Local Inspection with ZIA Private Service Edge and ZIA Virtual Service Edge

Reference Architecture

Contents

About Zscaler Reference Architectures Guides

The Zscaler Reference Architecture series delivers best practices based on real-world deployments. The recommendations in this series were developed by Zscaler's transformation experts from across the company.

Each guide steers you through the architecture process and provides technical deep dives into specific platform functionality and integrations.

The Zscaler Reference Architecture series is designed to be modular. Each guide shows you how to configure a different aspect of the platform. You can use only the guides that you need to meet your specific policy goals.

Who Is This Guide For?

The Overview portion of this guide is suitable for all audiences. It provides a brief refresher on the platform features and integrations being covered. A summary of the design follows, along with a consolidated summary of recommendations.

The rest of the document is written with a technical reader in mind, covering detailed information on the recommendations and the architecture process. For configuration steps, we provide links to the appropriate Zscaler Help site articles or configuration steps on integration partner sites.

A Note for Federal Cloud Customers

This series assumes you are a Zscaler public cloud customer. If you are a Federal Cloud user, please check with your Zscaler Account team on feature availability and configuration requirements.

Conventions Used in This Guide

The product name ZIA Service Edge is used as a reference to the following Zscaler products: ZIA Public Service Edge, ZIA Private Service Edge, and ZIA Virtual Service Edge. Any reference to ZIA Service Edge means that the features and functions being discussed are applicable to all three products. Similarly, ZPA Service Edge is used to represent ZPA Public Service Edge and ZPA Private Service Edge where the discussion applies to both products.

Notes call out important information that you need to complete your design and implementation.

⚠ Warnings indicate that a configuration could be risky. Read the warnings carefully and exercise caution before making your configuration changes.

Finding Out More

You can find our guides on the Zscaler website at Reference Architectures (https://www.zscaler.com/resources/reference-architectures).

You can join our user and partner community and get answers to your questions in the Zenith Community (https://community.zscaler.com/).

Terms and Acronyms Used in This Guide

Acronym	Definition
CARP	Common Address Redundancy Protocol
DC	data center
DMZ	demilitarized zone
DNS	Domain Name System
IoT	Internet of Things
IP	Internet Protocol
MAC	media access control
NAT	Network Address Translation
OSI	Open Systems Interconnection
SSL	Secure Sockets Layer (superseded by TLS)
TCP	Transmission Control Protocol
TLS	Transport Layer Security
ZDX	Zscaler Digital Experience
ZIA	Zscaler Internet Access
ZPA	Zscaler Private Access
ZTE	Zero Trust Exchange

Icons Used in This Guide

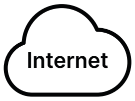
The following icons are used in the diagrams contained in this guide.

Laptop / User

User

ZIA Public Service Edge

Firewall



Internet

Load Balancer

Router

Introduction

Zscaler operates the world's largest security cloud, with over 150 data centers worldwide. Users connect through the nearest Zscaler Internet Access™ (ZIA™) Public Service Edge device to secure their connection to the internet. Users are automatically routed to the nearest Zscaler data center based on their geographic location. When your user authenticates at a ZIA Public Service Edge, your user's policy is automatically downloaded from the Zscaler Central Authority. This multitenant solution provides a seamless and predictable user experience no matter where your users are located or where they travel.

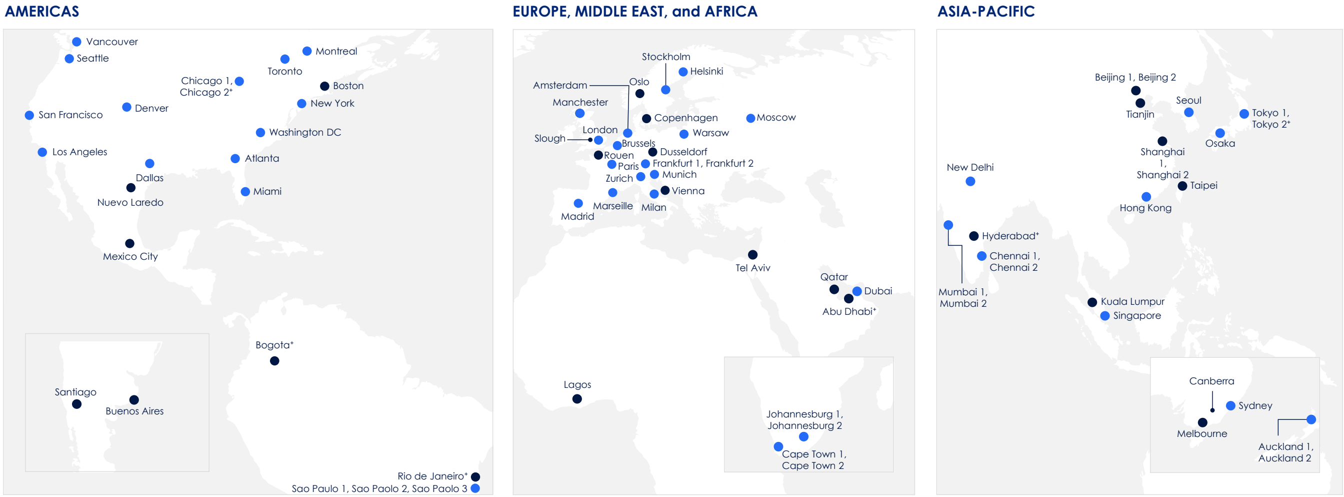


Figure 1: ZIA is delivered through Zscaler-owned data centers around the world

This works for the vast majority of Zscaler users, most of whom only use Zscaler's public clouds. However, there are situations where performing local inspection in your organization's data center is more effective. To accomplish this, Zscaler offers ZIA Private Service Edge and ZIA Virtual Service Edge devices. Unlike a traditional security stack, Zscaler extends the ZIA security cloud into your data center. These fully managed devices are deployed by you and managed by Zscaler.

