# Whale Communications
## A Microsoft Subsidiary

# Intelligent Application Gateway 2007

## A Technology and Features Overview

White Paper

# Contents

# Introduction

SSL VPN access technology provides access to corporate resources via an industry-standard web browser.  The SSL VPN access market has demonstrated sustained growth since 2002 when the product category first emerged, and is now widely considered a viable and cost-effective alternative to traditional access methodologies.

An SSL VPN platform can prove a valuable investment for your organization if:

1. Your organization would benefit from offering employees remote access to their applications and data.

    a. You want to provide employees with Web access to email (for example, via Microsoft® Outlook® Web Access or IBM Lotus Domino Web Access)

    b. You need to provide remote access, but find that IPsec does not work from many locations due to an inability to install client-side software and/or due to firewall restrictions.

2. You are looking for a flexible solution to providing IPsec and SSL VPN in a consolidated appliance.

3. You want to lower remote access costs.

4. You want to increase top-line revenue by expanding customer self-service capabilities and automating business interaction with partners.

5. Security and policy compliance are important concerns.

6. You are creating or updating your organization's disaster recovery or business continuity plan.

## What Makes IAG 2007 Application Access and Security Technology Unique?

The Intelligent Application Gateway 2007 integrated with Microsoft Internet Security and Acceleration (ISA) Server delivers a positive return on investment by enabling broad access to enterprise resources, both in terms of users -- remote and mobile employees, business partners, vendors and customers -- as well as the tasks each type of user can perform remotely.

**Security**

- Embedded positive logic application firewall.

- Full endpoint security and rich client-side policy compliance engine.

- Protection against network and operating system vulnerabilities.

- Reduction of reliance on patching to protect both the SSL VPN platform and internal servers from outside threats through positive logic application firewalling.

**Flexibility**

- Granularity of access controls based on user and access device, even within applications.

- Intra-application controls deliver the flexibility required to serve the business needs of remote access while maintaining a secure posture and network integrity, and enable productivity even from many unmanaged endpoints.

- Native integration with Microsoft Active Directory®, Windows® Networks, RADIUS, LDAP, Novell Directory and File Shares, Client Certificate, RSA SecurID, and strong authentication tools.

- Ability to support multiple virtual SSL VPN portals on a single appliance.

- A remote access platform that can extend remote access beyond employees to vendors, partners, contractors, customers and even other applications (via Web Services).


**Application Intelligence**

- Out-of-the-box functionality in pre-configured modules that incorporate application-specific positive logic to protect back-end servers, while allowing granular security policies based on client-machine state.

- Support for complex enterprise applications without requiring a component download to the client, or without opening a risky network-level connection.

- Highly granular endpoint compliance checks updated to mitigate the latest security threats.

- Technology to enforce client-side compliance policies within applications (e.g. "Can't wipe, can't download" or "No antivirus, no upload" or "Run a specific application from company-owned machines only" while allowing the rest of the respective applications to function normally).


**End-User Experience**

- Intuitive user interface with familiar Windows-like feel.

- Microsoft Internet Explorer® taskbar for easy navigation; no random pop-up windows.

- Extensive customization of the end-user experience including the portal, log in pages and single application launch significantly eases management and technical support workloads.

- Non-intrusive timeouts and periodic re-authentication (users will NOT lose work due to timeouts).

- Single Sign-on (SSO) enables collection of all credentials up-front and users are not re-prompted during the current session. SSO is supported for NTLM, form-based, PKI, and Basic Authentication schemes.

- Remote password management including the ability to change passwords via the SSL VPN as well as full RSA Agent integration to allow PIN renegotiation or new token activation.


**Management and Control**

- Web-based monitor allowing secure monitoring from anywhere.


# Leading in Enterprise Deployments

The Intelligent Application Gateway (IAG) 2007 has been recognized for providing enterprise-class SSL VPN and application gateway access by respected industry analysts -- Microsoft was named a Visionary in the Gartner SSL VPN Magic Quadrant 3Q06, and a Leader in the 2006 Forrester SSL VPN Wave.

The IAG 2007 continues to win industry and trade press awards, including SC Magazine's Best Security Solution for Government and Best Security Solution for Healthcare.

To learn more about IAG 2007 or to arrange for a free onsite evaluation, please visit:
**http://www.microsoft.com/iag**

# SSL VPN Access: Not as Simple as It Seems

SSL VPN vendors preach the simplicity of their solutions, and in most respects SSL-based access is easier to implement and maintain than alternative remote access technologies. Yet, there are numerous complexities inherent in SSL access, many of which generate security concerns.

