

A series of thin, light gray wavy lines that curve across the upper portion of the page, creating a sense of motion and depth.

Quick Guide: SSL VPN Technical Primer

This primer explains the basics of SSL VPN technology and includes distinguishing factors between Internet Protocol Security (IPSec) and SSL VPN technologies.



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Today's increasingly mobile and dynamic enterprise can now take advantage of ubiquitous broadband service, expanding wireless access and a proliferation of Internet-enabled devices. Mobile users expect access from anywhere—whether they're at home, in a hotel room, working from behind another company's firewall, at the neighborhood coffee shop or at an airport kiosk .

What's Driving the Need for Secure Remote Access?

To maintain the level of productivity that today's global businesses demands, more users are accessing more applications remotely than ever before. They are doing so from a broad range of devices and environments, including many that IT departments cannot control, such as personal mobile devices, home PCs and wireless hotspots.

With limited resources, IT must accomplish all of the following:

- Provide remote access to multiple complex applications
- Reduce risks from an increasing number of unmanaged access points
- Lower administration and support costs

A growing number of organizations are turning to Secure Sockets Layer (SSL) VPN technology for its flexibility, ease-of-administration and proven security. SSL VPNs are designed specifically to enable increased productivity for remote users by providing easy-to-use, secure remote access to applications and resources on a network while minimizing many associated risks and significantly lowering administration and support costs.

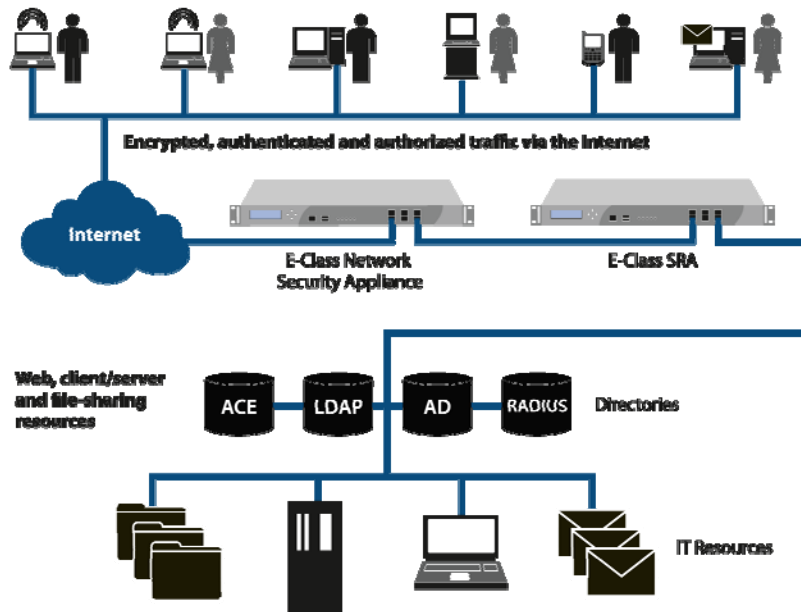
How to Use this Primer

This primer explains the basics of SSL VPN technology and includes distinguishing factors between Internet Protocol Security (IPSec) and SSL VPN technologies. You'll learn why these two technologies, based on fundamentally different designs and methodologies, each best serve specific use cases.

The format of this primer is designed to help you quickly find the necessary answers to many common questions about SSL VPNs and to understand the many advantages of SSL VPNs for everywhere remote access. Armed with facts about the capabilities of existing offerings, you'll be well-prepared to make decisions regarding the remote access technology that best meets your company's specific needs.

What is an SSL VPN?

Secure Sockets Layer (SSL) is the standard protocol for managing the security of message transmission on the Internet. An SSL VPN uses the SSL protocol to protect all traffic using encryption and authentication to keep communications private between two devices, which are typically a Web server and a user's computer. SSL was originally designed to secure the HTTP protocol for Web-based communications at the application layer. In the most simplified form, an SSL VPN is a reverse proxy that uses SSL for encryption and a sophisticated access control engine.



An SSL VPN solution provides secure remote access to specific corporate resources.

