SonicWALL Virtual Assist: Clientless Remote Support Over SSL VPN

Businesses can enhance user satisfaction, productivity, profitability and security by leveraging existing infrastructure to deliver secure remote support

CONTENTS

SONICWALL

Abstract

While advances in remote access technology have yielded business benefits in the form of a more flexible and productive workforce, it has left IT with less direct control over increasingly mission-critical remote laptops and desktop computers at worker's homes, remote offices and other sites. Traditional support methods for remote endpoint devices were tedious, costly, time consuming and potentially hazardous to system configuration and security. Emerging Web-based technologies such as thin clients and SSL VPN have paved the way for on-demand "clientless" remote support tools, delivered as software-only, hosted, or appliance-based solutions. This white paper evaluates the technical and business criteria for an effective clientless remote support implementation, and weighs the business benefits and competitive advantages of the SonicWALL® Virtual Assist solution.

Business Trends in Remote Access

Remote access technology is rapidly evolving. High-speed broadband connectivity is no longer limited to corporate headquarters, but also an expected standard at home and at other remote sites as well. The business "office" is no longer tied to a specific physical location: your office is where you are.

Optimally, this increased remote access can provide businesses with greater flexibility and productivity. Work can be conducted from home offices, field offices, partner sites and manufacturing sites. Companies are no longer restricted to local talent pools or salary markets, offering a potential competitive advantage. Third-party partners, vendors, and consultants are taking a more direct role in business operations, collaborating in cross-functional teams that require secure access to "inside" application resources from "outside" devices.

With the proliferation of remote access, however, IT has consequently lost its direct hands-on control over many of the access points, network environments and endpoint devices used in key business operations. The development of secure remote access technologies such as SSL VPN have enabled IT to provide secure on-demand connections between remote endpoint device users and corporate resources. Yet support technicians—whether they are employed with an in-house help desk, a third-party technical service provider, or a product call center—also require full and secure control over remote computers in order to install, configure and maintain mission-critical applications.

The evolution of remote support technology

In order for a technician to provide hands-on support for a remote computer, either the endpoint device must be shipped to a technical support center (incurring shipping costs and decreasing the productivity of the end-user by leaving them without their primary device for an extended period of time); or an IT technician must travel to the remote location (incurring travel and lodging costs, and decreasing the productivity of the technician while en route and offsite). Alternately, support software could be sent to the end-user in a mailed disk or CD, or when possible, as compressed format e-mail attachments. The end-user would then take on the role of technician by proxy, with the support technician walking them through procedures over a long-distance telephone call. These calls can be cumbersome, time-consuming, unpredictable and exceedingly frustrating for both parties.

Technicians have deployed peer-to-peer software solutions (e.g., pcAnywhere) to support hardened local area network devices for decades. However, since a technician needs hands-on access to the endpoint computer in order to install the peer-to-peer software prior to remote support sessions, these solutions are inherently ineffective for remote deployment. As a workaround, a technician might consider using an IPSec VPN client to connect to the endpoint computer in order to install the software; however, since the VPN client would have to be pre-installed as well, this workaround is also ineffective. Because the remote computer environments are also beyond direct IT control, deployment of these solutions on unmanaged remote devices can also often be plagued with configuration conflicts, network traversal failures and authorization issues. These solutions are also unsuitable in disaster recovery and business continuity

scenarios, such as after catastrophic disasters, when IT would need to support or repair core business computers at or from contingent locations that inhibit direct physical contact with the device.

To overcome these failings, technical support organizations now look to solutions that can provide secure remote support on-demand over the Web, without the need for pre-installed "thick" client software at the endpoint. Instead, these "clientless" solutions rely upon Web-based technologies such as Java-enabled "thin" clients and SSL VPNs to launch on-demand support sessions upon authorized login of the technician and end-user. As a result, industry analysts expect that the worldwide market for clientless remote support services tools is expected to grow to $274.3 million in 2011, at a compound annual growth rate of 19.6%.[1]

Assessing Clientless Remote Support Solutions

Various vendors offer hosted remote support services for ongoing monthly or annual fees. However, these pose the security concern of making internal support session activity visible to an external third-party, which could potentially expose organizations to malware threats, information leaks and regulatory noncompliance. Other remote support solutions are offered as licensed software. While this does address the security concerns of hosted solutions, these require IT to configure a dedicated device and install the application.

