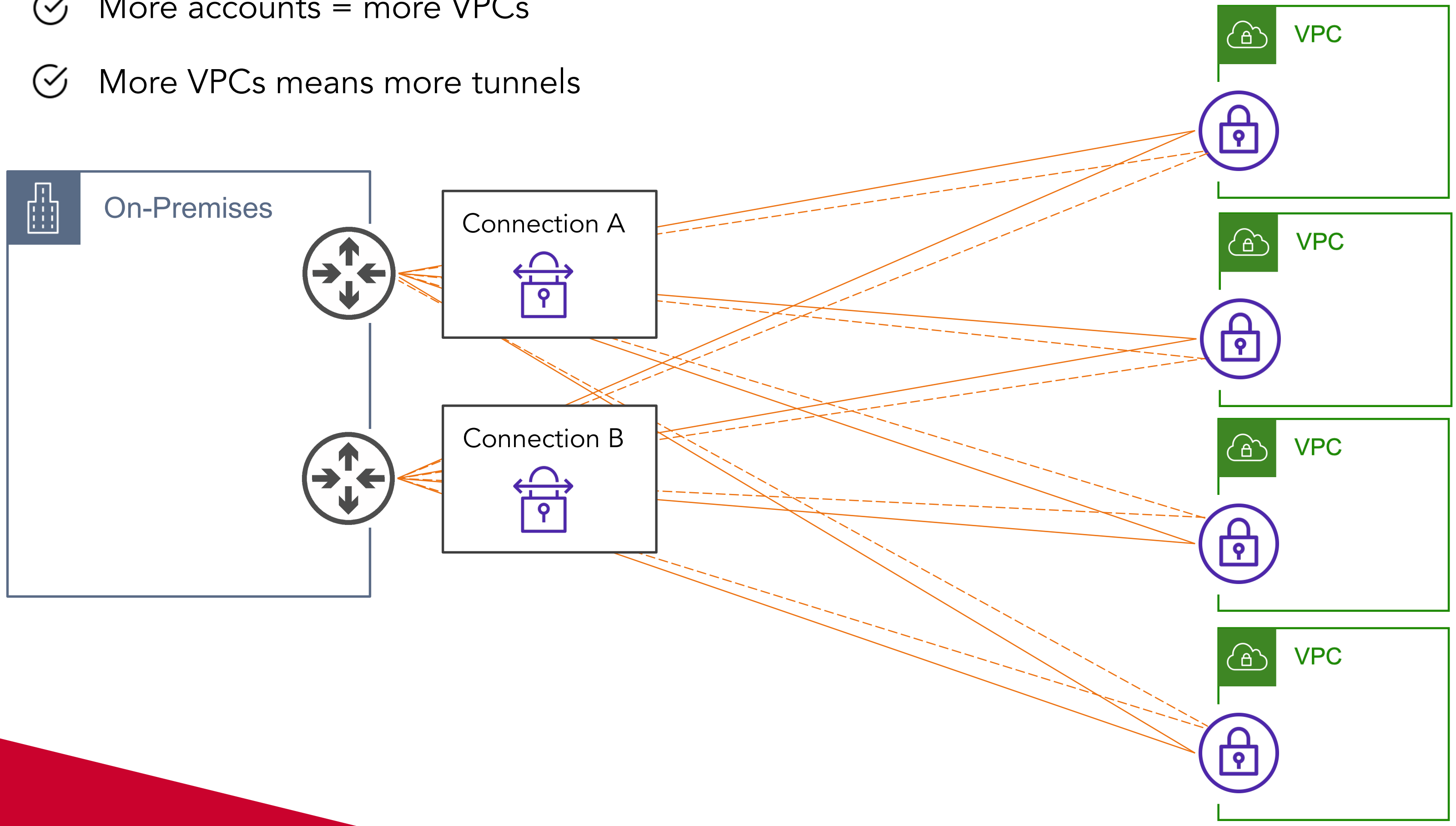
Standby Tunnel – – – –

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

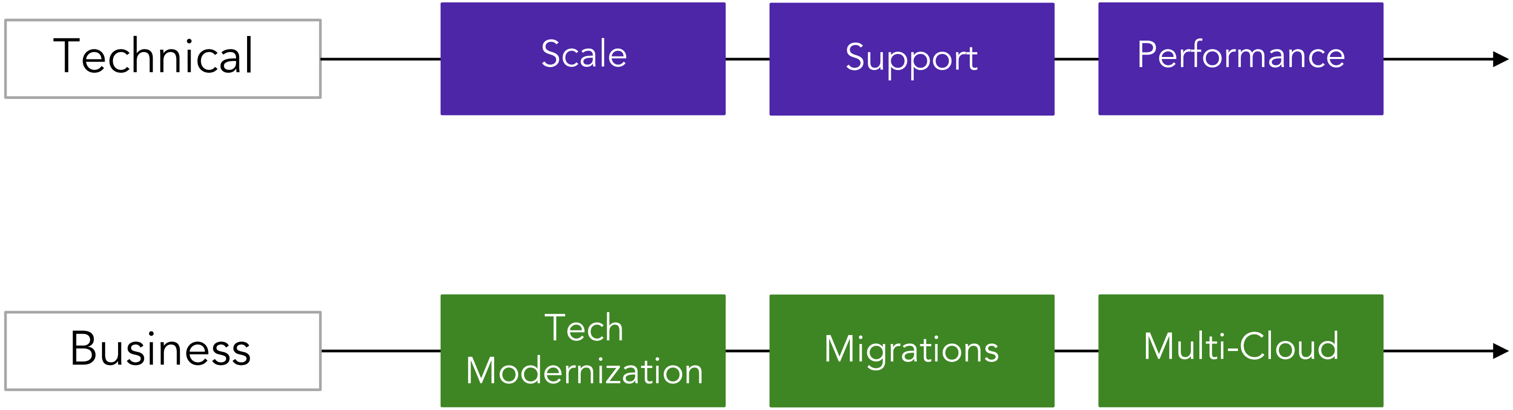


In the Beginning

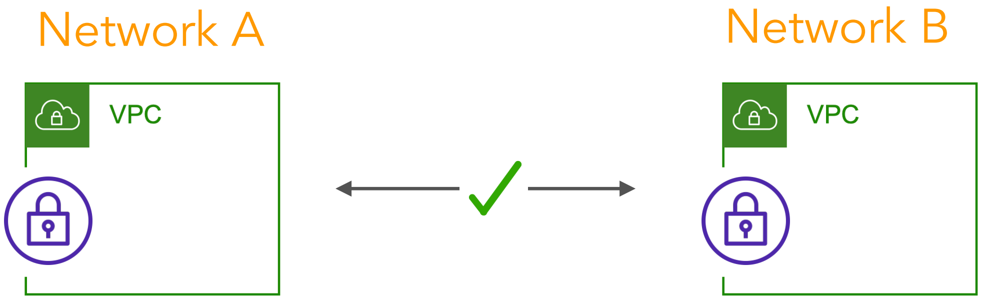
- ✓ Separate billing with accounts
- ✓ More accounts = more VPCs
- ✓ More VPCs means more tunnels



