Zscaler Private Access for Application Migration to AWS

Mapping Zscaler Private Access to the AWS Cloud Adoption Framework

Whitepaper
July 2021

Table of contents

Introduction

BENEFITS OF ZSCALER PRIVATE ACCESS (ZPA):

- Accelerate application migration and cloud adoption
- Enable granular control of user access to apps hosted on AWS
- Actively manage workload access pre- and post- migration
- Deliver end-to-end app visiblity and improve user experience

This document is intended to show how Zscaler™ accelerates user adoption by removing friction associated with achieving networking and security objectives. Exploring how Zscaler Private Access™ (ZPA™) applies to AWS migration use cases will help to provide a structured approach to the overall solution and illustrate how ZPA accelerates application migration.

Where Zscaler is engaged with commercial and public sector projects, the ZPA architecture is positioned as an enabler for enhanced user and application agility, which accelerates application migration.

The core function of ZPA is to actively manage authorized user access to - and interaction with - workloads before, during, and after migration to the cloud, while improving the overall end user experience.

Zscaler Private Access architectural best practices play a core function in the customer's cloud migration phases, including:

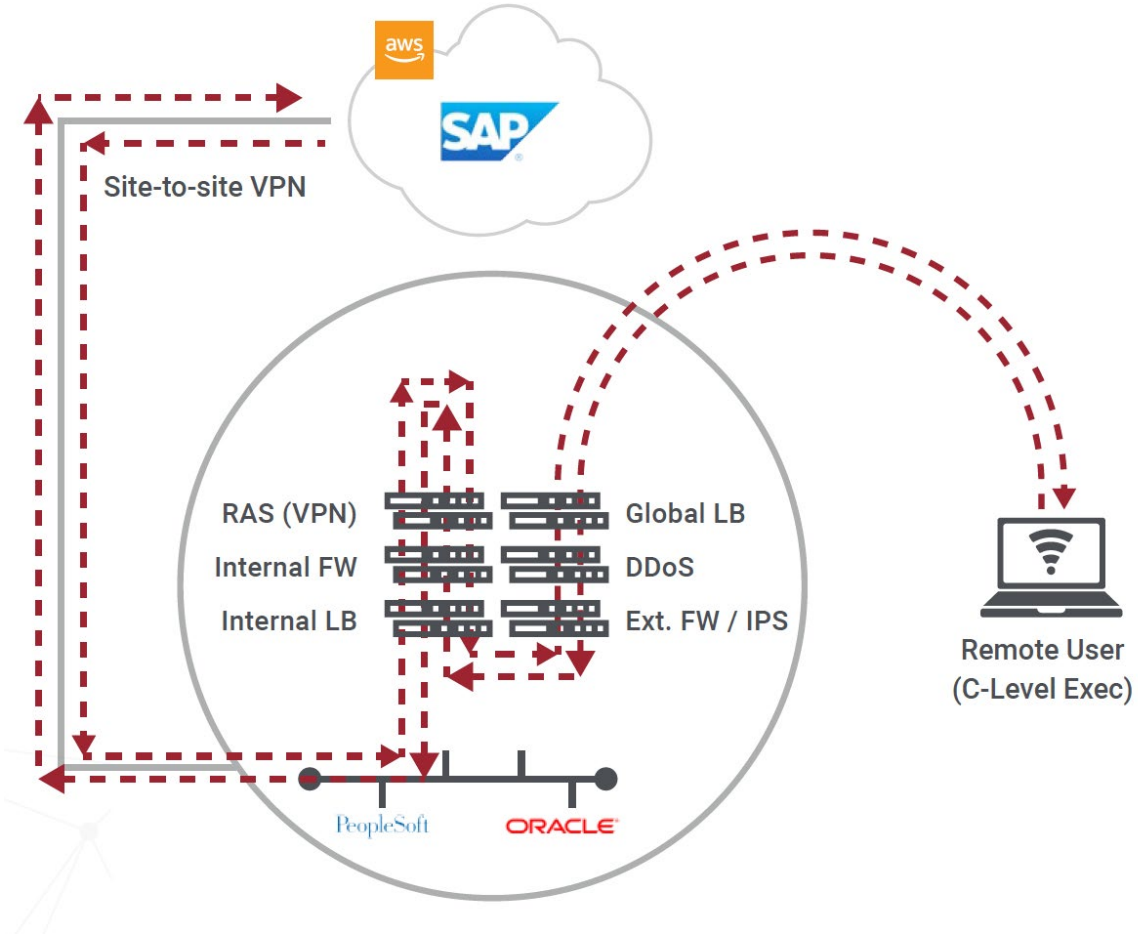
- Preparation and Planning
- Portfolio and Discovery
- Operational Planning and Delivery
- Migration and Validation
- Ongoing Operational functions

