

Protecting Your Boundaries: Why Clientless VPNs Are Not Worth The Risk

Abstract

Virtual Private Networks (VPNs) allow corporations to link together disparate portions of their Information Systems by 'tunnelling' their inter-site traffic over the internet in an encrypted form. Virtual Private Networks have traditionally required the use of dedicated, complementing software gateways that encrypt and decrypt the traffic leaving and entering the internal network segments. These software gateways have been implemented in large network firewalls and small 'client-based' software packages. VPNs from workstations, such as laptops, used by remote workers connecting to a corporation's Information System over a traditional VPN are usually referred to as Client- Based VPNs, due to the dedicated software required on the machine.

Recently, the Secure Socket Layer (SSL) technology, used in e-commerce to encrypt the traffic between a web browser and a secure web server, has been employed to create a new class of VPN known as an SSL-VPN. These SSL-VPNs do not require special software on the remote worker's workstation as the encryption and decryption software is included in all popular web browsers. This has led to VPNs from workstations used in this fashion becoming known as 'Clientless VPNs', due to the lack of any special VPN software on the client.

Where Client-Based VPNs require the remote workstation to be configured, and therefore managed and owned, by the corporation, Clientless VPNs can be established from any internet-connected workstation equipped with a modern web browser. This papers discusses the security implications of employing such technology within an enterprise Information System and suggests that the security concerns outweigh the potential management advantages.

1 Introduction

Historically, corporations linked together Information Systems at disparate sites through the purchase and use of private long-distance wiring. This wiring could be viewed by the corporation as an extension of their own network infrastructure, entirely under their own control, and impenetrable by outsiders. Each end of the private wires would be connected to company-owned IS infrastructure, controlled and managed by either a central head office, or through a partnership between the systems' administrators at each of the ends. These network links were often provided by a telephone company through the allocation of a switched circuit that guaranteed, to a reasonably high degree, the confidentiality and integrity of the data that traversed it.

The introduction of Virtual Private Networks (VPNs) has allowed corporations to move away from these expensive dedicated links to 'virtual network' links, often implemented by encrypting traffic sent over a shared network, such as the internet. Virtual Private Networks simulate private wiring circuits in the sense that each has two end-points, both in spaces controlled by the company, connected to disparate segments of the corporation network. Where private circuits consisted of 'frame relay' packets traversing a portion of a shared circuit-switched network, VPNs consist of encrypted Internet Protocol (IP) packets traversing a portion of the shared internet. The most popular VPN protocol is IPSEC, developed by the Internet Engineering Task Force (IETF), for the specific purpose of providing Virtual Private Networks over the internet.

2 Client-based or Clientless?

Traditional VPNs require special software at each end of the virtual link to encrypt and decrypt the traffic traversing the shared network. In the case of site-to-site VPNs this software is usually provided as part of the internet firewall at each of the sites; in the case of remote access VPNs this software is usually provided as part of the internet firewall at the company end and by a dedicated software package at the remote worker's end, installed on their company laptop or workstation. Due to the requirement of this special software, the remote worker is usually constrained to only being able to access the company's Information System via a company-owned laptop or workstation.

This constraint provides a specific level of security to the company IS by restricting the processing and storage of company information to equipment owned and managed by the company. This specific security manifests itself in the form of approved up-to-date virus checkers, company installed workstation firewalls, and the protection of the confidentiality and integrity of stored company data due to its storage on only approved assets. In contrast, the perceived drawback of the traditional remote worker VPN is the cost and overhead of managing the remote workstation, mainly due to its geographic and perceptual separation from the company systems' administration staff.

The recent alternative to these Client-Based VPNs is the Clientless VPN, based on encryption software included within modern web browsers. The Secure Socket Layer (SSL) technology used in e-commerce to encrypt a session between a web browser and a web server, usually for the passing of payment details, has been developed to provide web-based VPN services that do not require special software to be loaded on the remote workstation. The company end of the VPN tunnel exists within a web server protected by the company firewall, and the remote workstation end of the tunnel exists within the remote web browser.

The deployment of these SSL-VPNs allows any standard internet-connected workstation to become the remote end of the VPN tunnel. This reduces the cost and overhead of managing the remote workstation due to its comparative simplicity. The only software required to be maintained on the remote workstation is that involved in providing an internet connection; software which is often already managed by the remote workstation user.

The security drawback with Clientless VPNs is this lack of management of the remote workstation and the potential for the remote workstation to effectively be any of the workstations on the internet, including the small amount owned and managed by the company and the very large amount that are not. The following sections discuss the security implications of deploying SSL-VPNs.

