THE SONICWALL CLEAN VPN APPROACH FOR THE MOBILE WORKFORCE

A Clean VPN approach delivers layered defense-in-depth protection for the core elements of business communications.

Abstract

The consumerization of IT and "bring your own device" (BYOD) policies have made it more challenging for IT to secure network access for mobile laptops, smartphones and tablets. The SonicWall™ Clean VPN™ approach unites SSL VPN secure remote access and next-generation firewall technology to deliver layered defense-in-depth protection for the core elements of business communications:

- 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. In the U.S. alone, half of all information workers now split their time between the office, home and other remote locations. Mobile workers need constant access to key corporate information on the network.

The notion that employees conduct business only on IT-issued equipment within the traditional network perimeter is passé. 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.

In fact, the majority of new technologies adopted by enterprises are based in consumer products. This consumerization of IT has empowered end users to determine what computing platforms they use to do their work, whether in the office, at home or on the road. As a result, IT is losing control over what endpoint devices connect to the network.

Increasingly, organizations are embracing this concept by establishing BYOD policies that enable employees to select their own personal mobile devices for use at work. Allowing employees to use their own privately purchased mobile devices also adds the budgetary incentive to offset upfront hardware inventory costs.

Security demands vary by device

There are subtle yet significant distinctions between consumer mobile device platforms. For instance, laptops generally require greater endpoint control than smartphones and tablets, because these latter devices typically can download only applications that have undergone stringent white-list screening. (This does not apply, of course, to devices that have been jailbroken or rooted to allow the downloading of non-white-listed apps.) For unmanaged laptops in particular, 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.

Mobile platforms are generally perceived to be safer since most application distribution is done through white-listed stores only. Regardless, it would be a mistake to simply trust either the applications or the data flowing through such devices. Threats do exist, and there are multiple ways to take advantage of devices if security is not implemented specifically for these platforms.

> To protect the corporate network, IT must recognize that no mobile device should be trusted and that all access outside the corporate network is beyond IT control.

Endpoints — and threats — are everywhere

To protect the corporate network, IT must recognize that no mobile device should be trusted and that all access outside the corporate network is beyond IT control.

There is also potential for data loss and leakage, whether by theft, unauthorized transmission or unauthorized access, even on supposedly "unhackable" smartphone platforms. Mobile devices can retain sensitive or proprietary data while connected to the corporate wireless network and then leak it over unsecured cellular to the web via email attachments and FTP uploads.

IT must take comprehensive measures to protect corporate resources from existing and evolving threats. 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 blacklisted. At the same time, IT should deploy a solution that is capable of inspecting outbound traffic for data leakage, even if that traffic is encrypted.

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

The SonicWall Clean VPN approach

SonicWall Clean VPN delivers the critical dual protection of SSL VPN and high-performance, next-generation firewall necessary to secure both VPN access and traffic. The multi-layered protection of Clean 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 Clean VPN leverages SonicWall Secure Mobile Access (SMA) with Advanced End Point Control™ (EPC) to protect the integrity of VPN access. EPC establishes trust for remote users and their endpoint devices using enforced authentication, data encryption, and granular application-layer access policy. EPC can determine whether an iOS device has been jailbroken or an Android device has been rooted so that connections from those systems can be rejected or quarantined.

- The next-generation firewall component of Clean 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 Clean VPN in two ways:

- Integrated Clean VPN deployment—Administrators can establish a Clean VPN by using the integrated SSL VPN on SonicWall SuperMassive Series, NS*a*/ NS*sp*/ NS*v* Series and TZ Series firewalls.

- Combined Clean VPN deployment—Alternately, administrators can establish a Clean VPN by combining a SonicWall next-generation firewall with a SonicWall Secure Mobile Access (SMA).

Integrated Clean VPN deployment

In an integrated Clean 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 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 helps administrators control and manage both business and non-business related applications to enable network and user productivity.