How Does an SSL VPN Work?

An SSL VPN uses SSL to provide end-users with authorized and secure access for Web, client/server and file share resources. SSL VPNs deliver user-level authentication, ensuring that only authorized users have access to each specific resource allowed by the company's security policy.

SSL VPNs start with providing access via a Web browser, removing the time consuming need for IT to provision clients to each endpoint device. For advanced access, agents may be required but SSL VPNs allow IT to have agents provisioned and activated within the context of the Web browser. Typically, agents are Active X or Java-based thin clients which are transparently pushed through the browser.

Access can be proxied, so there is never a direct connection to the network. The entire data stream is encrypted using SSL. This access occurs at the application layer, not the network layer, enabling finely grained access control.

How do SSL VPNs Compare with IPSec VPNs?

Compared to an IPSec VPN, an SSL VPN offers:

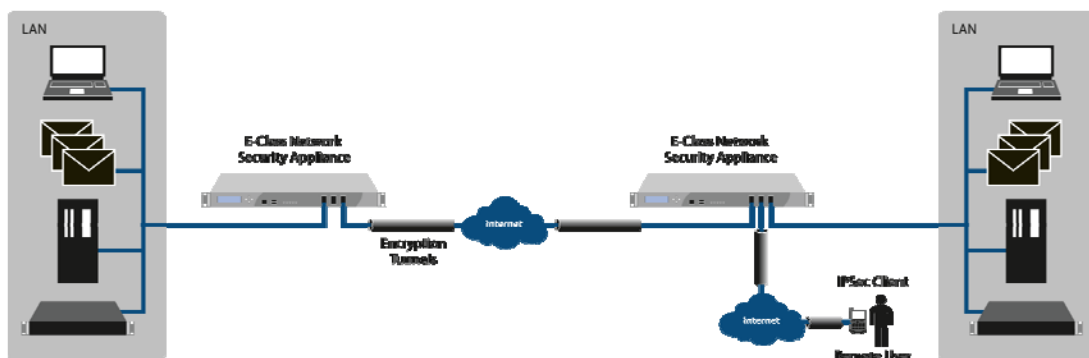
- Increased security specifically suited to remote access—by providing granular access controls and end-point control
- Increased productivity, because it works for a greater number of wired and wireless use cases—including home PCs, kiosks, PDAs, smartphones and other unmanaged devices.

- Lower costs, because it is “clientless” or uses lightweight Web-delivered clients rather than the more difficult-to-manage IPSec “fat” clients which need to be pre-installed on the remote machine, reducing management and support calls.

What is an IPSec VPN?

Internet Protocol Security (IPSec) VPN technology is predicated on the existence of a trusted relationship between networks or between users and a network and defines how to provide data integrity, authenticity and confidentiality across a public network such as the Internet. It accomplishes these goals through tunneling, encryption and authentication, but allows enterprises to select the specific security policy appropriate for their business. This suite of protocols provides security for IP traffic at the network layer.

IPSec VPN technology was originally developed to protect data communication between private, trusted networks over the Internet. IPSec solutions were later extended to protect data communication between mobile workers gaining remote access to an enterprise’s internal network in a more efficient manner than legacy dial-in methods. With an IPSec VPN, an IT department installs and maintains individual VPN clients on each PC from which a user needs access. An IPSec VPN may also require changes to the desktop. These factors result in higher management and support costs.



A typical IPSec VPN provides site-to-site remote access to the network via encryption tunnels.

How do the Two Underlying VPN Technologies Compare?

When applied appropriately, both IPSec and SSL VPNs use authentication and encryption standards that secure enterprise communications over the Internet. However, inherent design differences exist between IPSec and SSL VPN protocols. Again, IPSec VPN technology was designed only to establish a connection and protect private data streams between trusted networks. SSL VPN technology, on the other hand, was designed to protect data streams between associated sources, all of which are untrusted, regardless of whether they are users or a network, thereby qualifying access to applications. Understanding this key concept is fundamental to selecting and implementing the appropriate VPN solution for your business needs.