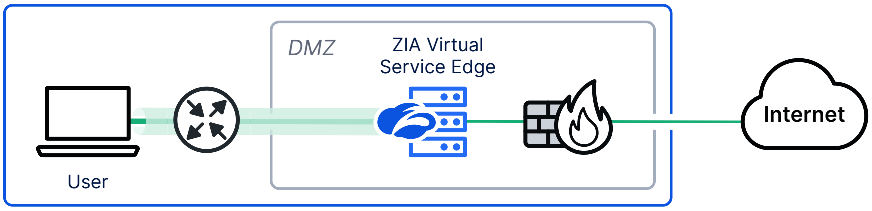


Figure 2: ZIA Private and Virtual Service Edge devices place ZIA inspection in your local networks

When the ZIA Private Service Edge or ZIA Virtual Service Edge is deployed, it becomes a co-managed extension of the ZIA cloud. Zscaler handles all of the ZIA Service Edge software upgrades and management, with your organization managing the underlying operating system (OS) for any virtual system. Your logs continue to be handled by Zscaler's logging infrastructure and appear alongside your existing logs from ZIA Public Service Edge devices.

ZIA Service Edge devices are where Zscaler secure internet and software as a service (SaaS) access happen. ZIA Private Service Edge and ZIA Virtual Service Edge devices extend the ZIA cloud into your organization's data centers and public cloud deployments. Thus, you get all of the same security and inspection benefits of the ZIA public cloud inside your network edge.

ZIA Private or Virtual Service Edge Use Cases

In most cases, Zscaler does not recommend deploying a ZIA Private Service Edge or ZIA Virtual Service Edge, as these additional subscriptions only add value in specific scenarios. The most common use cases for these devices include:

Locations with Geopolitical Requirements and Regulations

In some regions of the world where your organization might operate, the local political environment is such that Zscaler cannot easily deploy ZIA services before user traffic is inspected by the government or local ISPs in that location. In other cases, your traffic might have to leave the country over expensive international links to be inspected, even if the destination is within the same country. You might also want to deploy controls such as Zscaler Data Loss Prevention (DLP) to prevent trade secrets from being sent out and inspected by the local government. In these cases, a ZIA Private or Virtual Service Edge deployed within your network can handle inspection before the traffic is subject to local inspection and enforcement.

Locations with High–Bandwidth Requirements

In some cases, your organization's campus might generate high traffic due to the number of users and high-bandwidth applications they are using. Zscaler considers high bandwidth to be sustained traffic of 1 GB or more continuously from a single location. In these cases, a ZIA Private Service Edge or ZIA Virtual Service Edge gives you a local inspection and enforcement point in your data center for your organization's exclusive use.

Locations That Experience High Latency When Connecting to ZIA Public Service Edges

In many parts of the world, high-speed internet access and backbone infrastructure remain unavailable. These locations often require a long series of hops to reach the nearest ZIA Public Service Edge device. In these cases, local inspection might result in a perceived speed increase, especially when accessing internet resources that are geographically near the user.

Applications That Require an Organization's IP Address as the Source IP Address

In some situations, software licensing or regulatory requirements demand that all traffic originates from the organization's registered IP address and not the IP address of a Zscaler data center. These are often sensitive SaaS applications such as legal document tracking, medical records, or financial services. In these cases, a ZIA Private Service Edge or ZIA Virtual Service Edge allows for user authentication and full inspection before traffic passes to your standard routing procedures for that service or application. This allows all users to be authenticated, and for their traffic to be fully inspected and still originate from your organization's IP address space.

Users Who Need to See Localized Content or Have a Local IP Address

In some markets, a user's traffic must transit a ZIA Private Service Edge in another country with a different local language and addressing. In some instances, this foreign source IP address can prevent users from accessing appropriate resources. For example, some government service websites are restricted to IP addresses that exist within the country itself, preventing viewing for anyone outside its borders.

Additionally, websites and applications might automatically set the language for the user based on IP address instead of system settings. For these users, inspecting and routing locally with a ZIA Private Service Edge or ZIA Virtual Service Edge can improve the internet experience.

Key Features and Benefits

- Provides dedicated high-bandwidth infrastructure for your organization's largest sites.
- Provides the ability to inspect traffic before users leak sensitive information or visit sites that might trigger additional government inspection.
- Provides the ability to anchor your IP address when required by license or regulation.
- Ensures users see localized content and can access local services.

New to ZIA Service Edges?

- If you are new to ZIA, see Secure Internet and SaaS Access (https://www.zscaler.com/products/zscaler-internet-access).
- If you would like more details on the different ZIA Service Edge options, see:
    - About Public Service Edges (https://help.zscaler.com/zia/about-public-service-edges).
    - Understanding Private Service Edge (https://help.zscaler.com/zia/understanding-private-service-edge).
    - About Virtual Service Edges (https://help.zscaler.com/zia/about-virtual-service-edges).
- If you are planning to deploy a ZIA Private or Virtual Service Edge in China, Zscaler recommends Deploying Zscaler Internet Access in China (https://help.zscaler.com/zia/deploying-zscaler-internet-access-china).

