

Is SSL Ready for Enterprise Deployment?

White Paper



- The purpose of this paper is to examine the role of SSL as a remote access technology within a true enterprise architecture.
- This paper looks at the strengths and weaknesses of SSL as a remote access tool and identifies needed improvements before enterprises can adopt this capability as a true enterprise architecture.

Impact of the Internet

The internet has had a profound effect on the way business is performed today, combined with email it has the capability of bringing the whole world to our doorsteps, and enabled organizations to do much more “connecting” than ever before.

Recent events have brought home the realization that while centralized data centers are easy to manage, they can be vulnerable to disruption, and the pendulum has swung once again to de-centralized environments and multiple backup sites.

The combination of decentralized enterprises and a more dynamic workforce means that work is no longer limited to the workplace. Home offices are pretty much a standard feature for any professional, and laptops have replaced desktops as the system of choice as the business population has become more and more mobile.

According to the Digital Future Report (formerly the UCLA Internet Report), in January 1994, about 2 million computers — primarily used by academics, scientists, and corporate researchers — were connected to the Internet. Six years later, this had increased to 70 million, and today the Internet is used by about three-quarters of Americans, and online technology is a constant presence in two-thirds of American homes.

For IT managers this means that like it or not, the internet has become an essential component of the enterprise architecture, and has to be considered in any effective IT planning. For the enterprise the issue is not just how to “connect and protect” with the internet, but really how to securely integrate the public internet with the “private” network. It’s not just security and connection. It’s also about how to best take advantage of the potential of the internet, while at the same time protecting against, its openness unreliability and latency.

The Internet as a WAN

Enterprise users demand enterprise performance no matter where they are. They need to access their application and data when and wherever they may be. And from the users’ point of view the Internet is like one large WAN.

However, according to the Gartner group, the Internet will not be as reliable, secure or consistent as a private WAN until beyond 2007. Which is something that quite rightly concerns IT managers. At the same time however, Gartner also estimates the internet is underutilized from a corporate sense and that by 2007 the internet will be good enough for 100% of enterprises B2C traffic, 70 percent of their B2B traffic and more than 50% of their corporate WAN traffic.

Either way there are a large number of organizations out there today looking at integrating the internet completely into their Enterprise architectures, not just for point solutions or web sites, but as an integral part of the network planning and strategy.

Advantages of the Internet

The advantages of the internet are fairly obvious:

- **It's ubiquitous – available almost anywhere**
- **Compared to other networks it's very inexpensive**
- **It uses defacto standard technologies. There are very few computers out there without a web browser.**
- **It is easy and simple to use, there is no need to deploy or manage clients, and no need to train users on how to use the technology.**
- **Browsers and web enabled applications come with auto-update capabilities dramatically simplifying the tasks of deployment and management.**
- **There is no shortage of applications built to exploit the power of the internet; indeed most commercial enterprise applications have a web enabled "version".**
- **The Internet supports a wide range of devices, from computers to cellphones to PDA's to custom devices.**

So, it's cheap, easy to use, solves a whole range of support and manageability issues, and is compatible with most enterprise applications and devices... But it is nevertheless still a public network... which all of the challenges that public networks have.

Challenges of the Internet

The biggest issue with the internet is Security. The internet is not safe. It's a public network, the public can see the traffic that goes over it, and that traffic can be intercepted, read, re-routed, spoofed, changed etc. And because it is public, the Internet also provides a means of access to the enterprises "private side", which in turn puts the organizations intellectual property at risk.

Fortunately there are technologies that can resolve this; Firewalls protect the perimeter and virtual private networks (VPN's) are used extensively to turn the "public network" into a "private" one.

The Role of VPN's

VPN technologies today solve the privacy, integrity and access control issues related to the internet security.

Privacy is solved through encryption, ensuring that data cannot be inspected while in transit. Integrity is solved in much the same way, through use of the appropriate encryption algorithms it is possible to validate that the data has not been changed in any way during transit.

Access control is provided through a combination of authentication methods ranging from device level authentication, username and password, the use of 2 or 3 factor authentication tools all the way through to biometrics.

The Most Common VPN Technologies are IPsec and SSL

IPsec virtual private networks provide heavyweight tunnels from server to server. IPsec VPN's involve the installation of a client on the accessing machine and can be complex to deploy. They are used mostly for connecting networks across the internet (i.e. corporate office to branch office connections), and occasionally to connect networks to external personal computers, and they require an additional "hole" to be made in the firewall to allow the tunnel to pass.

SSL is ubiquitous and is already installed in most user systems today and doesn't need a client to be installed. It offers up to 168-bit encryption, (and TLS, the upgrade to SSL, includes even stronger encryption modes), providing a simple and secure way to enable access between internal servers and from internal to external computers.

