

Intelligent Application Gateway 2007

Comprehensive Secure Remote Access Solution

Forefront™ Edge Security and Access products, Internet Security and Acceleration (ISA) Server 2006 and Intelligent Application Gateway (IAG) 2007, help protect your IT environment from Internet-based threats while providing your users with fast, policy-based access to corporate applications and data.

- **Secure Remote Access:** access for employees, partners, and customers from virtually any device or location
- **Branch Office Security:** enhanced connectivity and security for remote sites
- **Internet Access Protection:** increased resiliency for IT infrastructure from Internet-based threats

Control Access

Secure, browser-based access to corporate applications and data from more locations and more devices without requiring client installation and provisioning.

Protect Assets

Integrated application protection helps ensure the integrity and safety of network and application infrastructure by blocking malicious traffic and attacks.

Safeguard Information

Comprehensive policy enforcement helps drive compliance with legal and business guidelines which require information usage criteria to limit exposure and liability when accessing sensitive corporate data.

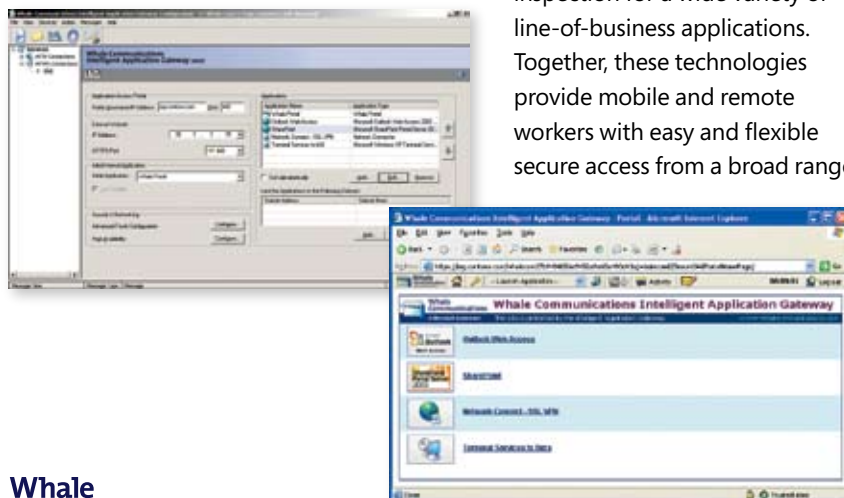
Comprehensive Secure Access

The Intelligent Application Gateway (IAG) with Application Optimizers provides SSL VPN, a Web application firewall, and endpoint security management that enable access control, authorization and content inspection for a wide variety of line-of-business applications. Together, these technologies provide mobile and remote workers with easy and flexible secure access from a broad range

of devices and locations including kiosks, PCs, and mobile devices. IAG also enables IT administrators to enforce compliance with application and information usage guidelines through a customized remote access policy based on device, user, application or other business criteria.

Integrated Appliance

The Intelligent Application Gateway is a comprehensive, high-performance application access and security appliance designed to help balance the tensions between security, application functionality and broad access. With the benefits of both a network-layer firewall (Microsoft® Internet Security and Acceleration Server 2006) and a full SSL VPN, the IAG delivers a policy-driven framework that unifies endpoint security, application access and access control in a highly-scalable platform to satisfy the demands of large-scale and complex environments. IAG can scale to a nearly unlimited number of users, supporting up to 64 high-availability nodes in a single array, and enables administrators to define complex authentication schemas, session residue shredding configurations and custom endpoint compliance requirements. The platform supports multiple portals on a single gateway, enabling administrators to customize the user experience and create specific policy configurations for each portal.



Intelligent Application Gateway 2007

Control Access

- Flexible application-intelligent SSL VPN from virtually any device or location.
- Differentiated and policy-driven access to a broad range of network, server and data resources.
- Highly granular access and security policy.
- Customizable, identity-based Web portal experience.

