June 13, 2016

# Securing Cloud Environments Using Identity-Based VNFs

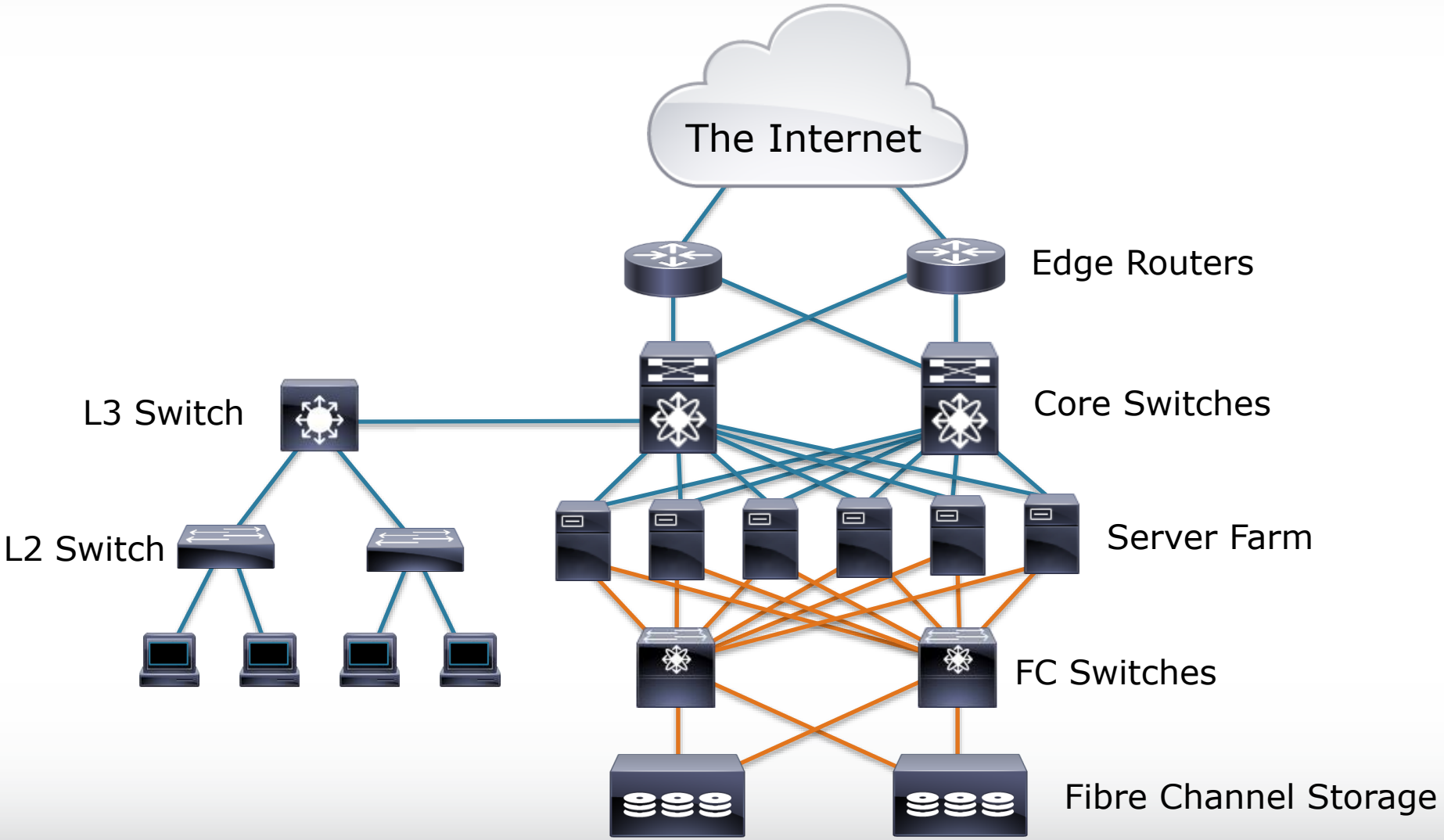
Robert M. Cannistra
robert.cannistra@marist.edu

