

# Zscaler Private Access

Secure remote access to internal applications for the digital enterprise



Enterprises are in the midst of a massive technology shift. Internal applications that were once hosted in the data center, running on an internal network protected by a DMZ, are now moving to the public cloud.

This migration delivers benefits in scale, simplicity, productivity, and more, but it extends the security perimeter to the internet, which breaks the traditional DMZ approach. At the same time, the number of unmanaged user devices connecting to internal applications has continued to rise, forcing IT to find the right balance between the need for access to sensitive applications from unmanaged devices and the need to minimize risk.

To find that balance, IT has often looked to incumbent remote access technologies, finding that they generally fall short, meeting neither users' nor IT's needs.

## The traditional DMZ is no longer effective in a cloud-first world

The traditional DMZ approach worked well for data center applications. It provided an additional layer of security for the internal LAN, allowing IT to expose only external facing services to the internet and place all other internal services behind a firewall. But with applications moving to cloud, the perimeter has been extended to the internet, which the DMZ was not built to secure.

Moving the DMZ to the cloud—often referred to as the “virtual DMZ”—is recommended by some cloud service providers, but it's expensive, difficult to architect, and complex to implement. It starts with a traditional VPN gateway stack hosted in the data center, and requires architecting and implementing a virtual network (VNET) specific to each cloud provider (often involving NIC,

additional network access variables, and more) and a VPN appliance to connect both the internal and virtual networks. The complexity of this method slows the adoption of public cloud, drives up appliance-related costs, and frustrates users attempting to access public cloud applications.

## Zscaler Private Access: Secure remote access in the cloud era

Zscaler Private Access (ZPA™) provides seamless and secure access to internal applications, whether they're hosted in the data center or cloud. ZPA delivers a software-defined perimeter, a network security method that stemmed from work of the Defense Information Systems Agency (DISA) in 2007. As such, ZPA is a completely different network security method than the traditional DMZ. It provides zero-trust access to internal applications using software—on a need-to-know basis—by looking at two criteria: user device and user identity.

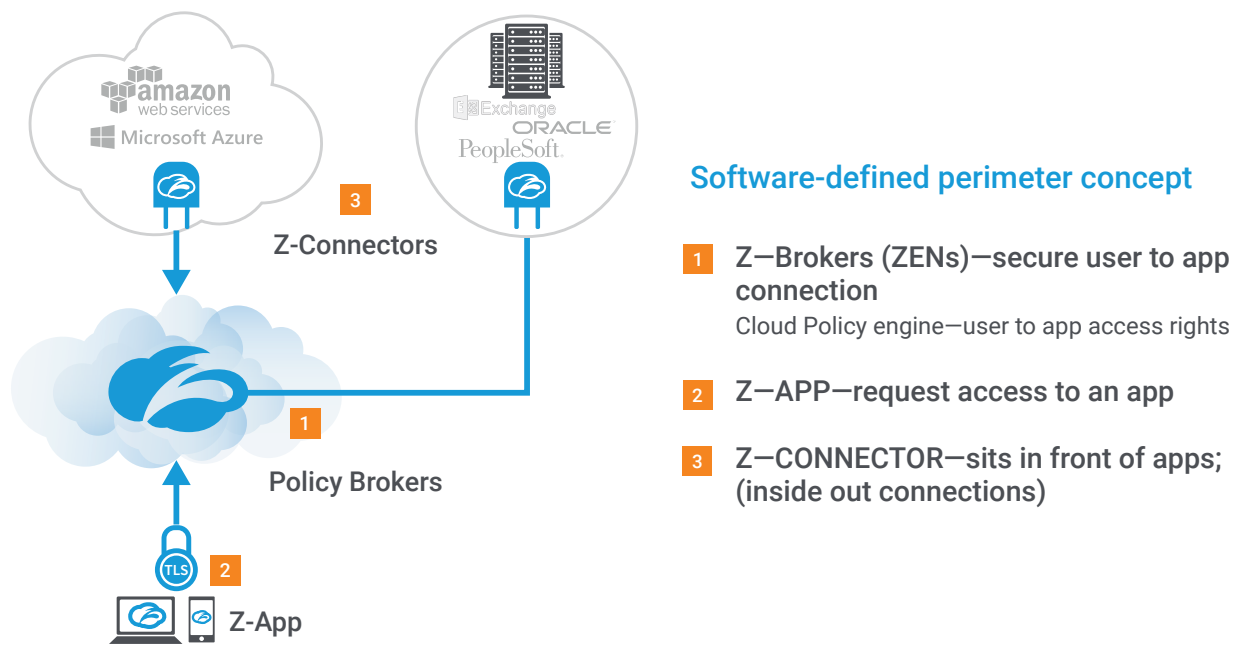
ZPA's unique design is based on four key tenets:

