AWS VPC

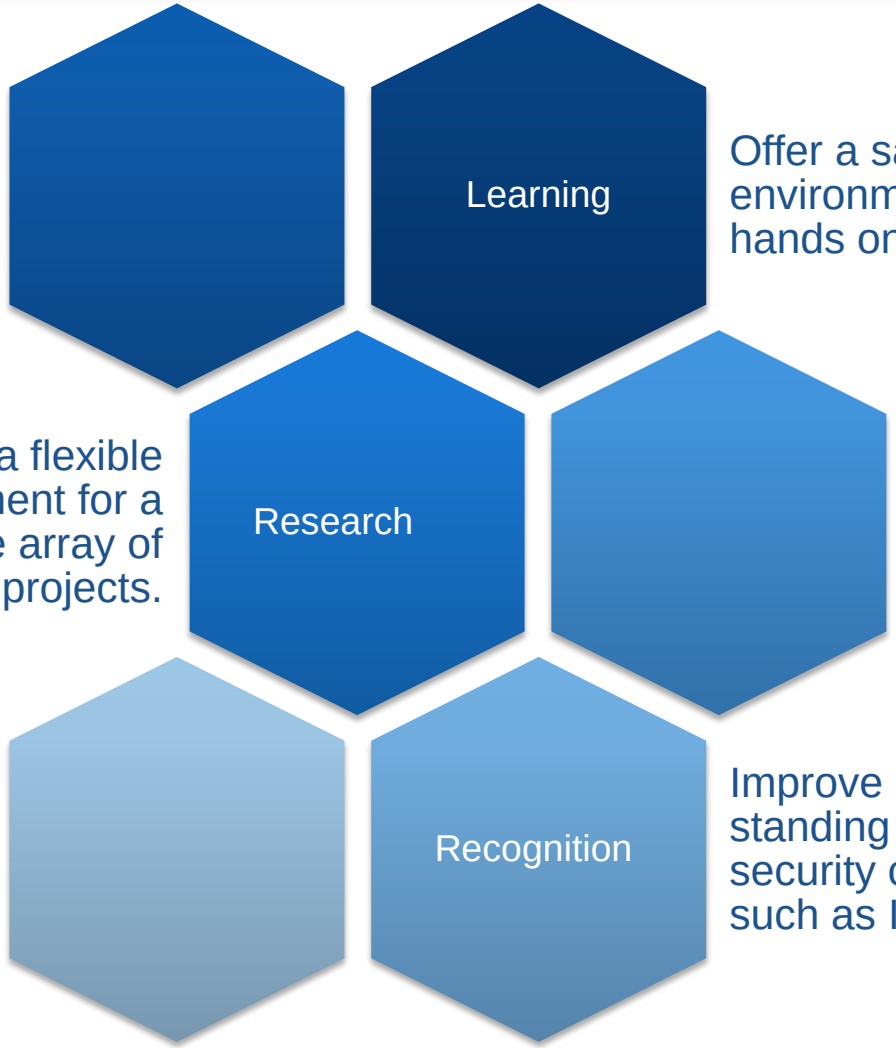
By Daniel Ruiz

Index

Introduction

- Amazon Web Services (AWS)
  - EC2, VPC, MapReduce, SimpleDB, CloudFront, Simple Storage Service(S3), CloudFormation….and more
- Amazon VPC
  - Cloud Isolation
  - Extension of existing infrastructure
    - Added Security
    - IP Assigning

UCCS VPC Objective



Offer a safe environment to gain hands on experience

Provide a flexible environment for a wide array of research projects.

Improve UCCS standing in cyber security competitions such as ICTF

Why VPC

Affordable

- Use a minimal amount of UCCS computer resources
- Require no additional equipment
- Practical operating cost

Flexible

- Ability to handle various user population sizes
- Ability to handle various project requirements

Safe

- Isolated from public environment
- Restricted to UCCS internal environment

Simple

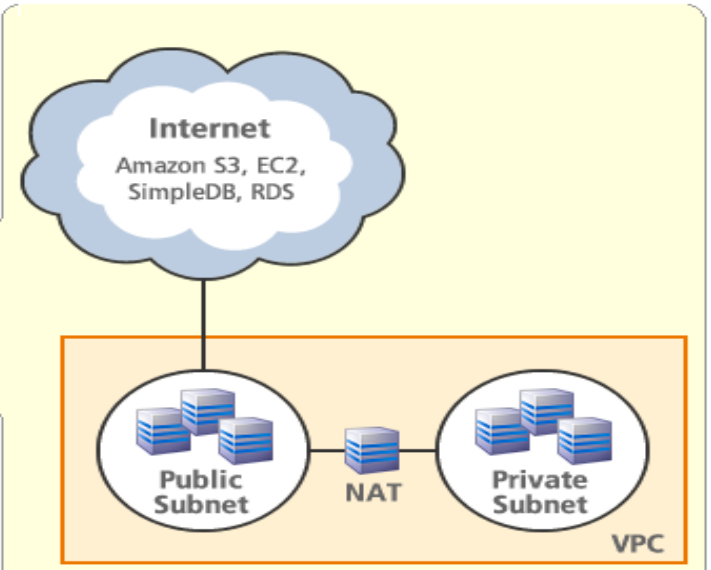
- Documented
- Automated “baseline” setup/teardown
- Easy to expand outside of “baseline”

VPC Options

Create an Amazon Virtual Private Cloud Cancel

Select a VPC configuration below:

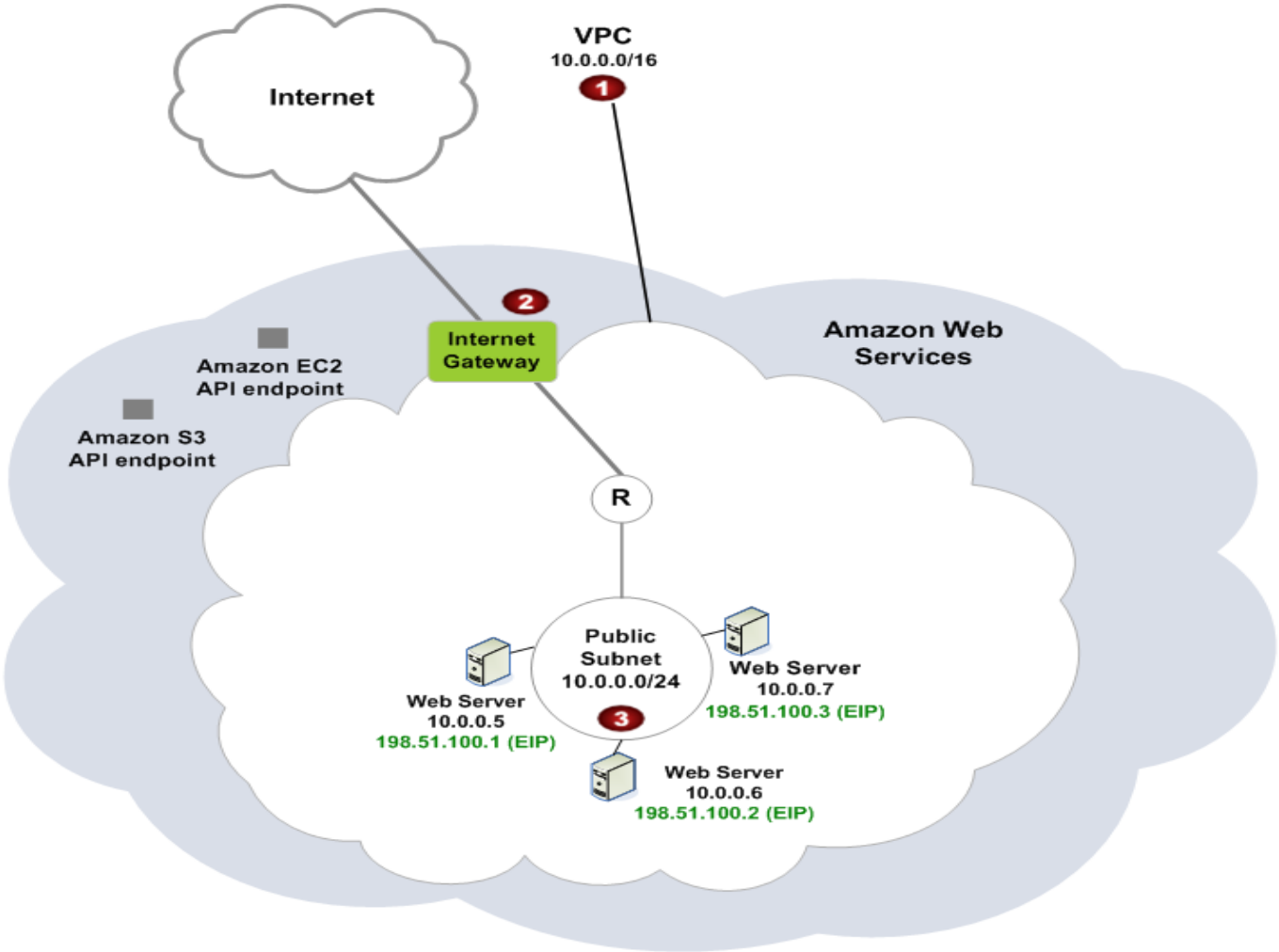
- **VPC with a Single Public Subnet Only**
  Your instances run in a private, isolated section of the AWS cloud with direct access to the Internet. Network access control lists and security groups can be used to provide strict control over inbound and outbound network traffic to your instances.
- **VPC with Public and Private Subnets**
  In addition to containing a public subnet, this configuration adds a private subnet whose instances are not addressable from the Internet. Instances in the private subnet can establish outbound connections to the Internet via the public subnet using Network Address Translation.
- **VPC with Public and Private Subnets and Hardware VPN Access**
  This configuration adds an IPsec Virtual Private Network (VPN) connection between your Amazon VPC and your datacenter - effectively extending your datacenter to the cloud while also providing direct access to the Internet for public subnet instances in your Amazon VPC.
- **VPC with a Private Subnet Only and Hardware VPN Access**
  Your instances run in a private, isolated section of the AWS cloud with a private subnet whose instances are not addressable from the Internet. You can connect this private subnet to your corporate datacenter via an IPsec Virtual Private Network (VPN) tunnel.



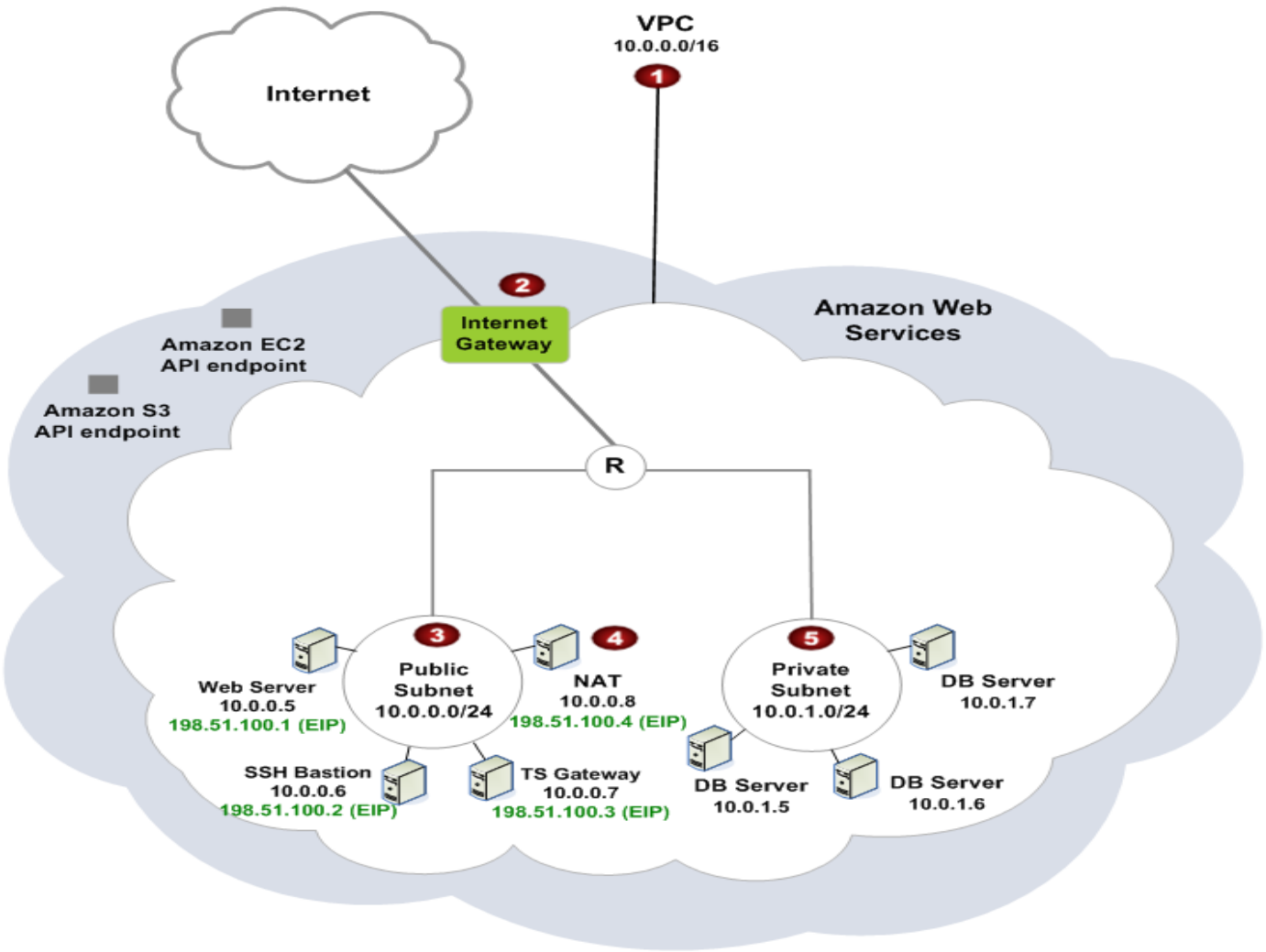
Creates: a /16 network with two /24 subnets. Public subnet instances use Elastic IPs to access the Internet. Private subnet instances access the Internet via a Network Address Translation (NAT) instance in the public subnet. (Hourly charges for NAT instances apply)

