



Clean VPN Approach to Secure Remote Access

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

CONTENTS

Extending Business Beyond the Perimeter	2
A Clean VPN Approach	3
The SonicWALL Clean VPN™ Solution	5
Conclusion	6

Abstract

Modern business practices have extended users, endpoints, traffic and resources beyond the limits of the traditional network perimeter. To remain viable, therefore, today's security solutions must enable and extend business beyond that perimeter. Status quo proprietary solution vendors recommend complex—and often expensive—retrofitting of perimeter defenses, even though the modern network perimeter has become inherently insecure. Alternatively, a “clean VPN” scenario integrates secure remote access and network security appliance technology to deliver layered defense-in-depth protection for the core elements of business communications: the endpoints and users; the data and application resources; and the traffic connecting them.

Extending Business Beyond the Perimeter

Once upon a time, IT managers could rest assured that their users, computers, data and applications all sat tight behind a hardened LAN. In a perfect world, IT would prefer to simply block all access to the resources from beyond the traditional network perimeter.

Modern business practices, however, have exploded beyond that traditional perimeter. The business benefits of networking beyond the perimeter, and the explosive acceptance of mobile technology by the workforce at large, have made the traditional hardened network model functionally obsolete. IT now must address network security in a way that enables and extends business beyond the perimeter.

Extending users beyond the perimeter

Today, workers do their jobs from field offices and home offices, partner sites and manufacturing sites. Employees, contractors and outsourced specialists can work from anywhere in the world, at any time of day or night, allowing businesses to leverage more flexible and affordable staffing pools. Traveling executives access network resources from their hotels and airline red carpet rooms. Prospects and customers are engaged via Web transactions, remote point-of-sale kiosks and interactive displays. Partners, vendors and consultants collaborate in cross-functional teams requiring access to “inside” application resources from “outside” offsite locations, traversing internal and external third-party firewalls. Employees ensure business continuity after natural disasters or unexpected disruptions by working either from home or other contingent sites.

Unfortunately, however, while today's user can work from virtually anywhere, their identities can be stolen, hacked, sniffed or inappropriately shared. Mobile devices can also get lost, stolen or borrowed by family members. The user attempting access cannot always be trusted to be the person they claim to be.

Extending endpoints beyond the perimeter

As mobile computing has become more cost-effective and popularly embraced, WiFi-enabled laptops, ultra-portable PDAs and 3G cellular smartphones have overtaken the predominant business role of traditional desktops. And where desktops and other fixed-site endpoint devices are still being used, they are more commonly situated in locations outside the network perimeter, such as in homes, on third-party partner or customer networks, or as public access Internet kiosks in airports, hotels and cafés.

As intended by design, mobile computing devices are routinely transported off and on site, and connected wirelessly over public and private networks. Yet the very mobility of these devices creates and expands opportunities for potential security breaches. Outside of IT control, these devices often can be damaged, reconfigured, or lack fundamental security maintenance and updates.

Extending traffic beyond the perimeter

Network traffic no longer consists only of store-and-forward and session-based applications like e-mail, Web pages and traditional client/server applications, but have expanded to include real-time collaboration tools, Web 2.0 applications, IM, peer-to-peer applications, VoIP, streaming media and telepresence conferencing.

A majority of business network traffic now either originates from or traverses endpoint devices located beyond the perimeter, opening new conduits for evolving threats. With new methods of gaining entry, savvy and financially-motivated criminal attackers have unleashed ultra-sophisticated threats, increasing the risk of compromised data, systems downtime, reduced productivity, bandwidth consumption, and monetary theft.

Extending resources beyond the perimeter

Business is increasingly dependent upon access to mission-critical resources from inside and outside the traditional LAN perimeter. Core business applications are being outsourced to third-party niche specialists and hosted Software as a Service (SaaS) providers.

Mission-critical and sensitive information is stored and computed on remote and mobile endpoint devices. Today, IT needs to take steps to secure data flowing in and out of these external resource repositories, as well their own corporate data centers.