Understanding ZIA Private Service Edge and ZIA Virtual Service Edge

Zscaler operates the largest security cloud in the world, with over 150 data centers worldwide. ZIA is a cloud security service providing secure internet and SaaS access for users and workloads within the Zscaler cloud. Traffic inspection is performed by ZIA Public Service Edge devices in Zscaler data centers. You generally don't need to purchase equipment for your users or sites.

In most cases, your organization builds a Generic Routing Encapsulation (GRE) or Internet Protocol Security (IPSec) tunnel between your major sites and the two nearest Zscaler public data centers. All your internet and SaaS traffic for those sites moves across those tunnels to a ZIA Public Service Edge for inspection.

For mobile users or sites where there is only public internet access, the Zscaler Client Connector agent securely connects your users' devices to the nearest ZIA Public Service Edge. This agent is always on and can detect when it's on a trusted network or the general internet. Your ZIA subscription includes Zscaler Client Connector for all your users.

Sometimes, ZIA Public Service Edge or Zscaler Client Connector is not the right choice for the organization. In such cases, it can be advantageous to extend the Zscaler cloud and ZIA services into a location you control. Zscaler offers two products that enable traffic inspection before the traffic exits your controlled network. In both cases, the devices require an additional Zscaler subscription.

- ZIA Private Service Edge – A hardware appliance with the same hardware that Zscaler uses in its public data centers.
- ZIA Virtual Service Edge – A virtual appliance that can run in your private data center or in a public cloud such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP).

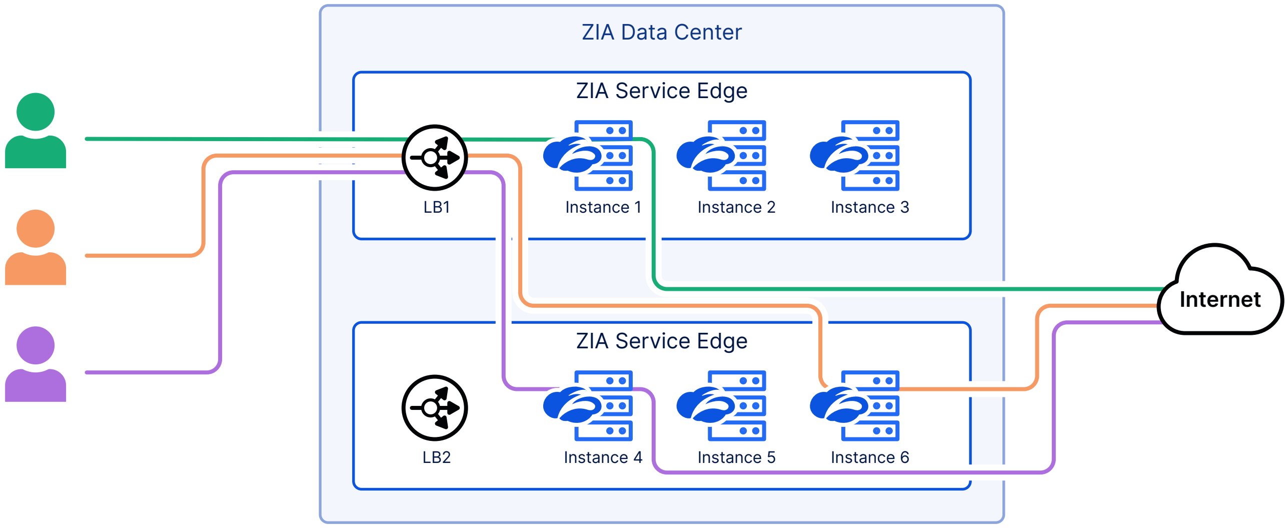


Figure 3: Each instance of a ZIA Private Service Edge or ZIA Virtual Service Edge contains multiple instances of the service

Each ZIA Private Service Edge comprises a virtual load balancer and 3 to 5 ZIA Virtual Service Edge redundant instances, depending on the device scale. The virtual load balancer is responsible for spreading the traffic across the ZIA Service Edge instances, including between multiple instances operating in a clustered location. This is the same model Zscaler employs in its public ZIA data centers. Zscaler recommends deploying two or more instances of either the ZIA Private Service Edge or ZIA Virtual Service Edge for local redundancy.

Choosing Between ZIA Private and Virtual Service Edges

When deciding between a ZIA Private Service Edge and a ZIA Virtual Service Edge, it helps to understand your use case in terms of bandwidth: both overall traffic, and how much traffic is TLS/SSL inspected. This is the primary factor when selecting the correct ZIA Service Edge for your organization. The following table summarizes the benefits and requirements for each platform type.

ZIA Private Service Edge	ZIA Virtual Service Edge
Benefits • Full benefits of the Zscaler cloud. • Good choice for high throughput, especially when the overall uplink throughput traffic is greater than 1 Gbps or download is greater than 2 Gbps total. • Supports remote user traffic. • Includes built-in ability to perform TLS/SSL inspection.	**Benefits** • Full benefits of the Zscaler cloud. • Deploys easily into your existing virtual machine (VM) infrastructure. • Can handle remote user traffic. • Flexible deployment in the demilitarized zone (DMZ), your internal network, or in the public cloud. • Virtual form factor that is horizontally scalable. • Instantly available, with no need to wait for shipping. • No need to use or purchase public IP addresses. • Built-in load balancer.
Requirements • At least two ZIA Private Service Edges are necessary for redundancy. • Zscaler provides hardware and software for ZIA Private Service Edge. • You must install and maintain the devices in your data centers as part of your network. • Zscaler Cloud Operations maintains, upgrades, and monitors the ZIA Private Service Edge in your data center.	**Requirements** • At least two ZIA Virtual Service Edges are necessary for redundancy. • You are responsible for deploying, configuring, and maintaining the host hypervisor OS. • Zscaler Cloud Operations maintains, upgrades, and monitors the ZIA Virtual Service Edge in your data center. • A TLS/SSL acceleration card is recommended for deployments requiring TLS/SSL inspection of 100 Mbps or more on ZIA Virtual Service Edge devices. To learn more, refer to the Marvell website (https://www.marvell.com/products/security-solutions.html).

