

IPSec vs. SSL VPN: Transition Criteria and Methodology

A comparison of SSL VPN and IPSec VPN technologies and recommended implementations based upon use case

CONTENTS

Abstract	2
IPSec VPNs: Designed for Site-to-Site	2
Criteria for Retaining IPSec VPN	3
Criteria for Replacing IPSec VPN	3
Management Criteria	4
- Security criteria	
- Network transversal criteria	
- Interoperability criteria	
Benefits of SSL VPN	6
Rationale for Transitioning to SSL VPN	6
Overcoming Obstacles and Objections	7
Comparing IPSec VPNs with SSL VPNs	9
Best practices for Transitioning to an SSL VPN	10
Lessons from the Real World	12
Conclusion	13



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Abstract

Business mobility has driven the need for secure remote access from more locations, end point devices, platforms and environments. Correspondingly, VPN technology has evolved to meet this need. Increasingly, enterprise IT organizations are upgrading their remote access technology from legacy IPsec VPNs to more sophisticated SSL VPN solutions. This white paper examines the differences between these VPN technologies and provides you with criteria for deciding whether you should replace your IPsec VPN with SSL VPN. It then presents a step-by-step, practical approach to implementing your replacement.

In this white paper, you will learn how to assess your VPN needs, identify the limitations and optimal uses of IPsec, understand the benefits of an SSL VPN, consider key remote access configuration variables and examine the particular use cases in which you might keep IPsec. You will also discover how to evaluate SSL VPN solutions and what crucial features and benefits you will need to compare. You will also review alternative deployment scenarios and learn best practices on how to implement a staged VPN replacement, including the best-practice transition methodology and the impact upon administrators and end-users. Finally, you will receive first-hand insights from a real-world replacement.

The information presented in this paper represents the industry experience of the SonicWALL® research and development team and reflects the requirements that can be met by applying SonicWALL solutions. The SonicWALL solutions are referenced in the conclusion to this paper and can be reviewed in detail on the SonicWALL Web site: <http://www.sonicwall.com>.

IPsec VPNs: Designed for Site-to-Site

Virtual private networks (VPNs), initially based on the IPsec protocol, were originally developed for site-to-site communications between branch offices. These site-to-site VPNs were an economical way to extend the corporate network to remote offices over the public Internet, avoiding the high cost of private wide area network (WAN) connections. The resulting secure connection between trusted private networks offered access similar to that of the corporate network. As companies broadened their use of VPNs to meet other remote access needs, proprietary extensions had to be added to the IPsec standard, or to vendor implementations of the protocol, to address the complexity of adding individual end-users to the remote access equation.

An IPsec VPN works by establishing a tunnel over the Internet to connect users outside a corporate firewall or gateway to the internal network. It requires compatible hardware or software—almost always from a single vendor—on both ends of the tunnel. With IPsec, the corporate IT department dictates the technology used on both ends of the tunnel. Although this can work well for systems managed by the IT department, few companies are willing or able to fully control or trust the end point environments of remote devices used by teleworkers, business partners or customers.

At one time, a traditional Internet Protocol Security (IPsec) virtual private network (VPN) was the only option for secure remote access. However, because IPsec solutions were designed for trusted site-to-site connectivity and not with a highly-mobile workforce in mind, IPsec solutions had limitations for supporting untrusted end point locations that were not directly managed by IT. In response to increasing user demands for remote access, a new kind of VPN emerged—SSL VPNs. These new VPNs, based on the Secure Sockets Layer (SSL) protocol that safeguards the world of e-commerce, quickly became the leading option for remote access.

As organizations grow and become more mobile, many are shifting to SSL VPNs, as they offer “everywhere” access while retaining complete control and security. Recent advances in SSL VPN technology offer many benefits for both users and companies. When compared to IPsec, SSL VPNs are typically less costly to manage, eliminate concerns related to open-by-default tunnels and offer a more flexible experience for employees and business partners using untrusted end point environments.

Criteria for Retaining IPSec VPN

IPSec VPNs are best suited for point-to-point access. Open tunneling protects data between two private networks or between IT-managed machines and a private network. IPSec is a perfectly viable solution when a permanent connection is required between two specific locations, for example between a branch or remote office and a corporate headquarters. It can also be used successfully to provide access to a small finite number of remote workers using tightly-controlled corporate-issued laptops.

