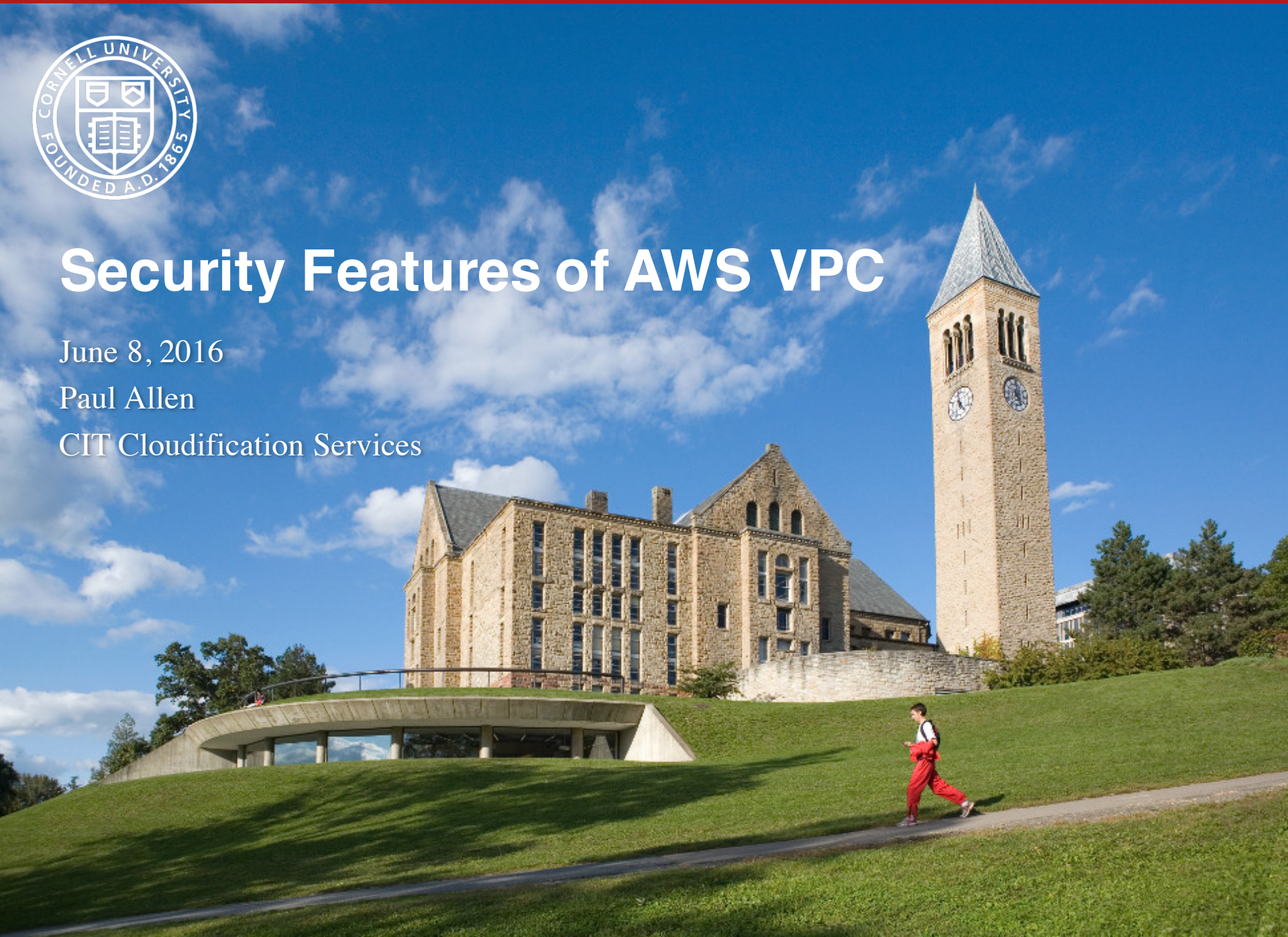


Security Features of AWS VPC

June 8, 2016

Paul Allen
CIT Cloudification Services

Cloudification Services Team

Mission:

