

Why Switch from IPSec to SSL VPN

And Four Steps to Ease Transition

SONICWALL[®]

PROTECTION AT THE SPEED OF BUSINESS[®]

Table of Contents

The case for IPSec VPNs	1
The case for SSL VPNs	2
What's driving the move to SSL VPNs?	3
IPSec VPN management concerns	4
IPSec VPN security concerns	5
Why switch to SSL VPN?	6
Overcoming obstacles and objections	7
Best practices: 4 steps to an easy transition	8
Real-world lessons	13
Conclusion	14

The case for IPSec VPNs

Internet Protocol Security (IPSec) virtual private networks (VPNs) were originally developed over a decade ago to help businesses avoid the costs of privately-leased WAN lines. IPSec VPNs work by establishing a tunnel over the Internet to connect the internal corporate network to a site outside a corporate firewall or gateway.

IPSec needs compatible hardware or software, often from a single vendor, at both endpoint locations. IPSec VPNs remain viable solutions for connecting trusted endpoint devices that are directly managed by IT (such as branch or remote office computers), but not for mobile or personal devices.



***Still, IPSec VPNs are not the best choice
for today's modern mobile workforce.***

The case for SSL VPNs

Today's highly mobile teleworkers demand more secure access to more resources from more remote devices and platforms than ever before. Corporate boundaries are blurring. In daily operations, partners, vendors and consultants have become as crucial as employees.

The old corporate network has inverted. The enclosed-perimeter model has evolved into a distributed global network that connects employees, partners and customers over multiple Internet, intranet and VoIP channels.

***SSL VPN is ideal for secure remote access
from anywhere with granular access control.***

SSL VPNs can:

Detect what is running on the endpoint 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.

What's driving the move to SSL VPNs?

- **Remote access** is required to connect employees, partners and customers, without hands-on IT intervention.
- **Mobile devices**—both IT-issued and personal—are increasingly being used for both data and voice.
- **Disaster recovery** could suddenly spike demand for remote access to include the majority of your workforce.
- **Wireless users** are now often treated as remote, due to concerns over who actually has access to their wireless device.
- **Extranet access** for collaborating with business partners must not compromise security.
- **Enforcing policy** to meet regulatory compliance has become more complex across disparate points of entry.
- **Network Access Control (NAC)** is expected to cover application access control, as well as host integrity and network access.
- **Green IT** initiatives dealing with rising transportation costs and environmental concerns are leading towards increased flexibility for employees wanting to work from home.



IPSec VPN management concerns

With an IPSec VPN, IT must install and maintain individual VPN clients on each remote device. An IPSec VPN may also require changes to the desktop configuration.

If users don't have IPSec clients preinstalled on their remote computers, they can't access needed resources. A remote teleworker would need to call the help desk to download a compatible client—if one is available—in order to get connected. Partner and vendor VPN clients can be incompatible. Network Address Translation (NAT), firewall traversal, broadband access and wireless hotspots can also create difficulty for IPSec VPN connectivity.

*IPSec VPN client configuration can
result in higher support costs*



IPSec VPN security concerns

Because they create a tunnel between two points, IPSec VPNs provide direct (non-proxied) access and full visibility to the entire network, which can be effective in certain highly-controlled branch office environments where authorized users on IT-managed devices are connecting to a corporate headquarters. When users work from home PCs or over wireless, however, they face a host of threats from malicious hackers, viruses, worms and malware.

*With IPSec VPNs,
home PC risks become corporate security risks.*



Unless accompanied by an additional network security appliance, companies also face the possibility that hackers will use the remote IPSec VPN network tunnel to gain unauthorized access to the corporate network.

Why switch to SSL VPN?

SSL works at the application layer instead of the network layer, providing the highly granular policy and access control needed 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 VPN clients.

SSL VPNs:

- **Increase 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.
- **Broaden security:** SSL VPNs provide granular access and endpoint control to managed and non-managed devices.

*SSL is the standard protocol
for secure message transmission on the Internet.*

Overcoming obstacles and objections



Since the sunk costs of existing IPsec VPN solutions are often fully amortized, IT can defend allocating budget to replace depreciated technology with newer SSL VPN solutions. IPsec clients and configurations can be efficiently removed from existing managed devices during scheduled maintenance or upgrades.

***SSL VPNs can provide the same user experience as IPsec VPN
—but with less management complexity and greater control.***

SSL VPN users do not require special training or hand-holding, as they can access their applications and resources with the same familiar interface. The user transition is simple: they just click the new VPN icon instead of the old icon. It's easy to provision SSL VPN access whether or not the user's device is managed by IT. If they are working from a personal device, they just open a browser and navigate to the SSL VPN URL.