An SSL VPN solution is not complete unless it includes:

- Application-level access for major applications

- An application firewall

- Rich endpoint client security

- Granularity and flexibility to meet all customer needs

The remainder of this document examines SSL access-related issues and security concerns, as well as how IAG 2007 addresses these challenges.

Building on Whale Communication's SSL VPN technology and incorporating Microsoft Internet Security and Acceleration (ISA) Server, the IAG 2007 integrates SSL VPN, IPsec VPN, application security, network security and endpoint security in a single, flexible business-driven platform.

Integrated with ISA Server, IAG 2007 delivers a single, consolidated solution for network perimeter defense, remote access, and application-layer protection, providing organizations with a broader set of choices for their remote access requirements.

# Intelligent Application Gateway Technology and Features

## Remote Access Functionality

### Robust Application Support
IAG 2007 provides remote access to all types of applications – Web-enabled, client/server and legacy (such as Terminal Services or Telnet).

### Remote Access to Email
Many enterprises deploy SSL VPN technology in stages, with remote access to email the first step in the process. Application-specific Optimizers simplify implementation of secure remote access to popular productivity applications such as Microsoft Exchange and IBM Lotus Domino, ensuring a smooth transition for companies into the world of Web-based remote access.

### Application-Level Communications
Although many SSL VPN vendors claim to support application-level communications, when faced with supporting complex applications most resort to tunneling data over a network-layer connection. As a result, remote devices are often connected directly to the corporate network, rendering access from non-corporate owned or controlled machines a grave security concern. In addition, the need to download a component to implement the connection could create incompatibility issues (since many endpoints will not allow component downloads) and in turn generates support and helpdesk costs when users cannot connect successfully.

The IAG 2007, on the other hand, does not depend on network-level communications to provide access; network-level communication is provided as an option but organizations are not compelled to use it to provide access to complex applications as they would be with other SSL VPNs. IAG 2007 is able to provide true application-level access even with non-standard applications due to the flexibility of the platform and the underlying Application Intelligence technology of the solution.

### Application Intelligence and Application Optimizers
Application Intelligence is the foundation for standalone software modules known as Intelligent Application Optimizers that are pre-configured for out-of-the-box security and remote access functionality enhancements. These Optimizers, the result of in-depth research into application behavior, browser-server interaction, and use of client components, encapsulate pre-defined logic and incorporate default settings and values for specific applications.

The Optimizers provide an intuitive wizard-driven policy management interface for customizing access to match particular enterprise requirements, saving the administrator from the complexities of configuration and policy setting.

The Intelligent Application Optimizer developed for Microsoft SharePoint® Portal Server is one example. It offers full integration between the Web portal and Microsoft Office, allowing documents to be opened, edited and saved on a SharePoint server remotely as if from a local file server.

The Web Services client-side component of SharePoint Portal Server does not recognize SSL VPN authentication. This component was found to behave the same way with any SSL VPN tool that works as a Web proxy.

The result is that the SSL VPN gateway rejects Web Services requests as unauthenticated. The only way that SSL VPN vendors were able to allow Web Services access to SharePoint Portal Server was 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.

IAG 2007's SharePoint Application Optimizer implements application access policy both at the SSL VPN gateway and at the client side. Together with the Attachment Wiper™ (discussed in detail later in this document) the Optimizer allows secure Web connection to SharePoint Portal Server *and* full document collaboration from anywhere.

## Non-HTTP Applications: Methods of Communication

The IAG 2007 can transmit non-HTTP traffic over SSL in two ways.

1. Port forwarding: An SSL VPN component listens on a specific local address and port for each application, and causes the application to send the traffic to this address rather than to the address of the real application server. The SSL VPN client then tunnels the traffic within SSL and sends it to the SSL VPN gateway. Port forwarding is secure since the SSL VPN has application-specific knowledge and provides tailored security accordingly.

