Global Information Assurance Certification Paper

Comparative Approach to Selecting Among Technologies to deploy VPN Access

By
Fred M. Van Drimmelen

SANS Security Essentials

GSEC

Practical Assignment Version 1.4b
Research Paper

December 2002

Overview
This paper will attempt to present a balanced view between Internet Protocol Security Protocol (IPSec) and Secure Socket Layer Protocol (SSL) for the Information Technology Professional responsible for selecting or implementing them for Virtual Private Network purposes. As each had an original intent, this will also be emphasized where appropriate. Understanding that these technologies can both compete with and complement each other is necessary for the Security Professional.

Any evaluation or product selection should start with a defined short list of products. They should be current, released, generally available and fully supported products from a variety of sources. This document will not attempt to limit or expand your specific choices; it will lay out criteria that can be used in the Process.

Defense in Depth….

As with any process, VPN deployment should be viewed as a component within your overall Security Systems and in the context of established Defense in Depth scope.

If you do not have a Firewall in place today, don't start here. Defining where your network perimeter exists, as well as what services are allowed to be originated within and external to that perimeter is the primary purpose of a firewall system. Without a defined perimeter you have no reference point of what is internal and what is external to your security domain. Since we are going to discuss secure external access we need a point of reference as to what we consider interior to our security domain.

If you don't have an education program in place for your customers/users today, don't start here. A Security education program will allow for support and compliance to be encouraged among all users. When staff is ignorant of what the company considers a security or intellectual property risk, they have no way of protecting against breaches of this definition. A well educated work force is a key to successful security practices.

If you don't have a DMZ system in place today, don't start here. Once the Firewall defines what is outside and what is inside, there are going to be cases of systems being placed exterior to the Firewall protections. Placing the system(s) externally without any protection is not generally considered a good security practice. The De-Militarized Zone concept was developed within IT circles to denote systems that are place in a position exterior to the corporate protections of full Firewall controls. The systems within the DMZ should be Operating System hardened as much as possible. Any system within the DMZ should also be considered highly at risk and validated on a regular basis for breaches and

corruption. While application flow to and from the DMZ is relatively open, basic controls are still put in place to allow only expected traffic types in and out. Also communications from the DMZ into the corporate network, if allowed, should be monitored at almost the same suspicion level as fully external to the corporate systems.

If you don't have established policies and procedures for Management and Configuration controls, don't start here. As with any Security system, guidelines and policies that give general as well as specific instruction should be defined for both risk management as well as technical guidance. This risk acceptance should be provided from Managerial and/or Executive levels for both authorization and business practices purposes. Technology and Information can only be protected without risk if only one person has the information. The purpose of most Information Technology efforts is to share the information with the appropriate people within a given sphere of influence. Be this a workgroup, a department, a division or a full corporation level of sharing definitions need to be in place.

If you are viewing IPSec and/or SSL as a complementary component of an overall Defense in Depth system, start here.

What is a VPN?
A VPN or Virtual Private Network, for the purposes of this document, is any external access to an IT resource via the IP Protocol. This can be as simple as remote dialup to a fully managed IP service provided by a Service Provider or Carrier. The material in this document is concerned with security at the IP level and above once the business decision has been made to 'open' the network to external access.

What is IPSec?
IPSec as defined by the IETF is a set of protocols that meet certain security criteria. The overall Security architecture is defined within RFC 2401 [2401]. Each protocol receives its own treatment within the IETF processes. The primary protocols that IPSec and specifically the IETF IPSec working group is involved with are:

Header Authentication [HA]
Encryption [ESP]
Internet Key Exchange [IKE]

IPSec has 21 IETF definitions that have progressed to the fully reviewed RFC level. There are currently several that have moved to an updated RFC. And there are 21 draft level documents being reviewed within 2002. This is according to the IETF IPSec Working group [IPSec WG]

What is SSL ?
Secure Socket Layer (SSL) has many implementations and several versions. This discussion will be in reference to the IETF submitted version 3.0 of SSL. This paper does not cover the many implementations of this protocol, other than to say that some implementations have considered security issues better than others, “caveat emptor”. Implementers should also be aware that TLS has, from an IETF perspective been built upon the work of SSL and is the official IETF reference point for Transport Layer Security. [TLS WG]

SSL version 3 (SSL3) was defined by Netscape Corporation and submitted for RFC in 1996.

TLS/SSL encompasses definitions that have progressed to fully reviewed RFC level of submissions within the IETF [TLS WG]. There are five full RFC level documents related to TLS/SSL. Eight other IETF documents to date are at the draft stage. Further working group materials are focused under TLS for current naming.

