KPMG

Cloud Security Architecture

Travis Quinn

—

9 Oct 23

Scope

01 Background

02 Network & Infrastructure

03 Identity

04 Data

05 Hybrid Cloud

06 Multi-Cloud

07 Future Challenges

08 Training Pathways

Background

Who Am I?

Professional

- Associate Director with KPMG cyber
- Specialise in security architecture, security engineering & GRC
- Previous time in:
  - Trustwave
  - Australian Army

Academic

- PhD candidate, UNSW Canberra, School of Computers & Systems
- Casual Lecturer (Cyber Security), UNSW Sydney, School of Professional Studies

Why Cloud?

Cloud Computing Trends

- Cloud computing spend exceeded $600B (USD) in 2023
- ~95% of medium to large enterprises use cloud computing or services

Market (Public Cloud)

- Largest* cloud service providers (CSPs):
  1. Amazon AWS (32%)
  2. Microsoft Azure (22%)
  3. Google GCP (11%)
  4. Others (35% - all <5% individually)

(*Largest cloud infrastructure provider)

Cloud Security

Importance

- Potential high **risk** operating model for ICT
- Greatest **exposure** for enterprises & individuals
- Can be expensive – expectation of inherent security

Pillars of Cloud Security

- Microsoft identifies several **pillars of cloud security**
- Today, we'll talk about **three essential** pillars:
  1. Network & infrastructure
  2. Identity
  3. Data
- We'll also talk about **hybrid cloud** & **multi-cloud** architectures (because they're challenging!)


Network & Infrastructure

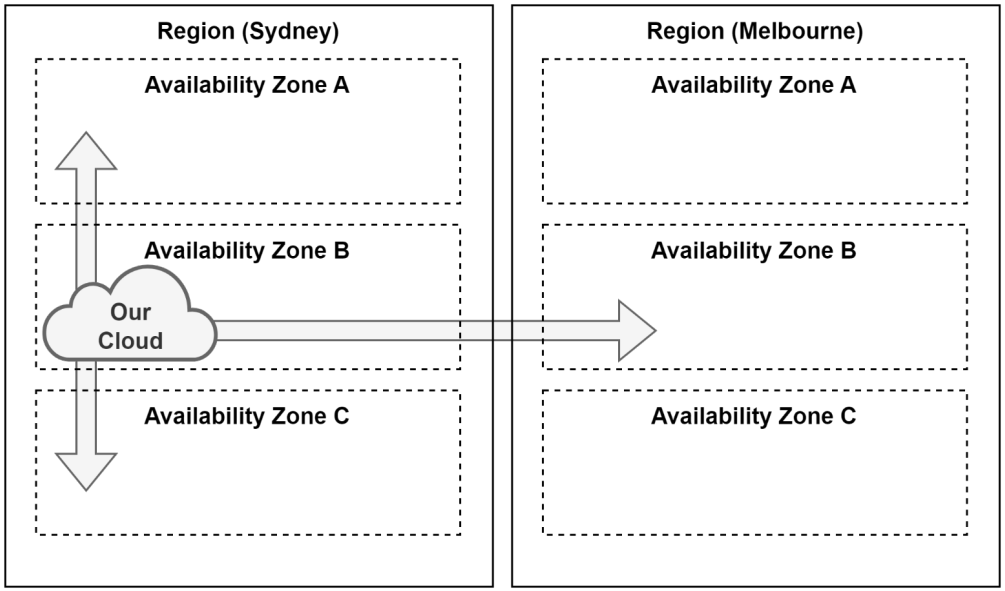
Cloud Infrastructure

Cloud Infrastructure Deployments

- **Private** – your own cloud
- **Public** – shared, usually commercial (e.g., AWS)
- **Hybrid** – some combination of private & public

Security Considerations

- Confidentiality & Integrity
  - Internet exposure
  - Threats & control requirements
  - Data (storage, provenance, privacy)
- Availability
  - Secure access
  - Reliability & performance .vs. cost