2. Socket forwarding: The SSL VPN client component hooks into the Microsoft Winsock service provider interface and uses Windows LSP/NSP (Layered Service Provider/Name Space Provider) interfaces to provide low-level handling. The NSP is used to resolve internal server names to ensure that they will be tunneled. One major security advantage of socket forwarding is that the SSL VPN client is able to identify the user and the process generating the traffic, and set appropriate application-specific security parameters. In addition, split tunneling can be avoided by trapping and forwarding all traffic to the SSL VPN gateway. Socket forwarding is far more secure that creating a virtual network adapter (as other SSL VPNs typically do) for the following reasons:

   a. Creating a virtual network adapter and tunneling network-level information circumvents network firewall security (as discussed earlier in this document). An SSL VPN would need to perform stateful inspection similar to that done by a network firewall if network-level access were to be made secure (and no SSL VPNs offer such a capability).

   b. Since a virtual adapter is normally implemented in kernel mode, it is not easy to associate the tunneled traffic with a specific application and to offer application-intelligent or user-specific security. One example of the many consequences of this weakness is that in multi-user environments such as Windows XP, one user may be able to access an SSL VPN tunnel opened by another user! As a result, in addition to the reasons described earlier, virtual network communications should never be used from a machine not under organizational control.

## Robust File Access Capabilities

An essential element of any remote access solution is its ability to allow users to access files remotely that are stored on drives and other repositories in the office. IAG 2007 provides two forms of remote file access.

- Remote Drive Mapping – IAG 2007 provides file sharing with the familiar naming and letter classifications used by users when working in the office. The Drive Mapping feature leverages the SSL Wrapper to enable mapping from a client machine to permitted drives on the network without using any network-level communications. Users gain the ability to work with network files as if they were on the LAN (i.e. accessing the X:\ drive), and can

use client applications that require a network connection to a particular share.

As opposed to all other SSL VPNs that offer such access by establishing a low-level connection back to the LAN (which should under NO circumstances be allowed from machines on non-trusted networks), IAG 2007 connects using Smart Port Forwarding Technology, without ever creating network-level communications. As a result, file access can be offered to partners and other semi-trusted parties without concern for security. Of course policies regarding which drives are available may be set based on User ID and endpoint policies.

- File Access GUI - In addition to access via Internet Explorer, the Intelligent Application Gateway provides a powerful Explorer-like interface that can be accessed from any standard Web browser. Access is available to both Novell and Microsoft file systems. Numerous file management functions are available, as can be seen in the following screenshot.
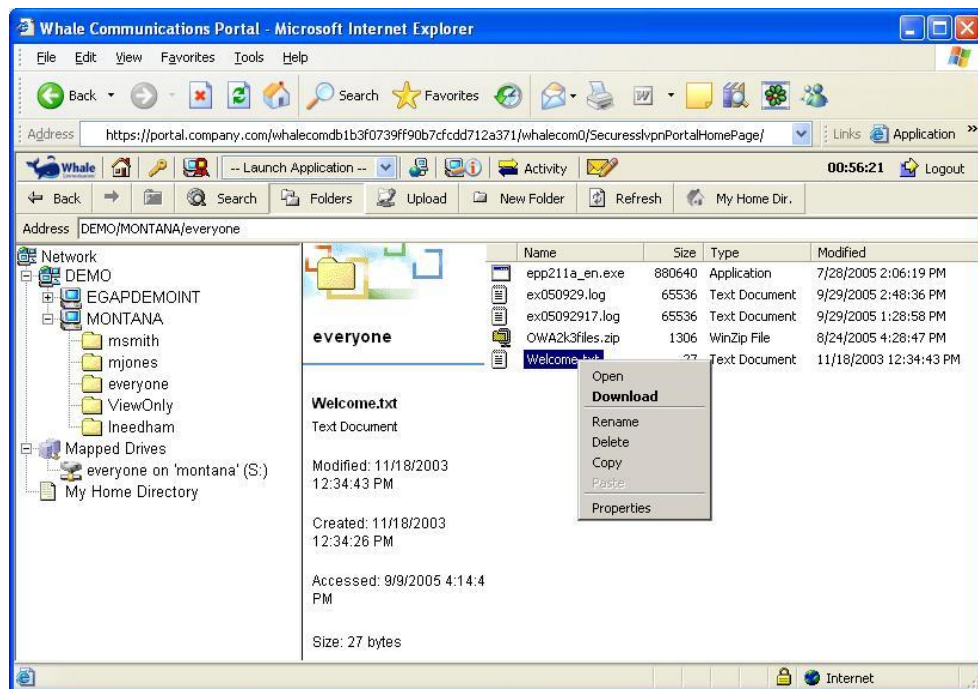


**Password Management for Remote Users**

Sound security policies dictate that passwords be modified periodically; if an organization forces its users to 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 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 the security benefits of enforcing smart policies surrounding password management, the password management capabilities offered by IAG 2007 lighten the burden placed on support personnel by password expirations. Remote employees can update passwords independently rather than being forced to involve helpdesk and IT staff.

