SOLUTION BRIEF: BEST PRACTICES FOR SECURE MOBILE ACCESS

Stay operational regardless of what tomorrow’s headlines may bring

Abstract
Supporting business goals for today’s digital workspace requires secure mobile access, yet obstacles stand in the way of balancing security, access, performance and value. Best practices for effectively implementing a protected mobile workforce include maintaining high security, connectivity, robust performance, and low total cost of ownership. This solution brief details practical steps to achieve those best practices.

Introduction
Whether for ensuring business continuity or enhancing workforce retention and productivity, more organizations are embracing mobility, work-at-home and flex-time for their employees. To achieve business goals with a mobile and remote workforce, having a robust and reliable access security service has never been more critical. A key element of ensuring reliable mobile access is maintaining security updates, but maintenance can disrupt service and performance. Organizations need to maintain a flexible work environment without losing availability, but deploying a highly available service can be complex, costly and time consuming.

Effective cybersecurity must include secure mobile access
Providing mobile access in today’s anywhere/anytime, hyper-distributed world opens an explosion of exposure points over a myriad of potentially insecure mobile endpoint devices.

Human fallibility and risky online behavior mandate that employees cannot be trusted to ensure the security of their own mobile devices.

Moreover, the array of threat types is expanding, deepening and getting smarter, including targeted ransomware, never-before-seen threats, memory-based malware, side-channel attacks and encrypted threats.

Ultimately, the security of your mobile network must match that of your wired network.
Best Practices: Simple, safe and agile mobility

To be effective, cybersecurity must provide mobile employees with easy and secure 24/7 access to key business resources in an agile, easy-to-use, cost-effective and scalable way.

This requires a zero-trust posture regarding any mobile device attempting to connect with corporate resources, whether those resources be on-prem or in the cloud. Secure mobile access is a core component of a zero-trust approach to anywhere, anytime access.

IT must also secure access from these mobile endpoints with limited budgets and skilled staff resources.

This means streamlining deployment, availability and support to lower total cost of ownership.

SonicWall Secure Mobile Access

The SonicWall Secure Mobile Access (SMA) solution enables anywhere, anytime access across hyper-distributed enterprises. This gives your business the agility to stay operational regardless of what tomorrow’s headlines may bring.

The SonicWall SMA 1000 Series provides distributed enterprises with comprehensive end-to-end secure remote access to corporate resources hosted across on-prem, cloud and hybrid datacenters. It applies identity-based, policy enforced access controls, context-aware device authentication, and application level VPN to grant access to data, resources and applications after establishing user and device identity and trust. Flexibly deployed as a hardened Linux appliance or virtual appliance in private clouds on ESXi or Hyper-V, or in AWS or Microsoft Azure public cloud environments. The unique combination of CMS with pooled licensing and global HA could manage up to 100 SMA 1000 (6200/6210/7200/7210/8200v) appliances and provide secure access to a million concurrent users.

SMA streamlines your company’s flex work initiatives with:
- Always-On VPN
- Single Sign On (SSO) using SAML Identity Provider
- Global High Availability and Disaster Recovery
- Multi-Factor Authentication (MFA)
- Capture Advanced Threat Protection (ATP) sandboxing
- TLS 1.3 Support
- Flexible and Scalable Deployment
- Centralized Management and Pooled Licensing
- Low TCO

Conclusion

Best practices for mobile security include zero-trust access control, seamless dependability and low total cost of ownership. Fortunately, there is a viable solution to help you implement all of these best practices.

Stay operational regardless of what tomorrow’s headlines may bring.
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.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.

www.sonicwall.com