

White Paper

VPN Decision Guide

IPSec or SSL VPN Decision Criteria

Roslyn Rissler
Director Product Marketing

Sarah Sorensen
Product Marketing Manager



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

Part Number: 350037-002 August 2005

Contents

The Secure Access Landscape	3
Network Layer IPSec VPNs.....	3
What Is An SSL VPN?	4
IPSec or SSL VPN?	5
Total Cost of Ownership	6
Security	6
Access to Network	7
Application Access	7
Access Management	7
Conclusion	8
Checklist.....	9
IT environment:.....	9
User constituency:.....	9
Client-side network and device:	9
Applications and content:	10

The Secure Access Landscape

Providing secure access to corporate resources has grown into a critical requirement for the enterprise, often making the difference between those companies that are successful and those that are not. Whether the user is working in a remote office or their hotel room, they need easy access to corporate resources to accomplish their job and maintain their productivity. In addition, corporate business partners and customers increasingly need real-time access to corporate resources and applications.

In the early 1990's, there were only limited options to extend the availability of the enterprise's network beyond the boundaries of the corporate central site, comprised mainly of extremely costly and inflexible private networks and leased lines. As the Internet grew, however, it spawned the concept of virtual private networks, or VPNs, as an alternative. Most of these solutions leveraged the free/public long-haul IP transport service and the proven IPSec protocol to provide a more flexible, cost-effective solution for secure access. IPSec VPNs effectively addressed the requirements for fixed, site-to-site network connectivity; however, for mobile users, they were often too costly, while for business partners or customers, they were impossible to deploy as they require software be installed and configured on each endpoint. It is in this environment that SSL VPNs were introduced, providing remote/mobile users, business partners and customers with the easy, secure access to corporate resources they needed. Together, IPSec and SSL VPNs enable enterprises to provide their offices and users secure, ubiquitous availability to the corporate network to support the overall success of the business.

This paper will look at how IPSec and SSL VPNs differ, and will examine the criteria to be considered in deciding which technology best fits each business need.

Network Layer IPSec VPNs

IPSec or network-layer VPNs can offer enterprises an easy, cost-effective way to route communications between sites, delivering high performance connectivity and resiliency to match the needs of the most demanding network environments. They were created as a low-cost transport alternative to private or leased lines, enabling enterprises to use the Internet infrastructure to quickly extend the private network across geographically distributed locations.

Technically, network-layer VPNs address the challenge of how to use the Internet (which uses the IP protocol only, and usually transmits text in the clear) as a transport for sensitive, multi-protocol traffic. Network-layer VPNs provide a combination of encryption and tunneling functions to meet these challenges. They use peer negotiation protocols, like IPSec, to encapsulate the data being transferred within an IP "wrapper" that will go over the Internet. This encapsulated data is received by the network-layer VPN gateway, "unwrapped," decrypted, and routed to the recipient. Traffic coming from the VPN gateway is handled as if it came from any user within the LAN itself. As a result, network-layer VPNs provide users the same, continuous access to the network that they would have if they were physically connected. This is ideal for facilitating regular communications and resource sharing among users at geographically separate offices to improve productivity enterprise-wide.

In certain instances, however, this level of access may be unnecessary or unfeasible. For example, mobile users that just need to check e-mail or retrieve certain documents from the Intranet don't need a dedicated pipeline to all the resources on the network. In addition, this

level of access could introduce security risks if the “end-point” that the user is coming from is insecure or easily compromised. Using an IPSec VPN in such an instance represents an open door to the LAN itself. A VPN that provides selective access control only to endpoints that meet corporate security policies, and can provide this control on a session-by-session basis is required to meet the needs of remote/mobile users, as the combination of endpoint and network attributes will change. For example, remote users coming from an untrusted network and/or unmanaged device such as those found in an Internet cafe should be restricted to appropriate applications and resources, not granted access to the corporate LAN as a whole. Likewise business partners may be allowed access to certain resources from an unmanaged device, but should not be granted LAN-wide connectivity.

