Pulse Secure®

WHITE PAPER

Pulse Secure's Software-Defined Perimeter

Secure Access in a Zero-Trust World

This paper provides a background on Software Defined Perimeter (SDP), illustrates some of the architectural elements (such as separation of the control and data planes), and highlights how it benefits businesses, CIOs, CISOs, security professionals and users alike.

Executive Summary

In today's world of multi-cloud customer environments, a secure access approach that is based purely on a network perimeter security model no longer suffices. Business and users (employees, contractors, partners and customers) need ubiquitous secure access to datacenter and cloud-based applications and resources, both from inside the corporate network as well as from outside. Software-defined Perimeter (SDP) architectures offer a compelling, "zero trust" model so that can be applied to new and existing hybrid IT deployments across industries as diverse as healthcare, manufacturing, or financial services.

Software-defined Perimeter (SDP) architectures offer a compelling, "zero trust" model so that can be applied to new and existing hybrid IT deployments across industries as diverse as healthcare, manufacturing, or financial services.

SDP prescribes an "authenticate and verify first" approach before granting direct, protected access to applications and resources – access that does not depend on network architecture and adds significant security enhancements. Application access can be restricted individually – to both applications and users. Resources can be rendered invisible or inaccessible to all users and devices until an explicit authentication, compliance check, and authorization have been completed, offering better security and protection. The overall result is a "dark cloud" where the attack surface of the network is diminished because hackers can't attack what they can't see.

Introduction

Traditional network architectures evolved to connect workers on local networks to local resources. Increasing workforce mobility, cloud, BYOD, and ever-growing threats exposed the perimeter security model's limited flexibility, security, and connectivity. Technologies like cloud and virtualization now enable more flexible network architectures that respond better to rapidly changing business and user needs, while enabling the means to further end-to-end security before the initial connection is made.

Leveraging cloud and virtualization technologies, and integrating authentication and authorization directly into the architecture, SDP enables effective segmentation and granular access control based on "zero trust", or "least privileged" trust models. This offers significant control over which users access particular resources, but without complex policy syntax or command-line usage.

SDP enables effective segmentation and granular access control based on "zero trust", or "least privileged" trust models. This offers significant control over which users access particular resources but without complex policy syntax or command-line usages.

In this paper, we describe SDP as an additional modality of Secure Access based on a "least privileged permission model", whereby individual connections between users and resources are created on-demand. Depending on pre-established trust or zero-trust prerequisites, different types and levels of secure connections can be created as authorized and/or as required. In addition to zero-trust and least-privilege security access models, the paper describes Pulse Secure's SDP approach, which also includes client-based and client-less secure access, cloud and data center-based applications, internal and external users, as well as on-demand VPN-tunnel, per-app VPN, Wi-Fi, LAN, PTP and proxy-based connectivity options.

Secure Access and SDP

Pulse Secure provides numerous key components, technologies and capabilities of SDP including:

- Centralized User Authentication
- Device-based Compliance Checks and Access Authorization
- Per-application Connectivity Options
- Cloud and Data Center-based Application Support
- Diverse Internal and External User Scenarios

By decoupling permission (control plane) and access (data plane) functions and enhancing deployments through cloud and virtualization technologies, diverse customer scenarios, such as enabling per-application access to users based on the type of device being used, are possible without extensive configuration, management, or integration.

The next few sections describe what SDP is, what the main components are, what its core principles are, and what Pulse Secure provides today and going forward.

SDP Building Blocks and Core Principles

A typical SDP reference solution consists of three distinct components that enable secure connectivity, enforcement, and management:

SDP Controller
The controller acts as the "control plane", directing the permission of network traffic to specific resources. It provides centralized policy management and AAA services. It also acts as a trust broker between the SDP client, certificate authority and identity providers.

SDP Client
Enforces device and user identity verification and routing to access whitelisted applications in the data center and authorized protected applications deployed in the cloud.

SDP Gateway
The gateway acts as the "data plane", transmitting network traffic to resources as specified by the SDP Controller. It serves as termination or access point for the mutual TLS connection from the SDP Client and the visible or invisible end-point for the application resources. The SDP Gateway is the primary policy enforcement point in the data path.

