

White Paper

IPSec and SSL VPN Decision Criteria

A Technology White Paper by Juniper Networks

Don Root
Solutions Marketing Manager

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: 200093-002 May 2006

Table of Contents

1	THE SECURE ACCESS LANDSCAPE	3
2	NETWORK LAYER IPSEC VPNS.....	3
3	WHAT IS AN SSL VPN?	5
4	IPSEC OR SSL VPN?.....	7
5	TOTAL COST OF OWNERSHIP.....	9
6	SECURITY	10
6.1	ACCESS TO THE NETWORK.....	10
6.2	APPLICATION ACCESS.....	11
6.3	ACCESS MANAGEMENT	11
7	CONCLUSION.....	12
8	DECISION GUIDELINES	13

1 The Secure Access Landscape

Providing secure access to network resources has become a critical requirement for virtually all federal agencies, often the defining difference between those agencies that successfully execute their mission and those requiring operational improvement. Whether the user is working in a hotel room, a field office, or deployed in a foreign land they need easy access to network resources to accomplish their mission and maintain productivity. In addition, suppliers and contractors increasingly need real-time access to network resources and applications, often on a temporary, finite-time basis.

In the early 1990's, there were only limited options to extend the availability of the agency's network beyond the boundaries of the 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, in many ways, still too costly to maintain, and the cost and issues for suppliers or contractors were even more difficult. It is in this environment that SSL VPNs were introduced, providing remote/mobile users, suppliers and contractors the easy, secure access to resources they needed. Together, IPSec and SSL VPNs enable organizations to provide their offices and users secure and ubiquitous availability to the network, thus supporting the overall success of the agency.

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 mission objective.

2 Network Layer IPSec VPNs

IPSec (a network-layer VPN protocol) can offer organizations an easy, cost-effective way to route communications between fixed sites, delivering high performance connectivity and resiliency to match the needs of the most demanding network environments. IPSec VPNs were created as a cost-effective encrypted transport alternative to private or leased lines enabling organizations to use the Internet infrastructure to 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, and usually transmits text in the clear) as a transport for sensitive, Multiprotocol traffic. Network-layer VPNs provide a combination of encryption and tunneling functions to meet these challenges. They use negotiation protocols, like

ISAKMP to authorize remote peers and tunneling protocols like ESP and AH to encapsulate user data within an IP “wrapper” that will traverse the Internet. This encapsulated data is received by the network layer VPN gateway, “unwrapped,” decrypted, and forwarded to the recipient. Traffic arriving from the VPN gateway is handled as if it originated 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 located at the same facility. This is ideal for facilitating regular communications and resource sharing among users at geographically separate offices to improve productivity agency-wide.

In certain instances, however, this level of access may be undesirable. For example, mobile users that simply need to check e-mail or retrieve documents from an agency intranet don’t need a dedicated pipeline to all the resources on the network. Furthermore, this level of access could introduce security risks if the computer the user is using is insecure or easily compromised. While it is possible to secure a PC that is actually within the LAN, such precautions are difficult and expensive to implement for remote PCs on unmanaged networks. As a result, connections that are not originating from a dedicated access point under the control of the organization should probably be limited in terms of the resources available to them and the permanence of the connection, to mitigate any security vulnerabilities. For example, remote users originating from an untrusted network to connect to an application or resource need a simple, cost-effective method to access it, but should be restricted to just that application and resource, not granted access to the corporate LAN in total. Likewise contractors may be allowed access to certain resources from an unmanaged device, but should not be granted LAN-wide connectivity.



NetScreen-5200

Part of the Juniper Network Security Product Portfolio with IPSec capabilities

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.

