perimeter 81

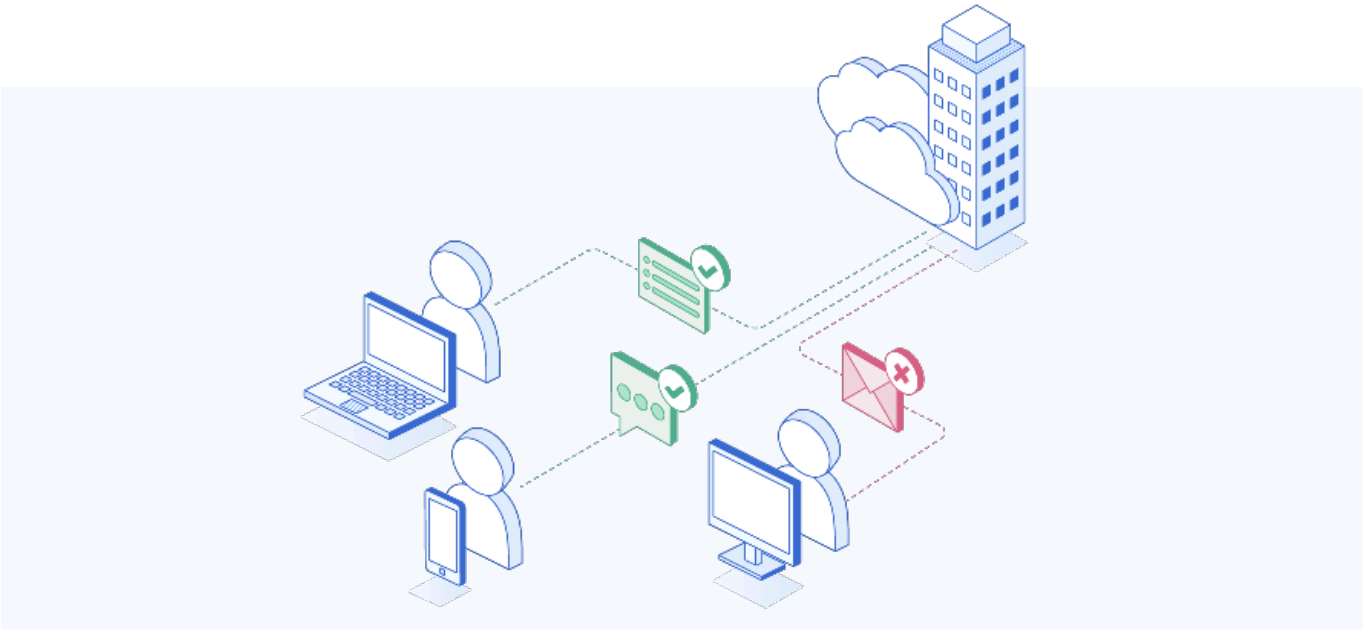
Deploying Zero Trust Cloud Network Services for the Enterprise

Introduction

Zero Trust (ZT) is a security concept based on the belief that organizations should not automatically trust anything inside or outside its perimeters but instead verify anything and everything trying to connect to IT systems before granting access. This Zero Trust model approach to secure network access services allows for the delivery of high-security, enterprise-wide network service virtually, on a subscription basis for small and mid-market companies to large enterprises.

"Companies cannot afford to trust internal network traffic as legitimate, nor can they trust employees and partners to always be well-meaning and careful with systems and data. To manage the complexities of their environment without constraining their digital transformation ambitions, many companies are moving toward a Zero Trust (ZT) security model — a more identity- and data-centric approach based on network segmentation, data obfuscation, security analytics, and automation that never assumes trust," states analyst firm Forrester Research.

Today's digital businesses need security technology partners that offer a range of capabilities that are easy to use and integrate, improve their network visibility and support the ZT model. The modern enterprise places high value on partner solutions, such as Perimeter 81, that can apply security controls across environments uniformly and quickly, with features that allow them to modify security policies and access as business needs change.



1 https://www.csoonline.com/article/3247848/network-security/what-is-zero-trust-a-model-for-more-effective-security.html

Zero Trust Security Models and Microsegmentation

When implementing a Zero Trust security architecture, IT managers must isolate resources within their IT infrastructure in the form of micro-segmentation. Forrester Research recommends dividing network resources at a granular level, allowing organizations to tune security settings to different types of traffic and create policies that limit network and application flows to only those that are explicitly permitted. This network microsegmentation approach allows security teams the flexibility to apply the right level of protection to a given workload based on sensitivity and value to the business.