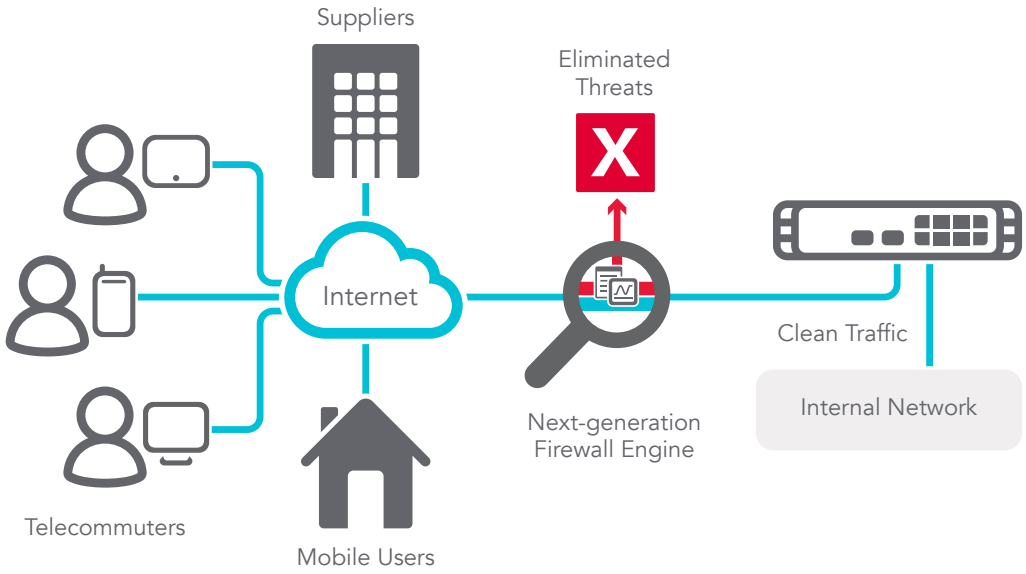

Figure 1. An integrated Clean VPN approach using the integrated SSL VPN on SonicWall next-generation firewalls

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

SonicWall Mobile Connect™ mobile applications for iOS, OS X, Android, Chrome OS, Kindle Fire and Windows 10 provide smartphone and tablet users with fast, easy network-level access to corporate, academic and government resources over encrypted SSL VPN.

> An integrated Clean VPN approach enables administrators to prioritize bandwidth available over the SSL VPN for business-critical applications.

Only SonicWall offers Clean 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.

Combined Clean VPN deployment

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

A combined Clean VPN using SonicWall SMA

SonicWall EPC (available for Windows, Macintosh and Linux-based devices) integrates unmanaged endpoint protection, Secure Virtual Desktop 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 leading vendors such as McAfee®, Symantec®, Computer Associates®, Sophos® and Kaspersky Lab®. When used in conjunction with SonicWall Mobile Connect, policy-based identification and enforcement also extends 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.

When combined with a SonicWall next-generation firewall as a Clean VPN, SMA delivers centralized access policy control and malware protection.

SonicWall SMA delivers full-featured, easy-to-manage, clientless or thin-client "in-office" connectivity for up to 20,000 concurrent mobile-enterprise users from a single appliance. 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 only authorized users to only authorized resources. Moreover, SMA solutions support Vasco, RSA, Active Directory, LDAP, RADIUS and SAML, as well as integrated One-Time Password (OTP) generation for two-factor authentication.

