Meta Networks

Whitepaper

SDP vs VPN

5 Reasons to Make the Switch

Traditional VPNs were invented more than 20 years ago, at a time when all enterprise apps were hosted in local data centers and most employees were working on-premise. Cloud infrastructure, virtualization, and microservices architectures were nowhere in existence, and the the site-centric security model worked just fine to connect a few C-level managers working remotely to the enterprise data center.

It's a different world today. The network perimeter that VPNs were designed to protect has essentially dissolved. A typical enterprise has dozens, and often hundreds, of applications hosted on public clouds like Amazon AWS. Instead of a few remote employees, the number of users working from homes, hotels, airports, and customer sites is enormous. A recent study found that 70 percent of professionals work remotely at least one day a week, while 53 percent work remotely at least half of the week.

A new solution, or what is often called 'a next generation VPN' is required to enable remote access to today's distributed corporate networks. In Gartner's words, "enterprise access requirements are growing ever more complex due to application dynamics, cloud adoption and mergers. To cut through this complexity, technical professionals should explore Software Defined Perimeter (SDP) — a new technology whose strength lies in facilitating access to enterprise apps."

This paper examines SDPs as a compelling alternative to traditional VPNs that allows organizations to standardize remote access security for all users, scale them more economically, and reduce the potential risk of attacks.

What is a Software-Defined Perimeter (SDP)?

An SDP is a network security framework that provides secure access to enterprise apps.

The term "perimeter" often creates confusion, since it is traditionally associated with a network perimeter and elements like demilitarized zones (DMZs) and firewalls. However, despite the somewhat confusing term, SDP takes the exact opposite approach. Unlike traditional architectures which separate the enterprise network from the outside world by a fixed perimeter, SDP dynamically creates one-to-one network connections between each user and the resources he/she accesses. All unauthorized network resources are inaccessible.

As implied by its name, an SDP is implemented in software on end-user devices, gateways, controllers or servers. It can be deployed either as a stand-alone product (deployed on-premise in data centers) or as a service (hosted on the cloud).

In this paper we focus on cloud SDPs, delivered as a service.

1 Tighter Security

SDPs provide tight control over data access, reducing the attack surface and risk to the enterprise network.

Network-centric vs. zero trust

Reliance on a network-centric security model is probably the top security limitation with VPNs. Once a remote user is authenticated, he/she is considered trusted. Consequently, VPN access is overly permissive, granting remote workers access to more of the network than is required to complete their tasks. Network resources are unnecessarily visible, overly vulnerable, and open to attack.

A software-defined perimeter, on the other hand, takes on an identity-based, zero-trust approach that enforces a custom policy for each user device. Each connection is treated as untrusted and, therefore, is verified continuously. Users have a unique, fixed identity and an IT administrator must grant permission for a one-to-one connection between a user and the resources that he/she needs to access. All unauthorized network resources are simply invisible.

