

White Paper

SSL VPN Decision Guide for Small to Medium Sized Enterprises

Roslyn Rissler
Director, Product Marketing



Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

Part Number: 200092-003
January 2006

Contents

An Overview of the SME Market	3
Remote Access Trends.....	3
Total Cost of Ownership – Purchase Price Plus Usability and Maintenance	4
Security	5
Access Ubiquity	5
Remote Access Solution Criteria	5
Functional Requirements.....	5
Total Cost of Ownership Considerations	6
Security.....	6
Scalability.....	6
Ubiquity.....	6
Introduction to SSL VPNs	6
SSL VPNs for the SME	7
Functional Requirements.....	7
Total Cost of Ownership Considerations	8
Security.....	9
Scalability.....	9
Ubiquity.....	10
Conclusions.....	10

An Overview of the SME Market

Small and medium-sized enterprises are one of the fastest growing segments in today's global economy. Any discussion of this market should begin by establishing the size of company being discussed. Although definitions vary, for the purposes of this paper we will define this segment as companies with more than 25 employees and less than 250.

Although these organizations may be small when seen as individual companies, they have tremendous aggregate power, both economically and politically. SMEs provide more than 60 percent of new jobs in the United States in 2005. In the European Union alone, they employ more than 74 million people. The emergence of the SME is supported in every region, from the Small Business Administration in the U.S. to the Organization for Economic Development in Europe to the Asia Pacific Economic Cooperation.

The growth of the global SME market is a natural offshoot of two phenomena – the emergence of a knowledge-based economy, and the ability of a broad audience to utilize the Internet for communications and access.

The use of computers and other automation makes it possible for smaller firms to compete in specialized areas where only large companies were previously viable. Moreover, smaller companies can be reactive to the changing business climate, and effectively take advantage of a change-driven operational style. This requires flexibility and agility to optimize every change in the global marketplace, with swift development, production and service. Because SMEs are not hampered by the organizational infrastructure of larger firms, they are able to react quickly to exploit changing business needs.

Today's SME drives agility with information technology. All SMB market CAGRs in North America will outpace worldwide markets, as a whole. Gone are the days when access to technology was the problem. The difference is in technology use -- less successful firms are not fully realizing the potential of the technology they already have.

Remote Access Trends

The other driving trend is the emergence of the Internet. Information-gathering was a function of time and resources – today, a wealth of information is available to anyone with an Internet connection, which levels the playing field. Real time communication with suppliers, customers, and remote or mobile employees used to be the exclusive domain of larger firms, using staff time, leased lines, or dial-up connections. Now companies of all sizes can take advantage of the Internet for connectivity, using Virtual Private Networks, or VPNs. A VPN is defined as a means to use a public network, such as the Internet, to send and receive private data, such as that found on the LAN. Today's VPNs provide site-to-site connections as well as access to remote or mobile users. The market for site-to-site connectivity has been well served by network-layer or IPSec VPNs, which were designed to handle this type of connection. The more complex challenge, particularly for the SME, is the varied and dynamic access requirements of remote or mobile employees whose ranks are growing rapidly for companies of all sizes.

According to Infonetics (3Q05) most companies offer remote access to only a small portion of their employees (typically less than 20%), because it is expensive to install and maintain; Infonetics estimates that by 2008 the technology will cause many companies to offer remote access to a broader set of employees, possibly bumping the average from 20% or less to over 50%.

"IDC estimates that by the end of 2003, there were roughly 8.9 million telecommuters in the United States - people who work at home three or more days a month," says Merle Sandler, senior research analyst in the Home Office program at IDC. SMEs, in particular, show growth in this area. According to Infonetics Research, "In 2002, 24% of small, 37% of medium, and 60% of large organizations had deployed remote access VPNs; by 2007 the numbers are 55%, 74%, and 90%." These statistics show the overall market in small and medium-sized businesses more than doubling over five years' time. However the remote access solutions that work well in larger companies are not always an immediate fit for most SMEs because of concerns about cost, ease of use, and day-to-day maintenance.

