Securing a Mobile Workforce with Zscaler App

Tony Fergusson, IT Infrastructure Architect, MAN Energy Solutions
David Creedy, Senior Product Manager, Zscaler
Your users are mobile…But what about your security?
Future in the making

Established in 1758
A subsidiary of Volkswagen Group

A German mechanical engineering company focused on engineering the future. From creating powerful engines, to new power solutions.
- Marine, energy & storage, Oil & gas, along with industry specific solutions

250+ years of advanced engineering
14,000 employees worldwide
120+ sites globally
Challenge for MAN Energy Solutions

How do we secure our employees’ access to enterprise applications while mobile or in a branch office?

How do we work with contractors and partners in a secure manner?

As MAN ES looks to expand, how do we secure these new users in new locations?
Securing a Mobile Workforce with Zscaler App
What is it?

Zscaler App
Enables secure mobile access to internet and SaaS applications and internal applications from any location and for any user.

Key feature
Auto-routes traffic through proper service
Seamless deployment via auto install and MDM
Selective entitlement for private app access

Benefit
Users no longer need to think about which apps are where
Simplify rollout onto all user devices
Enable internal access one use case at a time
Zscaler App

What is it?

Enables secure mobile access to internet and SaaS applications and internal applications from any location and for any user.

Supports laptops, phones, and tablets
- Windows, macOS, iOS, and Android

Integrates with MDM/EMM vendors
- Microsoft
- airwatch
- MobileIron
- IBM Maas360

Integrates with EDR vendors
- Carbon Black.
- SentinelOne
Zscaler App

Seamless user experience
Always-on for all devices
Knows when to forward traffic
Supports bypass configuration
Any app, anywhere, any device

Zscaler Internet Access
Full inline inspection to block the bad and protect the good

Zscaler Private Access
Connect an authorized user to an authorized internal app

Externally managed
Internally managed

Any app, anywhere, any device
Zscaler App
For secure internet and private access

Zscaler Internet Access
Secure internet access from anywhere
- Trusted network detection
- Compatible with other forwarding methods
- Works with existing Zscaler policies
- No backhauling traffic through corporate network
- Strict enforcement

Zscaler Private Access
Access to private apps from anywhere
- No VPN required
- No internal network visibility
- No network lateral movement
- No inbound ports required
- Mutually authenticated secure tunnel
- Transparent application access for users
3 reasons enterprises are choosing Zscaler App

Secure internet access
- Access to SaaS apps
- SD-WAN deployment

Secure access to private apps
- Contractors and consultants
- Access to cloud apps (AWS/Azure)
- M&A/data share

Seamless user experience
- Fast, secure access for all users globally
Enabling Mobility for MAN ES
MAN Energy Solutions

Just in the last three months, Zscaler App helped MAN Energy Solutions SE:

• 6.3 billion transactions processed
• 180.8 TB traffic (bandwidth) processed
• Total traffic from same time last year has grown by 13% — from 159.7 TB to 180.8 TB
• 416.5 million policy violations prevented
• 1.9 million security threats blocked

16,885
Zscaler App devices deployed
The Coffee Shop Solution

Corporate office

Z App creates a micro-perimeter around your client and extends this perimeter to the cloud.
The Coffee Shop Solution

On the road or at home

ZApp creates a micro-perimeter around your client and extends this perimeter to the cloud.
3 reasons enterprises are choosing Zscaler App

Secure internet access
- Access to SaaS apps
- SD-WAN deployment

Secure access to private apps
- Contractors and consultants
- Access to cloud apps (AWS/Azure)
- M&A/Data share

Seamless user experience
- Fast, secure access for all users globally
Secure internet access: Salesforce and SaaS

- Configure Zscaler as IDP for SFDC
- User is authenticated against Zscaler
- User accesses SFDC
- SFDC redirect to Zscaler for identity
- User is granted access
Zscaler App forwarding with SD-WAN
PAC and authentication bypass

Defined all Client traffic routing using namespace

Connect Tunnel

Connect Tunnel Using Global ZEN IP

SAP in cloud auth bypass
SEC ZEN

Office 365 in cloud auth bypass

PaaS
C4C
SAP Cloud for Customer

SaaS
Office 365

Applications
Network Filter Driver Z App
Fortigate SD-WAN
Client
Internet edge
3 reasons enterprises are choosing Zscaler App

Secure internet access
- Access to SaaS apps
- SD-WAN deployment

Secure access to private apps
- Contractors and consultants
- Access to cloud apps (AWS/Azure)
- M&A/Data share

Seamless user experience
- Fast, secure access for all users globally
Secure private access: Consultants & contractors

How do you securely publish an internal application to a third party without exposing your network?
Secure private access: Consultants & contractors
How do you securely publish an internal application to a third party without exposing your network?
Secure private access: **Consultants & contractors**

How do you securely publish an internal application to a third party without exposing your network?
Secure private access: **Consultants & contractors**

How do you securely publish an internal application to a third party without exposing your network?
Secure private access: **Consultants & contractors**

How do you securely publish an internal application to a third party without exposing your network?

- No network access has been granted, only [https://crm.company.com:443](https://crm.company.com:443)
- NSLOOKUP for crm.company.com will return a synthetic IP
- No inbound ports into the network
Secure private access: **Access to AWS and Azure**

Data center-to-cloud migration without exposing any connectivity
Secure private access: M&A/Data sharing

Enable multiple trusted networks and bypass the need for network consolidation

- **New beta feature:** Multiple trusted networks
- Define each office location as a specific trusted network
- Configure ZPA applications to tunnel or bypass based on that network
Multiple trusted networks

Tunnel or bypass based on location

Application A:
If “Office A” bypass
If “Office B” tunnel

Application B:
If “Office A” tunnel
If “Office B” bypass

Both offices are trusted networks
3 reasons enterprises are choosing Zscaler App

Secure internet access
- Access to SaaS apps
- SD-WAN deployment

Secure access to private apps
- Contractors and consultants
- Access to cloud apps (AWS/Azure)
- M&A/Data share

Seamless user experience
- Fast, secure access for all users globally
Seamless user experience with Zscaler App

• Load balancing for Z App is based on source and destination IP

• If devices are behind a NAT, they may get load balanced onto a single node

• Leverage ${GATEWAY\_FX}$ instead of ${GATEWAY}$
Load balancing in Z App

With and without ${GATEWAY_FX}$

Corporate network

$\text{NAT}$

Zscaler cloud

$\text{GATEWAY}$

$\text{GATEWAY_FX}$

Corporate network

$\text{NAT}$

Zscaler cloud
Lessons learned and recommendations

- Use filter driver, not routed mode
- Use Zscaler cloud upgrade process, not SCCM; Zscaler cloud upgrade is smooth
- Create profiles with different PACs ensure test, dev, QA, production rollout steps
- Use timeout policy to increase security and user ability
- Use debug logs and packet capture for troubleshooting
In an open forum with Zscaler employees, partners, and customers

Your knowledge and learn from experts in cloud security

The conversation at community.zscaler.com
Thank You