

Increase Productivity and Reduce Security Risks for Teleworkers

An overview of how teleworking helps meet today's productivity demands, what additional network security risks anywhere access can create, and how SonicWALL Aventail E-Class SSL VPN solutions addresses these concerns while offering additional benefits for today's mobile workforce.

CONTENTS

Teleworking is Emerging as Standard Operating Procedure	2
Security Risks Posed by Teleworkers	3
SonicWALL Aventail E-Class SSL VPNs Reduce the Security Risks of Teleworking	4
SonicWALL Aventail E-Class SSL VPNs Protect Your Resources with Maximum Security for Teleworkers	5
Manageability and Cost Effectiveness Enhance IT Productivity	9
SonicWALL Aventail E-Class SSL VPNs: the Best Choice for Remote Worker Productivity and Security	11

Abstract

Today, people work in more places more often. They use corporate laptops, home computers or airport kiosks. And they expect access to corporate resources from as many places as possible. With expanded access capabilities, organizations improve employee productivity. Yet, as productivity increases, so do risks to your network.

You want to give your users a solution that offers complete mobility and transparency so they can work more productively from anywhere. But to an IT professional, it's unthinkable to give users anywhere access without an underlying platform that makes it secure, scalable, and manageable. That's where SonicWALL Aventail's proven experience puts us ahead. SonicWALL® Aventail® E-Class SSL VPNs are designed specifically to enable increased productivity for teleworkers and other remote users, while minimizing many associated risks and costs.

This paper provides an overview of how teleworking helps meet today's productivity demands, what additional network security risks anywhere access can create, and how SonicWALL addresses these concerns while offering additional benefits for today's mobile workforce.

Teleworking is Emerging as Standard Operating Procedure

Ubiquitous computer technology and connectivity enable people to do their jobs virtually anywhere and at any time—while traveling or at home. Increasingly, “the office” is anywhere employees can get an Internet connection to access the resources they need. As a result, workers enjoy more flexibility in their work hours and work locations, leading to increased job satisfaction. Organizations benefit from extended work hours and improved employee productivity and morale. Several factors contribute to the growing number of teleworkers and increase in alternative work environments.

Inexpensive computing equipment and broadband connectivity

A desktop PC that used to cost \$2,000 a few years ago may cost under \$500 today, and the cost of portable PCs and mobile devices has also dropped significantly. At the same time, subscription costs for residential broadband service have decreased, proliferating access to high-speed connections. Many more employees can be cost-effectively equipped to work anywhere, any time.

Increased employee comfort with technology and connectivity

As the 10-hour work day is now typical at many companies, employers and employees increasingly blend professional and personal tasks. Many employees regularly respond to e-mail and work on critical projects from home. People have formed new habits of accepting and relying on technology in everyday life—regardless of their location.

Employees prefer flexible, around-the-clock, anywhere access

For maximum efficiency, today's mobile workers need around-the-clock access to key information, collaboration tools, and business applications. Employees who telework may experience greater job satisfaction than their onsite peers, and reduced levels of stress, due to control they have over organizing their tasks on a day-by-day basis. Anytime, anywhere access can contribute to worker satisfaction by enabling increased flexibility in work hours, better work/family balance, reduced commute times, and therefore, improved morale.

Disaster recovery drives need for teleworker contingency plans

Disaster recovery has become an urgent issue for governments and enterprises due to recent natural disasters, terrorist activities and the pandemic threats. Still, disaster recovery could also be triggered by something as simple as a snow storm, power outage or any other event that keeps your workers from

getting to the office. Disruptions to normal business operations often result in missed opportunities, lost revenue and a damaged reputation. Remote access is critical for any disaster recovery plan.

Tangible ROI for corporations

Today's business needs to be conducted away from the office. Workers are commuting longer distances, taking hours from their workdays. Distributed organizations and a global marketplace have expanded the need for business travel. At the same time, office space costs have skyrocketed. Eliminating office space for even a thousand teleworkers can potentially save millions of dollars a year.