In the Beginning

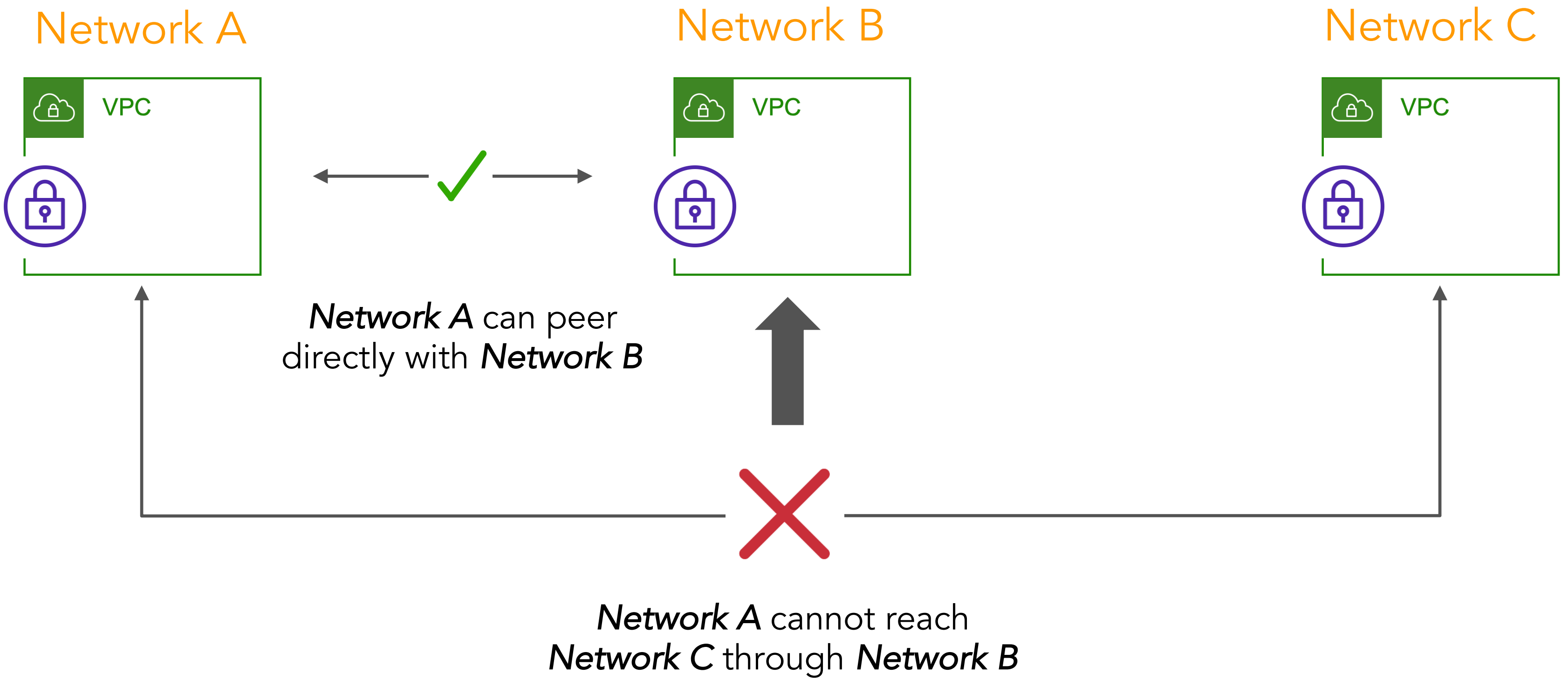


Things to Know



Network A can peer directly with ***Network B***

Things to Know



Network A can peer directly with ***Network B***

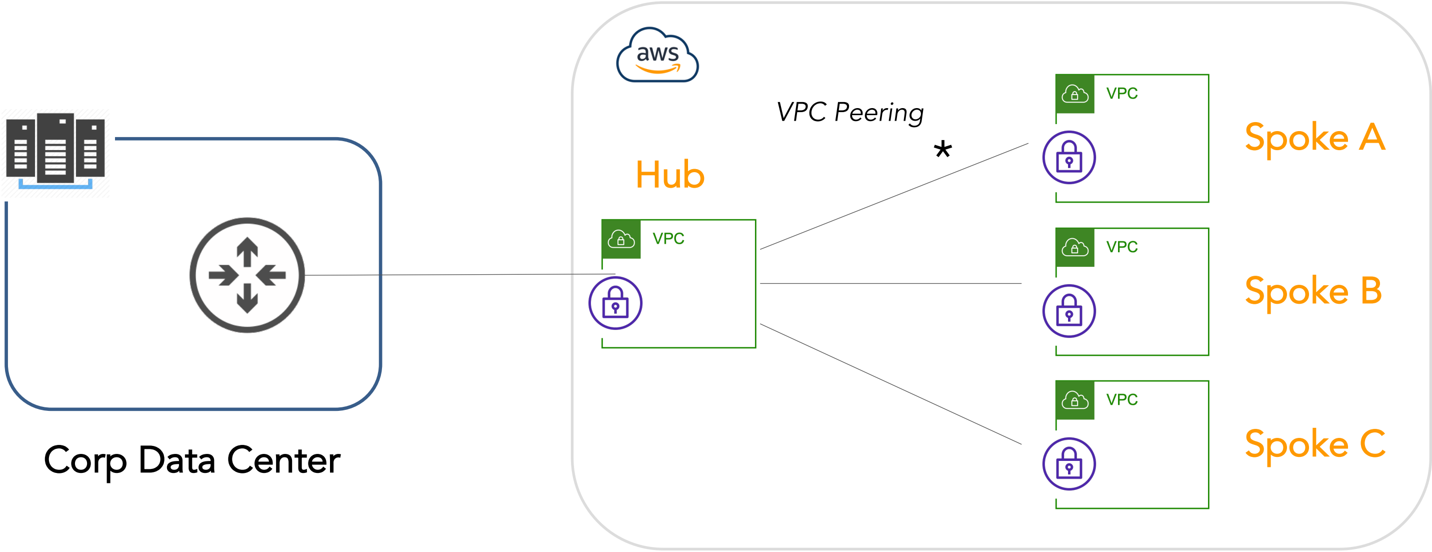