3 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, based on the Secure Sockets Layer (SSL) protocol. 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. 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 an agency-managed computer, SSL VPNs use SSL /HTTPS which is the secure transport mechanism built-in to all standard Web browsers. Using an SSL VPN, the connection between the user and the internal resource occurs via an HTTPS connection at the application-layer, as opposed to IPSec VPN's "tunnel" at the network-layer. SSL VPNs still utilize the robust security of 3DES encryption, but they don't require an "open pipe" to be established back to the internal resources. Instead, SSL VPNs are application and user aware, so access is granted only to the resources designated by the administrator on a per user basis. To ease the configuration of policy, the administrator can define roles which establish access privileges used by numerous users. Then each user is assigned to a role. But Juniper Networks realizes that a given user may not deserve the same access rights depending on where and when the access is to take place. A function called Host Check is downloaded as an applet when a user attempts to access the SSL VPN gateway. This host check is able to determine specific attributes about the computer from which access is being attempted. Items the host check may look for include, existence of known Trojans or viruses, latest virus definition files, network location, and flags that may specify whether the device is owned by the agency or not. The user's access privileges are granted based on who is accessing, and from where. The same user may have completely different access privileges from a home office versus a contractor's kiosk versus a public Internet terminal. This is the true difference between SSL and IPSec

VPNs. It's not a transport and encryption difference, but rather a statement of usage and policy. For this reason, Juniper Networks uses the term Instant Virtual Extranet, or IVE, to describe the SSL VPN product line.

The use of IVE is ideal for the mobile user because:

- It does not need to be installed and maintained on the device being used to access internal resources.
- It does not need to be configured by the end user.
- It is available anywhere and everywhere there is a standard Web browser with connectivity to the Internet

Furthermore the Juniper IVE allows the use of tokens, such as smart cards and time-synchronized password generators using the industry standard RADIUS protocol. Support for this additional level of authentication is built into the IVE platform.



Secure Access SA-4000-FIPS and SA-6000-FIPS
Part of the Juniper Network Security Product Portfolio with SSL VPN capabilities

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

4 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 posture, and which problems can each technology best address? What is required to deploy and administer an IPsec or 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 rather than the usage scenarios. The fact is that IPsec and SSL are not mutually exclusive technologies, and both technologies are equally secure in terms of bit transport over an insecure network. They can – and in fact, often are – deployed simultaneously in the same organization. The deciding factor between them lies not in what each protocol provides, 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.

Part of the problem across the Federal government in general is many users and network managers are struggling to decide which technology should be deployed where. Where do IPsec VPNs and SSL VPNs fit into their network policies, and which problems can each technology best address? This question can be best answered by looking at the usage scenarios themselves (see Figure 1). The fact is that IPsec and SSL are not mutually exclusive technologies. They can – and in fact, often are – deployed in the same enterprise.

- IPsec VPN – Administrators that need to achieve site-to-site connectivity will be well served by IPsec VPN offerings. They were created to meet the challenge of how to provide employees around the world with secure “always on” connectivity that will enable them to access all of the corporate resources they need to achieve optimal productivity.
- SSL VPN – Administrators that need to allow teleworkers, 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 resources allowed as the users’ circumstances change. SSL VPNs can also be configured to check end-point security compliance and to either provision resources accordingly or to provide the end user with the means to remediate.