Utilizing the ZT security model with micro-segmentation features, Perimeter 81's enterprise and SMB cloud-based secure network access solution quickly and easily secures on-premises and cloud resources combined with lightweight cross-platform client support for employee access, all controlled through a single management console.

Mobile employees are protected with Perimeter 81's Single Sign-On native client applications that can be used on any Windows, Mac, iPhone and Android device. Perimeter 81's innovative Automatic Wi-Fi Security also shields all data by automatically activating encrypted protection when employees connect to unknown or untrusted networks.

With centralized control and identity management integrated into the Perimeter 81 portal, employees and groups can easily be added to corporate network resources and cloud environments with secure policy-based resource access. Detailed activity reports provide insight into resource and bandwidth utilization while active connection and session information can be monitored.

Finally, all company data passing over any network is secured with 256-bit bank-level encryption and routed through a dedicated private server concealing a company's actual IP address with an IP mask. Perimeter 81 provides a global network of over 700 high-speed public servers in more than 34 locations, as well as fast and simple deployment of private gateways with dedicated IP addresses.

Additional Perimeter 81 platform key features include:

- SSO, SAML, AD integration
- Full auditing and monitoring
- Fast gateway deployment
- Easy network segmentation
- Rapid anomaly detection
- Web and mobile support

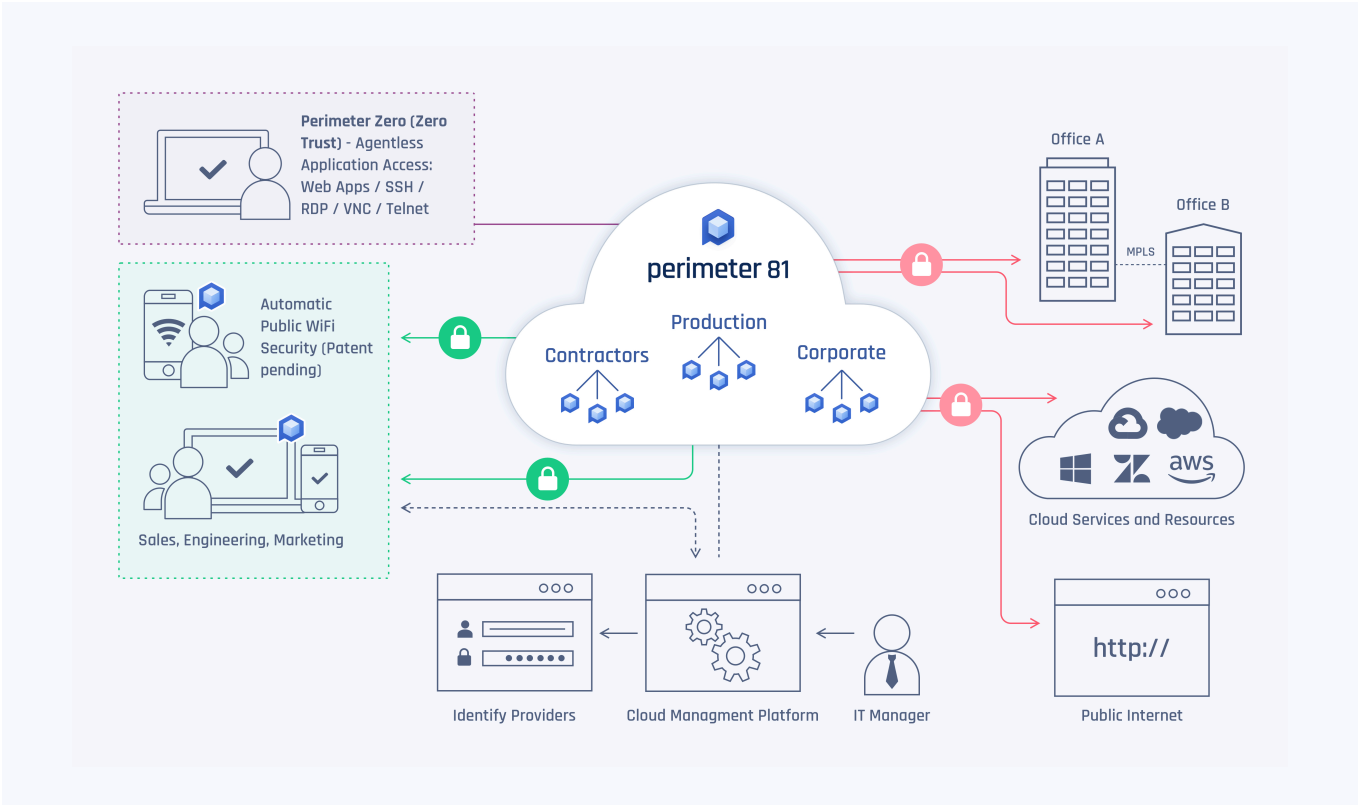
2 https://www.csoonline.com/article/3247848/network-security/what-is-zero-trust-a-model-for-more-effective-security.html

