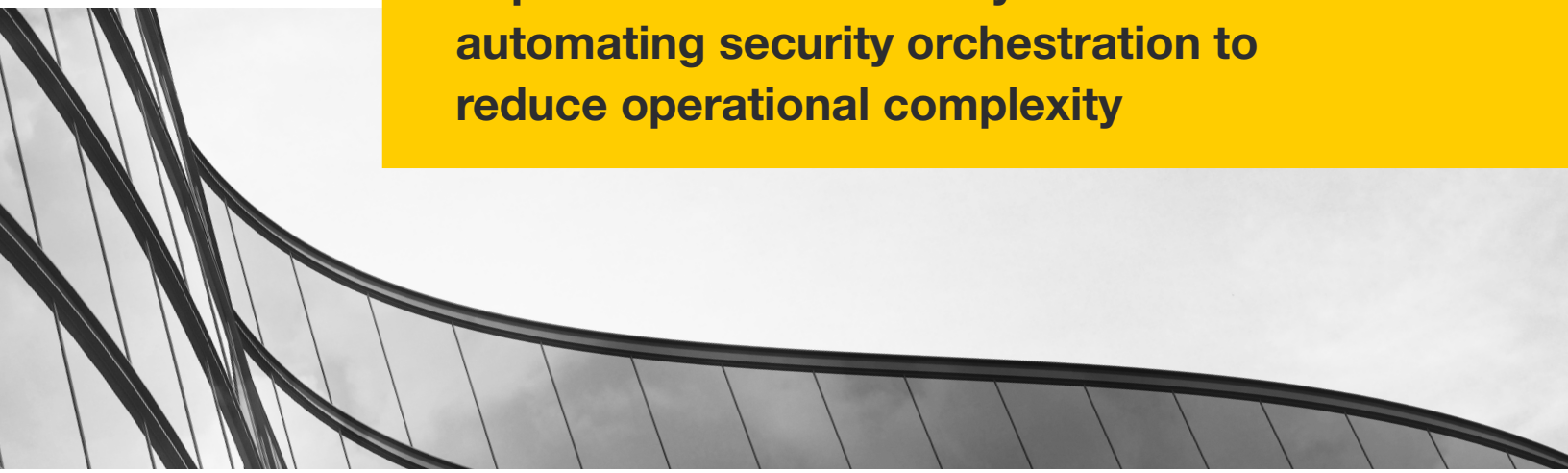
Tempered

An introduction to Zero Trust Software-Defined Perimeters

Improve network security while automating security orchestration to reduce operational complexity



Overview

Securing your network can be a challenge, especially as remote working has become the new norm, organizations have extended themselves to the public cloud and the traditional network perimeter with edge firewalls is dissolving. With COVID-19, companies are pushing forward with rapid digital transformation to maintain business continuity without the need to be in their physical office. Other use cases have reinforced the need to flexibly secure corporate access to meet rapidly changing business requirements. However, this has meant a larger attack surface, putting their most important data at greater risk to cybersecurity threats.

As such, network security should be a priority for every company now more than ever. And to address the new need for secure remote access and connectivity outside the traditional perimeter, strong consideration needs to be given to automated orchestration of new security policies to increase business agility and reduce errors. The most effective way to achieve this security with orchestration is through a Software-Defined Perimeter (SDP). This white paper provides an essential primer on Software Defined Perimeters, their benefits, ideal use cases, and how to deploy them.

Zero-Trust Network Access and Software-Defined Perimeters

What is Zero-Trust Network Access?