## Performance and Scalability Features

Designed with the requirements of large enterprises in mind, IAG 2007 accommodates the needs of even the largest of organizations, and has been time-tested in large production environments.

**High Performance**

The IAG 2007 is sold as an OEM appliance that scales to support thousands of concurrent user sessions.

**Load Balancing/Global Load Balancing**

Fault tolerance and increased performance for IAG 2007 can be achieved through arrays (up to 64 nodes), and appliances can be used in conjunction with an external load balancer. It also fully supports global load balancing.

**Support for Multiple SSL Access Points on a Single Appliance**

The IAG 2007 can be configured to run multiple virtual SSL VPNs on a single appliance. In this way, an enterprise can offer employees and partners completely different access mechanisms without incurring the unnecessary expense of duplicating its remote access infrastructure. Multiple access point functionality also allows enterprises implementing "Chinese Walls" and other regulatory-mandated separations to conform to legal requirements and simultaneously provide remote access to all users without having to replicate remote access infrastructures. In order to provide multiple access points with other SSL VPN products, an enterprise would need to purchase multiple appliances, costing far more in both purchase dollars and long-term management.

In addition, IAG 2007 can simultaneously serve as an SSL VPN and an access platform for other SSL-based activities including those performed by prospects, customers, and even Web Services.

**Support for Multiple Languages**

A natural requirement of global deployments, IAG 2007 supports applications using non-Latin character sets and can support multiple languages, even within a single SSL VPN configuration. Furthermore, home pages, error messages and toolbars, etc. can be configured to appear in different languages based on the user's identity or the location from which a user is accessing the SSL VPN. Such capabilities are important for multinational firms whose users do not communicate in a common language.

**Flexibility and Customizability**

As described elsewhere in this document, the ability of IAG 2007 to be adapted to its environment – or to multiple environments within an organization – provides for a much simpler enterprise-wide deployment (or expansion of existing implementations) than other SSL access products.

## Administration Features

**Application Modules Simplify Implementations**

IAG 2007 comes equipped with modules that simplify implementation of access to popular enterprise applications. Instead of having to tangle with complicated technical configurations as they would with other SSL VPNs, administrators simply select the application they require from a list provided out-of-the-box and IAG 2007 performs much of the configuration automatically. IAG 2007 offers the ability to manually modify configurations for situations in which non-standard back-end application configurations exist.

**Web-based Monitor**

The Web-based Event Monitor shows the status of the entire system and a snapshot view of specific user session events. The Event Monitor is integrated within the system not only as a monitor tool, but as an SSL VPN-supported application with its own Intelligent Application Optimizer. This allows the administrator the flexibility of local management as well as secure remote management.

A unique monitoring tool in the Event Monitor is a session snapshot monitor, which allows the administrator to examine user activities and zoom into a user's session in real time. This is an essential tool for an enterprise-class SSL VPN solution handling thousands of concurrent users. IAG 2007 works at the application level and therefore provides troubleshooting tools for quick resolution of users' application access problems.

Example: A user notifies the administrator of failure to launch a specific application from his SSL VPN portal. The administrator opens the Event Monitor, zooms into the user's session and discovers that the application failed because the Attachment Wiper is not installed, meaning that the endpoint is not compliant with the application's access policy requirements. The administrator instructs the user on how to download and install the IAG 2007 client components, and then to access the SSL VPN gateway again. The user successfully launches the desired application.

**Logging**

The Event Logger logs and records gateway related events in a variety of tool and output formats. Using the event logs, the administrator can gather information about system usage and user activities, and request alerts about security events.

The following event logging reporter tools are supported:

- The built-in reporter logs the events in an internal format used by the Event Monitor and report generator. The administrator can use the Event Query to filter events according to type, time, etc. and generate a report.

- The RADIUS reporter sends events to a RADIUS Accounting server. This server can be any external RADIUS Accounting server, or Microsoft Internet Authentication Server (IAS) - a standard Windows RADIUS Accounting server configured to run on the gateway's internal server.

- The Syslog reporter reports events to an external industry-standard Syslog server.

- The Mail reporter sends email messages regarding specific events via an SMTP server.

**Reports**

Events recorded by the event logging reporter can be queried and retrieved. IAG 2007 provides a powerful tool for selecting, filtering and sorting the required events by numerous parameters. The administrator can display an on-screen report, print or extract a report to Microsoft Excel format for further data manipulation. For example, he can calculate the number of users currently logged into the system at peak time, or create a chart illustrating system usage trends over time.