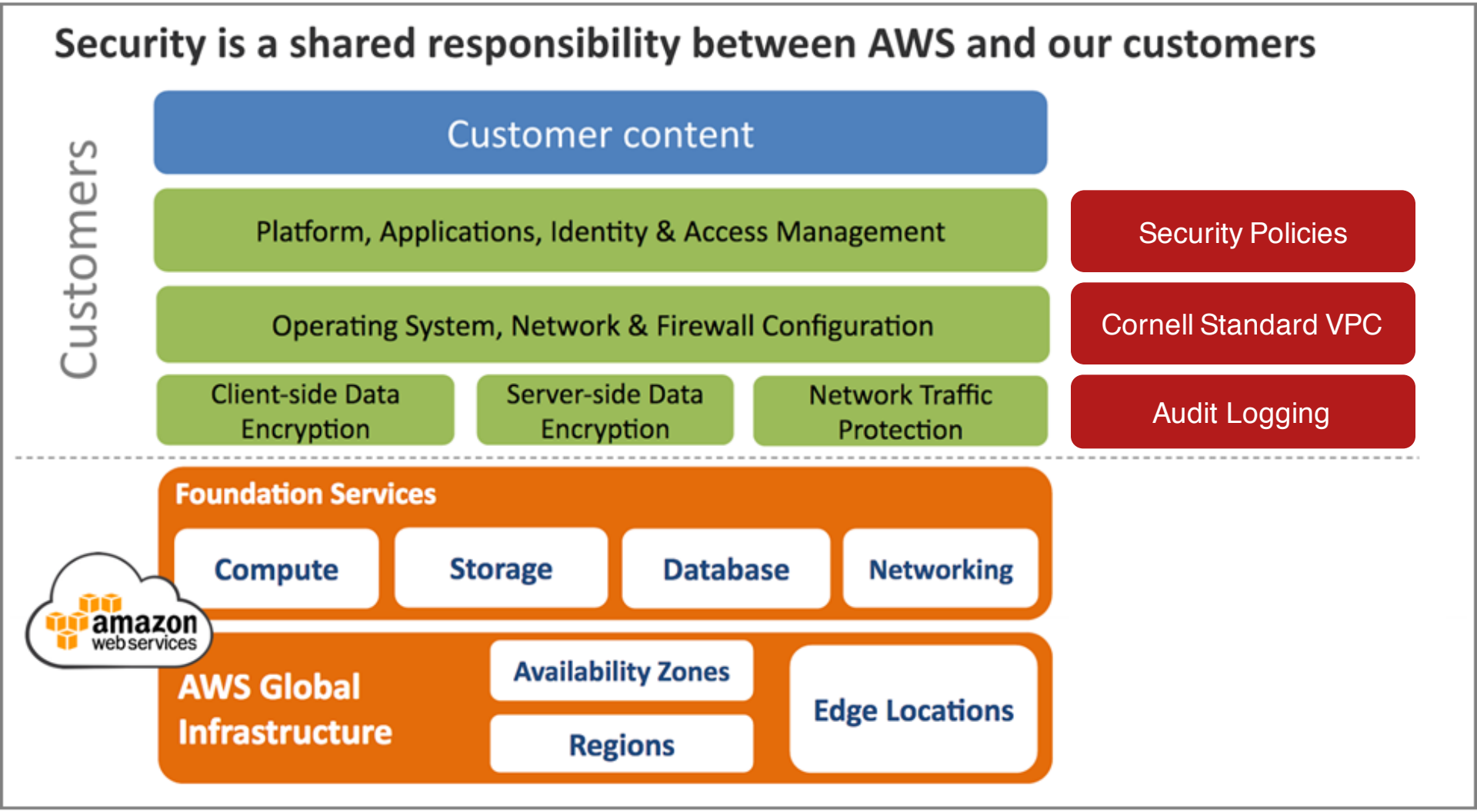
safe

Facilitate Campus' transition to the cloud while encouraging modern DevOps practices

Team

- Shawn Bower
- Ned La Celle
- Marty Sullivan
- Paul Allen
- Nicole Rawleigh
- Sarah Christen (mgr)

Shared Responsibility Model



Virtual Private Cloud

- logically isolated network in AWS cloud
- on-premise connectivity options
  - none
  - VPN
  - DirectConnect

VPC Components

required:

- subnets
- route tables
- network ACL
- security groups

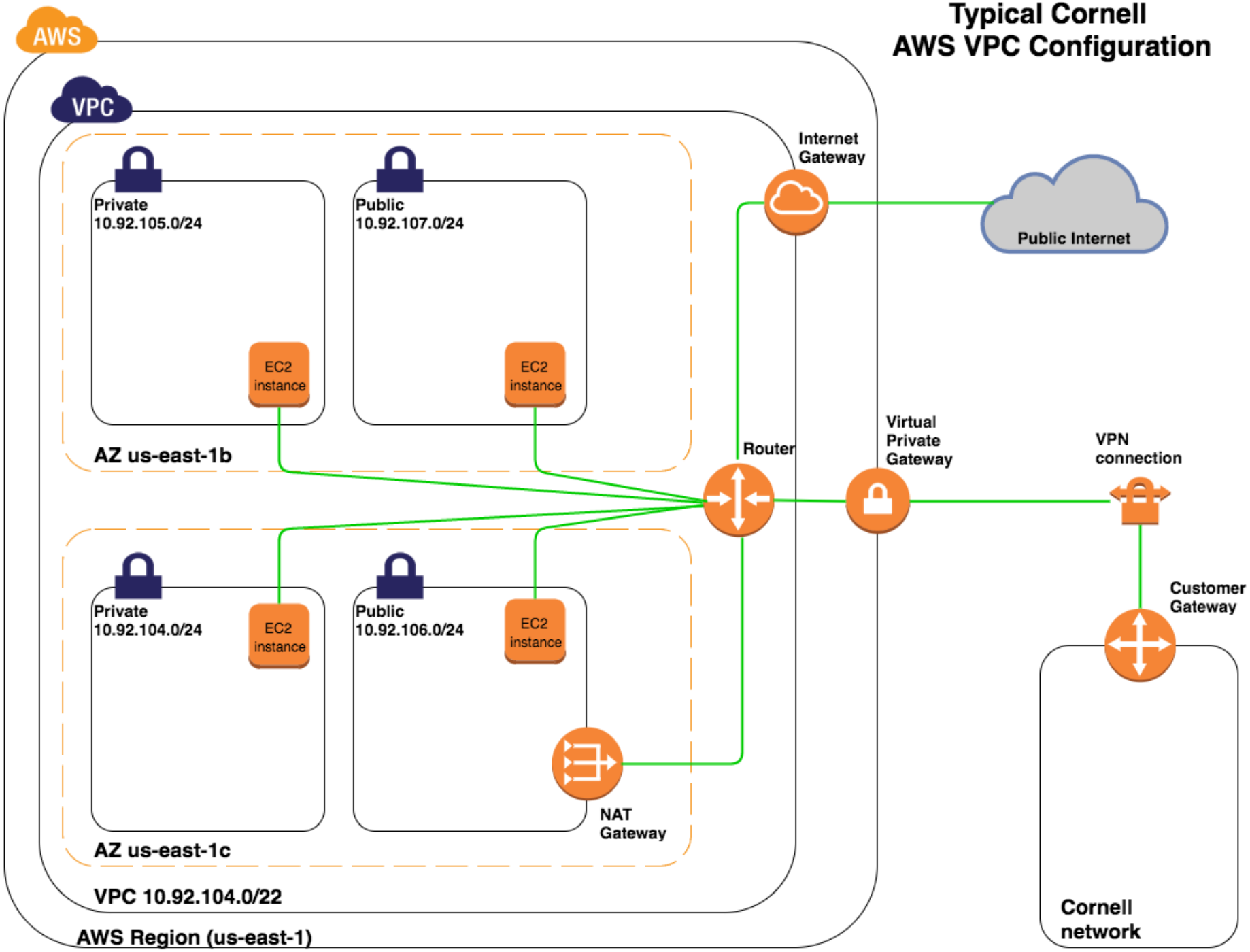
optional:

- internet gateway
- NAT gateway
- hardware VPN
- virtual private gateway
- customer gateway
- peering connection
- flow logs

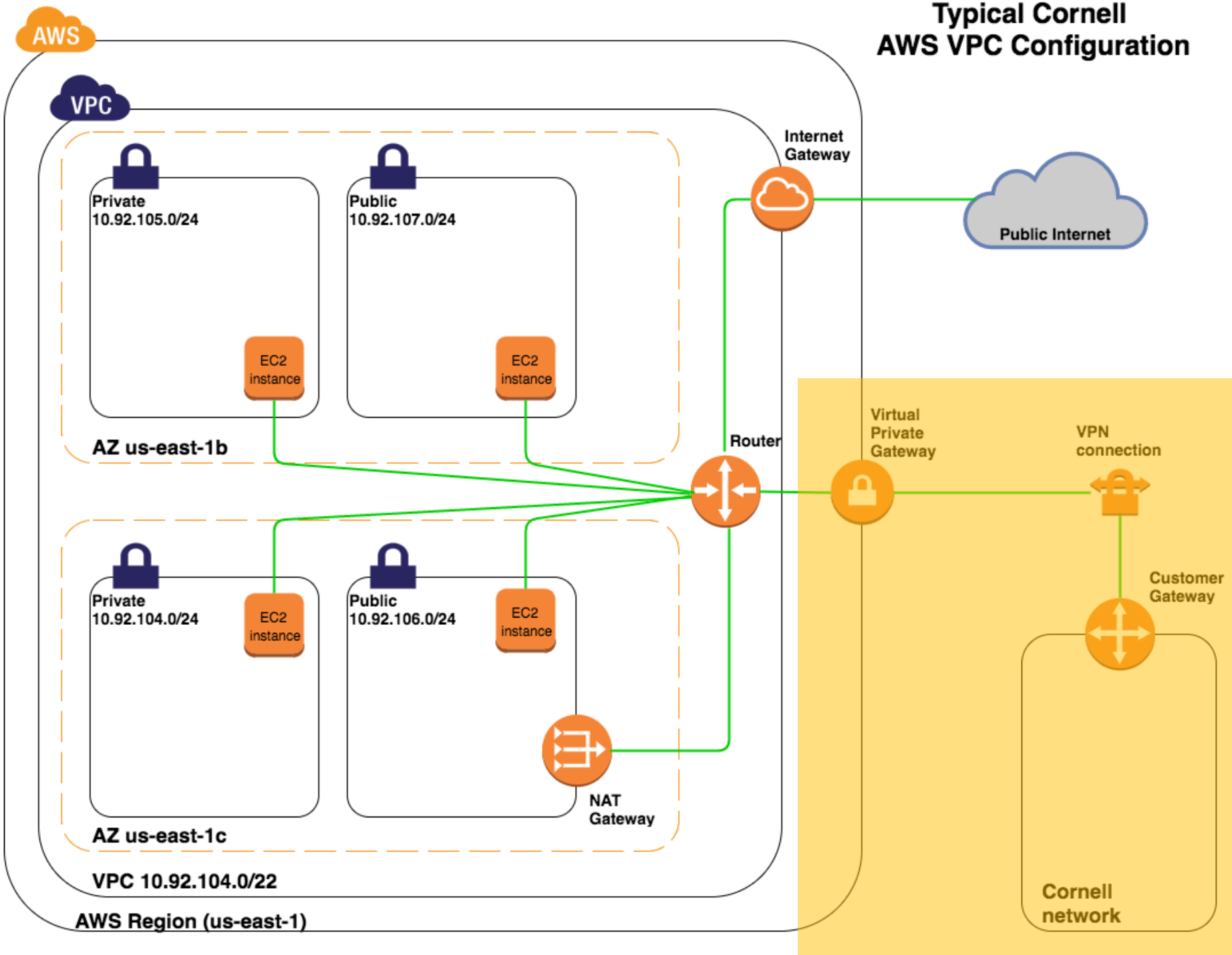
Benefits of VPC

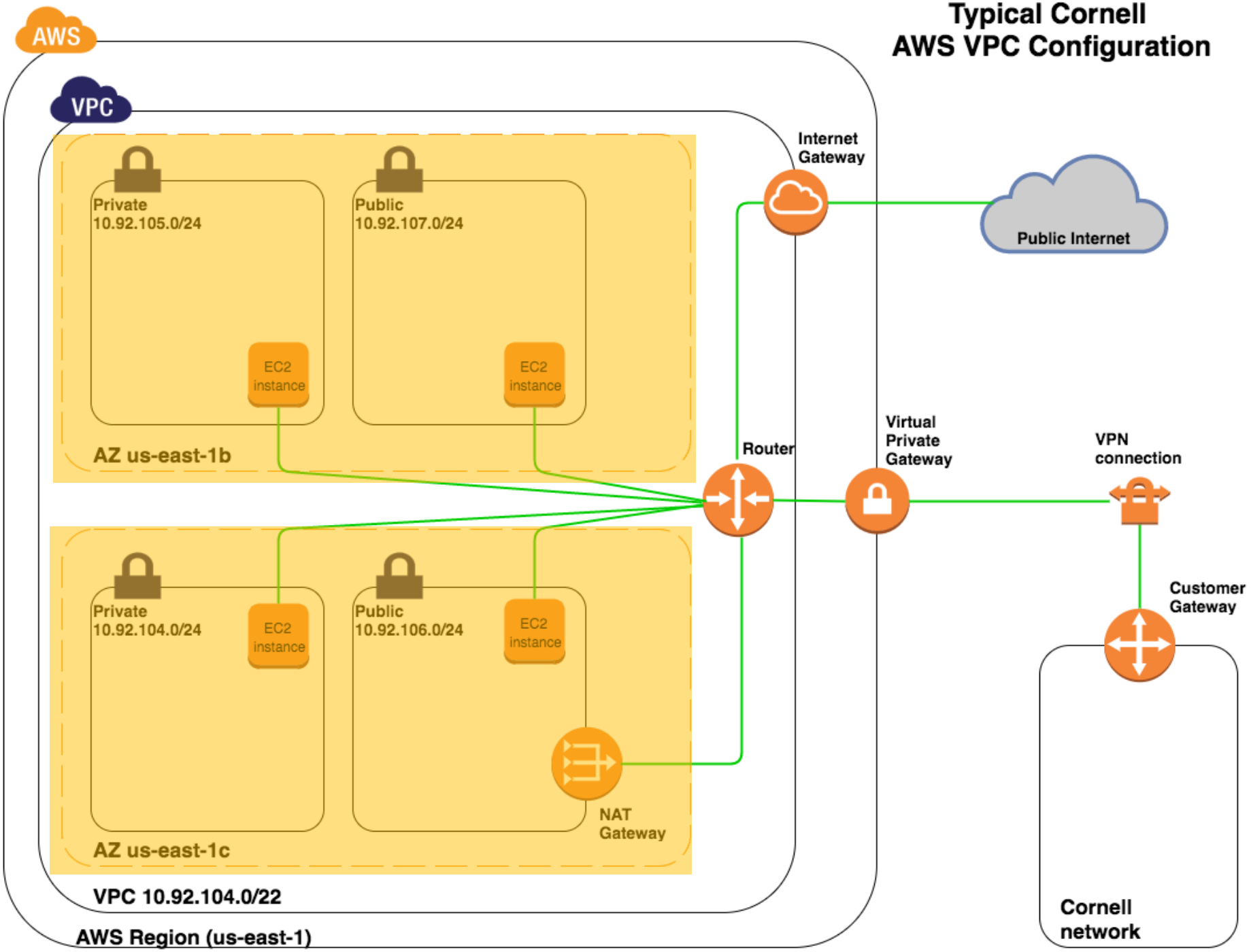
- connectivity options
- custom subnets, routing
- layered security
  - security groups
  - network ACL
- continuity with on-premise networks
- single-tenancy, if desired