Is SSL, By Itself Enough

The simple answer here is that by itself - No.

SSL has been deployed globally enough for us to say that it really can solve the security challenge that the internet brings. And yet the average SSL remote access implementation is still under 200 users ... there are lots of them out there, but very few at a true enterprise scale. So clearly there are other issues that are preventing enterprises from truly integrating the internet into its architecture...

In addition to security there are a number of other challenges that have to be met before the Internet can really be viewed as an extension to an enterprise WAN.

SSL doesn't scale very well.	The encryption / decryption /authentication workload that SSL imposes goes up with traffic, and consequently SSL doesn't scale very well. Even when using dedicated appliances to handle this traffic.
Application Performance.	The architecture of the internet imposes a certain amount of latency to the traffic, which the application hasn't necessarily been built to handle – consequently there is inevitable application performance degradation, which can make its performance unacceptable to the enterprise.
Unfamiliarity	Most web-enabled applications have a completely different look and feel from their "enterprise" versions. Sometimes it is not possible to provide the same functionality in a web version that is available in the standard version. A classic example of this is the web-enabled outlook when compared to the "standard" version.. I know which one I prefer to use. Members of the enterprise use the standard versions at their desks, and want to continue to doing the same when traveling or remote.
Legacy and proprietary applications.	While most enterprise applications are, or soon will be available in web enabled versions – it's still only "most". Before the internet can be viewed as a WAN extension it needs to be able support ALL the enterprise applications out there.

Bandwidth management	The Internet is a public network.. with all of the gronks and bottlenecks that come with that. In order to support all applications, it needs to find a way of dealing with bandwidth intense applications that work better over a layer 3 type connection.
End unit control	Uncontrolled access is always dangerous. A corporate road warrior today may be accessing his/her applications and data through a variety of different systems i.e. the corporate laptop, their office system, their home system, a web kiosk, a partner / customer computer etc. These “non corporate standard” computers could pose a potential risk to the enterprise through lack of virus protection, or if the protection is out of date, or if they use a personal firewall, etc. etc.
Client / Server applications	By their nature client server applications are not “web-friendly”, and comprise a significant proportion of the enterprise applications.

These limitations explain why SSL as a remote access technology has been typically limited to specific applications or specific user groups and not as a true enterprise technology for remote access.

What’s Missing in SSL

Before SSL can be considered as a viable enterprise remote access architecture it needs to grow beyond the privacy, integrity and access control role, and add features and capabilities that resolve the challenges identified above.

To fully resolve the challenges an enterprise SSL VPN solution will need to incorporate features and capabilities that:

- **Add additional security**
- **Improve the end user experience**
- **Extranet Capability**
- **Supports ALL enterprise applications**
- **Makes it truly scalable to meet the full needs of the enterprise.**
- **Interoperate seamlessly with current network infrastructures.**

Additional Security

End User Security: A corporate road warrior could potentially access his/her applications and data through a variety of different locations and computers. Allowing only “corporate standard” devices to access the enterprise infrastructure is a common way of controlling both the support calls and also mitigating against the risk of attacks. *To be considered a true Enterprise VPN, a SSL solution must be able to scan systems attempting to link up to the network, validate them against the defined corporate standard and take appropriate action if they don’t stack up.*

This action could be something as simple as redirecting the connection to a site where their virus protection could be updated (or installed), or limiting access to a specific subset of the environment that has its own built in protection.

Let's face it, not all systems are going to be corporate standard. And being denied access to applications or data because of this is not something that users (or organizations) in today's dynamic world can really accept.

Virtual Desktop Security: This can be done by creating a virtual work area on the users PC that doesn't link into any areas of the PC environment that it cannot scan for threats or control. i.e. create a working sandbox. Once the session is complete the sandbox needs to be disassembled, and all traces on the connection deleted, such that no files are left on the non-standard device, and nothing remains in cache or other temporary files. *Therefore a true enterprise remote access solution needs to be able to isolate and control the connection between the users PC and the network and ensure than no unauthorized information is left behind.*

Incremental Firewall Support: One of the valuable attributes of SSL is its ubiquity and ease of use. However, sometimes the greatest strength is also the greatest weakness - and this is certainly the case here.

SSL is a standard technology, and as the traffic is encrypted and therefore cannot be inspected, most firewalls simply pass SSL traffic straight through. This has the virtue of simplicity but means that SSL traffic doesn't get the "normal" firewall protection.

This makes the corporation vulnerable to many attacks based on content especially those where the remote machine has been infected by a worm or virus which sends malicious requests in to the corporate network every time the user connects. The infamous Nimda virus used "cmd.exe" to exploit vulnerabilities on Windows machines.