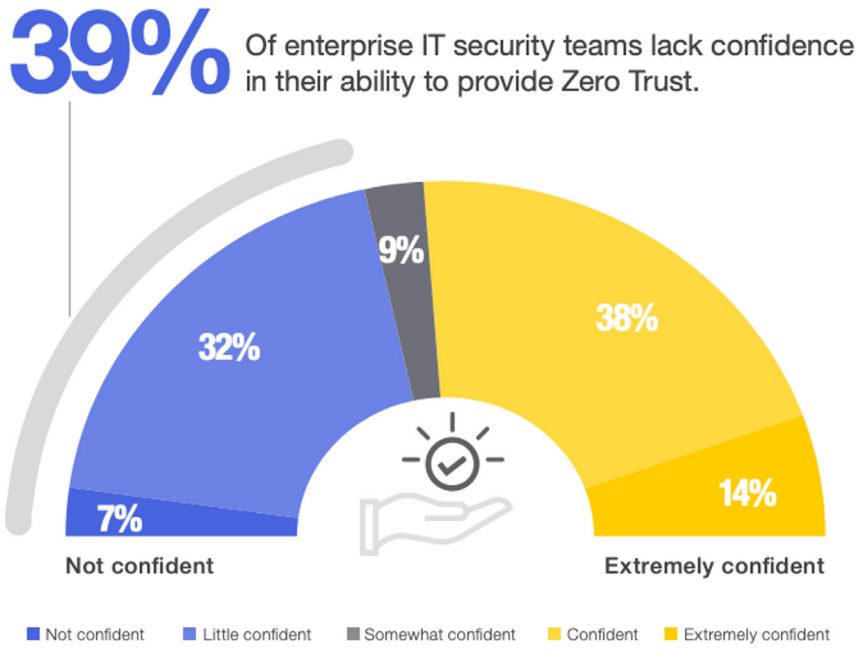
The path to understanding Software-Defined Perimeters begins with understanding Zero-Trust Network Access (ZTNA), a new approach to network security that has grown in both popularity and scope over recent years.

Zero Trust is a response to the inherent trust built into traditional security models and legacy north/south perimeters. Rather than grant "trusted" entities access to everything within a given network, the Zero Trust network security model begins with an initial security posture of zero implicit trust between both internal and external entities.

To this end, ZTNA is built on the following three principles:

- ❏ Granular security policies built around whitelists to all resources, regardless of resource type and user location
- ❏ Comprehensive traffic logging and inspection
- ❏ Enforcement of least privilege

How confident are you to apply Zero Trust model/tenets in your secure access architecture?



Source: Cybersecurity Insiders 2021 Zero Trust Report

What is a Software-Defined Perimeter?

A Software-Defined Perimeter (SDP) is a network security architecture that utilizes user authentication and network segmentation to enable access to resources based on a centrally managed policy system or SDP controller[1]. SDP analyzes user access permissions at a highly granular level and micro-segments the network by verifying every user and device before they can access any specific application and system. Network administrators can even use SDPs to customize, automate, and continuously enforce highly specific network security policies. Because of the possibility of automating the design and enforcement of highly granular policies, SDP is an ideal solution for a zero trust architecture.

Companies often implement SDP solutions because of the lack of granularity and complexity of management and automation of traditional network security measures. For example, hackers who are able to breach a traditional network may be able to access any number of applications within that network via east-west, or lateral, movement, making it challenging to determine which applications are vulnerable or have been compromised. SDP solves this problem by providing a continuous verification process that increases visibility into user privileges and behaviors, while mitigating lateral movement where such connections are not explicitly authorized.

For a network security product to qualify as a Software-Defined Perimeter solution, it must meet the following four requirements:

- ❏ Network segmentation (sometimes called overlays) that is both adaptive and granular (micro-segmentation)
- ❏ On-demand access to individual applications, networks, and services upon verification
- ❏ Continuous monitoring of activity and verification of network access requests
- ❏ One or more centralized policy controllers that simplify policy definition and management, oriented around application, device or user identities