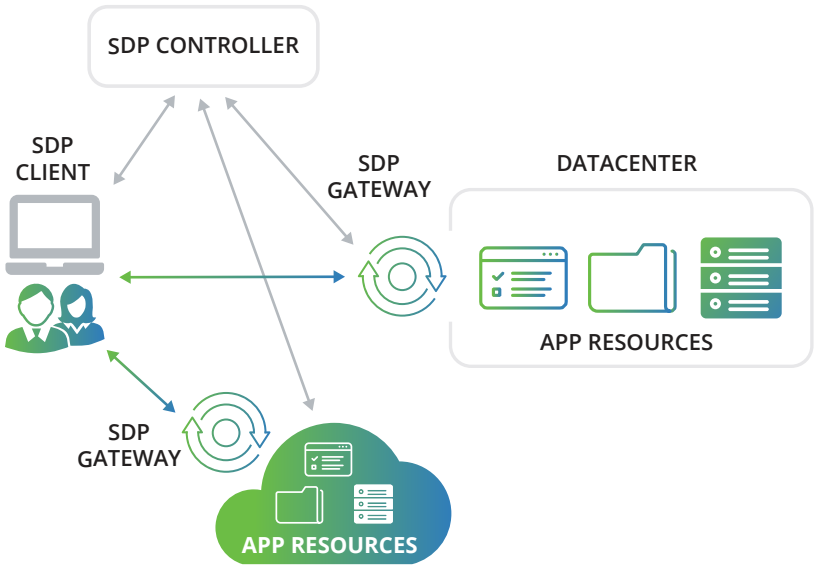

Figure 1 — SDP architecture overview

SDP's "Zero Trust" Model

SDP's primary design principle is to unify security between cloud or non-cloud resources and applications, and various internal or external user types and their devices. To ensure security, rigorous authentication and authorization is built into the architecture before a connection is established – and each connection is one-to-one and on-demand. This provides a needs-based access model with invisibile or "dark" service or network segments, thereby reducing the attack surface dramatically.

Authenticate and authorize before connecting

User and device authentication and authorization must succeed before any type of connection is established. Upon successful authentication and authorization, a specific level of trust is established that governs granular application or resource access. Access is based on user, device, and application context such as time-of-day, geographic location, user role and/or reputation, device reputation, and compliance.

On-demand connections

One-to-one, on-demand connections are established using an overlay network model. Micro-segmentation is applied for applications, resources, and privileged access. Different types of secure connections can be established dynamically depending on the application or resource security requirements.

Pulse Secure Access with SDP

Pulse Secure's SDP solution establishes a centrally and uniformly configured security perimeter between user devices and the resources they access. This flexible, zero-trust approach offers numerous benefits over traditional best-of-breed security architectures: authentication and authorization is enforced through policies, access control is more granular and customizable, and resources can be hidden from external or internal attack vectors.

Authentication & Authorization

Multiple Trust Models for different resource security levels on-demand

The Pulse Secure SDP implementation supports multiple/flexible trust models in order to meet the security requirements of applications and resources

- Zero-trust, least privilege, or connection permissive
- Client or client-less
- Multi-factor Authentication (MFA), reputation, and context-based authorization/permissions
- Privileged or restricted access
- Micro-segmentation

Privileged user segregation of duties

By providing more granular access authorization controls and support for micro-segmentation, high-privileged users may be required to use different sessions, devices, user credentials and/or levels of authentication to access various privileged and unprivileged parts of application. This would also provide varying controls for vendors and contractor user types who require access to specific resources and applications.

Access & Policy Enforcement

Granular Access Control

The Pulse Secure SDP approach provides users granular access as needed to applications, resources or sub-segments, with on-demand connectivity through policies. SDP supports segregation of external users (partners, customers) from internal users (employees, contractors) and privileged users (admin, DevOps, data scientists).

Uniform Policy & Enforcement

SDP provides a uniform policy model and Secure Access enforcement architecture. This applies to both internal and external users — and their devices — as well as for internal data center (private cloud) and public cloud (SaaS and IaaS/PaaS) applications.

Consistent centralized policy and configuration

By centralizing and unifying policy and configuration information, greater consistency is achieved across all instances enforcing connection and access policies. This results in fewer manual or custom errors, avoids configuration and policy drift and ultimately achieves higher levels of security.

Connectivity & Management

Needs-based connectivity

Also known as Dark Site or Dark Cloud support where services or resources remain completely hidden and isolated from either internal or external connectivity and access. The service will not accept a connection and access requests until a user and their device have been centrally authenticated and authorized. An added benefit of this" authenticate before connect" approach is the thwarting of DDOS attacks simply by declining (dropping) connectivity for rogue requestors.