Many existing IPSec implementations can continue to work well for these use cases for which they were originally deployed. IT might consider keeping IPSec in these limited areas and extend remote access to other areas, such as trusted partners or extranet users, via a parallel SSL VPN solution. While a parallel VPN implementation is a viable choice for some enterprises, transitioning all access use cases through a single SSL VPN gateway might ultimately cost less and be easier to manage.

While many organizations still implement IPSec solutions today, however, for secure remote access the momentum has clearly shifted to SSL VPNs. Some organizations replace older versions of IPSec with newer versions that better streamline the provisioning of agents, or provide elements of end point control. Nevertheless, these augmented IPSec VPNs still may not be as flexible or robust as SSL VPN solutions. With increased access from unmanaged end point devices, end point control becomes a key risk factor. For managed devices, some IPSec solution providers suggest keeping IPSec and adding a network access control (NAC) solution. However, this greatly adds to the costs and complexity of administering and maintaining a separate appliance to achieve end point control, and still does not provide granular access controls down to the application layer, essentially allowing the remote device to be a node on the network.

Criteria for Replacing IPSec VPN

The ascendancy of IPSec technology as an innovative remote access solution peaked nearly a decade ago. IPSec VPNs are no longer an effective remote access solution when comparing costs of IT overhead and the desire for granular access controls for highly portable devices with the current demands of an increasingly mobile workforce. With early IPSec implementations, the considerable overhead involved in provisioning, maintaining and supporting dedicated IPSec clients was tolerated because IPSec access tended to be restricted only to relatively few managed-device use cases. In recent years, however, since broadband has become widespread and laptops have become cheaper, there has been greater incentive for IT to deploy more laptops and other mobile devices to more users across the enterprise, increasing the overhead needed to support distributed-client IPSec VPNs. While these devices are more likely to be transported beyond the physical office to be used at home or other remote sites, IPSec still views them as nodes on the network, regardless of location.

Workers are also now accessing corporate resources from more end point devices that are not directly managed by IT, such as home computers, WiFi-enabled laptops, PDAs, smartphones and public kiosks. While most workers today are not full-time teleworkers, many commonly perform teleworking functions, such as sending and receiving email and attachments from home before or after work hours, on weekends, while on the road or while on vacation. In addition, business partners need limited access to specific network resources which introduces additional remote access challenges to the IT department in today's world of outsourced supply chains. By providing employees and business partners with wider access to business tools and information, the proliferation of unmanaged end point devices has directly resulted in increased productivity. But it has also greatly increased the complexity for IT in controlling remote access, thereby minimizing the viability of distributed-client IPSec VPNs as an efficient remote access solution.

Emerging Issues Driving Migration to SSL VPN

- **Remote access:** employees, partners and customers need a remote access solution that is easy to use and deploy
 - **Disaster recovery:** during a business disruption, demand for remote access could spike to include the majority of your workforce
 - **Wireless:** many organizations now treat users on the wireless network as remote users because of concerns over who has access to the wireless network
 - **Extranets:** to promote increased collaboration, wider access for business partners is needed, yet without compromising access control and security
 - **Mobility:** mobile devices are increasingly functional for both data and voice, leading to a rise of IT-managed (and non-managed) mobile devices used for voice and data.
 - **Enforcing policy:** collaboration and regulatory compliance is encouraging more granular access controls, yet IT may struggle to enforce policy across disparate points of entry
 - **Network Access Control (NAC):** NAC is positioned around host integrity checking and network access, yet many organizations want to extend that to cover application access control as well
-

IPSec VPNs are also based upon an enclosed-perimeter approach to policy control. IPSec is a network layer protocol. In many legacy IPSec implementations, policy control was actually a secondary consideration. This is because early remote access via IPSec tended to be limited to a small number of managed corporate laptops for trusted executives and sales “road warriors.” Since these IPSec devices were required to be closely IT-managed, those using the devices remotely were treated as if they had logged into the LAN from their on-site desktop: once authenticated, users often ended up with access to the entire network. IT was forced to find alternate access solutions for non-managed end points, such as phones, kiosks and home PCs, adding the burden of managing many different solutions to support an increasingly mobile workforce. IPSec VPNs do not have the granular policy controls that a good security policy now requires, especially for compliance with regulations such as Sarbanes-Oxley and HIPAA. In addition, competitive pressures are requiring organizations to extend their supply chain out geographically to more remote users, business partners and contractors. As a result, many IT departments are rethinking network security in such a way that focuses on controlling all access to the data center/applications vs. just authenticating users to the network. This requires granular application access controls uniformly applied across all internal and external devices that can be used remotely. Because of IPSec VPN’s enclosed-perimeter model, many IPSec VPNs are also ineffective in providing secure extranet access through NAT, proxy servers, or firewalls or can do so only with additional administrative support.