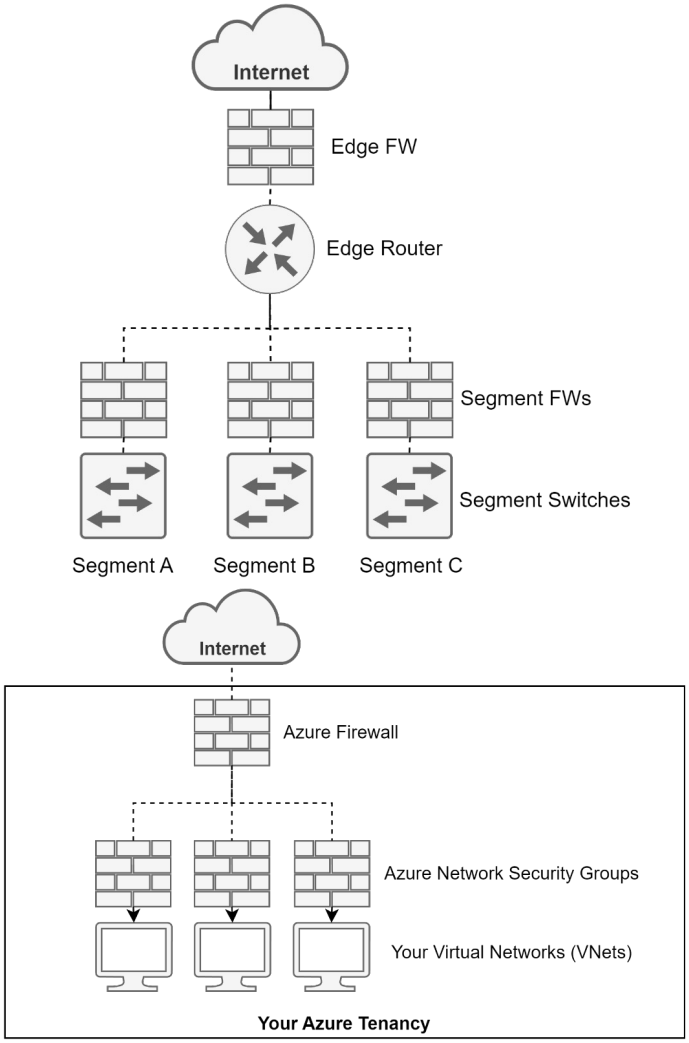
Cloud Networks

Cloud Network Security

- Our **objectives**:
  - Prevent access by malicious actors
  - Limit access of legitimate users (to *where* & *what* they need)
  - Limit impact of incidents

Methods

- **Proactive**
  - Segmentation & microsegmentation
  - Redundancy (limit single-points-of-failure)
  - DMZ & CDS
- **Reactive**
  - Firewall (stateless, stateful & next gen)
  - Intrusion detection/prevention
  - Monitoring & auditing (detective)



Identity

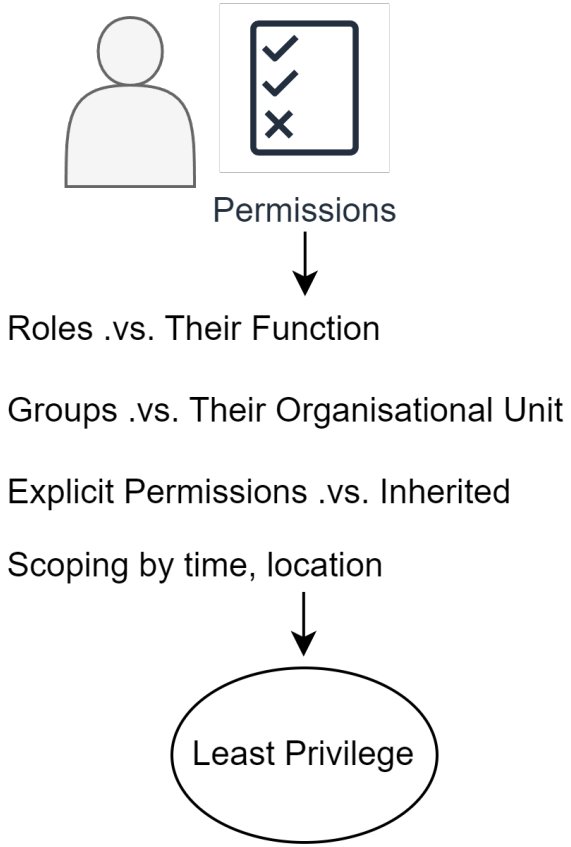
Identity Basics

Identity is sneakily important…

- Security for your **internal** workforce (IAM)
- Security for **externals** – customers & business partners (CIAM/B2B)
- Mechanisms for secure & moderated **access**
  - Protects our **environments** (networks, systems, etc.)
  - Protects our **assets** (resources) & data
  - Protects against malicious & non-malicious misuse

