(VA)NUG
Virginia Networking User Group

# Why *Networking* Still Matters with Cloud


**William Collins**

*Principal Cloud Architect*


Presented By:

(US)NUA
US Networking User Association

(VA)NUG
Virginia Networking User Group

# Agenda

- Perception versus ***Reality***
- So, this is the ***Cloud***
- Diving into ***CNE Trade Craft***
- Stepping on ***Land Mines*** (Ouch)
- Shifting the ***Complexity***

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


## 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*

# 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?

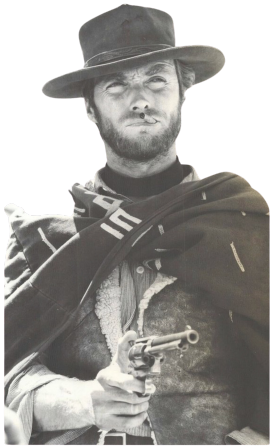
Jan 12, 2017 — Instead of '**perimeter** thinking', we need to implement policies that protect data and information regardless of the device being used or its ...

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

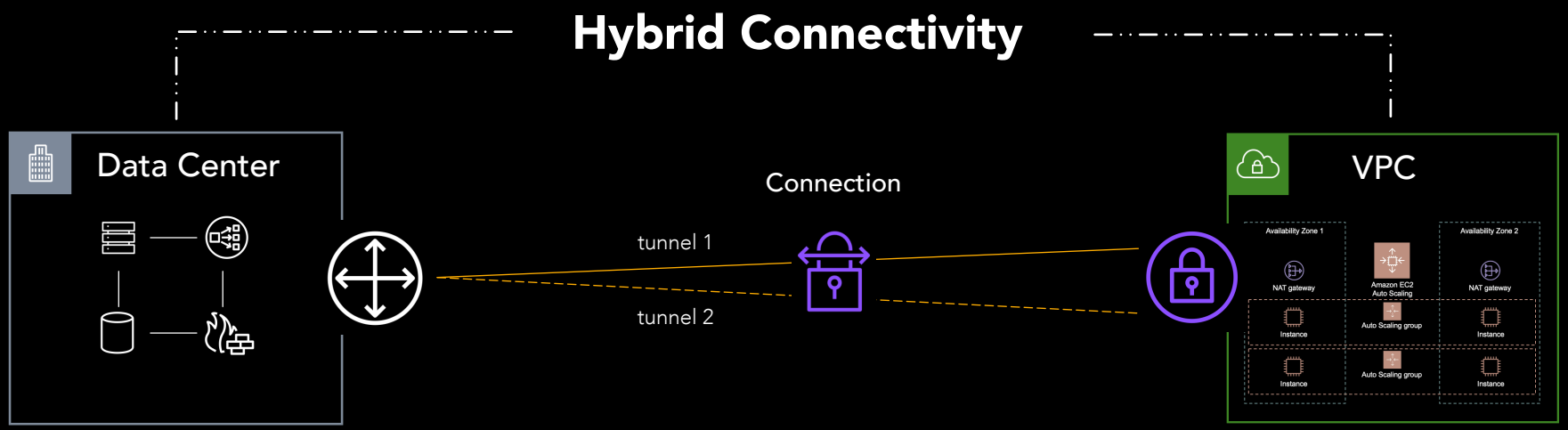
**The IP address is dead**

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 ...

# So, this is the ***Cloud***

"I find your lack of faith in proper *network design* in the cloud disturbing"

# So, this is the ***Cloud***



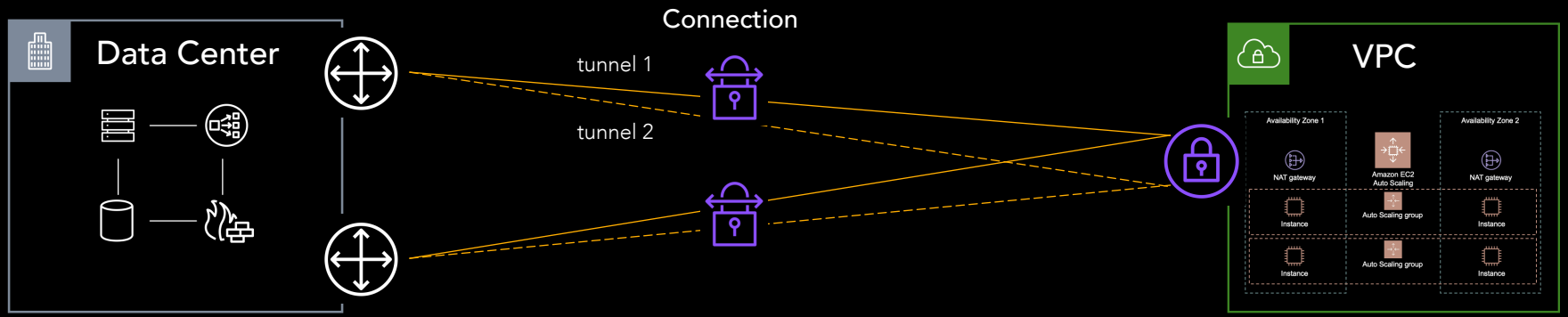

- 1x VPN connection = 2x VPN tunnels
- 1x VPN tunnel = 1.25 Gbps
- One tunnel is actively used