Doug Johnson
dj@blackridge.us

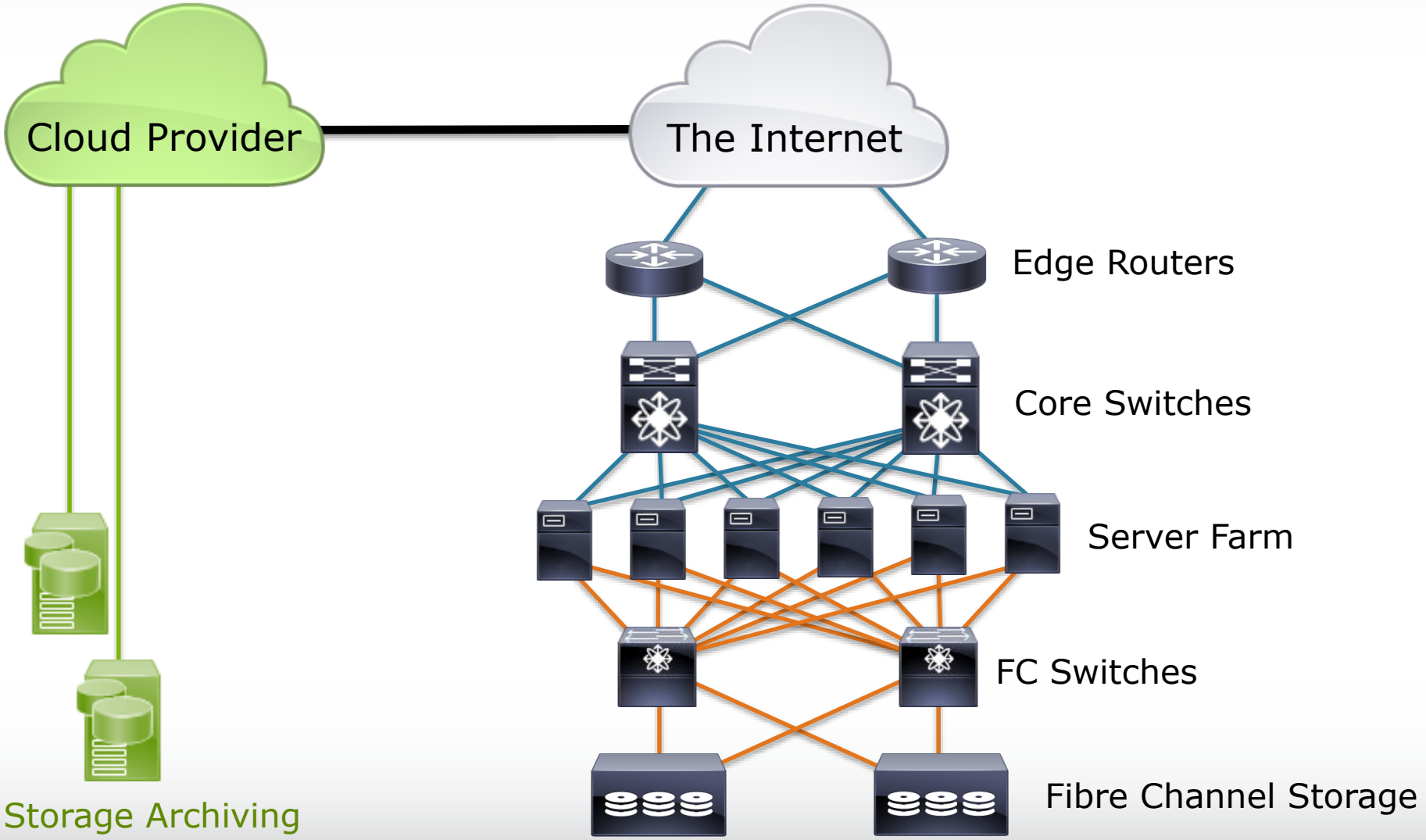
MARIST

BlackRidge TECHNOLOGY

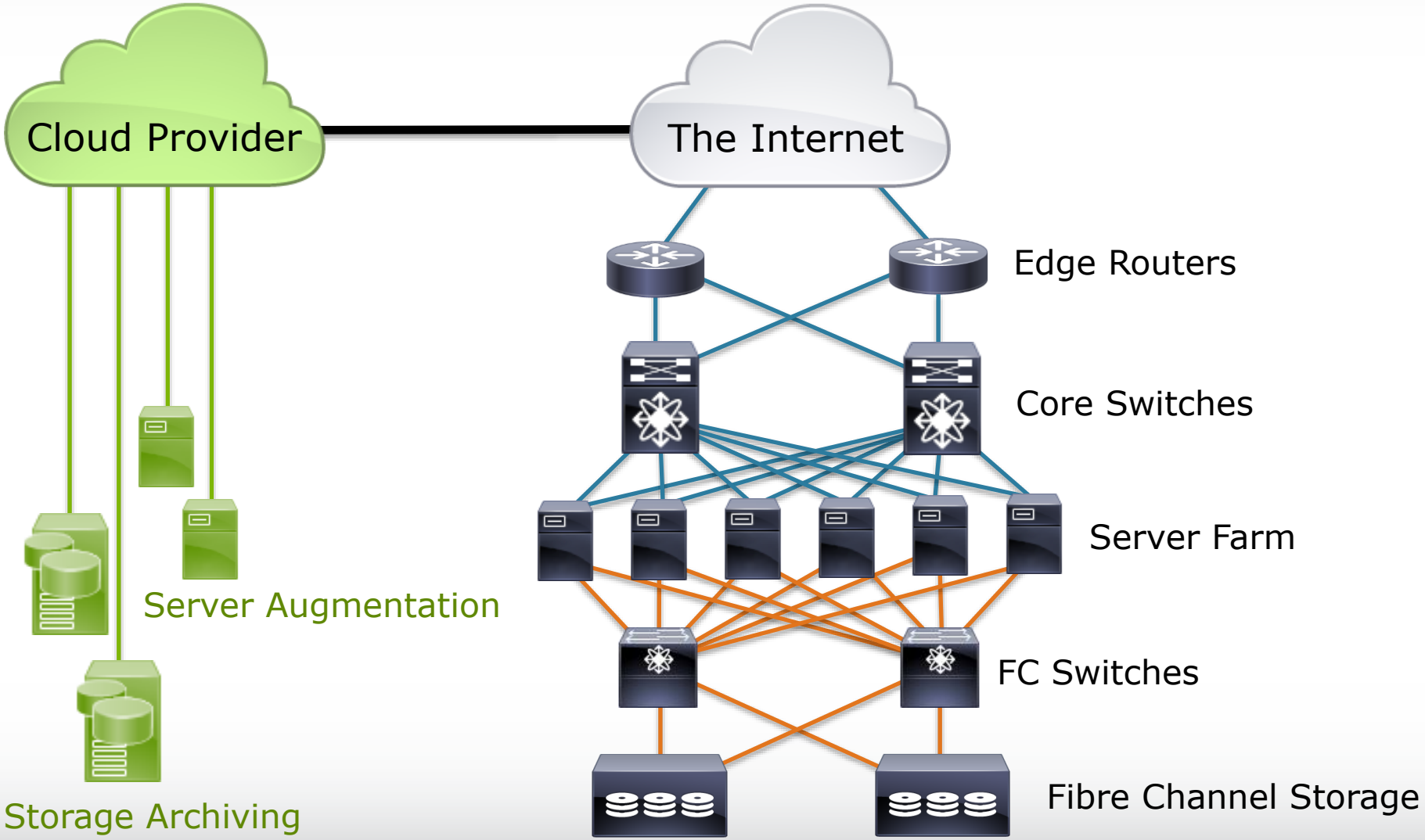
# Traditional Network



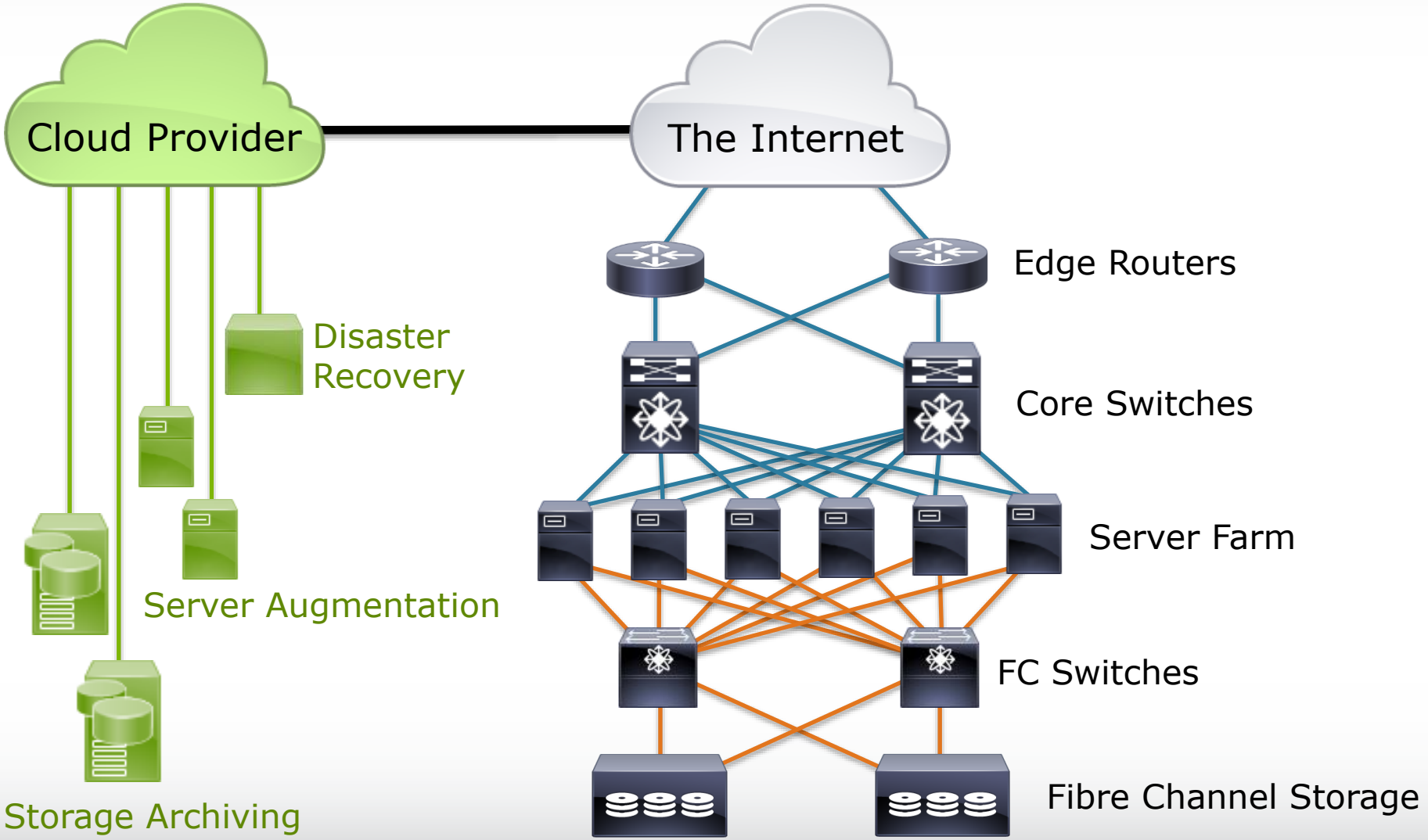
# Adding Cloud Services – Storage Archiving



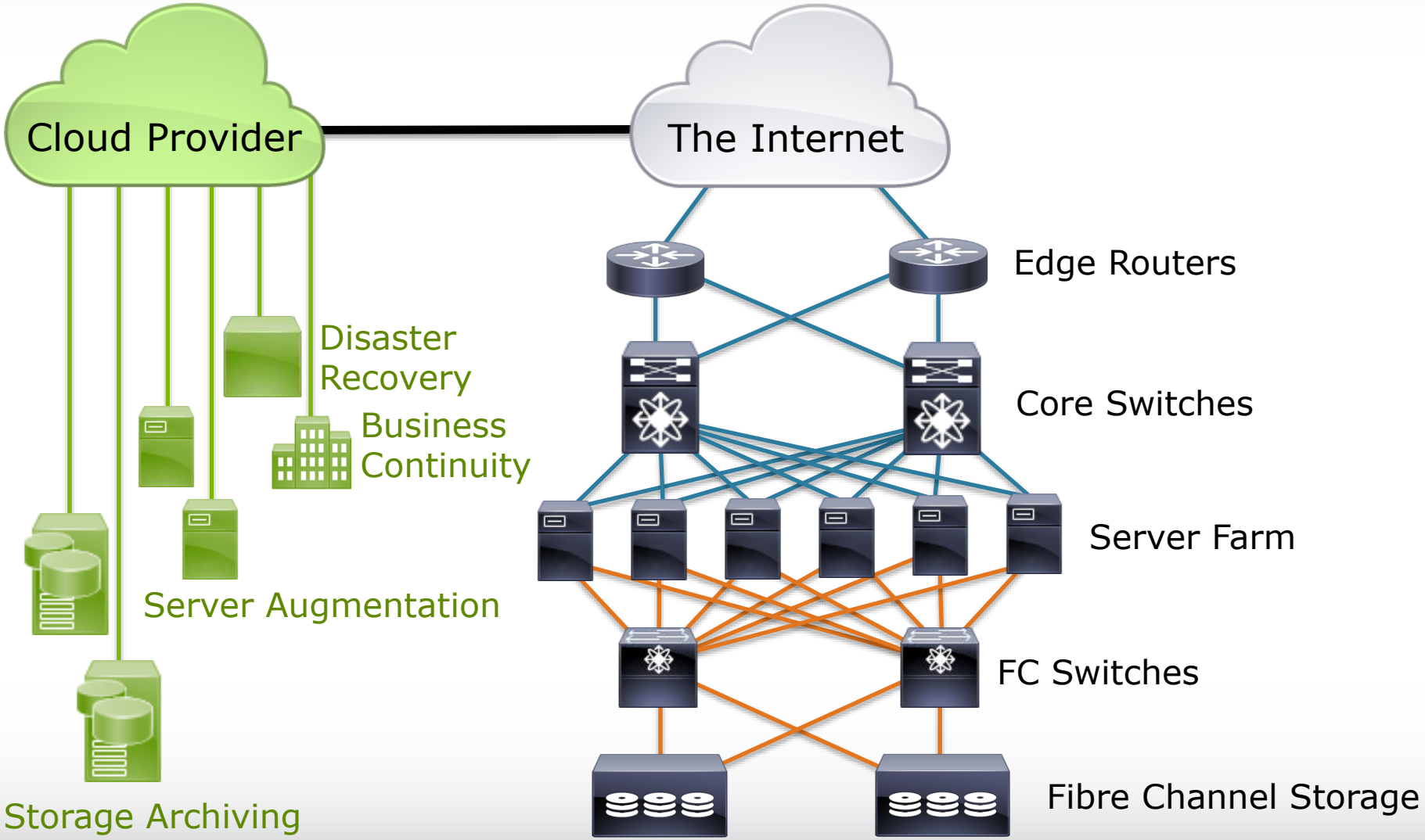
# Adding Cloud Services – Server Augmentation



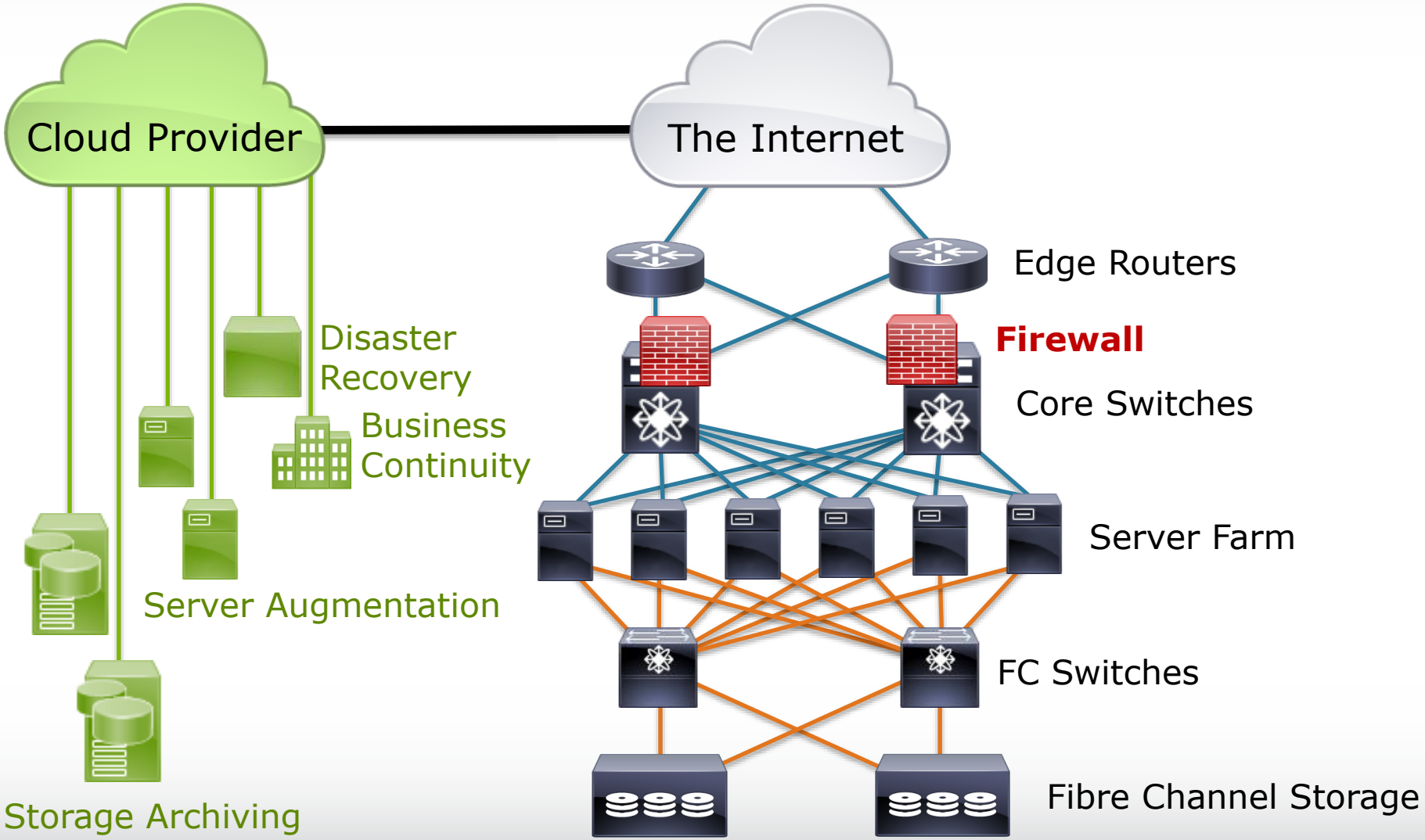
# Adding Cloud Services – Disaster Recovery



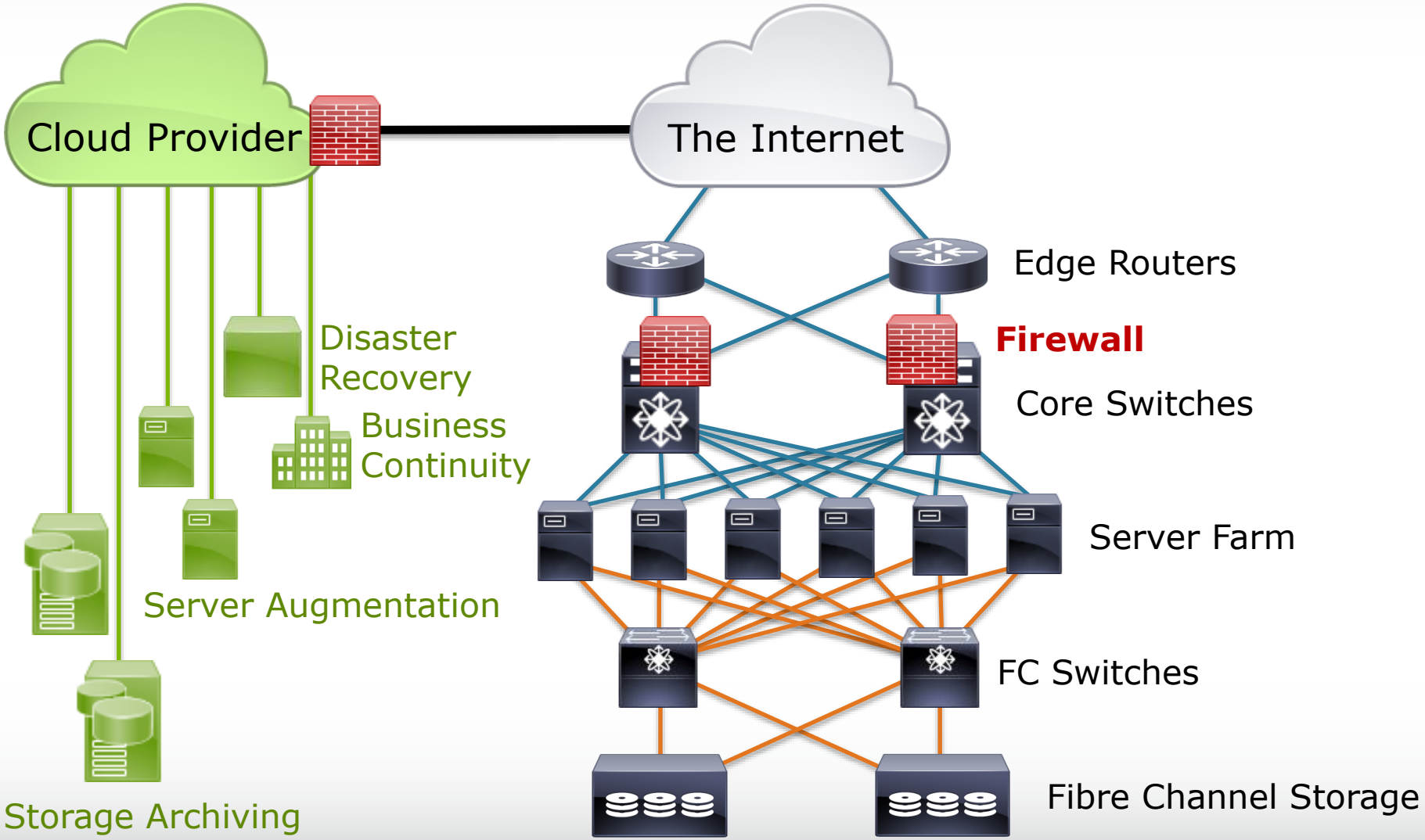
# Adding Cloud Services – Business Continuity