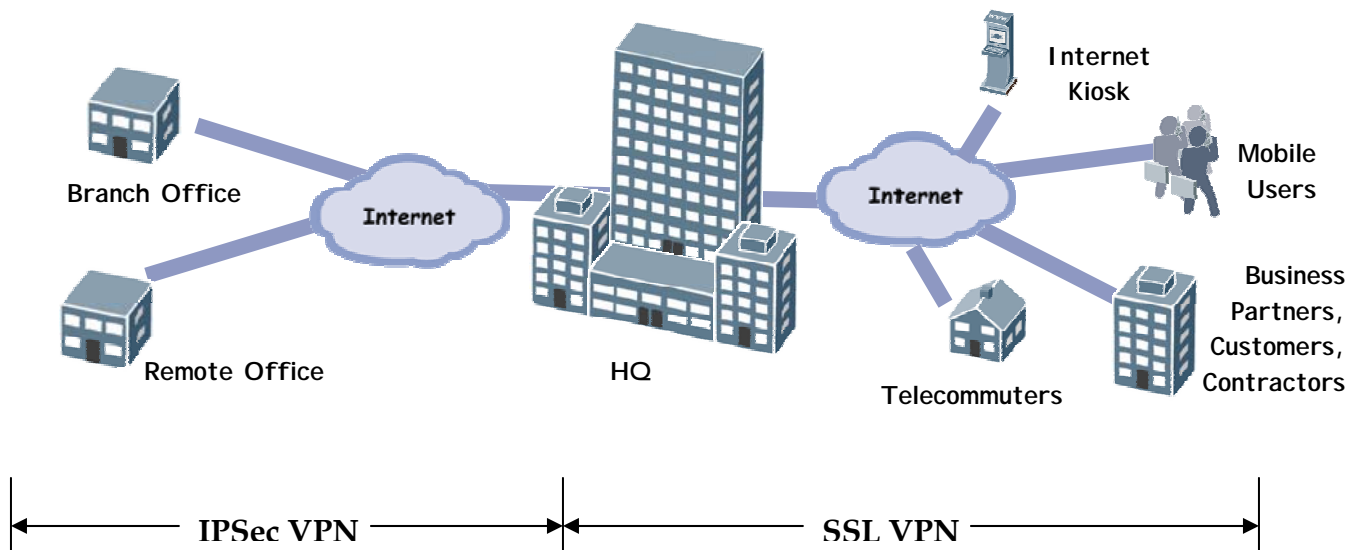


Figure 1 - Applications for IPSec VPN and SSL VPN

Administrators requiring high performance, redundant site-to-site connectivity will be well served by IPSec VPN offerings. They were created to meet the challenge of securely providing employees around the world with “always on” connectivity that enables access to the network resources they need. 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 agency headquarters, allowing them to easily access all network resources that they would be able to access if they actually were on the LAN at the main facility. User’s requiring access via EAL4+ Common Criteria certified products would be well-served by products like the Juniper Networks NetScreen 5200. This product provides integrated IPSec VPN and firewall functionality in the industry’s first product to be certified to EAL4+ for the Packet Filtering Protection Profile for Medium Robustness Environments. The product is also FIPS-140-2 Level 2 validated.

For more information on IPSec VPNs, please refer to Juniper’s Firewall/IPSec VPN product information page at: <http://www.juniper.net/products/integrated/>

Administrators that allow mobile employees and other users not originating from “trusted” end points (under the control of the agency) access to certain and specific network resources will be well served by Juniper Networks Secure Access line of products, which implement SSL VPNs or Instant Virtual Extranets. They are designed to address the needs of remote/mobile employees, as well as suppliers and contractors, which need to securely access administrator-specified network resources from anywhere.

IVE's allow administrators to implement very granular access control, designating to the URL, file or server level the applications that specific users may access. This functionality mitigates the risks that access to network resources from an unprotected endpoint, untrusted network, or unauthorized user could introduce. As a result, SSL VPNs offer users the convenience of accessing network resources using any Web-enabled device anywhere.

Leading analysts predict that SSL will become the dominate access method for remote and mobile employees within the next few years.

Examples	Remote Network Security	Type of Connection	Type of VPN
Remote Office/State Agency	Managed, Trusted	Fixed	IPSec
Mobile Employee/Contractor	Unmanaged, Untrusted	Mobile	SSL VPN
Supplier Extranet	Unmanaged, Untrusted	Mobile or Fixed	SSL VPN
Inter-Department Information Sharing	Unmanaged, Trusted	Fixed	SSL VPN
Law Enforcement Access to Federal Databases	Unmanaged, Untrusted	Mobile or Fixed	SSL VPN
Remote Backup/ Transfer to Contingency Operations Center	Managed, Trusted	Fixed	IPSec
Doctor Access to Patient Records	Unmanaged, Untrusted	Mobile or Fixed	SSL VPN
Transfer of Patient Radiological Images from Image Facility to Hospital	Managed, Trusted	Fixed	IPSec

Examples of How Different Types of Connections Require Different Types of VPNs

5 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 office, IPSec VPNs are the logical and most cost-effective choice. Users in these situations will enjoy the "on-the-LAN" experience that they require, without having to administer individual clients. If the need is for connectivity for remote/mobile users, suppliers or contractors, 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 systems, 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.

