SSL VPN Grows Up:
Time to Demand More from Your Next SSL VPN

Written for WatchGuard® Technologies by Lisa Phifer, Core Competence

May 2009

Introduction

Years ago, businesses started turning to SSL VPNs to reduce the cost and complexity of remote access. Early SSL VPNs focused on relieving IT pain associated with IPSec VPN clients, using web browsers to help more remote workers reach common business applications. This value proposition prompted many companies to rethink legacy VPNs and launch successful SSL remote access deployments.

Since then, business needs have continued to evolve. Today's workforce is more mobile than ever – demanding access to a wide variety of business applications and systems, from increasingly diverse devices and locations. IT departments must now find more efficient, effective ways to satisfy ever-changing connectivity needs. Moreover, they must do so without exposing corporate assets to malware or breach, while maintaining the control and visibility mandated by industry regulations and privacy laws.

Fortunately, SSL VPN gateways have also matured. Contemporary products have surpassed old access limitations, tightened IT controls, and increased automation. As your organization moves to master today's mobility challenges, it's time to dissolve any lingering misconceptions and demand more from your next SSL VPN.

Myth #1: SSL VPNs only support web and browser-interfaced applications

FACT: Today's SSL VPNs offer a choice of access methods to support any TCP/IP application, from "clientless" browser interfaces to thin-client SSL tunneling.

Early SSL VPNs began as HTTP proxies, letting workers reach web applications through a VPN gateway using nothing more than an ordinary browser. To reach non-web applications, SSL VPNs implemented browser-based GUIs and content translators that were specific to each business program. For example, workers might use a Java frontend to interact with network file servers, relying on an SSL VPN gateway to translate HTTP requests into native Windows SMB protocols.

But to keep up with rapidly changing business needs, SSL VPNs had to expand far beyond browser-interfaced applications. Today's products offer browser-launched thin clients that can support just about any application by tunneling non-web protocols over SSL. Many thin clients intercept messages sent to specified ports, forwarding TCP sessions through the VPN gateway to private application servers. Some intercept IP packets, routing all user traffic through the VPN gateway into the private network. SSL VPN thin clients can significantly expand business application reach, while continuing to leverage the browser as a ubiquitous access delivery platform.

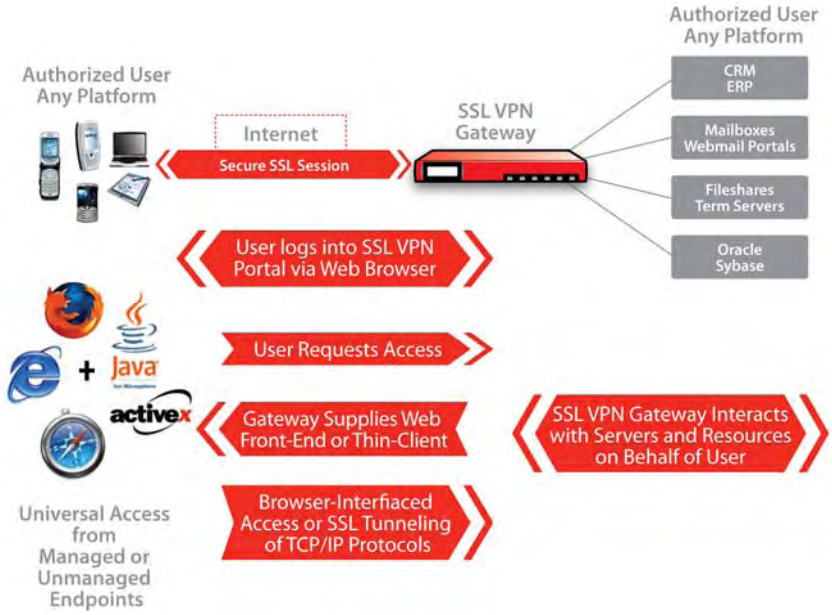

Figure 1: SSL VPNs offer flexible access methods

Myth #2: SSL VPNs are no different than ordinary web portals

FACT: SSL VPNs can deliver highly customized portal views that reflect and enforce each user's individual resource and application access rights.

SSL VPN gateways may have started as simple web access concentrators, but contemporary products now deliver sophisticated, dynamic access portals. A static web portal gives everyone the same browser-based view of a single service. Access is controlled independently by each server, with diverse user groups requiring different static portals to compartmentalize data.