Although this document focuses on migrating workloads to AWS, the ZPA solution and related software-defined perimeter solutions are not specific to AWS deployments. ZPA supports hybrid IT environments, and can be utilized to augment application migration frameworks defined by consulting practices.

Zscaler Private Access: Securing Access to Internal Applications

Zscaler Private Access provides secure access to internal applications, whether they're hosted in your private datacenter or public cloud. Zscaler lowers the cost and complexity of legacy networking and security challenges, while improving upon the user experience of traditional VPN-based network access.

Most customers start off with traditional on-premises, datacenter-centric, hardware-based network infrastructure with centralized remote access solutions which look like this:

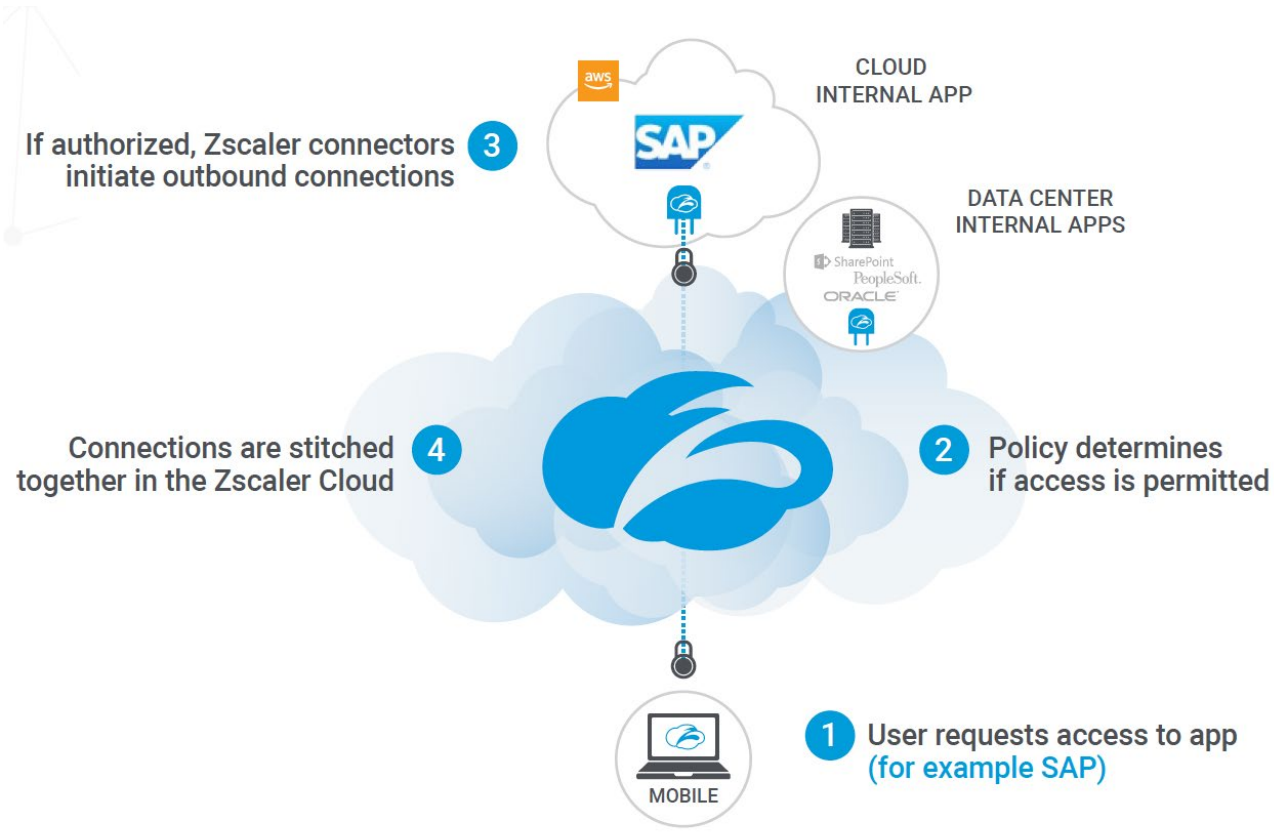


BEFORE ZSCALER: Traditional datacenter-centric remote access approach

Zscaler Private Access delivers a software-defined perimeter (SDP) solution. This user experience-focused methodology is designed specifically to address scaling and other needs of a modern agile business community moving to the cloud, and is completely different from traditional remote-access VPN solutions.

Zscaler Private Access leverages our global cloud architecture and establishes zero trust access to private applications. Trust is never assumed, but based on user and device authentication through SAML. Once each user is authenticated, an inside-out connection is established from an App Connector in AWS to the Zscaler cloud, where a secure connection is established between authorized users and their applications.

With **ZScaler Private Access,** application access is federated through a global security cloud, with the network becomes merely transport. Granular, policy-based access is used to connect authenticated users to the applications they're authorized for, so customers can keep their public cloud private.



WITH ZSCALER: Secure, policy-based access, with users off the network

Since the security posture of the user and device is evaluated before application access is granted, applications are invisible to users who do not have permission to access. Furthermore, since the applications are federated through the Zscaler cloud, there are no inbound connections to the AWS instance or customer datacenter, meaning the ACLs and Security Groups become simpler. The policy is based on user/device information rather than network objects, providing greater visibility and flexibility.