Employers also gain increased productivity and organizational responsiveness resulting in faster completion times for important initiatives. Due to the significant technology investments made over the last decade, more industries are now realizing increased workforce efficiencies. Companies are gaining this productivity by using technology to enable current workers to do more work, by hiring temporary workers, and by outsourcing, instead of hiring more full-time employees. For distributed organizations, secure, available and cost-effective remote access is key to increased productivity.

Anytime, anywhere access is here to stay

Your employees, customers, suppliers and business partners expect anytime, anywhere access. Increasingly, a majority of employees work at locations other than the headquarters building or campus, typically at a regional facility sales office, retail store or a home office. In order to benefit from the increased productivity and cost-savings generated from a more mobile workforce, your organization needs a solution that can address the remote access needs of teleworkers, and handle the additional security risks they bring about.

Security Risks Posed by Teleworkers

Without proper security measures in place, anytime, anywhere access introduces a number of risks for organizations. For example, unsafe user behavior can leave sensitive corporate information behind on a public machine, easily accessible to curious outsiders. More serious risks can come from viruses that may be inadvertently transmitted from an infected end-user device to other computers on your corporate network. The biggest risk comes from sophisticated malicious hackers. They may launch a full-fledged attack against your organization in an attempt to hijack your computing resources and sabotage your operations and reputation.

Out-of-date or improper settings increase security risks

Without IT oversight, home computers, personal laptops and mobile devices are more likely to be improperly configured for file and printer sharing, potentially exposing sensitive information to roommates, spouses and children. Teleworkers may not be using the latest operating system or application software. They may not have installed the latest security updates or kept up with their anti-virus definitions. All-in-all, personal devices are more likely to get infected by viruses or malicious code than corporate devices. And infections are slower to be detected and cleaned up on personal devices. Teleworkers increase corporate risks by potentially infecting other corporate machines and by spreading infections to customers and business partners.

Malware poses risks to remote devices

Worms and viruses cause damage by slowing down infected systems and networks, corrupting files and applications, and stealing bandwidth. Frequently, worms and viruses spread by e-mailing themselves to everyone in a user's contact lists or by exploiting network connections. Worms often install a back door on the infected computer that can later be used by spammers for sending junk e-mail or to infect other unauthorized traffic on the network. Although most viruses are successfully controlled by corporate anti-virus software, they still pose significant risks to personal device users.

Trojan horses and zombies are malicious processes disguised as familiar objects, such as shareware programs, pictures or music files, so that even educated users feel safe launching them. Both Trojan horses and zombies may be dormant until a predefined event occurs and then are controlled by a remote hacker. For example, some Trojan horses let attackers control infected PCs remotely. Unless appropriate information security products are deployed, hackers can use this type of malicious software to access corporate resources through an unprotected VPN tunnel, unbeknown to the authorized user.

Wireless LANs are insecure by default

Additional risks come from the nature of home computing environments. Today, many home computers are connected to wireless home networks (based on IEEE 802.11 wireless LAN standard). Most wireless network equipment is shipping with Wired Equivalent Privacy (WEP) security features turned off (to simplify installation), and many non-technical people do not turn on even rudimentary encryption and authentication available with WEP. Since wireless networks extend outside of the physical property boundaries, anyone just outside of the building can eavesdrop on traffic going through the wireless network or access file shares. Furthermore, sophisticated hackers can easily defeat WEP by exploiting its widely publicized security flaws.

Broadband exacerbates vulnerability to hackers

With always-on broadband connections, hackers can take their time penetrating a remote device. Unless products like a personal firewall are properly deployed, port scans, and other hacking attempts and intrusions can go undetected for a long time. And hackers can exploit all open ports to steal resources or to damage unprotected connected systems.

In most cases, IT cannot control the end user's environment

A remote user's access device might be a home computer, a friend's laptop, a shared computer on another organization's network, a wireless PDA, a smartphone or a public kiosk. This remote user device tends to be the weakest point of security, due to non-technical users' inexperience and IT's lack of control over the configuration settings and software updates. It is subject to a number of potential risks, including improper system or networking settings, or lack of the latest operating system or security updates. The remote device may be subject to a virus or a worm infections, Trojan horses and zombies. SonicWALL Aventail's E-Class SSL VPN and Network Security Appliance strong, adaptable security that can help you defend against these risks.

