SONICWALL

SonicWall Cloud Edge Secure Access

只需数分钟即可部署零信任安全

SonicWall Cloud Edge Secure Access 是一项功能强大的云服务，针对站点到站点连接以及与 AWS、Azure、Google Cloud 等的混合云连接，提供简单的网络即服务。其中，它将“零信任”和“最低权限”安全方法整合成一项集成服务。

与“知所必须”概念类似，“最低访问权限”方法限制特定用户的访问权限，使其仅能访问需要的内容。通过限制访问网络的其他敏感区域，各组织可以保护其资源，而不必牺牲运营灵活性。

SonicWall Cloud Edge Secure Access 基于以下四项核心安全操作来应用零信任安全：

- 验证用户和设备的凭据，即使对于内部流量也是如此
- 执行情景式请求，以确保真实性和遵守企业准则
- 对网络访问进行微分段，防止威胁横向扩散
- 仅授予对所请求应用程序的访问权限

Cloud Edge Secure Access 基础设施的核心是现代采用安全设计的软件定义边界 (SDP) 架构。

SDP 将验证用户和设备的控制器与充当信任代理的网关分离开来。通过分配靠近最终用户位置的网关，Cloud Edge Secure Access 服务可以快速扩展，以保持高性能并提供最佳的云体验。

此外，功能分离还能有效阻止常见的网络威胁（如 DDoS、公共 WiFi 劫持、SYN 洪水攻击和 Slowloris 攻击），并使 SonicWall 能够提供高度集成的零信任安全平台。

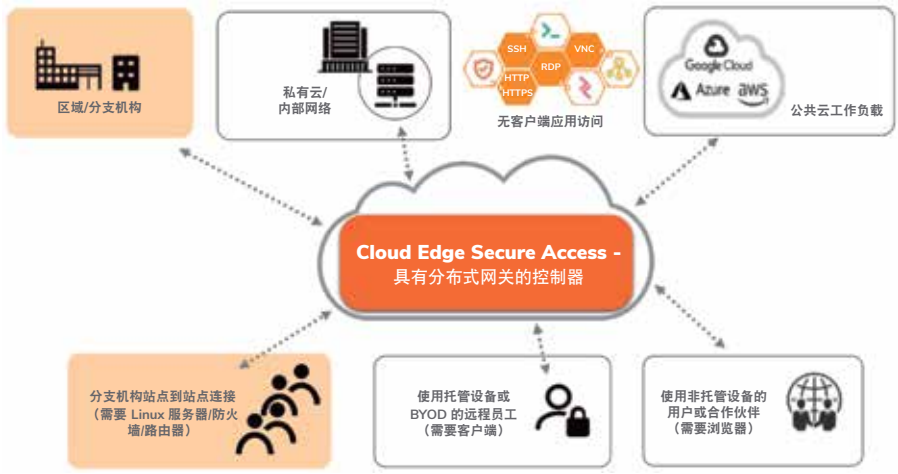

图 1 - SonicWall Cloud Edge Secure Access

优势：

- 适合分布式企业和远程员工的安全解决方案
- 快速、安全地访问混合云上的任何站点和资源
- 按网络、应用程序、用户和设备配置文件设置的零信任策略
- 内置微分段，防止未经授权的横向移动
- 用户规模从 100 扩展到成千上万
- IT 经理可在 15 分钟内完成配置
- 最终用户可在 5 分钟内完成部署
- 没有使用和带宽限制
- 公共 Wi-Fi 安全
- 高性能 WireGuard 加密
- 云身份提供程序集成
- 现代 SSO 和 MFA 集成
- 阻止 DDoS、Slowloris、SYN 洪水攻击
- 适用于 MSSP 的多租户
- 完整监控和报告，用于合规审计
- 为每位客户提供专用云网关和 IP 地址
- 该服务在美国、欧洲、中东地区和亚洲提供

传统 VPN 向零信任安全演进

在数字化转型时代，员工可以在任何地方工作，资源位于云端，而传统 VPN 解决方案过于复杂，导致无法部署，且存在太多限制。

典型的 VPN 部署可能要花费数天甚至数周的时间，且受制于供应可用性和难以安排停机时间。

传统 VPN 还可能为潜在漏洞打开后门，因为任何成功的登录都会给用户提供广泛的网络访问权限，并允许在网络子网内横向移动。

最后，VPN 还会导致额外的延迟，从而破坏用户的云体验，因为用户流量通过内部 VPN 集中器循环，而不是直接访问云端。

据 Gartner 预计，到 2023 年，60% 的企业将逐步淘汰其大部分远程访问虚拟专用网络 (VPN)，转而采用 ZTNA。

SonicWall Cloud Edge Secure Access 克服了上述问题，并为 ZTNA 提供了以下三项基本功能：

授予最低访问权限，保护企业资产

快速的自助式部署

从任意位置直接、可靠地访问云

图 2 - SonicWall Cloud Edge Secure Access 功能

主要用例

快速的自助式部署

- **快速部署 -** IT 经理可在 15 分钟内完成注册、网关实例化并基于网络和用户情景配置精细策略。
- **用户上手快速 -** 在使用公共计算机提供的浏览器时，最终用户可以选择通过移动或桌面客户端应用进行连接，也可以完全绕过客户端安装。使用自助部署模式，用户可在 5 分钟内启动和运行。
- **可靠地访问混合云 -** 完成部署之后，用户就可以从全世界任意位置快速、轻松、安全地访问内部和公共云资源。