Identity is not just people

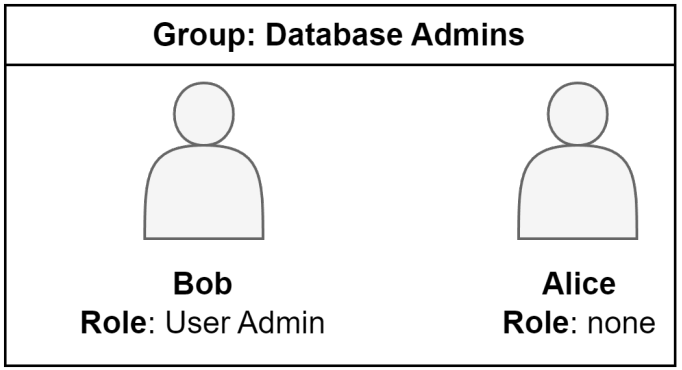
- Principal == any identity (e.g., admin, user, service)
- Service principals (e.g., a custom app) (aka service *account*)
- Devices (e.g., your laptop, your phone)
- **Why?** – shared security policies, observability, less ‘shadow IT’



Identity Security in the Cloud

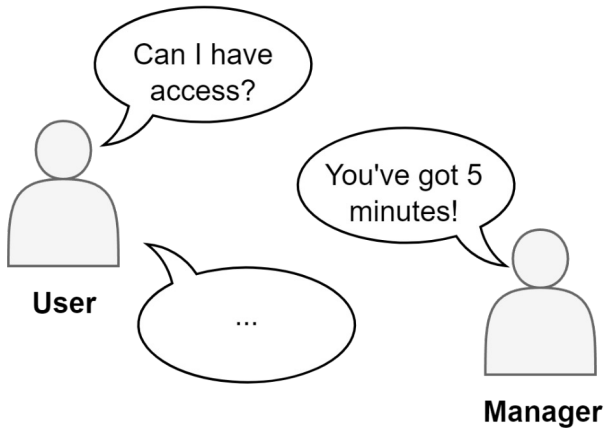
Implementing Identity Security

- Identity sources (internal .vs. external, e.g., IdP)
- Identity directories – where do your identities live?
- Granting permissions - to user, to a role, to a group, on demand



Challenges

- Insecure identities are a **major security risk**
- **Threats** include**:**
  - Privilege escalation
  - Malicious or inadvertent misuse
- **Time-bounding** - limiting access by *time*
  - Just-in-time (JIT) administration
- (Logical) **scoping** – limiting access by *location* or *resource*
  - Just-enough-access (JEA)



Data

Data

Data Problems

- **Storage**
  - Location (cloud-only .vs. hybrid)
  - Centralisation .vs. Decentralisation
  - Encryption (at rest & in transit, inspection)
- **Provenance**
  - Audit (access, actions)
  - Non-repudiation
- **Privacy**
  - e.g., confidentiality, anonymisation, tokenisation
- **Availability**
  - Replication
- **Compliance**
  - Regulations (e.g., *Archives Act*)
  - Archive

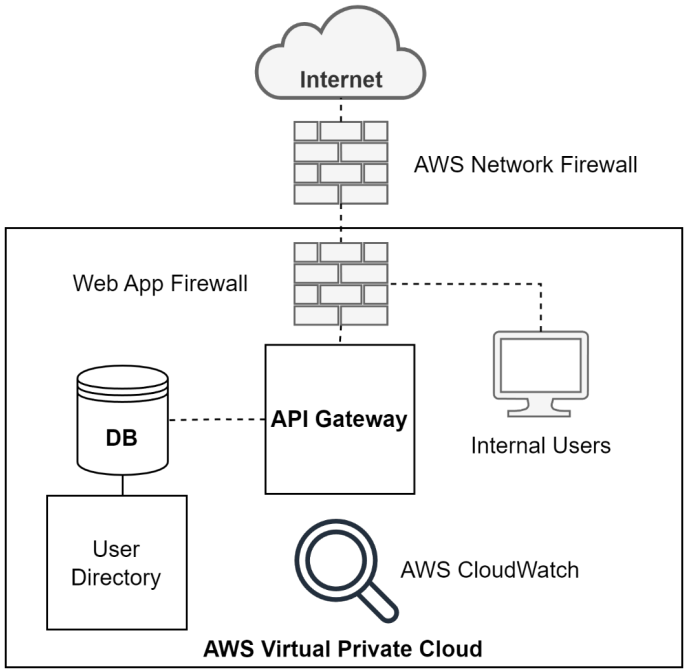
Databases

Database Security

- Security of the **database management system (DBMS)**
  - Network security
  - Access control (authentication + authorisation + conditionality)