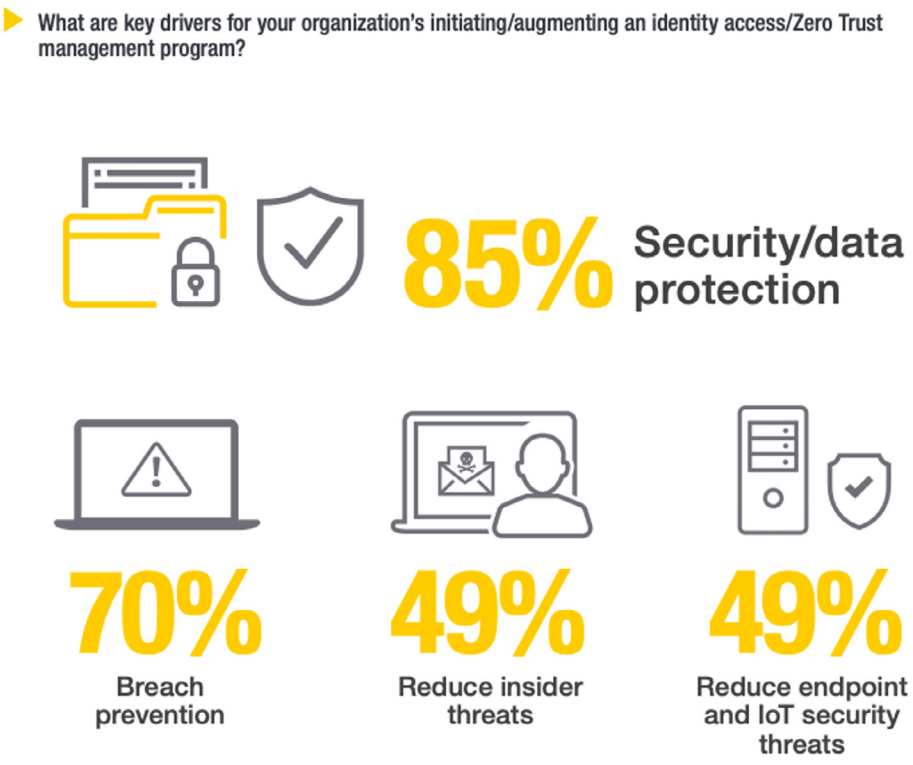
[1] WIkipedia: Software Defined Perimeter: https://en.wikipedia.org/wiki/Software_Defined_Perimeter

How ZTNA and SDP relate

If SDP sounds similar to ZTNA to you, you're not alone. Discussion of how ZTNA and SDP relate to one another continues to evolve, with some industry players referring to SDP as another name for ZTNA (Gartner), to ZTNA as a pillar of SDP, to SDP as a means to improving the success of ZTNA, and to SDP as a way to implement the principles of ZTNA. This last relationship is the understanding of choice for Cloud Security Alliance (CSA), the organization that first defined a group of specific requirements necessary to provide contemporary secure remote access capabilities and coined the term Software-Defined Perimeter.

In its Software-Defined Perimeter Architecture Guide, CSA explains how SDP helps implement the three principles of ZTNA listed above:

ZTNA principle	SDP implementation
Granular security policies built around whitelists to all resources, regardless of resource type and user location	SDP strongly authenticates devices and users and encrypts network connections, ensuring secure access of all resources regardless of user location. SDP also typically deploys as an overlay across existing networks, ensuring secure access of all resources regardless of resource location (cloud, on-premises, etc.).
Comprehensive traffic logging and inspection	Network connections are controlled in an SDP implementation, providing a centralized location to log which human and machine identities are accessing which resources.
Enforcement of least privilege	SDP begins with a default-deny security posture and strict whitelist access model, so identities can only access applications and systems when an SDP control explicitly allows them to do so.



Source: Cybersecurity Insiders 2021 Zero Trust Report

Benefits of SDPs

Security benefits of SDPs

SDPs provide the following security benefits:

- By hiding resources from public view, SDP reduces the attack surface and thus reduces security risks.
- SDP separates data planes and access control to make critical infrastructure and assets "black" (meaning undetectable), thus protecting them and preventing network-based attacks.
- SDPs' integrated security architecture includes elements such as network-aware firewalls and gateways, client-aware devices, and user-aware applications — a combination that traditional security products such as antimalware and NAC struggle to achieve.
- SDP solves the problem created by the recent surge in IP addresses and the perimeter loss in cloud environments, which weaken location-based security, by providing connection-based security architecture instead.

Organizations can use SDP to control all connections by preestablishing who can connect to which applications, services, and other parameters using which devices.

- ❏ SDP supports the creation and implementation of a comprehensive risk-based policy, including malware outbreaks, new software, and threat intelligence.

