Lessons Learned
Ensuring a Successful ZPA Deployment

Darren Miller, Principal Network Engineer, IG Group
Ian Perry, SE, Zscaler
Darren Miller
Principal Network Engineer IG Group

- Over 35 years technology infrastructure and security experience
- Leading “cloud first” technology strategy for TPG

Ian Perry
SE
Zscaler

- Assists customers in adopting Zscaler across EMEA
- Over 20 years of Network, Applications and System Architecture
Getting to Zero Trust Network Access
Zero trust doesn’t happen overnight

**Crawl** – Provide identical access to what users have today

**Walk** – Restrict access to critical applications

**Run** – Identify more applications, classify and build policy

**Fly** – Build identity and access controls into development lifecycle
Becoming comfortable with ZPA

• Application Discovery
  • Just-In-Time application access
  • Shortest-path to access

• Discovered Applications
  • Where and how are they accessed
  • Active Directory complexity
  • Domain Suffixes & Search Domains

• Troubleshoot application access
  • FQDN vs short-name vs IP Address
  • Application payload

• Application Connectivity
  • Connector Firewall Rules / ACLs
  • Routing / Access
  • Source IP / Application ACLs

There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns - the ones we don't know we don't know.

— Donald Rumsfeld —
Understanding the ZPA architecture

- Connectors Deployed
  - AWS
  - Azure
  - Google
  - Physical Datacenters
- ZAPP Deployed
- BBA Accessible
- Applications Discovered Wildcards
  - Shortnames + Domain Suffixes
  - IP Addresses for specific apps
- Log Streaming Connected to SIEM
  - Long term logging & diagnostics
Four Pillars of an Initial Deployment

1. **Identity**
   - Key to ZTNA
   - SAML for Users
   - Multi-Factor
     - User
     - Device
   - Consider attributes
   - Extend later

2. **Access**
   - Browser or ZAPP?
   - BBA for HTTP/HTTPS
   - BBA for Partners
   - ZAPP for everything else
   - Server to Client not supported

3. **Connectivity**
   - Plan Connectors
   - By Applications
   - By Gateways
   - In IAAS
   - Failover / Scalability

4. **Applications**
   - Wildcard Domains
   - All Ports
   - Avoid IP Addresses
   - Avoid UDP/53!
   - Bypasses for Internet
Keep it simple

Simple Discovery

Wildcard Discovery Domain
Keep it simple

Simple Discovery

Wildcard Discovery Domain

DNS Search Suffixes
Keep it simple

Simple Discovery

- Wildcard Discovery Domain
- DNS Search Suffixes
- Single Server Group
Keep it simple

Simple Discovery

- Wildcard Discovery Domain
- DNS Search Suffixes
- Single Server Group
- Connector Groups by Location
Keep it simple

Simple Discovery

- Wildcard Discovery Domain
- DNS Search Suffixes
- Single Server Group
- Connector Groups by Location
- Global Allow Policy
Becoming comfortable with ZPA

- Errors aren’t a problem that needs to be solved
- Errors provide detail of application access and functionality
- Policy can be changed or accepted
Troubleshooting

**How?**
- ZAPP Logs
- UI/LSA Logs
- Packet Captures
  - ZAPP
  - Connector
- Client & Connector
  - DNS
  - NetCat/Telnet

**Output**
- DNS resolution
- Is ZAPP Intercepting?
- Are Suffixes being appended?
- Connector Selection
- Connection Payload

**Results**
- Changes
  - Application Segments
  - Policy
  - DNS Suffixes
  - Connector Groups
  - Server Groups
  - Policy
  - Application Access
Granular Policy

Building out your policy

Keep wildcard discovery in place
Do not define “Active Directory” as all the Domain Controllers and ports

Define Application Segments
- Apply policy on the Segment Groups.
- Apply policy on SAML Attributes, Client, and Posture.
- After the “Allow” rules, create a “Deny” rule to block all other access to the applications

PRO TIP: Implied default deny (logged as Policy Not Configured for Access).
DNS Suffix - Segmentation

- DNS is integral part of ZTNA
- DNS is often a global namespace
- Example - Suffix is .company.com
  - Consider .emea.company.com, .us.company.com and .apac.company.com
  - Create 3 application segments
  - Application Segment = Connectors in Region

- What about IAAS?
  - Consider .aws.company.com or .us-west.aws.company.com?
  - Associate *.aws.company.com with only the AWS connectors
  - CNAME the application segments for the real FQDN of the service
Build ZPA into DevSecOps

- Build the ZPA into the development lifecycle
- Consider how applications are deployed – application namespace
- Build connectors to scale, build connectors to fail
  - Connectors should be part of AutoScale groups (even if it’s a group of max 2)
- Log Streaming to SIEM
- Consider least-privilege access – revoke access via policy after periods of no-use
- ZPA-API is being considered (see roadmap sessions)
  - DevSecOps could enable application to be deployed in SAAS
  - API creates Application Segment in ZPA
  - API creates Policy for application
  - Least Privilege access adds/removes users to groups/roles via API in Directory

Zero-trust model
Build ZPA into DevSecOps
• Crawl, Walk, Run – Fly!
• Don’t start with policy - Start with access
• Errors aren’t bad – They’re indicators for policy
• Discover user and application behaviour
• Change user and application behaviour!
• DevSecOps is here – and ZTNA is part of it
Deploying ZPA at IG
Darren Miller - Principal Network Engineer
IG Annual Award Winner

In the category

“Most unsuccessful attempts to deliver a VPN solution”
The Challenge

“I just want to be me wherever I am”

- IG CEO
What does that mean??

- Provide a frictionless experience regardless of location or connection type.
- Ensure security and access is identical in all cases.
IG’s ZPA Deployment

- How many ZPA users today?
- Do they all have Zscaler App deployed, or some have browser access?
- How many different private apps does ZPA secure?
- Where apps are running (on-prem, AWS, Azure etc.)?
- How long did the deployment take?
- Which legacy solutions did you replace?
- Any feedback from users?
Building a user access strategy to address the challenge
8 IG Offices running a ZPA Connector
ZPA Deployment Advice

• Keep it simple
  • Consider using a wildcard to aid discovery.
  • Simple policy, don’t complicate.

• Educate well prior to rollout to limit support calls
  • Captive Portal – Take care to get the settings correct.
  • Ping – You’ll be surprised how many people just try a ping and then log a call.

• Use support
  • Zscaler can help, often we’d try to engineer rather than ask.
  • Don’t be afraid to escalate, keep your Customer Success engaged.
What’s next at IG Group?

- Continuing deployment
- Additional ZPA use cases?
Cheers to flying

Thank You!
In an open forum with Zscaler employees, partners, and customers

Your knowledge and learn from experts in cloud security

The conversation at community.zscaler.com