**GUI-based Security Management Tools**

IAG 2007 includes several password-protected, GUI-based applications, providing for administration. In the High Availability array, master/slave capabilities assure consistency of rules across multiple systems. It also includes the Event Monitor, which can be run on the appliance's internal server or on any machine within the back office or network accessible to it, and offers robust operations monitoring and management capabilities.

**Standard OS Simplifies Management**
While most SSL VPNs utilize proprietary operating environments based on Linux, IAG 2007
utilizes a Microsoft Windows environment, greatly simplifying management of the gateway.
Standard management tools can be used in an environment already familiar to administrators.


## Security Features

Activity on a machine used to access an SSL VPN can directly affect the security of an
organization's internal network; the fact that an SSL VPN appliance is hardened does nothing
to combat many of the risks inherent in providing SSL access.  IAG 2007 has been widely
recognized for its powerful security innovations, and utilizes these technologies to ensure that
all aspects of security are properly addressed when enabling remote access.

Support for Strong Authentication and Standard Authentication Systems
IAG 2007 supports strong authentication from vendors such as RSA Security, Vasco, Swivel,
ActivCard, Aladdin and others. It interfaces with numerous authentication systems and
protocols such as Active Directory, RADIUS, LDAP, NTLM, Lotus Domino, and TACACS+. It
also supports PKI-based authentication (Client Certificates) as well as any user-defined
authentication scheme.

Authentication is performed by IAG 2007 at the network edge, eliminating the risk of
unauthenticated users attacking internal systems since users cannot communicate with
internal servers until after they are properly authenticated.

Login pages are completely customizable by the administrator; all HTML and DHTML features
may be used when constructing customized login pages.


**Single Sign-on**
IAG 2007 provides Single Sign-on capabilities. Credentials can be collected during the initial
login so users are not re-prompted for login information when selecting applications later on
during their sessions.


**Attachment Wiper**
The Attachment Wiper is a "virtual shredder"; on completion of a user session it erases all
traces of the session from the access device created during that session. It will be triggered
when:

- A user logs off.

- There is a timeout after a period of inactivity.

- The user is automatically logged off after a scheduled logoff threshold passes and the
  user does not re-authenticate.

- The browser crashes.

- The user closes the Web browser.

- The system is shut down.

The ability of the Attachment Wiper to ensure that security is maintained even after a browser
crash or system shutdown means that sensitive data will not be leaked, even under irregular
conditions.

The Attachment Wiper erases the following:

- Temporary files created by the opening of attachments during the user session.

- Browser cache entries created during the user session including non-standard caches
  such as those used by IBM Lotus Domino Web Access (iNotes) and Citrix Metaframe.

- Temporary files created by the downloading of files or any other mechanism during the user session.

- URL entries memorized for AutoComplete.

- Form-field contents memorized for AutoComplete.

- Cookies generated during the user session.

- Any history information created during the user session.

- Any user credentials memorized by the browser during the user session.

The Attachment Wiper is intelligent and will only erase information created during the user's SSL VPN session; all other temporary files, cookies, etc. will be left intact.

Additionally, 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. The file shredding feature also ensures compliance with HIPAA and GLB regulations.

As described elsewhere, policies may be created to govern when the Attachment Wiper runs, and how IAG 2007 handles situations in which it cannot run.

### Encryption of All Internal References

A major technical challenge associated with providing access to internal applications across the Internet is that of internal references within applications. Data, code and links may utilize system-naming conventions that do not work across the Internet. Although all SSL VPNs offer technology to perform translations of such references, each translation algorithm and implementation is unique. IAG 2007's host address translation engine encrypts all information related to the internal network so that external users never see anything that could be of assistance to them in launching attacks against internal resources.

### Secure Logoff

To prevent credentials from being cached on the access machine, IAG 2007 utilizes patent-pending Secure Logoff technology. This innovative proprietary mechanism is utilized by IAG 2007 as a replacement for "HTTP Basic Authentication," eliminating the possibility of malicious users reinstating user sessions.

### Inactivity Timeouts: Non-Intrusive and Application Intelligent

Inactivity timeouts are a necessary element of browser-side security and protect organizations from users who neglect to log off. Yet, implementing timeouts may greatly inconvenience legitimate users; an SSL VPN may automatically log a user out while composing a long email or completing a long Web form and may result in the user losing his work.

To combat this challenge, IAG 2007 utilizes non-intrusive timeouts whereby users are warned that a timeout based on inactivity is about to occur. The user then has the opportunity to prevent the timeout (as illustrated below).