Best practices: 4 steps to an easy transition

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 VPN clients—will depend upon the size of the enterprise.

Phased transitioning may take from 2-18 months.

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 VPN. A successful migration strategy for replacing an IPsec VPN with an SSL VPN might include the following four steps:

- 1 Define Security Policy.**
- 2 Implement Security Policy.**
- 3 Deploy SSL VPN.**
- 4 Phase out IPsec VPN.**

Step **1** : Define security policy

SSL VPN lets you restrict access to applications based on the user, the user's role, the user's device integrity and your established security policy, and segment access only to resources on the network that are appropriate. Prior to deploying SSL VPN, it is a good idea to establish a written corporate security policy covering:

- How a user's organizational role determines what resources they may access.
- How users may access the network from IT-managed and non-managed devices.

***Make sure
corporate security policy is understood
by all users.***

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.

Step **2** : Implement security policy

SSL VPNs let you implement policies ranging from wide-open access to very granular controls. Choose an enforcement method appropriate to your security policy. Granular policies are useful for remote access control from either IT-managed or non-managed devices, as there will always be trust concerns when you don't control the access environment. Generally, you will want to enforce different access for those devices that are managed by IT and those that are not. For implementing your security policy, consider these controls:

- **Restrict sensitive data types** (such as social security or credit card database information) from being downloaded, or limit access to view-only.
- **Apply two-factor authentication** using tokens or client-based digital certificates. This protects against passwords being viewed and stolen in public places, or personal computers being sold or discarded with login information still remaining on the disk.
- **Establish endpoint controls to interrogate the endpoint device** to confirm whether it is managed or unmanaged, and in a secure state before attempting access. For example, you might confirm the device has recently run a current-version anti-virus software scan, or that it contains a watermark based upon a device certificate.
- **Set up different access groups** that allow you to differentiate access based on user identity and endpoint interrogation. This ensures that appropriate access is provided for a business partner, an IT technician working from a home PC, or an executive traveling with an IT-managed laptop.

Step **3** : Deploy SSL VPN

Unlike IPSec VPN deployment, SSL VPN deployment is relatively simple and straightforward, usually consisting of providing users with a URL. For example, SonicWALL® Aventail® E-Class Secure Remote Access (SRA) appliances offer flexible deployment solutions for:

- **Unmanaged devices:** 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.
- **Managed devices:** 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.
- **Application-to-application:** SonicWALL Aventail Connect Service Edition delivers remote access for scenarios where no human intervention is required.
- **Mobile devices:** SonicWALL Aventail Connect Mobile™ provides “in-office” access for Windows Mobile-powered device users.

Step **4** : Phase out IPSec VPN

During the deployment phase, prior IPSec VPN users will have been provided parallel SSL VPN access via either an SSL VPN agent on IT-managed devices or a browser on unmanaged devices. The final phase is to deactivate the now-unused IPSec connections.

*Once all users have migrated,
the IPSec VPN may be deactivated at the appliance.*

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 set period of time before deactivation to help transition users from the old technology to the new. To minimize administrative impact, deactivated IPSec clients and configurations can be removed from IT-managed devices during scheduled maintenance or replacement.

Real-world lessons



Real-world Network Manager at Norwich University, Richard Quelch, shares some of his experiences in replacing IPsec with an SSL VPN:

"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."

"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. 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."

"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

IPSec VPN technology is designed for site-to-site VPNs, such as those connecting highly-controlled IT-managed branch office devices to corporate headquarters. SSL VPN technology, on the other hand, works much better for secure remote access.

SSL VPNs:

- Allows access to more resources from more endpoints.
- Lowers costs by easing administration with clientless (and easy-as-clientless) access and centralized control.
- Adds security with granular access and endpoint 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 and NSA Series appliances offer integrated IPSec VPN for secure site-to-site access. SonicWALL Aventail E-Class Secure Remote Access (SRA) appliances and SonicWALL SSL VPN appliances offer secure remote access for today's mobile workforce, including remote access, disaster recovery, wireless networking, extranet access, mobile networking, policy enforcement, and network access control.

How Can I Learn More?

- Download the Whitepaper "*IPSec vs. SSL VPN: Transition Criteria and Methodology*":
<http://www.sonicwall.com/whitepaper>
- Opt-in to receive SonicWALL Newsletters:
http://forms.sonicwall.com/forms/Subscription_NA

For feedback on this e-book or other SonicWALL e-books or whitepapers, please send an e-mail to **feedback@sonicwall.com**.

About SonicWALL

SonicWALL® is a recognized leader in comprehensive information security solutions. SonicWALL solutions integrate dynamically intelligent services, software and hardware that engineer the risk, cost and complexity out of running a high-performance business network. For more information, visit the company Web site at **www.sonicwall.com**.