Whale
Communications
A Microsoft Subsidiary

How to Select an SSL VPN for Remote Access to Microsoft SharePoint Portal Server 2007

Published: February 2007

For the latest information, please see http://www.microsoft.com/iag

Contents

Scope

This document presents an overview of the best practices for selecting an SSL VPN for fully functional remote access to Microsoft® SharePoint® portals and workspaces. It also shows how Intelligent Application Gateway (IAG) 2007 meets these requirements, and offers the most flexible and secure remote access tool for SharePoint portals.

For broader information about IAG 2007, its features and benefits, please see the white paper entitled “Intelligent Application Gateway: A Technology & Features Overview”, available on the Microsoft website at http://www.microsoft.com/iag.

Executive Summary

As organizations increasingly rely on their Microsoft SharePoint deployments as a means of driving business operations through Web-based collaboration, they look to extend its accessibility beyond the intranet to the extranet. SharePoint often serves as a unified front-end to a range of productivity and collaborative tools for employees on the LAN. Extending access beyond the confines of the network through the web allows enterprises to communicate with a broader set of users beyond employees to partners and customers. It also exploits the ubiquity of the Internet to deliver employees, partners and customers constant access to key business applications and network resources. Still, in order to maximize the business value of SharePoint's functionality and boost ROI, enterprises need to ensure that browser-based access for external users is secure, well-managed and supports complete functionality without creating vulnerabilities. As Microsoft expands the applications and resources available through SharePoint to embrace Microsoft Business Solutions applications portfolio, the need for cost-effective application-intelligent support for external users while maintaining security and network integrity grows to be central to efforts to leverage the utility of the software.

The solution used to enable the external access—the remote access gateway—must integrate seamlessly with SharePoint tools and applications, but in addition should offer its users the identical work environment to when they work within the office network. Moreover, it is desirable that the access gateway be able to *extend* SharePoint capabilities beyond just Web applications, transforming it into a single point of entry to all corporate applications including non-Web client/server applications such as Microsoft native Outlook®.

This document aims to assist the SharePoint project manager in understanding the criteria for evaluating a remote access enabler for any SharePoint installation. Assuming access *from anywhere* is required an SSL VPN will in most cases provide the best solution.

In order to implement an SSL VPN for remote access to SharePoint, the SSL VPN should allow for, at minimum, the following: data encryption and encapsulation; authentication; endpoint security compliance checks; cache cleaning; Single Sign-on (SSO); remote functioning of internally linked Web applications over a single encrypted tunnel. Without these basic requirements, SharePoint cannot *and should not* be accessed remotely from anywhere.

However, fully leveraging the SharePoint potential to maximize remote productivity and significantly increase SharePoint ROI is contingent on a number of additional requirements of your SSL VPN. It is strongly advised to use the list provided in this document as a checklist when comparing SSL VPNs to ensure an "apples to apples" evaluation of their ability to fulfill your SharePoint requirements.

The Intelligent Application Gateway (IAG) 2007 with SharePoint Application Optimizer is the only SSL VPN solution specifically designed for SharePoint. IAG 2007 complements the Microsoft Internet Security & Acceleration (ISA) Server 2006 solution for securely publishing SharePoint (and Exchange) by providing additional security elements, integrating third-party applications into the portal and publishing to unmanaged endpoints without requiring a component download. The gateway provides browser-based access, endpoint security including the Attachment Wiper™ session residue shredder, and the ability to host multiple portals on a single gateway. By leveraging these capabilities, customers can expand the availability of SharePoint to a broad range of users and access scenarios, entrenching its value as a collaboration platform.

In contrast to alternative approaches using a risky network-level connection from public machines not managed by the organization, IAG 2007 leverages its application-layer connection to enable support of Web Parts that are based on Web services. This allows full document collaboration without download of any component to the client device. IAG 2007's feature-rich solution offers the highest ROI by allowing more user groups to access *more*

applications from *more* locations for *more* productive working hours than any other SSL VPN solution.

