SONICWALL®

Secure Your Shared Assets with Zero-Trust Security

Introduction

With the adoption of public and private clouds, and the rapid increase in mobile devices, today's corporate network perimeter has been completely redefined. These borders are now fluid, as mobile workers with personal cellphones, tablets, notebook computers and more increasingly request access to corporate IT resources and applications. Since these devices can't be monitored or logged by IT, "Bring Your Own Device," or BYOD, can expose businesses to malware and hackers if employee devices do not comply with corporate BYOD security policies.

Global IT infrastructures, privately hosted datacenters and multi-vendor public cloud environments further expand the network perimeter, adding layers of complexity to organizations' cybersecurity strategies.

As organizations continue to move away from the traditional on-prem environment and toward this new IT reality, their legacy cybersecurity solutions have been unable to keep up, creating unmanageable complexity and increased opportunity for cybercriminals. This has led to a rise in the use of Zero-Trust security architectures, which do not automatically extend trust regardless of whether a user is inside or outside the perimeter.

When implementing a Zero-Trust security architecture, IT managers must use micro-segmentation to isolate resources within their IT infrastructure. Forrester Research recommends dividing network resources at a granular level, which allows organizations to tune security settings to different traffic types and create policies that limit network and application flows to only those explicitly permitted. This approach allows security teams the flexibility to apply the right level of protection to a given workload based on sensitivity and value to the business.

A Zero-Trust architecture also helps mitigate risks from increasing access needs. In today's businesses, access typically isn't limited to just employees and business partners — in many cases, it must also be extended to consultants, customers, suppliers and more. These individuals all need access to business applications and IT resources that reside in global private data centers and public clouds.

This fluid network perimeter and IT-enabled workforce represent a challenge for both employees needing reliable and secure mobile and global connectivity, as well as IT managers and legal and compliance departments.

Shortcomings of Traditional VPNs and the Need for Software-Defined Perimeters

Virtual private networks, also known as VPNs, provide secure and private connectivity for employees needing remote or site-to-site access to applications on internal corporate networks.

For instance, VPNs let employees access their company's intranet from home or while traveling for business. In contrast, site-to-site VPNs enable employees in different office locations to use one seamless virtual network for application access or data sharing.

As virtual point-to-point connections, VPNs can be created via dedicated connections, virtual tunneling protocols or through network traffic encryption.

While traditional VPNs provide secure remote access, they do have drawbacks, including limited client support for BYOD situations, cloud services or bandwidth restrictions, and global server support from VPN providers or corporate IT resources.

Additionally, some VPNs do not employ role-based access controls, user access logs or analytics capabilities. Due to the cost of external hardware, maintaining a VPN is also a challenge for IT departments with limited budgets and staff.

In contrast, the Software-Defined Perimeter (SDP) model addresses traditional VPN limitations by providing a flexible cloud-based platform; device and application configurability and accessibility; increased security; privacy; and user-access control granularity and analytics.

According to the Cloud Security Alliance (CSA), SDPs provide "the ability to deploy perimeters that retain the traditional model's value of invisibility and inaccessibility to 'outsiders,' but can be deployed anywhere — on the internet, in the cloud, at a hosting center, on the private corporate network, or across some or all of these locations."[1] The SDP brings together standard security tools including PKI, TLS, IPsec, SAML and standards, as well as concepts such as federation, device attestation and geo-location to enable connectivity from any device to any infrastructure.

Gartner predicted that, by the end of 2017, at least 10% of enterprise organizations would deploy SDP technology.[2] The following year, Gartner recommended that CISOs focus on SDPs as a top 10 project. This recommendation was based on the idea that SDPs would reduce risk and make a large impact on their businesses by reducing the attack surface and limiting IT resources to only named sets of external partners, remote workers and contractors.[3]
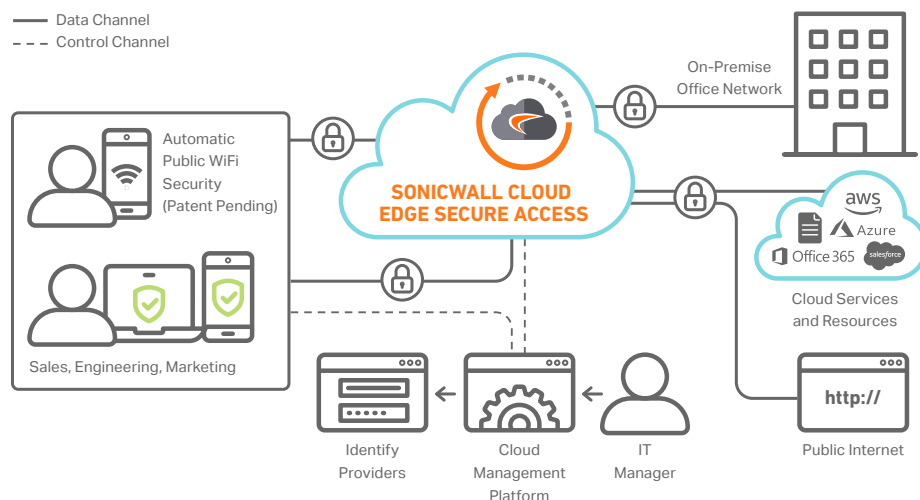
User-Centric SDP Security Model

The CSA defines a SDP as a network security model that dynamically creates one-to-one network connections between the user and only the resources they access.[4] The components include verifying a user's identity, their devices, and their role before granting access to network resources.

