Microsoft Forefront Unified Access Gateway and DirectAccess

Better Together

Disclaimer

Contents

Executive Summary

As the mobile work culture becomes more prevalent, the more important it is for organizations to have secure mechanisms for accessing the enterprise network from remote locations and devices. Enterprise IT groups, as a result, face growing demands on corporate networks to better serve geographically dispersed workers, remote employees, expanding networks of partners and vendors, and an ever-rising number of branch offices. Employees want to not only access information but to fully participate in business processes whether they are on or off the organization's premises. However, most organizations still face the challenges of facilitating quick and seamless access to corporate resources, keeping the assortment of remote devices up to date and well managed, and confronting ever-evolving security concerns. Additionally, organizations face the higher security risks and potentially higher IT costs that come with increased access.

To meet user demands and overcome the challenges associated with broad access to applications and information, many enterprises currently rely on disparate systems from multiple vendors that are difficult to integrate and manage. This white paper provides an overview of the Microsoft® solution for providing comprehensive, security-enhanced access. The solution combines the DirectAccess feature of Microsoft Windows® 7 and Windows Server® 2008 R2 together with Microsoft Forefront Unified Access Gateway (UAG) to help organizations provide seamless remote access to remote users while reducing IT risks and costs.

Who Should Read this White Paper

This white paper is intended for the following professionals:

- **IT Professionals** responsible for administering the solution, making software purchase decisions, and influencing the IT direction of their companies
- **IT Implementers** responsible for maintaining remote connectivity (from server deployment and network configuration to managing network security policies), ensuring that new networking technologies improve business needs, and helping remote users access the network without performance or other issues
- **IT Decision Makers** (IT Managers, Directors, Chief Information Officers, and others) primarily responsible for managing the staff that deploys, administers, and operates the remote access solution
- **Remote Infrastructure Optimization Managers** who work in branch offices and deal with latency, performance issues, and downtime (Most large and midsized companies have multiple locations. These offices are increasing in number and size, and do not normally have the best connectivity to the main office.)

Topics Covered in this White Paper

In this white paper, you will learn how DirectAccess and Forefront UAG can help your organization successfully adapt to the trends in remote access.

Connection in a Disconnected World | This section provides an overview of the state of remote access today and outlines the challenges that organizations face in adopting solutions.

The Future of Remote Access | This section examines the trends in remote access and describes what steps your organization needs to take to meet the security challenges of the future.

The DirectAccess Solution | This section provides an overview of the DirectAccess solution and discusses the benefits of combining DirectAccess with Forefront UAG.

Dealing with Real-World Scenarios | This section discusses three real-world scenarios and explains how organizations can achieve their business goals with DirectAccess and Forefront UAG.

DirectAccess + Unified Access Gateway Solution Architecture | This section provides an overview of the DirectAccess and Forefront UAG solution architecture and describes how the solution meets the needs of both managed and unmanaged clients.

Platform Integration | This section shows how DirectAccess and Forefront UAG can integrate with other Microsoft products to benefit your organization.

Conclusion

The future network will be viewed through a simplified web of seamless and security-enhanced connectivity. Enterprises will be able to empower remote employees, business partners, vendors, and customers to connect more readily to critical information when it is needed most. But while that world seems years away, the Microsoft DirectAccess + Forefront UAG solution can help you realize those benefits today.

Connections in a Disconnected World

Today's employees are more mobile than ever, and they expect to have unfettered access to the corporate intranet from wherever they are and on whatever device they use. As a result, enterprises need to securely expose their intranet resources to a growing network of partners and vendors, as well as to an ever-increasing number of branch offices across the world to facilitate business continuity. To stay competitive, IT groups are under increasing pressure to drive down costs by providing simplified access through corporate portals, yet it has been difficult to deliver this level of connectivity in a secure, manageable, and seamless way.

Infrastructure Challenges

Most organizations today run on a heterogeneous infrastructure—a mix of new and old clients, servers, and network services. To provide remote access to these systems from both managed and unmanaged clients, organizations will have to overcome the following challenges:

- Effectively managing access for multiple types of clients while using disparate management tools
- Providing partners and customers with access to corporate resources from machines that are not part of the corporate domain or are from untrusted sources
- Protecting the network from clients that do not meet established health requirements
- Separating trusted and untrusted domains while maintaining multiple directories and implementing different authentication methods

Network Access Technology Challenges

Historically, network access technologies have not kept pace with ever-growing connectivity needs and have had a high total cost of ownership (TCO). Additionally, network access technologies such as traditional VPNs typically do not provide quick and easy connectivity, limiting large-scale collaboration and impacting the efficiency of remote users. To complicate matters even more, enabling remote access means choosing from several options such as VPNs, Remote Desktop Protocol, Terminal Services, reverse proxy, and more. These technologies frequently pose the following challenges:

- Providing a remote connection with VPN technology that requires multiple user-input steps
- Keeping costs down and avoiding complicated technical problems with different access solutions from various vendors that are not always interoperable
- Managing remote computers without the ability of IT administrators to initiate inside-out connections
- Increasing system response-times resulting from firewall and (reverse) proxy translations
- Improving remote application performance and reliability with unpredictable network quality

These limitations and other security controls sometimes perceived as "oppressive" can further hamper user productivity.

There is virtually no remote access technology available that provides a single, comprehensive solution that fulfills all the connectivity needs of users and enterprises alike. To enable identity-based, policy-driven access to a new generation of clients and servers and to different types of down-level clients and legacy infrastructure, IT professionals have had to deploy multiple technologies and systems that complement each other. These disparate approaches typically come from different vendors and are complex to implement and integrate. Generally, managing a multi-vendor solution increases IT costs substantially.

As a best practice, it is important to recognize and plan to mitigate the following IT risks:

- Vulnerability of the underlying network
- Threats from managed and unmanaged clients and hosts
- Potentially untrustworthy users
- Inability to rely on location to dictate endpoint or link-level health

For always-on connectivity across networks that is both cost-effective and efficient, it is beneficial to focus on driving access decisions based on policy and a trusted identity, rather than on the limitations of network topology.

The Future of Remote Access

Addressing access needs in the twenty-first century means redefining the "edge" of the corporate network. The network edge is expanding beyond its role as a protective exterior to become a policy-driven boundary between differing usage practices and conditions used to insulate the datacenter and critical business resources. For example, you could be using a corporate-managed laptop and accessing your company's network while sitting in an airport lounge 2,000 miles from your office. Still, you want your network experience to be exactly the same as when you are plugged into the LAN: always-on, secure, and well managed. Everything should "just work," without requiring you to launch a connection manager, enter your credentials multiple times, and wait to clear quarantine— to ultimately get dropped from the network because you don't have the latest antivirus signature.

To meet the security challenges of the future and achieve your remote access goals, you will need to reduce operations costs and minimize security and business risks while:

- Unifying user identity, security, and access policies
- Adhering to regulatory guidance while providing access to users that work mostly outside the limits of your organization's network
- Rationalizing the ever-growing collection of remote devices, which can be IT-managed or not and may present incomplete or unreliable security state information
- Managing user accounts that cross organizational boundaries, competing protocols, untrusted networks, disparate directories, and authentication mechanisms

The solution is to deploy a consistent, easy-to-use, and manageable infrastructure with next-generation clients and servers that all use the same principles of policy and security when granting access. In practice, however, almost every network in the world is a heterogeneous mix of client and server operating systems, versions, protocols, legacy applications, and security systems—all of which must be supported, often at an increasing cost, as the infrastructure ages.

Organizations need a scalable, cost-effective, and unified approach to secure access that enables a simple yet powerful end-user experience from virtually any location or device, while protecting data, applications, and network resources from exploitation. The solution should support legacy infrastructure and applications to the greatest degree possible through an identity-centric, policy-based model with granular controls and endpoint health management.

The DirectAccess Solution

In general, remote access is easiest to implement and secure when all clients and servers are running the latest versions of Windows. However, administrators often find themselves supporting multiple operating systems for long periods, and providing a cost-effective solution to these machines is an important consideration. Windows Server 2008 R2 and Forefront UAG provide a consolidated, comprehensive, and security-enhanced remote access solution that enables users to stay connected with their corporate network regardless of location or device. Windows Server 2008 R2 and Windows 7—through the new IPv6-based DirectAccess service—deliver built-in policy-based technologies that form a robust platform offering virtually anytime, anywhere access to corporate applications and data, as well as bidirectional client management.

Through optimized integration of the latest Windows and Forefront technologies, DirectAccess and Forefront UAG seamlessly adapt to varying connectivity factors, including differences between managed (domain-joined) and unmanaged (not joined) clients, multiple network protocols (IPv4, IPv6), encryption standards (IPSec, SSL, and more), and legacy applications, thereby relieving the burden on the IT of administering a different system for each user class on the network.

DirectAccess enables organizations to provide always-on, secure connectivity to on-premises and remote users, improves security, and lowers TCO, enabling remote users to be more efficient with access to the right resources at the right time. With the addition of Forefront UAG, administrators can extend the benefits of secure remote access to users and applications still on older platforms through SSL VPN, enhancing scalability and availability while simplifying deployment and ongoing management.

DirectAccess and Forefront Unified Access Gateway are "Better Together"

With DirectAccess and Forefront UAG, remote workers and business partners can enjoy the same connectivity experience whether they are on-premises or at a remote location. As a result, users are always connected to the corporate network without needing to explicitly initiate connections or take extra steps to access resources remotely.

DirectAccess uses IPSec policies for authentication and encryption that allow IT administrators to implement many levels of authentication and authorization controls. The end-to-end security provided by IPSec allows security architects to precisely control who can access specific resources when they are remote, and helps ensure that clients will always be managed whenever they go online. This solution also supports peer-to-peer application scenarios such as instant messaging and helps enable trustworthy computing on the Internet, while facilitating security-enhanced communication and collaboration—even with end customers. Additionally, Forefront UAG helps provide non-domain joined clients with more simple and secure access to applications such as Microsoft Office SharePoint® Server 2007, Exchange Server, Dynamics® CRM, and many legacy applications.

Enterprise IT groups can implement compliance-driven remote access methods by defining granular policies over applications and servers. Integration with Windows Server and Domain Isolation (SDI) separates trusted and untrusted network traffic. DirectAccess enables organizations to implement inside- and outside-based network rules that restrict unwanted or malicious connections.

Forefront UAG further augments DirectAccess by helping IT Professionals improve manageability of remote resources through seamless, bidirectional access to remote PCs as if they were on the LAN. They can also push out security updates, retrieve hardware and software inventory reports, and install application updates. IT organizations can consolidate application gateways when they transition to a managed Microsoft DirectAccess + Forefront UAG solution.

	DirectAccess + Forefront UAG Solution
Enable Anytime, Anywhere Access	• Offers the same powerful experience both on- and off-premises with always-on, security-enhanced connectivity through IPv6 and IPSec • Protects corporate data and assets with enhanced policy-based strong authentication and authorization • Provides all IPv6-compatible network address translation technologies, including Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) in one solution for network extensibility and access from down-level and non-Windows clients • Supports peer-to-peer application scenarios such as Microsoft Office Groove®, Office Communicator, and Remote Desktop • Provides IPSec and SSL VPN access for both managed and unmanaged endpoints • Provides a simple and more secure remote user experience through a single portal • Grants access to legacy line-of-business (LOB) applications and resources with granular access controls and customizable application protection
Integrated Security	• Protects IPSec-based data such as 3DES and AES • Offers full compatibility with Server and Domain Isolation by isolating logical networks based on IPSec policy • Helps ensure device health compliance by tightly integrating with Windows Network Access Protection (NAP) • Supports multi-factor authentication technologies such as smart cards and tokens • Intelligently separates private and public data streams and traffic • Provides enhanced endpoint security for down-level clients, including integration with Microsoft Forefront Client Security • Protects the DirectAccess gateway with a hardened edge solution based on a proven architecture • Provides Application Optimizers for intelligent, functionality-based application-level security • Prevents information leakage with a client-side Attachment Wiper that deletes application-specific temporary files in the client's cache
Granular Policy-based Access	• Simplifies remote management of remote PCs and laptops • Provides enhanced Web-based monitoring and reporting on client health for driving policy compliance, on a consolidated access gateway for easier, centralized control and auditing • Helps reduce errors on common tasks with a single console for managing all remote access mechanisms for simplified wizard-driven configuration, deployment, and administration • Provides enhanced Windows Network Load Balancing-based scalability and availability with unified management of multiple nodes/clusters across different locations by using integrated server array management tools • Allows you to easily create and publish remote access policies for corporate portals • Provides enhanced policy-based management that incorporates two-factor authentication, validation, authorization, and granular policy controls over individual applications and servers • Offers an appliance as a pre-configured, ready-to-use virtual machine

The Benefits of Deploying DirectAccess and Forefront Unified Access Gateway Together

When Windows DirectAccess and Forefront UAG are deployed together they offer a unified, security-enhanced access solution across—as well as beyond—the enterprise environment. The combined value of these two technologies enables IT departments to deliver increased user productivity by striking a balance between exposing corporate resources to the outside world and maintaining security and regulatory compliance.

Forefront UAG extends the benefits of DirectAccess across your infrastructure, enhancing scalability and simplifying deployments and ongoing management.

Use DirectAccess to:

- Get always-on, bidirectional connectivity from locations inside or outside the corporate network through IPSec and IPv6
- Support pure IPSec and IPv6 environments (end-to-end), non-IPSec intranets with IPv6 application servers (end-to-edge), or IPv4-only application servers
- Provide seamless access to corporate resources with the same experience as being on the LAN
- Host and protect data by ensuring policy-based authentication and authorization for all devices, inside or outside of corporate boundaries
- Remotely manage, update, and monitor the health of remote computers even when the end user is not logged on
- Grant access to specific applications and servers based on an individual's identity and role

Add Forefront Unified Access Gateway to:

- Extend DirectAccess to legacy applications and resources running on existing infrastructure
- Support down-level and non-Windows clients using a variety of connectivity options
- Protect the DirectAccess gateway with a hardened edge solution
- Limit the exposure associated with connecting unmanaged, down-level, and non-Windows clients through granular application access controls and policies
- Minimize configuration errors and simplify deployment using built-in wizards and tools
- Enhance scale and ongoing administration through built-in array management and integrated load balancing
- Consolidate access gateways for centralized control and auditing

Dealing with Real-World Scenarios

This section includes real-world scenarios that show how organization's can meet their business and IT needs with a DirectAccess and Forefront UAG Solution.

	Scenario	Business Context	Solution: DirectAccess and Forefront Unified Access Gateway
Always On, Anywhere Access	**Branch Office and Field Personal:** An organization has decided to allow employees to access corporate applications and data from virtually any PC or device from virtually any location.	In many companies, branch office workers and field personnel need to connect to resources at the central office from subsidiaries, remote locations, or their homes. They require regular access to applications and data that are distributed across the enterprise.	• Enables workers to connect more securely to the corporate network using either IPSec or SSL VPN tunnels, depending on the type of device they are using • Allows the IT department to monitor and manage the updates and health of their remote computers • Simplifies connectivity and security policies by maintaining a unified and comprehensive set of rules for both types of access • Increases the organization's productivity without requiring employees to spend more time at the workplace
Remote Access from Heterogeneous Networks	**Business Partners:** An organization has a large number of partners and vendors who access the corporate network from different locations using both managed and unmanaged devices. With so many unmanaged devices, the organization is concerned about the security of their corporate data and needs a solution that helps prevent information leakage, spyware, and malware attacks as well as unauthorized use of data.	With recent trends in globalization and outsourcing, business partners frequently need to access corporate assets. Software as a Service (SaaS) and cloud computing has added to the complexities of securing company resources. The IT department needs to ensure secure access through a consolidated and well-managed point of entry from multiple endpoints to enterprise LOB applications—including Web, client/server, and legacy applications—while enforcing user authentication and authorization over a policy-defined application-layer connection.	• Leverages a policy-based framework that allows vendors and partners to have controlled and granular access to sensitive data and applications • Gives partners security-enhanced connectivity while ensuring that they access only relevant and authorized information, after ensuring the health of the remote device complies with policy requirements

	Scenario	Business Context	Solution: DirectAccess and Forefront Unified Access Gateway
Granular Policy-based Access	**Customer Portals:** An organization wants to enforce their security and compliance policies to prevent threats from untrusted networks used by their end customers, while allowing the right people to have access to the right information without requiring the IT department to manage separate and complex solutions for mobile devices, extranets, and home PCs.	Enterprises occasionally allow customers to connect to its environment to address specific client needs or provide up-to-date customer service information, which requires deploying a single, unified policy interface to control access from a broad range of devices, users, and network environments.	• Offers fast and easy access to end customers through a centrally managed gateway • Provides a single point of entry from multiple access points to customers through customizable and dynamic consumer portals that enhance the overall effectiveness of user participation in an organization's growth

DirectAccess + Forefront Unified Access Solution Architecture

The solution architecture below shows how using DirectAccess with Forefront UAG provides a better solution for both managed clients (Windows 7) and unmanaged or down-level clients (such as Microsoft Windows Vista®, Windows XP, non-Windows operating systems, and PDAs). Employees using managed, domain-joined clients can be automatically connected to the corporate network and access applications and servers through DirectAccess (IPSec and IPv6). Employees, partners, or customers using non-domain-joined (managed or unmanaged) clients need to initiate a connection via SSL VPN. When access is initiated, the client sends a request to the DirectAccess + UAG server along with its health statement. The DirectAccess + Forefront UAG server redirects this request to the Network Protection Server (NPS) to diagnose if the client trying to access the network is healthy or not. If the client is healthy, the user credentials are sent to Active Directory® Domain Services for user authentication. After being authenticated from both points, the client can now enable the secure tunnel session with the DirectAccess + UAG Server and protected internal servers.

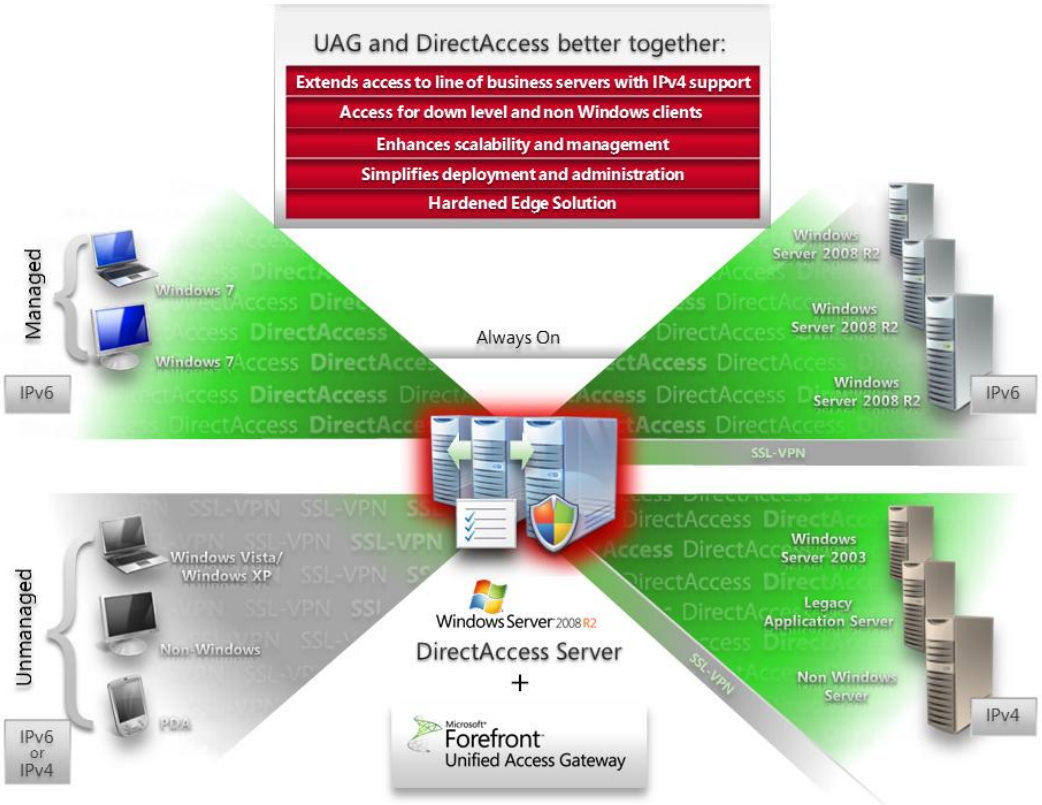

Figure 1: DirectAccess + Forefront UAG solution Architecture

Platform Integration

To provide remote access to various corporate applications and data, DirectAccess and UAG seamlessly integrate with technologies across the Windows platform, including client health technologies, messaging and collaboration servers, claims-based access, and identity management.

Identity and Access Management

By integrating DirectAccess with NAP from Microsoft, the IT department can assess and mitigate risks, while protecting assets from malware attacks. NAP is a platform that helps ensure compliance with mandated security policies and enables better protection of network assets. By integrating NAP with DirectAccess, the IT department can set system health requirements and verify compliance from client computers that access the corporate network from outside. Before managed clients connect to the network using DirectAccess, NAP forces them to meet security requirements, including updates, antimalware definitions, and other security settings. NAP can also be integrated with Forefront UAG to publish HRA Web services more securely, and to receive health information and issue certificates to external down-level clients. This enables employees, customers, and partners to stay productive regardless of location or device.

Identity Federation

Built on Windows Server 2008 R2 and Microsoft Forefront Threat Management Gateway, Forefront UAG provides integrated and comprehensive protection from internet-based threats. By integrating Forefront UAG and DirectAccess with Microsoft Code Name “Geneva,” Forefront UAG can extend the claims-based access platform to remote users and can use the capabilities of “Geneva” such as identity federation,

authentication, and single sign-on to provide simplified, unified, and security-enhanced user access to corporate resources.

Support for Secure Messaging and Collaboration

Enterprises increasingly rely on corporate portals such as SharePoint as a means of driving business operations through Web-based collaboration, looking to extend their accessibility beyond the intranet to the extranet. Extending access beyond the confines of the network through the Web allows enterprises to communicate with a broader set of users beyond employees to partners and customers. To provide such functionality, Forefront UAG can be optimized to integrate with collaboration technologies such as SharePoint. Using Forefront UAG, SharePoint portal functionality can be extended by integrating it with client/server applications and network resources. Integration of UAG with Active Directory and Web-based single sign-on enables enterprises to provide its remote users with easy and more secure access to their SharePoint portals. Forefront UAG offers pre-defined rules and policies to provide compliance for SharePoint, and integrates endpoint assessment and strong authentication into access and usage policies.

Forefront UAG is optimized to deliver employees, customers, or partners with security-enhanced access, from virtually anywhere, to their e-mail messages to help improve productivity. IT professionals can use built-in policies and rules to drive compliance for clients accessing Exchange Server from outside the corporate network. They can integrate strong authentication and endpoint health assessment policies with the security policies of Exchange Server to ensure that clients requesting access to their e-mail are healthy. With Forefront UAG, enterprises can create and publish remote access policies for Microsoft Outlook Web Access, Outlook Anywhere, Outlook Mobile Access, and ActiveSync® to ensure better security for remote users. Integration of Forefront UAG with Exchange Server drives scalability and provides efficient load balancing, offering remote users seamless access to e-mail messages.

UAG helps in delivering secure, anywhere access to collaboration platforms such as Dynamics CRM for employees, partners, and customers. Enterprises can empower employees, partners, and customers by delivering a simple and secure remote user experience for collaboration tools. IT professionals can easily drive compliance using out-of-the-box rules and policies for Dynamics CRM. Such integration helps to protect information and prevent leakage using built-in cache removal utility and access policies.

Conclusion

DirectAccess provides Windows 7 users with seamless, security-enhanced access to enterprise resources and data from virtually anywhere. This anywhere, anytime connectivity provides users the flexibility they need to be more productive while ensuring that security is always maintained. Forefront UAG ensures that virtually any user on virtually any device can securely connect to the corporate network, providing additional management and deployment tools that simplify the DirectAccess environment.

Resources

- Microsoft Forefront Unified Access Gateway Roadmap
  http://www.microsoft.com/forefront/prodinfo/roadmap/uag.mspx
- Microsoft Network Access Protection (NAP)
  http://microsoft.com/nap
- Microsoft DirectAccess
  http://www.microsoft.com/servers/directaccess.mspx
- Microsoft DirectAccess Introductory Overviews
  http://technet.microsoft.com/en-us/network/dd420463.aspx