

JUNIPER NETWORKS VPN DECISION GUIDE

Examining the Criteria for Deciding Whether IPsec or SSL VPN Best Fits
Your Business Need

Table of Contents

Executive Summary	1
Introduction	1
Network-layer IPsec VPNs.....	1
Application-layer SSL VPNs.....	2
IPsec or SSL VPN?.....	3
Total Cost of Ownership	4
Security.....	4
Network Access.....	4
Application Access	4
Access Management.....	5
Mobility	5
Thin Client Computing	5
Business Continuity	5
Conclusion	6

Executive Summary

This paper looks at how IPsec and SSL VPNs differ, and examines the criteria for deciding which technology best fits each business need. It is an ideal resource for IT personnel trying to determine when to deploy IPsec VPN vs. SSL VPN for their companies' remote access needs. After reading this paper, IT administrators will be able to understand the various factors they need to take into account to address their remote access needs and will understand which VPN solution can best address the different scenarios most effectively.

Introduction

Providing secure remote access to corporate resources has grown into a critical requirement for enterprises and service providers. It often makes the difference between those companies that are successful and those that are not. Whether the user is working in a remote office or hotel room or at an airport, using a laptop, handheld device, or public kiosk, they need easy access to corporate resources to accomplish their tasks and maintain their productivity. In addition, corporate business partners and customers increasingly need real-time access to corporate resources and applications.

In the early 1990s, there were only limited options to extend the availability of the enterprise's network beyond the boundaries of the corporate central site, which comprised mainly extremely costly and inflexible private networks and leased lines. As the Internet grew, however, it spawned the concept of 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 required software to be installed and configured on each endpoint device and provided only full network-layer access, unnecessarily exposing all the enterprise's resources.

Today, users need to access many different corporate applications from various types of client devices. Some of these devices, such as public kiosks, are outside of the enterprise's control and should be considered "untrusted." This makes it difficult, yet imperative, to ensure that all user connections comply with corporate security policies. It is in this environment that SSL VPNs were introduced, providing remote/mobile users, business partners, and customers with easy, secure access to only those corporate resources deemed necessary for that user. Together, IPsec and SSL VPNs enable enterprises to provide their offices and users secure, ubiquitous access to the corporate network to support the overall success of the business.

Network-layer IPsec VPNs

IPsec, or network-layer, VPNs can offer enterprises an easy, cost-effective way to route communications between sites, delivering the 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 unencrypted text) as a transport for sensitive, multiprotocol traffic. Network-layer VPNs provide a combination of encryption and tunneling functions to meet these challenges. They use peer negotiation protocols, such as IPsec, to encapsulate the data being transferred within an IP "wrapper" that travels 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 with the same full, continuous access to the network as 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 who just need to check email or retrieve certain documents from an 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 endpoint 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 that 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 café, 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, such as a remote office, must have client software preinstalled and configured 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 IPsec clients are 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, such clients are an impractical way to meet the needs of mobile/remote workers, business partners, and customers. For example, the need for VPN client software restricts users’ access to devices such as corporate laptops that have the software installed. Additional methods of access, such as Internet kiosks, PDAs, and so forth, which are often more convenient for the mobile user, are not accommodated, nor are devices that a 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 complements the reliable, powerful communication infrastructure that IPsec VPNs offer for site-to-site connections.

Application-layer SSL VPNs

The term “SSL VPN” is used to refer to a fast-growing product category that comprises a variety of technologies. To broadly define what products and technologies are within this category, one can begin with the term VPN itself. VPN, refers to using a public network (usually 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 IPsec, although some vendors used 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 HTTPS which is available in all standard Web browsers as a secure transport mechanism, with no need for additional software. With 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 VPN does not require client software to be preinstalled and maintained on the device being used to access corporate resources.
- SSL VPN does not need to be configured on the endpoint machine by a user or administrator.
- SSL VPN is available from any 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 operating system do not require an update of the SSL implementation. And because SSL VPNs operate at the application layer, it is possible to offer extremely granular access controls to applications based on user identity, the network that they are coming from, and the security posture of the device, making an SSL VPN ideal for mobile workers and those users coming from insecure endpoints.