Protect Assets

- Integration with enterprise infrastructure helps ensure the integrity and safety of network resources and applications.
- Adaptable Web application firewall enforces app-specific filtering to protect apps from unmanaged PCs and networks.
- Extensive monitoring and logging helps drive policy compliance by tracking user activity and data usage.

Safeguard Information

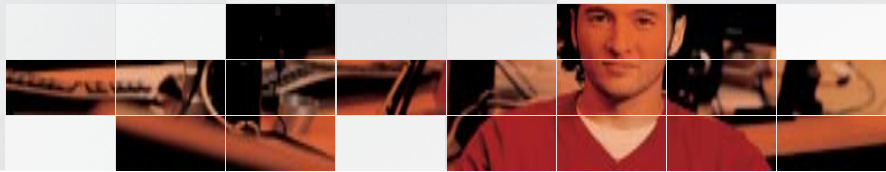
- Strong endpoint security management and verification helps ensure endpoint health compliance and session control.
- More granular control at the browser over users' access to Web and non-Web resources.
- Helps meet corporate information usage guidelines through client-side cache cleanup.

Application Optimizers

The IAG includes multiple Intelligent Application Optimizers, integrated software modules with pre-configured settings designed for secure remote access to widely used business applications. Optimizers enable endpoint security, application publishing and server request filtering for default values on a per-application basis to help ensure a flexible balance between achieving business objectives and enforcing network and data security. Included are customized granular access policy and security capabilities for Microsoft Exchange Server and SharePoint® Portal Server, as well as for many third-party business applications such as SAP, IBM Domino and Lotus Notes.

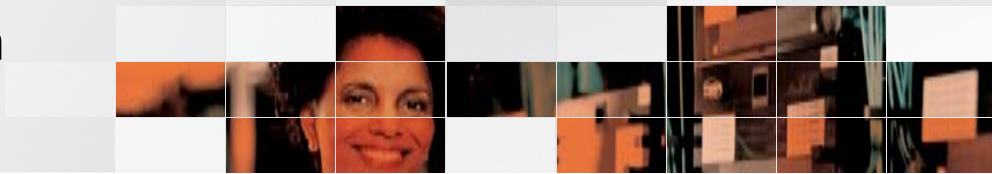
Functions	Connectivity		Access Policy	Application Security		Endpoint Security
	Single sign-on	Use as portal page	Limit access to application areas	Block functions	Application firewall	Attachment Wiper
Application Optimizer						
Exchange Outlook® Web Access	Yes	N/A	Yes	Upload / Download	Partial Positive	Yes
SharePoint Portal Server	Yes	Yes	Yes	Upload / Download / Edit	Full Positive Logic	Yes
Domino Web Access	Yes	N/A	Yes	Upload / Download	Full Positive Logic	Yes
IBM WebSphere	Yes	Yes	Yes	Upload / Download / Edit	Partial Positive	Yes
SAP Portal	Yes	Yes	Yes	Upload / Download / Edit	Negative only	Yes
Microsoft Dynamics™	Yes	N/A	Yes	Upload / Download / Export / Edit	Partial Positive	Yes

