perimeter 81

SDP vs. VPN: Advantages of Implementing an SDP Solution Over a Traditional VPN

Introduction

Providing employees, partners and customers with remote access to servers, applications and network resources, on-premise or in the cloud used to be rare, yet now it's the norm. At the same time, technologies such as Virtual Private Networks (VPNs) that provide remote access functionality has not kept pace with the security requirements and ever-evolving threat landscape of today.

The legacy VPN was introduced over 30 years ago. It enables secure, remote access to the Internet through a point-to-point connection by creating an encrypted 'tunnel' through which IP traffic flows. However, VPNs can make enterprises more vulnerable to attacks and data breaches because they give users within the organization access to the entire internal network in order to access company resources. Users are not restricted to specific network resources, making VPNs one of the weakest points of failure with respect to identity access and credential management. There is no segmentation, audit or control.

Critical VPN limitations include lack of network segmentation, traffic visibility, on-premises user security as well as lack of secure network security. VPNs are also not suited for dynamic networks because they require computer hardware, constant management and cannot easily adjust to network or server changes. This makes it more complicated to scale and rapidly adjust for new users and network locations and increasingly difficult to effectively manage hybrid and cloud-based computing architectures.

In contrast, the Software-Defined Perimeter (SDP) security 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.

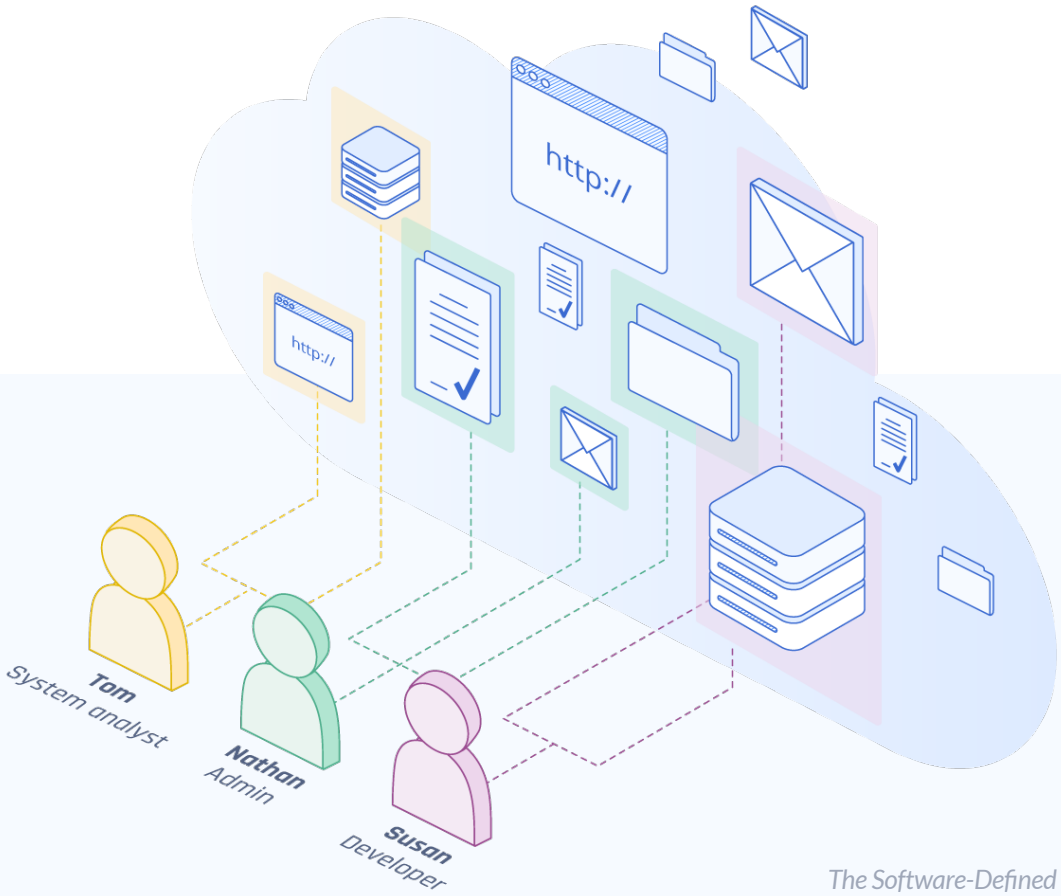
"With SDP, organizations can have a multi-region and policy-driven network security platform that covers their entire infrastructure (both on-premises and cloud) and their entire user population. This is a compelling vision – but one that's realistically achievable with SDP. Numerous organizations worldwide have used SDP to increase their security stance, reduce their attack surface, increase business and IT staff productivity, and reduce their compliance burden – while saving money," according to the Cloud Security Alliance (CSA).

By reducing the attack surface of exposed hosts, SDPs create a "least privileged access" model of security for servers and network resources to help reduce data breaches and data loss, system and application vulnerabilities, advanced persistent threats (APTs), denial of service attacks, account hijacking and malicious insiders.

User-centric Software-Defined Perimeter Security

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 secure integration of authenticated mobile devices such as tablets and phones or PCs, control over which users can access network resources and at what level, and dynamically provisioned connectivity through the use of VPN technologies.



The Software-Defined Perimeter

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.

