Composite VPN: A Modern Approach to Remote Access

A combined VPN approach that delivers Zero-Trust network security for your remote workforce

ABSTRACT

The collective support and growth of the remote/hybrid workforce (which is looking more permanent than temporary) has made it more challenging for IT to secure network access for the seemingly endless array of mobile devices in this environment. The SonicWall Composite VPN approach unites Secure Mobile Access (SMA) and next-generation firewall technology to protect your organization from the explosion of exposure points and new risks from remote and mobile workforces:

- *The endpoints and users*
- *The data and application resources*
- *The traffic connecting them*

Introduction

A network of personal mobile devices

Employees now work anywhere at any time. With safety a main concern for employers, we see more at-home and remote work options, and it's not just employees but partners, contractors, resellers, and more. Mobile workers need constant access to key corporate information on the network and will often use an array of devices to get to it, sanctioned or not. To extend their workday and increase efficiency, employees rely upon the same technology — including laptops, smartphones, and tablets — that they use in their personal lives.

Most modern technologies adopted by enterprises are based on consumer products. This consumerization of IT has empowered end-users to decide what computing platforms they use to do their work, whether in the office, at home, or on the road. As a result, IT has limited visibility into the endpoint devices that connect to the network.

Increasingly, organizations are embracing this concept by setting up BYOD policies that enable employees to select their personal mobile devices for use at work. They are essential – think of authenticators, MFA, and 2FA verification. Moreover, a BYOD-carrying employee adds real value to the company, research has shown they work more hours!

Security demands vary by device

There are subtle yet significant distinctions between mobile device platforms. For instance, laptops require greater endpoint control than smartphones and tablets, because these latter devices typically can download only applications that have undergone stringent allow-list screening. (This does not apply, of course, to devices that have been jailbroken or rooted to allow the downloading of non-allow-listed apps.) For unmanaged laptops, remote access security demands using reverse proxy portal access or a virtual private network (VPN) tunnel with endpoint control. This enables IT to see if the proper security applications are running on the device and enforce security policy to allow, quarantine, or deny access based on defined security policy.

For organizations wishing to embrace BYOD, flexible working, and securely enabling third-party access, the SMA 1000 series delivers a critical enforcement point. With best-in-class security, it minimizes the threat surface, secures valuable corporate assets, and ensures user confidentiality even in public hotspots. SMA empowers productivity in minutes. IT administrators can easily provide identity-based privileges to end-users, secure BYOD policies to protect their corporate networks and data from rogue access and malware.

TO PROTECT THE CORPORATE NETWORK, IT MUST RECOGNIZE THAT NO ENTITY SHOULD BE TRUSTED AND THAT ALL ACCESS OUTSIDE THE CORPORATE NETWORK IS SUSPECT.

Endpoints — and threats — are everywhere

For managed devices, the installation of a VPN client comes with the Advanced Endpoint Control™ (EPC) engine. EPC ensures risks originating from users, endpoints, or applications are evaluated before granting data access. Remediation actions, such as session quarantining and alerting, are enforced to minimize user frustration and reduce helpdesk calls.

IT must take comprehensive measures to protect corporate resources from unmanaged devices as well . Data in flight is vulnerable to man-in-the-middle and eavesdropping attacks, and therefore must be encrypted. IT should scan all data-in-flight for malware and prevent internally launched outbound botnet attacks that can damage corporate reputation and get business-critical email servers block-listed. At the same time, IT should deploy a solution that can inspect outbound traffic for data leakage, even if that traffic is encrypted.

A "Composite VPN" — combining SSL VPN with a next-generation firewall — can deliver these protections and more.

The SonicWall Composite VPN approach

SonicWall Composite VPN delivers the critical dual protection of SSL VPN and high-performance, next-generation firewall necessary to secure both VPN access and traffic. The combined approach of Composite VPN enables organizations to decrypt and scan for malware on all authorized SSL VPN traffic before it enters the network environment.

- The SSL VPN component of Composite VPN leverages SonicWall Secure Mobile Access (SMA) with Advanced End Point Control™ (EPC) to protect the integrity of VPN access. In addition, support for modern multi-factor authentication comes standard. Access is limited to only trusted users and devices, using context-aware authorization and 2FA. Whether the corporate resource is on-premises, on the web, or in a hosted cloud, the access experience is consistent and seamless.
- The next-generation firewall component of Composite VPN simultaneously secures the integrity of VPN traffic. It authorizes VPN traffic, cleans inbound traffic for malware and vulnerabilities, and verifies all outbound VPN traffic in real-time. This ensures that user data-in-flight receives the same security scanning whether it is from inside or outside the corporate network. SonicWall Application Intelligence and Control provides granular control and real-time visualization of applications to guarantee bandwidth prioritization for business-critical apps and ensure maximum network security and productivity.

Deployment options

SonicWall offers administrators the flexibility and scalability of deploying Composite VPN in two ways:

- Integrated Composite VPN deployment—Administrators can establish a Composite VPN by using the integrated SSL VPN on SonicWall NS*a*/ NS*sp*/ NS*v* Series and TZ Series firewalls.
- Combined Composite VPN deployment—Alternately, administrators can establish a Composite VPN by combining a SonicWall next-generation firewall with a SonicWall Secure Mobile Access (SMA).