A thorough examination of whether to replace IPSec VPNs with SSL VPNs must also take into consideration criteria in the areas of management, security, network traversal and interoperability.

Management Criteria

IPSec solutions can satisfy remote access requirements when there are a limited number of tunnels to create and the access scenarios are limited to corporate-managed systems. However, IPSec is not recommended for when there are dozens of remote users or more at different locations, as distributing and managing the required client software quickly places costly demands upon support resources. With an IPSec VPN, IT departments must install and maintain 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 support costs.

Unlike the workers at branch offices for whom IPSec VPNs were designed, today’s end-users are mobile. To be productive wherever they are, users need to be able to move freely between different devices such as portable and desktop computers used in the office, home computers, personal digital assistants (PDAs), smartphones, and public machines such as kiosks and between multiple networks including home networks, public WiFi networks, customer networks and others. With IPSec solutions, a VPN client must be provisioned to each supported system. Because IPSec clients don’t support all access points, users cannot get the everywhere access they expect and need. Also, IT departments must configure IPSec clients

differently, depending on the environment and networks used. Individuals who access corporate networks from different places require multiple configurations, increasing the complexity and cost of support. For example, IT might be called upon to manage installation of an IPSec client on a PC at a user's home, or troubleshoot issues arising from a user selling or handing-down personal computers with resident IPSec clients.

With IPSec, if a user doesn't have a pre-provisioned client on his or her computer, the user will not be able to access the resources needed. That means that today's highly-mobile employee who wants remote access from a home computer, a mobile device, an airport kiosk or any other remote location will need to call the corporate help desk to download a compatible client—if one is available—in order to get connected.

Security criteria

Because they create a tunnel between two points, IPSec VPNs provide direct (non-proxied) access and full visibility to the entire network. After a tunnel is created, it is as if the user's PC is physically on the corporate LAN: the user can directly access corporate applications and resources from the remote location. Although the user may not have access to each server, all of the available applications will be visible. Additionally, it is difficult to create policies that extend beyond the network layer i.e. the IP address level, meaning that it is difficult to segment access by the named applications that reside on each server. When users working from PCs at home or through wireless LANs, they face a host of threats from malicious hackers, viruses, worms and malware—threats that require organizations to counter them with extra security precautions. With IPSec VPNs, these personal risks can become corporate security risks; companies face the possibility that hackers will use the remote IPSec VPN network tunnel to gain unauthorized access to the corporate network unless accompanied by a network security appliance.

Network traversal criteria

IPSec VPN products and services offer no easy solutions to complex remote access situations involving Network Address Translation (NAT), firewall traversal, or broadband access. For example, a user with an IPSec client on his or her computer needs Internet access through a separate third-party network (such as a consultant working at a customer site or a traveling sales representative in a hotel). The IPSec connection may be stopped at that network's firewall unless the user negotiates the opening of another port in the firewall, typically by generating a call to their own IT department to follow-up with the administrator of the third-party network. Not only is this a tedious and time-consuming process, but it also creates a security risk that many companies may not want to take.

The same problem occurs at wireless hotspots. Because many public hotspots use NAT, non-technical users of IPSec solutions are often unable to figure out how to get connected and must contact their support staff for help in making configuration changes.

Interoperability criteria

The lack of standard technology between different IPSec vendors can create problems for the IT department tasked with setting up a VPN that involves integrating different vendors. For example, if an IT department must provide business partner or customer access, complex interoperability and integration hassles often delay the process.

Benefits of SSL VPN

SSL is the standard protocol for managing the security of message transmission on the Internet. SSL is a higher-layer security protocol than IPSec, working at the application layer rather than at the network layer. By operating at the application layer, SSL can provide the highly granular policy and access control required for secure remote access. Because SSL is included in all modern browsers, SSL VPNs can empower today's mobile workforce with clientless remote access—while saving IT departments the headache of installing and managing the complexity of IPSec clients. By extending the workplace to home PCs, kiosks, PDAs, and other unmanaged devices, SSL VPN solutions increase workforce productivity, resulting in a greater return on investment. And by eliminating the need to deploy and support "fat" clients, SSL VPN reduces IT overhead, resulting in a lower total cost of ownership.