Although the IETF did not adopt the native SSL protocol as a standard it has become a de facto standard in that it has been deployed by thousands if not hundred’s of thousands of developers into corporation’s applications. Thus this document considers SSL a standards based approach by the average development staffer. Tools formerly referenced via SSL should now become TLS [2246] compliant for interoperability into the future.

What was the expected use of each according to their RFC ?

IPSec by definition is to assure secure network access and transmission of data across a given network. This translates to IP level security. The group of protocols defined depends upon and interact between each other. One key characteristic that they use in common is the Security Parameter Index (SPI).

SSL is defined for the express use of transaction oriented services at the Application level. SSL was defined to protect a specific application or set of transactions within an application. SSL is inherently dependant on Public Key Infrastructure, whether this Key Infrastructure is actually provided by a public entity or not is optional. If the Key controls are turned over to a Certificate Authority (CA) there are inherent security evaluations that should go into evaluating these partnerships as well. Several risks have been pointed out since the concept of public CA control was being introduced in 2000 [CSJ].

How do the two interact? Are they mutually exclusive?

Since IPSec is defined to be used as a network level protocol (Protecting IP) it is not mutually exclusive of using SSL for applications security. When used against

their original primary objectives these two sets of tools can be used in combination to secure sensitive materials.

Dependency for secure deployment

As with any component of a Defense in Depth system you, the end user, will need to define what acceptable security practices are necessary relative to the various data repositories within your control.

IPSec depends on a trust relationship at the Key and Network levels. That is to say that you are willing to give a particular Application, Host or Network access if they supply the correct set of security information first. Another premise is that the Key system, whatever it is, is kept secure from intrusion, inappropriate access and misuse. [2401]

IPSec is intended and deployed to secure at the Network level. That is when an IPSec connection is completed successfully the Branch office or Client making this connection now has the appearance of being locally attached to a given network segment. If a resource is available from this segment, either locally or from a routed perspective, it is wide open from a native IPSec perspective. From a transport perspective between the two IPSec entities all transmissions are at a minimum encrypted; with compression being an option both for throughput as well as secondary security capabilities.

Many IPSec devices allow for additional security measures beyond just transport security. You as an evaluator need to keep in mind which of these additional features adds value within your network environment. Things from Access Control lists to Stateful Inspection Firewall capabilities into Bandwidth Management and Control are all add on functionality beyond your basic IPSec capacity within a product. Remember IPSec only secures the IP transport into the network you have connected to. It is up to the IT Professional to make sure those groups and individuals have the levels of access appropriate within their needs.

As for public usage, most companies providing managed services to a given client base believe that IPSec will be the dominant IP VPN technology into the near future. An example is Ted Studwell of Virtella Communications, when discussing SSL versus IPSec was asked “Do VPN service providers favor one technology over the other at this point?” his reply was “They’re all using IPSec today. The problem again with SSL is that it does have limited functionality which works great in some cases but doesn’t fix the problem for 90% of corporate IT infrastructure. If you have 10 corporate offices and you want to connect them together with a VPN, SSL is never going to fix that problem.” [SN]

SSL depends on an application’s intelligence and Operating Systems having been built appropriately. Ease of use by the end user was the primary definition criteria and security was a secondary consideration. As with any system with

primary and secondary goals it leaves it up the implementer to decide which is more important to their environment. You must have systems in place to test the actual applications coding within an SSL environment to guarantee security levels are maintained.

An example of the Operating System (OS) dependency is the 'Critical' Windows 2000 patch issued in August of 2002. This patch is to prevent privilege elevation vulnerability in the Network Connection Manager (NCM). In the original OS release an unprivileged user can run code within a security context appropriate to this user level that then can make a network connection within the OS allowing code to run via the NCM with full system privileges. The full security bulletin is at http://www.microsoft.com/technet/security/bulletin/MS02-042.asp.

The intent of SSL as a security tool is to allow individual applications to secure given transactions and functions. Since SSL operates up through layer seven it can cause heavy loads to be placed upon general purpose processors. In recent years several companies have produced SSL acceleration technology that offloads the majority of this processing and allows for larger scale deployments of the SSL protocol as a commercially viable security solution.

When the goal is to open up one or a few applications and provide high levels of security checks along with data validation, SSL is a prime candidate. The SSL model calls for an evaluation of a given application, versus providing full network access to a given client or partner. This approach allows for a much more granular approach to allowing clients or partners access to a given set of data. Along with this granularity comes the burden of providing this access on an application by application basis.

Security Evaluation Process Defined

As was stated in the preface to this document, after you have a Firewall, after you have an education program, after you have a DMZ, after you have established a set of enforceable Management and Configuration policies then and only then should you consider opening you environment up to outside access from a security point of view.