- Security of the **database(s)**
  - Network security
  - Access control (authentication + authorisation + conditionality)
  - APIs

- Security of the **data**
  - Encryption
  - Backups & archive
  - Rollback

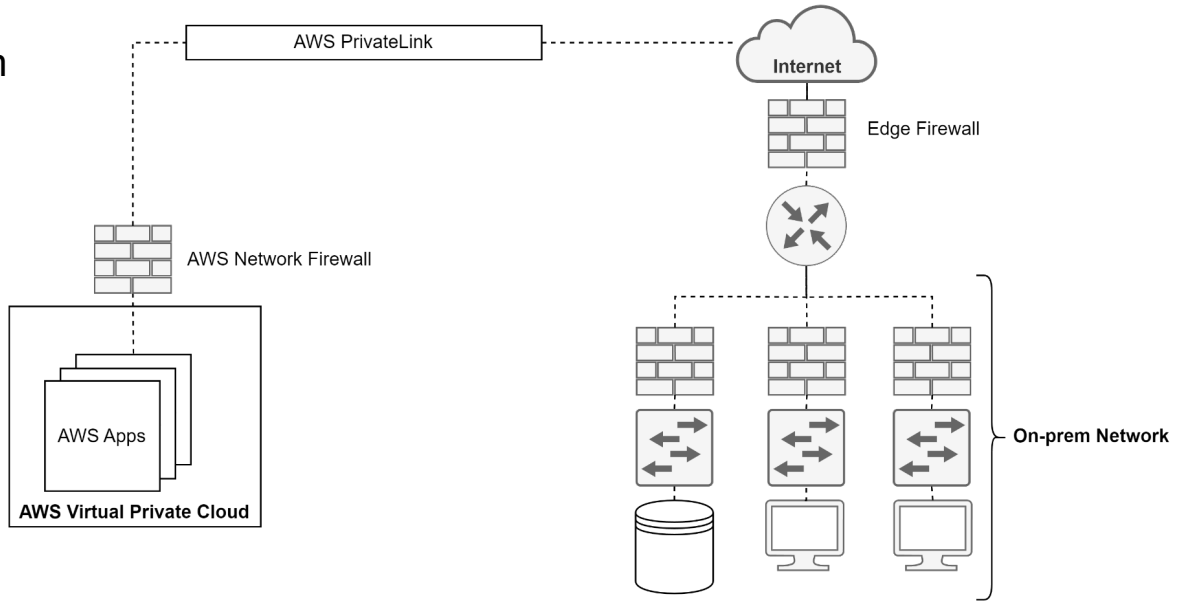



Hybrid Cloud

Hybrid Cloud

What is it?

- Enterprise working in cloud + on-prem
- Cloud is private or public



Security Challenges

- Data security
- Link security
- Monitoring (cross-site, audit)

Solutions

- High risk workloads on-prem
- Sensitive data on-prem
- Sync or federate identities
- Take advantage of cloud functionality & productivity (e.g., SaaS apps)


Multi-Cloud

Multi-Cloud

What is it?