Traditional VPNs and the Need for Software-Defined Perimeters

At the core of the Perimeter 81 platform is the Software Defined Perimeter, a security that model addresses traditional VPN limitations while providing a flexible cloud-based platform, device and application configurability as well as accessibility, increased security, privacy and user-access control granularity and analytics.

Within the SDP security model, the concept of Zero Trust or micro-segmentation functions as a trust broker between a client and a gateway by establishing a Transport Layer Security (TLS) tunnel terminating inside the network perimeter, thereby allowing access to applications and services.

According to the Cloud Security Alliance (CSA), Software Defined Perimeters provide "the ability to deploy perimeters that retain the traditional model's value of invisibility and inaccessibility to "outsiders," but can be deployed anywhere – on the internet, in the cloud, at a hosting center, on the private corporate network, or across some or all of these locations. The SDP brings together standard security tools including PKI, TLS, IPsec, SAML, and standards, as well as concepts such as federation, device attestation, and geo-location to enable connectivity from any device to any infrastructure."



2 https://www.csoonline.com/article/3247848/network-security/what-is-zero-trust-a-model-for-more-effective-security.html

User-Centric Software-Defined Perimeter Security Model

The CSA defines a Software-Defined Perimeter in terms of a network security model that dynamically creates one-to-one network connections between the user and only the resources they access. The components include verifying the identity of the user, their devices, and role before granting access to network resources.

This network security model based on authentication and authorization prior to network access has been in use by the US Department of Defense and Intelligence Communities for some time and is known as “need to know” access. The security model calls for every server to be hidden behind a remote access gateway that users must authenticate into and gain access before any authorized service is made available. The innovation behind Software-Defined Perimeters is the integration of device authentication, identity-based access and dynamically provisioned connectivity.

According to Gartner, the advantage of the SDP model is that “traditional attacks that rely on the default-trust flaws built into traditional TCP/IP will be thwarted when using SDP because any non-SDP trusted traffic is discarded prior to stack processing. SDPs address some of the most common network-based attacks such as server scanning, denial of service, SQL injection, OS and application vulnerability exploits, password cracking, man-in-the-middle, cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks.”