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 the specific resources allowed by the company's security policy. SSL VPNs start with providing access via a Web browser, removing the need for IT to provision clients to the end point 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 where Active X or Java based "thin" clients are transparently pushed through the browser. Alternatively, most SSL VPNs allow IT to pre-provision the agents directly to a user's device, allowing the user to directly access the SSL VPN without having to open a Web browser.

Potential Benefits of Transitioning to an SSL VPN:

- **Increased productivity: SSL VPNs work in more places, including home PCs, kiosks, PDAs and unmanaged devices over wired and wireless networks.**
 - **Lower costs: SSL VPNs are clientless or use lightweight Web-delivered clients rather than "fat" IPSec clients, reducing management and support calls.**
 - **Broadened security: SSL VPNs provide granular access and end point control to managed and non-managed devices**
-

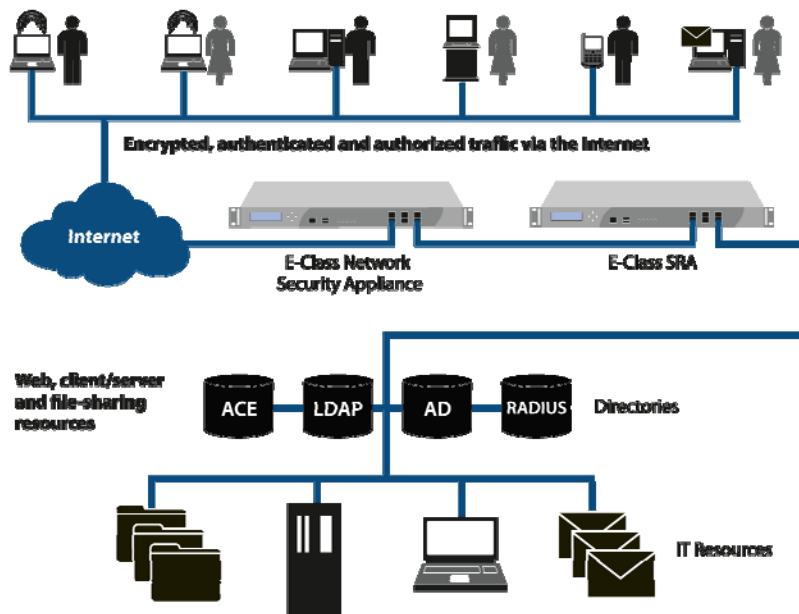
Rationale for Transitioning to SSL VPN

Today's modern mobile workforce demands more secure access to more resources from more remote devices and platforms than ever before. Corporate boundaries are blurring, with partners, vendors and consultants playing as vital a role in daily operations as employees do. These changes suggest the need for an inverted model for the corporate network, evolving from the traditional enclosed-perimeter model to a distributed global network that connects employees, partners and customers over multiple Internet, intranet and VoIP channels. IT managers must now assume that any user and device is a potential risk point, whether the user is accessing remotely or plugged directly into the LAN. Disaster recovery and business continuity initiatives pose additional incentive to provide remote access from any end point location. Policy-based granular access control becomes imperative.

Securing inverted networks with granular access control is an ideal use case for SSL VPN technology. SSL-based access control appliances are the key to achieving application access control. SSL VPN solutions can detect what is running on the end point device, protect applications with granular access control based on user identity and device integrity and connect users securely and easily to applications on any device.

Because SSL is part of any Web browser, SSL VPN solutions provide clientless and Web-delivered thin client access that significantly increases the number of points from which employees, partners and customers can access network data. SSL VPN solutions greatly simplify the connection process for mobile users, seamlessly traversing NAT, firewalls and proxy servers. SSL VPN solutions reduce IT support costs, lowering total cost of ownership. SSL VPN clientless access minimizes the IT overhead involved in provisioning, configuring and maintaining an enterprise remote access solution. Alternatively, certain SSL VPN tunnel solutions provide a complete "in-office" experience by deploying an auto-updating, Web-delivered thin client, eliminating the need for direct IT intervention. SSL VPN solutions also streamline administration costs by controlling all access to enterprise resources via a single, centralized gateway.

