



# The Move to SSL VPNs

Whitepaper

## Table of Content

Overview .....	3
Evolution .....	3
Dial-Up .....	3
IPSec VPNs .....	4
SSL-Access .....	4
SSL-VPNs .....	5
To be or not to be, is that the Question?.....	6
Network Provisioning or Application Provisioning .....	6
Clientless or Client Control .....	6
Secure Authentication is Success-factor for Remote Access.....	7
Business Drivers for SSL-VPNs .....	8
Return On Investment .....	8
Market Forecast.....	8
PortWise defines the SSL-VPN evolution .....	8

---

### Disclaimer of Warranty

PortWise AB makes no representations or warranties, either expressed or implied, by or with respect to anything in this document, and shall not be liable for any implied warranties of merchantability or fitness for a particular purpose or for any indirect, special, or consequential damages.

Copyright © 2004 PortWise AB. All rights reserved.

GOVERNMENT RIGHTS LEGEND: Use, duplication or disclosure by the U.S. Government is subject to restrictions set forth in the applicable PortWise AB license agreement and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013(c)(1)(ii) (Oct 1988), FAR 12.212(a) (1995), FAR 52.227-19, or FAR 52.227-14, as applicable.

PortWise and PortWise AB's products are trademarks of PortWise AB. References to other companies and their products use trademarks owned by the respective companies and are for reference purpose only.

# The Move to SSL VPNs

**Few new technologies within the security arena have received as much attention over the last year as SSL VPN. A multitude of companies are starting to discover its potential, thanks to visionaries such as PortWise.**

Industry experts are positive about the technology and IT-managers are following market advancement getting ready to ramp up for large deployments. This whitepaper focuses on the development of the remote access market and the advancement towards SSL-based VPNs.

For more product specific information, please read our product descriptions found on our website ([www.portwise.com](http://www.portwise.com)).

## Evolution

It has long been acknowledged that access to corporate resources for remote employees is a critical productivity-enhancer for companies. The last few years have seen several approaches to enabling remote access and the evolution towards less costly and more generic solutions has been relentless over the last years. The section below describes the evolution up-to-date. It is not unrealistic to assume that SSL VPNs will change the evolution of remote access solutions, since they meet all of the requirements that the enterprises currently demand. The future of remote access solutions will lie in fine tuning existing technologies.

### Dial-Up

The first widely deployed method for employees to access corporate resources was using dial-up. Using a modem and a phone-line, employees dialed a modem pool RAS (Remote Access Server) placed in the corporate network. Encryption was never an issue since traffic was transported over the fairly well protected and secure PSDN network (as opposed to the Internet).

The drawback of this approach was cost. Managing and operating the modem pool in-house became costly. A phone-line was needed for every concurrent user, which increased costs - especially since the IT staff had to compensate for peaks in the traffic.

Consequently, these services started to be outsourced, letting off the burden from the IT department to operate it. Under this new model, the RAS was operated by another company (similar to an ISP) and they could provide access to internal resources.

Some problems still remained. Users that needed to access the corporate on business trips were faced with very expensive phone calls from hotel rooms when dialing long distance or international back to the modem pool. Also, users that attempted to connect from a customer's office often had to struggle to find an analogue phone-line to connect through. Finally, as more and more employees invested in broadband connections such as DSL at home, solutions supporting high bandwidths, IP-based access forms were needed.

Benefits	Drawbacks
<ul style="list-style-type: none"> <li>▶ Security (no communication over the Internet)</li> <li>▶ No encryption of data needed</li> </ul>	<ul style="list-style-type: none"> <li>▶ High TCO, high variable costs (phone lines) and expensive to manage</li> <li>▶ Not compatible with broadband connections</li> <li>▶ Problems connecting through digital phone lines (common in office buildings)</li> </ul>

## IPSec VPNs

The cost of deploying and managing modem pools compelled corporations to look for other options. More precisely, corporation started to look at the potential of the Internet, which first had been judged as an insecure unreliable media, but was now seen as the only serious alternative. Many ISPs offered Internet Access either through ordinary dial-up but later also through broadband and DSL. However, the Internet had its drawbacks, and security became a great issue for the first time. This led to the development of IPSec VPNs.