To learn more about the differences in deployment types, see Choosing Between Private Service Edges and Virtual Service Edges (https://help.zscaler.com/zia/choosing-between-private-service-edge-and-virtual-service-edge).

For more information on TLS/SSL inspection, see TLS/SSL Inspection with Zscaler Internet Access (https://help.zscaler.com/zia/tls-ssl-inspection-zscaler-internet-access).

Software Updates and Shared Responsibility Model

A deployed ZIA Private Service Edge or ZIA Virtual Service Edge uses a shared responsibility model for maintaining the device and software. In this model, you and Zscaler share responsibility for different aspects of the deployment, from software maintenance to traffic routing.

The ZIA Private Service Edge and ZIA Virtual Service Edge are hardened software devices. The Zscaler operations team disables all unnecessary services and closes all unnecessary ports. The host platforms are built on Zscaler's custom UNIX-based OS with the minimum set of packages required for the system to function. The underlying services are also updated regularly.

Vulnerabilities are regularly found in core open-source components such as DNS resolvers to OS kernels, so Zscaler recommends patching your virtual machine hosts as part of your regular maintenance. Also be sure to protect your ZIA Private Service Edge or ZIA Virtual Service Edge using appropriate firewall policies.

Zscaler's operations team is responsible for upgrades of the ZIA Service Edge software. Upgrades occur outside of business hours in your location. Deploying ZIA Private Service Edge and ZIA Virtual Service Edge devices in pairs allows one to be upgraded while the other remains active to service user traffic.

When operating a ZIA Virtual Service Edge device, you are responsible for maintaining and securing the VM host platform. If you host the device with a cloud infrastructure provider, they manage parts of this task for you. If you host the device locally in your DMZ or other location, you must secure and maintain the host platform. In all cases, you should limit access to the host platform.

Learn more about shared responsibilities for ZIA Private Service Edge and ZIA Virtual Service Edge devices at Maintenance Support for Private Service Edge (https://help.zscaler.com/zia/maintenance-support-private-service-edge).

Deployment Locations and Network Firewall Changes

Zscaler's operations team must be able to access your ZIA Private Service Edge or ZIA Virtual Service Edge infrastructure to perform maintenance tasks. With regard to the internet, your firewalls require modification to allow remote access by Zscaler staff and the cloud management platform from Zscaler's known IP addresses. A list of Zscaler IP addresses by cloud is at Zscaler Config (https://config.zscaler.com/zscaler.net/cenr).

Your firewalls must be modified to bypass user traffic. It is important that your internal firewall does not perform a Network Address Translation (NAT) process on user data until it transits the ZIA Service Edge. If NAT is applied before the ZIA Service Edge sees the traffic, all traffic will appear to be from a single user.

There are three primary locations where you can deploy a ZIA Private Service Edge or ZIA Virtual Service Edge in your network: in your organization's DMZ, outside the organization's network firewall, or inside the organization's network firewall. Zscaler recommends deploying the devices inside your network DMZ. Most organizations already have an existing practice for deploying services inside the DMZ.

The virtual load balancer used by the ZIA Virtual Service Edge requires that the host have its network interface set to promiscuous mode when more than one device is servicing users. This is required to monitor ZIA Virtual Service Edge cluster member health and to properly balance user traffic across members. Promiscuous mode can be configured so that it is restricted to a dedicated port group for the ZIA Virtual Service Edge devices. If your security policy does not allow this, you can leverage an external load balancer in its place. See External Load Balancer Deployments in this guide.

The specific firewall changes that are required for your deployment are in the ZIA Admin Portal. To learn more, see Firewall Configuration Requirements for Private Service Edge Deployments (https://help.zscaler.com/zia/firewall-configuration-requirements-for-private-service-edge-deployments).

ZIA Private Service Edge deployments require multiple IP addresses inside your network. For more information, see Network and IP Address Requirements (https://help.zscaler.com/zia/understanding-private-service-edge#network-ip-address).

To learn more about ZIA Private Service Edge or ZIA Virtual Service Edge deployments, see Deploying Private Service Edge (https://help.zscaler.com/zia/deploying-private-service-edge).

Deploying Inside the DMZ (Recommended)

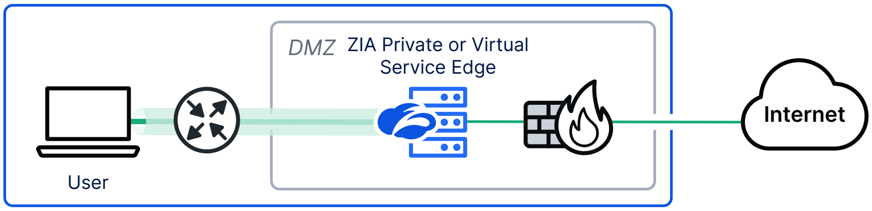


Figure 4: Deploying your ZIA Private Service Edge or ZIA Virtual Service Edge in the DMZ

Deploying your ZIA Private Service Edge or ZIA Virtual Service Edge in your DMZ allows you to limit direct access to the device. However, you must allow remote management by the Zscaler operations team for updates and configuration management. Zscaler also recommends setting up a backup tunnel to another ZIA Private Service Edge in another data center or to a ZIA Public Service Edge device in case your local device becomes unreachable.