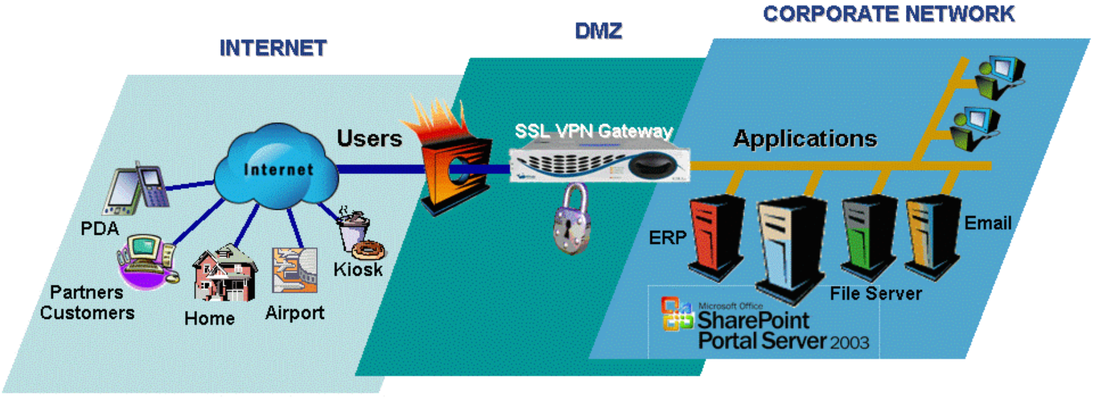
Selecting an SSL VPN for Remote Access to SharePoint: Overview

The following information will assist a SharePoint project manager looking for a remote access solution to SharePoint and workspaces *from anywhere*. It includes a short description of the features required for remote access to SharePoint, the related business benefits, and the functionality and security implications of not implementing each practice.

Remote access requirements to SharePoint can be categorized as follows:

Limited functionality requirements, mandatory for every remote access tool that offers access to SharePoint from endpoints that are under the company control, as well as from some customer and partner endpoints on which the user has administrative privileges. Network-level connections from non-trusted endpoints are absolutely unacceptable as they pose severe security risks.

Full service requirements for true anywhere access. Although many of these advanced features are not essential for opening your SharePoint server to access from outside the corporate network, failure of your SSL VPN to provide them will severely limit the levels of usability, security and integration with existing systems, thus dramatically decreasing productivity gain and Return on Investment on the project.



SSL VPN Infrastructure Diagram

Limited Functionality Requirements

Data encryption & encapsulation

Remote access to a SharePoint Server that manages sensitive corporate information requires data encryption for maintaining confidentiality of that information. In addition, a single SSL session for both SharePoint and complementary applications provides one access point that overlays encryption and encapsulation, enabling session-wide security enforcement such as secure logoff, endpoint security compliance and Single Sign-on. The IAG 2007 encapsulates all Web and non-Web applications within a single SSL session, irrespective of whether they are launched from SharePoint Web Parts or from the IAG 2007 SSL VPN toolbar.

Authentication overlay

Proper user identification is required for secure access to the SharePoint portal. The authentication should support numerous user repositories and authentication methods, in particular strong authentication tools such as one-time password, hardware token, biometrics, and client certificate. IAG 2007 supports a broad range of authentication methods, including Microsoft Active Directory®, LDAP and RADIUS. IAG 2007 can even combine multiple authentication methods in one login page. For example: requesting both a user name/password to be checked against the corporate Active Directory and a one time password provided by an RSA SecurID token.

Endpoint security compliance check

Since the basic assumption here is that access to SharePoint should be enabled from computers not under organizational control, enterprises should implement an endpoint security policy to govern whether access is permitted in specific circumstances. An example for such a policy: Allow access only if an anti-virus and Personal Firewall are installed.

The minimum mandatory requirement is to be able to limit access to the entire session if endpoint conditions are not met. The ability to handle multiple endpoint security policies limiting access not only to the entire portal but also to specific applications or even to business functions within applications is detailed later in this document.

IAG 2007 provides highly granular endpoint security compliance checks supporting tiered access with multiple security policies in order for users to perform specific business functions according to the security level they gave been granted.

