



Why Replace Your IPSec for Remote Access

David Piscitello and Lisa Phifer

To survive and thrive in an increasingly competitive world, forward-thinking organizations are encouraging workforce mobility and access agility—the ability for workers to transparently access any business application everywhere: at any time, from anywhere, using any device, over any network.

Several obstacles prevent organizations from providing access agility today. The first is the need to protect business applications and information from unauthorized disclosure and abuse, not only for the obvious business reasons but especially to comply in a confusing, evolving, and unforgiving regulatory environment (e.g., SOX, GLB, HIPAA). To satisfy these security needs, an organization must provide granular, resource-based access based on the level of trust it can establish for a given user, which may vary depending on access location and device.



The proliferation of devices and communications networks that workers use today to access business applications poses numerous obstacles. Access agility encompasses far more than a worker connecting to the corporate network from a company-owned laptop, using company-installed software, over a modem connection. Workers must access diverse business applications from the most convenient device available, at any time and place, using any network. It is no longer practical to deploy secure access solutions that rely on resident client software. Moreover, secure access solutions must perform well over networks that exhibit vastly different topologies, throughput, and latency.

A final obstacle is the need to protect the organization at large from a relentless stream of malicious attacks that may originate from devices used by workers to access business applications. Viruses, worms, blended threats, SPAM, and spyware are more prevalent today than ever before. Such attacks drain IT and network resources, threaten privacy and company reputation, and hamstring user productivity. Organizations must have solutions to block attacks from every possible point of entry, including remotely connected devices.

Traditional secure remote access solutions fall short of satisfying these requirements. In fact, secure, everywhere access business objectives cannot be met until we discard pre-existing paradigms, and invent and adopt solutions that achieve high degrees of end-user transparency and accessibility (access agility), granular policy control, and are, by design, able to adapt to and accommodate new device, OS, application, and access technologies.

In this white paper, we examine and compare traditional IPSec remote access, the advantage of SSL VPNs for remote access, and the evolution of today's smart SSL VPN solutions.



IPSec's limited, perimeter-based policy framework makes it a poor choice for a granular, location-sensitive VPN.

IPSec Remote Access: Too much and too hard...

IPsec is an effective solution for site-to-site Virtual Private Networking, but it is now abundantly clear that IPsec is a severely limited solution for remote access. Adopters of IPsec-based secure remote access must work within a world of inherent constraints, the sum of which all but eliminates IPsec as an "everywhere access" VPN solution.

IPsec deployment is fraught with addressing complexities. The widespread use of network address translation (NAT) and private addressing will forever limit IPsec deployment. VPN administrators cannot predict whether IPsec users will succeed in connecting to corporate networks because they simply cannot be certain where NAT is applied and what addresses are used in the remote network. Because the IPsec standards offer so little help, VPN administrators must also manage internal addressing: are addresses dynamically assigned, and from what pool? How are routing and security policies affected by such assignment? What if assignments change? Simply put, standard IPsec won't work everywhere.

IPsec authentication is limited. Standard IPsec provides mutual authentication of client and server using digital certificates and shared secret passwords. In practice, both authentication methods prove impractical. Shared secret passwords provide dangerously weak authentication and prove unmanageable in large, multi-organizational user deployments. The expense and complexities associated with issuing client certificates in IPsec deployment scenarios often lead organizations to consider token- or challenge response-based authentication, and standard IPsec supports these poorly. Proprietary and interim solutions exist, but are complicated and saddled with their own vulnerabilities.

IPsec authorization is not sufficiently granular. IPsec VPN selectors are insufficient to satisfy the authorization policies organizations desire or are obliged to define in today's regulated environments. To compensate, organizations must create complicated, user-, group-, or constituency-specific policies to limit user access. Often, organizations must coordinate policy across many security systems, including existing Internet firewalls. Complexity rarely improves security policy, thus IPsec's limited, perimeter-based policy framework makes it a poor choice for a granular, location-sensitive VPN.

IPsec requires resident client software. IPsec remote access requires VPN client software and policy configuration at the end point device. Deploying and troubleshooting client software, and distributing and maintaining security policies for large numbers of company-owned and managed end point devices is an expensive and formidable task for many single enterprises, and even more difficult in collaborative (multi-enterprise) environments. Simply put, IPsec doesn't scale well. Users cannot adopt new mobile devices until IPsec client software is available for those platforms, and they cannot use any non-managed device for secure remote application access. Because IPsec requires IT-installed client software, it simply cannot deliver cost-effective secure remote access to all users, from all devices.