6 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 using SSL and IPSec for remote access and site-to-site VPNs. Both protocols achieve similar goals; they provide secure key exchange and strong data protection during transport. Despite significant differences in the protocols, IPSec and SSL are actually quite similar 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 such as: 156-bit 3-DES, 128-bit RC4, MD5 and SHA-1.

6.1 Access to the Network

IPSec VPNs have been designed to enable a virtual extension of the agency 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 policies as are employed on the agency LAN, this constitutes no greater security risk than the LAN deployment itself. These security strictures cannot, however, be effectively extended to mobile users, suppliers, or contractors, 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 has, in fact, been criticized because it enables access through such a wide variety of devices, including those with no central management, and because it is easy to deploy to a broad range of end users. In practical terms, though, these are not fair criticisms. Juniper Network’s SSL VPN implementations now include methods to enforce endpoint security, as well as means to “clean” PCs of any information downloaded during a session.

IPSec VPNs protect IP packets exchanged between remote networks or hosts and an IPSec gateway located at the edge of your private network. SSL VPN products protect application streams from remote users to an SSL gateway. In other words, IPSec connects hosts to private networks, while SSL VPNs connect users to services and applications inside those networks.

6.2 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.

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. SSL has been criticized because, in the past, each application had to be Web-enabled, which required development of new functionality and distribution of new software. This problem has been eliminated by Juniper's SSL VPN products, which provide clientless Web access, as well as a client proxy for client/server applications or full network access. As a result, Juniper's SSL VPN products can be used to secure access to almost all applications by different types of users.

Juniper Networks is committed to the federal governments certification and validation processes. Currently most of Juniper's IPSec products are Common Criteria EAL4+ Certified for the Packet Filtering Protection Profile for Medium Robustness Environments. Most IPSec products are also FIPS-140-2 Level 2 validated. Several of Juniper's Secure Access products contain FIPS-140-2 Level 3 validated modules for key management.

Again, if the desired result of the deployment is for all users to have complete network access from managed devices on trusted networks, IPSec VPNs are ideal. If the desired result of the deployment is to enable controlled access to specific network resources on a per user basis, for users utilizing uncontrolled endpoints, such as suppliers or contractors, SSL VPNs are ideal.

6.3 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 creating the rules for each IP address. If an administrator must provide 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 agency security policies in a very cost-effective way. The Juniper Networks SSL VPN products perform an endpoint assessment, and can be configured to grant resource access based on the results of that analysis. Furthermore, the SSL VPN product also provide detailed audit logging capabilities.

7 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?” Since IPSec can be used to secure any IP traffic and SSL is focused on application-layer traffic, IPSec is well suited for long-lived connections where broad and persistent, network-layer connections are required. SSL, on the other hand, is well suited for applications where the system needs to connect individuals to applications and resources. Both technologies are equally secure; the choice between which to use should be based on the level of control needed for granting access to resources as well as the agency’s need to interoperate with other agencies and vendors. In fact, most agencies will use both technologies simultaneously.

8 Decision Guidelines

The following tables provide general guidelines as to which technology is suited for various applications.

IT environment:	IPSec VPN	SSL VPN
Type of connection	Fixed connection	Transient connection
Type of device	Managed agency device	Varying devices
Type of access	Site-to-site	Remote employee, supplier or contractor
Access Controls	Coarse access control capabilities	Granular access-management policy enforcement

User constituency:	IPSec VPN	SSL VPN
Remote office employees	✓	
IT staff	✓	✓
Mobile employees		✓
Employees at other agencies		✓
Consultants/Contractors		✓
Contingency Operations Center	✓	
Suppliers		✓

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

Copyright © 2006, 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.