This network security model, based on authentication and authorization prior to network access, has been in use by the U.S. Department of Defense and Intelligence Communities for some time. In that capacity, it's called "need-to-know" access. As applied to network security, this model calls for every server to be hidden behind a remote access gateway that users must authenticate into and gain access to before any authorized service is made available. The innovation behind SDPs is the integration of device authentication, identity-based access and dynamically provisioned connectivity.

According to Gartner, the advantage of the SDP model is that "traditional attacks that rely on the default-trust flaws built into traditional TCP IP will be thwarted when using SDP, because any non-SDP-trusted traffic is discarded prior to stack processing."[5] SDPs address some of the most common network-based attacks, such as server scanning, DDoS, public Wi-Fi hijacking, SYN flood and Slowloris, with ease.

1 https://downloads.cloudsecurityalliance.org/initiatives/sdp/Software_Defined_Perimeter.pdf
2 https://www.gartner.com/newsroom/id/3744917
3 https://www.gartner.com/smarterwithgartner/gartner-top-10-security-projects-for-2018/
4 https://downloads.cloudsecurityalliance.org/initiatives/sdp/Software_Defined_Perimeter.pdf
5 https://blogs.gartner.com/lawrence-pingree/2015/09/23/software-defined-perimeter-technology-is-more-a-fancy-vpn/

SONICWALL®

Comprehensive Cloud ZTNA Solution

Many enterprises today have employees based in different global offices that rely on cloud-based productivity applications (such as Office 365, AWS or Salesforce CRM) accessed viacorporate or employee-owned Windows, iOS, macOS and Android devices.

Remote connectivity has also become critical as employees work from home or travel for business, accessing corporate networks through unsecured Wi-Fi hotspots or public networks gated by geo-restrictions and online censorship.

The challenge for IT managers is to provide secure and reliable employee access without draining IT resources and budgets. Traditional VPNs can be complicated to deploy and maintain, both from a hardware and a software perspective. This includes the integration of physical servers and site-specific applications, cloud-based infrastructure and applications, and identity access and management. Therefore, IT managers must look beyond traditional VPN to cloud-based Zero-Trust Network Access (ZTNA) that can be quickly deployed and configured in a SDP configuration.

SONICWALL®

SonicWall Cloud Edge Secure Access

SonicWall Cloud Edge Secure Access offers an advanced Zero-Trust Network Access service delivered from the cloud and controlled through a single management console. By leveraging a SDP security model, it quickly and easily secures access to on-premises and cloud resources and offers lightweight cross-platform client support for employee access.

Cloud Edge Secure Access also eliminates expensive hardware with its cloud-based infrastructure, and enables seamless deployment of endpoints with device authentication, identity-based access and dynamically provisioned connectivity for every user.

Mobile employees are protected with Secure Access' Single Sign-On native client applications that can be used on any Windows, Mac, iPhone and Android device. Secure Access' innovative Automatic Wi-Fi Security also shields all data by automatically activating VPN protection when employees connect to unknown or untrusted networks.

With centralized control and identity management integrated into the Cloud Edge Secure Access portal, employees and groups can be easily added to corporate network resources and cloud environments with secure policy-based resource access. Detailed activity reports provide insight into resource and bandwidth utilization, while active connection and session information can be monitored in real-time.

Finally, all company data passing over any network is secured with 256-bit bank-level encryption and routed through a dedicated private server, concealing a company's actual IP address with an IP mask. The Cloud Edge global network of over 700 high-speed public servers, in more than 30 locations, provides fast and simple deployment of dedicated gateways servers with dedicated IP addresses.

About SonicWall Cloud Edge Secure Access

SonicWall Cloud Edge Secure Access offers an advanced Zero Trust Network Access (ZNTA) service delivered from the cloud for the modern and distributed workforce. With the cloud-native architecture, Secure Access delivers the Zero Trust Network Access service as the next-generation VPN

Legacy Approach	SDP Approach
⊗ Hardware	⊘ Software
⊗ Complex	⊘ Simple
⊗ Expensive	⊘ Affordable
⊗ Distributed managment	⊘ Unified managment
⊗ Highly technical	⊘ User-friendly
⊗ Manual	⊘ Automatic

technology. The solution's user-friendly interface, unified management and seamless integration with major cloud services allows employees to securely access on-premise and remote resources, and gives companies of all industries and sizes the power to be fully mobile and migrate to the cloud with confidence.

Contact us

www.sonicwall.com/customers/contact-sales

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SONICWALL®

SolutionBrief-CloudEdgeSecureAccess-COG-2522