在可信区域和公共热点区域中工作可随时随地受到保护

- **自动 Wi-Fi 防护 -** 适用于 Windows 和 mac OS 的 Cloud Edge Secure Access 代理应用程序可主动监控环境，并在公共热点区域自动激活安全访问连接。这可以保护用户免受极为常见的 Wi-Fi 拦截，以免导致数据被盗和违规。
- **终止开关 -** 为了阻止任何潜在的网络漏洞，当安全访问连接中断时，将立即断开设备与互联网的连接，从而防止从设备泄露任何数据。
- **可信 Wi-Fi 网络 -** 如果将某个 SSID 指定为可信任项，则自动 Wi-Fi 安全功能不会激活。
- **始终在线 VPN/应用程序 -** 这项便捷的功能可自动将用户或设备重新连接到一个或一组应用程序，而无需重新登录或重新验证身份。

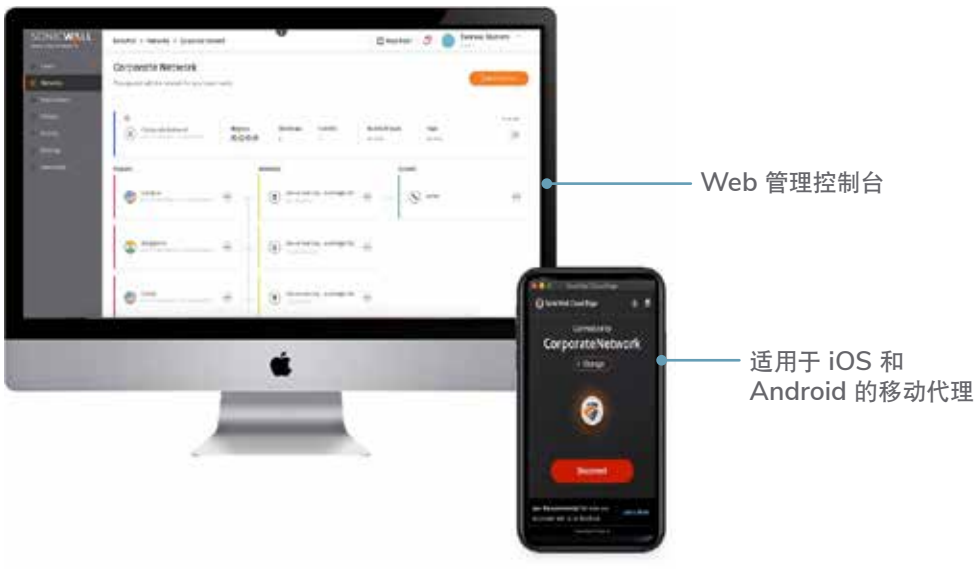

图 3 - SonicWall Cloud Edge Secure Access 管理控制台和移动代理应用程序（适用于 Apple iOS）

零信任应用程序访问

Cloud Edge Secure Access 为数字组织提供了急需的工具，以保护企业资源，同时为远程员工提供支持并赋权。

借助 Secure Access 的零信任策略，具有适当情景的外部用户可以安全地访问大量远程桌面和 Web 应用程序，而不会使企业网络面临网络威胁。

- **严格执行最低访问权限控制** - 组织可以根据相关属性（包括用户和群组身份以及所访问数据的敏感性）控制与资源的交互。
- **情景驱动** - 该解决方案可确保以用户为中心并基于策略来访问内部和云托管资源。
- **与领先的云端身份管理服务提供商集成** - 组织可以延长旧有内部资产的使用寿命，或者迁移到来自各提供商的现代云端身份管理服务，如 Azure AD、Google Authenticator 和 Okta。
- **微分段** - 通过精确分段每个传入流量，微分段可防止恶意软件或未经授权的用户横向移动，从而减少攻击面和总体网络威胁风险。
- **联合单点登录和多因素身份验证** - 该组合提供了一个单一门户，可让用户在进入混合 IT 环境时以一致、无缝的体验进行身份验证。
- **合规审计设施** - 每项零信任访问活动都得到完全监控和记录，以供未来审计之用。

图 4 - SonicWall Cloud Edge Secure Access ZTNA 流程

站点到站点的互联或网络即服务 (NaaS)