Network A cannot reach ***Network C*** through ***Network B***

(CT)NUG
Connecticut Networking User Group

Things to Know

Important Patterns

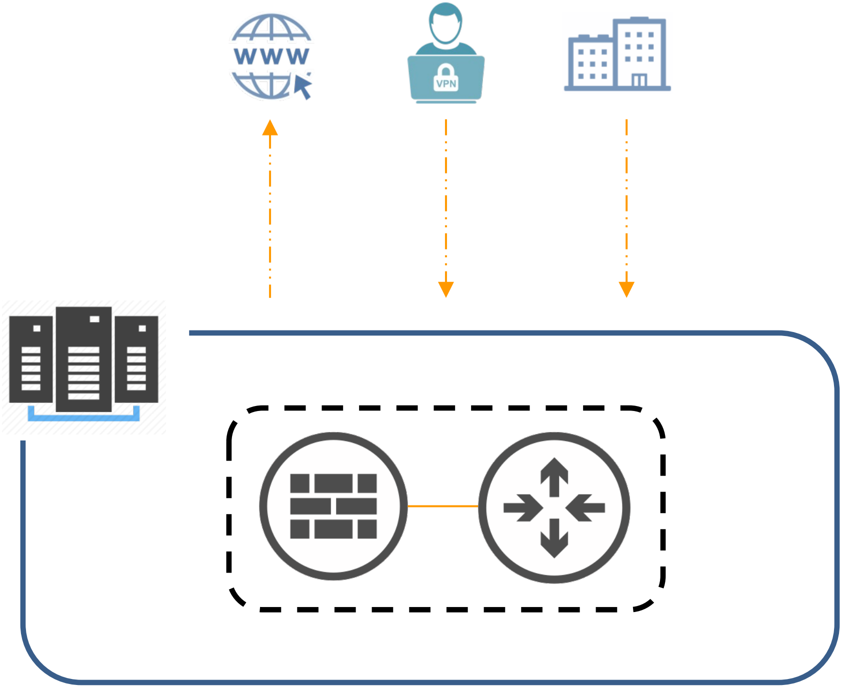
- ✓ Spoke to Spoke
- ✓ Spoke to on-premises
- ✓ Spoke internet egress
- ✓ Spoke internet ingress