Active Tunnel

Standby Tunnel

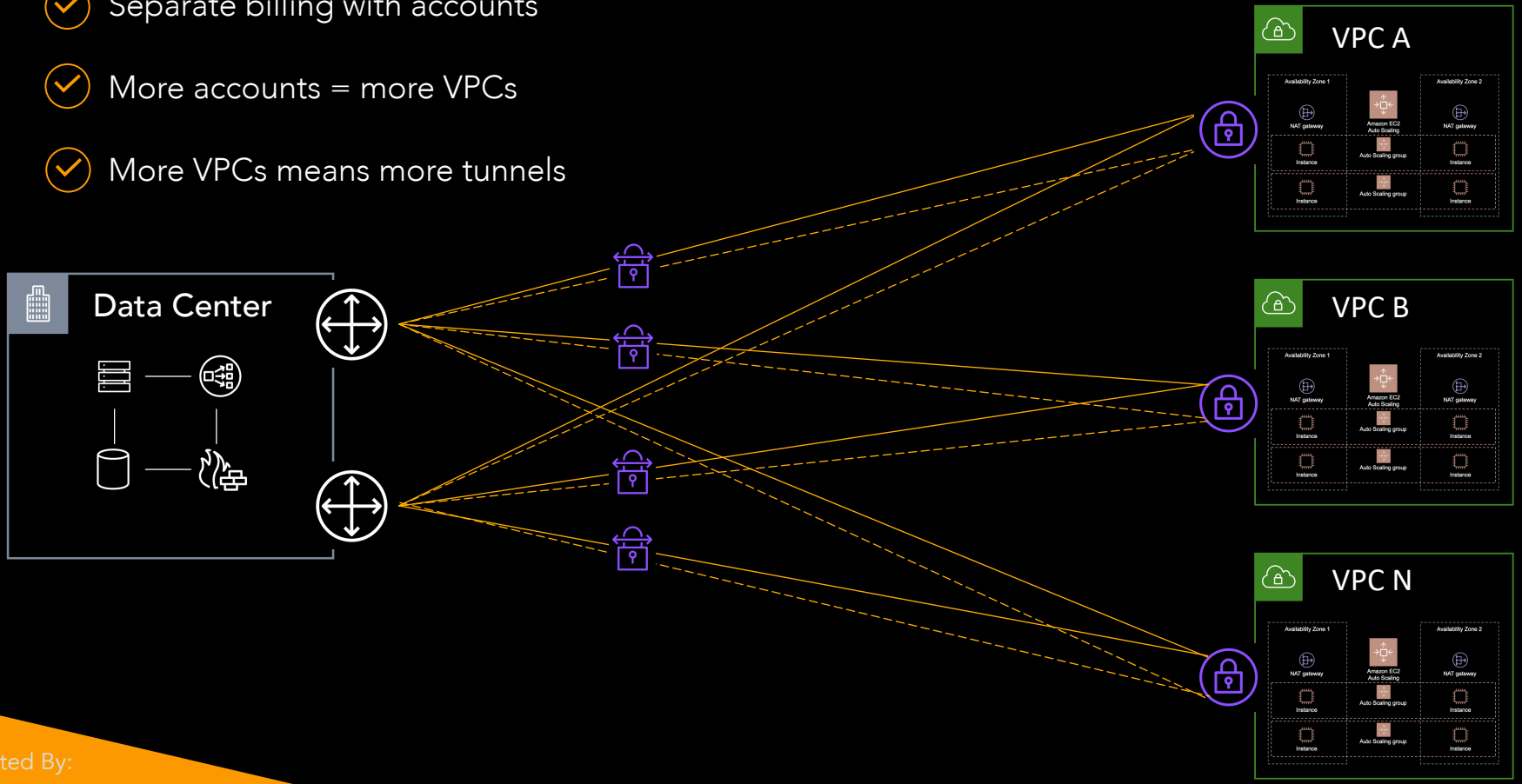
# So, this is the ***Cloud***

High Availability protects
against loss of connectivity!