Total Cost of Ownership – Purchase Price Plus Usability and Maintenance

Issues around device purchase price by themselves are relatively easy to resolve. Leading analysts firms say that the sub-\$5000 price point is ideal for secure remote access solutions for the SME market segment. However, this presumes that purchase costs are the only consideration for a remote access solution, and that the product used has no associated deployment or ongoing maintenance costs. This is not a correct assumption for all IPSec VPNs when those products are used for remote user connections. A recent edition of Network World cited a reader who strongly supports the use of IPSec for connecting offices, saying "... site-to-site VPNs required nothing from technically untrained end users." This is because when an IPSec VPN is used to connect site to site, the connection is handled between the remote office gateway and the corporate LAN gateway, and is completely transparent to the user. The reader goes on to talk about using the same technology to connect remote users, saying, "The problems we have encountered invariably arose from trying to connect non-technical remote users with client software. The cost of installing the client software, teaching the user how it worked, maintaining dropped connections, etc., became more trouble than it was worth."

According to Network Computing Asia (July 2004 issue), "Cost efficiency is as much an imperative for small businesses as it is for large ones, but unlike a large enterprise, an SME rarely has the technical infrastructure required to support mobile operations. Consider the simple issue of running a messaging or collaboration server which mobile employees can access. A large enterprise simply puts the server in a glass house where it is run by trained IT operations staff, and provides secure access to it for the mobile employees. An SME does not have the same luxury. At least some of the solutions which a large business might routinely use to support mobile operations do not scale down to the SME very well. An SME going mobile has to go about supporting mobile operations a little differently."

Even as today's small business becomes increasingly tech savvy – relying on computers to connect with customers, track inventory, or manage books – many cannot justify in-house IT support. Such staffing is required to deploy, install, and configure an IPSec VPN for remote access. Desktop support must be available to work with mobile users in case of problems, including Network Address Translation issues and firewall or proxy traversal problems. Additional maintenance is required in cases where an updated VPN client must be delivered to remote users. This is typically the case when there are changes to the underlying network topology, changes to the client operating system, or changes to the client software itself. And each new user in the organization increases the support burden. The result is that many SMEs feel that they do not have sufficient IT staff to manage IPSec VPNs.

Security

Still another important consideration is security. An open IPSec VPN tunnel is also a path into the corporate LAN. The tunnel itself is encrypted and secure, but that security is rendered meaningless if one end of the connection is open to the outside world. Clearly in the case of a site-to-site connection it is reasonable to assume that the VPN connection is between two known entities, but this is not the case with remote users tunneling into the LAN. Concerns about the security of network-layer VPNs used for remote access originally centered on information being removed from the LAN. Today's security concerns center around what can come in through the tunnel, taking advantage of VPN sessions that are often left open by users.

Security becomes a huge issue for the SME, if it is assumed that these companies may not have in-house IT. Smaller companies may feel that they would not be a target of a concentrated attack, yet many of today's worst threats are propagated by the Internet without being targeted at all. Complex viruses, Trojans and worms, such as CodeRed or Nimda, can come from anywhere. Meanwhile, larger companies are using their security staff to lock down their enterprise, making smaller companies an easier target. And unlike large companies, even a small security breach can ruin a smaller business. According to Microsoft, on average, small businesses respond to six security incidents per year – and spend 20 percent of their IT budgets on security. This is a significant amount of resources to spend on security for a small business. If the SME cannot afford to hire in-house security staff, they must be certain that safeguards are part and parcel of any remote access solution they choose.

Access Ubiquity

Another important consideration of remote access is the individual that needs access to resources from a device other than a company-managed laptop or PC. This is particularly vital in the case of the SME, where all employees may not have a managed device from which to connect. In addition, as workforce mobility increases, so too does the need to get access from a variety of different endpoints, some of which, like Internet cafes or airport kiosks, are completely unmanaged, public devices. One of the drawbacks of traditional IPSec solutions in this instance is that access can only be provided from a device that has the VPN client software resident on it. This can effectively deny access to any employee that does not have a managed PC, or have access to it at that moment. This can be significant in cases such as access needs while at a client site, during travel, as well as for disaster recovery scenarios.

Remote Access Solution Criteria

In order to evaluate a remote access solution, the SME should consider the following subsections of concern – functional requirements, that is, will the solution connect users to the resources they need; total cost of ownership, including initial purchase, setup, maintenance, and growth; security, including the end user, the data and the internal servers; scalability of the solution for the future; as well as ubiquity of the solution.