An appliance-based approach addresses the concerns of both hosted and software-only solutions, with the added benefit of allowing IT to control the solution behind their corporate firewalls. Certain appliance-based solutions offer clientless remote support only, without the capability to provide secure remote access.

Business criteria: satisfaction, productivity, profitability and security

Ideally, a clientless remote support solution should also promote the primary business criteria of support organizations, including the increase and enhancement of customer satisfaction, productivity, profitability and security.

- **Satisfaction:** To enhance customer satisfaction, an appropriate remote support solution must be deliverable anywhere on-demand via a Web browser, thereby freeing end-users from the burden of acting as a remote technical proxy, and speeding the resolution of their technical support issues. The solution must also be intuitively easy to use, and customizable to the end-user's needs, providing a familiar, user-friendly interface. For internal help desks, enhanced satisfaction promotes departmental objectives. For technical service providers and software manufacturers, it helps meet or exceed service level agreements and generates repeat and referral business.
- **Productivity:** To increase productivity, the solution must remove any need for manual pre-installation of software on the endpoint device, freeing both the end-user and the technician from that laborious task so that they may apply their skills and time on other mission-critical work that promotes business growth. It must also be easy for IT to deploy and manage, and easy for the support technician to learn and use.
- **Profitability:** By leveraging existing infrastructure, IT can increase profitability by optimizing its return on its investment in technology, as well as lowering total cost of ownership by eliminating redundancy. The solution should take full advantage of established secure remote access technology, such as SSL VPN, and seamlessly integrate existing security policy and domain authentication (e.g., LDAP, RADIUS, two-factor, etc.).
- **Security:** As with any Web-delivered solution, utmost attention must be given to providing uncompromising security. The solutions must enforce granular authentication for both technicians and end-users. The remote support session should be fully encrypted (e.g., 256-bit AES SSL encryption) in order to protect mission-critical resources and help businesses comply with internal and external regulations such as Sarbanes-Oxley, GLBA and HIPAA.

---

[1] IDC, "Worldwide and U.S. Clientless Remote Support Services Tools 2007-1011 Forecast and Analysis," March 2007

SonicWALL Virtual Assist: SSL VPN Secure Remote Support

SonicWALL® Virtual Assist™ is an optional licensable add-on to SonicWALL SSL-VPN 4000 and SSL-VPN 2000 secure remote access appliances, which allows a support technician to provide “clientless” on-demand support for a remote customer’s laptop or desktop via a Web browser.

Virtual Assist integrates seamlessly with the SonicWALL SSL VPN appliance behind any firewall, enabling IT to leverage existing network infrastructure without additional configuration or learning curve. Virtual Assist retains in-house control over session data while delivering a greater return on investment. The entire support session is secured via the SSL VPN appliance using 256-bit AES SSL encryption, assisting efforts to comply with internal and external regulations. Using SonicWALL’s intuitive SSL VPN administrative interface, IT administrators can easily license and configure the module for a variety of deployment configurations, including internal IT help desk, global call centers, or support from trusted third-party consultants. Seamless integration with existing LDAP, AD, NT Domain, RADIUS, RSA, Vasco or one-time password authentication infrastructure confirms technician identities and prevents unauthorized access to customers' systems. This also enables an administrator to granularly segment technicians into various groups, each with different access privileges.