Cache cleaning

It is essential that the SSL VPN provide a cache cleaner ensuring that no sensitive data is left behind when working from non-trusted endpoints. For example, editing and updating of Office 2003 documents through SharePoint Documents Libraries leaves a copy of the documents in the client cache.

Single Sign-on (SSO)

True Single Sign-on (SSO) enables collection of all credentials up-front and remote users are not re-prompted to log in to SharePoint or other applications during the same session. The IAG 2007 SharePoint Application Optimizer supports SSO for Active Directory, which is required by SharePoint, and in addition allows NTLM, form-based, PKI, and Basic

Authentication schemes. When SSO is implemented internally for SharePoint portal it is also transparently supported for external users with the SharePoint Application Optimizer.

Internet "readiness"

Internal references within Web applications present a major technical challenge when providing access to internal SharePoint infrastructures from the Internet. SharePoint Web Parts provide the framework for running internal Web applications, but do not touch the original application URLs. Data, code, and links may utilize system-naming conventions that do not work across the Internet. For example, references may be made to *http://hrserver* or use other server names that are not fully qualified. Additionally, references may be made to servers that are not published in public DNS listings. For example, while *mailserver1.whalecommunications.com* may be a valid server name, when accessed from Whale's network it will not work remotely.

IAG 2007 with SharePoint Application Optimizer provides a powerful translation engine that converts internal references to a form that will work across the Internet. Using a technology called host address translation, IAG 2007 with SharePoint Application Optimizer replaces references to internal systems with its own address coupled with an encrypted string that it (and only it) can translate to derive the actual internal address.

Full Service Requirements - Usability

Web Part support

Although SharePoint is a Web application, access through an SSL VPN acting as a Web proxy imposes usability constraints that limit full document collaboration. Since the client-side components of Office 2003 and Office 2007 for these Web Parts does not recognize SSL VPN authentication, the SSL VPN gateway rejects Web Services requests as unauthenticated, therefore preventing document collaboration and hindering utilization of Web Parts.

The way that almost all SSL VPN vendors have resolved the issue of allowing Web Services access to SharePoint has been to open a network-level connection. This practice, however, is risky at best and certainly not safe to use from non-trusted endpoints. Further, it may interfere with the proper functioning of other SSL VPN features such as Single Sign-on and authorization.

The IAG 2007 SharePoint Application Optimizer offers full-feature SharePoint remote functionality including full document collaboration without requiring the download of any components to the client (blocked by most public browsers) or opening network-level connections and thus compromising security.

Full Microsoft Office integration

Microsoft Office 2003 or Office 2007 is required at the endpoint for editing and updating of Office documents and for other SharePoint Web Parts and functions that are integrated with Office. The SSL VPN should enable Office 2003 or Office 2007 integration from non-privileged browsers, without requiring download of client-side components or opening a non-secure network-layer connection.

Some common SharePoint functions and Web Parts that rely on Office integration include Document Library, Form Library, Picture Library, List of contacts, List of events, Explorer view, Export to spreadsheet, and Edit on datasheet. The IAG 2007 SharePoint Application Optimizer transparently supports SharePoint and Office integration and allows remote functioning of SharePoint Web Parts and functions that rely on them.

Office-like environment with non-Web application support

SharePoint consolidates applications and data from various sources into one convenient interface, but some common business needs – such as accessing Outlook – are not delivered via a SharePoint portal. Although not a problem when users are working in the office (since access can be delivered via the LAN), it does become a problem when users are remote. To ensure maximum productivity, remote access needs to deliver more than just access to the SharePoint portal; it should also offer additional mechanisms to allow access to:

- Client/server applications
- Network files and folders
- Password management

The IAG 2007 offers the ability to tunnel client/server communications over SSL. This means that remote users accessing SharePoint via IAG 2007 with SharePoint Application Optimizer can use Outlook and communicate with their Exchange servers as if they were in the office. Similarly, Terminal Services can also be used. From an administration standpoint, the only port used for communications is the SSL port already in use for SharePoint-related communications (usually Port 443). No additional firewall ports need be opened.