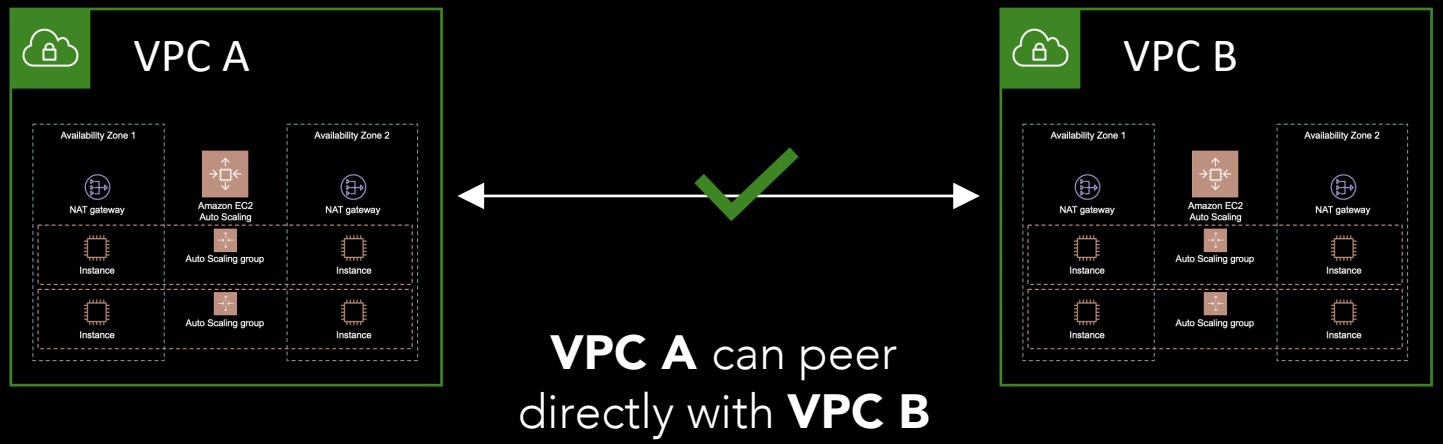
# So, this is the ***Cloud***

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



# So, this is the *Cloud*

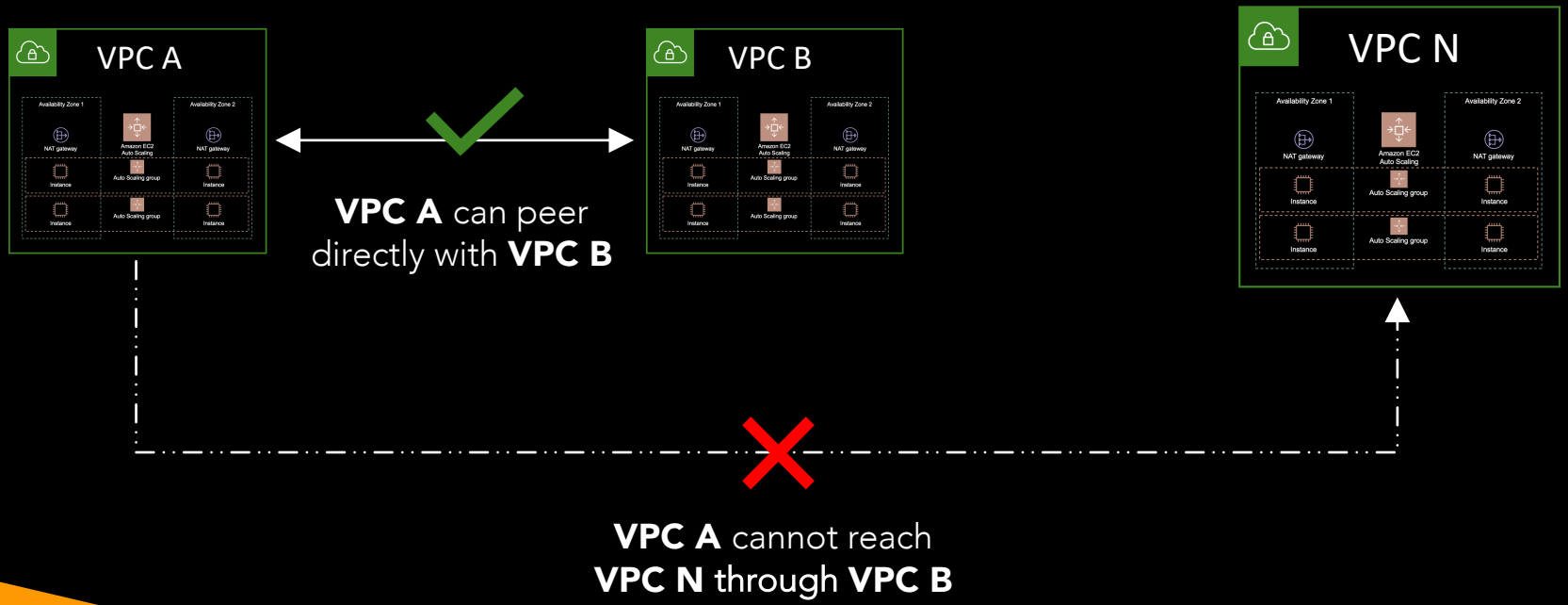
## What is Transitive Routing?