Intelligent Application Gateway 2007



Application	Features
<p>Microsoft SharePoint Portal Server Application Optimizer</p> <p>The preconfigured software module developed specifically for SharePoint delivers out-of-the-box capabilities to extend extranet access to SharePoint from any Internet-enabled device. The Optimizer provides the ability to:</p> <ul style="list-style-type: none"> • Ensure controlled access for unmanaged endpoints to SharePoint, enabling broader access that incorporates partners and customers • Delivers full Microsoft Office compatibility functionality without the need to download network tunneling components • Integrate third-party, legacy or client / server applications into SharePoint Portal Server 	<ul style="list-style-type: none"> • Web-based Single Sign-on <ul style="list-style-type: none"> • Web-based Single Sign-on incorporates out-of-the-box integration with any or multiple repositories supported by SharePoint (including native support for Microsoft Active Directory®). • Removes the need for multiple login steps and credential prompts for document access. • SharePoint Portal Server integration <ul style="list-style-type: none"> • Enables organizations to use SharePoint Portal Server as the main network entry point; After login, the user is sent directly to SharePoint Portal Server. • Embeds IAG components in a SharePoint Portal Server home page, including access to the IAG portal, file access, and IAG Toolbar to enhance the end-user experience. • Positive logic policy enforcement <ul style="list-style-type: none"> • Application firewall allows only known, non-malicious requests to pass to the SharePoint Portal Servers while blocking application-level attacks such as cross-site scripting and buffer overflow. • Intra-application policy enforcement <ul style="list-style-type: none"> • Policy framework enables Restrict/Permit Access to editing documents, uploading files, and downloading files based on endpoint inspection.
<p>Microsoft Exchange Server Application Optimizer</p> <p>The Exchange Server Application Optimizer enables a seamless user experience through support for Windows-based login scripts and Single Sign-on, removing the need for multiple authentication requests. In conjunction with implementation of the Client/Server Connector module, support is available for secure remote access to the native Microsoft Outlook® client with complete functionality as if accessed from within the LAN.</p>	<ul style="list-style-type: none"> • Web Single Sign-on <ul style="list-style-type: none"> • Remote access credentials delegated to native directories and email repositories to ensure user profiles and privileges are enforced. • Single Sign-on and Microsoft Windows®-based logon scripts leverage existing policy logic for quick configuration. • Endpoint security <ul style="list-style-type: none"> • Attachment Wiper clears downloaded pages and attachments. • Attachment viewing policies are based on endpoint attributes and the presence of the Attachment Wiper. • Application firewall <ul style="list-style-type: none"> • Out-of-the box positive logic rules configured specifically for Exchange Server and IIS to help ensure that only legitimate server requests are passed to downstream servers. • Supports multiple Outlook Web Access and Outlook versions through an intuitive wizard-driven GUI. • Secure logoff <ul style="list-style-type: none"> • Automates logoff and session inactivity prompts by filtering polling activity.
<p>Microsoft Dynamics Optimizer</p> <p>The Application Optimizer for Microsoft CRM 3.0 helps provide secure publishing of the CRM Web portal, with customized policies that handle CRM-specific user actions, security and information safeguards.</p>	<ul style="list-style-type: none"> • Upload / Download URL controls • Restricted Zones – Block Access to Settings area • Policy-based access control with Microsoft CRM 3.0 Enhanced Security <ul style="list-style-type: none"> • Disable printing • Disable export to Excel® • Allow / deny uploading attachments