SonicWALL Aventail E-Class SSL VPNs Reduce the Security Risks of Teleworking

You know that it's not realistic to give your teleworkers the benefits of an anywhere access solution without an underlying platform that makes it secure, scalable and manageable. SonicWALL Aventail's proven E-Class SSL VPN solutions give IT the control that makes this type of end user convenience possible.

SonicWALL Aventail's strong security protects corporate networks

SonicWALL Aventail's E-Class SSL VPN reverse proxy and granular access control technologies eliminate direct network connections, making your internal network topology invisible to outsiders. With no visibility onto your corporate network topology, remote hackers are unable to launch the denial of service and other malicious attacks against your mission-critical resources through the VPN tunnel.

SonicWALL Aventail E-Class SSL VPNs strong security reduces network risks including stolen bandwidth and launched spam, malicious attacks and infections on your corporate resources, and use of your corporate resources to attack others. Without proper precautions, these activities can all take place through the VPN tunnel while your authorized user is connected to your corporate network, unbeknown to your end user. If your mission-critical

systems are attacked, infected or hijacked, their response times may become unacceptably slow or they may become altogether unavailable. Your sensitive information stored on attacked or infected systems may become compromised or corrupted, requiring significant audit, cleanup and restore efforts and costs. Additionally, user confidence may suffer due to unmet service level agreements. If outsiders are impacted, risks and costs can become astronomically high, especially in cases of corporate liability and damaged brand equity.

For teleworkers in particular, the increasing availability of always-on broadband access and local area wireless networks gives hackers high-speed 24x7 opportunity to snoop and cause damage to the teleworker's PC. If successful in penetrating the teleworker's PC, hackers can try to use the compromised device and high-speed connection to go after your corporate network.

By adding SonicWALL Aventail's E-Class SSL VPN proven technology to your information security infrastructure, you can minimize your security risks. E-Class SSL VPN hardened appliances or managed services automatically perform the following functions at the edge of the network:

- **Detect** the security of an endpoint prior to teleworker authentication
- **Protect** resources with granular policy based on that user and endpoint
- **Connect** the teleworker effortlessly to only authorized resources

Benefits of SonicWALL E-Class SSL VPN

- **For the enterprise:** Increased employee and partner productivity
- **For the business user:** Transparency and ease of use, flexibility to work anytime and anywhere
- **For the IT staff:** Strong security, scalability, manageability and cost-effectiveness

SonicWALL Aventail E-Class SSL VPN Protects Your Resources with Maximum Security for Teleworkers

SonicWALL Aventail End Point Control™ (EPC™) is designed to help IT proactively control the security of the remote user's PC. With SonicWALL Aventail EPC, you get the precision you need to reduce risk. EPC provides the ability to enforce policy based on the level of trust that IT has for the user as well as his or her environment. EPC gives administrators the power to create highly granular access control rules that support today's broad range of access environments. SonicWALL Aventail's market-leading EPC increases security and flexibility using three essential components:

- **Device Interrogation:** SonicWALL Aventail End Point Control automatically interrogates the endpoint anytime a user accesses a SonicWALL Aventail E-Class SSL VPN. To ensure that the access point is free of malicious software, or malware, like keystroke loggers and Trojan horses before allowing access, the SonicWALL Aventail solution automatically launches an agent from one of our best-of-breed client integrity partners (like Symantec®). This happens prior to authentication so login can be stopped if any malware is discovered. And, unlike the security precautions of other VPN solution providers, only SonicWALL Aventail EPC incorporates full cross-platform support, operating system detection and client integrity checks for truly secure everywhere access.
- **Policy Zones:** With EPC, IT organizations can establish and define different Policy Zones to fit their needs. Common Policy Zones include zones for untrusted machines such as kiosks, semi-trusted machines such as home PCs, and trusted corporate assets like laptops. IT can then manage those zones with a simple set of parameters. Device Interrogation looks for certain applications or "watermarks" on the endpoint. For example, if a specified anti-virus product or a personal firewall is present, Device Interrogation may instantly classify the endpoint into one of the predetermined Policy Zones—such as