IPSec is network-layer centric, while SSL is application-layer centric. That means an SSL VPN can easily provide secure, granular access controls, ensuring that users gain access only to the designated resources

or applications specific to their needs and according to security policy. Using an IPsec VPN, it is difficult to create such precise control rules, so most organizations end up providing open access to their whole network.

IPsec was designed to tie together separate trusted networks in different locations. Because SSL VPN was designed for mobility, it delivers clientless anywhere access to the network from multiple locations and from the widest variety of devices possible through any Internet browser.

IPsec operates using pre-installed client software running on the user's machine. Because SSL is part of any Web browser, SSL VPNs provide clientless access that significantly increases the number of points from which employees, partners and customers can access network data. Clientless access also simplifies the connection process for the user, as well as the configuration and management for the IT administrator. Some SSL VPNs can also provide client-installed access, providing an ideal solution for corporate-issued laptops with full access control and minimal access complexity.

Not all IPsec VPN solutions provide secure access through network address translation (NAT) and firewalls; and those that do may require additional administrative support. Because SSL VPNs were designed specifically for remote access, they seamlessly traverse NAT, firewalls and proxy servers.

How do the Two VPNs Compare Regarding Security?

IPsec and SSL VPNs both provide flexibility in allowing enterprises to define the level of security that best meets their needs. But based on its architecture, the SSL protocol is best suited for securing application-based remote access. SonicWALL Aventail E-Class SSL VPN technology provides employees, business partners and customers with secure everywhere access—including clientless access to Web applications, client/server applications and file shares, as well as back-connect applications such as those using Voice over Internet Protocol (VoIP).

IPsec VPNs use tunneling and encryption to secure the data transfer over the Internet between a private network and a trusted computer. Therefore, IPsec assumes that the endpoint is secure and authorizes users unless otherwise restricted. However, IPsec alone might not prevent a user from entering with a virus or keystroke logger. To help overcome the security limitations of IPsec, the recommended approach is to ensure the communication is secured by a network security

IPsec VPN is ideal for site-to-site connectivity such as between a corporate headquarters and a branch office. IPsec can be more complex when used to connect home networks, consultants or business partners, since the different networks demand changes in configuration each time they are accessed.

Furthermore, IPsec's network-based connection model does not apply to determining application-layer access. IPsec solutions are not designed to provide granular access control due to their lack of application-layer support.

IPsec configuration choices include:

- Tunneling—Authentication Header (AH) or Encapsulating Security Payload (ESP)
- Encryption—56-bit DES; 112- or 168-bit 3DES; 128-, 192- or 256-bit AES; or none
- Authentication—username/password (such as Active Directory or RADIUS); user name and token pin (such as RSA SecurID); Internet key exchange (IKE); or X.509 digital certificates (such as Entrust and VeriSign) and IAM (such as eTrust SiteMinder and ClearTrust).

SSL VPNs use proxies, tunneling and encryption combined with access control to secure communications between users, the devices they use and the resources they access. With SSL VPNs, end-user access to any given resource is restricted unless authorized, a vastly different approach from that of IPsec VPNs. As a result, SSL VPN technology provides the granular access control that requires all users, regardless of location, to be granted explicit permission to access specific network resources. With SSL VPN technology, access control to applications and networks can be as general or specific as required. Some SSL VPNs offer name-based policy management, which enables administrators to set-up access policies based on the names of domains or resources. As long as resources stay within the same domain, no additional administration is required as resources are added, moved or changed.

SSL VPN configuration choices include:

- Encryption—40- or 128-bit RC4; 56-bit DES; 112- or 168-bit 3DES encryption; 128 or 256 AES encryption
- Authentication—username/password (such as Active Directory or RADIUS); user name and token pin (such as RSA SecurID); or X.509 digital certificates (such as Entrust or VeriSign)

Which of the Two VPNs Provide a Greater Return on Investment?

Today, the initial purchase price of an IPsec VPN is a little less than that of an SSL VPN. However, when organizations tally total cost of ownership (TCO), the return on investment (ROI) for an SSL VPN is much stronger for remote access. Because SSL VPNs have no client to deploy and manage and are much easier to use, the ongoing costs to IT for administration and support are significantly lower. In addition, since users have anywhere access, overall productivity increases.