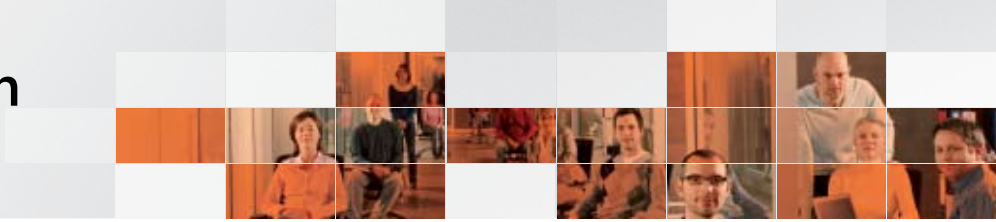
Intelligent Application Gateway 2007



Application	Features
<p>IBM Lotus Domino Web Access Optimizer</p> <p>The Application Optimizer for IBM Lotus Domino Web Access (DWA) allows organizations to fully harness Domino's value beyond the LAN while helping to preserve application functionality and protect network resources. The gateway helps protect the internal infrastructure by cloaking the application domain's IP addressing scheme and performing on-the-fly translation of internal Domino content.</p>	<ul style="list-style-type: none"> • Policy-driven access <ul style="list-style-type: none"> • Based on endpoint profile, attachment upload / download can be permitted or blocked. • Automatic server selection ("jump application") <ul style="list-style-type: none"> • Connects users to the appropriate server for messaging applications in multiple server environments, ensuring transparent access. • Endpoint security <ul style="list-style-type: none"> • Attachment Wiper cache cleaner is pre-configured to clear Domino-specific cached content. • Blocks forwarding with attachments and email history. • Web Single Sign-on <ul style="list-style-type: none"> • Users can be redirected to separate domains based on privileges and access rights. • Application firewall <ul style="list-style-type: none"> • Pre-defined positive logic rule set allows only valid commands. • Application-sensitive inactivity timeout <ul style="list-style-type: none"> • Automates logoff and session inactivity prompts by filtering out normal polling activity.
<p>IBM Lotus Domino Optimizer</p> <p>The IBM Lotus Domino Application Optimizer provides an integrated and out-of-the-box approach to securing and managing external Web-based access to the complete set of IBM Lotus Domino applications (including Domino Web Access).</p>	<ul style="list-style-type: none"> • Seamless user connection <ul style="list-style-type: none"> • Connects users seamlessly to the appropriate server for messaging applications in multiple server environments through transparent Lotus server selection and built-in "Webmail" redirect. • Full functionality for remote access <ul style="list-style-type: none"> • Enables use of Lotus Sametime from any access point, including non-privileged browsers without the need for tunneling from the endpoint client. • Supports Domino Offline Services enabling email to be read offline without a full native Lotus client. • Allows usage of full Lotus client strictly over HTTPS. • Web-based Single Sign-on <ul style="list-style-type: none"> • Remote access login credentials delegated to native directories and Lotus applications to help ensure user profiles and privileges are enforced. • Support for third-party authentication and authorization add-ons. • Endpoint security <ul style="list-style-type: none"> • Flexible policy editor provides ability to define custom checks for Lotus applications such as Sametime or Domino Offline Services. • Helps prevent users from bypassing download rules and forwarding content to external email accounts. • Application firewall <ul style="list-style-type: none"> • Out-of-the-box positive logic rules designed specifically for Lotus help ensure that only legitimate requests are passed to the server.
<p>SAP Enterprise Portal Optimizer</p> <p>The SAP-optimized solution provides granular, policy-based control over what areas or features of SAP applications and SAP Enterprise Portal the user has access to, enabling the best possible user experience, and heightens security through features such as custom cache cleaning and session timeouts, promoting increased productivity, reduced security risk, and lower costs.</p>	<ul style="list-style-type: none"> • Policy-driven access <ul style="list-style-type: none"> • Upload / download based on endpoint profile. • Control of local document editing and deleting based on endpoint profile. • Access to specific iViews – the iView will be displayed only if the applications have been assigned to the user. • Restricted access to personal folders. • Seamless portal integration <ul style="list-style-type: none"> • Users can be seamlessly directed to a portal with separately defined policies and secure Single Sign-on. • Enables support for SAP applications, third-party applications (such as email), databases and legacy systems. • Enables single application launch – no need for users to log in separately to SSL VPN portal. • Comprehensive security <ul style="list-style-type: none"> • Secured front end access (data encryption, reverse proxy). • Out-of-the-box application filtering (restricts certain actions on back-end servers, URL white-lists). • Endpoint checking. • Custom cache cleaning (local disk).