IAG 2007 also offers non-intrusive forced periodic re-authentication. After an administrator-determined time window has elapsed, users must re-enter credentials to continue working. If they do, they resume exactly where they left off, even if they were in the middle of completing a Web form. Of course, if they do not, their session will be terminated (and the Attachment Wiper will be activated).

The timeouts used by IAG 2007 can distinguish between automatic browser requests and true user activity, so that even user sessions with applications that leverage automatic refresh requests to keep data at the browser current (such as Microsoft Exchange and Lotus Domino) will be terminated if there is no user activity. Other SSL VPN products often cannot distinguish

between user and computer-originating activity emanating from the browser and will leave such sessions live for an indefinite period.

**Endpoint Compliance that Addresses Business Needs**

Since SSL VPNs derive much of their potency from their ability to enable access from computers not under organizational control, enterprises must implement endpoint security policies to govern what level of access may be achieved from specific devices.

Corporate security policies governing access devices normally dictate conditions that must be met on the access device in order for users to perform specific business functions. Yet, until now, SSL VPNs often have not been able to fully implement such policies; rather, they provide only the ability to limit access to entire sessions – and not specific functions – based on endpoint conditions. As such, they have crippled access unnecessarily.

For example, when users accessed the SSL VPN from non-trusted machines without anti-virus software, instead of being permitted to download but not upload files, users were either denied file access altogether (resulting in loss of productivity and convenience) or they were given full file-system access (putting the organization at risk of becoming infected with a virus). Additionally, application-specific implementations of abstract concepts often caused incompatibilities with SSL VPNs. For example, there was no way to instruct an SSL VPN to "block attachment downloads from email messages" if the wiping of temporary files was not assured or to "ignore automatic refresh requests" when considering user activity for purposes of calculating session timeouts.

IAG 2007 offers several endpoint security capabilities in addition to those discussed earlier in this document:

1. To identify machines and set security policies accordingly, users can download client certificates from IAG 2007 (if security policies so allow). Administrators can configure various policies regarding who may request certificates, whether certificates can be generated automatically, whether delivery is immediate or delayed. Certificates can be presented during future access sessions to indicate to IAG 2007 that the machine is "trusted" and that appropriate security policies (i.e. more leniency than for non-trusted machines) should be used. Alternatively, IAG 2007 can check the client machine for specific files, registry values or even hardware devices (SmartCards or USB Tokens) to determine whether the system is a "trusted" device.

2. When corporate policies mandate that remote users use a specific service provider such as iPass so that policies are enforced, IAG 2007 will verify dial-up connection attributes and decide accordingly whether or not to allow access.

3. To determine the security level of machines not otherwise certified, IAG 2007 can scan the access device to check for conformity to policies set by the organization. It can check for anti-virus software, personal firewalls, and other security mechanisms as well as how recently the software was updated. Policies for the user's session can be dynamically set according to the results of this scan. The granularity of the IAG endpoint policy engine coupled with application intelligent technology allows for superior implementation of sound business policies than any other SSL VPN access solution.

The following table illustrates one example:

| Endpoint Status | | User Functionality | | | |
| --- | --- | --- | --- | --- | --- |
| Attachment Wiper Able To Run | Anti-Virus Up-To-Date | Send Emails | Send Emails w/ Attachments | Read Emails | Open Email Attachments |
| ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ✓ | ✗ | ✓ | ✗ | ✓ | ✓ |
| ✗ | ✓ | ✓ | ✓ | ✓ | ✗ |
| ✗ | ✗ | ✓ | ✗ | ✓ | ✗ |

**Encryption Optimization and Security**

IAG 2007 overlays industry-standard 128-bit encryption SSL on all application data to deliver data to prevent hackers intercepting and reading data and enabling employees to use a standard browser to securely access sensitive information. Only one SSL certificate is necessary, despite the fact that the user may access a number of different applications and servers.

IAG 2007 also allows centralization of SSL acceleration; organizations can invest in a single accelerator to be located centrally within IAG 2007 rather than implement individual accelerators for each application.

Additionally, IAG 2007 allows the SSL decryption keys to be kept on the secure internal network and be managed centrally by the IT security staff, rather than on a server-by-server basis by application managers or in the DMZ as required by other SSL VPNs.

**Application Firewalling**

An application firewall is a powerful tool against known attacks, and even against vulnerabilities not yet discovered or patched, and deploying an SSL VPN without an application firewall creates severe risks (see Appendix for more details.)