IPsec perpetuates an obsolete security model. IPsec creates an IP- or network- level tunnel (connection) between a client computer and a VPN security gateway. This means that every remote user is directly connected to part of—or the entire—trusted network of an organization at that network's perimeter. When a client connects using IPsec, every resource inside this protected network is potentially available to the user, and therefore vulnerable to misuse and attack from that client during the entire connection. IPsec security associations often create a potential attack vector to every service on every host.

*SonicWALL
Aventail's
innovative
Smart
Tunneling
technology
provides
complete
and
controlled
network
access ...
without the
onerous
burden that
IPsec
imposes.*

After years of struggling with these limitations, many organizations have come to reconsider whether their requirements for remote and extranet access are really best served by IPsec VPNs.

Today's SSL VPNs: Closer to the mark ...

The current generation of SSL VPN products has proven superior to IPsec in a number of secure access scenarios:

SSL VPN deployment is simpler than IPsec. Today's SSL VPNs eliminate IP address management issues, avoid resident client software installation, and eliminate policy configuration at client devices, and thus reduce the total cost of ownership over IPsec. However, this increased flexibility heightens the need for robust end point security.

SSL VPNs support more granular policies than IPsec. Today's SSL VPNs employ Web portal and application proxy architectures. The portal or application proxy serves as a single entry point to a network, where authentication methods can be selectively applied to different user groups. Since portals and proxies by definition examine complete application data, policies can be applied to individual data objects to narrow authenticated user access to a specific set of servers, applications, and data objects. However, client-initiated application access is not always desirable or efficient.

SSL VPNs enable application access. Ultimately, the goal of a VPN is not to provide remote devices connections to networks, but to provide users with secure access to applications. Application layer gateways do not allow direct network connections. No network traffic passes through the gateway, and the gateway itself is hardened against network and transport level attacks. However, some applications do not proxy well, and so breadth of application support varies widely.

In short, SSL VPNs have proven highly desirable, but incomplete. Many companies have thus been forced to continue using IPsec for certain users and applications, despite IPsec's drawbacks.

The End Game for SSL VPNs

The end game marks the point during chess play when a player has moved all his pieces in position to check or stalemate his opponent. All that remains is to execute the final move. **SonicWALL Aventail E-Class SSL VPN appliances** successfully execute the following moves to meet today's secure application access requirements, and complete the end game:

SonicWALL Aventail SSL VPNs expand application support. For many applications, native application support is preferred over an alternative "Web portal" style of user interface. Outlook Web Access is a case in point. When users insist on native user interfaces for popular applications like Outlook, secure access solutions must accommodate them. Other applications, especially latency- and jitter-sensitive applications like IP telephony (IPT, VOIP) may not operate efficiently when proxied. Some applications, especially back connections from network to user, may not work at all over other VPNs. For such applications, SonicWALL's innovative Smart Tunneling technology provides complete and controlled network access where it is still necessary and desirable, but without the onerous burden that IPsec imposes.

SonicWALL Aventail SSL VPNs are easier to deploy. While today's SSL VPN solutions avoid client-side policy configuration, policy definition at the application gateway quickly becomes overly complex as the number of access methods, access locations, authentication methods, and authorization requirements grows. SonicWALL Aventail Unified Policies provide VPN administrators with a single access control model that can be applied easily and uniformly to all use cases.

SonicWALL Aventail SSL VPNs close end point security loopholes. SSL VPNs deliver access agility partly by accommodating user access from unmanaged hosts. Today, SSL VPNs often take measures to eliminate traces of secure access at client devices. To provide location, device, and network agnostic access without compromising security, SonicWALL Aventail End Point Control (EPC) provides robust end point security, including the ability to inspect all devices to determine whether they pose threats to the organization's network before admitting them, and authorizing the right level of access based on those results.

SonicWALL Aventail SSL VPNs accommodate everywhere VPN. Secure remote access and wireless access lead many organizations to conclude that the traditional notion of a secure perimeter, enforced by Internet-facing firewalls, is obsolete. Increasingly, organizations are collapsing security perimeters, moving firewalls close to servers and digital assets, and making them increasingly responsive to application-level threats. For users who need to access applications, however, the existence and disposition of a secure perimeter is irrelevant. With SonicWALL Aventail SSL VPN, users can connect from any network, using any device that satisfies end point checks. Resource-based policies can authorize access to applications anywhere inside the network, without exposing the corporation to greater risk than absolutely necessary.