Visibility

Given the different types and security models for on-demand connectivity, application resource requests can be observed, logged and audited as needed. This provides greater cloud and datacenter access visibility, analytics, compliance reporting and automated remediation of security issues, exceptions or anomalies.

Practical SDP Usage Considerations

SDP provides three primary access modes for internal users (employees, contractors) and external users (guests, partners).

Client-less, browser-based access
Often the most common usage, users access resources only with the browser installed on their device. SAML typically provides authentication to resources, or Secure Password Authentication (SPA) may be used as well. Privileged access to applications for administrators via the back-end is also possible.

Mobile native client application without SDP client
Remote users often access applications, such as Salesforce or Dropbox, using a specific link or applet on their device. Depending on the application, security may be built-in or required separately.

SDP client present
When using an SDP client for access, applications and resources may be reached via an SDP-gateway, or via SPA.

Given these three access models, the following specific use cases based on user location, resource location, and user privilege levels are possible:

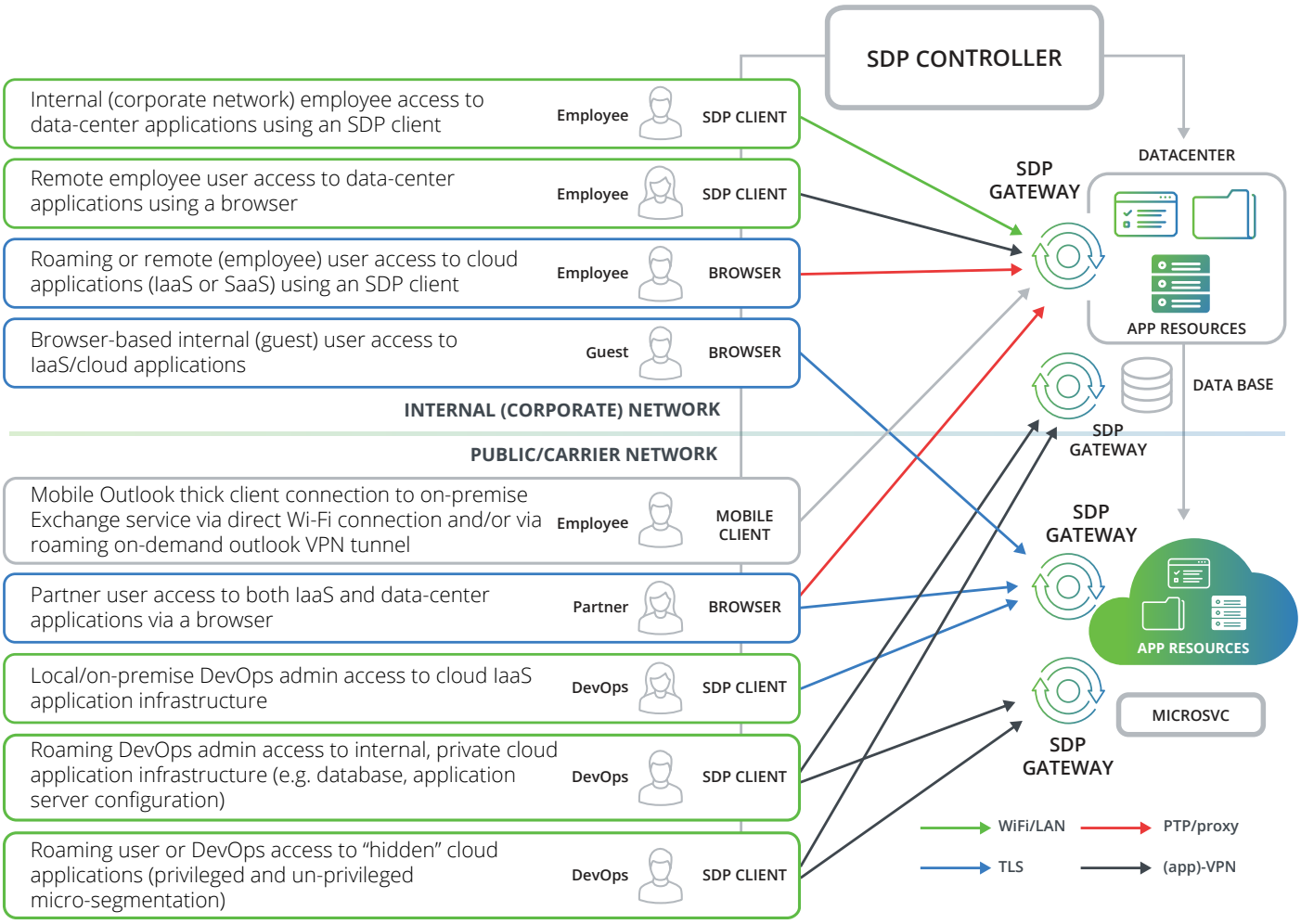

Figure 2 — SDP use cases

Pulse Secure Value Proposition

A true SDP architecture that meets today's business requirements — and adapts and grows as those requirements change — must include centralized policy management and authorization as well as distributed micro-segmented application and resource access control for both data center and cloud applications.

Secure access with micro-segmentation builds on an SDN network segment access model with distributed policy enforcement within the SDN (based on a centralized repository) and application/service-centric policies, which are not based on IP address. A Trust Model in this environment builds on SDN network segment access, implies/assumes a zero-trust model, and provides separate segments for privileged users.