If you operate your DMZ by using a single firewall, be aware that port exhaustion on the firewall is possible. The firewall tracks inbound and outbound sessions from the ZIA Private Service Edge, potentially leading to port mapping exhaustion. Be sure to consult your firewall documentation to understand your specific port limits on the device.

Deploying Outside the Network Firewall

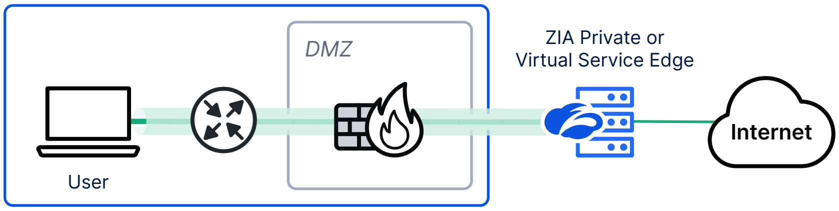


Figure 5: ZIA Private Service Edge or ZIA Virtual Service Edge deployed outside of the network firewall

In this model, you are essentially treating the ZIA Private Service Edge or ZIA Virtual Service Edge as if it were a ZIA Public Service Edge. Zscaler recommends building a GRE tunnel from your edge firewall to a ZIA Private Service Edge or ZIA Virtual Service Edge and directly forwarding your traffic. Zscaler also recommends building a redundant tunnel to either another ZIA Private or Virtual Service Edge or to a ZIA Public Service Edge.

Deploying Inside the Network Firewall (Requires Zscaler Approval)

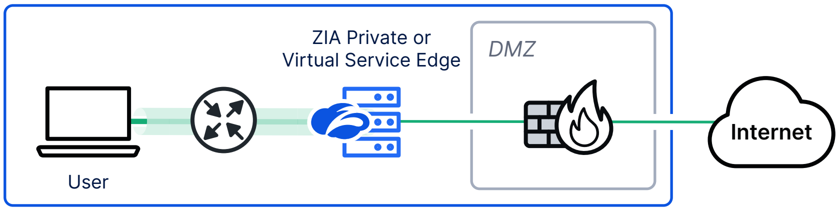


Figure 6: ZIA Private Service Edge or ZIA Virtual Service Edge deployed behind the organization's network firewall

It is possible to deploy a ZIA Private Service Edge or ZIA Virtual Service Edge inside your organization's firewall. However, this requires that you open ports into your local network for the ZIA Service Edge to be managed remotely. Because of the complexity involved, this deployment model requires specific approval by Zscaler prior to deployment. If your organization requires ZIA Service Edge devices to be deployed within its firewall, please contact your Zscaler Account team to discuss your requirements and deployment plan.

Redundancy and High Availability

When deploying a ZIA Private Service Edge or ZIA Virtual Service Edge device, this becomes your user's path to internet applications and websites. As such, Zscaler recommends installing at least two ZIA Service Edge devices at each location.

When configuring these devices, Zscaler recommends configuring the ZIA Service Edge to be a member of a local cluster. ZIA Service Edge clusters operate in an active-active deployment model, with all members servicing user traffic. One additional benefit is that the Zscaler cloud recognizes clusters as being shared in a location and servicing the same pool of users. When upgrades occur, only one cluster member at a time is updated, ensuring other members can continue to service users.

Cluster members share a common IP address and MAC address using Common Address Redundancy Protocol (CARP). This allows traffic to be routed to the devices without specifying an address of a particular member of the cluster. CARP operates at Layer 2 of the Open Systems Interconnection (OSI) stack and requires ZIA Virtual Service Edge devices to be on the same switched network.

A primary member is selected via the CARP protocol election and responds to traffic sent to the CARP IP address and MAC address. CARP also handles automatic failover if the current address holder becomes unresponsive.

The cluster primary member that holds the CARP address acts as the load balancer for all the cluster members. Traffic is distributed from this load balancer to other members on a per-session basis. The primary member also monitors the health of cluster members. If a member instance performance degrades, it is removed from the availability table until the system recovers and begins responding appropriately.

Zscaler recommends using the load balancers that are built in to the ZIA Private Service Edge and ZIA Virtual Service Edge devices. These are the same load balancers used by Zscaler's public data center deployments. The virtual load balancer requires promiscuous mode to operate so that it can coordinate IP addressing, load balancing, and member health checks.

To learn more about ZIA Service Edge clusters, see About Virtual Service Edge Clusters (https://help.zscaler.com/zia/about-virtual-service-edge-clusters).

To learn more about the CARP protocol, refer to Common Address Redundancy Protocol (https://en.wikipedia.org/wiki/Common_Address_Redundancy_Protocol).

External Load Balancer Deployments

If your network or security policy does not allow for network interfaces to operate in promiscuous mode, Zscaler supports deploying the ZIA Service Edge devices with an external load balancer. This can be in one of two modes: clustered ZIA Virtual Service Edges without switching (recommended), or as standalone ZIA Virtual Service Edge devices.

To learn more about external load balancer usage, see Using an External Load Balancer for Virtual Service Edge Clusters (https://help.zscaler.com/zia/using-external-load-balancer-virtual-service-edge-clusters).

Clustered ZIA Virtual Service Edges without Switching (Recommended)

In this model, you configure your ZIA Service Edge devices to be members of a cluster, as with the standard deployment model. However, you connect the ZIA Service Edge devices to your load balancer without having them share a common Layer 2 switched network. Each ZIA Service Edge then elects itself to be the primary and only active member of the cluster.

