Features

Forefront Unified Access Gateway (UAG) is a remote access solution that provides a gateway for managed and non-managed endpoints to access corporate applications and resources, as follows:

- **Remote Access to SharePoint and/or Exchange.** Optimized for SharePoint and Exchange, UAG delivers secure, anywhere access for your employees, partners and vendors. Leveraging a combination of granular application filtering capabilities, deep endpoint health detection and wizard driven configuration—UAG provides for a simple and highly secure means of publishing Exchange and SharePoint deployments.

- **Comprehensive Remote Access (SSL VPN).** As a comprehensive SSL VPN, UAG provides multiple levels of access and tunneling to deliver internal applications and network resources to remote users.

- **DirectAccess.** UAG extends the benefits of DirectAccess across the infrastructure, enhances scalability, and simplifies deployment and ongoing management.

Compare Forefront UAG with Intelligent Application Gateway

Forefront UAG Features

Application Publishing

Publish Web and non-Web applications by means of Forefront UAG trunks. You can create a portal trunk to provide a one-to-many connection with a single IP address, allowing users to access multiple applications from a consolidated portal gateway. You can also create a single-application trunk to provide a one-to-one connection; one IP address routes to a single published Web server, enabling access to any generic Web application.

Feature	Description
Web applications publishing	Provides an application layer inspection reverse proxy for publishing Web applications and Web farms. Application inspection provides positive logic inspection to ensure that only legitimate application connections are allowed. Forefront UAG application optimizers include out-of-the-box inspection settings for many key Microsoft and third-party applications.
RemoteApps publishing	Forefront UAG allows you to leverage Remote Desktop Services (Terminal Services) with an integrated Remote Desktop Services Gateway, to publish RemoteApps via a

	Forefront UAG portal.
Client/server application publishing	Forefront UAG allows you to publish non-Web applications over a secure connection using socket or port forwarding. You can request that users authenticate to Forefront UAG for access to user non-Web applications.
VPN client access	You can publish a VPN connection in a portal, allowing remote endpoints to connect to the internal network and access all network resources. For VPN client access, you can use the proprietary Forefront UAG Network Connector, or allow clients with SSTP support to connect using SSTP.
File access	You can publish internal file structures in a portal, thus allowing remote clients to access internal file servers and shares.

DirectAccess

Forefront UAG integrates Windows Server 2008 R2 DirectAccess to allow seamless connectivity to corporate networks regardless of location. DirectAccess can be configured directly in the Forefront UAG Management console.

- Extend access to line of business servers with IPv4 support such as Windows 2003 and non-Windows servers.

- Provide SSL VPN access for down level (Vista/XP) and non-Windows clients as well as PDAs.

- Enhance scale and management through array management capabilities and integrated load balancing.

- Simplify deployments and ongoing administration using wizards and automated tools.

- Deliver a hardened, edge-ready, solution that can swiftly be deployed.

Endpoint access controls

Forefront UAG provides a variety of mechanisms to control endpoint access to published applications, including:

Feature	Description
Client authentication	You can request remote clients to authenticate before establishing sessions to Forefront UAG sites, or allow anonymous access for passthrough authentication to backend servers. You can also configure single sign-on, so that credentials specified by users during session logon are passed to published servers that require authentication.

Endpoint access policies	You can set up endpoint policies with which endpoints must comply in order to gain access to Forefront UAG sessions and applications. Endpoint policies specify prerequisites that endpoint must meet for session access. Endpoint health can be inspected using built-in UAG policies or through integration with Network Access Protection (NAP).
Portal application authorization	When publishing applications and resources in a portal, you can enable application authorization to ensure that only specific users and groups can access the application.

High Availability and Array Management

Forefront UAG allows you to group multiple Forefront UAG servers into an array. All array members share the same configuration, and can be managed as a single entity. One of the array members acts as the array manager, storing configuration settings for the entire array. You can configure array members to use network load balancing (NLB) for high-availability and failover. Use integrated Forefront UAG NLB to configure NLB features of Windows Server 2008 R2 directly in the Forefront UAG Management console.

Enhanced Monitoring and Logging

You can log Forefront UAG events and errors to a variety of logging formats, including a built-in reporter, a RADIUS server, and a local or remote SQL server. Forefront UAG provides the Web Monitor console as a Web application for viewing events, and managing Forefront UAG sessions.

Appliance or Server Deployment Options

UAG is available as Hardware Appliances from the following OEM partners as well as server workload ("software-only") offerings. This provides for a wide variety of deployment options and flexibility in scaling.

Compare Forefront UAG with Intelligent Application Gateway

	IAG	UAG
Application Publishing		
Granular application filtering	√	√*
Session cleanup and removal	√	√
Endpoint health detection	√	√*
Integration		
Integrated with NAP policies		√
Remote Desktop and RemoteApp integration		√
Extends and simplifies DirectAccess deployments		√
Scale and Management		
Built in load balancing		√
Array management capabilities		√
Enhanced monitoring and management (SCOM)		√

*Feature is improved in UAG