IPSec VPNs uses the robust, yet complex, IPSec protocol to secure traffic over the Internet (or any IP-network). A VPN concentrator is used to terminate the different connections, and a single concentrator can terminate many different connections.

IPSec was initially developed to connect different branch offices to headquarters. It was necessary for a VPN concentrator to be placed in every office. Likewise, smaller concentrators could be placed in employees' homes to enable connection to corporate resources.

However, the latter deployment was however quickly shown to be a very difficult and expensive solution for employee access. The answer was to turn the client PC into a concentrator. The user could then connect from anywhere and be able to secure their communication to the corporate network.

IPSec provided what was required for the big rollouts as far as security was concerned. VPN client software was installed and configured onto all of the PCs. The only problem was the user. The VPN clients were too complicated to use (or too easy to misconfigure) and consequently, the support cost for these solutions proved to be very high.

There were also other problems with IPSec. The protocol is often blocked by corporate firewalls, which means that employees working at client sites are never guaranteed access. Likewise, IPSec has traditionally performed badly at traversing NATs (common in residential gateways), and some vendors have had to develop proprietary protocol extensions to solve this.

IPSec deployments have normally been configured to let the users have equal access if they work remotely as from inside the enterprise. However, this means that an intruder only has to compromise a single client PC to gain access to all business systems.

These issues lead to frustration and the IT departments started to look for new solutions.

Benefits	Drawbacks
<ul style="list-style-type: none"> <li>▶ Security - IPSec is regarded as a very mature and secure protocol</li> <li>▶ Less expensive than dial-up (TCO)</li> <li>▶ Low-cost connectivity regardless of geographic distance</li> <li>▶ Compatible with broadband connectivity</li> </ul>	<ul style="list-style-type: none"> <li>▶ Frustration over client support costs</li> <li>▶ Is usually blocked by firewalls</li> <li>▶ Does not handle NAT-traversal</li> <li>▶ Impossible to use for partner provisioning</li> <li>▶ Gives too much access</li> </ul>

## SSL-Access

The experience of IPSec VPNs (or L2TP and PPTP), made the requirements for the next generation of solutions obvious. Any future evolution can not require any client software to be preinstalled on the PC (apart from a standard web-browser), and access should only be given to certain applications that users need to access remotely. To address these issues, enterprises started to publish some of their internal resources on external servers. By redesigning the applications, they could be secured by SSL.

However, it soon became clear that redesigning applications demanded a lot of effort, and numerous applications dictate the need for a generic solution which does NOT require any changes in the existing application.

Benefits	Drawbacks
<ul style="list-style-type: none"> <li>▶ Security - SSL is very reliable and all the implementations has been widely tested (in browsers)</li> <li>▶ Lower support costs</li> <li>▶ Low-cost connectivity regardless of geographic distance</li> <li>▶ Compatible with broadband connectivity</li> <li>▶ Seldom blocked by firewalls</li> </ul>	<ul style="list-style-type: none"> <li>▶ Very expensive to redesign internal systems</li> </ul>

### SSL-VPNs

The SSL-VPN products that are making their way into the market today solve the problems seen in the early days of SSL. The technology still utilizes the embedded security features in web-browsers, therefore no additional software needs to be installed in the PC. The application requires no adaptations, since a new SSL-VPN concentrator is placed as a proxy in front of the applications. The deployment cost is slim to none.

Many organizations are transitioning towards these solutions, primarily due to the cost benefits. There are currently several vendors offering solutions with differing levels of complexity, and PortWise is one of the market-leaders.

The drawbacks with the early versions of SSL based VPNs was the limitation of access to http-based applications only. It was possible to access everything that provided a web-interface, but other services were excluded. The excluded services included Exchange servers, Citrix servers and Microsoft Terminal Servers, popular applications which made it clear that these needed to be supported.

The latest advancement in the SSL VPN area is utilizing SSL technology to create a secure tunnel into the corporate network, making it possible to transport any TCP or UDP traffic (this covers literally all modern office applications).

This is the same approach as the legacy VPN solutions have used, but with one major difference. In PortWise's solution the client application needed to create the tunnel is downloaded upon request. It is a Java applet and is only 10 Kbytes in size – making it very quick to download. It is also preconfigured which diminishes the risk of users misconfiguring it. This solution is the ultimate solution for secure remote access.