The SharePoint Application Optimizer further complements SharePoint by providing access to general shared files and folders that are not stored on the SharePoint server. It offers two forms of remote file access:

- Remote drive mapping – tunneling access to a network drive (i.e. X: drive) within SSL
- File access GUI – a powerful Explorer-like interface that can be accessed from any standard web browser. Access is available to Microsoft and Novell file systems.

In addition to supporting non-Web client/server applications, the SharePoint Application Optimizer embeds several SSL VPN objects within the SharePoint workspace. The IAG 2007 SharePoint Application Optimizer toolbar can become part of the page, permitting the launch of a number of SSL VPN applications and password changes, showing SSL VPN system information and countdowns, and adding the Logout button that terminates the entire SSL session. In addition the SharePoint Application Optimizer can integrate a File Access module into a generic Web Part, allowing the user access to shared files and folders stored outside of the SharePoint libraries. The administrator can embed the IAG Event Monitor in a Web Part; the IAG Event Monitor's built-in security tools (application firewalling) allows secure remote monitoring.

Single user experience for internal and external portal access

Many companies who have invested in SharePoint technology for enterprise portal purposes would prefer to use the same SharePoint workspace they use internally for external access as well. When using SSL VPN for remote access they would like the user to work with the familiar SharePoint portal interface rather than the built-in SSL VPN portal page.

The SharePoint Application Optimizer can display each user’s standard SharePoint workspace page as the remote access home page. Alternative SSL VPN approaches are less flexible and enforce the use of the SSL VPN portal page, regarding the SharePoint Portal as an application rather than as a unified portal for both internal and external access.

Password change management

Standard security policies usually dictate that users change passwords every few months by expiring old passwords. Users must be able to change their passwords before they lose access regardless of whether they are located in the office or are using systems remotely.

IAG 2007 supports remote password management; it provides remote users with prompts when passwords are nearing expiration, and enables employees to update passwords from any browser. It also supports remote resetting of token PINs for technologies such as RSA SecurID.

In addition to IAG 2007’s built-in password change utility, the SharePoint administrator can embed the Change Password feature of Microsoft Internet Information Services (IIS) within a SharePoint Web Part. IAG 2007 supports IIS Change Password, transparently performing host address translation (HAT) as it does with any other Web Part.

Full Service Requirements - Security

Application firewalling

An SSL VPN used for enabling remote access to SharePoint should incorporate built-in application firewall technology. This is similar in concept to the IPsec VPN that is usually implemented on a network firewall. Non-SSL traffic is directed to the standard interior firewall, whereas SSL traffic is securely managed and filtered at the application firewall. An application firewall is a powerful tool against known attacks, and even against vulnerabilities not yet discovered or patched. The risks of deploying SSL VPN without an application firewall include worm attacks and hackers exploiting server vulnerabilities to compromise an organization's infrastructure.

IAG 2007 application firewalling capabilities integrate powerful application aware filtering. It subjects incoming requests to stringent security checks before relaying any data to application servers on the internal network. Application-level control includes thoroughly inspecting URLs, methods and parameters, and all other incoming data.

The inspection rules can be based on the positive logic of the application, indicating a controlled set of legitimate URLs, method, and parameter combinations to which the requests are expected to conform. This prevents application-level attacks based on malformed URLs. IAG 2007 supports negative logic rules to block known attacks from reaching internal servers. Further, it enables generation of an IP block list, which will prevent users from a particular IP address from accessing the application.

Most rule sets will be implemented automatically when the system administrator selects a specific application module such as SharePoint or Outlook Web Access during initial installation. For non-standard applications, IAG 2007 offers tools for automating the generation of positive-logic rule sets.

Advanced endpoint security compliance checks

The SSL VPN should have several trust levels based on user and endpoint attributes. An extremely high level of granularity is warranted for applying the appropriate security policy-based on who you are, the type of device you have connected from, and what security tools are running on that device.