The main advantage to having your ZIA Service Edge devices in the cluster, even when unable to communicate with each other, is that the Zscaler cloud recognizes them as cluster members. As such, it still upgrades only one cluster member at a time, even though all of them are the "primary" member from that ZIA Service Edge device's point of view.

When configuring your load balancer to forward traffic, use the ZIA Service Edge IP address and not the CARP IP address for the cluster. Because all the ZIA Service Edge devices in the cluster see themselves as the primary, they all advertise and listen for traffic using the CARP IP address and MAC address assigned to the cluster. This can cause loss of throughput, as the load balancer sees the same device constantly switching ports in a race condition.

Standalone ZIA Virtual Service Edge Devices

In this model, each ZIA Service Edge is configured as a standalone device. Your external load balancer uses each of your ZIA Virtual Service Edge IP addresses as the destination. While the setup for this model initially requires fewer steps, it does require manual scheduling of upgrades.

Because the Zscaler cloud sees these devices as independent of each other, possibly not at the same location or serving the same user pool, the system interprets them as not impacting the same users. This can cause all instances of ZIA Virtual Service Edge devices to be upgraded at the same time, resulting in an outage. To protect against an outage, Zscaler recommends you stagger your upgrades so that your users always have an instance available to them.

You can stagger your upgrade time on ZIA Virtual Service Edge devices by up to 24 hours from the original upgrade time. After 24 hours, all ZIA Virtual Service Edge devices are upgraded automatically.

Dual-Arm ZIA Virtual Service Edge Deployments

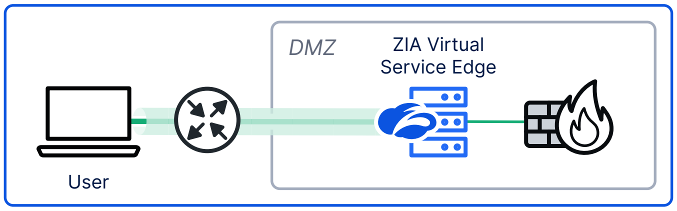


Figure 7: Dual-arm deployments physically separate user access from application access

In most cases, the ZIA Virtual Service Edge is deployed using shared links for internal and external access, with the device sitting in the DMZ. The ZIA Virtual Service Edge also supports using separate links for user-originated traffic. After inspection, different links are then used to send traffic to the internal network and the internet destinations.

The ZIA Virtual Service Edge devices can be deployed in a clustered or standalone mode when using an external load balancer. When supporting remote users in a dual-arm deployment, you must also decide what resources can be accessed via the ZIA Virtual Service Edge. Internal users are supported to internal and internet destinations. Remote users might be limited to accessing internal destinations only, or given the same access as internal users to all destinations. You can read more about ZIA Service Edge clustering in Redundancy and High Availability in this guide.

Deploying in a dual-arm mode requires additional IP addresses for the added interfaces based on your final deployment model. These are used for the proxy interface, cluster IP addresses, and optional management interfaces.

For instructions on how to configure a dual-arm deployment, see Virtual Service Edge Configuration Guide for Dual Arm Mode (https://help.zscaler.com/zia/virtual-service-edge-configuration-guide-dual-arm-mode).

The dual-arm deployment model is only supported on ZIA Virtual Service Edge instances.

Cluster Mode with User Traffic on One Arm

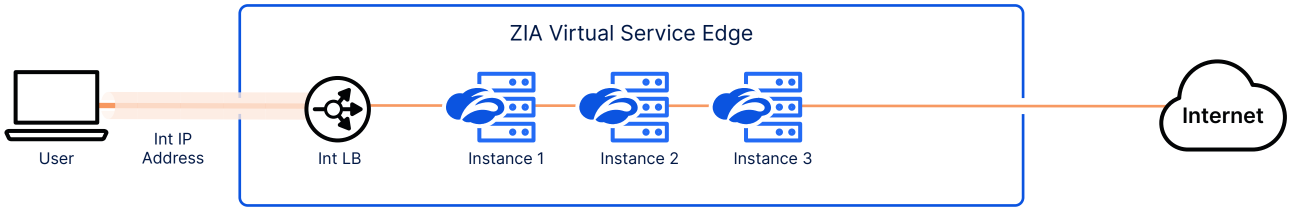


Figure 8: ZIA Service Edge cluster with user traffic on the internal arm

In this model, the ZIA Virtual Service Edge processes internal user traffic that is headed for internal destinations or the internet. Remote users are only allowed to access internal destinations, but internet-bound traffic is filtered. This model is deployed with a load balancer service on the internal side only. Remote user traffic appears to be sourced from the load balancer interface. This configuration requires one additional interface to act as the internet-facing proxy interface. Optionally, an internet-facing management interface can also be configured.

Cluster Mode with User traffic on Both Arms

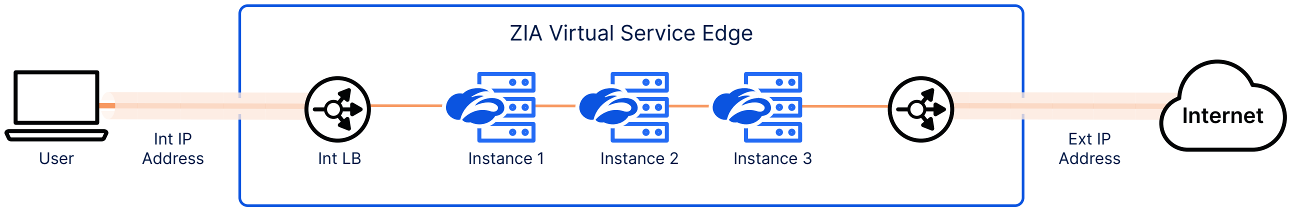


Figure 9: ZIA Service Edge cluster with user traffic on both arms

In this model, the ZIA Virtual Service Edge processes internal and external user traffic that is headed either for internal destinations or the internet. This model is deployed with a load balancer service on the internal and external side. Each side acts as a source address for remote users. This configuration requires one additional interface to act as the internet-facing proxy interface, in addition to one acting as the load balancer service interface. Optionally, an internet-facing management interface can also be configured.

