

Winfrasoft VPN-Q 2006

White Paper

Secure Remote Access – IPsec VPN with quarantine vs. SSL VPN

Author: Phillip Nicklos
Reviewers: Steven Hope
Published: December 2006
Applies to: Winfrasoft VPN-Q 2006
Web site: <http://www.winfrasoft.com>
Email: support@winfrasoft.com

Contents

| | |
|---|----|
| Executive Summary | 3 |
| SSL VPN | 3 |
| What is a SSL VPN?..... | 3 |
| Secure Sockets Layer detail | 3 |
| The SSL VPN client | 4 |
| SSL VPN Issues | 4 |
| Limited Application access | 4 |
| No offline access..... | 4 |
| Expensive..... | 5 |
| No mutual authentication..... | 5 |
| IPsec VPN | 5 |
| What is an IPsec VPN?..... | 5 |
| Common Misconceptions of IPsec VPNs..... | 5 |
| IPsec does not work with NAT (Network Address Translation) | 5 |
| IPsec Firewall traversal may be blocked | 5 |
| SSL VPNs are clientless | 6 |
| Interoperability issues between IPsec Vendors | 6 |
| Increased security risk for remote access via IPsec VPN | 6 |
| Client side configuration changes are required for users who do not have a Static IP address | 6 |
| Client software must be configured for all manner of access devices | 6 |
| IPsec VPNs are only designed for site-to-site connectivity..... | 6 |
| As client software is required on the remote user's system, management and support overheads become ludicrously expensive | 6 |
| No mutual authentication for PPTP based VPN's. | 7 |
| IPsec VPN with quarantine | 7 |
| What is a quarantine network? | 7 |
| Benefits of Quarantine..... | 7 |
| Characteristics of VPN-Q 2006 | 7 |
| VPN-Q 2006 vs. Microsoft's Quarantine sample using Scripts..... | 10 |
| Complementary technologies | 10 |
| Additional References | 10 |
| Point to Point Tunneling Protocol (PPTP)..... | 10 |
| Layer Two Tunneling Protocol (L2TP) | 10 |
| RFC's..... | 10 |

Executive Summary

As the world's work force becomes more mobile and corporation's boundaries extend over ever increasing geographical locations, VPNs have become a critical part of an organisations Information Technology strategy. Revolutionary government legislation that encourages companies to employ full-time remote workers place an even greater demand on the IT infrastructure. Remote workers, irrespective of their location, often require access to the same resources and functionality available to their headquarter-bound colleagues. Technological advances in broadband and wireless communications facilitates external access at speeds with near local response times. This remote access from anywhere, anytime, using any device must, without compromise, be SECURE.

Securing a network infrastructure housed in an organisation's localised managed environment is a challenge in itself. Maintaining a high-level of security on machines accessing the local topology from a coffee shop or even an airport on some tropical island makes the security question a little more interesting.

Initially, the only viable option for secure remote access was an IPsec based VPN. IPsec VPNs were initially developed to provide site-to-site connectivity. Most vendors created different propriety IPsec implementations for remote client access which did not conform to the ISO standards (RFCs 2401 and 2411) which led to many interoperability issues between vendors.

The Layer 2 Tunnel Protocol (L2TP) protocol (developed by Microsoft and Cisco), combined with IPsec (L2TP/IPsec), mitigated the IPsec tunnel mode limitations and was standards based (see RFC 2661). Unfortunately most VPN vendors chose not to adopt these standards, instead continuing to use proprietary methods which resulted in customers being tied to one solution. A major adopter of L2TP/IPsec was Microsoft, as such the VPN client built into Windows today is standards compliant, however interoperability issues still exist as many VPN concentrators still require their proprietary client to function. A native Microsoft implementation of VPN technologies eliminated most of the original limitations associated with initial IPsec VPN technologies, but adoption was not widespread due mostly to existing vendor tie in and concerns over the security of Microsoft products.

A combination of VPN security concerns and the evolution of web based applications also lead to a new breed of "VPNs" called SSL VPNs, which provide application level remote access based on the Secure Sockets Layer (SSL) protocol. It should be noted that SSL VPNs are not true VPNs as they are not an extension of the IP network. They are, however, another method of remotely accessing internal applications via a web browser.