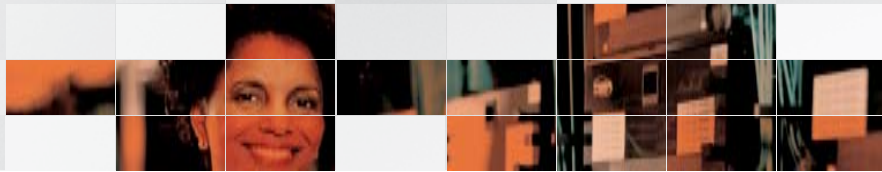


Intelligent Application Gateway 2007



Application	Features	
<p>Mobile Access Optimizer</p> <p>The Intelligent Application Gateway solution for Mobile Access provides a security-enhanced frontend to Exchange Servers, data encryption, and Microsoft ActiveSync® Single Sign-on for email push functionality. The Mobile Optimizer provides security-enhanced infrastructure for ActiveSync, a mobile micro-portal with two-factor authentication and mobile-specific login and logout procedures, and application command and URL filtering.</p>	<ul style="list-style-type: none"> • Mobile access micro-portal <ul style="list-style-type: none"> • The gateway supports a standalone portal for access from mobile devices to allow for separation of wireless traffic from Internet-based remote access activity. • Fully customizable micro-portal login, portal and logout pages. • Single Sign-on for mobile applications <ul style="list-style-type: none"> • Web-based Single Sign-on automates ActiveSync synchronization – no need for the additional login steps required with other SSL VPN implementations. • Full network separation <ul style="list-style-type: none"> • The gateway terminates traffic in the DMZ, avoiding the need for a direct connection from the mobile device to the Exchange Server. • Enforces user authentication and authorization. • Application-layer protection <ul style="list-style-type: none"> • Positive logic rules configured specifically for Outlook Web Access are designed to ensure that only legitimate server requests are passed on. • Enables the definition of restricted zones for mobile devices. 	
<p>Additional out-of-the-box supported applications</p> <p>With customized, integrated support for more than forty different applications and services, IAG provides one of the most comprehensive access experiences available. Pre-configured policies, application-specific security controls, and broad protocol support make it easy to give users secure access to business-critical infrastructure without extra effort.</p>	<p>Packaged solutions</p> <ul style="list-style-type: none"> • Windows Terminal Services / Web client • IBM Host-On-Demand • IBM WebSphere Portal 5.2 • Lotus Domino Webmail • Lotus Domino Offline Services • Lotus Sametime • PeopleSoft • SAP Enterprise Portal • Citrix Program Neighborhood • Citrix NFuse FR2/FR3 (SecureGateway) • Citrix Presentation Server • Citrix Secure Access Manager • NetManage Rumba Web-to-Host 	<p>Generic application support</p> <ul style="list-style-type: none"> • Apple Macintosh OS X Carbon applications • Web-based and browser-embedded applications • Client/server applications (e.g., RDP, RPC, ...) • HTTP proxy-enabled application (e.g., Microsoft Live Communications Server) • SOCKS enabled client applications • Enhanced host address translation (HAT) • Local drive mapping, Web-based file access • FTP • Telnet
<p>Application Optimizer Toolkit</p> <p>The Application Optimizer Toolkit enables policy customization for new applications, existing client/server applications and deeper modification of individual Optimizers to meet the needs of a specific enterprise implementation.</p>	<ul style="list-style-type: none"> • Extend existing Optimizers to build on standard configurations for specific business needs, and create new custom policies and content controls for in-house developed applications. • The IAG provides sophisticated policy editor features in order to help administrators define complex compliance checks, such as checking for anti-virus updates applied in the past week. The Advanced Policy Editor enables administrators to define policy using Boolean operations and new variables in place of labor-intensive policy management involved with competing SSL VPN appliances. 	