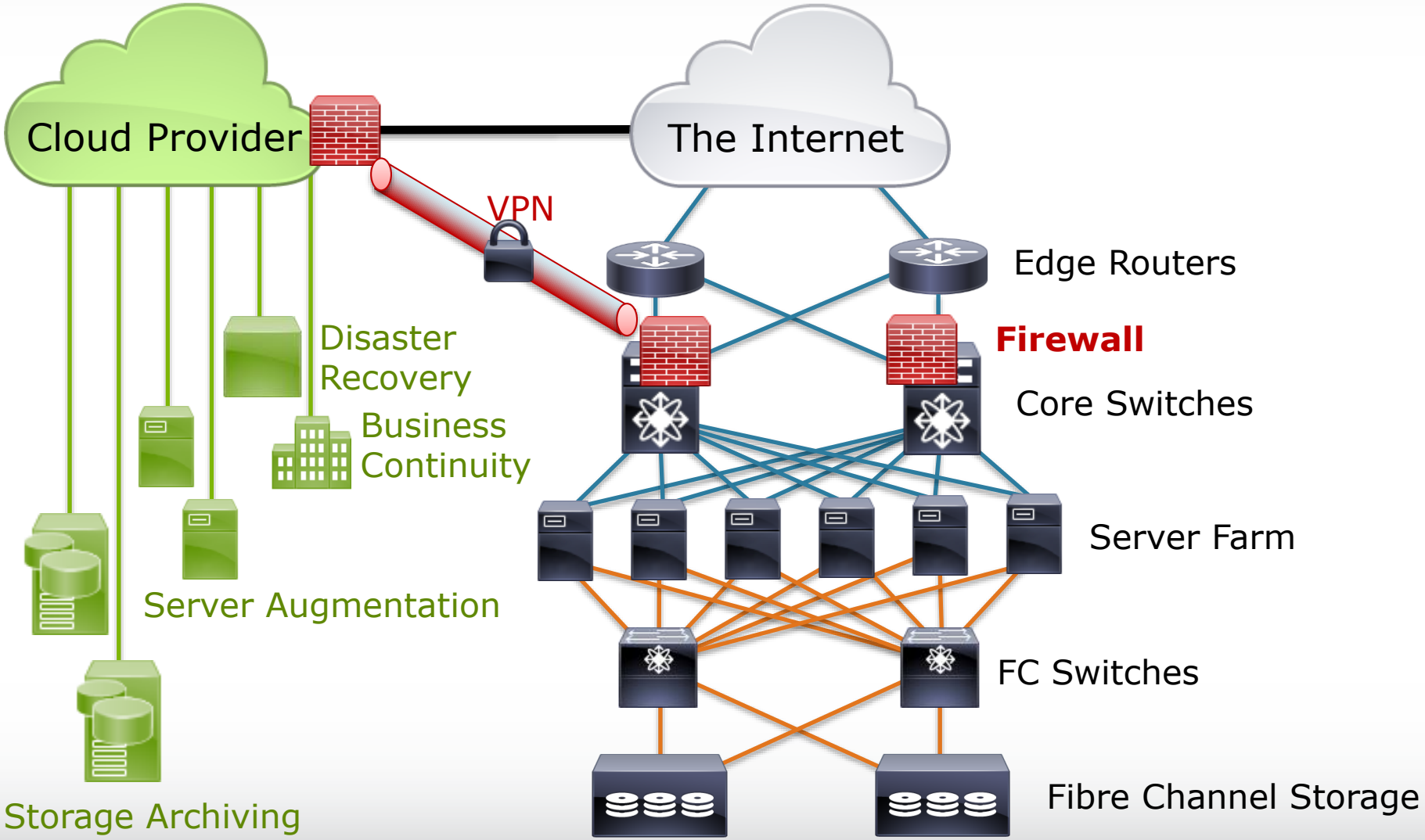
# Protecting the Network – Add Firewalls



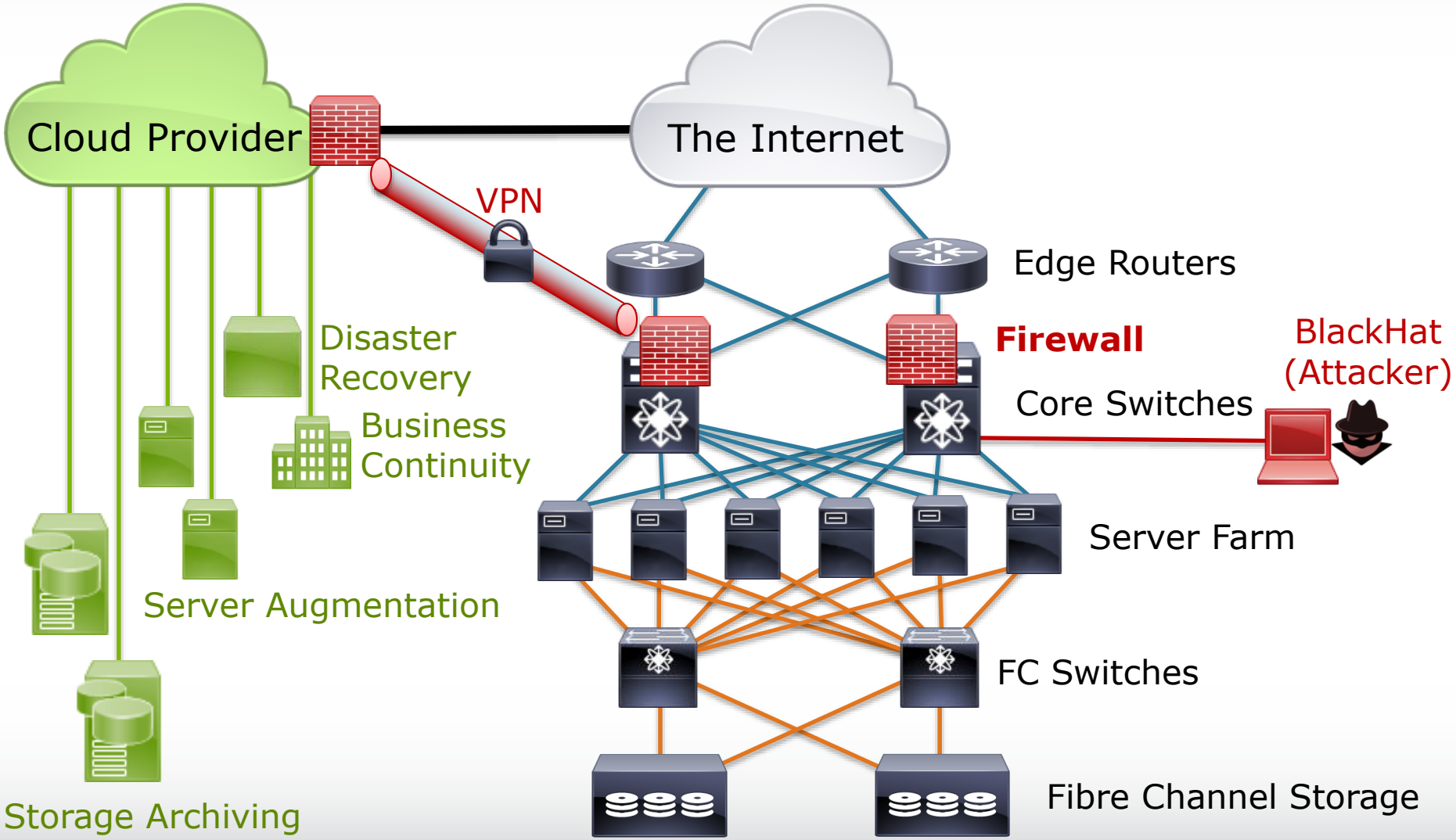
# Protecting Cloud Services – Add Firewalls



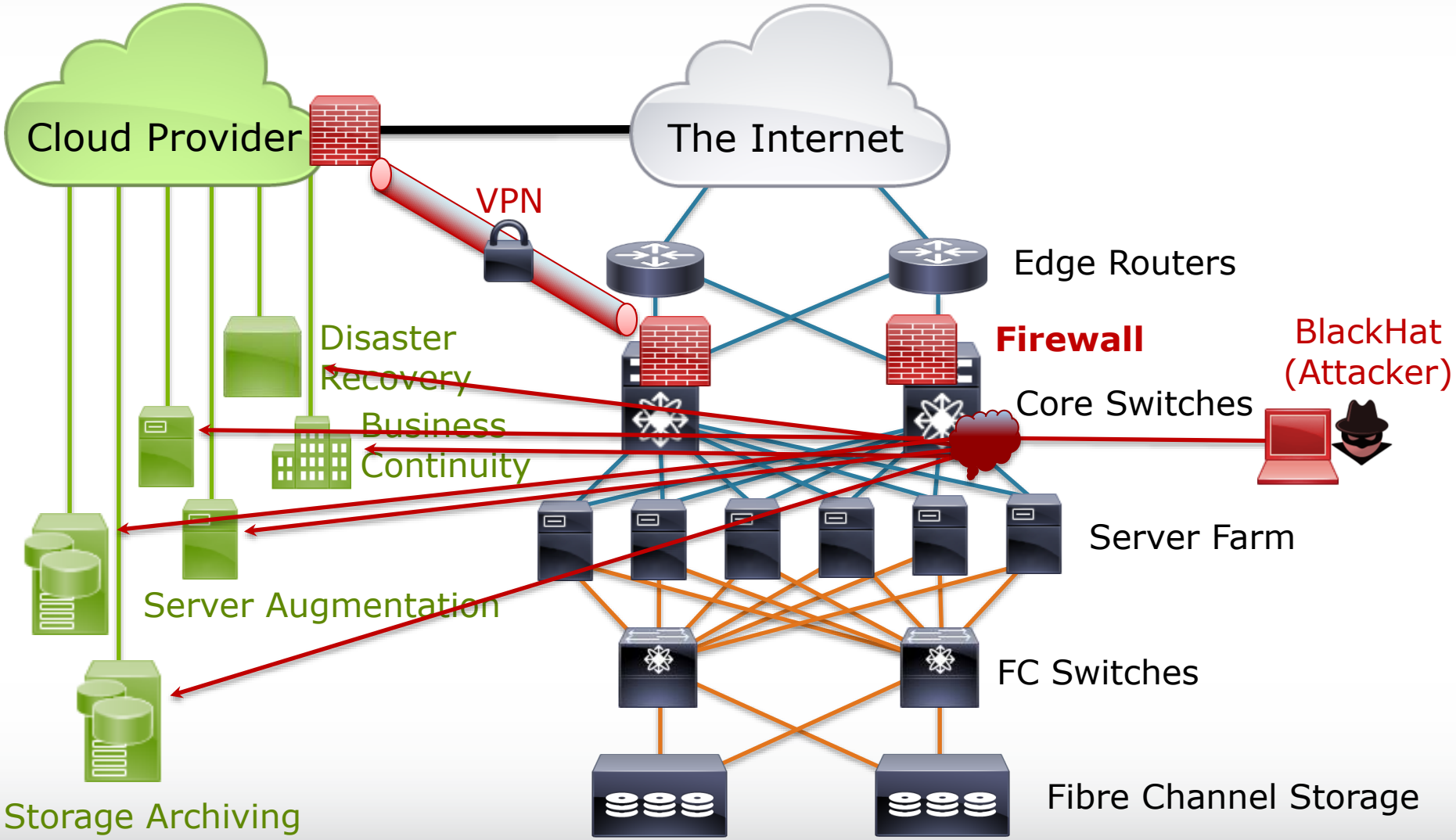
# Protecting Cloud Services – Add IPsec VPN