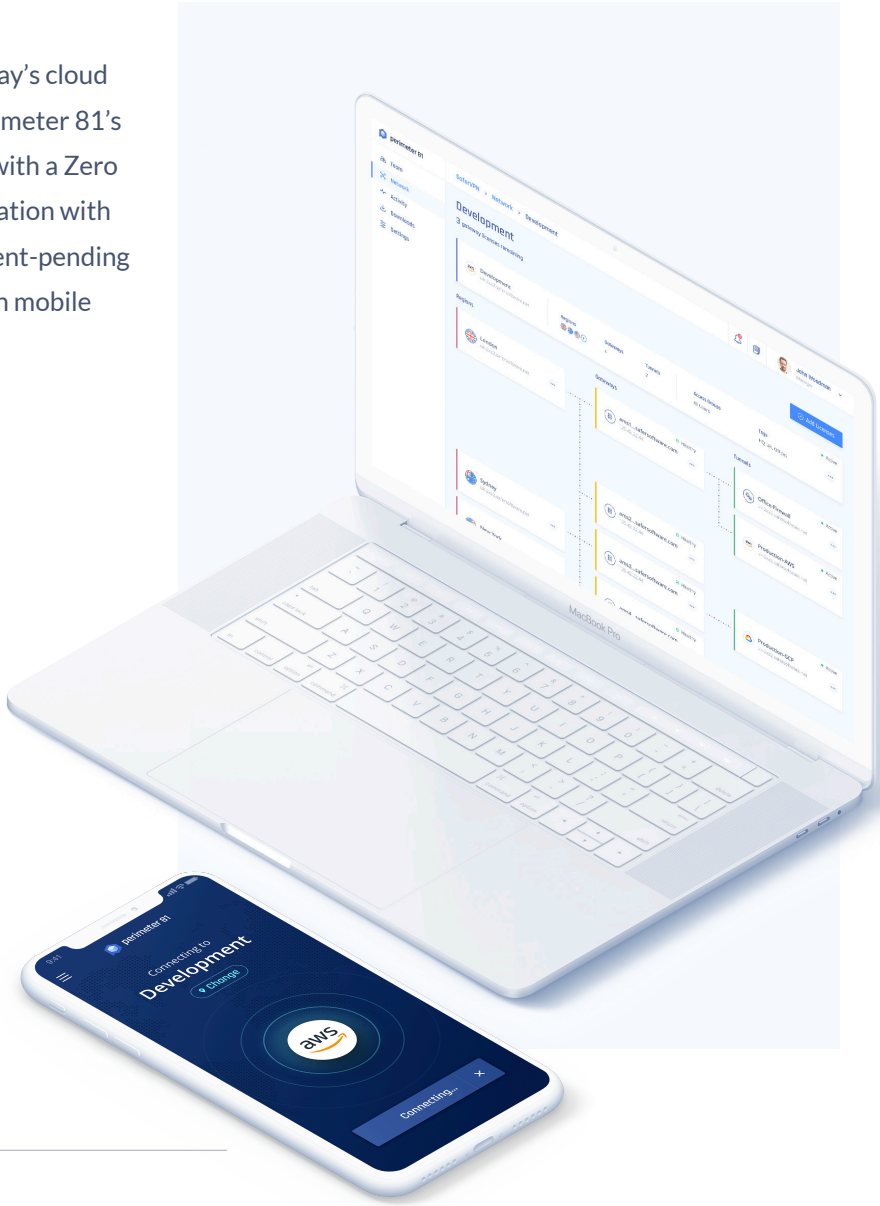
The challenge for IT managers is to provide secure and reliable employee access without draining IT resources and budgets. Traditional VPNs can be complicated to deploy and maintain, both from a hardware and software perspective. This includes the integration of physical servers and site-specific applications, cloud-based infrastructure and applications and identity access and management. Therefore, IT managers must look beyond traditional VPNs to cloud-based VPNs that can be quickly deployed and configured in a Software Defined Perimeter configuration.

Perimeter 81 Benefits

Configuring, operating and integrating Software-Defined Perimeter (SDP) architectures, cloud VPNs and identity access management services without a 3rd party managed platform can be complicated. By using a Zero Trust, cloud-based secure network access solution with multi-tenant management capabilities, however, all network services can be handled by the third-party for monitoring client remote access and endpoint security with complete ease.

Traditional VPNs are no longer relevant in today's cloud and mobile-first technology environment. Perimeter 81's cloud-based secure network access platform with a Zero Trust security model provides seamless integration with all leading cloud providers combined with patent-pending automatic Wi-Fi protection for today's modern mobile workforce.

Perimeter 81's scale-as-you-go software service also requires no expensive hardware installations, offering thousands of dollars in yearly cost-savings. With SaaS-based pricing, enterprises can pay as they go without any large upfront costs.



About Perimeter 81

Perimeter 81 is a cloud-based, Secure Network as a Service provider, driven by the mission to transform secure network access for the modern and distributed workforce. Built from scratch based on input from security leaders needing a change from legacy VPN technology, Perimeter 81's user-friendly interface, unified management and seamless integration with major cloud services, allows employees to securely access on-premise and remote resources, and gives companies of all industries and sizes the power to be fully mobile and confidently cloud-based.

Contact Us

www.perimeter81.com

+1-646-518-1997

Request a Free Demo

Follow Us




Blog

perimeter 81