IAG 2007 provides a tiered access SSL VPN solution and thus offers a greater level of granularity and flexibility than alternatives. In many situations in which standard SSL VPNs have to block access to enforce security, IAG 2007 is able to deliver some level of access. When one function within an application presents a security concern, but the rest of the application does not, IAG 2007 allows you one-click blocking of only the risky function(s) as opposed to blocking access to the entire application. For example, upload of new documents to SharePoint from non-trusted public locations can be blocked, while download and editing of documents already on the SharePoint server is permitted.

Security policy implementation

Security policies should be implemented based on endpoint attributes and not only by the user profile. The policy should distinguish between trusted and non-trusted machines, providing several trust levels according to the tools operated at the endpoint.

The SharePoint Application Optimizer can allow or deny access to specific SharePoint applications or functions within applications according to the endpoint trust level and endpoint security compliance. For example, if the IAG Attachment Wiper is not installed at the endpoint, the SharePoint Application Optimizer will allow SharePoint document view within the browser, but will not allow full document collaboration (editing and updating).

Secure logoff

Working from a public browser may pose a serious security risk if users fail to logout. It is essential for an SSL VPN to provide time outs that terminate the remote access session due to inactivity, and/or force re-authentication after a pre-defined time period thus minimizing the window of opportunity for hijacking or taking over an abandoned session.

IAG 2007 provides both non-intrusive inactivity timeouts and forced re-authentication timeouts. Both are non-intrusive in the sense that the user's session will not terminate unexpectedly causing a loss of unsaved work (e.g. writing a long email). Rather, a pop-up window will give the user the chance to prolong the session. IAG 2007 timeouts are application intelligent, distinguishing between regular user commands and system commands. The latter, which are automatic, are ignored. For instance, when the user workspace includes an Outlook Web Access (OWA) Web Part, it causes the endpoint to send a periodic command checking for new emails. IAG 2007 ignores this command for the inactivity timeout count.

SharePoint workspace logoff button

SharePoint does not provide a built-in logoff button. While this is not crucial when working internally as the user can log out of his Windows® session, SharePoint logout become a critical security issue when working remotely, especially from non-trusted endpoints.

The SharePoint Application Optimizer adds a logoff button in the SharePoint workspace. When SharePoint is used as the remote access portal page without the built-in IAG toolbar, the addition of the IAG-generated logoff button will allow for secure logoff, terminating the SSL session and all the underlying applications.

Attachment Wiper with file shredding

Cleaning the standard cache is essential for the 'edit a SharePoint document' function that leaves a copy of the document at the client machine. IAG 2007 provides a built-in Attachment Wiper that cleans the standard cache of the browser and the specific SharePoint offline cache at the end of each session, ensuring that copies of edited documents are deleted.

In addition to the standard and SharePoint caches, the Attachment Wiper clears other sensitive information left on the client, including: user credentials, cookies, auto-complete forms, auto-complete URLs and URL history. The IAG Attachment Wiper runs by default in "file shredding" mode, causing all deletions to conform to DoD 5220.22-M standard and ensuring that data cannot be reinstated using specialized electromagnetic equipment.

Cache cleaning is a mandatory requirement for ICSA Labs SSL VPN Certification.

Internal network name and address hiding

When working from an Internet café or other public browser, exposing internal domain names may pose a threat if a non-trusted person is watching. Host address translation (HAT) hides all information related to the internal network from external users; hackers and other unauthorized parties never see anything that could be of assistance to them in launching attacks against internal resources.

Internal network name and address hiding is a mandatory requirement for ICSA Labs SSL VPN Certification.

Secure platform protecting against network and OS level attacks

A question that often troubles security managers is where to place the remote access gateway. Placing the SSL VPN in the DMZ (demilitarized zone) or in the back office each poses a number of security risks. Even on the assumption that the SSL VPN is protected between two firewalls in the DMZ, security risks remain:

- Numerous ports would need to be opened in the interior firewall, resulting in serious security vulnerabilities and compromising most corporate security guidelines.
- SSL decryption keys are maintained in an unsafe environment (the DMZ).
- Decryption is performed in the DMZ, so that communication of sensitive information occurs as plaintext (not encrypted) on the insecure DMZ network.

