Security Bulletin: Volume One

Are SSL VPN's Really Secure?

by Glen Deskin, SE Manager Check Point Software

SSL VPNs are gaining in popularity for use in remote access to corporate networks. This is primarily due to the fact that unlike IPSec VPN solutions, SSL VPNs do not require the installation of software on the remote computer and use an Internet browser capable of SSL as the remote access client. But the ease of deployment to remote users has several trade-offs. One is the lack of endpoint control. The very idea of a "clientless" solution means that you typically have no control over whether or not the remote computer meets security standards and is safe to connect to your network. Remote workers can pose a greater security threat than those working in the office because they typically use their own computers. Many times these machines are attached to home networks, making it impossible to enforce any type of policy or configuration standards.

Another often overlooked shortcoming of many SSL VPN products is the lack of protection of the network for which it's providing access. Since the browser connects to the SSL VPN gateway over encrypted session, it's impossible for the corporate firewall to have visibility inside the packets; effectively a hole is poked right through to your corporate network, leaving you to rely on your SSL VPN gateway to protect your network. More and more attacks are being mounted against application vulnerabilities and when you have an unsecured remote user connecting to your corporate network it's easy for attacks to ride the VPN tunnel right in past your corporate firewall. A good SSL VPN product will provide protection for application layer attacks against the systems for which it provides access.

Last but not least is the problem of sensitive data being left behind in the form of cookies, URL histories, user credentials, page caches and files captured on SSL VPN endpoints such as Internet kiosks and home computers. When implementing an SSL VPN look for a product that provides a mechanism to encrypt and/or delete this type of information when the session is closed.

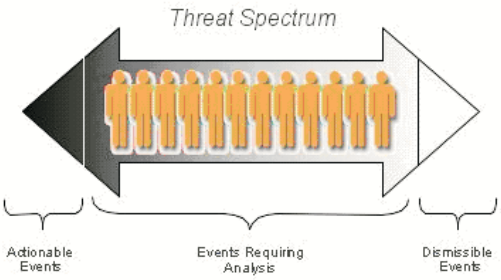
SSL VPNs can be a convenient and easy way to provide remote access to large numbers of users and even business partners, but implementing a solution without careful consideration of these items can put your network at greater risk.

The very idea of a "clientless" solution means that you typically have no control over whether or not the remote computer meets security standards and is safe to connect to your network.

A Revolutionary Shift to Real-time Network Defense

by Martin Roesch, CTO Sourcefire

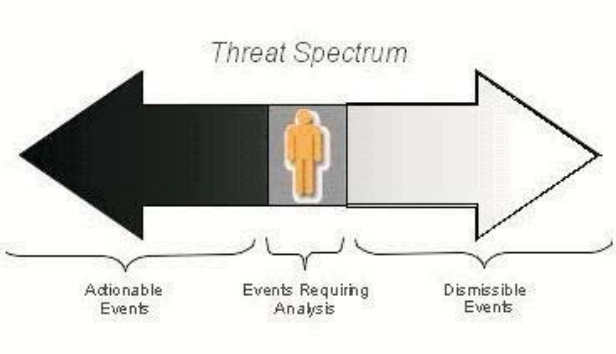
Today's reality is that traditional security tactics aren't effectively defending corporate assets – a new approach is long overdue.



The fact is that when looking at the spectrum of threats there is a vast area to consider. If we draw the threat spectrum in shades of grey, we have known threats requiring action at the black end and dismissible events at the white end. The threats at the black end of the spectrum are known to be dangerous; they can cripple a system or render it useless in a moment. The threats at the white end of the spectrum, while real, are generally dismissed as a nuisance. The threats in the middle are those that require detailed analysis to determine their actual impact to your business and how to properly respond. These threats require tremendous resources to actually find out which problems are critical to address and which threats can be ignored.

First generation intrusion detection and prevention devices do not effectively address these "grey area" threats – they are simply noise generators. The problem lies in the fact that these systems are completely dependant on people. A fundamental lack of information leads to a great deal of ambiguity – sensors operate with virtually no compositional knowledge of the network components they are defending. They require individuals to investigate and analyze each threat, determine where it lies on the spectrum and then how to best address it. This "man-in-the-loop" approach results in a significant cost to implement, maintain, and staff while introducing significant delays to resolution.

A technology that can provide awareness of the network to these systems in a real-time manner is needed. This awareness is critical to automating the response to change and protecting networks from all threats in the spectrum in real-time.



With Real-time Network Awareness, security systems can be automated to determine the impact of each threat and take the appropriate action to defend the network. This added context significantly reduces the number of events requiring human involvement – while offering faster, more effective response to critical threats. Real-time network awareness provides the foundation for a revolutionary new network defense strategy.

