Getting Started with Zscaler Private Access

Chris Hines, Head of Product Marketing (ZPA/Zscaler App), Zscaler
Kunal Shah, Principal Product Manager, ZPA
Zero Trust Network Access (ZTNA)

‘The old security mindset of “inside means trusted” and “outside means untrusted” is broken in the world of digital business.’

Gartner, Market Guide on Zero Trust Network Access
Steve Riley, Neil MacDonald, Lawrence Orans, April 2019

Read ZTNA Market Guide
It's time for a reality check.

The “defensible perimeter” no longer exists.

Security must be stronger and more scalable.
Zero trust network access

- Anytime security, from any device over the internet
- Decouple app access from network access
- Access is adaptive, identity-aware
- Private apps are made invisible to the internet
- “Virtual perimeters” around user, device, and app
Zero trust network access

- Anytime security, from any device over the internet
- Decouple app access from network access
- Access is adaptive, identity-aware
- Private apps are made invisible to the internet
- “Virtual perimeters” around user, device, and app

“By 2023, 60% of enterprises will phase out most of their remote access virtual private networks (VPNs) in favor of ZTNA.”

“By 2023, 40% of enterprises will have adopted ZTNA for other use cases.”

*Gartner, Market Guide on Zero Trust Network Access, April 2019*
Gartner recommends a ZTNA architecture

Market Guide for Zero Trust Network Access

Published 29 April 2019 - ID G00386774 - 24 min read

By Steve Riley, Neil MacDonald, Lawrence Orans

Zero trust network access replaces traditional technologies, which require companies to extend excessive trust to employees and partners to connect and collaborate. Security and risk management leaders should plan pilot ZTNA projects for employee/partner-facing applications.

Overview

Key Findings

- Digital business transformation requires that systems, services, APIs, data and processes be accessible through multiple ecosystems anywhere, anytime, from any device over the internet. This expands the surface area for attackers to target.

- Secure access capabilities must evolve to the cloud, where the users are and where the services and data are.
The advantage of this model is that no agent is required on the end user's device, making it an attractive approach for unmanaged devices. The disadvantage is that the application's protocols must be based on HTTP/HTTPS, limiting the approach to web applications and protocols such as Secure Shell (SSH) or Remote Desktop Protocol (RDP) over http. (See Figure 2 for a conceptual model.)

**Figure 2. Conceptual Model of Service-Initiated ZTNA**

**Conceptual Model of Service-Initiated ZTNA**

3. Authentication  
5. Session Established  
4. Verify Identity  
2. Connect to Provider  
1. Register Application  
          
End-User Device  
          
SDP Connector  
          
SDP Broker/Proxy  
          
Enterprise Directory  
          
Application

Source: Gartner (April 2019)  
ID 396294
Zscaler Private Access

Provides the experience users want with the security IT needs
Zscaler Private Access is a ZTNA implementation where...

1. Application access is decoupled from network access

2. Inside-out connections ensure private apps are invisible

3. Application segmentation does not require network segmentation

4. The internet is the new corporate network
Zscaler Private Access: Architecture overview

How it works...

1. An authenticated user requests access to an app

2. Policies determine if this user is authorized to access the app

3. If allowed, ZPA stitches inside-out connections from client to ZEN and from App Connector to same ZEN

Why it is more secure...

Users never connect to the corporate network
App access without network access

Apps are invisible to unauthorized users

App segmentation
Dynamic microsegments between users and internal apps

Increased visibility
Application discovery provides visibility into application landscape

Traffic Forwarding:
- Partners
- Employees
- Zscaler App

Identity provider

Multicloud: public/private

Data center

Security and Policy Enforcement

New York
London
Sydney

App Connectors
The advantage of this model is that no agent is required on the end user’s device, making it an attractive approach for unmanaged devices. The disadvantage is that the application’s protocols must be based on HTTP/HTTPS, limiting the approach to web applications and protocols such as Secure Shell (SSH) or Remote Desktop Protocol (RDP) over http. (See Figure 2 for a conceptual model.)