Intelligent Application Gateway 2007

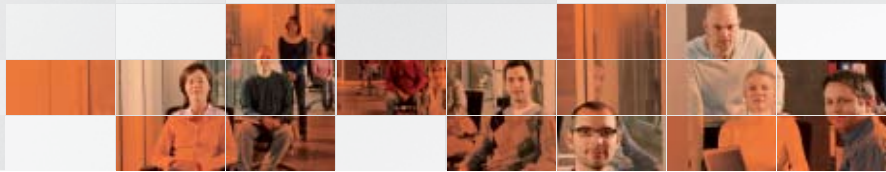


Product Features

Scalability	
Users	Supports an unlimited number of users on a single gateway.
High availability	Scales linearly with up to 64 high-availability node configurations.
Manageability	
Flexibility	Delivers out-of-the-box software configurations for widely-deployed enterprise applications, as well as customization capabilities including authentication, authorization and endpoint compliance profiles, and context-sensitive Web portals. Supports positive logic rule sets and URL filter customization, and has the ability to develop rule sets for customized or proprietary applications.
SSL VPN portal	Enables a convenient single access point for applications, yet supports multiple access points with distinct policy parameters such as partner extranets and employee portals on a single gateway.
Logging and reporting	Supports monitoring, logging and reporting for enterprise-level management and accounting (system, user security, and session views): <ul style="list-style-type: none"> • Event Monitor provides comprehensive event monitoring by user, application, and time period. • Integrated Event Logger that records system usage and user activities, and sends alerts about security events to an administration console. • Integrated Event Query tool with preconfigured query templates and full reporting capabilities.
Comprehensive policy framework	<ul style="list-style-type: none"> • Out-of-the-box application access settings and endpoint policy configurations designed to ensure minimal integration overhead and low ongoing management costs. • Supports Intelligent Application Toolkit for defining positive logic rule sets, URL filters to supplement Optimizer settings and to develop policies for customized or proprietary applications. • Supports Intelligent Application Template that provides a framework to build an Application Optimizer for both generic Web applications and complex enterprise applications incorporating components, web parts and objects.
Access Policy	
Endpoint compliance checks	Endpoint policy allows administrators to define compliance checks according to out-of-the-box variables including presence of security software and IAG-specific components such as Attachment Wiper. Supports complex endpoint policy rules with customizable compliance checks using Boolean operations.
End user experience	<ul style="list-style-type: none"> • Delivers a standard SSL VPN portal and log in pages to enable easy set up and low administrative overhead. • Supports comprehensive portal and login page customization to replicate existing intranet. Does not require conformance to a vendor portal template.
Integrated certificate authority management	Provides a built-in certificate authority in the event the administrator chooses not to use an external certificate authority. Enables administrators to grant a user a trusted endpoint certificate for a specific machine on request.



Intelligent Application Gateway 2007

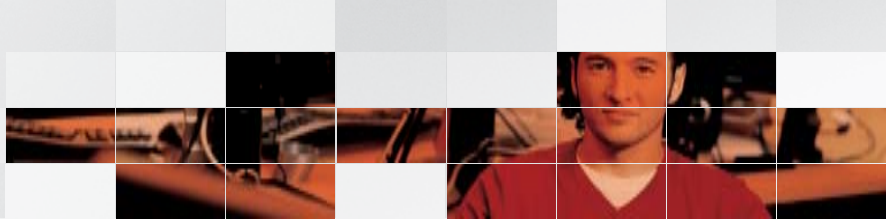


Integrated Solution Benefits

Your choice of access mechanism should be dictated by both business and security needs. Microsoft's goal is to provide a broad solution that can easily adapt to a variety of usage and deployment scenarios.

Deployment	ISA Server (2006) Standalone	Intelligent Application Gateway 2007
Branch Office Security	<ul style="list-style-type: none"> Gateway for site-to-site connectivity and security 	<ul style="list-style-type: none"> Delivered by ISA Server
Internet Access Protection	<ul style="list-style-type: none"> Data center Internet access control and Web caching with full network-layer firewall 	<ul style="list-style-type: none"> Delivered by ISA Server
Secure Remote Access	Control Access	
	<ul style="list-style-type: none"> Publish, secure and pre-authenticate access to specific Web applications (Exchange Server, SharePoint Server) 	<ul style="list-style-type: none"> Differentiated and policy-driven access to almost any application, network, server or data resources Flexible application-intelligent SSL VPN from any device or location Highly granular access and security policy, including intra-application controls Customizable, identity-based Web portal experience
	Protect Assets	
	<ul style="list-style-type: none"> Network edge protection through stateful packet inspection Application protection with advanced protocol filtering and validation 	<ul style="list-style-type: none"> Deep application content inspection and filtering with input validation and granular upload / download controls Adaptable Web application firewall enforces app-specific filtering to protect apps from unmanaged PCs and networks Integration with enterprise infrastructure helps ensure the integrity and safety of network resources and applications Extensive monitoring and logging helps drive policy compliance by tracking user activity and data usage
Safeguard Information		
<ul style="list-style-type: none"> Full IPsec VPN network connectivity integrated w/firewall engine for managed-PC access 	<ul style="list-style-type: none"> Browser-based full network access Strong endpoint security management and verification helps ensure endpoint health compliance and session control More granular control at the browser over users' access to Web and non-Web resources Helps meet corporate information usage guidelines through client-side cleanup 	