Typical Cornell AWS VPC Configuration

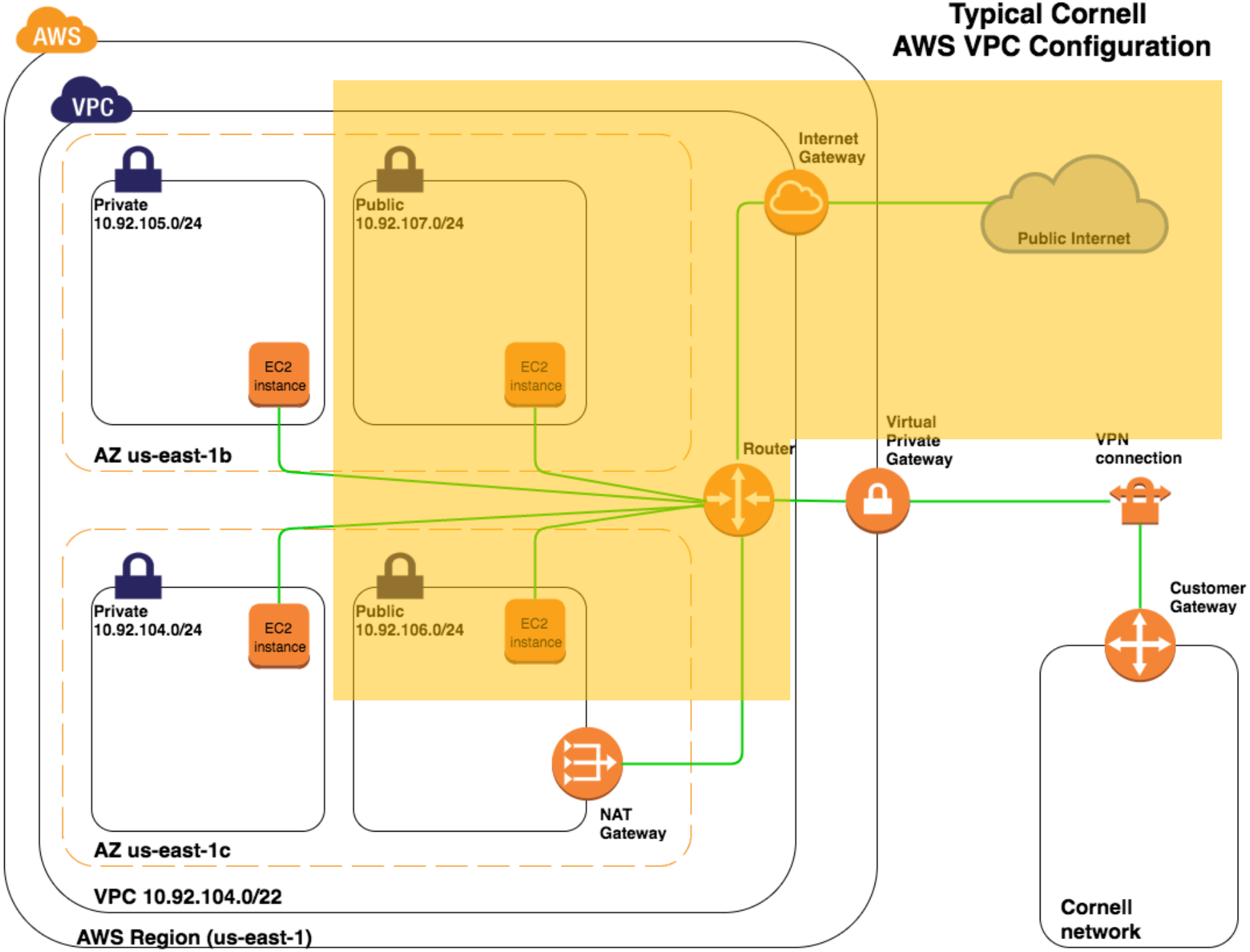


Typical Cornell AWS VPC Configuration

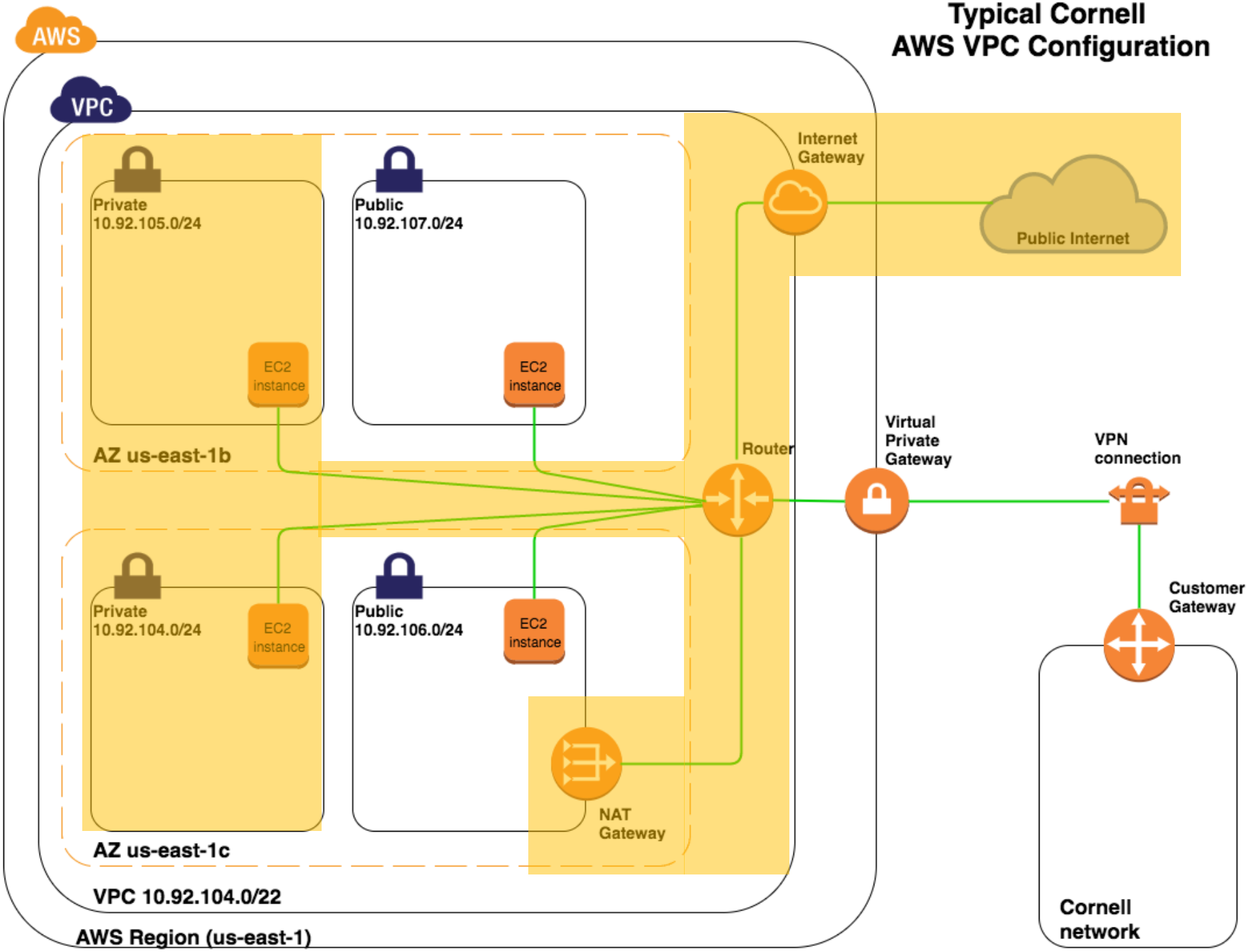


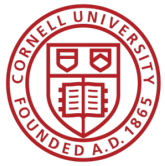

Typical Cornell
AWS VPC Configuration
AWS
VPC
Private
10.92.105.0/24
Public
10.92.107.0/24
EC2
instance
EC2
instance
AZ us-east-1b
Internet
Gateway
Public Internet
Router
Virtual
Private
Gateway
VPN
connection
Customer
Gateway
Private
10.92.104.0/24
EC2
instance
Public
10.92.106.0/24
EC2
instance
NAT
Gateway
AZ us-east-1c
VPC 10.92.104.0/22
AWS Region (us-east-1)
Cornell
network