SonicWALL Aventail E-Class SSL VPN: The legitimate successor to IPsec

SonicWALL Aventail is more than an enhanced SSL VPN solution—it's a next-generation secure access solution. By adding three critical elements that are missing from many other SSL VPN solutions—**Smart Access**, **Smart Tunneling**, and **Unified Policy**—SonicWALL Aventail has firmly positioned its E-Class SSL VPN appliances as the most viable choice for securing access, irrespective of application, location, device, and access network.

Until **SonicWALL Aventail Smart Access**, organizations had no alternative but to either offer secure-but-limited access through an SSL-based portal, or to expose a full network using IPsec connections. Far too many organizations had to implement both. Smart Access evaluates the user's end point environment and transparently selects the best access method to offer users an efficient and secure user experience, while exposing the organization's networked resources to the least risk of outside attack. Smart Access delivers a complete range of methods, from basic Web portal access to proxy-based client/server access or full network access.

SonicWALL Aventail's patent pending **Smart Tunneling** is a revolutionary approach to delivering full network access. Smart Tunneling supports all bi-directional IP-based protocols, including non-TCP/UDP IP protocols and unicast and multicast UDP. It supports streaming and conferencing applications, service discovery, IP telephony, X-Windows, and remote management and control protocols that prove challenging for IPsec

*SonicWALL
Aventail is
more than an
enhanced
SSL VPN
solution—it's
a next-
generation
secure
access
solution.*

and competitive SSL VPN solutions. Other alternatives continue to struggle with addressing, routing, and policy complexity. Smart Tunneling solves these problems today by automatically sensing and adapting to the user's environment, providing application reach that no other secure access solution can match.

Ultimately, all VPN administrators want advanced *policy management* capabilities that can reduce complexity, increase control over resources, and provide every user with access to any application he needs, whenever the need arises, from wherever he may be. Policies that are based on network address or access method do not scale well, and lead to mistakes and overexposure. With SonicWALL Aventail's **Unified Policy**, administrators can create a single policy for each group or user, to manage across every method of access and type of resource, with access control based on the level of trust for the user and the security status of the end point being used for each session.

Smart Tunneling: Innovative enabling technology for secure access

Smart Tunneling provides complete *and controlled* network access. It solves the most glaring problems that encumber IPsec remote access deployment today: NAT, internal address assignment, and routing in a simple yet elegant manner.

NAT. NAT is the bane of IPsec deployment. VPN administrators cannot control where network address translation might be applied in the global Internet. Users located behind NAT are often unable to connect or stay connected with IPsec protocols like ESP. By protecting IP traffic between a remote end point and a security gateway using SSL instead of IPsec's ESP, Smart Tunneling removes the unavoidable issue of NAT interference entirely from the picture. In Secure NAT mode, SonicWALL Aventail Smart Tunneling allows all users within a selected community to share a single IP address.

1 Access point initiates Connect Tunnel #1a (at startup or by launching an application) or OnDemand Tunnel #1b (through the WorkPlace portal).

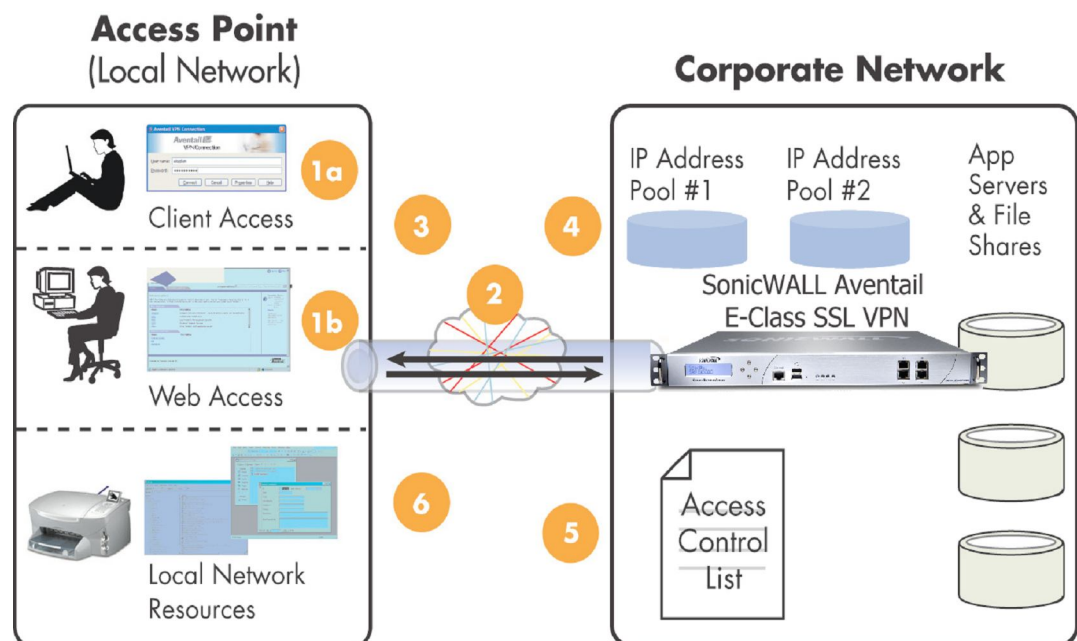
2 Smart Tunneling creates tunnel with SSL VPN.