Continue

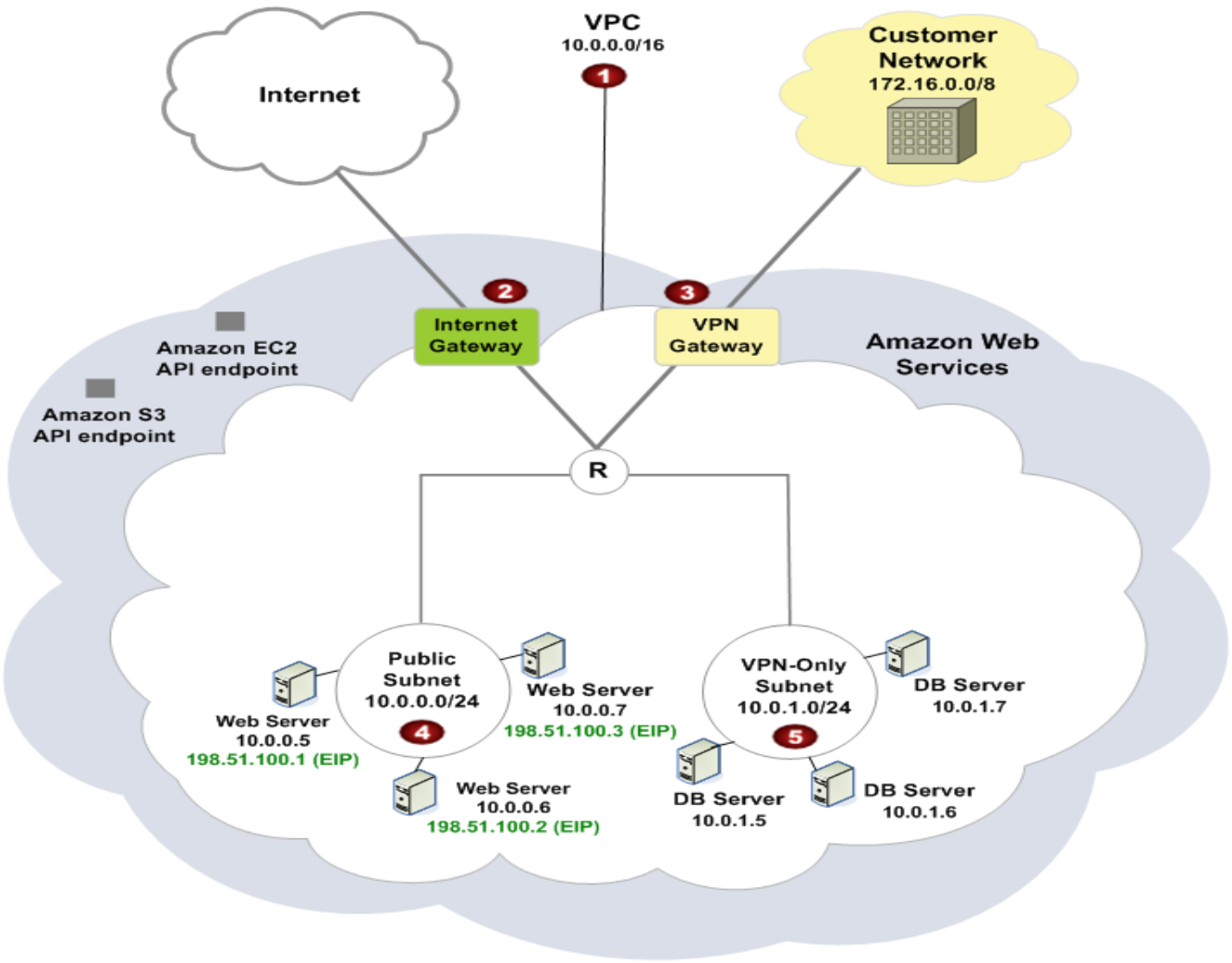
Single Subnet Only



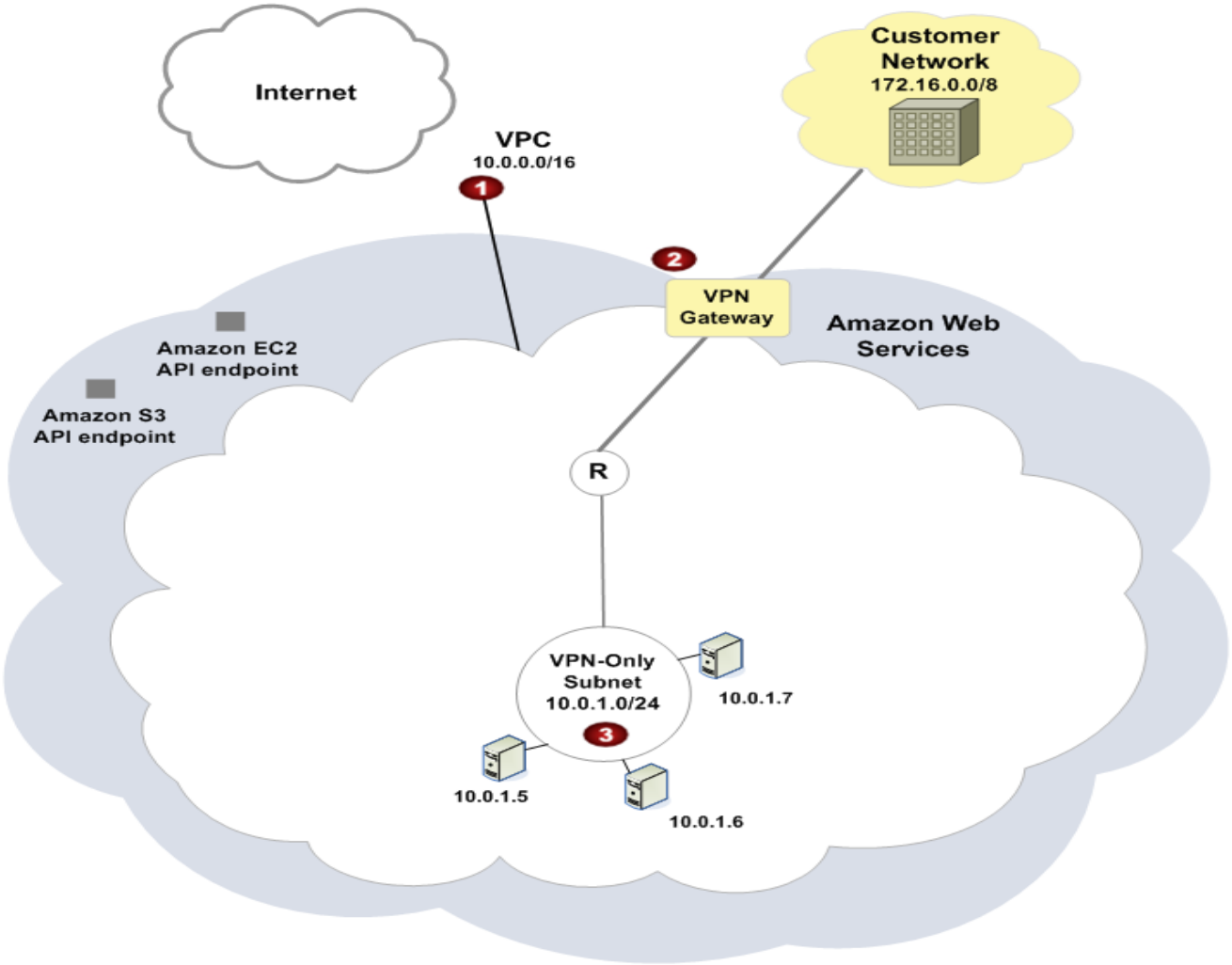
Public and Private Subnets



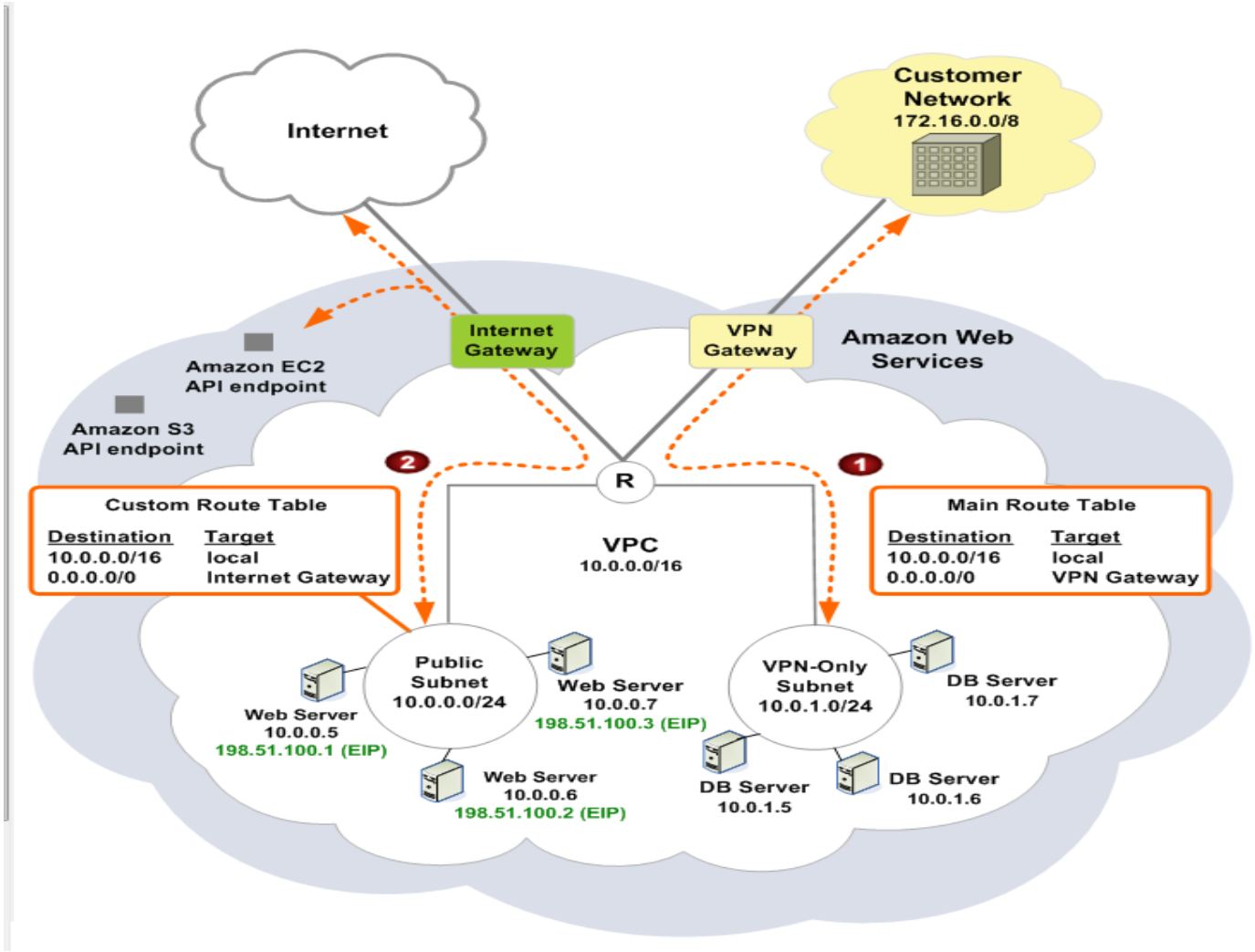
Public, Private and VPN



Private Subnet Only



VPC Subnet Routing



Cost

Amazon Elastic Compute Cloud

View/Edit Service

US East (Northern Virginia) Region			
Amazon EC2 running Linux/UNIX			
	$0.085 per Small Instance (m1.small) instance-hour (or partial hour)	315 Hrs	26.78
Amazon EC2 EBS			
	$0.10 per GB-month of provisioned storage	6.263 GB-Mo	0.63
	$0.10 per 1 million I/O requests	142,684 IOs	0.01
	$0.15 per GB-Month of snapshot data stored	2.128 GB-Mo	0.32
	$0.01 per 10,000 gets (when loading a snapshot)	5,936 Requests	0.01
Elastic IP Addresses			
	$0.01 per non-attached Elastic IP address per complete hour	584 Hrs	5.84
		Download Usage Report »	**33.59**