**VPC A** can peer directly with **VPC B**

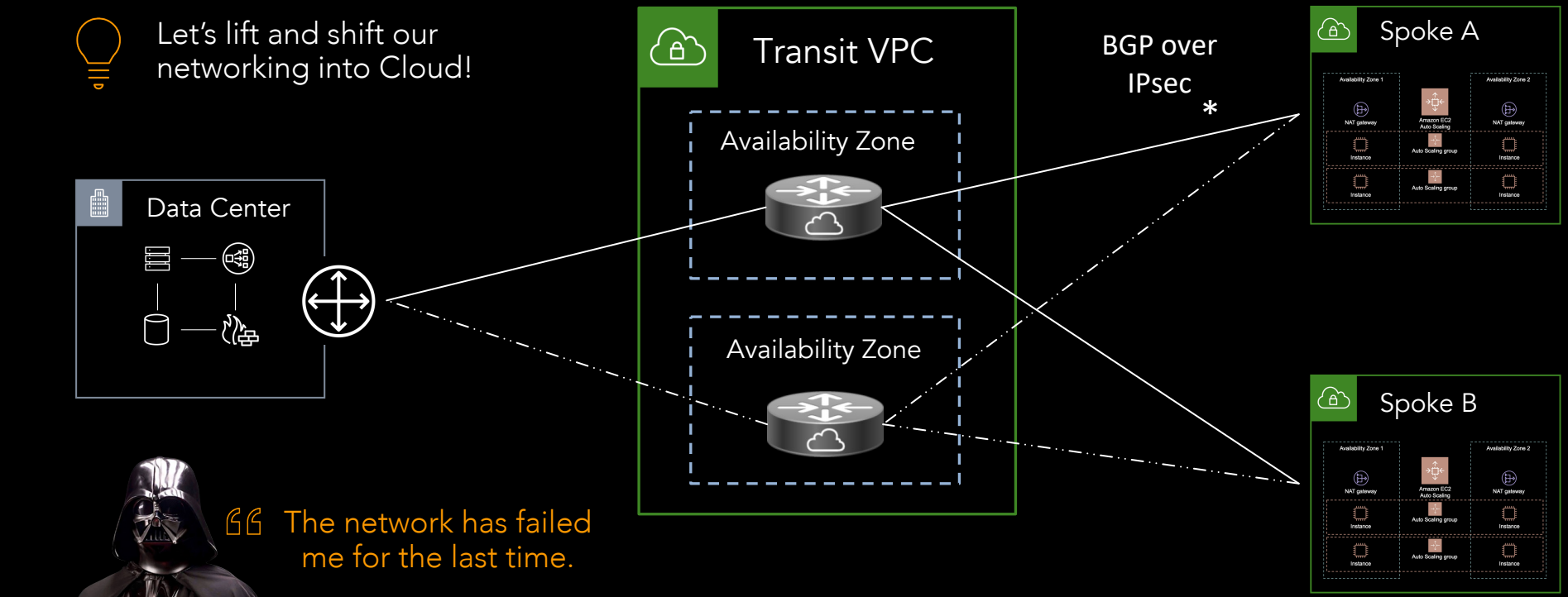
# So, this is the ***Cloud***

## What is Transitive Routing?



# So, this is the ***Cloud*** *(Dark Side)*

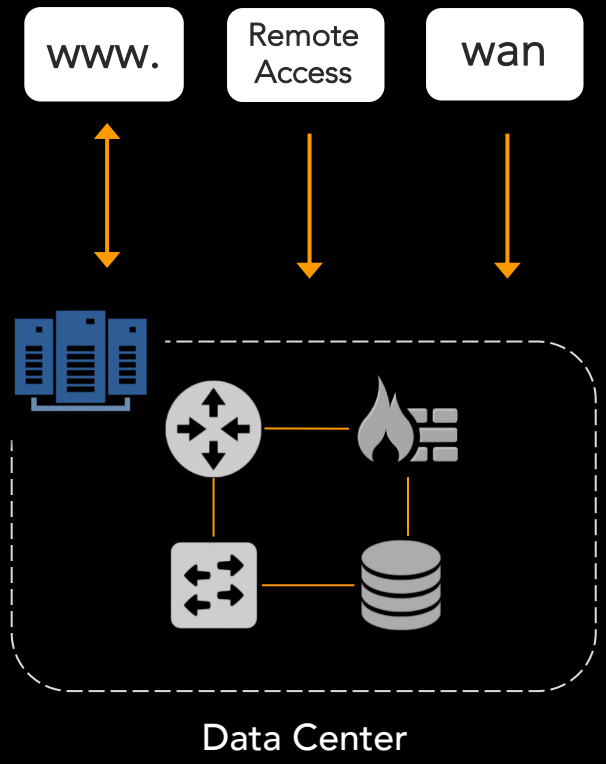
Let's lift and shift our networking into Cloud!