Another factor to consider with IPSec VPNs is the level of management resources required for deployment and maintenance. All remote or mobile users not at an aggregation point must have client software on their remote PC. For organizations trying to provide remote access to hundreds or thousands of mobile users, deploying, updating, configuring and managing all of these clients can be very time consuming and costly. If remote partners or customers are considered, the difficulties are multiplied. While a necessary and appropriate investment for regional, branch and remote offices where the enterprise needs reliable, “always on” connectivity and only has to manage a few network VPN devices, IPSec clients are, in many ways, an impractical investment to meet the needs of mobile/remote workers, business partners or customers. For example, because VPN client software is required to connect remote users, those users are restricted to devices where the software is installed; i.e., corporate laptops. This does not accommodate additional methods of access, such as Internet kiosks, PDA’s, etc., that are often more convenient for the mobile user, nor does it include devices that the business partner or customer might use from within their own network.

It is into this environment that SSL VPNs entered, providing an easy-to-use solution for the mobile user, business partner, or customer that compliments the reliable, powerful communication infrastructure that IPSec VPNs offer for site-to-site connections.

What Is An SSL VPN?

The term SSL VPN is used to refer to a new and fast-growing product category comprised of a variety of technologies. To broadly define what products and technologies are within this category, one can begin with the term “VPN” itself. VPN, or Virtual Private Network, refers to the practice of using a public network like the Internet to transmit private data. Up until 2001, most in IT did not add a descriptor to VPN because almost all VPNs available at that time used some type of network-layer transport. The early standard in the VPN space was the IP Security Protocol (IPSec), although some vendors use other methods, including Layer 2 Tunneling Protocol (L2TP), and Point-to-Point Tunneling Protocol (PPTP).

SSL VPNs use a different methodology to transport private data across the public Internet. Instead of relying upon the end user to have a configured client on a company laptop, SSL VPNs use SSL /HTTPS which is available without additional software deployment on all standard Web browsers, as a secure transport mechanism. Using an SSL VPN, the connection between the mobile user and the internal resource happens via a Web connection at the application-layer, as opposed to IPSec VPNs’ open “tunnel” at the network-layer. The use of SSL is ideal for the mobile user because:

- SSL does not need to be downloaded onto the device being used to access corporate resources.

- SSL does not need to be configured by the end user.
- SSL is available wherever there is a standard Web browser, so users don't need a company laptop.

SSL is familiar to most users, even those without a technical background. It is already installed on any Internet-enabled device that uses a standard Web browser, and no configuration is necessary. SSL operates at the application-layer, independent of any operating system, so changes to the OS do not require an update in the SSL implementation. And because SSL VPNs operate at the application-layer, it is possible to offer extremely granular access controls to applications, making it ideal for mobile workers and those users coming from an insecure end-point.

SSL VPN technology has evolved to include a variety of different types of access via dynamically downloaded agents. These advances enable the delivery of client/server applications, as well as network-layer connections which are enabled via SSL. Dynamic delivery facilitates the use of agent-based access methods, without the cost or hassle of installing and configuring individual client software.

Another advancement in SSL VPNs is the provisioning of additional endpoint security. Unlike IPSec VPNs, where a level of endpoint security can be assumed, SSL VPNs were designed to provide granular access from any endpoint. A means of ensuring that each endpoint is in compliance with a minimum corporate security policy is mandatory. This can be done via dynamic endpoint security checks which should be done both before a session is initiated and periodically throughout the session.

IPSec or SSL VPN?

Many users are struggling to decide which technology should be deployed where. Where do IPSec and SSL VPNs fit into your network security policies, and which problems can each technology best address? What does it really take to deploy and administer an IPSec and SSL VPN?

