Why ZTNA Spells the End of Remote Access VPN… & More

Pierre-Antoine Falaux-Bachelot, VP Systems Engineering, Engie
Scott Bullock, Technical Marketing Engineer, Zscaler
50% have two or more different clouds deployed

Agile, scalable, and seamless implementation

Business productivity via mobility

Dream
Securing your cloud transformation

Constant struggle to protect the business

Security at the expense of user experience

Reality

NotPetya

WannaCry

iEncrypt
Key trends Gartner says will redefine security

More users outside the enterprise

More unmanaged devices than managed

More apps delivered from outside enterprise

Access capabilities must evolve to the cloud – where users are, and where apps are moving.
VPN: The first approach to remote access

Remote users placed on network via IPsec tunnel

Lack of scale slows experience

Malware spreads laterally

Even as you move to cloud…
Zero Trust 1.0: VLAN and FWs and IPS

Network segmentation and virtual VLANs add complication

Users still placed on net and can get to anything that isn’t fully locked down
Securing your cloud transformation

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*
Zero Trust Network Access (ZTNA)

Inside-out connections make apps invisible to Internet

Users are never placed on the corporate network
Instead: Decouple app access from network access

**Network – Centric**

- Secure the corporate network to protect users and data
- Build a security moat of appliances to protect the network

**User – Centric**

- Securely connect users to apps or services
- Decouple network access from application access
Our belief in a “Service-Initiated” Architecture

- Apps remain cloaked to the Internet
- No exposure means no DDoS attacks
- Native app segmentations
- Secures access from managed & unmanaged devices

**Gartner, Market Guide for Zero Trust Network Access (ZTNA), April 2019**
Leverage scalability of cloud-delivered ZTNA

Best of both worlds

Faster user experience
Traffic path optimized based on closest cloud access point

Less cost to maintain
Cloud brokers are updated and managed by the service provider
Zscaler Private Access: fast and secure access to private apps

How it works:

1. Authenticated user requests access to an app.
2. Policies determine if the user has access to the app.
3. If allowed, the cloud establishes inside-out connection from App Connector to ZEN and client to same ZEN.

ZTNA approach:

- Remote users never brought on the corporate network.
- App access without network access.
- Apps are invisible: not exposed to the internet.
- Native app segmentation: Micro-tunnels connect authenticated user to authorized application.
Four main enterprise use cases

Business partners
- Control third-party access
- Minimize lateral movement to other apps
- Never place them on-net
- Gain visibility into activity

M&A
- Simplify IT integration during M&A to weeks
- Minimize network converge
- Reduce cost of appliances & additional infrastructure
- Standardize security across all entities

VPN alternative
- Remove inbound VPN gateway appliances
- Users never placed on-net
- Application segmentation by default
- Prevent inbound connections to apps

Multi-cloud access
- Avoid lock-in/enable multi-cloud strategies
- Provide secure access across hybrid cloud apps
- Improve user experience
- Streamline adoption of IaaS

Zero Trust Network Access
Embracing ZTNA at Engie
We make the zero carbon transition as a service* possible for our customers

**Produce**

Centralized and decentralized production and sale of low CO₂-emitting electricity, including renewable energies.

- The world’s leading independent power producer (IPP)
- 104.3 GW\(^1\) installed
- 93% of low CO₂-emitting activities
- The leader in wind and solar power in France

**Distribute**

Distribution, transportation and storage of gas and electricity upstream of supply to customers.

- The European leader in gas transportation and distribution
- 4,500 km of gas pipelines in Brazil
- The first demonstrator of the injection of green hydrogen into the gas distribution network in France
- A 600 km electricity grid between northern and central Chile

**Customer solutions**

Development of unique integrated solutions to support the transition to zero carbon of businesses and local authorities.

- 24 million contracts worldwide
- N°1 worldwide in cold networks
- N°2 worldwide in recharging systems for electric mobility
- N°1 worldwide in micro-grids

---

\(^1\) On 31/12/2018, at 100 %, *competitive, co-funded, made to measure*
Our worldwide presence*

160,000 employees
€60.6 billion in revenue
€2.5 billion recurring profit after tax
€11 billion of planned investment in growth in 2019-2021

*on 31/12/2018
Zero Trust Network at Engie
Our Goals

- Make every internal application a Cloud App
- User or Business Partner, not a security risk
- Keep business secured
Do you trust?

Internet is the Network
Home Office
Road Warriors

Password are weak
Partners

BYOD
Partner computer
Mobile devices

Network

Users

Workstation

VPN
## Initial use cases of ZPA within Engie

### VPN Replacement

**End User**
- Simple access to Apps
- No difference in or out network
- Applications on multiple DC
- SSO Apps

**IT Admin**
- Fine grain access
- Admin protocols
- MFA is mandatory
- Delegate to external partners

### Partner Access

**Remove IPSec**
- Time to deploy
- No change for user
- Multiple DC
- Enforce security
- Decouple from the workstation

### Application access

**Mobile access to internal Apps**
- Android tablets
- No impact on application, no redesign
- User Experience
- Integration with MDM
Main components

Authentication

Logging

Datacenters

Client Management
Recommended Resources

Gartner
• Market Guide for Zero Trust Network Access

Zscaler
• ZPA product page – https://www.zscaler.com/products/zscaler-private-access
• Demo: Take ZPA for a free test drive with ZPA Interactive

Try ZPA Now!
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