Business benefits of SDPs

Organizations can expect the following business benefits from SDP implementation:

- ❏ **Cost savings**: SDP reduces licensing and support costs, reliance on traditional security tools and operational complexity, and leased line utilization and multiprotocol label switching (MPLS), all of which in turn reduce costs. By making operations simpler and more efficient, SDP can further save organizations money.
- ❏ **Reduced administration and management**: VPN management becomes increasingly more complex when organizations expand even a single data center into a multi-cloud environment, forcing network administrators to configure and synchronize firewall and VPN policies across multiple locations. SDPs simplify this process by enabling administrators to add all network resources to the SDP platform just once and centrally manage all policies in the cloud, eliminating the need to repeat this process for different locations. Because all security and logic definitions are set in the SDP cloud platform, little setup, maintenance, or upgrades are necessary in the virtual private cloud (VPC) or data center
- ❏ **More agile IT operations**: While many IT processes hold business processes back, SDP implementations are largely automatic, driven by IT or identity and access management (IAM) events. This frees IT up to respond to other security and business needs.
- ❏ **Improved GRC management**: By reducing the attack surface, suppressing threats, keeping application vulnerabilities from being exploited, and preventing network-based attacks, SDP reduces the typical risk associated with traditional security measures. SDP can also be integrated into governance, risk, and compliance (GRC) systems to streamline compliance tasks.

- **Improved compliance**: SDP centralizes control of user connections to specific services and applications from registered devices, improving compliance data collection, auditing, and reporting processes. Additional connectivity traceability is also possible for online businesses, and the micro-segmentation that SDP provides can reduce compliance scope — and compliance reporting efforts.
- **Secure adoption of cloud architectures**: SDP reduces the complexity and cost of the security architecture required to support applications in data center, private cloud, public cloud, and mixed environments, enabling organizations to adopt and deploy cloud architectures more quickly and securely than is possible with other options.
- **Increased innovation and agility**: With SDP, organizations can quickly and securely implement priorities such as deploying company assets onto customer sites, outsourcing business functions to third parties, enabling customer-facing kiosks on remote third-party locations and networks, and transitioning from on-premises call center agents to home-based agents.
- **Better user experience**: VPNs are known for providing slow, unreliable performance, and they often make it difficult to connect and disconnect to remote applications across different locations. SDPs, on the other hand, utilize a global network of points-of-presence (PoPs) to optimize data routing and reduce latency, allowing remote users to connect to the closest PoP rather than a specific site. This provides better service quality from any location.
- **Better scalability**: Unlike VPNs, which are complicated and costly to manage at scale, SDP solutions come with a fixed price per user no matter how many network resources the user needs access to. SDP solutions are also easy, efficient, and cost-effective to scale up to millions of users — with no need for larger appliances for additional users.