The exterior firewall is undermined by the SSL VPN; protocols that are supposed to be blocked by the exterior firewall slip by as they are tunneled to the DMZ.

Placing the SSL VPN in the back office on the other hand poses a new set of threats (and corporate policies are again violated):

- The entire firewall infrastructure is undermined as protocols that the firewalls are supposed to block are tunneled over SSL all the way to the internal network.
- Network packets from unauthenticated users are sent directly to the internal network instead of being stopped at the perimeter.

Full Service Requirements - Integration

Integration with Microsoft Active Directory

Seamless integration of the SSL VPN with Active Directory, SharePoint's user repository, is critical. The SSL VPN should verify the user credentials and authenticate with Active Directory, enabling Single Sign-on without the need to authenticate again to SharePoint after the initial remote access authentication. IAG 2007 natively supports Active Directory through simple and fast integration. In addition, many other user repositories are supported, such as Novell eDirectory and Lotus Notes repository.

End-user troubleshooting tools

An enterprise-class remote access solution handling hundreds of concurrent users with numerous security policies and endpoint compliance options should provide high-level troubleshooting tools. If a user fails to perform a function, he should know the reason why: Is the function available remotely at all? Is the user authorized to use this function? Does the endpoint comply with the security policy for this function? Can the user remediate their endpoint to the appropriate security level? A trouble-shooting tool should analyze the reason for failure and provide the information to the user and/or administrator, including a suggested resolution of the failure.

IAG 2007 provides a unique troubleshooting tool with session snapshot monitor, which allows the administrator to examine user activities and zoom into a user’s session in real time. It shows the permitted user applications and functions, and the user activities during login process and applications launch.

Example: A user notifies the administrator on failure to launch a specific SharePoint function, for instance "Edit a document". The administrator opens the IAG Event Monitor, zooms into the user’s session and discovers that the function failed because the IAG Attachment Wiper is not installed, meaning that the endpoint is not compliant with the access policy requirements. The administrator instructs the user on how to download and install IAG client components, and then to access the SSL VPN gateway again. The user successfully launches the desired function.

Integration with a Certificate Authority

The SSL VPN should integrate with a digital certificate authority to identify privileged or trusted endpoints. IAG 2007 provides a built-in certificate authority in the event the administrator chooses not to use an external certificate authority. Using a button on the IAG toolbar, a user may request a trusted endpoint certificate for a specific machine. If the certificate is granted by the administrator, the next time the user logs in from the same computer he will receive the certificate of trust. Identifying certified endpoints is crucial for SharePoint implementation allowing certain functions from trusted endpoints and blocking them from elsewhere. For instance: Only a certified endpoint that holds a digital certificate can edit SharePoint documents without the need of Attachment Wiper. All other non-certified machines will require an Attachment Wiper for document editing.

Summary of Features and Business Impact

It is strongly advised that you use the summary table below as a checklist when comparing SSL VPNs to ensure an "apples to apples" evaluation of their ability to fulfill your SharePoint requirements.

