Whale Communications
A Microsoft Subsidiary

Intelligent Application Gateway 2007

How to Select an SSL VPN for Remote Access to an IBM Lotus Environment

Secure Front End for Remote Access to IBM Lotus Applications from Anywhere

Published: February 2007

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

Contents

Executive Summary

Lotus® applications are among the most powerful collaborative tools available today; they allow diverse groups of workers to communicate and work together on projects regardless of location and time. Of course, the value of Domino, Lotus QuickPlace, and Lotus Sametime is directly tied to their availability – if users can access these systems from anywhere at anytime they provide much more benefit than if they are only available from office computers and specific laptops.

However, implementing a remote access infrastructure to allow ubiquitous access can be complicated and costly. Numerous complex replication schemes, proxy servers, and other technologies have been put in place to combat the many security threats, often resulting in an infrastructure that is expensive and difficult to manage, and efforts to simplify the deployment can introduce serious security risks. As a result, organizations often hesitate to implement anywhere access to important Lotus applications, despite the obvious benefits achievable by doing so.

This document aims to assist the Lotus project manager in understanding the criteria for evaluating a remote access enabler for any Lotus 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 a Lotus environment, 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, collaborative Lotus applications cannot and should not be accessed remotely from anywhere.

However, fully leveraging the potential of these applications to maximize remote productivity and significantly increase 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 remote access requirements.

Intelligent Application Gateway (IAG) 2007 is an enterprise-class SSL VPN appliance. Deployed with the Intelligent Application Optimizer for Lotus Domino -- with its in-depth understanding of Lotus applications, how they work and their idiosyncrasies -- provides a single secure gateway into Lotus and other applications. It allows organizations to offer the convenience of anywhere, anytime access, while keeping implementations and management simple, and adhering to the highest standards of security.

Users can access important Lotus applications, databases, and files from standard web browsers in locations such as client sites, home offices, airport kiosks, or wireless devices – in fact from anywhere someone can run a simple Web-browser. And all this while back-end systems are protected against hackers and user data is prevented from being exposed on public computers. Single Sign-on and a customizable toolbar allow for easy navigation between applications. A simple appliance allows for rapid deployment and easy maintenance.

An Overview

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

Remote access requirements to Lotus environments can be categorized as follows:

Limited functionality requirements, mandatory for every remote access tool that offers access to Lotus environments from endpoints under 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 strongly advised against as they pose severe security risks.

Full service requirements for true anywhere access. Although opening your Lotus environment to access from outside the corporate network is possible without many of these advanced features, failure of your SSL VPN to provide them will severely limit the levels of usability, security and integration with existing systems, and thus dramatically decrease productivity gain and Return on Investment on the project.

Limited Functionality Requirements

Data encryption & encapsulation

Remote access to Lotus applications that manage sensitive corporate information requires data encryption for maintaining confidentiality of that information. A single SSL session for both Lotus servers and complementary applications results in a single access point that overlays encryption and encapsulation, enabling session-wide security enforcement such as secure logoff, endpoint security compliance, Single Sign-on, etc.

Authentication overlay

Proper user identification is required for secure access to the Lotus application servers. The authentication should support numerous user repositories and authentication methods, in particular strong authentication tools such as one time passwords, hardware tokens, biometrics, client certificate, etc. 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 a single login page. For example: Requesting both a user name/password to be checked against the Notes LDAP server and a one time password provided by an RSA SecurID® token.

Endpoint security compliance check

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

A mandatory requirement is the ability to limit access to an entire session if endpoint conditions are not met. The handling of multiple endpoint security policies that limit 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 have been granted.

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 Domino Web Access or other applications during the same session. IAG 2007 supports SSO for Lotus Notes Directory, which is required by Lotus applications, and in addition allows NTLM, form-based, PKI, and Basic Authentication schemes.

Replicating functionality for Web access

Internal references within Web applications present a major technical challenge when providing access to internal Lotus servers from the Internet. 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 outside Whale's network it will not work remotely.

IAG 2007 provides a powerful translation engine that converts internal references into a form that will work across the Internet. Using a technology called host address translation (HAT), IAG 2007 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

Transparent Lotus server selection

Most large deployments involve multiple Lotus servers. In many scenarios, each user account is assigned to a specific server. Since administrators can move a user database from one server to another, it is impractical to expect the user to know which of the servers his database is on. For a simplified user experience, users should be aware of only one server, which they connect to. On the corporate LAN the request is automatically connected to the correct Lotus server and handled appropriately.

Requiring the same functionality over an SSL VPN presents a challenge; tight security must be maintained while providing for central referral to multiple Lotus servers. Out-of-the-box Application Optimizer modules for Domino Web Access and Native Notes client provide the ideal blend of these requirements:

- The administrator configures multiple servers as one Lotus application.
- The user clicks on one link and is connected to the appropriate Lotus server.
- IAG 2007 independently determines which server the user should be connected to.