Pulse Secure extends this model by breaking the problem into four layers (user and information, application, device and infrastructure, and network) that are typically associated with distinct management domains within the IT organization. The top-level objective is to provide the user (or IoT device) secure access to create, store and retrieve information. This is based on client-side services and applications that connect to cloud and enterprise applications. These, in turn, rely on client devices connecting to cloud and datacenter infrastructure through wired and wireless connectivity into public and corporate networks.

Secure Access then translates into information access based on trust across and between the layers. Some use cases rely on implicit trust, while others require explicit trust relationships. For example, a user who logged into a legacy corporate computer connected to the corporate LAN could be implicitly trusted to access most internal/on-premise enterprise applications (file shares, mail server, intranet server, etc.). In today's environment, a user may need to authenticate with a mobile application that was installed and secured by an End-Point Management solution, using a device profile for corporate WiFi connections, to access the enterprise application behind the firewall. A user role and profile would determine which part and what information of the application would be

This SDP deployment and trust model aligns and integrates well with today's Pulse Secure solution portfolio, thereby avoiding the need for a rip-and-replace approach. Adding SDP-style security to a new or migrated application is as simple as deploying another SDP gateway instance (or adding the application to an existing pool or connection domain) and pushing the appropriate policy configuration.

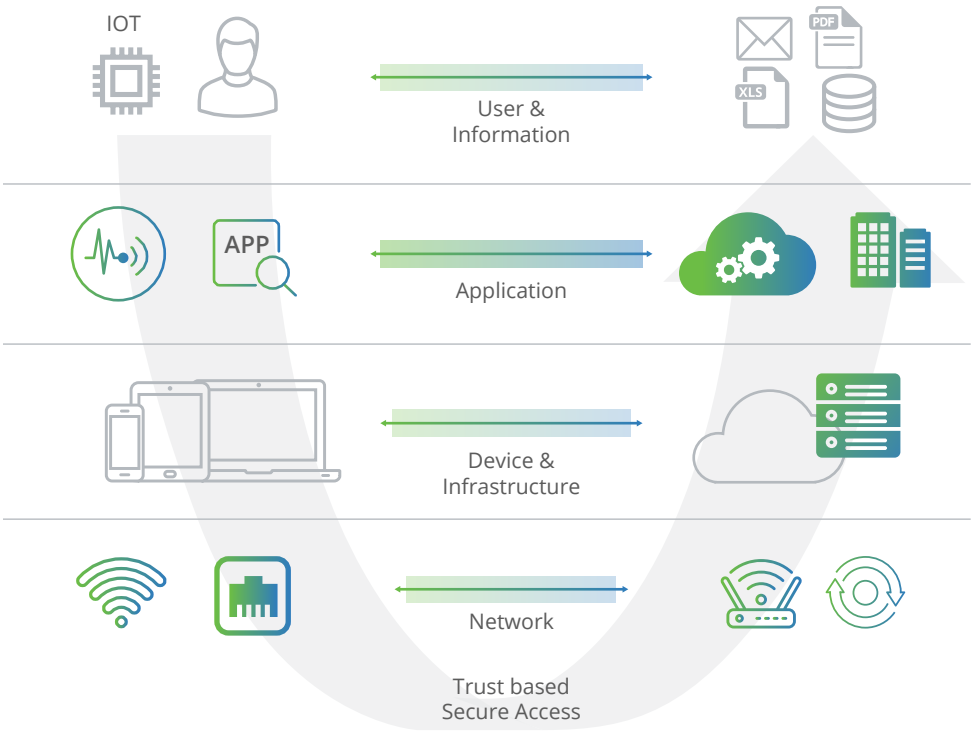

Figure 3 — SDP Deployment and Trust Model

This approach leverages Pulse Secure's proven capabilities that have long been used to protect our customer's data center and multi-cloud environments, which can now be extended to an SDP environment.