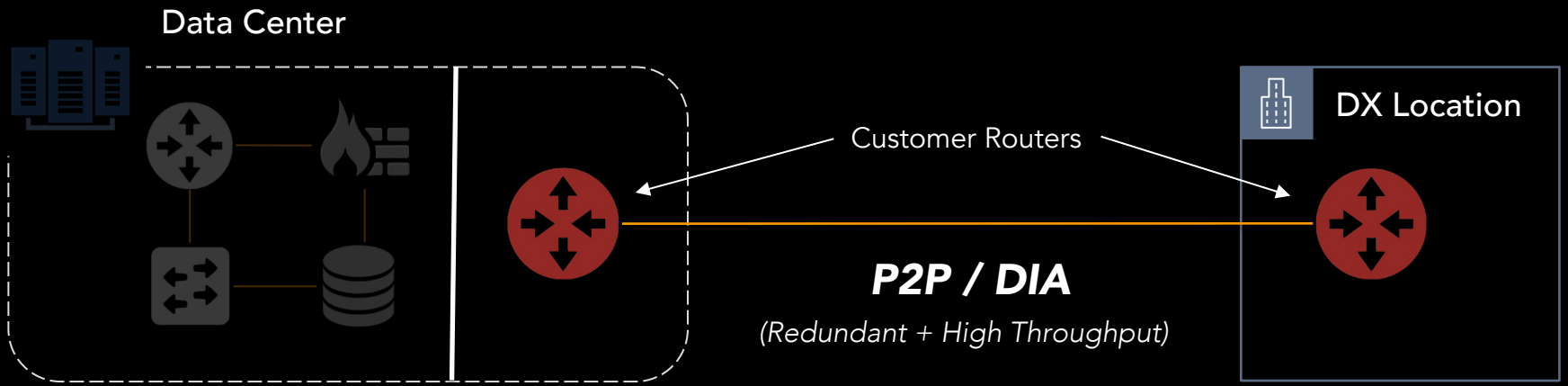

"The network has failed me for the last time.

# Diving into ***CNE Trade Craft***

Don't disrupt ***existing*** network infrastructure



# Diving into ***CNE Trade Craft***



# Thinking through Segmentation ***(Macro)***

Same problem, different lens

## Network Lens

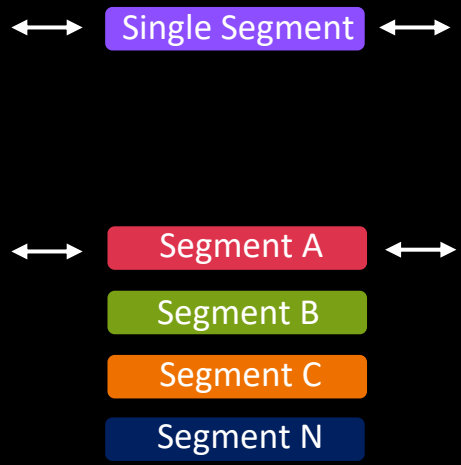
Large blast radius means high impact; Shared fate is introduced

Creates obstacles in reachability; Reliability is degraded

## Security Lens

Large attack surface means high risk; Lateral movement is easily attainable

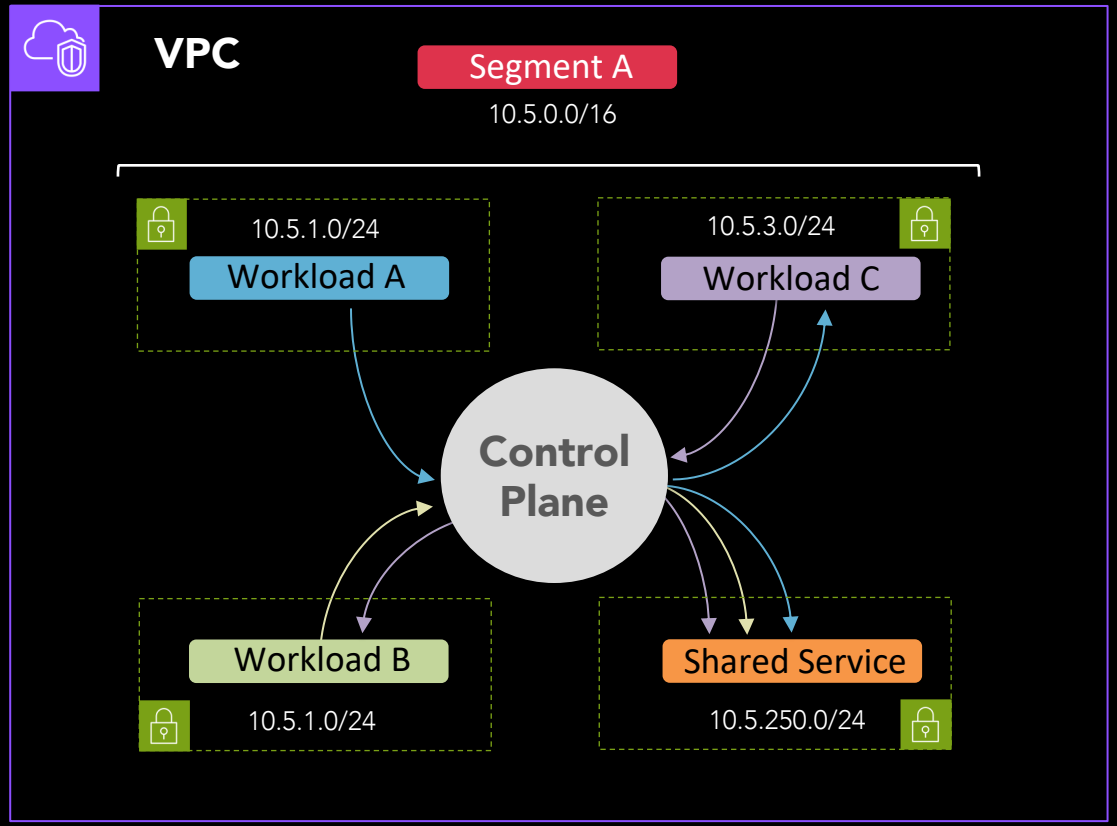
Creates additional touchpoints; User experience is degraded