SSL VPN solutions also provide greater security compared to IPSec. Since SSL is an application layer protocol, an SSL VPN is inherently better-suited for securing application-based remote access. SSL VPN solutions 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. With SSL VPN solutions, end-user access to any given resource is restricted unless authorized. 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 to meet regulatory compliance and corporate security mandates.



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

Overcoming Obstacles and Objections

As in any enterprise technology transition, there are serious considerations in replacing IPSec. In many cases, the expense of the existing IPSec solution is a sunk cost. Many older IPSec implementations have been paid off and those investments have become fully amortized. Today, IT managers are increasingly allocating budget and resources to replace old depreciated technology and implement newer SSL VPN solutions.

While deployment of an SSL VPN is relatively painless, you must still consider the logistics of removing IPSec clients and configurations from existing managed devices. This might be best approached during scheduled maintenance or replacement of these devices. For instance, many enterprises are upgrading managed end point devices to support Microsoft Windows 7, or rolling out managed Macintosh or Linux devices. IT could then simply refrain from deploying or configuring the IPSec client to these new devices.

At one time, administrators were hesitant to replace IPSec with SSL VPN because there was not an easy way to transition users between the technologies. Users were faced with unfamiliar interfaces and sometimes required separate training. However, over the last few years, advances in SSL VPN tunneling have enabled a seamless, transparent user experience. Since SSL VPN users can access their applications and resources with the same familiar interface whether they are at the office or working remotely, they no longer require special training or hand-holding. Users simply click the new VPN icon instead of the old icon. There is still a learning curve when IT administrators begin using new technology on a new console. However, with better SSL VPN solutions, object-based management and an intuitive, user-friendly GUI make administrator ramp-up significantly faster and easier.

Today's SSL VPN solutions can provide both Web-based and agent-based access. IT can point users of non-managed devices to an easy-to-use portal configured with appropriate levels of access control. In using SSL VPN to replace IPSec for managed devices, IT can easily provision an agent or thin client to provide the same user experience as IPSec, but with less management complexity and greater control.

Comparing IPSec VPNs with SSL VPNs

Attributes	Secure Access Options	
	IPSec VPNs	SonicWALL Aventail SSL VPN
Applications supported:		
Broad client/server support	Yes	Yes
Legacy applications	Yes	Yes
HTTP applications	Yes	Yes
File sharing	Yes	Yes
Mainframe applications	Yes	Yes
Terminal servers	Yes	Yes
Access support:		
Clientless access	No	Yes
Session persistence across IP addresses	No	Yes
Java applets activated by session and then turned off	No	Yes
Bi-directional access control for back-connect applications like VoIP	No	Yes
Environments supported:		
Corporate PC	Yes	Yes
From home or hotel with broadband	Varies	Yes
Business partner access	Varies	Yes
From behind another company's firewall	Varies	Yes
From home or a friend's PC	Not without client	Yes
Public kiosk or PC	No	Yes
Standard PC on wireless LAN	Yes	Yes
Wireless PDA	Yes	Yes
Smartphone/iPhone	Limited or NA	Yes
Macintosh device	Limited or NA	Yes
Linux device	Limited or NA	Yes
Security model:		
Proxy protection	No	Yes
Strong user authentication	Proprietary	Yes
Strong central authorization	Limited	Yes
Single Sign-On (SSO) support	No	Yes
Dual/Stacked Authentication	No	Yes
Forms-based Authentication	No	Yes
Granular access control to URL level and at the appliance level	No	Yes
Prohibits visibility of DNS names and IP addresses	No	Yes
Device Watermarking/Device Identification:	No	Yes
Quarantine and Deny Zones:	No	Yes
End Point Control of unmanaged devices:	No	Yes

Ease of administration:

Cost-effective deployment, configuration and support	No	Yes
Easy to use and support in any network without reconfiguring	No	Yes
Easy NAT and firewall traversal	No	Yes

Best fit:

Site-to-site VPNs: Sharing all network resources only with fully-trusted branch offices using locked-down IT-managed end-point devices	Yes	No
Sharing Web, client/server, legacy and custom applications with mobile users who require varying degrees of access, including remote employees, employees working remotely on a short-term basis due to disaster recovery, illness, or other business disruption, as well as business partners, suppliers and customers	No	Yes

Best practices for Transitioning to an SSL VPN

While SSL VPNs can be up and running in a matter of minutes, the timeline for a phased migration—from initial implementation of SSL VPN for unmanaged devices to expanded deployment to replacing existing IPSec clients—typically takes anywhere from a few months to up to 18 months, depending upon the size of the enterprise. This usually gives administrators enough time to run an SSL VPN pilot in a lab environment to establish and evaluate their security policy and configuration before phasing out IPSec.