This document will discuss and compare SSL VPNs and IPsec VPNs with quarantine (using Winfrasoft VPN-Q 2006) in more detail.

SSL VPN

What is a SSL VPN?

From the outset, industry expressed major concerns with extending their strictly controlled internal network to the internet allowing every malicious individual access directly to their systems. Thus a secure solution was required to address these concerns and give even the most paranoid network manager restful nights.

Secure Sockets Layer (SSL) is a secure tunnelling protocol that encrypts data between a client and server using single direction identification via a certificate. This technology attempts to mitigate a sniffing attack as all data passed between the 2 points is encrypted. In addition to encryption, an SSL Web Server Certificate also provides validation and verification of the remote server identity to the browser client. Merging SSL protocol with VPNs was the supposed answer to all the world's remote VPN access evils.

First and foremost, SSL VPNs are **NOT** VPNs in its true sense. To be considered as a VPN, a technology must perform at least 2 functions: (1) authenticate the end user and (2) assign a remote node an IP address routable on the local network. As SSL is a layer 7 protocol and not a layer 4 protocol, they fail to assign remote nodes IP addresses and therefore cannot be considered as a true VPN solution in networking terms. This nature of SSL VPNs has led some security consultants to refer to them as "desktop-over-HTTPS" as this is effectively the functionality they provide. The term "SSL VPN" is purely a marketing term designed to help a customer understand the functionality it provides, not how it does it.

Secure Sockets Layer detail

Native SSL has a few major flaws that undermine its status as the ultimate platform in a secure solution. These being:

- Certificates shared between clients and servers are provided by the server only, verification for the certificate is automatically handled by the browser and provided the certificate is a valid certificate from a trusted provider and that the certificate is not listed in a revocation list, the certificate is validated.

The issue is that there is no infallible method of confirming that the certificate used in the communication actually belongs to the company that the client believes he is dealing with as the client's trusted root list may not be under your control.



- Secondly, the SSL protocol is reliant solely on the server to provide its identity to the client, but the client does not need to provide any identification to the server. Thus, for a hacker controlling a client device, he can almost positively ensure that the server he is attacking is the correct server, but the server has no idea who the attacker is.

The answer to this problem is mutual authentication, this is the process whereby the client and server validate each others credentials, which is exactly what IPsec was originally designed to do thus it requires certificates on the server and the client.

- It is also possible to perform a man-in-the-middle attack on SSL VPN's if the client is accessing the server via a proxy server. In this case the SSL VPN client must be able to check that it is actually encrypting data using the correct certificate and not just the one presented to the browser. Many SSL VPN solutions don't do this important check.

The SSL VPN client

As in a SSL session, SSL VPN sessions are initiated by a client, typically through a web browser. On establishment of a connection, the server component sends a certificate to the client's devices. The client device will then validate the certificate against a trusted Certificate Authority (CA). As modern browsers cater for certificate sharing and validation automatically, the client requires limited intelligence to establish a connection. The client then provides his logon credentials and authenticates to the server. At this stage, effectively, one has established an encrypted web tunnel between the client and server. As the connection is web based, the type of applications available to the client is restricted. Provided the client's system has a semi-decent browser installed, a session can be established to the company's network, irrespective of the hardware installed at the client site.

The SSL VPN client is typically Java or ActiveX based, although SSL literature may allude to there being no client, a client is required, however small. This client will attempt to sandbox the connection from the rest of the PC to protect the connection; it may also perform some basic port redirection to allow specific applications to function. All of this assumes that the browser used will allow the client to run in the first place. As newer versions of browsers are becoming more secure all the time, this level of functionality can not always be assumed.

SSL VPN vendors tend to utilise Citrix / thin-client type technologies as their silver bullet to access applications that are not supported natively. This may be a nice solution, however, Citrix provide, within their solution, an internal Web access gateway (Citrix Presentation Server) for this very reason thus making a SSL VPN redundant in this scenario. Should you adopt a solution requiring additional technologies, the costs associated with implementing and maintaining the full solution increase exponentially.

