DATA SHEET

Zscaler Professional Services

SIPA (Source IP Anchoring)

Some cloud applications or web services restrict access based on the Source IP address of the traffic but not Zscaler.

Forwarding policies for Source IP Anchoring allows organizations to steer selective traffic processed by ZIA to the internal or external destination servers of their choice. This ensures that Zscaler secures the traffic and that the source IP address is of the organization's choice. The application traffic is forwarded through the intranet to the internal destination servers and through the internet to the external destination servers.

By using forwarding policies for Source IP Anchoring (SIPA), you can control the source IP address of the traffic that is forwarded to destination servers, without bypassing the Zscaler security service. Our Professional Services (PS) Consultant will help you with planning and policy creation to implement SIPA in your environment. This offering is for organizations who want to use ZIA and/or ZPA to selectively forward their application traffic to the appropriate destination servers via the App Connectors of their choice.

Benefits of Professional Services:

- **Valuable Zscaler Experience** Our PS Consultants bring deep architectural and operational experience, bolstered by thousands of implementations, that help you reduce risk and increase project success
- **Bridge Resources and Knowledge Gaps** Access Zscaler's expertise to efficiently fill potential skill or resource gaps, without having to hire additional resources
- **Leading Practice Guidance** Achieve your business objectives quickly by leveraging our years of experience and knowledge of leading practices
- **Accelerate ROI** Feel confident knowing your deployment has been set up for success, by relying on Zscaler's proven project methodology

SIPA		
Professional Services Scope	**SCOPE:** • Up to Two (2) pairs of App Connectors for SIPA, with configuration of up to 10 SIPA Applications **INCLUDED:** • **Review customer requirements to implement the solution for Source IP Anchored traffic using SIPA feature and policies required to implement in the Zscaler tenant** **EXCLUDED:** • Security Policies (Ex: DLP, Sandbox, etc) • ZIA Authentication • Support around Zscaler Client Connector (ZCC) or any Traffic Forwarding method(s) **DELIVERABLES:** • Design Plan • Functional Test Plan	
Credits	22	Redemption of sufficient credits for fulfillment of service offering per unit required
Maximum # of Units recommended	3	The maximum number of units recommended for this offering to be implemented in parallel. For organizations requiring more than stated recommended units, there are alternative SKUs that may better align to your needs
Resource Allocation	One (1) Professional Services Consultant	Assigned to deliver as per scope of deployment offering
Staffing	Resource assignment may take up to 2 weeks	
Duration	Up to 4 weeks; Not to exceed 90 days/3 Months	Upon the start of the project, all efforts should be completed within 4 weeks. In total the project will not exceed 3 months of engagement from Professional Services, based on the service start date
Delivery Method	Remote	Assigned PS Resources will be remote for the duration of the engagement
Non-Technical Prerequisites	The Customer: • Must provide appropriate lead resources to attend technical Kick-off and design sessions on the commencement date • Must provide Zscaler representatives with information and resources to successfully execute the Project. This can include, without limitation, providing access and credentials to systems, completing installation prerequisites, providing project resources, and attendance in planning, execution, or Knowledge Transfer meetings • Will ensure resources are available in a timely manner to undertake tasks such as change control and documentation review • Must ensure it has the necessary escalation and communication channels to resolve any blockers in a timely manner, including dependencies on third-parties and other customer vendors, suppliers, and Consultants	
Technical Prerequisites	• Authentication has been configured on the customer IdP and in the Zscaler Portal for ZIA • Baseline security policies (ZIA) and Traffic Forwarding method(s) are working in production • Zscaler Client Connector (ZCC) has been rolled out to users • Prerequisites for installing SIPA App Connectors, like IP Whitelisting, VMware machine builds are ready.	
Project Constraints	• This Project covers the deployment of only Zscaler licensed solutions. Additional product offerings may be purchased as add-ons, otherwise additional consulting work not contained in this Project is deemed out of scope. • Zscaler is not responsible for the installation, configuration, or validation of any third-party software, tools, or utilities. • Zscaler is not responsible for impacts to schedule caused by customer internal processes	

SIPA	
Project Expectations	• ZIA has been fully deployed and successfully tested • Customer to identify and provide their critical Applications for the SIPA test plan
Project Constraints	• This Project covers the deployment of only Zscaler licensed solutions. Additional product offerings may be purchased as add-ons, otherwise additional consulting work not contained in this Project is deemed out of scope • Zscaler is not responible for third party integration, Ex: SCCM configuration/support to deploy the Zscaler Workload Segmentation Agents • Zscaler is not responsible for impacts to schedule caused by customer internal processes
Terms and Conditions	Zscaler Deployment and Professional Services Terms and Conditions

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com