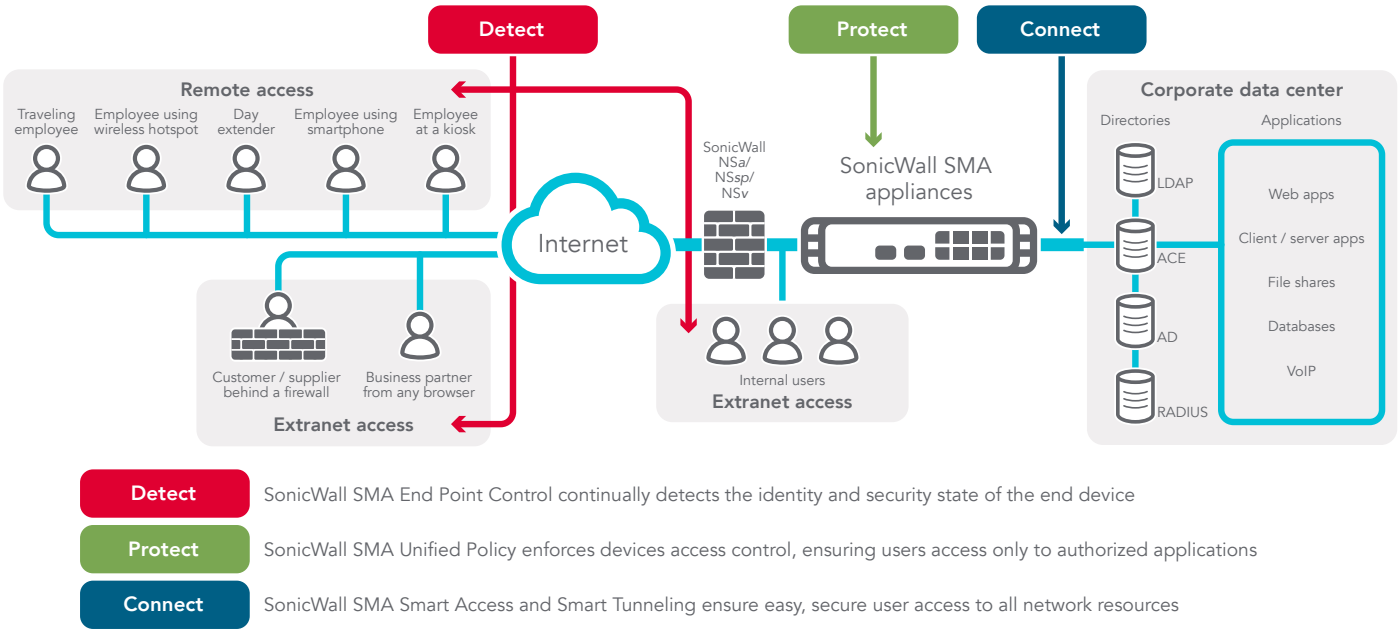

Figure 2. A combined Clean VPN approach using a SonicWall next-generation firewall with a SonicWall SMA appliance

A combined Clean VPN approach incorporating a SonicWall SMA solution is able to:

- Detect the integrity of users, endpoints and traffic from beyond the traditional network perimeter.
- Protect applications and resources against unauthorized access and malware attacks.
- Connect authorized users with appropriate resources seamlessly and easily in real time.

A combined Clean VPN using a SonicWall SMA solution for SMBs

An administrator for a small- to medium-sized business can also establish a combined Clean 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, Mac OS, iOS, Linux and Android, plus optional Web Application Firewall and multi-platform remote support. The SMA offers 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 virtually any network with no pre-installed clients, the SMA also eliminates costs of deploying and maintaining traditional IPSec VPNs. SonicWall Secure Virtual Assist permits Windows-based technicians to support Windows, Mac OS or Linux devices remotely.

Managing a combined Clean VPN

Moreover, the SonicWall Global Management System (GMS) allows administrators to configure and manage their combined Clean VPN implementation from a single management interface. SonicWall GMS delivers a flexible, powerful and resilient platform to centrally manage and rapidly deploy SonicWall appliances and security configurations. In addition, it provides centralized, real-time monitoring and comprehensive policy and compliance reports for even the most stringent auditing and regulatory compliance requirements.

In addition, SonicWall Analyzer delivers an easy-to-use, web-based traffic flow analytics and reporting tool that provides real-time and historical insight into the health, performance and security of the network. Analyzer supports SonicWall firewalls and secure remote access devices while leveraging application traffic flow analytics for security event reports. Organizations of all sizes benefit from enhanced employee productivity, optimized network bandwidth utilization and increased security awareness. SonicWall is the only firewall vendor that provides a complete solution that combines off-box application traffic flow analytics with granular IPFIX data generated by SonicWall firewalls.

Integrated Clean VPN	
Technology	SonicWall Solution
Next-generation firewall	SuperMassive Series, NS*a*/ NS*sp*/ 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 Clean VPN	
Technology	SonicWall Solution
SSL VPN	SMA with Advanced End Point Control, Connect Tunnel and Mobile Connect
Next-generation firewall	SuperMassive and NS*a*/ NS*sp*/ NS*v* 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 Clean VPN deployment options

Conclusion

SonicWall has strategically positioned itself as an industry leader in pioneering Clean VPN technology solutions for organizations of all sizes by enabling the managed integration of its award-winning secure remote access, next-generation firewall and management and reporting product lines. The integrated or combined deployment of these solutions offers organizations a single solution for defense-in-depth security.

A SonicWall Clean VPN can detect the identity of users and the security state of the endpoint device; protect against malware and unauthorized access based on granular policy before authorizing access; and connect authorized users easily to mission-critical network resources. Only SonicWall is capable of delivering a truly viable Clean VPN, because only SonicWall can offer granular endpoint control, a unified policy model allowing dynamic access 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.

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