Amazon Simple Storage Service

View/Edit Service

US Standard Region			
	$0.140 per GB - first 1 TB / month of storage used	1.999 GB-Mo	0.28
	$0.01 per 1,000 PUT, COPY, POST, or LIST requests	16 Requests	0.01
		Download Usage Report »	**0.29**

Amazon Virtual Private Cloud

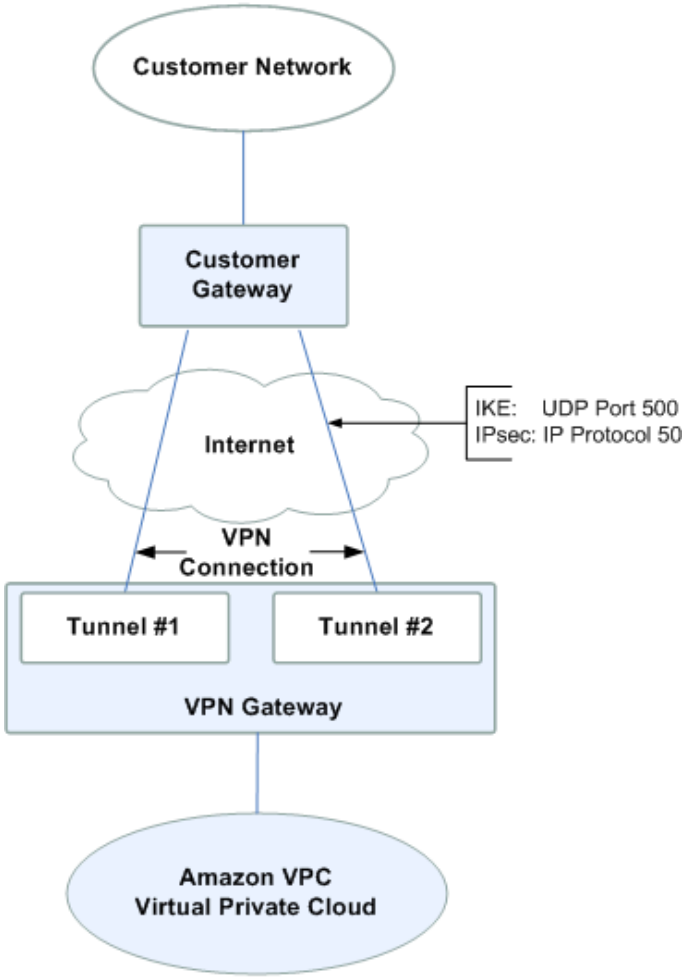
View/Edit Service

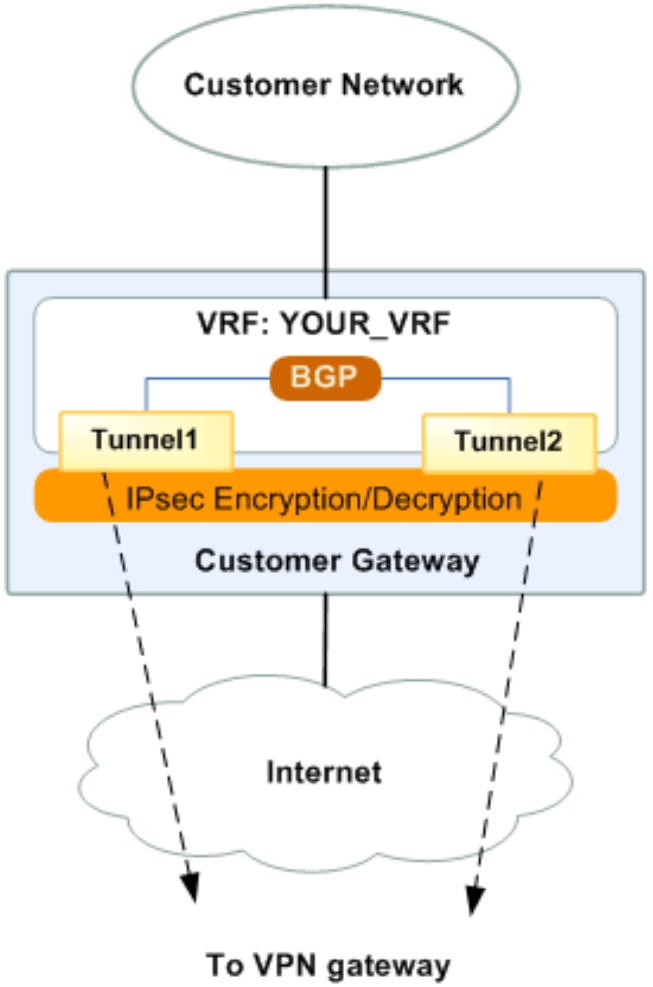
	$0.05 per VPN Connection-Hour	547 Hrs	27.35
		Download Usage Report »	**27.35**

Safe

- Use existing security infrastructure
  - Only available from within UCCS network
- Isolated
  - No outside connection from within VPC
  - Encrypted VPN connection
- Controlled operating time
  - Automated baseline setup
  - Automated complete teardown