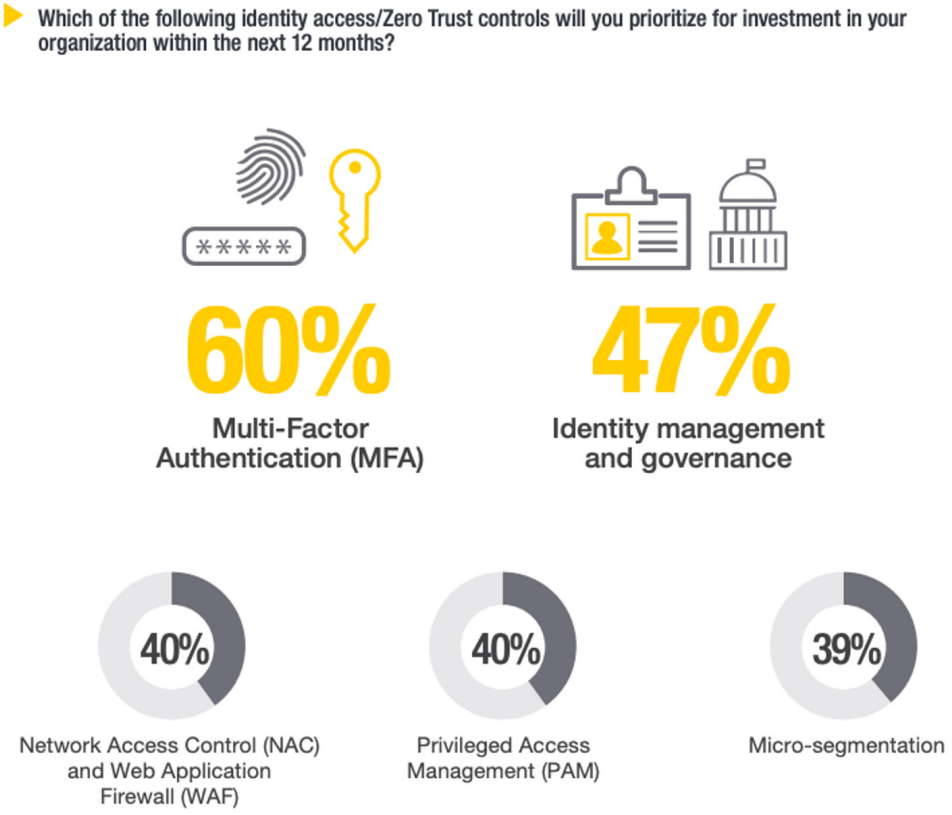
SDP use cases

Because SDP is a fundamental security framework , it has many potential uses and deployment scenarios. While these use cases are too numerous to list comprehensively, the following table includes common scenarios that can benefit from the implementation of SDP.

Use case	Existing technology's shortcomings	SDP advantages
Identity-based network access control	Legacy network security technologies are oriented around locations (IP addresses) and offer inferior network segmentation, making it difficult for organizations to enforce timely, identity-based, and precise user access controls.	SDP enables organizations to create and enforce identity-based user access controls at the network level. For instance, companies can use SDP to restrict web access to an HR system to HR users alone, and specifically to those who are connecting from corporate-managed devices.
Micro-segmentation	Traditional network security technologies make it costly and labor-intensive to increase network security via micro-segmentation. Rarely do traditional network enforcement points extend all the way to specific endpoints for granular policies.	Micro-segmentation based on user-defined controls is simple, as SDP automates granular control of network access to specific services and eliminates manual configurations.
Secure remote access	VPNs are the typical tool of choice to provide secure remote access for users, yet they have limited capability and scope. They also create additional compliance and security risks. For instance, VPNs do not secure on-premises users and generally cannot provide granular access controls to the endpoint, instead providing access to entire network subnets or segments, often violating the principle of least privilege.	Organizations can replace VPNs with a holistic SDP solution to secure both remote and on-premises users. SDP solutions enable granular access control to restrict resource access to authorized users, supporting the principle of least privilege.

Access for third-party users	A complex combination of VLANs, VPNs, and NAC is typically necessary to manage third-party access. Nevertheless, these solutions are usually siloed and cannot provide comprehensive or granular access control across hybrid environments (e.g., on premises and cloud).	SDP enables organizations to control and secure on-premises access for third parties easily, based on identity, allowing them to adapt and innovate.
Secure access for privileged users	Increased security, monitoring, and compliance are generally necessary to provide secure access for admins and other privileged users. Organizations tend to rely on credential vaulting to manage privileged access security, yet it does not provide remote access, network security, or context-sensitive access.	SDP can restrict privileged services to authorized users, hide them from unauthorized users, and secure them at the network level, reducing the attack surface. SDP can even allow access only when specific conditions have been met (such as only from certain devices or during a set maintenance window).
Secure access to managed servers	Admins require periodic network access to managed servers in large-scale IT and managed security service provider environments, sometimes on networks that have overlapping IP addresses. Traditional network security measures struggle to provide this, oftentimes leading to burdensome compliance reporting.	Organizations can use a business process (for example, an open service desk ticket) to control managed server access and an SDP to overlay network topologies, streamlining access. Meeting compliance requirements is as simple as logging user activities.
Secure transition to IaaS cloud environments	Many organizations using Infrastructure-as-a-Service (IaaS) are concerned about security, often because IaaS access controls are limited in scope or disconnected from the enterprise, and specific to the cloud provider.	SDP improves IaaS security by hiding applications behind default-deny firewalls, encrypting all traffic, and defining user access policies consistently across the enterprise.

