appgate

WHITEPAPER

SOFTWARE-DEFINED PERIMETER

A Layer 3 approach to dynamically control access to data based on identity-centric policies

Traditional network security approaches are failing to adequately protect organizations today. Trust is presumed and misplaced. It's an outdated model predicated on obsolete isolation of users and networks.

TIME FOR AN IDENTITY-CENTRIC APPROACH: SOFTWARE-DEFINED PERIMETER

Today's IT reality requires flexible and adaptive security, one centered on a user's identity instead of the various networks upon which they operate. This approach is called a Software-Defined Perimeter. It dynamically creates one-to-one network connections between users and the data they access.

A Software-Defined Perimeter is identity-centric. It's designed around the user. Users are authenticated BEFORE they are allowed to connect to a network. It enforces the "zero-trust model" so that anyone attempting to access a resource must authenticate first. All unauthorized resources are invisible.

This applies the principle of least privilege to the network and completely reduces the attack surface. By default, users are not allowed to connect to anything—opposite of traditional corporate networks, where once a user is given an IP address, they have access to everything it has access to. Instead, zero trust ensures that once proper access criteria is met, a dynamic one-to-one connection is generated from the user's machine to the specific resource needed. Everything else is completely invisible.

"AUTHENTICATE-FIRST, CONNECT SECOND"

The basic premise of a Software-Defined Perimeter is built on an "authenticate first, connect second" approach. Unlike a traditional network that connects various roles or groups to a network segment and then relies on application level permissions for authorization, a Software-Defined Perimeter creates individualized perimeters for each user, allowing for much more fine grained access control.

As a user's situation changes, the individualized security perimeter changes. Software-Defined Perimeters control access to network resources that are across hybrid environments – in a corporate datacenter or in the cloud—meaning that consistent access policies can be enforced.

The fundamental reason for the failure is that TCP/IP—which was originally designed to operate in an environment where the user community knew and trusted each other—is based on implicit trust, with a "connect first, authenticate second" approach. In today's hyperconnected and highly adversarial threat landscape, this approach puts organizations at risk, and has enabled far too many data breaches.

THIS TRADITIONAL FLAT LAYER 2 IP NETWORK APPROACH RESULTS IN:

Servers exposed to reconnaissance scans

Unauthenticated users able to exploit and gain access to servers and information

DDoS attack vulnerabilities

Unauthorized users consuming unauthorized server resources
Inherent over-entitlement

Broad lateral attack surface

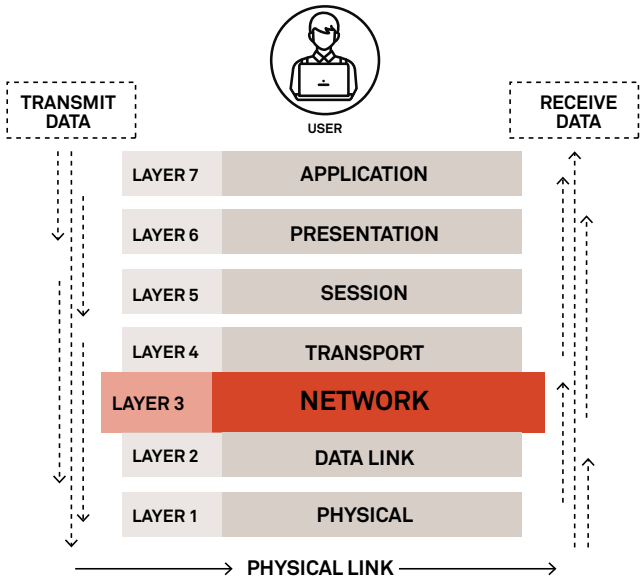
Exposed layer 3

This “authenticate first, connect second” approach, ensures that only authorized users can connect to network resources. This reduces the attack surface and significantly improves security:

- All resources are invisible to potentially dangerous reconnaissance
- Defeats hackers by denying ability to move laterally
- Only authenticated users can connect
- DDoS attacks are ineffective
- Unauthorized users cannot impact servers

BENEFITS OF LAYER 3 SECURITY VS. LAYER 7

Using an SDP solution to manage Layer 7 access results in significant repetitive tasks and overhead. With the continued proliferation of applications, wide-scale cloud adoption, and integration of container solutions, the complexity of maintaining a Layer 7 SDP solution continues to grow. Appgate SDP is focused on Layer 3 security, efficiently bringing your security closer to the data it is designed to protect.



APPGATE SDP:

- Enforces Zero-Trust by ensuring all resources are accessed securely regardless of location, adopting a least privilege strategy and strictly enforcing access control and inspecting and logging all traffic. This eliminates the TCP/IP trust but not verify risk.
- Creates individualized perimeters for each user, allowing for much more fine-grained access control and giving individual users access to only what they need to do their jobs .Users see only IP and hosts on authorized ports and protocols.
- Ensures access to the network is granted based on Live Entitlements, dynamic, context-aware security attributes that confirm user identity while providing the flexibility necessary to adjust to changing variables, such as environmental/ infrastructure changes, user location, time of day, and workload sensitivity.
- Allows for dynamically flat layer 2 networks. Organizations can micro-segment layer 2 networks to control users making layer 3 calls to IP’s residing within the layer framework.
- Deeply integrates with business systems including IDaM.
- Eliminates lateral movement—prevents unauthorized movement within the network schema.
- Reduces DDoS threats.
- Dramatically reduces and simplifies firewall policies. Each user is defined with his or her own access permissions/ policies on the gateway leaving the traditional edge firewall with a much simpler schema cutting down error prone access, user add/remove issues, routing mistakes, etc.
- Comply-to-Connect policies can be applied

appgate