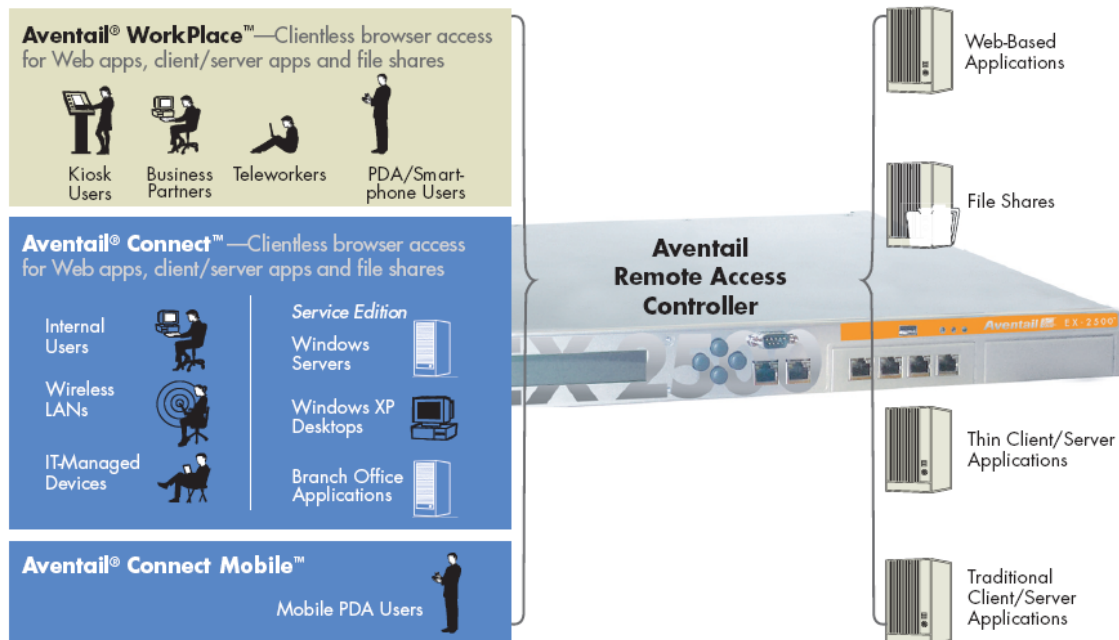
trusted, non-trusted or semi-trusted. Each zone enables a different level of access, appropriate to its level of risk.

- **Enhanced data protection and remediation:** Advanced EPC with Secure Desktop delivers the utmost data protection for unmanaged workstations—such as airport kiosks or Internet café PCs. Secure Desktop incorporates and integrates technology from Symantec to create best-of-breed security for your remote session—a “virtual” Windows® session that runs on top of the actual desktop. A mobile user can browse the Internet, check e-mail and work with personal files using client/server applications, but once the session is over, all sensitive data is automatically and thoroughly removed from the unmanaged workstation.

Advanced EPC also simplifies endpoint protection with a comprehensive checklist of anti-virus, personal firewall and anti-spyware products for Windows that even verifies versions and signature file updates.