Typical Cornell AWS VPC Configuration

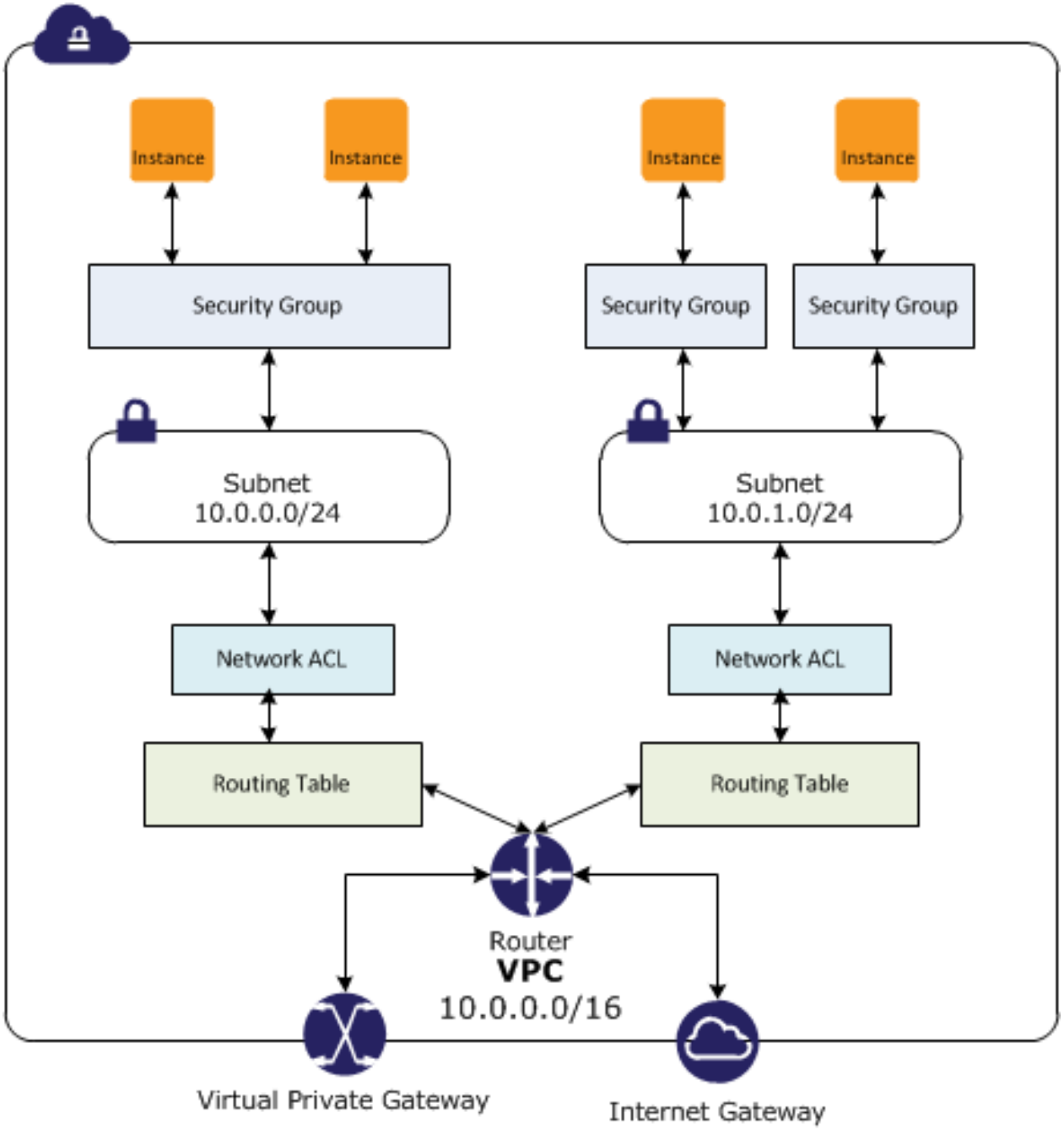


Typical Cornell AWS VPC Configuration





Security Groups and Network ACLs



Baseline Cornell Network ACL

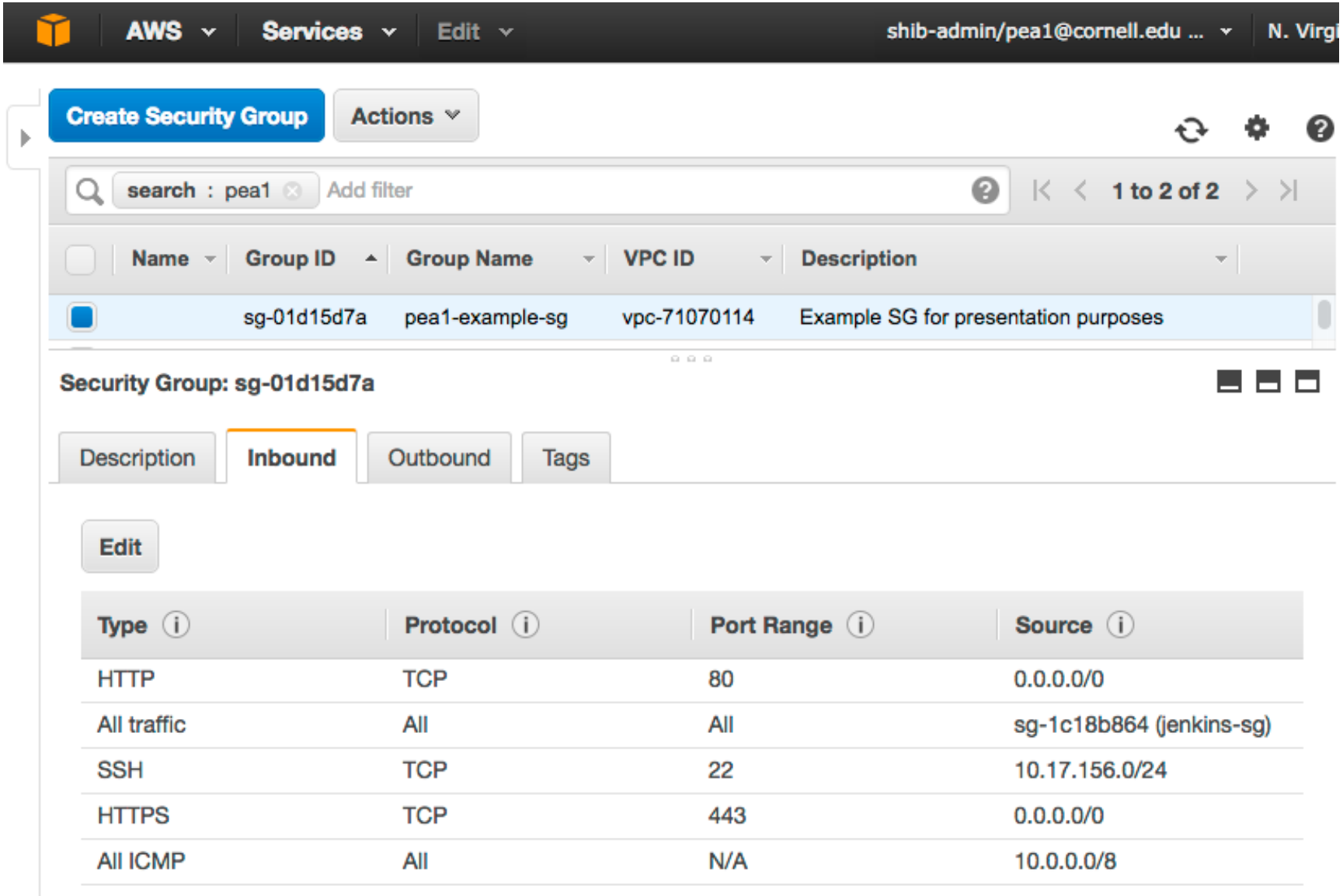
Summary | **Inbound Rules** | Outbound Rules | Subnet Associations | Tags