Standalone Mode with User Traffic on Both Arms

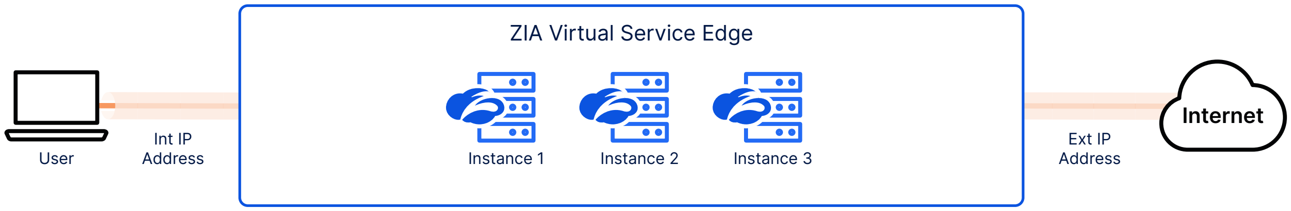


Figure 10: ZIA Service Edge using an external load balancer with user traffic on both arms

In this model, the ZIA Virtual Service Edge processes internal and external user traffic that is headed for internal destinations or the internet. You use your own load balancer to distribute traffic to your ZIA Virtual Service Edge devices. This configuration requires one additional interface to act as the internet-facing proxy interface. Optionally, an internet-facing management interface can also be configured.

Forwarding Traffic to Your ZIA Service Edge

When you choose your infrastructure and deploy either a ZIA Private Service Edge or a ZIA Virtual Service Edge, you must begin steering your traffic to the devices. Most of the standard forwarding modes are available on both platforms, as well as a local steering option. These methods fall into two categories: transparent proxy used at known locations, and explicit proxy used in forwarding mobile traffic. In most cases, you use more than one solution to meet connectivity needs across your users.

Transparent Proxy — Fixed Sites

- Generic Routing Encapsulation (GRE) (recommended) – GRE wraps a simple header around traffic that is destined for the nearest ZIA Service Edge. GRE is available on many enterprise routers and Software-Defined Wide Area Network (SD-WAN) devices. Note that GRE requires each of your organization's locations to have a static IP address. Learn more at Understanding General Routing Encapsulation (GRE) (https://help.zscaler.com/zia/about-generic-routing-encapsulation-gre).
- Layer 2 redirect – If your router or switch is on the same Layer 2 segment as your cluster IP address for your ZIA Private or Virtual Service Edge, that traffic can be forwarded via a Layer 2 redirect rule. If this is the case, consult your router or switch vendor documentation for feature support or configuration.

For information about Zscaler Cloud Connector as a forwarding mode for your cloud applications, see the following Reference Architectures focused on Zscaler Cloud Connector in Amazon Web Services, Microsoft Azure, and Google Cloud Platform (GCP):

- Zero Trust Security for AWS Workloads with Zscaler Cloud Connector (https://help.zscaler.com/cloud-connector/zero-trust-security-aws-workloads-zscaler-cloud-connector)
- Zero Trust Security for Azure Workloads with Zscaler Cloud Connector (https://help.zscaler.com/cloud-connector/zero-trust-security-azure-workloads-zscaler-cloud-connector)
- Zero Trust Security for GCP Workloads with Zscaler Cloud Connector (https://help.zscaler.com/cloud-branch-connector/zero-trust-security-gcp-workloads-zscaler-cloud-connector)

Explicit Proxy — Mobile Users and Some IoT Devices

- Zscaler Client Connector (recommended) – This lightweight agent is included in your ZIA subscription. It is installed on user devices and is the mobile gateway to the ZIA service. Zscaler Client Connector detects if you are on a trusted network at one of your configured locations, and if not, it builds a tunnel to the nearest ZIA Service Edge. Zscaler Client Connector on the end device can also be leveraged for use with other Zscaler services, including Zscaler Private Access™ (ZPA™) or Zscaler Digital Experience™ (ZDX™). This software supports the most common operating systems, including Windows, macOS, Android, iOS, and Linux. Learn more at What Is Zscaler Client Connector? (https://help.zscaler.com/z-app/what-zscaler-app).
- Proxy auto-config (PAC) files – PAC files provide a mechanism for setting up forwarding between a browser and ZIA. This is a JavaScript file that sets the proxy server address and, optionally, additional forwarding rules. This older technology is typically only used on devices without general purpose operating systems, where Zscaler Client Connector cannot be installed. Learn more at Understanding PAC Files (https://help.zscaler.com/zia/about-pac-file).

If you allow user access from the general internet, your infrastructure is vulnerable to DoS attacks. The ZIA Virtual Service Edge allows you to disable all connections other than via GRE and Z-Tunnels from Zscaler Client Connector or other Zscaler infrastructure. Note that if this is enabled, forwarding modes for L2 redirect and PAC files are disabled. To learn more, see Traffic from Home Users (https://help.zscaler.com/zia/forwarding-traffic-virtual-service-edges#traffic-from-home-user).