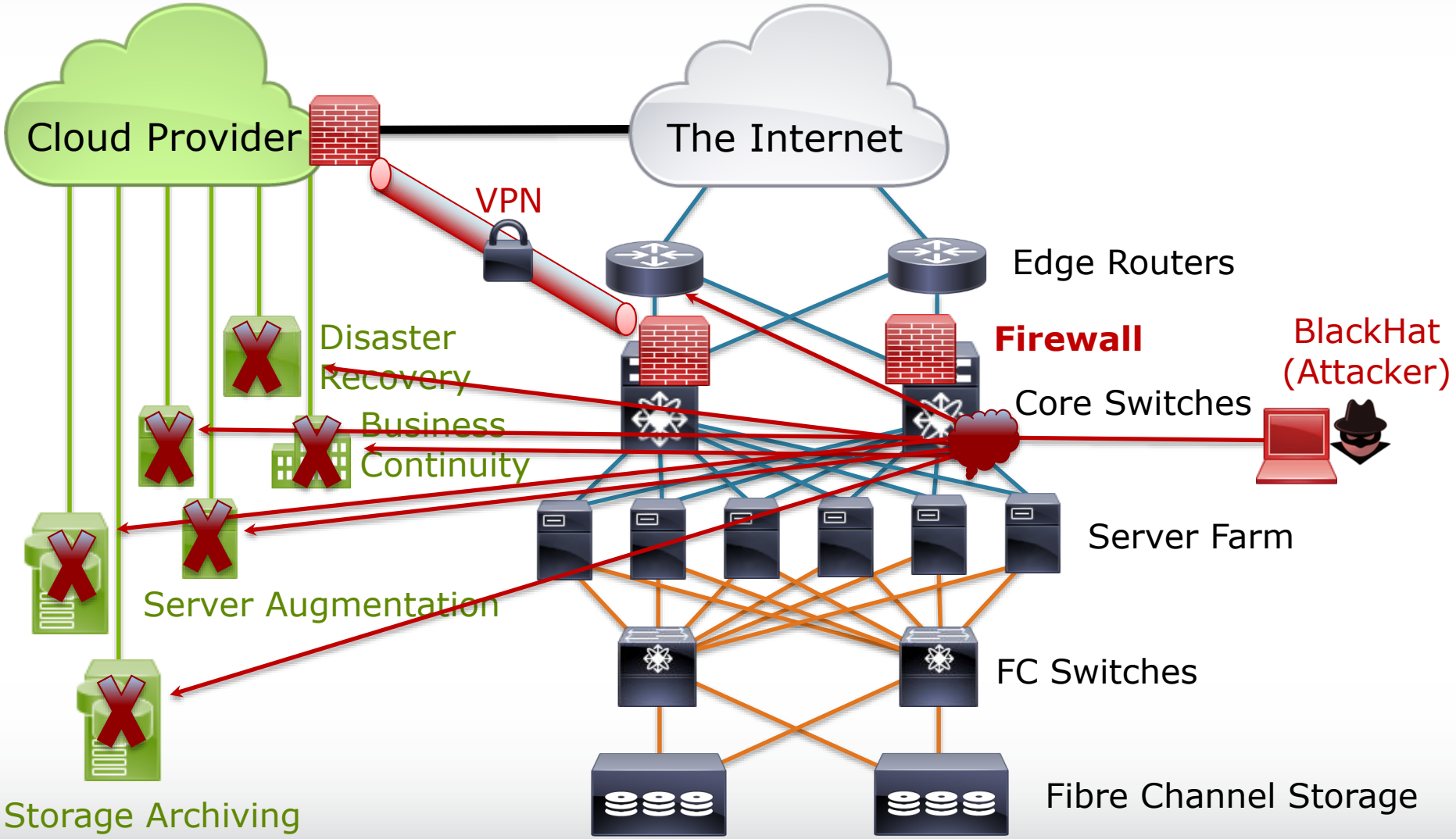
# Protecting Cloud Services – Attack! Uh Oh!



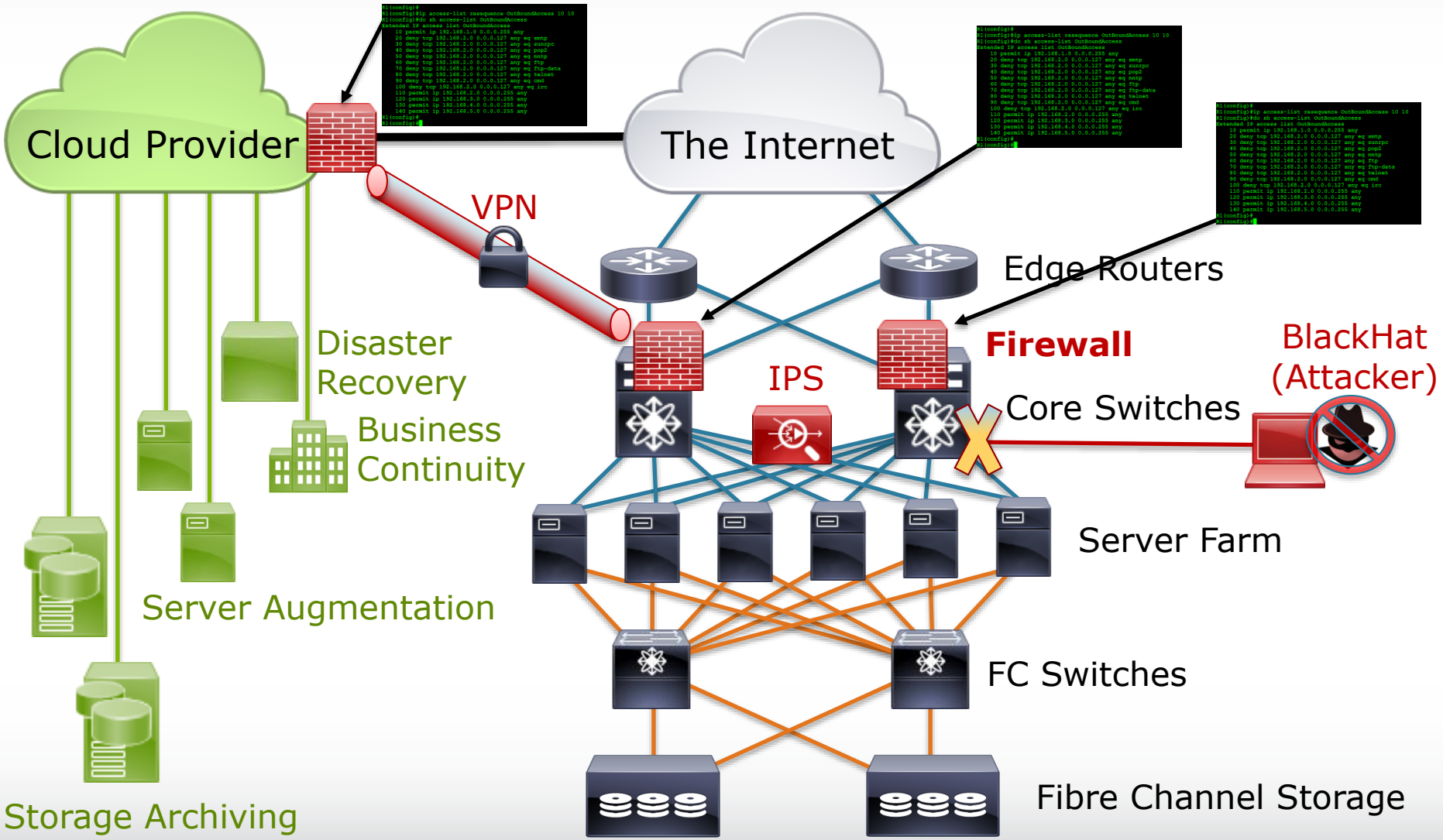
# Protecting Cloud Services – Attack! Uh Oh!



# Protecting Cloud Services – Resources Down!!!



# Protecting Cloud Services – Modify Firewall & Add IPS



# Cloud ⊄ Secure

- Cloud Services are prone to:
  - Vulnerabilities:
    - OS Security Vulnerabilities
    - Application Vulnerabilities
    - Database Vulnerabilities
    - Software Portal Vulnerabilities
  - Attacks
    - DDOS Attacks
    - Database Injection Attacks
    - Smurf Attacks
    - SYN flood Attacks
    - Buffer Overflow Attacks


But wait… the Cloud can be Secure! Let's see how…

# BlackRidge First Packet Authentication

Developed for the Military on the Battlefield

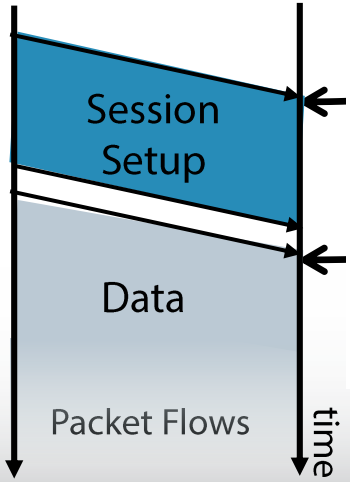
# BlackRidge First Packet Authentication

- Network security is a major weak point - networks do not allow user or device identity to be determined before establishing network sessions
- BlackRidge Transport Access Control (TAC) authenticates identity and enforces security policy on the First Packet, **before a network session is established**

## Cloaked and Protected

It is as if your servers are unplugged from the network.

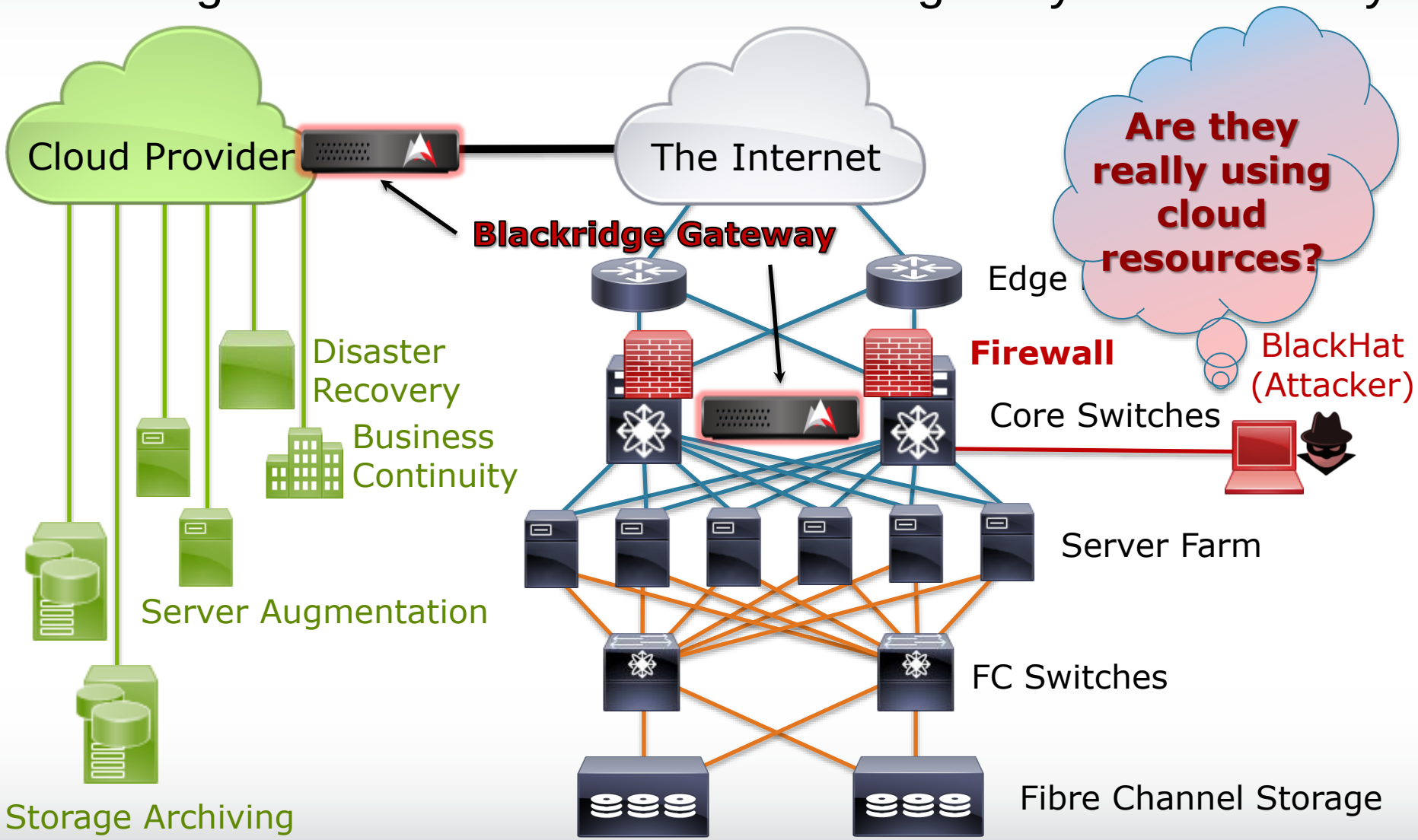
## First Packet Authentication




**First Packet Authentication stops unauthorized access at the earliest possible time.**

**Current security products start after network sessions are established.**

# Protecting Cloud Services – Add Blackridge Physical Gateway



# BlackRidge Protects Your Network and The Cloud

- Brings identity awareness to network security
- Integrates with your existing IDMS system
- Identities dynamically instantiated and pushed to all gateways (on prem, remote, and in the cloud)
- Protection occurs at session establishment using TCP protocol (no proprietary cloud solutions)