In the scenario above, the integrity of the client's system is never questioned. The solution does provide remote access to the company's network from any location using variant devices. Not verifying the integrity of the client's system would be either naïve or negligent. SSL VPNs address this by utilising Java or ActiveX controls that are downloaded to the local system, installed and then run locally. This Java / ActiveX client component is charged with ensuring the client system's integrity. However, determining the specific checks performed by the Java / ActiveX control are, often, not apparent and the comprehensiveness of these checks differ from vendor to vendor. Ask yourself, how comprehensive can a check be from a client that is only a few 100Kb and operates in isolation?

One last point, should the end device not have the ability to run Java Applets or block the downloading of ActiveX components, then connection to the SSL VPN server will not be established. Some solutions can fail back to a basic connection mode in this scenario, but the access provided is often inadequate to perform the required task.

SSL VPN Issues

Apart from just clarifying some of the SSL VPN sales material, we would like to highlight some additional issues with SSL VPN's which are often not mentioned.

Limited Application access

SSL VPNs have limited application compatibility as all applications must either be web enabled or the client control must have been designed to work with the specific application. This means that all internal systems, such as CRM, Financial, HR applications, must be compatible one way or another. Should a client have a key application required by remote users that is not web enabled or not compatible with the Java / ActiveX client, that application would then require modification or replacement. Naturally, this can become a costly exercise and is an unnecessary hidden cost.

SSL VPN vendors sometimes suggest that a Citrix/Thin client based system is implemented to cater for this scenario. However, anyone familiar with thin client implementations will be able to give you an indication of how expensive these solutions can become, which is yet another hidden cost.

No offline access

A major limitation of SSL VPNs is that they do not allow for any form of offline access to data. As all data comes through a web browser, a connection to the SSL VPN must be initiated in order to retrieve any data. This is less of an issue with IPsec VPNs as



many applications natively support offline access, such as email or CRM systems. These applications do not have to be aware of an IPsec VPN as it is a true network layer protocol which leaves the applications to function the way they were designed to.

Expensive

Quite simply, SSL VPNs are very, very expensive. VPN-Q 2006 running on Microsoft technologies which, most likely, is already installed at a customer's site reduces the cost of having a fully functional secure VPN and Quarantine solution for a fraction of the cost of its SSL VPN competitors.

No mutual authentication

No mutual authentication transpires between the client and server components. This is a limitation of all SSL VPN's as, at no stage is the client system requested credentials proving its identity, only the user details are requested. This is a nice feature for potential hackers as the server advertises and verifies who it is thus providing a potential malicious user the knowledge that this is indeed the system he wishes to attack.

IPsec VPN

What is an IPsec VPN?

IPsec VPNs were initially developed to provide site-to-site connectivity using IPsec tunnel mode and didn't, initially, cater adequately for the highly mobile workforce. IPsec VPNs provided limited functionality; primarily because vendors designed proprietary tunnel mode solutions for remote client access, ultimately creating a hybrid IPsec tunnel that never conformed to the ISO standards (see RFCs 2401 and 2411). This also led to many interoperability issues between vendors. These solutions tended to be both difficult and costly to deploy and manage. An addition, the security focus of these solutions tended to be on encryption strengths and cipher algorithms which, while important to an extent, didn't protect the network against the real world threats. Some IPsec VPN vendors saw the value in multi-factor authentication as a way to further strengthen the security proposition, however, authentication alone does not signify the intent of the remote device once connected.

A serious limitation of IPsec tunnel mode was that the IP of both the source and destination must be known in order to establish a connection, however, in a remote client scenario this is not possible – hence the requirement for proprietary extensions. The advent of Layer 2 Tunnel Protocol (L2TP) by Microsoft and Cisco, combined with IPsec (L2TP/IPsec), mitigated the IPsec tunnel mode limitations and was standards based (see RFC 2661). Unfortunately most VPN vendors chose not to adopt these standards, instead continuing to use proprietary methods which resulted in customers being tied to one solution. A major adopter of L2TP/IPsec was Microsoft, as such the VPN client built into Windows today is L2TP/IPsec (Standards based) compliant, however interoperability issues still exist as many VPN concentrators still require their proprietary client to function.