Embedded Lotus Sametime from anywhere

An important element of the Lotus family is Lotus Sametime. Lotus Sametime provides instant messaging and other collaboration capabilities such as shared whiteboard and screen sharing.

Most SSL VPN vendors require a client on the endpoint to tunnel the Lotus Sametime traffic. With Application Intelligent technology, Lotus Sametime is available even from limited endpoints which do not allow the downloading of ActiveX® or Java components such as Internet cafes and airport kiosks.

Domino Offline Services (DOLS)

For users interested in fully disconnected or "offline" use of Domino Web Access without having to install the native Notes client, DOLS is the ideal tool. A user can read mail via Domino Web Access, and then choose to synchronize his database, disconnect and continue working with native Notes locally – editing, composing, deleting, etc.

IAG 2007 allows clientless access to Domino Web Access from anywhere. However, if the user is using a corporate laptop he may choose to use DOLS for additional functionality. When the user selects to go offline, a self-loading client component is triggered to tunnel the synchronized data to the Lotus Notes server on the corporate network.

Password change management

Standard security policies usually dictate that passwords be changed every few months and users must be able to change old passwords before they expire, regardless of whether they are located in the office or 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.

Full Service Requirements – Security

Secure Lotus server selection

In multiple Lotus server environments, it is essential to allow access from the endpoint to all backend servers. On the other hand, access needs to be limited by the SSL VPN server so that no other corporate servers are exposed. Some vendors rely on the client to decide which server it wants to connect to. IAG 2007 provides access to the Lotus servers alone and blocks client requests to connect to other servers.

Application firewalling

An SSL VPN used for enabling remote access to a Lotus application server 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 an SSL VPN without an application firewall include worm attacks and hackers exploiting server vulnerabilities to compromise an organization's infrastructure.

IAG 2007application firewalling integrates powerful application intelligent filtering. It subjects incoming requests to stringent application-level controls before relaying any data to application servers on the internal network, including thorough inspection of URLs, methods and parameters.

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 also 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 Domino Web Access or Lotus Sametime during the initial installation. For non-standard applications, IAG 2007 offers an Intelligent Application Optimizer Toolkit for automated 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 which 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 alternative SSL VPNs. In many situations in which standard SSL VPNs block access to enforce security, IAG 2007 is able to deliver at least 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 to block only the risky function(s) with a click of the mouse, as opposed to blocking access to the entire application. For example, upload of new documents to Lotus QuickPlace from non-trusted public locations can be blocked, while download and editing of documents already on the server is permitted.

Security policy enforcement

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

IAG 2007can allow or deny access to specific Lotus 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, IAG 2007 will allow uploading of documents to Lotus QuickPlace but not downloading of e-mail attachments via Domino Web Access. Further, to combat attempts by users to bypass a no-download policy, granular application intelligent access rules allow the administrator to also set a policy blocking the forwarding of email messages with attachments to external accounts.

Secure logoff

Working from a public browser may pose a serious security risk if users fail to log out. It is essential that an SSL VPN terminate the remote access session when the session is no longer active, and/or force re-authentication by the user after a pre-defined time period in order to minimize the window of opportunity for hijacking or taking over an abandoned session.

IAG 2007 provides both inactivity timeouts and forced re-authentication timeouts. Both are non-intrusive in the sense that the user's session will not terminate unexpectedly and thereby cause 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. Timeouts are application intelligent, distinguishing between regular user commands and system commands. The latter, which are automatic, are ignored. For instance, when using Domino Web Access a periodic request is sent to the server checking for new emails. IAG 2007 ignores this command for the inactivity timeout count.

Attachment Wiper with file shredding

Cleaning the standard cache is a must if reading of attached documents via Domino Web Access is permitted since once a document is opened, a copy of that document is left on the client machine. IAG 2007 provides a built-in Attachment Wiper that cleans at the end of each session not only the standard browser cache but also the non-standard offline cache created by Domino Web Access, thus ensuring that all copies of downloaded documents are deleted.

In addition to the standard and proprietary Domino Web Access 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 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 cafe 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.

Incorporation of Microsoft Internet Security and Acceleration (ISA) 2006 protects the IAG appliance itself from Internet-based attacks.

Full Service Requirements – Integration

Built-in support for Lotus Notes/Domino LDAP server

Seamless integration of the SSL VPN with the Lotus Notes LDAP server, Lotus' user repository, is critical. The SSL VPN should verify the user credentials and authenticate with the Lotus Notes LDAP server, enabling Single Sign-on without the need to re-authenticate to Domino Web Access, Lotus Sametime or Lotus QuickPlace after the initial remote access authentication. It's as simple as choosing "Notes Directory" from the authentication server menu.