* Macro Segments

- North-South Communication
- High-Level Categories
- Paves the way for ‘micro’ segments

# Thinking through Segmentation ***(Micro)***




* Micro Segments

- East-West Communication
- Granular / Workload Focused
- Dependent on Well-Architected Macro-Segmentation

# Themes and Schemes - ***Names***

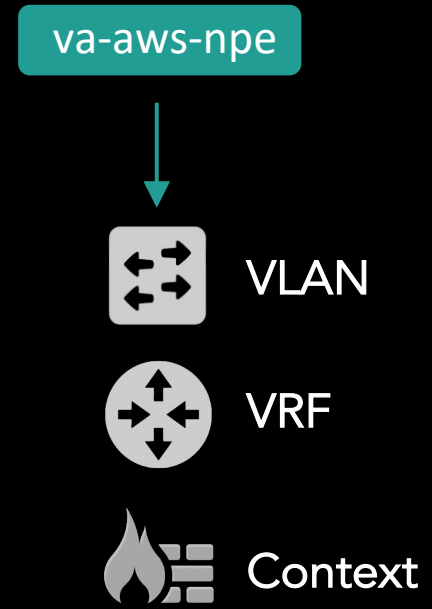
## Meaningful Names = Power

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


| dc_code | value |
|---|---|
| va | Ashburn, VA |
| il | Chicago, IL |

| cloud | value |
|---|---|
| aws | Amazon Web Services |
| azr | Microsoft Azure |

| function | value |
|---|---|
| prd | Production |
| npe | Non-Production |



# Themes and Schemes - ***Routing***

## BGP Communities


| type | meaning |
|---|---|
| 1 | link function |
| 2 | dc origin |
| 3 | cloud provider |

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

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

# Themes and Schemes - ***Routing***


| type | meaning |
|---|---|
| 1 | link function |
| 2 | dc origin |
| 3 | cloud provider |

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

aws

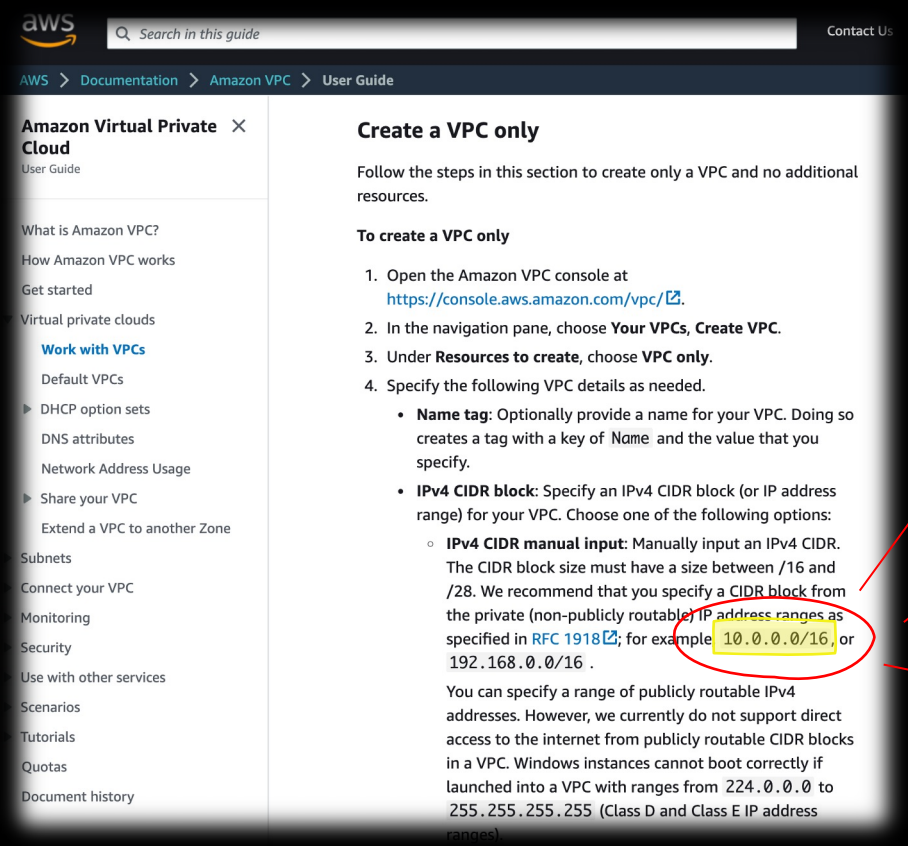
```
route-map aws-in permit 10
    match ip address prefix-list aws
    set community 1:1 2:1 3:1
```