SSL VPN also provides detailed auditing capabilities because of its application-layer proxy-based technology, aiding enterprises and service providers in complying with regulatory measures such as HIPAA, Sarbanes-Oxley, the Payment Card Industry Data Security Standard (PCI) and so forth. While IPsec VPNs can provide authorization and authentication capabilities, they cannot, for example, provide granular control of exactly what a user views or accesses, which is required by these regulations. As opposed to IPsec VPNs, which operate at the network layer, SSL VPNs work at the application layer and thus can provide the granular-level logging and auditing reports required by these regulations.

SSL VPN technology has evolved to include a variety of different types of access via dynamically downloaded agents. In addition to providing secure access to Web-based applications, these advances enable SSL VPNs to support client-server applications and to offer full network-layer tunnels, which deliver an experience similar to traditional

IPsec VPN access. Dynamic delivery facilitates the use of agent-based access methods, without the cost or hassle of installing and configuring individual client software. Additionally, SSL VPNs can solve the network address translation (NAT) and firewall traversal issues associated with IPsec VPNs, thus providing the broadest possible access.

Another advancement in SSL VPNs is the provisioning of additional endpoint security. Unlike IPsec VPNs, where a certain level of endpoint security can be assumed, SSL VPNs are designed to provide granular access from any endpoint. In an environment where IT administrators are asked to provide access to corporate resources from unmanaged and untrusted machines, 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 are to 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 to deploy and where to deploy it. Where do IPsec and SSL VPNs fit into existing 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. In actuality, IPsec and SSL are not mutually exclusive technologies. They can be—and often are—deployed in the same enterprise. The deciding factor in choosing between them lies not in what each protocol can do but in what each deployment is designed to accomplish. When one considers the costs and benefits of each type of deployment, as well as the problems each technology was designed to address, the deployment choices become clearer.

Administrators who need to achieve high-performance, redundant site-to-site connectivity will be well served by IPsec VPN offerings. These technologies were created to meet the challenge of securely providing employees around the world with the always-on connectivity and access to 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 of logging in at the corporate headquarters, allowing them to easily access all the network resources they would have at hand if they were on the LAN. In addition, the management resources required for deployment and maintenance are fairly limited in the site-to-site use case: the number of sites is limited; the device, which usually serves also as a firewall, is managed; and the session is fixed.

In contrast, administrators who need to allow mobile employees, contractors, offshore employees, business partners, and/or customers access to certain corporate resources will be better 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. They allow the administrator to change both access methods and the resources that can be accessed as the users' circumstances change. SSL VPNs can also be configured to check endpoint security compliance and to either provision resources accordingly or 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 with no preinstalled client software needed on the endpoint device.

Table 1: Scenarios For Using SSL VPN vs. IPsec VPN

TYPE OF APPLICATION	TYPE OF ENDPOINT DEVICE	REMOTE NETWORK SECURITY	TYPE OF CONNECTION	TYPE OF VPN
Remote office/ branch office	Corporate	Managed, trusted	Fixed site-to-site	IPsec
Mobile employee	Corporate or noncorporate	Unmanaged, untrusted	Mobile	SSL VPN
Partner/customer extranet	Noncorporate	Unmanaged, untrusted	Mobile	SSL VPN
Employee remote access	Corporate or noncorporate	Managed, trusted	Mobile	SSL VPN

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 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 used for access will change, SSL VPNs are the most cost-effective choice. Administrators can leverage their existing investment in authentication stores, create granular role- or resource-based policies, and provide access to large, diverse user populations in just hours, without having to deploy, configure, or continuously manage individual software clients.

Security

Comparisons between IPsec and SSL often lead to a “Which protocol is more secure?” debate. In reality, this question has little relevance to the choice between SSL and IPsec for remote access and site-to-site VPNs. These protocols achieve similar goals: they provide secure key exchange and strong data protection during transport. Despite the significant differences between the two 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. Although 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, and SHA-1.

Network Access

IPsec VPNs have been designed to enable a virtual extension of the corporate LAN or VLANs within them. Such access is vital for remote offices, where employees require unfettered access to function effectively. The 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 and provide remediation both before the session is initiated and throughout the session.

Endpoint security combined with dynamic, session-by-session access controls provide a solution that 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 or product has its own client interface and its own ways of relaying application streams through the gateway, and integrating with destination servers inside the private network. The use of SSL as a transport may lead some to believe that SSL VPNs are suitable only for providing access to Web-enabled applications. 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 vendors' SSL VPNs provide a dual-mode network-layer access capability that detects the best method of connection—IPsec or SSL transport—to ensure that the highest level of connectivity supported by the network environment is used. The dual-mode network-layer approach is ideal for accessing latency- and jitter-sensitive applications such as VoIP, while providing the universal access 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 to the trouble of creating or 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. Advanced 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.