- Connect users to applications without placing users on the network
- Never expose applications to unauthorized users
- Enable app segmentation without network segmentation
- Provide secure remote access without using VPN appliances

ZPA provides a simple, secure, and effective way to access internal applications. Access is based on policies created by the IT admin within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, a piece of software called Z-App is installed. Z-App ensures the user's device posture and extends a secure micro-tunnel out to the Zscaler cloud when a user attempts to access an internal application.

Adjacent to an application running in a public cloud or data center, ZPA places a small piece of software called Z-Connector, deployed as a VM, which is used to extend a micro-tunnel out to the Zscaler cloud. The Z-Connector establishes an outbound connection to the cloud, and does not receive any inbound connection requests, thereby preventing DDoS attacks. Within the Zscaler cloud, a Z-Broker approves access and stitches together the user-to-application connection. ZPA is 100 percent software defined, so it requires no appliances and allows users to benefit from the cloud and mobility while maintaining the security of their applications.

Below is a look at the architecture of the ZPA service.



## Empowering the enterprise with ZPA

### Deliver a cloud-like user experience

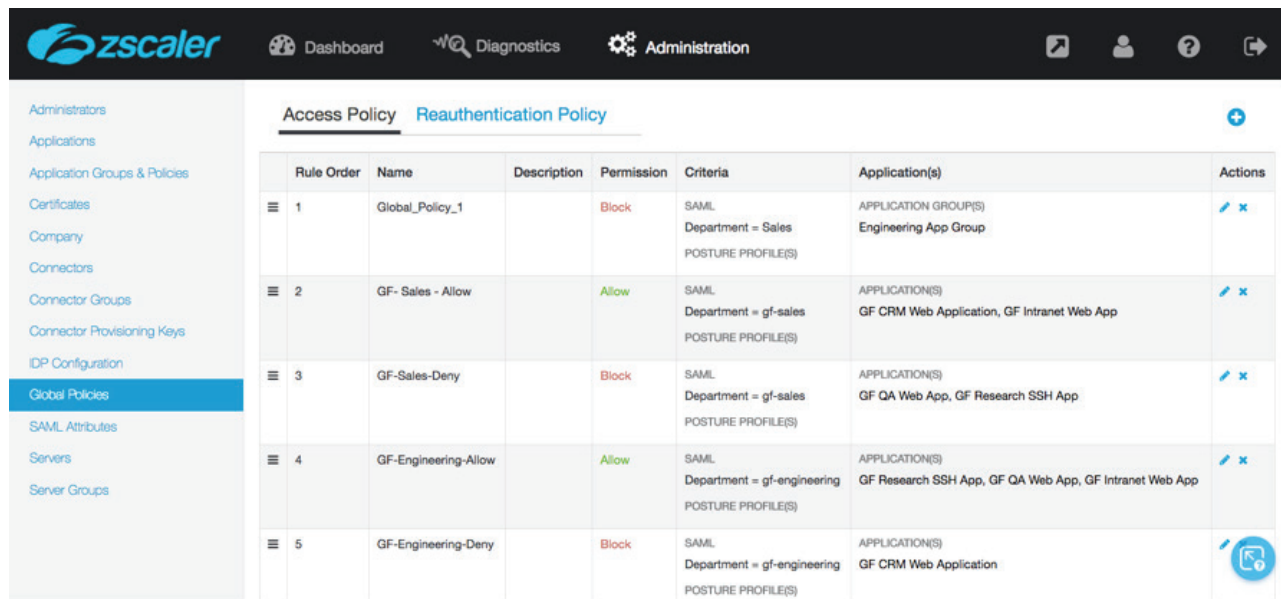
Users are playing a larger role in determining which technologies are deployed in the enterprise. ZPA delivers the experience users want with the security IT needs.

- Consistent user experience for both public cloud and data center applications
- The service integrates with Okta and other single sign-on providers for faster access
- Users are routed directly to the app via the nearest Z-Broker for faster access
- Admins can customize re-authentication timeframes to ensure the best experience for remote users











## Standardize and control access to internal applications

ZPA delivers a central platform that gives IT control over applications and the users authorized to access them.