- 3:1 — AWS route
- 2:1 — Originated from DC-01
- 1:1 — Learned via primary

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

- 3:2 — Azure route
- 2:2 — Originated from DC-02
- 1:2 — Learned via secondary

# Stepping on Land Mines - *Ouch*



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

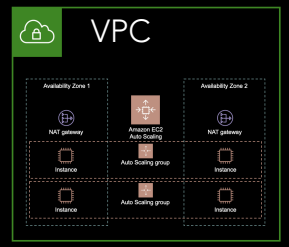
## Create a VPC only

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

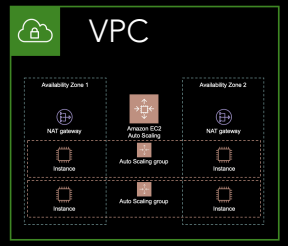
**To create a VPC only**

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`.

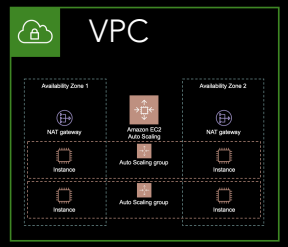
       You can specify a range of publicly routable IPv4 addresses. However, we currently do not support direct access to the internet from publicly routable CIDR blocks in a VPC. Windows instances cannot boot correctly if launched into a VPC with ranges from `224.0.0.0` to `255.255.255.255` (Class D and Class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