Cloud Edge Secure Access 提供了站点到站点的连接服务或网络即服务 (NaaS)，可快速引导地理位置分散的分支机构。

利用 NaaS，IT 经理可以快速、安全地将移动终端、零售店和销售点连接到云托管资源，而无需依赖昂贵的 MPLS。

- **站点到站点或站点到云互联服务** - 该解决方案可轻松连接到主流云环境（包括 AWS、Azure 和 Google Cloud），或在位于不同站点的两个不同网络之间建立安全的通信链接。
- **多区域部署** - 管理员可以在不同地点部署专用的 Cloud Edge 网关，以最佳速度为国际分支机构和员工提供最佳服务。
- **表现卓越的全球骨干网** - SonicWall Cloud Edge 服务面向全球推出。 该基础设施通过分配靠近客户位置的网关和服务器之间的负载平衡流量来提供最小延迟。
- **先进的 WireGuard 隧道** - IT 经理可以通过 IPsec 利用任何分支路由器或防火墙连接到最近的 Cloud Edge 网关。

  要实现最佳性能，SonicWall 推荐使用 WireGuard 连接器功能，该功能要求分支 Linux 服务器将 WireGuard 隧道服务安排到最近的网关。
- **网络审计与监控** - 更深入地了解网络的运行状况、活动和安全性，包括了解群组和服务器创建、团队成员身份验证、密码更改等。

规格

类别	功能	优势
规模与性能	用户	100-10000+
	性能	每个客户网关 1Gbps；使用更多网关进行横向云扩展
云平台	云管理平台	利用云管理平台，轻松创建贵组织的网络。包含在内部和云端
	快捷的网络部署	15 分钟内即可自动部署好网络
	可用性和正常运行时间	由该服务来自动管理。 要了解最新 Cloud Edge 服务状态，请访问 https://status.sonicwall.com/
	负载平衡	跨 SonicWall 托管和管理的 30 多个全球 POP，通过共享/专用网关提供
	站点到站点互联	两个站点之间的连接（本地、异地或云端）。支持 IPsec 和 WireGuard
	自定义 DNS	要使用内部 DNS 服务器，在定义隧道后，您还可以定义自定义 DNS 服务器，而不是使用默认 DNS
	无客户端应用程序访问	零信任应用程序访问 HTTP、HTTPS、RDP、VNC、SSH
	基于客户端的访问	可用于 Windows、Mac、iOS 和 Android 平台
	应用和环境	最适合混合环境和云工作负载
零信任功能	始终在线应用程序	始终在线应用程序可在连接到不受信任的网络时提供安全的互联网访问，从而保护您免受安全威胁
	基于策略的分段	按用户和应用程序来应用策略
	精细访问控制策略	基于用户、应用程序、地理 IP、地理位置（国家/地区）、浏览器类型、操作系统、日期和时间
	分离隧道	让您能够决定流量将通过哪个子网
	终止开关	为了阻止潜在的网络漏洞，当安全访问连接中断时，将立即断开设备与互联网的连接，从而防止从设备泄露任何数据
	自动 Wi-Fi 安全	我们这项获得专利的功能可自动保护连接到不安全公共 Wi-Fi 的员工设备
	DNS 过滤	阻止您网络中的用户通过互联网浏览器访问某些网站、站点类别和 IP 地址
身份验证	单点登录功能	通过单点登录提供程序（如 Okta、G Suite、Azure AD 和 Active Directory LDAP）实现统一登录
	双因素身份验证	使用内置 SMS、DUO Security 和 Google Authenticator 2FA 集成防止远程攻击
监测、记录和支持	全天候支持	包含支持的全面托管云解决方案
	活动审计和报告	监控登录、网关部署和应用连接
	SIEM 集成	实时捕获、保留安全信息和事件并将其交付给所有 SIEM 应用程序，包括与 Splunk 的轻松点击集成
	云服务状态	请访问 https://www.sonicwall.com/support
互操作性	企业防火墙	SonicWall、Check Point、Fortinet、Palo Alto Networks、WatchGuard、Sophos、Xyxel、UniFi、pfSense、Cisco 和 Untangle
自定义集成	提供 API	我们基于 REST 的全面 API 支持与第三方管理、自动化和编排工具轻松快速地集成，确保为新配置或迁移的虚拟应用程序提供保护
合规性	ISO 27001 & 27002，SOC-2 类型 2	SOC 2 类型 2 兼容云基础设施
订购	订阅	要订阅 Cloud Edge Secure Access 订阅服务，请与您的 MSSP、经销商和分销商联系

关于 SonicWall

SonicWall 为超分布式时代和每个人都远程办公、每个人都移动办公、每个人都不太安全的工作现实提供了 Boundless Cybersecurity。通过了解未知、提供实时可见性并实现经济学突破，SonicWall 为世界各地的大型企业、政府和中小企业弥补了网络安全业务缺口。有关详情，请访问 www.sonicwall.com。

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
有关详情，请访问我们的网站。
www.sonicwall.com

Datasheet-CloudEdge-US-VG-2807