Mobility

Mobility is a part of today's nonstop business environment. As mobile devices continue to proliferate, demand for remote access that goes beyond voice-to-voice or the Web is growing as well. Remote users, partners, and customers are no longer tied to PCs for Internet access. Phones and PDAs can access the Web wirelessly, making it even more convenient to stay connected from virtually anywhere.

SSL VPNs are the ideal solution for mobile remote access due to the browser-based technology that enables secure access to corporate resources. IPsec VPNs, on the other hand, require a heavy, installed client that is too resource intensive for many mobile devices; thus, fewer types of these devices can be supported. The SSL VPN application layer technology is also much more resilient to link fading than IPsec VPN network layer technology, and this makes SSL VPN ideal for securing access over wireless networks, where signal strength is not always reliable. And because SSL VPN operates at the application level, granular access to corporate resources from mobile phones and PDAs can be audited in great detail, compared to the binary on-off access of IPsec VPNs.

Thin Client Computing

Thin client computing (TCC), otherwise known as server-based computing, was designed to drive down the high costs associated with running applications on every desktop, to enable access to applications written for one computing platform from other platforms, and to provide remote access and control of applications. TCC is becoming increasingly competitive, and the technology continues to evolve. More and more IT departments are using applications from Citrix such as XenApp and/or Microsoft Windows Terminal Services. TCC vendors often offer SSL VPN as extensions to their product. SSL VPN is ideal to use with TCC in order to:

- Provide remote access to corporate resources
- Provide the ability to authenticate, authorize, and audit thin-client traffic
- Ensure endpoint device security
- Control access based on the combination of user, endpoint device, and network information

Business Continuity

Security threats from the today's global Internet community consistently challenge companies and organizations. Environmental threats and catastrophic events can also bring businesses to a halt. Business continuity relies on a company having the ability to maintain its productivity, services, and partnerships in the event of a disaster or other unpredictable event such as a hurricane, blizzard, terrorist attack, transportation strike, or communicable disease threat. A flu pandemic, for example, could require businesses to limit social interaction between employees, partners, and customers to prevent further spread of the virus. This scenario makes a compelling case for the wider adoption of remote access, as employees could then work productively from home for an extended period of time.

While IPsec VPNs are certainly effective for site-to-site connectivity, they may not be an ideal solution for addressing the need for remote access when a disastrous event occurs. For example, many employees will need to access corporate resources from unmanaged devices such as home PCs, public kiosks, or PDAs during such events. The endpoint security capabilities of SSL VPNs allow granular access from any type of endpoint device—unmanaged or managed—as long as it is in compliance with the minimum corporate security policy set that is in place. SSL VPN maintains productivity for employees by enabling them to work from anywhere using any type of device during these types of events.

Conclusion

Together, IPsec and SSL VPNs enable enterprises to provide their offices and users secure, ubiquitous access to the corporate network to support the overall success of the business. When deciding which technology best fits your organization's needs, make sure to weigh your requirements against the decision criteria outlined in this paper.

Table 2: Decision criteria checklist: SSL VPN vs. IPsec VPN

Criterion	IPsec VPN	SSL VPN
IT Environment		
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	None	Enables access management policy enforcement
User Constituency		
Remote or branch office	Yes	No
IT staff	Yes	Yes
Mobile employees	No	Yes
Day extenders	No	Yes
Consultants	No	Yes
Customers	No	Yes
Business partners	No	Yes
Client-Side Network and Device		
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 kiosk or Internet café), PDAs, customer or business partner's PC, home network
Applications and Content		
VoIP	Yes	Yes
Entire subnets with no application access control required	Yes	Yes
Networks, including intranets and extranets, that require access control	Yes	Yes
Web applications	Yes	Yes
XML and Flash applications	Yes	Yes
Client-server applications	Yes	Yes
Intranet content	Yes	Yes
Email	Yes	Yes
File servers	Yes	Yes
Server socket-dependent applications	Yes	Yes

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.



Copyright 2009 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. "Engineered for the network ahead" and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.