Zscaler Private Access enables a user to access permitted applications simultaneously in both their AWS VPCs and their physical datacenters. Abstracting the network from the user and providing a shortest-path connection to the application enhances the user experience, simplifies the network architecture, and provides greater visibility and control for security.

Accelerating Application Migration

ENHANCED IDENTITY AND ACCESS MANAGEMENT

- Applications are invisible to users/devices which have not been pre-authorized
- Helps address modern security threats like DDoS attacks and rogue access from third-party sources
- Restricts the ability of malware to move horizontally across your internal network

Zscaler Private Access can be leveraged to support a preliminary business case for a migration. The challenges of quantifying an existing application infrastructure are extensive; with this approach, Zscaler delivers a framework for seamless user experience both within the legacy and AWS environments. Policy based access control replaces traditional infrastructure and related configuration and ongoing administration.

The architecture lead or consulting practice lead can potentially shorten the overall timeline of the migration. ZPA provides a platform from which user access can be controlled during the migration of workloads to AWS without any changes to the legacy network infrastructure. Traditional VPN hardware can be avoided as a prerequisite for connecting users to private applications hosted in AWS, as can the related need for AWS Direct Connect to handle the suboptimal traffic path of bringing remote users through the datacenter into the AWS environment.

The adoption of the ZPA platform enables granular control of user access to applications hosted on AWS, in multiple regions, and in a hybrid environment. In practice, this approach can both simplify cloud adoption and allow the customer to build confidence with their user community during migration.

By enhancing the user experience, dramatically reducing the change control processes, delivering end-to-end application visibility, and providing the ability to choose discrete group/locations for migration to be undertaken simply through the use of centralized policy management, ZPA enables businesses to migrate faster and provide the best user experience.

When business applications like SAP, Oracle, or Microsoft workloads are migrated to AWS, it is often the case that networking and security approaches are deferred to be resolved later in the migration planning and execution cycle. AWS and APN Consulting Partner Solution Architects regularly report being confronted by friction and delays as a result. By having an elegant and well understood solution like ZPA in the planning toolbox at the start of the project, this friction can be understood, anticipated, and avoided.