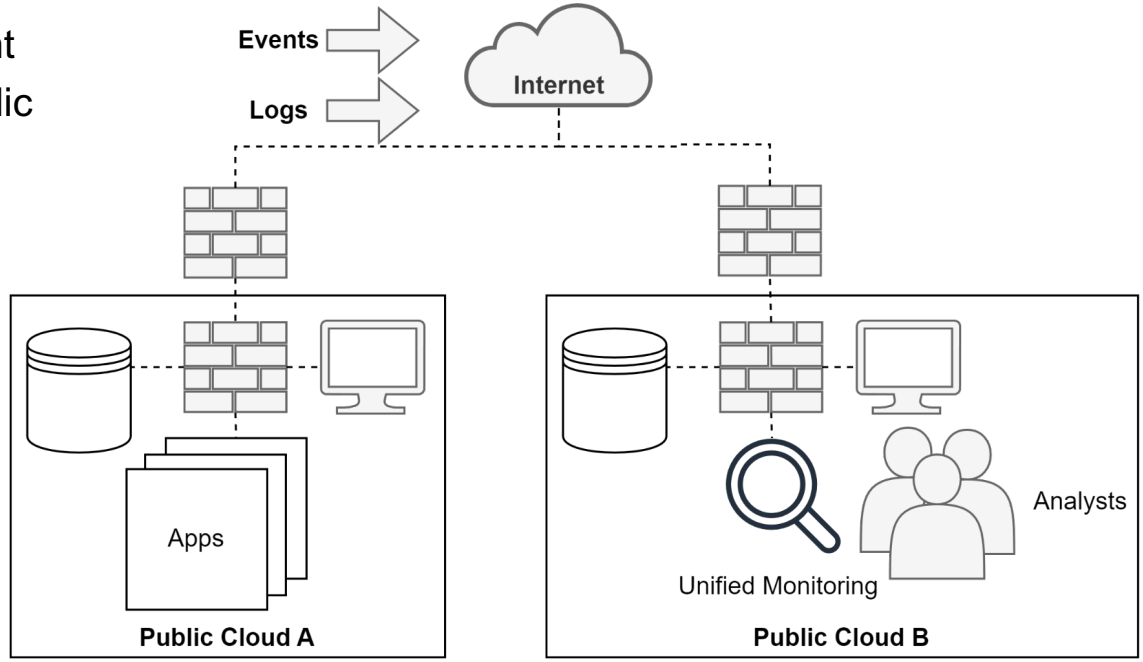
- Using **more than one** cloud environment
- **Examples**: Azure + AWS, Private + Public

Security Challenges

- Decentralisation
- Poor visibility of environments & threats
- Config drift / shadow IT
- Heterogeneous identity

Solutions

- Centralised monitoring (e.g., SIEM)
- Sync or federate identities



Future Challenges

Future Challenges

Supply Chain

- Need for secure development practices
- Incorporating security into the SDLC – in a *meaningful* way

Secure Access & Access Brokership

- Increased rates of WFH
- Secure remote access for employees
- Use of cloud access security brokers (where appropriate)

Data

- Protecting data *regardless* of where it is
- Data leaks

Intelligent Monitoring & Analysis

- Too many alerts + not enough analysts
- Support via automation & analytical support

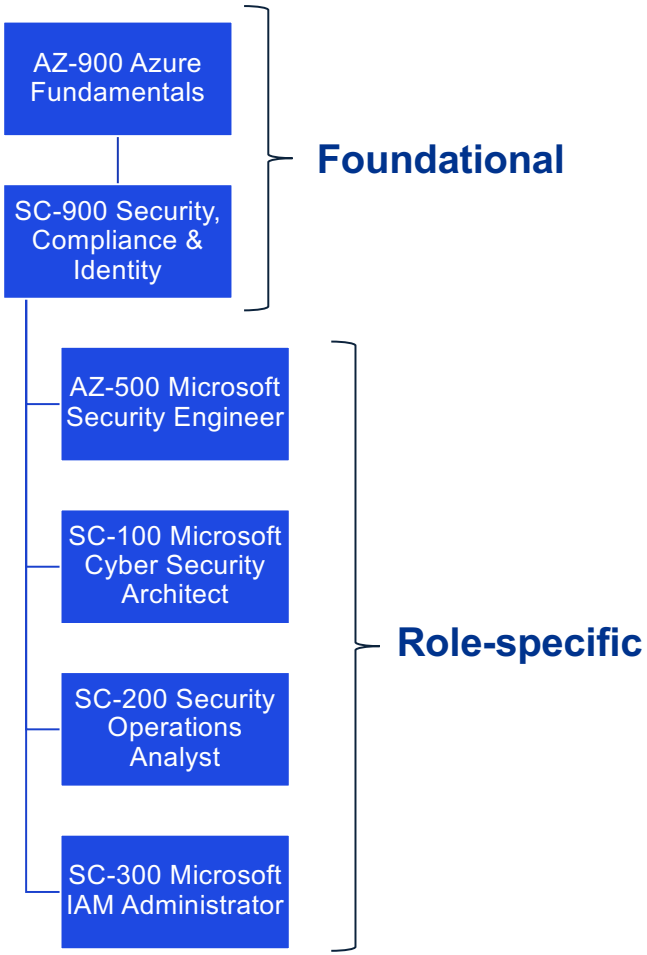

Training Pathways

Training Pathways (AWS)

Security Engineer

Security Architect

Training Pathways (Azure)



Thank you!


KPMG