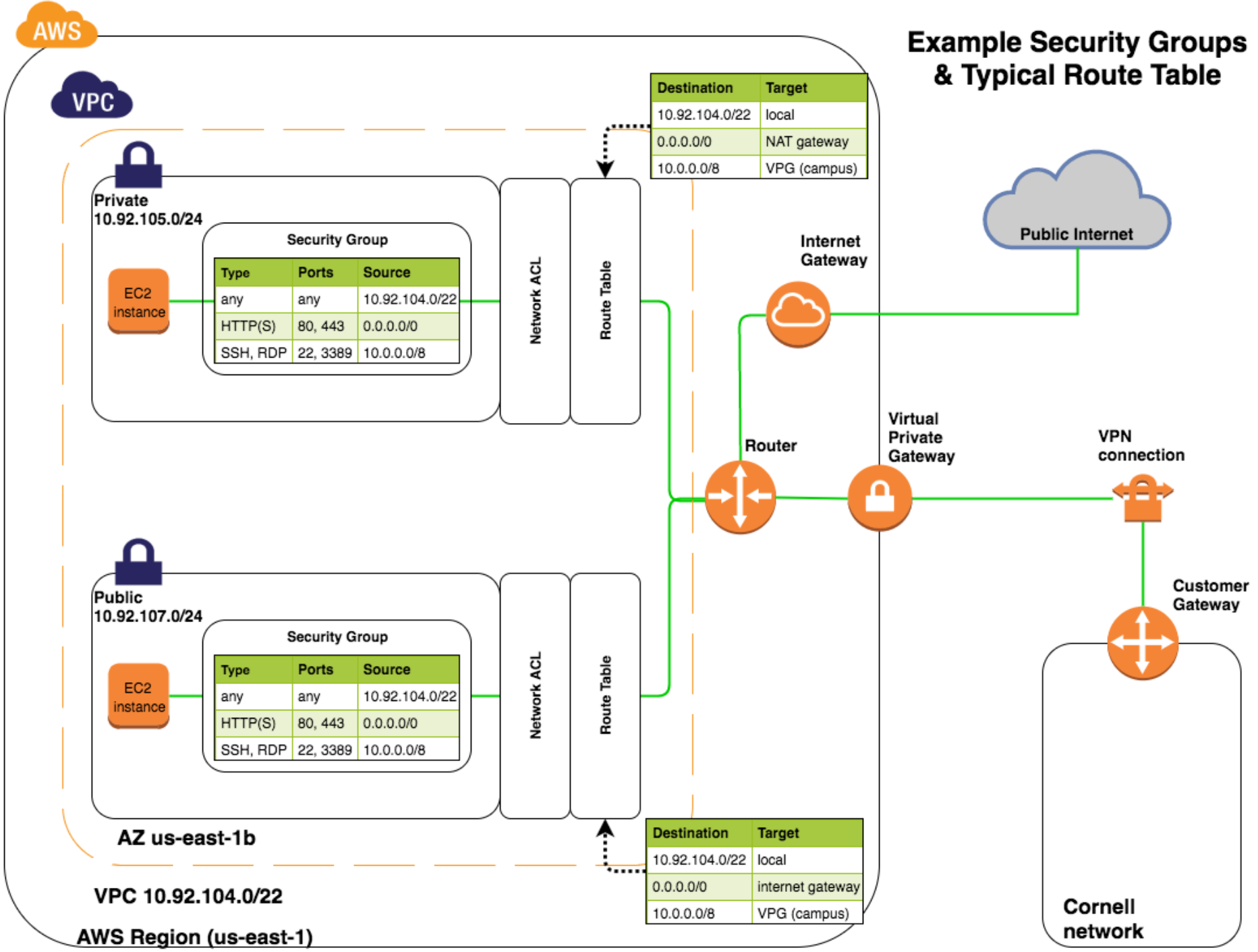
Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Edit

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW
200	HTTPS (443)	TCP (6)	443	0.0.0.0/0	ALLOW
300	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
400	Custom TCP Rule	TCP (6)	1024-65535	0.0.0.0/0	ALLOW
500	ALL Traffic	ALL	ALL	10.0.0.0/8	ALLOW
600	ALL Traffic	ALL	ALL	128.84.0.0/16	ALLOW
700	ALL Traffic	ALL	ALL	128.253.0.0/16	ALLOW
800	ALL Traffic	ALL	ALL	132.236.0.0/16	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Example Security Group




AWS
VPC
Example Security Groups
& Typical Route Table
Destination
Target
10.92.104.0/22
local
0.0.0.0/0
NAT gateway
10.0.0.0/8
VPG (campus)
Private
10.92.105.0/24
Security Group
Type
Ports
Source
EC2 instance
any
any
10.92.104.0/22
HTTP(S)
80, 443
0.0.0.0/0
SSH, RDP
22, 3389
10.0.0.0/8
Network ACL
Route Table
Public Internet
Internet Gateway
Router
Virtual Private Gateway
VPN connection
Customer Gateway
Public
10.92.107.0/24
Security Group
Type
Ports
Source
EC2 instance
any
any
10.92.104.0/22
HTTP(S)
80, 443
0.0.0.0/0
SSH, RDP
22, 3389
10.0.0.0/8
Network ACL
Route Table
AZ us-east-1b
Destination
Target
10.92.104.0/22
local
0.0.0.0/0
internet gateway
10.0.0.0/8
VPG (campus)
VPC 10.92.104.0/22
AWS Region (us-east-1)
Cornell network

Perimeter Assessment

CloudCheckr

This report shows you an analysis of all the entry points from the public Internet into your AWS account. Reviewing the public entry points allows you to determine if you've unintentionally left any openings in your AWS environment that expose you to the public Internet.