A native Microsoft implementation of VPN technologies eliminated most of the original limitations associated with initial IPsec VPN technologies, but adoption was not widespread due mostly to existing vendor tie in and concerns over the security of Microsoft products.

Over the last few years Microsoft has done more to improve the security standing of its software than any other vendor and the success of Windows Server 2003 and Windows XP SP2 is testament to that commitment. Microsoft has even gone so far as to achieve common criteria EAL4 for Windows Server 2003 and EAL4+ for ISA Server 2004, and introduced VPN quarantine functionality to ISA Server. Winfrasoft's VPN-Q 2006 leverages Microsoft's advancements to provide a comprehensive and secure remote access solution.

Common Misconceptions of IPsec VPNs

SSL VPN vendors often exploit the limitations of the legacy proprietary implementations of IPsec VPN solutions as a sales tactic to sell their devices. As Winfrasoft VPN-Q 2006 is based fully on Microsoft's standards based L2TP/IPsec VPN solutions, the majority of these historical issues are not a factor. Above, we briefly discussed some of the limitations associated with legacy IPsec solutions which have been, and still are, exploited for a SSL VPN vendor's benefit. Some of these vendors claims include:

IPsec does not work with NAT (Network Address Translation)

Microsoft and most other IPsec VPN vendors have implemented an enhancement to the original NAT specification called NAT-T (RFCs 3947 and 3948) which automatically allows IPsec to traverse a NAT device. Thus, this is no longer an issue and is a standards based solution. Microsoft's Knowledge Base article 818043 documents the enhancements to the functionality, including that of NAT-T, of Layer Two Tunneling Protocol (L2TP) and Internet Protocol security (IPsec) on Windows systems. This additional functionality is included in Windows XP Service Pack 2 (SP2).

IPsec Firewall traversal may be blocked

Users with an IPsec client that are accessing the Internet via another organisation's network may be blocked by outbound Firewall policies. This is indeed the case as both PPTP and L2TP ports/protocols may be blocked on the outbound leg. Naturally, whether or not this is the case will differ between organisations, however, the same risk applies to SSL VPNs as the outbound SSL port may



also be blocked at the Firewall – although less likely. Furthermore, many proxy and layer 7 firewalls (such as Microsoft ISA Server) are able to inspect outbound SSL connections and block outbound SSL VPN's while still allowing SSL access to key sites. So while SSL VPN's may have an advantage now, this may be short lived.

SSL VPNs are clientless

Despite most SSL VPN Vendor's claims, technically speaking, this statement is not totally true as most VPN client vendors download a Java or ActiveX control onto the user's local system. The client's system browser must allow Java or ActiveX controls to be installed on the local system for sessions to be established. This functionality is continually being reduced with newer releases of web browsers. There is also an assumption that there will be a web browser available which their typically is in Windows, much the same way that the Windows OS also has a built in VPN client.

Interoperability issues between IPsec Vendors

This may have been true in the past as IPsec VPN vendors created systems that did not conform to prescribed standards and varying proprietary solutions would often not interoperate. VPN-Q 2006 is built to leverage Microsoft's VPN technology that is built into Windows which conforms to the IPsec standards and is therefore not proprietary. The Microsoft solution can interoperate with any other standards based VPN solution and has even been certified by Cisco as a supported client for the PIX firewall when the PIX is configured to use L2TP/IPsec instead of Cisco's proprietary IPsec tunnel mode system. While the SSL protocol is a standard for encrypting HTTP traffic, SSL VPN solutions, are all proprietary and no interoperability exists between vendors. In fact, integrating other software, such as 2 factor authentication systems, is often very tricky for this reason.

Increased security risk for remote access via IPsec VPN

This misconception is due to the direct (non-proxied) access and full network visibility provided by most IPsec VPN vendors. This statement is true to a point, mostly because of the limited functionality provided by SSL VPNs as opposed to their IPsec VPN counterparts. As IPsec VPNs can expose the entire internal network to authorised users if configured to do so, thus all the functionality available to a local user is available to the remote user. This, however, does not always have to be the case as some IPsec VPN concentrators such as Microsoft ISA Server includes a full layer 7 firewall so that limited application filtered access can be provided to remote clients.