3 Which Workstations?

Deploying remote workstations is a complex issue for most organisations: How should the workstations connect to the enterprise? Who should have access to remote workstations? Where should the remote workstations be used? What management overheads will there be? What security issues need to be considered?

The what, how, who, and why of remote workstation deployment is outside of the scope of this paper, which will concentrate purely on the security implications. An organisation needs to consider which workstations it will allow to connect to its enterprise information system.

Traditional client-based VPNs require the remote workstation to be installed and configured with dedicated VPN workstation software. In these cases, the systems' administrators of the enterprise IS can control which workstations are allowed access to the enterprise. With clientless VPNs, almost any workstation may be used by the remote worker as almost all workstations are installed with the required software, a modern web browser capable of SSL encryption (that used to facilitate e-commerce).

If an organisation is to deploy clientless VPNs it will need to identify classes of workstations it considers suitable for connection to the enterprise. If the security policy is not explicit, or is not understood or followed, then remote workers may theoretically use any workstation at their disposal. These may include:

- Workstations allocated to them by the organisation, under the management of the organisation;
- Workstations owned by the remote worker, managed by themselves;
- Workstations available at an 'internet café', under the management of the internet café;
- 'Kiosk Workstations' such as those available at airports and hotels, under the management of the kiosk provider.

Technical controls for limiting which workstations may be used are discussed in section 6 below. Procedural controls may be implemented through security policies although it should be noted that without the required technical controls these may be difficult to police.

4 Commercial Confidentiality Issues

The ability for a remote worker to establish a VPN into a company's enterprise IS from a workstation that is not controlled by the organisation introduces a number of security issues. These include:

- Any files downloaded by the remote worker will reside on a workstation that is not protected by company-endorsed technical controls. These files may be compromised by:
 - an internet-based attacker, attacking the workstation being used;
 - another user of the workstation if the files are accidentally left and not deleted;
 - another user of the workstation if the files are recovered from deletion;
 - a virus that has infected the workstation;
 - a trojan horse maliciously or accidentally planted by another user of the workstation.
- Any temporary files created during the session may be recoverable by others with access to the workstation, such as other users or internet-based attackers. These temporary files may include the content of any files downloaded, the content of any internal web sites visited, or the content of any emails sent or received by the remote worker.
- A man-in-the-middle attack may be effected by either the administrator of the remote workstation, or a local or internet-based attacker. A man-in-the-middle attack consists of, in this case, directing the web browser to connect to an intermediary web server instead of the one requested. This intermediary will make a connection to the requested web server and relay all traffic to the web browser while copying some or all of the content. Man-in-the-middle attacks are often undetectable by both the client and the server and, in the case of SSL connections, have the potential to view all traffic unencrypted as the intermediary is effectively the end-point of the encrypted tunnel to the browser, and also the start-point of the encrypted tunnel the web server.
- The remote worker's session may be monitored by either the administrator of the remote workstation, or a local or internet-based attacker, through the use of special monitoring software. The monitoring of a session may include all content entering or leaving the browser or, indeed, real-time graphical session monitoring where the desktop is mirrored to an attacker's workstation. Monitoring of a workstation owned by a third party may be

undetectable by both the remote worker and the organisation's systems' administration staff.

While SSL-VPN vendors have developed solutions to some of these issues, such as the provision of a 'virtual shredder' to aid a remote worker in the deletion of their downloaded information, it is clear that some of these security issues have not yet been countered. The protection of the session and downloaded information on an uncontrolled workstation is practically impossible to provide while the session is active. Information is downloaded and stored in an unencrypted form as this is the only form that is accessible to the web browser and office tools. While most vendors concentrate on the removal of this information once the session has ended, none appear to provide any protection for this information during the session.

Internet hackers, spies, and criminals may easily target public access workstations in order to 'fish' for whatever information a remote worker has access to. While it is true that one would need to be unlucky to be compromised in this fashion, luck has never been regarded as a reliable tool in risk management. It should be noted that in most of the threats listed above, the remote worker will be unaware that they have been compromised, implying that one will not know when the luck has run out.

5 Legal Implications

Where the confidentiality of commercial information is at risk, legal implications are also likely to exist. Any organisation that stores or processes personal information is subject to the Data Protection Act and the Human Rights Act. These acts establish a legal requirement for organisations to provide adequate protection for the information covered by the acts.