Presented By:
(US)NUA
US Networking User Association

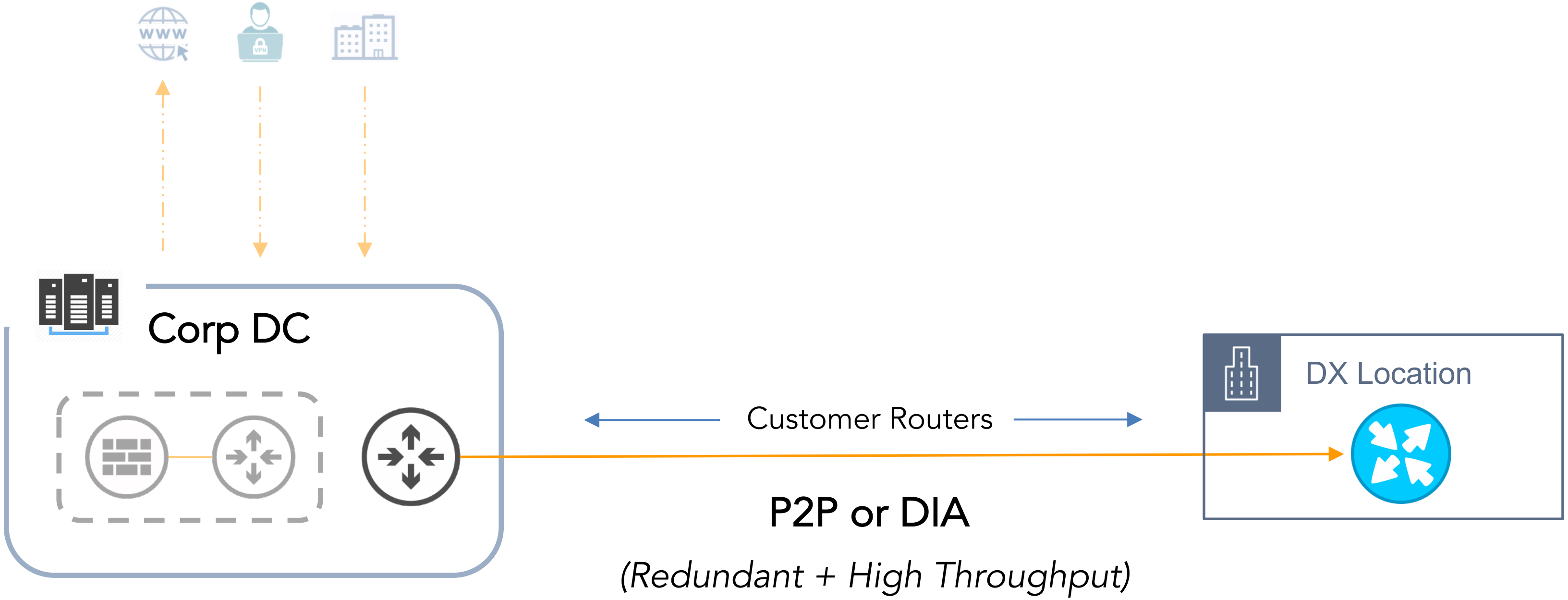
Old meets *New*

✓ Don't disrupt existing network infrastructure

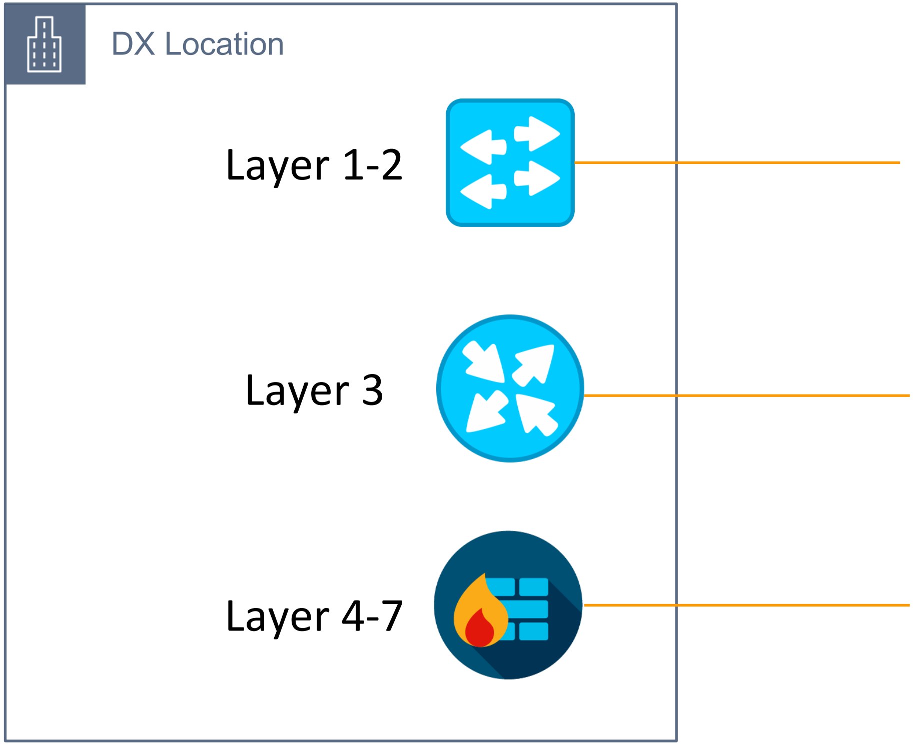


Corp Data Center

Old meets *New*



Old meets *New*



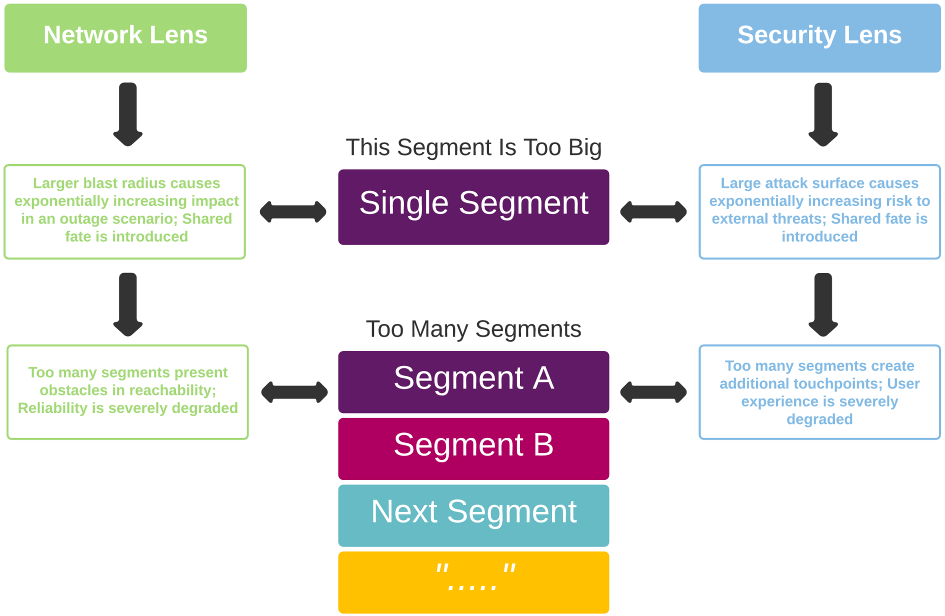
Terminate cross-connects for dedicated DX/ER/IX to Cloud

Routing for Multi-Cloud

Regionalized security stack

Thinking through *Segmentation*

Same problem, different lens



Network Lens

Security Lens

This Segment Is Too Big