Client side configuration changes are required for users who do not have a Static IP address

This is again an issue that existed in the initial stages of IPsec VPNs as static IP's are required by the RFC's for mutual authentication. This problem ceased to be an issue with the creation of the L2TP/IPsec & PPTP VPN's which allowed for clients with dynamically assigned IP addresses to access the VPN. Other vendors used proprietary solutions, mentioned previously, to work around this issue.

Client software must be configured for all manner of access devices

This statement is true. Many vendors required their custom client to create the VPN connection, as does a SSL VPN. The software that analyses the client's systems will vary from platform to platform as security concerns on a Windows Laptop may not be applicable to Linux workstation, and vice-versa. For this reason VPN-Q 2006 leverages the existing security software on the client PC in order to ascertain the security profile. However, SSL VPN vendors maintain that a small Java / ActiveX control, activated through a web browser, is sufficiently capable in ensuring the health of all systems on all platforms without the need to interact with locally installed security software.

IPsec VPNs are only designed for site-to-site connectivity

The initial IPsec VPNs were indeed designed for site-to-site connectivity. However, since the advent of PPTP and L2TP protocols many years ago, the technology has been portable to support a multitude of remote users.

As client software is required on the remote user's system, management and support overheads become ludicrously expensive

This claim has mixed validity. The overhead on maintaining client software depends on the nature of the software, the level of the user using the software from remote locations and the ability to deploy the software. In SSL VPN technologies, similar assistance to clients is required to ensure all client's systems browser are configured to allow the Java / ActiveX controls to install and run on their system. Many vendors IPsec clients were notorious for causing system instabilities and for not being user friendly. For this reason VPN-Q 2006 leverages the native VPN client functionality of Windows so as not to introduce any network level drivers that may affect the systems stability. Any updates that are required to the Microsoft VPN code can be managed like any other Windows update that is deployed today. As nothing changes, no extra cost is accrued. Any VPN-Q 2006 specific updates are automatically downloaded via the Winfrasoft update service. Additionally, the VPN-Q 2006 client is just under 1Mb in size making it easy to distribute, it doesn't ask any questions during the setup which is only 2 clicks and doesn't require administrative rights to install which makes it easier than installing a Java / ActiveX control!



No mutual authentication for PPTP based VPN's.

This is a valid issue with PPTP, however, VPNs based on Microsoft technologies as well as the VPN-Q 2006 software allow for the use of L2TP/IPsec which, by design addresses this issue. Even so, no SSL VPN on the market allows for mutual authentication either, as the underlining SSL protocol also does not cater for this feature.

IPsec VPN with quarantine

What is a quarantine network?

A quarantine network is sectioned off area of the LAN that has very limited access to resources, in particular internal resources. These quarantine areas are highly effective for keeping un-trusted machines away from your core assets, while still providing a minimum level of connectivity to allow business to function.

A VPN quarantine network is a virtual network that remotely connected machines are placed in until their health status can be determined. You may wish that certain PC's such as external B2B customers or consultants can connect to your network but with limited connectivity - regardless of their systems health status.

Benefits of Quarantine

The logic behind the quarantine within a VPN is to keep client systems off the internal network until the remote system has been proven to be healthy. In the case of a quarantine solution in a Microsoft environment, a client within quarantine may have access to partial functionality afforded to local users. Protocol and application filter policies in an ISA Server 2004 / 2006 VPN can be used to limit resource access to the quarantined user. A client can remain in quarantine until a time when the servers quarantine agent releases the client from quarantine or rejects them totally from the system. An example of where leaving a non-compliant remote user in quarantine may be beneficial is; quarantined clients can have access to the Windows Update Service in order to retrieve the latest patches and updates provided by Microsoft and in turn possibly rectifying their non-compliance state.

Characteristics of VPN-Q 2006

VPN-Q 2006 operates with both PPTP and L2TP/IPsec VPN protocols. The ability of VPN-Q 2006 to work over both of these protocols provides enhanced security over SSL VPNs as the L2TP/IPsec protocol is the only standards based protocol that allows for mutual authentication for client remote access. To date, L2TP in conjunction with IPsec is the only IETF approved method of remote access to VPNs.