Integrated Composite VPN deployment

In an integrated Composite VPN approach, SonicWall next-generation firewalls, featuring Reassembly-Free Deep Packet Inspection® (RFDPI) technology, apply tightly integrated intrusion prevention, malware protection, and application intelligence, control, and real-time visualization

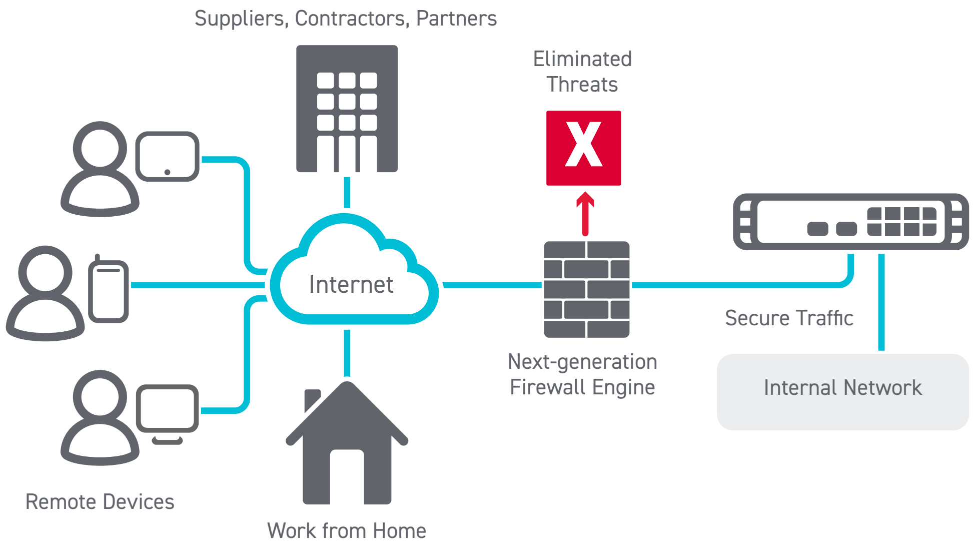


Figure 1. An integrated Composite VPN approach using the integrated SSL VPN on SonicWall next-generation firewalls

to SSL VPN traffic from laptops, smartphones, and tablets. SonicWall next-generation firewalls scan all inbound and outbound traffic and scale to meet the needs of the highest-performance networks. Tightly integrated application intelligence, control, and visualization help administrators control and manage both business and non-business-related applications to enable network and user productivity.

An integrated Composite VPN approach lets administrators prioritize bandwidth available over the SSL VPN for business-critical applications. For SSL VPN access over SonicWall's next-generation firewalls, SonicWall NetExtender provides thin-client access for Windows, Windows Phone and Linux-based systems.

SonicWall Mobile Connect™ mobile applications for iOS, macOS, Android, and Chrome OS provide smartphone and tablet users with fast, easy network-level access to corporate, academic, and government resources over encrypted SSL VPN.

Only SonicWall offers a Composite VPN (when deployed with a SonicWall next-generation firewall) to authorize, decrypt and remove threats from all major mobile platforms traffic over SSL VPN outside the network perimeter. Additionally, SonicWall Application Intelligence and Control allows organizations to define and enforce how application and bandwidth assets are used.

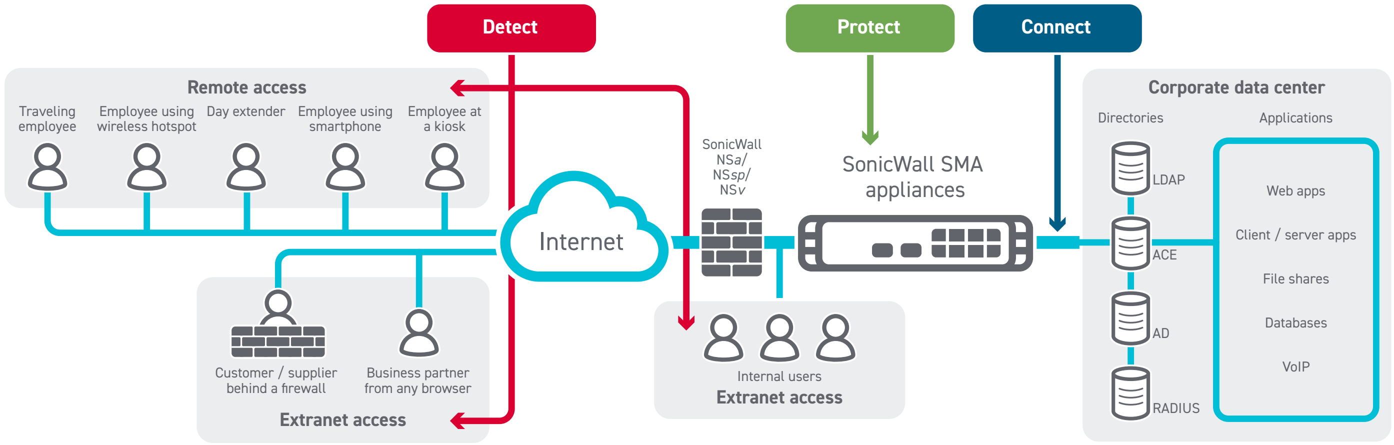
AN INTEGRATED COMPOSITE VPN APPROACH ENABLES ADMINISTRATORS TO PRIORITIZE BANDWIDTH AVAILABLE OVER THE SSL VPN FOR BUSINESS-CRITICAL APPLICATIONS.