Security Overview

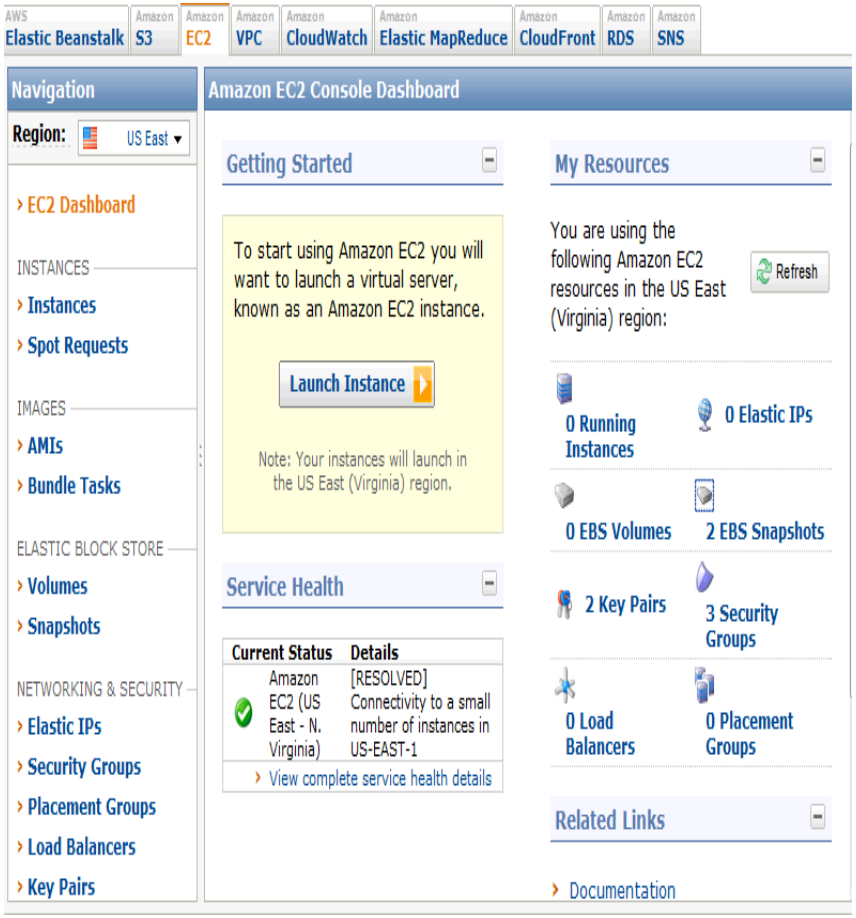


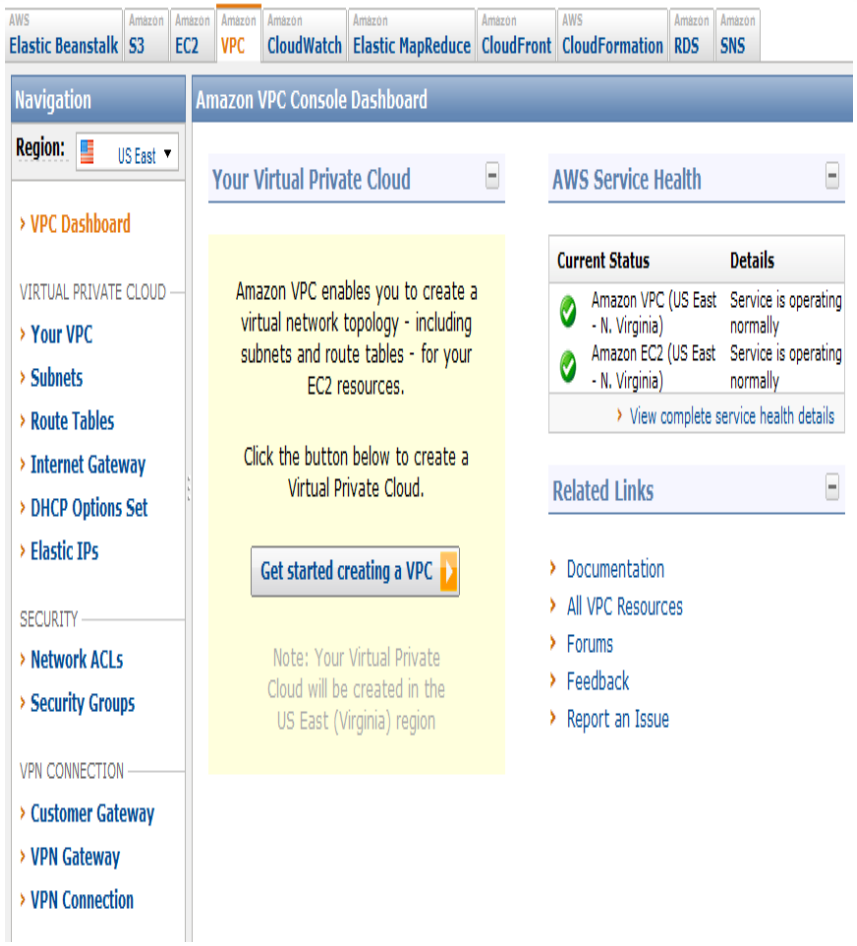


Simple

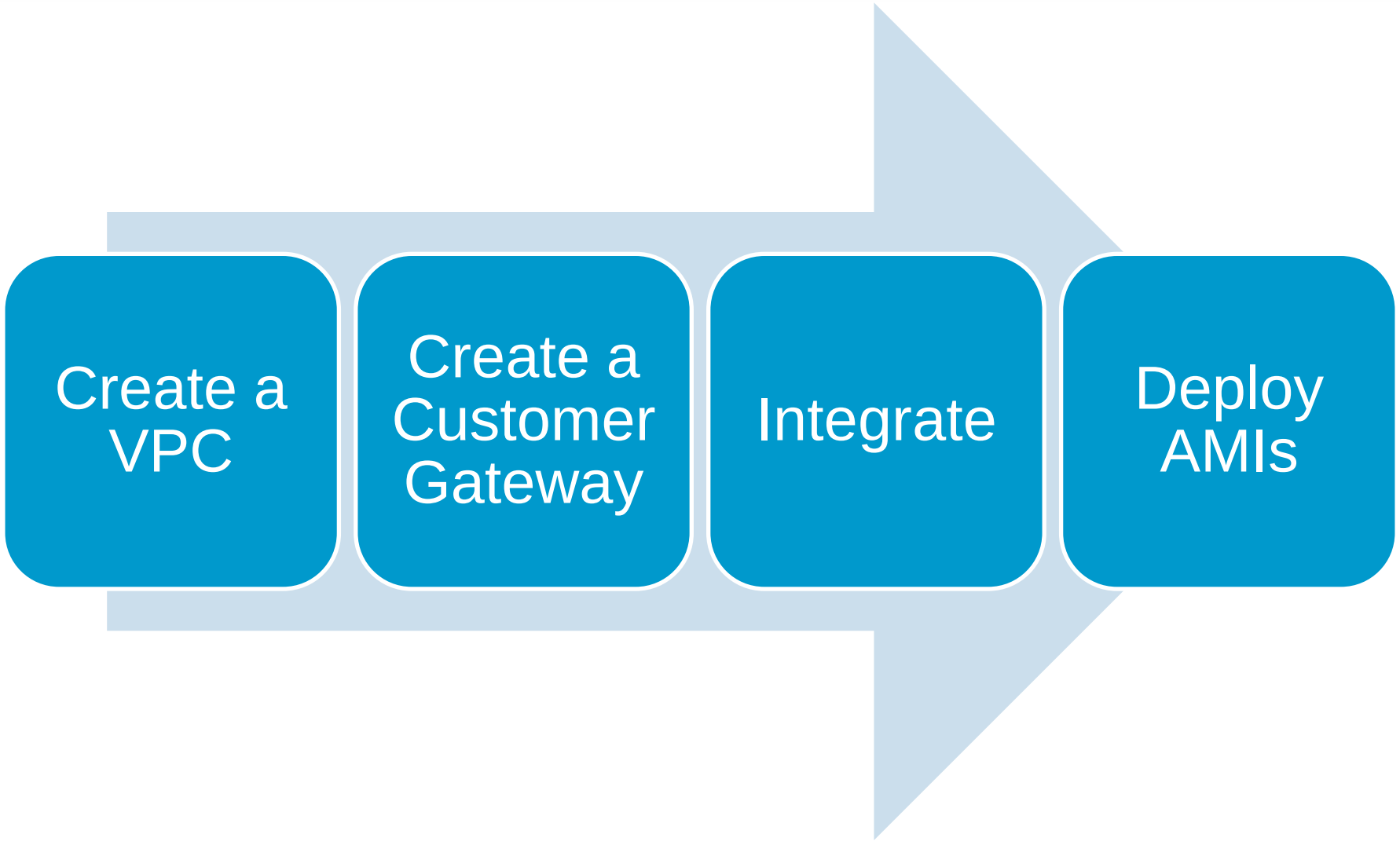
- Amazon Web Service (AWS) Management Console
  - Point-and-click web interface
  - Monitor services
  - Simplified setup
- AWS SDK for .NET
  - Automation using .NET framework
- Lots of documentation