To protect against worms and hackers exploiting server vulnerabilities and compromising an organization's infrastructure, IAG 2007 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 also supports "negative logic" rules to specially block known attacks from reaching internal servers. Further, it enables generation of an IP blocklist, 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 during initial installation. For non-standard applications, IAG 2007 offers tools to automate the process of generating positive logic rule sets.

Another significant benefit of the application filtering capabilities is that patching internal servers becomes less urgent. Normally, failure to patch vulnerabilities on internal servers in a timely fashion could lead to disaster; with embedded application firewall technology running, however, all user activity is inspected and unrecognized requests will not reach internal machines so that patching against vulnerabilities becomes less critical.

# User Experience

**Fully Customizable User Interface (UI)**

The user interface of IAG 2007 (including elements such as the portal home page, toolbar, links and bookmarks) is entirely customizable.

**Customizable Home Page**

Upon successful login to IAG 2007, users are presented with a "home page" that can be customized by the system administrator. The home page typically provides links to applications, as well as a "URL bar" for entering URLs normally only accessible from the internal network (for example *http://hrserver*).

Home pages can be configured on a per-user, per-user-group or per-organization basis – offering enterprises the flexibility to provide users with menu choices of only those applications that are appropriate. For example, an engineer working in the MIS department may see Telnet and a Trouble-Ticket Tracking System among his applications, whereas an accountant in the finance department may see the Accounts Receivable and Accounts Payable systems.

Further, IAG 2007 can check whether certain applications have been installed on the device being used for access before displaying the menu of applications. Applications not installed (or outdated) will not be selectable from the portal page, thus minimizing help desk calls.

**Customizable Toolbar**

System administrators can configure IAG 2007 to automatically overlay a customized Internet Explorer-like toolbar at the top of every screen (or anywhere else on the screen), seen while accessing via SSL. The toolbar provides quick and easy navigation between applications, access to the logout button, a timer showing time remaining until the next forced re-authentication, and any other items the system administrator wishes to add.

**Support for Multiple Languages**

As is described elsewhere in this document, IAG 2007 supports applications using non-Latin character sets and can support multiple languages, even within a single SSL VPN configuration.

**Simplification of User Experience Reduces Help Desk Calls**

To reduce help desk calls and speed up problem resolution, IAG 2007 includes:

1. Informational messages while downloading the Attachment Wiper, SSL Wrapper, and policy compliance engines to the access device. When users enter the portal site address, they will be greeted with a page that explains that it is safe to select "Yes" on the ActiveX® installation dialog boxes, as well as a progress bar acknowledging the downloading of the components. This eliminates confusion and reduces help desk calls.

2. An information window can be displayed showing information about the current SSL VPN session. This window can assist technical support staff in debugging any support issues.

# Conclusion

IAG 2007 is clearly the most technologically advanced SSL VPN gateway on the market today, and the application access and security solution that delivers the greatest return on investment. It works with more applications than other SSL products, can service more types of user groups, and provides better security. Its granularity and flexibility ensures that maximum access is provided in a secure fashion. Perhaps most importantly, users prefer IAG 2007 because of the flexibility of its user experience. Implementing IAG 2007 improves productivity, lowers remote access costs, bolsters security and delivers a positive ROI on existing infrastructure and applications.

For further information on IAG 2007, or to arrange for a live demonstration, please contact: whaleinf@microsoft.com (Americas) or whaleeur@microsoft.com (EMEA).

# Appendix: Impact of an SSL VPN Platform on Infrastructure

## Why a Secure SSL Product Must Include an Application Firewall

When choosing to deploy an SSL-based access solution, it is instructive to understand a few important issues relating to their implementation.

One critical aspect often overlooked when selecting an SSL VPN is the potential impact on existing security technologies and infrastructure. When examined in a vacuum, many SSL VPNs are considered to be secure; when placed in a real-world infrastructure, however, they may undermine other security components and generate serious security vulnerabilities.

## Security Risks Created by Placing a Standard SSL VPN in a DMZ

Placing an SSL VPN in a DMZ poses a number of risks. The SSL VPN tunnels various protocols through the external firewall, but then rebuilds them in the DMZ. As a result:

- Numerous ports would need to be opened in the interior firewall, creating a serious security vulnerability and compromising corporate security guidelines.

- SSL decryption keys are maintained in an unsafe environment (the DMZ).