SQL Worm used UDP open ports to take control of machines on the internal network.

Other potential attacks include DDos attacks, IP Spoofing, attempts to create buffer overflows on the backend servers by sending them requests that are much longer than they are designed to handle, or an ill-behaved employee trying to browse around the corporate network looking for information that they may not have access to by using techniques such as forceful browsing.

Any form of tunneling either SSL or IPSec allows requests into the corporation without inspection for these vulnerabilities. *Therefore a true enterprise remote access solution needs to be able to provide the firewall support that the nature of tunneling negates. In order to effectively protect the enterprise standard defensive firewall capabilities have be available the moment that decryption takes place.*

Extranet Capability

The term “Extranet” while not used quite as much today as it used to be, almost every organizations has at least one, and it comes with very specific access challenges.

Used to connect partners of all descriptions to an enterprise, Extranets pose four very real challenges to any organization over and above those solved by the VPN (Privacy, integrity and access control).

1. Must be clientless

The corporate IT organizations do not control the partner’s computer. Which means that deploying a client based VPN becomes very difficult for the corporate IT organizations. And if we take the case of a consultant group for example, where a given consultant may be working with many organizations, he or she could not install multiple VPN clients on their system and expect things to work.

Therefore an enterprise level remote access solution must “standard” and clientless.. A perfect fit for SSL.

2. The two “connected” environments must be isolated.

The corporate IT policies are not the same as the partners.

For a corporate IT organization, there are no guarantees that the level of protection employed on a partner environment will meet the standards that the corporation employees. And even if they do, there is no guarantee that virus protection will be maintained, or that backdoors into the partner’s environment may not be inadvertently opened over time.

Therefore a true Enterprise SSL solution will need to be able to isolate the two environments from each other, while at the same time providing the needed application access.

3. Must be able to limit access to specific applications and data, with different security implementation for different classes of partners.

Partners only need access to the applications and data that the organization deems necessary to optimize the partnership. And today’s legislative environment means that this compartmentalization is not only necessary for business, but it may be necessary by law. With different security and access requirements for different classes of “partner”

Therefore a true Enterprise SSL solution will need to not only restrict access to those specific application or data elements necessary, but also be capable of implementing different security rules for different classes of users.

4. Must be able to support client server and “legacy” applications.

This is one of the most difficult aspects of an Extranet environment. On one side, as we have discussed, this must be a clientless environment which is ideally suited to SSL. On the other side not all enterprise applications are clientless.

Some applications must use a client to work. Other applications will be older ones that are not SSL ready. While others might be custom applications.

Therefore a true Enterprise SSL solution must be able to support all applications, whether a client is needed or not.

5. Must be easy to set up, manage and tear down.

We live in a very dynamic world. Today's partner may be tomorrow's competitor and back to a partner on Friday. If an extranet solution is complicated to set up and manage it becomes unworkable in the real world.

Therefore a true Enterprise SSL solution must be simple to set up, manage and deploy.

The End User Experience

Any network imposes some kind of penalty to an application, and the internet is no exception. Additionally enterprise applications tend to be built and tuned for a standard enterprise environment, and the additional latencies occasioned by the internet can cause timeouts, and forced refreshes dramatically reducing an applications performance.

People are generally smart individuals, and when faced with unacceptable application performance they find ways of not using the application. *Therefore a true enterprise remote access solution must be capable of actively improving an applications performance at the end user machine.*

Some applications require a great deal of bandwidth to perform adequately, and while the internet is ubiquitous, it is not yet at the stage where you can rely on having access to all the bandwidth you need when you need it. *Therefore a true enterprise remote access solution must be capable of managing bandwidth such that bandwidth intense applications will function adequately.*

Be Truly Scalable

In general SSL remote access solutions do not scale very well. The encryption, decryption, authentication and security policy workload increases with the number of users and number of applications the remote access solution needs to support, which creates challenges for any VPN technology including SSL - even when using dedicated appliances to handle this traffic. *Therefore a true enterprise remote access solution must be capable of scaling to enterprise level requirements.*

Summary

The internet is slowly but surely intruding into the life of the enterprise, but the current standard SSL remote access solutions do not meet the needs of a true enterprise VPN and until it they do, SSL will be limited to point solutions involving specific applications or specific user groups.

In order to be considered a true Enterprise level remote access solution the SSL VPN will need to

1) Add additional security

- a) Client side security:
 - Scan systems attempting to link up to the network, validate them against the defined corporate standard and take appropriate action if they don't stack up.
 - Isolate and control the connection between the users PC and the network and ensure that no unauthorized information is left behind
- b) Application Firewall:
 - Provide additional standard defensive firewall capabilities the moment that decryption takes place. These should include protection against worms, and the more common attacks like buffer overflow, forceful browsing and DDos attacks.
- c) Access control:
 - Isolate the two environments from each other, while at the same time providing the needed application access.
 - Not only restrict access to those specific application or data elements necessary, but also be capable of implementing different security rules for different classes of users.