If such an organisation deploys a remote worker solution that allows the remote workers access to information subject to these acts, whether or not it is part of their job to access this information, then it is the responsibility of the organisation to provide adequate controls to protect this information when it is stored or processed on a remote workstation. If the deployed remote worker solution allows the remote workers to use an uncontrolled workstation then it is likely that these controls can not be technical by nature and therefore may be impossible to implement successfully.

It is suggested that where legal implications exist in relation to the information stored or processed by an organisation that these implications are considered in every aspect of the design of the Information System. Where an Information System extends beyond the traditional boundaries of the corporate enterprise to include remote workers, then the legal implications tend also to extend. An organisation that is prepared to accept a risk to the confidentiality of its own information is still required to provide adequate protection to information covered by the acts.

Claiming in court that the organisation was 'unlucky' is unlikely to remove the burden of responsibility and the relevant consequences.

6 Potential Solutions

It should be understood from the discussions in sections 4 and 5 above that there are a number of serious security issues inherent in the use of clientless VPNs. For organisations that wish to make use of SSL-VPNs there needs to be methods of combating these security concerns.

The major issue with clientless VPNs is entirely the lack of client software required to operate them, which is precisely the benefit that they offer. In order to effectively secure a clientless VPN one needs to constrain which workstations may be used to establish the VPN. Only workstations that afford the required security should be allowed as any others introduce a risk of unknown proportions.

It is recommended that organisations mandate that only company-owned equipment is used when connecting to the enterprise over a clientless VPN as this is the only means by which the organisation will be able to adequately identify and quantify the risk associated with the remote workers. Any workstation not owned or managed by the organisation may exhibit the vulnerabilities identified in section 4, mainly through not being shown to meet the baseline security requirement of company IT assets.

If an organisation wishes to make use of procedural controls to ensure that remote workers only use company managed equipment when connecting to the enterprise, then the organisation will need to place trust in its remote workers not to abuse their freedom of workstation choice. It is recommended, however, that these procedural controls be augmented with technical controls to ensure that they are followed. Potential technical controls include:

- Restrict access to the SSL-VPN web server to IP addresses known to belong to company workstations. This control is difficult to implement as a workstation may be identified by many different IP addresses at different times depending upon how and where it connects to the internet. Dial-up access usually results in a dynamically allocated IP address so any workstation that needs to connect over a dial-up link, as many remote workers often need to, will not be able to be identified by its IP address.
- Restrict access to the SSL-VPN web server to MAC addresses known to belong to company workstations. While this may work for workstations that connect via an ethernet network card, it will not work for workstations that connect over a protocol that does not use MAC addresses, such as PPP used in dial-up connections.
- Restrict access to the SSL-VPN web server to workstations that can demonstrate possession of a signed digital certificate. While this will limit the connections to those made by people and workstations in possession of a valid certificate, this unfortunately does not limit the connections to specific workstations as the certificate, along with the rest of the configuration, is transportable to any other machine that can run the same software and, as the software required is a modern web browser, this means almost any machine.

The unfortunate truth of securing clientless VPNs is that the clientless nature of the remote end-point means that any workstation can effectively be the remote end-point. If no special software is required and configuration (and username and authentication) holds the key to a successful connection then while these are transportable between workstations it will be impossible to limit connections to specific workstations by technical means.

7 Conclusion

Clientless VPNs (SSL-VPNs) have an inherent security vulnerability which poses a risk to any organisation deploying them to facilitate remote worker access. At present there do not appear to be any technical solutions to mitigate this risk, although procedural controls may provide sufficient security in some instances.

The major vulnerability with clientless VPNs is their ability to be facilitated by any remote workstation. To secure a clientless VPN, an organisation has to limit the workstations that may be used to those approved by the organisation.

It should be noted that if a remote worker is to be constrained to establishing VPN access from a single workstation that is provided, owned and managed by the organisation, then one should question the benefits gained from the use of a clientless VPN. If the ability to establish a VPN has been limited to one workstation, then the only benefits of the clientless VPN are the removal of the need to install and maintain a VPN client, and the costs associated with this.

The security risks to an organisation arising from the use of clientless VPNs are the ability for a remote worker to cause the compromise of the confidentiality of company information through the unapproved use of non-company workstations. Employees who are not fully aware of the security risk they may be causing may occasionally (or often) break this rule out of a simple desire for convenience. It is unlikely that an organisation would be able to log this usage until the related breach occurs.

For the small benefits of offer, clientless VPNs are simply not worth the risk.

The Author

Kevin Sheldrake MIEE CISSP is an Information Security Consultant at VEGA Group PLC. He is registered with the CESG Listed Advisor Scheme, is a certified CESG CHECK Team Leader, and is a Certified Information Systems Security Professional (CISSP).