The following table summarizes different teleworker risks and how SonicWALL Aventail can help control these risks	
Teleworker Risk	SonicWALL Aventail SSL VPN Solution
Outdated software or settings	SonicWALL Aventail End Point Control™ confirms the presence of anti-virus updates, device certificates and Windows registry entries. Optional SonicWALL Aventail Advanced EPC simplifies endpoint protection with a comprehensive checklist of anti-virus, personal firewall, and anti-spyware products for Windows that even verifies versions and signature file updates.
Malware, viruses, worms, Trojan horses, zombies	The SonicWALL Aventail solution automatically launches an agent from one of our best-of-breed client integrity partners. This happens prior to authentication so login can be stopped if any malware is discovered.
Hackers exploiting broadband and wireless insecurities	SonicWALL Aventail E-Class SSL VPNs provide cross-platform security, with personal firewall, operating system, and application detection, as well as other client-integrity safeguards.
Intruders masquerading as legitimate users	SonicWALL Aventail ensures that only authenticated users can gain access by checking privileges against an LDAP-enabled database, a RADIUS server, a Windows NT domain, a UNIX Username/Password database, or an RSA® SecurID ACE server.
Data left behind on unmanaged devices	SonicWALL Aventail Advanced EPC with Secure Desktop creates an encrypted virtual Windows session that is entirely removed from unmanaged devices such as kiosks after the session.
Lost or stolen devices	SonicWALL Aventail device watermarks

One secure gateway for all remote access control



SonicWALL Aventail E-Class SSL VPN is the only remote access controller that provides one solution with centralized management for all devices, applications and users, delivering manageability, security and productivity.

SonicWALL Aventail's strong emphasis on security alone would not provide teleworkers and other remote users with the access they need to do their jobs. That's why SonicWALL offers a full range of clientless access options plus the award-winning SonicWALL Aventail Connect Windows SSL VPN client, giving users convenient yet secure access from un-trusted, semi-trusted and trusted Internet-enabled devices. The SonicWALL Aventail E-Class SSL VPN is flexible enough to work well in any remote access situation, providing you with the best possible security for that environment. SonicWALL Aventail provides three flexible access options:

SonicWALL Aventail WorkPlace™ provides clientless browser access for Web applications, client/server applications and file shares.

- Complete and transparent Web application access including client/server applications and file shares
- Ideal for individuals accessing the network from machines that aren't managed by the IT organization, such as home PCs, public kiosks and PDAs
- Customized Web portal provides easy access to Web based applications from virtually any smartphone or mobile device
- Optimized portal for mobile devices, including personal bookmarks

- Symbian®, Windows Mobile® 5 and 4.x, Palm®, DoCoMo® and Blackberry® devices
- Only links relevant to mobile devices are displayed
- Session Persistence across IP address changes

SonicWALL Aventail Connect™ provides a Web-delivered client for secure access to the corporate network.

- Provides users with a transparent, easy-to-use, “in-office” experience
- Broad support for Web applications, client/server applications and file shares
- Unlimited mobility and complete integration with the Windows desktop
- Ideal for situations where users need full application access, and IT wants secure access support with strong desktop security, split-tunneling control and personal firewall detection
- SonicWALL Aventail Connect Service Edition for policy-driven application-to-application access, perfect for branch office applications that need dedicated or scheduled connections without human intervention

SonicWALL Aventail Connect Mobile™ delivers the “in-office” experience for mobile devices

- Provides support for Windows Mobile devices
- Deployed on demand from a portal
- Lightweight and easy to install
- Does not provide a direct connection to the network
- Proxied connection
- Granular access control ensures relevant content only to authorized users
- Session Persistence across IP address changes
- SonicWALL Aventail Connect Mobile is a certified application for Windows Mobile-based devices

In its E-Class SSL VPN offerings, SonicWALL Aventail combines the security and full Windows functionality you would expect from an IPSec VPN and delivers it with the convenience and cost-savings of a clientless SSL VPN. SonicWALL Aventail’s multiple access options enable secure, transparent access to virtually any application or corporate resource from any device.

Broadest application access from the most endpoints

SonicWALL Aventail E-Class SSL VPNs deliver transparent access to all network resources, including Web-based, client/server, server-based, host-based and back-connect applications such as VoIP, seamlessly across all platforms—Windows, Windows Mobile, Linux® or Macintosh®—from desktops, laptops, kiosks, PDAs, smartphones, as well as automated application-to-application remote access. This unparalleled ease of use significantly increases productivity, while reducing support costs associated with more cumbersome solutions.

From the user’s perspective, SonicWALL Aventail Smart Access™ does all the work. Smart Access dynamically determines and deploys the appropriate access method and security level based on the type and state of the device, user identity and resources needed. Adaptive addressing and routing dynamically adapts to networks, eliminating addressing and routing conflicts common with other solutions. And users can define their own shortcuts to frequently-used resources, personalizing their experience.