Single Segment

Larger blast radius causes exponentially increasing impact in an outage scenario; Shared fate is introduced

Large attack surface causes exponentially increasing risk to external threats; Shared fate is introduced

Too Many Segments

Segment A

Segment B

Next Segment

"….."

Too many segments present obstacles in reachability; Reliability is severely degraded

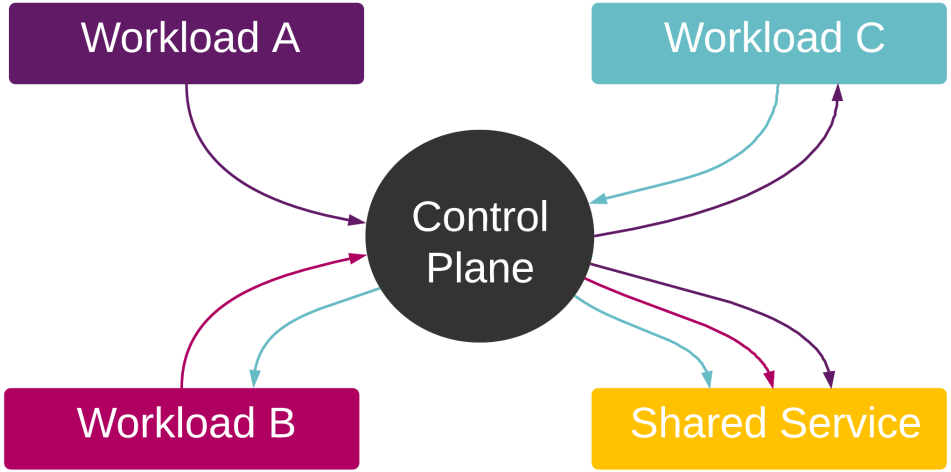
Too many segments create additional touchpoints; User experience is severely degraded

