SONICWALL®

SOLUTION BRIEF

All-Inclusive Zero-Trust Network Access Solution To Grow Your MSP Business

Introduction

As enterprises continue their rapid adoption and deployment of cloud services, virtual machines and containers, the number of endpoints that need to be protected is quickly rising. Cloud service providers are responsible for securing cloud service infrastructures; however, businesses are responsible for securing their exposed endpoints, data, applications, workloads and containers, both in the cloud and on-premises. This new dilemma of endpoint and resource exposure has necessitated a shift away from traditional network security solutions such as VPNs and classic firewalls, and toward the need for 24/7 visibility, and resource and user management.

The 60% of enterprises that implement appropriate cloud visibility and control tools will experience one-third fewer security failures in 2018, as estimated by analyst firm Gartner.

By using a Zero-Trust security model and next-generation secure cloud network services, Managed Service Providers (MSPs) can now create and easily secure client networks in the cloud and on-premises, accessible from anywhere globally at any time, to provide full visibility into what cloud and on-premises resources are being used and by whom.

Revenue-generating services

ZTNA services per customer

Zero Trust Security from SonicWall Cloud Edge Secure Access

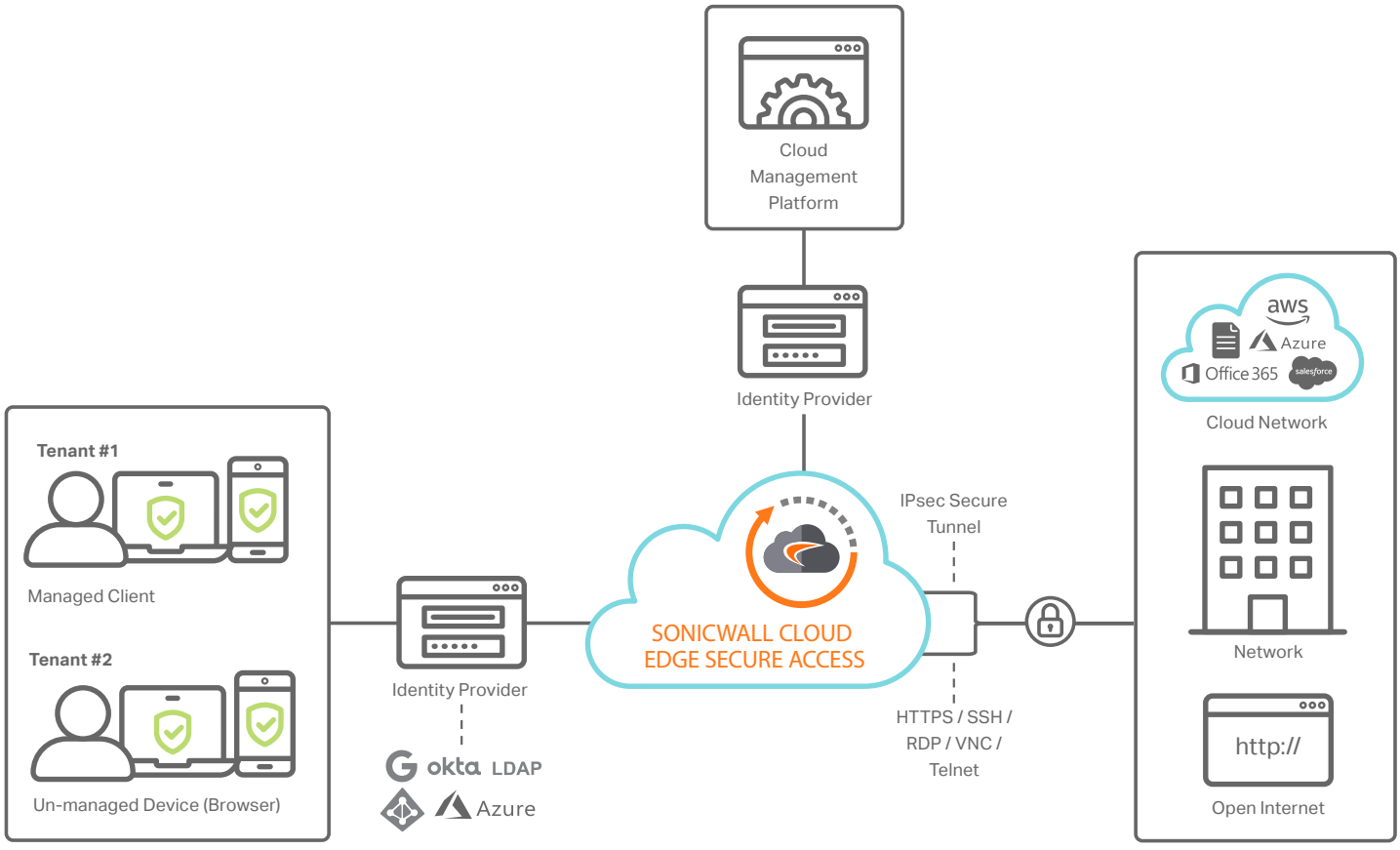
Modern-day secure remote access infrastructure consists of many disparate components. The integration goes beyond the initial deployment and configuration, extending into follow-up maintenance of different technologies, network additions, client application management and fine-tuning the identity access management services.