By using SSL VPN for remote access, you increase productivity by allowing users easier access to more corporate resources from more locations and devices, without interaction with IT. These users could be comprised of executive, sales, technical, consulting and healthcare professional staff, where even incremental increases in productivity will result in significant benefits. Other ancillary benefits may include faster time-to-market, increased responsiveness to customers, enhanced reputation and reduced attrition of internal staff.

Because SSL VPNs are clientless and rules-based—meaning you get highly granular access control—you can create a portal for your business partners so that they can access only the applications and resources they need. This scenario considers the potential cost savings and revenue enhancement from having a business partner extranet, resulting in lower costs and improved productivity, based upon fewer missed business opportunities, greater speed to market and eliminated overhead from paper-based transactions.

What are the Best Use Case Scenarios for Each VPN?

Providing remote access improves user productivity, yet carries security risks. Access is no longer limited to corporate-managed devices, so external resources such as personal digital assistants (PDAs) and smartphones must be incorporated into a growing list of supported devices and environments. Although you probably don't place equal trust in all points of access, such as partner networks or airport kiosks, you'll need to grant access to them, as well as to corporate wireless users, consultants, VoIP users and teleworkers working from other untrusted networks. A successful remote access solution controls access across a broad range of internal and external users securely from any endpoint.

IPSec VPNs are best-suited for site-to-site access. Open tunneling protects data between two private networks or between IT-managed machines and a private network. IPSec VPNs are optimal for transmissions between headquarters and:

- Branch offices
- Data centers

SSL VPNs are best suited for remote access. They are network independent, so there is no need to reconfigure administration rights as the user changes endpoints. Their clientless capability provides an easy end-user experience, reducing support costs. Additionally, application-level access ensures that all users gain access only to the information and applications they require. SSL VPNs are optimal for accessing applications and data on the corporate network, including VoIP communications, from any location or device with Internet access, including:

- Mobile devices, PDAs and smartphones
- Kiosks (computer terminals) at airports, tradeshow and libraries
- Hotel rooms
- Home offices
- Behind a customer's firewall
- Corporate-issued laptops (clientless or those installed with clients)

Why Choose a SonicWALL Aventail E-Class Secure Remote Access?

SonicWALL® Aventail® E-Class Secure Remote Access appliances (SRAs) provide universal application access with complete control and security. No other solution offers this level of access combined with full tunnel security and easy-to-use unified policy management. SonicWALL Aventail SRAs detect the security of an endpoint prior to application access, protect resources with granular policy based on that user and endpoint and connect the user effortlessly to authorized resources.

SonicWALL Aventail Smart SSL VPN technology offers the most transparent, flexible everywhere access options and is extremely easy to administer and use. SonicWALL Aventail's award-winning technology offers superior endpoint control, efficient centralized policy management and greater scalability, resulting in a lower TCO.

Supported applications and protocols include:

- Web-based applications, including most Java script and Visual Basic (VB) script content (HTTP and HTTPS protocols)
- Any TCP-based application
- UDP-based or multicast applications
- Applications that use VoIP
- Remote application-to-application access with SonicWALL Aventail Connect Tunnel™ Service Edition

SonicWALL Aventail SRAs include the SonicWALL Aventail Smart Tunneling™ technology, which offers bidirectional policy management, the ability to easily resolve any addressing conflicts for access from locations such as behind a company's firewall and full application access. With a Layer 3 connection and

support for UDP, TCP and IP protocols, SonicWALL Aventail E-Class SRAs offer an alternative to IPSec VPNs and all other remote access solutions.

How Do SonicWALL Aventail E-Class SRAs Provide Protection from Security Threats?

SonicWALL's Aventail SSL VPN technology sets the standard for delivering full secure access to a broad range of applications on your corporate network from anywhere—including many locations and devices that your IT department cannot control. Time-tested and standards-based, SonicWALL's Aventail SSL VPN technology helps reduce risk through its combination of SSL and access control technologies, along with a single point of management.