Simplified network integrations	The rapid integration of previously distinct networks is sometimes necessary, such as during disaster recovery or mergers and acquisitions. Traditional IP networking makes this complicated and tedious, relying on deep understanding of existing network topologies. IP conflicts in merged networks can also pose challenges.	Organizations can use SDP to interconnect networks efficiently without disruptions or wholesale changes. SDP allows you to easily define and enforce policies based on identity access requirements without relying on routing details in the existing networks. By using identity-tags, SDP can also avoid IP address conflicts in the merged networks seamlessly and quickly.
Prevention of distributed denial of service (DDoS)	Traditional solutions for remote access are vulnerable to DDoS attacks and expose ports and hosts on the internet. DDoS attacks circumvent traditional security controls for DDoS and drop good packets.	Organizations can deploy SDP without granting any visibility to unauthorized users, so only good packets are allowed through. SDP utilizes a default-drop firewall.
Streamlined enterprise compliance reporting and controls	IT and security teams often face incredibly time-consuming and expensive compliance reporting. Existing network security solutions do not align with business-oriented security policies, so audit tasks are complex and tedious.	SDP uses micro-segmentation to decrease compliance scope and identity-based access logging and reporting to automate compliance reporting. Audit reports easily align with identity-focused access policies.



Source: Cybersecurity Insiders 2021 Zero Trust Report

How the Tempered Airwall SDP architecture works

SDP architecture includes several main components:

- ❏ Initiating host (IH), or client — the software installed on the endpoint that manages tasks such as device verification
- ❏ Accepting host (AH)
- ❏ SDP controller or Conductor — manages policy, and the authentication and authorization process
- ❏ Gateway — in lieu of client software, a upstream device grants access to the resources, subnet or services
- ❏ Relay – another centralized infrastructure component that allows policies to extend across multiple networks

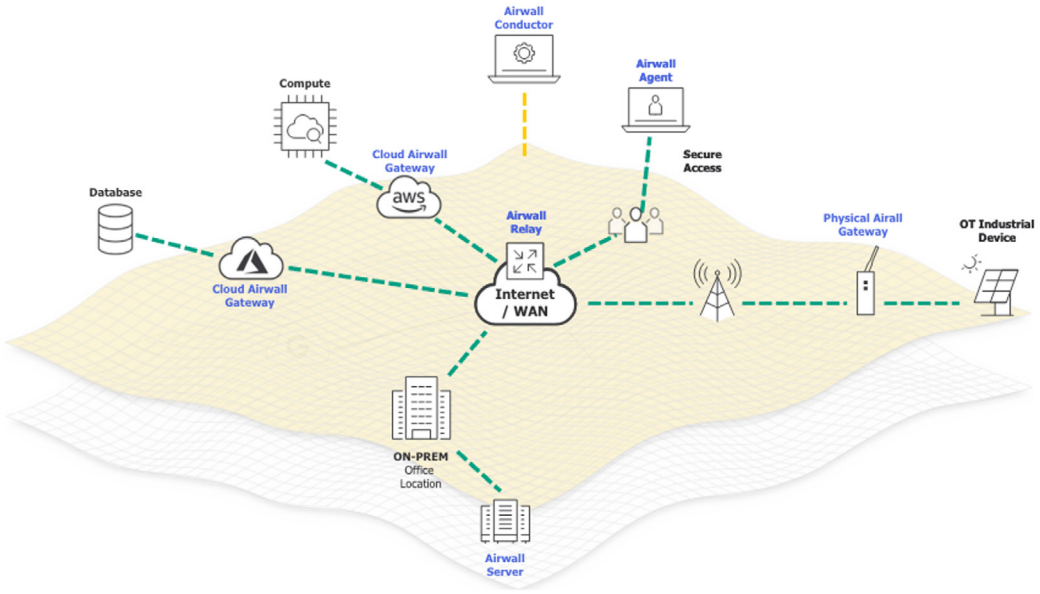


Figure – Tempered Airwall includes the centralized Conductor, Relay, as well as agent software and gateways for an entire SDP framework

These components work together throughout the following workflow:

1. The SDP client software on the IH initiates connections with the SDP.
2. Because many IH devices are user-facing (think smartphones, tablets, and laptops), the SDP software runs on the devices themselves. The network can be outside the SDP-operating organization's control.
3. AHs accept the connections from the IHs and then provide SDP-secured-services. AHs generally "live" on a network that's under the control of the SDP-operating organization, and potentially even under a direct representative. (Some SDPs like Tempered's Airwall, enable AHs to live anywhere)
4. The SDP gateway grants authorized devices and users access to protected services and processes, also potentially monitoring, logging, and reporting these activities.
5. IHs and AHs connect to an SDP controller to undergo authentication and authorization processes. The SDP controller establishes secure communications and keeps user and management network traffic separate from one another.
6. Single-packet authorization (SPA) protects the controller and AH by hiding them from unauthorized devices and users.