2) Improve the end user experience

- a) Accelerate applications providing improved performance for the end user.
- b) Optimize bandwidth for cost savings and performance and to ensure that bandwidth intense applications will perform adequately.

3) Support all enterprise applications

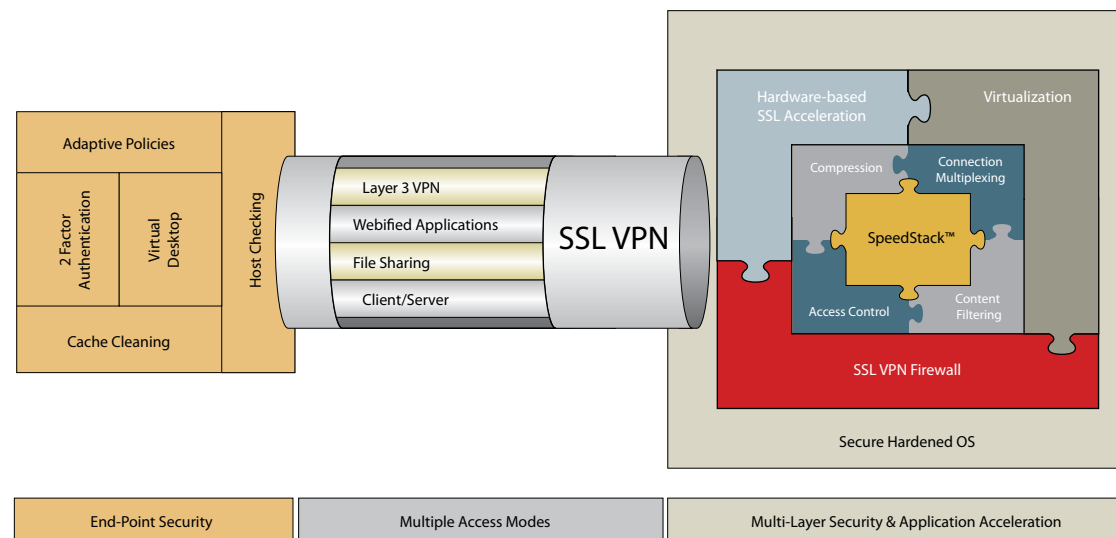
- a) Web enabled applications
- b) File transfer
- c) Client server applications
- d) Legacy applications
- e) Provide direct network access for those who need it.

4) Incorporate enterprise level manageability elements:

- a) Be simple to set up, manage and deploy.
- b) Capable of scaling to enterprise level requirements.
- c) Interoperate seamlessly with current network infrastructures.

In a recent report the Gartner Group identified the market drivers for SSL VPN technology from 2002 to 2004 to be WTS support, application availability, the portal experience and flexible access. However they feel that moving forward, the main drivers for SSL VPN adoption for remote access between 2004 and 2007 will not be the ease of use and simplicity of the appliance but rather the integration of application optimization capabilities including; Compression, Application Optimization, Fail-over methodology, In-site load balancing, and Cross-site load balancing.

Introducing the true Enterprise SSL VPN model



Incorporating client side security, multiple VPN capability, firewall level protection, application and network optimization combined with built in extranet capabilities, breakthrough performance and enterprise level scalability.

It is said that "necessity is the mother of invention" - and this is certainly true in the high tech world, where nothing stands still for too long. The capabilities described in this white paper are not theoretical. They exist and are available today, and savvy organizations are using them to incorporate the internet as an extension to their WAN and build a true enterprise level SSL remote access architecture.

See www.arraynetworks.net for case studies and more information on this growing market trend.

About Array Networks

Founded in 2000, Array Networks is a leading provider of high-performance, secure universal access solutions. Array delivers product lines that address the rapidly growing SSL VPN market as well as the application acceleration market. More than 500 customers including enterprises, service providers, government and vertical organizations in healthcare, finance and education rely on Array to provide anytime, anywhere secure and optimized access. Array provides the world's fastest and most scalable SSL VPN products on the market today. Array's technology performs 8 times faster and scales 12 times higher than its nearest competitor. As a result, no other company can deliver high-performance SSL VPN solutions at a comparable cost. Array has been recognized by industry leaders including Deloitte, Red Herring, and Synergy as a market and technology leader.

Array is headquartered in Milpitas, California with sales offices around the world. The company has approximately 60 resellers and VARs worldwide.

For more information, please visit www.arraynetworks.net or call **1-866-MY-ARRAY**.