Features and benefits

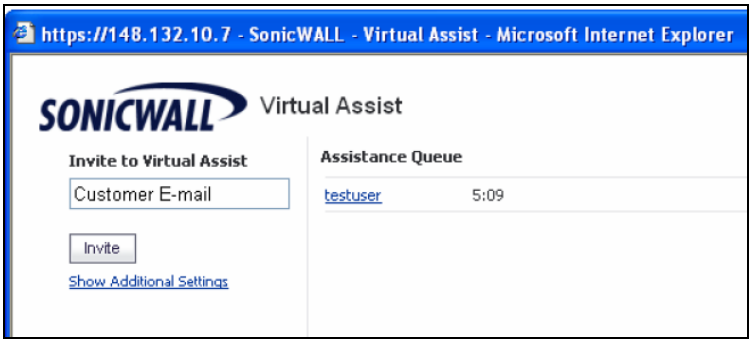
The robust remote support feature set of SonicWALL Virtual Assist can dramatically increase and enhance customer satisfaction, productivity, profitability and security.

Virtual Assist Features	**Business Benefits**
Enhanced Customer Satisfaction	
▪ On-demand “clientless” solution via the Web ▪ Easy for end-user customer	▪ Frees end-users from technical proxy role ▪ Speeds time to resolution ▪ Familiar look-and-feel ▪ Provides exceptional levels of service ▪ Promotes new and referral business
Increased Productivity	
▪ Easy to deploy ▪ Easy to manage ▪ Easy for support technician	▪ Increases management productivity ▪ Increases technician productivity ▪ Increases end-user productivity ▪ Improves and extends service levels ▪ Opens support resource bandwidth to promote business growth

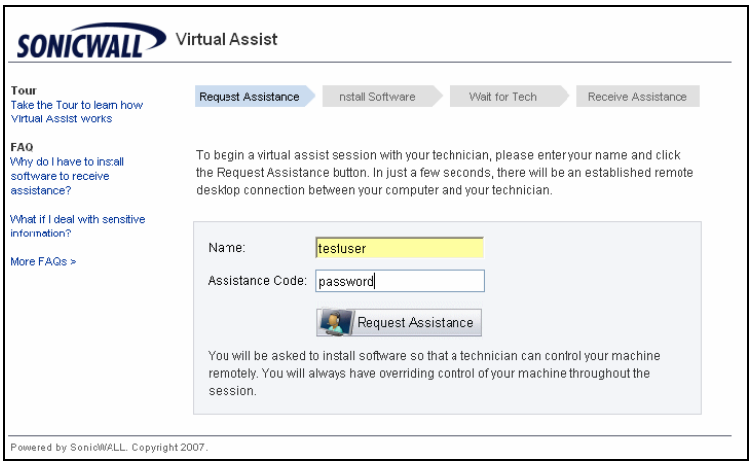
Greater Profitability	
▪ Integrated secure remote access infrastructure and capability ▪ Leverages existing security policy ▪ Seamless domain architecture integration ▪ Add-on appliance component ▪ One-time perpetual licensing	▪ Maximizes IT staff time and resources ▪ Centralizes remote administration ▪ Reduces learning curves ▪ Increases return on technology investment ▪ Lowers total cost of ownership ▪ No separate hosted service required ▪ Eliminates recurring service fees
Uncompromising Security	
▪ Secure SSL VPN authentication ▪ 256-bit AES SSL session encryption ▪ Granular policy control ▪ Securable behind firewall ▪ No session data disclosure to third-party hosted services	▪ Protects mission-critical data and applications ▪ Assists in compliance with industry and governmental regulations

How it works

1. *Technician authentication.* Virtual Assist delivers an easy-to-use SSL VPN Web portal through which technicians can manage, schedule, and maintain their support queue as well as invite end-users to support sessions via e-mail. Upon SSL VPN login, the technician is authenticated, and a thin client Java agent is pushed seamlessly to the technician's browser.