Combined Composite VPN deployment

A combined Composite VPN approach delivers all the security and SSL VPN elements of an integrated Composite VPN deployment, plus the added SonicWall SMA capability to perform device interrogation and enforce policy-based endpoint controls.

A combined Composite VPN using SonicWall SMA

SonicWall EPC (End Point Control) integrates unmanaged endpoint protection and comprehensive cache control. EPC offers advanced endpoint detection and data protection for enterprises by interrogating endpoint devices to confirm the presence of all supported anti-virus, personal firewall, and anti-spyware solutions from a comprehensive, predefined



Detect SonicWall SMA End Point Control continually detects the identity and security state of the end device

Protect SonicWall SMA Unified Policy enforces devices access control, ensuring users access only to authorized applications

Connect SonicWall SMA Smart Access and Smart Tunneling ensure easy, secure user access to all network resources

Figure 2. A combined Composite VPN approach using a SonicWall next-generation firewall with a SonicWall SMA appliance

list. When used in conjunction with SonicWall Connect Tunnel & Mobile Connect, policy-based identification and enforcement also extend to all major mobile platforms. This allows IT to enforce a DeviceID, restrict devices from which users can log in, ensure the presence of client certificates, and determine whether an iOS device has been jailbroken or an Android device has been rooted.

SonicWall SMA 1000 supports Zero-Trust Access architecture with 2FA user verification, device verification and continuous monitoring (EPC), segmented app access, and Least-Access Privilege policy enforcement. When combining the CMS with pooled licensing and global high availability, the infrastructure could manage up to 100 SMA (6200/6210/7200/7210/8200v) appliances and provide secure access for up to a million concurrent users. SMA enhances productivity and business continuity with policy-enforced remote access to network resources from Windows, Apple Mac OS, iOS, Linux, and Android devices.

Built on the powerful, best-of-breed SonicWall SSL VPN platform, SMA connects authorized users only to what they need, limiting exposure and preventing threats from moving laterally. SMA solutions support Vasco, RSA, Active Directory, LDAP, RADIUS, and SAML, as well as integrated One-Time Password (OTP) generation for two-factor authentication.

A combined Composite VPN approach incorporating a SonicWall SMA solution can:

- Detect the integrity of users, endpoints, and traffic from beyond the traditional network perimeter.
- Protect applications and resources against unauthorized access and malware attacks.
- Securely connect authorized users in real-time with Least-Access Privilege policies.

A combined Composite VPN using a SonicWall SMA solution for SMBs

An administrator for a small- to medium-sized business can also establish a combined Composite VPN by connecting a SonicWall next-generation firewall with a best-selling SonicWall SMA for the SMB.

The SMA offers clientless and tunnel access for Windows, Windows Phone, macOS, iOS, Linux, and Android, plus optional Web Application Firewall, and multi-platform remote support. The SMA offers a granular unified policy, two-factor authentication, load balancing, and high availability. The SMA lets authorized mobile workers and contractors connect over SSL VPN using the Mobile Connect application or a standard web browser. Easily and flexibly deployed into any network with no pre-installed clients, the SMA also cuts the costs of deploying and maintaining traditional IPsec VPNs.

Integrated Composite VPN	
Technology	SonicWall Solution
Next-generation firewall	NSa/NSsp/NSv Series, TZ Series
Deep packet inspection	Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service
Application intelligence, control and visualization	Application Intelligence and Control Service
SSL VPN	Mobile Connect, Net Extender

Combined Composite VPN	
Technology	SonicWall Solution
SSL VPN	SMA with Advanced End Point Control, Connect Tunnel and Mobile Connect
Next-generation firewall	NSa/NSsp/NSv Series
Deep packet inspection	Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service
Application intelligence, control and visualization	Application Intelligence and Control Service

Figure 3. Comparing the two Composite VPN deployment options

Conclusion

SonicWall has strategically positioned itself as an industry leader in pioneering Composite VPN technology solutions for organizations of all sizes by enabling the managed integration of its award-winning Secure Mobile Access, next-generation firewall, and management and reporting product lines. The integrated or combined deployment of these solutions offers organizations a single solution for securely connecting their remote workforce.

A SonicWall Composite VPN can detect the identity of users and the security state of the endpoint device; protect against malware and unauthorized access based on a granular policy before authorizing access and connect authorized users easily to mission-critical network resources. Only SonicWall can deliver a truly practical Composite VPN with Zero-Trust, least-access privilege policies, and the revolutionary, ultra-high-performance security of Reassembly-Free Deep Packet Inspection® over a multi-core processing platform.

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

SONICWALL®

© 2022 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.