This process often brings together Cloud Architects, IT, Networking, and Security stakeholders in a positive discourse that is otherwise not typically a part of the Preparation and Planning phase.

For those applications, the migration to IaaS will be attractive and often obvious given the size and scope of their deployments. However, we find that a common initial challenge is identifying all the applications that are being accessed by users and are also candidates for migration. At times, the number of discovered apps is an order of magnitude greater than IT executives estimate the number to be. ZPA provides private application discovery and reporting to provide customers with visibility into all the applications being accessed in their physical datacenter. This helps the consulting organization and the customer to prioritize which apps should be migrated to IaaS cloud and to enhance the security controls around those applications.

Customers can then more easily identify workloads to migrate to AWS, but will need to decide how to provide the applications to their users securely—a significant challenge if the application is not designed for cloud-based delivery.

Identity and Access Management is key to delivering on IaaS. However, this access control can be enhanced further—by rendering the applications invisible to all except users/devices which have been pre-authorized. This helps to address modern security threats including DDoS attacks, rogue access from third-party sources, and the ability for malware to move horizontally across the internal network.

> **"We were able to implement a zero trust model…and replaced traditional approaches with this modern, secure, cloud-first implementation. We also have granular control over user permissions, with each employee and contractor getting access to only what they need to have access to."**
>
> — Tony Fergusson, IT Infrastructure Architect, MAN Energy Solutions

Enhanced Security

Zscaler Private Access provides a granular policy framework to connect users to applications, irrespective of where those applications reside. ZPA doesn't connect users to the network, but rather it abstracts the network entirely from the user. This application connectivity has multiple benefits:

- Users can access applications across multiple environments (AWS, on-premises, or hybrid) via encrypted TLS tunnels that are spun up on demand.
- Users have access to internal apps without ever being placed on the network.

- IP addressing may overlap in the data centers. Since the network is abstracted from the user, the overlap is irrelevant.
- Application access policy is evaluated in the Zscaler cloud. Only when user+device access is authenticated, an outbound application connection is established via the App Connector running in the app environment. The app environment is "dark" to the internet, which means that there are no inbound connections to the device or the app environment.
- Granular per-application and per-user/attribute policy can be written and maintained by the customer or an MSP.

By granting users access only to the applications they need for their role, instead of to the entire network, ZPA provides greater security than a traditional VPN approach. This approach enables a security posture that is inherently more effective against the most common forms of intrusion and malware. Additionally, Zscaler will both support and accelerate the adoption of an end-state zero trust approach for AWS customers.

In relation to the AWS migration framework, ZPA enables application-specific user access – providing a consistent approach for all workloads deployed on AWS. Restricting users to only the specific applications they need for their role enhances the company security posture. In addition to user role, device management status can also be used as context for an application request. ZPA helps AWS customers to fulfil their part of the AWS Shared Responsibility Model by providing mechanisms and methodologies for managing granular control over which users, on what devices, can access which applications.

How Zscaler Private Access Accelerates Migration to AWS

This section outlines further details and benefits for each of the following steps, referenced in **AWS cloud migration** practice recommendations, which are often adopted by customers and in consulting practices:

- **Preparation and Planning**
- **Portfolio and Discovery**
- **Operational Planning and Delivery**
- **Migration and Validation**
- **Ongoing Operations and Future Investment**

Preparation and Planning

Zscaler Private Access can be used to accelerate AWS adoption and avoid multiple traditional project phases that would otherwise be required in order to meet this goal. Specifically, by establishing a baseline for the most demanding and important, yet often overlooked, part of any migration—your users.