- Global policies hosted in the Zscaler cloud determine which users can access which applications
- Admins create and manage policies for users, user groups, applications, and application groups
- IT can segment access by applications with no need to segment by network or use ACLs



The screenshot shows the Zscaler Administration Console interface. The top navigation bar includes the Zscaler logo, Dashboard, Diagnostics, and Administration tabs. A left sidebar lists various configuration areas like Administrators, Applications, and Global Policies. The main content area is titled 'Access Policy' and displays a table of five rules.

Rule Order	Name	Description	Permission	Criteria	Application(s)	Actions
1	Global_Policy_1		Block	SAML Department = Sales POSTURE PROFILE(S)	APPLICATION GROUP(S) Engineering App Group	 
2	GF- Sales - Allow		Allow	SAML Department = gf-sales POSTURE PROFILE(S)	APPLICATION(S) GF CRM Web Application, GF Intranet Web App	 
3	GF-Sales-Deny		Block	SAML Department = gf-sales POSTURE PROFILE(S)	APPLICATION(S) GF QA Web App, GF Research SSH App	 
4	GF-Engineering-Allow		Allow	SAML Department = gf-engineering POSTURE PROFILE(S)	APPLICATION(S) GF Research SSH App, GF QA Web App, GF Intranet Web App	 
5	GF-Engineering-Deny		Block	SAML Department = gf-engineering POSTURE PROFILE(S)	APPLICATION(S) GF CRM Web Application	 

## Reduce risk and exposure

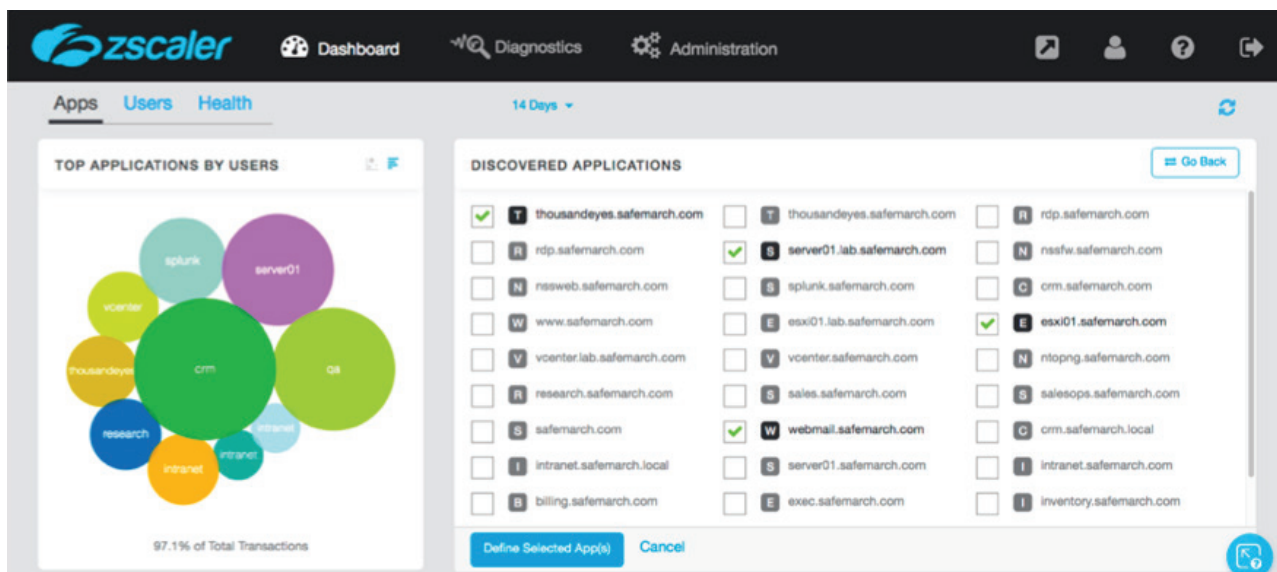
ZPA helps enterprises reduce their attack surface and protect internal applications from external threats.