Checklist

	Features	Short Description	Business Impact
MANDATORY FEATURES			
	Data encryption and encapsulation	Encryption is essential for privacy of sensitive data. Encapsulation within SSL standard encryption protocol allows publishing of SharePoint apps at a single access point with a single session.	Remote access to SharePoint is not secure without this feature.
	Authentication	Proper user identification is required for secure access to SharePoint portal.	Remote access to SharePoint is not secure without this feature.
	Basic endpoint security compliance check	Access is limited/blocked from endpoints not complying with minimal security needs	Remote access to SharePoint is not secure without this feature.
	Cache cleaning	Sensitive data must be deleted from the cache on voluntary or involuntary session completion.	Remote access to SharePoint is not secure without this feature.
	Single Sign-on (SSO)	Remote access login credentials must be delegated to Active Directory, SharePoint Portal and its applications.	Remote access to SharePoint is not secure without this feature.
	Internally linked Web applications must be Internet ready (i.e. work remotely)	SSL VPNs require bi-directional URL rewrite for remote access to Web Parts/internal Web applications.	Remote access to SharePoint is not secure without this feature.
FULL SERVICE FEATURES			
Usability	Full Web Part support without client-side components/network-level connections	SharePoint Web Parts must work even from public browsers that block Java and Microsoft ActiveX® downloads.	Required for anywhere access. Without it, many Web Parts will not function, limiting user productivity.
	Full Office document collaboration without client-side components or network-level connections	Enables editing and updating of Office documents from non-privileged browsers and SharePoint functions that rely on full Office integration	Failure to provide this function will limit productivity. Attempting to edit or to use functions such as 'Export to spreadsheet' will cause severe OS errors.
	Provide Office-like environment with non-Web application support	Securely extend SharePoint usage to non-Web client/server applications.	Without this, access will be limited to Web apps only, or access to non-Web apps will compromise security.
	Use SharePoint Portal as the remote access home page	Both internal and remote users use identical portals.	Increases ROI: investment in SharePoint technology is leveraged; users spend more working time on busi-ness apps; fewer support calls; lower operational costs.
	Password change management	Users can update/change password via the SSL VPN.	Saves end-user time, increases ROI.

	Features	Short Description	Business Impact
Security	Application firewalling	Positive logic protects against HTTP viruses and attacks.	Increases security especially from public browsers, and semi-/non-trusted users such as customers/partners.
	Advanced endpoint security compliance check	Flexible recognition of a broad range of tools and company certificates.	Granularity of attributes (e.g. AV updated for the last 7 days) means better security. Customized detection process results in access from more places to more applications, i.e. higher ROI.
	Security policy implementation	When allowing/denying access based on endpoint compliance specific Web Parts or functions can be blocked instead of entire applications.	Enables more access from more locations thus significantly increases productivity and ROI.
	Secure Logoff	Inactivity/forced re-authentication timeouts reduce risks of session hijack from public browsers.	Crucial for access from non-trusted endpoints. Non-intrusive timeouts are necessary for improved productivity and user satisfaction.
	Add Logoff button to SharePoint	Essential when SharePoint is used as the SSL VPN home page.	Increases security. Without it users may fail to log out.
	Cache cleaning with SHREDDING of the sensitive data on non-secure endpoints	Sensitive data should be wiped from non-trusted endpoints, with file shredding to prevent 'undelete'.	Failing to do so will limit access from non-trusted machines.
	Hiding internal network names and addresses	Translate internal names into encrypted strings.	Increases security by preventing risk of unwanted person looking over the shoulder.
	Secure platform protecting against network and OS level attacks	Secure infrastructure hardens the SSL VPN itself from attacks.	Increases security. Blocks hackers from gaining control over the appliance via OS and network vulnerabilities.
Integration	Native integration with Active Directory	Active Directory is required for SharePoint authentication with SSO.	Simple, out-of-the-box integration reduces installation time.
	End-user troubleshooting tools	End-user can troubleshoot integration between network elements and the user's machine.	Time savings for help desk services. Improved user productivity.
	Integration with a certificate authority (CA) for identifying trusted endpoints	Convenient and proven identification of endpoint machine.	Better identification results in access from more places to more applications thus increasing ROI.

Conclusion

IAG 2007 integrated with ISA Server is the ideal method for extending SharePoint implementations through remote access. It dramatically increases the ROI attainable from deploying SharePoint, without introducing any security risks. Combining ISA Server's ability to pre-authenticate users and provide comprehensive edge security with Whale's ability to integrate third-party Web and client/server applications, customer can expand access to business-critical collaboration tools while minimizing risks to network integrity and data safeguards.

For further information on IAG 2007 and the SharePoint Application Optimizer, or to arrange for a live demonstration, you may contact: whaleinf@microsoft.com (North & Latin America) or whaleeur@microsoft.com (International).

The information contained in this document represents the current view of Whale Communications on the issues discussed as of the date of publication. Because Whale Communications must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Whale Communications, and Whale Communications cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. WHALE COMMUNICATIONS MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Whale Communications may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

SSL VPN for SharePoint-WP-200702.doc