3 Access point provides Smart Tunneling with local network IP address information.

4 Smart Tunneling examines local network IP address information for potential address and proxy traversal conflicts, and provides appropriate client virtual IP address.

5 Smart Tunneling examines the Unified Policy access control list and provides the access point with routing information based on what resources the user is allowed to access. Routes are only used for specific resources, minimizing routing conflicts.

6 Applications on the client device initiate flows with network resources. Conversely, applications on the client device accept flows from resources. Policy is enforced on the flow bi-directionally.



Address assignment. IPsec VPN administrators must manage the IP addresses that remote end points will use when communicating with resources inside internal networks. IPsec VPN administrators are often forced to configure these *virtual IP* addresses statically. Even when virtual IPs are supplied at connect time, IPsec cannot take into consideration the client's local addressing environment. This introduces the possibility that virtual IP addresses will conflict with addresses assigned to other (local to the client) systems. This creates situations where users are prevented from accessing local resources, or worse, where users cannot complete business tasks with the VPN tunnel connected.

Smart Tunneling avoids this problem by querying end points for local address information—the local network adapter address, local IP gateway address, local DHCP server and HTTP proxy server—before it configures virtual IP address information for that end point, so that it can avoid these kinds of address conflicts. Smart Tunneling's Web-delivered agent makes any end point device behave as if it were connected to a protected (internal) network, transparently, without the need for user intervention or end point re-configuration. Administrators can also specify Post Connection Scripting to automatically run executables on Windows systems after a connection is established.

Routing. IPsec VPN administrators typically define internal network routes manually, which presents several problems. One problem is inherited from static VIP assignment—routes on the user's local network may conflict with routes defined elsewhere within the corporate network. Another problem is that network level routes do not provide adequate granularity. When a VPN administrator creates a network level route to permit remote user access to a Web server, he can at most configure a policy to restrict the user to a specific destination IP address (e.g., 192.168.1.15) and port (e.g., HTTP/80). Any additional access controls on application data objects must be implemented within the corporate network, on departmental firewalls, security systems, or individual servers.

Smart Tunneling dynamically generates routes to authorized resources based on per-user, object-level policies. Every Smart Tunneling agent begins with the equivalent of a DENY ALL traffic policy. Routes are dynamically activated and access permitted only when the user is trying to access that specific resource. Thus, for a given user, a route to www.example.com at 192.168.1.15:80 may not be present if the user requests the general resource <http://www.example.com>, but only if the user requests <http://www.example.com/resource.html>, and only for the duration of that transaction.

Redirection. When organizations migrate from IPsec to SSL VPNs, administrators may want to institute familiar policies, like the ability to tunnel all traffic or let end points send selected traffic outside the VPN. SonicWALL Aventail SSL VPNs can also support these kinds of IP-based redirection policies. Redirect All mode sends all traffic through a Smart Tunnel to a designated proxy server. Split Tunneling mode sends traffic for designated resources (and only those resources) through a Smart Tunnel. Redirect Non-Local mode automatically differentiates between the end point's local LAN and all other destinations, letting users bypass the Smart Tunnel to reach nearby printers and shares. Smart Tunneling agents can also be directed to fall back to a secondary SSL VPN appliance if the primary is unavailable. Finally, VPN administrators accustomed to launching IPsec post-connect scripts (e.g., for laptop maintenance) can also do so with Smart Tunnels.

In summary, Smart Tunneling is unique, innovative, and forward looking. Smart Tunneling provides complete application and protocol access with greater focus on performance and throughput and dynamic as-needed activation than existing secure remote access solutions.

Smart Tunneling is unique, innovative, and forward looking.

