

STRATEGY & PLANNING

Info-Tech Advisor Premium - Strategize



About this research note:

Strategy & Planning notes define the critical decisions and actions surrounding successful adoption of a specific technology, tool, or process.

Realize the Cost Savings and Benefits of SSL VPNs

Publish Date: June 22, 2007

Enterprises that need to provide secure network connectivity for remote employees, guests, partners, and contractors should evaluate SSL VPN solutions. For new VPN remote access deployments, or upgrading existing IPSec or PPTP VPN implementations, SSL VPN technology provides the most attractive TCO of all currently available remote access solutions.

INFO~TECH
research group

Passionate About Research.

Driven By Results.

www.infotech.com

© 1998-2007 Info-Tech Research Group



Executive Summary

Whether implementing a new remote connectivity solution, upgrading or augmenting an existing VPN implementation, most enterprises will find that SSL VPNs offer the lowest TCO, highest security, and the easiest administration. While an SSL VPN deployment is not the best fit for all usage scenarios, it is the most appropriate solution for the vast majority of enterprises with remote connectivity requirements. This research note focuses on the following aspects of SSL VPN solutions:

- » Enterprises and users best suited for an SSL VPN deployment.
- » Operational and security benefits of an SSL VPN implementation.
- » TCO and ROI considerations.

When evaluating remote connectivity solutions, enterprises seeking to provide secure, simplified access at the lowest TCO should consider an SSL VPN solution.



Planning Point

Many enterprises have defined remote access for employees, guests, partners, and contractors as a business necessity. The challenge for IT is to implement a solution that is scalable, secure, easy to use, and easy to manage at a cost that is palatable to the business. SSL VPN technology largely addresses these issues, allowing IT departments to provide secure, clientless browser-based access to only the network resources and applications that users need.

The most significant tangible benefits of an SSL VPN include simplified administration and management, and reduced support requirements. However, less quantifiable benefits in the form of improved security and user productivity should be considered in a financial analysis wherever possible. Enterprises with minimal remote connectivity requirements will likely be served sufficiently with existing IPsec or PPTP VPN implementations, but those that need to service more than 20 remote users are good candidates to benefit from SSL VPN technology.

Key Considerations

Assess Enterprise and User Requirements

Not every enterprise needs, or will benefit from an SSL VPN deployment. For instance, businesses that support less than 20 VPN connections for IT staff and power users will not likely reap any significant cost savings. However, even smaller shops that must support less tech-savvy users, guests, partners, and contractors will benefit from the added security that SSL VPN products offer in the form of Network Access Control (NAC), strong encryption, and granular access control.

The Info-Tech research note [“SSL VPNs Provide Flexibility, Security, and Simplified Management”](#) provides more insight into how SSL VPNs function in contrast to IPsec and PPTP, and the most appropriate use case scenarios. The most compelling functions of an SSL VPN are reduced management and administrative burden, flexible policy creation and granular application access, and enhanced security features including Network Access Control (NAC).



Operational and Security Benefits

The management and administration of an SSL VPN infrastructure is typically much less cumbersome than the alternatives. Installing a client on the end user device is time consuming, and makes troubleshooting more complex. Because SSL VPNs are clientless, there is a considerable time and cost saving in provisioning new users. Network administrators simply add users in the SSL VPN appliance/server and grant them permissions to the required applications and network resources. Users simply use their existing Web browser to access these resources.

Calls to the help desk from remote users will be reduced with an SSL VPN. Most end users are very comfortable operating a browser, and because the browser is the client in an SSL VPN deployment, users are less likely to have problems. When there is a problem, troubleshooting is simplified because help desk staff do not have to troubleshoot a client they cannot see on the remote user's device.

The average end user is likely to be more productive using an SSL VPN because all of the applications and network resources they require are on a single portal Web page – one that is customized for each user or group of users. A simple click on a hyperlink on the Web page will take the user to a network share, the CRM application, office productivity suites, or any other network resource or application. Everything the user needs access to is on one page, greatly simplifying the end user experience.

Business continuity is another key benefit of implementing an SSL VPN. In the event of a disaster, pandemic or other business interruption, users can very quickly and easily be setup to work from home. Simply direct users to the secure SSL VPN URL and provide them with a username and password, with no requirement to install client software on the device. In fact, many SSL VPN vendors provide licensing options specifically for this situation.

The security benefits of an SSL VPN implementation can be significant. Aside from very granular access control, SSL VPNs provide encrypted authentication or two-factor authentication, strong data encryption, browser cache cleansing at the end of a session, and NAC – including endpoint inspection and forced remediation. Some SSL VPN products are truly fully featured security and NAC devices as well. Considering what many enterprises are paying to implement NAC solutions today, the benefits providing secure remote access with NAC are compelling from a cost perspective.