SonicWall Cloud Edge Secure Access offers a fully integrated Zero-Trust Security solution with multi-tenant management capabilities that can be delivered as a managed service.

Zero-Trust is a security concept based on the belief that organizations should not automatically trust anything inside or outside their perimeters, but instead verify anything and everything trying to connect to IT systems before granting access.

According to analyst firm Forrester Research, "Companies cannot afford to trust internal network traffic as legitimate, nor can they trust employees and partners to always be well-meaning and careful with systems and Zero Trust Security data. To manage the complexities of their environment without constraining their digital transformation ambitions, many companies are moving toward a Zero Trust (ZT) security model — a more identity- and data-centric approach based on network segmentation, data obfuscation, security analytics and automation that never assumes trust."

This Zero-Trust model approach to secure network access services lets Managed Service Providers (MSPs) deliver high-security, enterprise-wide network service virtually on a subscription basis for clients ranging from small and midmarket companies to large enterprises. SonicWall Cloud Edge Secure Access' market-leading, cloud-based network security platform is designed to transform secure network access for the modern and distributed workforce.



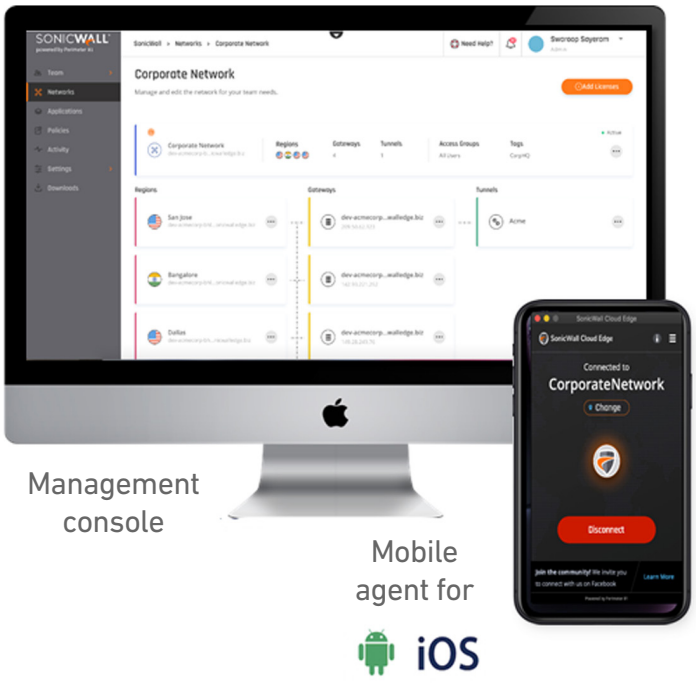
Benefits for MSPs

Traditional VPNs are less flexible in today's cloud and mobile-first technology environment. A platform with a Zero-Trust security model provides seamless integration with all leading cloud providers combined with patent-pending automatic Wi-Fi protection for today's modern mobile workforce.

This scale-as-you-go software service also requires no expensive hardware installations, offering thousands of dollars in yearly cost savings. With SaaS-based pricing, MSPs can pay as they go without any large upfront costs. MSPs can get their clients up and running quickly without tedious configurations, and all updates and upgrades are deployed through the cloud, making maintenance instant and easy.

A dedicated partner portal account management system, hands-on training, marketing resources, 24/7 partner support and deal registration are all designed to help MSPs generate recurring revenue and steady profits.

In addition to the partner portal, the multi-tenant management platform enables MSPs to manage customers, resellers, multiple organizations, team members and networks all in one place. Partners can manage billing and customer licenses, gain greater network visibility and intelligence for client accounts, and benefit from consolidated auditing and reporting. With these features, MSPs can use the new multi-tenant management platform to easily switch between multiple organizations and implement access, billing, licensing and network changes almost instantly.



Additional SonicWall Cloud Edge Secure Access' key features include:

- SSO, SAML, AD integration
- Full auditing and monitoring
- Fast gateway deployment
- Easy network segmentation
- Multi-tenancy
- Unmanaged device and BYOD support

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

At the core of the platform is the Software Defined Perimeter, a security model that addresses traditional VPN limitations while providing a flexible, cloud-based platform; device and application configurability and accessibility; increased security; privacy; and user-access control granularity and analytics.

Within the SDP security model, the concept of Zero-Trust or micro-segmentation functions as a trust broker between a client and a gateway. It does this by establishing a Transport Layer Security (TLS) tunnel terminating inside the network perimeter, thereby allowing access to applications and services.

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. 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."

User-Centric Software-Defined Perimeter Security Model

The CSA defines a Software-Defined Perimeter as a network security model that dynamically creates one-to-one network connections between the user and only the resources they access. 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 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 Software-Defined Perimeters is the secure integration of authenticated mobile devices such as tablets and phones or PCs, control over which users can access network resources and at what level, and dynamically provisioned connectivity through the use of VPN technologies.

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. SDPs address some of the most common network-based attacks."

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 VPNs to cloud-based VPNs that can be quickly deployed and configured in a Software Defined Perimeter configuration.

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

SolutionBrief-ZeroTrustMSSP-COG-3125