# End-to-End Network Security Protection at the Earliest Possible Time

Engages before network sessions are established

- Authenticates identity and enforces security policy on the first TCP packet
- Applies identity-based policy that is network topology independent and supports flat networks
- Low latency and highly scalable – no DPI and complements and enhances existing security infrastructure

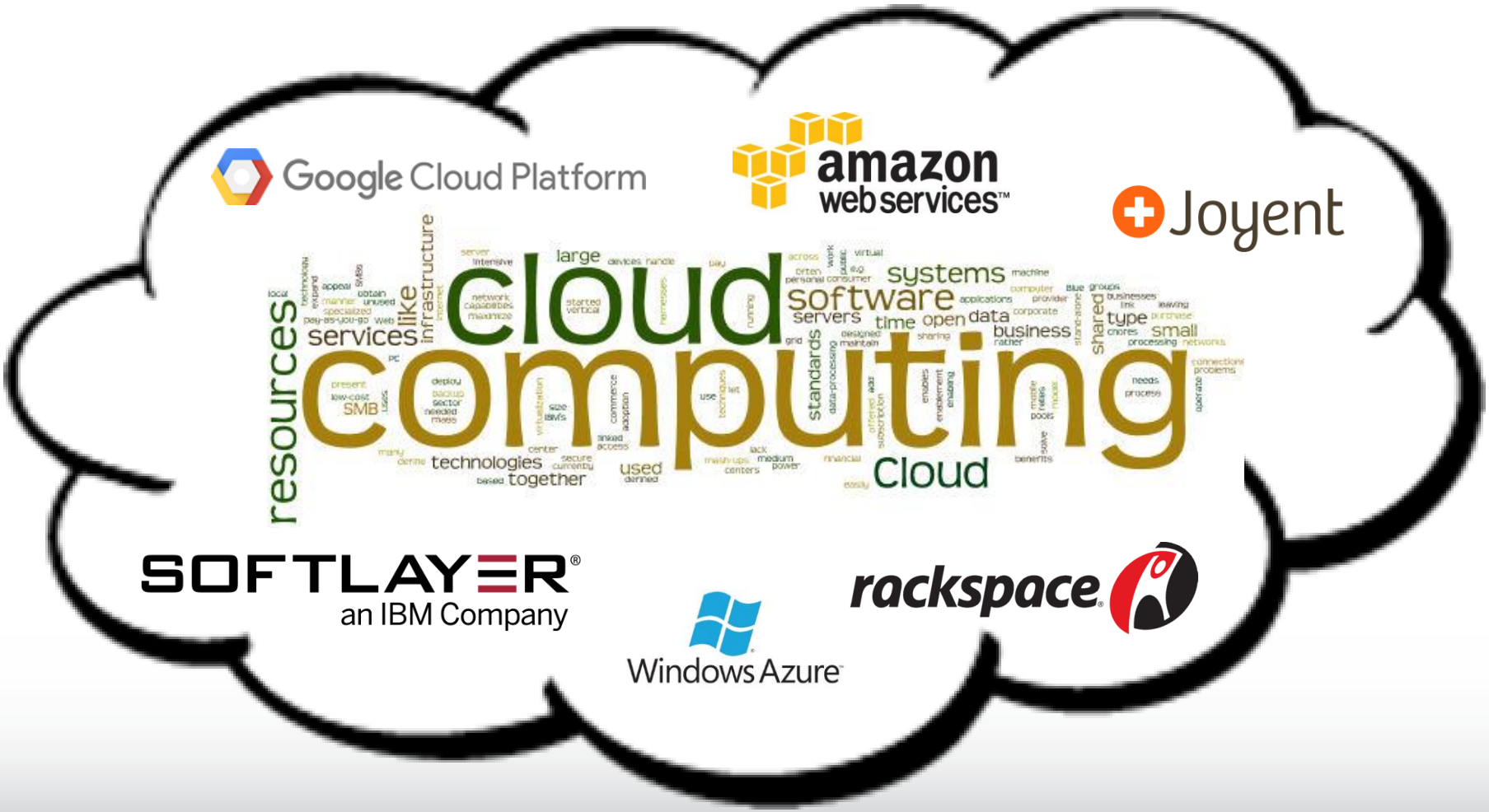
Insider and third party threat protection and risk management

- Cloaks (as if unplugged) servers and clouds from unauthorized users
- Segments and isolates networks to limit risk and meet compliance
- Provide real-time user identity attribution to SIEM/Analytics systems

Outside threats - stops the attack "kill chain"

- Prevents scanning and reconnaissance - ports cannot be found
- Blocks known and unknown threats and reduces network traffic
- Stops lateral (east/west) spreading and data exfiltration

# Cloud Environments of Today



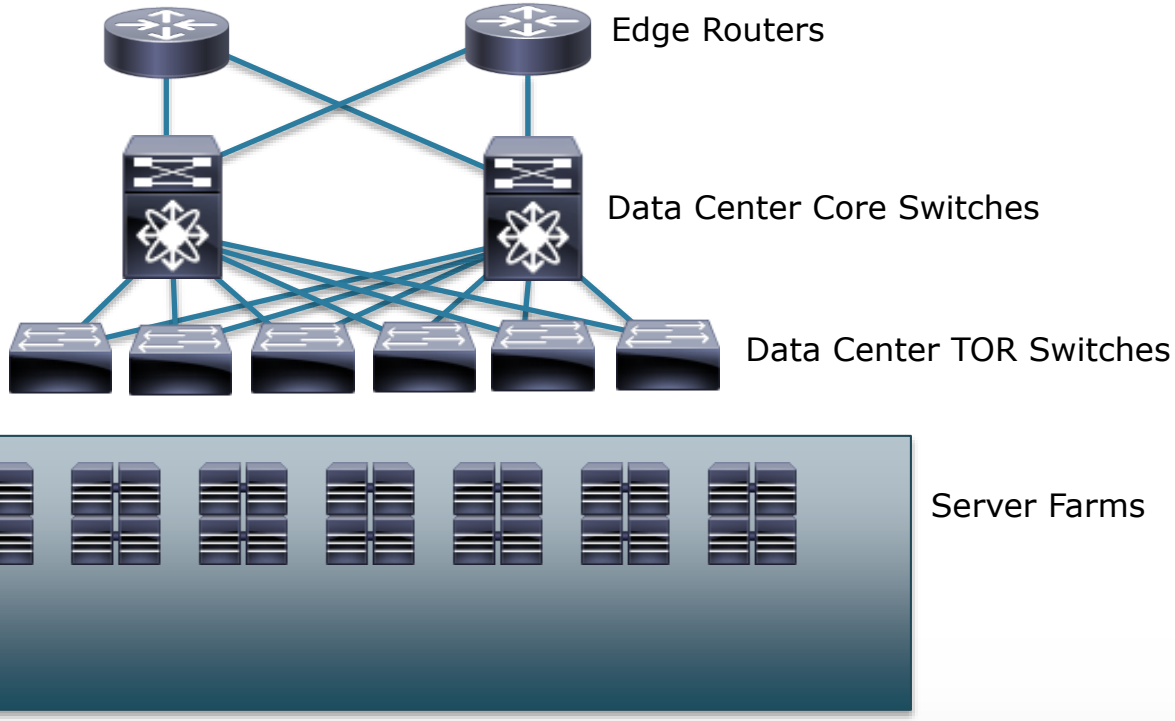
# Cloud-Based Virtualized Infrastructure

- Typically…
  - Built on Open Architecture
  - Highly Customized to ensure expedited service requests