Smart Access: Meeting diverse user needs, securely

Smart Access provides two methods of secure access delivery (as shown in Table 1.), **Aventail® WorkPlace™** and **Aventail® Connect™**, to help VPN administrators enable the optimal access method(s) for the type of application a user intends to access, when using either managed or non-managed end point devices.

Smart Access Method	Aventail WorkPlace	Aventail Connect
Web App Access	Transparent or translated from any Web browser	Transparent or translated from any Web browser
Full Network Access	OnDemand Tunnel The Smart Tunnel agent is downloaded from portal and installed on first use	ConnectTunnel The Smart Tunnel agent can be permanently installed on managed devices or configured to run as a service.

Administrators can use **WorkPlace** portals to provide users with easy access to Web applications, client/server applications, and portal-based resources (e.g., shares) from any public (kiosk) or teleworker PC through a standard Web browser. Administrators can create multiple WorkPlace sites, each configured with its own unique Fully Qualified Domain Name (FQDN). No temporary agent or resident client software is required in these cases, and full network access is effectively blocked from these at-risk devices.

Teleworkers and day extenders who need full network access from self-administered end point devices can use **OnDemand Tunnel**—a lightweight, Web-delivered agent that provides native network file sharing, local printing, personal bookmarks, and split-tunneling control. This alternative is ideal for users with administrative rights (first use only) to an end point they use on a regular basis.

To deliver full network access to managed end points, administrators can allow **Connect Tunnel** agents. Connect Tunnel is small footprint, easy-to-activate agent that delivers bi-directional access to all TCP/IP applications from Windows 2000/2003, Windows XP, Windows Vista (32 and 64 bit), Macintosh, and Linux OS end point devices. Connect Tunnel can be activated through user self-service Web provisioning or standard installer packaging, and can automatically update itself whenever a new version is available. On Windows end points, Connect Tunnel may even be installed to run as a service.

Finally, **Aventail® Connect Mobile™** provides Windows Mobile users with the “in office” SonicWALL Aventail SSL VPN experience. Connect Mobile supports Windows Mobile version 4.2 and higher, including 2003 Pocket PC Phone Edition, Windows Mobile 5 Pocket PC and Smartphone, and Windows Mobile 6. Session Persistence lets Windows Mobile users roam between office, commute, and home without re-authentication. And Device Watermarks make it easy to instantly deny access from lost or stolen devices.

The bottom line: SonicWALL Aventail’s Smart Access portfolio gives administrators unprecedented control and flexibility: Web-based or full-network access can be granted to any user, from appropriate managed end point devices, controlled by a single set of Unified Policies. No other remote access alternative satisfies as many usage scenarios as a SonicWALL Aventail E-Class SSL VPN, or offers as complete and automated activation of the most optimal access method.

No other remote access alternative satisfies as many usage scenarios as SonicWALL Aventail E-Class SSL VPN.

SonicWALL Aventail Unified Policy and End Point Control

To reduce administrative complexity and cost, organizations commonly implement unacceptably open remote access security policies. Open access means that a remote user is granted access to any resource once he is authenticated, irrespective of location, access method, and device.

This is a common practice among IPsec remote access deployments. IPsec's access controls were designed to secure IP traffic between trusted networks when packets traversed untrusted networks. The same policy mechanisms are inadequate for implementing user access to individual file shares and hyperlinks, or to block specific commands and actions within individual applications like FTP. When IPsec VPN administrators attempt to define strict access controls for remote access, the number of policies quickly grows unmanageable but still doesn't provide the granularity of control needed. VPN administrators have little alternative but to fall back on the trustworthiness implied from user authentication, and allow users to see everything on the network. SSL VPN administrators have more granular controls at their disposal, but when faced with a myriad of access networks, end point devices, and use cases, they too may define simpler/broader policies than business needs and security regulations dictate.

Today, a variety of risk and liability factors—user mobility, dissolving security perimeters, regulatory compliance, competition, unprecedented levels of digital fraud, network abuse, and computer attacks—put extraordinary pressure on organizations to revise policy thinking towards a stricter authorization model. Organizations must impose a higher burden of proof before access to any resource is permitted. Instead of implying trust from authentication, organizations now seek to ask, “Is this user authorized to access this resource, at this time, from this location, and using this device?” Two important benefits emerge from this resource-based access control model:

- Closed access becomes the default security posture. Access is permitted on an as needed basis, and only when authentication and authorization criteria are met.
- The resource (asset) becomes the basis for a unified policy definition. Different levels of access can be defined for data objects, based on trust for a user, the risk presented by a given end point device, as well as access method, location, and end point security status.