SDP deployment models

Several SDP deployment models are possible depending on the way that interactions among gateways, servers, and clients are structured:

- **Client-to-gateway**: The servers are positioned behind an AH that acts as a gateway between the IHs and the protected servers. Client-to-gateway SDPs can be deployed within a network to reduce lateral movement attacks such as server scanning, main-in-the-middle attacks, and application and operating system (OS) vulnerability exploits. When deployed directly on the internet, client-to-gateway SDPs can keep unauthorized users off of protected servers to prevent attacks.
- **Client-to-server**: The difference between client-to-gateway and client-to-server SDP deployment models is that, with client-to-server deployment, the SDP is protecting the system that runs the AH software instead of the gateway. Which of these two deployment models is best depends on factors such as the number of servers requiring protection, the cloud servers' elasticity (adaptability to changes in workloads), and load-balancing needs.
- **Server-to-server**: The server-to-server SDP deployment model utilizes servers that offer some kind of application programming interface (API) over the internet. It uses the API to communicate between the AH and the IH, and protects against all unauthorized hosts on the network, including representational state transfers (RESTs), remote procedure calls (RPCs), and simple object access protocols (SOAPs).
- **Client-to-server-to-client**: In client-to-server-to-client deployments, peer-to-peer (P2P) client relationships are used for applications such as IP telephony, video conferencing, and chat. The SDP hides the IP addresses of the connecting clients, for which the server acts as the intermediary.
- **Client-to-gateway-to-client**: A variation of the client-to-server-to-client deployment model, client-to-gateway-to-client implementation supports peer-to-peer network protocols and requires that clients connect directly to each other, so that each client acts as either IH, AH, or both. The SDP gateway acts as a firewall between the connecting clients.
- **Gateway-to-gateway**: In gateway-to-gateway SDP deployment models, the AH and IH both act as gateways between servers and clients, with at least one server sitting behind the AH and at least one client sitting behind the IH. Depending on the implementation, the gateways may operate as firewalls, routers, or proxies. As client devices do not run the SDP software in this model, it is generally used when devices that cannot support the SDP client are involved, such as IoT devices, printers, or scanners.

SDP deployment steps

Organizations can follow these five steps to deploy an SDP and improve their security posture:

1. Identify the resources you want to protect by using DAAS:
   - ❏ Data: Exactly what data do I need to protect?
   - ❏ Applications: Which applications do I have that consume sensitive information?
   - ❏ Assets: Which assets are most sensitive?
   - ❏ Services: Which specific services can be exploited?
2. Map the transaction flows – How does traffic move across the network?
3. Create the Zero Trust architecture – Deploy necessary components at desired endpoints and subnets as required.
4. Design the details of the policy – Which resources can have access to the network? (Include who, what, when, where, how, and why.) Define the policy in the centralized SDP controller.
5. Monitor and maintain the Zero Trust architecture – Adapt and respond quickly by analyzing data from the network and refining security and microsegmentation policies.

Conclusion

This paper has examined outlined how Software Defined Perimeters deliver can apply zero trust network access principles to support a range of use cases. Each of these provide a combination of security and business benefits worthy of further examination. In 2021, IT organizations are faced with the imperative to deliver secure networking services across an embattled and dissolving perimeter like never before. SDPs represent a more cost-effective and secure approach for modern organizations from a single unified platform, in support of a broad range of initiatives, including remote work, edge computing, IoT, cloud migration & hybrid cloud, and mobility.

Tempered Networks' Airwall is an advanced zero-trust software defined perimeter solution for anything, anywhere. Based on the IETF standard Host Identity Protocol (HIP), Airwall provides all the advantages of traditional SDPs, and more. We invite you to learn more about Airwall at https://www.tempered.io

Schedule a call with our experts to learn more.

experts@tempered.io | +1 206.452.5500

Additional Resources

- Cybersecurity Insiders 2021 Zero Trust Report
- https://en.wikipedia.org/wiki/Software_Defined_Perimeter
- Gartner: Three Styles of Identity-based Segmentation (https://www.gartner.com/reprints/?id=1-255M0P9G&ct=210204&st=sb)
- Airwall: A revolution in secure networking
- HIP Protocol Primer