With the understanding that businesses must move quickly and with agility, the following sections outline a process to review and evaluate a given set of IPSec and/or SSL products to be deployed. This evaluation criterion is ordered from a security perspective, you may find it needs different ordering criteria in your environment, remembering security in the real world is a series of trade offs.

First define the end goal of what is to be secured and to what degree it needs this security. As you look at any resource ask these questions at a minimum. What is being defended? How is it accessed today? How will it be accessed six months from now? Who has access today? Who has authority to grant access?

Why is this resource accessed? Once you have the outline of Who, What, When, Where and Why in a written form the process becomes much simpler.

Next consider the existing environment that any new product will need to be integrated into. If you have a data resource to protect, you have a set of infrastructure supporting that data resource already. Items such as Bandwidth, Physical LAN connectivity, Logical LAN connectivity, IP Addressing are just a few of the items that need consideration any time a new device is placed into a networked environment. Taking into consideration what exists today usually allows you to narrow your field of research considerably. If you have an environment that consists of switched 10Mb/s Ethernet. Then 10Mb/s line rate for the security device could be quite appropriate for a maximum. However, if you are aggregating multiple switching devices into a core and your security device must support this aggregation as well you would be looking for throughput numbers in the 100Mb/s into the multiple 100Mb/s range. These could be products within a given product set or you may end up with completely different products to meet the various needs. Defining your needs up front usually saves time and effort as you move through the project.

Reading product literature is a good starting point. Don't stop here. Vendor claims can range from conservative to vapor ware. Make sure any product that you put on your short list comes with a list of customers that have deployed it before you. Unless you are part of a development team partnered with a manufacturer bringing a new product to market, the vendor should be able to provide this reference listing.

What any reasonable IT staffer should be concerned with is what your company needs to accomplish, not how many bells and whistles a given product has. Stay focused on the business requirements and your IT career has a lot more room for growth. Below is a table that can be used as a starting point for your evaluation purposes. The items within the table are discussed below as well. Use of the table as it exists or the individual items within the table will give you a starting point, expand it to your companies needs as you see fit.

General Guidelines for IPSec and/or SSL Product Evaluation	
Throughput (on the product specified, not the product family)	
Encryption	
Compression	
Connectivity	
Firewall – Stateful versus Access Lists	
SNMP Access	
Management Access	
Quality of Service Control/Recognition	
Expected Internal Development efforts	
Expected External Customization efforts	
Trade offs	
	Performance vs Security
	Price vs. Performance
	Price vs. Features
	Management Security vs. Convenience
IPSec	
	IKE Holes Tested
	HA Holes Tested
	ESP Holes Tested

As outlined in the table above, make sure you have product specific numbers for throughput. The next item to verify against these numbers is that they cover both speeds with security features enabled as well as throughput for clear text forwarding. If these numbers are significantly different it would benefit your research process to verify that additional hardware is not required to obtain the marketed performance.

As for Encryption, in order to qualify as an IPSec deployment there is only one encryption methodology required; all others are optional for development purposes. So if you are looking for flexibility as well as future protection double check that the equipment on your list does not simply 'meet minimum' when it comes to IPSec compliance.

In regards to Compression you will want to make sure, again, that this capability is not an add-on that will cause unexpected expenses in the initial or future deployment. Being aware of the need and being caught off guard is only a matter of degrees. If management requires a particular performance characteristic,

compression can help increase gross throughput, compression may be required. If compression is being used as an additional security measure it may also be a requirement. Make sure your analysis takes into account the full cost of implementation concerning this feature.

Connectivity is usually a starting point for any device you are bringing on board. However, you would be well advised to make sure the products you are considering have additional interfaces beyond your immediate requirements. If it has Fast Ethernet today, how would I deploy Gigabit Ethernet in the future? If it has a V.35 or T1 interface today, how do I deploy DS-3 or multiple T1 interfaces in the future? Make sure you are accounting for your 18 to 24 month technology horizons. Most manufacturers will not give a guarantee 24 months out, but they can provide guidance to whatever degree their corporation is willing to commit to a specific product set.

VPN devices and software packages providing VPN services only secure particular components of a given environment. The need to secure with Firewall technologies (Trusted and Non-Trusted) is an even larger requirement now that you are opening your environment up to external access. Many products will claim Firewall capabilities while only providing manual Access Control Lists. Some products offer combinations of Access Control Lists and Stateful Packet Inspection capabilities. Making sure what comes with the base product code and what needs to be purchased separately makes your design sessions productive from day one. If you bought it you can design with it. If you run “What if?” design sessions you can qualify the benefits versus the additional costs. Depending on your organization low cost, feature flexibility or full functionality may be the priority. Make sure the cost of each is identified in the evaluation.