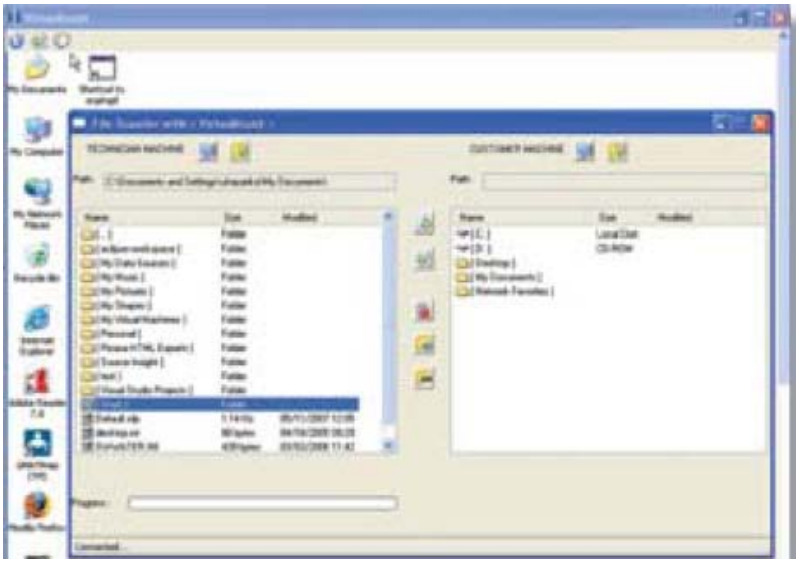


2. *End-user authentication.* Virtual Assist provides an easy-to-use Web portal to enhance the customer's experience. To start a Virtual Assist remote support session, the customer may either log on at a predefined support portal and request remote support directly, or accept an e-mail invitation from a technician. Subsequently, a thin client Java agent is pushed seamlessly to the customer's browser.



3. *Granting permission.* The technician can now see the end-user in the Virtual Assist queue, and requests access to computer. Once the customer grants permission, the technician can gain instant access to actively control the remote computer.

4. *Session-in-progress.* The customer can see what the technician does on the screen in real time, and may interact directly with the technician in during the support session using the robust Virtual Assist built-in live chat feature. Virtual Assist's file transfer capabilities also allow the customer to receive update or remediation files from IT in real-time.



5. *Session termination.* Either the technician or customer may end the session at any point in time with a single mouse-click.

Deployment scenarios

The SonicWALL Virtual Assist solution can be applied to a range of use-cases, including internal help desks, technical service providers, and product support call centers. Virtual Assist has been successfully deployed in retail, financial, academic and other business environments of all sizes.

Topping the world's number-one-selling SSL VPN product line for small- to mid-sized businesses, SonicWALL SSL-VPN 2000 and SonicWALL SSL-VPN 4000 appliances provide an ideal clientless remote support solution for mid-range organizations when deployed with Virtual Assist.

Scaling to large enterprise deployments, the SonicWALL SSL-VPN/Virtual Assist solution can be seamlessly integrated with a SonicWALL Aventail® E-Class SSL VPN appliance, globally extending the remote support capability over either SonicWALL Aventail Workplace portal or SonicWALL Aventail Connect Tunnel sessions. For a comprehensive integrated enterprise deployment, the entire solution may be placed behind a SonicWALL E-Class Network Security Appliance featuring ultra high-speed multi-core technology with unrestricted deep packet inspection, with all components managed centrally using the award-winning SonicWALL Global Management System.

"Virtual Assist makes setting up new franchises with POS and reporting systems a simple process. We've cut setup times in half."
- Ben Gray, IT Director
Palm Beach Tanning, Inc

Conclusion

Businesses have become significantly dependent upon remote endpoint devices that are no longer under direct hands-on control of corporate IT. Archaic support methods are not only costly and cumbersome, but are also potential security risks. IT must now implement clientless remote support tools that effectively promote the key business drivers of customer satisfaction, productivity, profitability and security. SonicWALL Virtual Assist offers the unique capability to deliver appliance-based SSL VPN remote support seamlessly integrated with existing network and authentication infrastructure. When deployed with SonicWALL SSL-VPN 2000 and 4000 appliances, SonicWALL Virtual Assist can be easily scaled to provide a secure on-demand remote support solution that meets the business needs of any size organization.