**Figure 2. Conceptual Model of Service-Initiated ZTNA**

**Conceptual Model of Service-Initiated ZTNA**

1. Register Application
2. Connect to Provider
3. Authentication
4. Verify Identity
5. Session Established

- **End-User Device**
- **SDP Broker/Proxy**
- **Enterprise Directory**
- **Application**
- **SDP Connector**

**Source:** Gartner (April 2019)

© ZenithLive, Inc. All rights reserved. ZISCALR CONFIDENTIAL INFORMATION
What Gartner recommends is the **ZPA architecture**

The advantage of this model is that no agent is required on the end user's device, making it an attractive approach for unmanaged devices. The disadvantage is that the application’s traffic must traverse an SDP Broker/Proxy that could intercept and compromise information. SDP Broker/Proxy solutions leverage protocols such as Secure Shell (SSH) or Remote Desktop Protocol (RDP) over http. (See Figure 2 for a conceptual model.)
Getting Started with ZTNA in the Real World
Four main enterprise ZPA use cases

- **VPN alternative**
- **Multicloud access**
- **Secure partner access**
- **Mergers & acquisitions**
Zscaler Private Access as a **VPN alternative**

**VPN alternative**

- **Risk**: is introduced as users are placed on network.
- **Complexity**: of ACLs make remote access complicated.
- **Users**: are frustrated with a slow and inconsistent experience.
- **Months**: are often spent getting appliance infrastructure set up.

Virtual private network (VPN) access

- Global Load Balancing
- DDoS
- External Firewall / IPS
- VPN Concentrator
- Internal Firewall
- Internal Load Balancer

Remote user

Trusted Network
Zscaler Private Access as a **VPN alternative**

Virtual private network (VPN) access

- Global Load Balancing
- DDoS
- External Firewall / IPS
- VPN Concentrator
- Internal Firewall
- Internal Load Balancer

Remote user

Zscaler Private Access

- Private Cloud / On-Premises DC

Policy Enforcement Checkpost

Remote user
Zscaler Private Access as a **VPN alternative**

**Always on** service provides **superior** end-user experience.

Apps are **invisible** to **unauthorized** users.

Policies are defined **once** and enforced **globally**.

**Eliminates** the risk of DDoS.
Zscaler Private Access for **access to public clouds**

Virtual private network (VPN) access

- Global Load Balancing
- DDoS
- External Firewall / IPS
- VPN Concentrator
- Internal Firewall
- Internal Load Balancer

Remote user

VPN software is **not** designed for public cloud access.

**Additional** latency from site-to-site tunnel provides poor user experience.
Zscaler Private Access for **access to public clouds**

**Virtual private network (VPN) access**

- Global Load Balancing
- DDoS
- External Firewall / IPS
- VPN Concentrator
- Internal Firewall
- Internal Load Balancer

**Zscaler Private Access**

- Public Clouds
- Private Cloud / On-Premises DC

**Policy Enforcement Checkpost**

Remote user

Remote user
Zscaler Private Access for access to public clouds

Users **always** connect to apps using the shortest path.

Eliminates **incoming** connections to public cloud instances.
Zscaler Private Access for **partner access**

**Contractor**

**Partners**

- **Limit visibility** only to the authorized applications.
- **Leverage identity** from partner identity provider while preserving full control of policy.
- Provide **Browser Access** to internal web apps without requiring Zscaler App.
- Quickly set up end-user **Portal** to provide visibility into allowed internal apps.
- **Gain** real-time visibility into partner access.

**Secure partner access**
Zscaler Private Access for **M&As and divestitures**

Internal apps in parent organization

Internal apps in acquired organization

Mergers & acquisitions
Provide access in **weeks** instead of months.

- Eliminates complexity of IP overlap and site-to-site tunnels
- Consume Identity ZPA supports MIDP; own policy and leverage multiple identity sources

Allows you to **retire** your M&A kit.

Provide a **standardized** remote access solution across business units.

IT becomes an **enabler** for acquisitions and divestitures.
ZPA Interactive

Free 7-day hosted demo of Zscaler Private Access!

https://www.zscaler.com/zpa-interactive
ENGAGE | In an open forum with Zscaler employees, partners, and customers

SHARE | Your knowledge and learn from experts in cloud security

JOIN | The conversation at community.zscaler.com
Thank You