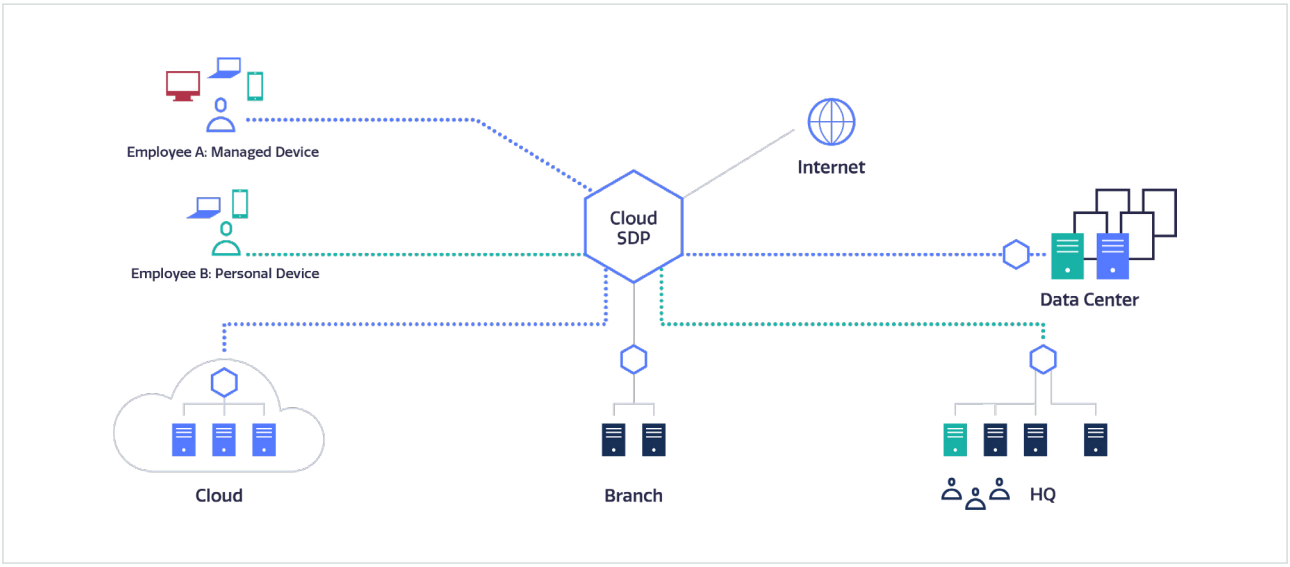
Exposure to DDoS attacks

Traditional VPN gateways can be discovered with reconnaissance methods and fall victim to distributed DoS (DDoS) attacks. An on-premise SDP solution - or better yet - a cloud-hosted SDP essentially disables reconnaissance attacks.

Access capabilities

In addition to identity-based security, some SDP solutions provide extended capabilities, or what Forrester calls 'Next Generation Access (NGA) capabilities, which includes:

- Correlation between access and user behavior. For example, the continuous authentication and verification of the user and/or device at the packet level using identity-based networking technology.
- Multi-factor authentication - to reduce access threats
- Single sign-on (SSO) - to centralize identity management



Unlike VPNs' overly permissive access, SDPs enforce restricted, identify-based access. Here, we see that Employee A can access one application in the data center and one in the cloud, while Employee B can only access a single application at HQ.

2 Concurrent Access to Multiple Apps and Clouds

VPNs were never designed for hybrid clouds and distributed cloud computing. It's not uncommon for a sales person working remotely to require access to a manufacturing system in the data center, a supply chain app hosted on AWS, and a CRM system hosted on Azure.

Facilitating such multi-app, multi-cloud access at scale for many users isn't that simple with VPN. It makes no sense to backhaul remote users' traffic through corporate headquarters only to send it back out to the relevant public cloud. The alternative - setting up secure access directly to multiple public clouds - is unmanageable.

From an end user's perspective, working remotely with multiple apps using a VPN translates to an annoying stream of connecting and disconnecting to different resources. In some cases, users must even switch between several VPN clients.

In contrast, SDP architecture inherently supports multi-app, multi-cloud connectivity, enabling clients to establish and maintain concurrent encrypted tunnels between many applications and service endpoints.

> With the new system, each user is only exposed to the specific applications he or she needs, regardless of which data center it's located in. Compared to managing VPNs in each of our data centers, this is much simpler and more convenient both for both our IT team and for our users."
>
> MyHeritage Read case study

3 Simplified Management

VPN management balloons in complexity as more and more enterprise applications are moved to the cloud. Rarely does a cloud deployment involve just a single cloud instance. At many SaaS vendors, IT must provide access to dozens or hundreds of instances in multiple cloud providers, which means deploying, configuring and maintaining VPNs for every instance.

Consider a SaaS company where administrators must provide access to 200 VPCs on AWS and Azure, over dedicated VPN connections. In addition to setting up a virtual private gateway for each AWS VPC, corresponding configuration files need to be installed and maintained on each gateway device at each office. This can quickly turn into a management nightmare.

In data centers, things are not much different. VPNs are often placed between an external firewall, which handles internet traffic and an internal firewall that manages access control lists. These policies must be synced between data centers in order to maintain a consistent security policy.