- Decryption is performed in the DMZ, so 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.
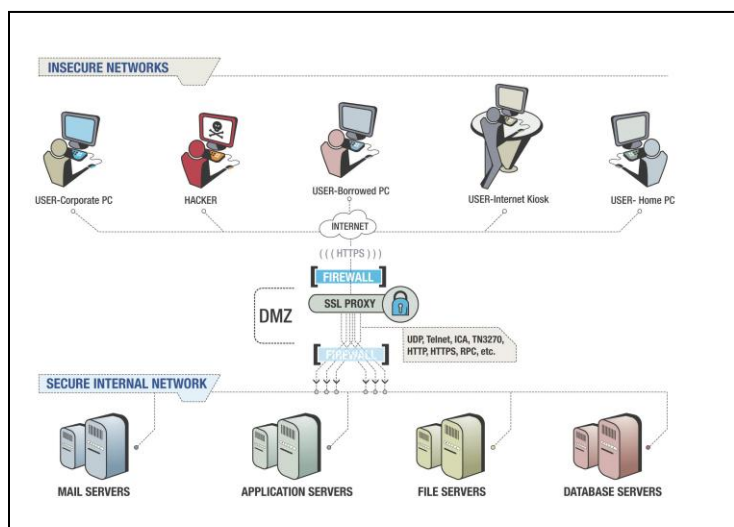


**Standard DMZ-based SSL VPNs tunnel network protocols into the internal network, undermining the perimeter firewalls and violating corporate security policies.**

## Security Risks Created by Placing a Standard SSL VPN in the Back Office

Placing the SSL VPN in the back office 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.
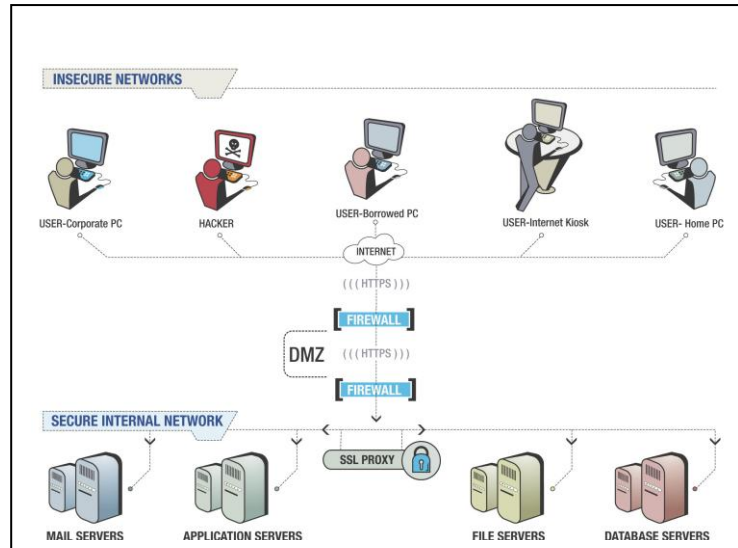


**Placing the SSL VPN in the back office also presents serious security risks.**

## Application Firewall Technology Allows Secure SSL VPN Deployment

For an SSL VPN to be safely incorporated into corporate infrastructure, it must incorporate built-in application firewall technology. This is similar in concept to the IPsec VPN which 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.
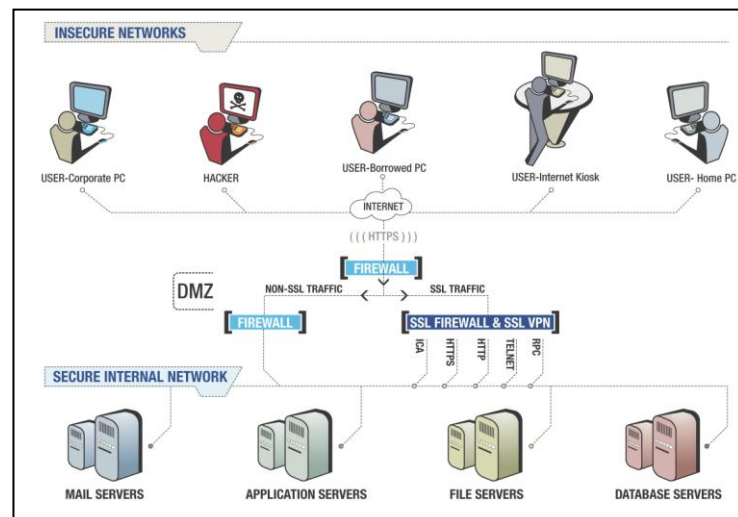


**Application firewall technology allows secure implementation of SSL VPNs**