A “Clean VPN” Approach

Traditional enclosed business LANs have rapidly evolved into distributed global networks that connect employees, partners and customers over multiple Internet and intranet, private and public, wired and wireless networks. IT now looks for ways to leverage public networks and shared infrastructure, while users demand greater reliability and transparency of service.

These trends run counter to arguments by status quo proprietary solution vendors to develop “smarter” networks through complex—and often expensive—retrofitting of perimeter defenses. Instead, the underlying premise for ongoing security decisions is that the perimeter of any functionally accessible network must be considered inherently insecure. The focus for IT security shifts to refining control over the core elements of the business communications: the endpoints and users; the data and application resources; and the traffic connecting them.

To ensure thorough protection of all of these elements, best practices warrant utilization of multiple layers of defense. Such a defense-in-depth approach could secure access to resources by users and endpoint devices beyond the perimeter, as well as secure data traffic penetrating the perimeter.

A “clean VPN” approach establishes intelligent layers of secure remote access, gateway firewall, and policy control by integrating SSL VPN (Secure Sockets Layer virtual private network) and UTM (Unified Threat Management). To be practically effective, a clean VPN must be 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

Detecting integrity of endpoints, users and traffic

SSL VPN technology can enable the interrogation of the endpoint to verify the presence or absence of attributes (e.g., operating systems, applications, domain membership, certificates, files, anti-virus, anti-spyware, personal firewalls, etc.) that are required to adhere to IT security policy, before authorizing access to a clean VPN.

Even so, there may still be potential for malicious packets to breach the network when connections are established from untrusted endpoints like home computers or kiosks, where specific security applications would be practically difficult to enforce. By integrating high-performance Unified Threat Management (UTM) technology with the SSL VPN, all traffic could be scanned and decontaminated before traversing the resource perimeter. Because modern attacks can pass undetected through stateful packet inspection, the UTM component of a clean VPN should be engineered to conduct deep packet inspection of the entire traffic data stream.

Protecting resources against unauthorized access and attacks

With businesses extending beyond the traditional LAN perimeter, IT no longer has final say on securing corporate data. The majority of both private and public sector organizations must now comply with governmental and industry regulations (e.g., HIPAA, GBLA, SOX and PCI) that mandate the protection of sensitive data resources under penalty of significant fines or business restrictions.

A clean VPN can protect resources through enforced authentication, data encryption, granular access policy and gateway threat protection. An effective clean VPN policy engine should control admission based upon the level of trust for each remote user and endpoint device, and control access based upon the applications that each user is authorized to access. Different access policy should be enforced depending upon whether the endpoint is a fully IT-managed device, or an unmanaged public or personal device.

While access controls are critical to protecting resources, even the most granular access controls potentially could be undermined by ultra-sophisticated criminal attacks and evolving threats. Best practices for a clean VPN warrant the additional layered protection of a comprehensive UTM firewall on the resource perimeter that can deliver auto-updating anti-virus, anti-spyware, intrusion prevention and content filtering.

Connecting users to resources easily in real-time

Optimally, a clean VPN should be designed to intelligently and seamlessly connect users to authorized resources based upon device interrogation, user authentication and access policy, while employing an access method and interface appropriate to the specific endpoint device (e.g., laptop, PDA, smartphone, hotel kiosk, etc.).

To prevent performance bottlenecks, a clean VPN must be configured to balance traffic policy enforcement with system performance. The UTM firewall component should also be able to alert administrators to any bandwidth anomalies that could infer policy abuse, and trigger appropriate use restrictions. Any clean VPN environment must be engineered leveraging ultra-high-performance architecture, such as multi-core processor platforms, to enable comprehensive scanning of bandwidth-intensive mobile traffic in real time without bringing network throughput to a standstill.