☑ Filter out all Regions with no publicly accessible resources

Export by Region | Export by Resources

Show: 10 25 50

	Region name
⊖	US East (Northern Virginia) **

Expand All Details

	No Publicly Accessible S3 Buckets
⊖	Publicly Accessible VPCs

⊕	vpc-e99f428e (ucp-VPC) *
⊖	vpc-71070114 (cu-cs-vpc)

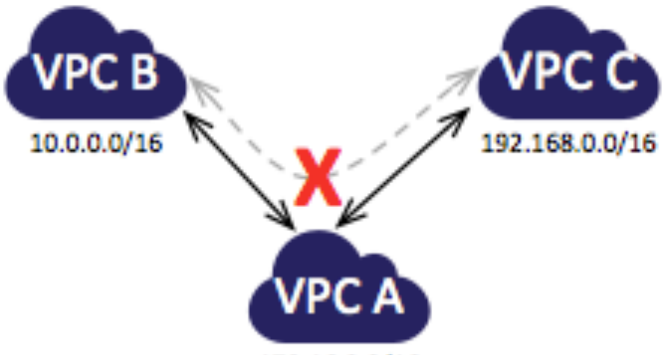
Network ACL Rules allowing inbound traffic from the following ports from all IPs

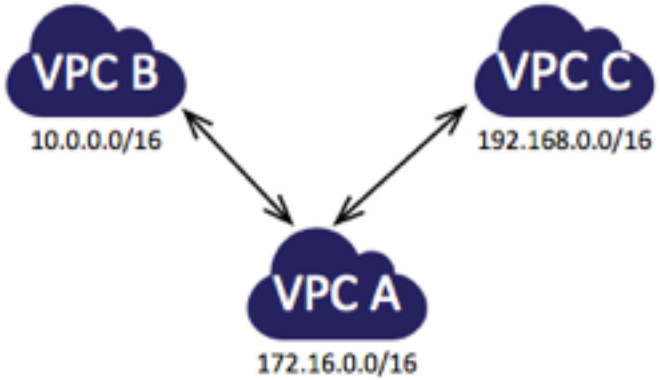
Rule Number	From	To
100	ALL	ALL

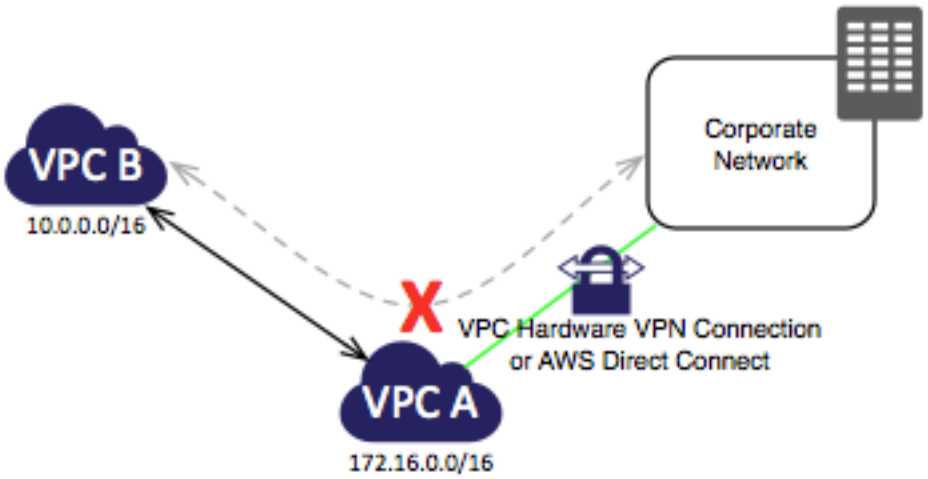
! This Network ACL allows inbound traffic from all IP Addresses and ports. You should be very careful about ensuring you are using security groups properly.

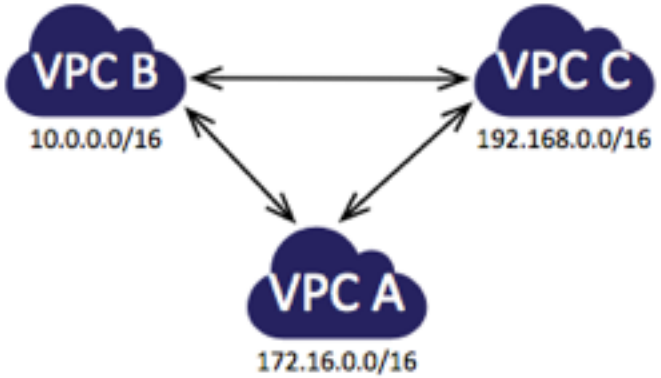
VPC Peering


VPC A
172.16.0.0/16
VPC B
10.0.0.0/16


VPC B
10.0.0.0/16
VPC C
192.168.0.0/16
X
VPC A


VPC B
10.0.0.0/16
VPC C
192.168.0.0/16
VPC A
172.16.0.0/16


Corporate
Network
VPC B
10.0.0.0/16
X
VPC Hardware VPN Connection
or AWS Direct Connect
VPC A
172.16.0.0/16


VPC B
10.0.0.0/16
VPC C
192.168.0.0/16
VPC A
172.16.0.0/16

VPC-related Pricing

	base charges	data charges
VPC	free	n/a
VPN connections	$0.05/connection-hour	n/a
NAT gateway	$0.045/hr	$0.045/GB (ingress) $0.045/GB (egress)
Direct Connect – 1G	$0.30/hr	$0.00/GB (ingress) $0.03/GB (egress**)
Direct Connect – 100M	$0.06/hr	$0.00/GB (ingress) $0.03/GB (egress**)
Standard Data Transfer	n/a	$0.00/GB (ingress) $0.09/GB (egress to internet**)

** Research Data Egress waiver (15% of total bill)

Questions?

- https://blogs.cornell.edu/cloudification/tech-blog/
- https://confluence.cornell.edu/display/CLOUD/
- cloudification-l@cornell.edu
- pea1@cornell.edu