Zscaler ZIA + ZPA Advanced Deployment
Scope of Work

Summary and Background

This Statement of Work (SOW) defines the scope of a new customer deployment and outlines the roles and responsibilities of both EpicCyber engineers and the customer. It provides implementation guidance for Zscaler Internet Access (ZIA), Zscaler Private Access (ZPA), and Zscaler Digital Experience (ZDX), but only applies if the customer is licensed for these products at the start of the engagement and they are deployed together.

If the customer requires additional Zscaler products not covered in this SOW—such as Airgap, Deception, SD-WAN, or others—or wishes to deploy any of the listed products that were not initially purchased, a separate quote will be required to expand the scope of services.

General Guidelines

- ZIA + ZPA Advanced deployment is limited to 90 days.
- Administrative read/write access to the Zscaler console must be provided by the client if it is not already available to EpicCyber. EC engineers will perform the necessary work via Zoom calls and behind the scenes.
- The client will provide a dedicated resource for this deployment project. The client shall be responsible for timely support of IDP administration and server administration (on-prem, cloud, etc…) for integration of Zscaler products with other vendors.
- EpicCyber records all video meetings for accountability and historical reference.
- Deployment engineers will require a pilot test group of 5-20 users before proceeding with a company-wide deployment, which will be carried out using an MDM solution.
- The client's extended change control process must not hinder the progress of this accelerated deployment.

ZIA In-Scope Build Configurations

- Baseline Template Policy
- Best Practice SSL Inspection Rules
- Client Connector Forwarding or PAC File Options
- IDP Integration (Entra, Okta, etc…)
- URL Filter Rules
- Tunnels
- Pilot Testing
- File Type Rules
- Cloud App DLP for internet file websites (Poor man's DLP)
- Basic Reporting Setup Assistance
- Tenancy Filtering (blocking personal onedrive but allow corporate onedrive)
- Posture Checking
- Adv Cloud Sandbox
- Advanced
- Custom DLP Engines and Policies (both Inline & Cloud API (CASB) DLP)

- SIPA
- NSS Setup (both On-prem and Cloud)
- Advanced DNS and Firewall Rules
- Cloud Browser Isolation
- Private Service Edge
- Smartphone/iPad Setup (managed by MDM)
- Cloud Connector
- Unmanaged DLP + Cloud Browser Isolation

ZPA In-ScopeIDP Integration

- IDP Integration
- Client Connector Forwarding
- Pilot Testing
- SIPA
- Cloud Log Streaming Setup
- Advanced
- Private Service Edge
- Browser Access
- Privilege Remote Access
- App Protection
- Cloud Browser Isolation
- Nano Log Streaming Service (on-prem collector)
- Disaster Recovery / Resiliency

Other Administrative Boundaries and Out-Of-Scope Points

- Please ensure familiarity with the In-Scope Matrix, as it provides a clear reference for identifying out-of-scope items.

- EpicCyber (EC) will provide expertise and strategic guidance on integrating Zscaler solutions while expecting the client to manage and provide expertise for all non-Zscaler technologies within their environment. This includes, but is not limited to:

  -API integrations with third-party security products
  -Configuration of GRE and IPSec tunnels for firewalls without specific Zscaler documentation
  -Identity Proxy configurations that do not have Zscaler-specific guidance

  Exception: EC will take the lead on **Identity Provider (IDP) integration**. During a screen-sharing video conference, EC will guide the client through all necessary steps on the IDP side while managing the Zscaler-side configuration. This process will require the exchange of relevant API keys and files as needed to ensure a seamless integration.

- These links help identify In-Scope FW tunnel configurations.
  https://help.zscaler.com/zia/about-ipsec-vpns#zscaler-interoperability-list
  https://help.zscaler.com/zia/configuring-ipsec-vpn-tunnel
  https://help.zscaler.com/zia/configuring-gre-tunnels

- EC may engage with Zscaler Support by opening tickets on behalf of client users; however, client users will be responsible for direct communication with Zscaler support agents and following up as needed. For any conference calls or support threads involving Zscaler Support, the client is encouraged to keep EC informed and extend invitations as appropriate.

- During an EC deployment, the client's third-party IT contractors are welcome to participate. However, scheduling should prioritize maintaining project timelines, ensuring that coordination with multiple parties does not cause deployment delays.

- For a successful ZPA deployment, EC requires the client to have a comprehensive understanding of their application environment, including URLs, IP addresses, ports, and DNS servers. The client should also be knowledgeable about any firewalls within their environment that may affect communication.

- Identity Proxy configurations beyond the eight Zscaler-documented examples are out of scope. However, EC has experience with select additional use cases and can provide guidance, documentation, and limited assistance for the customer to implement these configurations independently.

- Non-urgent working sessions scheduled outside the standard service delivery hours (Monday through Friday, 6:00 AM PST to 5:00 PM EST, excluding U.S. national holidays) are considered out of scope unless covered by a custom Statement of Work (SOW)

- EC is not a staff augmentation service and does not provide dedicated, named resources. Instead, engagements are managed by our Service Delivery Team, with a designated primary point of contact assigned to ensure continuity throughout the project.

- Service delivery resources are available as scheduled during the kickoff phase and can be accessed through the EpicCyber Customer Portal for working sessions and issue resolution throughout the deployment.

- EC is not a training provider. We recommend that all Zscaler customers take advantage of Zscaler's comprehensive library of on-demand and instructor-led training courses for in-depth learning and skill development.

- EC does not offer emergency incident response services and should not be depended on for after-hours support during security breaches or service outages.