SSL VPNs can accomplish this more efficiently and effectively by offering highly customizable portals that provide each individual with granular access to all authorized applications and resources – and nothing more. Furthermore, SSL VPNs may consider not just authenticated user identity, but the endpoint used to obtain access. Application and resource rules may then be used to determine who is granted access, the actions they can perform, and how resources are named and displayed. In this way, organizations can present portal views, tailored to each individual and situation, while relying on a single gateway to control and track access for all.

Myth #3: SSL VPNs don't support access from PDAs or phones

FACT: SSL VPNs may now be accessed from a broad range of devices, including those running Windows CE, Symbian, Palm, and even WAP phones.

SSL VPNs that focused exclusively on browser-based access reached many more endpoint devices than legacy IPSec VPN clients ever could. But some early web frontends and thin-clients created new compatibility concerns, like ActiveX controls that could only run on Win32 PCs or browser interfaces that were hard to use on small screen PDAs.

As workforce mobility grew, securing access from wireless handheld devices was no longer "nice to have" – for many enterprises, this is now a business necessity. Fortunately, SSL VPNs have also expanded endpoint platform support. Thin-clients have been ported to Linux and Mac OS and tapped Java's near-universal reach. New web frontends adapt automatically to mobile operating environments on Windows Mobile, Symbian, and Palm smartphones. Some SSL VPNs even support "ordinary" cell phones with WAP browsers. As new mobile devices like the iPhone and Android continue to emerge, contemporary SSL VPNs are well-positioned to deliver consistently secure access across the entire mobile workforce.

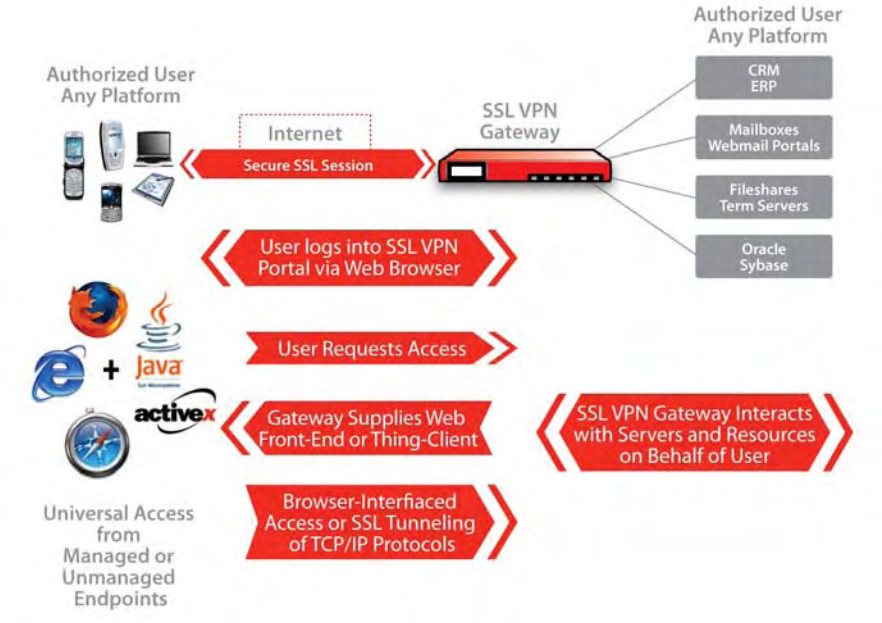

Figure 2: SSL VPNs support a wide variety of endpoints and applications

Myth #4: SSL VPNs expose corporate assets to malware on unmanaged PCs

FACT: SSL VPNs can evaluate endpoint health and compliance before deciding whether and how to grant access to authorized business resources.

By using ordinary web browsers, early SSL VPNs made remote access possible from unmanaged endpoints such as Internet cafés, teleworker home PCs, and business partners. But unmanaged systems are inherently vulnerable to malware, and even well-intentioned people have an unfortunate tendency to leave sensitive data behind. In such environments, an authenticated, encrypted tunnel is simply not good enough – corporate resources and data must also be insulated from loss, theft, or attack.