TCO and ROI Considerations

Based on the benefits outlined above, SSL VPNs can reduce TCO and provide attractive ROI for many enterprises. Some of the benefits related to security and productivity are difficult to quantify, but some of the operational benefits can be brought down to hard numbers. The table below provides direction on where to look for hard and soft costs and benefits.

| Cost/Benefit | SSL VPN | IPSec/PPTP VPN |
|-----------------------------|---|---|
| Initial cost | Typically \$45-\$90 per user. | Limited number of users usually included in cost of firewall, additional licenses \$25-\$50. |
| Provisioning new users | Required on the server side only – once initial groups and policies are defined a new user can be provisioned in 5-10 minutes by the help desk. Assuming the fully loaded cost of a help desk employee is \$24/hr the cost to provision a new user is roughly \$2-\$4. | Configuration required on VPN concentrator as well as client device. A software client must be installed in many cases. Typically a 30 minute job per user. This may require a more skilled resource to provision the VPN concentrator. Assuming the fully loaded cost of a second level help desk or network admin is \$35/hr the cost to provision a new user is roughly \$17.50. |
| Support and troubleshooting | No client side application to troubleshoot. Most users are very comfortable with a browser. Assuming there are 10 VPN help desk calls per day and each lasts 20 minutes, if the number of calls is reduced by 50% and those calls are 50% shorter the theoretical cost savings would be \$60/day, or roughly \$15,600/year. | Using the figures in the column to the left, the cost of support and troubleshooting for IPSec/PPTP VPN infrastructure would be four times that of SSL VPN. |



| | | |
|--|--|---|
| Endpoint security and NAC | Consider the cost of a virus, worm, or Trojan wreaking havoc on the network and users. Downtime, IT staff time, lost productivity, loss of goodwill, etc. can cost tens of thousands of dollars. | A separate endpoint security/NAC solution would have to be implemented to mitigate the risk of exposure due to an infected or insecure endpoint. The cost would be \$45-\$90 per user and typically requires client side installation and/or configuration. |
| Improved productivity from internal and external users | Allows IT to provide access to internal applications to partners, contractors, or guests without opening the entire network. This can greatly improve productivity and efficiency for internal and external users. | Another solution would have to be implemented to allow limited access, such as Citrix. This would require a client install as well. |
| Business continuity | Contingency licensing is available from many vendors, allowing enterprises to pay for additional user licenses in the event of a situation that required many users to connect from remote locations. | Additional hardware is often necessary to accommodate a large increase in users. Every employee would also have to have a software client installed and configured on their home PCs. |

Recommendations

Whether the enterprise is considering providing remote access for the first time, or looking for options to augment or replace existing IPSec/PPTP VPN connectivity, SSL VPN is worth exploring. Use the Info-Tech Advisor Premium [“Cost/Benefit Analysis Tool”](#) to determine the TCO and ROI of an SSL VPN implementation, and consider the following:

1. **Prepare for the initial capital cost.** If the solution is being deployed in-house, there will be a capital cost for the VPN appliance(s) and licensing. The cost varies by number of users, but very small appliances start at under \$1,000 for 20 users, and exceed \$50,000 for appliances that support 1,000 users.



2. **Evaluate the time and effort spent with the current infrastructure.** In some cases larger enterprises may even be able to eliminate an FTE position by moving to an SSL VPN. Enterprises with more than 1,000 VPN users are likely to have at least the equivalent of an FTE maintaining and administering an IPSec/PPTP infrastructure.
3. **Consider the potential security benefits.** Think about the cost of current endpoint security or NAC point solutions currently in place. It's possible that the cost of these solutions can be recouped, and the management and administration eliminated. If there is no endpoint security solution in place, consider the costs of a security breach caused by an infected or insecure endpoint.

Bottom Line

Enterprises that need to provide secure network connectivity for remote employees, guests, partners, and contractors should evaluate SSL VPN solutions. For new VPN remote access deployments, or upgrading existing IPSec or PPTP VPN implementations, SSL VPN technology provides the most attractive TCO of all currently available remote access solutions.

Info-Tech provides IT research and advice to more than 21,000 IT professionals worldwide. Our practical, actionable research is specifically designed to have a clear and direct impact on your organization.

Info-Tech's products and services help our clients work faster and more effectively. Our research improves the IT decision-making process, expedites critical IT projects, and helps our clients keep current – enabling them to achieve greater personal and corporate success.

[More About Info-Tech](#)