Benefits at a Glance: SDP vs VPN

SDP

- ✓ Adaptive to every network
- ✓ Global access
- ✓ Precise segmentation
- ✓ Secured & encrypted
- ✓ Policies based on users
- ✓ Seamless audit and report
- ✓ Rejects account hijacking
- ✓ Reduced costs
- ✓ Least privilege access

VPN

- ✗ Zero automation of network policies
- ✗ Lack of remote user security
- ✗ Doesn't integrate with identity providers
- ✗ Weak network traffic visibility
- ✗ Unable to create identification rules
- ✗ No network activity reports
- ✗ An easy target for hackers
- ✗ Implementation can be costly
- ✗ Easy access to unauthorized users

Zero Trust and Software-Defined Perimeters

Zero Trust (ZT) security is 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. 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.

Configuring, operating and integrating cloud security services without a 3rd party managed platform can be complicated. By using a Zero Trust (ZT), 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.

According to analyst firm Forrester Research, “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 towards a Zero Trust security model — a more identity- and data-centric approach based on network segmentation, data obfuscation, security analytics, and automation that never assumes trust.”

This Zero Trust model approach to secure network access services lets organizations deploy a managed high-security, enterprise-wide network service virtually, on a subscription basis.

Software-Defined Perimeter Use Cases

Secure Remote Access

SDPs act as a VPN replacement for mobile and remote employees with company-owned devices or third-party contractors and business partners using their own devices that are given specific access to networks, applications and cloud resources.

Software Defined WAN (SD WAN)

remote office/branch offices (ROBO) offices with secure network access using IPSec tunneling over the public internet without the need for on-premise hardware. SD-WANs manage the IP networking infrastructure while SDPs secure connections, cloud resources and users.

Multi-cloud Connectivity

Connect to and manage all on-premises and public cloud resources based on policies to isolate services from unsecured networks.

Identity and Access Management (IAM)

Manage and authenticate identities and user account roles that enable access to secured infrastructure, platforms, applications and cloud services.

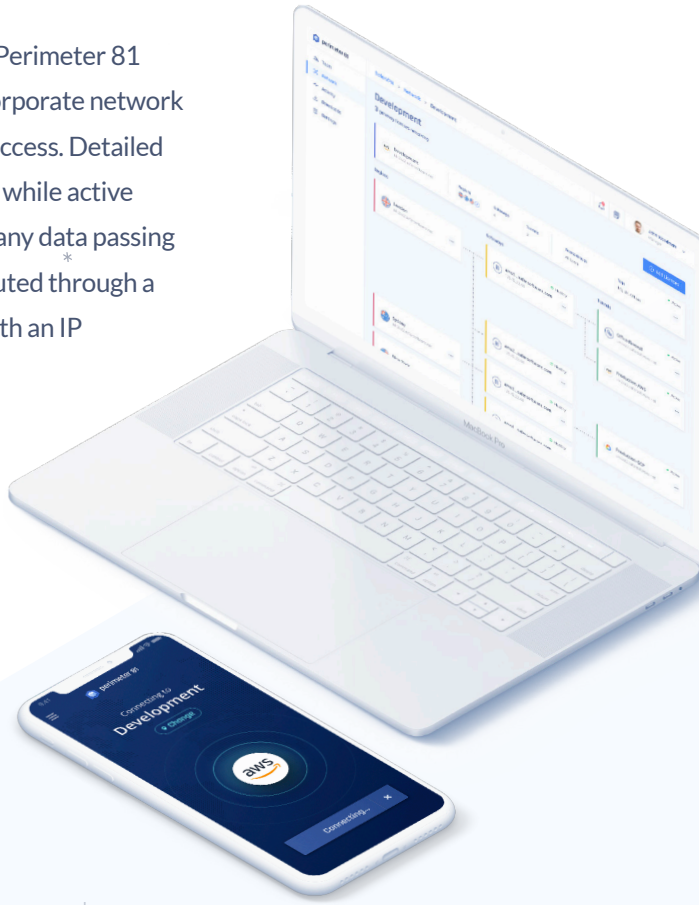
Zero Trust Security and the Perimeter 81 Solution

To implement a ZT security architecture combined with a SDP, 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 micro-segmentation 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 SDP, Perimeter 81's secure network access solution quickly and easily secures access to on-premises and cloud resources, as well as web applications. With a single management console, Perimeter 81 offers user-centric and adaptive, policy-based network access to on-premise resources, SaaS applications and cloud environments; interconnectivity among cloud environments and different network branches; and fully audited agentless access to web applications, SSH, RDP, VNC or Telnet.

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 devices. Perimeter 81's innovative Automatic Wi-Fi Security also shields all data by automatically activating protection when employees connect to unknown or untrusted networks.

With centralized control and identity management integrated into the Perimeter 81 management platform, 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 gateway concealing a company's actual IP address with an IP mask.



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, organizations can pay as they go without any large upfront costs and get up and running quickly without tedious configurations while all updates and upgrades are deployed through the cloud, making maintenance instant and easy.

About Perimeter 81

Perimeter 81 is a Zero Trust Network as a Service that has taken the outdated, complex and hardware-based traditional network security technologies, and transformed them into a user-friendly and easy-to-use software solution — simplifying secure network access for the modern and distributed workforce. Perimeter 81 serves a wide range of businesses, from midsize to Fortune 500 companies, and has established partnerships with the world's foremost integrators, managed service providers and channel resellers.

Contact Us

www.perimeter81.com

+1-646-518-1997

Request a Free Demo

Follow Us




Blog

perimeter 81