Easy to use anywhere, any time

SonicWALL Aventail Smart Access offers transparent, dynamic deployment of the appropriate access method based on user identity, endpoint security, and resource desired. With easy real-time access to information from everywhere, users get more done, whether they are in or out of the office. SonicWALL Aventail E-Class SSL VPNs offer:

- Intuitive, convenient access to all applications from everywhere: managed corporate laptops, or unmanaged home computers, Internet kiosks and mobile devices like PDAs and smartphones
- Support for Windows, Windows Mobile, Macintosh and Linux environments
- The most robust set of access options in the industry, including SonicWALL Aventail Connect and Connect Mobile for a full “in-office” experience and client/server application access from any endpoint
- User-friendly features including personal bookmarks and Session Persistence to enable IP address changes for mobile device users
- Bi-directional support for complex applications like voice over Internet protocol (VoIP)
- Optional integrated access to Citrix® farms and Windows Terminal Services applications, as well as to host-based applications

Manageability and Cost Effectiveness Enhance IT Productivity

With recent staff reductions and increased workloads, organizations need products that are easy for end users, and are easy for IT to manage and support. In fact, one of the reasons many organizations are adopting SSL VPNs is to reduce the cost and complexity they are experiencing with IPsec. Built for site-to-site VPN, IPsec technology has been unable to adapt to changes inherent with mobile workforces.

With IPsec, many end users are unable to access the information they need. Corporate help desk staff may spend hours on the phone with end users, trying out different client software and networking configurations to work around the access issues. Complex technology leads to dissatisfied end users, overburdened support staffs, decreased productivity and increased costs. With SSL VPNs, the reduced complexity and increased end user self-sufficiency quickly translates into improved user productivity and reduced workloads for IT.

SonicWALL Aventail’s E-Class SSL VPNs connect to the enterprise, traversing all network boundaries

SonicWALL Aventail E-Class SSL VPNs traverse firewalls, Network Address Translations (NAT) and proxy services, preventing configuration conflicts common with other remote access products. SonicWALL Aventail’s E-Class SSL VPN works trouble-free and consistently in virtually any environment, with no client or server changes.

SonicWALL Aventail’s E-Class SSL VPNs leverage broadband ubiquity

Residential broadband connections can be less than half the cost of business broadband connections, although the speed and service levels are the same. Occasional day extenders and teleworkers use their at-home broadband connection to do company business, especially while sick, on vacation or snowed-in. Since many organizations use IPsec for remote access, some service providers have blocked IPsec traffic over residential broadband connections, in an attempt to get home workers to upgrade to business-level pricing.

SonicWALL Aventail’s E-Class SSL VPN is an attractive alternative for these situations. SSL is a commonly used Internet protocol, and service providers cannot distinguish between SSL used by a person logging onto eBay® and SSL used to connect to the corporate network. Additionally, SonicWALL Aventail automatically

adapts to NAT, wireless switches and routers, and dynamically assigned IP addresses common with home networks.

SonicWALL Aventail advantages over proprietary solutions for mobile e-mail

Since SonicWALL Aventail E-Class SSL VPNs provide universal access to e-mail and other resources from multiple devices, there is no need to support mobile e-mail using a separate proprietary infrastructure, like Blackberry Enterprise Server (BES).

SonicWALL Aventail E-Class SSL VPNs enhance productivity and ROI because besides just reading e-mail, users can also open attached files, or follow links to other applications. SonicWALL Aventail E-Class SSL VPNs can deliver leading e-mail like Outlook®, without format translation, POP redirection or user retraining.

Using granular access control, SonicWALL Aventail can scan a Treo or BlackJack for OS patches, watermarks or other security applications; confirm a user's organizational identity; or redirect a user to a self-remediation link.

SonicWALL Aventail can lower costs by providing a single-appliance universal solution for laptops and other remote endpoints (not just PDAs and smartphones), while leveraging predefined directories and rules—without adding complex and expensive multi-server BES (or Exchange Mobile Messaging) infrastructure.