Benefits	Drawbacks
<ul style="list-style-type: none"> <li>▶ Security - SSL is very reliable and all the implementations has been widely tested (in browsers)</li> <li>▶ Lower support costs</li> <li>▶ Low-cost connectivity regardless of geographic distance</li> <li>▶ Compatible with broadband connectivity</li> <li>▶ Seldom blocked by firewalls</li> <li>▶ No need to redevelop applications</li> <li>▶ Ideal to provision partners to specific applications</li> </ul>	<ul style="list-style-type: none"> <li>▶ Less control of the client since no client software is installed. However, it is overcome by client security assessment done at every login to ensure certain applications (like virus scans) are installed.</li> </ul>

## To be or not to be, is that the Question?

In the previous section, we discussed the evolution of SSL-VPNs. The typical dilemma that an IT administrator will face is whether to implement an IPsec VPN or an SSL-based solution.

Although we have highlighted the clear advantages of SSL, both as a solution and a technology, the world is never black or white. SSL will solve most of enterprises remote access needs, but not all. There are still users and organizations that are ready to bear the increased cost burden associated with VPNs in order to receive some of the particular features.

PortWise agrees with many of the leading analysts firms which state that SSL-VPNs will dominate the market in a couple of years, but never completely exclude the IPsec-technology. Below we have listed and discussed what we believe is important to take into consideration when selecting a mobile access technology and products.

### ***Network Provisioning or Application Provisioning***

Traditionally, legacy IPsec-VPN solutions have been used to open a tunnel to the corporate network. Unless dedicated policies and rules are applied, the tunnel gives access to the complete corporate network, just as if the user was working in-house.

For a remote access solution, this is often regarded as too risky. The network is exposed to a considerable threat if someone manages to compromise the client computer. Access is then granted not only to a certain application, but to the whole network. Viruses are easily spread and an intruder can gain complete access and consequently create serious damage.

In networking language this could be referred to as network provisioning. A user receives access to a network and all the included servers, rather than an application. The opposite is application provisioning, the method adopted by PortWise. Instead of giving users access to complete networks or subnets, a user receives access only to applications they need to access and are supposed to use.

The benefit with application provisioning lies first and foremost in security. User access is restricted to a certain number of explicitly chosen applications and a specified protocol. As mentioned above, with network provisioning the user receives access to the whole network and all included servers.

Obviously, this is not a security threat as long as honest employees are accessing the network. But by the nature of remote access, the client computer could be compromised by someone else. In that situation it does become a great security threat.

Another benefit with application provisioning is that its more user friendly, the user does not need to search through the entire network to find the appropriate application.

Application provisioning ensures that users only have access to the applications they need. PortWise also enables application provisioning depending on how strong an authentication method is. For certain applications, a user has to authenticate with a two-factor method but for others a username and password is enough. This way the remote access solution can be adapted to the corporate security policies in a dynamic and flexible way.

### ***Clientless or Client Control***

The need for client software is a critical part of IPsec VPNs. SSL-VPN vendors argue that relying a built-in personal firewall and virus protection is the perfect solution and saves administration costs. Traditional IPsec vendors argue that a required client increases control of the client machine. The perfect solution is

somewhere in the middle; customers will always have different needs and requirements, therefore both solutions will co-exist in a foreseeable future. Below, we have included a detailed description of the pros and cons of both technologies.

The traditional view that an IPSec-client increases client control is not disputed. The question one should ask is, what client control is and what is the purpose for it. For most people it means that IT department only control the PCs and have certain applications installed (such as personal firewall and virus scans) which are allowed to connect on the network. The threat is that an individual PC could be infected with a virus, or compromised by an intruder, and spread over the entire network. This threat is valid for IPSec solutions since the connectivity is done on a network layer (see section above). For SSL VPNs, no viruses can be spread in the same manner (as there is no network layer connectivity), and an intruder would not be able to access anything other than the provisioned applications. Some SSL vendors are however able to perform checks on the client machine for specific software or certificates to make sure the machine conforms to corporate IT-standards before granting access. Also, most SSL VPN products are able to grant different access based on what device is used (controlled or uncontrolled). This could be achieved with client certificates, for example. The conclusion is that SSL VPN can achieve the a client security level in parity with the security level brought by an IPSec client solution.