* Macro Segments

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

Thinking through *Segmentation*

Same problem, different lens



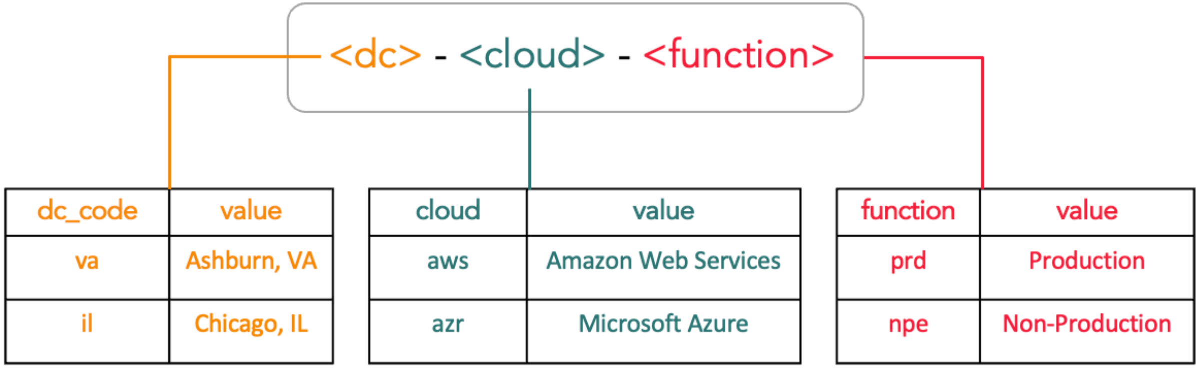
* Micro Segments

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

Themes and Schemes - *Names*

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

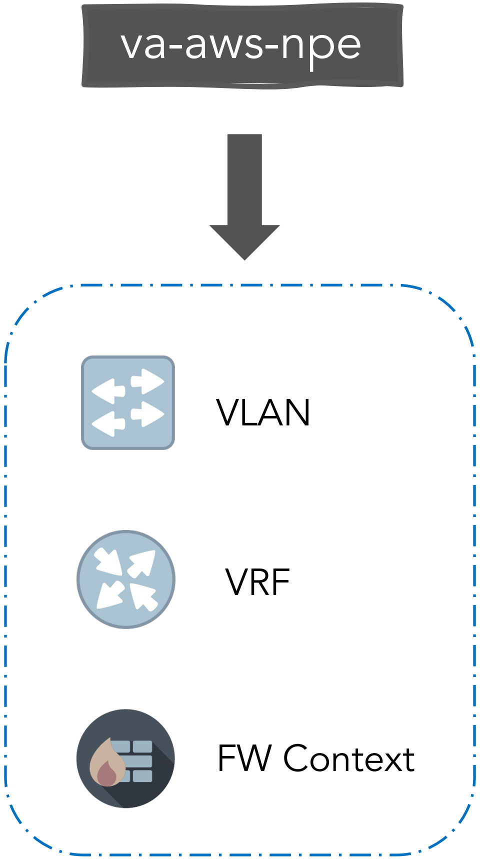


<dc> - <cloud> - <function>

dc_code	value
va	Ashburn, VA
il	Chicago, IL

cloud	value
aws	Amazon Web Services
azr	Microsoft Azure

function	value
prd	Production
npe	Non-Production



va-aws-npe

VLAN

VRF

FW Context

Themes and Schemes - *Routing*

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

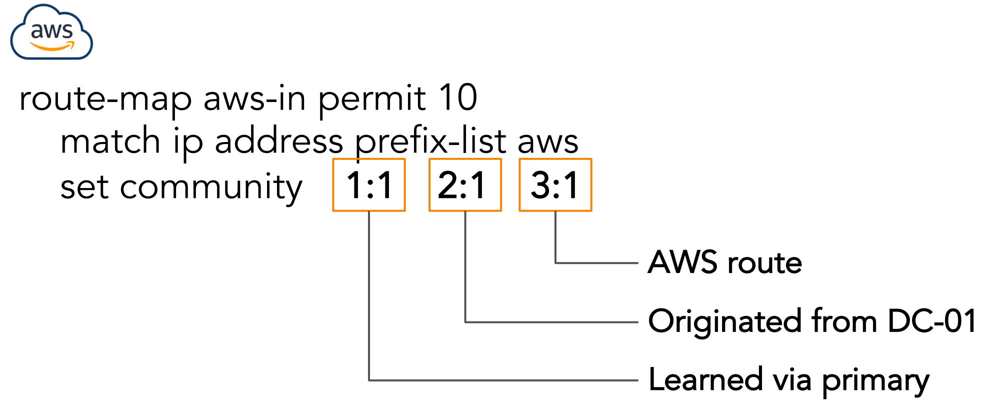
type	meaning
1 2	primary peer secondary peer
1 2 3	dc-01 dc-02 dc-03
1 2 3	aws azure gcp