With a real-time network defense strategy based on pervasive network context, potential network weaknesses are proactively identified and risks are removed well before they are exploited...and attack and threat management solutions are poised to quickly respond, mitigate and remediate attacks from all threat vectors. By bringing contextual awareness to the intrusion prevention landscape, organizations are able to more confidently block known attacks before they can cause damage.

Controlling Spyware: A multi-pronged approach

by Sam McClane, SE Manager Blue Coat Systems

Spyware is easily the largest security concern faces the enterprise today. The issues created with spyware infestations in man-power and network resource usage can eat through an entire IT budget for a year without much room for success. While there are several approaches to dealing with the spyware issue, the best approach is to have multiple levels of defense and a sound policy for access to internal resources for mobile users.

Most users today will have several desktop packages to eliminate spyware from their desktops, and most enterprise vendors of desktop anti-virus are updating their products to deal with the spyware issue, and while this approach is good, this method is reactive, and if the user does not realize they have spyware, then they usually do not run these programs. Gateway spyware prevention is a method to prevent the download and installation of spyware before it can grab hold of a desktop. Gateway protection generally involves at least 3 different types of protection, url blocking by category, gateway anti-virus, and gateway content security, the removal of active components and files that are malicious in nature.

Url blocking by category, also known as content filtering, has been around for years and is the simplest way to limit the penetration of spyware within an enterprise. Pornography, gambling, P2P, and online gaming sites are the largest group of spyware installation sites. By preventing access to these sites, spyware installs can be reduce by as much as 70%, depending on the quality of the category list and on the strictness of the policies at the gateway. Since many of these sites change domain names and IP addresses weekly if not daily, this approach is not as effective as one would hope. Most new sites, used along side a spam attack, wind up in the dreaded unknown

category along side many B2B sites and valuable resources that are not popular enough to get categorized.

The second tier of gateway defense, virus scanning, prevents infestation further by scanning the allowed web content for viruses and spyware. The antivirus industry has recognized this and all major vendors are adding spyware definitions to their a/v signature files and as the spyware defense industry matures, as did the anti-virus industry these signatures will get better. The key to successful gateway A/V is speed. Most gateway A?V implementations are removed before they have a chance to be effective because of the change is end user experience. The goal of any gateway A/V project should be to not change the user experience during implementation. The mantra of any successful a/v solution should be, We could not tell it was there.

Content security is last line of defense against spyware installation and it involves the most thought. Blocking and replacing active content and files by extension or mime-type can provide the most security of any of the tiers of gateway spyware prevention. It also has the greatest impact on the end user web experience. Downloading executables and DLL's from unknown or uncategorized web sites is a recipe for infestation and should be denied. But as mentioned previously, many B2B and partner web sites are not porpular enough to be categorized. By utilizing white lists, allowed web sites, and categorization, the impact of the technique can be limited and controlled. Any such content security solution should have the granularity neccessary to implement such policy and flexability to adapt to new installation techniques and attacks without wholesale software upgrades.

Finally reporting on web activities will also prove to be a vital tool for any spyware solution. The ability to report on who attempted to download spyware, as well as the ability to report on who has spyware installed by targeting the "spyware phone home" sites as well as the spyware applications (Gator, hotbar, etc) can provide a quick hit list for desktop cleansing. Even better still is the ability to have such user quarantined until they can get cleansed, with notification being sent tot he enterprise security management system.

Spyware defense and irradication requires multiple levels of procedures and products to be effective. By combining desktop, gateway, and reporting systems into a cohesive soltution most enterprises find they can reclaim the lost man hours and bandwidth currently used to deal with the problem. As spyware vendors adapt to current solutions, flexibility and granularity of any solution will help win the battle to prevent and remove spyware from the desktop.

Develop a Routine and Stick to It

by Don Poorman, CTO Evolution

So often network managers and system administrators get caught up in the chaos that comes with their jobs, fundamental items that should be reviewed on a regular basis are often forgotten. Step back for a second and ask yourself – when was the last time you reviewed firewall logs, event viewer messages, the existing configurations, or other byproducts of the systems you've implemented to protect your IT environment?

Strong IT system security, or security in general for that matter, should be mired in a consistent and disciplined review of possible trouble indicators as they relate to vulnerabilities. This mentality even outside of the IT world is why you guards in high security buildings walk in shifts to check if doors or locked or sentries pace back and forth in front of a gate. Don't make the mistake one of our customers recently did in assuming his antivirus software was working, since it was configured to update and scan every night and he hadn't witnessed an outbreak. Upon further investigation on another project, it was discovered a core software patch delivered to the antivirus product three months earlier had corrupted the whole definitions list and was constantly out of date, thus ineffective. Luckily, the software was fixed and only a few rogue trojans were found.

Take 20 minutes per day over a cup of coffee to review what your IT security systems are telling you – what you don't know CAN hurt

For more information on any of these solutions contact us: info@goevolution.com