*SonicWALL
Aventail End
Point Control
ensures that
only end
points that
meet
stringent
security
criteria are
admitted to
networks.*

SonicWALL Aventail Unified Policy provides a single, integrated policy framework to manage anywhere access to any type of resource, with access controls based on the user trust, end point device, and location. With Unified Policy, VPN administrators define a single policy (rule set) that automatically controls the resources a user may access, the actions he may perform on those resources, and the zones from which each resource/action is permitted. Once a policy is defined, a user may attempt to connect through their portal from anywhere, using any device. Smart Access interrogates the end point device; identifies (authenticates) the user; and, based on the risk level resulting from these interrogations, automatically selects the appropriate access method—e.g., Web access or full network connection—and, where appropriate, transparently uploads and installs a Connect Tunnel agent to the end point device.

Once the user and device are permitted access through the portal, the user's actions are constrained within the resource-based access controls defined for this access instance or Zone: permitted actions on this resource, by this user, given the current level of security of this end point device. For example, Deny Zones can ensure unauthorized access is denied, and Quarantine Zones can redirect users for remediation. This level of access control granularity is unique among today's VPN solutions.

Furthermore, **SonicWALL Aventail End Point Control (EPC)** ensures that only end points that meet stringent security criteria are admitted to networks. End Point Control is a multi-dimensional approach to trust assertion on users and devices, including:

Client Integrity Protection – EPC integrity scans assure that the end point device is free of malicious threats before a user enters authentication credentials.

Device interrogation – EPC allows VPN administrators to evaluate end point devices based on a profile of security measures, applications, and configuration settings that must be present.

Policy Zone Definition – A VPN administrator can define degrees of device interrogation and provide a user with a different level of access based on the admission criteria an end point device can satisfy.

Data Protection – Available across Windows, Linux, Macintosh, and leading mobile platform operating systems, and the most popular browser software in use today, EPC offers a comprehensive set of browser and desktop measures to ensure that no sensitive data is left behind when a secure access session is terminated.

With the exceptionally flexible EPC framework of Smart Access, VPN administrators create multiple Zones to keep users connected and optimally productive. When end point devices cannot satisfy all the criteria of a device interrogation, administrators can place devices in quarantine until security shortcomings are remedied, or they can grant users access with reduced permissions. Moreover, administrators do not need to specify multiple independent policies to cover each use case—a single unified policy can be defined for each group or user, incorporating a Zone as another policy element.

Conclusion

SonicWALL Aventail E-Class SSL VPN appliances are the only SSL VPN platforms that provide single unified solution for everywhere access across all access methods, access environments, and resources. From a VPN administrator's perspective, SonicWALL Aventail satisfies the most pressing requirements for secure, everywhere access. SonicWALL Aventail SSL VPNs detect potential threats in end points, protect resources based on unified policies, and connect authorized users across a wide range of devices.

Smart Access provides a complete secure access solution for Web application access, client-server applications, and full network access as dictated by business need. SonicWALL Aventail automatically selects the optimal access method, transparent to the user. Users get everywhere VPN access without requiring client software installation, network-specific configuration, or access-method dependent policies.

SonicWALL Aventail Unified Policies makes it easy to define granular user admission and end point device policies in a consistent fashion. SonicWALL Aventail can screen and control end point devices used for secure access and automatically activate the appropriate access method based on the level of risk presented by the end point, without exposing more resources inside corporate networks than absolutely necessary.

SonicWALL Aventail E-Class SSL VPN appliances have the end game in hand.

*SonicWALL
Aventail
E-Class
SSL VPNs
have the
end game
in hand.*

About the authors: David Piscitello and Lisa Phifer own Core Competence, Inc., a consulting firm specializing in emergent network and security technologies. For over 15 years, the company has offered a wide variety of services, ranging from requirements development and competitive analysis to product testing and vulnerability assessment. Core Competence has delivered network security advice and consultation to hundreds of clients, small and large, including market-leading network equipment manufacturers, broadband providers, and Fortune 100 companies. David and Lisa both have extensive experience with secure remote access and have taught many deep-dive VPN workshops at large enterprises and industry conferences like Interop and InfoSec World.

© 2009 Core Competence, Inc. All rights reserved. SonicWALL Aventail, Aventail Workplace, Aventail Connect, Aventail Connect Mobile, and their respective logos are trademarks, registered trademarks, or service marks of SonicWALL, Inc. Other products and company names mentioned are the trademarks of their respective owners.