SSL VPNs have evolved to address these challenges – not just on unmanaged PCs, but for all endpoints. Specifically, SSL sessions can be used as a conduit to evaluate each endpoint's integrity *before* authenticating the user or authorizing access. For example, some SSL VPNs can query endpoint OS version/patches and anti-virus presence/signatures. Some can look for trusted endpoint identifiers like hardware addresses or host certificates. Some SSL VPNs can even check managed endpoints for compliance with corporate security policies. Armed with this intelligence, businesses can make access decisions to mitigate malware threats. For example, policies might deny endpoints that cannot satisfy minimum safety requirements, grant tunneled access from compliant laptops, and permit narrow "kiosk mode" access elsewhere.

Myth #5: SSL VPN authentication can be compromised by keystroke loggers

FACT: SSL VPNs can deter this threat using strong authentication methods, paired with external authentication servers or built-in strong authentication services.

Malware itself has evolved; organized cyber-criminals are increasingly focused on personal identify theft for financial gain. Spyware has grown common – especially trojans that turn compromised endpoints into remotely managed attack platforms. Keystroke logger trojans are of particular concern to VPN administrators because they might capture a reusable text password before endpoint security checks can be completed.

Contemporary SSL VPNs address this threat. Some can display "virtual keyboards" to avoid text passwords. Most can be paired with enterprise two-factor authentication servers (e.g., RSA SecurID). But balancing strength, ease of use, and cost can be challenging. To facilitate strong authentication, some SSL VPNs can generate one-time passwords that don't require hardware tokens or external authentication server purchase. Some can even map VPN strong authentication methods to less robust LAN logins (e.g., Active Directory), delivering single sign-on experience without exposing corporate passwords to keystroke loggers.

Myth #6: SSL VPNs leak corporate data onto home and public PCs

FACT: SSL VPNs can avoid this by limiting what each user can do, keeping data safe during an SSL session, and deleting it at log-off.

SSL VPNs have long reduced risks posed by home and public PCs by enforcing granular access controls. For example, policies may deny thin-client SSL or IP tunnels from endpoints that are not fully trusted, or provide read-only access to files, displayed in graphic rather than text format. In addition, most SSL VPNs offer post-session cleanup options that can automatically disconnect inactive users and delete traces of user activity (e.g., browser history, cached objects, temp files).

However, as SSL VPNs becomes the dominant form of secure remote access, workforces are shifting. More and more SSL VPN users are "frequent flyers" that access corporate resources repeatedly from the same unmanaged endpoint. Those users can operate more productively when given broader access and some degree of persistence. For example, pairing SSL VPN sessions with secure virtual desktops can provide a consistent, safe execution environment that remains encrypted in between sessions. In short, all unmanaged endpoints are not public PCs – more discriminating SSL VPNs can improve user experience without compromising security.

Myth #7: SSL VPN connections go down a lot and require repeated logins

FACT: VPNs can use high availability and single sign-on techniques to keep users continuously connected and maximally productive.

IPSec VPN users know the pain of lost connectivity. Network layer tunnels require reestablishment when IP addresses change, disrupting application sessions and requiring repeated logins – if not to the VPN, then to each application. All too often, IPSec users end up frustrated and unproductive – especially nomadic wireless users.

SSL VPNs inherently bypass these IPSec limitations. SSL sessions resume automatically after loss of connectivity, quickly and without user intervention. Some SSL VPNs go further to facilitate network roaming. For example, a user's authenticated state may be preserved during brief loss of connectivity or reinstated transparently by single sign-on. SSL VPNs that tunnel IP packets use virtual addresses that do not change when roaming. Finally, high availability SSL VPN clusters can keep users continuously connected during gateway maintenance or failure.

Myth #8: SSL VPN policies are complex and hard to manage

FACT: SSL VPNs can use central policy managers and be integrated with enterprise authentication servers and directories to simplify administration.

Certainly, there is plenty of potential for SSL VPN policies to grow unwieldy. With granular policies, multiple access methods, endpoint security checkers, and customizable portals, VPN administrators have a lot of power that must be wielded wisely to achieve desired results.

Here, experience shows; mature SSL VPN products have undergone years of refinement. Techniques like group or role-based policies, reusable policy objects, and templates have streamlined SSL VPN administration. SMBs can benefit from wizards and built-in integrity checkers or authentication services that might otherwise lie beyond their means. Larger businesses can leverage integration with enterprise authentication servers, single-point policy administration for multiple gateways, and consolidated logs for compliance audits and reporting.