Another benefit of VPN-Q 2006 is that the software installed at the client side is tied to its server component existing on the VPN concentrator. This provides an additional security layer via a soft token as the correct client software is required on the remote user's system as well as authentication credentials in order to access the VPN.

VPN-Q 2006 utilises the standard Microsoft VPN client which is built into Windows. Coupled to this, it has been designed to allow multiple authentication types, those being PAP, MS-CHAP and MS-CHAPv2. Since PAP is a compatible authentication type, VPN-Q 2006 can easily integrate with 3rd-party 2 factor authentication solutions such as token providers RSA and SecurEnvoy.

An integral part of VPN-Q 2006 is its end-point compliance checking facility. Below is a table listing the checks that can the VPN-Q 2006 client software performs and the associated risks of non-conformance.

| Security Check | Detail | Risk | To clear quarantine |
|--|---|--|--|
| Minimum operating system and service pack level | This test checks the version of the operating system and service pack level. VPN-Q 2006 was specifically designed to work with the Windows Security Center which was first introduced in Windows XP Service Pack 2 and has been maintained in Windows XP x64 Edition and Windows Vista. | Windows XP SP2 introduces many new security features, such as the Security Center, that form key components of a secure PC base. PCs without SP2 technology on Windows XP are susceptible to many well known attacks and are fundamentally a less secure platform. | Windows XP SP2, Windows XP x64 or Windows Vista is required. Note: Any other OS or SP level will halt further checks. |
| Windows IP routing status | Various versions of Windows have the ability to be an IP based router which enables it to allow communication between multiple networks. This feature is disabled by default in Windows XP. More information about IP routing in Windows XP can be found here: http://support.microsoft.com/?kbid=315236 | Having this feature enabled on a VPN client poses a security risk to the corporate network. Under certain circumstances, it may be possible to route unsolicited traffic from the local LAN, that the VPN client is connected to, onto the corporate network. Windows XP helps to protect against this risk by | IP Routing must be disabled. |



| Security Check | Detail | Risk | To clear quarantine |
|---|---|--|---|
| | http://support.microsoft.com/?kbid=140859 | disabling the feature by default. | |
| Screen Saver Security status | By default, Windows XP does not require password protected screen savers, however, this can be enabled by the user. This setting is maintained on a per user basis by Windows. | Screen saver security may at first glance appear to be unimportant, however, it helps to protect the PC when the user has left it unattended for a period of time. Good security practice dictates that users lock their PCs when they are left unattended however users do not always follow such policies. Enforcing screen saver passwords is a method of automatically locking the PC desktop. | Screen Saver password protection must be enabled. Note: A warning is displayed if the screen saver timeout setting is greater than 15 minutes. |
| Personal Firewall status | Another key security feature of Windows XP SP2 is the Windows Firewall, which is now enabled by default. This feature was previously called the Internet Connection firewall and was disabled by default. This security check will report on the status of the Windows Firewall and many 3 rd party personal firewalls if one is installed. | Many worms and viruses roam the Internet looking for targets to infect. Infected PCs can in turn infect corporate networks by bypassing network firewalls using VPN connections. Any system which connects directly to the Internet, e.g. VPN clients, should have some level of local firewall protection installed and active. | Either the Windows XP Firewall must be active or a 3 rd party personal firewall must be installed and active. |
| Windows Firewall File and Print Sharing exception status | The Windows Firewall has the ability to create exceptions to allow some traffic into the PC. VPN-Q detects if the File and Print sharing exception is enabled on the firewall. Note: This is only available when the Windows Firewall is in use and is not available with 3 rd party firewall products. | The Windows Firewall can provide excellent protection for a Windows XP PC, however if it is mis-configured then its value is reduced. A common inadvertent configuration error is the enabling of File and Print sharing exception through the firewall which could allow unauthorised access to shared data on the PC. | There is no requirement for this setting to pass quarantine. A warning is displayed if the File and Print sharing exception is enabled. |
| Internet Connection Sharing status | Internet Connection Sharing (ICS) is a feature of Windows XP that allows many PCs to share a single Internet connection. Unlike the Windows IP routing setting, ICS uses a NAT engine to route traffic. This feature is disabled by default in Windows XP. | As with IP Routing, under certain circumstances, it may be possible to route unsolicited traffic from the local LAN that the VPN client is connected to onto the corporate network. Windows XP helps to protect against this risk by disabling the feature by default. | ICS must be disabled. |
| Anti-Virus scanner status | A key protection technology for a PC is Anti-Virus (AV). There are many AV vendors in the market creating a vast choice of products. Most products are file system based scanning products while others have expanded into the realms of email content checking and Anti-Spyware. VPN-Q 2006 works with the Windows Security Center to monitor the status of the installed AV software. This includes the detection of an installed product, ensuring that it is enabled and has recent AV signature files. | An unprotected client is highly prone to infection by malicious code in the form of worms and viruses. While other mechanisms can also help mitigate these threats, a defence in-depth strategy should be adopted. AV technology is based on signature updates, thus an out of date AV product is of limited value and should be kept up-to-date at all times to provide adequate protection. | Anti-Virus must be installed, active and up-to-date. Note: AV vendors report the up-to-date status of their products in different ways, thus different products may produce varying results. |
| Automatic | A key component of systems security is patch management. Windows XP has the | Any PC that is un-patched is susceptible to attack. Anti-Virus and | Automatic updates must not be disabled, i.e. Auto |