**Migration Strategy:
Four-Phase Approach
to Replacing IPSec**

- Policy definition
- Lab tests
- SSLVPN deployment
- IPSec phase-out

Phase I: Policy definition

An SSL VPN allows you to restrict access to applications based on the user, the user's role, the user's device identity and health and your established security policy. That way, you can change authorization based on both user and device and segment access only to resources on the network that are appropriate. By excluding unauthorized users from inappropriately accessing resources, you reduce the risk to those resources. Prior to deploying an SSL VPN, you should establish a written corporate security policy. Your security policy should cover acceptable usage for IT-managed devices, as well as cover responsible behavior for access from non-managed devices. An SSL VPN can provide a single solution that allows you to centrally enforce policy for both IT-managed and non-managed access devices.

Your policy should clearly define access based upon a user's role in the organization. Roles determine the level of access users should have, the appropriate resources they should be able to access and the security requirements for authorizing access, both for the user and their end point devices. Once defined, make sure corporate security policy is understood by all users.

Define what user roles should be allowed access to what resources and also define the trust levels for different types of devices that can be used for access. For example, a financial manager needs access to account receivables applications, but not human resources applications; and a human resources manager needs access to human resources records—but not account receivables applications. Alternately, a CEO might be allowed access to both resources; however, while attempting access from a public airport kiosk, that same person might be identified in the role of "kiosk user," and be restricted from accessing either resource.

Phase II: Lab tests

A lab environment pilot lets you "road test" your SSL VPN in various real-world scenarios, without directly impacting your users or putting your resources at risk.

For unmanaged devices, apply access control policies to specifically restrict sensitive data types (such as social security or credit card database information) from being downloaded to a mobile wireless device. This

might be done by limiting access to view-only. Alternately, you might apply a terminal services or virtual desktop approach (such as Windows Terminal Services over Citrix.) You should also mandate what data-at-rest security applications (such as antivirus software) must be resident on a particular end point device type in order to permit access.

Consider robust user authentication, such as mandatory two-factor authentication using tokens or client-based digital certificates. Strong authentication is important for both unmanaged devices and managed devices that are highly mobile. For instance, a “shoulder-sniffer” might steal username or password information from a user typing on a laptop in the next seat at in an airport or other public place. Or a user might sell a personal home computer without fully removing security information, such as network passwords, from its hard drive.

Establish end point controls to interrogate the end point device to confirm whether it is managed or unmanaged and that the device environment is in a secure state when attempting access. For example, you might require that the SSL VPN checks the device to confirm it has recently run a current-version antivirus software scan, that the user is authorized to use that particular device, or that it contains a watermark based upon a device certificate. Then, should the end point device be reported as lost or stolen, the certificate could be revoked and access to your network from that device would be denied.

Phase III: SSL VPN deployment

Unlike with IPsec, SSL VPN deployment is relatively simple and straightforward, usually consisting of providing users with a URL. For example, with SonicWALL® Aventail® E-Class SSL VPN solutions, SonicWALL Aventail WorkPlace™ provides out-of-the-box clientless browser access to Web and client/server applications and file shares from *unmanaged devices* using Windows, Windows Mobile, Macintosh and Linux platforms, including home computers, public machines, smartphones and PDAs. SonicWALL Aventail Connect™ adds a Web-delivered thin client on the same broad range of platforms for *managed devices*, enabling a complete “in-office” experience without having to access a portal. In addition, SonicWALL Aventail Connect Service Edition delivers remote application-to-application access for scenarios where no human intervention is required and SonicWALL Aventail Connect Mobile™ provides “in-office” access for Windows Mobile-powered device users.

Phase V: IPsec phase-out

The final step is to run all devices previously using IPsec through SSL VPN. Prior IPsec users will already have parallel access to the SSL VPN through their browsers. As IT-managed devices are scheduled for maintenance or replacement, the IPsec clients and configurations can then be removed. Since, in general, SSL VPN tunneling should not conflict with IPsec, you might optionally leave both IPsec and SSL VPN agents running on the same device for a period of time to help transition users from the old technology to the new. Finally, the IPsec VPN appliance can simply be deactivated once all users have been migrated.

