

Zscaler™ Enables Network and Application Transformation for MAN Energy Solutions



MAN Energy Solutions

man-es.com

Location: Augsburg, Germany

Industry: Manufacturing and Transportation Services

User Count: 12,000 users in over 100 locations and 70 countries

Zscaler Products: Zscaler Private Access (ZPA), Zscaler Internet Access (ZIA)

MAN Energy Solutions, based in Augsburg, Germany, is the world's leading provider of large-bore diesel engines and turbomachinery for marine and stationary applications. It designs two-stroke and four-stroke engines that are manufactured both by the company and by its licensees. MAN Energy Solutions also designs and manufactures gas turbines. The product range is rounded off by turbochargers, propellers, gas engines and chemical reactors.

Challenge

While experiencing global growth of the business, there are rapid changes occurring in technologies such as IoT on engines and systems of all sizes deployed around the globe, many of which are in motion in transportation. At the same time, a large and distributed global workforce are increasingly mobile and requiring **mobile access** to web apps and custom business applications.

The traditional castle and moat approaches to network and app **security** are mismatched to the modern cloud deployments which enabled global scale, global access, and the potential for an improved security posture as workloads migrated to AWS and Azure, and the internet became the new corporate network. What is desired is to make these applications dark to the internet, with authenticated access only between trusted users and trusted applications.

MAN Energy Solutions found that the improved **speed and agility** gained in cloud deployment was being offset by a poor user experience

“The Enterprise IT landscape is changing with the adoption of mobility and cloud services, and enterprises need to change their architecture to meet the growing needs of securing users from anywhere on any device.”

– Tony Fergusson
IT Infrastructure Architect
MAN Energy Solutions

associated with accessing apps through legacy corporate VPN solutions, with increasing appliance, software, and MPLS networking costs. Furthermore, there was a desire to gain security advantages associated with making the apps invisible on the internet.

“We were providing application access to a distributed, mobile workforce using traditional VPN to discoverable access ports. Performance was suffering. Our employees were not satisfied with their experience. Our

security stance was not realizing its potential. This was inconsistent with what our AWS and Azure deployments could provide,” says Tony Fergusson IT Infrastructure Architect for MAN. “Also, we have a relatively small operations team managing on-premises infrastructure, while our data set and need for real-time analytics and app access was exploding. That was getting more difficult to do as we modernized our internal applications, brought more data sources online, and deployed advanced products and technologies globally.”

Why Zscaler

For MAN Energy Solutions (MAN), moving to the cloud provided clear advantages for realizing its business challenges. “We continued to see more companies successfully implementing global scale use cases to the cloud, and we identified architectural approaches that fit our technical objectives,” Fergusson says.

MAN turned to Zscaler in 2011 to improve user experience, reduce bandwidth cost, and meet increasing security objectives. MAN started by connecting globally distributed mobile users to their SaaS applications using Zscaler Internet Access (ZIA). Zscaler was later selected to address advanced persistent threat (APT) requirements. Next, Zscaler Private Access (ZPA) was selected to provide anywhere any time access for the mobile workforce and contractors to apps running on premises. Most recently, ZPA was introduced for secure access to apps running on AWS and Azure, improving mobile user experience while reducing networking costs.

Zero Trust Access to Internal Applications

Zscaler Private Access (ZPA) provides policy-based, secure access to private applications and assets without the cost, complexity, or security risks of a VPN. The idea of making the internal applications “dark” to unauthorized users has gained momentum since the introduction of Software Defined Network (SDN). The Zero Trust Model approach makes your services invisible, and both apps and users need to be authorized using SAML before user access is established.

“We were able to implement a zero trust model, or what I call [Blackcloud \(SDP\)](#),” said Mr. Fergusson. “We have

BENEFITS

- Delivers a better experience for end users
- Reduced attack surface via application access without network access
- Enables strong authentication and granular application access control, globally
- Ability to deploy, and securely access and manage VPCs
- Ensures optimal path between users and apps for increased performance
- Increased visibility into applications and user activity

implemented our solution so as to reduce our attack surface, 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.” With ZPA, contractor access is segmented by application, not network.

This approach also prevents the ability for malicious software to move laterally. It ensures that access is initiated only by a client to a server, and never the other way around. Combining these two paradigms prevents malicious lateral movement by validating all sessions before access is granted. Thus greater security is achieved by assuming a zero trust model, and enforcing policy based on user authentication, authorization, and known and unknown applications.

A Modern Approach to Connecting Users on a Global Scale

There were a number of business drivers that required a faster, more secure way of connecting end users to their apps, including the migration of internal business apps and development projects to the cloud, increased adoption of cloud services, and the need to roll out access to a growing set of globally distributed employees and partners. While this provides increased business flexibility and agility, if they were to continue to rely on traditional VPN approaches it would increase the burden on both IT and network resources.

The Zscaler cloud provides an elegant and powerful alternative. It removed the need for traditional hardware and software security stacks for remote access, eliminates the need for end users to use a VPN client and remote access heuristics when traveling, and it provides an alternative path for traffic. This reduces the need for MPLS tunnels for internet-based connectivity.

Gaining Speed, Agility, and Performance

MAN Energy Solutions improved the end user experience while reducing complexity and costs. End users now have a completely seamless, cloud-like experience when accessing internal applications, regardless of whether the applications is running in the datacenter or cloud. Users are taken direct to applications, via the global Zscaler cloud, completely bypassing traditional

remote access choke points. This provides complete flexibility of where applications are hosted, and protects sensitive data with a TLS-based encrypted micro tunnel connection. Users are never placed on the network, applications are never exposed to unauthorized users and cloud reduces complexity typically introduced by traditional solutions.

Double-digit percentage reduction in costs were realized by eliminating VPN infrastructure and software licensing. Furthermore, network performance was improved by utilizing bandwidth controls to prioritize mission-critical traffic over lower priority traffic, such as web browsing.

One of the main technical benefits is that their team was able to reduce their attack surface and secure all administration into AWS and Azure. MAN utilizes ZPA's logging and analytics cluster for log streaming to their SIEM for increased visibility into user access and activity.

"We can deploy new VPCs, and create new namespaces, within minutes. The big advantage for us is using namespace routing, so we can control traffic based on namespace, not IP. This allows us to create meaningful policies. We can decrease network cost and complexity. Our consultant onboarding process is much faster. We can now onboard within hours, rather than weeks," said Mr. Fergusson.

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.