SNMP and Management access can be combined for discussion purposes. In the evaluation they should be treated separately. Can you access information from the ‘security device’ without any authentication, challenge, or validation? Does this type of access require that you are authenticated to at least a level above what you are asking your customers to utilize? Can the average user gain access to the Management interface? Can the user that is authorized to read (only) SNMP information gain access to manage and change the configuration on the given system? Run your systems through a series of questions like those above to make sure that security was the primary thought going into the “security device”.

Quality of Service (QOS) can be implemented in many ways and marketed in just as many. If one of the goals of the system is to differentiate between user groups or individuals QOS mechanisms can be highly beneficial. It benefits the evaluation to make sure the QOS implementation fits the overall QOS system deployed or expected to be deployed. The most common in today’s market is Differentiated Services (DiffServ). Again this comes back to the point of

implementing new technologies and solutions into existing environments, don't do it in a vacuum!

Development and Customization issues can cause a perfectly good plan to fail. If you are a small company that needs a self contained VPN solution or only wants to open a single application up to Internet access this is a very different requirement from a Multi-National corporation needing to open many networks and applications to Partners, Suppliers, Remote Employees, Contractors, etc. Make sure the products you evaluate are meeting your short term horizons as well as ask the questions of: "How do I grow this implementation?", "How do I move from a self contained implementation to an enterprise wide deployment?", "What modifications are allowed or available?". Some of these questions and any others you can think of will prepare you to discuss the Security deployment in business terms, which is what Management cares about.

As for the two categories of Trade Offs and IPSec, these are starting points for your real world evaluation. In any project there are trade offs. Even within protocols designed for security such as IPSec or SSL for that matter, reviewing known issues or vulnerabilities on public listings such as CERT can save time and effort when it comes to weeding out and then deploying platforms. Security listings generally point out the Platform and Software revisions any known issues are found on. Make sure your deployment is of code known to correct any pertinent issues discovered in the evaluation process.

Complementary usage expectation

Some evaluators will find that writing a statement of expectation here will be useful in discussions with various stake holders in the process. Do you expect a single log on process for all access? Does a user need to be tracked for some transactions and not others? Do regulations or business policies require transaction logging? What level of security is expected by the producer of the information? What level of security is expected by the user or the information? These starting point questions can guide you into or out of the need for using both IPSec and SSL in combination or individually. The list is not exhaustive, it is meant to give a starting point for the IT Professional at the evaluation stage.

As with any IT Process, Security is not a static entity. Keeping the following items in mind during an evaluation can keep sanity in the process.

Why do we care about securing?

Where do we care about securing?

What level of security is acceptable?

What complexity level is acceptable?

How many boxes are too many?

Thank you for your time and consideration of the materials I have presented. My hope is that the information and process above will assist your efforts in creating an acceptably secure VPN environment.

References:

[2401] Kent, R. Atkinson, “Security Architecture for the Internet Protocol”, Network Working Group, Standards Track, RFC 2401, November 1998
http://www.ietf.org/rfc/rfc2401.txt

[HA] S. Kent, R. Atkinson, “IP Authentication Header”, Network Working Group, Standards Track, RFC 2402, November 1998
http://www.ietf.org/rfc/rfc2402.txt

[ESP] S. Kent, R. Atkinson, “IP Encapsulating Security Payload”, Network Working Group, Standards Track, RFC 2406, November 1998
http://www.ietf.org/rfc/rfc2406.txt

[IKE] S. Kent, R. Atkinson, “The Internet Key Exchange”, Network Working Group, Standards Track, RFC 2409, November 1998
http://www.ietf.org/rfc/rfc2409.txt

[IPSec WG] IPSEC Working Group Charter
http://www.ietf.org/html.charters/ipsec-charter.html

[TLS WG] TLS Working Group Charter
http://www.ietf.org/html.charters/tls-charter.html

[2246] Dierks, C. Allen “The TLS Protocol Version 1.0” Network Working Group, Standards Track, RFC 2246, January 1999
http://www.ietf.org/rfc/rfc2246.txt

[CSJ] Computer Security Journal Vol XVI, Number 1 2000
“Ten Risks of PKI: What you’re not being told about Public Key Infrastructure.”

[SN] SearchNetworking, June 20, 2002
“SSL VPNs: Great for basic access but not for power users
http://searchnetworking.techtarget.com/qna/0,289202,sid7_gci834329,00.html