SDP offers a dramatically simpler management and administration paradigm for any number of data centers and cloud deployments. An administration console in the cloud allows administrators to onboard each network resource to the SDP platform once, and then manage all policies centrally in the cloud, avoiding the need to configure and sync across different locations. There is little to set up or maintain and upgrade in the data center or VPC, since all logic and security definitions are done in the SDP cloud platform.

Similarly, onboarding new remote employees is much simpler compared to VPN. An administrator assigns the security policies for a new user based on his/her role, and can then send the user a link to access applications from his/her browser, or to install an SDP client.

> We're growing quickly and the solution is robust and flexible enough to grow with us - it's easy to onboard new customers and assure the granular security that we need."
>
> VIA Read case study

4 Improved End-User Experience

For anyone who has used a corporate VPN, slow and unreliable performance is common. It gets even worse if your job involves several applications in multiple data centers or cloud instances - forcing you to repeatedly connect to and disconnect from each remote application.

With SDP, the user experience is dramatically improved. First, an SDP client maintains concurrent connections to many applications and transparently routes traffic to the appropriate destination. A user can therefore work simultaneously with multiple applications, regardless of their location.

A cloud-based SDP solution can provide a global presence of SDP gateways, or points-of-presence (PoPs), which reduces latency and optimizes the routing of data. Instead of connecting to a remote data center or cloud, a user is automatically connected to the nearest PoP, thereby experiencing improved performance and quality of service regardless of geographical location.

5 Better Scalability with Lower Costs

The total cost of ownership (TCO) of deploying and maintaining corporate VPNs climbs fast with expansion. Firewall VPN appliances (virtual or physical) can be expensive, and as the number of data centers, cloud instances and remote users increases, enterprises must purchase additional capacity to scale and support growth. An additional cost factor is the continuous updates and maintenance of VPN devices, consuming IT administrators' time.

Nevertheless, the largest hidden price tag of VPNs is the IT/help desk time for end user technical support - covering the setup and configuration of VPN client software, as well as ongoing troubleshooting.

A SaaS SDP solution, on the other hand, can scale instantaneously when demand increases, without the need for additional server or software. Leveraging a backbone of global PoPs, an SDP solution deployed in the cloud can scale up to millions of concurrent users, without requiring any upfront investment or ongoing maintenance. It offers a simpler SDP client that can be installed independently with no IT support, and in some cases also a clientless option for temporary remote workers, like contractors with unmanaged BYOD.

Summary: Traditional VPN vs SDP

	SPD	VPN
Data access	Zero trust	Trust-based network design
Access authorization	Granular user/resource access with continuous assessment	Network access authorization
Vulnerability to attacks	Hides enterprise topology	Exposes gateways to the internet
Integration with other security services	Pre-integrated security services	Complex to integrate with existing/new services
End user experience	Great	Mediocre
Service delivery	Software as a Service (SaaS)	Appliance, complex meshing between sites, high availability

Taking the Next Step – From VPN to SDP

Transitioning from VPNs to a software defined perimeter solution does not require a complete overhaul of your IT infrastructure. In fact, it does not require any overhaul at all.

Meta Networks lets you adopt Google's BeyondCorp approach to a software defined perimeter without changing any of your network infrastructure or applications. You can provide remote/mobile employees, partners, contractors and customers with convenient, granular access to specific web or legacy applications - with tighter security, and without the need for a conventional VPN.

GET A DEMO: AN SDP IN ACTION

Meta Networks

Learn More about Meta NaaS™

Meta NaaS is the next evolution in networking and network security. Companies already consume applications as a service (SaaS), and compute and storage as a service (PaaS and IaaS). Now is the time to consume enterprise networking and zero-trust network security as a service.

Contact Meta Networks at www.metanetworks.com/get-a-demo to see a live demo.

© Copyright 2018, Meta Networks Ltd. All rights reserved. Meta Networks and Meta NaaS are trademarks of Meta Networks, Ltd.