ZPA will enable the customer to:

- Leverage 'identity' as the new perimeter by providing a layer of abstraction between users and the applications they are trying to consume.
- Assume a security posture which does not inherently trust users based on whether they are inside or outside of the enterprise network perimeter. Instead, users are authenticated via their Identity and Access Management (IAM) solution and granted access to their applications, taking into account a number of policy controls. Controls can be based on SAML attributes returned by the IAM solution.
- Enable a risk-based approach using multi-factor authentication (MFA).
- Reduce the need for elevated privileged access and minimize the attack surface for any inbound access dramatically. This is achieved by intercepting user requests for internal applications and enforcing policy before connecting the user to the app, essentially making the applications 'dark' both to the Internet and to unauthorized internal users.
- Deliver a frictionless user experience by integrating transparently into the users' normal workflow, regardless of whether the user is on a corporate or public network. With Zscaler Client Connector (formerly Zscaler App) installed, no user action is required to connect to applications, regardless of their location or the device they chose to use.

Portfolio and Discovery

Many customers are now on the journey to becoming cloud-first businesses. At Zscaler we understand that the challenges customers want to avoid in moving to the cloud migration initiatives include:

- Poor user experience as applications are moved from private datacenters to the public cloud –both from continually educating users on how to consume apps, and from complexity around performance of the applications.
- Network complexity caused by connecting private data centers to the public cloud.
- Cost and complexity of dimensioning, managing, and predicting the desired capacity required by your global business.
- Significant security threat and uncertainty represented by allowing trusted and untrusted users onto the enterprise network

Zscaler Private Access overcomes these challenges by delivering visibility into internal apps through the following three key security design phases:

- **Discovery:** User access-driven application discovery illustrates which internal applications are being consumed within an organisation, and subsequently which apps are being consumed from AWS.
- **Tuning:** Once an application has been discovered, you can then undertake tuning of policy to establish a baseline prior to migration. This avoids exposure once moved to AWS and also reduces time to final delivery.
- **Production:** Application segmentation allows you to quickly and granularly apply policy to match the security and delivery posture that is required for full production.

Customer Spotlight:
For a large global drinks manufacturer, discovery revealed 500+ applications on premises. Zscaler enabled the IT department in 95 minutes; tuning involved MFA and other attributes. Production deployment has changed little since the initial deployment.

Zscaler Private Access helps to accelerate the discovery phase by integrating transparently into the users' workflow. Users simply access the app they would like to use, without a requirement for them to first interact with any security software such an endpoint client. Users no longer need to understand how an application is accessed, whether new or legacy, and administrators have full end-to-end visibility of application flows.

Operational Planning and Delivery

As customers identify the applications to migrate to AWS, they make a decision on how to deliver the application to the users. This essentially takes one of three forms:

Virtualize - Keep Private

- Understand the current architecture of the application. In a three tier environment (web server, app server, database server) each component would be virtualized and migrated to AWS in turn.
- Front-end might be migrated first, and the app server / database server may remain available via VPN or a dedication connection such as Direct Connect.
- The application remains "private" and only accessible via the VPN or dedicated connection.

> **"Because of Zscaler, we were able to be very agile…We have been getting nothing but praise from other departments that they are able to continue their work from home. Zscaler basically sunsets the idea of a traditional VPN."**
>
> —Marc De Serio, CTO, Henry M. Jackson Foundation (HJF)

Virtualize - Make Public

- Similar to the first form; however, the front-end web server becomes available on the Internet directly.
- The application is resolvable publicly.
- A requirement to implement a Web Application Firewall (WAF) to control content inbound/outbound to the application, DDoS protections, and implement Identity and Access Management to restrict user access.

Re-architect for Cloud

- Applications which cannot or will not be migrated in their current form.
- Front-end will move to EC2 or Serverless with CloudFront - web server re-purposing and re-coding.
- Middle tier to move to EC2 or Serverless - re-purpose middleware.
- Back-end to move to RDS/Aurora/etc - update schema, DB, etc.
- IAM controls access; WAF controls content.
- User experience and access change in line with migration to a new architecture.

Making the application public has a security risk, which can be quantified. For some applications, this risk - both with re-architecting and with virtualization - can be acceptable to the business. ZPA can enable customers to advertise applications publicly while providing the same security architecture by leveraging browser-based access - this consumes the same SAML Authentication into ZPA, uses the same ZPA Architecture for no-inbound access, and provides the same policy framework and visibility.