Myth #9: SSL VPNs are just as difficult to deploy as IPSec VPNs

FACT: SSL VPNs avoid client installation and provisioning by offering clientless and thin client alternatives, accompanied by user auto-enrollment and self-service management.

SSL VPNs were created to address the single-most significant cost associated with IPSec VPNs: client software installation, configuration, and update. Today, clientless SSL VPN access can meet the needs of many users, avoiding software administration altogether. However, some worry that SSL VPN thin clients simply require a different kind of software administration.

That might be true for some products, but not for all SSL VPNs. Thin clients and web frontends are evolving to reduce platform dependencies. SSL VPNs that do offer installable clients use portal page links to supply them. In most cases, portals just launch the best thin client automatically, eliminating user involvement or guesswork. Downloading thin clients and web frontends as needed means the latest version is always used. And there are no client configuration updates; policy is applied at the gateway for each session. SSL VPNs can even offer self-service web interfaces for user-directed changes, like updating passwords or customizing portal shortcuts. In short, SSL VPNs not only bypass the cost of installed clients – the browser paradigm reduces total cost of administration.

Conclusion

Clearly, SSL VPNs have come a long way over the past few years. New SSL VPN gateways can do considerably more than their predecessors, at a lower total cost of ownership. However, product capabilities do vary – shop carefully and select a solution that meets your own business needs. To learn about the WatchGuard® SSL 100, visit www.watchguard.com or contact you reseller.

About the WatchGuard® SSL 100

The WatchGuard® SSL 100 appliance is the ideal solution for small to mid-size business networks that need easy-to-use, secure remote access at a great price. The beauty of this appliance is its flexibility. You can make your SSL deployment as simple or as sophisticated as your business needs require.

- Small businesses looking for extreme ease of use can have access to standard network resources remotely with virtually no management overhead.
- Businesses with more complex needs can choose a mix of tunnel and portal-based resources, provide tech support to remote desktops, and control access based on granular user/device criteria.

Other features of the WatchGuard SSL 100 include:

- An all-in-one appliance – just plug and play – with no additional software components to buy, install, or manage
- Client and clientless access – including Vista 32-bit and 64-bit support

- Easy access to essential corporate resources including email, web conferencing, and CRM from any web-enabled device with optional non-native applications, including SSH and RDP, delivered through a remote user's web browser for maximum productivity
- Comprehensive endpoint integrity checking ensures network protection by allowing organizations to configure and enforce endpoint compliance including checks for anti-virus, anti-spyware, firewall software, and many other device attributes
- Session clean up removes all traces of access from the endpoint – including file deletion and cache cleaning – to prevent data leakage through another user's covert re-entry to network resources
- Local and third party authentication support, including strong authentication, ensures only authorized users can access the network, keeping intruders out
- Consolidated auditing collects all information about access, identity, and system events in a central repository for quick insight into user and system-based activities
- IT administrators can integrate solution with existing third-party authentication solution, such as Microsoft Active Directory, or rely on onboard LDAP server to configure local authentication, as well as use built-in two-factor authentication including SMS-based tokens and web keypad for identity validation

WatchGuard SSL 100 allows you to deliver exactly the level of remote access your business needs, at a price you can afford. For more information about the WatchGuard SSL 100 appliance, visit www.watchguard.com/ssl.

About The Author

Lisa Phifer is President of Core Competence Inc. (www.corecom.com), a consulting firm focused on business use of emerging network and security technologies. At Core Competence, Lisa draws upon her 27 years of network design, implementation, and testing experience to advise companies large and small regarding network security best practices to manage risk and meet business needs. She teaches and writes extensively about a wide range of technologies, from wireless/mobile security to virtual private networking and network access control.

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:
www.watchguard.com

U.S. SALES:
1.800.734.9905

INTERNATIONAL SALES:
+1.206.613.0895

ABOUT WATCHGUARD
Since 1996, WatchGuard has been building award-winning unified threat management (UTM) network security solutions that combine firewall, VPN and security services to protect networks and the businesses they power. We recently launched the next generation: extensible threat management (XTM) solutions featuring reliable, all-in-one security, scaled and priced to meet the unique security needs of every enterprise. Our products are backed by 15,000 partners representing WatchGuard in 120 countries. More than a half million signature red WatchGuard security appliances have already been deployed worldwide in industries including retail, education, and healthcare. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America.