An Architects Guide to Securing Access to Multi-Clouds

Mark Ryan, Principal ZPA Solution Architect, Zscaler

Thomas Quinlan, Solutions Architect, Zscaler
Agenda

• Legacy Application Access Model
• Infrastructure as a Service Model
• Global Architecture
• Connectivity Challenges
• Zero Trust Network Access
• Security and Control
• DevSecOps Model
• Map to Zscaler Private Access. Same Application – DC, Azure, AWS
• Demonstration of MultiCloud Application Access
Application Access

1. Users on Network
2. Access DNS and LoadBalancer
3. Connectivity To Web/App
4. Database read/write

- Private DNS
- Active Directory
- User
- LoadBalancer
- Webservers
- Application Servers
- Database
- Connectivity to Web/App
- Read/write to Database
Gartner Says:

Network and network security architectures were designed for an era that is waning, and they are unable to effectively serve the dynamic secure access requirements of digital business. The enterprise data center is no longer the center of access requirements for users and devices. Digital business transformation efforts, the adoption of SaaS and other cloud-based services, and emerging edge computing platforms have turned the enterprise network “inside out,” inverting historical patterns.
Infrastructure-As-A-Service
Connectivity to IAAS

ExpressRoute to Azure
DirectConnect to AWS
Cloud Interconnect to GCP
Site to Cloud VPN from Remote Offices
Backhaul Remote User via VPN

You’ve moved to cloud. Why use Legacy network connectivity to deliver applications to users?

Private Link for replication is not ideal for user access

Additional latency from site-to-site tunnel provides poor user experience
Connectivity to IAAS

Virtual private network (VPN) access

- Global Load Balancing
- DDoS
- External Firewall / IPS
- VPN Concentrator
- Internal Firewall
- Internal Load Balancer

VPN software is **not** designed for public cloud access

**Additional** latency from site-to-site tunnel provides poor user experience
ZPA Connectivity to Multi-Cloud

ZPA Connector in Azure

ZPA Connector in AWS

ZPA Connector in GCP

ZPA Connector in Physical DC

Users in HQ and Branches may also use ZPA

Remote Users connect through ZTNA Broker to Apps in AWS/Azure/AWS/DC
Zscaler Private Access is a **ZTNA implementation** where...

1. **Application access is decoupled from network access**
2. **Inside-out connections ensure private apps are invisible**
3. **Multi-cloud application access does not require complex connectivity**
4. **Migration of applications is transparent to user access and experience**
DevSecOps & CARTA

- Infrastructure as code, scalability & availability
- Advertising applications through ZPA as part of DevOps
- Monitor application access through log streaming
- CARTA - Continuous Adaptive Risk and Trust Assessment (Gartner)
  - Zero Trust is an initial step
  - Establish Trust based on context
  - Continuously re-assess trust

Futures - Using APIs to adjust policy and control

- Least Privilege Access
- Deploy Connectors in new regions
Demonstration

- Zscaler App User Accesses Apache Application
- Move Apache from DC to AWS
- Application still available to user
- Shut down Zscaler App – Applications not available
- What about Browser Based?
Please share your feedback on this session!

Four easy steps:

2. Select Session Ratings
3. Choose this session from the list
4. Provide your feedback
Into the clouds!

Thank You!