AWS Management Console

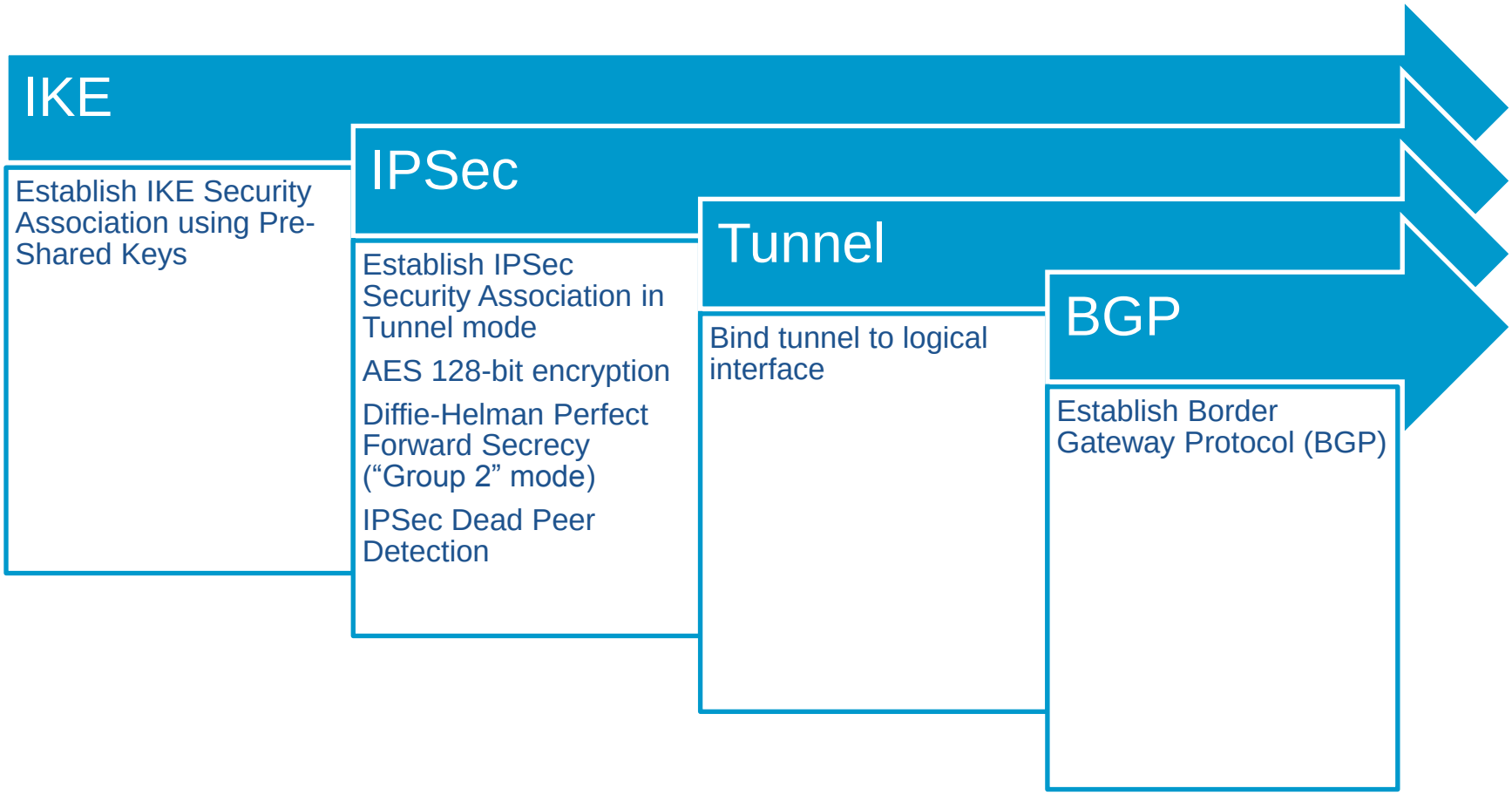




Connecting to VPC



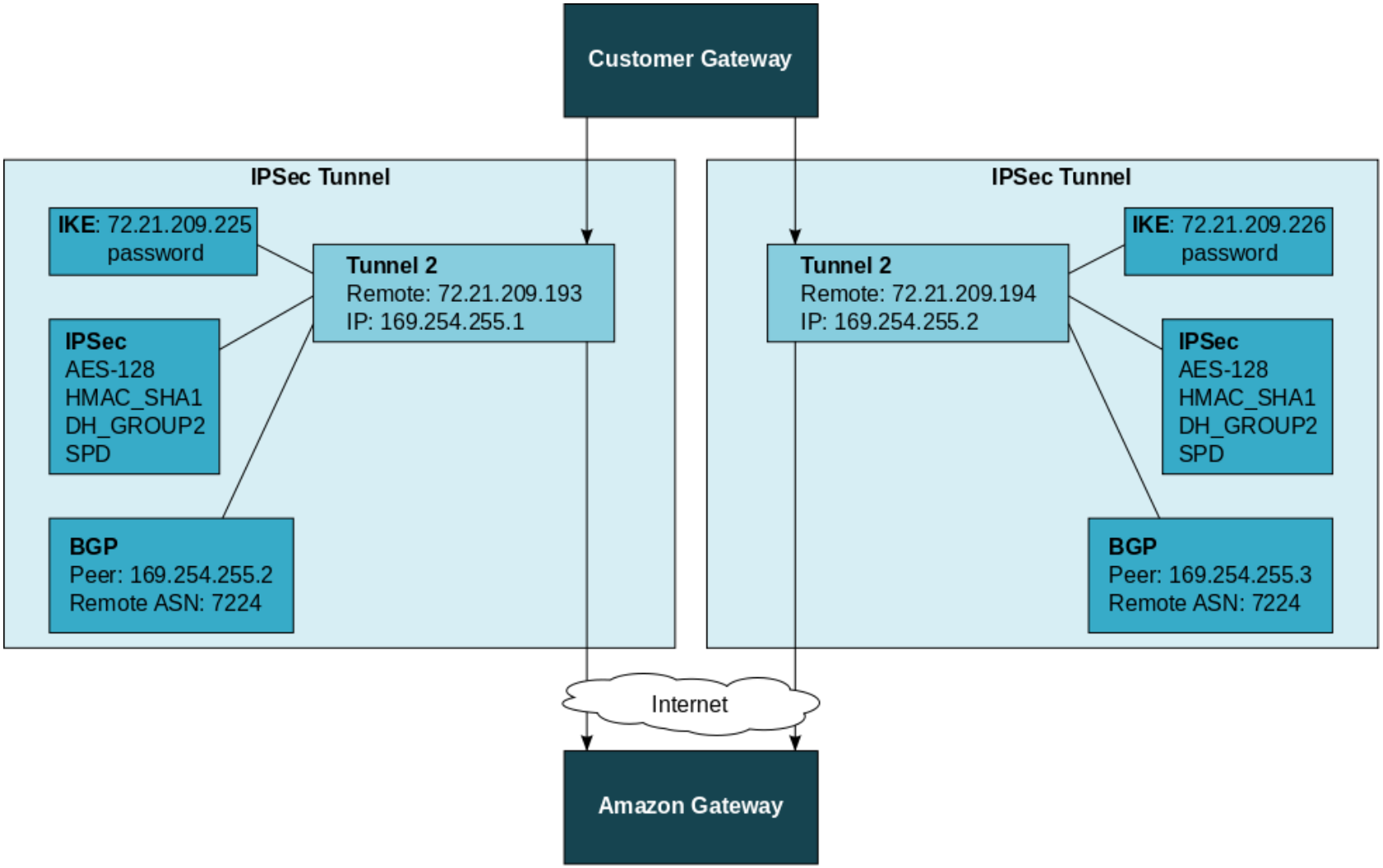
Gateway Requirements



CentOS Custom Gateway

- Install ipsec-tools
  - Racoon
  - Setkey
- Install quagga
  - Zebra
  - Bgpd
- Bind tunnels to a logical interface
- Create point-to-point connection

CentOS Gateway Cont…



Summary

- Using Amazon's VPC all three goals can be reached
  - Learning
    - Help solidify concepts through "hands on" experience
  - Research
    - Flexible environment with a vast support matrix to meet a wide array of research needs
  - Recognition
    - Through learning and research UCCS will be better equipped to compete on the world stage

Questions

IPSec

```
path include "/etc/racoon";
path pre_shared_key "/etc/racoon/psk.txt";


remote 72.21.209.225 {
        exchange_mode main;
        lifetime time 28800 seconds;
        dpd_delay 10;
                                                dpd_retry 3;
        proposal {
                encryption_algorithm aes128;
                hash_algorithm sha1;
                authentication_method pre_shared_key;
                dh_group 2;
        }
        generate_policy off;
}

remote 72.21.209.193 {
        exchange_mode main;
        lifetime time 28800 seconds;
        dpd_delay 10;
        dpd_retry 3;
        proposal {
                encryption_algorithm aes128;
                hash_algorithm sha1;
                authentication_method pre_shared_key;
                dh_group 2;
        }