SonicWALL Aventail Secure Remote Access Appliances (SRAs):

- Detects the identity and security state of each end device with the market-leading device interrogation and data protection of SonicWALL Aventail Endpoint Control™ (EPC™)
- Protects corporate resources using SonicWALL Aventail Unified Policy™ as its enforcement engine to control admission based upon the level of trust for remote users and their endpoint devices and control access based upon the applications that users are authorized to access
- Connects admitted users easily and securely to access all authorized network resources using SonicWALL Aventail Smart Access™ and SonicWALL Aventail Smart Tunneling™ transport mechanisms
- Delivers an end-to-end layered security approach using innovative, open architecture that integrates well with best-of-breed technology partners.
- Provides market leading device interrogation and granular data protection across Windows, Windows Mobile, Apple iPhone®, iPad™, Macintosh and Linux platforms
- Interrogates for presence of malware, such as key-stroke loggers, as well as for security criteria like anti-virus update status, prior to authentication.
- Allows centrally-managed Policy Zones including Deny and Quarantine Zones
- Facilitates quick and easy denial of access from lost or stolen devices through certificate-based Device Watermarking
- Ensures user is authorized to use a particular device through Device Identification
- Extends beyond basic cache cleaning to purge browser cache, session history, cookies and passwords with SonicWALL Aventail Cache Control
- Closes connections by default, providing "deny all" firewall-style protection
- Optional SonicWALL Aventail Advanced EPC™ simplifies endpoint detection with a comprehensive checklist of anti-virus, personal firewall and anti-spyware and adds the encrypted virtual desktop protection of SonicWALL Aventail Secure Desktop
- CleanVPN™ with SonicWALL Network Security Appliance

How Does SonicWALL Aventail E-Class SRA Compare with Other VPNs for Ease-of-Use?

SonicWALL Aventail E-Class SRAs offer an unparalleled combination of everywhere application reach, ease-of-use and value extension.

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 SRAs offer:

- Intuitive, convenient SSL VPN access to all applications from anywhere: managed corporate laptops or unmanaged home computers, Internet kiosks and mobile devices such as PDAs and smartphones
- Support for Windows, Windows Mobile, Apple Macintosh, iPhone, iPad, 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 end-point
- 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 VoIP
- Virtual Hosts support complex Web applications, including those that leverage Flash and JavaScript
- Optional integrated access to Citrix farms and Windows Terminal Services applications, as well as to IBM, UNIX®, OpenVMS and Linux host-based applications

SonicWALL Aventail Smart Tunneling™ delivers fast and easy access to all applications—including Web-based, client/server, server-based, host-based or back-connect applications like VoIP—over a unique architecture that combines the application-layer control of SSL with the reach of a Layer 3 tunnel.

SonicWALL Aventail Mobile™ provides the most robust secure access for mobile PDAs and smartphones, featuring Session Persistence across office, home or mobile IP addresses without re-authentication.

How does SonicWALL Aventail E-Class Secure Remote Access Compare with Other VPNs for Ease-of-Control?

SonicWALL Aventail lets network managers easily set up and deploy a single secure access gateway for all users, internal and external, to all resources with complete control. SonicWALL Aventail's Set-up Wizard makes it the easiest "out of the box" experience and fastest solution to set up and deploy.

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.