| Security Check | Detail | Risk | To clear quarantine |
|-------------------------------|--|---|---|
| updates status | <p>built-in ability to auto-update itself by detecting and downloading required updates directly from Microsoft. Automatic Updates can be set to one of 4 states:</p> <p>Automatic: Updates are downloaded and installed automatically.</p> <p>Download: Auto download updates and notify you when they are ready to be installed.</p> <p>Notify: You are notified when new updates are available but nothing is downloaded or installed automatically.</p> <p>Off: Automatic Updates are disabled.</p> | <p>personal firewalls can help protect a PC from being exploited due to a known vulnerability and should be considered a temporary solution while the security update / patch is tested and deployed. Security updates / patches should be maintained on PCs to close known holes in software.</p> <p>It is highly recommended that Automatic Updates is set to at least Notify to create awareness of security updates.</p> | <p>Updates must be set to either Automatic, Download or Notify.</p> <p>Note: If Auto Updates are set to Notify a warning is displayed although the PC will not fail the quarantine check.</p> |
| Security Update status | <p>This security check works in conjunction with the Automatic Update status check and is only run if Automatic updates are enabled.</p> <p>Updates from Microsoft have varying security ratings including, Critical, Important, Moderate and Low. Other updates that, key to the OS, are considered mandatory but may not specifically fix a security issue.</p> | <p>Having a system for managing updates is critical in today's networking environments. However, it is also key to ensure that required updates are actually installed on a PC according to a defined policy.</p> <p>VPN-Q 2006 verifies the PCs compliance against all published Microsoft updates using the Microsoft severity rating system. If an organisation wishes to control their own security update policy then VPN-Q 2006 will also integrate with WSUS and verify the PC against the WSUS approved updates.</p> | <p>All downloaded updates, regardless of their severity rating, must be installed. In addition, all updates with a rating of Critical or Important must be installed regardless of their download status.</p> <p>Note: Missing updates with a status of Mandatory, Moderate, Low or unspecified will produce a warning.</p> |
| Legal Notice | <p>The Legal Notice check is not a technology specific check. It is a human control to allow administrators to be sure that the user has had clear visibility of a remote access policy prior to connecting to the network from a remote location. The user then has the option to either confirm that they agree to the stated policy or if they do not agree the remote connection will be disconnected.</p> <p>The Legal Notice is disabled by default and is only available in Enterprise Edition.</p> | <p>Network access control best practice and recent legislative compliance policies (such as Sarbanes-Oxley etc) place heavy emphasis on an administrator to ensure that anybody connecting over network boundaries into private network are informed about the implications of doing so.</p> <p>This should provide notice that only authorised access is permitted and the prescribed usage policy must be adhered to. The information should be clearly visible and should not be able to be bypassed. Any acceptance of the policy should be logged.</p> | <p>The user must click on the "I Agree" button.</p> <p>The result of the policy acceptance is logged on the VPN server for future reference.</p> |