        generate_policy off;
}
```

```
#!/sbin/setkey -f
flush;
spdflush;

spdadd 169.254.255.2/30 169.254.255.1/30 any -P out ipsec
   esp/tunnel/a.b.c.d-72.21.209.225/require;

spdadd 169.254.255.1/30 169.254.255.2/30 any -P in ipsec
   esp/tunnel/72.21.209.225-a.b.c.d/require;

spdadd 169.254.255.6/30 169.254.255.5/30 any -P out ipsec
   esp/tunnel/a.b.c.d-72.21.209.193/require;

spdadd 169.254.255.5/30 169.254.255.6/30 any -P in ipsec
   esp/tunnel/72.21.209.193-a.b.c.d/require;

spdadd 169.254.255.2/30 192.168.0.0/24 any -P out ipsec
   esp/tunnel/a.b.c.d-72.21.209.225/require;

spdadd 192.168.0.0/24 169.254.255.2/30 any -P in ipsec
   esp/tunnel/72.21.209.225-a.b.c.d/require;

spdadd 169.254.255.6/30 192.168.0.0/24 any -P out ipsec
   esp/tunnel/a.b.c.d-72.21.209.193/require;

spdadd 192.168.0.0/24 169.254.255.6/30 any -P in ipsec
   esp/tunnel/72.21.209.193-a.b.c.d/require;

 spdadd 0.0.0.0/0 192.168.0.0/24 any -P out ipsec
   esp/tunnel/a.b.c.d-72.21.209.193/require;

spdadd 192.168.0.0/24 0.0.0.0/0 any -P in ipsec
   esp/tunnel/72.21.209.193-a.b.c.d/require;
```

Quagga

```
hostname cgw-2493774d
password testPassword
enable password testPassword
!
log file /var/log/quagga/bgpd
!debug bgp events
!debug bgp zebra
debug bgp updates
!
router bgp 65000
bgp router-id a.b.c.d
network 169.254.255.2/30
network 169.254.255.6/30
network 0.0.0.0/0
!
! aws tunnel #1 neighbor
neighbor 169.254.255.1 remote-as 7224
!
! aws tunnel #2 neighbor
neighbor 169.254.255.5 remote-as 7224
!
line vty
```