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 or she should know the reason why: Is the function available remotely? Is the user authorized to use this function? Does the endpoint comply with the security policy for this function? Can the user bring their endpoint to the appropriate security level?

A troubleshooting tool should analyze the cause of failure of a function 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 a 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 and application launch.

Example: A user notifies the administrator on failure of a Domino Web Access function, for instance "Forward with Attachment". The administrator opens the IAG Event Monitor, zooms into the user's session and discovers that the function failed because the Attachment Wiper has not automatically installed itself, meaning that the endpoint is not compliant with the access policy requirements. The administrator instructs the user on how to download and install IAG 2007 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's built-in Certificate Authority is provided in case the customer chooses not to use an external certificate authority. Using a button on IAG 2007, 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 or she will receive the certificate of trust.

Identifying a certified endpoint is important for Lotus environments allowing certain functions from trusted endpoints only and blocking them from elsewhere. For instance, only an endpoint that holds a digital certificate can download attachments without the Attachment Wiper being installed. All other non-certified machines will need an Attachment Wiper for reading attachments.

Summary of Features and Business Impact

We strongly advise that you use the summary table that follows as a checklist when comparing SSL VPNs to ensure an "apples to apples" evaluation of their ability to fulfill your Lotus requirements.

Checklist

Features		Short Description	Business Impact
MANDATORY FEATURES			
Data encryption and encapsulation		Encryption is essential for privacy of sensitive data. Encapsulation within the SSL standard encryption protocol enables publishing of Lotus applications at a single access point with a single session.	Remote access to Lotus applications is not secure without this feature.
Authentication		Proper user identification is required for secure access to Lotus applications.	Remote access to Lotus applications is not secure without this feature.
Basic endpoint security compliance check		Access is limited/blocked from endpoints not meeting minimal security needs	Remote access to Lotus applications is not secure without this feature.
Single Sign-On (SSO)		Remote access login credentials must be delegated to Lotus Notes LDAP server and Lotus applications.	Remote access to Lotus applications is not secure without this feature.
Internally linked Web apps must be Internet ready (work remotely)		SSL VPNs require bi-directional URL rewrite for remote access to Lotus web and web-embedded applications.	Remote access to Lotus applications is not secure without this feature.
FULL SERVICE FEATURES			
Usability	Transparent Lotus server selection	Connection to the appropriate server in a multiple Lotus server environment has to be done transparently and securely	Required for multiple server deployments. Without it, users are confused and administrative work is less centralized.
	Embedded Lotus Sametime from anywhere	Enables using the Lotus Sametime functionality from anywhere, including non-privileged browsers.	Failure to provide this function will limit productivity. In addition, attempts to use embedded Lotus Sametime from a non-privileged machine will fail.
	Domino Offline Services (DOLS)	Enables reading e-mail offline without requiring a full native Lotus client to be installed on the endpoint. DOLS and the SSL VPN client are launched only when required, not keeping any ports open when DOLS is not in use.	Failure to provide this function will limit productivity. Without this, reading e-mail will be limited to online access only.
	Password change management	Users can update/change password via the SSL VPN.	Saves end user time, offloads calls from the helpdesk, increases ROI.
	Secure Lotus server selection	Administrator-controlled list of accessible Lotus servers in a multi-server environment	Increases security by preventing the client side from gaining access to prohibited servers.

	Features	Short Description	Business Impact
Security	Application Firewall	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 within last 7 days) translates into better security. Customized detection process results in access from more places to more applications, i.e. higher ROI.
	Security policy enforcement	When allowing or denying access based on endpoint compliance specific functions can be blocked instead of entire applications.	Enables more access from more locations thus significantly increases productivity and ROI. Prevents bypassing of download rules by forwarding to external e-mail accounts.
	Secure logoff	Inactivity and 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.
	Cache cleaning with SHREDDING of sensitive data on non-secure endpoints	Sensitive data should be wiped from non-trusted endpoints, with file shredding to prevent 'undelete'.	Failing to delete Domino Web Access specific cache will jeopardize sensitive information, hence causing administrators to 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 (e.g. ISA Server) hardens the SSL VPN itself from attacks.	Increases security. Prevents hackers from gaining control over the appliance.
Integration	Built in support for Lotus Notes/Domino LDAP server	Lotus Notes LDAP Server required for Lotus 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 with Lotus Domino Application Optimizer enables simple, secure remote access to Lotus applications from anywhere a web-browser can be found. With its unmatched security features enabling secure access even from the most insecure locations, it is the simplest and most cost-efficient way to deploy remote access to large numbers of Lotus users.

IAG 2007 can enhance employee productivity, while saving money and reducing complexity and management issues.

For further information on IAG 2007 and Lotus Domino Application Optimizer, or to arrange for a live demonstration, please contact: whaleinf@microsoft.com North & South America) or whaleeur@microsoft.com (International).