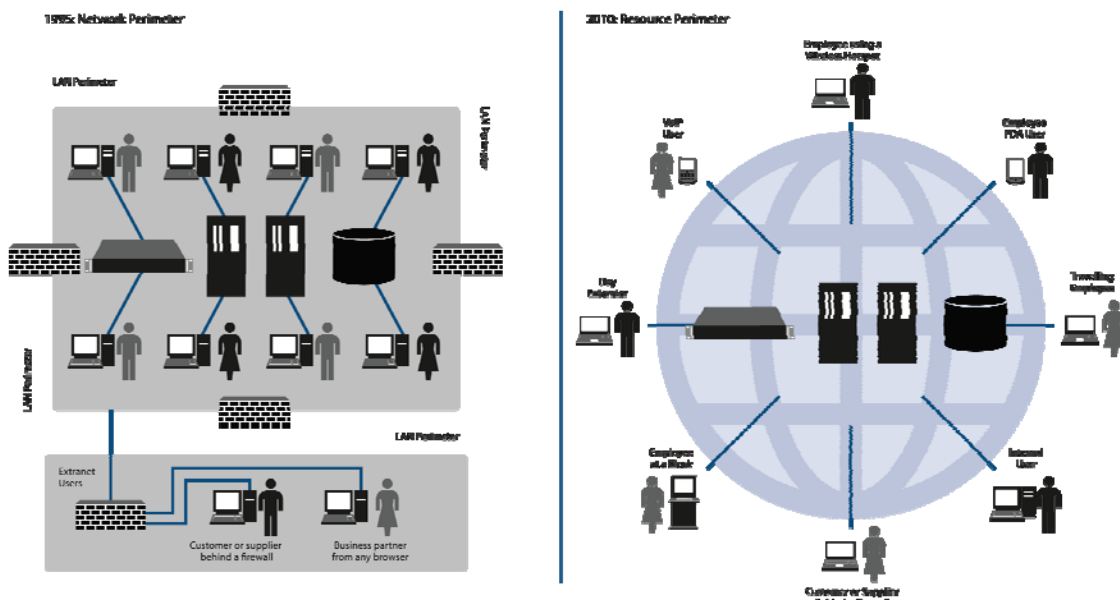
With SonicWALL Aventail E-Class SRAs:

- 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 SSL VPN appliance
- Intuitive, transparent user experience means fewer support calls, for lower IT overhead
- For most deployments, policy set-up 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
- In NAT mode, no set up of IP address pools is required

SSL VPNs also play a critical role in disaster recovery planning, serving as a secure application gateway at primary or backup data centers, as well as hot, warm or cold disaster recovery sites. The SonicWALL Aventail Spike License provides SonicWALL customers with an insurance policy toward future planned or unplanned increases in remote users. It's ideal as part of a company's overall disaster recovery plan or for firms that experience seasonal spikes.

What is the SonicWALL Aventail Vision for the Future of Remote Access Technology?



The security perimeter is changing. Companies today need to ensure that all resources accessed, data transmitted, and endpoint devices are protected against any type of security threat — internal or external.

Over the past decade, traditional network boundaries have been disappearing and “the office” no longer has anything to do with a physical location. People are working differently and more remotely. And enterprise

boundaries are blurring, with partners, vendors and consultants playing as vital a role in daily operations as employees do.

With these changes, the corporate network model has effectively inverted, evolving from the traditional enclosed LAN/WAN to a distributed global network that connects employees, partners and customers over multiple Internet, intranet and VoIP channels. The modern mobile workforce demands more secure access to more resources from more remote devices and platforms than ever before.

IT managers must now assume that any user and device is a potential risk point, whether the user is accessing resources or exchanging data remotely or are plugged directly into the LAN. Therefore, rather than secure networks, enterprises should focus on "secure communication."

To succeed in this changing environment, we believe that enterprises should re-examine how they view network security. And we would argue that networks are, in fact, inherently insecure. At SonicWALL, we believe the heart of the modern corporate network is the secure remote access control provided by SSL VPN technology.

We envision a world where secure remote access is made simple—where users have the freedom to securely access critical resources from anywhere and IT departments have the power to easily and securely manage access by all users and devices.

With our focus on SSL VPNs that are easy-to-use and control, SonicWALL is leading the way in making that vision a reality.

About SonicWALL

Guided by its vision of Dynamic Security for the Global Network, SonicWALL develops advanced intelligent network security and data protection solutions that adapt as organizations evolve and as threats evolve. Trusted by small and large enterprises worldwide, SonicWALL solutions are designed to detect and control applications and protect networks from intrusions and malware attacks through award-winning hardware, software and virtual appliance-based solutions. Visit <http://www.sonicwall.com/>



SonicWALL, Inc. 2001 Logic Drive, San Jose, CA 95124 T +1 408.745.9600 F +1 408.745.9300 www.sonicwall.com

©2010 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. 06/2010