Forwarding Decision Tree

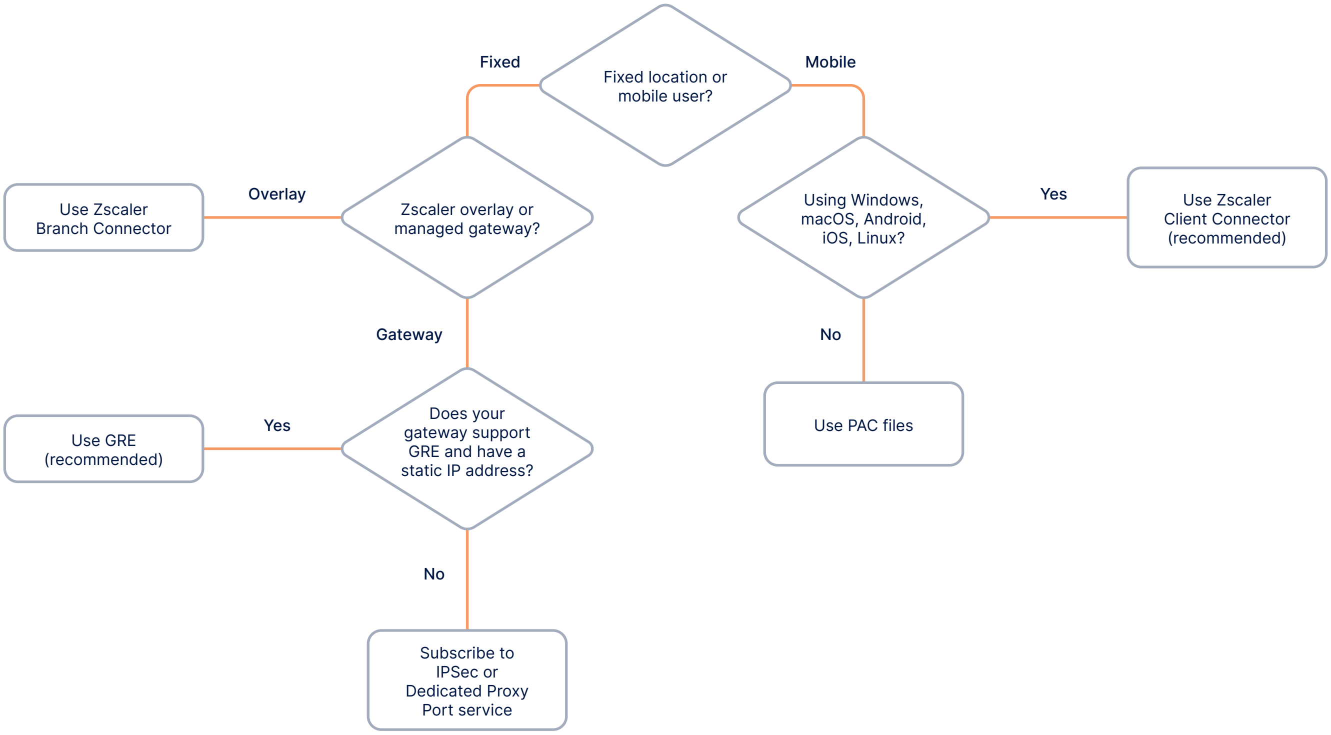

Fixed location or mobile user?
Fixed
Mobile
Zscaler overlay or managed gateway?
Overlay
Use Zscaler Branch Connector
Gateway
Using Windows, macOS, Android, iOS, Linux?
Yes
Use Zscaler Client Connector (recommended)
No
Use PAC files
Does your gateway support GRE and have a static IP address?
Yes
Use GRE (recommended)
No
Subscribe to IPSec or Dedicated Proxy Port service

Figure 11: Forwarding mode decision tree

The method you use to connect to ZIA depends on where the forwarding occurs. You likely use a mix of technologies across your organization. Refer to the diagram to quickly select a solution for each of your use cases.

No matter which transparent forwarding option you choose, Zscaler recommends installing Zscaler Client Connector on all devices. This ensures your users are protected with the same security in and out of the office. Zscaler Client Connector is included for all users in your ZIA subscription.

To learn more about configuring forwarding to your ZIA Private Service Edge or ZIA Virtual Service Edge, see Forwarding Traffic to Virtual Service Edges (https://help.zscaler.com/zia/forwarding-traffic-virtual-service-edges).

For more information on traffic forwarding, see Traffic Forwarding in Zscaler Internet Access (https://help.zscaler.com/zia/traffic-forwarding-zscaler-internet-access).

Summary

The ZIA Private Service Edge and ZIA Virtual Service Edge platforms extend the Zscaler cloud into your data center, bringing the full power of ZIA inspection inside your organization. These devices run the same software that operates in the Zscaler cloud for organizations facing geopolitical, bandwidth, and location-based challenges.

ZIA Private Service Edges and ZIA Virtual Service Edges perform the same service as the ZIA Public Service Edges in the Zscaler cloud—including support for features such as Firewall, Sandbox, and DLP—and are part of the Zscaler cloud. They communicate with the Zscaler cloud for user authentication, policy updates, logging, and reporting. Additionally, after users are signed in and authenticated to the Zscaler service, the service always applies their policies, whether they connect to an on-premises ZIA Private or Virtual Service Edge or to a ZIA Public Service Edge, anywhere in the world.

Logs are transmitted to and stored in the Zscaler cloud as a central repository for integrated analytics, so you can view and monitor internet traffic activity on the dashboard and make full use of the real-time logging and interactive reporting capabilities of the service. Zscaler operations handles software updates, monitoring, and management of the Zscaler service and Zscaler ZIA Private Service Edge and ZIA Virtual Service Edge instances.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform.