Solution: Microsoft Forefront™ Unified Access Gateway 2010
Client: BrassLNG

Access Gateway 2010 delivers secure, anywhere-access to messaging, collaboration, and other resources, increasing productivity while maintaining compliance with policy. Forefront Unified Access Gateway provides a single solution for administrators to deliver access and implement granular policies based on the user's identity and the health of the device.

Overview

Forefront Unified Access Gateway 2010 delivers comprehensive, secure remote access to corporate resources for employees, partners, and vendors from a diverse range of endpoints and locations, including managed and unmanaged PCs and mobile devices.

Building on the secure remote access capabilities in Microsoft Intelligent Application Gateway 2007, Forefront UAG draws on a combination of connectivity options, ranging from SSL VPN to Windows® DirectAccess, as well as built-in configurations and policies. These enable Forefront UAG to provide centralized and easy management and thereby reduce management costs. In addition, Forefront UAG integrates a deep understanding of the applications published, the state of health of the devices being used to gain access, and the user's identity to enforce granular access controls and policies.

Key Features and Benefits

- **Access anywhere**

  Empowers users to be productive from virtually any device or location

  Forefront UAG acts as a consolidated gateway from a diverse range of endpoints and locations, providing access through a single portal. Remote users including employees, partners, and customers, can access Web and non-Web applications and gain full VPN access to corporate networks.

  Simplifies secure remote access Forefront UAG supports a wide range of Microsoft applications, including Microsoft SharePoint, Microsoft Exchange Server, Remote Desktop Services, and Microsoft Dynamics CRM through predefined optimizer modules. These modules include optimum settings and rules for securing specific applications and are based on deep research into application behavior, browser–server interactions, and endpoint requirements.

  Administrators can publish the following types of applications using Forefront UAG:

  - Web applications and Web farms via reverse proxy.
  - RemoteApps through a Forefront UAG portal by using Remote Desktop Services (Terminal Services) with an integrated Remote Desktop Services Gateway.
  - Non-Web applications over a secure connection using socket or port forwarding as well as VPN connections.

Extends Windows DirectAccess Forefront UAG delivers DirectAccess to legacy applications and resources running on existing infrastructure and supports down-level and non-Windows clients through integrated SSL VPN capabilities and other connectivity options.

- **Seamless and Secure Connectivity With DirectAccess**
  With DirectAccess in Windows 7 and Windows Server® 2008 R2, mobile workers can seamlessly and securely access the entire corporate network—file shares, intranet, and line-of-business applications—wherever they have an Internet connection. Forefront UAG works with DirectAccess to:
  - Extend these benefits to legacy applications and resources, and support down-level and non-Windows clients through integrated SSL VPN capabilities and other connectivity options.
  - Limit exposure associated with connecting unmanaged, down-level, and non- Windows clients through granular access controls and policies.
  - Protect the DirectAccess gateway with a hardened edge solution and built-in firewall.
  - Simplify deployment using built-in wizards and tools.
  - Support scalability and ongoing administration through built-in array management and integrated load balancing.

Integrated security

Enhances security and increases corporate compliance

- Limits exposure through a combination of granular access policies, deep endpoint health inspection, and user authorization information.
- Enables administrators to set up policies that specify prerequisites that endpoints must meet for each transaction. Endpoint health can be inspected using built-in UAG policies or through integration with Network Access Protection (NAP).

Enables a variety of strong authentication methods

- Integrates with Active Directory® and easily overlays a wide variety of third-party authentication solutions and repositories, allowing for strong authentication and enforcement through granular policies. This helps ensure that only authorized users or groups can access particular applications or execute transactions.
- Leverages credentials provided during a session to enable single sign-on to internal applications.

Simplified management

Reduces total cost of ownership by consolidating infrastructure

Delivers remote access connectivity through a combination of VPN, SSL VPN, Web publishing, and DirectAccess solution. This enables organizations to standardize and consolidate a disparate infrastructure onto one cost-effective platform.

Simplifies deployment and ongoing management

- Offers flexibility through form factors including hardware appliance (through OEM partners) and server software.
- Facilitates the grouping of multiple Forefront UAG servers into an array. All array members share the same configuration and can be managed as a single entity.
- Uses wizards to simplify initial deployment and key ongoing tasks.
- Easily integrates Forefront UAG logging through Microsoft SQL Server® and management through System Center Operations Manager.

Reduces support costs by simplifying connectivity for users

Typically security and access technologies are fragmented, resulting in a complex user experience. Forefront UAG consolidates access to corporate resources, simplifying the user's experience and reducing support calls and their costs.

System Requirements

Features and functionality described require a 2.66 GHz or faster processor with dual core CPU; 4 GB RAM; 30 GB available hard-disk space; Windows Server 2008 R2 Standard or Windows Server 2008 R2 Enterprise X64 bit editions; at least two network adapters.