Intelligent Application Gateway 2007 Product Overview

Published: February 1, 2007

What Is IAG 2007?

Microsoft's Intelligent Application Gateway (IAG) 2007 with Application Optimizers provides secure socket layer (SSL) virtual private network (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. Key benefits include:

- A unique combination of SSL VPN-based access, integrated application protection, and endpoint security management.
- A powerful, Web-application firewall that helps keep malicious traffic out, and sensitive information in.
- Reduced complexity of managing secure access and protecting business assets with a comprehensive, easy to use platform.
- Interoperability with core Microsoft application infrastructure, third-party enterprise systems, and custom in-house tools.

IAG 2007 Components

IAG 2007 also 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 Microsoft SharePoint Portal Server, as well as for many third-party business applications such as SAP, IBM Domino, and Lotus Notes.

Adding to IAG 2007's portfolio of access tools are the connectivity modules: the Client/Server Connector and the Network 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 almost any additional client/server application through a generic application definition tool. The Network Connector enables administrators to install, run, and manage remote connections that give users full network-layer connectivity over a virtual and security-enabled transparent connection, and gives users the same functionality they would have if they were connected directly to the corporate network.

For more information, read the detailed IAG 2007 and Intelligent Application Optimizer datasheets. For a detailed list of IAG 2007 features and functionality, see the table on the IAG 2007 Key Feature Overview page.

Why Choose an Appliance?

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.

ISA Server, combined with IAG 2007, 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.

For more information about ISA Server 2006 and IAG 2007 appliance-based solutions delivered by OEM partners, review the Forefront Edge Security and Access Hardware Solutions page.

Usage Scenarios

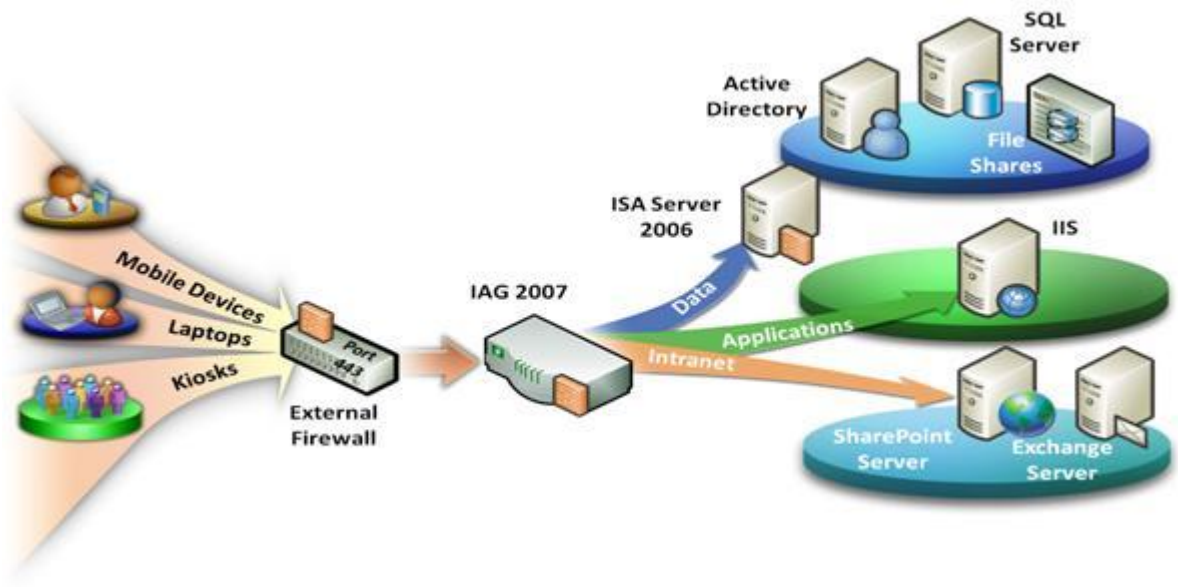
IAG 2007 is ideal for IT managers, network administrators, and information security professionals who are concerned about the security, performance, manageability, and reduced cost of network operations. IAG 2007 can help you:

- **Provide Secure Remote Access to Corporate Applications and Data.** IAG 2007 helps you control access through unified SSL VPN, application-layer filtering, and endpoint security management, providing employees with secure intranet access to critical applications, documents, and data from a broad range of devices and locations.
- **Strengthen Information Security Specific to Your Environment.** With flexible and differentiated access to extranet resources for employees and partners to Web and legacy applications, IAG 2007 protects infrastructure through easily adaptable application-specific security.
- **Defend Against Web-based Data Exploits and Theft.** IAG 2007 enables Internet-based and mobile access from unmanaged endpoints, and enforces proper information usage with granular identity-based policies, helping the business comply with legal and regulatory guidelines.