  - …therefore… **Inherently InSecure**

# Before SDN (Software Defined Networking)

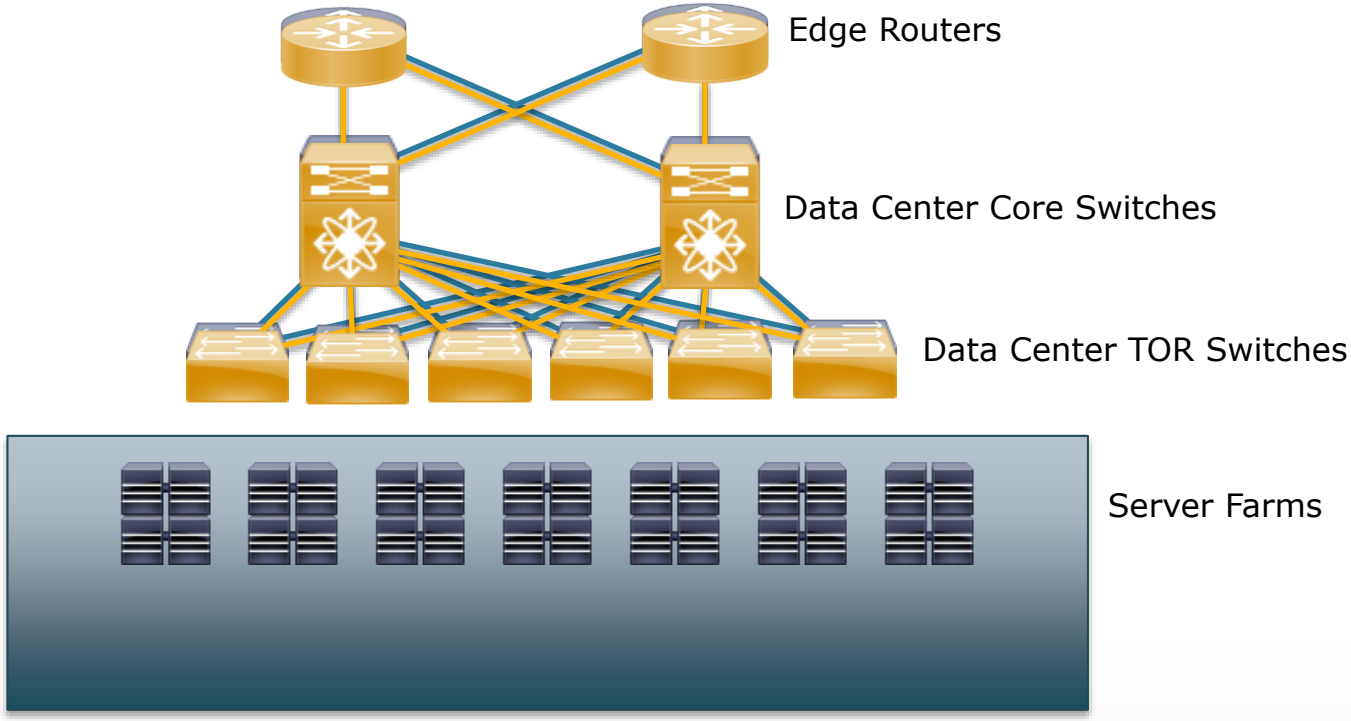
Basic Data Center Topology




= Data Plane

# Before SDN (Software Defined Networking)

Basic Data Center Topology

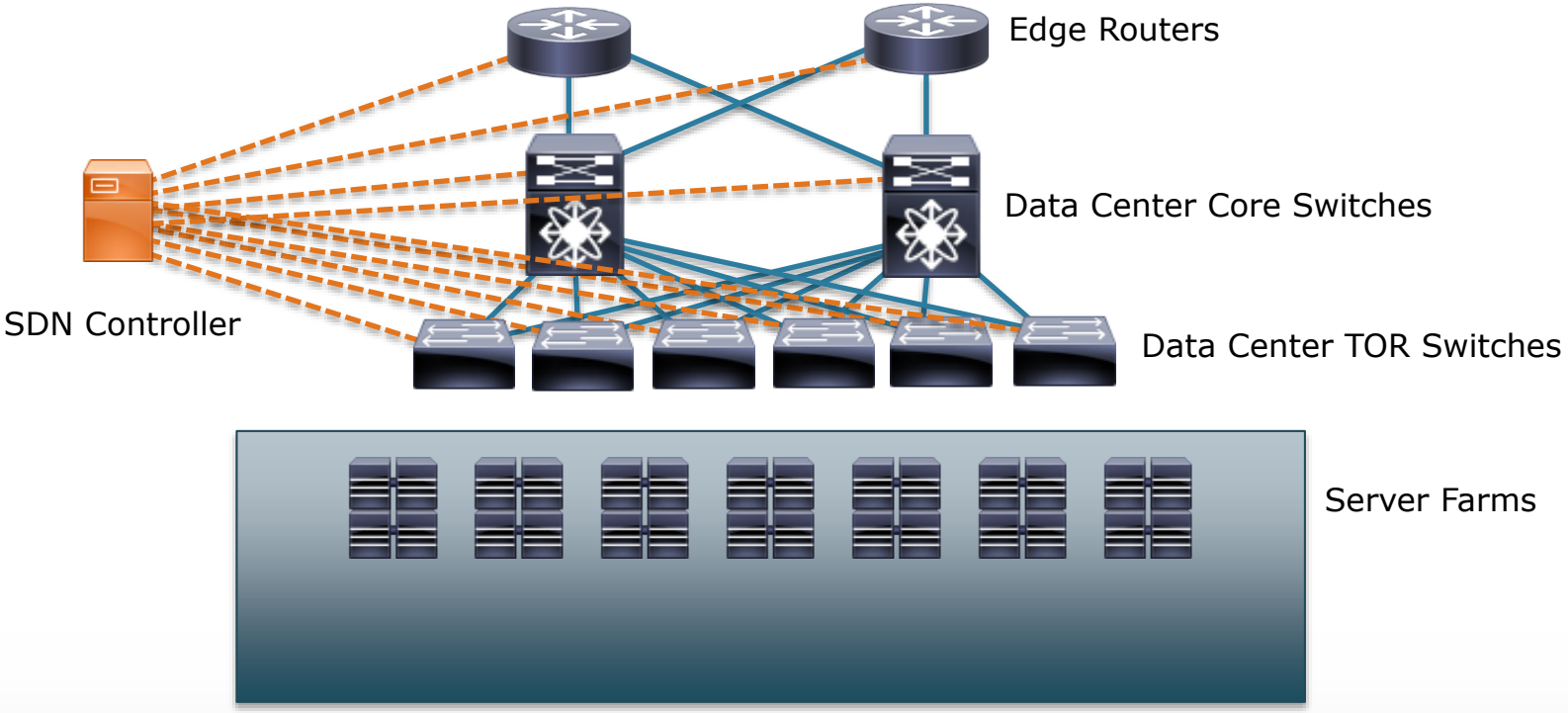



= Data Plane

= Control Plane

# After SDN (Software Defined Networking)

## Software Defined Data Center Topology

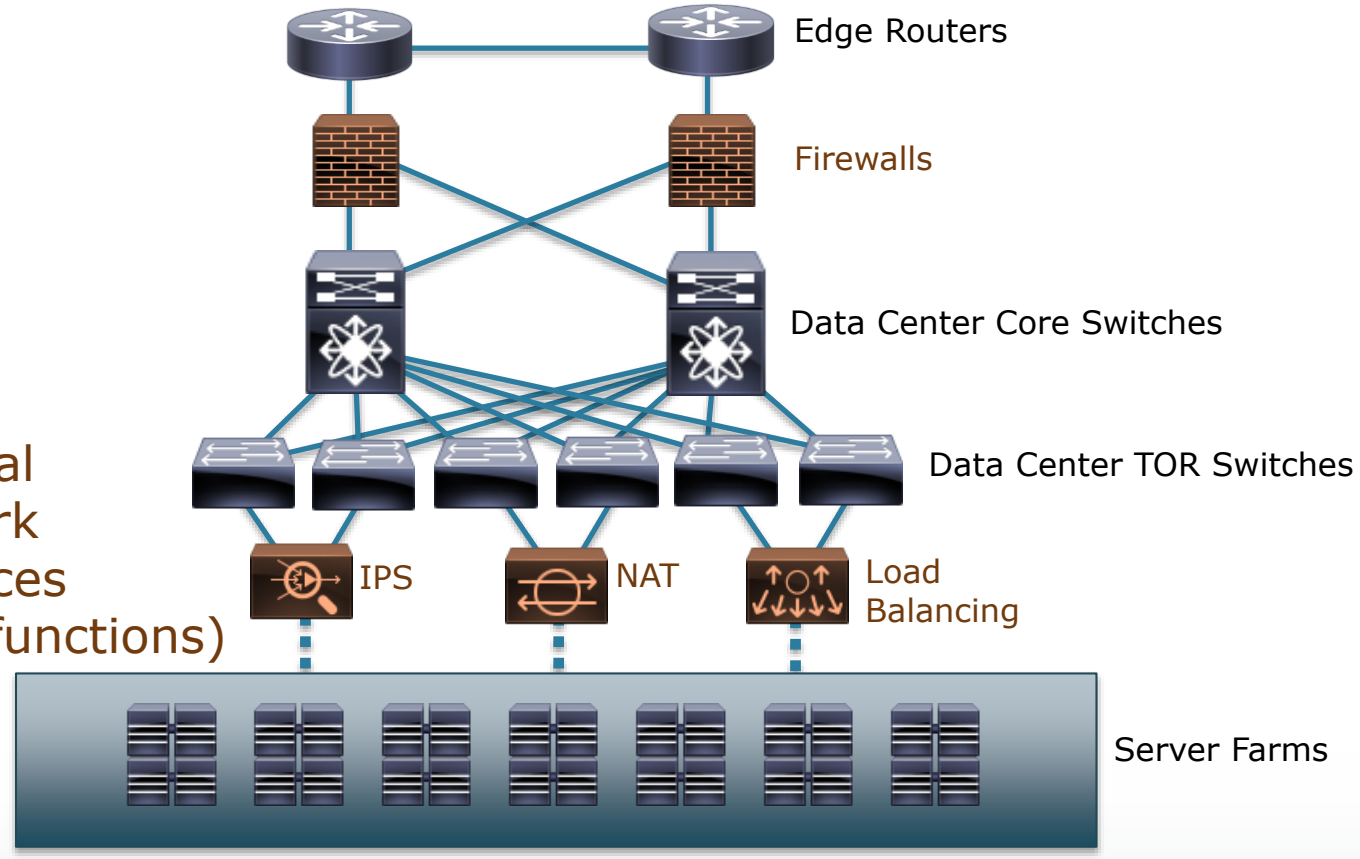



= Data Plane

= Control Plane

# Before NFV (Network Functions Virtualization)

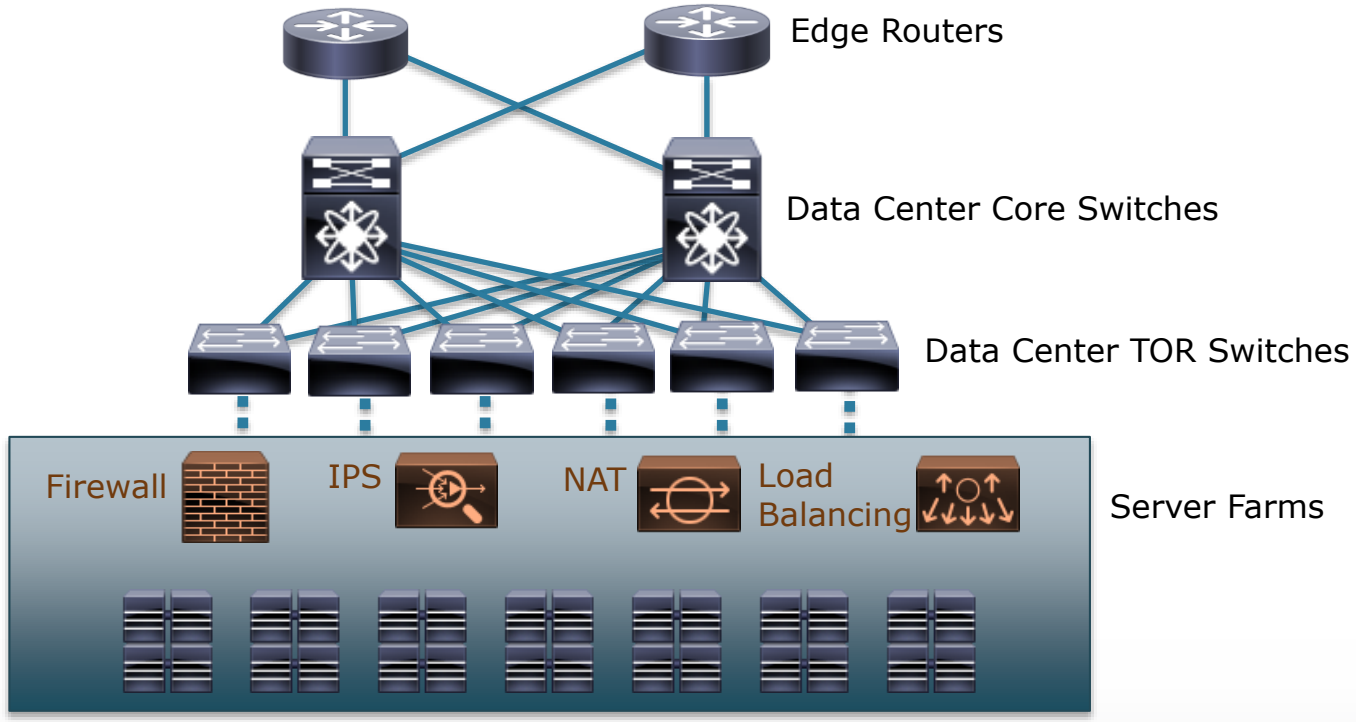
Basic Data Center Topology with physical network appliances




Physical Network Appliances (with specific functions)

# After NFV (Network Functions Virtualization)

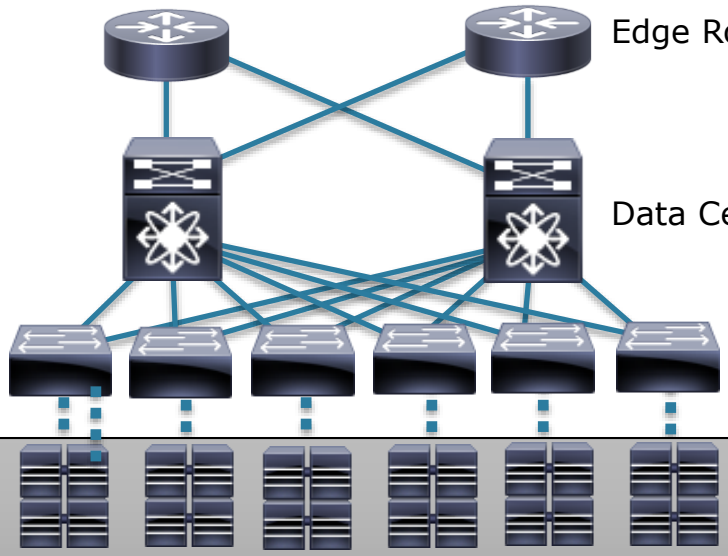
Basic Data Center Topology with virtual network functions (VNFs)




Virtual Network Functions (VNFs)

# After NFV (Network Functions Virtualization)

Virtualized Data Center Topology with virtual network functions (VNFs)