Functional Requirements

- Should solve the specific problem the SME is purchasing it to solve
- Must be able to work with all applications used by the SME

- End user experience should be comprehensible by non-technical employees
- Should require minimal network reconfiguration

Total Cost of Ownership Considerations

- Purchase price
- Day-to-day maintenance
- End user training
- User support (helpdesk)
- Cost in hours, hardware, and software of providing remote access for new employees
- Cost in downtime

Security

- Must have a means to encrypt data in transit
- Should integrate with policy enforcement, particularly on the client-side and provide robust endpoint security for managed and unmanaged devices
- Must leverage any investment already made in security, such as use of an authentication server, or deployment of security policies or applications
- Should in itself provide extra security for the network and should be secure enough to be placed in the DMZ facing the public network
- Should be audited by third parties

Scalability

- Must meet the SMEs remote access needs today
- Should be able to meet the SMEs remote access needs in the future

Ubiquity

- Should be able to provide access from any PC, anywhere
- Administrator-controlled access should be variable by user and by session, for maximum control

Introduction to SSL VPNs

SSL VPNs take advantage not only of the Internet, but of certain protocols intrinsic to its use, specifically Secure Sockets Layer, or SSL. SSL was originally created for use in securing online financial transactions and is one of the foundations of Web commerce. SSL is part of all standard Web browsers, so the client software that initiates secure data transit is already on the end user's device. Instead of relying upon the end user to have a configured client on a company laptop, SSL VPNs use SSL /HTTPS, available without additional downloads on all standard Web browsers, as a secure transport mechanism. The "tunnel" between the end user and the LAN happens at the application-layer, not the network layer. The use of SSL

solves a variety of problems associated with IPSec VPNs, including:

- SSL does not need to be installed.
- SSL does not need to be configured.
- SSL is available in standard Web browsers, so users can gain access via just a web browser.
- SSL is an application layer protocol, not a network layer protocol, so it can provide better visibility and more granular control
- SSL has no NAT or firewall traversal issues.
- SSL is familiar to most users, even those without a technical background (e.g. used every time you buy a book in Amazon).

The result is that leading analysts have predicted that 80% of remote access will take place over SSL by 2007.

It must also be said that all SSL VPNs are not the same – in fact, the use of SSL as a secure transport mechanism is sometimes the only thing that these solutions actually have in common. While the actual definition may be correct, however, the commonality of the transport is much less important than the way each vendor's solutions work. SSL VPN solutions should be examined under the same strictures as any other remote access solution would be considered.

SSL VPNs for the SME

Juniper Networks offers a complete range of SSL VPN appliances designed to meet the needs of small, medium and large enterprises. The Juniper Networks Secure Access 700 (SA 700) is designed specifically for small to medium sized organizations. Here you can see how SSL VPNs from Juniper Networks stack up on the important SME criteria established earlier in this paper.

Functional Requirements

- **Should solve the specific problem the SME is purchasing it to solve**

IPSec VPNs have been used for years to provide remote access, when they were actually designed to provide site-to-site connections. The SA 700 was designed to provide secure access for remote or mobile employees, customers and partners of SMEs.

- **Should be designed for the SME**

The SA 700 was specifically designed for companies with less than 250 employees. This design is reflected in the price point for the appliance.

- **Must be able to work with all applications used by the SME**

The SA 700 uses Network Connect as its primary access method, while Core Clientless access is also available as an optional upgrade. Juniper's Network Connect provides an adaptive dual mode network-layer access capability that detects the best method of connection between IPSec and SSL transport to ensure the highest level of connectivity resulting in greater reliability. Network Connect can be deployed via a lightweight dynamic download for all the benefits of an IPSec VPN, with none of the management overhead.

And because Network Connect is supported on multiple platforms, the SME is not limited in its choice of operating system.

The Core Clientless access method provides completely clientless access to select resources from any endpoint. The Core Clientless method provides secure access to Web-enabled applications, files, standards-based e-mail, and telnet/SSH sessions, as well as to applications containing complex Javascript, DHTML, VBScript, Flash, XML and more.

- **End user experience should be comprehensible by non-technical employees**

The SA 700 uses SSL, which is the global standard for financial transactions on the Web. Users don't need to have any technical knowledge to get access.

- **Should require minimal network reconfiguration**

The SA 700 is literally plug-n-play. It can be deployed in under 1 hour and requires no changes to network infrastructure. Most firewalls are configured to admit traffic from port 443, which is the port for SSL traffic, which eliminates the need for firewall configuration changes.

Total Cost of Ownership Considerations

- **Purchase price**

The SA 700 SSL VPN has a list price that can be easily accommodated by most SMEs. It also allows for growth from 10 concurrent users up to 25 concurrent users.

- **Day-to-day maintenance**

The SA 700 requires no day-to-day maintenance. New users and new applications can be added in just a few mouse clicks.

