Cloud Networking and Security Workshop Intro

The Case for Avoiding Your Legacy Network in Your Cloud Adoption Strategy

John Bailey
Asst. Director, Cloud Computing
Washington University in St. Louis
jwbailey@wustl.edu

Washington University in St. Louis
Information Technology

2022 Internet2 Tech Exchange

Agenda

- Introduction and level setting – John Bailey (WashU)
- 1st cloud native networking example – Kevin Murakoshi (AWS)
- 2nd cloud native networking example – Kristy Patullo (Google)
- 3rd cloud native networking example – Ken Hoover (Microsoft)
- Break
- Panel discussion & Q&A – Panelists: John Bailey (WashU), Kevin Murakoshi (AWS), Kristy Patullo (Google), Ken Hoover (Microsoft)

Level Setting

- Through examples and conversation, we hope to expand the group's knowledge of how and when to consider not using "traditional" private network approaches.
- The vendor engineers are not here for a vendor feature comparison deathmatch; they are here to collaborate with us to help enhance our understanding of these networking and security concepts.
- We understand and acknowledge that there are some workloads and use cases that will still require traditional private networking.

Proposing a New Approach

Current:

- Network first.
- Network perimeter.
- IaaS First, PaaS Second.
- Apply encryption at the network layer to ensure all traffic is private.
- Use VPN / Direct Connect.

Proposed Future:

- Cloud native first.
- Identity perimeter with MFA.
- PaaS first, IaaS second.
- Adopt technologies that provide encryption at the app/platform layer.
- Use the Internet!

Benefits of Avoiding Cloud Networking

- Faster rollout / adoption of cloud services.
- Increased simplicity and supportability.
- Better security.*
  - *If services are configured properly.
  - Forces your infrastructure teams to learn cloud security because the “edge firewall” protection isn’t there.

Example Architecture: CMMC Enclave