Read the solution scenarios below for more detailed information about how IAG 2007 can help you deploy secure remote access to corporate applications and data from almost any device or location.

Secure Application Access

Organizations require the ability to easily enable external access from unmanaged computers over the Internet to a range of enterprise resources located behind corporate firewalls, without requiring dedicated client software. IAG 2007 enables user access from diverse Internet-enabled endpoints through a single gateway to Web applications, file shares, high-value client/server applications, and network resources through an intuitive portal delivered over a policy-defined connection. To learn more, read about Secure Application Access with IAG 2007 .

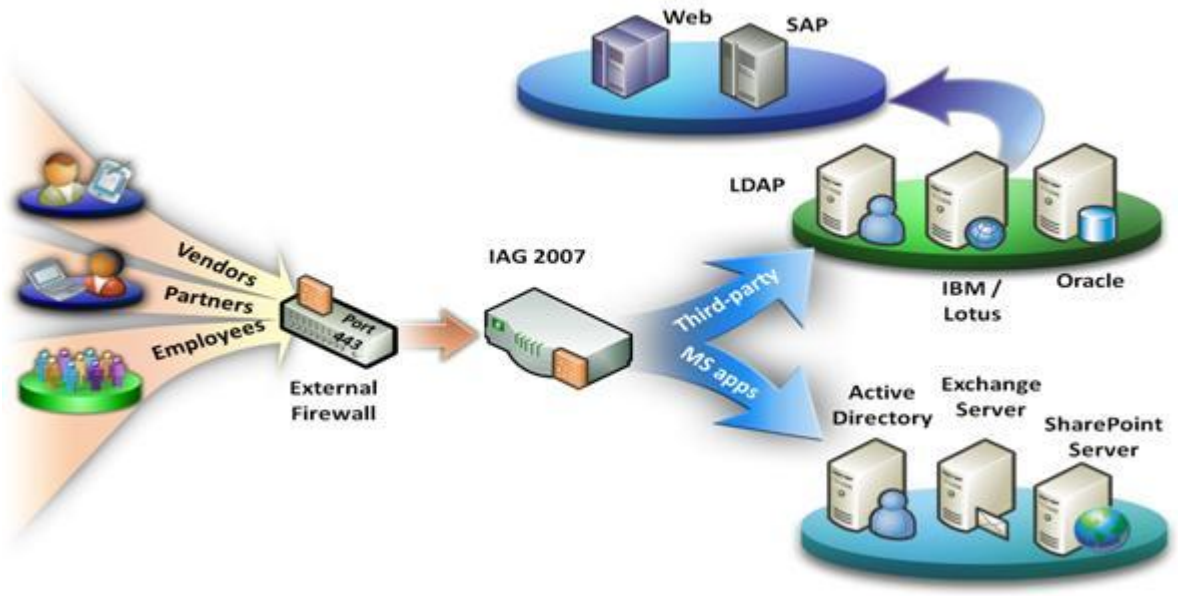


IAG 2007 provides:

- A fully customizable portal interface accessible from any Internet-enabled browser to deliver a consistent and easy end-user experience supporting single sign-on that helps ensure low support and training costs.
- Browser-based access to a wide range of Web applications that effectively handles embedded browser applications such as the Microsoft Terminal Services Web Client, Citrix NFuse and SAM, IBM Host-On-Demand, Lotus iNotes, and Instant Messaging.
- Connectivity and control for client/server and legacy applications, including generic client applications (HTTP Proxy and SOCKS enabled), FTP (passive), local drive mapping and UNC file shares, Terminal Services Client, Lotus Notes client, Microsoft Outlook for Windows 2000, XP, and 2003, and Telnet.
- Comprehensive authentication of mobile and remote users through integration with Active Directory, RADIUS, LDAP, and RSA SecurID via basic, NTLM, and forms-based methods as well as strong authentication options.

Customizable Enterprise Security

Corporate IT groups need mechanisms to protect internal assets from application-layer threats such as worms, viruses, and targeted attacks, while still enabling access to users outside of the corporate network. IAG 2007's application security capabilities insulate back-end servers from malicious traffic and deliver control over application-layer data published to external endpoints. The intelligent application delivery capabilities in IAG help ensure that no unsecure elements of an application—including buttons, links, text, header or cookies—are exposed via the browser. To learn more, read about Customizable Enterprise Security with IAG 2007.