This confusion is not mitigated by the fact that most debates over IPSec and SSL have largely focused on the technical details of the protocols and not on what should be the most significant deciding factor between these methods – the usage scenarios themselves. The fact is that IPSec and SSL are not mutually exclusive technologies. They can – and in fact, often are – deployed in the same enterprise. The deciding factor between them lies not in what each protocol can do, but in what each deployment is designed to accomplish. When one considers the cost/benefit of each type of deployment, as well as what problems each technology was designed to address, the deployment choices become clearer.

Administrators that need to achieve high performance, redundant site-to-site connectivity will be well served by IPSec VPN offerings. They were created to meet the challenge of how to securely provide employees around the world with “always on” connectivity that will enable them to access the corporate resources they need to achieve optimal productivity. For years, IPSec VPNs have been delivering the resilient, reliable connectivity that is imperative for ongoing communications between coworkers at different offices. IPSec VPNs provide users at geographically distributed locations an experience akin to that which they would receive if they were logging in at the corporate headquarters, allowing them to easily access all network resources that they would be able to access if they actually were on the LAN.

Administrators that need to allow mobile employees, contractors, offshore employees, business partners or customers access to certain corporate resources will be well served by SSL VPNs. SSL VPNs are designed to address the needs of diverse audiences that need secure access to administrator-specified corporate resources from anywhere and to change both the access methods and the resources allowed as the users' circumstances change. SSL VPNs can also be configured to check endpoint security compliance and to either provision resources accordingly or to provide the end user with a means to remediate. This combination of granular access and endpoint defense functionality mitigates the risks that access to corporate resources from an unprotected endpoint, untrusted network, or unauthorized user can introduce. As a result, SSL VPNs offer users the convenience of being able to access corporate resources using any Web-enabled device from anywhere.

<i>Type of Application</i>	<i>Type of PC</i>	<i>Remote Network Security</i>	<i>Type of Connection</i>	<i>Type of VPN</i>
<i>Remote Office/Branch Office</i>	<i>Corporate</i>	<i>Managed, Trusted</i>	<i>Fixed</i>	<i>IPSec</i>
<i>Mobile Employee</i>	<i>Corporate or Non-Corporate</i>	<i>Unmanaged, Untrusted</i>	<i>Mobile</i>	<i>SSL VPN</i>
<i>Partner/Customer Extranet</i>	<i>Non-Corporate</i>	<i>Unmanaged, Untrusted</i>	<i>Mobile</i>	<i>SSL VPN</i>

Total Cost of Ownership

Total cost of ownership is a vital consideration when deciding which VPN technology to deploy. Once again, it is essential to look at the deployment, not at the technology, to make this decision. If the need is for site-to-site connectivity, such as seen in a remote or branch office, IPSec VPNs are the logical and most cost-effective choice. Users in these situations will get the "on-the-LAN" experience that they require, without having to administer individual clients. If the need is for connectivity for remote/mobile users, business partners or customers, however, where the devices and networks from which access is desired will change, SSL VPNs are the most cost-effective choice. Administrators can leverage their existing investment in authentication stores, create granular role-/resource-based policies and deploy access to large diverse user populations in just hours, without having to deploy, configure, or manage individual software clients.

Security

Comparisons between IPSec and SSL often lead to a "Which protocol is more secure?" debate. In reality, these debates have little relevance to the choice between SSL and IPSec for remote access and site-to-site VPNs. These protocols achieve similar goals; they provide for secure key exchange and provide strong data protection during transport. Despite significant differences in the protocols, IPSec and SSL are actually quite similar in terms of transport security at a high level. Both technologies effectively secure network traffic, and each has associated trade-offs, which make them appropriate for different applications. Though the protocol implementations differ greatly, the two systems share many similarities, including strong encryption and authentication, and protocol session keys that are specified in a conceptually similar manner. Each protocol offers support for leading encryption, data integrity and authentication technologies: 3-DES, 128 bit RC4, AES, MD5 or SHA-1.