However, for a number of applications, such as SAP, the risk of exposing the application directly to the Internet is too great. Indeed, the security needs to be enhanced as part of the migration to AWS. ZPA enables customers to plan their migration, enhance the security as part of that migration, and keep applications private.

Migration and Validation

As part of the migration it's important to understand where progress is being made. Zscaler Private Access provides visibility of where applications are being consumed and the security policy around them.

Zscaler Private Access acts as an abstraction layer between the user and the app. The location of the app can be changed, from datacenter to public cloud or VPC to VPC, without any negative impact on user experience. Users never connect directly to applications; the traffic must pass through the ZPA cloud service. Additionally, users are never placed on the network - resulting in a stronger security posture. All ZPA communications are outbound connections from the datacenter or public cloud to the ZPA cloud service. Consequently, the datacenter firewalls or ACLs can now be configured to deny all inbound connections, and the datacenter / VPC can become completely dark to the rest of the world.

Zscaler Private Access integrates with a customer's Security Operations Center (SOC) for SIEM feed and reporting/analytics. Graphical representation of applications and users is provided via the ZPA management console, and policy changes can be made to control user access to applications.

Customer Spotlight:
For the UK Government, ZPA is now an integral tool used to deliver applications and access into AWS. This customer has adopted a zero trust model – ALL apps are consumed only via ZPA.

Zscaler doesn't provide migration services; however, Zscaler does bolster the process of validating the migration and ensuring the user experience being delivered is inline with the business requirements. Customer and consultant visibility into how application migrations are progressing is a key deliverable supported by ZPA.

Ongoing Operations and Future Investment

Zscaler Private Access allows AWS and our customer admins to create custom policies on a per-app, per-user basis, at a global scale. This can reduce the complexity imposed by network-based segmentation.

- Simple policies to segment access based on identity and application.
- Avoid the need to create and implement hard to manage IP address-based policies. In other words, operations can be agile internally – but the application consumer is not affected. Leverage DevSecOps to migrate applications from private to public cloud, while keeping the public cloud private.
- Provide customers with greater visibility and control over which applications can be accessed by third parties and contractors.
- Zscaler continuously invests in the Zscaler cloud and advancing capabilities. These advances are based on customer learnings and requirements that span traffic across many global organizations, providing scope and visibility that no organization can replicate on their own. This will provide continued value-add with the ZPA investment.

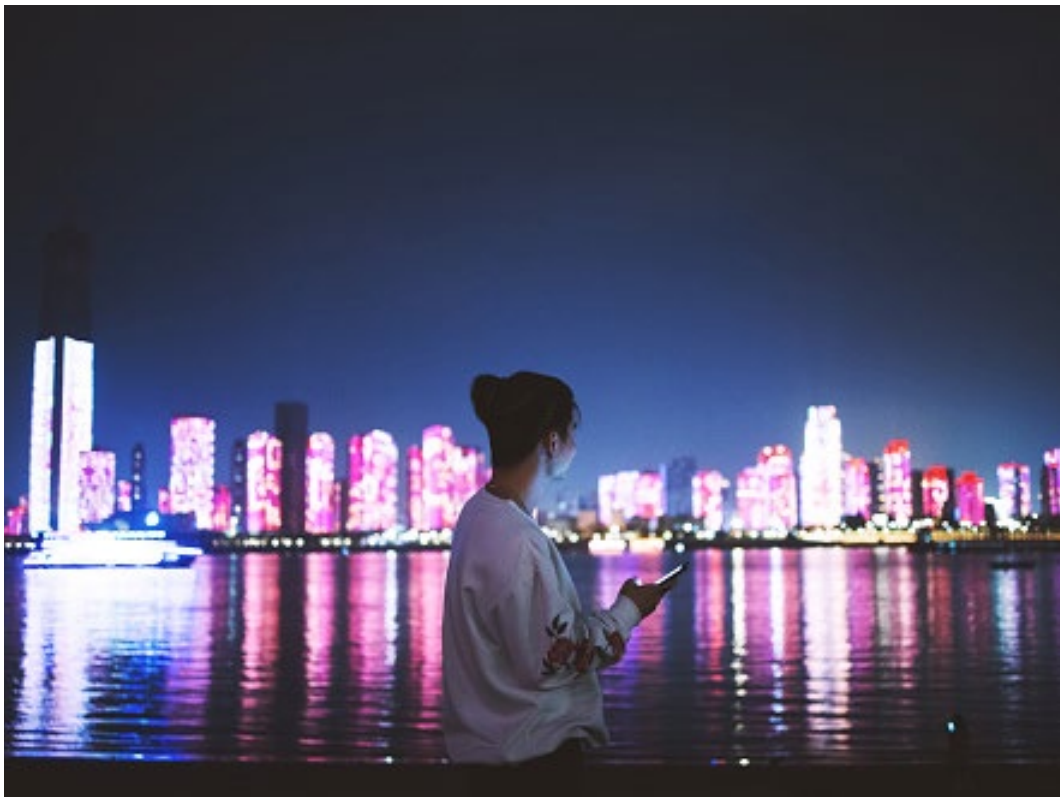
Traditional remote access VPN infrastructure presents a risk to any migration strategy, as it broadens the threat surface through always putting a user on the network.