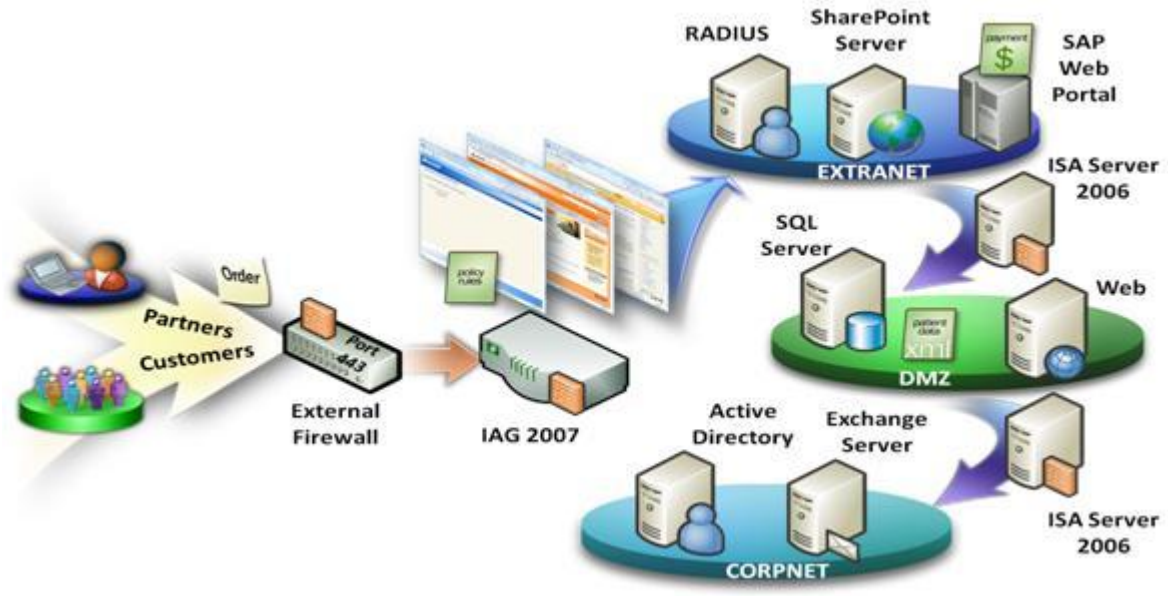
IAG 2007:

- Helps protect back-end servers with comprehensive protocol validation and deep content inspection that filters traffic through both positive and negative logic rule sets (block known attacks and illegal requests, and/or list and allow only valid application commands) against a wide range of HTTP parameters (such as method, value, header, and cookie).
- Helps ensure URL cloaking and full functionality for remote users through intelligent application delivery features such as dynamic URL rewrite and HTTP filtering.
- Delivers out-of-the-box protection for critical and high-value Web applications, such as Exchange Outlook Web Access, SharePoint, SAP Enterprise Portal and IBM Lotus and WebSphere through predefined rule sets.

Granular Information Protection

As organizations look to expand access to corporate resources to external users including employees, partners, vendors, and customers, they require a mechanism to help ensure that only healthy clients connect to the network and that all session residue is erased to avoid exposure of sensitive data.

IAG 2007's granular access controls, endpoint security, and cleanup tailored to specific applications enables organizations to maintain data integrity and drive compliance with legal or business regulations. To learn more, read about Granular Information Protection with IAG 2007.



IAG 2007:

- Extends utility of organizational resources through granular authorization policy defining which parts of an application or even which files a user has access to, based on identity and role and endpoint profile and device compliance. Through integration of workflow logic, IAG can be configured to make users aware of possible contraventions of policy mid-session.
- Delivers comprehensive endpoint security verification includes client-side policy and session management through pre- and post-session checks, including host integrity inspection of the SSL VPN client using an automated download manager, personal firewall settings, anti-virus updates, and system configuration and compliance information gathered from a broad range of endpoint security products (such as CA, McAfee, Microsoft, Symantec, Trend, and others).
- Cache wiping removes downloaded files and pages, auto-complete form contents and URLs, custom caches, cookies, history, and user credentials, with triggers for user and scheduled logoff, session timeout, browser crash or closure, and system shutdown.