Access to Network

IPSec VPNs have been designed to enable a virtual extension of the corporate LAN or VLANs within it. Such access is vital for remote offices, where employees require unfettered access to function effectively. Because users in site-to-site deployments are subject to the same security strictures as are employed on the corporate LAN, including corporate-owned and managed devices and a trusted network topography, this constitutes no greater security risk than the LAN deployment itself. These security strictures cannot, however, be effectively extended to mobile users, business partners, or customers, who may wish to access resources from a variety of devices and networks. For their use, an SSL VPN can mitigate access risks in a cost-effective fashion.

SSL VPNs were criticized in the past for enabling access through such a wide variety of devices, including those with no corporate management. This concern has been mitigated, however, with the creation of endpoint defense mechanisms that are able to check the security posture of any device both before the session is initiated and throughout the session. Endpoint security combined with dynamic, session-by-session access controls provide a solution which is ubiquitous and secure.

Application Access

IPSec VPNs can support all IP-based applications--to an IPSec VPN product, all IP packets are the same. This makes them the logical choice for site-to-site deployments, where it would be unacceptable for a resource or application to be limited to the corporate LAN only.

SSL VPN application services vary, because each vendor/product has its own way of presenting client interfaces through browsers, relaying application streams through the gateway, and integrating with destination servers inside the private network. The use of SSL as a transport can lead some to believe that SSL VPNs are suitable to provide access to Web-enabled applications only. In reality, most SSL VPN vendors solved this problem long ago, with dynamically provisioned downloads that enable client/server application access and/or full network-layer access. In fact, some vendor's SSL VPNs can also provide a 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 supported by the network environment. This enables the high performance required for accessing latency and jitter-sensitive applications like VoIP, while providing the ubiquity and reliability that SSL VPNs are known for with none of the IPSec VPN management overhead.

Again, if the desired result of the deployment is for all users to have complete network access from managed devices and trusted networks, IPSec VPNs are ideal, but if the desired result of the deployment is to enable controlled access to specific corporate resources to mobile employees or users coming from uncontrollable endpoints, such as business partners or customers, SSL VPNs are ideal.

Access Management

Another consideration is access control. While IPSec standards do support packet filter-based selectors, in practice most organizations grant hosts access to entire subnets rather than go through the hassle of creating/modifying the selectors for each IP address change or new application. If you need to give trusted user groups access to private servers and subnets, IPSec VPNs are an excellent choice. On the other hand, if the deployment requires per-user/per-group, or per-resource access control, an SSL VPN is the best choice, because it

operates at the application layer, making such controls easy to set up. New access management capabilities can enable dynamic authentication and role-mapping, as well as very flexible and expressive resource-based authorization, enabling adherence to corporate security policies in an extremely cost-effective way.

Conclusion

More important than the question of which transport encryption protocol is “better” is the question: “Which security technology best fills the need for a remote access solution?”

Checklist

Decision Criterion SSL Vs IPSec

IT environment:	IPSec VPN	SSL VPN
Type of connection	Fixed connection	Transient connection
Type of device	Managed corporate device	Varying devices
Type of access	Site-to-site	Remote employee, business partner, customer
Access Controls		Enables access management policy enforcement

User constituency:	IPSec VPN	SSL VPN
Remote or branch office employees	X	
IT staff	X	X
Mobile employees		X
Day extenders		X
Consultants		X
Customers		X
Business partners		X

Client-side network and device:	IPSec VPN	SSL VPN
Type of device	Enterprise owned and managed	Managed or Unmanaged
Type of network	Trusted	Trusted or Untrusted
Specific use cases	Remote or branch office	Hotel Internet access; public use terminal (such as kiosks or internet café); customer or business partner's PC; home network

Applications and content:	IPSec VPN	SSL VPN
Voice Over IP	X	X
Entire subnets with no application access control required	X	
Networks, including intranets and extranets, that require access control		X
Web applications	X	X
XML & Flash applications	X	X
Client/server applications	X	X
Intranet content	X	X
Email	X	X
File Servers	X	X
Server socket dependent applications	X	X

Copyright 2005, Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.