Authentication, Authorization
Pulse Secure's SDP architecture offers a single point of authentication and authorization across cloud and on-premise applications -- and includes extensive pre-connect and post-connect host/device security compliance verification.

Host Checking
Host Checker validates the endpoint device for the presence of advanced malware protection, anti-virus software, firewalls, spyware, specific operating systems, and so on. Out-of-compliance devices can be remediated or quarantined by the administrator.

Granular access to applications and resources
Extensive policies offer administrators the ability to restrict or allow access to specific applications and resources to specific users. This reduces the possibility of data loss or leakage.

Role- or realm-based authorization
Users can be grouped, including privileged users, to enable or prevent access to different classes of applications and resources. This reduces the administrative overhead of managing individual users or applications.

Multi-factor Authentication (MFA) & Device-specific Policies
MFA and device-specific policies provide role-based access control (RBAC) that can be used to separate users or restrict access based on specific device types and levels of authentication.

Per-app & Connection Categorization
Users can be on-boarded quickly based on connection type, such as NAC-based Wi-Fi or LAN micro-segment, reducing time-to-provision.

On-demand and per-app VPN connections for local and remote workers are supported, so that connections are fully secure no matter the users' location.

Pass-through proxy or reverse proxy connections to enable more secure application and resource access to servers in the cloud or behind the firewall.

Pulse Secure's vADC and load balancing applications can be leveraged to inspect and route traffic in real-time, control service levels, and reduce costs.

Future Possibilities

Policies are a key element of the SDP architecture that uses a centralized SDP controller and distributed SDP gateways to enable flexible, fast, and secure connectivity. Uniform, natural-language policies help reduce data loss and leakage by controlling access only to specific applications, resources, and information.

Dynamic, connection-based models like SDP based on user, device, or application security is a natural extension from per-application or NAC-based connections. This further secures the network and reduces the potential of malware infiltration. Moreover, integrating and enhancing the SDP client with policies offers true zero-trust security with additional, dynamic granular connectivity options. And, enabling application visibility via the SDP gateway data path (VPN, NAC and/or (G)LB/vTM/WAF) provides compelling value to modern enterprises: ensuring applications are up and running, and that workforces have secure, 24x7 access regardless of location.

Conclusion

The Zero Trust model aims to advance conventional Secure Access mechanisms to one that assures authentication, compliance and protected connectivity directly between users, devices and applications/resources held in data centers or the cloud. In essence, Pulse Secure's Secure Access solutions have always provided Zero Trust capabilities.

Software-defined Perimeter offers compelling security benefits: rendering resources "dark" to hackers, enabling always-on connections, increasing network resilience and flexibility, and reducing malware infiltration.

However, it does not mean that other Secure Access models should be excluded or are now invalid. Not all scenarios or resources require a true zero-trust based policy, all the time. Different applications or classes of information can be mapped to a spectrum of trust levels that need to be established, per secure access policies, in order to grant protected access. Rest assured, Pulse Secure has the experience, solution portfolio and core capabilities that can enable SDP and mixed Secure Access models as enterprises migrate to or fully leverage Hybrid IT. Organizations looking to augment security and compliance posture, enable true workforce agility, and increase business responsiveness should explore how SDP can address their business requirements.

About Pulse Secure

Pulse Secure, LLC offers easy, comprehensive Secure Access solutions that provide visibility and seamless, protected connectivity between users, devices, things and services. The company delivers suites that uniquely integrate cloud, mobile, application and network access to enable hybrid IT. More than 20,000 enterprises and service providers across every vertical entrust Pulse Secure to empower their mobile workforce to securely access applications and information in the data center and cloud while ensuring business compliance. Learn more at www.pulsesecure.net.

Pulse Secure®

For more information on Pulse One, please go to pulsesecure.net/pulse-one

(844) 807-8573 info@pulsesecure.net pulsesecure.net