Zscaler Private Access™ for Amazon Web Services

Faster, more secure remote access to AWS – no remote access VPN required
The number one reason Amazon Web Services (AWS) customers say they choose to move to the cloud is for the agility and speed that comes with it. With cloud computing, enterprises are able to spin up thousands of AWS instances within minutes as opposed to the 10 to 18 weeks it typically takes to purchase and deploy servers on-premises. The AWS Cloud boasts a robust set of more than 90 enterprise services, including everything from compute, storage, and databases to continuous integration, data analytics, and artificial intelligence.

It’s this convenience that leads many enterprises to begin migrating their internal applications from their data centers to AWS, using the cloud service provider to meet a variety of business initiatives. Some are looking to increase the productivity of their workforce by delivering a “cloud-like” experience. While others are looking to consolidate their data centers so that they may cut down on the overhead associated with maintaining hardware, reduce infrastructure sprawl, or prepare for a merger or divestiture. In addition, there are companies looking to completely reimagine their businesses using modern cloud technology as part of a larger digital transformation initiative. And of course, enterprises technology leaders are always looking for ways to improve their bottom lines by reducing their costs.

AWS makes it easier for an increasingly large remote workforce, regardless of location or time zone, to access applications by using the cloud’s global reach to ensure minimal latency and provide an optimal user-to-app path. This drives additional value for the business, allowing enterprises to maximize the productivity of their remote employees.

Why enterprises are moving to AWS

AWS continues to be the most widely used public cloud service, according to the RightScale 2017 State of the Cloud report.
In the early days of security, the focus was on protecting the data and internal applications running within the data center. Security architects determined that the best way to ensure that protection was to build a secure perimeter around the network. And thus, the castle-and-moat architecture that many security teams are familiar with today was born.

From a networking perspective, hosting internal applications within a single data center was a natural fit with the castle-and-moat security architecture. It meant that all traffic from remote users or branch offices would be backhauled to that data center in order to access applications. In many cases, this data center was located in another part of the world.

Now, applications that once resided in the data center are being migrated to the AWS cloud. This breaks the idea of a secure perimeter, as the apps and data that need protecting now reside outside the perimeter. The hub-and-spoke strategy of routing traffic to a central data center becomes inefficient with apps running in AWS.

Since the 1990s, there’s been only one way to provide remote access to internal applications: the remote access virtual private network (VPN). But with internal apps moving to cloud providers like AWS, and being accessed by an ever-increasing number of remote workers, it no longer makes sense to route traffic through a static gateway hosted within a data center. AWS adoption calls for a new approach to secure remote access. One that eliminates the challenges of incumbent solutions.

“DMZs and legacy VPNs were designed for the networks of the 1990s and have become obsolete because they lack the agility needed to protect digital businesses.”

Gartner
September 2016
Zscaler Private Access (ZPA™) is a revolutionary service from Zscaler that uses the Zscaler™ cloud to provide secure remote access to internal applications. ZPA enables enterprises to break free from the remote access VPN-driven mindset that has been centered around the data center to one of a more modern, cloud-based approach.

ZPA works by brokering a connection between an authenticated user and an application. Policies are enforced in the Zscaler cloud and users can only see the apps to which they have been granted access.

**Challenges of the remote access VPN**

**Poor user experience**
Users attempting to access applications running within AWS are forced to log in to a remote access VPN. Their traffic is the routed through the data center, instead of going directly to AWS.

**High cost and complexity**
Remote access VPNs require multiple gateway appliances. This makes it difficult to scale across multiple geographies, as teams would have to replicate gateways across each data center. By forcing traffic through centralized gateways, VPNs hinder the cloud’s benefits, such as its elasticity, simplicity, and cost savings.

**Risk of attack**
Remote access VPNs place remote users on the corporate network. This exposes the network to malware or other security attacks that stem from untrusted user devices. Lateral movement makes it easier for attacks to spread to multiple apps.

Zscaler Private Access (ZPA™) is a revolutionary service from Zscaler that uses the Zscaler™ cloud to provide secure remote access to internal applications. ZPA enables enterprises to break free from the remote access VPN-driven mindset that has been centered around the data center to one of a more modern, cloud-based approach.

ZPA works by brokering a connection between an authenticated user and an application. Policies are enforced in the Zscaler cloud and users can only see the apps to which they have been granted access.

**App Connector:** Sits in front of apps (inside-out connections)

**ZPA Public Service Edge:** Secure user-to-app connection

**Zscaler Client Connector:** Requests access to an app

**AWS Direct Connect**

**Data Center**
The ZPA service ensures that user traffic always traverses the optimal path based on the location of the user. Because remote users access the application nearest to them, the user experience improves and so does productivity.

With ZPA, remote users are no longer required to take the time to log in to a VPN client each time they want to access an application. The Zscaler Client Connector (formerly Zscaler App/Z App) installed on their mobile devices only requires a one-time login (it integrates with single sign-on providers, such as Okta). After that, the user never has to log in again, which provides a more seamless experience for remote employees as they connect to applications hosted in the AWS Cloud.

**Secure remote access to apps on AWS**

The cloud-delivered security approach enables enterprises to determine who has access to which internal applications, even as they are migrated from the data center to AWS. The solution is built upon the four key tenets of the Zscaler Private Access service.

1 | **Users are not on the network** – Users are never given access to the corporate network. Access is application specific, with no need to define policy by IP address or ACL.

2 | **Applications are invisible** – Internal IP addresses are never exposed to the internet. Internal applications are on a corporate “dark-net” and are completely invisible to users, unless users are authorized to access them.

3 | **The internet becomes the new secure network** – Zscaler Private Access leverages the internet for dynamic, app-specific, TLS-based end-to-end encryption. All data remains private and customers can use their own PKIs.

4 | **Policies provide application-level segmentation** – There is no user-to-network access. Users have direct access only to specific applications, and each application session has its own micro-tunnel.
Why Zscaler Private Access for AWS?

A better experience for remote users

- Faster access to apps on AWS
- No more VPN client for each login session
- Seamless experience for apps on AWS or hybrid IT environments

Less complexity for administrators

- Easy to implement within one hour; no need to set up VPN gateways
- Application segmentation, not network segmentation
- Integrates with single sign-on (SSO) providers, such as Okta
- Can be deployed alongside AWS Direct Connect

Secure remote access to internal apps on AWS

- Users are never on the network
- Policy-based access to specific applications on AWS
- No lateral access to additional internal applications
- Visibility into all apps running on AWS
- Visibility into user activity taking place

Increased business value

- No need to purchase hardware results in cost savings
- Increase in remote user productivity
- Service model converts security to a simple, predictable operating expense

Getting started with ZPA for AWS

The Zscaler Private Access cloud service represents the revolution of secure remote access. It gives remote users access to applications, without placing them on the network and does so in a way that is completely seamless to the user. Enterprises no longer have to rely on outdated remote access VPN services hosted in the data center.

ZPA for AWS has redefined the way internal applications running in AWS can be accessed, and it enables enterprises to receive the full benefits of the AWS Cloud. With this new solution, security—often viewed as an inhibitor of change—becomes a catalyst for the migration of internal applications to AWS.

To learn more, visit zscaler.com/aws, or contact us at sales@zscaler.com.