- Users are never placed on the network, enabling the use of unmanaged devices while limiting risk
- Applications are “dark” to unauthorized users, eliminating lateral access
- Applications are never exposed to the internet, which reduces the threat of DDoS attacks
- Secure TLS-based encrypted micro-tunneling is used for data protection
- Partners and third parties have access to specific applications—without access to the network

## Gain visibility into the application environment

ZPA provides the intelligence admins need to understand who is accessing applications and take action when necessary, all from within the admin UI.

- Discover unknown applications running in your public cloud and apply granular access controls
- Identify users who are interacting most frequently with these applications
- View past and real-time user activity
- View the health of applications, servers, and connectors in your environment
- Automatically stream user audit logs to your SIEM provider



## Simplify remote access to the cloud

Remote user access to public cloud services like Azure, AWS, and Google Cloud platforms is now faster, less complex, and more secure with ZPA.

- ZPA provides user-to-public cloud application access via the Zscaler cloud, not VPN appliances
- Removes the need for the VPN gateway stack or connecting to a virtual DMZ for secure access to public clouds
- Drastically reduces the complexity of network and security architectures, accelerating cloud adoption
- Accelerates app migration by simply routing user traffic to a new connector once an app is moved
- Simplifies network security for cloud adoption through partnerships with both Microsoft (Azure) and Amazon (AWS)

## Accelerate mergers and acquisitions

Mergers and acquisitions can take months or even years to implement. ZPA reduces the network complexity and cost often experienced by IT architects and admins during an M&A.

- ZPA standardizes security for all current and newly acquired assets
- Eliminates the need to consolidate multiple networks or IP addresses
- Can speed M&A timeframes through simply ZPA software deployment
- Places no employees—existing or acquired—on the network
- Requires no changes to current infrastructure

### Zscaler Private Access is available in three different product suites:

FEATURE	PROFESSIONAL	BUSINESS	ENTERPRISE
<b>Global visibility for users and application</b> — Single pane of glass shows which users are accessing private, internal apps	✓	✓	✓
<b>Secure Private Application access</b> — Access to unlimited private internal applications (whether public/private/hybrid cloud or legacy datacenters) without exposing the network to users or applications to the Internet	✓	✓	✓
<b>App and server discovery</b> — Wildcard policy shows application and server locations as they are requested by users	✓	✓	✓
<b>Enterprise DarkNet with DDoS protection for applications</b> — Applications are only visible to users that are authorized to connect to them	✓	✓	✓
<b>Single console for policy definition and management</b> — All policy for global deployment via a single pane of glass	✓	✓	✓
<b>Passive health monitoring</b> — Application health is monitored when access is requested	✓	✓	✓
<b>Zscaler App</b> — Lightweight application used to provide access to Zscaler Internet Access and Zscaler Private Access	✓	✓	✓
<b>Microsegmentation by application (up to 5 application segments)</b> — Granular access control by user or group for up to five specific application definitions, each of which may contain multiple hosts and/or ports.	✓		
<b>Microsegmentation by application (up to 10,000 application segments)</b> — Granular access control by user or group for up to 10,000 specific application definitions, each of which may contain multiple hosts and/or ports.		✓	✓
<b>Continuous health monitoring</b> — Application health is continuously monitored to ensure that ports are available and users can connect to the app		✓	✓
<b>Device posture enforcement</b> — Checks device fingerprint and certificate, as well as other postures		✓	✓
<b>*Customer-provided PKI</b> — Customer-provided certificates ensure complete privacy			✓
<b>*Double encryption</b> — Provides encryption to microtunnel using customer's PKI			✓
<b>Real-time user transaction view</b> — Instantaneous logs for end-user support			✓
<b>*Log Streaming Service</b> — Automatically streams logs to SIEM provider		✓	✓

Note: An application segment is any number of FDQNs/IP addresses on a standard set of ports.

\*Feature can be added separately

To learn more about Zscaler Private Access visit [zscaler.com/products/zscaler-private-access](https://zscaler.com/products/zscaler-private-access)

#### About Truststream

Truststream is a fully-accredited partner of Zscaler that provides expert cyber security professional services and managed security services. We help customers improve their threat protection and reduce their risk of financial and reputational loss.

0131 473 2354 | [info@truststream.co.uk](mailto:info@truststream.co.uk) | [truststream.co.uk](https://truststream.co.uk)

#### About Zscaler

Zscaler was founded in 2008 on a simple but powerful concept: as applications move to the cloud, security needs to move there as well. Today, we are helping thousands of global organizations transform into cloud-enabled operations.