Themes and Schemes - *Routing*

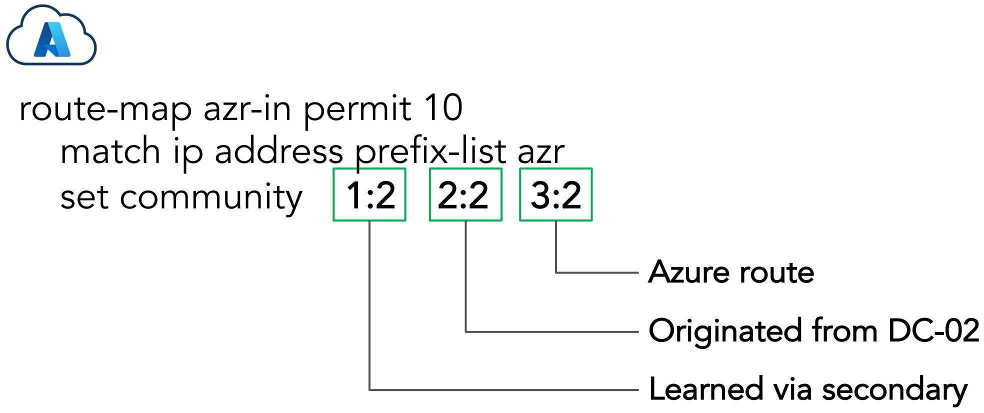
<type> : <value>

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



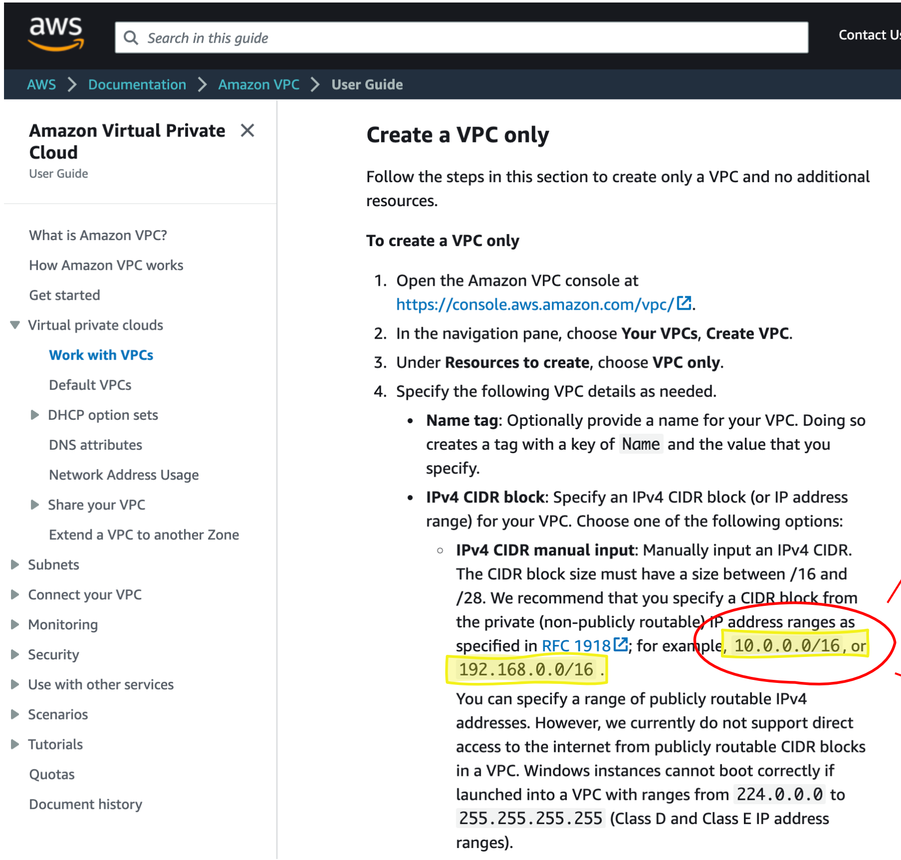
```
route-map aws-in permit 10
   match ip address prefix-list aws
   set community 1:1 2:1 3:1
```



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

(CT)NUG
Connecticut Networking User Group

Stepping on Land Mines


aws | Search in this guide | Contact Us

AWS > Documentation > Amazon VPC > User Guide

Amazon Virtual Private Cloud
User Guide

- 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
- Document history

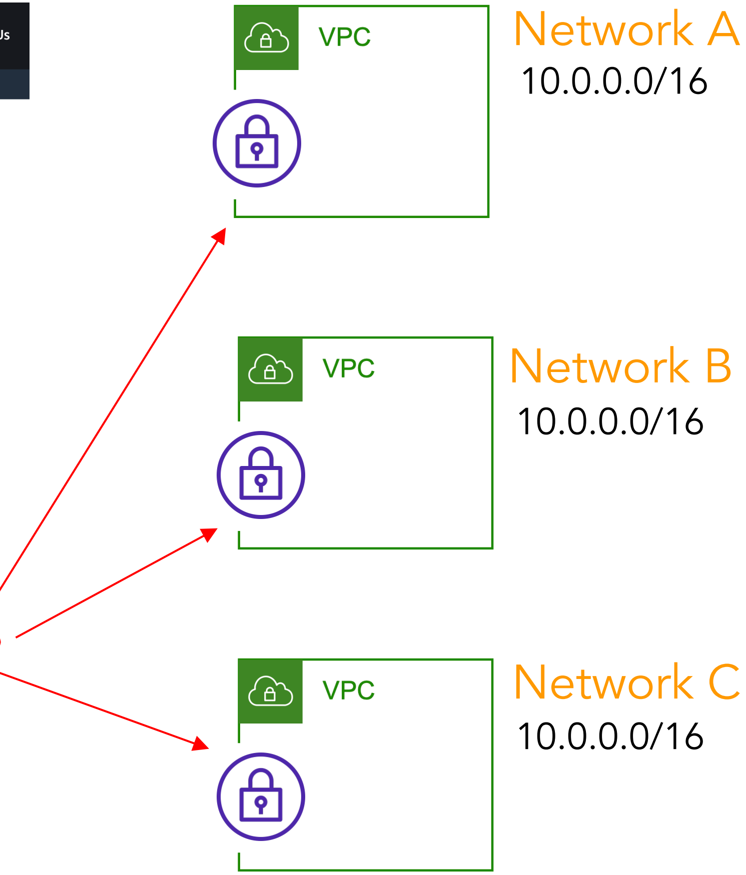
Create a VPC only

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`.

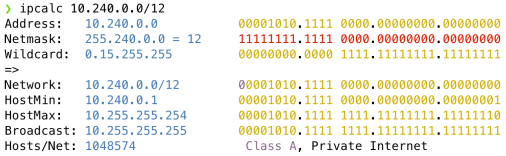
       You can specify a range of publicly routable IPv4 addresses. However, we currently do not support direct access to the internet from publicly routable CIDR blocks in a VPC. Windows instances cannot boot correctly if launched into a VPC with ranges from `224.0.0.0` to `255.255.255.255` (Class D and Class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



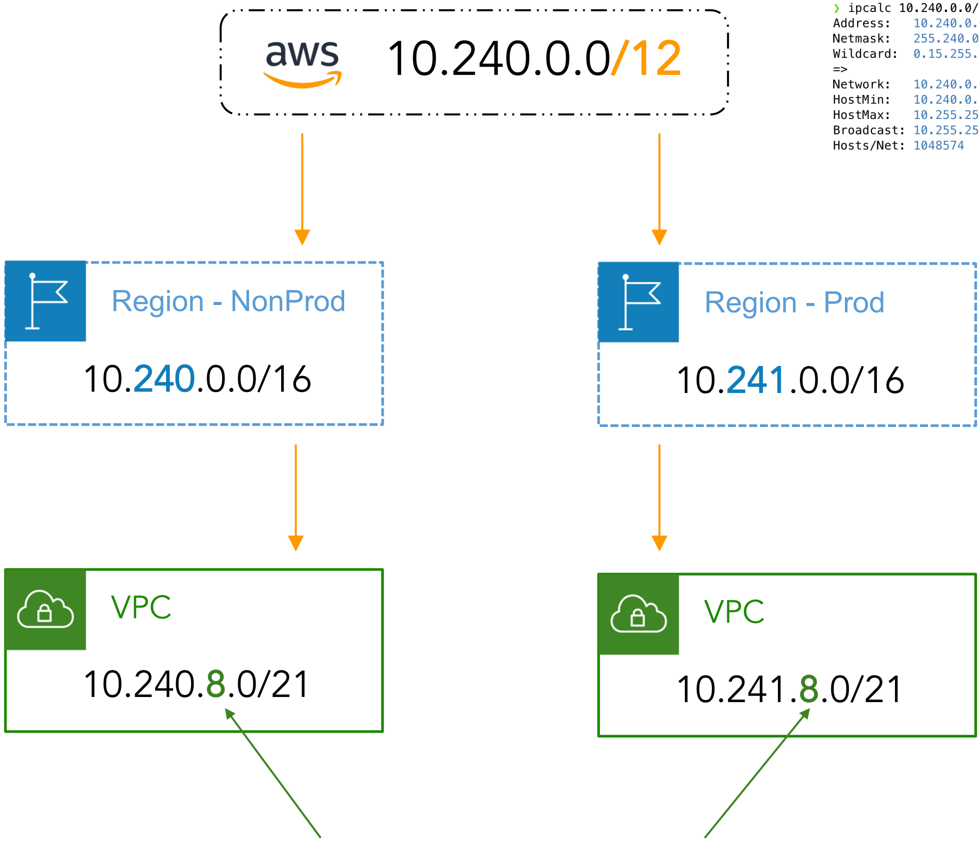
Presented By:
(US)NUA
US Networking User Association

Stepping on Land Mines

IP Addressing still matters…



```
❯ ipcalc 10.240.0.0/12
Address:   10.240.0.0           00001010.1111 0000.00000000.00000000
Netmask:   255.240.0.0 = 12     11111111.1111 0000.00000000.00000000
Wildcard:  0.15.255.255         00000000.0000 1111.11111111.11111111
=>
Network:   10.240.0.0/12        00001010.1111 0000.00000000.00000000
HostMin:   10.240.0.1           00001010.1111 0000.00000000.00000001
HostMax:   10.255.255.254       00001010.1111 1111.11111111.11111110
Broadcast: 10.255.255.255       00001010.1111 1111.11111111.11111111
Hosts/Net: 1048574               Class A, Private Internet
```



Even numbered /16 allocated to all non-production

Odd numbered /16 allocated to all production

3rd octet matches between NonProd and Prod VPCs.

(CT)NUG
Connecticut Networking User Group

Thanks!

Presented By:

(US)NUA
US Networking User Association