SonicWALL Aventail's flexible, object-based policy model simplifies management

You can easily manage any resource, application or network file share for all of your remote access policies and user organizations from a centralized location. SonicWALL Aventail approaches access control policy using the same security and management principles that underlie leading firewalls. This offers administrators a robust—yet familiar—model for handling their every-day organizational complexities.

Scalability to thousands of users and connections

As additional users start accessing your corporate network remotely, scalability of your infrastructure becomes a real issue. Add new high-bandwidth applications like voice over IP and document sharing, and scalability and reliability quickly percolate to the top of your list of concerns.

Your scalability risks are exacerbated if you have a large, distributed organization with highly mobile employees who may need to access different applications from different parts of the world. Lack of availability or slow access to corporate resources quickly translates into lost productivity for end users. Users get frustrated and complain. And their phone calls and trouble tickets increase the burden on your already overworked IT staff.

Multiple authentication realms provide added flexibility and scalability

SonicWALL Aventail E-Class SSL VPNs can support more than one authentication repository (e.g., Active Directory and RADIUS) as well as differing methods of authentication (e.g., username/password and tokens), providing more flexibility and scalability. This makes it easy to support a policy model spread across multiple directories or to support situations where differing authentication credentials are required.

High availability is key for predictable performance and service level agreements

SonicWALL Aventail's E-Class SSL VPN is a scalable, reliable solution can be easily added to your infrastructure with minimal configuration changes. It is the first SSL VPN to offer integrated active/active high availability that makes it easy for organizations to roll out and implement a reliable and scalable SSL VPN solution. The integrated load balancing with stateful failover means that you do not have to add a third-party load balancer. However, for distributed installations supporting hundreds of thousands of users, SonicWALL

Aventail also works with third-party load balancers to provide secure, fault-tolerant and scalable anywhere access.

Easy to deploy, manage and support

SonicWALL Aventail Unified Policy™ offers a centralized object-based policy model with a single rule set to easily manage and automatically cascade policy across all users, groups, resources and devices, and establish policy decisions based on the security of the endpoint. With SonicWALL Aventail E-Class SSL VPNs:

- All policy is easily managed through a single secure gateway using the SonicWALL Aventail Management Console
- Optional SonicWALL Aventail Advanced Reporting™, a robust hierarchical log analysis tool to audit all remote user access, lets you generate and customize reports
- Role-based administration allows workload distribution without allowing access to the entire E-Class SSL VPN appliance
- Intuitive, transparent user experience means fewer support calls. for lower IT overhead
- For most deployments, policy setup takes only minutes—up to three times faster than other VPNs—for more rapid deployment and faster return on investment
- Robust support for single sign-on (SSO) and Web forms-based authentication
- Dynamic grouping based on RADIUS, LDAP or Active Directory authentication repositories

SonicWALL Aventail E-Class SSL VPNs: the Best Choice for Remote Worker Productivity and Security

Technology, economics and competitive pressures are forcing organizations to enable workers to work more places more often. Users' own expectations for anywhere access reinforce this need. For economic and technical reasons, older IPsec-based technology is no longer adequate to support the nearly constant need for secure anywhere access.

Because they combine the IT need for advanced security with the end user's need for convenient, flexible access, SonicWALL Aventail E-Class SSL VPNs are today's best choice for remote worker productivity. Every day, hundreds of thousands of users and thousands of organizations depend on SonicWALL Aventail E-Class SSL VPN appliances and services. SonicWALL helps them to securely and cost-effectively access protected network resources from the broadest range of remote locations and devices of any SSL VPN vendor today. SonicWALL Aventail E-Class SSL VPNs offer easy, flexible access options to secured resources and reduce companies' information security risks. By extending secure remote access from more places and to more resources at a low total cost of ownership, SonicWALL Aventail increases productivity for teleworkers and all mobile and remote users.

To learn more about SonicWALL Aventail E-Class SSL VPN solutions, visit: <http://www.sonicwall.com>