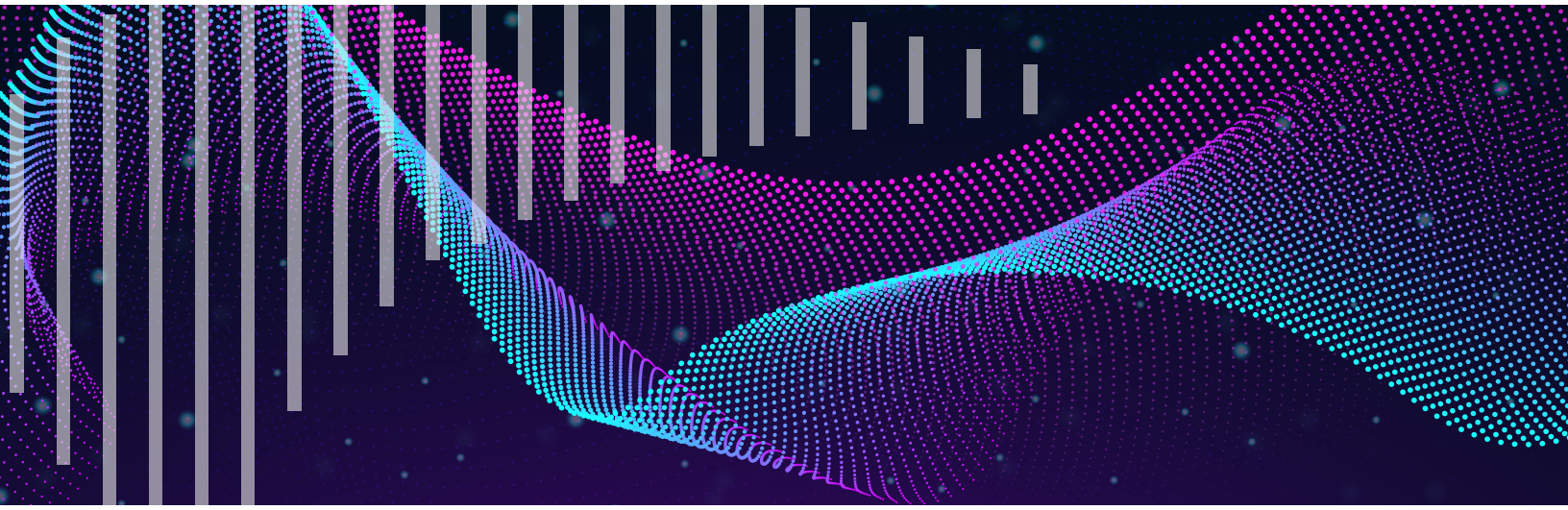
SONICWALL®



SOLUTION BRIEF

Secure Your Shared Assets With Zero Trust Security

Introduction

Driven by public and private clouds, legacy on-premises networks, and mobile devices, the definition of today's corporate network perimeter is undergoing a dynamic change. Perimeters are now fluid, as mobile workers using their own devices that can't be monitored or logged request access to corporate IT resources and applications.

In contrast, global IT infrastructures, privately-hosted data-centers, multi-vendor public cloud environments, and the trend of "Bring Your Own Device" or BYOD, ranging from mobile phones to tablets and notebook computers, further expands the network perimeter and exposes businesses to malware and hackers if an employee's device do not comply with corporate BYOD security policies.

When implementing a Zero Trust security architecture, IT managers must isolate resources within their IT infrastructure in the form of micro-segmentation.

Forrester Research recommends dividing network resources at a granular level, allowing organizations to tune security settings to different traffic types and create policies that limit network and application flows to only those explicitly permitted. This network micro-segmentation 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.

Today's modern workforce also consists of full-time employees and business partners, consultants, customers, and suppliers needing 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 represents 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.

Copyright SonicWall Inc, 2020, All rights reserved

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 costs of external hardware, maintaining a VPN is also a challenge for IT departments with limited budgets and staff.

In contrast, the Software-Defined Perimeter model addresses traditional VPN limitations by providing a flexible cloudbased platform, device and application configurability as well as accessibility, increased security, privacy and user-access control granularity and analytics.

According to the Cloud Security Alliance (CSA), Software-Defined Perimeters 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.

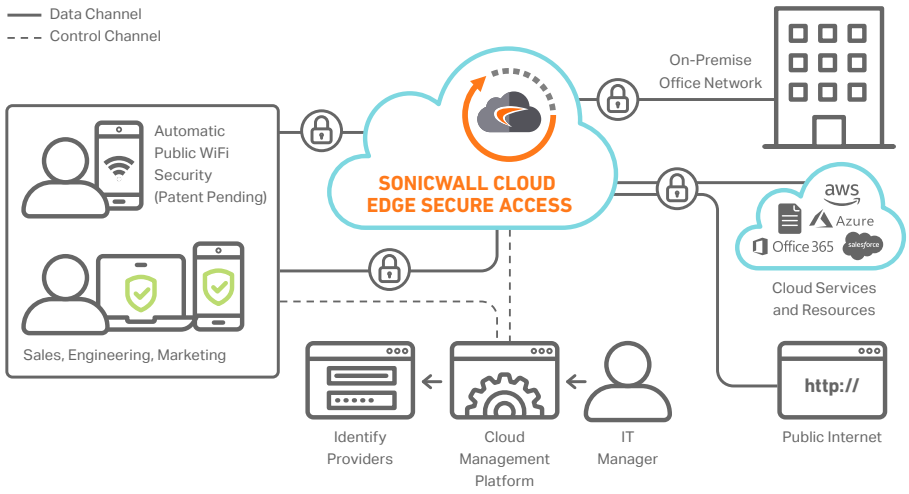
Gartner predicted that by the end of 2017 at least 10 percent of enterprise organizations would deploy Software-Defined Perimeter technology.[2] In 2018, Gartner recommended that CISOs focus on Software-Defined Perimeters as a Top 10 project that would reduce risk and make a large impact on their businesses through attack surface area reductionand IT resource limitations to only named sets of external partners, remote workers and contractors.[3]

User-Centric Software-Defined Perimeter Security Model

The CSA defines a Software-Defined Perimeter in terms of 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 the identity of the user, their devices, and 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 US Department of Defense and Intelligence Communities for some time and is known as "need to know" access. The security model calls for every server to be hidden behind a remote access gateway that users must authenticate into and gain access before any authorized service is made available. The innovation behind Software-Defined Perimeters 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, denial of service, public WiFi 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/

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 via corporate or employee-owned Windows, iOS, Mac OS, 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 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 that can be quickly deployed and configured in a Software-Defined Perimeter configuration.

Copyright SonicWall Inc, 2020, All rights reserved

SonicWall Cloud Edge Secure Access

SonicWall Cloud Edge Secure Access offers an advanced Zero Trust Network Access (ZNTA) service delivered from the cloud that quickly and easily secures access to on-premises and cloud resources combined with lightweight cross-platform client support for employee access, all controlled through a single management console. Utilizing a Software-Defined Perimeter security model, Secure Access eliminates expensive hardware with its cloud-based infrastructure that 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 Secure Access' portal, employees and groups can easily be 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.

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. Cloud Edge's 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.

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

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 technology. Secure Access' 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

https://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.

Copyright SonicWall Inc, 2020, All rights reserved

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL®

© 2020 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

SolutionBrief-CloudEdgeSecureAccess-COG-2522