Lessons from the Real World

In the real world, IT decisions are made in response to a range of pressures, existing infrastructure and practical limitations. The following is an interview with Richard Quelch, Network Manager at Norwich University, on his experiences in replacing IPsec with an SSL VPN.

How do you know when you should replace your IPsec VPN?

I think who uses the VPN—and how the VPN is used—drives the type of VPN needed. For example, if you have many Web or GUI-based applications, then it is probably best to move to a SSL VPN. Additionally, if your users expect applications to just work, expect little or no work to maintain or launch their VPN solution, frequently have limited bandwidth, or use satellite connections, it is probably best to move to a SSL VPN.

Should you add SSL VPN to your existing IPsec VPN, or replace IPsec entirely?

An SSL VPN solution should meet most, if not all, of your VPN needs. However, IPsec VPN solutions can still work well for advanced IT-level users in scenarios requiring specific ports, such as in Oracle administration.

When should you phase out your IPsec VPN, once the SSL VPN has been fully implemented?

We've found that six months seemed to be ideal. This accommodates users who tend to drag their feet but did not stretch out the process too long. The length of time depends on the process used and the amount of users making the transition. Ongoing costs of licensing, supporting and maintaining two VPNs also should be considered.

What is the best way to make the transition?

There is definitely a graceful way to make the transition. We found it best to add a minimal amount of users first, representing different areas of our organization. Time needs to be given to address access issues, to discover how the SSL VPN is used, which applications are accessed via the SSL VPN and to determine key areas of interest.

What risks do administrators need to avoid?

With an SSL VPN, we store more information on a device, whereas with IPsec we stored only configuration information. It is critical to maintain a backup of the information and the configuration of your SSL VPN.

What ROI can administrators expect from replacing IPsec with an SSL VPN?

We've found that the maintenance and support time for SSL VPN is much less than was with IPsec, resulting in less cost. Also, end user productivity is higher, because access to resources over the VPN is available more often.

How did the transition impact your end-users?

It was very easy for us to roll out SSL VPN to our users. They needed minimal training—usually we only needed to give the users the URL to get them started and connected. Our solution allowed us to give our users a desktop look-and-feel and personalized shortcuts. Understanding what our users like—and don't like—greatly helped in "selling" the new VPN.

What tips do you have for administrators to make the transition easier?

While the replacement process wasn't difficult for us at all, it is important to know the applications well that will be accessed through the SSL VPN and to thoroughly test each application before deployment. And you should consider rolling out more advanced SSL VPN features over time, so that you don't initially overwhelm your users with too many new options.

Conclusion

Whether an IPSec or SSL VPN is the right choice ultimately depends on the extent of your company's secure remote access needs:

- IPSec VPN technology is designed for site-to-site VPNs or for remote access from a small finite number of tightly-controlled corporate assets. If these are the primary needs of your company, IPSec performs these functions quite well.
- SSL VPN technology, on the other hand, works much better for secure remote access. SSL VPN technology is an ideal replacement for—or adjunct to—IPSec, because it increases productivity by allowing access to more resources from more end points; lowers costs by easing administration with clientless (and easy-as-clientless) access and centralized control; and adds security with granular access and end point control. Best practices for transitioning to an SSL VPN include establishing a corporate security policy, conducting a lab environment pilot and implementing a phased migration.

SonicWALL has a VPN solution to match your specific requirements. SonicWALL TZ , NSA and E-Class NSA Series appliances offer integrated SSL VPN for secure remote access and/or IPSec VPN for secure site-to-site remote access scenarios. SonicWALL E-Class Secure Remote Access and Secure Remote Access Series appliances offer SSL VPN to endpoints beyond IT control, without the costly overhead needed to deploy and maintain per-seat “fat” clients, boosting workforce productivity, easing manageability, and enhancing enterprise network security. SonicWALL SSL VPNs offer easy, effective solutions for the evolving remote access demands of today's mobile workforce, including remote access, disaster recovery, wireless networking, extranet access, mobile networking, policy enforcement, and network access control.

SonicWALL can help your organization deliver anywhere access to any application from the broadest range of devices and help you lower costs and increase the productivity of both your end-users and IT staff. To learn more, visit 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