Intelligent Application Gateway 2007



Connectivity Modules

Client/Server Connector

The Client/Server Connector provides out-of-the-box secure access to business-critical client/server applications including Microsoft Exchange, Lotus Notes native client, Citrix, Microsoft Terminal Services, FTP and Telnet while allowing straightforward configuration for any additional client/server application through a generic application definition tool.

Tunneling modes

- *Port Forwarding:* The client component listens on a specific local address and port and causes the application to send the TCP traffic to this address rather than to the real application server's IP address. The SSL VPN client then encapsulates the intercepted traffic within SSL and sends it to the gateway. This mode functions optimally for applications using static TCP ports, or with applications supporting an HTTP or SOCKS proxy.
- *Socket Forwarding:* The client component hooks into the Microsoft Winsock Service Provider interface. It uses Windows Layered Service Provider/Name Space Provider (LSP/NSP) interfaces and provides low-level socket handling. The NSP is used to resolve internal server names to ensure they will be tunneled. It provides full support for all Winsock applications – TCP and dynamic ports.

Network Connector

The Network Connector allows administrators to install, run and manage remote connections that give users full network-layer connectivity over a virtual and security-enabled transparent connection and give users the same functionality they would have if they were connected to the corporate network.

- The Network Connector Module provides external users with a local IP address as if they are on the network, allowing for remote access to corporate servers and complex systems such as file shares and internal databases over secure network-layer connection (shared folders).
- The Network Connector Module tunnels almost any IP-based protocol, enabling support for Voice over IP (VoIP).
- The Network Connector's ability to implement a direct connection to departmental servers based on user identity, rather than mandating a fully open network-layer connection for all users through the SSL VPN gateway directly to the LAN, delivers significant security benefits.
- Provides administrators with the options of launching the connection immediately after user login using a predefined script, following compliance check, or on demand by the user by clicking the Network Connector icon on the portal page once authorized.

Best of Both Worlds

Integrated with ISA Server 2006, IAG 2007 delivers a single, consolidated appliance for network perimeter defense, remote access and application-layer protection over both SSL and IPsec connections, providing businesses with a broader set of choices for their remote access requirements. Integration of SSL VPN into existing Microsoft infrastructure supports secure access to both Microsoft and non-Microsoft applications and services from a single appliance.

The IAG 2007 appliance features a new streamlined and cost effective design that can help lower cost of ownership and removes the need for multiple devices from multiple vendors for different access methods. Your corporate IT group can adopt a consolidated security appliance solution that is flexible and easy to deploy.

Securing the Perimeter

ISA Server, combined with the Intelligent Application Gateway, serves the need for network separation and full control of inbound and outbound content and adds significant edge security functionality to address a broad range of Internet threats. The consolidated appliance provides a flexible software-driven solution that is responsive to the need for performance, management and scalability in addition to comprehensive security. The blending of stateful packet filtering, circuit filtering, application-layer filtering, Web proxy, and endpoint security into a single appliance affords the administrator a variety of options for configuring policy-driven access to applications and network resources.

ISA Server delivers the ability to filter traffic rather than rely on a mechanistic solution, providing three types of firewall functionality: packet filtering (also called circuit-layer), stateful filtering, and application-layer filtering. The ability to apply rule-based filtering to all traffic that traverses the network boundary enables the combined solution to directly address threats such as worms or malware that may originate from authenticated users.

Powered by:

Microsoft®
**Internet Security &
Acceleration Server 2006**

For more information about the Intelligent Application Gateway 2007, visit <http://www.microsoft.com/iag>.

This data sheet is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. © 2007 Microsoft Corporation