SSL technology makes it possible for users to be more mobile and more productive. A user can access his mail and selected options from any machine, without any risk of network vulnerabilities. The fact that the solution is clientless increase cost savings in terms of support and maintenance for the IT department. For partner or customer access to applications, SSL-VPN is the only choice, because it is impossible to enforce client installations on a remote machine.

Finally, there are some applications that are not supported by SSL VPN solutions. Applications that are not based on TCP or UDP are typically not supported. One example is the well known Ping command daily used by many IT-administrators. Therefore, it is likely to assume that some smaller fractions of the enterprises user groups will still be using IPSec solutions. This fraction is however small and usually competent usersbase that will not suffer from the configuration and installation problems that a mass-installation of IPSec clients will generate.

In summary, it is understandable that the industry and analyst firms are predicting a bright future for SSL-based VPNs. There are, however, reasons why some enterprises will continue to use IPSec for all or part of their employees. The future will be diversified.

## Secure Authentication is Success-factor for Remote Access

Any product or technology is only as strong as its weakest link. This old saying is also true for a security solution. There is no point in enforcing strong encryptions if the user is not securely authenticated.

Therefore, all SSL-based VPN solutions have to be supported by robust authentication methods. For strong authentication, people usually refer to one-time passwords and two-factor authentication methods. In most cases these methods are based on a piece of hardware, used to generate One-Time Passwords.

With SSL-VPNs, the user is not required to have a particular computer, it would therefore be wise for the authentication method not to require a dedicated hardware. PortWise provides an authentication server which focuses on providing innovative methods for user authentication. PortWise's methods utilizes the user's cellular phone for either SMS transmitted One-Time Password (OTP) or to install a user-unique software-based OTP-generator. The cellular phone is less frequently lost and something the user remembers to bring with them. This way corporations can save both time and money, since maintenance of broken or lost tokens is no longer needed.

## Business Drivers for SSL-VPNs

Despite all of the different aspects on the technology and the market presented above, there are other clear measures of the future for the SSL technology. One is looking at ROI for an SSL-installation in comparison with an IPSec installation. In today's tough economic climate, a positive ROI is a prerequisite for a technology investment. Another way is to study analyst opinions, because they have an excellent understanding of the market trends and demands.

### **Return on Investment**

There is one major cost benefit with SSL solutions over IPSec – there is no need for a VPN client software on the remote PC.

A client not only cost money, but it is also expensive to install, manage and distribute. Yankee Group estimates the cost of managing and owning an IPSec solution at 360 USD per user, per year. The same estimate for an SSL solution according to Yankee is 240 USD per user, per year. To invest in an SSL VPN solution, according to these figures, is paid back in less than one year.

### **Market Forecast**

All of the leading analyst firms have been studying the SSL VPN market to better understand its potential. Below is a quote from Gartner.

#### **Gartner**

*"Bottom Line: The simplicity and portability of Secure Sockets Layer Virtual Private networks (SSL VPN) can lower the cost to implement remote-user VPNs for corporate workstations, as well as access from non corporate systems such as personal computers. Where traditional VPNs are not required, enterprises should expect immediate value from investments in SSL VPNs in the form of easier deployment and support."*<sup>1</sup>

In figures Garner estimates that SSL VPNs will account for 95 percent of all remote access solutions by 2007.

#### **Frost & Sullivan**

The American analyst firm Frost & Sullivan predicts that the SSL-VPN market will grow heavily in the next years. By 2008 the market is worth over 1000 million USD.

## PortWise defines the SSL-VPN evolution

As with all new markets, there are a lot of entrants. The number of players in the SSL VPN market is reaching well above 20. For a typical IT department it is hard to get an understanding of the products' diverse capabilities and maturity.

PortWise has been developing SSL-VPNs since 1997, and has the most mature product on the market. Thanks to our extensive market experience and numerous blue chip customer installations, including some of the world's largest SSL VPN implementations, we have been successful in building an unbeatable feature-set in our products.

Through our creative development team and dedication to the SSL VPN marketplace we are certain to continue defining the future of strong authentication and SSL VPN.

**If you would like to know more about our products and how PortWise could make your business run more smoothly, please e-mail us at [sales@portwise.com](mailto:sales@portwise.com) or visit our homepage [www.portwise.com](http://www.portwise.com)**