**Network A**
10.0.0.0/16




**Network B**
10.0.0.0/16



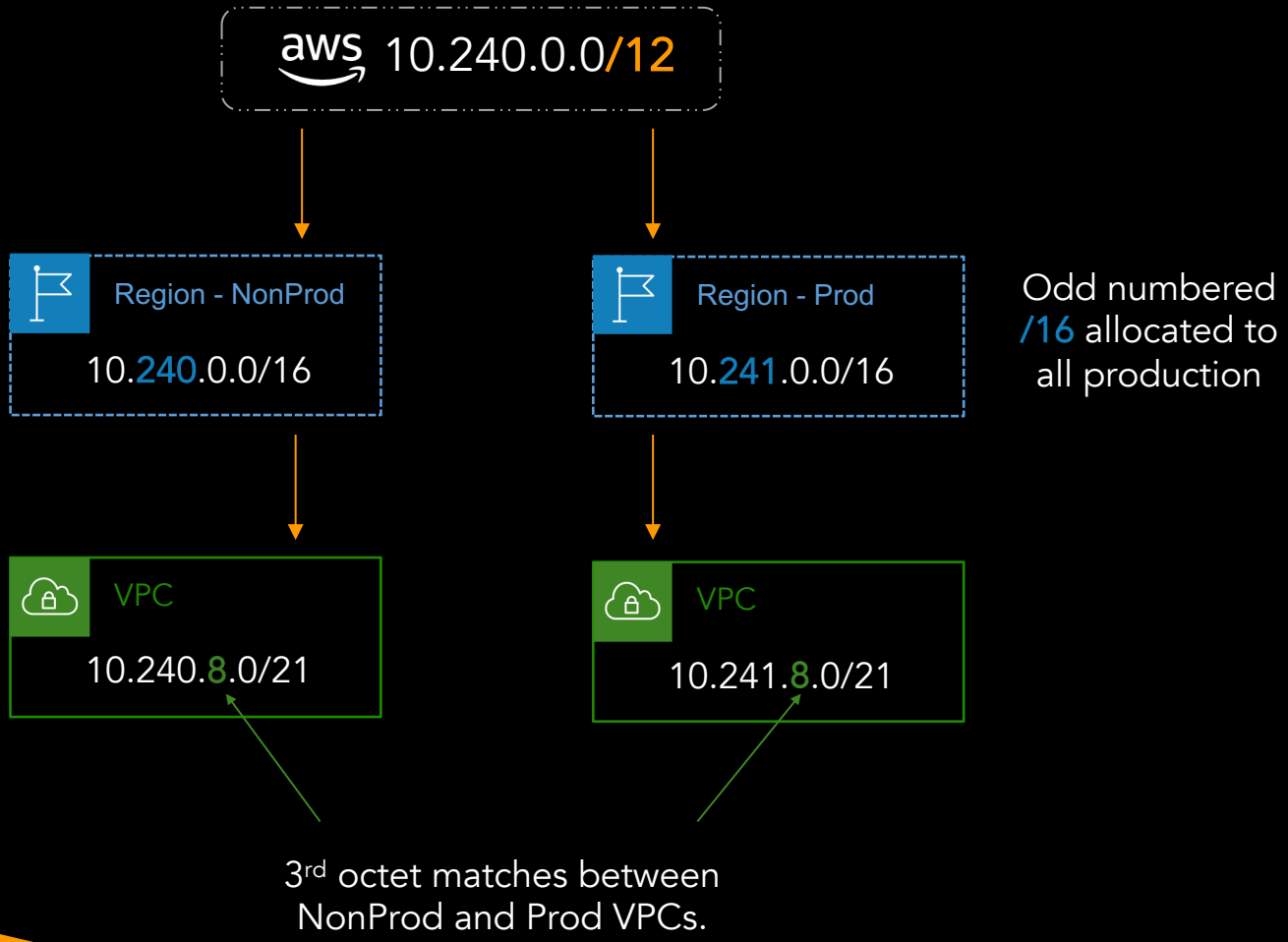

**Network C**
10.0.0.0/16

Presented By:

(US)NUA
US Networking User Association

# Stepping on Land Mines - *Ouch*

IP Addressing still matters…




Even numbered /16 allocated to all non-production

Odd numbered /16 allocated to all production

3rd octet matches between NonProd and Prod VPCs.

# Looking into the Future with *(NaaS)*

## NaaS

Operate networking without the necessity of deploying and maintaining network infrastructure

# Shifting the ***Complexity***

**API Backends**

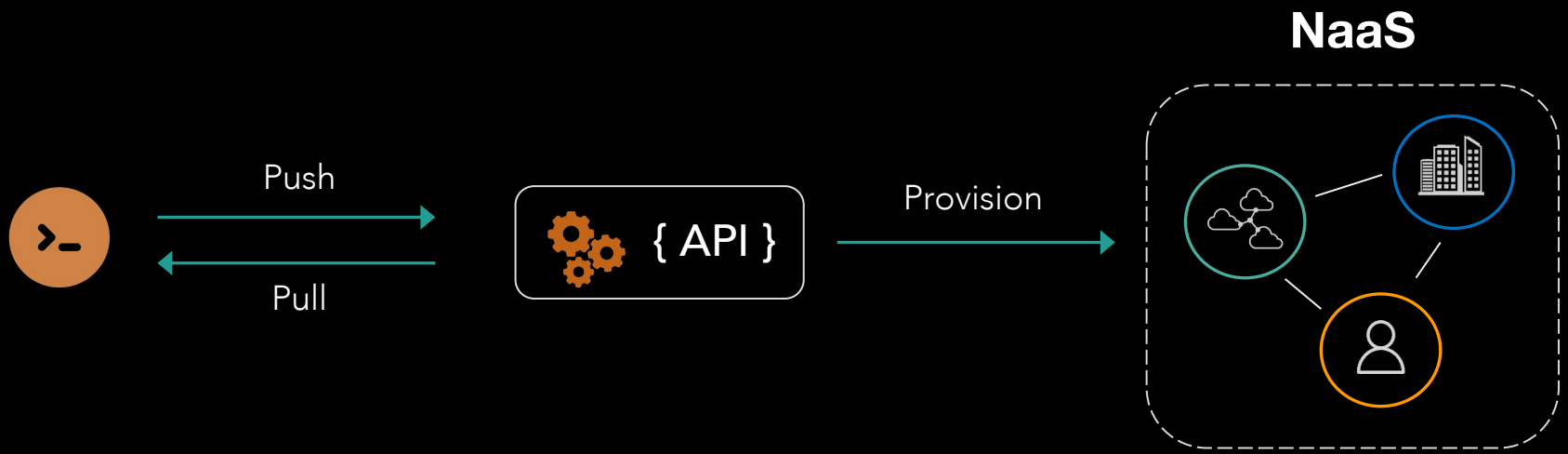
Power user interfaces and automated abstractions

**Reduce Touchpoints**

Minimize operational friction by reducing touchpoints and interaction surfaces

***'as-code'*** **Delivery**

Robust Infra-as-Code tooling and RESTful APIs



# Thank You! *Want to Connect?*

william-collins

wcollins502

wcollins

wcollins.io

**Podcast** → The Cloud Gambit

Presented By:

(US)NUA

US Networking User Association