Zscaler Private Access overcomes this risk by implementing the following four key security tenets:

- Connecting users to private applications (in VPC or physical DC) without bringing them onto any internal networks
- Never exposing applications to unauthorized users
- Enabling application segmentation without relying on complex and costly network segmentation, but closely aligned to VPC, Security Groups, and/or other service functions
- Using the Internet as a secure network transport without relying on VPNs that can increase the attack surface and complicate the user experience

This approach means that there can be no lateral movement to unauthorized applications. Furthermore, those applications that the user does not have access to remain completely dark; they cannot be discovered via port scans or any other mechanism, either locally or from the Internet directed at the hosted environment. Applications do not receive any inbound connections directly from users.

Customer Spotlight:
MAN Energy Solutions can now provide partner developer access to only the DevOps environments and apps required. Partner access had represented a potential attack surface; that is now contained, as their identity-based access controls keep these users and their devices off of the network.



Conclusion

The core function of Zscaler Private Access is to actively manage authorized user access to - and interaction with - workloads before, during, and after migration to the cloud, while improving the overall end user experience.

The primary transformation benefits include
- Reducing transformation and migration project timelines
- Enhancing the security posture with migrated apps
- Improved user experience during and following application migration

Use cases for ZPA adoption include
- Cloud adoption and application migration
- Mergers and acquisitions
- Third party access

Zscaler Private Access can be deployed in limited or all-in modalities. ZPA is built on AWS and ZPA Public Service Edge is deployed in AWS as well as other locations across the globe. Zscaler App Connectors are in VPCs. The Zscaler Client Connector is a light-weight app that supports all major PC and mobile device operating systems. Contact us for a free trial, a formal POC, or an incremental production rollout that takes the place of a POC. ZPA is available in the **AWS Marketplace** as a SaaS Contracts listing, supporting Private Offers.

References

Additional resources for your information.

Zscaler home page
www.zscaler.com

ZPA home page
www.zscaler.com/products/zscaler-private-access

ZPA for AWS home page
www.zscaler.com/products/zpa-for-aws

Support and technical docs
help.zscaler.com/zia?filter=documentation

MAN Energy Solutions
https://www.zscaler.com/resources/case-studies/man-energy-solutions.pdf

AWS Cloud Adoption Framework
aws.amazon.com/professional-services/CAF/

AWS Shared Responsibility Model
aws.amazon.com/compliance/shared-responsibility-model/

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.

Visit Zscaler in AWS Marketplace

aws marketplace

Zscaler, Inc.
Level 35, Tower One
100 Barangaroo Avenue,
Sydney 2000
+61 2 9225 7864
www.zscaler.com