Contrary to popular belief, the majority of worms, viruses and trojans that affect a network's integrity are not introduced into an organisation by criminals penetrating the defences from the great beyond, but rather by employees who, for the most part, inadvertently infect the system. Company's IT departments are usually very vigilant in securing the internal managed systems using a combination of products and policies to enforce security measures. However, staff members who can access the internal systems from a remote location typically do not have the same safe guards in place. IT departments have limited influence on these unmanaged machines and therefore, any access via these machines compromises the network's integrity.

VPN-Q 2006 vs. Microsoft's Quarantine sample using Scripts

Windows Quarantine Service (RQS) releases a user from quarantine when it receives an 'All Clear' from its sibling service on the client (RQC). Microsoft have published Sample Scripts that detail the process whereby a client system can initiate an 'All Clear' signal to the RQS service thus releasing a quarantined user from the quarantined area. Certain basic security checks can be performed on the client's system to validate the integrity of the system prior to the 'All clear' signal being sent to RQS.

There are 2 major flaws with this approach and they are:

- The checks that are performed on the client's system are typically very basic and therefore do not thoroughly confirm the integrity of the client's system;
- More importantly, the 'All clear' string that is to be sent to the RQS service is clearly stated within the script file in plain text so a user could quite simply, via the command line, bypass the client checks, execute the RQC command only and remove himself from quarantine irrespective of the state of his system's health. This would then negate the effectiveness of the entire quarantine solution as it can be easily bypassed.

In the case of VPN-Q 2006, the 'All clear' command is calculated at run time by the client and further encrypted with AES 256-bit encryption before being transmitted to the VPN server. It is infeasible for a client to bypass the VPN-Q 2006 checks and release himself from quarantine manually, as in the case of the Script solution, as this would require administrator access to the VPN Server to access the server copy of the encrypted code prior to the subversion.

Complementary technologies

This is something you are unlikely to hear most vendors say, "SSL and IPsec solutions are complementary".

There is a valid place for both within a network and the important thing to do is identify the best solution to use for each application. This may be determined by the protocols it uses (is it web based or custom port based) or the nature of the client application. Many companies have been sold the SSL VPN story only to find that it is not the be-all and end-all of remote access and, although it may meet many of the requirements, companies are never quite able to switch off their IPsec solution. With VPN-Q 2006 you don't need to, you can plan to maintain both if required while implementing the latest in cost effective remote access security.

Additional References

Point to Point Tunneling Protocol (PPTP)

Point-to-Point-Tunneling Protocol (PPTP) is a networking technology that supports multiprotocol virtual private networks (VPN), enabling remote users to access corporate networks securely across point-to-point protocol (PPP)-enabled systems to dial into a local Internet service provider to connect securely to their corporate network through the Internet.

Layer Two Tunneling Protocol (L2TP)

The Layer 2 Tunnel Protocol (L2TP) is an Internet Engineering Task Force (IETF) standard that combines the best features of two existing tunneling protocols: Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP uses packet-switched network connections to make it possible for the endpoints to be located on different machines. The user has a Layer 2 (L2) connection to an access concentrator, which then tunnels individual PPP frames to the NAS, so that the packets can be processed separately from the location of the circuit termination

RFC's

For a greater detailed view of some of the underlying technologies referenced in this document, please refer to the published RFCs listed below:

| | |
|---|--------------------|
| IPsec NAT-T | RFCs 3847 and 3948 |
| Layer Two Tunneling Protocol (L2TP) | RFC 2631 |
| Point to Point Tunneling Protocol (PPTP) | RFC 2637 |
| Security Architecture for the Internet Protocol | RFC 2401 |
| IP Security Document Roadmap | RFC 2411 |
| Securing L2TP using IPsec | RFC 3193 |

Email: info@winfrasoft.com
Tel: +44 (0)870 236 8346

Web: www.winfrasoft.com
Fax: +44 (0)870 236 8349