Edge Routers

Data Center Core Switches

Data Center TOR Switches

VNFs deployed as elastic VMs

Server Farms

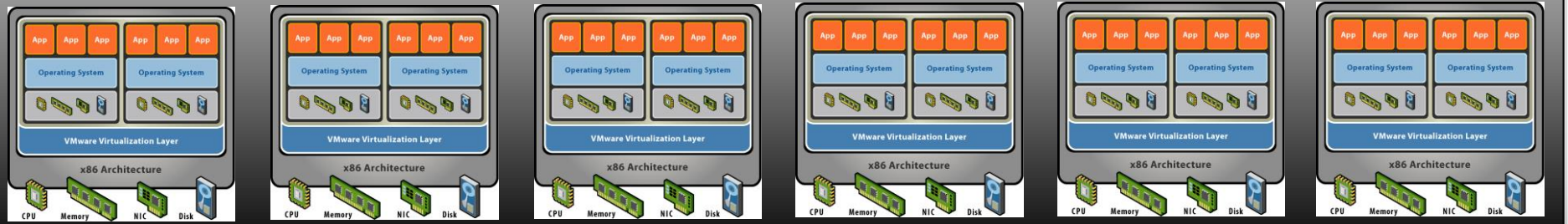
Firewall

Load Balancing

IPS

NAT

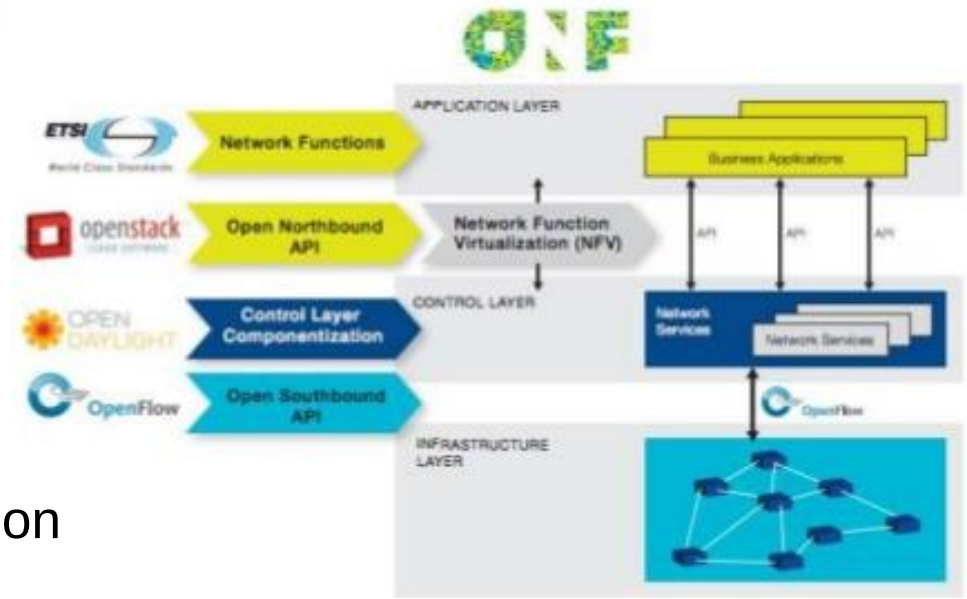
QoS



# SDN + NFV = SDNFV

Together they can:

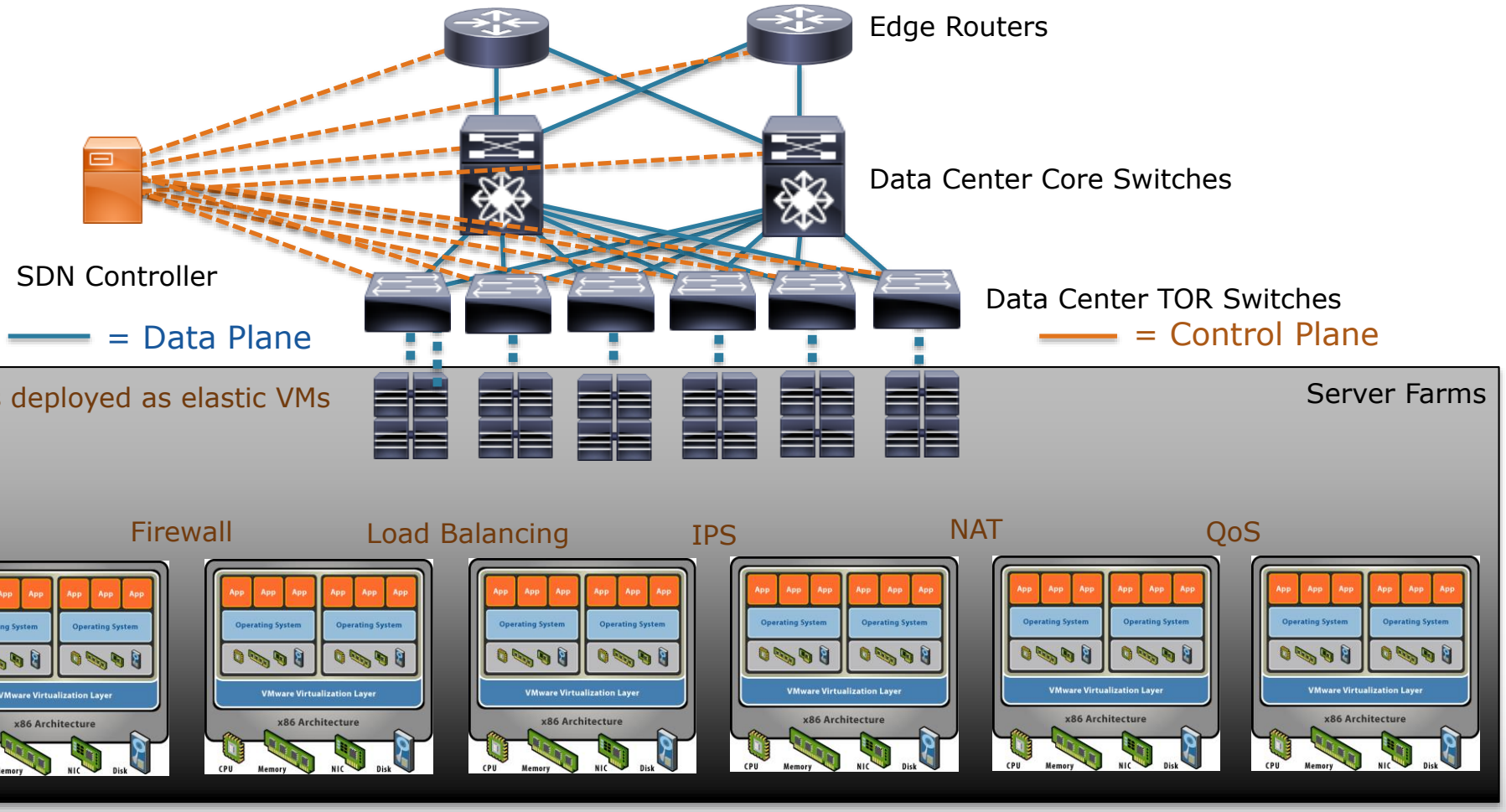
- Simplify configuration of the entire network often comprised of thousands of physical routers and switches from different vendors through the use of a single API
- Simplify operations of the entire network since the network is now reduced to a single switch from an application or a policy control function
- Reduce cost of the network
- Accelerate time-to-market of new services since application-level changes will no longer require hardware-level modifications
- Simplify the process of procurement, design, integration and maintenance of the infrastructure since it is standardized
- Increase agility and scalability by dynamically allocating hardware level capacity to the network functions needed at a specific time




Source: opennetworking.org and etsi.org

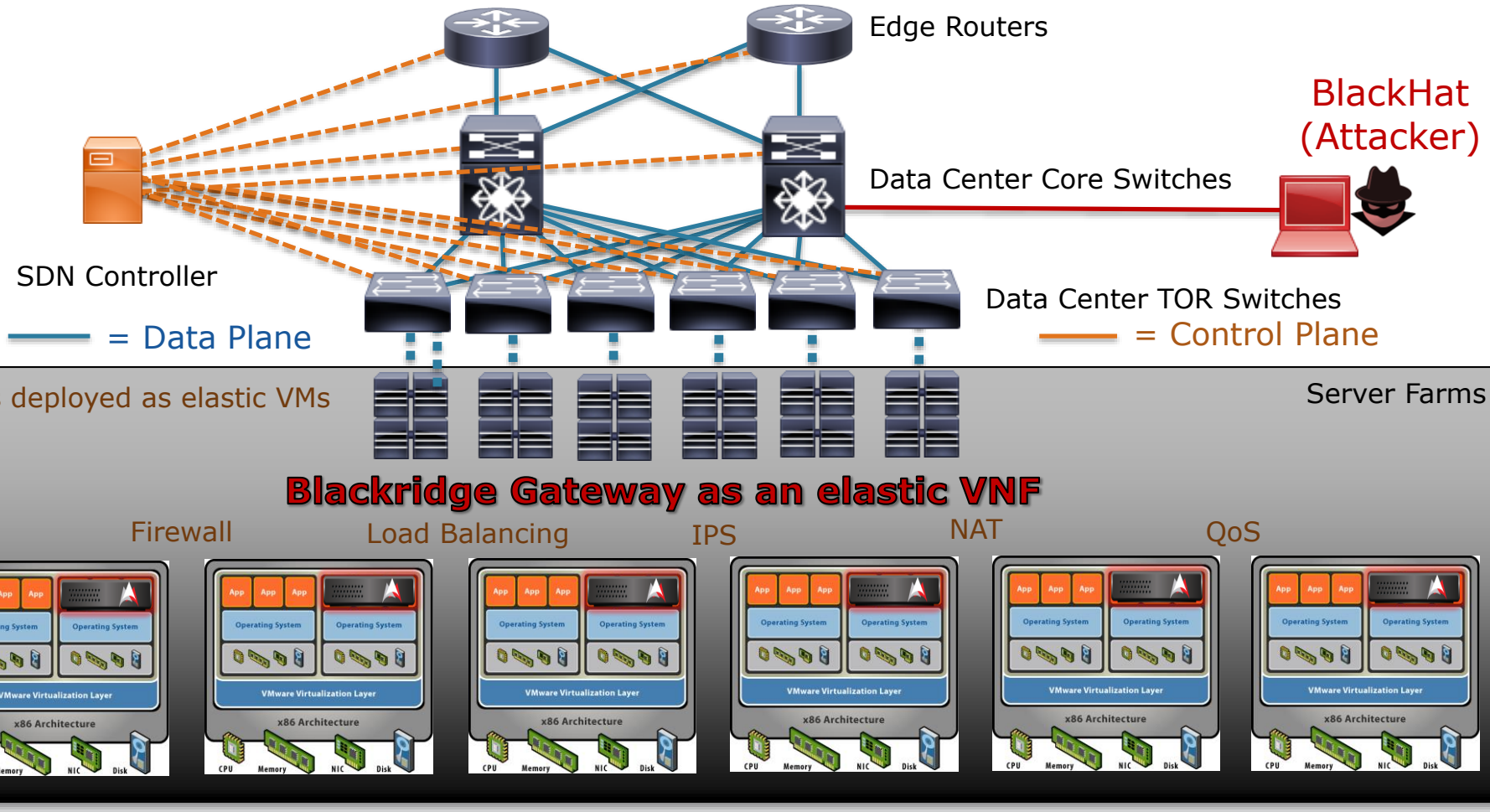
# SDNFV Infrastructure

Virtualized Data Center Topology with virtual network functions (VNFs)



# Protecting the Data Center with Blackridge VNFs

Virtualized Data Center Topology with **Blackridge Virtual Gateway**



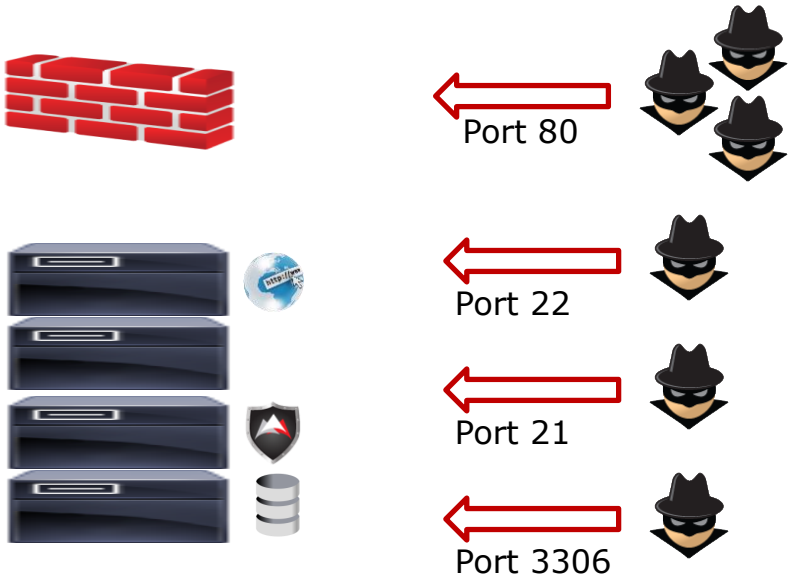
# Leveraging NFV for Security

- By assigning a network function such as a firewall or gateway to a virtual machine an entire functionality can be deployed as needed.
- From a security perspective you can deploy additional VNF's when you are under attack or in an elevated threat risk.
- When the threat is mitigated you can remove the VNF's to reduce performance impacts (compute, storage, bandwidth).