Centralized management and reporting

In order to ensure compliance beyond the perimeter, it is also crucial for IT to have centralized management that can generate comprehensive event reporting, proactive alerts, rapid forensic analyses and complete audit trails. Integrating dedicated security management oversight simplifies administration, helps identify gaps or anomalous activity, and facilitates regulatory compliance audits.

The SonicWALL Clean VPN Solution

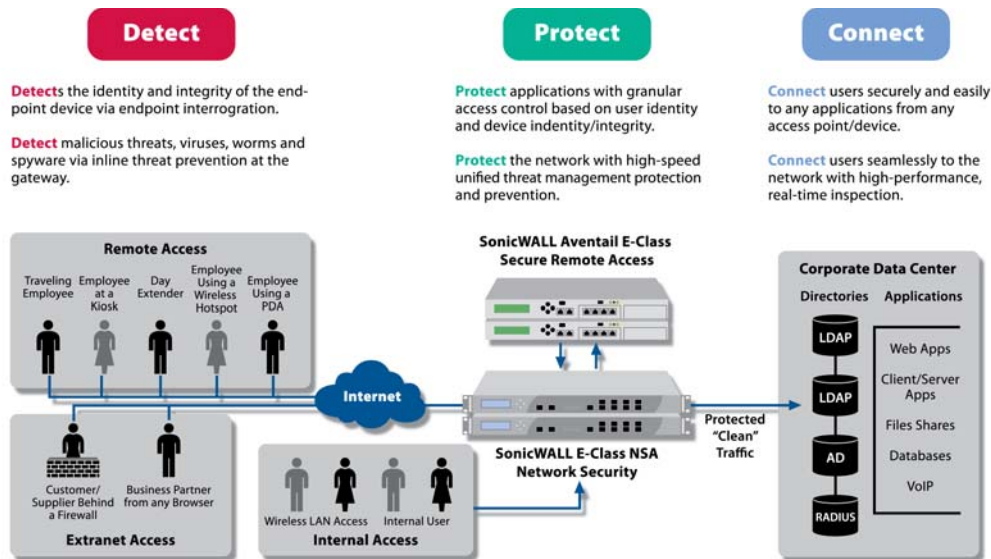
SonicWALL® has strategically positioned itself as an industry leader in pioneering clean VPN technology solutions for organizations of all sizes by enabling the managed integration of its award-winning Secure Remote Access, Network Security Appliance and Global Management System product lines. The SonicWALL Clean VPN™ solution unites next-generation SSL VPN and UTM technologies to enforce granular application-layer access policies while comprehensively inspecting all traffic at the gateway, all the while correlating event information to streamline and enhance security efficiencies.

A SonicWALL Clean VPN scenario

SonicWALL Secure Remote Access solutions feature the best-selling SSL VPN product line in the world, including the best-of-breed SonicWALL Aventail® E-Class SSL VPN. Aventail End Point Control™ interrogates every endpoint device to check for specific criteria or attributes needed to adhere to security policy, such as running applications, domain membership, certificates, files, and common anti-virus, anti-spyware and personal firewall applications.

To add a layer of UTM protection to the SonicWALL Clean VPN solution, a SonicWALL Network Security Appliance (NSA) or E-Class NSA component could be deployed in conjunction with the SSL VPN component. SonicWALL's multi-core NSA architecture and patented Reassembly-Free scanning technology delivers ultra-high-speed Deep Packet Inspection, Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Content Filtering and Application Firewall capabilities. The SonicWALL NSA component ensures that all traffic is scanned in real time and decontaminated before traversing the Clean VPN.

Finally, the SonicWALL Global Management System (GMS) component allows administrators to configure and manage their entire 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 delivers comprehensive policy and compliance reports for even the most stringent auditing and regulatory compliance requirements.



Conclusion

The integration of SonicWALL SSL VPN/Secure Remote Access, SonicWALL Network Security Appliance, and SonicWALL Global Management System solutions offer organizations a single solution for defense-in-depth security. A SonicWALL Clean VPN can detect the identity of users and 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.