- **End user training**

Because the SA 700 uses a simple Web user interface and the SSL that most end users have employed, there is no training required for end users.

- **User support (helpdesk)**

Most end user support for IPSec VPNs is caused by availability issues, ISP compatibility problems, NAT issues, or firewall or proxy traversal problems. The SA 700 faces none of these problems.

- **Cost in hours, hardware, and software of adding a new remote employee**

This is any easy way for most enterprises to see the hidden costs of an IPSec VPN. The time and effort required to bring up each new user is a cost that cannot be leveraged over the deployment, and it's also a cost that the SA 700 does not share. Adding new users is as simple as adding their name, credentials, and access controls to the appliance or leveraging existing user directories.

- **Cost in downtime**

A sometimes hidden cost is the cost of a downtime due to either reliability or security issues. The SA 700 is a hardened appliance that was designed to face the public network and is being continuously audited by multiple third-part security outfits. In addition, by integrating best-in-class Malware protection it can help protect the network from downtime caused by attacks.

Security

- **Must have a means to encrypt data in transit**

IPSec and SSL both use strong encryption, and provide similar protections for data in transit.

- **Should integrate with policy enforcement, particularly on the client-side and provide robust endpoint security for managed and unmanaged devices**

Enforcing security policies is simple with the SA 700. The end user's device can be checked for security compliance before they are even allowed to present credentials to the SSL VPN (and therefore protect against a key stroke logger for example). The SA 700 also comes with integrated Malware protection to ensure that the endpoint is indeed secure. As a fully-enabled device of the Juniper Networks Secure Access product line, the SA 700 also leverages the Juniper Endpoint Defense Initiative, which features both client- and server-side APIs to facilitate the easy integration of best-of-breed third party security applications (e.g. Antivirus, Personal Firewall, Virtual Desktop, etc).

After the initial assessment the endpoint can be contained to a specific role based on the result and even remediated without helpdesk involvement. For example: you can have a policy that requires the latest antivirus signature before granting any access and then help the end user to download that signature without any need for helpdesk involvement.

The SA 700 is also fully compatible with all leading authentication methods and stores. Yet another level of policy enforcement can be configured at the resource itself.

- **Must leverage any investment already made in security, such as use of an authentication server, or deployment of security policies or applications**

The SA 700 has its own encrypted database for authentication information, or is seamlessly compatible with other leading methods, including dual factor authentication and X.509 digital client certificates, and with all the leading AAA servers (e.g LDAP, AD/NT, RADIUS, etc). It also provides API level integration with best-of-breed security vendors, to ensure that the enterprise has a consistent security posture, and provides non-compliant endpoints with a way to remediate.

- **Should in itself provide extra security for the network**

The SA 700 is based on the Juniper Networks Instant Virtual Extranet platform, which is a hardened, purpose-built platform that has passed stringent audits by leading third party security experts.

- **Should be audited by third parties**

SMEs usually do not have the in-house expertise and cannot afford to spend the resources on evaluating the security posture of every device. Therefore it is imperative to rely on third parties to provide that expertise. The Juniper Networks Secure Access platform has been continuously audited by third party security experts like CyberTrust (previously TruSecure), iSEC Partners as well as ICISA Labs and more.

Scalability

- **Must meet your remote access needs today and tomorrow**

Because the SA 700 is an application-layer device, and does not require the deployment, installation, configuration or maintenance of client software, adding users is easy. If you

want to add the capability of more simultaneous users, it requires just a simple upgrade to the software. No changes in hardware are required.

Ubiquity

- **Should be able to provide access from any PC, anywhere**

Core Clientless Access is available on any browser so it's really anytime, anywhere access.

- **Must be able to administer access by user and session for maximum control**

The SA700's comprehensive AAA framework combined with the two access methods (Core and NC) allow customers to provision granular access based on user and session.

Conclusions

The SME market is growing rapidly around the world, and coincides with the trend toward remote and mobile employees. Having a cost-effective, robust remote access solution is no longer a luxury – it is a business necessity. At the same time, these firms may not yet have an in-house IT staff, so the solution employed must be easy to install and manage. End users must be able to use the solution intuitively, without previous technical background or training.

SSL VPNs meet the needs of the SME very well, and have become the recommended approach of analysts, technical press, and end users. The Juniper Networks SA 700 SSL VPN provides the remote access solution that the SME has been looking for – simply, securely, and affordably.