**Software Defined Perimeter**

Software-defined perimeter (SDP) is a network security model that provides secure, authenticated, and authorized access to a network perimeter. It does this by creating an encrypted virtual “perimeter” around an internal network, making it much more difficult for an attacker to penetrate. The SDP approach also allows for secure access to specified resources within the perimeter, such as specific applications, services, and databases. It is implemented using software-defined networking (SDN) technologies, which allow the network to be more easily managed, configured, and monitored. This makes it a powerful tool for organizations looking to increase security and reduce risk.

**How does an SDP work?**

With an SDP, it should not be technologically possible to connect with a server unless authorized to do so. SDPs allow access to users only after verifying **user identity**.

Once the user and device are [authenticated](https://www.cloudflare.com/learning/access-management/what-is-authentication/), the SDP sets up an individual network connection between that device and the server it is trying to access. An authenticated user is not logged in to a larger network, but rather is given their own network connection that no one else can access and that only includes the services that the user has approved access to.

Imagine a web server that is connected to the Internet but does not open connections with anything. It does not accept requests or send responses; it has no open ports and no network access even though it is plugged into the Internet (somewhat like a toaster or a lamp that is plugged into a wall outlet but turned off so that electricity does not flow through it). This is the default state for servers inside a software-defined perimeter.

Another way to think of SDPs is to imagine a front door that is always kept locked. No one can come through the door, or even look inside, until the person on the other side of the door verifies who the visitor is and what they are doing. Once the visitor is allowed inside, the person in the house locks the door again.

**Synopsis of Zero Trust Network Access**

The scenario of dealing with a well-planned cyberattack has become quite prevalent in the world of IT. Thus, many software and hardware programs are also being launched in the market, which can potentially prevent these threats. However, the ZTNA (Zero Trust Network Access) framework seems to be the most reliable one.

For Example, due to the COVID-19 pandemic, most organizations are still going for remote work. Thus, security threats have become pretty prominent again. However, this is where Zero Trust comes in. It helps the workers of the association to assess their network security constantly through **identity authentication.** When working in a ZTNA-implemented network, you will need to prove yourself trustworthy and non-malicious.

**How to implement Zero Trust Network Access?**

1. Create a network segmentation strategy: Start by dividing the network into different segments, such as user segments, application segments, and data segments, and restrict access to each segment.

2. Authenticate user access: Implement multi-factor authentication (MFA) for all users, including external users, so that only authenticated and authorized users can access the network.

3. Enforce least privilege access: Implement least privilege access controls to ensure that users only have access to the information they need to do their jobs.

4. Monitor user activity: Implement user activity monitoring to detect any malicious activity or suspicious behavior.

5. Implement a firewall: Implement a firewall to detect and block any malicious traffic and protect the network from external threats.