# Leveraging SDN for Security

- An SDN controller can make decisions and execute actions faster than a human.
  - Attacks are happening faster.
  - In some cases assets are compromised, exploited, and then abandoned in a matter of seconds.
- Automates repetitive (mundane) tasks.
  - Creating firewall rules for a dynamic blacklist.
- Eliminates human error.
  - Incorrect firewall rules, network configurations, policy definitions can allow the bad guys to do more than you want

# Let's Look at An Attack




**Security Countermeasures**

1) Block TCP 80 from attacking IP Addresses (blacklist).
2) Block TCP 22 from outside world.
3) Deploy BlackRidge VNF to restrict SSH (TCP 22) connections to authenticated users.
4) Block TCP/UDP 21 connections from outside world. Block internal unauthenticated connections via BlackRidge VNF.
5) Drop any connection to database server unless it comes from web server via BlackRidge VNF.

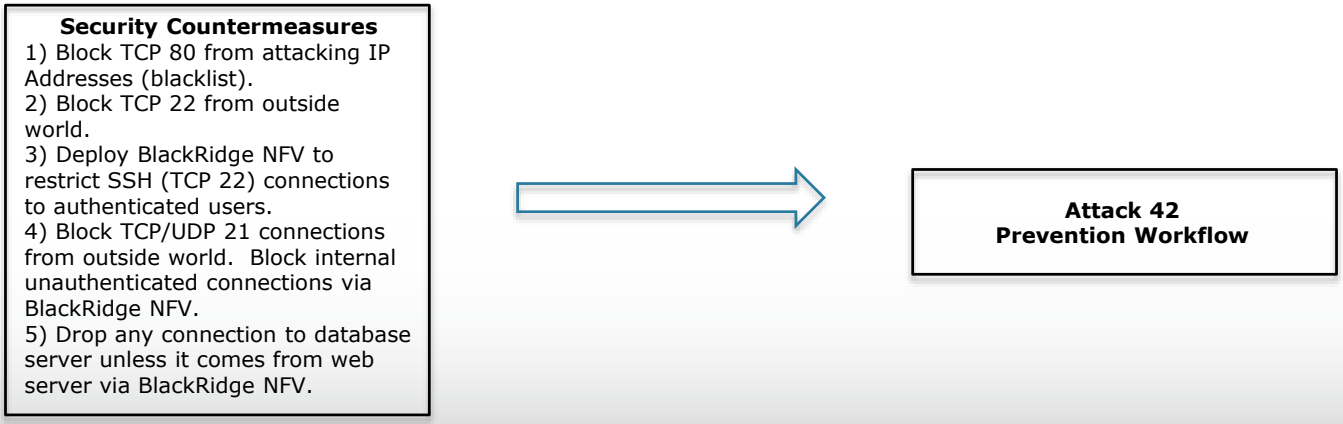
When the attack is over you can undo these countermeasures

…but what if the attack comes back?

# Creating a Repeatable Workflows

- The SDN controller can create a workflow from the countermeasures that helped.

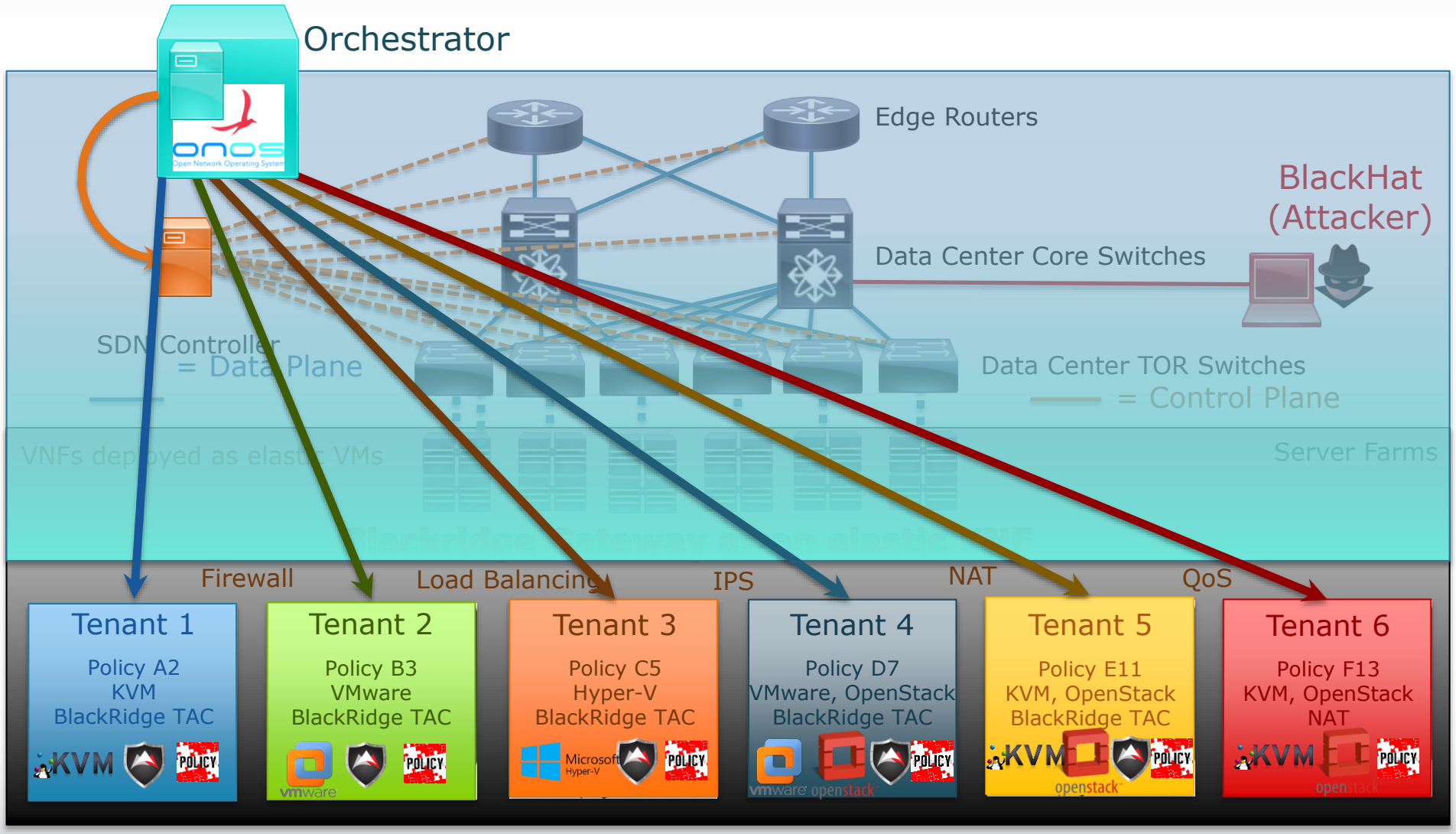
- The workflow can be implemented again when needed by a single action.



# Creating a Signature for the Future

- Signatures are commonly used by antivirus tools and intrusion detection/prevention systems.
- The SDN controller can create a signature for each attack it encounters.
- When a signature is recognized the appropriate workflow can be implemented thereby reducing your vulnerability window.

# Orchestrating Proactive Security Provisioning with BlackRidge



# Live Research Results:
# You Can't Attack What You Can't See

http://longtail.it.marist.edu/honey/statistics_all.shtml

## Firewall IPS Protection

| Time Frame | Number of Days | Total SSH attempts | Average Per Day | Std. Dev. |
|---|---|---|---|---|
| erhp So Far Today | 1 | 3 | N/A | N/A |
| erhp This Month | 8 | 56 | 7.00 | 10.21 |
| erhp Last Month | 31 | 4,237 | 136.68 | 413.12 |
| erhp This Year | 208 | 20,055 | 96.42 | 410.36 |
| erhp Since Logging Started | 208 | 20,055 | 96.42 | 410.36 |
| erhp Normalized Since Logging Started | | | 0.00 | 0.00 |
| erhp2 Educational Site, Protected By a Juniper SRX 3600 | | | | |
| Time Frame | Number of Days | Total SSH attempts | Average Per Day | Std. Dev. |
| erhp2 So Far Today | 1 | 42 | N/A | N/A |
| erhp2 This Month | 8 | 36 | 4.50 | 6.40 |
| erhp2 Last Month | 31 | 343 | 11.06 | 15.20 |
| erhp2 This Year | 176 | 4,338 | 24.65 | 81.05 |
| erhp2 Since Logging Started | 176 | 4,338 | 24.65 | 81.05 |
| erhp2 Normalized Since Logging Started | | | 0.00 | 0.00 |

**Firewall/IPS allows large number of port connection attempts and information to leak.**

## BlackRidge Protection

| Hosts protected by BlackRidge Technologies | | | | |
|---|---|---|---|---|
| blackridge Educational Site, Protected By a BlackRidge Technology Eclips | | | | |
| Time Frame | Number of Days | Total SSH attempts | Average Per Day | Std. Dev. |
| blackridge So Far Today | 1 | 0 | N/A | N/A |
| blackridge This Month | 8 | 0 | 0.00 | 0.00 |
| blackridge Last Month | 31 | 0 | 0.00 | 0.00 |
| blackridge This Year | 121 | 0 | 0.00 | 0.00 |
| blackridge Since Logging Started | 121 | 0 | 0.00 | 0.00 |
| blackridge Normalized Since Logging Started | | | 0.00 | 0.00 |

**BlackRidge does not allow any unauthorized connection attempts or scans (information leakage) to occur.**

Longtail was developed by Eric Wedaa at Marist College

# Questions?

June 13, 2016

# Securing Cloud Environments Using Identity-Based VNFs

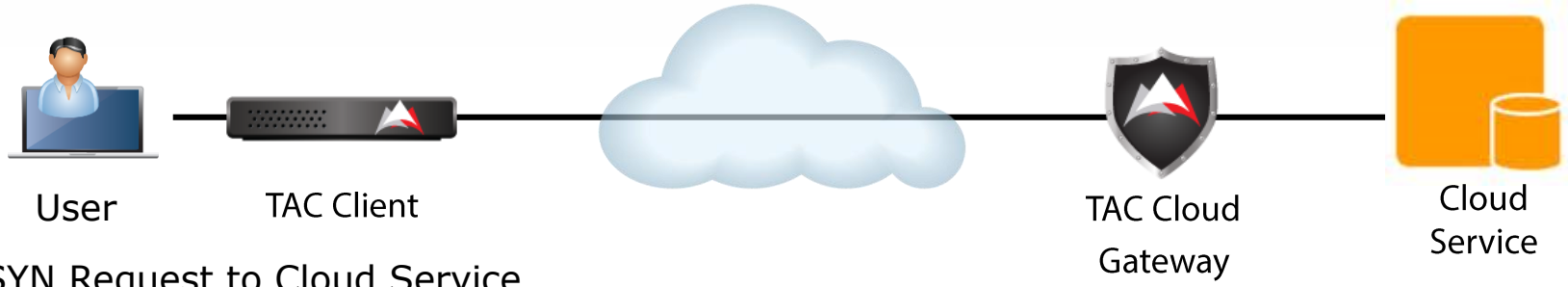
Robert M. Cannistra
robert.cannistra@marist.edu

Doug Johnson
dj@blackridge.us

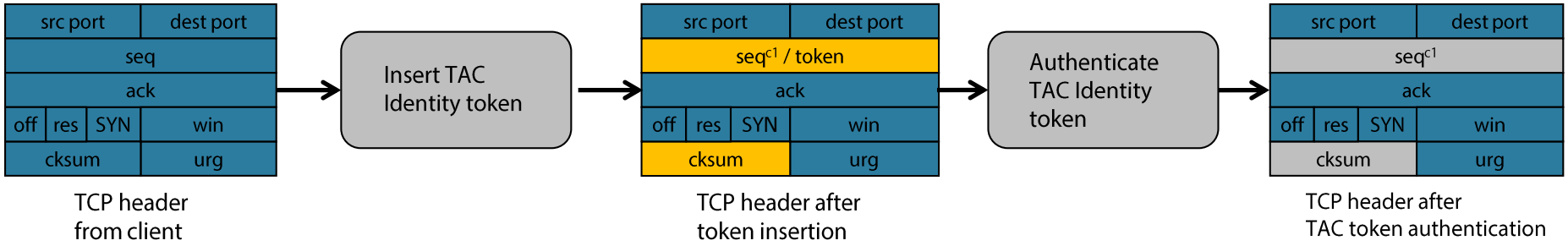
MARIST

BlackRidge TECHNOLOGY

# First Packet Token Insertion and Authentication




## TCP-SYN Request to Cloud Service




## TCP-SYN/ACK Response from Cloud Service